

Cyber Attacks

Top 8 Cyber Attacks – 2024

Phishing Attack

- 1 The use of deceptive emails, texts, or websites to gain sensitive information.
1. Attacker Sends Phishing Link
2. User Opens It
3. Hacker collects credentials
4. Hacker Uses Credentials
- Hacker Target

Ransomware

- 2 Malware that can encrypt data and make you pay to get them back.
- Infected Pen Drive
- User is Infected by Ransomware
- User Data is Locked
- Ransom Demand To Unlock Data

Denial-of-Service (DoS)

- 3 Loading excessive load on a machine or network so that it stops working normally.
- Hacker
- Bot
- Open DNS Server
- Target Server

Man-in-the-Middle (MitM)

- 4 Engaging in covert interception and manipulation of communication between two parties without noticing it.
- User
- Hacker
- Web App
- Original Connection

SQL Injection

- 5 To get the Access to the database, Vulnerabilities in Database queries can be exploited
- Hacker
- Web API Server
- Victim's SQL DB Server
- `http://website.com?user=99`
- `SELECT * FROM users..`
- Data For all users is returned to attacker
- Return data For all users

Cross-Site Scripting (XSS)

- 6 Putting malicious code into websites that other people visit.
- Database
- Server
- INSERT
- SELECT
- POST/comment.php?text script-alert(1)/script>
- <script>alert(1)</script>
- <html><script>alert(1)</script></html>

Zero-Day Exploits

- 7 Attacks take advantage of unknown vulnerabilities before programmers can fix them.
- A Security Flaw Exists
- Hacker Discovers it
- Attack is Launched
- Developers Detect attack and have 0 days to mitigate it

DNS Spoofing

- 8 Sending DNS queries to malicious sites so that they can be accessed without permission.
- User
- DNS
1. Injects Fake DNS Entry
2. Issues request to real website
3. Request Resolves to fake website