CYBER SECURITY REPORT

NETWORK SECURITY THREATS

Network Security Threat

In today's day to day life, we often experience or hear about hacking down of devices or vulnerable attacks on devices often leading to leak of official and confidential files. These includes online frauds like phising, DoS attack, blackmailing, DNS Spoofing and many more. In simple word we can refer it as e-crime.

Network Security Threat can be defined as any malicious activity that **compromises** the **confidentiality** and **integrity** of online data and systems. The purpose of these threat is to exploit system vulnerabilities or finding loopholes to penetrate or gain unauthorized access to company networks and inflict damage to sensitive data, applications, and workloads. It can be performed by many ways like detecting weak spots in system through IP address scanning to whale phising or sending coded messages, Images or videos which if user opens either accidentally or purposefully will give access of the device to cyber criminals or sender and result in loss of financial and personal data's. One of the fact of cyber crime's according to Cloudwards Cybersecurity Statistics 2024 is ***"Cybersecurity intrusions had been increased by 613% from 2013 to 2023".***

These are the raw and estimated data's and can vary under some circumstances but still exist as point of worry among online world where a single mistake can risk everything. Staying ahead of network threats is difficult, but not impossible. One needs to understand the nature of different network security vulnerabilities in their own system as the first step of mitigating the security risk. Since, perpetrators constantly search for ways to take advantage of network vulnerabilities in the dynamic virtual world and so recognizing the typical categories of network security weaknesses can be the first line of defense for your digital assets against intrusions and in this section of my documentation, I will try to share everything that I had learnt after deep research and study in the field of cyber threats and ways to stay safe from these attacks.

Common Security threats :-

- **Malware Attacks:** Viruses, worms, ransomware, and spyware.

- **Phishing:** Deceptive attempts to steal credentials or sensitive Information.

- **Unauthorized Access:** Exploiting weak authentication to break into systems.

- **DoS/DDoS Attacks:** Overwhelming systems to make them Unavailable.

- **MITM Attacks:** Intercepting and altering communication between two parties.

- **SQL Injection & Exploits:** Attacks exploiting software or database vulnerabilities.

The above are the forms of security threats that exist in these world of Internet.

DoS/DDoS Attacks :-

DoS/DDoS or **Denial of Service (DoS) attack** is a malicious attempt to disrupt the normal functioning of a server, service, or network by overwhelming it with a flood of traffic or sending malicious requests. When a attacker launch from multiple sources simultaneously, it result in malfunctioning of the system and thus disrupting the server and this process of launching from multiple sources is called **Distributed Denial of Service (DDoS) attack**.

How it works :-

Attackers use vulnerabilities in protocols, networks, or applications to overload a system. It includes methods like Flooding Requests, Exploiting Protocol Weaknesses, Application Layer Exploits, etc.

Detailed view of the following are as follow:-

Flooding Requests:- In this method,

- The attacker sends a huge volume of traffic (packets, requests, or queries) to target and the target system uses all its bandwidth, CPU, or memory to handle the load which result in failure of device and may result in Loss of data

Exploiting Protocol Weaknesses :- In this method,

Hackers exploit how protocols like **TCP/IP, UDP, ICMP** work. For example, they send incomplete connection requests (SYN flood), forcing the server to wait indefinitely.

Application Layer Exploits

Attackers simulate normal user requests (like repeated HTTP GETs to a website) and the server crashes under too many fake "legit-looking" requests.

Real incident that took in history :-

- In 2018, GitHub faced the **largest DDoS attack ever recorded at the time** — 1.35 terabits per second (Tbps).

- Dyn DNS attack from Mirai botnet, built from hacked IoT devices (like cameras & routers), attacked DNS provider **Dyn**. This brought down Netflix, Twitter, Amazon, and Reddit.

- The entire country of Estonia faced large-scale DoS attacks against banks, media, and government services, allegedly from political hackers.

Impacts of DoS Attacks

1. **Financial Loss** – Companies lose revenue during downtime.
2. **Reputation Damage** – Customers lose trust if services keep failing.
3. **Operational Disruption** – Critical apps (banking, healthcare, e-commerce) stop working.
4. **Legal/Compliance Issues** – Some industries (finance, healthcare) must meet uptime regulations.

Prevention & Defense Mechanisms :-

To prevent and defend from these attacks requires a layered strategy of firewalls, IDS, cloud mitigation, and monitoring.

Man-in-the-Middle (MITM) Attacks :-

A **Man-in-the-Middle (MITM) attack** occurs when a cybercriminal secretly intercepts and possibly alters communication between two parties who believe they are directly communicating with each other.

In simple words it's like a postman secretly opening, reading, and rewriting letters before delivering them.

How MITM Attacks Work :-

MITM typically involves three steps:

Interception:

- In this attacker positions themselves between the victim and the service.
- Example: Hijacking a public Wi-Fi or spoofing IP/DNS/ARP.

Decryption (if needed):

- If interception fails due to communication is encrypted, attacker tries to downgrade or bypass encryption (e.g., SSL stripping).

Manipulation:

- Attacker can read, steal, or modify messages.
- Example: Change "transfer ₹1000" to "transfer ₹10,000."

Types of MITM Attacks :-

Passive MITM (Eavesdropping)

- In this method attacker only listens without altering communication.
- Example: Sniffing unencrypted Wi-Fi traffic.

Real life example can be someone listening phone calls between two people secretly without knowing them.

Active MITM (Interception + Alteration)

- In this method attacker modifies the communication and change according to itself.
- Example: Redirecting funds in an online banking session.

Real life example that can be for relating this case is postman changing the content of your letter before delivering it.

Techniques Used in MITM

Packet Sniffing:

- Using Tools like Wireshark capture data packets over insecure networks.

ARP Spoofing (LAN Attack):

- In this technique, Attacker sends fake ARP messages, linking their MAC address to victim's IP.
- All victim's traffic flows through attacker.

DNS Spoofing:

- An easy but dangerous technique in which User types "www.bank.com" → attacker redirects them to a fake lookalike site.

IP Spoofing:

- Attacker pretends to be a trusted IP address.

SSL Stripping:

- Attacker downgrades HTTPS (secure) connection to HTTP (insecure) in such way that Victim thinks they are secure but actually exposed.

Wi-Fi Eavesdropping (Evil Twin Attack):

- Attacker sets up a fake Wi-Fi hotspot (same name as genuine one) when Victim connects, attacker sees all data.

Real-World MITM Attacks :-

- In 2011, Hackers compromised a Dutch Certificate Authority and issued fake SSL certificates. This allowed MITM attacks on Gmail and other services.
- In 2015, an odd case is found in which Pre-installed adware created fake security certificates were found in Lenovo laptop which enabled attackers to inject ads and spy on encrypted traffic.
- Hackers used cheap devices to create rogue Wi-Fi access points in airports/cafes, tricking people into connecting which is also known as Wi-fi pineapple attacks.

Impacts of MITM Attacks

MITM results in thefts like -

- **Credential Theft:** Passwords, banking info stolen.
- **Identity Theft:** Victim's personal info misused.
- **Financial Fraud:** Unauthorized money transfers.
- **Corporate Espionage:** Sensitive data leaks.
- **Trust Damage:** Users lose trust in online platforms.

Detection of MITM attacks :-

MITM attacks can be postponed by detecting it at earlier stages only. During attacks symptoms or messages popped up like

- Sudden SSL certificate warnings in browsers.
- Unusually slow or dropped connections, Suspicious login failures or sessions from unknown devices.
- Different website URLs/IPs than usual.

---- safety measure that can be taken includes using of https websites, avoiding public wifi for banking or critical login, using VPN for encryption and enabling Multi factor authentication, etc.

Spoofing:

Spoofing means **forging or faking information** to trick a computer system or user into believing it is coming from a trusted source. In simple terms it's like **caller ID fraud** → someone calls you, and your phone shows it's from your bank, but in reality, it's a scammer.

In networking, spoofing is used to:

- Bypass security.
- Redirect communications.
- Steal sensitive information**.**

Types of Spoofing Attacks:

A. IP Spoofing

- In this category, the attacker forges the **source IP address** of packets to make victim believes that the packet had came from a trusted IP.
- It is Commonly used in **DoS/DDoS attacks** to hide the attacker's real identity.

Analogy: Sending a letter but writing someone else's address as the sender.

B. ARP Spoofing (LAN-based MITM Attack)

- ARP or Address Resolution Protocol (links IP ↔ MAC address).
- In thi type, attacker sends fake ARP messages, associating their MAC with the victim's IP which results in diverting of traffic through the attacker to victim's.

Analogy: In an office directory, attacker changes the mapping so that phone extension rings on their desk.

C. DNS Spoofing

- In thi s category, attacker alters DNS responses so that a legitimate domain (like www.bank.com) points to a **fake malicious server**.
- Commonly Used in phishing & MITM attacks.

Analogy: You ask for directions to the bank, but someone sends you to a fake shop that looks like a bank.

D. Email Spoofing

- Attacker forges the "From:" field in emails.
- In this category, Victim receives an email that *appears* to be from a trusted source (like bank, PayPal, or a professor).
- Commonly used in **phishing scams**.

Analogy: A scammer signs a letter pretending to be your bank manager.

E. Caller ID / SMS Spoofing

- As name states, attackers fake caller IDs or SMS numbers to appear as if messages are from trusted contacts (e.g., OTP scams).

F. GPS Spoofing

- Fake GPS signals trick devices into believing they are at a different location.
- Commonly used against **drones, ships, or navigation systems**.

Real-World Examples of Spoofing:

- In 2016 hackers modified DNS settings of Brazil in millions of routers, redirecting users to fake banking websites.
- IN 2013, Attackers sent fake emails to employees from "CEO" asking for urgent money transfers which results in millions of lost.
- A best example of GPS spoofing is been seen previous months where Indian Air force creates a fake navigated drone in the area of Pakistan border through help of AI and this was so realistic that Pakistan Air Force considered it the original one thus misleading their attacks and successful execution of Mission Operation sindoor.

Consequences of Spoofing

- **Financial theft** (redirecting payments).
- **Credential theft** (stealing usernames/passwords).
- **System compromise** (injecting malware via fake packets).
- **Loss of trust** (users stop trusting emails, websites, or systems).

Defense Mechanisms Against Spoofing:

- A strong defense against spoofing can be done by packet filtering

ARP Inspection, using spam filters and email security gateways.

- Always check websites URLs, be cautious of unsolicited emails or OTP request .

There are still many categories of internet security threat and discovering them and learning from them can be a efficient way to live in this world of online Fraudsters.