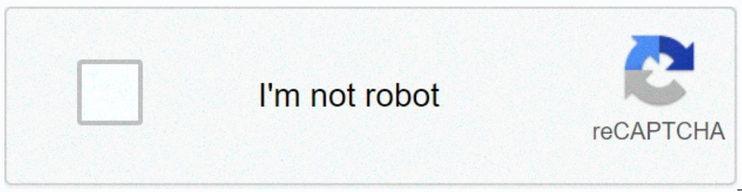

Continue

Ubuntu checklist cyberpatriot

Ubuntu Checklist (CyberPatriot) Input team ID Read that Read me a. Read readme VERY carefully – could give you a clue, ex. if readme says no media files are allowed it would be wise to search for media files. 3. Install Gnome, a more familiar interface a. sudo apt-get install gnome-session-fallback 4. Application Update > System Tools > Administration > Update Manager allows automatic security updates i.e. Update Manager -> Firewall Settings In Ubuntu all ports are blocked by default Default Firewall - ufw (off by default sudo ufw status sudo ufw enables / disables Firestarter for graphical interface (recommended) sudo apt-get install User Account User Preferences & Group Do not use root users (disabled by default) sudo passwd sudo passwd -l root Use sudo instead of root (/etc/sudoers) sudo visudo OR sudo gedit /etc/sudoers james ALL=(ALL) ALL sudo adduser user_name sudo Add users i. username sudo adduser e. Deleting a user is the username sudo deluser f. Remove world-readable permissions for home directory i.e. sudo chmod 0750 /home/username Locking/Unlocking user sudo passwd -l username sudo passwd -u username Passwords i. Expired sudo chage username sudo chage –l username 7. Antivirus a. ClamTK (under Accessories) 8. Uninstall Applications Applications → Ubuntu Software Center Installed Software section Select applications and click Remove 9. A process. To view the process ps aux or top system monitor b. Know 10. Log Some /var/log/boot : System boot log /var/log/debug : Debugging log messages /var/log/auth.log : User login and authentication log /var/log/daemon.log : Running services such as squid, ntpd and other log messages to this file /var/log/kern.log : Kernel log files View tail logs, more, cats, less, grep GNOME System Log Viewer If the command errors or fails, try again with sudo (or sudo !! to save typing) any Google and everything. If you don't know or understand something, google it When you see the $word syntax, don't type it verbatim, but replace the appropriate word (usually referenced in the previous command). When the sequence of steps does not matter, point points have been used instead of ordinal. To edit a file, run gedit, a graphics editor similar to notepad; nano, simple command line editor; or vim, a powerful but less intuitive command-line editor. Note that vim may need to be installed with apt-get install vim. Checklist Read readme notes under which ports/users are allowed. Do Forensic Questions You can destroy the necessary information if you are working on a checklist! Secure root set PermitRootLogin no in /etc/ssh/sshd_config User Disable guest users. Open /etc/lightdm/lightdm.conf and add the allow-guest=false line Then restart your session with lightdm sudo restart. This will get you out, so make sure you don't execute anything important. Open Open and check which users uid 0 Can login Allowed in readme Delete unauthorized users: sudo userdel -r $user sudo groupdel $user Check /etc/sudoers.d and make sure only sudo group members can sudo. Check /etc/group and remove non-admins from the sudo and admin groups. Check the user directory. cd / home sudo ls -Ra * Look at any directory that appears for media files / tools and / or hacking tools. Apply password requirements. Add or change password expiration requirements to /etc/login.defs. PASS_MIN_DAYS 7 PASS_MAX_DAYS 90 PASS_WARN_AGE 14 Add minimum password length, password history, and add complexity requirements. Open /etc/pam.d/common-password with sudo. Add minlen=8 to the end of the line that has pam_unix.so in it. Add remember=5 to the end of the line that has pam_unix.so in it. Find the line you pam.cracklib.so inside. If you can't find that line, install cracklib with sudo apt-get install libpam-cracklib. Add ucredit=-1 lcredit=-1 dcredit=-1 ocredit=- to the end of the line. Apply an account locking policy. Go to /etc/pam.d/common-auth. Add deny=5 unlock_time=1800 to the end of the line with pam_tally2.so in it. Change all passwords to meet these requirements. chpasswd is very useful for this purpose. Turn on automatic updates In gui set Update Manager->Settings->Updates->Check for updates:->Daily. Secure port sudo ss -ln If the port has 127.0.0.1:$port in its line, it means it is connected to loopback and not exposed. Otherwise, there should only be a port specified in the open readme (but there will probably be tons more). For each open port that must be closed: sudo lsof -i :$port Copy the listening program in the port. where to $program Copy where the program is located (if there is more than one location, simply copy the first one). dpkg -S $location This indicates which package provides the file (If there is no package, it means you may be able to delete it with rm $location; killall -9 $program). sudo apt-get cleans the $package Check to make sure you don't accidentally remove an important package before pressing y. sudo ss -l to make sure the port is completely closed. Secure network Enable firewall sudo ufw enable Enable cookie protection syn sysctl -n net.ipv4.tcp_syncookies Disable IPv6 (Potentially harmful) echo net.ipv6.conf.all.disable_ipv6 = 1 | sudo tee -a /etc/sysctl.conf Disable IP Forwarding echo 0 | sudo tee /proc/sys/net/ipv4/ip_forward Prevent IP Spoofing echo nospoof on | sudo tee -a /etc/host.conf Install this Update Start before halfway. Perform general updates. sudo apt-get update. sudo apt-get upgrade. Update the services specified in readme. Google to find out what is the latest stable version. Google install the service version. Follow the instructions. Make sure you have points for updating the kernel, each service specified in readme, and bash if it is vulnerable to Configure the Service configuration file check service file for the required services. Usually the wrong settings in the configuration file for sql, apache, etc. will be the point. Make sure all services are valid. --status-all service Check installed packages for hacking tools, such as password crackers. Run another (more comprehensive) checklist. This is a checklist designed to get most of the general points, but may not catch it all. Netcat tips installed by default in ubuntu. Most likely you won't get points for deleting this version. Some services (such as ssh) may be required even if they are not mentioned in readme. The other might point even if they were explicitly mentioned in the confessional readings of Michael MB Bailey and Christopher CJ Gardner without a checklist that this would never have been possible. Alexander Dittman and Alistair Norton for being friends. My 2015-16 CP team: Quiana Dang, Sieun Lee, Jasper Woolley and David Randazzo. In a certain order: Marcus Phoon, Joshua Hufnagel, Patrick Hufnagel, Michael-Andrew Keays, Christopher May, Garrett Brothers, Joseph Kelley, and Julian Vallyeason. And the CyberPatriot program. This checklist is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License. Page 2 You cannot perform these actions at this time. You sign in with another tab or window. Reload to refresh your session. you exit in another tab or window. Reload to refresh your session. We use optional third-party analytics cookies to understand how you use GitHub.com that can build better products. Learn more. We use optional third-party analytics cookies to understand how you use GitHub.com that can build better products. You can always update your options by clicking Cookie Preferences at the bottom of the page. For more information, see our Privacy Statement. We use important cookies to perform important website functions, for example they are used to log in. Learn more Always on We use analytics cookies to understand how you use our website so we can make them better, for example they are used to collect information about the pages you visit and how many clicks you need to complete tasks. Learn more I am trying to find a common Ubuntu checklist for the team I am practicing with to get to know ubuntu better. Anything will help Ubuntu Checklist (CyberPatriot) Input team ID Read me a. Read readme VERY carefully – could give you a clue, ex. if readme says no media files are allowed it would be wise to media files. 3. Install Gnome, a more familiar interface a. sudo apt-get install gnome-session-fallback 4. Application Update > System Tools > Administration > Update Manager enables automatic security updates i.e. Update Manager -> Firewall Settings In Ubuntu all ports are blocked by default firewall - ufw (off by default sudo ufw status status ufw enables / disables Firestarter for graphical interface (recommended) sudo apt-get install Firestarter User Account Preferences & Group Do not use root users (disabled by default) sudo passwd sudo passwd -l root Use sudo instead of root (/etc/sudoers) sudo visudo OR sudo gedit /etc/sudoers james ALL=(ALL) ALL sudo adduser user_name sudo Add users i.e. sudo adduser username e. Deleting a user is the username sudo deluser f. Remove world-readable permissions to home directory sudo chmod 0750 /home/username Locking/Unlocking user sudo passwd -l username sudo passwd -u username Passwords i. Expired sudo chage username sudo chage –l username 7. Antivirus a. ClamTK (under Accessories) 8. Uninstall Applications Applications → Ubuntu Software Center Installed Software section Select applications and click Remove 9. A process. To view the process ps aux or top system monitor b. Know 10. Log Some /var/log/boot : System boot log /var/log/debug : Debugging log messages /var/log/auth.log : User login and authentication log /var/log/daemon.log : Running services such as squid, ntpd and other log messages to this file /var/log/kern.log : Kernel log file View log tail, more, cat, less, Grep GNOME System Log Viewer Viewer