The Linux Security Journey Workbook

Version 1.0
June-2025

By Dr. Shlomi Boutnaru

Created using Google Gemini

Introduction

Having explored "The Linux Security Journey," you now possess a foundational understanding of Linux's security features. This companion workbook is designed to transform that knowledge into true mastery.

Through carefully crafted multi-choice questions and challenging hand-on tasks, you will actively engage with the concepts, applying theory to practical scenarios. This hands-on approach is crucial for solidifying your understanding and developing the essential skills needed to navigate the intricacies of the different security features included as part of Linux.

Lastly, you can follow me on twitter - @boutnaru (https://twitter.com/boutnaru). Also, you can read my other writeups on medium - https://medium.com/@boutnaru. Lastly, You can find my free eBooks at https://TheLearningJourneyEbooks.com.

Prepare to delve deeper; true expertise is achieved through practice. Let's begin!

Multiple Choice Questions (Beginner Level)

Question 1

What is the primary purpose of a UID (User Identifier) in Linux?

1. To manage file system quotas for users
2. To represent each Linux user in the kernel
3. To assign network addresses to users
4. To define the shell environment for a user

Question 2

Where is the UID for a specific user typically defined in a Linux system?

1. /var/log/auth.log
2. /etc/shadow
3. /etc/passwd
4. /boot/grub/grub.cfg

Question 3

Which UID is typically reserved for the 'root' user in Linux?

1. 500
2. 1
3. 0
4. 1000

Question 4

What does RUID (Real User ID) represent in a Linux system?

1. The user ID assigned to a process by the kernel
2. The user who initiated a specific operation or started a task/process
3. The user ID used for determining file permissions
4. The user ID that a process will switch to after execution

Question 5

What is the primary role of EUID (Effective User ID) in Linux?

1. Saving the user ID for future operations
2. Determining the permissions of a task (process/thread).
3. Identifying the original user who logged in
4. Tracking changes made to user accounts

Question 6

What is the purpose of SUID (Saved User ID) in the context of process execution?

1. To provide an alternative to the Real User ID
2. To store the original EUID when a high-privilege task temporarily lowers its privileges
3. To permanently change the EUID of a process
4. To define the maximum privileges a user can attain

Question 7

Which command-line utility can be used to create a new group in Linux?

1. gpasswd
2. groupdel
3. useradd
4. groupadd

Question 8

In Linux file permissions, what do 'r', 'w', and 'x' represent respectively?

1. Read, Write, eXecute
2. Rename, Wipe, eXtract
3. Report, Warn, eXamine
4. Read-only, Write-once, eXclusive

Question 9

What are the three categories of ownership for files/directories in Linux?

1. Owner, Creator, Guest
2. Root, System, User
3. User, Group, Other
4. Primary, Secondary, Public

Question 10

How can you numerically represent "read" permission when using the “chmod” command?

1. 1
2. 7
3. 4
4. 2

Question 11

What is the purpose of “umask” in Linux?

1. To change the ownership of existing files
2. To mask/filter default file mode permissions when creating new files/directories
3. To display the current working directory
4. To apply specific permissions only to executable files

Question 12

If the default file mode permissions for a new file are “666” and the umask is set to “0022”, what will be the resulting permissions of the newly created file?

1. 600 (rw-------)
2. 644 (rw-r--r--)
3. 777 (rwxrwxrwx)
4. 666 (rw-rw-rw-)

Question 13

What does the concept "File Permissions are Not Cumulative" mean in Linux?

1. All permissions from user, group, and other are combined to determine access
2. File permissions only apply to the owner, not to groups or others
3. Permissions accumulate over time as a file is accessed
4. Permissions are checked in a specific order (user, group, other), and the first applicable permission stops the check

Question 14

What is the effect of setting the SUID bit on an executable file in Linux?

1. The file can only be executed by its owner
2. The file will be executed with the permissions of its owner
3. The file's modification time is reset upon execution
4. The file becomes read-only for all users

Question 15

What is the main goal of ASLR (Address Space Layout Randomization)?

1. To increase system performance by optimizing memory usage
2. To prevent unauthorized access to user data
3. To make it more difficult for attackers to exploit memory corruption vulnerabilities by randomizing memory locations
4. To encrypt all data stored in RAM

Question 16

What is the main function of Secure Computing Mode (seccomp) in the Linux kernel?

1. To restrict the system calls that applications can use
2. To optimize CPU scheduling for critical applications
3. To provide secure network communication channels
4. To encrypt user data at rest

Answers

1. 2
2. 3
3. 3
4. 2
5. 2
6. 2
7. 4
8. 1
9. 3
10. 3
11. 2
12. 2
13. 4
14. 2
15. 3
16. 1

Hand-On Tasks (Beginner Level)

Task 1	
Objective	Learn to identify and differentiate between various user and group IDs associated with your session and processes
Instructions	1. Log in as a non-root user 2. Use the “id” command for observing your uid, gid, euid, and egid 3. Examine how UIDs and GIDs are stored by viewing the contents of the password and group files: “cat /etc/passwd” and “cat /etc/group”. Locate your user entry and note its UID and GID 4. Switch to the root user using “sudo -i” (you'll need to enter your password). 5. Run id again: id. Observe how your uid, gid, euid, and egid have changed

Task 2	
Objective	Observe the randomization of memory addresses for common memory regions across different process executions
Instructions	1. Use the “ldd” command (which is basically a script) to print shared object dependencies (by default it also prints the memory addresses) 2. Run it twice on the same binay like: “ldd `which ps`” 3. Observe the the results
Questions	1. Please explain the results of the commands executed and their relationship to ASLR 2. Bonus: what kind of dependencies do you think “ldd” does not show?

Task 3	
Objective	See how the SUID bit allows a program to run with the privileges of its owner while maintaining the real user's identity
Instructions	1. As a normal user, observe the permissions of the passwd executable: “ls -l /usr/bin/passwd” 2. Open a new terminal session 3. In this new terminal, start the “passwd” utility (you don't need to change your password) 4. While passwd is running, switch back to your original terminal. 5. Observe euid, suid and ruid of “passwd” using the following command: “ps -e -o comm,pid,euid,ruid,suid | grep passwd”

Task 4	
Objective	Practice changing permissions of files and folders
Instructions	1. Create a simple text file (like with the “echo” command) 2. Change the permissions of the file to “rw-r--r--" 3. Create a directory (using “mkdir”) 4. Set the permissions of the created directory to “rwxr-xr-x” 5. Remove both the directory and the file created

Task 5	
Objective	Understand how umask influences the permissions of newly created files and directories
Instructions	1. View your current umask value (using the “umask” command) 2. Create a new file with the “touch” command 3. Create a new empty directory 4. Check their permissions
Question	Based on your umask value, why do the created file and directory have those specific permissions?