CIDM 6340

Network Management and Information Security

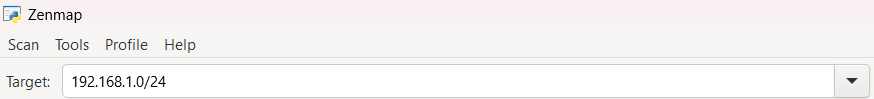
Research Report 1 – NMAP

Vernice Tanquerido

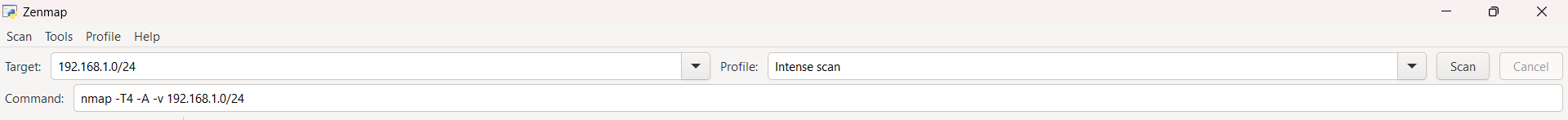
**Question 1: What did you do?**

The focus of the activity is to analyze a medium to large network by mapping out the components and connections using NMAP. However, due to the denial of permission to scan the company network, the home network was used for this assignment.

As a prerequisite to the activity, Nmap was downloaded and installed. The IP address of the network was then identified and entered into the target input box on the Zenmap interface:



An intense scan was then performed to map the network. The intense scan initiates an ARP ping scan first to identify the hosts on the network. It then does a TCP SYN Stealth Scan to determine open ports in the network. To reveal more information about the connection, it would then perform a service scan and OS detection:



After the scan was complete, the devices and their corresponding IP address, device type, protocols and services, and operating system were listed individually in a separate document. Each of these devices was analyzed for open ports, services associated with them, and their potential vulnerabilities or attack surfaces.

To visualize how these devices interact, the topology map was generated.

**Question 2: What were the results?**

Network mapping exposed a diverse collection of components and protocols. The ping scan identified a total of 16 active hosts. A comprehensive scan was performed on each of these components, revealing a variety of devices including mobile, IoT devices, routers, and others.

For each host, the open ports and the corresponding service, device type, operating system, and other details are identified. A sample output is shown below:

A computer screen shot of a computer

Description automatically generated

***Figure 1****. Sample scan report*

Table 1 shows the components identified by nmap on the network. The open ports identified signify the area of the network’s attack surface. These open ports are the entry points into a network therefore it is crucial to identify their vulnerabilities and employ robust security measures to protect the network.

***Table 1****. Components identified by nmap*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Host | Number of open ports | Services | Device type | Operating System |
| 192.168.1.1 | 8 | Domain,http, netbios-ssn, upnp | General purpose (server) | Linux 2.6.12-2.6.36 |
| 192.168.1.105 | 1 (filtered) | glrpc | Not detected | Not detected |
| 192.168.1.109 | 1 | irc | Not detected | Not detected |
| 192.168.1.111 | 4 open, 1 filtered | tcpwrapped, printer jetdirect | Not detected (Printer) | Not detected |
| 192.168.1.112 | 0 |  | Not detected | Not detected |
| 192.168.1.114 | 1 | enpp | General Purpose (PC) | Microsoft Windows 10|11 |
| 192.168.1.115 | 2 | ccproxy-http, ms-wbt-server | General purpose (PC) | Windows 10|11 |
| 192.168.1.117 | 0 |  | Not detected | Not detected |
| 192.168.1.123 | 5 | http, ssl/ajpl3, https-alt, cslistener, scp-config | Media device (Google home) | Google home device |
| 192.168.1.124 | 1 | abyss | Specialized (router) | lwIP 1.4.1 - 2.0.3 |
| 192.168.1.129 | 0 |  | Not detected | Not detected |
| 192.168.1.133 | 2 | tcpwrapped | Phone | Apple iOS 15.X |
| 192.168.1.140 | 6 | msrpc, netbios-ssn, Microsoft-ds, enpp, mysql, http | General purpose (PC) | Microsoft windows 10 |
| 192.168.1.145 | 0 |  | Not detected (camera) | Not detected |
| 192.168.1.147 | 0 |  | Not detected (washing machine) | Not detected |
| 192.168.1.148 | 1 | irc | Specialized | lwIP 1.4.1 - 2.0.3 |

TCP is the main protocol detected with the following services on the open ports. Each of these services, if they have known vulnerabilities, can be exploited. The following are the services identified by nmap on the network and their vulnerabilities:

**Domain.** Domain services store information in a centralized directory and allows users and domains communicate (Lutkevich, 2021). Attackers can exploit this service by using a user’s login credentials to gain access to the system.

**http.** The http service allows a web application to communicate with another web application through the transfer of data (Magidi, n.d.). The transfer of data through plain text opens opportunities for attackers to intercept and read data which can include sensitive information such as passwords (purevpn, n.d.)

**UPnP.**  The universal plug and play service allows devices on the same network to discover and possibly control each other. If the service establishes connections with devices that are infected with malware then the network, then the network can be exposed to malicious activity which can affect other devices also connected to the network.

**MSRP.** The MSRP service allows communication through a remote server. If this is exploited, code execution can be done over the network without requiring authentication or user interaction (Borlea, 2022).

**NetBIOS-ssn.** This service allows users to share resources. This service is vulnerable to revealing computer names, IP addresses, and other sensitive information to attackers.

**MySQL.** Unauthorized access to MySQL and databases could lead to data breaches.

**Jetdirect.** Jetdirect is a service that allows computer printers to be directly connected to the local network. Sensitive information that is sent to printers can be subject to exploitation by attackers. Attackers could also take advantage of this control by accessing internal memory to re-print previous jobs (Guerrero, n.d.)

**https-alt.** An attacker can use the HTTP Alternative Services service to scan all TCP ports of any host that the accessible to a user when web content is loaded (Mozilla Corporation, 2019).

**Irc.** IRC networks and servers are susceptible to Distributed Denial of Service attacks (WIREX, n.d.). The network may be flooded with traffic causing it to freeze and be unable to process legitimate requests.

**ajp13.** A remote, unauthenticated/untrusted attacker might use this AJP configuration to retrieve web application files from a server, exposing the AJP port to untrustworthy clients (Red Hat, 2024).

Other potential attack surfaces on the network can be identified by looking at the types of devices connected and how users interact with them. Each device and interaction creates vulnerabilities, which must be addressed.

Transactions on our computers can create opportunities for attackers to compromise the network. Phishing emails are a common method used by attackers to infiltrate systems. These emails may contain malicious links or attachments that, when clicked or downloaded, can install ransomware on the device.

Aside from the interactions we do on the internet, mobile devices introduce an additional attack surface through SMS spoofing where attackers can send seemingly legitimate messages to deceive users into clicking on links, download malicious software, or disclose sensitive information.

Transferring and accepting data via Bluetooth or AirDrop can also introduce malicious content to other devices which can potentially compromise their security.

For wireless networks, weak security protocols or easily guessable passwords are vulnerable to attacks. Many routers come with default names and passwords which are often visible on the device. Leaving these defaults unchanged significantly increases the risk of network exposure and unauthorized access. Strong and unique passwords and up-to-date security processes are important to mitigate these risks.

Figure 2 shows the topology of the network. All devices are connected to the local host, and there appears to be no direct interaction between the devices themselves beyond this connection.A diagram of a network

Description automatically generated

*Figure 2. Network topology*

The full Nmap scan output and topology map can be found in the attached pdf.

**Question 3: What did you learn?**

Nmap is a great tool to keep track of the devices connected to your network. It is also useful for identifying points of vulnerability or attack surfaces. Through this activity, I have gained a good understanding of the components and protocols that make up a network. I have also learned different techniques and scans that can be done on the network depending on the purpose of the client. I understood how each of the components can be a target of an attack and how important it is to secure the entry points in the network.

This knowledge is valuable to improve the organization’s network security by regularly tracking and monitoring the components connected to the network. With network mapping done, risk assessments and vulnerability checks can be performed as part of the organization’s goal of increased security and continuous improvement.

# References

Borlea, A. (2022, April 20). *CVE-2022-26809 MS\_RPC*. Retrieved from Runecast: https://www.runecast.com/blog-posts/cve-2022-26809-ms-rpc-vulnerability-explained-and-covered#:~:text=An%20integer%20overflow%20in%20MSRPC,requiring%20authentication%20or%20user%20interaction.

Guerrero, S. (n.d.). *Exploiting Printers via Jetdirect Vulnerabilities*. Retrieved from NowSecure: https://www.nowsecure.com/blog/2017/01/13/exploiting-printers-via-jetdirect-vulnerabilities/

Loshin, P. (2021, September). *Secure Shell*. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/definition/Secure-Shell

Lutkevich, B. (2021, July). *Active Directory Domains Services*. Retrieved from TechTarget: https://www.techtarget.com/searchwindowsserver/definition/Microsoft-Active-Directory-Domain-Services-AD-DS#:~:text=Domain%20Services%20stores%20centralized%20directory,login%20credentials%20and%20access%20permissions.

Magidi, P. (n.d.). *HTTP Service Source Step*. Retrieved from Synatic: https://help.synatic.com/en/articles/4719865-http-service-source-step

Mozilla Corporation. (2019, 07 23). *Vulnerability Details : CVE-2019-11728*. Retrieved from CVEdetailscom: https://www.cvedetails.com/cve/CVE-2019-11728/

NordVPN. (n.d.). *TCP Wrapper*. Retrieved from NordVPN: https://nordvpn.com/cybersecurity/glossary/tcp-wrapper/#:~:text=TCP%20Wrapper%20is%20a%20security,let%20them%20in%20or%20not.

purevpn. (n.d.). *HTTP vulnerability*. Retrieved from purevpn: https://www.purevpn.com/ddos/http-vulnerability#:~:text=HTTP%20is%20considered%20less%20secure,passwords%20and%20credit%20card%20numbers.

Red Hat. (2024, June 14). *AJP File Read/Inclusion in Apache Tomcat (CVE-2020-1938) and Undertow (CVE-2020-1745)*. Retrieved from Red Hat : https://access.redhat.com/solutions/4851251#:~:text=The%20AJP%20protocol%20is%20enabled,AJP%20port%20to%20untrusted%20clients.

WIREX. (n.d.). *IRC: Network Protocol Explained*. Retrieved from Wirex: https://wirexsystems.com/resource/protocols/irc#:~:text=DDoS%20attacks%3A%20IRC%20networks%20and,ultimately%20leading%20to%20service%20disruptions.