What's New for Security in Microsoft Windows Server 2016 ?

Jason Fossen
Enclave Consulting LLC
Securing Windows with PowerShell (SEC505)
http://www.sans.org/sec505

About The Speaker

- Jason Fossen
  - SANS Institute Fellow
  - Consultant, Dallas, Texas, USA
  - LinkedIn and Twitter:
    - @JasonFossen
- Author and Instructor of:
  - The Windows day of Security Essentials (SEC401.5)
  - Six-day Securing Windows with PowerShell (SEC505)
  - Course SEC505 → http://sans.org/sec505

Get All My Talks And PowerShell Scripts

- Get the full slide deck:
  - http://fossen.net (redirects to the SANS download page)
  - Download the SEC505 zip file, look in the \Extras folder
  - SEC505 zip includes hundreds of scripts written in PowerShell and VBScript (all in the public domain)

A New Microsoft ?

Old Microsoft

- CEO Steve Ballmer
  - Pushed out by the Board of Dirs
  - Missed search (Bing was late)
  - Laughed at the iPhone
  - Ironically, missed tablets
  - Hostile to open source movement
  - Late to the cloud party
  - Bought Nokia (too late, overpaid)
  - His center of the world was Windows on PCs and laptops, everything else secondary
  - Stuck in 1990's and left behind…

New Microsoft

- CEO Satya Nadella
  - New CEO since February 2014
  - Reads poetry, plays cricket
  - Cloud First:
    - Azure AD, Office 365, OneDrive
    - Bought Minecraft
  - Mobile First:
    - Including Android and iPhone!
  - Open Source:
    - PowerShell, ASP.NET, Roslyn, etc.
  - Free:
    - Windows on 9" and smaller screens
    - Free upgrades to Windows 10
    - Free Office Apps (with limitations)

Setting the Stage for Server 2016 (1 of 2)

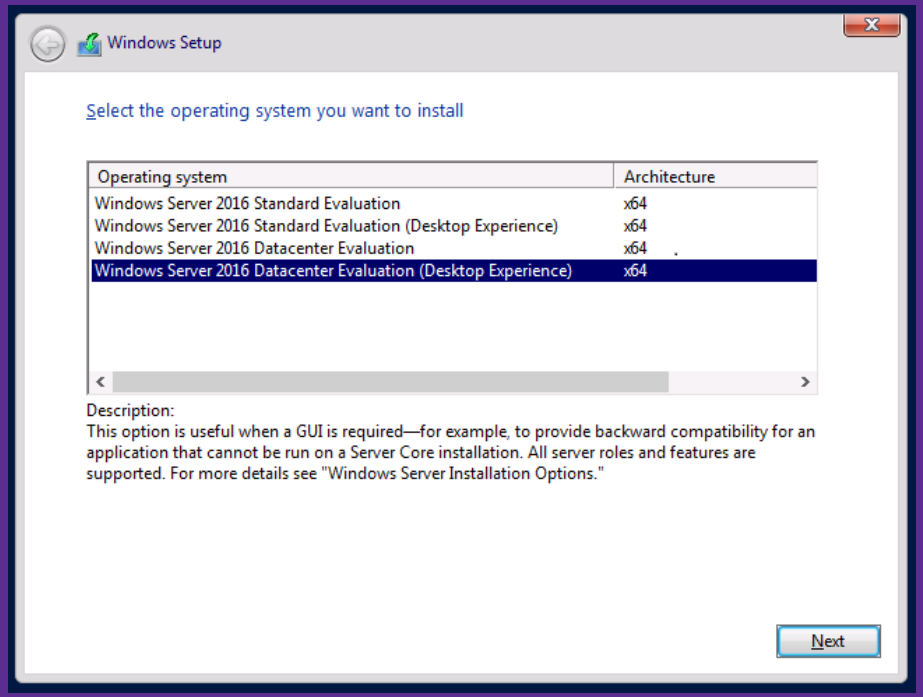
- Dogfooding
  - Azure datacenters scattered around the world
  - Azure runs tens of millions virtual machines
- Selling Cloud Services
  - Still must support on-premises servers, but as "hybrid cloud" to help ease integration with and migration to Azure (all roads lead to Azure now)

Setting the Stage for Server 2016 (2 of 2)

- Linux Domination
  - Dominates in web applications, cloud infrastructure, high-performance computing, academia, AI, etc.
  - *Totally* dominates the Internet of Things (IoT)
  - Excitement/Cool Factor: start-ups, 20-somethings

Installation Options

Installation Default



- Defaults to No GUI (top one)
  - Not called "Core" anymore
- With "Desktop Experience"
  - Graphical Admin Tools
  - Start Menu
  - Notification Area + Settings App
  - Control Panel (not gone yet)
  - No Cortana
  - No Edge Browser
  - Internet Explorer 11

Server Core: Only a CMD Shell

- When you hit Ctrl-Alt-Del, you get this:

Switch Without Reinstalling The OS?

- Server 2012: the GUI desktop could be (un)installed without reinstalling the entire OS
- Server 2016: to switch between Core and Desktop Experience mode, you must reinstall the OS again, just like with Server 2008

Server Nano

- Nano runs completely headless
  - No graphical desktop whatsoever
  - Runs the tiny OneCore kernel (similar to stripped-down Linux)
  - Can run from RAM drive (PXE boot, then SMB download of WIM image)
  - Managed through PowerShell remoting, DSC, WMI, serial cable EMS

- Mainly intended for hosting VMs and web apps:
  - Currently supports Hyper-V, Chef, PHP, Nginx, Python 3.5, Node.js, GO, Redis, MySQL, OpenSSL, Java (OpenJDK), Ruby 2.1.5, SQLite, and ASP.NET 5 (limited to Core CLR)

User name: _____
Domain: _____
Password: _____

ENTER Authenticate

```
                              Server Configuration
================================================================================
Computer Name: Nano1
Workgroup:     WORKGROUP
OS:            Microsoft Windows Server 2016

--------------------------------------------------------------------------------
 Ethernet
 192.168.1.119 fe80::e164:9f69:edd:4da2%3            00-15-5D-01-66-11
               2605:6001:e6c8:d000:e164:9f69:edd:4da2



--------------------------------------------------------------------------------

                                 > Networking

Up|Dn Scroll|ESC Log out|Ctl+F6 Restart|Ctl+F12 Shut down
```

Default Processes:

PowerShell remoting into Nano box from admin laptop ->

F:\Hyper-V-Images\Server2016-BETA3-Nano ($?=True : LastExitCode=0)

File Edit View Tools Debug Add-ons Help

Script

```
[192.168.1.119]: PS C:\> Get-Process | Format-Table -AutoSize

Handles NPM(K) PM(K) WS(K)   VM(M) CPU(s)   Id ProcessName
------- ------ ----- -----   ----- ------   -- -----------
     98      6   584  1592 2097161   0.00  320 csrss
     66      5   800  3444 2097166   0.00 1044 EMT
      0      0     0     4       0          0 Idle
    598     17  3132  9248 2097187   0.13  396 lsass
    166      8  1532  4772 2097166   0.00  376 services
     44      3   296  1112 2097156   0.00  244 smss
    351     15  5524 12804 2097228   0.13  280 svchost
    175      8  1380  4856 2097177   0.06  488 svchost
    235     13  1492  5304 2097178   0.05  524 svchost
    132      8  1408  4984 2097175   0.06  620 svchost
    119      7  1260  5692 2097175   0.00  632 svchost
    273     15  7128 11580 2097192   0.09  688 svchost
    385     17  5644 14112 2097230   0.16  760 svchost
    210     13  2064  6792 2097179   0.00  796 svchost
    326     25  3416 10296 2097197   0.06  820 svchost
    286     28  3704  8752 2097189   0.06  888 svchost
    302      0    80    76       2   0.84    4 System
     72      7   660  3596 2097167   0.00  348 wininit
    136      7  1668  6352 2097175   0.00 1360 WmiPrvSE
    527     52 58896 77552 2097622   4.80 1584 wsmprovhost


[192.168.1.119]: PS C:\> |
```

Ln 28 Col 26 100%

Default Services:

PowerShell remoting into Nano box from admin laptop ->

F:\Hyper-V-Images\Server2016-BETA3-Nano ($?= True : LastExitCode=0)

File Edit View Tools Debug Add-ons Help

Script

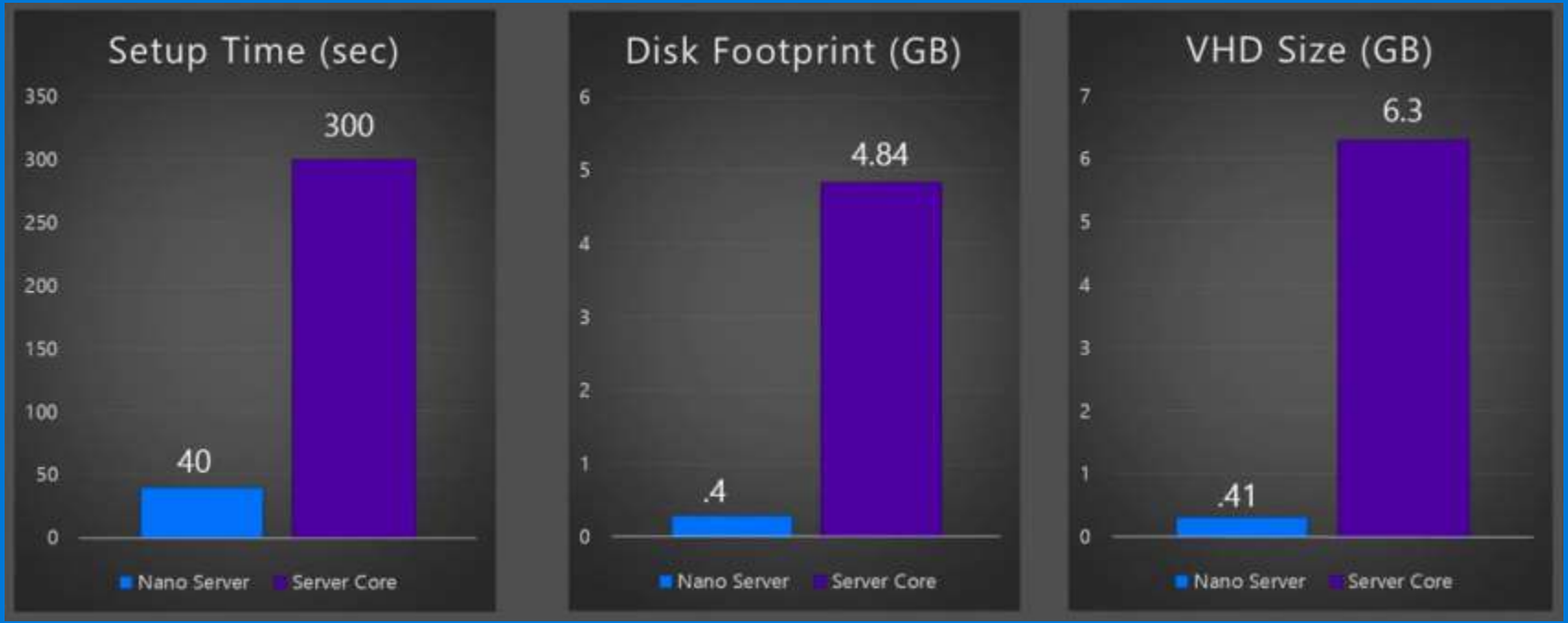
```
[192.168.1.119]: PS C:\>
[192.168.1.119]: PS C:\> Get-Service | Where Status -eq Running

Status   Name               DisplayName
------   ----               -----------
Running  BFE                Base Filtering Engine
Running  CryptSvc           Cryptographic Services
Running  DcomLaunch         DCOM Server Process Launcher
Running  Dhcp               DHCP Client
Running  DiagTrack          Diagnostics Tracking Service
Running  Dnscache           DNS Client
Running  EventLog           Windows Event Log
Running  LanmanServer       Server
Running  LanmanWorkstation  Workstation
Running  lmhosts            TCP/IP NetBIOS Helper
Running  MpsSvc             Windows Firewall
Running  nsi                Network Store Interface Service
Running  Power              Power
Running  ProfSvc            User Profile Service
Running  RpcEptMapper       RPC Endpoint Mapper
Running  RpcSs              Remote Procedure Call (RPC)
Running  SamSs              Security Accounts Manager
Running  Schedule           Task Scheduler
Running  SystemEventsBroker System Events Broker
Running  UserManager        User Manager
Running  vmicguestinterface Hyper-V Guest Service Interface
Running  vmicheartbeat      Hyper-V Heartbeat Service
Running  vmickvpexchange    Hyper-V Data Exchange Service
Running  vmicshutdown       Hyper-V Guest Shutdown Service
Running  vmictimesync       Hyper-V Time Synchronization Service
Running  W32Time            Windows Time
Running  WinHttpAutoProx... WinHTTP Web Proxy Auto-Discovery Se...
Running  winmgmt            Windows Management Instrumentation
Running  WinRM              Windows Remote Management (WS-Manag...


[192.168.1.119]: PS C:\>
```

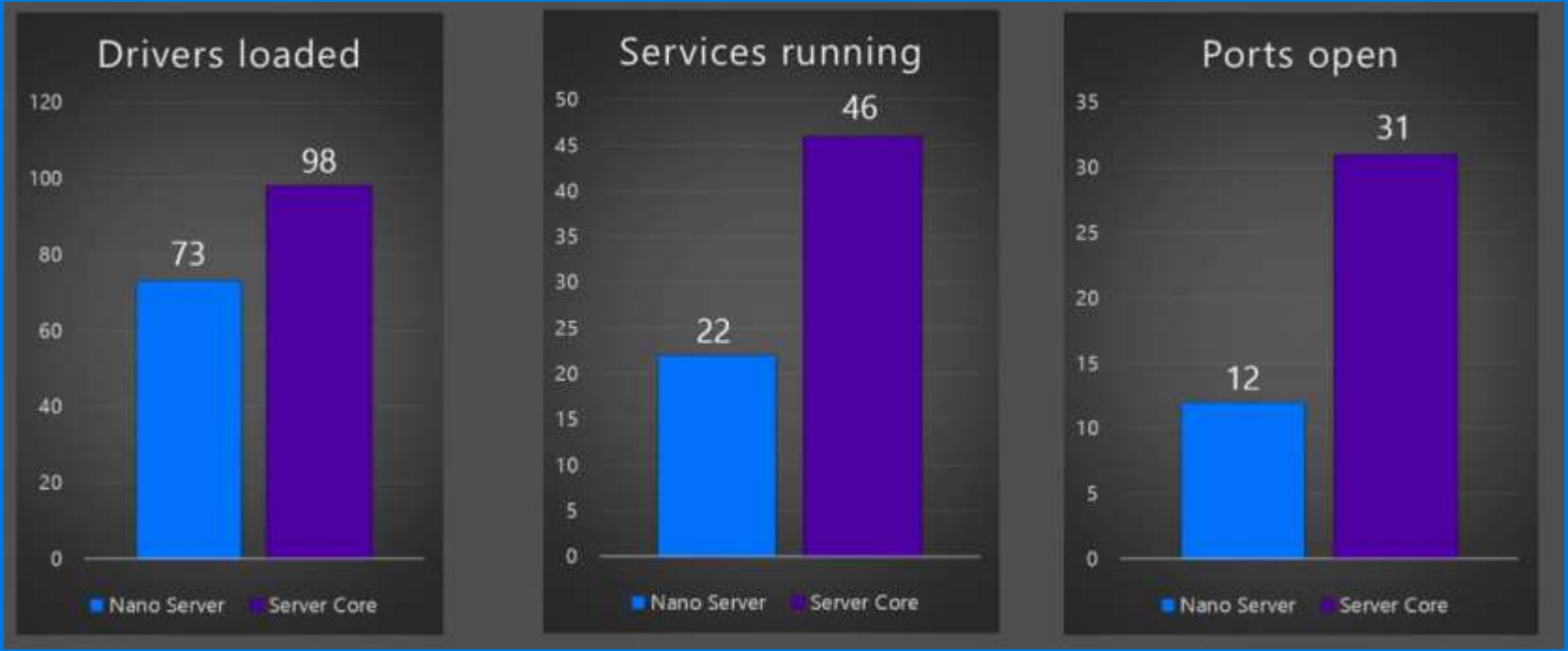
Ln 38 Col 26 100%

Nano vs. Core: Footprint



Credit: https://channel9.msdn.com/Events/Ignite/2015/BRK2461?WT.mc_id=IG15XCSOSC

Nano vs. Core: Attack Surface



Credit: https://channel9.msdn.com/Events/Ignite/2015/BRK2461?WT.mc_id=IG15XCSOSC

Nano Scalability Test

- HP ProLiant DL980 G7
  - 8 Xeon CPUs (80 cores + HT)
  - 1 TB Memory

- 3,486 Nano VMs running
  - 52% of memory consumed with idle VMs (531GB)

https://channel9.msdn.com/Series/Nano-Server-Team/Nano-Server-as-a-Hyper-V-Host-on-an-80-core-machine
Getting started guide: http://www.aka.ms/nanoserver

Licensing Headaches

- Server Nano
  - Must have Software Assurance agreement… :-(
  - Current Branch servicing only, no LTSB
  - 2 to 3 feature updates per year
  - Only the latest release and the prior release supported!
- Datacenter and Standard Editions
  - Licensed per-core now, not per-processor

Containers (*à la* Docker)

- Server Nano supports the container runtime
  - Best for pure web apps: ASP.NET, Node.js, Nginx, PHP, MySQL, etc.
- Server Core supports the container runtime
  - Best for anything that requires Windows API or full .NET support
- Nano/Core container hosts can themselves be VMs
  - Hyper-V supports nested VMs in Server 2016
- Manage with PowerShell or regular Docker tools

Even Better: Hyper-V Container Runtime

- Traditional containers run as *shared-kernel*
  - Not ideal for security, there can be "container escape"

- Hence, there are <u>two</u> container runtimes:
  1. Traditional shared-kernel runtime
  2. Hyper-V isolated runtime
     - This is <u>not</u> a VM that happens to have traditional containers inside it
     - Hyper-V uses hardware-assistance to wrap the containers
     - A container made for one can be used in the other runtime as-is
     - Windows 10 Pro & Enterprise support too
     - Windows containers FAQ: http://aka.ms/WindowsContainers

Hyper-V Container Runtime: Sessions

- Each container has its own MAC and IP address
  - Plugs directly into Hyper-V virtual switch, just like a VM
- You can RDP into a container to get a GUI desktop
- Each container has its own Session ID number:
  - Session 0: for kernel threads, device drivers, SMSS.EXE
  - Session X: for console, RDP sessions, and each container
    - Each container with its own LSASS.EXE, SVCHOST processes, files, etc!

Licensing Headaches

- Regular containers do not require separate licenses
- Hyper-V containers can consume licenses:
  - Datacenter Edition: Unlimited
  - Standard Edition: 2

Other Hyper-V Improvements

- Far too many to discuss (or even list…)
  - http://www.aidanfinn.com
  - http://www.thomasmaurer.ch

- Examples:
  - Nested VMs
  - Direct VM access to some PCIe devices (GPUs, NVMe SSDs)
  - "PowerShell Direct" through the Hyper-V VMBus, not any NIC
  - Linux Secure Boot with virtual UEFI firmware
  - Virtual TPM for guest VMs
  - Shielded VMs are encrypted, can only run on your servers/network

Windows as a Service

Update Distribution Mechanisms

- Windows Update in Settings app
- Windows Server Update Services (WSUS)
- Windows Update for Business (WUB)
  - Uses same infrastructure as Windows Update
  - Permits the delay of installation of updates and upgrades
  - Manage through Group Policy, MDM, or registry edits

Monthly Service Packs

- No more individual patch files (mostly)
- Monthly patches to become cumulative, so you only have to apply the most recent patch
- This applies to Windows 7/8.1/10, Server 2008 R2, Server 2012, Server 2012 R2, and Server 2016
- https://blogs.technet.microsoft.com/windowsitpro/2016/10/07/more-on-windows-7-and-windows-8-1-servicing-changes/

Servicing Branches

- Current Branch
  - All fixes and new features through Windows Update
- Current Branch for Business
  - Update vs Upgrade
  - Max update delay: 12 months (WSUS), 1 month (WUB)
  - Max upgrade delay: 12 months (WSUS), 8 months (WUB)
- Long-Term Servicing Branch
  - Max delay: 10 years

Maximum Values ->

Pause: 35 Days Max

Select when Quality Updates are received

Select when Quality Updates are received

Previous Setting | Next Setting

- Not Configured
- Enabled
- Disabled

Comment:

Located in the GPO under Computer Configuration > Administrative Templates > Windows Components > Windows Update > Defer Windows Updates

Supported on:

At least Windows Server 2016 or Windows 10

Options:

After a quality update is released, defer receiving it for this many days:

30

☐ Pause quality updates

Help:

Enable this policy to specify when to receive quality updates.

You can defer receiving quality updates for up to 30 days.

To prevent quality updates from being received on their scheduled time, you can temporarily pause quality updates. The pause will remain in effect for 35 days or until you clear the check box.

Note: If the "Allow Telemetry" policy is set to 0, this policy will have no effect.

OK | Cancel | Apply

Credential Guard

Purpose of Credential Guard

- To protect secrets from kernel-mode malware:
  - Password hashes
  - Encryption keys
  - Licensing keys
  - DRM enforcement?

- Stops mimikatz
  - https://github.com/gentilkiwi/mimikatz

Hardware & Firmware Requirements (1)

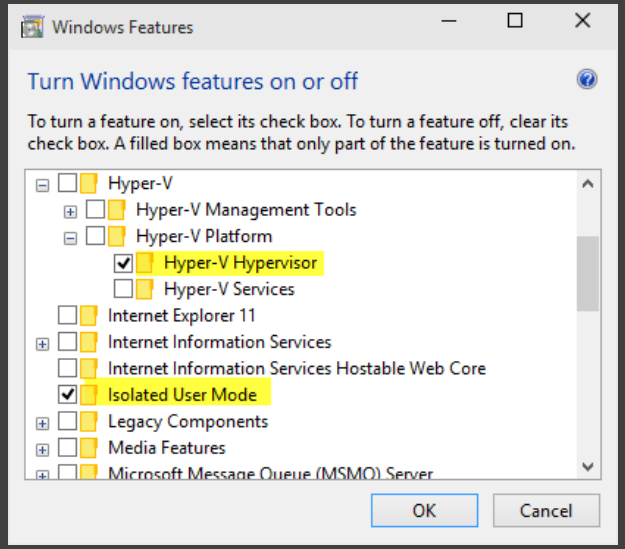
- UEFI 2.3.1 Secure Boot enabled and locked down
- TPM 1.2 or later in motherboard
- Intel VT-x or AMD RVI virtualization CPU extensions
- Intel EPT or AMD RVI Second Level Address Translation
- Intel VT-d or AMD-Vi IOMMU chipset support

Hardware & Firmware Requirements (2)

- UEFI Secure Boot
  - Firmware and OS loader must be signed and trusted
  - UEFI variables for controlling boot and OS runtime settings
- Trusted Platform Module (TPM)
  - Version 1.2 or later
  - Crypto chip in the motherboard
  - Virtual smart cards (phones/tablets)
  - Microsoft Passport key protection
  - Virtual TPMs for Hyper-V guests

Software Requirements

- Windows Server 2016
- Windows 10 Enterprise or Education Edition
- Only Microsoft corp trusted by UEFI for Secure Boot
- Can be physical or virtual machine



Where Are User Credentials In Memory?

- Run LSAISO.EXE in a tiny, hidden, hardened "VM"
  - Move LSASS.EXE credential secrets into LSAISO.EXE
  - Credential data never leaves the LSAISO.EXE process
  - LSASS requests non-replayable tokens from LSAISO.EXE

- Rely on type-1 hypervisor protections for LSAISO.EXE
  - Requires specific CPU and chipset features.
  - Normal kernel communicates with the "other kernel" through shared memory region (VMBus).

About that "Virtual Machine"…

- VM has no protocol stack
- VM has no desktop or GUI
- VM has a minimum set of Microsoft-only binaries
- VM requires strict digital signature level protections
- Communicates only through the hypervisor VMBus

- Even malware running in Ring 0 (kernel mode) in the hypervisor root partition cannot access VM

OK, It's Not A Real VM, But …

CPU Protections	Normal User/OS Land	Virtual Secure Mode
Ring 3	Normal User Mode, LSASS.EXE	Isolated User Mode, LSAISO.EXE, vTPM, CI
Ring 0	Normal Kernel, Malware	Proxy Secure Kernel
Ring -1	Hyper-V Hypervisor & VMBus	
Hardware	CPU with VT-x, SLAT, IOMMU	

SLAT memory address translation tables map addresses, but these tables also include CPU-enforced *permissions*.

Remote Credential Guard

- MSTSC.EXE /RemoteGuard
  - Requires Server 2016 and Windows 10 version 1607+
  - Supports single sign-on to third boxes beyond target
  - Not compatible with stand-alones or Azure AD-joined
  - Kerberos authentication is redirected back to the client
  - Only for Remote Desktop Protocol (RDP)

Attack Vectors (1 of 2)

- Compromise kernel, turn off protections, reboot
  - Enforce hypervisor protections from UEFI Secure Boot
- Compromise the UEFI firmware and/or use bootkit
  - Keep firmware updated, manage trusted CAs, HIDS
- Attack the VM through the VMBus
  - Keep OS updated, HIDS for VMBus (what in the world???)

Attack Vectors (2 of 2)

- Keystroke logger for smart card PIN, use card
  - Use every AV defense possible, physical security, hope…
  - Use multi-factor authentication, like SMS challenge
- The VM is an "oracle" for Q&A data leakage
  - Blocks MS-CHAPv2 and NTLMv1 with VM
  - Smart cards must use DHE, just like for PFS with TLS
  - Kerberos armoring to bind key to a computer (RFC 6113)
  - Authentication Policy Silo binds a user to machine(s)
    - https://www.youtube.com/watch?v=K21J5X4HO04

Device Guard

Purpose of Device Guard

- To protect integrity of OS and application code:
  - On disk
  - In memory
- To block unauthorized process launch:
  - Similar to AppLocker, but better
  - Applies to background services and drivers too

Requirements

- UEFI Secure Boot enabled and locked down
- Only Microsoft trusted by UEFI for Secure Boot
- TPM 2.0 or later in motherboard
- Intel VT-x or AMD RVI virtualization CPU extensions
- Intel EPT or AMD RVI Second Level Address Translation
- Intel VT-d or AMD-Vi IOMMU chipset support
- All kernel-mode binaries signed by Microsoft

- Server 2016 or Windows 10 (Enterprise or Education)

Authenticode and Catalog Files

- OS binaries are digitally signed and/or hashed
  - Multiple signature levels based on certificate EKU field
  - .CAT files contain SHA-1 or SHA-256 hashes of OS files
  - .CAT files are themselves signed by Microsoft

- Kernel variable determines minimum level allowed
  - Cannot launch processes below that EKU level (next slide)
  - Different defaults for Windows Mobile or OEM appliances
  - UEFI variable can override the default at boot

Protected Processes and Services

- Digital signature levels (not the full list)
  1. No signature
  2. Some signature (including third-party or LOB apps)
  3. Windows Store app
  4. Anti-malware driver (approved by Microsoft)
  5. Microsoft app (built into Windows)
  6. Windows kernel (Trusted Computing Base or TCB)

- Child processes at same or lower level of parent
  - Set during launch, recorded in EPROCESS object header

Not Just Process Launch Control

- Process and services are protected from various forms of meddling by lower-level processes:
  - Process or thread termination or suspension
  - Reading or writing virtual memory address space
  - (Un)loading of modules
  - What else? Well, not exactly well-documented…

- Note: this is not Mandatory Integrity Control, User Account Control, Dynamic Access Control, or AppLocker

Will Your Own Binaries Run?

- If they're your apps, sign them! ☺

- If you cannot sign the binaries you need
  1. Create your own catalog (.CAT) files of hashes
  2. Sign the .CAT with your own PKI or through a Microsoft web portal for Device Guard (not available yet)

- Many new PowerShell tools to wrangle:
  - Device Guard Deployment Guide (https://technet.microsoft.com)
  - Alex Ionescu (@aionescu) and Matt Graeber (@mattifestation)

PowerShell

Open Source and Cross Platform

- PowerShell for Linux and Mac OS X
  - https://github.com/PowerShell
  - MIT License
  - .NET Core Framework open source too

SSH Client and Server (but not yet)

- "[T]his is the 3rd time the PowerShell team has attempted to support SSH. … Given our changes in leadership and culture, we decided to give it another try …"

The Register®

Biting the hand that feeds IT

DATA CENTER SOFTWARE NETWORKS SECURITY BUSINESS HARDWARE SCIENCE BOOTNOTES VI

Holy SSH-it! Microsoft promises secure logins for Windows PowerShell

Now that the door has hit Ballmer on the way out, OpenSSH support is go

2 Jun 2015 at 19:52, Shaun Nichols 619 127 83

Microsoft has finally decided to add support for SSH to PowerShell, allowing people to log into Windows systems and use software remotely over an encrypted connection.

Incident Response & New AV API

- Greatly enhanced transcription logging
  - Includes scriptblocks, Base64, in-memory only, console
  - Encrypt transcript data with your own public key
    - Manage through GPO or script to provide the key path/Base64
    - Descrypt at SIEM or with Unprotect-CmsMessage (uses CMS standard)

- Anti-Malware Scan Interface (AMSI)
  - Not just PowerShell: JScript, VBScript, Python, Ruby, etc.
  - AV after deobfuscation and just before it is executed

Security

- Enhancements for Just Enough Admin (JEA)
  - Control the commands/parameters available
  - Copy files within remoting sessions (no new open ports)
  - JEA Helper Tool 2.0+
- AppLocker can place PowerShell into "constrained language mode" to contol interactive commands
  - Get-Help about_Language_Modes -ShowWindow
- Enhancements for Desired State Configuration (DSC)
  - The future of security templates and config automation; similar to Puppet

MISC

- DNS Policies for split-brain DNS, sinkholes, etc.
- SMB Encryption: AES-GCM is 40% faster!
- Shielded VMs: "You can trust us, we swear!"

- What is going on with Dynamic Access Control?
- Subsystem for Linux on Server Nano?

- Expect more wheel-greasing towards Azure…

Thank You for Attending!

- See you in my *Securing Windows* course (SEC505)?
  - December 2016: Washington DC
  - http://sans.org/sec505
- Let's connect on Twitter and LinkedIn!
  - @JasonFossen
- Get my PowerShell scripts and slide decks:
  - http://fossen.net (redirects to SANS download page)
  - Get the SEC505 zip file, then look in the \Extras folder