**Basic Hardening Guide UNT CCDC 2014**

**Windows Server 2012**

**Note:** Windows 2012 has Metro UI(same as Windows 8) . To access any system tool, press windows key and start typing its name. Also server manager icon is by default firsr button on task bar, at bottom-left corner

To get run box type Windows+R.

* Change Local admin password (Server manager->Tools->Computer Manager -> ‘Local Users and Groups’ -> ‘users’ -> right click on ‘administrator’ -> ‘change password’) **OR** ( in cmd.exe “net user administrator ‘type new password here”’)
* Check for additional admin accounts/Disable Guest (same location as above) **OR** (Server manager->Tools > computer management > local users and groups > users)
* Check for updates Control Panel->Windows Updates ( in cmd.exe “wuapp.exe”)
* Disable RDP (start > right click ‘my computer’ > properties > remote settings > disable) **AND** ( ‘select users’ -> remove all)
* Download and install antivirus (“Microsoft security essentials”)
* Security Configuration Wizard If not installed(in cmd.exe type “mmc” and hit enter -> click ‘console’ -> add snap-in -> add security configuration and security templates if needed) **THEN** (start -> administrative tools -> SCW)
* Remove unnecessary roles/services (\*\*Know your server\*\*You don’t need IIS on an AD/DNS\*\* Run configuration wizard under start)
* Disable IPv6 (control panel -> network and internet -> change adapter settings -> right click ‘properties’ on active NIC -> uncheck ipv6 )
* Microsoft Security Baseline Analyzer (download and run -> will show missing issues)
* Windows Firewall Configuration control panel -> windows firewall (\*\*SCW should enable it but double check\*\*Make sure unnecessary exceptions\*\*)

Click *Allow apps to communicate through Firewall* (top option on left pane)

Base Line security analyzer walks through firewall settings.

Disable NTLMv1 (GPO ‘NoLMHash’)

* Configure BitLocker(in cmd.exe ‘-install BitLocker –restart’ )
* Disable Shares (\*\*if any, in cmd.exe ‘net share’ )

**Windows server 2008/Windows7**

* Change Local admin password (start -> right click on ‘computer’ -> ‘manage’ -> ‘Local Users and Groups’ -> ‘users’ -> right click on ‘administrator’ -> ‘change password’) **OR** ( in cmd.exe “net user administrator ‘type new password here”’)
* Check for additional admin accounts/Disable Guest (same location as above) **OR** (start > admin tools > computer management > local users and groups > users)
* Check for updates (start -> control panel -> windows updates) **OR** ( in cmd.exe “wuapp.exe”)
* Disable RDP (start > right click ‘my computer’ > properties > remote settings > disable) **AND** ( ‘select users’ -> remove all)
* Download and install antivirus (“Microsoft security essentials”)
* Security Configuration Wizard If not installed(in cmd.exe type “mmc” and hit enter -> click ‘console’ -> add snap-in -> add security configuration and security templates if needed) **THEN** (start -> administrative tools -> SCW)
* Remove unnecessary roles/services (\*\*Know your server\*\*You don’t need IIS on an AD/DNS\*\* Run configuration wizard under start)
* Disable IPv6 (start -> control panel -> network and internet -> change adapter settings -> right click ‘properties’ on active NIC -> uncheck ipv6 )
* Microsoft Security Baseline Analyzer (download and run -> will show missing issues)
* Windows Firewall Configure Start -> control panel -> windows firewall (\*\*SCW should enable it but double check\*\*Make sure unnecessary exceptions\*\*)

Click *Allow apps to communicate through Firewall* (top option on left pane)

Base Line security analyzer walks through firewall settings.

* Disable NTLMv1 (GPO ‘NoLMHash’)
* Configure BitLocker(in cmd.exe ‘-install BitLocker –restart’ )
* Disable Shares (\*\*if any, in cmd.exe ‘net share’ )

**Windows Server 2003**

* Change Local admin password (start -> right click on ‘computer’ -> ‘manage’ -> ‘Local Users and Groups’ -> ‘users’ -> right click on ‘administrator’ -> ‘change password’) **OR** ( in cmd.exe “net user administrator ‘type new password here”’)
* Check for additional admin accounts/Disable Guest (start > admin tools > computer management > local users and groups > users)
* Check for updates (start -> control panel -> windows updates) **OR** ( in cmd.exe “wuapp.exe”)
* Check Time/Date
* Disable RDP (start > right click ‘my computer’ > properties > remote tab > select users)
* Antivirus (“Microsoft security essentials”)
* Configure Shadow Copies (Start > Manager your server > file server > shares > Shadow)
* Remove unnecessary roles/services (\*\*Know your server\*\*You don’t need IIS on an AD/DNS\*\* Run configuration wizard under start)
* Check disk quota
* Microsoft Security Baseline Analyzer (download and run -> will show missing issues)
* Security Config Wizard (if not installed start > Control panel > add remove programs > add windows components)
* Disable IPv6 (start -> control panel -> network and internet -> change adapter settings -> right click ‘properties’ on active NIC -> uncheck ipv6 )
* Windows Firewall Configure Start -> control panel -> windows firewall (\*\*SCW should enable it but double check\*\*Make sure unnecessary exceptions\*\*)

Click *Allow apps to communicate through Firewall* (top option on left pane)

Base Line security analyzer walks through firewall settings.

Disable LanMan (Start -> Settings -> Control Panel -> Administrative Tools -> Local Security Polic-> Expand the “Local Policies” folder and select “Security Options” beneath it. Double click “Network security: LAN Manager authentication level”.Change the setting to “Send NTLMv2 response only\refuse LM & NTLM”.)

**Windows Tools:**

Process hacker

Tcp viewer

Security essentials

Security Baseline analyzer

Belarc Advisor

Autoruns

Event triggers (**eventtriggers**[**.exe**] **/create** [**/s** Computer [**/u** Domain\User [**/p** Password]]] **/tr** TriggerName [**/l** [**APPLICATION**] [**SYSTEM**] [**SECURITY**] ["**DNS Server**"] [**LOG**] [DirectoryLogName] [**\***] ] {[**/eid** ID]|[**/t** {**ERROR**|**INFORMATION**|**WARNING**|**SUCCESSAUDIT**|**FAILUREAUDIT**}]|[**/so** Source]} [**/d** Description] **/tk** TaskName [**/ru** {[Domain\]User | **"System"**} [**/rp** Password]])