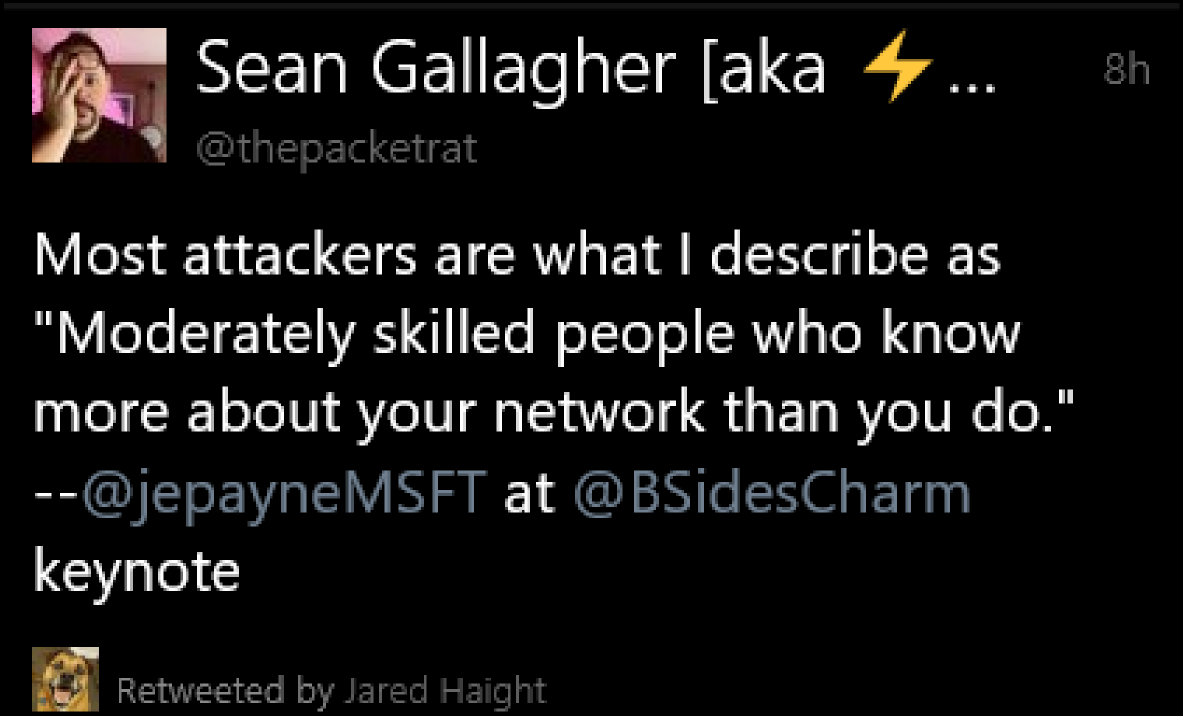
# Hardening your Windows Server Environment

**Orin Thomas**

**@orinthomas**

**Principal Cloud Operations Advocate**

orin.thomas@microsoft.com



Sean Gallagher [aka ⚡... 8h

@thepacketrat

Most attackers are what I describe as "Moderately skilled people who know more about your network than you do." --@jepayneMSFT at @BSidesCharm keynote

Retweeted by Jared Haight

# Caveats

- There is no perfect security solution
- You can harden your systems so that casual attackers move on to easier targets
- If you are being attacked by a nation state or an insanely competent attacker then you are $#$%#^!!d
- Aim to systematically do your best with the resources you have
- Server hardening is a journey …

# Aim of the Session

- Provide you with the information about your options for securing Windows Server environments
  - Focus on Server 2016 & 2019
  - Running the latest OS with all updates applied is more secure than running a 10 year old OS with all updates applied
- Keep turning the security dial setting by setting as your extingencies allow

# Domain Dominance

- Ultimate aim of attackers of Windows based networks is to get domain admin privileges
- Pwn a DC and you have access to every system in the network

# Baselines and Hardening

- Windows Server ships in a “moderately hardened” configuration
- There is more that you can do, but the more you do, the more you risk introducing problems into your environment

# Important Baselines

- Microsoft only publishes general baselines as part of the SCT
- National Checklist Repository
  - https://nvd.nist.gov/ncp/repository
  - Detailed low level guidelines
- Center for Internet Security
  - https://www.cisecurity.org/cis-benchmarks
- IASE Windows Server 2016 (Defense Information Systems Agency Security Technical Implementation Guide)(DISA STIG)
  - https://public.cyber.mil/stigs/downloads/
  - Noted by MS as a top-level security posture for Windows Server

# Challenges of Server Hardening

- Harden the servers too much and things stop working
- Harden servers in a manner commensurate with your organization’s risk profile
- Harden incrementally
  - Tighten, test, tighten rather than starting with a fully hardened configuration and then trying to debug it to make stuff work.
- Don’t invest in a $10,000 safe to protect a $1000 diamond

# Minimizing chance of log compromise

- Event Log Forwarding
  - Forward events from servers to a central location for collection and storage
- If attacker compromises server and clears logs, events are still stored in an alternate location
- Can also use Azure Monitoring to collect event data from on-prem/IaaS servers

# DC configuration

- DCs should always run most recent version of Windows Server
- Should be Server Core
- Should have device guard enabled
- Should be blocked from directly communicating with hosts on the internet
- Admin sessions (RDP/PowerShell) only from known PAW/Jump Server IP addresses

# Admin Accounts

- Lock down when and where an account can be used
  - Specify restricted logon times
  - Specify restricted logon locations
  - Specify account expiration
  - Ensure that password policies are enforced

# DEMO: LOGON RESTRICTIONS

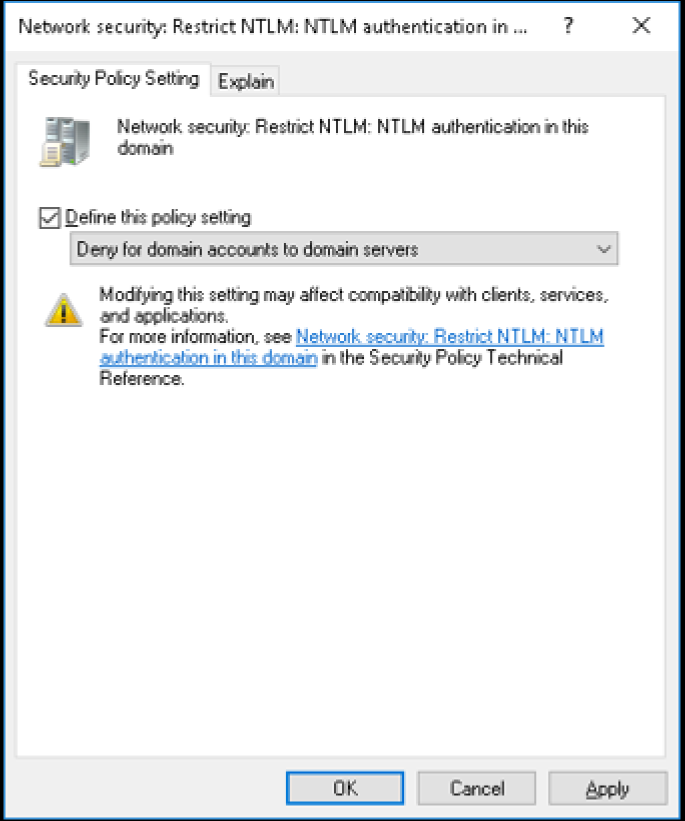
# Protected Users

- Special group in Server 2016 & 2019
- Members of this group
  - No cached credentials
  - Cannot use NTLM authentication
  - Cannot use older cipher suites for Kerberos pre-authentication
- Add all privileged accounts to this group to minimize chances of cached credential harvesting

# DEMO: PROTECTED USERS

# Disabling NTLM

- Prior to disabling, audit current use of NTLM
- Configure Network Security: Restrict NTLM authentication in this domain policy



Network security: Restrict NTLM: NTLM authentication in this domain

☑ Define this policy setting

Deny for domain accounts to domain servers

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: Restrict NTLM: NTLM authentication in this domain in the Security Policy Technical Reference.

# Credential Guard

- Uses virtualization based security to protect cached account credentials
- Used to mitigate pass-the-hash & pass-the-ticket attacks
- Does not allow
    - Unconstrained Keberos delegation
    - NTLMv1
    - MS-CHAPv2
    - Digest Authentication
    - CredSSP
    - Kerberos DES encryption

# ESAE Forests

- Admin forest is trusted in one way relationship by Production forest
- All admin accounts in Production forest are standard user accounts in Admin forest
- If admin account is compromised, it can’t be used to compromise other accounts in admin forest
- Any accounts that have admin privileges that aren’t hosted in Admin forest are suspect

# Principle of Least Privilege

- Assign minimum required rights to an account
- If account is compromised, attacker will only be able to perform limited set of tasks
- Create accounts to perform specific administrative tasks
- Avoid swiss army knife accounts

# PAWs and Jump Servers

- Locked down workstation that can only be used for administrative tasks
  - Blocked from accessing internet
  - Servers only accept admin connections from PAWs or Jump Servers
- Jump Server
  - Connection made to jump server
  - Admin connection made from jump server to target system to be managed

# Good Admin Habits

- Daily driver account used to read email, generate TPS reports should be standard user account
  - Should not be member of local Admins group
- Only use privileged accounts from PAWs to perform administrative tasks

# Just Enough Administration

- RBAC for Windows PowerShell remoting
- Specially configured endpoints limit access so that user can only use a defined set of PowerShell cmdlets, parameters, and parameter values
- Actions are performed using a special machine local virtual account

# Just Enough Administration

- Not appropriate where problem and solution are not clearly defined
- Requires that you understand exactly which cmdlets, parameters, aliases, and values are needed to perform specific tasks
- Only works with PowerShell sessions

# JEA Endpoint

- Connect to a specific endpoint to access JEA session
- A server can have multiple endpoints
- Account does not have to be privileged, only authorized to connect to a JEA endpoint

# DEMO: DNS & JEA

# Windows Admin Center

- Web based console for the remote administration of Windows Server
- Existing admin tools will be supported, but new admin functionality will be placed in Windows Admin Center
- Eventually will replicate functionality of all existing RSAT tools & MMCs
  - Not any time soon, you know, eventually

# Privileged Access Management

- Also known as Just in Time Administration
- Request privileged access using PowerShell or Web Interface
- Granted administrative privileges for a limited duration of time (by default 60 minutes)
- After 60 minutes expires, returned to normal unprivileged user configuration
- Requires
  - ESAE Forest to host admin accounts
  - Microsoft Identity Manager 2016

# PAM/JIT Administration

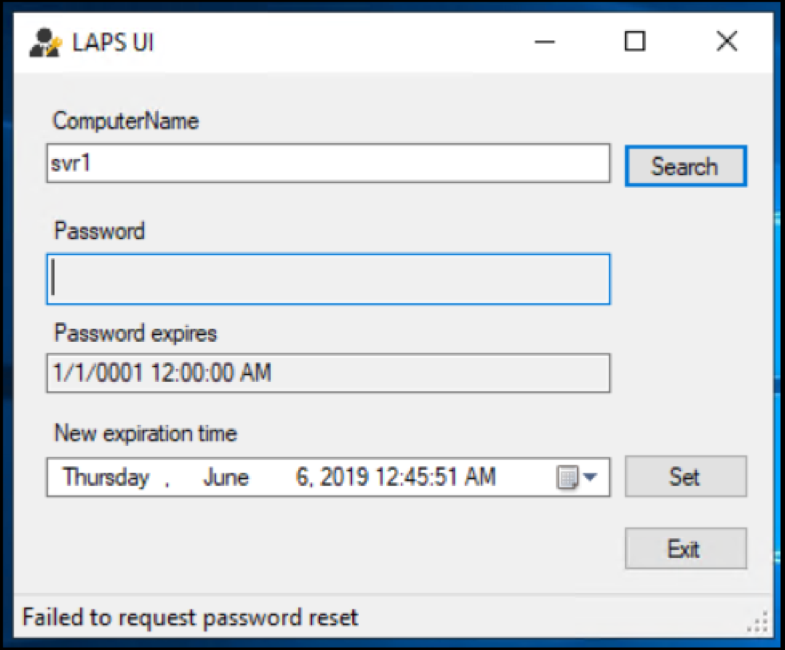
- Can specify which users are able to request privileges
- Can automatically allow some privileges whilst requiring approval for others
  - Approver does not need to be a privileged account
  - Can require MFA
  - Approver and requestor may be required to provide reason for request/approval
- Can be combined with Just Enough Administration

# Local Administrator Password Solution (LAPS)

- Local administrator passwords are unique on each computer that LAPs manages
- LAPS randomizes and changes local administrator passwords every 30 days
- LAPS stores local admin passwords and secrets within AD
- Configurable permissions
- Retrieved passwords transmitted in encrypted manner

# LAPS

- Works only with domain joined computers
- Requires only Server 2003 or higher AD functional level
- Does require schema extension
- Add computer accounts to an OU and then enable the OU to use LAPs
- Configure password policies in group policy
- View passwords in PowerShell, ADUC or the LAPS UI



ComputerName: svr1

Password:

Password expires: 1/1/0001 12:00:00 AM

New expiration time: Thursday , June 6, 2019 12:45:51 AM

Failed to request password reset

# Server Core

- Smaller attack surface than Server with a GUI
- Requires fewer software updates and reboots
- Can be managed using Windows Admin Center
- Use sconfig.cmd to perform basic configuration tasks
- Windows Server 2019 has improved Server Core functionality

# 2019 Server Core App Compatibility

- Improves app compatibility for Server Core by including set of binaries and packages from Server with GUI without adding Server with GUI experience
  - Performance Monitor (PerfMon.exe)
  - Resource Monitor
  - Device Manager
  - MMC
  - PowerShell ISE
  - Failover Cluster Manager
  - ProcMon & other Sysinternals

# DEMO: 2019 Server Core

# BitLocker

- Provides boot environment protection
- Provides encrypted storage protection
- MBAM tool allows you to integrate BitLocker management for domain joined devices into AD
  - Simplifies the process of BitLocker recovery

# Network Isolation Policies

- Use IPsec policies to restrict which hosts are able to communicate with servers
  - For example, block a file server from communicating with any computer that is not a member of the domain
  - Block sensitive servers from communicating with hosts that don’t have a computer certificate from a specific CA installed

# Group Managed Service Accounts

- Special type of account that can be used for services
- AD DS manages the service account password
- Requires Server 2012 or higher functional level
- Virtual accounts are local equivalent of GMSA

# Anti-Malware Configuration

- Windows Defender ATP is available in Server 2019
- Integrates with Microsoft Security Graph for behavior based detection of attacks
- Can also use Azure Security Center to manage security configuration of on-prem and IaaS servers
  - View issues such as lack of firewall configuration & missing updates

# Windows Defender Exploit Guard

- Exploit protection
  - Blocks malicious files, scripts, lateral movement, ransomware behavior
- Attack surface reduction rules
  - Brining EMET into the operating system
- Network protection
  - Block apps from communicating with untrusted network locations
  - Leverages SmartScreen
- Controlled folder access
  - Block untrusted apps
  - Mitigates Ransomware

# DEMO: Exploit Guard

# Security Compliance Toolkit

- Allows you to analyze and configure systems against security baselines
- Replacement for Security Compliance Manager

# Virtualization Dominance

- Virtualization fabric administrators can
  - Export VMs and exfiltrate their contents
  - Perform offline attacks against VMs
    - Offline dictionary attack against NTDS.dit on virtualized domain controller

# Shielded VMs

- Shielded VMs: Like “BitLocker” for VMs
  - VM is encrypted
  - VM will only boot if the virtualization fabric passes attestation integrity check
  - VM cannot be run on unapproved Hyper-V host
  - No local console connections, debuggers, access only using remote network administration tools

# Guarded Fabrics

- VM will only run on specific “pre-authorized” virtualization host
- Each virtualization host must pass
  - Verified TPM identity
  - Code integrity check
  - Measured boot sequence
- VM will  only run when Host Guardian Service attests to health & identity of VM host

# Shielded VM Templates

- VM owner can publish signed template and encrypted settings file to guarded fabric
  - Encrypted settings file includes all VM secrets such as local admin password
  - Inaccessible to virtualization fabric admnistrator
- VM template cannot be modified because of signature

# Windows Defender Application Guard

- When user visits untrusted site in Edge or Chrome, browser opens in isolated Hyper-V container
- This makes it difficult for malware that may be dropped using the browser to interact with the operating system
- Requires Enterprise/Pro edition of Windows 10
- 64 bit CPU with virtualization extensions & 8 GB of RAM
- Can block cut/paste from untrusted sites

# Windows Defender Device Guard

- Hardware based code integrity policies
- Uses Virtual Secure Mode blocks interaction of apps with sensitive parts of the operating system via virtualization
  - Kernel mode code integrity
  - User mode code integrity
- Requires TPM, Secure Boot, UEFI, and Virtualization Extensions

# Securing AD

- ESAE Forest
- Use RODC in locations where security is not assured
- Run virtualized DC as shielded VMs
- Use Security Configuration Manager to apply configuration baselines
- Use AppLocker and Device Guard to control execution of application and scripts
- Limit inbound RDP/PowerShell connection to known PAWs/Jump Servers
- Block traffic from domain controllers to and from Internet

# Securing DNS

- Configure DNS policies to mediate how queries are handled on the basis of the characteristics of the DNS request
- Configure DNSSEC and NRPT so that all internal DNS records are digitally signed and authenticated

# Securing DHCP

- Configure MAC address filtering so that only known MAC addresses can request IP addresses
- Configure secure dynamic DNS update settings
  - Restrict updates to static records
  - Restrict updates to records marked as sensitive
    - Block dynamic updates based on record type (MX, SRV, PTR, TXT etc)

# Securing File Servers

- Disable SMB1
- File Server Resource Manager File Screens
- Exploit Guard Controlled Folder Access to minimize chance of Ransomware encryption of sensitive files

# Securing IIS

- Deploy IIS on standalone server
  - Avoid deploying on a DC
- Only install required modules, don’t install every IIS option
- Run SQL and other servers on separate hosts
- Move INETPUB to separate volume instead of on OS volume
- Isolate web applications
  - Separate sites & application pools
- Isolate ASP.NET temp folders

# Securing IIS

- If using Windows Auth, turn on extended protection
- Do not allow anonymous writes to the server
- Enable request filtering rules
- Configure request limits based on how the IIS server is used
- Don’t use built in accounts for Application Pool identities
  - Virtual accounts are a good idea
- Enforce use of SSL/TLS and disable non TLS where possible
- Turn off debug mode for classic ASP application

# Containerizing Applications

- Where possible, shift applications into Server Core / Nano Server containers
- Easier to blow away a container that has become corrupted than it is to blow away a server that has become corrupted

# Easy Wins

- Upgrade your domain controllers to Server 2019
- Disable NTLM in your domain
- Implement privileged access workstations & limit where admin accounts can be used
- Add admin accounts to protected users group
- Deploy Local Administrator Password Solution

# Easy Wins

- Configure Domain Isolation Policies
- Deploy Group Managed Service Accounts
- Place unsupported operating systems on air-gapped/isolated "life support" networks that are inaccessible from the internet
- Deploy ATA/Azure ATP

# Q&A