iGNITE
Technologies

ENROLL NOW

LINUX PRIVILEGE ESCALATION

TRAINING PROGRAM

www.ignitetechnologies.in

Why you should choose this course?

The Privilege Escalation Training curriculum consists of approaches that help students comprehend how an adversary gains access to higher-level privileges on a system or network. A network's adversaries are often able to go around within the system without proper credentials.

As part of your cybersecurity strategy, this course explains how to protect user accounts in your systems and web application.

Who should Join this course?

Do this course if you want to improve your Capture the Flag skills and get ready for certifications like the OSCP.

If your Senior Security Analyst, need to conduct comperihensive testing or Grey Box Pentesting.

Prerequisites

This course is for those interested in penetrating Linux-based operating systems. Anyone interested in taking this course should be familiar with Linux basic commands, ethical hacking, and the Kali Linux Platform and its well-known tools.

COURSE DURATION: 20 HOURS

iGNITE Technologies

LINUX PRIVILEGE ESCALATION TOPICS

Linux Fundamentals

- *Understanding Permissions in Linux*
- *Understanding Linux Users and Groups*
- *Popular Linux Editors and Tools*
- *Popular Linux Shell*
- *Spawning Root Shell*

Writable Files

- *Writable /etc/passwd*
- *Writable /etc/shadow*
- *Writable script invoked by root*
- *Python Library Hijacking*

SUID Binaries

- *What is SUID*
- *Lab Setup*
- *Finding Exsiting SUID Binaries*
- *Abusing SUID binary*
- *PATH Variable*

Misconfigured NFS

- *NFS Enumeration*
- *NFS Root Squashing*

Groups

- *Docker*
- *LXC/LXD*

Abusing Sudo Rights

- *What is Sudoers*
- *Ld_Preload*
- *Sudo_Inject (CVE2019-14287)*
- *Abusing Sudo Right*

Capabilities

- *List capabilities of binaries*
- *Edit capabilities*
- *Interesting capabilities*
- *Abusing Capabilities*

Exploiting Cron jobs

- *What is Cron jobs*
- *Systemd timers*
- *Abusing Cron Jobs*
- *Wildcard Injection*

iGNITE Technologies

Kernel Exploit

- *What is kernel*
- *Kernel exploit hunting*
- *Compiling exploit code*
- *DirtyCow*

Shell Escaping

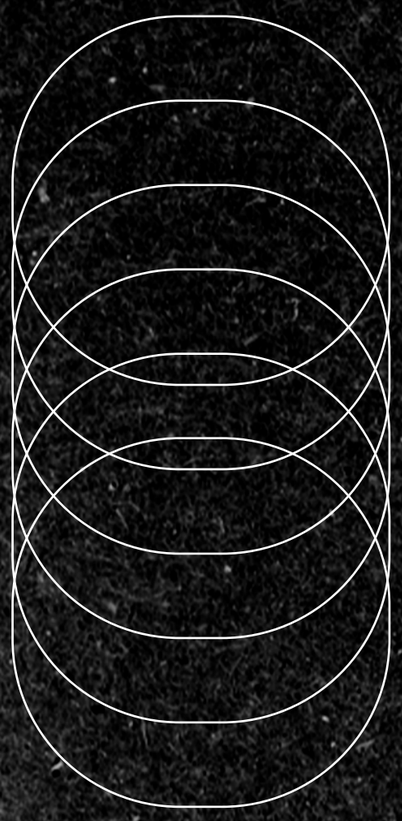
- *Restricted shell*
- *Pros of a restricted shell*
- *Cons of a restricted shell*
- *Multiple methods to bypass rbash*

Password Hunting

- *Files containing passwords*
- *Bash History*
- *SSH Key*
- *Brute forcing*

Automated Script

- *LinPEAS*
- *LinEnum*
- *LES: Linux Exploit Suggester*



iGNITE Technologies

CONTACT US

Phone No.

+91 9599 387 41 | +91 1145 1031 30

WhatsApp

https://wa.me/message/HIOPPNENLOX6F1

EMAIL ADDRESS

info@ignitetechnologies.in

WEBSITE

www.ignitetechnologies.in

BLOG

www.hackingarticles.in

LINKEDIN

https://www.linkedin.com/company/hackingarticles/

TWITTER

https://twitter.com/hackinarticles

GITHUB

https://github.com/ignitetechnologies

iGNITE Technologies