Mariam Adegbindin

CIDM 6340 Network Management & InfoSec

NMAP

**What did I do?**

I conducted Nmap scanning on my home network using my IP address (10.251.0.1). I used the command “nmap -F 10.251.0.1” to perform a fast scan of my network. I also used the “nmap - sP 10.251.0.1/24” which performed a ping scan on the IP address range 10.251.0.1/24 which covers the entire network. I checked for open ports that are typically opened when you access a website (Port 80 & 40) using “sudo nmap -sT -p 80,443 10.251.0.1/24”. I also played around with the Nmap vulnerability script “nmap --script vuln 10.251.0.1” The script goes through and analyses the network for any vulnerabilities using CVE’s (Common Vulnerabilities and Exposures). For the IP address, it shows if the host is up and provides the latency of the response when you run the Nmap scripts.

**What were the results?**

The Nmap scan shows that only one host is up after scanning 256 IP addresses. The host 10.251.0.1 has a latency of 0.0056s. There are five ports that show up and 995 filtered tcp ports not shown because there was no response from them. The image below shows the port that are shown with their state and service.

A screen shot of a computer

Description automatically generated

The closed ports suggest that the associated services are not actively listening for incoming connections. We can say having the above ports opened is not inherently a security risk, it depends on the necessity of the service and the security measures in place.

**53/tcp**: Port 53 is open and running a DNS (Domain Name System) service. DNS is used for translating domain names into IP addresses.

**80/tcp**: Port 80 is open and running an HTTP (Hypertext Transfer Protocol) service, which is the foundational protocol for the World Wide Web, used for serving web pages.

**443/tcp**: Port 443 is open and an HTTPS (HTTP Secure) service is operating. Widely utilised on the Internet, HTTPS is the secure iteration of HTTP and is designed to facilitate secure communication over computer networks by encrypting data to protect privacy and security.

**3128/tcp**: Port 3128 is accessible, and the Squid proxy service is operating. The Web caching proxy Squid is compatible with HTTP, HTTPS, FTP, and additional protocols. It caches repeated queries, filters content, and restricts access to controlled content in order to increase the performance of the web server.

**8081/tcp**: Port 8081 is recognised as the destination of the "blackice-icecap" service. While there are numerous possible applications for this, it is frequently associated with software or security services. The actual service operating on this port may, however, be identified by a distinct designation or a default service name assigned by NMAP to this port number. Operating on port 8081 is a prevalent practice among web servers, application servers, and custom services.

Also, the presence of filtered ports indicates the network may have a firewall or other security measures in place to restrict access to certain services.

In checking for vulnerabilities, one host was discovered, and it showed that all hosts are all up and not vulnerable to attacks.

**A screenshot of a computer screen

Description automatically generated**

**What Did You Learn?**

This activity facilitated my comprehension of the significance of being knowledgeable about the protocols and components that comprise a network. Nmap proficiency for host discovery and network monitoring. Identifying exposed channels and services on the network through analysis of the output. By evaluating the services that are exposed, one can acquire knowledge regarding the attack surface of the network. To reduce potential risks, it is crucial to acknowledge the significance of securing services that operate on open ports. To safeguard against prospective attacks and unauthorised access, it is crucial to recognise the importance of network monitoring and access control measures. The importance of assessing potential vulnerabilities and implementing suitable security measures is further underscored in relation to the analysis of the attack surface exhibited by the network. Enhancing the overall network security posture of an organisation or residence and safeguarding against potential cybersecurity threats can be facilitated by the information gleaned from the network mapping.