

PSP0201

Week 6

Writeup

Group Name: Gold

Members:

ID	Name	Role
1211101707	Nur'aina Binti Ikhwan Moeid	Leader
1211103984	Nur Afreen Junaidah Binti Noorul Mohamed Eliyas	Member
1211101519	Aisyah Binti Ahmad Komarolaili	Member
1211102590	Nur Hanisah Binti Mohd Pauzi	Member

Day 21: Blue Teaming- Time for some ELForensics

Tools used: THM Attackbox, Remmina

Solution/walkthrough:

Question 1

Read the contents of the text file within the Documents folder. What is the file hash for db.exe? -

596690FFC54AB6101932856E6A78E3A1

```
PS C:\Users\littlehelper\Documents> more '.\db_file_hash.txt'
Filename:      db.exe
MD5 Hash:     596690FFC54AB6101932856E6A78E3A1
```

Question 2

What is the MD5 file hash of the mysterious executable within the Documents folder? -

5F037501FB542AD2D9B06EB12AED09F0

```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm MD5 .\deebee.exe
Algorithm      Hash
-----        -----
MD5           5F037501FB542AD2D9B06EB12AED09F0
```

Question 3

What is the SHA256 file hash of the mysterious executable within the Documents folder? -

F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED

```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm SHA256 .\deebee.exe
Algorithm      Hash
-----        -----
SHA256         F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED
```

Question 4

Using Strings find the hidden flag within the executable? -

THM{f6187e6cbeb1214139ef313e108cb6f9}

```
Using SSO to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -Value $(Get-Byte) -Encoding Byte -Stream hidedb
```

Question 5

What is the powershell command used to view ADS? - Get-Item -Path file.exe -Stream *

The command to view ADS using Powershell: `Get-Item -Path file.exe -Stream *`

Question 6

What is the flag that is displayed when you run the database connector file? -

THM{088731ddc7b9fdeccaed982b07c297c}

```
Choose an option:  
1) Nice List  
2) Naughty List  
3) Exit
```

THM{088731ddc7b9fdeccaed982b07c297c}

Question 7

Which list is Sharika Spooner on? - Naughty list

```
Missy Stiner  
Sanford Geesey  
Jovan Hullett  
Sherlene Loehr  
Melisa Vanhoose  
Sharika Spooner
```

Sucks for them .. Returning to the User Menu...

Question 8

Which list is Jaime Victoria on? - Nice list

```
Delphine Gossard  
Jaime Victoria
```

Awesome .. Great! Returning to the User Menu...

Thought Process/ Methodology:

use the AttackBox and Remmina to connect to the remote machine. For Server provide **(MACHINE_IP)** as the IP address provided to you for the remote machine. The credentials for the user account is, user name: **littlehelper** and user password: **iLove5now!**.With PowerShell, we can obtain the hash of a file by running the following command: **Get-FileHash -Algorithm MD5 file.txt**. The command to run for the Strings tool to scan the mysterious executable: **c:\Tools\strings64.exe -accepteula file.exe**. Alternate Data Streams (ADS) is a file attribute specific to Windows NTFS (New Technology File System). The command to view ADS using Powershell: **Get-Item -Path file.exe -Stream ***. The command to run to launch the hidden executable hiding within ADS: **wmic process call create \$(Resolve-Path file.exe:streamname)**. And we are done.

Day 22: Blue Teaming- Elf McEager becomes CyberElf

Tools used: THM Attackbox, Remmina, Keepass, Cyberchef

Solution/walkthrough:

Question 1

What is the password to the KeePass database? - thegrinchwashere

The screenshot shows the CyberChef interface. On the left, under 'Recipe', there is a 'Magic' section with 'Depth' set to 3 and 'Intensive mode' checked. Below that is a checkbox for 'Extensive language support'. A 'Crib (known plaintext string or regex)' field contains the text 'From_Base64('A-Za-z0-9+=',true,false)'. On the right, the 'Input' field shows the encoded string 'dGhlZ3JpbmNod2FzaGVyZQ=='. Above the input, status information is displayed: 'start: 24', 'end: 24', 'length: 0', and 'len li'. The 'Output' section shows the decoded result: 'thegrinchwashere'. There is also a 'Result snippet' section below it.

Question 2

What is the encoding method listed as the 'Matching ops'? - base64

Result snippet	Properties
thegrinchwashere	Possible languages: English German Dutch Indonesian Matching ops: From Base64,

Question 3

What is the note on the hiya key? - Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P

The screenshot shows a KeePass password entry dialog. The 'Title' field is filled with 'hiya'. The 'User name' and 'Password' fields are empty. The 'Repeat' field shows a masked password. The 'Quality' bar is mostly yellow, indicating 47 bits of entropy. The 'URL' field is empty. The 'Notes' field contains the text: 'Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P'.

Question 4

What is the decoded password value of the Elf Server? - sn0wM4n!

The screenshot shows a hex editor interface. On the left, under 'Recipe', there is a 'From Hex' section with a 'Delimiter' dropdown set to 'Auto'. On the right, under 'Input', the hex value '736e30774d346e21a' is shown. Under 'Output', the ASCII representation 'sn0wM4n!' is displayed. The status bar at the bottom indicates 'start: 62 end: 62 length: 0 lines: 1'.

Question 5

What was the encoding used on the Elf Server password? - hex

Question 6

What is the decoded password value for ElfMail? - ic3Skating!

The screenshot shows a hex editor interface. On the left, under 'Recipe', there is a 'From HTML Entity' section. On the right, under 'Input', the HTML entity code 'ic3Skating!' is shown. Under 'Output', the ASCII representation 'ic3Skating!' is displayed. The status bar at the bottom indicates 'time: 1ms length: 11 lines: 1'.

Question 7

What is the username:password pair of Elf Security System? - superelfadmin:nothinghere

The screenshot shows a password manager interface titled 'Edit Entry'. The 'Entry' tab is selected. The entry details are as follows:
Title: Elf Security System
User name: superelfadmin
Password: nothinghere
Repeat: (empty)
Deadline: 22 May 11 AM

Question 8

Decode the last encoded value. What is the flag? - THM{657012dcf3d1318dca0ed864f0e70535}

The screenshot shows the CyberChef interface with two decoding steps. The first step, "From Charcode" (Base 10), takes the input: eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 32, 61, 32, 100, 111, 99, 117, 109, 101, 110, 116, 46, 99, 114, 101, 97, 116, 101, 69, 108, 101, 109, 101, 110, 116, 40, 39, 115, 99, 114, 105, 112, 116, 39, 41, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 116, 121, 112, 101, 32, 61, 32, 39, 116, 101, 120, 116, 47, 106, 97, 118, 97, 115, 99, 114, 105, 112, 116, 30, 50, 32, 115, 111, 100, 101, 115, 116, 114, 105, 110, 103, 46). The second step, "From Charcode" (Base 10), takes the output of the first step and decodes it to ".https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8". The final output is displayed in a terminal window as "1 THM{657012dcf3d1318dca0ed864f0e70535}".

Thought Process/ Methodology:

We use Attackbox and Remmina to connect to the remote machine. After we create a RDP with credentials **username:Administrator** and **password:sn0wF!akes!!!**, we can now log into the remote system. Decode the filename on the desktop using cyberchef to get the Keepass's master password. Now that we have successfully unlocked Keepass, we can see that there are more encodings within the Keepass database file. There are also notes in each file that contain clues such as cyberchef recipes to decode the passwords. To get the flag, we should decode the encoded value first and open the link from the decoded value to get the flag.

Day 23: Blue Teaming- The Grinch strikes again!

Tools used: THM Attackbox, Remmina

Solution/walkthrough:

Question 1

What does the wallpaper say? -THIS IS FINE



Question 2

Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

-nomorebestfestivalcompany

```
root@ip-10-10-132-12:~  
Window Menu  Search  Terminal  Tabs  Help  
root@ip-10-10-132-12:~  x  root@ip-10-10-132-12:~  x  
root@ip-10-10-132-12:~# echo "bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==" | base64 -d  
nomorebestfestivalcompanyroot@ip-10-10-132-12:~#
```

Question 3

At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files? -.grinch

	Name	Date modified	Type
	master-password.txt.grinch	12/23/2020 1:41 PM	GRINCH

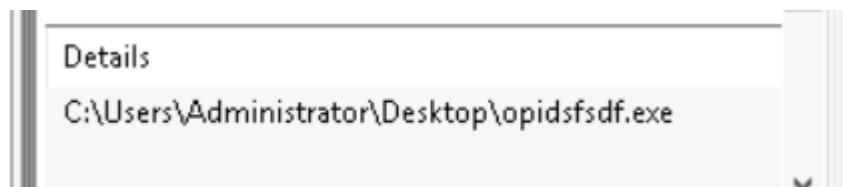
Question 4

What is the name of the suspicious scheduled task? -opidsfsdf

	Name	Date modified	Type
▼ This PC	opidsfsdf	11/25/2020 8:19 PM	Applic
> 3D Objects	RansomNote	12/7/2020 7:53 AM	Text D

Question 5

Inspect the properties of the scheduled task. What is the location of the executable that is run at login? -C:\Users\Administrator\Desktop\opidsfsdf.exe



Question 6

There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?
-7a9eea15-0000-0000-0000-010000000000

General	Triggers	Actions	Conditions	Settings	History (disabled)
Name:	ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}				
Location:	\				

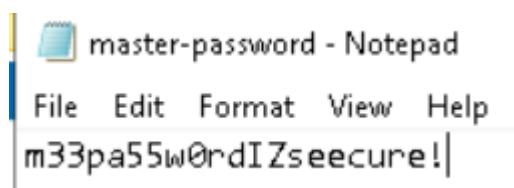
Question 7

Assign the hidden partition a letter. What is the name of the hidden folder? -confidential

	Name	Date modifi
▼ This PC	confidential	12/2/2020 9:
> 3D Objects	database	12/2/2020 9:

Question 8

Right-click and inspect the properties for the hidden folder. Use the 'Previous Versions' tab to restore the encrypted file that is within this hidden folder to the previous version. What is the password within the file? -m33pa55w0rdIZseecure!



Thought Process/ Methodology:

We start by booting Remmina (remmina &) on the terminal which will lead us to **Remmina Remote Desktop Client**. Next, we open Remmina Preferences on the RDP section where we change the Quality settings: Poor (fastest) and select: wallpaper. Then, we press the + button and enter the IP Address in the **Server**, the given username and password in the **User name** and **User password** field and manipulate the **Color depth** to RemoteFX (32 bpp). This will open the Admin Port. There, we have access to admin files.

Day 24: Final Challenge- The Trial Before Christmas

Tools used: THM AttackBox, Gobuster, BurpSuite, CrackStation

Solution/walkthrough:

Question 1

Scan the machine. What ports are open? -80, 65000

```
Not shown: 65533 closed ports
PORT      STATE SERVICE
80/tcp    open  http
65000/tcp open   unknown
```

Question 2

What's the title of the hidden website? -Light Cycle



Question 3

What is the name of the hidden php page? -/uploads.php

```
=====
2020/12/20 05:53:02 Starting gobuster
=====
/uploads.php (Status: 200)
/assets (Status: 301)
```

Question 4

What is the name of the hidden directory where file uploads are saved? -/grid

```
/api (Status: 301)
/grid (Status: 301)
```

Question 5

What is the value of the web.txt flag? -THM{ENTER_THE_GRID}

```
cat web.txt
THM{ENTER_THE_GRID}
```

Question 6

What lines are used to upgrade and stabilize your shell?

- export TERM=xterm
- python3 -c 'import pty;pty.spawn("/bin/bash")'
- stty raw -echo; fg

Working inside the reverse shell:

1. The first thing to do is use `python3 -c 'import pty;pty.spawn("/bin/bash")'`, which uses Python to spawn a better-featured bash shell. At this point, our shell will look a bit prettier, but we still won't be able to use tab autocomplete or the arrow keys, and Ctrl + C will still kill the shell.
2. Step two is: `export TERM=xterm` – this will give us access to term commands such as `clear`.
3. Finally (and most importantly) we will background the shell using `Ctrl + Z`. Back in our own terminal we use `stty raw -echo; fg`. This does two things: first, it turns off our own terminal echo (which gives us access to tab autocompletes, the arrow keys, and `Ctrl + C` to kill processes). It then foregrounds the shell, thus completing the process.

The full technique can be seen here: [here](#)

Question 7

Review the configuration files for the webserver to find some useful loot in the form of credentials.

- tron:IFightForTheUsers

```
$dbpass = "IFightForTheUsers";
$database = "tron";
```

Question 8

Access the database and discover the encrypted credentials. -tron

```
File Edit View Search Terminal Help
mysql> use tron;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

Question 9

Crack the password. What is it? -@computer@

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Question 10

Use su to login to the newly discovered user by exploiting password reuse. What is the user you are switching to? -flynn

```
mysql> select * from users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1  | flynn   | edc621628f6d19a13a00fd683f5e3ff7 |
+----+-----+-----+
1 row in set (0.00 sec)
```

Question 11

What is the value of the user.txt flag? -THM{IDENTITY_DISC_RECOGNISED}

```
cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
```

Question 12

Check the user's groups. Which group can be leveraged to escalate privileges? -lxd

```
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
flynn@light-cycle:~$
```

Question 13

What is the value of the root.txt flag? -THM{FLYNN_LIVES}

```
cat root.txt
THM{FLYNN_LIVES}
```

Thought Process/ Methodology:

We use Nmap tool to scan open ports on a system using command `nmap -vv 10.10.230.41`. After we've found the open ports, we look for the hidden website by entering the ip address along with the ports we've found earlier; `10.10.230.41:65000`. Next, we're using gobuster to look for the name of the hidden php page. Using gobuster result we've got, we try to accessing the listed directory where server keeps the uploaded files is in /grid. To upload and execute a reverse shell, we first change the script's configuration. After we're done with the php reverse shell script, we move to bypass the client-side filter. With Burpsuite tools help, we manage to upload the reverse shell script. We set up netcat before we execute the file using command `nc -nlvp 1234` followed by clicking on the uploaded script on web's /grid directory to execute the script. To find the value of the web.txt flag, where the flag can be seen on /var/www/ directory and we're using `cat web.txt` to read the contents inside text file. To upgrade and stabilize the shell we use lines `export TERM=xterm`, `python3 -c 'import pty; pty.spawn("/bin/bash")'` and `stty raw -echo; fg`. Then, we navigate to /var/www/ directory and list all the items inside where we found bunch of .php files inside and `dbauth.php` and here we got to discover the encrypted credentials we needed. Using credentials we've found, we use it to login into mysql database to look for the name of the database we find these in before, using command

`mysql -utron -p` followed by entering the password. We use the database using `use tron;` to look for the db. We use sql query to display all the contents in it, the syntax is `select * from users;` . With the password that we've found in mysql database before is in hash form, so to determine the exact password, we bruteforce it using Crackstation. After we know both of the username and password combination for another account now we use `su` command to login. Next, to find the value of the user.txt flag we navigate into flynn's home directory and to read the text value, we use linux command `cat user.txt` . To view to which group can be leveraged to escalate privileges we type `id` in terminal and found that flynn's account is inside group lxd. To abuse this group to escalate privileges to root we only follow along the DarkStar's tutorial video. Lastly, to find the value of the root.txt flag, we navigate into `/mnt/root/root` because we've knew that there is a file called 'root.txt' while we're abusing the lxc container before. To open it up, we use `cat root.txt` and there we got our last flag for this task.