

PSP0201

Week 6

Writeup

Group Name: **Cyberteam**

Members

ID	Name	Role
121110186 4	Julian Koh Chee Yong	Leader
121110360 5	Danial Ierfan Bin Hazmi	Member
121110328 1	Jievenesh Arvind Naidu A/L Uma Selvam	Member
121110378 5	Brijhindhra A/L Saravanaraj	Member

Day 21 - Time for some ELForensics

Tools used: Kali Linux, Firefox, Remmina

Question 1: Read the contents of the text file within the Documents folder. What is the file hash for db.exe?

Command "more './db file hash.txt'"

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

Answer: 596690FFC54AB6101932856E6A78E3A1

Question 2: What is the MD5 file hash of the mysterious executable within the Documents folder?

Command "Get-FileHash -Algorithm MD5 .\deebie.exe"

```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm MD5 .\deebie.exe

Algorithm      Hash                                          Path
-----
MD5            5F037501FB542AD2D9B06EB12AED09F0         C:\Users\littlehelpe...
```

Answer: 5F037501FB542AD2D9B06EB12AED09F0

Question 3: What is the SHA256 file hash of the mysterious executable within the Documents folder?

Use the same command as question 2 but change 'MD5' to 'SHA256'.

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

Algorithm      Hash                                          Path
-----
SHA256         F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED C:\Users\littlehelper\Documents\deebie.exe
```

Answer: F5092B78B844E4A1A7C95B1628E 39B439E B6BF
2117B06D5A7B6EED99F5585FED

Question 4: Using Strings find the hidden flag within the executable?

Command “c:\Tools\strings64.exe -acceptula .\deebie.exe” and it will print the whole strings including the flag.

```
Select Windows PowerShell
args
Object
Accessing the Best Festival Company Database...
Done.
Using SSD to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\Documents\db.exe).Path -ReadCount 0 -Encoding Byte) -Encoding Byte -Stream hidedb
Hahaha ... guess what?
Your database connector file has been moved and you'll never find it!
I guess you can't query the naughty list anymore!
p!9
!V
WrapNonExceptionThrows
deebie
Copyright
2020
Jc8374a1e-384f-4cf2-b8c0-81f74ec36ab2
1.0.0.0
.NETFramework,Version=v4.0
FrameworkDisplayName
.NET Framework 4
RSDS
+FF
D:\code\src\deebie\deebie\obj\Debug\deebie.pdb
_CorExeMain
ascoree.dll
VS_VERSION_INFO
VarFileInfo
Translation
StringFileInfo
000004b0
Comments
CompanyName
FileDescription
deebie
FileVersion
1.0.0.0
InternalName
deebie.exe
LegalCopyright
Copyright
2020
LegalTrademarks
```

Answer: THM{f6187e6cbeb1214139ef313e108cb6f9}

Question 5: Q5: What is the PowerShell command used to view ADS?

Command “Get-Item -Path .\deebie.exe -Stream” to find the stream’s name then insert it in the “wmic process call create \$(Resolve-Path file.exe:streamname)” command by changing the ‘streamname’.

```
PS C:\Users\littlehelper\Documents> Get-Item -Path .\deebie.exe -Stream *

PSPath           : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebie.exe::$DATA
PSParentPath     : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName      : deebie.exe::$DATA
PSDrive          : C
PSProvider       : Microsoft.PowerShell.Core\FileSystem
PSIsContainer    : False
FileName        : C:\Users\littlehelper\Documents\deebie.exe
Stream           : ::$DATA
Length          : 5632

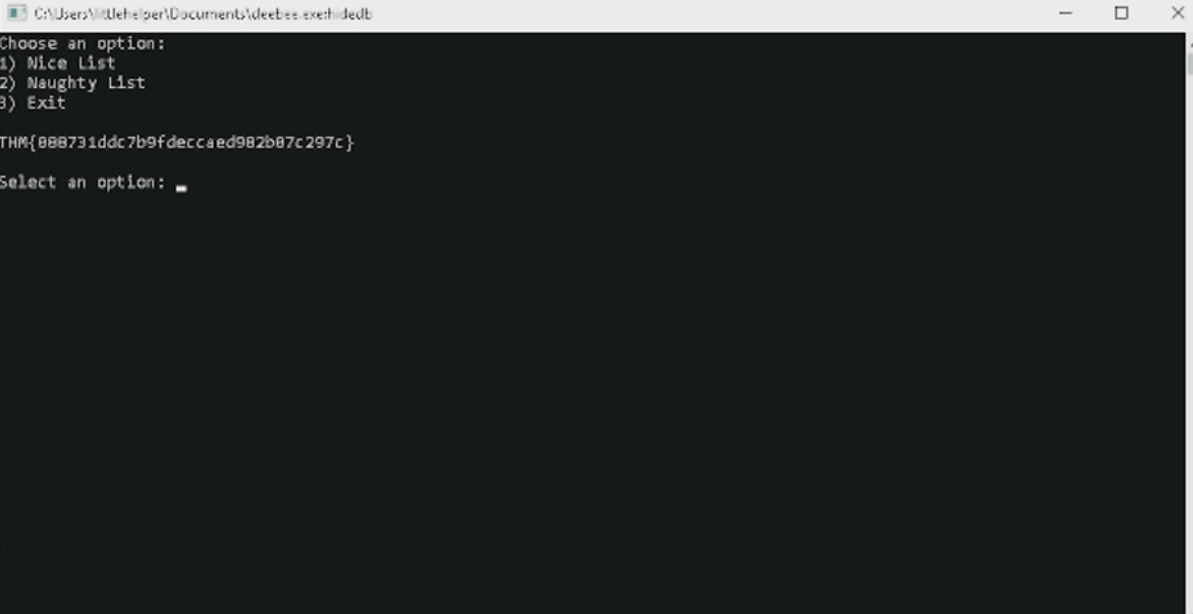
PSPath           : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebie.exe:hidedb
PSParentPath     : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName      : deebie.exe:hidedb
PSDrive          : C
PSProvider       : Microsoft.PowerShell.Core\FileSystem
PSIsContainer    : False
FileName        : C:\Users\littlehelper\Documents\deebie.exe
Stream           : hidedb
Length          : 6144
```

Answer: wmic process call create \$(Resolve-Path .\deebie.exe: hidedb)

Question 6: What is the flag that is displayed when you run the database connector file?

Run the command from question 5 and it will launch the hidden executable hiding within ADS. The flag will be displayed.

```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path .\deebie.exe:hiddenb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
Instance of __PARAMETERS
{
    ProcessId = 3316;
    ReturnValue = 0;
}
```



```
C:\Users\littlehelper\Documents\deebie.exe:hiddenb
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}
Select an option: _
```

Answer: THM{088731ddc7b9fdeccaed982b07c297c}

Question 7: Which list is Sharika Spooner on?

Question 8: Which list is Jaime Victoria on?

Run the program

Answer 7: Naughty list

Answer 8: Nice list

Thought/Processes:

Firstly, we use remmina to connect to the remote machine. Then, we logged into the remote system. Next, we use the Windows PowerShell from the remote system to obtain file hashes of files on the endpoint. Command “more ‘./db file hash.txt’” to read the contents of the text file within the Documents folder. After that, command “Get-FileHash -Algorithm MD5 .\deebie.exe” to find the MD5 file hash of the mysterious executable. Then, by using Strings to find the hidden flag within the executable, command “c:\Tools\strings64.exe -acceptula .\deebie.exe” and it will print the whole strings. Next, to run the database connector file, we need to find the stream’s name. Therefore, we command “Get-Item -Path .\deebie.exe -Stream” and then we insert the stream’s name in the “wmic process call create \$(Resolve-Path file.exe:streamname)” command by changing the ‘streamname’. After running the command, it launches the hidden executable hiding within ADS. By running the program, it will show the list of Nice and Naughty list.

Day 22: Elf McEager becomes CyberElf

Tools used: Kali Linux, Firefox, Remmina

Solution/Walkthrough:

Q1: What is the password to the KeePass database?

The screenshot shows the CyberChef website in a web browser. The interface includes a sidebar with various operations like Magic, Image, Detect File Type, etc. The main area displays the 'Magic' recipe configuration with a depth of 3. The input field contains the string 'dGh1Z3JpbmNod2FzaGVyZQ=='. The output field shows the result 'thegrinchwashere' and a table of properties including 'Possible languages' (English, German, Dutch, Indonesian) and 'Matching ops' (From Base64, From Base85, Valid UTF8, Entropy: 3.28).

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

We use cyberchef website and input the files name to convert the input and the output shows the hidden password of the KeePass

Answer: thegrinchwashere

Q2: What is the encoding method listed as the 'Matching ops'?

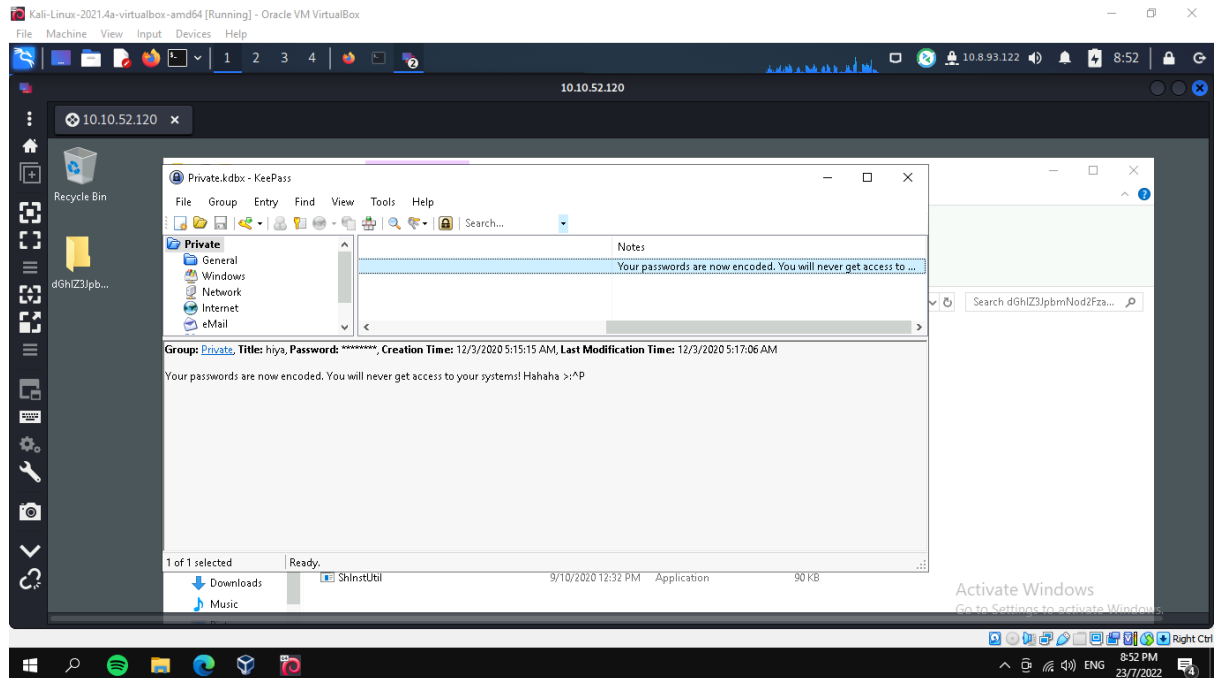
This screenshot is identical to the one above, showing the CyberChef website with the 'Magic' recipe configured to decode the input string 'dGh1Z3JpbmNod2FzaGVyZQ=='. The output is 'thegrinchwashere', and the 'Matching ops' property lists 'From Base64', 'From Base85', 'Valid UTF8', and 'Entropy: 3.28'.

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

The output under properties shows that the encoding method is Base64

Answer: base64

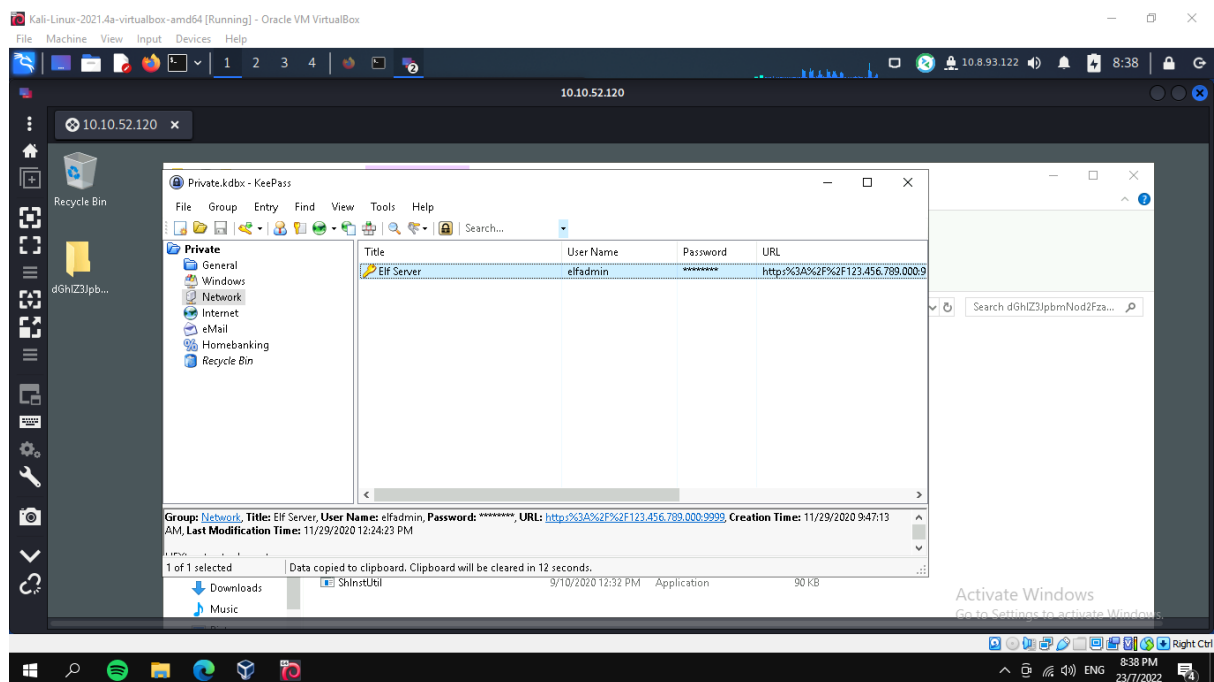
Q3: What is the note on the hiya key?

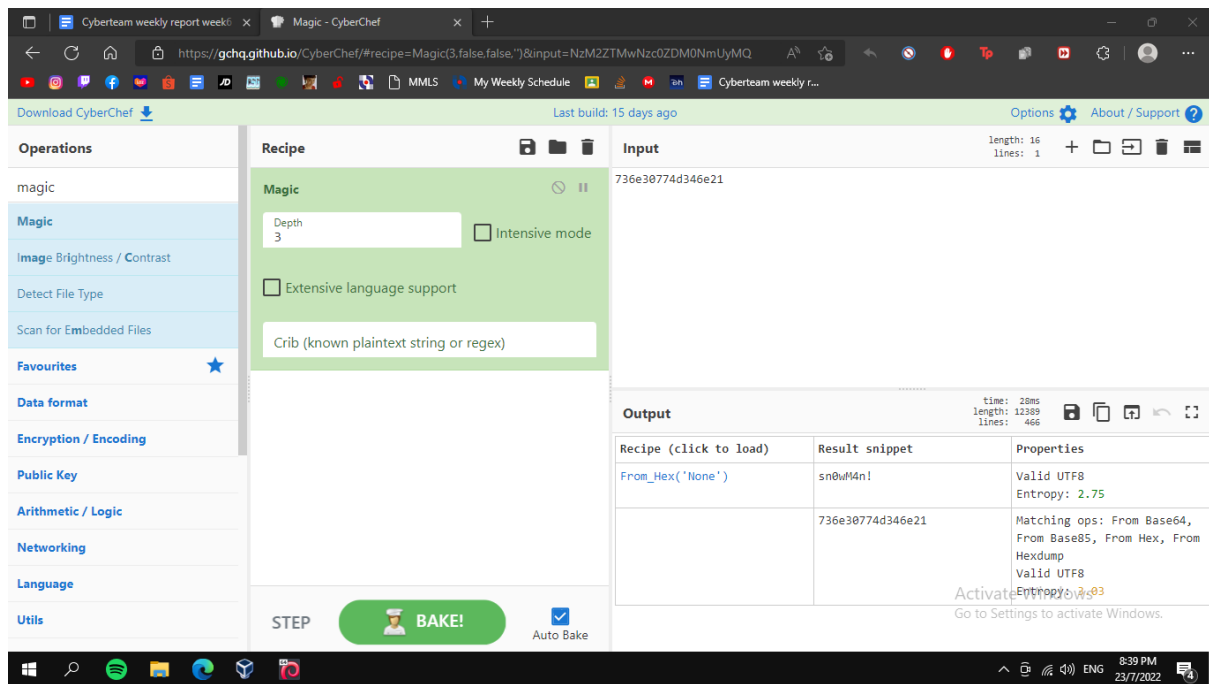


We can see the notes of the Hiya key clearly once we are in.

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

Q4: What is the decoded password value of the Elf Server?

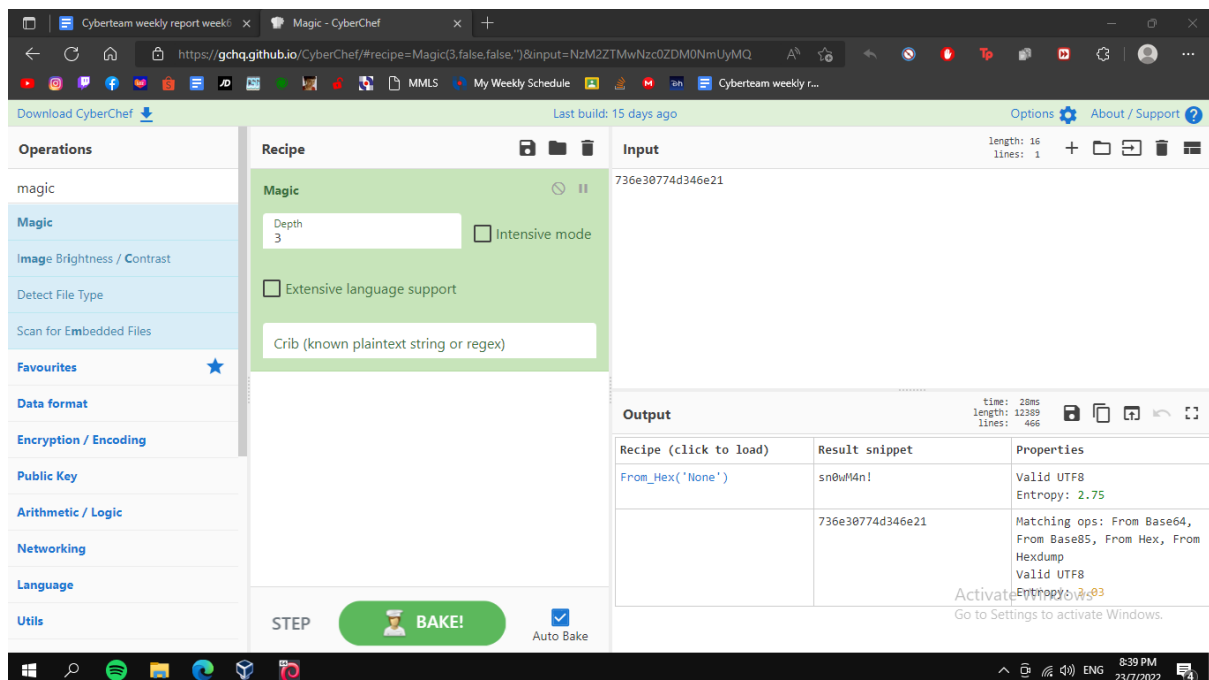




We right click on the elf server to show the password and input into Cyberchef and the output shows the password for elf server.

Answer: sn0wM4n!

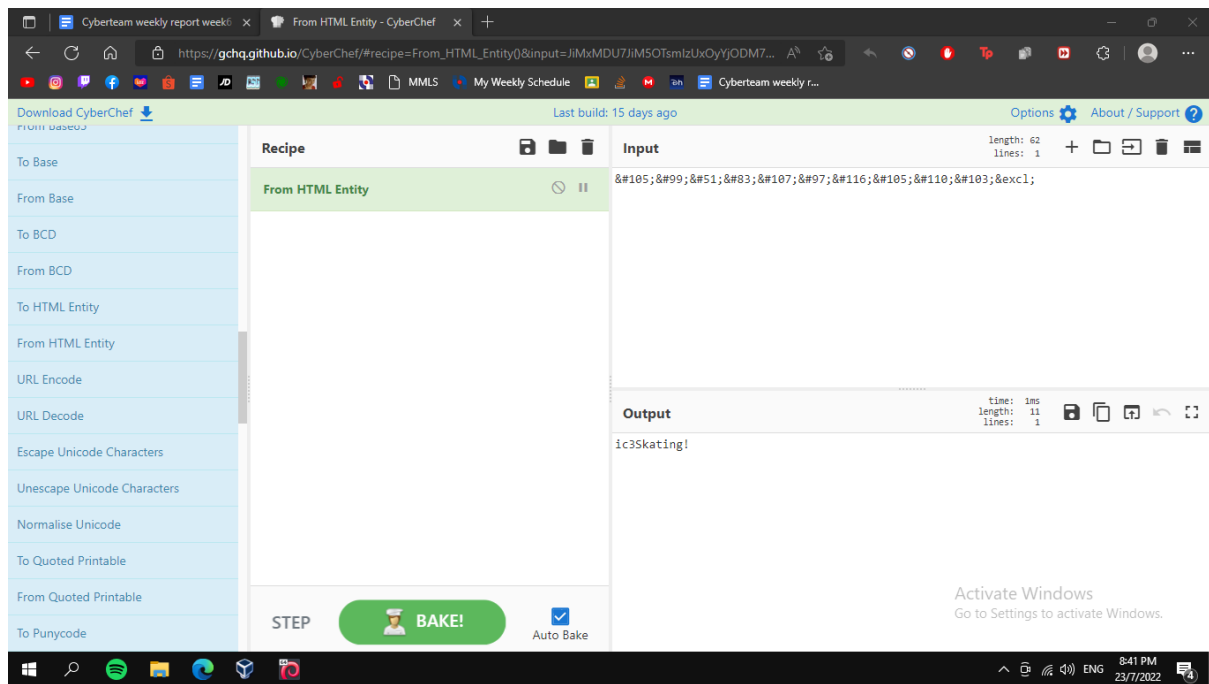
Q5: What was the encoding used on the Elf Server password?



The encoding is Hex as we can see in the properties.

Answer: hex

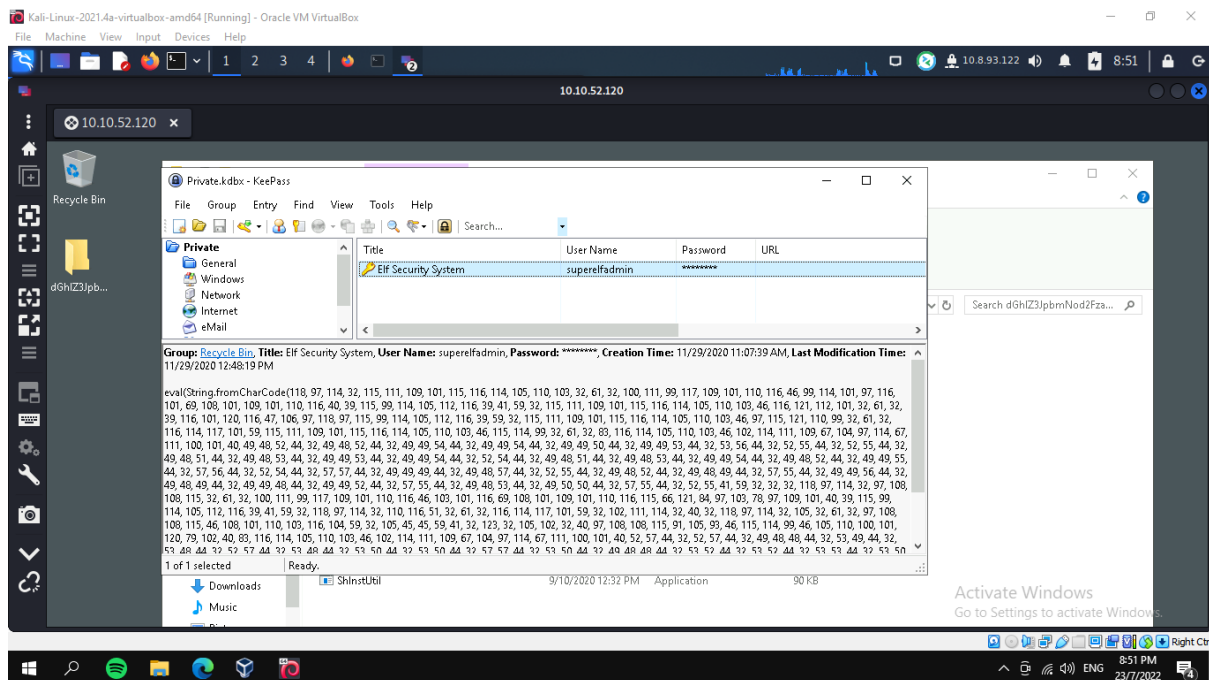
Q6: What is the decoded password value for ElfMail?



When the password from ElfMail is copied and applied into Cyberchef, we use HTML entity to convert the input and the output shows the password for ElfMail.

Answer: ic3Skating!

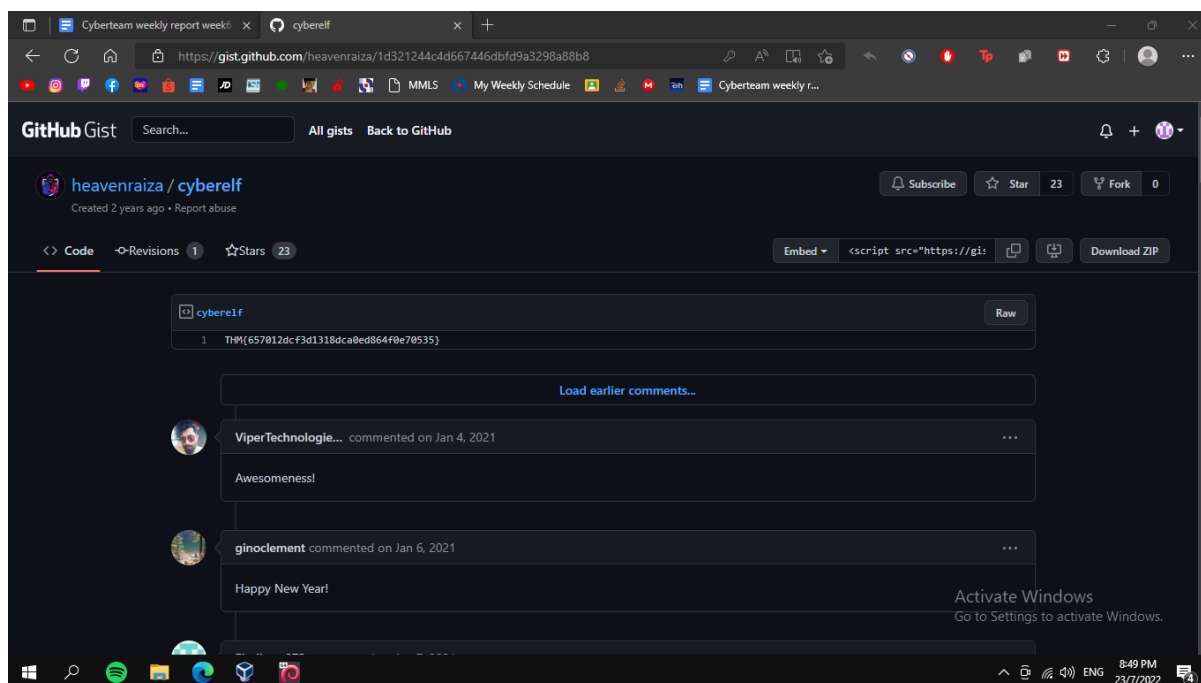
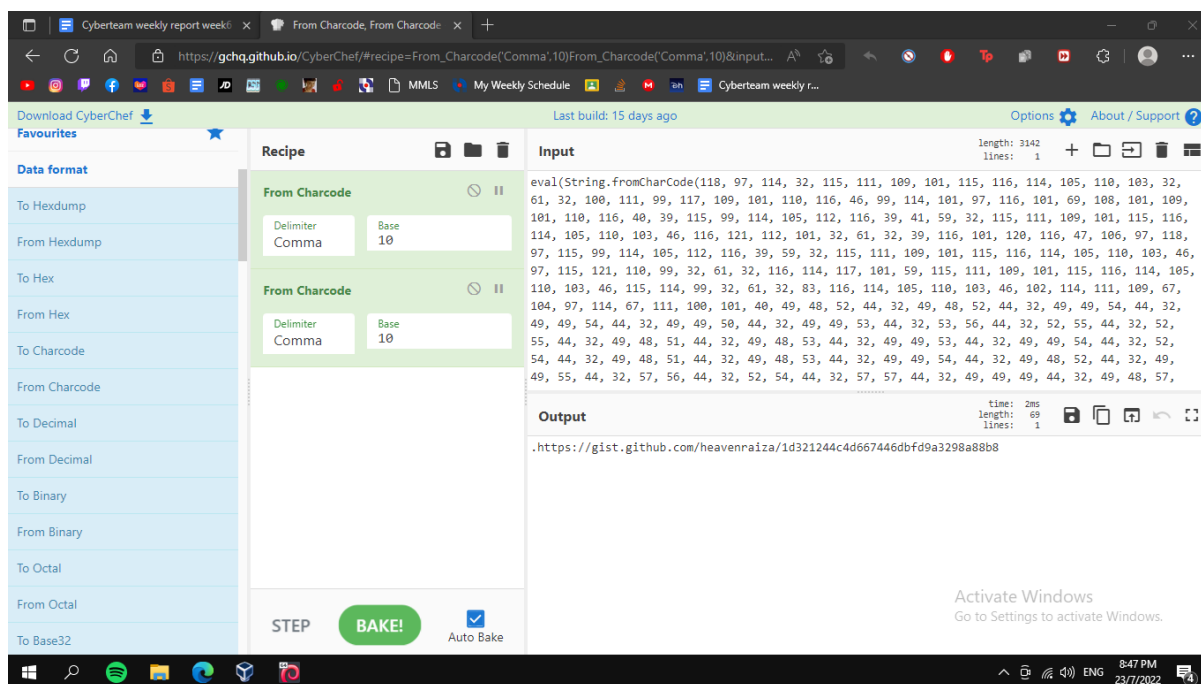
Q7: What is the username:password pair of Elf Security System?



The username is shown there as 'superelfadmin' and the password is 'nothinghere' when we right click on the password and show password to reveal the password.

Answer: superelfadmin:nothinghere

Q8: Decode the last encoded value. What is the flag?



We input the last encoded value from the KeePass and input into Cyberchef with 'from charcode' recipe with base 10 twice which gives us a github link where the flag is shown.

Answer: THM{657012dcf3d1318dca0ed864f0e70535}

Thought process/Methodology

We first access the machine using remmina with the IP given. Then we figure out the password to the KeePass by converting the file name in Cyberchef to decode the password. Once the password is figured out, we can access into KeePass where we can access into folder such as the Elf server where we input the hidden password

into Cyberchef to decode the password. This is repeated for the ElfMail and Elf security system. For the flag, we input the last encoded value to Cyberchef with 'from charcode' recipe with base 10 twice which gives us a github link where the flag is shown.

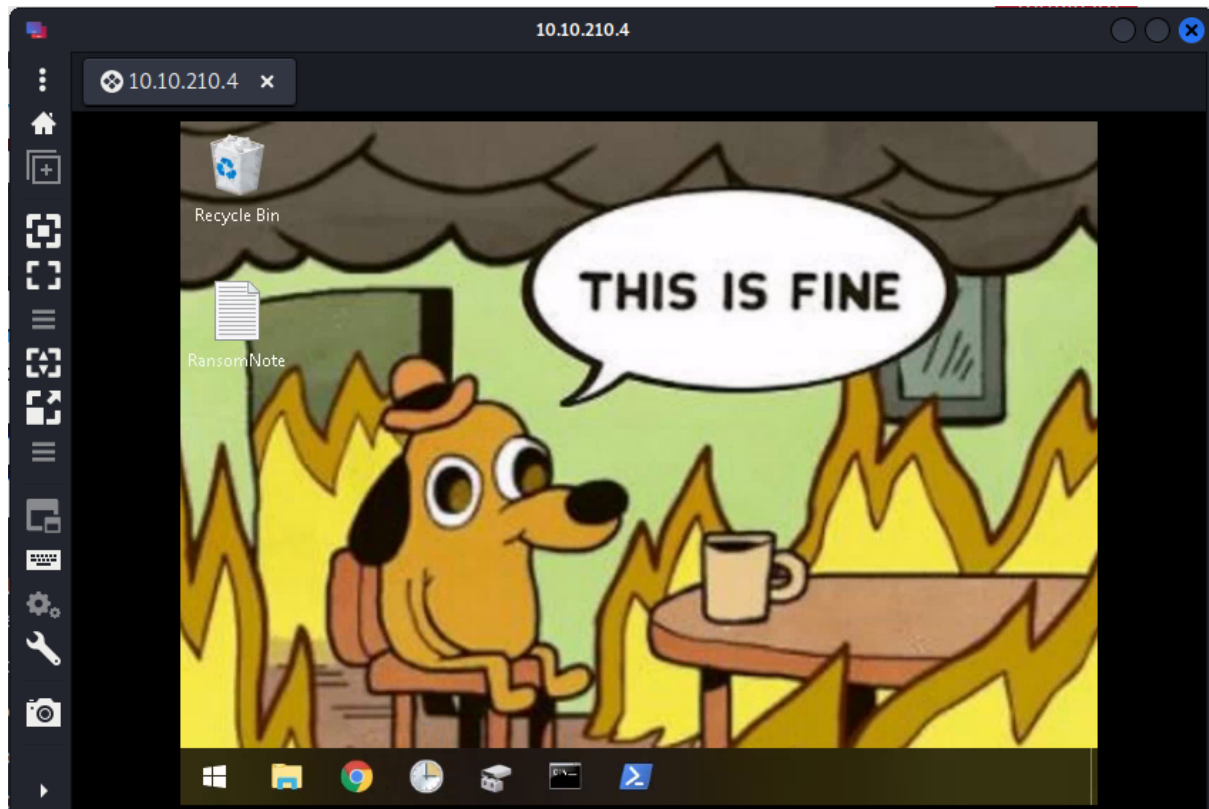
Day 23: Elf McEager becomes CyberElf

Tools used: Firefox, Kali Linux, Remmina

Solution/Walkthrough

Question 1: What does the wallpaper say?

Insert the IP Address, username and password based on THM.

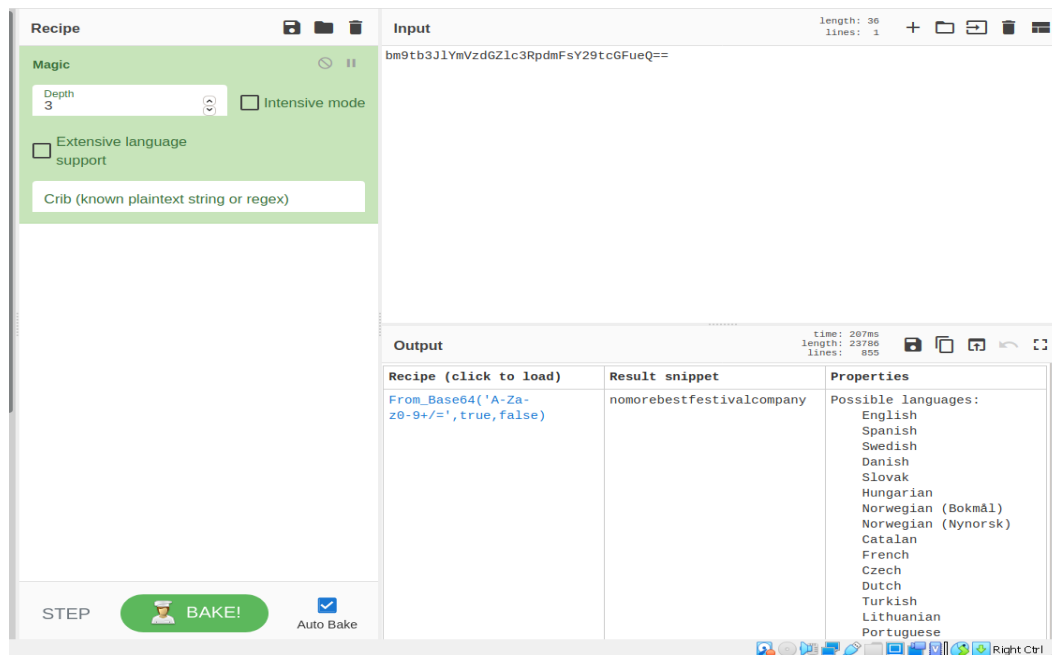


Answer:

THIS IS FINE

Question 2: Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

Open 'RansomNote'. Copy the bitcoin address and paste into CyberChef.

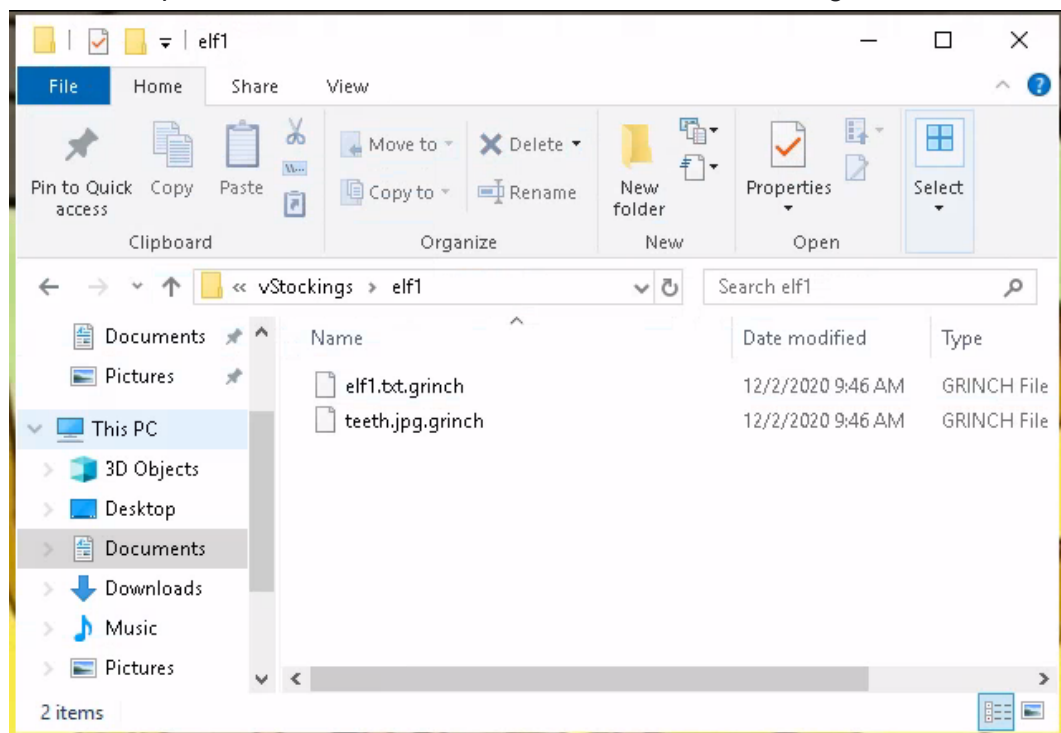


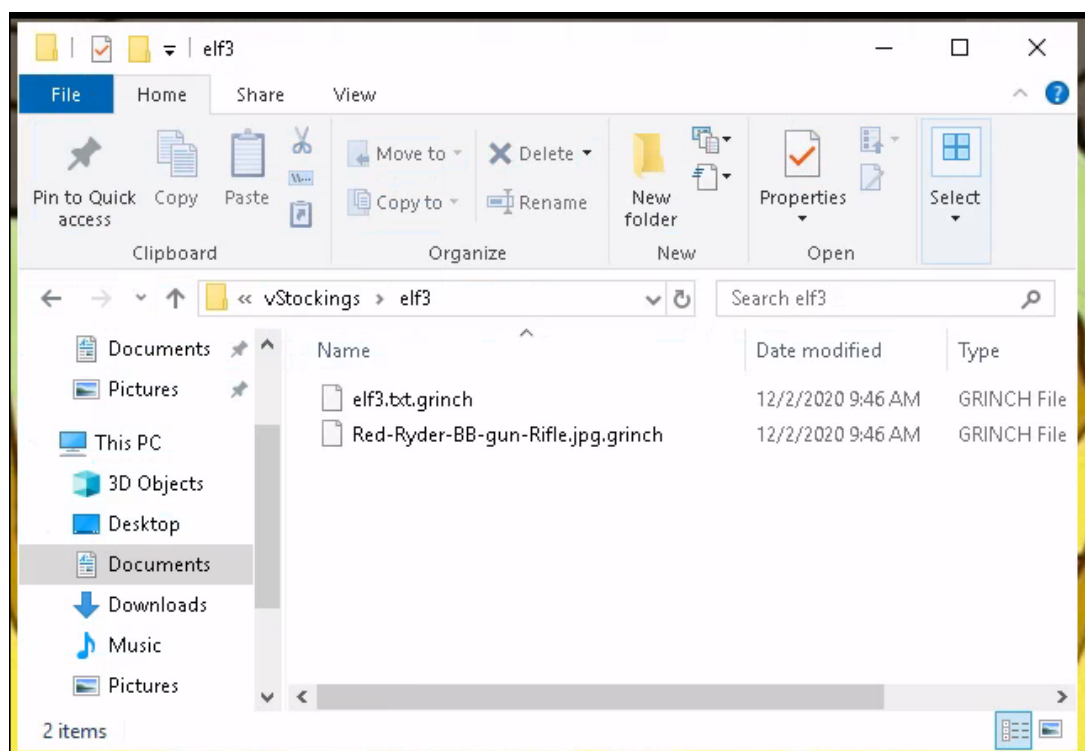
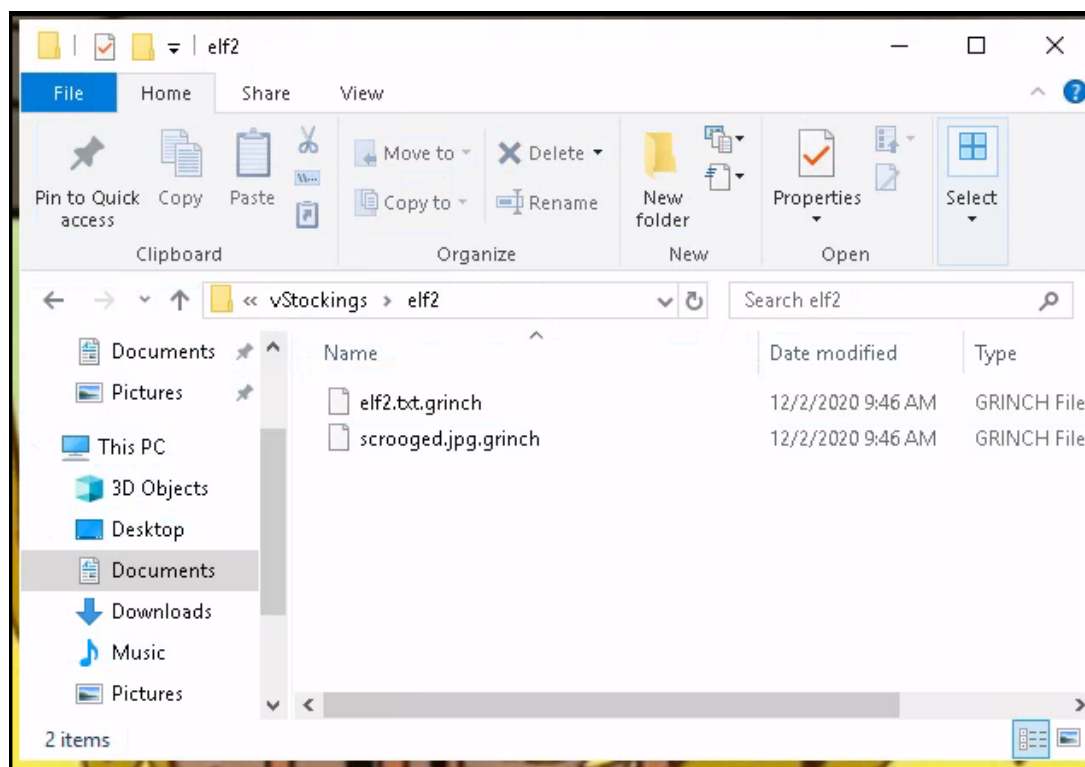
Answer:

nomorebestfestivalcompany

Question 3: At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?

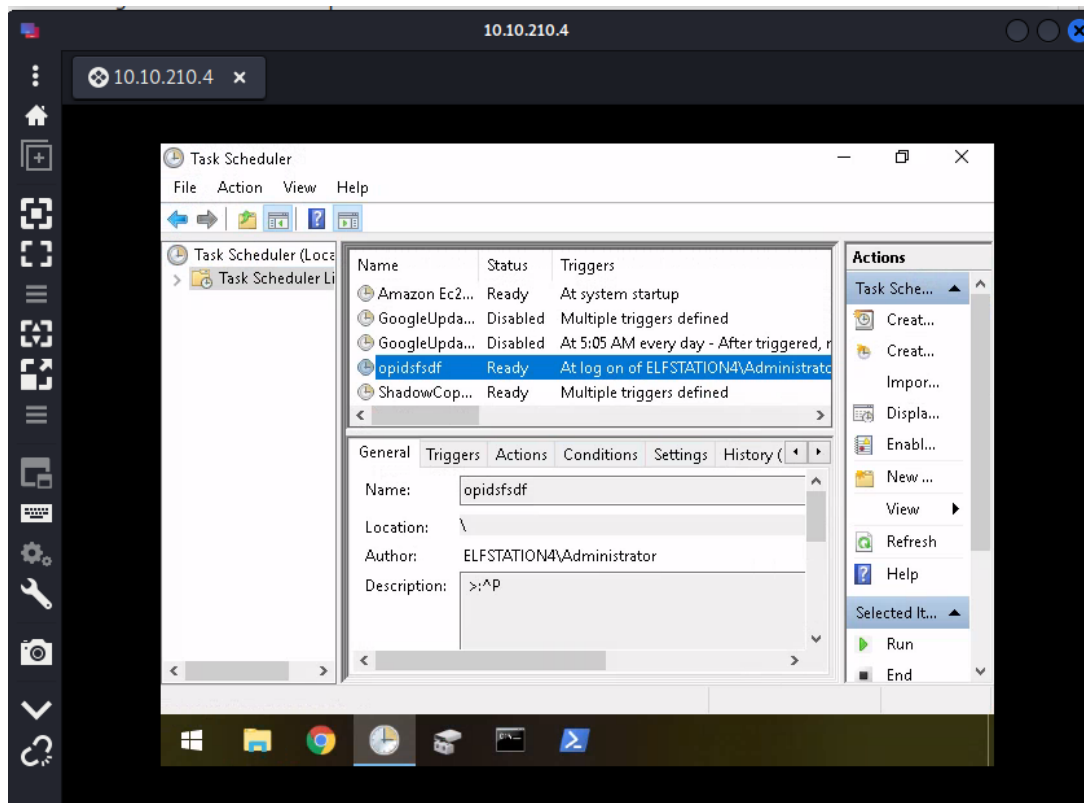
Go to file explorer and click on documents. Search for 'vStockings' and search every file in it.





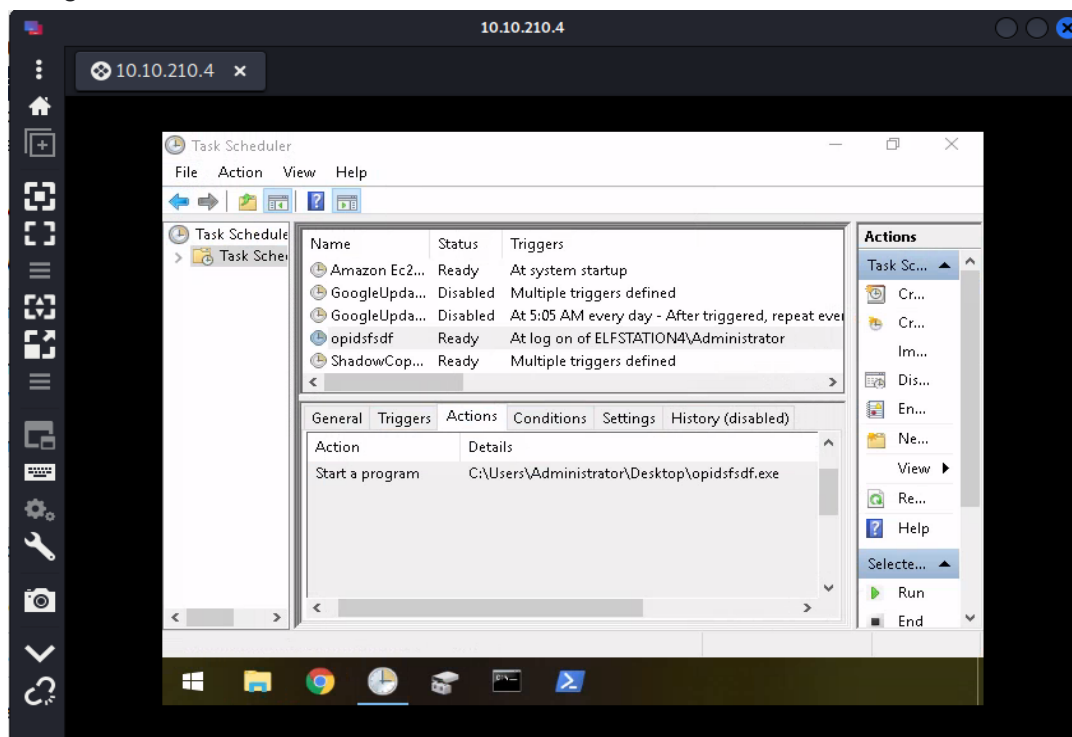
Answer:
.grinch

Question 4: What is the name of the suspicious scheduled task?
Go to Task Scheduler. Open library and inspect for suspicious task.



Answer:
opidsfsdf

Question 5: Inspect the properties of the scheduled task. What is the location of the executable that is run at login?
Navigate to Actions.

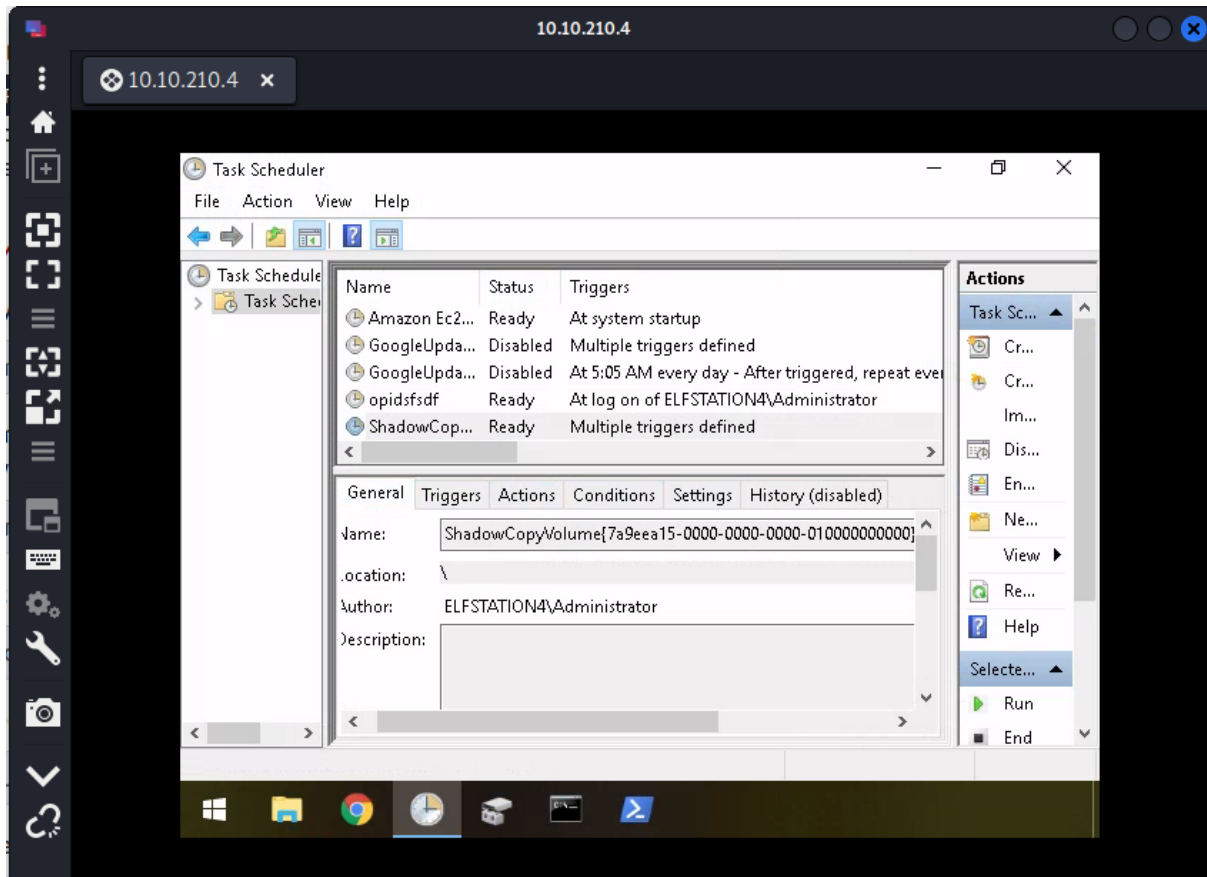


Answer :

C:\Users\Administrator\Desktop\opidsfsdf.exe

Question 6: There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?

Go to ShadowCopyVolume and navigate to General.

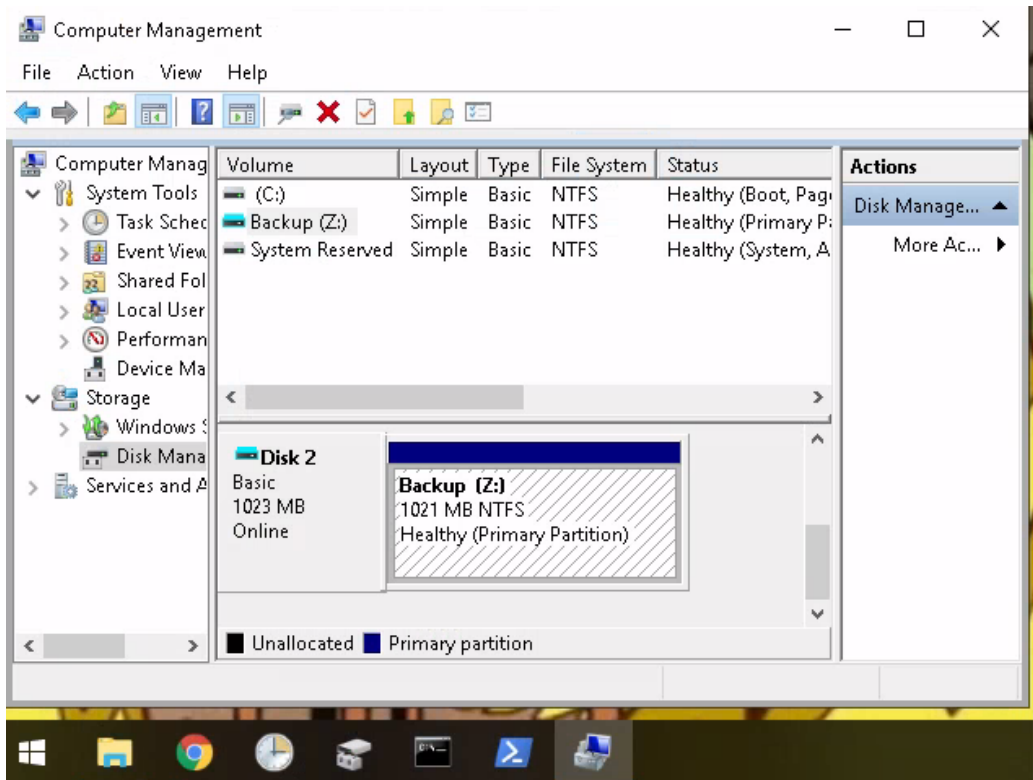


Answer :

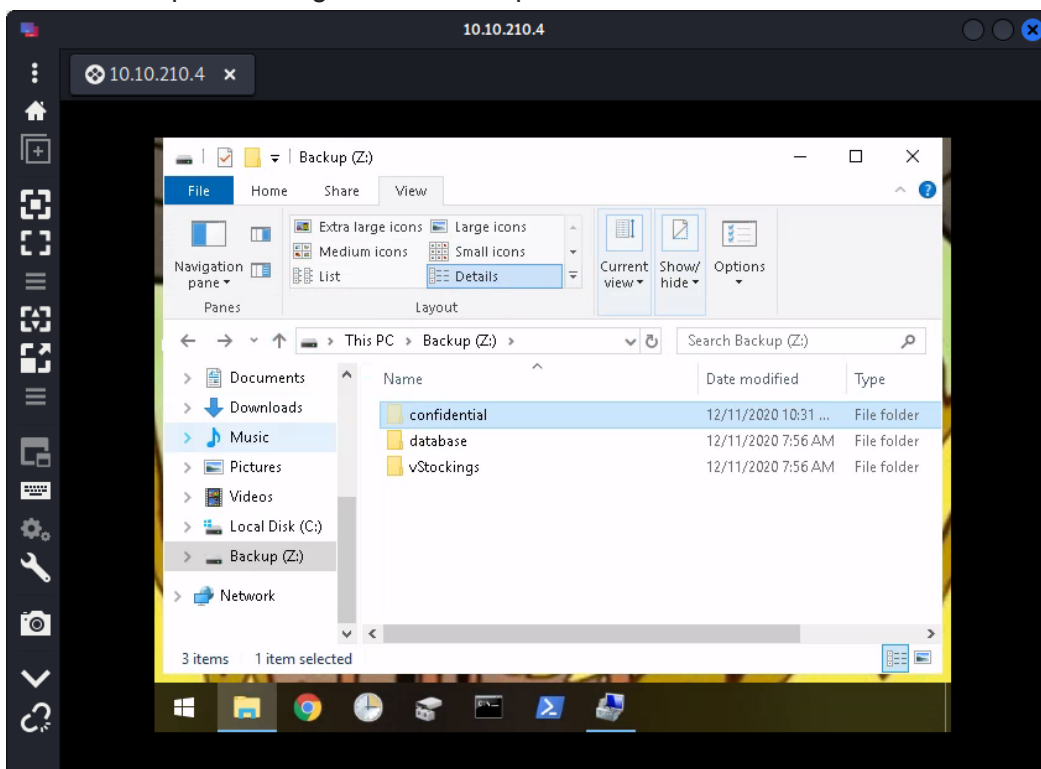
7a9eea15-0000-0000-0000-010000000000

Question 7 : Assign the hidden partition a letter. What is the name of the hidden folder?

Go to Computer Management. Search for Disk Management and go to Backup. From there, ChangeDrive Letter and Paths to any letter.



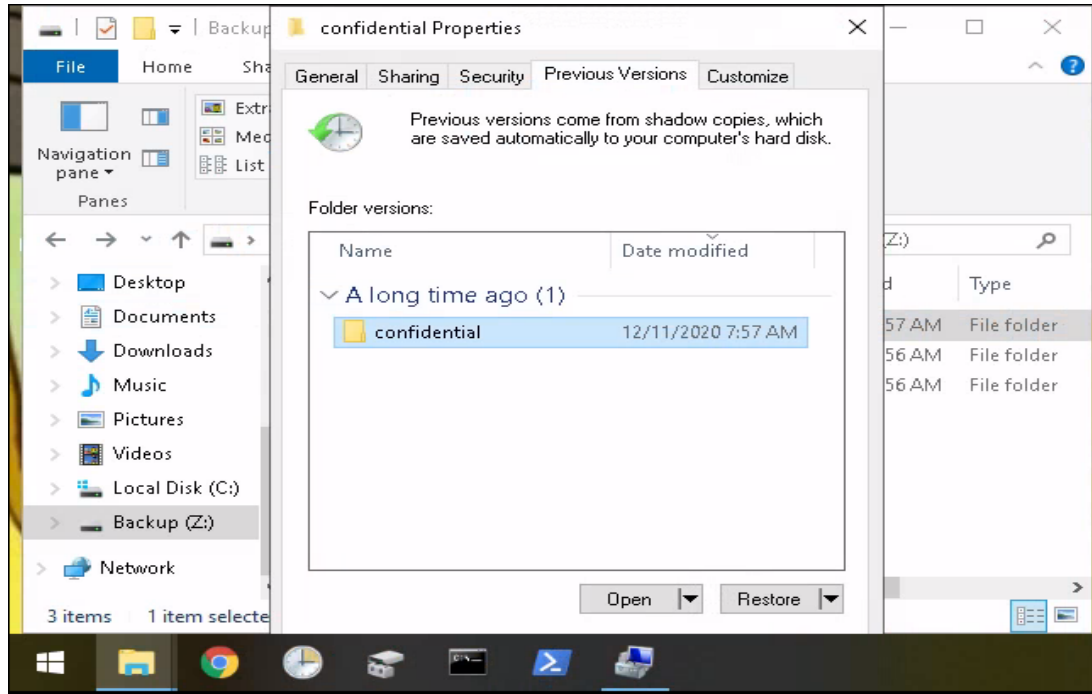
Go to File Explorer and go to the Backup. Then, show the hidden items.



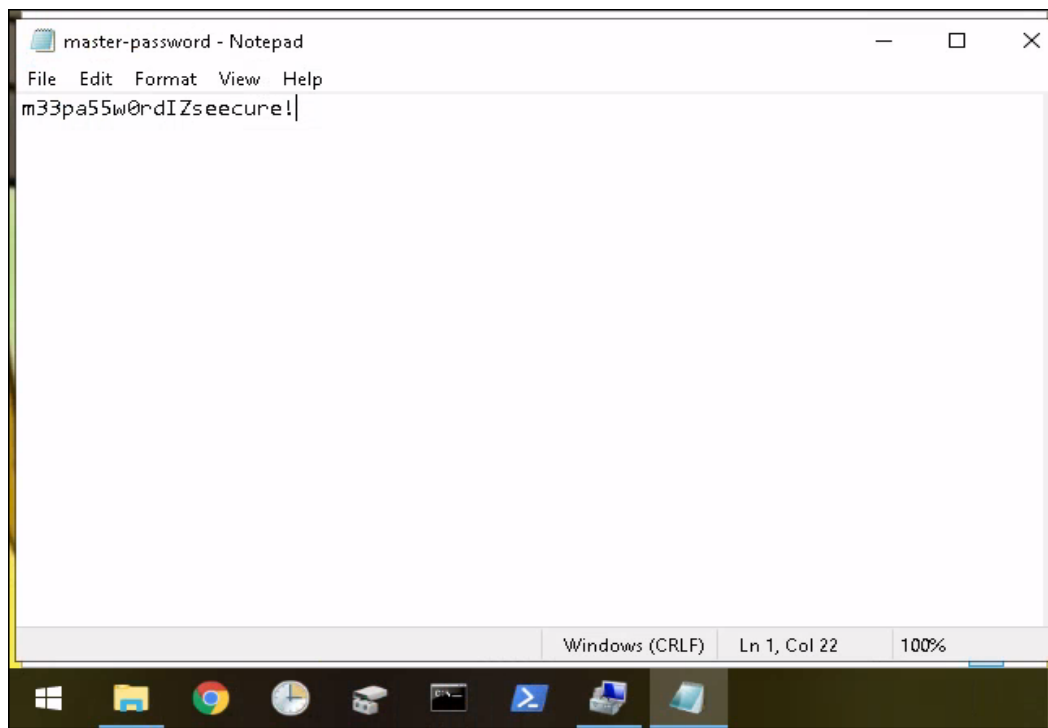
Answer:
confidential

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?

Go to properties of confidential and restore the file.



After restoring the file, go back and there would be a new file 'master password'.



Answer :
m33pa55w0rdIZsecure!

Thought/Processes:

Go to Remmina and fill in the details of IP address, username and password. After that, copy the note from RansomNote and paste into CyberChef to get the plain text value. Go to File Explorer and search for vStockings in Document. Then, we go to Task Scheduler and go to the library to find the suspicious task. Go to actions to get the location. We then go to ShadowCopyVolume and copy the ID. In Computer Management, change the letter of Backup. Then go to the Backup in File Explorer and show the hidden files. Restore the hidden file to get the master password.

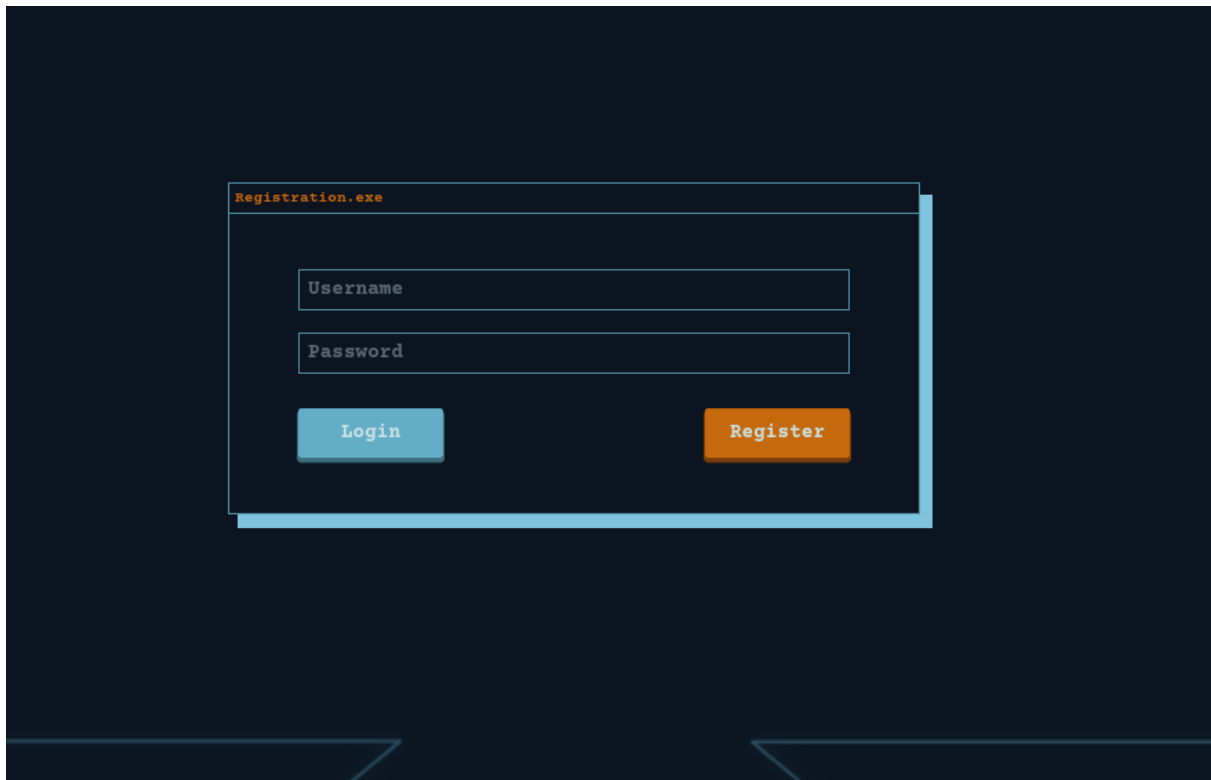
Day 24: The Trial Before Christmas

Q1: Scan the machine. What ports are open?

```
(kali㉿kali)-[~]  
$ sudo nmap 10.10.177.241  
[sudo] password for kali:  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-23 23:00 EDT  
Nmap scan report for 10.10.177.241  
Host is up (0.21s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
80/tcp    open  http  
65000/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 26.21 seconds
```

Answer: port 80 and 65000 are open

Q2: What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.

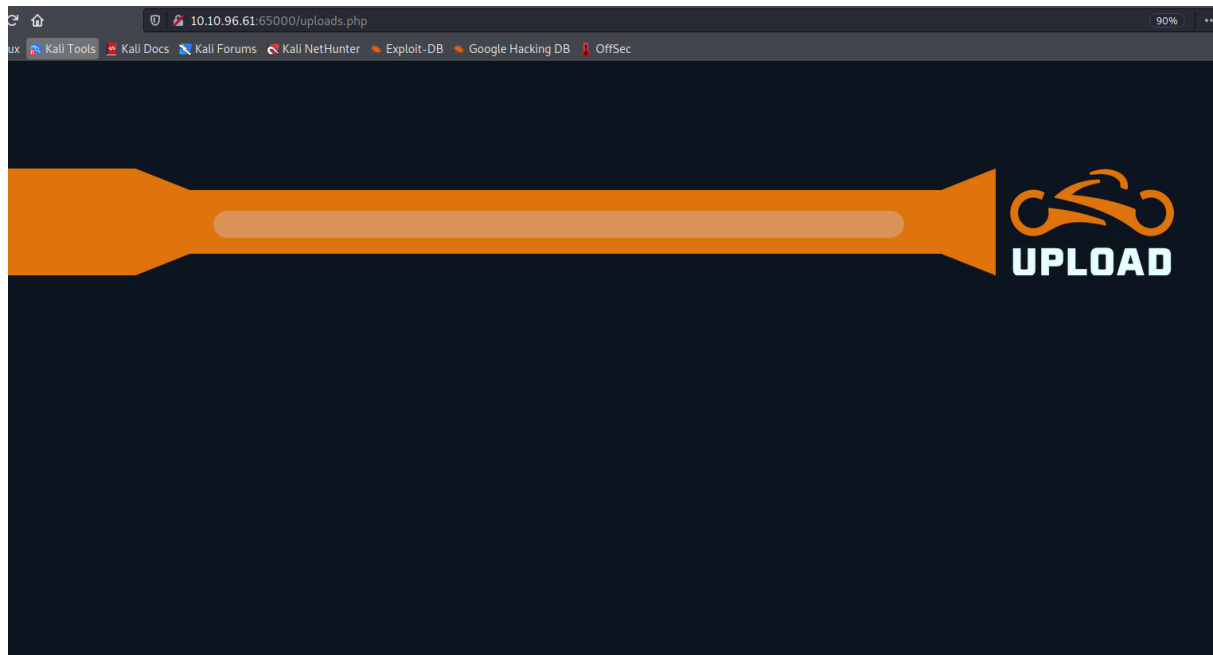


By entering port 65000, I gain access to this hidden website with the title Light Cycle

Answer: Light Cycle

Q3: What is the name of the hidden php page?

Using gobuster with big.txt on the url in the terminal, there returned a list of directories



After testing each of them, uploads.php was found to be the hidden php page

Answer: /uploads.php

AQ4: What is the name of the hidden directory where file uploads are saved?

For this, we will have to use reverse shell php

generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Regenerate CA certificate

Requests

Role which requests are stalled for viewing and editing in the Intercept tab.

Based on the following rules:

id	Operator	Match type	Match condition
1	And	File extension	Does not match
2	Or	Request	Content-Type
3	Or	HTTP method	Does not match
4	And	URL	Is in

Remove trailing or superfluous new lines at end of request

Content-Length header when the request is edited

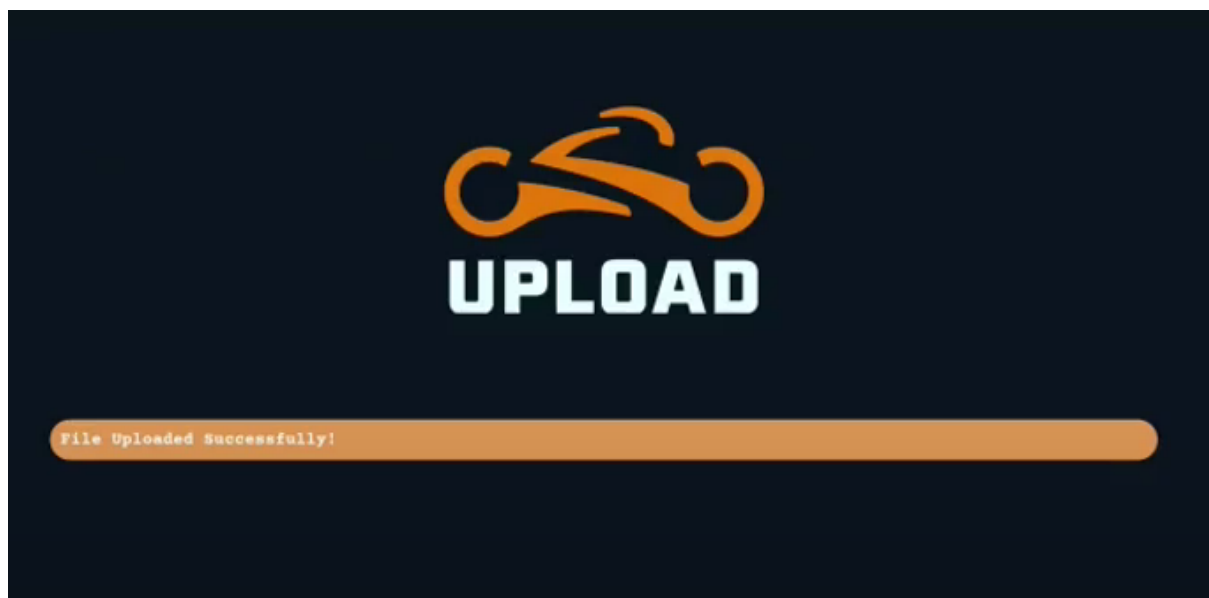
Responses

Role which responses are stalled for viewing and editing in the Intercept tab.

Based on the following rules:

Delete ^js\$ so that it can be intercepted

After uploading and then forwarding in burpsuite, I was able to upload the reverse shell php



It has appeared in grid where file uploads are found

Answer: /grid

Q5: What is the value of the web.txt flag?

Running `python3 -c 'import pty;pty.spawn("/bin/bash")'` spawns a new shell with the host name, then to get access to other commands like clear, run the command `export TERM=xterm`

```
www-data@light-cycle:/$ ls
bin   home   lib64   opt    sbin    sys    vmlinuz
boot  initrd.img  lost+found  proc  snap    tmp    vmlinuz.old
dev   initrd.img.old  media    root  srv     usr
etc   lib      mnt      run   swapfile  var

www-data@light-cycle:/$ cd
bash: cd: HOME not set
www-data@light-cycle:/$ cd /var/www
www-data@light-cycle:/var/www$ ls
ENCOM  TheGrid  web.txt
www-data@light-cycle:/var/www$ cat web.txt
THM{ENTER THE GRID}
www-data@light-cycle:/var/www$
```

Answer: THM{ENTER_THE_GRID}

Q6: What lines are used to upgrade and stabilize your shell?

- ☐ `SELECT * FROM users;`
- ☒ `stty raw -echo; fg`
- ☐ `mysql -uUSERNAME -p`
- ☒ `export TERM=xterm`
- ☒ `python3 -c 'import pty;pty.spawn("/bin/bash")'`
- ☐ `lxc exec CONTAINERNAME /bin/sh`

Q7: Review the configuration files for the webserver to find some useful loot in the form of credentials. What credentials do you find? **Username:password**

The credential info can be found in dbauth.php

```
File Actions Edit View Help
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 = "IFightForTheUsers";
    $database = "tron";

    $dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database);
    if($dbh->connect_error){
        die($dbh->connect_error);
    }
?>
www-data@light-cycle:/var/www/TheGrid/includes$
```

Answer: tron:IFightForTheUsers

Q8: Access the database and discover the encrypted credentials. What is the name of the database you find these in?

Answer: tron

Q9: Crack the password. What is it?

Crack the password by entering the encrypted password into a password hash cracker

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

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

[Download CrackStation's Wordlist](#)

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping

Answer: @computer@

Q10: Use su to login to the newly discovered user by exploiting password reuse. What is the user you are switching to?

Ans: flynn

Q11: What is the value of the user.txt flag?

It can be found in user.txt

```
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$
```

Ans: THM{IDENTITY_DISC_RECOGNISED}

Q12: Check the user's groups. Which group can be leveraged to escalate privileges?

Ans: lxd

Q13: What is the value of the root.txt flag?

```
/bin/sh: whoami: not found
- # whoami
root
~ # cd /mnt/root/root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}
```

Ans: THM{FLYNN_LIVES}

Thought/Processes:

After using the nmap to find which ports are open, we find the hidden page with one of the ports, then using gobuster and big.txt using a command, we found the directories and the directory where the files are uploaded. Burpsuite is then used to bypass the filter which determine what file can be uploaded. Then after access to gained, we are able to find the username and password