Windows Endpoint Analysis

Windows: When Bad Things Happen

- In this section we will go through some core “live forensics” commands
- These are commands you should know and love
- They can mean the difference between a quick incident and a long painful one
- They can mean the difference between knowing, and just staring at a screen waiting for blinky lights to tell you things

Start with network connections

- We begin by looking at our system as a big, haystack
- Knowing where to start can be overwhelming
- I recommend starting with the network connections and then working backwards
- You have to start somewhere
- Core Windows network commands to know
    - netstat
    - net view
    - net use
    - net session

C:\> net view

- Let's start by looking at shares
- Attackers like to have staging systems on the inside of a network
- Pull files to one location and then exfil out
- What is normal?

C:\> net session

- Who is currently talking with the current system?
- X -> Y -> Z: You may be investigating system Y. But, it is compromised via system X
- Don’t think of incidents as just isolated systems to be reviewed
- Attacks are often a chain

C:\> net use

- Who is the current system talking to?
- X -> Y -> Z: You may be investigating system Y. But, it is attacking system Z
- This is kind of the opposite of net session

C:\> netstat

- This one can get complicated… Quick
- But, it is a go to for any SOC analyst
- netstat will show you network connections

```
C:\Users\adhd>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.142.135:50371   52.242.211.89:https    ESTABLISHED
  TCP    172.16.142.135:50475   152.199.6.14:https     TIME_WAIT
  TCP    172.16.142.135:50521   dfw25s34-in-f2:https   TIME_WAIT
  TCP    172.16.142.135:50548   152.195.12.131:https   TIME_WAIT
  TCP    172.16.142.135:50865   a-0003:https           TIME_WAIT
  TCP    172.16.142.135:50866   a-0003:https           TIME_WAIT
  TCP    172.16.142.135:50879   a-0001:https           TIME_WAIT
  TCP    172.16.142.135:50880   a-0001:https           TIME_WAIT
  TCP    172.16.142.135:50881   a-0003:https           TIME_WAIT
  TCP    172.16.142.135:50882   a-0003:https           TIME_WAIT
  TCP    172.16.142.135:50884   media-router-fp74:https  TIME_WAIT
  TCP    172.16.142.135:50885   media-router-fp74:https  TIME_WAIT
  TCP    172.16.142.135:50888   192.229.211.216:https  TIME_WAIT
  TCP    172.16.142.135:50902   dfw25s34-in-f2:https   TIME_WAIT
```

C:\> netstat -naob

- Now we can see the open TCP and UDP connections
- -a: Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
- -n: Displays active TCP connections, however, addresses and port numbers are expressed numerically and no attempt is made to determine names
- -o: Displays active TCP connections and includes the process ID (PID) for each connection.
- -b: displays the executable involved in creating each connection or listening port.
- https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat

C:\> netstat -naob

```
C:\Users\adhd>netstat -naob

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       920
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       1064
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       700
 [lsass.exe]
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       524
 Can not obtain ownership information
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       736
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       380
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       1844
 [spoolsv.exe]
```


BLACK HILLS Information Security

Backdoors & Breaches

C:\> netstat -f

- -f shows the fully qualified domain name (when available)
- Does not work too well with -naob (unfortunately)
- Will require running netstat a few times and cross-referencing
- Saves a ton of time
- How about… You know, killing ads?
- Look for things “out of the ordinary”
  - Weird domains
  - Non-M$/Google/Yahoo connections
- Reduce the haystack, one piece at a time

C:\> netstat -f

```
C:\Users\adhd>netstat -f

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    172.16.142.135:50357   40.126.0.71:https      TIME_WAIT
  TCP    172.16.142.135:50366   40.126.0.71:https      TIME_WAIT
  TCP    172.16.142.135:50367   13.74.179.117:https    TIME_WAIT
  TCP    172.16.142.135:50368   gap-prime-finance.msn-int.com:https  TIME_WAIT
  TCP    172.16.142.135:50369   13.74.179.117:https    TIME_WAIT
  TCP    172.16.142.135:50370   13.74.179.117:https    TIME_WAIT
  TCP    172.16.142.135:50371   52.242.211.89:https    ESTABLISHED
  TCP    172.16.142.135:50378   dfw28s04-in-f3.1e100.net:https  TIME_WAIT
  TCP    172.16.142.135:50400   a-0003.a-msedge.net:https  TIME_WAIT
  TCP    172.16.142.135:50401   a-0003.a-msedge.net:https  TIME_WAIT
  TCP    172.16.142.135:50402   13.74.179.117:https    TIME_WAIT
  TCP    172.16.142.135:50412   a-0001.a-msedge.net:https  TIME_WAIT
  TCP    172.16.142.135:50414   a23-64-5-158.deploy.static.akamaitechnologies.com:https  CLOSE_WAIT
  TCP    172.16.142.135:50415   a23-64-5-158.deploy.static.akamaitechnologies.com:https  ESTABLISHED
  TCP    172.16.142.135:50416   40.81.45.29:https      ESTABLISHED
  TCP    172.16.142.135:50417   40.81.45.29:https      ESTABLISHED
  TCP    172.16.142.135:50418   a-0003.a-msedge.net:https  ESTABLISHED
  TCP    172.16.142.135:50419   a-0003.a-msedge.net:https  ESTABLISHED
  TCP    172.16.142.135:50422   a-0001.a-msedge.net:https  ESTABLISHED
  TCP    172.16.142.135:50423   a-0001.a-msedge.net:https  ESTABLISHED
  TCP    172.16.142.135:50424   40.77.18.167:https     ESTABLISHED
  TCP    172.16.142.135:50427   a-0003.a-msedge.net:https  ESTABLISHED
  TCP    172.16.142.135:50428   a-0003.a-msedge.net:https  ESTABLISHED
  TCP    172.16.142.135:50431   13.107.21.200:https    ESTABLISHED
  TCP    172.16.142.135:50432   13.107.21.200:https    ESTABLISHED
```

Windows Processes

- After we have looked at the network connections, we need to drill down on the processes
- Hopefully, we have a handful of “suspect” network connections
- Armed with the data we get from commands like netstat -naob we can start to look at the actual process data
- Still can be a lot of data
- Takes time, practice, practice, practice
- Pro tip, do this first on a system that is not infected

C:\> tasklist

- Just about the most boring command ever… Or is it?

```
C:\Users\adhd>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0         96 K
Secure System                   48 Services                   0     12,404 K
Registry                        96 Services                   0     19,132 K
smss.exe                       308 Services                   0        908 K
csrss.exe                      448 Services                   0      2,768 K
wininit.exe                    524 Services                   0      3,584 K
csrss.exe                      540 Console                    1      3,096 K
winlogon.exe                   620 Console                    1      5,768 K
services.exe                   628 Services                   0      6,572 K
LsaIso.exe                     676 Services                   0      2,404 K
```

C:\> tasklist /svc

- Let's look at services!

```
C:\Users\adhd>tasklist /svc

Image Name                     PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
Secure System                   48 N/A
Registry                        96 N/A
smss.exe                       308 N/A
csrss.exe                      448 N/A
wininit.exe                    524 N/A
csrss.exe                      540 N/A
winlogon.exe                   620 N/A
services.exe                   628 N/A
LsaIso.exe                     676 N/A
lsass.exe                      700 KeyIso, SamSs, VaultSvc
fontdrvhost.exe                792 N/A
fontdrvhost.exe                800 N/A
svchost.exe                    808 BrokerInfrastructure, DcomLaunch, LSM,
                                   PlugPlay, Power, SystemEventsBroker
svchost.exe                    920 RpcEptMapper, RpcSs
dwm.exe                       1004 N/A
svchost.exe                    380 Appinfo, gpsvc, hns, IKEEXT, iphlpsvc,
                                   LanmanServer, lfsvc, ProfSvc, Schedule,
                                   SENS, SharedAccess, ShellHWDetection,
                                   Themes, TokenBroker, UserManager, UsoSvc,
                                   Winmgmt, wisvc, wlidsvc, WpnService,
```

C:\> tasklist /m

```
C:\Users\adhd>tasklist /m

Image Name                     PID Modules
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
Secure System                   48 N/A
Registry                        96 N/A
smss.exe                       308 N/A
csrss.exe                      448 N/A
wininit.exe                    524 N/A
csrss.exe                      540 N/A
winlogon.exe                   620 ntdll.dll, KERNEL32.DLL, KERNELBASE.dll,
                                   msvcrt.dll, sechost.dll, RPCRT4.dll,
                                   combase.dll, ucrtbase.dll, advapi32.dll,
                                   powrprof.dll, UMPDC.dll, profapi.dll,
                                   user32.dll, win32u.dll, GDI32.dll,
                                   gdi32full.dll, msvcp_win.dll, IMM32.DLL,
                                   winsta.dll, SspiCli.dll, USERENV.dll,
                                   profext.dll, ntmarta.dll, Bcrypt.dll,
                                   bcryptprimitives.dll, firewallapi.dll,
                                   DNSAPI.dll, IPHLPAPI.DLL, NSI.dll,
                                   fwbase.dll, uxinit.dll, shcore.dll,
                                   dwmapi.dll, UxTheme.dll, CRYPT32.dll,
                                   DPAPI.dll, CRYPTBASE.dll, dwminit.dll,
                                   apphelp.dll, dsreg.dll, OLEAUT32.dll,
```

C:\> tasklist /m ntdll.dll

```
C:\Users\adhd>tasklist /m ntdll.dll

Image Name                     PID Modules
========================= ======== ================
winlogon.exe                   620 ntdll.dll
lsass.exe                      700 ntdll.dll
fontdrvhost.exe                792 ntdll.dll
fontdrvhost.exe                800 ntdll.dll
svchost.exe                    808 ntdll.dll
svchost.exe                    920 ntdll.dll
dwm.exe                       1004 ntdll.dll
svchost.exe                    380 ntdll.dll
svchost.exe                    432 ntdll.dll
svchost.exe                    736 ntdll.dll
svchost.exe                   1064 ntdll.dll
svchost.exe                   1132 ntdll.dll
svchost.exe                   1228 ntdll.dll
svchost.exe                   1516 ntdll.dll
svchost.exe                   1616 ntdll.dll
svchost.exe                   1636 ntdll.dll
svchost.exe                   1788 ntdll.dll
```


C:\> tasklist /m /fi "pid eq [proc_id]"

```
C:\Users\adhd>tasklist /m /fi "pid eq 3500"

Image Name                     PID Modules
========================= ======== ============================================
explorer.exe                  3500 ntdll.dll, KERNEL32.DLL, KERNELBASE.dll,
                                   msvcp_win.dll, ucrtbase.dll, combase.dll,
                                   RPCRT4.dll, OLEAUT32.dll, shcore.dll,
                                   msvcrt.dll, advapi32.dll, sechost.dll,
                                   shlwapi.dll, user32.dll, win32u.dll,
                                   GDI32.dll, gdi32full.dll, SHELL32.dll,
                                   AEPIC.dll, bcrypt.dll, TWINAPI.dll,
                                   USERENV.dll, powrprof.dll,
                                   windows.storage.dll, dxgi.dll,
                                   kernel.appcore.dll, PROPSYS.dll,
                                   WININET.dll, UxTheme.dll, dwmapi.dll,
                                   SspiCli.dll, twinapi.appcore.dll,
                                   WTSAPI32.dll, ntmarta.dll, cryptsp.dll,
```

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/tasklist

C:\> wmic process list full

```
C:\Users\adhd>wmic process list full


CommandLine=
CSName=DESKTOP-I1T2G01
Description=System Idle Process
ExecutablePath=
ExecutionState=
Handle=0
HandleCount=0
InstallDate=
KernelModeTime=1237077343750
MaximumWorkingSetSize=
MinimumWorkingSetSize=
Name=System Idle Process
OSName=Microsoft Windows 10 Enterprise|C:\WINDOWS|\Device\Harddisk0\Partition3
OtherOperationCount=0
OtherTransferCount=0
PageFaults=9
PageFileUsage=60
ParentProcessId=0
```

C:\> wmic process get name,parentprocessid,processid

```
C:\Users\adhd>wmic process get name,parentprocessid,processid
Name                          ParentProcessId  ProcessId
System Idle Process           0                0
System                        0                4
Secure System                 4                48
Registry                      4                96
smss.exe                      4                308
csrss.exe                     432              448
wininit.exe                   432              524
csrss.exe                     516              540
winlogon.exe                  516              620
services.exe                  524              628
LsaIso.exe                    524              676
lsass.exe                     524              700
fontdrvhost.exe               620              792
fontdrvhost.exe               524              800
svchost.exe                   628              808
svchost.exe                   628              920
dwm.exe                       620              1004
svchost.exe                   628              380
svchost.exe                   628              432
```

C:\>wmic process where processid=[pid] get commandline

```
C:\Users\adhd>wmic process where processid=808 get commandline
CommandLine
C:\WINDOWS\system32\svchost.exe -k DcomLaunch -p
```

Making it easier with Powershell: DeepBlueCLI

```
PS C:\tools\DeepBlueCLI-master> .\DeepBlue.ps1 .\evtx\smb-password-guessing-security.evtx

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If
you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run
C:\tools\DeepBlueCLI-master\DeepBlue.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R


Date    : 9/19/2016 10:50:06 AM
Log     : Security
EventID : 4625
Message : High number of logon failures for one account
Results : Username: Administrator
          Total logon failures: 3560
Command :
Decoded :

Date    : 9/19/2016 10:50:06 AM
Log     : Security
EventID : 4625
Message : High number of total logon failures for multiple accounts
Results : Total accounts: 2
          Total logon failures: 3561

Command :
Decoded :
```

LAB: Windows CLI