## LESSON: System Management

## Primer For this lesson and upcoming lessons, instructors are required to ensure the following activities are completed for each lesson

* Check-in with the students to see if they have any questions or need further clarification from any subject from the last class and self-study module.
* Review the “Lesson Opener” and “Real World Scenario” with the learners prior to starting the module.
* Throughout the module, you will find “Consider the Real World Scenario” slides. Review the questions found on these slides, tie the concepts back to the scenario discussed at the start of the lesson as well as content you are presenting, and encourage the learners to share their thoughts.
* For each lesson, you will find a “Pulse Check” slide which is the opportunity for instructors to open a poll to gather feedback from the learners. Leave the poll open for about 1 minute and after you close the poll, share the results with the learners. Encourage the learners to share their thoughts. This information will help the instructors as well as the learners better understand where they are with regards to the lesson.
* Labs are to be demonstrated live for each module. The demonstration and student engagements of the labs are the top priority for the lead instructor. While demonstrating each lab, encourage students to participate and explore.
* At the end of each lesson, it is important to take a few minutes to review the key concepts for the lesson, provide guidance on what the learners can do to prepare for the next lesson, and wrap up with Q&A.
* Instructors should manage breaks based on need, considering both timing and duration. You may take a break if you feel the students need it or if a particularly challenging topic has just been covered.

### 

### Summary

In this lesson, learners will discuss essential Linux administration and security topics. Learners will delve into package management, understanding packages and the APT system. They'll explore the significance of repositories and source lists for software installation. Linux services and their management using 'service' and 'systemctl' will be thoroughly covered, with a focus on Apache2 and SSH. The Secure Copy Protocol (SCP) for secure file transfer will be mastered, along with user activity monitoring through the 'last' and 'w' commands. Learners will grasp the intricacies of securing services, delve into log monitoring practices, learn about iptables as a firewall tool, and discover firewalld's zone-based firewall management. Lastly, crontab security best practices for script automation in Linux will be emphasized, providing a well-rounded understanding of Linux administration and security.

### Objectives

* Define software packages.
* Explain the use of the advanced package tool (APT) and its various commands for installing, updating, and removing software packages.
* Describe the role of repositories and source lists in package management, including their configuration files.
* Identify the apt update and apt upgrade commands and recognize their roles in updating the system and its packages.
* Define Linux services.
* Compare and contrast the service and systemctl commands within service management.
* Describe Apache2 web server service, as well as its installation, configuration, and default behavior.
* Illustrate the use of the Secure Shell Protocol (SSH) and Secure Copy Protocol (SCP) for secure remote access and file transfers.
* Identify the last and w commands for user activity monitoring.
* Recognize the importance of securing services.
* Summarize hardening essentials for Apache2 and SSH.
* Explain Linux log monitoring and the processes it involves.
* Define iptables, including its chain types, responses, and flags for rule management.
* Illustrate the use of firewalld as an alternative to iptables.
* Analyze the benefits and risks of using crontab for task automation.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 5 min | **Career Outcomes Content Reminder** | * Remind learners about the Career Outcomes modules to ensure that they know that the materials are available and to complete the assigned modules. * The first module will help the learners do the following:   + Use the required custom template that was created based on specific feedback from cyber employers.   + Begin creating their resume by adding their contact information, education, and professional experience.   + Submit their resume to receive actionable feedback from the Career Readiness team.   + This module can be found in Week 2 of Integrating Your Infrastructure Security. * Additional information for the second module regarding the resume submission assignment:   + Students must use the Career Outcomes resume templates to receive credit for this assignment.   + This is step one of a two-part resume writing process so students can more easily develop a strong technical resume. It will help them adopt a format aligned with resume-writing best practices.   + This module can be found in the “Resume and LinkedIn Submissions” course in Canvas. * Students can reach out to their SSM for questions and help if they need it. |
| 2 min | **Lesson Opener:**  System Management | * Introduce learners to the importance of system management in cybersecurity. |
| 5 min | **Real World Scenario:**  System Management | * Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation. |
| 2 min | **Lesson Companion Review:** Advancing System Management Skills in CloudTech's Linux Ecosystem | * Review the lesson companion, and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation. |
| 20 min | **Cyber Uncovered:**  Package Management | * Explain the concept of packages in Linux, including their contents and purpose. * Discuss how packages are managed and installed in Linux systems. * Introduce the advanced package tool (APT) and its significance in Debian-based Linux distributions. * Explain the role of APT in streamlining the installation, updating, and removal of software packages. * Demonstrate the use of the 'apt install' command to download and install new software packages, emphasizing the inclusion of dependencies. * Describe the process of uninstalling packages in Linux using the 'apt remove' command. * Highlight the difference between 'apt remove' and 'apt purge' regarding package and configuration file removal. * Define software repositories and their importance in Linux package management. * Explain the concept of source lists and their role in specifying repository locations. * Guide learners through accessing and configuring repositories. * Stress the importance of keeping Linux systems up-to-date for security and performance. * Walk learners through the 'apt update' command to refresh package information and the 'apt upgrade' command for updating installed packages. * Provide examples and practical exercises to reinforce the concept of system updates and upgrades. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 5 min | **Real World Scenario:**  Package Management | * Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation. |
| **5 min Break** | | |
| 20 min | **Cyber Uncovered:**  Common Management Services and Protocols | * Explain what Linux services are and their significance in system functionalities. * Emphasize how services differ from regular user applications and their role in background operations. * Introduce the 'service' command for managing services. * Detail the functionalities of 'service' including starting, stopping, and checking the status of services. * Provide real time demonstrations of 'service' commands to activate and deactivate the Apache2 web server service. * Present 'systemctl' as a powerful utility for managing services in newer Linux systems. * Describe how 'systemctl' integrates with the systemd system management framework. * Explain the key advantage of 'systemctl' in enabling services to start automatically at boot. * Conduct live demonstrations of 'systemctl' commands, focusing on starting services and configuring them for automatic startup. * Use Apache2 as an example to demonstrate how to enable and start the service using 'systemctl.' * Provide an overview of Apache2 as an open-source web server software designed for Linux. * Explain its capabilities in hosting web applications and services, as well as its default behavior. * Mention the installation process using 'sudo apt install apache2.' * Describe the primary directory for Apache2 web pages and its significance. * Highlight the main configuration file for Apache2 and its role in controlling server behavior. * Showcase the default homepage of an Apache2 web server. * Introduce SSH as an application-level protocol for secure remote command-line access. * Explain its client-server architecture and focus on data confidentiality and integrity over unsecured networks. * Mention SSH's compatibility with Unix-like operating systems, including Linux and its relevance to network security. * Detail the installation of SSH on Linux systems using 'sudo apt install openssh-server.' * Explore the location of SSH configuration files, including 'ssh\_config' for the client and 'sshd\_config' for the server in the '/etc/ssh/' directory. * Demonstrate the process of starting the SSH service and checking its status. * Guide learners on how to initiate SSH connections using commands like 'ssh <ip> -l <user>' and 'ssh <user>@<ip>.' * Explain SSH authentication methods, including password and key-based authentication. * Teach learners how to exit an SSH session. * Highlight the importance of SSH configuration files for fine-tuning security. * Discuss potential adjustments in the 'sshd\_config' file, such as changing the SSH port and security settings. * Introduce SCP as a secure protocol for file transfer over SSH. * Explain its advantages in ensuring secure file transfers. * Illustrate SCP syntax for copying files both locally and remotely. * Conduct a live demonstration on how to use SCP to copy a file from a local system to a remote host. * Show learners how to transfer files securely between systems. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 5 min | **Real World Scenario:**  Common Management Services and Protocols | * Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation. |
| 20 min | **Lab:**  Common Management Services and Protocols | * Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. * **In the ssh lab, you have to enter the exact commands in the lab, any additional command you enter will result in a prompt for a user password.** |
| 5 | **Pulse Check** | * Before you launch the pulse check, explain each section clearly, and encourage the learners to participate in the survey. * After administering the survey, share the poll results with learners and ask learners to provide feedback * Encourage learners to attend office hours with the associate instructor |
| **5 min Break** | | |
| 20 min | **Cyber Uncovered:**  System Hardening and Security Configurations | * Provide an overview of the importance of securing services in Linux. * Explain how secure services are essential for preventing unauthorized access and cyberattacks. * Detail the key security measures for Apache2, including regular updates and disabling directory listing. * Describe the importance of enabling HTTPS and limiting request sizes. * Explain how to restrict access based on IP addresses, hide version info, and implement web application firewalls. * Emphasize the significance of enabling logging and disabling unnecessary modules. * Conduct live demonstrations of all the Apache2 hardening essentials, showing learners how to execute the commands and configure settings. * Explain the critical steps for securing SSH, starting with backing up the SSH configuration file. * Describe how to edit the SSH configuration file to disable root login and whitelist specific users. * Highlight the importance of changing the default SSH port and implementing SSH key-based authentication. * Demonstrate how to set limits for password attempts, audit SSH connections, and limit connection rates. * Teach learners how to use a firewall to restrict incoming SSH connections from trusted IPs. * Lead learners through hands-on exercises for each SSH hardening essential, ensuring they can apply these security measures effectively. * Highlight the need to restart the SSH service after making changes. * Explain the role of log monitoring in system hardening and security configurations. * Describe the types of logs, including auth.log, Apache2 logs (access.log and error.log), and iptables log. * Emphasize the importance of monitoring logs for detecting unauthorized access and security breaches. * Provide demonstrations of log collection and management techniques. * Show how to access and interpret log examples from various sources, including authentication events and network access attempts. * Explain how Linux uses Logrotate configuration to efficiently manage log space. * Describe the process of maintaining a fixed number of logs, appending new entries, and deleting older logs. * Provide practical examples, such as keeping syslog files for a week and automatic log deletion. * Introduce iptables as a rule-based firewall daemon crucial for system hardening and security configurations. * Describe its role in managing network traffic through different chains, including INPUT, FORWARD, and OUTPUT. * Explain the various responses to chains, such as Accept, Drop, and Reject. * Present commonly used flags for rule management. * Conduct hands-on exercises to help learners understand and configure iptables. * Demonstrate how to add, check, delete, flush, and list rules using iptables commands. * Explain firewalld as a firewall management tool used in certain Linux distributions. * Describe its use of "zones" for granular control of network traffic. * Mention its flexibility in associating zones with multiple network interfaces. * Conduct live demonstrations of firewalld commands, including listing zones and services, reloading configurations, and adding ports. * Showcase how to create new zones and activate "panic mode" for emergency network isolation. * Explain the firewalld summary and its role in reviewing firewall settings. * Describe the concept of zone configuration and its relevance in network security. * Introduce crontab as a powerful utility for automating tasks through scripts. * Emphasize the security risks associated with poorly secured scripts. * Describe best practices for ensuring script integrity, secure permissions, and privilege management. * Guide learners through hands-on exercises to practice securing automated tasks in crontab. * Encourage learners to implement secure script storage, regular script integrity checks, strict permissions, and action logging. * Be prepared to discuss the implication of the real world scenario presented at the beginning of class on network types and devices. There are specific prompts that you should ask learners to reflect on to apply this concept to the real world scenario. |
| 5 min | **Real World Scenario:**  System Hardening and Security Configurations | * Review the real world scenario challenge and inform learners that you will be constantly coming back to this scenario throughout the lesson to discover how to solve and apply concepts to this real situation. |
| 20 min | **Lab:**  System Hardening and Security Configurations | * Remind learners to use this lab to practice and apply the concepts they have learned throughout the day. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. * Task #5 is a bit tricky. Ensure that you review the lab solution and practice before the class;   + **Copy chmod 777 /home/student/not-a.secret**  to /home/sysadmin/Desktop/ubiquitousness.sh |
| 2 min | **Midpoint Course Survey** | * Allocate 2 minutes to facilitate the completion of the Midpoint Survey. * Encourage learners to provide honest and constructive feedback about their learning experience. |
| 3 min | **Discussion Board** | * Allocate 3 minutes Review Discussion Board Slides and how it impacts students’ final grades. |
| 15 | **Lesson Closure** | * Encourage learners to read ahead of time * Provide learners additional resources to read / practice and assign homework (e.g., future labs) before you demonstrate the labs during the next class * Spend some time to highlight what are the key takeaways from today’s lesson * Important topics covered during the class includes   + Linux Package Management: update, upgrading, installing, uninstalling packages   + Provide a summary of repositories, sources.list file   + Provide a summary of linux services and difference between ‘service’ and ‘systemctl’ command   + Highlight the key takeaway for apache server such as hosting a web application, the installation process, and configuration   + Secure Shell Protocol / SCP and provide various use cases   + Explain Linux activity monitoring and what the learned observed in the class to monitor resources   + An overview of Linux hardening   + Contextualize what they learned with linux hardening such as apache, ssh, etc.   + Provide a summary of linux logging such as access.log, auth.log, etc.   + Provide a summary of iptables and policy chain such as input, Forward chain, and Output Chain and response such as accept, drop, and reject   + Provide a summary of firewalld and highlight various security zones   + Explain the key takeaway for crotab and how it can be used to automate tasks   + Highlight that if crontab is not configured correctly, it may result in potential compromise of the system. * **Q&A** |
|  | **Add Additional Time Filler** | * Review using Kahoot or other similar platforms * Conduct interview preparation conversations * Continue discussions on real-world scenarios * Demonstrate how to create users in Linux and grant them permissions * Discuss different career paths in cybersecurity and highlight the roles that require Linux skills |