Minor Project 2

Company: Senselearner Technologies Pvt. Ltd.
Group Name: Hosta
Submitted by: Darshan Patel (Member)

Overview:

Metasploitable 2 is a deliberately vulnerable virtual machine (VM) created for security testing and educational purposes. It is designed to simulate various security vulnerabilities and misconfigurations, allowing users to practice and learn about penetration testing techniques. This report provides an installation of Metasploitable 2 in virtual machine to setup and analyze security posture of the system, using Nessus and Nmap to perform vulnerability assessment. The report also outlines identified vulnerabilities, their severity levels, and potential remediation actions to mitigate the risk and recommendations for improving the overall security posture of Metasploitable 2.

Metasploitable 2:

The installation process of Metasploitable 2 involves the following steps:

1. Download the Metasploitable 2 VM: Metasploitable 2 can be downloaded as a pre-configured virtual machine image from various reliable sources. It is available in different formats such as VMware, VirtualBox, and other popular VM platforms.

2. Set up a virtualization platform: Before installing Metasploitable 2, we need to have a virtualization platform installed on your host machine. Popular virtualization platforms include VMware Workstation, VirtualBox, and VMware Fusion.

3. Import the Metasploitable 2 VM: Once we have set up virtualization platform, import the downloaded Metasploitable 2 VM image into the platform. This process may vary depending on the virtualization software we are using, but it usually involves selecting the downloaded VM image file and importing it into the platform.

4. Configure the VM settings: After importing the VM image, we may need to configure the VM settings according to our system resources. Adjust settings such as CPU, memory, and network configurations based on our hardware capabilities and requirements.

5. Start the Metasploitable 2 VM: Once the VM is imported and configured, start the Metasploitable 2 VM within our virtualization platform. The VM will boot up and present with a login prompt.

Network configuration:

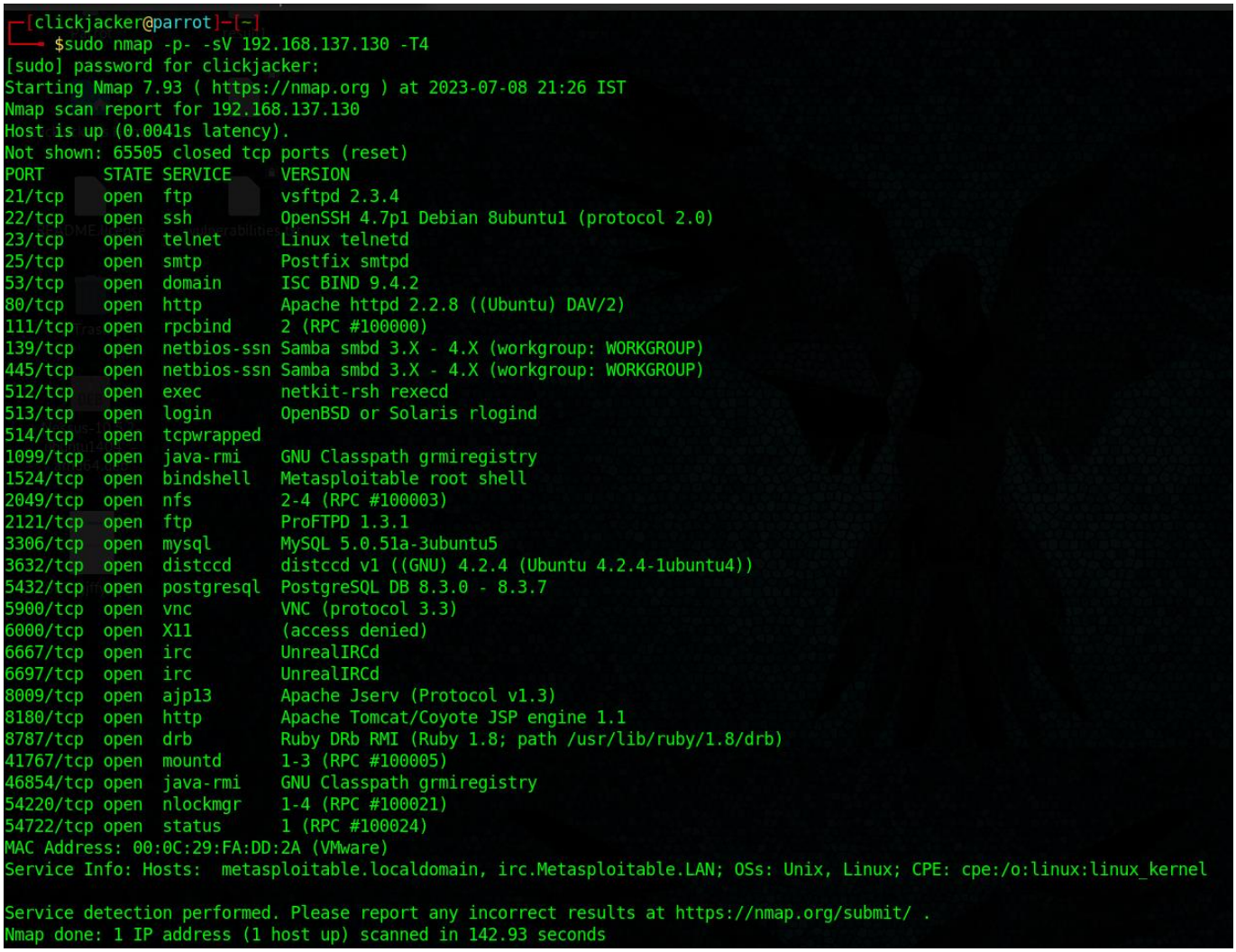
Metasploitable 2 is configured with a default network setup to allow easy access for testing and exploitation. By default, it uses a NAT (Network Address Translation) network configuration, which enables the VM to access the internet and allows inbound connections from the host machine or other VMs within the same virtual network.

When the Metasploitable 2 VM boots up, it typically obtains an IP address automatically from the virtualization platform's DHCP server. The IP address assigned to the VM may vary depending on our network setup.

To access the Metasploitable 2 VM from the host machine or other machines on the same network, we can use the IP address assigned to the VM. We may need to configure port forwarding or network settings within your virtualization platform to enable inbound connections to the Metasploitable 2 VM.

It's important to note that Metasploitable 2 is intentionally vulnerable and should only be used in controlled environments for educational or security testing purposes. It should not be deployed in production networks or connected to the internet without appropriate security precautions.

NMAP scan results, highlighting open ports and services.



NMAP using NSE (Script used is Vulner)

Nmap 7.93 scan initiated Fri Jul 8 18:35:05 2023 as: nmap -p- -sV --script vulners -oN vulnerabilities.txt 192.168.137.130

Nmap scan report for 192.168.137.130

Host is up (0.0028s latency).

Not shown: 65505 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

| vulners:

| cpe:/a: openbsd: openssh:4.7p1:

| SECURITYVULNS: VULN:8166 7.5
https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166

| CVE-2010-4478 7.5 https://vulners.com/cve/CVE-2010-4478

| CVE-2008-1657 6.5 https://vulners.com/cve/CVE-2008-1657

| SSV:60656 5.0 https://vulners.com/seebug/SSV:60656 *EXPLOIT*

| CVE-2010-5107 5.0 https://vulners.com/cve/CVE-2010-5107

53/tcp open domain ISC BIND 9.4.2

| vulners:

| cpe:/a: isc: bind:9.4.2:

| SSV:60184 8.5 https://vulners.com/seebug/SSV:60184 *EXPLOIT*

| CVE-2012-1667 8.5 https://vulners.com/cve/CVE-2012-1667

| SSV:60292 7.8 https://vulners.com/seebug/SSV:60292 *EXPLOIT*

| CVE-2014-8500 7.8 https://vulners.com/cve/CVE-2014-8500

| CVE-2012-5166 7.8 https://vulners.com/cve/CVE-2012-5166

| CVE-2012-4244 7.8 https://vulners.com/cve/CVE-2012-4244

| CVE-2012-3817 7.8 https://vulners.com/cve/CVE-2012-3817

| CVE-2008-4163 7.8 https://vulners.com/cve/CVE-2008-4163

| CVE-2010-0382 7.6 https://vulners.com/cve/CVE-2010-0382

80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

| vulners:

| cpe:/a: apache: http_server:2.2.8:

| SSV:72403 7.8 https://vulners.com/seebug/SSV:72403 *EXPLOIT*

| SSV:26043 7.8 https://vulners.com/seebug/SSV:26043 *EXPLOIT*

| SSV:20899 7.8 https://vulners.com/seebug/SSV:20899 *EXPLOIT*

| PACKETSTORM:126851 7.8 https://vulners.com/packetstorm/PACKETSTORM:126851 *EXPLOIT*

| PACKETSTORM:123527 7.8 https://vulners.com/packetstorm/PACKETSTORM:123527 *EXPLOIT*

| PACKETSTORM:122962 7.8 https://vulners.com/packetstorm/PACKETSTORM:122962 *EXPLOIT*

| EXPLOITPACK:186B5FCF5C57B52642E62C06BABC6F83 7.8 https://vulners.com/exploitpack/EXPLOITPACK:186B5FCF5C57B52642E62C06BABC6F83 *EXPLOIT*

| EDB-ID:18221 7.8 https://vulners.com/exploitdb/EDB-ID:18221 *EXPLOIT*

| CVE-2011-3192 7.8 https://vulners.com/cve/CVE-2011-3192

| 1337DAY-ID-21170 7.8 https://vulners.com/zdt/1337DAY-ID-21170 *EXPLOIT*

| SSV:12673 7.5 https://vulners.com/seebug/SSV:12673 *EXPLOIT*

| SSV:12626 7.5 https://vulners.com/seebug/SSV:12626 *EXPLOIT*

| ECC3E825-EE29-59D3-BE28-1B30DB15940E 7.5
https://vulners.com/githubexploit/ECC3E825-EE29-59D3-BE28-1B30DB15940E *EXPLOIT*

| CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679

| CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167

| SSV:11802 7.1 https://vulners.com/seebug/SSV:11802 *EXPLOIT*

| SSV:11762 7.1 https://vulners.com/seebug/SSV:11762 *EXPLOIT*

| CVE-2009-1891 7.1 https://vulners.com/cve/CVE-2009-1891

| CVE-2009-1890 7.1 https://vulners.com/cve/CVE-2009-1890

2121/tcp open ftp ProFTPD 1.3.1

| vulners:

| cpe:/a: proftpd: proftpd:1.3.1:

| SAINT: FD1752E124A72FD3A26EEB9B315E8382 10.0
https://vulners.com/saint/SAINT:FD1752E124A72FD3A26EEB9B315E8382 *EXPLOIT*

| SAINT:950EB68D408A40399926A4CCAD3CC62E 10.0
https://vulners.com/saint/SAINT:950EB68D408A40399926A4CCAD3CC62E *EXPLOIT*

| SAINT:63FB77B9136D48259E4F0D4CDA35E957 10.0
https://vulners.com/saint/SAINT:63FB77B9136D48259E4F0D4CDA35E957 *EXPLOIT*

| SAINT:1B08F4664C428B180EEC9617B41D9A2C 10.0
https://vulners.com/saint/SAINT:1B08F4664C428B180EEC9617B41D9A2C *EXPLOIT*

| PROFTPD_MOD_COPY 10.0 https://vulners.com/canvas/PROFTPD_MOD_COPY
EXPLOIT

| PACKETSTORM:162777 10.0 https://vulners.com/packetstorm/PACKETSTORM:162777
EXPLOIT

| PACKETSTORM:132218 10.0 https://vulners.com/packetstorm/PACKETSTORM:132218
EXPLOIT

| PACKETSTORM:131567 10.0 https://vulners.com/packetstorm/PACKETSTORM:131567
EXPLOIT

| PACKETSTORM:131555 10.0 https://vulners.com/packetstorm/PACKETSTORM:131555
EXPLOIT

| PACKETSTORM:131505 10.0 https://vulners.com/packetstorm/PACKETSTORM:131505
EXPLOIT

| EDB-ID:49908 10.0 https://vulners.com/exploitdb/EDB-ID:49908 *EXPLOIT*

| 1337DAY-ID-36298 10.0 https://vulners.com/zdt/1337DAY-ID-36298 *EXPLOIT*

| 1337DAY-ID-23720 10.0 https://vulners.com/zdt/1337DAY-ID-23720 *EXPLOIT*

| 1337DAY-ID-23544 10.0 https://vulners.com/zdt/1337DAY-ID-23544 *EXPLOIT*

| SSV:26016 9.0 https://vulners.com/seebug/SSV:26016 *EXPLOIT*

| SSV:24282 9.0 https://vulners.com/seebug/SSV:24282 *EXPLOIT*

| CVE-2011-4130 9.0 https://vulners.com/cve/CVE-2011-4130

| SSV:96525 7.5 https://vulners.com/seebug/SSV:96525 *EXPLOIT*

| CVE-2019-12815 7.5 https://vulners.com/cve/CVE-2019-12815

|

3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

| vulners:

| cpe:/a: mysql: mysql:5.0.51a-3ubuntu5:

| SSV:19118 8.5 https://vulners.com/seebug/SSV:19118 *EXPLOIT*

| CVE-2009-2446 8.5 https://vulners.com/cve/CVE-2009-2446

| SAINT: D505D53863BE216621FDAECA22896071 7.5
https://vulners.com/saint/SAINT:D505D53863BE216621FDAECA22896071 *EXPLOIT*

| SAINT: A9E0BE0CEF71F1F98D3CB3E95173B3D0 7.5
https://vulners.com/saint/SAINT:A9E0BE0CEF71F1F98D3CB3E95173B3D0 *EXPLOIT*

| SAINT:79BA92A57C28E796ADD04A6A8AE158CE 7.5
https://vulners.com/saint/SAINT:79BA92A57C28E796ADD04A6A8AE158CE *EXPLOIT*

| SAINT:3101D21E4D8017EA5B14AF668DC39CAD 7.5
https://vulners.com/saint/SAINT:3101D21E4D8017EA5B14AF668DC39CAD *EXPLOIT*

| PACKETSTORM:85678 7.5 https://vulners.com/packetstorm/PACKETSTORM:85678
EXPLOIT

| PACKETSTORM:82247 7.5 https://vulners.com/packetstorm/PACKETSTORM:82247
EXPLOIT

| CVE-2008-0226 7.5 https://vulners.com/cve/CVE-2008-0226

| SSV:15006 6.8 https://vulners.com/seebug/SSV:15006 *EXPLOIT*

|

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

| vulners:

| cpe:/a: postgresql: postgresql:8.3:

| SSV:60718 10.0 https://vulners.com/seebug/SSV:60718 *EXPLOIT*

| CVE-2013-1903 10.0 https://vulners.com/cve/CVE-2013-1903

| CVE-2013-1902 10.0 https://vulners.com/cve/CVE-2013-1902

| SSV:30015 8.5 https://vulners.com/seebug/SSV:30015 *EXPLOIT*

| SSV:19652 8.5 https://vulners.com/seebug/SSV:19652 *EXPLOIT*

| POSTGRESQL: CVE-2013-1900 8.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2013-1900

| POSTGRESQL: CVE-2010-1169 8.5 https://vulners.com/postgresql/POSTGRESQL:CVE-2010-1169

| CVE-2010-1447 8.5 https://vulners.com/cve/CVE-2010-1447

| CVE-2010-1169 8.5 https://vulners.com/cve/CVE-2010-1169

| SSV:19754 7.5 https://vulners.com/seebug/SSV:19754 *EXPLOIT*

| SSV:30152 6.8 https://vulners.com/seebug/SSV:30152 *EXPLOIT*

|

MAC Address: 00:0C:29: FA:DD:2A (VMware)

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 at Fri Jul 8 18:37:23 2023 -- 1 IP address (1 host up) scanned in 137.57 seconds

NESSUS Vulnerability findings:

192.168.137.130

12	6	20	5	79
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 122

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	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
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*	7.4	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
CRITICAL	10.0*	6.7	10203	rexecd Service Detection
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	6.8	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
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	-	12085	Apache Tomcat Default Files
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	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	-	39446	Apache Tomcat Detection
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	-	20094	VMware Virtual Machine Detection
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	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	11422	Web Server Unconfigured - Default Install Page Present
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

Remediations:

Critical

1. Apache Tomcat AJP Connector Request Injection (Ghostcat)
   - Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

2. Bind Shell Backdoor Detection
   - Verify if the remote host has been compromised, and reinstall the system if necessary.

3. SSL Version 2 and 3 Protocol Detection
   - Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

4. Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
   - Contact your DNS server vendor for a patch.

5. Apache Tomcat SEoL (<= 5.5.x)
   - Upgrade to a version of Apache Tomcat that is currently supported.

6. Unix Operating System Unsupported Version Detection
   - Upgrade to a version of the Unix operating system that is currently supported.

7. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
   - Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

8. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
    - Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

9. NFS Exported Share Information Disclosure
    - Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

10. UnrealIRCd Backdoor Detection
    - Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

11. VNC Server 'password' Password
    - Secure the VNC service with a strong password.

12. rexecd Service Detection
    - Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

High

13. ISC BIND Service Downgrade / Reflected DoS
    - Upgrade to the ISC BIND version referenced in the vendor advisory.

14. NFS Shares World Readable
    - Place the appropriate restrictions on all NFS shares.

15. SSL Medium Strength Cipher Suites Supported (SWEET32)
    - Reconfigure the affected application if possible to avoid use of medium strength ciphers.

16. Samba Badlock Vulnerability
    - Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

17. rlogin Service Detection
    - Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

18. rsh Service Detection
    - Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

Medium

19. SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE)
    - Disable SSLv3.

20. 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.

21. SSL Certificate Cannot Be Trusted
    - Purchase or generate a proper SSL certificate for this service.

22. SSL Self-Signed Certificate
    - Purchase or generate a proper SSL certificate for this service.

23. TLS Version 1.0 Protocol Detection
    - Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

24. Unencrypted Telnet Server
    - Disable the Telnet service and use SSH instead.

25. ISC BIND Denial of Service
    - Upgrade to the patched release most closely related to your current version of BIND.

26. SSL Anonymous Cipher Suites Supported
    - Reconfigure the affected application, if possible, to avoid use of weak ciphers.

27. SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened encryption)
    - Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

28. SSL RC4 Cipher Suites Supported (Bar Mitzvah)
    - Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

29. Apache Tomcat Default Files
    - Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

30. DNS Server Cache Snooping Remote Information Disclosure
    - Contact the vendor of the DNS software for a fix.

31. HTTP TRACE / TRACK Methods Allowed
    - Disable these HTTP methods. Refer to the plugin output for more information.

32. SMB Signing not required
    - Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications

(always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

33. SSL Certificate Expiry
    - Purchase or generate a new SSL certificate to replace the existing one.

34. SSL Certificate with Wrong Hostname
    - Purchase or generate a new SSL certificate to replace the existing one.

35. SSL Weak Cipher Suites Supported
    - Reconfigure the affected application, if possible to avoid the use of weak ciphers.

36. SMTP Service STARTTLS Plaintext Command Injection
    - Contact the vendor to see if an update is available.

37. SSH Weak Algorithms Supported
    - Contact the vendor or consult product documentation to remove the weak ciphers.

38. SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
    - Reconfigure the service to remove support for EXPORT_RSA cipher suites.

Low

39. SSH Weak Key Exchange Algorithms Enabled
    - Contact the vendor or consult product documentation to disable the weak algorithms.

40. SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
    - Reconfigure the service to remove support for EXPORT_DHE cipher suites.

41. SSH Server CBC Mode Ciphers Enabled
    - Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

42. SSH Weak MAC Algorithms Enabled
    - Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

43. X Server Detection
    - Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-no listen tcp).

Conclusion and Recommendations:

After assessing the security posture of Metasploitable 2, several conclusions can be drawn regarding its vulnerabilities and weaknesses. To improve its security, the following recommendations are provided:

1. Patch and Update: Metasploitable 2 is intentionally vulnerable and outdated. To enhance its security, the first step is to update and patch all software and operating systems running on the system. This includes the base operating system, web servers, database servers, and any other software components. Keeping software up to date ensures that known vulnerabilities are patched and reduces the risk of exploitation.

2. Vulnerability Management: Implement a robust vulnerability management program to regularly scan and assess the system for vulnerabilities. This includes using vulnerability scanners and penetration testing tools to identify weaknesses and prioritize them based on their severity. Regularly apply security patches and updates to address identified vulnerabilities promptly.

3. Network Segmentation: Isolate Metasploitable 2 from the production network or any other critical systems. By implementing network segmentation, you limit the potential impact of an attack on Metasploitable 2, ensuring that any compromise remains contained within the isolated environment.

4. Access Control and User Permissions: Review and enforce proper access controls and user permissions. Restrict access to only authorized individuals and ensure that each user has the appropriate level of access required for their responsibilities. Implement strong and unique passwords, two-factor authentication, and regularly review and update user accounts and privileges.

5. Disable Unnecessary Services: Identify and disable any unnecessary services or protocols running on Metasploitable 2. Each service or protocol running increases the potential attack surface. By disabling unused services, you reduce the number of potential entry points for attackers.

6. Security Monitoring and Logging: Implement comprehensive logging and monitoring capabilities. Monitor system logs, network traffic, and user activity for signs of suspicious or unauthorized behaviour. This includes implementing an intrusion detection system (IDS) or intrusion prevention system (IPS) to detect and prevent known attack patterns.

7. Regular Backup and Recovery: Perform regular backups of the system and its data. Ensure that the backups are stored securely and can be restored effectively in the event of a compromise or data loss. Regularly test the restoration process to validate its effectiveness.

8. Security Awareness and Training: Conduct security awareness training for all personnel who interact with Metasploitable 2. Educate users on best practices for secure password management, phishing awareness, and safe browsing habits. By promoting a culture of security awareness, you can reduce the risk of successful social engineering attacks.

9. Monitor and Stay Informed: Stay up to date with the latest security vulnerabilities, exploits, and patches related to the software and services used in Metasploitable 2. Regularly monitor security advisories and vendor announcements for critical updates that may affect the system's security.

10. Consider Transitioning to Metasploitable 3: Metasploitable 2 is outdated and may not reflect current real-world vulnerabilities accurately. Consider transitioning to Metasploitable 3, which is a more up-to-date and realistic vulnerable virtual machine. Metasploitable 3 provides a wider range of vulnerabilities and a more accurate representation of modern security risks.

By implementing these recommendations, the security posture of Metasploitable 2 can be significantly improved, reducing the risk of exploitation and providing a safer environment for testing and learning about security vulnerabilities.