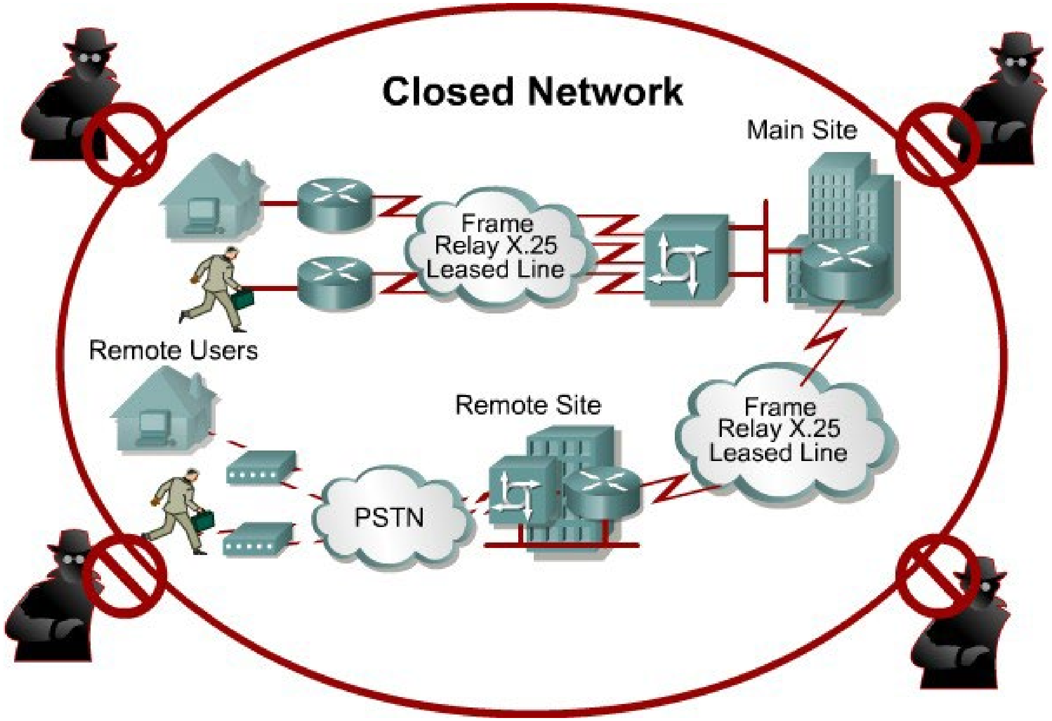
# CIS-4080
# Network Security

## Network Security Threats

# Purpose of Security

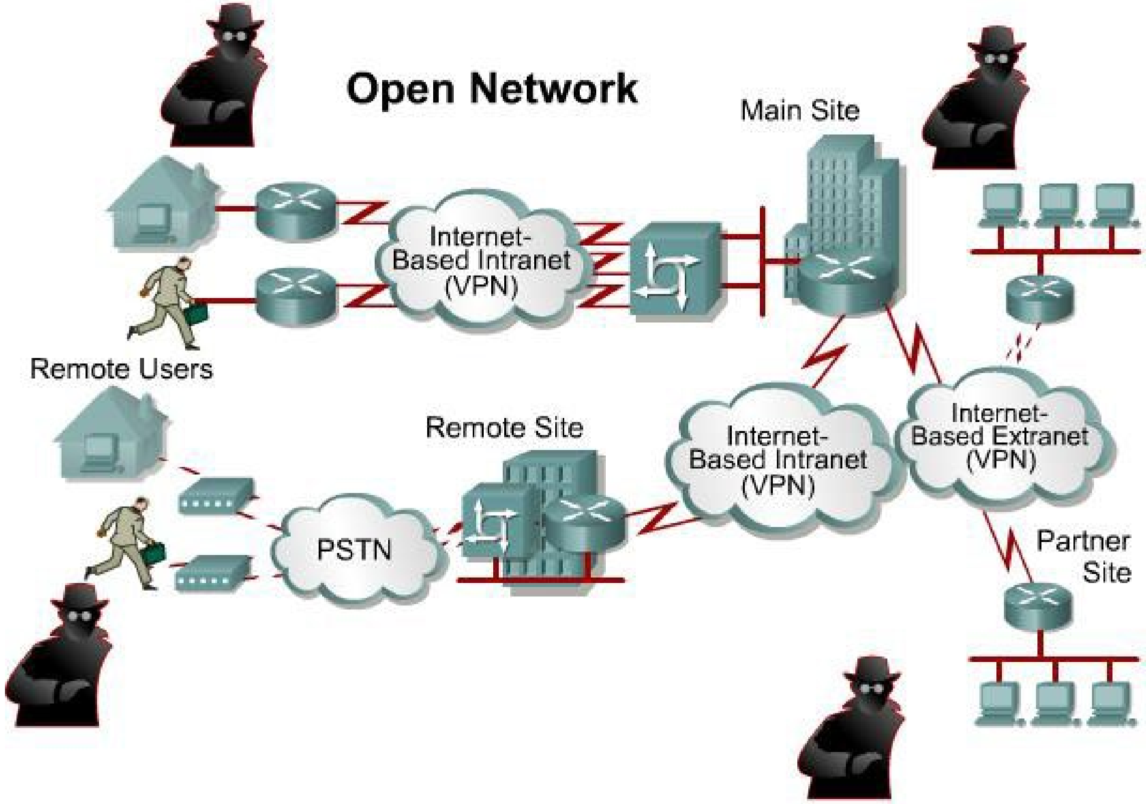
- **To protect assets!**

- Historically done through physical security and closed networks.



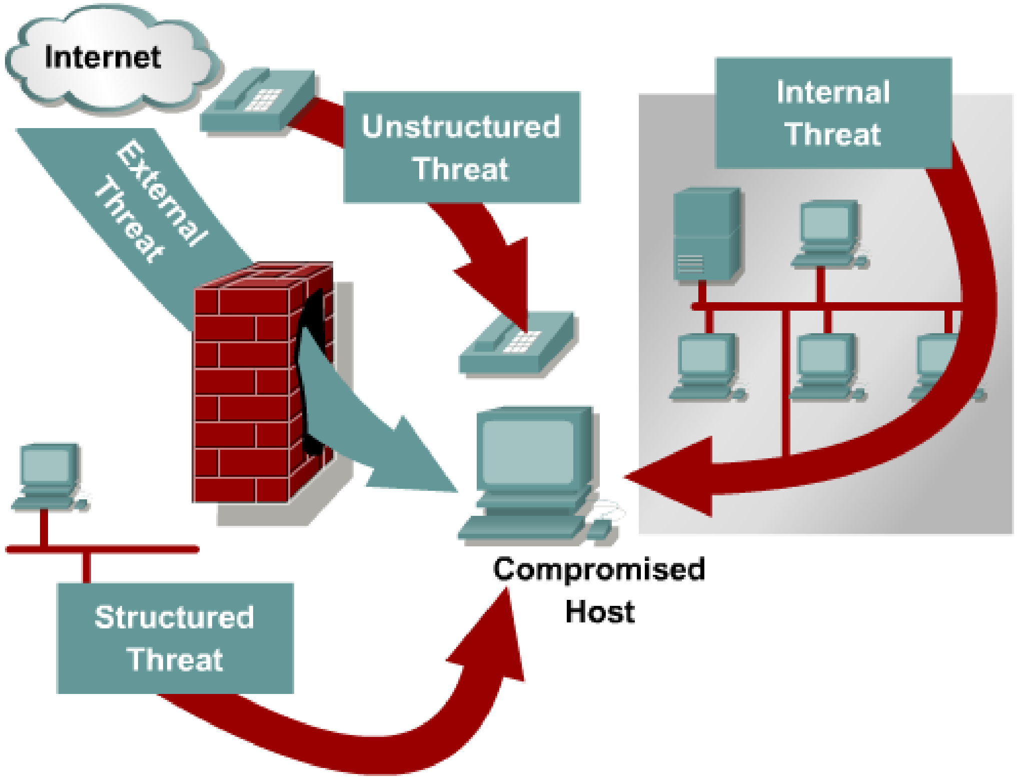
# The Network Today

- With the advent of personal computers, LANs, and the wide-open world of the Internet, the networks of today are more open.

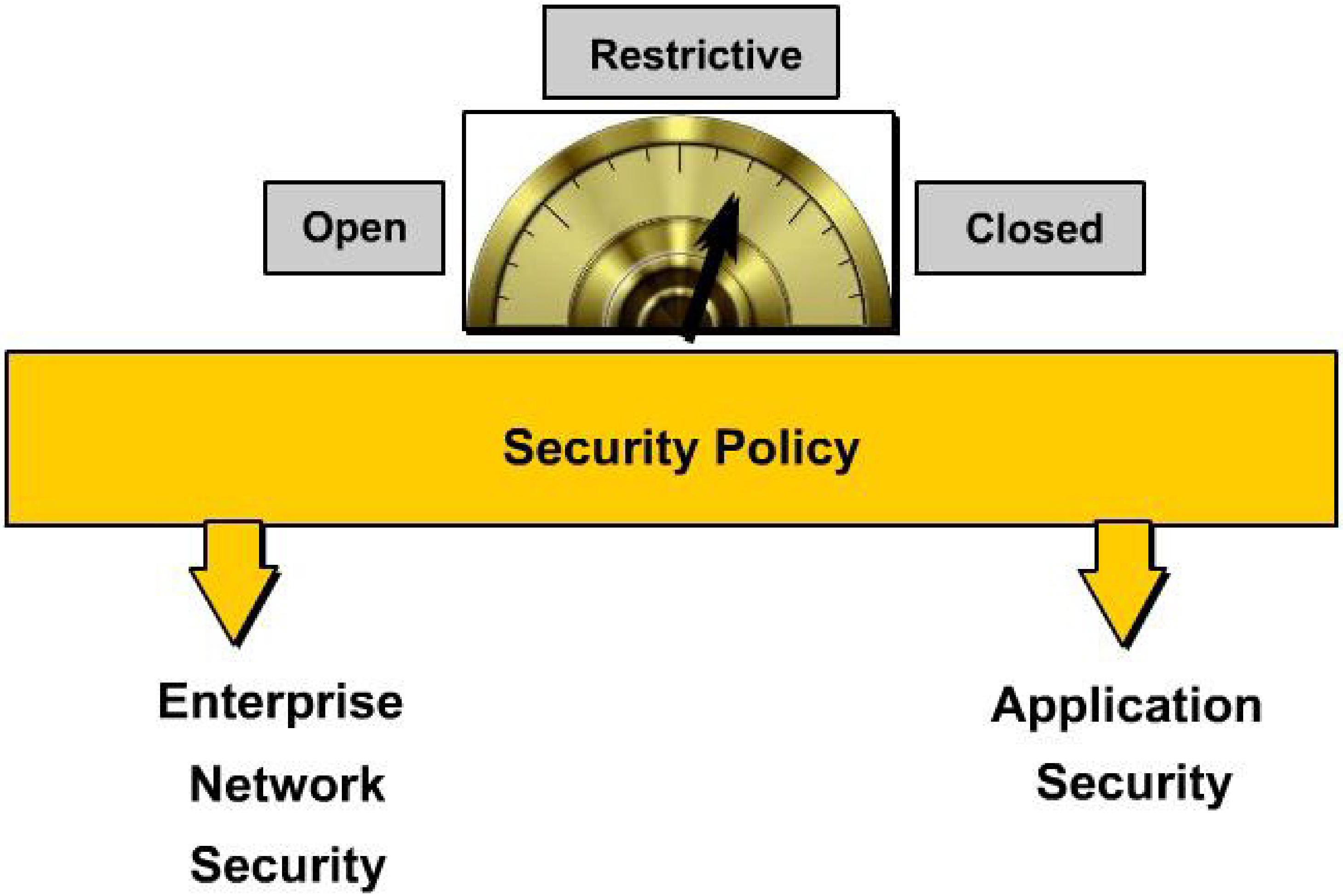

Open Network
Main Site
Internet-Based Intranet (VPN)
Remote Users
Remote Site
Internet-Based Intranet (VPN)
Internet-Based Extranet (VPN)
PSTN
Partner Site

# Threats

- There are four primary classes of threats to network security:
  - Unstructured threats (non-specific, unorganized)
  - Structured threats (specific)
  - External threats (outside org.)
  - Internal threats (inside org.)

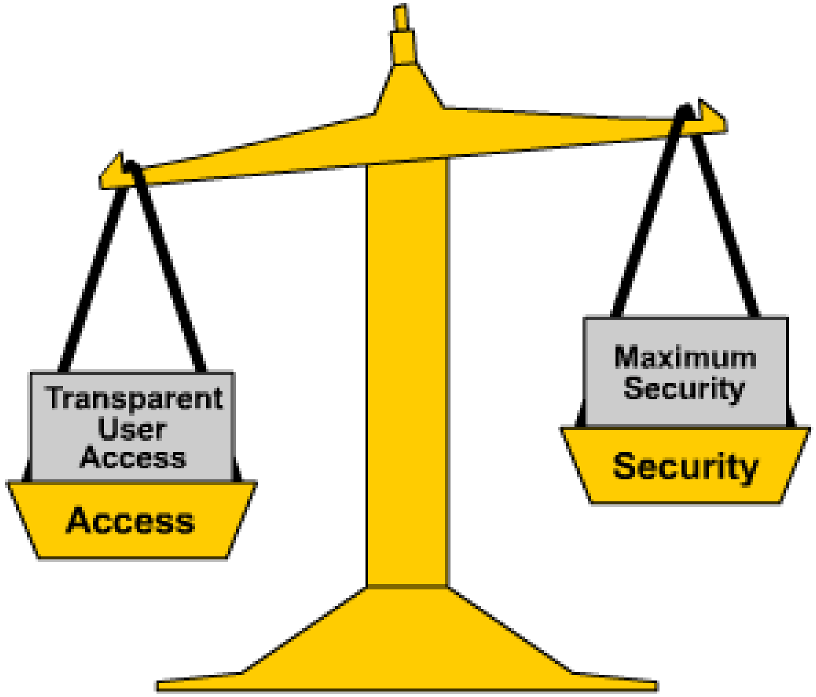


# Network Security Models



# Open Security Model

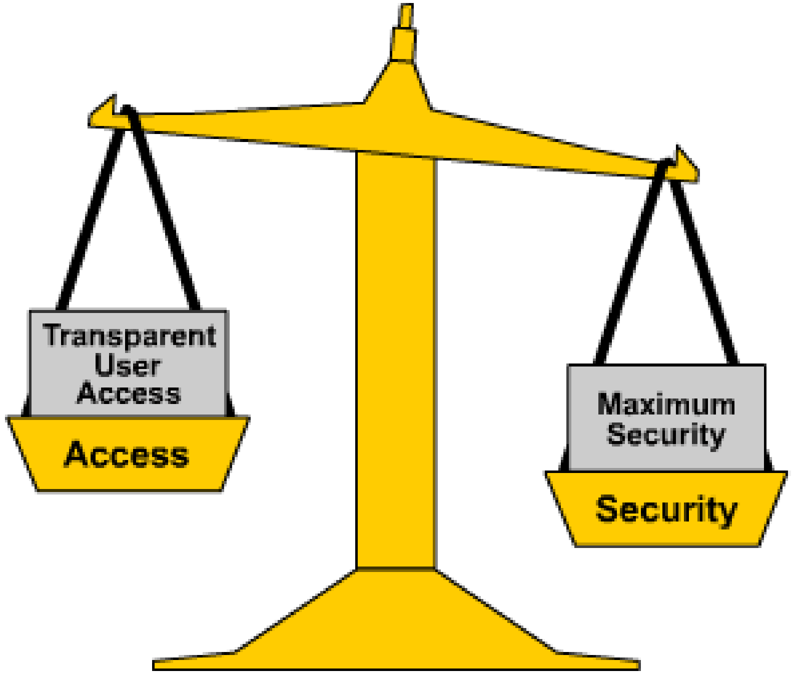
**Permit everything that is not explictly denied**



- Easy to configure and administer
- Easy for network users
- Security Costs: Least expensive

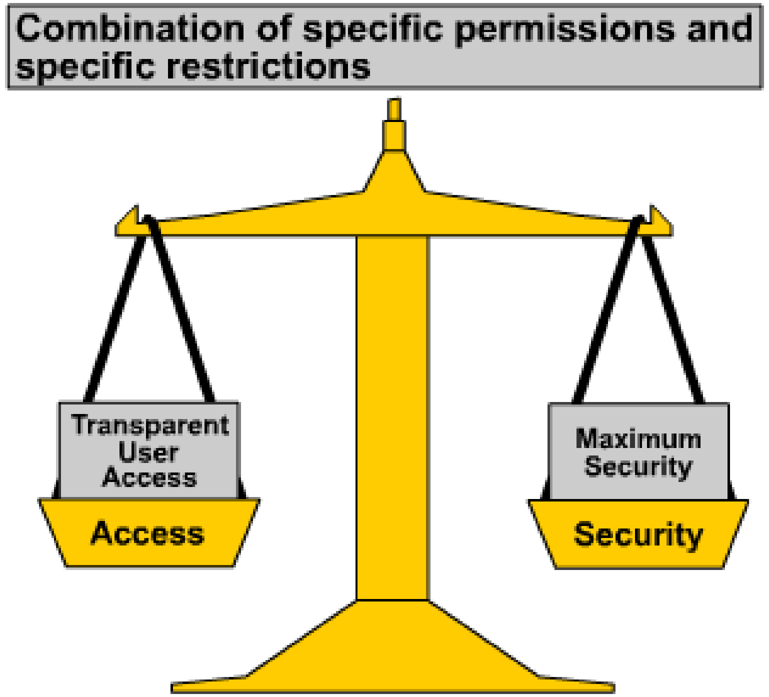
# Closed Security Model

That which is not explicitly permitted is denied



- Most difficult to configure and  administer
- Most difficult network users
- Security Cost: Most expensive

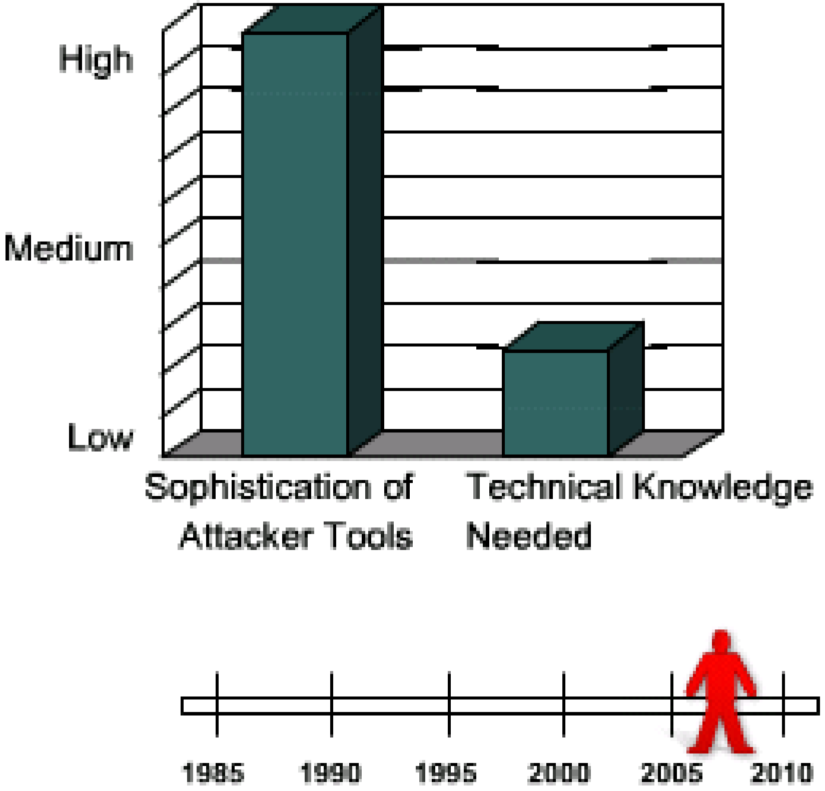
# Restrictive Security Model


Combination of specific permissions and specific restrictions
Transparent User Access
Access
Maximum Security
Security

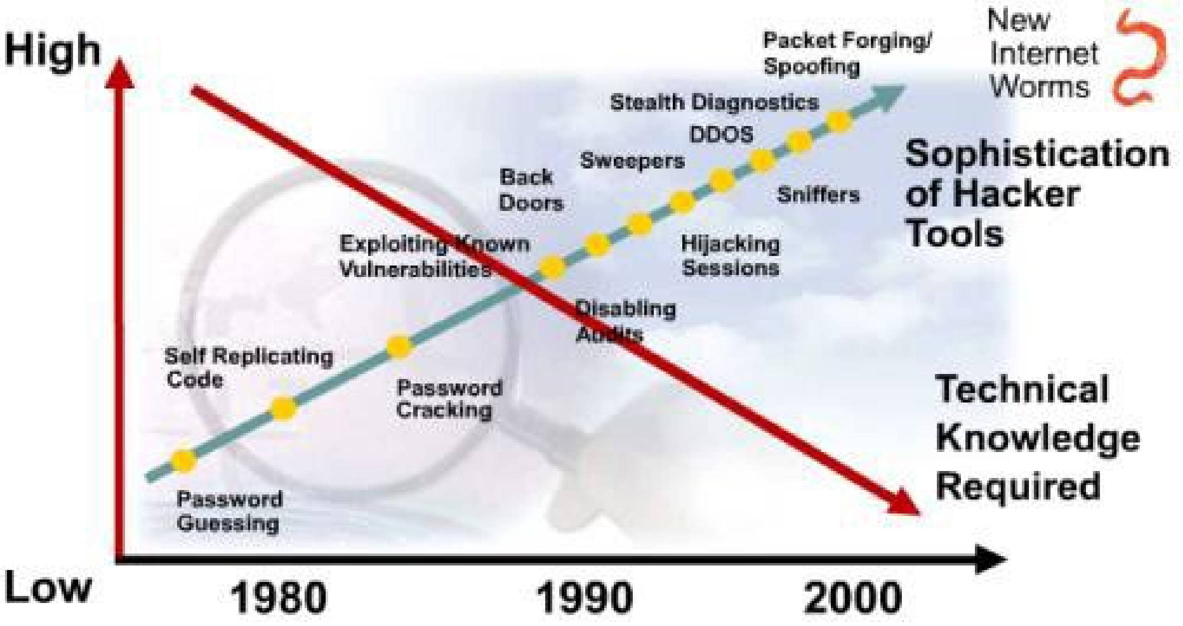
- More difficult to configure and  administer
- More difficult network users
- Security Cost: More expensive

# Evolution of Network Security

# Sophistication of Tools vs. Technical Knowledge



Drag the attacker along the timeline.



Threats continue to become more sophisticated as the technical knowledge required to implement attacks deminishes.

# Morris Worm

- The Morris worm or Internet worm was the first computer worm distributed via the Internet
- It was written by a student at Cornell University, Robert Tappan Morris, and launched on November 2, 1988 from MIT
- It is considered the first worm and was certainly the first to gain significant mainstream media attention
- It also resulted in the first conviction in the US under the 1986 Computer Fraud and Abuse Act.

# Morris Worm

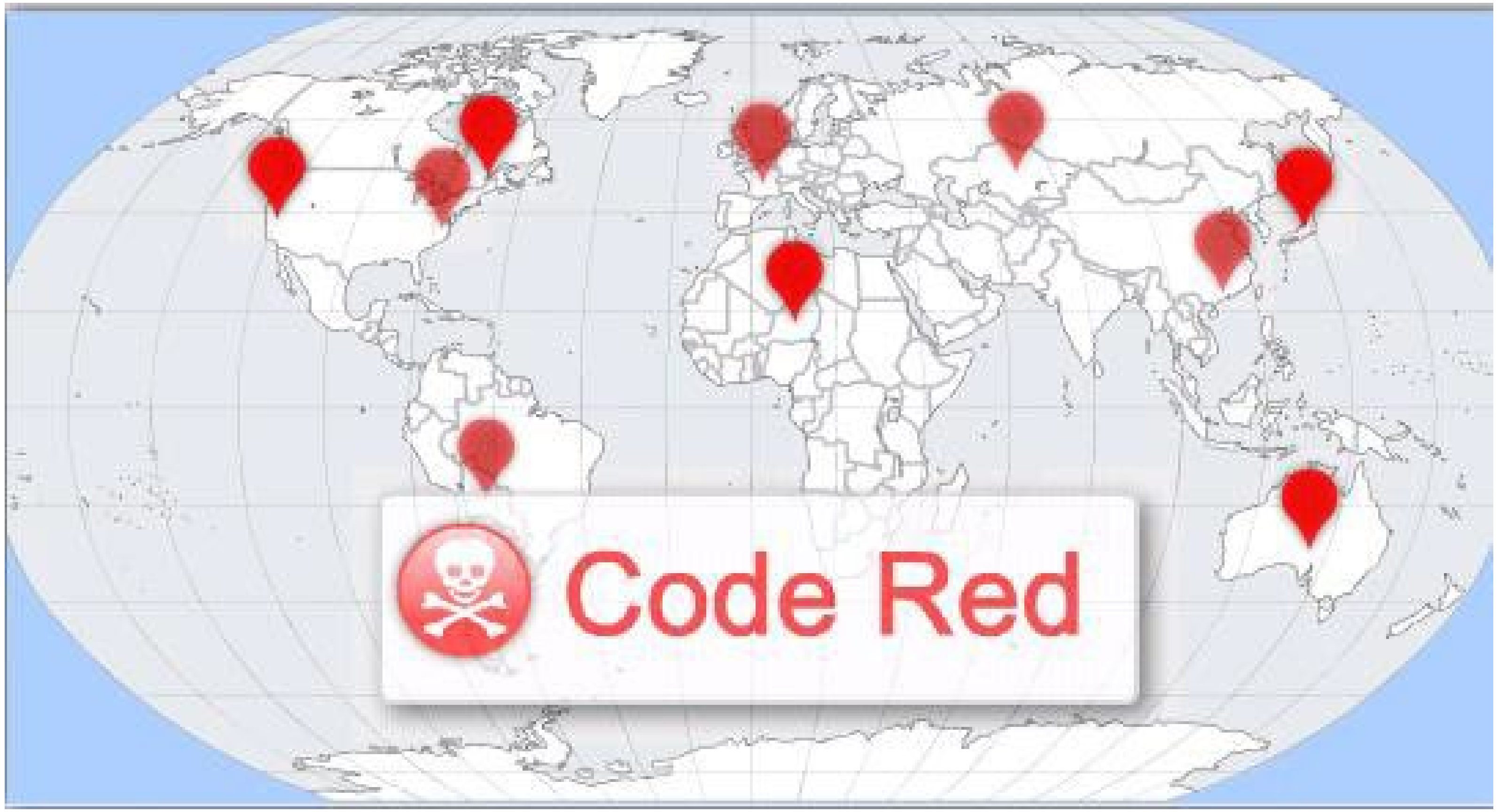
- According to Morris, the worm was not written to cause damage, but to gauge the size of the Internet.
- … but the worm was released from MIT, not Cornell where Morris was a student
- The Morris worm worked by exploiting known vulnerabilities in Unix sendmail, Finger, rsh/rexec and weak passwords.
- It is usually reported that around 6,000 major Unix machines were infected by the Morris worm
- The cost of the damage was estimated at $10M–100M.

# Good Thing?

- The Morris worm prompted DARPA to fund the establishment of the CERT/CC at Carnegie Mellon University to give experts a central point for coordinating responses to network emergencies.
- Robert Morris was tried and convicted of violating the 1986 Computer Fraud and Abuse Act.
- After appeals he was sentenced to three years probation, 400 hours of community service, and a fine of $10,000.

# What is “Code Red”?

- The Code Red worm was a DoS attack and was released on July 19, 2001 and attacked web servers globally, infecting over 350,000 hosts and in turn affected millions of users.



# What is “Code Red”?

Code Red:

- Defaced web pages.
- Disrupted access to the infected servers and local networks hosting the servers, making them very slow or unusable.
- Network professionals responded slowly to system patches which only exacerbated the problem.

# What Did It Do?

- The "Code Red" worm attempted to connect to TCP port 80 on a randomly chosen host assuming that a web server will be found.

- Upon a successful connection to port 80, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow in the Indexing Service.

- The same exploit (HTTP GET request) is sent to other randomly chosen hosts due to the self-propagating nature of the worm.

- However, depending on the configuration of the host which receives this request, there are varied consequences.

# What Did It Do?

- If the exploit was successful, the worm began executing on the victim host.

- In the earlier variant of the worm, victim hosts experienced the following defacement on all pages requested from the server:

**HELLO! Welcome to http://www.worm.com! Hacked By Chinese!**

# What Did It Do?

- Actual worm activity on a compromised machine was time sensitive and different activity occurred based on the date of the system clock:
- Day 1 - 19: The infected host will attempt to connect to TCP port 80 of randomly chosen IP addresses in order to further propagate the worm.
- Day 20 - 27: A packet-flooding denial of service attack will be launched against a particular fixed IP address.
- Day 28 - end of the month: The worm "sleeps"; no active connections or denial of service.

# How is it stopped?

- Although the worm resides entirely in memory, a reboot of the machine will purge it from the system.

- However, patching the system for the underlying vulnerability remains imperative since the likelihood of re- infection is quite high due to the rapid propagation of the worm.

- Network security professionals must develop and implement a security policy which includes a process to continually keep tabs on security advisories and patches.

# Code Red – A good thing?

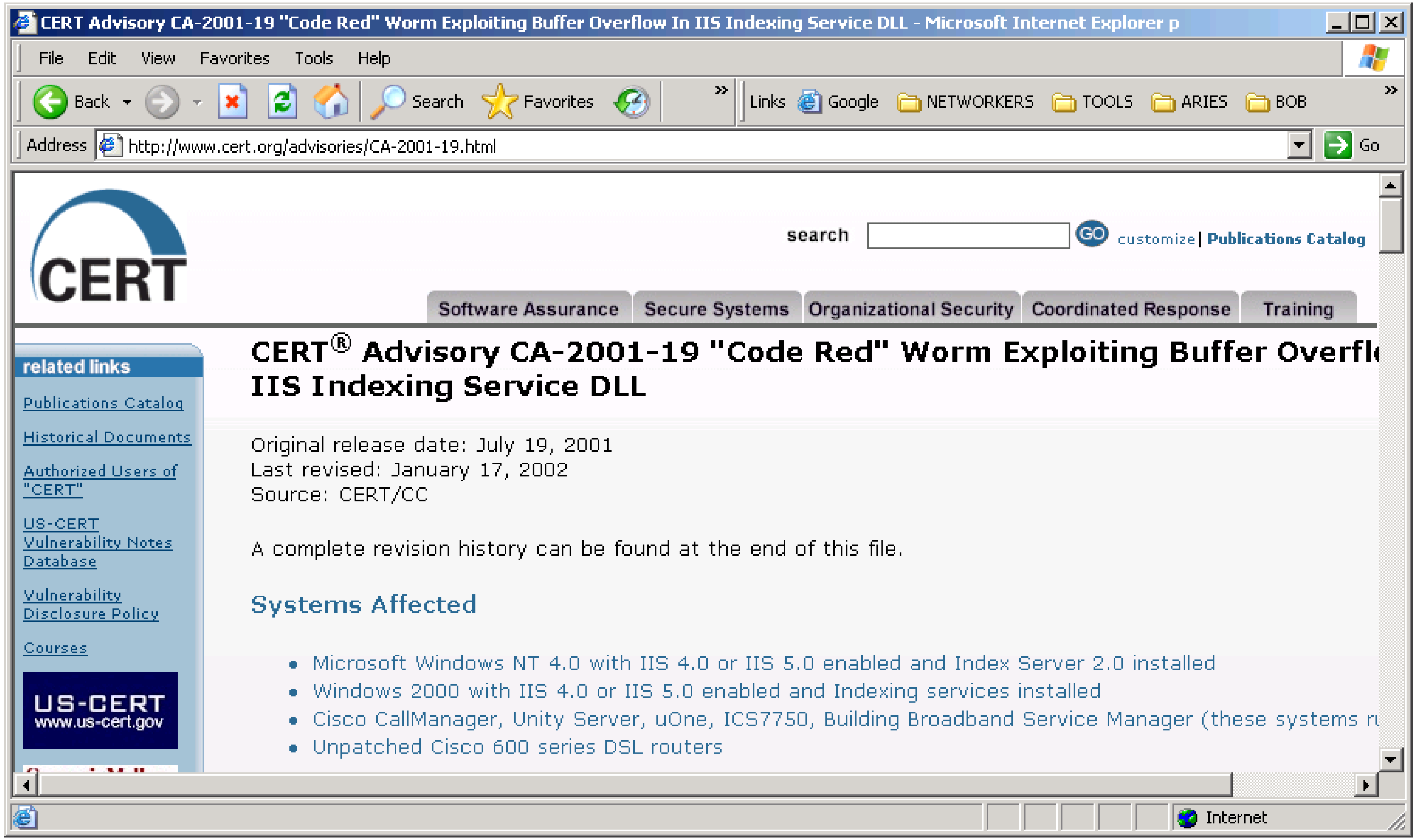
- It was a wake up call for network administrators.

- It made it very apparent that network security administrators must patch their systems regularly.

- If security patches had been applied in a timely manner, the Code Red worm would only merit a footnote in network security history.

# CERT Code Red

- http://www.cert.org/advisories/CA-2001-19.html


CERT Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL - Microsoft Internet Explorer p
File Edit View Favorites Tools Help
Back
Search
Favorites
Links
Google
NETWORKERS
TOOLS
ARIES
BOB
Address
http://www.cert.org/advisories/CA-2001-19.html
Go
CERT
search
GO
customize | Publications Catalog
Software Assurance
Secure Systems
Organizational Security
Coordinated Response
Training
related links
Publications Catalog
Historical Documents
Authorized Users of "CERT"
US-CERT Vulnerability Notes Database
Vulnerability Disclosure Policy
Courses
US-CERT
www.us-cert.gov
Internet

## CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overfl IIS Indexing Service DLL

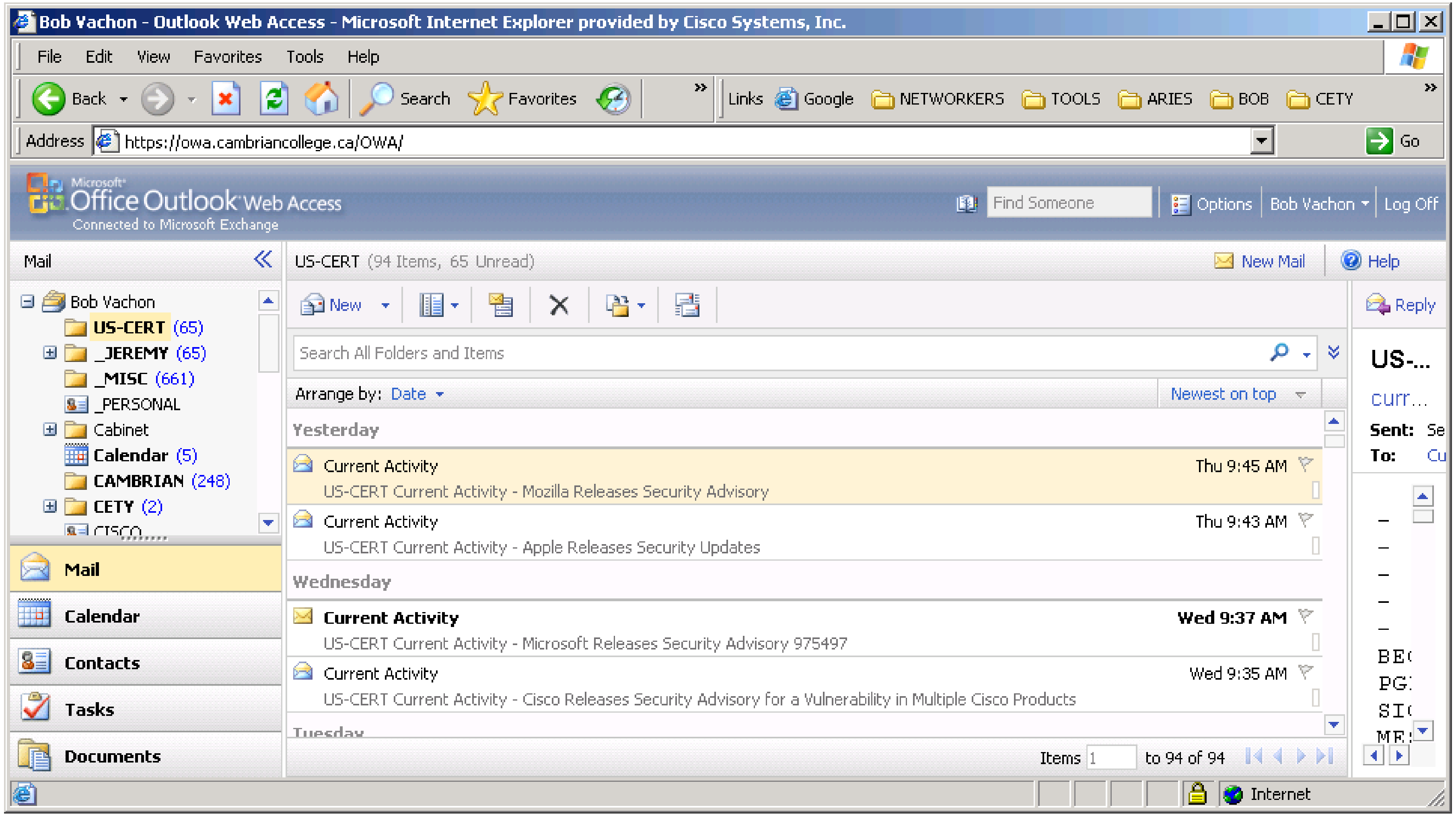
Original release date: July 19, 2001
Last revised: January 17, 2002
Source: CERT/CC

A complete revision history can be found at the end of this file.

### Systems Affected

- Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled and Index Server 2.0 installed
- Windows 2000 with IIS 4.0 or IIS 5.0 enabled and Indexing services installed
- Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager (these systems r
- Unpatched Cisco 600 series DSL routers

# New Threats


Bob Vachon - Outlook Web Access - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back
Search
Favorites
Links Google NETWORKERS TOOLS ARIES BOB CETY
Address https://owa.cambriancollege.ca/OWA/
Go
Microsoft Office Outlook Web Access
Connected to Microsoft Exchange
Find Someone
Options
Bob Vachon
Log Off
Mail
Bob Vachon
US-CERT (65)
_JEREMY (65)
_MISC (661)
_PERSONAL
Cabinet
Calendar (5)
CAMBRIAN (248)
CETY (2)
CISCO
Mail
Calendar
Contacts
Tasks
Documents
New Mail
Help
New
Reply
Search All Folders and Items
Internet

US-CERT (94 Items, 65 Unread)

Arrange by: Date — Newest on top

Yesterday

Current Activity — Thu 9:45 AM
US-CERT Current Activity - Mozilla Releases Security Advisory

Current Activity — Thu 9:43 AM
US-CERT Current Activity - Apple Releases Security Updates

Wednesday

**Current Activity** — **Wed 9:37 AM**
US-CERT Current Activity - Microsoft Releases Security Advisory 975497

Current Activity — Wed 9:35 AM
US-CERT Current Activity - Cisco Releases Security Advisory for a Vulnerability in Multiple Cisco Products

Tuesday

Items 1 to 94 of 94

US-...
curr...
Sent: Se
To: Cu

# New Cisco Tool!

- Cisco IOS Checker:

http://tools.cisco.com/security/center/selectIOSVersion.x

# Drivers for Network Security

# Hacker Titles

Phreaker

An individual that manipulates the phone network in order to cause it to perform a function that is normally not allowed such as to make free long distance calls. Captain Crunch (John Drapper)

# Hacker Titles

Spammer

Individual that sends large quantities of unsolicited email messages. Spammers often use viruses to take control of home computers to send out their bulk messages.

Phisher

Individual uses email or other means in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords.

# Evolution of Hacking

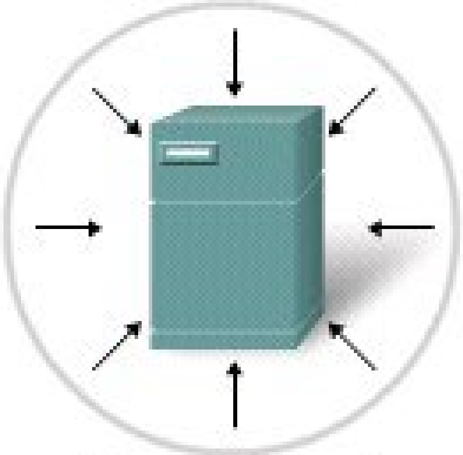
- 1960s - Phone Freaks (Phreaks)
- 1980s - Wardialing (WarGames)
- 1988 - Internet Worm
- 1993 - First def Con hacking conference held
- 1995 - First 5 year federal prison sentence for hacking
- 1997 - Nmap released
- 1997 - First malicious scripts used by script kiddies
- 2002 - Melissa virus creator gets 20 months in jail

# Security firsts …

First Virus

First Worm

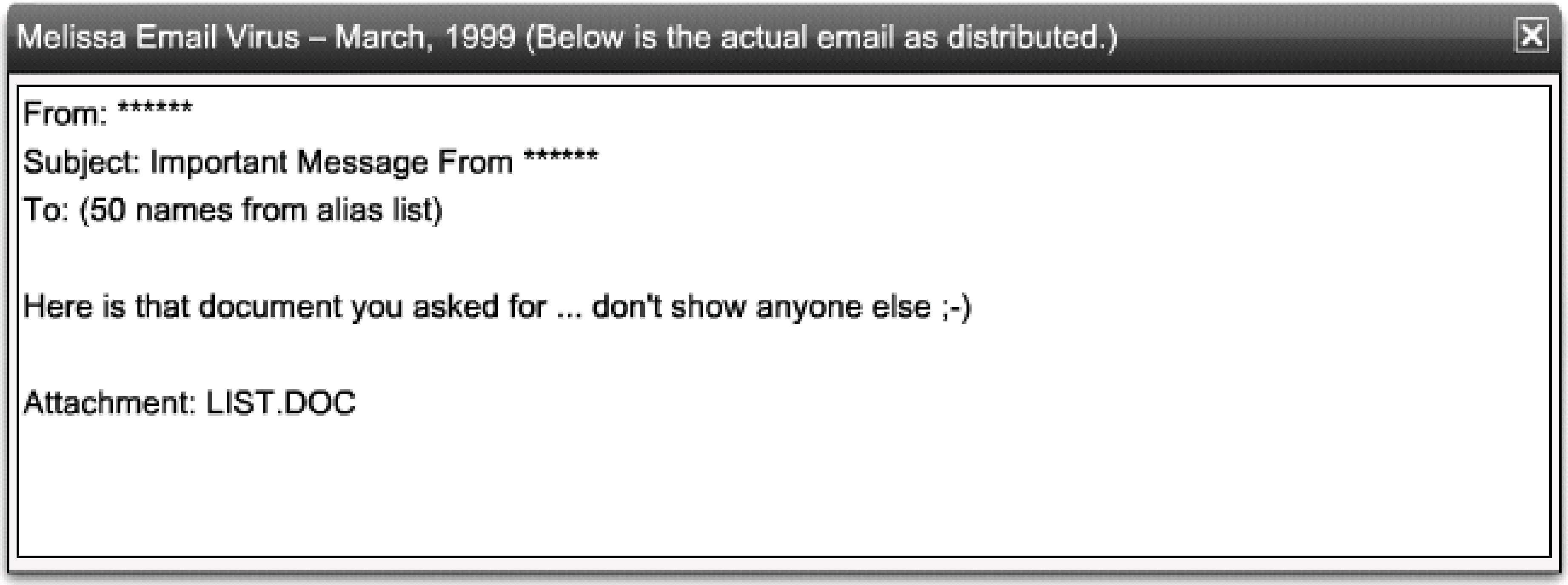
First Spam



First DoS Attack

# First Email Virus

- The first email virus, the Melissa virus, was written by David Smith and resulted in memory overflows in Internet mail servers due to excessive traffic.
- David Smith was sentenced to 20 months in federal prison and a $5,000 fine.



Melissa Email Virus – March, 1999 (Below is the actual email as distributed.)

From: ******

Subject: Important Message From ******

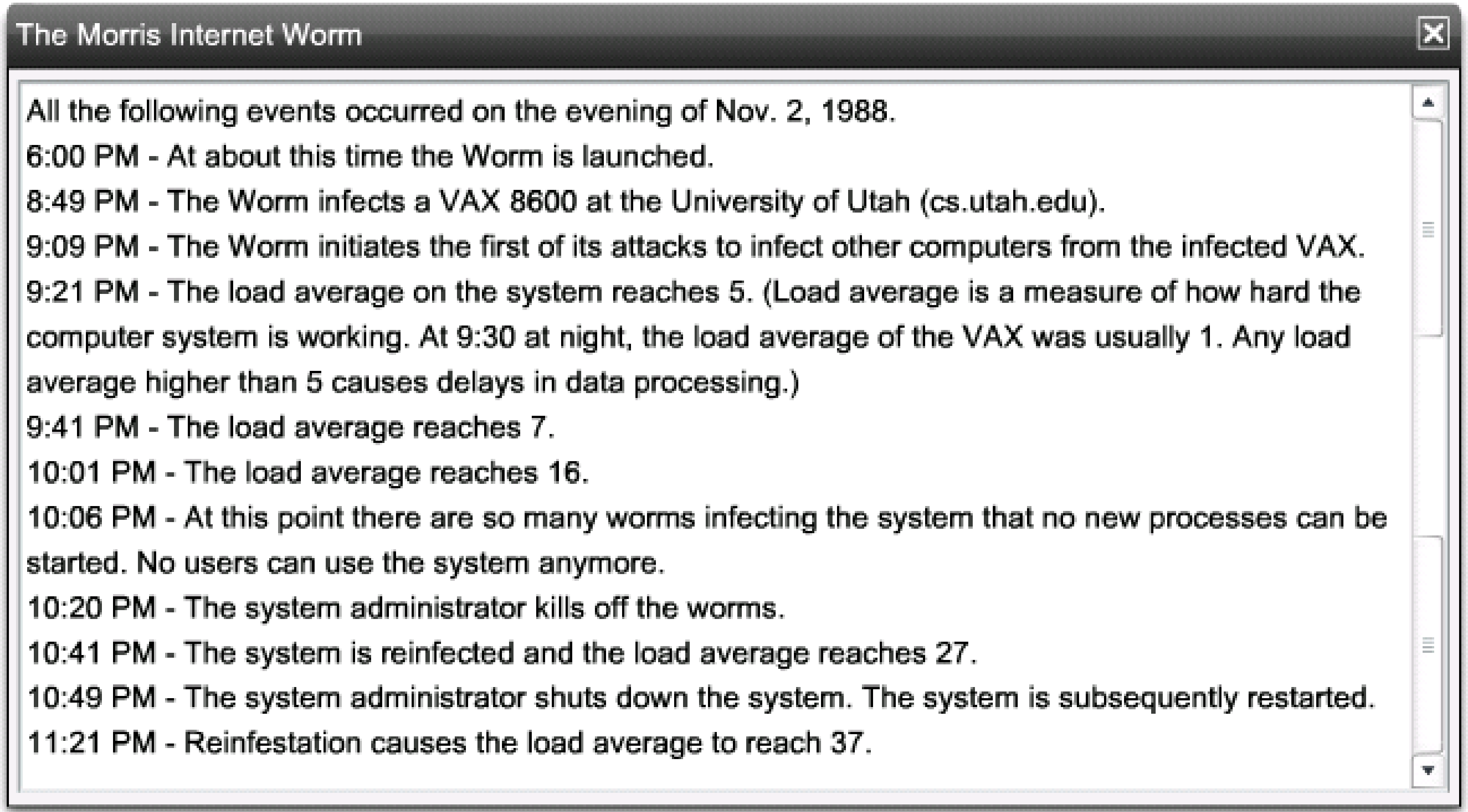
To: (50 names from alias list)

Here is that document you asked for ... don't show anyone else ;-)

Attachment: LIST.DOC

# First Worm

- Robert Morris created the first Internet worm with 99 lines of code.
- When the Morris Worm was released, 10% of Internet systems were brought to a halt.



All the following events occurred on the evening of Nov. 2, 1988.

6:00 PM - At about this time the Worm is launched.

8:49 PM - The Worm infects a VAX 8600 at the University of Utah (cs.utah.edu).

9:09 PM - The Worm initiates the first of its attacks to infect other computers from the infected VAX.

9:21 PM - The load average on the system reaches 5. (Load average is a measure of how hard the computer system is working. At 9:30 at night, the load average of the VAX was usually 1. Any load average higher than 5 causes delays in data processing.)

9:41 PM - The load average reaches 7.

10:01 PM - The load average reaches 16.

10:06 PM - At this point there are so many worms infecting the system that no new processes can be started. No users can use the system anymore.

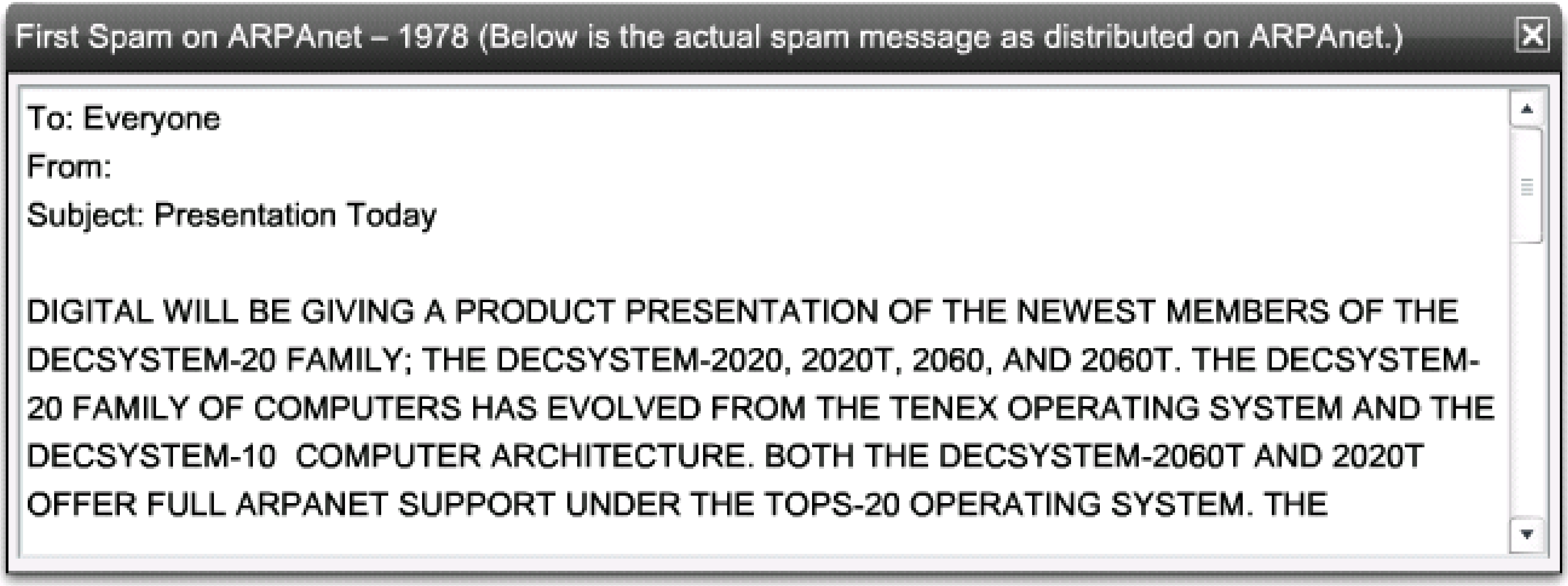
10:20 PM - The system administrator kills off the worms.

10:41 PM - The system is reinfected and the load average reaches 27.

10:49 PM - The system administrator shuts down the system. The system is subsequently restarted.

11:21 PM - Reinfestation causes the load average to reach 37.

# First SPAM



First Spam on ARPAnet – 1978 (Below is the actual spam message as distributed on ARPAnet.)

To: Everyone
From:
Subject: Presentation Today

DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM AND THE DECSYSTEM-10 COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM. THE

# First DoS Attack

- MafiaBoy was the Internet alias of Michael Calce, a 15 year old high school student from Montreal, Canada.

- He launched highly publicized DoS attacks in Feb 2000 against Yahoo!, Amazon.com, Dell, Inc., E*TRADE, eBay, and CNN.

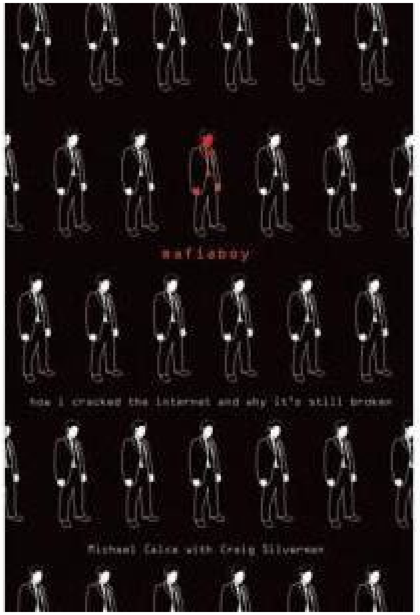
# Mafiaboy

- In 2001, The Montreal Youth Court sentenced him on September 12, 2001 to eight months of "open custody," one year of probation, restricted use of the Internet, and a small fine.

- In 2005, Mr. Calce wrote as a columnist on computer security topics for the Francophone newspaper Le Journal de Montréal.

- In 2008, he published Mafiaboy: “How I Cracked the Internet and Why It's Still Broken.”

- He has also made numerous TV appearances.


mafiaboy
how i cracked the internet and why it's still broken
Michael Calce with Craig Silverman

# Trends Driving Network Security

- Increase of network attacks
- Increased sophistication of attacks
- Increased dependence on the network
- Wireless access
- Lack of trained personnel
- Lack of awareness
- Lack of security policies
- Legislation
- Litigation

# Legal and Governmental Policy Issues

- Organizations that operate vulnerable networks will face increasing and substantial liability.
  - http://en.wikipedia.org/wiki/Information_security#Laws_and_regulations

- US Federal legislation mandating security includes the following:
- Gramm-Leach-Blilely (GLB) bill financial services legislation
- Government Information Security Reform Act
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Children Internet Protection Act (CIPA)
- The Payment Card Industry Data Security Standard (PCI DSS)
- Sarbanes-Oxley Act of 2002

# How to Keep on Top?

- Network security professionals must collaborate with professional colleagues more frequently than most other professions

- Attending workshops and conferences that are often affiliated with, sponsored or organized by local, national, or international technology organizations.

- Must also know about various security organizations which provide help on:
- Detecting and responding to both established and emerging information security threats.
- Operating system weaknesses, best practices for security, and security training and certification information is also available.

# Network Security Organizations

# Information Security Organizations

- Three of the more well-established network security organizations are:
  - Computer Emergency Response Team (CERT)
  - SysAdmin, Audit, Network, Security (SANS) Institute
  - International Information Systems Security Certification Consortium (pronounce (ISC)2 as "I-S-C-squared")
- Cisco also has the Security Intelligence Operations (SIO)

# Network Security Policies and Domains

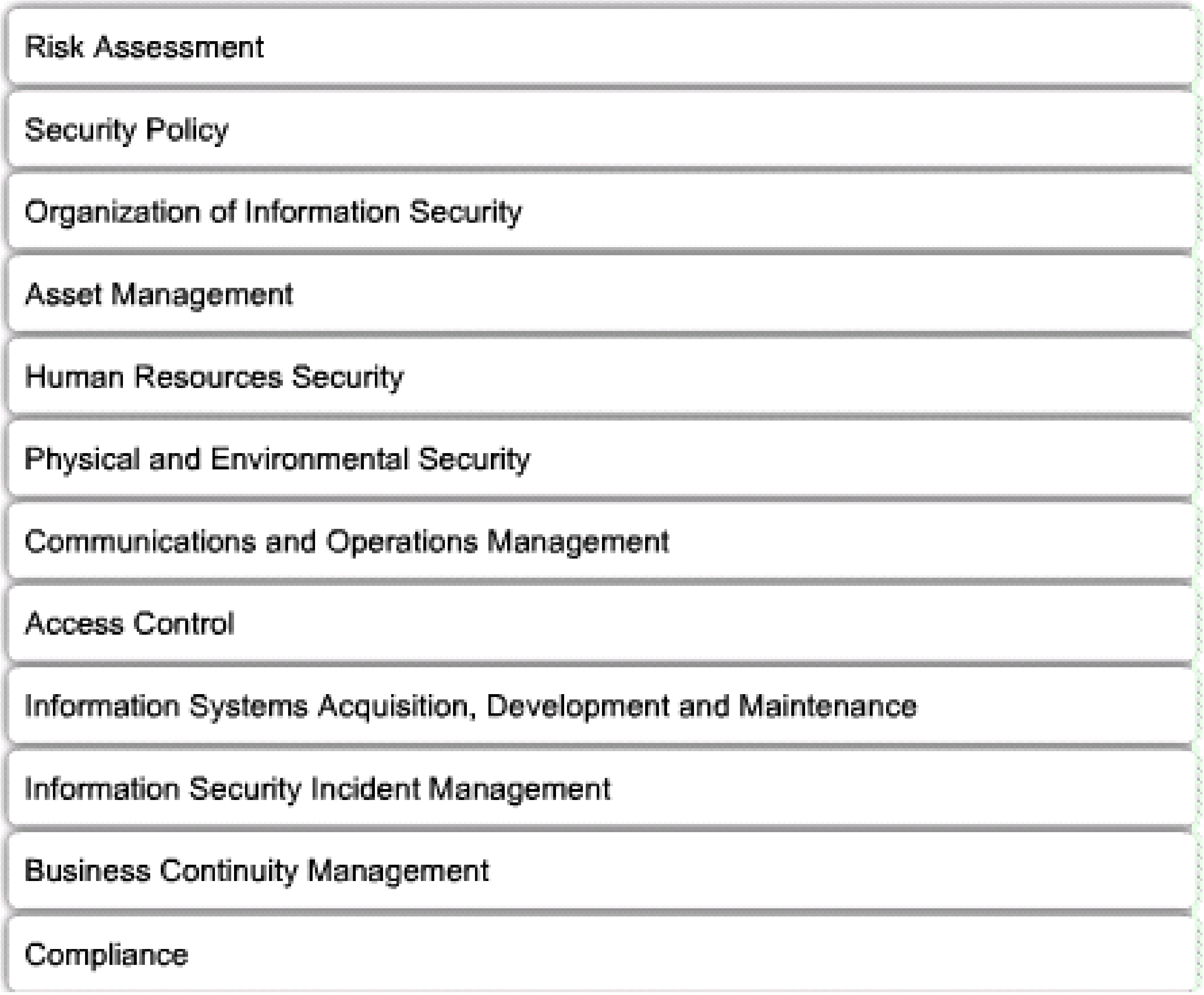
# Domains of Network Security

- It is also important to have an understanding of the various network security domains.
  - Domains provide an organized framework to facilitate learning about network security.

- ISO/IEC 27002 specifies 12 network security domains.
  - These 12 domains serve to organize at a high level the vast realm of information under the umbrella of network security.

  - The 12 domains are intended to serve as a common basis for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

# Domains of Network Security



- Risk Assessment
- Security Policy
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

# Cisco SecureX

- This architecture includes the following five major components:
    - Scanning Engines – Network level devices that examine content, authenticate users, and identify applications. They can include firewall/IPS, proxy or a fusion of both.
    - Delivery Mechanisms – The way the scanning engine is implemented in the network. It can be via a standalone appliance, a blade in a router, or a software package.
    - Security Intelligence Operations (SIO) – A traffic monitoring database, used to identify and stop malicious traffic.
    - Policy Management Consoles – Policy creation and management that determines what actions the scanning engines will take.
    - Next-generation Endpoint – Any variety of devices. All traffic to or from these devices are pointed to a scanner.

# Security Policy

1. What do you have that others want?
2. What processes, data, or information systems are critical to you, your company, or your organization?
3. What would stop your company or organization from doing business or fulfilling its mission?

The security policy should protect the assets of your organization by answering several security questions.

# Malware, Malicious Code

# Types of Attacks

- There are four categories of attacks:
  - Malicious Code: Viruses, Worms and Trojan Horses
  - Reconnaissance Attacks
  - Access Attacks
  - Denial of Service (DoS) Attacks

Let’s focus on Malicious Code

# Malware

- “Malicious software” is software designed to infiltrate a computer without the owner's informed consent.

- Malware includes:

    - Computer viruses

    - Worms

    - Trojan horses

    - Rootkits

    - Backdoors (Method of bypassing normal authentication procedures and usually installed using Trojan horses or worms.)

    - For profit (Spyware, botnets, keystroke loggers, and dialers)

# Spyware

- Spyware is a strictly for-profit category of malware designed to:
    - Monitor a users web browsing.
    - Display unsolicited advertisements.
    - Redirect affiliate marketing revenues to the spyware creator.
- Spyware programs are generally installed by exploiting security holes or as Trojan horse programs such as most peer-to-peer applications.

# Why Write Malicious Code?

- Most early worms and viruses were written as experiments or pranks generally intended to be harmless or merely annoying rather than to cause serious damage to computers.

- Young programmers learning about viruses and the techniques wrote them for the sole purpose that they could or to see how far it could spread.

    - In some cases the perpetrator did not realize how much harm their creations could do.

- As late as 1999, widespread viruses such as the Melissa virus appear to have been written chiefly as pranks.

# Malicious Code Writing Today

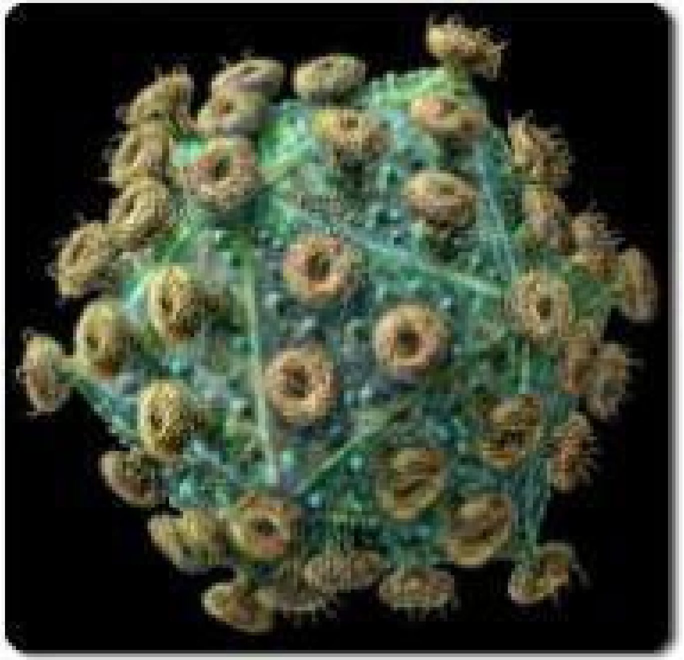
- Malicious code writing has changed for profitable reasons.
    - Mainly due to the Internet and broadband access.
    - Since 2003 the majority of viruses and worms have been designed to take control of users' computers for black-market exploitation.
    - Infected "zombie computers" are used to send email spam, to host contraband data, or to engage in DDoS attacks as a form of extortion.
- In 2008, Symantec published:
    - The release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications.

# Viruses, Trojan Horses, and Worms

- A virus is malicious software that is attached to another program to execute a particular unwanted function on a user's workstation.
- A worm executes arbitrary code and installs copies of itself in the infected computer’s memory, which infects other hosts.
- A Trojan horse is different only in that the entire application was written to look like something else, when in fact it is an attack tool.

# Viruses

- A computer virus is a malicious computer program (executable file) that can copy itself and infect a computer without permission or knowledge of the user.
- A virus can only spread from one computer to another by:
  - Sending it over a network as a file or as an email payload.
  - Carrying it on a removable medium.
- Viruses need USER INTERVENTION to spread ...



# Viruses

- Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk.

- Others are not designed to do any damage, but simply replicate themselves and perhaps make their presence known by presenting text, video, or audio messages.

# Worms

- Worms are a particularly dangerous type of hostile code.
    - They replicate themselves by independently exploiting vulnerabilities in networks.
    - Worms usually slow down networks.
- Worms DO NOT NEED USER INTERVENTION!
    - Worms do not require user participation and can spread extremely fast over the network.

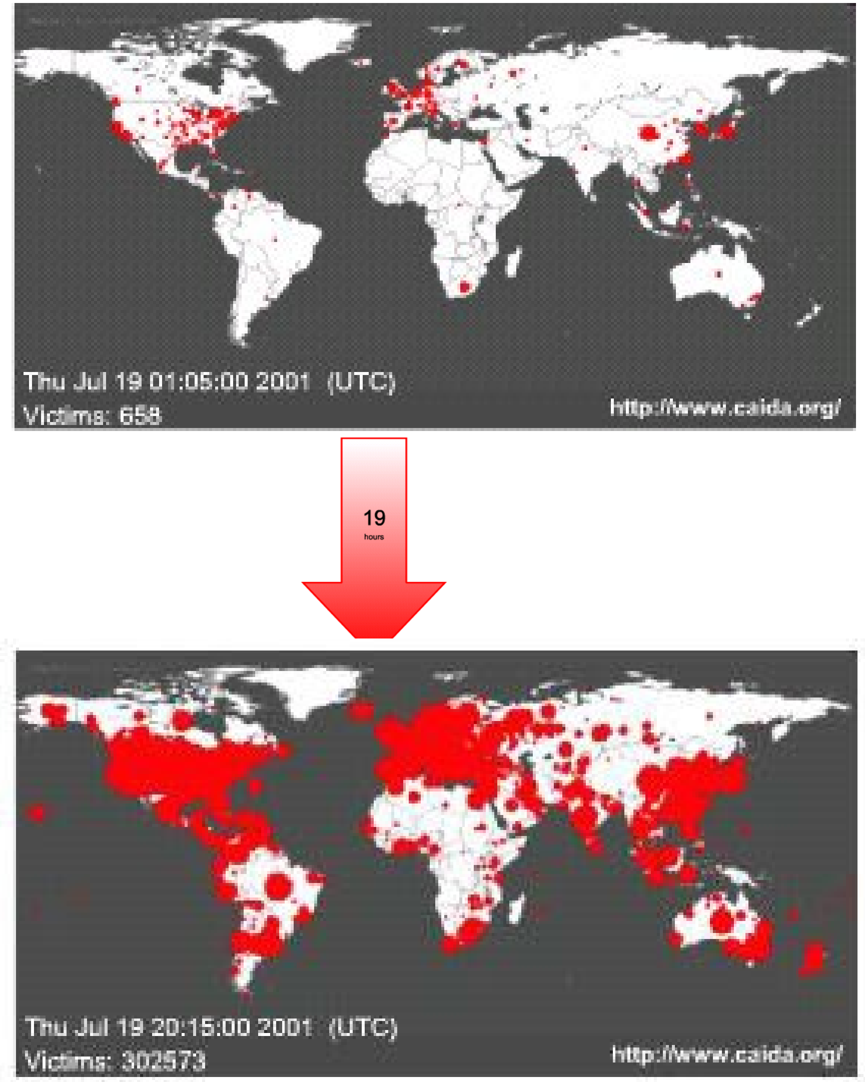
# SQL Slammer Worms

- In January 2001, the SQL Slammer Worm slowed down global Internet traffic as a result of DoS.

- Over 250,000 hosts were affected within 30 minutes of its release.

- The worm exploited a buffer overflow bug in Microsoft's SQL Server.

    - A patch for this vulnerability was released in mid-2002, so the servers that were affected were those that did not have the update patch applied.



# Anatomy of a Worm

- The enabling vulnerability
    - A worm installs itself using an exploit vector on a vulnerable system.
- Propagation mechanism
    - After gaining access to devices, a worm replicates and selects new targets.
- Payload
    - Once the device is infected with a worm, the attacker has access to the host – often as a privileged user.
    - Attackers could use a local exploit to escalate their privilege level to administrator.

# Trojan Horses

# The year's most-hacked software

- *“Kits that go by names like ‘T-IFramer,’ ‘Liberty Exploit Systems’ and ‘Elenore’ all turned up on underground markets selling for $300 to $500, Kandek says, and allow the attacker to install a Trojan program ready to download whatever malicious software a cybercriminal wishes, from spyware to click-fraud software. All three of those kits exploit three unique Adobe Reader bugs, along with a smaller number of bugs in Internet Explorer, Microsoft Office, Firefox and even Quicktime.”*

Excerpt from the article at:

http://www.cbc.ca/technology/story/2009/12/16/f-forbes-adobe-hacked-software.html

# Trojan Horse

- A Trojan horse is a program that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.
- Trojan horses may appear to be useful or interesting programs, or at the very least harmless to an unsuspecting user, but are actually harmful when executed.
- Trojan horses are not self-replicating which distinguishes them from viruses and worms.

# Trojan Horse Classification

- Remote-access Trojan Horse
    - Enables unauthorized remote access
- Data sending Trojan Horse
    - Provides the attacker with sensitive data such as passwords
- Destructive Trojan Horse
    - Corrupts or deletes files
- Proxy Trojan Horse
    - User's computer functions as a proxy server
- FTP Trojan Horse (opens port 21)
    - Security software disabler Trojan Horse (stops anti-virus programs or firewalls from functioning)
- Denial of Service Trojan Horse (slows or halts network activity)

# Five Phases of a Virus/Worm Attack

- Probe phase:
  - Vulnerable targets are identified using ping scans.
  - Application scans are used to identify operating systems and vulnerable software.
  - Hackers obtain passwords using social engineering, dictionary attack, brute-force, or network sniffing.
- Penetrate phase:
  - Exploit code is transferred to the vulnerable target.
  - Goal is to get the target to execute the exploit code through an attack vector, such as a buffer overflow, ActiveX or Common Gateway Interface (CGI) vulnerabilities, or an email virus.

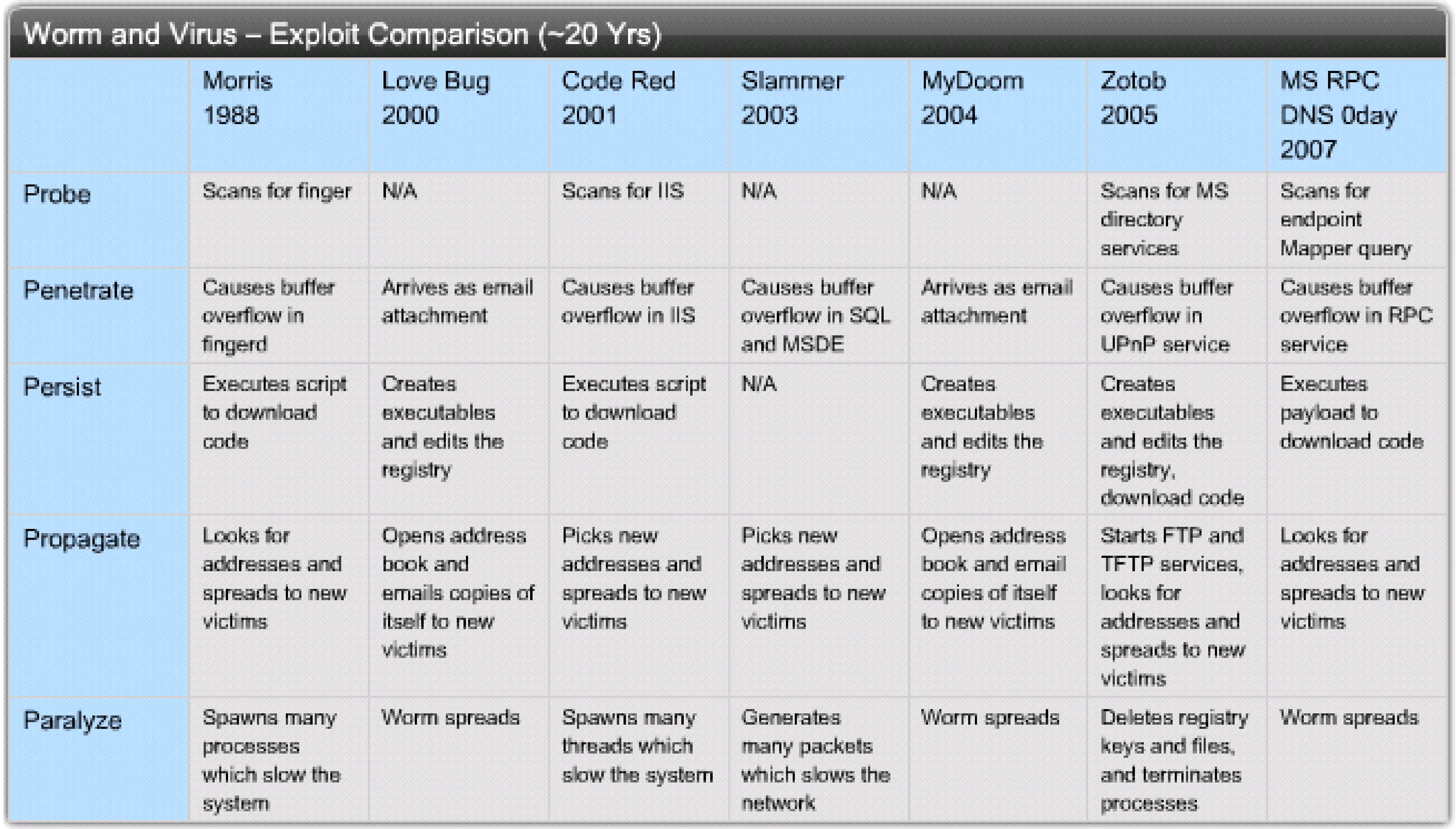
# Five Phases of a Virus/Worm Attack

- Persist phase:
- After the attack is successfully launched in the memory, the code tries to persist on the target system.
- Goal is to ensure that the attacker code is running and available to the attacker even if the system reboots.
- Achieved by modifying system files, making registry changes, and installing new code.

# Five Phases of a Virus/Worm Attack

- Propagate phase:
- The attacker attempts to extend the attack to other targets by looking for vulnerable neighboring machines.
- Propagation vectors include emailing copies of the attack to other systems, uploading files to other systems using file shares or FTP services, active web connections, and file transfers through Internet Relay Chat.
- Paralyze phase:
- Actual damage is done to the system.
- Files can be erased, systems can crash, information can be stolen, and distributed DDoS attacks can be launched.

# Exploit Comparison



Worm and Virus – Exploit Comparison (~20 Yrs)

| | Morris<br>1988 | Love Bug<br>2000 | Code Red<br>2001 | Slammer<br>2003 | MyDoom<br>2004 | Zotob<br>2005 | MS RPC<br>DNS 0day<br>2007 |
|---|---|---|---|---|---|---|---|
| Probe | Scans for finger | N/A | Scans for IIS | N/A | N/A | Scans for MS directory services | Scans for endpoint Mapper query |
| Penetrate | Causes buffer overflow in fingerd | Arrives as email attachment | Causes buffer overflow in IIS | Causes buffer overflow in SQL and MSDE | Arrives as email attachment | Causes buffer overflow in UPnP service | Causes buffer overflow in RPC service |
| Persist | Executes script to download code | Creates executables and edits the registry | Executes script to download code | N/A | Creates executables and edits the registry | Creates executables and edits the registry, download code | Executes payload to download code |
| Propagate | Looks for addresses and spreads to new victims | Opens address book and emails copies of itself to new victims | Picks new addresses and spreads to new victims | Picks new addresses and spreads to new victims | Opens address book and email copies of itself to new victims | Starts FTP and TFTP services, looks for addresses and spreads to new victims | Looks for addresses and spreads to new victims |
| Paralyze | Spawns many processes which slow the system | Worm spreads | Spawns many threads which slow the system | Generates many packets which slows the network | Worm spreads | Deletes registry keys and files, and terminates processes | Worm spreads |

# Commonalities

- A majority of the software vulnerabilities that are discovered relate to buffer overflows.
    - Buffer overflows are usually the primary conduit through which viruses, worms, and Trojan Horses do their damage.
- Viruses and Trojan Horses tend to take advantage of local root buffer overflows.
    - A root buffer overflow is intended to attain root privileges to a system.
- Worms such as SQL Slammer and Code Red exploit remote root buffer overflows.
    - Remote root buffer overflows are similar to local root buffer overflows, except that local end user or system intervention is not required.

# How Do You Mitigate Viruses and Worms?

Antivirus Software

AVG Internet Security 2012
Norton AntiVirus 2012 with Antispyware
McAfee Internet Security 2012
Kaspersky PURE
Kaspersky Anti-Virus 2012
Titanium Antivirus+
avast! Pro Antivirus
ZoneAlarm Antivirus + Firewall
Bitdefender Internet Security 2012
ESET NOD32 Antivirus 5
Panda Antivirus Pro 2012

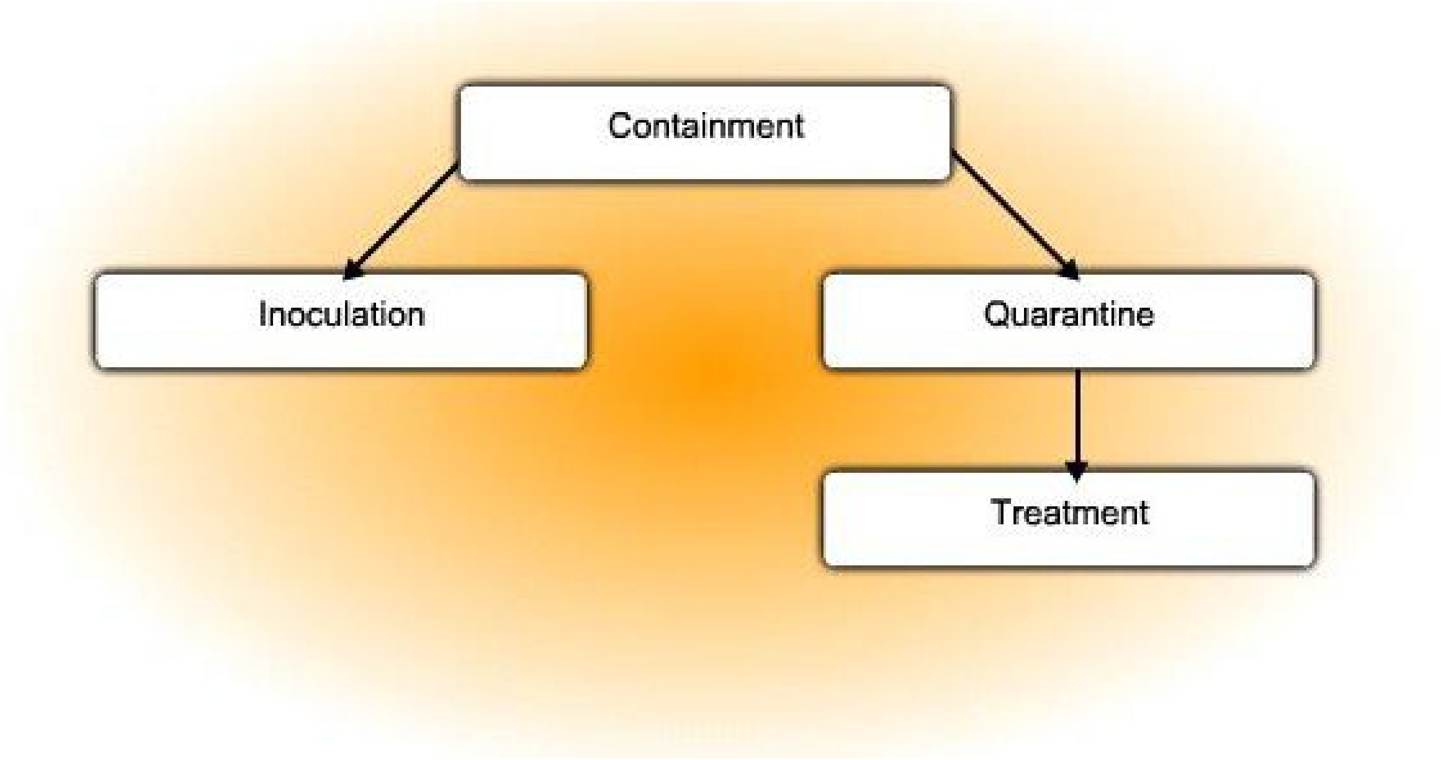
# Viruses and Trojan Horses - Mitigation

- The primary means of mitigating virus and Trojan horse attacks is anti-virus software.
    - For total protection, host-based intrusion prevention systems (HIPS), such as Cisco Security Agent should also be deployed.
    - HIPS protects the OS kernel.
- Anti-virus software helps prevent hosts from getting infected and spreading malicious code.
    - However, antivirus software must be used properly.
    - Always update with the latest antivirus .dat and application versions.
    - Consider that it requires much more time to clean up infected computers than it does to maintain up-to-date anti-virus software and anti-virus definitions on the same machines.

# Mitigating an Active Worm

- Worm attack mitigation requires diligence on the part of system and network administration staff.

- There is a four phase process to mitigate an active worm attacks.



# Worms - Mitigation

- Containment Phase:
  - Limit the spread of a worm infection to areas of the network that are already affected.
  - Compartmentalize and segment the network to slow down or stop the worm to prevent currently infected hosts from targeting and infecting other systems.
  - Use both outgoing and incoming ACLs on routers and firewalls at control points within the network.
- Inoculation Phase:
  - Runs parallel to or subsequent to the containment phase.
  - All uninfected systems are patched with the appropriate vendor patch for the vulnerability.
  - The inoculation process further deprives the worm of any available targets.

# Worms - Mitigation

- Quarantine Phase:
  - Track down and identify infected machines within the contained areas and disconnect, block, or remove them.
  - This isolates these systems appropriately for the Treatment Phase.
- Treatment Phase:
  - Actively infected systems are disinfected of the worm.
  - Terminate the worm process, remove modified files or system settings that the worm introduced, and patch the vulnerability the worm used to exploit the system.
  - In more severe cases, completely reinstalling the system to ensure that the worm and its by products are removed.

# Example: Mitigating SQL Slammer

- The SQL Slammer worm used UDP port 1434.
    - This port should normally be blocked by a firewall on the perimeter.
    - However, most infections enter internally and therefore, to prevent the spreading of this worm it would be necessary to block this port on all devices throughout the internal network.
- When SQL Slammer was propagating, some organizations could not block UDP port 1434 because it was required to access the SQL Server for legitimate business transactions.
    - Permit only selective access to a small number of clients using SQL Server.

# Types of Attacks

- There are four categories of attacks:
  - Malicious Code: Viruses, Worms and Trojan Horses
  - Reconnaissance Attacks
  - Access Attacks
  - Denial of Service (DoS) Attacks

Let’s focus on Reconnaissance attacks

# Reconnaissance

- Reconnaissance also known as information gathering is the unauthorized discovery and mapping of systems, services, or vulnerabilities.
    - In most cases, precedes an access or DoS attack.
- Reconnaissance attacks can consist of the following:
    - Internet information queries
    - Ping sweeps
    - Port scans
    - Packet sniffers

# Internet Information Queries

- DNS queries can reveal information such as who owns a particular domain and what addresses have been assigned to that domain.
    - Use tools such as **whois**, **nslookup**, …

# Ping Sweeps and Port Scans

- A ping sweep, or ICMP sweep, scans to determine which range of IP addresses map to live hosts.

- A port scan consists of sending a message to each port, one port at a time.

    - Response received indicates whether the port is used and can therefore be probed for weakness.

# Ping Sweeps and Port Scans

- As legitimate tools, ping sweep and port scan applications run a series of tests against hosts to identify vulnerable services.
- The information is gathered by examining IP addressing and port data from both TCP and UDP ports.

# Packet Sniffing

- A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets that are sent across a LAN.
    - Packet sniffers can only work in the same collision domain as the network being attacked.
    - Promiscuous mode is a mode in which the network adapter card sends all packets that are received on the physical network wire to an application for processing.
    - Wireshark is an example of a packet sniffer.

# Packet Sniffing

- Some network applications (FTP, Telnet, TFTP, SNMP, …) distribute network packets in plaintext.
    - The packets can be processed and understood by packet sniffing applications.
    - Numerous freeware and shareware packet sniffers are available that do not require the user to understand anything about the underlying protocols.

# Types of Attacks

- There are four categories of attacks:
    - Malicious Code: Viruses, Worms and Trojan Horses
    - Reconnaissance Attacks
    - Access Attacks
    - Denial of Service (DoS) Attacks

Let’s focus on Access attacks

# Access Attacks

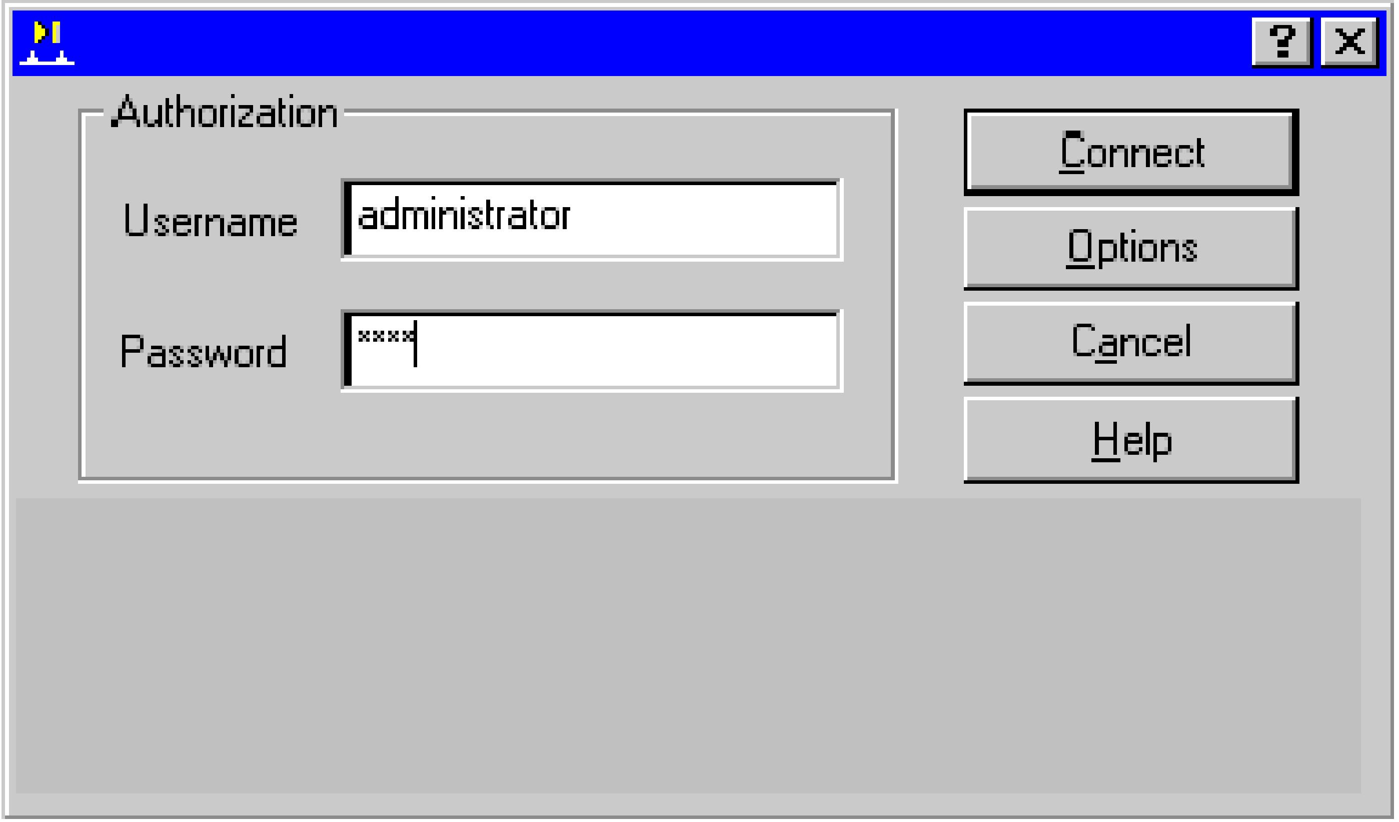
- Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information for these reasons:
    - Retrieve data
    - Gain access
    - Escalate their access privileges

# Access Attacks

- Access attacks can be performed in a number of different ways, including:
  - Password attacks
  - Trust exploitation
  - Port redirection
  - Man-in-the-middle attacks
  - Buffer overflow

# Password Attacks

- Hackers implement password attacks using the following:
  - Brute-force attacks
  - Trojan horse programs
  - IP spoofing
  - Packet sniffers



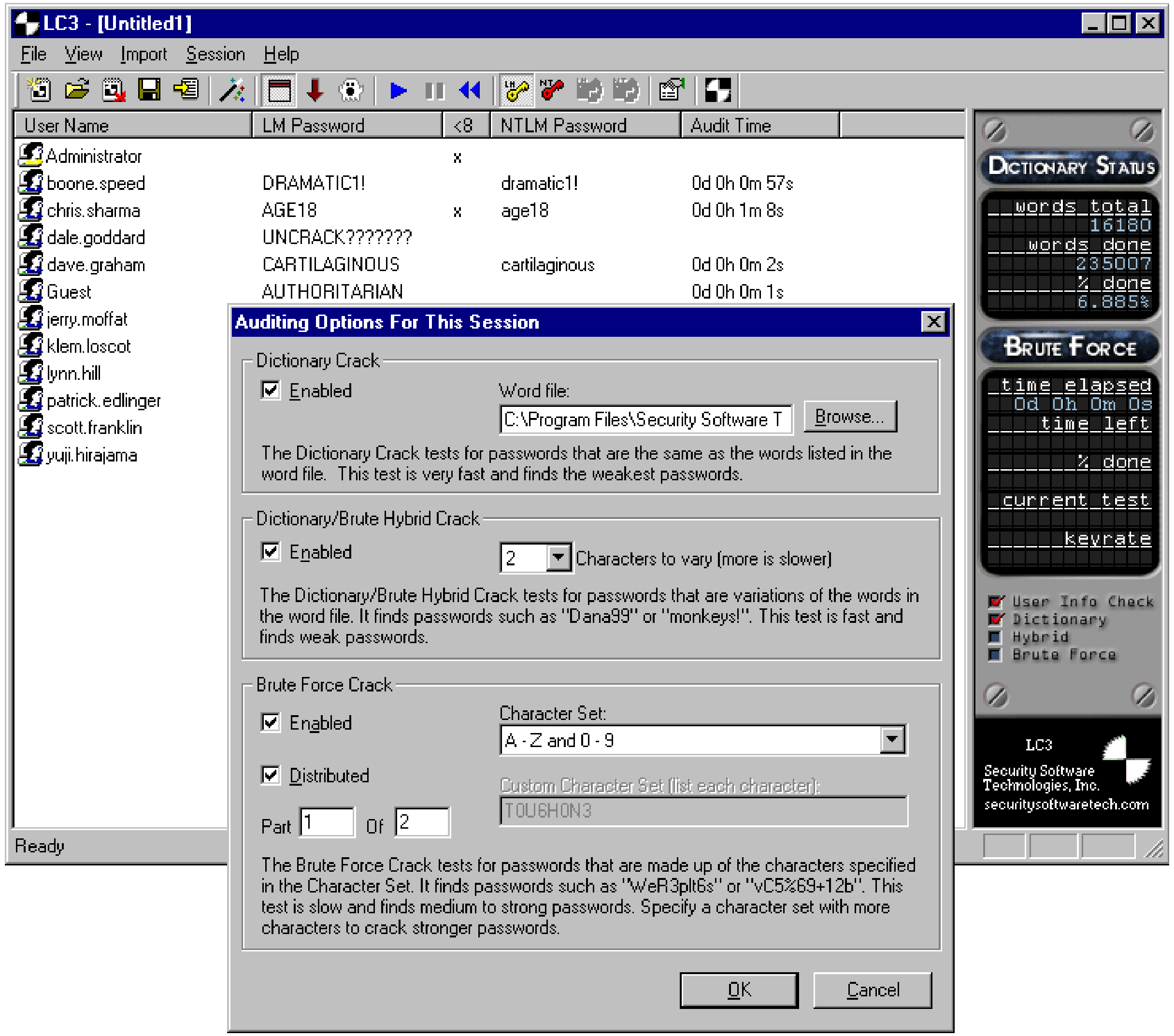
Authorization

Username: administrator

Password: ****

# Password Attack Example

- L0phtCrack (“loft-crack”) takes the hashes of passwords and generates the plaintext passwords from them.
- Passwords are compromised using one of two methods:
    - Dictionary cracking
    - Brute-force computation



| User Name | LM Password | <8 | NTLM Password | Audit Time |
|---|---|---|---|---|
| Administrator | | x | | |
| boone.speed | DRAMATIC1! | | dramatic1! | 0d 0h 0m 57s |
| chris.sharma | AGE18 | x | age18 | 0d 0h 1m 8s |
| dale.goddard | UNCRACK??????? | | | |
| dave.graham | CARTILAGINOUS | | cartilaginous | 0d 0h 0m 2s |
| Guest | AUTHORITARIAN | | | 0d 0h 0m 1s |
| jerry.moffat | | | | |
| klem.loscot | | | | |
| lynn.hill | | | | |
| patrick.edlinger | | | | |
| scott.franklin | | | | |
| yuji.hirajama | | | | |

Ready

**Auditing Options For This Session**

Dictionary Crack

☑ Enabled

Word file: C:\Program Files\Security Software T

Browse...

The Dictionary Crack tests for passwords that are the same as the words listed in the word file. This test is very fast and finds the weakest passwords.

Dictionary/Brute Hybrid Crack

☑ Enabled

2 Characters to vary (more is slower)

The Dictionary/Brute Hybrid Crack tests for passwords that are variations of the words in the word file. It finds passwords such as "Dana99" or "monkeys!". This test is fast and finds weak passwords.

Brute Force Crack

☑ Enabled

Character Set: A - Z and 0 - 9

☑ Distributed

Custom Character Set (list each character): T0U6H0N3

Part 1 Of 2

The Brute Force Crack tests for passwords that are made up of the characters specified in the Character Set. It finds passwords such as "WeR3pIt6s" or "vC5%69+12b". This test is slow and finds medium to strong passwords. Specify a character set with more characters to crack stronger passwords.

OK Cancel

Dictionary Status

words total 16180

words done 235007

% done 6.885%

Brute Force

time elapsed 0d 0h 0m 0s

time left

% done

current test

keyrate

☑ User Info Check
☑ Dictionary
□ Hybrid
□ Brute Force

# Trust Exploitation

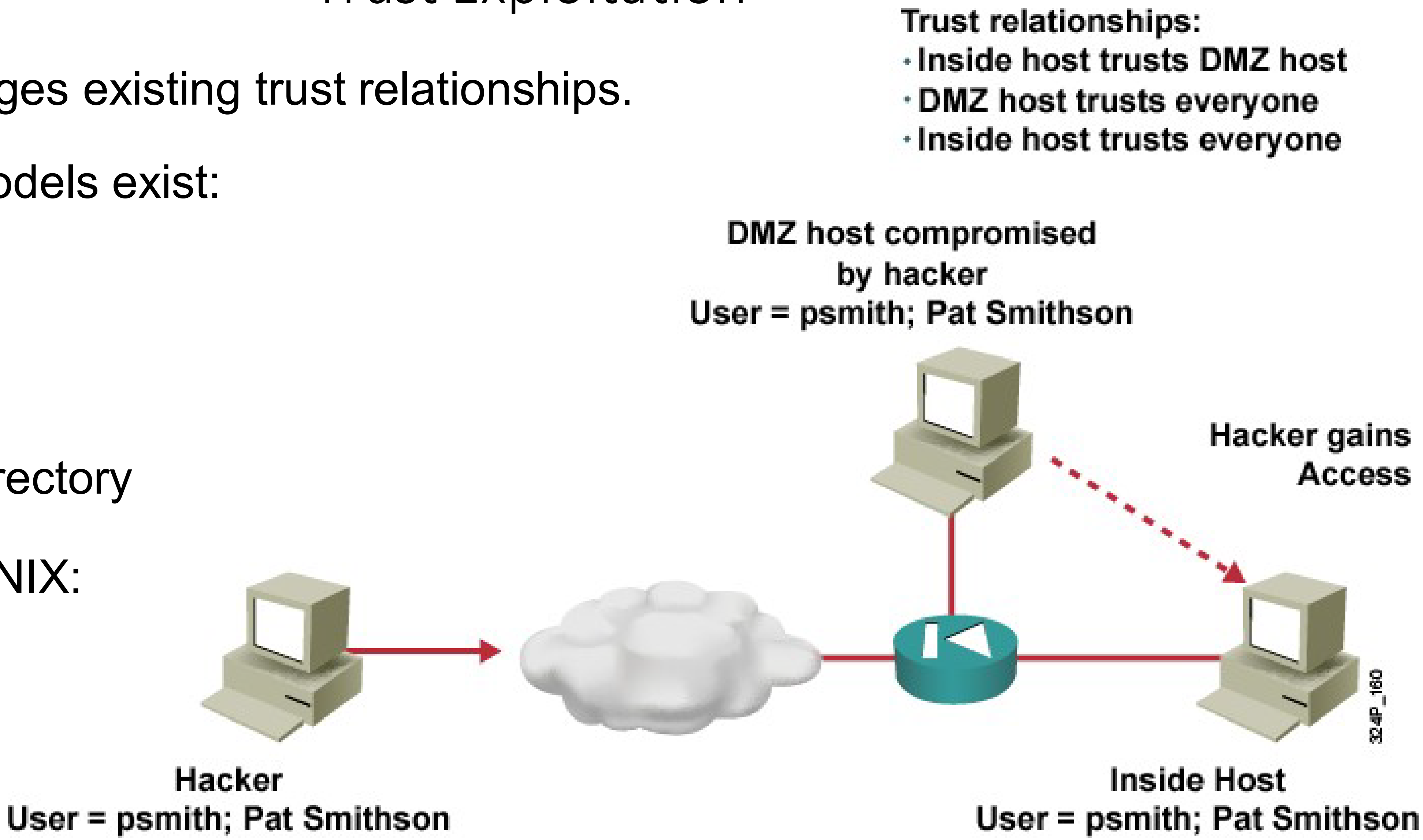
- Trust exploitation refers to an individual taking advantage of a trust relationship within a network.
- An example of when trust exploitation takes place is when a perimeter network is connected to a corporate network.
  - These network segments often contain DNS, SMTP, and HTTP servers.
  - Because these servers all reside on the same segment, a compromise of one system can lead to the compromise of other systems if those other systems also trust systems that are attached to the same network.

# Trust Exploitation

- Another example of trust exploitation is a Demilitarized Zone (DMZ) host that has a trust relationship with an inside host that is connected to the inside firewall interface.
- The inside host trusts the DMZ host.
  - When the DMZ host is compromised, the attacker can leverage that trust relationship to attack the inside host.

# Trust Exploitation

- A hacker leverages existing trust relationships.
- Several trust models exist:
    - Windows:
        - Domains
        - Active directory
    - Linux and UNIX:
        - NIS
        - NIS+



Trust relationships:
· Inside host trusts DMZ host
· DMZ host trusts everyone
· Inside host trusts everyone
DMZ host compromised by hacker
User = psmith; Pat Smithson
Hacker gains Access
Hacker
User = psmith; Pat Smithson
Inside Host
User = psmith; Pat Smithson
324P_160

# Port Redirection

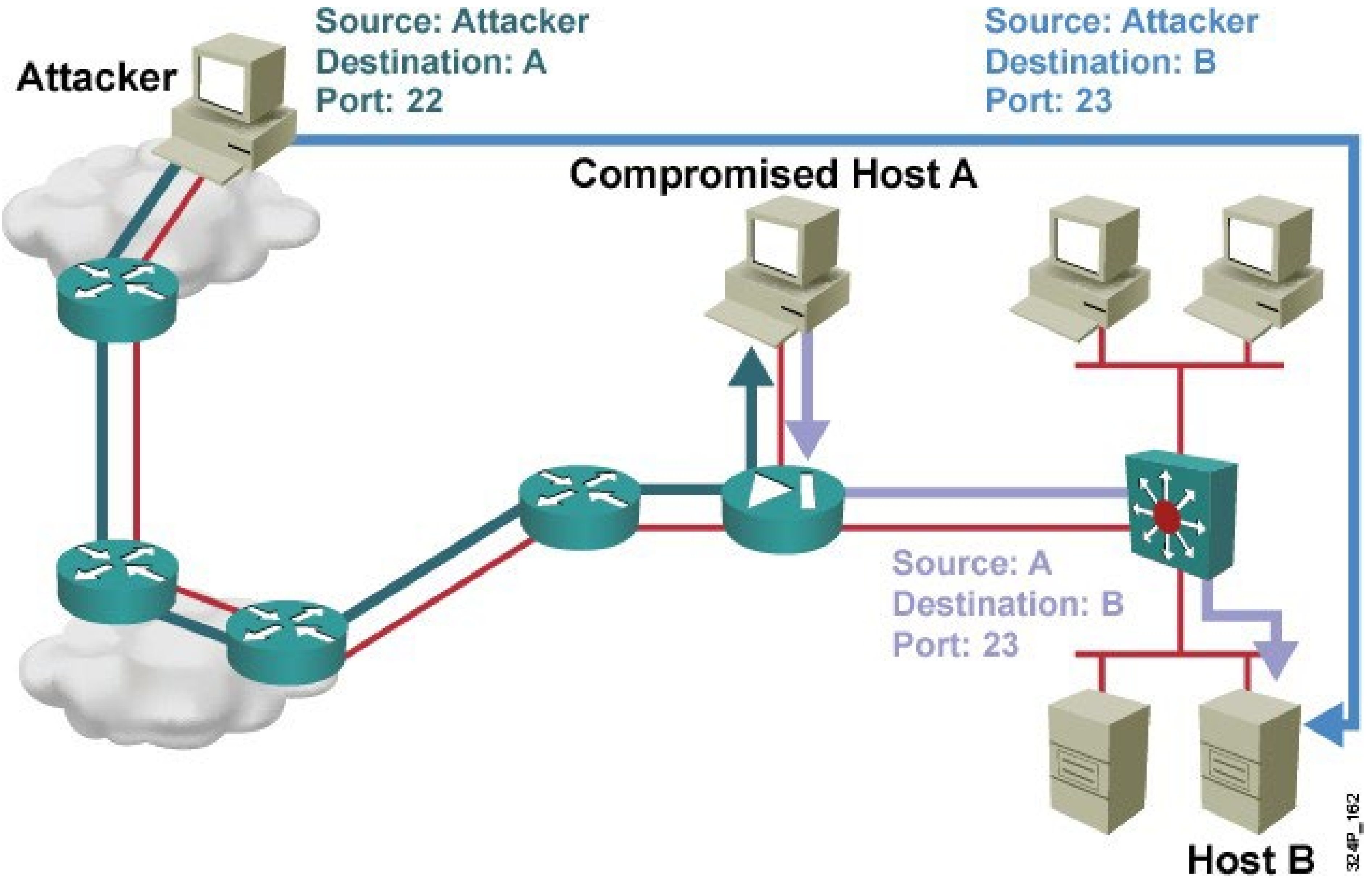
- A port redirection attack is a type of trust exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise have been dropped.

  - Port redirection bypasses the firewall rule sets by changing the normal source port for a type of network traffic.

  - You can mitigate port redirection by using proper trust models that are network-specific.

  - Assuming a system is under attack, an IPS can help detect a hacker and prevent installation of such utilities on a host.

# Port Redirection



# “Man-in-the-Middle” Attacks

- Man-in-the-middle attacks have these purposes:
    - Theft of information
    - Hijacking of an ongoing session to gain access to your internal network resources
    - Traffic analysis to obtain information about your network and network users
    - DoS
    - Corruption of transmitted data
    - Introduction of new information into network sessions
- An example of a man-in-the-middle attack is when someone working for your ISP gains access to all network packets that transfer between your network and any other network

# Types of Attacks

- There are four categories of attacks:
    - Malicious Code: Viruses, Worms and Trojan Horses
    - Reconnaissance Attacks
    - Access Attacks
    - Denial of Service (DoS) Attacks

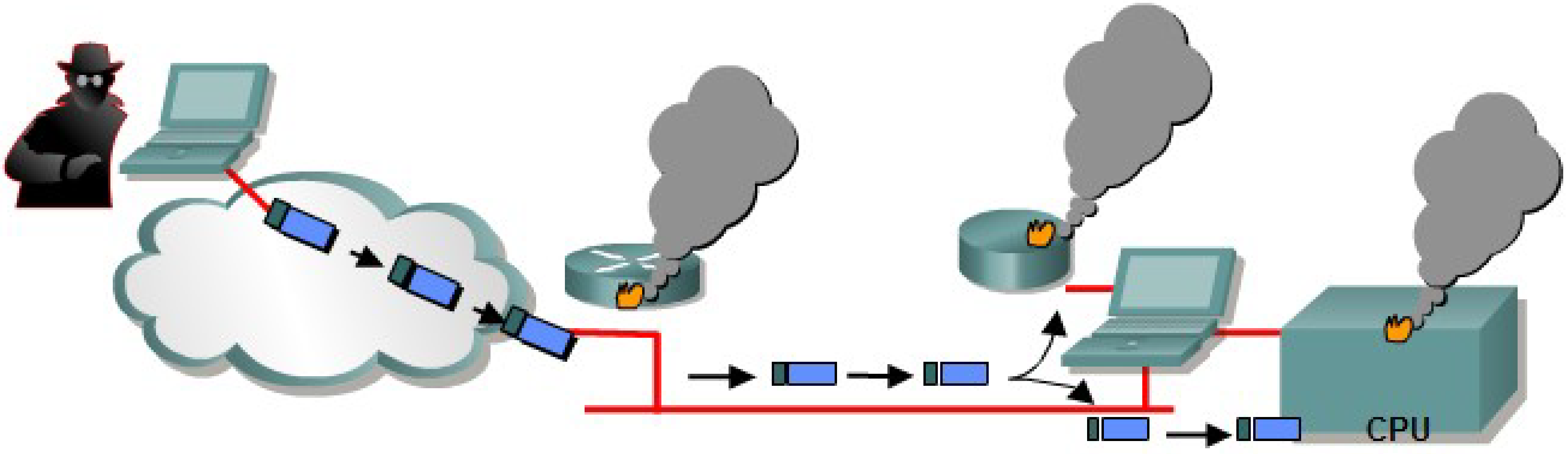
Let’s focus on DoS attacks

# Denial of Service Attack (DoS)

- Among the most difficult to completely eliminate because they require so little effort to execute.
- Types of DoS attacks include:
  - Ping of death
  - Smurf Attack
  - TCP SYN flood attack
- Others include packet fragmentation and reassembly, E-mail bombs, CPU hogging, Malicious applets, Misconfiguring routers, the chargen attack, out-of-band attacks such as WinNuke, Land.c, Teardrop.c, and Targa.c.

# DoS Attacks

DoS attacks prevent authorized people from using a service by using up system resources.



**Resource overloads**

- Disk space, bandwidth, buffers, and so on.
- Ping floods: smurf, and so on.
- Packet storms: UDP bombs, fraggle, and so on.

**Malformed data**

- Oversized packets: ping of death, and so on.
- Overlapping packets: winuke, and so on.
- Un-handled data: teardrop, and so on.

# Ping of Death

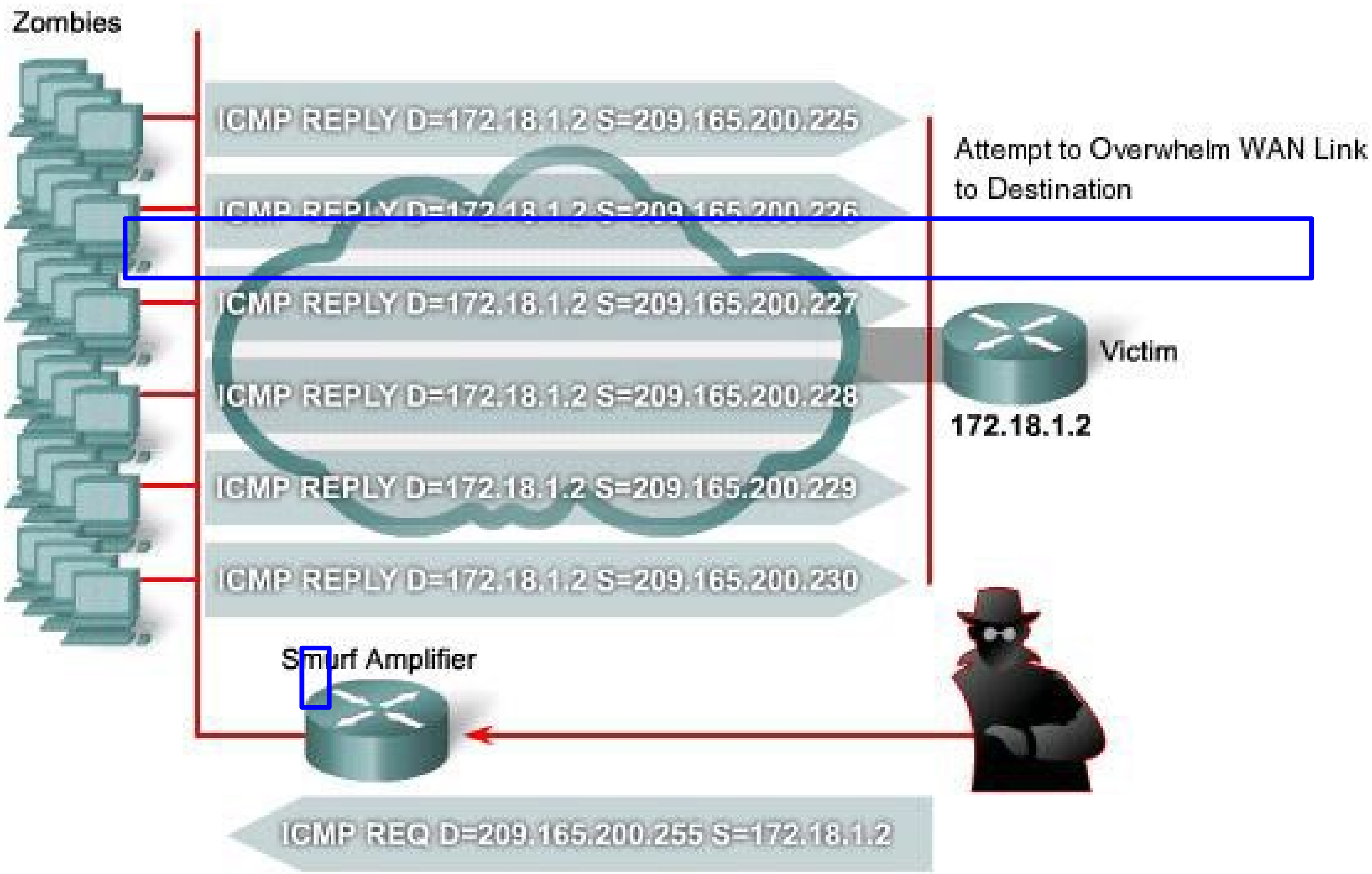
- Legacy attack that sent an echo request in an IP packet larger than the maximum packet size of 65,535 bytes.
    - Sending a ping of this size can crash the target computer.
- A variant of this attack is to crash a system by sending ICMP fragments, which fill the reassembly buffers of the target.

# Smurf Attack

▪This attack sends a large number of ICMP requests to directed broadcast addresses, all with spoofed source addresses on the same network as the respective directed broadcast.

- If the routing device delivering traffic to those broadcast addresses forwards the directed broadcasts, all hosts on the destination networks send ICMP replies, multiplying the traffic by the number of hosts on the networks.
- On a multi-access broadcast network, hundreds of machines might reply to each packet.

# Smurf Attack


Zombies
ICMP REPLY D=172.18.1.2 S=209.165.200.225
ICMP REPLY D=172.18.1.2 S=209.165.200.226
ICMP REPLY D=172.18.1.2 S=209.165.200.227
ICMP REPLY D=172.18.1.2 S=209.165.200.228
ICMP REPLY D=172.18.1.2 S=209.165.200.229
ICMP REPLY D=172.18.1.2 S=209.165.200.230
Attempt to Overwhelm WAN Link to Destination
Victim
172.18.1.2
Smurf Amplifier
ICMP REQ D=209.165.200.255 S=172.18.1.2

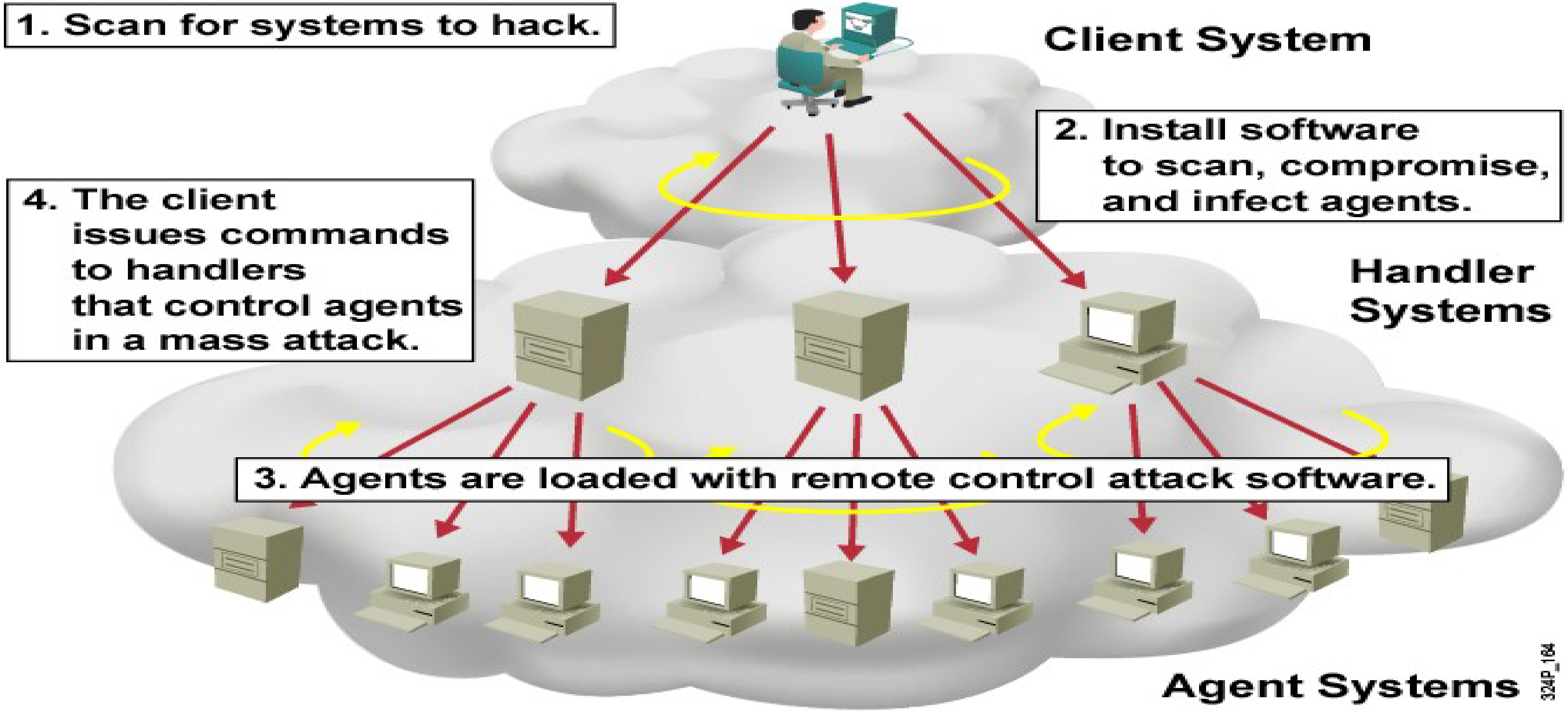
# SYN Flood Attack

- A flood of TCP SYN packets is sent, often with a forged sender address.
  - Each packet is handled like a connection request, causing the server to spawn a half-open (embryonic) connection by sending back a TCP SYN-ACK packet and waiting for a packet in response from the sender address.
  - However, because the sender address is forged, the response never comes.
  - These half-open connections saturate the number of available connections the server is able to make, keeping it from responding to legitimate requests until after the attack ends.

# DoS and DDoS Attacks and Mitigation

- A DDoS attack and the simpler version of a DoS attack on a server, send extremely large numbers of requests over a network or the Internet.
  - These many requests cause the target server to run well below optimum speeds.
  - Consequently, the attacked server becomes unavailable for legitimate access and use.
  - By overloading system resources, DoS and DDoS attacks crash applications and processes by executing exploits or a combination of exploits.
  - DoS and DDoS attacks are the most publicized form of attack and are among the most difficult to completely eliminate.

# DDoS Attack Example



1. Scan for systems to hack.

2. Install software to scan, compromise, and infect agents.

3. Agents are loaded with remote control attack software.

4. The client issues commands to handlers that control agents in a mass attack.

# DDoS Attack Risks

- DDoS attack risks include:
    - Downtime and productivity loss
    - Revenue loss from sales and support services
    - Lost customer loyalty
    - Theft of information
    - Extortion
    - Stock price manipulation
    - Malicious competition

# Distributed Denial of Service Attack (DoS)

- DDoS attacks are designed to saturate network links with spurious data which can overwhelm a link causing legitimate traffic to be dropped.
  - DDoS uses attack methods similar to standard DoS attacks but operates on a much larger scale.
  - Typically hundreds or thousands of attack points attempt to overwhelm a target.
- Examples of DDoS attacks include the following:
  - Tribe Flood Network (TFN)
  - Stacheldraht

# Reconnaissance Attacks - Countermeasures

- Implementing and enforcing a policy directive that forbids the use of protocols with known susceptibilities to eavesdropping.

- Using encryption that meets the data security needs of the organization without imposing an excessive burden on the system resources or the users.

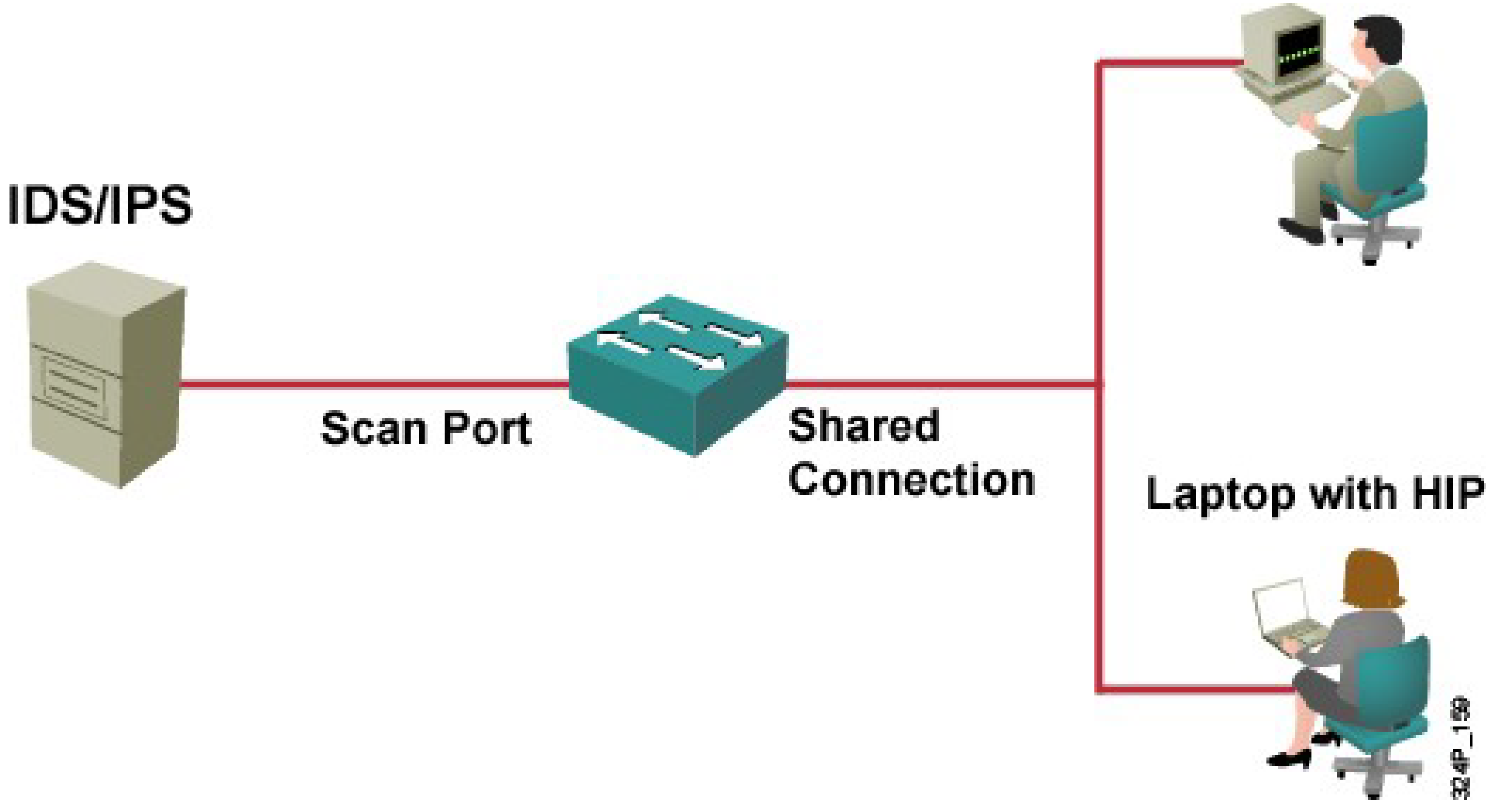
- Using switched networks.

# Port Scan and Ping Sweep Mitigation

- Port scanning and ping sweeping is not a crime and there is no way to stop these scans and sweeps when a computer is connected to the Internet.
    - There are ways to prevent damage to the system.
- Ping sweeps can be stopped if ICMP echo and echo-reply are turned off on edge routers.
    - When these services are turned off, network diagnostic data is lost.

# Ping Sweeps and Port Scans Mitigation

- Can’t be prevented without compromising network capabilities.
  - However, damage can be mitigated using intrusion prevention systems (IPS) at network and host levels.



# Packet Sniffer Mitigation

- Authentication
  - Strong authentication is a first line for defense

.

- Cryptography
  - If a communication channel is cryptographically secure, the only data a packet sniffer detects is cipher text.

- Anti-sniffer tools
  - Antisniffer tools detect changes in the response time of hosts to determine whether the hosts are processing more traffic than their own traffic loads would indicate.

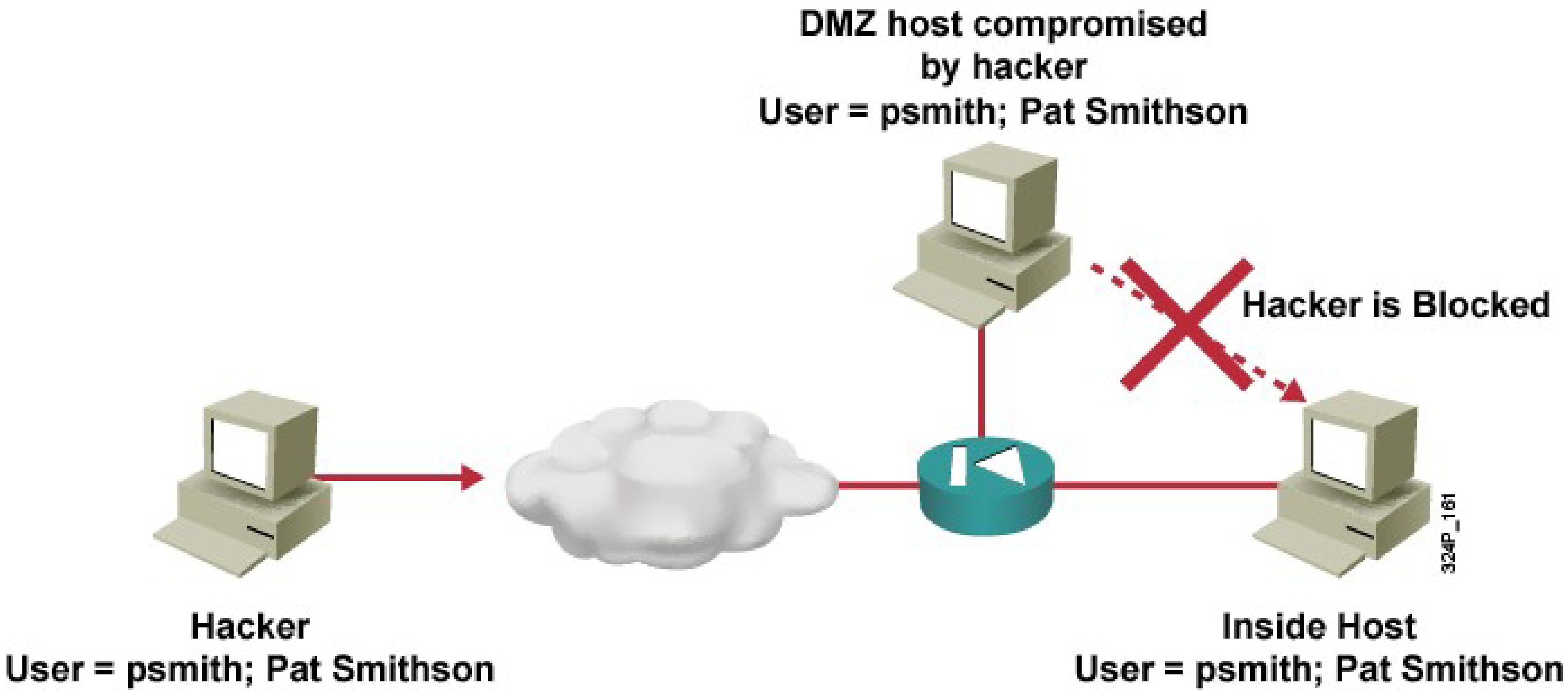
- Switched infrastructure
  - A switched infrastructure obviously does not eliminate the threat of packet sniffers but can greatly reduce the sniffers’ effectiveness.

# Password Attack Mitigation

- Password attack mitigation techniques include:
    - Do not allow users to use the same password on multiple systems.
    - Disable accounts after a certain number of unsuccessful login attempts.
    - Use OTP or a cryptographic password is recommended.
    - Use “strong” passwords that are at least eight characters long and contain uppercase letters, lowercase letters, numbers, and special characters.
    - Do not use plain text passwords.

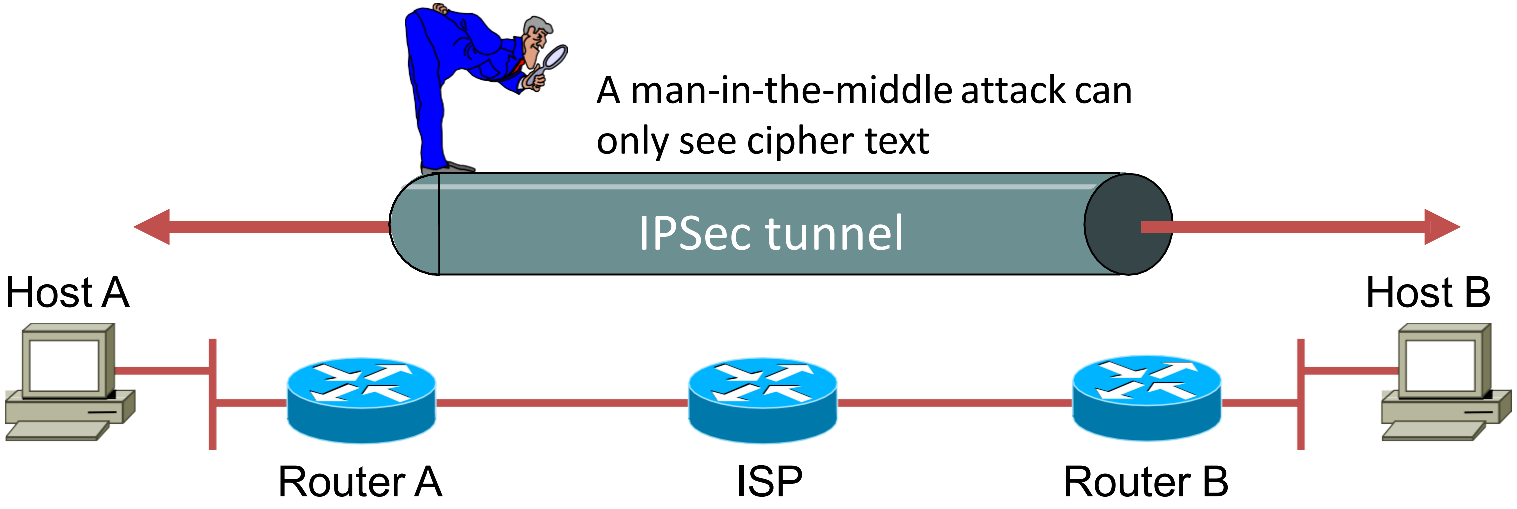
# Trust Exploitation Attack Mitigation

•Trust levels within a network should be tightly restrained by ensuring that systems inside a firewall never absolutely trust systems outside the firewall.


DMZ host compromised
by hacker
User = psmith; Pat Smithson
Hacker is Blocked
Hacker
User = psmith; Pat Smithson
Inside Host
User = psmith; Pat Smithson
324P_161

# Man-in-the-Middle Mitigation

- Man-in-the-middle attacks can be effectively mitigated only through the use of cryptography (encryption).



A man-in-the-middle attack can only see cipher text

# DoS and DDoS Attack Mitigation

- Anti-DoS features on routers and firewalls:
  - Proper configuration of anti-DoS features on routers and firewalls can help limit the effectiveness of an attack.

  - These features often involve limits on the amount of half-open TCP connections that a system allows at any given time.
- Anti-spoof features on routers and firewalls:
  - Proper configuration of anti-spoof features on your routers and firewalls can reduce your risk of attack.

  - These features include an appropriate filtering with access lists, unicast reverse path forwarding that looks up the routing table to identify spoofed packets, disabling of source route options, and others.

# DoS and DDoS Attack Mitigation

- Traffic rate limiting at the ISP level:
    - An organization can implement traffic rate limiting with its Service Provider.

# IP Spoofing Attack Mitigation

- The threat of IP spoofing can be reduced, but not eliminated, using these measures:
    - Access control configuration
    - Encryption
    - RFC 3704 filtering
- Additional authentication requirement that does not use IP address-based authentication; examples are:
    - Cryptographic (recommended)
    - Strong, two-factor, one-time passwords

# 10 Best Practices

1.Keep patches up to date by installing them weekly or daily, if possible, to prevent buffer overflow and privilege escalation attacks.

1.Shut down unnecessary services and ports.

1.Use strong passwords and change them often
.
1.Control physical access to systems.

# 10 Best Practices

5. Avoid unnecessary web page inputs.

- Some websites allow users to enter usernames and passwords.
- A hacker can enter more than just a username.
- For example, entering "jdoe; rm -rf /" might allow an attacker to remove the root file system from a UNIX server.
- Programmers should limit input characters and not accept invalid characters such as | ; < > as input.

# 10 Best Practices

1.Perform backups and test the backed up files on a regular basis

.

1.Educate employees about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.

- http://www.networkworld.com/news/2010/091610-social-networks.html?source=NWWNLE_nlt_daily_pm_2010-09-16
- http://searchsecurity.techtarget.com/news/1519804/Phishing-attacks-target-users-of-Facebook-other-social-networks?asrc=EM_NLN_12420860&track=NL-102&ad=784799&

1.Encrypt and password-protect sensitive data.

1.Implement security hardware and software such as firewalls, IPSs, virtual private network (VPN) devices, anti-virus software, and content filtering.

1.Develop a written security policy for the company.

# Know Thine Enemy

- "If you know yourself but not your enemy, for every victory gained you will also suffer a defeat."

    - Sun Tzu – The Art of War

- Before learning how to defend against attacks, you need to know how a potential attacker operates.

# Hacking a Network

- The goal of any hacker is to compromise the intended target or application.

- Hackers begin with little or no information about the intended target.

- Their approach is always careful and methodical—never rushed and never reckless.

- The seven-step process outlined on the next slide is a good representation of the method that hackers use – and a starting point for an analysis of how to defeat it.

# Seven Steps to Hacking a Network

- Step 1 — Perform footprint analysis (reconnaissance).
- Step 2 — Detail the information.
- Step 3 — Manipulate users to gain access.
- Step 4 — Escalate privileges.
- Step 5 — Gather additional passwords and secrets.
- Step 6 — Install back doors.
- Step 7 — Leverage the compromised system.

# Step 1 - Footprint Analysis (Reconnaissance)

- Gain knowledge of acquisitions using Web pages, phone books, company brochures, subsidiaries, etc.

- Use commands to develop a more detailed footprint:
  - **nslookup** command to reconcile domain names against IP addresses of the company's servers and devices.

  - **traceroute** command to help build topology.

- Use program and utilities:
  - **WHOIS** queries (http://www.who.is/)

  - Port scanning to find open ports and operating systems installed on hosts.

  - **Nmap**: Network Mapper (Nmap) is a free open source utility for network exploration or security auditing.

# How to Defeat Footprinting

- Keep all sensitive data off-line (business plans, formulas, and proprietary documents).
- Minimize the amount of information on your public website.
- Examine your own website for insecurities.
- Run a ping sweep on your network.
- Familiarize yourself with one or more of the five Regional Internet Registries – such as ARIN for North America – to determine network blocks.

# Step 2 - Detail the Information

- Find your server applications and versions:
  - What are your web, FTP, and mail server versions?

  - Listen to TCP and UDP ports and send random data to each.

  - Cross-reference information to vulnerability databases to look for potential exploits.

- Exploit selected TCP ports, for example:
  - Windows NT, 2000, and XP file sharing using SMB protocol which uses TCP port 445.

  - In Windows NT, SMB runs on top of NetBT using ports 137, 138 (UDP), and 139 (TCP).

# Software Tools

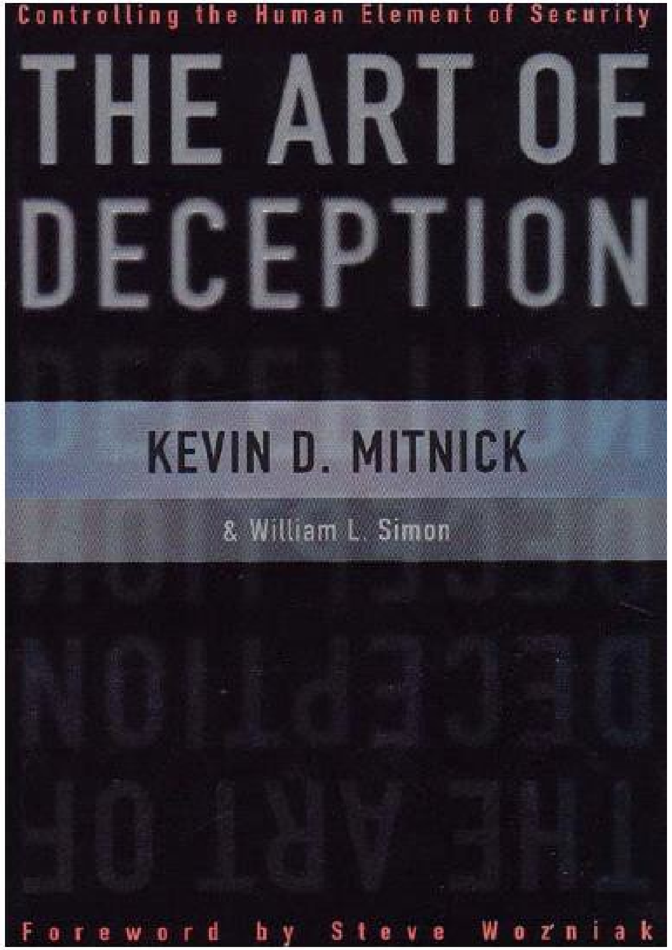
- A great deal of hacker tools are available:
  - Netcat: Netcat is a featured networking utility that reads and writes data across network connections using the TCP/IP protocol.
  - Microsoft EPDump and Remote Procedure Call (RPC) Dump: These tools provide information about Microsoft RPC services on a server:
    - The Microsoft EPDump application shows what is running and waiting on dynamically assigned ports.
    - The RPC Dump (rpcdump.exe) application is a command-line tool that queries RPC endpoints for status and other information on RPC.
  - GetMAC: This application provides a quick way to find the MAC (Ethernet) layer address and binding order for a computer running Microsoft Windows 2000 locally or across a network.
  - Software development kits (SDKs): SDKs provide hackers with the basic tools that they need to learn more about systems.

# Step 3 - Manipulate Users to Gain Access

- Even with the most sophisticated security in place, a company is still vulnerable because of securities weakest link: People!
- The first thing that hackers need is a password and there are two ways to get that password:
  - Social engineering
  - Password cracking attacks

# Step 3 - Manipulate Users to Gain Access

- Social engineering is a way to manipulate people inside the network to provide the information needed to access the network.
  - A computer is not required!!
  - Social engineering by telephone
  - Dumpster diving
  - Reverse social engineering
- Recommended reading:
  - “The Art of Deception: Controlling the Human Element of Security”
  - Mitnik, KD and Simon, WL; Wiley; New Ed edition


Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN D. MITNICK
& William L. Simon
Foreword by Steve Wozniak

# Social Engineering Example #1

- Call in the middle of the night:
  - **‘Hi this is _______from Bell. I’m very sorry to wake you up but we’ve noticed some very unusual activity on your Bell calling card and we’re wondering if you’re using it to call Baghdad, Iraq for the last 6 hours?’**
  - **‘Well, we have a call that’s actually still active right now and it’s now well over $2,000 worth of charges. I’ll terminate that call right now but unfortunately you are responsible for the charges made on your card.’**
  - **‘Look I sympathize with you and can see that you’ve been victimized here, but if I get rid of that charge I can loose my job.’**
  - **‘Okay … but you’ll have to confirm some details first. What is your full name and address?’**
  - **‘Can you confirm the Bell calling card number?’**
  - **‘Finally, please confirm your PIN number?’**
  - **‘Great. Everything matches. I’ll get rid of that charge for you.’**
  - **‘You’re welcome and thank you for being a Bell Canada client.’**

# Social Engineering Example #2

- **The facilitator of a live Computer Security Institute neatly illustrated the vulnerability of help desks when he “dialed up” a phone company, got transferred around, and reached the help desk:**
  - ‘Who’s the supervisor on duty tonight?’
  - ‘Let me talk to ______.’     (he’s transferred)
  - ‘Hi ______, this is ______from security in the IT center. Having a bad day?’
  - ‘No, why?...Your systems are down.’
    - Response: ‘my systems aren’t down, we’re running fine.’
  - ‘Hmmm … Really? Do me a favor then and sign off and on again.’
  - ‘We didn’t even show a blip, we show no change. Sign off again.’
  - ‘There’s something funny going on here. I’m going to have to sign on with your ID to figure out what’s happening. Let me have your user ID and password.’

# Other Social Engineering Examples

- A confused and befuddled person will call a clerk and meekly request a password change.

- People identifying themselves as executives, will telephone a new system administrator and demand access to their account IMMEDIATELY!

- Somebody will call and confidently instruct a computer operator to type in a few lines of instruction at the console.

- At an airport, somebody will look over a shoulder, ‘shoulder surfing,’ (sometimes even using binoculars or camcorders) as telephone credit card numbers or ATM PINs are keyed.

# Common Social Engineering Methods

•Posing as a fellow employee, as an employee of a vendor, partner company, or law enforcement, as someone in authority, as a new employee requesting help, as a vendor or systems manufacturer calling to offer a system patch or update.

•Offering help if a problem occurs, then making the problem occur, thereby manipulating the victim to call them for help.

•Sending free software or patch for victim to install.

•Sending a virus or Trojan Horse as an email attachment.

•Using a false pop-up window asking user to log in again or sign on with password.

•Leaving a USB stick, or CD around the workplace with malicious software on it.

# Common Social Engineering Methods

- Using insider lingo and terminology to gain trust.
- Offering a prize for registering at a Web site with username and password.
- Dropping a document or file at company mail room for intra-office delivery.
- Modifying fax machine heading to appear to come from an internal location.
- Asking receptionist to receive then forward a fax.
- Asking for a file to be transferred to an apparently internal location.
- Getting a voice mailbox set up so call backs perceive attacker as internal.
- Pretending to be from remote office and asking for email access locally.

# Warning Signs of an Attack

- Refusal to give call back number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens negative consequences of non compliance
- Shows discomfort when questioned
- Name dropping
- Compliments or flattery
- Flirting

# Password Cracking

- Hackers use many tools and techniques to crack passwords:
  - Word lists
  - Brute force
  - Hybrids
  - The yellow Post-It stuck on the side of the monitor, or in top of desk drawer

# Password Cracking

- Password cracking attacks any application or service that accepts user authentication, including those listed here:
  - NetBIOS over TCP (TCP 139)
  - Direct host (TCP 445)
  - FTP (TCP 21)
  - Telnet (TCP 23)
  - SNMP (UDP 161)
  - PPTP (TCP 1723)
  - Terminal services (TCP 3389)

# Step 4 - Escalate Privileges

- After securing a password for a user account and user-level privileges to a host, hackers attempt to escalate their privileges.

- The hacker will review all the information he or she can see on the host:
  - Files containing user names and passwords

  - Registry keys containing application or user passwords

  - Any available documentation (for example, e-mail)

- If the host cannot be seen by the hacker, the hacker may launch a Trojan application such as W32/QAZ to provide it.

# Step 5 – Gather Passwords and Secrets

- Hackers target:
  - The local security accounts manager database
  - The active directory of a domain controller
- Hackers can use legitimate tools including pwdump and lsadump applications.
- Hackers gain administrative access to all computers by cross-referencing user names and password combinations.

# Step 6 - Install Back Doors and Port Redirectors

- Back doors:
  - Provide a way back into the system if the front door is locked.
  - The way into the system that is not likely to be detected.
- Back doors may use reverse trafficking:
  - Example: Code Red which used TCP port 80 to instruct unpatched web servers to execute a TFTP connection from the server.
- Port redirectors:
  - Port redirectors can help bypass port filters, routers, and firewalls and may even be encrypted over an SSL tunnel to evade intrusion detection devices.

# Step 7 - Leverage the Compromised System

•Back doors and port redirectors let hackers attack other systems in the network.

•Reverse trafficking lets hackers bypass security mechanisms.

•Trojans let hackers execute commands undetected.

•Scanning and exploiting the network can be automated.

•The hacker remains behind the cover of a valid administrator account.

•The whole seven-step process is repeated as the hacker continues to penetrate the network.

# Best Practices to Defeat Hackers

- Keep patches up to date
- Shut down unnecessary services and ports.
- Use strong passwords and change them often.
- Control physical access to systems.
- Avoid unnecessary web page inputs.
    - Some websites allow users to enter usernames and passwords.
    - A hacker can enter more than just a username and programmers should limit input characters and not accept invalid characters (| ; < >).

# Best Practices to Defeat Hackers

- Perform system backups and test them on a regular basis.
- Educate users about social engineering.
- Encrypt and password-protect sensitive data.
- Use appropriate security hardware and software.
- Develop a written security policy for the company.

# Securing the Management Plane

- Implement a login and password policy to restrict device accessibility.
- Present legal notification developed by legal counsel of a corporation.
- Ensure the confidentiality of data by using management protocols with strong authentication.
- Use role-based access control (RBAC) to ensure that access is only granted to authenticated users, groups, and services.
- Restrict the actions and views that are permitted by any particular user, group, or service.
- Enable management access reporting to log and account for all access.

# Securing the Data Plane

- Use ACLs to perform packet filtering. ACLs can be used to:
  - Block unwanted traffic or users.
  - Reduce the change of a DoS attack.
  - Mitigate spoofing attacks.
  - Provide bandwidth control.
  - Classify traffic to protect the management and control planes.
- Implement Layer 2 security using:
  - Port security
  - DHCP snooping
  - Dynamic ARP Inspection (DAI)