Report on common network security threats

Objective:
Writing a thorough research report on common networking security threats.

Steps Taken:
1.Research and explain common network security threats
2.Describe how each threat works, its impact, and how to mitigate it.

Common Network Security Threats:
***** IP Spoofing
* Routing Table Poisoning
* Active Reconnaissance
* Fragmentation Attack
* TTL Manipulation
* Burnout in security teams
* DDoS Attack
* Man-in-the-Middle (MITM) Attack

Findings:
1.IP Spoofing: When a threat actor forges the source IP address. Threats actors tamper with the IP header of a packet to forge the source IP address. This is then accepted by the system because it seems legit. The impact of this attack can be dire. This can cause a security breach where the threat actor can have unauthorized access to sensitive information like usernames and passwords. The threat actor can also have unauthorized access to the system. The threat actors can also steal information and invade firewalls if they are misconfigured.

2.Routing Table Poisoning: When the information in the routing table is altered. This inhibits the router from sending packets through a router. The packets are going to be transmitted to a threat actor. The user will not be

able to access the network. This can lead to traffic being redirected and threat actors gaining unauthorized access to the system. This can increase latency and waste bandwidth this will lead to packets being lost.

3.Active Reconnaissance: This network attack interacts directly with the targeted system so that they can gather information on how to exploit the system. Active scanning can trigger alerts and if the intruder floods the system with alerts this will then cause the security team to be overwhelmed with alerts which can cause burnout since they are human. This will create a loophole in the system. This is where the threat actor will exploit the network or system. The threat actor can also gather information like open ports and services running.

4. Fragmentation Attack: When the process where IP packets are broken down into smaller parts is intercepted. Threat actors can use this as a foundation of an attack especially if there are many hidden threats inside multiple fragments, this will bypass Intrusion Detection System (IDS), and Intrusion Prevention Systems (IPS). Fragmentation attacks if too many can overwhelm the CPU, which makes the computer more vulnerable to more drastic attacks.

5.TTL Manipulation: In this attack, threat actor sends packets with artificially low Time to Live (TTL) values to disrupt network monitoring. This attack also causes the system to crash or become unresponsive. When the attack is created the threat actor can insert malicious code which can install malware silently.

6.Burnout in security teams: Burnout occurs when security teams get tired and that often leads to human error. Constant pressure does affect the mind and sometimes causes brain fog. System alerts can often be flooded with a lot of false positive alerts which can make it easy for security teams to miss the alerts that are more imperative. Threats are constantly evolving so catching up with threats, increases the pressure of constantly defending the organisation.

7.DDoS Attack: The Distributed Denial of Service attack aims to disrupt traffic by overwhelming it. Flooding the traffic slows down the network and sometimes users cannot access the network or system. This also causes downtime which in most cases contributes to financial loss because there is no productivity. It also affects the operations within the organisation. Incident response and handling will be delayed. The organisation's reputation will also be negatively affected. Threat actors can also use this as the door to creating more attacks.

8.Man-In-The-Middle (MITM) Attack: The threat actor intercepts the communication between two parties and eavesdrops. This attack compromises the integrity of the information transmitted. This attack leads to data theft and identity theft. An individual's information can be used in fraud. Once the threat actor uses this attack as an entry point. They can use the access they have to cause further damage.

Recommendations:

1.IP Spoofing: Block packets from invalid source IP addresses.
Use packet inspection tools like Wireshark and SolarWinds. One can also use the tcpdump command since it captures and filters packets.

2.Routing Table Poisoning: Use cryptographic authentication on routing updates. Use SIEM tools to detect anomalies in routing behaviour. Use route poisoning in a defensive way, mark failed routes with an infinite metric. Use Zeek to detect anomalies in in routing updates and traffic.

3.Active Reconnaissance: Use Access List Controls to block unauthorized scanning. Have an IDS and Multi-Factor Authentication (MFA) to stop threat actors from using information gathered to escalate privileges. Have a honeypot in place. Tools one can use are Snort and Fail2Ban.

4.Fragmentation Attack: Firewalls should reassemble packets before inspection. Make sure that the operating system and network are always up to date. Block overlapping packets or packets that are too small. Tools like Fragrouter and Suricata can be used.

5.TTL Manipulation: Drop packets below the safe threshold TTL value. Do guard against being flooded by expired TTL by using Control Plane Placing (CoPP). Tools like Linux sysctl and Wireshark can be of great assistance in handling this attack.

6.Burnout in security teams: Use tools like SOAR that permit automation. There must not be shortage in the security team staff. There must be work-life balance and workers must not be contacted about work matters when they not on duty so that their minds can rest to function properly. Refrain from unrealistic workloads. Invest in your team, motivate them to do better. Tools like Elastic Stack and Microsoft Viva Insights can also help.

7.DDoS Attack: When monitoring the traffic for a long time you get to know it at the back of your head. You get to understand it well which makes it easy to spot anomalies. Create a DDoS Response Plan. Network segmentation must be done to reduce the attack surface. Web Application Firewalls (WAF) must be in place as well. Tools like Suricata and Zeek can also be used.

8. Man-In-The-Middle (MITM) Attack: A Network Intrusion Prevention Systems (NIPS) can be used to block traffic in network boundaries. Make sure that data in transit is encrypted. Train users so that they can be more aware on such attacks and be able to prevent them from happening. Everyone in the organisation must use a VPN. Use Bettercap/Ettercap to simulate MITM attacks to test the strength of defence. Mitmproxy and other SIEM tools can be of great assistance.

Real-world examples of attacks:

1. IP Spoofing- Mirai Botnet Attack (2016)

What happened: The Mirai malware infected thousands of IoT devices (like routers and cameras), turning them into a massive botnet. How IP spoofing was used: Attackers forged the source IP addresses of packets to make them appear as if they came from legitimate sources. This made it nearly impossible to block the traffic by IP alone. Impact: Over 1 terabit per second of traffic was directed at DNS provider Dyn.

Major websites like Netflix, Twitter, Reddit, and Amazon were knocked offline. The attack disrupted internet access across large parts of the U.S. and Europe.

2. Routing Table Poisoning- BGP Hijacking Incident
Example: In 2008, Pakistan Telecom accidentally poisoned BGP routing tables to block YouTube. How: They advertised incorrect BGP routes, causing global traffic to reroute through Pakistan. Impact: YouTube was inaccessible worldwide for hours. This incident highlighted how vulnerable global routing infrastructure is to poisoning.

3. Active Reconnaissance- DNC Hack (2016)
Attackers: Fancy Bear (Russian APT). Recon Techniques: spear-phishing using OSINT from social media. Internal network mapping and email monitoring. Impact: leaked sensitive political communications during U.S. elections.

4. Fragmentation Attack- Teardrop Attack
What happened: attackers sent fragmented IP packets with overlapping offset values. Target: vulnerable systems running Windows NT, Windows 95, and early Linux kernels. Impact: systems crashed or rebooted due to errors during packet reassembly. It caused Denial of Service (DoS) by overwhelming the target's ability to process malformed fragments. Why it worked: The operating systems couldn't handle overlapping fragments properly, leading to buffer overflows and system instability.

5.TTL Manipulation- TTL Manipulation in Firewalking
Firewalking is a reconnaissance technique that uses TTL values to map firewall rules. Attackers send packets with TTLs that expire just beyond the firewall. Based on ICMP "Time Exceeded" responses, they infer which ports and protocols are allowed.

6.Burnout in security teams- Case: Lumma Stealer Infection Due to Burnout Malware: Lumma Stealer — a simple phishing-based infostealer disguised as a CAPTCHA script. Cause: the security team had overlooked

basic safeguards like PowerShell restrictions and phishing training. Why it happened: the team was overwhelmed by alert fatigue and tool overload. Shrinking budgets and rising expectations led to deprioritization of routine tasks. Burnout caused missed updates, weak endpoint oversight, and poor hygiene enforcement. Impact: the malware spread internally and exfiltrated sensitive data, despite being easily preventable.

7. DDoS Attack- Dyn DNS DDoS Attack (2016)
Target: Dyn, a major DNS provider. Attack Vector: The Mirai botnet, composed of over 100,000 compromised IoT devices (like cameras and routers), launched a massive DDoS attack. Method: attackers flooded Dyn's DNS infrastructure with junk traffic, making it impossible for users to resolve domain names. Impact: major websites including Twitter, Netflix, Reddit, GitHub, PayPal, and Airbnb were knocked offline. The attack peaked at 1.2 Tbps, one of the largest at the time. It exposed the vulnerability of core internet infrastructure and the dangers of insecure IoT devices.

8. Man-In-The-Middle (MITM)- NSA MITM Attack on Google (2013)
What happened: The NSA intercepted traffic between Google's data centers using forged SSL certificates.
Technique: They spoofed Google's SSL encryption, making it appear as if users were securely connected to Google, while the NSA was decrypting and monitoring the traffic. Impact: massive surveillance of U.S. citizens and global users. Sparked global outrage and led to major reforms in encryption and data privacy. Google responded by encrypting internal data center traffic and strengthening certificate pinning.