What's New for Security in Windows 10 and Server 2016 ?

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

About The Speaker

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

User Acceptance

Many platforms, one user interface

Desktop PC
Laptop
Tablet
Phone
Xbox
Surface Hub
Raspberry Pi
HoloLens
Car

Image Credit: msdn.microsoft.com

Many platforms, one BSOD

Image Credit: The Verge

Graphical User Interface

- Return of the Start Menu!
- Apps can run full screen or in normal windows
- Charms bar is gone
- Notification Area (like Android)
- Virtual desktops (like Linux)
- Settings app steadily replacing the Control Panel

- Switch between "Tablet Mode" and "PC Mode"

Cortana

- Cortana is not just "Microsoft Siri"
- Cortana is "Microsoft Watson" (as in, IBM's Watson)
- Cortana will be integrated into *everything*
  - Including Android, iPhone, Xbox, Office 365, Start Screen
- "Human language is the new user interface layer" --Satya Nadella (speaking of "bots" generally).

Cortana Cortana Everywhere …

Cortana on Windows 10 devices

Because Cortana is available across device types, she's able to help you even more effectively

Cortana was first available on Windows phones

Then Cortana came to Windows 10 PCs, tablets, Windows Holographic and Xbox

With upcoming Windows 10 Creators Update, Cortana will be available on Windows 10 IoT Core devices with displays

Image Credit: Microsoft.com

Cortana Privacy Rampancy

- You might want to read the license agreement…
- https://fix10.isleaked.com
- Microsoft's official position:
  - http://news.microsoft.com/stories/inthecloudwetrust/
  - https://player.vimeo.com/video/133627472

Image Credit: Microsoft Halo and msdn.microsoft.com

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

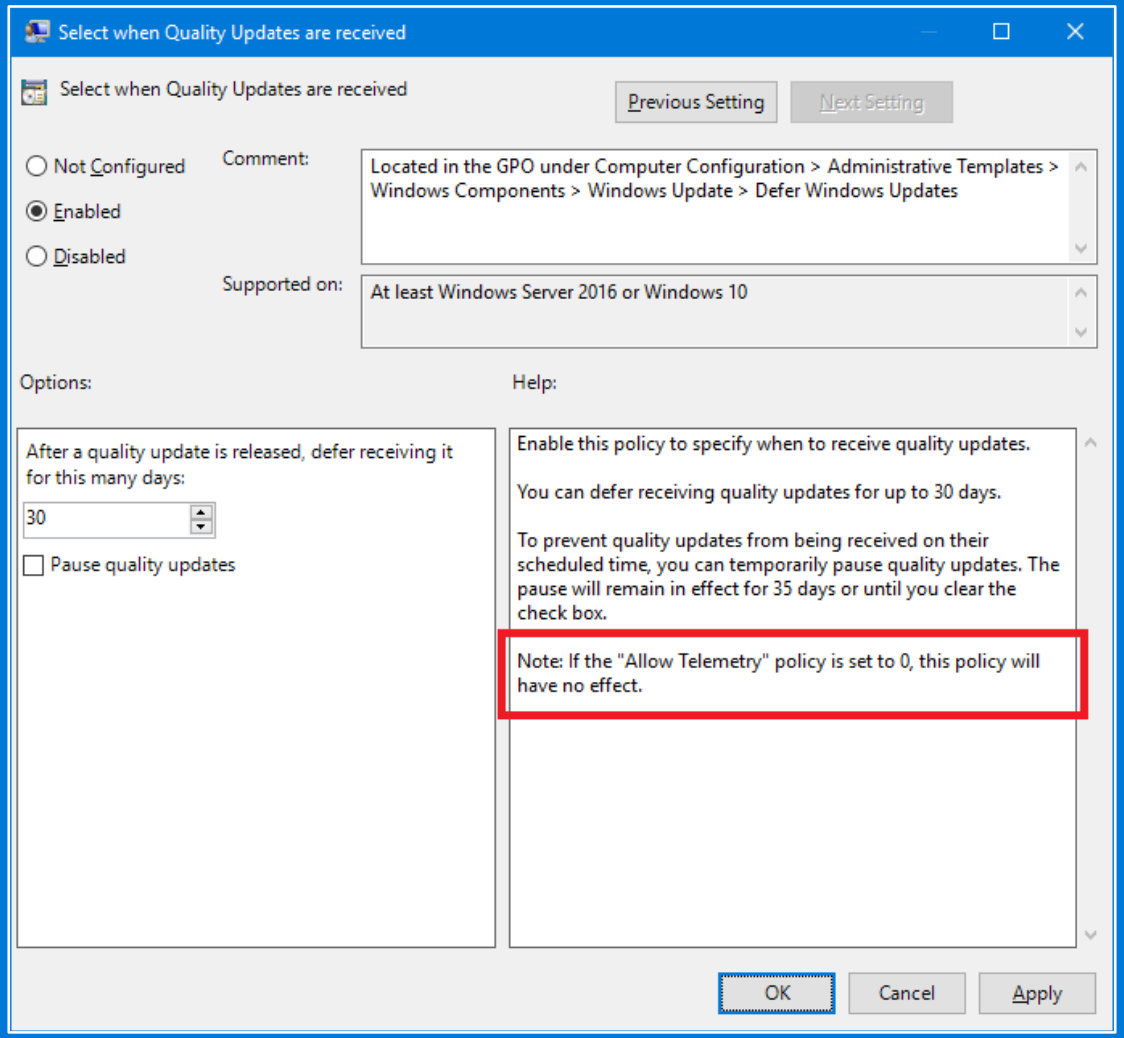
- No more individual patch files (mostly)
- Monthly patches to become cumulative, so you only have to apply the most recent patch
- This also applies to Windows 7 and 8.1, Server 2008 R2, Server 2012, Server 2012 R2, and Server 2016
- https://blogs.technet.microsoft.com/windowsitpro/2016/10/07/more-on-windows-7-and-windows-8-1-servicing-changes/

Servicing Branches

- Current Branch (All Editions)
  - All fixes and new features through Windows Update
- Current Branch for Business (Pro, Enterprise, Edu)
  - 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 (Enterprise only)
  - Max delay: 10 years

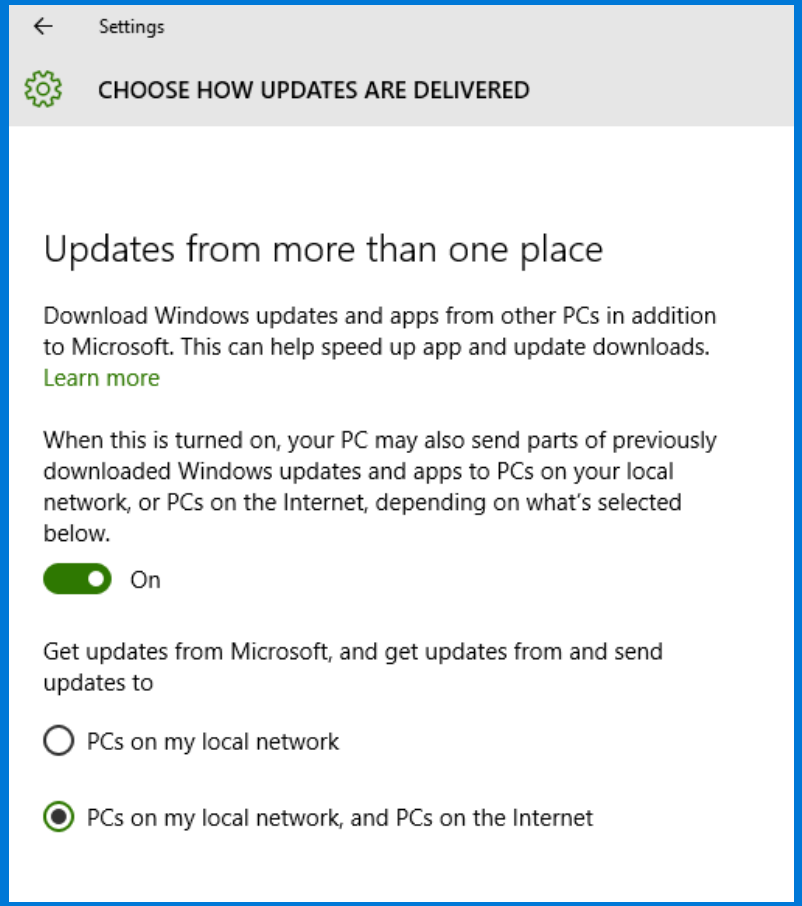
Maximum Values ->

Pause: 35 Days Max



Peer-to-Peer Updates

- Similar to BitTorrent
  - SSL/TLS to transfer chunks
  - Digital signatures checked
  - Not just updates, apps too
  - Metered NICs excluded
- Pro & Home Editions
  - Both LAN and Internet updating
- Enterprise & Education
  - By default, local network only



To configure, go to Settings > Update & Security > Windows Update > Advanced Options.

To exploit, see Flame malware documentation for guidance and technical support…

Azure Active Directory

Azure Active Directory

- Planetary-scale authentication database
- Used today for Office 365, OneDrive, Outlook.com, Xbox, Windows Phone, and (soon) LinkedIn too.
- One-way or two-way sync with your on-premises Active Directory…or just replace it entirely
- The Goal: enroll every human and every device

Windows 10

- Microsoft Account login or creation integrated into the Windows 10 installation process
- Log onto desktop with Microsoft Account or Organizational Account
- Single sign-on with Universal apps and MS Office
- All Settings > Accounts > Your Account

Settings

ACCOUNTS

Find a setting

Your account

Sign-in options

Work access

Family & other users

Sync your settings

Thor Monty

hughhugh@yahoo.com

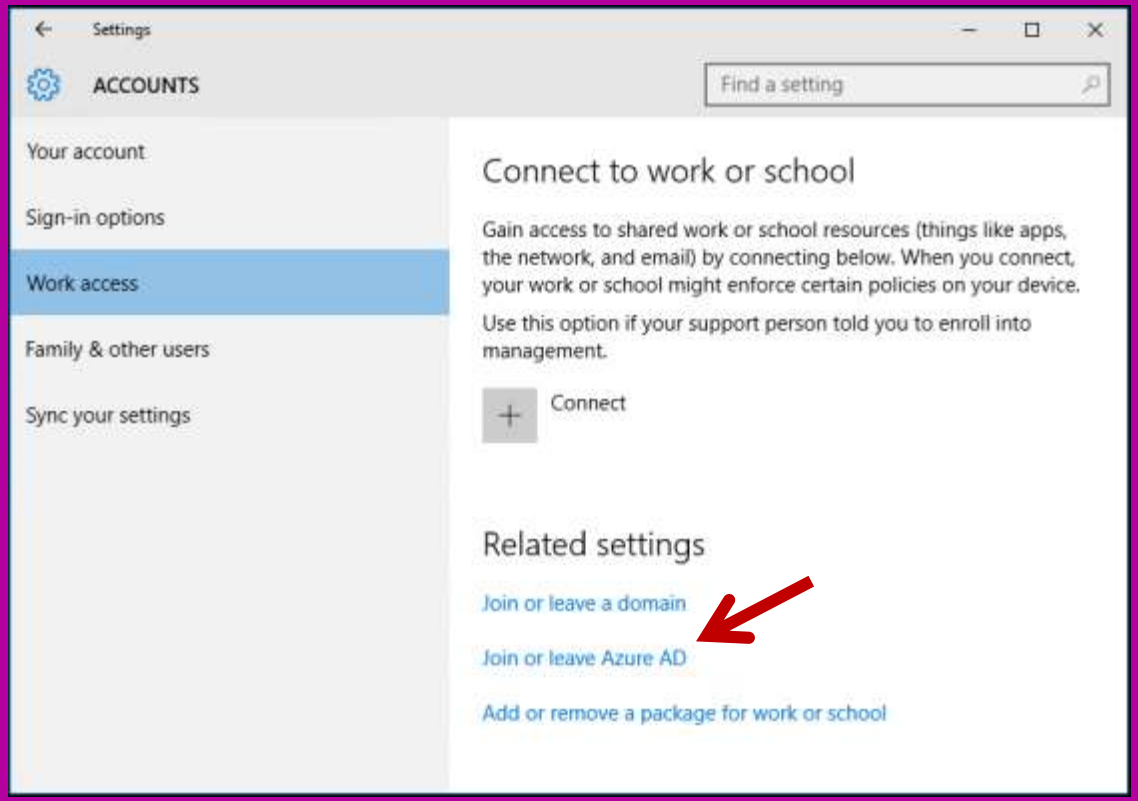
Administrator

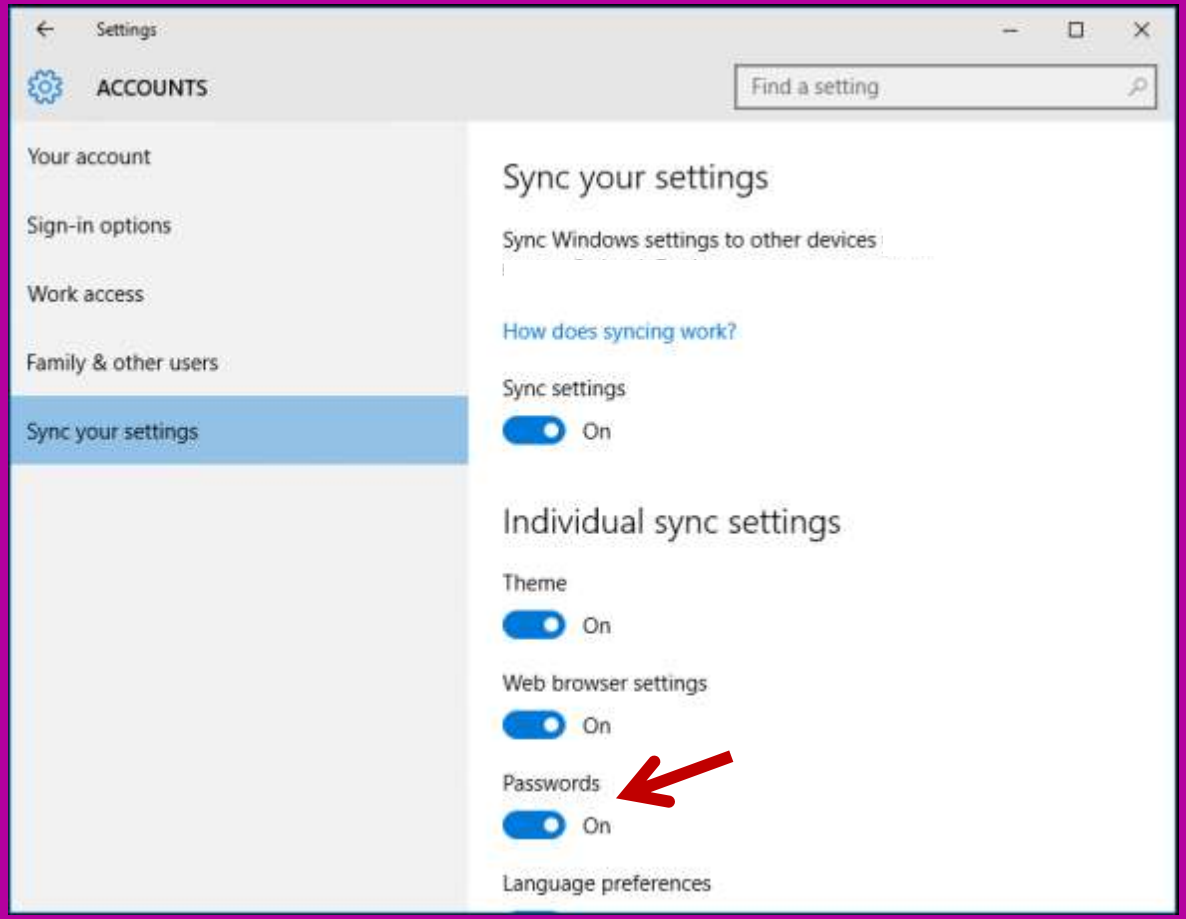
Billing info, family settings, subscriptions, security settings, and more

Manage my Microsoft account

Sign in with a local account instead

Your picture


Settings
ACCOUNTS
Find a setting
Your account
Sign-in options
Work access
Family & other users
Sync your settings
Connect to work or school
Gain access to shared work or school resources (things like apps, the network, and email) by connecting below. When you connect, your work or school might enforce certain policies on your device.
Use this option if your support person told you to enroll into management.
Connect
Related settings
Join or leave a domain
Join or leave Azure AD
Add or remove a package for work or school


Settings
ACCOUNTS
Find a setting
Your account
Sign-in options
Work access
Family & other users
Sync your settings
Sync your settings
Sync Windows settings to other devices
How does syncing work?
Sync settings
On
Individual sync settings
Theme
On
Web browser settings
On
Passwords
On
Language preferences

Windows Hello

Hello = Biometrics Framework

- New biometric authentication support built into OS
  - Fingerprint and palm
  - Iris and retina
  - 3D facial geometry
  - YubiKey (and other non-biometric devices)

  - Plug-in support for new biometric data sources/devices

Fingerprint

- Supports surface, ultrasound, and thermal scanning
- Multiple individual fingers may be enrolled per user

Image Credit: gizmag.com, Eikon Mini USB

- After five failures, user must enter PIN or passphrase
- Fingerprint data encrypted by TPM or passphrase

Iris Scanner

- Lumia 950 XL Phone
  - Infrared Iris Scanner
  - Continuum docking station with HDMI and USB ports for keyboard and mouse
  - Windows on ARM

Image Credit: http://www.theverge.com/2015/8/26/9212985/microsoft-lumia-flagship-phones-leak

Infrared 3D Camera

- Built into phones, tablets, laptops, monitors
- Available as an external webcam (USB)

- Not just one camera, it includes:
  - Infrared laser emitter
  - Infrared camera
  - 4K webcam (4096x2160)

Image Credit: Logitech.com

The Australian Twins Test

Life

NEWS OPINION BUSINESS REVIEW NATIONAL AFFAIRS SPORT LIFE TECHNOLOGY ART

Windows Hello: can identical twins fool Microsoft and Intel?

THE AUSTRALIAN | AUGUST 30, 2015 12:00AM

SAVE

Chris Griffith
Senior Technology Journalist
Sydney

- Six sets of twins:
  - "In the end, there were some cases of Windows Hello taking its time to identify a twin, but no case of it wrongly granting access."
  - But some false rejections when both enrolled on same computer
  - http://www.theaustralian.com.au

The Specs

- Authentication requires about 1 second
- 60 datapoints to construct vector map of face

- False Rejection Rate: 2-4%
- False Acceptance Rate: 1 in 100,000

- Liveness check can require the user to turn their head left and right a few centimeters

Settings

ACCOUNTS

Your account

Sign-in options

Work or school

Family & other users

Sync your settings

PIN

You can use this PIN to sign in to Windows, apps, and services.

Change | I forgot my PIN

Windows Hello

Sign in to Windows, apps and services using

Fingerprint

Add another | Remove

Face

Improve recognition | Remove

Automatically unlock the screen if we recognize your face

On

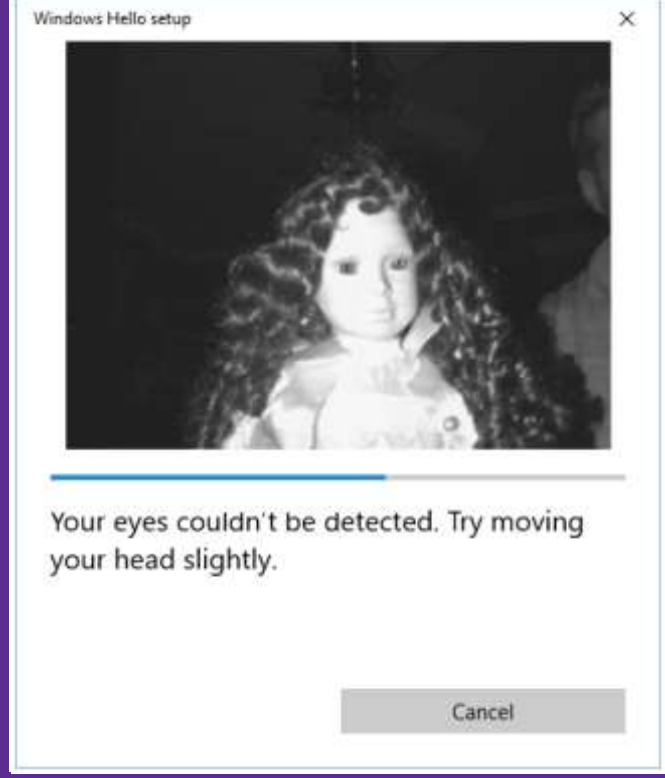
For extra security, require turning your head left and right to unlock the screen.

Off

Picture password

Sign in to Windows using a favorite photo

Add



Attacks

- 2D photograph will never work
- Maybe use multiple hi-res photographs from social media and a 3D printer to do an "evil twin" attack?
- After five scan failures, user must enter PIN
- TPM blocks further attempts after 32 PIN failures
- Facial geometry data encrypted with TPM or the user's logon passphrase, plus whole disk encryption

Microsoft Passport

Microsoft Passport = FIDO Authentication

- Passport = public/private key web authentication
  - To be used by both Edge and Universal apps
- Designed to work with Windows Hello biometrics
  - Unlocks access to user's private keys
- Conforms to FIDO Alliance standards
  - FIDO = Fast IDentity Online

The FIDO Alliance

- FIDO Board Members:
  - Microsoft
  - Google
  - PayPal
  - Bank of America
  - Visa
  - MasterCard
  - Samsung
  - And others
- www.fidoalliance.org

- FIDO Goals:
  - Replace passwords entirely (UAF)
  - Augment password auth (U2F)
  - Open scalable protocols
  - Support many auth device types
- Important:
  - One key pair per site, not shared
  - Each device enrolled separately

Passport Requirements (1 of 2)

- PKI not required, key pair may be self-generated
  - But a PKI may be used instead of using "raw" keys
- Public key linked to the user's account *somewhere*
- May use Azure AD, on-premises AD, a hybrid of the two with sync, or a third-party identity provider
  - Azure AD is Microsoft's main target (all roads lead to Azure now)
  - On-premises AD requires Server 2016 and a schema update
  - On-premises AD also requires AD Federation Services

Passport Requirements (2 of 2)

- Windows 10
  - Any edition
  - Any type of device: phone, tablet, laptop, PC, maybe Xbox
- Client device joined to Azure AD, to an on-premises AD domain, or BYOD with a "work account" added
- TPM or smart card preferred, but not required

Credential Guard

Purpose of Credential Guard

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

- Stops mimikatz (for now, hopefully forever)
  - https://github.com/gentilkiwi/mimikatz

Hardware & Firmware Requirements (1)

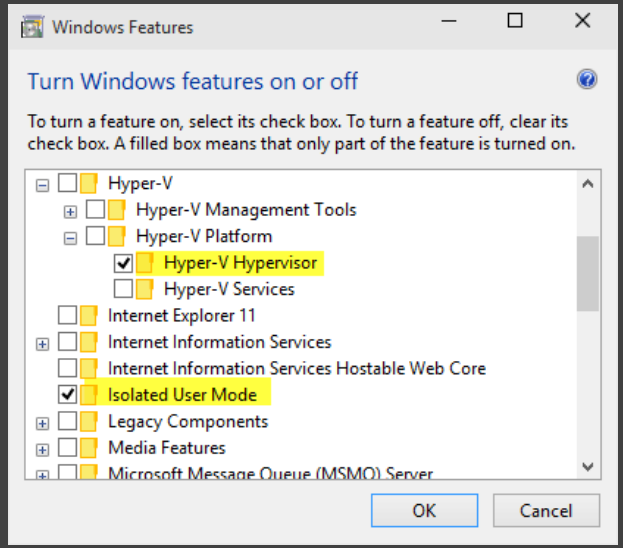
- UEFI 2.3.1 Secure Boot enabled and locked down
- TPM 1.2 or later in motherboard
- Intel VT-x or AMD RVI virtualization CPU extensions
- Intel EPT or AMD RVI Second Level Address Translation
- Intel VT-d or AMD-Vi IOMMU chipset support

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"

- So, it's not really a VM…
- VM has no desktop or protocol stack
- 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

Hardware + Firmware + Hypervisor

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)

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 Phone 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

O PowerShell
velut luna
statu variabilis
semper crescis
aut decrescis;
posh detestabilis
nunc obdurat
et tunc curat
ludo mentis aciem

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 …"

Incident Response & New AV API

- Greatly enhanced transcription logging
  - Includes scriptblocks, Base64, in-memory only, console
  - Encrypt transcript data with your own public key
- 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 and parameters allowed
  - Similar to setuid root + sudo + restricted bash + PowerShell remoting
- 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

Edge Browser

Internet Explorer Is Finally Dead?

- Edge not included in Long Term Servicing Branch
- Edge not included with Windows Server 2016 either
- Desktop SKUs will still have IE installed too
- Not many extensions available yet
- Edge does not support:
  - ActiveX
  - Browser Helper Objects
  - VBScript
  - SilverLight

Edge Security

- Will run in a Docker-style container (Q4'2017)
- Edge already runs in an AppContainer sandbox
- Flash runs in a separate AppContainer process too
- Control Flow Guard + Forced ASLR + DEP + SEHOP

Subsystem for Linux

Run Linux binaries on Windows

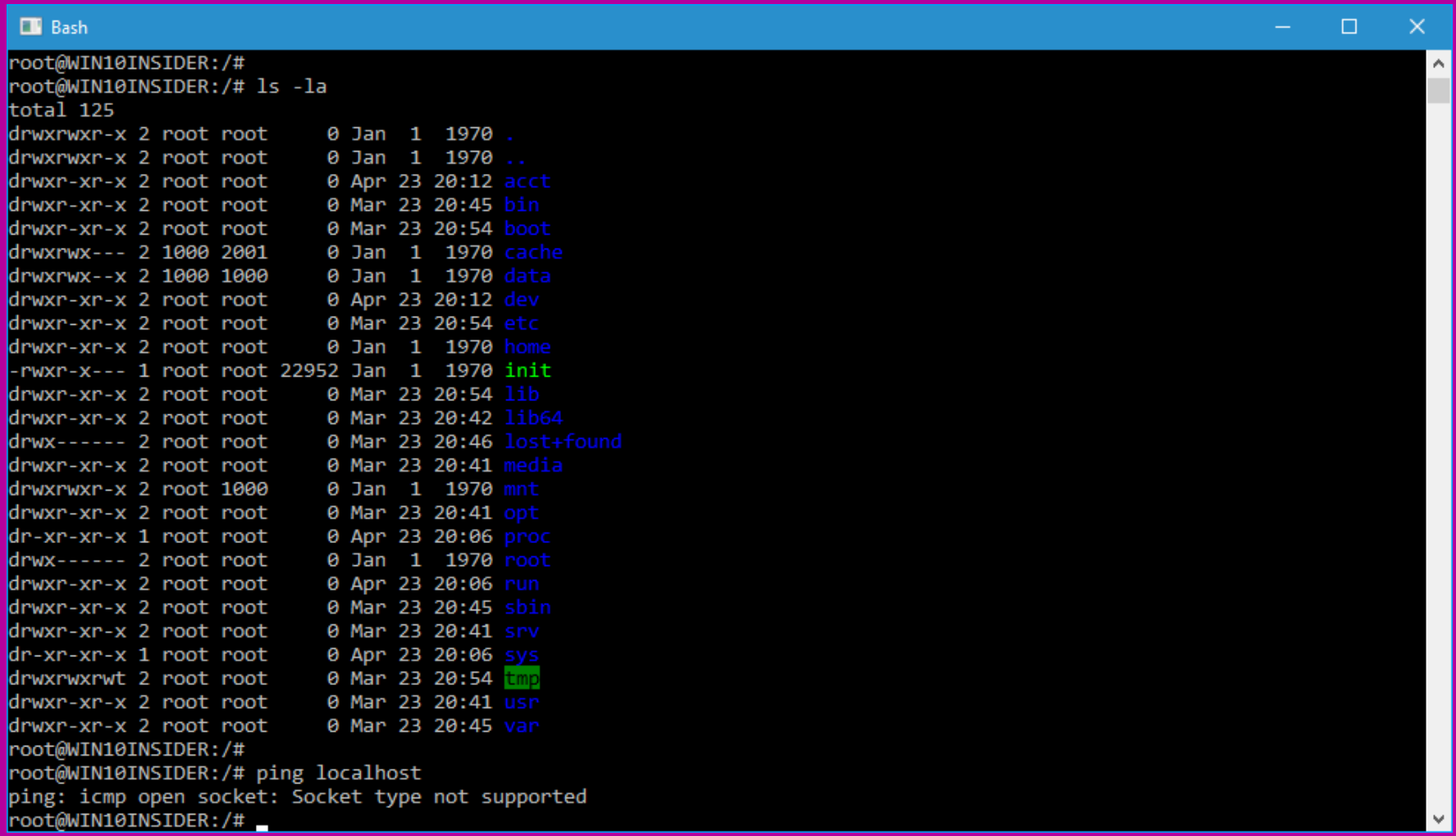
- Not a Linux virtual machine
- Not Cygwin
- Not the old Services for Unix (SFU), which included user-mode binaries written by Microsoft

- The Goal: allow developers and sysadmins to run unmodified, user-mode, command-line Linux binaries directly on Windows, including bash, ruby, python, grep, ssh, apt-get, gcc, Docker tools, etc.

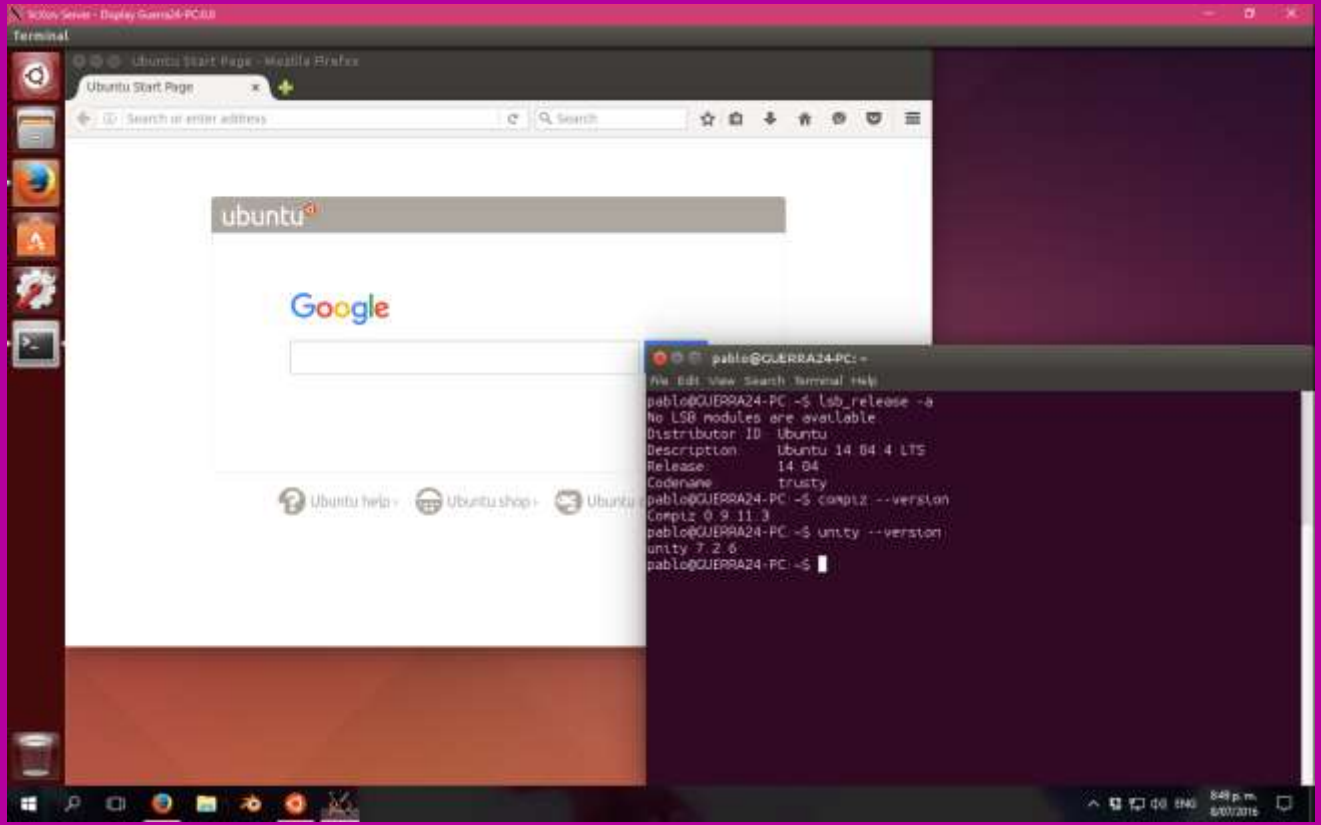
How does it work?

- Not enabled by default (go to Control Panel)

- Linux binary runs in a "pico process":
  - Pico processes do not include the Windows subsystem
  - Linux syscalls are intercepted (lxss.sys, lxcore.sys)
  - Windows kernel emulates Linux kernel APIs
  - Plan is to eventually implement all Linux syscall APIs


Bash
root@WIN10INSIDER:/#
root@WIN10INSIDER:/# ls -la
total 125
drwxrwxr-x 2 root root   0 Jan 1 1970 .
drwxrwxr-x 2 root root   0 Jan 1 1970 ..
drwxr-xr-x 2 root root   0 Apr 23 20:12 acct
drwxr-xr-x 2 root root   0 Mar 23 20:45 bin
drwxr-xr-x 2 root root   0 Mar 23 20:54 boot
drwxrwx--- 2 1000 2001   0 Jan 1 1970 cache
drwxrwx--x 2 1000 1000   0 Jan 1 1970 data
drwxr-xr-x 2 root root   0 Apr 23 20:12 dev
drwxr-xr-x 2 root root   0 Mar 23 20:54 etc
drwxr-xr-x 2 root root   0 Jan 1 1970 home
-rwxr-x--- 1 root root 22952 Jan 1 1970 init
drwxr-xr-x 2 root root   0 Mar 23 20:54 lib
drwxr-xr-x 2 root root   0 Mar 23 20:42 lib64
drwx------ 2 root root   0 Mar 23 20:46 lost+found
drwxr-xr-x 2 root root   0 Mar 23 20:41 media
drwxrwxr-x 2 root 1000   0 Jan 1 1970 mnt
drwxr-xr-x 2 root root   0 Mar 23 20:41 opt
dr-xr-xr-x 1 root root   0 Apr 23 20:06 proc
drwx------ 2 root root   0 Jan 1 1970 root
drwxr-xr-x 2 root root   0 Apr 23 20:06 run
drwxr-xr-x 2 root root   0 Mar 23 20:45 sbin
drwxr-xr-x 2 root root   0 Mar 23 20:41 srv
dr-xr-xr-x 1 root root   0 Apr 23 20:06 sys
drwxrwxrwt 2 root root   0 Mar 23 20:54 tmp
drwxr-xr-x 2 root root   0 Mar 23 20:41 usr
drwxr-xr-x 2 root root   0 Mar 23 20:45 var
root@WIN10INSIDER:/#
root@WIN10INSIDER:/# ping localhost
ping: icmp open socket: Socket type not supported
root@WIN10INSIDER:/#

Ubuntu GNOME Unity in Windows



This is not from Microsoft

Still very beta, but a taste of what's coming.

https://github.com/microsoft/bashonwindows/issues/637

Windows Server 2016

Server Nano

- Zero GUI: Nano runs completely headless
- Zero Disk: Can run from RAM drive with PXE boot

- ARM platform support possibly in 2017/2018 (rumor)
- Subsystem for Linux possibly in 2017/2018 (rumor)

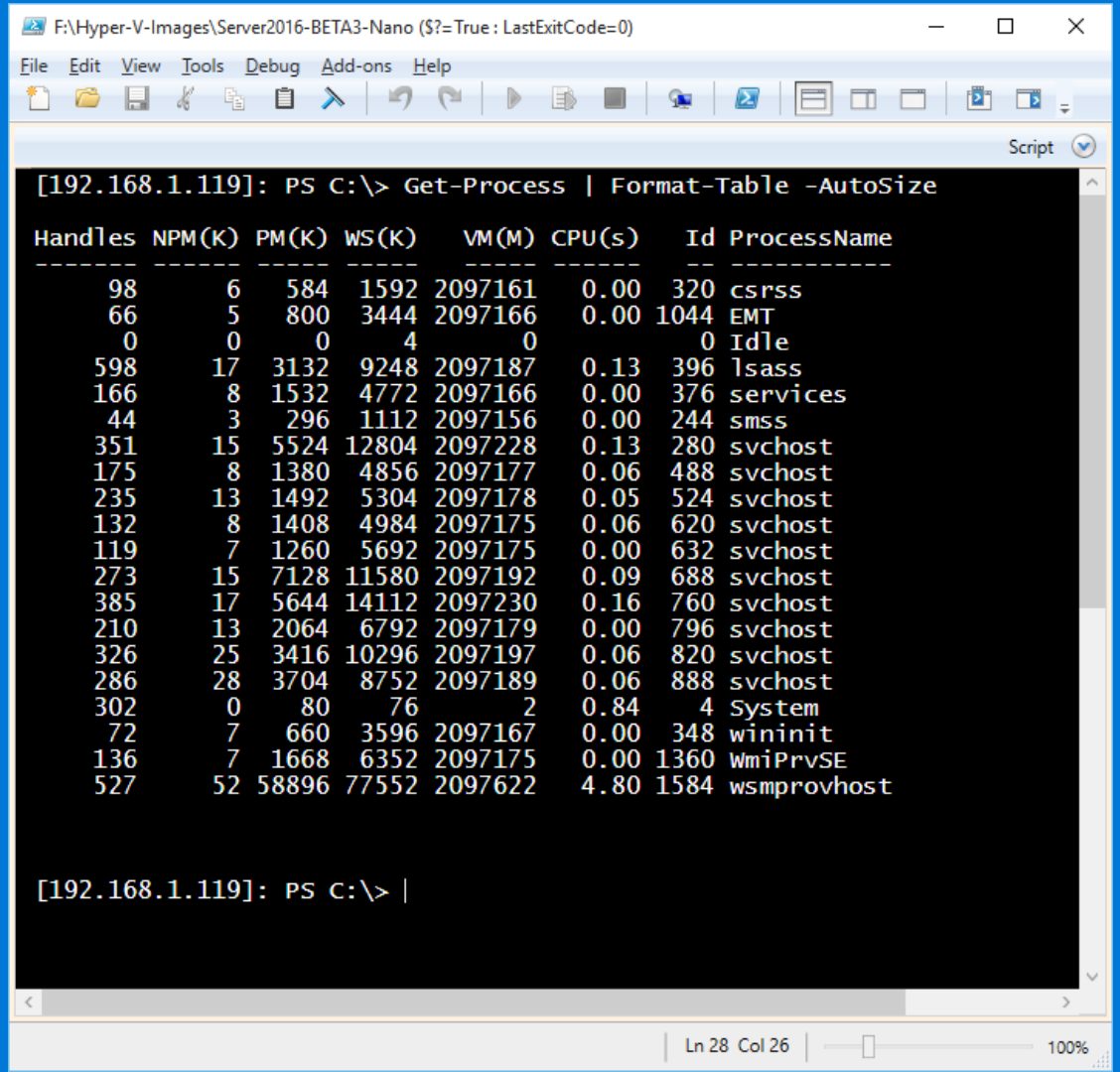
- Mainly intended for hosting VMs and web apps:
  - Already supports Hyper-V, Chef, PHP, Nginx, Python 3.5, Node.js, GO, Redis, MySQL, OpenSSL, Java (OpenJDK), Ruby 2.1.5, SQLite, and ASP.NET 5 (limited to Core CLR)


User name: _____
Domain: _____
Password: _____
ENTER Authenticate


Nano Server Recovery Console
Computer Name: Nano1
User Name: .\Administrator
Workgroup: WORKGROUP
OS: Microsoft Windows Server 2016 Datacenter
Local date: Monday, November 28, 2016
Local time: 6:23 AM
> Networking
Inbound Firewall Rules
Outbound Firewall Rules
WinRM
Up/Dn: Scroll | ESC: Log out | F5: Refresh | Ctl+F6: Restart
Ctl+F12: Shutdown | ENTER: Select

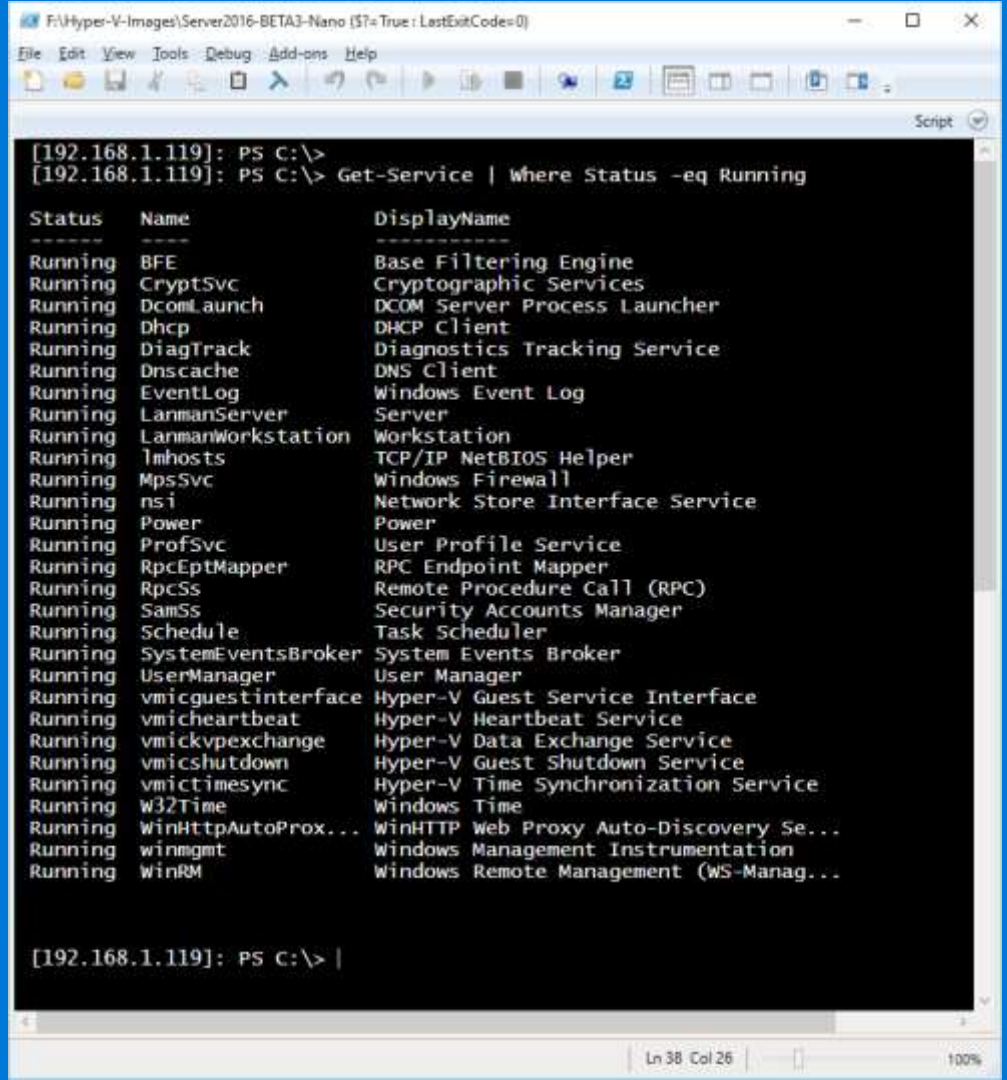
Default Processes:

PowerShell remoting into Nano box from admin laptop ->

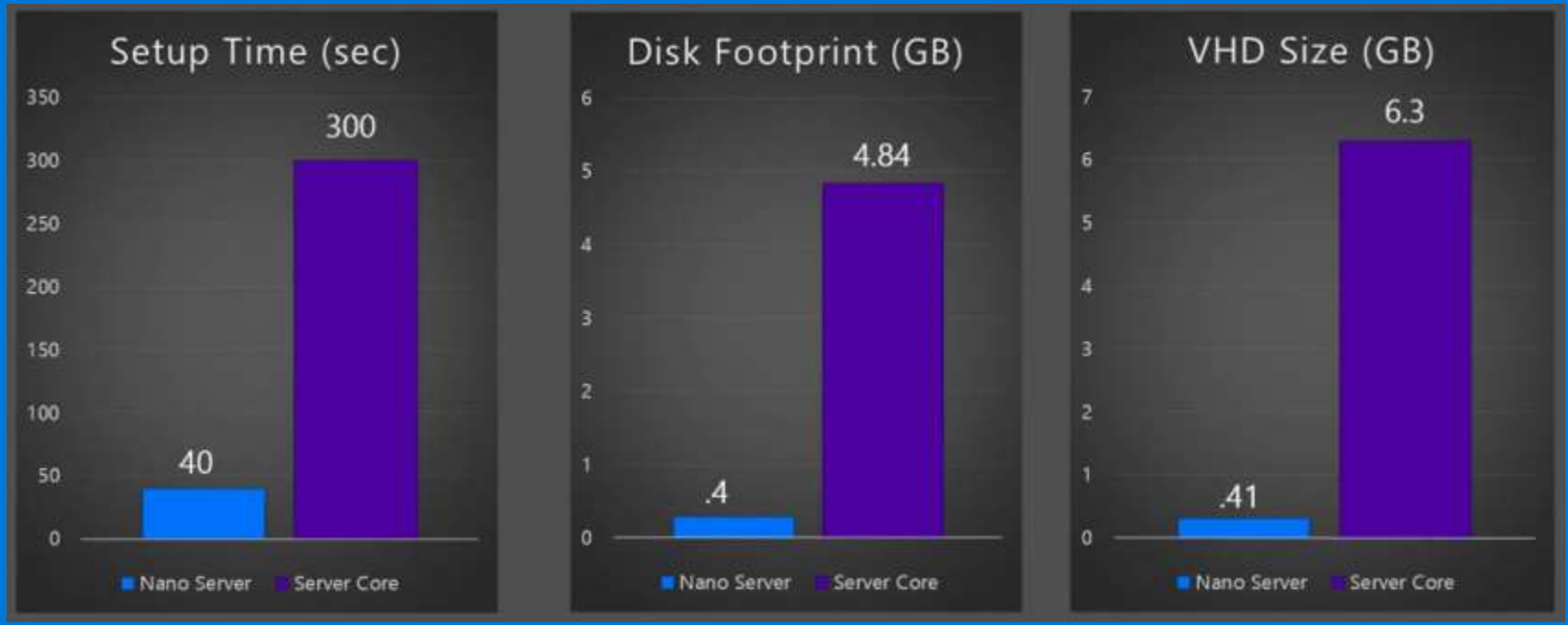


Default Services:

PowerShell remoting into Nano box from admin laptop ->

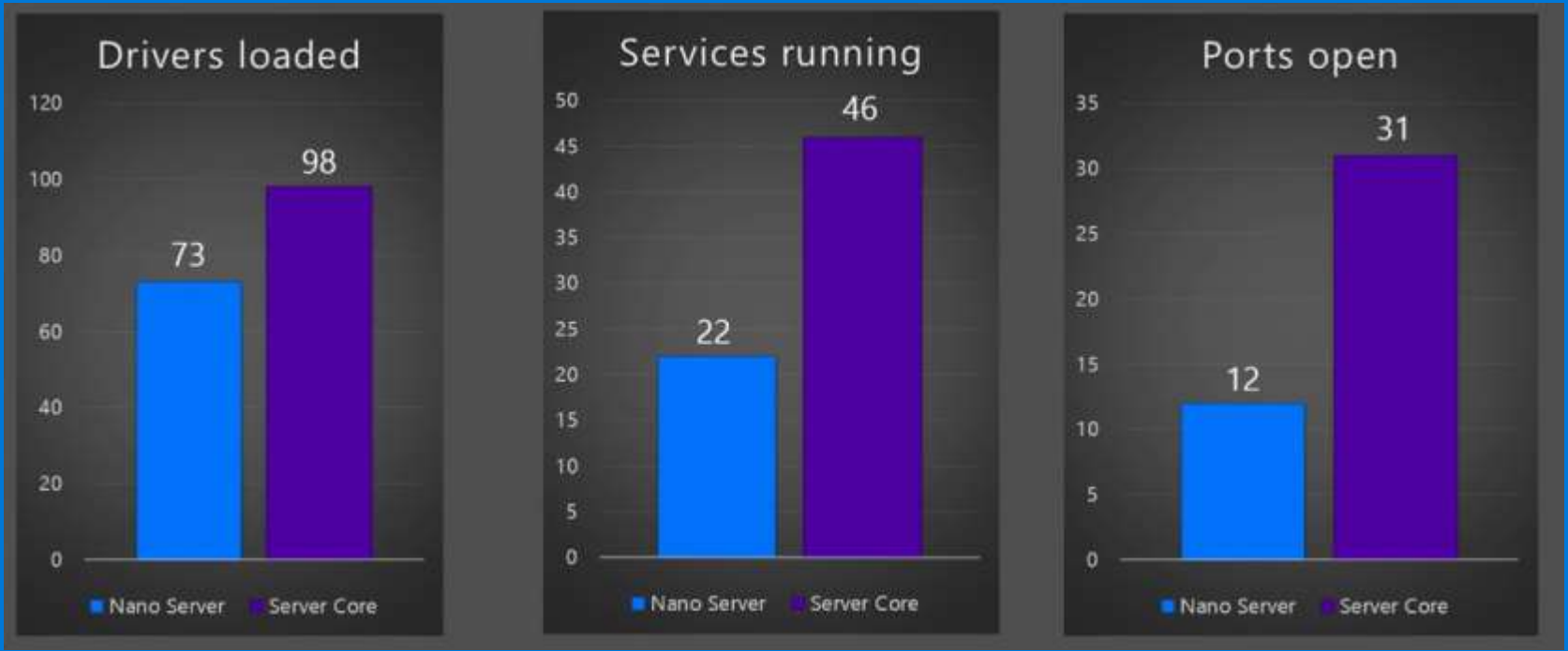


Nano vs. Core: Footprint



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

Licensing Headaches

- Server Nano
  - Must have Software Assurance agreement … *argh!* :-(
  - 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

Server 2016 Supports Docker Containers

- 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 two container runtimes:
  1. Traditional shared-kernel runtime
  2. Hyper-V isolated runtime
     - This is not 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 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 Instances
  - Standard Edition: 2 Max

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

Thank You for Attending!

- See you in my *Securing Windows* course (SEC505)?
  - http://sans.org/sec505
- Let's connect on LinkedIn and Twitter!
  - @JasonFossen
- Get my PowerShell scripts and this slide deck:
  - http://SEC505.info
  - Get the SEC505 zip file, then look in the \Extras folder