Windows 2012 R2 Hmail Checklist

**Phase 1:**

1. **Change Administrator password**

*net user Administrator [password]*

1. **Create local backup administrator**

*net user [name] [password] /add*

*net localgroup Administrators [name] /add*

1. **Baseline users && Lower Privileges && Disable**

*net user > C:\users.txt*

*net localgroup Administrators*

*net localgroup Administrators [backdoor] /delete*

*net user [backdoor] /active:no*

*Net user Guest /active:no*

1. **Kill explorer.exe**

*Taskkill /f /im iexplore.exe*

*Taskkill /f /im chrome.exe*

*Taskkill /f /im firefox.exe*

*taskkill /f /im explorer.exe*

*C:\Windows\explorer.exe* ORWin + R -> C:\Windows\explorer.exe OR

CTRL + ALT + DELETE -> Task Manager -> C:\Windows\explorer.exe

1. **Set DNS upstream forwarder to 1.1.1.1, uncheck Root hints**

Server manager > Tools > DNS > Right Click Domain > Properties > Forwarders > Edit > 1.1.1.1, uncheck root hints

1. **REPEAT PASSWORD CHANGES ON ADMINS and BACKUP ADMINS**

*Net user [name] [newpassword]*

1. **Baseline services**

*wmic service list brief > C:\servicebrief.txt*

*wmic service list full > C:\servicefull.txt*

1. **Baseline connections**

*netstat -abno > %USERPROFILE%\Desktop\ports.txt*

*nestat -abno | find /i “LISTENING” > C:\listeningports.txt*

1. **Audit Running Processes**

*tasklist /v > C:\processes.txt*

1. **Audit Scheduled Tasks**

*schtasks > C:\schtasks.txt*

1. **Delete All Scheduled Tasks**

*schtasks /delete /TN \* /F*

1. **Audit DNS cache**

*ipconfig /displaydns > C:\dnscache.txt*

*Ipconfig /displaydns >*

1. **Disable IIS (UNLESS UR THE IIS SERVER)**

*iisreset /stop*

1. **Screenshot && Delete recently installed programs**

*appwiz.cpl*

1. **Investigate Scored Services (Direct and Indirect) and screenshot**

Look at network connections (netstat -anbo, resource monitor)

Look at processes (taskmgr.exe)

Look at logs

1. **Audit firewall rules && Delete && Set Broad Rules && Configure Firewall Logs**

Audit:

*netsh advfirewall firewall show rule name=all > C:\fwrules.txt*

Delete:

*netsh advfirewall firewall delete rule name=all*

*wf ->*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Dir** | **Name** | **Program** | **Pro.** | **LPort** | **Remote IP** |
| I | Scored | Any | TCP | 25,80, 443, 110,143, 139, 445, 3389 | Any |
| I | Scored-DNS-In | C:\Windows\System32\dns.exe | UDP | 53 | Any |
| I | lanlocal | Any | Any | Any | 127.0.0.0/8,172.20.240.0/22,172.25.#.0/24,172.25.20+#.0/24 |
| O | Firefox | C:\Program Files\Mozilla Firefox\firefox.exe | TCP | Any | Any |
| O | DNS-Out | C:\Windows\System32\dns.exe | UDP | 53 | Any |
| O | lanlocal | Any | Any | Any | 127.0.0.0/8,172.20.240.0/22,172.25.#.0/24,172.25.20+#.0/24 |

Turn on, set default policy:

*netsh advfirewall set allprofiles state on*

*netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound*

Logging:

If 2012 or older:

*netsh firewall set logging C:\fwlogs.txt 32767 ENABLE ENABLE*

If 2016 or newer:

*wf ->* Firewall Properties

On all profiles logging to C:\fwlogs.txt, 32676 bytes, Yes Yes

1. **Scored Service Backups:**

IIS: backup inetpub directory

Copy %SystemDrive%\inetpub\

*cd c:\Windows\system32\inetsrv*

*appcmd add backup [backupname]*

Restore Backup:

Copy backup folder to c:\Windows\system32\inetsrv\backup

*appcmd restore backup [backupname]*

Hmail backup:

*net stop hmailserver*

*net stop hmailservermysql*

*Cd C:\Program Files (x86)\hMailServer*

*Xcopy Data C:\hmaildata /S /Y /M*

*Xcopy Database C:\hmaildatabase /S /Y /M*

*Xcopy bin\\*.ini C:\hmailbin\\*.ini /S /Y /M*

*net start hmailservermysql*

*net start hmailserver*

Restore hmail:

*net stop hmailserver*

*net stop hmailservermysql*

*Xcopy C:\hmaildata \data /Y /S /M*

*Xcopy C:\hmaildatabase \Database /Y /S /M*

*Xcopy C:\hmailbin\\*.ini \bin\\*.ini /Y /S /M*

*net start hmailservermysql*

*net start hmailserver*

Backup MySQL:

*cd C:\Program Files\mysql\[mysql version]\bin*

*mysqldump.exe -u root -p [password] [database name (or --all-databases)] > backupname.sql*

*mysql -u root -p [password] < backupname.sql*

**Phase 2:**

1. **Download Firefox or Chrome**

[*https://www.mozilla.org/en-US/firefox/new*](https://www.mozilla.org/en-US/firefox/new)

[*https://www.google.com/chrome*](https://www.google.com/chrome)

1. **Download Nessus**

<https://www.tenable.com/downloads/nessus>

Keys:

04DC-496C-9135-2406-D239

**NESSUS NEEDS IT OWN FIREWALL RULES!!!**

C:\Program Files\Tenable\Nessus\nessusd.exe in/out any any

<https://community.tenable.com/s/article/What-ports-are-required-for-Tenable-products>

netsh advfirewall firewall add rule name=“NESSUS-IN” dir=in action=allow protocol=TCP localport=8834

netsh advfirewall firewall add rule name=”NESSUS-OUT-TCP” dir=out action=allow protocol=TCP

localport=443,25 program= %ProgramFiles%\Tenable\Nessus\

netsh advfirewall firewall add rule name=”NESSUS-OUT-UDP” dir=out action=allow protocol=UDP localport=53

1. **Install Notepad++**

<https://notepad-plus-plus.org/downloads/>

1. **Download Process Hacker**

<https://processhacker.sourceforge.io/downloads.php>

1. **Download Autoruns**

<https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>

1. **Download Process Monitor**

<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>

1. **Download Python 3.8**

<https://www.python.org/downloads/release/python-381/>

1. **Download PuTTY**

<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

1. **Download Wireshark**

<https://www.wireshark.org/>

1. **TFTPD**

<https://sourceforge.net/projects/tftp-server/>

1. **Download & Configure Splunk Forwarder**

<https://www.splunk.com/en_us/download/universal-forwarder.html>

secseczulu : Password123!

*C:\Program Files\SplunkUniversalForwarder\etc\system\local\inputs.conf*

[WinEventLog://Microsoft-Windows-Sysmon/Operational]

disabled=false

renderXml=true

1. **Create Shared Folder on Administrator Desktop**

Place the following:

Autoruns

Process Hacker

Splunk Forwarder

Notepad++

Putty

Wireshark

Python 3.8

1. **Initialize GPO Security Audit Logs**
2. **Configure DNS Logs**
3. **Disable NetBIOS and IPv6**

*ncpa.cpl*

1. **Disable utilman.exe**

*takeown.exe /A /F %windir%\system32\utilman.exe*

*cacls %windir%\system32\utilman.exe /C /D Everyone*

1. **Lower dns.exe port pool to 50**

*dnscmd /Config /SocketPoolSize 50*

*net stop dns && net start dns*

1. **Disable RDP**

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\fDenyTSConnections : 1*

1. **Disable Spooler, DCOM Launcher & UPNP**

*services.msc*

Print Spooler

DCOM Server Process Launcher

UPnP Device Host

1. **Disable LLMNR**

*Computer Configuration\Administrative Templates\Network\DNS Client\Turn Off Multicast Name Resolution policy by changing its value to Enabled*

1. **Establish Redundant services**

Create folder on Administrator Desktop

Place backup files in new directory

From new directory, open Command Prompt

*python -m http.server 1234*

Shout to Gavin/Windows team to let them know this is up!

**Phase 3:**

1. **Disable Automatic Proxy settings**
2. **Disable Administrative Shares**

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters*

Create new DWORD named *AutoShareWks* and set it to 0

1. **Disable DCOM**

Right click My Computer -> *Properties* -> Deselect *Enable Distributed COM*

1. **Force RDP to always prompt for password**

*Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt for password upon connection*

*“Enabled”*

1. **Disable RDP Local Resources**

*Computer Configuration\Policies\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Device and Resource Redirection*

1. **Inspect Startup Registry keys (for both local machine and current user)**

*[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]*

*[HKLM\Software\Microsoft\Windows\CurrentVersion\Run]*

*[HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce]*

*[HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices]*

*[HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]*

*[HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit]*

*[HK\_CU\Software\Microsoft\Windows\CurrentVersion\Run]*

*[HK\_CU\Software\Microsoft\Windows\CurrentVersion\RunOnce]*

*[HK\_CU\Software\Microsoft\Windows\CurrentVersion\RunServices]*

*[HK\_CU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]*

*[HK\_CU\Software\Microsoft\Windows NT\CurrentVersion\Windows]*

*[HKLM\System\CurrentControlSet\Control\Session Manager\subsystems]*

1. **Inspect Startup GPOs/Default GPOs & Startup folders**

*Computer Configuration\Policies\Windows Settings\Scripts\Startup*

*User Configuration\Policies\Windows Settings\Scripts\Logon*

*%USERPROFILE%\AppData\Roaming\Microsoft|Windows\Start Menu\Programs\Startup*

*%WINDIR%\Start Menu\Programs\Startup*

1. **Disable network discovery (network and sharing center)**
2. **Monitor ARP table**

*arp -a*

*route /print*

1. **Monitor Sessions:**

Computer Management > Shared Folders > Sessions

**NTP Server Configuration:**

1. **SET TIME ZONE TO CST (UTC-06:00)**
2. **Unregister & re-register w32tm (reset Registry)**

*net stop w32time*

*w32tm /unregister*

*w32tm /register*

*net start w32time*

1. **Source NTP from external server**

*w32tm /config /manualpeerlist:”time.google.com,0x1” /syncfromflags:manual /reliable:yes /update*

1. **Configure NTP Server**

*w32tm /config /syncfromflags:domhier /update*

Change Registry Key to “NTP”:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type : NTP*

<https://support.microsoft.com/en-us/help/816042/how-to-configure-an-authoritative-time-server-in-windows-server>

*\*THIS WILL FORCE LOCAL SYNC TO LOCAL CMOS, BUT PUSH THAT TIME OUT TO ALL CLIENTS*

1. **Configure logging:**

*w32tm /debug /enable /file:C:\windows\temp\w32time.log /size:10000000 /entries:0-300*

**Palo-user ID Integration:**

1. **Group policy management and right click default domain policy > edit**
2. **“Audit account logon events”**

*Config\Local Policies\Windows Settings\Security Settings\Local Policies\Audit Policies\Audit Account Logon Events*

1. **Apply policy**

*gpupdate*

1. **Create useragent : Password123!**

Add user to:

Distributed COM

Event log readers

Server operators

1. **Open WMI Manager (LOCAL)**

*wmimgmt.msc*

1. **Right click, select “Properties”**
2. **Open Root, CIMV2, Security**

Add useragent

**DNS Troubleshooting:**

1. **Verify integrity of hosts file**

*type %windir%\system32\drivers\etc\hosts*

There should not be any specific configurations there!

1. **Uncheck root hints**
2. **Verify integrity of A and MX records**

*DNS Manager*

1. **Verify DNS Forwarder**

*8.8.8.8*

1. **Verify 53 inbound firewall rule**

*wf*

1. **Analyze DNS logs (are we receiving queries?)**

Check firewall drops if we are not receiving logs

1. **Can I translate?**

*ipconfig /flushdns*

*nslookup [name]*

Who is my DNS Server? Is it me? 127.0.0.1?

1. **Is everyone’s default DNS server my IP?**
2. **Did any IP addresses change? Were any boxes added?**

**RDP Troubleshooting:**

1. **Verify port 3389 is allowed inbound**

*wf*

1. **Verify user/group is allowed to RDP to Domain Controller**

*Domain Controllers\Default Domain Controllers Policy -> Computer Configuration\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services*

1. **Verify RDP is on through Registry**

*regedit*

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\fDenyTSConnections : 0*

**Configure Certificate Services (directions courtesy of Microsoft):**

1. Log on as a member of both the Enterprise Admins group and the root domain's Domain Admins group
2. In Server Manager, click Manage, and then click Add Roles and Features. The Add Roles and Features Wizard opens
3. In Before You Begin, click Next.
4. In Select Installation Type, ensure that Role-Based or feature-based installation is selected, and then click Next.
5. In Select destination server, ensure that Select a server from the server pool is selected. In Server Pool, ensure that the local computer is selected. Click Next.
6. In Select Server Roles, in Roles, select Active Directory Certificate Services. When you are prompted to add required features, click Add Features, and then click Next.
7. In Select features, click Next.
8. In Active Directory Certificate Services, read the provided information, and then click Next.
9. In Confirm installation selections, click Install. Do not close the wizard during the installation process. When installation is complete, click Configure Active Directory Certificate Services on the destination server. The AD CS Configuration wizard opens. Read the credentials information and, if needed, provide the credentials for an account that is a member of the Enterprise Admins group. Click Next.
10. In Role Services, click Certification Authority, and then click Next.
11. On the Setup Type page, verify that Enterprise CA is selected, and then click Next.
12. On the Specify the type of the CA page, verify that Root CA is selected, and then click Next.
13. On the Specify the type of the private key page, verify that Create a new private key is selected, and then click Next.
14. On the Cryptography for CA page, keep the default settings for CSP (RSA#Microsoft Software Key Storage Provider) and hash algorithm (SHA2), and determine the best key character length for your deployment. Large key character lengths provide optimal security; however, they can impact server performance and might not be compatible with legacy applications. It is recommended that you keep the default setting of 2048. Click Next.
15. On the CA Name page, keep the suggested common name for the CA or change the name according to your requirements. Ensure that you are certain the CA name is compatible with your naming conventions and purposes, because you cannot change the CA name after you have installed AD CS. Click Next.
16. On the Validity Period page, in Specify the validity period, type the number and select a time value (Years, Months, Weeks, or Days). The default setting of five years is recommended. Click Next.
17. On the CA Database page, in Specify the database locations, specify the folder location for the certificate database and the certificate database log. If you specify locations other than the default locations, ensure that the folders are secured with access control lists (ACLs) that prevent unauthorized users or computers from accessing the CA database and log files. Click Next.
18. In Confirmation, click Configure to apply your selections, and then click Close.

**Command Line Application commands:**

* *mmc :* Microsoft Management Console
* *gpmc :* Group Policy Management
* *admgmt :* AD Manager
* *dssite :* Domain Sites/Services
* *dsa.msc :* Active Directory Users and Computers
* *gpmc :* Domain Group Policy Manager
* *gpedit :* Local Group Policy Editor
* *dnsmgmt :* DNS Manager
* *dhcpmgmt* : DHCP Manager
* *wf :* Windows Firewall with Advanced Security
* *lusrmgr :* Local Users and Groups
* *control :* Control Panel
* *ncpa.cpl :* Network Adapter Panel
* *compmgmt :* Computer Manager (Task Scheduler, Event Viewer, Shared Folders)
* *explorer :* Windows Explorer (aka File Explorer)
* *appwiz.cpl :* Programs and Features
* *doskey /HISTORY :*

**Useful Commands:**

* *dir <filename.ext> /S /B :* find file in directory by name
* *net user <username> <password> /add /logonpasswordchg:yes :* Add user, require password change upon logon
* *wmic process where ProcessId=# get ExecutablePath*
* *wmic /? :* search for any alias (process, service, useraccount, etc.)
* *wmic <alias> get /? :* get information regarding any alias