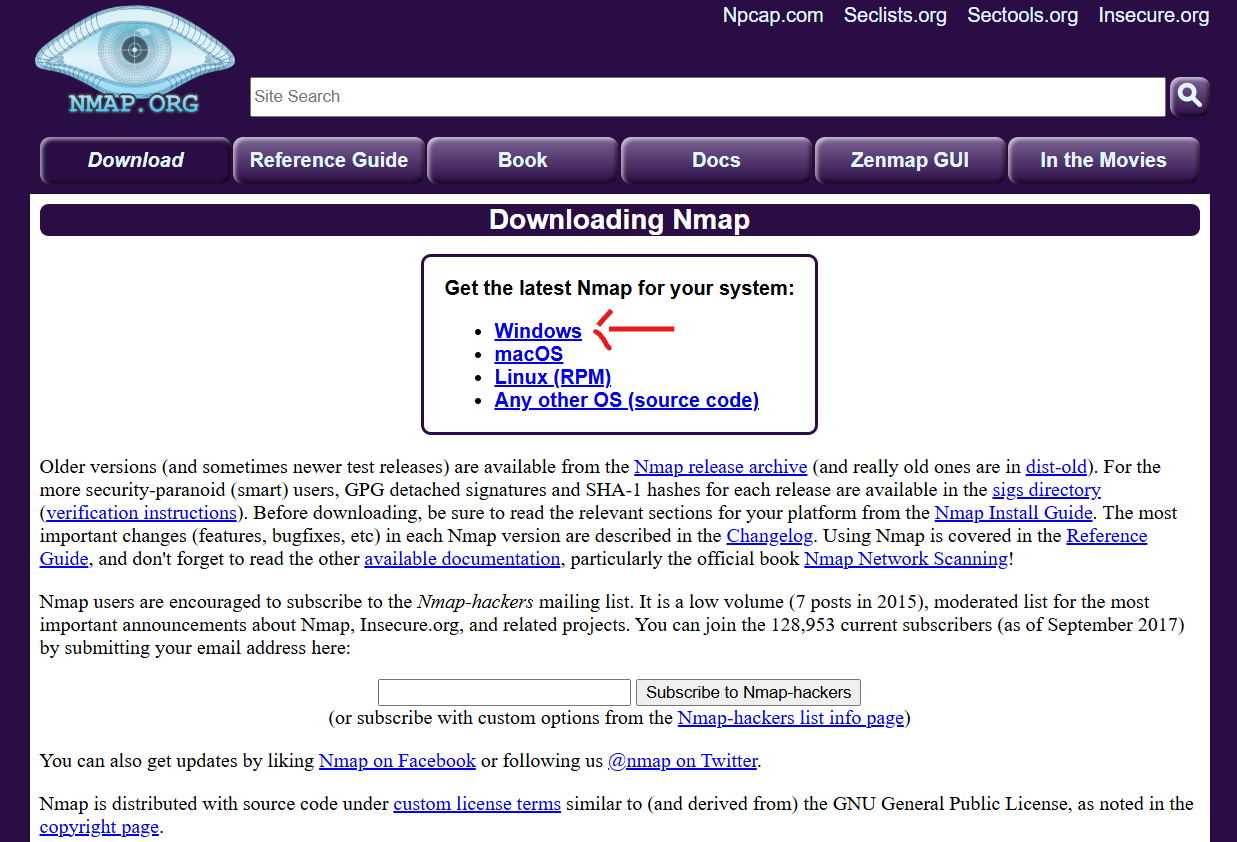
**TASK -1**

**Scan your Local Network for Open ports**

**[Tools Used:** Nmap, Wireshark**]**

**Installing Nmap**

1. Go to <https://nmap.org/download.html>
2. Click on Windows

****

1. Click on the Latest stable release self-installer

**A screenshot of a computer

AI-generated content may be incorrect.**

1. Once the download is complete, locate the nmap-version-setup.exe file and double click on it to run
2. Click Yes to the prompt to allow the app to make changes to your device
3. Click Agree after reading the License Agreement
4. Choose the default components and click Next
5. Choose the installation path and click Install
6. Accept the default settings
7. Click Install and Finish once Npcap is done

**Finding the IP Range**

1. Open the command prompt on the system and type in the below command **ipconfig**

****

1. From the available information, look for the “Wireless LAN adapter Wi-Fi:”

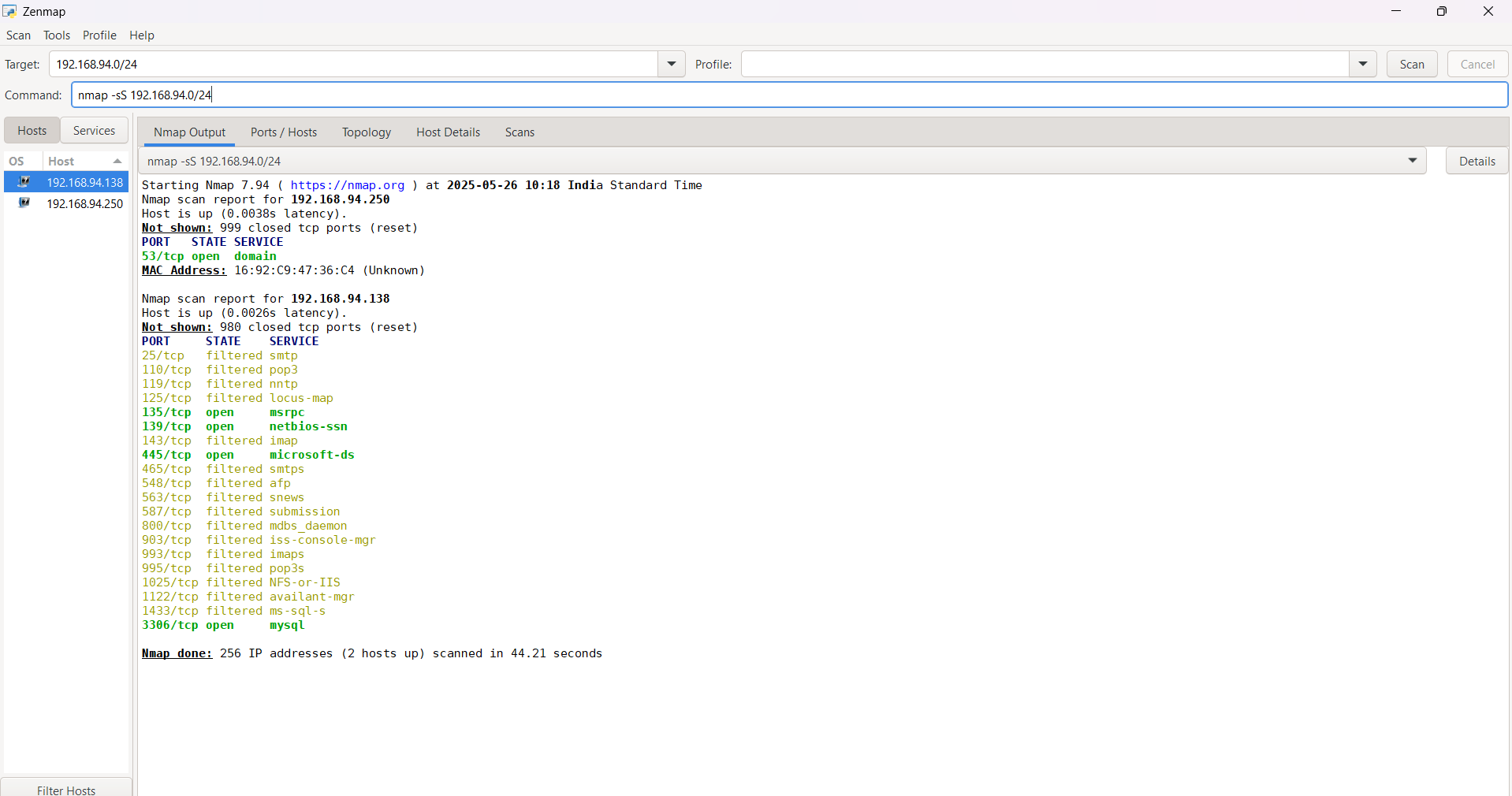
**A screenshot of a computer

AI-generated content may be incorrect.**

1. Here, from the IP address, subnet mask and default gateway, the IP range is found
2. The IP range is **192.168.94.0/24**

**Perform TCP SYN Scan using Nmap:**

1. Type the command **nmap -sS 192.168.94.0/24** and click enter
2. The list of hosts and the open ports are displayed below



1. The two hosts are **192.168.94.138** and **192.168.94.250**
2. The host **192.168.94.250** is a **DNS** server and it has only port **53** open which is used for DNS services
3. The host **192.168.94.138** is the IP address assigned for the system to access internet and the open **4 tcp ports** are **135, 139, 445, 3386**. There are **16 filtered** ports too

**Open, Filtered and Closed Ports**

**1. Open Port**

**Simple Meaning:** There's an application or service actively listening and ready to communicate on that port.

**Analogy:** This is like a door that's wide open and someone (a receptionist, a shop owner) is standing there, ready to greet you and do business.

**Technical Detail:** When a port scanner sends a probe (like a knock on the door), the target system responds in a way that clearly indicates a service is running and accepting connections.

**Security Implication:** This is the primary goal for both legitimate users (who want to use the service) and attackers (who want to find vulnerable services). Each open port is a potential entry point.

**2. Closed Port**

**Simple Meaning:** No application or service is currently listening on that port, but the port itself is accessible.

**Analogy:** This is like a locked door that you can still reach and knock on. The building's security system (operating system) responds by saying, "Nobody's home on this door."

**Technical Detail:** When a port scanner sends a probe, the target system explicitly responds with a "port unreachable" or "reset" message, indicating no service is listening.

**Security Implication:** While not an immediate vulnerability, a closed port still tells an attacker that there's a live computer at that address. It also means the port could become open later if a service starts.

**3. Filtered Port**

**Simple Meaning:** A firewall, router, or other security device is blocking or "filtering" the connection attempts to this port. The scanner can't tell if a service is listening or not.

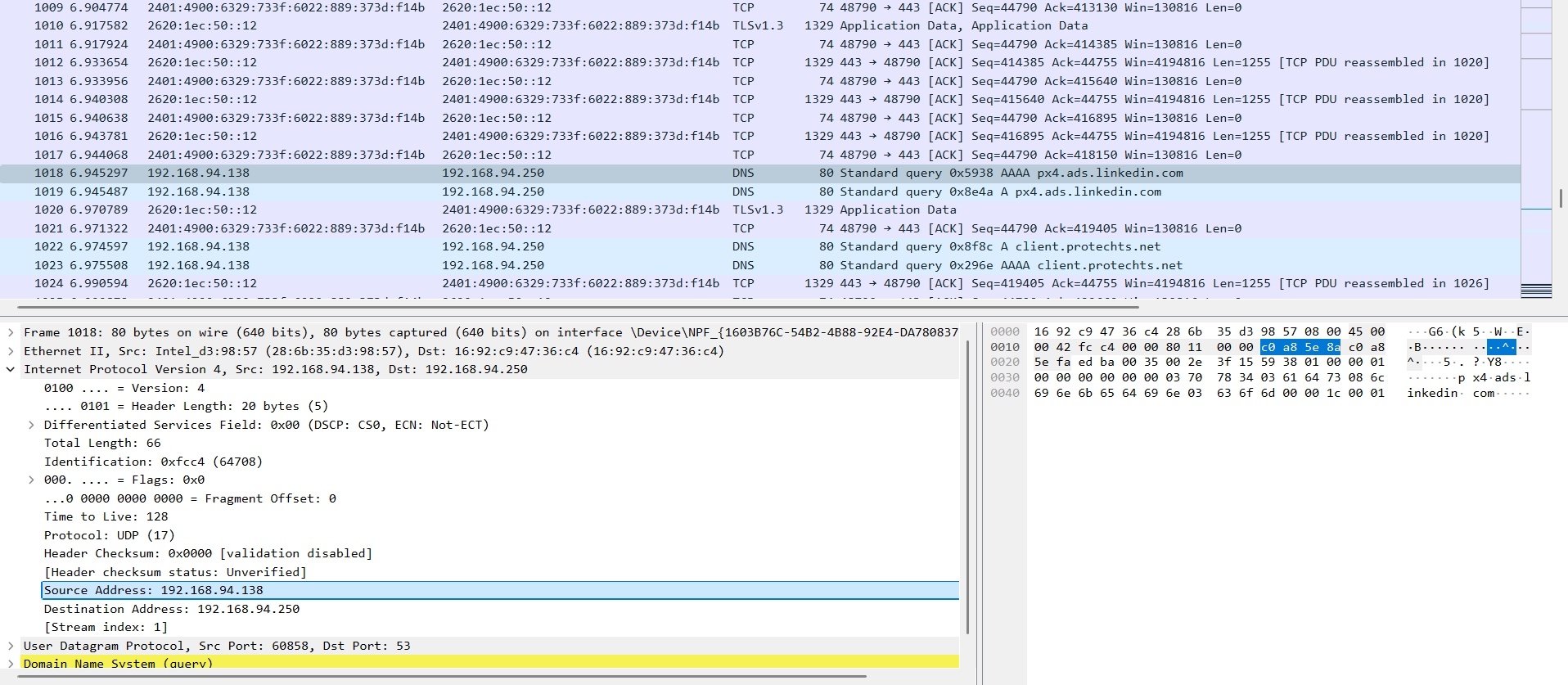
**Analogy:** This is like a door behind a bodyguard or a thick, soundproof wall. When you knock, you get no response at all, or perhaps a vague message that the bodyguard is "not accepting visitors." You don't know if there's someone inside or not.

**Technical Detail:** When a port scanner sends a probe, it receives no response back, or sometimes an ICMP "administratively prohibited" error. The firewall is simply dropping the packets.

**Security Implication:** This is generally good from a security standpoint because it provides the least information to an attacker. It hides the true state of the port, making it harder for an attacker to determine if a service is running behind the filter. However, it also means Nmap (or other scanners) can't definitively say if the port is open or closed, only that it's protected by a filter.

**Packet Capture with Wireshark**

1. In the below captured Wireshark packets, the highlighted blue packet has the destination address of the DNS server as found by the Nmap Scan



1. Here, the source address is the device’s IP address, it sends query to the DNS server to fetch the right IP address for the given domain linkedin.com
2. The DNS uses port 53, which is also available in the Wireshark capture
3. With the help of Wireshark, each packet can be analyzed for detailed inspection

**Common Services running on ports**

1. **Port 53** – As already mentioned above in the Wireshark capture, the port 53 is used for running DNS services. DNS is a critical service that translates human-readable domain names (like google.com) into machine-readable IP addresses (like 172.217.160.142) that computers use to locate each other on the internet. Without DNS, you wouldn't be able to browse websites, send emails, or use most internet services by their domain names.

**Risks**:

**DNS Amplification/Reflection Attacks (DDoS):**

* This is one of the most significant risks. Attackers send small DNS queries to an open DNS resolver (a server that will answer queries from anyone) while spoofing the source IP address to be that of their target
* The DNS resolver responds with a much larger DNS response (amplification) to the spoofed IP address
* By sending many such small queries to multiple open resolvers, attackers can flood the target with massive amounts of traffic, leading to a Distributed Denial of Service (DDoS) attack

**DNS Cache Poisoning / DNS Spoofing:**

* **Cache Poisoning:** Attackers inject forged or malicious data into a DNS server's cache. When legitimate users query that DNS server, they receive the malicious data, redirecting them to attacker-controlled websites (e.g., a fake banking site to steal credentials)
* **DNS Spoofing:** Similar to cache poisoning, but might involve directly sending forged DNS responses to a client, tricking them into connecting to a malicious server instead of the legitimate one

**DNS Hijacking:**

* Attackers gain unauthorized control over a DNS server or a domain's DNS records, redirecting traffic for an entire domain to their malicious servers. This can be achieved by compromising the DNS server itself or the domain registrar account

**Data Exfiltration (DNS Tunneling):**

* Attackers can use DNS queries and responses to tunnel data out of a compromised network, bypassing traditional firewalls and security controls. Since DNS traffic is often allowed, they can encode sensitive information within DNS requests or responses to secretly leak data

**Information Gathering / Reconnaissance:**

* An open DNS server can be queried to gather information about a network's internal structure, domain names, subdomains, and other sensitive details that can aid in further attacks

**Brute-Force Attacks:**

* While less common on port 53 itself, if the DNS server software has vulnerabilities, attackers could try to brute-force credentials or exploit other weaknesses

**Security measures:**

**Restrict Access (Firewalling):**

* Crucial: Do not expose your DNS server to the public internet unless it's explicitly designed to be a public-facing authoritative DNS server for your domain
* Implement strict firewall rules (ACLs) to allow DNS traffic only from trusted sources (e.g., your internal network, specific trusted DNS resolvers)
* If you must run a public-facing DNS server, ensure it's only an authoritative server for your domains and does not act as an open recursive resolver (meaning it should not answer queries for domains it's not authoritative for from arbitrary external IPs)

**Implement DNSSEC:**

* DNS Security Extensions (DNSSEC) add cryptographic signatures to DNS data, allowing resolvers to verify the authenticity and integrity of DNS responses. This helps protect against cache poisoning and spoofing

**Rate Limiting:**

* Configure your DNS server to rate-limit responses and queries from a single source to prevent it from being used in amplification attacks

**Keep Software Updated:**

* Regularly patch and update your DNS server software (e.g., BIND, Microsoft DNS, Unbound) to protect against known vulnerabilities

**Monitor DNS Traffic:**

* Implement logging and monitoring of DNS queries and responses to detect unusual activity, such as unusually high query volumes, strange query types, or suspicious source IPs

**Separate Recursive and Authoritative DNS:**

* If you manage both, run your public-facing authoritative DNS servers separately from your internal recursive DNS resolvers. This limits the attack surface

1. **Port 135 –** This port is used by Windows Remote Procedure Call (RPC) Endpoint Mapper service. It is crucial for many core Windows services and applications, especially in a network environment, including:

* **Active Directory (AD):** Essential for managing users, computers, and resources in Windows domains
* **Windows Management Instrumentation (WMI):** Allows administrators to manage Windows systems remotely
* **Microsoft Exchange Server:** Used for email, calendaring, and contact synchronization
* **Distributed Component Object Model (DCOM):** Enables object-based communication between applications on different machines
* **Windows Updates:** Can be involved in the process of systems receiving security patches
* **Distributed File System (DFS):** Used for managing shared folders across multiple servers
* **Other remote management tools:** Many remote administration and management tools for Windows rely on RPC

**Risks:**

If left exposed to the public internet, it can be vulnerable to exploits, including:

* **Remote Code Execution (RCE):** Attackers could potentially run arbitrary code on a vulnerable system
* **Sensitive Data Exposure:** Gaining access to information about services running on the system
* **Denial-of-Service (DoS) Attacks:** Overwhelming the port with requests to disrupt service

**Security measures:**

* **Firewalling:** Port 135 should generally not be exposed to the public internet. If you need remote access, use a VPN or restrict access via firewalls to only trusted internal IP addresses
* **Disable if Not Needed:** If you are not in a Windows environment or do not require remote access and management capabilities, you should consider blocking or disabling port 135
* **Regular Patching:** Keep your Windows systems and applications up to date with the latest security patches to mitigate known vulnerabilities

1. **Port 139 –** It is associated with NetBIOS Session Service. To understand this, it's helpful to know about two related protocols:

* **NetBIOS (Network Basic Input/Output System):** This is an older, non-routable networking API (Application Programming Interface) that provides services for applications to communicate over a local area network (LAN). It handles name resolution (mapping computer names to network addresses), datagram distribution, and session management
* **SMB (Server Message Block):** This is an application-layer network protocol used for sharing access to files, printers, serial ports, and other communications between nodes on a network. It's the foundation of Windows file and print sharing

**Risks:**

Due to its historical widespread use and inherent vulnerabilities in older NetBIOS/SMB implementations (especially SMBv1), port 139 has been a frequent target for attackers, including:

* **Ransomware:** Many ransomware strains (like WannaCry) exploited vulnerabilities in SMBv1 exposed on ports 139 and 445 to spread rapidly across networks
* **Unauthorized Access:** Attackers could exploit misconfigurations or vulnerabilities to gain unauthorized access to shared files and printers
* **Information Gathering:** It can be used to enumerate network resources and users

**Security measures:**

* **Block Port 139 (and 445) from the Internet:** These ports should never be directly exposed to the public internet. Use a VPN if you need remote access to internal file shares
* **Disable SMBv1:** On modern Windows systems, it's highly recommended to disable SMBv1 due to its known security flaws. This also helps reduce the reliance on port 139
* **Firewalling:** Implement strict firewall rules to restrict access to ports 139 and 445 to only necessary internal devices and subnets
* **Patching:** Keep all Windows systems and network devices patched and updated to fix known SMB/NetBIOS vulnerabilities
* **Strong Access Controls:** Ensure proper authentication and authorization for shared resources

1. **Port 3386** - TCP port 3386 is officially registered by the IANA (Internet Assigned Numbers Authority) for GPRS Data, specifically related to GTP' (GPRS Tunnelling Protocol Prime).

* **GPRS (General Packet Radio Service):** This is a 2G/3G mobile data technology that enables packet-switched data transfer over cellular networks
* **GTP (GPRS Tunnelling Protocol):** This is a key IP-based protocol used within mobile core networks (2G, 3G, and 4G/LTE) to manage subscriber data sessions and carry user data. It essentially creates tunnels for mobile data. There are several forms of GTP:
  + **GTP-U (User Plane):** Carries actual user data
  + **GTP-C (Control Plane):** Handles signaling for session management (e.g., setting up and tearing down data sessions)
  + **GTP' (Prime):** This specific variant is used for transferring charging data records (CDRs) from GPRS Support Nodes (GSNs) to the Charging Gateway Function (CGF) for billing purposes

**Risks:**

Given its role in mobile network billing, an open TCP port 3386 on a system exposed to untrusted networks (especially the public internet) can pose significant security risks:

**Billing Fraud and Revenue Loss:**

* **Manipulation of CDRs:** Attackers could intercept or manipulate charging data records, potentially leading to fraudulent billing (e.g., reducing charges for their own usage, or falsely inflating charges for others)
* **Denial of Service (DoS) to Billing System:** Flooding the port could disrupt the charging data transfer, impacting the operator's ability to accurately bill subscribers, leading to revenue loss

**Information Disclosure:**

* **Subscriber Data Leakage:** While GTP' is primarily for charging data, if the protocol or the underlying system has vulnerabilities, it might be possible to glean sensitive subscriber information or usage patterns from the data flow
* **Network Reconnaissance:** An attacker could use the presence of this port to identify the system as part of a mobile core network, providing valuable information for more targeted attacks

**Network Compromise:**

* **Exploitation of Vulnerabilities:** Like any network service, the software handling GTP' traffic on port 3386 might have vulnerabilities (e.g., buffer overflows, authentication bypasses, protocol parsing errors).Exploiting these could lead to:
  + **Remote Code Execution (RCE):** Allowing an attacker to run arbitrary code on the billing system or connected network elements
  + **Privilege Escalation:** Gaining higher-level access to the system
  + **Lateral Movement:** Using the compromised system as a pivot point to attack other critical components within the mobile core network

**Disruption of Mobile Services:**

* A compromise of core network billing systems can indirectly impact mobile service delivery if critical components are disrupted or if the billing system's failure leads to service suspension for subscribers

**Security Measures:**

Securing systems running services on TCP port 3386, especially in a mobile network environment, requires a robust and multi-layered approach:

**Strict Network Segmentation and Firewalling:**

* **Absolute Isolation:** Systems running GTP' services should be placed in highly segmented and isolated network zones (e.g., billing network segments) that are physically and logically separated from other parts of the network and, critically, from the public internet
* **Least Privilege Principle for Firewalls:** Implement strict firewall rules (ACLs) that explicitly allow only the necessary source and destination IP addresses and ports to communicate with port 3386. Block all other inbound and outbound traffic
* **No Direct Internet Exposure:** Port 3386 should never be directly accessible from the public internet. Access should only be from specific, authorized internal network components

**Regular Patching and Updates:**

* Keep the operating system, the GTP' implementation, and any related software components (databases, middleware, etc.) fully patched and up-to-date to address known vulnerabilities

**Strong Authentication and Authorization:**

* If the service involves any form of authentication, ensure strong, multi-factor authentication (MFA) is enforced for all administrative and operational access
* Implement granular access controls (role-based access control - RBAC) to ensure only authorized personnel and systems can interact with the service

**Intrusion Detection/Prevention Systems (IDS/IPS):**

* Deploy IDS/IPS solutions capable of inspecting GTP' traffic for anomalies, known attack signatures, and unauthorized access attempts
* Monitor alerts from these systems diligently

**Logging and Monitoring:**

* Enable comprehensive logging on the system hosting the service and on network devices (firewalls, routers)
* Collect logs centrally in a Security Information and Event Management (SIEM) system
* Actively monitor logs for suspicious activities, failed connection attempts, unusual traffic patterns, or error messages related to port 3386

**Secure Configuration:**

* Harden the operating system and the GTP' application by following security best practices (e.g., disabling unnecessary services, removing default credentials, secure coding practices if custom applications are involved)
* Disable any features or protocols of the GTP' service that are not strictly required for its operation

**Regular Security Audits and Penetration Testing:**

* Periodically conduct security audits, vulnerability assessments, and penetration tests against systems hosting port 3386 to identify and remediate weaknesses before attackers can exploit them

**Potential Security Risks from open ports:**

When you have open ports on your computer or network, it's like leaving unlocked doors or windows in your house. Here are the main security risks,

**Key Security Risks from Open Ports**

* **Easy Entry for Attackers (Exploitation):** Open ports allow services to listen for incoming connections. If these services have security flaws (bugs, unpatched software, weak default settings), attackers can exploit them to gain unauthorized access, install malware, or take control of your system. It's like a burglar finding a specific weakness in your door's lock
* **Data Theft and System Takeover:** Attackers can try to guess passwords (brute-force) or use stolen login details to get into services on open ports (like remote desktop). Once inside, they can steal sensitive data, encrypt your files for ransom (ransomware), or use your computer for their own malicious activities
* **Your System Becomes a Weapon (DDoS Attacks):** Attackers can use your open ports, especially on services like DNS (port 53), to launch attacks against other people or websites. Your system becomes an unwitting participant in a "Distributed Denial of Service" (DDoS) attack, where the target is flooded with traffic
* **Information Leakage (Reconnaissance):** An open port can reveal details about your system, like what software you're running or its version. This information helps attackers plan more effective attacks by knowing exactly what "doors" to target

**Key Security Measures**

**To protect yourself:**

* **Close Unnecessary Ports:** If a port isn't needed for a specific service you actively use, close it immediately. Less open doors means fewer ways in
* **Use Firewalls:** Configure your firewall to act as a security guard, allowing only legitimate traffic to reach necessary ports
* **Keep Everything Updated:** Regularly update your software and operating system. These updates patch security holes that attackers exploit
* **Strong Passwords & MFA:** Use strong, unique passwords and enable Multi-Factor Authentication (MFA) whenever possible for services that require logins

By managing your open ports carefully, you significantly reduce your vulnerability to cyberattacks.