

**Age of the Ge3k**

**Linux Checklist CSCS Wolfpack**



Prerequisits:

|  |  |  | 1 | Read README |
| --- | --- | --- | --- | --- |
|  |  |  | 2 | Answer Forensics Questions |
|  |  |  | 3 | Write down current user password from README |
|  |  |  | 4 | Promote yourself to Root   * sudo su - |
|  |  |  | 5 | Install All Programs   * apt-get install clamtk * apt-get install libpam-cracklib * apt-get install auditd * apt-get install rkhunter |
|  |  |  | 6 | If needed, Open Vi Reference Guide  http://www.astrohandbook.com/ch20/vi\_guide.html |

Checklist:

|  |  |  | 1 | Examine passwd file   * vi /etc/passwd  1. Ensure that only root has UID of 0 2. Remove unnecessary users |
| --- | --- | --- | --- | --- |
|  |  |  | 2 | Examine shadow file   * vi /etc/shadow  1. Make sure all users have a “!”, “\*” or an encrypted password (All valid users should not have a “!” or “\*”) 2. Ensure that root (top line) has a “\*” instead of an encrypted password remove unnecessary users from the file |
|  |  |  | 3 | Examine group file   * vi /etc/group |
|  |  |  | 4 | 1. Make sure only administrators are in the sudo group 2. Delete all bad user groups 3. Change Passwords for all Valid Users (Not including current account depending on README. Replace **Username** with name of user.)  * passwd **Username** * chage -m 1 -M 30 -W 5 -I 7 **Username** * useradd -D -f 7 (Only type once) |
|  |  |  | 5 | Remove Guest Account   * vi /etc/lightdm/lightdm.conf   At the end of the file add:   * allow-guest=false   Insert the seat directives:   * 12.04-14.04: [SeatDefaults] * 16.04: [Seat:\*]   If that file does not work go to these files and enter the same thing as above:   * /usr/share/lightdm/lightdm.conf.d/\*.conf * /etc/lightdm/lightdm.conf.d/\*.conf * /etc/lightdm/lightdm.conf |
|  |  |  | 6 | Updates   1. Go to the gear icon in the top right corner of the screen and click on System Settings -> Updates 2. Ensure that all software repositories are checked 3. Ensure that updates are set to Download and Install automatically 4. Click all of the update checkboxes to ensure that all updates are installed 5. Open up a new terminal, promote yourself to root and type the following commands: apt-get update then apt-get upgrade 6. Go back to your original terminal and continue working   NOTE: If you get a black screen on reboot, or at any time, you can get a terminal by pressing Control-Shift-F2. You can get back to a GUI by pressing Control-Shift-F7 |
|  |  |  | 7 | Update Login Parameters   * touch /etc/security/opasswd * chown root:root /etc/security/opasswd   vi /etc/login.defs   * Look for PASS\_MIN\_DAYS and set to 7 * Look for PASS\_MAX\_DAYS and set to 30   Add the following lines:   * PASS\_MIN\_LEN\_14 * ENCRYPT\_METHOD SHA512 * LOGIN\_RETRIES   vi /etc/pam.d/common-password   * Look for the text pam\_cracklib and change minlen=14 and add at the end of that line: ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 * Look for the text pam\_unix.so and add remember=12   vi /etc/pam.d/common-auth   * Add this line to the bottom of the file (This is one line): auth required pam\_tally2.so deny=5 onerr=fail unlock\_time=1800 |
|  |  |  | 8 | Set audit policy   * auditctl -e 1 |
|  |  |  | 9 | Configure Firewall   * ufw disable   Change the port number to whatever service is required to be let in through the firewall   * ufw allow in to any port **port number** from any * ufw default deny incoming * ufw default allow outgoing * ufw logging medium * ufw enable   vi /etc/default/ufw   * Find IPv6 and change it from yes to no |
|  |  |  | 10 | Examine Sudoer Files (Look for NO PASSWD or !Authenticate)   * vi /etc/sudoers * cd /etc/sudoers.d   Examine all files in the sudoers.d directory |
|  |  |  | 11 | Cleanup Unnecessary Network Services   * netstat -tunlp   For all programs that are listening that are unneeded:   * apt-get purge “program name”   If you cannot find the name of a program that is listening use these commands to find them:   * which “name of program in netstat” * dpkg –search “Output of which command”   If you still could not find the name of the program, there is probably a rogue script running.  Run pstree -p and find the program with the process id of the program running in the netstat  If it is being started by cron, go to step 12  If it is being started by something else, examine it further. It may be started by init.d which is in the rc files. Go to step 13 for Rc Files |
|  |  |  | 12 | Cron  Look through all cron files  cd /var/spool/cron (Look through all files in directory)  cd /etc/cron.d (Look through all files in directory)  vi /etc/crontab  vi /etc/anacrontab  cd /etc/cron.monthly (There are many cron.\* directories. Look through all of them) |
|  |  |  | 13 | RC Files  Look through all rc directories from rc0.d to rc5.d and look at rc.local.   * cd /etc/init.d * ls -ltr   Check the timestamp. If there is a weird timestamp (out of place) then investigate the file further. |
|  |  |  | 14 | Cleanup SSH   * vi /etc/ssh/sshd\_config   Look for line that contains allow root login. Change it from yes to no. |
|  |  |  | 15 | Set Permissions on Files   * cd /etc * chmod 644 group * chmod 644 passwd * chmod 600 shadow * cd /dev * chmod a-x null * chmod a-x tty\* * chmod a-x console |
|  |  |  | 16 | Update Kernel Parameters   * vi /etc/sysctl.conf   Insert these lines at the bottom of the file   * net.ipv4.tcp\_max\_orphans = 256 * net.ipv4.conf.all.log\_martians = 1 * net.ipv4.ip\_forward = 0 * net.ipv4.conf.all.send\_redirects = 0 * net.ipv4.conf.default.send\_redirects = 0 * net.ipv4.tcp\_max\_syn\_backlog = 4096 * net.ipv4.tcp\_syncookies=1 * net.ipv4.conf.all.rp\_filter = 1 * net.ipv4.conf.all.accept\_source\_route = 0 * net.ipv4.conf.all.accept\_redirects = 0 * net.ipv4.conf.all.secure\_redirects = 0 * net.ipv4.conf.default.rp\_filter = 1 * net.ipv4.conf.default.accept\_source\_route = 0 * net.ipv4.conf.default.accept\_redirects = 0 * net.ipv4.conf.default.secure\_redirects = 0 * net.ipv4.icmp\_echo\_ignore\_broadcasts = 1   Save and quit the file and then type in the following commands:   * chown root:root /etc/sysctl.conf * chmod 600 /etc/sysctl.conf * /sbin/sysctl -p |
|  |  |  | 17 | Run ClamAV   * freshclam (This updates definitions, It will take awhile, open up another command prompt and keep working) * clamscan -r --bell -i / |
|  |  |  | 18 | Check Start-up Programs   * cd /etc/xdg/autostart * sed -in-place `s/NoDisplay=true/NoDisplay=false/g` \*.desktop   Search for the program “Startup Applications” and look through all startup programs. |
|  |  |  | 19 | Find Rogue Scripts on a Webserver (Only do this if you have a webserver)   * find . -type f -print | xargs grep -irl c99   Repeat the command above but everytime replace **c99** with passthru, Obfuscation, base64\_decode, angel.  Investigate all .php files found by those searches. |
|  |  |  | 20 | Remove SSH Keys   * vi /etc/ssh/sshd\_config   Look for the term AuthorizedKeysFile and find the file name. If this element does not exist or is commented out, then the file name.   * is authorized\_keys * cd / * find . -name “name of file above”   If there were files located, delete them.   * cd /etc/ssh * rm ssh\_host.\* * dpkg --reconfigure openssh-server |
|  |  |  | 21 | Examine /etc/xinetd.d  If the directory does not exist, move on   * cd /etc/xinetd.d   Disable all services that are not specified by the readme by adding disable=yes to each file. |
|  |  |  | 22 | Examine /etc/inetd.conf  If the file does not exist, move on   * vi /etc/inetd.conf * Comment out all lines that are not needed * If changes are made to the file the service needs to be restarted by typing: * ps -edaf | grep inetd * kill -HUP “process id from the above command” |
|  |  |  | 23 | Analyze DNS   * vi /etc/resolv.conf   Ensure that it is listening on localhost |
|  |  |  | 24 | Analyze Host file   * vi /etc/hosts   Compare it to a clean image |
|  |  |  | 25 | Check the Ubuntu Software center for rogue programs  Use the installed tab and use keywords such as “crack”, “hack”, “keylog”, “backdoor”, “netcat”, “sniff”, “trace”, “track”, “exploit”, “rootkit”, “rainbow”, “mine”, “trojan”, “nmap”, “map”  Also make sure to check the history tab at the top. |
|  |  |  | 26 | Look for SETUID programs   * find . \( -perm -04000 -o -perm -02000 \) -type f -print   Compare this list to a clean image list. |
|  |  |  | 27 | Look for world writable files   * find . -type f \(-perm -0002 -a ! -perm -1000 \) -print | egrep -v ‘^..proc’   Compare this to a clean image. If there are any out of place world writable files run : chmod o-x “filename” |
|  |  |  | 28 | NOSETUID on Floppy and/or CDROM Partitions   * vi /etc/fstab   Add to the end on the column that starts with rw or read only: ,nodev, nosuid |
|  |  |  | 29 | Run rkhunter   * rkhunter --update * rkhunter --check * vi /var/log/rkhunter   Look for things that were in red during the check. |
|  |  |  | 30 | Check Log Files for Hints of Compromise   * cd /var/log   Look through logs such as access logs |
|  |  |  | 31 | Write down points. (You should be doing this as you get them, but if not, make sure they are all written down before rotating. |
|  |  |  | 32 | **ROTATE!** Let fresh eyes on the system.   1. **If you are on a promising trail, complete just the one (1) and then rotate. Do not get Tunnel Vision!** |

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.