**PA Firewall Hardening Plan (v.8.0.5)**

*PA Firewall Information:*

|  |  |
| --- | --- |
| IP address for MGT port: | 172.20.242.150 |
| Netmask: | 255.255.255.0 |
| Default Gateway: | 172.20.242.1 |
| Team | 6 |
| DNS server address: | [primary=Ubuntu 12.04] [secondary=2008 R2] |

1. Change Admin Password: Use PuTTY to sign in.

**configure**

**set mgt-config users admin password**

yellow monkey face (default = admin/admin) (admin/changeme)

**commit**

**exit**  (to leave configuration mode)

1. Past configuration script: <https://file.io/hPrtpX>

**set cli scripting-mode on** (make sure you’re not in configuration mode)

**configure**

(paste contents)

**commit**

1. Update default rules if present:
   1. In WebGUI, default rules: intrazone-default, interzone-default
   2. Click the Name of the policy and then “Override” in the bottom toolbar. Set both to Deny and Log at Session End.
2. Backup Configuration: (Manual: <https://file.io/wKFbBE> )
   1. Use GUI/Web Interface
3. Check for Updates:
   1. Download the base 6.0.1 (Do not install) and then the latest. (Install this one)
4. Update virus/threat definitions:
   1. In WebGUI, go to **Device > Dynamic Updates** and click “**Check now**.” After the new update is listed, download and install it.
   2. You can also manually download the updates from: <https://support.paloaltonetworks.com/Support/Index>
      1. Requires a valid Support Account
      2. Instructions: <https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PMZuCAO>

*make sure that port 21 is blocked to UbuntuDNS...in and out. It's configured for an anon FTP server running as root*

*Potential Injects:*

* Forward logs to splunk:
  + <https://splunkbase.splunk.com/app/491/>
* Marking packets as AF42
* Static IP NAT. (i.e. External IP 77.33.22.11 to internal 172.20.242.100 port 3389)
* After creating new user accounts on domain, sync users
* Custom URL blocking (i.e. facebook.com)

**Windows 8**

1. Change password (Default: binddn / !Password123 ) to **10 Pink Apples**
   1. [admin cmd]
      1. net user binddn “10 Pink Apples”
   2. [charms menu]
      1. Win+c
      2. “Settings” > Change PC Settings > Accounts > Sign-in options
      3. Under Password, click “change”
2. Fixing Problems:
   1. enable built-in admin account:
      1. <https://www.ghacks.net/2012/06/11/windows-8-enable-the-hidden-administrator-account/>
3. Download updates: [https://www.catalog.update.microsoft.com](https://www.catalog.update.microsoft.com/)

Windows Updates via Powershell (test)

<https://www.petri.com/manage-windows-updates-with-powershell-module>

1) Extract PSWindowsUpdate contets to C:\Windows\System32\WindowsPowerShell\v1.0\Modules

2) Open PowerShell (admin)

Set-ExecutionPolicy RemoteSigned

Import-Module PSWindowsUpdate

# Add-WUServiceManager -ServiceID 7971f918-a847-4430-9279-4a52d1efe18d

$KBList = "KB890830","KB4524445","KB4534309","KB4516115","KB3185319","KB4486105","KB4532940"

Get-WUInstall -Type "Software" -KBArticleID $KBList -AcceptAll -AutoReboot

Update Order:

(Manual Download: 773 MB not zipped)

**First Round**

1) KB890830

Windows Malicious Software Removal Tool x64 -Jan 2020

Run a Quick Scan.

2) KB4524445

Service Stack Windows Update (Latest for Jan 2020)

3) KB4534309

Security Only Windows Update (Jan 2020)

Restart

4) KB4516115

Adobe Flash Player (2019-09)

5) KB3185319

IE Cumulative Security Update (Same KB for IE 11, 10, 9)

6) KB4486105

Microsoft .NET Framework 4.8 for W 8.1 x64

Reboot

7) KB4535104 [KB4532940 , for 4.8 only]

Security and Quality Rollup for .NET 4.8

8) Run Windows Defender Update Bat file.

To install Sec Intel Update for Win Defender KB2267602

\* Will this work with “-removedefinitions” ? Takes a long time.

Hit enter after it says searching for updates.

**Second Round**

20.1) KB4534297

Monthly Rollup

Reboot

20.2) KB4516115

2019-09 Sec Update for Adobe Flash for Win 8.1 x64

1. Import GPO
   1. PowerSTIG?
      1. Install-Module -Name PowerSTIG
      2. <https://www.powershellgallery.com/packages/PowerSTIG/4.2.0>
      3. <https://github.com/microsoft/PowerStig>
         1. (oldest) .NET framework 4.6.2 offline installer win 8.1
            1. <https://www.microsoft.com/en-us/download/details.aspx?id=53344>
            2. <https://support.microsoft.com/en-us/help/4054530/microsoft-net-framework-4-7-2-offline-installer-for-windows>
         2. (newest) .NET framework 4.8 …
            1. <https://dotnet.microsoft.com/download/dotnet-framework/net48>
            2. Preview of quality rollup: KB4534134

<https://www.catalog.update.microsoft.com/Search.aspx?q=KB4534134>

* 1. Download LGPO and PolicyAnalyzer from Microsoft Sec. Analyzer:
     1. From Microsoft Securtiy Compliance Toolkit 1.0: <https://www.microsoft.com/en-us/download/details.aspx?id=55319> ?
  2. Import Local GP
     1. <https://techcommunity.microsoft.com/t5/microsoft-security-baselines/lgpo-exe-local-group-policy-object-utility-v1-0/ba-p/701045>

1. Ensure Defender is on and Updated:
   1. Ensure Defender is on:
      1. <https://docs.microsoft.com/en-us/intune-user-help/turn-on-defender-windows>
         1. If being blocked from changes: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/configure-local-policy-overrides-windows-defender-antivirus>
   2. Update:
      1. UpdateDefender.bat

cd %ProgramFiles%\Windows Defender

MpCmdRun.exe -removedefinitions -dynamicsignatures

MpCmdRun.exe -SignatureUpdate

* + 1. Manual download: <https://www.microsoft.com/en-us/wdsi/defenderupdates>

1. Check for other accounts
2. Firewall:
   1. Turn on
3. Download Microsoft Baseline Configuration Manager 2.0
   1. <https://www.microsoft.com/en-us/download/details.aspx?id=16475>

*Potential Injects:*

* Set login banner
  + **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\winlogon\**
  + **Edit the LegalNoticeCaption and put a title text like “Warning” and,**
  + **edit the LegalNoticeText and put a message like “I have the owner ship!”**
  + **Could also be:**
    - **POLICY\_KEY = “HKLM\Software\Microsoft\Windows\CurrentVersion\policies\system\”**
    - **Const LEGAL\_CAPTION\_VALUENAME = “legalnoticecaption”**
    - **Const LEGAL\_TEXT\_VALUENAME = “legalnoticetext”**
  + **Or:** 
    - Run -> secpol.msc -> Local Policies -> Security Options -> "Interactive logon: Message text for users attempting to log on" and change/remove the text here.
* Set ntp
  + Right click clock > Adjust Date/Time
  + Tab: Internet Time > Change Settings…(admin)
  + Type server name, click update then ok.
* Forward logs to splunk
  + <https://splunkbase.splunk.com/app/3067/>

**NTP Servers:** <https://www.ntppool.org/en/use.html>

1.north-america.pool.ntp.org

2.pool.ntp.org

**Windows 8: to fix (from enumeration)**

duck duck go works but google does not

* smb message signing, turn on
* ports to close:
  + Microsoft Windows RPC
  + OpenSSH

Scanned at 2020-02-03 11:53:29 CST for 394s

Not shown: 65523 closed ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn

445/tcp open netbios-ssn

23570/tcp open ssh OpenSSH 7.2 (protocol 2.0)

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49156/tcp open msrpc Microsoft Windows RPC

49157/tcp open msrpc Microsoft Windows RPC

49160/tcp open msrpc Microsoft Windows RPC

49161/tcp open msrpc Microsoft Windows RPC

Use regshot to monitor registry?

Turn off Remote Desktop:

Possibly:

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG\_DWORD /d 1 /f

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG\_DWORD /d 0 /f

If everything else errors out, set a rule to turn off the firewall just because.

if %errorlevel%==1 netsh advfirewall firewall set service type = remotedesktop mode = disable

[**https://github.com/mike-bailey/CCDC-Scripts/blob/master/WINDOWS.md**](https://github.com/mike-bailey/CCDC-Scripts/blob/master/WINDOWS.md)

**Clean DNS**

ipconfig /flushdns

**Clear the HOSTS file?**

Before we can clear it we have to actually get access to it, hence the attrib command. -r clears any read-only bit and -s removes it's designation as a system file.

echo Writing over the hosts file...

attrib -r -s C:\WINDOWS\system32\drivers\etc\hosts

echo > C:\Windows\System32\drivers\etc\hosts

**Services:**

echo Showing you the services...

net start

echo Now writing services to a file and searching for vulnerable services...

net start > servicesstarted.txt

**Disabling Services:**

net start | findstr “Remote Registry”

if %errorlevel%==0 (

echo Remote Registry is running!

echo Attempting to stop...

net stop RemoteRegistry

sc config RemoteRegistry start=disabled

if %errorlevel%==1 echo Stop failed... sorry...

) else (

echo Remote Registry is already indicating stopped.

)

**Remove Windows Saved Credentials:**

//shouldn’t this be echo// REM Remove all saved credentials

cmdkey.exe /list > "%TEMP%\List.txt"

findstr.exe Target "%TEMP%\List.txt" > "%TEMP%\tokensonly.txt"

FOR /F "tokens=1,2 delims= " %%G IN (%TEMP%\tokensonly.txt) DO cmdkey.exe /delete:%%H

del "%TEMP%\\*.\*" /s /f /q

**Disabling Accounts: Use for Guest, and the two accounts already in there**

REM Guest Account is deactivating

net user Guest | findstr Active | findstr Yes

if %errorlevel%==0 echo Guest account is active, deactivating

if %errorlevel%==1 echo Guest account is not active, checking default admin account

net user Guest /active:NO

**Disabling Default Admin (checks if ou’re default admin first)**

**echo Making sure you are not on the default admin account...**

net user | findstr Administrator

if %errorlevel%==0 (

echo "Administrator" account exists

echo Looking to see if you are on it

if "%username%"=="Administrator" (

echo Awkward, you ARE the Administrator account

goto :skipcode

)

net user Administrator /active:NO

)

:skipcode

**Password Reset**:

set /p newpwd=Enter a new password for your accounts:

net users > userlist.txt

(

for /F %%h in (userlist.txt) do (

echo %%h | findstr NEXS

if %errorlevel%==1 net user %%h %newpwd% >> userlist.txt

)

)

**Firewall:**