Chapter 1: Modern Network Security Threats

CCNA Security

Cisco | Networking Academy®
Mind Wide Open™

Chapter 1: Objectives

In this chapter you will:

- Describe the evolution of network security.
- Describe the various drivers for network security technologies and applications.
- Describe the major organizations responsible for enhancing network security.
- Describe a collection of domains for network security.
- Describe network security policies.
- Describe computer network viruses.
- Describe computer network worms.
- Describe computer network Trojan Horses.
- Describe the techniques used to mitigate viruses, worms, and Trojan Horses.
- Explain how reconnaissance attacks are launched.
- Explain how access attacks are launched.
- Explain how Denial of Service attacks are launched.
- Describe the techniques used to mitigate reconnaissance attacks, access attacks, and DoS attacks.
- Explain how to secure the three functional areas of Cisco routers and switches.

Chapter 1

1.0 Introduction

1.1 Fundamental Principles of a Secure Network

1.2 Viruses, Worms, and Trojan Horses

1.3 Attack Methodologies

1.4 Cisco Network Foundation Protection Framework

1.5 Summary

1.1 Fundamentals of a Secure Network

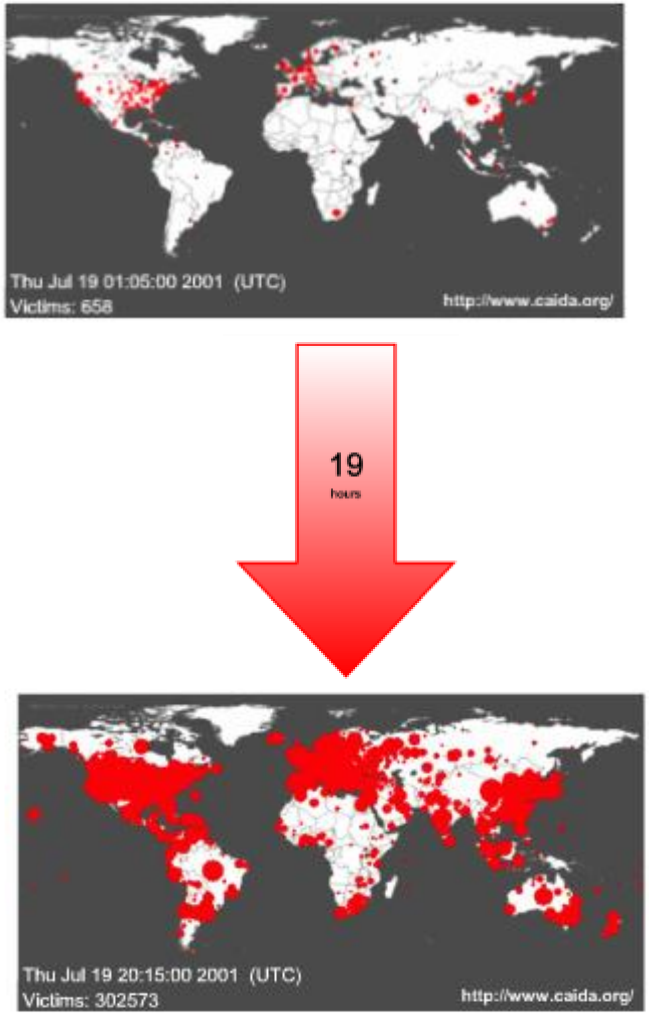
Cisco | Networking Academy®
Mind Wide Open™

Evolution of Network Security

Code Red Worm Attack

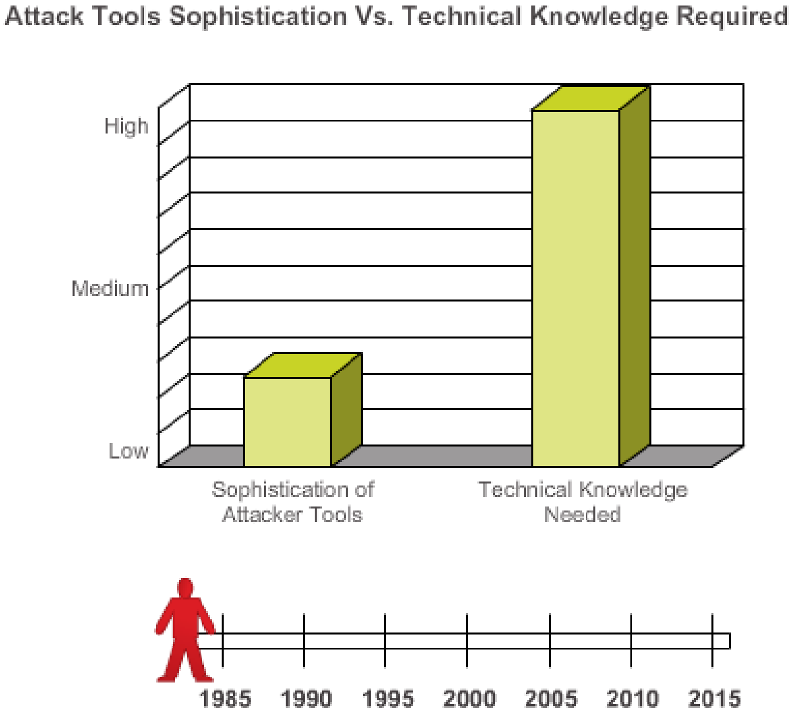
What is “Code Red”?

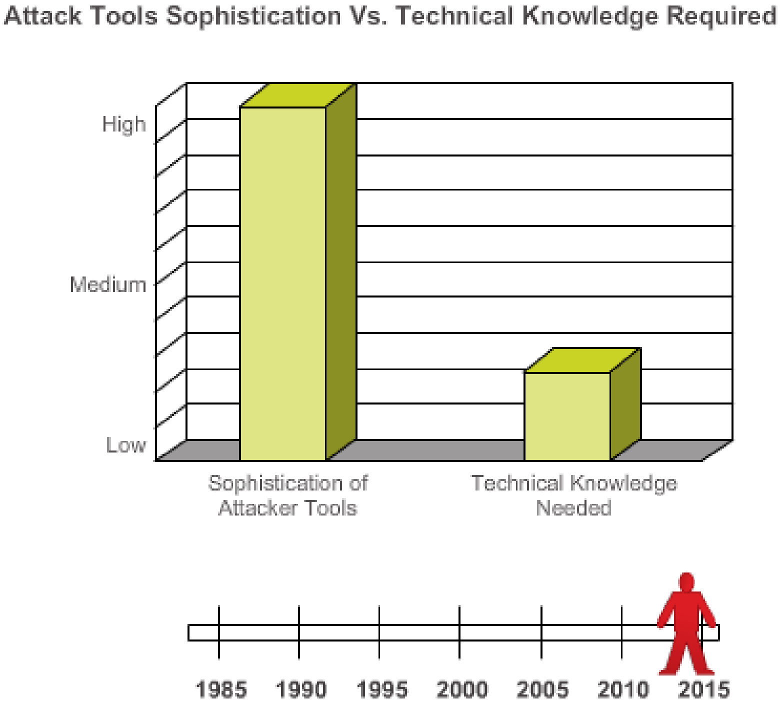
The Code Red worm was a DoS attack and was released on July 19, 2001 and attacked web servers globally, infecting over 350,000 hosts and in turn affected millions of users.



Evolution of Security Threats

- The early users of the Internet did not spend much time thinking about whether or not their online activities presented a threat to the network or to their own data.
- Today, the Internet is a very different network compared to its beginnings.
- More people rely on the network for their personal, financial, and business needs.





Evolution of Network Security

Evolution of Network Security Tools

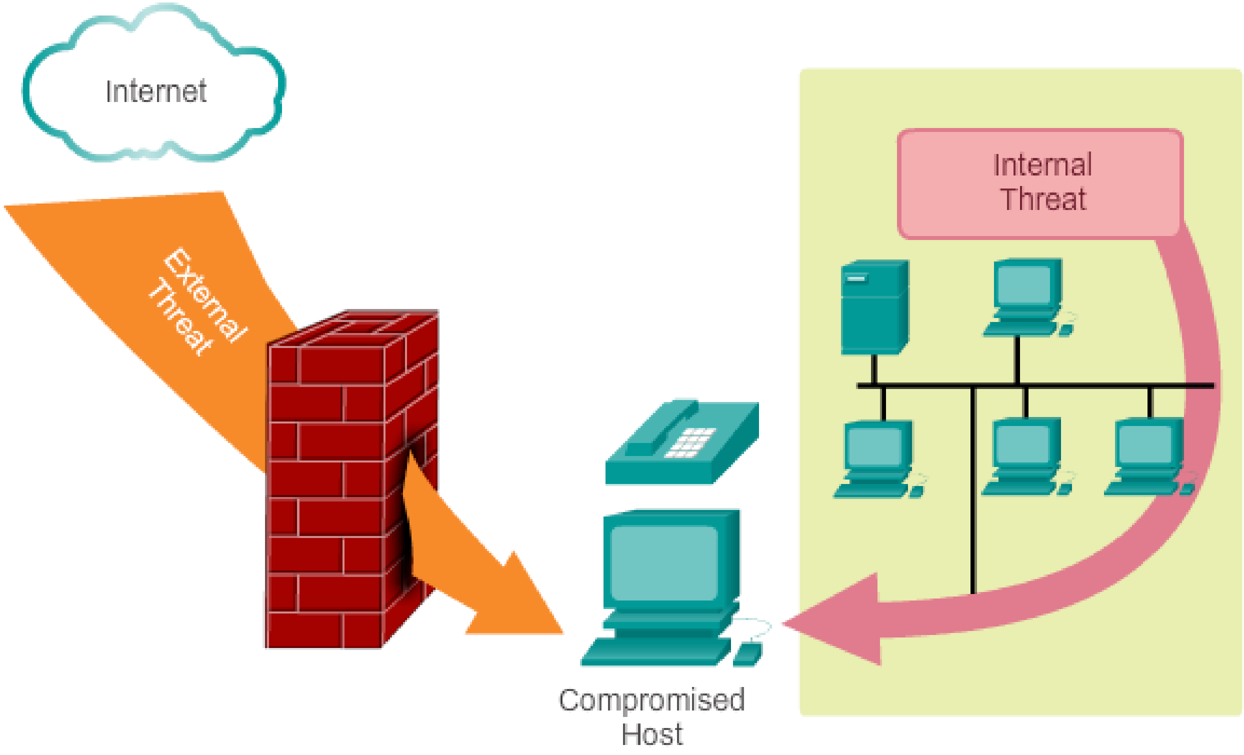
- 1988 – DEC Packet Filter Firewall
- 1989 – AT&T Bell Labs Stateful Firewall
- 1991 – DEC SEAL Application Layer Firewall
- 1994 – Check Point Firewall
- 1995 – NetRanger IDS
- 1997 – RealSecure IDS
- 1998 – Snort IDS
- 1999 – First IPS
- 2006 – Cisco Zone-Based Policy Firewall
- 2010 – Evolution of Network Security Tools

Evolution of Network Security

Threats to Networks

- Network attack vectors include:
  - **Internal threats**
  - **External threats**
- The attacks can be structured or unstructured.

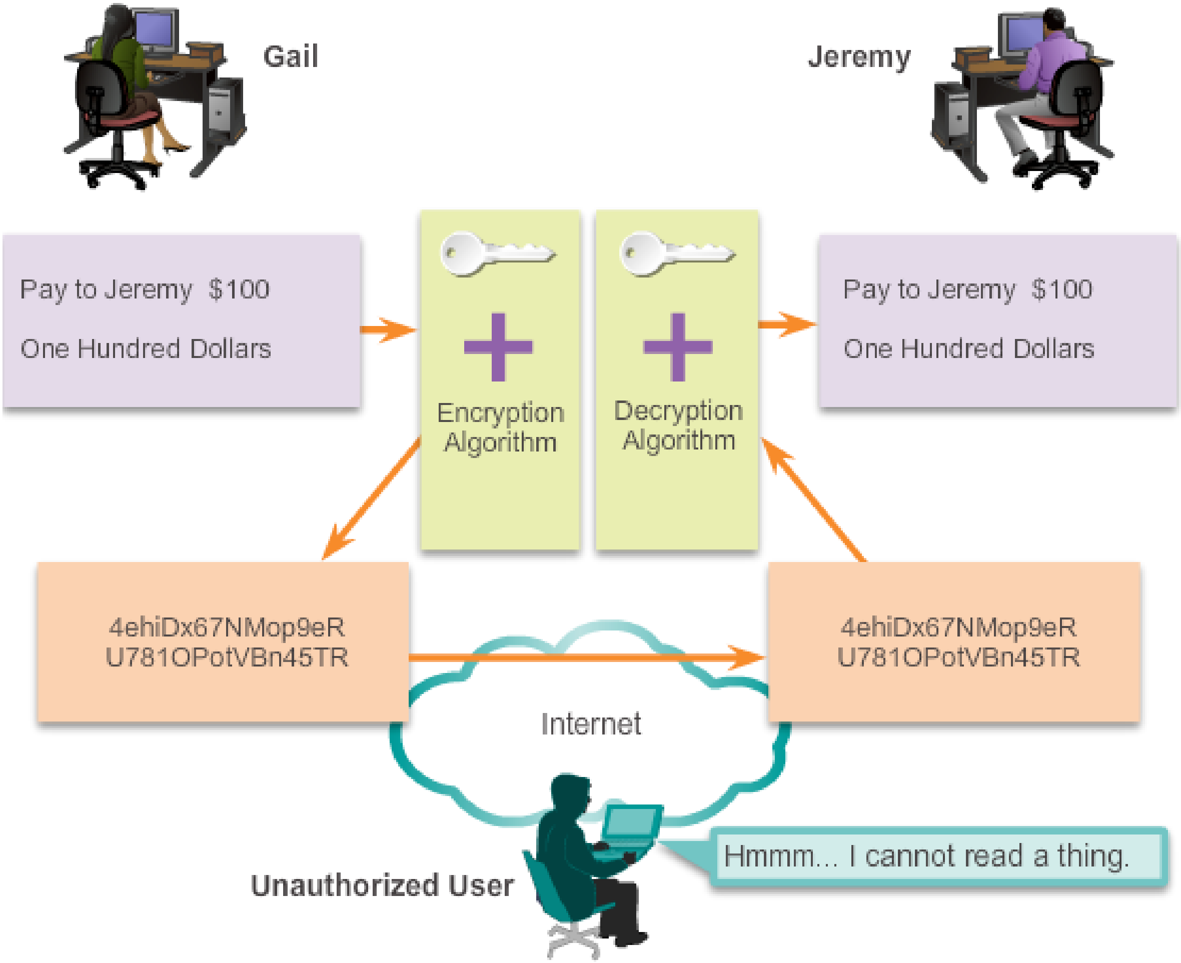
Threats to Networks



Evolution of Network Security

Encryption and Cryptography

Cryptography is the study and practice of hiding information, and is used pervasively in modern network security.



Evolution of Network Security

Evolution of Data Protection Technologies

- 1993 – Cisco GRE Tunnels
- 1996 – Site-to-Site VPNs
- 1999 – SSH
- 2000 – MPLS VPNs
- 2001 – Remote-Access IPsec VPN
- 2002 – Dynamic Multipoint VPN
- 2005 – SSL VPN
- 2009 – Group Encrypted Transport VPN (GET VPN)

Drivers for Network Security

The Hacker

- **Defining the word "Hacker"**
  - General term that has historically been used to describe a computer programming expert.
  - Internet programmers who try to gain unauthorized access to devices on the Internet.
  - Individuals who run programs to prevent or slow network access to a large number of users, or corrupt or wipe out data on servers.

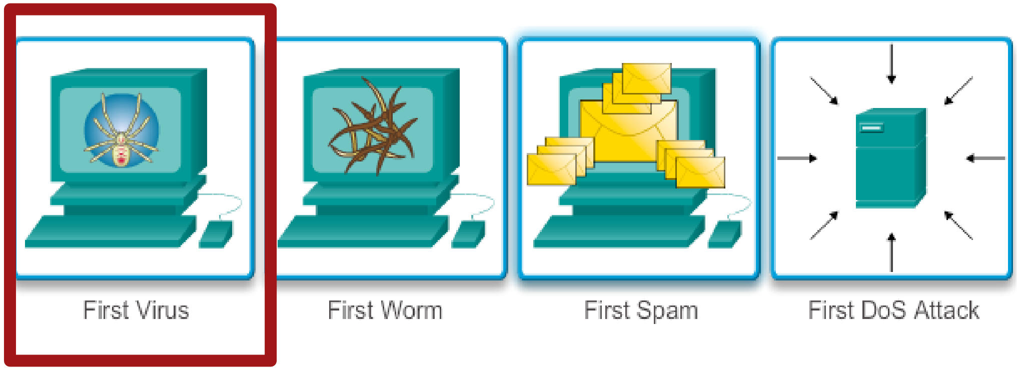
Drivers for Network Security

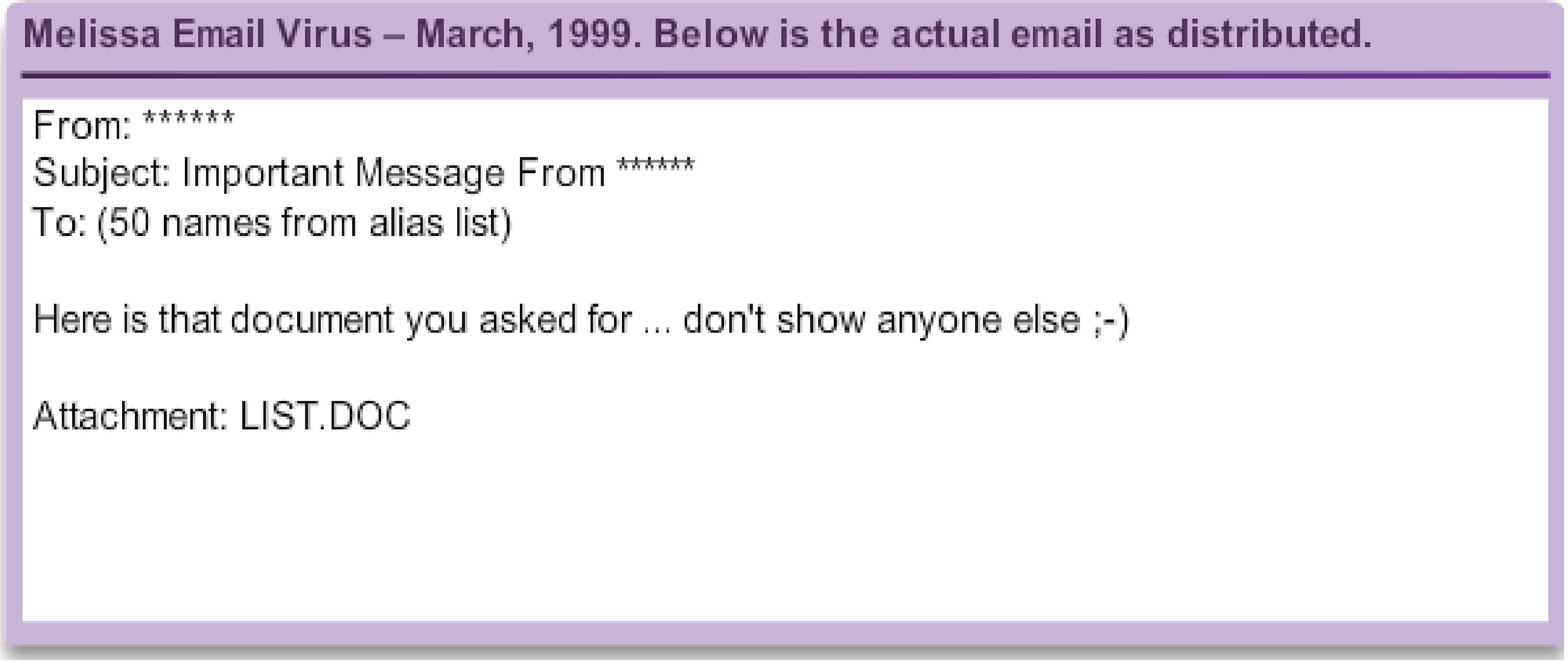
Evolution of Hacking

- 1960s – Phone freaks
- 1980s – Wardialing
- 1988 – First Internet worm
- 1993 – First Def Con hacking conference
- 1995 – First 5 year federal prison sentence for hacking
- 1995 – Kevin Mitnick sentenced to 4 years in prison for hacking cred card accounts.
- 1995 – SATAN released
- 1997 – Nmap released
- 1997 – First malicious scripts (script kiddies) and used by less education hackers
- 1998 – Wardriving
- 2002 – Melissa virus creator gets 20 months in jail
- 2006 – Vishing, smishing
- 2009 – First malicious iPhone worm
- 2011 – Script kiddies hacked NBC News Twitter account posting fake updates

Drivers for Network Security

First Network Attacks




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

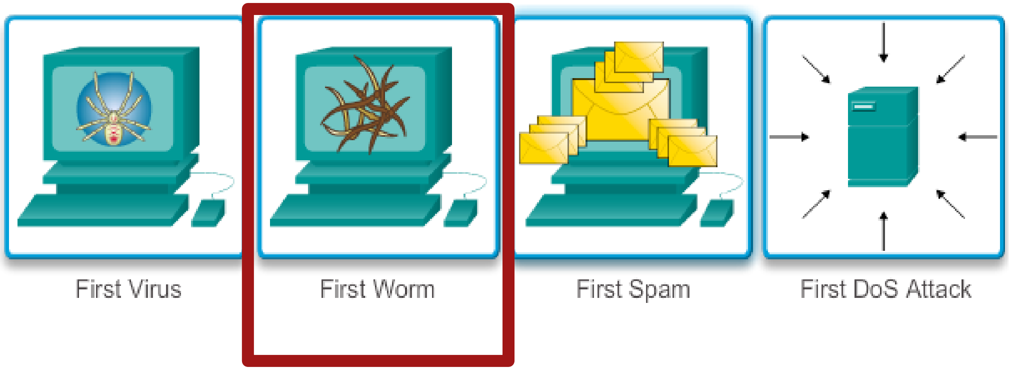
From: ******
Subject: Important Message From ******
To: (50 names from alias list)

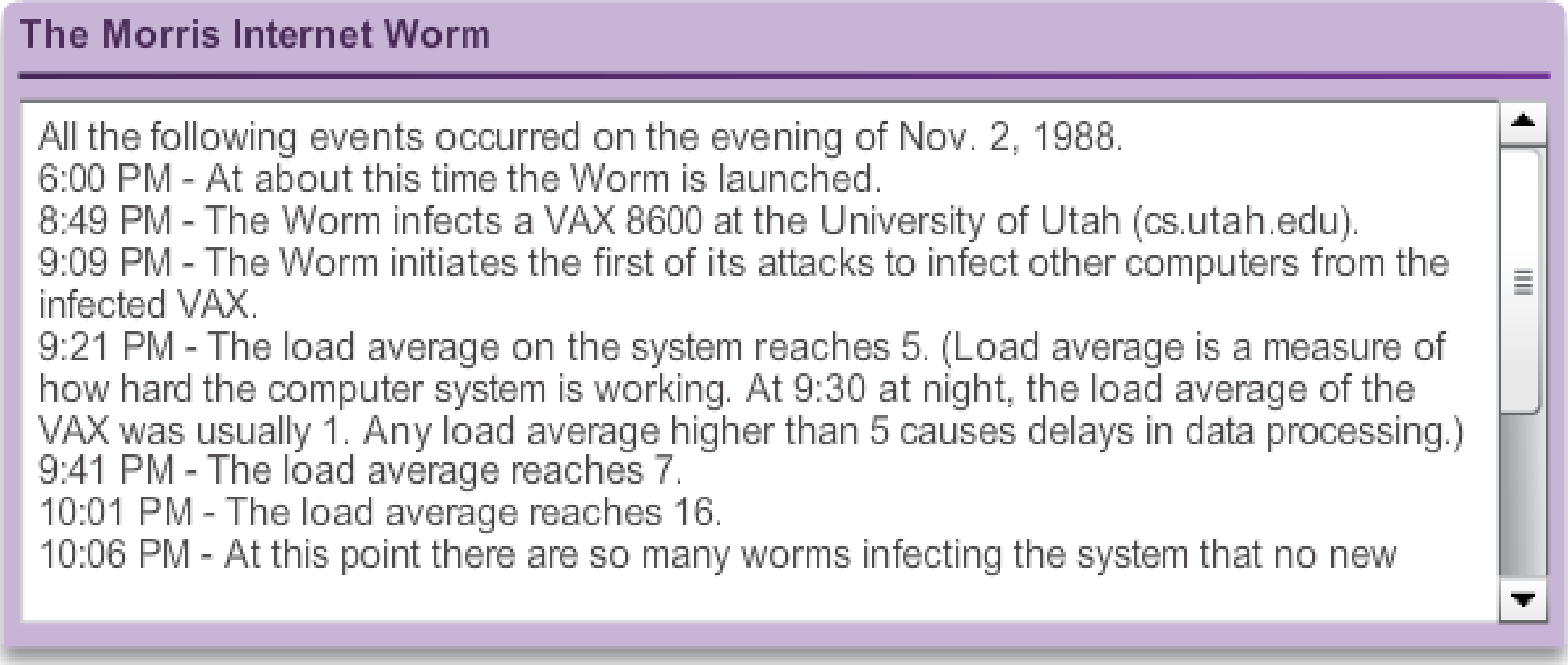
Here is that document you asked for ... don't show anyone else ;-)

Attachment: LIST.DOC

Drivers for Network Security

First Network Attacks Cont.



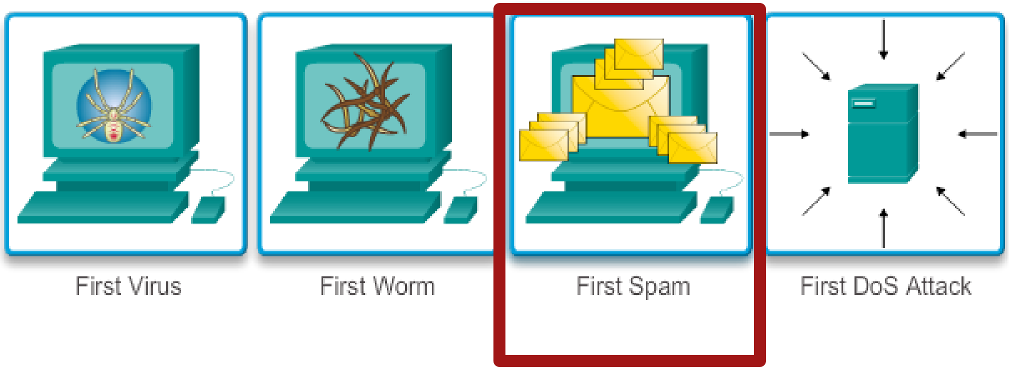


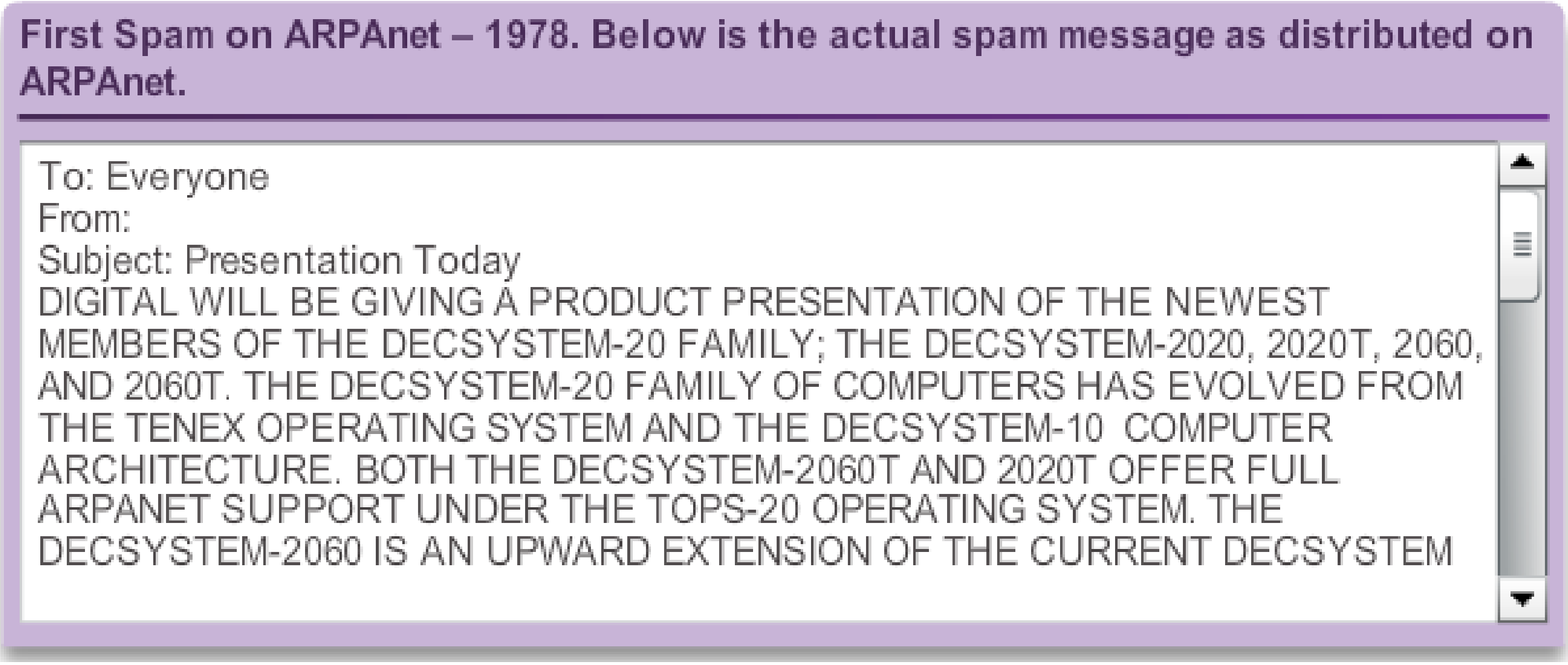
The Morris Internet Worm

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

Drivers for Network Security

First Network Attacks Cont.





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

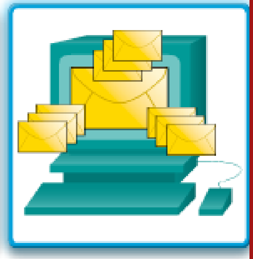
To: Everyone
From:
Subject: Presentation Today
DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM AND THE DECSYSTEM-10 COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM. THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM

Drivers for Network Security

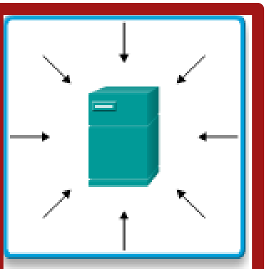
First Network Attacks Cont.

First Virus

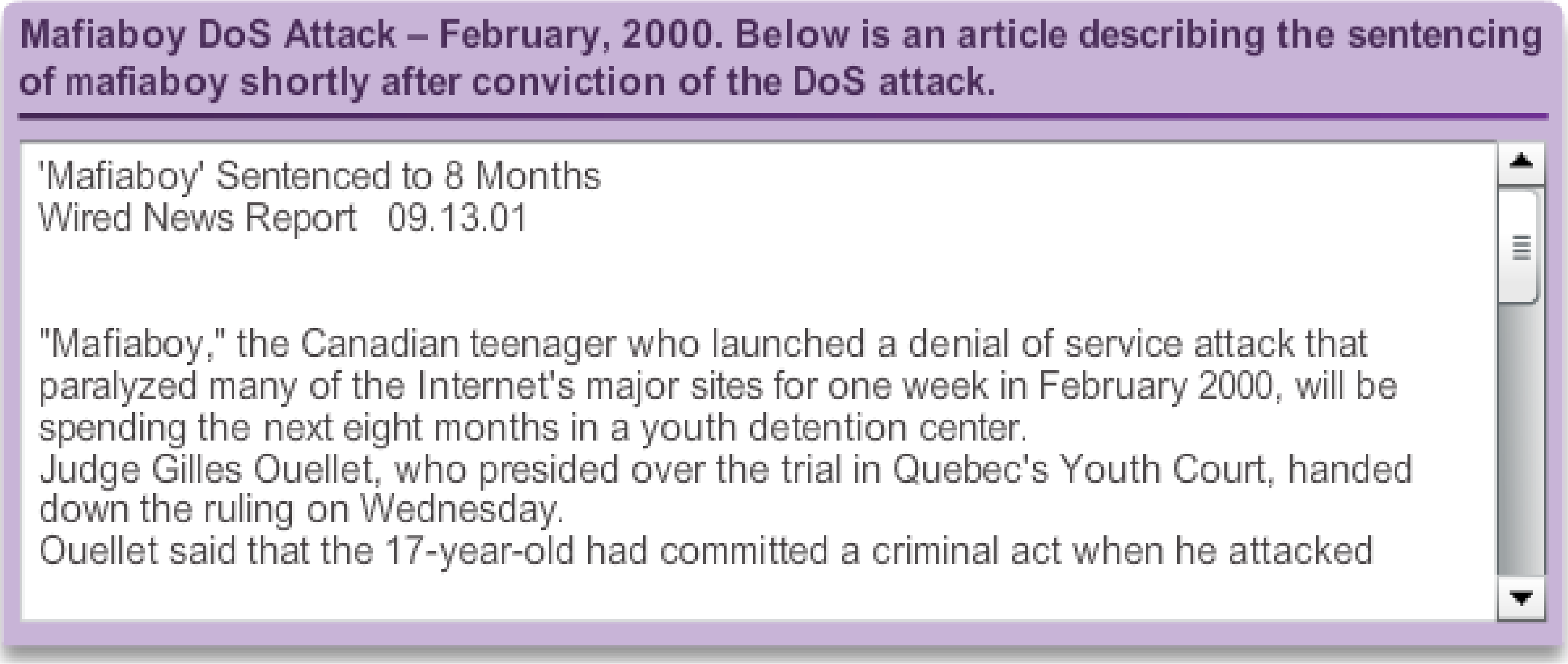
First Worm



First Spam



First DoS Attack



Mafiaboy DoS Attack – February, 2000. Below is an article describing the sentencing of mafiaboy shortly after conviction of the DoS attack.

'Mafiaboy' Sentenced to 8 Months
Wired News Report 09.13.01

"Mafiaboy," the Canadian teenager who launched a denial of service attack that paralyzed many of the Internet's major sites for one week in February 2000, will be spending the next eight months in a youth detention center.
Judge Gilles Ouellet, who presided over the trial in Quebec's Youth Court, handed down the ruling on Wednesday.
Ouellet said that the 17-year-old had committed a criminal act when he attacked

Drivers for Network Security

Network Security Professionals

Network Security Engineer

Information Security Analyst

Network Security Specialist

Network Security Administrator

Network Security Architect

Systems Engineer

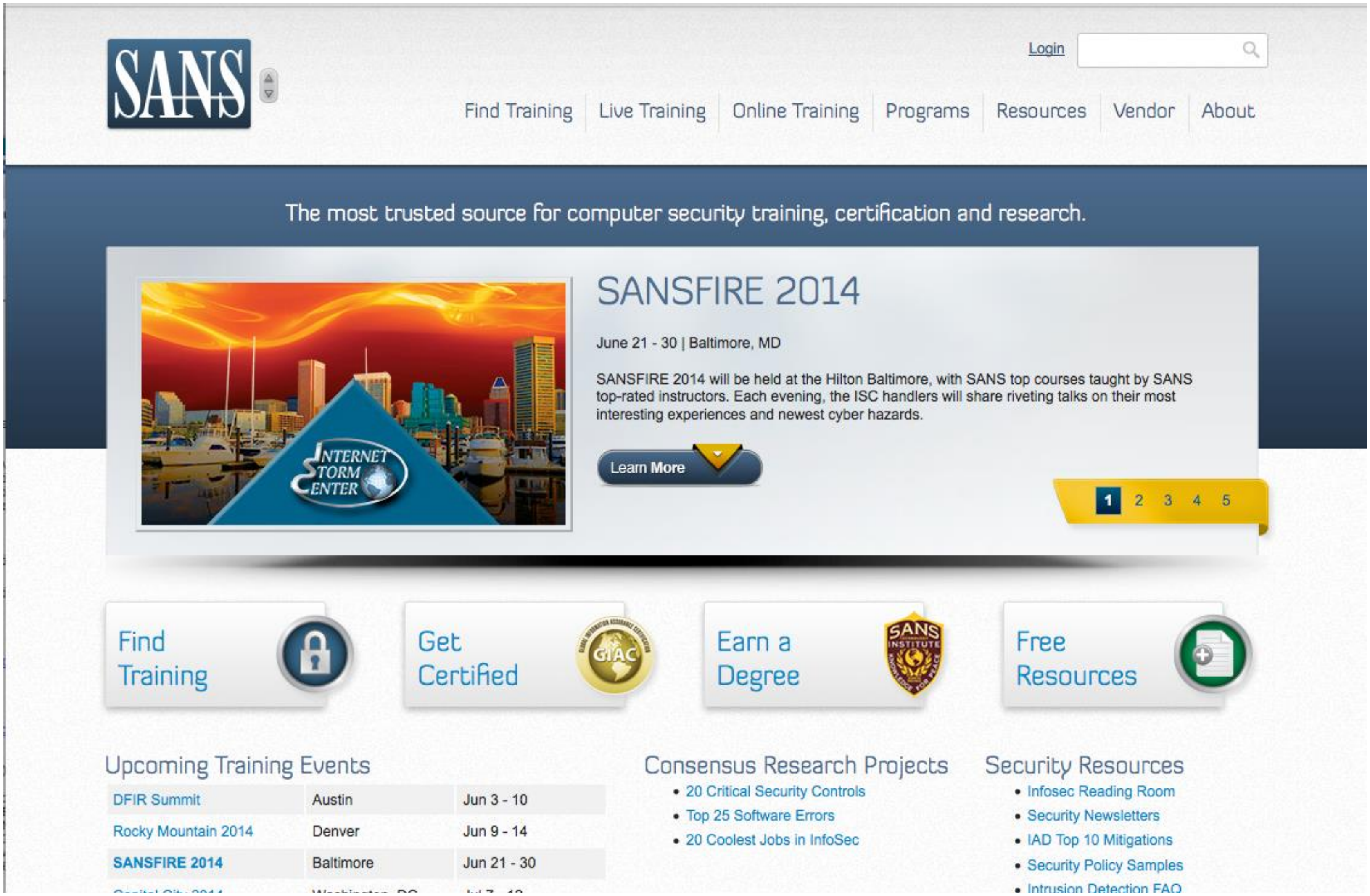
Network Security Organizations

FIRST Forum of Incident Response and Security Teams
www.first.org
MITRE
www.mitre.org
CERT
www.cert.org
SANS
www.sans.org
INFOSYSSEC Information System Security
www.infosyssec.com
the CENTER for INTERNET SECURITY
www.cisecurity.org
(ISC)² SECURITY TRANSCENDS TECHNOLOGY
www.isc2.org

- 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 Organizations

SANS Institute



The most trusted source for computer security training, certification and research.

SANSFIRE 2014

June 21 - 30 | Baltimore, MD

SANSFIRE 2014 will be held at the Hilton Baltimore, with SANS top courses taught by SANS top-rated instructors. Each evening, the ISC handlers will share riveting talks on their most interesting experiences and newest cyber hazards.

Upcoming Training Events

DFIR Summit	Austin	Jun 3 - 10
Rocky Mountain 2014	Denver	Jun 9 - 14
SANSFIRE 2014	Baltimore	Jun 21 - 30
Capital City 2014	Washington, DC	Jul 7 - 12

Consensus Research Projects

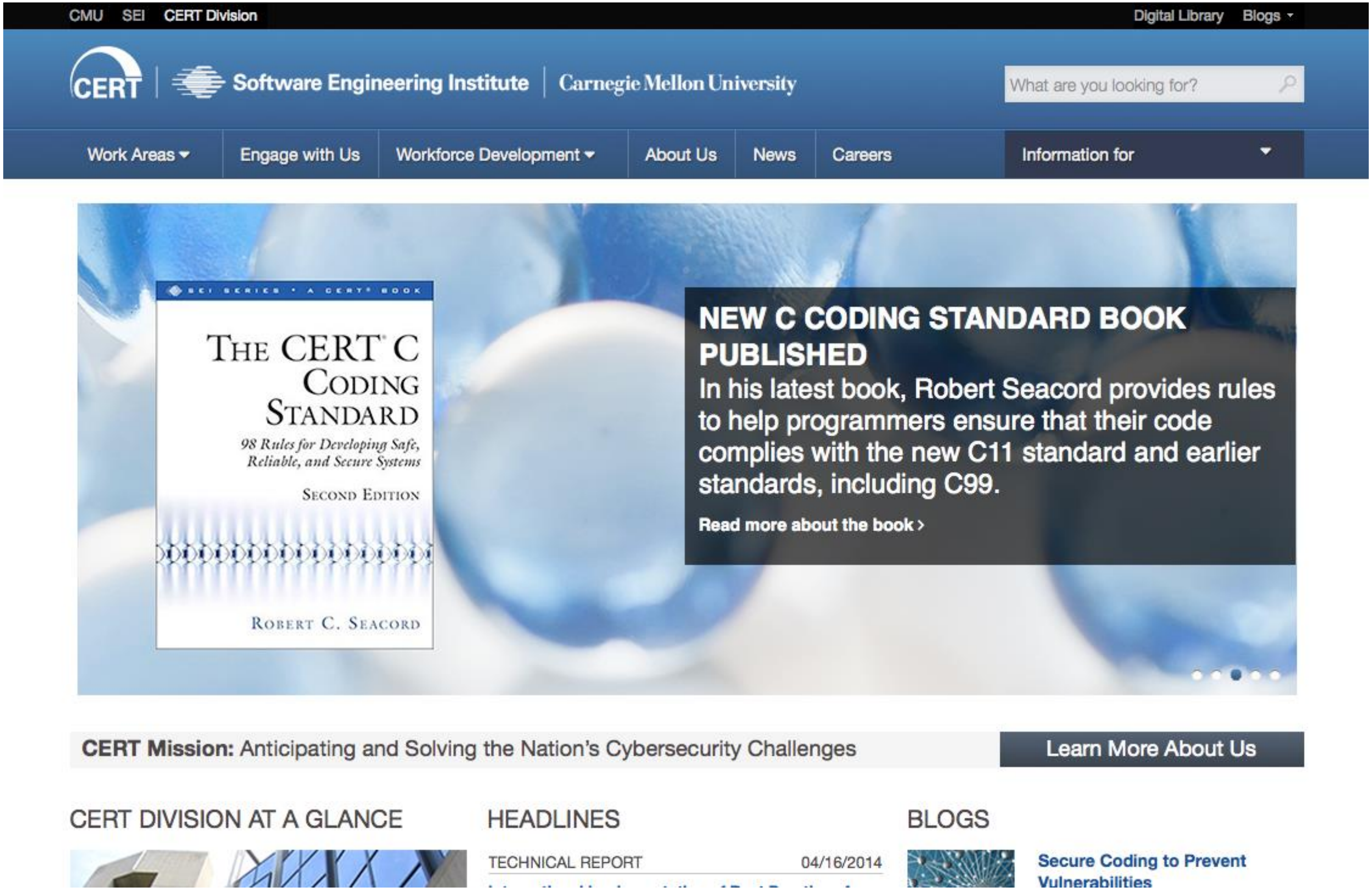
- 20 Critical Security Controls
- Top 25 Software Errors
- 20 Coolest Jobs in InfoSec

Security Resources

- Infosec Reading Room
- Security Newsletters
- IAD Top 10 Mitigations
- Security Policy Samples
- Intrusion Detection FAQ

Network Security Organizations

CERT



CMU
SEI
CERT Division
Digital Library
Blogs
CERT
Software Engineering Institute
Carnegie Mellon University
What are you looking for?
Work Areas
Engage with Us
Workforce Development
About Us
News
Careers
Information for
SEI SERIES · A CERT® BOOK
THE CERT® C CODING STANDARD
98 Rules for Developing Safe, Reliable, and Secure Systems
SECOND EDITION
ROBERT C. SEACORD

NEW C CODING STANDARD BOOK PUBLISHED

In his latest book, Robert Seacord provides rules to help programmers ensure that their code complies with the new C11 standard and earlier standards, including C99.

Read more about the book ›

CERT Mission: Anticipating and Solving the Nation's Cybersecurity Challenges

Learn More About Us

CERT DIVISION AT A GLANCE

HEADLINES

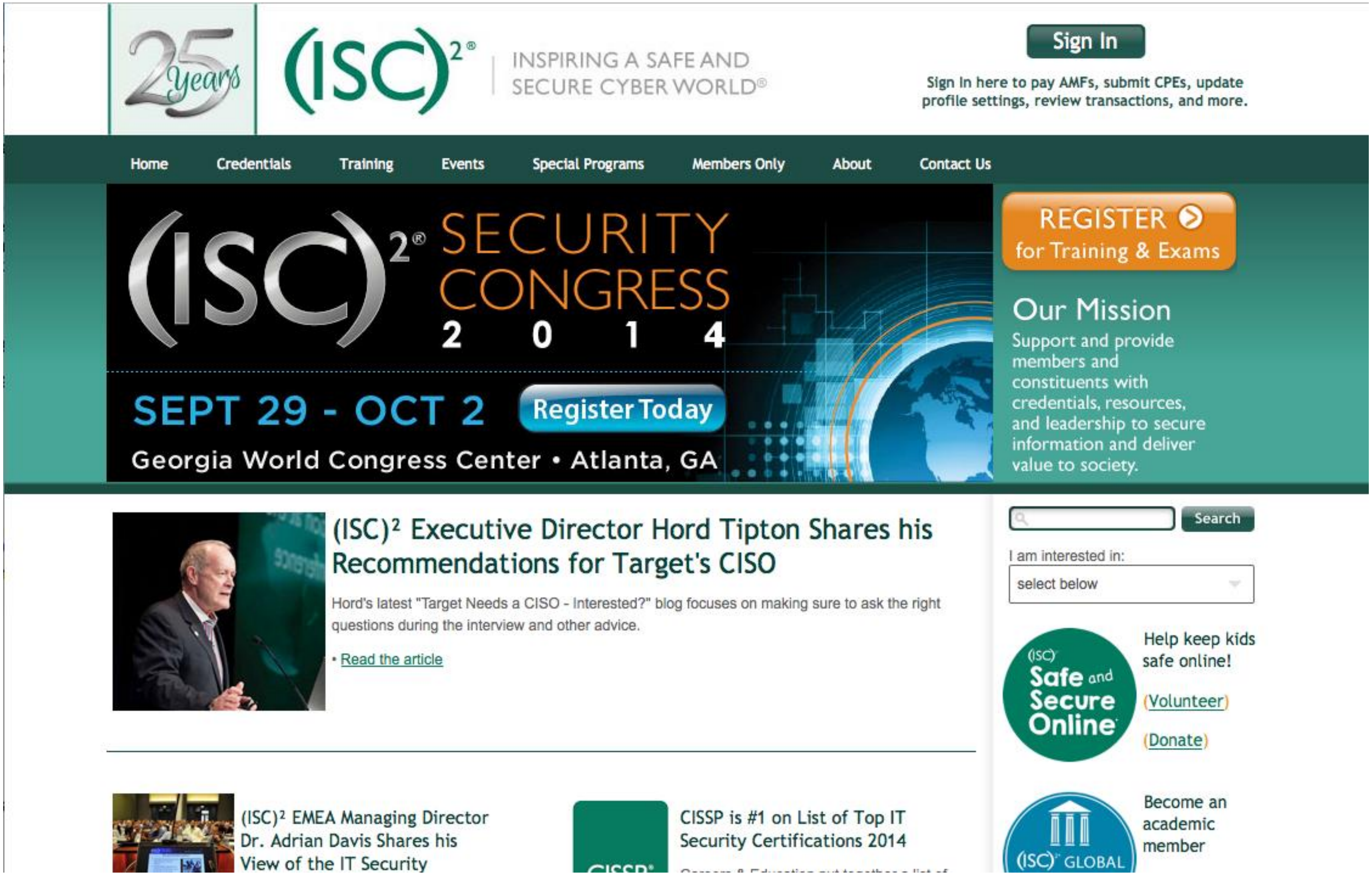
TECHNICAL REPORT 04/16/2014

BLOGS

Secure Coding to Prevent Vulnerabilities

Network Security Organizations

CERT Cont.



(ISC)² ®

INSPIRING A SAFE AND SECURE CYBER WORLD®

Sign In

Sign In here to pay AMFs, submit CPEs, update profile settings, review transactions, and more.

(ISC)² ® SECURITY CONGRESS 2 0 1 4

SEPT 29 - OCT 2

Register Today

Georgia World Congress Center • Atlanta, GA

REGISTER for Training & Exams

Our Mission

Support and provide members and constituents with credentials, resources, and leadership to secure information and deliver value to society.

(ISC)² Executive Director Hord Tipton Shares his Recommendations for Target's CISO

Hord's latest "Target Needs a CISO - Interested?" blog focuses on making sure to ask the right questions during the interview and other advice.

• Read the article

I am interested in:

select below

(ISC)² Safe and Secure Online

Help keep kids safe online!

(Volunteer)

(Donate)

Become an academic member

(ISC)² GLOBAL

(ISC)² EMEA Managing Director Dr. Adrian Davis Shares his View of the IT Security

CISSP®

CISSP is #1 on List of Top IT Security Certifications 2014

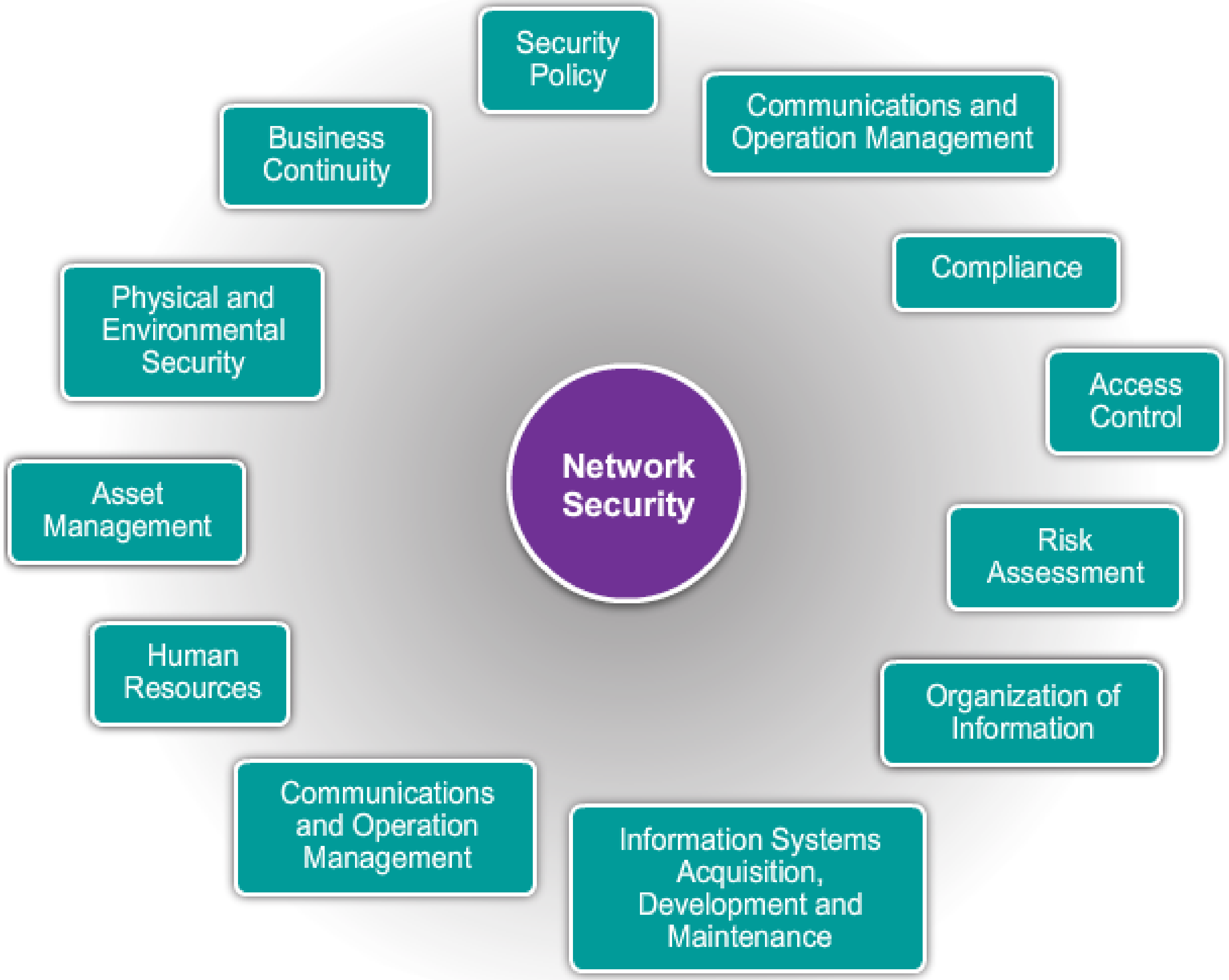
Network Security Organizations

US-CERT RSS Feed

- Really Simple Syndication (RSS) feeds provide a very useful tool for the network security professional.
- By subscribing to RSS security feeds, such as the one available from Cisco's SIO http://tools.cisco.com/security/center, you receive security notifications when new information is available.

Domains of Network Security

Network Security Domains


Network Security

Security Policy

Communications and Operation Management

Compliance

Access Control

Risk Assessment

Organization of Information

Information Systems Acquisition, Development and Maintenance

Communications and Operation Management

Human Resources

Asset Management

Physical and Environmental Security

Business Continuity

Domains of Network Security

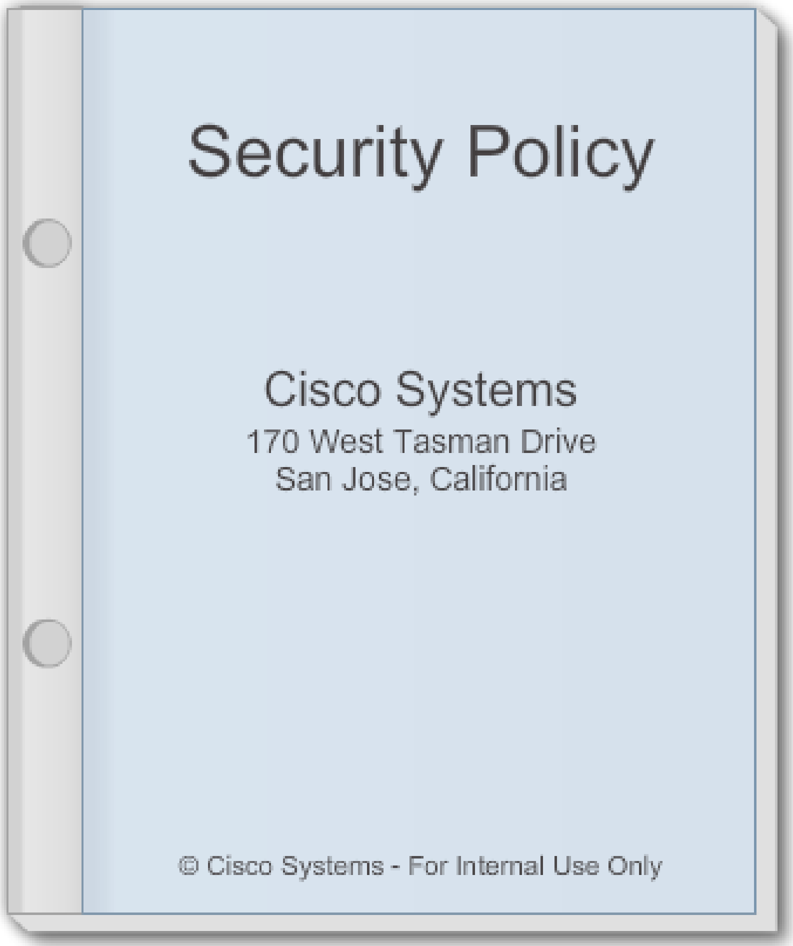
Network Security Domains Cont.

- 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

Security Policy

- One of the most important domains is the security policy domain.
- A security policy is a formal statement of the rules by which people must abide who are given access to the technology and information assets of an organization.



Security Policy

Cisco Systems
170 West Tasman Drive
San Jose, California

© Cisco Systems - For Internal Use Only

Network Security Policies

Network Security Policy

The network security policy outlines rules for network access, determines how policies are enforced, and describes the basic architecture of the organization’s network security environment.

The next item on the security policy that we need to discuss is the rules for network access.
We must keep in mind that we have remote workers. They will have different access rules than our onsite employees.

Network Security Policies

Cisco SecureX

- The Cisco SecureX architecture is designed to provide effective security for any user, using any device, from any location, and at any time.
- Security architecture uses a higher-level policy language that takes into account the full context of a situation the who, what, where, when, and how.
- With highly distributed security policy enforcement, security is pushed closer to where the end user is working.

Network Security Policies

Cisco SecureX Architecture

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** – Defines the way the scanning engine is implemented in the network. It can be via a traditional network appliance, a module in a router or switch, or an image in a Cisco security cloud.
- **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.

Network Security Policies

Cisco SecureX Product Categories

Secure Edge and Branch

- **Cisco ASA 5500 Series Adaptive Security Appliance** - Combines firewall, VPN, optional content security, and intrusion prevention.
- **Cisco Intrusion Prevention System** - Identifies and stops malicious traffic, worms, viruses, and application abuse.
- **Integrated Security on the ISR G2** - Delivers firewall, intrusion prevention, VPN, and content filtering.

Network Security Policies

Cisco SecureX Product Categories Cont.

Secure Email and Web

- **Cisco IronPort Email Security Appliance** - Fights spam, viruses, and blended threats for organizations of all sizes.
- **Cisco IronPort Web Security Appliance** - Integrates web-usage controls, data security, reputation and malware filtering.
- **Cisco ScanSafe Cloud Web Security** - Analyzes web requests for malicious, inappropriate, or acceptable content.

Network Security Policies

Cisco SecureX Product Categories Cont.

Secure Access

- **Cisco Identity Services Engine** - Applies policy-based access control.
- **Network Admission Control Appliance** - Enforces network security policies by allowing access only to trusted devices.
- **Cisco Secure Access Control System** - Controls network access based on dynamic conditions and attributes.

Network Security Policies

Cisco SecureX Product Categories Cont.

Secure Mobilitiy

- **VPN Services for Cisco ASA Series** - Provides remote access for up to 10,000 SSL or true IPsec connections.
- **Cisco Adaptive Wireless IPS Software** - Provides automated wireless vulnerability and performance monitoring.
- **Cisco AnyConnect Secure Mobility Solutions** - Provides an intelligent, smooth, and reliable connectivity experience.

Network Security Policies

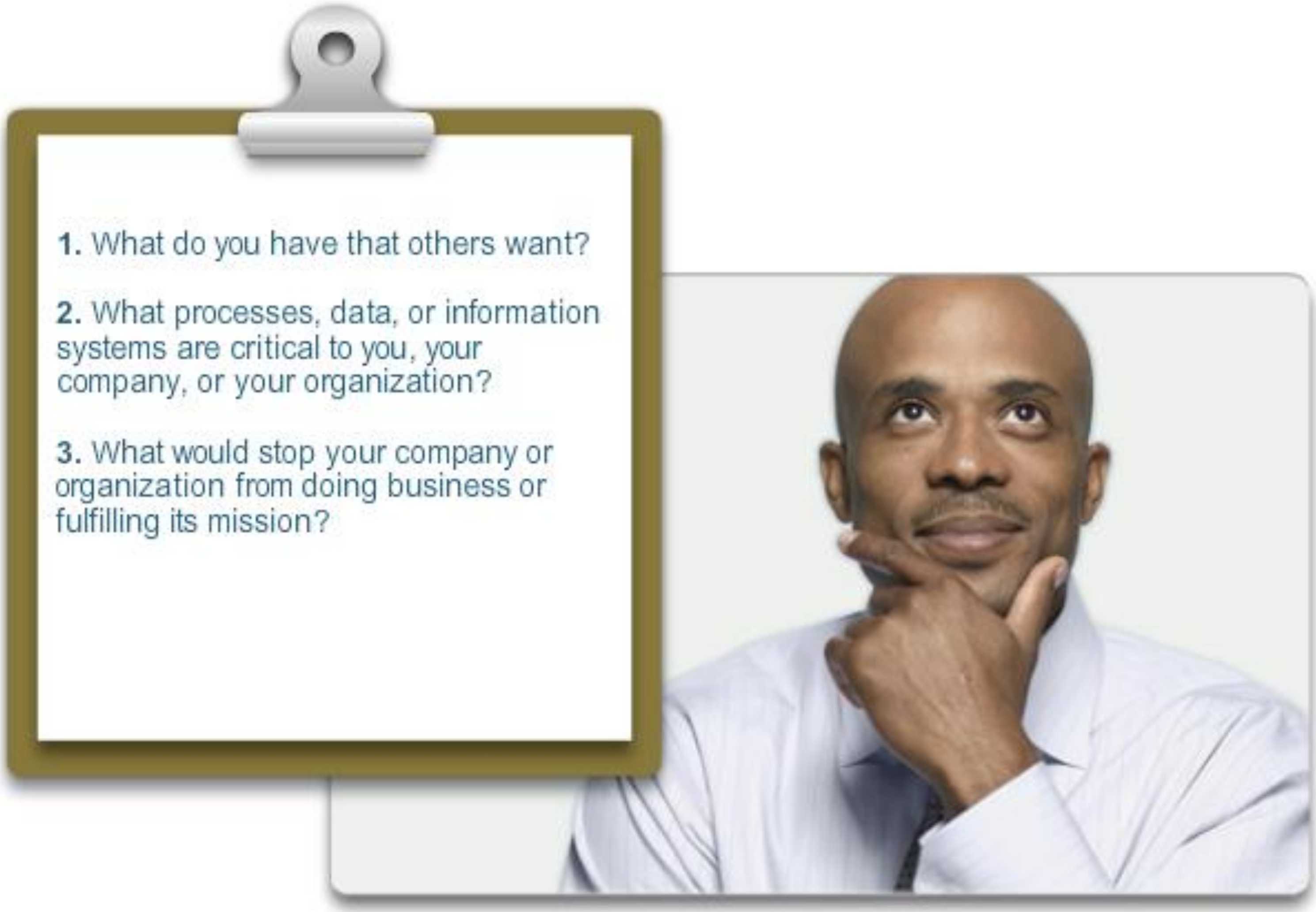
Cisco SecureX Product Categories Cont.

Secure Data Center

- **Cisco ASA 5585-X Adaptive Security Appliance** - Combines a proven firewall, comprehensive intrusion prevention, and VPN.
- **Cisco Catalyst 6500 ASA Services Module** - Combines full-featured switching with best-in-class security.
- **Cisco Virtual Security Gateway** - Integrates with Cisco Nexus 1000V virtual switch hypervisors.

Network Security Policies

Network Security Policy Objectives



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?

1.2 Viruses, Worms, and Trojan Horses

Cisco | Networking Academy®
Mind Wide Open™

Viruses

Primary Vulnerabilities for End User Devices

- 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

Comparison of a Human Virus and a Computer Virus

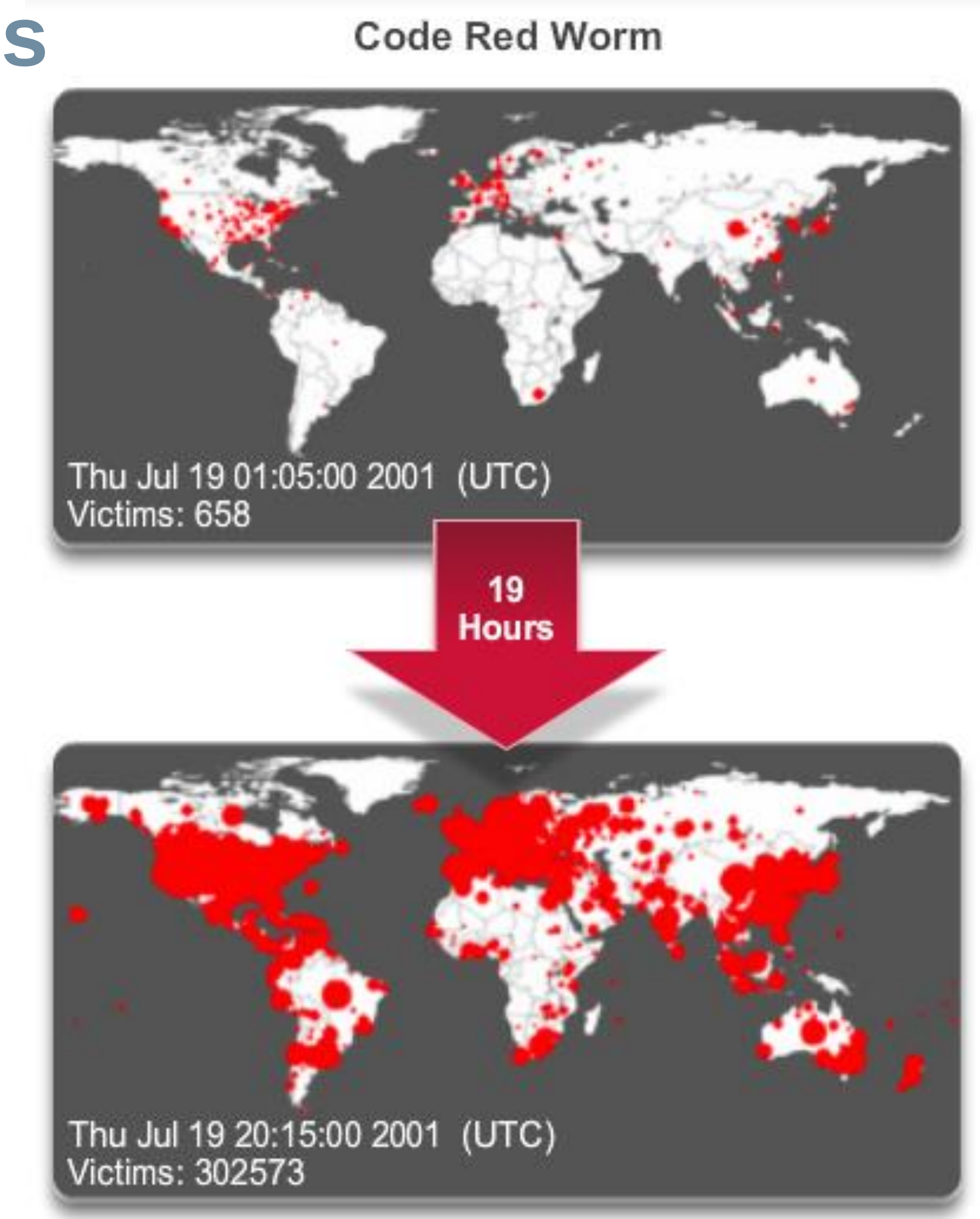
Human Virus

Computer Virus

Worms

Worms Characteristics

- 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 require user intervention, and can spread extremely fast over the network.


Code Red Worm
Thu Jul 19 01:05:00 2001 (UTC)
Victims: 658
19 Hours
Thu Jul 19 20:15:00 2001 (UTC)
Victims: 302573

Worms

Worm Components

- **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**
  - When 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.

Worm and Virus Exploit and Comparison

- **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.
- **Persist phase:**
  - After the attack is successfully launched in the memory, the code tries to persist on the target system.
  - The 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.

Worm and Virus Exploit and Comparison

- **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.

Trojan Horses

Trojan Horse Concept

- 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 can 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 Horses

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 antivirus programs or firewalls from functioning)
- **Security software disabler Trojan horse** - Stops antivirus programs or firewalls from functioning.
- **DoS Trojan Horse** - Slows or halts network activity

Mitigating Viruses, Worms, and Trojan Horses

Buffer Overflows

- **Buffer -** An allocated area of memory used by processes to store data temporarily.
- **Buffer overflow -** Occurs when a fixed-length buffer reaches its capacity and a process attempts to store data beyond that maximum limit. This can result in extra data overwriting adjacent memory locations, as well as causing other unexpected behaviors. 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.

Mitigating Viruses, Worms, and Trojan Horses

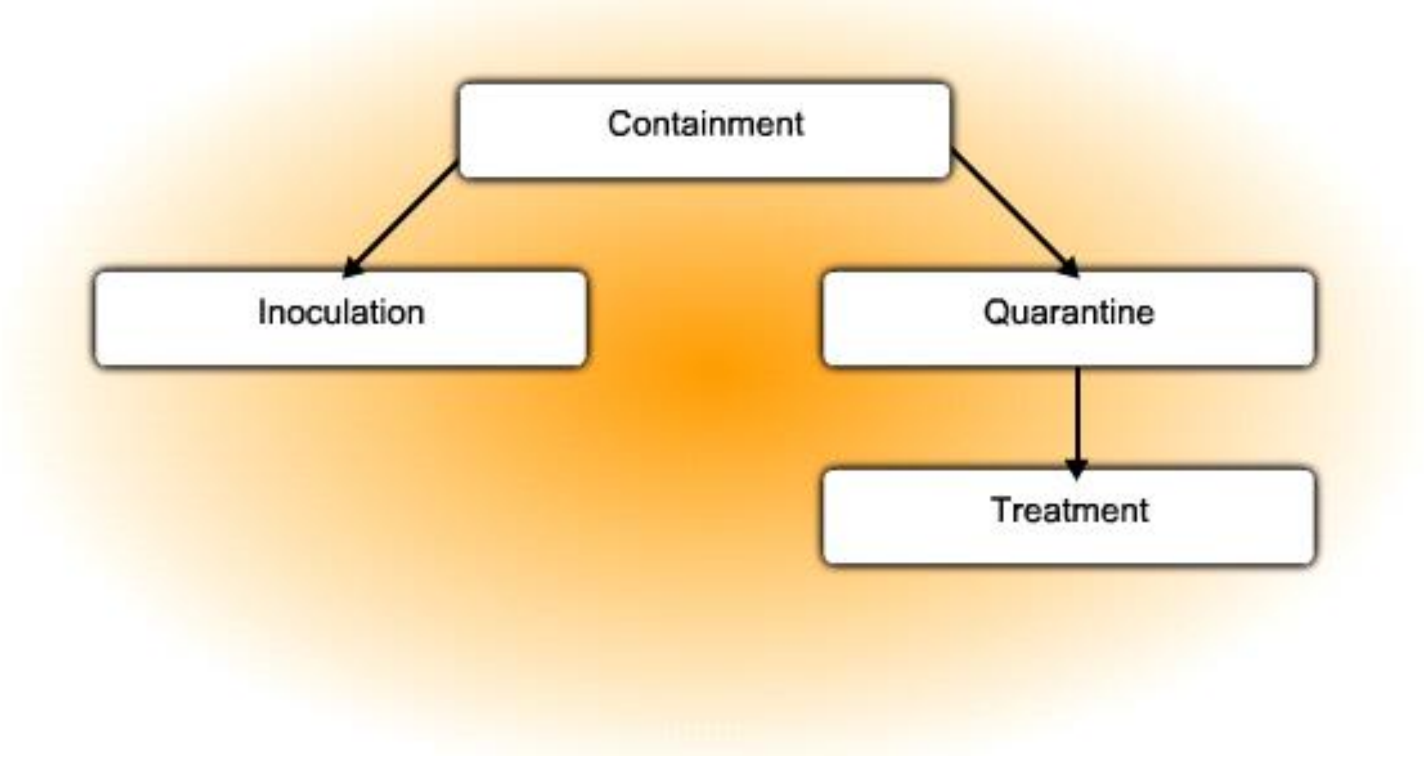
Antivirus Software

Antivirus Software
AVG Internet Security 2014
Panda
ESET NOD32 Antivirus
Bitdefender Internet Security
ZoneAlarm Antivirus + Firewall
avast! Pro Antivirus 2014
Antivirus+ Security
Kaspersky Internet Security
Kaspersky PURE
McAfee Antivirus Plus 2014
Norton AntiVirus

Mitigating Viruses, Worms, and Trojan Horses

Worm Mitigation

- 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.



Mitigating Viruses, Worms, and Trojan Horses

Worm Mitigation Cont.

- **Containment Phase**
  - Limits the spread of a worm infection to areas of the network that are already affected.
  - Compartmentalizes and segments the network to slow down or stop the worm to prevent currently infected hosts from targeting and infecting other systems.
  - Uses 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.

Mitigating Viruses, Worms, and Trojan Horses

Worm Mitigation Cont.

- **Quarantine Phase**
  - Tracks down and identifies infected machines within the contained areas and disconnects, blocks, or removes them.
  - This isolates these systems appropriately for the Treatment Phase.
- **Treatment Phase**
  - Actively infected systems are disinfected of the worm.
  - Terminates the worm process, removes modified files or system settings that the worm introduced, and patches 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.

Mitigating Viruses, Worms, and Trojan Horses

SQL Slammer Worm

- 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.

1.3 Attack Methodologies

Cisco | Networking Academy®
Mind Wide Open™

Attack Methodologies

Types of Attacks

- There are four categories of attacks:
  - **Reconnaissance Attacks** - Involves the unauthorized discovery and mapping of systems, services, or vulnerabilities.
  - **Access Attacks** - Exploits known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information.
  - **Denial of Service (DoS) Attacks** - Sends extremely large numbers of requests over a network or the Internet.
    - These excessive requests cause the target device to run sub-optimally.
    - Consequently, the attacked device becomes unavailable for legitimate access and use.

Attack Methodologies

Types of Reconnaissance Attacks

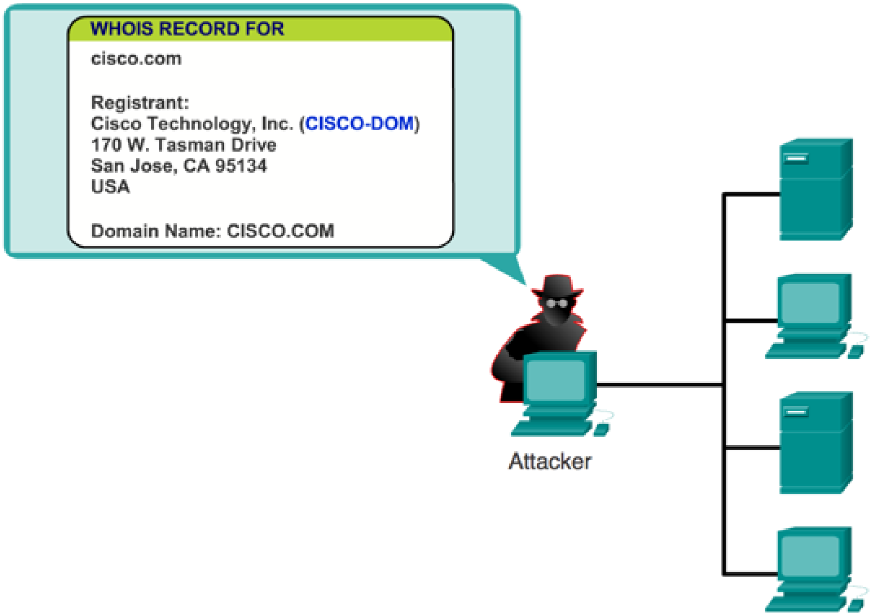
- Reconnaissance, also known as *information gathering,* is the unauthorized discovery and mapping of systems, services, or vulnerabilities. In most cases, precedes an access or DoS attack.
- Reconnaissance attacks can consist of the following:
  - Internet information queries
  - Ping sweeps
  - Port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

Attack Methodologies

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**, …



WHOIS RECORD FOR
cisco.com

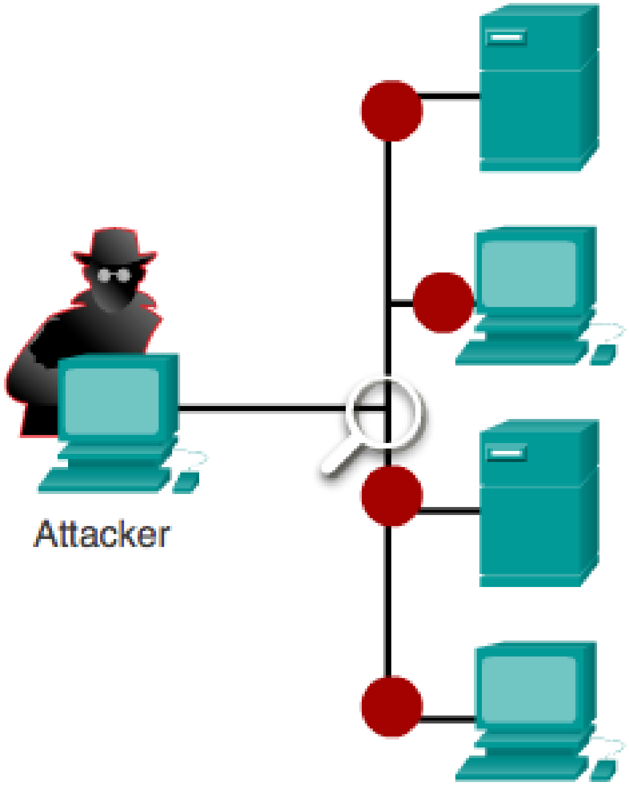
Registrant:
Cisco Technology, Inc. (CISCO-DOM)
170 W. Tasman Drive
San Jose, CA 95134
USA

Domain Name: CISCO.COM

Attack Methodologies

Packet Sniffer

- 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.

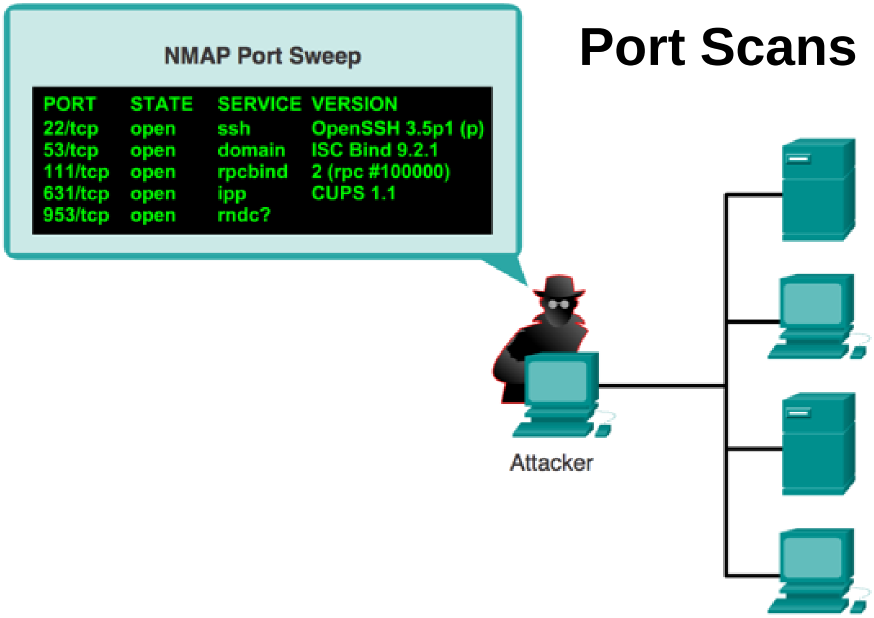


Attack Methodologies

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.

Port Scans



NMAP Port Sweep

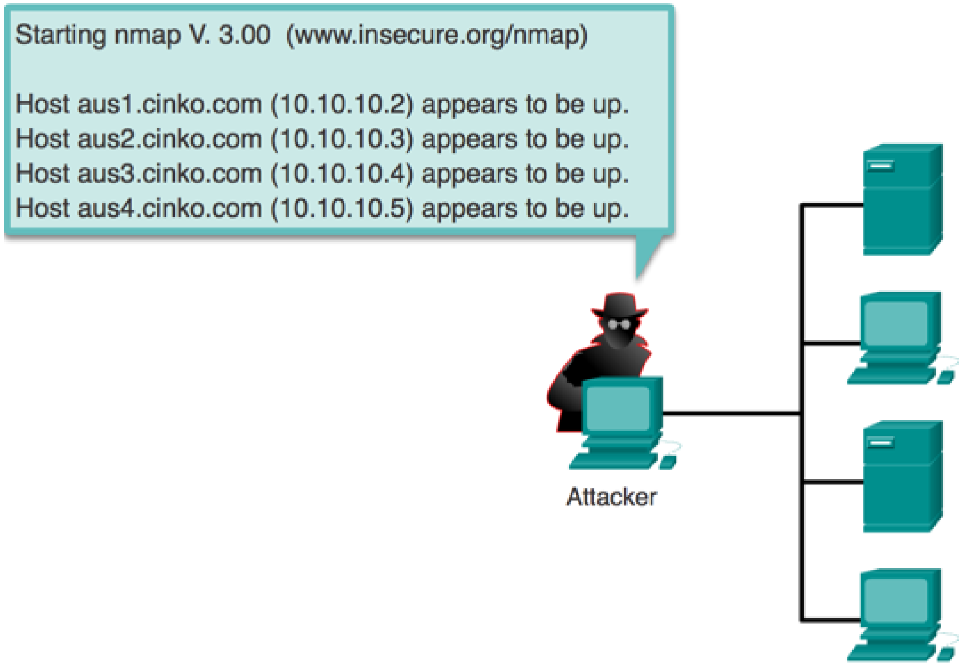
```
PORT     STATE  SERVICE  VERSION
22/tcp   open   ssh      OpenSSH 3.5p1 (p)
53/tcp   open   domain   ISC Bind 9.2.1
111/tcp  open   rpcbind  2 (rpc #100000)
631/tcp  open   ipp      CUPS 1.1
953/tcp  open   rndc?
```

Attack Methodologies

Ping Sweeps and Port Scans Cont.

- 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.

Ping Sweep



```
Starting nmap V. 3.00  (www.insecure.org/nmap)

Host aus1.cinko.com (10.10.10.2) appears to be up.
Host aus2.cinko.com (10.10.10.3) appears to be up.
Host aus3.cinko.com (10.10.10.4) appears to be up.
Host aus4.cinko.com (10.10.10.5) appears to be up.
```

Attack Methodologies

Mitigating Reconnaissance Attacks

- Reconnaissance attacks are typically the precursor to additional attacks, with the intent of gaining unauthorized access to a network or disrupting network functionality.
- A network security professional can detect when a reconnaissance attack is underway by receiving notifications from preconfigured alarms, such as the number of ICMP requests per second.

Attack Methodologies

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

Attack Methodologies

Types of Access Attacks

Access attacks can be performed in a number of different ways

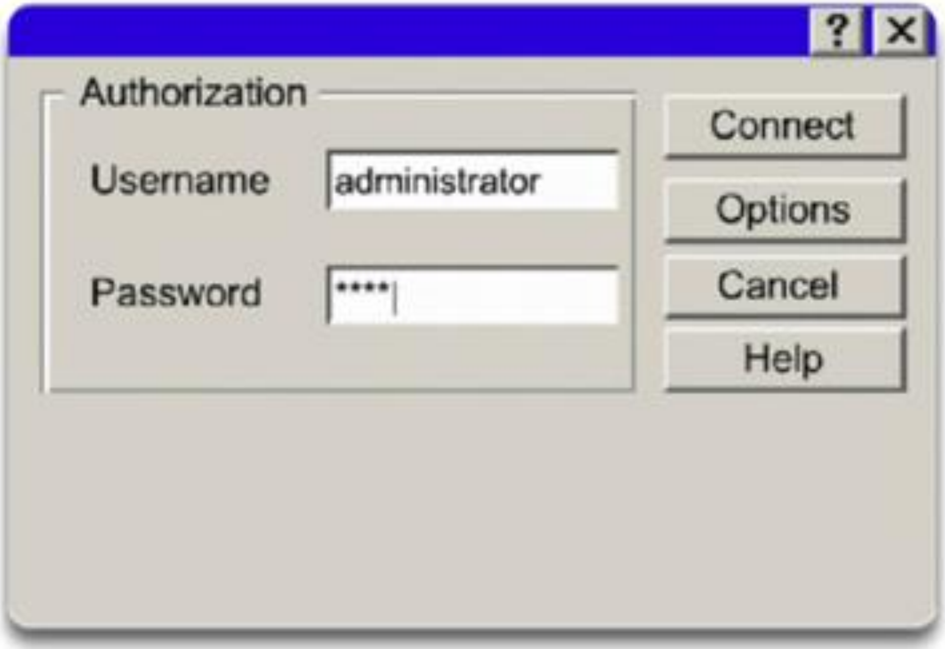
- Password attacks
- Trust exploitation
- Port redirection
- Man-in-the-middle attacks
- Buffer overflow

Types of Attacks

Password Attacks

Hackers implement password attacks using the following:

- Brute-force attacks - An access attack method that involves a software program attempting to discover a system password by using an electronic dictionary.
- Trojan horse programs
- IP spoofing
- Packet sniffers
- Manipulating users



Authorization

Username administrator

Password ****

Types of Attacks

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.

Types of Attacks

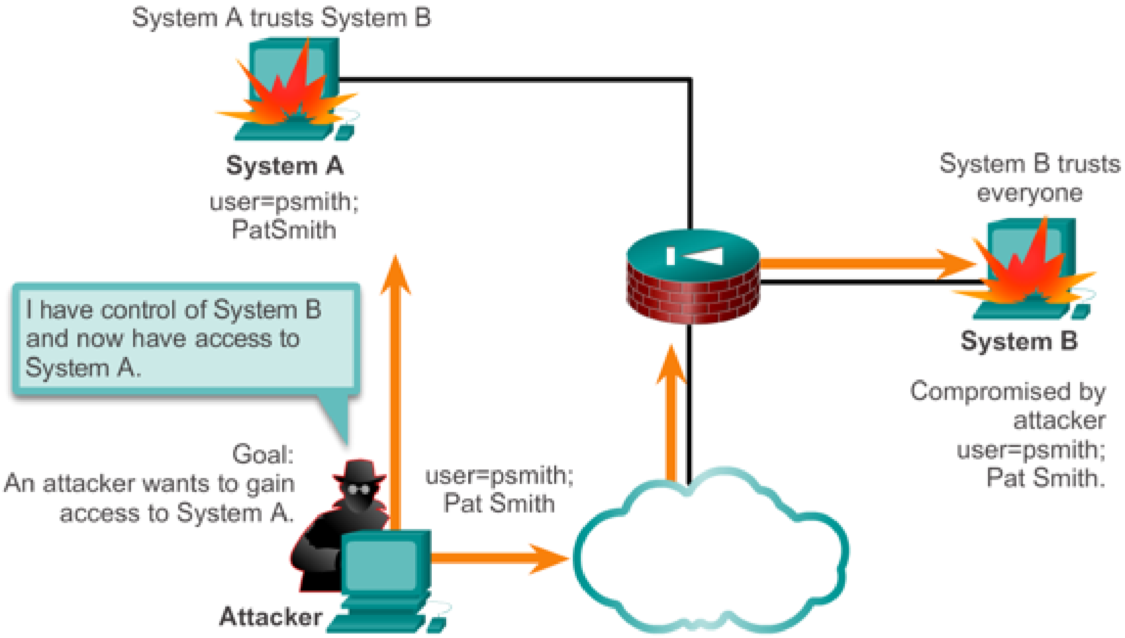
Trust Exploitation Cont.

- 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.

Types of Attacks

Trust Exploitation

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


System A trusts System B
System A
user=psmith; PatSmith
System B trusts everyone
I have control of System B and now have access to System A.
System B
Compromised by attacker user=psmith; Pat Smith.
Goal: An attacker wants to gain access to System A.
user=psmith; Pat Smith
Attacker

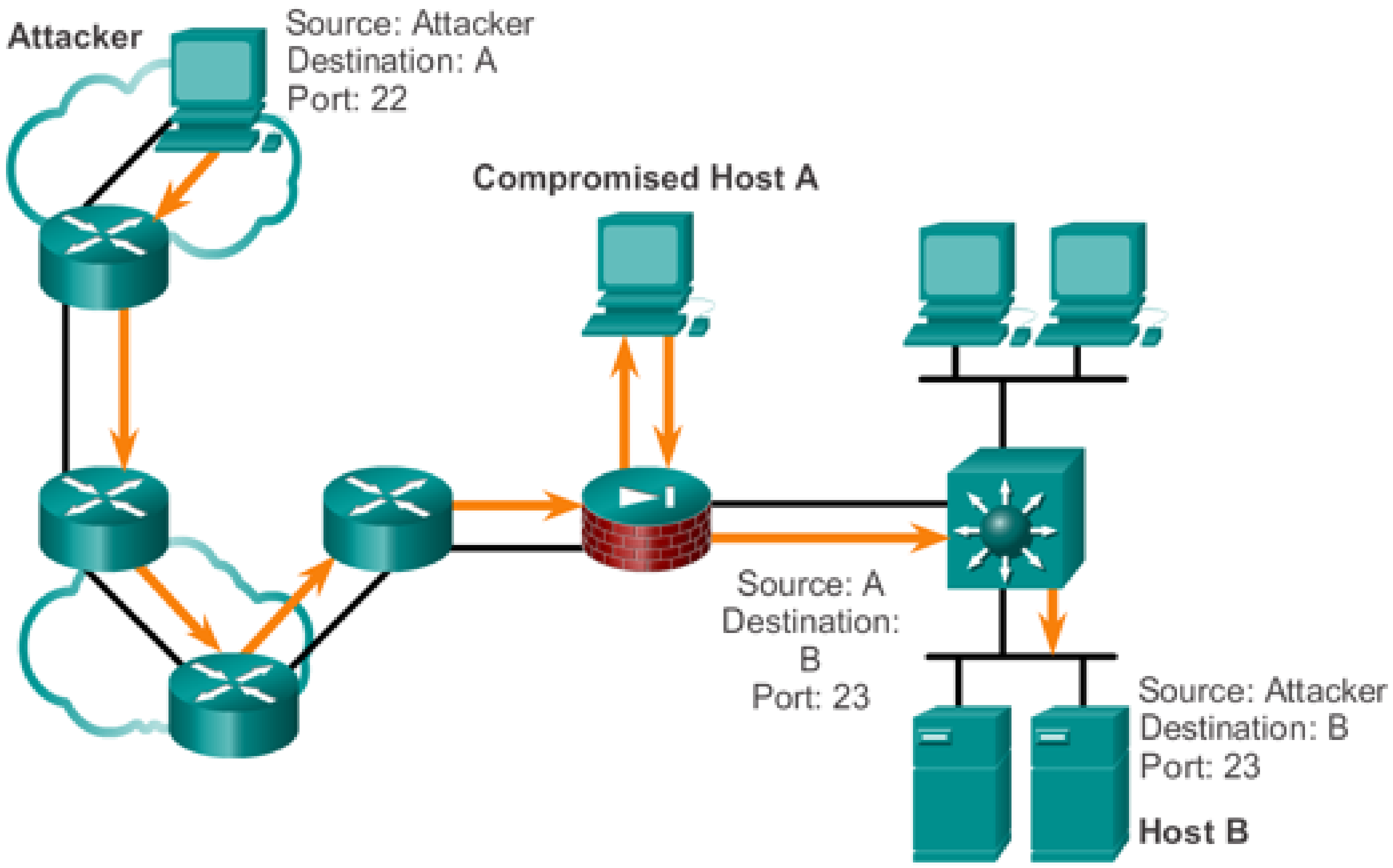
Types of Attacks

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.

Types of Attacks

Port Redirection Cont.



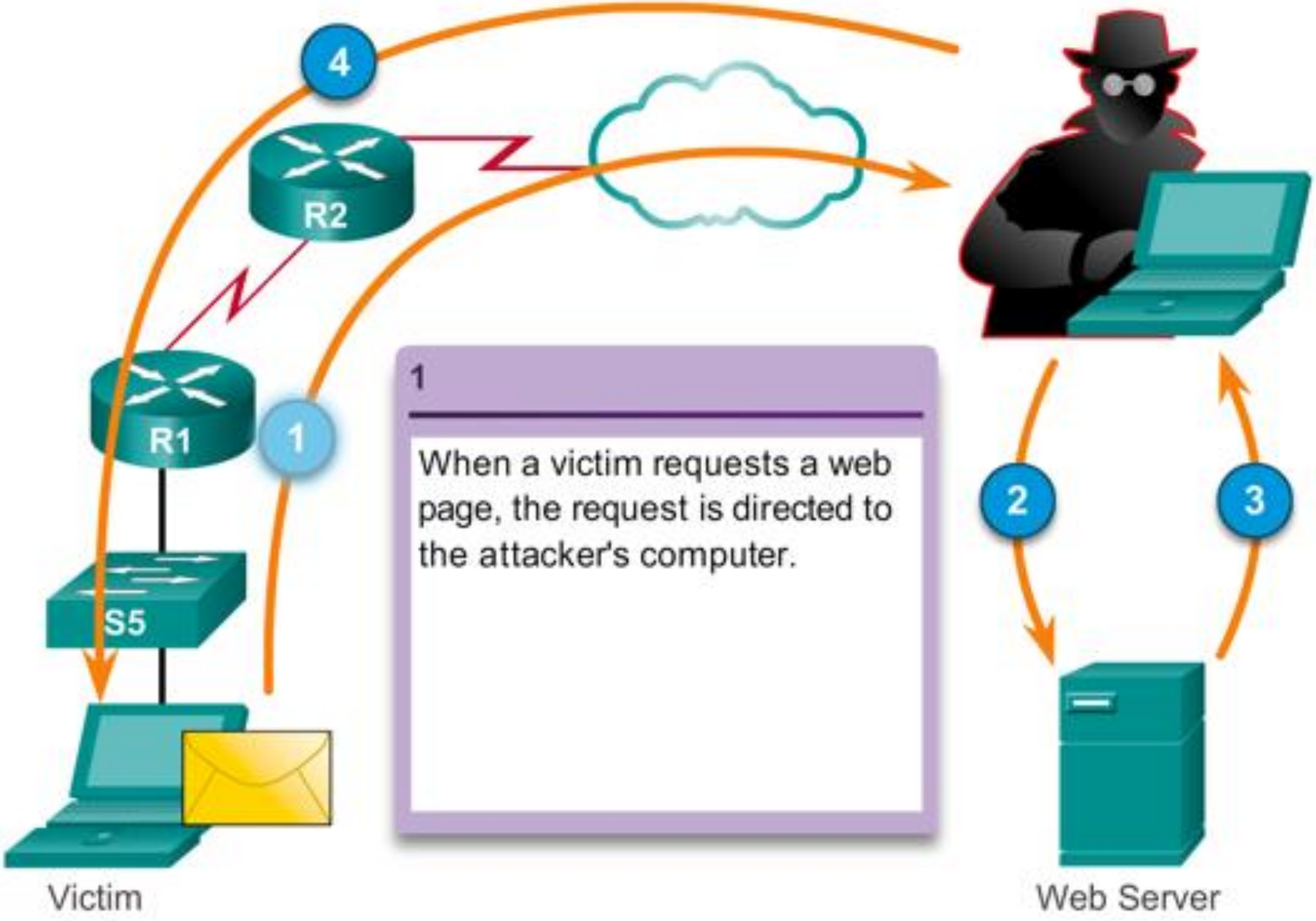
Types of Attacks

Man-in-the-Middle Attacks (MITM)

- MITM 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 MITM 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

Man-in-the-Middle Attacks (MITM) Cont.



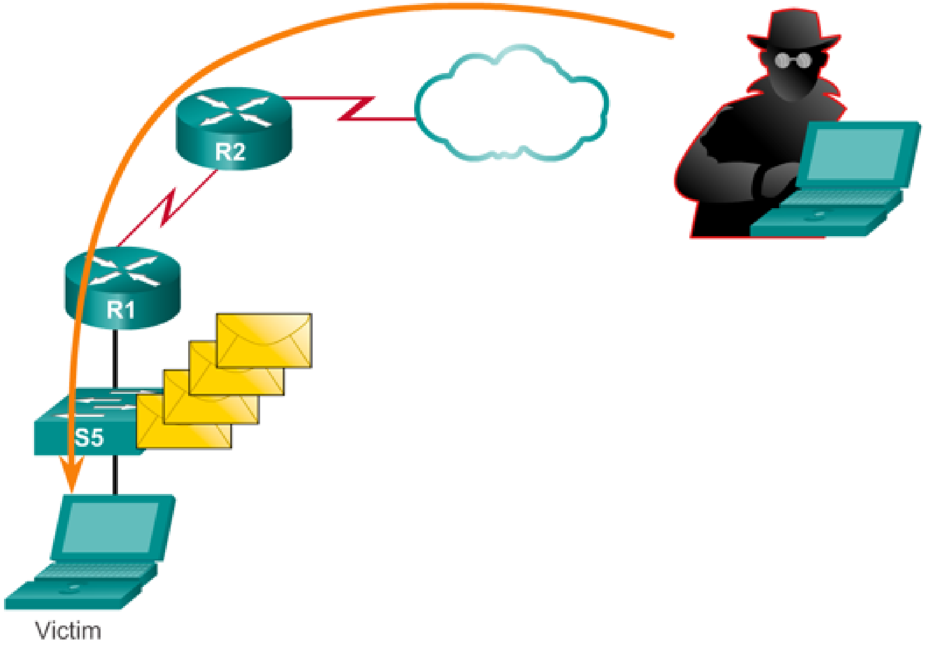
1

When a victim requests a web page, the request is directed to the attacker's computer.

Types of Attacks

Buffer Overflow Attacks

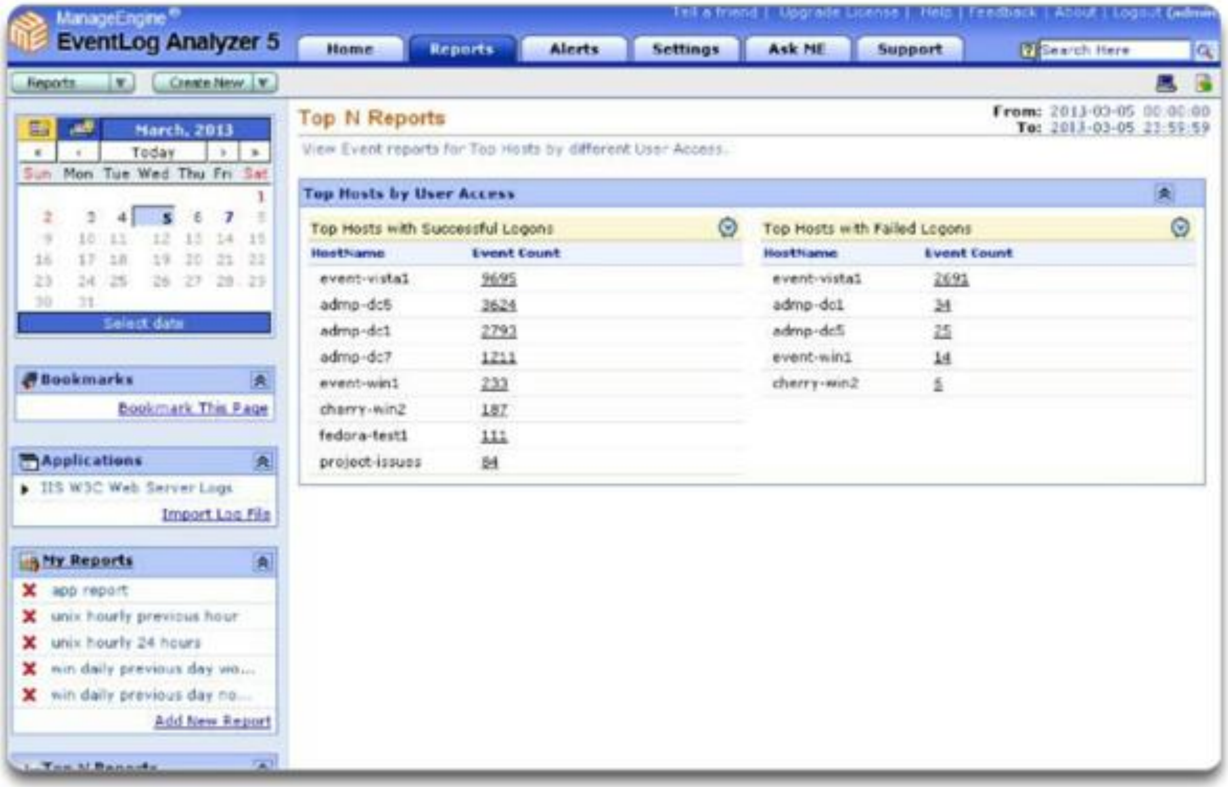
- A program writes data beyond the allocated buffer memory.
- Buffer overflows usually arise as a consequence of a bug in a C or C++ program.
- A result of the overflow is that valid data is overwritten or exploited to enable the execution of malicious code.
- The overflow can be used to modify the values of program variables and cause the program to jump to unintended places, or even replace valid program instructions with arbitrary code.



Attack Methodologies

Mitigating Access Attacks

- Access attacks in general can be detected by reviewing logs, bandwidth utilization, and process loads.
- The network security policy should specify that logs are formally maintained for all network devices and servers.



Top N Reports

From: 2013-03-05 00:00:00
To: 2013-03-05 23:59:59

View Event reports for Top Hosts by different User Access.

Top Hosts by User Access

Top Hosts with Successful Logons

HostName	Event Count
event-vista1	9695
admp-dc5	3624
admp-dc1	2793
admp-dc7	1211
event-win1	233
cherry-win2	187
fedora-test1	111
project-issues	84

Top Hosts with Failed Logons

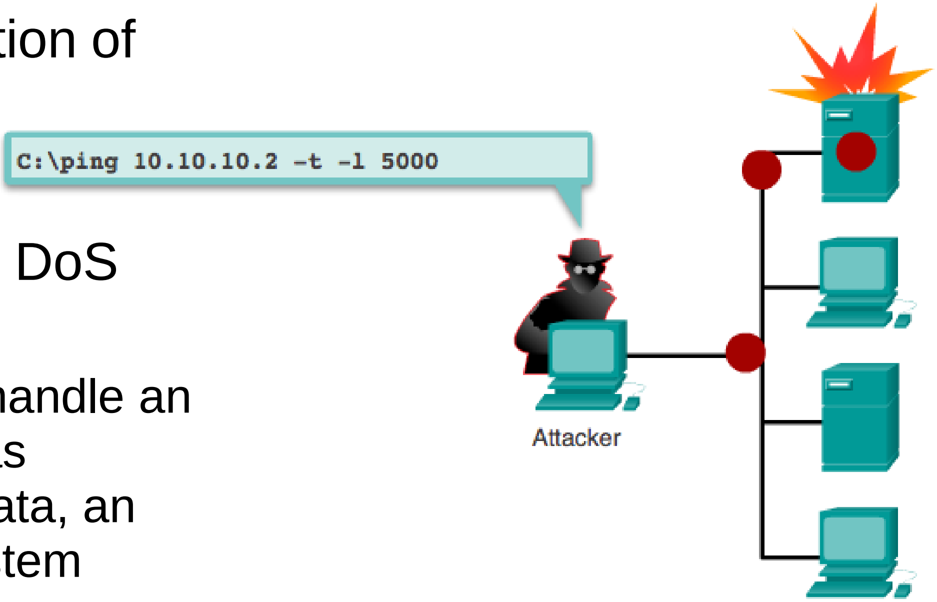
HostName	Event Count
event-vista1	2691
admp-dc1	34
admp-dc5	25
event-win1	14
cherry-win2	5

Applications
- IIS W3C Web Server Logs

My Reports
- app report
- unix hourly previous hour
- unix hourly 24 hours
- win daily previous day wo...
- win daily previous day no...

DoS Attack

- A **DoS** attack is a network attack that results in some sort of interruption of service to users, devices, or applications.
- There are two major reasons a DoS attack occurs:
  - A host or application fails to handle an unexpected condition, such as maliciously formatted input data, an unexpected interaction of system components, or simple resource exhaustion.
  - A network, host, or application is unable to handle an enormous quantity of data, causing the system to crash or become extremely slow.

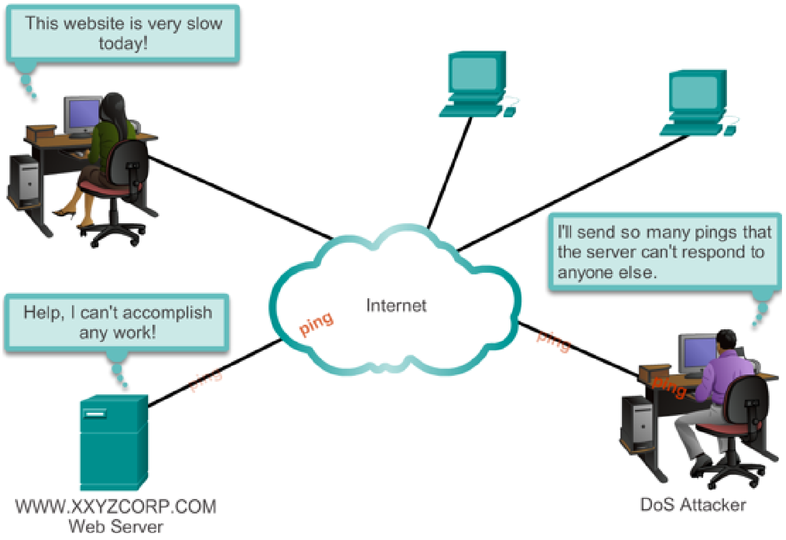


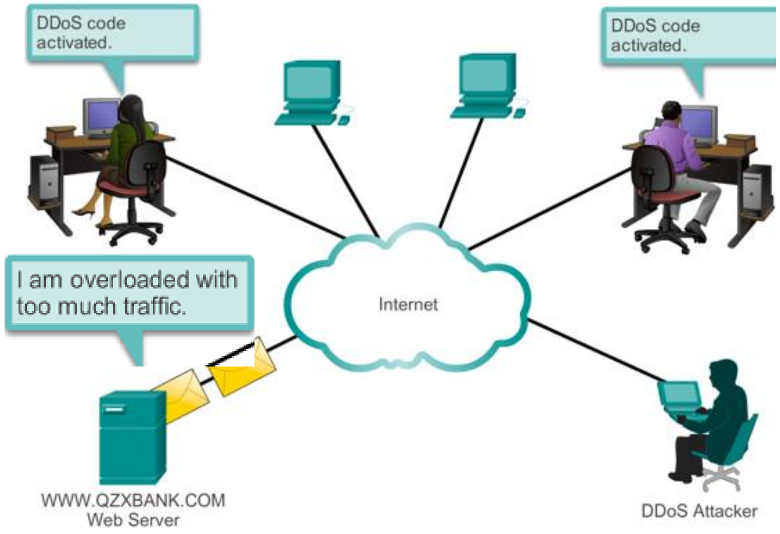
```
C:\ping 10.10.10.2 -t -l 5000
```

DoS Attacks

DoS and DDoS

A **Distributed DoS Attack (DDoS)** is similar in intent to a DoS attack, except that a DDoS attack originates from multiple coordinated sources.

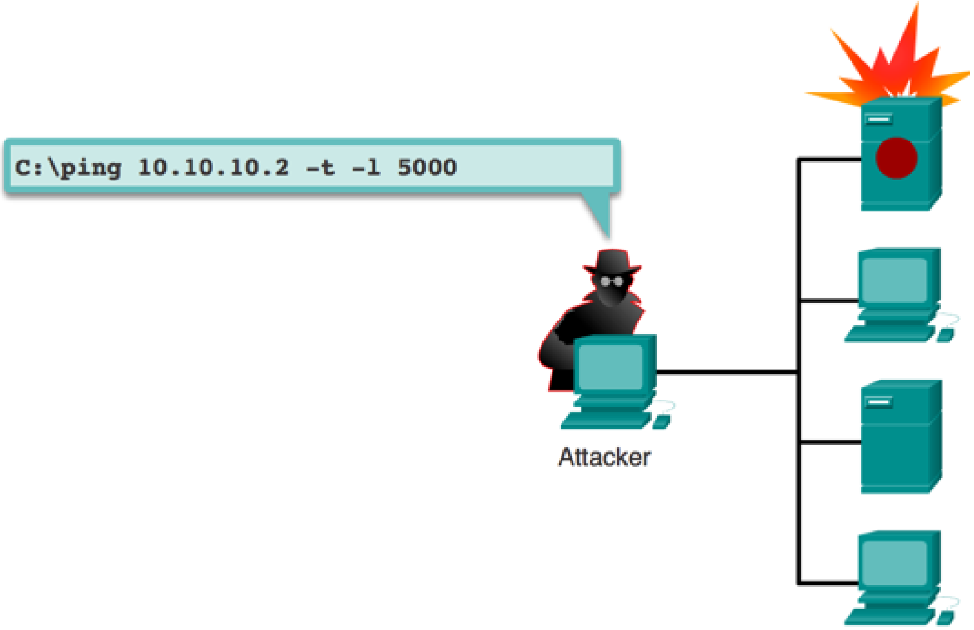

This website is very slow today!
Help, I can't accomplish any work!
Internet
ping
ping
ping
ping
I'll send so many pings that the server can't respond to anyone else.
WWW.XXYZCORP.COM Web Server
DoS Attacker


DDoS code activated.
DDoS code activated.
I am overloaded with too much traffic.
Internet
WWW.QZXBANK.COM Web Server
DDoS Attacker

DoS Attacks

Types of DoS Attacks

- 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.

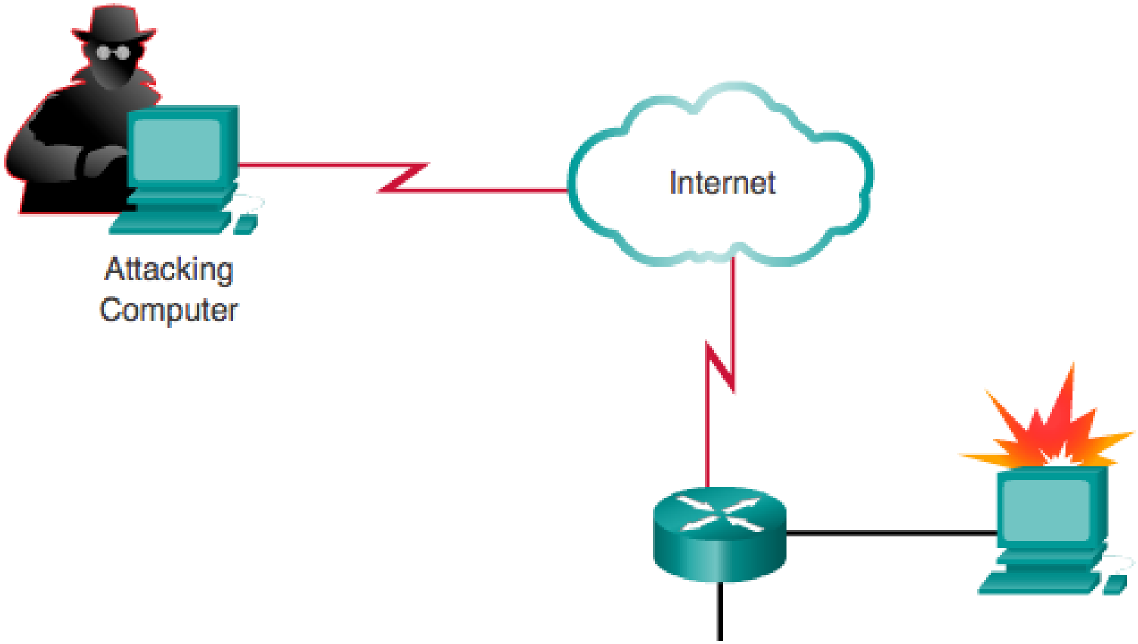


```
C:\ping 10.10.10.2 -t -l 5000
```

DoS Attacks

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 fills the reassembly buffers of the target.



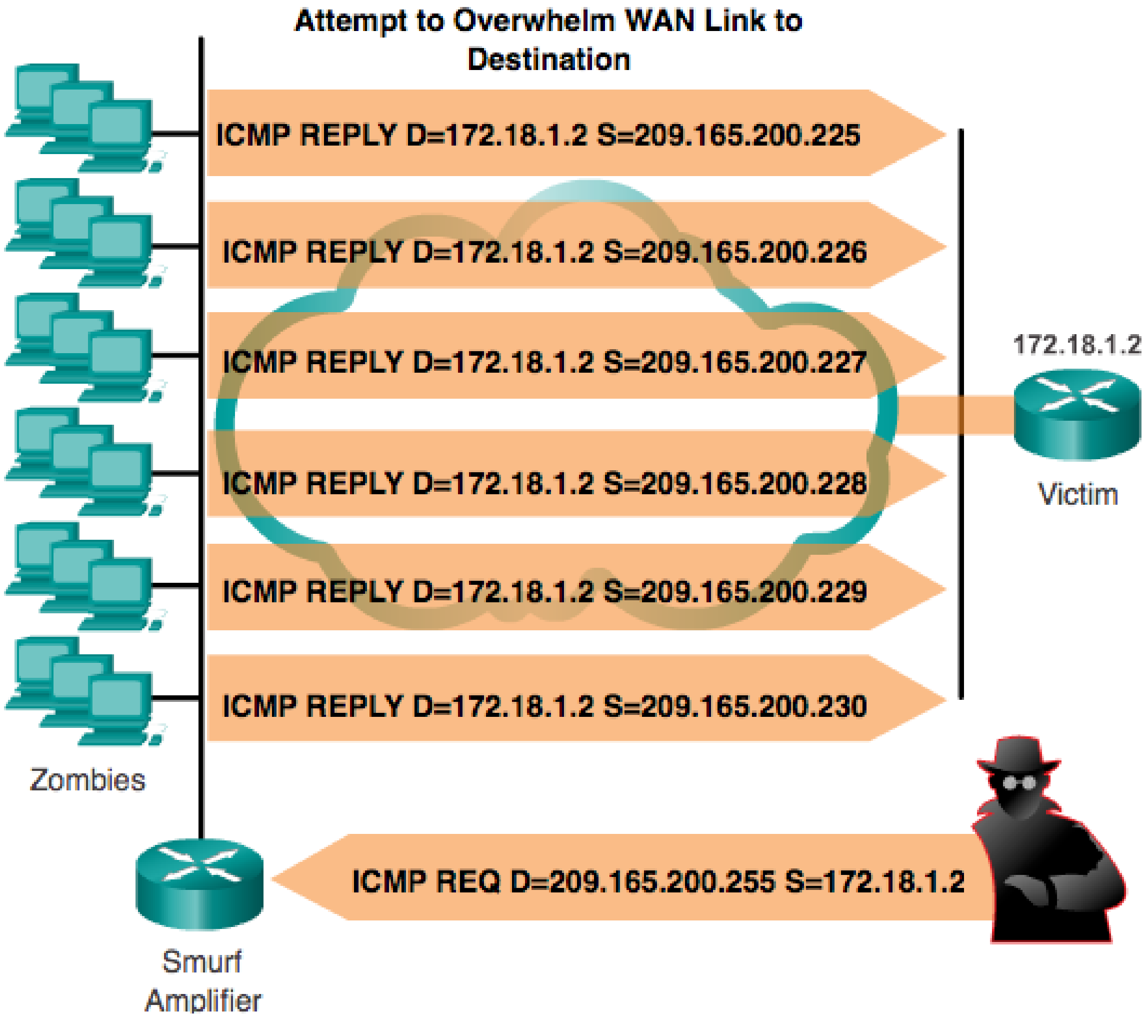
DoS Attacks

Smurf Attack

- A Smurf Attack is a DDoS attack in which large numbers of ICMP packets with the intended victim's spoofed source IP are broadcast to a computer network.
- 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.

DoS Attacks

Smurf Attack Cont.


Attempt to Overwhelm WAN Link to Destination
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
172.18.1.2
Victim
Zombies
ICMP REQ D=209.165.200.255 S=172.18.1.2
Smurf Amplifier

DoS Attacks

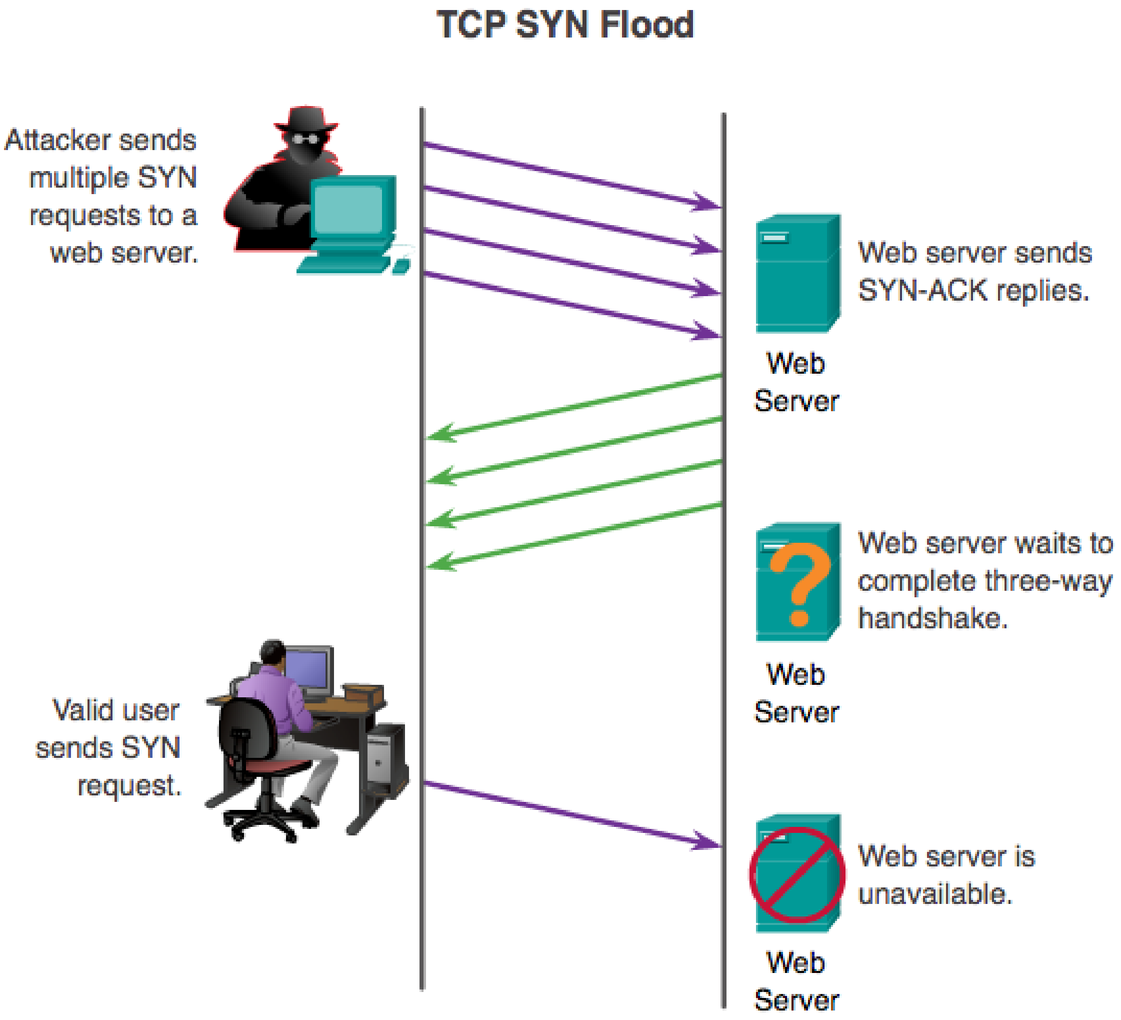
SYN Flood Attack

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 Attacks

SYN Flood Attack Cont.


TCP SYN Flood
Attacker sends multiple SYN requests to a web server.
Web server sends SYN-ACK replies.
Web Server
Web server waits to complete three-way handshake.
Web Server
Valid user sends SYN request.
Web server is unavailable.
Web Server

DoS Attacks

Symptoms of a DoS Attack

There are five basic ways that DoS attacks can do harm:

1. Consumption of resources, such as bandwidth, disk space, or processor time.
2. Disruption of configuration information, such as routing information.
3. Disruption of state information, such as unsolicited resetting of TCP sessions.
4. Disruption of physical network components.
5. Obstruction of communication between the victim and others.

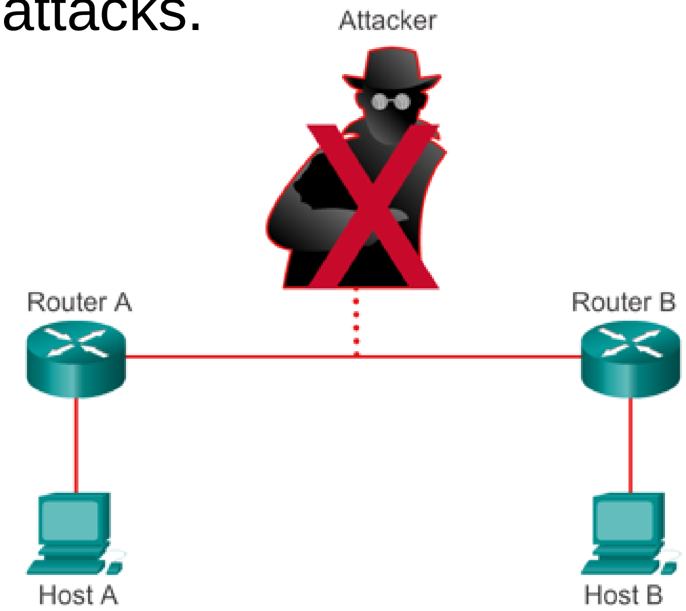
Mitigating Network Attacks

Mitigating Network Attacks

The type of attack, as specified by the categorization of reconnaissance, access, or DoS attack, determines the means of mitigating a network threat.

Mitigating Reconnaissance Attacks

- 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.
- Use anti-sniffer tools to detect sniffer attacks.
- Using switched networks.
- Use a firewall and IPS.



Mitigating Network Attacks

Mitigating Access Attacks

- Techniques to mitigate access attacks include:
  - Strong password security
  - Principle of minimum trust
  - Cryptography
  - Applying operating system and application patches
- Practices that help to ensure a strong password policy:
  - Disable accounts after a specific number of unsuccessful logins. This practice helps to prevent continuous password attempts.
  - Do not use plaintext passwords. Use either a one-time password or encrypted password.
  - Use strong passwords. Strong passwords are at least eight characters and contain uppercase letters, lowercase letters, numbers, and special characters.

Mitigating Network Attacks

Mitigating DoS Attacks

- IPS and firewalls (Cisco ASAs and ISRs)
- Antispoofing technologies
- Quality of Service-traffic policing

Mitigating Network Attacks

Mitigating DoS Attacks Cont.

- 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.

Mitigating Network Attacks

10 Best Practices

1. Keep patches current by installing them weekly or daily, if possible, to prevent buffer overflow and privilege escalation attacks.
2. Shut down unnecessary services and ports.
3. Use strong passwords and change them often.
4. Control physical access to systems.
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.

Mitigating Access Attacks

10 Best Practices Cont.

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

7. 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&

8. Encrypt and password-protect sensitive data.

9. Implement security hardware and software such as firewalls, Intrusion Prevention Systems (IPSs), Virtual Private Network (VPN) devices, antivirus software, and content filtering.

10. Develop a written security policy for the company.

1.4 Cisco Network Foundation Protection Framework

Cisco | Networking Academy®
Mind Wide Open™

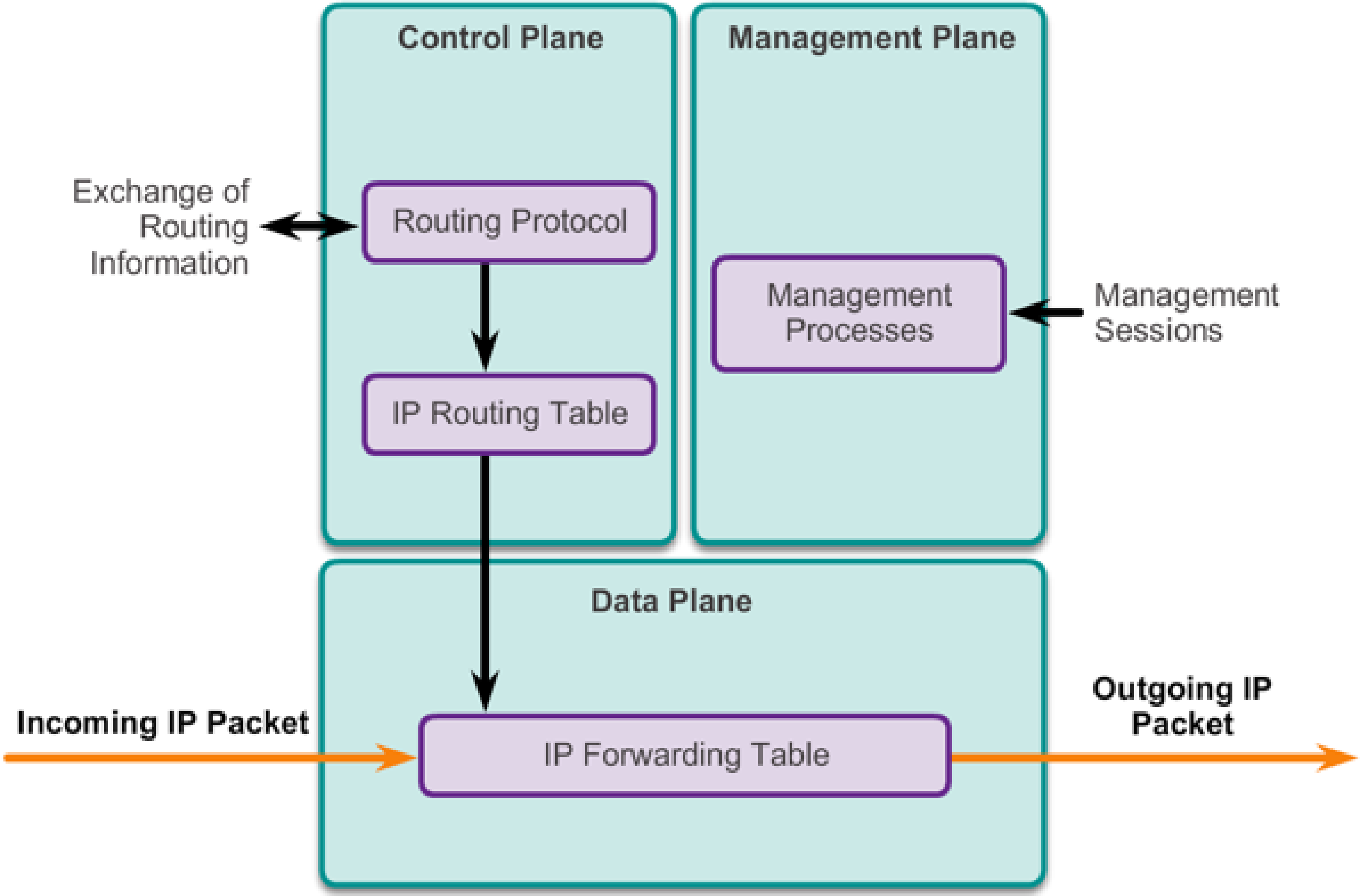
Cisco Network Foundation Protection

The Cisco Network Foundation Protection (NFP) logically divides routers and switches into three functional areas:

- **Control Plane** - Responsible for routing data correctly. Consists of device-generated packets required for the operation of the network itself such as ARP message exchanges or OSPF routing advertisements.
- **Management Plane** - Responsible for managing network elements. Generated either by network devices or network management stations using processes and protocols, such as Telnet, SSH, TFTP, FTP, NTP, AAA, SNMP, syslog, TACACS+, RADIUS, and NetFlow.
- **Data Plane** (Forwarding Plane) - Responsible for forwarding data. Consists of user-generated packets being forwarded between end stations. Most traffic travels through the router, or switch, via the data plane.

Cisco Network Foundation Protection Framework

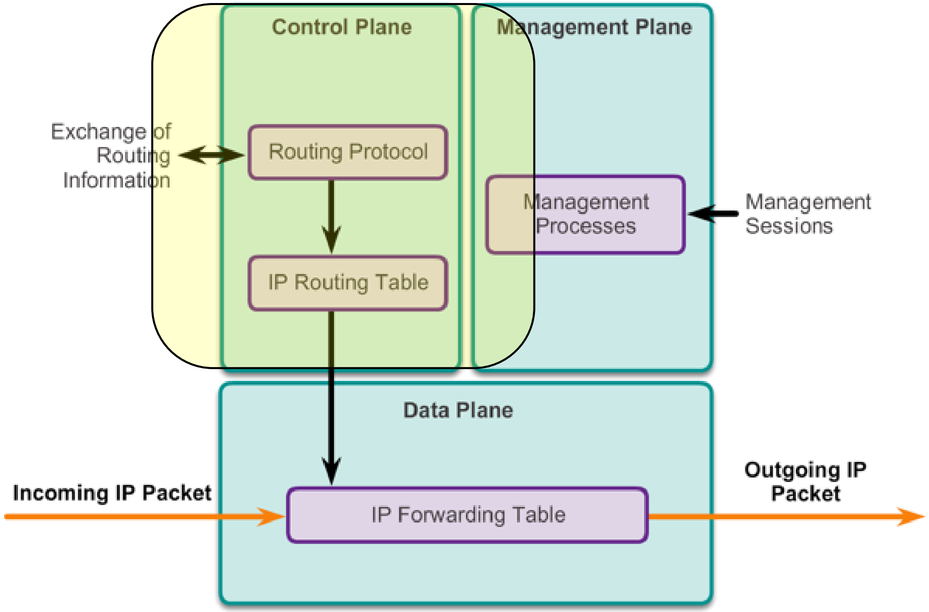
Cisco Network Foundation Protection Cont.



Cisco Network Foundation Protection Framework

Control Plane

- **Cisco AutoSecure** provides a one-step lockdown for the control, management, and data planes.
- **Routing protocol authentication** prevents the router from accepting fraudulent routing updates.
- **Control Plane Policing (CoPP)** prevents unnecessary traffic from overwhelming the route processor. CoPP treats the control plane as a separate entity and applies rules to the input and output ports.



Cisco Network Foundation Protection Framework

Control Plane Cont.

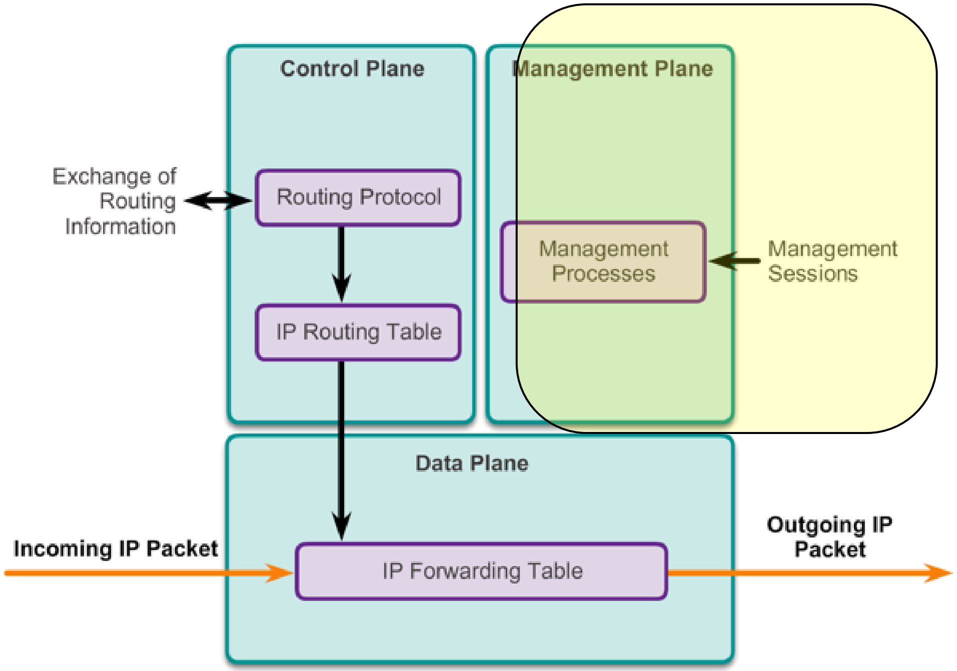
- CoPP is designed to prevent unnecessary traffic from overwhelming the route processor.

- CoPP consists of the following features:
  - **Control Plane Policing (CoPP)** - Allows users to configure a QoS filter that manages the traffic flow of control plane packets. This protects the control plane against reconnaissance and DoS attacks.
  - **Control Plane Protection (CPPr)** - An extension of CoPP that allows for policing granularity. For example, CPPr can filter and rate-limit the packets that go to the control plane of the router and discard malicious and error packets (or both).
  - **Control Plane Logging** - Enables the logging of packets that CoPP or CPPr drop or permit. It provides the logging mechanism needed to deploy, monitor, and troubleshoot CoPP features efficiently.

Cisco Network Foundation Protection Framework

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.
- **Authorize actions** by restricting 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.

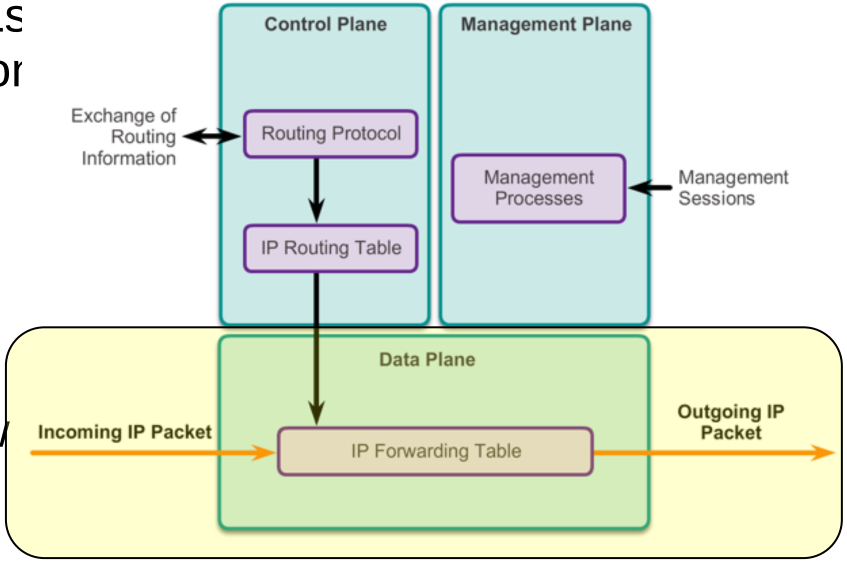


Cisco Network Foundation Protection Framework

Data Plane

Use ACLs to perform packet filtering. ACLs can be used to:

- **Block unwanted traffic or users -** ACLs can filter incoming or outgoing packets on an interface.
- **Reduce the change of a DoS attack -** ACLs can be used to specify whether traffic from hosts, networks, or users access the network.
- **Mitigate spoofing attacks -** ACLs allow security practitioners to implement recommended practices to mitigate spoofing attacks.
- **Provide bandwidth control -** ACLs on a slow link can prevent excess traffic.
- **Classify traffic to protect the management and control planes -** ACLs can be applied on the vty lines.

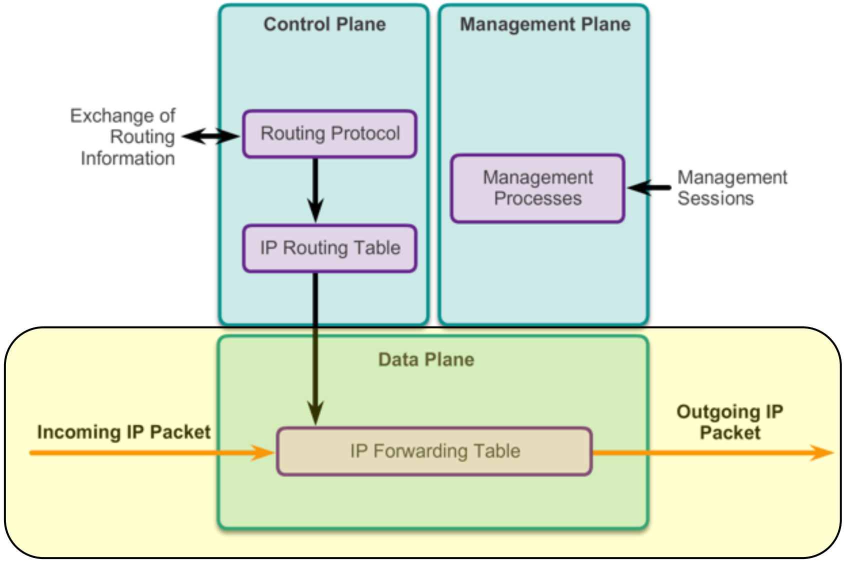


Cisco Network Foundation Protection Framework

Data Plane Cont.

Implement Layer 2 security using:

- **Port security -** Prevents MAC address spoofing and MAC address flooding attacks.
- **DHCP snooping -** Prevents client attacks on the DHCP server and switch.
- **Dynamic ARP Inspection (DAI) -** Adds security to ARP by using the DHCP snooping table to minimize the impact of ARP poisoning and spoofing attacks.
- **IP Source Guard -** Prevents spoofing of IP addresses by using the DHCP snooping table.



Summary

- Network security is now an integral part of computer networking.
- Network security involves protocols, technologies, devices, tools, and techniques to secure data and mitigate threats.
- Network security is largely driven by the effort to stay one step ahead of ill-intentioned hackers.
- Network security organizations have been created to establish formal communities of network security professionals.
- The complexity of network security makes it difficult to master all it encompasses.
- Different organizations have created domains that subdivide the world of network security into more manageable pieces.
- This division allows professionals to focus on more precise areas of expertise in their training, research, and employment.

Summary Cont.

- Network security policies are created by companies and government organizations to provide a framework for employees to follow during their day-to-day work.
- Network security professionals at the management level are responsible for creating and maintaining the network security policy.
- Network attacks are classified easily learn about them and address them appropriately.
- Viruses, worms, and Trojan horses are specific types of network attacks. More generally, network attacks are classified as reconnaissance, access, or DoS attacks.
- Mitigating network attacks is the job of a network security professional.

Cisco | Networking Academy®

Mind Wide Open™