## LESSON: Linux Administration and Security

## 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 of labs is 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.

### Summary

In this lesson, learners will dive into the world of Linux user types, including regular, sudo, and root users, which each have distinct permissions and roles. They will discover how to use specific commands to efficiently manage users, from listing to creating and deleting them. Strong password practices will be emphasized, guiding them in creating secure passwords and effective password management.

Learners will explore the significance of Linux groups, which simplify permission assignment to multiple users. They will also gain practical experience using commands to handle groups, much like with users. Understanding the pivotal roles of the /etc/passwd and /etc/shadow files, as well as the unique user identifiers (UIDs), will become second nature. Linux permissions, encompassing Read, Write, and Execute, will be thoroughly explained, with insights into both symbolic (UGO) and numeric representations.

The essential commands chmod and chown will equip learners with the skills to take control of file and directory ownership and permissions. Furthermore, they will unlock the power of SUID and GUID permissions, allowing them to perform specific administrative tasks while avoiding full root access. The importance of the PATH environment variable will be highlighted, showcasing its role in locating executable files. Transitioning to the realm of Linux networking, learners will become proficient in network interface commands like ipconfig and ip addr, both essential for displaying detailed network settings. They will master the art of network troubleshooting with indispensable tools like ping and traceroute, gaining insights into packet paths.

For IP configuration, learners will discover the versatility of dhclient and ifconfig commands or the option to edit the /etc/network/interfaces file, each method tailored to specific use cases. Finally, they will explore network monitoring through commands like netstat, ss, and lsof, honing their ability to detect unauthorized or malicious activity in the Linux environment.

### Objectives

* Identify the different Linux user types.
* Explain how to list, create, and delete users, along with the commands and files involved.
* Recognize the importance of implementing strong password practices.
* Identify the role of the /etc/shadow and /etc/passwd files for credentials management.
* Describe the uses of Linux groups.
* Explain how to list, create, and delete groups, along with the commands and files involved.
* Recognize the importance of the user identifier (UID) for resource access and permissions.
* Identify the three main Linux permission types and how they control access to files and directories.
* Compare and contrast the use of symbolic (UGO) and numeric permission representations for file management.
* Describe the use of the chmod and chown commands for managing file and directory ownership and permissions.
* Explain how special permissions like SUID and GUID allow the performance of special administrative tasks without full root access.
* Illustrate the use of the PATH environment variable to search for executable files.
* Illustrate the use of the network interface commands ifconfig and ip addr.
* Describe the diagnostic tools ping and traceroute.
* Compare and contrast different static ip configuration methods.
* Explain how to use the network monitoring commands netstat, ss, and lsof for malicious activity detection.

### Lesson Activities and Teaching Strategies

|  |  |  |
| --- | --- | --- |
| Estimated Time | Lesson Portion | Directions |
| 2 min | **Lesson Opener:**  Linux | * Introduce learners to the importance of Linux Administration and Security in cybersecurity. |
| 5 min | **Real World Scenario:**  Linux Administration | * 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:** Empowering CloudTech Through Linux | * 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:**  User and Group Management | * Briefly introduce the three main Linux user types: Regular users, sudo users, and the root user. * Explain their different levels of permissions and roles in a Linux system. * Describe the importance of listing, creating, and deleting users in Linux. * Demonstrate the use of the awk command to list usernames from the /etc/passwd file. * Highlight the differences between the useradd and adduser commands for user creation. * Provide examples of user creation and deletion using the adduser and deluser commands. * Emphasize the significance of strong passwords for cybersecurity. * Explain why strong passwords are important for security, privacy, compliance, trust, and data integrity. * Share tips for creating strong passwords, including length, complexity, avoiding common words, password history, and more. * Discuss the importance of password management, not sharing passwords, and using password managers. * Highlight the benefits of regularly updating passwords and enabling multi-factor authentication (MFA). * Explain how user management and authentication are handled in Linux. * Introduce the **/etc/shadow** file, which stores encrypted or hashed passwords for local users. * Describe the role of user identifiers (UIDs) in Linux for resource access and permissions. * Discuss the purpose of groups in Linux for collectively assigning permissions to users. * Explain the concept of primary groups and how they are assigned to users by default. * Demonstrate how to list groups using the **groups** command. * Describe the process of creating and deleting groups using commands like **addgroup**, **groupadd**, and **groupdel**. * Show how the **usermod** command can be used to add users to specific groups. * 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. * **Prepare to give learners a 5 minute break after the lab** |
| 5 min | **Real World Scenario:**  Linux Administration | * 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:**  User and Group Management | * Remind learners to use this lab to practice and apply the concepts they have learned throughout the class. * Learners will receive direct feedback on their lab to properly assess their knowledge and determine where they might need additional assistance. |
| **5 min Break** | | |
| 20 min | **Cyber Uncovered:**  File Permissions, Access Controls, and Environment Variables | * Explain the importance of permissions in Linux for security and proper system functioning. * Introduce the three main types of permissions: Read, Write, and Execute, and their roles. * Mention that permissions can be assigned to the owner, group, or others for granular control. * Describe the file permission breakdown, including file type, owner permissions, group owner permissions, and other user permissions. * Explain the significance of fields like hard links, file owner, group, file size, and modification date. * Discuss the two main ways to represent permissions: Symbolic (UGO) and numeric. * Explain the symbolic representation using "U" for User, "G" for Group, "O" for Others, and symbols for permissions (r, w, x). * Introduce numeric representation, where each permission is assigned a value, and show the table illustrating different permission values. * Introduce the **‘chmod'** command for changing permissions and explain its syntax using both numeric and symbolic representations. * Provide practical examples of changing file permissions using **‘chmod.'** * Introduce the **‘chown'** command for changing file ownership and group ownership, and explain its syntax. * Provide practical examples of changing file ownership and group ownership using **‘chown.'** * Explain the concept of SUID (Set User ID) and how it allows file execution with the owner's permissions. * Provide an example of SUID's common use case with the 'passwd' command. * Introduce GUID (Set Group ID) and explain its purpose when executed files inherit group permissions. * Provide an example of GUID's use on directories. * Describe the PATH environment variable and its role in locating executable files. * Explain how the system searches directories listed in PATH when a command is run. * 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:**  File permissions, Access Controls, and Environmental Variable | * 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:**  User and Group Management | * 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. |
| 5 min | **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:**  Network Configuration | * Explain the significance of network interfaces in Linux for communication. * Mention the ifconfig and ip addr commands for displaying interface information. * Highlight Linux's support for both IPv4 and IPv6 protocols. * Demonstrate how to use the ifconfig command to display detailed network interface settings. * Show the format and structure of ifconfig output with examples. * Introduce the alternative command, ip addr, and explain its usage. * Explain the purpose of the ping command as a network diagnostic tool. * Describe how ping checks connectivity by sending and receiving packets. * Provide examples of using ping to test network connections. * Introduce the traceroute command for observing packet paths in the network. * Explain how traceroute displays the sequence of routers and devices. * Show examples of using traceroute for network troubleshooting. * Describe the dhclient command for obtaining, renewing, or releasing DHCP leases. * Explain the -r option for releasing the current IP lease. * Discuss static IP configuration and its importance. * Show examples of configuring a static IP address using ifconfig and **editing /etc/network/interfaces.** * Introduce the netstat command for displaying network connections, routing tables, and interface statistics. * Explain the use of flags like -t for TCP, -u for UDP, and -l for listening sockets. * Provide examples of using netstat to monitor network connections. * Introduce the ss command as an alternative to netstat for investigating sockets. * Explain how ss provides more detailed information about TCP, UDP, and other protocol sockets. * Show examples of using ss to inspect network connections. * Describe the lsof command for listing open files and displaying network connections. * Explain the use of the -i flag to view network connections and -n for numerical IP addresses. * Provide examples of using lsof to detect unauthorized or malicious activity. * 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. |
| 20 min | **Real World Scenario:**  Network Configuration | * 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. |
| 10 min | **Lab:**  Network Configuration | * 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. |
| 15 min | **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   + Types of Linux users   + Strong password policies   + Different types of permissions in Linux (e.g., Read, Write, Execute)   + Where users and passwords are stored in Linux   + Groups in Linux and how they help to manage permissions   + SUID and SGID special permissions   + How the system uses environmental variables to find executable files   + Linux interface commands such as ifconfig, ip addr   + Use cases for traceroute, netstat, ss, ping, and lsof commands in Linux   + Explain how Linux is an integral part of cybersecurity. Share your professional experience with what was learned today * **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 |

### 