CIS Top 20 Critical Security Controls for Effective Cyber Defense

Planning, Implementing, and Auditing

@petermorin123

Peter Morin

- Over 20yrs in the field
- Director at KPMG
- IR, threat hunting, cloud security, insider threat, etc.
- Worked in the past for the various military and government agencies
- Specialize in protection of critical infrastructure and DFIR

All your base are belong to us…

- **Wannacry ransomware**
  - Initial outbreak on May 12-15, 2017
  - Encrypted files $300-$600 ransom
  - Over 300,000 hosts infected
  - Affected almost every flavor of Windows
  - Affected embedded systems

NHS FedEx HITACHI NISSAN MÆRSK

All your base are belong to us…

- **Wannacry ransomware**

  - Infection vector was the EternalBlue exploit
  - Exploited a vulnerability in MS's implementation of the SMB protocol (used for file, printer sharing, etc.) - CVE-2017-0144
  - Listens over port TCP/445 - used for delivery and propagation

All your base are belong to us…

- **Wannacry ransomware**
  - Patch MS17-010
  - Don't expose SMB
  - Update indicators
  - Disable SMBv1
  - **MS has been preaching the removal of SMBv1**
  - **How did we get here?**

SHODAN

- **2,045,897** SMB services available on the Internet at the moment
- **42%** allow Guest access
- **96%** support SMBv1
- **91,081** are vulnerable to MS17-010

US Comprehensive National Cybersecurity Initiative (CNCI) states:

“offense must inform defense.”

Essentially the knowledge of actual attacks that have compromised systems provides the essential foundation on which to construct effective defenses…

CIS Controls

- In 2008, the Office of the Secretary of Defense asked the NSA for help in prioritizing the myriad security controls that were available for cybersecurity with strong emphasis on **"What really Works”**.
- Currently release is version 6.1
- Maintained via security community through the **Center for Internet Security**

Overall Goal

- Protect critical assets, infrastructure, and information
- Strengthening your organization's defensive posture through **continuous, automated protection and monitoring** of infrastructure to reduce compromises
- Minimize the need for recovery efforts, and lower associated costs.

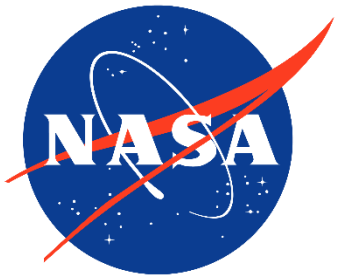
Many Involved…

- NSA Red and Blue Teams
- US DHS – US-CERT
- US DoD Computer Network Defense Architecture Group
- US DoD Joint Task Force: Global Network Operations
- US DoD Cyber Crime Center(DC3)
- US DoE – Los Alamos Lab
- US Dept. of State, Office of the CISO
- US Air Force
- US Army Research Laboratory
- US Dept. of Transportation, Office of the CIO
- US Dept. of Health and Human Services, Office of the CISO
- US Government Accountability Office (GAO)
- MITRE
- SANS
- Numerous commercial penetration testing and forensic experts (i.e. InGuardians and Mandiant)

Does this Replace other Frameworks?

- Not a replacement for any existing regulatory, compliance, or authorization scheme
- The controls map to most major compliance frameworks
  - NIST Cybersecurity Framework
  - NIST 800-53
  - ISO 27000 series
  - Regulations such as PCI DSS, HIPAA, NERC CIP, and FISMA

Integrators and Adopters



Telenet

@petermorin123

Top 20 Critical Security Controls

- Guiding principals:
  - Defenses should **focus on addressing the most common** and damaging attack activities occurring today, and those **anticipated in the near future**.
  - Enterprise environments must **ensure consistent controls across an enterprise** to effectively negate attacks.

Top 20 Critical Security Controls

- Guiding principals:
  - Defenses should be **automated where possible**, and **periodically or continuously measured** using automated measurement techniques where feasible
  - **Quick wins** - rapidly improve its security stance generally without major procedural, architectural, or technical changes to its environment.

Controls

No.	Control Name	Effect of Attack Mitigation (NSA)
CSC1	Inventory of Authorized and Unauthorized Devices	Very High
CSC2	Inventory of Authorized and Unauthorized Software	Very High
CSC3	Secure Configurations for Hardware and Software	Very High
CSC4	Continuous Vulnerability Assessment and Remediation	Very High
CSC5	Controlled Use of Administrative Privileges	High
CSC6	Maintenance, Monitoring and Analysis of Audit Logs	High
CSC7	E-mail and Web Browser Protections	High
CSC8	Malware Defenses	Moderately High to High
CSC9	Limitation and Control of Network Ports	Moderately High to High
CSC10	Data Recovery Capability	Moderately High
CSC11	Secure Configurations for Network Devices	Moderately High
CSC12	Boundary Defense	Moderately to Moderately High
CSC13	Data Protection	Moderately
CSC14	Controlled Access Based on the Need to Know	Moderately
CSC15	Wireless Access Control	Moderately
CSC16	Account Monitoring and Control	Moderately
CSC17	Security Skills Assess. and Appropriate Training To Fill Gaps	Moderately Low to Moderately
CSC18	Application Software Security	Moderately Low to Moderately
CSC19	Incident Response and Management	Low
CSC20	Penetration Tests and Red Team Exercises	Low

First 5 controls eliminate the vast majority of vulnerabilities

Want to focus on…

No.	Control Name	Effect of Attack Mitigation (NSA)
CSC1	Inventory of Authorized and Unauthorized Devices	Very High
CSC2	Inventory of Authorized and Unauthorized Software	Very High
CSC3	Secure Configurations for Hardware and Software	Very High
CSC4	Continuous Vulnerability Assessment and Remediation	Very High
CSC5	Controlled Use of Administrative Privileges	High
CSC6	Maintenance, Monitoring and Analysis of Audit Logs	High
CSC7	E-mail and Web Browser Protections	High
CSC8	Malware Defenses	Moderately High to High
CSC9	Limitation and Control of Network Ports	Moderately High to High
CSC10	Data Recovery Capability	Moderately High
CSC11	Secure Configurations for Network Devices	Moderately High
CSC12	Boundary Defense	Moderately to Moderately High
CSC13	Data Protection	Moderately
CSC14	Controlled Access Based on the Need to Know	Moderately
CSC15	Wireless Access Control	Moderately
CSC16	Account Monitoring and Control	Moderately
CSC17	Security Skills Assess. and Appropriate Training To Fill Gaps	Moderately Low to Moderately
CSC18	Application Software Security	Moderately Low to Moderately
CSC19	Incident Response and Management	Low
CSC20	Penetration Tests and Red Team Exercises	Low

Control 1: Inventory of Authorized and unauthorized devices

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls CM-8 (a, c, d, 2, 3, 4), PM-5, PM-6

- Reduce the ability of attackers to find and exploit unauthorized and unprotected systems: use active monitoring and configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops and remote devices.

Why is asset management key?

- Understand what is authorized to run in an environment
- Discover new assets that have not yet patched
- Detect returning hardware such as laptops that have missed previous updates
- Determining remediation priorities
- Data protection needs
- IR – what are the affected assets?
- Exploits – how vulnerable am I?
- Should those assets be there in the first place?

Control 1: Details

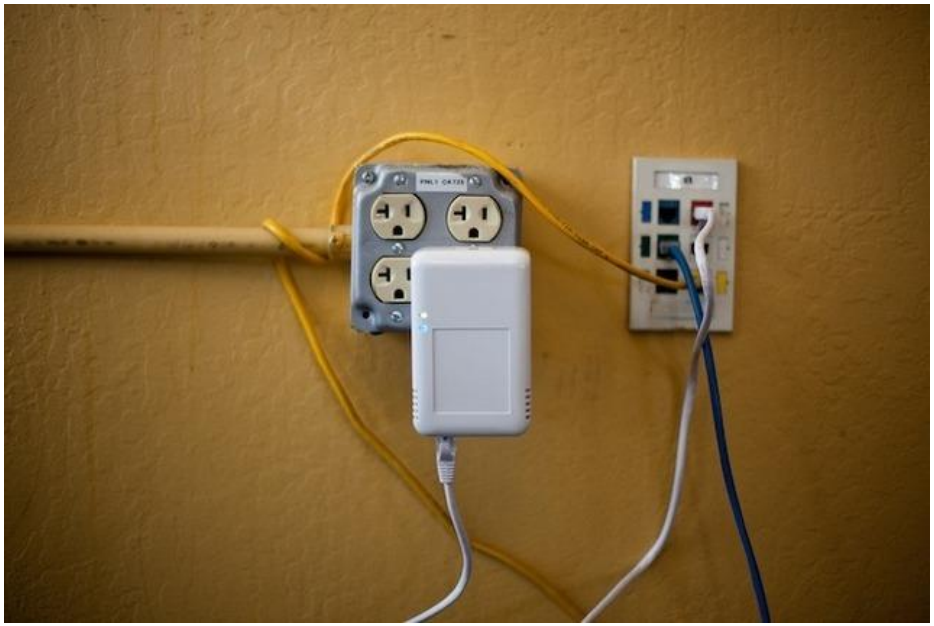
- Attackers constantly scanning our devices looking for unprotected systems
- Attackers also look for devices (especially laptops) which come and go off of the enterprise's network, and so get out of synch with patches or security updates.

Control 1: Details

- BYOD — where employees bring personal devices into work and connect them to the network — is becoming very common.
- These devices could already be compromised and be used to infect internal resources.

Control 1: Details

- Rogue “test” server
- VM sprawl
- Cloud infrastructure
- Raspberry PI
- Pwnie Express



You should be mostly concerned about non-fixed hosts
Most servers don’t move!

Meeting the Control Requirements

- Includes 6 sub-controls
  1. Automated asset inventory discovery tool
  2. DHCP logging
  3. All new equipment is automatically added
  4. Maintain all the asset inventory
  5. Deploy network level authentication via 802.1x
  6. Use client certificates to validate and authenticate systems prior to connecting to the private network.

Control 1: What Can We Do?

- Deploying DHCP logging is also a key contributor to better asset control
- Allows for correlation against your known assets to discover “rogue” devices
- Regular scanning to appropriately maintain the list → once this gets away from you….very bad.

Control 1: What Can We Do?

- Up-to-date floor plan and understand where your people live
- If you ever use ARP to track an offender, and can link them to a port, not knowing **where that port to drop is a problem.**
- Also note where wireless APs are

Control 1: What Can We Do?

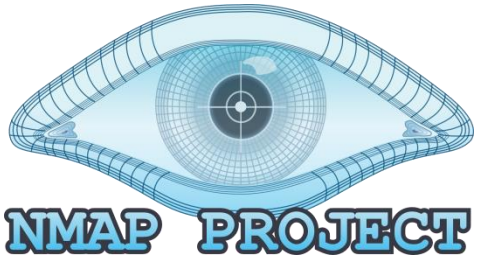
- Can do other things like deploy 802.1x network access control (NAC) to control who can connect to the network….very expensive.
- Must ensure that your network equipment is capable of supporting your network as a NAC enforcement point

Control 1: Commercial Tools?

Ensure the product meets your needs – integrates with your vulnerability management tool, ITSM solution, IR solution, supports all your platforms, etc.

NMAP

- Use nmap to scan our network blocks and output to XML
  - # nmap –sS –A –iYourHosts.txt –oX Outputfile.xml
- Use **scanpbnj** to take output write it to a MySQL DB and diff the data each time it is run



***Scanpbnj** - https://www.aldeid.com/wiki/ScanPBNJ

NMAP

- Let's Script all this…. and backup source files

```
#!/bin/sh
current_date=$(date "+%Y%m%d")
echo "Current Date : $current_date"
echo "NMAP Asset Scan Running“
nmap -sS -A -ihostlist.txt  -oX hosts-$current_date.xml
scanpbnj -x hosts-$current_date.xml
```

```
Starting Scan of 10.22.3.13
Machine is already in the database
Checking Current Services
      ! Service 22:tcp ssh is down
      = smtp:25 is (unknown version) Postfix smtpd
Scan Complete for 10.22.3.13
```

NMAP

- Now, let's run this through a scheduled cron job at 3pm and voila, a daily diff'ing asset DB…
  - 0 15 * * * /scripts/runNmap.sh
- Remember, if you have mobile users, you may want to run this twice
  - During business hours on your network block reserved for laptops, etc.
  - During non-business hours for everything that doesn't leave the premises

NMAP

- Maybe a quick and dirty PHP view???

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>NMAP Asset Results</title>
</head>
<body>

…SNIP…

<?php
mysql_connect("localhost","root","password");
mysql_select_db("pbnjdb");
$res=mysql_query("SELECT m.* ,s.* FROM machines m,services s WHERE m.mid=s.mid");
while($row=mysql_fetch_array($res))
{
 ?>
```

NMAP

Maybe a quick and dirty PHP view? Maybe make it searchable?

Asset Report [NMAP]

Hostname	IP Address	Operating System	Service	Port	Version	Banner	Status	Host Identified	Last Scan Update
localhost	127.0.0.1	unknown os	ssh	22	6.0p1 Debian 4	OpenSSH	up	Sat Oct 3 07:25:02 2015	Sat Oct 3 07:25:02 2015
localhost	127.0.0.1	unknown os	mysql	3306	5.5.28-1	MySQL	up	Sat Oct 3 07:52:55 2015	Sat Oct 3 07:25:02 2015
0	192.168.2.17	unknown os	ssh	22	5.3	OpenSSH	up	Sat Oct 3 11:57:58 2015	Sat Oct 3 11:57:58 2015
0	192.168.2.19	unknown os	ssh	22	5.3	OpenSSH	up	Sat Oct 3 11:57:58 2015	Sat Oct 3 11:57:58 2015
0	192.168.2.19	unknown os	rpcbind	111	2-4	unknown product	up	Sat Oct 3 11:57:58 2015	Sat Oct 3 11:57:58 2015
0	192.168.2.19	unknown os	mysql	3306	unknown version	MySQL	up	Sat Oct 3 11:57:58 2015	Sat Oct 3 11:57:58 2015

NMAP

- You know have updating asset data in a searchable database
- Sky is the limit on what you want outputted….
- Nice thing is you now have an “agent-less”, free asset system
- Can be used to detect rogue machines

DHCP Logs

- Obtain access to the DHCP logs
- Parse and sort into a format that can be dropped in to a script to automate the detection process
- SIEM can be used as well
- Helpful if your org has a good host naming convention and a common HW manufacturer

DHCP Logs

- Then with a simple script, you can whitelist your company details:
  - My HP ProBook laptop uses am Intel Ethernet (I217-LM) chipset with a MAC address of 48:0F:CF:B8:30:CB
  - We know the first 3 sets of characters tells us the chipset manufacturer (480FCF)
  - A standard host naming convention will assist as well (i.e. asset tag == hostname, G464552.acme.com
  - By correlating the two in a script, you should be able to isolate rogue systems

DHCP Logs

- System hostnames:
  - Hostnames of JamesMegaLappy, SkyRocket and hax0r don't fit that naming standard and a basic regular expression check against the naming standard will be able to pick this up instantly
- Mac address:
  - A script reading DHCP logs detecting either a non-standard hostname or OID and sending an email or SIEM alert can be an effective detection method to find those non-company approved systems.

DHCP Logs

- Expiry time entry to confirm when the device obtained its IP address
- Time frame of when the device was added to the network
- Starting point to ask questions in looking for the unauthorized system

DHCP Logs

- This isn’t fool proof
- Trivial to change both the hostname and MAC address to blend in
- Highly effective against the majority of devices being plugged in to networks

DHCP – Active Defense

- Offending MAC address can be added as a DHCP reservation with DHCP scope options that point the default gateway and DNS server to, say 127.0.01 – or a honeypot.
- This is limits what the offending device can connect to the next time it renews it DHCP lease or requests a new IP address.

Control 1: Auditing for Effectiveness

- How long does it take to detect new devices added to the organization's network (time in minutes)?
- How long does it take the scanners to alert the organization's administrators that an unauthorized device is on the network (time in minutes)?
- How long does it take to isolate/remove unauthorized devices from the organization's network (time in minutes)?
- Are the scanners able to identify the location, department, and other critical details about the unauthorized system that is detected (yes or no)?

Control 2: Inventory of Authorized and unauthorized software

Associated NIST Special Publication 800-53, Revision 3, Priority 1 Controls CM-1, CM-2 (2, 4, 5), CM-3, CM-5 (2, 7), CM-7 (1, 2), CM-8 (1, 2, 3, 4, 6), CM-9, PM-6, SA-6, SA-7

- Restrictions Identify vulnerable or malicious software to mitigate or root out attacks: devise a list of authorized software for each type of system, and deploy tools to track software installed (type, version and patches) and monitor for unauthorized or unnecessary software

Meeting the Control Requirements

- Includes 4 sub-controls
  1. Devise a list of authorized software and versions. Perform file integrity checking to ensure authorized software hasn't been modified
  2. Deploy application whitelisting
  3. Deploy software inventory tools
  4. VMs should be air-gapped to isolate the use of high-risk applications

Control 2: Details

- Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited
  - Un-patched Acrobat + Office allow for attacks using “weaponized” files.
  - When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines

Control 2: Details

- Attackers that take control of your systems may install unwanted tools on your systems to assist in their lateral movement
- Insider threats may install apps to assist in ex-filtrating sensitive intellectual property
- Employees may install unapproved applications and expose the company (i.e. BitTorrent client)

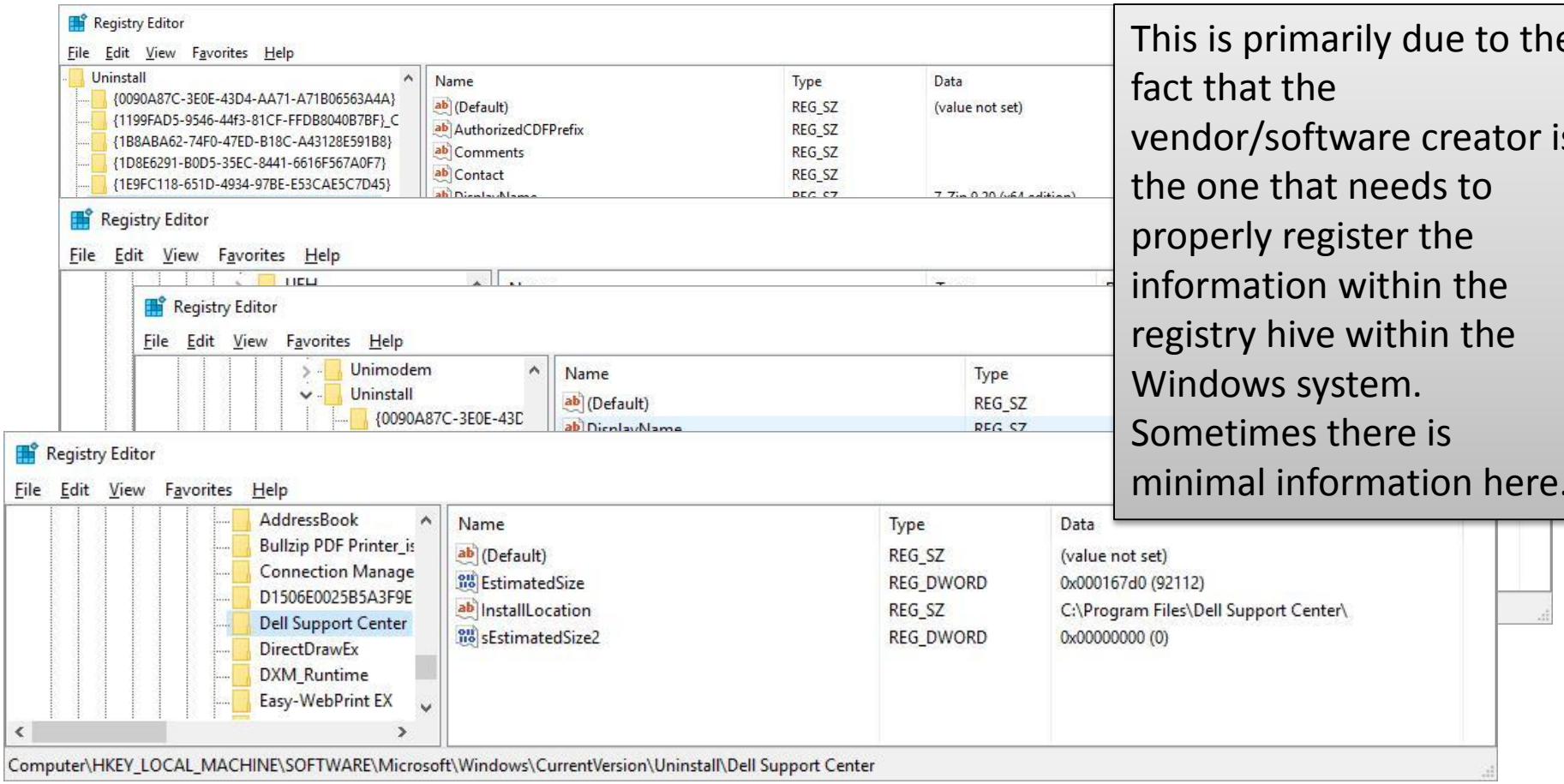
Control 2: Commercial Tools?

Ensure the product meets your needs – integrates with your ITSM solution, supports your various operating systems, etc.

Windows installed software – where to find details

- Windows does not have just one location to register an installed program
- It is not mandatory to store information at all
- Example registry key locations include:
  - *'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\'*
  - *'HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\'*
- No single query can return the required information – MS doesn't make this easy!

Collection Challenges



This is primarily due to the fact that the vendor/software creator is the one that needs to properly register the information within the registry hive within the Windows system. Sometimes there is minimal information here.

Available tools for collection

- Free tools
  - E.g. OCS inventory, PsInfo
- Built-in tools
  - E.g. WMIC, PowerShell

PsInfo

- PsInfo is a Microsoft Sysinternals tool that can collect local or remote system information
- Version 1.77 used in paper (more later)
- Run from command line

  psinfo.exe -s applications

PsInfo output example

Command Prompt

```
c:\Temp>psinfo -s application

PsInfo v1.78 - Local and remote system information viewer
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for \\JONATHAN-PC:

Applications:
Adobe AIR 22.0.0.153
Adobe AIR 22.0.0.153
Adobe Acrobat Reader DC 15.020.20039
Adobe Community Help 3.4.980
Adobe Community Help 3.4.980
Adobe Content Viewer 1.4.0
Adobe Content Viewer 1.4.0
Adobe Digital Editions 3.0 3.0.1
Adobe Download Assistant 1.0.6
Adobe Download Assistant 1.0.6
Adobe Flash Player 21 NPAPI 21.0.0.213
Adobe Flash Player 23 PPAPI 23.0.0.185
```

WMIC

- Windows Management Instrumentation Command-line
- Permits access to query and change system functionality
- To collect inventory information

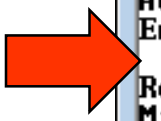
  wmic product get name,version

WMIC example

Command Prompt

```
C:\Users\Jonathan>wmic product get name,version
Name                                                                Version
Garmin MapSource                                                    6.15.11
Citrix Online Launcher                                              1.0.408
Grammarly for Microsoft® Office Suite                               6.5.43
PxMergeModule                                                       1.00.0000
Microsoft Application Error Reporting                               12.0.6015.5000
Microsoft Office OneNote MUI (English) 2010                         14.0.7015.1000
Microsoft Office Office 32-bit Components 2010                      14.0.7015.1000
Microsoft Office Shared 32-bit MUI (English) 2010                   14.0.7015.1000
Microsoft Office InfoPath MUI (English) 2010                        14.0.7015.1000
Microsoft Office Visio MUI (English) 2010                           14.0.7015.1000
Microsoft Office Project MUI (English) 2010                         14.0.7015.1000
Microsoft Office Access MUI (English) 2010                          14.0.7015.1000
Microsoft Office Shared Setup Metadata MUI (English) 2010           14.0.7015.1000
Microsoft Office Excel MUI (English) 2010                           14.0.7015.1000
Microsoft Office Access Setup Metadata MUI (English) 2010           14.0.7015.1000
Microsoft Office PowerPoint MUI (English) 2010                      14.0.7015.1000
Microsoft Office Publisher MUI (English) 2010                       14.0.7015.1000
Microsoft Office Outlook MUI (English) 2010                         14.0.7015.1000
Microsoft Office Groove MUI (English) 2010                          14.0.7015.1000
Microsoft Office Word MUI (English) 2010                            14.0.7015.1000
Microsoft Office Proofing (English) 2010                            14.0.7015.1000
Microsoft Office Shared MUI (English) 2010                          14.0.7015.1000
Microsoft Office Proof (English) 2010                               14.0.7015.1000
```

WMIC output issues



Command Prompt

```
TortoiseSVN 1.7.9.23248 (64 bit)                                    1.7.9.23248
Microsoft Visual Studio 2010 Tools for Office Runtime (x64)         10.0.50903
Java 8 Update 111                                                   8.0.1110.14
Java 8 Update 111 (64-bit)                                          8.0.1110.14
Roxio Creator Copy                                                  16.0.0.6348
Cisco WebEx Meeting Center for Firefox or Chrome                    8.23.2500
Adobe Flash Player 23 NPAPI                                         23.0.0.162
Adobe Acrobat XI Pro                                                11.0.17
EndNote X6                                                          16.0.0.6348
                                                                    16.5.0.0
Roxio Creator Tools                                                 3.7.0
Microsoft .NET Framework 4 Extended                                 4.0.30319
Google Earth Pro                                                    7.1.5.1557
Roxio Update Manager                                                6.0.0
Microsoft Silverlight                                               5.1.41212.0
Configuration Manager Client                                        4.00.6487.2400
Roxio Creator Data                                                  3.7.0
Microsoft .NET Framework 4 Client Profile                           4.0.30319
Titus Labs Message Classification                                   3.21.5
Cisco WebEx Meeting Center for Internet Explorer                    8.23.2500
Roxio Express Labeler 3                                             3.2.2
Roxio Creator Audio                                                 3.7.0
Intel® Trusted Connect Service Client                               1.24.738.1
```

Only as good as the information that is contained within the registry keys being queried!

PowerShell

- Uses the *OpenSubKey* and *GetValue* cmdlets within PowerShell
- Accesses the following registry locations and iterates through each subkey
  - *SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*
  - *SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall*

Scripts examples

- Number of scripts by Jonathan Risto
  - Batch file for PsInfo and WMIC collection
  - PowerShell script for PS commands
- All query for IP address to inventory
- Some checking is performed for valid data types and entry
- Output stored in text file for archiving and future reference
- https://www.giac.org/paper/gccc/554/windows-installed-software-inventory/121403

Probe Linux with SSH

- #ssh root@192.168.2.17 "rpm -q -a“
- #ssh root@192.168.2.17 "rpm -q -a“ > AppList.txt
- # ssh root@192.168.2.17 "rpm -q -a | wc -l“
  - ssh-keygen -t rsa
  - ssh-copy-id user@123.45.56.78

#ssh admin@192.168.2.17 "rpm -q -a"
pmorin@127.0.0.1's password:
at-3.1.10-48.el6.i686
acl-2.2.49-6.el6.i686
jasper-libs-1.900.1-16.el6_6.3.i686
quota-3.17-23.el6.i686
libXi-1.7.4-1.el6.i686
gnupg2-2.0.14-8.el6.i686
xorg-x11-font-utils-7.2-11.el6.i686
foomatic-db-4.0-7.20091126.el6.noarch
perl-parent-0.221-141.el6_7.1.i686

…..

Tripwire (Open Source)

- TW agents monitor Linux systems to detect and report any unauthorized changes to files and directories.
- First creates a baseline of all files in an encrypted file (protects from malware tampering)
- Monitors (using cryptographic hashes) the files for changes, including permissions, internal file changes, and timestamp details.

Tripwire

- Running an integrity check
  - tripwire --check –interactive
- This will produce the report

```
Open Source Tripwire(R) 2.4.1 Integrity Check Report

Report generated by:          root
Report created on:            Tue 06 Oct 2015 11:50:16 AM ADT
Database last updated on:     Tue 06 Oct 2015 11:42:46 AM ADT

===============================================================================
Report Summary:
===============================================================================

Host name:                    snort
Host IP address:              Unknown IP
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/snort.twd
Command line used:            tripwire --check --interactive

===============================================================================
Rule Summary:
===============================================================================

-------------------------------------------------------------------------------
  Section: Unix File System
-------------------------------------------------------------------------------

  Rule Name                       Severity Level    Added    Removed  Modified
  ---------                       --------------    -----    -------  --------
  Invariant Directories           66                0        0        0
  Temporary directories           33                0        0        0
* Tripwire Data Files             100               0        0        1
  Critical devices                100               0        0        0
  User binaries                   66                0        0        0
  Tripwire Binaries               100               0        0        0
  Libraries                       66                0        0        0
  Operating System Utilities      100               0        0        0
  File System and Disk Administraton Programs
                                  100               0        0        0
  Kernel Administration Programs  100               0        0        0
```

Tripwire

- Touched a file: /root/testHack

```
Total objects scanned:  50131
Total violations found:  2

================================================================================
Object Summary:
================================================================================

--------------------------------------------------------------------------------
# Section: Unix File System
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Rule Name: Root config files (/root)
Severity Level: 100
--------------------------------------------------------------------------------

Remove the "x" from the adjacent box to prevent updating the database
with the new values for this object.

Added:
[x] "/root/testHack"

Modified:
[x] "/root"

================================================================================
Object Detail:
================================================================================

--------------------------------------------------------------------------------
  Section: Unix File System
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Rule Name: Root config files (/root)
Severity Level: 100
```

Tripwire

- Scheduling a Nightly Tripwire Analysis
  - Create the file "runtw.sh" in the directory /usr/local/bin that has the following contents:
  - #!/bin/sh /usr/sbin/tripwire --check --interactive | mail -s "Tripwire Report from [HOST]" root@localhost
  - Run nightly within a cron job

Control 2: Auditing for Effectiveness

- Periodically install several benign software test programs that are not included in the authorized software list on a number of systems on the network.
- Verify that the software is blocked and unable to run
- How effective was the process? How fast was the software blocked?
- What kind of notification was provided?

In Closing

- **Best practices for success – in my humble opinion**
  - Don’t do it all at once
  - If you don’t have any controls – start small and basic
  - Build solutions that match your organization’s size
  - In the case of control 1 and 2 – work on them together
  - Make sure your controls are requirements for vendor
  - Ensure you know what your dependencies are

Questions? Comments?

Peter Morin

petermorin123@gmail.com

Twitter: @petermorin123

http://www.petermorin.com