Securing Windows Systems – Communicate changes with Spencer/Bryan

1. Adding yourself as part of the Admin Group with a new password
2. Changing Administer user password to something new
3. Remove users from Administrator group
4. Change users passwords
5. Look at Administrator Group and remove any users that you don’t know
6. Look at the Guest account and disable
7. Look at any other accounts (Default Account) and make sure disabled

Find out what version you are running – Communicate changes with Spencer/Bryan

1. Command prompt, type Winver and it tells you what version and build
2. Download and install MS security patches
   1. Windows Update Setting
   2. Check for updates

Look at Services running:

1. Netstat

Eternal Blue Security Patch link:

https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

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

**Link to Windows Security Policy Settings**: <https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/security-policy-settings>

**Audit tools for Windows to see holes**:

Dumpsec - https://www.systemtools.com/somarsoft/

Netcat - https://nmap.org/ncat/

Hyena - <https://www.systemtools.com/hyena/>

**Forensic Tools:**

EZ (Eric Zimmerman) Tools : <https://www.sans.org/tools/ez-tools/>

<https://www.sans.org/posters/eric-zimmerman-tools-cheat-sheet/>

https://reconshell.com/incident-response-resources/

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

**Netbios countermeasures** : Block TCP/UDP to 135-139 and 445 at Firewall

**Trojans/Backdoor countermeasures**: Block high listening ports on Firewall – some are 31337, 12345, 20034, 27374

List of ports : http://www.chebucto.ns.ca/~rakerman/trojan-port-table.html

**Active Dir Countermeasures**: Block 389 and 3268 at Firewall

**Disable SMB services**? - Files and Print Sharing for MS Networks from adapter under Network/Advance/Advanced Settings

**Add RestrictAnonymous –** regedit > HKLM\SYSTEM\CurrentControlSet\Control\LSA (Win2000)

Edit>Add Value

-Restrict Anonymous Reg\_DWORD Value to 1 (or 2 if Win 2000)

Regedit > HKLM\System\CurrentControlSet\Services\LanManServer\Parameters

-Set value to 1 in RestrictNullSessAccess

Hacking Anonymous logins:

Net use [\\10.0.0.26\ipc$](file:///\\10.0.0.26\ipc$) “” /u:’’ –This is bad because allows anonymous connections and a system. Countermeasure is to restrictanonymous

**Lock down SNMP**-Turn off SNMP service in Service Control Panel. If can’t shut down, remove default “public” and use private names or edit Registry to allow those systems access.

>HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities > Security > Permissions set to permit only approved users access.

>HKLM\System\CurrentControlSet\Services\SNMP\Parmemters\ExtensionAgents – delete value that contains “LANManagerMIB2Agent” then rename values 2, 3, and so on, until sequence begins with 1.

**Block DNS Zone Transfers**

Start>Programs>Administrative Tools> DNS and restrict Zone Transfer

Active Directory –

**Lock Down Registry Enumeration**

Check for remote access to registry:

OLDER Windows systems: >HKLM\System\CurrentControlSet\Control\SecurePipeServers\Winreg – if key present then restricted to Admins which is good

Windows 10> Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts-and-shares

**Turn off Dialup unless specifically needed for application**

OLD Windows systems: Dial-up connection settings are not kept in the Registry, but in a dedicated file. The path to this file is %APPDATA%\Microsoft\Network\Connections\Pbk\rasphone.pbk. Fortunately enough, this is an INI file, so it can be directly edited in Notepad; no need to delete it and re-create all connections from scratch.

Windows 10:

1. HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
2. From the Edit menu select New - String Value
3. Enter a name of RASDisable
4. Double click the new value and set to 1. Click OK
5. Close the registry editor

The change will take effect at next reboot and the logon using dial-up networking box will be greyed out.

**Determine what executables are running on the system**

Run command: dir /ah

On Windows 10 system, PF folder contains all programs running.

>\ Windows\Prefetch folder

> Make sure any remote access software such as PCAnyware, Remote FTP, etc are property set up.

Server has prefetch disabled by default. Enter all these commands into PS Administrator to get Prefetch working on a server:

reg add "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters" /v EnablePrefetcher /t REG\_DWORD /d 3 /f

reg add "HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Prefetcher" /v MaxPrefetchFiles /t REG\_DWORD /d 8192 /f

Enable-MMAgent -OperationAPI

net start sysmain

**Turn off Autorun/automount of CD/zip files**

https://support.languard.gfi.com/hc/en-us/articles/360016550120-Why-do-I-get-AutoRun-is-enabled-vulnerability-

>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

https://steflan-security.com/windows-privilege-escalation-exploiting-autorun/