iGNITE Technologies

WINDOWS PRIVILEGE ESCALATION

TRAINING PROGRAM

info@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: 20 HOURS

info@ignitetechnologies.in

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

Passwords Hunting

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

info@ignitetechnologies.in

iGNITE Technologies

Weak Services/Permissions

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

Bypass ACL

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

Automated Tools

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

info@ignitetechnologies.in