Active Directory Security and Attacking Kerberos Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Active Directory is the Tier 0 crown jewel of nearly every Windows enterprise, making its security non-negotiable. As the single point for identity and access management, a compromised AD environment translates directly to full domain compromise. Modern adversaries, whether sophisticated nation-state actors or organized cybercrime groups, target fundamental authentication protocols like Kerberos to achieve their objectives. Attacks such as Kerberoasting, Pass-the-Hash, and Golden Ticket forgery are now standard phases in the cyber kill chain, enabling lateral movement and privilege escalation to Domain Admin. Traditional perimeter defenses fail here; security professionals must adopt an "assume breach" mindset and master the internal workings of AD and Kerberos.

Active Directory Security and Attacking Kerberos Training Course is designed to shift the focus from simple perimeter security to an adversary emulation perspective. Attendees will learn the latest Red Team techniques to identify, exploit, and pivot through a domain by weaponizing AD's inherent trust relationships and Kerberos protocol flaws. Crucially, the course is dual-focused: every offensive technique is immediately followed by Blue Team detection engineering, SIEM integration, and mitigation strategies based on the Secure Tiered Administration Model and Zero Trust principles. By understanding the attacker's tradecraft, defense teams can transform their security posture from reactive to proactive, ensuring resilience against the most persistent threats.

Programme Curriculum

Active Directory Security and Attacking Kerberos Training Course

Introduction

Active Directory is the Tier 0 crown jewel of nearly every Windows enterprise, making its security non-negotiable. As the single point for identity and access management, a compromised AD environment translates

directly to full domain compromise. Modern adversaries, whether sophisticated nation-state actors or organized cybercrime groups, target fundamental authentication protocols like Kerberos to achieve their objectives. Attacks such as Kerberoasting, Pass-the-Hash, and Golden Ticket forgery are now standard phases in the cyber kill chain, enabling lateral movement and privilege escalation to Domain Admin. Traditional perimeter defenses fail here; security professionals must adopt an "assume breach" mindset and master the internal workings of AD and Kerberos.

Active Directory Security and Attacking Kerberos Training Course is designed to shift the focus from simple perimeter security to an adversary emulation perspective. Attendees will learn the latest Red Team techniques to identify, exploit, and pivot through a domain by weaponizing AD's inherent trust relationships and Kerberos protocol flaws. Crucially, the course is dual-focused: every offensive technique is immediately followed by Blue Team detection engineering, SIEM integration, and mitigation strategies based on the Secure Tiered Administration Model and Zero Trust principles. By understanding the attacker's tradecraft, defense teams can transform their security posture from reactive to proactive, ensuring resilience against the most persistent threats.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Comprehend the intricate mechanics of the Kerberos protocol, including TGTs, TGSs, and Service Principal Names
2. Successfully perform and understand the defense for Kerberoasting against service accounts.
3. Identify and exploit accounts with disabled Kerberos pre-authentication.
4. Leverage AD misconfigurations to achieve Domain Admin rights.
5. Generate and utilize forged Golden Tickets and Silver Tickets for persistence and domain-wide access.
6. Use BloodHound to map and visualize complex attack paths within Active Directory forests.
7. Understand how Mimikatz and SecretsDump steal credentials and implement Credential Guard defenses.
8. Implement Group Managed Service Accounts and strong password policies to mitigate Kerberos attacks.
9. Integrate AD security with a Zero Trust Architecture and Least Privilege model.
10. Design and enforce a Tiered Administration Model to limit the blast radius of a Domain Controller compromise.
11. Configure Active Directory Auditing and integrate logs with a SIEM for detection.
12. Address modern threats specific to Hybrid Active Directory and Azure AD security.
13. Analyze compromised Domain Controllers for Indicators of Compromise related to AD attacks

Target Audience

1. Penetration Testers.
2. Security Analysts.
3. Active Directory Administrators.
4. Security Architects.
5. Incident Responders.
6. SOC Analysts.
7. Cybersecurity Consultants.
8. Compliance and Audit Professionals.

Course Modules

Module 1: Kerberos Protocol and Reconnaissance

- Kerberos fundamentals
- Understanding AD trust relationships and forests.
- Enumerating users, computers, and SPNs with PowerShell/BloodHound.
- Logging and monitoring LDAP queries
- Case Study: Analyzing the initial recon phase of the SolarWinds/SUNBURST attack to map compromised entities.

Module 2: Credential & Hash Theft Attacks

- Pass-the-Hash and LLMNR/NBT-NS Poisoning.
- Introduction to Golden Ticket and Silver Ticket.
- Credential Dumping.
- Implementing LSA Protection, Credential Guard, and disabling legacy protocols.
- Case Study: Replicating the "DCShadow" technique used for stealthy persistence and credential abuse.

Module 3: Active Kerberos Roasting & Account Misconfigurations

- Execution with Rubeus against Service Account tickets.
- Exploiting accounts with disabled pre-authentication.
- Exploiting weak DACLs/ACLs for privilege escalation.
- Auditing SPNs, strong service account passwords, and gMSAs.
- Case Study: The "WannaCry" ransomware pivot, where misconfigured service accounts facilitated lateral movement.

Module 4: Persistence and Lateral Movement

- Pass-the-Ticket and reusable TGTs.
- Forging the right to replicate AD data (NTDS.dit).
- Injecting malicious changes directly into the AD database.
- Detecting anomalous replication requests and monitoring for DCShadow events.
- Case Study: A Ransomware group's use of DCSync to dump all user hashes and hold the domain hostage.

Module 5: Advanced Privilege Escalation and Delegation

- Delegation Attacks.
- AD CS Exploitation.
- Attacking the KRBTGT account.
- Enforcing the Tiered Administration Model and auditing delegation settings.
- Case Study: Analyzing the Target Breach post-exploitation phase where delegation was abused to compromise critical systems.

Module 6: Blue Team: Detection Engineering & SIEM Integration

- Advanced Active Directory Auditing
- SIEM Integration.
- Creating custom detection rules for Kerberoasting and ticket forging.
- Using Microsoft Defender for Identity for IoA detection.

- Case Study: Developing an alert rule to detect a surge of Kerberos Service Ticket requests, a key Kerberoasting indicator.

Module 7: Active Directory Hardening & Zero Trust

- Implementing Local Administrator Password Solution
- Enforcing a Secure Tiered Administration Model
- Zero Trust for AD.
- Hardening Group Policy Objects and Organizational Unit structure.
- Case Study: A successful defense against a persistent threat using Tiering to contain the breach to Tier 2.

Module 8: Hybrid and Azure AD Security

- Hybrid AD Synchronization and security considerations.
- Azure AD and its unique attack vectors
- Conditional Access policies and MFA for privileged users.
- Securing AD Connect and monitoring for suspicious cloud activity.
- Case Study: An attacker exploiting misconfigured Conditional Access in a Hybrid AD environment to gain persistence.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com