CYBER SECURITY

TYPES OF CYBER ATTACK

Detailed overview of key cyber attack types, their categories, methods, examples, and impacts on security and data integrity.

Submitted To

Mam Rabya Riaz

About Me	
Name	Syed Mansoor ul Hassan Bukhari
Roll No.	19
Session	2021-25
Class	BS(AI)

1. Phishing

Category: Social Engineering

Description: Phishing is a technique used to trick individuals into divulging sensitive information such as usernames, passwords, and credit card details by pretending to be a trustworthy entity. This is typically done through emails, messages, or websites that appear legitimate.

Example: An email that looks like it's from a bank, asking the recipient to click a link and enter their account details. The link directs the user to a fake website that captures their information.

Impact: Phishing can lead to identity theft, financial loss, and unauthorized access to personal and corporate accounts.

2. Malware

Category: Malicious Software

Description: Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. Types of malware include viruses, worms, trojans, ransomware, and spyware.

Example: Ransomware encrypts a user's files and demands payment for the decryption key. WannaCry is a famous example of ransomware that affected numerous organizations worldwide.

Impact: Malware can lead to data loss, financial damage, and disruption of services.

3. Denial of Service (DoS)

Category: Network Attack

Description: A DoS attack aims to make a machine or network resource unavailable to its intended users by overwhelming it with a flood of internet traffic. This can be achieved through various methods, including flooding the target with superfluous requests.

Example: A website being flooded with traffic from multiple sources, causing it to crash. The 2016 Dyn attack is a notable example, where major websites like Twitter and Netflix were affected.

Impact: DoS attacks can cause significant downtime, loss of revenue, and damage to reputation.

4. Man-in-the-Middle (MitM)

Category: Eavesdropping Attack

Description: In a MitM attack, the attacker secretly intercepts and relays messages between two parties who believe they are directly communicating with each other. This allows the attacker to steal or manipulate the data being exchanged.

Example: An attacker intercepting communication between a user and a banking website to steal login credentials. This can be done through techniques like session hijacking or SSL stripping.

Impact: MitM attacks can lead to data theft, financial loss, and unauthorized access to sensitive information.

5. SQL Injection

Category: Injection Attack

Description: SQL injection involves inserting malicious SQL code into a query to manipulate the database and gain unauthorized access to data. This can allow attackers to view, modify, or delete data within the database.

Example: An attacker entering SQL code into a login form to bypass authentication and access the database. For instance, entering ' OR '1'='1 in a login field to gain access without a valid username and password.

Impact: SQL injection can lead to data breaches, loss of data integrity, and unauthorized access to sensitive information.

6. Cross-Site Scripting (XSS)

Category: Injection Attack

Description: XSS attacks involve injecting malicious scripts into content from otherwise trusted websites. These scripts can then execute in the user's browser, potentially stealing information or performing actions on behalf of the user.

Example: A malicious script embedded in a comment section of a website that executes when other users view the comment. This can be used to steal cookies, session tokens, or other sensitive information.

Impact: XSS attacks can lead to data theft, session hijacking, and unauthorized actions performed on behalf of the user.

7. Password Attacks

Category: Credential Attack

Description: Password attacks involve attempting to obtain or decrypt a user's password. Common methods include brute force attacks, dictionary attacks, and keylogging.

Example: A brute force attack where an attacker tries multiple combinations of passwords until the correct one is found. Tools like Hydra or John the Ripper are often used for such attacks.

Impact: Successful password attacks can lead to unauthorized access to accounts, data breaches, and identity theft.

8. Zero-Day Exploit

Category: Exploit Attack

Description: A zero-day exploit targets a software vulnerability that is unknown to the software vendor and has no patch available. Attackers exploit this vulnerability before it is fixed.

Example: An attacker using a previously unknown vulnerability in a web browser to execute arbitrary code. The Stuxnet worm is a famous example of a zero-day exploit used to target industrial control systems.

Impact: Zero-day exploits can lead to significant damage, data breaches, and unauthorized access to systems.

9. DNS Tunneling

Category: Data Exfiltration

Description: DNS tunneling involves encoding the data of other programs or protocols in DNS queries and responses. This can be used to bypass firewalls and exfiltrate data from a network.

Example: An attacker using DNS queries to send data from a compromised system to an external server. This method can be used to steal sensitive information without detection.

Impact: DNS tunneling can lead to data breaches, loss of sensitive information, and unauthorized data transfer.

10. Insider Threats

Category: Insider Attack

Description: Insider threats come from individuals within an organization who misuse their access to harm the organization. This can be intentional or unintentional.

Example: A disgruntled employee stealing sensitive company data and selling it to competitors. Alternatively, an employee accidentally leaking confidential information due to lack of awareness.

Impact: Insider threats can lead to data breaches, financial loss, and damage to the organization’s reputation.