Lecture One

Network Security Framework

Dr. M. Mahfuzul Islam
Professor, Dept. of CSE, BUET

Faculty and Assessment details

- **Faculty Information**

Dr. M. Mahfuzul Islam

Room: ECE-115, Tel: 0191 307 1907

E-mail: *mahfuz@cse.buet.ac.bd*

- **Reference Book:**
  - Matt Bishop, Introduction to Computer Security, Pearson
  - CCNA Security
  - Chun-Shien Lu, Multimedia Security, Ideal Group Publishing

- **Mark distribution**

Attendance	10%
Midterm	25%
Report	20%
Draft Paper	10%
Final	35%
Total	100%

Class Time:

- Sunday (5:00 pm -8:00 pm)

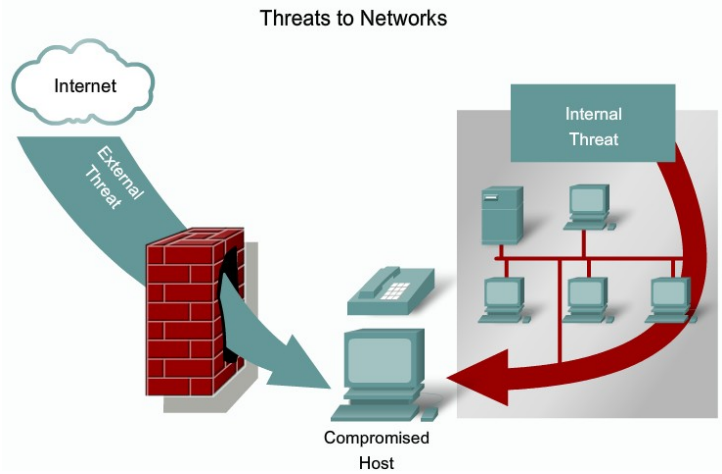
Evolution of Network Security

Security of the network is ultimately the responsibility of everyone that uses it.

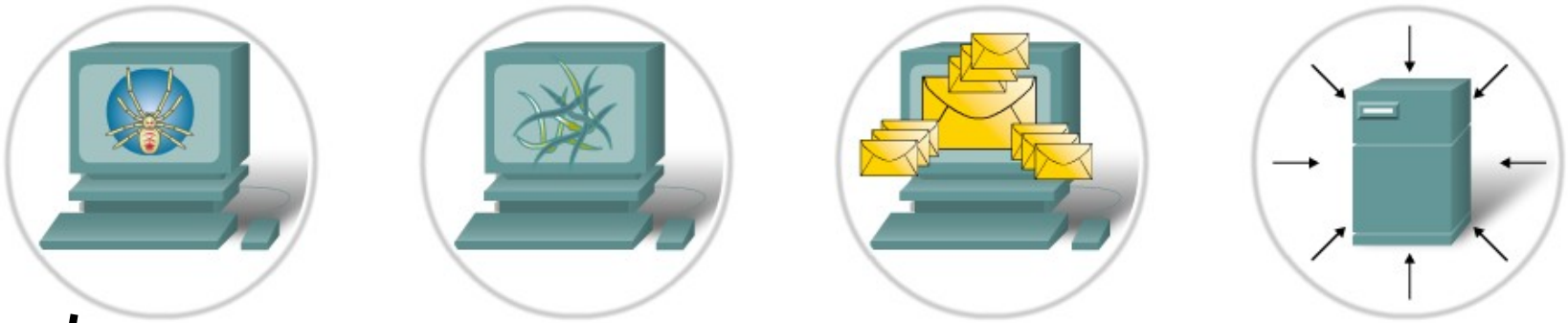
Network Security is to protect network from any unauthorized access.

Internal threats can cause even greater damage than external threats.

Protection System describes the conditions under which a system is secure.



Network Security Drivers



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 ... d

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

To: Everyone
From:
Subject

The Morris Internet Worm

All the following events occu

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.

Evolution of Network Security

Three Dimensions of Security:

- Confidentiality: concealment of information or resources.
  - Prevent the disclosure of sensitive information from unauthorized people, resources, and processes.
  - Access control mechanisms and Resource hiding supports confidentially.
- Availability: the ability to use the information or resources desired.
  - The assurance that systems and data are accessible by authorized users when needed.
  - Availability is an important aspect of reliability.
  - Attempts to block availability, called DOS attack is the most difficult to detect, if unusual access patterns are attributable to deliberate manipulation of resources ot of environment.

Evolution of Network Security

- Integrity: Trustworthiness of data and resources.
  - The protection of system information or processes from intentional or accidental modification.
  - Integrity includes data integrity (the contents of information) and origin integrity (the source of data often called authentication). The source of information may bear on its accuracy and credibility.
  - Integrity mechanisms fall into two classes: Prevention Mechanism and detection mechanism (report that the data integrity is no longer trustworthy).
    - Prevention blocks any unauthorized attempts to change the data (lack of authentication) or any attempts to change the data in unauthorized way (lack of authorization)

- Hackers
  - Negative
  - Positive

Hacking is a driving force in network security.

Threats

Threats: Potential violation of security.

Attacks: Actions that could cause violation of security.

Threats can be divided into four broad classes:

- **Disclosure:** unauthorized access of information.
- **Deception:** acceptance of false data.
- **Disruption:** Interruption or prevention of correct operation.
- **Usurpation:** Unauthorized control of some part of a system.

- Hackers
  - Negative
  - Positive

Hacking is a driving force in network security.

Threats

Some Important threats are:

- **Snooping:** unauthorized interception of information.
  - ✓ Passive wiretapping: Listening to communications or browsing files or system information.
  - ✓ Active wiretapping: Modification or alteration of information, e.g., the man-in the middle attack.
- **Masquerading or spoofing:** Impersonation of one entity by another. Delegation occurs when one entity authorizes a second entity to perform functions on its behalf. Masquerading is a violation of security whereas delegation is not.
  - ✓ Passive masquerading: does not attempt to authenticate the recipient but merely accesses it.
  - ✓ Active masquerading: Masquerader issues response to mislead the user about its identity.
- **Repudiation of origin:** A false denial that an entity sent (or created) something.
- **Denial of receipt:** a false denial that an entity received some information or message.
- **Delay:** a temporary inhibition of a service. This requires manipulation of system control structures, such as network components or server components.
- **Denial of Service (DoS):** a long term inhibition of a service. This an infinite delay.

Network security professionals

Network Security Engineer

Information Security Analyst

Network Security Specialist

Network Security Administrator

Network Security Architect

Systems Engineer

Network Security Organizations

www.infosyssec.com

www.sans.org

www.cisecurity.org

www.cert.org

www.isc2.org

www.first.org

www.infragard.net

www.mitre.org

www.cnss.gov

Network Security Certifications

(ISC)² SECURITY TRANSCENDS TECHNOLOGY®

Information security certifications Offered by (ISC)2

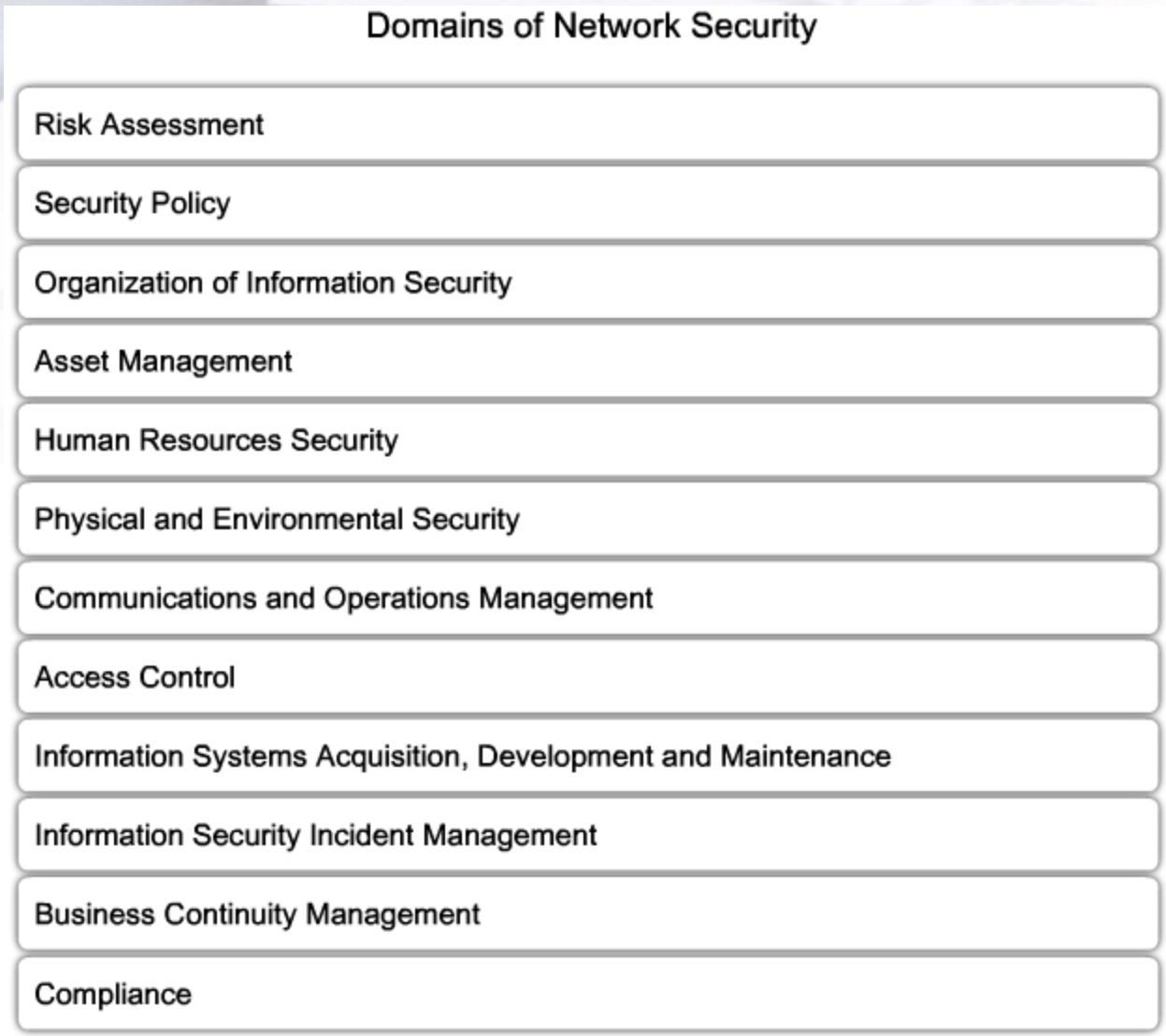
Systems Security Certified Practitioner (SCCP)

Certification and Accreditation Professional (CAP)

Certified Secure Software Lifecycle Professional (CSSLP)

Certified Information Systems Security Professional (CISSP)

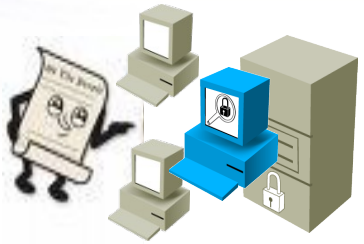
Domains of Network Security



ISO/IEC 17799

Security Policy

- A document that states how an organization plans to protect its tangible and intangible information assets
  - Management instructions indicating a course of action, a guiding principle, or appropriate procedure
  - High-level statements that provide guidance to workers who must make present and future decisions
  - Generalized requirements that must be written down and communicated to others



- Network security policy outlines:
  - Rule of network access: Establishes a hierarchy of access permissions.
  - How policies are enforced
  - Describes the basic architecture of the organization's network security environment

Documents Supporting Security Policies

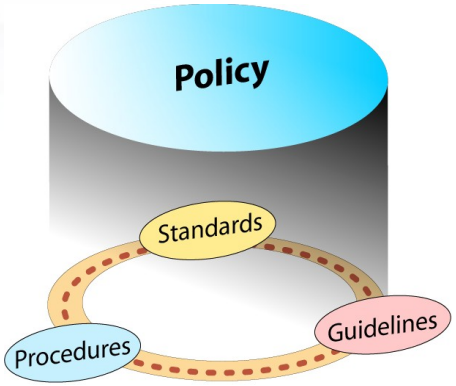
- Standards – dictate specific minimum requirements in our policies
- Guidelines – suggest the best way to accomplish certain tasks
- Procedures – provide a method by which a policy is accomplished (the instructions)

Subsection	6.1 PERSONNEL SECURITY Change Control #: 1.0
Policy	6.1.3 Confidentiality Agreements Approved by: SMH
Objectives	Confidentiality of organizational data is a key tenet of our information security program. In support of this goal, ABC Co will require signed confidentiality agreements of all authorized users of information systems. This agreement shall conform to all federal, state, regulatory, and union requirements.
Purpose	The purpose of this policy is to protect the assets of the organization by clearly informing staff of their roles and responsibilities for keeping the organization's information confidential.
Audience	ABC Co confidentiality agreement policy applies equally to all individuals granted access privileges to an ABC Co Information resources
Policy	This policy requires that staff sign a confidentiality policy agreement prior to being granted access to any sensitive information or systems. Agreements will be reviewed with the staff member when there is any change to the employment or contract, or prior to leaving the organization. The agreements will be provided to the employees by the Human Resource Dept.
Exceptions	At the discretion of the Information Security Officer, third parties whose contracts include a confidentiality clause may be exempted from signing individual confidentiality agreements.
Disciplinary Actions	Violation of this policy may result in disciplinary actions, which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or dismissal for interns and volunteers. Additionally, individuals are subject to civil and criminal prosecution.

Example: Policy for password use

Policy:

- All users must have a unique user ID and password that conforms to the company password standard
- Users must not share their password with anyone regardless of title or position
- Passwords must not be stored in written or any readable form
- If a compromise is suspected, it must be reported to the help desk and a new password must be requested



Standards:

- Minimum of 8 upper- and lowercase alphanumeric characters
- Must include a special character
- Must be changed every 30 days
- Password history of 24 previous passwords will be used to ensure passwords aren't reused

Example: Policy for password use

The Guideline:

- Take a phrase
  Up and At ‘em at 7!
- Convert to a strong password
  Up&atm@7!
- To create other passwords from this phrase, change the number, move the symbol, or change the punctuation mark

Procedure for changing a password

1. Press Control, Alt, Delete to bring up the log in dialog box
2. Click the “change password” button
3. Enter your current password in the top box
4. …

The OSI Security Architecture

- Security Attack: An action that compromises the security of information owned by an organization.
- Security Mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent or recover from a security attack.
- Security Service: A processing or communication service that enhances the security of the data processing systems and the information transfer of an organization.

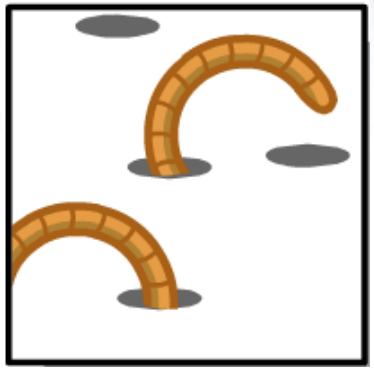
Threat and Attack (RFC 2828)

- Threat: A potential for violation of security, which exits when there is a circumstance, capability, action, or event that could breach security and cause harm.
- Attack: An assault on system security that derives from an intelligent threat.

  i.e., an intelligent act that is a deliverable attempt to evade security services and violet the security policy of a system

Security Attacks

- **Virus:** A malicious software which attaches to another program to execute a specific unwanted function on a computer.

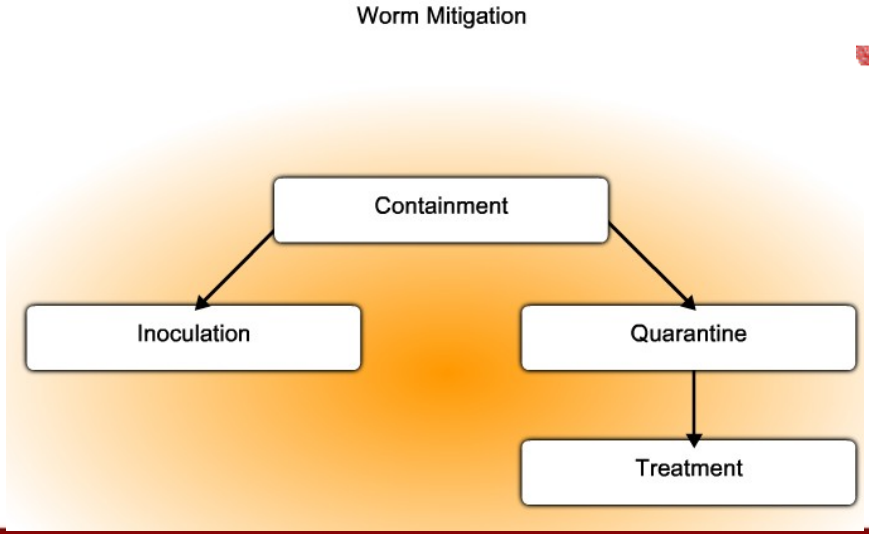


- **Worm:** executes arbitrary code and installs copies of itself in the memory of the infected computer, which then infects other hosts.

- **Trojan Horse:** An application written to look like something else. When a Trojan Horse is downloaded and opened, it attacks the end-user computer from within.

Security Attacks

- Three major components to most worm attacks:
  - Enabling vulnerability - A worm installs itself using an exploit mechanism (email attachment, executable file, Trojan Horse) on a vulnerable system.
  - Propagation mechanism - After gaining access to a device, the worm replicates itself and locates new targets.
  - Payload - Any malicious code that results in some action. Most often this is used to create a backdoor to the infected host.



- Response to a worm infection:
  - Containment - A policy for checking the expansion of worm to other files or devices.
  - Inoculation- Increase computer's Immunity.
  - Quarantine- Separate infected files.
  - Treatment- disinfect the worm from the files.

Security Attacks

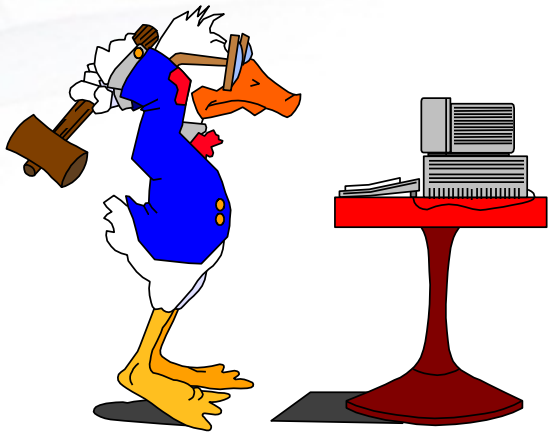
- The term Trojan Horse originated from Greek mythology.
- A Trojan Horse in the world of computing is malware software.
  - "Spread" via human engineering or by manually emailing.
  - It does not replicate itself, and it does not infect other files.

Classification of Trojan horse:

- **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)

Attack Methodologies

- Reconnaissance Attacks
  - unauthorized discovery and mapping of systems, services, or vulnerabilities.
- Access Attacks
  - exploit known vulnerabilities in authentication services, FTP services, and web services.



- Denial of Service Attacks
  - send extremely large numbers of requests over a network or the Internet.

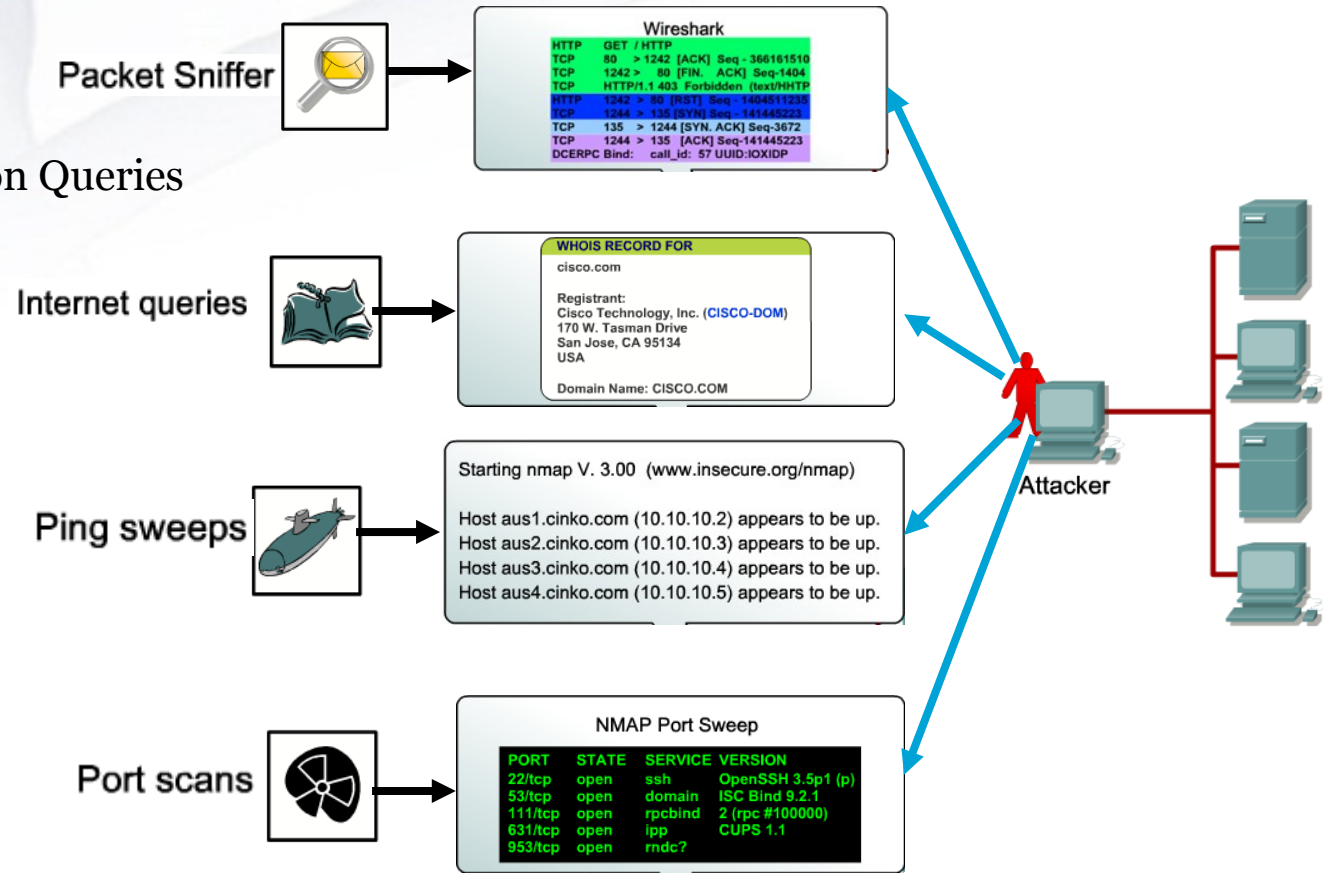
Reconnaissance Attacks

- Reconnaissance attacks are the precursor to further attacks.
- Various tools are used to gain access to a network
  - Packet Sniffers
  - Ping Sweeps
  - Port Scans
  - Internet Information Queries

Reconnaissance

Some network packets in unencrypted plaintext.

Numerous freeware and shareware packet sniffers.



Reconnaissance Attacks

- Reconnaissance Attacks can be mitigated in several ways:

Techniques Available for Reconnaissance Attack Mitigation Include:

- Implement authentication to ensure proper access.
- Use encryption to render packet sniffer attacks useless.
- Use anti-sniffer tools to detect packet sniffer attacks.
- Implement a switched infrastructure.
- Use a firewall and IPS.

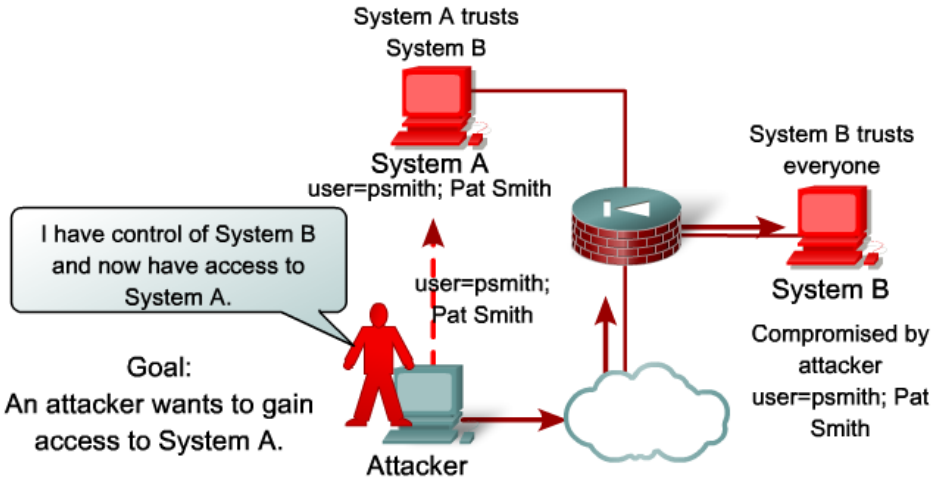
Access Attacks

- Five types of access attacks:
  - ✓ Password attack
  - ✓ Trust exploitation
  - ✓ Port redirection
  - ✓ Man-in-the-middle attack
  - ✓ Buffer overflow

Three methods for password attacks
- ✓ Brute-force attacks
- ✓ Trojan Horse Programs
- ✓ Packet sniffers

Network OS	Trust Models
Windows	Domains Active Directory (AD)
Linux and UNIX	Network File System (NFS) Network Information Service Plus (NIS+)

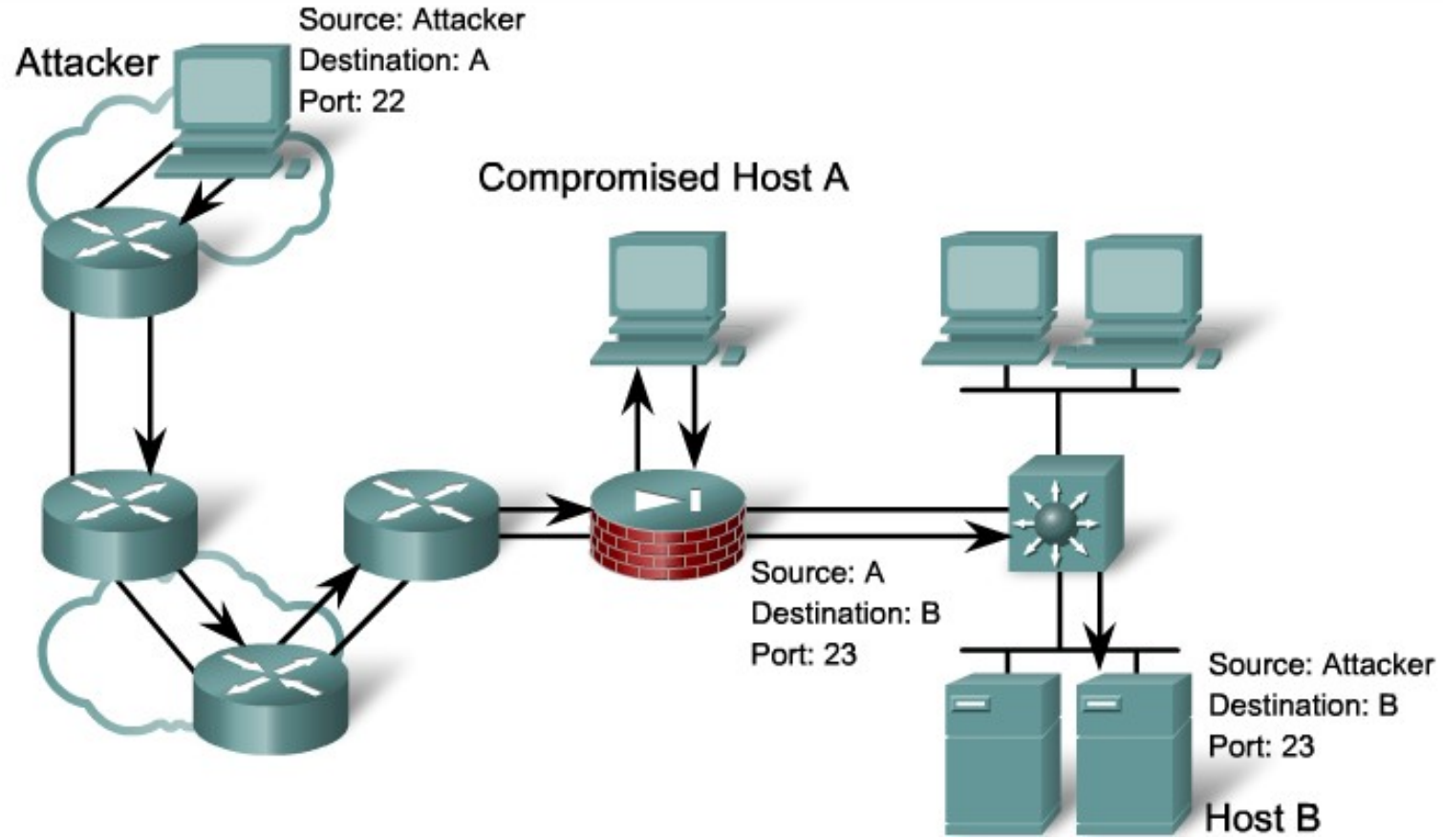
Trust exploitation



Access Attacks

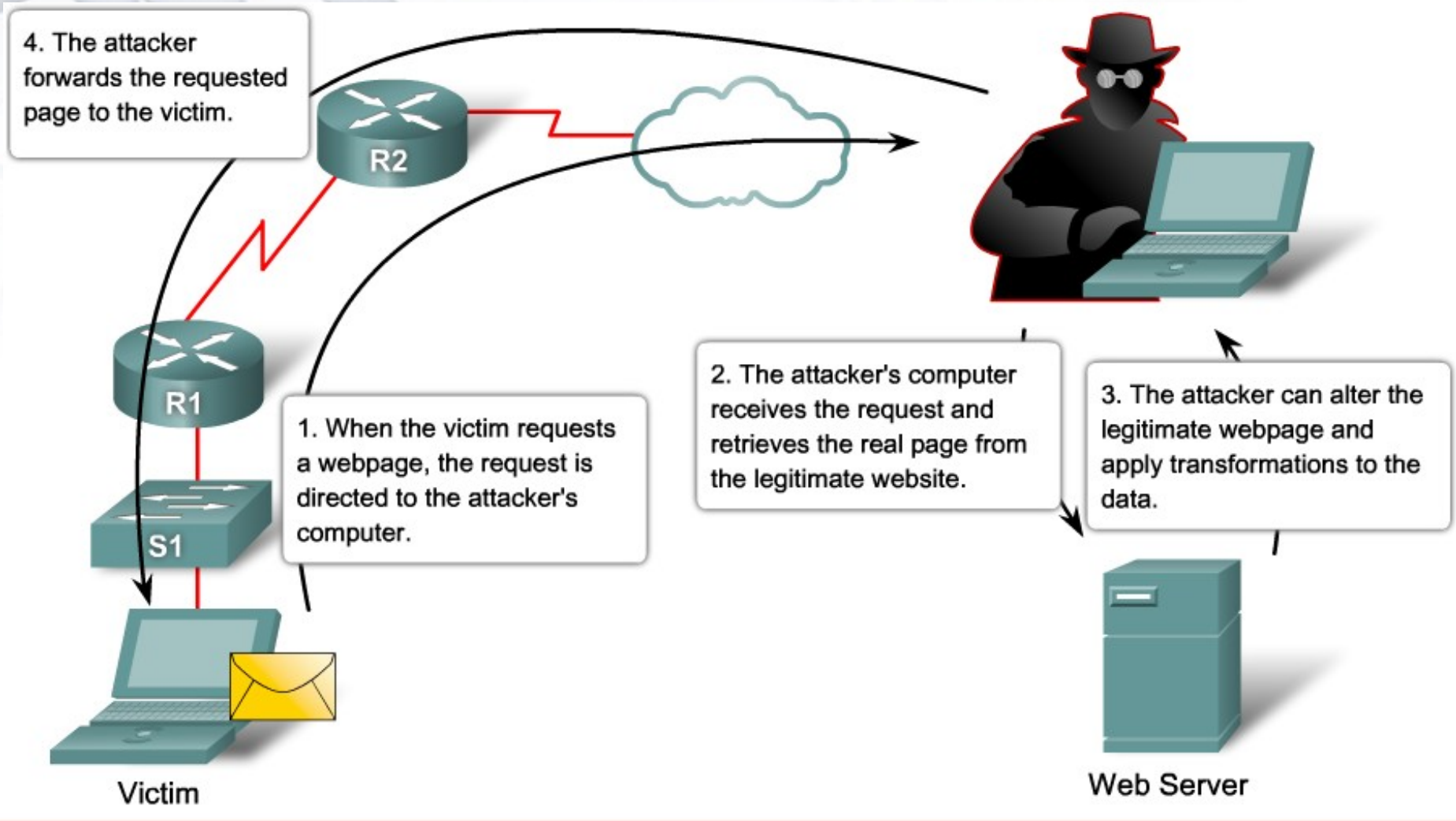
Port Redirection

Port redirection is a type of trust-exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped. It is mitigated primarily through the use of proper trust models. Anti-virus software and host-based IDS can help detect and prevent an attacker installing port redirecting utilities on the host.



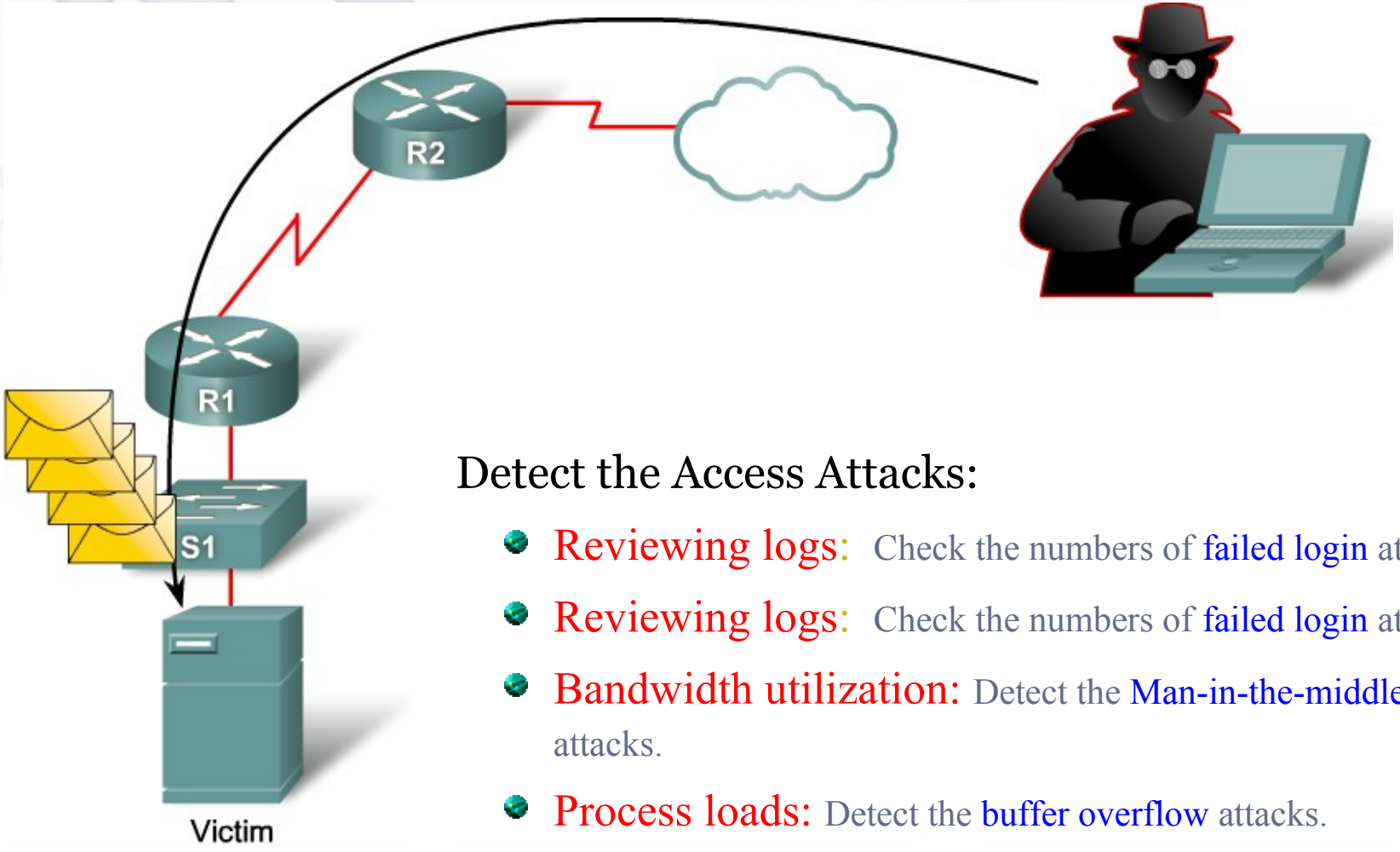
Access Attacks

- **Man-in-the-middle attack**



Access Attacks

Buffer Overflow Attack



Detect the Access Attacks:

- Reviewing logs: Check the numbers of failed login attempts.
- Reviewing logs: Check the numbers of failed login attempts.
- Bandwidth utilization: Detect the Man-in-the-middle attacks.
- Process loads: Detect the buffer overflow attacks.

Access Attacks

Several techniques are available for mitigating access attacks.

Strong password policy:

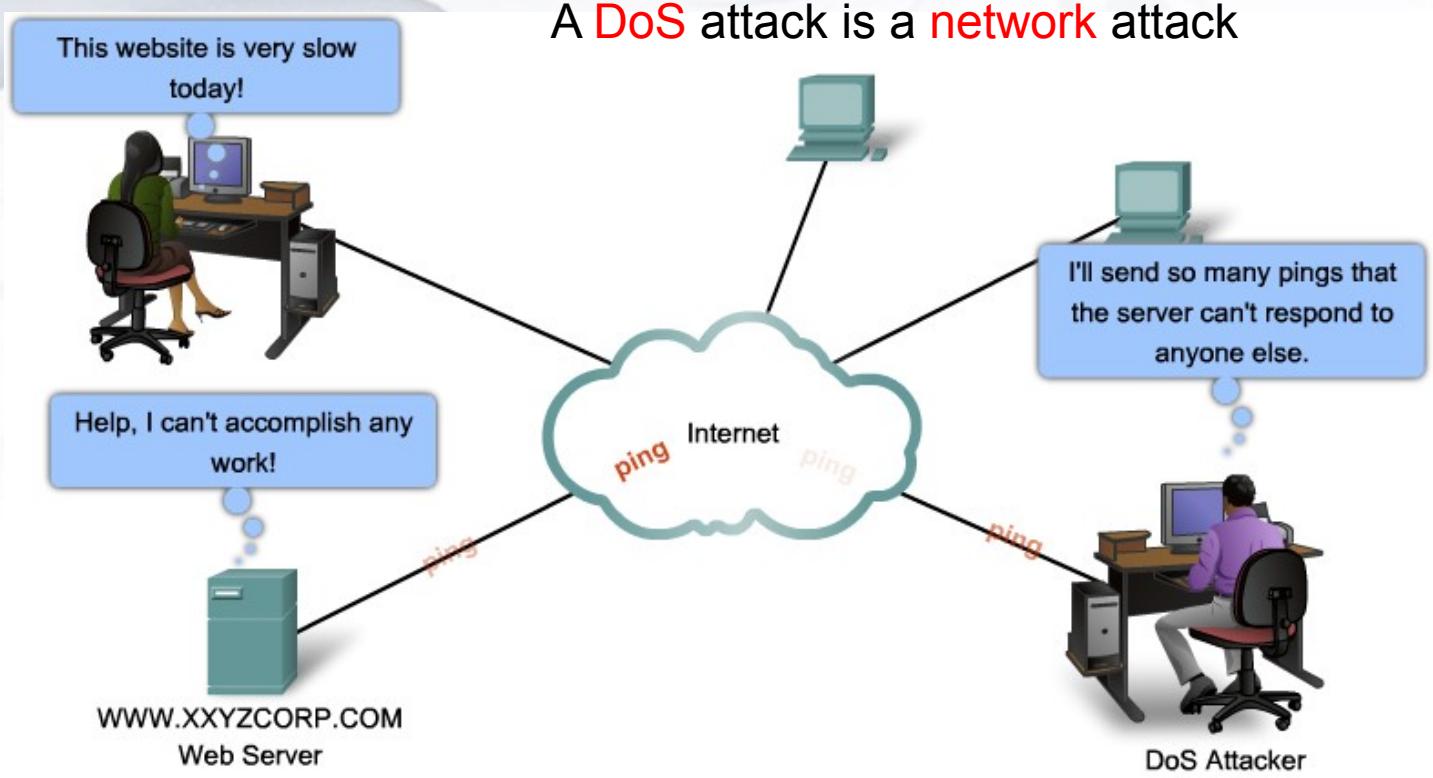
- Disabling accounts after a specific number of unsuccessful logins. This practice helps to prevent continuous password attempts.
- Not using plaintext passwords. Use either a one-time password (OTP) or encrypted password.
- Using strong passwords. Strong passwords are at least eight characters and contain uppercase letters, lowercase letters, numbers, and special characters.

Techniques Available for Access Attack Mitigation Include:

- Strong password security
- Principle of minimum trust
- Cryptography
- Applying operating system and application patches

Denial of Service (DoS) Attacks

A DoS attack is a network attack



compromise the availability of a network, host, or application

There are two major reasons a DoS attack occurs:

- A host or application fails to handle an unexpected condition.
- A network, host, or application is unable to handle an enormous quantity of data.

Denial of Service (DoS) Attacks

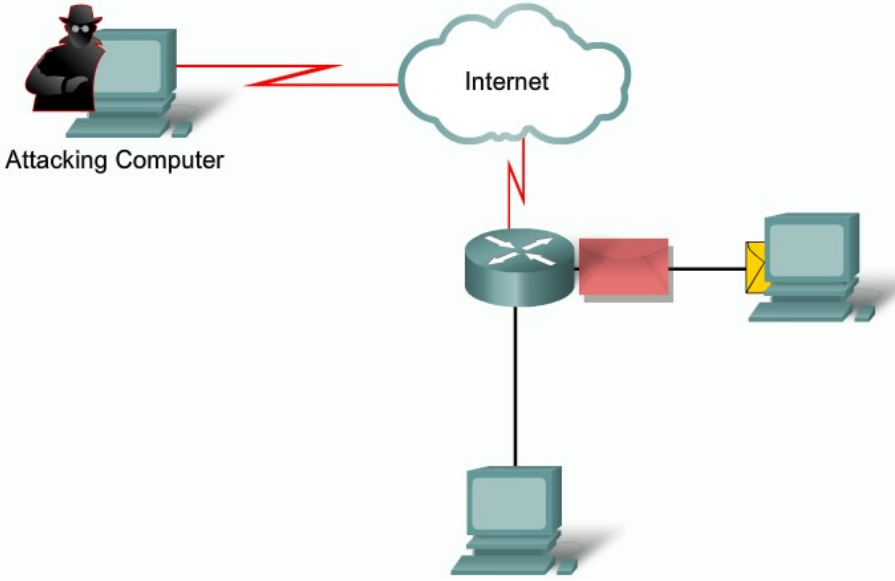
Some examples of DoS attacks

- Ping of death attack
- Smurf Attack
- TCP SYN Flood attack
- email attack
- Physical Infrastructure attacks

Denial of Service

The Symptoms of a DoS Attack Include:

- Unusually slow network performance (opening files or accessing web sites)
- Unavailability of a particular web site
- Inability to access any web site
- Dramatic increase in the number of spam emails received ("mail bomb")

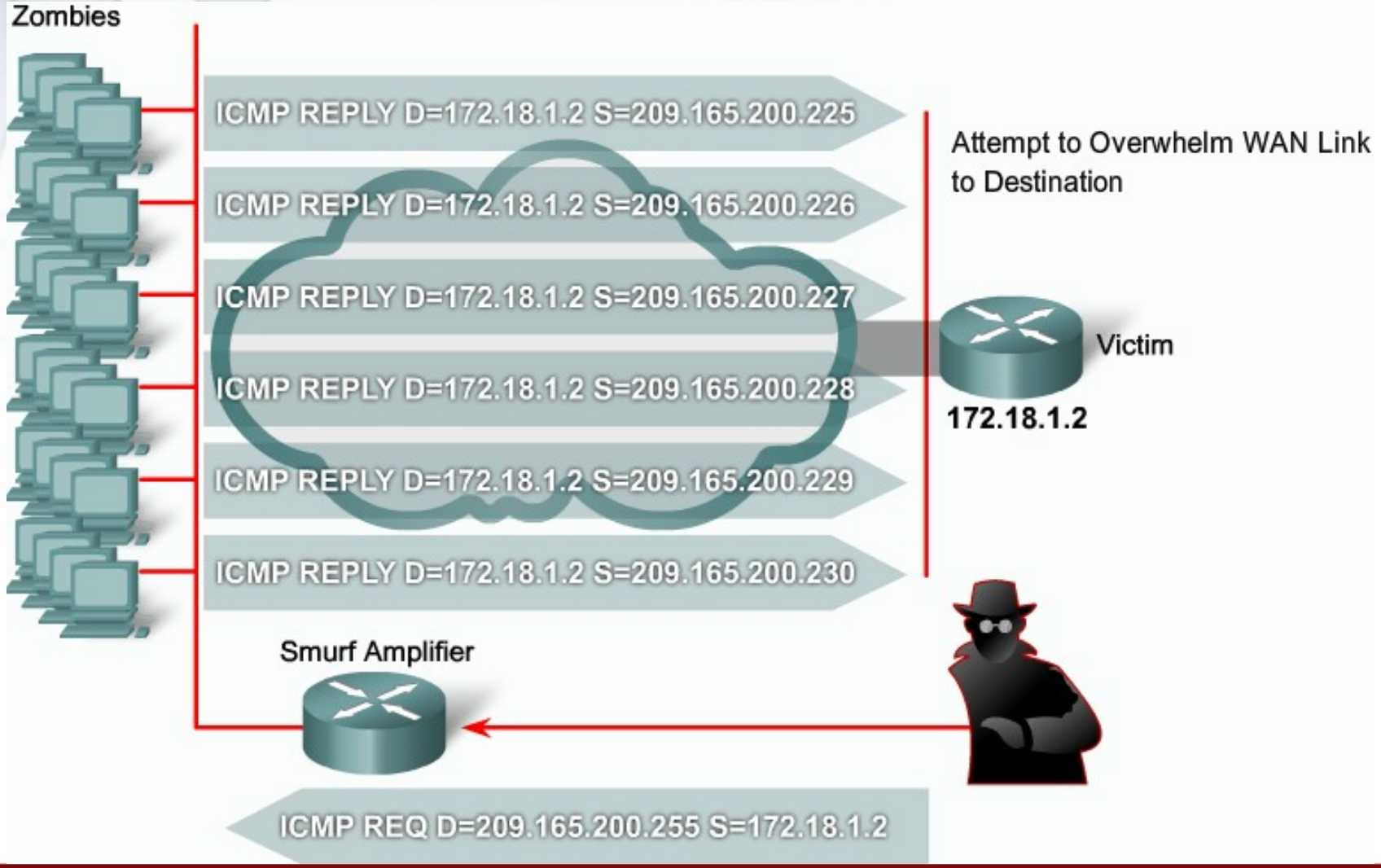


Ping of death attack

- A hacker sends an echo request in an IP packet larger than the maximum packet size of 65,535 bytes
- *ping -t -l 65550 192.168.1.1*

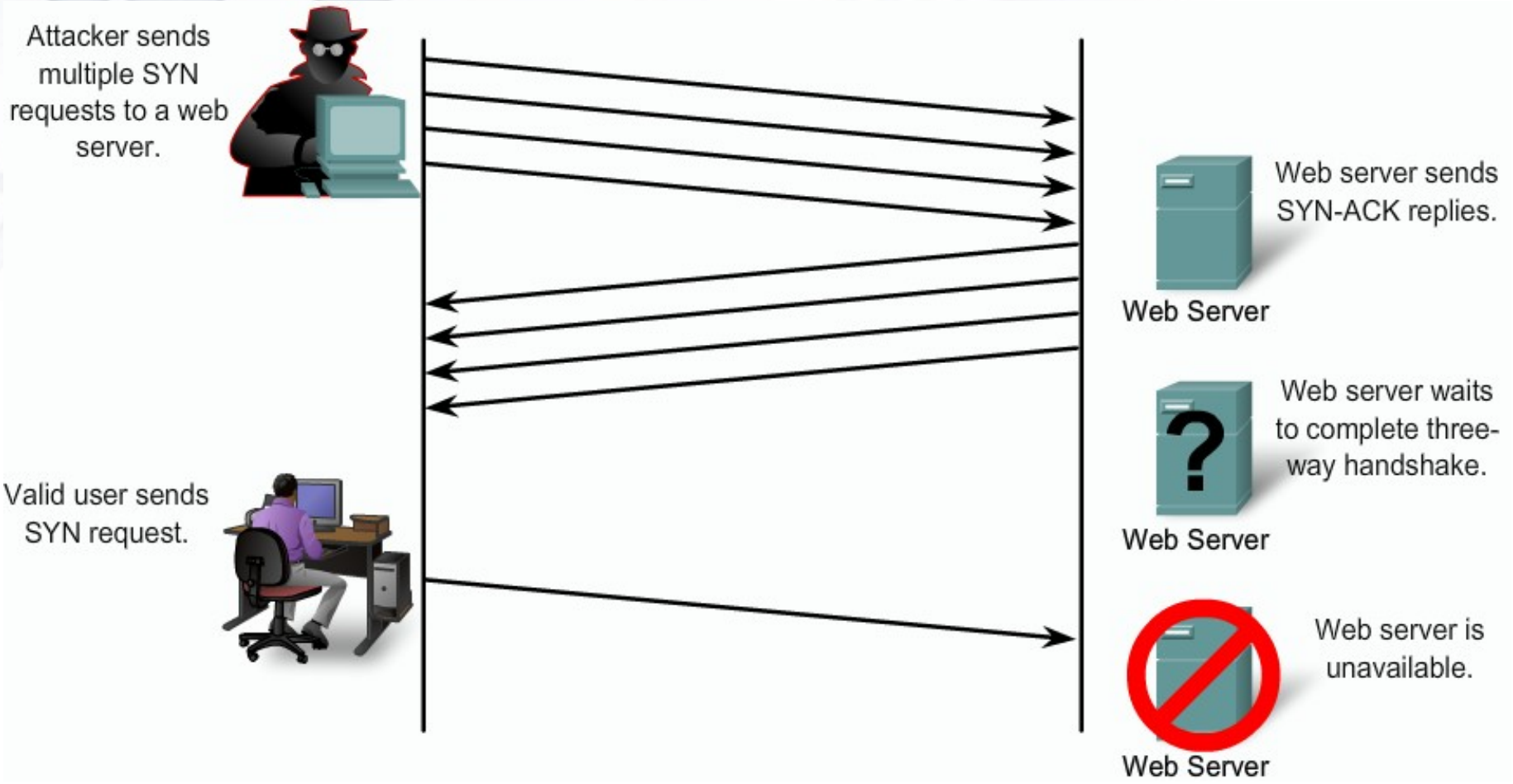
Denial of Service (DoS) Attacks

- Smurf Attack



Denial of Service (DoS) Attacks

- TCP SYN Flood attack



Denial of Service (DoS) Attacks

email attack:

- When using Microsoft Outlook, a script reads your address book and sends a copy of itself to everyone listed there, thus propagating itself around the Internet.
- The script then modifies the computer's registry so that the script runs itself again when restarted.

Physical infrastructure attack:

- Someone can just simply snip your cables! Fortunately this can be quickly noticed and dealt with.
- Other physical infrastructure attacks can include recycling systems, affecting power to systems and actual destruction of computers or storage devices.

Denial of Service (DoS) Attacks

- To date, hundreds of DoS attacks have been documented.
- There are five basic ways that DoS attacks can do harm:
  - Consumption of computational resources, such as bandwidth, disk space, or processor time
  - Disruption of configuration information, such as routing information
  - Disruption of state information, such as unsolicited resetting of TCP sessions
  - Disruption of physical network components
  - Obstruction of communication between the victim and others.

Mitigating DoS attack: Mitigating DoS attacks requires careful diagnostics, planning, and cooperation from Firewalls and ISPs.

- Firewalls and IPS
- Anti-spoofing technologies
- Quality of Service – traffic policing

Security Attacks

Social Engineering attacks:

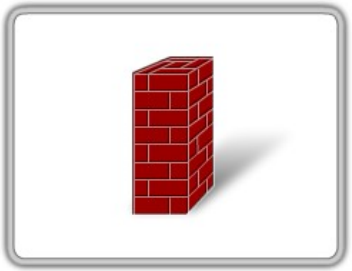
- Hacker-speak for tricking a person into revealing some confidential information
- An attack based on deceiving users or administrators at the target site
- Done to gain illicit access to systems or useful information
- The goals of social engineering are fraud, network intrusion, industrial espionage, identity theft, etc.

Few most popular tools used by network attackers:

- Enumeration tools (dumpreg, netview and netuser)
- Port/address scanners (AngryIP, nmap, Nessus)
- Vulnerability scanners (Meta Sploit, Core Impact, ISS)
- Packet Sniffers (Snort, Wire Shark, Air Magnet)
- Root kits
- Cryptographic cracking tools (Cain, WepCrack)
- Malicious codes (worms, Trojan horse, time bombs)
- System hijack tools (netcat, MetaSploit, Core Impact)

Best 10 practices for mitigating attacks

1. Keep patches up to date 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.


Firewall


Control Physical Access


Patches and Updates

Develop a Security Policy


Password Protect Sensitive Data


Anti-Virus

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.
8. Encrypt and password-protect sensitive data.
9. Implement security hardware and software firewalls, IPSs, virtual private network (VPN) devices, anti-virus software, and content filtering.
10. Develop a written security policy for the company.