NETWORK VULNERABILITY SCANNING PROJECT USING NESSUS, NMAP AND WIRESHARK

By Snehal Borhade

INDEX

NETWORK VULNERABILITY SCANNING PROJECT USING NESSUS, NMAP AND WIRESHARK

Abstract

The Network Vulnerability Scanning project provides a thorough understanding of the tools, network protocols, procedures, vulnerabilities, and documentation involved. Network Vulnerability Scanning involves scanning a network to identify potential vulnerabilities within the system. In this project, Metasploitable 2, an intentionally vulnerable Linux version, was used as the target system. Nmap and Nessus were utilized to scan the network, uncovering various vulnerabilities. These vulnerabilities were categorized into critical, medium, and low levels. Additionally, Wireshark was employed to analyze the protocols used during the assessment.

System description

A secure virtual environment was established using VirtualBox. Kali Linux was installed on VirtualBox to perform scans on Metasploitable 2, which was also set up within the virtual lab. Metasploitable 2, designed to be intentionally vulnerable, contains numerous vulnerabilities and open ports that can be exploited to gain control over the machine. In summary, a home lab was created to facilitate safe and legal network scanning activities.

Purpose

The purpose of scanning the network is to understand the procedures and gain hands-on experience with various essential cybersecurity tools. This project is crucial for comprehending protocols and the mechanisms of data transfer. The primary objective is to understand how a machine can be exploited by threat actors and to learn how to remediate these vulnerabilities.

Approach

A systematic approach was employed to conduct the scan. Initially, Nmap was used to ping the network and verify its active status. Once the machine's status was confirmed, additional Nmap commands were executed to gather detailed information about the system. Wireshark was utilized to verify the network protocols in use. Nessus was then used to perform a comprehensive network scan, generating a detailed vulnerability report. All findings and procedures were meticulously documented.

Procedure

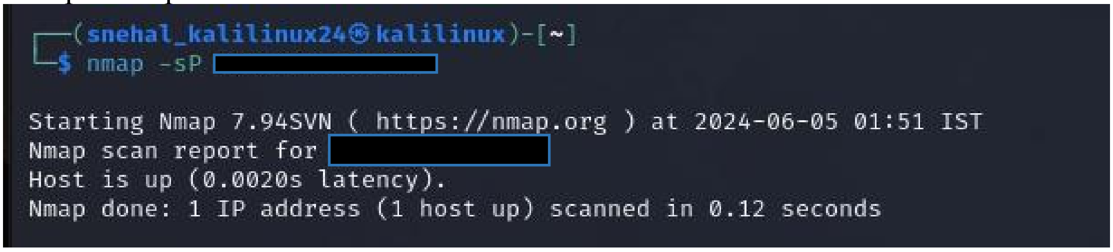
Nmap , Nessus and wireshark were used in the process for systematic development of project.

Nmap

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. It offers a variety of features for probing networks, including host discovery, service detection, and operating system identification. The following Nmap commands were utilized to gather additional information:

Ping is used to check for live system. It gives us information about what is live on the network subnet.
Nmap -sP is the command used and then simple nmap command is used to check for open ports

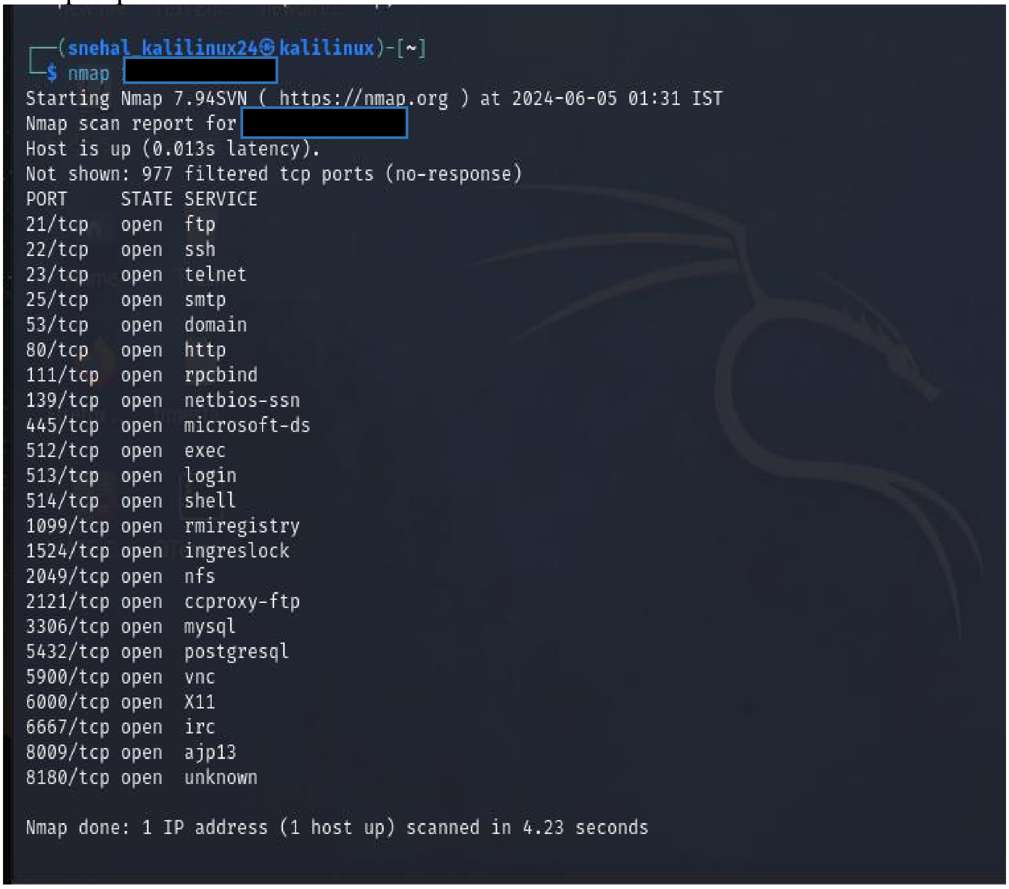
Nmap -sP <ip address>



```
┌──(snehal_kalilinux24㉿kalilinux)-[~]
└─$ nmap -sP [redacted]

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 01:51 IST
Nmap scan report for [redacted]
Host is up (0.0020s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Fig .1 ping command

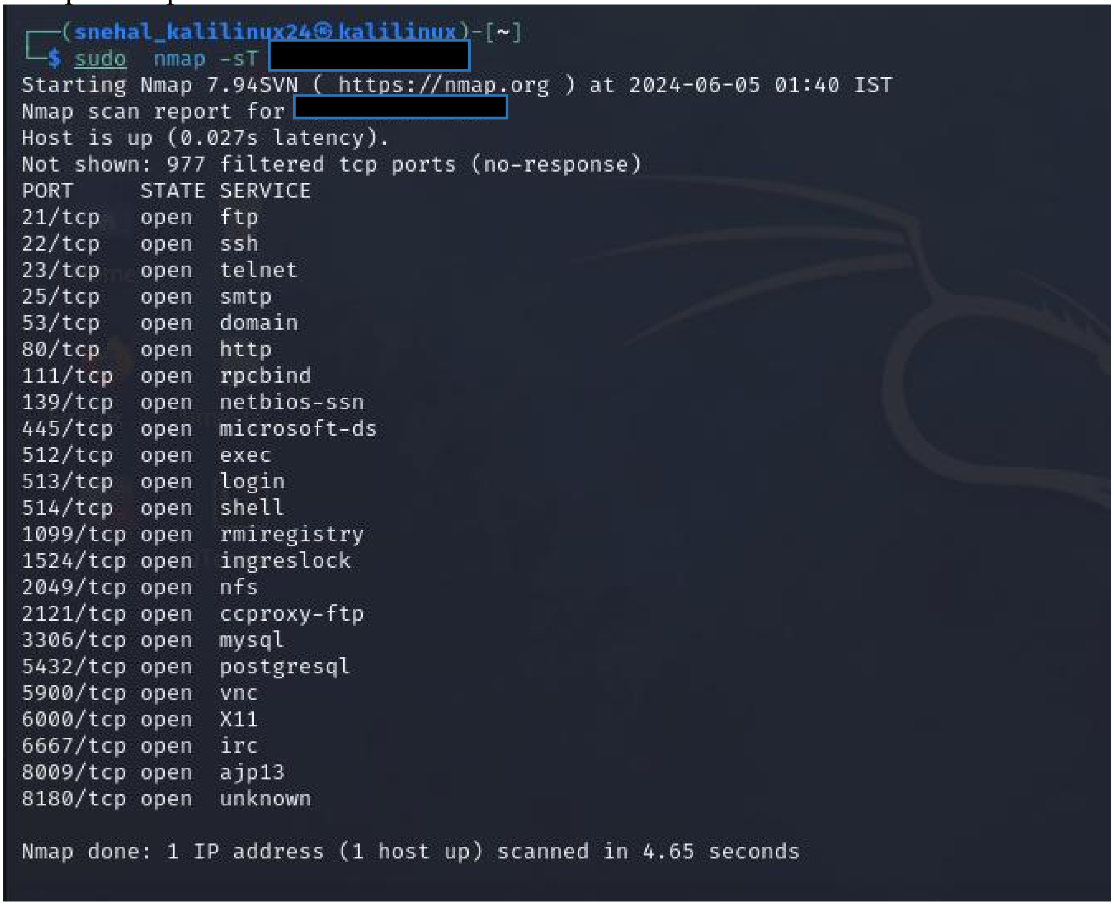
Nmap <ip address>



```
┌──(snehal_kalilinux24㉿kalilinux)-[~]
└─$ nmap [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 01:31 IST
Nmap scan report for [redacted]
Host is up (0.013s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
```

Fig .2 Nmap <ip address>

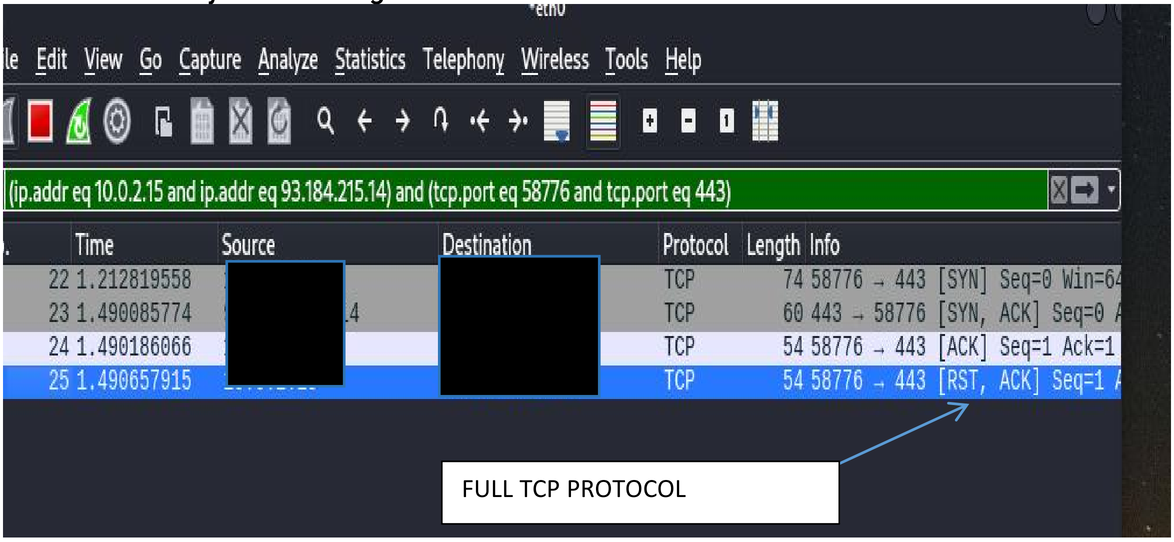
Nmap -sT <ip address>



```
┌──(snehal_kalilinux24㉿kalilinux)-[~]
└─$ sudo nmap -sT [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 01:40 IST
Nmap scan report for [redacted]
Host is up (0.027s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.65 seconds
```

Fig .3 Nmap -sT <ip address>

Its important to note here that -sT represent tcp protocol. TCP 3 way handshake protocol is used to check whether the port is open . It is also called as full handshake because complete handshake protocol is executed. We can verify this by analysing network using wire-shark while simultaneously conducting -sT command.


*eth0
le Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

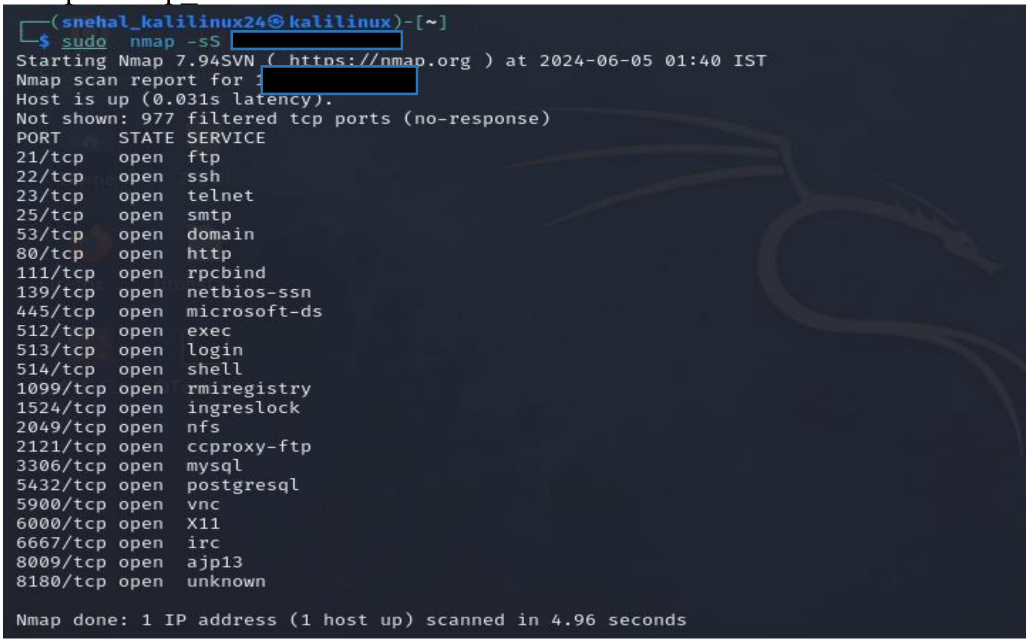
```
(ip.addr eq 10.0.2.15 and ip.addr eq 93.184.215.14) and (tcp.port eq 58776 and tcp.port eq 443)

.  Time           Source      Destination  Protocol Length Info
22 1.212819558    [redacted]  [redacted]   TCP      74 58776 → 443 [SYN] Seq=0 Win=64
23 1.490085774                             TCP      60 443 → 58776 [SYN, ACK] Seq=0 A
24 1.490186066                             TCP      54 58776 → 443 [ACK] Seq=1 Ack=1
25 1.490657915                             TCP      54 58776 → 443 [RST, ACK] Seq=1 A
```

FULL TCP PROTOCOL

Fig .4 Full TCP

Here it can be observed that a complete tcp protocol is performed i.e SYN , SYN ACK and ACK and RST i.e the connection is terminated.

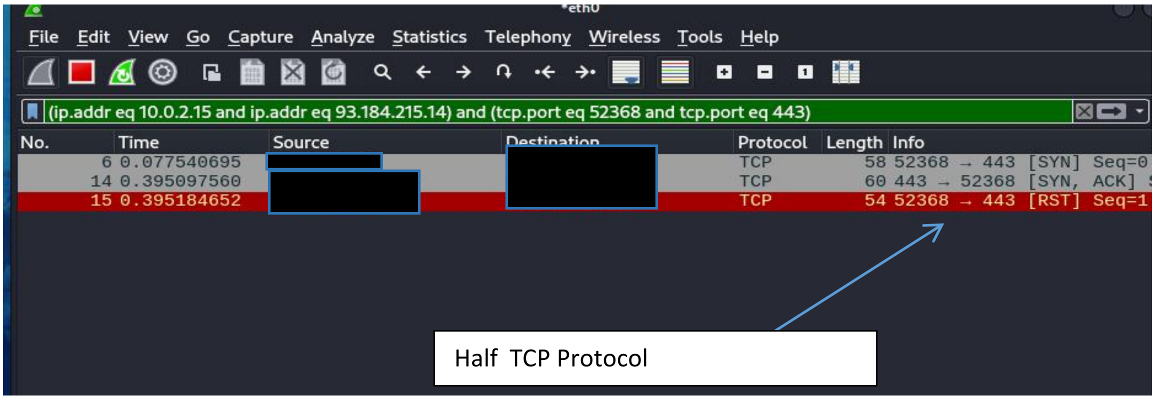
The problem with full TCP scan is it is often detected by firewalls and is blocked. So to overcome this Half TCP scan or SYN scan is used.
As the TCP scan is not completed it is left undected.
Nmap -sS <ip_address>



```
┌──(snehal_kalilinux24㉿kalilinux)-[~]
└─$ sudo nmap -sS [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 01:40 IST
Nmap scan report for [redacted]
Host is up (0.031s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.96 seconds
```

Fig .5 Nmap -sS <ip_address>

Same can be verified on wireshark as



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.addr eq 10.0.2.15 and ip.addr eq 93.184.215.14) and (tcp.port eq 52368 and tcp.port eq 443)

```
No.   Time          Source      Destination  Protocol Length Info
    6 0.077540695   [redacted]  [redacted]   TCP         58 52368 → 443 [SYN] Seq=0
   14 0.395097560   [redacted]               TCP         60 443 → 52368 [SYN, ACK] S
   15 0.395184652                            TCP         54 52368 → 443 [RST] Seq=1
```

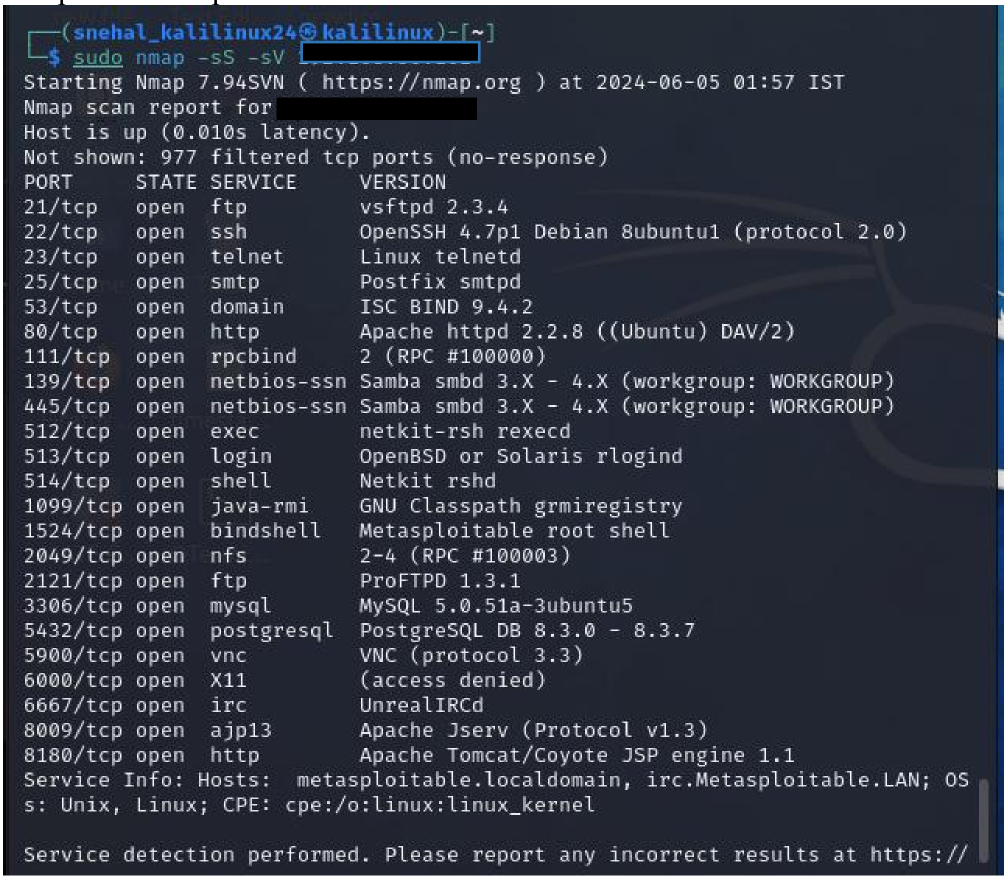
Half TCP Protocol

Fig .6 Half TCP

It can be seen that TCP protocol is not completed and is half SYN , SYN ACK , RST i.e the connection is terminated.

We can also scan the network to identify the verion of protocol they are using.

nmap -sS -sV <ip address>

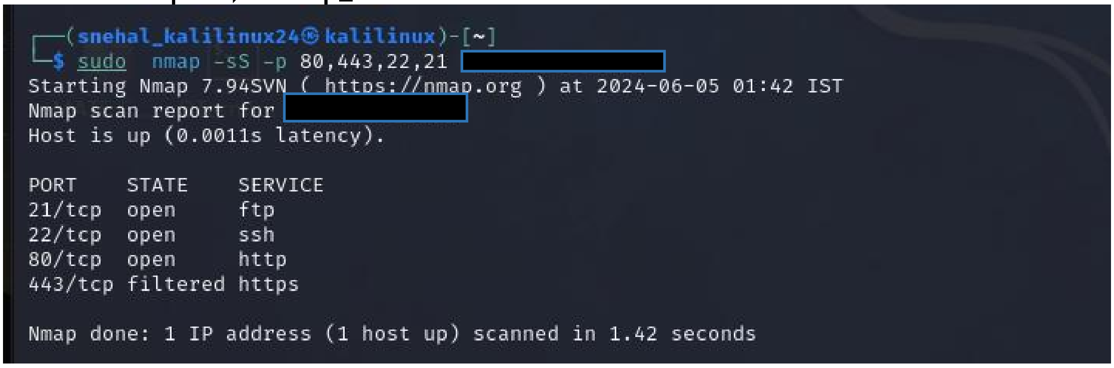


```
┌──(snehal_kalilinux24㉿kalilinux)-[~]
└─$ sudo nmap -sS -sV [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 01:57 IST
Nmap scan report for [redacted]
Host is up (0.010s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OS
s: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://
```

Fig .7 nmap -sS -sV <ip address>

To obtain information about only particular protocol is also possible with nmap.

nmaP -sS -p 80,443 <ip_address>



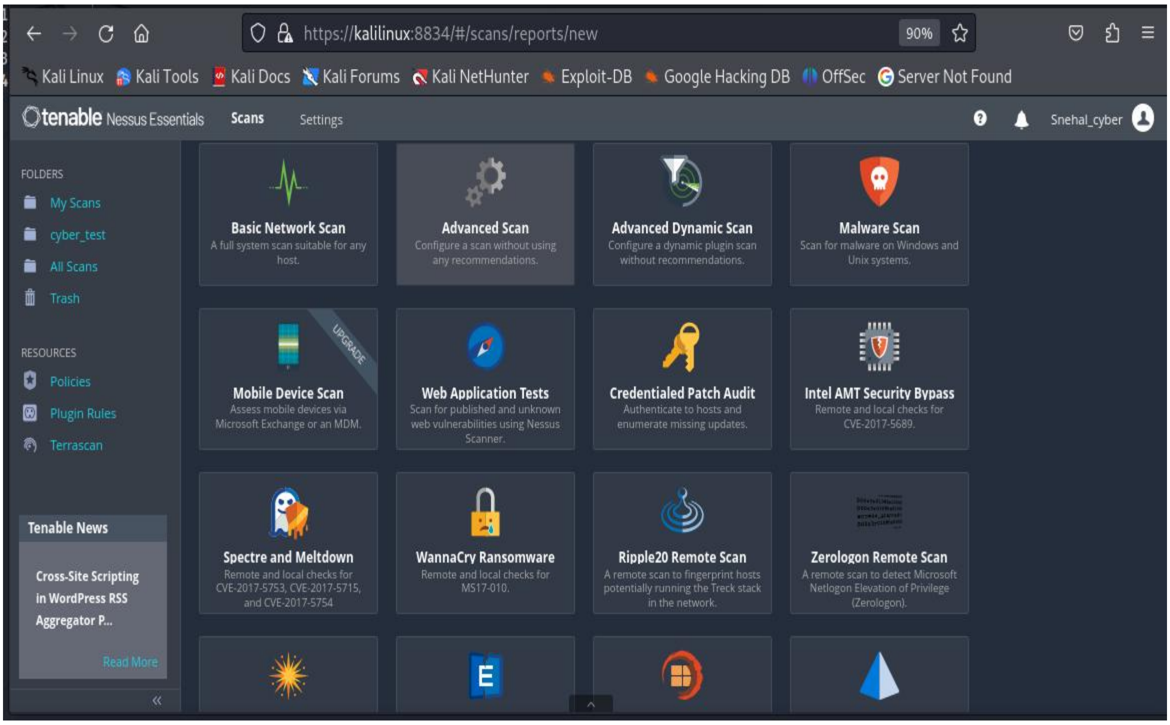
```
┌──(snehal_kalilinux24㉿kalilinux)-[~]
└─$ sudo  nmap -sS -p 80,443,22,21 [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 01:42 IST
Nmap scan report for [redacted]
Host is up (0.0011s latency).

PORT    STATE    SERVICE
21/tcp  open     ftp
22/tcp  open     ssh
80/tcp  open     http
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds
```

Fig .8nmaP -sS -p 80,443 <ip_address>

Hence Nmap provides various indepth information about system which can be further used to exploit it.

Nessus:

Nessus is a widely-used vulnerability scanner that helps identify security issues within a network. It scans systems for vulnerabilities, misconfigurations, and compliance issues, providing detailed reports to aid in securing the network.
It provides variety of options for scannning a network.



Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware
Remote and local checks for MS17-010.

Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

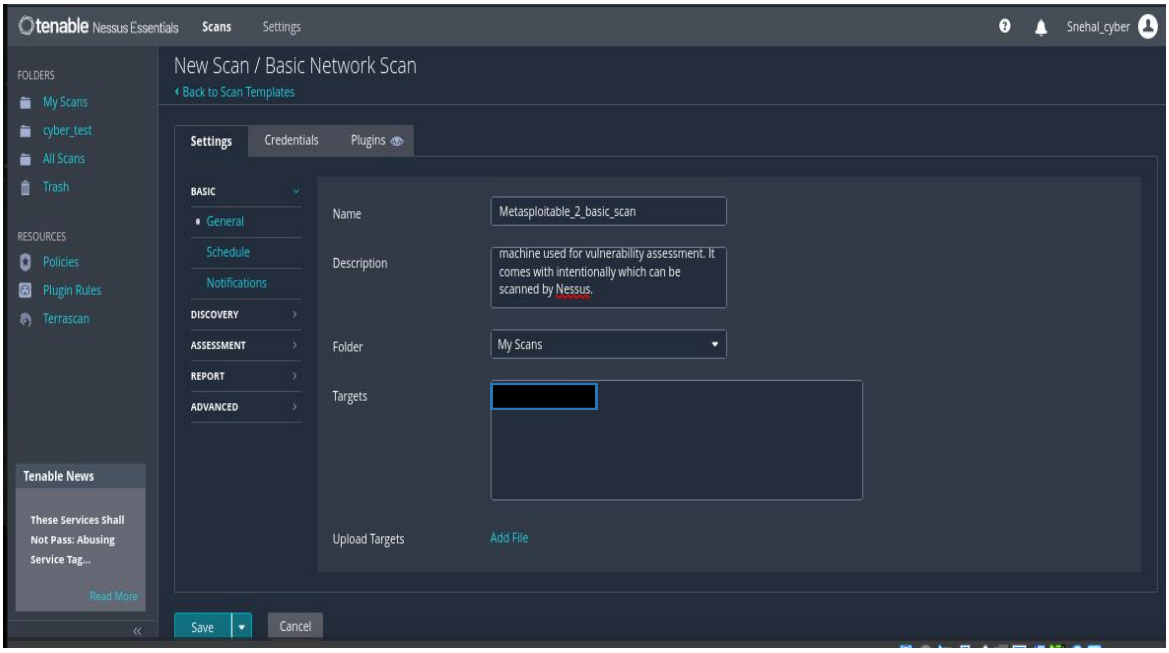
Fig .9Nessus Screen

Some of the scans that nessus provide are

Basic Network scan :- This scan has basic configuration suitable for any network.A basic scan in Nessus provides a comprehensive overview of the security posture of the scanned systems, helping to identify and mitigate potential security threats.

Adavanced Network scan is same like basic scan but it provides more configuration options such as port selection and enabling specific vulnerabilities etc

Basic network scan :-



New Scan / Basic Network Scan

Name: Metasploitable_2_basic_scan

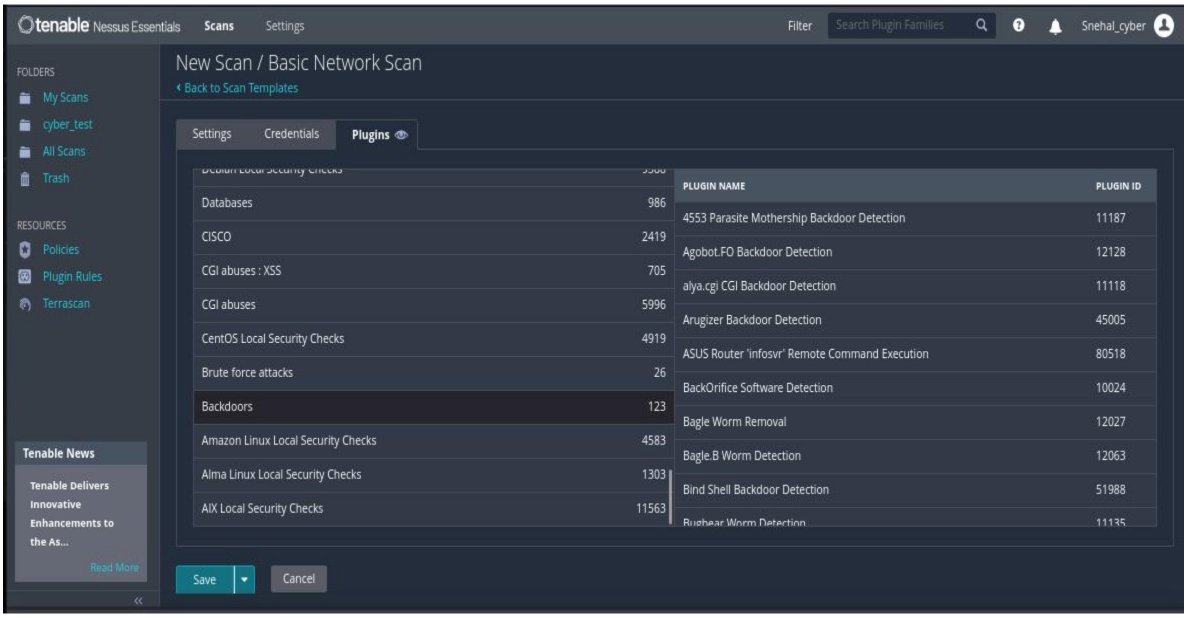
Description: machine used for vulnerability assessment. It comes with intentionally which can be scanned by Nessus.

Folder: My Scans

Targets: [redacted]

Upload Targets: Add File

Fig .10 Basic Network Scan1



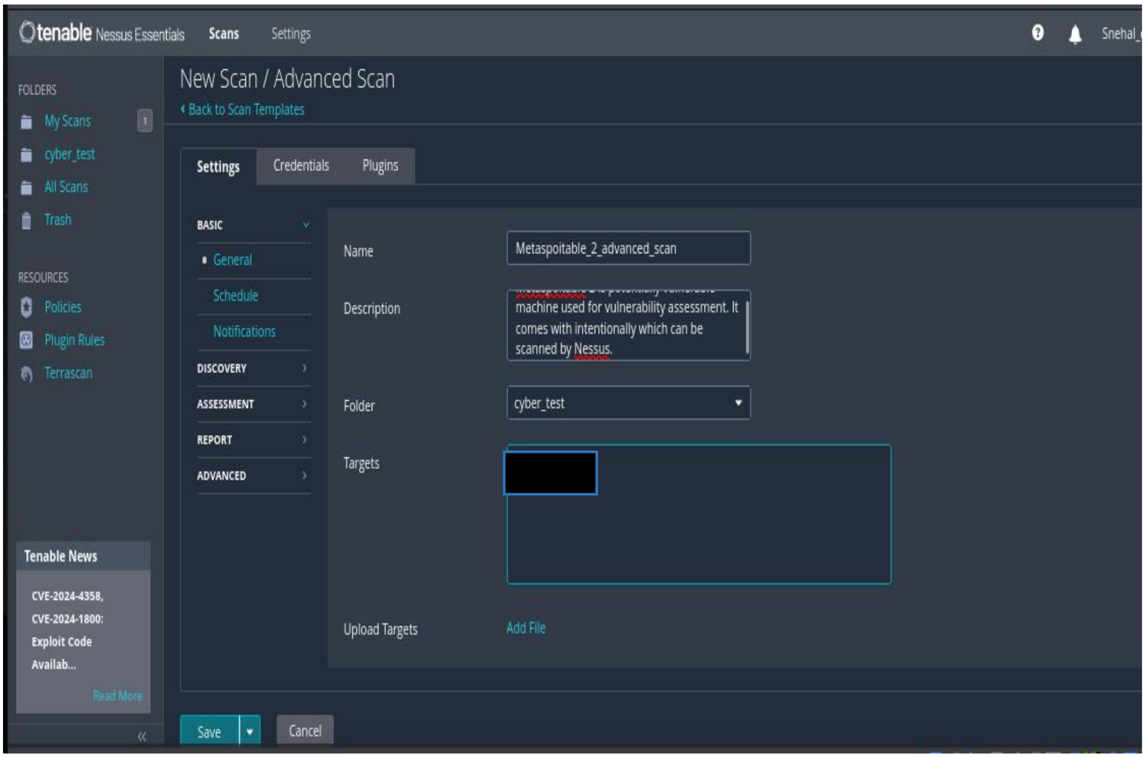
New Scan / Basic Network Scan

Debian Local Security Checks	[illegible]
Databases	986
CISCO	2419
CGI abuses : XSS	705
CGI abuses	5996
CentOS Local Security Checks	4919
Brute force attacks	26
Backdoors	123
Amazon Linux Local Security Checks	4583
Alma Linux Local Security Checks	1303
AIX Local Security Checks	11563

PLUGIN NAME	PLUGIN ID
4553 Parasite Mothership Backdoor Detection	11187
Agobot.FO Backdoor Detection	12128
alya.cgi CGI Backdoor Detection	11118
Arugizer Backdoor Detection	45005
ASUS Router 'infosvr' Remote Command Execution	80518
BackOrifice Software Detection	10024
Bagle Worm Removal	12027
Bagle.B Worm Detection	12063
Bind Shell Backdoor Detection	51988
Bugbear Worm Detection	11135

Fig .11 Basic Network Scan2

Advanced Network Scan :-



Name: Metaspoitable_2_advanced_scan

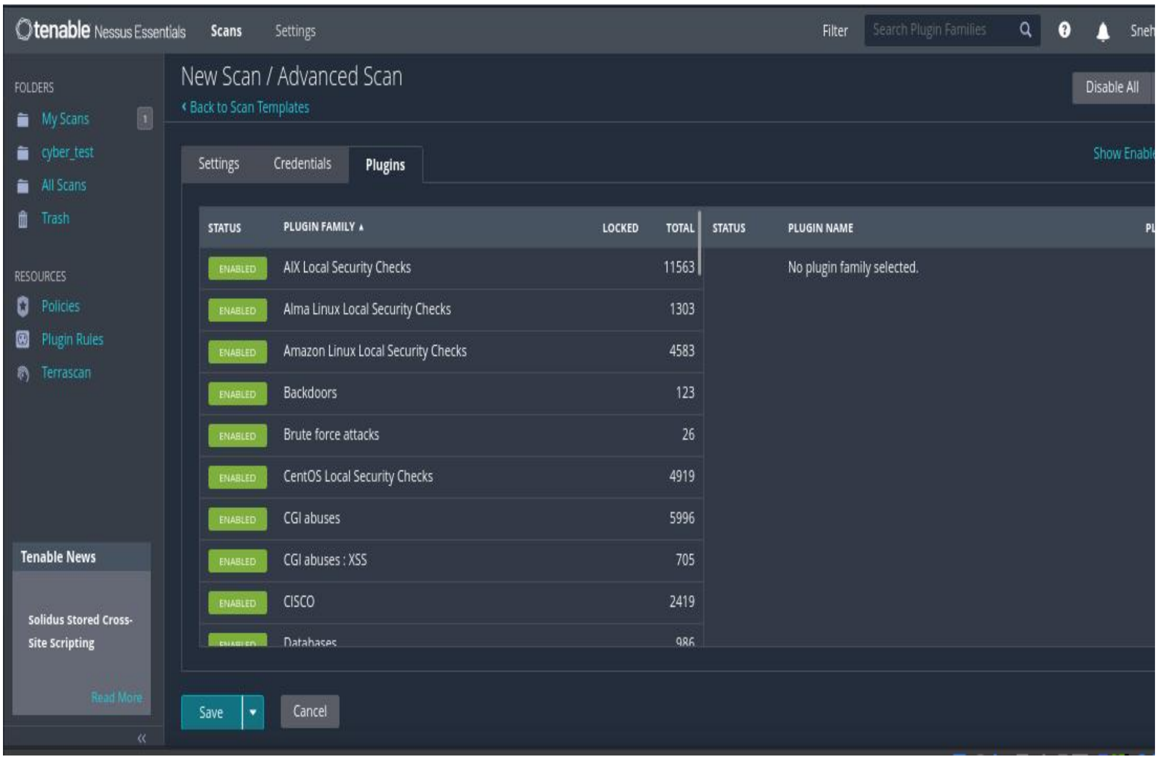
Description: machine used for vulnerability assessment. It comes with intentionally which can be scanned by Nessus.

Folder: cyber_test

Targets: [redacted]

Upload Targets: Add File

Fig .12 Advance Network Scan1



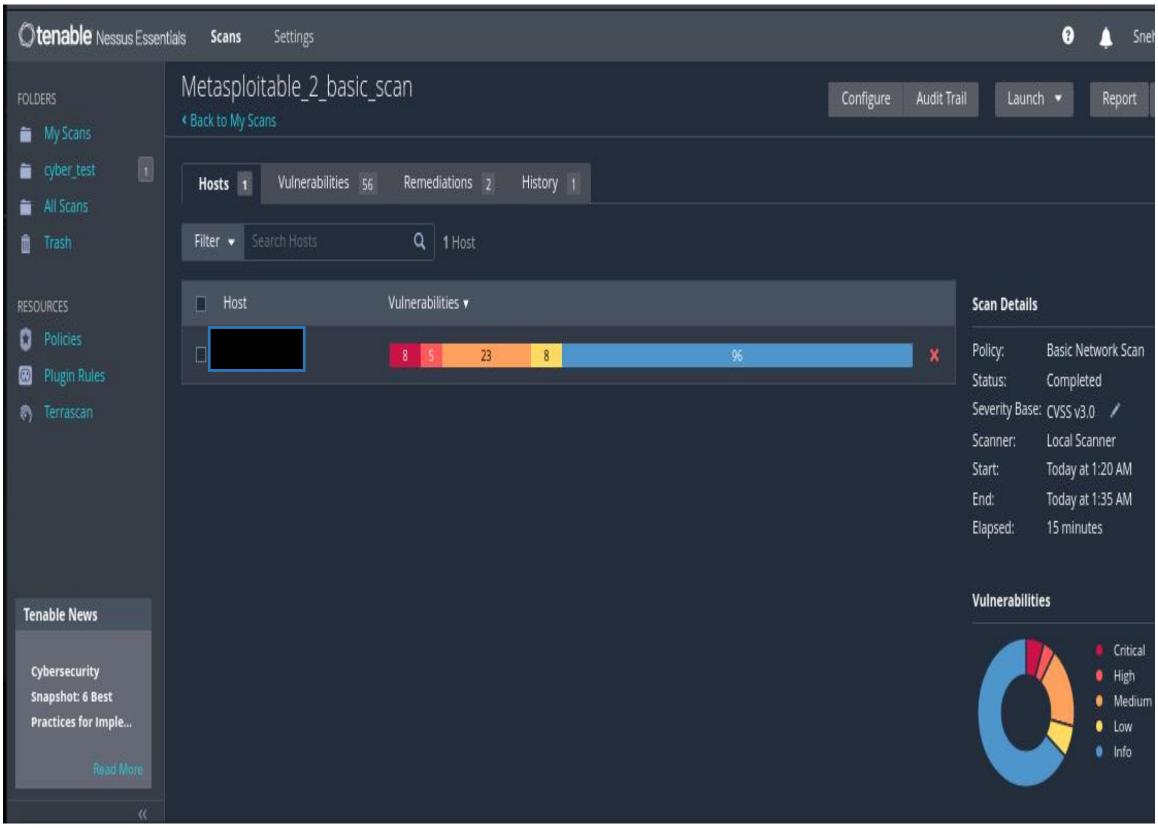
STATUS	PLUGIN FAMILY ▲	LOCKED	TOTAL
ENABLED	AIX Local Security Checks		11563
ENABLED	Alma Linux Local Security Checks		1303
ENABLED	Amazon Linux Local Security Checks		4583
ENABLED	Backdoors		123
ENABLED	Brute force attacks		26
ENABLED	CentOS Local Security Checks		4919
ENABLED	CGI abuses		5996
ENABLED	CGI abuses : XSS		705
ENABLED	CISCO		2419
ENABLED	Databases		986

STATUS	PLUGIN NAME
	No plugin family selected.

Fig .13 Advance Network Scan2

SCAN RESULTS

The scan outcome shows that there are potentially 6 critical, 4 high , 17 medium ,7 low and 62 informative vulnerabilities.



Metasploitable_2_basic_scan

‹ Back to My Scans

[redacted]

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 1:20 AM

End: Today at 1:35 AM

Elapsed: 15 minutes

Fig .14 scan results

Risk assessment

This report identifies security risks that could significantly impact mission-critical applications essential for daily business operations.

A cyber security risk assessment involves the systematic identification, analysis, and evaluation of potential risks. Its purpose is to ensure that the cyber security measures you implement are suitable for the specific risks your organization encounters. Failing to conduct a risk assessment could result in inefficient allocation of time, energy, and resources in your cyber security efforts.

Table. 1 risk categorization

critical	high	medium	low	informative
6	4	17	7	62

Critical Level Vulnerability :

Critical vulnerabilities demand urgent attention as they pose a severe risk to system security. These vulnerabilities are typically relatively easy for attackers to exploit, often requiring minimal expertise or resources. Once exploited, critical vulnerabilities can grant attackers full control over the affected systems, allowing them to execute malicious actions, steal sensitive data, or disrupt operations. Given the potential consequences of exploitation, prompt remediation is essential to mitigate the risk and safeguard the integrity and confidentiality of the systems and data.

Cvss is Common vulnerability scoring system is it used to evaluate the severity of security vulnerabilities in computer systems

Table. 2 Critical Level Vulnerability

Plugin id	Name	description	cvss
134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)	A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE)	9.8
20007	SSL Version 2 and 3 Protocol Detection	The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.	9.8
33850	Unix Operating System Unsupported Version Detection	According to its self-reported version number, the Unix operating system running on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.	10

High Level Vulnerability :

High severity vulnerabilities can be characterized as flaws that may lead to an attacker accessing application resources or unintended exposure of data.

Table. 3 High Level Vulnerability

Plugin id	Name	description	cvss
90509	Samba Badlock Vulnerability	The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels	7.5
42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.	7.5

Medium Level Vulnerability :

Medium severity vulnerabilities usually arise from misconfiguration of systems or lack of security controls. Exploitation of these vulnerabilities may lead to accessing a restricted amount of data or could be used in conjunction with other flaws to gain unintended access to systems or resources.

.

Table. 4 Medium level vulnerability

Plugin id	Name	description	cvss
51192	SSL Certificate Cannot Be Trusted	the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.	6.5
104743	TLS Version 1.0 Protocol Detectio	The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws.	6.5

Low Level Vulnerability:

Low severity vulnerabilities contain flaws that may not be directly exploitable but introduce unnecessary weakness to an application or system.

Table. 5 Low level vulerability

Plugin id	Name	description	cvss
153953	SSH Weak Key Exchange Algorithms Enabled	he remote SSH server is configured to allow weak key exchange algorithms	3.7
83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.	2.6

Recommendation

While vulnerability scanning is valuable, it is just one method for evaluating the security.It's crucial not to solely rely on these results as the sole indicator of the network's security posture. Additional assessments, such as policy reviews, examination of internal security controls and protocols, or internal red teaming/penetration testing, should also be considered to gain a comprehensive understanding of the network's security status.

Few remediations are:-

1) Ensure that all software components, including operating systems, applications, and libraries, are regularly updated to the latest versions.
2) Configure SSL/TLS protocols and cipher suites to use modern, secure encryption standards and disable deprecated protocols and weak cipher suites.
3) Securely manage cryptographic keys throughout their lifecycle, including generation, storage, distribution, usage, and destruction, following industry best practices and standards.

Conclusion

In conclusion, the Network Vulnerability Scanning project serves as a comprehensive exploration into the intricacies of cybersecurity tools, network protocols, and procedural methodologies. By focusing on the scanning of networks to detect potential vulnerabilities, this project offers invaluable insights into the critical aspects of safeguarding digital infrastructures. Through the utilization of Metasploitable 2 as a deliberate target system, alongside powerful tools such as Nmap and Nessus, a diverse range of vulnerabilities were uncovered and meticulously categorized based on their severity levels. Moreover, the incorporation of Wireshark for protocol analysis further enhanced the depth of understanding in assessing network security. Overall, this project underscores the importance of proactive vulnerability management in fortifying digital environments against potential threats.