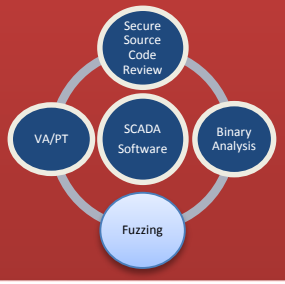
Vulnerability Assessments on SCADA Systems: Outsmarting the Smart Grid

Fadli B. Sidek
Security Specialist @
CODENOMICON

BSidesVienna 2014

Whoami

- HeartBleed Bug
- Security Engineer
- Software Security



- 8 years in IT
- S-O-E-C
- VA/PT
- Research
- Write Articles

- SecureSingapore
- Defcon Kerala (India)
- The Hackers Con (India)
- BSidesLV (USA)
- BSidesVienna

CODENOMICON

Legend

General Information

Technical Information

Something to refer to

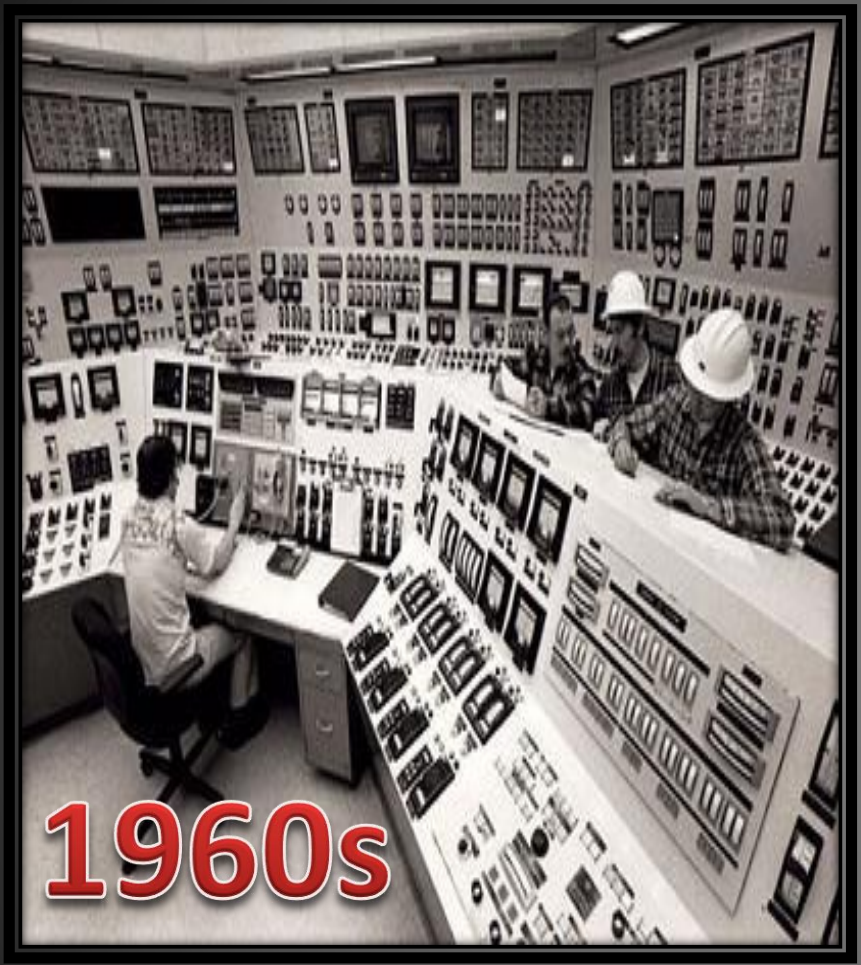
CODENOMICON

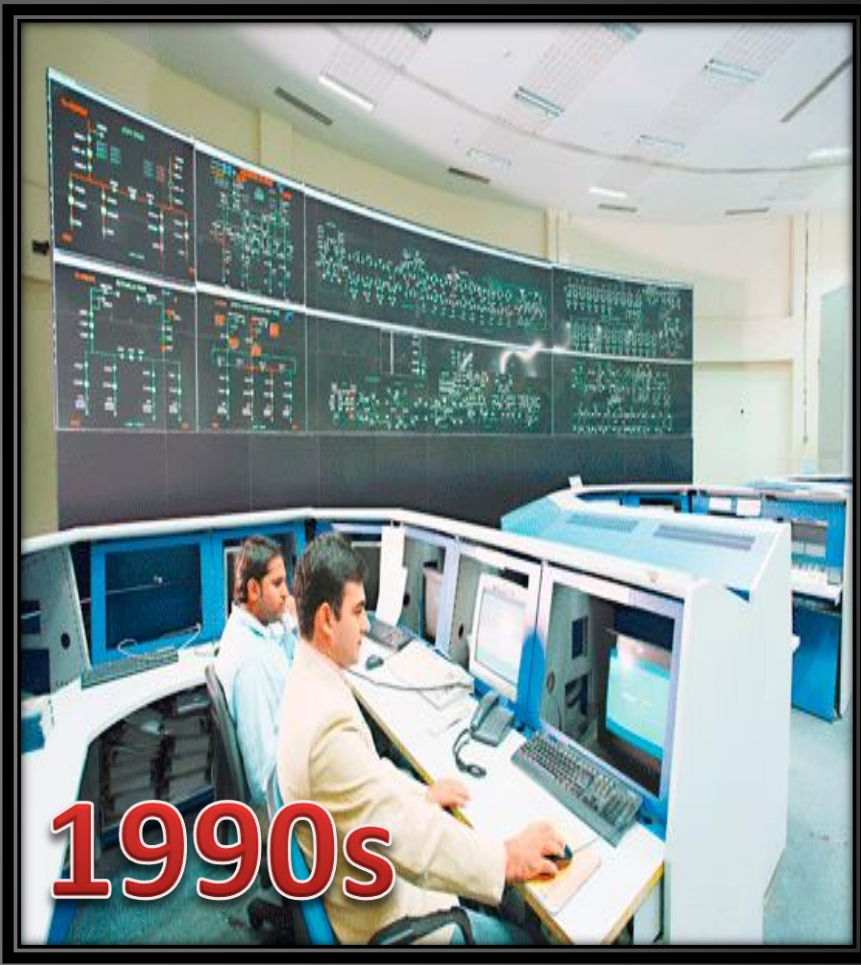
What is a Critical Infrastructure?

What is SCADA?

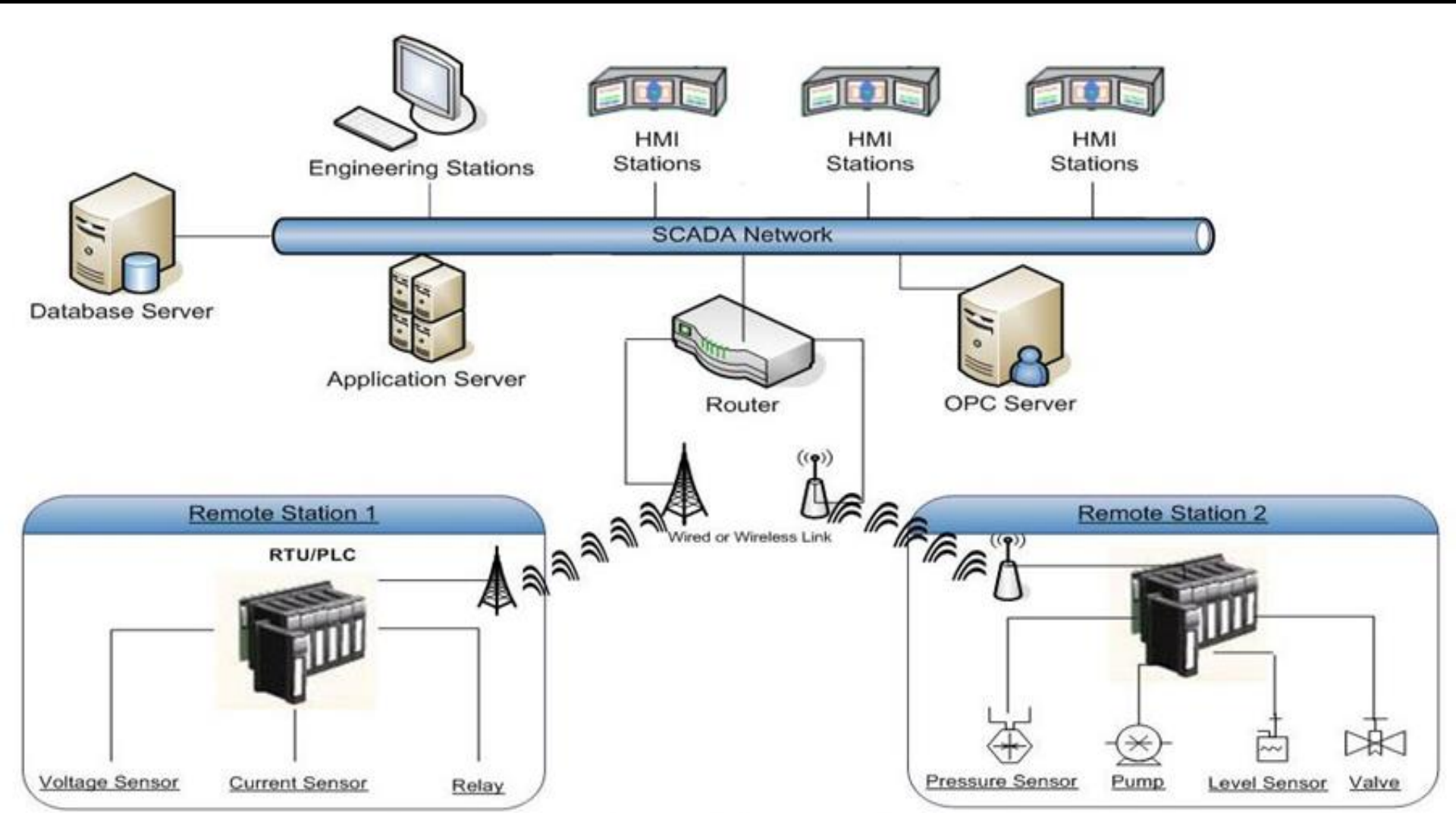
CODENOMICON

Typical SCADA Control Room





A Typical SCADA Network Architecture



What's the Big Deal?

CODENOMICON

Die Hard 4.0 – 4 real!!!

Be afraid: Die Hard 4 reveals a real threat

May 28, 2012 Comments 44 Read later

David Braue

Five years on, John McClane's security nightmare is not so sci-fi.

News › Technology › Internet

Eugene Kaspersky: major cyberterrorist attack is only matter of time

Nations must be ready for a remote attack on critical infrastructure, including power and transport systems, says security expert

A cyberterrorist attack is inevitable, says Eugene Kapersky. Photograph: Kaspersky Labs

"I watched the movie for 20 minutes, then pressed pause, got a cigarette and a glass of Scotch. To me it was really scary: they were talking about real scenarios. It was like a user guide for cyber terrorists. I hated that movie," the flamboyant Russian entrepreneur says.

CODENOMICON

ATTACKS!!!

Posted at 12:44 PM ET, 11/18/2011

Foreign hackers targeted U.S. water plant in apparent malicious cyber attack,

By Ellen Nakashima

Foreign hackers caused a pump at an Illinois
week, according to a preliminary state report.
attack, if confirmed, would be the first known t
the systems that supply Americans with water,
essentials of modern life.

Companies and government agencies that rel
years been routine targets of ha
from attempts to steal informatic
sites. The incident in Springfield
apparently caused physical des

Mysterious cyberattack compromises more than a thousand power plant systems

By Russell Brandom on June 30, 2014 01:39 pm Email @russellbrandom

DON'T MISS STORIES FOLLOW THE VERGE

TECHNOLOGY

Electricity Grid in U.S. Penetrated By Spies

Email Print 145 Comments A A

By SIOBHAN GORMAN

Updated April 8, 2009 11:59 p.m. ET

Growing Concerns Over Russian Hackers Targeting US Critical Infrastructure

By: Amanda Vicinanzo, Contributing Editor

07/05/2014 (12:01pm)

SHARE

week, the Department of Homeland Security (DHS) alerted critical infrastructure operators
sian hacking group known as "Energetic Bear," or "Dragonfly," as being behind an ongoing
ampaign primarily targeting the energy sector in the United States and Europe with the
capability to sabotage the power supply of the attacked countries.

DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), which works to reduce risks within and across all critical infrastructure sectors, issued the alert based on information received from two computer security companies, Symantec Corporation and Finland-based F-Secure. The companies indicated that Energetic Bear's attacks primarily target the US and Spain, followed by France, Italy, Germany, Turkey and Poland.

"ICS-CERT strongly recommends that organizations check their network logs for activity associated with this campaign," DHS said in an alert on its website.
ity related to this report should preserve available evidence for
orcement purposes."

DHS: America's water and power utilities under daily cyber-attack

DHS industrial-control systems (ICS) response team offers glimpse into how bad it is

Robert Moran mon
vulnerable to cyber

WASHINGTON
software progra
former national-

Report: Cyber Attacks Caused Power Outages in Brazil

WIRED

BY KEVIN POULSEN 11.07.09 | 12:55 AM | PERMALINK

CODENOMICON

And Despite All That...

Unisys Sur
Infrastruct
Past Year
Utility, oil and
ext

Critic
Defen
By Robert

ber-Attack

nies

Danielle Walker, Reporter

Follow @daniellewlkr

July 11, 2014

Study: Security not prioritized in critical infrastructure, though most admit compromise

Share this article:

In a study, most IT execs at critical infrastructure companies revealed that their organization was compromised in the last year, but only 28 percent of them said that security was a top priority across their enterprise.

Nearly 70 percent of critical infrastructure orgs said their company experienced a security compromise in the last year.

Nearly 600 global IT and IT security execs across 13 countries were polled for the "Critical Infrastructure: Security Preparedness and Maturity" report, released Thursday. And of those respondents, 67 percent said they had dealt with at least one security compromise, leading to the loss of confidential information or disruption to operations, at their companies.

The report (PDF), published jointly by global IT firm Unisys and the Ponemon Institute, aimed to shed light on how critical infrastructure organizations – including utilities and those serving the energy, manufacturing, and oil and gas sectors – addressed cyber security threats.

NSA finally admits!!!

China & others can cripple US power grid, NSA admits for the first time

Published time: November 20, 2014 18:52
Edited time: November 21, 2014 06:32

Get short URL

U.S. Navy Vice Admiral Michael S. Rogers (Reuters/U.S. Navy/Handout)

3.5K 540

The head of the National Security Agency warned Congress on Thursday that China and "one or two" other nations currently possess the capability of crippling the American power grid through cyberattacks.

Tags
China, Hacking, Information Technology, Intelligence, Internet, Security, USA

CODENOMICON

Security Professionals to the Rescue

CODENOMICON

What this talk is not about

Hacking SCADA Applications

Hacking SCADA Systems

Hacking SCADA Networks

Black Hat 2013 - Out of Control: Demonstrating SCADA Device Exploitation

by **HackersOnBoard** • 7 months ago • 599 views

Eric Forner + Brian Meixel.

HD

Black Hat 2013 - The SCADA That Didn't Cry Wolf - Who's Really Attacking Your ICS Devices - 2/2

by **HackersOnBoard** • 7 months ago • 430 views

Kyle Wilhoit.

HD

24C3: Hacking SCADA

by Christiaan008 • 3 years ago • 3,107 views

Speaker: mayhem, **Raoul** "Nobody" Chiesa how to own critical infrastructures **SCADA** acronym stand for "Supervisory Control And ...

nullcon Goa 2012: Attacking and Defending the Smart Grid - By Justin Searle

by **nullOxOO** • 2 years ago • 246 views

The Smart Grid brings greater benefits for electric utilities and customer alike, however these benefits come at a cost from a ...

HD

Black Hat USA 2010: Electricity for Free: The Dirty Underbelly of SCADA and Smart Meters 1/4

by **Christiaan008** • 3 years ago • 2,019 views

Speaker: Jonathan Pollet **SCADA** Systems control the generation, transmission, and distribution of electric power, and Smart ...

ConFidence 2011 - SCADA Hacking for Dummies

by **SecurityTubeCons** • 2 years ago • 1,702 views

This video is part of the Infosec Video Collection at SecurityTube.net: http://www.securitytube.net ConFidence 2011 - **SCADA** ...

CODENOMICON

Cos this is about

How I performed the VA

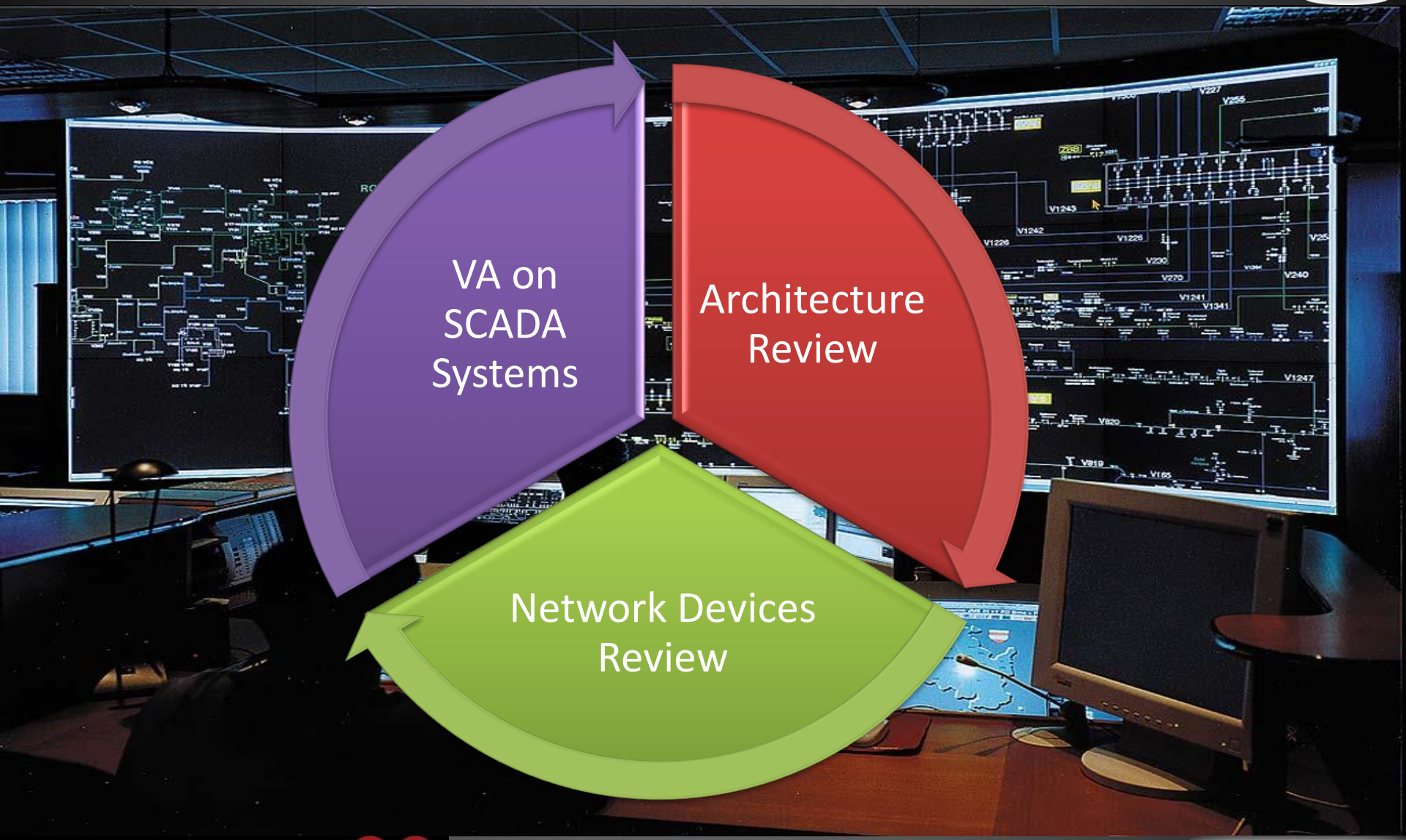
Share Assessment Findings

Types of Attacks on SCADA

Finding SCADA Systems Online

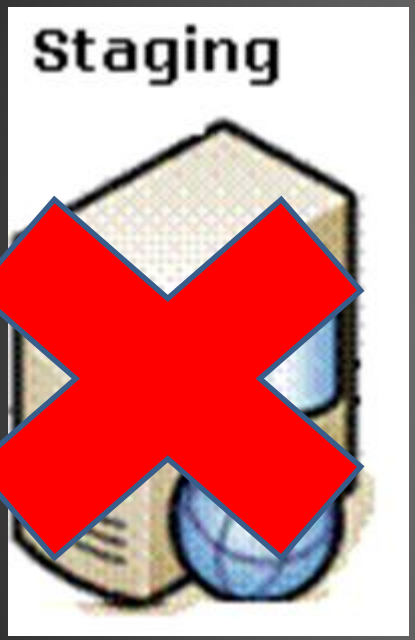
Compromising a Critical Infrastructure

What I've Done



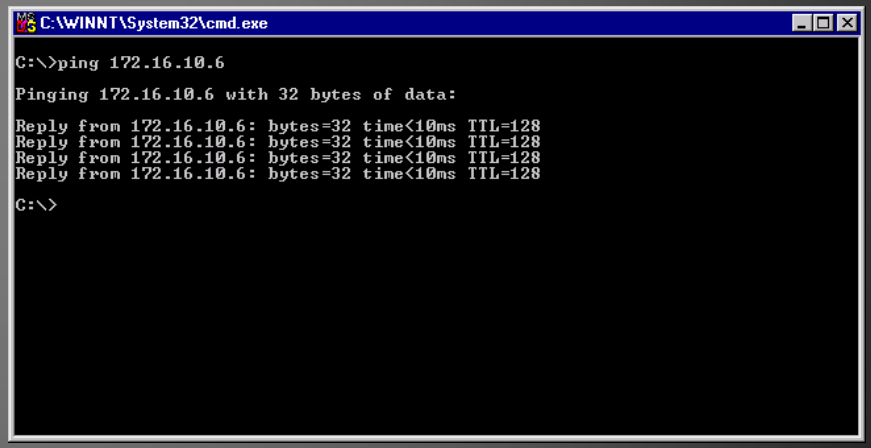
SCADA vs Corporate Environment

CAUTION

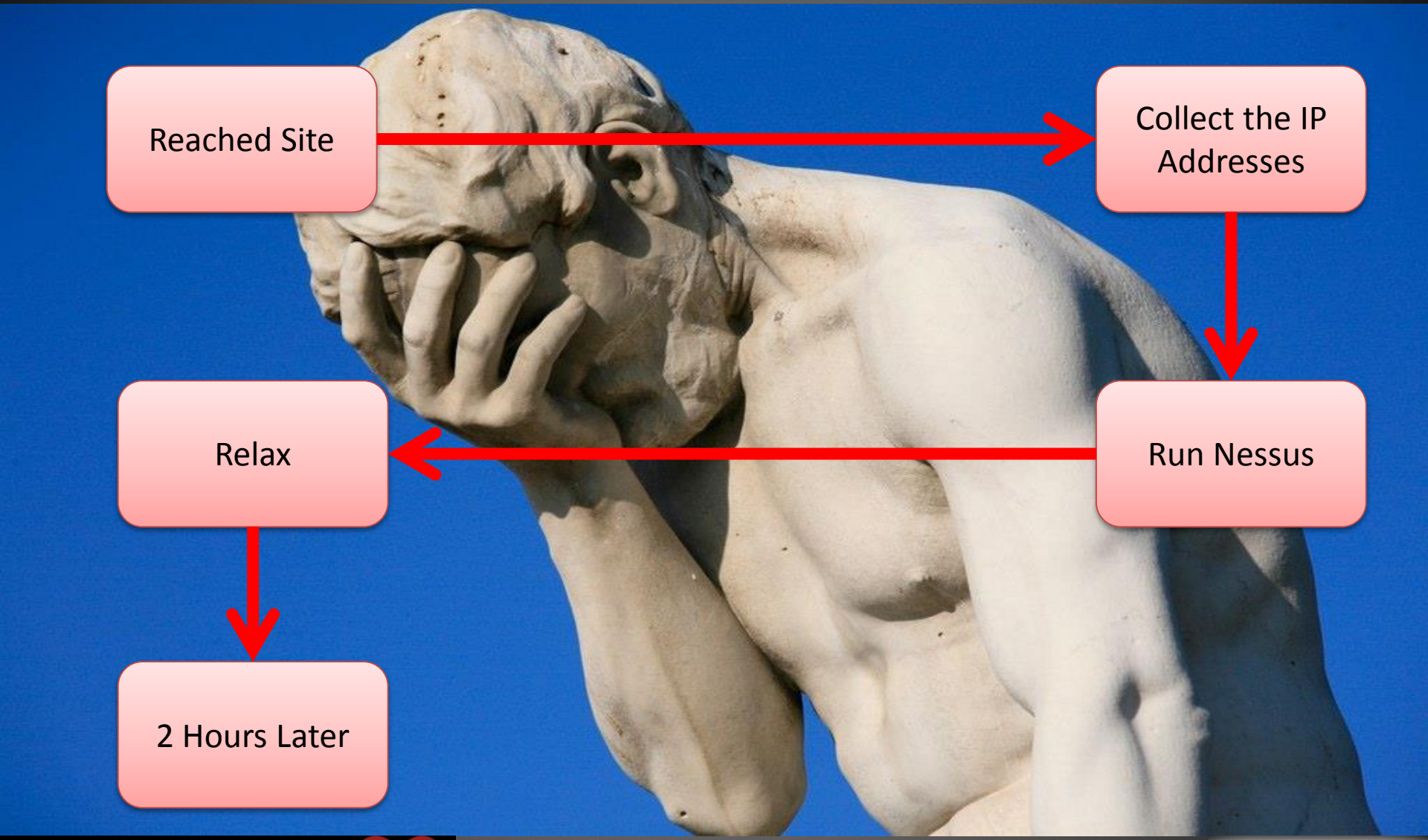


CODENOMICON

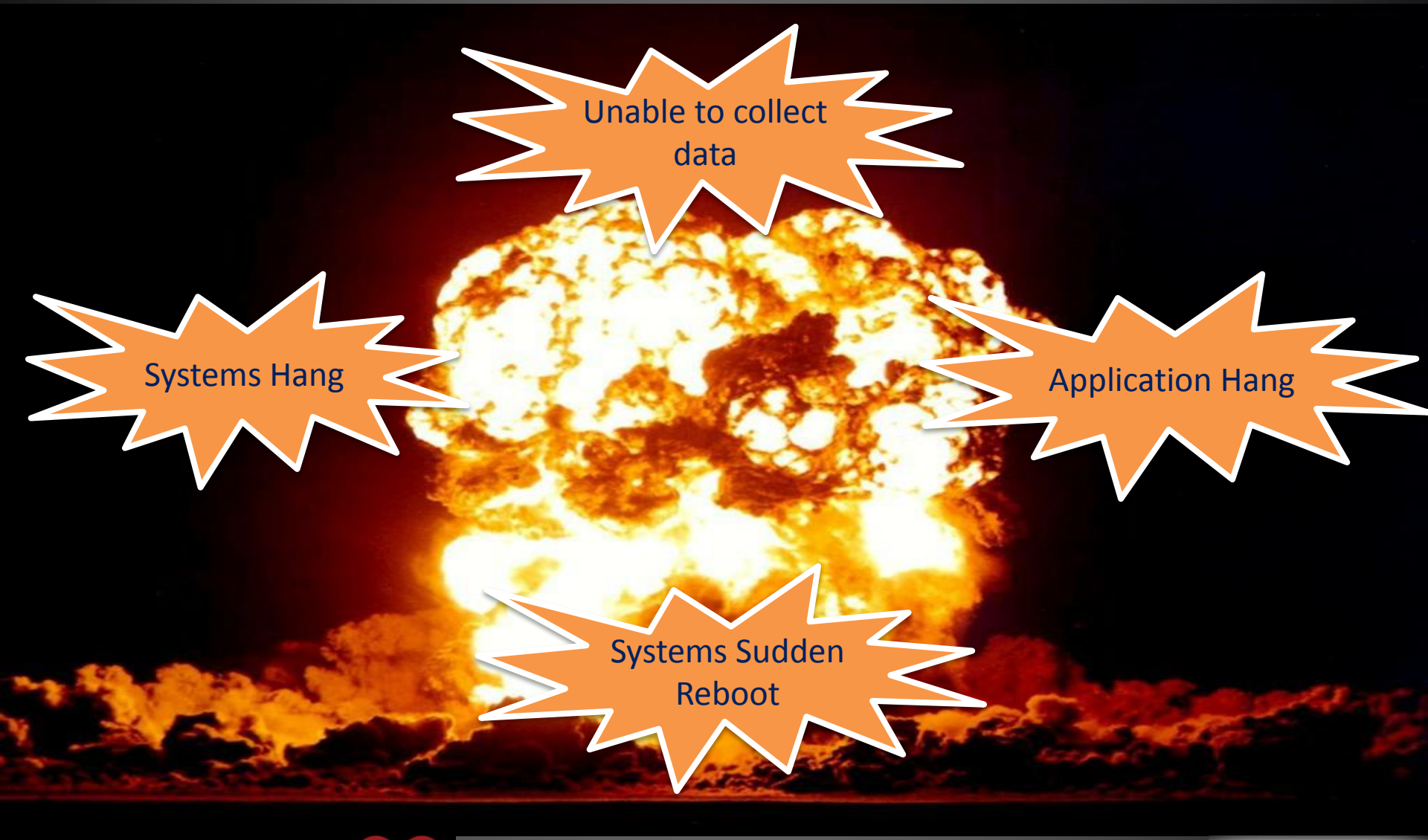
Automatic Tools used



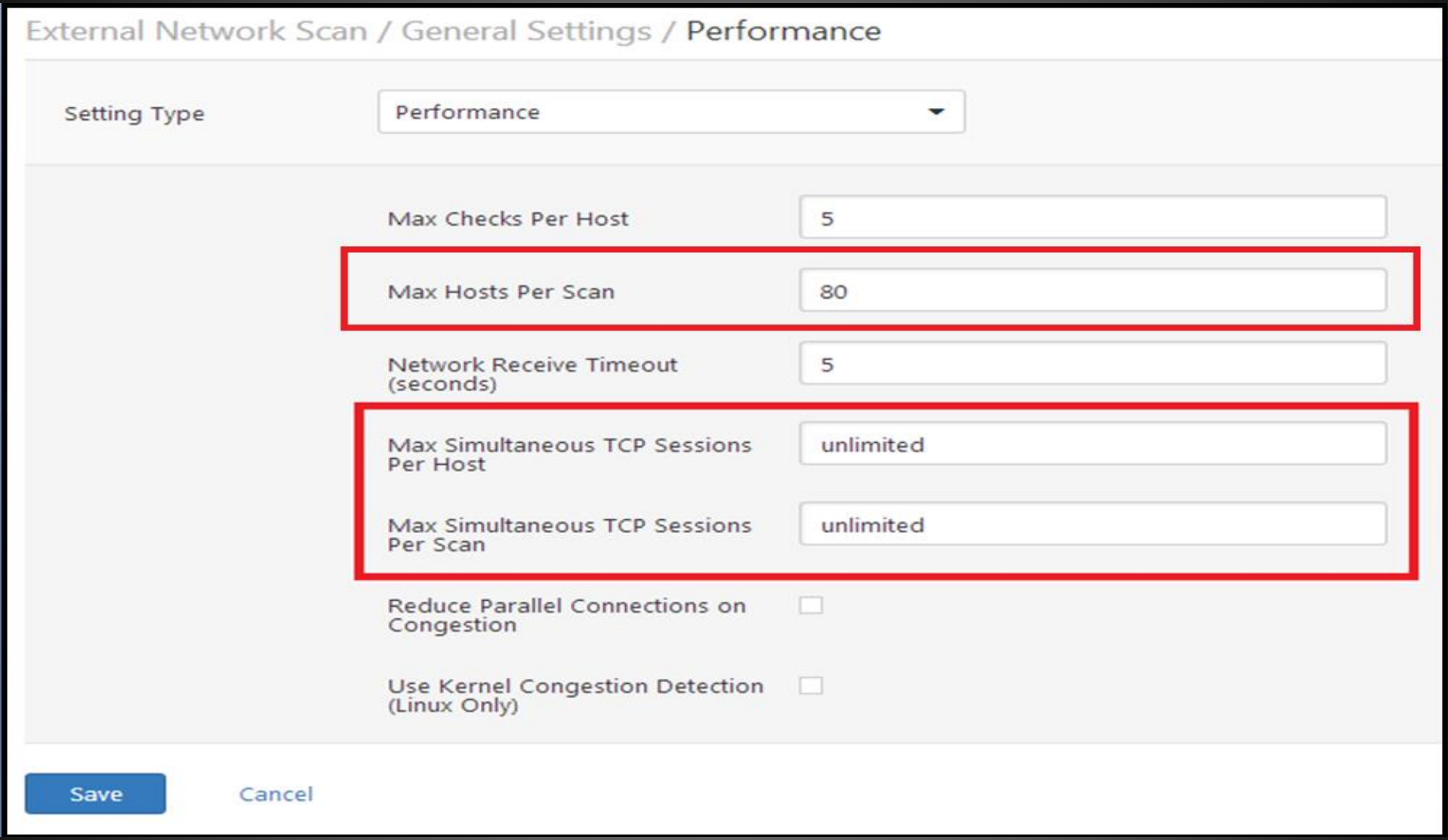
Day 1


Reached Site
Collect the IP Addresses
Run Nessus
Relax
2 Hours Later

The Impact


Unable to collect data
Systems Hang
Application Hang
Systems Sudden Reboot

Nessus Scanning Policies



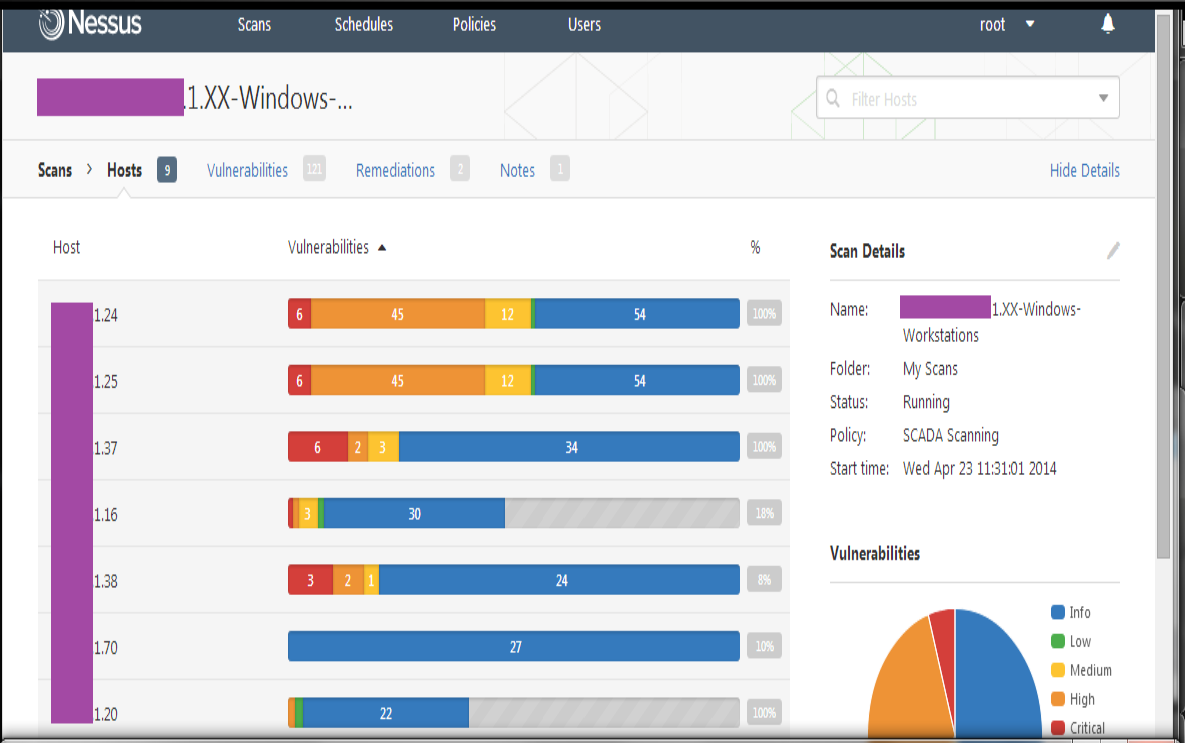
Nessus Plugins Selection

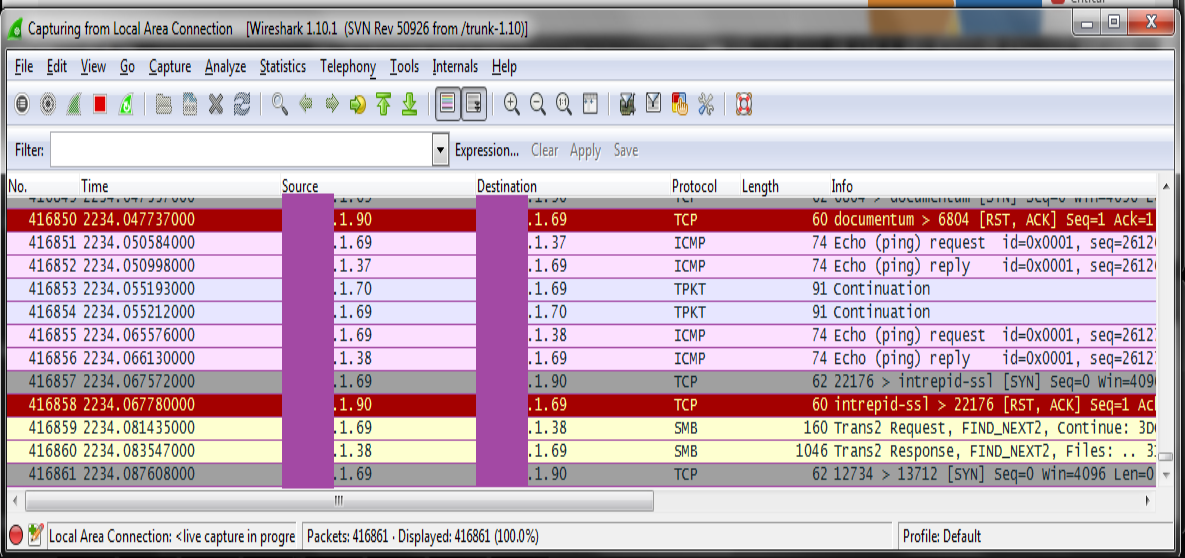
SCADA Scanning - Ultra Sensitive Windows / Plugins

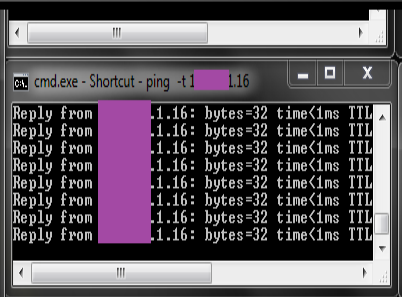
DISABLED	Oracle Linux Local Security Checks	1671
DISABLED	Palo Alto Local Security Checks	15
ENABLED	Peer-To-Peer File Sharing	71
DISABLED	Policy Compliance	32
DISABLED	Red Hat Local Security Checks	2901
ENABLED	RPC	36
ENABLED	SCADA	169
DISABLED	Scientific Linux Local Security Checks	1628

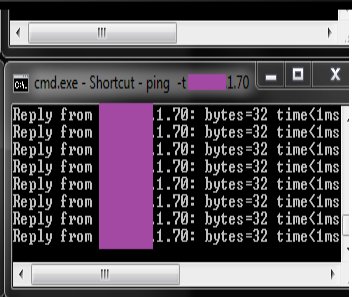
Save Cancel

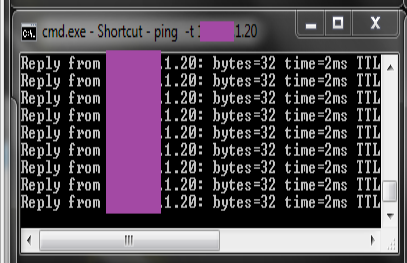
Day 2 - 10

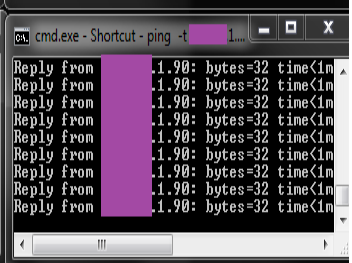

Nessus
Scans
Schedules
Policies
Users
root
[redacted]1.XX-Windows-...
Filter Hosts
Scans
Hosts 9
Vulnerabilities 121
Remediations 2
Notes 1
Hide Details
Host
Vulnerabilities
%
1.24 6 45 12 54 100%
1.25 6 45 12 54 100%
1.37 6 2 3 34 100%
1.16 3 30 18%
1.38 3 2 1 24 8%
1.70 27 10%
1.20 22 100%
Scan Details
Name: [redacted]1.XX-Windows-Workstations
Folder: My Scans
Status: Running
Policy: SCADA Scanning
Start time: Wed Apr 23 11:31:01 2014
Vulnerabilities
Info
Low
Medium
High
Critical

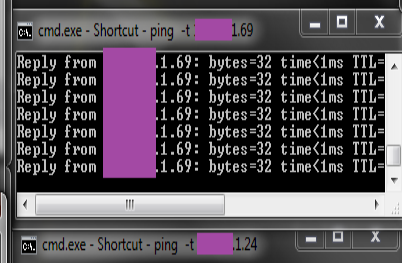

Capturing from Local Area Connection [Wireshark 1.10.1 (SVN Rev 50926 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
416850 2234.047737000 [redacted].1.90 [redacted].1.69 TCP 60 documentum > 6804 [RST, ACK] Seq=1 Ack=1
416851 2234.050584000 [redacted].1.69 [redacted].1.37 ICMP 74 Echo (ping) request id=0x0001, seq=2612
416852 2234.050998000 [redacted].1.37 [redacted].1.69 ICMP 74 Echo (ping) reply id=0x0001, seq=2612
416853 2234.055193000 [redacted].1.70 [redacted].1.69 TPKT 91 Continuation
416854 2234.055212000 [redacted].1.69 [redacted].1.70 TPKT 91 Continuation
416855 2234.065576000 [redacted].1.69 [redacted].1.38 ICMP 74 Echo (ping) request id=0x0001, seq=2612
416856 2234.066130000 [redacted].1.38 [redacted].1.69 ICMP 74 Echo (ping) reply id=0x0001, seq=2612
416857 2234.067572000 [redacted].1.69 [redacted].1.90 TCP 62 22176 > intrepid-ssl [SYN] Seq=0 Win=409
416858 2234.067780000 [redacted].1.90 [redacted].1.69 TCP 60 intrepid-ssl > 22176 [RST, ACK] Seq=1 Ac
416859 2234.081435000 [redacted].1.69 [redacted].1.38 SMB 160 Trans2 Request, FIND_NEXT2, Continue: 3D
416860 2234.083547000 [redacted].1.38 [redacted].1.69 SMB 1046 Trans2 Response, FIND_NEXT2, Files: .. 3
416861 2234.087608000 [redacted].1.69 [redacted].1.90 TCP 62 12734 > 13712 [SYN] Seq=0 Win=4096 Len=0
Local Area Connection: <live capture in progre
Packets: 416861 · Displayed: 416861 (100.0%)
Profile: Default

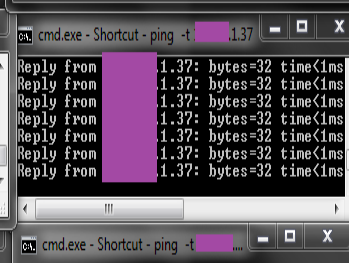

cmd.exe - Shortcut - ping -t [redacted]1.16
Reply from [redacted].1.16: bytes=32 time<1ms TTL

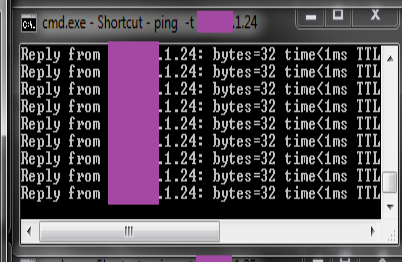

cmd.exe - Shortcut - ping -t [redacted]1.70
Reply from [redacted].1.70: bytes=32 time<1ms

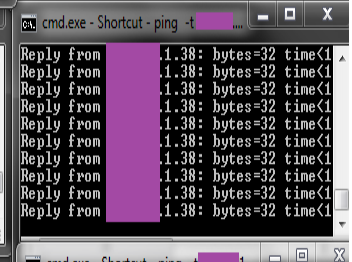

cmd.exe - Shortcut - ping -t [redacted]1.20
Reply from [redacted].1.20: bytes=32 time=2ms TTL

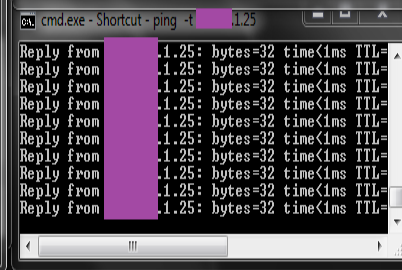

cmd.exe - Shortcut - ping -t [redacted]1.90
Reply from [redacted].1.90: bytes=32 time<1ms

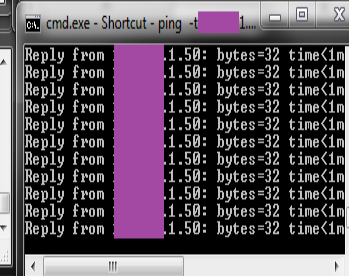

cmd.exe - Shortcut - ping -t [redacted]1.69
Reply from [redacted].1.69: bytes=32 time<1ms TTL


cmd.exe - Shortcut - ping -t [redacted].1.37
Reply from [redacted].1.37: bytes=32 time<1ms


cmd.exe - Shortcut - ping -t [redacted]1.24
Reply from [redacted].1.24: bytes=32 time<1ms TTL

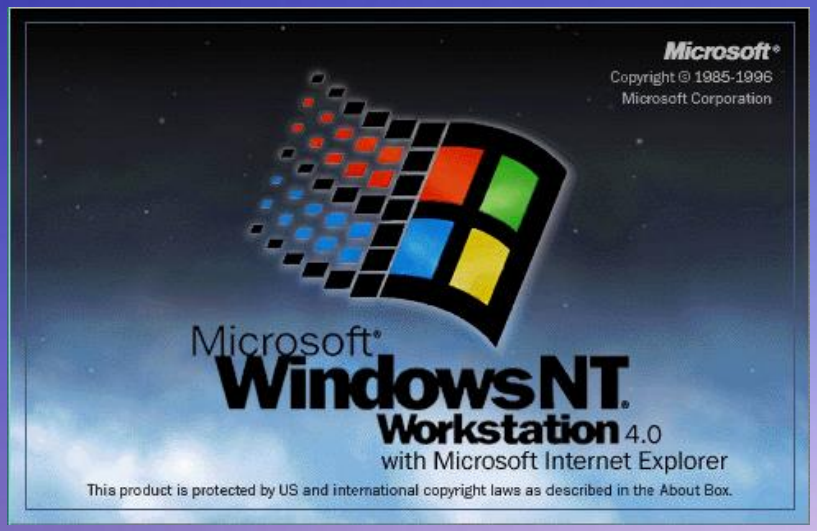

cmd.exe - Shortcut - ping -t [redacted]
Reply from [redacted].1.38: bytes=32 time<1


cmd.exe - Shortcut - ping -t [redacted]1.25
Reply from [redacted].1.25: bytes=32 time<1ms TTL


cmd.exe - Shortcut - ping -t [redacted]1...
Reply from [redacted].1.50: bytes=32 time<1m

Day 11

Ancient & Unsupported OS & Hardware



CODENOMICON

Techniques

Table 4-1. Suggested Actions for ICS Vulnerability Assessments

To Be Identified	Usual IT Action	Suggested ICS Actions
Hosts, nodes, and networks	Ping sweep (e.g., nmap)	• Examine router configuration files or route tables • Perform physical verification (chasing wires) • Conduct passive network listening or use intrusion detection (e.g., snort) on the network • Specify a subset of IP addresses to be programmatically scanned
Services	Port scan (e.g., nmap)	• Do local port verification (e.g., netstat) • Scan a duplicate, development, or test system on a non-production network
Vulnerabilities within a service	Vulnerability scan (e.g., nessus)	• Perform local banner grabbing with version lookup in Common Vulnerabilities and Exposures (CVE) • Scan a duplicate, development, or test system on a non-production network

Methodology

Validate non intrusion vulnerabilities

Validation

Scan the systems by
- Individual
- Groups
- Sites
- Operating Systems
- Active/Passive/Backups

Scanning

Select plugins based on
- Operating systems
- Applications
- Devices (Network)

Policy & Plugins

Segregate systems based on
- Servers
- Workstations
- Network Devices
- Operating Systems
- Redundancy/failovers

Groupings

- Interviewing
- Documentation
- Live Hosts
- OS fingerprinting
- Systems Specification (HD size/Ram)

Information Gathering

Reporting

SCADA Assessment Incidents

- **Vulnerability Scanner Incidents[13].** While a ping sweep was being performed on an active SCADA network that controlled 3 meter (9 foot) robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated. In a separate incident, a ping sweep was being performed on an ICS network to identify all hosts that were attached to the network, for inventory purposes, and it caused a system controlling the creation of integrated circuits in the fabrication plant to hang. This test resulted in the destruction of $50,000 worth of wafers. See Section 4.2.6 for additional guidance on ICS vulnerability assessments.

- **Penetration Testing Incident[14].** A natural gas utility hired an IT security consulting organization to conduct penetration testing on its corporate IT network. The consulting organization carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours. The outcome was the loss of service to its customer base for those four hours.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
Special Publication 800-82

Vulnerabilities Found

CRITICAL	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)
CRITICAL	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)
CRITICAL	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)
CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
CRITICAL	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)
CRITICAL	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)
CRITICAL	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)
CRITICAL	Oracle Database Unsupported
HIGH	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)
HIGH	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)
HIGH	SNMP Agent Default Community Name (public)
HIGH	Unsupported Web Server Detection
HIGH	Microsoft Windows SMB Shares Unprivileged Access
HIGH	Oracle Database Multiple Remote Vulnerabilities (Mar 2005)
HIGH	Oracle Net Services CREATE DATABASE LINK Query Overflow
MEDIUM	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	Microsoft Windows SMB NULL Session Authentication
MEDIUM	HTTP TRACE / TRACK Methods Allowed
MEDIUM	Microsoft Windows SMB Guest Account Local User Access
MEDIUM	MS06-008: Vulnerability in Web Client Service Could Allow Remote Code Execution (911927) (uncredentialed check)

Additional Findings:

- Default Admin Password
- Default Cisco Password
- Blank Passwords
- Default Web Server Passwords
- Anonymous FTP
- Obsolete OS (NT4.0, XP)
- 64MB/128MB RAM
- Old Hardware

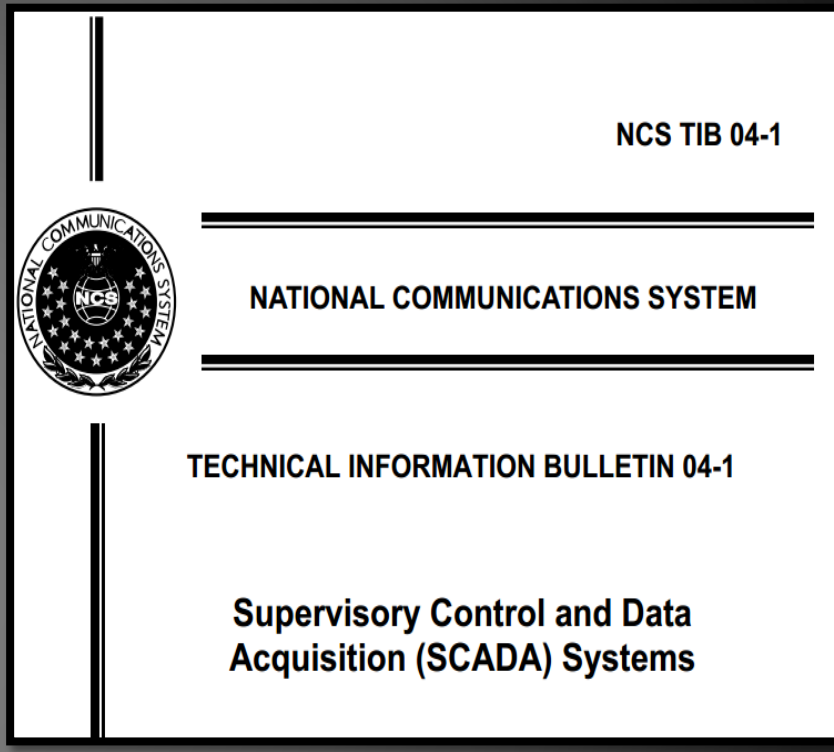
CODENOMICON

Vulnerabilities Found

CRITICAL	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)
CRITICAL	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)
CRITICAL	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)
CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
CRITICAL	MS10-012: Vulnerabilities in SMB Could Allow Remote Code Execution (971468) (uncredentialed check)
CRITICAL	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)
CRITICAL	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)
CRITICAL	Oracle Database Unsupported

SCADA Attack Matrix

Description of Attack	Type of Attack	Attack Motive	Impact to Victim
Change Data Points or Change Setpoint(s) in SCADA System	Information Tampering	Desire to modify corporate data or process setpoints for malicious purposes	Higher impact since modified setpoint or control points can have adverse effects on controlled process, and potentially cause a shutdown condition
Log any Operational or Corporate data for personal gain or sell to competition or hold as ransom	Information Mining	Try to steal corporate data and either sell to other companies or hold for ransom amount	Low environmental or immediate damage, but can damage corporate image if attacker builds attention to the fact that this system was compromised
Modify Data points on SCADA graphics to deceive Operators that system is out of control and must ESD (Emergency Shut Down)	System Shutdown	Cause danger to the facility or company by staging a false alarm shutdown of the plant or facility	Operations can no longer trust the SCADA System, and the attacker has deceived the Operator into thinking that there was an emergency condition in the plant



CODENOMICON

SCADA Attack Matrix

Description of Attack	Type of Attack	Attack Motive	Impact to Victim
Denial of Service	System Shutdown	Wish to take down server and cause immediate shutdown situation	SCADA Server locks up and must be rebooted. When SCADA Server comes back on-line, it locks up again. Operations can no longer monitor or control process conditions, and the system will ultimately need to be shut down
Delete System Files (Low-level format on all local drives)	System Shutdown	Wish to take down server and cause immediate shutdown situation	Critical Server and SCADA files are lost and operations can no longer monitor process or control plant or facility
Take Control of SCADA System	Gain Control	Gain control of SCADA System to impact damage on industrial systems, possibly causing environmental impact, and damage corporate identity through public exposure	Highest impact, since attacker can then manually override safety systems, shut down the system, or takes control of the plant operational conditions.
Log Keystrokes, Usernames, Passwords, System Setpoints, and any Operational Information	Information Mining	Gain Information for future attacks or satisfy curiosity	Lower immediate impact, but information gained can be used for future attacks.

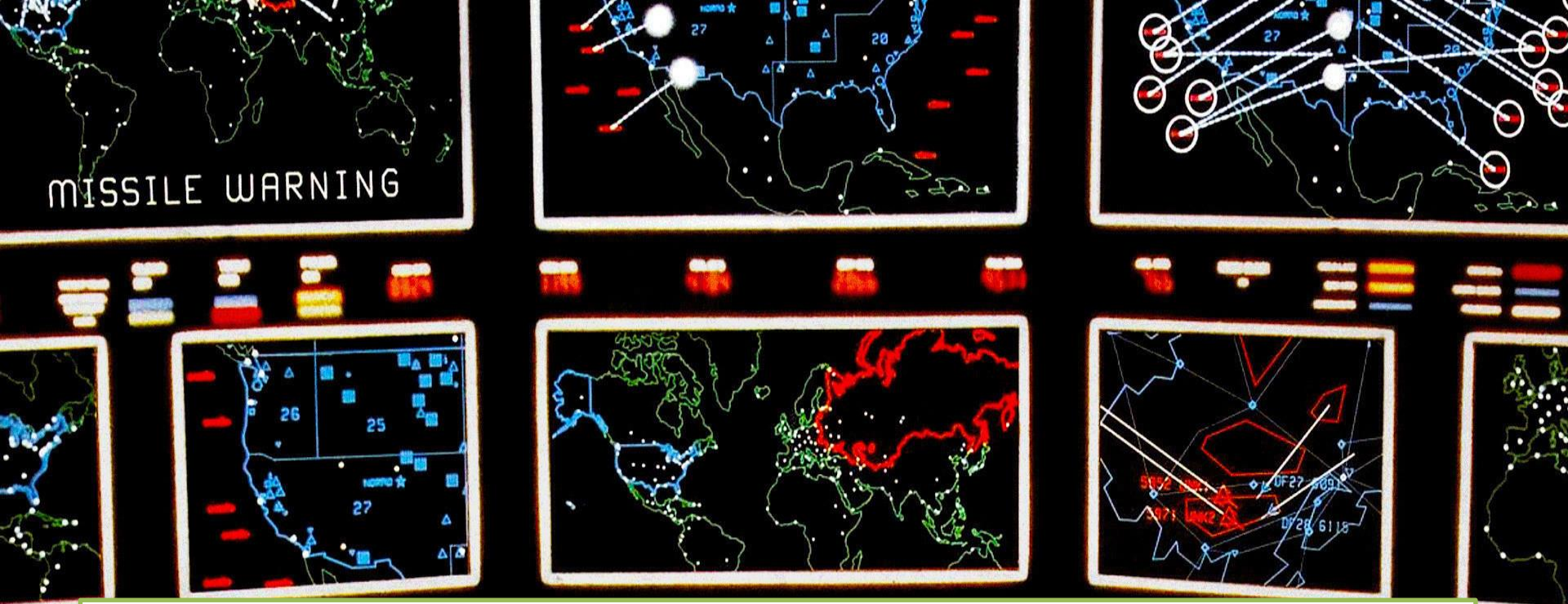
NCS TIB 04-1

NATIONAL COMMUNICATIONS SYSTEM

TECHNICAL INFORMATION BULLETIN 04-1

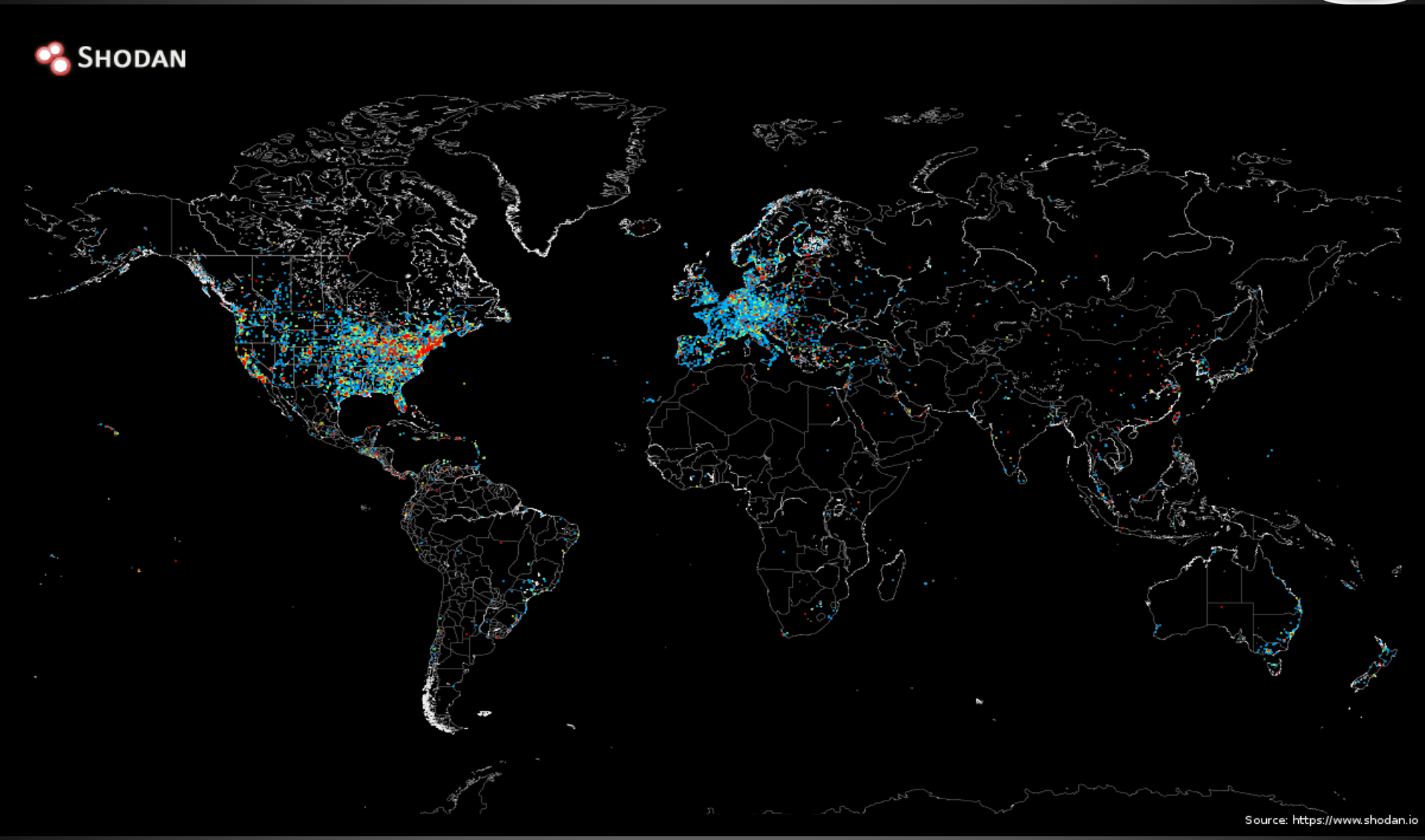
Supervisory Control and Data Acquisition (SCADA) Systems

CODENOMICON

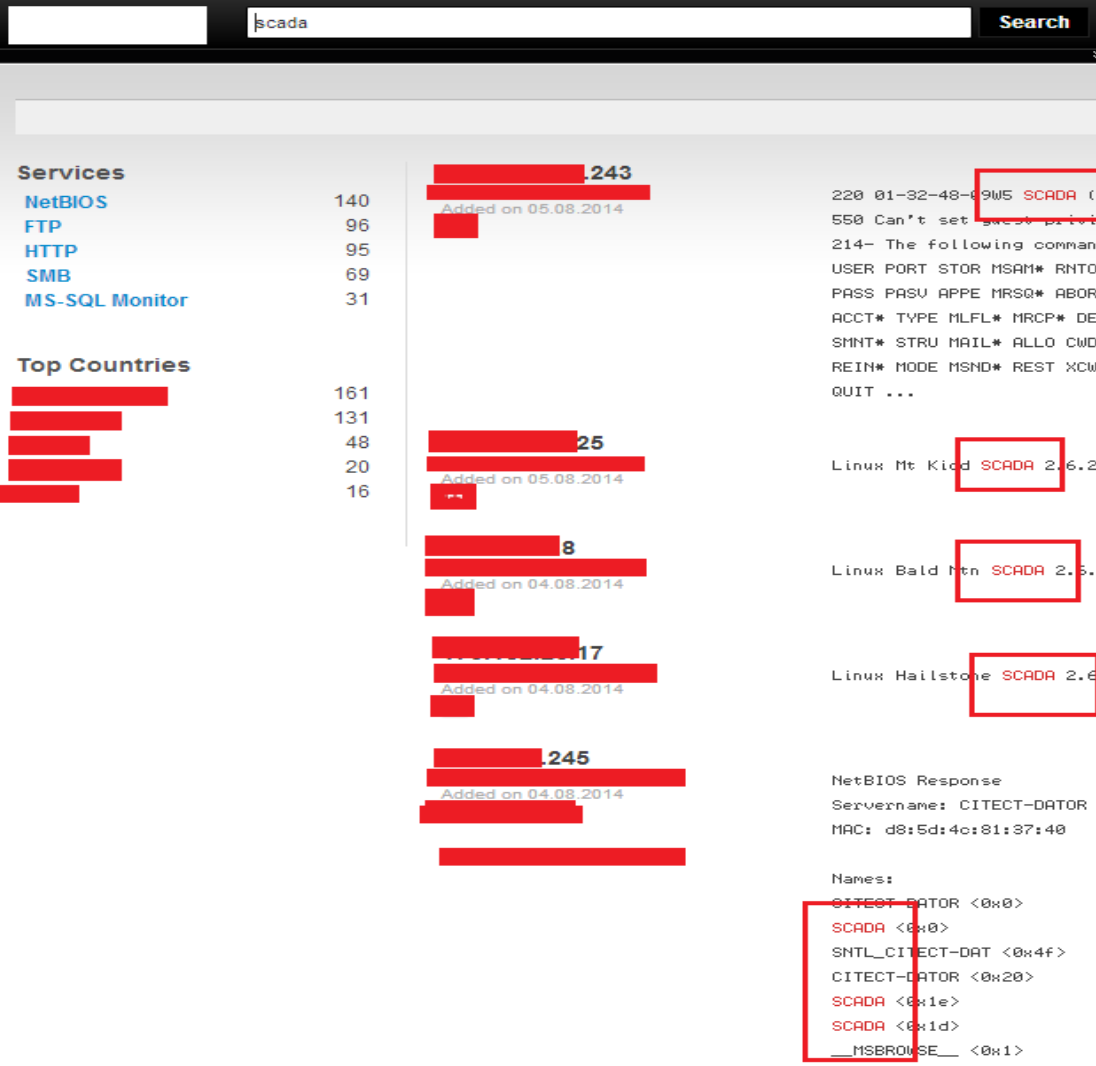


Thank God SCADA systems are Isolated and not part of the Internet..... But hang on....

Map of ICS/SCADA Systems on the Internet

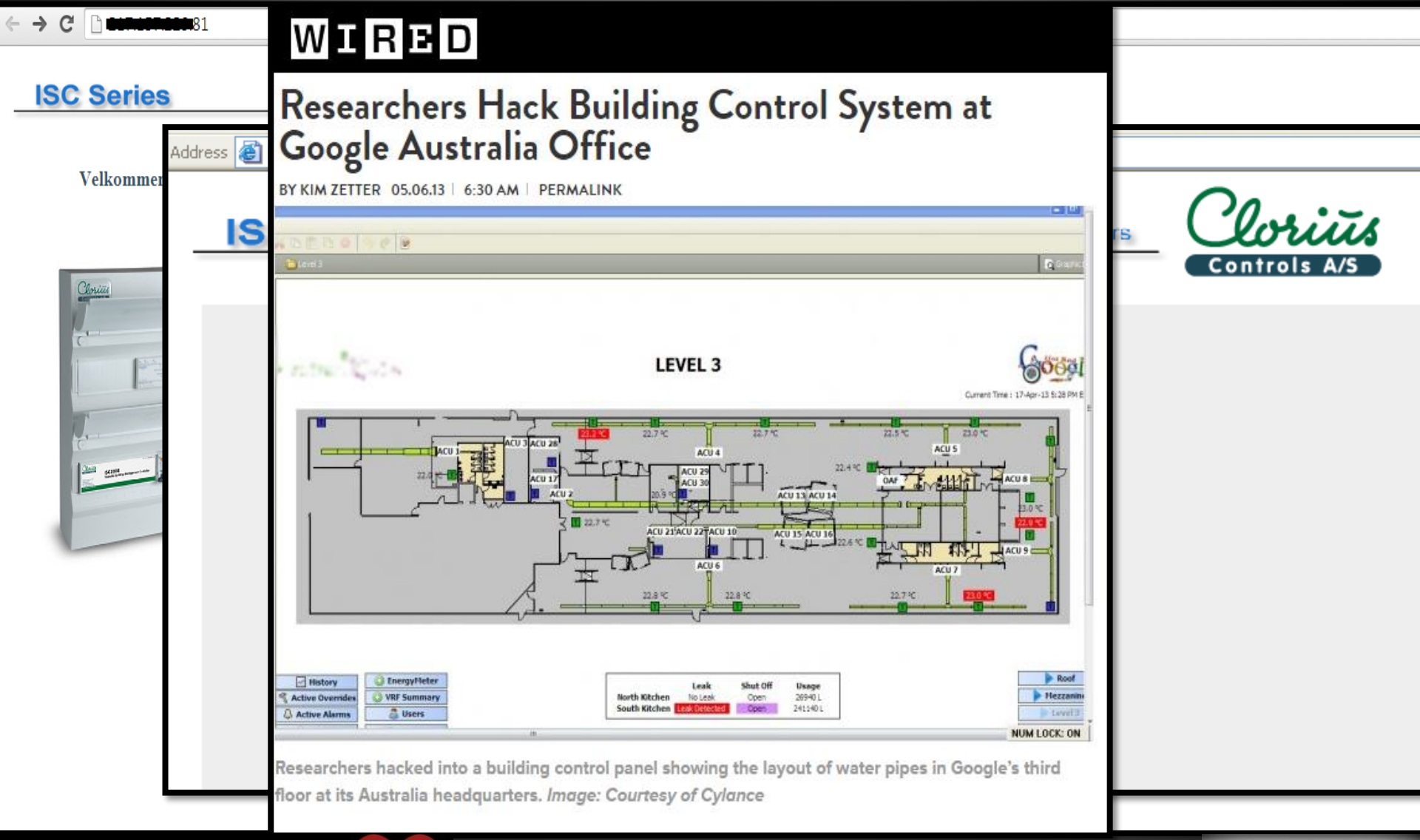


Searching for SCADA Systems in the Internet



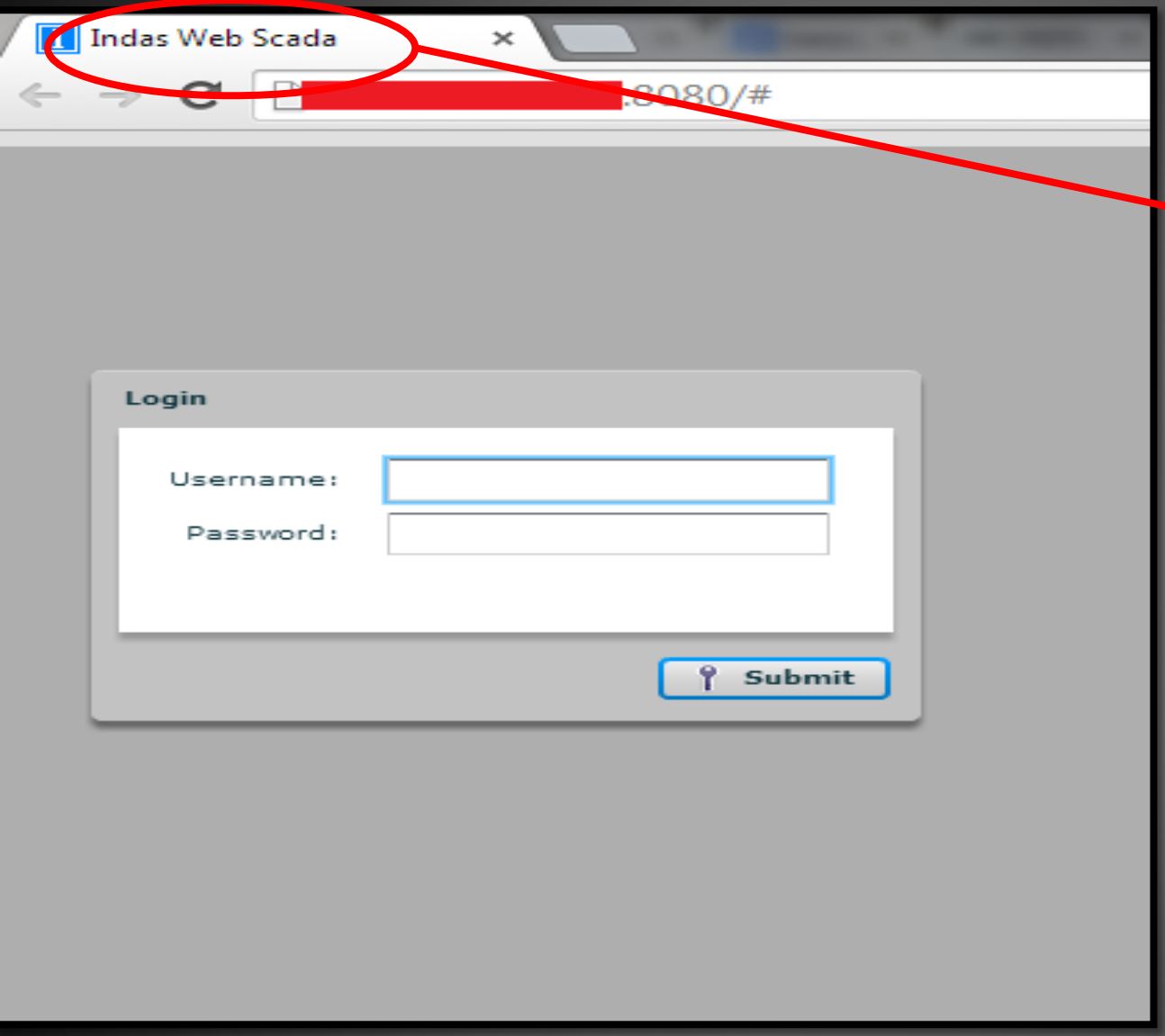
CODENOMICON

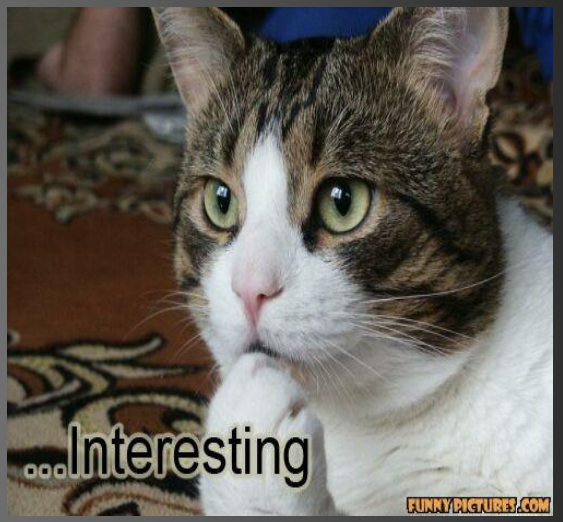
SCADA Login Console



CODENOMICON

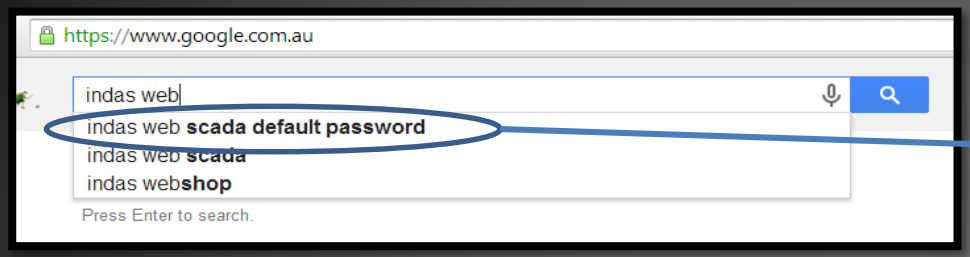
SCADA Login Console

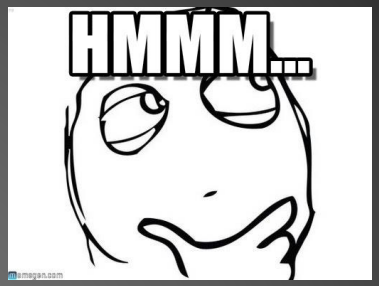


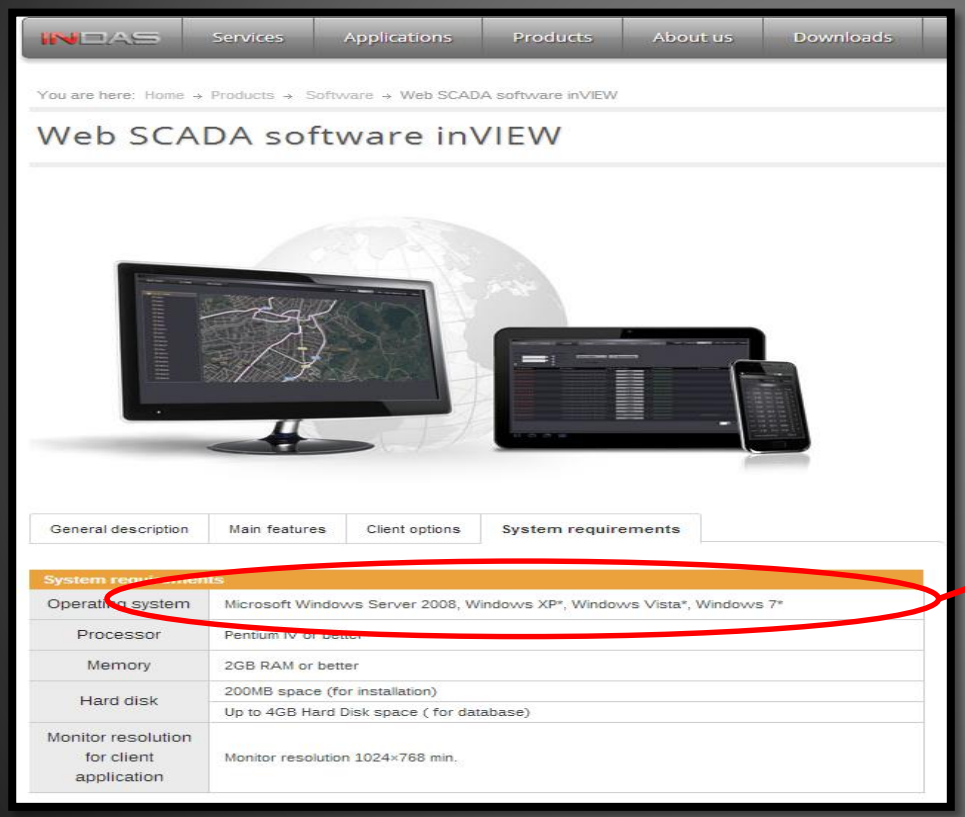


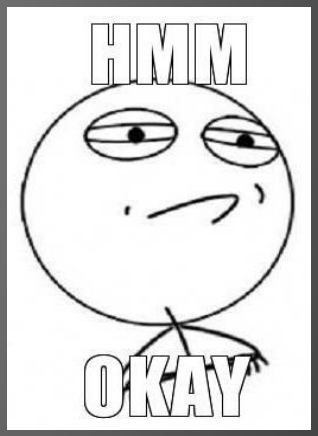
CODENOMICON

Reconnaissance on SCADA Application



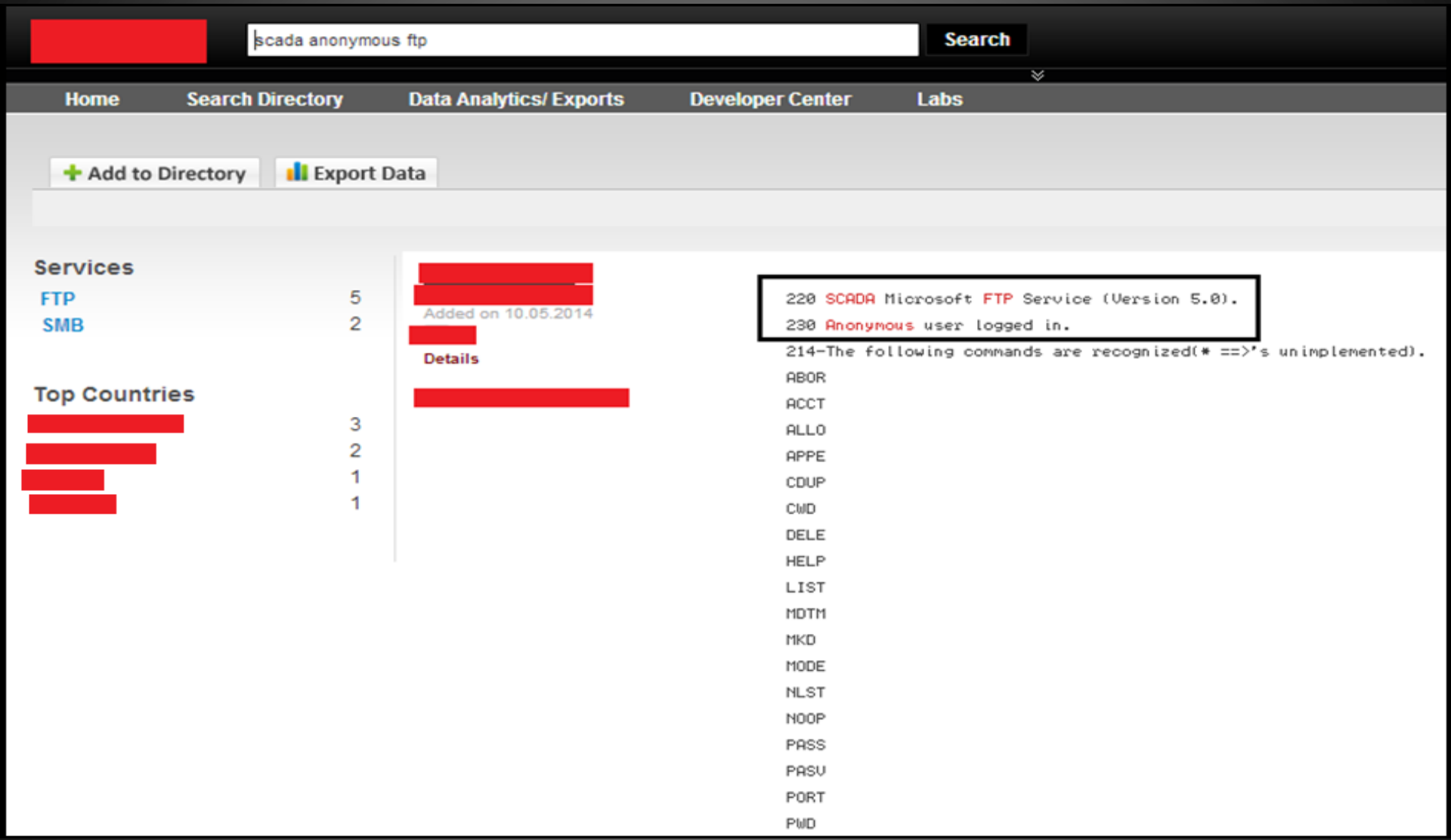






CODENOMICON

Anonymous FTP Access in SCADA Systems



CODENOMICON

Finding Application Vulns in SCADA Systems

SHODAN

scada proftpd

Search

Home | Search Directory | Data Analytics/ Exports | Developer Center | Labs

Add to Directory | Export Data

[redacted]
Added on 04.05.2014
Columbus
Details

220 ProFTPD 1.3.3c Server (Scada) [redacted]
530 Login incorrect.
214-The following commands are recognized (* =>'s unimplemented):
CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV
EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD
XRMD MKD XMKD PWD XPWD SIZE SYST HELP
NOOP FEAT OPTS AUTH* CCC* CONF* ENC* MIC*
PBSZ* PROT* TYPE STRU MODE RETR STOR STOU
APPE ...

[redacted]
Added on 29.04.2013
Details

220 ProFTPD 1.3.3d Server (Scada) [redacted]
530 Login incorrect.
214-The following commands are recognized (* =>'s unimplemented):
214-CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV
214-EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD
214-XRMD MKD XMKD PWD XPWD SIZE SYST HELP
214-NOOP FEAT OPTS AUTH* CCC* CONF* ENC* MIC*
214-PBSZ* PROT* TYPE STRU MODE RETR STOR STOU
214-APPE R...

CODENOMICON

Check Version Against CVEs

Proftpd » Proftpd » 1.3.3 RC1 : Security Vulnerabilities

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2012-6095	362			2013-01-24	2013-01-25	1.2	None	Local	High	Not required	None	Partial	None
ProFTPD before 1.3.5rc1, when using the UserOwner directive, allows local users to modify the ownership of arbitrary files via a race condition and a symlink attack on the (1) MKD or (2) XMKD commands.														
2	CVE-2011-4130	399		Exec Code	2011-12-06	2011-12-08	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
Use-after-free vulnerability in the Response API in ProFTPD before 1.3.3g allows remote authenticated users to execute arbitrary code via vectors involving an error that occurs after an FTP data transfer.														
3	CVE-2011-1137	189	1	DoS Overflow	2011-03-11	2011-09-06	5.0	None	Remote	Low	Not required	None	None	Partial
Integer overflow in the mod_sftp (aka SFTP) module in ProFTPD 1.3.3d and earlier allows remote attackers to cause a denial of service (memory consumption leading to OOM kill) via a malformed SSH message.														
4	CVE-2010-4652	119		DoS Exec Code Overflow	2011-02-01	2011-03-17	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Heap-based buffer overflow in the sql_prepare_where function (contrib/mod_sql.c) in ProFTPD before 1.3.3d, when mod_sql is enabled, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted username containing substitution tags, which are not properly handled during construction of an SQL query.														
5	CVE-2010-4221	119		Exec Code Overflow	2010-11-09	2011-09-14	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Multiple stack-based buffer overflows in the pr_netio_telnet_gets function in netio.c in ProFTPD before 1.3.3c allow remote attackers to execute arbitrary code via vectors involving a TELNET IAC escape character to a (1) FTP or (2) FTPS server.														
6	CVE-2010-3867	22		Dir. Trav.	2010-11-09	2011-09-14	7.1	None	Remote	High	Single system	Complete	Complete	Complete
Multiple directory traversal vulnerabilities in the mod_site_misc module in ProFTPD before 1.3.3c allow remote authenticated users to create directories, delete directories, create symlinks, and modify file timestamps via directory traversal sequences in a (1) SITE MKDIR, (2) SITE RMDIR, (3) SITE SYMLINK, or (4) SITE UTIME command.														
7	CVE-2009-3639	310		Bypass	2009-10-28	2009-12-19	5.8	None	Remote	Medium	Not required	None	Partial	Partial
The mod_tls module in ProFTPD before 1.3.2b, and 1.3.3 before 1.3.3rc2, when the dNSNameRequired TLS option is enabled, does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 client certificate, which allows remote attackers to bypass intended client-hostname restrictions via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.														

Checking Application Exploits in Metasploit

```
msf > search proftpd

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

   Name                                  Disclosure Date        Rank       Description
   ----                                  ---------------        ----       -----------
   exploit/freebsd/ftp/proftp_telnet_iac 2010-11-01 00:00:00 UTC great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   exploit/linux/ftp/proftp_sreplace     2006-11-26 00:00:00 UTC great      ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   exploit/linux/ftp/proftp_telnet_iac   2010-11-01 00:00:00 UTC great      ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   exploit/linux/misc/netsupport_manager_agent 2011-01-08 00:00:00 UTC average    NetSupport Manager Agent Remote Buffer Overflow
   exploit/unix/ftp/proftpd_133c_backdoor 2010-12-02 00:00:00 UTC excellent  ProFTPD-1.3.3c Backdoor Command Execution
```

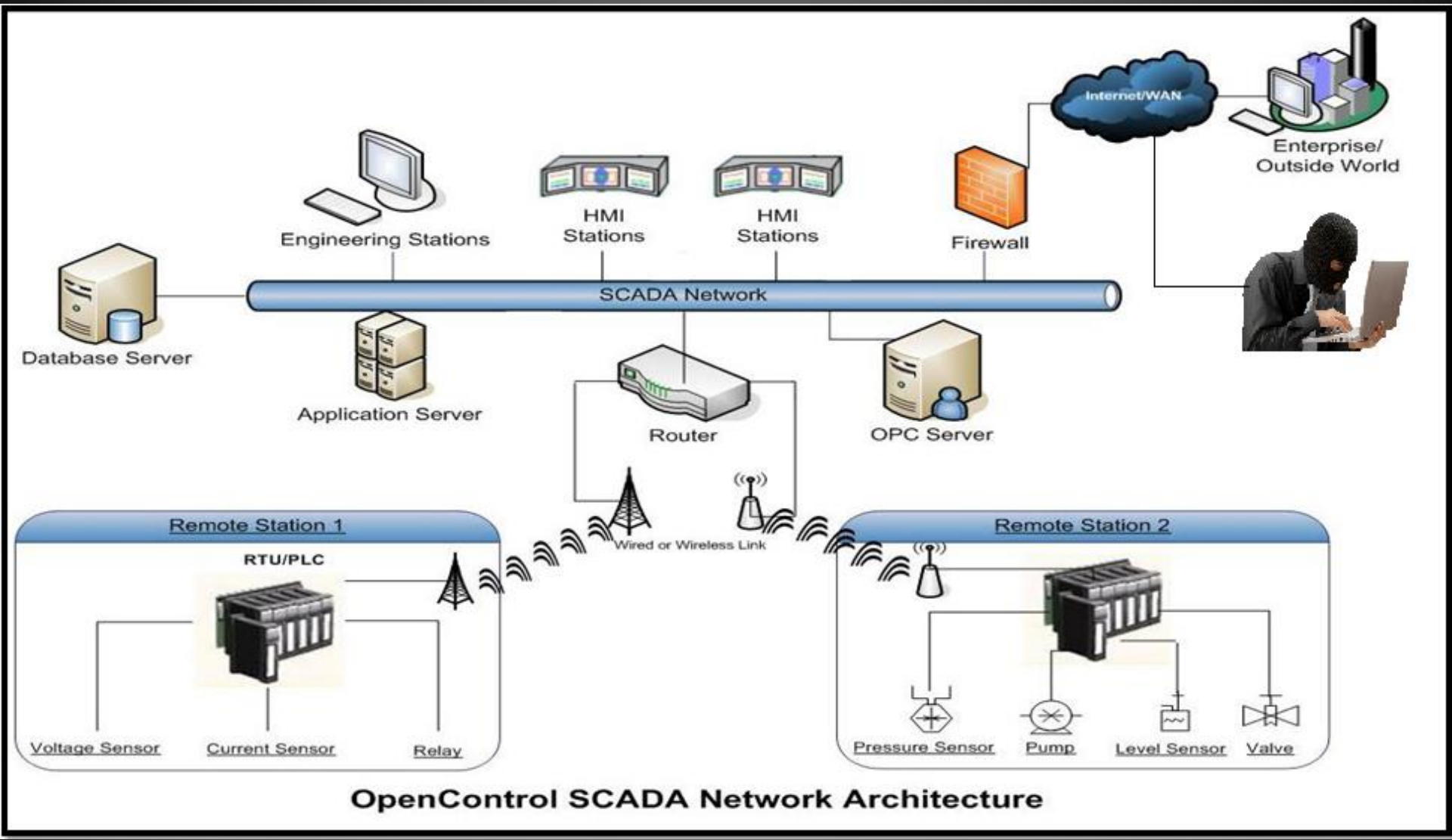

PWNED!


[redacted]
Added on 04.05.2014
Columbus
Details
[redacted]
220 ProFTPD 1.3.3c
[redacted]
incorrect.
214-The
plemented):
QUIT PORT PAS
ALLO* RNFR RNTO
MDTM RMD
XRMD
XPWD SIZE SYST HELP
FEAT OPTS AUTH* CCC* CONF* ENC* MIC*
PBSZ* PROT* TYPE STRU MODE RETR STOR STOU
APPE ...
PWNED!

Compromising a Critical Infra – Is it Possible?

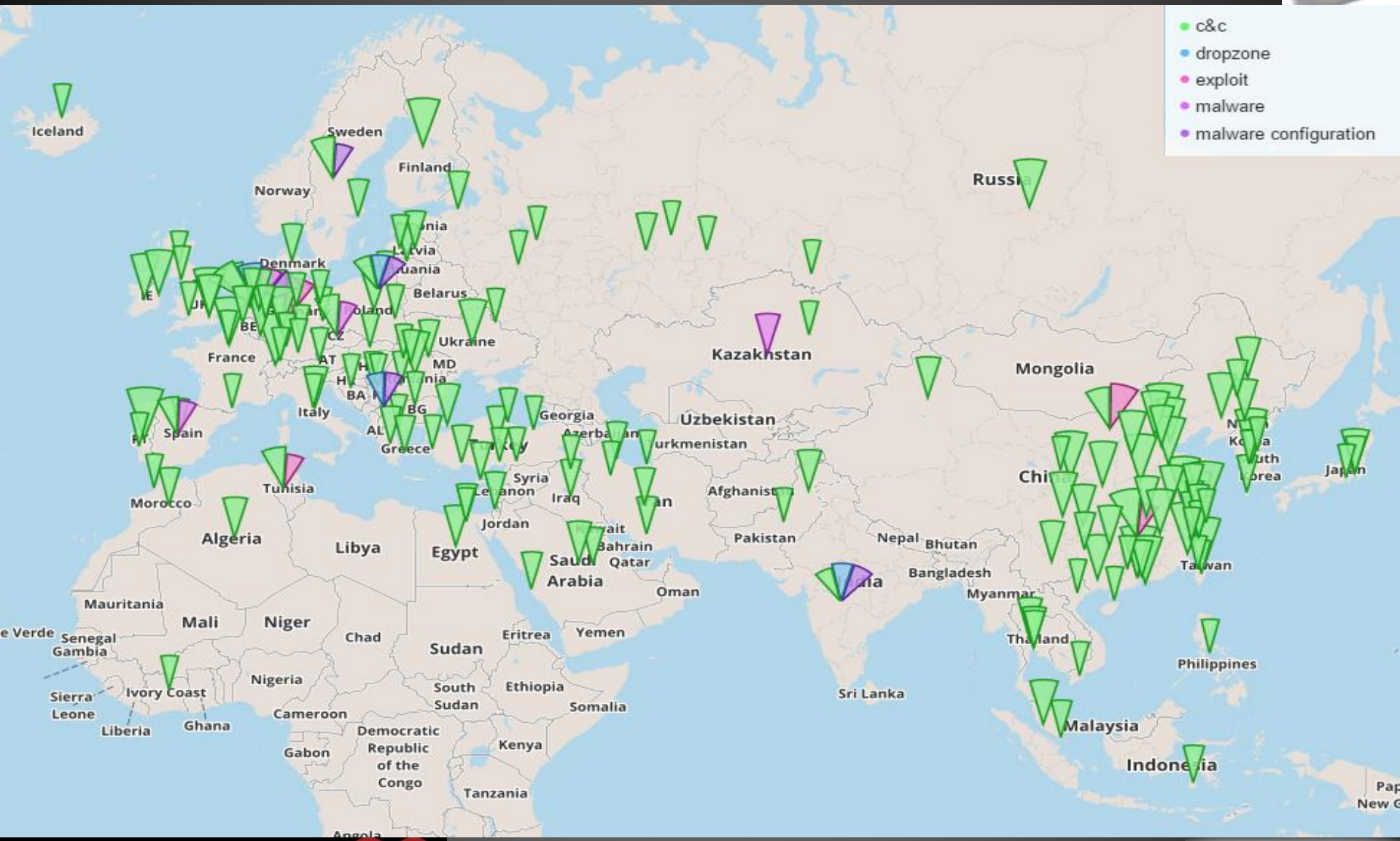
CODENOMICON

Owning a Critical Infra – Is it Possible?



OpenControl SCADA Network Architecture

Think We are at Peace???



CODENOMICON

Takeaways

- Require Extra Precaution when performing VA on SCADAs
- Information Gathering is very very Important!
- Vulnerabilities Exist in Both Software & System
- Critical Infrastructures a Favorite Amongst Hackers
- Types of Attack are similar
- But Impact of Attack Can be Deadly
- Cyber Conflict is Never Ending
- We need to guard our Critical Infrastructures

- Twitter: @hang5jebat
- Blog: http://securityg33k.blogspot.sg
- LinkedIn: Fadli B. Sidek
- Website: www.codenomicon.com