Chapter 2

Security Attacks

Contents

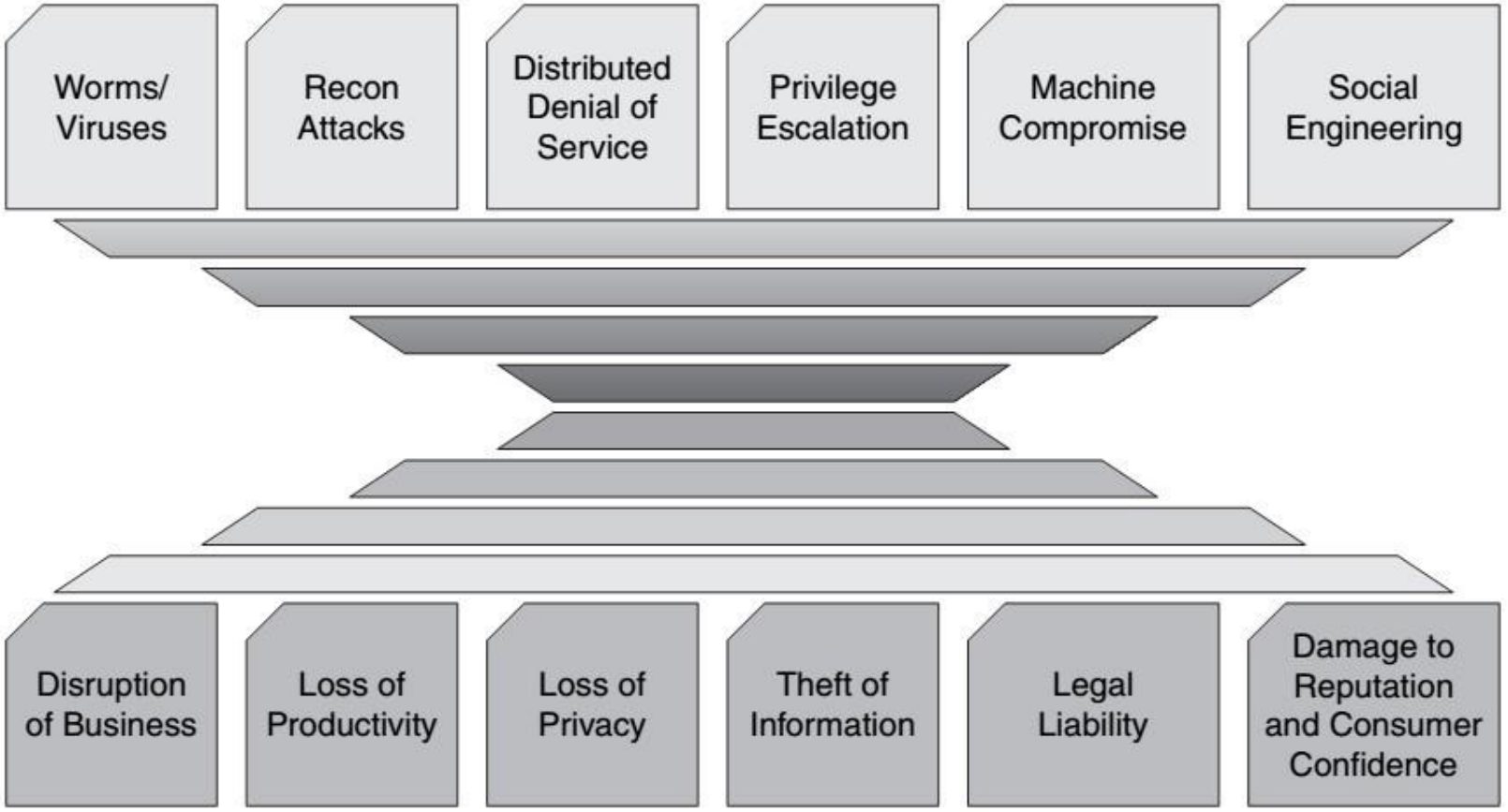
- Introduction to cyber attacks
- Typical Attacks Scenario and classes
- Classification of attacks on OSI layers
- Malicious software
- Common attacks signs and symptoms
- Mitigation of cyber attacks

Introduction to cyber attacks

Attacks

- An abstract concept which is represented by some pieces of information that may vary according to the situation
- Threat: outcome, probability
- Intrusion: elementary actions, composition rules
- Alert: FP probability, FN probability, alert/attack weight

Threats and Potential Consequences



Treats & Alerts

- Threats and alerts: used to select the *optimal* set of countermeasures for a specific attack scenario (according to a cost-benefit balance)
- Characterized by an amount of **uncertainty** (making decisions based on threat or alert)
- **Modeling a threat** → thwarting the attack before its occurrence by adding rules to the security policy.
- Alerts provide a strong means for reacting against intrusions

Hacking

- The ingenuity-driven activity of manipulating or modifying technologies without respect to their original functions, which should be distinguished from *cracking, a more destructive or transgressive form of* hacking.

Hacker (white hacker)

1. A person who enjoys learning the details of programming systems and how to stretch their capabilities, as opposed to most users who prefer to learn only the minimum necessary.

2. One who programs enthusiastically, or who enjoys programming rather than just theorizing about programming.

3. A person capable of appreciating hack value (q.v.).

4. A person who is good at programming quickly. Not everything a + produces is a hack.

5. An expert at a particular program, or one who frequently does work using it or on it; example: "A SAIL hacker". (Definitions 1 to 5 are correlated, and people who fit them congregate.)

6. A malicious or inquisitive meddler who tries to discover information by poking around. Hence "password hacker", "network hacker".

Hacker's dictionary, MIT.

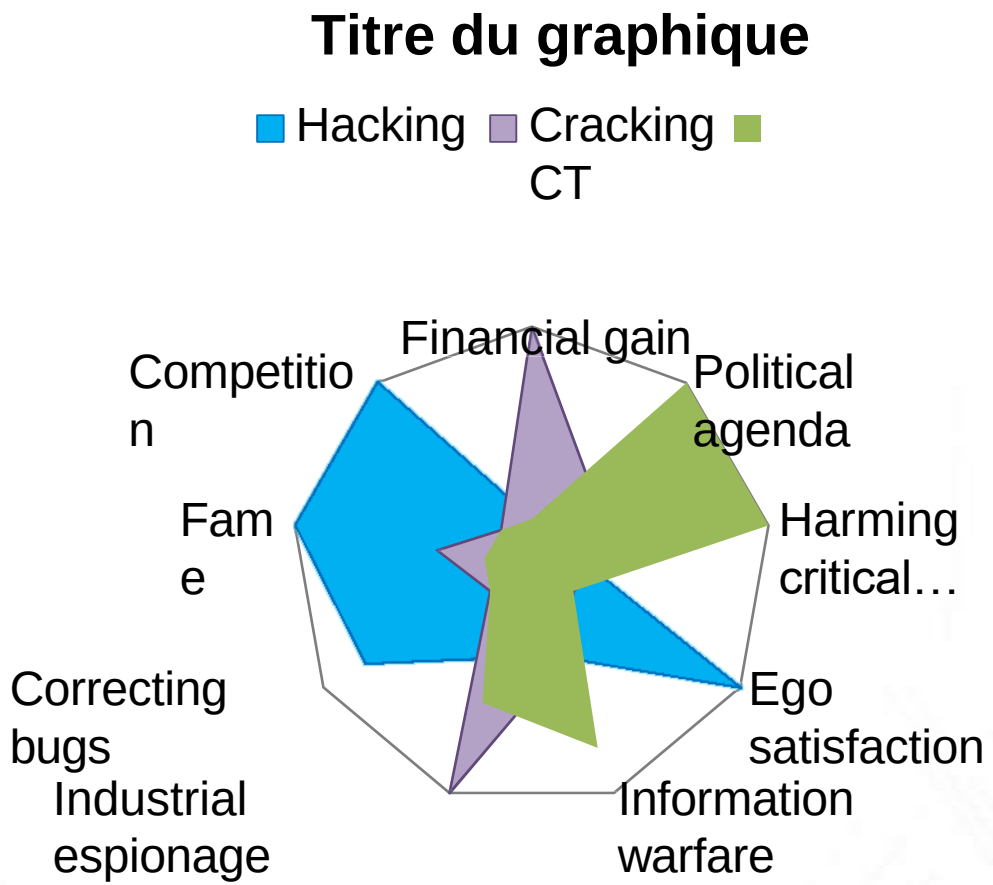
Cracker (black hacker)

- Someone who trespasses onto the computers or networks of other persons without authorization and with an intent to harm.
- The terms *hacker and hacking encompass only unauthorized* computer intrusions *not intended to cause damage, whereas cracker and cracking encompass only unauthorized computer intrusions intended to* cause damage.

Cyberterrorism

- An evolving body of activity that includes both acts *in cyberspace and using cyberspace* tools to create fear or panic, often done by subnational groups or clandestine agents and directed toward intimidating or coercing a government or some segment of the noncombatant civilian population, usually in furtherance of political or social objectives

Hacking – Cybercrime- Cyberterrorism



Typical attacks scenario and classes

Attack features

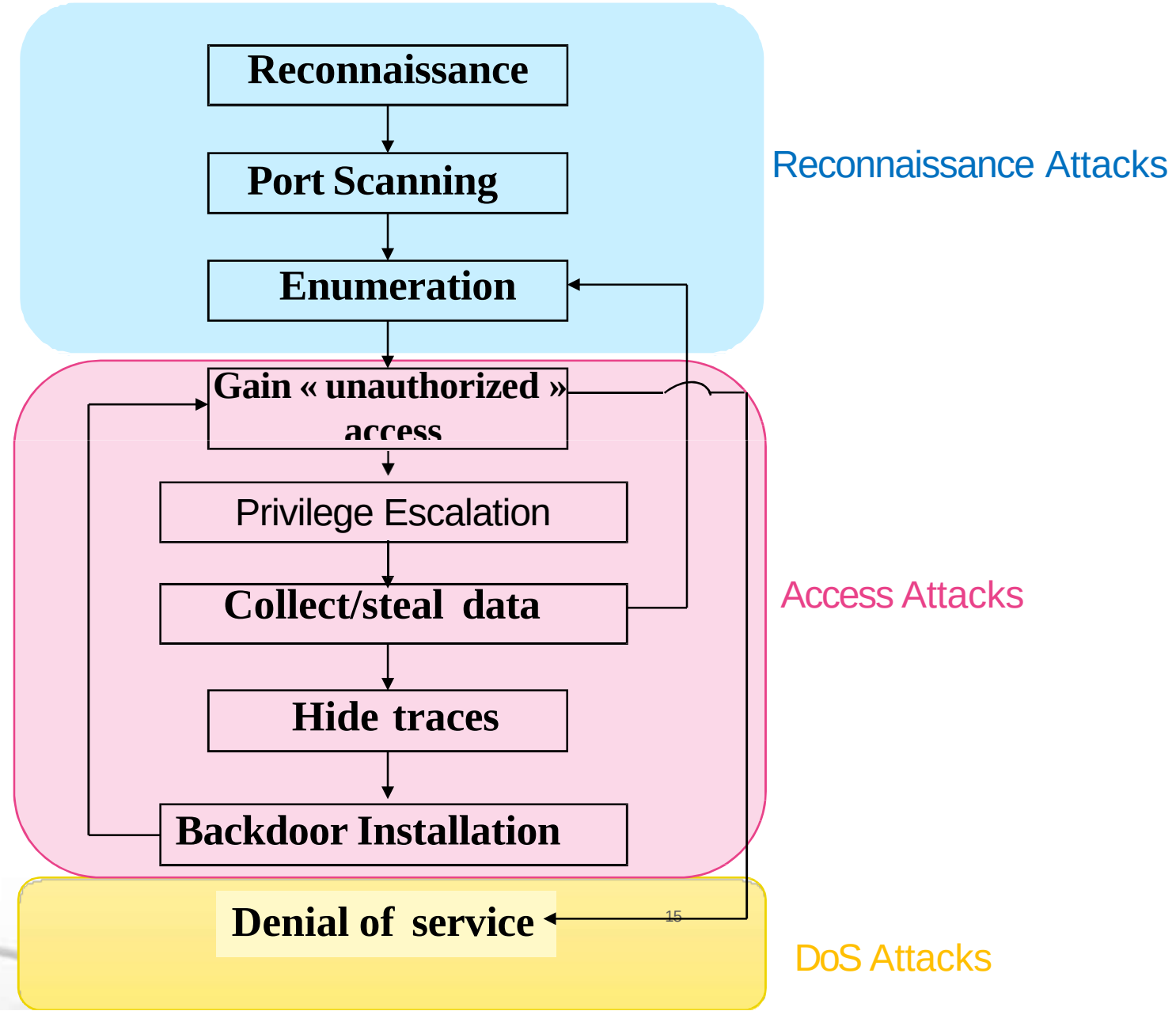
- **Coordination:** the attacker often combines multiple elementary attacks or uses several external resources difficult to detect, difficult to characterize
- **Incomplete knowledge**: an amount of uncertainty always characterizes the attack events
- **Versioning**: the attack scheme is kept modulo slight modifications

Attacks Classification

- Passive attacks: provide information about the information system Prevention

- Active attacks: involve some modification of the data stream or the creation of a false stream Prevention, Detection, Recovery.

Typical Attack Scenario



Stages of a Cyber Attack:

Reconnaissance – Attackers gather intelligence on their target.
Exploitation – Attackers exploit vulnerabilities (e.g., phishing, malware, SQL injection).
Privilege Escalation – Gaining unauthorized access to sensitive systems.
Data Exfiltration – Stealing, encrypting, or manipulating data.
Covering Tracks – Erasing logs and avoiding detection.

Attacks Types

Reconnaissance Attacks

- Involve the unauthorized discovery and mapping of systems, services, or vulnerabilities.
- Employ the use of packet sniffers and port scanners,

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. An access attack can be performed in many different ways.
- Employs a dictionary attack to guess system passwords.

Denial of Service Attacks (DoS)

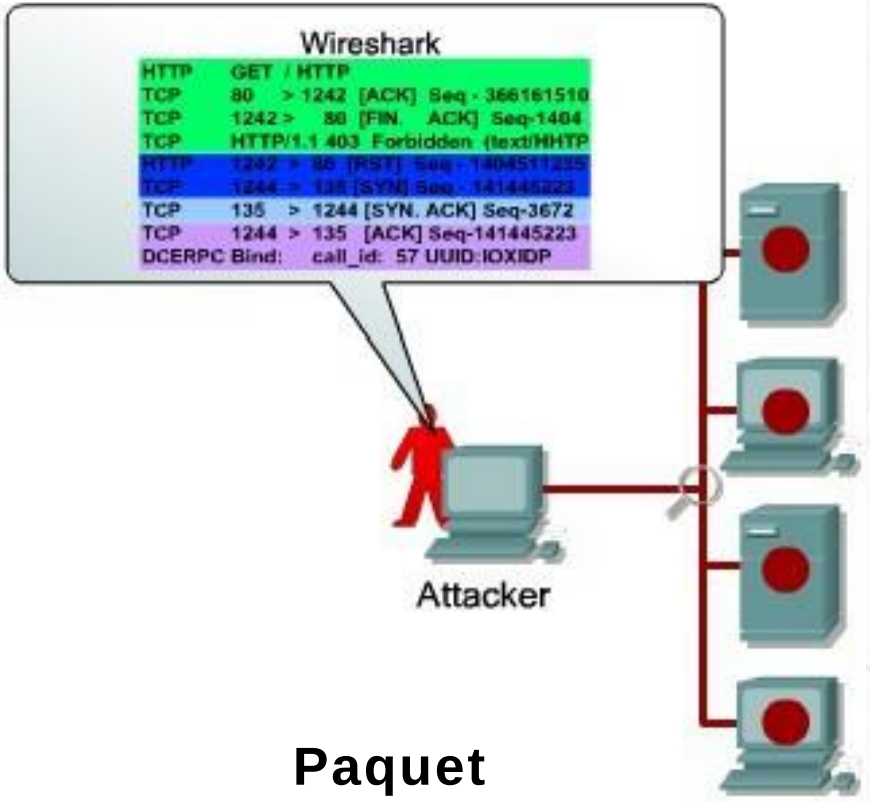
- Send extremely large numbers of requests over a network or the Internet.
- Cause the target device to run suboptimally.
- The attacked device becomes unavailable for legitimate access and use.

Reconnaissance attacks: Examples (1/3)

- Information gathering: Eavesdropping and packet sniffing .
- Malicious intruder:
  1) Conducts a ping sweep of the target network to determine which IP addresses are active.
  2) Determines which services or ports are available on the live IP addresses. (Nmap port scans)
  3) Queries the ports to determine the type and version of the application and operating system that is running on the target host.
- Reconnaissance attacks use various tools to gain access to a network:
  - Packet sniffers
  - Ping sweeps
  - Port scans
  - Internet information queries

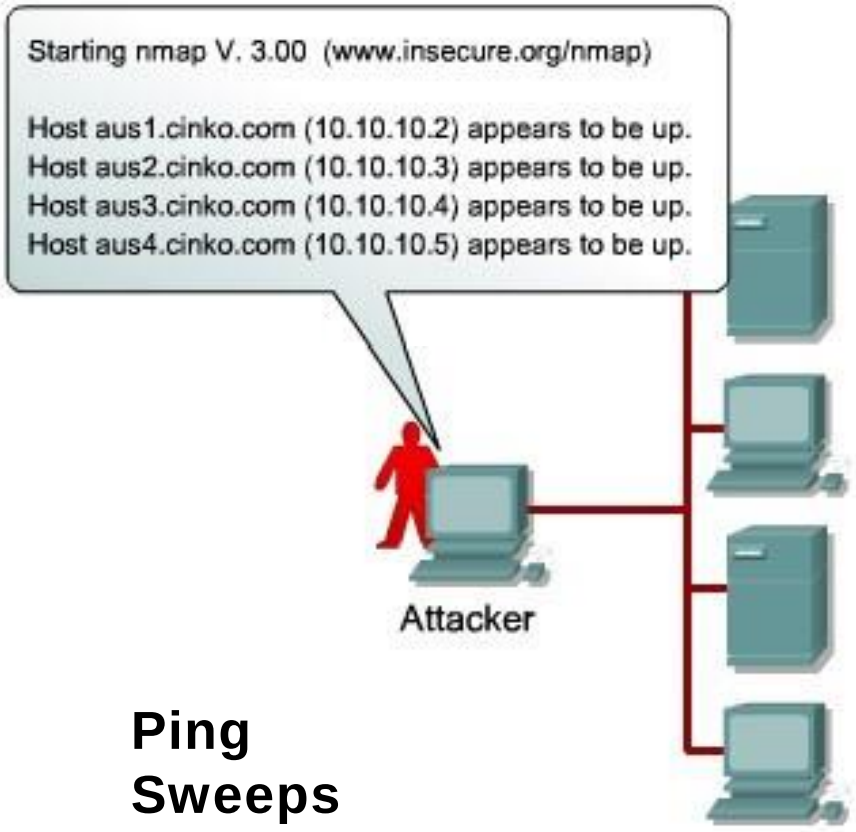
Reconnaissance attacks (2/3)

Internet Queries

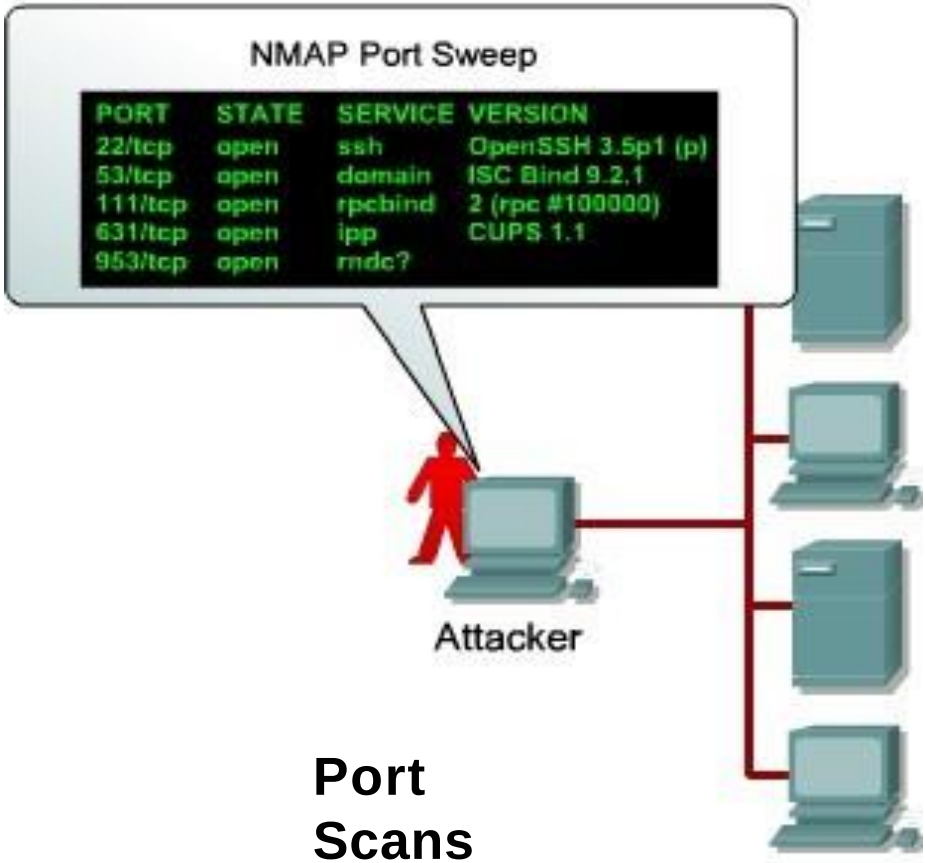


Paquet Sniffer

Reconnaissance attacks (3/3)



Ping Sweeps



Port Scans

Phishing & Social Engineering –

Tricking users into revealing credentials.

Real Scenario: In 2016, a hacker impersonated a Google and Facebook vendor, sending fake invoices that resulted in $100 million in losses.

Attack Steps:

- The hacker identified employees responsible for payments.
- Created fake email addresses mimicking real vendors.
- Sent fraudulent invoices, tricking finance teams into wire transfers.
- Money was transferred to overseas bank accounts.

Access attacks

- Hackers use access attacks on networks or systems for three reasons:
  - retrieve data,
  - gain access,
  - escalate access privileges.
- Password attacks (**brute-force attacks**, Trojan Horse programs, IP spoofing, packet sniffers)
- **Brute-force attack**: performed using a program that runs across the network and attempts to log in to a shared resource, such as a server.
- Gains access to a resource same access rights as the user whose account was compromised sufficient privileges can create a back door for future access

Types of Access Attacks

There are five types of access attacks:

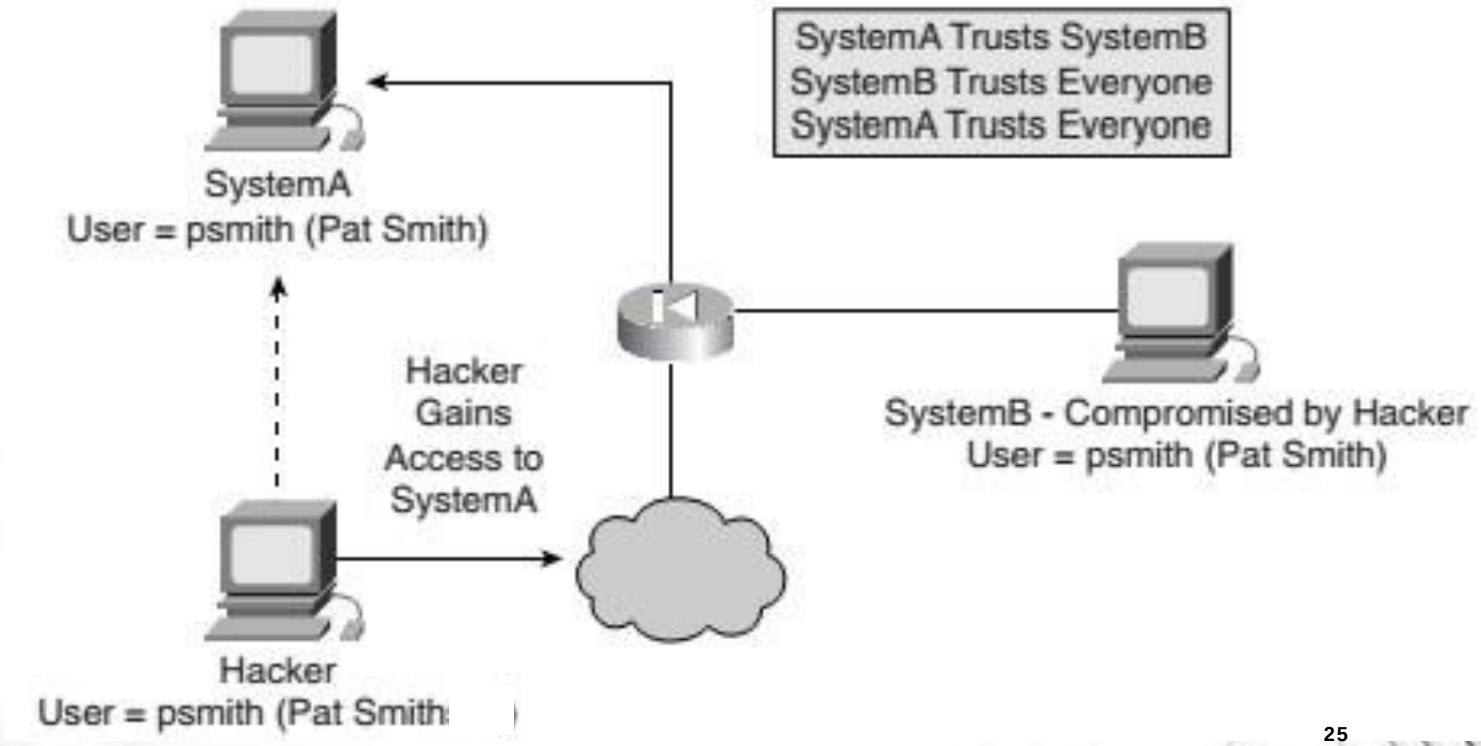
- Password attack
- Trust exploitation
- Port redirection
- Man-in-the-middle attack
- Buffer overflow

Password attack

- An attacker attempts to guess system passwords.
- A common example is a dictionary attack.
- Attackers can implement password attacks using different methods:
  - Brute-force attacks
  - Trojan Horse programs
  - Packet sniffers

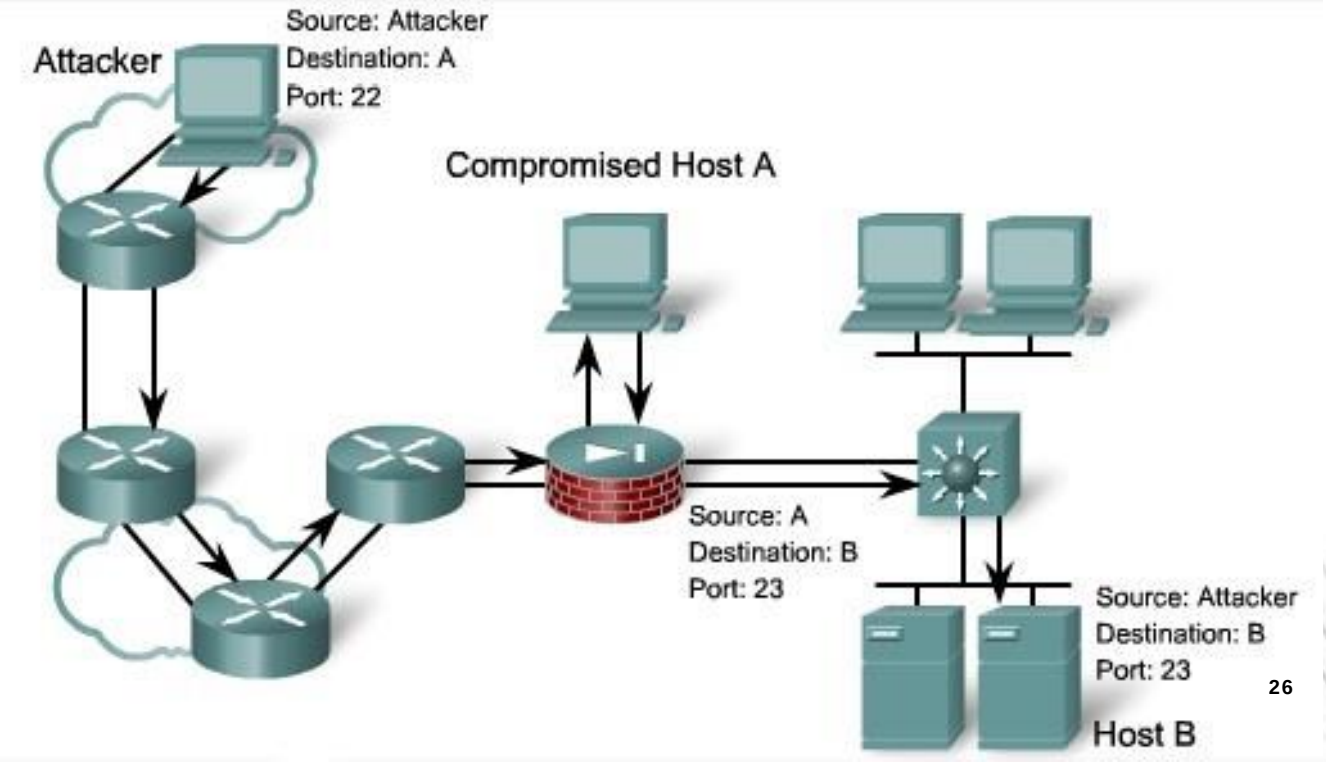
Trust exploitation

- **Trust exploitation** - An attacker uses privileges granted to a system in an unauthorized way, possibly leading to compromising the target.



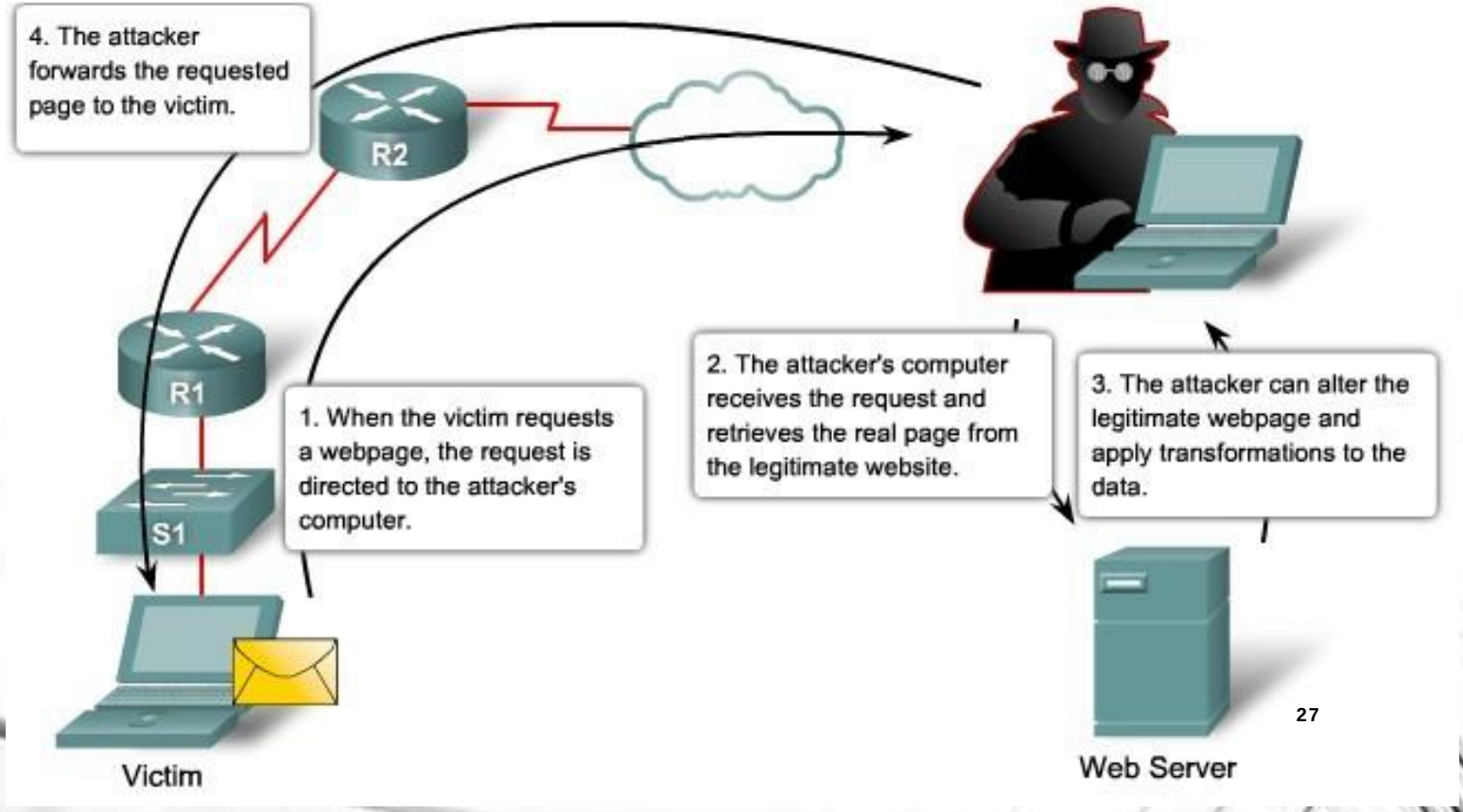
Port redirection

- A compromised system is used as a jump-off point for attacks against other targets.
- An intrusion tool is installed on the compromised system for session redirection.



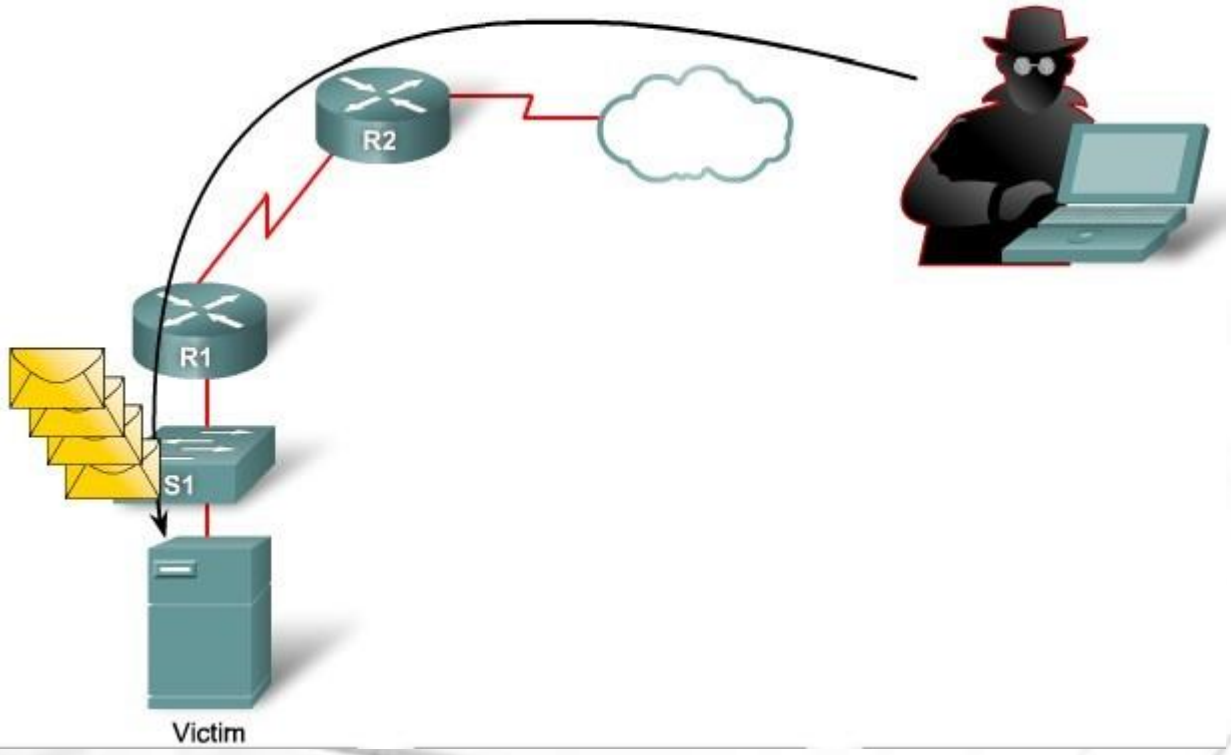
Man-in-the-middle attack

- An attacker is positioned in the middle of communications between two legitimate entities
  - read or modify the data that passes between the two



Buffer overflow

- A program writes data beyond the allocated buffer memory.
- A consequence of a bug in a C or C++ program valid data is overwritten or exploited to enable the execution of malicious code



Denial of Service Attacks (DoS)

- **DoS**: Interruption of service to users, devices, or applications.

- **Example** : generate large amounts of what appears to be valid network traffic ➔ saturates the network ➔ valid usertraffic cannot get through.

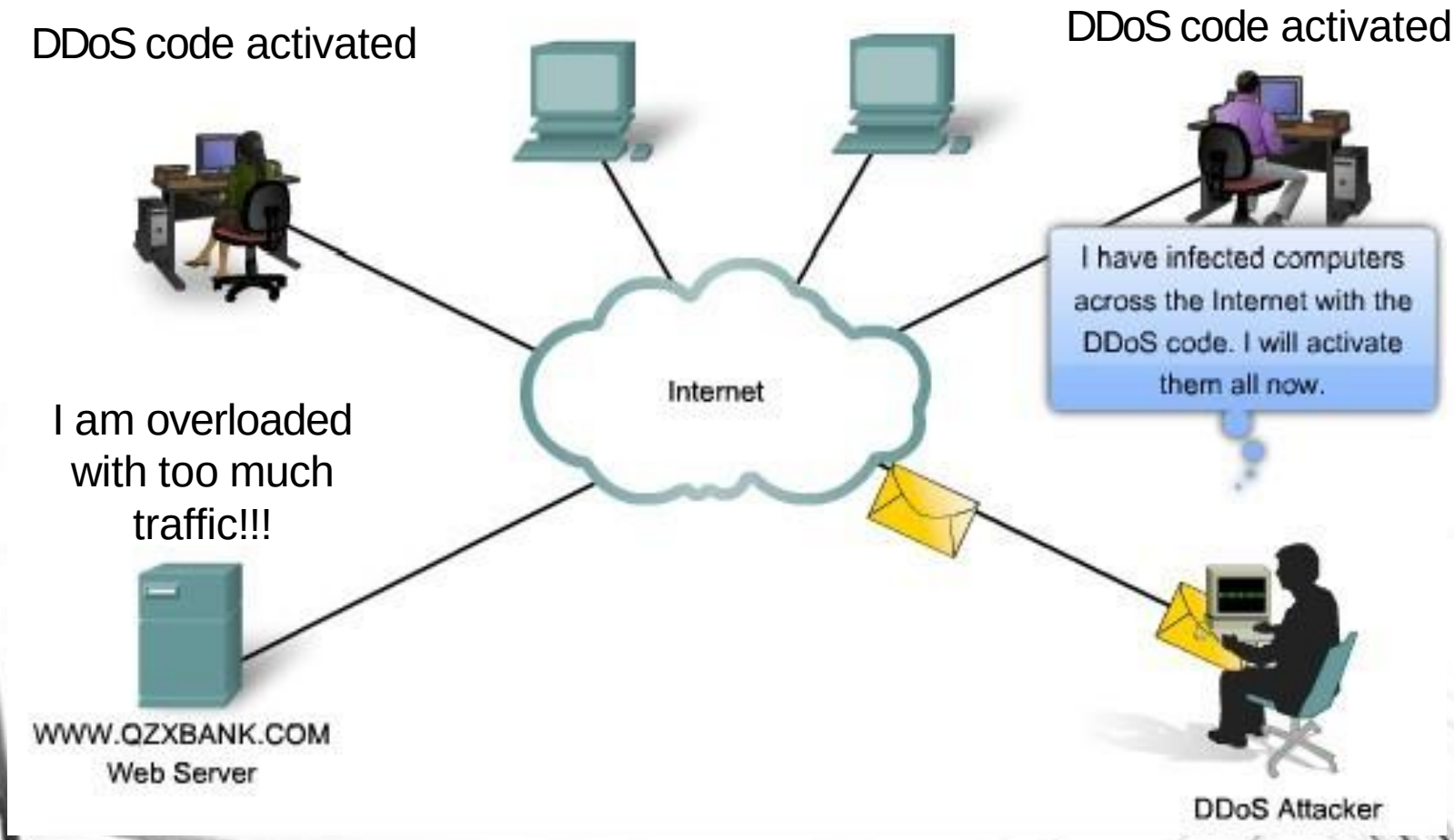
- There are two major reasons a DoS attack occurs:
  - A host or application fails to handle an unexpected condition
  - A network, host, or application is unable to handle an enormous quantity of data

DDoS (Distributed Denial of Service) – Overloading systems to disrupt service.

- **Real Scenario:** In 2016, the Mirai botnet attack took down major websites (Twitter, Netflix, Amazon).

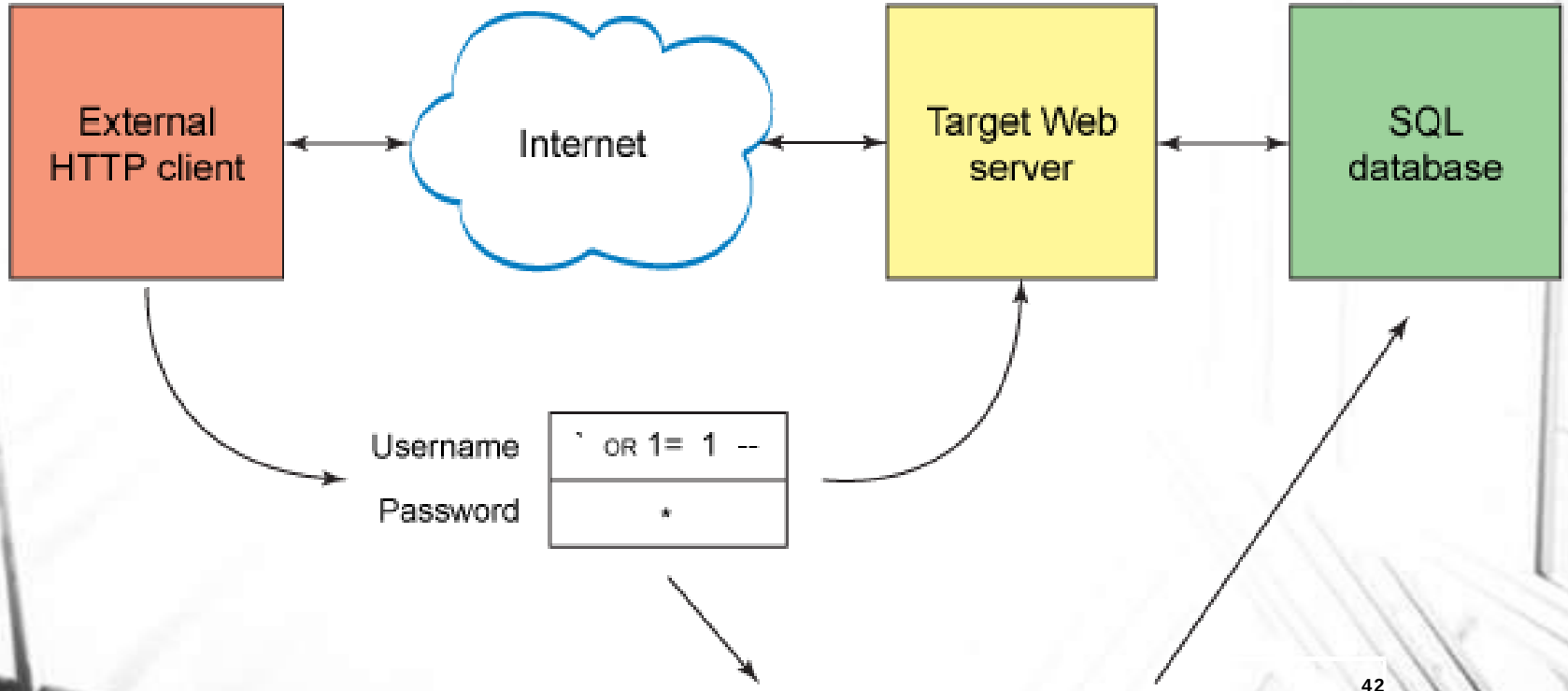
- **Attack Steps:**
  1. Malware infected IoT devices with weak passwords.
  2. Created a botnet army of compromised devices.
  3. Launched massive traffic floods at DNS providers.
  4. Websites relying on these services experienced outages.

Distributed Denial of Service Attack (DDoS)



SQL Injection

- SQL Injection – a subset of unverified user input vulnerability that injects malicious code (or SQL query) into strings. This code is executed when passed on to the SQL server.



SQL Injection

– Manipulating database queries to gain unauthorized access.

Real Scenario: In 2019, an attacker exploited an SQL Injection vulnerability in a government website, leaking millions of citizen records.

Attack Steps:

Attacker identified a vulnerable form input on a website.

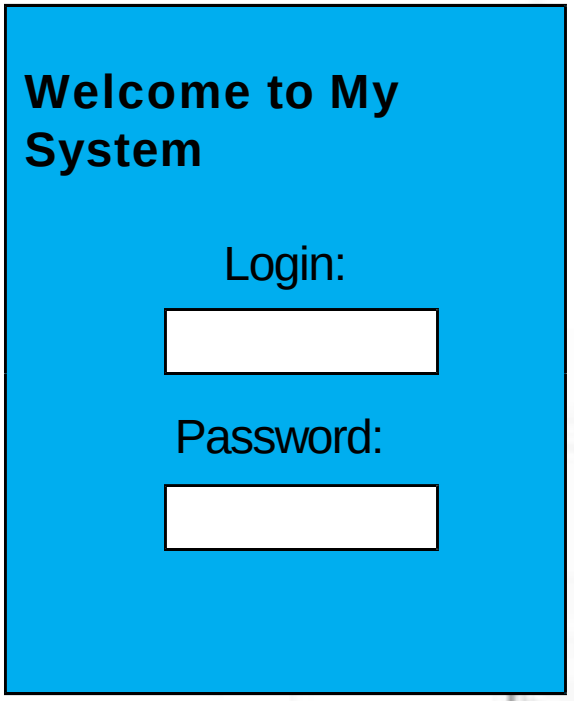
Injected malicious SQL code (' OR '1'='1), bypassing authentication.

Extracted sensitive database information such as passwords and personal data.

Used data for identity theft and financial fraud.

SQL Injection

- **Java Original**: "SELECT * FROM users_table WHERE username=" + "'" + username + "'" + " AND password = " + "'" + password + "'";
- **Inserted Password**: Aa' OR ''='
- **Java Result**: "SELECT * FROM users_table WHERE username='anyname' AND password = 'Aa' OR ' ' = ' ';
- **Inserted Password**: foo';DELETE FROM users_table WHERE username LIKE '%
- **Java Result**: "SELECT * FROM users_table WHERE username='anyname' AND password = 'foo'; DELETE FROM users_table WHERE username LIKE '%'
- **Inserted entry**: '|shell("cmd /c echo " & char(124) & "format c:")|'



Ransomware Attacks

– Encrypting data and demanding a ransom.

Real Scenario: WannaCry Ransomware Attack (2017) affected over 200,000 computers worldwide.

Attack Steps:

Attackers exploited an SMB protocol vulnerability in Windows.

Malware spread automatically across networks.

Encrypted files and displayed ransom notes demanding Bitcoin payments.

Organizations without backups were forced to pay ransom or lose data.

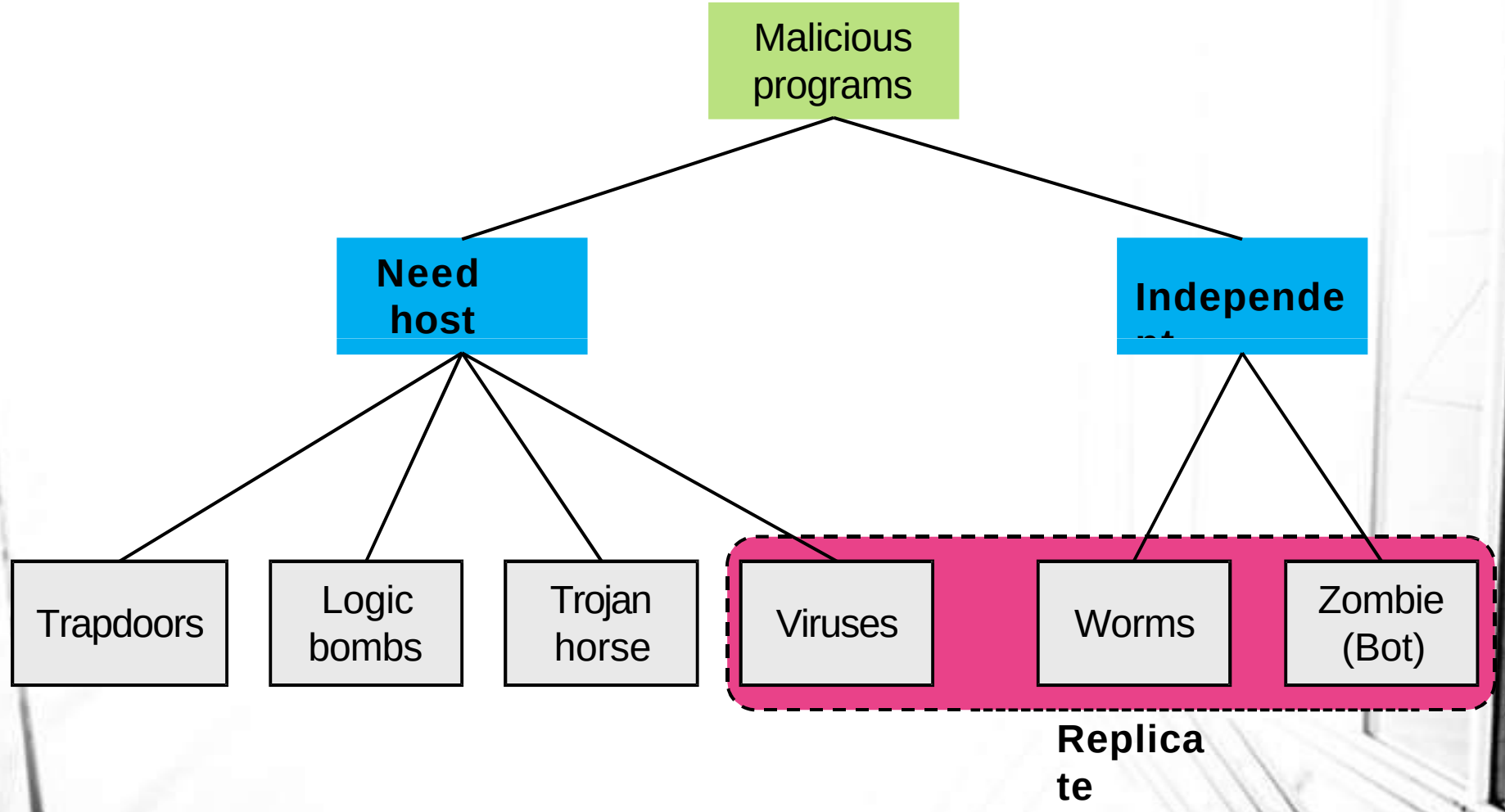
Malicious Software

Malware

- Programs exploiting computing system vulnerabilities
- Malware can be divided into two categories
  - Program fragments that need host program - **parasitic** malware
    - E.g. **viruses**, logic bombs, and backdoors – cannot exist independently of some actual application program, utility or system program
  - Independent self-contained programs
    - E.g. **worms**, bots – can be run directly by the operating system

- We differentiate between software threats that
  - Do not replicate – activated by a trigger (e.g., logic bombs, bot)
  - Do replicate/propagate itself (e.g., viruses and worms)

Malicious Software



Malware Terminology (1/2)

- **Virus:** A piece of code that inserts itself into a host program (infects it). It cannot run independently. It requires that its host program be run to activate it.
- **Worm:** A program that can run independently and can propagate a complete working version of itself onto other hosts on a network.
- **Logic bomb:** A program inserted into software by an intruder. It executes on specific condition (trigger). Triggers for logic bombs can include change in a file, by a particular series of keystrokes, or at a specific time or date.

```
legitimate code
        if date is Friday the 13th;
            crash_computer();
legitimate code
```

Malware Terminology (2/2)

- **Trojan horse:** Programs that appear to have one (useful) function but actually perform another (malicious) function, without the user's knowledge.

- **Backdoor (trapdoor):** Any mechanism that bypasses a normal security check. It is a code that recognizes for example some special input sequence of input; programmers can use backdoors legitimately to debug and test programms.

```
username = read_username();
password = read_password();
if username is "112_h4ck0r"
          return ALLOW_LOGIN;
if username and password are valid
          return ALLOW_LOGIN
else return DENY_LOGIN
```

Computer Virus

- A **self-replicating** code attached to another program
- **Infects** another (host) program with a copy of itself
- It executes secretly when the host program is run
- Propagates and carries a payload
  - Carries code to make copies of itself
  - As well as code to perform some covert and malicious task

Virus Operation

- During lifetime, typical virus goes through four phases
  - **Dormant** phase
    - Virus is idle, waiting for trigger event (e.g., date, time, program)
  - **Propagation phase**
    - Virus places a copy of itself into other programs or system areas on disk
    - The copy may not be identical – it morphs to avoid detection
  - **Triggering phase**
    - Virus is activated by some trigger event to perform intended function
    - Some system event, targeted # copies of itself has been reached
  - **Execution phase**
    - The intended function is performed
    - E.g., showing a message on the screen, destroying programs or data files
- Virus details are hardware/OS specific

Virus Structure

- Major components
  - **Infection mechanism** – the code that enables replication
  - **Trigger** – te event that makes payload activate
  - **Payload** - what it does, malicious or benign
- Prepended / Postpended / Embedded

- The key to virus operation is that
  - The infected program when invoked, first executes virus code then original program code
- Prevention: block initial infection (difficult) or propagation (with **access controls** as in early UNIX systems)

Zero-Day Exploits

– Attacking unpatched software vulnerabilities.

- **Real Scenario:** The Stuxnet worm (2010) targeted Iranian nuclear facilities.
- **Attack Steps:**

1. Malware was introduced via infected USB drives.
2. Exploited zero-day vulnerabilities in Windows.
3. Took control of industrial control systems.
4. Sabotaged uranium enrichment processes by altering centrifuge speeds.

End of lecture