Cheatography

# Windows IR Live Forensics Cheat Sheet

by koriley via cheatography.com/12660/cs/11352/

## 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 advfir ewall show curren tpr of ile` |
| | `netsh firewall show config` |

## Unusual Accounts

| | |
|---|---|
| **Unexpected Users in the Administrators Group** | `lusrmg r.msc` |
| **List Users** | `net user` |
| **List Members of Admin Group** | `net localgroup admini str ato rs` |
| **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 > domain Use rs.txt`

## Windows Security & System Events To Look For

## Search for Other Startup Items

| | |
|---|---|
| **Users' Autostart Folders** | `dir /s /b " C: \Doc uments and Settings\ [u u\"` |
| | `dir /s /b " C: \Users\ [user name]\Start Me` |
| **Use WMIC To find Start Up Programs** | `wmic startup list full` |

## Unusual Processes

| | |
|---|---|
| **Task List** | `tasklist` |
| | `wmic process list full' |
| Parend Process ID | `wmic process get name,p are ntp roc essid, p id` |
| **Comman d-Line Options and DLLs** | `tasklist /m /fi "pid eq [pid]"` |
| | `wmic process where proces sid =[pid] get cor ine` |

**Run Task Manager: Start->Run... and type** `taskmg r.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 lau**

- 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\s oft war e\m icr oso ft \win dow s
 ver sio n\run
```

These can also be analyzed with `regedi t.exe`.

`Autoru ns.exe` from **SystInternals** will pull all **Auto Start Entry**

| | |
|---|---|
| **Security 4720** | User Account Created |
| **Security 4722** | User Account Enabled |
| **Security 4724** | Password Reset |
| **Security 4738** | User Account Change |
| **Security 4732** | Accout 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 |

**Points**.

| Unusual Services | |
|---|---|
| **Services Control Panel** | `servic es.msc` |
| **List Of Sevices Available** | `nets start` |
| **Show Service Datail** | `sc query \| more` |
| **Map of Service from Which Process** | `tasklist /svc` |

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

Published 4th April, 2017.
Last updated 5th April, 2017.


Sponsored by **ApolloPad.com**
Everyone has a novel in them. Finish Yours!
https://apollopad.com