ARMOURINFOSEC®

Hands-On Cyber Security Training · Indore, India

# Active Directory Security & Enterprise Attacks

*Course Syllabus*

Master Active Directory enumeration, Kerberos attacks, LDAP reconnaissance, credential attacks, privilege escalation, relay attacks, and advanced post-exploitation techniques used in enterprise penetration testing environments.

// COURSE INFORMATION

## Course Information

| | |
|---|---|
| DURATION | 1 Months / 4 Weeks / 30 Hours |
| LEVEL | Advanced |
| MODULES | 13 |
| FORMAT | Hands-on Labs / Hybrid (Online + Indore Classroom) |

// COURSE OVERVIEW

## Course Overview

The Advanced Active Directory Penetration Testing course is designed for ethical hackers, penetration testers, red teamers, SOC analysts, and cybersecurity professionals who want to specialize in attacking and assessing Active Directory environments. This course covers LDAP enumeration, Kerberos authentication internals, Kerberoasting, AS-REP Roasting, Pass-the-Hash, Pass-the-Ticket, SMB/LLMNR relay attacks, domain enumeration, privilege escalation, credential extraction, BloodHound analysis, and complete AD attack methodology.

// LEARNING OBJECTIVES

## Learning Objectives

- Enumerate Active Directory environments using LDAP and manual techniques
- Exploit Kerberos authentication (Kerberoasting, AS-REP Roasting)
- Perform Pass-the-Hash and Pass-the-Ticket attacks
- Conduct LLMNR poisoning and SMB relay attacks
- Extract credentials from SAM, SYSTEM, and NTDS.dit
- Escalate privileges from standard user to domain administrator
- Analyze attack paths using BloodHound
- Pivot through multi-subnet AD environments
- Use industry-standard tools (Mimikatz, CrackMapExec, Impacket, Evil-WinRM)

- Identify and exploit AD certificate services misconfigurations
- Provide enterprise hardening and remediation recommendations

// PREREQUISITES
## Prerequisites

- Basic networking knowledge
- Familiarity with Windows environments
- Understanding of Active Directory basics
- Knowledge of Linux command line
- Basic penetration testing experience

// MODULE BREAKDOWN
## Module Breakdown

### 01 LDAP Enumeration

- Overview of LDAP
- LDAP Enumeration Techniques
- LDAP Enumeration Tools
- LDAP Queries and Filters
- Nmap Scripts for LDAP Enumeration
- ldapsearch Usage
- JXplorer GUI Tool
- Active Directory Structure Mapping

### 02 Kerberos Authentication

- Introduction to Kerberos
- Kerberos Authentication Flow
- Kerberos Encryption Types
- Ticket Granting Ticket (TGT)
- Service Tickets (ST)
- Kerberos Attack Surface
- Key Distribution Center (KDC)
- Authentication Service (AS) and Ticket Granting Service (TGS)

### 03 Kerberoasting Attacks

- Service Principal Names (SPNs)
- Kerberoasting Methodology
- Extracting Service Tickets
- Offline Password Cracking
- Kerberoasting Tools
- Targeted Kerberoasting
- Detection and Mitigation

### 04 Pass-the-Ticket (PtT)

- Kerberos Ticket Abuse
- Ticket Injection Techniques

- Lateral Movement via Tickets
- Session Hijacking
- Kerberos Ticket Manipulation
- Golden Ticket Attacks
- Silver Ticket Attacks

## 05 AS-REP Roasting

- Kerberos Pre-Authentication
- AS-REP Roasting Methodology
- User Enumeration for AS-REP
- Offline Password Cracking
- Identifying Vulnerable Accounts
- Kerbrute Enumeration
- Detection and Prevention

## 06 Manual Enumeration

- Manual Enumeration Techniques
- Operating System Enumeration
- Domain User Enumeration
- Enumerating Logged-On Users
- Enumerating Permissions and ACLs
- SPN Enumeration
- Domain Share Enumeration
- Group Membership Mapping

## 07 Password Attacks & Credential Dumping

- Password Attack Methodologies
- Credential Dumping Techniques
- Accessing SAM File
- Accessing SYSTEM File
- Extracting SECURITY Files
- NTDS.dit Extraction
- Offline Hash Cracking
- Password Spraying
- Hashcat and John the Ripper Usage

## 08 Pass-the-Hash (PtH)

- NTLM Authentication Internals
- Pass-the-Hash Attack Methodology
- Lateral Movement with PtH
- Remote Authentication Abuse
- CrackMapExec for PtH
- Mimikatz Hash Extraction
- Detection and Countermeasures

## 09 LLMNR Poisoning & SMB Relay Attacks

- LLMNR/NBT-NS Poisoning
- SMB Relay Attack Methodology
- Name Resolution Poisoning
- NTLM Relay Attacks
- Credential Interception
- Responder Tool Usage
- NTLMv2 Hash Capture
- Relay Attack Mitigation

## 10 Active Directory Offensive Security Tools

- Impacket Framework
- ldapsearch and JXplorer
- Kerbrute
- Responder
- PowerUp
- PowerView
- BloodHound and SharpHound
- Mimikatz
- CrackMapExec
- Evil-WinRM
- Rubeus

## 11 Active Directory Privilege Escalation

- Windows Privilege Escalation Vectors
- Token Impersonation
- Service Exploitation
- DLL Hijacking
- Constrained Delegation Abuse
- Unconstrained Delegation Exploitation
- Resource-Based Constrained Delegation
- DCSync Attacks
- ADCS Exploitation (ESC1-ESC8)

## 12 Enterprise Lateral Movement & Persistence

- Lateral Movement Techniques
- Pivoting and Port Forwarding
- SSH Tunneling from Windows
- Chisel and Ligolo Usage
- Multi-Hop Pivoting
- Golden and Silver Ticket Forging
- Shadow Credentials
- Persistence Mechanisms
- Domain Trust Exploitation

### 13 Active Directory Hardening & Reporting

- AD Security Best Practices
- Kerberos Hardening
- NTLM Restriction Policies
- Privileged Access Management
- Detection Strategies
- SIEM Integration for AD Attacks
- Penetration Test Reporting
- Remediation Recommendations
- Enterprise Security Posture Assessment

// TOOLS & HANDS-ON LABS

## Tools & Hands-On Labs

- Multi-domain Active Directory forest
- Multiple organizational units with various permissions
- Certificate Services (ADCS) lab
- Multi-subnet network with segmentation
- Realistic enterprise user and group structure
- Kerberos attack simulation targets
- Relay attack practice environment
- BloodHound data collection and analysis lab

// TRAINING MODE

## Training Mode

Every Armour Infosec course runs as a unified programme delivered in two parallel modes — the same curriculum, the same trainers, the same certification, regardless of how you join.

- ✓ Online Live Classes — real-time, instructor-led, fully interactive sessions
- ✓ On-Premise Classroom Training — in-person at our Indore centre (Sudama Nagar)
- ✓ Both modes run concurrently in every batch; switch between them as your schedule needs
- ✓ Same syllabus, lab access, and certification track for online and on-premise students

// CERTIFICATIONS & CAREER OUTCOMES

## Certifications & Career Outcomes

This course aligns with industry-recognised certifications and prepares graduates for offensive-security, application-security, and infrastructure-security roles.

- OSCP+ AD module — Advanced Offensive Security Certification
- CEH (Certified Ethical Hacker)
- CRTP (Certified Red Team Professional)
- CRTE (Certified Red Team Expert)
- HTB Pro Labs (Offshore, RastaLabs)
- PNPT (Practical Network Penetration Tester)

// ENROL WITH ARMOUR INFOSEC

## Enrol With Armour Infosec

Reach out to discuss enrolment, batch schedule, and lab access. Our Indore training centre runs both in-person and live online cohorts with placement assistance.

| | |
|---|---|
| PHONE | +91 99777 47168 |
| EMAIL | info@armourinfosec.com |
| ADDRESS | 674, Sudama Dwar, Narendra Tiwari Marg, Sudama Nagar, Indore, Madhya Pradesh 452009 |
| WEBSITE | https://armourinfosec.com |

Scan to View Course Online

https://www.armourinfosec.com/training/active-directory-security/