Prepared By: Gopi Gor

Date: 03/17/2024

Vulnerability Discovery Investigation

This report analyses the vulnerability discovery and plays a role in incident reporting. This report has been created using Sumologic for lab purposes. Previously parsed logs have been used to run the scripts. Multiple tools have been used for threat simulations including nmap and the business implications and holistic remediations have been analyzed and documented in the report.

Threat Simulation

The Nmap tool is a very useful tool that is used by multiple network engineers to understand open ports, services running and scripts. There are multiple other things that Nmap can be used for, which not only by network engineers but even by hackers in a network to learn about all details of a specific target on a network. It makes a map of the network and allows for different scanning like network discovery, port scanning, service versions, operating systems and automation.

For the open ports command that we ran to discover open ports on the loopback address **nmap 127.0.0.1** can be run on any other host in another setting. This command can be used to investigate incidents that may allow entry into the network by an attacker. An open port is usually what an attacker looks for initial access into a network. Discovering the open ports on each network address and analysing this is a good starting point to avoid any unwanted access into the whole domain. Another common type of incident that can be caused by open ports is a DoS attack. Open ports allow the targets to be exploited and then change admin permissions to completely cutting off resources for the user. Additionally, the services command which was used **nmap <target_ip> -sV** allows to understand the services and versions running on the port which then can be researched further to exploit vulnerabilities in the services source code which may be there on many outdated versions. The NSE scripts concern with very complex scans relating to vulnerabilities, or brute force and many others as shown in the appendix. This allows further exploration into a target if a port is found open.

For an SOC analyst who would be trying to investigate any incidents, there are multiple commands that can be used to detect things. First, the **nmap -p- <target>** will allow to check all open ports on the selected target host. The **nmap -sV <target>** allows to identify all services running on the open ports discovered. The scripting engine command **nmap –script <script> <target>** gives the output of the selected script which allows us to evaluate the vulnerabilities, banner information and so many more scripts that can be run to collect information of the specific target but on a deeper level. Additionally, the command **nmap -O <target>** to learn about the operating system and version running on the target.

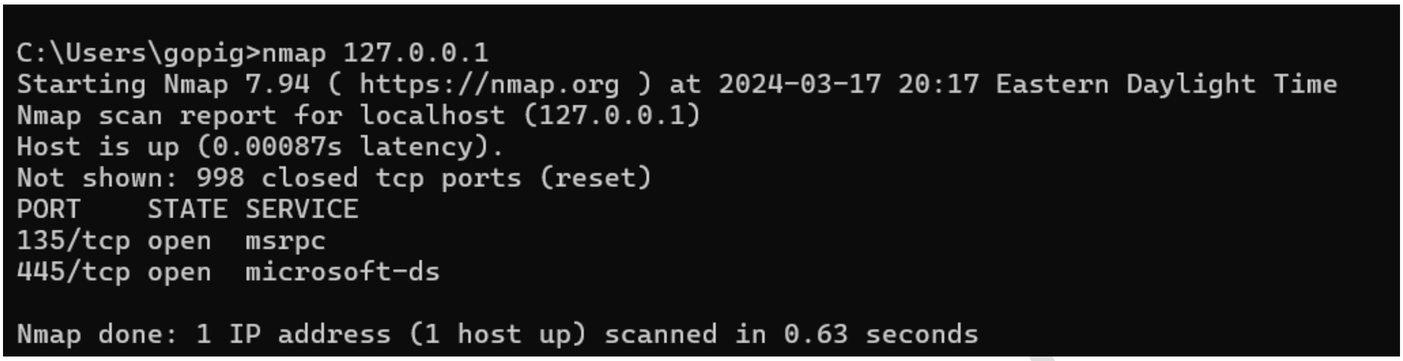
Business Implications

Like we discussed before, Nmap can be useful for scanning a host and the network to get a lot of information. While network engineers can use this to the advantage, on the other hand, attackers can use this information to penetrate a network and cause major damage to the network, or organization. Some of the short-term risks associated with Nmap discovery scans are disruptions in case an attacker tries to send a lot of requests into the network and may even cause service unavailability. This allows them to get complete reconnaissance of the network and identify the potential targets to enter into the network. The scans if very aggressive can even cause alert triggering in the firewalls or IDS, which could eventually bypass these alerts if ignored. These lead to long term risks which means exposure of services, versions and vulnerabilities on the current target. The attackers can exploit these vulnerabilities to steal sensitive information or cause financial harm to the organization.

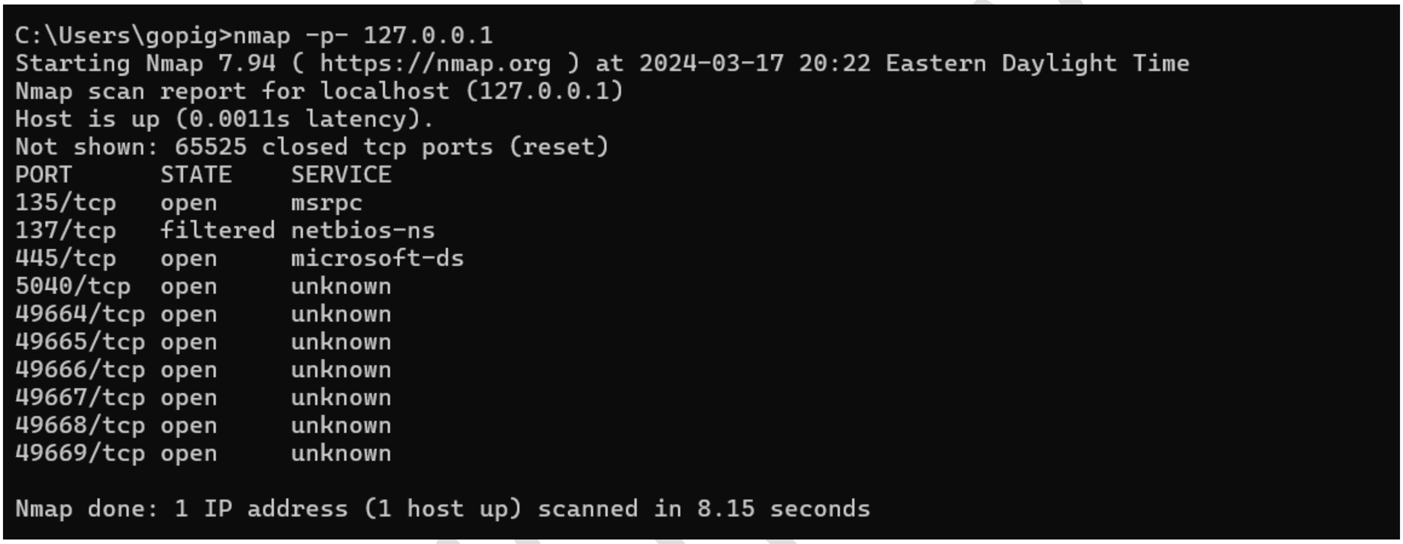
Holistic Remediations

For remediations against Nmap scans, the first thing that can be done is network segmentation. This allows to limit how the unauthorized scans affect the target. There would not be much information to view or exploit. Additionally, the firewall and IDS should be set up in a way to alert for unauthorized network scans that are being performed to identify potential attackers trying to exploit the systems. Operating systems being used should be constantly upgrades and updated with the latest patches. Incident response planning should be in place in case an alert is detected, or an incident occurs. Furthermore, it is crucial that users, employees and even guests are advised about the ill-effects of attackers and how it can harm the organization. This also means educating them and making sure they don't keep any sensitive information or confidential information on their company network until required. The least privilege policy should be implemented at all times, and access control mechanisms should be in place. If all these measures are implemented from time to time, it would be possible to detect and avoid network scanning by potential adversaries.

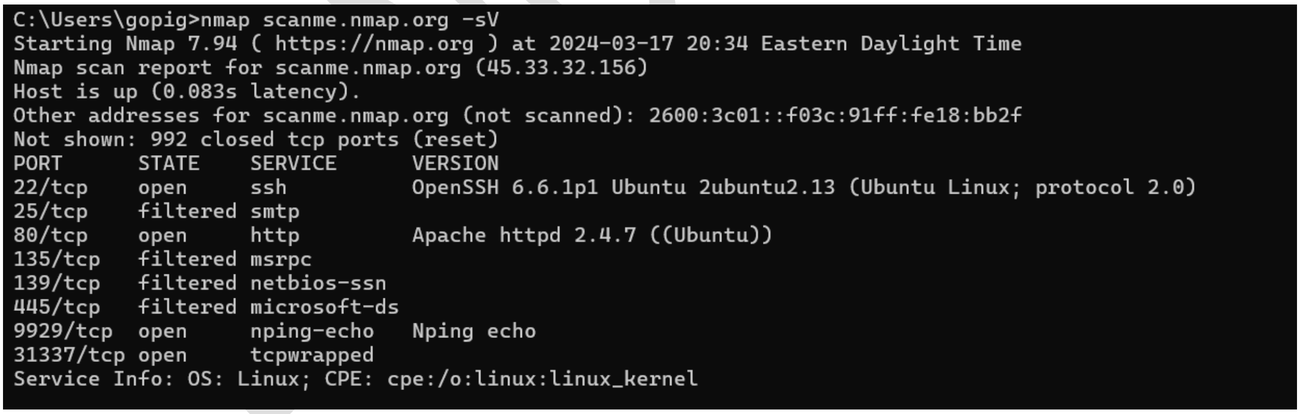
Appendix



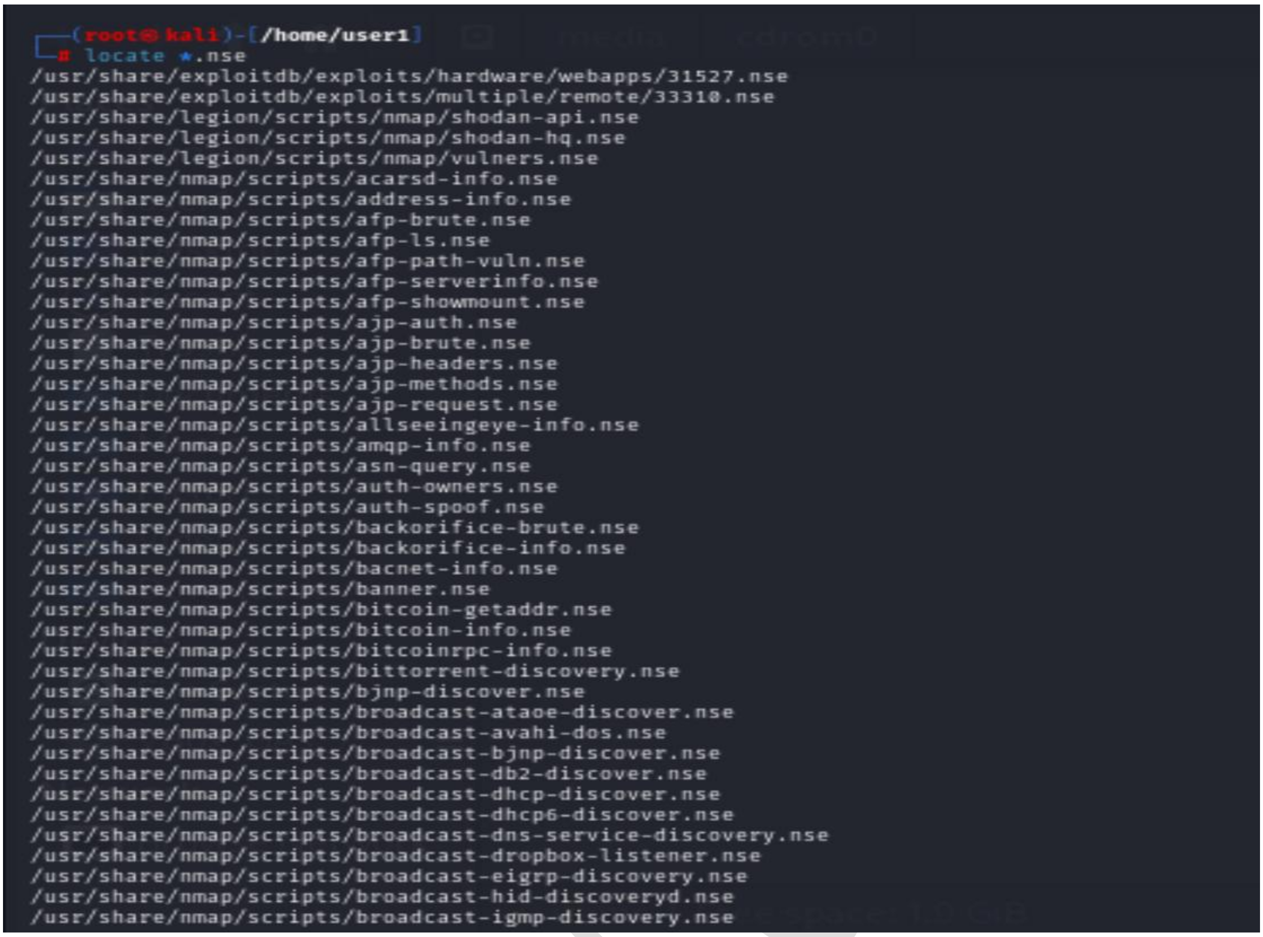
```
C:\Users\gopig>nmap 127.0.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-17 20:17 Eastern Daylight Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00087s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
```



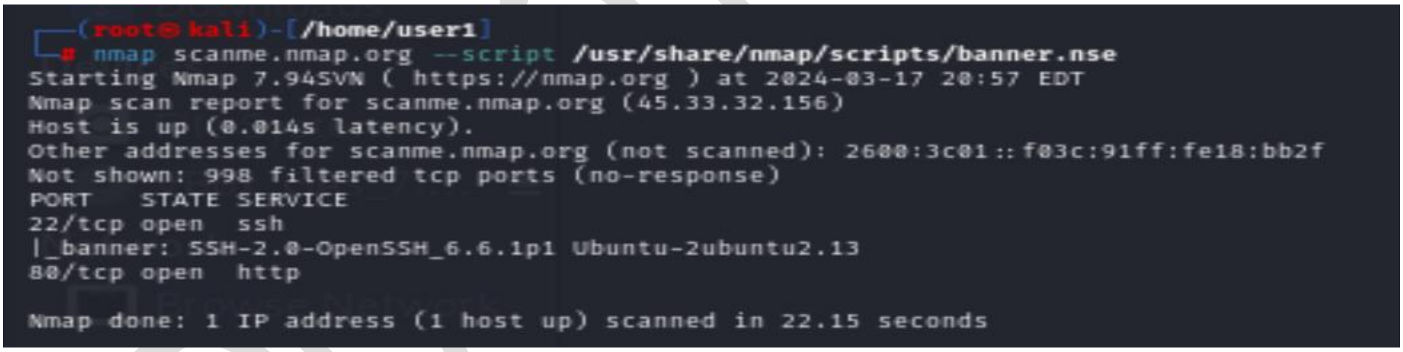
```
C:\Users\gopig>nmap -p- 127.0.0.1
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-17 20:22 Eastern Daylight Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0011s latency).
Not shown: 65525 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
445/tcp   open     microsoft-ds
5040/tcp  open     unknown
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49669/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 8.15 seconds
```



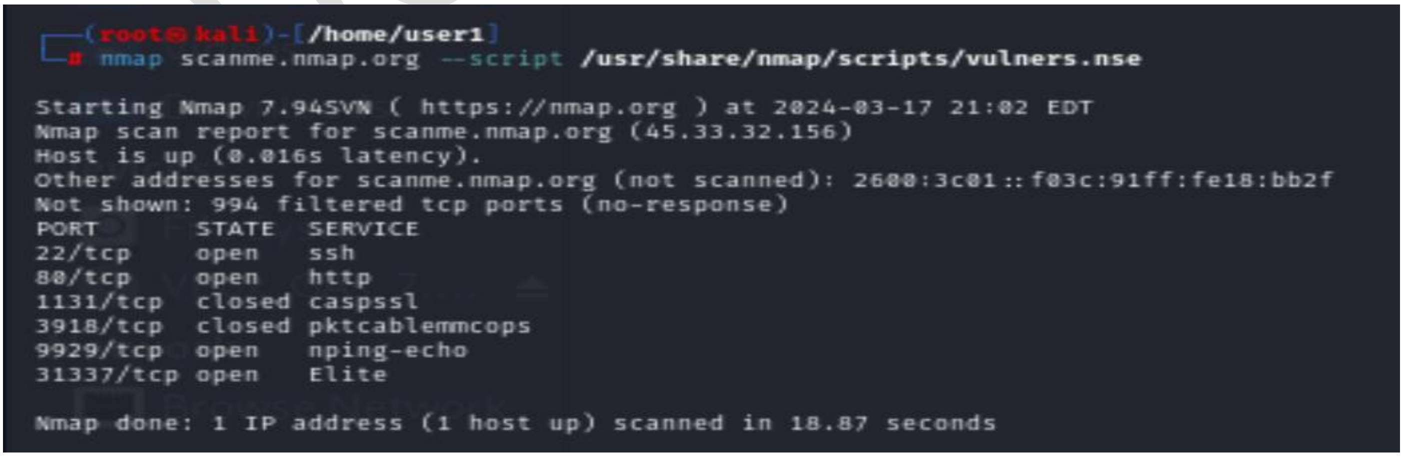
```
C:\Users\gopig>nmap scanme.nmap.org -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-17 20:34 Eastern Daylight Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.083s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
┌──(root㉿kali)-[/home/user1]
└─# locate *.nse
/usr/share/exploitdb/exploits/hardware/webapps/31527.nse
/usr/share/exploitdb/exploits/multiple/remote/33310.nse
/usr/share/legion/scripts/nmap/shodan-api.nse
/usr/share/legion/scripts/nmap/shodan-hq.nse
/usr/share/legion/scripts/nmap/vulners.nse
/usr/share/nmap/scripts/acarsd-info.nse
/usr/share/nmap/scripts/address-info.nse
/usr/share/nmap/scripts/afp-brute.nse
/usr/share/nmap/scripts/afp-ls.nse
/usr/share/nmap/scripts/afp-path-vuln.nse
/usr/share/nmap/scripts/afp-serverinfo.nse
/usr/share/nmap/scripts/afp-showmount.nse
/usr/share/nmap/scripts/ajp-auth.nse
/usr/share/nmap/scripts/ajp-brute.nse
/usr/share/nmap/scripts/ajp-headers.nse
/usr/share/nmap/scripts/ajp-methods.nse
/usr/share/nmap/scripts/ajp-request.nse
/usr/share/nmap/scripts/allseeingeye-info.nse
/usr/share/nmap/scripts/amqp-info.nse
/usr/share/nmap/scripts/asn-query.nse
/usr/share/nmap/scripts/auth-owners.nse
/usr/share/nmap/scripts/auth-spoof.nse
/usr/share/nmap/scripts/backorifice-brute.nse
/usr/share/nmap/scripts/backorifice-info.nse
/usr/share/nmap/scripts/bacnet-info.nse
/usr/share/nmap/scripts/banner.nse
/usr/share/nmap/scripts/bitcoin-getaddr.nse
/usr/share/nmap/scripts/bitcoin-info.nse
/usr/share/nmap/scripts/bitcoinrpc-info.nse
/usr/share/nmap/scripts/bittorrent-discovery.nse
/usr/share/nmap/scripts/bjnp-discover.nse
/usr/share/nmap/scripts/broadcast-ataoe-discover.nse
/usr/share/nmap/scripts/broadcast-avahi-dos.nse
/usr/share/nmap/scripts/broadcast-bjnp-discover.nse
/usr/share/nmap/scripts/broadcast-db2-discover.nse
/usr/share/nmap/scripts/broadcast-dhcp-discover.nse
/usr/share/nmap/scripts/broadcast-dhcp6-discover.nse
/usr/share/nmap/scripts/broadcast-dns-service-discovery.nse
/usr/share/nmap/scripts/broadcast-dropbox-listener.nse
/usr/share/nmap/scripts/broadcast-eigrp-discovery.nse
/usr/share/nmap/scripts/broadcast-hid-discoveryd.nse
/usr/share/nmap/scripts/broadcast-igmp-discovery.nse
```



```
┌──(root㉿kali)-[/home/user1]
└─# nmap scanme.nmap.org --script /usr/share/nmap/scripts/banner.nse
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-17 20:57 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.014s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
|_banner: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.13
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 22.15 seconds
```



```
┌──(root㉿kali)-[/home/user1]
└─# nmap scanme.nmap.org --script /usr/share/nmap/scripts/vulners.nse

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-17 21:02 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.016s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
1131/tcp  closed caspssl
3918/tcp  closed pktcablemmcops
9929/tcp  open   nping-echo
31337/tcp open   Elite

Nmap done: 1 IP address (1 host up) scanned in 18.87 seconds
```

References

1. https://www.holmsecurity.com/blog/what-is nmap#:~:text=Common%20Use%20Cases%20For%20Nmap,open%2C%20closed%2C%20or%20filtered.
2. https://nmap.org/book/legal-issues.html