

**Age of the Ge3k**

**Windows Nationals Guide**



Prerequisites:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | 1 | Read Readme and Q&A file   * Be sure to take note of questions in Q&A file * FIX any highlighted problems ASAP |
|  |  |  | 3 | Back up Critical files   * Place in C:\Windows\System 32\BU |
|  |  |  | 4 | Configure Firewall   1. Control Panel → Windows Firewall → Restore Default 2. Control Panel → Administrator Tools → Windows Firewall W/ Advanced Security 3. Make sure all firewalls are turned on 4. Configure rules to only allow required and system services through |
|  |  |  |  | Search for C99’s and such   1. Findstr /r /s /m “**string**” \*.php   Replace **string** with each of the following:  Passthru, shell\_exec, system, phpinfo, base64\_decode, edoced\_46esab, chmod, mkdir, fopen, fclose, readfile |
|  |  |  |  | Change passwords for all users |
|  |  |  | 5 | Programs and Features   1. Uninstall unnecessary programs 2. Update programs that are installed that are necessary. 3. For Windows 10, check “Start Tiles” and configure appropriately.   **Note:** For Windows services, go into programs and features and delete the Windows feature associated with it. |
|  |  |  | 6 | Analyze Running Tasks   1. Run: netstat -ano 2. Shutdown services based on results. 3. Run task manager and compare PID’s if needed. 4. Kill the appropriate tasks/processes   Note: Process Explorer can help with this step  Note: Keep analyzing for Red team connections |
|  |  |  | 7 | View Hidden Files   * Control panel → folder options → view → show hidden |
|  |  |  | 8 | Complete the Forensics questions and take care of found items as needed. |

Checklist:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | 1 | Create user script to delete, disable, and change user’s passwords.  **Replace bolded text with actual user names!**   1. wmic useraccount set disabled=false 2. net user **BadUser** /delete 3. net user **GoodUser** C00l-be@ns2016! 4. wmic useraccount set PasswordExpires=true 5. wmic useraccount set PasswordChangeable=true |
|  |  |  | 2 | Manage users and groups   1. Check to make sure users passwords **expire** and that they are **not locked out** 2. Check Administrator Group to make sure that only administrators are in it. 3. Check to make sure all REQUIRED users are in groups 4. DELETE home directories for removed users.   **NOTE:** net user **UserName** gives useful info on specific users |
|  |  |  | 3 | Service Pack   * Get from Patch server * Continue on checklist while waiting |
|  |  |  | 4 | Enable Automatic Updates  **NOTE:** Make sure Service Pack is complete!   1. Turn Automatic Updates on 2. Check Get updates for Windows and other Microsoft products. |
|  |  |  | 5 | Windows Update  **NOTE:** Make sure Service Pack is complete!   1. Make sure Automatic Updates is turned on 2. Check Get updates for Windows and other Microsoft products 3. Make sure most recent service pack is installed 4. Make sure you install updates BEFORE reboot 5. Repeat 3 times ⬜ 1st time ⬜ 2nd time ⬜ 3rd time |
|  |  |  | 6 | Analyze Services   1. Open Control Panel→ Administrator Tools→ Services 2. Compare with clean service List |
|  |  |  | 7 | Install Malwarebytes |
|  |  |  | 8 | Scan with Malwarebytes |
|  |  |  | 9 | **Configure README requirements:**   1. Example: If the readme requires the system to run a web server, make sure to set up the server and test it to make sure it is working properly. |
|  |  |  | 10 | Scheduled Tasks   1. Analyze each task    1. Disable rogue tasks    2. Delete actual file using path found in ACTIONS tab    3. Delete Task |
|  |  |  | 11 | Startup Programs   1. Start → programs → accessories → system tools → system information → software environment → startup 2. “Windows Key” + R, type: msconfig    1. Sysinternals Auto run 3. Analyze startup programs 4. Delete rogue entries from the registry and file system |
|  |  |  | 12 | Check *C:\Program Files* and *C:\Program Files (x86)* for Rogue Programs   1. Look for programs that do not show up in Programs and Features 2. ANY program not listed in Readme or necessary for Windows must be removed. |
|  |  |  | 13 | Load STIGS   1. “Windows Key”+R, type: mmc 2. File → add snapin → security config and analysis → open database → “hi” → select inf file from where you put it. 3. Analyze and Configure computer 4. **MANUAL STEP:** Go into Local Security Policies and change these values manually:    1. Minimum Password Age = 10    2. Maximum Password Age = 30    3. Account Lockout Duration = 30    4. Audit: Force audit policy subcategory settings… = Disabled\Not Defined    5. All Audit Policies = Success, Failure    6. Audit: Audit the use of Backup and Restore privilege = Enabled    7. Devices: Allow undock without having to log on - Disable    8. Devices: Restrict CD-ROM access to locally logged-on user only -Enable    9. Interactive logon: Number of previous logons… - 0    10. Interactive logon: Require Domain Controller auth… - Enabled    11. Network access: Remotely accessible registry paths - null (no value)    12. Network access: Remotely accessible registry paths and sub-paths - null    13. Shutdown: Clear virtual memory pagefile - Enabled    14. System Cryptography: Force strong key protection… - User must enter a password each time they use a key    15. System settings: Use Certificate Rules on Windows Exe… - Enabled |
|  |  |  | 14 | Disable Shares   1. In GUI:    1. Control Panel → Administrator Tools → Computer Management    2. Open the “Shares” tab    3. Right click and delete unnecessary shares       1. IPC$ is necessary and cannot be deleted 2. For C$ and ADMIN$    1. “Windows Key”+R, type: *regedit*       1. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\:LanmanServer\Parameters       2. Insert dword(32 bit) ||| Name it AutoShareWks and leave value 0 |
|  |  |  | 15 | Host Files   1. Open notepad as administrator and open C:\Windows\system32\drivers\etc 2. Analyze host file, look for rogue entries 3. Remove entries that are no local host or commented out. |
|  |  |  | 16 | Analyze DNS   1. Network and Sharing Center → Adapter Settings 2. Disable unneeded adapters if any 3. Go to properties of adapters being used.    1. Uncheck any protocols not being used or needed (IPv6, File and Printer)    2. Double click IPv4    3. Check to make sure no rogue entries are in any of the tabs. |
|  |  |  | 17 | Disable AutoPlay   1. Control Panel → AutoPlay 2. Click “Reset all defaults” THEN uncheck “Use AutoPlay for all media devices” |
|  |  |  | 18 | Run “Everything”   1. Look for rogue files, especially in the “Users” directory |
|  |  |  | 19 | Make sure that the system has a screensaver that locks the computer   * Right click on Desktop → personalize → screen saver |
|  |  |  | 20 | User Account Control   1. Action Center → Change User Account Control settings 2. Set to highest security. |
|  |  |  | 21 | Internet Explorer   1. Go to Control panel → Internet Explorer Options 2. Make sure all settings are at highest security. |
|  |  |  | 22 | Go back over Readme and Q&A file   1. Go back over readme file and configure system appropriately and make sure that all questions are answered. |
|  |  |  | 23 | Run Microsoft Baseline Security Analyzer   1. Download online or get from hard drive |
|  |  |  | 24 | Recheck System   1. **NOTE:** Check over users manually in Computer Management for password expiration. |
|  |  |  | 25 | SERVERS ONLY:   1. Go to Server Manager    1. Find IE ESC.    2. Set on for Admin and Users 2. Search for Rogue Scripts using the Explorer search bar    1. passthru, Obfuscation, base64\_decode, angel, C99, R57, C100, |
|  |  |  | 26 | **WINDOWS 10**   1. Go into System Settings and then Privacy. 2. Turn off all the options. 3. Go into System 4. Check settings for proper configuration. |
|  |  |  | 27 | Write down points. (You should be doing this as you get them, but if not, make sure they are all written down before rotating. |

Contact [tcoffey@cscs.cowg.cap.gov](mailto:tcoffey@cscs.cowg.cap.gov) and [nbowe@cscs.cowg.cap.gov](mailto:nbowe@cscs.cowg.cap.gov) to report errors.