The PMC Group LLC

Engineering a better tomorrow today

Cybersecuring DoD Facility-Related Control Systems

www.pmcgroup.biz

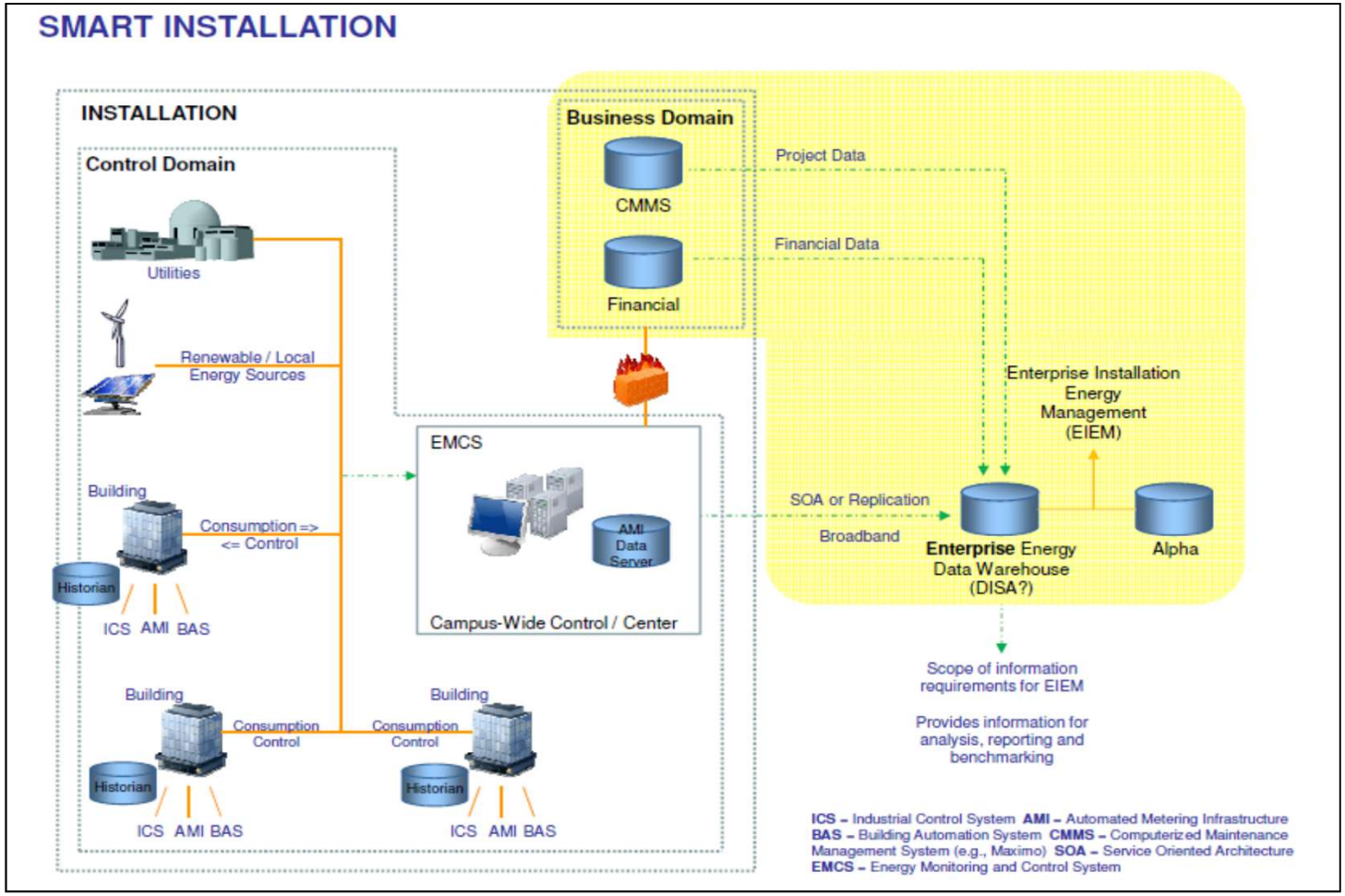
Workshop Overview

0800-0900	Unit 1 Overview of DoDI 8500/8510/8530 RMF and PIT FRCS, NIST Standards & Drivers, FRFRCS Protocols,
0900-1000	Unit 2 Hacker Methodology, Attacking and Defending, 1000-1015 Break
1015-1100	Unit 3 Footprinting FRCS using Whois, Google Hacking, Google Earth, Google Earth, BING, Shodan, Kali Linux, Control Things I/O, NMAP, GrassMarlin, Wireshark
1100-1200	Unit 4 UFC 4-010-06 Cybersecurity Of Facility-Related Control Systems, FRCS Reference Architecture, Platform Enclave, FRCS IA Contract Language for SME's, Test and Development Environment, FAT/SAT Checklist, Penetration Testing Checklist, Design/Construction Sequence TableHardening FRCS using Software Content Automation Program and Security Technical Implementation Guides
1200-1300	Lunch
1300-1330	Unit 5 Using CSET: SAL, Network Arch Diagram, Inventory, Templates, Security Controls Evaluation, Reports, Data Aggregation & Trending, System Security Plan
1330-1430	Unit 6 RMF KS Control Systems Webpage and eMASS demonstration, FRCS Master List and C-I-A, Using the Interim Excel files for uploading into eMASS
1430-1445	Break
1445-1545	Unit 7 Joint Mission Assurance Vulnerability Benchmarks; Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures; Forensics, Incident Reporting; Wrap Up Q&A

Unit 1

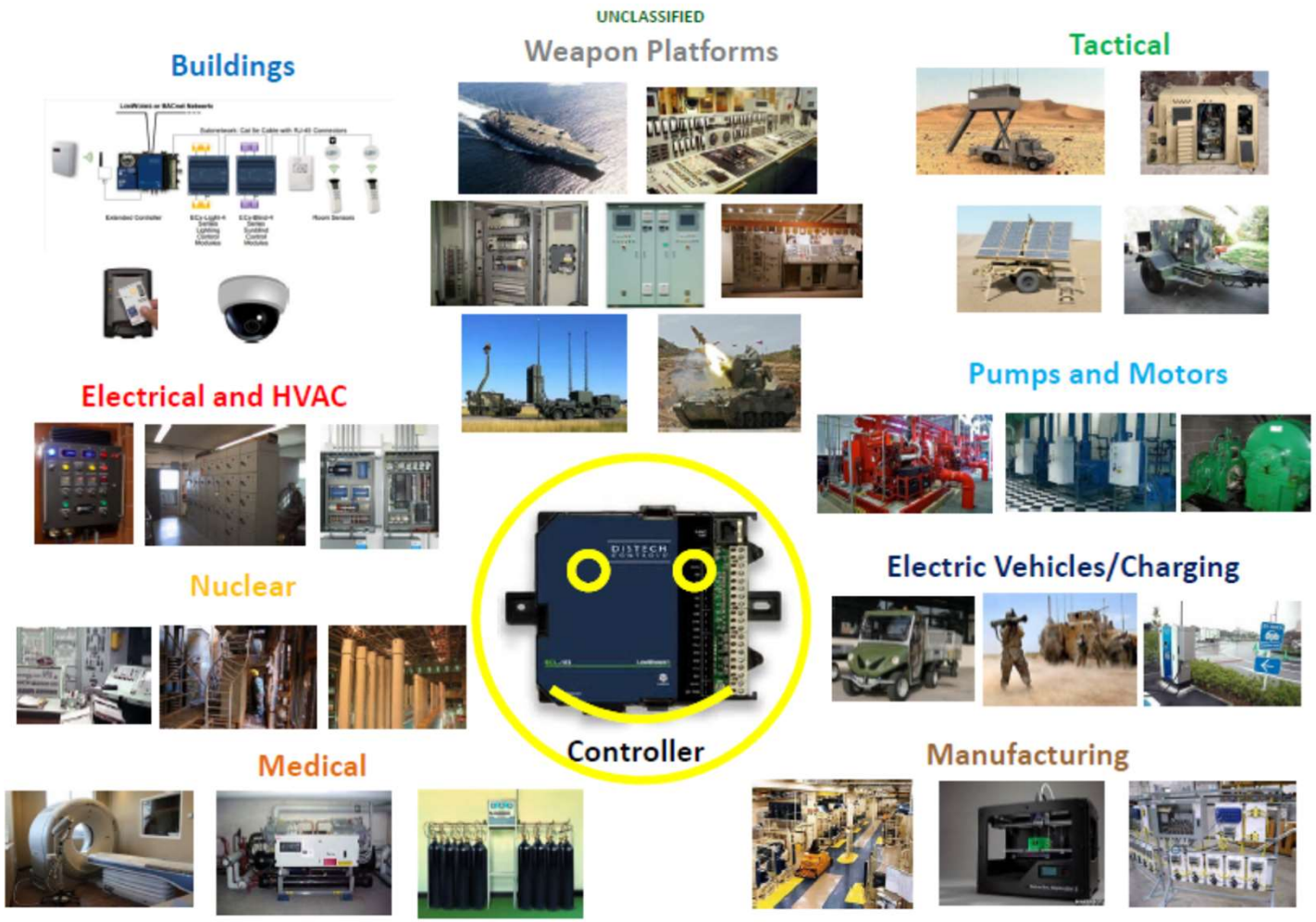
Overview of DoDI 8500/8510 RMF and PIT Control Systems, NIST Standards & Drivers, ICS Protocols

In the Beginning – Smart Installations



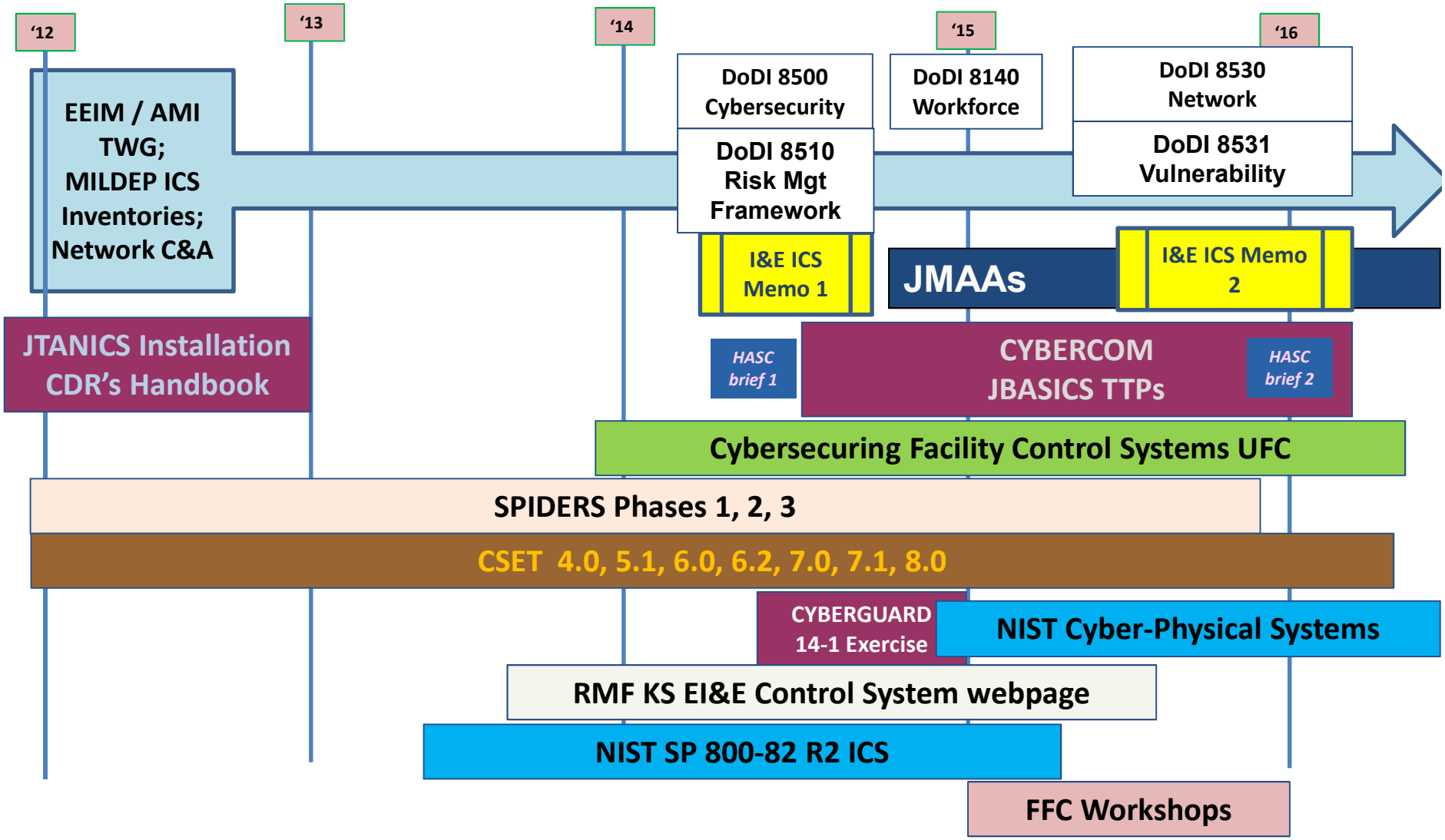
A great idea rudely interrupted by reality…CIO AMI ATO denial,… Stuxnet attack on Iranian Centrifuges, Flame, Duqu, Shamoon….

OT IP Based Controllers Are in Everything



Same Commercial Device Installed Across DoD Enterprise; PIT & PIT Systems

Broader DoD Cybersecurity Efforts 2012-2017



NDAA 2017

DoD facilities transitioning to smart buildings; increased connectivity has increased threat and vulnerability to cyber-attacks, particularly in ways existing DoD regulations were not designed to consider. Therefore, SECDEF deliver a report:

(1) Structural risks inherent in control systems and networks, and potential consequences associated with compromise through a cyber event;

(2) Assesses the current vulnerabilities to cyber attack initiated through Control Systems (FRCS) at DoD installations worldwide, determining risk mitigation actions for current and future implementation;

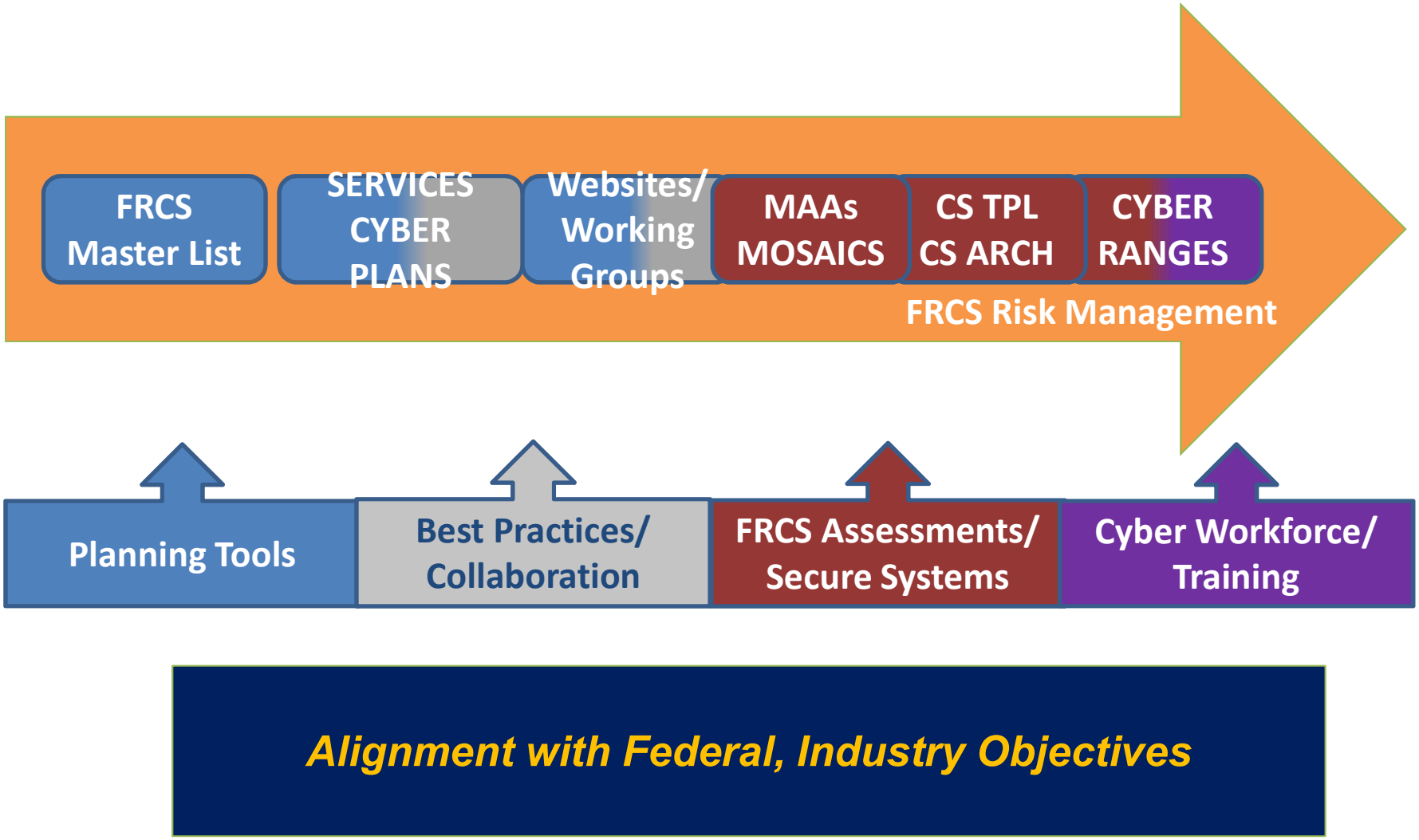
(3) Propose a common, DoD-wide implementation plan to upgrade & improve security of FRCS and networks to mitigate identified risks;

(4) Assesses DoD construction directives, regulations, and instructions; **require the consideration of cybersecurity vulnerabilities and cyber risk in preconstruction design processes and requirements development processes for military construction projects;** and

(5) Assess capabilities of Army Corps of Engineers, Naval Facilities Engineering Command, Air Force Civil Engineer Center, and other construction agents, as well as participating stakeholders, to **identify and mitigate full-spectrum cyber-enabled risk to new facilities and major renovations.**

FRCS include, but are not limited to, **Supervisory Control and Data Acquisition Systems, Building Automation Systems Utility Monitoring and Energy Management and Control Systems.** Such report shall include an estimated budget for the implementation plan, and delivered no later than **180 days** after the date of the enactment of this Act.

ODASD(E) Cybersecurity Initiatives 2019



Alignment with Federal, Industry Objectives

DoD FRCS Cyber Plans 2016, 2018

DoD FRCS Cyber Plans 2016, 18…

ASSISTANT SECRETARY OF DEFENSE

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Facility-Related Control Systems (FRCS) Cybersecurity Plan Updates

Cyber vulnerabilities continue to jeopardize critical infrastructure that enables DoD operations. Unsecured Facility-Related Control Systems (FRCS) can expose connected DoD information networks to risk. Over the past year, we've seen increased activity throughout the Department towards cyber securing mission critical FRCS. DoD Components are, to varying degrees, planning, programming, budgeting, and executing measures to develop enhanced cyber hardening and risk reduction plans to detect, mitigate, and recover their systems and information from the advanced, persistent cyber threat.

The purpose of this memorandum is to request updated DoD Component FRCS Cybersecurity Plans that cover Fiscal Years (FY) 2016-2023. To gauge progress, I am also requesting information on accomplishments during FY2016-2017. You should give priority to completing Plans by the end of FY 2019 for the most critical FRCS with particular emphasis on:

(1) FRCS supporting Defense Critical Assets and Tier 1 Task Critical Assets.
(2) FRCS that connect to the DoD Information Network (DoDIN), are internet-facing or stand-alone (Closed Restricted Network (CRN)), and which require an Authorization to Operate (ATO).

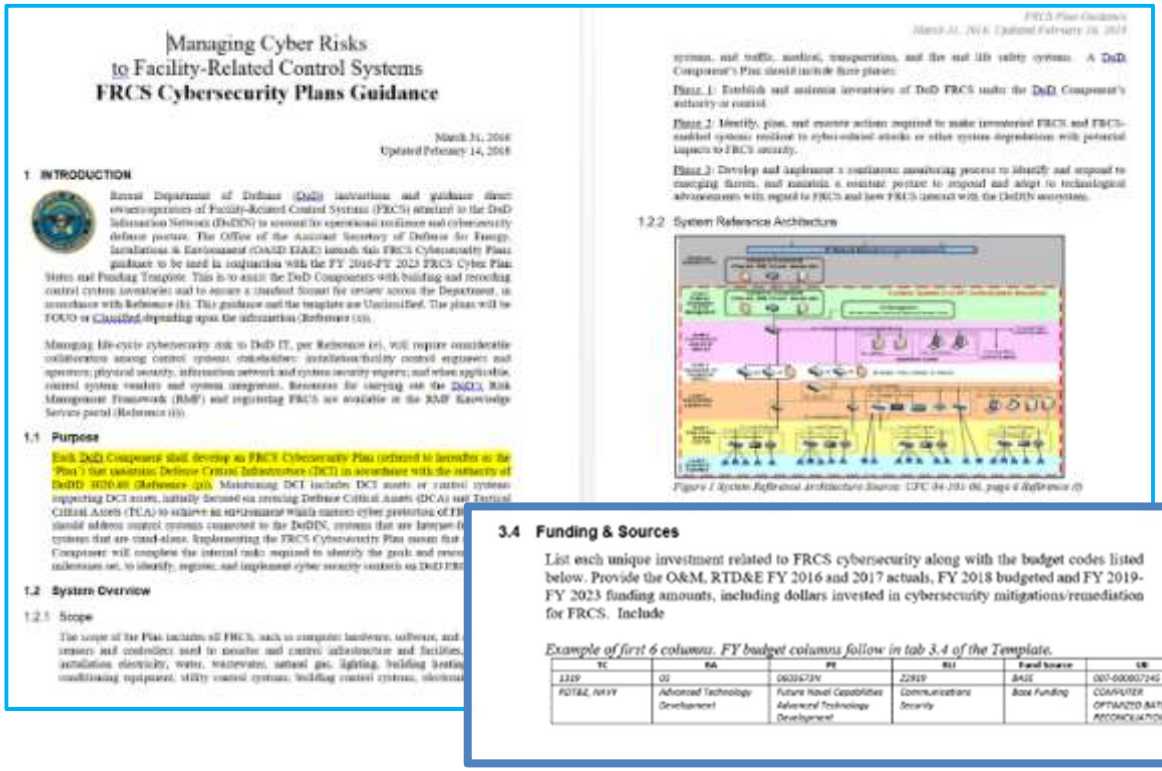
Attachment A provides guidance for formulating your FRCS Cybersecurity Plans. Attachment B provides a recommended template. The template may be used for submission, but previous formats are acceptable, if updated to include the new and updated plan requirements. Note that in addition to the previous plan submissions, this data call requires submission of new content.

Please submit all FRCS Cyber Plans to my point of contact, Mr. Daryl Hingley, daryl.s.hingley.civ@mail.mil (571) 372-6857 by July 31, 2018.

Thank you for your continued support to improve FRCS resilience and security posture.

Louis Numayer

ATTACHMENTS:
(A) Managing Cyber Risks to Facility-Related Control Systems FRCS Cybersecurity Plans Guidance, February 14, 2018
(B) FY 2018-FY 2023 FRCS Cybersecurity Plan Status and Funding Template



Managing Cyber Risks
to Facility-Related Control Systems
FRCS Cybersecurity Plans Guidance

March 31, 2018
Updated February 14, 2018

1 INTRODUCTION

Recent Department of Defense (DoD) instructions and guidance direct owners/operators of Facility-Related Control Systems (FRCS) attached to the DoD Information Network (DoDIN) to account for operational resilience and cybersecurity defense posture. The Office of the Assistant Secretary of Defense for Energy, Installations & Environment (OASD EI&E) intends this FRCS Cybersecurity Plans guidance to be used in conjunction with the FY 2016-FY 2023 FRCS Cyber Plan Status and Funding Template. This is to assist the DoD Components with building and recording control system inventories and to ensure a standard format for review across the Department, in accordance with Reference (b). This guidance and the template are Unclassified. The plans will be FOUO or Classified depending upon the information (Reference (c)).

Managing life-cycle cybersecurity risk to DoD IT, per Reference (e), will require considerable collaboration among control systems stakeholders: installation/facility control engineers and operators; physical security, information network and systems security experts; and when applicable, control systems vendors and system integrators. Resources for carrying out the DoD's Risk Management Framework (RMF) and registering FRCS are available in the RMF Knowledge Services portal (Reference (i)).

1.1 Purpose

Each DoD Component shall develop an FRCS Cybersecurity Plan (referred to hereafter as the "Plan") that identifies Defense Critical Infrastructure (DCI) in accordance with the authority of DoDD 3020.40 (Reference (a)). Maintaining DCI includes DCI assets or control systems supporting DCI assets, initially focused on securing Defense Critical Assets (DCAs) and Tactical Critical Assets (TCAs) to achieve an environment which ensures cyber protection of FRCS should address control systems connected to the DoDIN, systems that are hardwired to systems that are stand-alone. Implementing the FRCS Cybersecurity Plan means that each Component will complete the internal tasks required to identify the goals and review milestones set, to identify, register, and implement cyber security controls on DoD FRCS.

1.2 System Overview

1.2.1 Scope

The scope of the Plan includes all FRCS, such as computer hardware, software, and sensors and controllers used to monitor and control infrastructure and facilities, installation electricity, water, wastewater, natural gas, lighting, building heating, conditioning equipment, utility control systems, building control systems, electronic

FRCS Plan Guidance
March 31, 2018, Updated February 14, 2018

systems, and traffic, medical, transportation, and fire and life safety systems. A DoD Component's Plan should include three phases:

Phase 1: Establish and maintain inventories of DoD FRCS under the DoD Component's authority or control.

Phase 2: Identify, plan, and execute actions required to make inventoried FRCS and FRCS-enabled systems resilient to cyber-related attacks or other system degradations with potential impacts to FRCS security.

Phase 3: Develop and implement a continuous monitoring process to identify and respond to emerging threats, and maintain a constant posture to respond and adapt to technological advancements with regard to FRCS and how FRCS interact with the DoDIN ecosystem.

1.2.2 System Reference Architecture

Figure 1 System Reference Architecture Source: UFC 04-010 06, page 6 Reference (f)

3.4 Funding & Sources

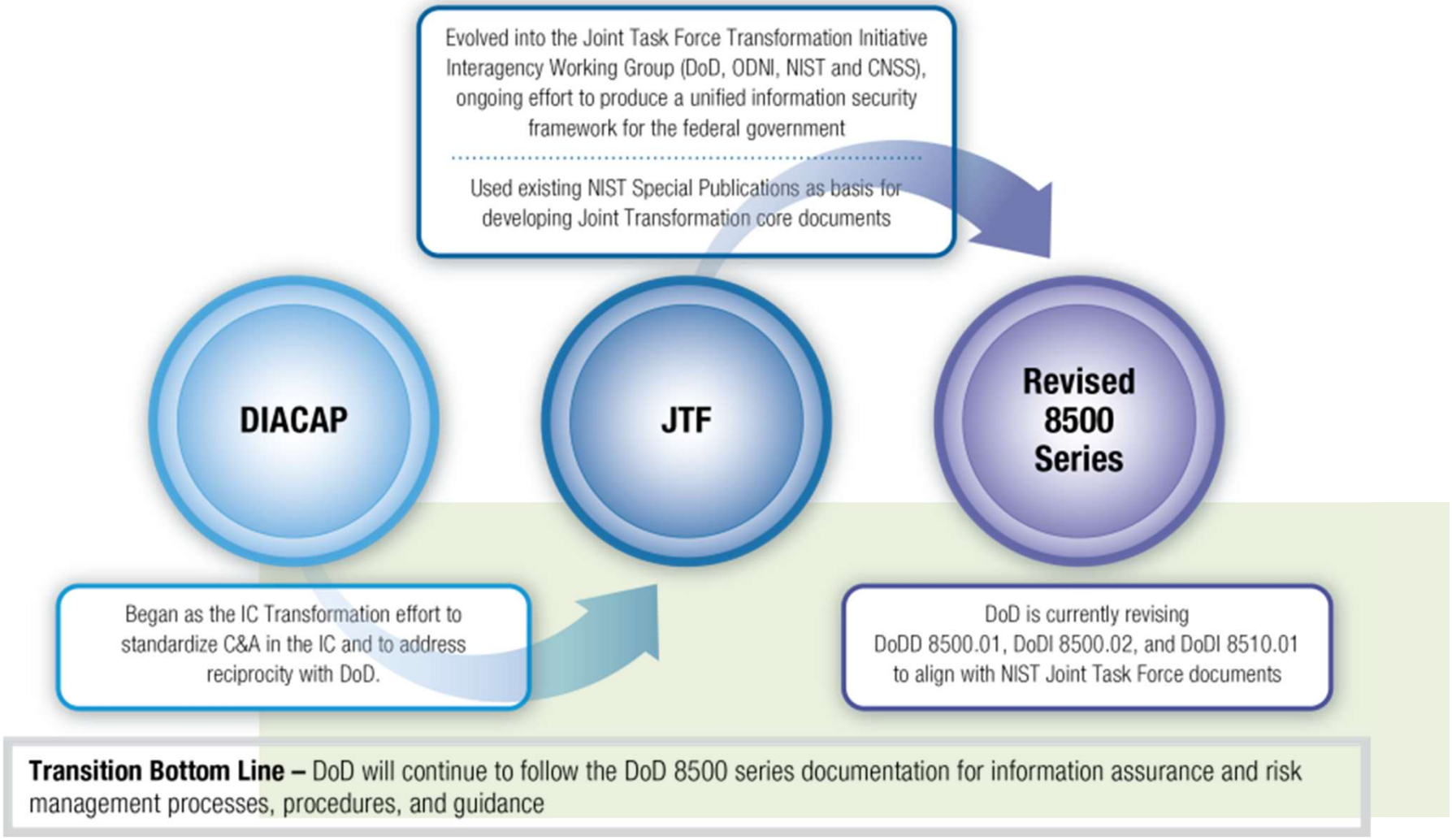
List each unique investment related to FRCS cybersecurity along with the budget codes listed below. Provide the O&M, RTD&E FY 2016 and 2017 actuals, FY 2018 budgeted and FY 2019-FY 2023 funding amounts, including dollars invested in cybersecurity mitigations/remediation for FRCS. Include

Example of first 6 columns. FY budget columns follow in tab 3.4 of the Template.

TC	BA	PE	BLI	Fund Source	UR
1319	03	0603673N	22959	BASE	007-000007245
RDT&E, NAVY	Advanced Technology Development	Future Naval Capabilities Advanced Technology Development	Communications Security	Base Funding	COMPUTER OPTIMIZED BATCH RECONCILIATION

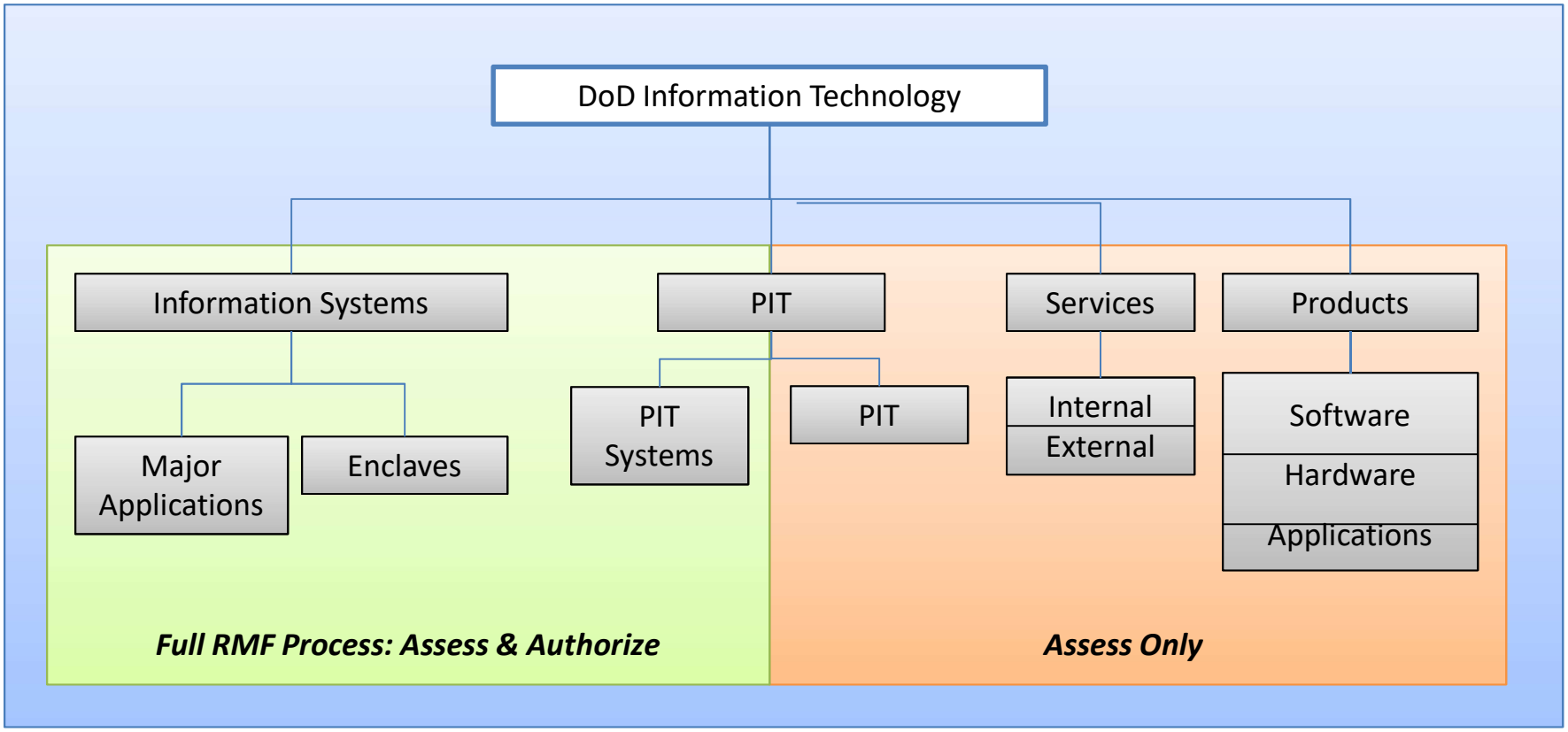
Is Your FRCS Cyber Plan Adequately Resourced?

DoDI 8500.01 and 8510.01 Update



RMF for DoD IT

DoDI 8510.01 "Risk Management Framework for DoD IT"
- Provides clarity regarding what IT should undergo the RMF process and how



New: Assess and Evaluate

8500 PIT Cybersecurity Considerations

(2) PIT

(a) All PIT has cybersecurity considerations. The Defense cybersecurity program only addresses the protection of the IT included in the platform. See Reference (ah) for PIT cybersecurity requirements.

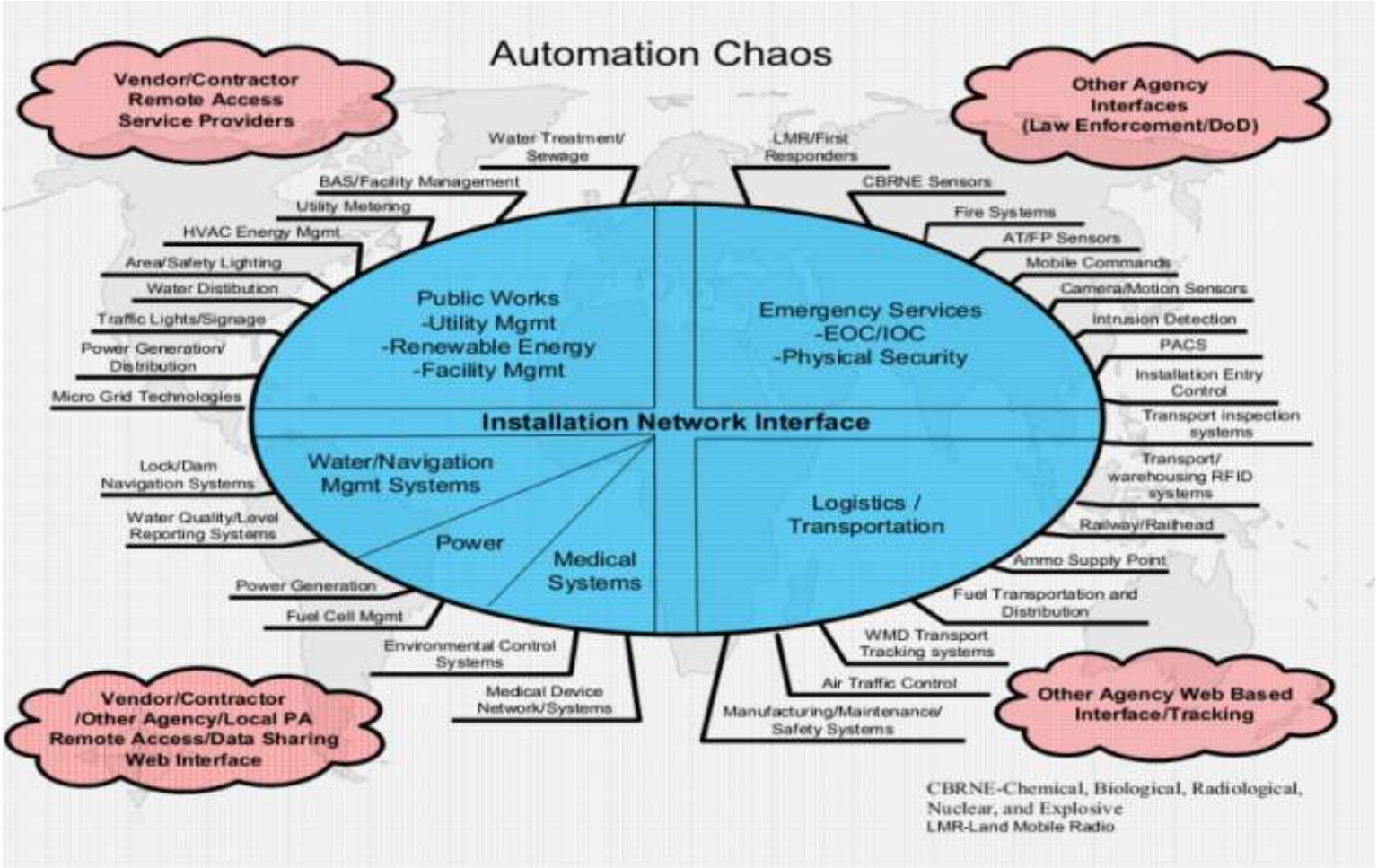
(b) Examples of platforms that may include PIT are: weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), **buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for industrial control systems to include supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering,** including associated data transport mechanisms (e.g., data links, dedicated networks).

8500 PIT Systems

(d) PIT Systems

1. Owners of special purpose systems (i.e., platforms), in consultation with an AO, may determine that a **collection of PIT rises to the level of a PIT system. PIT systems are analogous to enclaves but are dedicated only to the platforms they support.** PIT systems must be designated as such by the responsible OSD or DoD Component heads or their delegates and authorized by an AO specifically appointed to authorize PIT systems.

DoD ICS Complexity – Many Systems



Courtesy of Fred Abbitt USACE

DoD alone has more than 2.5 million unique FRCS systems

DoD Facility-Related Control Systems (FRCS)

Categories

- Airfield Systems
- Building Control System
- Dam, Lock and Levee Systems
- Electronic Security Systems
- Environmental Monitoring
- Fire & Life Safety
- Pier Systems
- Traffic Control Systems
- Transportation & Fueling Systems
- Utility Control Systems
- Utility Monitoring & Control Systems
- Control System Platform Enclave

Systems

- Building Automation System
- Building Lighting System
- Conveyance/Vertical Transport System
- Electrical Systems
- Heating, Ventilation, Air Conditioning
- Irrigation System
- Shade Control System
- Vehicle Charging System
- Cathodic Protection Systems
- Compressed Air (Or Compressed Gases) System
- Central Plant (District) Chilled Water System
- Central Plant (District) Electrical Power Production
- Central Plant (District) Hot Water System
- Central Plant (District) Steam System
- Electrical Distribution System
- Gray Water System
- Industrial Waste Treatment System
- Microgrid Control Systems
- Natural Gas System
- Oily Water/Waste Oil System
- Potable Water System
- Pure Water System
- Salt Water System
- Sanitary Sewer/Wastewater System
- Utility Metering System (Advanced Meters, AMI, etc.)
- *Many More…*

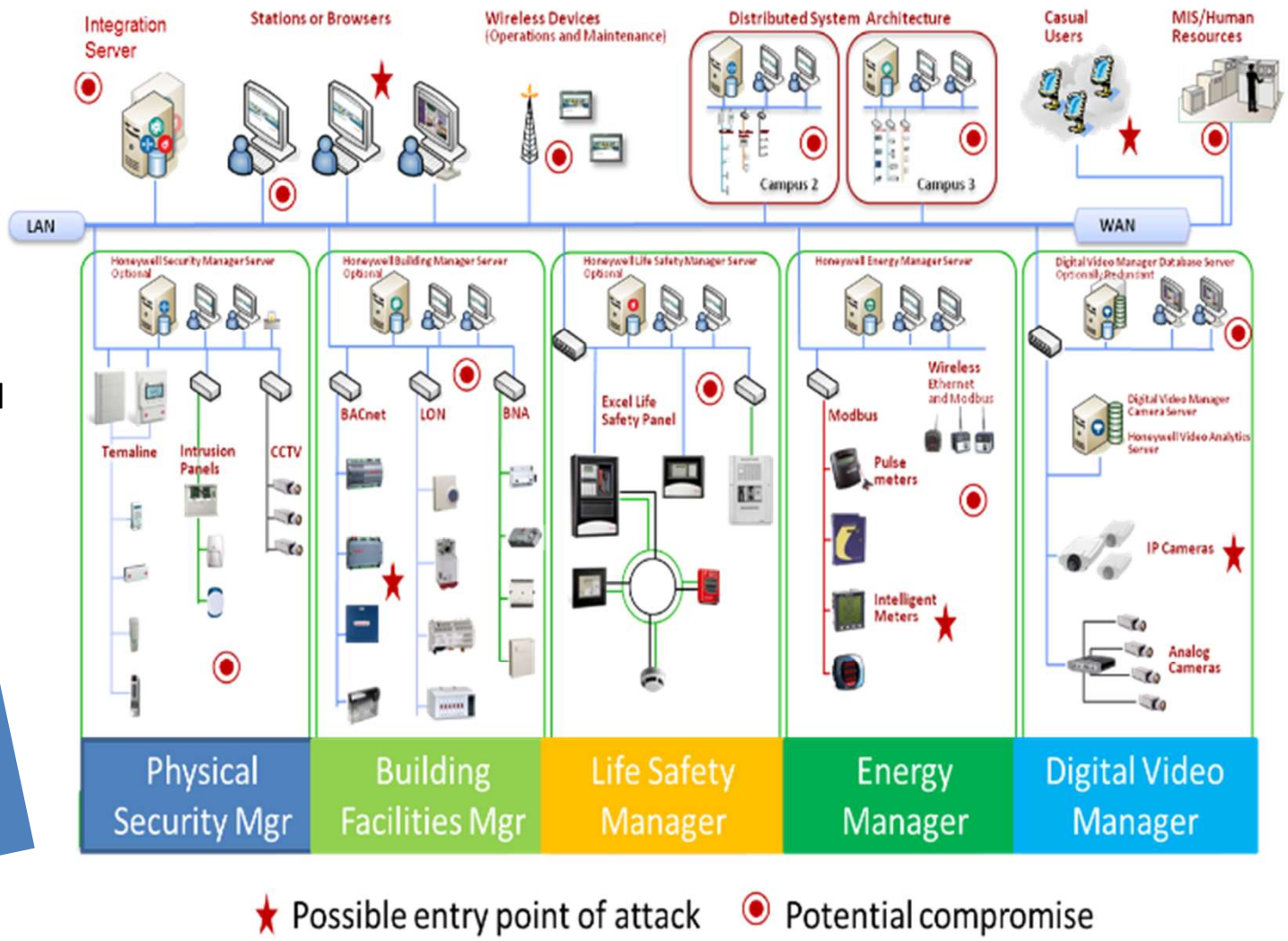
DoD Control Systems are just as vulnerable as industry, how do we protect them?

DoD Building FRCS

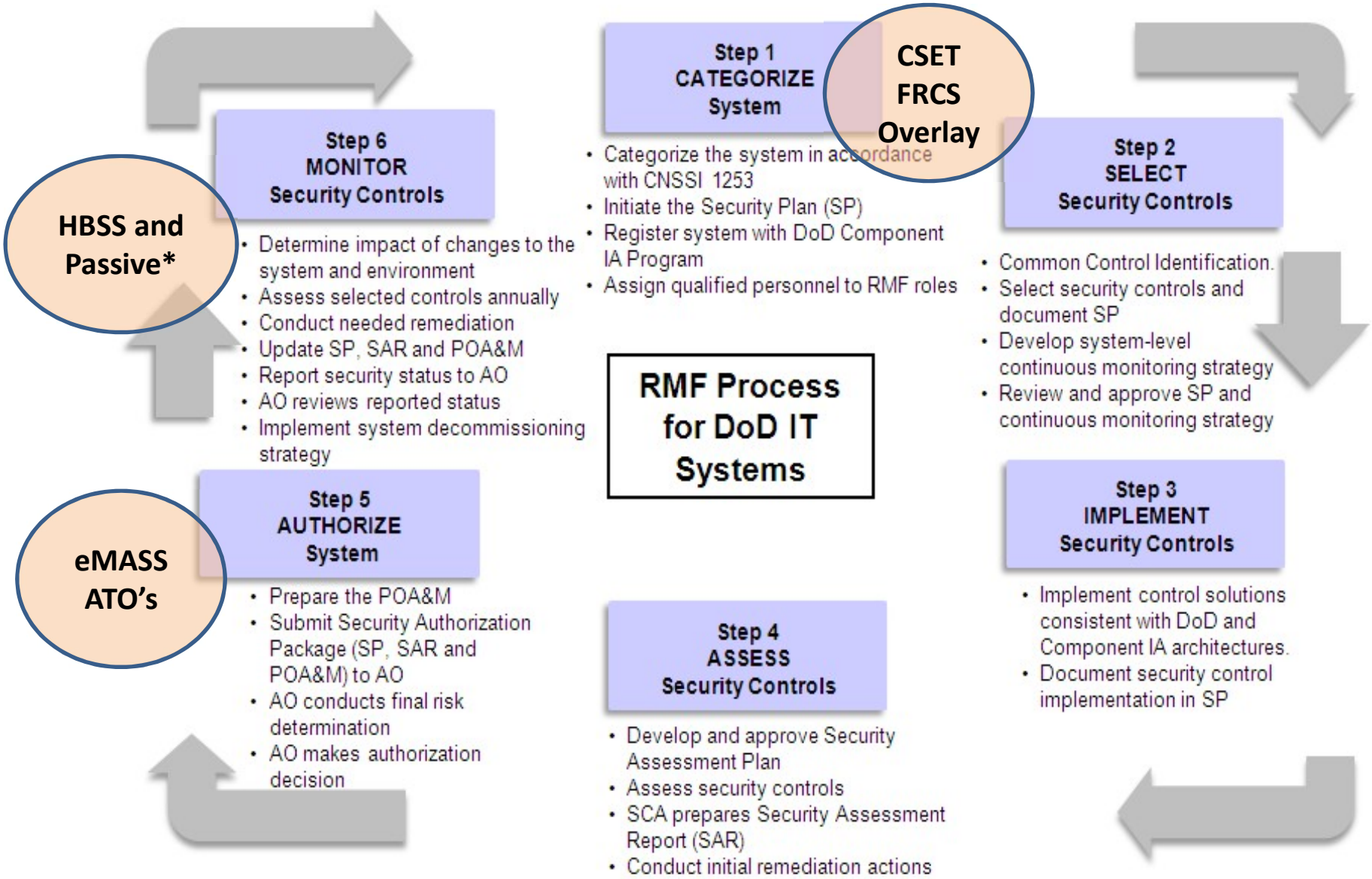
DoD
Real Property
Portfolio

- 48 countries
- 523 installations
- 4,855 Sites
- 562,600 buildings and structures
- 24.7 M acres
- $847 B value

What's in Your Building?



FRCS Overlay & RMF Implementation

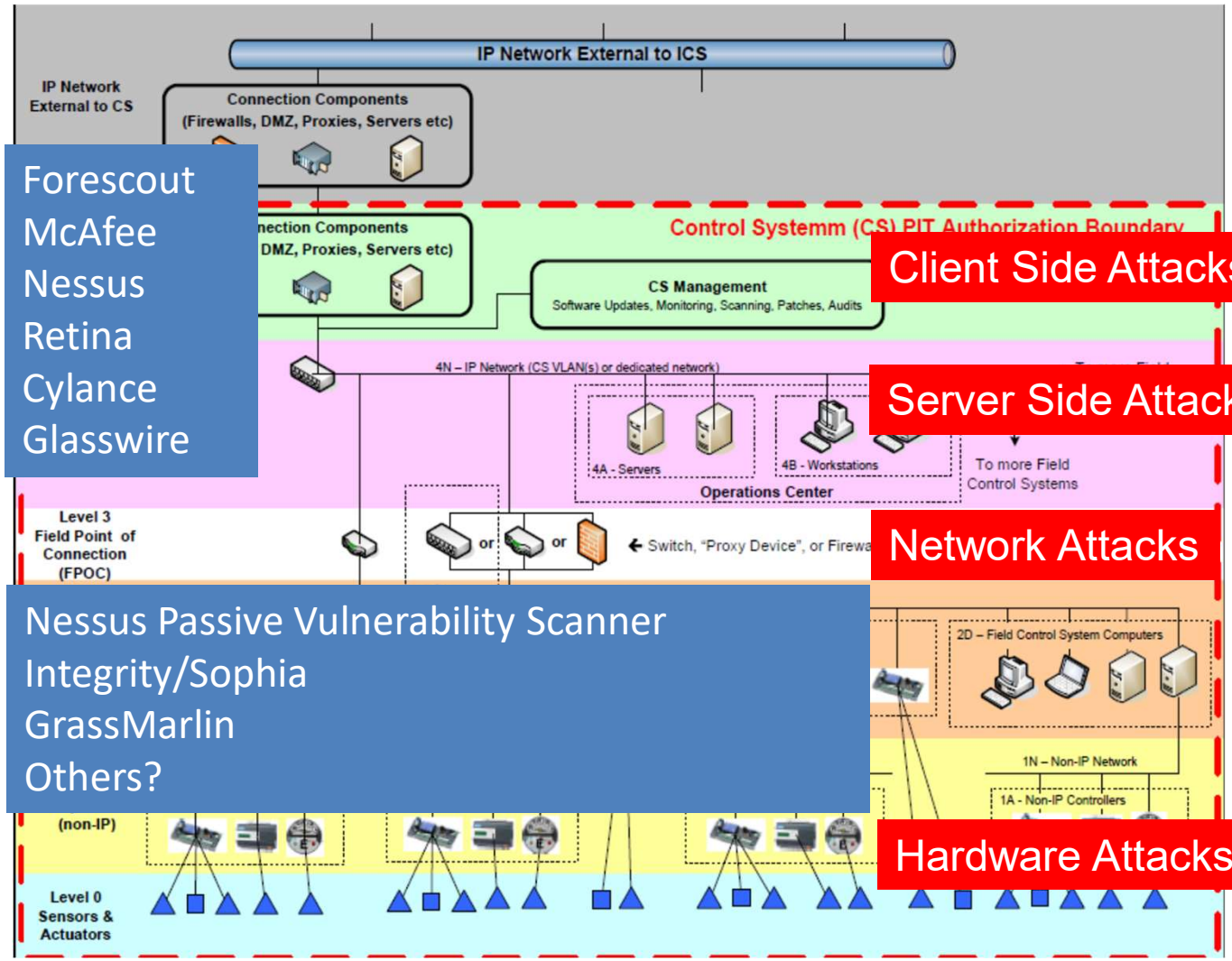


Continuous Monitoring and Attack Surfaces

Host Based
Security Systems
Scanning (Active)

Windows, Linux
HTTP, TCP, UDP

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



Forescout
McAfee
Nessus
Retina
Cylance
Glasswire

Client Side Attacks

Server Side Attacks

Network Attacks

Nessus Passive Vulnerability Scanner
Integrity/Sophia
GrassMarlin
Others?

Hardware Attacks

Standards – NIST SP 800-82 R2


NIST Special Publication 800-82
Revision 1

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Joe Falco
Karen Scarfone

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DFRCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors.

This document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

800-82 Rev 2 was released May 2015 – has 800-53 Rev 4 800+ controls,
Appendix G ICS Overlay

NIST SP 800-82 R2 Key Security Controls

Inventory
- CM-8 Information System Component Inventory
- PM-5 Information System Inventory
- PL-7 Security Concept of Operations
- PL-8 Information Security Architecture
- SC-41 Port and I/O Device Access
- PM-5 Information System Inventory

Central Monitoring
- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- IR-5 Incident Monitoring
- IR-6 Incident Reporting
- PE-6 Monitoring Physical Access
- PM-14 Testing, Training and Monitoring
- RA-5 Vulnerability Scanning
- SC-7 Boundary Protection
- SI-4 Information System Monitoring
- SI-5 Security Alerts, Advisories, and Directives

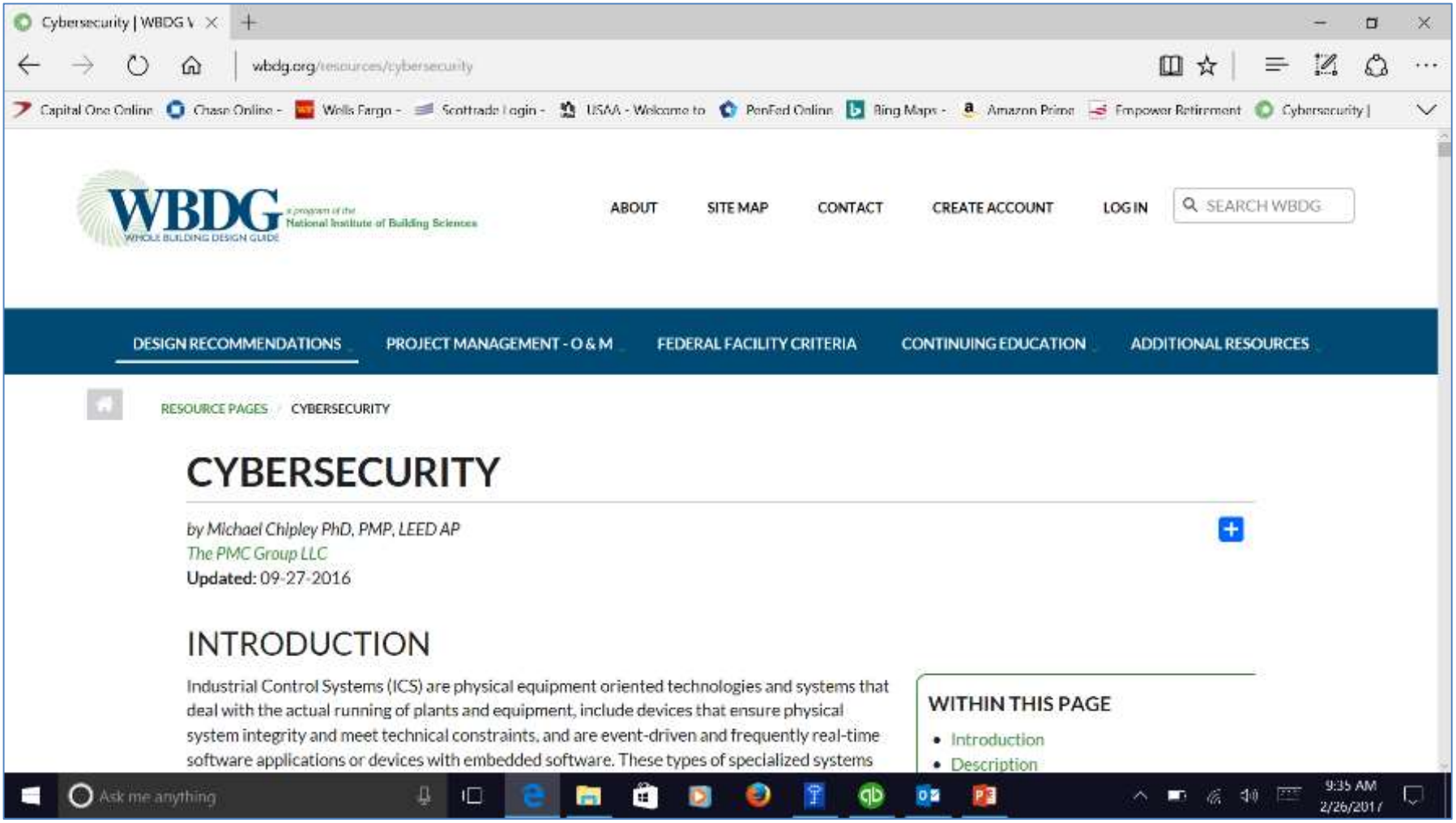
Test and Development Environment
- CA-8 Penetration Testing
- CM-4 Security Impact Analysis
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- PM-14 Testing, Training and Monitoring

Critical Infrastructure
- CP-2 Contingency Plan
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-10 Information System Recovery and Reconstitution
- PE-3 Physical Access Control
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-12 Emergency Lighting
- PE-13 Fire Protection
- PE-14 Temperature and Humidity Controls
- PE-17 Alternate Work Site
- PM-8 Critical Infrastructure Plan

Acquisition and Contracts
- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- SA-4 Acquisitions
- PM-3 Information System Resources
- PM-14 Testing, Training and Monitoring

Inbound Protection, Outbound Detection

WBDG Cybersecurity Resource Page



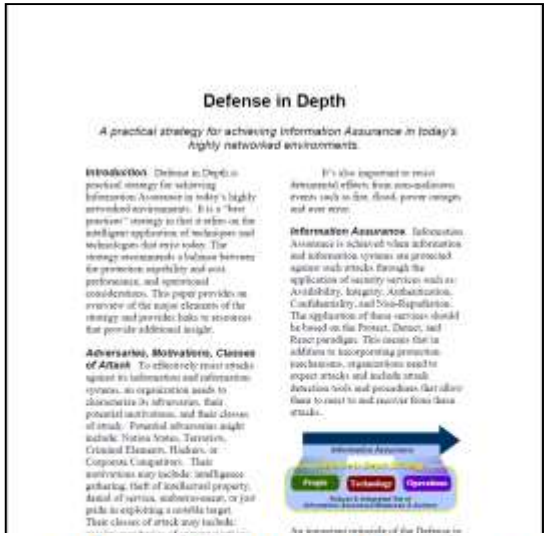
http://www.wbdg.org/resources/cybersecurity.php

Defense in Depth

The underlying principal of Defense in Depth addresses IA needs with **people** executing **operations** supported by **technology**.

Defense in Depth recommends a balance between capability, cost, performance, and operational considerations. An organization must deploy protection mechanisms as multiple locations to resist all methods of attack. - Layered Defense (CJFRCSI 6510.01D)

The Defense in Depth strategy focuses on four key areas:
Defend the Network and Infrastructure
Defend the Enclave Boundary
Defend the Computing Environment
Supporting Infrastructures (PKI, CAC)


Defense in Depth

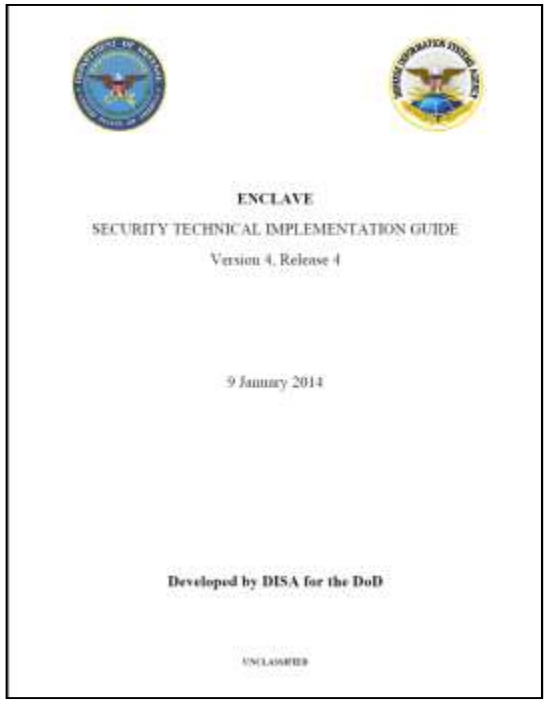
A practical strategy for achieving Information Assurance in today's highly networked environments.

Examples of Layered Defenses

Class of Attack	*First Line of Defense*	*Second Line of Defense*
Passive	Link & Network Layer Encryption and Traffic Flow Security	Security Enabled Applications
Active	Defend the Enclave Boundaries	Defend the Computing Environment
Insider	Physical and Personnel Security	Authenticated Access Controls, Audit
Close-In	Physical and Personnel Security	Technical Surveillance Countermeasures
Distribution	Trusted Software Development and Distribution	Run Time Integrity Controls

http://issep.wikifoundry.com/page/Defense+in+Depth

DoD Enclaves



ENCLAVE

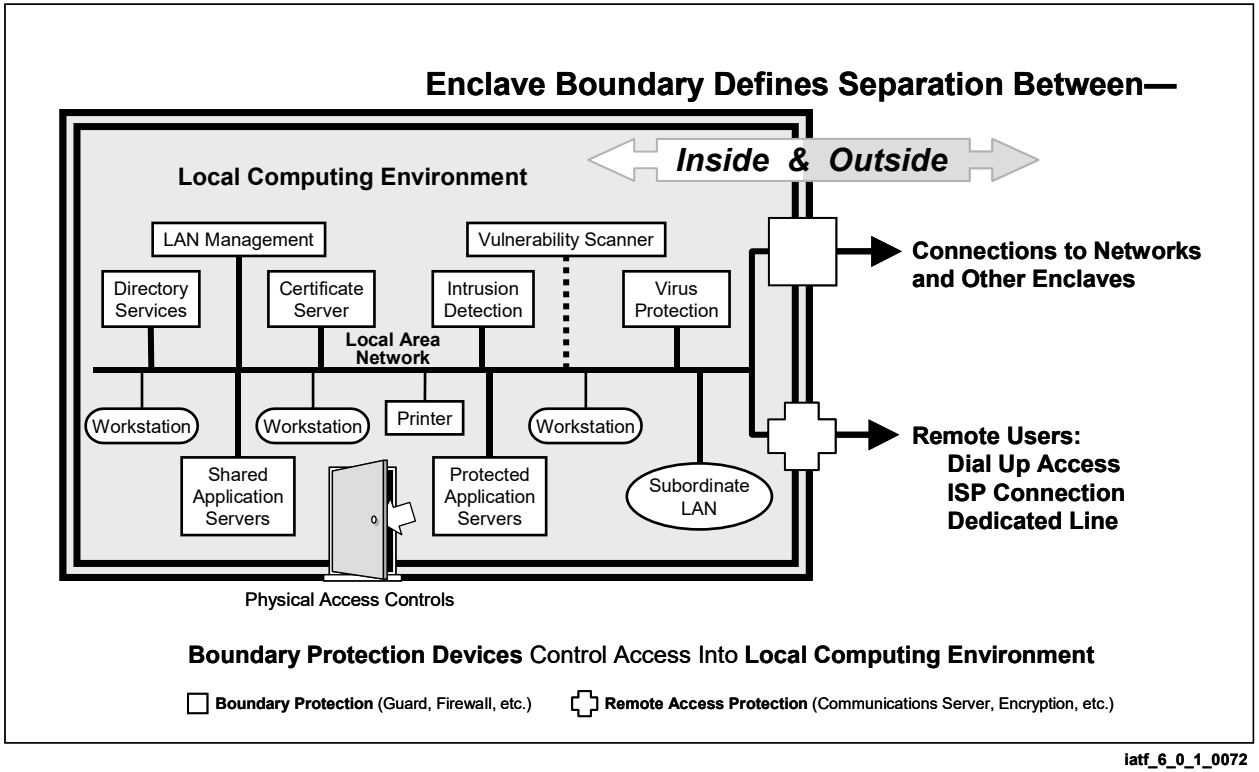
SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 4, Release 4

9 January 2014

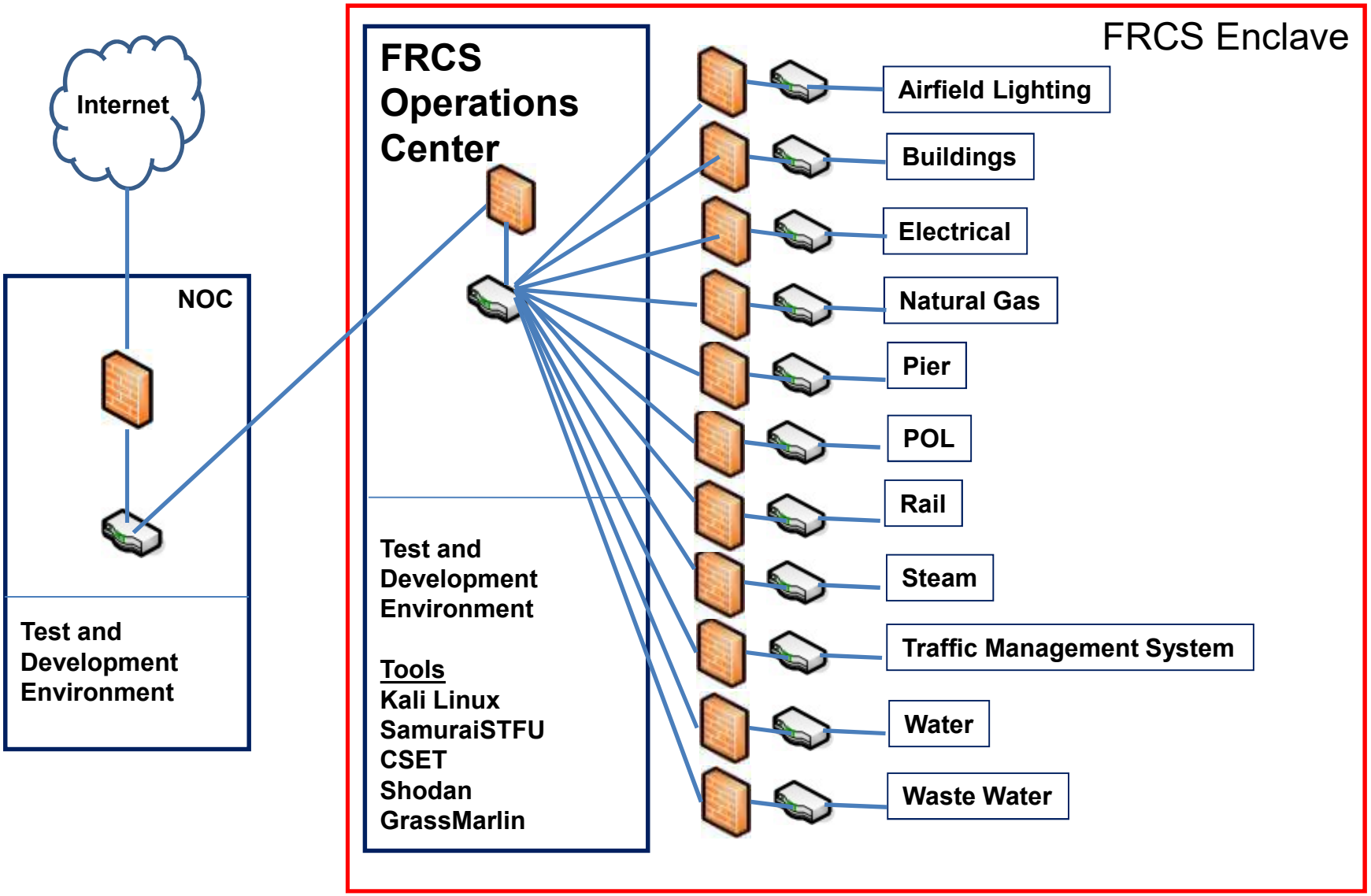
Developed by DISA for the DoD

UNCLASSIFIED

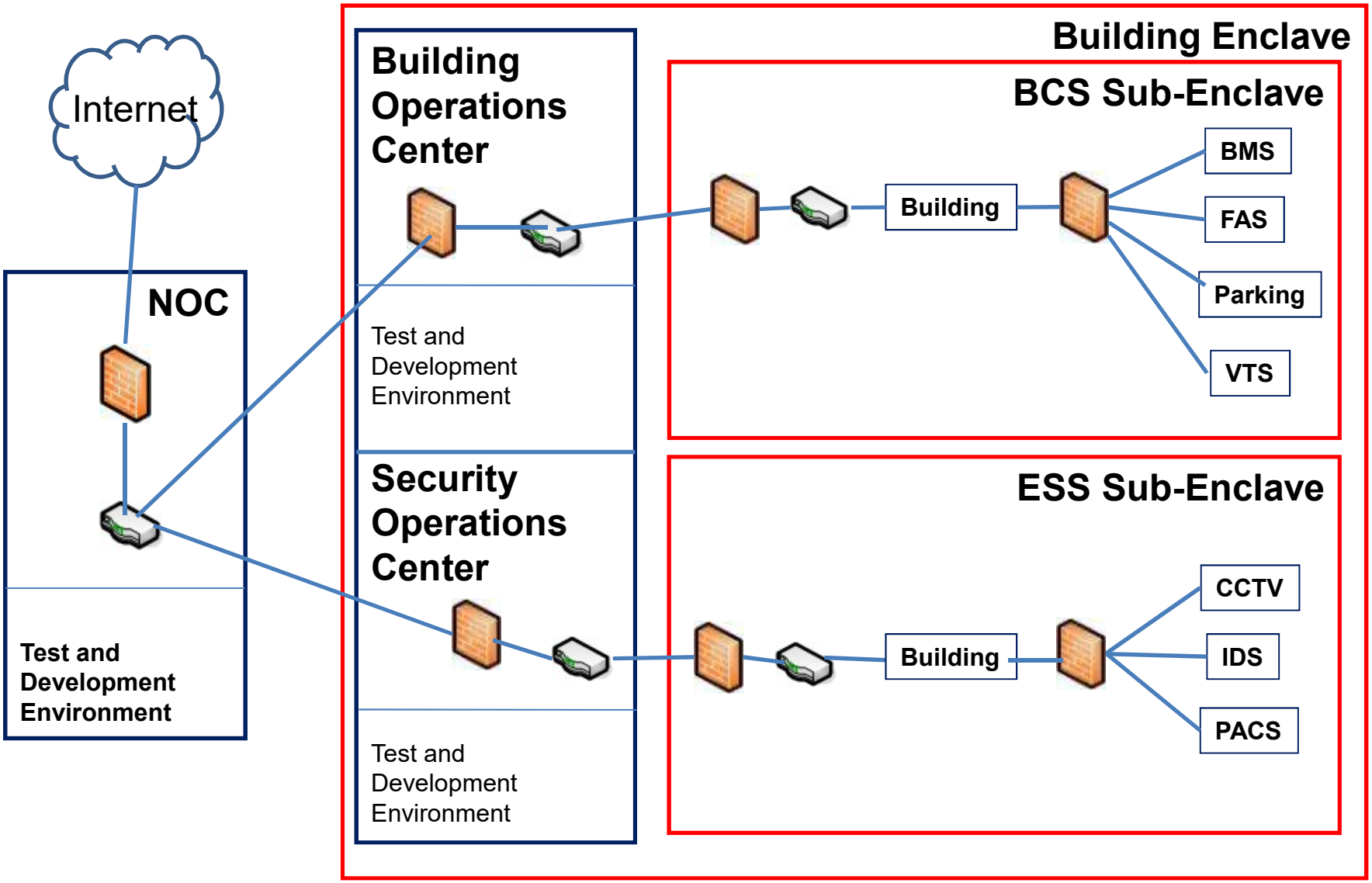


An enclave is an environment under the control of a single authority with personnel and physical security measures. Enclaves typically contain multiple local area networks (LAN) with computing resource components such as user platforms; network, application, and communication servers; printers; and local switching/routing equipment.

Numerous Sub-Enclaves

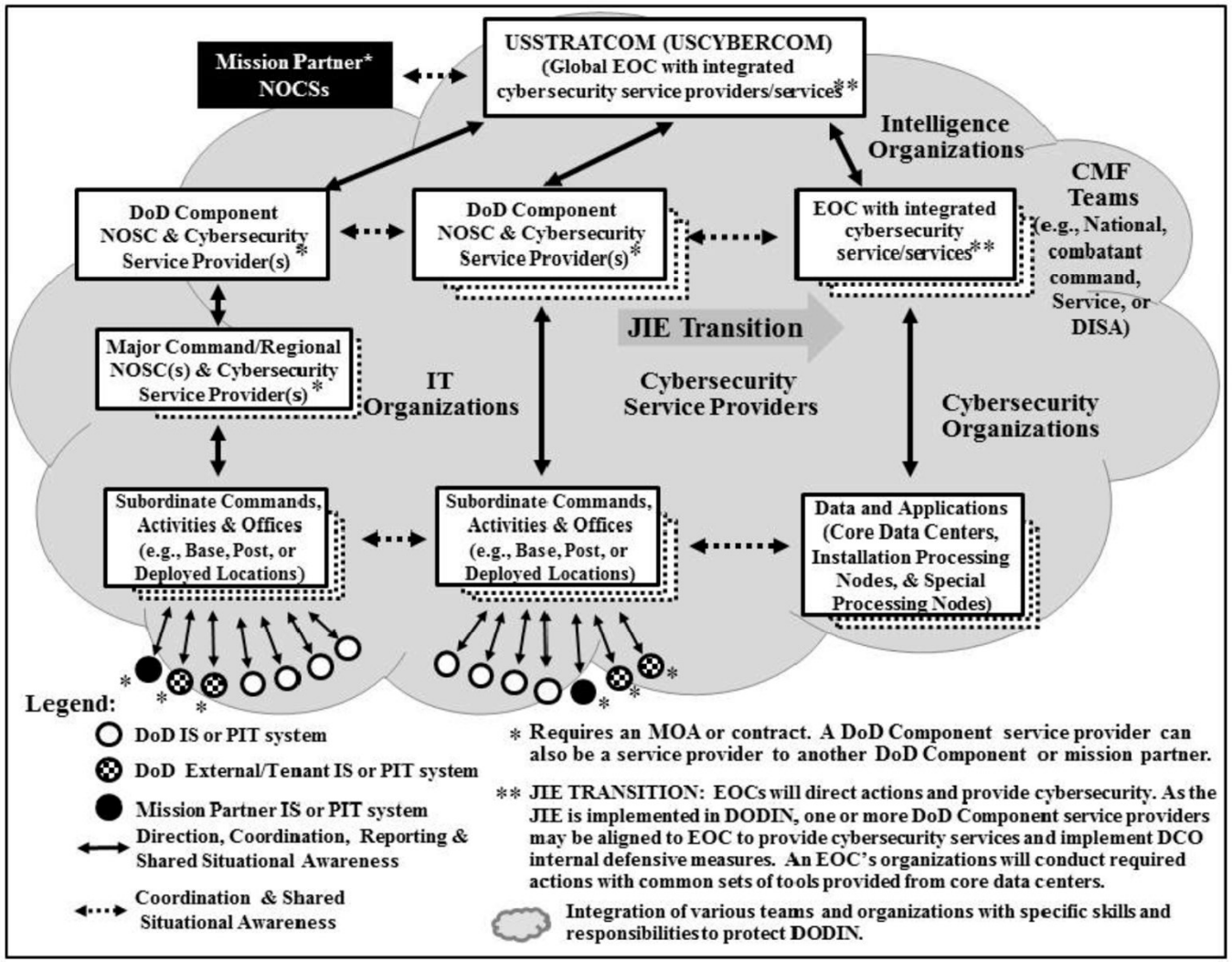


Hybrid FRCS and Security Enclaves

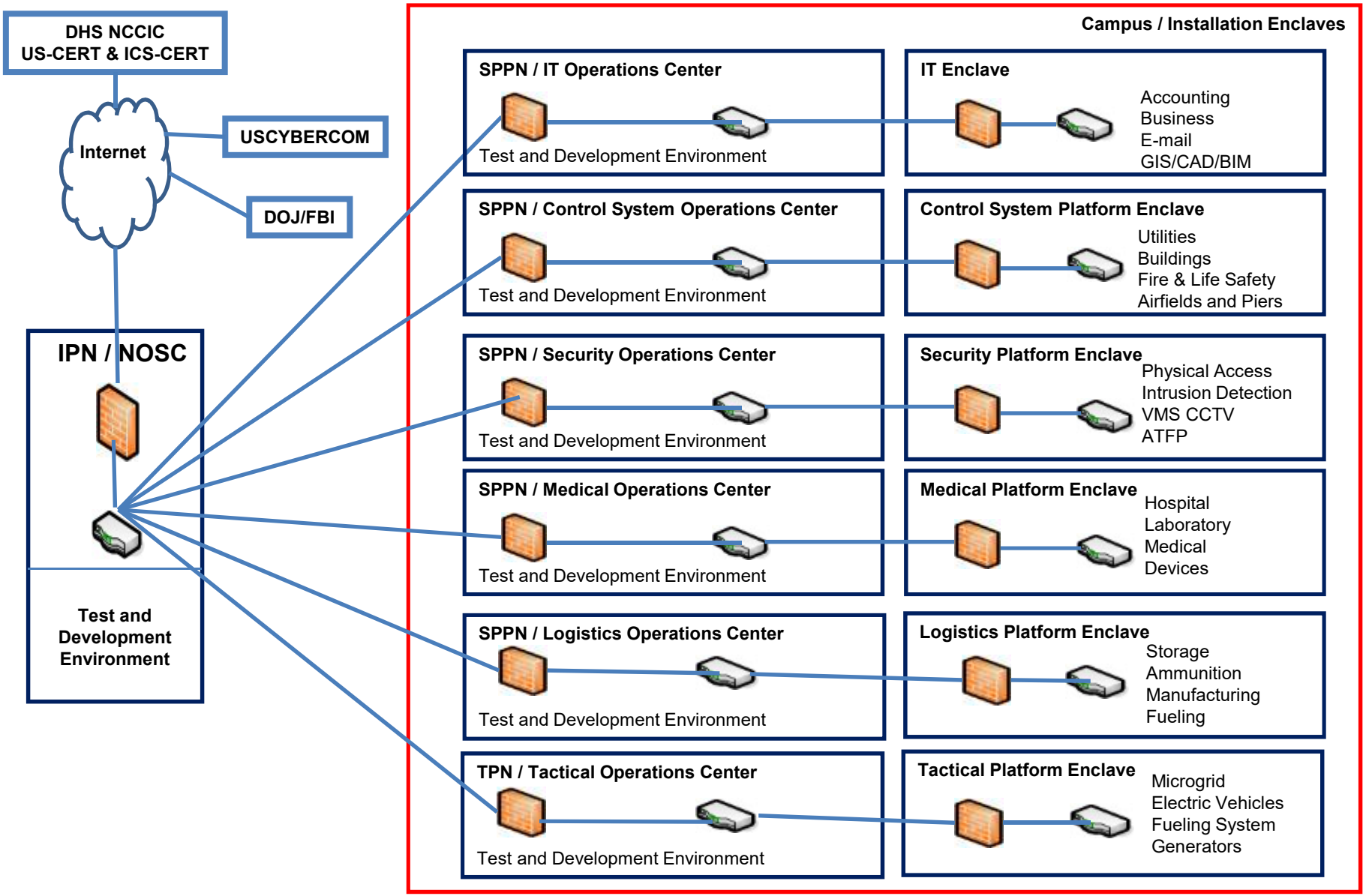


DODI 8530 - JIE

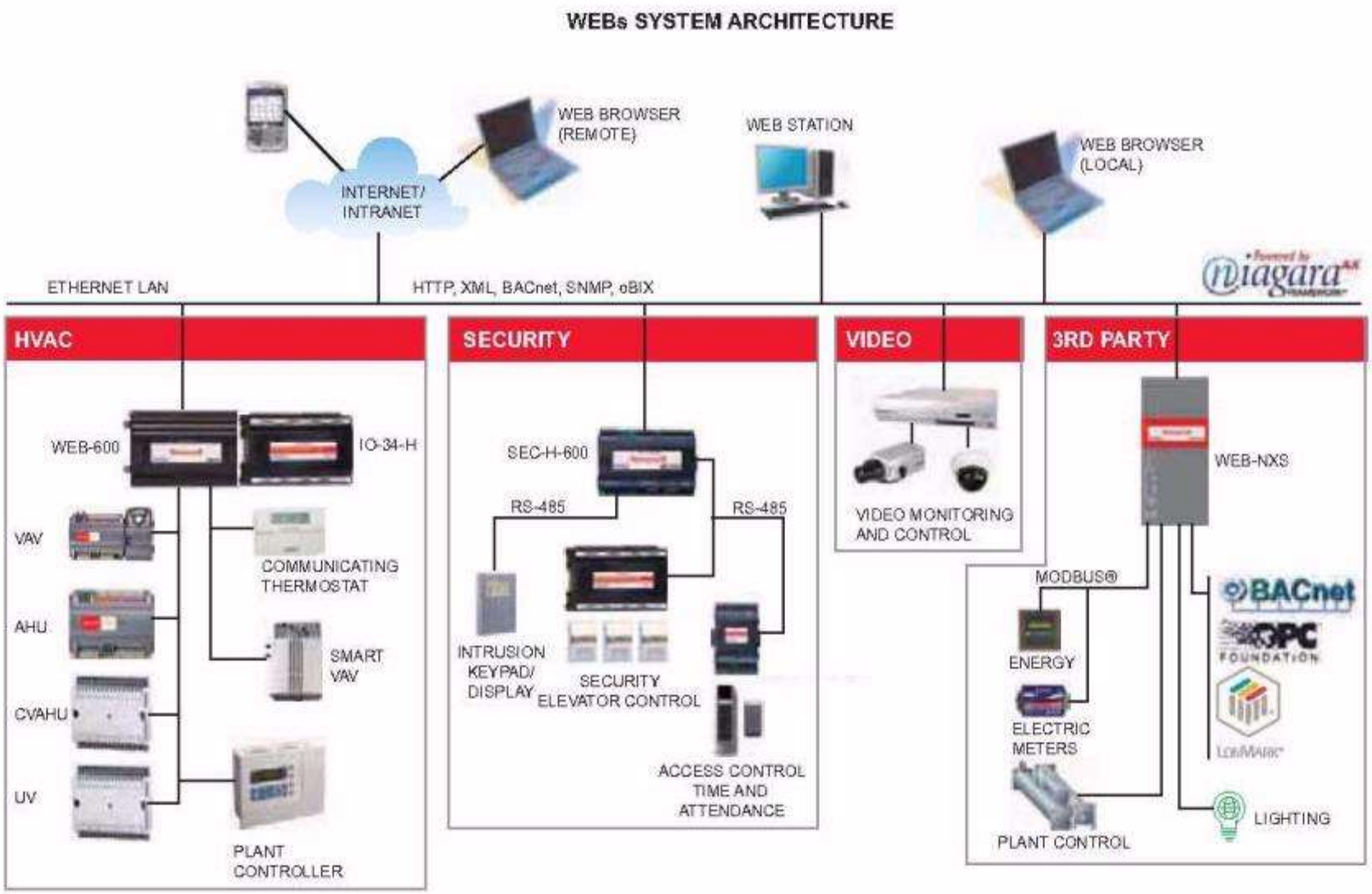
Figure 2. Notional View of Current and Future Integration of Cybersecurity Activities



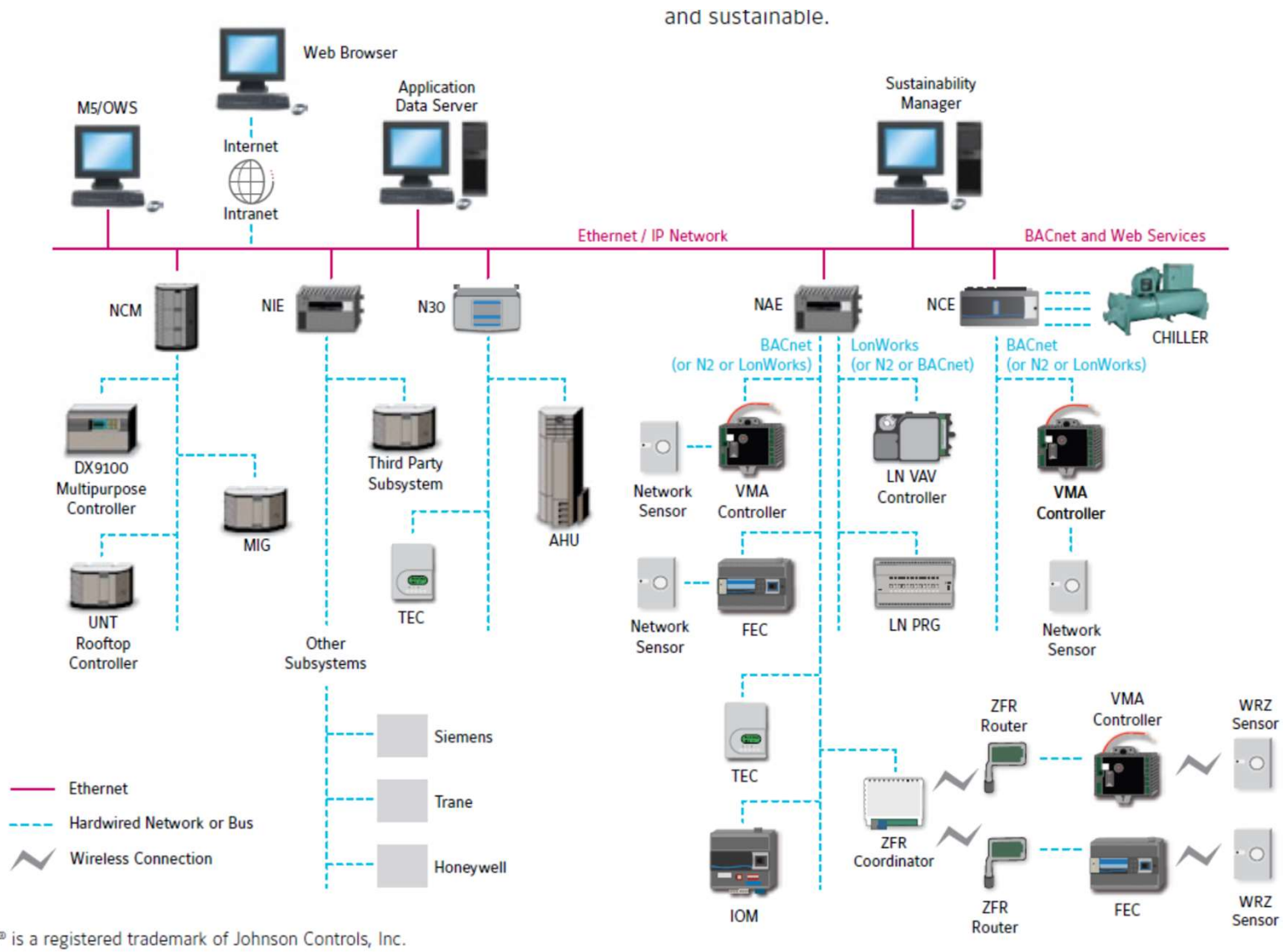
Notional JIE Control Systems



Tridium Architecture

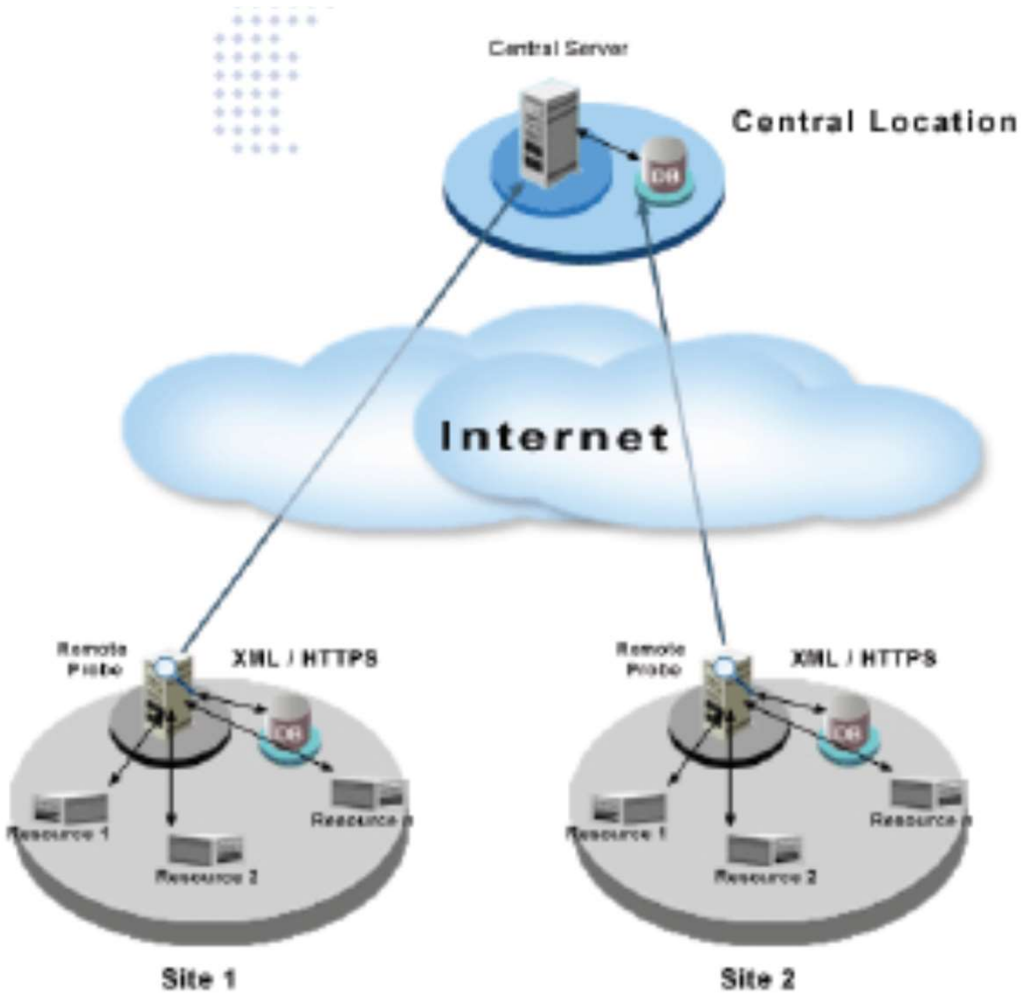


Johnson Controls Architecture



Metasys® is a registered trademark of Johnson Controls, Inc.

Software House Architecture



http://www.swhouse.com/

System & Terminal Unit Controllers, Actuators

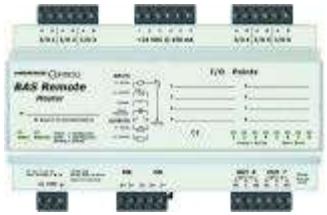
JACE

Field Server

iLon Smart Server

VAV

L-switch



BAS Remote Server

Valve Actuator

Valve Actuator

Pressure Sensor

Temperature Sensor

Analog voltage, resistance, current signal is converted to digital and then IP

Control System Protocols

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…

Control System Protocols

Control systems are fundamentally different than IT

- Can be based on Master and Slaves or Peer to Peer
- Slaves have Registers and Coils
- Devices use several different programming languages to perform operations
- Not originally designed for security or encryption

Master = Client : sends requests for values in the address
Slave = Server : replies with data
Registers and Coils = memory locations

Typical file extensions:

*.ACD
*.CXP
*.ESD
*.ESX
*.LDA
*.LCD
*.LDO
*.LCX
*.plcproject
*.PRJ
*.PRT
*.RSP
*.QXD
*.SCD

Unit 2

Hacker Methodology, Attacking and Defending

Attack Processes

SANS Process

- Reconnaissance
- Scanning
- Intrusion Detection System (IDS) evasion
- Network-Level attacks
- Gathering and parsing packets
- Operating System and application-level attacks
- Netcat: The attacker's best friend
- Password cracking
- Web application attacks
- Denial of service attacks
- Maintaining access
- Covering the tracks

http://www.sans.org/course/hacker-techniques-exploits-incident-handling

Root9b Process (Advanced Workshop)

- Footprinting
- Scanning
- Enumeration
- Network Mapping
- Gaining Access
- Privilege Escalation
- Post Exploitation
- Target Survey & Remote Forensics Analysis
- Cover Tracks (cleanup)
- Data Collection
- Rootkit (aka Backdoor, aka Implant, aka Persistence)
- Computer Network Attack

Attack Sequence (1)

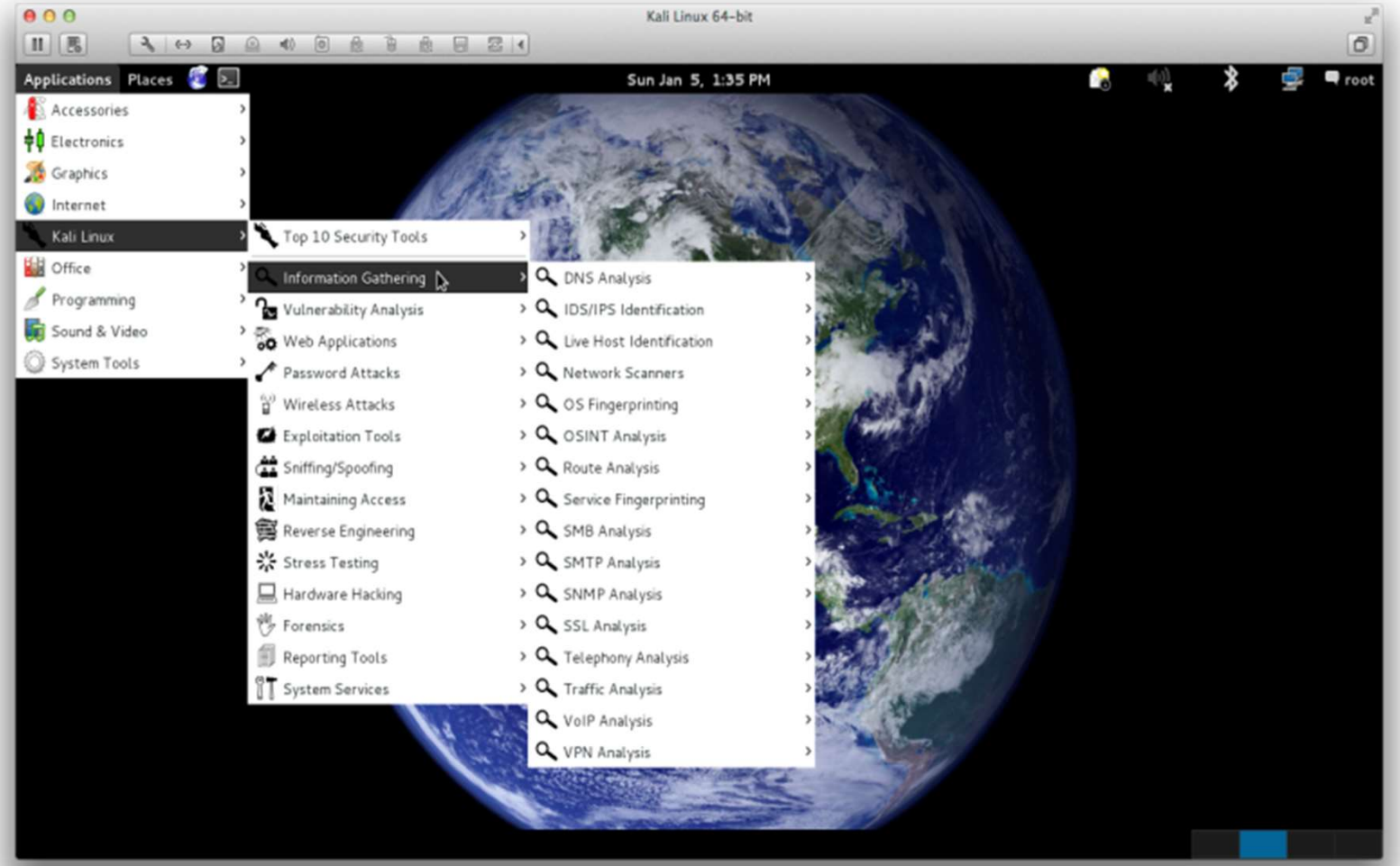
Footprinting: This is the process of ***conducting target analysis, identification, and discovery***; typically through the use of open source tools. This includes dumpster diving, social engineering and the use of utilities such as web-search hacking, traceroutes, pings, network lookups, etc.

Scanning: This step will take the findings from footprinting and begin to drill-down a bit further. In a traditional sense, this step includes ***port scanning, OS identification, and determining whether or not a machine is accessible***.

Enumeration: This is the phase where you further interrogate specific services to determine exact operating systems, software, etc. Normal enumeration techniques include searching for ***network share information, specific version of applications running, user accounts, SNMP traffic***, etc.

Network Mapping: This step is exactly as the name implies, laying out an illustration of the targeted network. This includes taking all available resources (logs, target surveys, etc.) to ***create a visualization of the target environment***. This often looks different from the exploiters perspective then from the Admin's perspective. Depending on the scope of activities being conducted this step may or may not be necessary.

Kali Linux Information Gathering

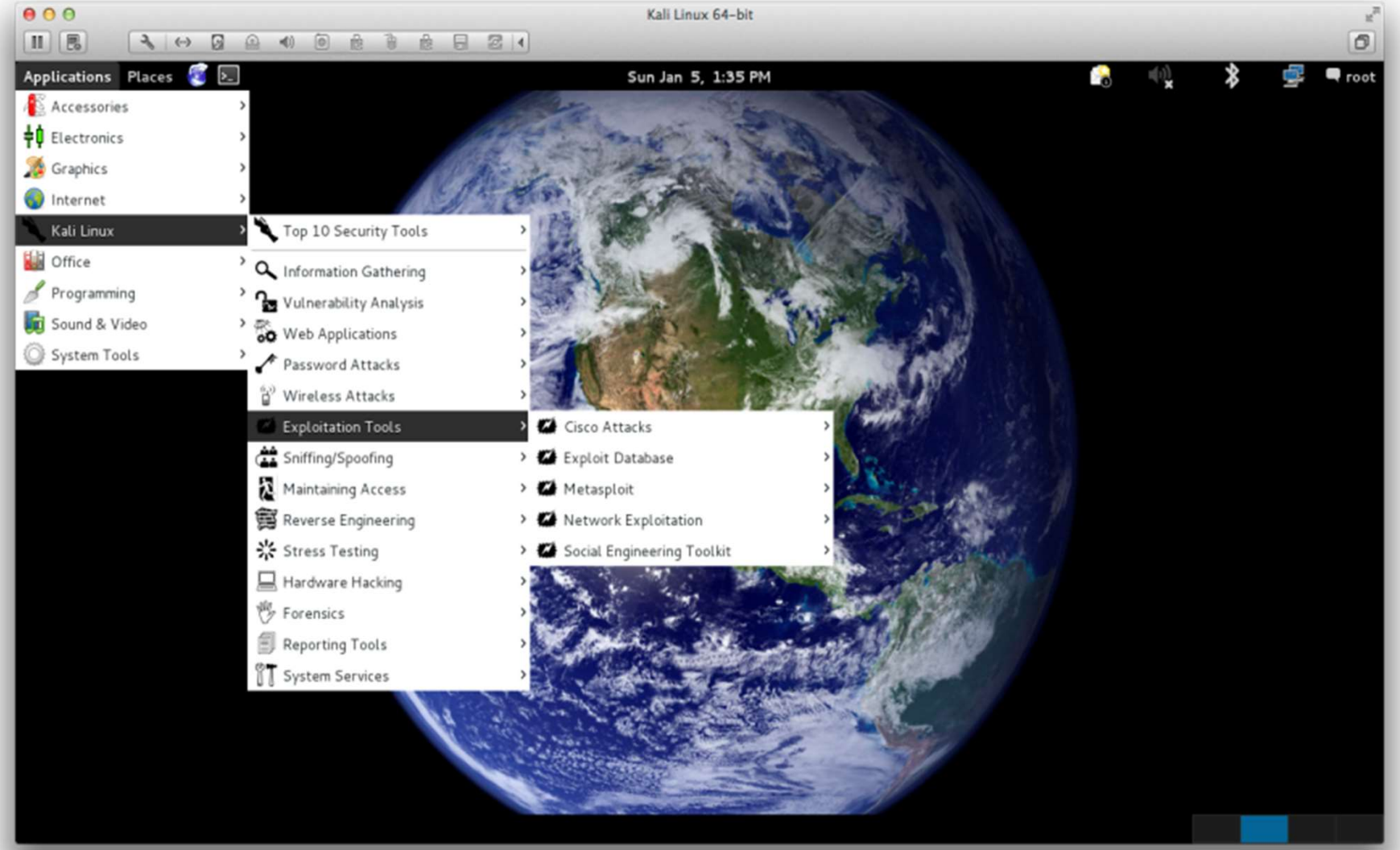


Attack Sequence (2)

Gaining Access: This step is the exploitation process. Basically, this is gaining ***access to the machine or the network by a client-side exploit, insider threat, supply interdiction attack, or remote exploitation opportunity***. This could be conducted via spear-fishing attacks, buffer overflows, embedded device exploitation, credential masquerade attacks, etc.

Privilege Escalation: Depending on the exploitation opportunity which was used the attacker may need to elevate privileges to a different user. There are various different scenarios in which the attacker will need to use this procedure. Typically, this is conducted through the use of a ***local exploit opportunity in order to gain root or system-level privileges – the highest possible user***.

Kali Linux Exploitation Tools



Attack Sequence (3)

Post Exploitation: This step is really a compilation of many steps and is dependent upon the objective of the mission. This step could include any combination or all of the following examples;

- ✓ Target Survey & Remote Forensics Analysis
- ✓ Cover Tracks (cleanup)
- ✓ Data Collection
- ✓ Rootkit (aka Backdoor, Implant, Persistence)
- ✓ Computer Network Attack (the 6 D's)
  - ✓ Disrupt
  - ✓ Deny
  - ✓ Degrade
  - ✓ Deceive
  - ✓ Destroy
  - ✓ Delay

Attack Sequence (4)

Target Survey & Remote Forensics Analysis: This step is to conduct analysis on the target machine for potential security mechanisms, files, or users which could either assist in obtaining the objective or harm the assessment. This is the ***process of analysing the targets operating environment***.

Cover Tracks (cleanup): This step is the process ***of removing any forensically relevant residue that was left behind as the result of exploitation or presence***. This is one of the most important steps that a ***hacker can perform to maintain stealth***. This is often one of the most important opportunities for ***defenders to profile an attacker***.

Data Collection: The attacker is in the network to perform some activity. Usually, this is not to show Cyber prowess, but instead to ***extract as much data as possible***. ***Network traffic analysis is key*** during this phase.

Rootkit (aka Backdoor, aka Implant, aka Persistence): This step is the process of ***installing an application, hooking the kernel, or laying down some mechanism which allows the attacker to maintain continued access*** to the host or network. If the implant is well designed, the attacker can live in your network for extended periods of time.

Kali Linux NMAP

NMAP – Network Mapper

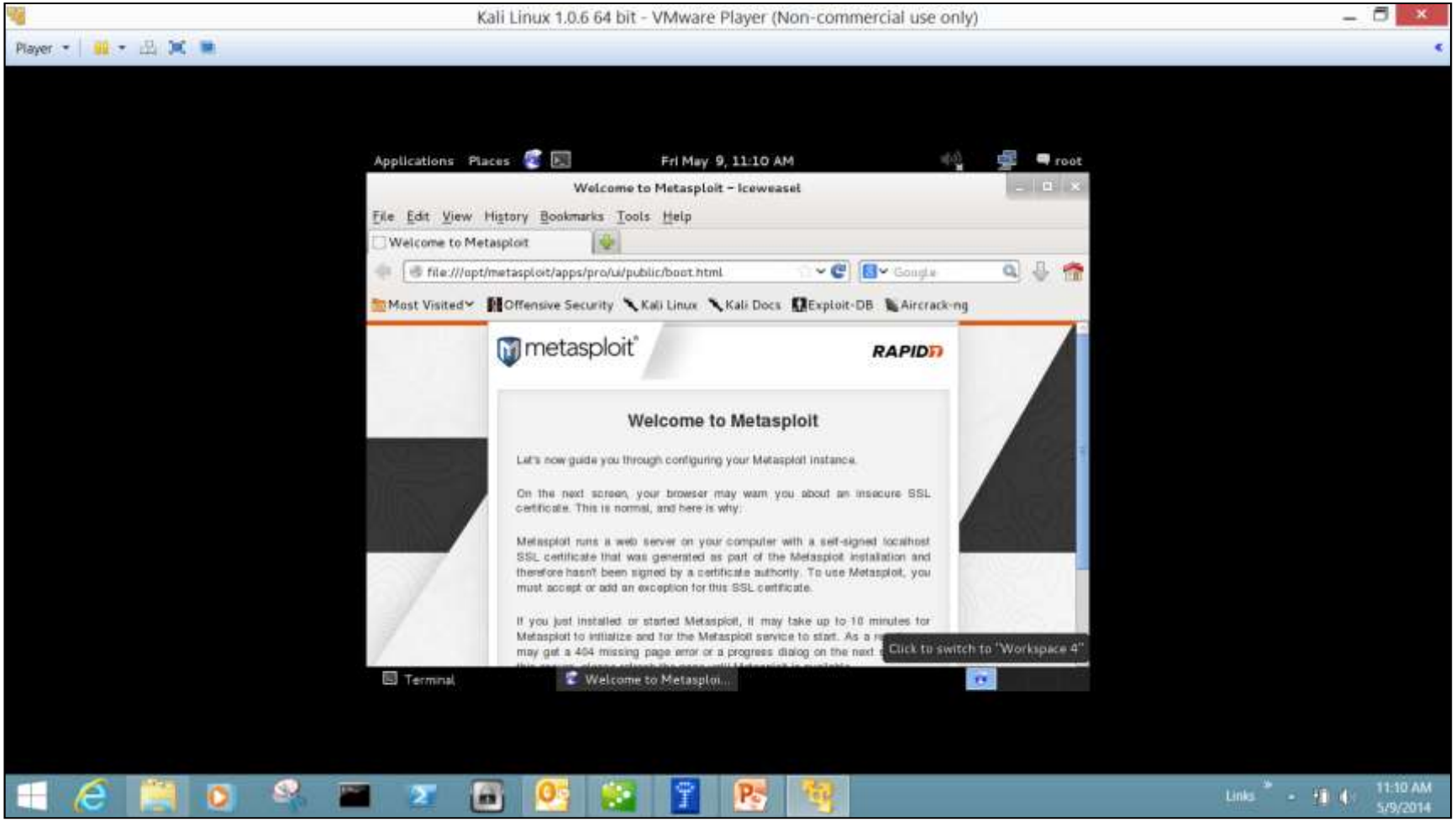
- ✓ Generates Network Traffic to Specific Hosts or Range of Hosts
- ✓ Helps identify potential vulnerable services
- ✓ Determines Open\Closed Network Ports
- ✓ Supports multiple protocols
- ✓ Can identify Operating System

Attack Sequence (5)

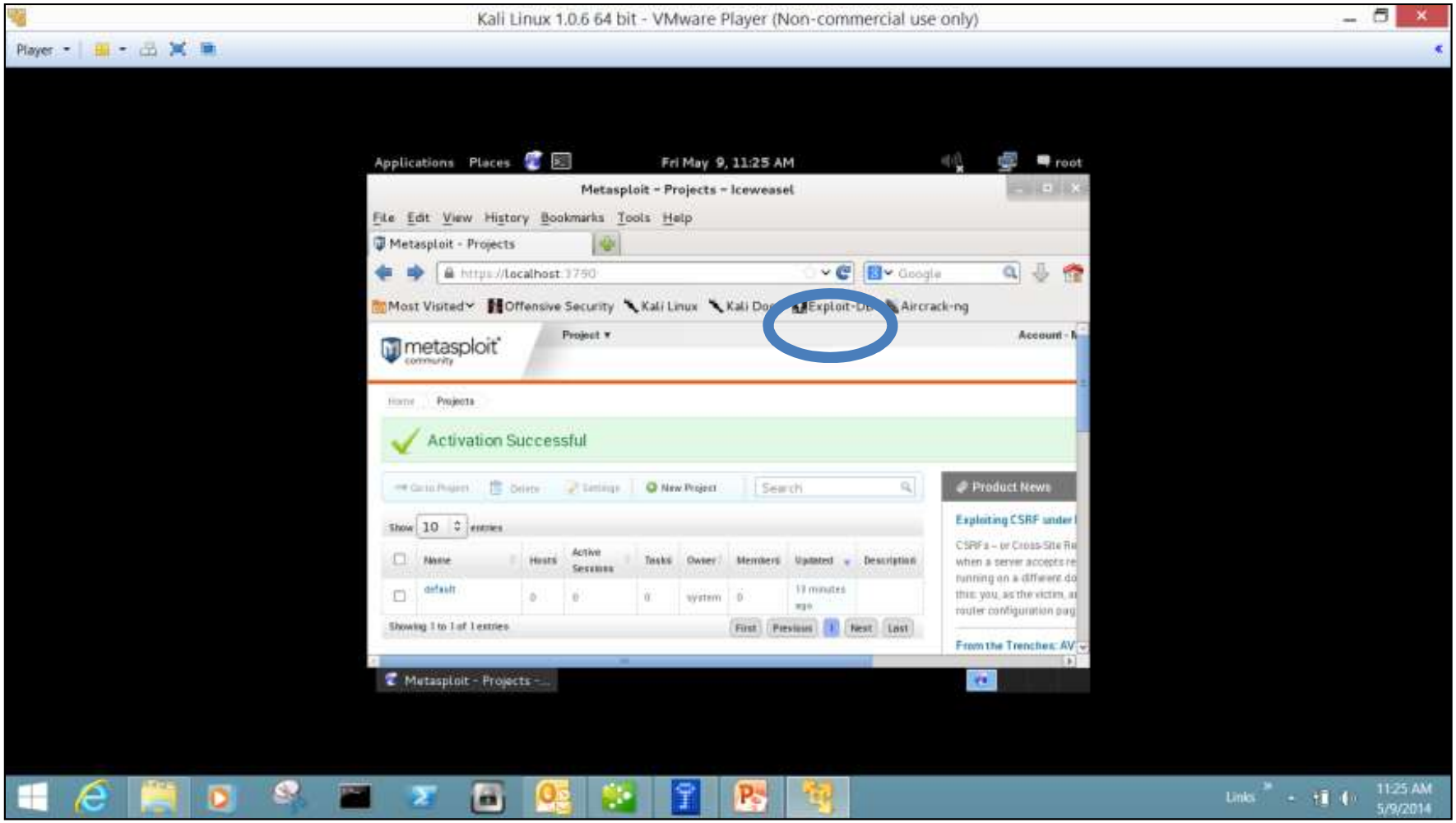
Computer Network Attack. In this step the attacker has already identified the network as a target of opportunity and has identified plans to launch an attack. This attack could be remote or local in nature and could come from already established access or with no access to the targeted environment. The attacker will ***typically identify core and vital network processes and perform various attacks to disrupt, deny, degrade, destroy, or deceive their "adversary.***"

The most sophisticated attackers would likely obtain access to the target environment. After obtaining access to the critical infrastructure, techniques will be utilized to achieve the 6D's of Computer Network Attack.

Kali Linux Metasploit (1)



Kali Linux Metasploit (2)



Kali Linux (1)

http://www.kali.org/

Kali Linux Features

Kali is a complete re-build of BackTrack Linux, adhering completely to Debian development standards. All-new infrastructure has been put in place, all tools were reviewed and packaged, and we use Git for our VCS.

More than 300 penetration testing tools: After reviewing every tool that was included in BackTrack, we eliminated a great number of tools that either did not work or had other tools available that provided similar functionality.

Vast wireless device support: We have built Kali Linux to support as many wireless devices as we possibly can, allowing it to run properly on a wide variety of hardware and making it compatible with numerous USB and other wireless devices.

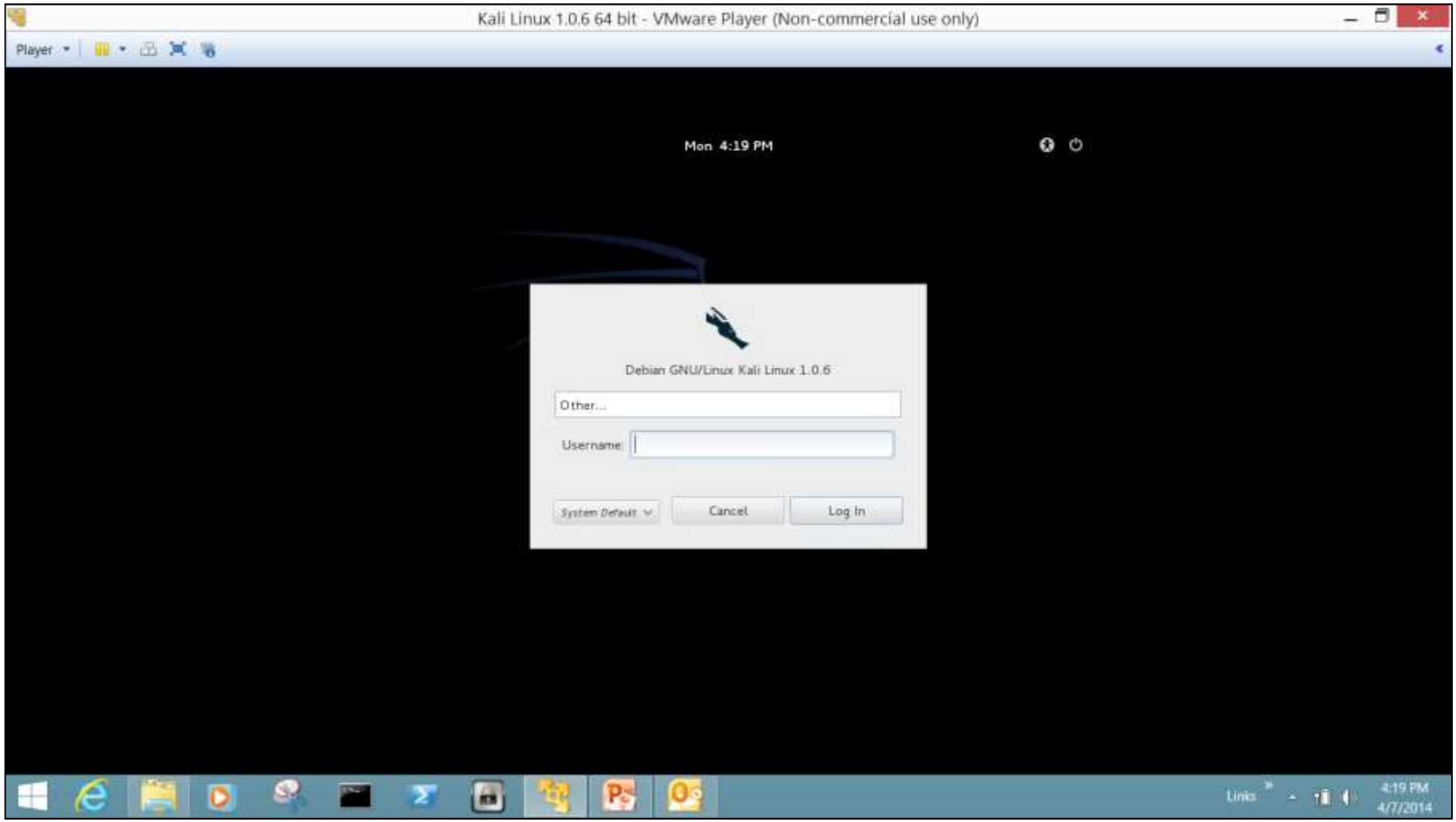
Custom kernel patched for injection: As penetration testers, the development team often needs to do wireless assessments so our kernel has the latest injection patches included.

Multi-language: Although pentesting tools tend to be written in English, we have ensured that Kali has true multilingual support, allowing more users to operate in their native language and locate the tools they need for the job.

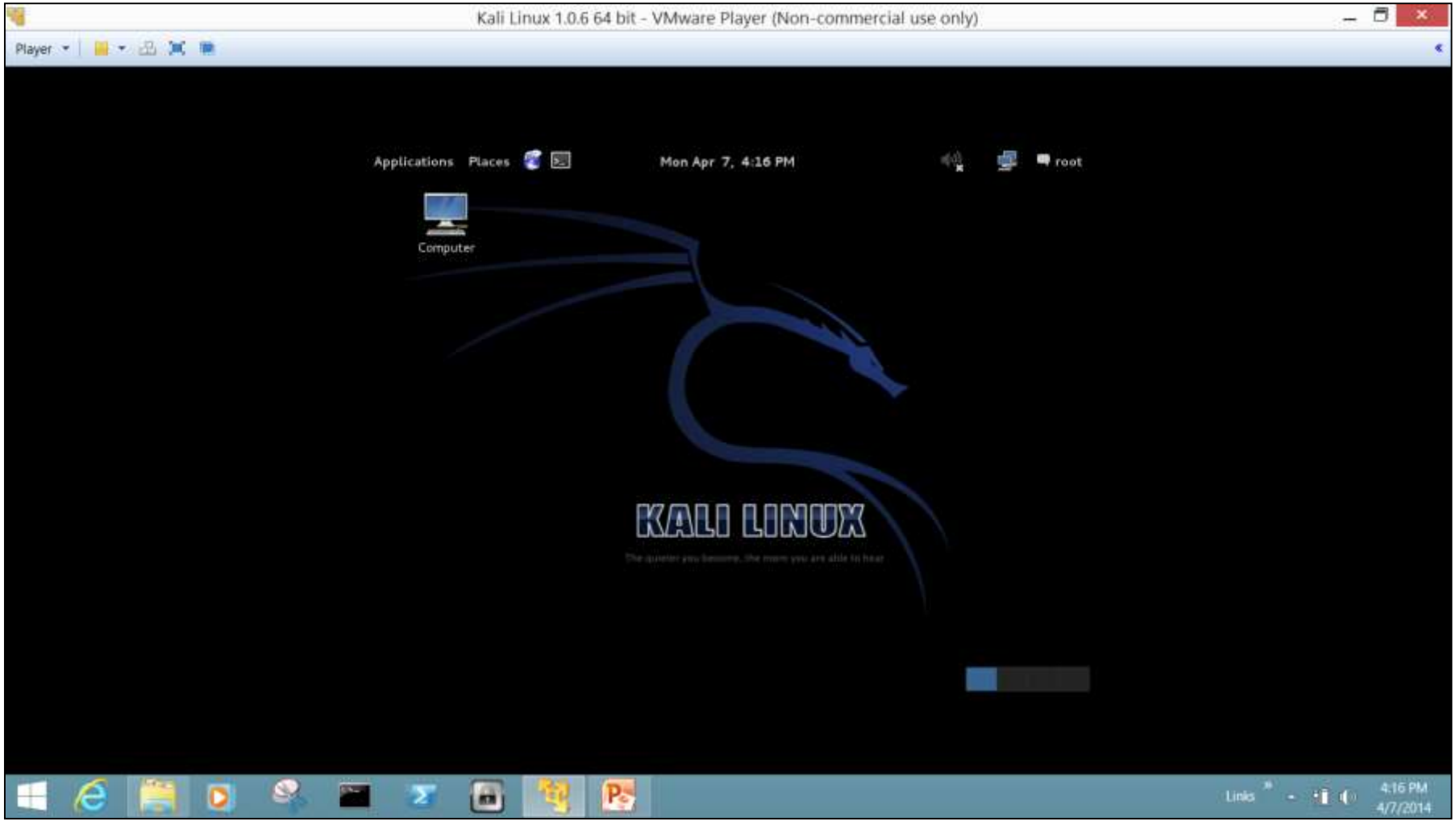
Completely customizable: We completely understand that not everyone will agree with our design decisions so we have made it as easy as possible for our more adventurous users to customize Kali Linux to their liking, all the way down to the kernel.

ARMEL and ARMHF support: Since ARM-based systems are becoming more and more prevalent and inexpensive, we knew that Kali's ARM support would need to be as robust as we could manage, resulting in working installations for both ARMEL and ARMHF systems. Kali Linux has ARM repositories integrated with the mainline distribution so tools for ARM will be updated in conjunction with the rest of the distribution.

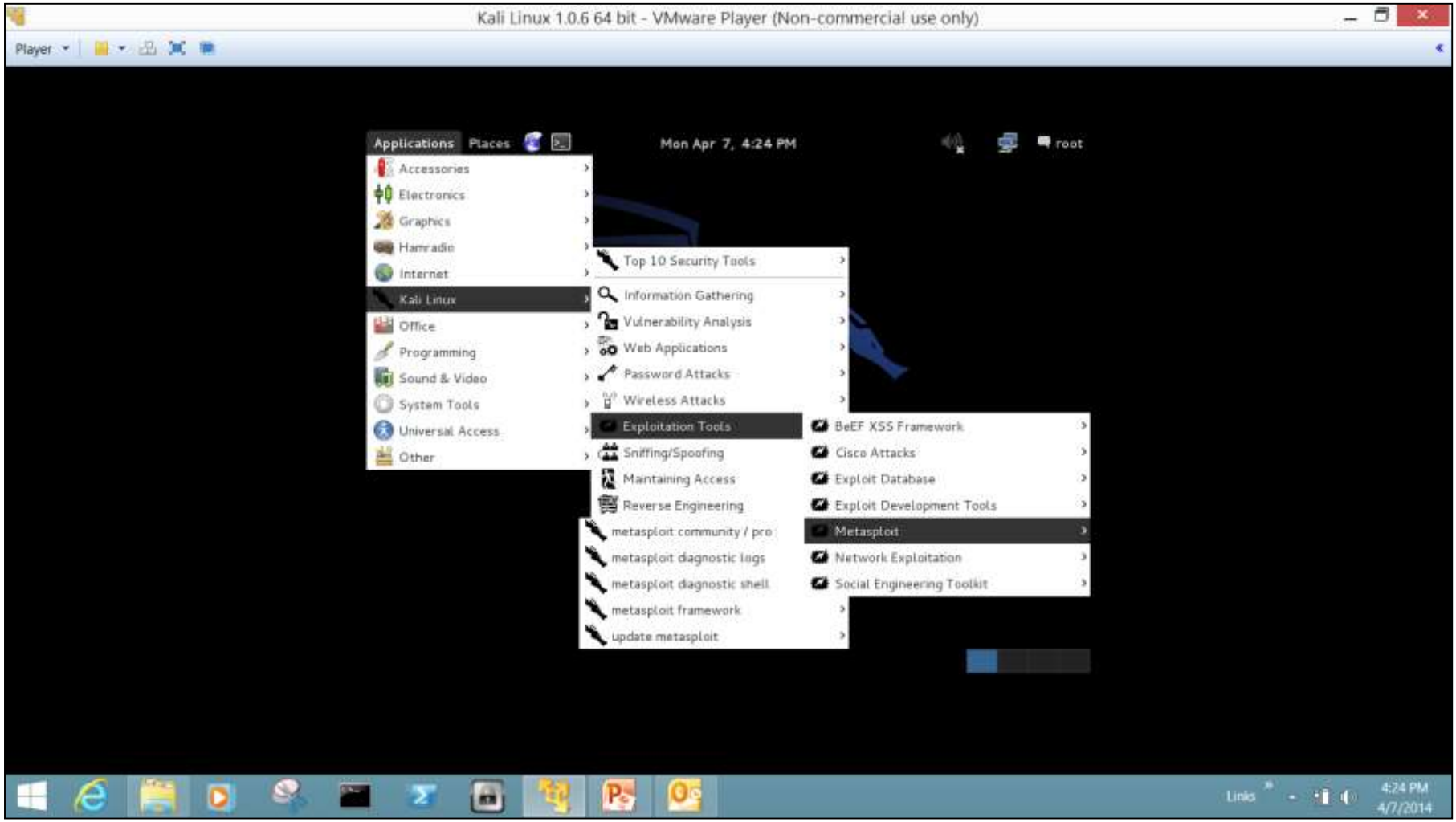
Kali Linux Login



Kali Linux Home



Kali Linux Metasploit



SamuraiSTFU Pen Testing Tool

Samurai contains several best-of-breed and open source tools such as:

- SamuraiWTF – a web pentesting tool
- Backtrack – a network pentesting tool
- 2 web browsers – Chromium and Konqueror
- Zed Attack Proxy (ZAP) – a protocol fuzzing tool
- Wireshark for Traffic capture and analysis
- Dojo-Basic is a web app used to teach how to pen test web apps
- ModbusPal is a Modbus-TCP simulator that can be used to model a typical control system environment
- Mbtget is a command line tool used to interact with the modbus-tcp protocol
- The xxd tool is a hex dumping tool that can be used to find passwords in EEPROM dumps
- Bastille Linux
- Several sample packet captures and tool documentation

http://www.samuraistfu.org/

Control System Vulnerabilities

http://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

Control System Exploitation Vectors

Access to the Control System LAN

- Common Network Architectures
- Dial-up Access to the RTUs
- Vendor Support
- IT Controlled Communication Gear
- Corporate VPNs
- Database Links
- Poorly Configured Firewalls
- Peer Utility Links

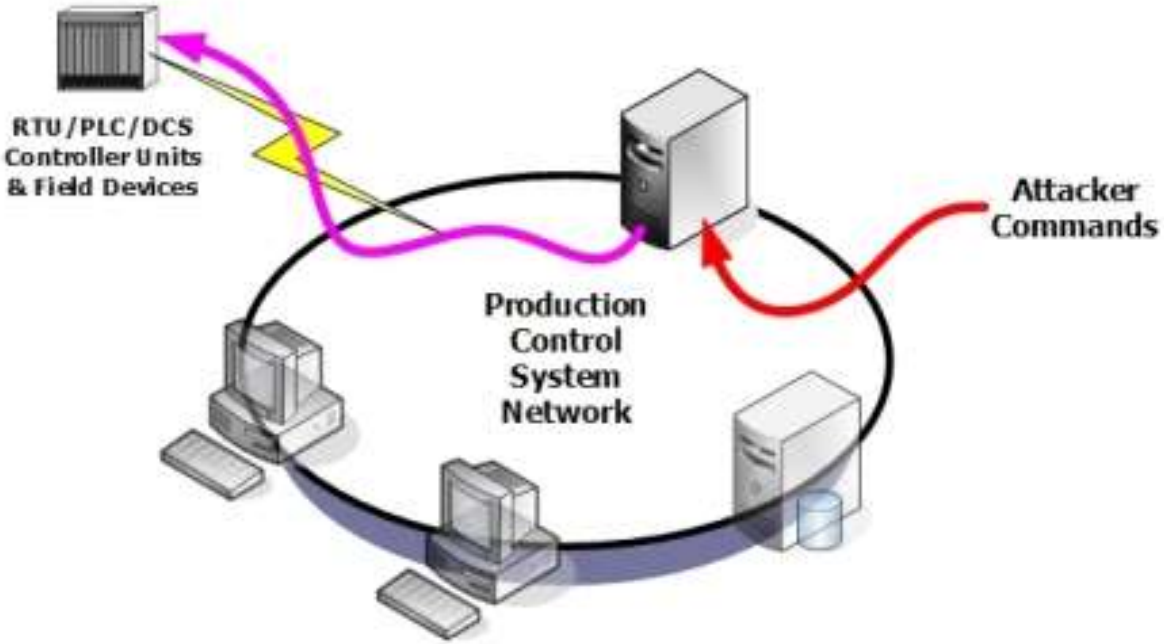
Discovery of the Process

- Details of how the process is implemented to surgically attack it
- Find the points in the data acquisition server database and the HMI display screens

Control of the Process

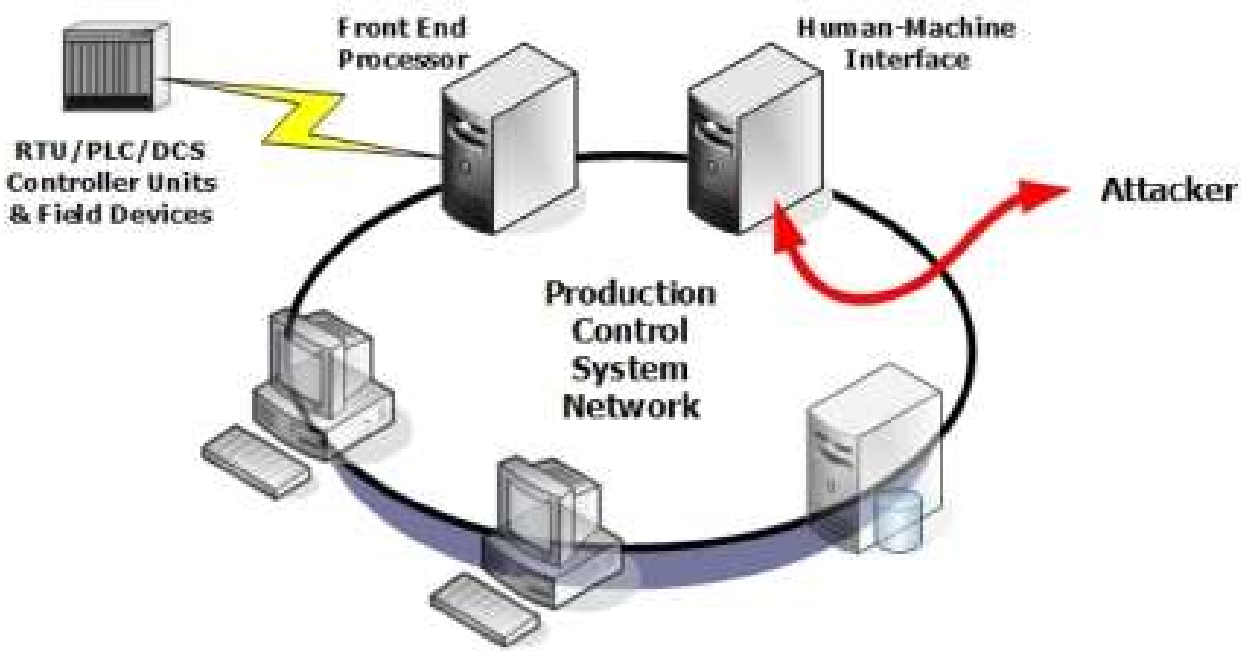
- Sending Commands Directly to the Data Acquisition Equipment
- Exporting the HMI Screen
- Changing the Database
- Man-in-the-Middle Attacks

Sending Commands Directly



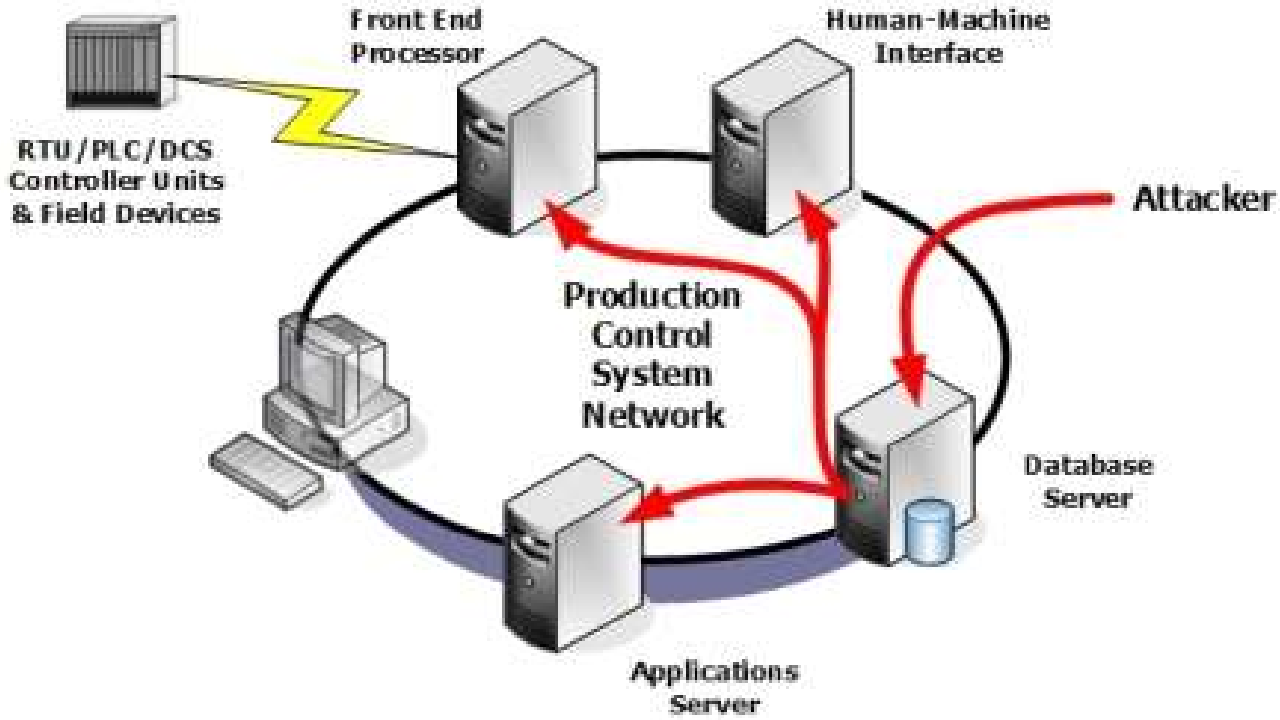
The easiest way to control the process is to send commands directly to the data acquisition equipment. **Most PLCs, protocol converters, or data acquisition servers lack even basic authentication. They generally accept any properly formatted command.** An attacker wishing control simply establishes a connection with the data acquisition equipment and issues the appropriate commands.

Exporting the HMI Screen



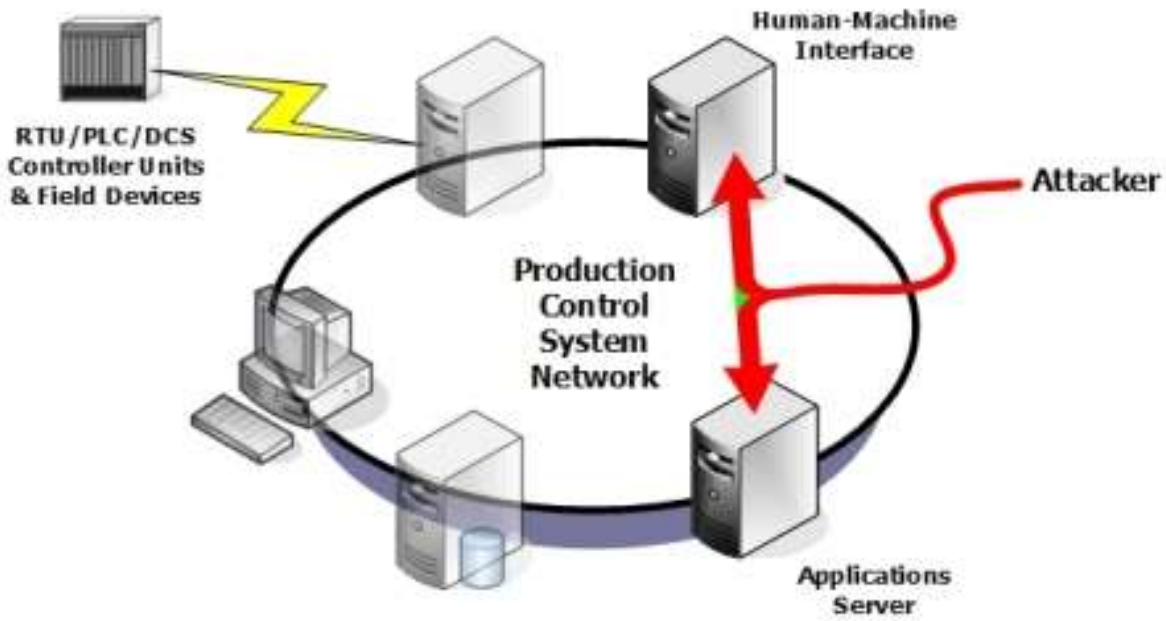
An effective attack is to export the screen of the operator's HMI console back to the attacker (see Figure 14). Off-the-shelf tools can perform this function in both Microsoft Windows and Unix environments. **The operator will see a "voodoo mouse" clicking around on the screen unless the attacker blanks the screen.** The attacker is also limited to the commands allowed for the currently logged-in operator. For instance, he probably could not change the phase tap on a transformer.

Changing the Database



In some, but not all, vendor's control systems, **manipulating the data in the database can perform arbitrary actions on the control system**

Man-in-the Middle Attacks



Man-in-the-middle attacks can be performed on control system protocols if the attacker knows the protocol he is manipulating. **An attacker can modify packets in transit, providing both a full spoof of the operator HMI displays and full control of the control system (see Figure 16). By inserting commands into the command stream the attacker can issue arbitrary or targeted commands.** By modifying replies, the operator can be presented with a modified picture of the process.

Defending – DHS Recommended Practices

http://ics-cert.us-cert.gov/Recommended-Practice

Defending ICS Against Cyberth... | sans.org | Recommended Practices | I...

Official website of the Department of Homeland Security

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

HOME | ABOUT | ICSJWG | INFORMATION PRODUCTS | TRAINING | FAQ

Control Systems

- Home
- Calendar
- ICSJWG
- Information Products
- Training
- Recommended Practices
- Assessments
- Standards & References
- Related Sites
- FAQ

Recommended Practices

The recommended practices working group selects topics to be implemented in the recommended practices section. This page provides abstracts for existing recommended practices and links to the source documents. Additional supporting documents detailing a wide variety of control systems topics associated with cyber vulnerabilities and their mitigation have been developed and vetted by the working group for accuracy. These documents will be updated and topics added to address additional content and emerging issues.

- **Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies**
  Abstract
  Full document
- **Creating Cyber Forensics Plans for Control Systems**
  Abstract
  Full document
- **Developing an Industrial Control Systems Cybersecurity Incident Reponse Plan**
  Abstract
  Full document
- **Good Practice Guide for Firewall Deployment on SCADA and Process Control Networks**
  Abstract
  Full document
- **Recommended Practice Case Study: Cross-Site Scripting**
  Abstract

Links 2:07 PM 5/7/2014

DHS Control Systems Defense in Depth (1)

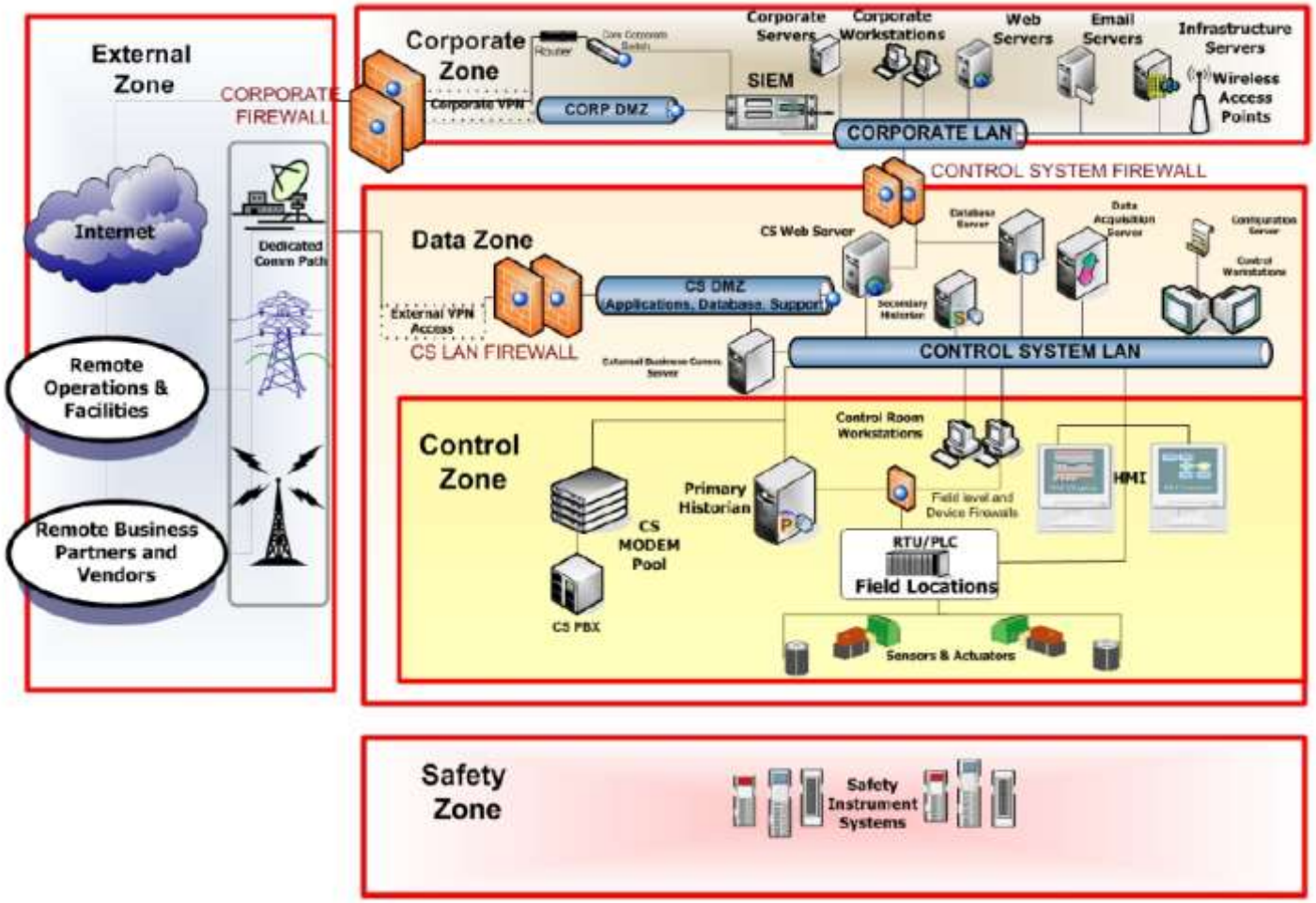
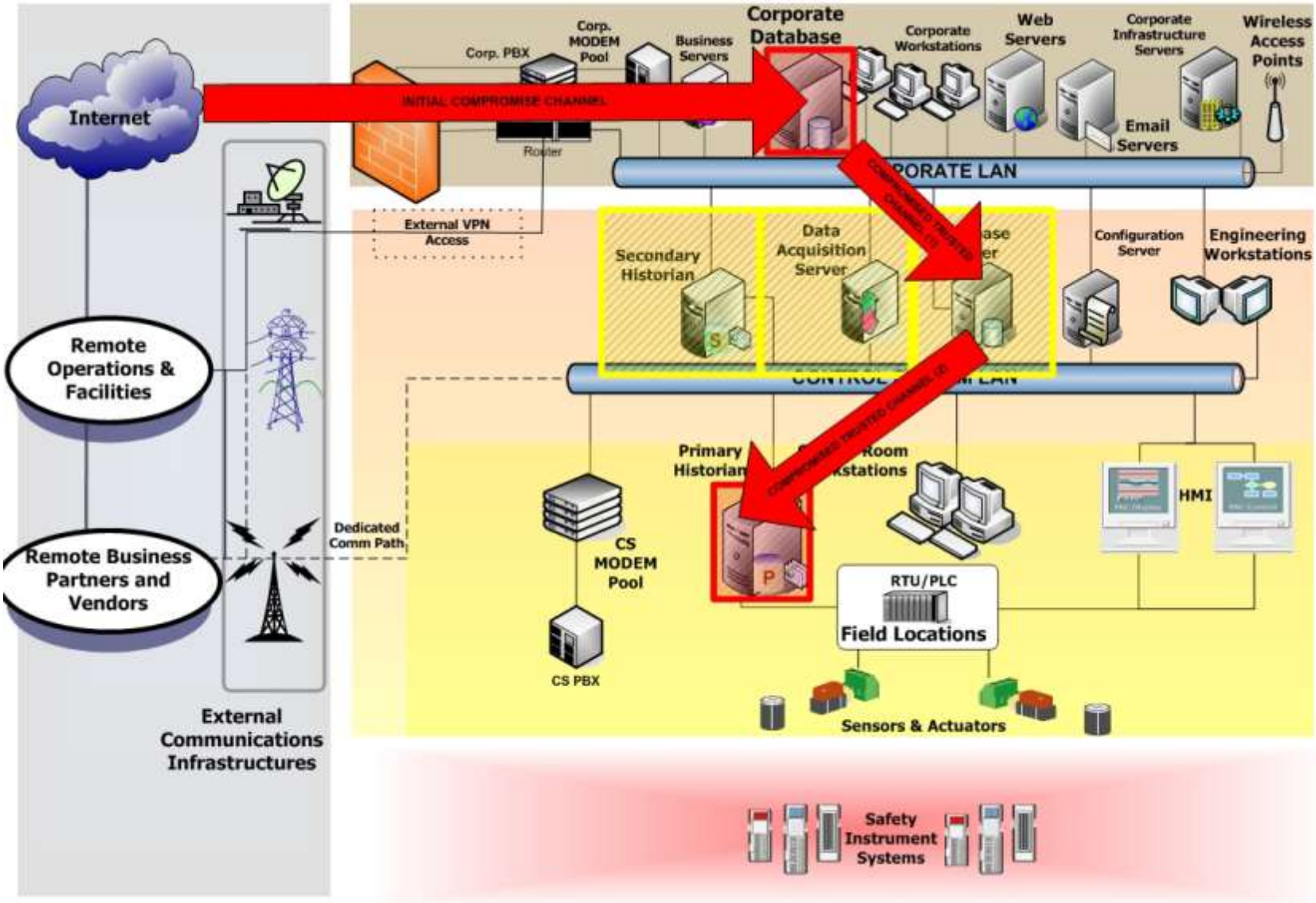


Figure 10. Complete defense-in-depth strategy with the intrusion detection system and SIEM.

Inbound Protection, Outbound Detection

DHS Control Systems Defense in Depth (2)



Five Key Countermeasures (1)

1. Security policies. ***Security policies*** should be developed for the control systems network and its individual components, but they should be ***reviewed periodically*** to incorporate the current threat environment, system functionality, and required level of security.

2. Blocking access to resources and services. This technique is generally employed on the ***network through the use of perimeter devices with access control lists*** such as firewalls or proxy servers. It can be enabled on the host via host-based firewalls and antivirus software.

3. Detecting malicious activity. Detection activities of malicious activity can be networked or host-based and ***usually require regular monitoring of log files by experienced administrators***. IDS are the common means of identifying problems on a network, but can be deployed on individual hosts as well. Auditing and event logs should be enabled on individual hosts when possible.

Five Key Countermeasures (2)

4. Mitigating possible attacks. In many cases, vulnerability may have to be present because removal of the vulnerability may result in an inoperable or inefficient system. ***Mitigation allows administrators to control access to vulnerability in such a fashion that the vulnerability cannot be exploited***. Enabling technical workarounds, establishing filters, or running services and applications with specific configurations can often do this.

5. Fixing core problems. The resolution of ***core security problems almost always requires updating, upgrading, or patching the software vulnerability or removing the vulnerable application***. The software hole can reside in any of the three layers (networking, operating system, or application). When available,

US-CERT Intruder Detection Checklist (1)

Intruder Detection Checklist

This document outlines suggested steps for determining if your system has been compromised. System administrators can use this information to look for several types of break-ins. We encourage you to review all sections of this document and modify your systems to close potential weaknesses.

In addition to the information in this document, we provide three companion documents that may help you:

- http://www.cert.org/tech_tips/unix_configuration_guidelines.html
  contains suggestions for avoiding common UNIX system configuration problems that have been exploited
- http://www.cert.org/tech_tips/root_compromise.html
  contains suggested steps for recovering from a root compromise on a UNIX system
- http://www.cert.org/tech_tips/security_tools.html
  contains descriptions of tools that can be used to help secure a system and deter break-ins

We also encourage you to check with your vendor(s) regularly for any updates or new patches that relate to your systems.

F. Look For Signs That Your System May Have Been Compromised

Note that all action taken during the course of an investigation should be in accordance with your organization's policies and procedures.

1. Examine log files for connections from unusual locations or other unusual activity. For example, look at your 'last' log, process accounting, all logs created

Look for Signs That Your System May Have Been Compromised

1. Examine log files
2. Look for setuid and setgid Files
3. Check system binaries
4. Check for packet sniffers
5. Examine files run by 'cron' and 'at'.
6. Check for unauthorized services
7. Examine /etc/passwd file
8. Check system and network configuration
9. Look everywhere for unusual or hidden files

Unit 3

Footprinting using Whois, Google Hacking, BING, Google Earth, Shodan, Kali Linux, Control Things I/O, NMAP, Wireshark, Belarc and Glasswire

Key RMF Documents and Plans

Key RMF Documents/Plans (for commercial/private sector most now required by insurance) – in recommended sequence of completion

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

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

Templates at: https://www.serdp-estcp.org/Investigator-Resources/ESTCP-Resources/Demonstration-Plans/Cybersecurity-Guidelines

Client-Server and Cloud Architectures

Traditional FRCS Client-Server Architecture

- Vast majority of FRCS 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 buildings are moving to cloud architectures at a rapid pace
- Manages the building 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, building controllers default to safe mode

RMF Documents Using QUICX

Document Management	Design and Construction	QC & Commissioning	Transition	Operations
Policy Management	Contract Management	Master Equipment List	Transition Management	Life Cycle Cost Analysis
Risk Management Framework	Permit Process	Location List	O&M Manuals	Condition Assessments
System Security Plans	Drawings and Specifications	Field Reporting	Training Facilitation	Building Controls Analytics
Cyber System Categorization	Submittals	Deliverables Tracking	Warranty Certificates	Cyber Risk Assessments
Configuration Management	Requests for Information	Inspections and Checklists	Spare Parts/Special Tools	Cyber Continuous Monitoring
Record Documents	Change Management	Cyber Procedures		
		Performance Testing		
		Action Lists		

QUICX is a Facility Management and document management application that integrates facility equipment data, work orders, construction documents and specifications, geospatial, IT and OT network and component information

Typical Plans & Audit Logs Directory Using QUICX

Permits | Dwgs | Specs | Docs | Rev Pkgs | Submit-tals | RFIs | Change Docs | Inspec-tions | Punch-lists | Equip-ment | Check-lists | FPTs | Close-out | Issues | Field Reports | Mtgs | Trans-mittals | Contacts & Co. | Places | Con-tacts | Setup

Permit | Design | CM | Q/SF TY | Cx | PM | Setup

Documents | New Item | Reports | Export | Help | 20 - 01 - System Security Plan

Name	Document No	Document Type	Area of Work	Status
01 - System Security Plan	20	01 Document Phase	Policy	Template
02 - IT Policies	22	01 Document Phase	Policy	Template
03 - IT Contingency Plan	18	01 Document Phase	Policy	Template
04 - Security Audit Plan	28	01 Document Phase	Policy	Guide
05 - Plan of Action and Milestones	23	01 Document Phase	Policy	Guide

1 2 3 4 | 5 items per page | 1 - 5 of 16 items

General | Revisions | Transmittal History | Disposition | Related Records | More

Document No: 20

Name: 01 - System Security Plan

Description: System Security Plan

Status: Template (Add new)

Document Type: 01 Document Phase (Add new)

Date: 11/16/2015

Design Company: Chinook Systems Inc. (Add new)

Comments: These are the primary documents in your company CCRMP.

An organization can use standard data drives, SharePoint, etc. to store the Plans and Audit Logs

Tools

Information Gathering

- Google Search and Hacking
- Google Earth
- The Harvester
- Recon-NG
- Shodan
- Costar

Network Discovery and Monitoring

- Nmap
- Snort
- Kismet
- Nessus
- McAfee
- Sophia
- Bandolier
- SCAP
- Belarc
- Glasswire
- GrassMarlin

Attack and Defend Tools

- Kali Linux (Backtrack)
- SamuraiSTFU
- Wireshark
- Gleg
- Windows PowerShell
- Windows Management Information Console
- Windows Enhanced Mitigation Tools
- Windows Sysinternals

Assessment Tools

- DHS ICS-CERT Cyber Security Evaluation Tool (CSET)

Virtual Machines

- VM Player
- Windows Hypervisor

FRCS 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
- Simple Mail Transfer Protocol – Port 587

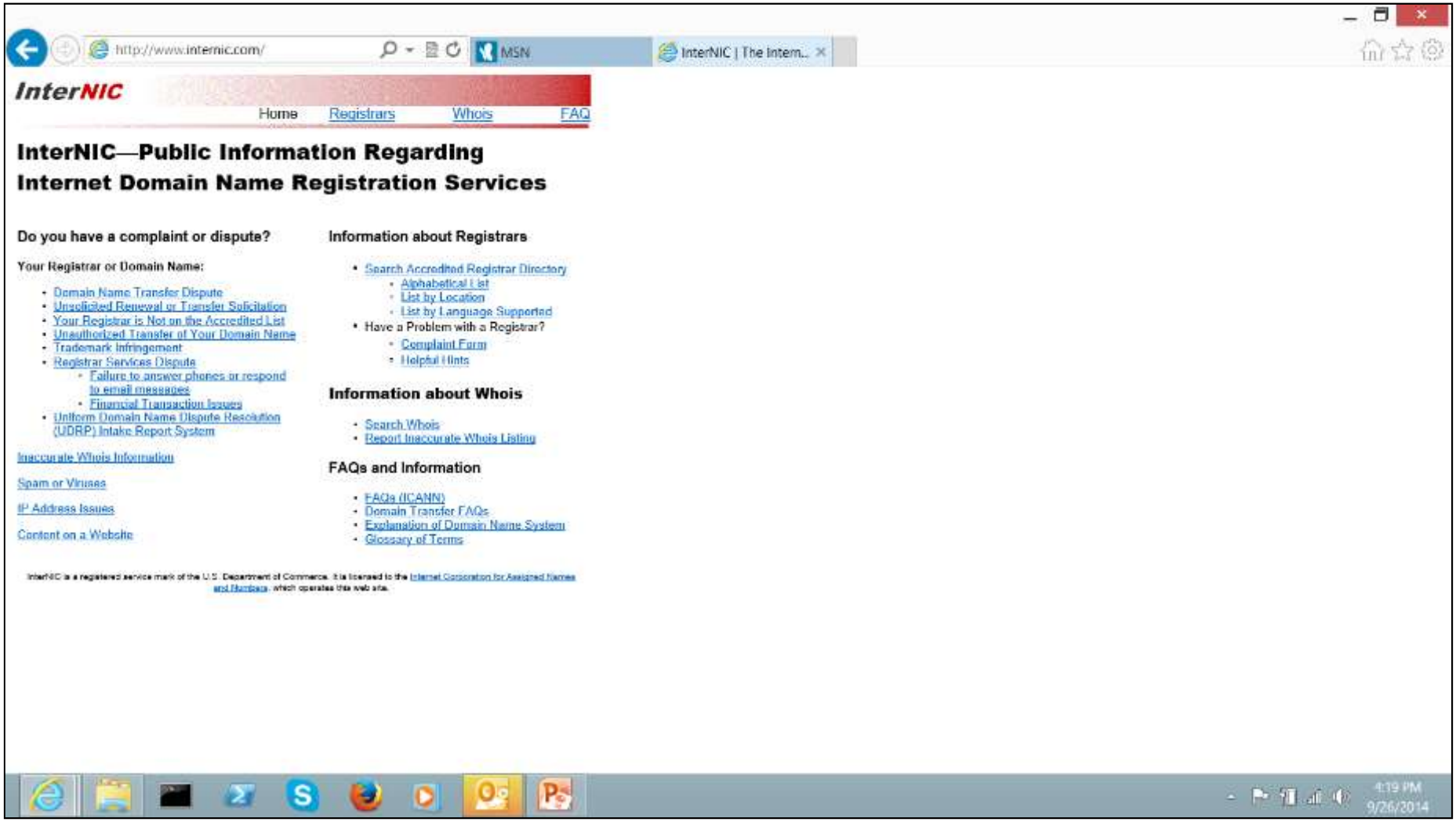
Open Control Systems Protocols

- 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
- HART: Peer to Peer – Port 5094

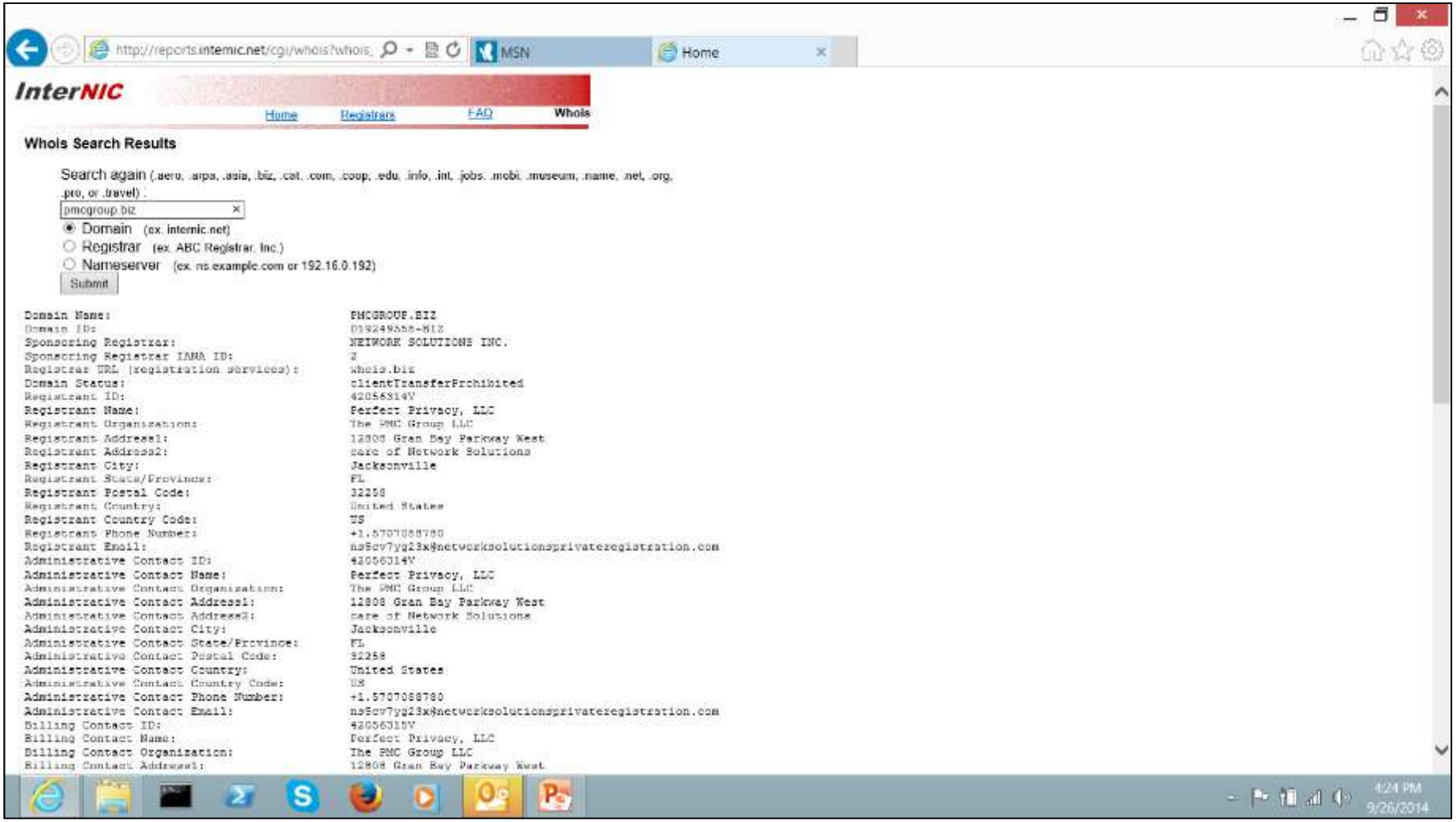
Proprietary Control Systems Protocols

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

Whois Search on InterNIC



Whois Domain Search on InterNIC



Whois Nameserver Search on InterNIC

http://reports.internic.net/cgi/whois?whois_

InterNIC

Home Registrars FAQ Whois

Whois Search Results

Search again (.aero, .arpa, .asia, .biz, .cat, .com, .coop, .edu, .info, .int, .jobs, .mobi, .museum, .name, .net, .org, .pro, or .travel):

NS43.WORLDNIC.COM

- (•) Domain (ex. internic.net)
- ( ) Registrar (ex. ABC Registrar, Inc.)
- ( ) Nameserver (ex. ns.example.com or 192.16.0.192)

Submit

```
Whois Server Version 3.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Server Name: NS43.WORLDNIC.COM
   IP Address: 207.204.40.122
   Registrar: NETWORK SOLUTIONS, LLC.
   Whois Server: whois.networksolutions.com
   Referral URL: http://networksolutions.com

>>> Last update of whois database: Fri, 26 Sep 2014 20:29:56 UTC <<<

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
```

4:30 PM
9/26/2014

Google Hacking

What is Google Hacking?

Google hacking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.

Google hacking involves using advanced operators in the Google search engine to locate specific strings of text within search results. Some of the more popular examples are finding specific versions of vulnerable Web applications. The following search query would locate all web pages that have that particular text contained within them. It is normal for default installations of applications to include their running version in every page they serve, for example, "Powered by XOOPS 2.2.3 Final".

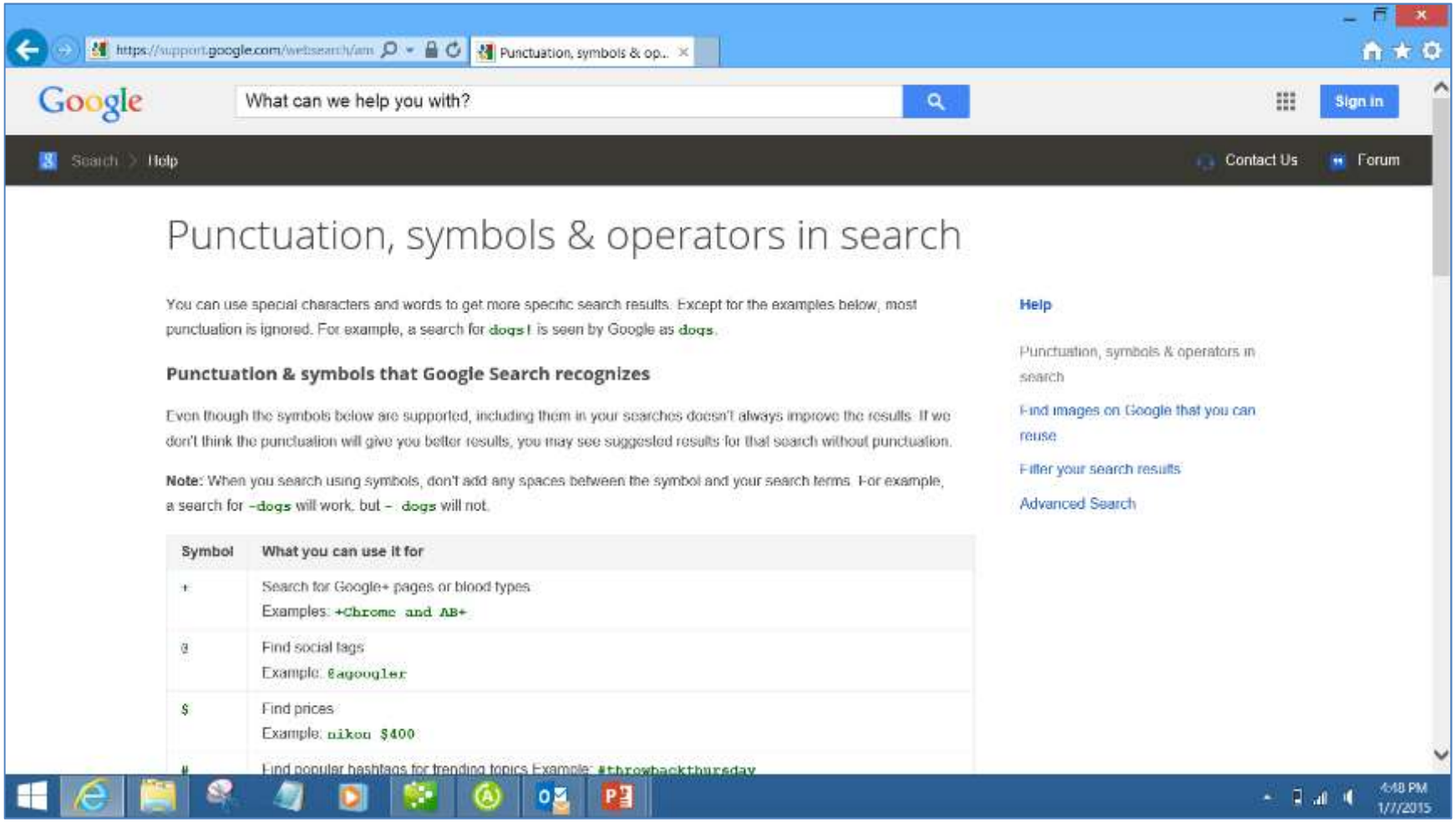
The following search query will locate all websites that have the words "admbook" and "version" in the title of the website. It also checks to ensure that the web page being accessed is a PHP file intitle:admbook intitle:version filetype:php

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

Google Search and Hacking Tools

Google Shortcut	Finds Pages That Have...
nokia phone	the words **nokia** and **phone**
sailing **OR** boating	either the word **sailing** or the word **boating**
"love me tender"	the exact phrase **love me tender**
printer -cartridge	the word **printer** but NOT the word **cartridge**
Toy Story +2	movie title including the number 2
~auto	looks up the word **auto** and synonyms
define:serendipity	definitions of the word **serendipity**
how now * cow	the words **how now cow** separated by one or more words
+	addition; **978+456**
-	subtraction; **978-456**
*	multiplication; **978*456**
/	division; **978/456**
% of	percentage; **50% of 100**
^	raise to a power; **4^18** (4 to the eighteenth power)
old **in** new (conversion)	**45 celsius in Fahrenheit**
site:(search only one website)	**site:websearch.about.com "invisible web"**
link:(find linked pages)	**link:www.lifehacker.com**
#...#(search within a number range)	**nokia phone $200...$300**
daterange:(search within specific date range)	**bosnia daterange:200508-200510**
safesearch: (exclude adult content)	**safesearch:breast cancer**
info: (find info about a page)	**info:www.websearch.about.com**
related: (related pages)	**related:www.websearch.about.com**
cache: (view cached page)	**cache:google.com**
filetype:(restrict search to specific filetype)	**zoology filetype:ppt**
allintitle: (search for keywords in page	**allintitle:"nike" running**

Google Search Operators



Google

What can we help you with?

Sign in

Search > Help

Contact Us

Forum

Punctuation, symbols & operators in search

You can use special characters and words to get more specific search results. Except for the examples below, most punctuation is ignored. For example, a search for `dogs!` is seen by Google as `dogs`.

Punctuation & symbols that Google Search recognizes

Even though the symbols below are supported, including them in your searches doesn't always improve the results. If we don't think the punctuation will give you better results, you may see suggested results for that search without punctuation.

Note: When you search using symbols, don't add any spaces between the symbol and your search terms. For example, a search for `-dogs` will work, but `- dogs` will not.

Symbol	What you can use it for
+	Search for Google+ pages or blood types Examples: `+Chrome and AB+`
@	Find social tags Example: `@agoogler`
$	Find prices Example: `nikon $400`
#	Find popular hashtags for trending topics. Example: `#throwbackthursday`

Help

Punctuation, symbols & operators in search

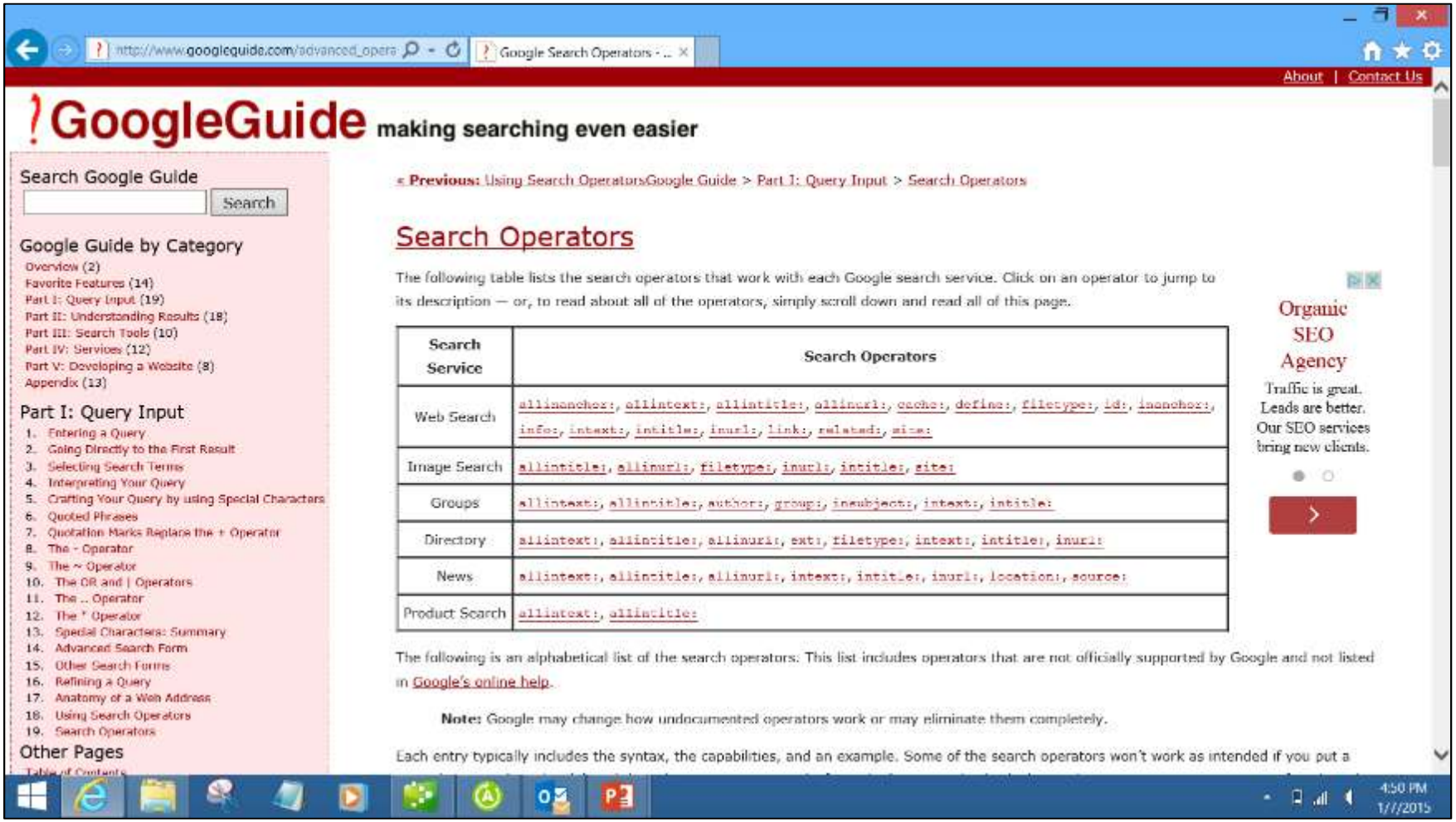
Find images on Google that you can reuse

Filter your search results

Advanced Search

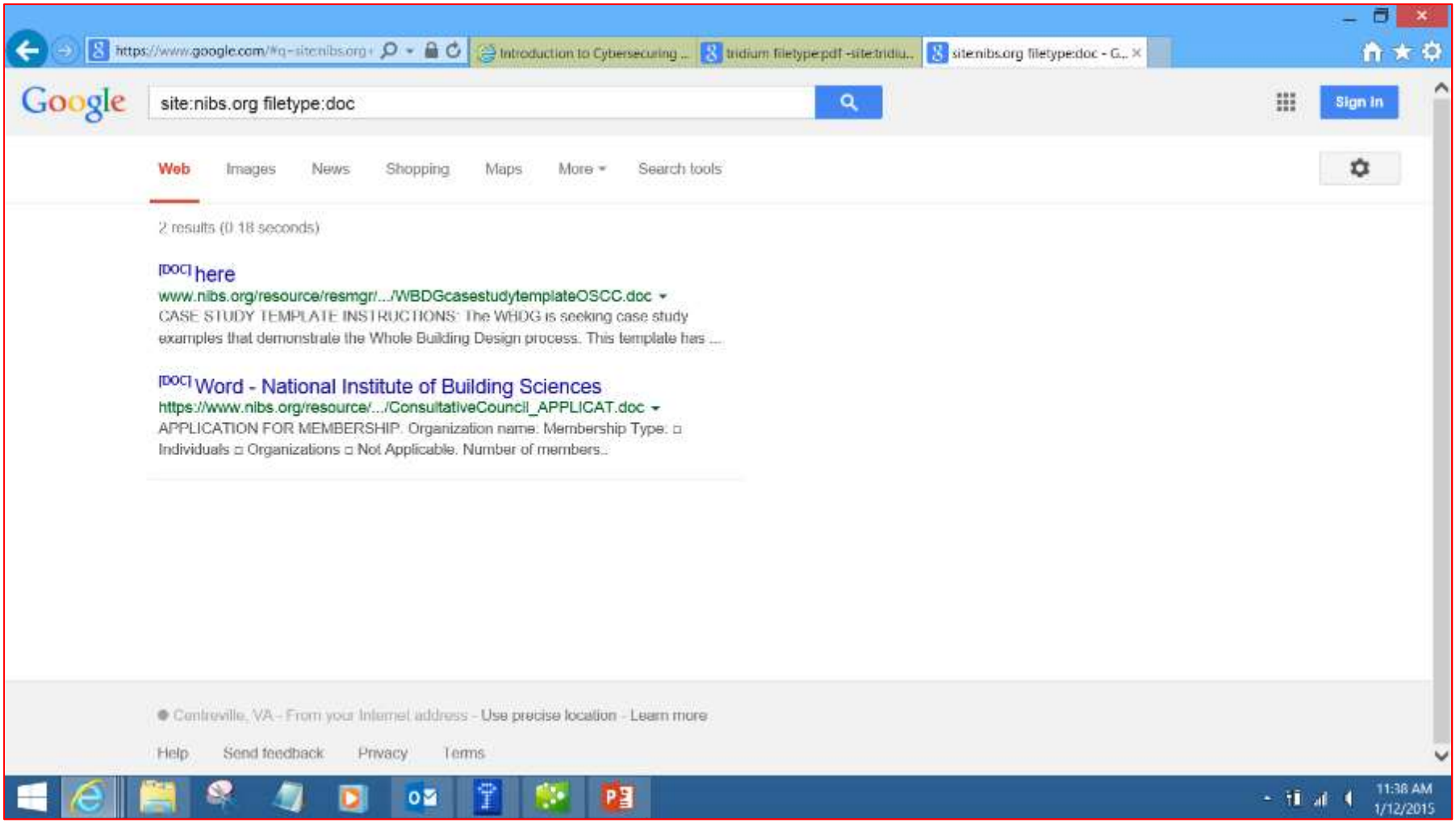
https://support.google.com/websearch/answer/2466433?hl=en

GoogleGuide



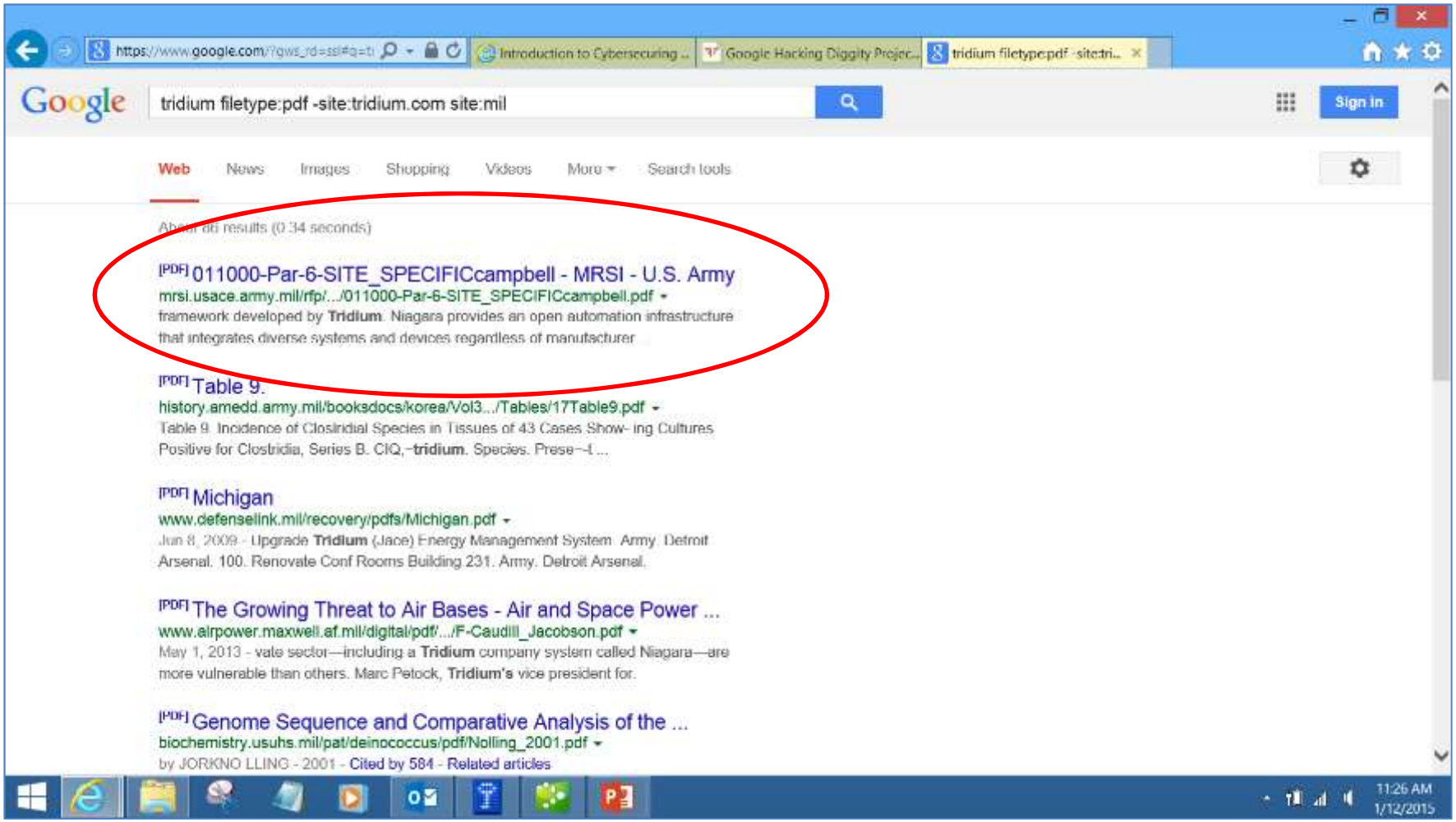
http://www.googleguide.com/advanced_operators_reference.html

Google Hacking



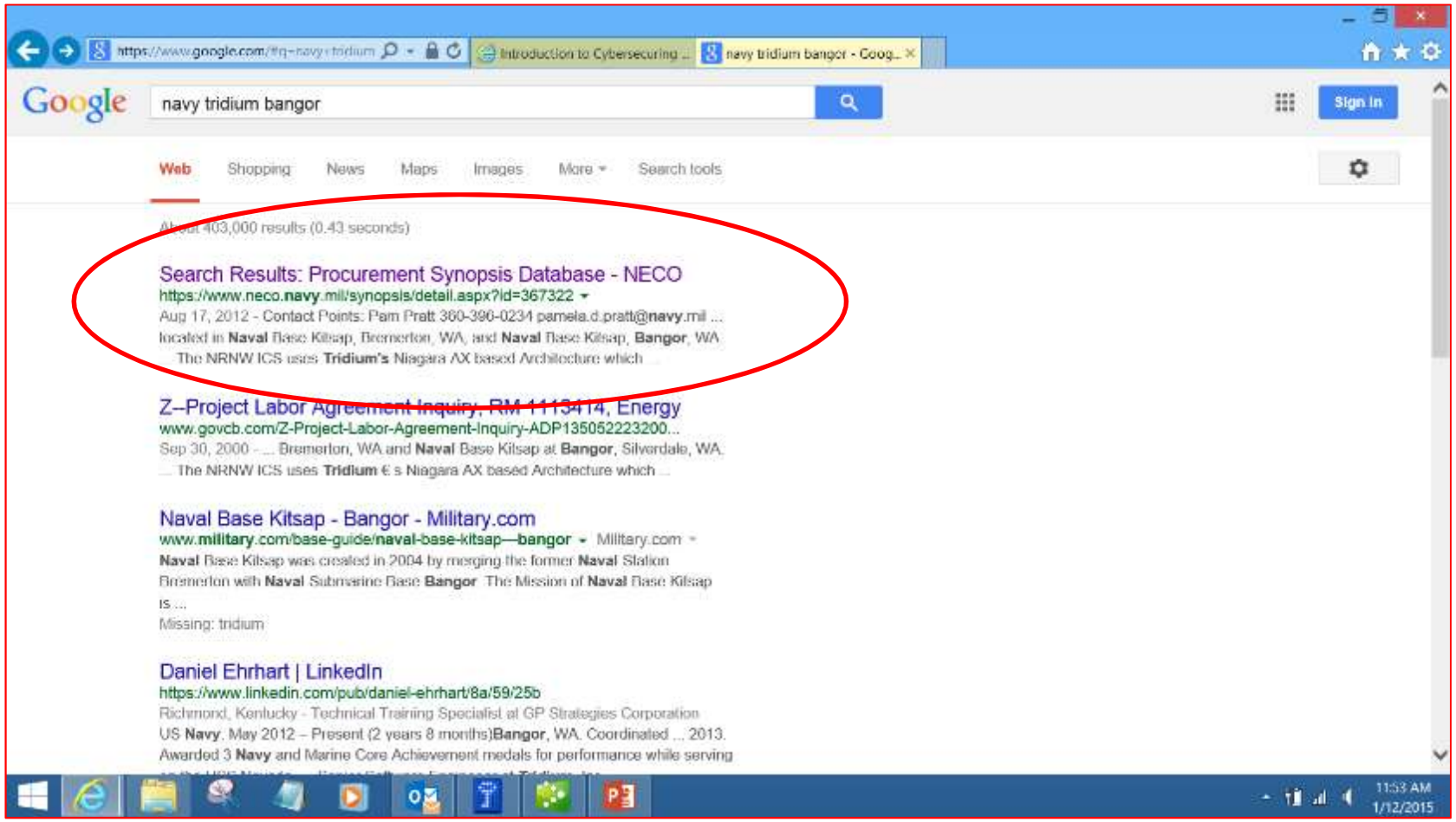
site:nibs.org filetype:doc

Google Hacking



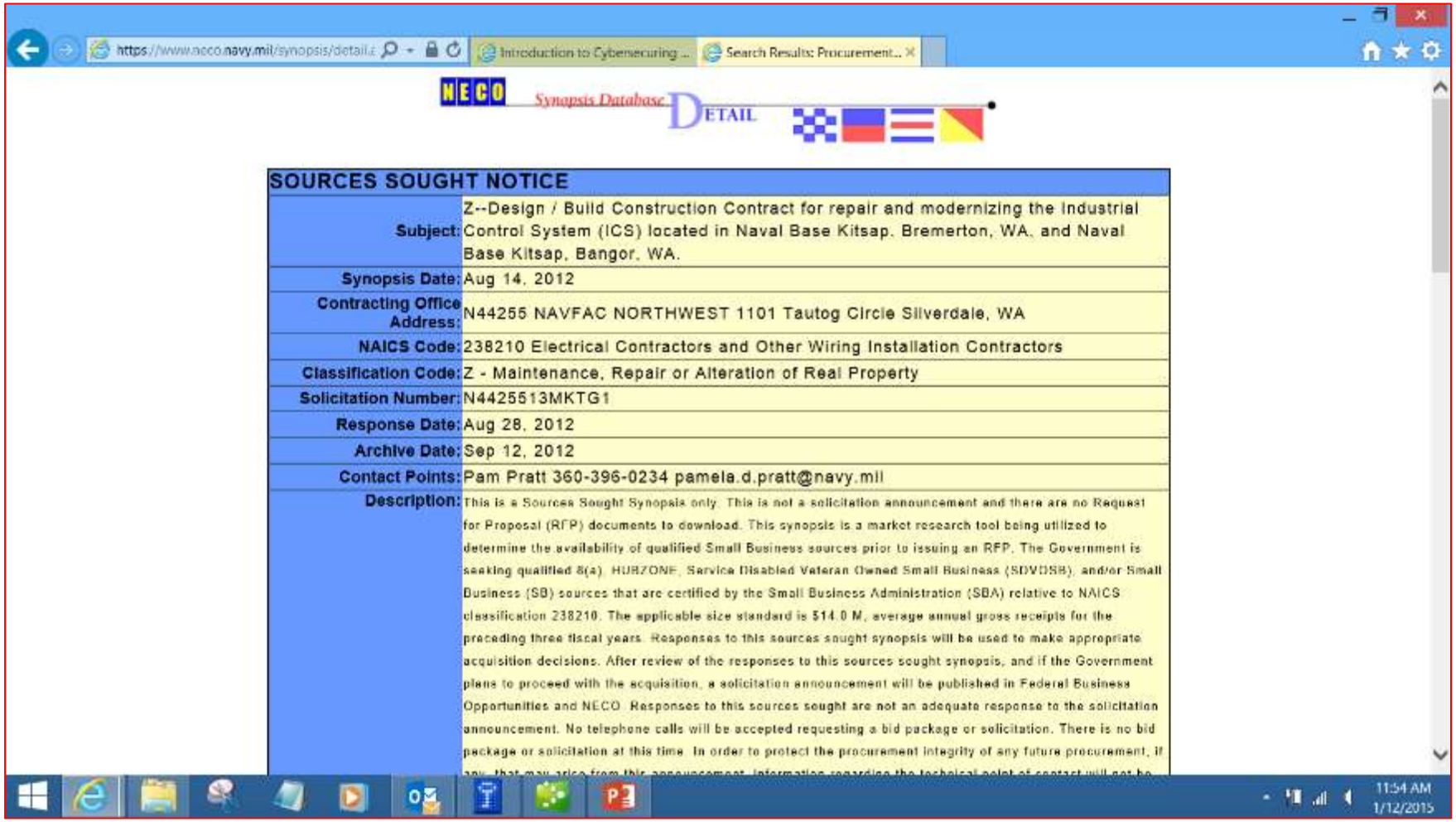
filetype:pdf -site:tridium.com site:mil

Google Hacking



https://www.google.com/#q=navy+tridium+bangor

Google Hacking

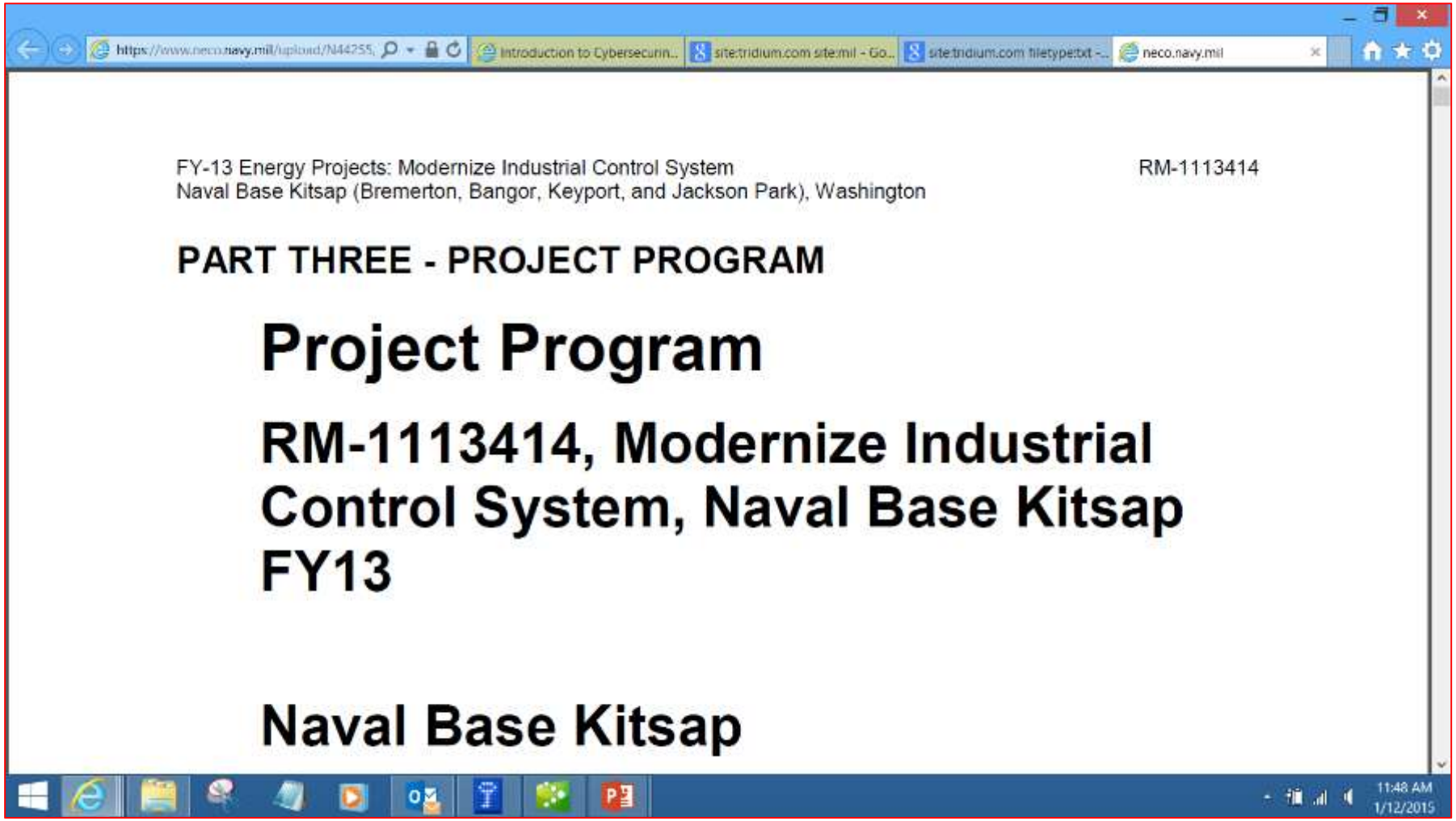


NECO Synopsis Database DETAIL

SOURCES SOUGHT NOTICE	
Subject:	Z--Design / Build Construction Contract for repair and modernizing the Industrial Control System (ICS) located in Naval Base Kitsap, Bremerton, WA, and Naval Base Kitsap, Bangor, WA.
Synopsis Date:	Aug 14, 2012
Contracting Office Address:	N44255 NAVFAC NORTHWEST 1101 Tautog Circle Silverdale, WA
NAICS Code:	238210 Electrical Contractors and Other Wiring Installation Contractors
Classification Code:	Z - Maintenance, Repair or Alteration of Real Property
Solicitation Number:	N4425513MKTG1
Response Date:	Aug 28, 2012
Archive Date:	Sep 12, 2012
Contact Points:	Pam Pratt 360-396-0234 pamela.d.pratt@navy.mil
Description:	This is a Sources Sought Synopsis only. This is not a solicitation announcement and there are no Request for Proposal (RFP) documents to download. This synopsis is a market research tool being utilized to determine the availability of qualified Small Business sources prior to issuing an RFP. The Government is seeking qualified 8(a), HUBZONE, Service Disabled Veteran Owned Small Business (SDVOSB), and/or Small Business (SB) sources that are certified by the Small Business Administration (SBA) relative to NAICS classification 238210. The applicable size standard is $14.0 M, average annual gross receipts for the preceding three fiscal years. Responses to this sources sought synopsis will be used to make appropriate acquisition decisions. After review of the responses to this sources sought synopsis, and if the Government plans to proceed with the acquisition, a solicitation announcement will be published in Federal Business Opportunities and NECO. Responses to this sources sought are not an adequate response to the solicitation announcement. No telephone calls will be accepted requesting a bid package or solicitation. There is no bid package or solicitation at this time. In order to protect the procurement integrity of any future procurement, if any, that may arise from this announcement, information regarding the technical point of contact will not be

https://www.neco.navy.mil/synopsis/detail.aspx?id=367322

Google Hacking



https://www.neco.navy.mil/upload/N44255/N4425513R40020005N4425513R40020005 N44255-13-R-4002_Part_3_Draft.pdf

Google Hacking Diggity Project

http://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/#searchdiggity

Google Hacking Diggity Project

Google | CodeSearch | Bing | LinkFromDomain | DLP | Flash | Malware | PortScan | NotInMyBackyard | BingMalware | Shodan

Simple | Advanced

Query Appender

Queries

- Default Credentials
- FTP
- Printer
- Router
- SCADA
  - Electro Industries Gauc
  - Photovoltaic
  - Rockwell SLC-505 PLC
  - SCADA USA
  - SCADA
    - scada
    - Niagara Web Serve
  - Siemens s7

SCAN | Cancel | Settings

API Key: | Create | Hide

Enter SHODAN API key

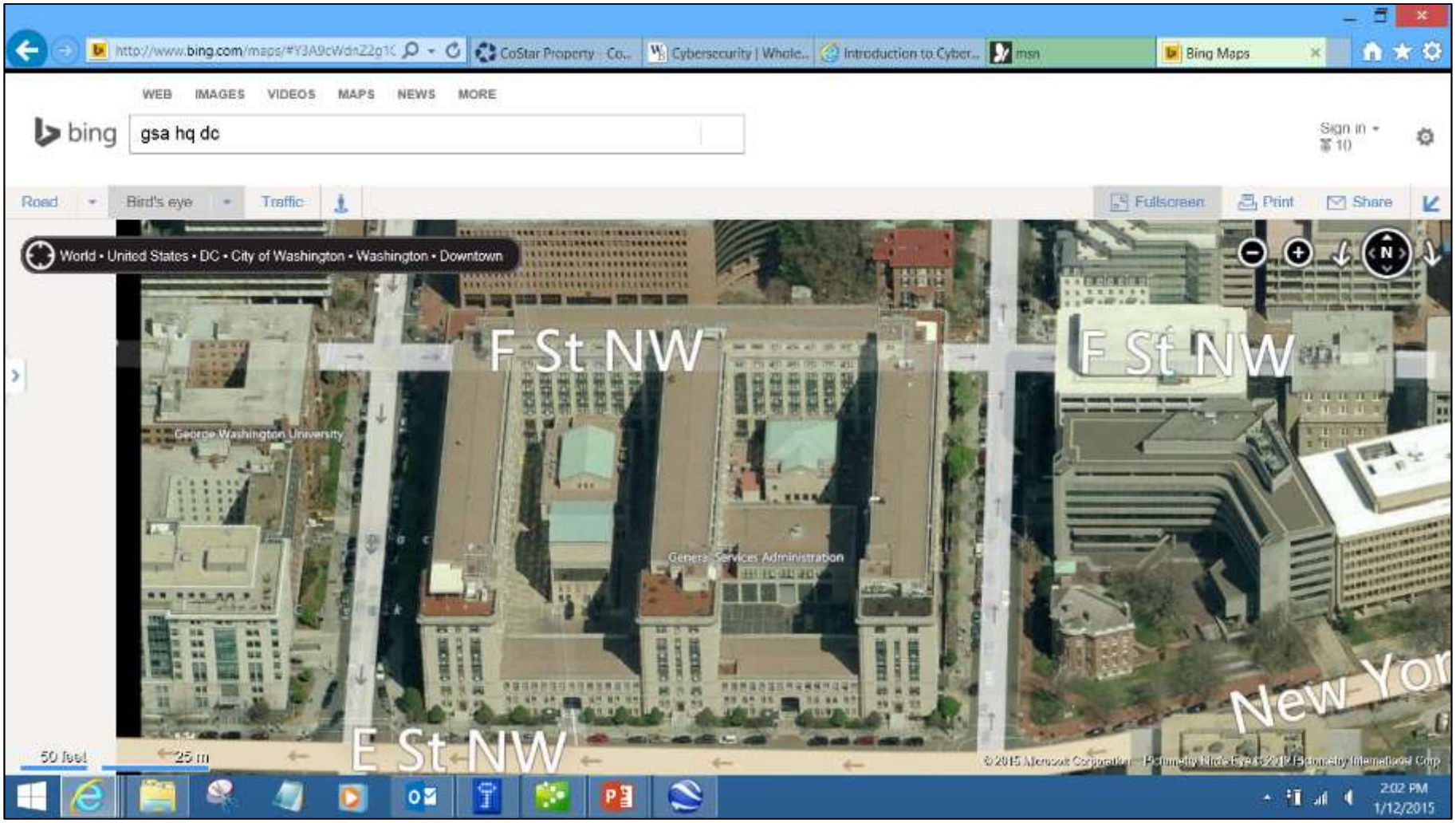
Category	Search String	URL	Hostnames	City	Country
SCADA	Niagara Web Server	http://193.185.169.90/			Finland
SCADA	Niagara Web Server	http://12.171.57.87/			United States
SCADA	Niagara Web Server	http://70.168.40.243/	wsip-70-168-40-243.	Cleveland	United States
SCADA	Niagara Web Server	http://216.241.207.94/	sciop-ip94.scinternet.	Colorado City	United States
SCADA	Niagara Web Server	http://206.82.16.227/	niagarafred.norleb.k1	Lancaster	United States
SCADA	Niagara Web Server	http://184.187.11.158/		Omaha	United States

Output | Selected Result

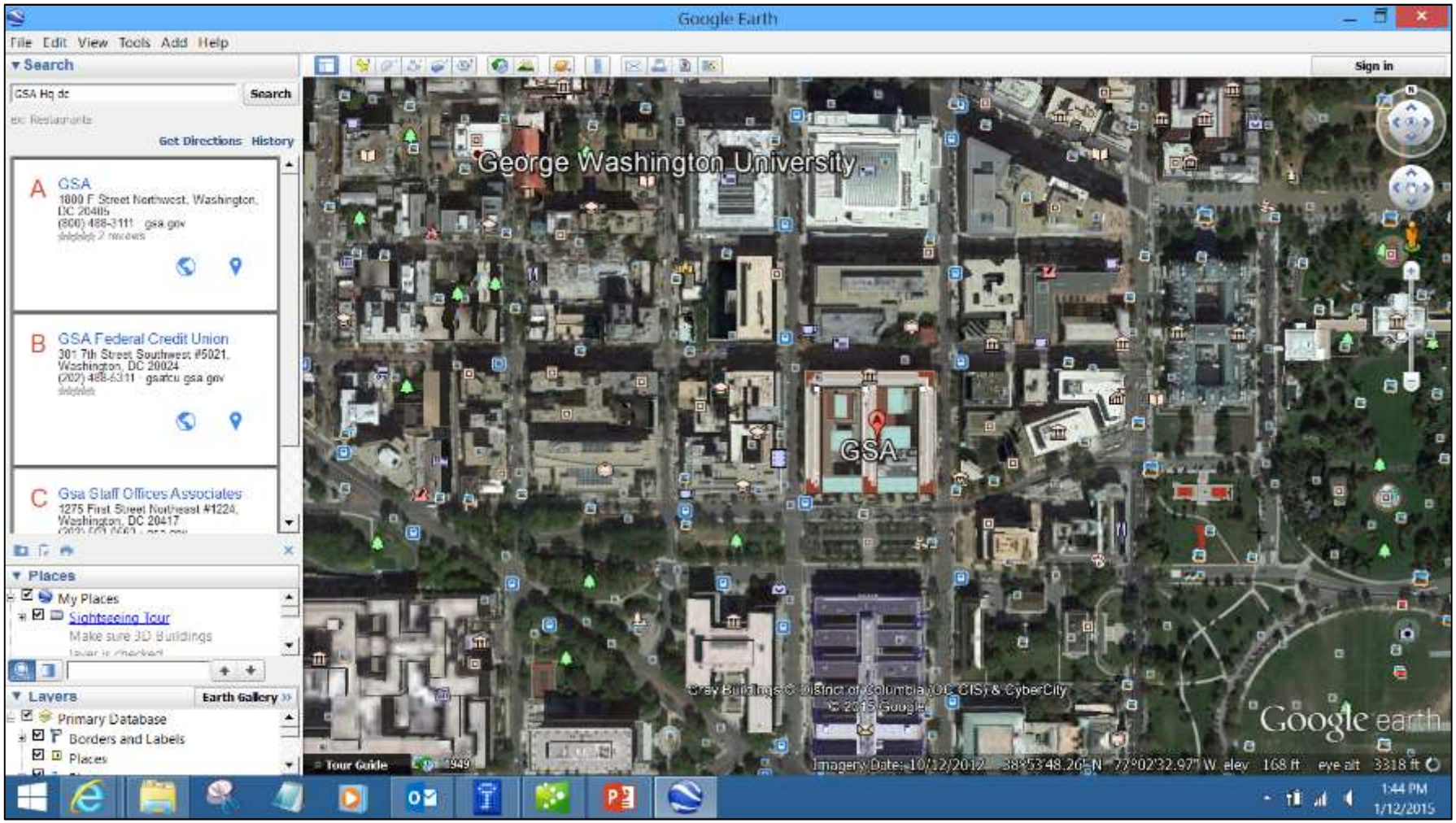
```
HTTP/1.0 302 Moved Temporarily
location: http://70.168.40.243/login
content-type: text/html; charset=UTF-8
content-length: 116
set-cookie: niagara_audit=guest; path=/
server: Niagara Web Server/3.5.34
```

Finding SCADA systems via SHODAN Diggity

BING


WEB
IMAGES
VIDEOS
MAPS
NEWS
MORE
bing
gsa hq dc
Road
Bird's eye
Traffic
Fullscreen
Print
Share
World • United States • DC • City of Washington • Washington • Downtown
F St NW
F St NW
E St NW
George Washington University
General Services Administration
50 feet
25 m
2:02 PM
1/12/2015

Google Earth



IPLocation

http://www.iplocation.net/

GSA Smart Buildings Sources Sought

Google Code The Harvester

https://code.google.com/p/theharvester/

theharvester
Information Gathering

Project Home | Downloads | Wiki | Issues | Source

Summary | People

Project Information

Project feeds

Code license
GNU GPL v2

Labels
informationgathering, osint, infogathering, security, public, information, profiling

Members
laramies@gmail.com

The objective of this program is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database.

This tool is intended to help Penetration testers in the early stages of the penetration test in order to understand the customer footprint on the Internet. It is also useful for anyone that wants to know what an attacker can see about their organization.

This is a complete rewrite of the tool with new features like:

- Time delays between request
- All sources search
- Virtual host verifier
- Active enumeration (DNS enumeration, Reverse lookups, TLD expansion)
- Integration with SHODAN computer database, to get the open ports and banners
- Save to XML and HTML
- Basic graph with stats
- New sources

Passive discovery:

Google: google search engine - www.google.com

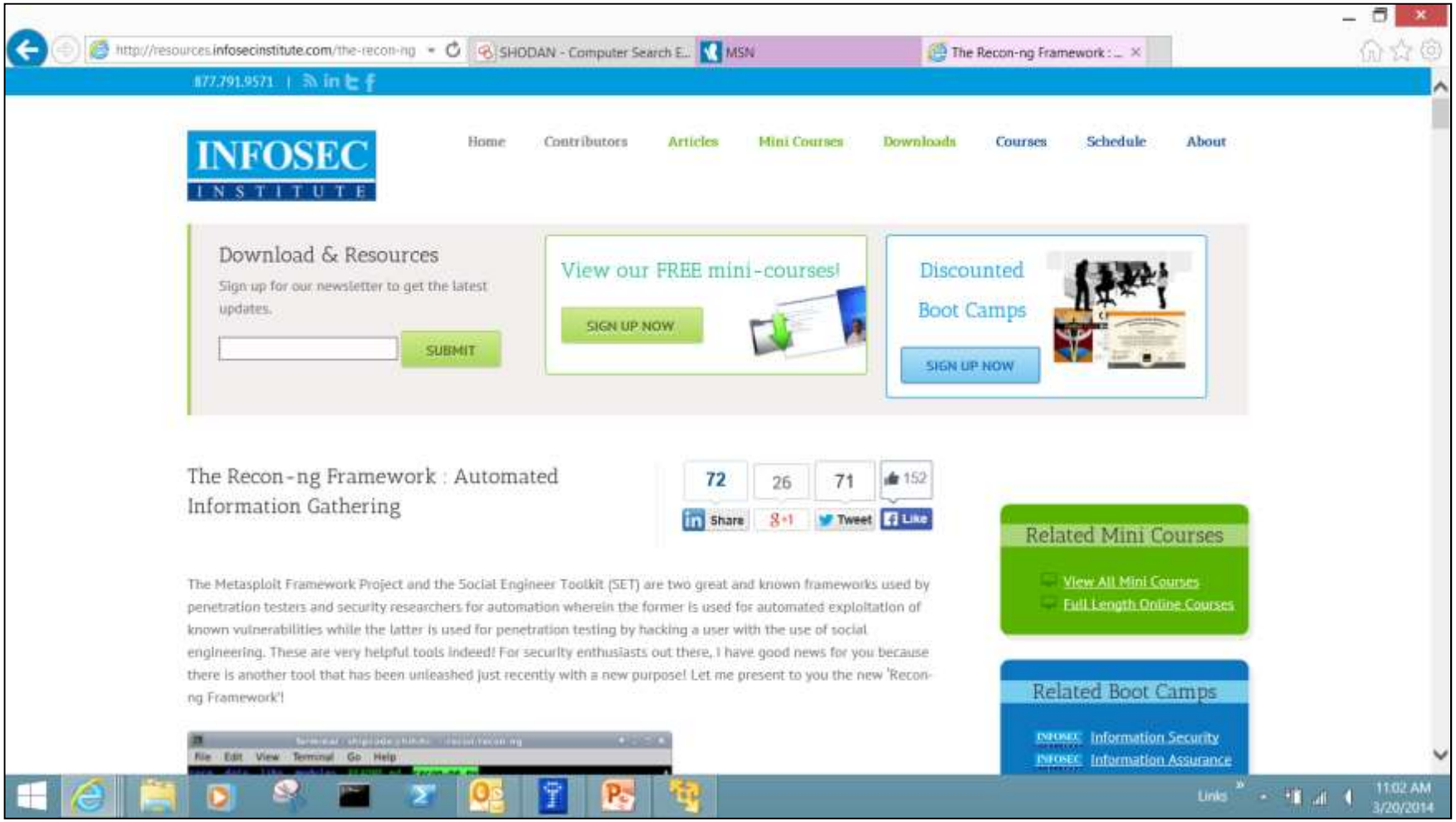
Google-profiles: google search engine, specific search for Google profiles

Bing: microsoft search engine - www.bing.com

Bingapi: microsoft search engine, through the API (you need to add your Key in the discovery/bingsearch.py file)

Pgp: pgp key server - pgp.rediris.es

Recon-NG

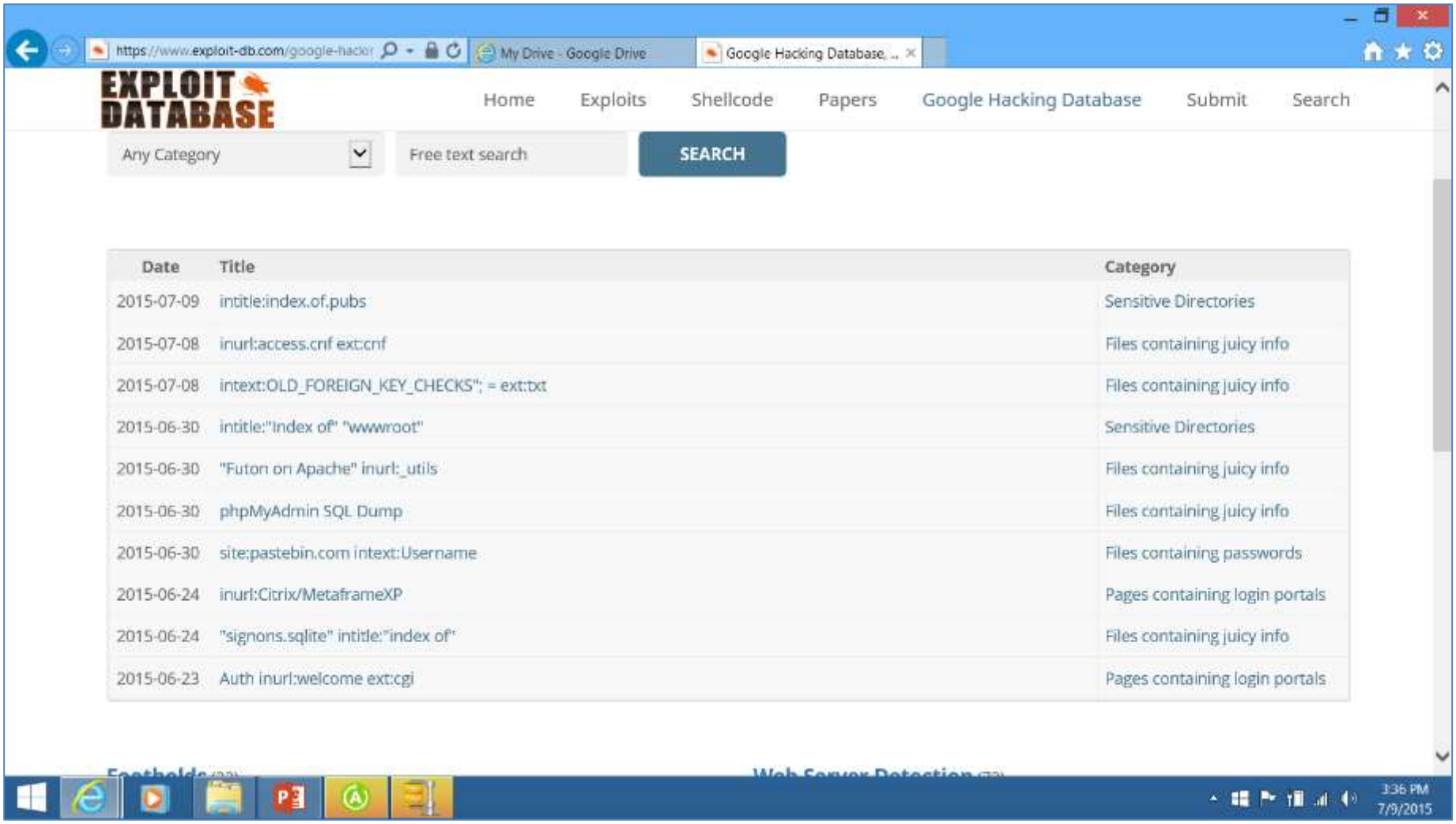


http://resources.infosecinstitute.com/the-recon-ng-framework-automated-information-gathering/

Exploit Database

https://www.exploit-db.com/

Exploit DB Categories



Exploit DB Search

https://www.exploit-db.com/google-hackin

My Drive - Google Drive | Google Hacking Database (...

EXPLOIT DATABASE

Home | Exploits | Shellcode | Papers | Google Hacking Database | Submit | Search

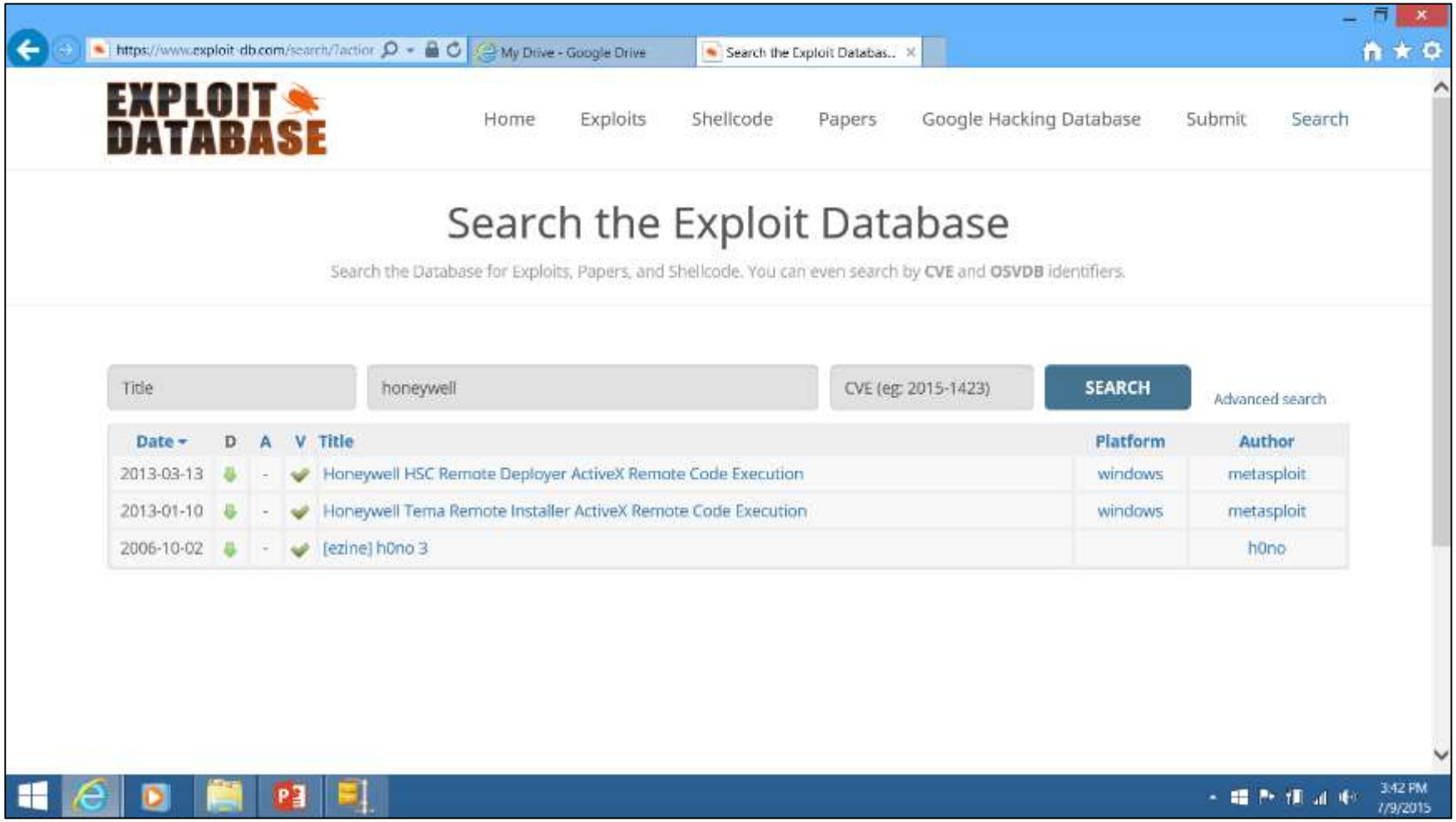
Any Category | Free text search | SEARCH

<< prev 1 2 3 4 5 6 7 8 9 10 >> next

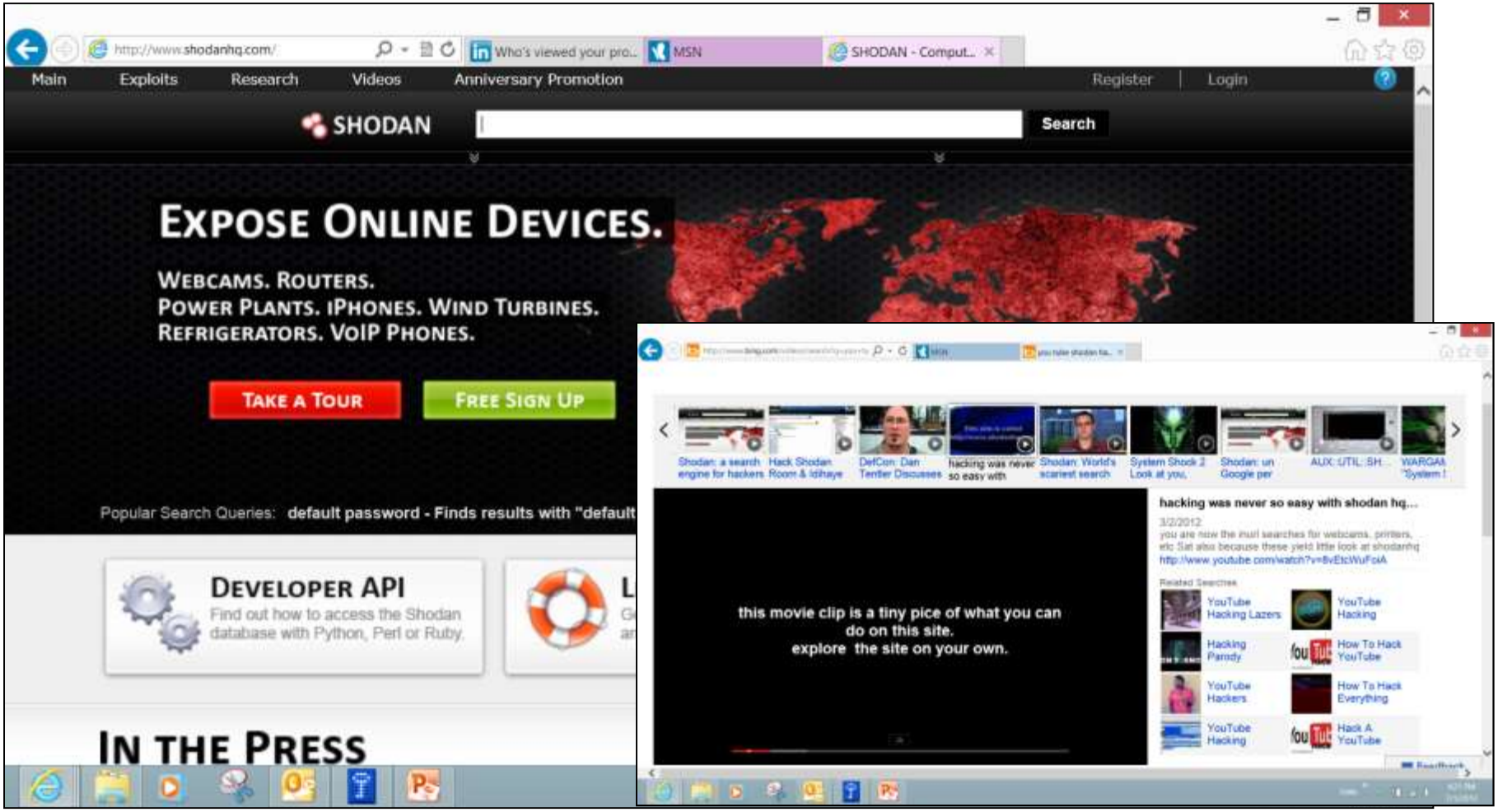
Date	Title	Summary
2015-07-09	inurl:"/certsrv" intext:"Select a task"	Various Online Devices Microsoft Certificate Request Webpage. Author: Felipe Molina (@felmoltor)
2015-07-09	intitle:index.of.pubs	Sensitive Directories Exploit title: intitle:index.of.pubs Description: intitle:index.of.pubs Sensitive Directories Author:fidah.org
2015-07-08	intext:OLD_FOREIGN_KEY_CHECKS"; = ext:txt	Files containing juicy info Google dork Description: MySQL dumpGoogle search: intext:OLD_FOREIGN_KEY_CHECKS"; = ext:txt by TN-N3SQU1K :)
2015-07-08	inurl:access.cnf ext:cnf	Files containing juicy info File vulnerability, reveals the path of Password Server. Have fun. This Dork is present By Rootkit.
2015-06-30	site:pastebin.com intext:Username	Files containing passwords # Exploit Title: [site:pastebin.com intext:Username] # Google Dork: [Pastebin Username & Password] # Date: [6/29/2015] # Exploit Author: [Daz Holme...

3:38 PM
7/9/2015

Exploit DB Search - Honeywell

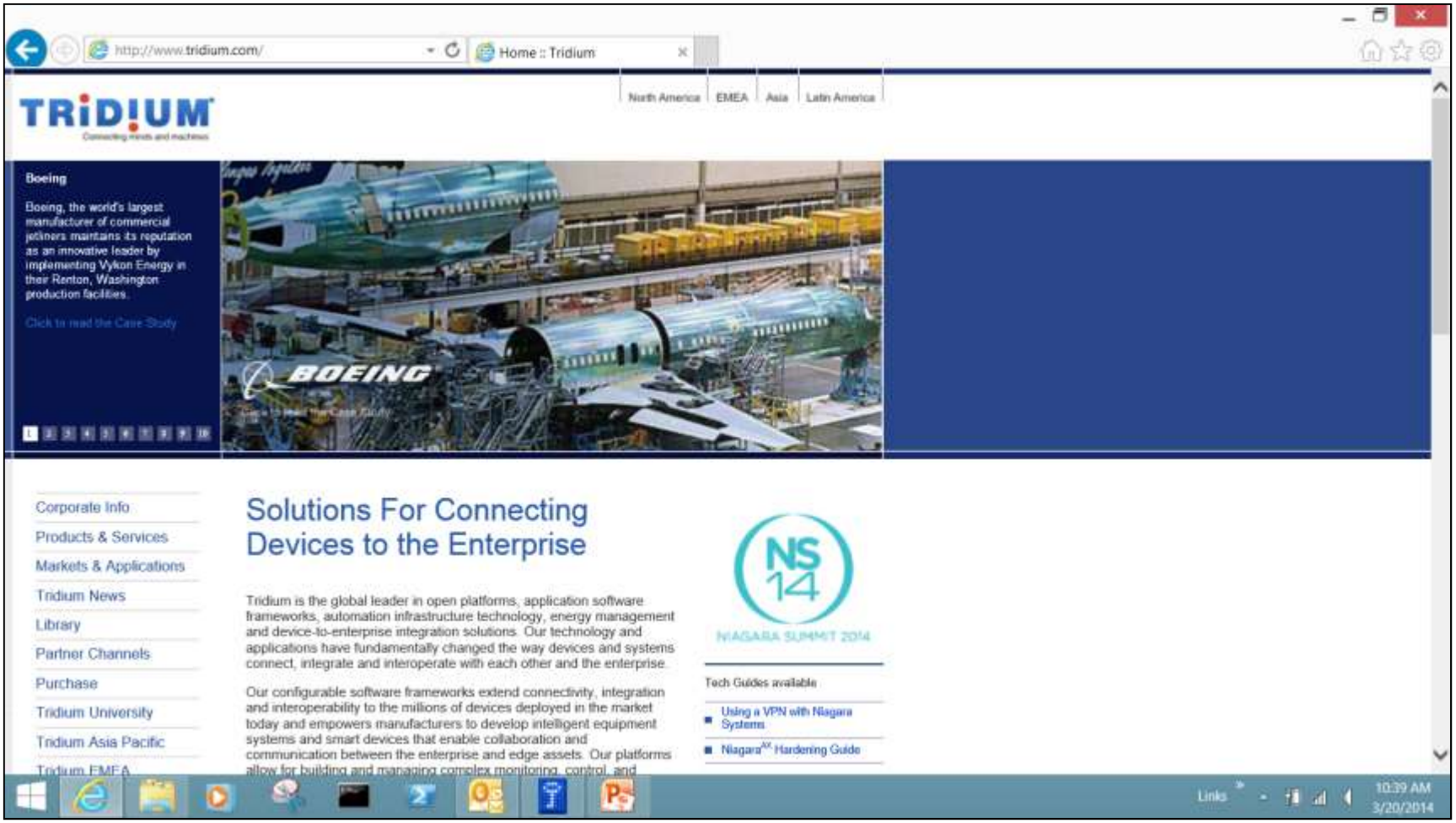


Shodan

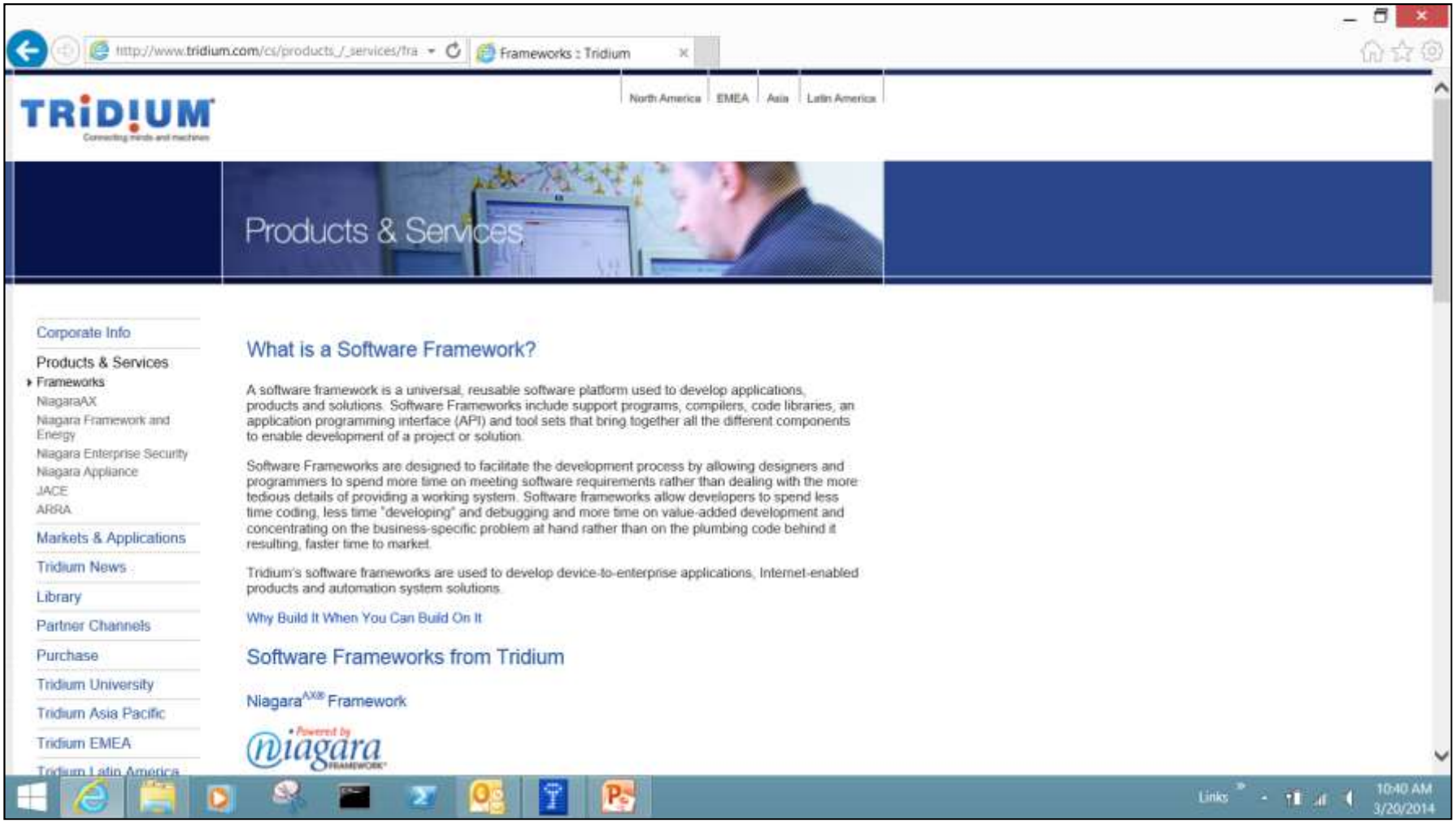


Shodan is to OT IP addresses as is Google is to text search

Tridium


http://www.tridium.com/
Home :: Tridium
TRIDIUM
North America
EMEA
Asia
Latin America
Boeing
Boeing, the world's largest manufacturer of commercial jetliners maintains its reputation as an innovative leader by implementing Vykon Energy in their Renton, Washington production facilities.
Click to read the Case Study
BOEING
Corporate Info
Products & Services
Markets & Applications
Tridium News
Library
Partner Channels
Purchase
Tridium University
Tridium Asia Pacific
Solutions For Connecting Devices to the Enterprise
Tridium is the global leader in open platforms, application software frameworks, automation infrastructure technology, energy management and device-to-enterprise integration solutions. Our technology and applications have fundamentally changed the way devices and systems connect, integrate and interoperate with each other and the enterprise.
Our configurable software frameworks extend connectivity, integration and interoperability to the millions of devices deployed in the market today and empowers manufacturers to develop intelligent equipment systems and smart devices that enable collaboration and communication between the enterprise and edge assets. Our platforms allow for building and managing complex monitoring, control, and
NS 14
NIAGARA SUMMIT 2014
Tech Guides available
Using a VPN with Niagara Systems
Niagara AX Hardening Guide
Links
10:39 AM
3/20/2014

Tridium Products and Services



Shodan – Tridium Search

http://www.shodanhq.com/search?q=tridium

SHODAN - Computer Searc...

Shodan | Exploits | Scanhub | Maps | Blog | Anniversary Promotion

SHODAN tridium Search

Services

NetBIOS	11
SNMP	9
SMB	3
HTTPS	1
FTP	1

Top Countries

United States	15
Norway	3
Malaysia	2
Turkey	1
Italy	1

Top Organizations

Telenor Norge AS	3
Techavenue Data Center...	2
tw telecom holdings	1
Wyoming.Com	1
Wave Broadband	1

97.78.98.252
Time Warner Cable
Added on 20.03.2014
Tampa
rrcs-97-78-98-252.se.biz.rr.com

```
NetBIOS Response
Servername: TRIDIUM-PC
MAC: b8:ca:3a:84:86:4f

Names:
TRIDIUM-PC <0x0>
WORKGROUP <0x0>
TRIDIUM-PC <0x20>
WORKGROUP <0x1e>
WORKGROUP <0x1d>
__MSBROWSE__ <0x1>
```

116.6.58.158
China Telecom Next Generation Carrier Network
Added on 20.03.2014
Guangzhou

```
NetBIOS Response
Servername: TRIDIUMPWS04
MAC: 00:50:b6:52:46:c3

Names:
TRIDIUMPWS04 <0x0>
TRIDIUM <0x0>
TRIDIUMPWS04 <0x20>
```

76.12.61.228
HostMy Site
Added on 18.03.2014
Newark

```
Tridium station
```

DDAN - Computer Search E... | Login

VictorPark_Super

Username:

Password:

Login

Distech Controls

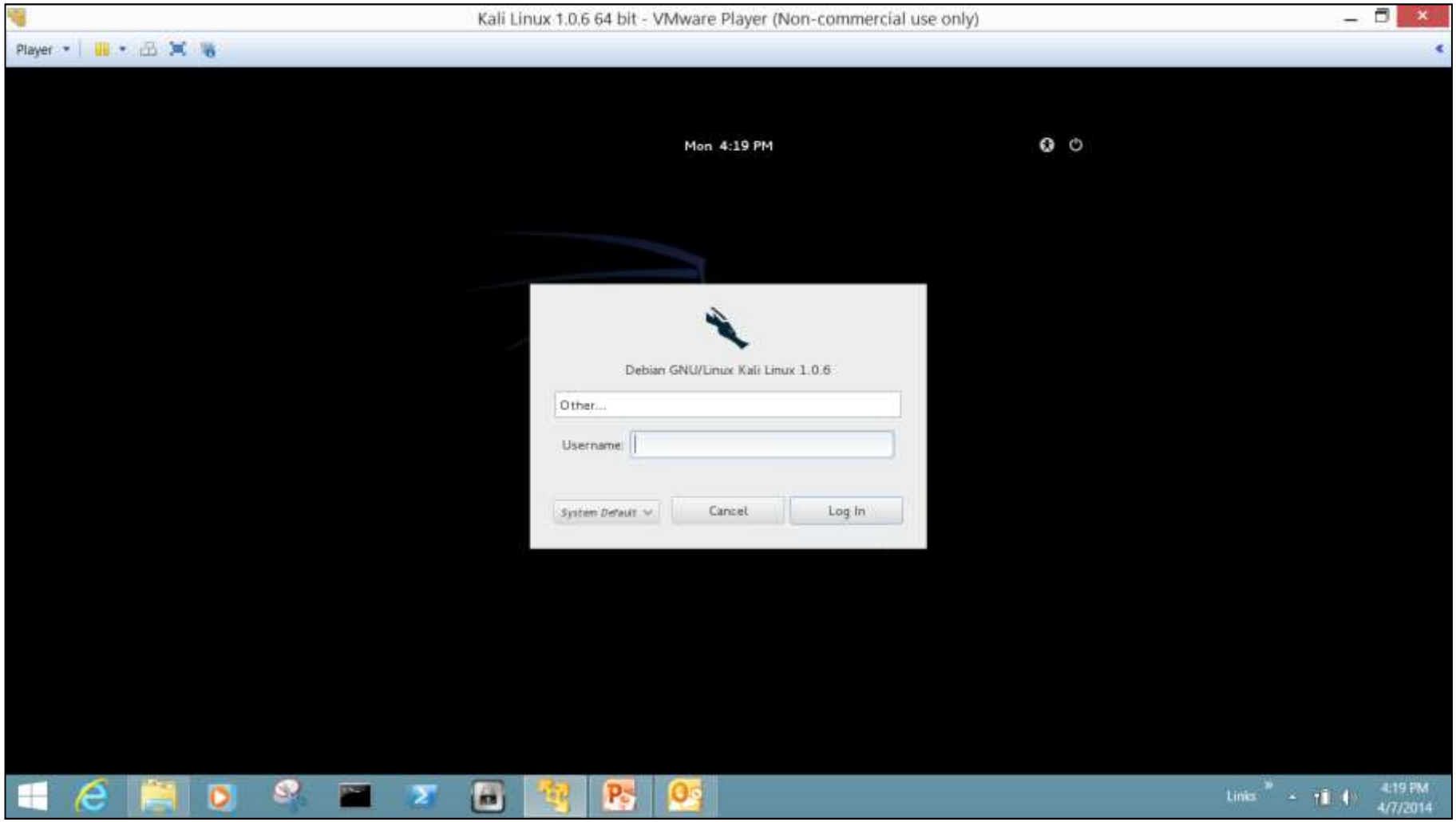
Shodan – Distech Search

HTTP/1.0 401 Unauthorized
WWW-Authenticate: Digest realm="**Niagara-Admin**", qop="auth", algorithm="**MD5**", nonce="UvdraWNmNDAwNjE1ODc4NzBhYTc5NjMyYzlkYTk3NTg1ZDQy"
Content-Length: 56
Content-Type: text/html
Niagara-Platform: QNX
Niagara-Started: 2013-8-3-4-11-32
Baja-Station-Brand: **distech**
Niagara-HostId: Qnx-NPM2-0000-12EA-FDCC
Server: **Niagara Web Server/3.0**

Kali Linux

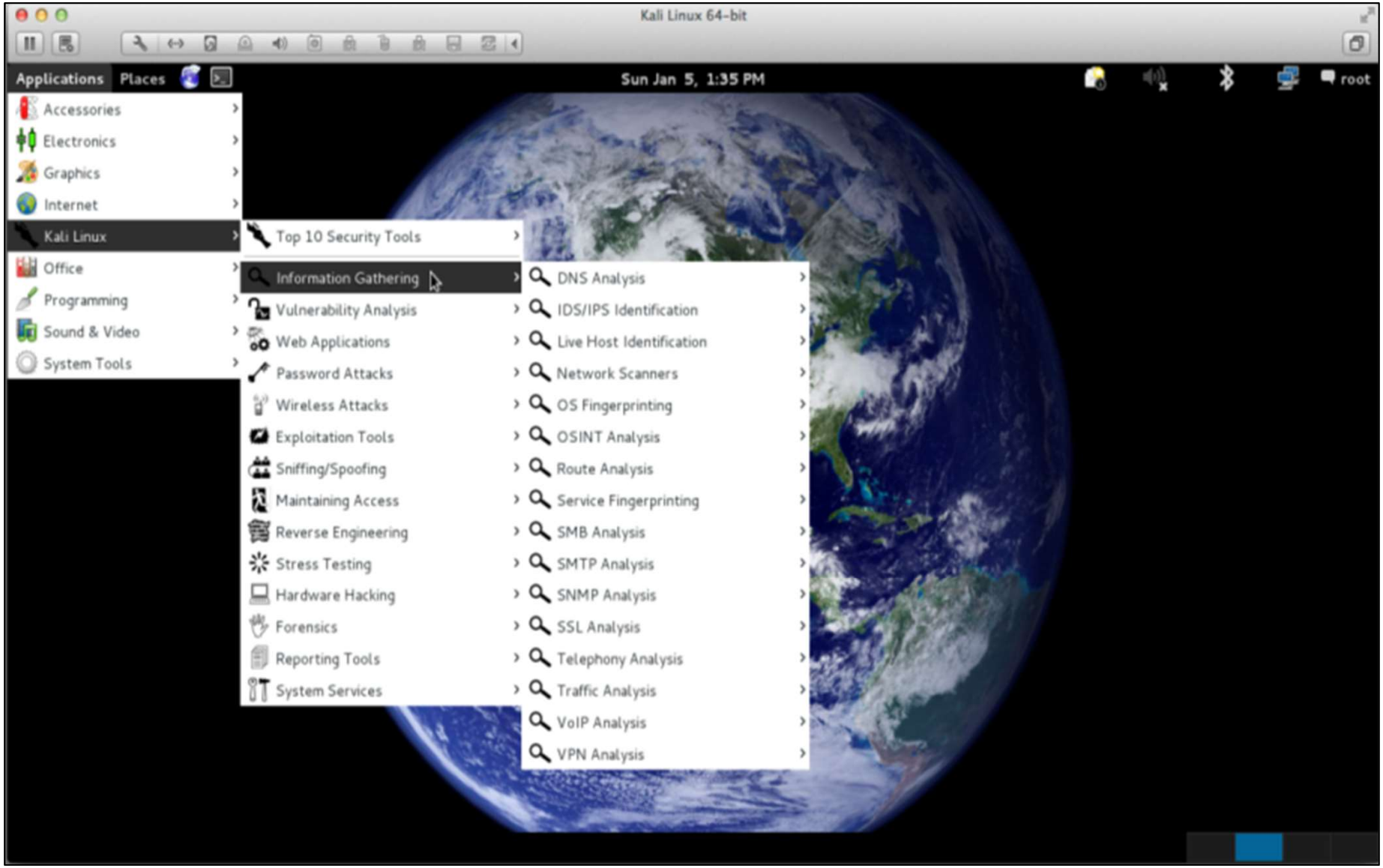
http://www.kali.org/

Kali Linux Login

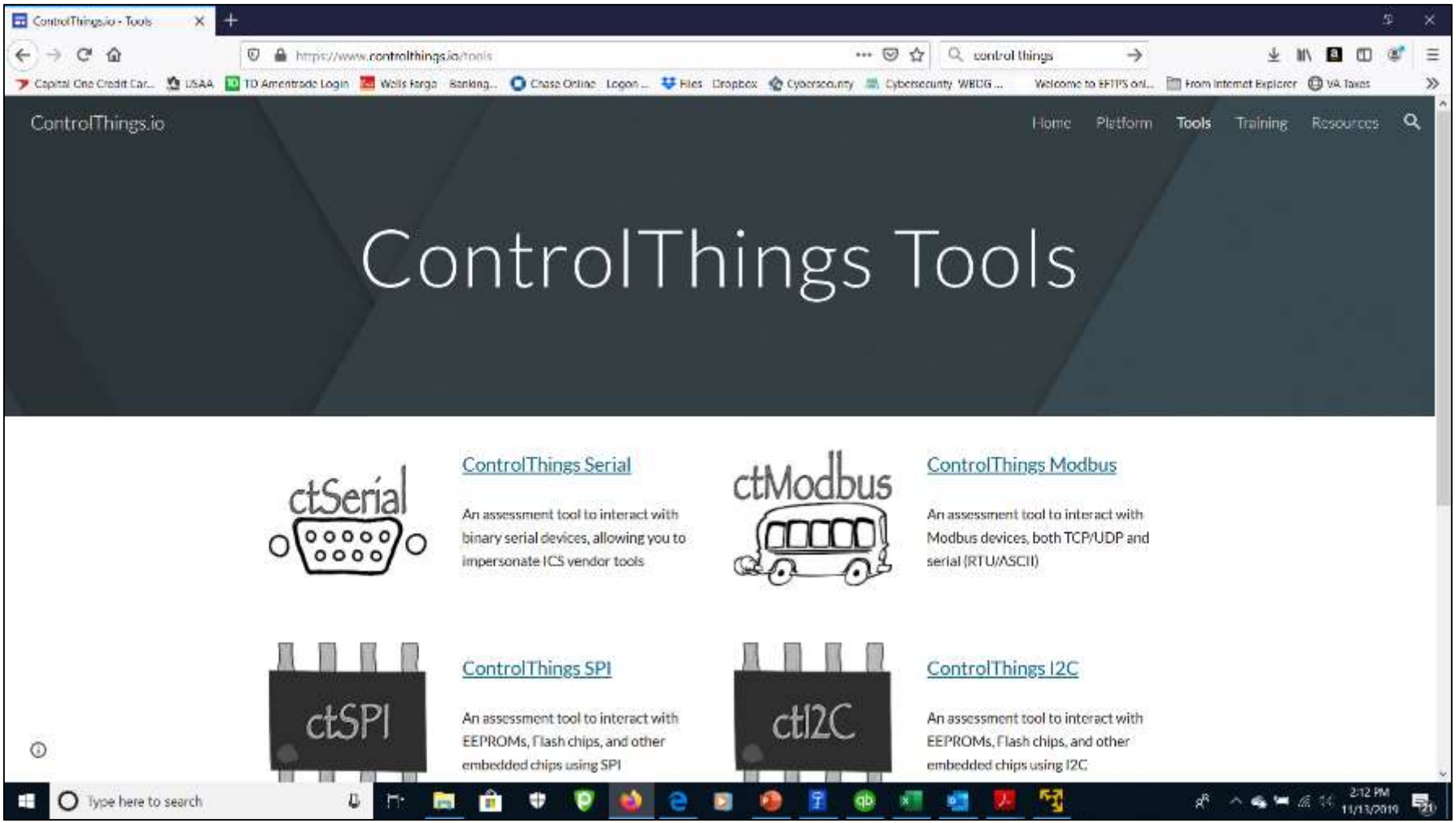


Bonus Section 2 illustrates using Kali to attack a control system

Kali Dojo Menu

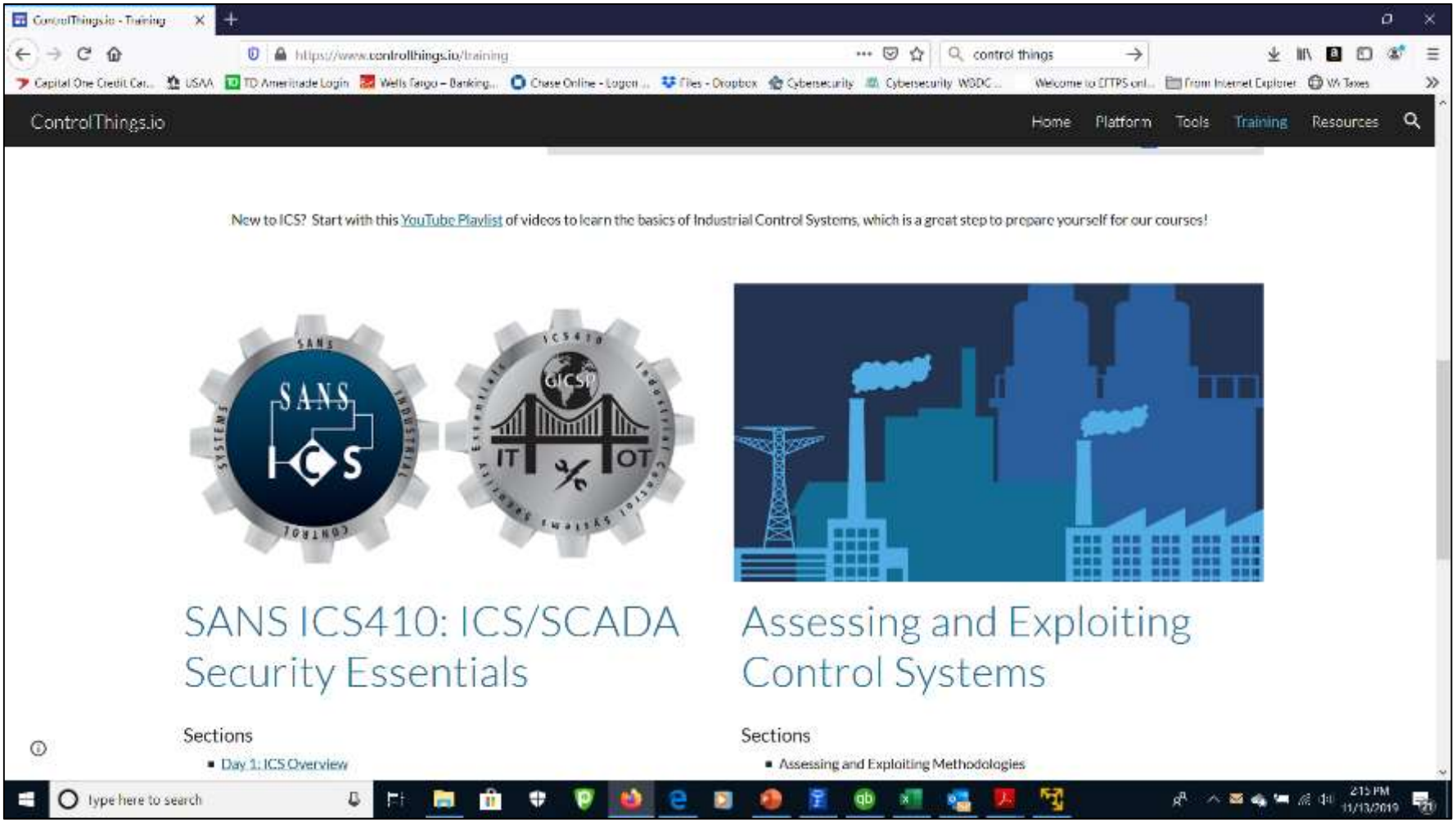


Control Things I/O



https://www.controlthings.io/tools

Control Things I/O



https://www.controlthings.io/training

SamuraiSTFU Applications

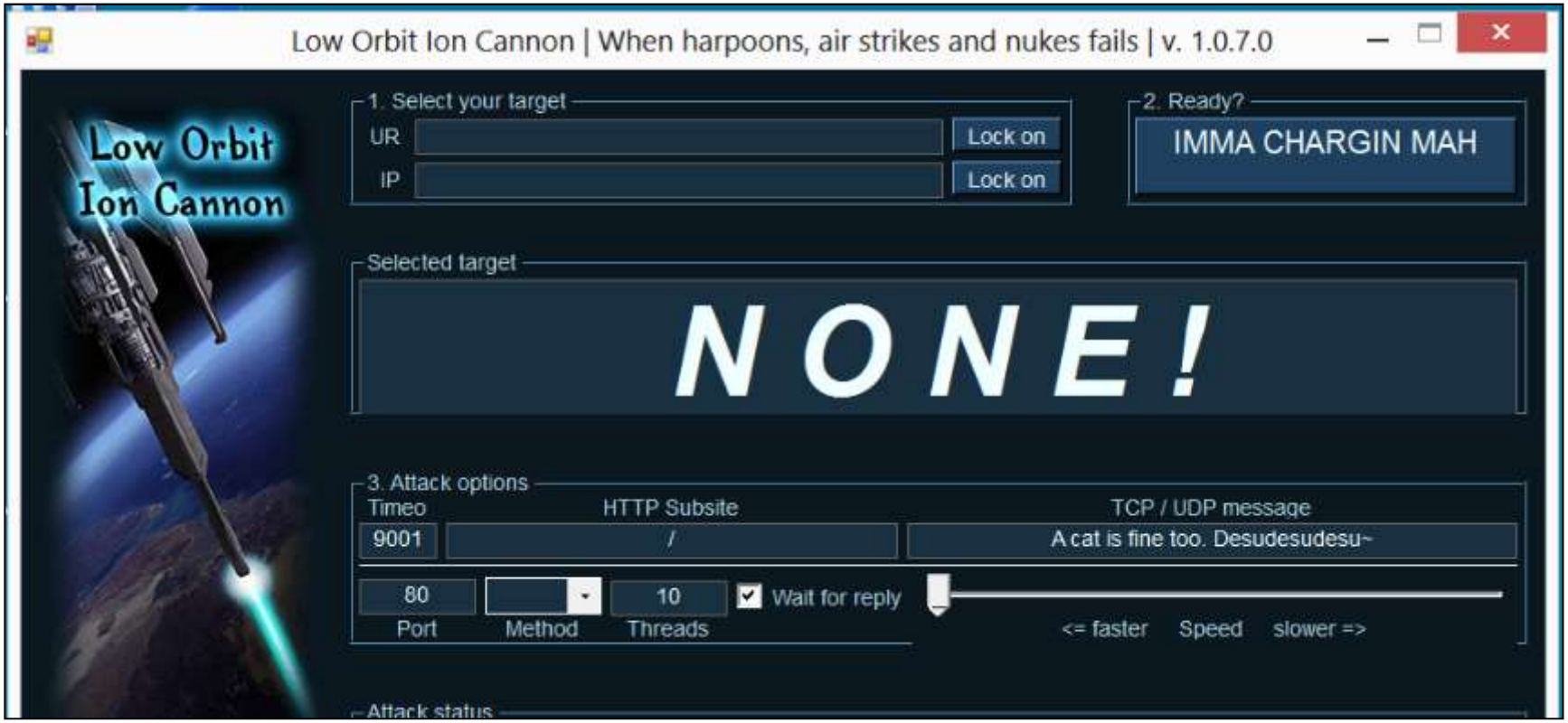
SamuraiSTFU Applications User Interfaces

Bonus Section 1 uses STFU and Modbus Pal to simulate controllers and network commands

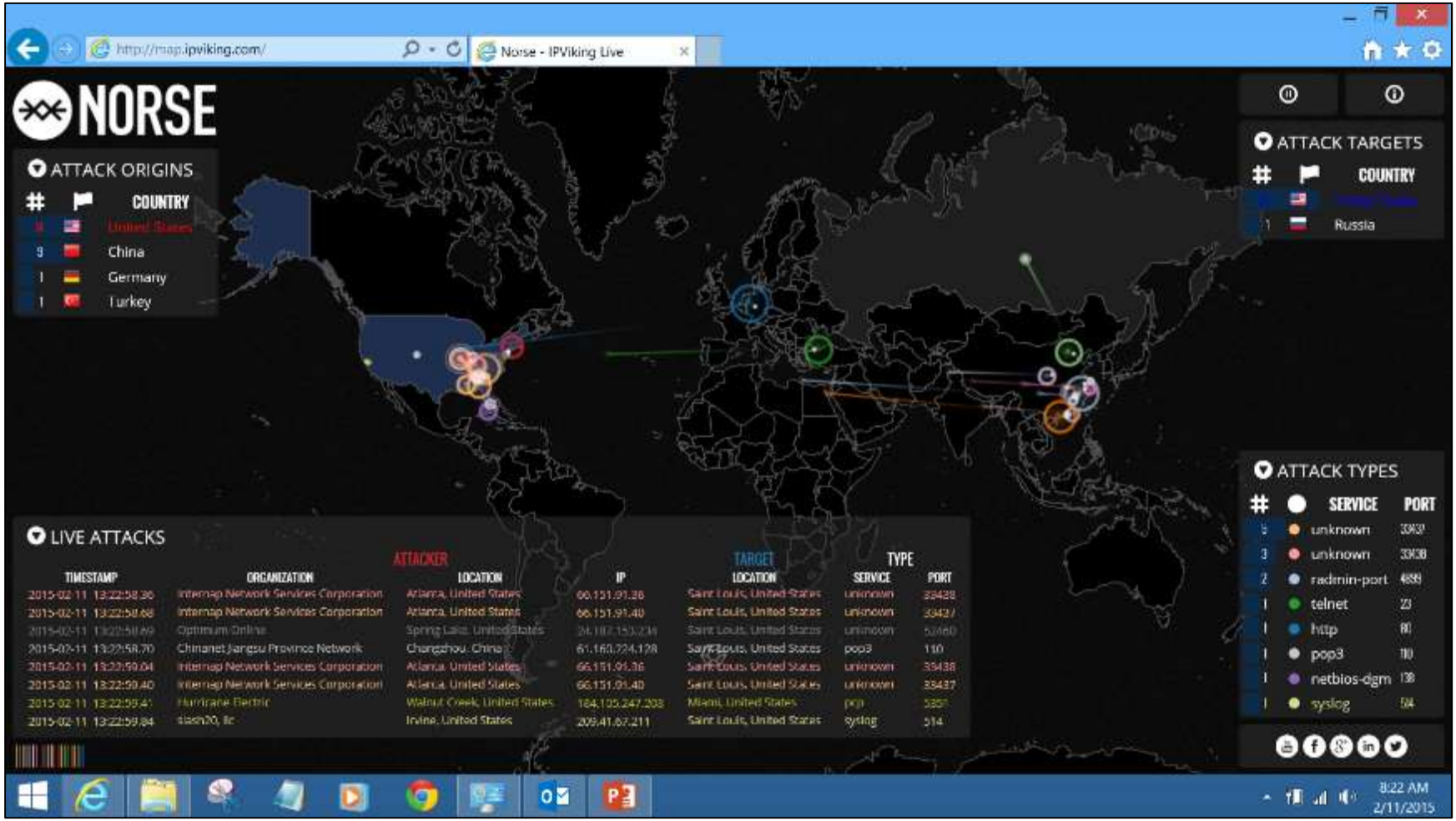
Tunneling - TOR

http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29

Low Orbit Cannon



IP Viking



http://map.ipviking.com/

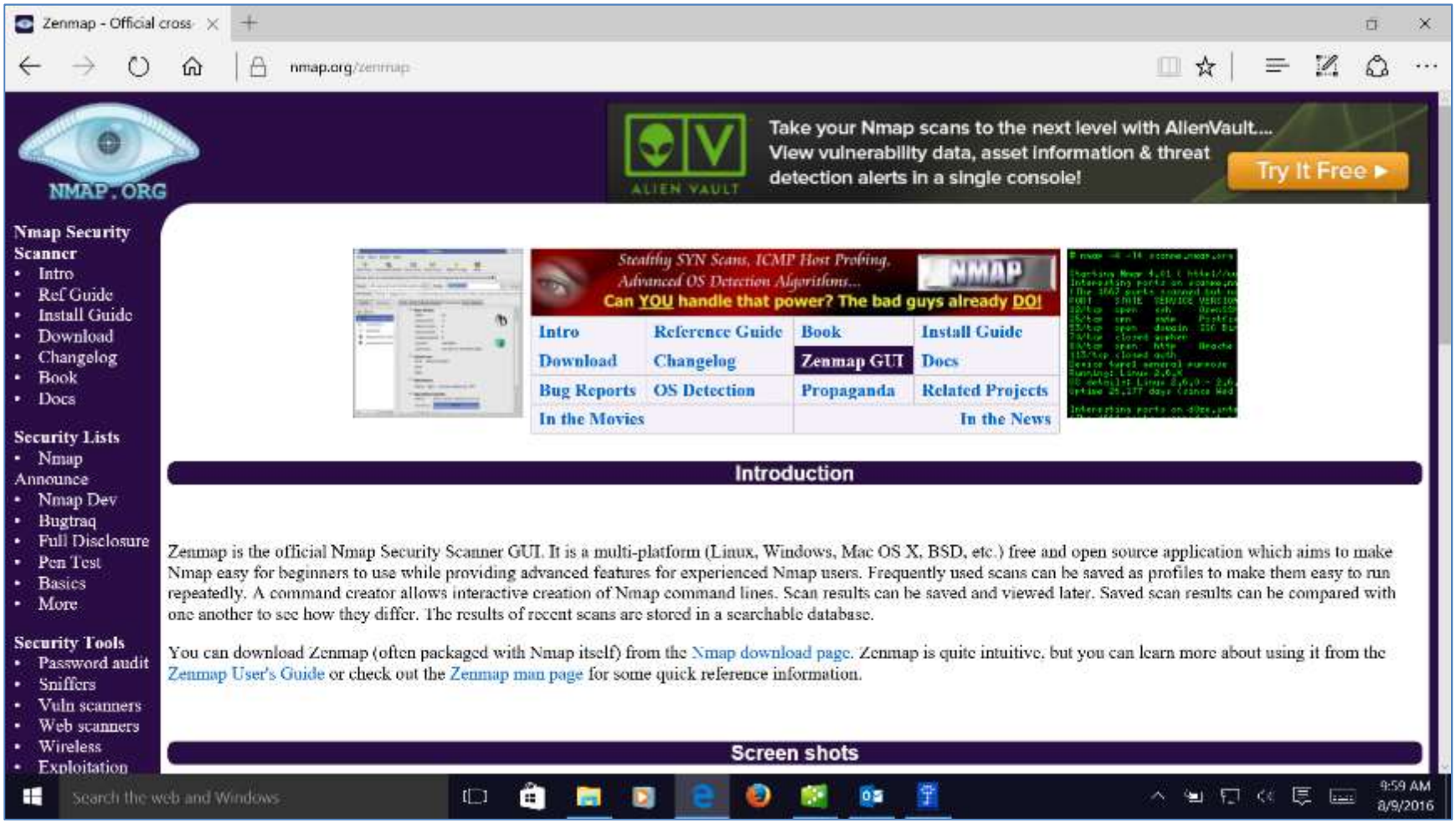
NMAP Homepage

http://nmap.org/

NMAP

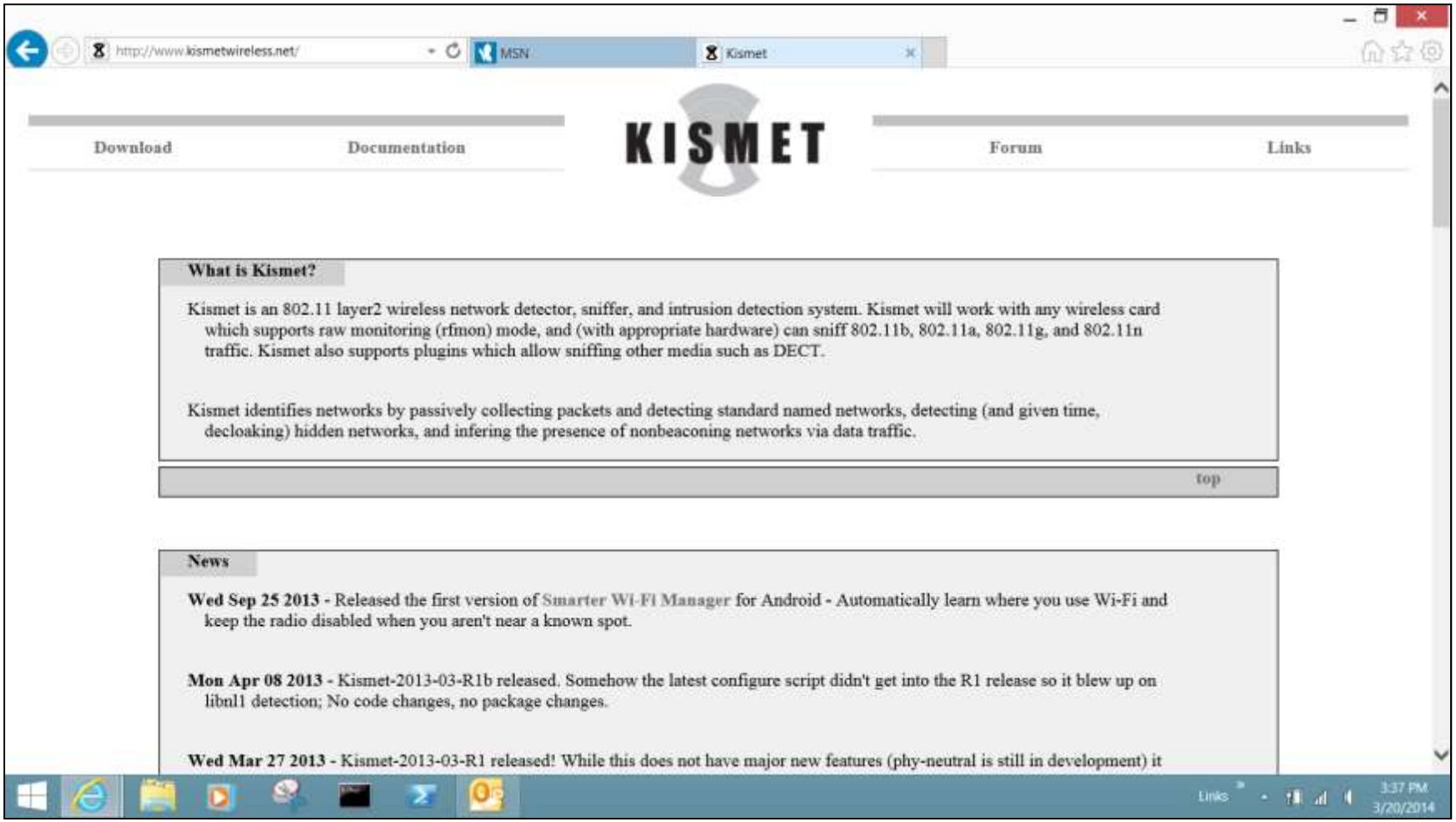
```
root@kali:~# nmap -h
Nmap 6.47 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```

Zenmap – Security Scanner



https://nmap.org/zenmap/

Kismet – 802 Detector, Sniffer and IDS



http://kismetwireless.net/

Digital Bond Bandolier (1)

http://www.digitalbond.com/tools/bandolier/

Blog Consulting S4 Critical Intelligence Podcast SCADApedia Tools About Us Advertise

digital bond

CODENOMICON

SECURE YOUR CRITICAL INFRASTRUCTURE AGAINST CYBER ATTACKS

ISASecure™ compliant robustness testing solutions

S4x14 Videos OTDay Presentations Project Basecamp Bandolier

Pages

- Consulting
- S4
- Critical Intelligence
- Podcast
- SCADApedia
- Tools
  - Bandolier
    - Bandolier FAQ
    - Downloads
    - List of Bandolier Security Audit Files
    - Bandolier Demonstration Video
    - Bandolier User Guide for Nessus
    - Bandolier and NERC CIP
    - Bandolier Baselines
    - NERC CIP Scan Policies
  - Basecamp
  - Portaledge
  - Quickdraw SCADA IDS
  - The Rack
  - SCADA Honeynet
  - ICS Security Tool Mail List
- About Us
- Advertise

Bandolier

Digital Bond's Bandolier project helps asset owners and vendors identify and audit optimal security configuration for industrial control system (ICS) servers and workstations. Digital Bond partners with leading ICS vendors to identify the optimal security configuration that still allows the vendor's product to operate properly. This requires access to the vendor's security experts, lead engineers and a test lab. Digital Bond then creates Bandolier Security Audit Files that work with the compliance plugin in the Nessus vulnerability scanner. Bandolier Security Audit Files are available for over twenty control system components, with more on the way.

Overview

- Defines optimal security configuration for SCADA and DCS servers and workstations
- Provides vendor-supported, customized security audit files for control system applications
- Provides a safe and effective way to audit the security of control system components

How it Works

- No client software, services, or agents are required on the control system server or workstation
- User uploads Bandolier Security Audit Files to the Nessus vulnerability scanner
- Nessus policy compliance plugins make a low impact connection to the ICS server or workstation
- Nessus uses built-in operating system functionality to compare the settings on the control system server to those defined in the Bandolier Security Audit File

Digital Bond Bandolier (2)

SCADA IDS Signatures

Digital Bond's SCADA IDS signatures, ***or rules in Snort parlance***, identify unauthorized requests, malformed protocol requests and responses, rarely used and dangerous commands, and other situations that are likely or possible attacks. There currently are signatures available for four control system protocols, a set of signatures to identify attacks on disclosed control system vulnerabilities, and a group of signatures that identify security events specific to a vendor system.

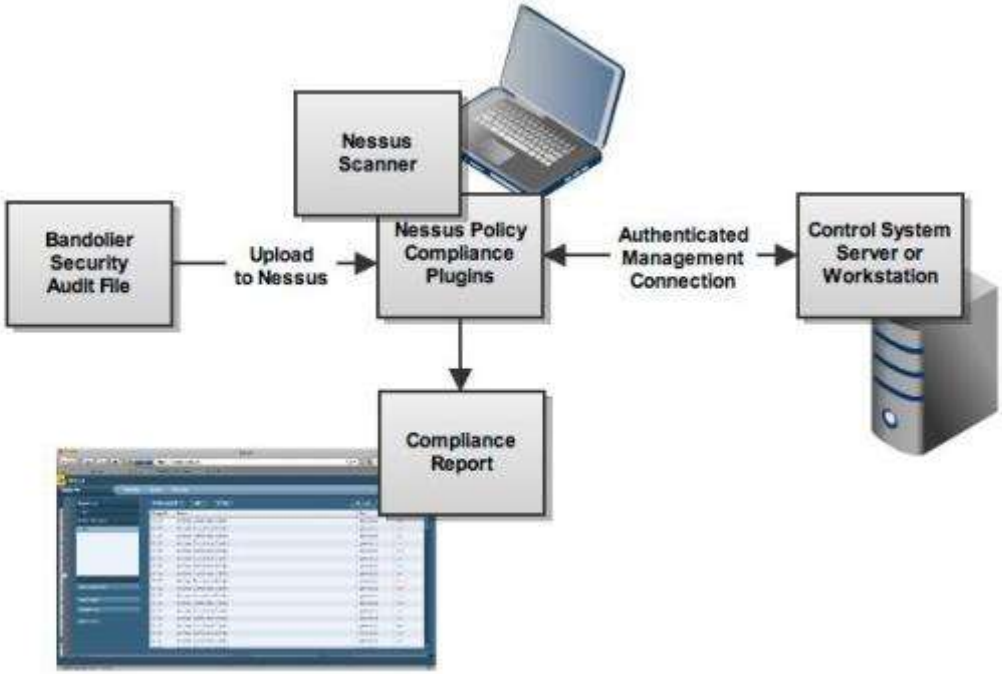
Available SCADA IDS Signatures

DNP3 IDS Signatures
EtherNet/IP Signatures
Modbus TCP Signatures
Vulnerability Signatures
Device Signatures

http://www.digitalbond.com/tools/quickdraw/

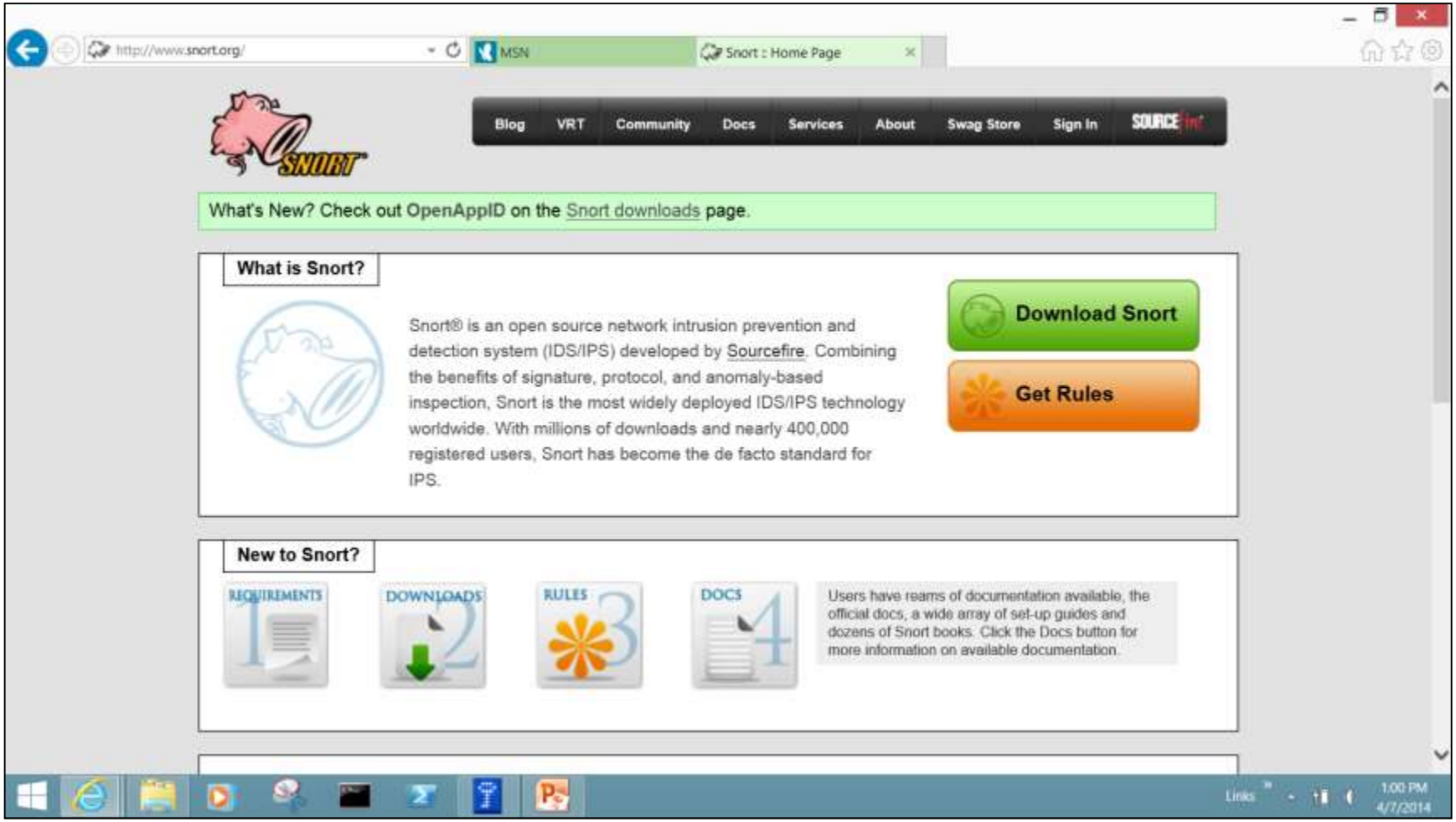
Digital Bond Bandolier-Nessus

Vendor	Application Name	Version	Operating System	Status
ABB	800xA PPA Connectivity Server	5.x	Windows Server 2003	1.0
ABB	800xA PPA Aspect Server	5.x	Windows Server 2003	1.0



https://www.digitalbond.com/tools/bandolier/

Snort



Snort is the most widely deployed IDS/IPS technology worldwide.

http://www.snort.org/

Gleg

GLEG - information ...

GLEG

Home Products Services Partners About

When security is not an option

The eldest among Canvas addon pack developers

→ READ MORE

agora

NEW: SCADA+ Pack

- An effort towards 100% public SCADA vulns coverage
- 0 Days for SCADA!
- Focused on Industrial software & hardware environment
- Weak points analyses

→ READ MORE

GLEG - information ...

GLEG

contact us | support

search

Home Products Services Partners About

Home > Products

- Agora Pack
- SCADA+ Pack
- Immunity's Canvas + 3rd party packs
- How to buy

SCADA+ Pack

This is an attempt to collect ALL publicly available SCADA vulnerabilities in one exploit Pack.
SCADA and related vulnerabilities are very special due to their sensitive nature and possible huge impact involved to successfull exploitation.
SCADA Systems are also "hard to patch", so even old vulnerabilities are actual.

The SCADA+ Pack features:

- Growing value
  Due to low real systems patch rank
- We try to cover most of the public SCADA vulns!
  Including old and newly discovered bugs
- 0 Days for SCADA
  We conduct our own in depth research
- Focused on Industrial software & hardware environment
  Not only SCADA, but also Industrial PCs, smart chips and industrial protocols are reviewed.
- Weak points analyses
  Many industrial things suffer from weaknesses like hardcoded password and etc.

Latest updates stuff is here :
Some videos and demos here :
For how to buy information - refer here

Exploits written specifically for SCADA

Hypervisor and Virtual Machines

A **hypervisor** or **virtual machine monitor** (**VMM**) is a piece of computer software, firmware or hardware that creates and runs virtual machines.

What are Virtual Machines (VM)?

A virtual machine (VM) is a ***software implementation of a machine*** (e.g., a computer) that ***executes programs like a physical machine***.

A system virtual machine provides a complete system platform which supports the execution of a complete operating system (OS). These usually ***emulate an existing architecture***, and are built with the purpose of either providing a platform to run programs where the real hardware is not available for use (for example, ***executing on otherwise obsolete platforms***), or of having multiple instances of virtual machines leading to ***more efficient use of computing resources***, both in terms of energy consumption and cost effectiveness (known as hardware virtualization, the key to a cloud computing environment), or both.

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

Why Use a VM?

Advantages of VM

- Can open multiple VM's with different OS
- Can create a complete reproduction of a Production environment
  Can create a Test and Development environment
- Reproducibility, can
- Malware in a VM is terminated when VM is powered down
- Server consolidation is the most compelling benefit of VMs. A typical non-virtualized application server may reach just 5% to 10% utilization. But a virtual server that hosts multiple VMs can easily reach 50% to 80% utilization. The net result is that more virtual machines can be hosted on fewer physical servers, translating into lower costs for hardware acquisition, maintenance, energy and cooling system usage.

Disadvantages of VM

- Requires heavy CPU use, memory, and hard disk space
- Not as efficient as a real machine when accessing the actual hardware
- Can cause instability

http://searchservervirtualization.techtarget.com/tip/Understanding-the-benefits-of-a-virtual-machine

Windows Virtual Machines

http://windows.microsoft.com/en-us/windows-8/h

MSN

Run virtual machines on Wi...

Windows

MEET WINDOWS DOWNLOAD & SHOP HOW-TO SUPPORT

Sign in

Installation Search & touch Personalization Security & accounts Apps & Windows Store Web & networks Email & communication Music & photos

Run virtual machines on Windows 8.1 with Client Hyper-V

Applies to Windows 8.1

Whether you're a software developer, IT administrator, or simply an enthusiast, you might want to run multiple operating systems on a single PC.

Windows 8.1 includes Hyper-V, the same machine virtualization technology that is part of Windows Server. Hyper-V lets you run more than one 32-bit or 64-bit x86 operating system at the same time on the same PC, by running them inside a virtual machine. Hyper-V replaces Windows Virtual PC in Windows 7, but doesn't include Windows XP Mode.

Install the Hyper-V role and configure a virtual machine

To enable Hyper-V on Windows 8.1

1. In Control Panel, tap or click **Programs**, and then tap or click **Programs and Features**.
2. Tap or click **Turn Windows Features on or off**.
3. Select **Hyper-V**, tap or click **OK**, and then tap or click **Close**.
4. Shut down your PC, and then restart it.

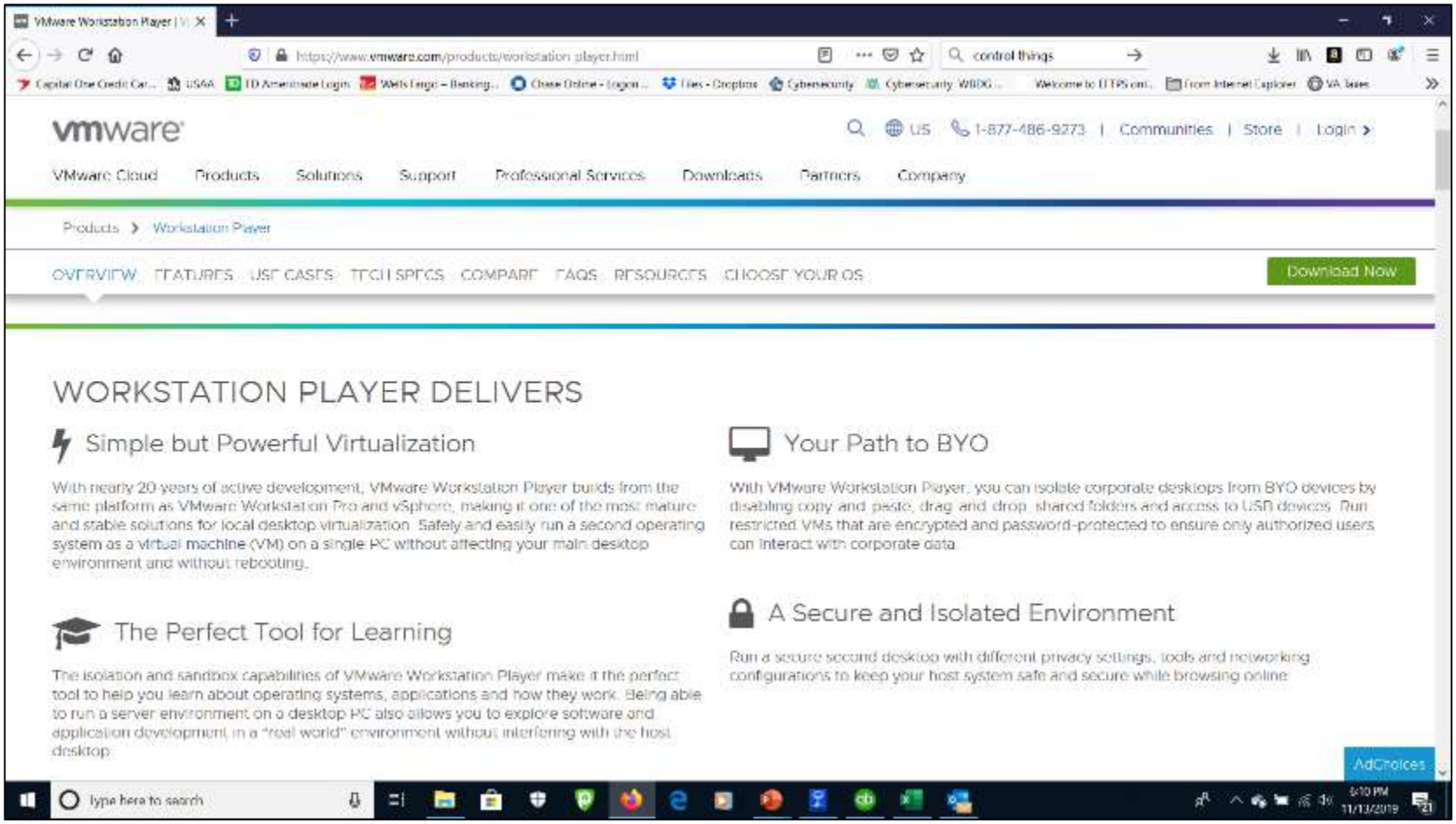
   Depending on your manufacturer, you might have to pause a few seconds with the PC off before restarting for the required changes to take effect. If you're using a laptop, you might have to remove the battery before restarting.

Links

4:07 PM
3/27/2014

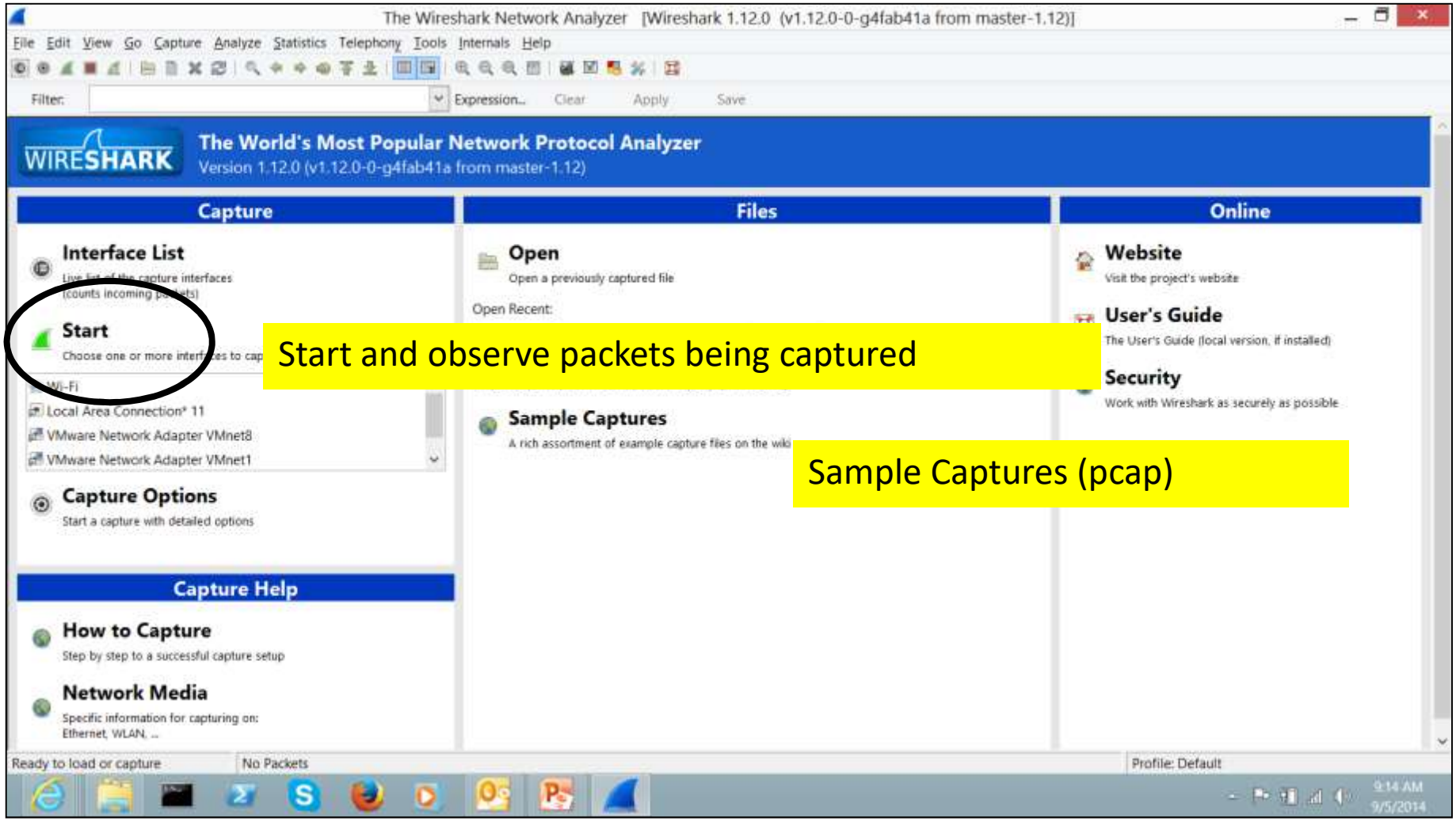
http://windows.microsoft.com/en-us/windows-8/hyper-v-run-virtual-machines

VMWare



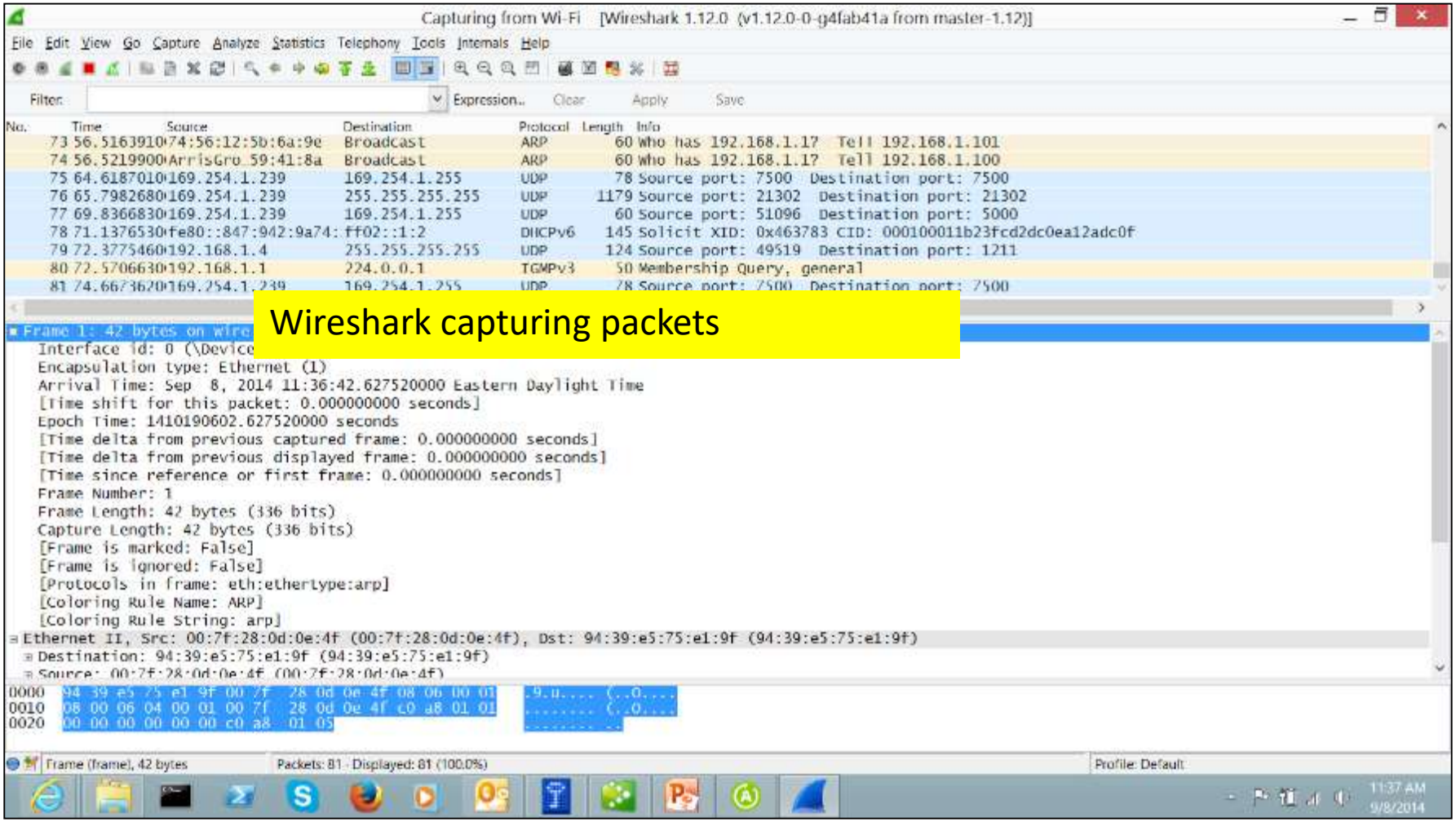
https://www.vmware.com/products/workstation-player.html

Wireshark Home

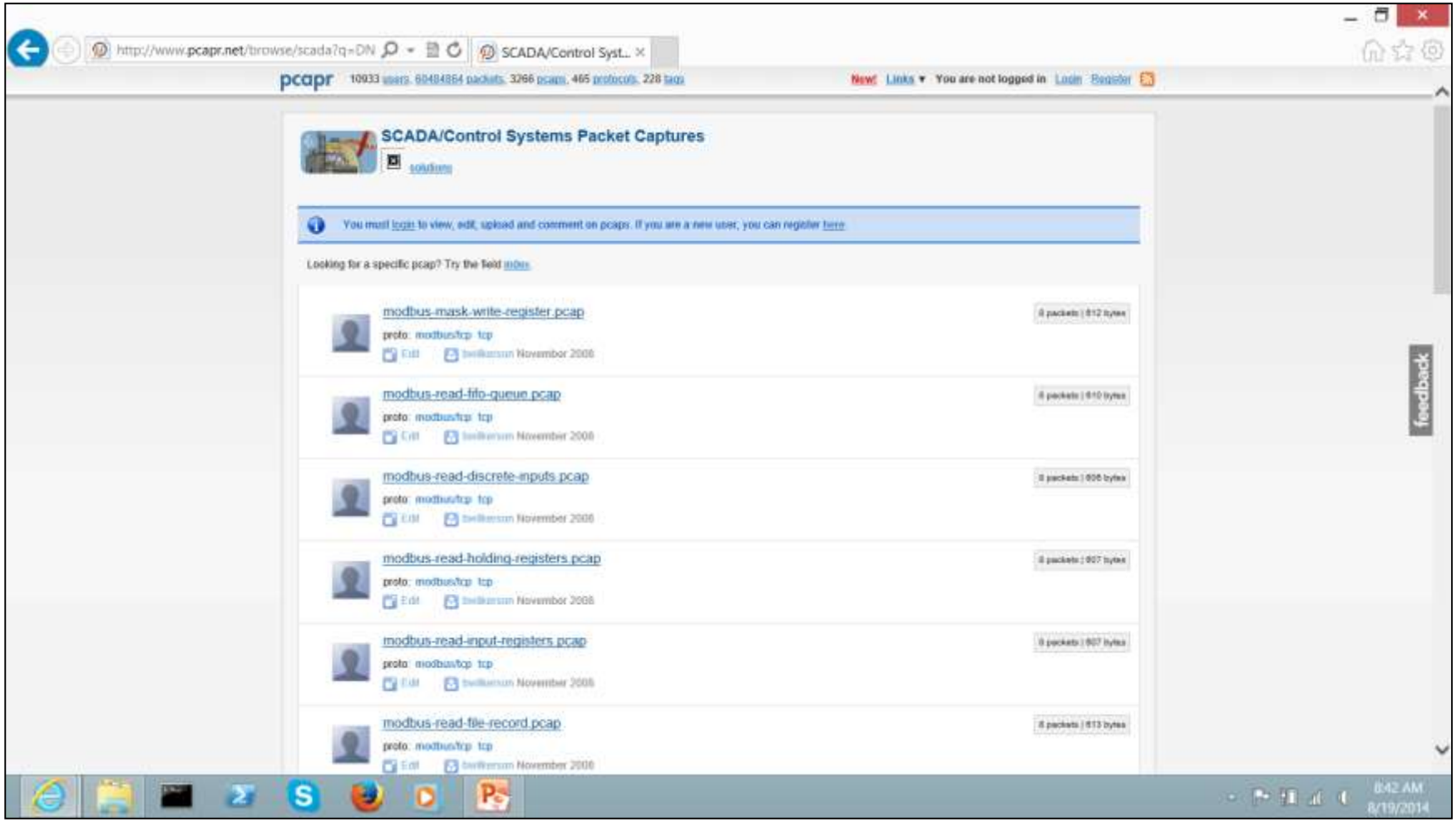


https://www.wireshark.org/about.html

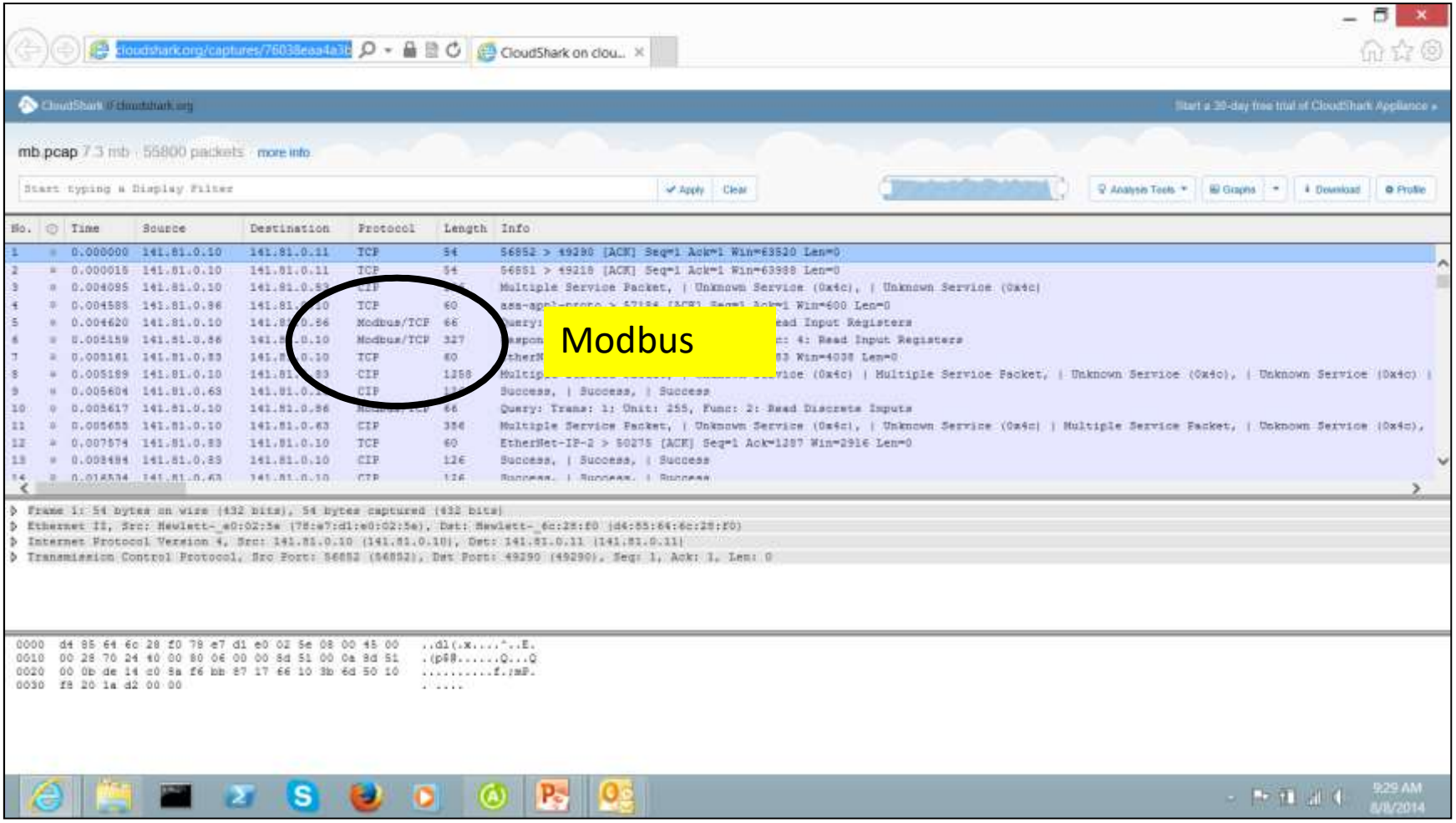
Wireshark Active Packet Capture



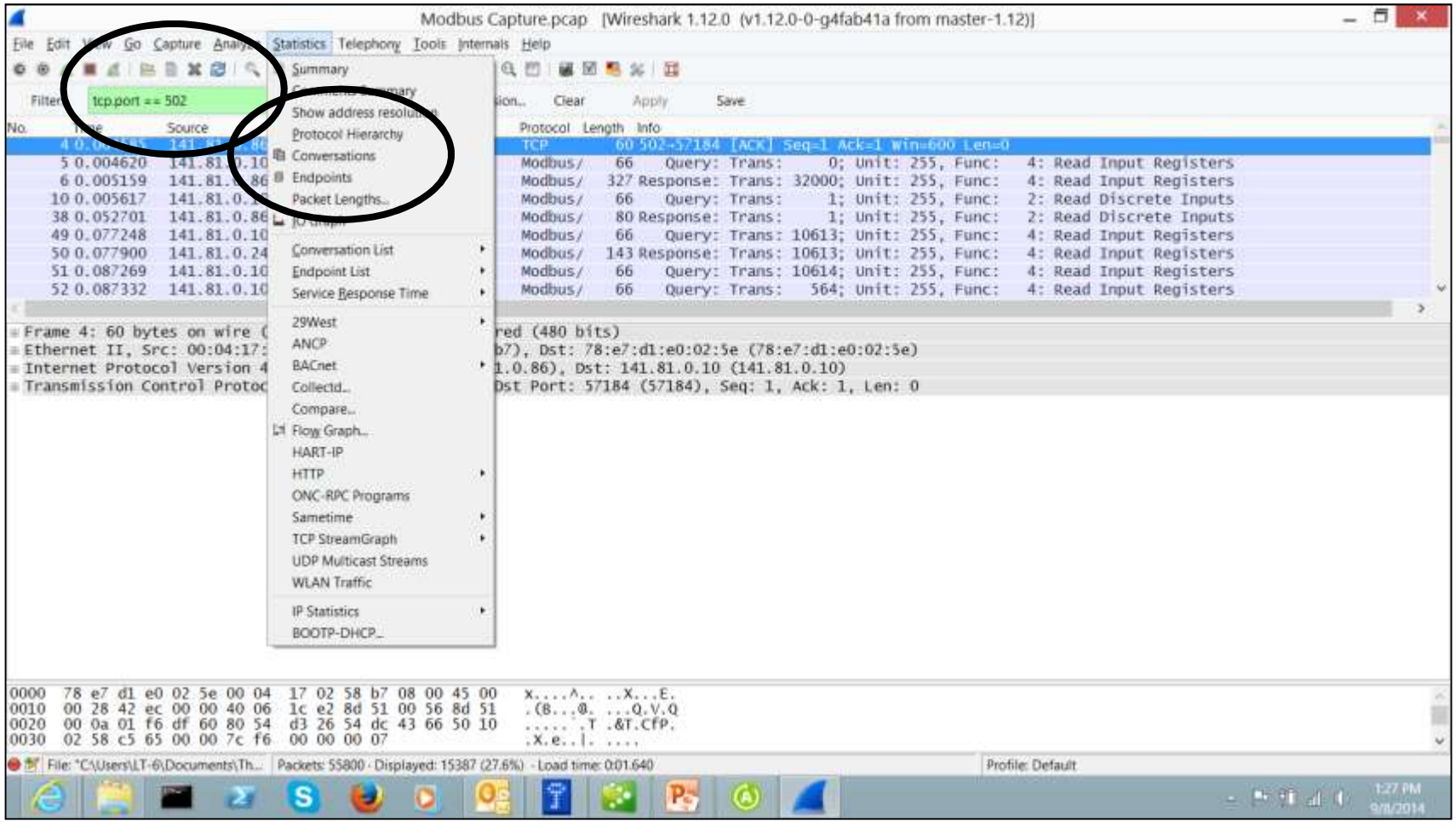
Modbus pcap files



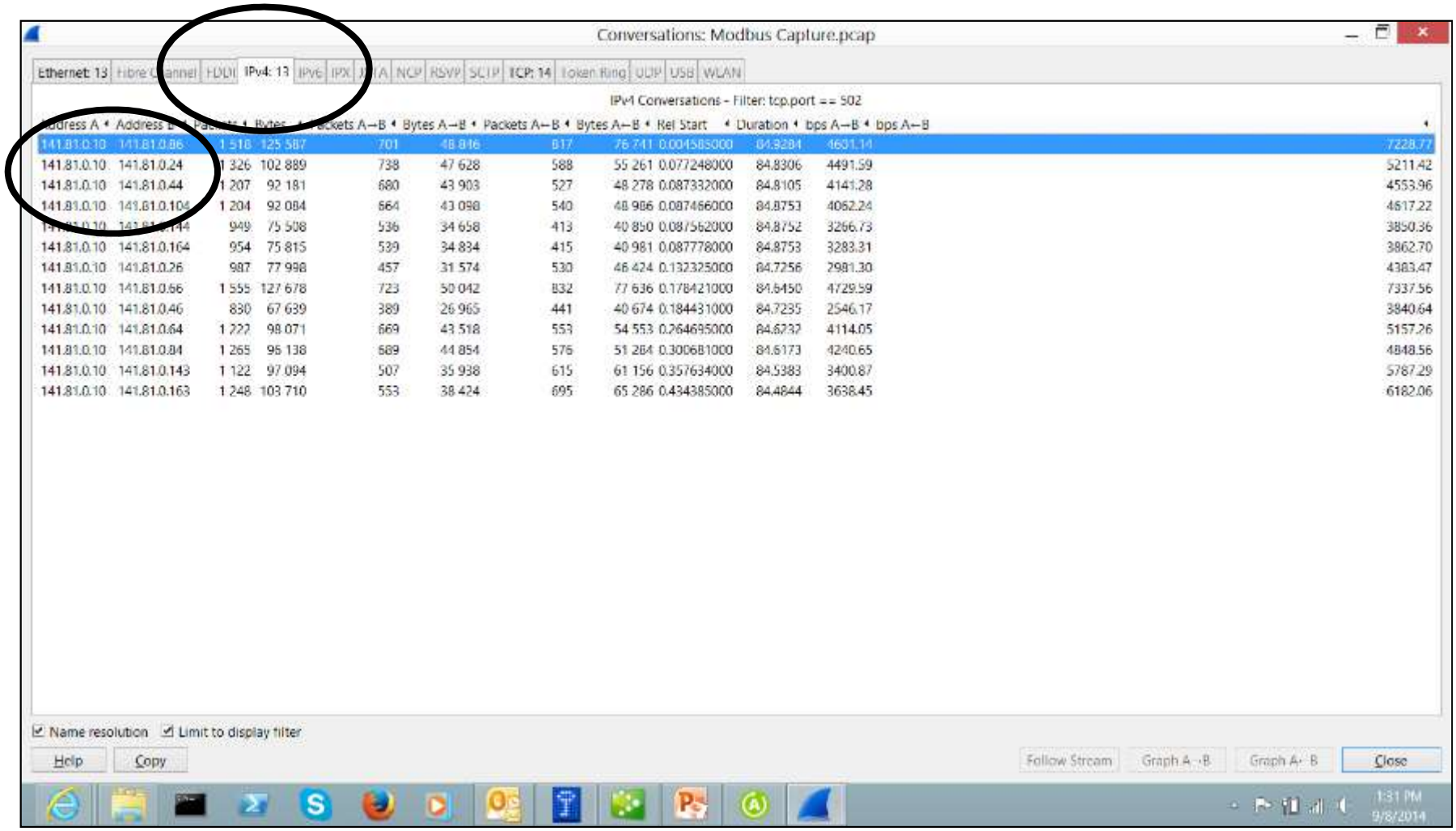
Wireshark Captures (pcap's)



Wireshark Captures (pcap's)



Wireshark Captures (pcap's)



Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B	bps A←B
141.81.0.10	141.81.0.86	1 518	125 587	701	48 846	817	76 741	0.004585000	84.9284	4631.14	7228.77
141.81.0.10	141.81.0.24	1 326	102 889	738	47 628	588	55 261	0.077248000	84.8306	4491.59	5211.42
141.81.0.10	141.81.0.44	1 207	92 181	680	43 903	527	48 278	0.087332000	84.8105	4141.28	4553.96
141.81.0.10	141.81.0.104	1 204	92 084	664	43 098	540	48 986	0.087466000	84.8753	4062.24	4617.22
141.81.0.10	141.81.0.144	949	75 508	536	34 658	413	40 850	0.087562000	84.8752	3266.73	3850.36
141.81.0.10	141.81.0.164	954	75 815	539	34 834	415	40 981	0.087778000	84.8753	3283.31	3862.70
141.81.0.10	141.81.0.26	987	77 998	457	31 574	530	46 424	0.132325000	84.7256	2981.30	4383.47
141.81.0.10	141.81.0.66	1 555	127 678	723	50 042	832	77 636	0.178421000	84.6450	4729.59	7337.56
141.81.0.10	141.81.0.46	830	67 639	389	26 965	441	40 674	0.184431000	84.7235	2546.17	3840.64
141.81.0.10	141.81.0.64	1 222	98 071	669	43 518	553	54 553	0.264695000	84.6232	4114.05	5157.26
141.81.0.10	141.81.0.84	1 265	96 138	689	44 854	576	51 284	0.300681000	84.6173	4240.65	4848.56
141.81.0.10	141.81.0.143	1 122	97 094	507	35 938	615	61 156	0.357634000	84.5383	3400.87	5787.29
141.81.0.10	141.81.0.163	1 248	103 710	553	38 424	695	65 286	0.434385000	84.4844	3638.45	6182.06

BACNet pcap files

http://wiki.wireshark.org/Protocols/bacnet?

WIRESHARK

Protocols/bacnet

FrontPage | RecentChanges | FindPage | HelpContents | Protocols/bacnet

Redirected from page "BACnet"

Clear message

Immutable Page | Info | Attachments | More Actions:

BACnet

BACnet, the ASHRAE building automation and control networking protocol, has been designed specifically to meet the communication needs of building automation and control systems for applications such as heating, ventilating, and air-conditioning control, lighting control, access control, and fire detection systems. The BACnet protocol provides mechanisms by which computerized equipment of arbitrary function may exchange information, regardless of the particular building service it performs. As a result, the BACnet protocol may be used by head-end computers, general-purpose direct digital controllers, and application specific or unitary controllers with equal effect.

The BACnet protocol specifies transport over a number of datalink layers including ARCNET, MS/TP (RS-485), PTP (RS-232), LonTalk, and Ethernet. BACnet also specifies communication over UDP/IP which is known as BACnet/IP. Other datalink layers are proposed.

History

A brief BACnet history can be found at http://en.wikipedia.org/wiki/BACnet

Protocol dependencies

- UDP: BACnet/IP uses UDP as its transport protocol. The default UDP port for BACnet traffic is 47808 (0xBAC0), but depending on the project specification other ports are also possible.
- LLC: BACnet Ethernet uses LLC atop Ethernet as its transport protocol, and BACnet ARCNET uses LLC atop ARCNET as its transport protocol. For BACnet traffic, DSAP is 0x82, SSAP is 0x82.
- MSTP: BACnet MS/TP uses either MSTP natively, or from the Cimetrics U+4 converter, LLC SNAP as its transport protocol.

Example traffic

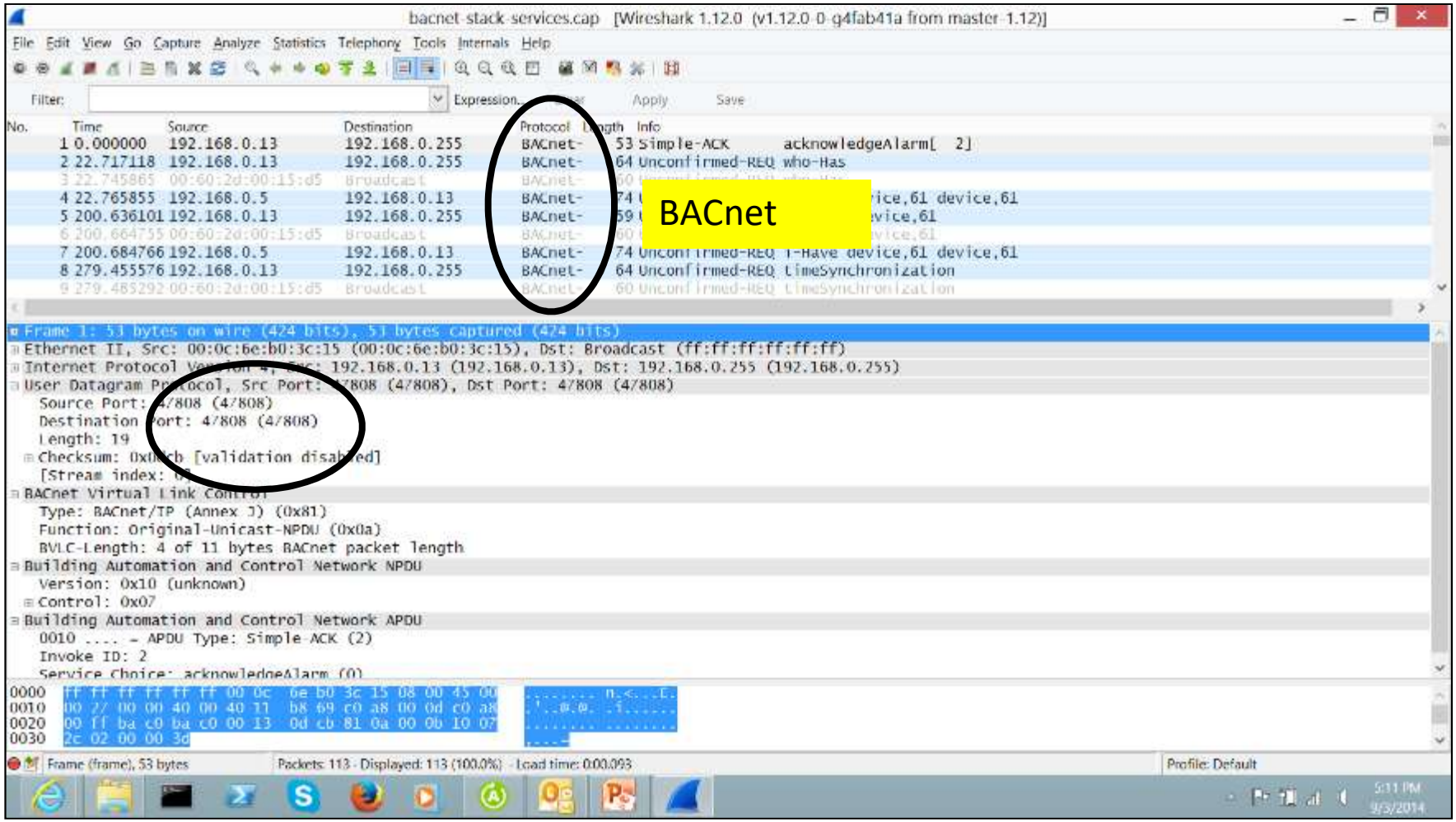
bacnet-stack-services.cap - Wireshark

File Edit View Go Capture Analyze Statistics Tools Help

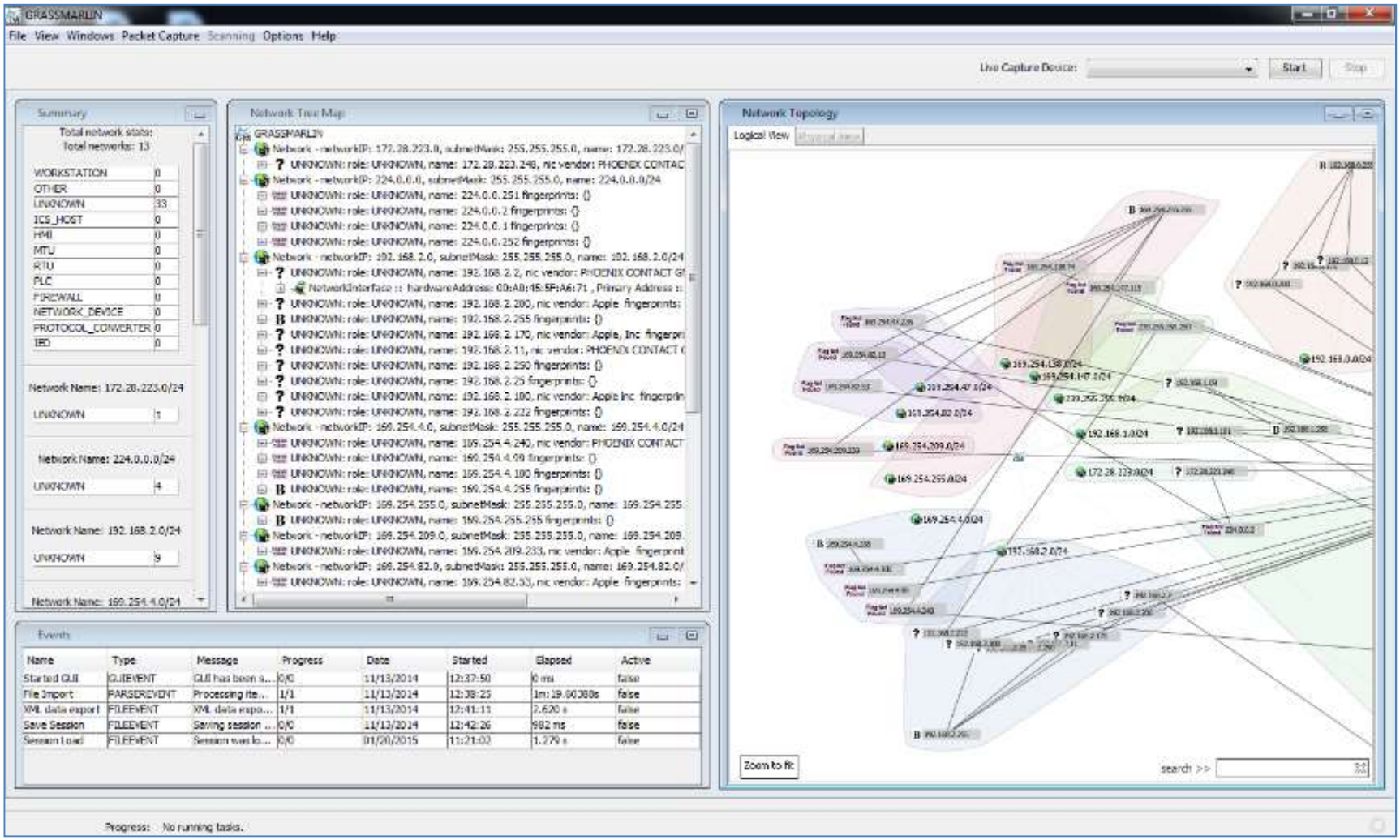
Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info

Wireshark BACnet pcap



GrassMarlin Passive Network Collector



CyberX

CYBERX | Risk Assessment

Security Score 38%

36 Vulnerable Devices

5 Devices Needing Improvement

24 Secure Devices

- 1 Unauthorized asset
- 14 Internet connections detected
- 7 connections to ICS networks detected
- Firewall rules: 0 out of 0 firewall rules are vulnerable
- No backup servers detected
- 7 Devices accessible remotely
- No engineering stations detected
- 1 Scanning device detected
- No AV software detected
- 3 top attack vectors generated (highest risk)

CYBERX | Risk Assessment

Attack Vector #2

(1) Unauthorized Internet Connection
Technician_PC is exposed to external threats due to unauthorized internet connectivity

(2) Known CVE
Device OSISoft_PI_HIS has a known CVE vulnerability CVE-2014-1776 that can be exploited.
Description: Use-after-free vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to the CMarkup::IsConnectedToPrimaryMarkup function, as exploited in the wild in April 2014. NOTE: this issue originally emphasized VGX.DLL, but Microsoft clarified that "VGX.DLL does not contain the vulnerable code leveraged in this exploit. Disabling VGX.DLL is an exploit-specific workaround that provides an immediate, effective workaround to help block known attacks."

(3) Outdated OS
Device HMI_Line10 is running Windows XP operating system, which is no longer supported and contains multiple known vulnerabilities with no security updates or hotfixes

(4) Outdated OS
Device EWS_Line10 is running Windows Server 2003 operating system, which is no longer supported and contains multiple known vulnerabilities with no security updates or hotfixes

This server can be used by the attacker to persist malware in the network

(5) Network Connection
Direct connection between devices

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

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]

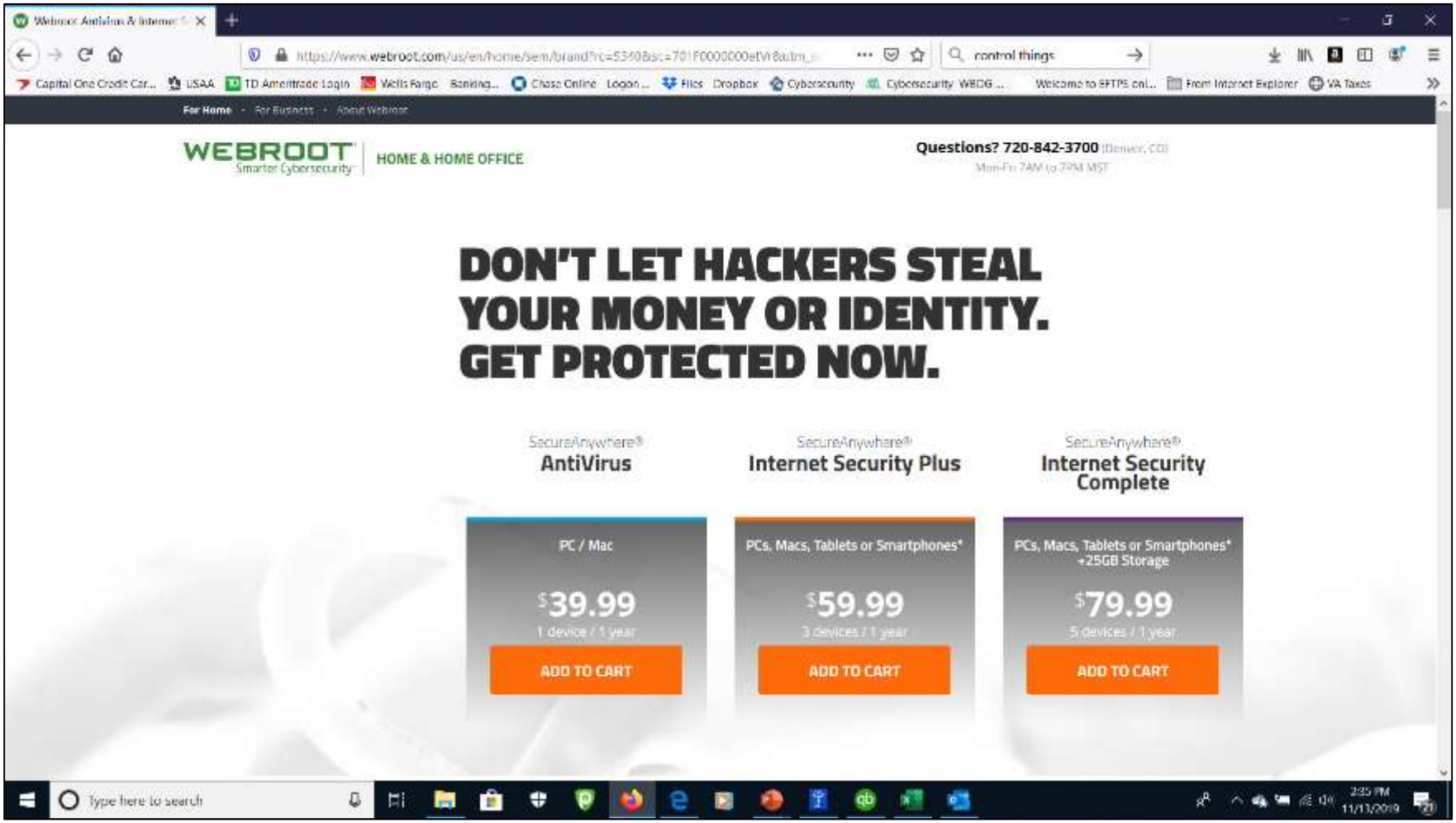
Board: Acer Zoro_SL V1.10
Serial Number: NBG3711D016130A55E7600
Bus Clock: 100 megahertz
UEFI: Insyde Corp. V1.10 11/27/2015

Search the web and Windows

11:14 AM
7/11/2016

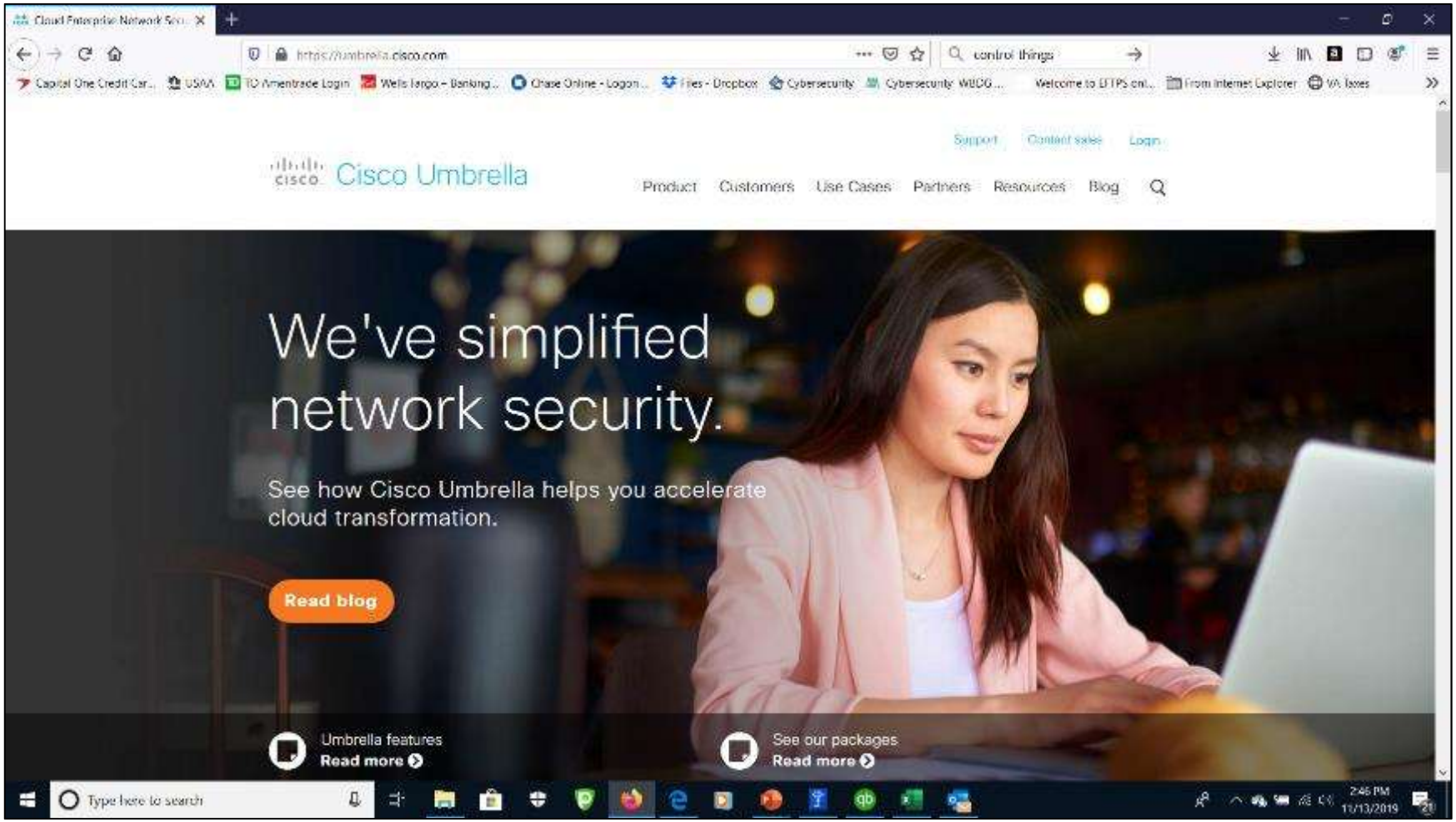
http://www.belarc.com/

Webroot



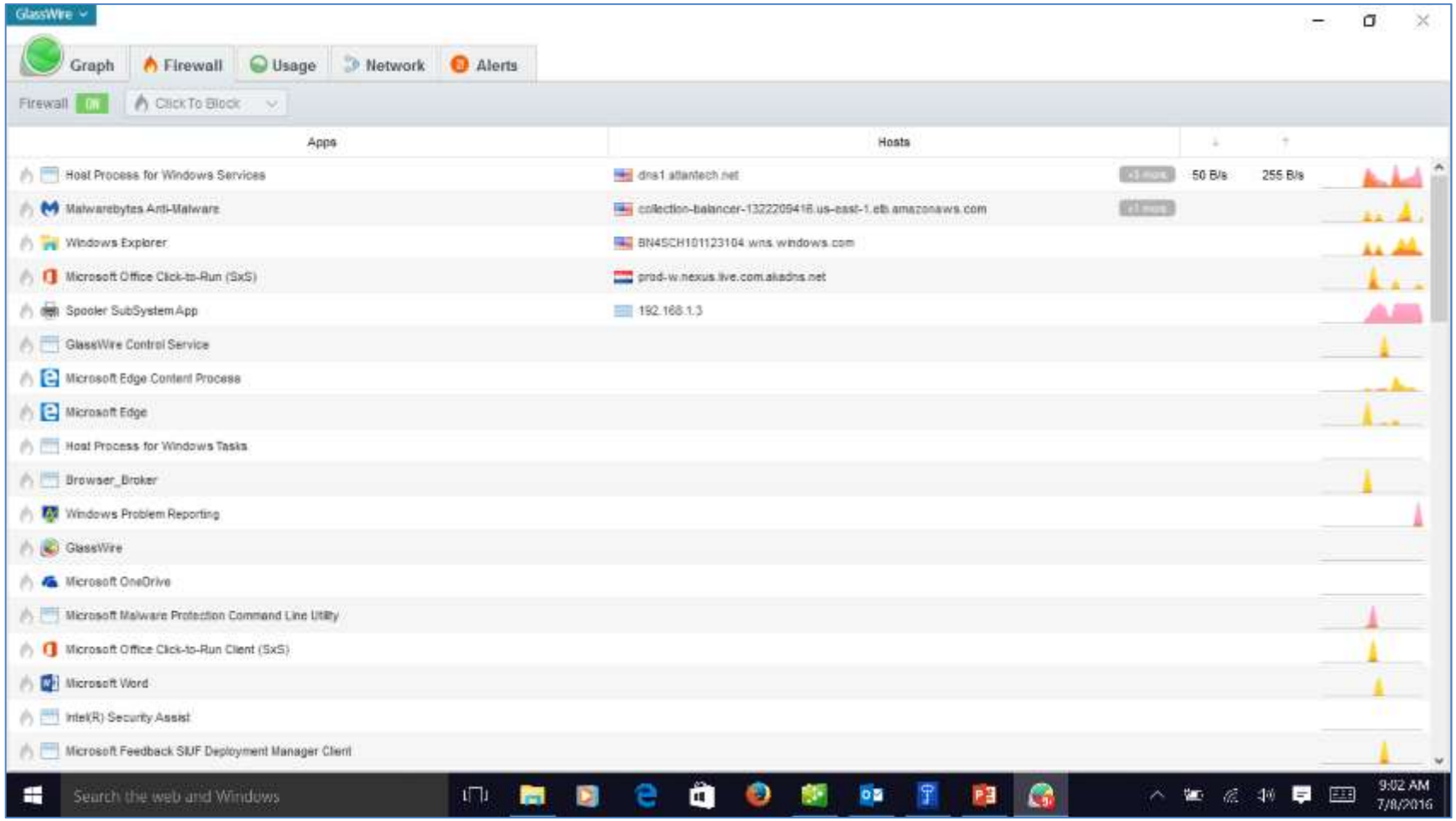
https://www.webroot.com/us/en/home/sem/brand?rc=5340&sc=701F0000000etVr&utm_source=bing&utm_medium=cpc&utm_campaign=btc-bing-branded&msclkid=8309d7a4d1f01aa92be98a688b110e22

Cisco Umbrella

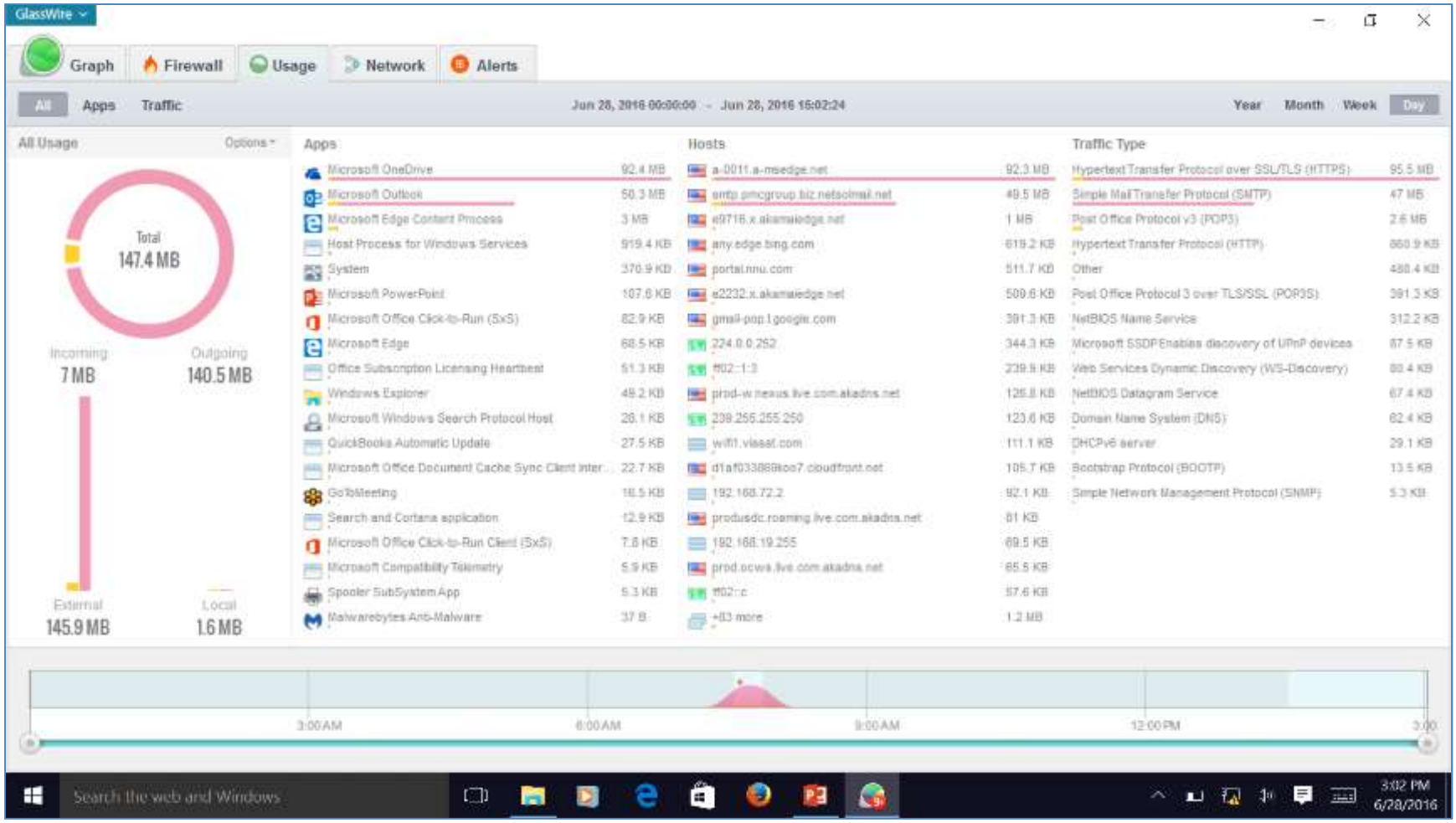


https://umbrella.cisco.com/

Glasswire Firewall

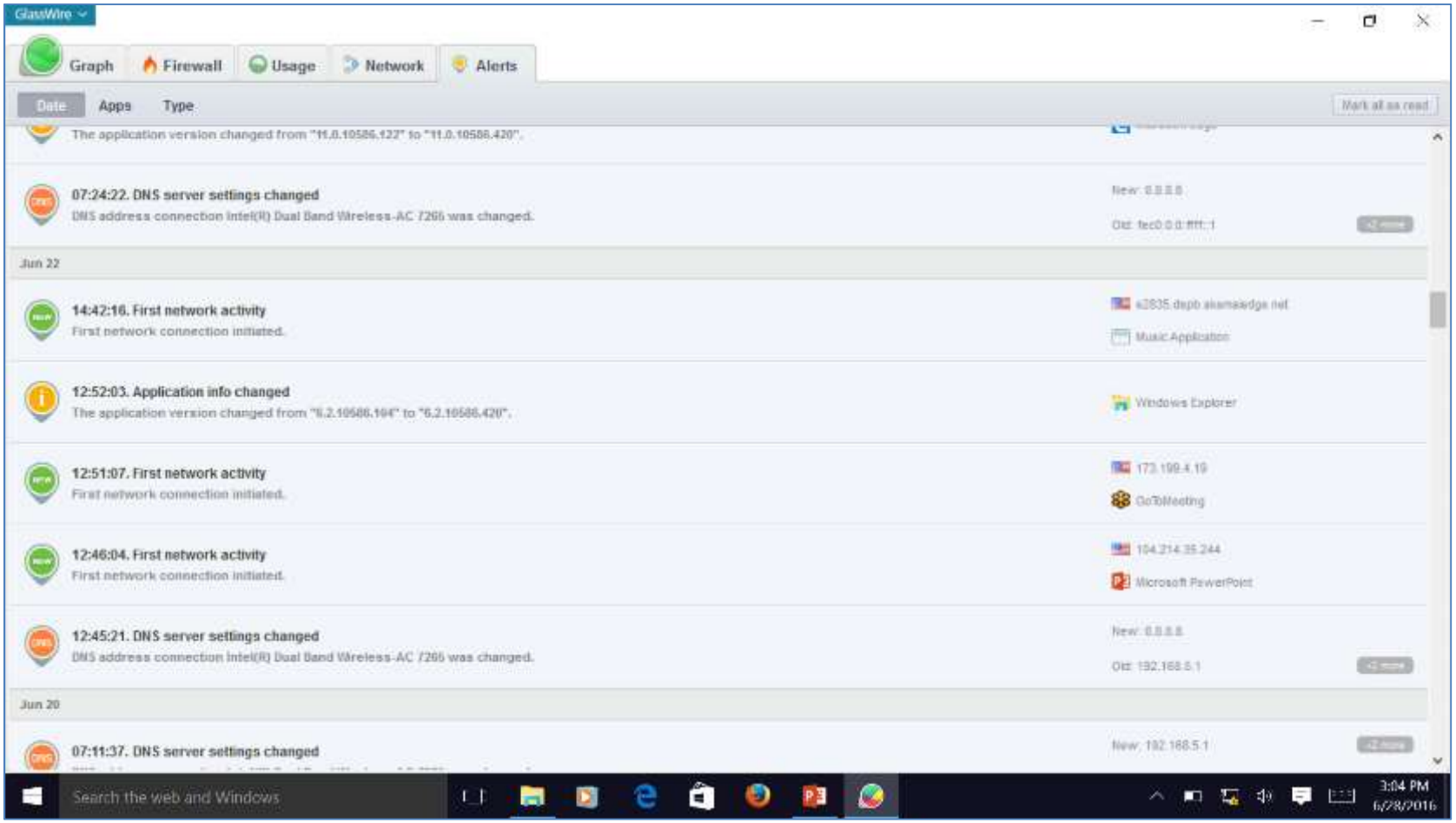


Glasswire Usage



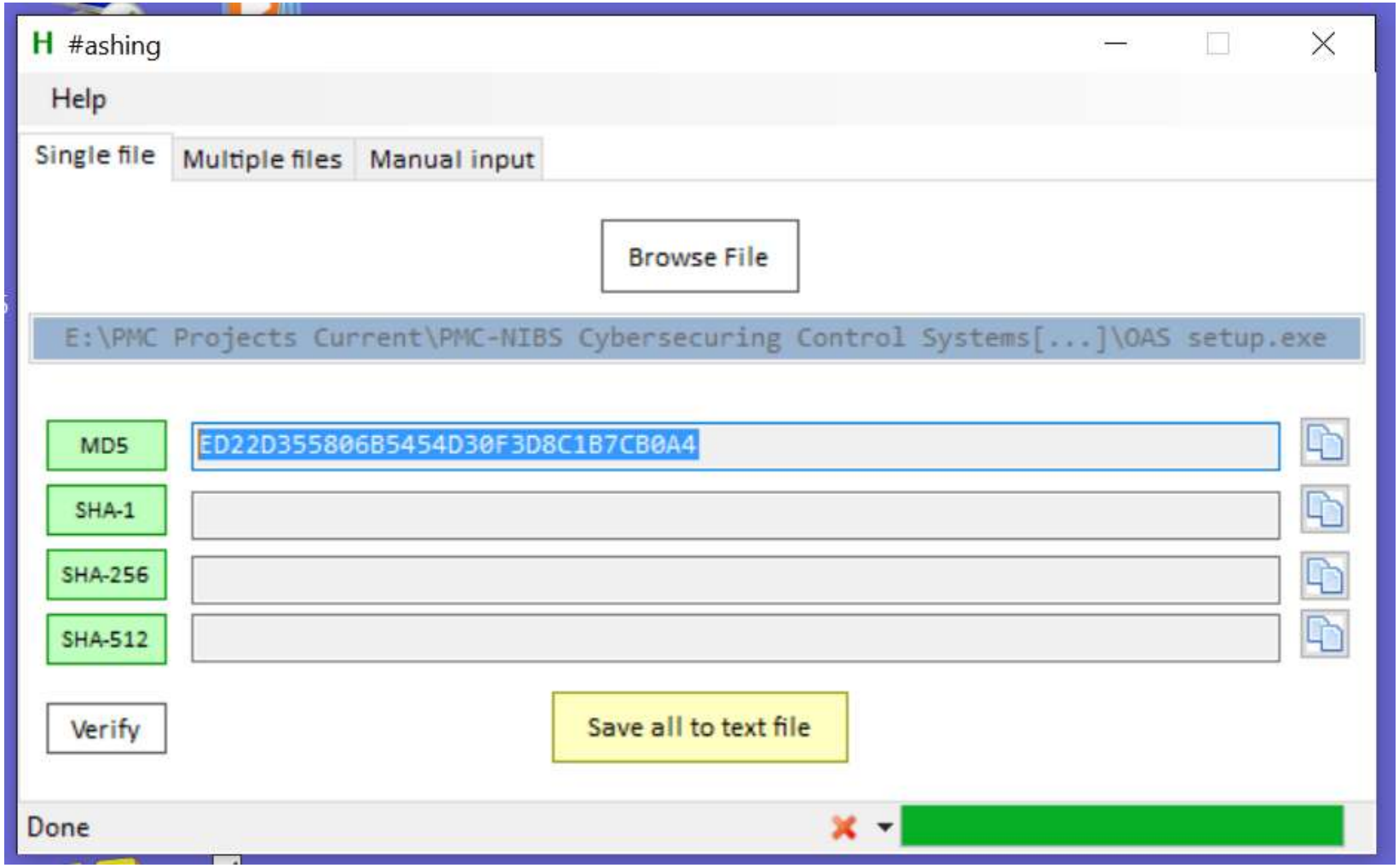
Apps, Hosts and Traffic Type

Glasswire Alerts

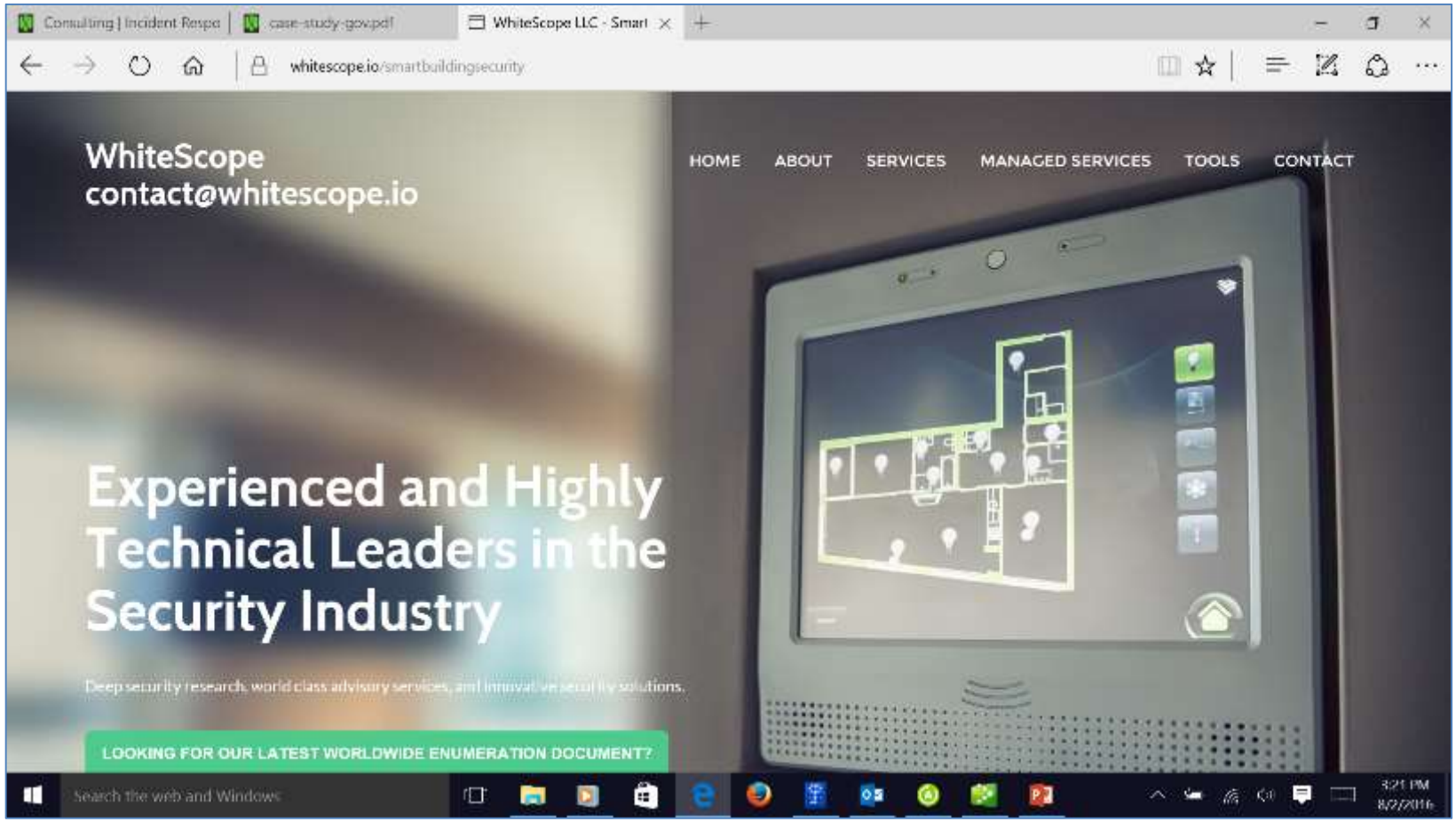


DNS, Executable, Version

Software / Firmware Inventory Hash



WhiteScope BCS Homepage



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

WhiteScope BCS 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

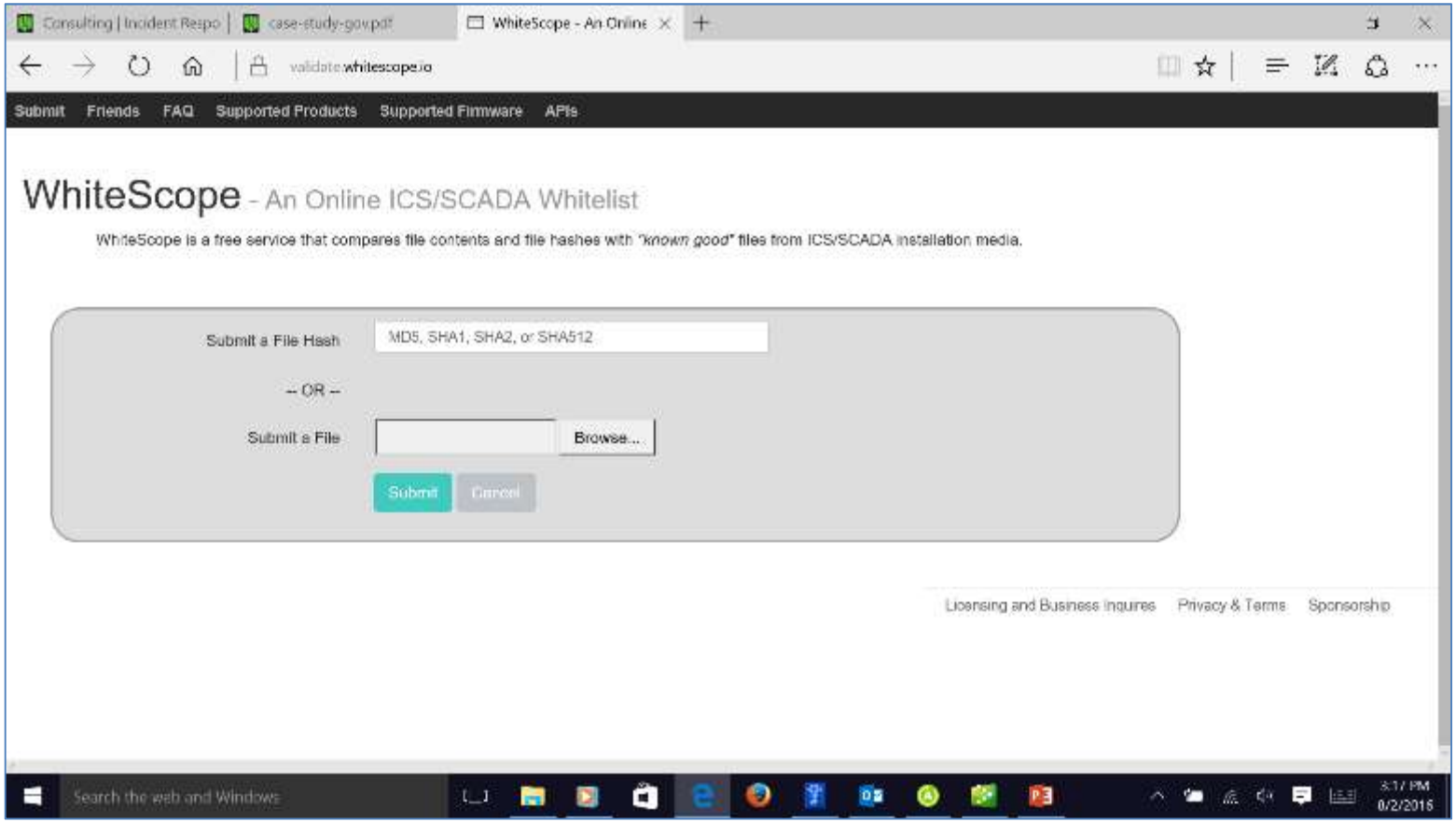
Summary

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

Details

Severity	Name
Critical	User guest Has No Password

WhiteScope Whitelist Products



https://validate.whitescope.io/

WhiteScope Whitelist Firmware

Consulting | Incident Respo | case-study-gov.pdf | WhiteScope - An Online

validate.whitescope.io/static/firmware.html

Submit Friends FAQ Supported Products Supported Firmware APIs

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.

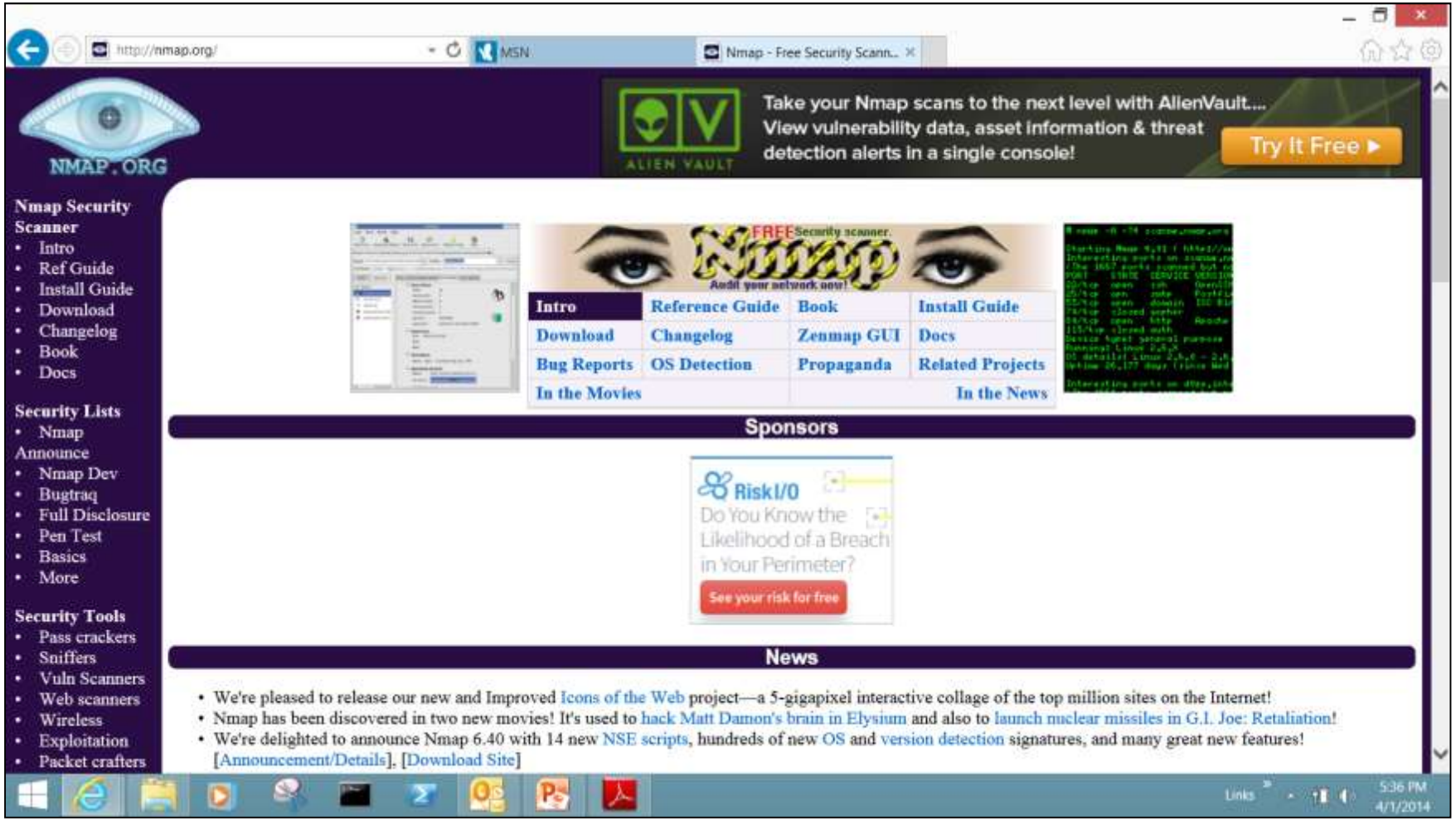
The following firmware is currently loaded in the WhiteScope Database:

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

Search the web and Windows

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

Nmap – Security Scanner



http://nmap.org/