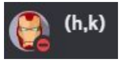
Fireside Friday's

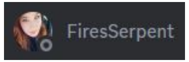
Series Overview & Windows CLI
Week 1

Thanks to our sponsors!

Antisyphon Training

Special Thanks to…

- Hermon 

- Emily 

- Both gave up many late nights to help with QA and development of this content
- Very much appreciate their efforts!
- Please give them a warm "thanks" the next time you see them online

Lab requirements for this section

- Modern Windows system
- Access to the command line (cmd.exe)

What this series will cover

- Networking & network security concepts
- Evaluating risk
- Network security architecture
- Network traffic control
- Network traffic monitoring
- Security testing
- Compliance and security frameworks

Our path to get there

- Expect sessions to run for 16-20 weeks
- One hour each Friday (same bat time, same bat channel)
- Will start with the basics and build up from there
- Want this to be a holistic class that fills in gaps
- What about after week 20?
  - I'll ask you what you want to learn :-)
  - Deeper dive on specific technologies if folks are interested
  - We refer to Antisyphon if training is already established

Why focus on secure network design?

- The network is what binds it all together
- Responsible for both functionality and security
- Challenging to troubleshoot/blue team/red team without understanding how it works
- May go down some rabbit holes when needed
  - Difference between stateful packet filtering & stateful inspection??
- But let's first start with the basics

Today's focus is Windows

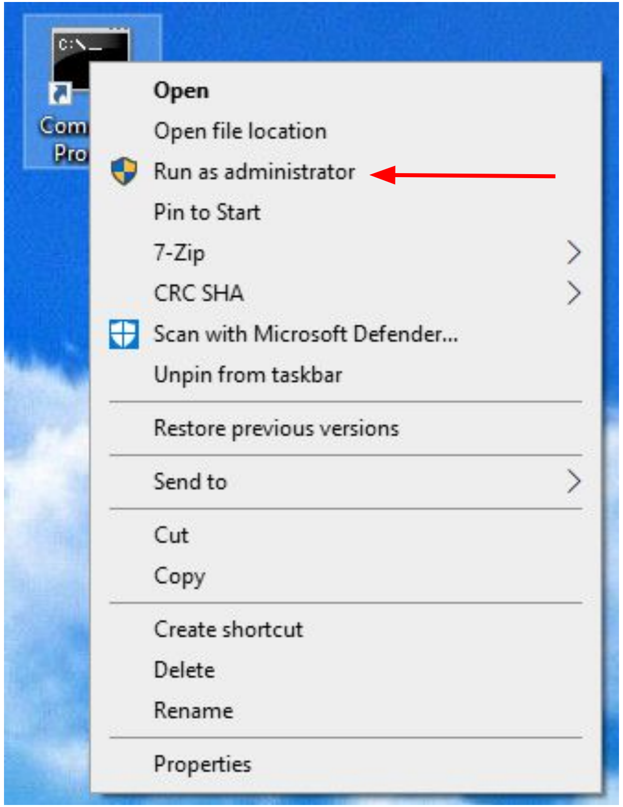
- Mostly Windows command line interface (CLI)
- Core skills needed for labs and troubleshooting
- Goal is to have folks comfortable working at the CMD

Run CMD as administrator

Pin to the Desktop
Right click icon
Select "Run as administrator"

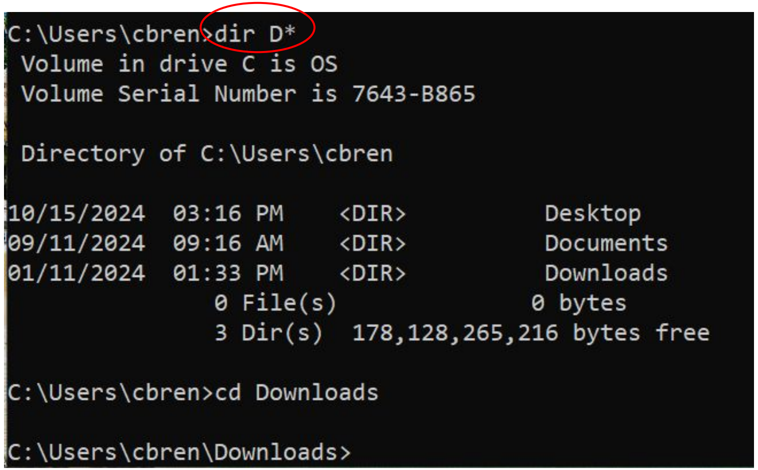
Some tools need high level permissions

Do this if what you are trying does not seem to work



Basic navigation

- dir = List contents of current directory
- cd <name> = Change directory
- cd .. = Move up 1 directory
- <tab> = Autocomplete cycle
- up/down arrow = cmd recall



```
C:\Users\cbren>dir D*
 Volume in drive C is OS
 Volume Serial Number is 7643-B865

 Directory of C:\Users\cbren

10/15/2024  03:16 PM    <DIR>          Desktop
09/11/2024  09:16 AM    <DIR>          Documents
01/11/2024  01:33 PM    <DIR>          Downloads
               0 File(s)              0 bytes
               3 Dir(s)  178,128,265,216 bytes free

C:\Users\cbren>cd Downloads

C:\Users\cbren\Downloads>
```

Listing files and directories

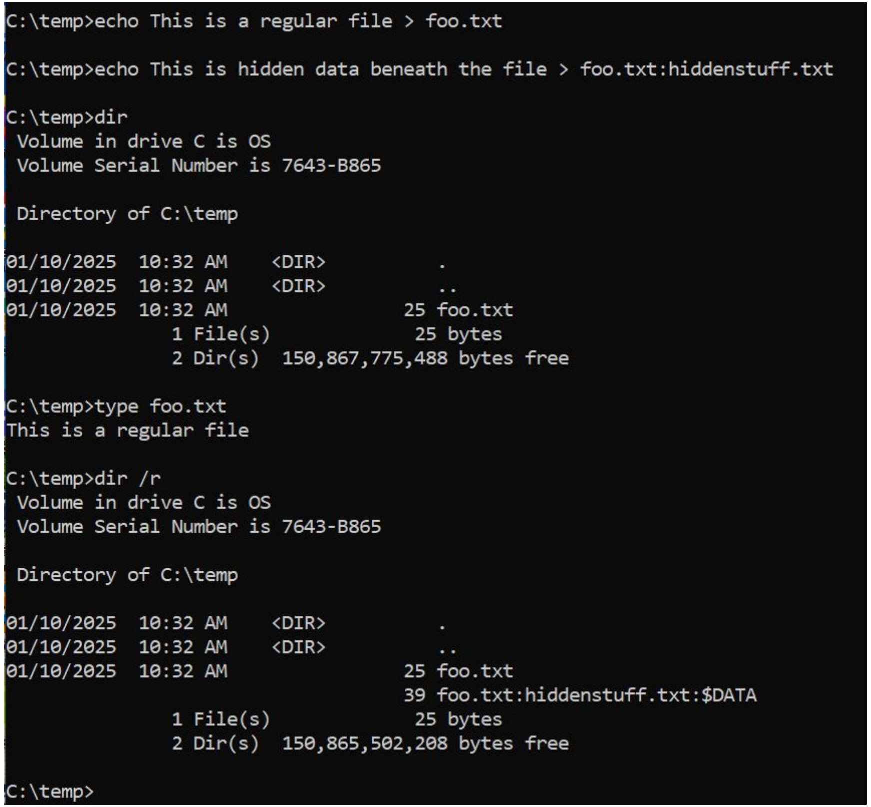
- dir /s | more = Show subdirectories and files, "q" to quit
- tree | more = Show directory structure
- more <file name> = Attempt to display contents of file
  - Works best with text based files
- cls = Clear the screen
- /? or -? or /h or -h = Help with command

Alternate data streams

- Hidden area under the main file system
- Can be used to hide data associated with a file
- Created to be compatible with Apple file system
- Used today for metadata on downloaded files
- Can also be used to hide info on a drive

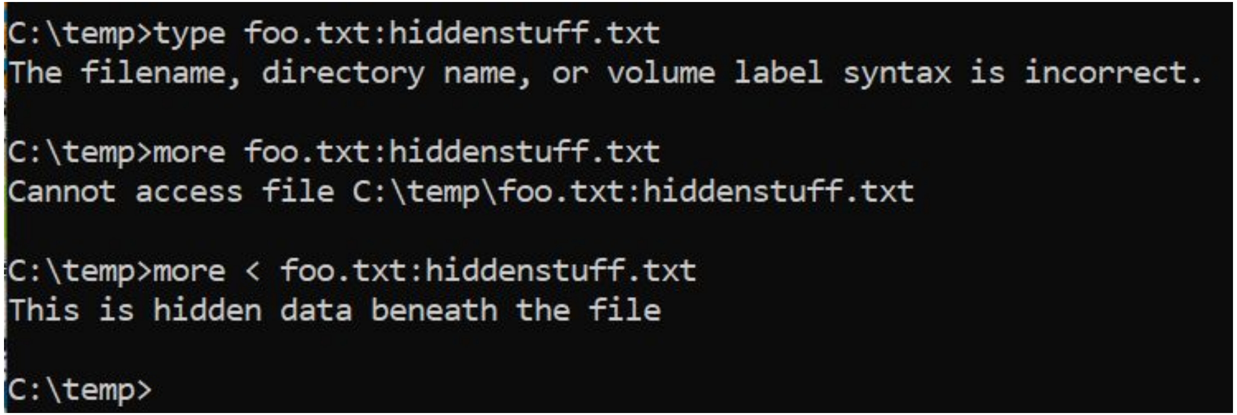
```
dir /s /r | findstr /e ":$DATA"
```

Working with alternate streams



```
C:\temp>echo This is a regular file > foo.txt

C:\temp>echo This is hidden data beneath the file > foo.txt:hiddenstuff.txt

C:\temp>dir
 Volume in drive C is OS
 Volume Serial Number is 7643-B865

 Directory of C:\temp

01/10/2025  10:32 AM    <DIR>          .
01/10/2025  10:32 AM    <DIR>          ..
01/10/2025  10:32 AM                25 foo.txt
               1 File(s)             25 bytes
               2 Dir(s)  150,867,775,488 bytes free

C:\temp>type foo.txt
This is a regular file

C:\temp>dir /r
 Volume in drive C is OS
 Volume Serial Number is 7643-B865

 Directory of C:\temp

01/10/2025  10:32 AM    <DIR>          .
01/10/2025  10:32 AM    <DIR>          ..
01/10/2025  10:32 AM                25 foo.txt
                                    39 foo.txt:hiddenstuff.txt:$DATA
               1 File(s)             25 bytes
               2 Dir(s)  150,865,502,208 bytes free

C:\temp>
```

How do I see that data?

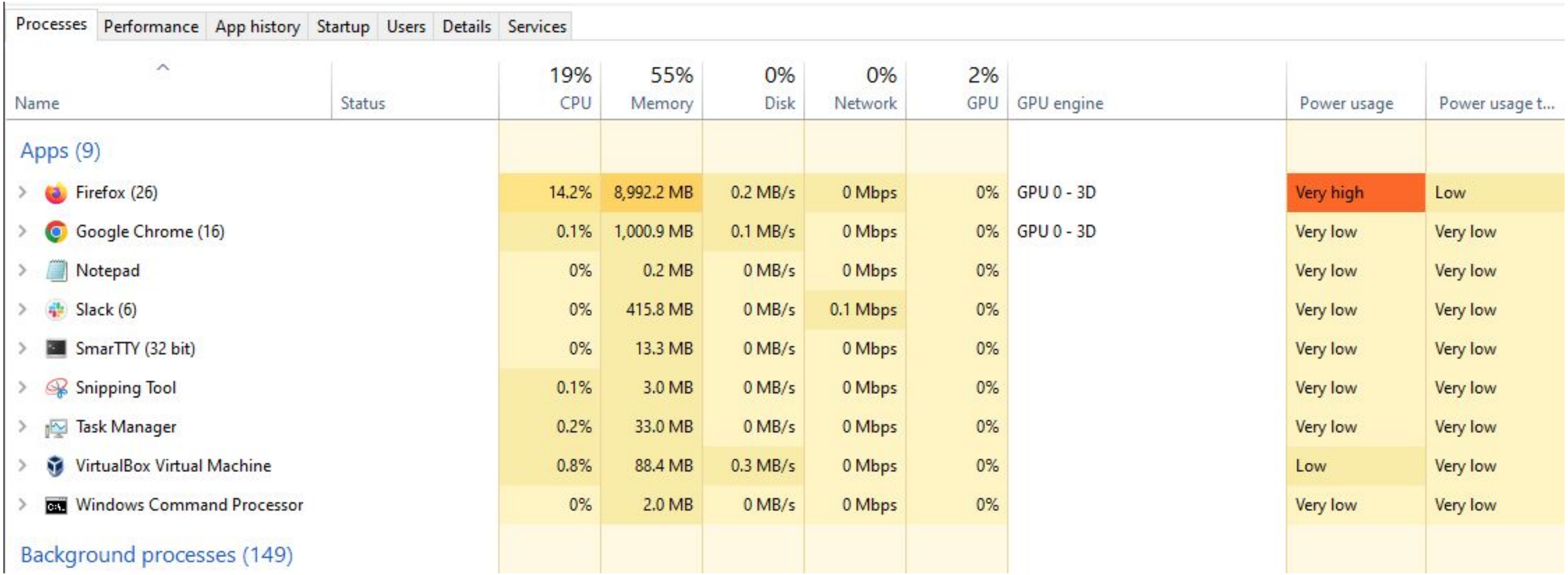


```
C:\temp>type foo.txt:hiddenstuff.txt
The filename, directory name, or volume label syntax is incorrect.

C:\temp>more foo.txt:hiddenstuff.txt
Cannot access file C:\temp\foo.txt:hiddenstuff.txt

C:\temp>more < foo.txt:hiddenstuff.txt
This is hidden data beneath the file

C:\temp>
```

"`notepad foo.txt:hiddenstuff.txt`" works as well

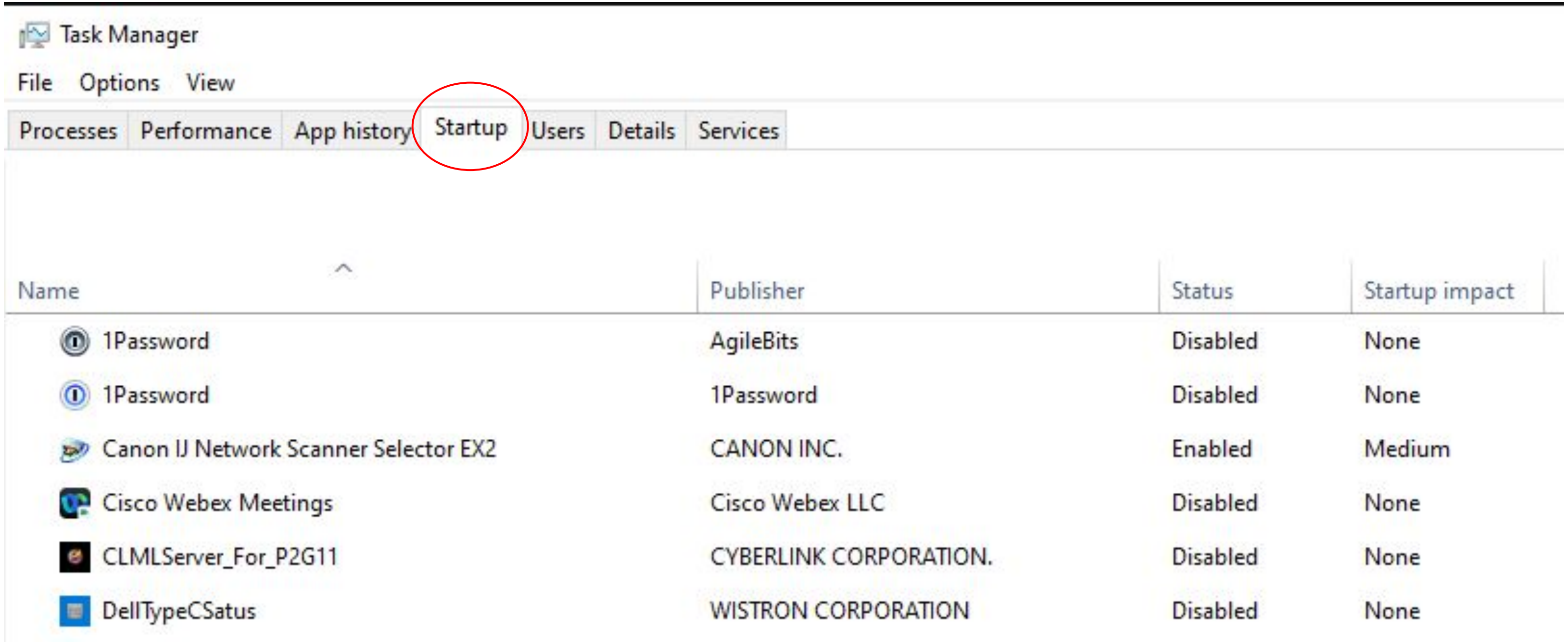
The Sysinternals toolkit has some useful ADS tools

taskmgr - What's running on my system?



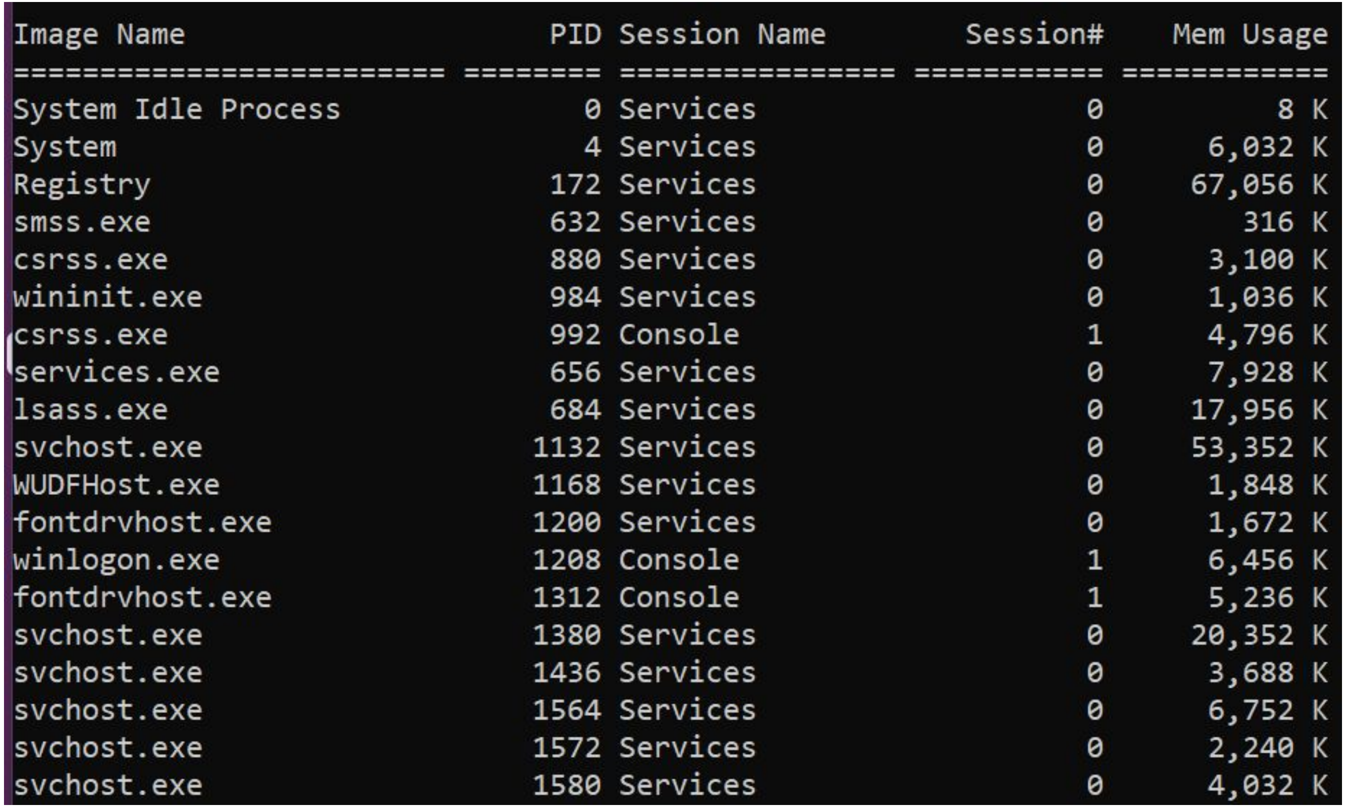
		19%	55%	0%	0%	2%			
Name	Status	CPU	Memory	Disk	Network	GPU	GPU engine	Power usage	Power usage t...
Apps (9)									
Firefox (26)		14.2%	8,992.2 MB	0.2 MB/s	0 Mbps	0%	GPU 0 - 3D	Very high	Low
Google Chrome (16)		0.1%	1,000.9 MB	0.1 MB/s	0 Mbps	0%	GPU 0 - 3D	Very low	Very low
Notepad		0%	0.2 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Slack (6)		0%	415.8 MB	0 MB/s	0.1 Mbps	0%		Very low	Very low
SmarTTY (32 bit)		0%	13.3 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Snipping Tool		0.1%	3.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Task Manager		0.2%	33.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
VirtualBox Virtual Machine		0.8%	88.4 MB	0.3 MB/s	0 Mbps	0%		Low	Very low
Windows Command Processor		0%	2.0 MB	0 MB/s	0 Mbps	0%		Very low	Very low
Background processes (149)									

What's loading at boot?


Task Manager
File Options View
Processes Performance App history Startup Users Details Services

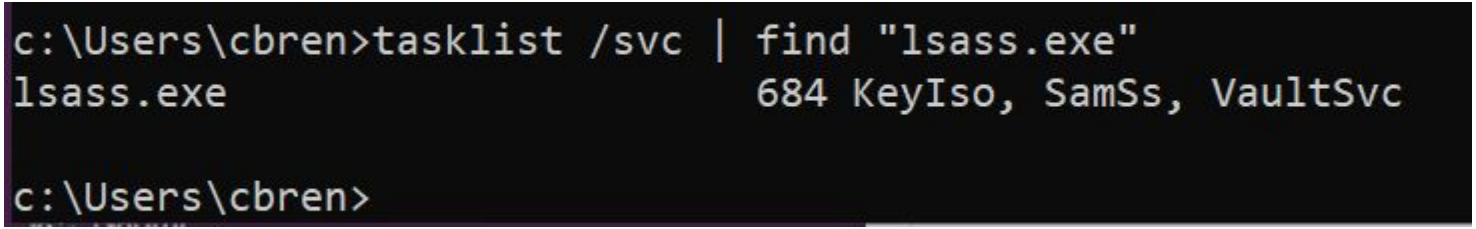
Name	Publisher	Status	Startup impact
1Password	AgileBits	Disabled	None
1Password	1Password	Disabled	None
Canon IJ Network Scanner Selector EX2	CANON INC.	Enabled	Medium
Cisco Webex Meetings	Cisco Webex LLC	Disabled	None
CLMLServer_For_P2G11	CYBERLINK CORPORATION.	Disabled	None
DellTypeCSatus	WISTRON CORPORATION	Disabled	None

tasklist - View running processes



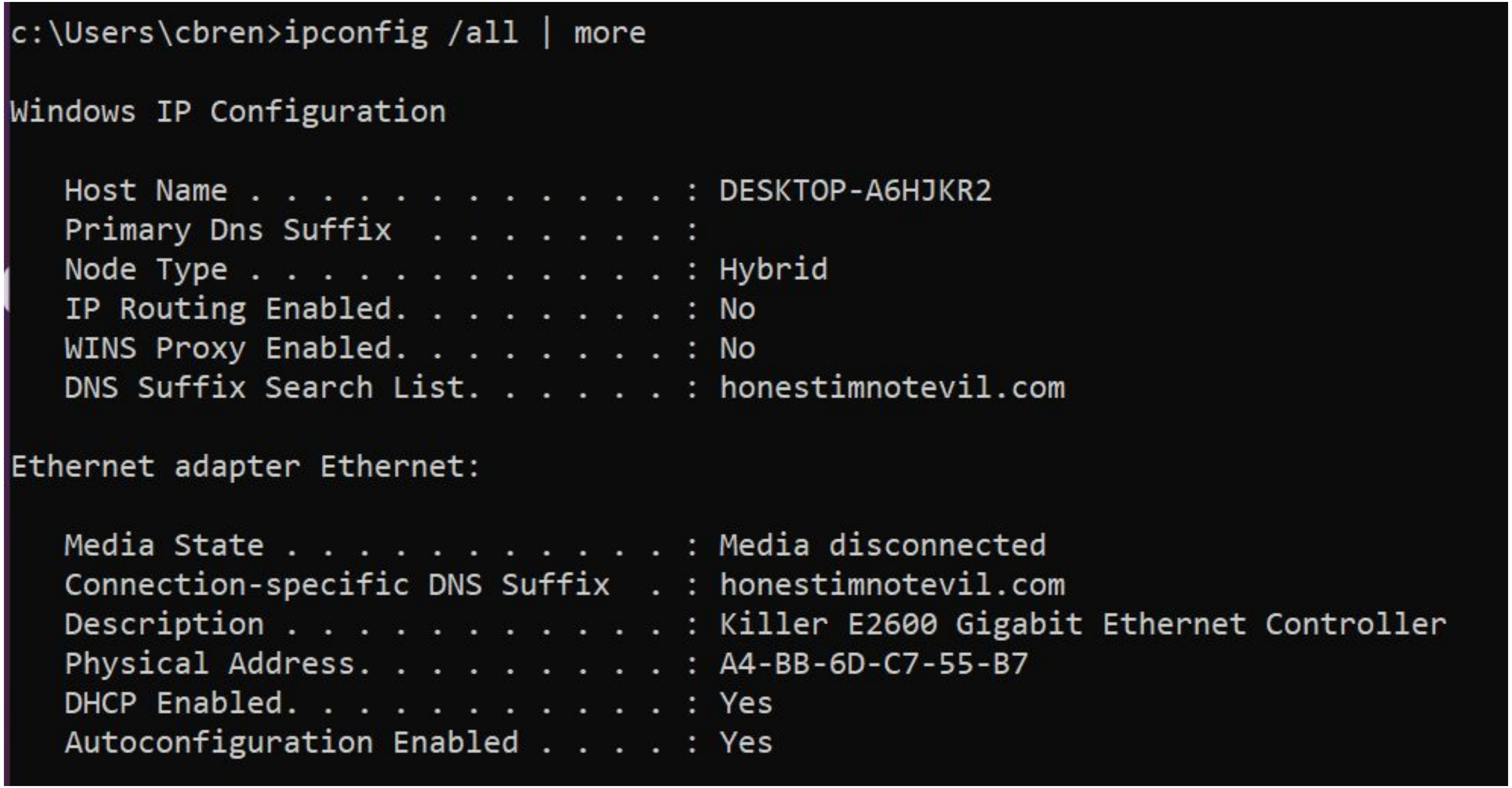
```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      6,032 K
Registry                       172 Services                   0     67,056 K
smss.exe                       632 Services                   0        316 K
csrss.exe                      880 Services                   0      3,100 K
wininit.exe                    984 Services                   0      1,036 K
csrss.exe                      992 Console                    1      4,796 K
services.exe                   656 Services                   0      7,928 K
lsass.exe                      684 Services                   0     17,956 K
svchost.exe                   1132 Services                   0     53,352 K
WUDFHost.exe                  1168 Services                   0      1,848 K
fontdrvhost.exe               1200 Services                   0      1,672 K
winlogon.exe                  1208 Console                    1      6,456 K
fontdrvhost.exe               1312 Console                    1      5,236 K
svchost.exe                   1380 Services                   0     20,352 K
svchost.exe                   1436 Services                   0      3,688 K
svchost.exe                   1564 Services                   0      6,752 K
svchost.exe                   1572 Services                   0      2,240 K
svchost.exe                   1580 Services                   0      4,032 K
```

Finding sub processes



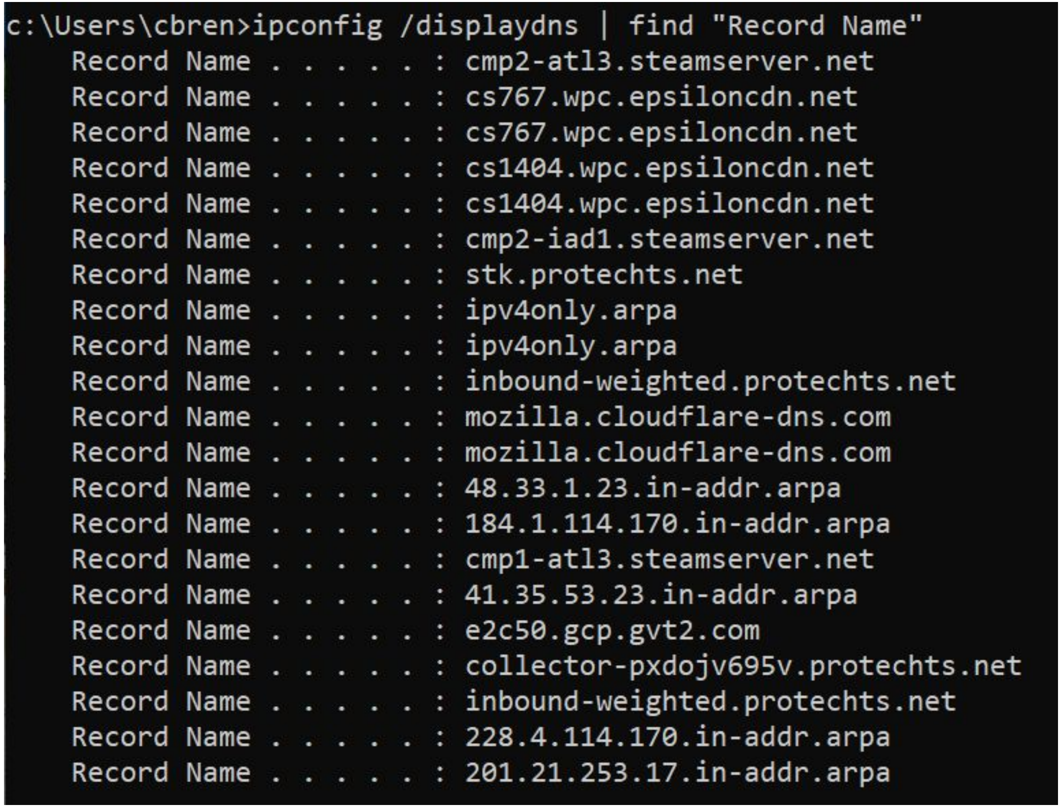
```
c:\Users\cbren>tasklist /svc | find "lsass.exe"
lsass.exe                    684 KeyIso, SamSs, VaultSvc

c:\Users\cbren>
```

IP info with ipconfig



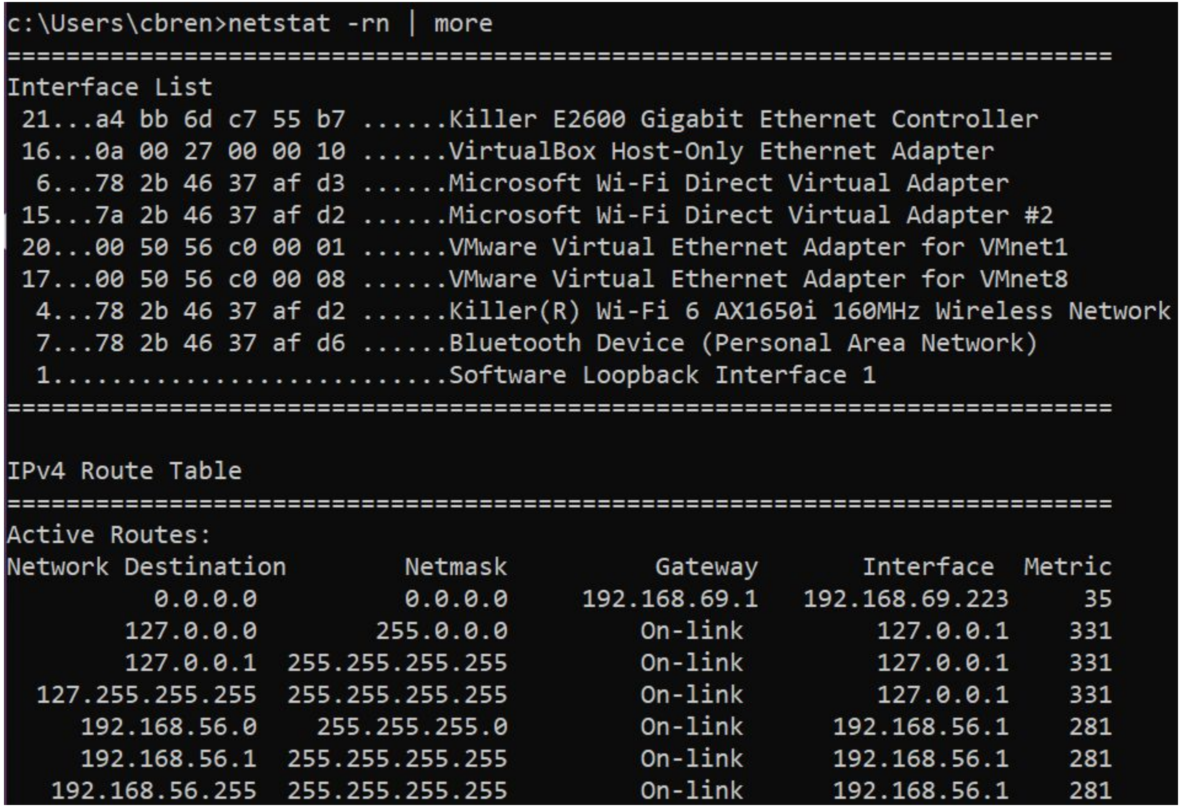
```
c:\Users\cbren>ipconfig /all | more

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-A6HJKR2
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : honestimnotevil.com

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : honestimnotevil.com
   Description . . . . . . . . . . . : Killer E2600 Gigabit Ethernet Controller
   Physical Address. . . . . . . . . : A4-BB-6D-C7-55-B7
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

Cached DNS queries with ipconfig



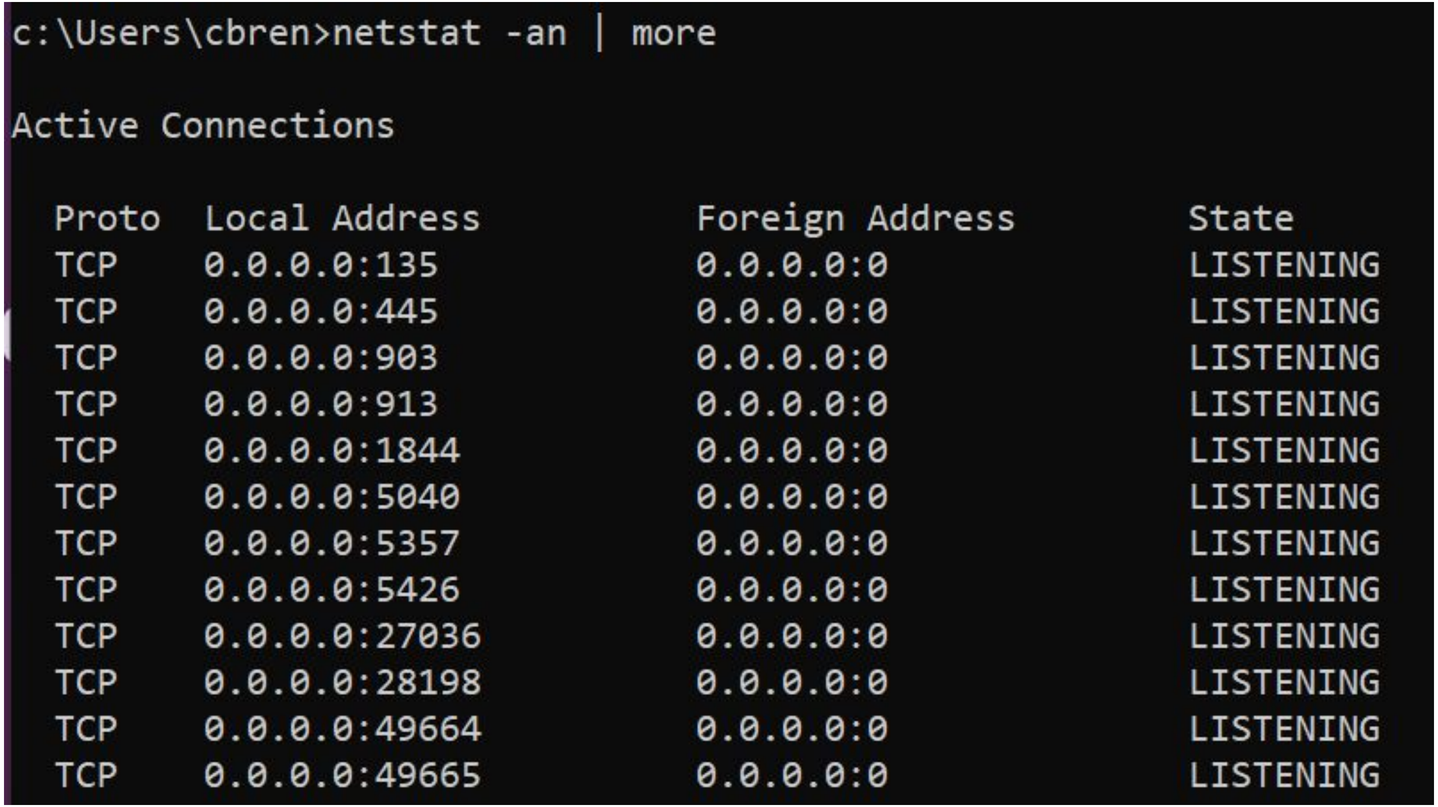
```
c:\Users\cbren>ipconfig /displaydns | find "Record Name"
    Record Name . . . . . : cmp2-atl3.steamserver.net
    Record Name . . . . . : cs767.wpc.epsiloncdn.net
    Record Name . . . . . : cs767.wpc.epsiloncdn.net
    Record Name . . . . . : cs1404.wpc.epsiloncdn.net
    Record Name . . . . . : cs1404.wpc.epsiloncdn.net
    Record Name . . . . . : cmp2-iad1.steamserver.net
    Record Name . . . . . : stk.protechts.net
    Record Name . . . . . : ipv4only.arpa
    Record Name . . . . . : ipv4only.arpa
    Record Name . . . . . : inbound-weighted.protechts.net
    Record Name . . . . . : mozilla.cloudflare-dns.com
    Record Name . . . . . : mozilla.cloudflare-dns.com
    Record Name . . . . . : 48.33.1.23.in-addr.arpa
    Record Name . . . . . : 184.1.114.170.in-addr.arpa
    Record Name . . . . . : cmp1-atl3.steamserver.net
    Record Name . . . . . : 41.35.53.23.in-addr.arpa
    Record Name . . . . . : e2c50.gcp.gvt2.com
    Record Name . . . . . : collector-pxdojv695v.protechts.net
    Record Name . . . . . : inbound-weighted.protechts.net
    Record Name . . . . . : 228.4.114.170.in-addr.arpa
    Record Name . . . . . : 201.21.253.17.in-addr.arpa
```

Interfaces & networks with netstat



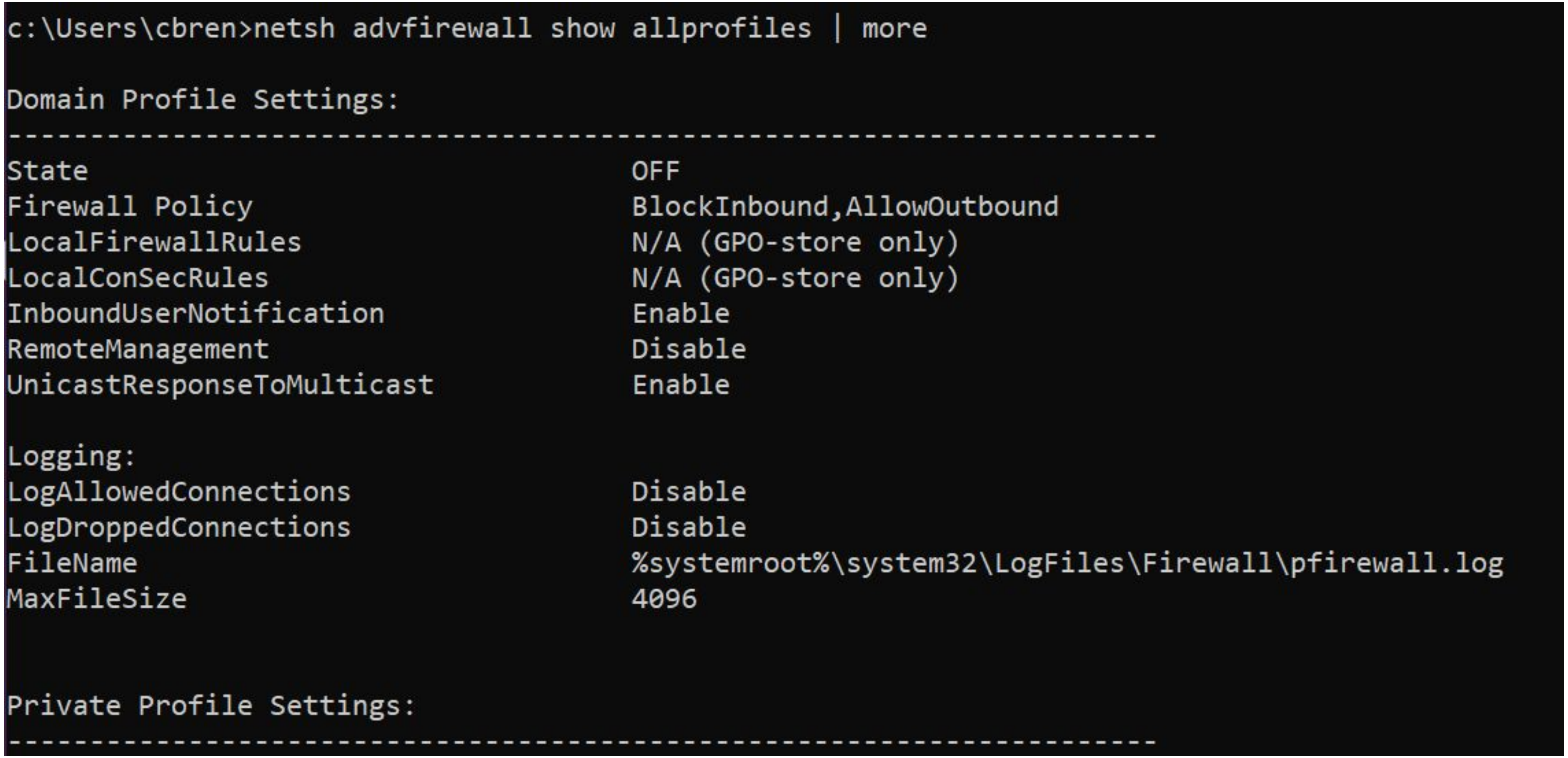
```
c:\Users\cbren>netstat -rn | more
===========================================================================
Interface List
 21...a4 bb 6d c7 55 b7 ......Killer E2600 Gigabit Ethernet Controller
 16...0a 00 27 00 00 10 ......VirtualBox Host-Only Ethernet Adapter
  6...78 2b 46 37 af d3 ......Microsoft Wi-Fi Direct Virtual Adapter
 15...7a 2b 46 37 af d2 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 20...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 17...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  4...78 2b 46 37 af d2 ......Killer(R) Wi-Fi 6 AX1650i 160MHz Wireless Network
  7...78 2b 46 37 af d6 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.69.1   192.168.69.223     35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link      192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link      192.168.56.1    281
```

What ports are open with netstat



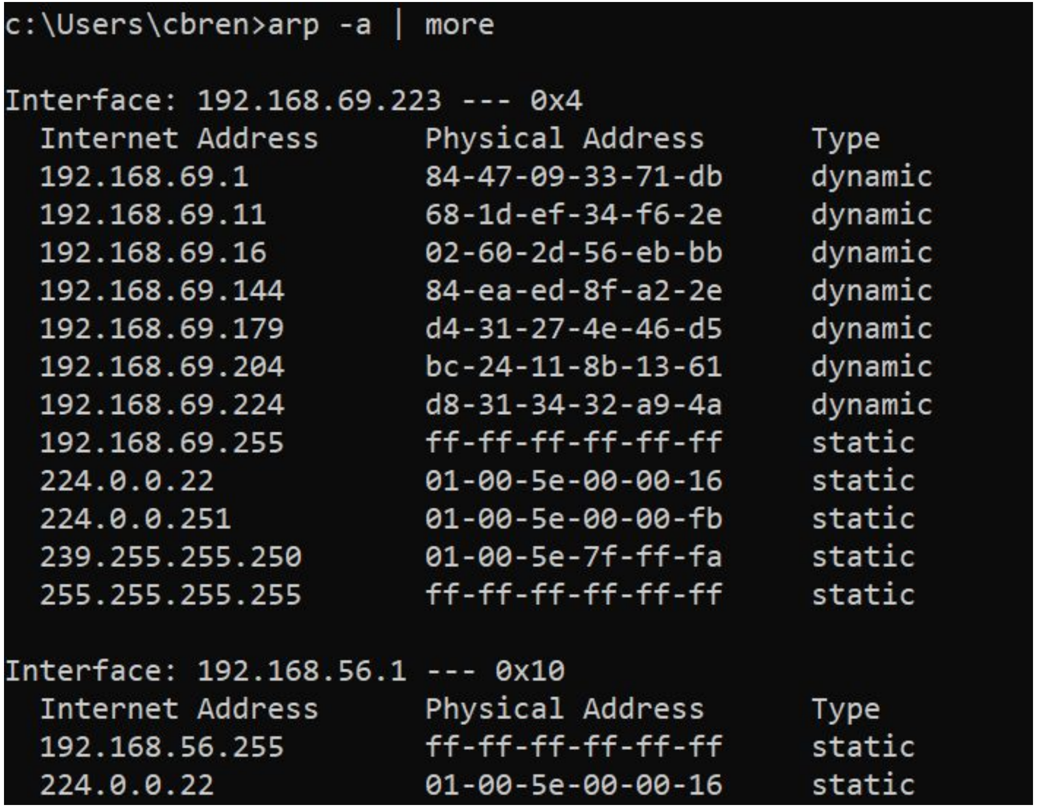
```
c:\Users\cbren>netstat -an | more

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:903            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:913            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1844           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5426           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:27036          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:28198          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
```

Firewall settings with netsh



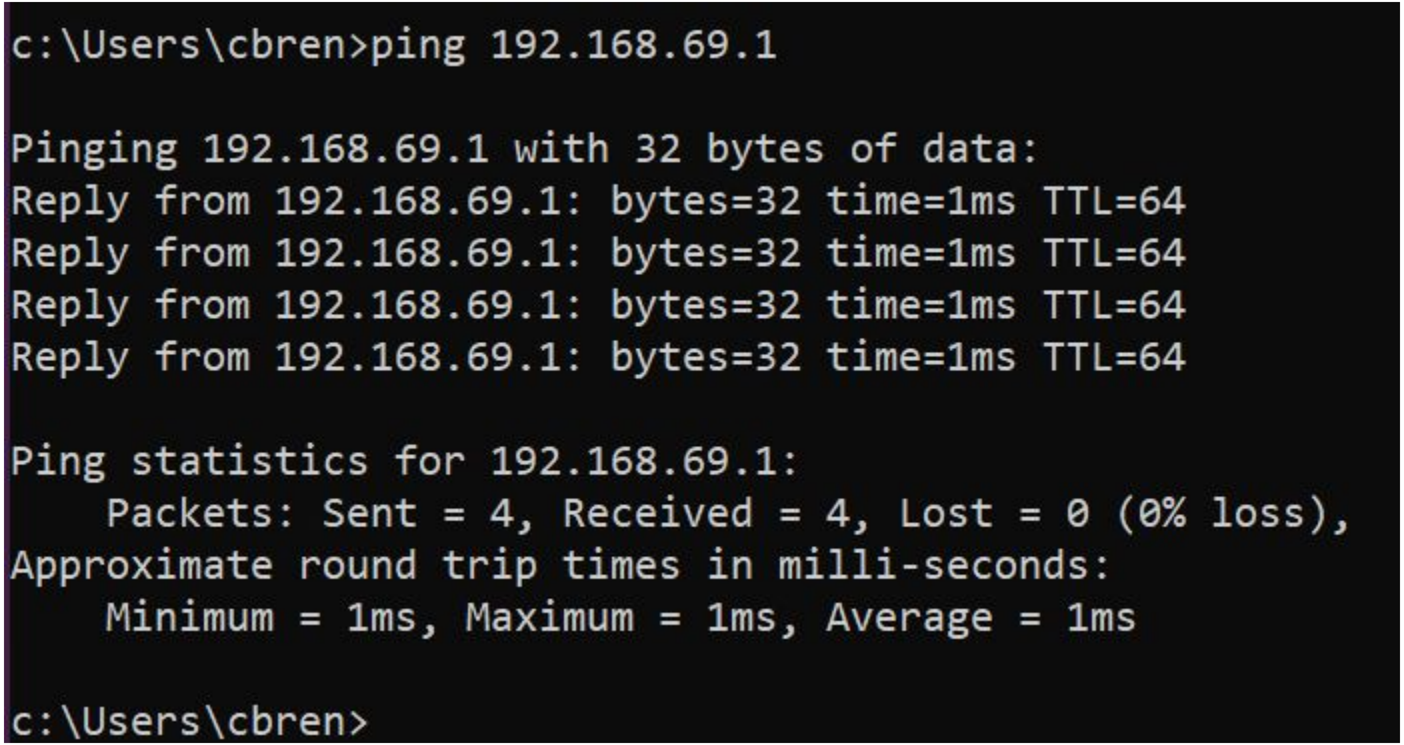
```
c:\Users\cbren>netsh advfirewall show allprofiles | more

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:
----------------------------------------------------------------------
```

Finding local systems with arp



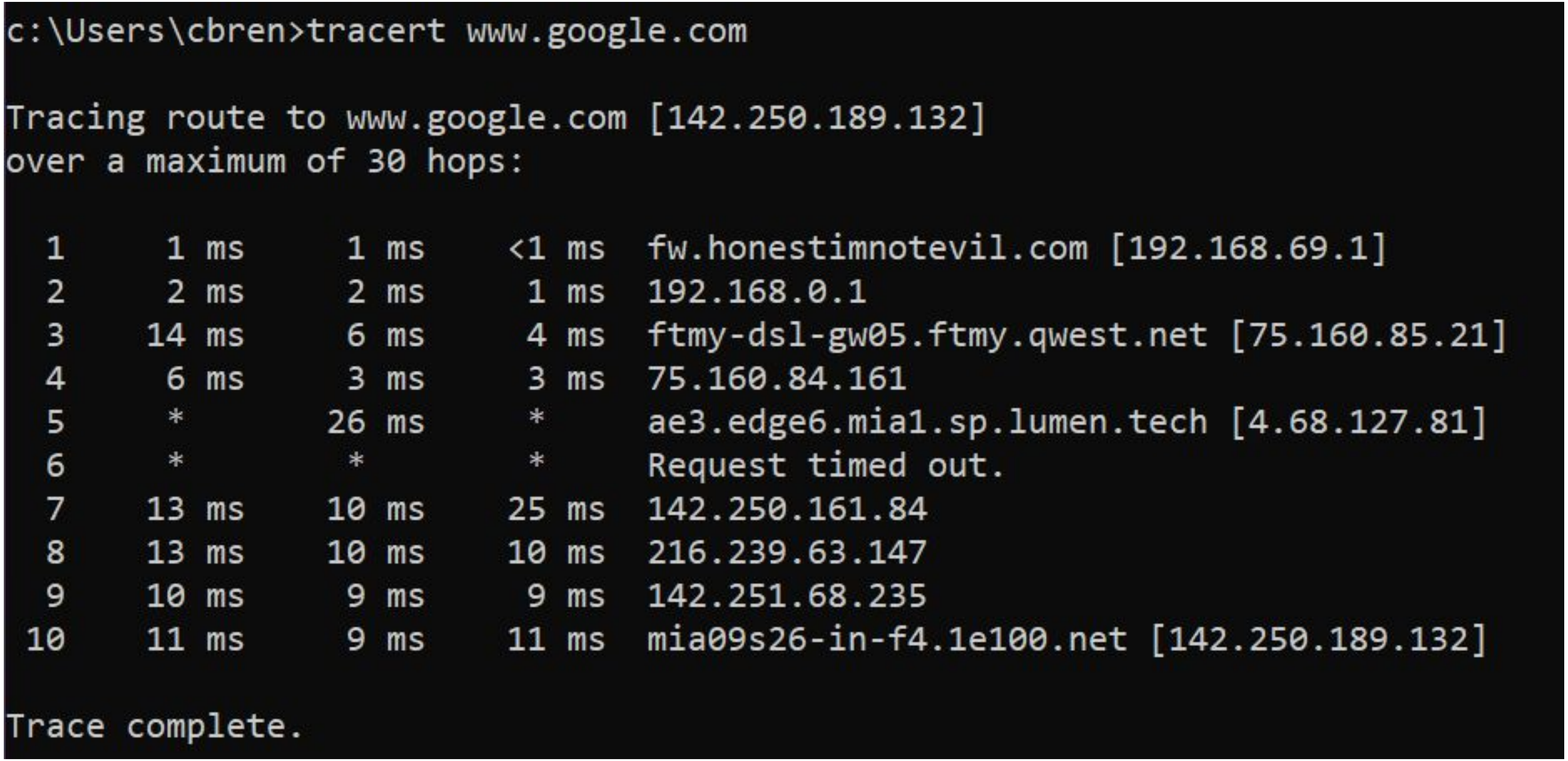
```
c:\Users\cbren>arp -a | more

Interface: 192.168.69.223 --- 0x4
  Internet Address      Physical Address      Type
  192.168.69.1          84-47-09-33-71-db     dynamic
  192.168.69.11         68-1d-ef-34-f6-2e     dynamic
  192.168.69.16         02-60-2d-56-eb-bb     dynamic
  192.168.69.144        84-ea-ed-8f-a2-2e     dynamic
  192.168.69.179        d4-31-27-4e-46-d5     dynamic
  192.168.69.204        bc-24-11-8b-13-61     dynamic
  192.168.69.224        d8-31-34-32-a9-4a     dynamic
  192.168.69.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0x10
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
```

Check connectivity with ping



```
c:\Users\cbren>ping 192.168.69.1

Pinging 192.168.69.1 with 32 bytes of data:
Reply from 192.168.69.1: bytes=32 time=1ms TTL=64
Reply from 192.168.69.1: bytes=32 time=1ms TTL=64
Reply from 192.168.69.1: bytes=32 time=1ms TTL=64
Reply from 192.168.69.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.69.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

c:\Users\cbren>
```

Check networks with tracert



```
c:\Users\cbren>tracert www.google.com

Tracing route to www.google.com [142.250.189.132]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  fw.honestimnotevil.com [192.168.69.1]
  2     2 ms     2 ms     1 ms  192.168.0.1
  3    14 ms     6 ms     4 ms  ftmy-dsl-gw05.ftmy.qwest.net [75.160.85.21]
  4     6 ms     3 ms     3 ms  75.160.84.161
  5     *       26 ms     *     ae3.edge6.mia1.sp.lumen.tech [4.68.127.81]
  6     *        *        *     Request timed out.
  7    13 ms    10 ms    25 ms  142.250.161.84
  8    13 ms    10 ms    10 ms  216.239.63.147
  9    10 ms     9 ms     9 ms  142.251.68.235
 10    11 ms     9 ms    11 ms  mia09s26-in-f4.1e100.net [142.250.189.132]

Trace complete.
```

Wrap up

- Thank you for attending!
- Certs & video usually go out in 24 hours
- If you have any lingering questions, the Discord channel will remain active
    - Also a good chance to socialize with others in the class
    - Have other tips and tricks? Please share with others!
    - Posting screenshots can be helpful :-)