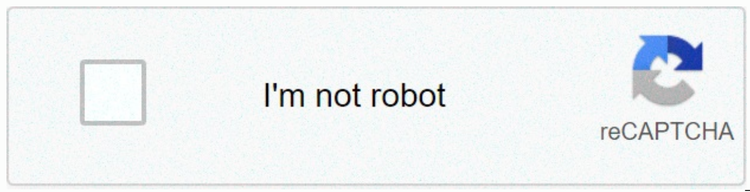

Continue

Cq wpx contest

Before you can use any of these images, you must install vmware on your computer. If you are confused or want to learn more about the software we use in CyberPatriot, here is a guide that contains the manuals of any critical service that you will ever need to configure. Hard Ubuntu Image Custom Ubuntu Image (Homemade) Full Windows Checklist [COMING SOON] Custom Windows Image Cisco Packet Tracer Resources To practice doing Cisco, you need to sign into your CyberPatriot Netacad account here. Once you have access to your account, you can open the class dedicated to Cisco and install Cisco Packet Tracer, which is located under student resources on the class home page. Note that you can only access the CyberPatriot version of the class if you are outside of a CyberPatriot computer. There is, however, a free class that is open to the public. Packet Tracer Navigation Tutorial Competition Checklists Linux Checklist [COMING SOON] Windows Checklist [COMING SOON] Cisco Checklist [COMING SOON] Cisco CLI Command Cheat Sheet Other Resources CyberPatriot Official Web Training Modules r/CyberPatriot Competition Sound Board Ubuntu Checklist (CyberPatriot) Input Equipment ID Read A. Read the file VERY carefully- you could give it advice, for example, if the file says no media files are allowed it would be prudent to search for media files. 3. Install Gnome, a more familiar interface a. sudo apt-get install gnome-session-fallback 4. Updates Applications > System Tools > Administration > Update Manager enable automatic security updates i. Update Manager -> Firewall Settings On Ubuntu all ports are blocked by the default firewall – ufw (disabled by default sudo ufw status sudo ufw enable/disable Firestarter for graphical interface (recommended) sudo apt-get User Preferences Users & Groups Do not use root user (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 Adding users i. sudo adduser username e. Deleting users i. sudo deluser username f. Deleting readable permissions from the world to the home directory i. sudo chmod 0750 /home/username Locking/Unlocking user sudo passwd -l username sudo passwd -u username Passwords i. Expiration sudo chage username sudo chage –l username 7. Antivirus a. ClamTK (under Accessories) 8. Uninstall Applications → Ubuntu Software Center installed software section Select Application and click Remove 9. Processes a. To view the processes ps aux or top System Monitor b. Know Logs Some /var/log/boot : System boot log /var/log/debug : Debugging log messages /var/log/auth.log : Login logs and user authentication /var/log/daemon.log : Running services such as squid, ntpd and other log messages in this file : Kernel log file View queue logs, plus, cat, minus, grep GNOME System Log Viewer If a command fails or fails, try again with sudo (or sudo !! to save write) Google anything and everything. If you don't know or understand something, google when you see the $word syntax, don't type it verbatim, but replace the appropriate word (usually referenced in a previous command). When the order of the steps does not matter, bullets have been used instead of ordinal. To edit files, run gedit, a graphical editor similar to notepad; nano, a 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 the Readme Note file on which ports/users are allowed. Asking forensic questions Can destroy the necessary information if you work on the checklist! Secure root set PermitRootLogin not in /etc/ssh/sshd_config Secure Users Disable the guest user. Go to /etc/lightdm/lightdm.conf and add the allow-guest-false line then restart the session with sudo restart lightdm. This will log you out, so make sure you're not running anything important. Open /etc/passwd and check which users are uid 0 You are allowed to log in to the Readme Delete unauthorized users: sudo userdel -r $user sudo groupdel $user Check /etc/sudoers.d and make sure that only members of the sudo group can sudo. Check /etc/group and delete the non-administrators groups from sudo and admin groups. Check the user directories. cd /home sudo ls -Ra * Search any directory that appears for media files/tools and/or hacking tools. Apply password requirements. Add or change password expiration requirements to /etc/login.defs. PASS_MIN_DAYS 7 PASS_MAX_DAYS 90 PASS_WARN_AGE 14 Add a minimum password length, password history, and add complexity requirements. Open /etc/pam.d/common-password with sudo. Add minlen-8 to the end of the line you pam_unix.so on it. Add remember-5 to the end of the line that has pam_unix.so on it. Locate the line you have pam.cracklib.so on it. If you cannot find that line, install cracklib with sudo apt-get install libpam-cracklib. Add ucredit-1 lcredit-1 dcredit-1 ocredit-- at the end of that line. Implement an account lockout policy. Open /etc/pam.d/common-auth. Add deny-5 unlock_time-1800 to the end of the line with pam_tally2.so on it. Change all passwords to meet these requirements. chpasswd is very useful for this purpose. Enable automatic updates In the Update Manager->Settings->Updates->Check GUI set for Secure ports sudo ss -ln If a port has 127.0.0.1:$port on its line, that means it is connected to the loopback and is not exposed. Otherwise, there should only be ports that are specified in the open Readme file (but there will probably be tons more). For each open port to be closed: sudo lsof -i :$port Copy the program you are listening to on the port. Port. $program Copy where the program is (if there is more than one location, simply copy the first one). dpkg -S $location Shows which package the file provides (If there is no package, that means you can probably delete it with rm $location; killall -9 $program). sudo apt-get purge $package Check to make sure you are not accidentally deleting critical packets before hitting and. sudo ss -l to make sure the port is really closed. Secure Network Enable the sudo ufw enable Enable syn cookie protection sysctl -n net.ipv4.tcp_syncookies Disable IPv6 (Potentially Harmful) firewall 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 Avoid IP impersonation echo nospoof on sudo tee -a /etc/host.conf Install updates Start this before half. Perform general updates. sudo apt-get update. sudo apt-get upgrade. Update the services specified in The Readme file. Google to find out what the latest stable version is. Google version of ubuntu installation service. Follow the instructions. Make sure that you have points to update the kernel, each service specified in the Readme and bash file if you are vulnerable to shellshock. Configure Services Check the service configuration files for the required services. Usually, an incorrect configuration in a configuration file for sql, apache, etc. will be a period. Ensure that all services are legitimate. service --status-all Check installed packages for hacking tools, such as password crackers. Run other (more complete) checklists. This is a checklist designed to get most common points, but it may not detect everything. Netcat Tips is installed by default on ubuntu. Chances are you won't get points to delete this version. Some services (such as ssh) may be required even if they are not mentioned in the Readme file. Others may be points even if explicitly mentioned in the Readme Acknowledgements Michael MB Bailey and Christopher CJ Gardner without whose checklists this would never have been possible. Alexander Dittman and Alistair Norton for being Linux companions. My 2015-16 CP team: Quiana Dang, Sieun Lee, Jasper Woolley and David Randazzo. In no particular 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 an international Creative Commons Attribution-ShareAlike 4.0 license. Page 2 You cannot perform that action at this time. You are logged in with another tab or window. Reload to session. You are logged out of another tab or window. Reload to refresh the session. We use optional third-party analytics cookies to understand how you use GitHub.com so that we can create better products. Learn more. We use optional third-party analytics cookies to understand how you use GitHub.com so we can create better You can always update your selection by clicking Cookie Preferences at the bottom of the page. For more information, please see our Privacy Statement. We use essential cookies to perform essential functions of the website, for example, they are used to log in. More information Always On We use analytics cookies to understand how you use our websites so that we can improve them, for example, they are used to collect information about the pages you visit and how many clicks you need to perform a task. Learn more github.com/Forty-...Page 2github.com/Forty-... All entries in the WPX Competition for CW/SSB since 1973 have been entered into a searchable database. Search the online database for any station or operator call signals: Online certificates are available for 2010 and later. Use search to find your call in the database. Then click the [Cert] link to view the certificate in pdf format. Loading web logs The Log Check page allows you to upload your log and check its format. Once all the bugs have been fixed, you can have it send your record directly to the robot. ADIF Log File Converter The ADIF page allows you to upload your ADIF format log file and convert it to the Cabrillo format used for contest entries. You can then have it send your record directly to the robot. Nothing could be easier to send log files from your general purpose logger! Log Check Reports Log check reports are provided online for all participants. The notification is by email. If you have not received yours, please contact director@cqwpx.com. You can see examples of log checking reports for some of the best scorers. Do you have questions about the rules and what they mean? Visit the Rules FAQ page for answers to frequently asked questions. Future dates of the SSB contest is always the last full weekend of March.2022: March 26 - 272023: March 25 - 262024: March 30 - 31 CW is always the last full weekend of May.2022: 28 - 292023 May: 27 - 282024 May: 25 - 26 May 26