



# The PMC Group LLC

*Engineering a better tomorrow today*

## Cybersecuring DoD Facility-Related Control Systems

[www.pmcgroup.biz](http://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

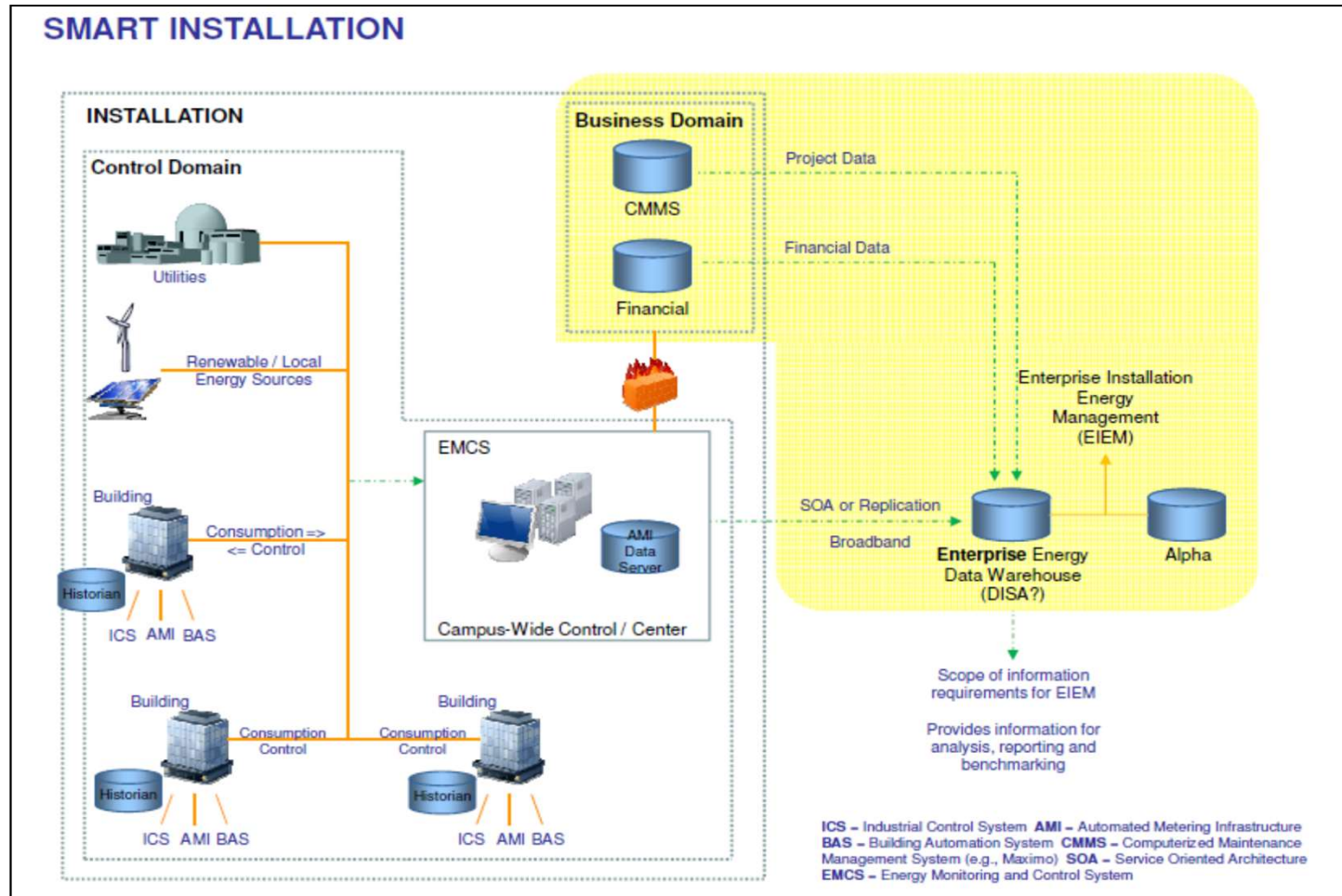


## **Unit 1**

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

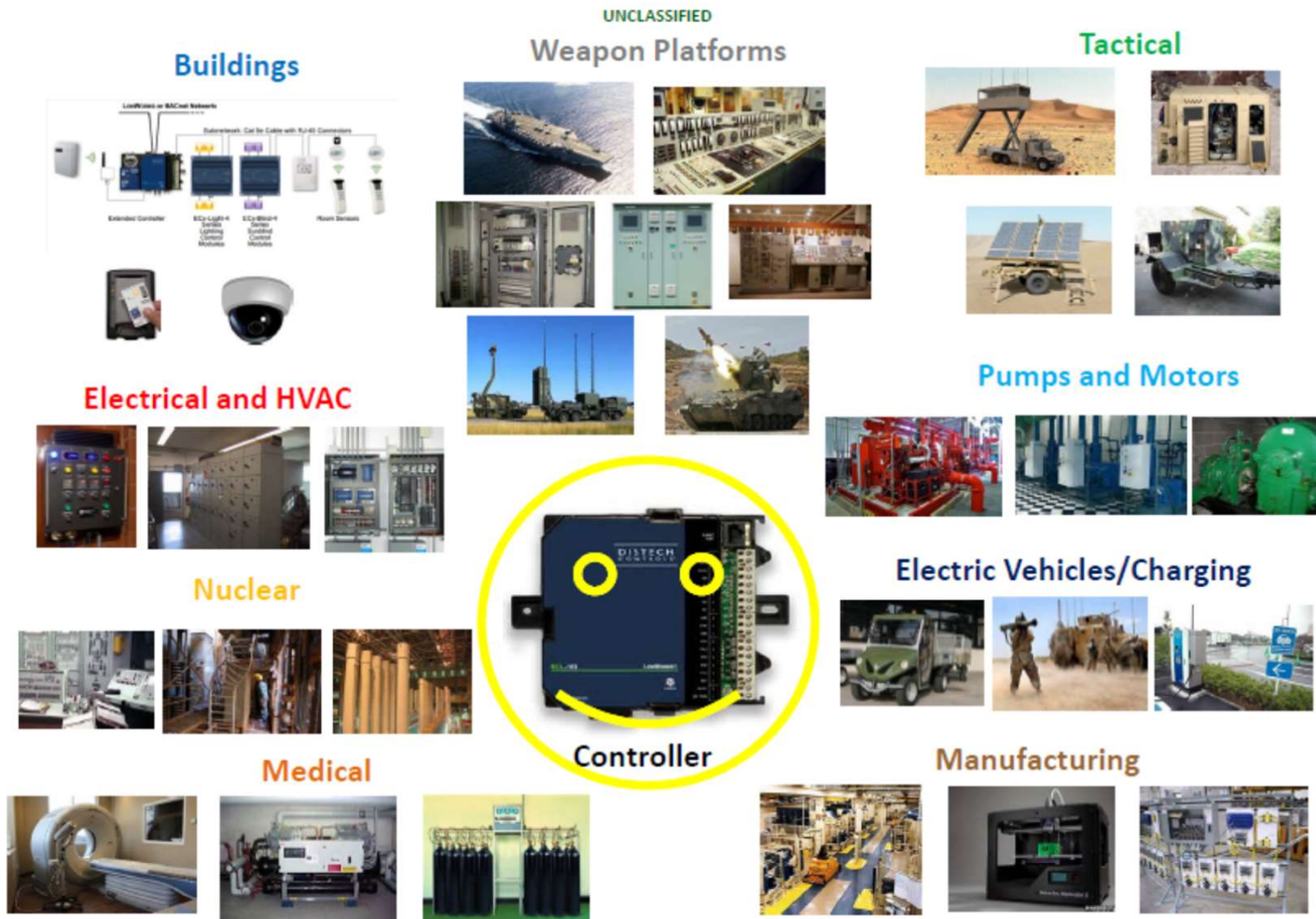


# In the Beginning – Smart Installations



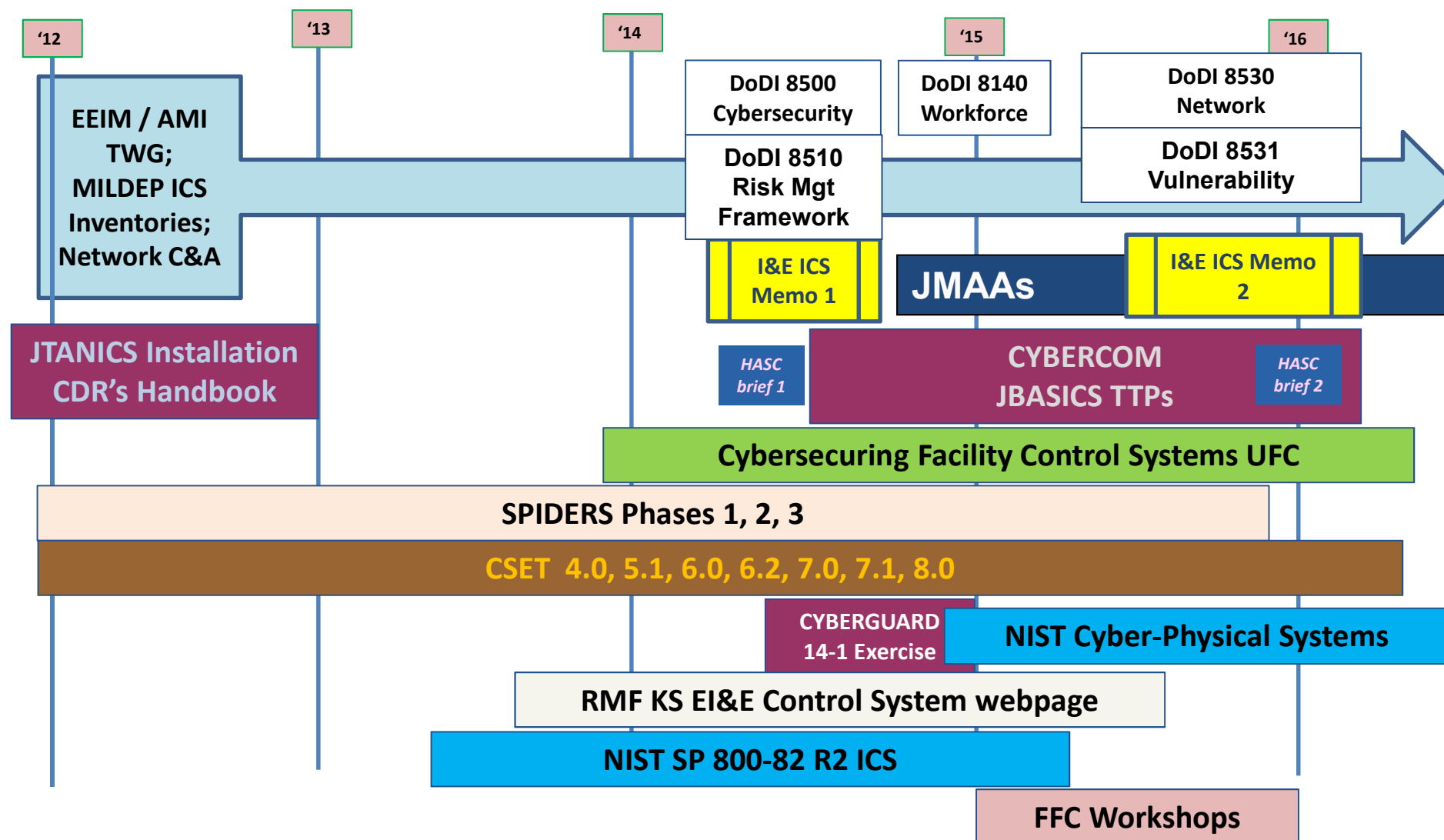
A great idea rudely interrupted by reality... CIO AMI ATO denial,... Stuxnet attack on Iranian Centrifuges, Flame, Duqu, Shamoon....

# OT IP Based Controllers Are in Everything



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

# Broader DoD Cybersecurity Efforts 2012-2017



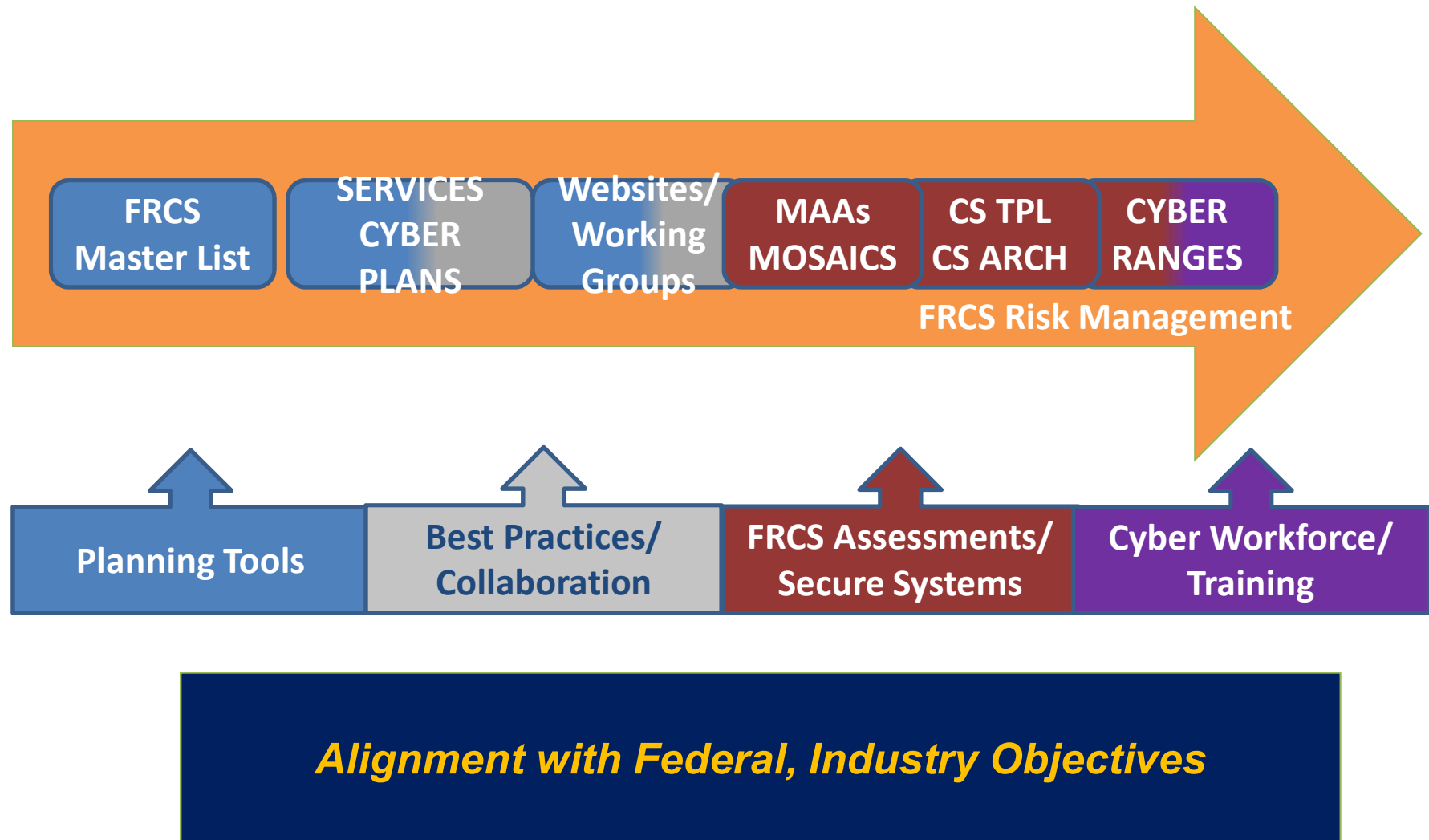
# NDAA 2017

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.

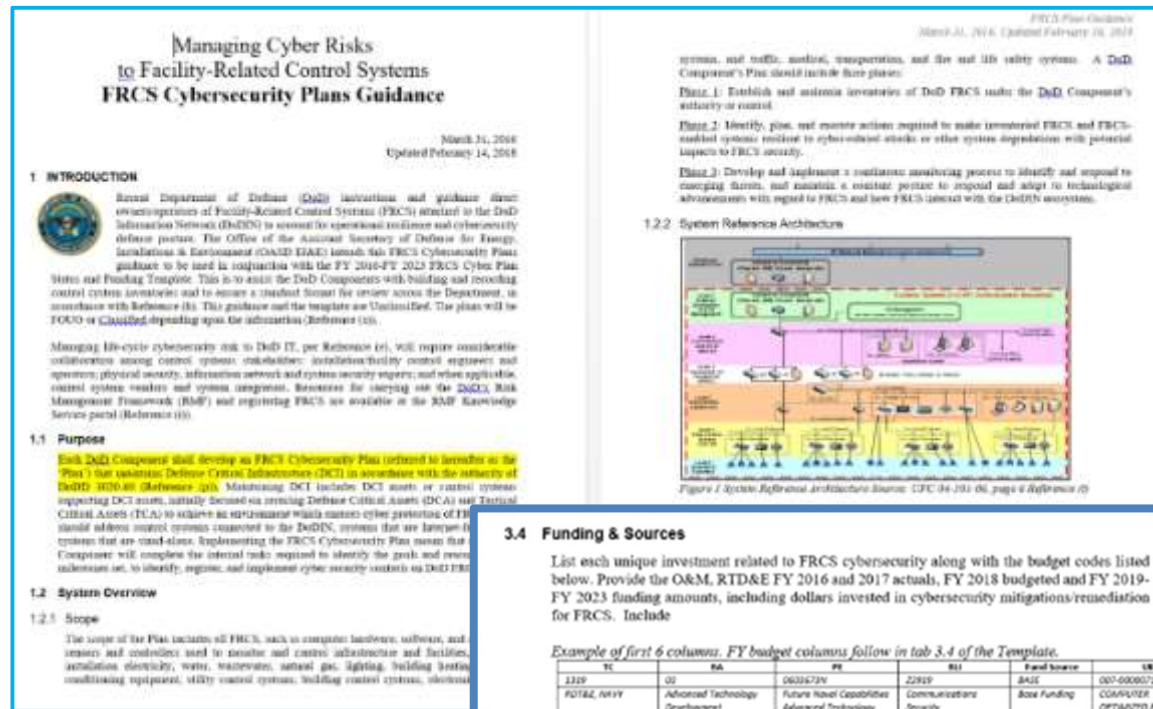
# ODASD(E) Cybersecurity Initiatives 2019





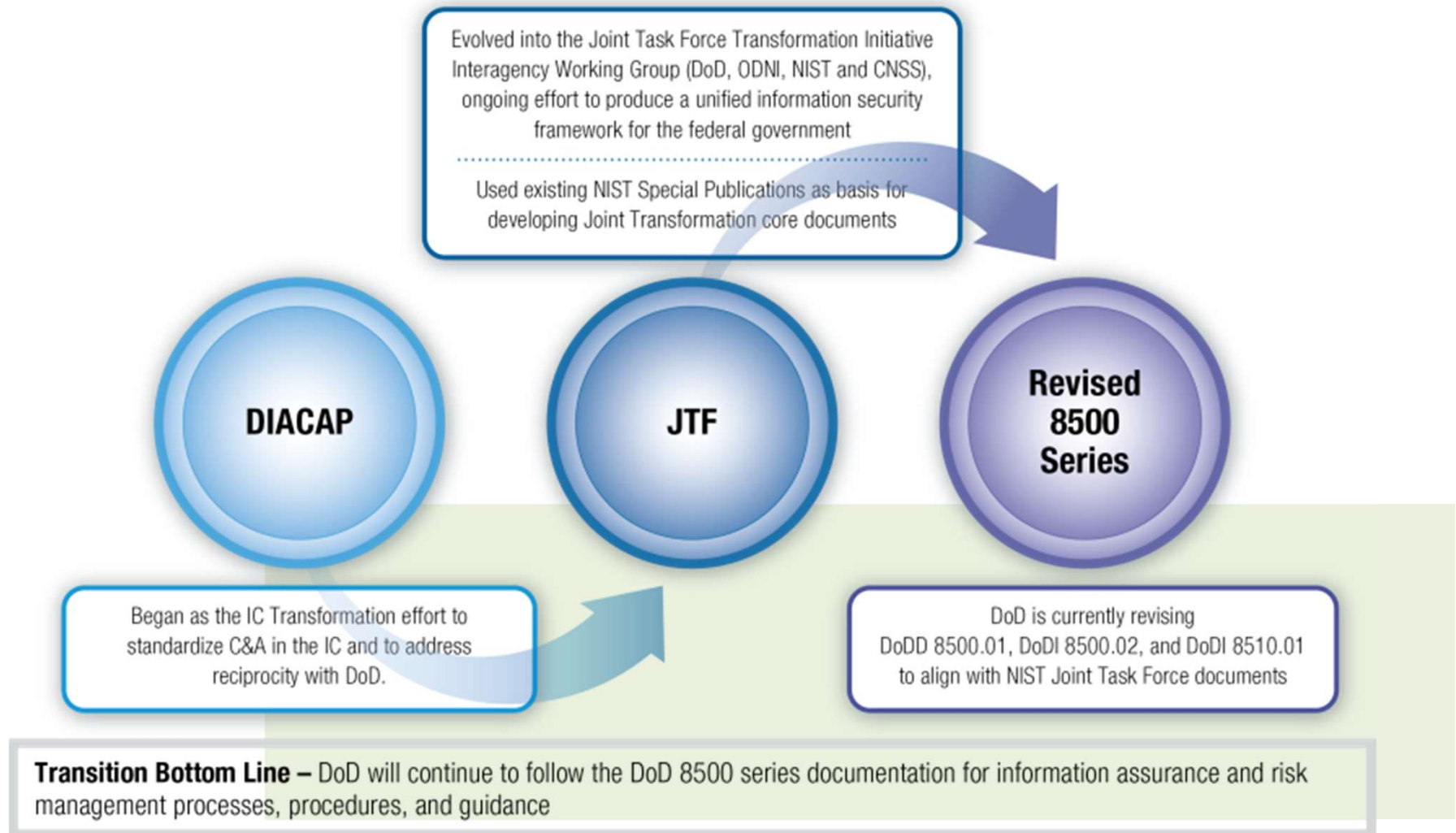
# DoD FRCS Cyber Plans 2016, 2018

## DoD FRCS Cyber Plans 2016, 18...



**Is Your FRCS Cyber Plan Adequately Resourced?**

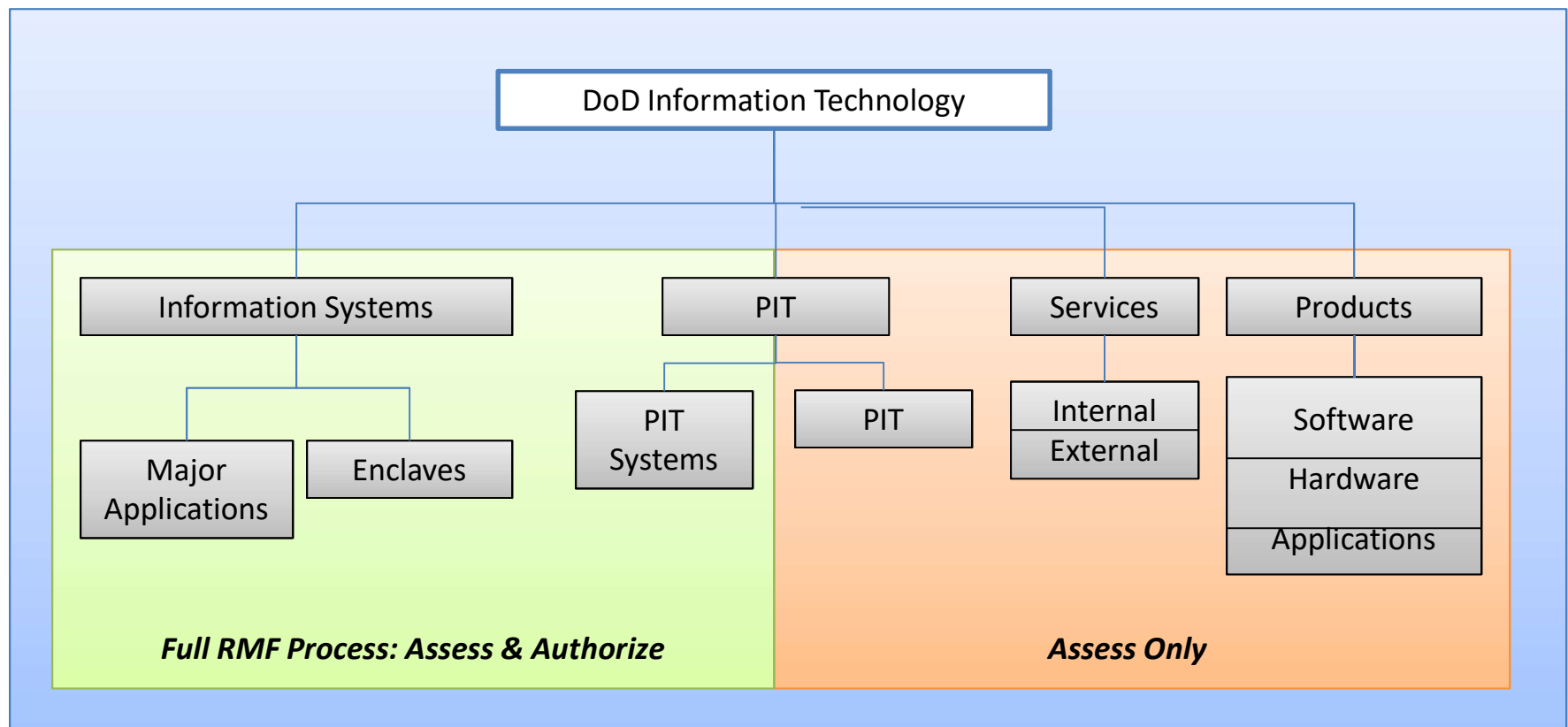
# DoDI 8500.01 and 8510.01 Update



# 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).

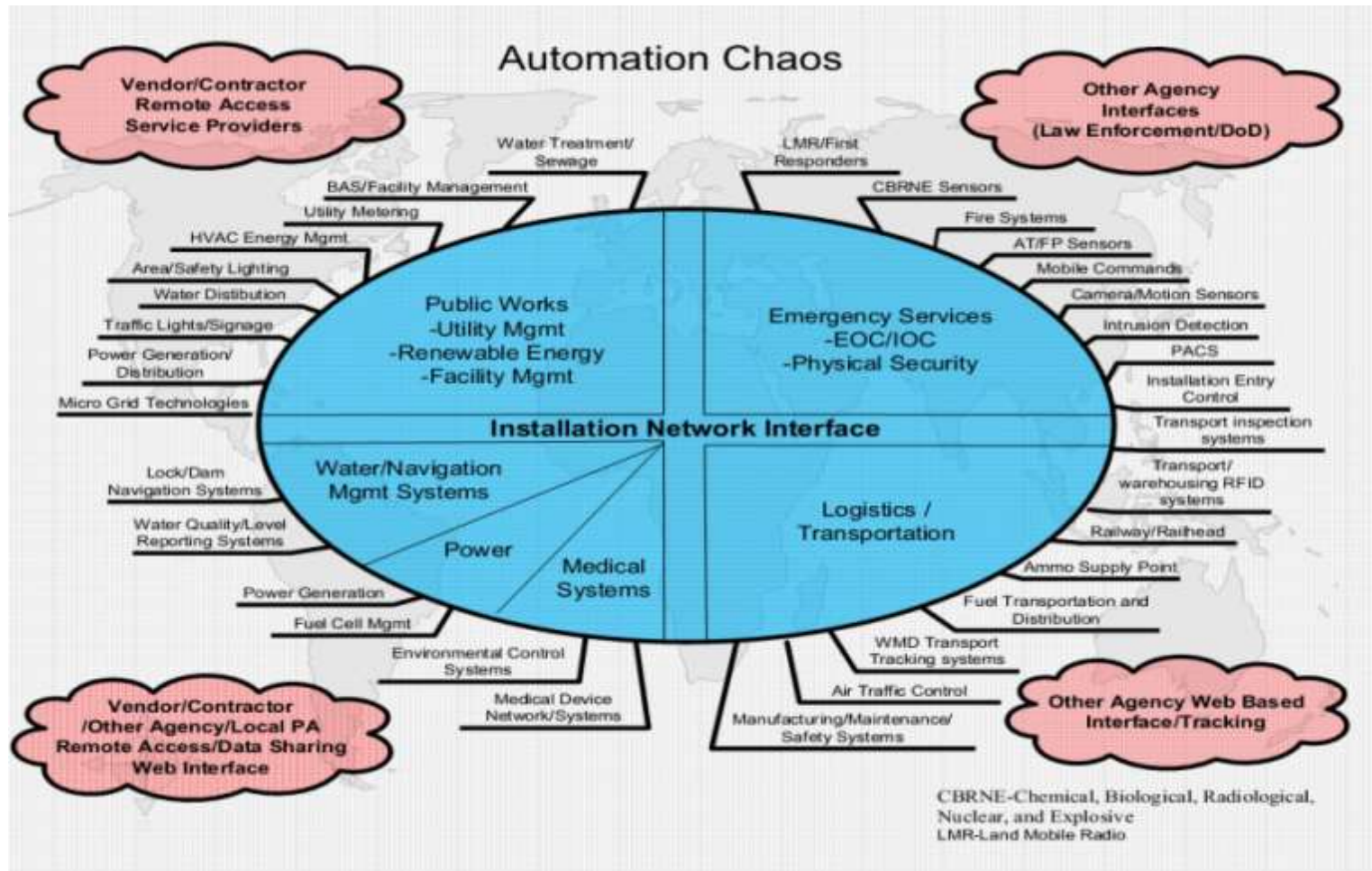


# 8500 PIT Systems

## (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

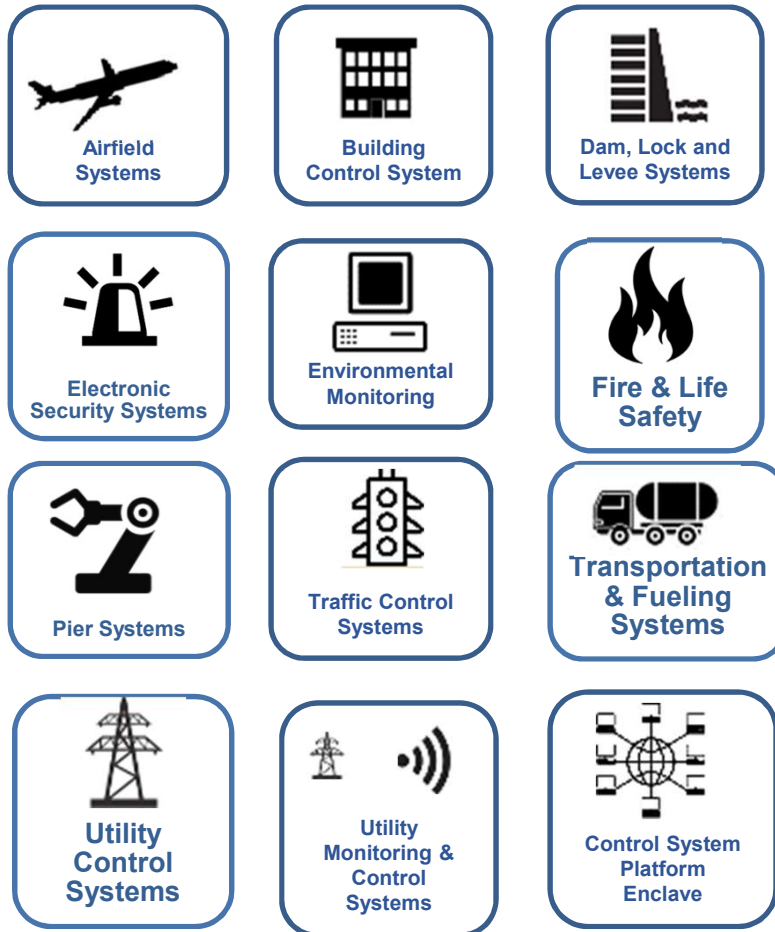


Courtesy of Fred Abbitt USACE

***DoD alone has more than 2.5 million unique FRCS systems***

# DoD Facility-Related Control Systems (FRCS)

## Categories



## 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...*

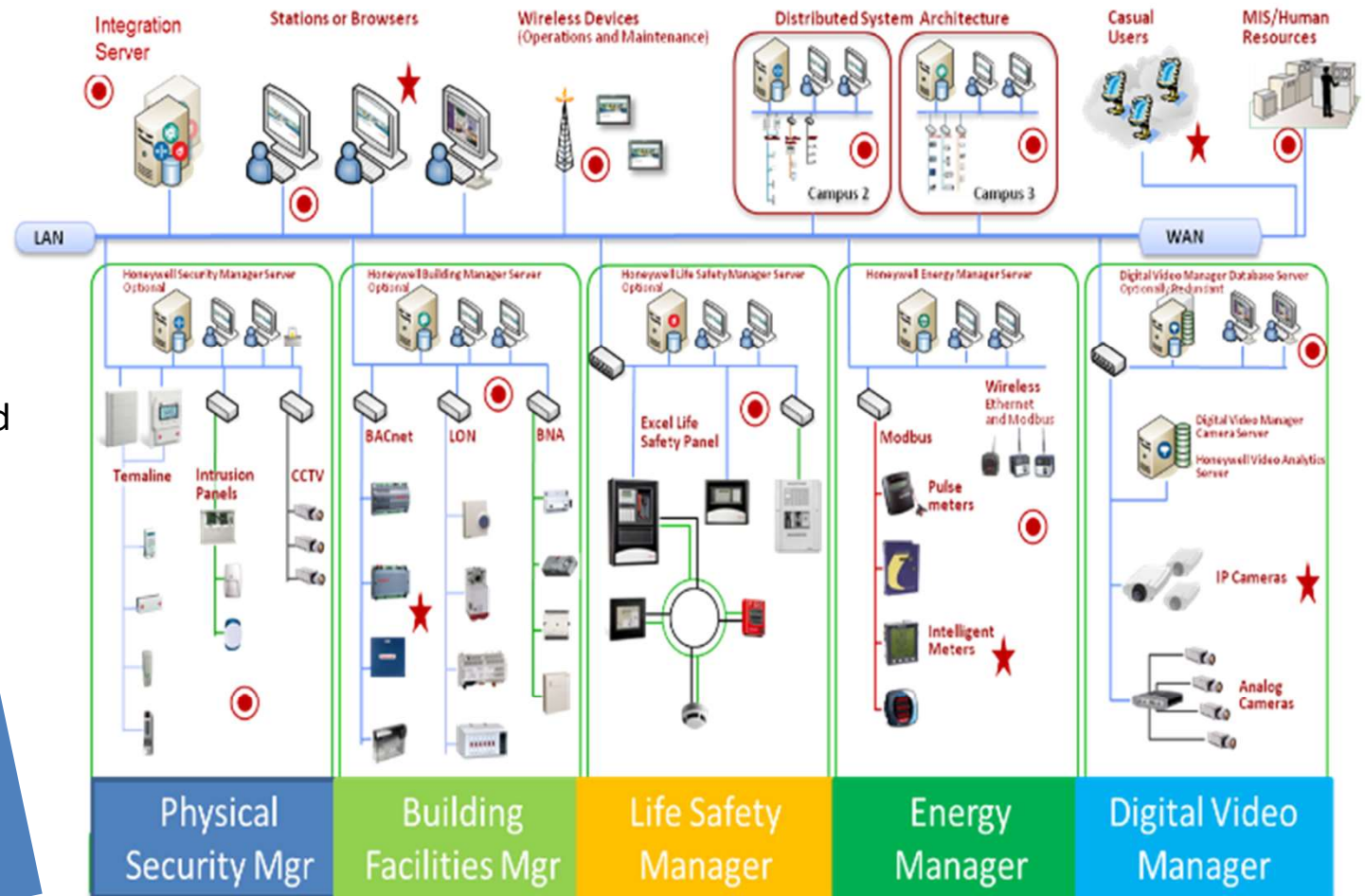
**DoD Control Systems are just as vulnerable as industry, how do we protect them?**

# DoD Building FRCS

## DoD Real Property Portfolio

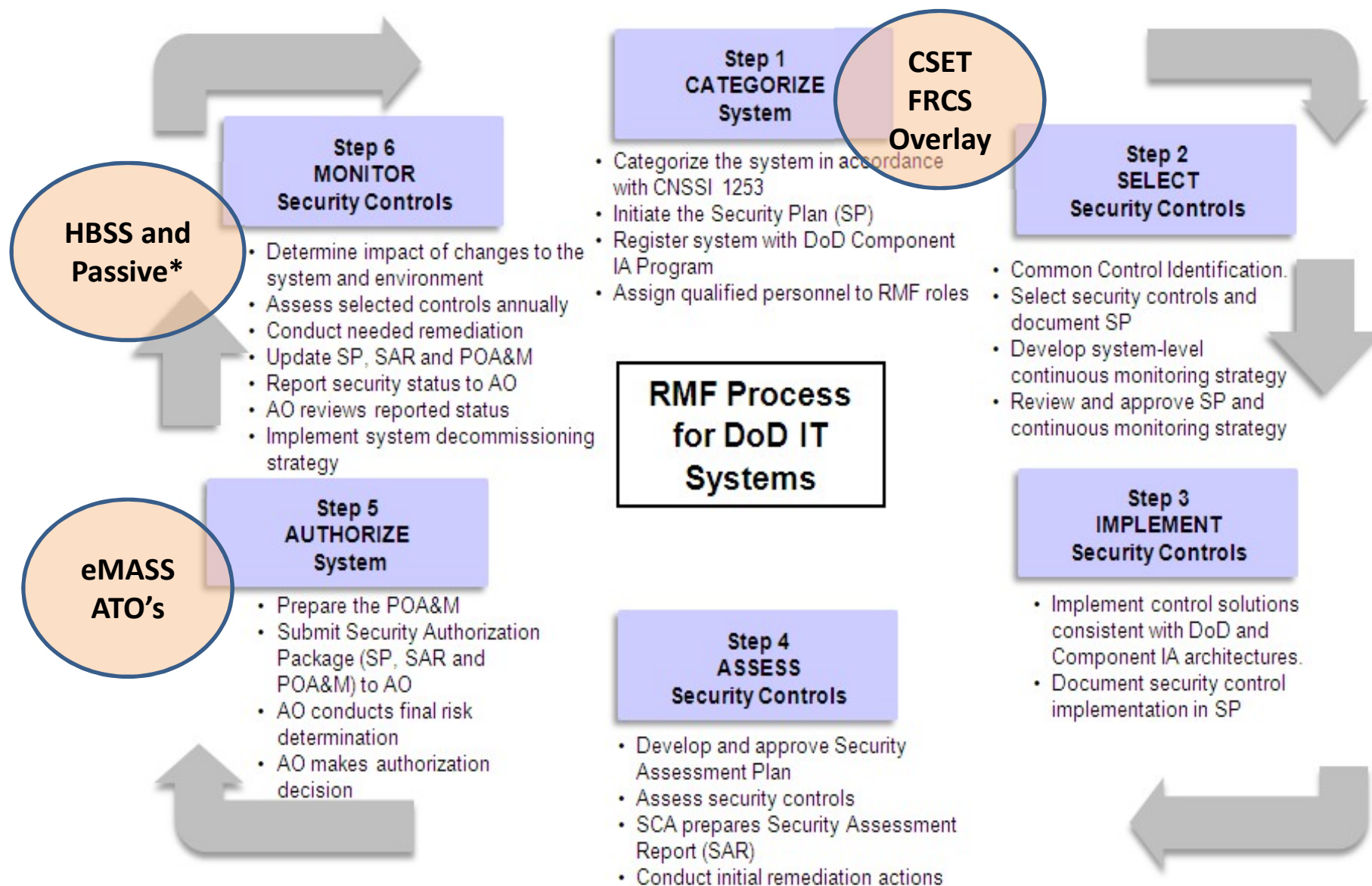
- 48 countries
- 523 installations
- 4,855 Sites
- 562,600 buildings and structures
- 24.7 M acres
- \$847 B value

What's in  
Your  
Building?





# FRCS Overlay & RMF Implementation

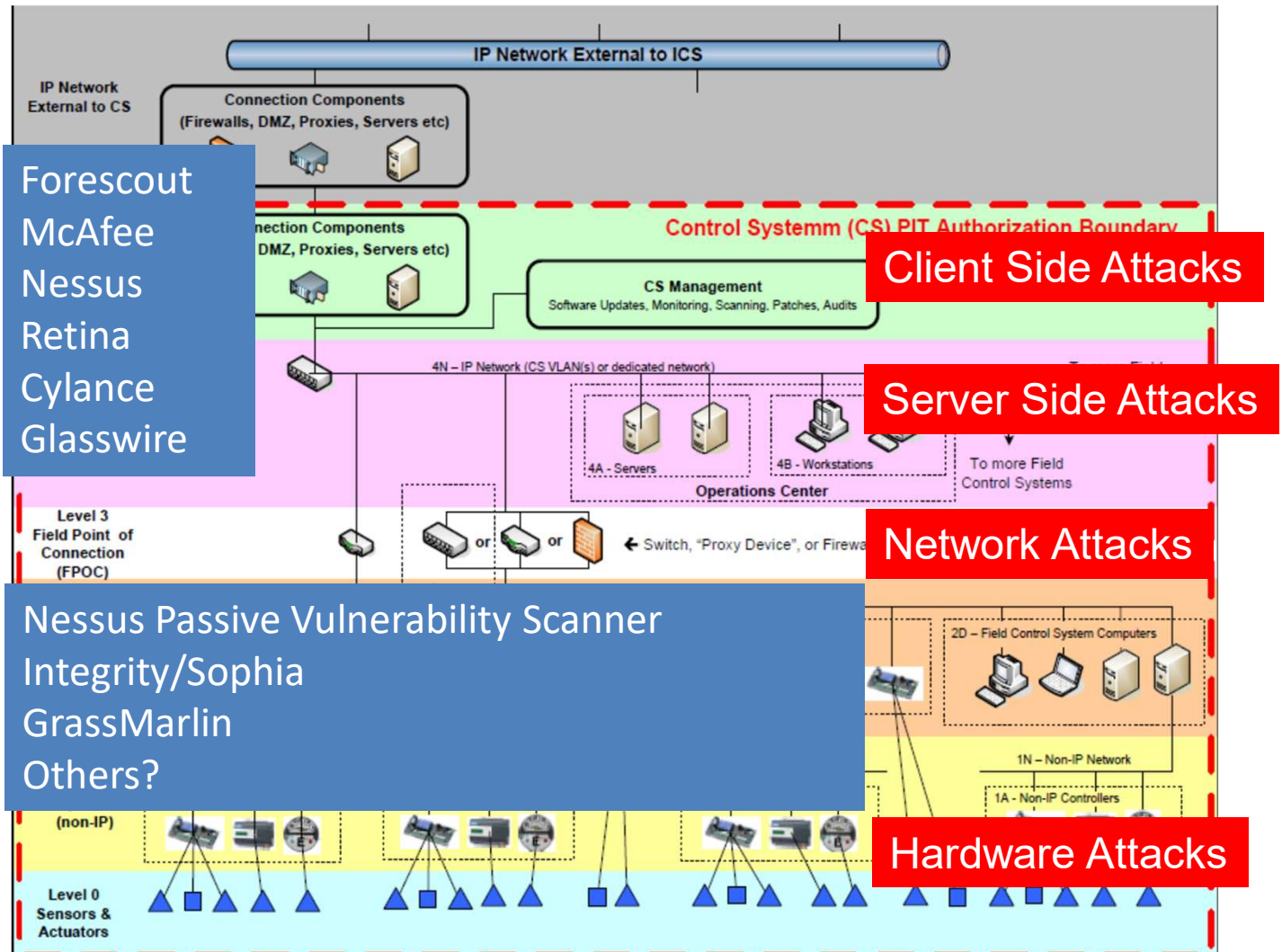


# Continuous Monitoring and Attack Surfaces

Host Based  
Security Systems  
Scanning (Active)

Windows, Linux  
HTTP, TCP, UDP

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



# Standards – NIST SP 800-82 R2



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

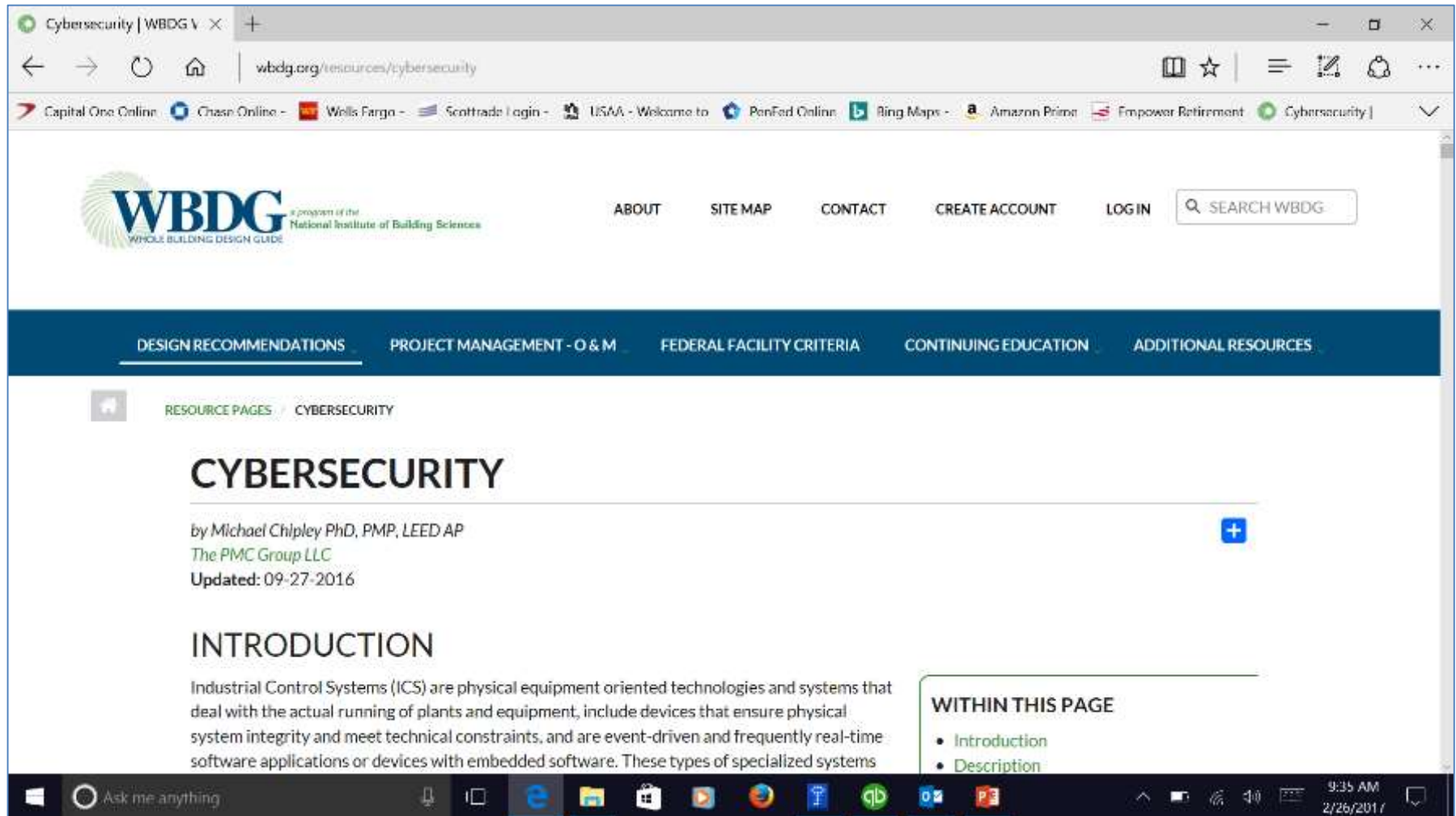
## Acquisition and Contracts

- 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



The screenshot shows a web browser window displaying the WBDG Cybersecurity Resource Page. The browser's address bar shows the URL [www.wbdg.org/resources/cybersecurity](http://www.wbdg.org/resources/cybersecurity). The page features the WBDG logo (Whole Building Design Guide) and a navigation menu with links for ABOUT, SITE MAP, CONTACT, CREATE ACCOUNT, and LOGIN. A search bar is also present. Below the navigation menu, a dark blue banner contains links for DESIGN RECOMMENDATIONS, PROJECT MANAGEMENT - O & M, FEDERAL FACILITY CRITERIA, CONTINUING EDUCATION, and ADDITIONAL RESOURCES. The main content area is titled "CYBERSECURITY" and is authored by Michael Chipley PhD, PMP, LEED AP, from The PMC Group LLC. The page was updated on 09-27-2016. The introduction text states: "Industrial Control Systems (ICS) are physical equipment oriented technologies and systems that deal with the actual running of plants and equipment, include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software. These types of specialized systems". A sidebar on the right titled "WITHIN THIS PAGE" lists links for Introduction and Description. The Windows taskbar at the bottom shows the time as 9:35 AM on 2/26/2017.

Cybersecurity | WBDG V X

← → ↻ 🏠 | [www.wbdg.org/resources/cybersecurity](http://www.wbdg.org/resources/cybersecurity) | 📖 ☆ | ☰ | 🗺️ 🔍 🔔 ⋮

🔗 Capital One Online 🔗 Chase Online 🔗 Wells Fargo 🔗 Scottrade Login 🔗 USAA - Welcome to 🔗 PenFed Online 🔗 Bing Maps 🔗 Amazon Prime 🔗 Empower Retirement 🔗 Cybersecurity |

**WBDG** a program of the  
National Institute of Building Sciences

ABOUT SITE MAP CONTACT CREATE ACCOUNT LOGIN 🔍 SEARCH WBDG

DESIGN RECOMMENDATIONS PROJECT MANAGEMENT - O & M FEDERAL FACILITY CRITERIA CONTINUING EDUCATION ADDITIONAL RESOURCES

RESOURCE PAGES / CYBERSECURITY

## CYBERSECURITY

by Michael Chipley PhD, PMP, LEED AP  
The PMC Group LLC  
Updated: 09-27-2016

### INTRODUCTION

Industrial Control Systems (ICS) are physical equipment oriented technologies and systems that deal with the actual running of plants and equipment, include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software. These types of specialized systems

#### WITHIN THIS PAGE

- Introduction
- Description

<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)

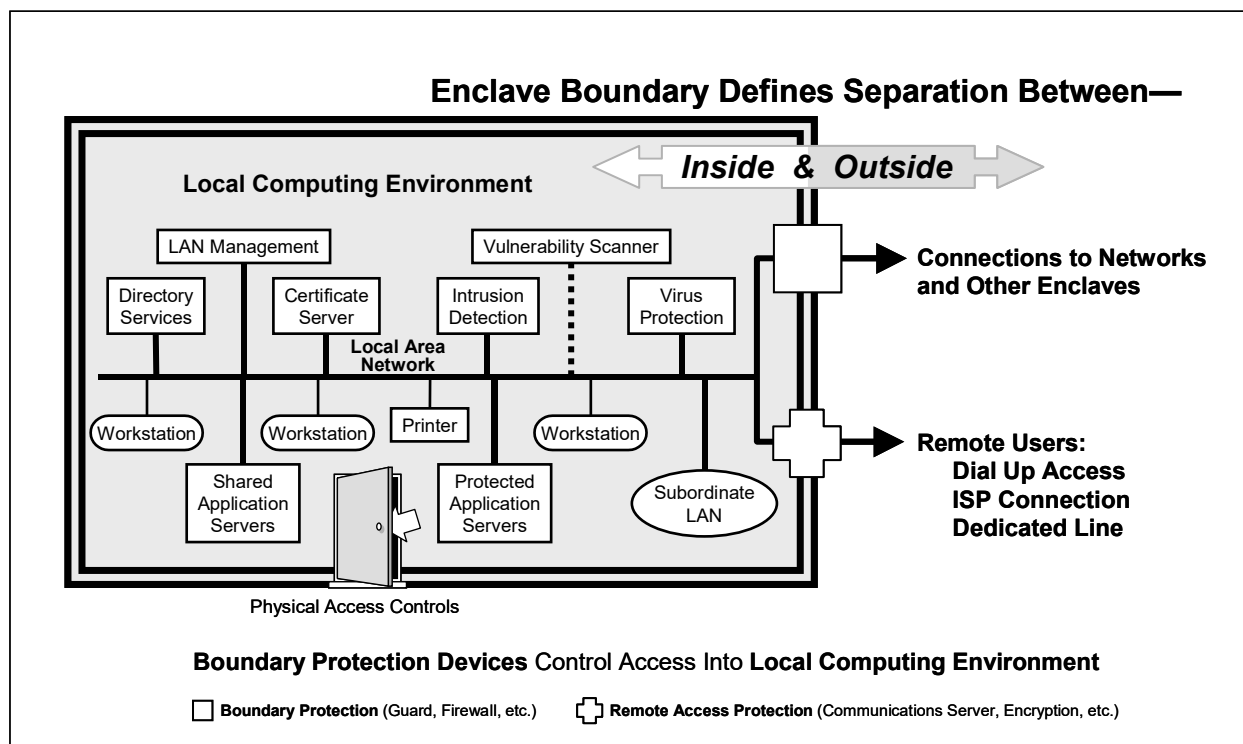


## Examples of Layered Defenses

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>

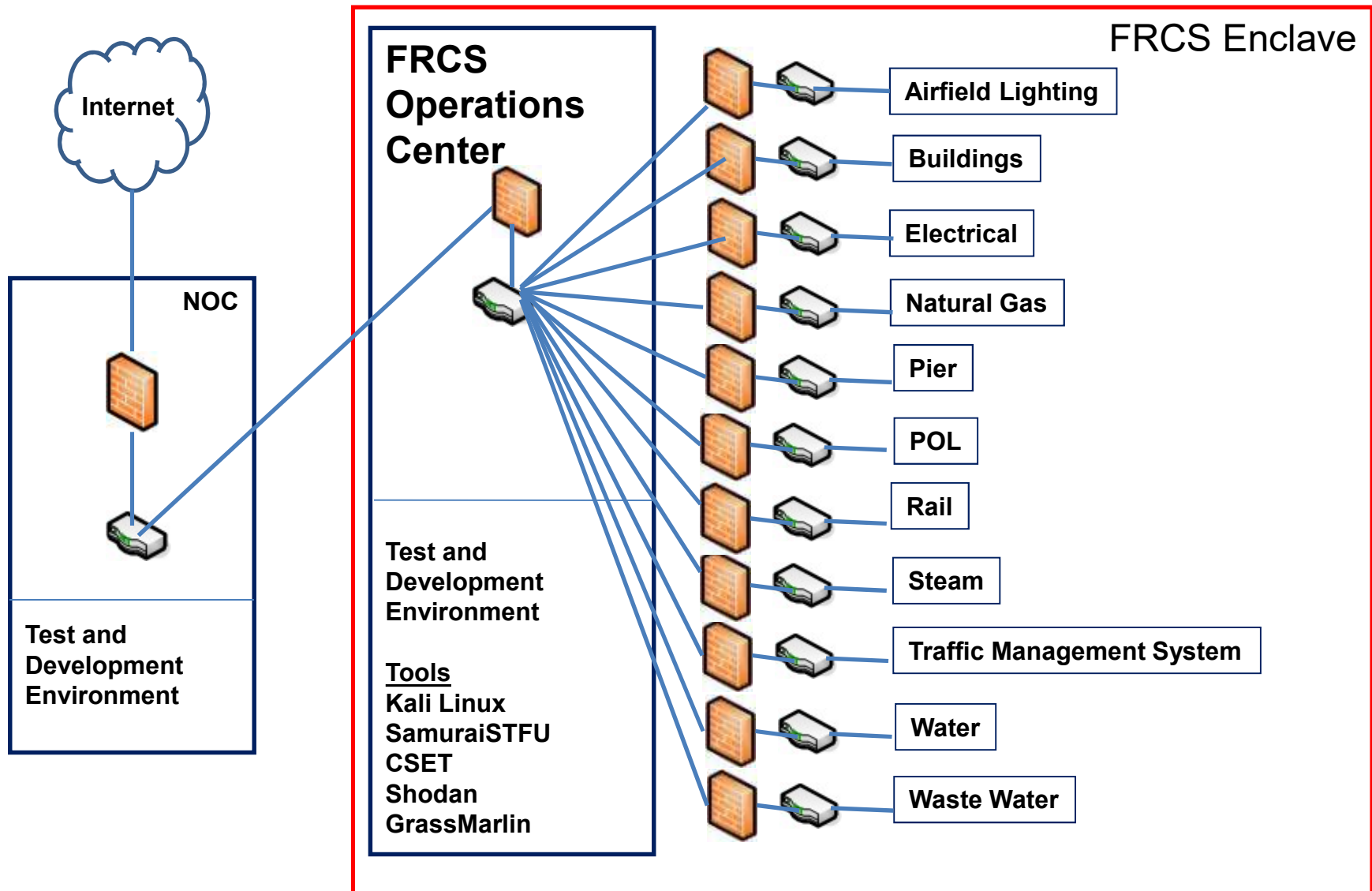
# DoD Enclaves



iatf\_6\_0\_1\_0072

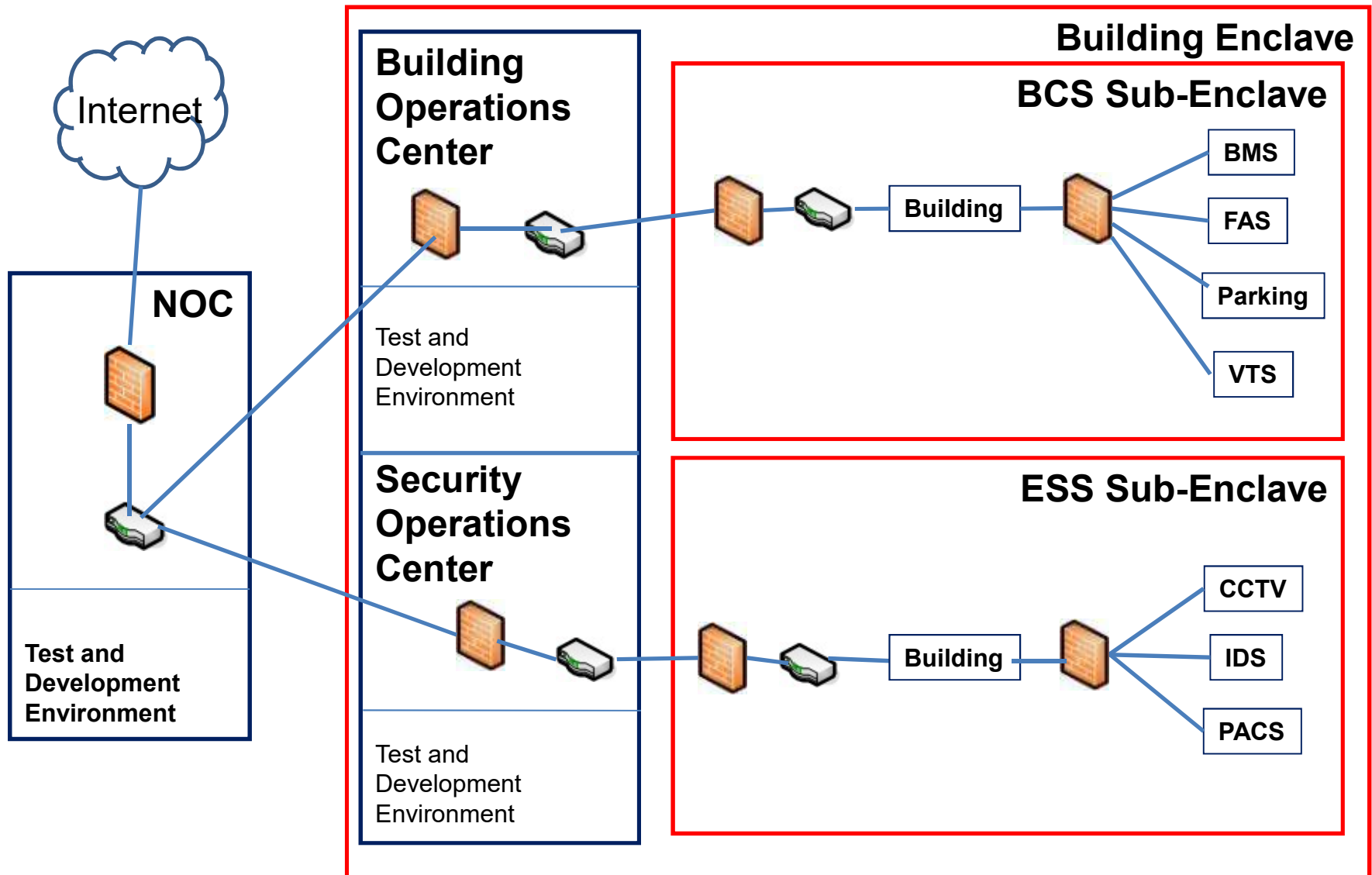
**An enclave is an environment under the control of a single authority with personnel and physical security measures.** Enclaves typically contain multiple local area networks (LAN) with computing resource components such as user platforms; network, application, and communication servers; printers; and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

# Numerous Sub-Enclaves



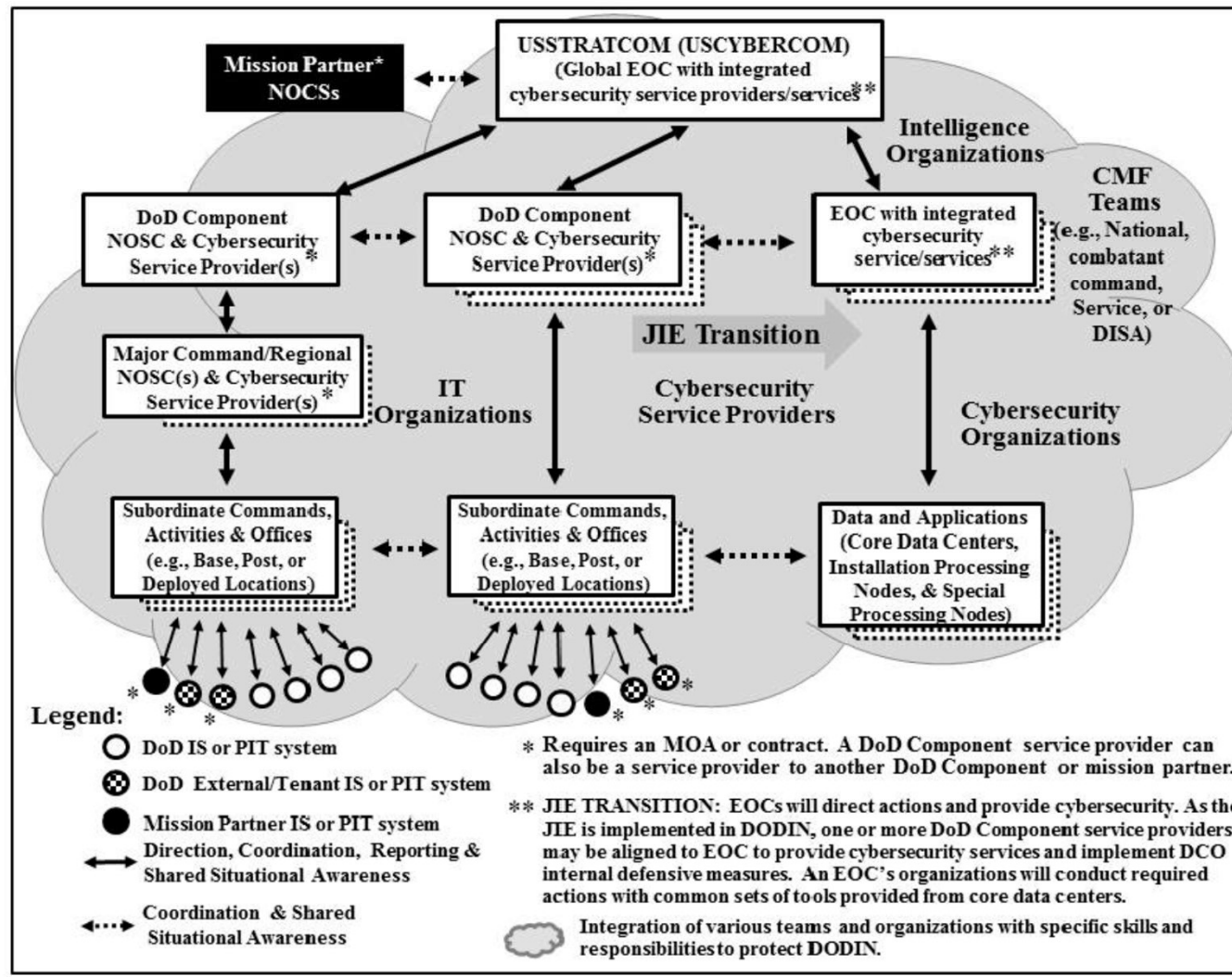


# Hybrid FRCS and Security Enclaves

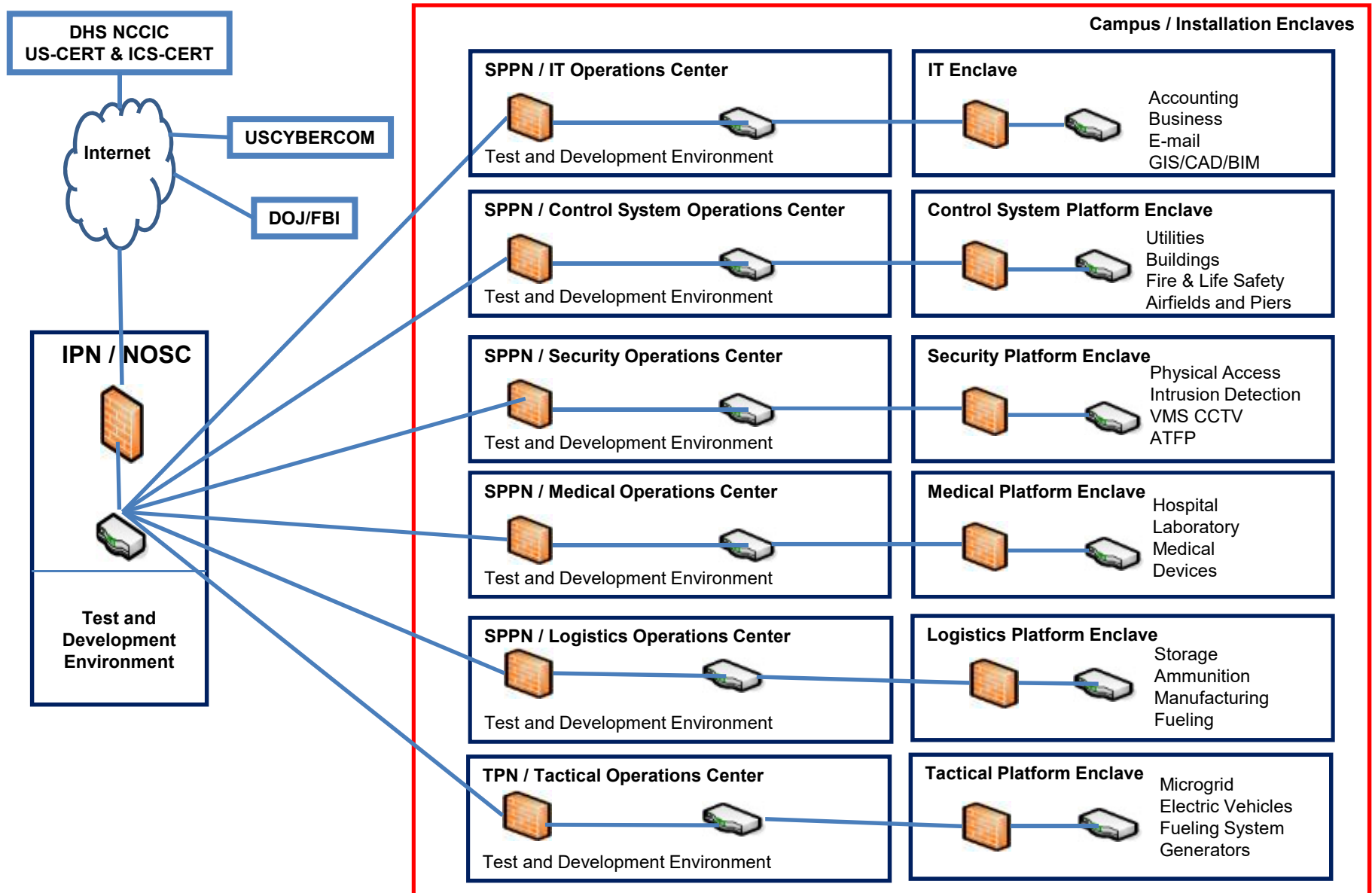


# DODI 8530 - JIE

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

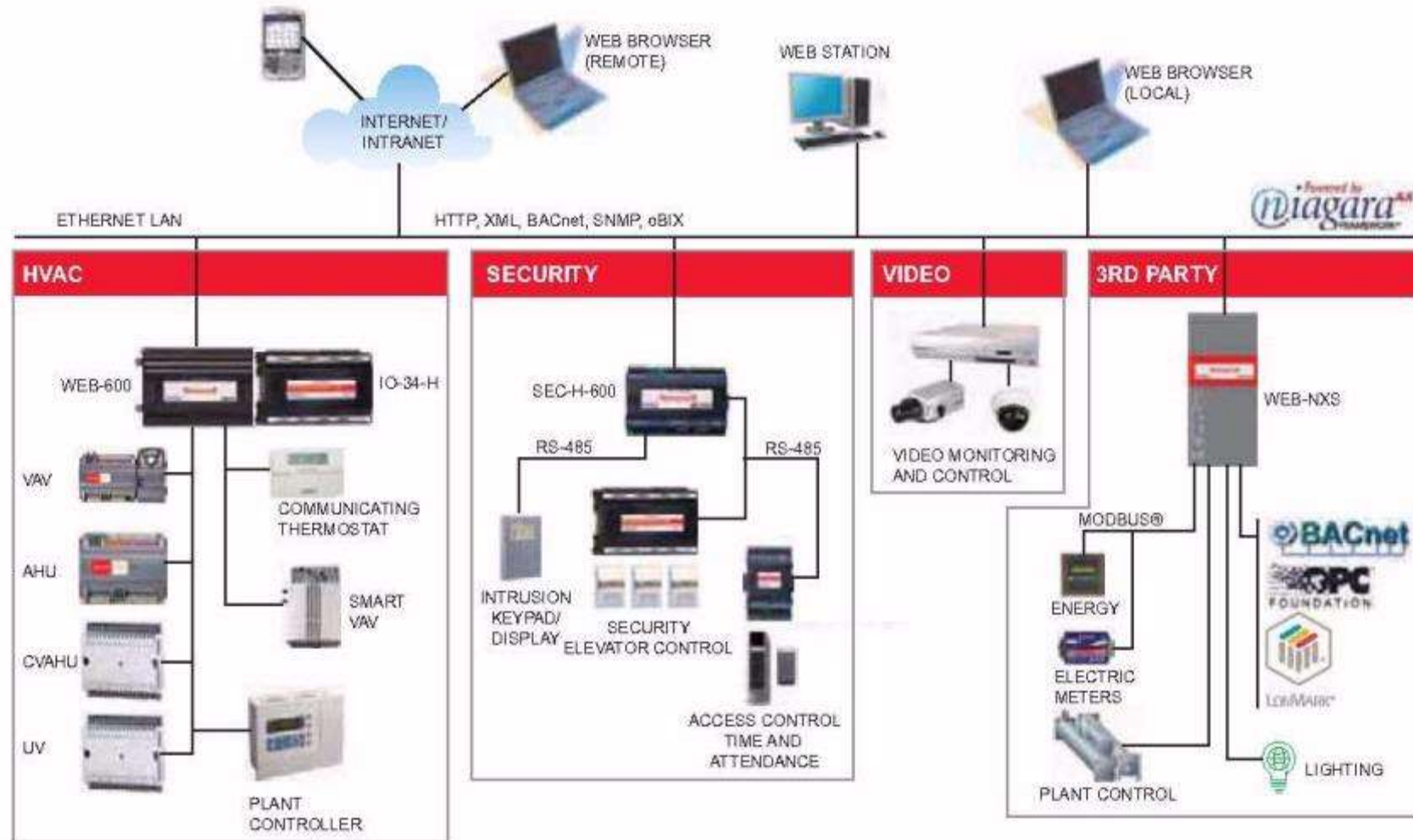


# Notional JIE Control Systems

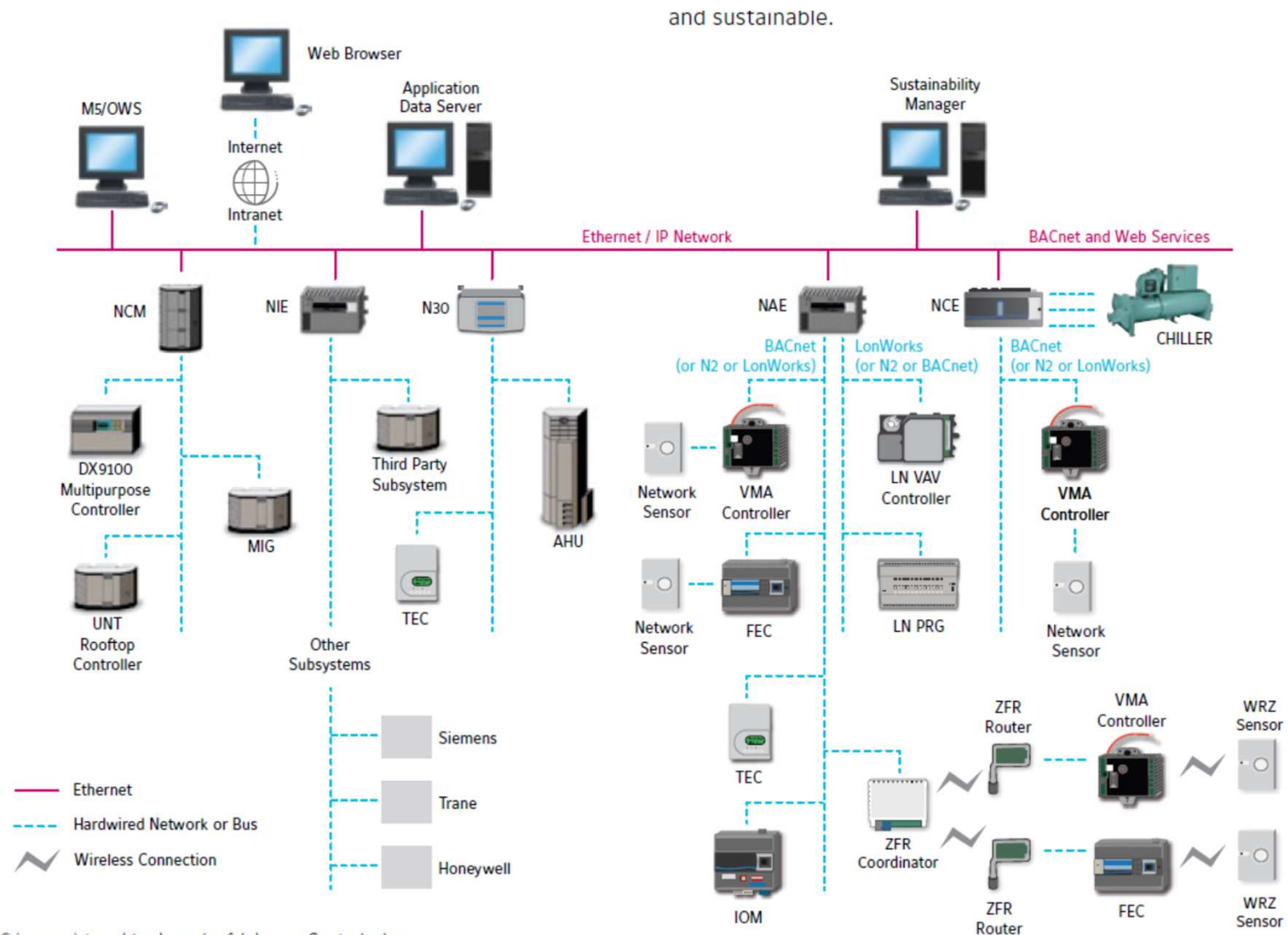


# Tridium Architecture

## WEBs SYSTEM ARCHITECTURE



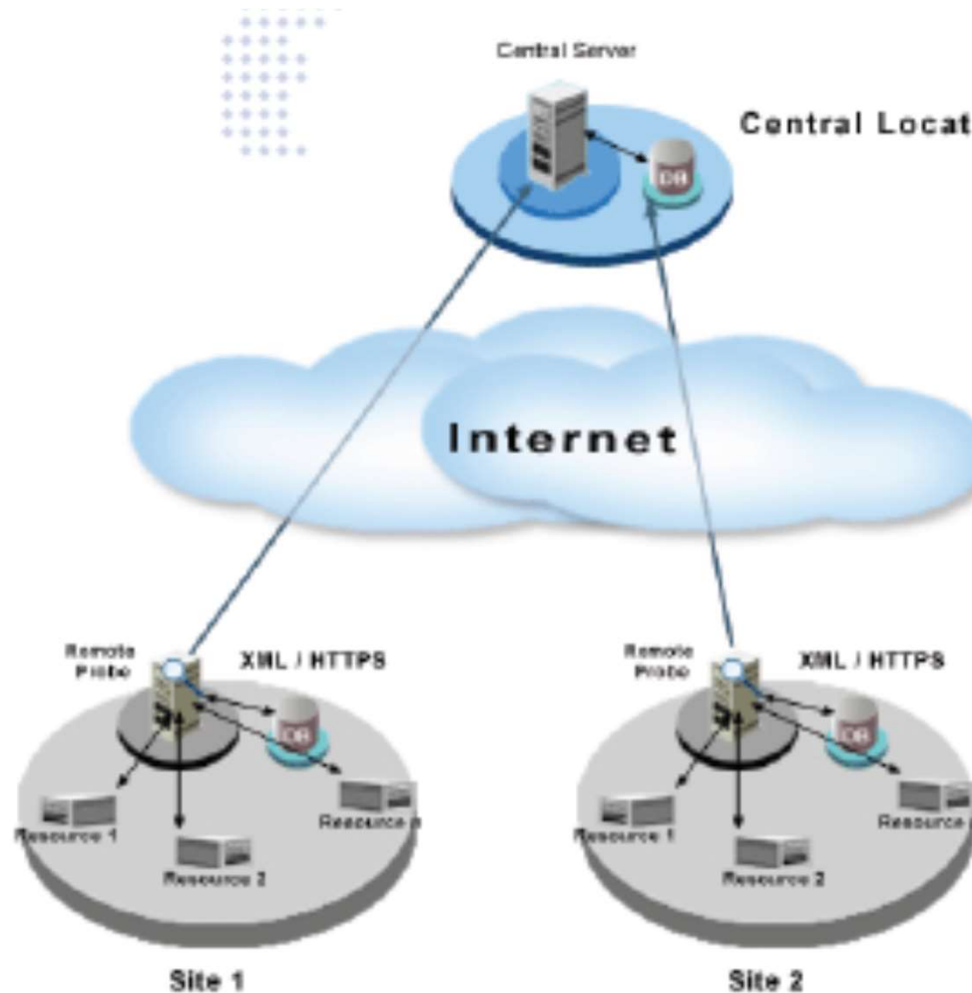
# Johnson Controls Architecture



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 NiagaraAX/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

## **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

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

# 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

A screenshot of a Kali Linux desktop environment. The desktop background is a blue and white image of Earth from space. A terminal window is open in the center, displaying the output of an NMAP scan. The terminal title is 'root@kali: ~'. The command entered is 'nmap -sS 172.16.78.131 -p 21,22,23,80,135,139,443,445'. The output shows the scan results for 172.16.78.131, including open ports (135/tcp, 139/tcp, 443/tcp, 445/tcp) and closed ports (21/tcp, 22/tcp, 23/tcp, 80/tcp). The MAC address is identified as 00:0C:29:C2:F0:02 (VMware). The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The desktop has a top bar with 'Applications', 'Places', and a clock showing 'Sun Jan 5, 1:45 PM'. A 'Computer' icon is visible on the left side of the desktop.

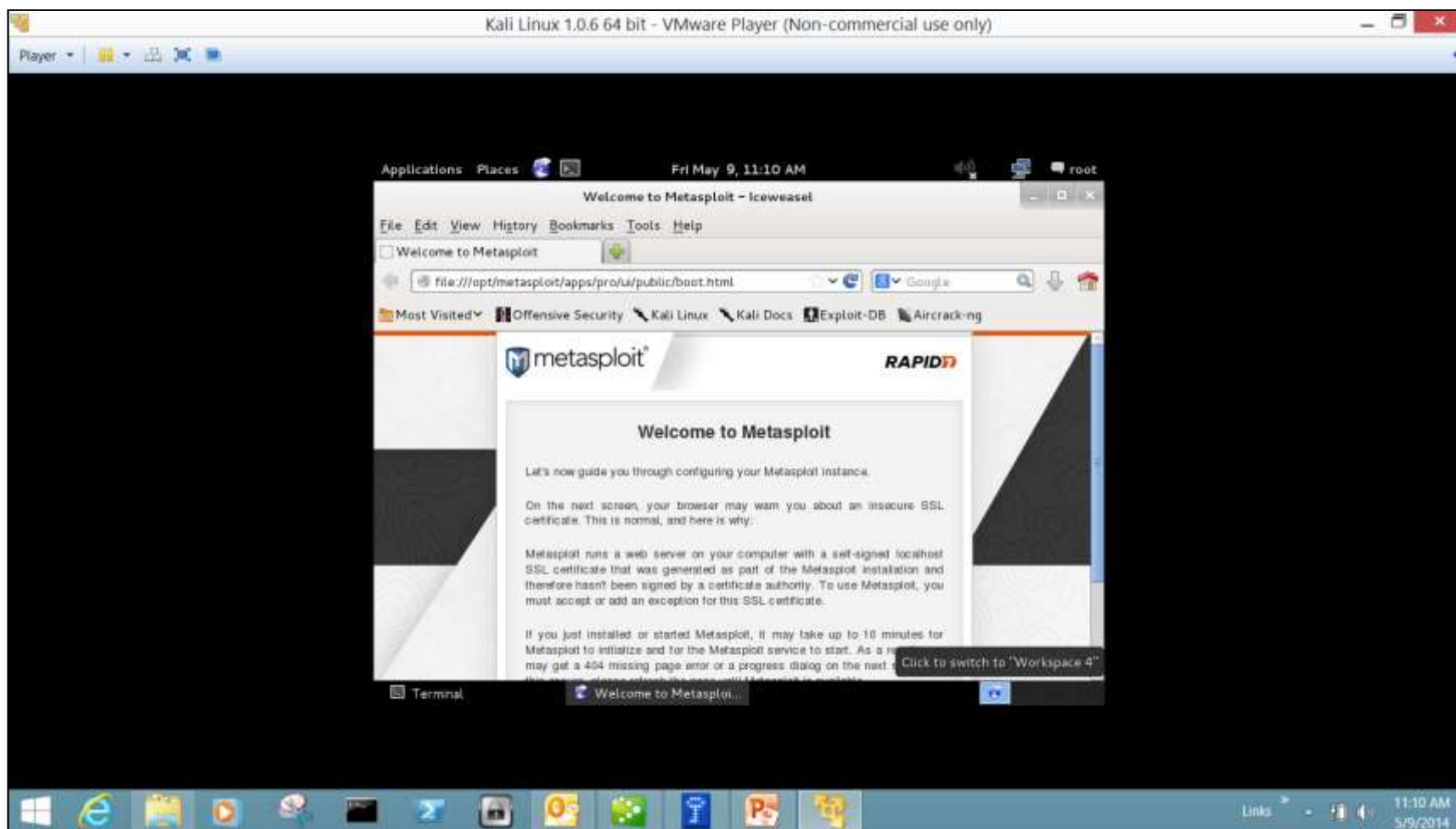
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -sS 172.16.78.131 -p 21,22,23,80,135,139,443,445  
Starting Nmap 6.25 ( http://nmap.org ) at 2014-01-05 13:44 CST  
Nmap scan report for 172.16.78.131  
Host is up (0.0012s latency).  
PORT      STATE SERVICE  
21/tcp    closed ftp  
22/tcp    closed ssh  
23/tcp    closed telnet  
80/tcp    closed http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
443/tcp   closed https  
445/tcp   open  microsoft-ds  
MAC Address: 00:0C:29:C2:F0:02 (VMware)  
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds  
root@kali:~#
```

# 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.”*

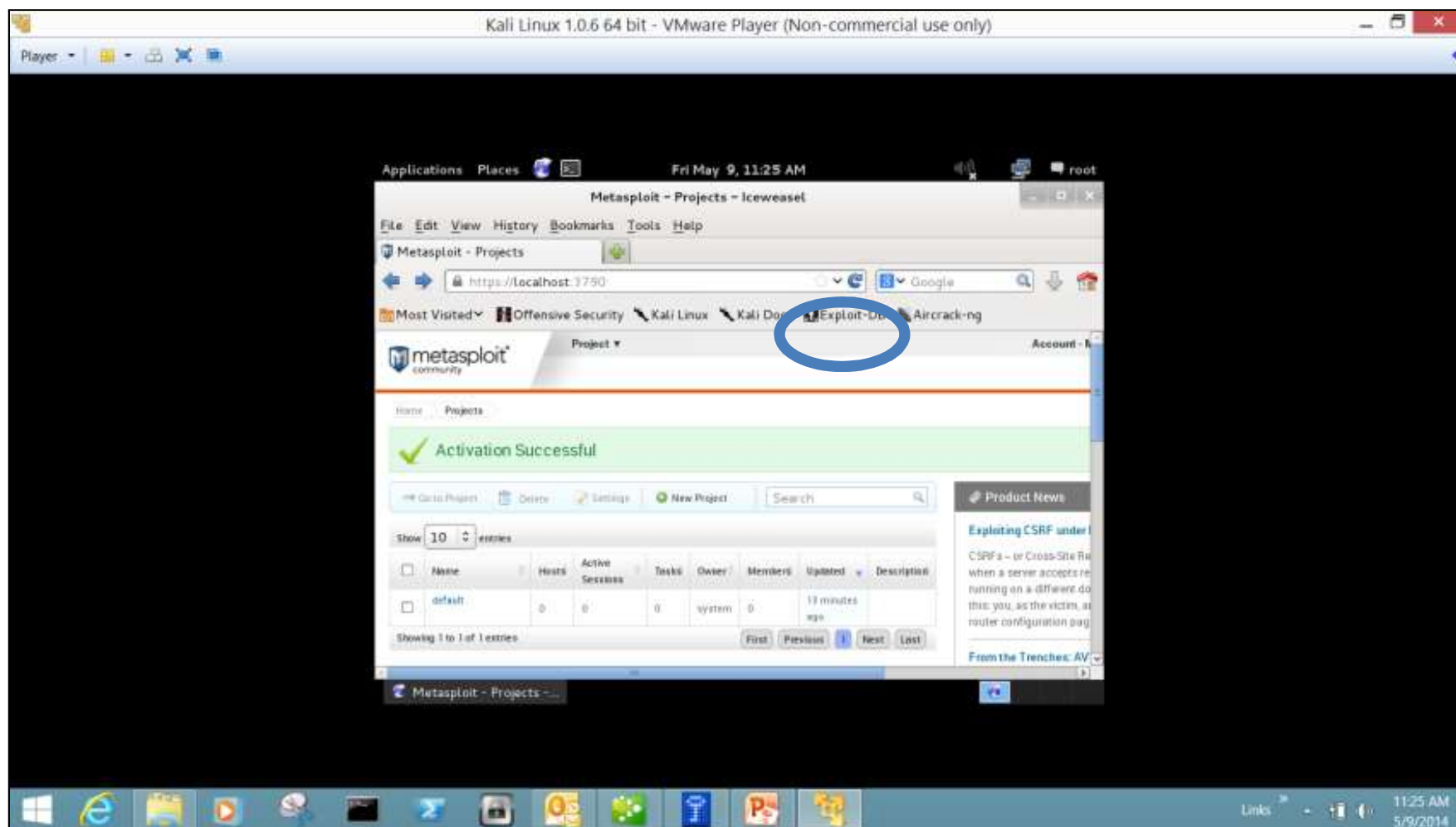
The most sophisticated attackers would likely obtain access to the target environment. After obtaining access to the critical infrastructure, techniques will be utilized to achieve the 6D's of Computer Network Attack.

# 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.

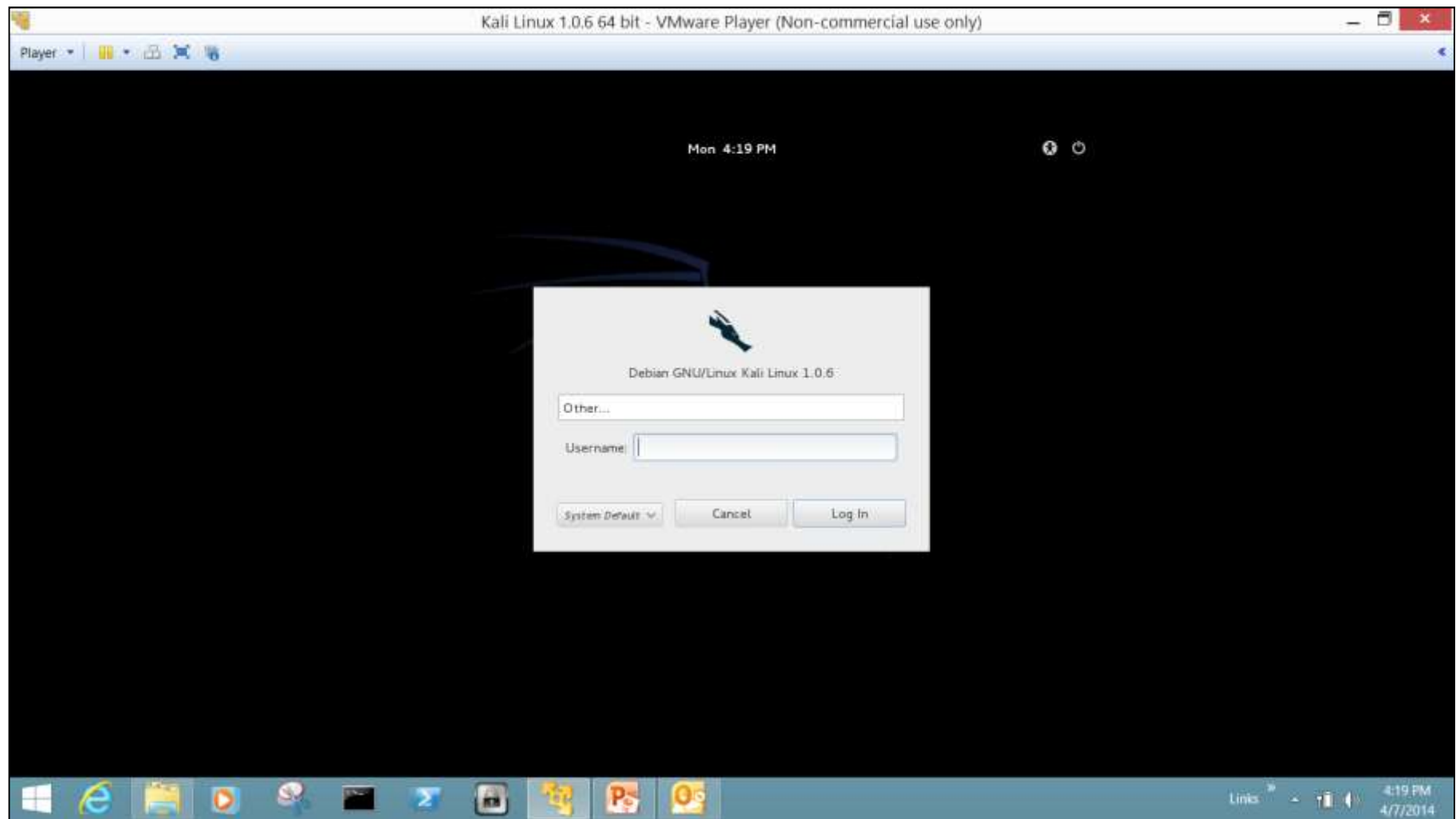
**Custom kernel patched for injection:** As penetration testers, the development team often needs to do wireless assessments so our kernel has the latest injection patches included.

**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.

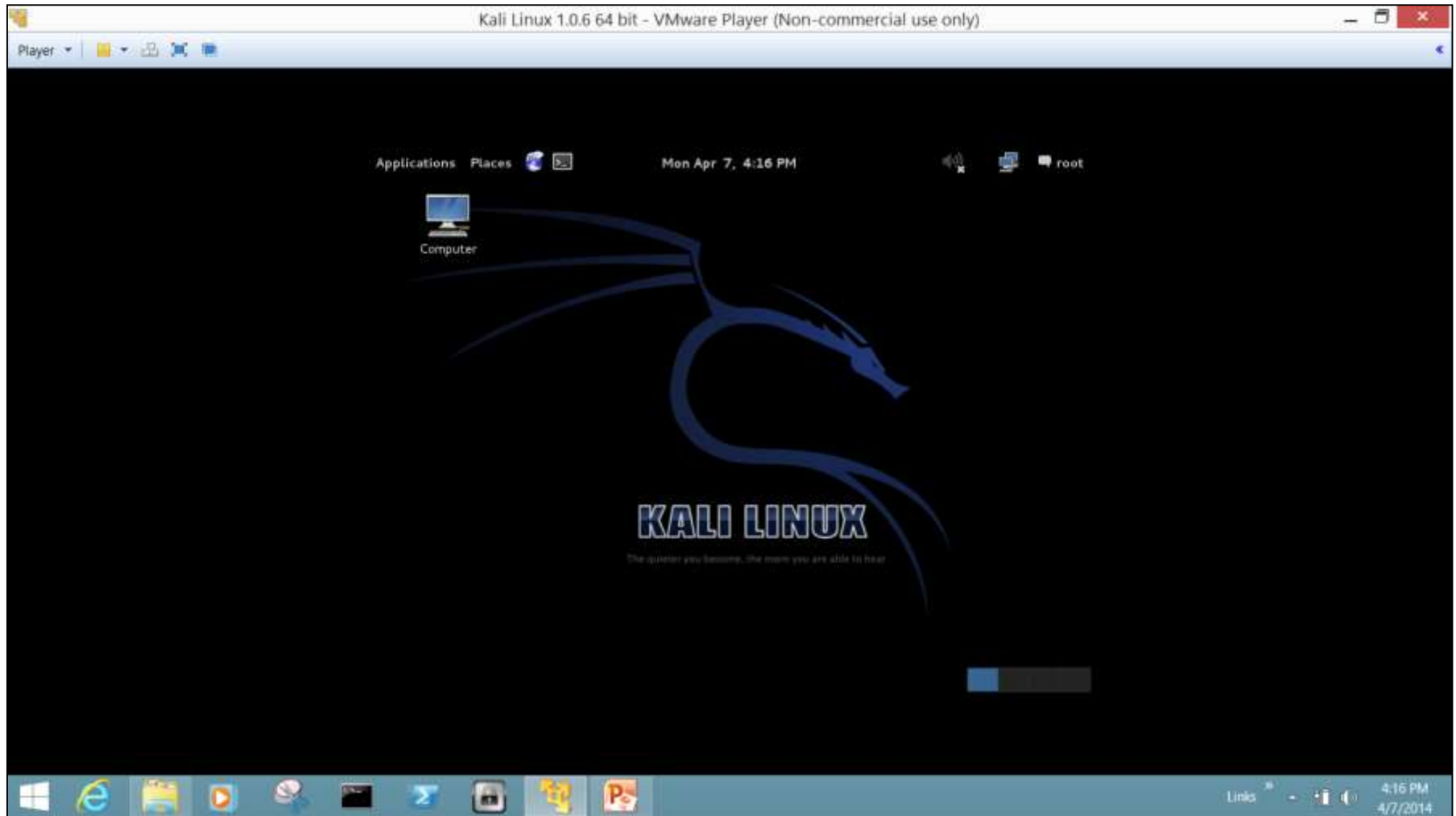
**Completely customizable:** We completely understand that not everyone will agree with our design decisions so we have made it as easy as possible for our more adventurous users to [customize Kali Linux](#) to their liking, all the way down to the kernel.

**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.

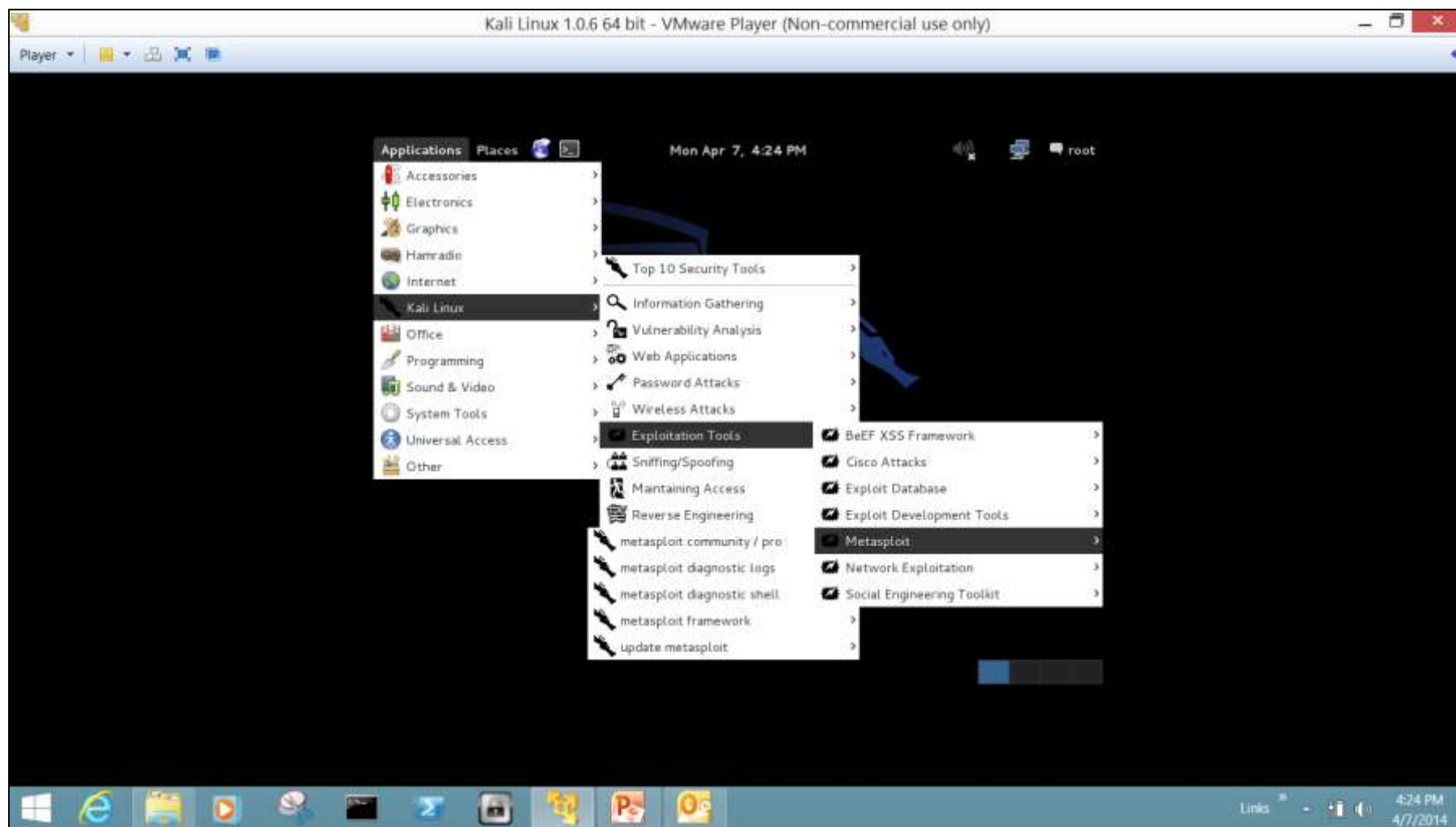
# Kali Linux Login



# 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

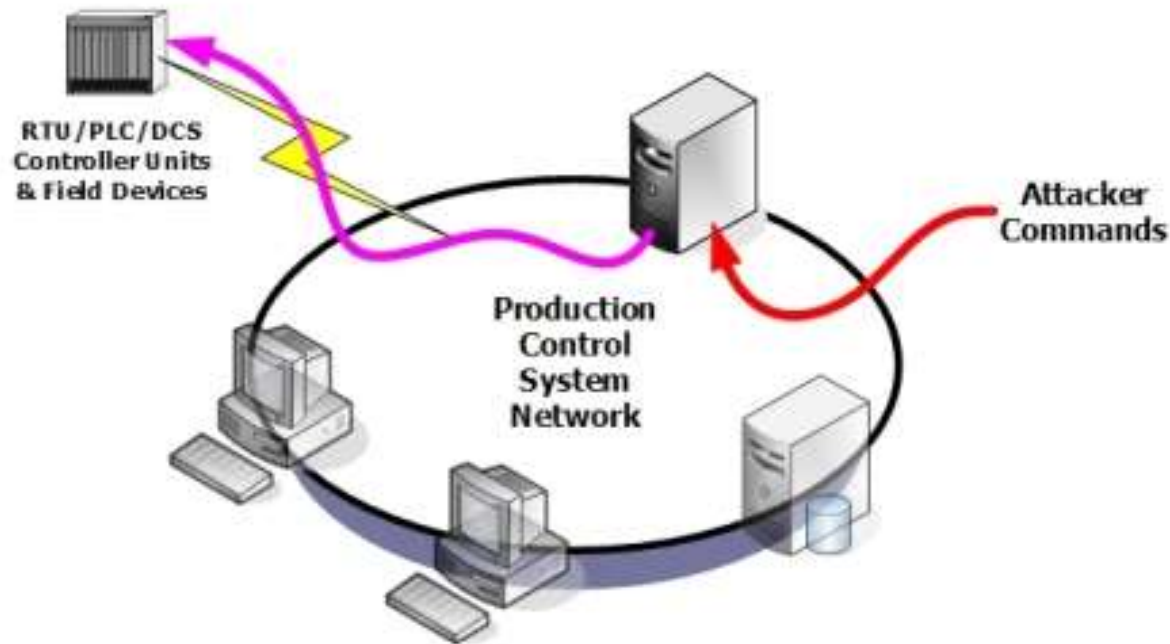
## **Discovery of the Process**

- 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**

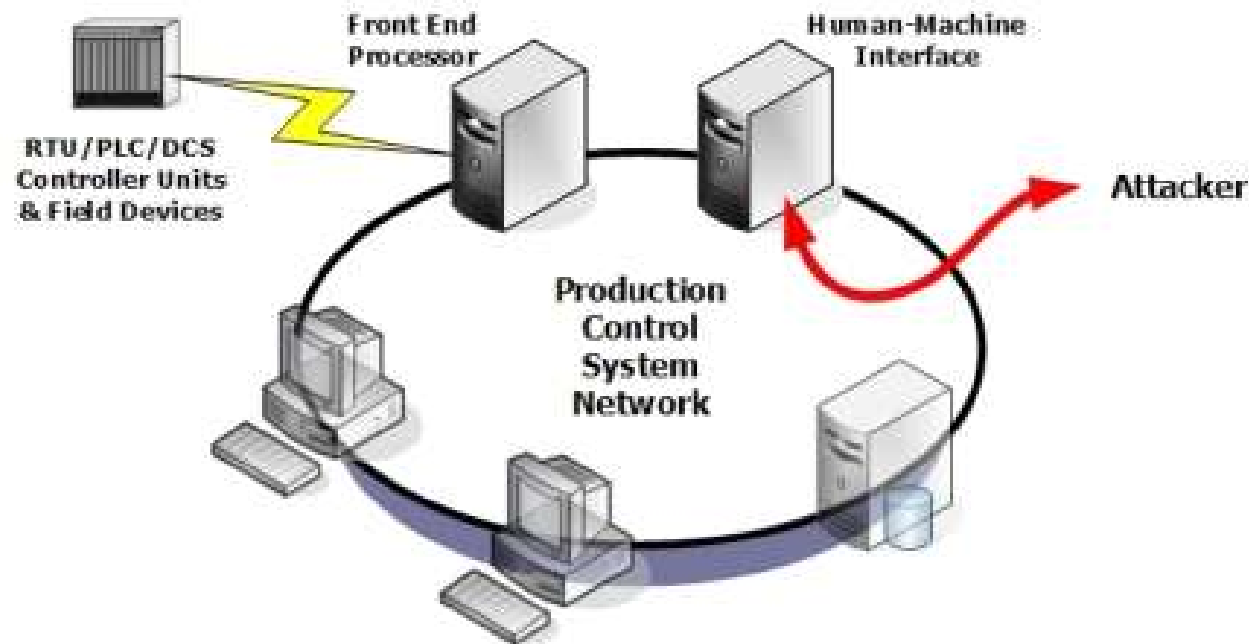
- Sending Commands Directly to the Data Acquisition Equipment
- Exporting the HMI Screen
- Changing the Database
- Man-in-the-Middle Attacks

# Sending Commands Directly



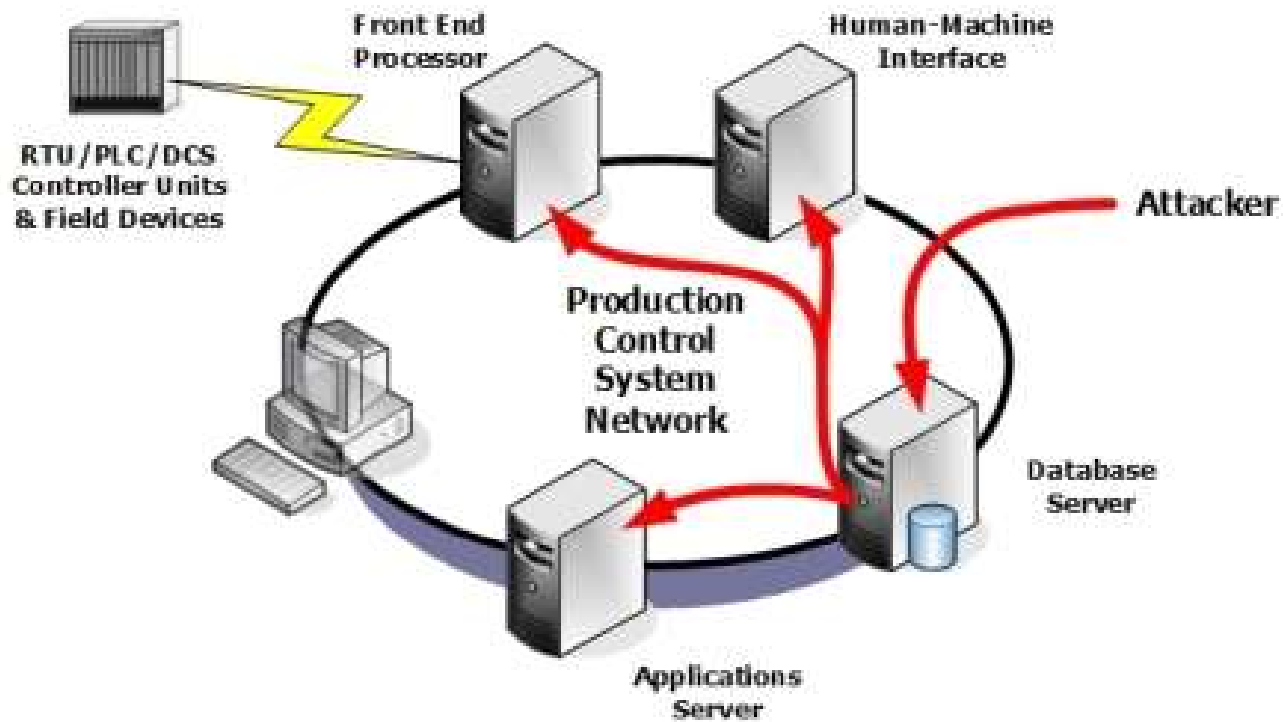
The easiest way to control the process is to send commands directly to the data acquisition equipment. **Most PLCs, protocol converters, or data acquisition servers lack even basic authentication. They generally accept any properly formatted command.** An attacker wishing control simply establishes a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

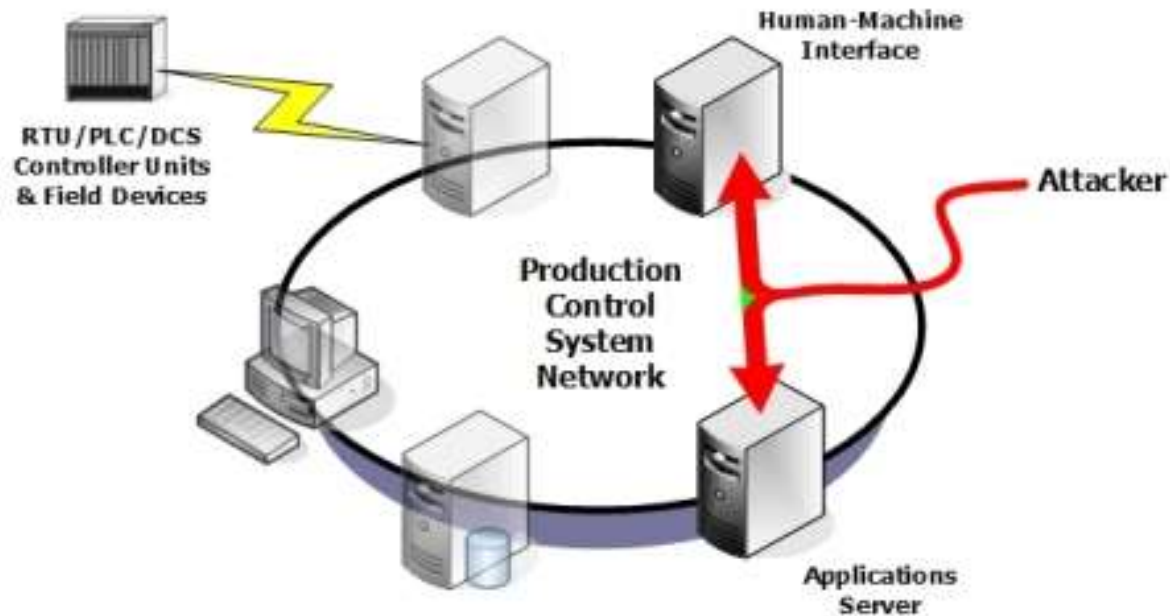
# Changing the Database



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

The screenshot shows the ICS-CERT website in a web browser. The browser's address bar displays the URL <http://ics-cert.us-cert.gov/Recommended-Practice>. The website header includes the ICS-CERT logo and the text "INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM". A navigation menu at the top contains links for HOME, ABOUT, ICSJWG, INFORMATION PRODUCTS, TRAINING, and FAQ. On the left side, a sidebar menu lists various resources, with "Recommended Practices" highlighted. The main content area is titled "Recommended Practices" and contains a paragraph explaining the purpose of the section. Below this, a list of recommended practices is provided, each with links to abstracts and full documents.

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 Response 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](#)

Windows taskbar at the bottom shows the Start button, Internet Explorer, File Explorer, and other applications. The system clock indicates 2:07 PM on 5/7/2014.

# DHS Control Systems Defense in Depth (1)

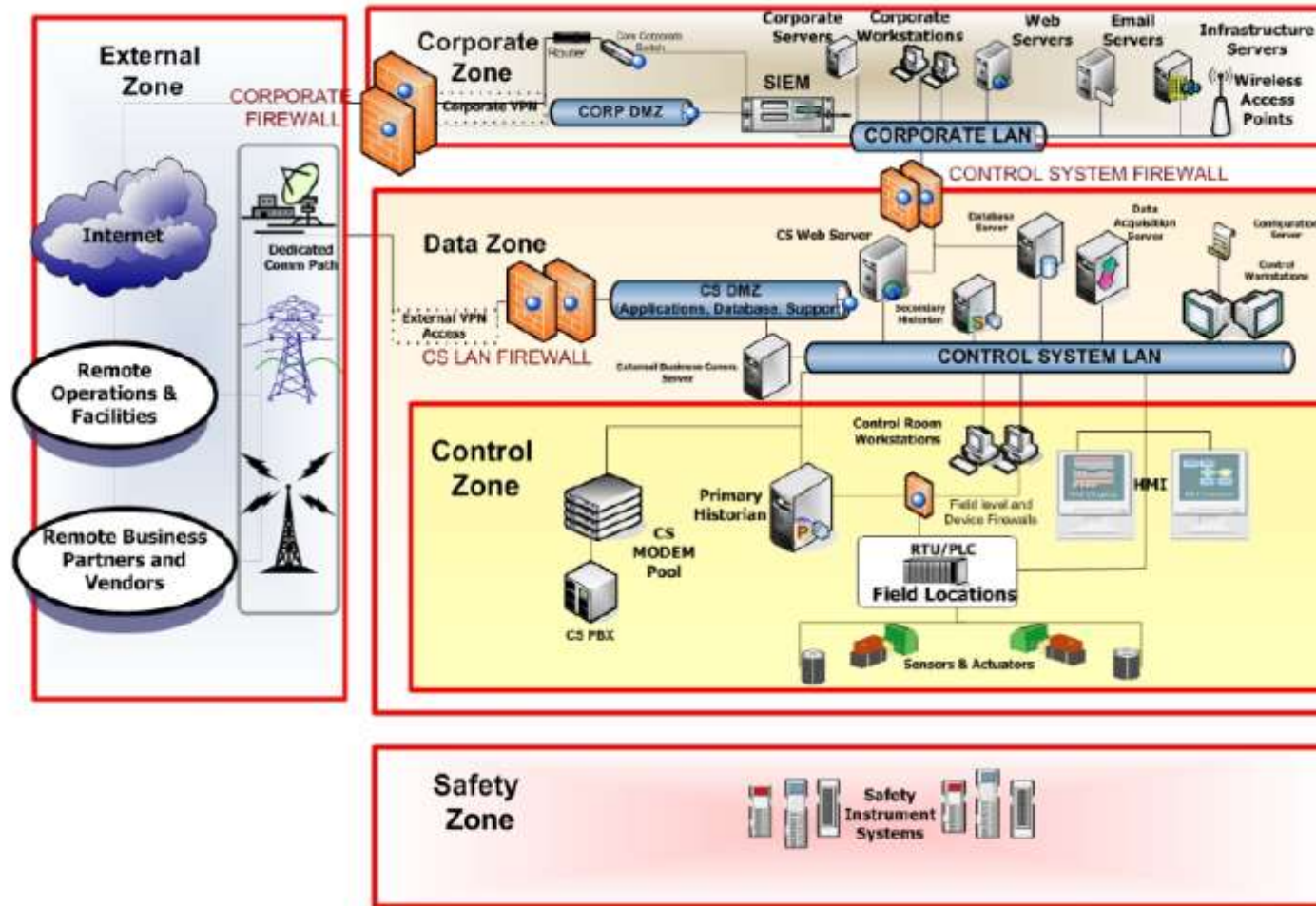
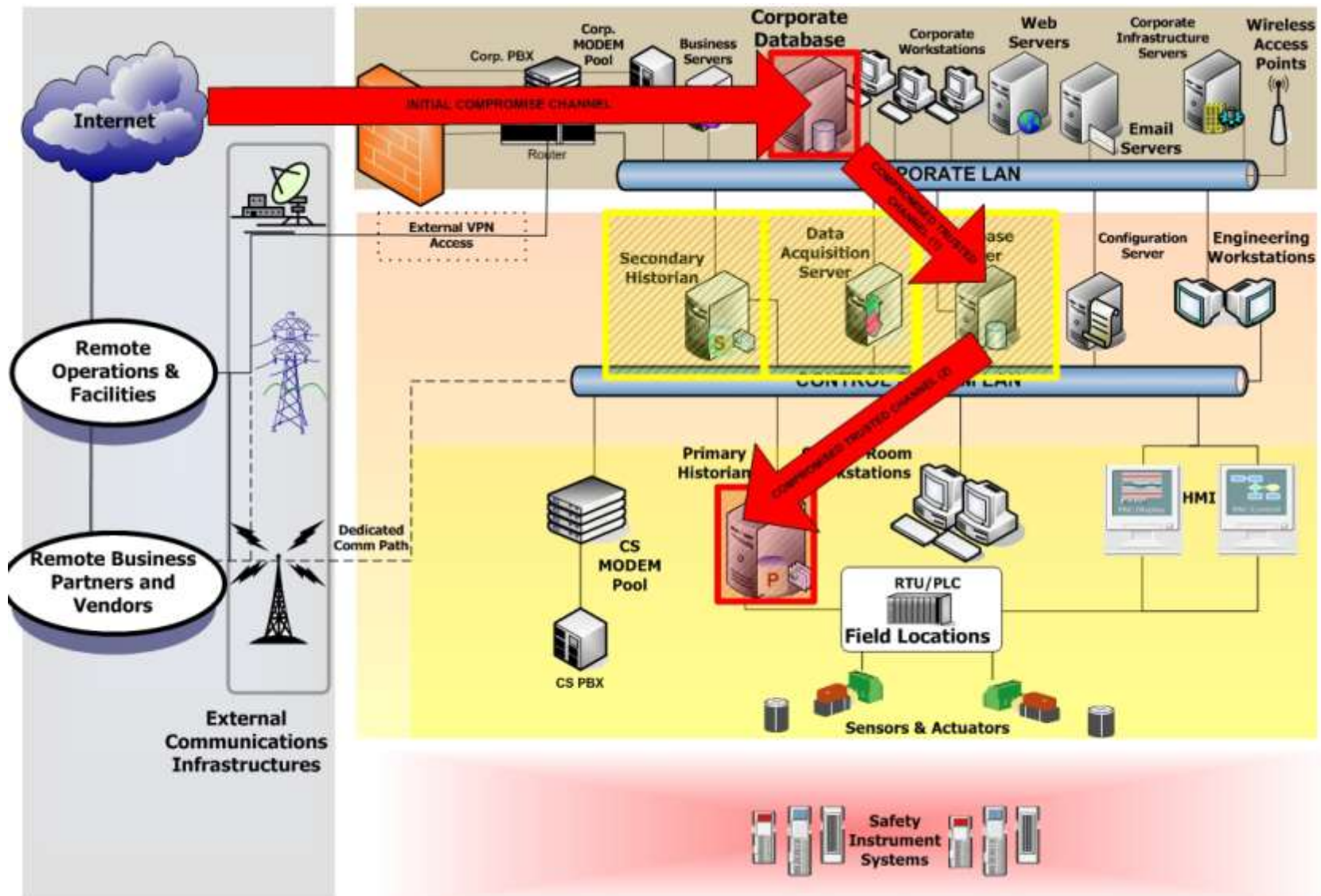


Figure 10. Complete defense-in-depth strategy with the intrusion detection system and SIEM.

***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

### Introduction

#### A. 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
10. Examine all machines on the local network

#### B. Review Other CERT Documents

1. CERT Summaries
2. "Steps for Recovering from a UNIX Root Compromise"
3. Contacting CERT/CC

### Revision History

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](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](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](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
<input type="checkbox"/> Policy Management	<input type="checkbox"/> Contract Management	<input type="checkbox"/> Master Equipment List	<input type="checkbox"/> Transition Management	<input type="checkbox"/> Life Cycle Cost Analysis
<input type="checkbox"/> Risk Management Framework	<input type="checkbox"/> Permit Process	<input type="checkbox"/> Location List	<input type="checkbox"/> O&M Manuals	<input type="checkbox"/> Condition Assessments
<input type="checkbox"/> System Security Plans	<input type="checkbox"/> Drawings and Specifications	<input type="checkbox"/> Field Reporting	<input type="checkbox"/> Training Facilitation	<input type="checkbox"/> Building Controls Analytics
<input type="checkbox"/> Cyber System Categorization	<input type="checkbox"/> Submittals	<input type="checkbox"/> Deliverables Tracking	<input type="checkbox"/> Warranty Certificates	<input type="checkbox"/> Cyber Risk Assessments
<input type="checkbox"/> Configuration Management	<input type="checkbox"/> Requests for Information	<input type="checkbox"/> Inspections and Checklists	<input type="checkbox"/> Spare Parts/Special Tools	<input type="checkbox"/> Cyber Continuous Monitoring
<input type="checkbox"/> Record Documents	<input type="checkbox"/> Change Management	<input type="checkbox"/> Cyber Procedures		
		<input type="checkbox"/> Performance Testing		
		<input type="checkbox"/> 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

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

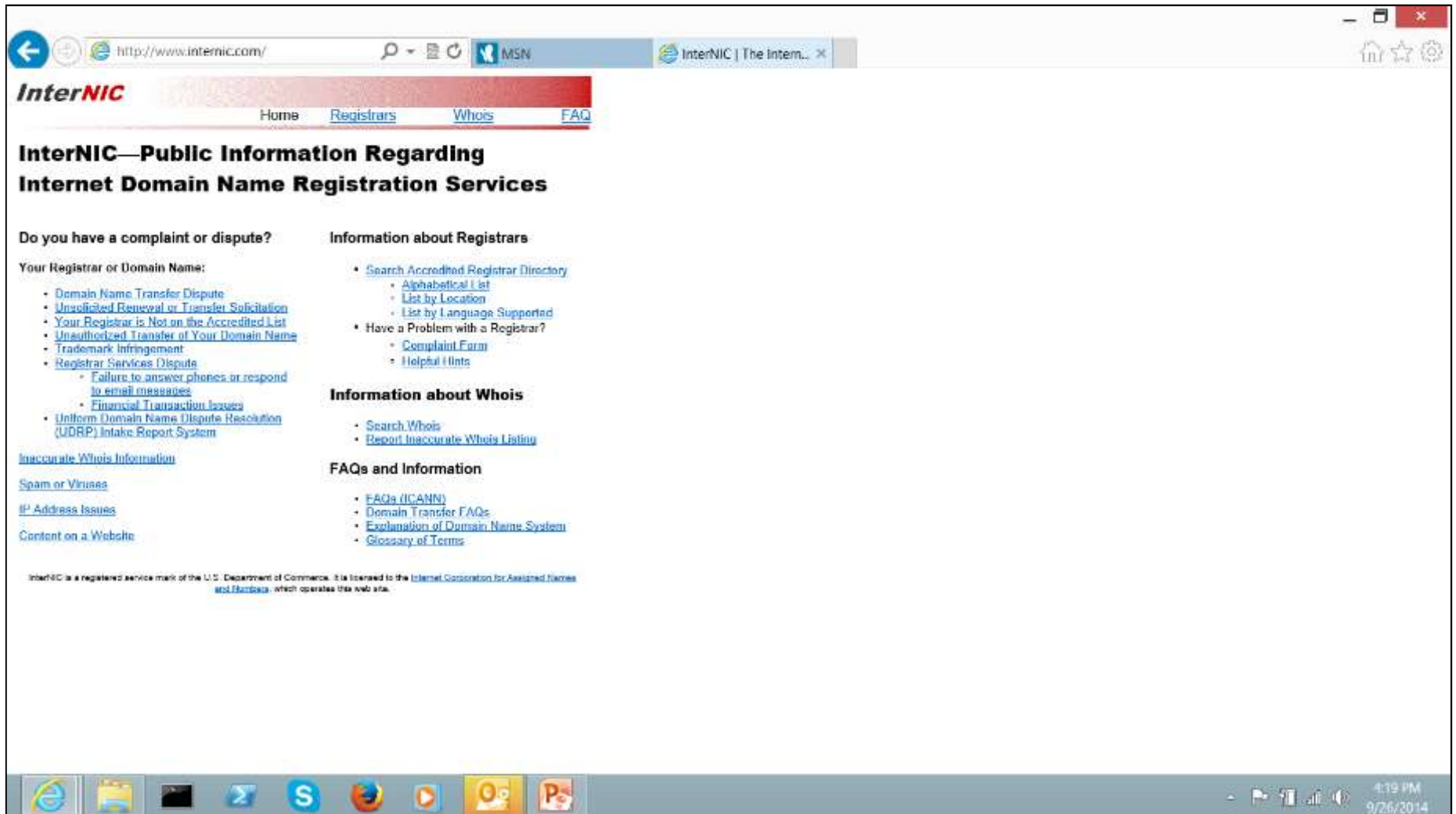
## **Open Control Systems Protocols**

- 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 NiagaraAX/Fox
- Johnson Metasys N2
- OSIsoft Pi System
- Many others...

# Whois Search on InterNIC



The screenshot shows a web browser window with the URL <http://www.internic.com/>. The browser's address bar also shows "InterNIC | The Intern...". The website's header features the "InterNIC" logo and navigation links: "Home", "Registrars", "Whois", and "FAQ".

The main heading reads: **InterNIC—Public Information Regarding Internet Domain Name Registration Services**

Under the heading "Do you have a complaint or dispute?", there is a section "Your Registrar or Domain Name:" with a list of links:

- [Domain Name Transfer Dispute](#)
- [Unsolicited Renewal or Transfer Solicitation](#)
- [Your Registrar is Not on the Accredited List](#)
- [Unauthorized Transfer of Your Domain Name](#)
- [Trademark Infringement](#)
- [Registrar Services Dispute](#)
  - [Failure to answer phones or respond to email messages](#)
  - [Financial Transaction Issues](#)
- [Uniform Domain Name Dispute Resolution \(UDRP\) Intake Report System](#)

Below this list are links for [Inaccurate Whois Information](#), [Spam or Viruses](#), [IP Address Issues](#), and [Content on a Website](#).

Under the heading "Information about Registrars", there is a list of links:

- [Search Accredited Registrar Directory](#)
  - [Alphabetical List](#)
  - [List by Location](#)
  - [List by Language Supported](#)
- [Have a Problem with a Registrar?](#)
  - [Complaint Form](#)
  - [Helpful Hints](#)

Under the heading "Information about Whois", there is a list of links:

- [Search Whois](#)
- [Report Inaccurate Whois Listing](#)

Under the heading "FAQs and Information", there is a list of links:

- [FAQs \(ICANN\)](#)
- [Domain Transfer FAQs](#)
- [Explanation of Domain Name System](#)
- [Glossary of Terms](#)

At the bottom of the page, a small text block states: "InterNIC is a registered service mark of the U.S. Department of Commerce. It is licensed to the Internet Corporation for Assigned Names and Addresses, which operates this web site."

The Windows taskbar at the bottom shows the time as 4:19 PM on 9/26/2014, along with various system icons and open application windows.

# Whois Domain Search on InterNIC

The screenshot shows a web browser window with the URL [http://reports.internic.net/cgi/whois?whois\\_pmcgroup.biz](http://reports.internic.net/cgi/whois?whois_pmcgroup.biz). The page features the InterNIC logo and navigation links for Home, Registrars, FAQ, and Whois. The main section, titled "Whois Search Results", includes a search bar with the domain "pmcgroup.biz" and radio buttons to select the search type: Domain (selected), Registrar, or Nameserver. Below the search options, a detailed list of domain and contact information is displayed.

**Whois Search Results**

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

pmcgroup.biz

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

Submit

Domain Name:	PMCGROUP.BIZ
Domain ID:	D19249558-BIZ
Sponsoring Registrar:	NETWORK SOLUTIONS INC.
Sponsoring Registrar IANA ID:	2
Registrar URL (registration services):	whois.biz
Domain Status:	clientTransferProhibited
Registrant ID:	42056314V
Registrant Name:	Perfect Privacy, LLC
Registrant Organization:	The PMC Group LLC
Registrant Address1:	12808 Gran Bay Parkway West
Registrant Address2:	care of Network Solutions
Registrant City:	Jacksonville
Registrant State/Province:	FL
Registrant Postal Code:	32258
Registrant Country:	United States
Registrant Country Code:	US
Registrant Phone Number:	+1.5707088780
Registrant Email:	ns5ev7yp23x@networksolutionsprivateregistration.com
Administrative Contact ID:	42056314V
Administrative Contact Name:	Perfect Privacy, LLC
Administrative Contact Organization:	The PMC Group LLC
Administrative Contact Address1:	12808 Gran Bay Parkway West
Administrative Contact Address2:	care of Network Solutions
Administrative Contact City:	Jacksonville
Administrative Contact State/Province:	FL
Administrative Contact Postal Code:	32258
Administrative Contact Country:	United States
Administrative Contact Country Code:	US
Administrative Contact Phone Number:	+1.5707088780
Administrative Contact Email:	ns5ev7yp23x@networksolutionsprivateregistration.com
Billing Contact ID:	42056315V
Billing Contact Name:	Perfect Privacy, LLC
Billing Contact Organization:	The PMC Group LLC
Billing Contact Address1:	12808 Gran Bay Parkway West

# Whois Nameserver Search on InterNIC

The screenshot shows a web browser window with the URL <http://reports.internic.net/cgi/whois?whois>. The page features the InterNIC logo and navigation links for Home, Registrars, FAQ, and Whois. The main section is titled "Whois Search Results" and contains a search form with the text "NS43.WORLDDNIC.COM" entered. Below the form are radio buttons for "Domain" (selected), "Registrar", and "Nameserver". A "Submit" button is at the bottom of the form.

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.WORLDDNIC.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,

The browser's taskbar at the bottom shows the Windows Start button and several application icons. The system tray in the bottom right corner displays the time as 4:30 PM and the date as 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](http://en.wikipedia.org/wiki/Google_hacking)



# Google Search and Hacking Tools

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

[HOME](#)
[ETHICAL HACKING](#)
[ARTICLES](#)
[GUEST POST](#)
[COPYRIGHT](#)
[ADVERTISEMENT](#)
[QUEST](#)

[GAME HACKS](#)
[WINDOWS T HACKS](#)
[GOOGLE HACKS](#)
[CMD HACKS](#)
[ABOUT](#)
[CONTACT US](#)

## PC HACKS / STEP BY STEP

Home » Google Hacks

### Google Hacks

[f Like](#) [T](#)

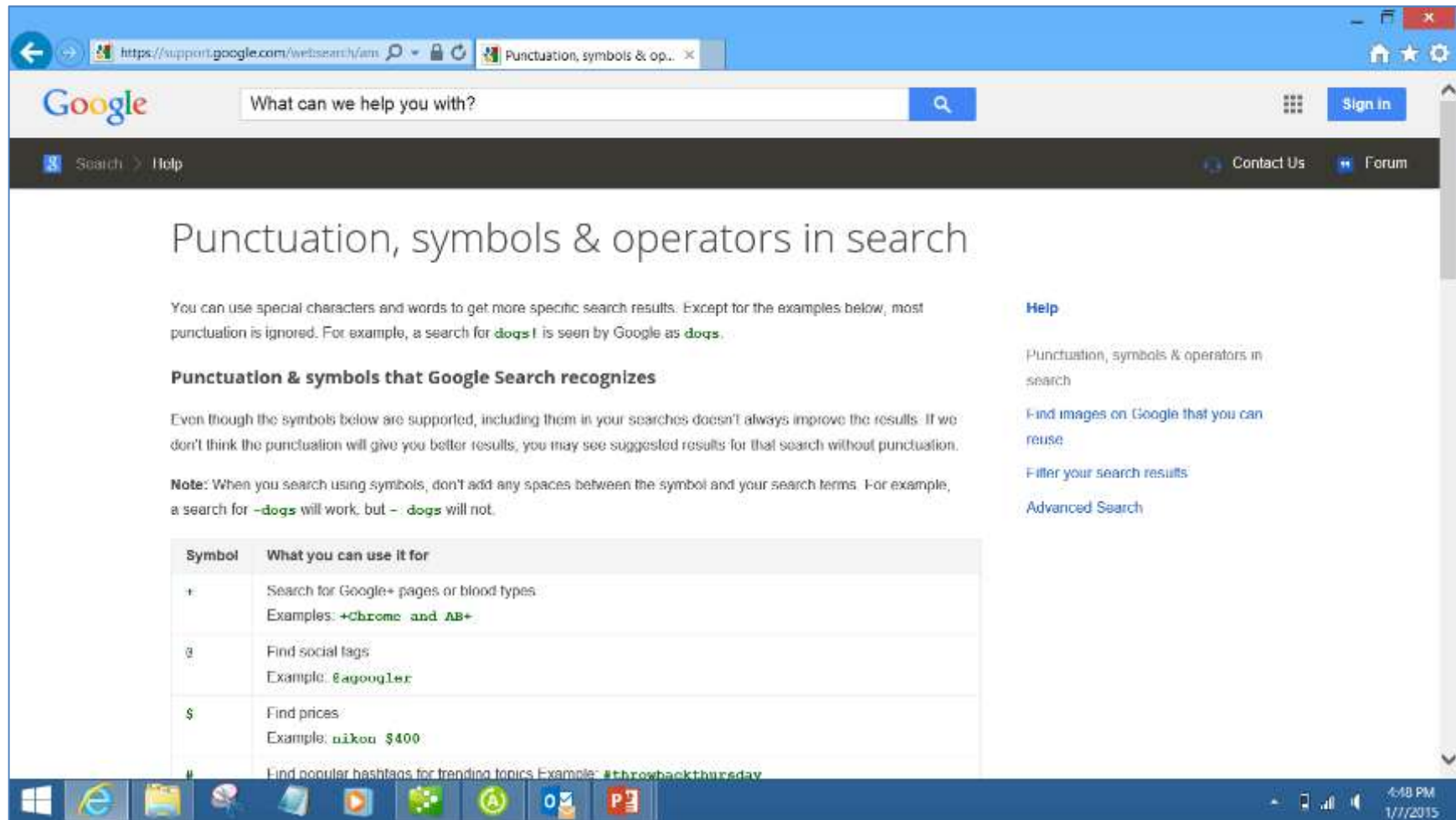
Want to learn cool and useful google hacks? Here is a [list of top](#) google hacks , that will teach you a lot new things about google!

#### How To Access Google Docs Without A Google Account

Posted on Feb 6th, 2013 - By Frank Taber - 0 Comments

Google Docs supplies us with a great amount of [free tools](#) that let us do [spreadsheets](#), create PowerPoint presentations or make projects. Another...

# Google Search Operators



The screenshot shows a web browser window with the Google Search Operators help page. The address bar shows the URL <https://support.google.com/websearch/answer/2466433?hl=en>. The page title is "Punctuation, symbols & operators in search". The main content explains that special characters can be used for more specific search results, with the example that a search for `dogs!` is seen by Google as `dogs`. It lists symbols that Google Search recognizes: `+` (Search for Google+ pages or blood types), `@` (Find social tags), `$` (Find prices), and `#` (Find popular hashtags for trending topics). A table summarizes these symbols and their uses. The right sidebar contains links for "Help", "Punctuation, symbols & operators in search", "Find images on Google that you can reuse", "Filter your search results", and "Advanced Search". The Windows taskbar is visible at the bottom.

**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: <code>+Chrome</code> and <code>AB+</code>
@	Find social tags Example: <code>@google</code>
\$	Find prices Example: <code>nikon \$400</code>
#	Find popular hashtags for trending topics Example: <code>#throwbackthursday</code>

[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

The screenshot shows the GoogleGuide website in a web browser. The page title is "GoogleGuide making searching even easier". The main heading is "Search Operators". A table lists search operators for various Google services. The left sidebar contains a search bar and a list of categories. The right sidebar features an advertisement for "Organic SEO Agency".

**Search Google Guide**

Search

**Google Guide by Category**

- Overview (2)
- Favorite Features (14)
- Part I: Query Input (19)
- Part II: Understanding Results (18)
- Part III: Search Tools (10)
- Part IV: Services (12)
- Part V: Developing a Website (8)
- Appendix (13)

**Part I: Query Input**

1. Entering a Query
2. Going Directly to the First Result
3. Selecting Search Terms
4. Interpreting Your Query
5. Crafting Your Query by using Special Characters
6. Quoted Phrases
7. Quotation Marks Replace the + Operator
8. The - Operator
9. The ~ Operator
10. The OR and | Operators
11. The .. Operator
12. The \* Operator
13. Special Characters: Summary
14. Advanced Search Form
15. Other Search Forms
16. Refining a Query
17. Anatomy of a Web Address
18. Using Search Operators
19. Search Operators

**Other Pages**

Table of Contents

**Search Operators**

The following table lists the search operators that work with each Google search service. Click on an operator to jump to its description — or, to read about all of the operators, simply scroll down and read all of this page.

Search Service	Search Operators
Web Search	<a href="#">allinanchor:</a> , <a href="#">allintext:</a> , <a href="#">allintitle:</a> , <a href="#">allinurl:</a> , <a href="#">cache:</a> , <a href="#">define:</a> , <a href="#">filetype:</a> , <a href="#">id:</a> , <a href="#">inanchor:</a> , <a href="#">info:</a> , <a href="#">intext:</a> , <a href="#">intitle:</a> , <a href="#">inurl:</a> , <a href="#">link:</a> , <a href="#">related:</a> , <a href="#">site:</a>
Image Search	<a href="#">allintitle:</a> , <a href="#">allinurl:</a> , <a href="#">filetype:</a> , <a href="#">inurl:</a> , <a href="#">intitle:</a> , <a href="#">site:</a>
Groups	<a href="#">allintext:</a> , <a href="#">allintitle:</a> , <a href="#">author:</a> , <a href="#">group:</a> , <a href="#">insubject:</a> , <a href="#">intext:</a> , <a href="#">intitle:</a>
Directory	<a href="#">allintext:</a> , <a href="#">allintitle:</a> , <a href="#">allinurl:</a> , <a href="#">ext:</a> , <a href="#">filetype:</a> , <a href="#">intext:</a> , <a href="#">intitle:</a> , <a href="#">inurl:</a>
News	<a href="#">allintext:</a> , <a href="#">allintitle:</a> , <a href="#">allinurl:</a> , <a href="#">intext:</a> , <a href="#">intitle:</a> , <a href="#">inurl:</a> , <a href="#">location:</a> , <a href="#">source:</a>
Product Search	<a href="#">allintext:</a> , <a href="#">allintitle:</a>

The following is an alphabetical list of the search operators. This list includes operators that are not officially supported by Google and not listed in [Google's online help](#).

**Note:** Google may change how undocumented operators work or may eliminate them completely.

Each entry typically includes the syntax, the capabilities, and an example. Some of the search operators won't work as intended if you put a

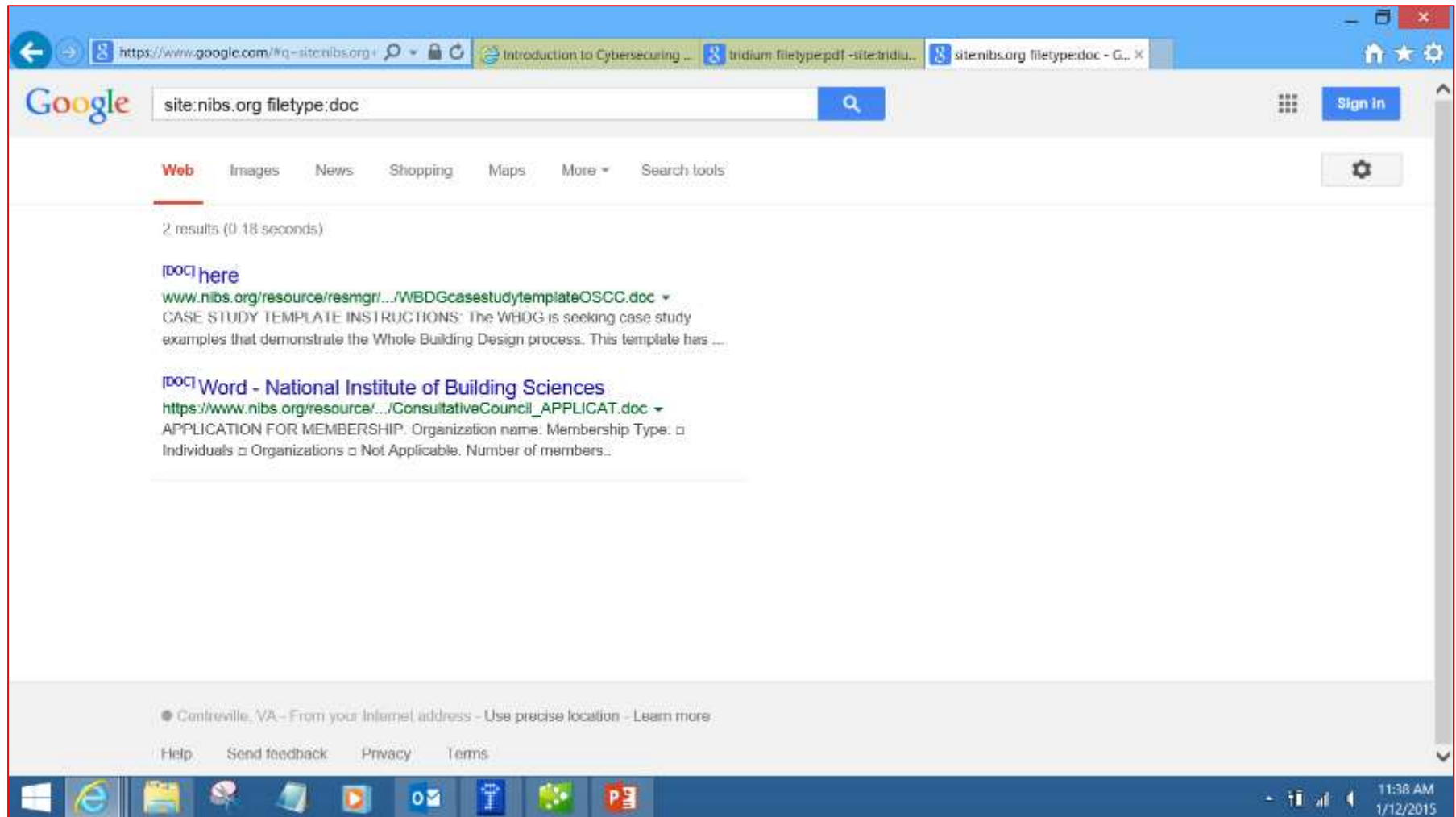
**Organic SEO Agency**

Traffic is great. Leads are better. Our SEO services bring new clients.

4:50 PM 1/1/2015

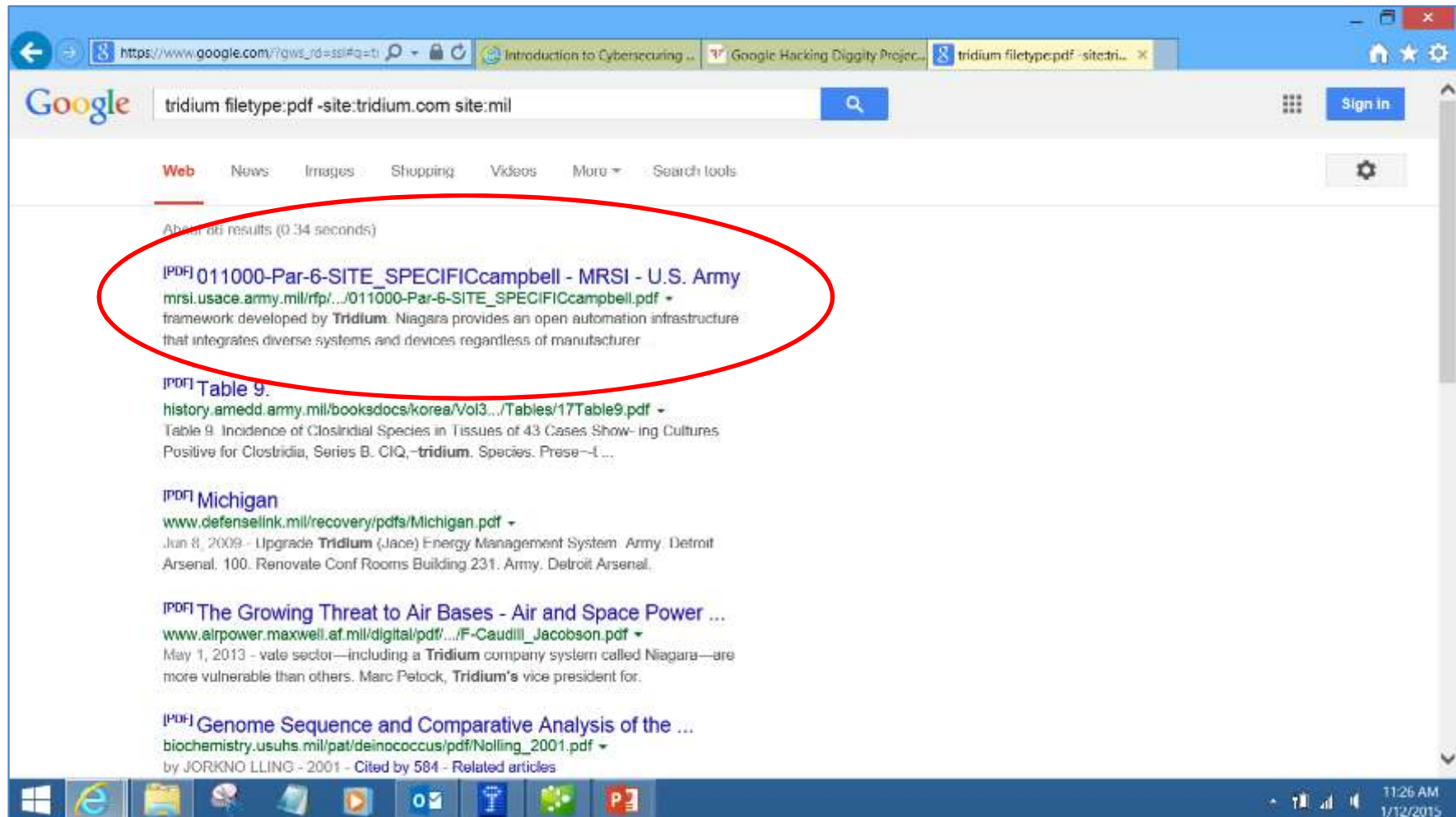
[http://www.googleguide.com/advanced\\_operators\\_reference.html](http://www.googleguide.com/advanced_operators_reference.html)

# Google Hacking



site:nibs.org filetype:doc

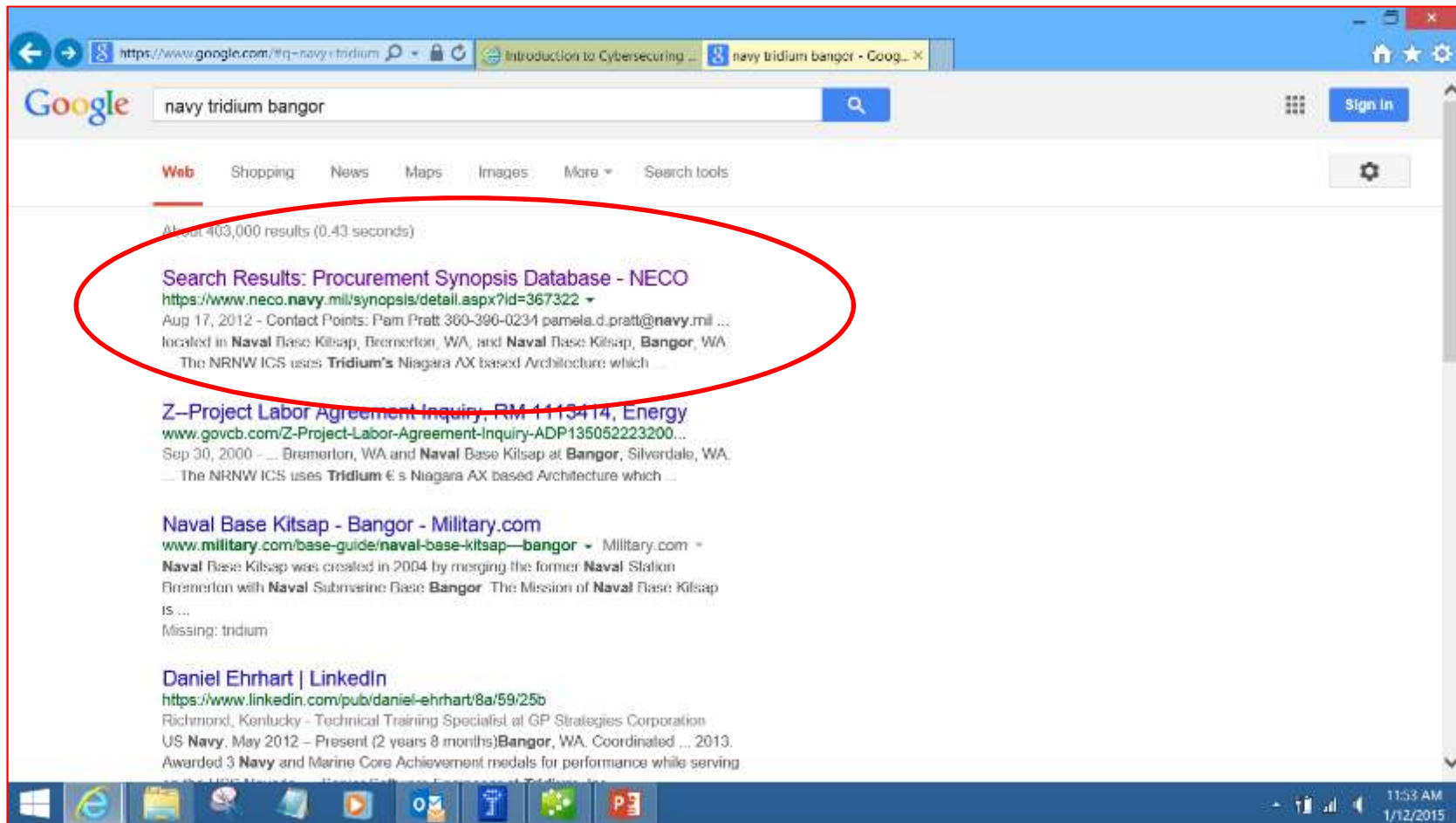
# Google Hacking



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



# Google Hacking



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



# Google Hacking

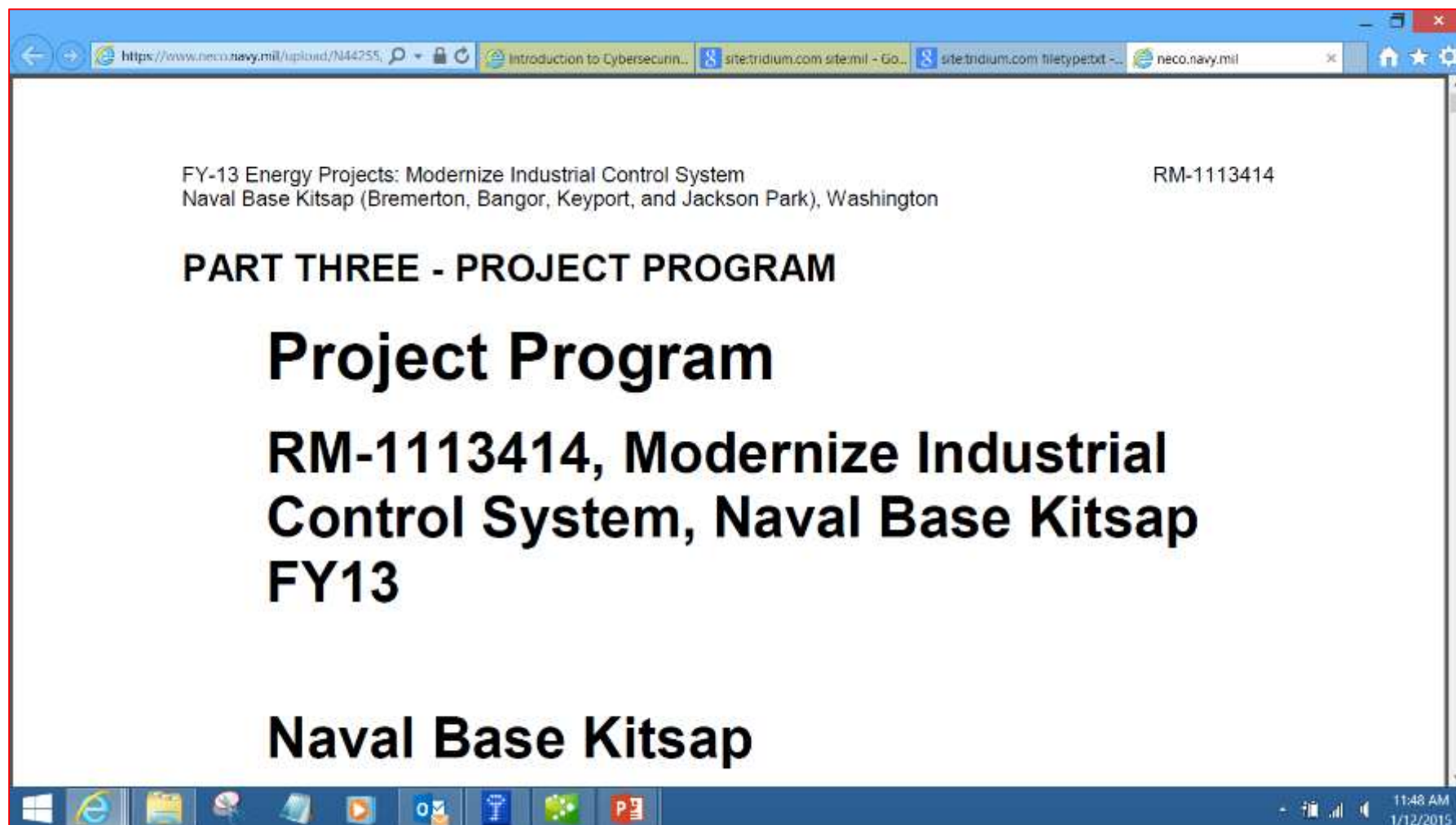
**NECO Synopsis Database**

**SOURCES SOUGHT NOTICE**

<b>Subject:</b>	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.
<b>Synopsis Date:</b>	Aug 14, 2012
<b>Contracting Office Address:</b>	N44255 NAVFAC NORTHWEST 1101 Tautog Circle Silverdale, WA
<b>NAICS Code:</b>	238210 Electrical Contractors and Other Wiring Installation Contractors
<b>Classification Code:</b>	Z - Maintenance, Repair or Alteration of Real Property
<b>Solicitation Number:</b>	N4425513MKTG1
<b>Response Date:</b>	Aug 28, 2012
<b>Archive Date:</b>	Sep 12, 2012
<b>Contact Points:</b>	Pam Pratt 360-396-0234 pamel.a.d.pratt@navy.mil
<b>Description:</b>	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

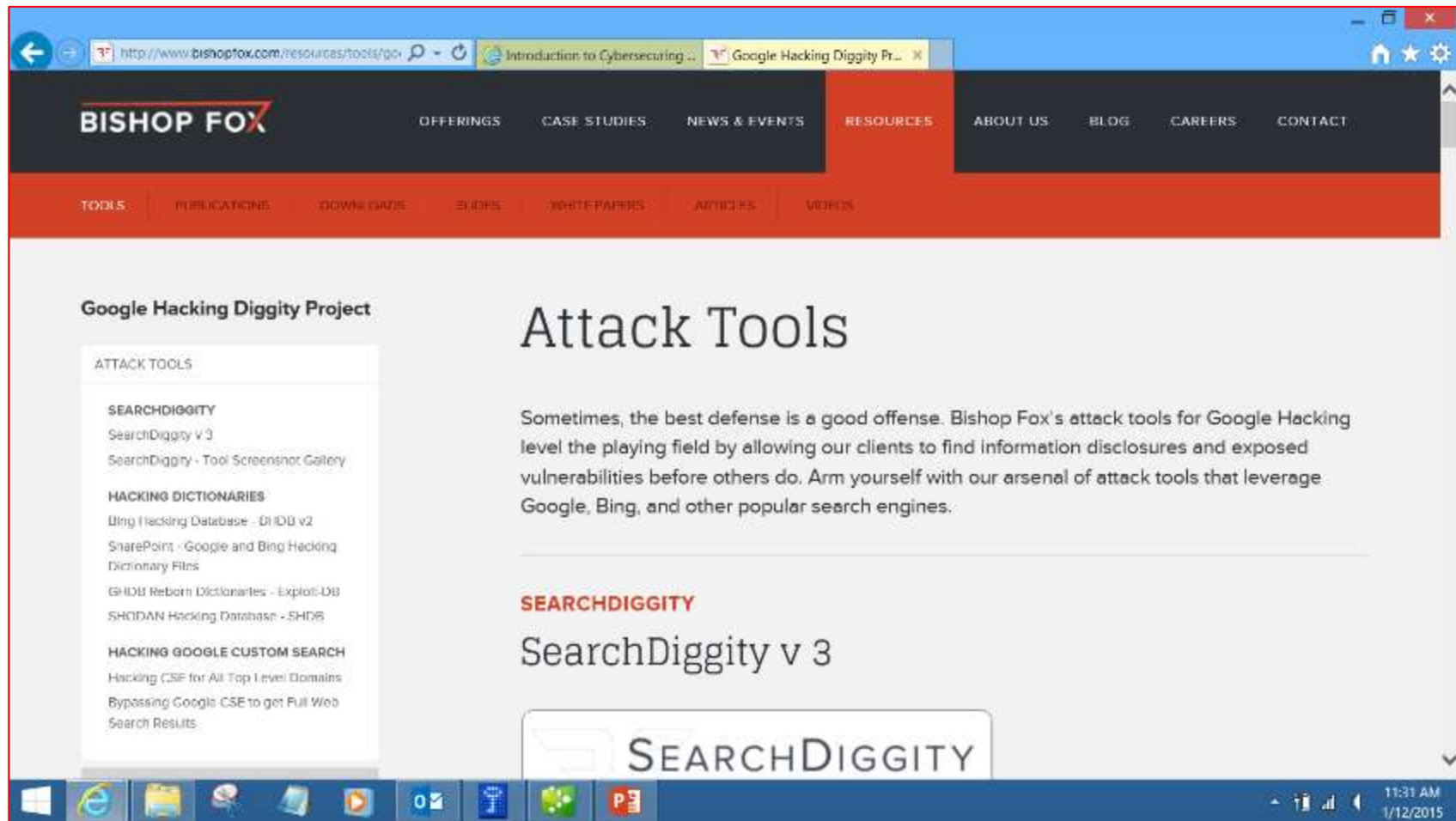
<https://www.neco.navy.mil/synopsis/detail.aspx?id=367322>

# Google Hacking



[https://www.neco.navy.mil/upload/N44255/N4425513R40020005N4425513R40020005N44255-13-R-4002\\_Part\\_3\\_Draft.pdf](https://www.neco.navy.mil/upload/N44255/N4425513R40020005N4425513R40020005N44255-13-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

The screenshot displays the Google Hacking Diggity Project web interface. At the top, a navigation bar includes links for Google, CodeSearch, Bing, LinkFromDomain, DLP, Flash, Malware, PortScan, NotInMyBackyard, BingMalware, and Shodan. The Shodan link is highlighted with a red box. Below this, the interface is divided into two main sections: Simple and Advanced. The Simple section is active, showing a Query Appender and a list of Queries. The Queries list includes various categories like Default Credentials, FTP, Printer, Router, SCADA, and Siemens s7. The SCADA category is expanded, showing sub-items like Electro Industries Gaug, Photovoltaic, Rockwell SLC-505 PLC, SCADA USA, and SCADA. The SCADA sub-item is selected. The Advanced section is also visible, showing a SCAN button, a Settings button, and an API Key field. The API Key field is highlighted with a red box, and a red callout bubble points to it with the text "Enter SHODAN API key". Below the API Key field, there is a table of search results. The table has columns for Category, Search String, URL, Hostnames, City, and Country. The results are filtered for SCADA systems. The third row is highlighted in yellow, showing a SCADA system with the URL http://70.168.40.243/. A red callout bubble points to this row with the text "Finding SCADA systems via SHODAN Diggity". Below the table, there is an Output section with a Selected Result button. The Selected Result button is active, showing the details of the selected SCADA system: 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.

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

Simple Advanced

Query Appender

Queries

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

SCAN Settings

API Key: Create  ☒ Hide

Cancel

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.kl	Lancaster	United States
SCADA	Niagara Web Server	http://184.187.11.158/		Omaha	United States

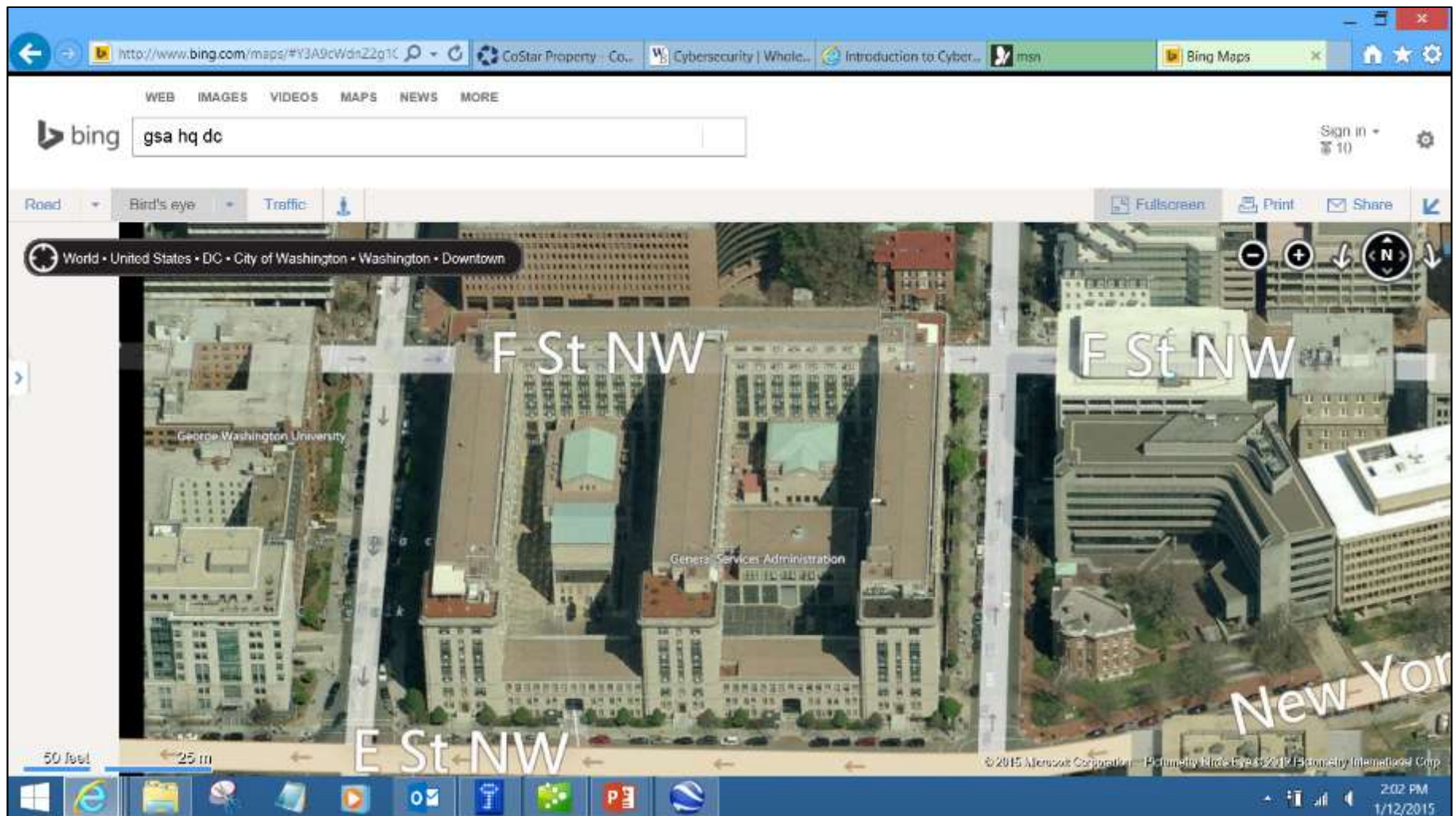
Output Selected Result

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

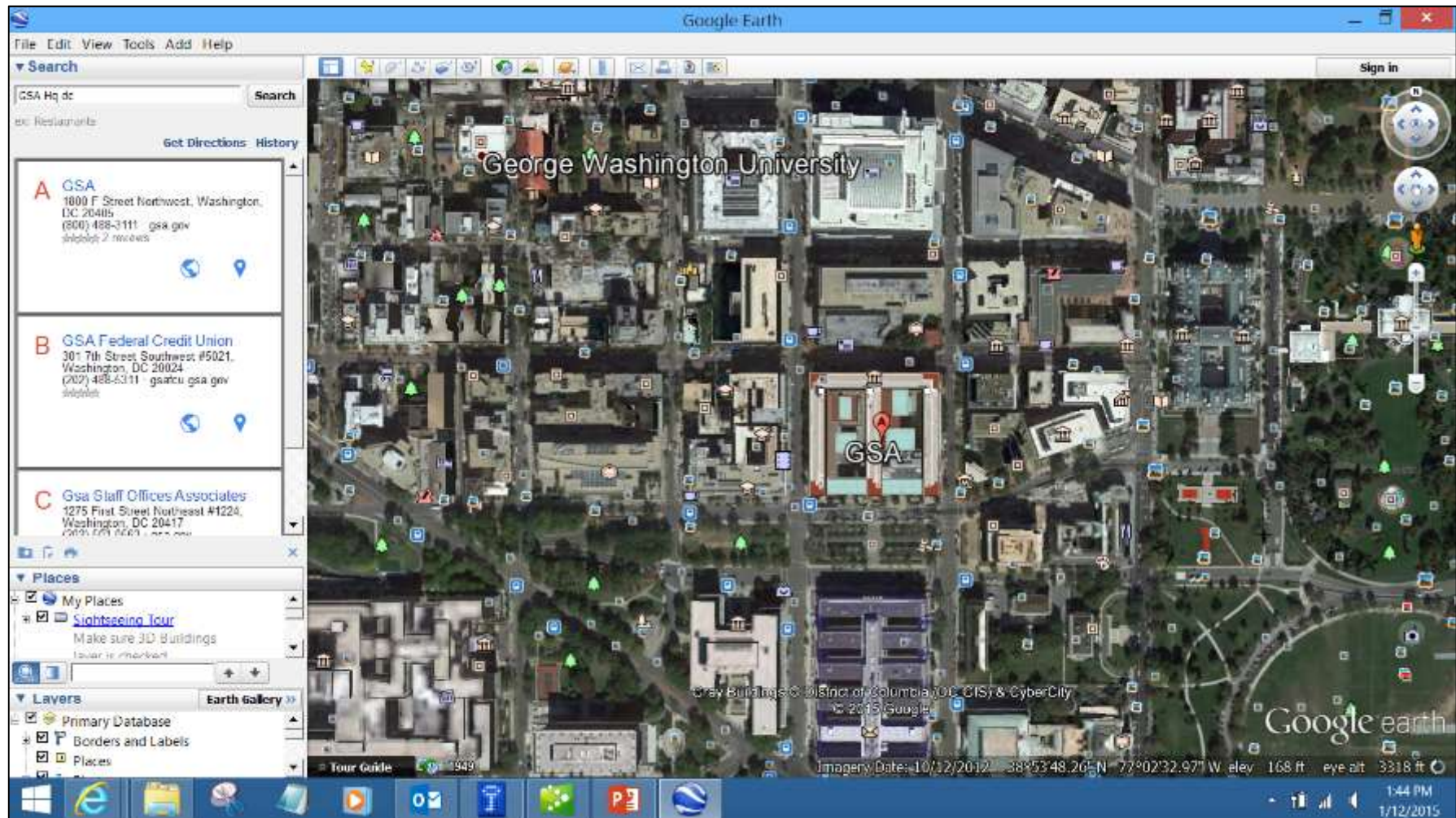
Finding SCADA systems via SHODAN Diggity



# BING



# Google Earth





# IPLocation

The screenshot shows the IPLocation website interface. At the top, there's a navigation bar with links: Home, Find My IP, Hide My IP, Change My IP, Domain Tools, and Forums. The main content area is titled "How to find geolocation of an IP Address?" and features a "REVERSE PHONE LOOKUP" section with a search input field and a "Query" button. Below this, it displays "Your IP Address is 173.73.169.42." and "IP Location Finder". A table of geolocation data is shown, with columns for IP Address, Country, Region, City, and ISP. The table contains one row of data. To the right, there's a sidebar with "IP ARTICLES" and a Dell advertisement for Windows Server 2012 migration.

**IP LOCATION** Project Mgmt Software  
Try it Free for 30 Days- Start Now! Automate Business Processes &

Home Find My IP Hide My IP Change My IP Domain Tools Forums

### How to find geolocation of an IP Address?

+1/80 Recommend this on Google

## REVERSE PHONE LOOKUP

ENTER PHONE NUMBER AND SEARCH FOR OWNER INFORMATION

Your IP Address is **173.73.169.42.**

IP Location Finder

IP Address:

Here are the results from a few Geolocation providers. Accuracy of geolocation data may vary from a provider to provider. Test drive yourself, and decide on the provider that you like.

Do you have a problem with IP location lookup? [Report a problem.](#)

Geolocation data from **IP2Location** (Product: DB4 updated on 11/30/2014)

IP Address	Country	Region	City	ISP
173.73.169.42	United States	California	San Francisco	Verizon

### IP ARTICLES

- What is an IP Address?
- What is a Subnet Mask?
- What is MAC address?
- What is TCP/IP?
- What is DHCP?
- What is Ipconfig utility?
- What is IP Spoofing?
- Find IP address of a network printer?
- Find IP addresses of a private network
- What is IPv6 Addresses?

**DELL**

Migrate from Windows Server 2003 with Dell Solutions.

[Learn More >](#)

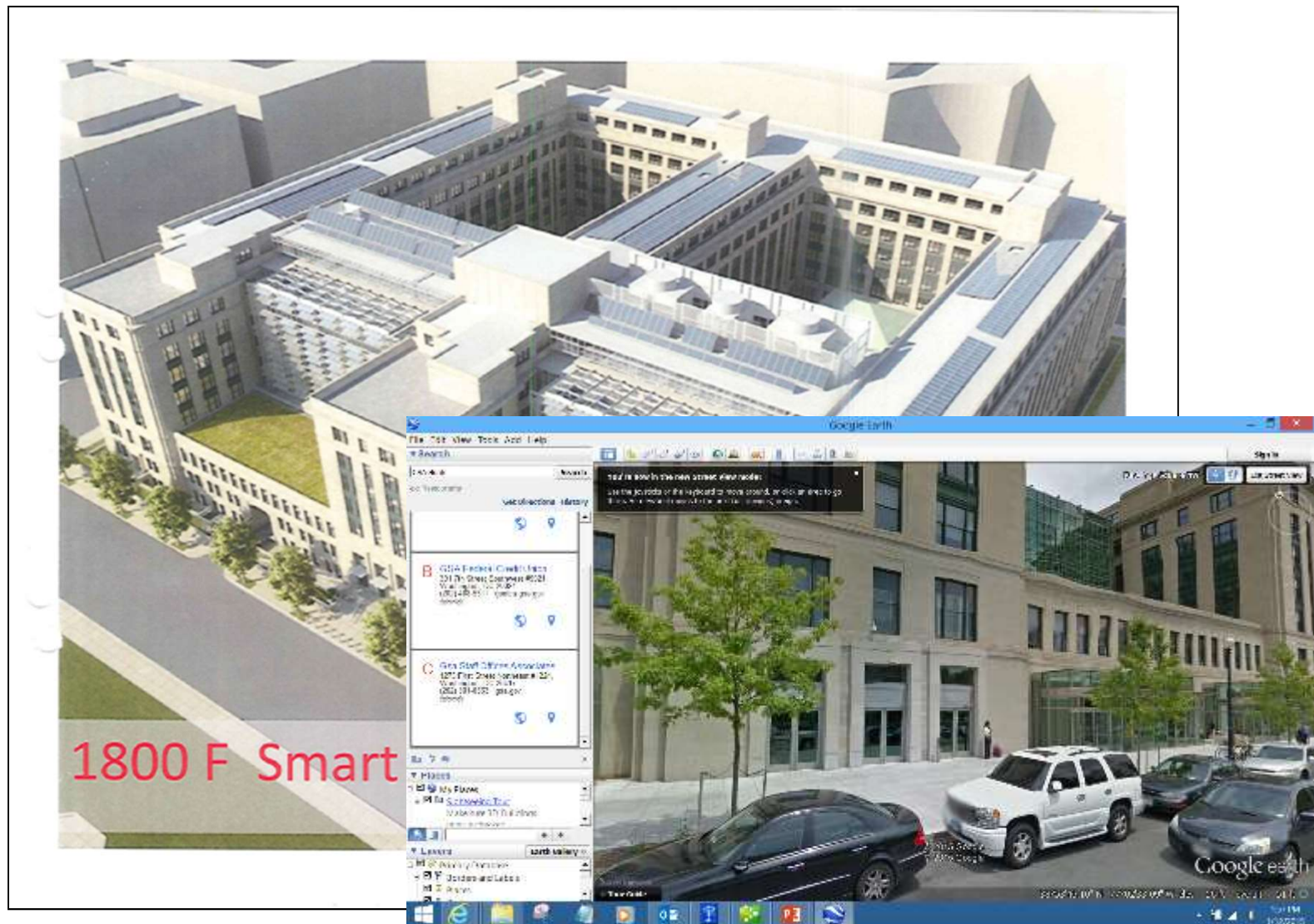
**Windows Server 2012**

\*Roll over for legal.

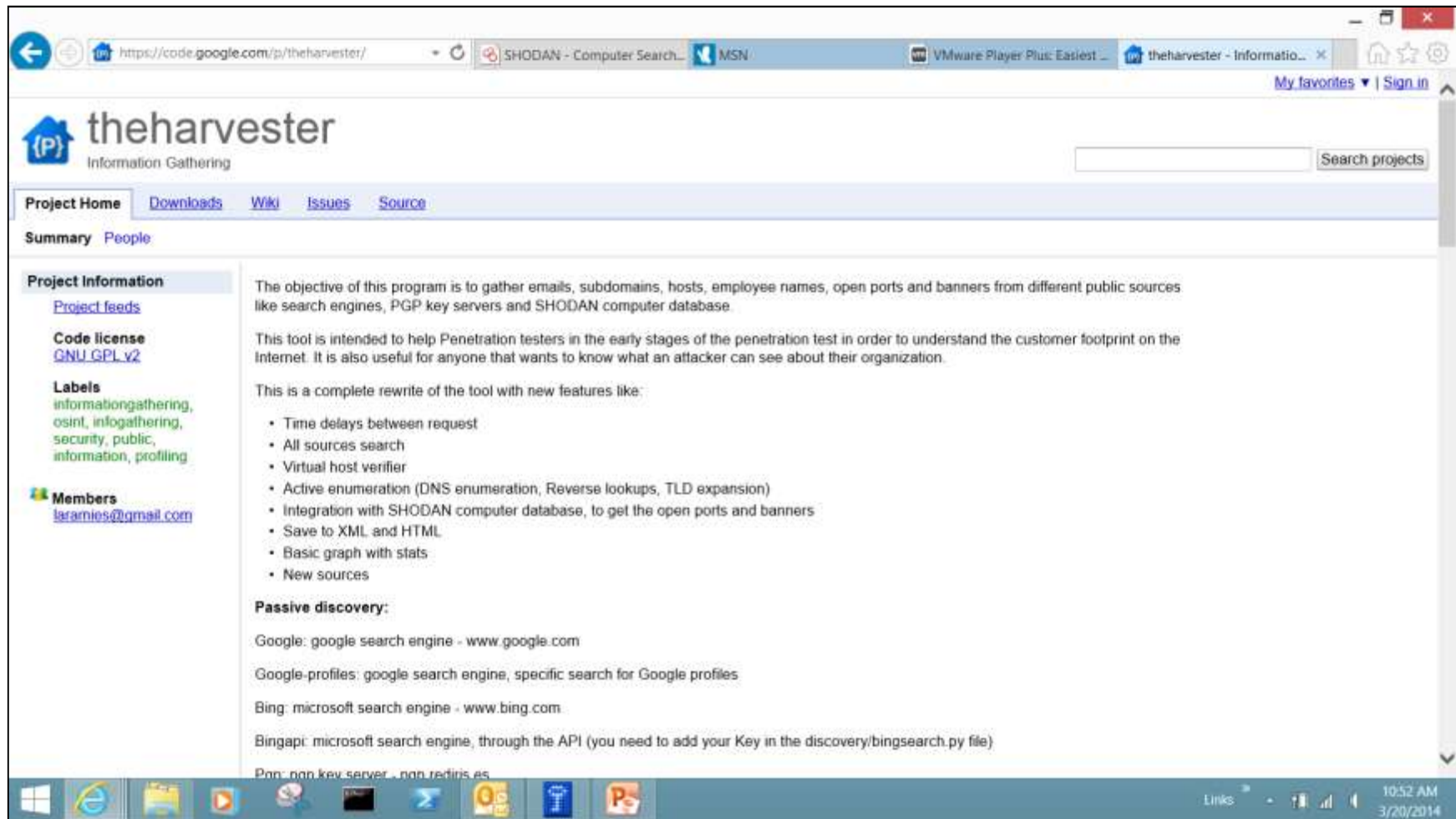
12:29 PM 1/18/2015

<http://www.iplocation.net/>

# GSA Smart Buildings Sources Sought



# Google Code The Harvester



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



# Recon-NG

The screenshot shows a web browser window displaying the article "The Recon-ng Framework : Automated Information Gathering" on the Infosec Institute website. The browser's address bar shows the URL <http://resources.infosecinstitute.com/the-recon-ng>. The website's navigation bar includes links for Home, Contributors, Articles, Mini Courses, Downloads, Courses, Schedule, and About. The main content area features a sidebar with "Download & Resources" (newsletter sign-up), "View our FREE mini-courses!" (SIGN UP NOW), and "Discounted Boot Camps" (SIGN UP NOW). The article text discusses the Metasploit Framework Project and the Social Engineer Toolkit (SET), highlighting the Recon-ng Framework as a new tool for automated information gathering. Social media sharing buttons for LinkedIn, Google+, Twitter, and Facebook are visible. The right sidebar contains "Related Mini Courses" (View All Mini Courses, Full Length Online Courses) and "Related Boot Camps" (INFOSEC Information Security, INFOSEC Information Assurance). The Windows taskbar at the bottom shows the time as 11:02 AM on 3/20/2014.

INFOSEC INSTITUTE

Home Contributors Articles Mini Courses Downloads Courses Schedule About

Download & Resources  
Sign up for our newsletter to get the latest updates.

View our FREE mini-courses!

Discounted Boot Camps

The Recon-ng Framework : Automated Information Gathering

72 26 71 152

The Metasploit Framework Project and the Social Engineer Toolkit (SET) are two great and known frameworks used by penetration testers and security researchers for automation wherein the former is used for automated exploitation of known vulnerabilities while the latter is used for penetration testing by hacking a user with the use of social engineering. These are very helpful tools indeed! For security enthusiasts out there, I have good news for you because there is another tool that has been unleashed just recently with a new purpose! Let me present to you the new 'Recon-ng Framework'!

Related Mini Courses  
[View All Mini Courses](#)  
[Full Length Online Courses](#)

Related Boot Camps  
[INFOSEC Information Security](#)  
[INFOSEC Information Assurance](#)

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

# Exploit Database



The screenshot shows the homepage of the Exploit Database. The browser's address bar displays <https://www.exploit-db.com/>. The website features a navigation menu with links to Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. The main heading is "Offensive Security Exploit Database Archive" with a count of "33878 Exploits Archived". Below this, a banner for "The Exploit Database" describes it as a CVE compliant archive of exploits and vulnerable software, with a button to "Download the Exploit Database Archive". The banner also includes the text "CVE Compliant" and the CVE logo. A section titled "Remote Exploits" is visible, with a description: "This exploit category includes exploits for remote services or applications, including client side exploits." The bottom of the page shows a Windows taskbar with various application icons and a system clock indicating 3:35 PM on 7/9/2015.

**EXPLOIT DATABASE**

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Offensive Security Exploit Database Archive **33878**  
Exploits Archived

The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn [about the Exploit Database](#).

**The Exploit Database**

The Exploit Database (EDB) is a CVE compliant archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our goal is to collect exploits from various sources and concentrate them in one, easy to navigate database

[Download the Exploit Database Archive](#)

**EXPLOIT DATABASE**

**CVE Compliant** 

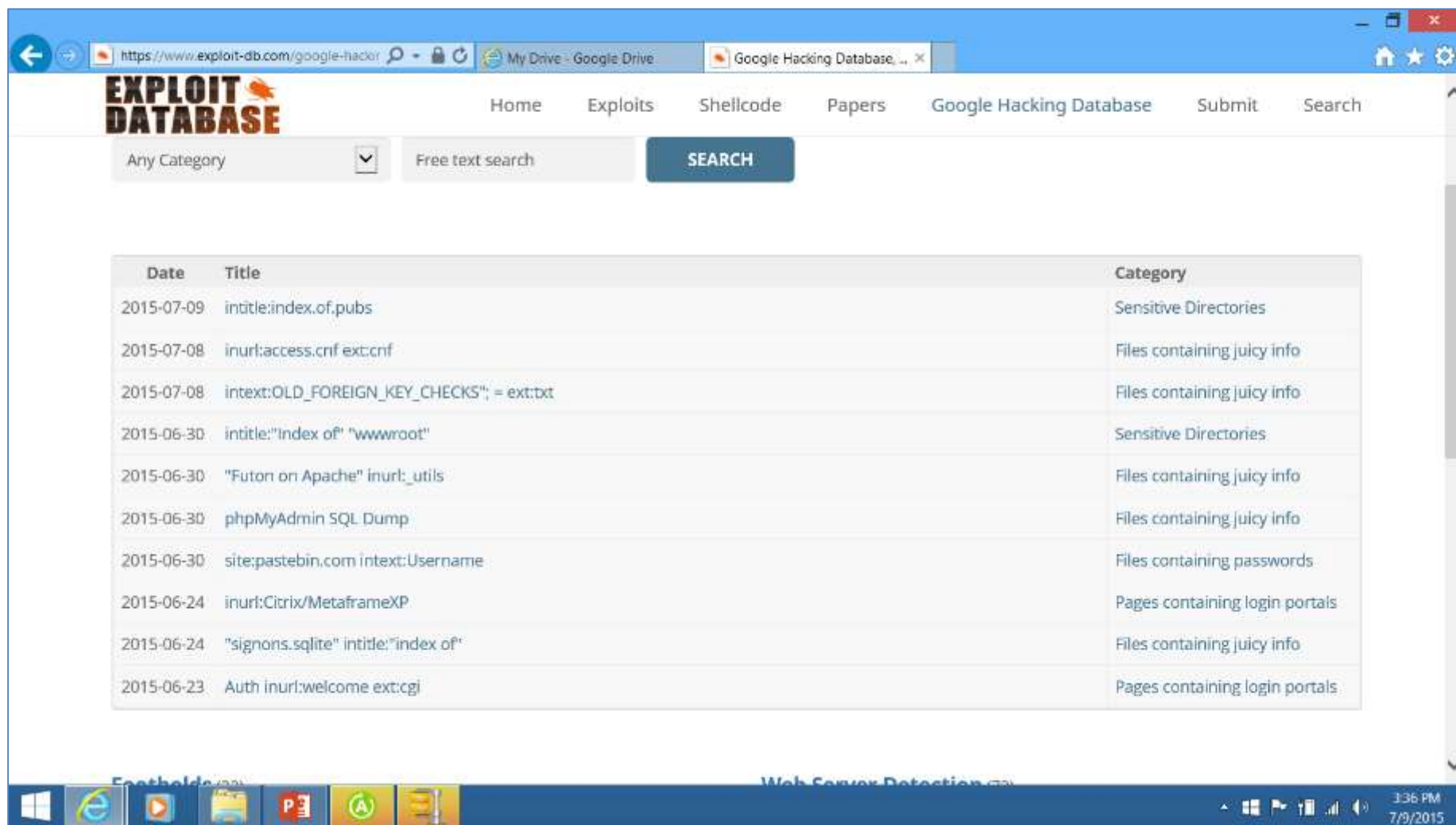
**Remote Exploits**

This exploit category includes exploits for remote services or applications, including client side exploits.

Windows taskbar: 3:35 PM 7/9/2015

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

# Exploit DB Categories



The screenshot shows the Exploit DB website interface. The browser address bar displays the URL <https://www.exploit-db.com/google-hacker>. The website header includes the "EXPLOIT DATABASE" logo and navigation links: Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. Below the header, there is a search bar with a dropdown menu set to "Any Category", a text input field containing "Free text search", and a "SEARCH" button. The search results are displayed in a table with three columns: Date, Title, and Category.

Date	Title	Category
2015-07-09	intitle:index.of,pubs	Sensitive Directories
2015-07-08	inurl:access.cnf ext:cnf	Files containing juicy info
2015-07-08	intext:OLD_FOREIGN_KEY_CHECKS"; = ext:txt	Files containing juicy info
2015-06-30	intitle:"index of" "wwwroot"	Sensitive Directories
2015-06-30	"Futon on Apache" inurl:_utils	Files containing juicy info
2015-06-30	phpMyAdmin SQL Dump	Files containing juicy info
2015-06-30	site:pastebin.com intext:Username	Files containing passwords
2015-06-24	inurl:Citrix/MetaframeXP	Pages containing login portals
2015-06-24	"signons.sqlite" intitle:"index of"	Files containing juicy info
2015-06-23	Auth inurl:welcome ext:cgi	Pages containing login portals

The Windows taskbar at the bottom shows the Start button, Internet Explorer, and several other application icons. The system clock in the bottom right corner indicates the time is 3:36 PM on 7/9/2015.



# Exploit DB Search

The screenshot shows the Exploit Database website interface. The browser's address bar displays the URL `https://www.exploit-db.com/google-hacker`. The website's navigation bar includes links for Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. Below the navigation bar, there is a search section with a dropdown menu set to 'Any Category', a text input field containing 'Free text search', and a blue 'SEARCH' button. The search results are displayed in a table with three columns: Date, Title, and Summary. The table shows five results, with the first result being the most recent. The results are as follows:

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

At the bottom of the page, there is a Windows taskbar with various application icons and a system clock showing 3:38 PM on 7/9/2015.

# Exploit DB Search - Honeywell

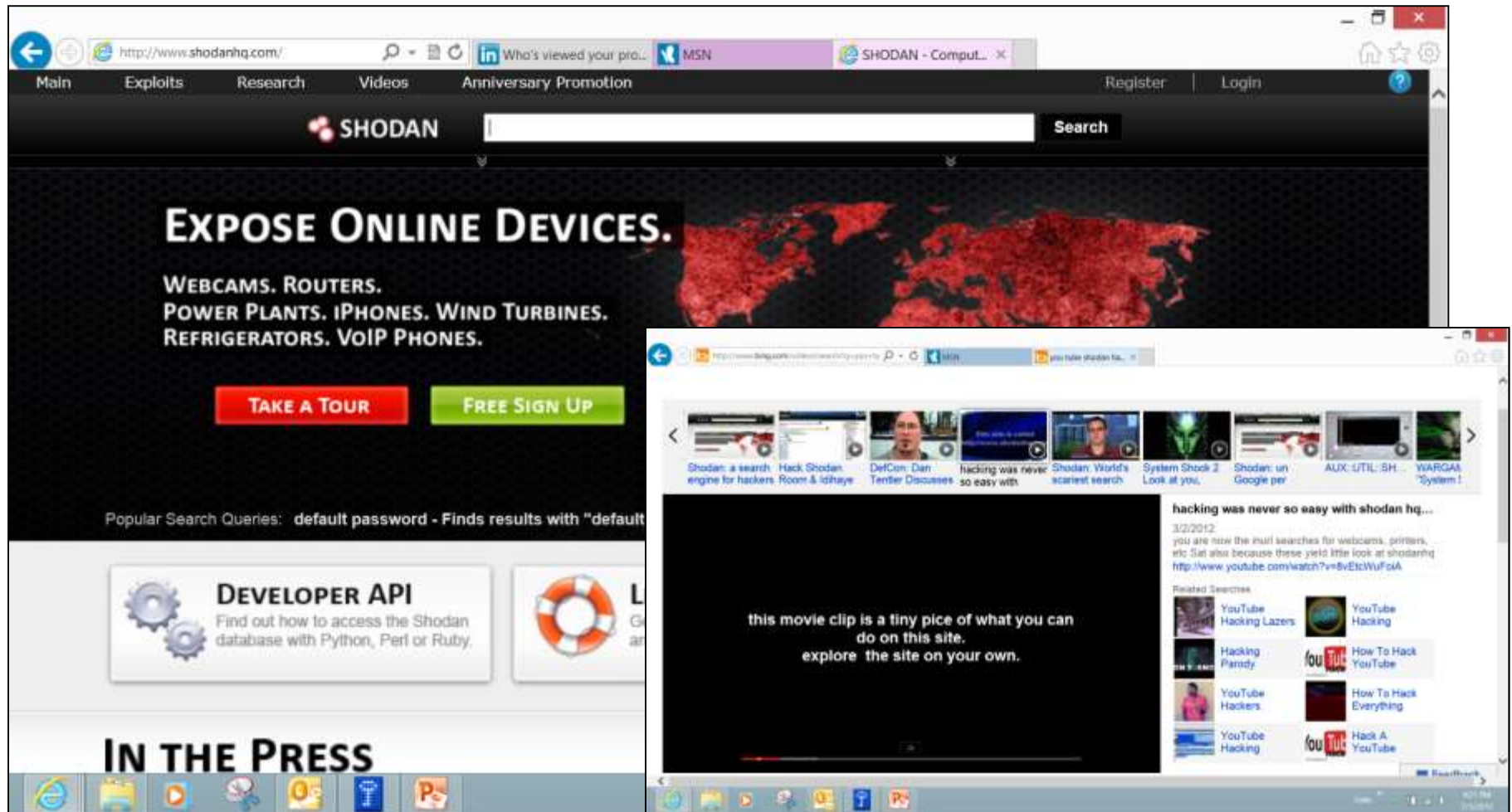
The screenshot shows a web browser window with the URL <https://www.exploit-db.com/search/?action=results>. The page title is "Search the Exploit Database". Below the title, there is a search bar with the text "honeywell" and a "SEARCH" button. To the right of the search bar, there is a link for "Advanced search".

The search results are displayed in a table with the following columns: Date, D, A, V, Title, Platform, and Author. The table contains three rows of results:

Date	D	A	V	Title	Platform	Author
2013-03-13	↓	-	✓	Honeywell HSC Remote Deployer ActiveX Remote Code Execution	windows	metasploit
2013-01-10	↓	-	✓	Honeywell Tema Remote Installer ActiveX Remote Code Execution	windows	metasploit
2006-10-02	↓	-	✓	[ezine] h0no 3		h0no

The Windows taskbar at the bottom shows the time as 3:42 PM on 7/9/2015.

# Shodan



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

# Tridium

The screenshot shows the Tridium website homepage within a web browser window. The browser's address bar displays `http://www.tridium.com/`. The website features a navigation bar with links for North America, EMEA, Asia, and Latin America. The main header includes the Tridium logo and the tagline "Connecting minds and machines". A large banner image shows a Boeing aircraft assembly line, with a text overlay stating: "Boeing, the world's largest manufacturer of commercial jetliners maintains its reputation as an innovative leader by implementing Yokun Energy in their Renton, Washington production facilities. Click to read the Case Study." Below the banner, a sidebar on the left lists various sections: Corporate Info, Products & Services, Markets & Applications, Tridium News, Library, Partner Channels, Purchase, Tridium University, Tridium Asia Pacific, and Tridium EMEA. The main content area is titled "Solutions For Connecting Devices to the Enterprise" and describes Tridium's role as a global leader in open platforms, application software frameworks, automation infrastructure technology, energy management and device-to-enterprise integration solutions. It highlights how their technology and applications have fundamentally changed the way devices and systems connect, integrate and interoperate with each other and the enterprise. A section titled "Tech Guides available" lists two guides: "Using a VPN with Niagara Systems" and "Niagara<sup>AX</sup> Hardening Guide". The bottom of the page shows a Windows taskbar with various application icons and a system clock indicating 10:39 AM on 3/20/2014.

Tridium  
Connecting minds and machines

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 Yokun Energy in their Renton, Washington production facilities.

Click to read the Case Study

Corporate Info  
Products & Services  
Markets & Applications  
Tridium News  
Library  
Partner Channels  
Purchase  
Tridium University  
Tridium Asia Pacific  
Tridium EMEA

## 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<sup>AX</sup> Hardening Guide

Links 10:39 AM 3/20/2014



# Tridium Products and Services

The screenshot displays the Tridium website's 'Products & Services' page. The browser's address bar shows the URL [http://www.tridium.com/cs/products/\\_services/tra](http://www.tridium.com/cs/products/_services/tra). The Tridium logo, with the tagline 'Connecting minds and machines', is in the top left. Navigation links for 'North America', 'EMEA', 'Asia', and 'Latin America' are in the top right. A large banner image with the text 'Products & Services' is below the header. On the left, a sidebar menu lists: 'Corporate Info', 'Products & Services' (expanded), 'Frameworks' (with sub-items: NiagaraAX, Niagara Framework and Energy, Niagara Enterprise Security, Niagara Appliance, JACE, ARRA), 'Markets & Applications', 'Tridium News', 'Library', 'Partner Channels', 'Purchase', 'Tridium University', 'Tridium Asia Pacific', 'Tridium EMEA', and 'Tridium Latin America'. The main content area features the heading 'What is a Software Framework?' followed by a paragraph: 'A software framework is a universal, reusable software platform used to develop applications, products and solutions. Software Frameworks include support programs, compilers, code libraries, an application programming interface (API) and tool sets that bring together all the different components to enable development of a project or solution.' Below this is another paragraph: 'Software Frameworks are designed to facilitate the development process by allowing designers and programmers to spend more time on meeting software requirements rather than dealing with the more tedious details of providing a working system. Software frameworks allow developers to spend less time coding, less time "developing" and debugging and more time on value-added development and concentrating on the business-specific problem at hand rather than on the plumbing code behind it resulting, faster time to market.' This is followed by a paragraph: 'Tridium's software frameworks are used to develop device-to-enterprise applications, Internet-enabled products and automation system solutions.' and a sub-heading 'Why Build It When You Can Build On It'. The section 'Software Frameworks from Tridium' includes 'Niagara<sup>AX</sup> Framework' and a logo for 'niagara<sup>AX</sup> Framework' with the text 'Powered by'. The Windows taskbar at the bottom shows the Start button and several application icons. The system clock in the bottom right corner indicates '10:40 AM 3/20/2014'.

TRIDIUM  
Connecting minds and machines

North America | EMEA | Asia | Latin America

## Products & Services

Corporate Info

Products & Services

- Frameworks
  - NiagaraAX
  - Niagara Framework and Energy
  - Niagara Enterprise Security
  - Niagara Appliance
  - JACE
  - ARRA
- Markets & Applications
- Tridium News
- Library
- Partner Channels
- Purchase
- Tridium University
- Tridium Asia Pacific
- Tridium EMEA
- Tridium Latin America

### What is a Software Framework?

A software framework is a universal, reusable software platform used to develop applications, products and solutions. Software Frameworks include support programs, compilers, code libraries, an application programming interface (API) and tool sets that bring together all the different components to enable development of a project or solution.

Software Frameworks are designed to facilitate the development process by allowing designers and programmers to spend more time on meeting software requirements rather than dealing with the more tedious details of providing a working system. Software frameworks allow developers to spend less time coding, less time "developing" and debugging and more time on value-added development and concentrating on the business-specific problem at hand rather than on the plumbing code behind it resulting, faster time to market.

Tridium's software frameworks are used to develop device-to-enterprise applications, Internet-enabled products and automation system solutions.

Why Build It When You Can Build On It

### Software Frameworks from Tridium

Niagara<sup>AX</sup> Framework

Powered by  
**niagara**<sup>AX</sup> FRAMEWORK

Windows taskbar: 10:40 AM 3/20/2014

# Shodan – Tridium Search

The screenshot shows the Shodan search results for the query 'tridium'. The browser address bar displays 'http://www.shodanhq.com/search?q=tridium'. The Shodan navigation bar includes links for Shodan, Exploits, Scanhub, Maps, Blog, and Anniversary Promotion. The search bar contains 'tridium' and a 'Search' button. The results are categorized into Services, Top Countries, and Top Organizations. The Services section lists NetBIOS (11), SNMP (9), SMB (3), HTTPS (1), and FTP (1). The Top Countries section lists United States (15), Norway (3), Malaysia (2), Turkey (1), and Italy (1). The Top Organizations section lists Telenor Norge AS (3), Techavenue Data Center... (2), tw telecom holdings (1), Wyoming.Com (1), and Wave Broadband (1). The main results list includes three entries: 97.78.98.252 (Time Warner Cable, Tampa), 116.6.58.158 (China Telecom Next Generation Carrier Network, Guangzhou), and 76.12.61.228 (HostMySite, Newark). A blue arrow points from the 'TRIDIUM-PC' server name in the first result to the login form on the right.

IP Address	Organization	Location	NetBIOS Response
97.78.98.252	Time Warner Cable	Tampa	Servername: TRIDIUM-PC MAC: 00:0a:3a:00:00:00
116.6.58.158	China Telecom Next Generation Carrier Network	Guangzhou	Servername: TRIDIUMFWS04 MAC: 00:50:b6:52:46:c3
76.12.61.228	HostMySite	Newark	Tridium station

The screenshot shows a login form titled 'VictorPark\_Super'. It features a yellow key icon, a 'Username:' field, a 'Password:' field, and a 'Login' button. The form is displayed in a browser window titled 'SHODAN - Computer Search E... 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

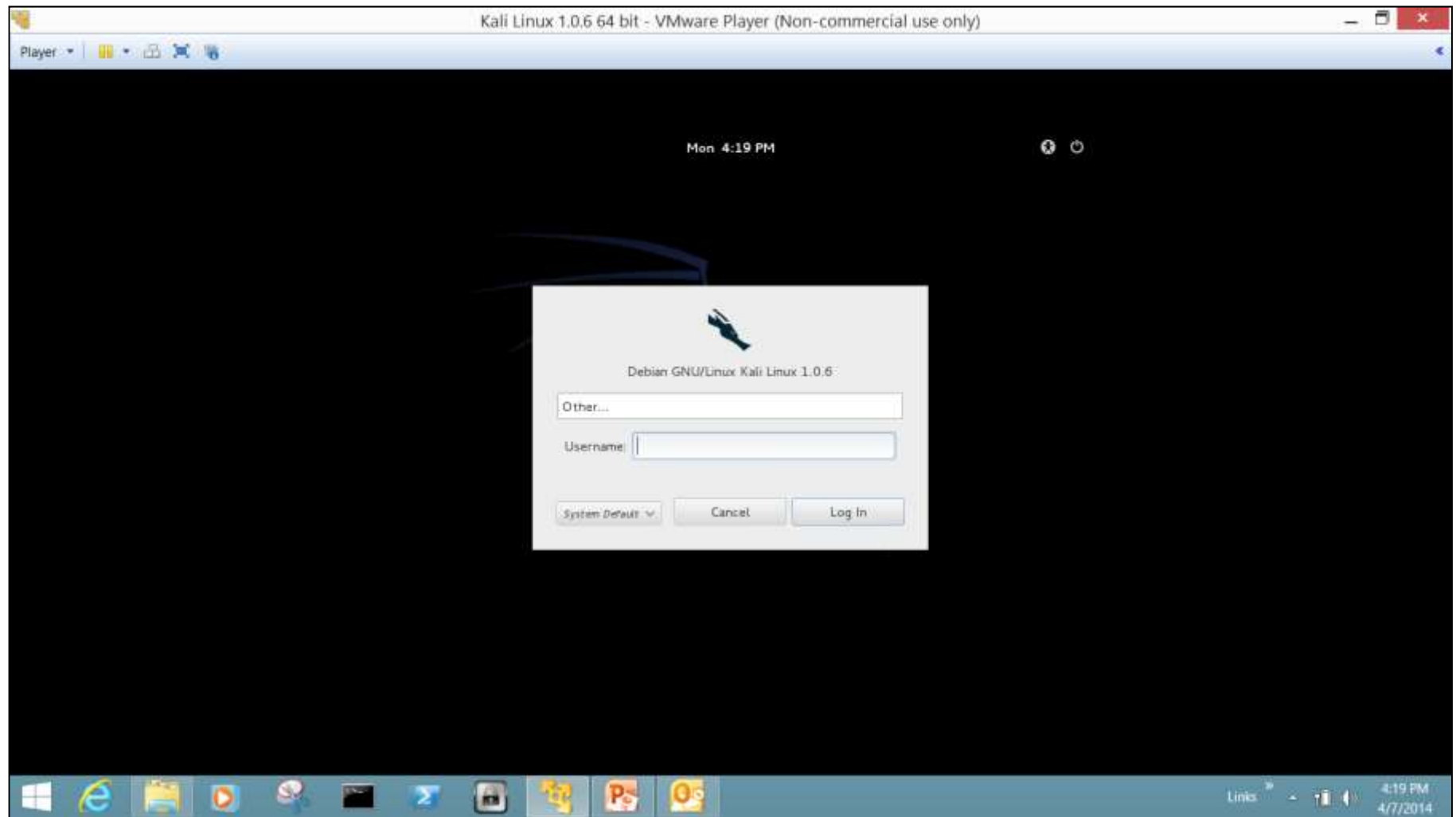
Server: **Niagara Web Server/3.0**

# Kali Linux



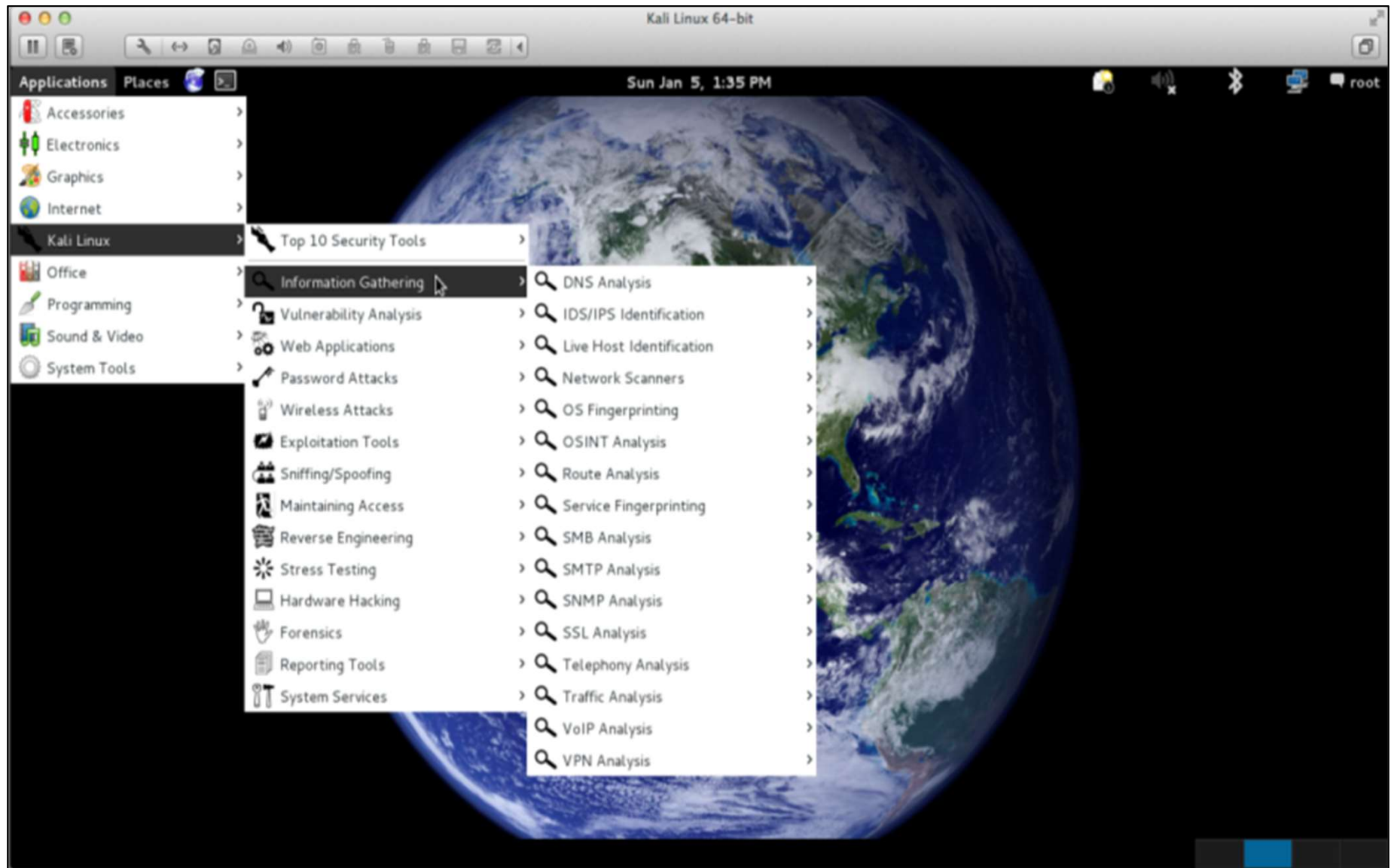
<http://www.kali.org/>

# Kali Linux Login



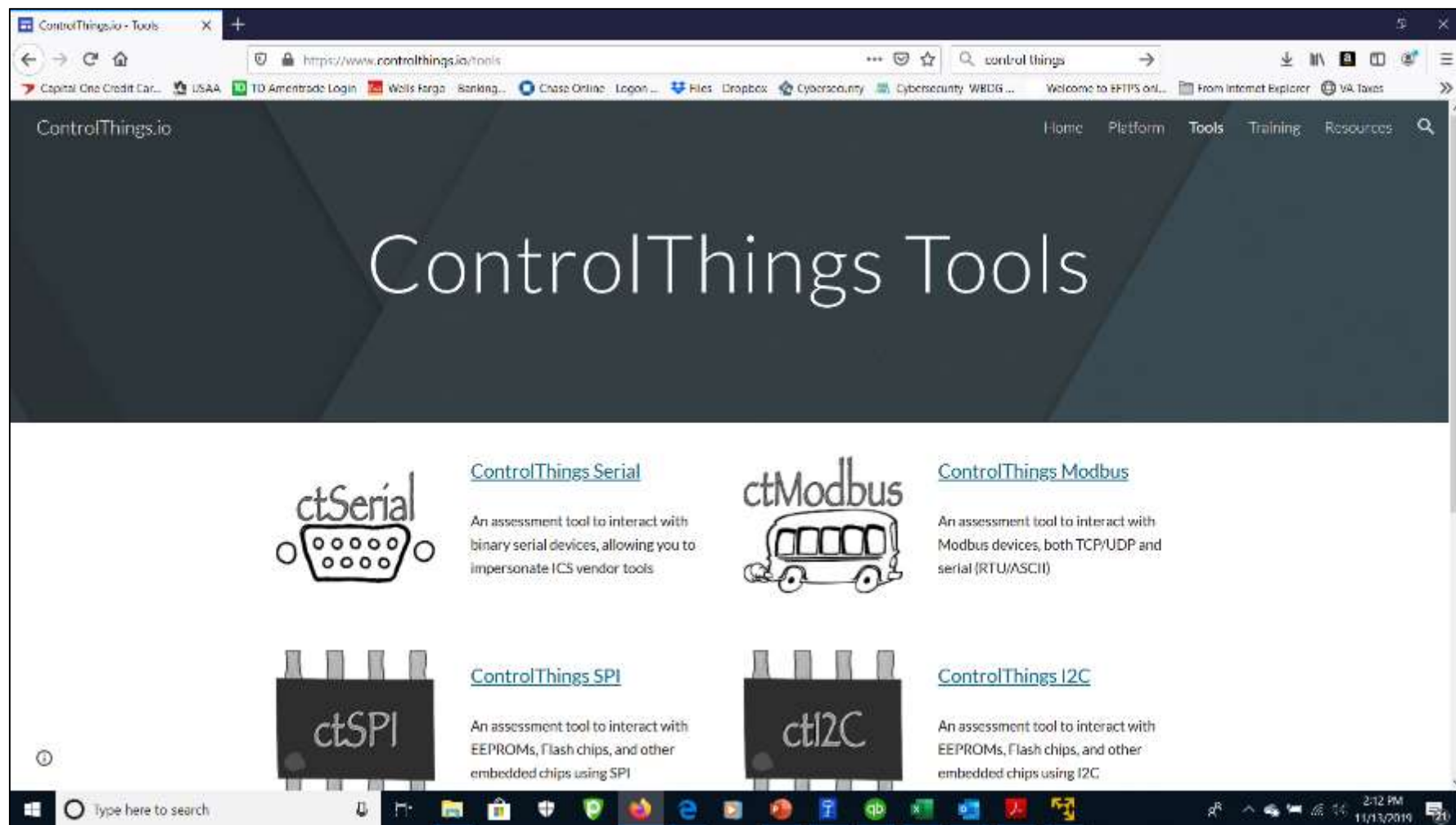
Bonus Section 2 illustrates using Kali to attack a control system

# Kali Dojo Menu





# Control Things I/O



<https://www.controlthings.io/tools>



# Control Things I/O


ControlThings.io - Training

https://www.controlthings.io/training

ControlThings.io

Home Platform Tools Training Resources


New to ICS? Start with this [YouTube Playlist](#) of videos to learn the basics of Industrial Control Systems, which is a great step to prepare yourself for our courses!



SANS ICS410: ICS/SCADA Security Essentials

Sections

- Day 1: ICS Overview



Assessing and Exploiting Control Systems

Sections

- Assessing and Exploiting Methodologies

Windows taskbar: 2:15 PM 11/13/2019

<https://www.controlthings.io/training>

# SamuraiSTFU Applications

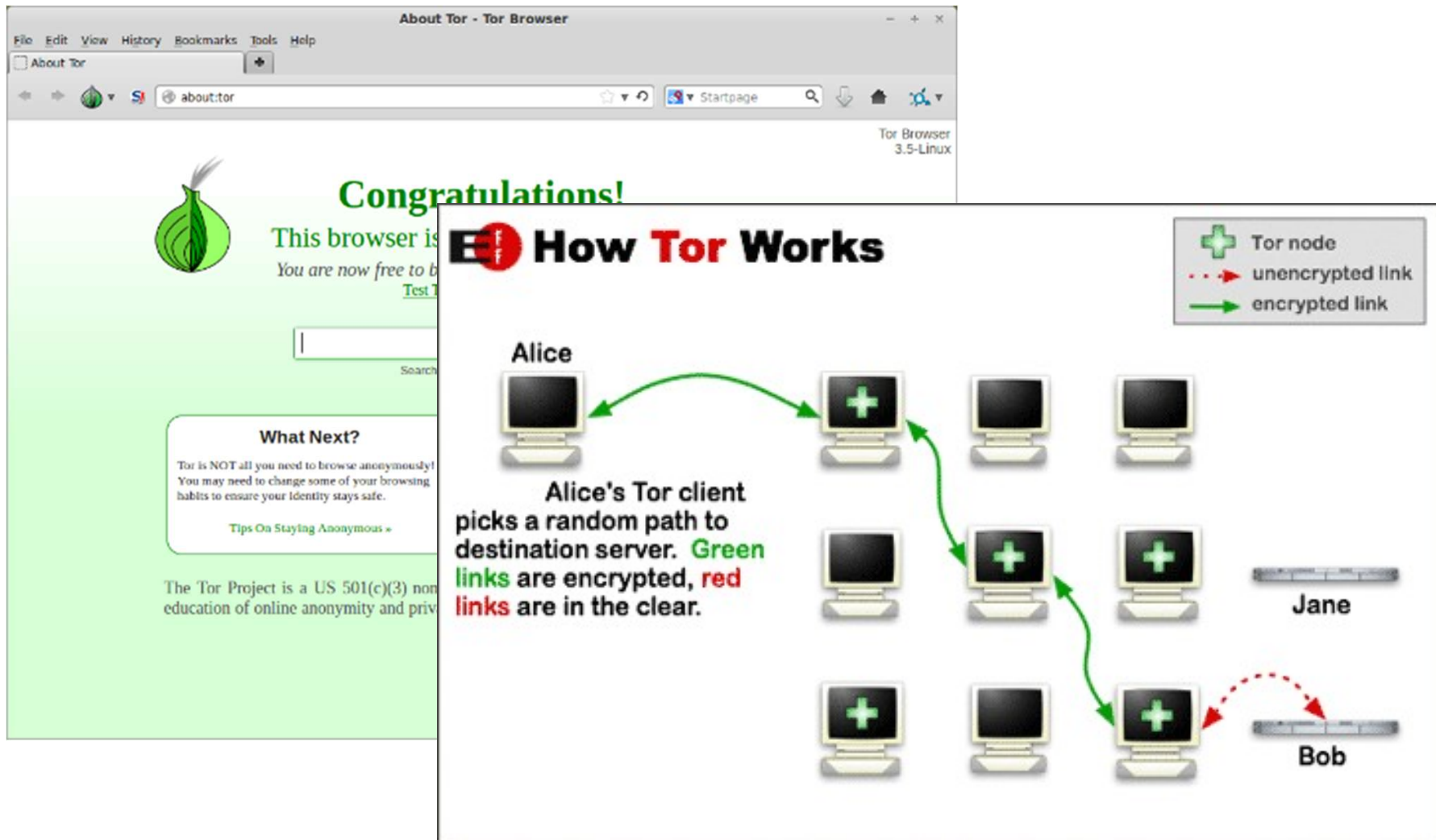


# SamuraiSTFU Applications User Interfaces



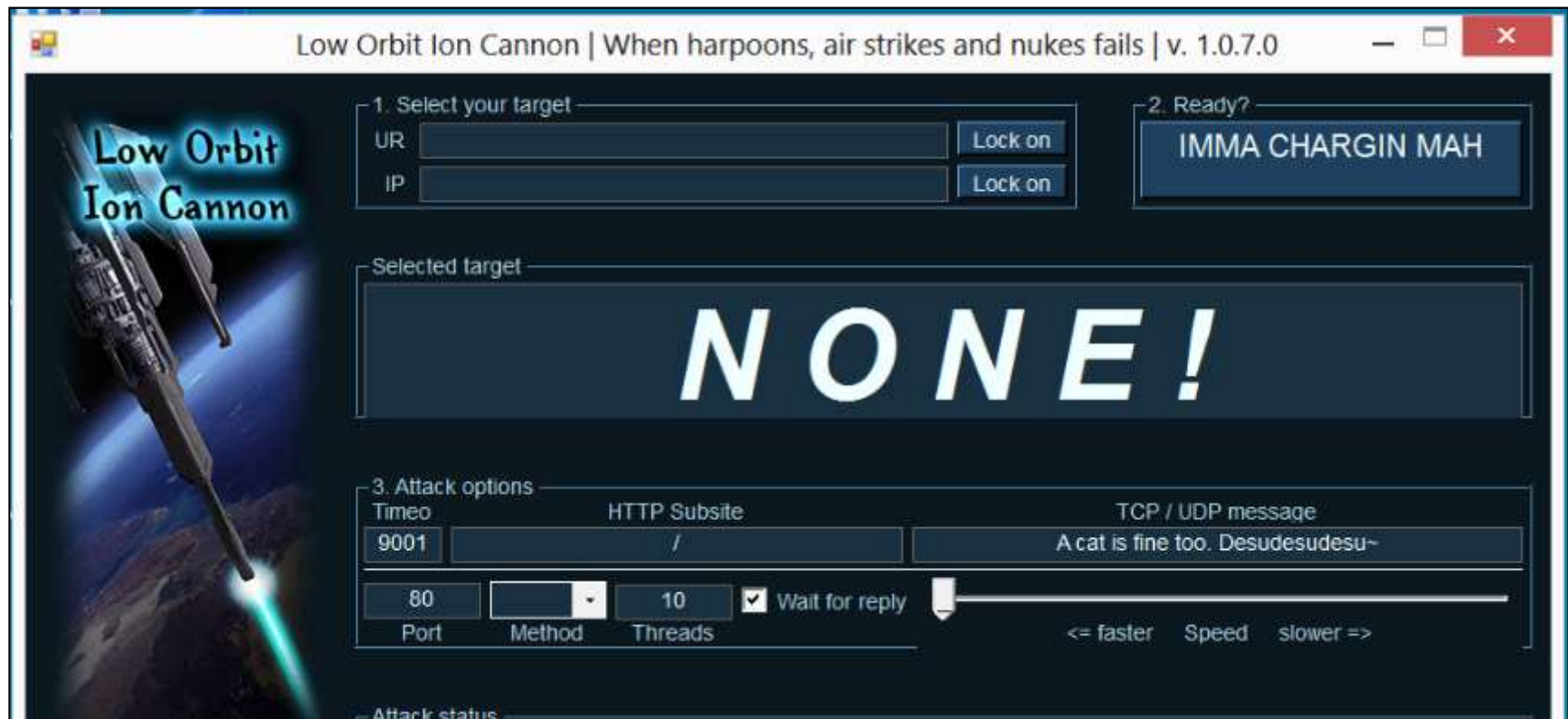
Bonus Section 1 uses STFU and Modbus Pal to simulate controllers and network commands

# Tunneling - TOR



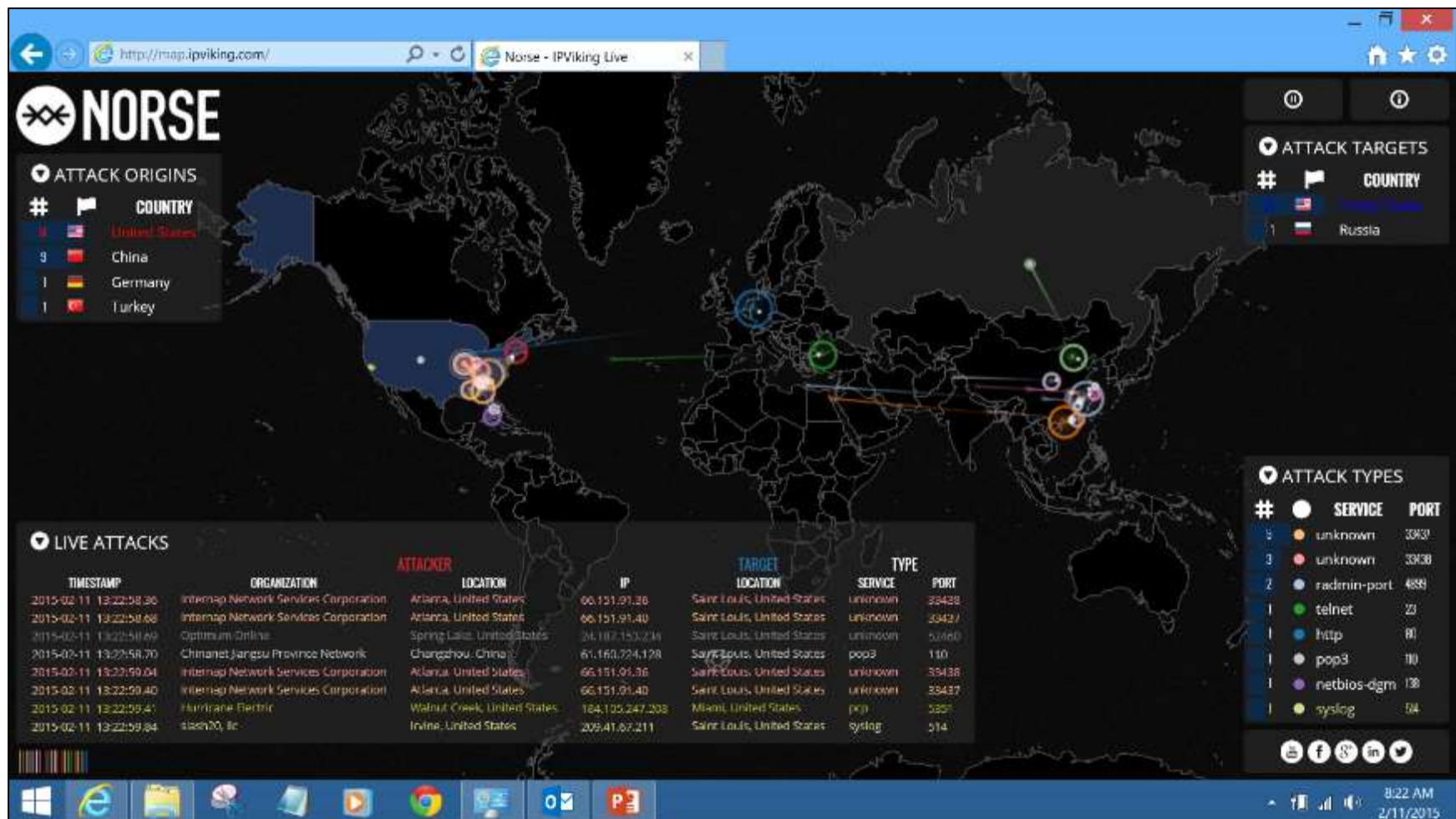
[http://en.wikipedia.org/wiki/Tor\\_%28anonymity\\_network%29](http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29)

# Low Orbit Cannon





# IP Viking



<http://map.ipviking.com/>

# NMAP Homepage

The screenshot shows the Nmap.org homepage in a web browser. The address bar displays <http://nmap.org/>. The page layout includes a left sidebar with navigation links, a main content area with a large banner for the Nmap Free Security Scanner, and a 'News' section at the bottom. The banner for the Nmap Free Security Scanner includes the text 'Network-wide ping sweep, portscan, OS Detection' and 'Audit your network security before the bad guys do'. Below the banner is a table of links for various resources. The 'News' section contains several bullet points about recent releases and updates.

**Navigation Menu (Left Sidebar):**

- Nmap Security Scanner
  - Intro
  - Ref Guide
  - Install Guide
  - Download
  - Changelog
  - Book
  - Docs
- Security Lists
  - Nmap
  - Announce
  - Nmap Dev
  - Bugtraq
  - Full Disclosure
  - Pen Test
  - Basics
  - More
- Security Tools
  - Pass crackers
  - Sniffers
  - Vuln Scanners
  - Web scanners
  - Wireless
  - Exploitation
  - Packet crafters
  - More
- Site News
- Advertising
- About/Contact

**Main Content Area:**

**Nmap Free Security Scanner**  
Network-wide ping sweep, portscan, OS Detection  
Audit your network security before the bad guys do

Intro	Reference Guide	Book	Install Guide
Download	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies			In the News

**Sponsors:**

- Cyber Penetration Testing (nettools.com)
- Free Device Scanner (lumension.com/Device-Scanner)
- Network Port Scanner (gf.com)

**News:**

- We're pleased to release our new and Improved [Icons of the Web](#) project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to [hack Matt Damon's brain in Elysium](#) and also to [launch nuclear missiles in G.I. Joe: Retaliation](#)!
- We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features! [\[Announcement/Details\]](#), [\[Download Site\]](#)
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [\[Announcement/Details\]](#), [\[Download Site\]](#)
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with [Nmap 6.01!](#)
- Nmap 6 is now available! [\[release notes\]](#) | [download](#)
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched [SecTools.Org](#). It is sort of like Yelp for security tools. Are you familiar with all of the [49 new tools](#) in this edition?
- [Nmap 5.50 Released](#): Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS fingerprints, and 7,319 version detection signatures. Release focuses were the Nmap Scripting Engine, performance, Zenmap GUI, and the Nping packet analysis tool. [\[Download page\]](#) | [Release notes](#)
- Those who missed Defcon can now watch Eudor and David Fifield demonstrate the power of the Nmap Scripting Engine. They give an overview of NSE, use it to explore Microsoft's global network, write an NSE

<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/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
  -s0: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```



# Zenmap – Security Scanner

The screenshot shows the Zenmap website interface. At the top, there's a navigation bar with the Nmap logo and a banner for AlienVault. Below this, a left sidebar contains a 'Nmap Security Scanner' menu with links like Intro, Ref Guide, Install Guide, Download, Changelog, Book, and Docs. Another section in the sidebar lists 'Security Lists' and 'Security Tools'. The main content area features a central navigation grid with links to Intro, Reference Guide, Book, Install Guide, Download, Changelog, Zenmap GUI, Docs, Bug Reports, OS Detection, Propaganda, Related Projects, In the Movies, and In the News. Below this grid, the 'Introduction' section describes Zenmap as a multi-platform GUI for Nmap, highlighting its ease of use and advanced features. A 'Screen shots' section is partially visible at the bottom. The browser's address bar shows 'nmap.org/zenmap' and the system clock indicates 9:59 AM on 8/9/2016.

**NMAP.ORG**

Take your Nmap scans to the next level with AlienVault...  
View vulnerability data, asset information & threat detection alerts in a single console! [Try It Free ▶](#)

**Nmap Security Scanner**

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

**Security Lists**

- Nmap
- Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

**Security Tools**

- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation

**Intro**   **Reference Guide**   **Book**   **Install Guide**  
**Download**   **Changelog**   **Zenmap GUI**   **Docs**  
**Bug Reports**   **OS Detection**   **Propaganda**   **Related Projects**  
**In the Movies**   **In the News**

## Introduction

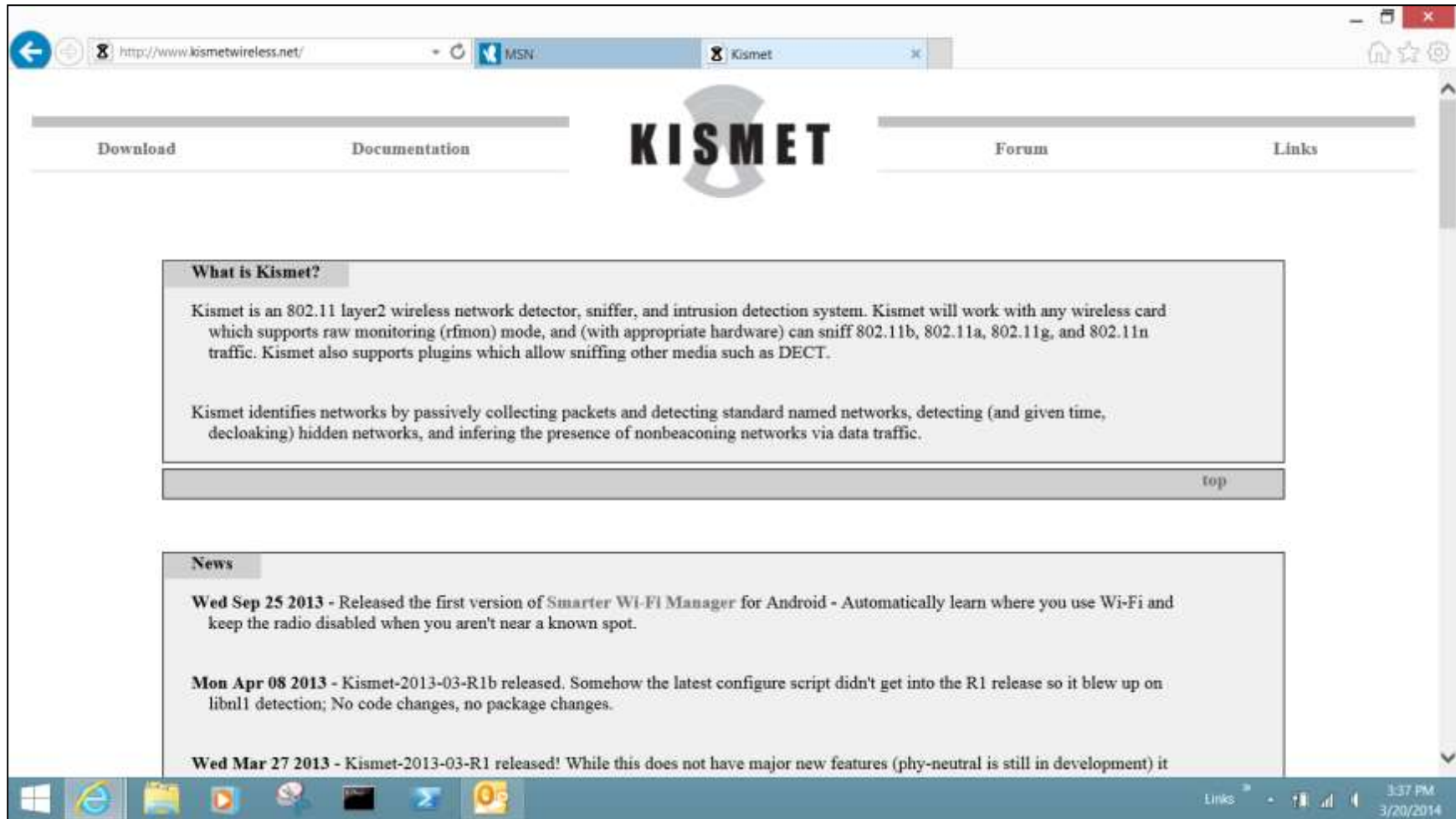
Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

You can download Zenmap (often packaged with Nmap itself) from the [Nmap download page](#). Zenmap is quite intuitive, but you can learn more about using it from the [Zenmap User's Guide](#) or check out the [Zenmap man page](#) for some quick reference information.

## Screen shots

<https://nmap.org/zenmap/>

# Kismet – 802 Detector, Sniffer and IDS



<http://kismetwireless.net/>



# Digital Bond Bandolier (1)

The screenshot shows a web browser window displaying the Digital Bond Bandolier website. The browser's address bar shows the URL <http://www.digitalbond.com/tools/bandolier/>. The website has a green and white color scheme. At the top, there is a navigation bar with links: Blog, Consulting, S4, Critical Intelligence, Podcast, SCADApedia, Tools, About Us, and Advertise. Below this is a banner for "digital bond" and "CODENOMICON" with the text "SECURE YOUR CRITICAL INFRASTRUCTURE AGAINST CYBER ATTACKS" and "ISA9999 compliant robustness testing solutions". A secondary navigation bar includes links: What's Hot, S4x14 Videos, OTDay Presentations, Project Basecamp, and Bandolier. The main content area is titled "Bandolier" and describes the project's purpose: helping asset owners and vendors identify and audit optimal security configuration for industrial control system (ICS) servers and workstations. It mentions that 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. The "Overview" section lists three bullet points: 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. The "How it Works" section lists four bullet points: 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. A left sidebar titled "Pages" lists various links: 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, and Advertise. The Windows taskbar at the bottom shows the Start button, Internet Explorer, and several other application icons. The system clock in the bottom right corner indicates 1:04 PM on 4/7/2014.

Blog Consulting S4 Critical Intelligence Podcast SCADApedia Tools About Us Advertise

**digital bond**

**CODENOMICON**

**SECURE YOUR CRITICAL INFRASTRUCTURE AGAINST CYBER ATTACKS**  
ISA9999 compliant robustness testing solutions

What's Hot S4x14 Videos OTDay Presentations Project Basecamp **Bandolier**

## 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

#### 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

Links 1:04 PM 4/7/2014

# 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](#)

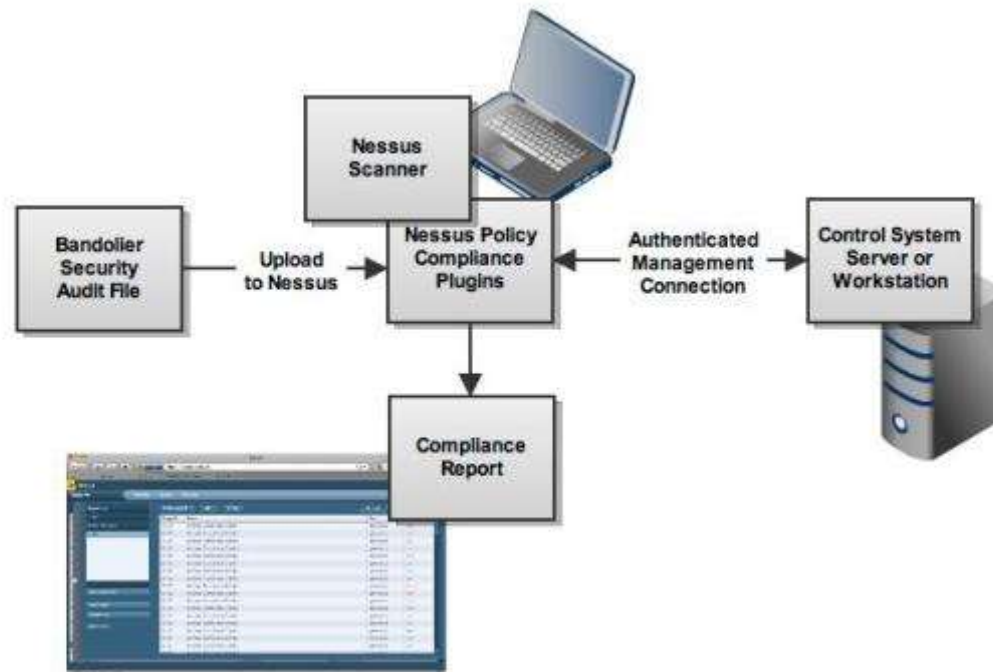
[Vulnerability Signatures](#)

Device Signatures

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

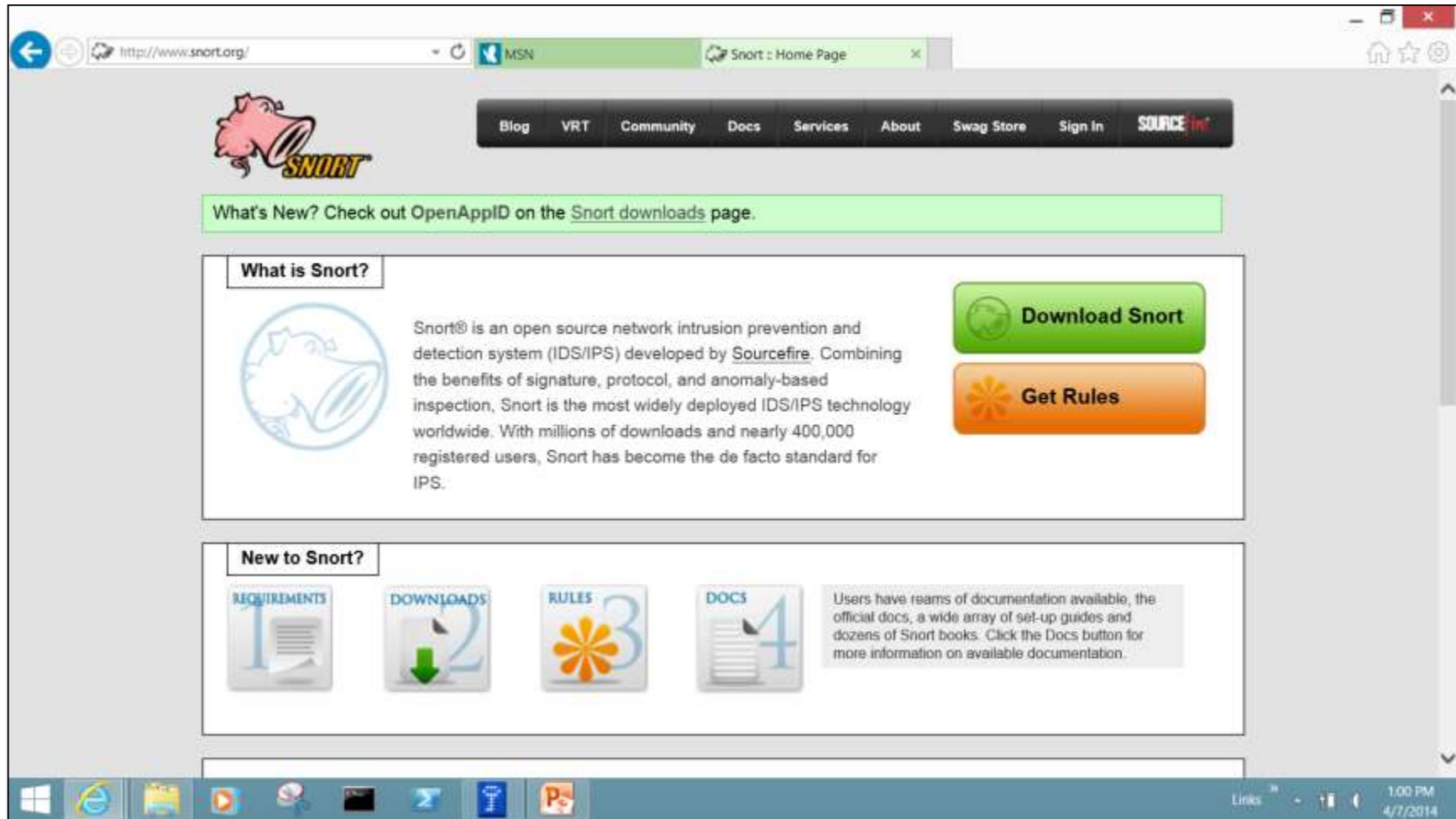
# Digital Bond Bandolier-Nessus

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/>

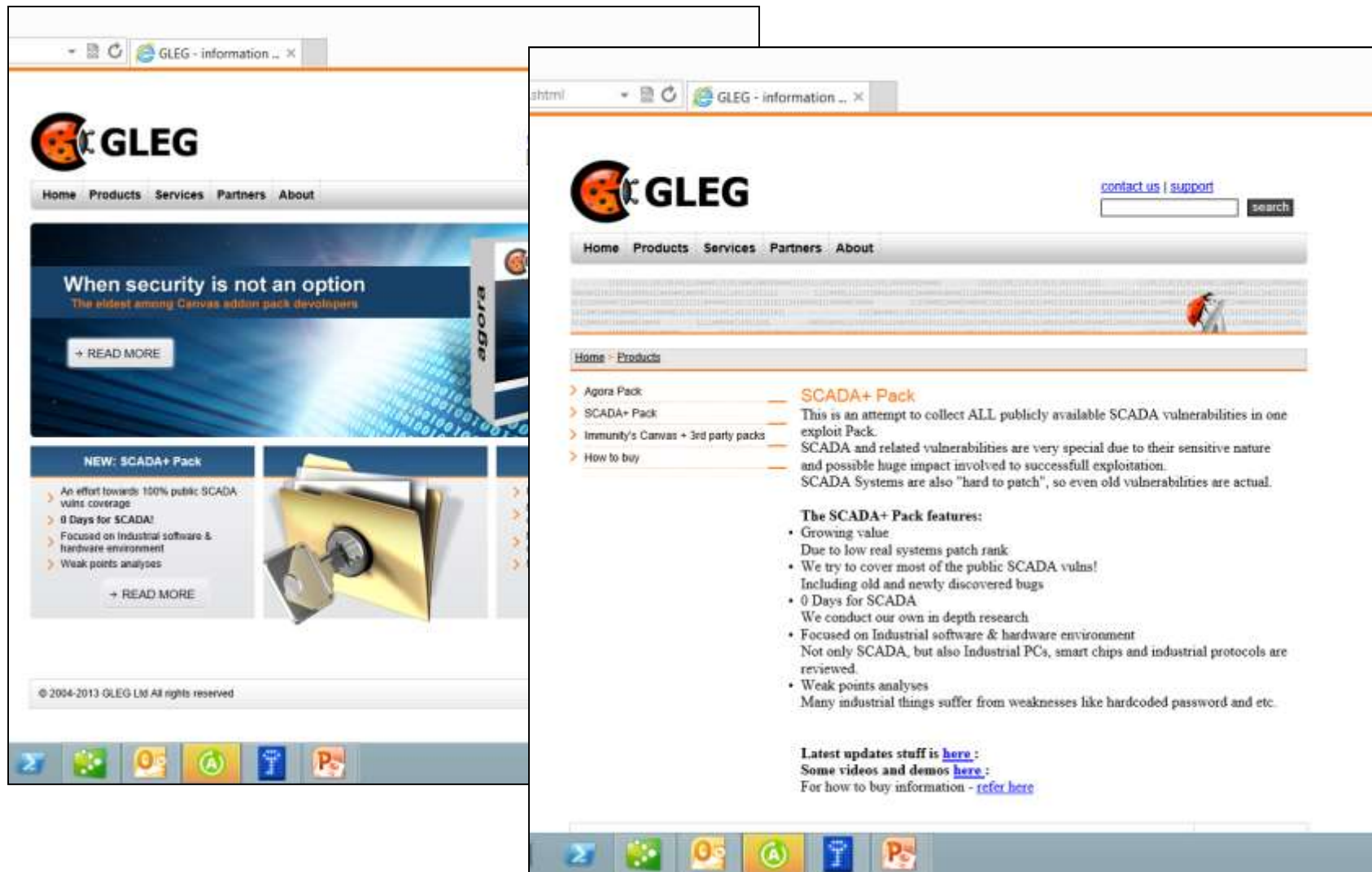
# Snort



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

<http://www.snort.org/>

# Gleg



**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](http://en.wikipedia.org/wiki/Virtual_machine)

# Why Use a VM?

## **Advantages of VM**

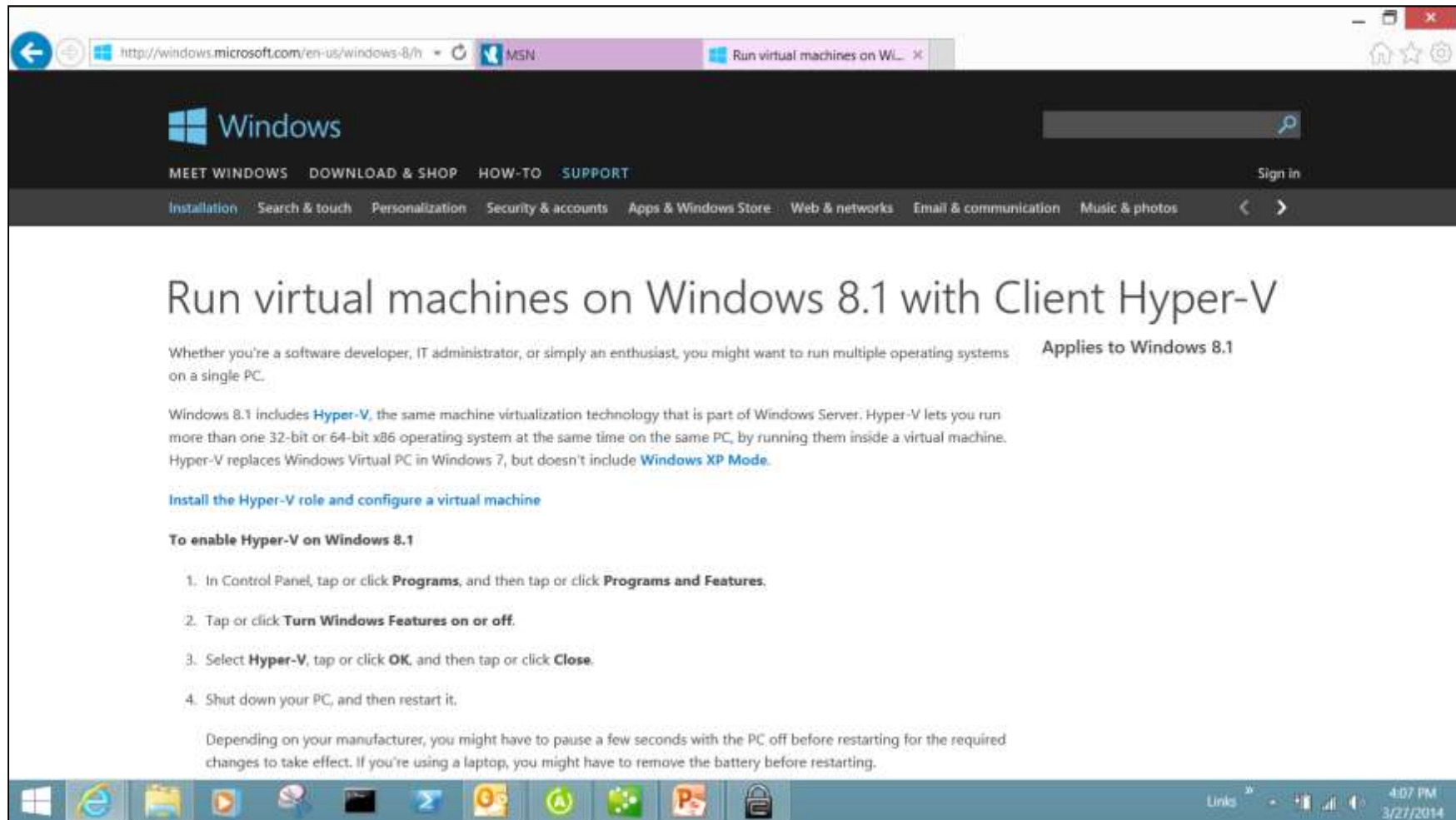
- Can open multiple VM's with different OS
- Can create a complete reproduction of a Production environment  
Can create a Test and Development environment
- Reproducibility, can
- Malware in a VM is terminated when VM is powered down
- Server consolidation is the most compelling benefit of VMs. A typical 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

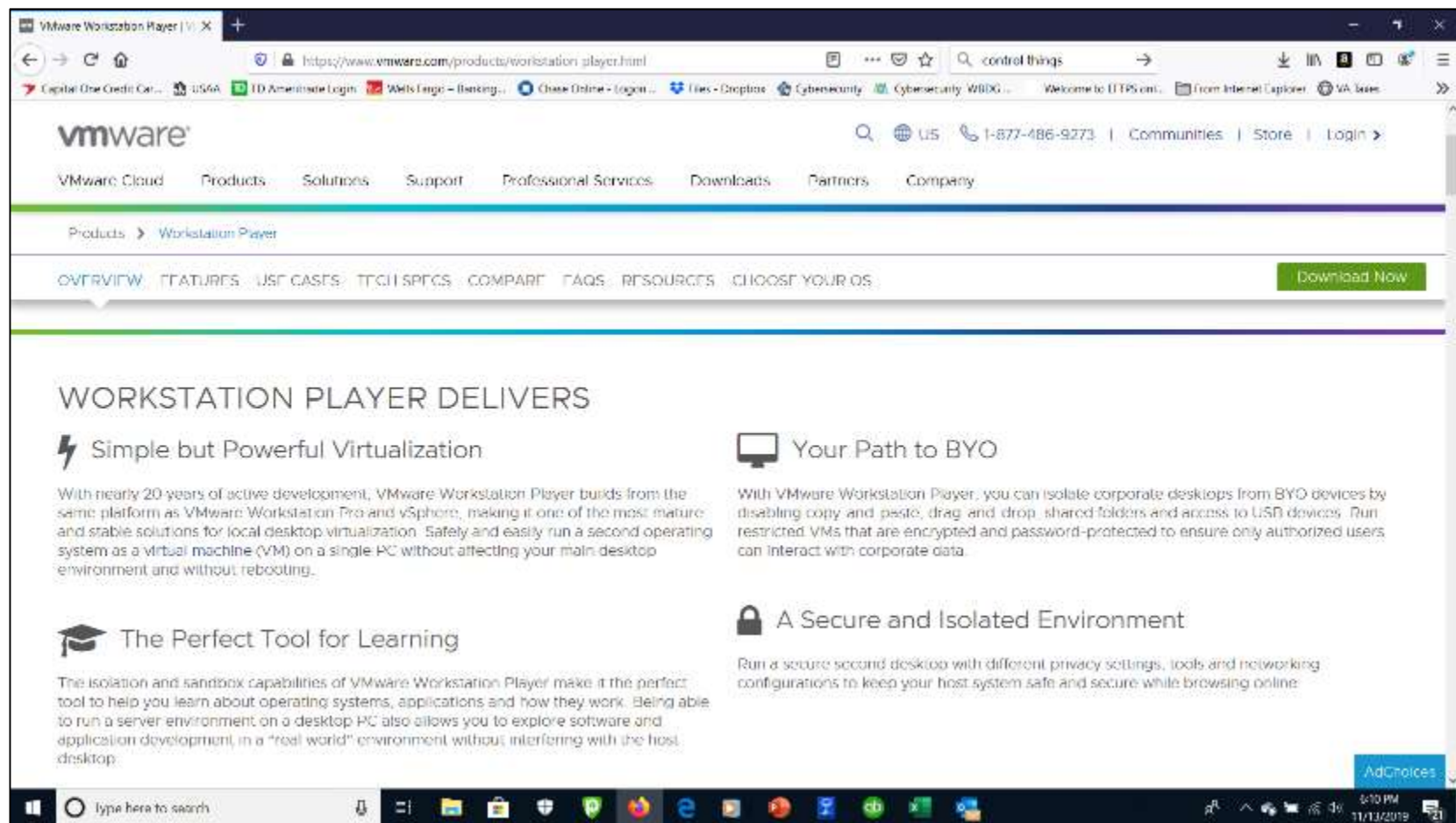
<http://searchservirtualization.techtarget.com/tip/Understanding-the-benefits-of-a-virtual-machine>

# Windows Virtual Machines



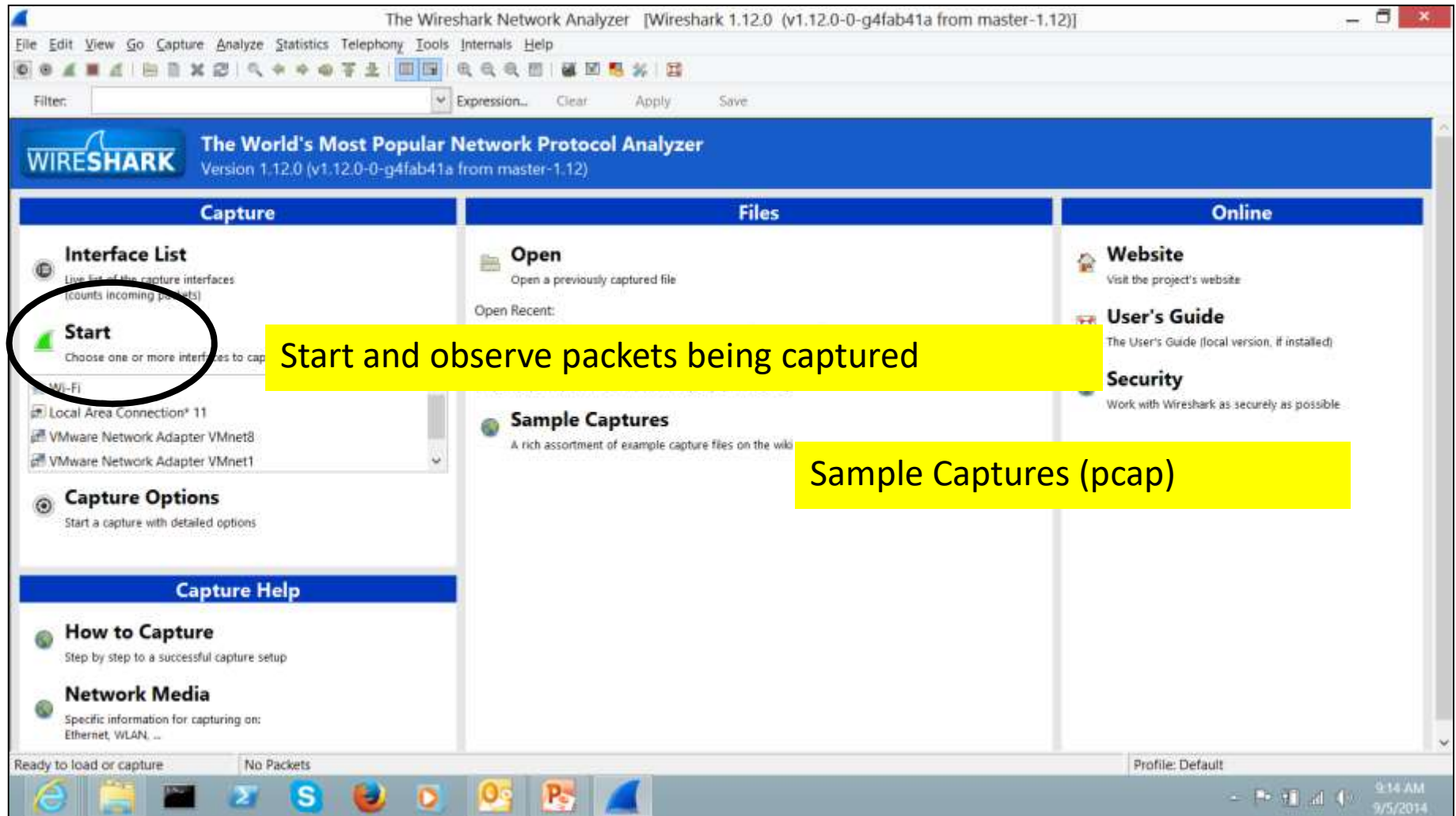
<http://windows.microsoft.com/en-us/windows-8/hyper-v-run-virtual-machines>

# VMWare



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

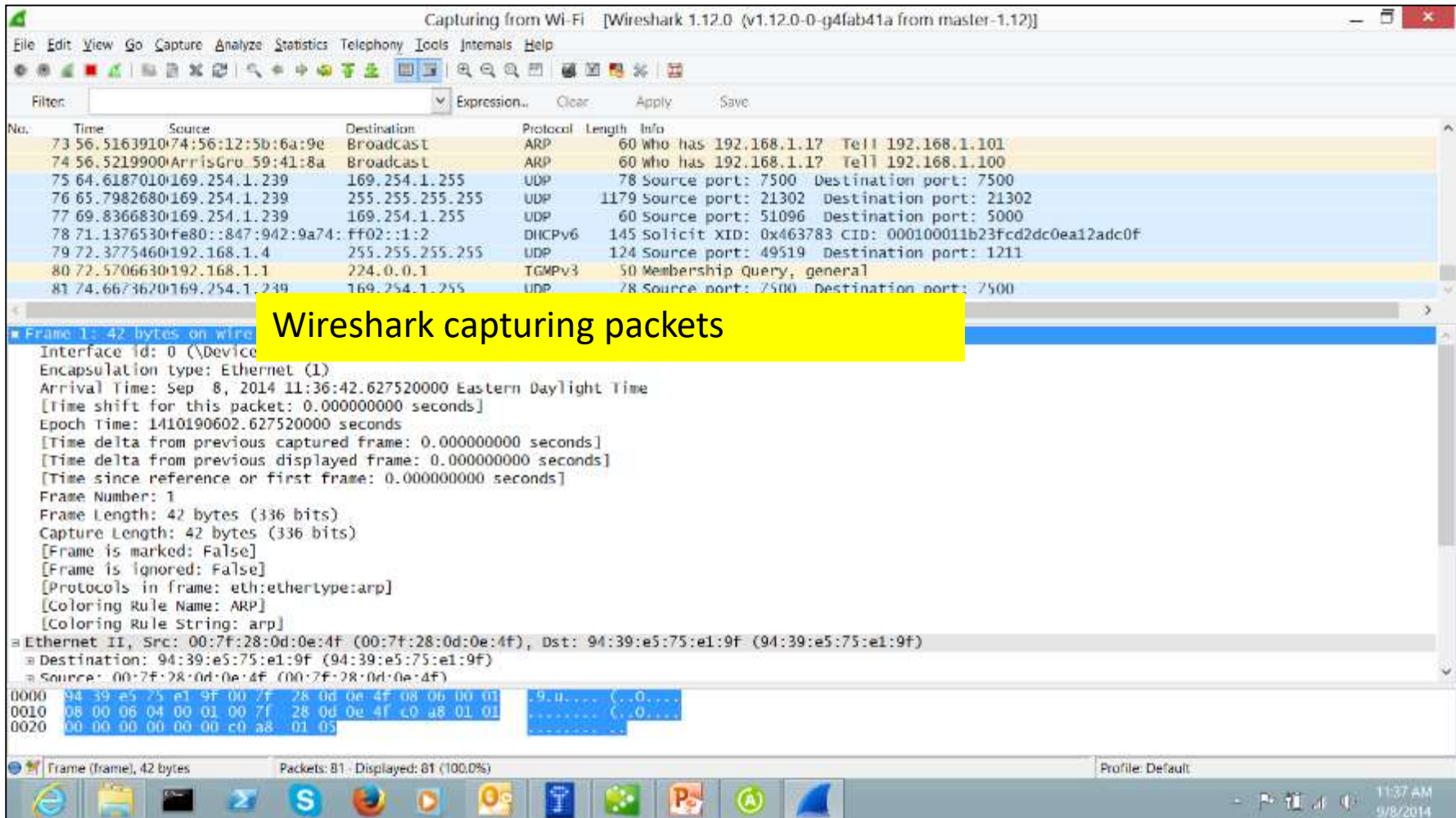
# Wireshark Home



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



# Wireshark Active Packet Capture



The image shows the Wireshark 1.12.0 interface capturing data from a Wi-Fi interface. The main packet list displays several entries, including ARP requests, UDP traffic, and a DHCPv6 Solicit message. A yellow highlight is placed over the first packet, Frame 1, which is an ARP request. The packet details pane on the right shows the structure of this frame, including the Ethernet II header, source and destination MAC addresses, and the ARP payload. The packet bytes pane at the bottom shows the raw hexadecimal and ASCII data of the frame.

Wireshark capturing packets

No.	Time	Source	Destination	Protocol	Length	Info
73	56.5163910	74:56:12:5b:6a:9e	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.101
74	56.5219900	ArrisGro 59:41:8a	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.100
75	64.6187010	169.254.1.239	169.254.1.255	UDP	78	Source port: 7500 Destination port: 7500
76	65.7982680	169.254.1.239	255.255.255.255	UDP	1179	Source port: 21302 Destination port: 21302
77	69.8366830	169.254.1.239	169.254.1.255	UDP	60	Source port: 51096 Destination port: 5000
78	71.1376530	fe80::847:942:9a74::ff02::1:2	ff02::1:2	DHCPv6	145	Solicit XID: 0x463783 CID: 000100011b23fcd2dc0ea12adc0f
79	72.3775460	192.168.1.4	255.255.255.255	UDP	124	Source port: 49519 Destination port: 1211
80	72.5706630	192.168.1.1	224.0.0.1	IGMPv3	50	Membership Query, general
81	74.6673620	169.254.1.239	169.254.1.255	UDP	78	Source port: 7500 Destination port: 7500

Frame 1: 42 bytes on wire (Interface id: 0 (\Device...))  
Encapsulation type: Ethernet (1)  
Arrival Time: Sep 8, 2014 11:36:42.627520000 Eastern Daylight Time  
[Time shift for this packet: 0.000000000 seconds]  
Epoch Time: 1410190602.627520000 seconds  
[Time delta from previous captured frame: 0.000000000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 0.000000000 seconds]  
Frame Number: 1  
Frame Length: 42 bytes (336 bits)  
Capture Length: 42 bytes (336 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:arp]  
[Coloring Rule Name: ARP]  
[Coloring Rule String: arp]  
Ethernet II, Src: 00:7f:28:0d:0e:4f (00:7f:28:0d:0e:4f), Dst: 94:39:e5:75:e1:9f (94:39:e5:75:e1:9f)  
Destination: 94:39:e5:75:e1:9f (94:39:e5:75:e1:9f)  
Source: 00:7f:28:0d:0e:4f (00:7f:28:0d:0e:4f)  
0000 94 39 e5 75 e1 9f 00 7f 28 0d 0e 4f 08 06 00 01  
0010 08 00 06 04 00 01 00 7f 28 0d 0e 4f c0 a8 01 01  
0020 00 00 00 00 00 00 c0 a8 01 05

# Modbus pcap files

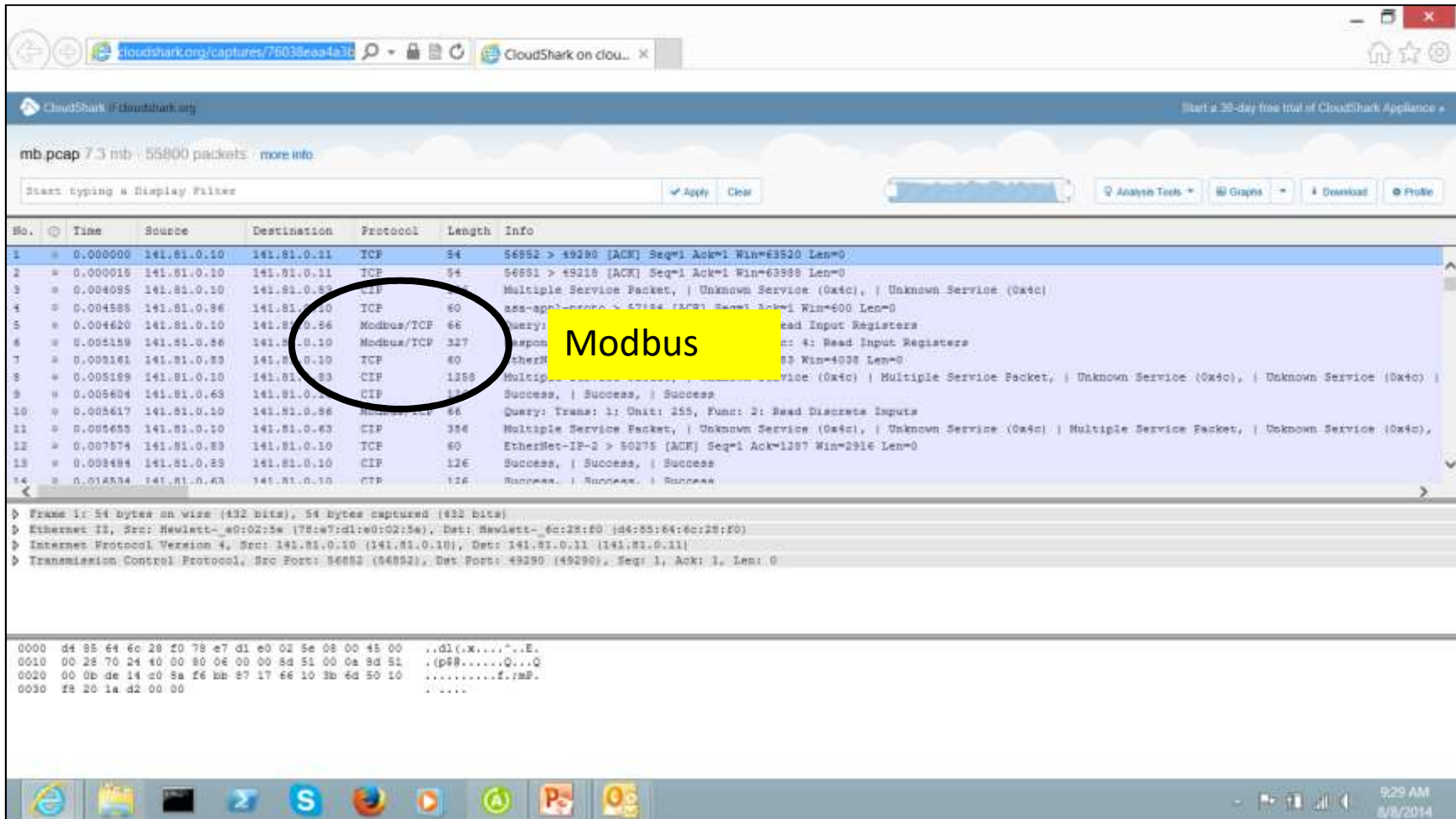
The screenshot shows a web browser window displaying the PCAPr website. The address bar shows the URL <http://www.pcapr.net/browse/scada?q=DIN>. The page title is "SCADA/Control Systems Packet Captures". A blue banner at the top of the content area states: "You must [login](#) to view, edit, upload and comment on pcaps. If you are a new user, you can [register here](#)". Below this, a link says "Looking for a specific pcap? Try the [field index](#)".

The main content area displays a list of six Modbus pcap files, each with a user profile icon, the filename, the protocol, and the date:

- [modbus-mask-write-register.pcap](#) (8 packets | 812 bytes) - proto: modbus/tcp tcp - Edit - twilkinson November 2008
- [modbus-read-fifo-queue.pcap](#) (8 packets | 810 bytes) - proto: modbus/tcp tcp - Edit - twilkinson November 2008
- [modbus-read-discrete-inputs.pcap](#) (8 packets | 808 bytes) - proto: modbus/tcp tcp - Edit - twilkinson November 2008
- [modbus-read-holding-registers.pcap](#) (8 packets | 807 bytes) - proto: modbus/tcp tcp - Edit - twilkinson November 2008
- [modbus-read-input-registers.pcap](#) (8 packets | 807 bytes) - proto: modbus/tcp tcp - Edit - twilkinson November 2008
- [modbus-read-file-record.pcap](#) (8 packets | 813 bytes) - proto: modbus/tcp tcp - Edit - twilkinson November 2008

The website footer shows the time 8:42 AM and date 8/19/2014. The Windows taskbar at the bottom includes icons for Internet Explorer, File Explorer, and several other applications.

# Wireshark Captures (pcap's)

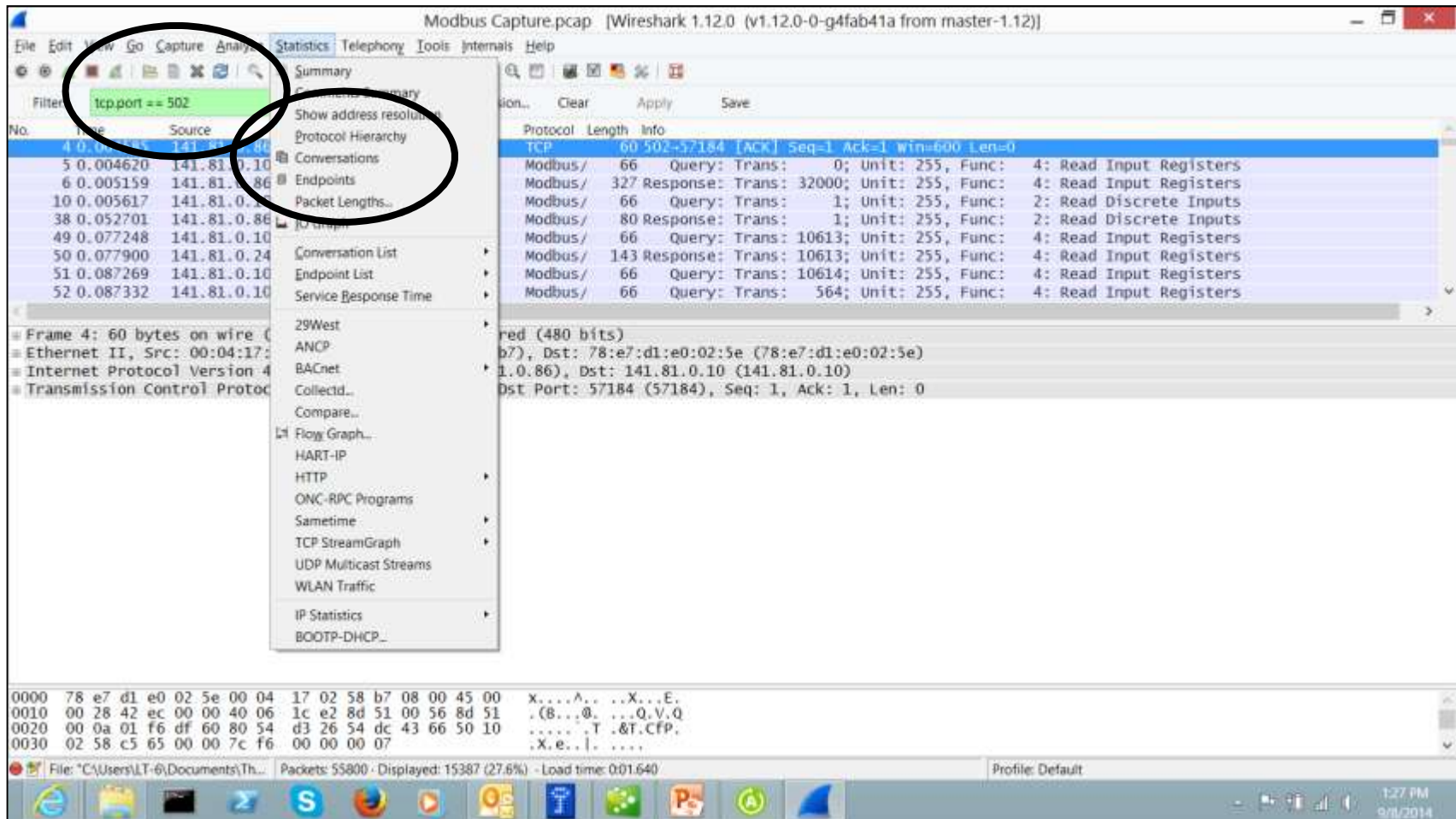


The screenshot displays a web browser window with the URL `cloudshark.org/captures/760385ea4a3c`. The page shows a capture of a file named `mb.pcap` (7.3 mb, 55800 packets). The packet list table is visible, with the following columns: No., Time, Source, Destination, Protocol, Length, and Info. The packet list shows a series of packets, with the 10th packet (No. 10) highlighted in blue. This packet is a Modbus/TCP packet from 141.81.0.10 to 141.81.0.11. The packet details pane shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The Modbus section is expanded, showing the following details:

- Modbus/TCP: 66 bytes
- Query: Trans: 1; Unit: 255; Func: 2: Read Discrete Inputs
- Response: 66 bytes
- Header: 6 bytes
- Unit ID: 255
- Function: 2: Read Discrete Inputs
- Start Address: 0
- Quantity: 1
- Response Data: 0

A yellow box with the text "Modbus" is placed over the packet details pane. The packet details pane also shows the raw data of the packet in hexadecimal and ASCII format.

# Wireshark Captures (pcap's)





# Wireshark Captures (pcap's)

Conversations: Modbus Capture.pcap

Ethernet: 13 | Fibre Channel | FDDI | IPv4: 13 | IPv6 | IPX | JITA | NCP | RSVP | SCTP | TCP: 14 | Token Ring | UDP | USB | WLAN

IPv4 Conversations - Filter: tcp.port == 502

Address A	Address B	Packets A→B	Bytes A→B	Packets B→A	Bytes B→A	Packets A→B	Bytes A→B	Ref Start	Duration	bps A→B	bps B→A
141.81.0.10	141.81.0.86	1 518	125 587	701	48 816	817	76 741	0.004585000	0.19284	1631.14	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	81.6450	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	84.6737	4114.05	5157.26
141.81.0.10	141.81.0.84	1 265	96 138	689	44 854	576	51 264	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

☒ Name resolution ☒ Limit to display filter

Help Copy Follow Stream Graph A→B Graph B→A Close

1:31 PM 9/8/2014



# BACNet pcap files

The screenshot shows a web browser window displaying the Wireshark website. The address bar shows the URL <http://wiki.wireshark.org/Protocols/bacnet?>. The page title is "Protocols/bacnet". A message at the top states "Redirected from page 'BACnet'". The main content area is titled "BACnet" and contains the following text:

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 Cimetrix U-4 converter, **LLC SNAP** as its transport protocol.

**Example traffic:**

Below the text is a screenshot of a Wireshark packet capture window titled "bacnet-stack-services.cap - Wireshark". The window shows the standard Wireshark interface with a menu bar, toolbar, filter field, and a packet list table. The table has columns for "No.", "Time", "Source", "Destination", "Protocol", and "Info". The first packet is selected, showing details for "BACNET-STACK-SERVICES" and "BACNET-STACK-SERVICES". The system tray at the bottom shows the time as 5:05 PM on 8/3/2014.

# Wireshark BACnet pcap

The screenshot displays the Wireshark interface with a BACnet packet capture. The packet list shows a Simple-ACK packet. The packet details pane shows the BACnet Virtual Link Control and Building Automation and Control Network (BACnet) fields. The packet bytes pane shows the raw data.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.13	192.168.0.255	BACnet	53	Simple-ACK acknowledgeAlarm[ 2]
2	22.717118	192.168.0.13	192.168.0.255	BACnet	64	Unconfirmed-REQ who-Has
3	22.745865	00:60:2d:00:15:d5	Broadcast	BACnet	60	Unconfirmed-REQ who-Has
4	22.765855	192.168.0.5	192.168.0.13	BACnet	74	Unconfirmed-REQ I-Have device,61 device,61
5	200.636101	192.168.0.13	192.168.0.255	BACnet	59	Unconfirmed-REQ I-Have device,61 device,61
6	200.664755	00:60:2d:00:15:d5	Broadcast	BACnet	60	Unconfirmed-REQ I-Have device,61 device,61
7	200.684766	192.168.0.5	192.168.0.13	BACnet	74	Unconfirmed-REQ I-Have device,61 device,61
8	279.455576	192.168.0.13	192.168.0.255	BACnet	64	Unconfirmed-REQ TimeSynchronization
9	279.485292	00:60:2d:00:15:d5	Broadcast	BACnet	60	Unconfirmed-REQ TimeSynchronization

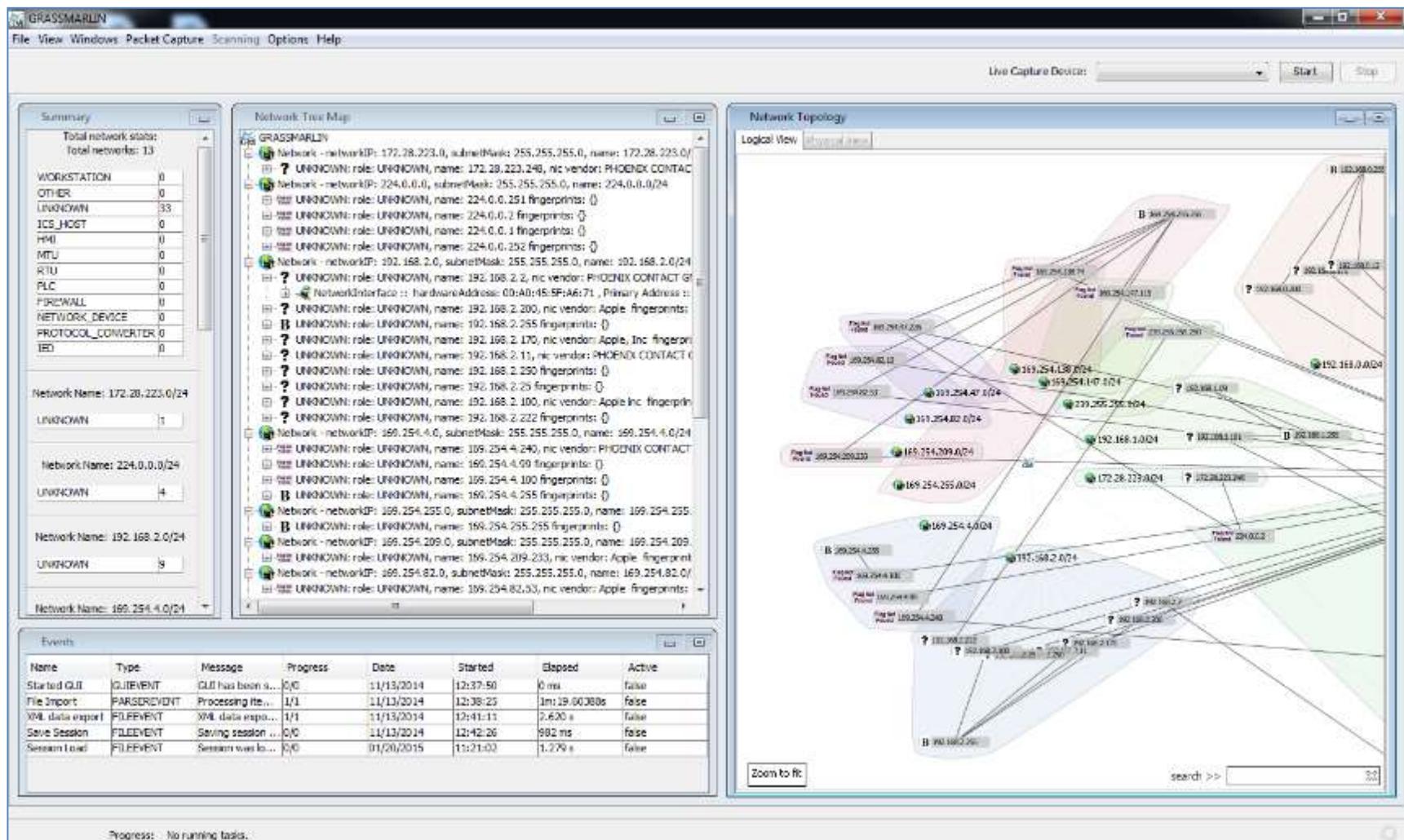
**Packet Details:**

- Frame 1: 53 bytes on wire (424 bits), 53 bytes captured (424 bits)
- Ethernet II, Src: 00:0c:6e:b0:3c:15 (00:0c:6e:b0:3c:15), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 192.168.0.13 (192.168.0.13), Dst: 192.168.0.255 (192.168.0.255)
- User Datagram Protocol, Src Port: 47808 (47808), Dst Port: 47808 (47808)
  - Source Port: 47808 (47808)
  - Destination Port: 47808 (47808)
  - Length: 19
  - Checksum: 0x00cb [validation disabled]
  - [Stream index: 0]
- BACnet Virtual Link Control
  - Type: BACnet/TP (Annex J) (0x81)
  - Function: Original-Unicast-NPDU (0x0a)
  - BVLC-Length: 4 of 11 bytes BACnet packet length
- Building Automation and Control Network NPDU
  - Version: 0x10 (unknown)
  - Control: 0x07
- Building Automation and Control Network APDU
  - 0010 .... = APDU Type: Simple ACK (2)
  - Invoke ID: 2
  - Service Choice: acknowledgeAlarm (0)

**Packet Bytes:**

Offset	Hex	ASCII
0000	ff ff ff ff ff ff 00 0c 6e b0 3c 15 08 00 43 00	.....n.<...L
0010	00 27 00 00 40 00 40 11 b8 69 c0 a8 00 0d c0 a8	...@...@...@
0020	00 ff ba c0 ba c0 00 13 0d cb 81 0a 00 0b 10 07	...fba...@...@
0030	2c 02 00 00 3d	...c...@...

# GrassMarlin Passive Network Collector



# CyberX

## CYBERX | Risk Assessment

Security Score

38%

36  
Vulnerable  
Devices



5  
Devices Needing  
Improvement

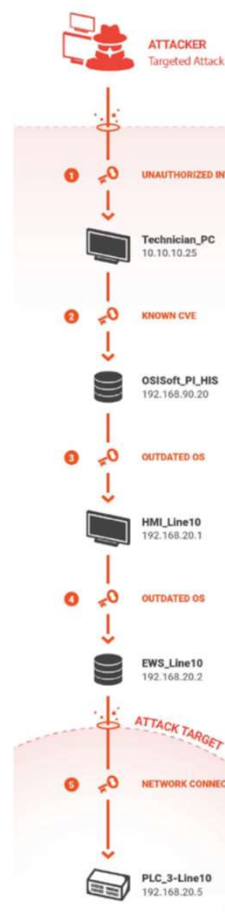


24  
Secure Devices



- Q 1 Unauthorized asset
- Q 14 Internet connections detected
- Q 7 connections to ICS networks detected
- Q Firewall rules: 0 out of 0 firewall rules are vulnerable
- Q No backup servers detected
- Q 7 Devices accessible remotely
- Q No engineering stations detected
- Q 1 Scanning device detected
- Q No AV software detected
- Q 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\_PL\_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

The screenshot displays the Belarc Advisor web interface within a browser window. The browser's address bar shows the file path: `file:///C:/Program%20Files%20(x86)/Belarc/BelarcAdvisor/System/tmp/LT9.html`. The Belarc Advisor logo is prominently displayed at the top. Below the logo, a disclaimer states: "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.](#)"

The interface features several key sections:

- System Security Status:** Includes a "Security Benchmark Score" (Available only for Windows 7, Vista, and XP Pro) and a "Virus Protection" status (Up-to-date).
- Security Updates:** Indicates that 3 updates are missing.
- Computer Profile Summary:** Provides details about the computer, including the name (LT9 (in WORKGROUP) — ACER), profile date (Monday, July 11, 2016 10:49:39 AM), advisor version (8.5c), and Windows login (LT7).
- Try BelManage, the Enterprise version of the Belarc Advisor**

The "In page Links" section on the left includes links for Software Licenses, Software Versions & Usage, Missing Updates, and USB Storage Use.

The main content area is divided into four sections:

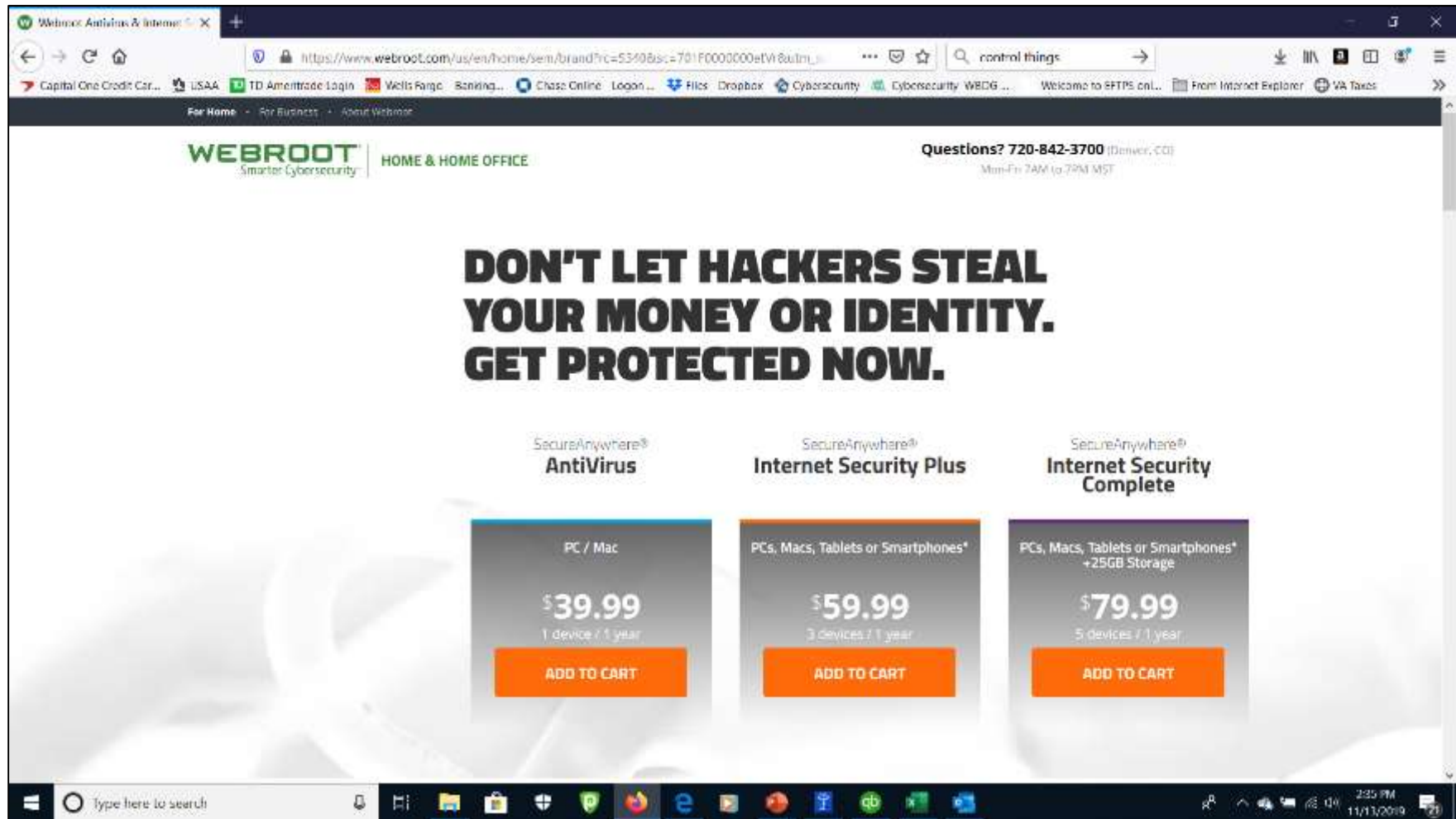
- Operating System:** Windows 10 Home (x64) Version 1511 (build 10586.420). Install Language: English (United States). System Locale: English (United States). Installed: 6/18/2016 4:27:43 AM. Servicing Branch: Current Branch (CB). Boot Mode: UEFI with successful [Secure Boot](#).
- System Model:** Acer Aspire V3-575T V1.10. System Serial Number: NXG5JAA0086130A55E7600.
- Processor:** 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:** Board: Acer Zoro\_SL V1.10. Serial Number: NBG3711D016130A55E7600. Bus Clock: 100 megahertz. UEFI: Insyde Corp. V1.10 11/27/2015.

The Windows taskbar at the bottom shows the search bar and various application icons. The system clock indicates the time is 11:14 AM on 7/11/2016.

<http://www.belarc.com/>

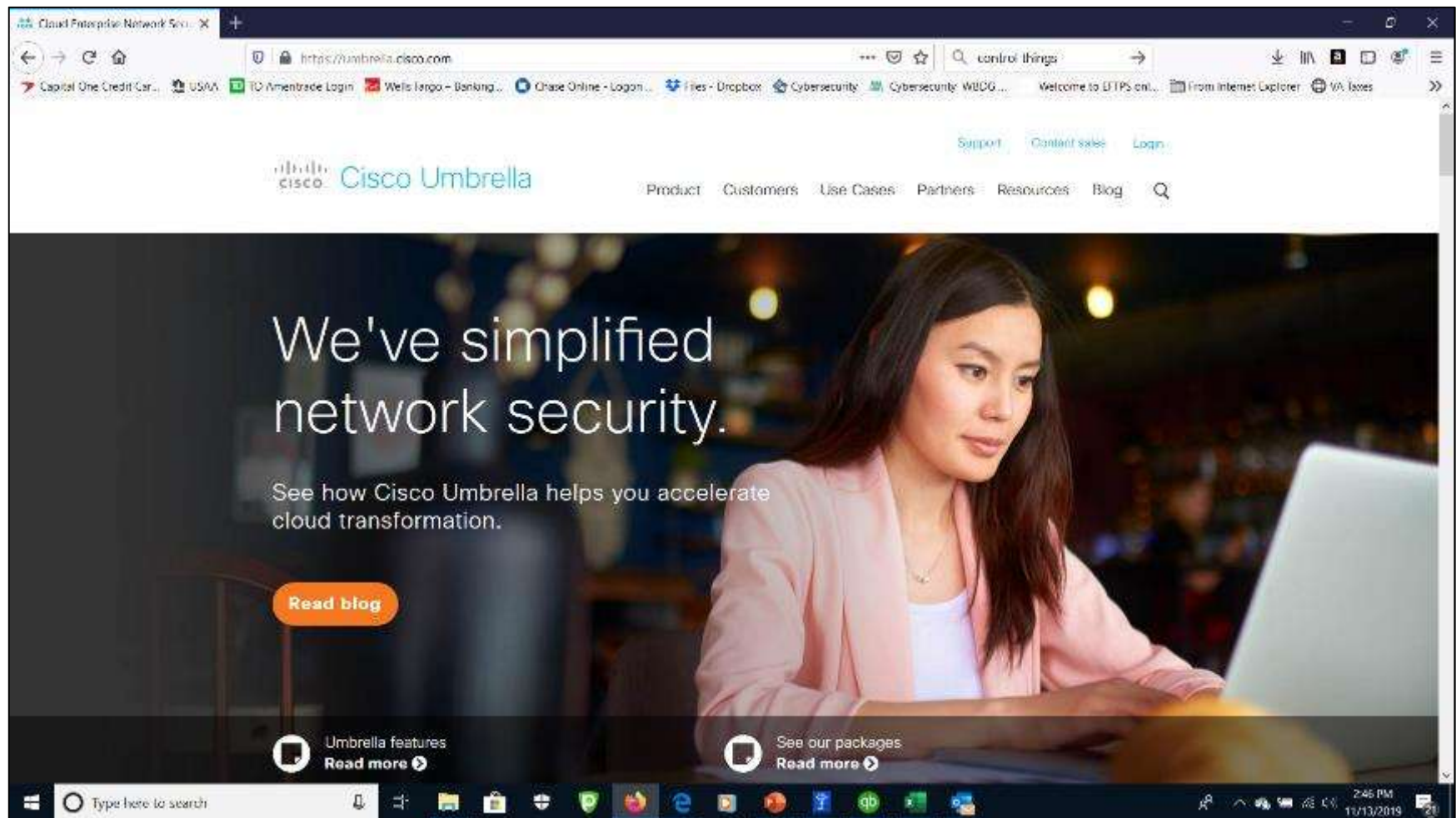


# Webroot



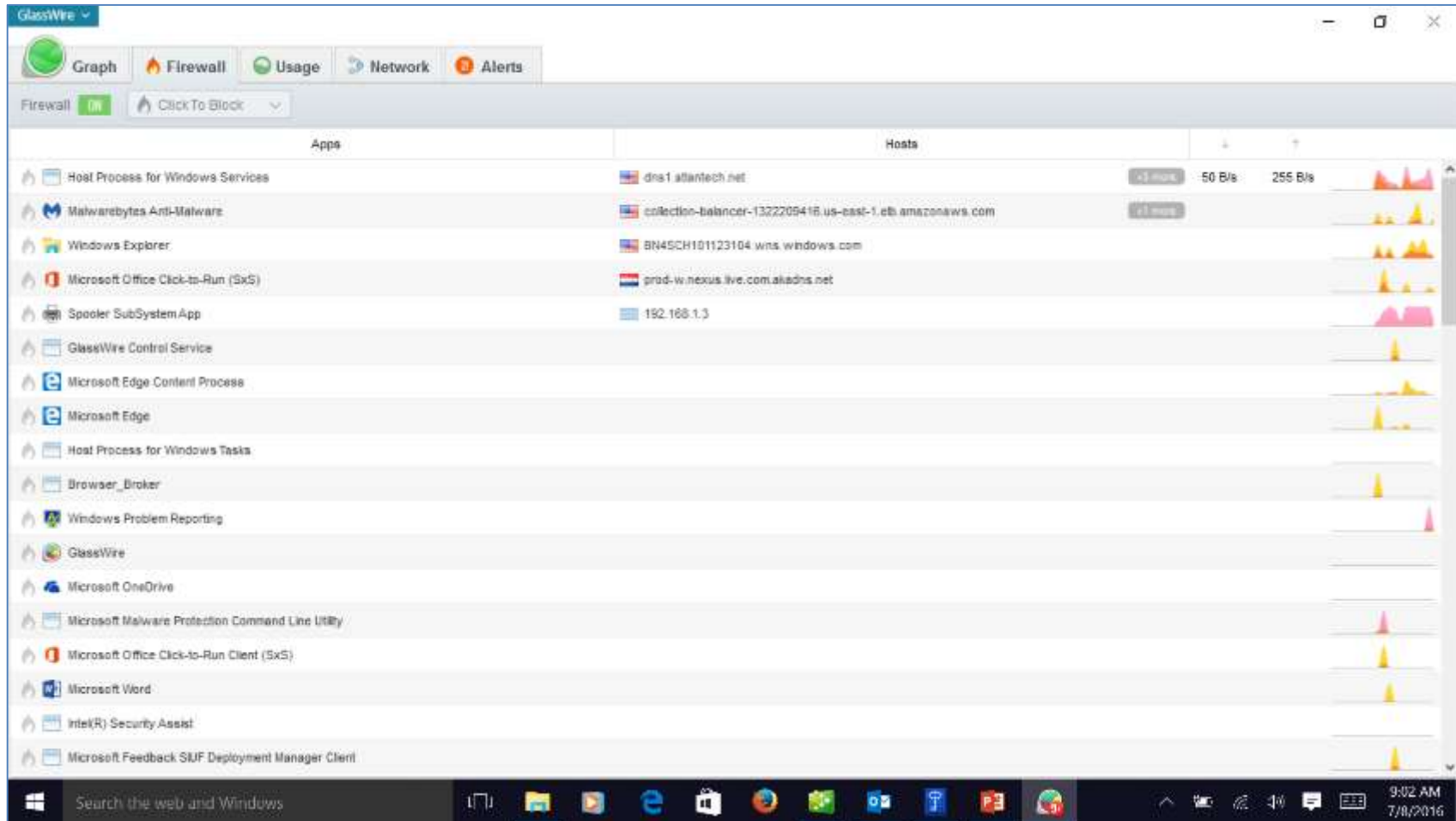
[https://www.webroot.com/us/en/home/sem/brand?rc=5340&sc=701F0000000etVr&utm\\_source=bing&utm\\_medium=cpc&utm\\_campaign=btc-bing-branded&msclkid=8309d7a4d1f01aa92be98a688b110e22](https://www.webroot.com/us/en/home/sem/brand?rc=5340&sc=701F0000000etVr&utm_source=bing&utm_medium=cpc&utm_campaign=btc-bing-branded&msclkid=8309d7a4d1f01aa92be98a688b110e22)

# Cisco Umbrella

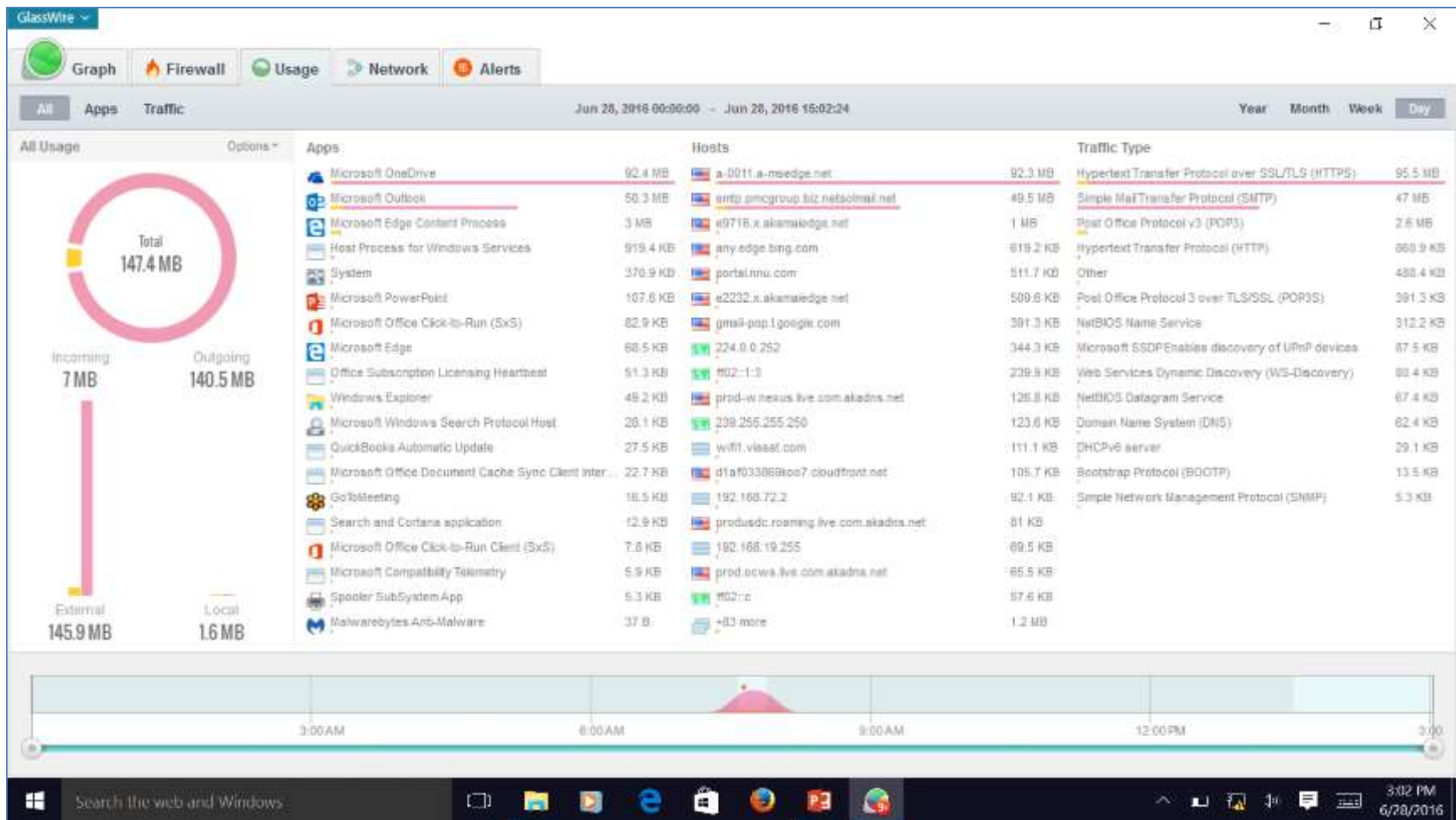


<https://umbrella.cisco.com/>

# Glasswire Firewall

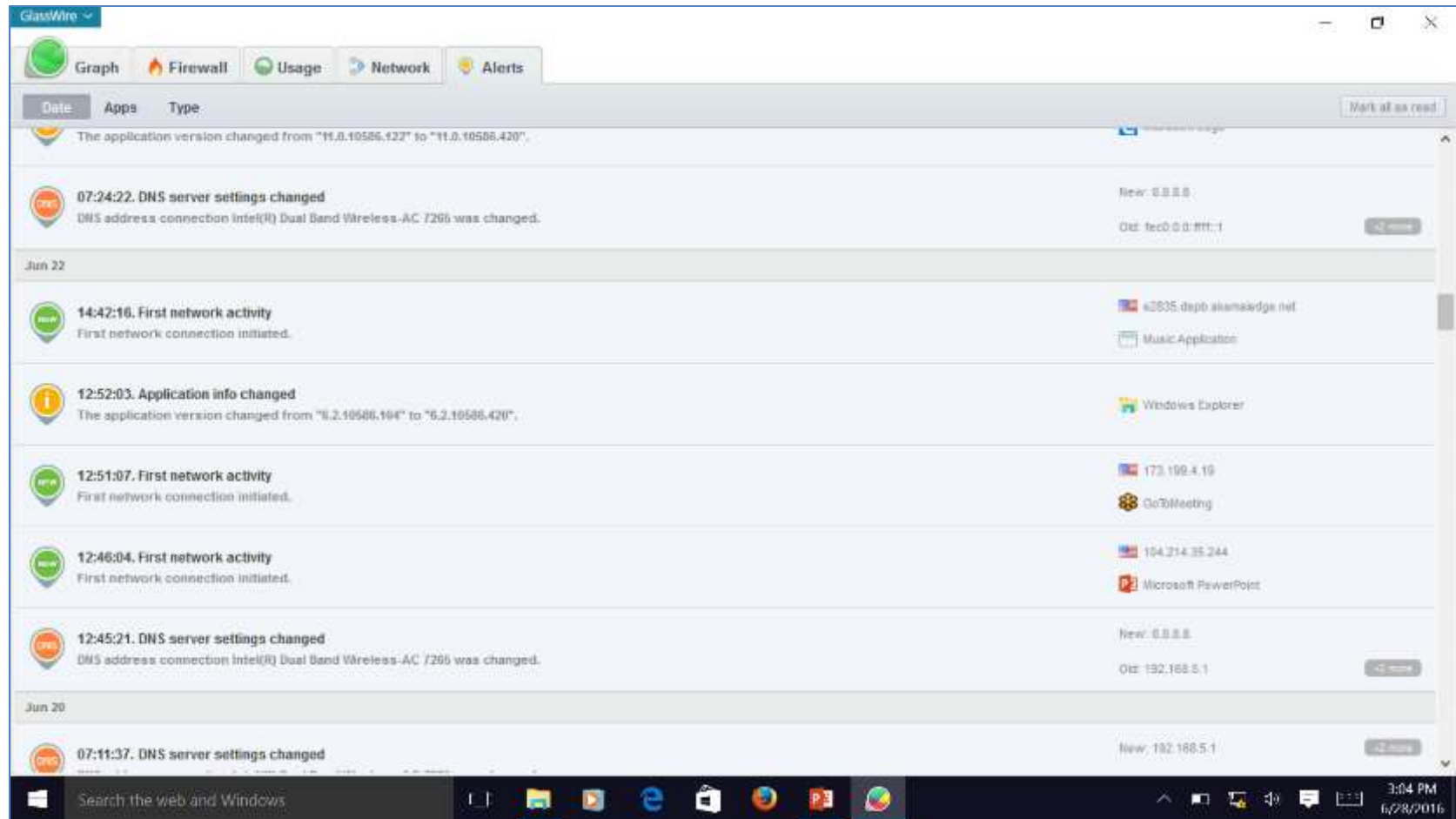


# Glasswire Usage



Apps, Hosts and Traffic Type

# Glasswire Alerts



DNS, Executable, Version



# Software / Firmware Inventory Hash





**H #ashing**

Help



Single file Multiple files Manual input

Browse File

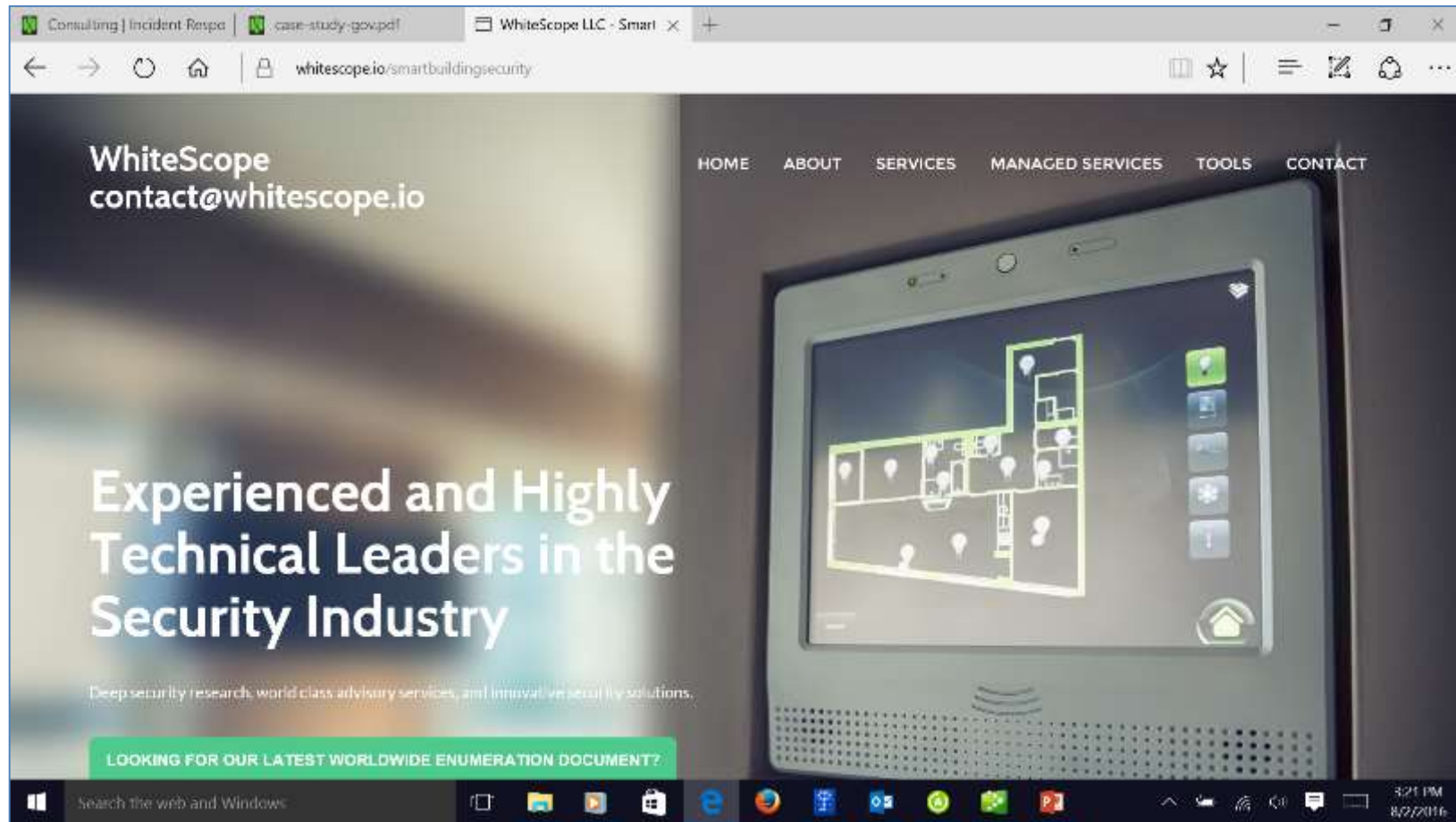
E:\PMC Projects Current\PMC-NIBS Cybersecuring Control Systems[...]\OAS setup.exe

MD5	ED22D355806B5454D30F3D8C1B7CB0A4	
SHA-1		
SHA-256		
SHA-512		

Verify Save all to text file

Done  

# WhiteScope BCS Homepage



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

# WhiteScope BCS Configuration Analysis



## 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

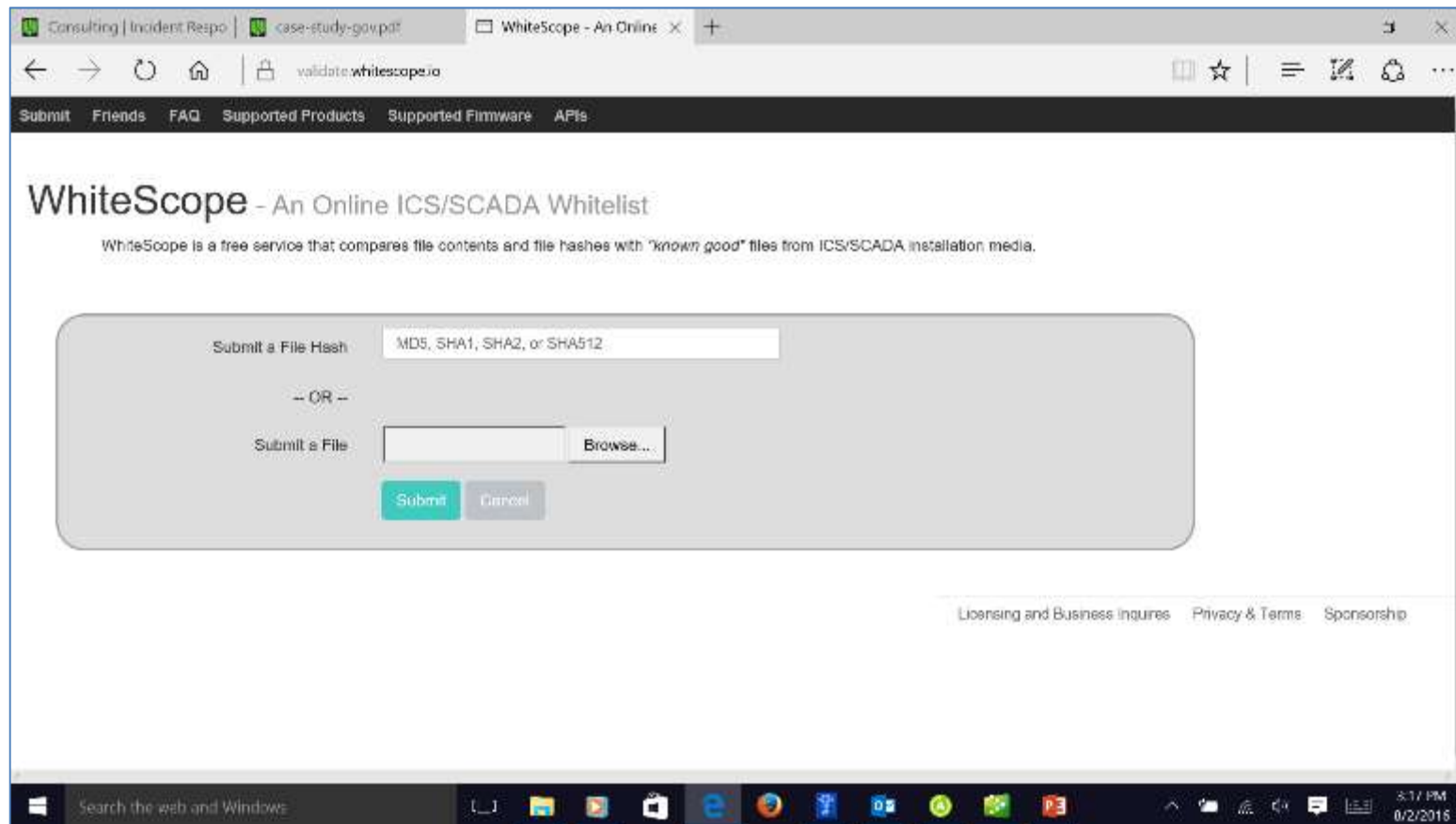
#### Summary

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

#### Details

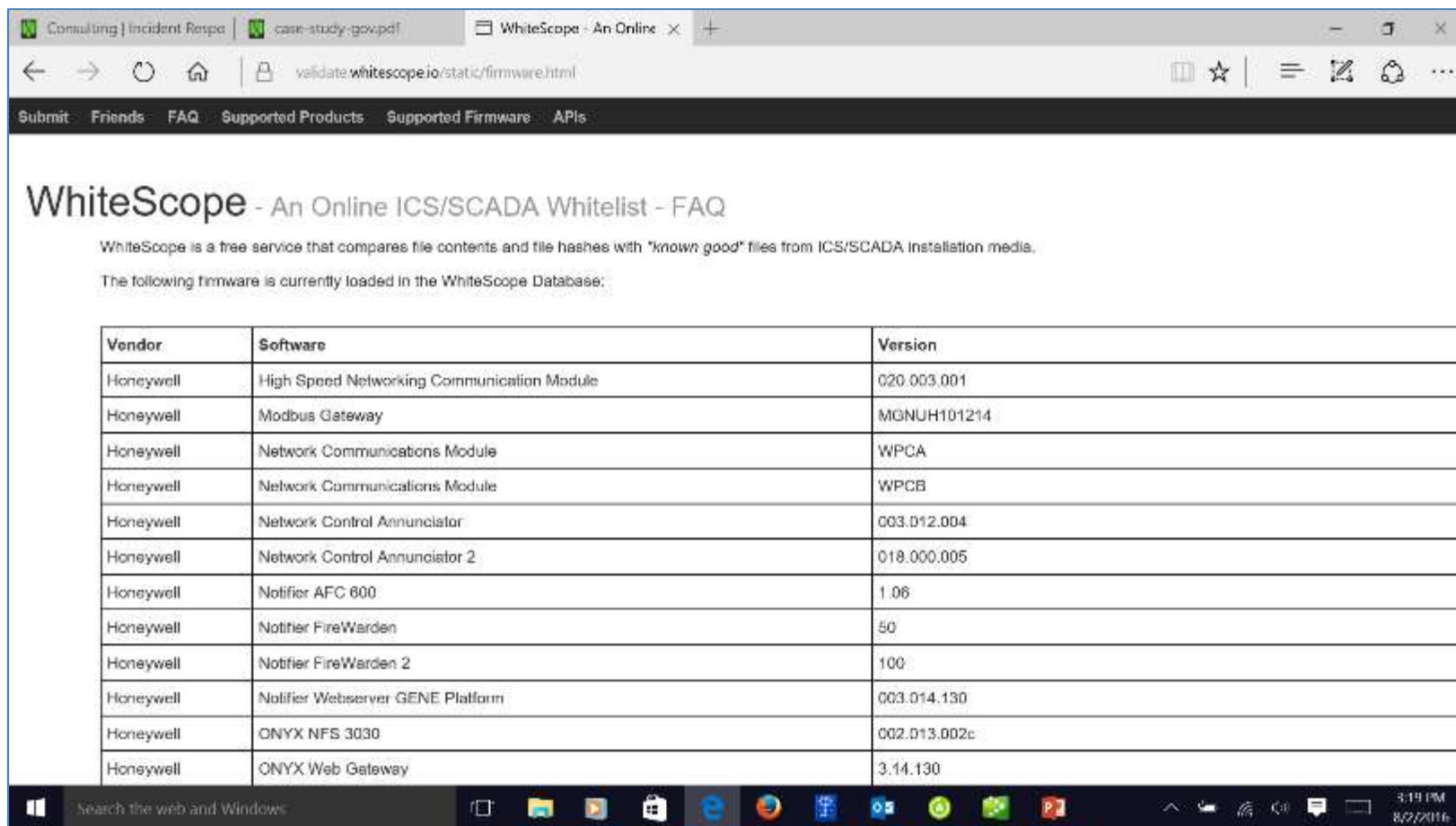
Severity	Name
Critical	User guest Has No Password

# WhiteScope Whitelist Products



<https://validate.whitescope.io/>

# WhiteScope Whitelist Firmware



The screenshot shows a web browser window with the URL `validate.whitescope.io/static/firmware.html`. The page title is "WhiteScope - An Online ICS/SCADA Whitelist - FAQ". Below the title, there is a description of the service and a statement that the following firmware is currently loaded in the database. A table follows, listing various Honeywell software products and their versions.

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.

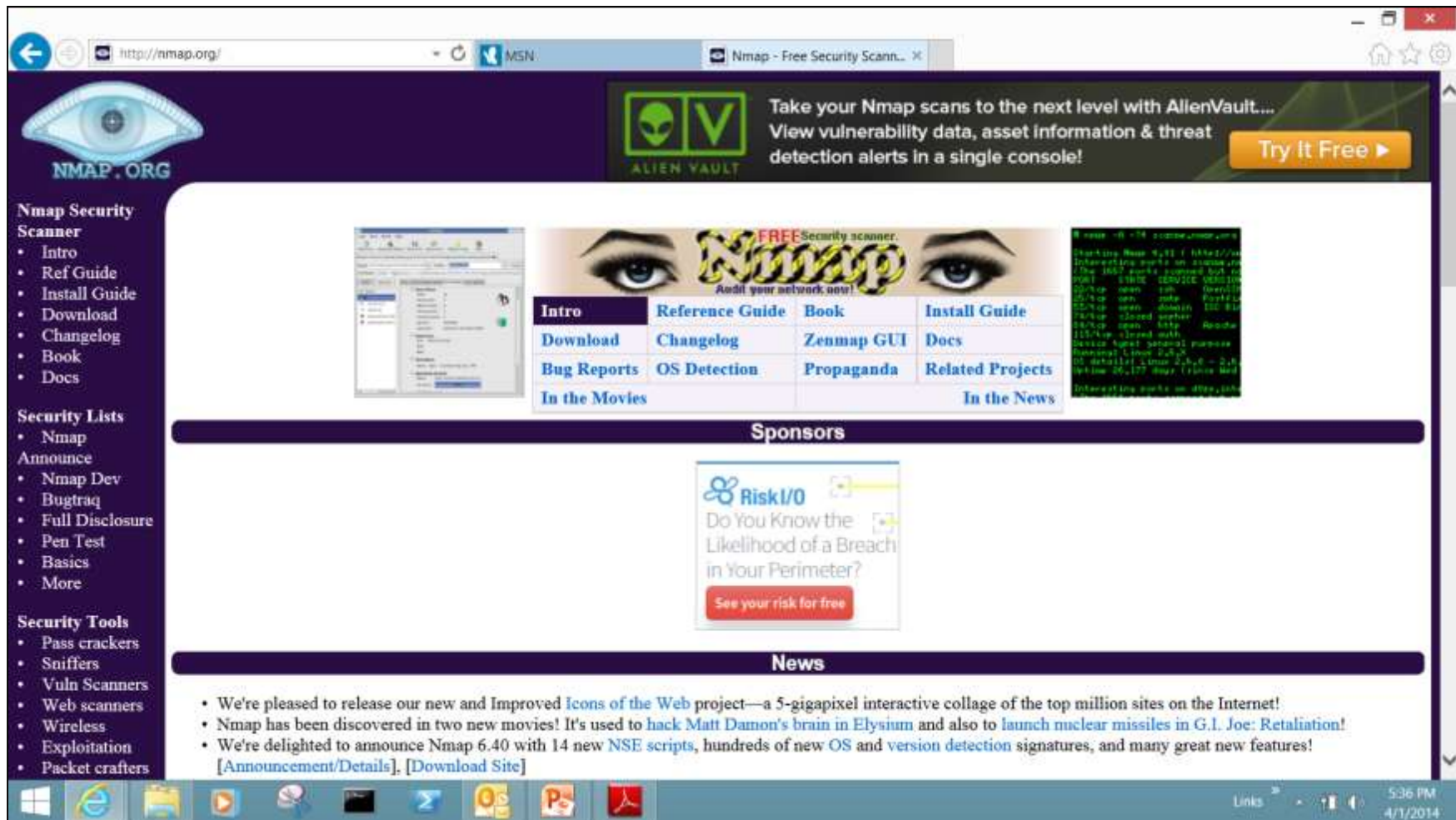
The following firmware is currently loaded in the WhiteScope Database:

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 800	1.06
Honeywell	Notifier FireWarden	50
Honeywell	Notifier FireWarden 2	100
Honeywell	Notifier Webserver GENE Platform	003.014.130
Honeywell	ONYX NFS 3030	002.013.002c
Honeywell	ONYX Web Gateway	3.14.130

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



# Nmap – Security Scanner



The screenshot shows the Nmap.org website in a web browser. The browser's address bar displays 'http://nmap.org/'. The website has a dark purple header with the Nmap logo (an eye) and the text 'NMAP.ORG'. A banner for 'AlienVault' is visible, with the text 'Take your Nmap scans to the next level with AlienVault... View vulnerability data, asset information & threat detection alerts in a single console!' and a 'Try It Free' button. Below the header, there is a central area with a large 'Nmap' logo and the text 'FREE Security scanner. Audit your network now!'. To the left of this central area is a sidebar with a list of links under the heading 'Nmap Security Scanner', including 'Intro', 'Ref Guide', 'Install Guide', 'Download', 'Changelog', 'Book', and 'Docs'. Below this is a section for 'Security Lists' with links like 'Nmap', 'Announce', 'Nmap Dev', 'Bugtraq', 'Full Disclosure', 'Pen Test', 'Basics', and 'More'. Further down is a 'Security Tools' section with links for 'Pass crackers', 'Sniffers', 'Vuln Scanners', 'Web scanners', 'Wireless', 'Exploitation', and 'Packet crafters'. To the right of the central 'Nmap' logo is a table with links: 'Intro', 'Reference Guide', 'Book', 'Install Guide', 'Download', 'Changelog', 'Zenmap GUI', 'Docs', 'Bug Reports', 'OS Detection', 'Propaganda', 'Related Projects', 'In the Movies', and 'In the News'. Below the table is a 'Sponsors' section featuring a Risk/I/O logo and the text 'Do You Know the Likelihood of a Breach in Your Perimeter? See your risk for free'. At the bottom is a 'News' section with three bullet points: 'We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million sites on the Internet!', 'Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to launch nuclear missiles in G.I. Joe: Retaliation!', and 'We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features!'. The bottom of the screenshot shows a Windows taskbar with various application icons and a system clock indicating 5:36 PM on 4/1/2014.

**Nmap Security Scanner**

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

**Security Lists**

- Nmap
- Announce
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

**Security Tools**

- Pass crackers
- Sniffers
- Vuln Scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters

**FREE Security scanner.**  
Audit your network now!

Intro	Reference Guide	Book	Install Guide
Download	Changelog	Zenmap GUI	Docs
Bug Reports	OS Detection	Propaganda	Related Projects
In the Movies			In the News

**Sponsors**

**Risk/I/O**  
Do You Know the Likelihood of a Breach in Your Perimeter?  
See your risk for free

**News**

- We're pleased to release our new and Improved [Icons of the Web](#) project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to [hack Matt Damon's brain in Elysium](#) and also to [launch nuclear missiles in G.I. Joe: Retaliation!](#)
- We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features! [\[Announcement/Details\]](#). [\[Download Site\]](#)

<http://nmap.org/>