iGNITE Technologies

ENROLL NOW

PRIVILEGE ESCALATION

WINDOWS AND LINUX

TRAINING PROGRAM

WWW.IGNITETECHNOLOGIES.IN

iGNITE Technologies

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: 40 to 60 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

Misconfigured NFS

- NFS Enumeration
- NFS Root Squashing

Abusing Sudo Rights

- What is Sudoers
- Ld_Preload
- Sudo_Inject (CVE-2019-14287)
- Abusing Sudo Right

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

Groups

- Docker
- LXC/LXD

iGNITE Technologies

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

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

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

Password Hunting
- Files containing passwords
- Bash History
- SSH Key
- Brute forcing

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

Automated Script
- LinPEAS
- LinEnum
- LES: Linux Exploit Suggester

iGNITE Technologies

WINDOWS PRIVILEGE ESCALATION TOPICS

Introduction & Lab Setup
- Types of Privilege Escalation
- ACL Permissions
- Mitre ID T1547

Logon Autostart Execution
- Run Registry key
- Always Install Elevated
- Startup Folder

Exploiting Scheduled Tasks
- Task Scheduler
- Misconfigured Scheduled Task/Job
- Abusing Scheduled Task/Job
- Detection & Mitigation

Kernel Exploits
- What is kernel
- Compiling exploit code
- Enumerating missing patches
- Kernel exploit hunting

Weak Services/Permissions
- Insecure Service Properties
- Unquoted Service Path
- Weak Registry Permissions
- Insecure Service Executables
- Insecure GUI Apps

iGNITE Technologies

Passwords Hunting

- Registry
- Bruteforce
- Credential Manager (run as)
- Configuration File

Automated Tools

- WinPEAS
- Seatbelt
- SharpUp
- JAWS
- PowerUp
- Metasploit
- Watson
- Windows-Exploit-Suggester
- Sherlock

Bypass ACL

- SeBackupPrivilege
- SeRestorePrivilege
- Token Impersonation (Hot/Rotten/Juicy Potato/Printspoofer)
- HiveNightmare