Privilege Escalation Techniques in Windows/Linux Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The path from a foothold to total system control is defined by Privilege Escalation. This crucial phase of any penetration test or Red Team operation separates intermediate security professionals from true elite hackers. Privilege Escalation Techniques in Windows/Linux Training Course is designed to arm you with the tactical methodologies and cutting-edge exploit development skills necessary to bypass the latest security controls on both Windows and Linux environments. From abusing misconfigurations like weak file permissions and unquoted service paths to exploiting advanced techniques like Kernel Vulnerabilities and Active Directory (AD) lateral movement, this course provides a deep dive into the attacker's mindset.

Mastering PrivEsc is essential for Offensive Security professionals and defensive Blue Teams alike who seek to rigorously test and fortify their network defenses. Through extensive hands-on labs and real-world Capture, The Flag (CTF) scenarios, you will not only learn how to identify critical weaknesses like exploitable SUID/GUID binaries and vulnerable services but also how to effectively enumerate systems, weaponize custom scripts, and ultimately achieve a root shell or SYSTEM access. Elevate your cybersecurity career by mastering these high-impact techniques and become an indispensable asset in the fight against sophisticated cyber threats.

Programme Curriculum

Privilege Escalation Techniques in Windows/Linux Training Course

Introduction

The path from a foothold to total system control is defined by Privilege Escalation. This crucial phase of any penetration test or Red Team operation separates intermediate security professionals from true elite hackers. Privilege Escalation Techniques in Windows/Linux Training Course is designed to arm you with the tactical methodologies and cutting-edge exploit development skills necessary to bypass the latest security controls on

both Windows and Linux environments. From abusing misconfigurations like weak file permissions and unquoted service paths to exploiting advanced techniques like Kernel Vulnerabilities and Active Directory (AD) lateral movement, this course provides a deep dive into the attacker's mindset.

Mastering PrivEsc is essential for Offensive Security professionals and defensive Blue Teams alike who seek to rigorously test and fortify their network defenses. Through extensive hands-on labs and real-world Capture, The Flag (CTF) scenarios, you will not only learn how to identify critical weaknesses like exploitable SUID/GUID binaries and vulnerable services but also how to effectively enumerate systems, weaponize custom scripts, and ultimately achieve a root shell or SYSTEM access. Elevate your cybersecurity career by mastering these high-impact techniques and become an indispensable asset in the fight against sophisticated cyber threats.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Master System Enumeration on both Linux and Windows to discover vital weak links and misconfigurations.
2. Exploit SUID/SGID and SUDO misconfigurations on Linux, including shell escape vectors via programs like vi, find, and Nmap.
3. Perform Token Impersonation and exploit Windows services, including AlwaysInstallElevated and Unquoted Service Paths.
4. Leverage Weak File/Folder Permissions on both operating systems to gain unauthorized access or modify critical binaries.
5. Identify and weaponize Kernel Vulnerabilities
6. Execute Credential Harvesting from memory, configuration files, and registry hives on Windows
7. Analyze and exploit Vulnerable Services to gain elevated command execution.
8. Utilize and automate industry-standard tools like LinPEAS and WinPEAS for rapid, post-exploitation environment scanning.
9. Develop and deploy custom, reliable Reverse Shells using Python, Bash, PowerShell, and other Living Off the Land binaries.
10. Understand and mitigate defense evasion techniques, specifically focusing on AppLocker/SELinux/AppArmor bypasses.
11. Practice Post-Exploitation persistence methods, including Startup Folder abuse and manipulating Cron Jobs and Windows Tasks.
12. Formulate a structured PrivEsc Methodology based on the MITRE ATT&CK framework for consistent penetration testing.
13. Apply all learned techniques in complex, multi-layered Hack The Box and TryHackMe style CTF scenarios.

Target Audience

1. Penetration Testers
2. Red Team Operators.
3. Security Analysts
4. Security Engineers.
5. Ethical Hackers
6. IT/System Administrators.

7. Vulnerability Researchers.
8. Cybersecurity Students.

Course Modules

Module 1: Foundational Enumeration and Low-Privilege Foothold

- Comprehensive file system, running processes, network, and installed software checks
- Initial system reconnaissance, including running services, installed applications, and network shares
- Introduction to initial discovery scripts like LinEnum and initial steps of PowerUp.
- Case Study: Identifying a low-privileged user on a Linux server via a vulnerable web application, gaining a basic reverse shell.
- Understanding the Principle of Least Privilege from an attacker's perspective.

Module 2: Linux Misconfiguration Exploitation

- Exploiting binaries with the SUID/SGID bit set to gain root access
- Abusing flawed SUDO permissions and shell escape sequences via GTFOBins and custom techniques.
- Manipulating the PATH environment variable for command injection into scripts run by root.
- Case Study: The infamous SUDO CVE-2019-14287 or a similar recent SUDO vulnerability exploitation.
- Identifying and exploiting writable configuration files and application services run by a high-privilege user.

Module 3: Windows Service and Token Exploitation

- Exploiting Unquoted Service Paths and service binaries with weak permissions to execute malicious payloads.
- Understanding and exploiting AlwaysInstallElevated registry key settings to run an MSI installer with SYSTEM privileges.
- Access Token Impersonation
- Case Study: Achieving SYSTEM access by exploiting a vulnerable, unpatched third-party service running as LocalSystem with an unquoted service path.
- DLL Hijacking techniques in vulnerable Windows applications.

Module 4: Kernel and Vulnerability Exploitation

- Identifying the target OS and Kernel version, checking for known CVEs using tools like Exploit-DB and Metasploit.
- Downloading, compiling, and safely executing public Kernel Exploits for both Linux and Windows.
- Developing custom exploit wrappers or scripts to improve reliability and stealth.
- Case Study: Successful local privilege escalation on an outdated Linux distribution using a recently patched, but unpatched-on-target, kernel vulnerability.
- The importance of prompt Patch Management and vulnerability assessment.

Module 5: File Permissions and Data Misconfigurations

- Exploiting Weak Permissions on sensitive files like, or unencrypted Windows SAM/SYSTEM registry hives.
- Abusing writable Cron Jobs and Windows Scheduled Tasks to inject malicious scripts for automated root access.
- Harvesting credentials and keys from SSH keys, web application configuration files, and developer backups.

- Case Study: Gaining a root shell by overwriting a script located in a writable folder that is called by a high-privilege scheduled cron job.
- Advanced techniques for exploiting NFS/Samba misconfigurations.

Module 6: Windows Credential & Post-Exploitation

- Using Mimikatz and similar tools to extract plaintext passwords and NTLM hashes from memory
- Performing Pass-the-Hash and Over-Pass-the-Hash for lateral movement.
- Techniques for manipulating the Windows Registry to achieve persistence
- Case Study: Compromising a Domain User, harvesting a cached Administrator hash, and using PtH to authenticate to a Domain Controller.
- Exploring fileless attack techniques and leveraging PowerShell for post-exploitation activities.

Module 7: Defensive Evasion and Advanced Tactics

- Bypassing basic endpoint detection by utilizing Living Off the Land Binaries
- Techniques to bypass application whitelisting solutions like AppLocker or exploit misconfigured Linux Mandatory Access Control
- Analyzing and manipulating system logs to erase traces
- Case Study: Successfully achieving command execution by invoking a trusted, signed Windows utility that is allowed by the system's AppLocker policy.
- Introduction to custom shellcode and payload generation to bypass signature-based antivirus.

Module 8: Comprehensive Methodology and CTF Practice

- Formulating a systematic, repeatable PrivEsc Methodology aligned with the Cyber Kill Chain and MITRE ATT&CK matrix.
- The importance of automated versus manual enumeration and decision-making during a penetration test.
- Hands-on, guided walkthroughs of complete end-to-end CTF machines
- Case Study: A final, timed exam scenario requiring participants to chain multiple techniques to achieve root.
- Professional documentation and Remediation Reporting for discovered privilege escalation vulnerabilities.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com