SEC406: **Linux Security for InfoSec Professionals**

5 Day Program	30 CPEs	Laptop Required

Authors' Statements

"Linux is an essential component of today's technology ecosystem, powering critical infrastructure across the spectrum. If you want to enhance your security knowledge and skills, there is no better place to start than SEC406. Our class offers a hands-on approach that will enable you to acquire the essential knowledge and skills required to effectively manage and secure a Linux system. When I look back on my own journey into the security field, I realize that taking a course on Linux Security would have been an invaluable first step. Join us and gain the expertise you need to succeed in the security industry and advance your career. Are you ready to take that first step?"
—Charlie Goldner

"I've been thinking about how my career could have been different if this course had been available when I first started using computers. In those days, my lack of knowledge in Linux prevented me from utilizing the full potential of open-source tools. Fast forward to today, where technology is predominantly cloud based and reliant on Linux systems, these essential skills have never been more important. That is why I am so excited about bringing this course to a wider audience and assisting them in unleashing the power of Linux Administration and Security."
—Mark Baggett

Most new Information Security Professionals are more familiar with Windows than Linux, yet many of the critical tools used in today's offensive, defensive, ICS, and forensics positions require a strong understanding of Linux. This presents a serious challenge for those without the requisite experience because these systems are frequently utilized in highly exposed environments such as DMZs and the cloud. The irony is that now our information security platforms are creating new security risks. This Linux security course solves the problem by offering numerous hands-on exercises allowing students to quickly develop the Linux skills necessary to become a valuable asset to any Information Security team.

This Linux security training focuses on the fundamental aspects of Linux Administration, covering topics such as configuring a secure Linux system, working with the command line, and managing users and permissions. It also emphasizes the security aspects of these skills, teaching students how to secure their Linux systems and defend against potential attacks. You will learn how a misconfiguration introduces a vulnerability, how to attack that vulnerability and how to mitigate those risks. Upon completing the course, students will have the knowledge and skills required to secure Linux systems, identify potential security threats, and implement appropriate measures to prevent them. With our course, you can gain the experience necessary to become a skilled and confident Linux user, ensuring that you are an asset rather than a liability to your employer.

This Linux security class is suitable for a wide range of professionals who work with Linux systems and want to learn about securing them. Whether you are a system administrator, DevOps professional, security professional, network defender, blue-team, red-team, ICS, incident-responder, or cloud architect, this class will provide you with the knowledge and skills you need to secure your Linux-based infrastructure. By attending this class, you will learn about Linux security concepts, best practices, and tools, and how to implement them in your organization.

In this course, you will gain essential skills that will transform the way you work with a Linux-based Operating System. Starting in section one, you will navigate around your computer with ease using the terminal and master advanced file management techniques to boost productivity. By section two, you will understand how to customize your environment and locate programs. We will also cover everything you need to know about user accounts and groups. In section three, we will discuss file and system access controls and techniques to maintain robust system security. With section four, you'll discover how to manage your computer's resources and monitor its performance, whether you're working with a server or cloud-based systems. Finally, in section five, you'll unlock the power of package management, remote server management via SSH, networking, and other impressive tips and tricks. With our course, you will gain the confidence and proficiency to achieve more with your computer than you ever thought possible!

sans.org/sec406

- **Watch a preview of this course**
- **Discover how to take this course: Online**

Section Descriptions

SECTION 1: Linux Command Line

In this gentle orientation to Linux you will be introduced to the operating system, kernel, and the terminal. Here we begin by discussing essential skills such as using a terminal to navigate and identify programs. You will learn how to find and execute Linux programs and how to refine the results returned using appropriate options and parameters found in the manual pages. We will cover how to find help when you don't know how to use a command. We will teach you how history and command completion can level up your terminal skills and speed up your commands. Managing files within Linux is unique and we will cover various tips and tricks to make you an expert at this complicated subject. You will learn to know how and where files exist in the filesystem. This section concludes with a discussion on the Visual Editor which is a crucial skill for security and administration of any Linux system. By the end of this section, you will know how to use the terminal effectively, including understanding basic commands, file system navigation, and program execution. These skills will enable you to locate and launch programs, refine search results, and leverage manual pages.

TOPICS: Kernel, Operating System, and Distributions; Terminals; Manual pages; Command History; Navigation; File Management; Visual Editor

SECTION 2: Shell Syntax and Account Management

Digging into the terminal commands straight away is the best way to build muscle memory. This section builds off the terminal skills of Section 1. You will learn how to search for files within the filesystem and the various ways that grep can be used to search for information within files. Operating system functions and user experience are highly configurable, and we will learn how to modify our environment using variables and aliases and how that can be abused by a malicious actor. Every system contains some type of authentication mechanism for accounts and groups. We will explore how to manage accounts, discover and change the groups those accounts belong to, and how to switch between accounts. We will also cover how to manage file ownership. You will gain advanced file management techniques, including creating, copying, moving, and deleting files and directories, as well as using filters and pipes.

TOPICS: Searching the Filesystem; Various Forms of Grep; Environment Variables and Aliases; Account Management; Switching Users; Group Management; File Ownership

SECTION 3: File and User Access Control

Section 3 covers essential user access control concepts, including restricting administrative privileges, permissions, and security. Users interact with the filesystem in various ways with different levels of access. If you come to this class with a networking background, you know this as Authentication, Authorization, and Accounting. If you come into the class with a Windows background, you probably think of this as managing users and groups. We will translate those skills into the Linux world. We will learn how to ensure accounts have least-privilege access. Least privilege can be implemented in multiple ways, and we will cover how to do that with file level permissions and ownership. You will learn how to secure and appropriately leverage administrative credentials and closely guard them with Least Required Privilege. You will learn some of the tools available that can verify system settings are applied by auditing your system.

TOPICS: File Permissions; Special Permissions; Sudoers; SELinux and AppArmor

SECTION 4: Process and Log Management

Resource management and system monitoring skills, such as understanding processes, system load, and memory usage, are fundamental to working with servers and cloud-based systems. As you move resources to the cloud and establish micro-services in containers, knowing how to limit the resources consumed is a good security practice and can prevent you from incurring unanticipated costs. Managing system resources is how we can maintain the availability of our servers and prevent you from losing time and money. Since everything in Linux is essentially a file, we can look at running process file information and how to manage the processes running on our distributions. In addition, we will look at what a core dump is and how it can be abused. You will also learn several essential skills that enable your incident response process and continuous monitoring. Those essential skills will include things like scheduling tasks on Linux, keeping historical record of user activity, centralized logging, log rotation, and how to effectively manage and review those logs.

TOPICS: Resource Limits; Process Management and Scheduling; Services, Systemd, and Init; Logging and Log Rotation; Auditd

SECTION 5: Package, SSH and Network Management

Section 5 provides you with the opportunity to delve into package management, remote server management via SSH, networking, and other advanced tips and tricks. Like any operating system, we must keep our distributions up to date or we may need a new tool installed to accomplish a task. Often this is done through a package manager. You will learn how to leverage python virtual environments, configure, and manage the built-in package manager, and compile packages after a code review. You will learn encryption of data (at rest and in transit), and how that provides the necessary confidentiality from prying eyes. We will cover how to properly leverage SSH, SCP, and OpenSSL to secure communications. Linux is the basis for most of the networking gear out there. You can even use it as a router and firewall if you wish. We will cover how to manage networking settings and the host-based firewall.

TOPICS: Python Package Management; Installing and Running Open Source Software; Linux Package Management; SSH, Tunneling, and Post-Quantum Cryptography; Networking and Firewalls

Who Should Attend

- Anyone who manages Linux servers and is responsible for ensuring the security of those systems
- Everyone who deploys and manages applications on Linux-based cloud solutions
- Security professionals who want to learn about Linux security best practices and how to implement them in their organization.
- Technology professionals who want to gain a deeper understanding of Linux security concepts and improve their skills in securing Linux systems
- Anyone interested in learning about Linux security and how to protect their organization's systems and data from cyber threats