Azure Penetration Testing and Red Teaming 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

In the age of Cloud-First strategies, Microsoft Azure has become the critical infrastructure backbone for global enterprises, storing immense volumes of sensitive data and hosting mission-critical applications. This shift has created an urgent and rapidly evolving need for elite security professionals skilled in Azure security and adversary simulation. Traditional network penetration testing methodologies are insufficient against the dynamic, identity-centric environment of the cloud. Our cutting-edge training course is specifically designed to bridge this critical skill gap, transforming security practitioners into top-tier Cloud Red Teamers capable of identifying, exploiting, and providing robust defenses against the most advanced Threat Actors targeting Azure and Microsoft Entra ID. Azure Penetration Testing and Red Teaming Training Course emphasizes a hands-on lab environment that simulates a complex, enterprise-level hybrid setup, focusing on real-world Cloud Attack Vectors and advanced MFA Bypass and Privilege Escalation techniques.

The essence of effective defense lies in understanding the offensive mindset. This course immerses students in the entire Azure Red Team engagement lifecycle, from initial Reconnaissance and Initial Access through to Persistence, Lateral Movement across multi-tenant and hybrid environments, and ultimate Data Exfiltration. We drill down into cloud-native misconfigurations and the subtle abuses of Identity and Access Management, which are the most common initial exploitation paths. Upon completion, participants won't just know how to find a vulnerability; they'll master the art of Adversary Emulation simulating targeted attacks to rigorously test the efficacy of an organization's security controls, including Microsoft Defender for Cloud and Microsoft Sentinel. This mastery of Cloud Penetration Testing and Red Team Tactics provides the indispensable skills required to secure next-generation cloud infrastructure and elevate an organization?ÇÖs overall Cloud Security Posture Management.

Programme Curriculum

Azure Penetration Testing and Red Teaming Training Course

Introduction

In the age of Cloud-First strategies, Microsoft Azure has become the critical infrastructure backbone for global enterprises, storing immense volumes of sensitive data and hosting mission-critical applications. This shift has created an urgent and rapidly evolving need for elite security professionals skilled in Azure security and adversary simulation. Traditional network penetration testing methodologies are insufficient against the dynamic, identity-centric environment of the cloud. Our cutting-edge training course is specifically designed to bridge this critical skill gap, transforming security practitioners into top-tier Cloud Red Teamers capable of identifying, exploiting, and providing robust defenses against the most advanced Threat Actors targeting Azure and Microsoft Entra ID. Azure Penetration Testing and Red Teaming Training Course emphasizes a hands-on lab environment that simulates a complex, enterprise-level hybrid setup, focusing on real-world Cloud Attack Vectors and advanced MFA Bypass and Privilege Escalation techniques.

The essence of effective defense lies in understanding the offensive mindset. This course immerses students in the entire Azure Red Team engagement lifecycle, from initial Reconnaissance and Initial Access through to Persistence, Lateral Movement across multi-tenant and hybrid environments, and ultimate Data Exfiltration. We drill down into cloud-native misconfigurations and the subtle abuses of Identity and Access Management, which are the most common initial exploitation paths. Upon completion, participants won't just know how to find a vulnerability; they'll master the art of Adversary Emulation simulating targeted attacks to rigorously test the efficacy of an organization's security controls, including Microsoft Defender for Cloud and Microsoft Sentinel. This mastery of Cloud Penetration Testing and Red Team Tactics provides the indispensable skills required to secure next-generation cloud infrastructure and elevate an organization?ÇÖs overall Cloud Security Posture Management.

Course Duration

5 days

Course Objectives

1. Master Azure-Specific Reconnaissance and OSINT techniques to map complex cloud and hybrid environments, including Entra ID tenants and connected services.
2. Perform Initial Access exploitation using trending vectors like Illicit Consent Grants, Device Code Phishing, and AI-driven Social Engineering.
3. Execute Advanced Multi-Factor Authentication (MFA) Bypass and Session Hijacking attacks to gain unauthorized access to protected resources.
4. Identify and exploit Identity and Access Management (IAM) and Role-Based Access Control (RBAC) misconfigurations for rapid Privilege Escalation within Azure subscriptions.
5. Develop expertise in leveraging compromised Managed Identities and Service Principals as high-value persistence and lateral movement pivots.
6. Perform Lateral Movement between Azure tenants, across subscriptions, and from Cloud to On-Premises leveraging Pass-the-PRT and federation abuses.
7. Compromise and exfiltrate secrets from key Azure Services including Key Vaults, Storage Accounts, Automation Accounts, and Azure DevOps pipelines.
8. Understand and exploit vulnerabilities in Cloud-Native Applications and Serverless functions for deeper system access.
9. Plan and conduct a full-scope, objective-based Adversary Emulation exercise following the MITRE ATT&CK for Cloud framework.

10. Analyze the effectiveness of Azure Security Controls like Conditional Access Policies (CAP), PIM, and Just-In-Time (JIT) access provisioning.
11. Master Defense Evasion techniques to circumvent logging, alerting, and detection by Microsoft Defender for Cloud and Microsoft Sentinel.
12. Generate actionable, high-impact Red Team Reports detailing the full kill chain, impact severity, and prioritized Zero Trust remediation strategies.
13. Integrate DevSecOps security testing into CI/CD pipelines to proactively prevent the deployment of new cloud misconfigurations.

Target Audience

1. Security Consultants/Penetration Testers.
2. Red Team Operators.
3. Cloud Security Engineers.
4. Security Architects.
5. Blue Team/SOC Analysts.
6. Incident Response Teams.
7. Ethical Hackers.
8. IT/DevOps Professionals.

Course Modules

Module 1: Azure and Entra ID Reconnaissance & Initial Access

- Mapping tenants, users, groups, application registrations, and federated domains using non-authenticated and authenticated OSINT tools.
- Exploiting unsecured Azure App Service endpoints and misconfigured Logic App and Function App triggers.
- OAuth & Consent Grant Attacks.
- Phishing & Credential Theft.
- Case Study: Compromise via Exposed App Service.

Module 2: Identity, Access, and Privilege Escalation

- RBAC Misconfiguration Abuse.
- Managed Identity Exploitation.
- Service Principal & Automation Account Abuse.
- Conditional Access & MFA Bypass Tactics.
- Case Study: Review an engagement where a flaw in a client's Privileged Identity Management setup allowed for permanent escalation of a low-privileged user to a Global Administrator role.

Module 3: Lateral Movement & Persistence in Hybrid Environments

- Cross-Tenant Lateral Movement.
- Cloud to On-Premises Attacks.
- Persistence Mechanisms.
- Token Theft & Reuse.
- Case Study: Simulation of a full-scale attack where the Red Team used a vulnerability in the Azure AD Connect server to perform an on-premises lateral move and take control of the entire AD forest.

Module 4: Data Mining and Exploitation of Core Services

- Key Vault Secrets Exfiltration.
- Storage Account Pwnage.
- Cloud Data Exfiltration.
- App Configuration and Function Code Retrieval.
- Case Study: An exercise involving the breach of a staging Azure DevOps environment, leading to the extraction of production database credentials from a CI/CD variable group.

Module 5: Post-Exploitation and Attack Infrastructure

- Command & Control (C2) in the Cloud.
- Evasion of Azure Security Services.
- Living Off the Land (LOTL) in Azure.
- Adversary Tradecraft.
- Case Study: A live-fire scenario where the Red Team successfully executed a multi-stage attack by exploiting a zero-day-like logic flaw that MDfC was not configured to detect.

Module 6: Hands-On Adversary Emulation and Red Team Methodology

- Red Team Planning & Scoping.
- Threat Intelligence Integration.
- Scenario Development.
- Reporting and Debriefing.
- Case Study: A capstone lab where students execute a full Red Team operation against a live-like Azure environment, from external recon to achieving the critical flag/objective.

Module 7: Cloud Defense and Remediation Strategies

- Microsoft Sentinel for Detection Engineering.
- Implementing Zero Trust Principles
- Cloud Security Posture Management Remediation.
- Reviewing Security Logs and Auditing.
- Case Study: Demonstrate integrating security scanning tools into an Azure DevOps CI/CD pipeline to catch the deployment of an insecure ARM template before it reaches production.

Module 8: Serverless, Container, and Emerging Attack Surfaces

- Container Security Exploits.
- Azure Machine Learning and AI Security.
- IoT & Edge Computing Security.
- Modern API Security.
- Case Study: A lab exercise focused on gaining initial access to an insecure container, performing a container escape to the underlying VM host, and pivoting to an internal subnet.

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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