# Networking

# Lecture
# Network Security

-Introduction
- Security Goals
-Security Terminologies
-Threats
-Attack Methods
-Security Policy
-Firewalls

# Introduction

- People use networks to exchange sensitive information with each other.
- People purchase products and do their banking over the Internet.
- Network Security is a shared responsibility that each person must accept when they connect to the network.

# Defining Network Security

- Network security is the implementation of security devices, policies, and processes to prevent the unauthorized access to network resources or the alteration or destruction of resources or data.

- Security involves protecting resources:
  - End-user resources
  - Network resources
  - Server resources
  - Information storage resources

# Balancing Business Need with Security Requirement

# What are Security Goals?

- Security goals can be defined:
  - Depending on the application environment
  - Technical

- Security Goals are also called Security Objectives

# Security Goals Technically Defined

# Security Goals Technically Defined

- **Confidentiality**
  - Ensuring that information is not allowed to unauthorized persons
  - Data transmitted or stored should only be allowed to an authorized persons
- **Integrity**
  - It should be possible to detect any modification of data
- **Availability**
  - Ensuring that authorized users are not denied access to information and resources

# Security goals in different environments

- Banking
- Electronic trading
- Medical
- Private Networks

# Security goals in different environments

- **Banking**
  - Protect against fraudulent or accidental modification of transactions
  - Protect PINs from disclosure
  - Ensure customers privacy
- **Electronic trading**
  - Assure source and integrity of transactions
  - Protect corporate privacy
  - Provide legally binding electronic signatures on transactions

# Security goals in different environments

- **Medical**
  - Protect privacy
  - Confidentiality is most critical
- **All Networks**
  - Prevent outside penetrations (who wants hackers?)

# Security Terminologies

- Assets
- Threat
- Vulnerability
- Risk
- Exploits
- Impacts

# Risks of Network


# Risks of Network

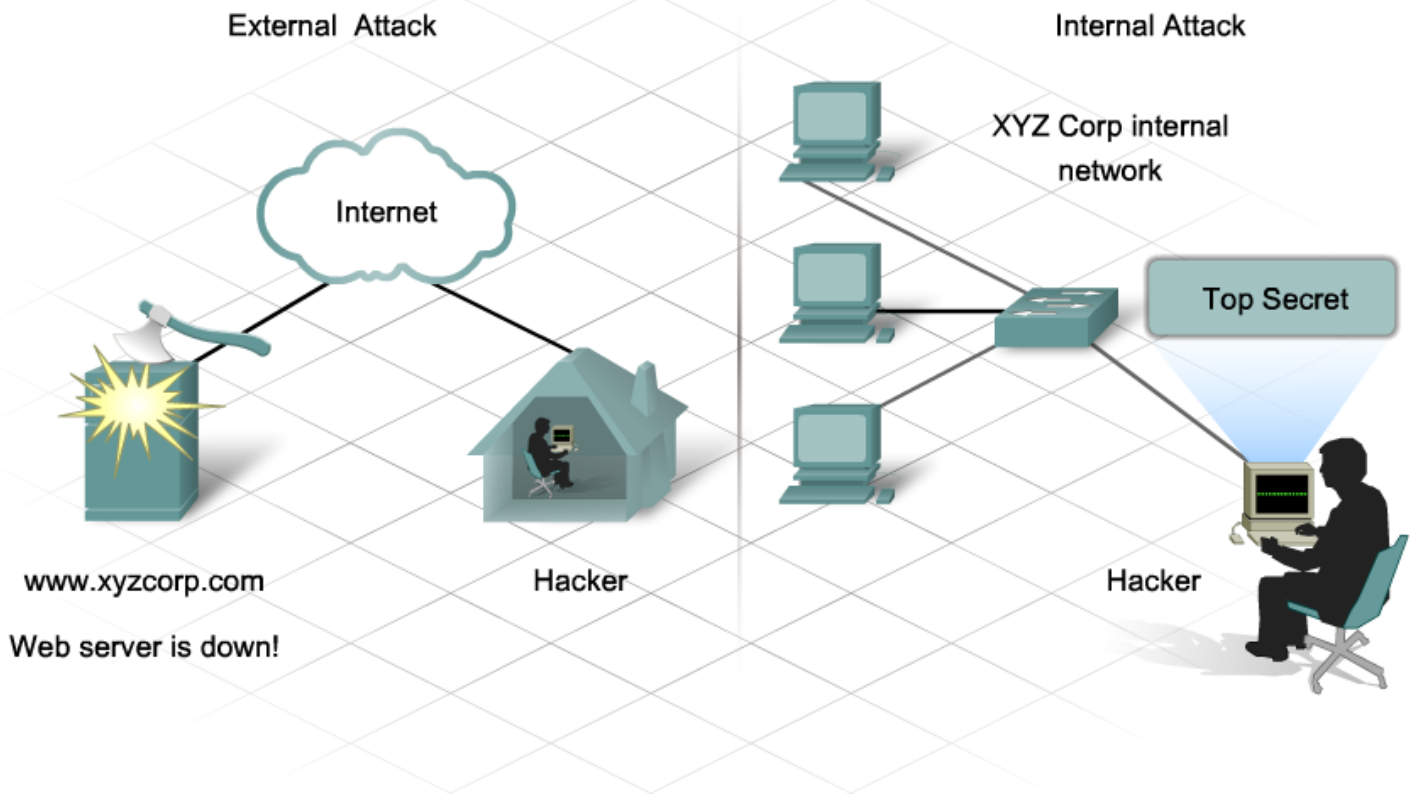
- Information Theft
  - Breaking into a computer to obtain confidential information. Information can be used or sold for various purposes.
- Data Loss and Manipulation
  - Breaking onto a computer to destroy or change data records.

# Risks of Network

- Identity Theft
  - Personal Information is stolen for the purpose of taking over someone's identity. Using this information anyone can obtain legal documents, apply for credits and make unauthorized online activities.

- Disruption of Service
  - Preventing authorized users from accessing services to which they should be access.

# Sources of Network



# Social Engineering

- Social engineering is a term that refers to the ability of something or someone to influence the behavior of a group of people.

# Social Engineering

## Social Engineering Explained

Also known as human hacking, social engineering is the manipulation of someone to divulge confidential information that can be used for fraudulent purposes.

1

The social engineer gathers information about their victims.

2

The social engineer poses as a legitimate person and builds trust with their victims.

3

The social engineer gathers information about their victims.

4

The social engineer poses as a legitimate person and builds trust with their victims.

# Social Engineering


Scareware


Email hacking

Access tailgating

Phishing


DNS spoofing


Baiting

Physical breaches

Pretexting

Watering hole attacks

Quid pro quo

## Social engineering explained

### 1. Preparation

Social engineer researches their victim

### 2. Build Assurance

Social engineer poses as genuine person in attempt to build trust

### 3. Persuasion

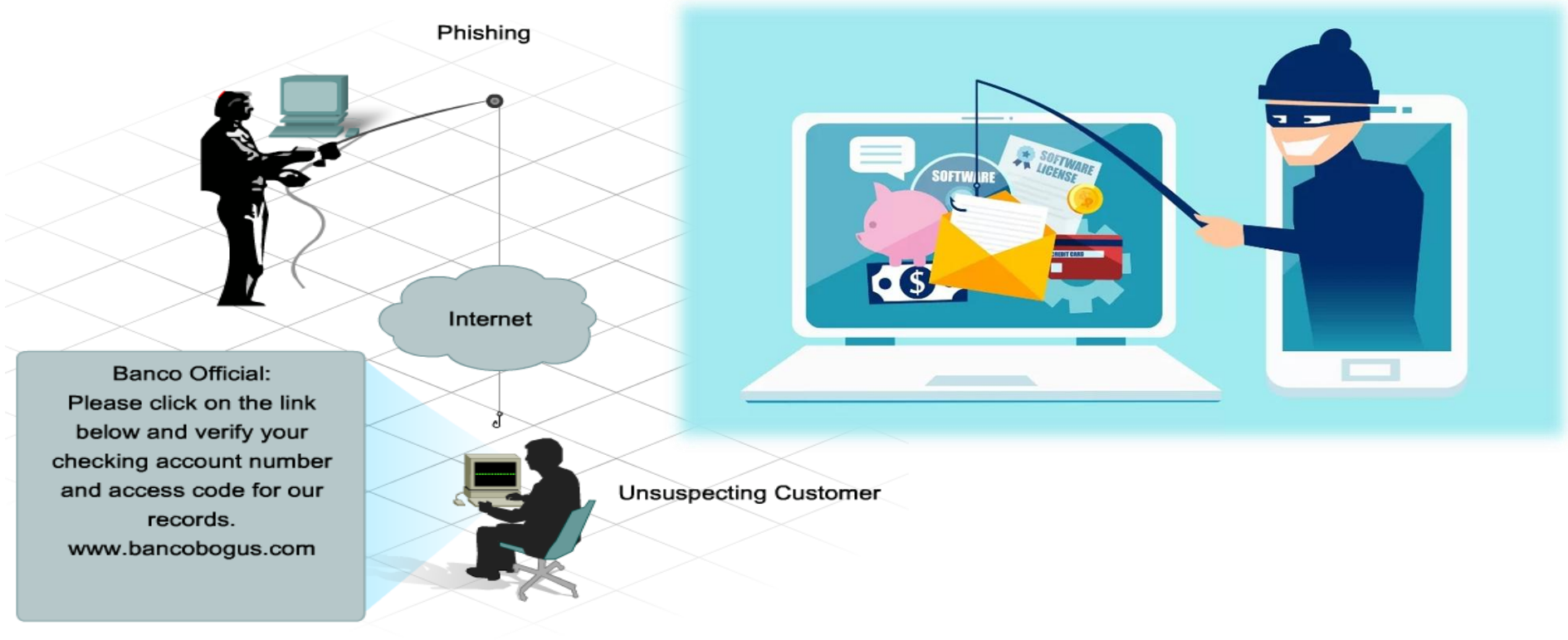
Social engineer manipulates victim into releasing private data

### 4. Exploitation

Social engineer stops communication with victim and makes their attack

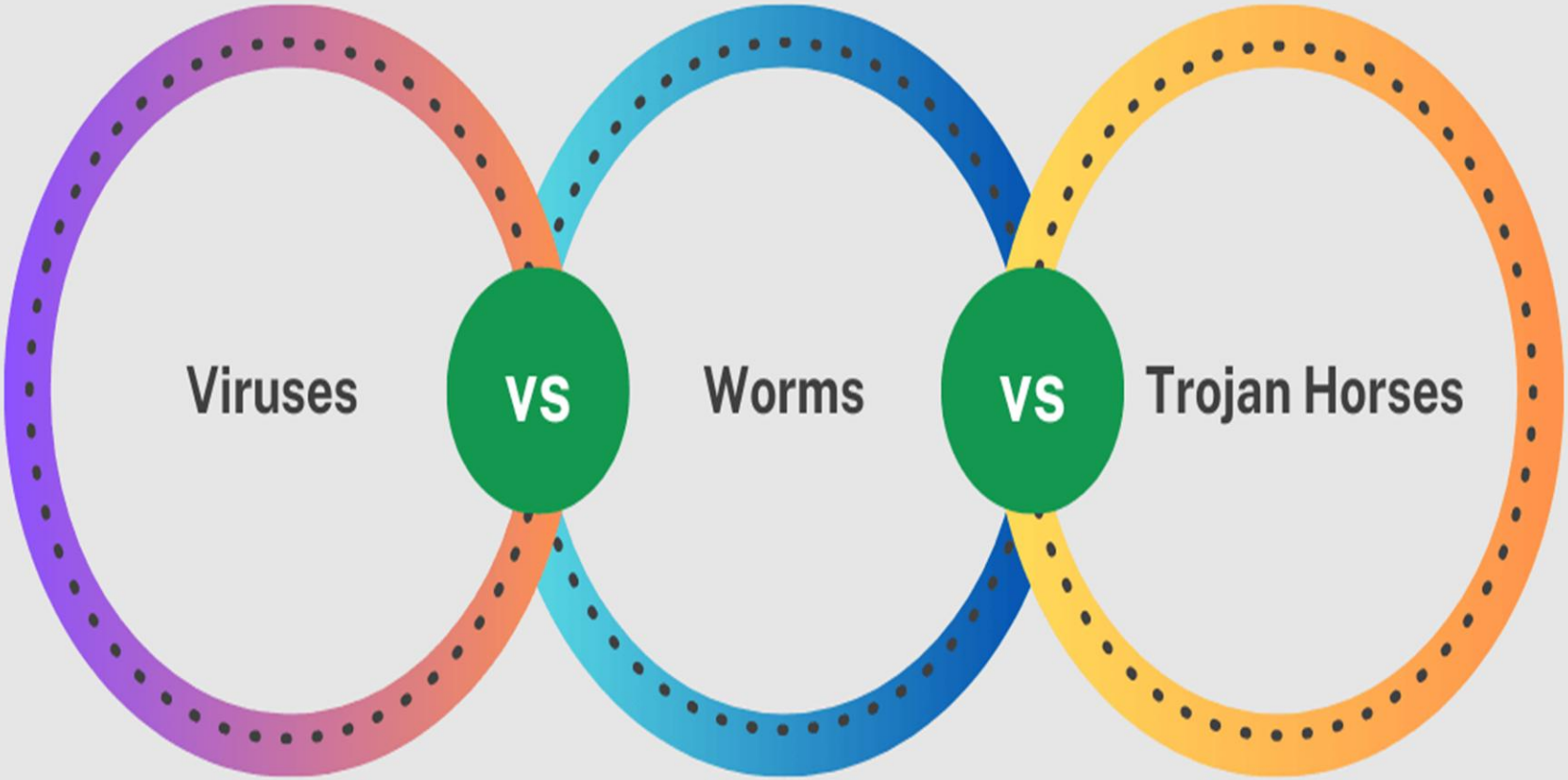
# Phishing

- Phishing is a form of social engineering where the phisher pretends to represent a legitimate outside organization.



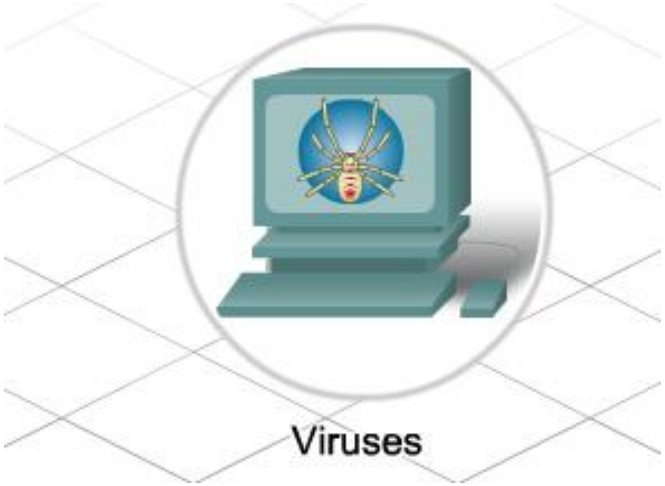
# Methods of Attack

- Viruses, Worms and Trojan Horses
- Denial of Service and Brute Force attacks
- Spyware, Tracking Cookies, Adware and Pop-ups
- Spam


Viruses
VS
Worms
VS
Trojan Horses

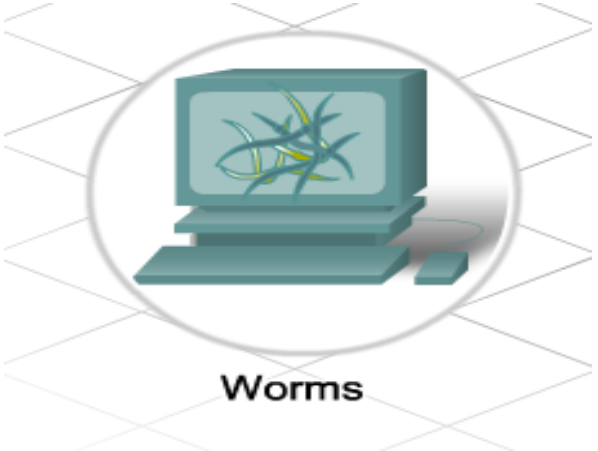
# Viruses, Worms and Trojan Horses

- Viruses
  - A virus is a program that runs and spreads by modifying other programs or files. A virus cannot start by itself; it needs to be activated. Once activated, a virus may do nothing more than replicate itself and spread.

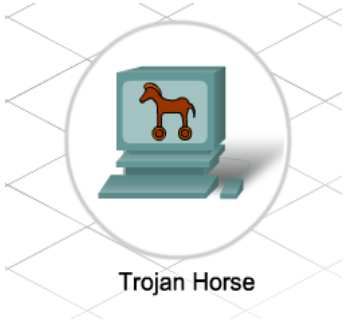


# Viruses, Worms and Trojan Horses

- Worms
  - A worm is similar to a virus, but unlike a virus does not need to attach itself to an existing program. A worm uses the network to send copies of itself to any connected hosts. Worms can run independently and spread quickly. They do not necessarily require activation or human intervention



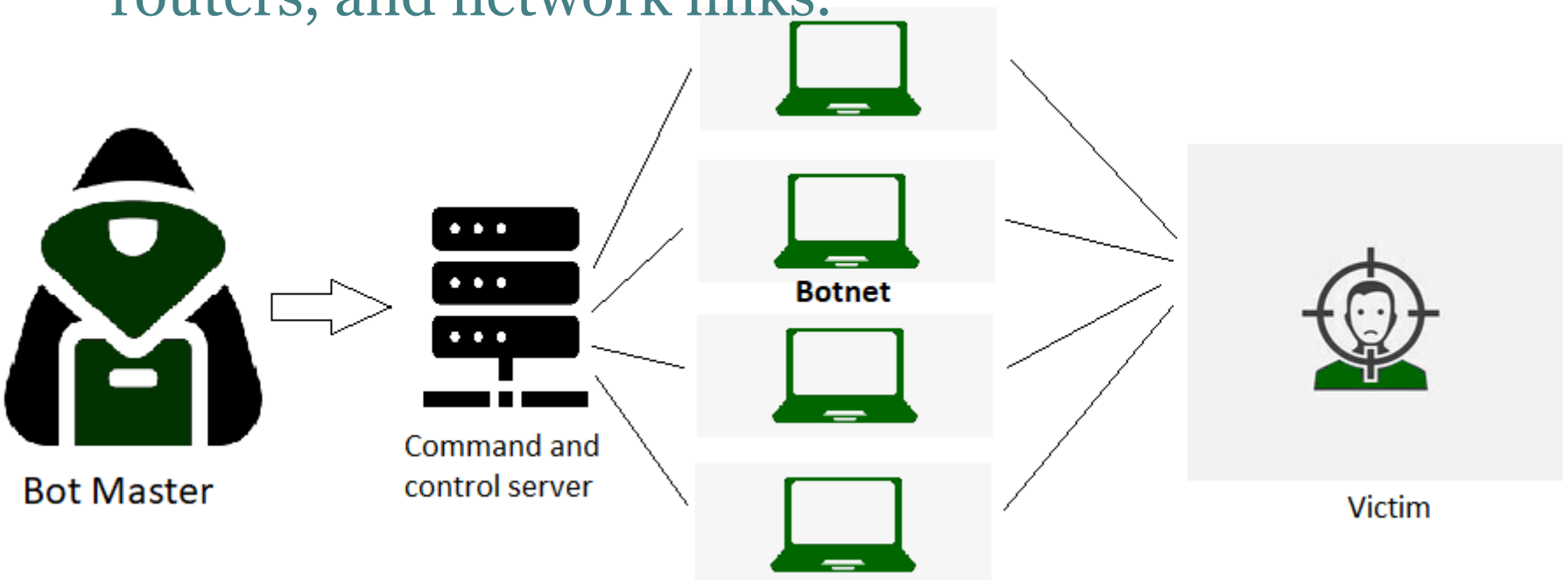
# Viruses, Worms and Trojan Horses



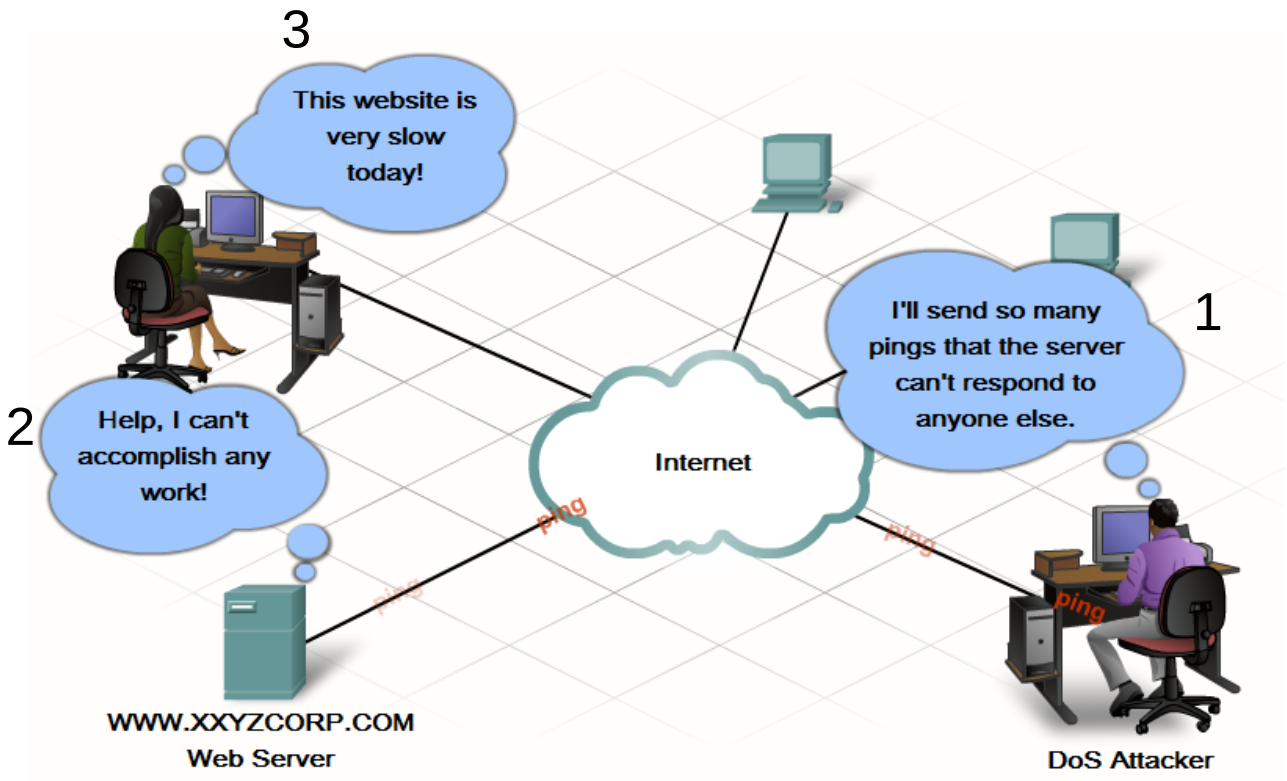

- Trojan Horses
  - A non-self replicating program that is written to appear like a legitimate program, when in fact it is an attack tool.
  - Relies upon its legitimate appearance to deceive the victim into initiating the program. It may be relatively harmless or can contain code that can damage the contents of the computer's hard drive.
  - Trojans can also create a back door into a system allowing hackers to gain access.

# Denial of Service

- Denial of Service (DoS)
  - DoS attacks are aggressive attacks on an individual computer or groups of computers with the intent to deny services to intended users. DoS attacks can target end user systems, servers, routers, and network links.

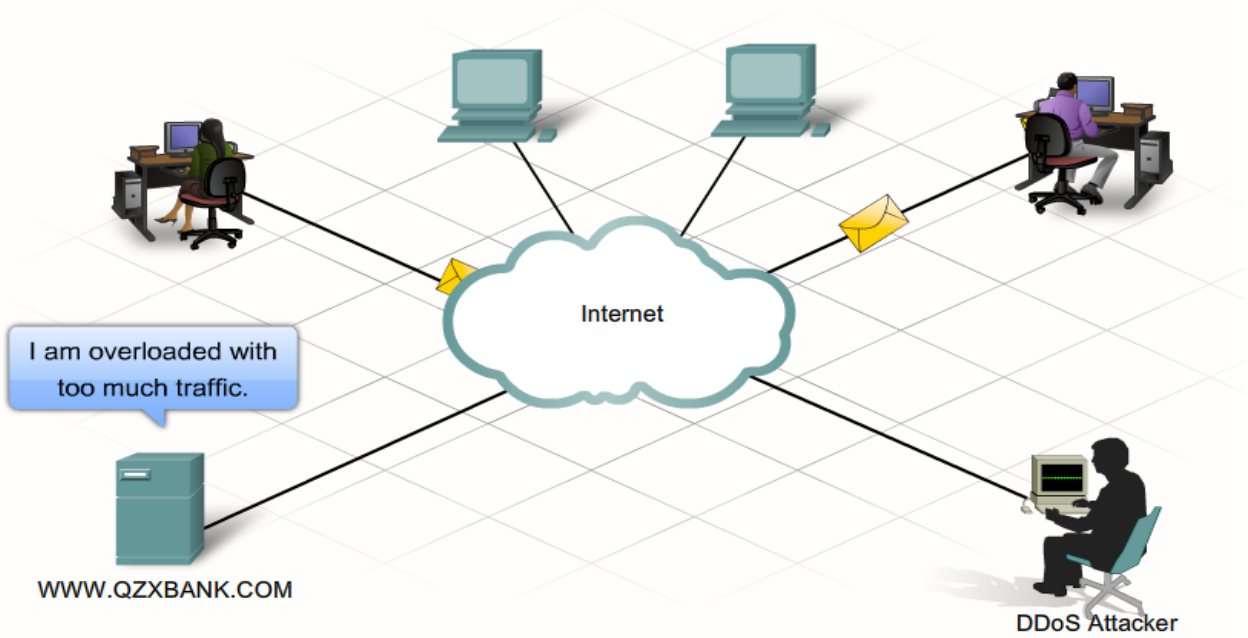


# Denial of Service Example



# Distributed Denial of Service

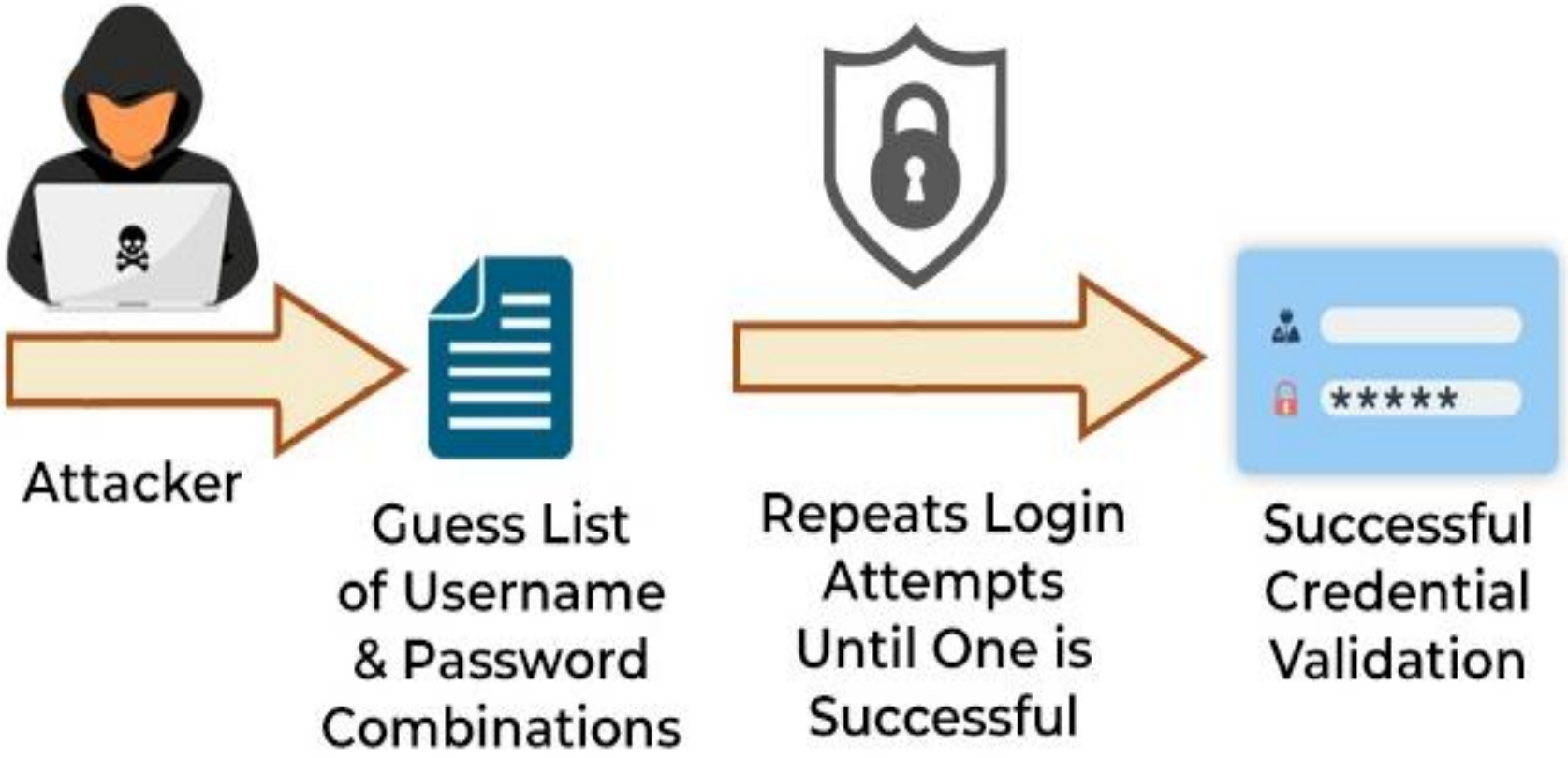
- Distributed Denial of Service (DDoS)
  - DDoS is a more sophisticated and potentially damaging form of the DoS attack. It is designed to saturate and overwhelm network links with useless data.



# Brute Force Attacks

- With brute force attacks, a fast computer is used to try to guess passwords.
- The attacker tries a large number of possibilities in rapid succession to gain access or crack the code. Brute force attacks can cause a denial of service due to excessive traffic to a specific resource or by locking out user accounts.

# KEY STEPS OF A BRUTE FORCE ATTACK



# Brute Force Attacks Explained

In a brute force attack, a cybercriminal uses trial and error to try and break into a device, network, or website.

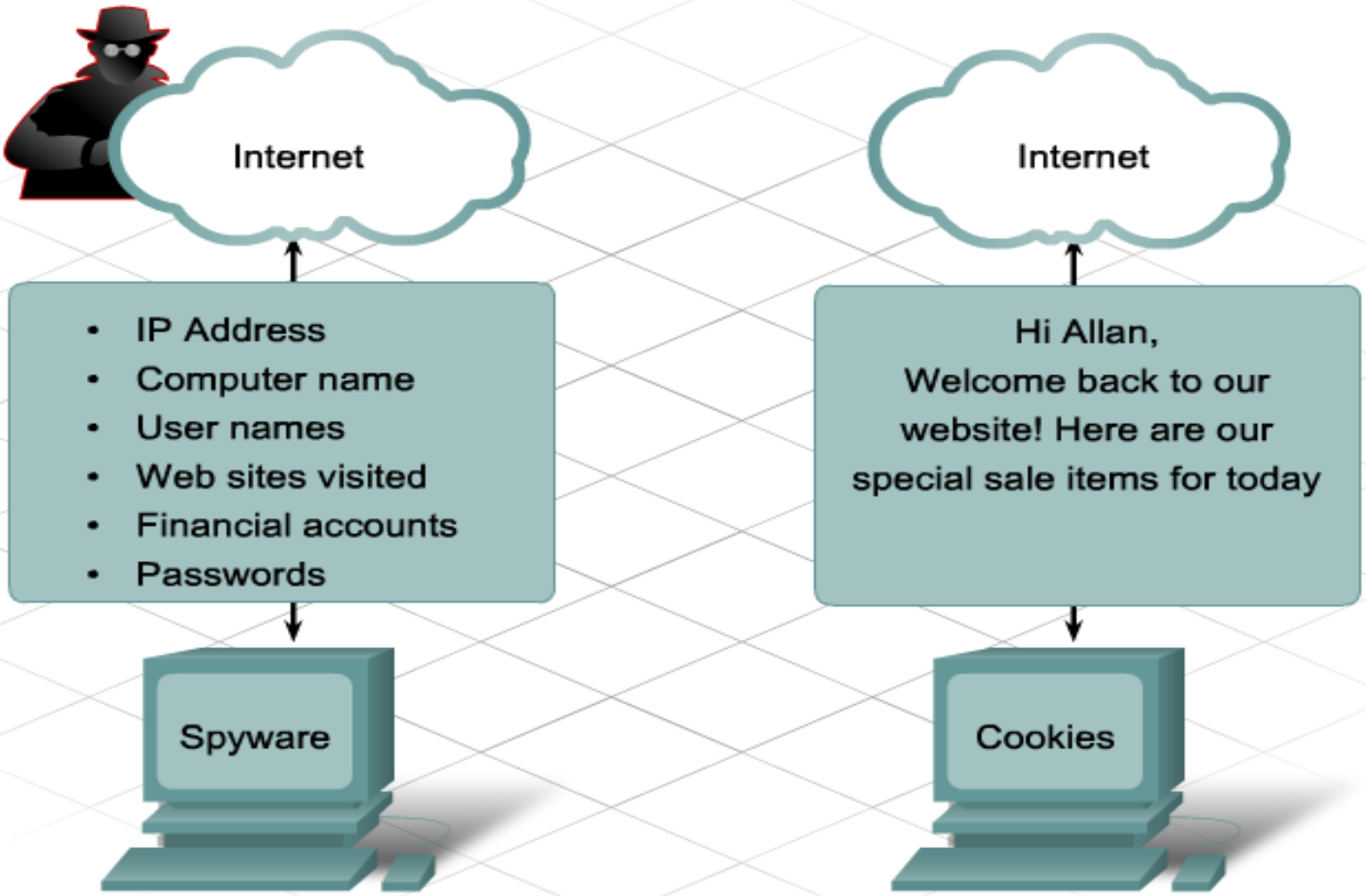

An attacker **utilizes a hacking tool.**

The hacking tool **attempts multiple logins.**

The system **returns a valid or invalid response.**

# Spyware and Tracking Cookies

- Spyware
  - Spyware is any program that gathers personal information from your computer without your permission or knowledge. This information is sent to advertisers or others on the Internet and can include passwords and account numbers.
- Tracking Cookies
  - Cookies are a form of spyware but are not always bad. They are used to record information about an Internet user when they visit websites.


Internet
Internet
IP Address
Computer name
User names
Web sites visited
Financial accounts
Passwords
Hi Allan,
Welcome back to our website! Here are our special sale items for today
Spyware
Cookies

# Spyware and Tracking Cookies

- Adware
  - Adware is a form of spyware used to collect information about a user based on websites the user visits. That information is then used for targeted advertising. Adware is commonly installed by a user in exchange for a "free" product.
- Pop-ups
  - Pop-ups are additional advertising windows that display when visiting a web site. Unlike Adware, pop-ups are not intended to collect information about the user and are typically associated only with the web-site being visited.


- Spam is a serious network threat that can overload ISPs, email servers and individual end-user systems. A person or organization responsible for sending spam is called a spammer. Spammers often make use of unsecured email servers to forward email. Spammers can use hacking techniques, such as viruses, worms and Trojan horses to take control of home computers.

# Common Security Measures

- Security risks cannot be eliminated or prevented completely. However, effective risk management and assessment can significantly minimize the existing security risks.
- True network security comes from a combination of products and services, combined with a thorough Security Policy and a commitment to adhere to that policy.

# Data Security Measures

# Authentication and Authorization

## Authentication

Verifies You Are Who You Say Are

**Methods**

- Login Form
- HTT Authentication
- HTTP Digest
- X.509 Certificates Custom Authentication
- Method

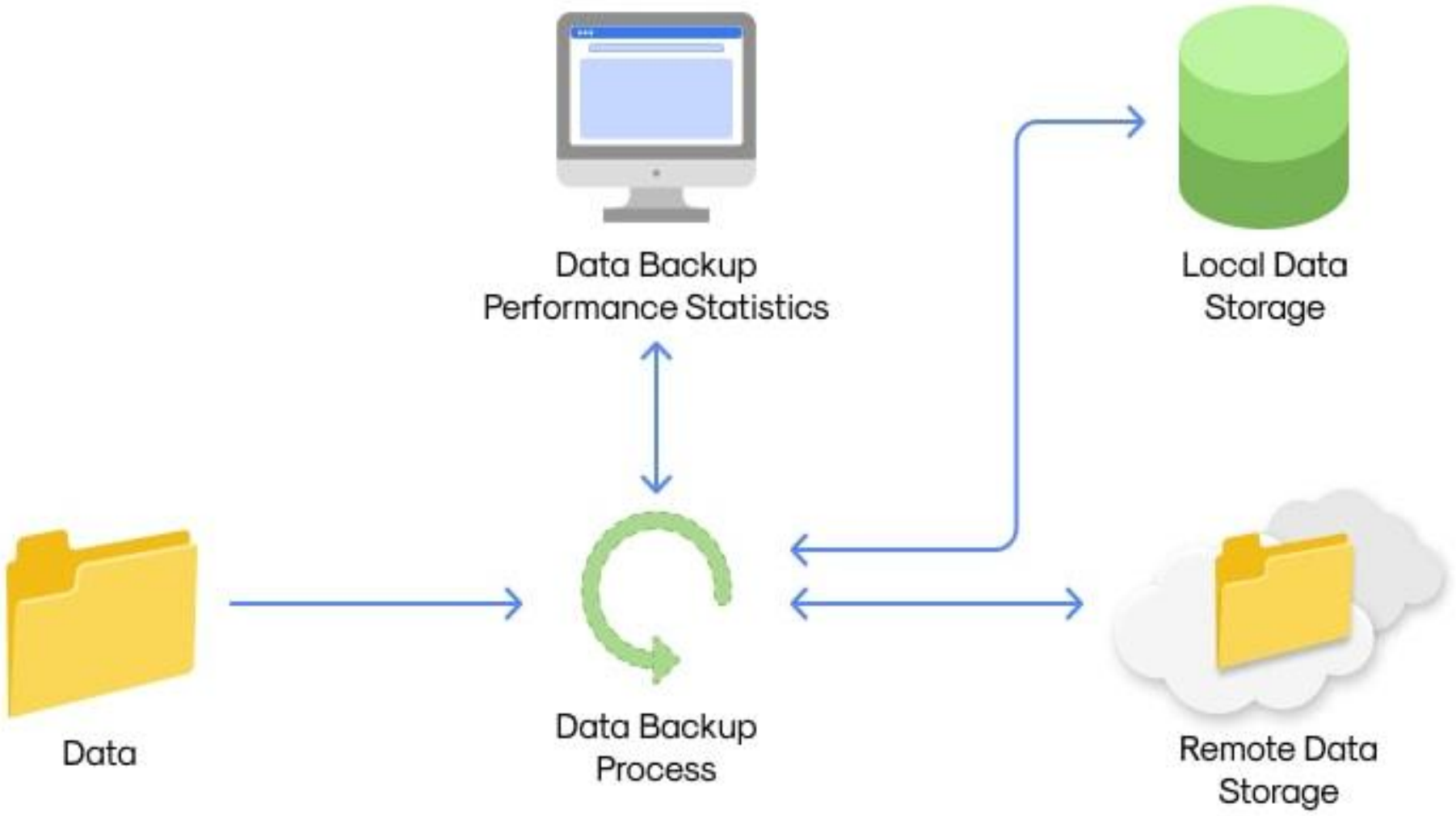
## Authorization

Decides If You Have Permission To Access A Resource

**Methods**

- Access Controls for URLs
- Secure Objects and Methods
- Access Control Lists (ACLs)

# Backups and Data Recovery



# Common Security Measures

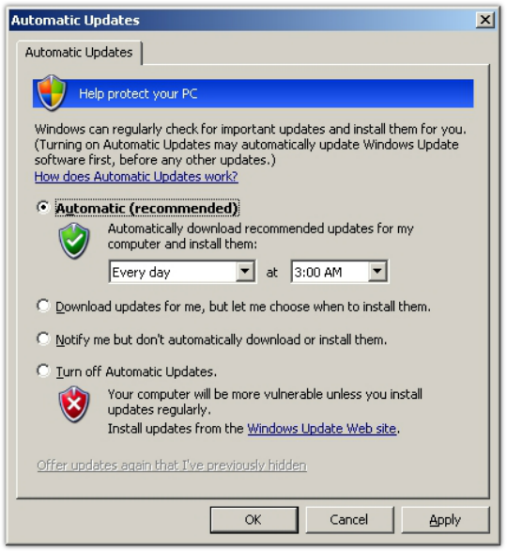
- Security Policy
- Updates and Patches
- Anti-virus Software
- Anti-Spam
- Anti-Spyware

# Common Security Measures

- A Security Policy is a formal statement of the rules that users must adhere to when accessing technology and information assets.
- It can be as simple as an acceptable use policy, or can be several hundred pages in length, and detail every aspect of user connectivity and network usage procedures.

# Patches and Updates

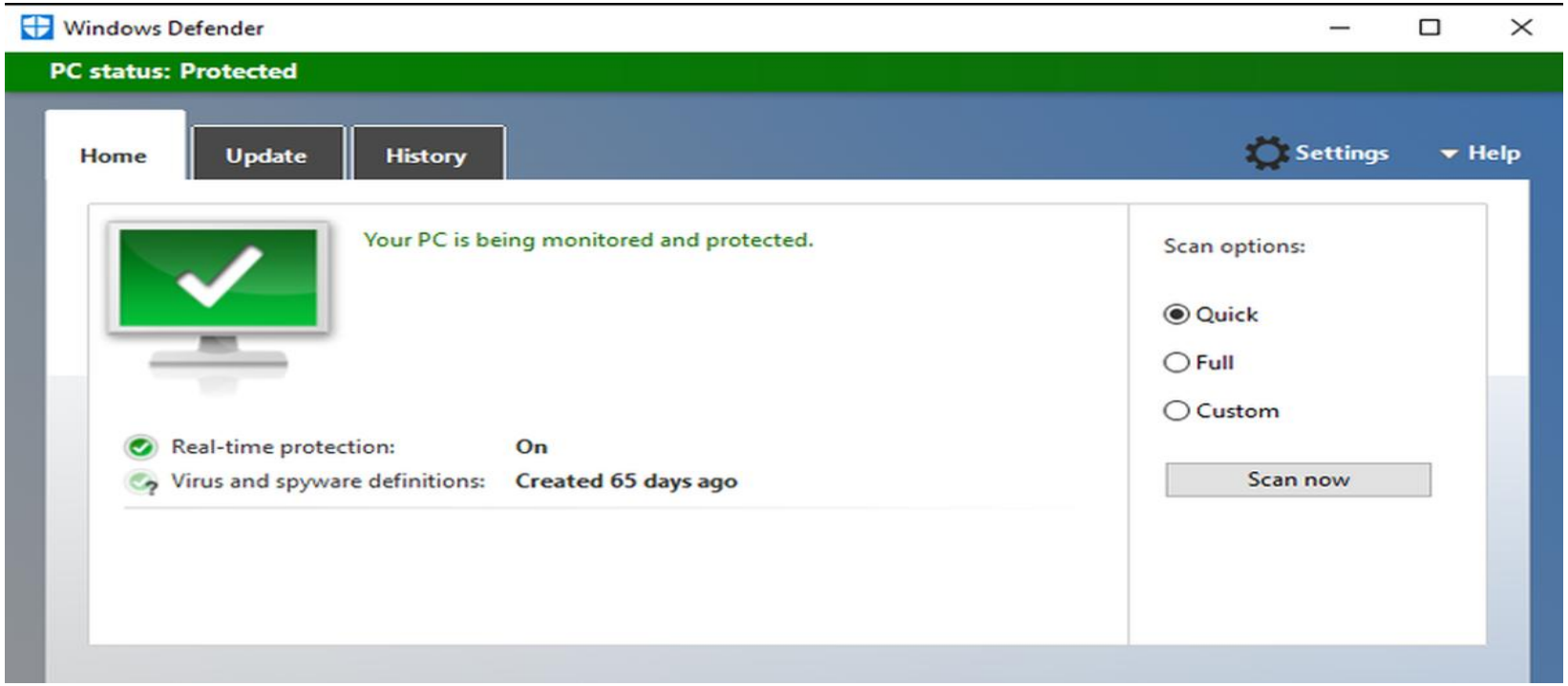
- A patch is a small piece of code that fixes a specific problem.
- An update, on the other hand, may include additional functionality to the software package as well as patches for specific issues.



# Anti-Virus Software

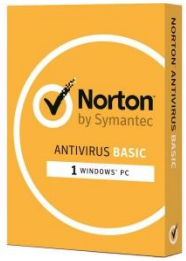
- Anti-virus Software
  - Anti-virus software can be used as both a preventative tool and as a reactive tool. It prevents infection and detects, and removes, viruses, worms and Trojan horses. Anti-virus software should be installed on all computers connected to the network.

# Anti-virus Software



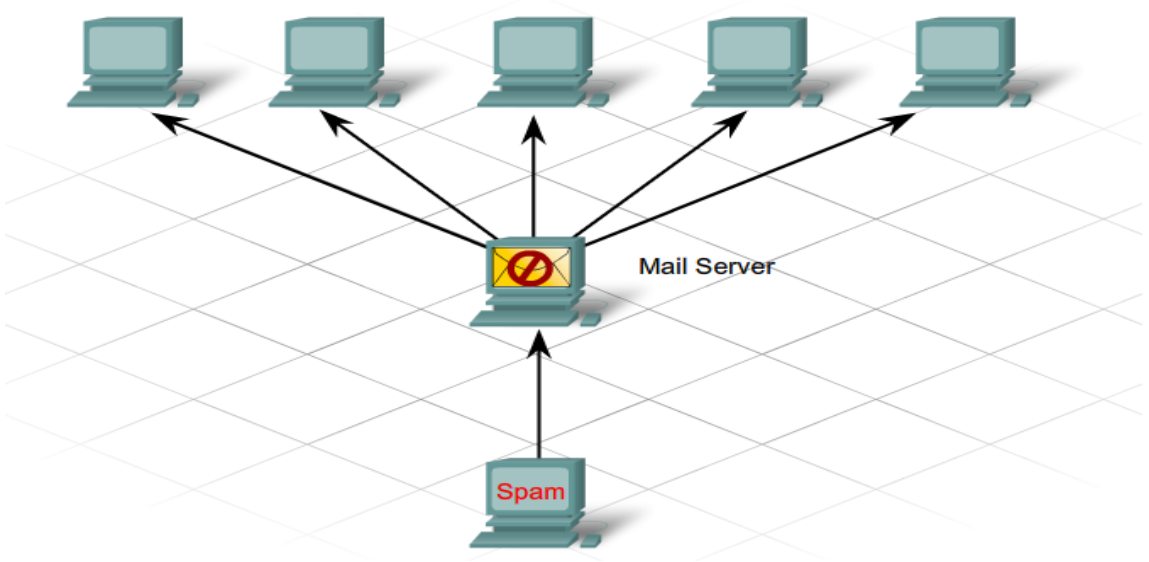






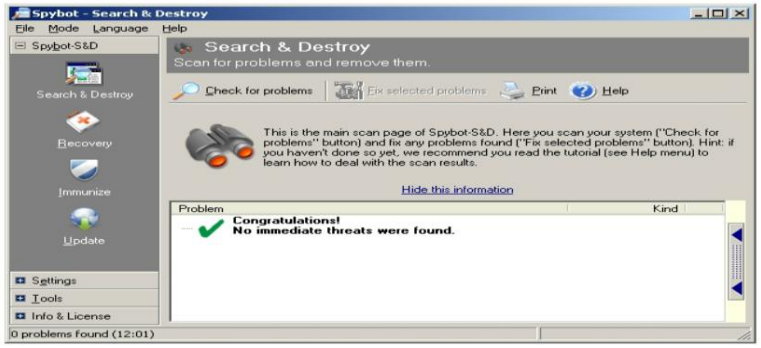
# Anti-Spam

- Anti-spam software protects hosts by identifying spam and performing an action, such as placing it into a junk folder or deleting it. It can be loaded on a machine locally, but can also be loaded on email servers.



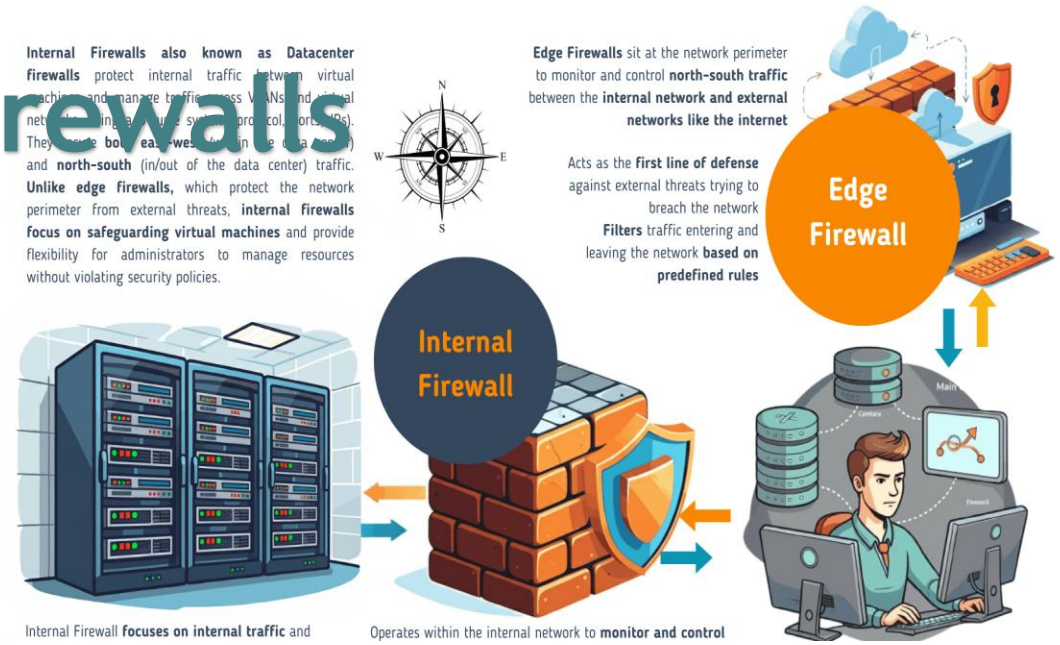
# Anti-Spyware

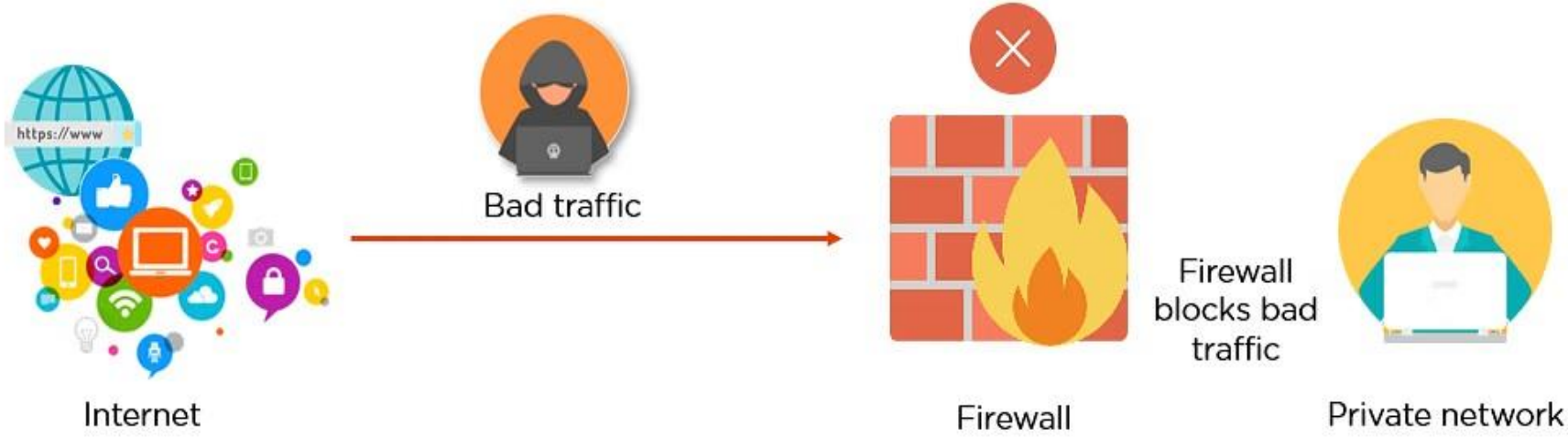
- Anti-spyware software detects and deletes spyware applications, as well as prevents future installations from occurring. Many Anti-Spyware applications also include detection and deletion of cookies and adware.
- Pop-up stopper software can be installed to prevent pop-ups.



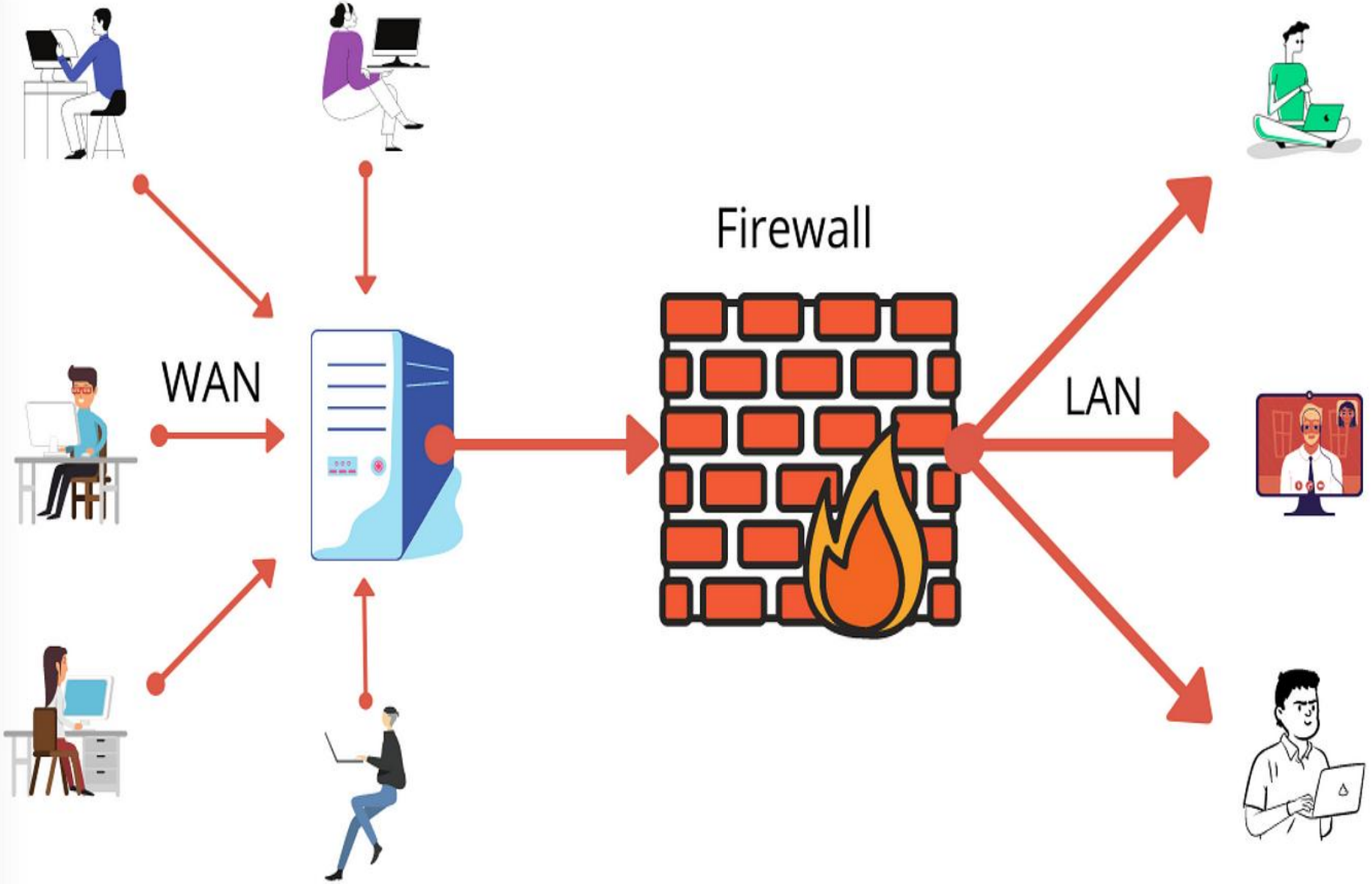
# Using Firewalls

- What is a Firewall?
- Using a Firewall
- Best Practices



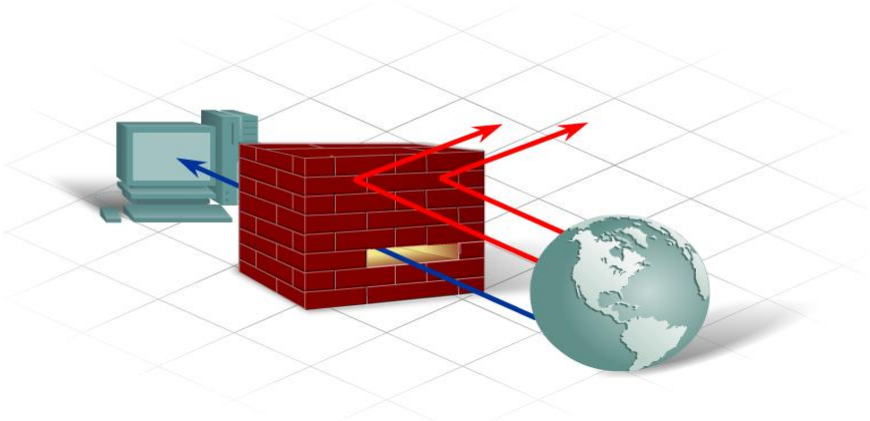



# What is a Firewall?



# What is a Firewall?

- A Firewall is one of the most effective security tools available for protecting internal network users from external threats.
- A firewall resides between two or more networks and controls the traffic between them as well as helps prevent unauthorized access.



# What is a Firewall?

- Packet Filtering - Prevents or allows access based on IP or MAC addresses.
- Application / Web Site Filtering - Prevents or allows access based on the application. Websites can be blocked by specifying a website URL address or keywords.

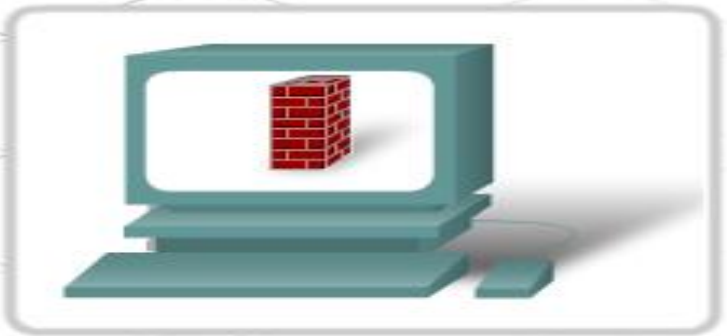
# What is a Firewall?

- Firewall products come packaged in various forms:

Cisco Security Appliances

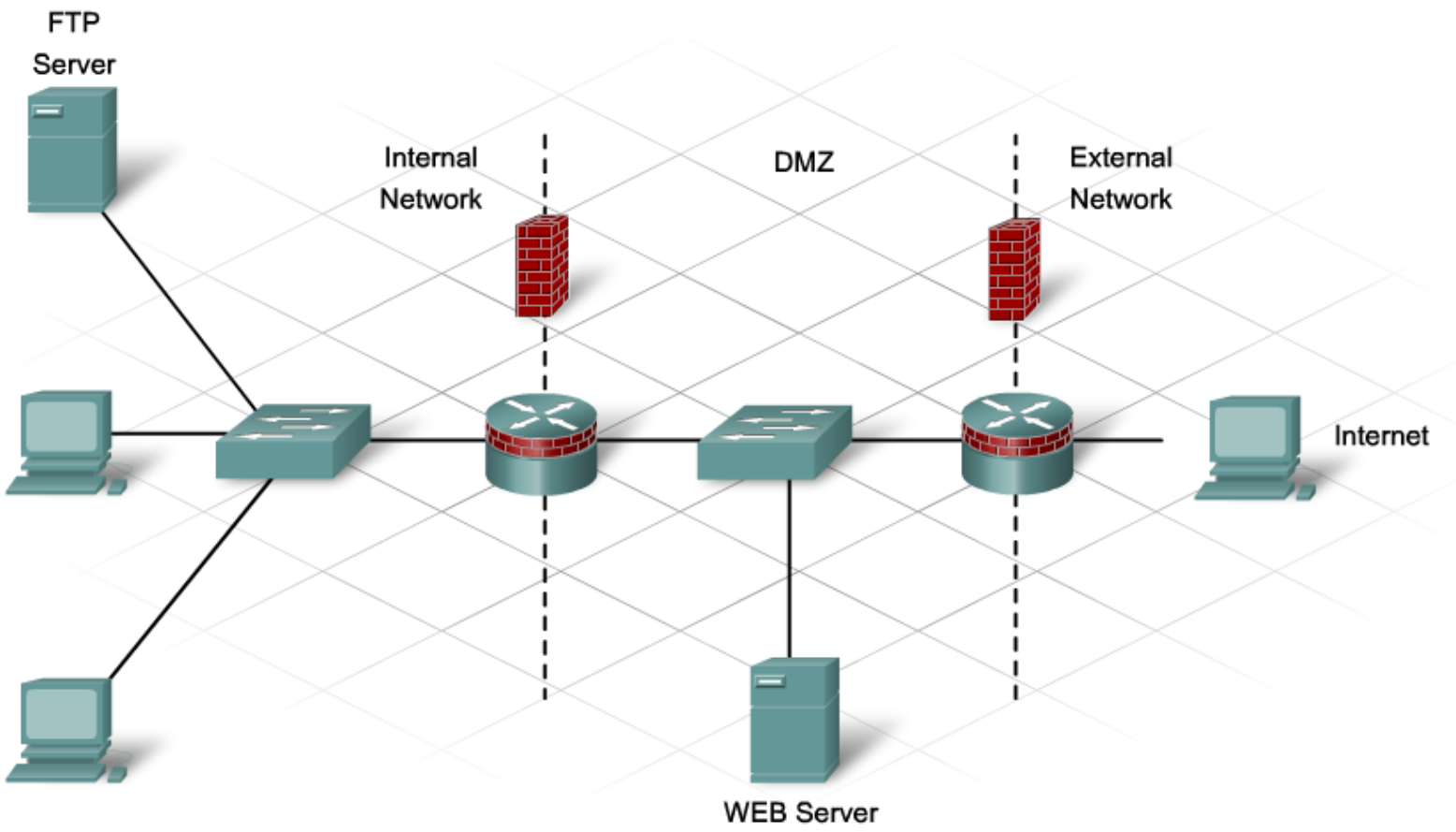
Server-Based Firewall

Linksys Wireless Router with Integrated Firewall

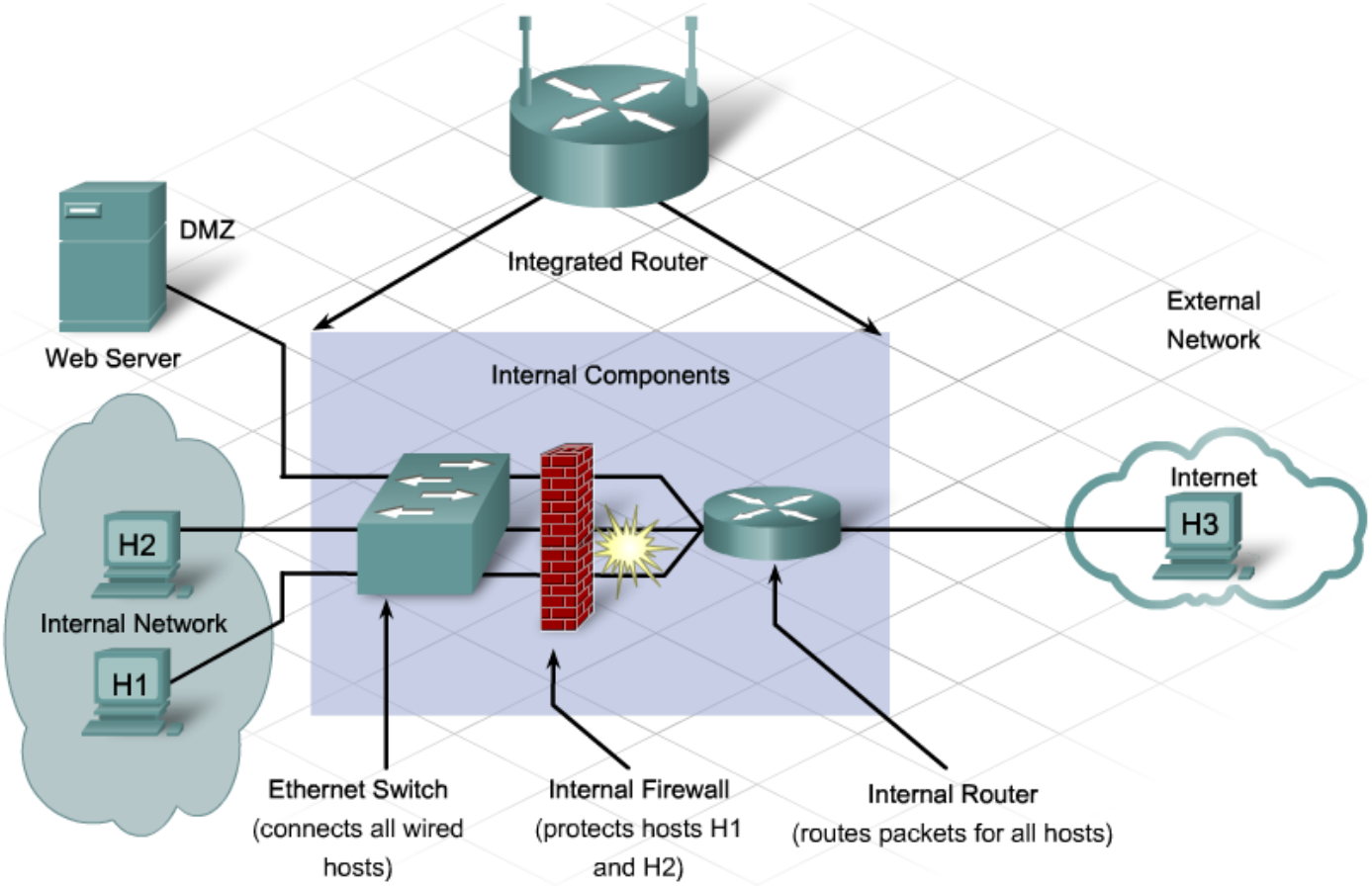


Personal Firewall

# Using a Firewall



# Using a Firewall



# OSI LAYERS AND ATTACK

| | | | |
|---|---|---|---|
| 7 | Application Layer | HTTP, FTP, SMTP | • SQL Injection<br>• Cross-Site Scripting (xss)<br>• DDos attacks |
| 6 | Presentation Layer | Compression, Encryption, Encocoding, SSL, TLS | • Character Encoding Attacks<br>• SSL Striping<br>• Data Compression + Manipulation |
| 5 | Session Layer | SOCKETS | • Session replay<br>• Session fixation attacks<br>• MiiM attacks |
| 4 | Transport Layer | Segmentation, TCP, Reassembly, UDP | • UDP flood<br>• SYN flood |
| 3 | Network Layer | PACKETS ASSEMBLY<br>ICMP, IGMP, IPSec, IP | • IP spoofing<br>• Route table manipulation<br>• Smurf attack |
| 2 | Data Link Layer | INTRA NETWORK COMM.<br>ETHERNET, WIFI | • MAC address spoofingood<br>• ARP spoofing<br>• Switch flooding |
| 1 | Physical Layer | DATA SENDING CABLE<br>FIBRE | • Eavesdropping<br>• Physical tampering<br>• Electromagnetic interference |

# Top Cybersecurity Tools ✦ | Cyber Press

## Social Engineering

1. GoPhish
2. HiddenEye
3. SocialFish
4. EvilURL
5. Evilginx
6. SET (Social-Engineering Toolkit)

## Password Cracking

1. Hashcat
2. John the Ripper
3. Hydra
4. Medusa
5. Cain & Abel
6. Ophcrack

## Web Application Assessment

1. OWASP ZAP
2. Burp Suite
3. Nikto
4. WPScan
5. Acunetix
6. Arachni

## Cloud Security

1. AWS GuardDuty
2. Azure Security Center
3. Google Cloud Security Command Center
4. Prisma Cloud
5. Lacework
6. wiz

## Wireless Hacking

1. Aircrack-NG
2. Wifite
3. Kismet
4. TCPDump
5. Reaver
6. Wireshark

## Exploitation

1. Metasploit Framework
2. Burp Suite
3. SQL Map
4. ExploitDB
5. Core Impact
6. Cobalt Strike
7. Empire

## Vulnerability Scanning

1. Nessus
2. OpenVAS
3. Nexpose
4. Qualys
5. Acunetix
6. Lynis

## Forensics

1. Wireshark
2. Autopsy
3. Volatility
4. SleuthKit
5. Binwalk
6. Foremost
7. EnCase

## Network Defense

1. Snort
2. Suricata
3. pfSense
4. Security Onion
5. AlienVault OSSIM

## Endpoint Security

1. CrowdStrike Falcon
2. SentinelOne
3. Carbon Black
4. Symantec Endpoint Protection
5. Microsoft Defender for Endpoint

## Threat Intelligence

1. ThreatConnect
2. Recorded Future.
3. AlienVault OTX
4. IBM X-Force Exchange
5. MISP (Malware Information Sharing Platform)

## Information Gathering

1. Nmap
2. Shodan
3. Maltego
4. TheHarvester
5. Recon-NG
6. Amass
7. Censys
8. OSINT Framework
9. Gobuster
10. Spiderfoot

# Ports mostly used by Hackers:

1. Port 21- File Transfer Protocol (FTP)
2. Port 22- Secure Shell (SSH)
3. Port 23 - Telnet
4. Port 25 - Simple Mail Transfer Protocol (SMTP)
5. Port 53- Domain Name System (DNS)
6. Port 69 - TFTP
7. Port 80, 443, 8080, 8443- HTTP/ HTTPS
8. Port 135- Windows RPC
9. Port 137-139 - Windows NetBIOS over TCP/IP

# Thank you