PSP0201 T2130 - Tutorial Week 4
1 message

Google Forms <forms-receipts-noreply@google.com> Sat, 2 Jul 2022 at 19:04
To: 1211101303@student.mmu.edu.my

Google Forms

Thanks for filling in PSP0201 T2130 - Tutorial Week 4

Here's what was received.

Edit response

PSP0201 T2130 - Tutorial Week 4

Your email address (**1211101303@student.mmu.edu.my**) was recorded when you submitted this form.

Student ID

1211101303

Student Name *

AIMAN FARIS BIN AIDI ZAMRI

Tutorial Group *

- ○ T12L
- ○ T13L

- [ ] T14L
- [ ] T15L
- [x] T16L
- [ ] T17L
- [ ] T18L

Group Name *

Marceline

Day 11 - Networking The Rogue Gnome

Transfer the answers from THM to this form. Be on the lookout for possible additional questions.

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

- [x] Vertical
- [ ] Horizontal

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? *

Copy and paste from THM

- [x] Vertical
- [ ] Horizontal

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? *

- ○ Vertical
- ◉ Horizontal

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

Answer in lowercase.

sudoers

Q4: What is the Linux Command to enumerate the key for SSH? *

Answer: find * ***** ****** *>/***/***

find / -name id_rsa 2> /dev/null

Q5: 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? *

Answer: chmod ** ****.**

chmod +x filename find.sh

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? *

Answer: python3 ** ****.****** ****

python3 -m http.server 9999

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

Copy and paste the flag from THM.

thm{2fb10afe933296592}

Day 12 - Networking Ready, set, elf.

Transfer the answers from THM to this form. Be on the lookout for possible additional questions.

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

Answer: x.x.xx where x are numerical digits.

9.0.17

Q2: What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX) *

Answer: CVE-xxxx-xxxx where x are numerical digits

CVE-2019-0232

Q3: What are the contents of flag1.txt *

Copy and paste the flag from THM

thm{whacking_all_the_elves}

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

Copy and paste the flag from THM.

- [x] LHOST
- [ ] LPORT
- [x] RHOST

Day 13 - Networking Coal for Christmas

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

Answer in lowercase.

telnet

Q2: What credential was left for you? *

Copy and paste from THM.

clauschristmas

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

Copy and paste from THM.

Ubuntu 12.04

Q4: Who got here first? *

Please answer in lowercase.

grinch

Q5: What is the verbatim syntax you can use to compile, taken from the real C source code comments? *

Copy the gcc comand from THM.

gcc -pthread dirty.c -o dirty -lcrypt

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

Copy the username from THM.

firefart

Q7: What is the MD5 hash output? *

Copy the MD5 hash value from THM.

8b16f00dd3b51efadb02c1df7f8427cc

Q8: What is the CVE for DirtyCow? *

Answer: CVE-XXXX-XXXX where Xs are numerical digits

CVE-2016-5195

Day 14 - [OSINT] Where's Rudolph?

Transfer the answers from THM to this form. Be on the lookout for possible additional questions.

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

copy and paste the URL

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

Q2: According to Rudolph, where was he born? *

Answer is the name of a city

Chicago

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

Answer as a name, uppercase first character

May

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

Answer as a name, uppercase first character

Twitter

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

Copy and paste from Twitter Username

IGuideClaus2020

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

Answer as a name, uppercase first character

Bachelorette

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

Answer is the name of a city.

Chicago

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

Copy and paste the coordinates from THM. Careful to keep the proper spacing.

41.891815, -87.624277

Q9: Did you find a flag too? *

Copy and paste the flag from THM

{FLAG}ALWAYSCHECKTHEEXIFD4T4

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

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

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? *

Hint: Answer is the street number for the Marriot.

540

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

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

Copy and paste from THM

2

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

Copy and paste from THM

PyPi

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

Copy and paste from THM

True

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

Copy and paste from THM

Requests

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

Run and code and follow the output, including the spacing.

[1, 2, 3, 6]

Q6: What causes the previous task to output that? *

Answer in lowercase

Pass by reference

Examine the following code:

```
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.")
```

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

- (●) The Wise One has allowed you to come in.
- ( ) The Wise One not has allowed you to come in.

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

- ( ) The Wise One has allowed you to come in.
- (●) The Wise One not has allowed you to come in.

Upload Links

Writeup Upload Link *

https://github.com/aimnfris/Report-PSP0201-Week-4-Marceline-.git