# Phishing (Detailed Study)

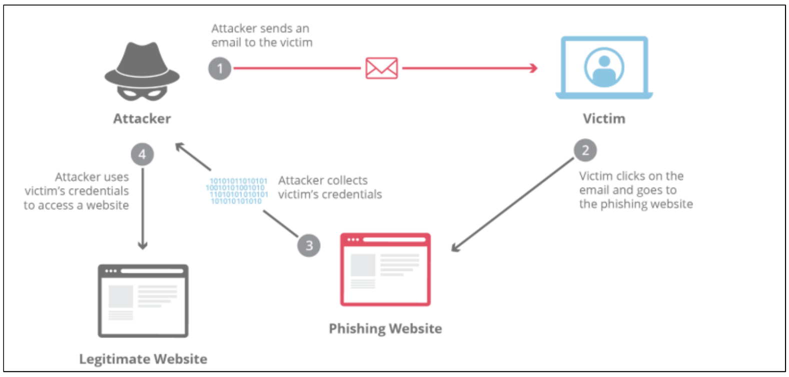

Attacker sends an email to the victim
1
Attacker
Victim
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
2
Victim clicks on the email and goes to the phishing website
3
Phishing Website
Legitimate Website

Figure 1: Phishing attack

Phishing is a social engineering cyber attack in which an attacker impersonates a trusted entity to deceive users into revealing sensitive information or performing malicious actions.

Phishing primarily targets the human factor rather than technical vulnerabilities.

## Why Phishing Is Dangerous

- Bypasses firewalls and antivirus systems
- Exploits trust, fear, urgency, and authority
- Works across all operating systems
- Often used as the first step in larger attacks

## Phishing Attack Lifecycle

### Step 1: Reconnaissance

- Collects email addresses and phone numbers
- Identifies target roles such as employee or admin

### Step 2: Bait Creation

- Fake emails or messages
- Fake login pages
- Malicious links or attachments

**Step 3: Delivery**

- Email
- SMS
- Phone calls
- Social media

**Step 4: Exploitation**

- Victim clicks a malicious link
- Victim enters credentials

**Step 5: Data Capture**

- Username and password theft
- OTP and sensitive data theft

**Step 6: Post-Exploitation**

- Account takeover
- Malware or ransomware deployment

## Types of Phishing

**Email Phishing:** Mass emails sent to many users with generic messages.
**Spear Phishing:** Targeted phishing aimed at a specific individual.
**Whaling:** Targets senior executives.
**Smishing:** Phishing via SMS messages.
**Vishing:** Voice-based phishing using phone calls.
**Clone Phishing:** Legitimate emails copied and resent with malicious links.

## CIA Triad Impact

- Confidentiality is primarily affected
- Integrity may be compromised
- Availability may be indirectly affected

## Phishing Prevention

- User awareness training
- Multi-Factor Authentication
- Email filtering and verification

## One-Line Exam Answer

Phishing is a social engineering attack that tricks users into revealing sensitive information by impersonating trusted entities.

## Malware (Detailed Study)

Malware is malicious software designed to disrupt systems, steal data, or gain unauthorized access to computers and networks.

Malware operates by executing harmful code on the victim's system.

## Why Malware Is Dangerous

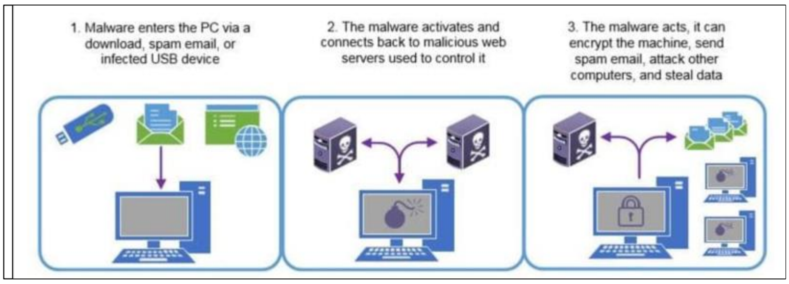

1. Malware enters the PC via a download, spam email, or infected USB device
2. The malware activates and connects back to malicious web servers used to control it
3. The malware acts, it can encrypt the machine, send spam email, attack other computers, and steal data

Figure 2: Malware

- Can operate silently without user awareness
- Can steal, modify, or destroy data
- Can spread to other systems
- Often used to deliver ransomware or spyware

## How Malware Works

### Step 1: Infection

- Malicious file is downloaded or executed
- Infection occurs through email, websites, or USB devices

### Step 2: Execution

- Malware runs automatically or via user action
- Establishes persistence in the system

### Step 3: Payload Activation

- Steals data
- Records keystrokes
- Downloads additional malware

**Step 4: Propagation**

- Spreads across network
- Infects removable media

## Common Types of Malware

**Virus:** Attaches to legitimate files and spreads when executed.
**Worm:** Self-propagates across networks without user interaction.
**Trojan:** Disguised as legitimate software but executes malicious actions.
**Spyware:** Monitors user activity and steals sensitive data.
**Keylogger:** Records keystrokes to capture credentials.
**Rootkit:** Hides malware presence and maintains privileged access.

## Malware Delivery Methods

- Email attachments
- Malicious websites
- Software cracks and pirated programs
- Infected USB devices

## CIA Triad Impact

- Confidentiality: Data theft
- Integrity: File modification
- Availability: System disruption

## Real-World Malware Example

1. User downloads a cracked application
2. Malware executes in the background
3. Keystrokes and credentials are captured
4. Attacker gains unauthorized access

## Malware Detection Indicators

- Slow system performance
- Unexpected pop-ups
- Unknown processes running
- Unauthorized network traffic

## Malware Prevention

- Antivirus and endpoint protection
- Regular software updates
- Avoid untrusted downloads
- Principle of least privilege

## One-Line Exam Answer

Malware is malicious software designed to compromise confidentiality, integrity, or availability of systems.

# Distributed Denial of Service (DDoS)

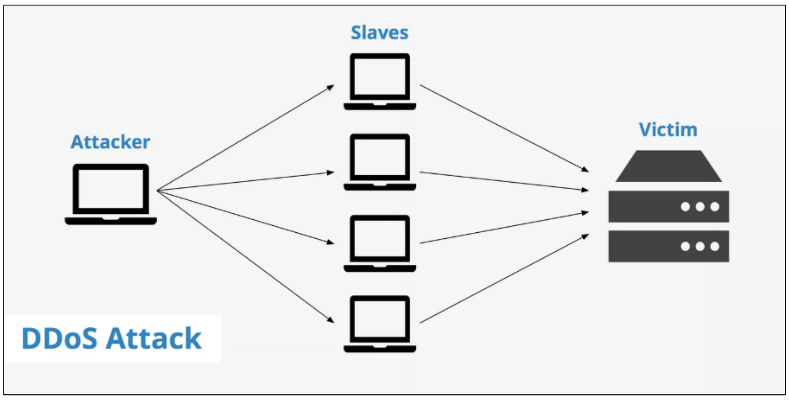


Figure 3: Distributed Denial of Service attack using multiple sources

A Distributed Denial of Service (DDoS) attack is a cyber attack in which multiple compromised systems simultaneously flood a target system, server, or network with traffic, making it unavailable to legitimate users.

## Why DDoS Is Dangerous

- Overwhelms servers and networks
- Disrupts critical online services
- Difficult to block due to multiple sources
- Causes financial and reputational damage

## How DDoS Works

**Step 1: Botnet Creation**

- Attacker compromises multiple devices
- Devices are controlled remotely

**Step 2: Command and Control**

- Attacker sends attack commands
- Botnet prepares to flood the target

**Step 3: Traffic Flooding**

- Massive traffic sent simultaneously
- Server resources are exhausted

## Common Types of DDoS Attacks

**Volume-Based Attacks:** Consume bandwidth using UDP or ICMP floods.
**Protocol Attacks:** Exploit protocol weaknesses such as SYN floods.
**Application Layer Attacks:** Target web applications using HTTP floods.

## CIA Triad Impact

- Primary Impact: Availability
- Confidentiality is not affected
- Integrity is not affected

## Real-World Example

1. Attacker controls thousands of infected devices
2. All devices send traffic to a single website
3. Website becomes unreachable for real users

## DDoS Detection Indicators

- Sudden spike in traffic
- Slow or unresponsive services
- Large number of requests from many IPs

## DDoS Prevention and Mitigation

- Rate limiting
- Load balancing
- Content Delivery Networks
- Traffic filtering and scrubbing

## One-Line Exam Answer

A DDoS attack disrupts service availability by overwhelming a target with traffic from multiple compromised systems.

## SQL Injection (SQLi)

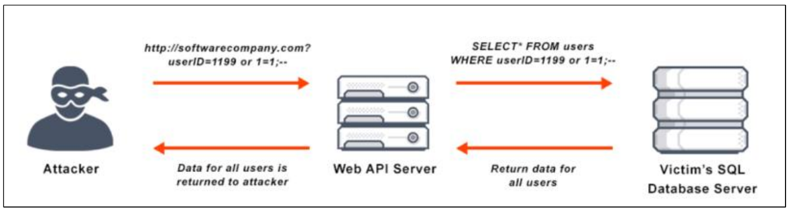


Figure 4: SQL Injection attack exploiting unsanitized user input

SQL Injection is a web application attack where an attacker injects malicious SQL queries into user input fields to manipulate or access the backend database.

It occurs due to improper input validation.

## Why SQL Injection Is Dangerous

- Allows unauthorized access to databases
- Can bypass authentication mechanisms
- Can expose sensitive user information
- May allow deletion or modification of data

## How SQL Injection Works

### Step 1: Vulnerable Input

- Application accepts user input
- Input is directly used in SQL queries

### Step 2: Malicious Payload Injection

- Attacker inserts SQL code into input fields
- Application fails to sanitize input

### Step 3: Query Execution

- Database executes the injected SQL command
- Unauthorized action is performed

## Common SQL Injection Types

**Classic SQL Injection:** Injection using logical conditions to alter queries.
**Union-Based SQL Injection:** Uses UNION operator to extract data from other tables.
**Blind SQL Injection:** Data is inferred through true or false responses.
**Time-Based SQL Injection:** Uses delays to infer database behavior.

## CIA Triad Impact

- Confidentiality: Sensitive data exposure
- Integrity: Data modification or deletion
- Availability: Database disruption (in severe cases)

## Real-World Example

1. Attacker enters malicious input into a login form
2. SQL query logic is altered
3. Authentication is bypassed
4. Database records are accessed or modified

## SQL Injection Detection Indicators

- Database errors displayed on web pages
- Unexpected application behavior
- Login bypass without valid credentials

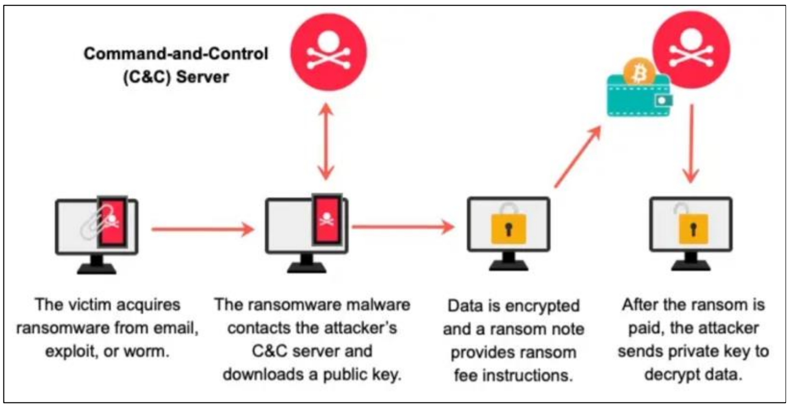
## SQL Injection Prevention

- Prepared statements and parameterized queries
- Input validation and sanitization
- Least privilege for database users
- Web Application Firewalls

## One-Line Exam Answer

SQL Injection is an attack where malicious SQL code is injected into user input to manipulate backend databases.

## Ransomware



Command-and-Control (C&C) Server
The victim acquires ransomware from email, exploit, or worm.
The ransomware malware contacts the attacker's C&C server and downloads a public key.
Data is encrypted and a ransom note provides ransom fee instructions.
After the ransom is paid, the attacker sends private key to decrypt data.

Figure 5: Ransomware attack lifecycle showing file encryption and ransom demand

Ransomware is a type of malware that encrypts a victim's files or systems and demands payment, usually in cryptocurrency, in exchange for restoring access.

The primary goal of ransomware is extortion.

## Why Ransomware Is Dangerous

- Causes complete loss of access to critical data
- Can halt business operations
- Financial loss due to ransom and downtime
- Data may never be recovered even after payment

## How Ransomware Works

### Step 1: Initial Infection

- Phishing emails with malicious attachments
- Exploiting unpatched vulnerabilities

### Step 2: Execution

- Malware executes on the system
- Establishes persistence

### Step 3: Encryption

- Files are encrypted using strong cryptography

- Original files become inaccessible

**Step 4: Ransom Demand**

- Ransom note is displayed
- Payment demanded within a time limit

## Common Ransomware Types

**Crypto Ransomware:** Encrypts files and demands payment for decryption.
**Locker Ransomware:** Locks the entire system without encrypting files.
**Double Extortion Ransomware:** Encrypts data and threatens to leak stolen data.

## CIA Triad Impact

- Primary Impact: Availability
- Secondary Impact: Integrity
- Confidentiality may be affected if data is exfiltrated

## Real-World Example

1. User opens a malicious email attachment
2. Ransomware encrypts all local files
3. Ransom note demands cryptocurrency payment
4. Organization systems become unusable

## Ransomware Detection Indicators

- Sudden inability to open files
- Unusual file extensions
- Ransom notes appearing on the desktop

## Ransomware Prevention

- Regular offline backups
- Email security and phishing awareness
- Patch management
- Endpoint protection

## One-Line Exam Answer

Ransomware is malware that encrypts victim data and demands payment to restore access.

## Brute Force Attack

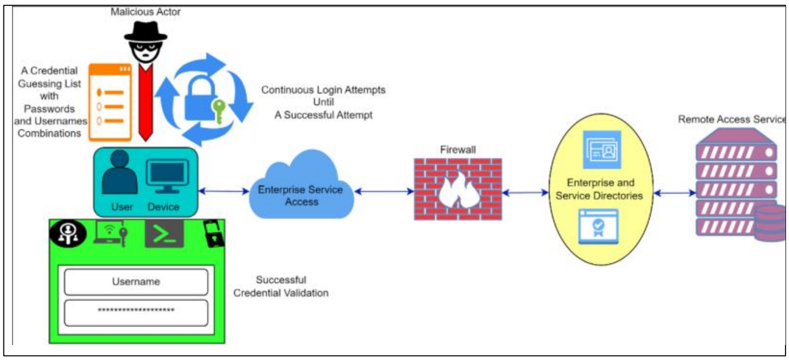

Malicious Actor
A Credential Guessing List with Passwords and Usernames Combinations
Continuous Login Attempts Until A Successful Attempt
Remote Access Servic
User
Device
Enterprise Service Access
Firewall
Enterprise and Service Directories
Username
********************
Successful Credential Validation

Figure 6: Brute force attack attempting multiple password combinations

A Brute Force attack is a method where an attacker systematically tries many username and password combinations until the correct credentials are discovered.

This attack relies on automation and weak password policies.

## Why Brute Force Is Dangerous

- Can compromise accounts with weak passwords
- Automated tools can attempt thousands of logins per second
- Often goes unnoticed without proper monitoring

## How Brute Force Works

### Step 1: Target Identification

- Login pages such as SSH, FTP, web applications

### Step 2: Credential Attack

- Tries multiple password combinations
- Uses wordlists or generated passwords

### Step 3: Access Gained

- Correct credentials discovered
- Unauthorized access obtained

## Common Brute Force Variants

**Simple Brute Force:** Attempts all possible combinations.
**Dictionary Attack:** Uses a predefined list of common passwords.
**Credential Stuffing:** Uses leaked username and password combinations.
**Hybrid Attack:** Combines dictionary words with variations.

## CIA Triad Impact

- Confidentiality: Account data exposure
- Integrity: Unauthorized actions performed
- Availability may be affected if accounts are locked

## Real-World Example

1. Attacker targets an SSH login service
2. Automated tool attempts thousands of passwords
3. Weak password is cracked
4. Attacker gains system access

## Brute Force Detection Indicators

- Multiple failed login attempts
- Login attempts from unusual IP addresses
- Account lockouts

## Brute Force Prevention

- Strong password policies
- Account lockout mechanisms
- Multi-Factor Authentication
- Rate limiting

## One-Line Exam Answer

A Brute Force attack attempts to gain access by systematically trying multiple credential combinations.