iGNITE Technologies

Version – 3.0

Active Directory

Latest Attack & Defense

Attack. Analyze. Defend. All in One Comprehensive Program.

Master Active Directory: Advanced Attack for Red Team & Defense Strategies for Blue Team

Deep Dive into Active Directory Security – Redefine Your Expertise
This isn't just another course—it's a complete transformation of how you approach Active Directory (AD). Designed for security analysts and pentesters, this advanced, hands-on program goes beyond the basics, teaching not only how attacks happen but also the root causes and strategies for prevention.

Why This Course Stands Out:

- Learn every attack type—from privilege escalation to lateral movement.
- Uncover misconfigurations that make AD vulnerable and their real-world implications.

Practical Mastery:

- Live Practice Sessions: Tackle real-world challenges with guidance from experienced trainers.
- Dive into upgraded content, featuring the latest attack methods and defense strategies.

Root Cause Analysis:

- Move beyond surface-level detection—understand why attacks succeed and how to fix systemic flaws.

Expert Trainers:

- Get insights from industry veterans who have worked on enterprise-level breaches and top-tier defenses.

iGNITE Technologies

COURSE OUTLINE

M1 Initial AD Exploitation
- Introduction to AD
- AD-DC Lab Setup
- ADCS Lab Setup
- Blackbox Pentesting
- LLMNR Poisoning Attack
- Grey Box Pentest UPDATED
- PrintNightmare
- HiveNightmare

M2 AD Post Enumeration
- RPCClient
- Bloodhound
- PowerView
- ADRecon
- Nxc ldap NEW

M3 DACL Abuse NEW
- Generic ALL
- Generic Write
- ALL Extended Write
- Force Change Password
- Write DACL
- Write Owner
- Self-Membership

M4 Abusing Kerberos
- Kerberos Authentication & Delegation
- AS-REP Roasting
- ASREQroast-MITM NEW
- Timeroasting NEW
- Kerberoasting Attack
- Kerberos Brute Force Attack

M5 Credential Dumping
- NTDS.dit Vs SAM and Registry Hive
- Domain Cache Credential
- LAPS UPDATED
- DCSync Attack UPDATED
- GMSA NEW
- Reversible Encryption NEW

M6 Kerberos Ticket Attack
- Golden Ticket
- Silver Ticket
- Diamond Ticket NEW
- Saphire Ticket NEW
- Pass the Ticket Atack

M7 Privilege Escalation
- Unconstrained Delegation
- Resource-Based Delegation
- S4U2self & S4U2Proxy Protocol NEW
- SAMAccountName Spoofing
- Token Impersonation
- Automated Script for Post Enumeration-ADpeas NEW

M8 Group Based Attack NEW
- Server Operator
- Account Operator
- Enterprises Key Admin /Key Admin (Shadow Credential Attack)
- DNS Admins Group
- Backup Operators

iGNITE Technologies

M9 Persistence

- Golden Certificate Attack
- DSRM
- AdminSDHolder
- DC Shadow Attack
- Skeleton Key

M10 ADCS NEW

- Misconfigured Certificate Templates - ESC1
- Misconfigured Certificate Templates - ESC2
- Misconfigured Enrollment Agent Templates - ESC3
- Vulnerable Certificate Template Access Control - ESC4
- Vulnerable PKI Object Access Control - ESC5

CONTACT US

PHONE

+91-9599387841 | +91 9599387845

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