Azure Application Security

Upskill to one of the most in-demand skillsets – application security in Azure. Learn to hack, attack and defend web applications in Azure.

What You'll Learn

This 4-week beginner-friendly bootcamp is for application security professionals, developers and cloud security professionals. Improve your understanding of Azure Cloud, Azure AD, Authentication & Authorization process, Enterprise Apps, APIs, OAuth Permissions and more. Learn about Azure services used for deploying and running applications such as AppServices, Function Apps, Key Vaults, Storage Accounts, Databases, etc.

This hands-on class covers abusing application flaws/misconfiguration, features and interoperability to compromise an enterprise-like live lab environment. Each student gets a dedicated lab! As a bonus, there is a shared lab to practice with fellow students. The class also covers security controls useful in defending against the discussed attacks. The Bootcamp will focus on methodology and techniques through instructor demos, exercises, and hands-on labs.

Build Your Cybersecurity Credentials

Become a Certified Azure Web Application Security Professional (CAWASP)

A certification holder demonstrates hands-on knowledge of application security in Azure. A Certified Azure Web Application Security Professional (CAWASP) would have practical knowledge of doing security assessments of various web application technologies on Azure and understanding of security controls that could be used for defense.

Prerequisites

1. Basic understanding of Application security and Azure is desired but not mandatory.

2. System with 4 GB RAM and ability to install OpenVPN client and RDP to Windows boxes.

3. Privileges to disable/change any antivirus or firewall.

Bootcamp Syllabus

Module I:

- Introduction to Azure Cloud
- Recon, Discovery and Enumeration
- Azure RBAC Roles and ABAC
- Rest APIs in Azure
- Authentication & Authorization
- Deep dive into OAuth
- Authentication methods supported by Azure

Module II:

- Tokens in Azure and their use in attacks
- About App Registrations
- About Enterprise Apps (Supported credentials, App roles and claims etc.)
- Attacking App Registrations and Enterprise Apps
- OAuth Permissions and their abuse (Privilege Escalation, Persistence and Lateral Movement)
- Consents and Permissions in Azure
- Illicit Consent Grant Attack (OAuth Phishing)
- Microsoft Graph API and its abuse

Module III:

- Abuse Azure services for Extracting secrets, Priv Esc, Persistence and Lateral Movement
- About App Services (Deployment, Configuration, SCM etc.)
- Attacking App Services by abusing app vulnerabilities and interoperability with other Azure services
- About Function Apps (Durable Function Apps, Triggers, Deployment etc.)
- Attacking Function Apps (Abusing integration with other Azure services)
- Understanding and Attacking Key Vaults (Access Policies, Retention Policies etc.)
- Understanding and Attacking Storage Accounts (Management plane to Data plane, SAS tokens, Connection Strings, Shared key, Information gathering from Metadata)

Module IV:

- Understanding and abusing Databases Services in Azure (Cosmos DB, SQL Server etc.)
- Understanding Application Proxy
- Azure API Management and API Security
- Defending Applications in Azure (Web Application Firewall, Microsoft Defender for Cloud Apps and Microsoft Defender for Cloud)
- Bypassing Defenses