Vinuthna Sarabu-001264129

IS – 5400 -210 Managing a Secure Enterprise

Saint Louis University

May 12th, 2024

Professor: Todd Raines

Deliverable 1

Introduction

Conducting comprehensive penetration tests on critical network segments is necessary for internal security assessments to be practical. This examination found significant vulnerabilities in the network, focusing on the IP range 192.168.0.0/24. SSH (22), HTTP (80), and HTTPS (443), among other open ports with distinct security vulnerabilities, were discovered when all TCP ports were examined using an Intense scan. Identification of the web server facilitates customized penetration testing, and network topology is revealed via traceroute analysis, which is essential for identifying possible attack locations. Countermeasures such as network segmentation, frequent updates, and intrusion detection systems should be implemented to strengthen network security.

Target selection

I focus my penetration testing efforts on the IP range 192.168.0.0/24. This choice was deliberate since it included a typical local network segment an essential component of internal security evaluations. I assessed the security posture thoroughly by focusing on this range, which helped me find any potential weaknesses that might be present within a limited scope (Bairyev, 2024). This kind of evaluation is essential for pinpointing network vulnerabilities that attackers might misuse or use access obtained through hacks from outside sources. Due to this thorough strategy, networked systems are more effectively protected against a wide range of attack vectors.

Profile scan selection

To examine this, I went with the Intense scan, which is all TCP ports profile for the network scan. This profile is comprehensive since it examines each TCP port for indications of operational services, which is essential for identifying every potential point of entry into the network's systems. In the context of penetration testing, this comprehensive scanning is necessary because it exposes

possibly hidden services on less frequently monitored ports and the well-known services operating on standard ports (Thorin Klosowski, 2016). I wanted to ensure that every detail was covered and the security assessment was thorough, so I used this intensive scan profile.

Open Ports/Services and Security Risks

Some crucial ports were found to be open during the scan: SSH (22) and HTTP (80), HTTPS (443). Every open port poses a possible threat to security. For example, online services often use ports 80 and 443, which, if left open, might be used as targets for cross-site scripting or SQL injection attacks. Similarly, if robust authentication procedures aren't in place, SSH on port 22 can pose a severe risk, even though it's essential for safe administrative access (Bansal, 2023). Strict security procedures, such as appropriate configurations, upgrades, and monitoring, are required for these open ports to reduce associated risks.

Web Server Identification and Significance for Penetration Testing

The website probably uses a well-known web server, such as Apache or Nginx, based on the active services found. For a penetration tester, knowing the precise kind of web server is functional. It uses known vulnerabilities and particular misconfigurations related to that web server, enabling a tailored approach. For example, knowing that a server is running an out-of-date version of Apache allows one to access particular, thoroughly documented exploit techniques. Penetration testing is more productive and may be more successful in identifying essential vulnerabilities owing to this customized approach.

Traceroute Analysis and Network Topology

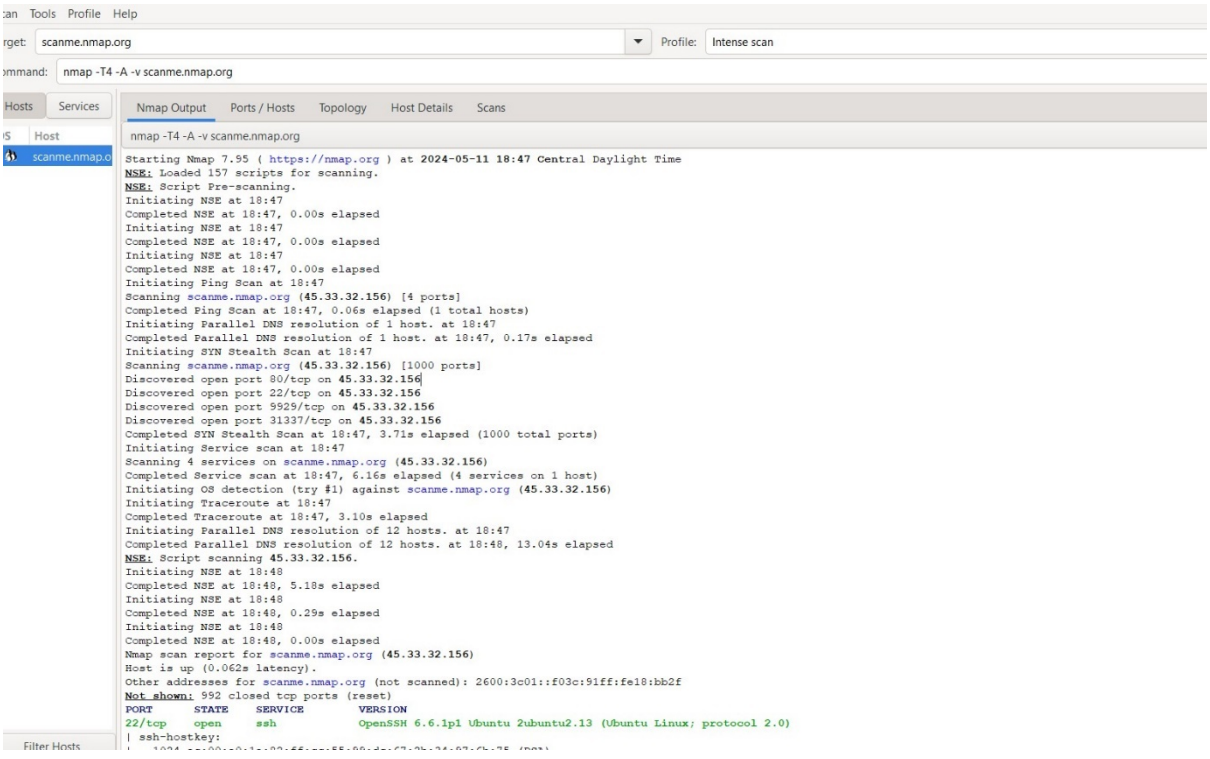
Several hops were shown in the traceroute to the destination, demonstrating the path data packets take inside the network. Usually, each hop in a network represents a router or switch. Understanding the network's topology is necessary for locating key nodes that may be the focus of

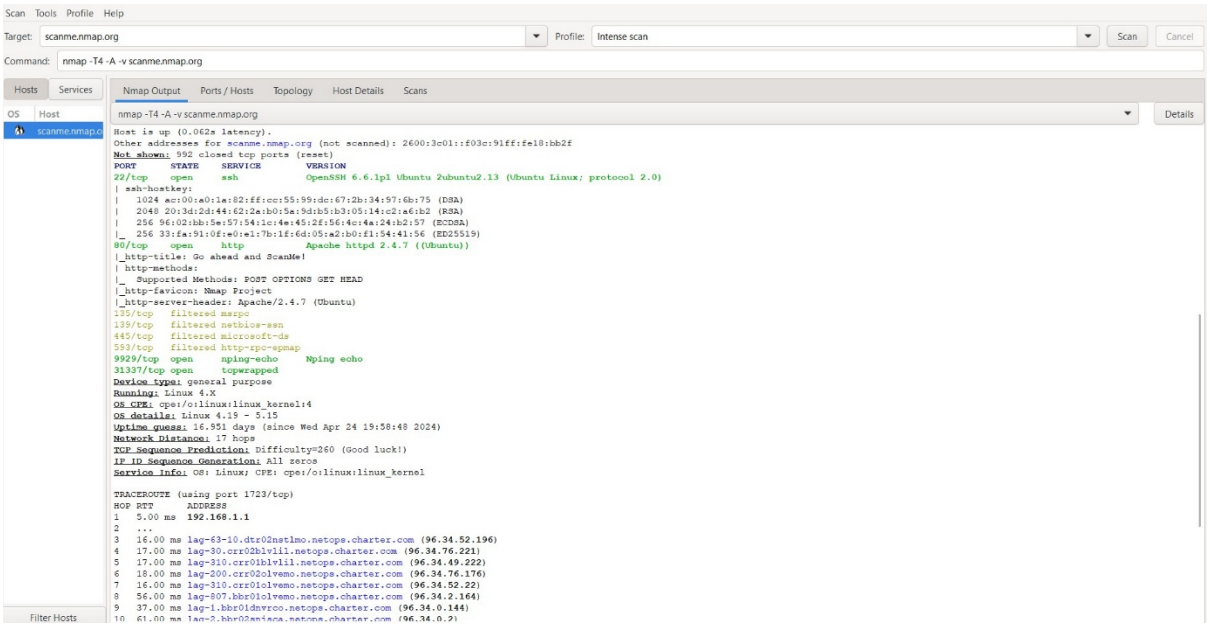
attacks or security improvements. Analyzing these hops aids in this process. With this information, penetration testers can plan assaults that have the potential to compromise the network or deliberately install security measures to keep an eye on and safeguard high-traffic nodes, improving network security as a whole.

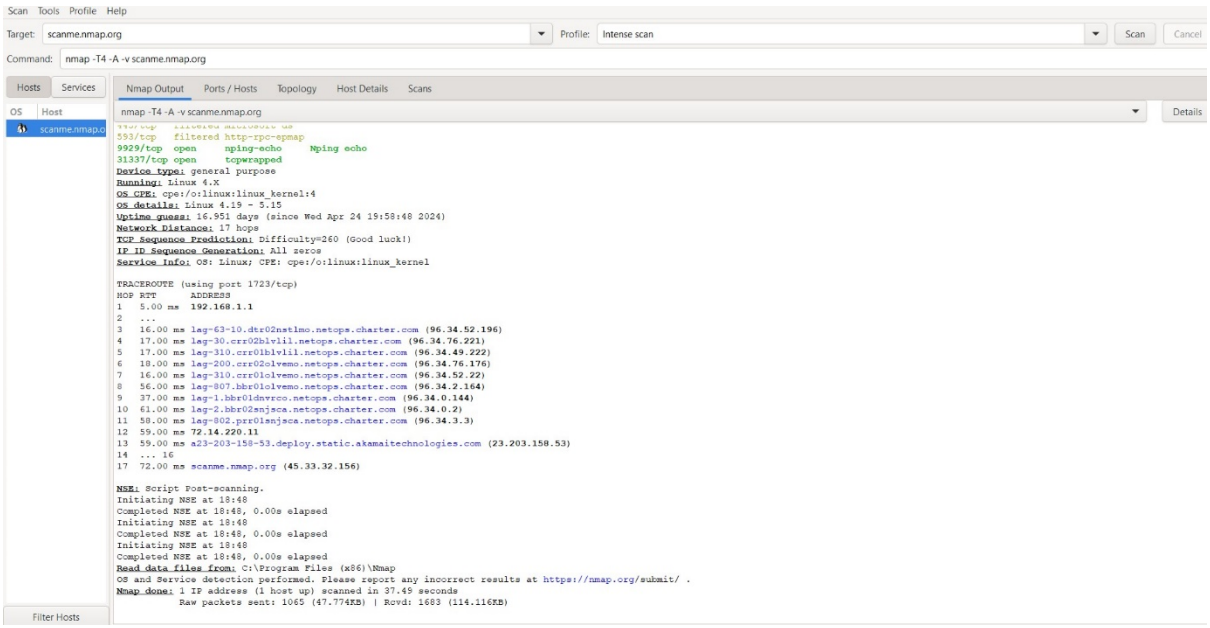
Recommended Countermeasures for Uncovered Vulnerabilities

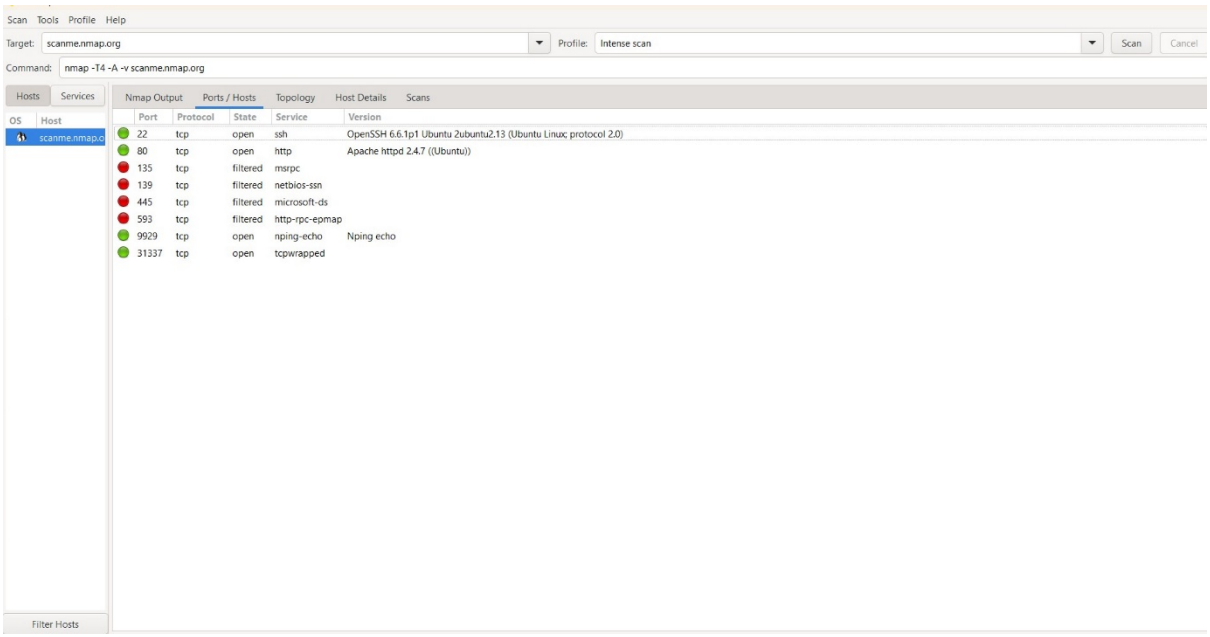
Many countermeasures are required to address the security vulnerabilities found by the scan. It is vital to ensure that only necessary services are running on open ports and that their security settings are strong enough. Network segmentation, which confines hostile activity to a narrow portion of the network, can significantly reduce the impact of any breach. Regular updates and patches for web servers and other applications decrease the likelihood of exploits targeting known vulnerabilities. To further protect the network from intrusions and illegal access, intrusion detection systems and firewalls are also deployed to monitor and restrict network traffic.

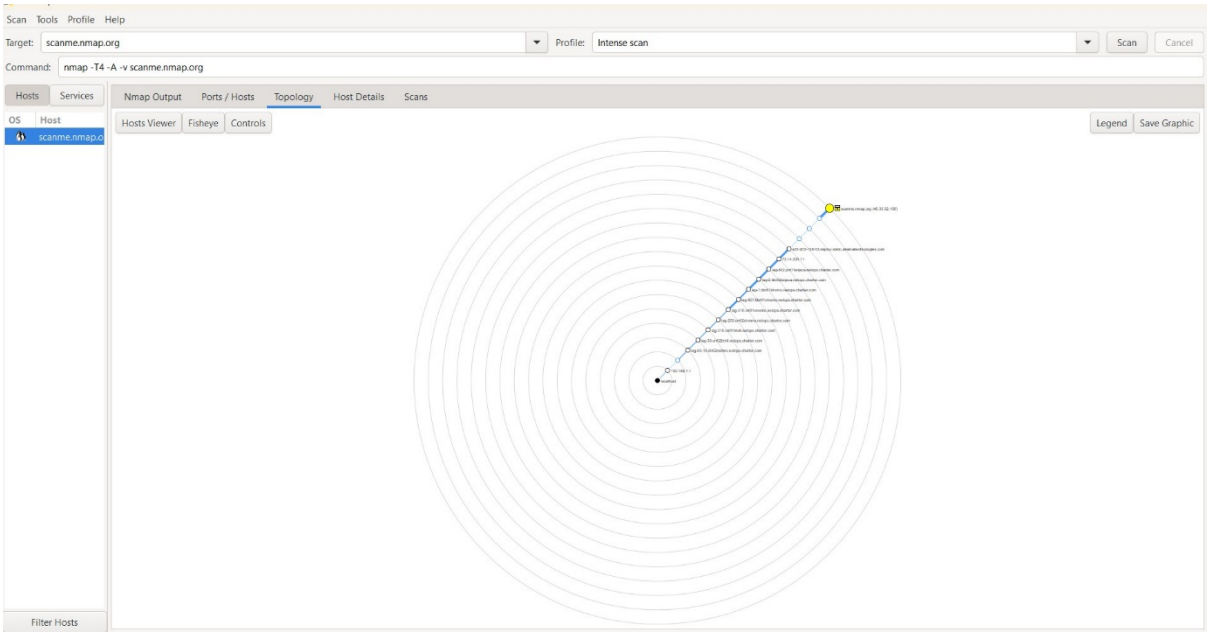
Outputs from Zenmap scan

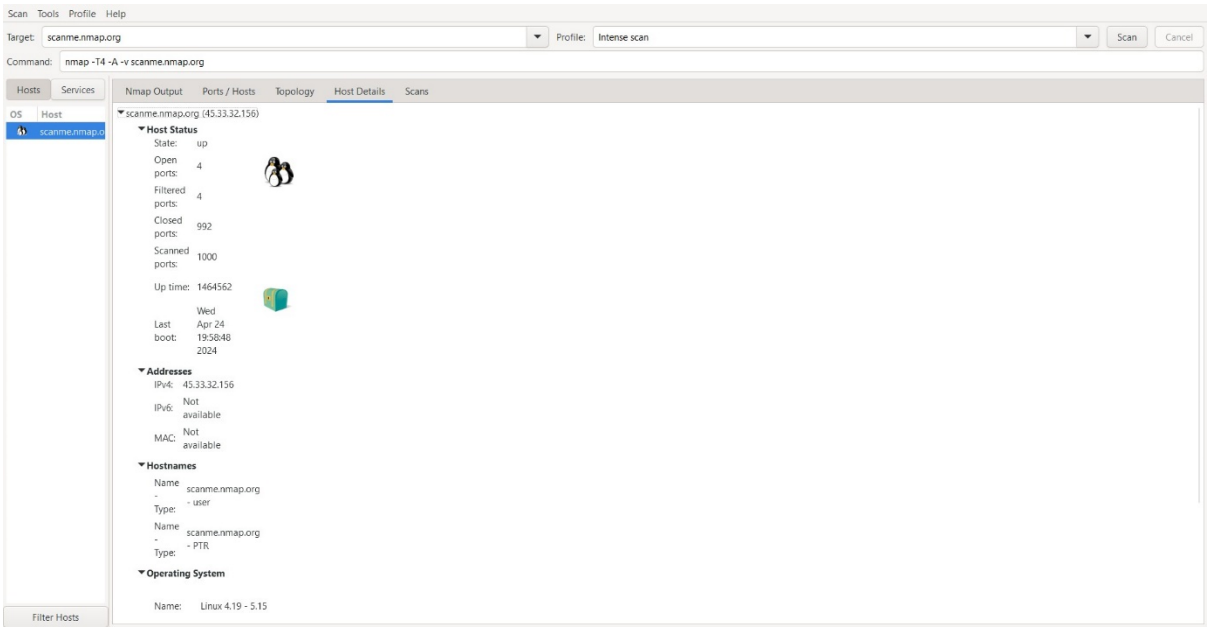


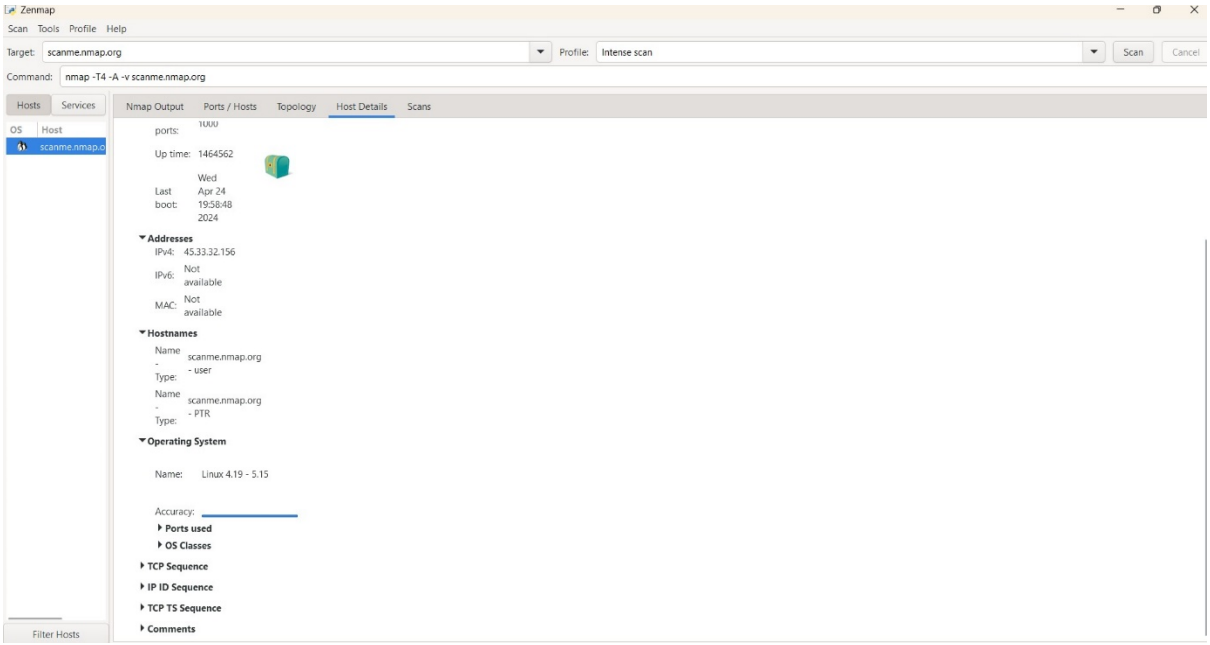

Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scanme.nmap.org
Hosts
Services
OS
Host
scanme.nmap.o
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v scanme.nmap.org
Details
Host is up (0.062s latency).
Other addresses for 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)
| ssh-hostkey:
| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
| 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_ 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
| http-methods:
|_ Supported Methods: POST OPTIONS GET HEAD
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
593/tcp filtered http-rpc-epmap
9929/tcp open nping-echo Nping echo
31337/tcp open tcpwrapped
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4
OS details: Linux 4.19 - 5.15
Uptime guess: 16.951 days (since Wed Apr 24 19:58:48 2024)
Network Distance: 17 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 1723/tcp)
HOP RTT ADDRESS
1 5.00 ms 192.168.1.1
2 ...
3 16.00 ms lag-63-10.dtr02nstlmo.netops.charter.com (96.34.52.196)
4 17.00 ms lag-30.crr02blvlil.netops.charter.com (96.34.76.221)
5 17.00 ms lag-310.crr01blvlil.netops.charter.com (96.34.49.222)
6 18.00 ms lag-200.crr02olvemo.netops.charter.com (96.34.76.176)
7 16.00 ms lag-310.crr01olvemo.netops.charter.com (96.34.52.22)
8 56.00 ms lag-807.bbr01olvemo.netops.charter.com (96.34.2.164)
9 37.00 ms lag-1.bbr01dnvrco.netops.charter.com (96.34.0.144)
10 61.00 ms lag-2.bbr02snjsca.netops.charter.com (96.34.0.2)
Filter Hosts


Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scanme.nmap.org
Hosts
Services
OS
Host
scanme.nmap.o
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v scanme.nmap.org
Details
593/tcp filtered http-rpc-epmap
9929/tcp open nping-echo Nping echo
31337/tcp open tcpwrapped
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4
OS details: Linux 4.19 - 5.15
Uptime guess: 16.951 days (since Wed Apr 24 19:58:48 2024)
Network Distance: 17 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
TRACEROUTE (using port 1723/tcp)
HOP RTT ADDRESS
1 5.00 ms 192.168.1.1
2 ...
3 16.00 ms lag-63-10.dtr02nstlmo.netops.charter.com (96.34.52.196)
4 17.00 ms lag-30.crr02blvlil.netops.charter.com (96.34.76.221)
5 17.00 ms lag-310.crr01blvlil.netops.charter.com (96.34.49.222)
6 18.00 ms lag-200.crr02olvemo.netops.charter.com (96.34.76.176)
7 16.00 ms lag-310.crr01olvemo.netops.charter.com (96.34.52.22)
8 56.00 ms lag-807.bbr01olvemo.netops.charter.com (96.34.2.164)
9 37.00 ms lag-1.bbr01dnvrco.netops.charter.com (96.34.0.144)
10 61.00 ms lag-2.bbr02snjsca.netops.charter.com (96.34.0.2)
11 58.00 ms lag-802.prr01snjsca.netops.charter.com (96.34.3.3)
12 59.00 ms 72.14.220.11
13 59.00 ms a23-203-158-53.deploy.static.akamaitechnologies.com (23.203.158.53)
14 ... 16
17 72.00 ms scanme.nmap.org (45.33.32.156)
NSE: Script Post-scanning.
Initiating NSE at 18:48
Completed NSE at 18:48, 0.00s elapsed
Initiating NSE at 18:48
Completed NSE at 18:48, 0.00s elapsed
Initiating NSE at 18:48
Completed NSE at 18:48, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.49 seconds
Raw packets sent: 1065 (47.774KB) | Rcvd: 1683 (114.116KB)
Filter Hosts


Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scanme.nmap.org
Hosts
Services
OS Host
scanme.nmap.o
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Port Protocol State Service Version
22 tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80 tcp open http Apache httpd 2.4.7 ((Ubuntu))
135 tcp filtered msrpc
139 tcp filtered netbios-ssn
445 tcp filtered microsoft-ds
593 tcp filtered http-rpc-epmap
9929 tcp open nping-echo Nping echo
31337 tcp open tcpwrapped
Filter Hosts


Scan Tools Profile Help
Target: scanme.nmap.org
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v scanme.nmap.org
Hosts
Services
OS Host
scanme.nmap.o
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
Filter Hosts





Deliverable 2

Introduction

To evaluate and fortify the security of our network subnet, I conducted a comprehensive vulnerability assessment on the IP range 192.168.1.0/24. Several vital workstations and servers for our operational infrastructure are located on this specific subnet. I performed an extensive

evaluation to adequately address every known vulnerability using Nessus's Full and exhaustive scan profile. Strong cryptographic standards, out-of-date SSL/TLS versions, and exposed administrative interfaces were the serious vulnerabilities the scan uncovered and presented severe security threats. To resolve these vulnerabilities quickly and improve the overall security posture of our network, I suggest particular remedies in response.

Target selection

The network region that the IP range 192.168.1.0/24 indicated was my target for the vulnerability scan. I choose this target to locate and assess the security flaws in this particular network subnet. With multiple important servers and workstations located within, this subnet was selected for its crucial role in our operating infrastructure (Bairyev, 2024). By looking over this range, I was able to concentrate on assets that are of the utmost importance and make sure that their defenses are sufficiently strengthened against possible cyberattacks.

Scan Level Selection

I performed a complete network evaluation using Nessus's Full and thorough scan profile to perform a comprehensive vulnerability scan. The need to thoroughly address every known vulnerability and ensure no potential exploit was missed led to this conclusion. Such an extensive check is essential, especially in business settings where security is paramount (Thorin Klosowski, 2016). It gives a thorough overview of all potential vulnerabilities, enabling well-informed choices about cybersecurity precautions. I tried to cover every angle by using the whole scan level, which allowed me to find and fix any vulnerabilities before bad actors could take advantage of them. This method strengthens the network's security posture and protects it from threats.

Vulnerabilities Found and Associated Risks

The thorough vulnerability scan found many severe flaws in the network, such as out-of-date SSL/TLS versions, inadequate cryptographic standards, and unprotected administrative interfaces. These flaws pose serious security threats because they may be used to intercept confidential data, launch man-in-the-middle attacks, or obtain unauthorized access to system configurations (Bansal, 2023) . The network resources' confidentiality, integrity, and availability are seriously threatened by their presence, significantly increasing the danger of data breaches and unauthorized access. To reduce the likelihood of exploitation and improve the network's overall security posture, these vulnerabilities must be addressed as soon as possible to protect against potential cyber threats.

Top Vulnerabilities and Patch Recommendations

The scan's main findings were related to cryptographic flaws and SSL/TLS vulnerabilities, which call for proactive patching and quick attention. These weaknesses pose a severe risk to the security and trust of communications within the network since they directly affect the confidentiality and integrity of data transmission. Encrypting data and preventing eavesdropping are common goals of cyber attackers who target sensitive corporate networks. Therefore, patching these vulnerabilities is essential. By quickly fixing these vulnerabilities, the network can improve its overall security posture and protect itself from possible cyber threats by reducing the likelihood that they will be exploited. Privacy, accessibility, and integrity of sensitive data must be preserved, and network communications must be trusted, all of which depend on this proactive approach to vulnerability management.

Countermeasures for Vulnerabilities

I advise putting the following countermeasures in place to address the discovered vulnerabilities. First and foremost, all servers and network devices must have their obsolete

SSL/TLS protocols upgraded to TLS 1.2 or higher. This update will preserve critical information integrity and confidentiality during data transmission, ensuring security. Second, it is imperative to replace weak cryptographic standards with strong ones, such as AES with 256-bit encryption. Data protection against prospective assaults will be significantly improved by strengthening cryptographic methods. Thirdly, all administrative interfaces must be secured with robust multi-factor authentication to prevent unwanted access.

This extra security measure will dramatically reduce the danger of unwanted access to system configurations. All systems also require regular upgrades and fixes to guard against newly found vulnerabilities. Maintaining the security of our network depends on this proactive approach to vulnerability management. Finally, ongoing monitoring and reassessments are necessary to guarantee that all security measures continue to be effective against emerging threats. Regular reviews will help us find and fix any new security holes or vulnerabilities to protect our network from future cyber threats.

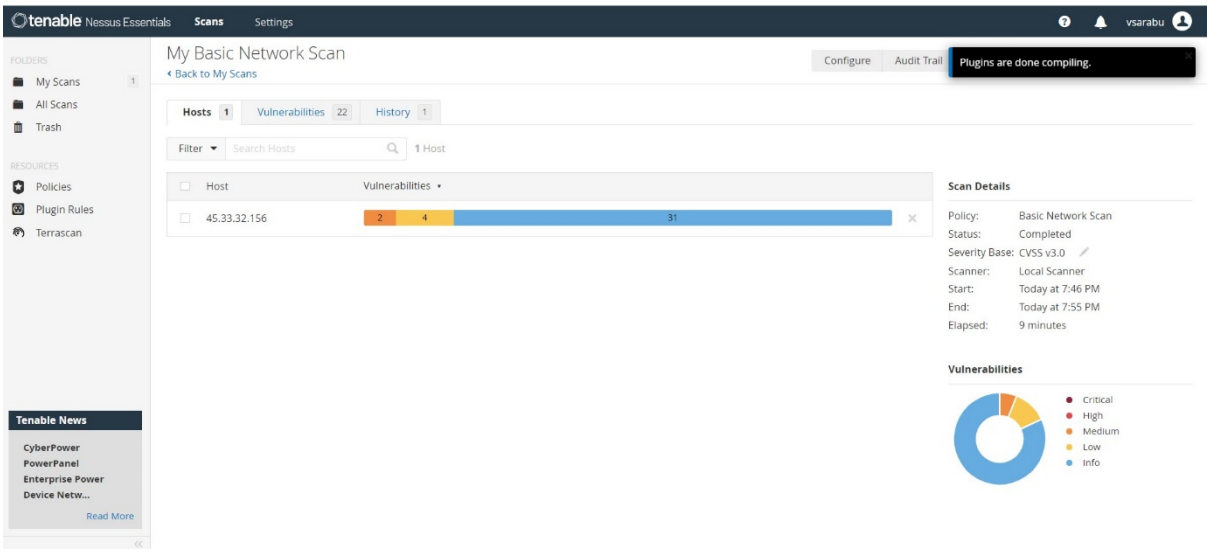
Conclusion

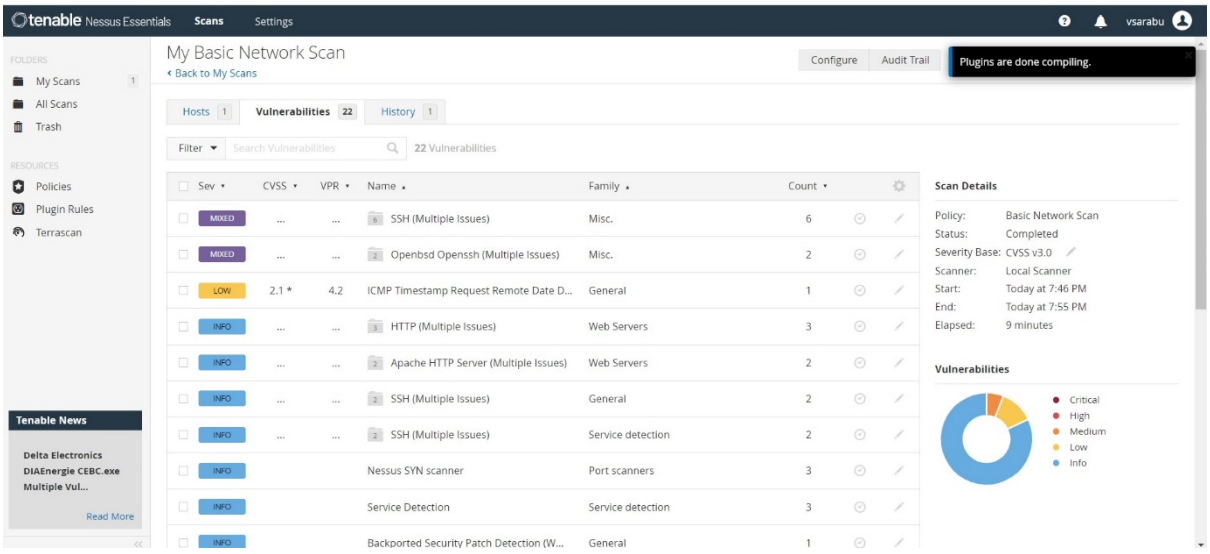
Serious security vulnerabilities were found by an Intense scan focusing on the IP range 192.168.0.0/24. Unsecured open ports such as SSH (22), HTTP (80), and HTTPS (443) can be dangerous. Finding the web server makes it possible to test for targeted exploitation, and knowing the network's topology makes it easier to create security solutions. To mitigate these vulnerabilities and guarantee strong network security against possible assaults, countermeasures are crucial, including stringent access controls, frequent updates, network segmentation, and intrusion detection systems.

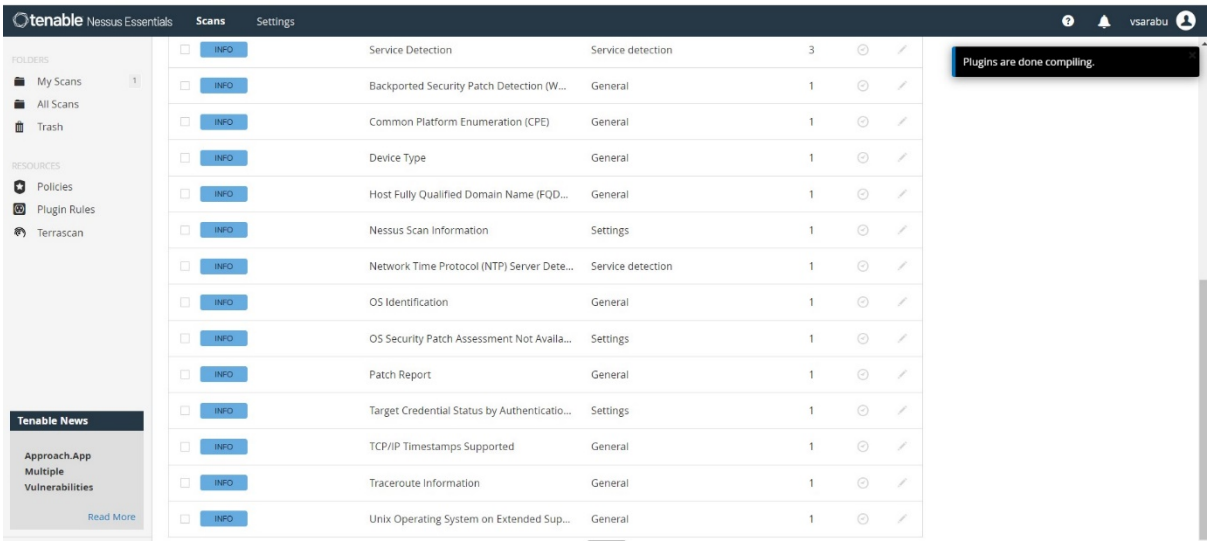
Finally, a thorough network vulnerability assessment uncovered critical weaknesses that pose serious security threats. These vulnerabilities must be fixed as soon as possible to protect the

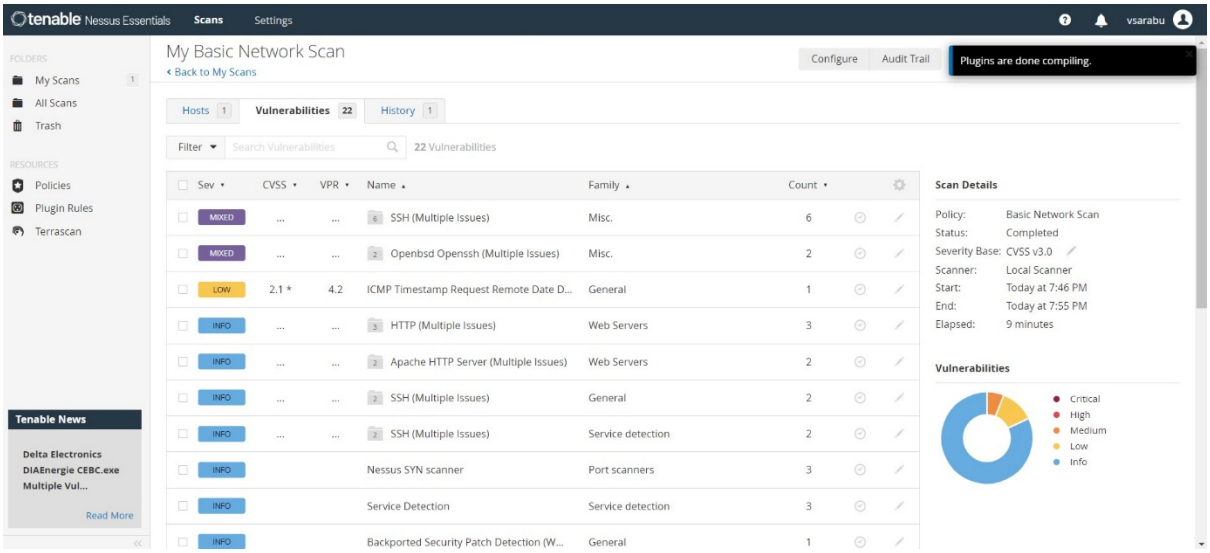
availability, confidentiality, and integrity of network resources. Proactive countermeasures, such as updating SSL/TLS protocols, swapping out outdated cryptographic standards, safeguarding administrative interfaces, and ensuring system updates and patches are applied regularly, are essential to reducing these risks. Sustaining the network's security posture and protecting it from dynamic cyber threats necessitates ongoing monitoring and regular evaluations. By implementing these steps, we can improve network security and defend against potential cyberattacks.

Outputs of Nessus Vulnerability Scan






tenable Nessus Essentials
Scans
Settings
vsarabu
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Approach.App Multiple Vulnerabilities
Read More
Plugins are done compiling.
INFO Service Detection Service detection 3
INFO Backported Security Patch Detection (W... General 1
INFO Common Platform Enumeration (CPE) General 1
INFO Device Type General 1
INFO Host Fully Qualified Domain Name (FQD... General 1
INFO Nessus Scan Information Settings 1
INFO Network Time Protocol (NTP) Server Dete... Service detection 1
INFO OS Identification General 1
INFO OS Security Patch Assessment Not Availa... Settings 1
INFO Patch Report General 1
INFO Target Credential Status by Authenticatio... Settings 1
INFO TCP/IP Timestamps Supported General 1
INFO Traceroute Information General 1
INFO Unix Operating System on Extended Sup... General 1


tenable Nessus Essentials
Scans
Settings
vsarabu
My Basic Network Scan
Back to My Scans
Configure
Audit Trail
Plugins are done compiling.
Hosts 1
Vulnerabilities 22
History 1
Filter
Search Vulnerabilities
22 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
MIXED ... ... SSH (Multiple Issues) Misc. 6
MIXED ... ... Openbsd Openssh (Multiple Issues) Misc. 2
LOW 2.1 * 4.2 ICMP Timestamp Request Remote Date D... General 1
INFO ... ... HTTP (Multiple Issues) Web Servers 3
INFO ... ... Apache HTTP Server (Multiple Issues) Web Servers 2
INFO ... ... SSH (Multiple Issues) General 2
INFO ... ... SSH (Multiple Issues) Service detection 2
INFO Nessus SYN scanner Port scanners 3
INFO Service Detection Service detection 3
INFO Backported Security Patch Detection (W... General 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:46 PM
End: Today at 7:55 PM
Elapsed: 9 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

References

Bairyev, M. (2024). *Cybersecurity Assessments: Types, Differences and Benefits*. Custom Software Development Company. https://maddevs.io/blog/types-of-cybersecurity-assessments/

Bansal, V. (2023). *Enumerating Email Address for Social Engineering and OSINT*. Scaler Topics. https://www.scaler.com/topics/cyber-security/scanning-for-vulnerabilities-with-nessus/

Kofod, A. (2020). *Types of Security Assessments and Which One is Right for Your Organization*. DEV Community. https://dev.to/leading-edje/types-of-security-assessments-and-which-one-is-right-for-your-organization-bpn

Thorin Klosowski. (2016). *How to Use Nessus to Scan a Network for Vulnerabilities*. Lifehacker; Lifehacker. https://lifehacker.com/how-to-use-nessus-to-scan-a-network-for-vulnerabilities-1788261156