PSP0201 Week 4 Writeup

GROUP NAME:GLHF

ID	NAME	ROLE
1211103400	Rohit	Leader
1211103299	Shuuban Subramaniam	Member

Day 11 - The rogue Gnome
Tools Used:linux

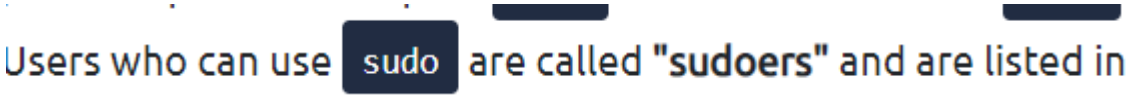
Question 1

> 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.
>
> Remember the attack you performed on "*Day 1 - A Christmas Crisis*"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only accessible by Santa (an administrator), so you are moving your permissions upwards in this sense.

Question 2

> 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.

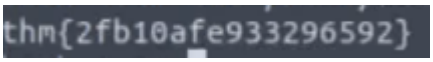
Question 4



Question 6

Question 7

Question 8

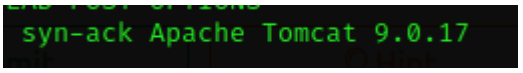


Thoughts:

We first accessed the machine using ssh cmnatic ip address.then we copied the linenum script from github and pasted in linenum.sh file and we ran python3 http.server and downloaded the linenum file using wget command and we are root.

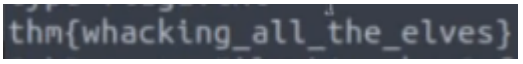
Day 12 - READY,SET,ELF
Tools Used: Linux

Question 1

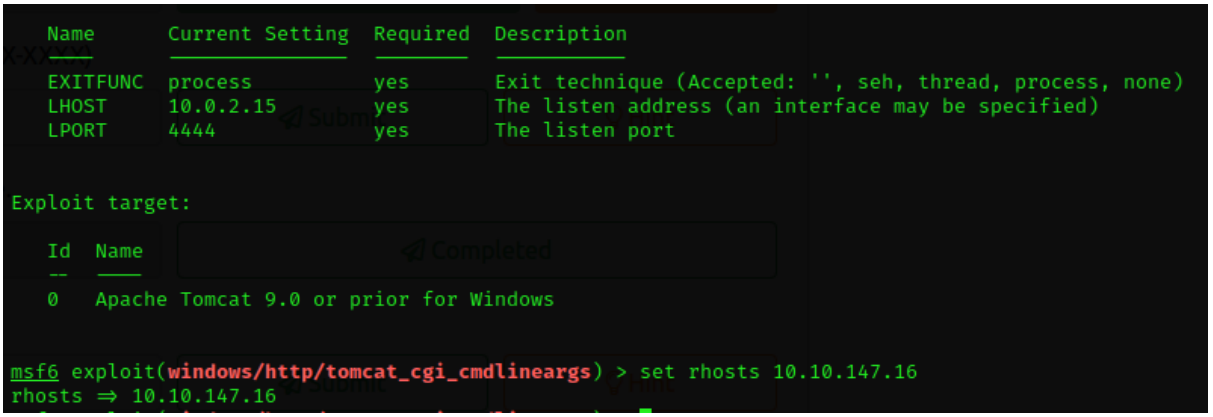


Question 2

Question 3



Question 4



Thoughts:
We accessed the machine, then we got the information through nmap. Then we searched for the cve code in the cheat sheet and once we found it we entered it on msfconsole. Once we entered it, we set the rhost and ran it.then, we entered cgi-bin/elfwhacker.bat as a target and started to exploit it.

Day 13- Coal For Christmas
Tools Used: Linux

Question 1

```
23/tcp  open  telnet
```

Question 2

```
We knew you were coming and we wanted to make
it easy to drop off presents, so we created
an account for you to use.

Username: santa
Password: clauschristmas
```

Question 3

```
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
```

Question 4

```
/**************************************************
// HAHA! Too bad Santa! I, the Grinch, got here
// before you did! I helped myself to some of
// the goodies here, but you can still enjoy
// some half eaten cookies and this leftover
// milk! Why dont you try and refill it yourself!
//    - Yours Truly,
//          The Grinch
//**************************************************/
```

Question 5

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

Question 6

```
'firefart'
```

Question 7

```
8b16f00dd3b51efadb02c1df7f8427cc
```

Question 8

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 advantage of a race

Thoughts :
We accessed the machine, and then used nmap to get the port and then we used telnet to gain the username and password,then we opened the cookies and milk text file and found that grinch came first.we got the dirty cow's raw sourcecode from github and got the verbatim syntax.After getting the new username, we proceeded to run tree/mdsum5 to get the bash.

DAY 14: Where's Rudolph

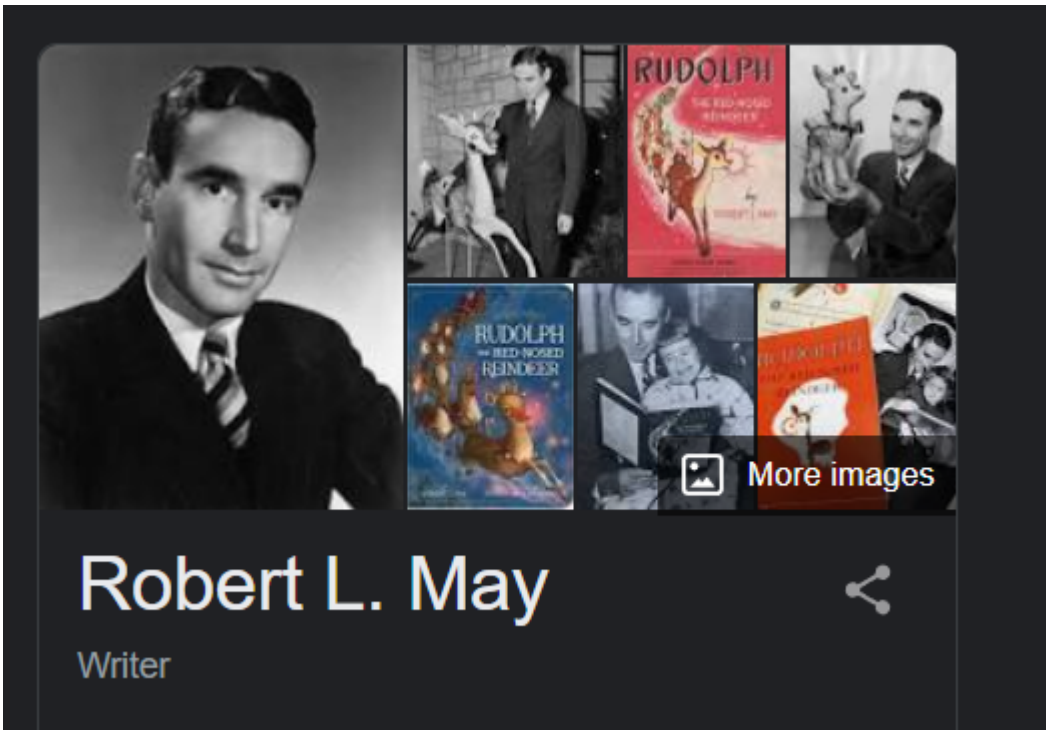
Question 1

```
https://www.reddit.com/user/IGuidetheClaus2020/comments
```

Question 2

```
I was actually born in Chicago
```

Question 3



Question 4

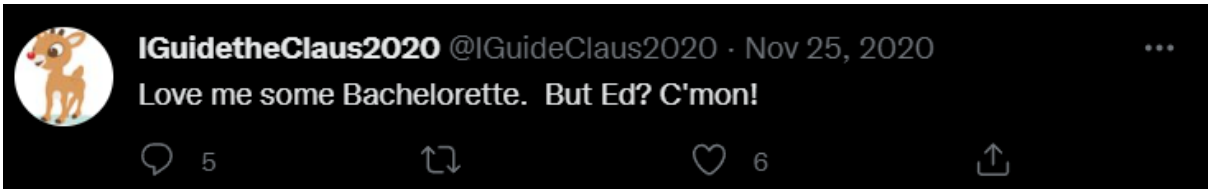
IGuidetheClaus2020 1 point · 2 years ago

Ouch. Some days I love Twitter. Some days, it's just...lol.

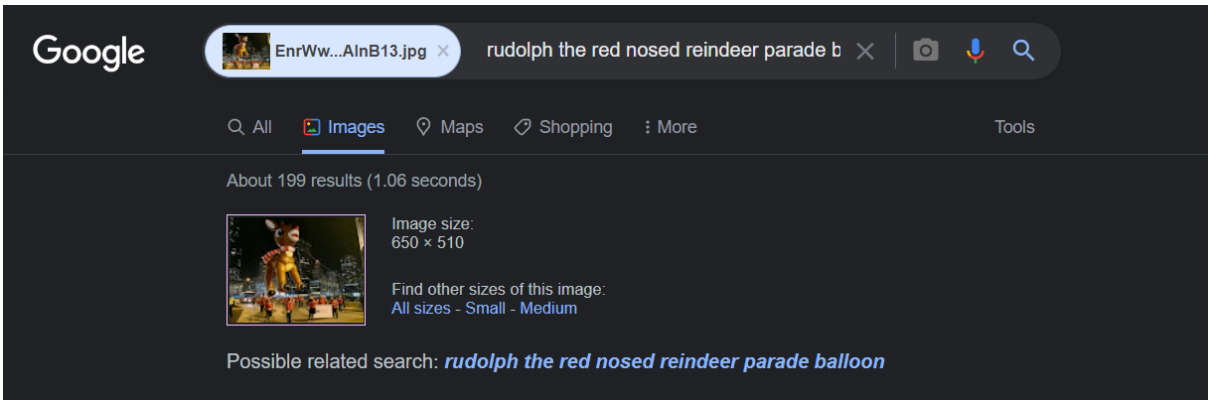
Reply Share •••

Question 5

Question 6



Question 7



Question 9

{FLAG}ALWAYSCHECKTHEEXIFD4T4

Question 10

540 Michigan Ave, Chicago, IL 60611, United States

Day 15- There's a python in my stocking.
Tools Used: Linux, Python

Question 1

```
>>> True + True
2
>>>
```

Question 3

```
>>> bool("false")
True
>>>
```

Question 5

```
>>> x = [1, 2, 3]
>>>
>>> y = x
>>>
>>> y.append(6)
>>>
>>> print(x)
[1, 2, 3, 6]
>>>
```

Question 6

Now let's say we wante
We pass by reference.

Question 7

```
What is your name? Skidy
The Wise One has allowed you to come in.
```

Question 8

```
What is your name? elf
The Wise One has not allowed you to come in.
```

Thoughts: We went through the notes and refreshed our memories about python that we've learned from semester 1.