Admin windows Cheat Sheet

User Accounts

- Identify curious-looking accounts in the administrators group [use lusrmgr.msc for GUI access]
- Related command: net user
- Related command: net localgroup administrators

Processes **(focus on those running with high privileges)**

- Identify abnormal processes [use taskmgr.exe for gui access]
- Related command: tasklist
- Related command: wmic process list full
- Related command: wmic process get name,parentprocessid,processid
- Related command: wmic process where processid=[pid] get commandline

Services

- Identify abnormal services [use services.nsc for GUI access]
- Related command: net startports
- Related command: sc query | more
- Related command: (associate running services with processes): tasklist /svc

Scheduled tasks

- Identify curious-looking scheduled tasks [search for task scheduler in start menu search]
- Related command: schtasks

Extra startup items

- Identify users' autostart folders
- Related command: dir /s /b "c:\documents and settings\[username]\start menu\"
- Related command: dir /s /b "c:\users\[username]\start menu\"

Auto-start reg key entries

- Check below registry keys for malicious autorun configurations [use regedit for GUI access and inspect both HKLM and HKCU]
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx
- Related command: reg query [reg key]

Listening and active TCP and UDP ports

- Identify abnormal listening and active TCP and UDP ports
- Related command: netstat -nao 10

File Shares

- All available file shares of a machine should be justified
- Related command net view \\127.0.0.1

Files

- Identify major decreases in free space [you can use file explorer's search box and enter "size:>5M"

Firewall Settings

- Examining current firewall settings to detect abnormalities from a baseline
- Related command: netsh advfirewall show currentprofile

Systems connected to the machine

- Identify NetBIOS over TCP/IP activity
- Related command: nbtstat -S

Open sessions

- Knowing who has an open session with a machine is very important
- Related command: net session

Sessions with other systems (NetBIOS/SMB)

- Identify sessions the machine has opened with other systems
- Related command: net use

Log entries

- Identify curious-looking events [you can use eventvwr.msc for GUI access to logs]
- Related command: wevtutil qe security (must be done with admin privileges)

Account management events

4720	A user account was created.
4722	A user account was enabled
4723	A user password was changed.
4724	A user password was set.
4726	A user account was deleted.
4727	A global group was created.
4728	A member was added to a global group.
4729	A member was removed from a global group.
4730	A global group was deleted.
4731	A new local group was created.
4732	A member was added to a local group.
4733	A member was removed from a local group.
4734	A local group was deleted.

4735	A local group account was changed.
4737	A global group account was changed.
4738	A user account was changed.
4739	A domain policy was modified.
4740	A user account was auto locked.
4741	A computer account was created.
4742	A computer account was changed.
4743	A computer account was deleted.
4744	A local security group with security disabled was created. Note: SECURITY_DISABLED in the formal name means that this group cannot be used to grant permissions in access checks
4745	A local security group with security disabled was changed.
4746	A member was added to a security-disabled local security group.
4747	A member was removed from a security-disabled local security group.

4748	A security-disabled local group was deleted.
4749	A security-disabled global group was created.
4750	A security-disabled global group was changed.
4751	A member was added to a security-disabled global group.
4752	A member was removed from a security-disabled global group.
4753	A security-disabled global group was deleted.
4754	A security-enabled universal group was created.
4755	A security-enabled universal group was changed.
4756	A member was added to a security-enabled universal group.
4757	A member was removed from a security-enabled universal group.
4758	A security-enabled universal group was deleted.
4759	A security-disabled universal group was created.
4760	A security-disabled universal group was changed.

4761	A member was added to a security-disabled universal group.
4762	A member was removed from a security-disabled universal group.
4763	A security-disabled universal group was deleted.
4764	A group type was changed.
4780	Set the security descriptor of members of administrative groups.