PENTESTER ACADEMY

Attacking and Defending Azure AD Cloud – Beginner's Edition Bootcamp

Objective

More than 95 percent of Fortune 500 companies use Azure today! A huge number of organizations now use Azure AD as an Identity and Access Management platform using the hybrid cloud model. It is therefore imperative to understand the risks associated with Azure AD; not only do Windows apps and infrastructure use it, but the identities of users across an enterprise are also authenticated using it.

In addition to Azure AD's cloud-only identity, the ability to connect on-prem Active Directory, applications and infrastructure to Azure AD also brings with it some very interesting opportunities and risks. Often complex to understand, this setup of components, infrastructure and identity is a security challenge.

This hands-on training is aimed towards abusing Azure AD and a number of services offered by it. We will cover multiple complex attack lifecycles against a lab containing **multiple live Azure tenants**.

All the phases of Azure Red Teaming and pentesting are covered – recon, initial access, enumeration, privilege escalation, lateral movement, persistence and data mining. We will also discuss the detection and monitoring of the techniques we use.

The course is a mixture of fun, demos, hands-on exercises and lectures. The training focuses more on methodology and techniques than tools.

If you are a security professional trying to improve your skills in Azure AD cloud security, Azure pentesting, or red teaming the Azure cloud, this is the right class for you!

Module I

- Introduction to Azure AD
- Discovery and Recon of services and applications
- Enumeration
- Initial Access Attacks (Enterprise Apps, App Services, Logical Apps, Function Apps, Unsecured Storage, Phishing, Consent Grant Attacks)

Module II:

- Authenticated Enumeration (Storage Accounts, Key vaults, Blobs, Automation Accounts, Deployment Templates etc.)
- Privilege Escalation (RBAC roles, Azure AD Roles, Across subscriptions)

Module III:

- Lateral Movement (Pass-the-PRT, Pass-the-Certificate, Across Tenant, cloud to on-prem, on-prem to cloud)
- Persistence techniques

Module IV:

- Data Mining
- Defenses, Monitoring and Auditing (CAP, PIM, PAM, Security Center, JIT, Risk policies, MFA, MTPs, Azure Sentinel)
- Bypassing Defenses