

Unusual Network Usage

Look at File Shares `net view \\127.0.0.1`

Open Sessions with Machine `net session`

Session This machine has Opened `net use`

NetBIOS over TCP/IP Activity `nbtstat -S`

List Listening TCP and UDP Ports `netstat -na`

5 - Continuous Scrolling every 5 seconds `netstat -na 5`

-o flag shows process ID -b flag shows executable `netstat -naob`

Inspect Firewall rules `netsh advfirewall show currentprofile`

`netsh firewall show config`

Unusual Accounts

Unexpected Users in the Administrators Group `lusrmgr.msc`

List Users `net user`

List Members of Admin Group `net localgroup administrators`

List Domain Users `net user /domain`

When looking at domain accounts, the command will be run on the domain controller. A large domain may take some time - redirect to a text file to analyze:

`net user /domain > domainUsers.txt`

Windows Security & System Events To Look For

Security 4720 User Account Created

Security 4722 User Account Enabled

Security 4724 Password Reset

Security 4738 User Account Change

Security 4732 Account Added or Removed From Group

Security 1102 Audit Log Cleared

System 7030 Basic Service Operations

System 7045 Service Was Installed

System 1056 DHCP Server Oddities

System 10000 COM Functionality

System 20001 Device Driver Installation

System 20002 Remote Access

System 20003 Service Installation

Search for Other Startup Items

Users' Autostart Folders `dir /s /b "C:\Documents and Settings\ [user name]\Start Menu\"`

`dir /s /b "C:\Users\ [user name]\Start Menu\"`

Use WMIC To find Start Up Programs `wmic startup list full`



By **koriley**
cheatography.com/koriley/

Published 4th April, 2017.
Last updated 5th April, 2017.
Page 1 of 2.

Sponsored by **Readability-Score.com**
Measure your website readability!
<https://readability-score.com>

Unusual Processes

Task List	<code>tasklist</code>
	<code>`wmic process list full'</code>
Parent Process ID	<code>wmic process get name,parentprocessid, processid</code>

Command-Line `tasklist /m /fi "pid eq [pid]"`

Options and DLLs

```
wmic process where processid=[pid]
get commandline
```

Run Task Manager: Start->Run... and type `taskmgr.exe`

- Look for unusual/unexpected processes
- Focus on processes with username **SYSTEM** or **ADMINISTRATOR** or user in the **Local Administrator's** group.

Unusual Scheduled Tasks

List System Scheduled Tasks `schtasks`

You can also use the Task Scheduler GUI:

Start->Programs->Accessories->System Tools->Scheduled Tasks

Look for unusual Tasks run as a user of the Local Admin, SYSTEM, or blank username

Unusual Reg Key Entries

Check the Registry Run keys for malware that has made an entry to launch itself.

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunonceEx

`C:\reg query`

`hklm\software\microsoft\windows\currentversion\run`

These can also be analyzed with `regedit.exe`.

`Autoruns.exe` from **SysInternals** will pull all **Auto Start Entry**

Points.

Unusual Services

Services Control Panel	<code>services.msc</code>
List Of Sevices Available	<code>nets start</code>
Show Service Detail	<code>sc query more</code>
Map of Service from Which Process	<code>tasklist /svc</code>



By **koriley**
cheatography.com/koriley/

Published 4th April, 2017.
Last updated 5th April, 2017.
Page 2 of 2.

Sponsored by **Readability-Score.com**
Measure your website readability!
<https://readability-score.com>