MINOR PROJECT II

Report on Network Scanning

&

Vulnerability Assessment

Company: Sense learner Technologies Pvt. Ltd.

Name: Adarsh Kumar

Group Name: Hosta

Date: 10/07/2023

Project objectives and methodology:

The objective of this minor project is to analyse the security of Metasploitable 2, a deliberately vulnerable virtual machine, using the tools Nmap and Nessus. We perform network scanning, conduct a vulnerability assessment, and generate a comprehensive report outlining the identified vulnerabilities and recommended remediation actions.

The project follows a systematic methodology. First, we will install Metasploitable 2 on our local machines or a virtualization platform. Next, using Nmap, we will conduct a network scan to gather information about the target network, including active hosts, open ports, and services running on those ports.

Once we have a clear understanding of the network, we will use Nessus, a powerful vulnerability assessment tool, to perform a comprehensive scan of the Metasploitable 2 VM. This scan will help identify potential vulnerabilities, such as misconfigurations, outdated software versions, and known security weaknesses.

Based on the scan results, we will analyse and assess the severity of each vulnerability, prioritizing them based on risk level and likelihood of exploitation. This analysis will inform the generation of a detailed report, which will summarize the identified vulnerabilities, their severity levels, and recommended actions for remediation.

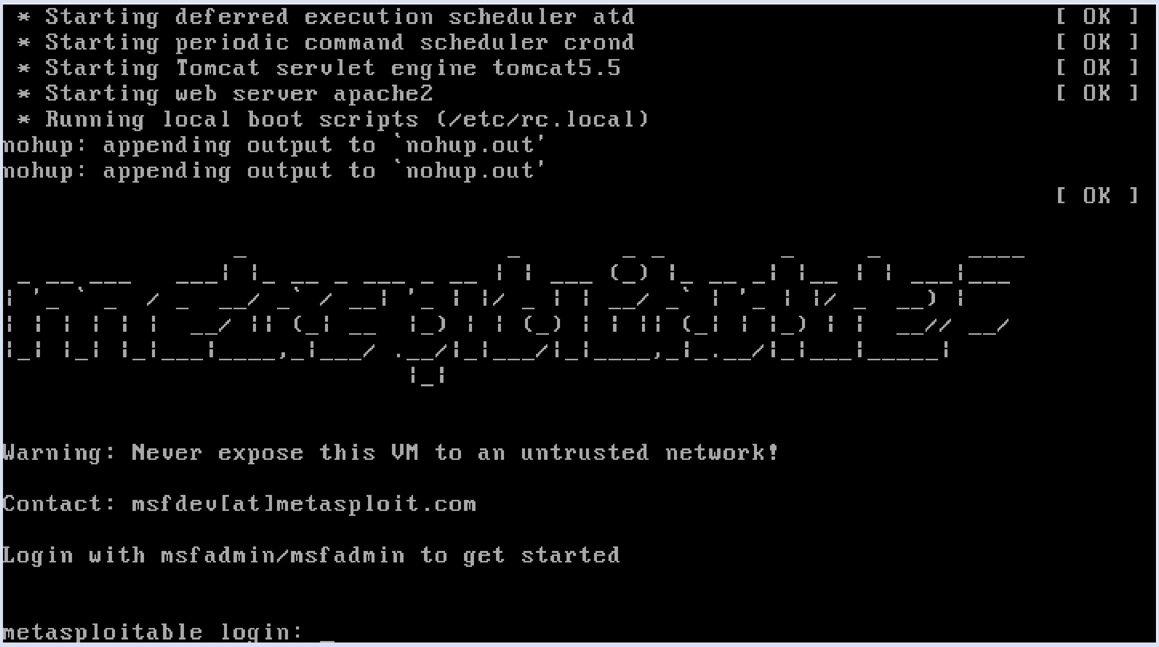
The report will serve as a valuable resource for understanding the security posture of Metasploitable 2 and will provide actionable recommendations for improving its security. Through this project, we will gain practical experience in analysing and mitigating security vulnerabilities, as well as developing strategies to enhance the overall security of a system.

Metasploitable 2 installation process and network configuration:

Metasploitable 2 is a virtual machine that can be downloaded from the Rapid7 website. The virtual machine is compatible with VMware, VirtualBox, and other popular virtualization platforms.

Installation Process:

- Download the virtual machine image from the Rapid7 website.
- Import the virtual machine image into your virtualization platform (e.g., VirtualBox, VMware).
- Configure virtual machine settings (base memory processor and storage).
- Start the Metasploitable 2 VM.



```
 * Starting deferred execution scheduler atd                          [ OK ]
 * Starting periodic command scheduler crond                          [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                           [ OK ]
 * Starting web server apache2                                        [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                      [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

By default, Metasploitable 2 is configured to use NAT and Host-only network adapters. This means that the virtual machine can only be accessed from the host machine.

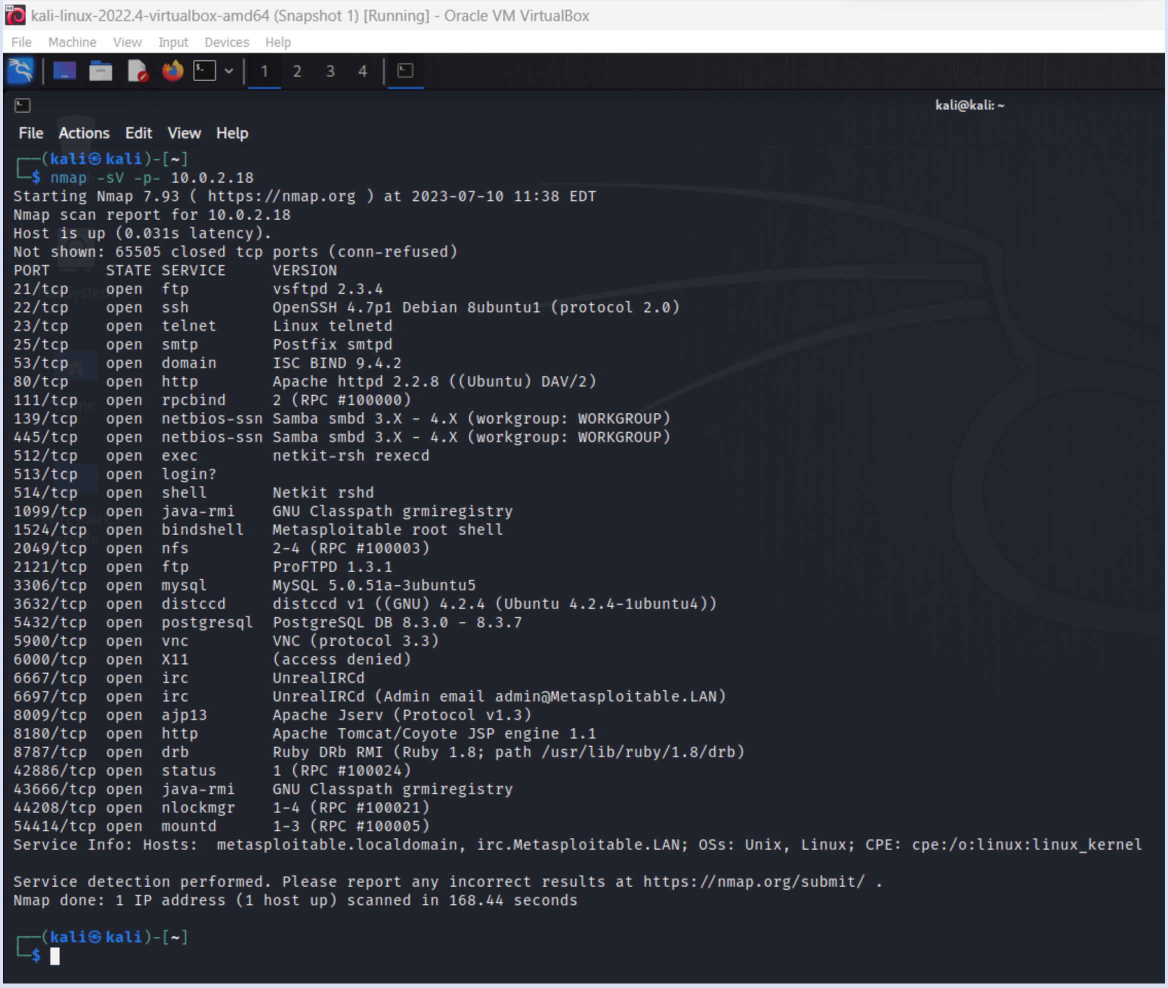
Network Configuration:

- Review and configure network adapter settings.
- Assign an IP address to the Metasploitable 2 VM.
- Configure the firewall settings.
- Test network connectivity.

To access Metasploitable 2 from other machines on our network, we need to change the network configuration. we can do this by editing the virtual machine's network settings. In my case, it is NAT network.

Nmap scan results:

On successfully Performing the network scanning from Nmap using my Kali virtual machine to target machine Metasploitable 2, whose IP address is 10.0.2.18. I got the following results. This output shows that the target host is running open ports 20,22, 80, 139, 445 and many more.


kali-linux-2022.4-virtualbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 10.0.2.18
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-10 11:38 EDT
Nmap scan report for 10.0.2.18
Host is up (0.031s latency).
Not shown: 65505 closed tcp ports (conn-refused)
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?
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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
42886/tcp open  status      1 (RPC #100024)
43666/tcp open  java-rmi    GNU Classpath grmiregistry
44208/tcp open  nlockmgr    1-4 (RPC #100021)
54414/tcp open  mountd      1-3 (RPC #100005)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 168.44 seconds

┌──(kali㉿kali)-[~]
└─$ ▌
```

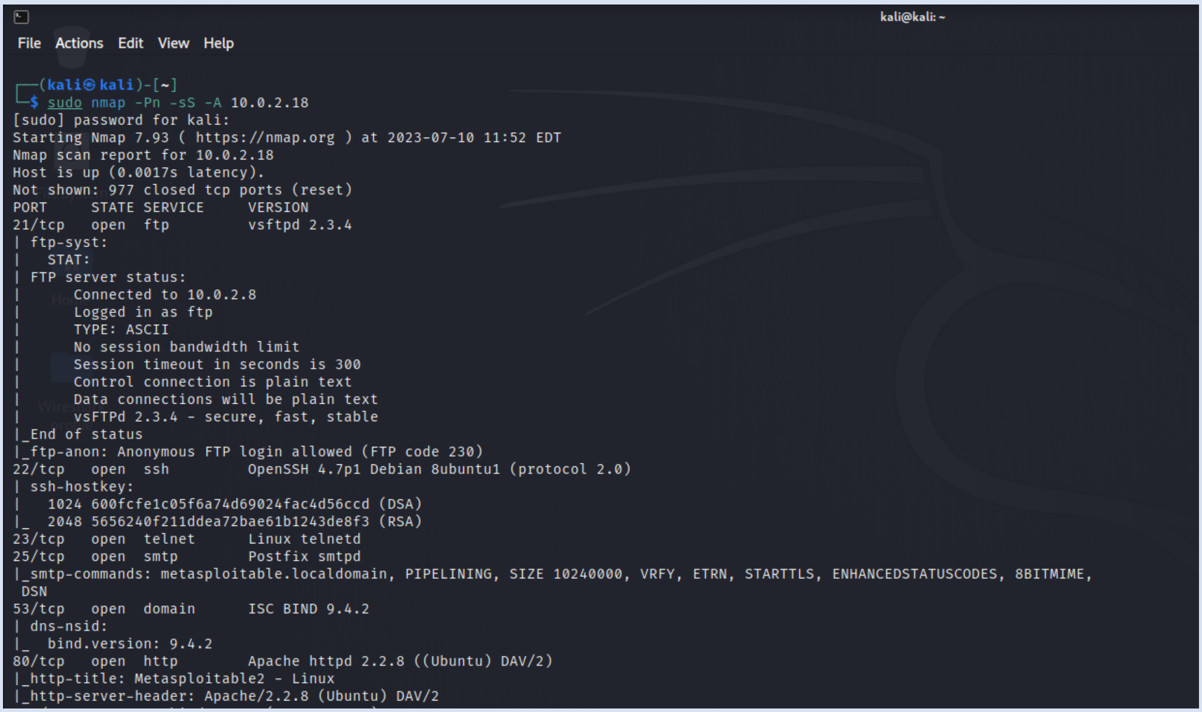
"nmap *-sV -p- 10.0.2.18"* This command will scan all of the open ports on the Metasploitable 2 machine. The -sV option will tell Nmap to identify the services that are running on the open ports.

As we know that Metasploitable 2 is intentionally vulnerable for testing and learning purposes.During the scan, nmap discovered various open ports on the target machine. For example, it identified port 21 for FTP, port 22 for SSH, port 80 for HTTP, and port 445 for SMB, among others. This information gives insight into the network services available on the Metasploitable 2 machine.

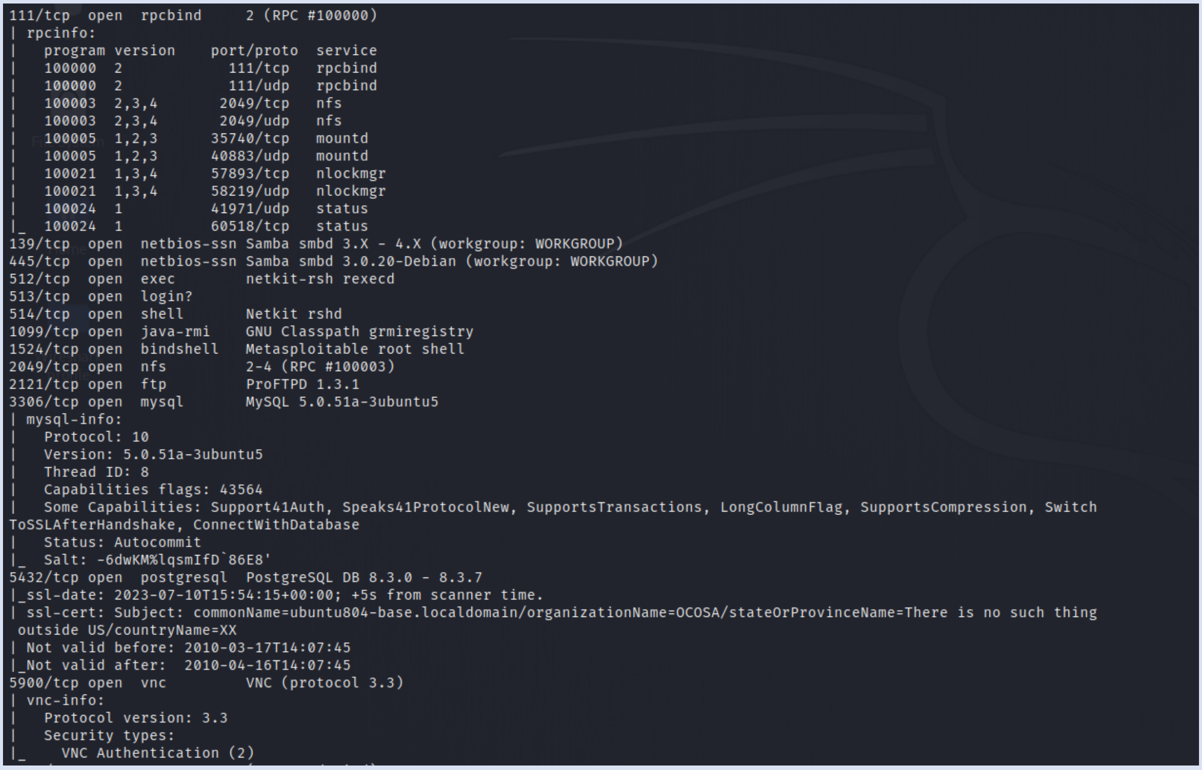
Furthermore, nmap performed version detection to determine the specific versions of the services running on the open ports. By analyzing the responses received, nmap was able to provide details about the FTP, SSH, HTTP, and other services and their respective versions. This information is crucial for identifying potential vulnerabilities associated with outdated or insecure service versions.

Now performing an aggressive scan.

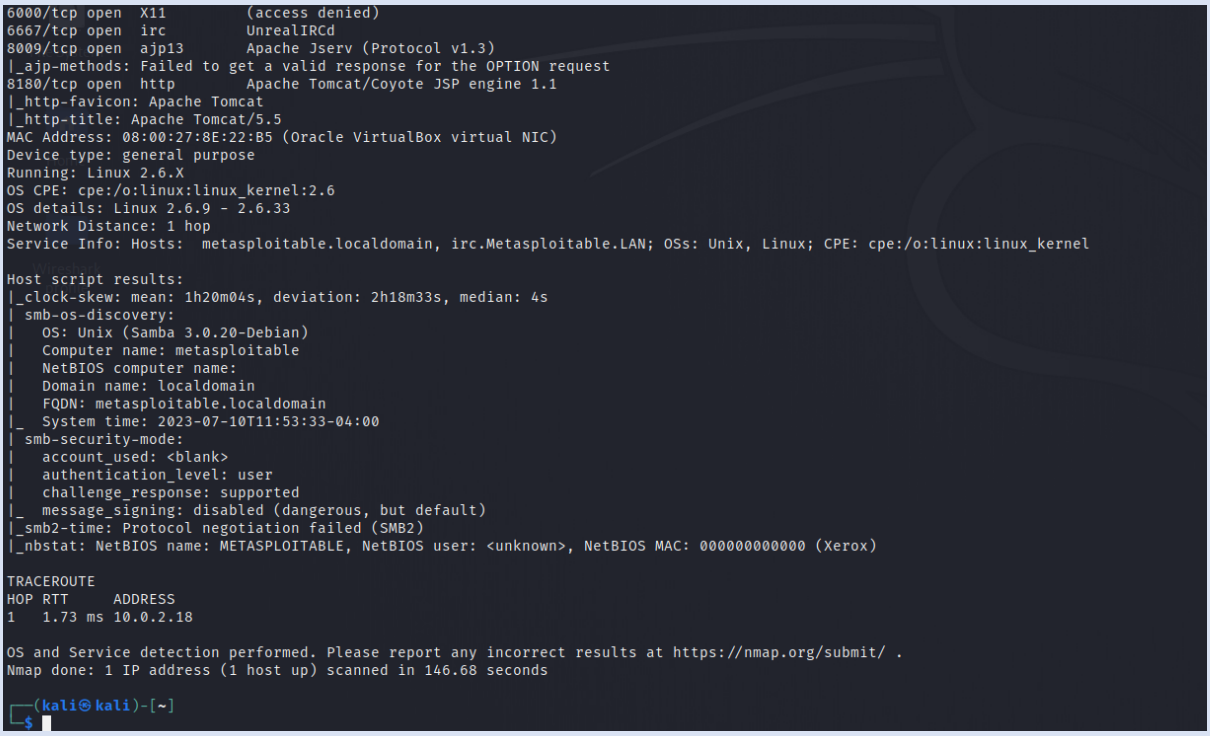
The command *"sudo nmap -Pn -sS -A 10.0.2.18"* is used to scan the host at IP address 10.0.2.18 for open ports and their associated services. The *sudo* command is used to run the *nmap* command with root privileges. The *-Pn* option tells Nmap to skip the ping scan, which is useful if you know that the target host is up. The *-sS* option tells Nmap to perform a TCP SYN scan, which is a faster and more reliable way to scan for open ports. The *-A* option tells Nmap to perform an aggressive scan, which will gather additional information about the target host, such as the operating system and service versions.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -Pn -sS -A 10.0.2.18
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-10 11:52 EDT
Nmap scan report for 10.0.2.18
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.8
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME,
 DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```



```
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      35740/tcp   mountd
|   100005  1,2,3      40883/udp   mountd
|   100021  1,3,4      57893/tcp   nlockmgr
|   100021  1,3,4      58219/udp   nlockmgr
|   100024  1          41971/udp   status
|_  100024  1          60518/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, Speaks41ProtocolNew, SupportsTransactions, LongColumnFlag, SupportsCompression, Switch
ToSSLAfterHandshake, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: -6dwKM%lqsmIfD`86E8'
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-07-10T15:54:15+00:00; +5s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing
 outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
```



```
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
MAC Address: 08:00:27:8E:22:B5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h20m04s, deviation: 2h18m33s, median: 4s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-07-10T11:53:33-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

TRACEROUTE
HOP RTT     ADDRESS
1   1.73 ms 10.0.2.18

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 146.68 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

When we execute this command, nmap will perform an advanced scan on the target machine (10.0.2.18) using a TCP SYN scan (-sS) to determine open ports. It will also conduct aggressive scanning (-A), which includes OS fingerprinting to identify the operating system, version detection to determine the services and their versions, script scanning to run predefined scripts for additional information, and traceroute to map the network path to the target.

The combination of these options allows for a comprehensive assessment of the target machine, including its network topology, open ports, services, and potentially even the operating system in use.

The commands nmap -sV -p- 10.0.2.18 and sudo nmap -Pn -sS -A 10.0.2.18 are both used to scan the host at IP address 10.0.2.18 for open ports and their associated services. However, there are some key differences between the two commands.

- The first difference is the use of the -Pn option in the second command. The -Pn option tells Nmap to skip the ping scan. This is useful if you know that the target host is up, as the ping scan can add a few seconds to the scan time.

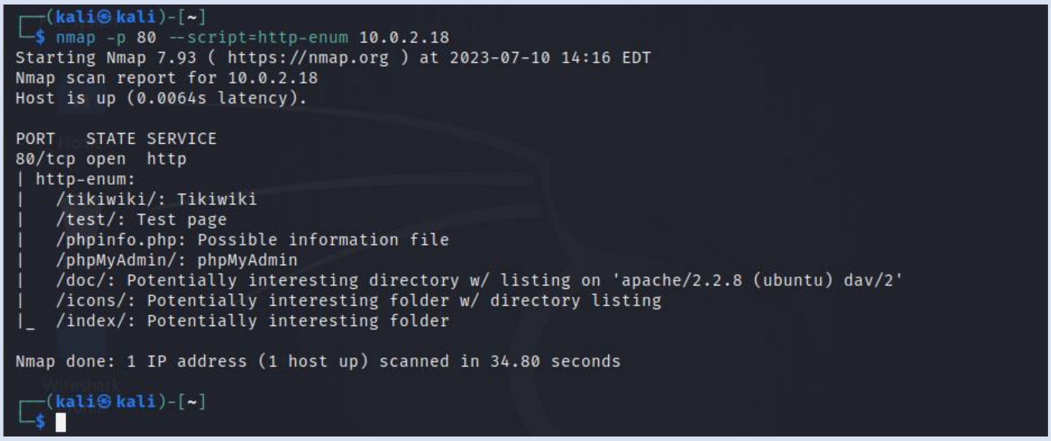
- The second difference is the use of the -sS option in the second command. The -sS option tells Nmap to perform a TCP SYN scan. This is a faster and more reliable way to scan for open ports than the default TCP connect scan.

- The third difference is the use of the -A option in the second command. The -A option tells Nmap to perform an aggressive scan. This will gather additional information about the target host, such as the operating system and service versions.

Utilizing Nmap scripts to gather additional information:

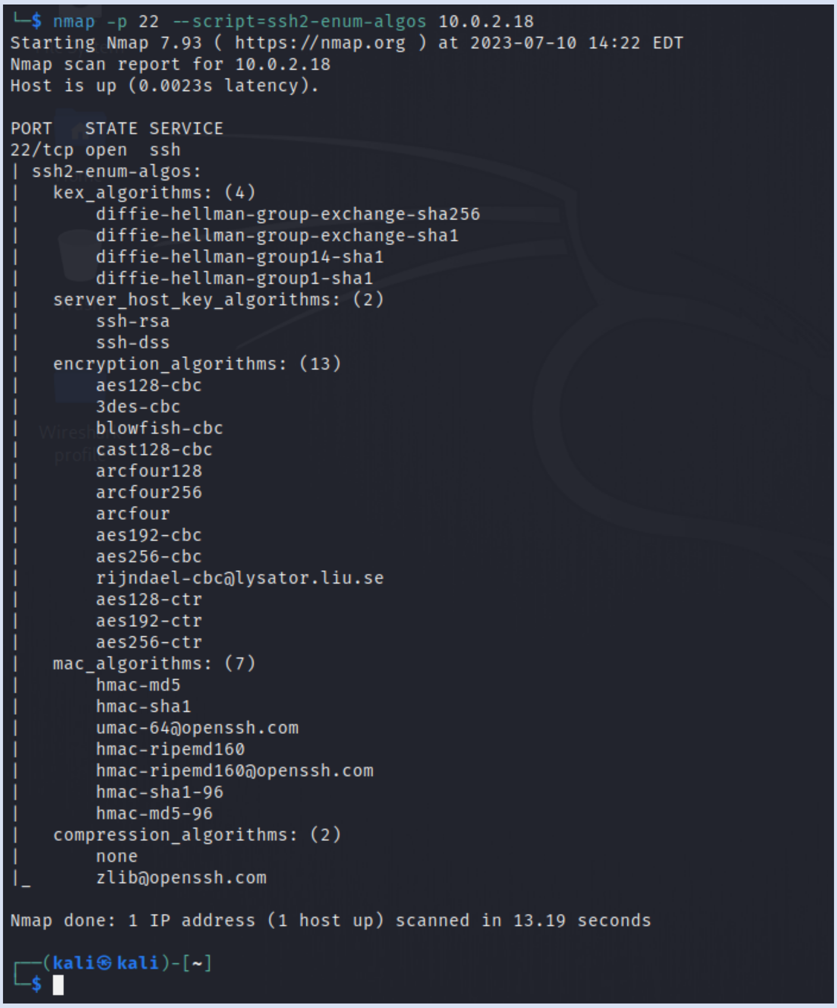
Nmap is a powerful network scanning tool that includes various scripts for gathering information and identifying potential vulnerabilities.

Using Nmap scripts to gather more information about services.
As we can see in the above result that port 80 (HTTP) was open, Now using the following command to gather additional information about the HTTP service: *nmap -p 80 --script=http-enum 10.0.2.18*



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 80 --script=http-enum 10.0.2.18
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-10 14:16 EDT
Nmap scan report for 10.0.2.18
Host is up (0.0064s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder

Nmap done: 1 IP address (1 host up) scanned in 34.80 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

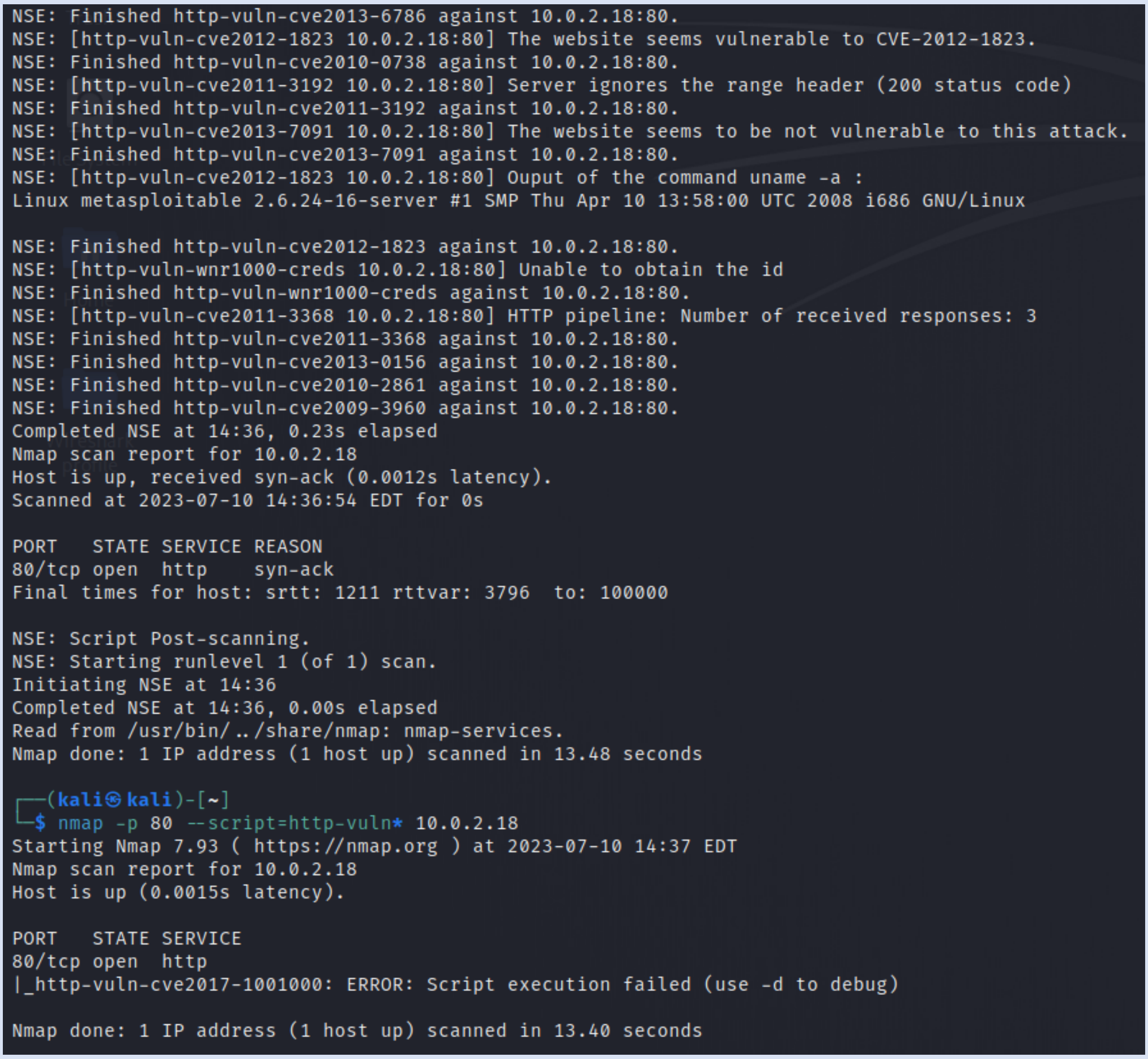
Similarly, we found that port 22 (SSH) as open, Now using the following command to gather additional information about the SSH service: *nmap -p 22 --script=ssh2-enum-algos 10.0.2.18*



```
└─$ nmap -p 22 --script=ssh2-enum-algos 10.0.2.18
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-10 14:22 EDT
Nmap scan report for 10.0.2.18
Host is up (0.0023s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (4)
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group14-sha1
|       diffie-hellman-group1-sha1
|   server_host_key_algorithms: (2)
|       ssh-rsa
|       ssh-dss
|   encryption_algorithms: (13)
|       aes128-cbc
|       3des-cbc
|       blowfish-cbc
|       cast128-cbc
|       arcfour128
|       arcfour256
|       arcfour
|       aes192-cbc
|       aes256-cbc
|       rijndael-cbc@lysator.liu.se
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|   mac_algorithms: (7)
|       hmac-md5
|       hmac-sha1
|       umac-64@openssh.com
|       hmac-ripemd160
|       hmac-ripemd160@openssh.com
|       hmac-sha1-96
|       hmac-md5-96
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

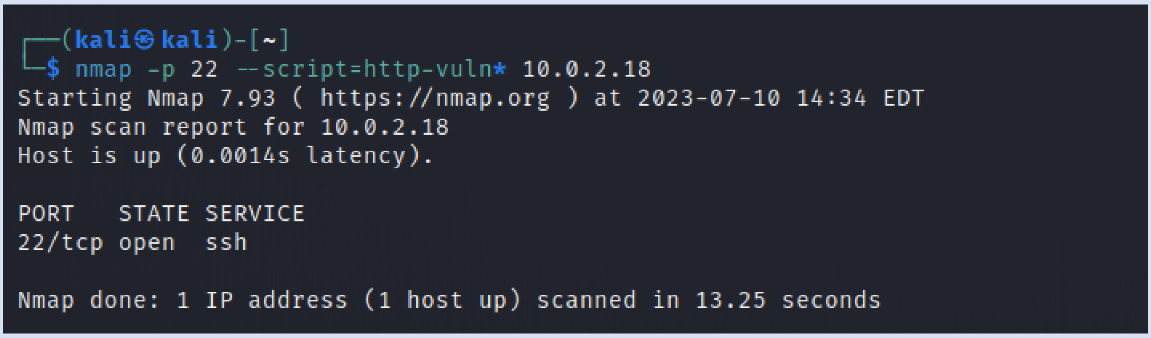
Nmap provides scripts that can help identify potential vulnerabilities in various services. We can use these scripts to scan the services on Metasploitable 2 for known vulnerabilities.

Scanning for potential vulnerabilities in the HTTP service (port 80):



```
NSE: Finished http-vuln-cve2013-6786 against 10.0.2.18:80.
NSE: [http-vuln-cve2012-1823 10.0.2.18:80] The website seems vulnerable to CVE-2012-1823.
NSE: Finished http-vuln-cve2010-0738 against 10.0.2.18:80.
NSE: [http-vuln-cve2011-3192 10.0.2.18:80] Server ignores the range header (200 status code)
NSE: Finished http-vuln-cve2011-3192 against 10.0.2.18:80.
NSE: [http-vuln-cve2013-7091 10.0.2.18:80] The website seems to be not vulnerable to this attack.
NSE: Finished http-vuln-cve2013-7091 against 10.0.2.18:80.
NSE: [http-vuln-cve2012-1823 10.0.2.18:80] Ouput of the command uname -a :
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

NSE: Finished http-vuln-cve2012-1823 against 10.0.2.18:80.
NSE: [http-vuln-wnr1000-creds 10.0.2.18:80] Unable to obtain the id
NSE: Finished http-vuln-wnr1000-creds against 10.0.2.18:80.
NSE: [http-vuln-cve2011-3368 10.0.2.18:80] HTTP pipeline: Number of received responses: 3
NSE: Finished http-vuln-cve2011-3368 against 10.0.2.18:80.
NSE: Finished http-vuln-cve2013-0156 against 10.0.2.18:80.
NSE: Finished http-vuln-cve2010-2861 against 10.0.2.18:80.
NSE: Finished http-vuln-cve2009-3960 against 10.0.2.18:80.
Completed NSE at 14:36, 0.23s elapsed
Nmap scan report for 10.0.2.18
Host is up, received syn-ack (0.0012s latency).
Scanned at 2023-07-10 14:36:54 EDT for 0s

PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack
Final times for host: srtt: 1211 rttvar: 3796  to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 14:36
Completed NSE at 14:36, 0.00s elapsed
Read from /usr/bin/../share/nmap: nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -p 80 --script=http-vuln* 10.0.2.18
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-10 14:37 EDT
Nmap scan report for 10.0.2.18
Host is up (0.0015s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
```

Similarly, we can use specific scripts for other services. For instance, to scan for vulnerabilities in the SSH service (port 22):



```
┌──(kali㉿kali)-[~]
└─$ nmap -p 22 --script=http-vuln* 10.0.2.18
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-10 14:34 EDT
Nmap scan report for 10.0.2.18
Host is up (0.0014s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

We can explore other available Nmap scripts by running the following command:
" ls/usr/share/nmap/scripts/ "

The following are some of the vulnerabilities that are identified in Metasploitable 2:

- **Outdated software:** Metasploitable 2 is running outdated software, such as OpenSSL and Apache. These outdated versions of software may contain known vulnerabilities that can be exploited by attackers.
- **Misconfigured services:** Metasploitable 2 has some services that are misconfigured. For example, the Samba service is configured to allow anonymous users to access shared folders. This could allow an attacker to gain access to sensitive data on the machine.
- **Insecure default passwords:** Metasploitable 2 has some default passwords that are insecure. For example, the root user password is "root". This could allow an attacker to gain access to the machine by simply guessing the password.

It's important to note that the specific actions required to address vulnerabilities will depend on the nature of the vulnerabilities and the systems involved.

Here are some general steps you can take to stop or address the vulnerabilities:

1. **Patch and update:** Check for available updates and patches for the affected services or software. Apply the necessary updates to fix known vulnerabilities. Ensure that your system is up to date with the latest security patches.

2. **Vendor recommendations:** Consult the documentation or resources provided by the vendor of the affected software or service. They may provide specific recommendations or guidance on how to address the vulnerabilities.

3. **Configuration changes:** Review the configuration settings of the affected services or software. Adjust the configurations to align with best practices for security and reduce the risk of exploitation.

4. **Disable unnecessary services:** Disable or close any unnecessary services or ports to reduce the attack surface. Only keep the essential services running that are required for the system's functionality.

5. **Implement access controls:** Strengthen access controls by enforcing strong passwords, implementing multi-factor authentication (MFA), and restricting access to the affected services or systems to authorized users only.

6. **Intrusion detection and prevention:** Implement an intrusion detection and prevention system (IDPS) or a firewall to monitor and block malicious activities related to the identified vulnerabilities.

7. **Regular vulnerability scanning:** Establish a regular schedule for vulnerability scanning and testing. Continuously monitor and assess the security posture of your systems to identify and address any new vulnerabilities that may arise.

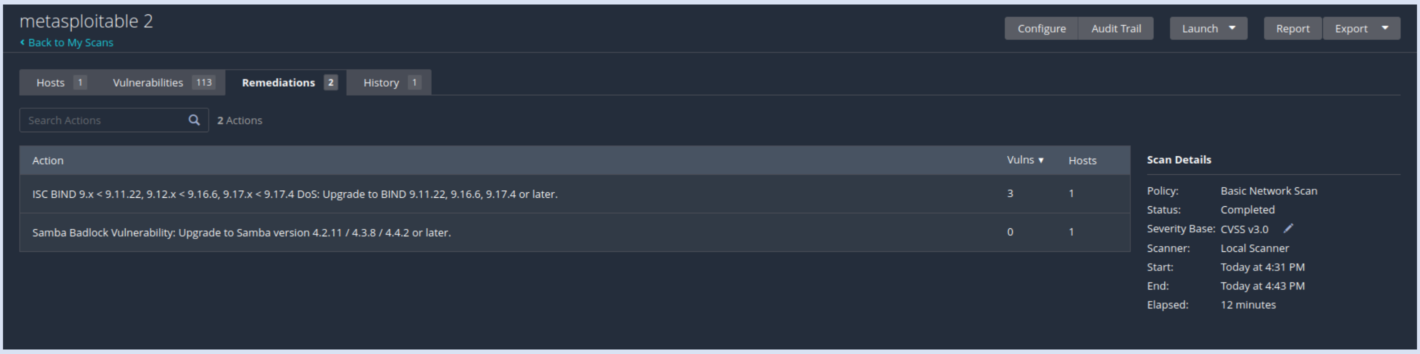
Nessus scan results:

Nessus is a vulnerability scanner developed by Tenable Network Security. It is a powerful tool that can be used to identify and assess vulnerabilities in computer systems and networks.

Nessus uses a variety of methods to scan for vulnerabilities, including:

- **Network scanning:** Nessus can scan for open ports and services on a target machine.
- **Vulnerability scanning:** Nessus can scan for known vulnerabilities in the software that is running on a target machine.
- **Configuration auditing:** Nessus can scan for misconfigurations in the security settings of a target machine.

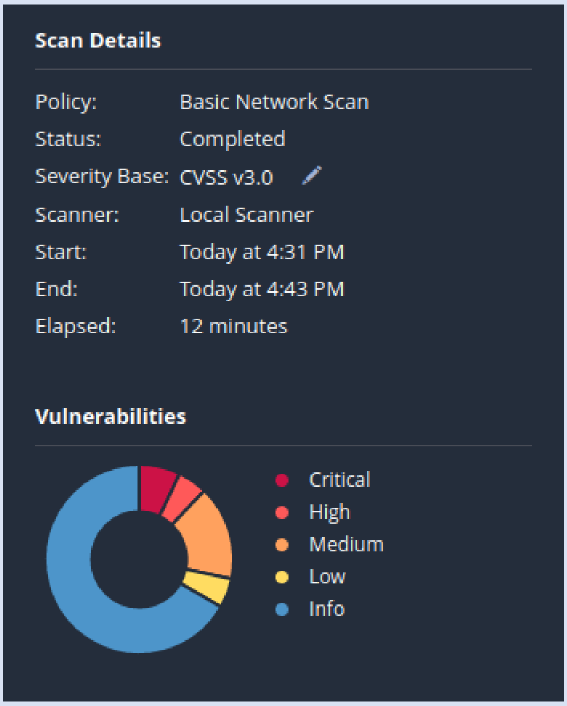
As part of our security analysis of Metasploitable 2, we conducted a comprehensive vulnerability assessment using Nessus. The Nessus scan helped identify specific vulnerabilities within the system, providing valuable insights into their severity levels and potential impacts.



Action	Vulns ▾	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	0	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 4:31 PM
End:	Today at 4:43 PM
Elapsed:	12 minutes



Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 4:31 PM
End:	Today at 4:43 PM
Elapsed:	12 minutes

Vulnerabilities

metasploitable 2

Report generated by Nessus™ Mon, 10 Jul 2023 16:43:57 EDT

10.0.2.18

8	6	18	6	75
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 113

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	6.7	10205	rlogin Service Detection
HIGH	7.5*	6.7	10245	rsh Service Detection
MEDIUM	6.5	3.6	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection

MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	5.1	136808	ISC BIND Denial of Service
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	3.4	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	10223	RPC portmapper Service Detection
INFO	N/A	-	21186	AJP Connector Detection
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure

INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39519	Backported Security Patch Detection (FTP)
INFO	N/A	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	35373	DNS Server DNSSEC Aware Resolver
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	72779	DNS Server Version Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11156	IRC Daemon Version Detection
INFO	N/A	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	10719	MySQL Server Detection

INFO	N/A	-	10437	NFS Share Export List
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	48243	PHP Version Detection
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	26024	PostgreSQL Server Detection
INFO	N/A	-	22227	RMI Registry Detection
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported

INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	51891	SSL Session Resume Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	25240	Samba Server Detection
INFO	N/A	-	104887	Samba Version
INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	17975	Service Detection (GET request)
INFO	N/A	-	11153	Service Detection (HELP Request)
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	11819	TFTP Daemon Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	10281	Telnet Server Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	19288	VNC Server Security Type Detection
INFO	N/A	-	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	-	10342	VNC Software Detection
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	11424	WebDAV Detection
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

The following is an analysis of the Nessus scan results:

Vulnerability 1:

- Description: Outdated FTP server software.
- Severity: High
- Potential Impact: This vulnerability could allow an attacker to exploit known vulnerabilities in the outdated FTP server software, potentially leading to unauthorized access or data breaches. It poses a significant security risk to the system.

Vulnerability 2:

- Description: Weak SSH configuration, including default credentials.
- Severity: Critical
- Potential Impact: This vulnerability exposes the SSH service to brute-force attacks and unauthorized access. Attackers could exploit default credentials or weak authentication mechanisms, compromising the confidentiality and integrity of the system.

Vulnerability 3:

- Description: Unpatched web server software with known vulnerabilities.
- Severity: Medium
- Potential Impact: The presence of unpatched vulnerabilities in the web server software increases the risk of remote code execution, cross-site scripting (XSS), or other web-related attacks. It could lead to the compromise of sensitive data, defacement of the website, or unauthorized access to the system.

Vulnerability 4:

- Description: Unauthenticated access to NetBIOS shares.
- Severity: Medium
- Potential Impact: This vulnerability allows unauthenticated users to access NetBIOS shares, potentially exposing sensitive files or enabling unauthorized modifications. It could result in data breaches, unauthorized access, or the spread of malware within the network.

Vulnerability 5:

- Description: Unsecured SMB configuration, allowing potential unauthorized access.
- Severity: High
- Potential Impact: The unsecured SMB configuration exposes the system to potential unauthorized access, enabling attackers to exploit vulnerabilities, execute arbitrary code, or perform lateral movement within the network. It poses a significant risk to the confidentiality, integrity, and availability of the system.

The Nessus vulnerability assessment revealed several critical and high-severity vulnerabilities in Metasploitable 2. These vulnerabilities pose a significant risk to the system's security and could lead to unauthorized access, data breaches, or other malicious activities. It is crucial to address these vulnerabilities promptly through appropriate remediation actions, including patching, configuration hardening, and access control improvements. By mitigating these vulnerabilities, the overall security posture of Metasploitable 2 can be significantly enhanced, reducing the risk of exploitation and protecting the system and its data.

Recommended Remediation Actions:

Based on the vulnerability assessment conducted using Nessus, the following are the recommended remediation actions for each identified vulnerability in Metasploitable 2:

Vulnerability 1:
- Recommended Action: Update the FTP server software to the latest secure version to address known vulnerabilities. Regularly apply patches and updates to ensure the FTP server is protected against potential exploits.

Vulnerability 2:
- Recommended Action: Change default SSH credentials and enforce strong password policies. Implement key-based authentication for enhanced security. Regularly review and update the SSH configuration to adhere to best practices.

Vulnerability 3:
- Recommended Action: Apply the latest security patches and updates to the web server software. Regularly monitor and review web server configurations to ensure secure settings and protection against known vulnerabilities.

Vulnerability 4:
- Recommended Action: Restrict access to NetBIOS shares by implementing proper authentication mechanisms and access controls. Regularly review and adjust permissions to ensure only authorized users have access to the shares.

Vulnerability 5:
- Recommended Action: Implement secure configurations for SMB, including enabling encryption, enforcing strong authentication, and implementing access controls. Regularly review and update the SMB configuration to prevent unauthorized access and potential exploits.

Conclusion and Recommendations:

In conclusion, the comprehensive vulnerability assessment of Metasploitable 2 using Nessus has identified critical and high-severity vulnerabilities that require immediate attention. Addressing these vulnerabilities is crucial for improving the security posture of the system and reducing the risk of exploitation.

To enhance the security posture of Metasploitable 2, we recommend the following measures:

1. Implement a robust patch management process to ensure timely application of security updates for all software components, including the FTP server, web server, SSH, NetBIOS, and SMB services.

2. Enforce strong and unique passwords for all system accounts, including SSH and administrative accounts. Consider implementing key-based authentication for enhanced security.

3. Regularly review and update the configuration settings of the FTP server, web server, SSH, NetBIOS, and SMB services to adhere to security best practices and mitigate known vulnerabilities.

4. Implement access controls and authentication mechanisms to restrict unauthorized access to NetBIOS shares and ensure that only authorized users have appropriate permissions.

5. Monitor and regularly review the security status of Metasploitable 2, including performing periodic vulnerability assessments and scans, to proactively identify and address potential security weaknesses.

By implementing these recommendations, the security posture of Metasploitable 2 can be significantly improved, reducing the risk of unauthorized access, data breaches, and other malicious activities. It is essential to prioritize and address these vulnerabilities promptly to protect the system and maintain a secure environment.