INDUSTRIAL CONTROL SYSTEMS CYBER SECURITY DEMONSTRATION

Prepared for the NRC Fuel Cycle Cyber Security Threat Conference

Presented by: Jon Chugg, Ken Rohde
Organization(s): INL
Date: May 30, 2013

Disclaimer

References made herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the U.S. Government, any agency thereof, or any company affiliated with the Idaho National Laboratory, Pacific Northwest National Laboratory or Sandia National Laboratory.

Acknowledgement

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

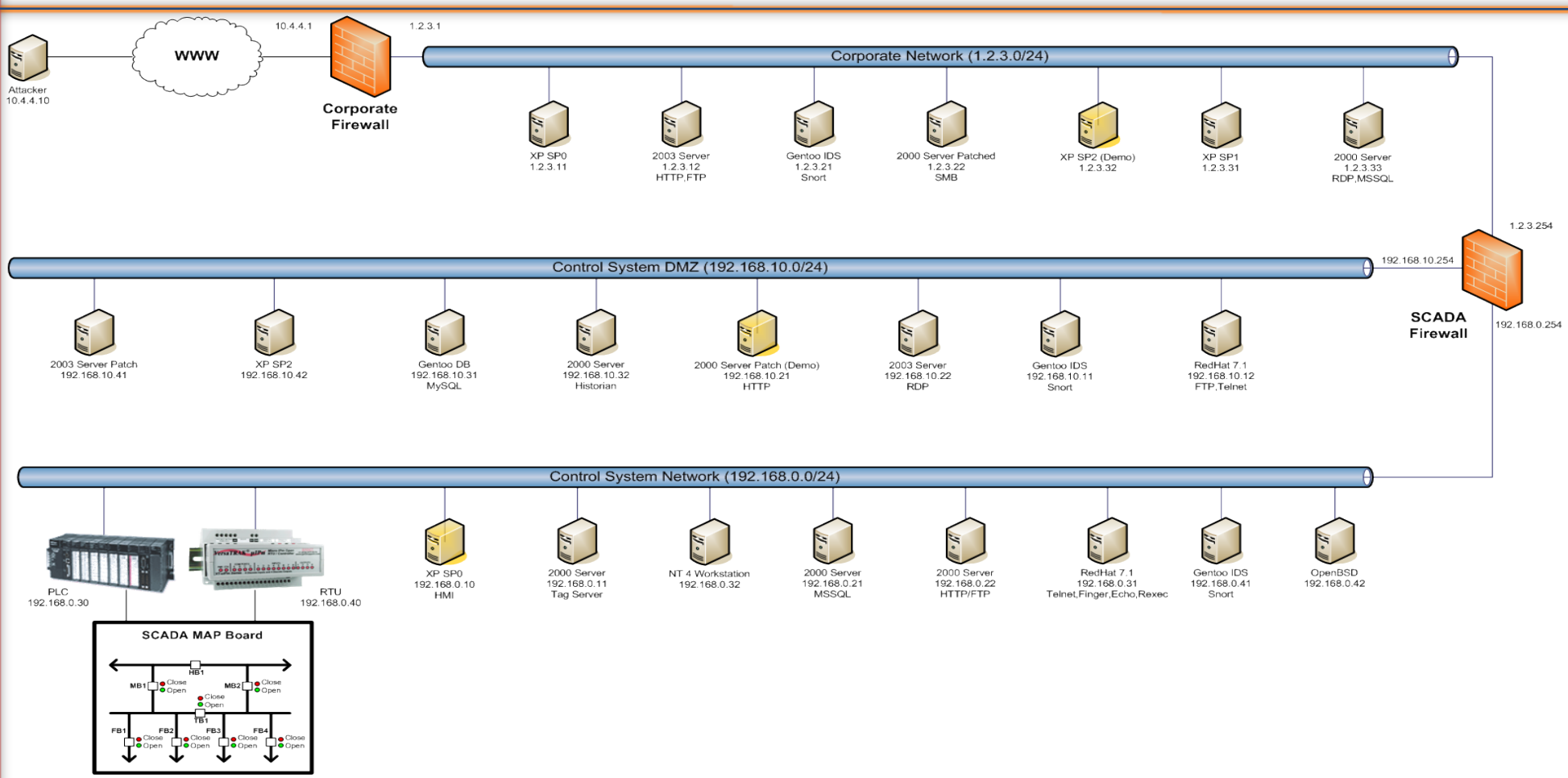
The equipment for this demo was provided by the US Department of Homeland Security ICS-CERT.

Additional resources and training on cyber security for industrial control systems are available at

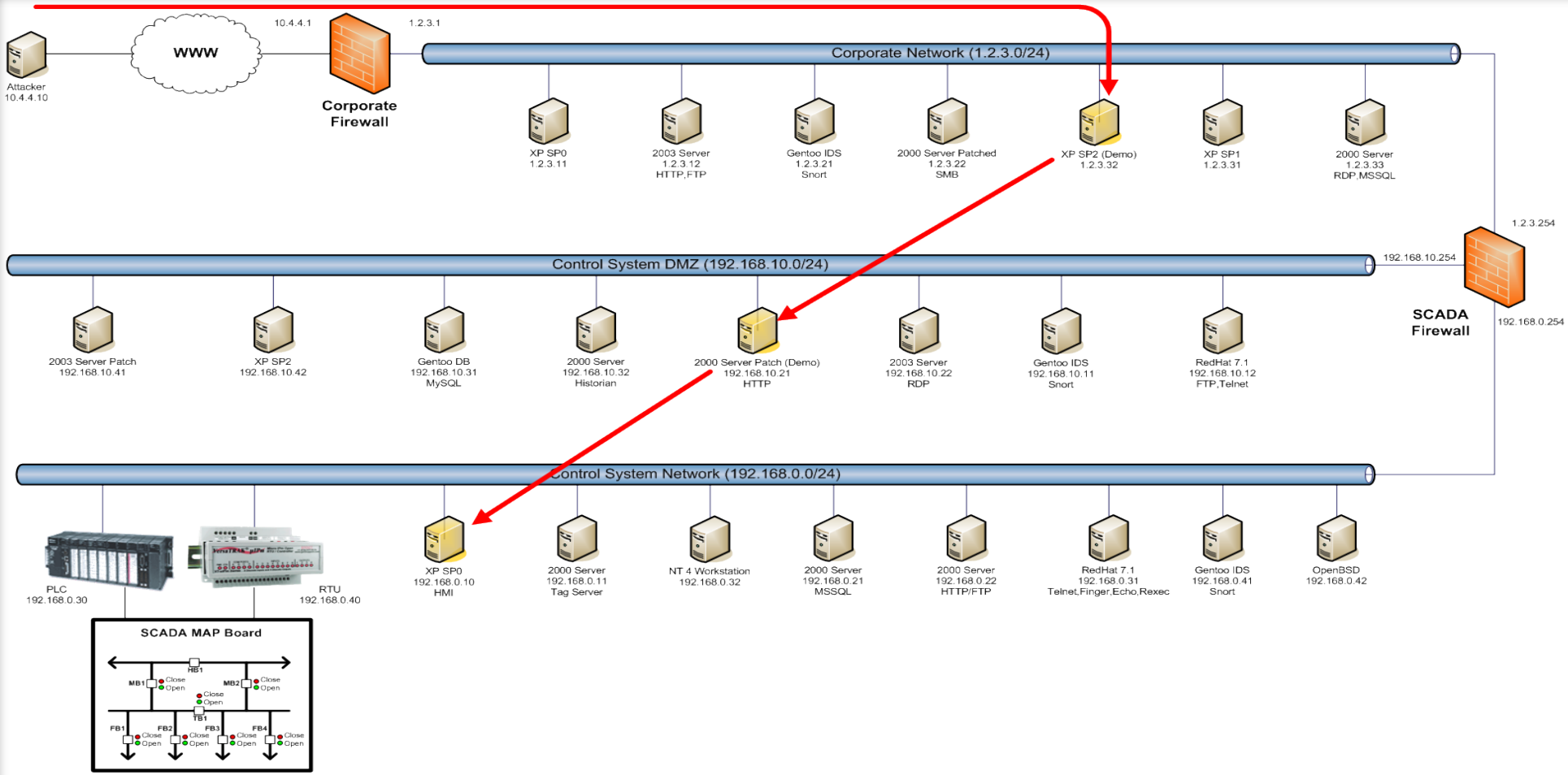
http://ics-cert.us-cert.gov/

Demonstration

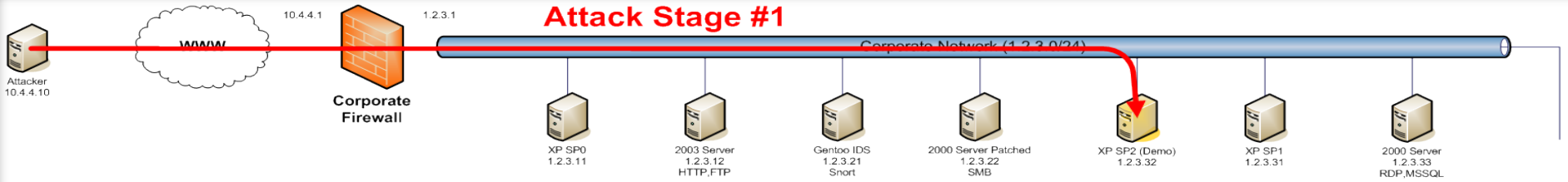
Demo Network Layout

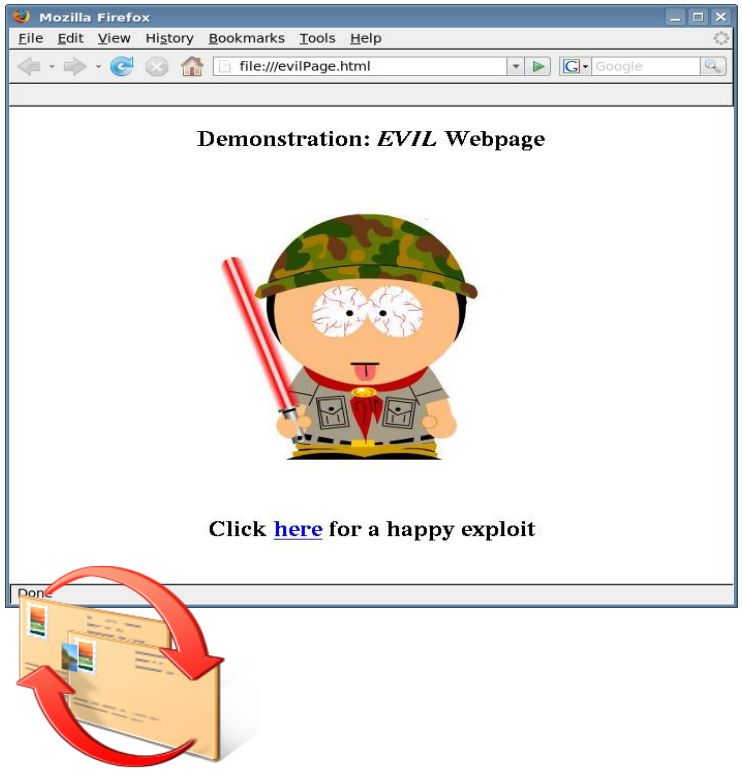


Demo Exploit Path



Attack Stage #1 – Internet to Corporate





Client Side Attack:

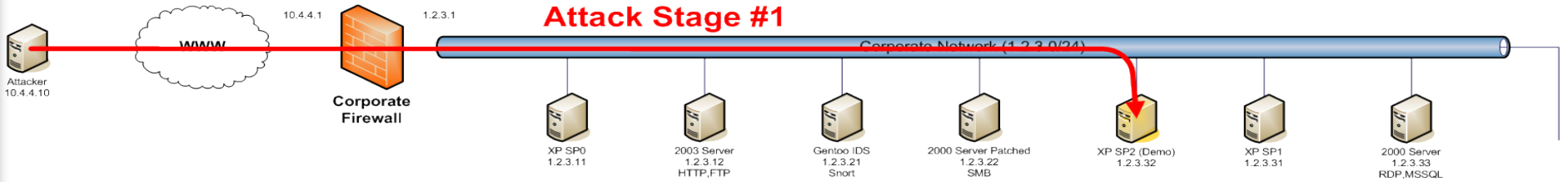
Corporate user follows a malicious URL

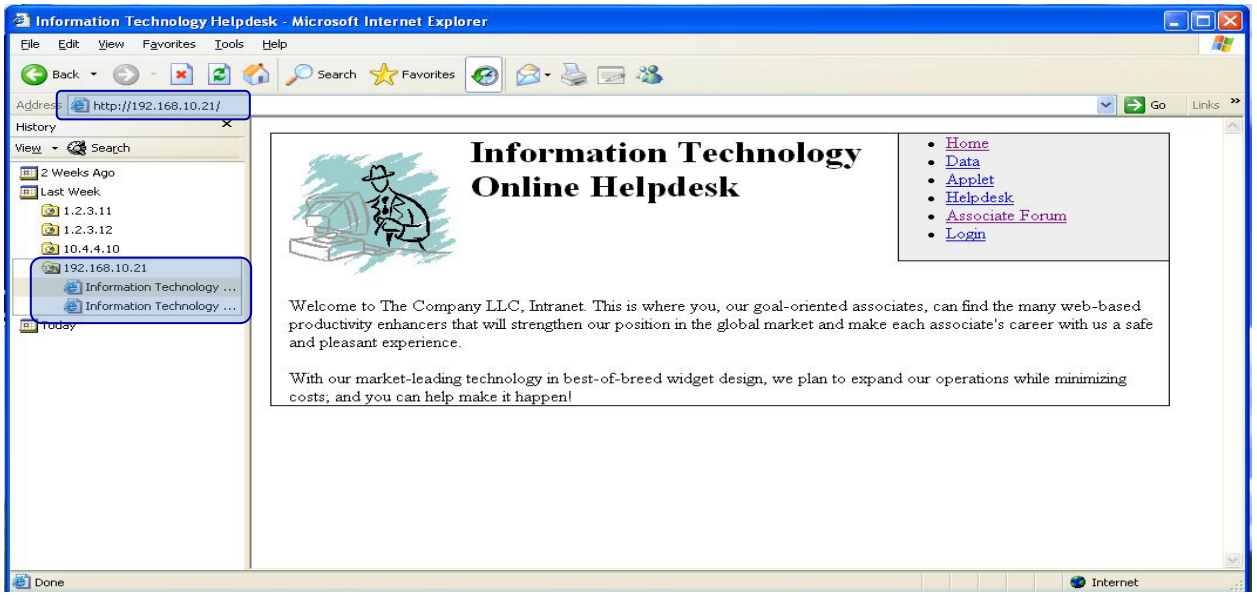
- Social engineering
  - From an email
  - From a suspicious web page

Triggers a vulnerability on the corp box

- Exploit payload calls outbound through the firewall to the attacker internet host
- Attacker gains remote control of the corporate victim

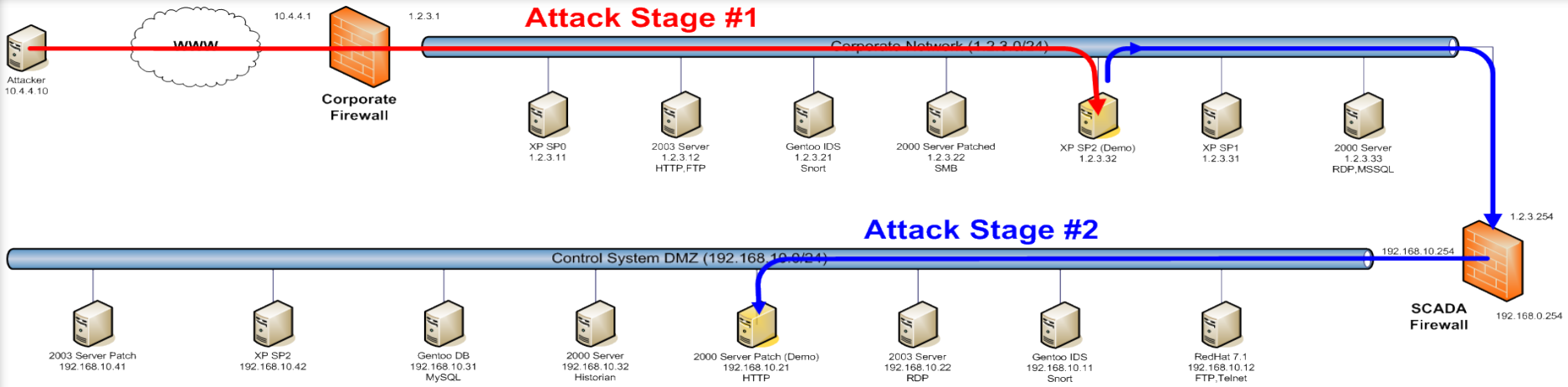
Attack Stage #2 – Reconnaissance





Victim #1 browser history indicates access to a separate subnet (Victim #1 IP – 1.2.3.32, HTTP IP - 192.168.10.21)

Attack Stage #2 – Corporate to DMZ



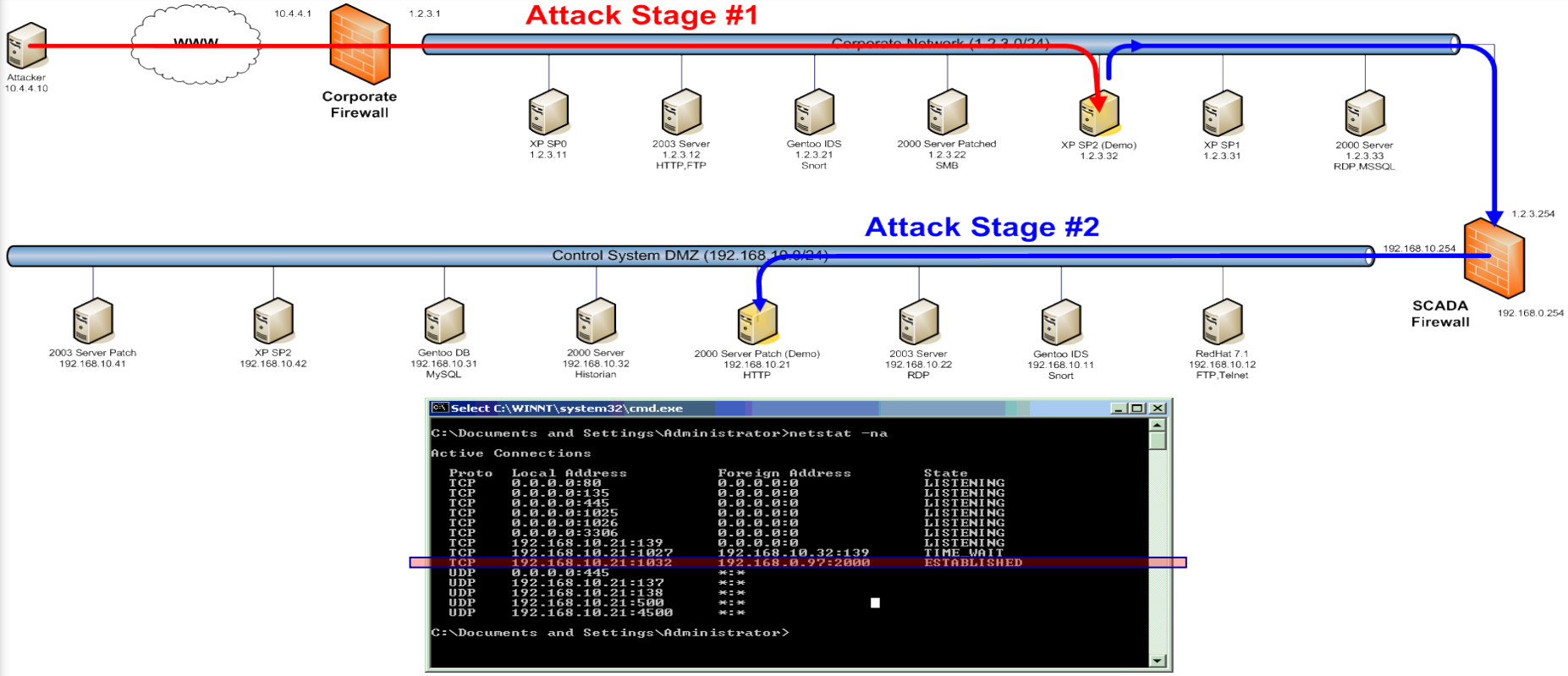
Web Application Vulnerabilities

- Help desk web application allows user to upload arbitrary files (trouble tickets)
  - Attacker uploads a new PHP file and also an executable rootkit
- Website code has an SQL injection problem
  - Provides admin access to the website (privileged features)
  - Attacker makes an HTTP request to an existing admin page and changes the 'action' on the URL to **include** (aka execute) the uploaded PHP page
    - PHP is able to run system commands and launch the rootkit

Firewall policy:

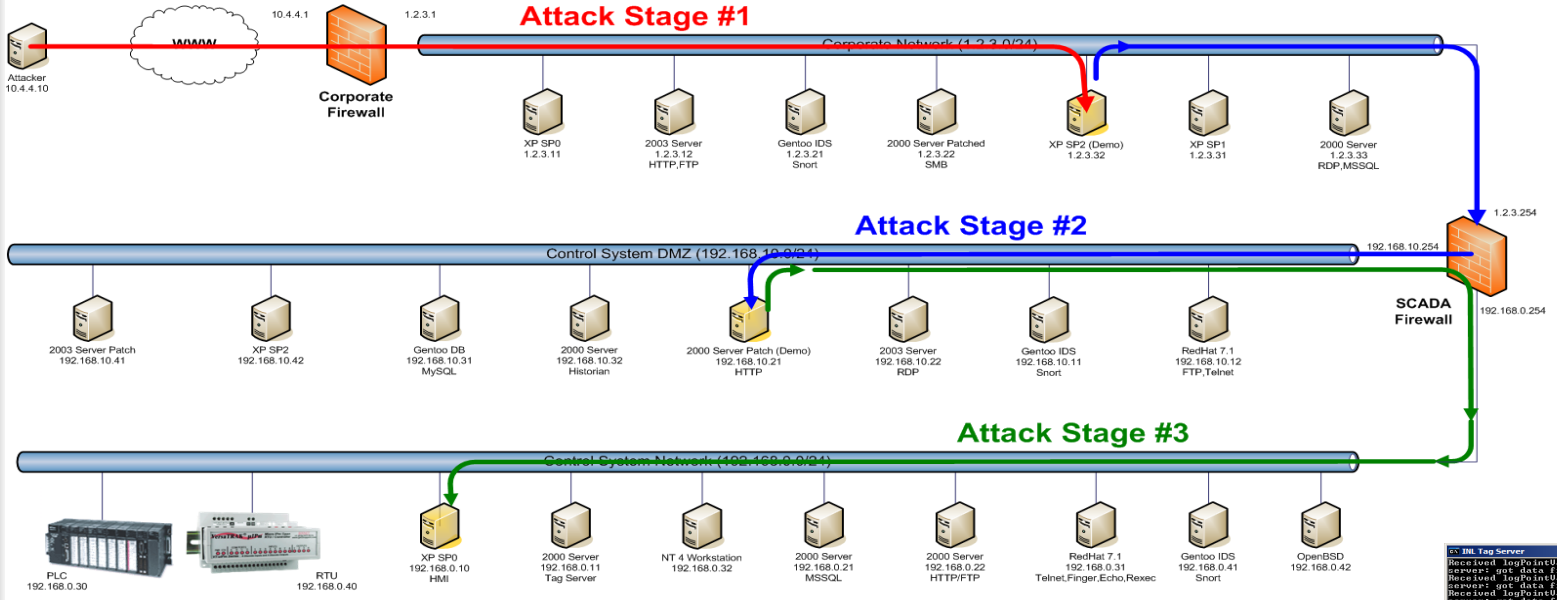
- Grants **Victim #1** HTTP access to **Victim #2**
- **Victim #2** allowed 'any' TCP connection to internet
  - Uploaded rootkit calls back to attacker machine

Attack Stage #3 – Reconnaissance



Victim#2 Netstat shows an established connection to a new subnet (Victim #2 IP – 192.168.10.21, Remote Server IP – 192.168.0.10)

Attack Stage #3 – DMZ to SCADA

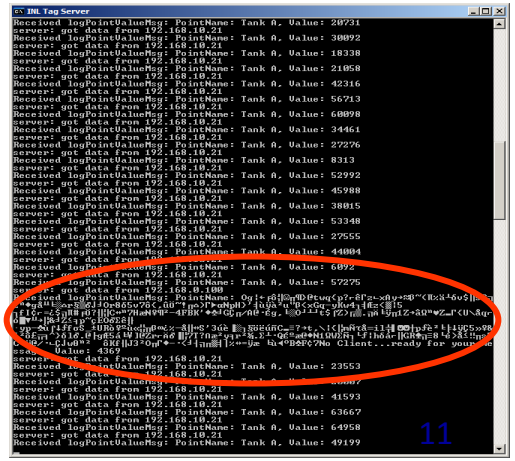


Tag Server Buffer Overflow

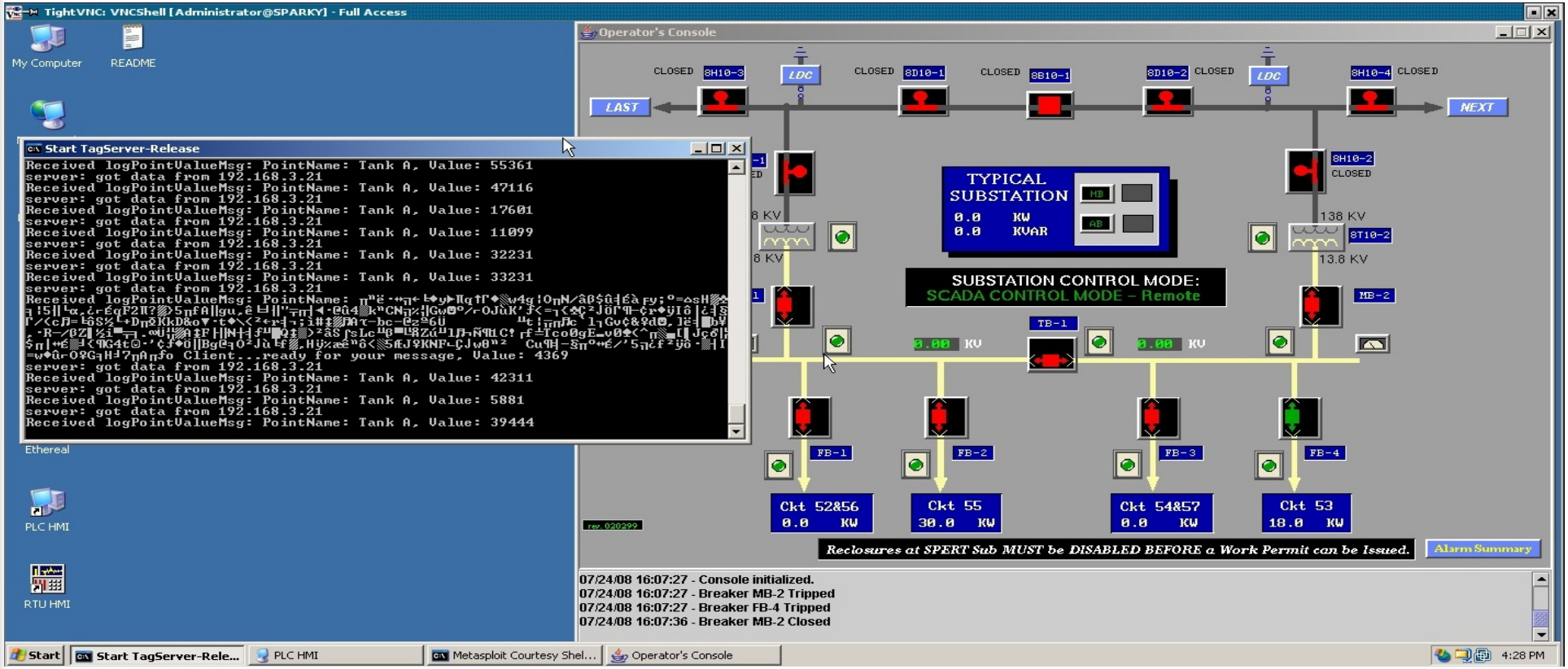
Exploit overflows the point name field

Firewall policy:

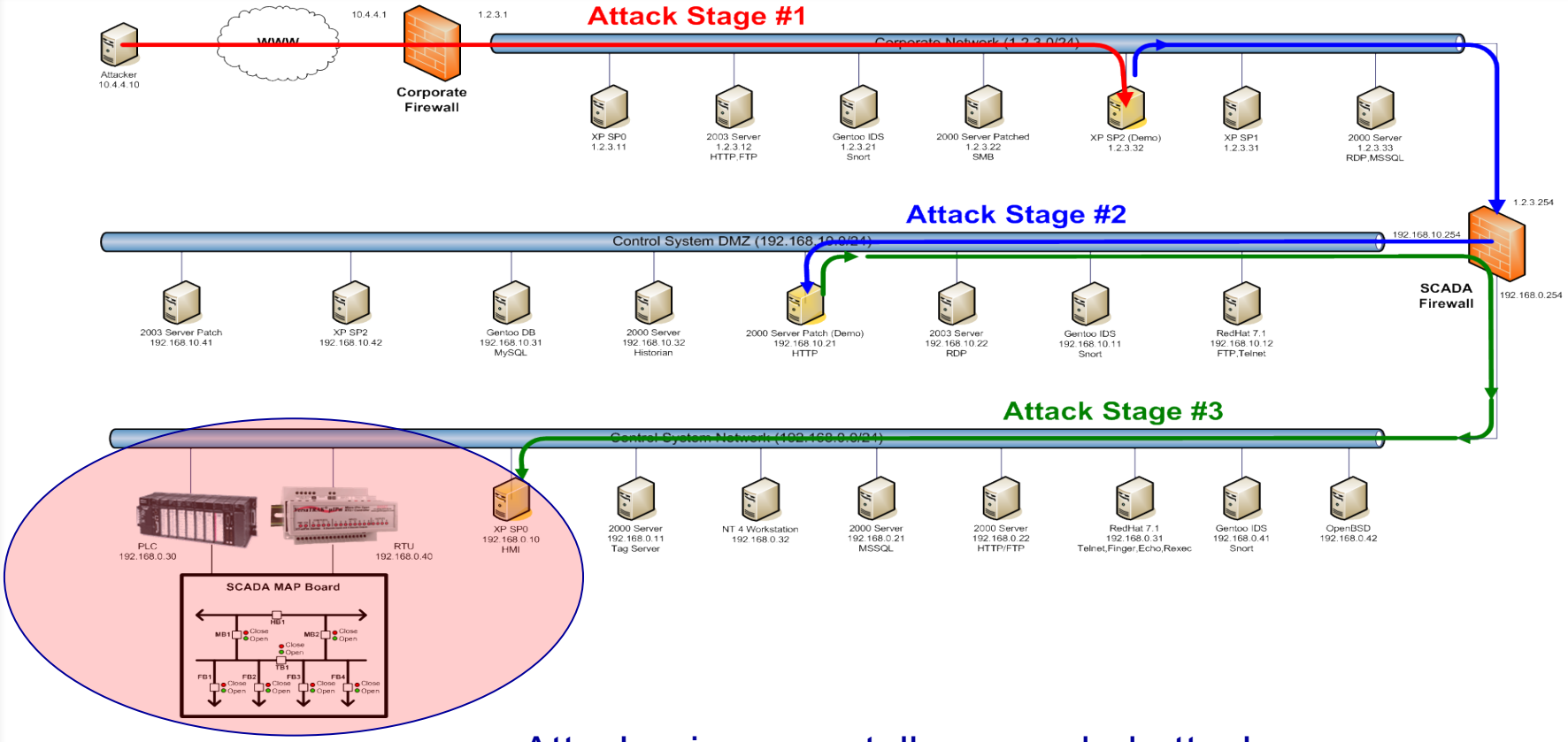
- Grants **Victim #2** access to **Victim #3** on port 2000
- **Victim #3** allowed 'any' TCP connection to internet
  - Exploit payload calls back to attacker machine



Attack Stage #3 – HMI



Attack – Commands Directly to the PLC



Attacker incrementally expanded attack

- Gained remote control of host inside the control LAN
  - Controls the HMI or Substation from the internet

Demo Vulnerabilities & Possible Mitigations

Problems

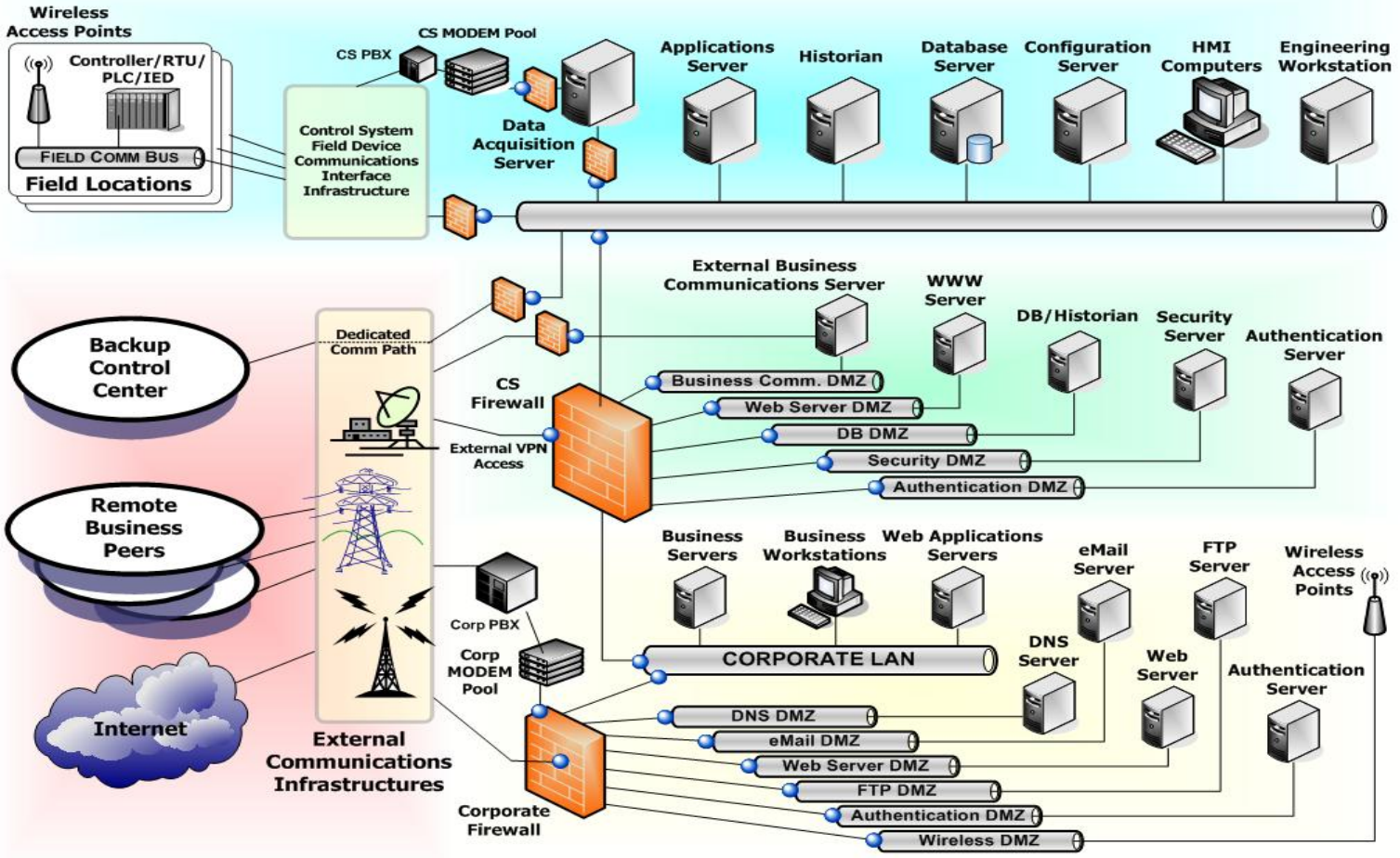
- Antiquated and/or unpatched
  - Operating systems
  - Services
- Poorly defined firewall policy (any outbound traffic allowed)
- Intrusion detection system (IDS) is underutilized
- Application coding problems
  - Unsafe function usage
  - Logic problems
- Least privileges principle has not been applied to all applications, services, and the network design

Fixes

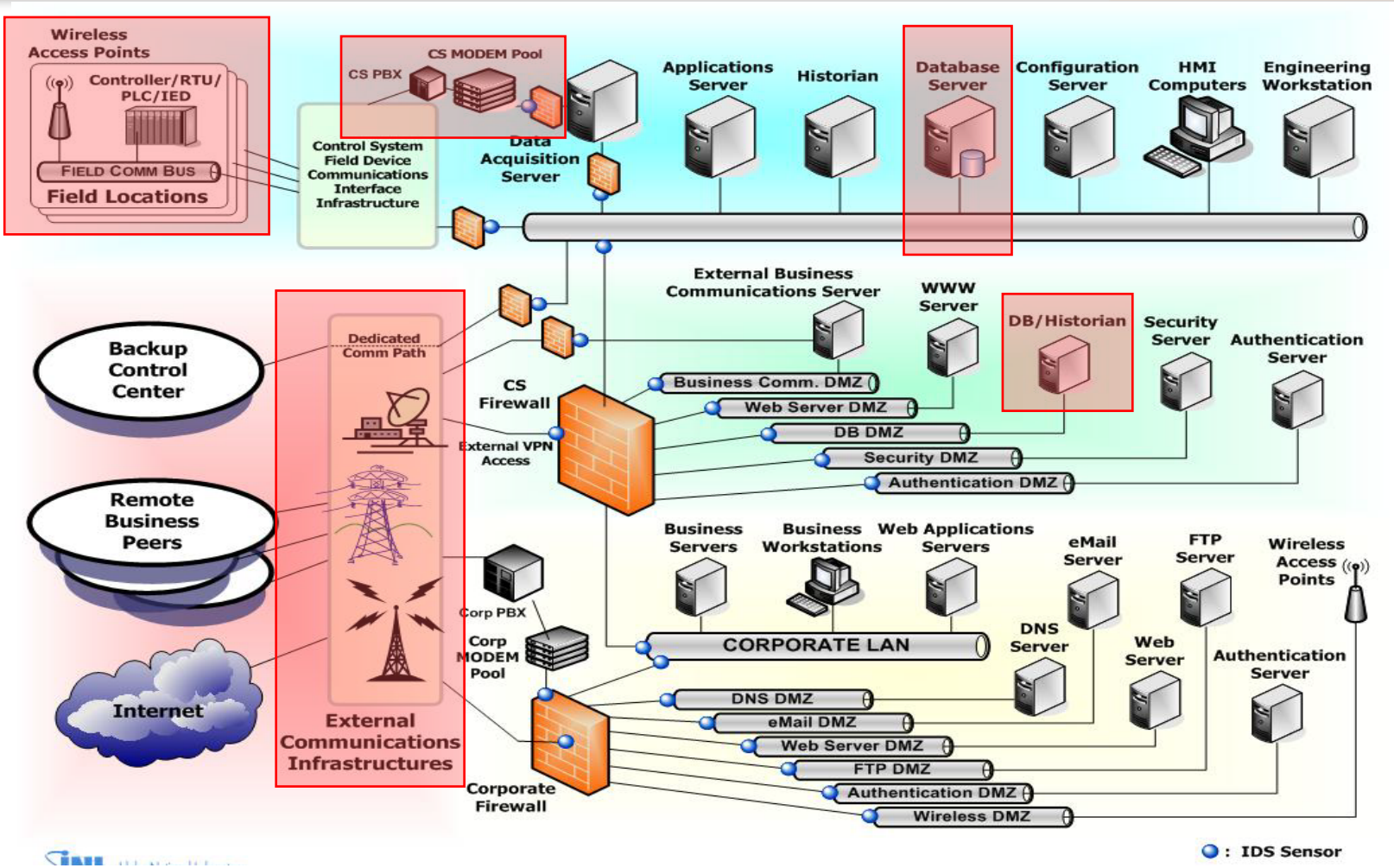
- Keep “public” systems fully patched
- Audit firewall rules and analyze all exceptions
  - Push data rather than pull
  - Outbound firewall policies
- Deploy and monitor IDS in border networks
- Audit “home grown” applications for problems
- Ensure services are running as users rather than Administrator or System

How and Why it Happens

Potential Entry Points

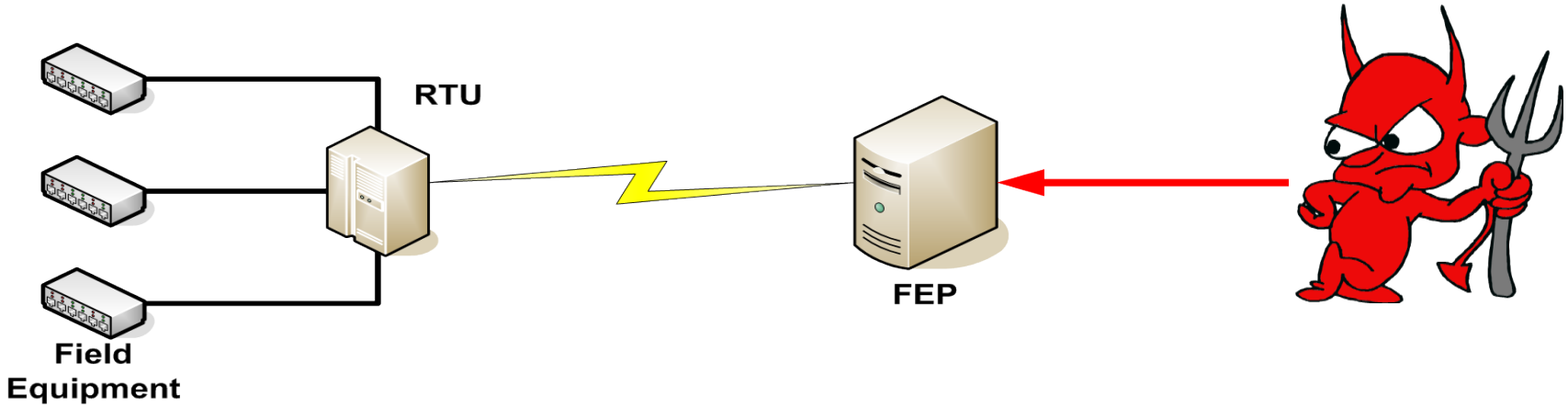


Potential Entry Points



Manipulation of the System

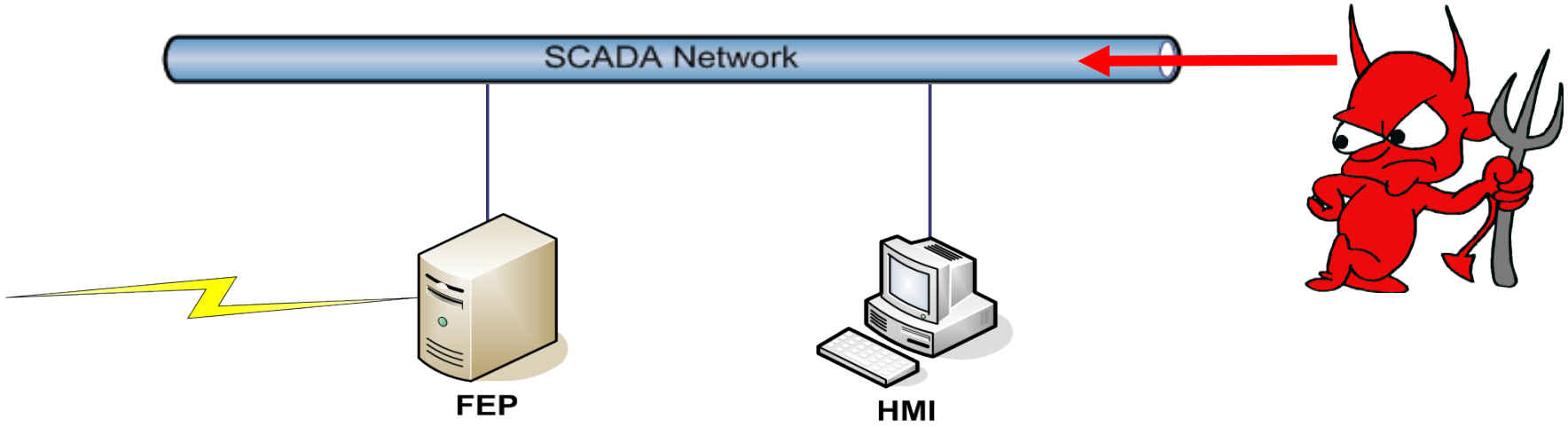
Talk Directly to the Front-End Equipment



- Often no userid/passwords required
- Undocumented vendor protocols are common
- Commands are generally not logged

Manipulation of the System

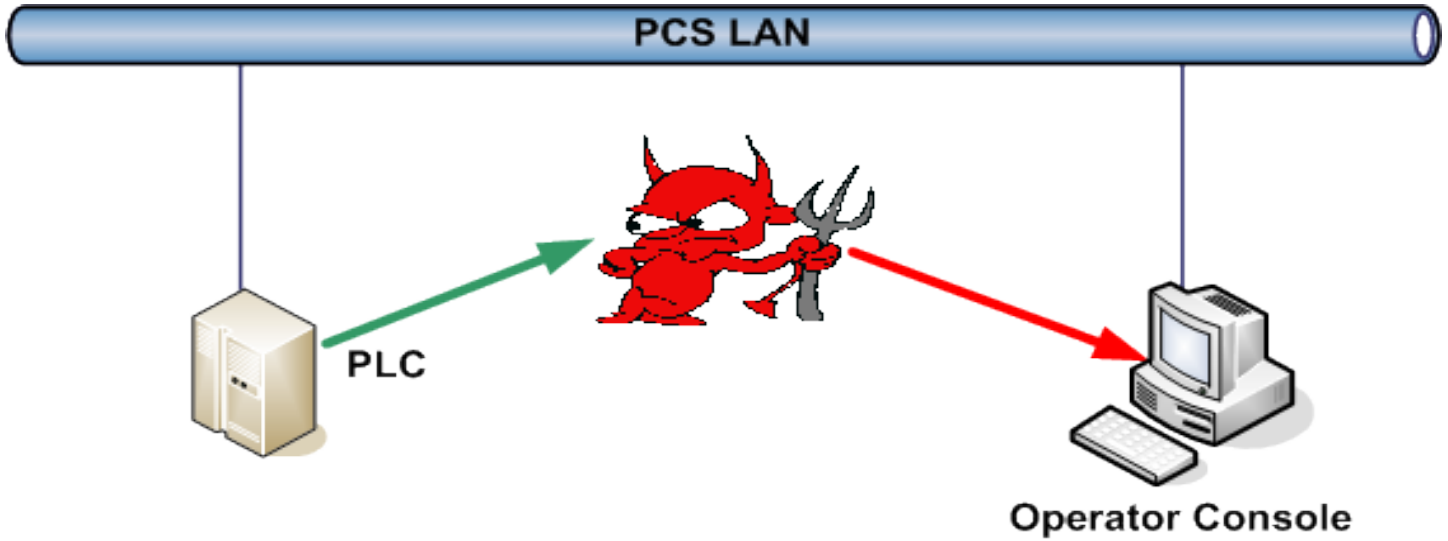
Export the HMI Screen



- Graphic pictures to describe the process
- Noticeable by the operator
- Can use your off-the-shelf tools
  Have credentials of logged in user
  - May not be able to manipulate to failure

Manipulation of the System

Change Operator's Display



- If presented with an out-of-control system, operator will take steps to shut down
- Logs will reflect operator actions & true state of system
- Detailed knowledge of process needed to make believable

Open Source Tools

Enumerate Network: Nmap

Nmap Enumerates (scans) networks to determine which hosts are up and/or what services they are offering.

Vulnerability Scanning

Software tools are available to assess computers, computer systems, networks, or applications for weaknesses, e.g.,

- Unpatched operating systems
- Unpatched applications
- Open ports and services
- Web applications

Two examples are Nessus (commercial) and OpenVAS (open source)

Capture Communications: Tcpdump

- Open-source packet sniffer (reader) that is available for most modern operating systems.
- Allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.
- Can be used to analyze network behavior, performance and applications that generate or receive network traffic.
- It's native capture file format is libpcap format, which is also the format used by various other tools.

Analyze Communications: Wireshark

- Open-source GUI network protocol analyzer.
- Browse packet data from a live network or from a previously saved capture file.
- Export data objects to files (documents, pictures)
- Native capture file format is libpcap format, which is also the format used by tcpdump & various other tools.

Host Compromise

The Metasploit Project

- Created to provide information on exploit techniques and to create a useful resource for exploit developers and security professionals.
- Provides useful information to people who perform penetration testing, IDS signature development, and exploit research.
- Provided for *legal* security research and testing purposes only.
- Exploits often added for new vulnerabilities within days of vulnerability disclosure.

An open-source hacking toolkit

http://www.metasploit.com/

Cyber Incidents

Basic Attack Steps

Monitor for these Activities

1. Targeting
2. Discovery and Fingerprinting
3. Exploitation
4. Maintaining Access
5. Cleaning-up/Covering their tracks
6. … Repeat

Third-Party Access and Malware Protection

Davis Besse Nuclear Power Plant

Event: January 25, 2003, Slammer worm infects plant.

Threat: Cracker (Group I)

Impact: Complete shutdown of digital portion of Safety Parameter Display System (SPDS) and Plant Process Computer (PPC).

Specifics: Worm started at contractors site then jumped from the corporate to plant network and found an unpatched server.

Lessons learned:

- Secure remote (trusted) access channels
- Ensure Defense-in-depth strategies with appropriate procurement requirements
- Critical patches need to be applied

Patch Management for ICS

Hatch Nuclear Power Plant

Event: March 7, 2008, software update on business system causes plant shutdown.

Threat: Insider (accidental)

Impact: Reset of measured coolant levels, causing shutdown of Unit 2.

Specifics: Engineer installed software update on a computer that monitored data from the facility's primary control systems.

The computer was on the business network.

When the computer rebooted, it reset data on coolant levels, which caused safety systems to shut down the reactor.

Lessons learned:

- Control and data acquisition systems are sensitive to data availability.
- Patches should be tested on an off-line system (e.g. simulator) prior to being applied in the field for supervisory data acquisition systems and control systems.

Data Availability

Brown's Ferry Nuclear Plant

Event: August 19, 2006, "Excessive traffic" on the control system network caused two water pumps to fail.

Threat: Insider (accidental)

Impact: "High power, low flow condition" forced manual SCRAM of the reactor.

Specifics: The controllers for the pumps locked up following a spike in data traffic on the power plant's internal control system network.

Lessons learned:

- Control and data acquisition systems are sensitive to data availability.
- Unexpected & high volumes of network traffic (data spike) can cause some controllers to become unresponsive.

Security for Portable Media and Devices

Nuclear Facility (Name Withheld) Infected with Malware

Event: 2010 - Mariposa Botnet Crimeware Infects a nuclear facility's enterprise network.

Threat: Criminals (for-profit, Group II)

Impact: Over 100 hosts on the enterprise network were infected.

Specifics: The infection occurred when an employee attended an industry event and used an instructor's USB flash drive to download presentation materials to the employee's laptop.

Other nuclear industry personnel had also used the same infected USB drive at the industry event.

Lessons learned:

- Organizations should have polices and procedures for use of portable media and devices.
- Portable media and devices should be scanned prior to use on critical systems.

Source: http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Incident_Response_Summary_Report_09_11.pdf

Access to Critical Digital Systems

Natanz Uranium Enrichment Facility (Iran)

Event: November 30, 2010, Iranian president admits that a cyber attack affected Iran's uranium enrichment centrifuges.

Threat: Possibly nation-state-sponsored (Group III)

Impact: Shut down of Iran's uranium enrichment facility for 6 days in November 2010.

Lessons learned:

- Organizations should have polices and procedures for use of portable media.
- Portable media should be scanned prior to use on critical systems.

Targeted Attack on Control Systems - Stuxnet

Exploited multiple flaws:

- Multiple 0-days
- Certificate Compromise
- Privilege Escalation
- Default password in control system software