Windows Malware Detection

# Defender

Windows Defender, the successor to Microsoft Security Essentials, is built into Win 10 and Server 2016+. It is best used from Powershell.

**Check the status of Defender**

> Get-MpComputerStatus

Also see the WdNisSvc, WinDefend, wscsvc, services. These should all be running when Defender is configured normally.

**Update Signatures**

> Update-MpSignature

**Run a manual scan**

> Start-MpScan -ScanPath <dir or file path>

**Review threats**

When Defender finds something “bad”, it is added to a threat list. You will want to review threats, and then probably remove them.

> Get-MpThreat

> Remove-MpThreat

**Enable / Disable**

> Set-MpPreference -DisableRealtimeMonitoring $true # or $false

If real-time monitoring is disabled, scans can still be manually run.

**Group Policy**

If you have a functioning domain to work with, the best way forward is to enable group policy to push a good Defender config out to everybody.

# Manual Checks

netstat

* -a -> display all active TCP and UDP connections and the port they are on
* -n -> display connections but display the process names numerically
* -o -> display the PID (Process ID), you can then look this up in windows task manager
* Using intervals -> [Ex: netstat -na 1] by adding a space and number you specify a interval (in seconds) on which to repeat check and dump to screen. Allows you to track something if you would like.

Check Start Up Processes

* dir /A “C:\Documents and Settings\All Users\Start Menu\Programs\Startup”
* alternatively check the startup tab in msconfig

Check Users and Admins

* > Get-LocalUser
  + Defaults include Administrator, DefaultAccount, Guest. These can be disabled.
* > Get-LocalGroupMember -Group Administrators # get members of the admin group
* > Get-LocalGroup #View the groups. Both Administrators and Power Users are default groups.

Check Running Processes

* tasklist /svc -> shows running processes and services they’re using. Some things insert services into processes that don’t usually use that service.
* Often normal processes may be using services that are legitimate, but you would rather not leave running.
  + Note: “net start [service]” “net stop [service]”

Check Which Processes Are Reading A File

* Install “handle”, a Sysinternals tool
* > handle <file or directory name> # prints all of the processes currently working with that resource
* Process explorer can also do this

Rootkit Detection

* Enable “Boot Log” in the “boot” tab of msconfig and restart
  + Use “search files and folders” to look for suspiciously named files. Some common examples:
    - rot, gas, gaopdx, seneka, uacd, tdss, tdss, kungsf, gxvxc, ovsfth, msqp, ndisp, msivx, skynet
* Disable the file permission on anything you find using:
  + cacls C:WINDOWSsystem32drivers [filename] /d everyone
  + restart
* Delete the suspicious file(s) you found

# Other AV

Software to download, some new versions don’t work with older versions of windows

Shortened url is beneath full url

Malwarebytes(enable premium)

<https://www.malwarebytes.org/mwb-download/thankyou/>

<https://goo.gl/6LxKFE>

EMET 5.5(use recommended settings and “import” popularsoftware.xml)

<https://www.microsoft.com/en-us/download/confirmation.aspx?id=50766>

<https://goo.gl/RW8oMv>

Microsoft Baseline Security Scanner (good scan in general)

<https://www.microsoft.com/en-us/download/details.aspx?id=7558>

<https://goo.gl/hxgO9X>