

Mind of the Hacker:

Understanding Vulnerabilities, Exploits, and Hacker Methods

Critical Infrastructure



Clint Bodungen

President

Critical Infrastructure Institute (USA)

clint.bodungen@ci-institute.org

This is not child's play...



Objectives

- Review the differences between threats, vulnerabilities, exploits, and risks
 - Gain an overview of the threats
 - Understand vulnerabilities and look at examples in the process control industry
 - Examine hacker methodologies and how they exploit these vulnerabilities
 - Demos
- Note – Some slides contain very detailed technical data. Due to time restraints, some of it may only be briefly discussed but has been left in as a reference for those wanting more technical data.

Objectives

➤ Why?

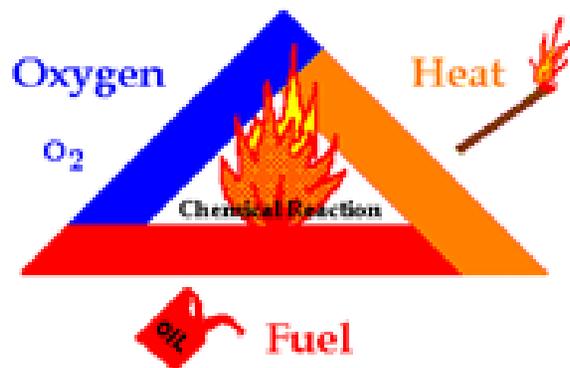
- “Know Thine Enemy”
- The best way to safeguard against threats and vulnerabilities is to understand them.



Ingredients for a Successful Cyber Security Attack

- A Cyber Attack is the result of the presence of a **Threat**, taking advantage of a **Vulnerability**, through a successful **Exploit**
 - Threats typically stem from people or organizations
 - Vulnerabilities are deficiencies in the security of a system
 - Exploits are created by Threats to take advantage of Vulnerabilities
- Think of this like the Fire Triangle

Fire Triangle

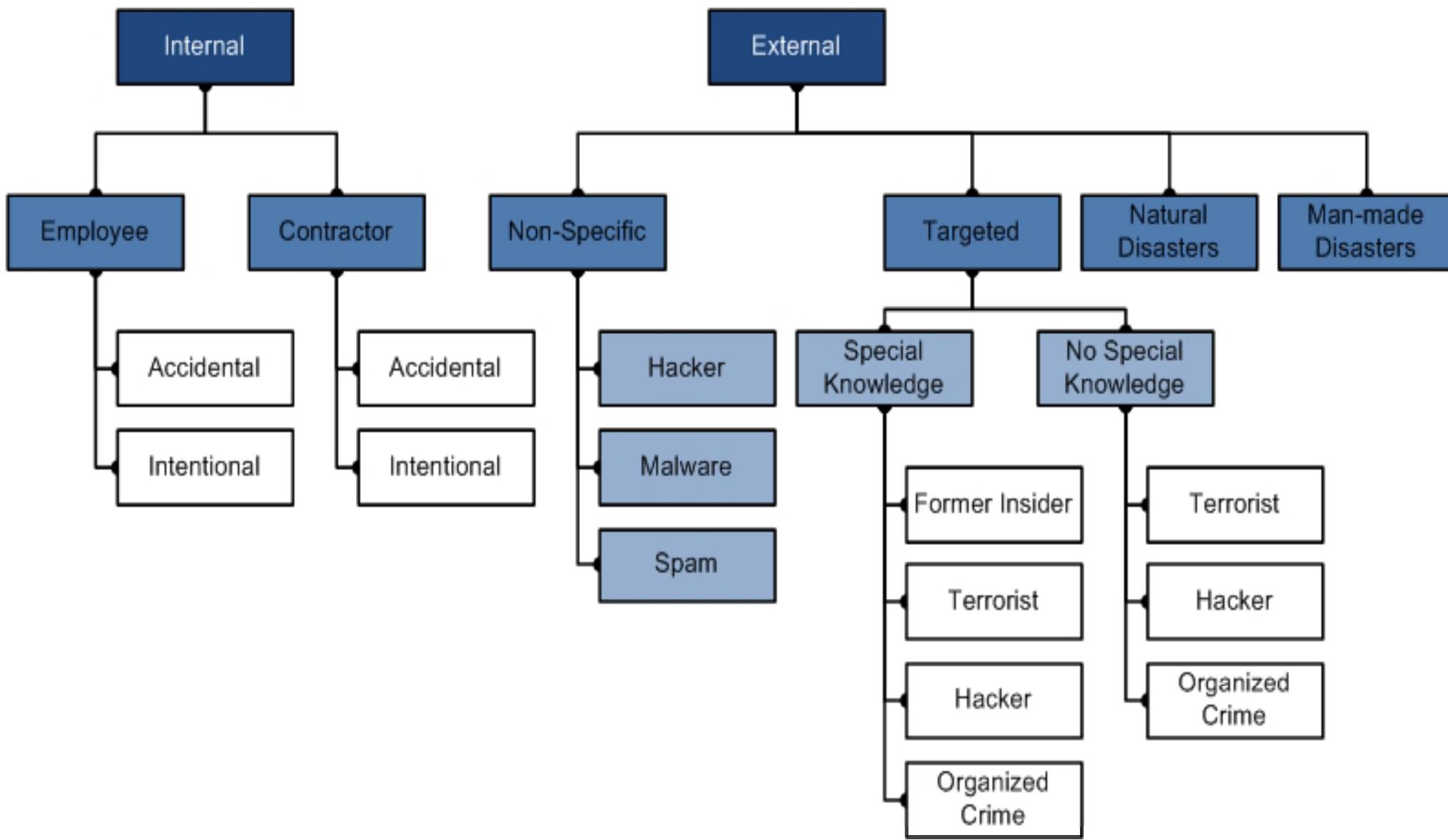


Cyber Attack



- The likelihood of a vulnerability getting exploited combined with the possible result / impact to the infrastructure is the **Risk**

Taxonomy of Potential Threat Sources



Malware

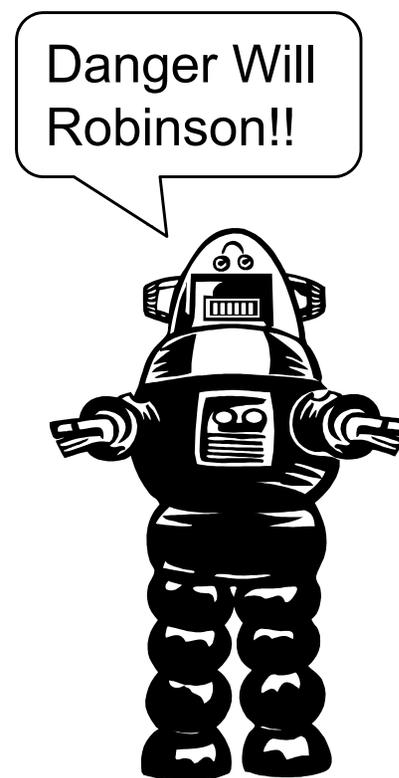
➤ Malware – Malicious Software

- Viruses
- Worms
- Adware
- Spyware
- Trojans
- Hostile Scripts

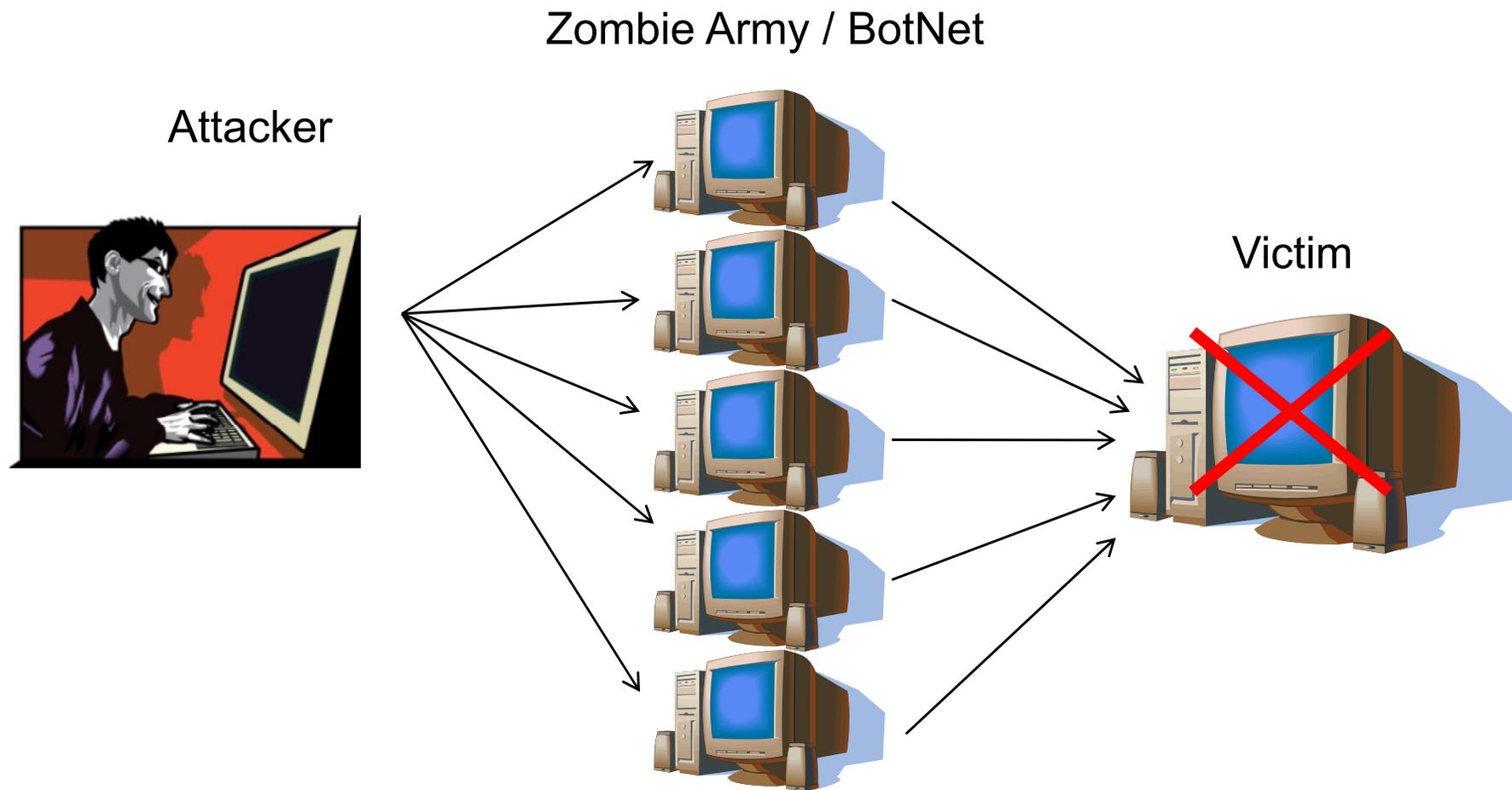


Bots / BotNets

- AKA Agents
- Performs automated tasks
 - Chat Bots
 - Web Bots
- Malicious bots are
 - Zombies
 - Programs that listen and respond to commands on Internet Relay Chat (IRC) channels
- BotNet
 - A group of bots acting in concert
 - Run autonomously
 - Common command and control
- Most prevalent in Windows environment
- Used in DDoS (More on this later)



Bots / BotNets



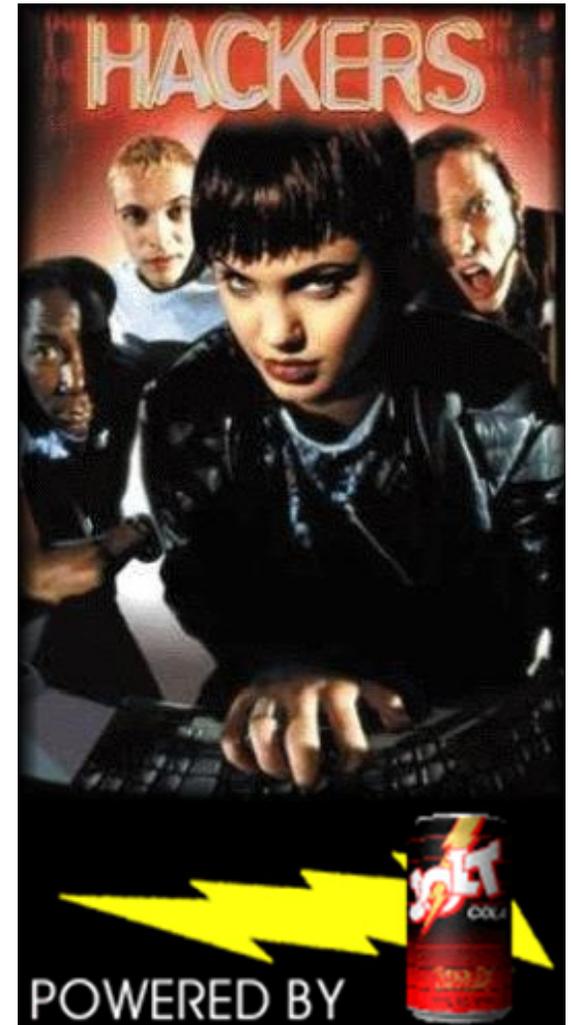
Users (Employees and Contractors)

- Inadvertently cause problems
 - Misconfigurations
 - System / Network congestion
 - Explore
- Bring in outside threats
 - Removable media
 - Games
 - Screensavers
- EMAIL!
 - Users will open anything!
- Internet



The Hacker

- What is hacking?
 - Original Meaning
 - Gaining an Understanding of Technology
 - Creative Solutions
 - Creative Programming
 - Passion for computers and technology
 - Common / Media Definition
 - Computer Criminal (Cracker)
 - Child Prodigy Gone Wrong



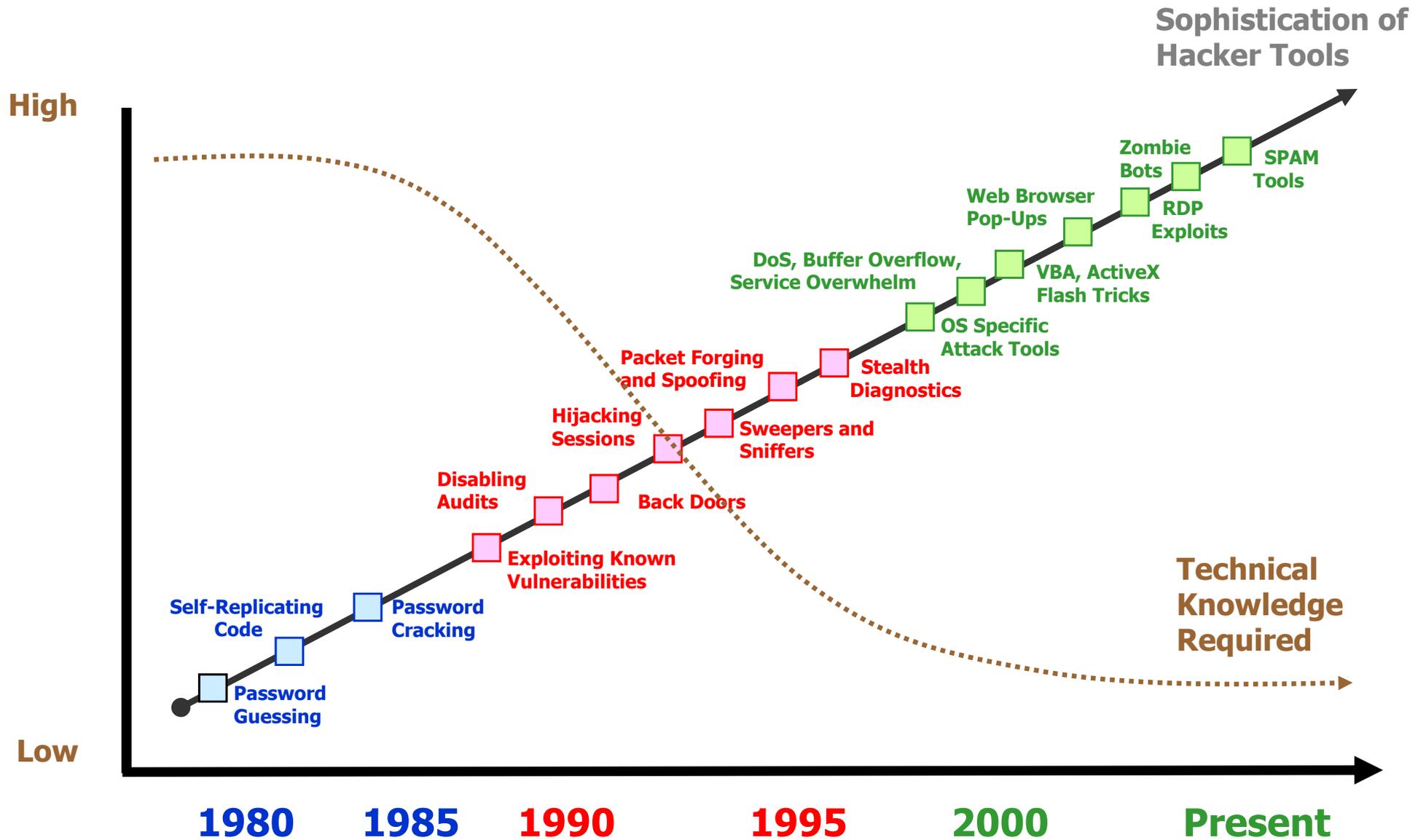
Hacker Classes and Motivations

➤ “Hackers”

- Script Kiddie – (Usually low skill) looking for a challenge or to be recognized
- Hacker – Because they can and to learn
- Organized Crime – Profit
- Extremists/Activists – Making a statement
- Terrorists – Economic Damage, Destruction, Self Sacrificing
- Foreign Governments – Strategic
- Insiders – Disgruntled or Paid
- Alliance of any of the above



Hacker Trends



Houston, DO we have a problem?



- IS there a real threat?
- But aren't systems like process control and SCADA too proprietary?
- Is it likely it could happen to me?
- Are there any documented incidents?



The Hackers are Bridging the Knowledge Gap

washingtonpost.com

Hackers Target U.S. Power Grid

Government Quietly Warns Utilities To Beef Up Their Computer Security

By Justin Blum

Washington Post Staff Writer

Friday, March 11, 2005; Page E01

Hundreds of times a day, hackers try to slip past cyber-security into the computer network of Constellation Energy Group Inc., a Baltimore power company with customers around the country.

"We have no discernable way of knowing who is trying to hit our system," said John R. Collins, chief risk officer for Constellation, which operates Baltimore Gas and Electric. "We just know it's being hit."

Hackers have caused no serious damage to systems that feed the nation's power grid, but their untiring efforts have heightened concerns that electric companies have failed to adequately fortify defenses against a potential catastrophic strike. The fear: In a worst-case scenario, terrorists or others could engineer an attack that sets off a widespread blackout and damages power plants, prolonging an outage.

Patrick H. Wood III, the chairman of the Federal Energy Regulatory Commission, warned top electric company officials in a private meeting in January that they need to focus more heavily on cyber-security. Wood also has raised the issue at several public appearances. Officials will not say whether new intelligence points to a potential terrorist strike, but Wood stepped up his campaign after officials at the Energy Department's Idaho National Laboratory showed him how a skilled hacker could cause serious problems.

Process historian becomes online gaming server

Problem

A power generation company in the U.S. had a historian collecting SCR data for the EPA. Possibly through a vendor's maintenance dial in modem, the historian was subverted to become an online gaming server.

Consequences

Bandwidth to the historian was greatly curtailed resulting in the loss of 1.5 days worth of emissions monitoring data. The company was fined \$1.5M US in addition to production, litigation, and recovery costs.

Key Control System Recommendations

Technology: Host dial-in, process, bandwidth, socket, file monitoring

Policy :Institute dial back modems, strong dial-in authentication

Source: Verano contact

Hacked historian becomes spam server

Problem

A power generation company in the U.S. had a historian connected to the Internet to receive time syncing data (NTP). The server was compromised and used as a spam relay and a file server.

Consequences

Operators had slow display refresh rates and there was a huge bandwidth usage increase. Additionally, spam servers eventually become blacklisted in the Internet community. Valid emails from that company could be rejected by other companies subscribing to blacklisting services.

Key Control System Recommendations

Technology: Firewall, IDS/IPS, and file, process and bandwidth monitoring

Policy :Have dedicated NTP servers and put historians in a DMZ

Source: Verano contact

SCADA defect contributes to August 2003 US East Coast blackout

Problem

Much of the N. American east coast lost power on August 14, 2003. Contributing to the problem was a bug in GE's XA/21 EMS system installed at FirstEnergy's Akron, OH control center. A combination of conditions caused operators to operate for over an hour without realizing that they weren't receiving updated information. Additionally when the backup server finally came online, it crashed due to the queue of unprocessed events. The operators lacked situational awareness to manage their portion of the grid.

Consequences

The blackout was a major continental economic loss. GE and FirstEnergy had a great deal of negative publicity.

Key Control System Recommendations

Technology: Application performance and alarm queue monitoring

Policy :Validate system data using crosschecks with other systems

Source: Public Record <http://www.securityfocus.com/news/8016>

Slammer worm crashes US nuclear plant network

Problem

The 873 MW Davis-Besse nuclear plant in Oak Harbor, OH was infected by the Slammer worm on January 25, 2003. The worm entered via a T1 line that bypassed firewalls and infected the control system network. Plant monitoring systems were out for 5-6 hours. In addition to various other holes in network security, plant engineers had not applied, and nor were aware of a patch available for the Slammer worm.

Consequences

Additional bad publicity for FirstEnergy (already implicated in August 2003 blackout). FirstEnergy now used as example of what can go wrong in control system security

Key Control System Recommendations

Technology: IPS and patching

Policy :Create and enforce proper network architecture
Create and enforce proper patching policy

Source: Public Record <http://www.securityfocus.com/news/6767>

Fired employee plants trojan to shutdown transport site

Problem

An employee disgruntled at being fired from a major Asian transport site planted a trojan to wipe out 3 of the site's main SCADA servers. Due to a fault in the trojan, only one server was completely wiped out.

Consequences

Transport services controlled by the SCADA server were stopped for several days. Several days work was also required to reconstruct the server.

Key Control System Recommendations

Technology: host intrusion monitoring incl. file and process monitoring

Policy :restrict control system access as a prelude to firing employees

Source: Verano Contact

CIA plants trojan to shutdown trans-Siberian pipeline

Problem

In the late 1970s the US CIA planted a trojan in control system software that was acquired by the Soviet Union. The trojan was designed to set pump speeds and valve settings over tolerance. The software was used in the newly built trans-Siberian pipeline and activated in June, 1982.

Consequences

An estimated 3 kiloton explosion visible from space by NORAD satellites. “The result was the most monumental non-nuclear explosion and fire ever seen from space.”

Key Control System Recommendations

Technology: buy control systems from reputable vendors

Policy :test unknown systems components before implementation

Source: Public Record

<http://www.nytimes.com/2004/02/02/opinion/02SAFI.html?ex=1128484800&en=8f4cabff85e9014e&ei=5070&ex=1099022400&en=7029ca0373f5d4d0&ei=5070&oref=login>

Disgruntled ex-employee hacks SCADA system and releases sewage

Problem

During early 2000, ex-Hunter Watertech employee Vitek Boden hacked into the Maroochy Shire wastewater system in Queensland, Australia 46 times. He used commercially available equipment, took complete control of the system including fresh water control nodes, and was undetected. Boden was only apprehended when police stopped his car and found a stolen computer and radio transmitter.

Consequences

Several million liters of sewage was released into waterways, marine life was killed, stench unbearable to residents, negative publicity, AUS\$13k cleanup, and AUS\$176k in extra security and monitoring costs

Key Control System Recommendations

Technology: control system monitoring: NIDS, HIDS

Policy :implement secure access policy and network architecture

Source: Public Record

<http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26?language=printer>

Airline systems crippled by multiple worms

Problem

On January 25, 2003 Continental Airlines lost electronic ticketing, kiosk and web site services due to Slammer worm. On August 19, 2003 Air Canada lost reservation and check-in systems due to the Nachi worm. On May 1, 2004 Delta Airlines was allegedly infected by Sasser worm. In many cases properly patched systems were overwhelmed by network traffic from infected systems.

Consequences

Many cancelled flights, extra manual work, lost bookings, lost revenue

Key Control System Recommendations

Technology: IPS and network segmentation

Policy :implement secure patching policy

Source: Public Record

<http://www.washingtonpost.com/wp-dyn/articles/A46928-2003Jan26.html>

Vulnerabilities

- What is a security vulnerability?
 - Weakness, “Lack of...”
 - DHS Definition: “Vulnerability is the existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of an organization, system, network, application, or protocol.”



What are Vulnerabilities?

➤ What causes a vulnerability?

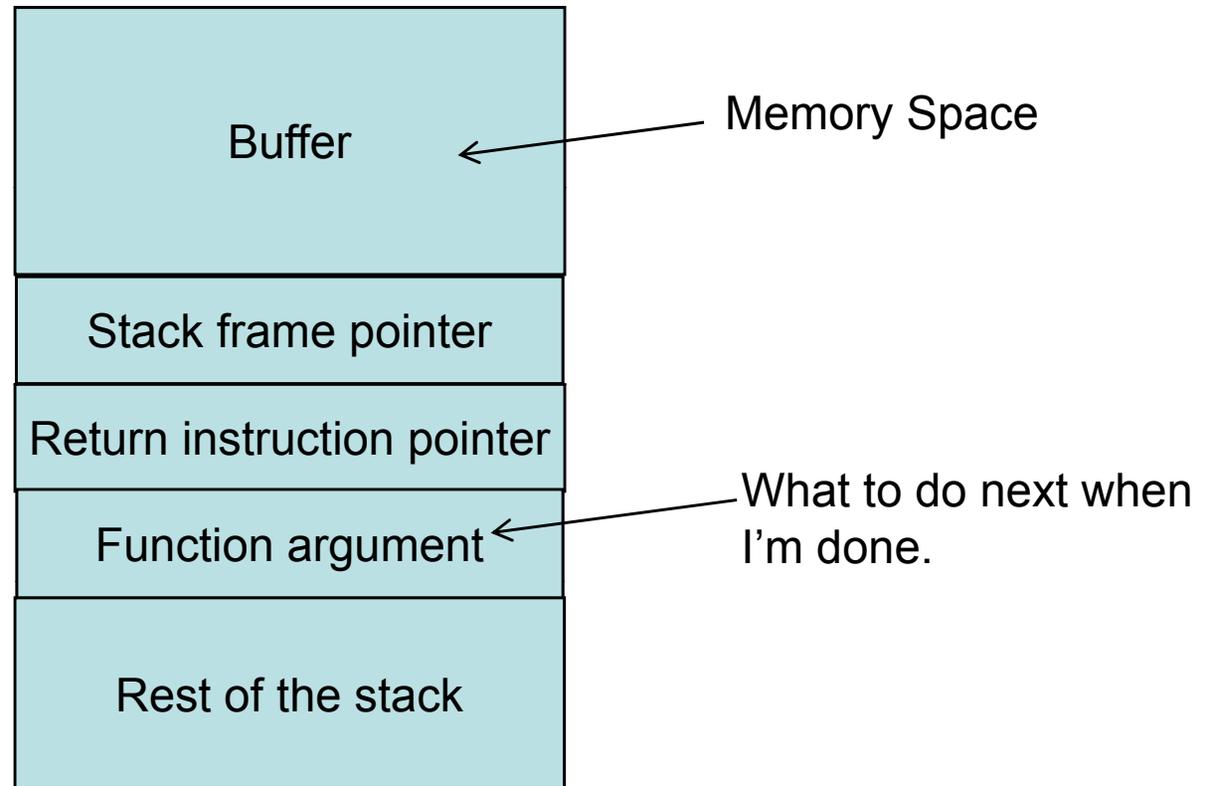
Human error

1. Misconfigurations
 - Permissions and Access
2. Mismanaged / non-enforced policy
 - Trust Relationships (Dual-homed systems)
3. Lack of user training / understanding
 - Unauthorized web surfing or software
4. Poorly written code
 - Exploits USE the rules... not break them.
 - Buffer Overflows



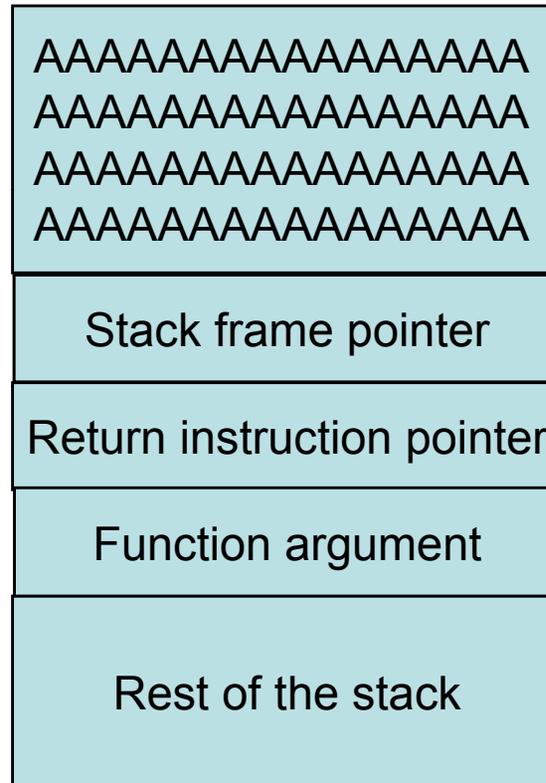
30,000 Foot View of Buffer Overflows

The Buffer/Stack Overflow



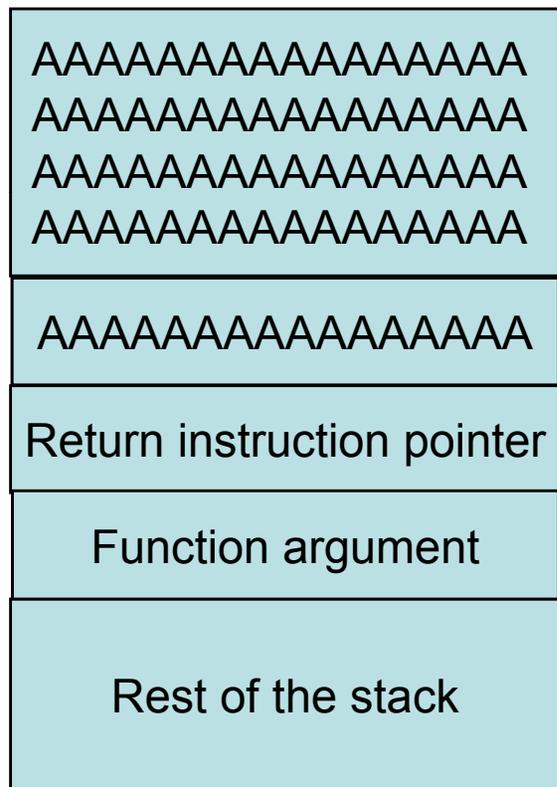
30,000 Foot View of Buffer Overflows

The Buffer/Stack Overflow



30,000 Foot View of Buffer Overflows

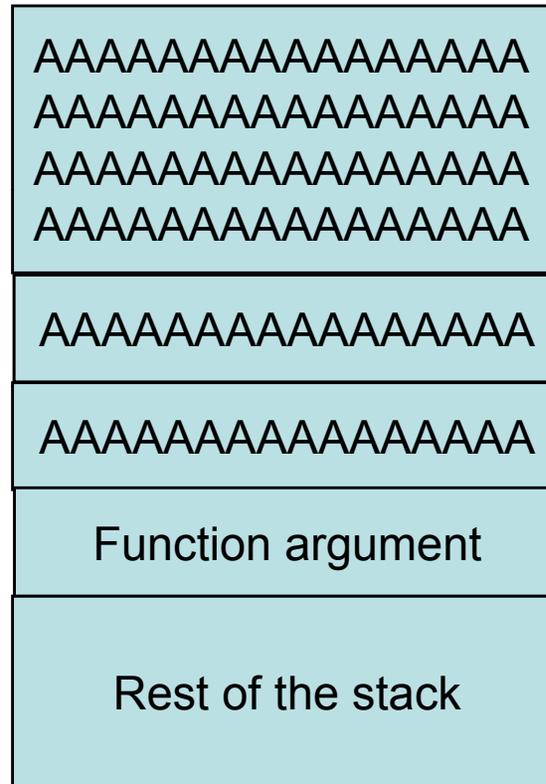
The Buffer/Stack Overflow



The Buffer has overflowed

30,000 Foot View of Buffer Overflows

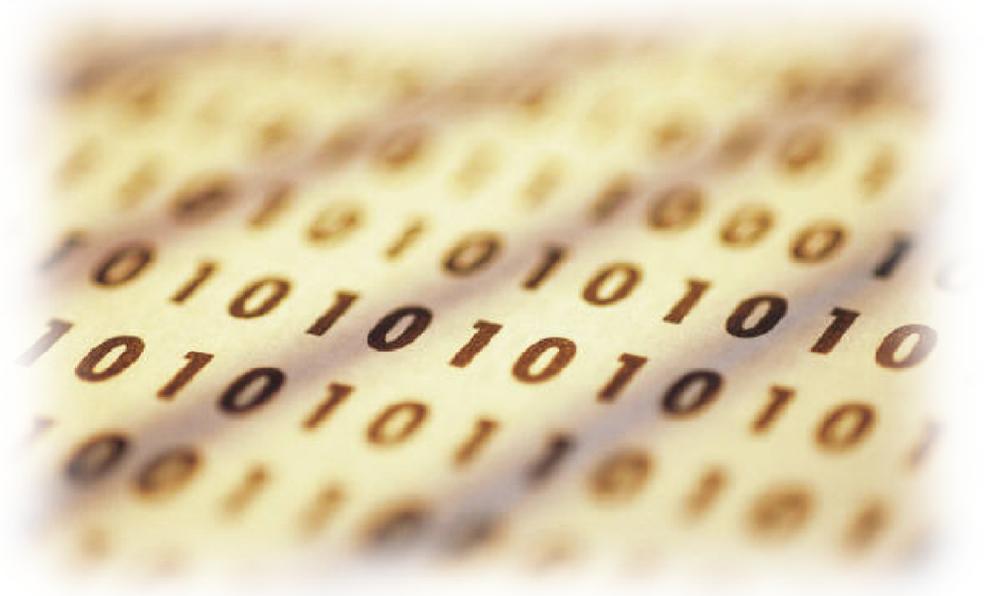
The Buffer/Stack Overflow



My instructions are gone! What do I do now?

30,000 Foot View of Buffer Overflows

- Now What?
- New Instructions (“Arbitrary Code”)
- Denial of Service (DoS) – Discussed later



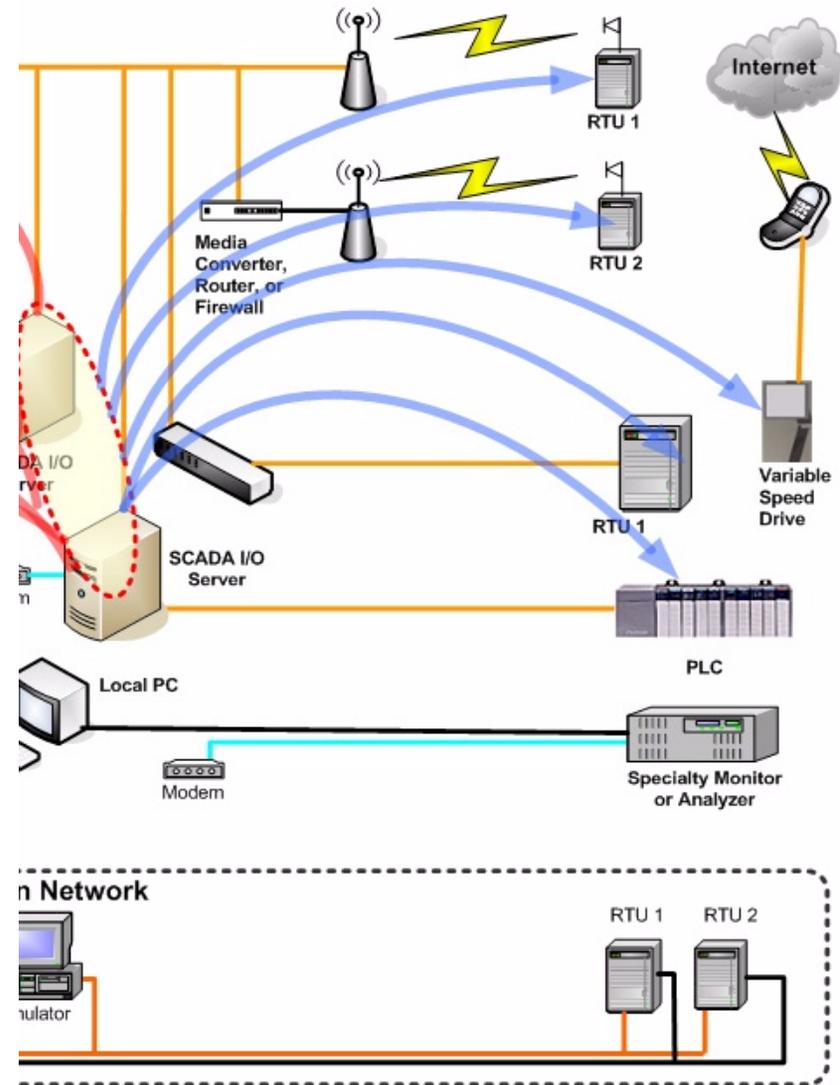
Overall Most Common Vulnerabilities

➤ Network

- Security efforts focused solely on Corporate Internet interface point (Castle Model)
- Routers vs. Firewalls
- Out-of-date Router and Firewall Firmware
- Sharing network infrastructure with business/IT systems
- Use of clear-text protocols for device configuration
- Insufficient network separation between corporate and real-time control systems
- Access to critical systems for 3rd parties and remote users often wide open once authentication is made (too many privileges)
- Network Performance and Security Monitoring not typically found on the Industrial Networks.
- Field Devices Vulnerable to various TCP/IP communication packets

SCADA Protocols with Control Devices Vulnerable

- Communications between SCADA Servers and control devices sent in the clear (no encryption)
- Computers do not need to authenticate to the end devices (no authentication)
- Sessions between SCADA Servers and end devices can be hijacked
- High network traffic and malformed packets often crash PLCs, RTUs, and other control devices (DoS)



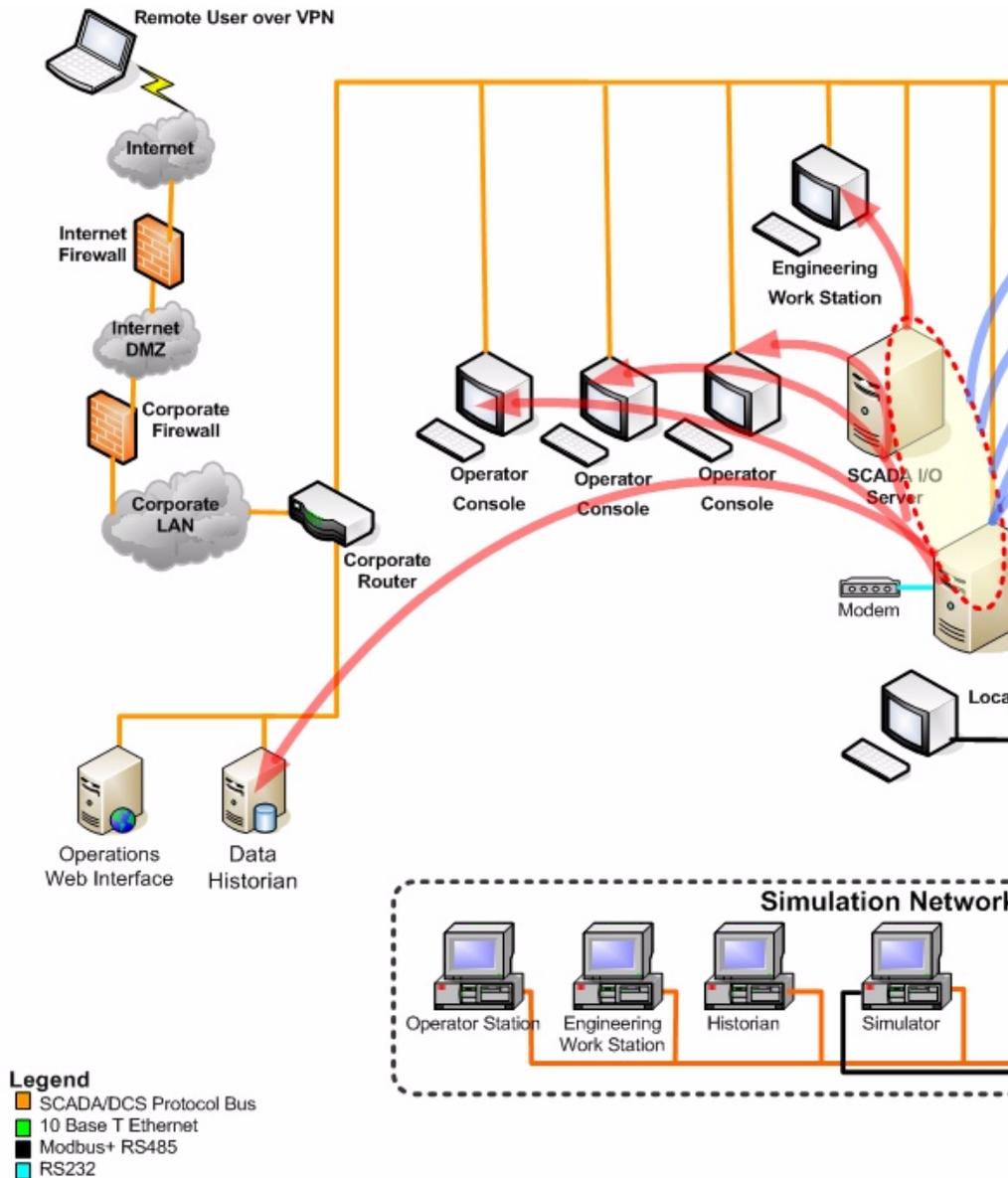
Sample Logical Network Diagram

Overall Most Common Vulnerabilities

➤ Workstations/Servers Configuration

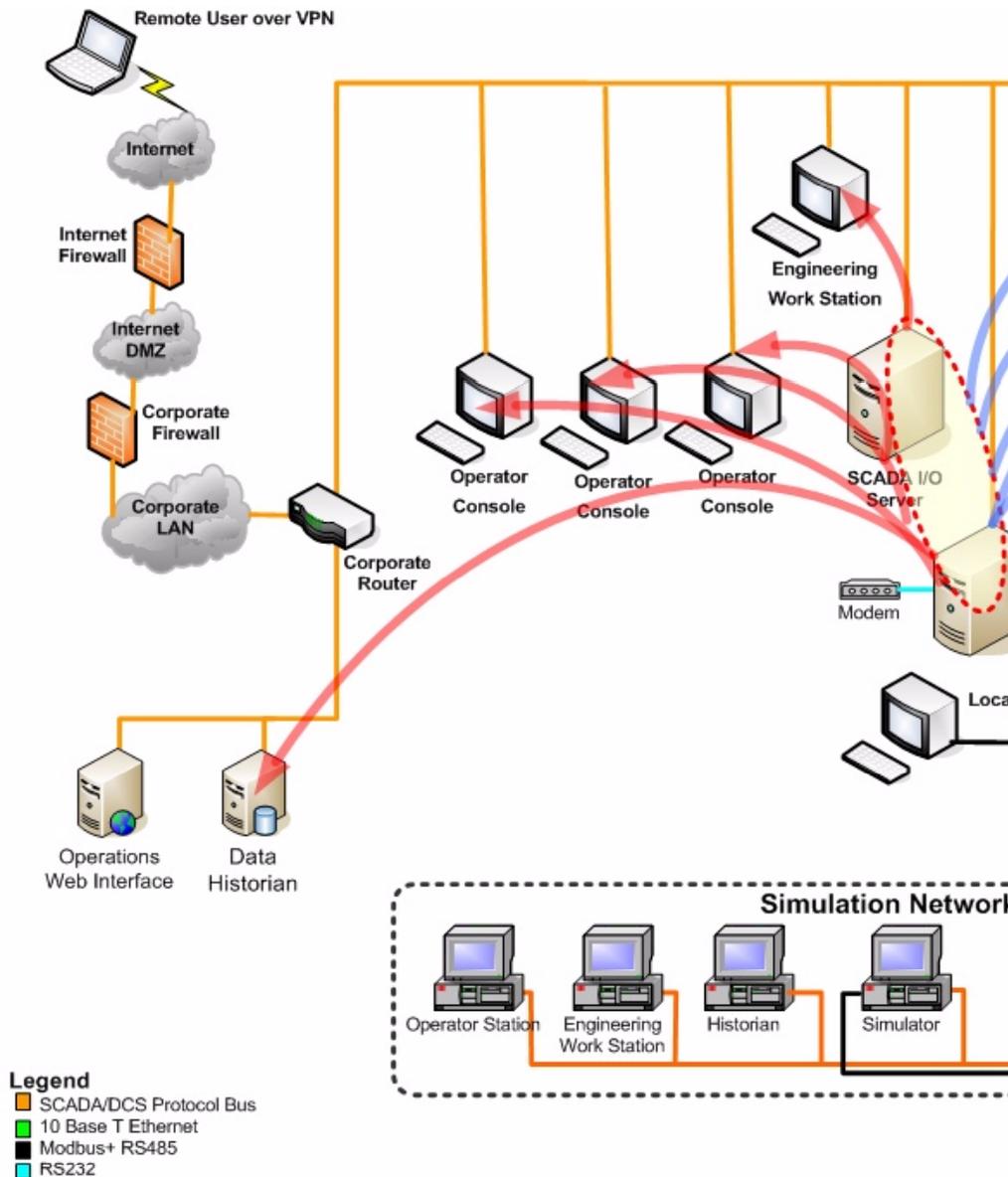
- Password cracking made easy with LMHash enabled (left ON by default installation)
- Easy-to-Guess Passwords
- Null-Session Authentication
- Local Security Policy left with defaults
- Security Event Logging Often Not Enabled
- Domain Security Policy often not used in real-time systems due to multiple domains
- Heavy use of Shared Folders on workstations
- Shared Folders have access set to “Everyone”
- Dual-Network cards installed and in use

SCADA API Communications Vulnerable



- Communications between SCADA workstations are often sent in the clear (no encryption)
- Computers do not need to authenticate to the SCADA system (no authentication)
- Sessions between SCADA workstations and servers can be hijacked
- If key critical servers go down, the whole system will go down (DoS)
- System operator graphic files can be altered

Take control of SCADA system



- Sessions between SCADA workstations and servers can be hijacked
- TELNET, X-sessions, and other client/server based communications can be intercepted through “Man-in-the-Middle” attacks
- While in a session hijack, the attacker can do anything that the source or destination can do
- In a SCADA System, a session hijack can be used to take control of the control room LAN

Anatomy of an Attack



1. Recon – Casing the joint
2. Scanning – Target and entry point acquisition
3. Enumeration – Gather inside Intel
4. Gaining Access – We're in
5. Escalating Privileges – Own the System
6. Pilfering – Own the network. Game over.
7. Covering Tracks – Hide the evidence
8. Leaving Back Doors – Come Back later
9. Denial of Service – Time out.

Anatomy of an Attack



1. **Recon – Casing the joint**
2. Scanning – Target and entry point acquisition
3. Enumeration – Gather inside Intel
4. Gaining Access – We're in
5. Escalating Privileges – Own the System
6. Pilfering – Own the network. Game over.
7. Covering Tracks – Hide the evidence
8. Leaving Back Doors – Come Back later
9. Denial of Service – Time out.

Recon > Public Information

➤ Gathering public information

- Helps determine IP ranges, entry points, social engineering tactics, DNS/host information, and other crucial bits of information.
- <http://www.sec.gov/cgi-bin/srch-edgar> - Securities and Exchange commission public database on all publicly traded companies
- <http://www.networksolutions.com> - Find out who owns a particular domain
- <http://www.arin.net> - Find out who owns a particular IP block
- <http://www.samspace.org> - Several online information tools
- <http://www.netcraft.com> - Find out the operating system and uptime of the host

Recon > Public Information

Netcraft - Search Web by Domain - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://searchdns.netcraft.com/?restriction=site+contains&host=ca

Customize Links Free Hotmail Windows Marketplace Windows Media Windows

Netcraft Netcraft - Search Web by Domain

site contains

example: site contains .sco.com

Results for careerbuilder.com

Found 69 sites

Site	Site Report	First seen	Netblock	OS
1. www.careerbuilder.com		July 1996	CareerBuilder	Windows Server 2003
2. msn.careerbuilder.com		April 2004	CareerBuilder, Inc.	Windows Server 2003
3. tec.careerbuilder.com		August 2005	Crossvale	Linux
4. careerbuilder.com		April 1997	CareerBuilder	Windows Server 2003
5. information-technology.careerbuilder.com		December 2004	Quality Technology Services, LLC.	Windows Server 2003
6. jobs.msn.careerbuilder.com		April 2005	Quality Technology Services, LLC.	Windows Server 2003
7. accounting.careerbuilder.com		November 2003	Quality Technology Services, LLC.	Windows Server 2003
8. admin-clerical.careerbuilder.com		August 2005	Quality Technology Services, LLC.	Windows Server 2003

888.664.6388

Learn how we can help your online business.

Call INetU today to schedule a free consultation.

888.664.6388

Recon > Public Information

Netcraft What's That Site Running Results - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://uptime.netcraft.com/up/graph/?host=www.careerbuilder.com

Netcraft

Whats that site running?

Netcraft Services

- Sites on the Move
 - Today's changes
 - Last week
 - Last Month
- Internet Exploration
 - Netcraft Toolbar
 - What's that site running?
 - Search Web by Domain
- Internet Data Mining
 - Hosting Provider Switching Analysis
 - Hosting Provider Server Count
 - Hosting Reseller Survey
 - SSL Survey
 - Web Server Survey Archive
- Performance
 - Hosting Providers' Network Performance
 - Dedicated Server Monitoring
- Security
 - Anti-Phishing Toolbar
 - Automated Security

OS, Web Server and Hosting History for www.careerbuilder.com

http://www.careerbuilder.com was running Microsoft-IIS on Windows Server 2003 when last queried at 27-Jan-2007 00:16:16 GMT - refresh now Site Report

OS	Server	Last changed	IP address	Netblock Owner
Windows Server 2003	Microsoft-IIS/6.0	2-Jan-2007	64.88.161.59	CareerBuilder
Windows Server 2003	Microsoft-IIS/6.0	29-Dec-2006	66.179.0.222	CareerBuilder, Inc.
Windows Server 2003	Microsoft-IIS/6.0	23-Dec-2006	64.88.161.59	CareerBuilder
Windows Server 2003	Microsoft-IIS/6.0	22-Dec-2006	66.179.0.222	CareerBuilder, Inc.
Windows Server 2003	Microsoft-IIS/6.0	19-Dec-2006	64.88.161.59	CareerBuilder
Windows Server 2003	Microsoft-IIS/6.0	15-Dec-2006	66.179.0.222	CareerBuilder, Inc.
Windows Server 2003	Microsoft-IIS/6.0	13-Dec-2006	64.88.161.59	CareerBuilder
Windows Server 2003	Microsoft-IIS/6.0	11-Dec-2006	66.179.0.222	CareerBuilder, Inc.
Windows Server 2003	Microsoft-IIS/6.0	8-Dec-2006	64.88.161.59	CareerBuilder
Windows Server 2003	Microsoft-IIS/6.0	7-Dec-2006	66.179.0.222	CareerBuilder, Inc.

No uptime is currently available for www.careerbuilder.com.

INetU
Managed Hosting
www.inetu.net
888.664.6388

Learn how we can help your online business.
Call INetU today to schedule a free consultation.
888.664.6388

Recon > Google Hacking

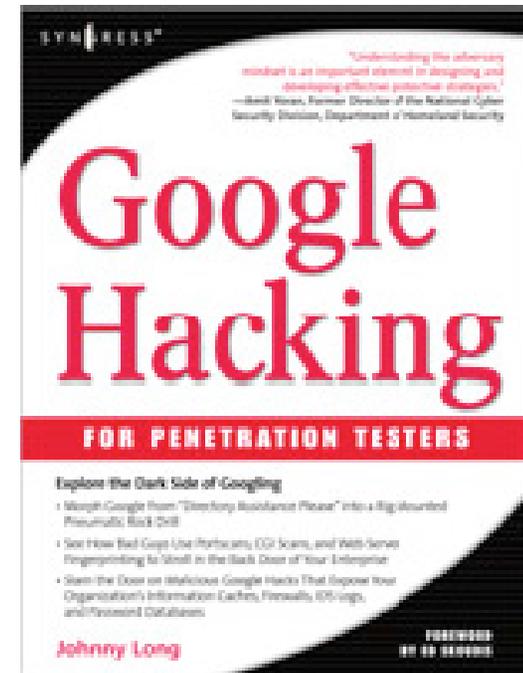
➤ Google

➤ What Has Been Found Using Google?

- Backend Databases (SQL/Access/Oracle)
- File Servers, Intranet (Hidden Pages), Internal Web Cams, Network Devices (routers, firewalls, IDS appliances, and more), Print Servers, VoIP Management Interfaces, PBX Systems, UPS Systems, and Physical Access Control Administration pages
- **Process control Software and Equipment Administration Web Interfaces**
- Sensitive Government Documents
- Usernames, Passwords, and Identify Thief
- Corporate Identify Thief on the Rise

➤ Want to Know More?

- “Google Hacking for Penetration Testers” by Johnny Long
- Syngress Publishing
- <http://johnny.ihackstuff.com>



Recon > Server Information

- Online Whois servers:
 - <http://www.ripe.net> - European IP address allocations
 - <http://www.apnic.net> - Asia Pacific IP address allocations
 - <http://whois.nic.mil> - US military
 - <http://www.nic.gov/whois.html> – US government
- DNS (Domain Name Server) Zone Transfer using “nslookup”
 - Requires DNS relaxed configuration
 - The zone_transfer file can now be easily filtered or parsed for keywords and information we are looking for such as MX and A records.

Recon > Path Information

- Use “traceroute” to map the path traffic takes to get to the target
 - Shows every hop
 - “Visualroute” and “NeoTrace” can show you physical locations on a world map
 - Many times, using the “fixed port” option can get you right past firewalls!
 - (Bypassing firewalls is discussed more in depth in the advanced hacker methodology).

Recon > Path Information

The screenshot shows the NeoTrace application window with the following details:

- Browser Title:** NeoTrace: www.ci-institute.org
- Target:** www.ci-institute.org
- Map:** A map of North America with a green path starting at Calgary, Alberta, Canada, and ending at New York, USA. The path passes through Toronto, Ontario, Canada.
- Info Pane (Right):**
 - Address: iphost-64-56-144-218.cgy.wiband.net
 - Navigation: Previous | Node 18 of 18 | Next
 - Name: iphost-64-56-144-218.cgy.wib
 - IP Address: 64.56.144.218
 - Location: 51.000N, 113.750W
 - Network: Unknown
 - Text: See Registrant Pane for registrant con
- Footer:** Version 3.25 - TRIAL

Recon > Social Engineering

➤ Social Engineering

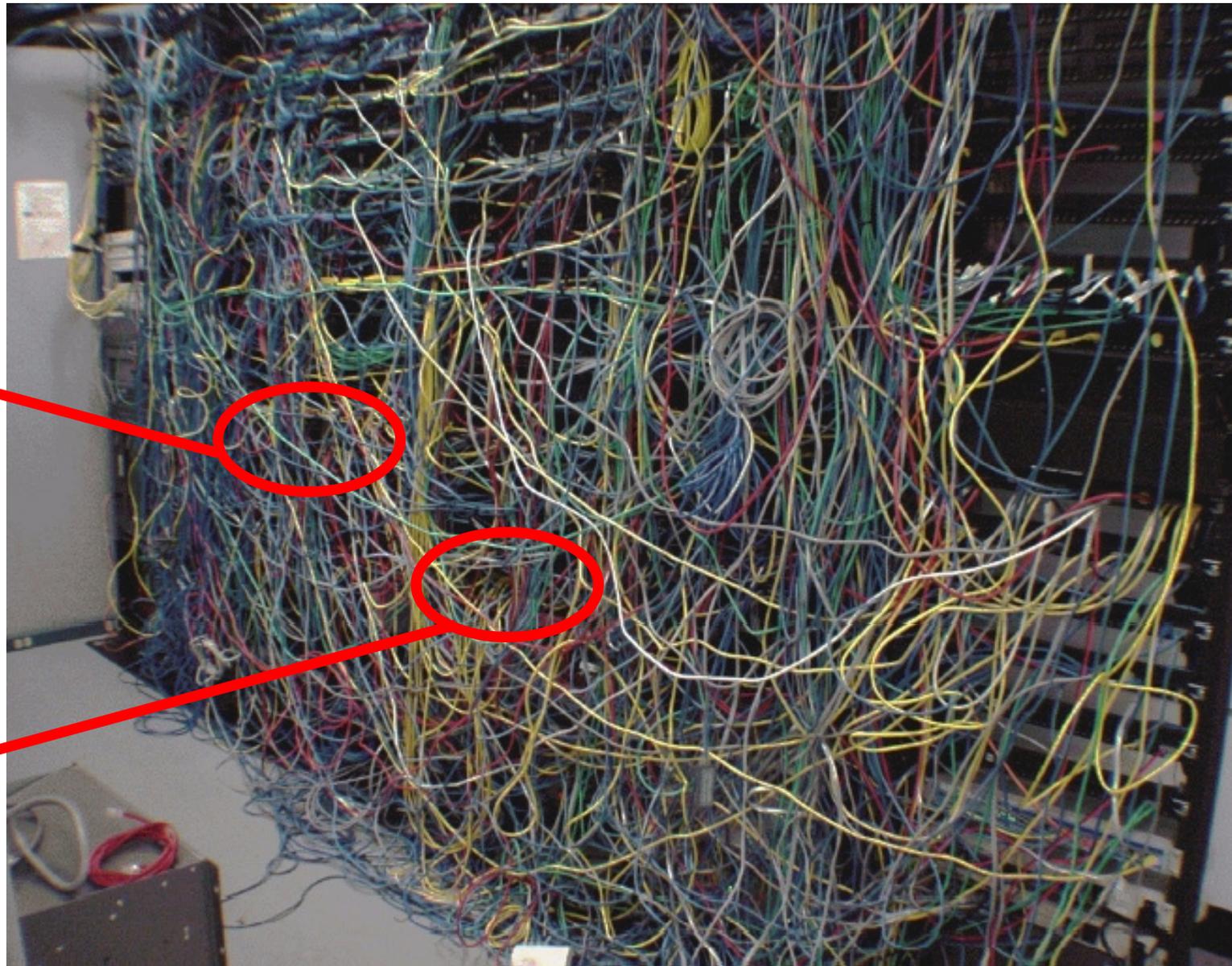
- Very easy to get information from untrained users
- 98% of users are not properly trained
- Gain trust
- Talk fast and/or cause confusion
- Use technical jargon on less technical users
- “Pull Rank”, bully
- Perfect reference:
“The Art of Deception” – Kevin Mitnick
- Best examples in the film “Sneakers”, “Hackers”,
and “Hackers 2: Takedown.”
- Plant devices for later access



Recon > Social Engineering > Nice Place to Hide Things....

Can you find that planted PDA that is capturing over 4 Gigs of passwords, emails, and all communications In and out of the network?

Can you find that planted WiFi Access Point that is allowing rouge access to your network?



Anatomy of an Attack

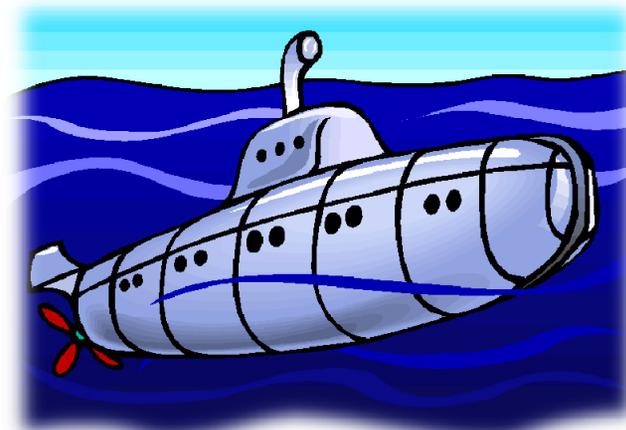


1. Recon – Casing the joint
2. **Scanning – Target and entry point acquisition**
3. Enumeration – Gather inside Intel
4. Gaining Access – We're in
5. Escalating Privileges – Own the System
6. Pilfering – Own the network. Game over.
7. Covering Tracks – Hide the evidence
8. Leaving Back Doors – Come Back later
9. Denial of Service – Time out.

Scanning

➤ Ping/Host Scanning

- Ping, or host, Scanning allows us to see what hosts are up on a given subnet.
- Nmap typically used
- The Windows tool Superscan can automate this process with point and click functionality.



Scanning

```
c:\ Command Prompt

C:\Documents and Settings\Clint>nmap -sP 192.168.1.0/24

Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2007-01-29 11:01 Central
Standard Time
Host 192.168.1.1 appears to be up.
MAC Address: 00:14:BF:4A:8E:F3 (Cisco-Linksys)
Host 192.168.1.102 appears to be up.
Host 192.168.1.112 appears to be up.
MAC Address: 00:90:4B:B8:DD:08 (GemTek Technology Co.)
Nmap finished: 256 IP addresses (3 hosts up) scanned in 34.484 seconds

C:\Documents and Settings\Clint>_
```

Scanning

➤ Port Scanning

- Allows us to determine what ports are open and what services might be on discovered hosts.
- Scan Types:
 - **TCP connect scan**
 - **TCP SYN scan**
 - **TCP FIN Scan**
 - **TCP Xmas Tree Scan**
 - **TCP Null**
 - **TCP ACK Scan**
 - **TCP Windows**
 - **TCP RPC Scan**
 - **UDP Scan**

Scanning

➤ **Operating System Detection**

- Each OS handles different facets of the IP stack in different ways.
- Several different probes crafted in different ways can be sent to the target and, based on the return information, we can guess the target's operating system.
- Active IP Stack characteristics:
 - **FIN Probe**
 - **Bogus Flag Probe**
 - **Initial Sequence Number (ISN) Sampling**
 - **“Don't Fragment Bit” Monitoring**
 - **TCP Initial Window Size**
 - **ACK Value**
 - **ICMP Error Message Quenching**
 - **ICMP Message Quoting**
 - **ICMP Error Message-Echoing Integrity**
 - **Type of Service (TOS)**
 - **Fragmentation Handling**
 - **TCP Options**

Scanning

- Nmap can automate this using the “-O” option.

```
Command Prompt
C:\Documents and Settings\Clint>nmap -O 192.168.1.112

Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2007-01-29 11:04 Central
Standard Time
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
Interesting ports on 192.168.1.112:
(The 1670 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:90:4B:B8:DD:08 (GemTek Technology Co.)
Device type: general purpose
Running: IBM AIX 4.X, Microsoft Windows 2003/.NET|NT/2K/XP
OS details: IBM AIX 4.3.2.0-4.3.3.0 on an IBM RS/*, Microsoft Windows 2003 Server or XP SP2, Microsoft Windows XP SP2

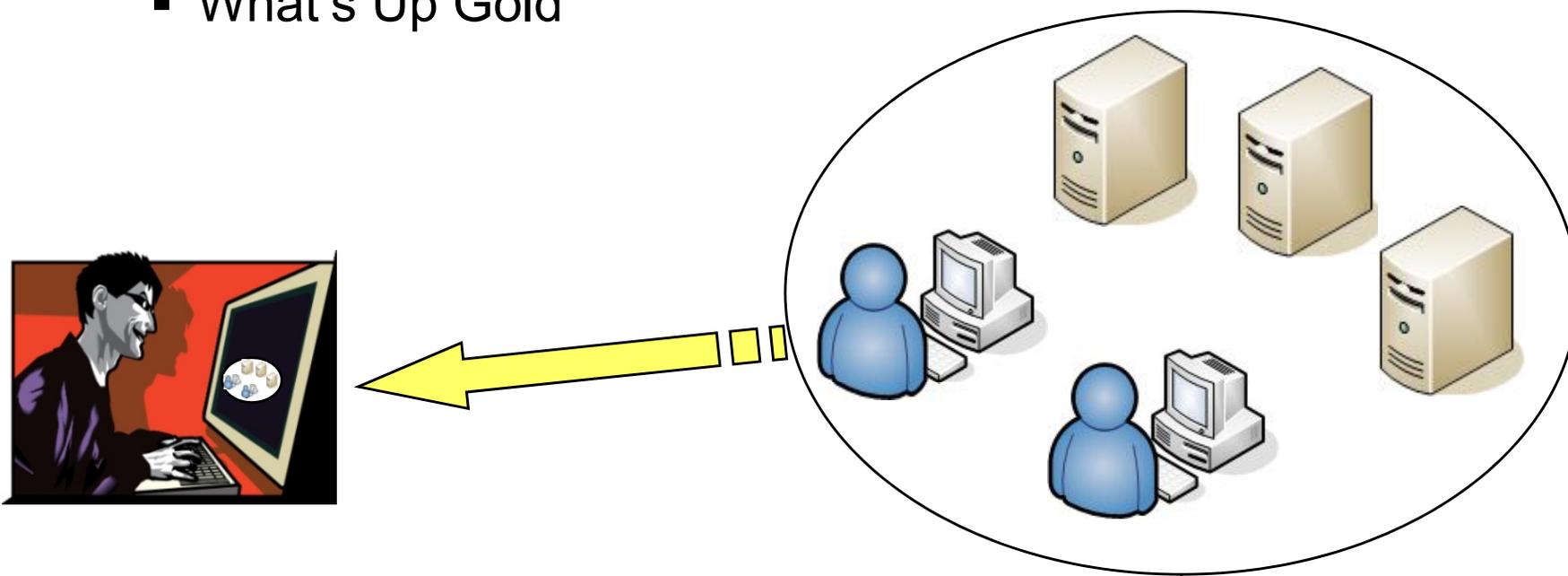
Nmap finished: 1 IP address (1 host up) scanned in 38.250 seconds

C:\Documents and Settings\Clint>
```

Scanning

➤ Automated Discovery Tools

- Many aspects of both the Recon and Scanning stages are automated in several easy to use tools both open source and commercial.
 - Cheops (<http://www.marko.net/cheops/>)
 - What's Up Gold



Anatomy of an Attack



1. Recon – Casing the joint
2. Scanning – Target and entry point acquisition
3. **Enumeration – Gather inside Intel**
4. Gaining Access – We're in
5. Escalating Privileges – Own the System
6. Pilfering – Own the network. Game over.
7. Covering Tracks – Hide the evidence
8. Leaving Back Doors – Come Back later
9. Denial of Service – Time out.

➤ Banner Grabbing

- Banner grabbing is the most fundamental aspect of enumeration.
- Many tools and techniques from the previous two sections have banner grabbing functions.
- Banner grabbing is as simple as connecting to an open port and observing the output:

Enumeration

TCP Port	Banner
21 File Transfer [Control]	220 Welcome to Verano's FTP service. --> USER anonymous 530 This FTP server does not allow anonymous logins. 331 Please specify the password. --> PASS anon@anon.com 530 Login incorrect. --> SYST 530 Please login with USER and PASS. --> QUIT 221 Goodbye.
22 SSH Remote Login Protocol	SSH-2.0-OpenSSH_3.9p1
80 World Wide Web HTTP	HTTP/1.1 200 OK Date: Mon, 29 Jan 2007 19:38:28 GMT Server: Microsoft-IIS/5.0 X-Powered-By: ASP.NET X-AspNet-Version: 1.1.4322 Set-Cookie: ASP.NET_SessionId=vbwrpaqen2qff3qwcw5c25ae; path=/ Cache-Control: private Content-Type: text/html; charset=utf-8

Enumeration

➤ Enumerating Network Services

- SMTP
 - “vrfy” command verifies the existence of a given username.
 - “expn” command reveals the actual delivery address of aliases and mailing lists.
- DNS
 - Zone transfers discussed earlier
 - “ls -d”
- Microsoft RPC (MSRPC), TCP Port 135
 - Epdump
 - Rpcdump
 - Superscan

Enumeration

➤ NetBIOS Name Service, UDP 137

- As of Windows 2000 no longer necessary but still enabled by default
- Net View will enumerate workgroups and domains:

```
C:\>net view /domain
```

```
Domain
```

```
-----
```

```
-----
```

```
WORKGROUP
```

```
CORPORATE_DOMAIN
```

```
TEST_LAB
```

```
SMITH
```

```
The command has completed successfully.
```

Enumeration

- Net View will also enumerate computers in a particular domain:

```
C:\>net view /domain:test_lab
```

```
Server Name                                     Remark
```

```
-----
```

```
-----
```

```
\\TEST1
```

```
\\TEST2
```

```
\\FILESERVER
```

```
\\SQLSERVER
```

The command has completed successfully.

Enumeration

- Other tools from the Windows Resource Kit provide more information.
- Nltest – enumerates domain controllers
- Netviewx – enumerates network services
- Nbtstat – dumps the NetBIOS name table on a particular host. This shows users and shares.
- Nbtscan (<http://www.inetcat.org/software/nbtscan.html>) is great for enumerating windows hosts and information on a network:

```
C:\>nbtscan 192.168.234.0/24
```

```
Doing NBT name scan for addresses from 192.168.234.0/24
```

IP address	NetBIOS Name	Server	User	MAC address
192.168.234.36	WORKSTN12	<server>	CSMITH	00-00-86-16-47-d6
192.168.234.112	SQLSVR	<server>	ADMIN	00-a0-cc-57-8c-8a

Enumeration > Null Session

➤ NetBIOS Session Enumeration, TCP Port 139

- Establish a session first using “net use”.

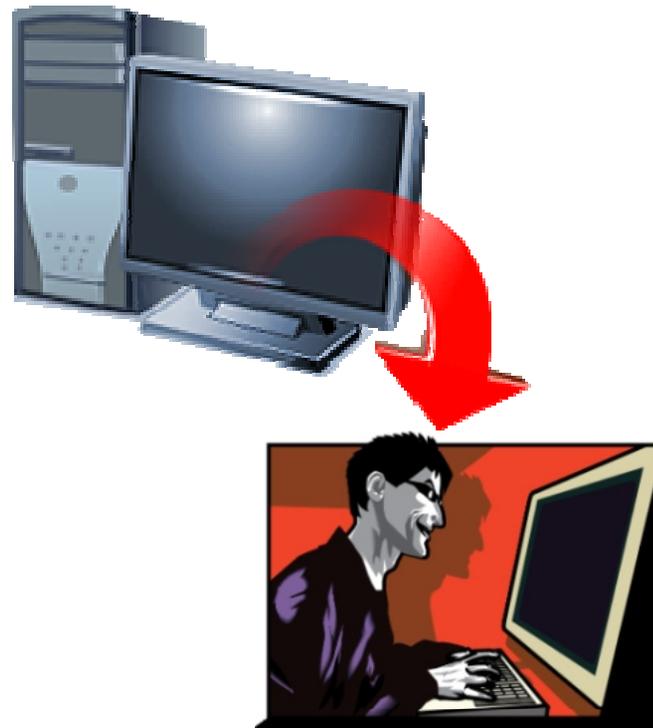
```
C:\>net use \\192.168.202.33\IPC$ "" /z:""
```

- Once a session is established you can enumerate shares using “net view”.
- Some automated share enumeration tools include:
 - DumpSec
 - Legion
 - NetBIOS Auditing Tool (NAT)
 - Superscan 4 by Foundstone.
- With an admin password the registry can be enumerated through this session.

Enumeration

➤ NetBIOS Session Enumeration, TCP Port 139 (cont)

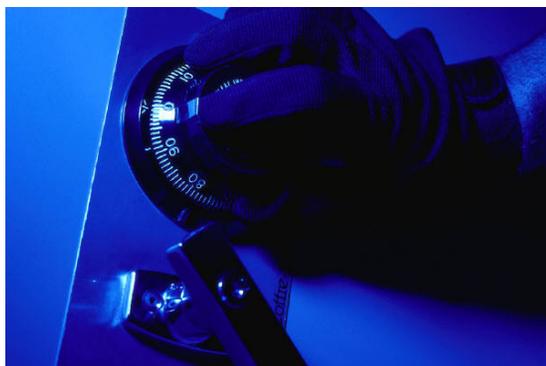
- “enum” written by Bindview (<http://razor.bindview.com>)
 - can perform all of the windows enumerations tools mentioned above and more including remotely guessing and cracking passwords to NetBIOS and SMB sessions.



Enumeration

- SNMP Enumeration, UDP Port 161
 - SNMP enumeration is more than just gathering parameter device configuration data.
 - SNMP can betray even the most locked down systems due to the implementation of MIBs since many strings are left default or easily guessed.
 - Tools include snmputil, snmpget (linux), and snmpwalk (linux).
 - Solarwind's IP Network Browser (<http://www.solarwinds.net>) can provide an easy to use graphical interface for SNMP enumerating.

Anatomy of an Attack



1. Recon – Casing the joint
2. Scanning – Target and entry point acquisition
3. Enumeration – Gather inside Intel
4. **Gaining Access – We're in**
5. Escalating Privileges – Own the System
6. Pilfering – Own the network. Game over.
7. Covering Tracks – Hide the evidence
8. Leaving Back Doors – Come Back later
9. Denial of Service – Time out.

Gaining Access > Passwords

- At this point not cracking (That's later)
- Password guessing
- Dictionary attacks
- Password brute forcing
 - Defeat cryptographic scheme with large number of possibilities
 - Hydra (www.thc.org)



Gaining Access > Bypassing Authentication

- Let's just bypass the password altogether!
- Must be at the local console
- Technique uses LiveCD distribution



Gaining Access

- Finding a way in with known exploits
 - Vulnerability Databases/Repositories
 - www.securityfocus.com
 - www.securitytrap.com
 - www.packetstormsecurity.org
 - <http://osvdb.org>
 - “Canned Exploits”
 - Require little skill
 - Most production systems are susceptible due to patch implementation time
 - Security Scanning/Testing

Gaining Access

➤ Automated Testing Tools

- Automatically scan an entire network for known vulnerabilities
- Two types... Security Scanners, Security Testers (Automated Hacking Tool)
 - Scanners do not penetrate/exploit
 - Tester WILL exploit systems
- Scanners can be easy to detect... very “noisy”
- Scanners not always reliable... can produce false positives
- All depends on quality and quantity of signatures
- Free Tools seem to have more functionality but have more controls in place.

Gaining Access



- Popular Automated Testing Tools:
 - SARA – Descendant of S.A.T.A.N. (**S**ystem **A**ddministrator's **T**ool for **A**nalyzing **N**etworks)
 - SAINT – Commercial Descendant of S.A.T.A.N.
 - Nessus – Free
 - NeWT – Free Windows Based Nessus
 - Retina – Commercial
 - ISS Scanner – Commercial

Gaining Access

➤ Automated Hacking Tools

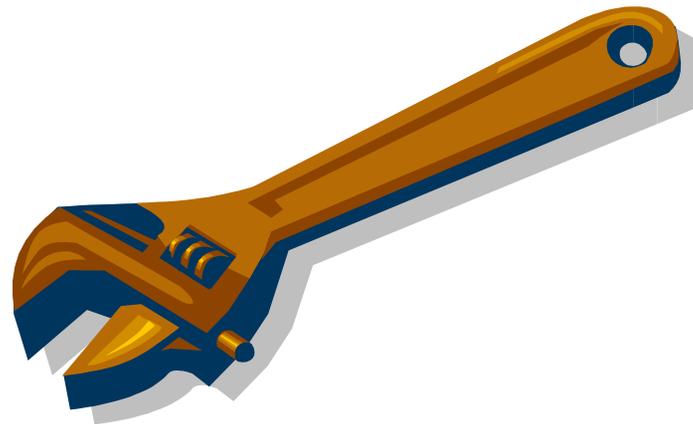
- Automatically check hosts for known vulnerabilities
- Can be stealthy
- Very reliable
- All depends on quality and quantity of exploits
- Slow – One host at a time



Gaining Access

➤ Popular Automated Testing Tools:

- Immunitysec CANVAS (www.immunityinc.com)
- Core IMPACT (www.coresecurity.com)
 - Full Featured Security Penetration Tester
- Metasploit (www.metasploit.com)
 - Open-source version of CANVAS and Impact



Gaining Access > Defeating Firewalls

- Bypassing ACL (Access Control Lists) and firewall rules
 - Configuration vulnerabilities
 - Techniques
 - Use an existing service that has a
 - Source “porting”
 - Pretending to be another service
 - Outbound
 - Can use external proxies
 - Session hijacking (TCP Splicing)
 - Protocol Tunneling
 - Ping (ICMP data)
 - Http
 - TCP extra 6 bits
 - Tool: Firewalk



Gaining Access > Web-Based Attacks

Web-based Attacks - Traditional

- Directory Traversal
 - Permission configuration flaw
- DNS hijacking based web defacement
 - Exploiting the server and take over
 - DNS cache poisoning



Gaining Access > Web-based Attacks - Advanced

➤ SQL (Structured Query Language) injection

- Vulnerable web interface
- Non-filtered input fields
- Allows “break” characters
 - Login: hi' or 1=1--
 - Pass: hi' or 1=1—
 - <http://duck/index.asp?id=hi' or 1=1-->



	+2.000
	+5.000
	+1.500
	+1.125
	+1.062

Gaining Access > WiFi

➤ WiFi

- Way too many issues to cover in this presentation
- Numerous unsecured access points
- Access not contained do DMZ
- Traffic in the air easily monitored
- WEP easily cracked
- Tools:
 - Kismet
 - Aircrack
 - Airsnort
 - AirPcap



Bluetooth Hacking (Bluejacking)

- Network connected peripherals use bluetooth
- Security usually left open by default
- New technology
 - Security not a forethought
 - Hackers find ways to exploit faster than security is implemented
- Tools:
 - Bluesniff
 - Redfang
 - Bluestumbler



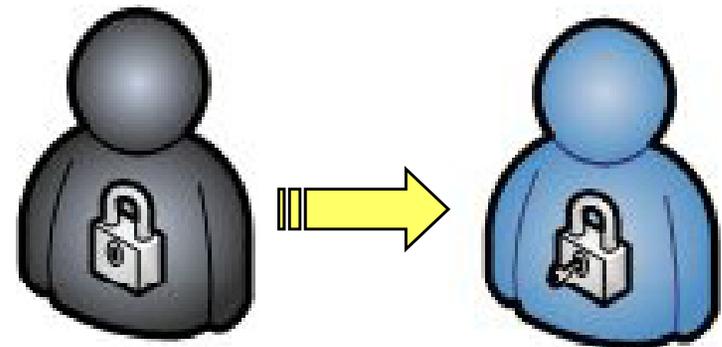
Anatomy of an Attack



1. Recon – Casing the joint
2. Scanning – Target and entry point acquisition
3. Enumeration – Gather inside Intel
4. Gaining Access – We're in
5. **Escalating Privileges – Own the System**
6. Pilfering – Own the network. Game over.
7. Covering Tracks – Hide the evidence
8. Leaving Back Doors – Come Back later
9. Denial of Service – Time out.

Privilege Escalation

- Privilege Escalation Techniques
- Obtaining Root or Admin
 - Buffer Overflows
 - Permissions
 - Permission “cascades” can be overwhelming
 - Permission inheritance may allow unwanted access
 - Applications may add unexpected permissions
 - SUID Root
 - Password Cracking
 - Known Exploits



Anatomy of an Attack



1. Recon – Casing the joint
2. Scanning – Target and entry point acquisition
3. Enumeration – Gather inside Intel
4. Gaining Access – We're in
5. Escalating Privileges – Own the System
6. **Pilfering – Own the network. Game over.**
7. Covering Tracks – Hide the evidence
8. Leaving Back Doors – Come Back later
9. Denial of Service – Time out.

➤ Pilfering and Information Gathering

- Here, the information gather begins again to identify mechanisms to gain further access and identify trusts
- Could accompany “Escalating Privileges”
- Searching, gathering, and dumping password files
- Collecting configuration files and policies
- Searching the registry
- Using this information to move throughout the rest of the network

Pilfering > Sniffing

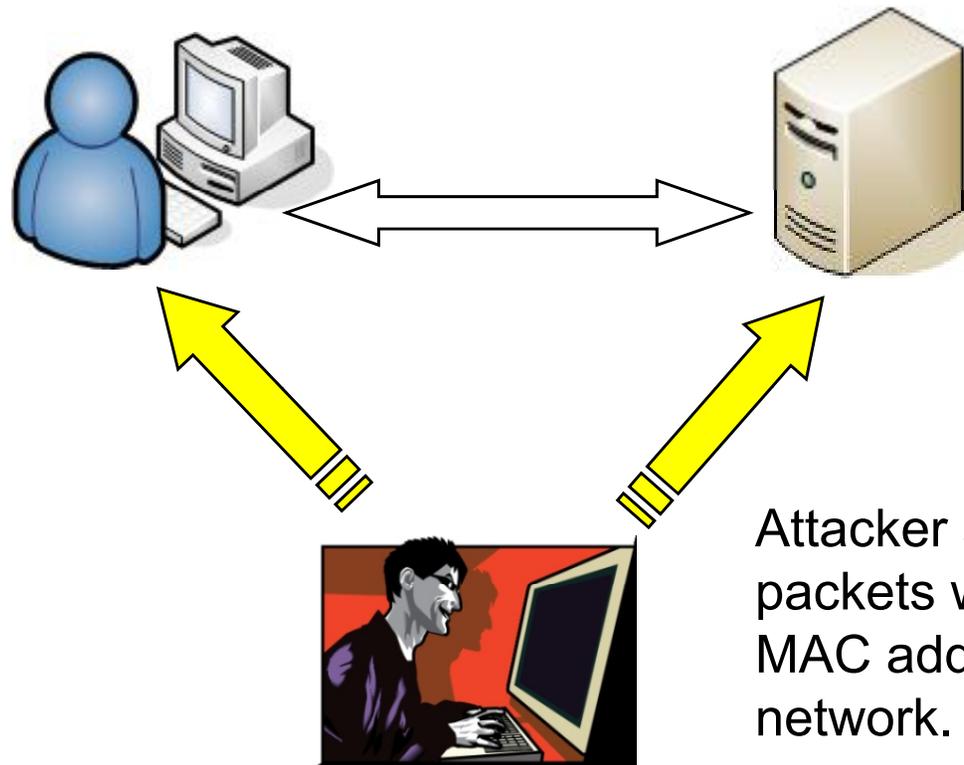
➤ Sniffing

- looking for clear text passwords, LM (LAN Manager) hashes, or anything else that can lend a hand in gaining access to the target or any other system on the network.
- may also be looking for other sensitive information such as confidential emails possibly containing anything of interest, ftp sessions, and more...
- Now that the use of switches is standard, sniffing is not as easy as it used to be.
- Hubs are broadcast devices. Switches forward packets only to the specified destination, making passive switching impossible.
- Attackers must gain access to a mirrored port or find a way around the switching technology.

Pilfering > Man in the Middle (MITM)

➤ Sniffing a Switched Network

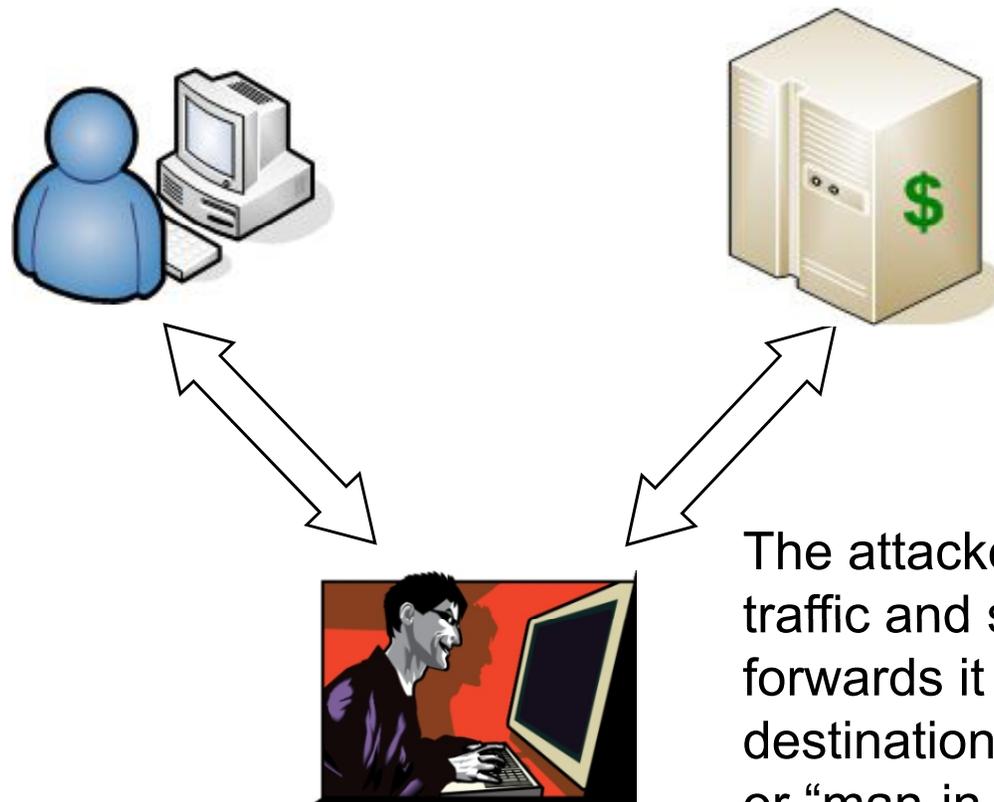
- Sniffing a switched network with ARP (Advanced Routing Protocol) “poisoning”



Pilfering > Man in the Middle (MITM)

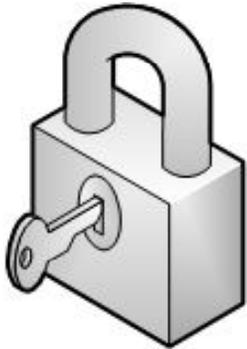
➤ Sniffing a Switched Network

- Sniffing a switched network with ARP “poisoning”



The attacker now receives all traffic and seamlessly forwards it on to the actual destination acting as a bridge or “man-in-the-middle”.

Pilfering > Defeating Encryption



- Are HTTPS and SSH safe?
 - No
 - Dsniff can make use of DNSSpoofer, webmitm, and sshmitm to perform a MITM (just as we saw previously) attack that can hijack HTTPS and SSH sessions
 - Ettercap also has the ability to fake certificates

Pilfering > Defeating Encrypted Sessions

➤ Session Hijacking 2

- Weakness in the the way IP is handled in conjunction with ARP
- Techniques
 - Sequence number calculation
 - Combined with a DoS Attack
 - ARP Poisoning
- Can defeat VPN
- Can defeat PKI (Public Key Infrastructure) Encryption

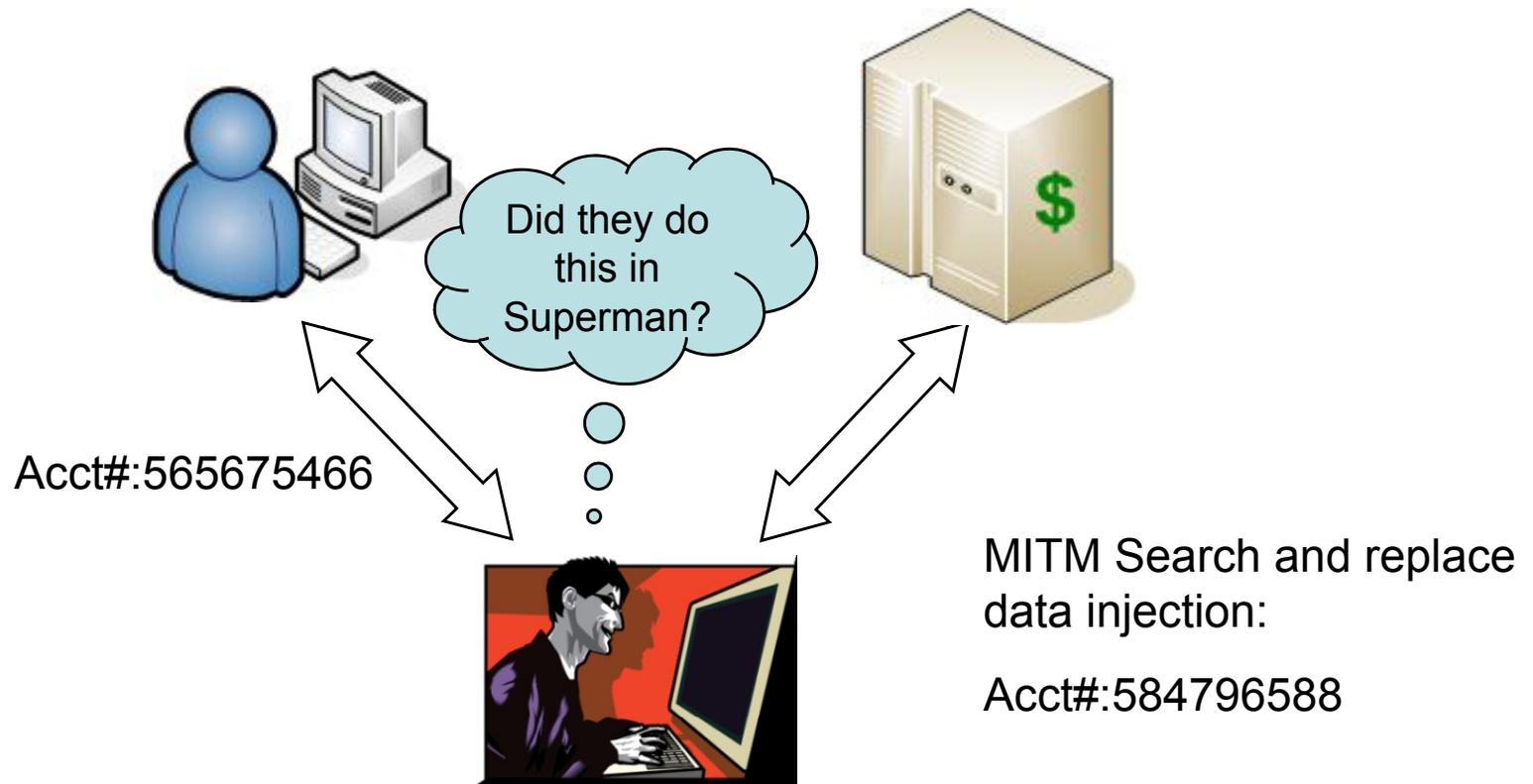
Pilfering > Defeating Encrypted Sessions

➤ Session Hijacking – Bypassing Encryption

- Weakness in PKI (certificate handling)
- Forging certificates and other PKI mechanisms
 - Relies heavily on unsuspecting users
 - Can circumvent SSL (Secure Socket Layer), digital signatures, SSH (Secure Shell), and VPN (Virtual Private Networks)

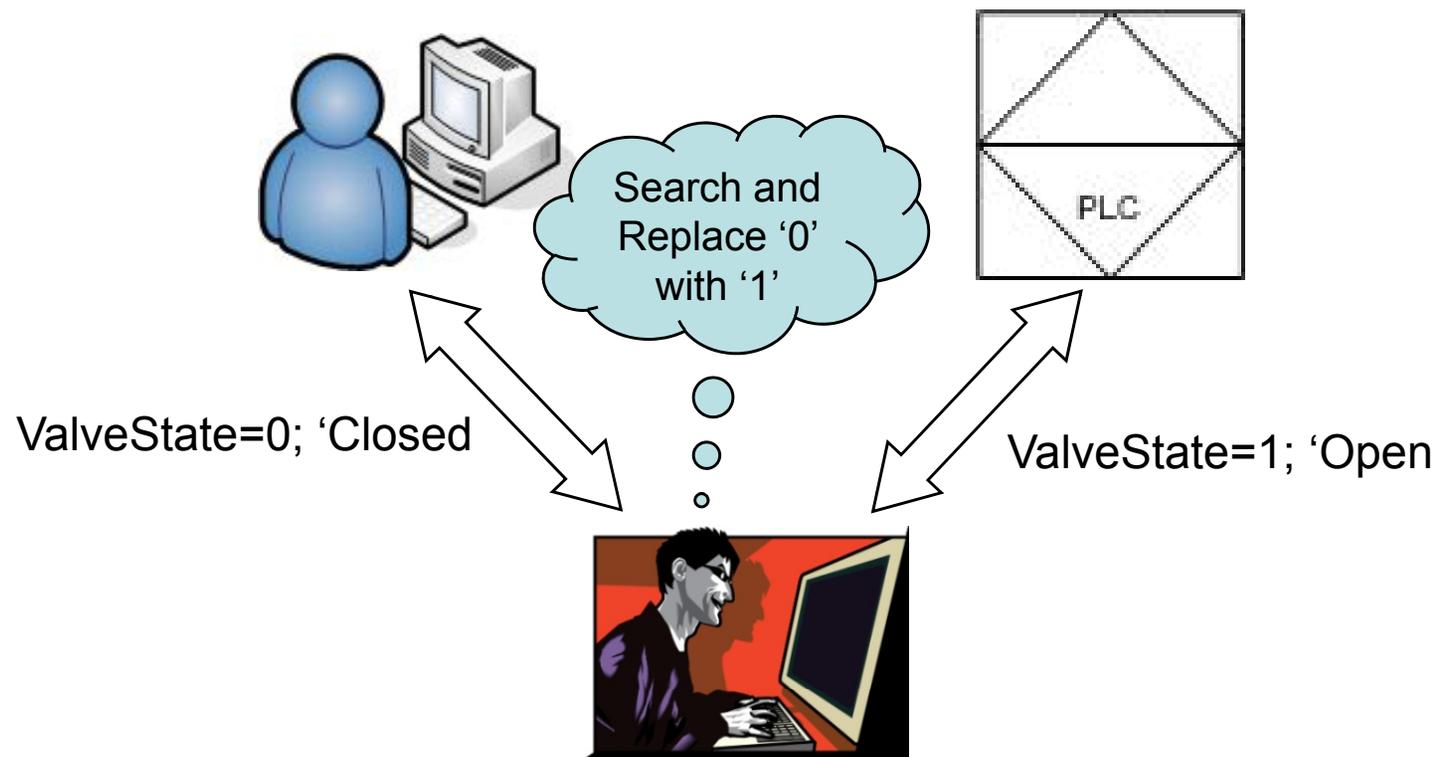
Pilfering > Packet Injection

➤ MITM Data Injection (Financial System)



Pilfering > Packet Injection

➤ MITM Data Injection (Industrial Control System)



Pilfering > Sniffing– Sniffing

➤ Popular Sniffing Tools

- Tcpdump
 - Very powerful
 - Basis for many other tools
- Sniffit
 - Monitor chat sessions in real time
- Dsniff
 - Dnsspoof
 - Webmitm
 - Sshmitm
 - Mailsnarf
 - Webspy
 - Automatically grabs and identifies several protocol passwords



Pilfering Sniffing

- Ettercap
 - Perform MITM attacks
 - Automatically grabs and identifies several protocol passwords
- Ethereal (Wireshark)
 - Tcpdump based
 - GUI
 - Command line functional via tethereal
 - Limited Wi-Fi
- Cain
 - Multi Tool
 - ARP Poisoning
 - Password Dictionary and brute force cracking
 - LM Hash Grabbing

Etheral - Ethernet

No.	Time	Source	Destination	Protocol	Info
48	1.141245	10.10.0.26	205.188.234.67	TCP	1080 > 800
49	1.141661	10.10.0.19	65.208.228.222	HTTP	GET / HTTP
50	1.149615	205.188.234.67	10.10.0.26	socks	unknown
51	1.157536	205.188.234.67	10.10.0.26	socks	unknown
52	1.157584	10.10.0.26	205.188.234.67	TCP	1080 > 800
53	1.2713819	65.208.228.222	10.10.0.19	TCP	80 > 4395

Frame 49 (345 on wire, 345 captured)

- Ethernet II
- Internet Protocol, Src Addr: 10.10.0.19 (10.10.0.19), Dst Addr: 65.208.228.222
- Transmission Control Protocol, Src Port: 4395 (4395), Dst Port: 80 (80), Seq: 1080, Win: 0, Len: 0
- Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Accept: */*\r\n
 - Accept-Language: en-us\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - If-Modified-Since: Tue, 18 Dec 2001 07:09:10 GMT\r\n
 - If-None-Match: "1bf32-2262-3c1eeb96"\r\n
 - User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; windows NT; DigExt)\r\n
 - Host: www.ethereal.com\r\n
 - Connection: Keep-Alive\r\n

Filter: [] [Reset]

➤ Password Cracking

- Means of circumventing passwords
 - Hashes
 - Dictionary Attacks
 - Brute Force Attacks (as in “Gaining Access”)
 - Windows LM Hash
 - Unix/Linux “passwd” and shadow file
- Tools
 - L0pth Crack
 - Cain
 - John the Ripper
 - Rainbow Tables
 - Many More

Password Cracking > Rainbow Tables

- Uses a history of hundreds of thousands of already decrypted hashes. Sometimes terabytes worth.
- Exponentially speeds up cracking hashes
- What used to take weeks now takes minutes.
- 8 characters is no longer safe
- Rainbow tables make quick work of anything less than 14 characters.
- Tools
 - Rainbowcrack
 - Rcrack

Pilfering

➤ System Admin Profiling

- A system's admin is likely to make the same mistakes throughout a system.
- Learning a system admin's habits can give clues to other vulnerabilities throughout the network.
- Requires some skills or talents in psychological profiling

➤ Cross-correlation

- Many system admins use common passwords and configurations (themes) throughout the network.
- Documents found on one computer can give access information to others
- Network configurations can give a picture of the entire network.

Anatomy of an Attack



1. Recon – Casing the joint
2. Scanning – Target and entry point acquisition
3. Enumeration – Gather inside Intel
4. Gaining Access – We're in
5. Escalating Privileges – Own the System
6. Pilfering – Own the network. Game over.
7. **Covering Tracks – Hide the evidence**
8. Leaving Back Doors – Come Back later
9. Denial of Service – Time out.

Covering Tracks

➤ Covering Tracks

- Once total ownership is obtained, hiding the evidence from system's administrators is crucial.
- Clearing logs
- Hiding tools

“... But I only saw one set of footprints...”

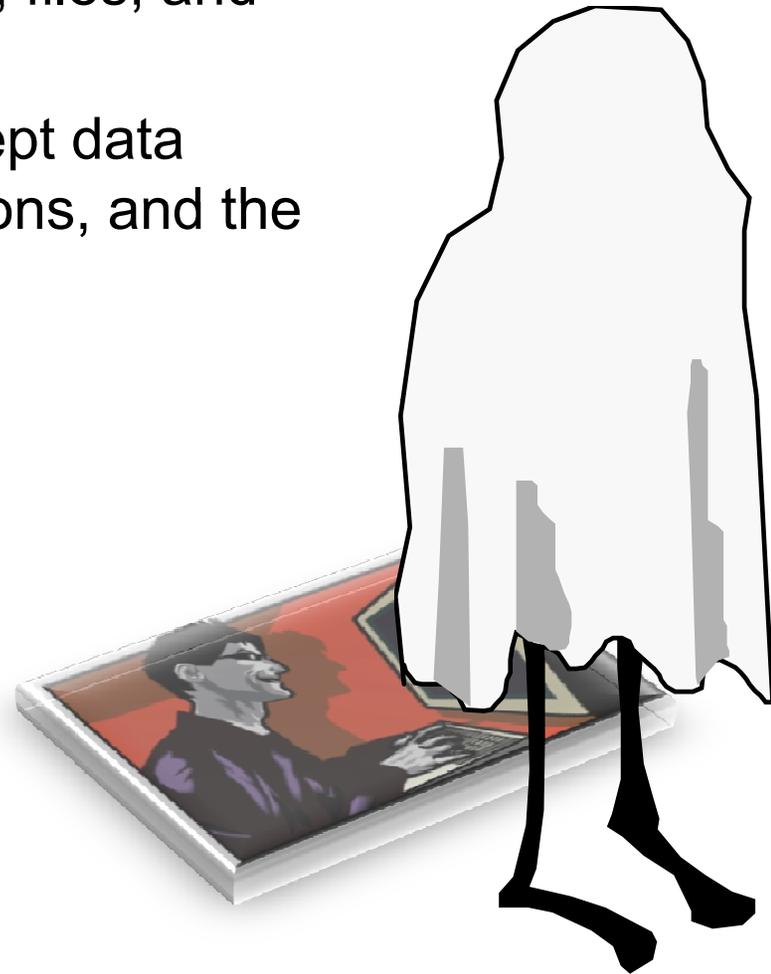
This is because I covered my tracks...”



Covering Tracks > Rootkits

➤ Rootkits

- Typically hides logins, processes, files, and logs
- Often includes software to intercept data from terminals, network connections, and the keyboard
- Types of rootkits
 - Kernel
 - Application
- Tools:
 - FU Rootkit
 - SuckIT
 - T0rn
 - Ambient's Rootkit (ARK)
 - Hacker Defender



➤ Alternate Data Streams

- Relatively unknown compatibility feature of NTFS
- Used for .ico files
- Provides hackers with a method of hiding root kits or hacker tools on a breached system
- Allows them to be executed without being detected by the systems administrator
- *Virtually* impossible to detect
- File sizes do not change
- Do not show up in process lists

```
type c:\anyfile.exe > c:\winnt\system32\calc.exe:anyfile.zip
```

Covering Tracks > Covert Channels

➤ “Covert Channels” and Protocol Tunneling

- Sending data through other protocols
- Using a proxy server
 - Example: Anonymizer
- Tools
 - Netcat
 - Loki
 - HTTP-Tunnel - http://www.http-tunnel.com/html/solutions/http_tunnel/client.asp
 - Ping Tunnel - <http://www.cs.uit.no/~daniels/PingTunnel/>
 - Several scripts



Covering Tracks > IDS Evasion

IDS Evasion

- IDS is still a young technology (Relatively speaking)
- IDS easily misconfigured
- Usually not maintained
- Techniques
 - DoS
 - Camouflage
 - Timed attacks
 - Slow down before IDS threshold (clipping)
 - Protocol tunneling
 - Source porting

Anatomy of an Attack



1. Recon – Casing the joint
2. Scanning – Target and entry point acquisition
3. Enumeration – Gather inside Intel
4. Gaining Access – We're in
5. Escalating Privileges – Own the System
6. Pilfering – Own the network. Game over.
7. Covering Tracks – Hide the evidence
8. **Leaving Back Doors – Come Back later**
9. Denial of Service – Time out.

Leaving Backdoors

➤ Leaving Backdoors

- Make sure return access is available
- Usually part of a root kit, or a feature that the root kit can conceal
- Methods
 - Create rogue user accounts
 - Schedule batch jobs
 - Infect startup files
 - Replace apps with trojans
- Tools
 - Netcat, keyloggers, VNC, etc
 - Back orifice, netbus, etc.



Anatomy of an Attack



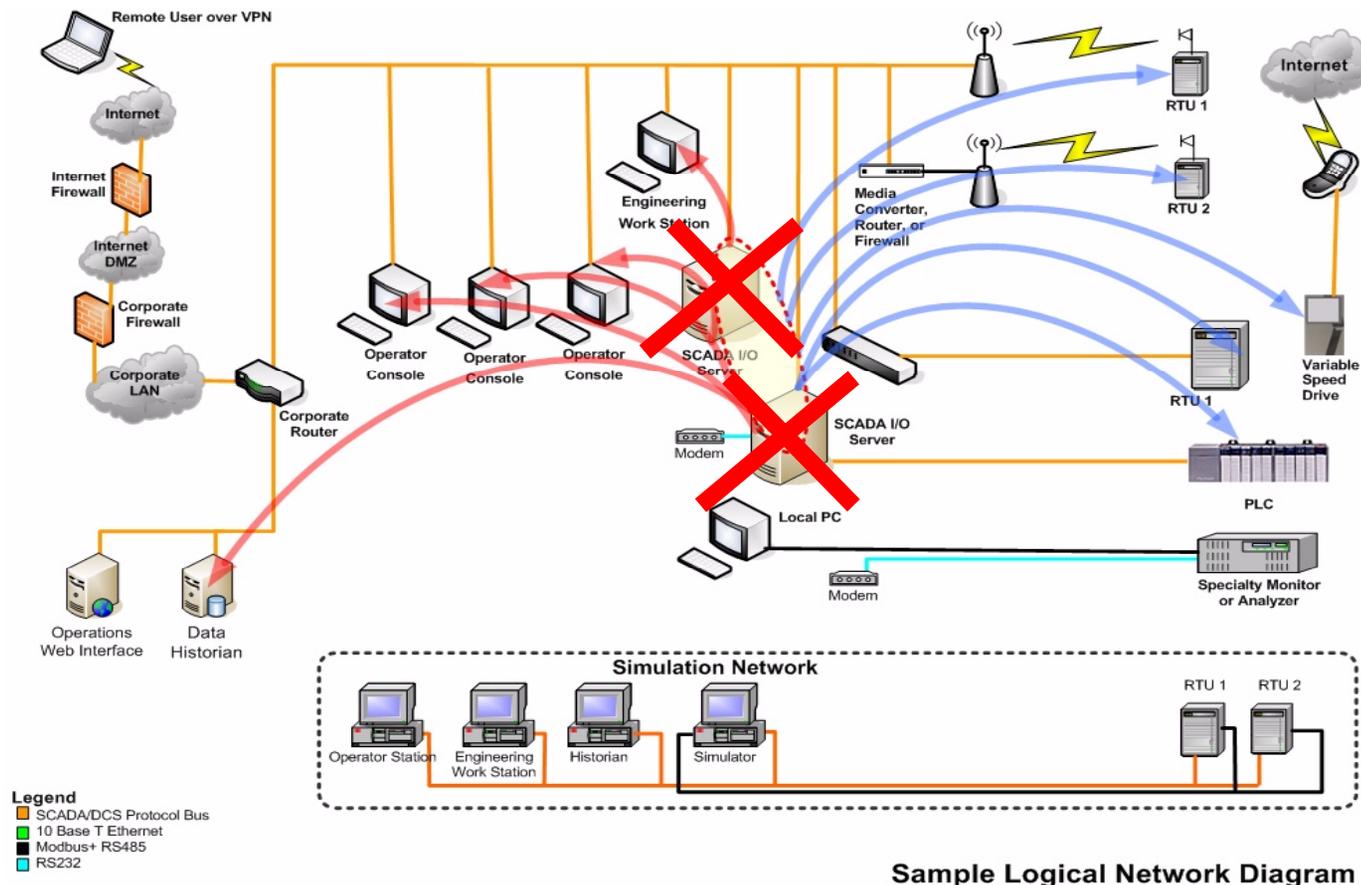
1. Recon – Casing the joint
2. Scanning – Target and entry point acquisition
3. Enumeration – Gather inside Intel
4. Gaining Access – We're in
5. Escalating Privileges – Own the System
6. Pilfering – Own the network. Game over.
7. Covering Tracks – Hide the evidence
8. Leaving Back Doors – Come Back later
9. **Denial of Service – Time out.**

Denial of Service (DoS)

➤ Denial of Service

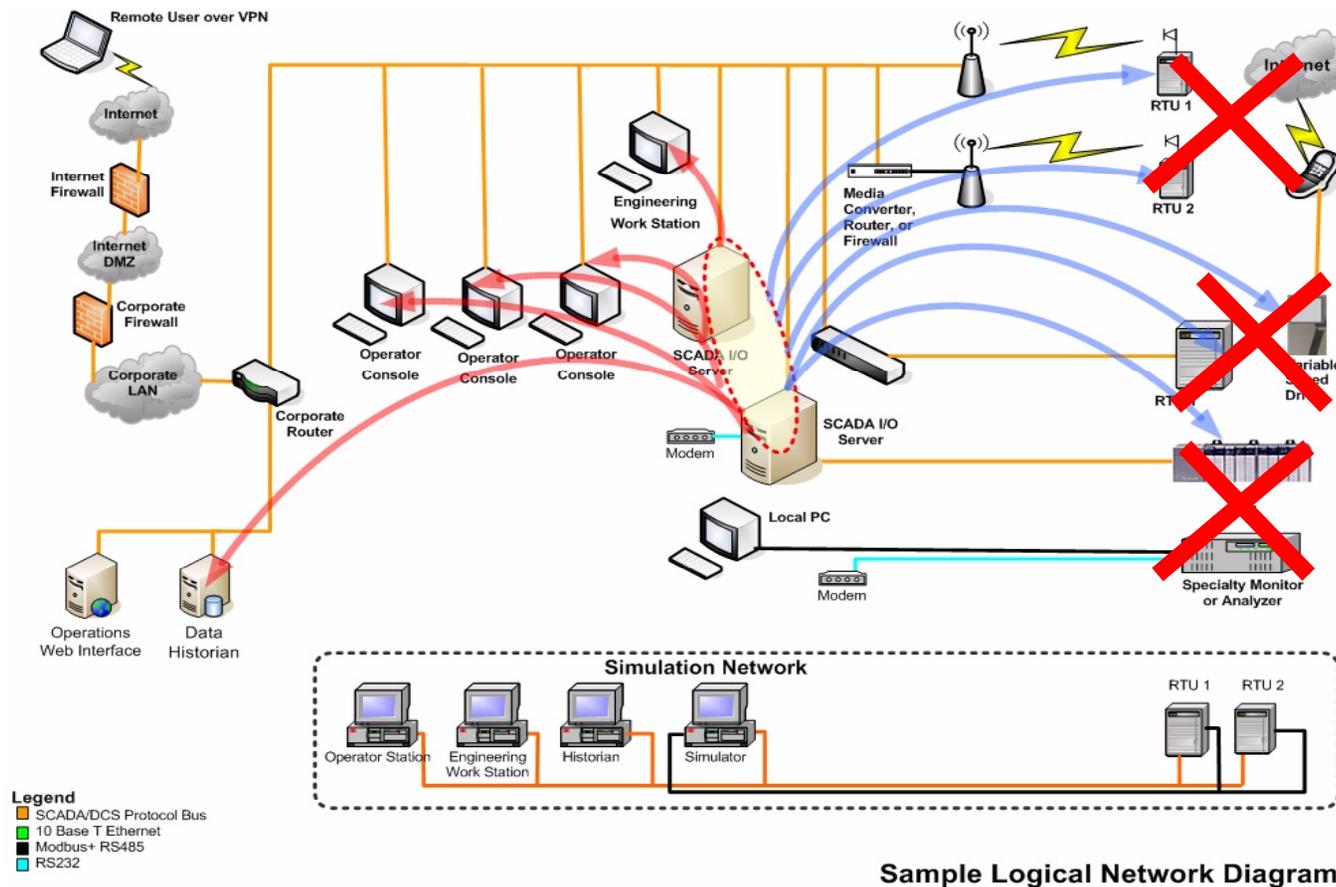
- EASIEST of all attacks yet most devastating to process control environments!
- Attacker is unsuccessful in gaining access and may disable the target as a last resort
- May be part of a larger mission objective
 - Cyber-terrorism
 - Industrial “espionage”
 - Disable critical communication, transaction, monitoring, financial, or other critical system.
- SYN flood, ICMP techniques, identical src/dst SYN requests, overlapping fragment/offset bugs, out of bounds TCP options (OOB), DDoS (Distributed Denial of Service), etc.
- Ping of Death, Smurf, Land, Teardrop, Bonk, Newtear, and MANY MORE...

SCADA Tag Database Servers are Most Critical



- If SCADA Tag Database Servers are not functioning, communications stop with the system, but the system continues operating at last known setpoint or condition
- Key critical servers must always be operational

Taking out control devices STOPS the process

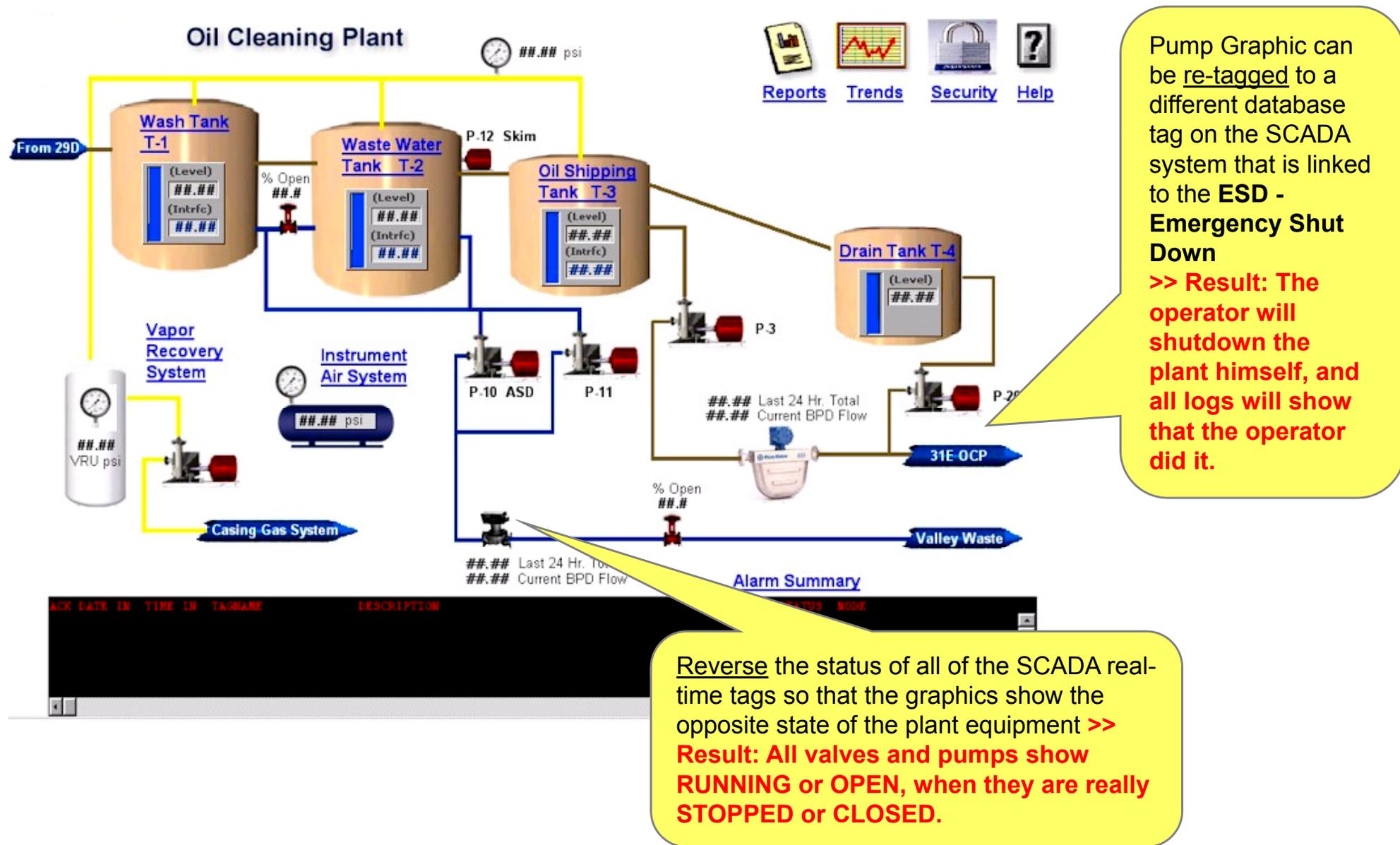


- If the control devices fail, then whatever process condition they were programmed to control is no longer under control, and can swing out of safe operating conditions immediately

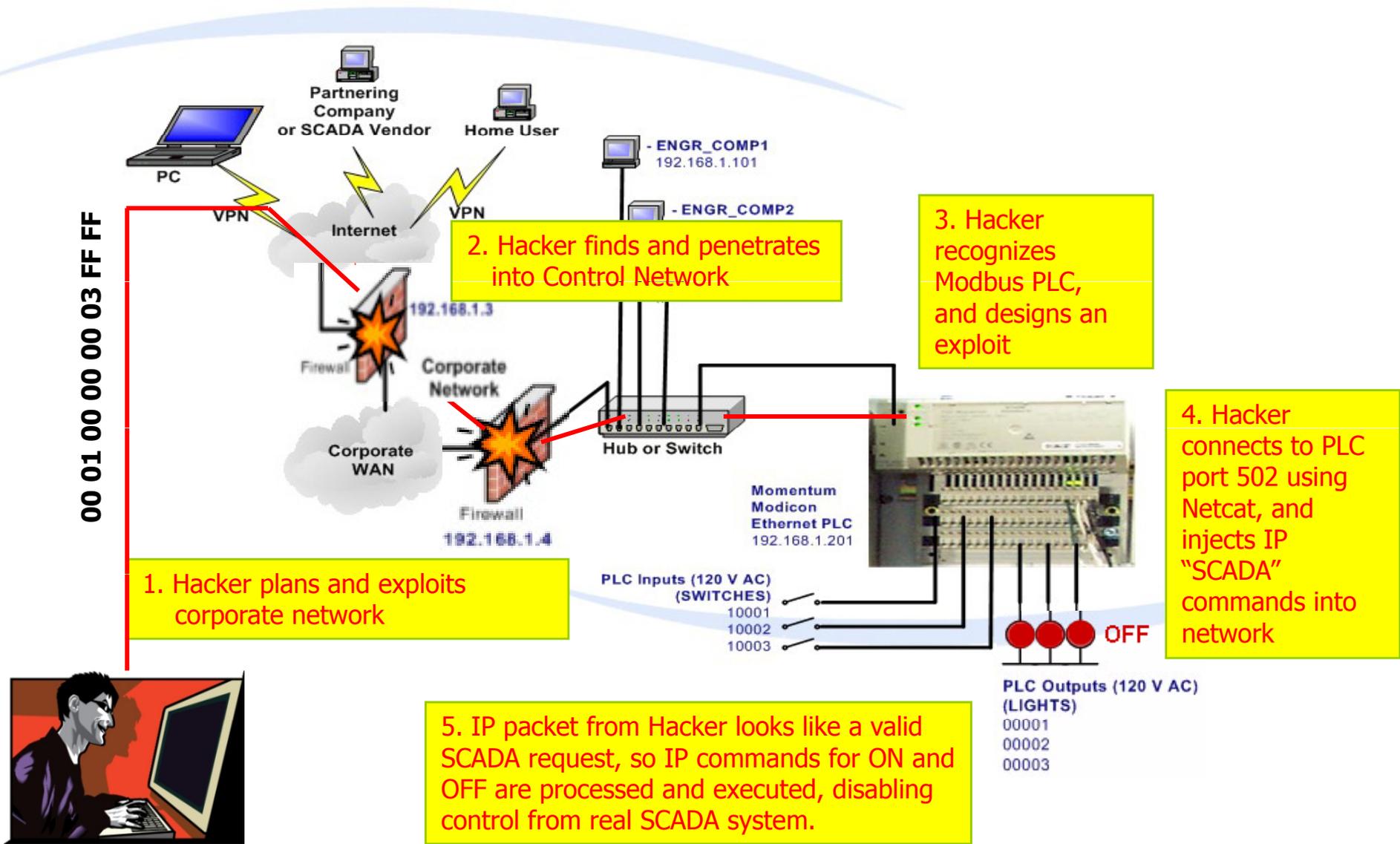
What can cause a control device to fail?

- PLCs, RTUs, and DCS controllers are used to slow, metered communications
 - SCADA Vendors just encapsulated older protocols in TCP/IP but did not make the TCP/IP versions hardened
 - Any communications sent to these control devices that is “out of the norm” can have adverse affects on the controller
 - PLCs and RTUs typically have very POOR TCP/IP stack handling capability, and the CPU that is solving the logic for controlling the facility will be consumed with stack priority, and eventually fail the processor within a matter of seconds
- Malformed packets sent to process control NIC (Network Interface Cards) - *Example Chevron Visio Scanning*
- Network congestion or PINGFLOOD sent to PLC network or COMM module
- Example: printer ran out of ink, spammed a control network with SNMP data to replace the cartridge, and these packets took down over 12 PLCs in a large plant

Cause confusion, make operators make bad actions



Example: PLC Access and Force Setpoint Changes



Conclusion

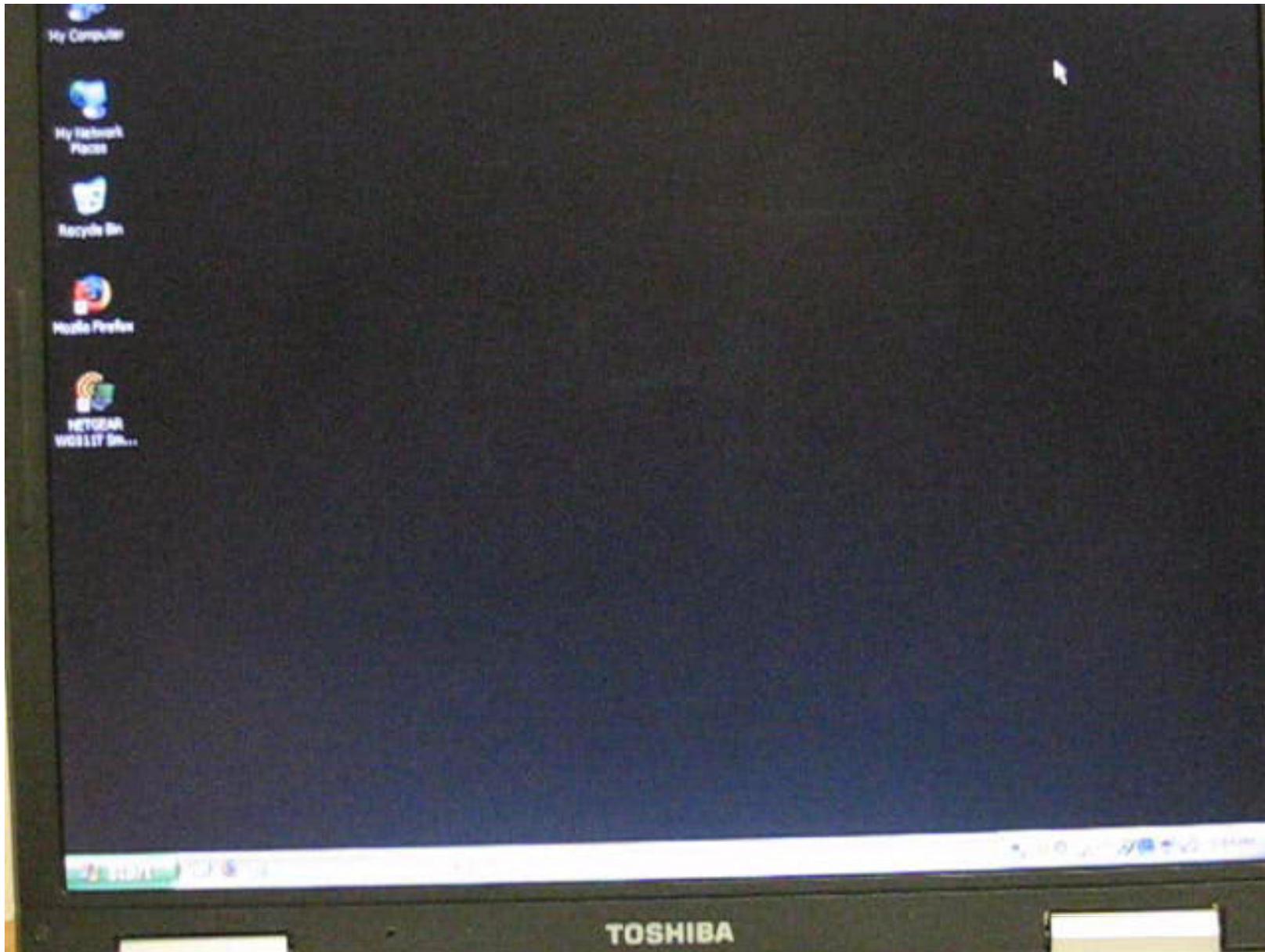
Questions?
Demo Videos



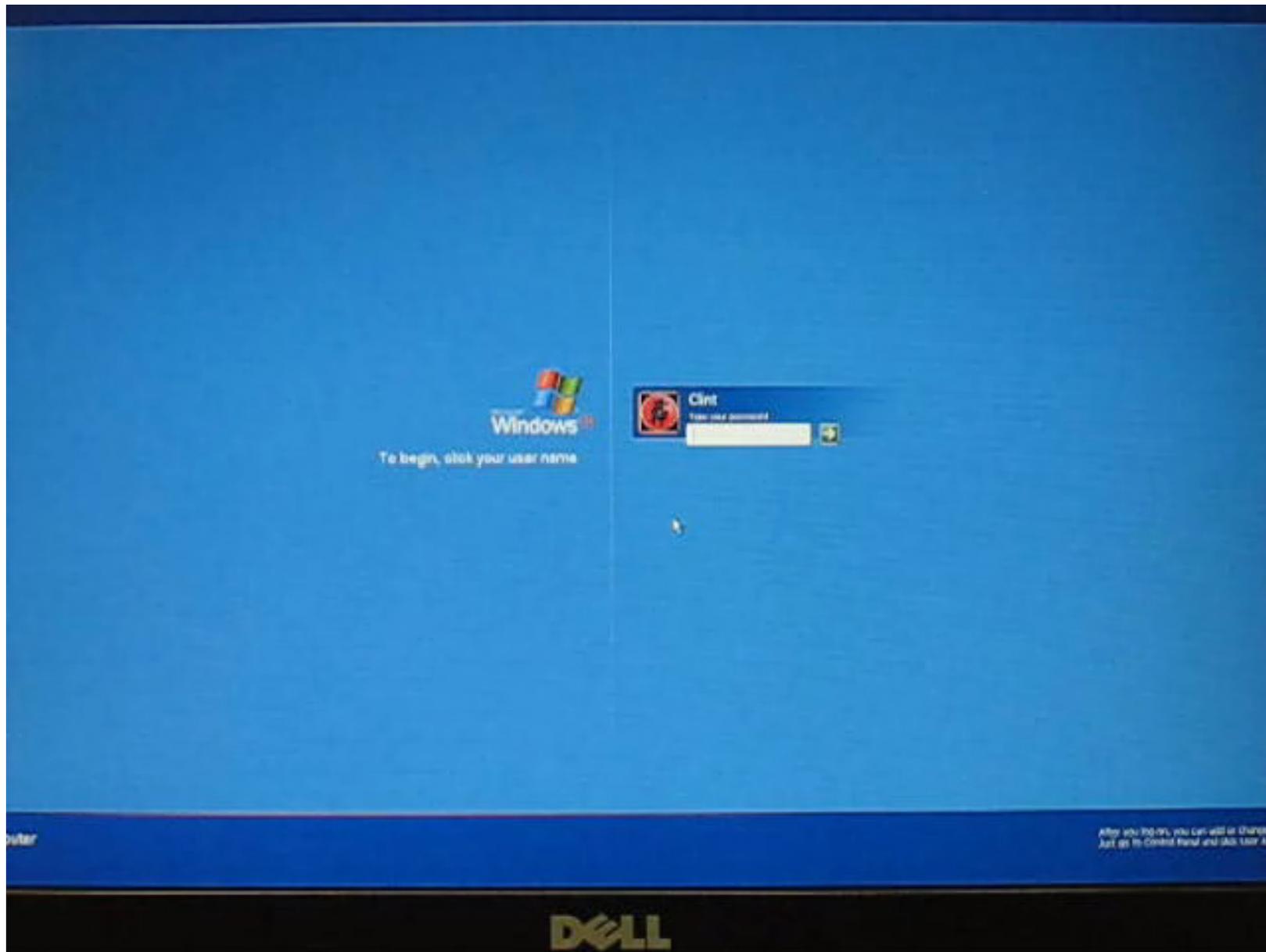
Quick Exploit with Metasploit



Man In The Middle



Bypassing Windows Logon



Social Engineering – “Hackers”



Social Engineering – “Sneakers”



SQL Injection



SQL Injection 2



Web Application Security Application Firewall Demonstration

www.webscurity.com

© 2006 webScurity, inc. – All Rights Reserved

Cracking WEP in Under 10 Minutes

