Layer 1 - Finding rogue devices on the network using Nmap

Nmap, and its uses:

Nmap, or Network Mapper, is a free and open-source utility for network discovery and security auditing. Its many features include host discovery, service and operating system detection, and vulnerability scanning. It's widely used in cybersecurity to find rogue devices on a network, identify open ports, and detect security risks.

Nmap helps find rogue network devices through its host discovery feature. By scanning the IP addresses on a network, Nmap can identify all devices connected to it. Any device that is not recognized or authorized can be considered a rogue device. Nmap can also provide information about the services running on these devices, which can further aid in identifying rogue devices.

In addition to host discovery, Nmap's service and operating system detection capabilities are also useful in identifying rogue devices. By determining the types of services running on a device and its operating system, network administrators can compare this information with their inventory and identify any discrepancies. For instance, if a device is running a service or operating system not typically used in the network, it could be a rogue device.

Moreover, Nmap’s vulnerability scanning feature can detect security risks associated with rogue devices. For example, if a rogue device has open ports susceptible to known vulnerabilities, Nmap can detect them and alert administrators. This makes it easier for them to mitigate potential threats from the rogue device.

Lastly, Nmap's scripting engine allows users to write scripts for more specific tasks, such as detecting certain types of rogue devices. This feature makes Nmap a highly flexible tool for dealing with the complex issue of rogue devices on a network.

Network Intruders

Network intruders are individuals or software, such as viruses, that gain unauthorized access to a network. They often use rogue devices as a means to infiltrate. These devices, which are not recognized or authorized by the network's administrators, can create a backdoor for intruders to access sensitive data, manipulate systems, or disrupt network operations. Therefore, identifying

and managing rogue devices using tools such as Nmap is crucial in maintaining a network's security and preventing intrusion.

Network intruders pose a serious risk to any organization, as they can exploit vulnerabilities in the network to steal sensitive information, disrupt operations, or even launch attacks against other networks. This unauthorized access often involves the use of rogue devices, which can be anything from an unsecured wireless router to a malicious IoT device.

Rogue devices, being unrecognized or unauthorized by the network's administrators, act as a backdoor into the network. They can often go unnoticed, blending in with the multitude of legitimate devices connected to the network. This makes them an effective tool for network intruders, allowing them to bypass conventional security measures.

Nmap, with its versatile set of features, plays a vital role in combating this threat. By scanning the network and identifying all connected devices, it can help administrators identify potential rogue devices. Its service and operating system detection capabilities can further aid in recognizing any discrepancies, such as a device running a service or an operating system not typically used in the network.

Furthermore, Nmap's vulnerability scanning can detect security risks associated with these rogue devices, such as open ports that are susceptible to known vulnerabilities. This allows administrators to take immediate action, closing off these potential entry points and mitigating the risk posed by network intruders.

In essence, the effective use of tools like Nmap is crucial in maintaining a secure network. By identifying and managing rogue devices, organizations can significantly reduce the risk of intrusion and ensure the integrity and security of their networks.

General Network Discovery

General network discovery involves identifying all devices connected to a network, irrespective of their status. It provides a comprehensive view of the network's infrastructure, aiding in the management and planning of resources. Tools like Nmap are instrumental in this process, as they can accurately map out a network's topology. This is the first step in identifying rogue devices and potential security vulnerabilities. Ultimately, general network discovery is a fundamental component of effective network management and security.

You need to know more than just what ports are open, because these services may be listening on ports that aren't built for that purpose. From a safety point of view, you should also know what software and version is behind the port. With Nmap's Service and Version Detection features, you can do a full network inventory as well as host and device finding. You can check every port on every device or host to see what software is running on each one.

Nmap uses monitoring tools that the software may understand to connect to and ask questions about each open port. This way, Nmap can give you a full picture of what's out there instead of just a list of empty ports.

Steps:

1. Use the option -sV to turn on Service and Version Detection.
2. Add the --allports flag to check every port. On its own, Nmap doesn't check port 9100. This port is used by a lot of printers, and Nmap can sometimes make them print.
3. Use -T4 to speed up the processing, since this finding could take a while.

The output:

#nmap -sV --allports -T4 192.168.34.0/24 Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-21 11:28 EDT Nmap scan report for 192.168.34.1 Host is up (0.00013s latency). Not shown: 996 closed TCP ports (reset) PORT STATE SERVICE VERSION 88/tcp open Kerberos-sec Heimdal Kerberos (server time: 2024-03-21 15:29:09Z) 5000/tcp open rtsp AirTunes rtspd 710.79.1 5900/tcp open vnc Apple remote desktop vnc 7000/tcp open rtsp AirTunes rtspd 710.79.1 MAC Address: 3E:22:FB:FE:7B:65 (Unknown) Service Info: OS: Mac OS X; CPE: cpe:/o:apple:mac_os_x

Nmap scan report for 192.168.34.2 Host is up (0.00027s latency). All 1000 scanned ports on 192.168.34.2 are in ignored states. Not shown: 1000 closed tcp ports (reset) MAC Address: 00:50:56:F8:09:C8 (VMware)

Nmap scan report for 192.168.34.254 Host is up (0.00034s latency). All 1000 scanned ports on 192.168.34.254 are in ignored states. Not shown: 1000 filtered TCP ports (no-response) MAC Address: 00:50:56:FA:BC:5E (VMware)

Nmap scan report for 192.168.34.141 Host is up (0.0000030s latency). All 1000 scanned ports on 192.168.34.141 are in ignored states. Not shown: 1000 closed TCP ports (reset)

Service detection was performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 256 IP addresses (4 hosts up) scanned in 32.08 seconds

Let’s break down the key elements of the scan output:

- **Scan Command**: **nmap -sV --allports -T4 192.168.34.0/24**
    - **sV**: Enables version detection, attempting to determine the version of the services running on open ports.
    - **-allports**: Scans all 65535 ports, not just the well-known ports (1-1024) and certain high-numbered ports where specific services are known to run.
    - **T4**: Sets the timing template to "aggressive," speeding up the scan by making more frequent and parallel requests.

    - **192.168.34.0/24**: Specifies the target network range to scan, covering all IP addresses from 192.168.34.0 to 192.168.34.255.
- **Nmap Version**: The scan was conducted using Nmap version 7.94SVN.
- **Scan Results**: The output details the findings for several hosts within the specified network range:
    - **192.168.34.1**: A device with several open ports, indicating active services:
        - Port 88/tcp: Open, running a Heimdal Kerberos service (a network authentication protocol).
        - Port 5000/tcp: Open, running AirTunes rtspd version 710.79.1 (likely part of an Apple AirPlay setup).
        - Port 5900/tcp: Open, running an Apple Remote Desktop VNC service.
        - Port 7000/tcp: Open, also running AirTunes rtspd version 710.79.1.
        - The MAC address and operating system (Mac OS X) are identified, which can help in understanding the device's role and potential vulnerabilities.
    - **192.168.34.2 and 192.168.34.254**: These hosts are up, but all scanned ports are in "ignored states." For 192.168.34.2, all ports are closed, and for 192.168.34.254, all ports are filtered with no response. Both devices have MAC addresses identified as VMware, suggesting they are virtual machines.
    - **192.168.34.141**: This host is up, but like 192.168.34.2, all scanned ports are in ignored states, with all 1000 scanned ports closed. No further information is provided about this host.
- **Service Detection**: The scan performed service detection, as indicated by the **sV** flag, to try and identify the versions of the services running on open ports.
- **Reporting**: The output encourages reporting any incorrect results to the Nmap project for improvement.
- **Scan Duration**: The scan covered 256 IP addresses and took 32.08 seconds to complete, which is relatively fast, thanks to the aggressive timing option (**T4**).

You'll need a reference point for future comparisons when you scan the network to identify new hosts and services. Assess the security vulnerabilities of all detected software, ensuring that you can accurately identify each device.

Rogue DHCP servers

A Dynamic Host Configuration Protocol (DHCP) server is a network server that automatically provides and assigns IP addresses, default gateways, and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol to respond to broadcast queries by clients.

A DHCP server dynamically assigns an IP address to every device that connects to the network. This process is quicker and less prone to errors than manual configuration. It also prevents IP conflicts by ensuring that each IP address is unique.

In addition to providing IP addresses, a DHCP server also gives the client other information it needs to communicate on the network, such as the subnet mask, default gateway, and the DNS server address.

In the context of a network, a DHCP server is important because it simplifies the management and configuration of network connectivity by administrators. Instead of manually assigning IP addresses for every new device, the DHCP server automates this process, saving time and reducing the likelihood of errors, such as duplicate IP addresses, that can cause network issues.

However, it's important to note that rogue DHCP servers, which are unauthorized DHCP servers that can be set up maliciously or inadvertently, can pose a significant threat to network security. These rogue servers can provide false information, redirect network traffic, or cause network connectivity problems. Tools such as Nmap can help identify these rogue servers, aiding network administrators in maintaining secure and efficient networks.

Rogue DHCP servers can cause significant damage to a network. They can be set up by malicious actors to distribute incorrect IP addresses or other network configurations to unsuspecting clients. This can result in a variety of problems, including incorrect routing of network traffic, inability to reach certain parts of the network, and exposure to sensitive information. It is crucial for network administrators to regularly utilize tools such as Nmap to scan their networks for the presence of rogue DHCP servers and take appropriate action to remove them.

Steps:

To perform DHCP discoveries, Nmap includes a script called **broadcast-dhcp-discover**. This script will send a DHCP request to the broadcast address using the MAC address of DE:AD:CO:DE:CA:FE and report the results.

Now, let us use the script **broadcast-dhcp-discover** on the interface **bond0** and discover if there is any rogue DHCP server.

The output:

#sudo nmap --script broadcast-dhcp-discover -e eth0

Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-22 01:43 EDT Pre-scan script results: | broadcast-dhcp-discover: | Response 1 of 1: | Interface: eth0 | IP Offered: 192.168.34.143 | DHCP Message Type: DHCPOFFER | Server Identifier: 192.168.34.254 | IP Address Lease Time: 30m00s | Subnet Mask: 255.255.255.0 | Router: 192.168.34.2 | Domain Name Server: 192.168.34.2 | Domain Name: localdomain | Broadcast Address: 192.168.34.255 | NetBIOS Name Server: 192.168.34.2 | Renewal Time Value: 15m00s |_ Rebinding Time Value: 26m15s WARNING: No targets were specified, so 0 hosts scanned. Nmap done: 0 IP addresses (0 hosts up) scanned in 10.15 seconds

This **Nmap** output is the result of running the **broadcast-dhcp-discover** script with **Nmap**, targeted through the **eth0**network interface. The script broadcasts a DHCP discovery request on the network and captures any DHCP offer responses from DHCP servers. Here's a breakdown of the key components of the output:

- **Interface: eth0** - This indicates that the discovery request was sent through the **eth0** network interface.
- **IP Offered: 192.168.34.143** - This is the IP address that the DHCP server is offering to the client sending the DHCP discovery request.
- **DHCP Message Type: DHCPOFFER** - This response is a DHCP offer, which means a DHCP server is offering network configuration parameters to the DHCP client.
- **Server Identifier: 192.168.34.254** - This is the IP address of the DHCP server that sent the offer. This information is crucial for identifying the server.
- **IP Address Lease Time: 30m00s** - This is the duration for which the offered IP address can be used before it needs to be renewed.
- **Subnet Mask: 255.255.255.0** - This defines the subnet of the IP address being offered, indicating which portion of the address is the network portion and which part is available for host addresses.
- **Router: 192.168.34.2** - This is the default gateway that devices should use to connect to other networks.
- **Domain Name Server: 192.168.34.2** - This is the DNS server that devices should use for resolving domain names to IP addresses.
- **Domain Name: localdomain** - This is the domain name provided by the DHCP server, which can be used for local network name resolutions.
- **Broadcast Address: 192.168.34.255** - This address is used for broadcasting messages to all devices on the network.
- **NetBIOS Name Server: 192.168.34.2** - This indicates the server that should be used for NetBIOS name resolution, often relevant in Windows networking environments.
- **Renewal Time Value: 15m00s** - This is the time interval before the lease's halfway point when the DHCP client starts trying to renew its lease.
- **Rebinding Time Value: 26m15s** - This is the time interval before the lease expires when the DHCP client will try to extend its lease with any DHCP server, not just the original server.

The warning about "No targets were specified, so 0 hosts scanned" is typical for this type of **Nmap** scan because the script is designed to broadcast and listen for responses rather than scanning specific targets.

This output primarily informs you about the presence and configuration offered by a DHCP server on your network via the **eth0** interface. If **192.168.34.254** is an expected and authorized DHCP server in your network, this output confirms it is operational and responding to discovery requests. If it's not recognized, further investigation would be warranted to understand why it's offering DHCP services, as it could be an unauthorized (rogue) DHCP server.

UPnP

Universal Plug and Play (UPnP) is a set of networking protocols that allows devices on a network to discover each other and automatically establish working configurations. This technology can simplify the process of connecting devices on a network by enabling them to configure network services for data sharing, communications, and entertainment.

UPnP is widely used in home and business networks for the seamless integration of computers, printers, Internet gateways, Wi-Fi access points, mobile devices, and more. It allows these devices to connect without the need for human intervention, making the process of setting up a network much less complicated.

However, while UPnP is designed for ease of use, it can also pose significant security risks. Because UPnP doesn't have built-in authentication, any device on the network can use UPnP services. This means that malicious software or rogue devices can leverage UPnP to open ports on your network's router, potentially exposing your network to external threats.

For instance, a malicious actor could exploit UPnP to reroute traffic, cause denial of service (DoS) attacks, or gain unauthorized access to networked devices. In some cases, malware can use UPnP to turn devices into part of a botnet, which can then be used to launch coordinated attacks.

Moreover, UPnP can be exploited by viruses and worms to spread across devices on a network quickly. Since UPnP assumes that local communications are trusted, malware can spread to other devices without being detected by firewalls or other security measures.

To mitigate these risks, it is important to monitor the use of UPnP on your network. Tools like Nmap can be used to identify devices using UPnP and to check for any unexpected or suspicious network configurations. Additionally, it may be advisable to disable UPnP on your network router, or at least limit its use to trusted devices.

In conclusion, while UPnP can provide convenience in setting up a network, it can also open up potential vulnerabilities if not properly managed. Regular monitoring and careful configuration of UPnP settings are key to maintaining a secure network environment.

Steps:

To scan the network and discover devices using UPnP, the following command should be run to execute the plugin **broadcast-upnp-info**. We can use **-T4** to speed up the discovery:

The output:

#sudo nmap --script=broadcast-upnp-info 192.168.34.0/24

Starting Nmap 7.94SVN (https://nmap.org) at 2024-03-22 13:20 EDT Nmap scan report for 192.168.34.1 Host is up (0.00025s latency). Not shown: 996 closed tcp ports (reset) PORT STATE SERVICE 88/tcp open kerberos-sec 5000/tcp open upnp 5900/tcp open vnc 7000/tcp open afs3-fileserver MAC Address: 3E:22:FB:FE:7B:65 (Unknown)

Nmap scan report for 192.168.34.2 Host is up (0.00018s latency). All 1000 scanned ports on 192.168.34.2 are in ignored states. Not shown: 1000 closed tcp ports (reset) MAC Address: 00:50:56:F8:09:C8 (VMware)

Nmap scan report for 192.168.34.254 Host is up (0.00050s latency). All 1000 scanned ports on 192.168.34.254 are in ignored states. Not shown: 1000 filtered tcp ports (no-response) MAC Address: 00:50:56:FA:31:78 (VMware)

Nmap scan report for 192.168.34.141 Host is up (0.0000030s latency). All 1000 scanned ports on 192.168.34.141 are in ignored states. Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 11.03 seconds

A comprehensive network scan was conducted on the subnet **192.168.34.0/24** to identify active devices and assess the presence of UPnP services across the network. The scan was performed using Nmap, a network discovery and security auditing tool, leveraging the **broadcast-upnp-info** script designed to discover UPnP services by broadcasting discovery requests.

Scan Execution Details

- **Command Used: sudo nmap --script=broadcast-upnp-info 192.168.34.0/24**
- **Nmap Version:** 7.94SVN
- **Date and Time of Scan:** March 22, 2024, at 13:20 EDT
- **Subnet Scanned: 192.168.34.0/24**

Key Findings

The scan identified 4 hosts as being active within the subnet. For each host, the scan attempted to enumerate open ports and identify services:

1. Host IP: 192.168.34.1
- **Latency:** 0.00025 seconds
    - **Open Ports:**
    - **88/tcp** (Kerberos Security)
    - **5000/tcp** (UPnP)
    - **5900/tcp** (VNC)
    - **7000/tcp** (AFS3 Fileserver)
- **MAC Address:** 3E:22:FB:FE:7B:65 (Manufacturer Unknown)
2. Host IP: 192.168.34.2
- **Latency:** 0.00018 seconds

- **Status:** All 1000 scanned ports are in ignored states (closed).
- **MAC Address:** 00:50:56:F8:09:C8 (VMware)

3. Host IP: 192.168.34.254

- **Latency:** 0.00050 seconds
- **Status:** All 1000 scanned ports showed no response (filtered).
- **MAC Address:** 00:50:56:FA:31:78 (VMware)

4. Host IP: 192.168.34.141

- **Latency:** 0.0000030 seconds
- **Status:** All 1000 scanned ports are in ignored states (closed).

Analysis

The scan successfully identified several services across the devices on the network, including potential UPnP services on host **192.168.34.1** (port 5000/tcp). However, the expected detailed UPnP discovery information from the **broadcast-upnp-info** script is not present in the output. This could indicate the script did not find additional UPnP services beyond those identifiable through open port detection, or that the UPnP services did not respond to the discovery requests as anticipated.

The presence of VMware MAC addresses suggests the use of virtualization on the network, which could be relevant for understanding the network's infrastructure and the deployment of services.

Conclusion

The Nmap scan provided valuable insights into the active hosts within the **192.168.34.0/24** subnet and identified open ports that could be indicative of UPnP services. Further investigation and targeted UPnP discovery efforts may be necessary to comprehensively assess the deployment and configuration of UPnP services across the network. This information is crucial for understanding network service configurations, identifying potential security exposures, and planning for network security enhancements.

Conclusion

This document explores how Nmap can be effectively used to identify potential unauthorized devices on our networks. Given the increasing complexity of network environments and the diverse range of devices that can connect to them, it's more important than ever to maintain a comprehensive awareness of all network-connected devices. Nmap is a practical and efficient tool that is highly valuable for these situations and more.

We delved into the multitude of features that make Nmap an essential tool for detecting unauthorized devices on networks. As networks become increasingly complex, with a wide array of devices connecting to them, it becomes crucial to preserve full visibility of all

network-connected devices. Nmap serves as a functional and efficient tool, providing significant value in these endeavors.