Metasploitable3

Penetration Test

Peter Treacy
September 8th 2023

1.0 Executive Summary

Metasploitable3 will be conducted a penetration testing against the security controls within their system environment to provide a practical demonstration of those controls' effectiveness as well as to provide an estimate of their susceptibility to exploitation and/or data breaches. The test was performed for flatiron school, as a testing procedure.

The system contains numerous vulnerabilities, including some very serious security flaws Highly important files would be at risk of being captured if the current system remained as it is now.

1.2 High-Level Test Outcomes

Internal penetration test: Intended to simulate the network-level actions of a malicious actor who gained a foothold within the internal network zone.

Overall, Metaspoitable3 presents a high-risk attack surface with major critical vulnerabilities that allowed complete root access to multiple systems exist within the system.

Root access can be obtained in multiple ways and the testing will show how we gained that low of controls in under a 4 hour period .

Kali Linux (192.168.100.8) was used to conduct the penetration test

Metasploitable3 was discovered at ip address 192.168.100.11 on the NAT Network using Nmap/Netcat/Netstat. From there, port scanning was done

Nmap scan report for 192.168.100.11

Host is up (0.0013s latency).

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

80/tcp open http

445/tcp open microsoft-ds

631/tcp open ipp

3000/tcp closed ppp

3306/tcp open mysql

3500/tcp open rtmp-port

6697/tcp open ircs-u

8080/tcp open http-proxy

8181/tcp closed intermapper

1 -Easy **Password**

Weak credentials (vagrant:vagrant) allowed us to SSH into the machine fairly easily

SSH vagrant@192.168.100.11

we shared key fingerprints, which allowed us to gain a shell into the machine.

2- **FTP** with Metasploit

Seeing that port 21 FTP is open was one chosen method in which to enter the system. The commands would be as follows

Msfconsule (search FTP)

Info exploit/unix/ftp/vsftpd_234_backdoor - set, run

3- **Apache** HTTP Server

The Apache web application running on the system has a remote code execution vulnerability which can be exploited using the Apache mod_cgi Bash Environment Variable Code Injection (Shellshock) module.

The Apache web servers also runs WebDAV allowing unauthenticated file uploads to the /uploads/ directory on the web server. This could be used to get a shell by uploading a malicious PHP file.

First step would be to generate a web shell.

Next, upload it through Apache WebDAV.

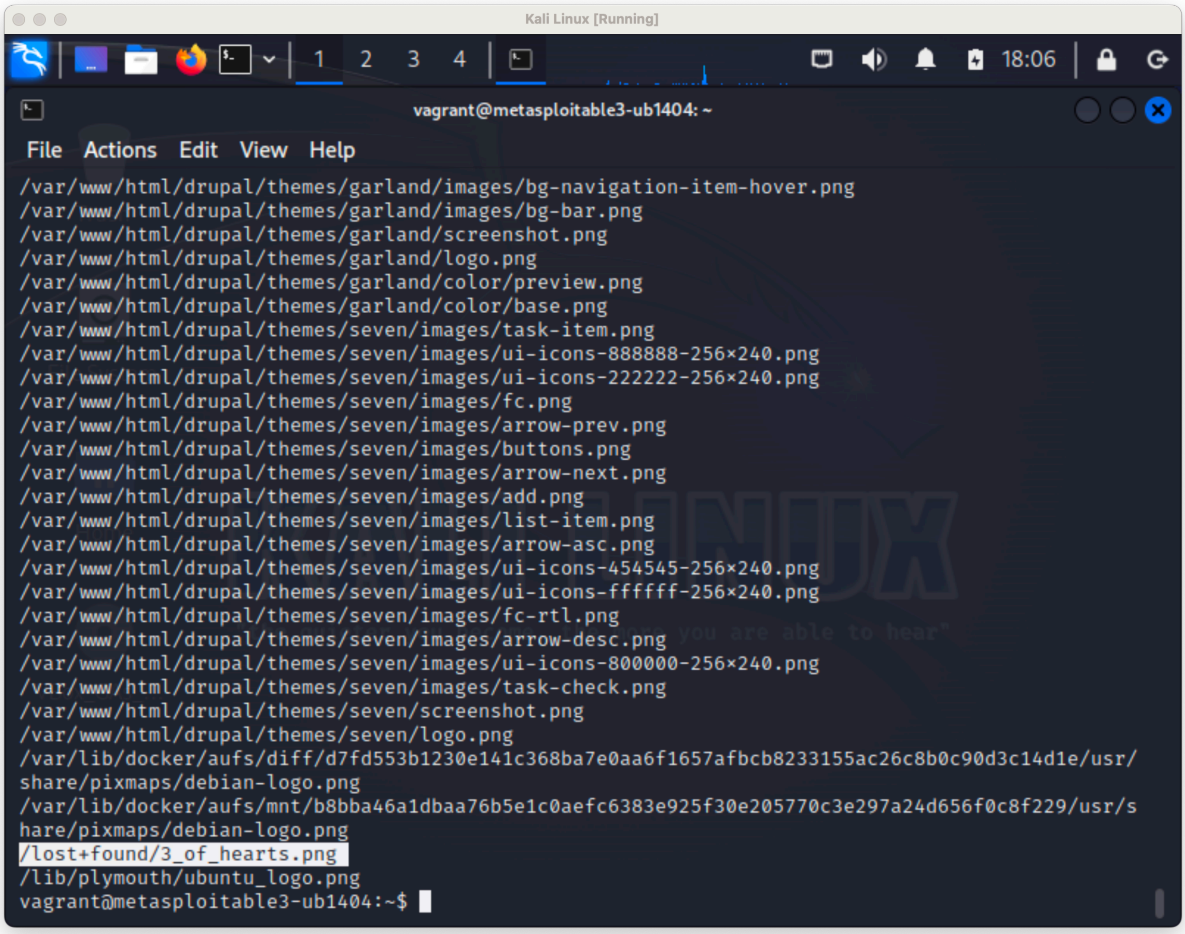
And trigger it by requesting the file through the webserver. Making sure to have a handler running to catch the shell

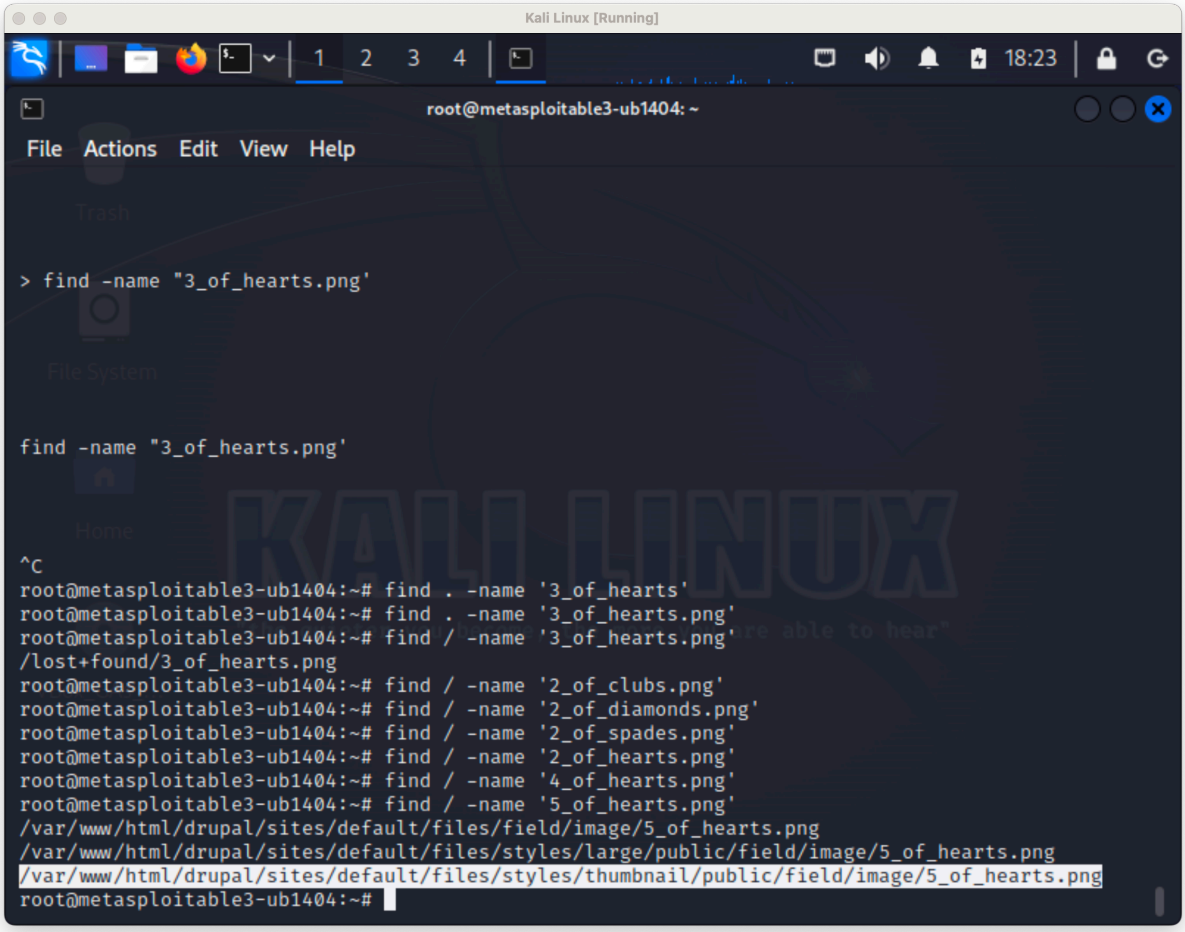
Finding The Cards

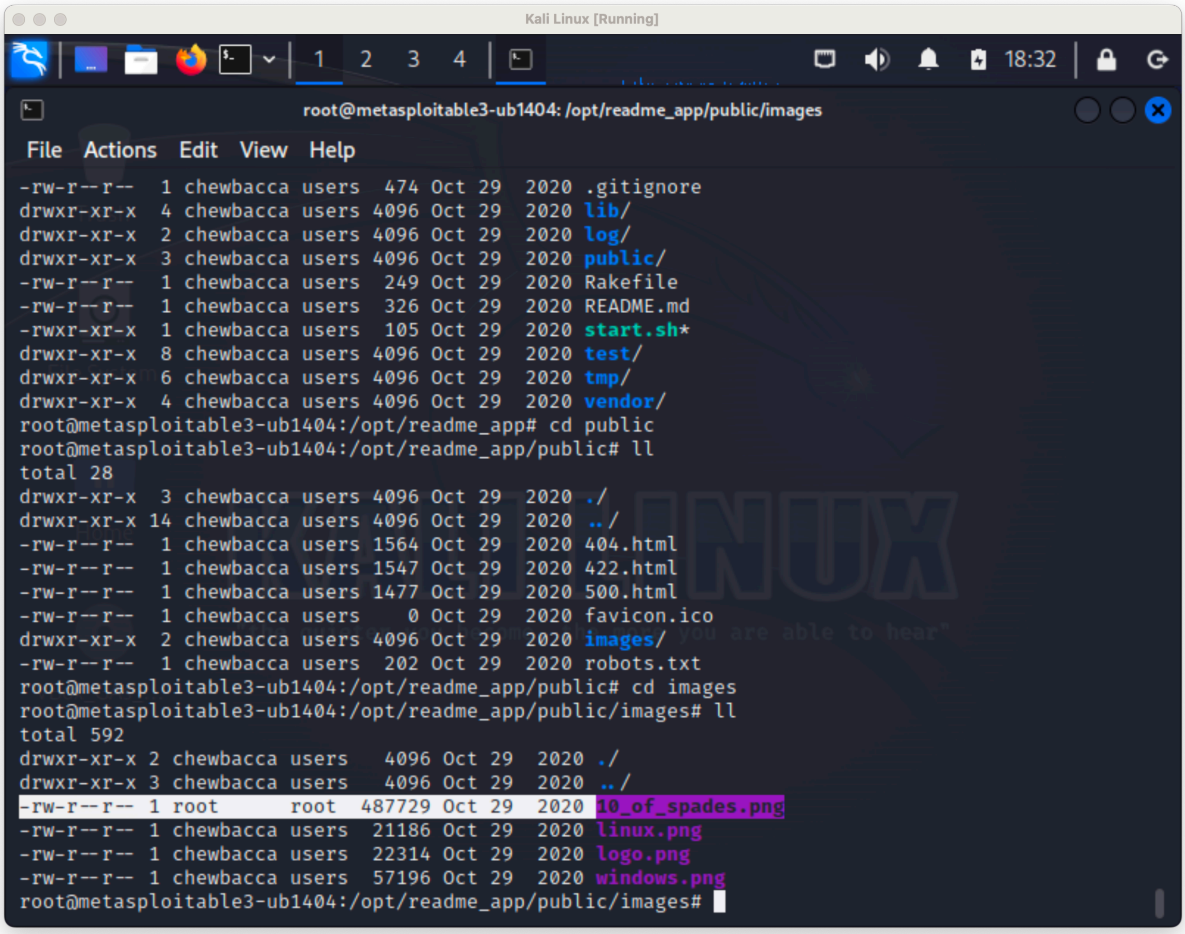
Command-

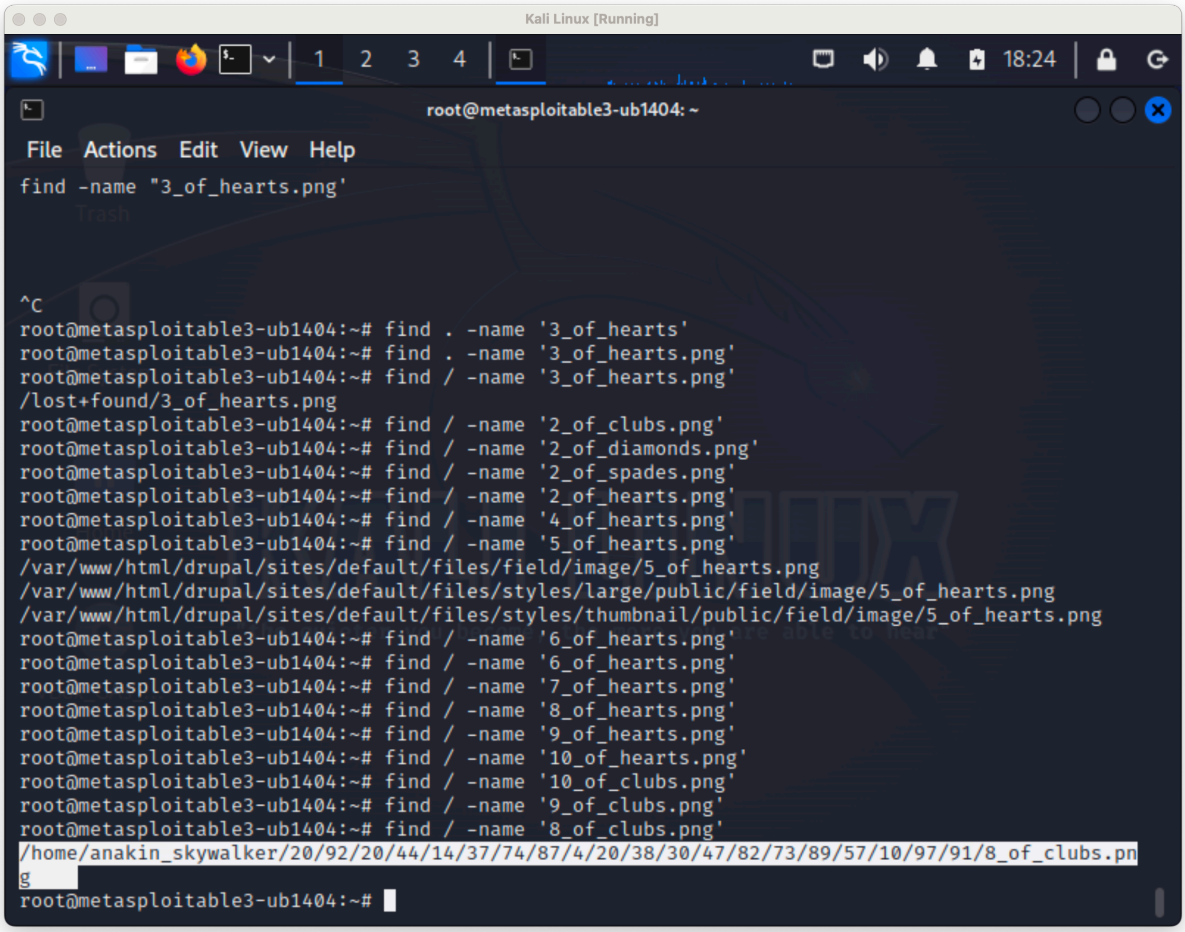
find / -type f -name “spades*”

Dropping into **root**@metasploitable3 and using the ‘find’ command helped the search process for combing through the file directories and 5/13 cards were discovered within 4 hours.




Kali Linux [Running]
1 2 3 4
18:23
root@metasploitable3-ub1404: ~
File Actions Edit View Help
> find -name "3_of_hearts.png'
find -name "3_of_hearts.png'
^C
root@metasploitable3-ub1404:~# find . -name '3_of_hearts'
root@metasploitable3-ub1404:~# find . -name '3_of_hearts.png'
root@metasploitable3-ub1404:~# find / -name '3_of_hearts.png'
/lost+found/3_of_hearts.png
root@metasploitable3-ub1404:~# find / -name '2_of_clubs.png'
root@metasploitable3-ub1404:~# find / -name '2_of_diamonds.png'
root@metasploitable3-ub1404:~# find / -name '2_of_spades.png'
root@metasploitable3-ub1404:~# find / -name '2_of_hearts.png'
root@metasploitable3-ub1404:~# find / -name '4_of_hearts.png'
root@metasploitable3-ub1404:~# find / -name '5_of_hearts.png'
/var/www/html/drupal/sites/default/files/field/image/5_of_hearts.png
/var/www/html/drupal/sites/default/files/styles/large/public/field/image/5_of_hearts.png
/var/www/html/drupal/sites/default/files/styles/thumbnail/public/field/image/5_of_hearts.png
root@metasploitable3-ub1404:~#


Kali Linux [Running]
1 2 3 4
18:32
root@metasploitable3-ub1404: /opt/readme_app/public/images
File Actions Edit View Help
-rw-r--r-- 1 chewbacca users 474 Oct 29 2020 .gitignore
drwxr-xr-x 4 chewbacca users 4096 Oct 29 2020 lib/
drwxr-xr-x 2 chewbacca users 4096 Oct 29 2020 log/
drwxr-xr-x 3 chewbacca users 4096 Oct 29 2020 public/
-rw-r--r-- 1 chewbacca users 249 Oct 29 2020 Rakefile
-rw-r--r-- 1 chewbacca users 326 Oct 29 2020 README.md
-rwxr-xr-x 1 chewbacca users 105 Oct 29 2020 start.sh*
drwxr-xr-x 8 chewbacca users 4096 Oct 29 2020 test/
drwxr-xr-x 6 chewbacca users 4096 Oct 29 2020 tmp/
drwxr-xr-x 4 chewbacca users 4096 Oct 29 2020 vendor/
root@metasploitable3-ub1404:/opt/readme_app# cd public
root@metasploitable3-ub1404:/opt/readme_app/public# ll
total 28
drwxr-xr-x 3 chewbacca users 4096 Oct 29 2020 ./
drwxr-xr-x 14 chewbacca users 4096 Oct 29 2020 ../
-rw-r--r-- 1 chewbacca users 1564 Oct 29 2020 404.html
-rw-r--r-- 1 chewbacca users 1547 Oct 29 2020 422.html
-rw-r--r-- 1 chewbacca users 1477 Oct 29 2020 500.html
-rw-r--r-- 1 chewbacca users 0 Oct 29 2020 favicon.ico
drwxr-xr-x 2 chewbacca users 4096 Oct 29 2020 images/
-rw-r--r-- 1 chewbacca users 202 Oct 29 2020 robots.txt
root@metasploitable3-ub1404:/opt/readme_app/public# cd images
root@metasploitable3-ub1404:/opt/readme_app/public/images# ll
total 592
drwxr-xr-x 2 chewbacca users 4096 Oct 29 2020 ./
drwxr-xr-x 3 chewbacca users 4096 Oct 29 2020 ../
-rw-r--r-- 1 root root 487729 Oct 29 2020 10_of_spades.png
-rw-r--r-- 1 chewbacca users 21186 Oct 29 2020 linux.png
-rw-r--r-- 1 chewbacca users 22314 Oct 29 2020 logo.png
-rw-r--r-- 1 chewbacca users 57196 Oct 29 2020 windows.png
root@metasploitable3-ub1404:/opt/readme_app/public/images#


Kali Linux [Running]
1 2 3 4
18:24
root@metasploitable3-ub1404: ~
File Actions Edit View Help
find -name "3_of_hearts.png'
^C
root@metasploitable3-ub1404:~# find . -name '3_of_hearts'
root@metasploitable3-ub1404:~# find . -name '3_of_hearts.png'
root@metasploitable3-ub1404:~# find / -name '3_of_hearts.png'
/lost+found/3_of_hearts.png
root@metasploitable3-ub1404:~# find / -name '2_of_clubs.png'
root@metasploitable3-ub1404:~# find / -name '2_of_diamonds.png'
root@metasploitable3-ub1404:~# find / -name '2_of_spades.png'
root@metasploitable3-ub1404:~# find / -name '2_of_hearts.png'
root@metasploitable3-ub1404:~# find / -name '4_of_hearts.png'
root@metasploitable3-ub1404:~# find / -name '5_of_hearts.png'
/var/www/html/drupal/sites/default/files/field/image/5_of_hearts.png
/var/www/html/drupal/sites/default/files/styles/large/public/field/image/5_of_hearts.png
/var/www/html/drupal/sites/default/files/styles/thumbnail/public/field/image/5_of_hearts.png
root@metasploitable3-ub1404:~# find / -name '6_of_hearts.png'
root@metasploitable3-ub1404:~# find / -name '6_of_hearts.png'
root@metasploitable3-ub1404:~# find / -name '7_of_hearts.png'
root@metasploitable3-ub1404:~# find / -name '8_of_hearts.png'
root@metasploitable3-ub1404:~# find / -name '9_of_hearts.png'
root@metasploitable3-ub1404:~# find / -name '10_of_hearts.png'
root@metasploitable3-ub1404:~# find / -name '10_of_clubs.png'
root@metasploitable3-ub1404:~# find / -name '9_of_clubs.png'
root@metasploitable3-ub1404:~# find / -name '8_of_clubs.png'
/home/anakin_skywalker/20/92/20/44/14/37/74/87/4/20/38/30/47/82/73/89/57/10/97/91/8_of_clubs.png
root@metasploitable3-ub1404:~#