James Munyabugingo

**Task 1: Stealthy Port Scan Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario**: You have been asked to perform a network reconnaissance without alerting the target's security systems. This requires conducting a port scan that doesn't complete the TCP handshake, thereby reducing the likelihood of detection. By sending SYN packets and waiting for responses, you can infer which ports are open, closed, or filtered without establishing a full connection.

**Command:** sudo nmap –sS seclists.org

**Summary notes:**

**Open Ports:** Ports 22 (SSH), 80 (HTTP), and 443 (HTTPS) are open and actively responding to SYN packets.

**Closed Ports:** Ports 70 (Gopher), 113 (Ident), and 31337 (Elite) are closed and responded with RST packets.

**Filtered Ports:** 994 ports did not respond, indicating they may be protected by a firewall or other network security device.

**Task 2: Complete TCP Connection Scan Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario:** For a more thorough analysis, you need to perform a scan that completes the three-way TCP handshake, providing a definitive list of open and closed ports on the target system. This method, while more detectable, ensures that every connection attempt is fully established

**Command:** sudo nmap –sT seclists.org

**Summary notes:**

**Open Ports:** The ports 22 (SSH), 80 (HTTP), and 443 (HTTPS) are open and responded to the TCP connect scan.

**Closed Ports:** Ports 70 (Gopher), 113 (Ident), and 31337 (Elite) are closed and responded with connection refusals.

**Filtered Ports**: A significant number of ports (994) did not respond, which could indicate they are protected by a firewall or other network security measures**.**

**Task 3: Service Version Identification Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario:** To understand the potential vulnerabilities in the target's network, you need to identify the software versions running on the open ports. This information will allow you to check for any known exploits or weaknessesassociated with these  
versions.

**Command:** sudo nmap –sV seclists.org

**Summary Notes:**

**22/tcp (SSH):** Running OpenSSH version 7.4 with protocol 2.0. This service allows secure remote login and command execution. Ensuring that it is updated and configured securely is a great security practice.

**80/tcp (HTTP)**: Running Apache httpd version 2.4.6. This is a widely-used web server software.

**443/tcp (SSL/HTTP**): Also running Apache httpd version 2.4.6, but configured for HTTPS (SSL/TLS). Reviewing SSL/TLS configurations and ensure they are up to date with current security practices.

**Task 4: IP Address and DNS Server Information Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario:** You need to gather basic information about the target by determining its IP address and the DNS server handling its queries. This foundational step will help in understanding the network structure and planning further reconnaissance activities.

**Command:** sudo nslookup seclists.org

**Summary Notes:**

**Server**: The DNS server used for the query was located at IP address 192.168.2.1.

**Non-authoritative Answer:** The result provided is not authoritative, meaning it may come from a cached response rather than directly from the authoritative DNS servers for seclists.org.

**Addresses**: The domain seclists.org resolves to both an IPv4 and an IPv6 address, indicating support for both address types.

**Reverse DNS Lookup Result:** The IP address 50.116.1.184 resolves to the domain ack.nmap.org.

**Task 5: Domain Name Associated with IP Target: 50.116.184**

**Scenario:** To verify the association between the target's IP address and its domain name, perform a reverse DNS lookup. This step ensures that the domain name is correctly mapped to its IP address, which is crucial for accurate targeting and  
reporting.

**Command:** sudo nslookup 50.116.184

**Summary Notes:**

**Reverse DNS Lookup Result:**

* The IP address 50.116.1.184 resolves to the domain ack.nmap.org.
* This means that ack.nmap.org is the PTR record associated with the IP address.
* Reverse DNS Lookups: These are used to verify that an IP address corresponds to a domain name, which can be useful for various network management and security tasks.

**Task 6: Domain Registration Information Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario:** You need to retrieve detailed domain registration information to understand who owns the target domain and how long it has been registered. This data can provide insights into the target's background and potentially reveal contact  
information for further investigation.

**Command:** sudo whois seclists.org

**Summary Notes:**

* **Registrant Details:**
  + **Name:** REDACTED FOR PRIVACY
  + **Organization:** Super Privacy Service LTD c/o Dynadot
  + **Street:** REDACTED FOR PRIVACY
  + **City:** REDACTED FOR PRIVACY
  + **State/Province:** California
  + **Postal Code:** REDACTED FOR PRIVACY
  + **Country:** US
  + **Phone:** REDACTED FOR PRIVACY
  + **Email:** Please query the RDDS service of the Registrar of Record for contact information.
* **Creation and Expiration Dates:**
  + **Creation Date:** October 2, 2003, 05:46:32 UTC
  + **Expiration Date:** October 2, 2029, 05:46:32 UTC
* **DNS Servers:**
  + **DNS Server 1:** ns1.linode.com
  + **DNS Server 2:** ns2.linode.com
  + **DNS Server 3:** ns3.linode.com
  + **DNS Server 4:** ns4.linode.com
  + **DNS Server 5:** ns5.linode.com
* **Registrant Privacy:** The registrant’s personal details are protected by privacy services, and the contact information is managed through Super Privacy Service LTD via Dynadot.
* **Registration Duration:** The domain has been registered since October 2, 2003, and is set to expire on October 2, 2029.
* **DNS Servers:** The domain uses multiple DNS servers provided by Linode, indicating its reliance on Linode’s DNS infrastructure for resolving domain queries.

**Task 7: Reachability of the Target Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario:** To check if the target host is online and reachable, send ICMP Echo Requests. This basic network test will help youdetermine the availability of the target and whether it is responding to network queries.

**Command:** sudo ping –c 4 seclists.org

**Summary Notes:**

**Response Times:** The round-trip times are relatively consistent, with slight variation, indicating stable network conditions**.**

**Packet Loss:** There was no packet loss, suggesting reliable network connectivity to the target host**.**

**TTL (Time to Live):** The TTL value of 51 indicates the number of hops the packets can take before being discarded, which is a standard value for a route.

**Task 8: Identifying Live Hosts in a Network Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario:** You need to discover other potential targets within the same network range as your main target. By performing a ping sweep, you can identify live hosts that might also be of interest for further investigation

**Command:** sudo nmap –sn seclists.org

**Summary Notes:**

* Only the IPv4 address 50.116.1.184 was scanned.
* The scan was completed in 0.24 seconds.

**Task 9: Checking Specific Ports Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario:** To focus on commonly used ports, such as 80 (HTTP), 22 (SSH), and 443 (HTTPS), perform a targeted scan. This will help you determine if these critical services are accessible on the target system, which could be points of entry or interest.

**Command:** sudo nmap –p 22,80,443 seclists.org

**Summary Notes:**

All specified ports (22, 80, 443) are open on the target domain name and could be a point of entry for attackers if not properly secured.

**Task 10: Firewall Filtering Check Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario:** To understand the security measures in place, determine if specific ports are being filtered by a firewall. By sending specially crafted packets, you can infer whether the firewall is blocking access to certain services

**Command:** sudo nmap –p 80,22,443 –sS seclists.org

**Summary Notes**:

All the ports specified (80, 22, and 443) are open and accepting connections. There is no indication that these ports are filtered by a firewall, as the scan results show that the services are responsive.

**Task 11: Comprehensive Target Analysis Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario:** Perform a thorough scan that combines several techniques to gather extensive information about the target, including OS detection, service versions, and traceroute data. This comprehensive analysis will provide a detailed overview of  
the target's network and potential vulnerabilities

**Command:** sudo nmap –A seclists.org

**Summary Notes:**

The aggressive scan reveals that the target is running Apache HTTPD 2.4.6 for both HTTP and HTTPS services. SSH is accessible with OpenSSH 7.4. The scan also identifies a number of ports as filtered, and provides insight into the network route taken to reach the target, showing a total of 17 hops.

**Task 12: Evasion Techniques Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario:** To bypass firewalls and IDS systems, perform a scan that fragments packets. This technique can help evade detection while still gathering information about open ports and running services on the target**.**

**Command:** Sudo nmap -sS -T4 –A –f –v seclists.org

**Summary Notes:**

The scan identified three open ports: 22 (SSH, OpenSSH 7.4), 80 (HTTP, Apache 2.4.6), and 443 (HTTPS, Apache 2.4.6). The server is up with a low latency of 0.071 seconds. The scan also included service detection, OS detection, and traceroute, revealing various Linux versions and embedded systems as potential OS candidates. Additionally, 994 ports were found to be filtered

**Task 13: Silent Scan with no Flags 5 Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario:** Identify open ports using a scan that sends packets with no flags set. This silent method can help determine the state of ports without triggering defensive mechanisms that might be watching for more traditional scan types**.**

**Command:** sudo nmap -sN seclists.org

**Summary Notes:**

The scan revealed that the host is active with a latency of 0.072 seconds. However, the scan results indicated that all 1000 TCP ports were in "ignored" states, meaning no response was received from any of the ports. This result suggests that all scanned ports could be either open and filtered by a firewall or simply not responding to the Null scan technique. The scan, which does not send any flags and relies on receiving responses to infer port status.

**Task 14: Firewall Detection with ACK scan 5 Target:** [**www.seclists.org**](http://www.seclists.org)

**Scenario:** Check if ports are being filtered by a firewall by sending ACK packets. This method helps determine whether a firewall is present and how it is handling incoming traffic**.**

**Command:** sudo nmap –sA seclists.org

**Summary Notes:**

The TCP ACK Scan has identified a number of ports as unfiltered, meaning they are accessible and responding to ACK packets. The high number of filtered ports indicates that there is likely a firewall or security device filtering traffic on the majority of the ports. This scan helps in understanding the network's filtering and security posture but does not provide detailed information about the state of the filtered ports.