CYBERIUM

AZURE

Azure

PENETRATION TESTING & SECURITY

INTRODUCTION

As more organizations move their infrastructure to Microsoft Azure, securing cloud environments has become a top priority. This course is designed to give you practical, hands-on skills to identify, exploit, and secure vulnerabilities in Azure cloud platforms.

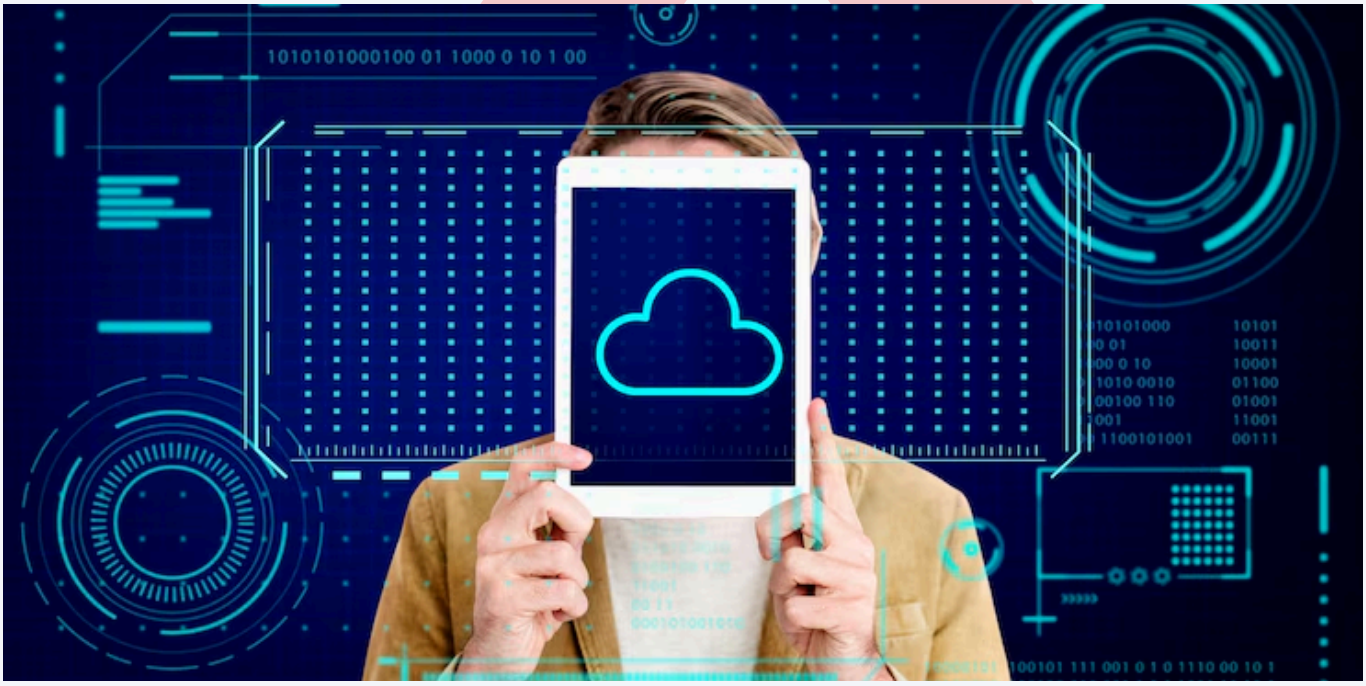
Whether you're a cybersecurity enthusiast, red teamer, cloud engineer, or IT professional, this course will guide you through real-world attack scenarios and defense techniques used in Azure environments.

You'll learn:

- **Azure architecture and core services from a security perspective**
- **Identity & Access Management (IAM) exploitation**
- **Misconfigured roles, permissions, and policies**
- **Azure AD attacks, token manipulation, and privilege escalation**
- **Tools like AADInternals, MicroBurst, and PowerZure**
- **Best practices to secure your Azure infrastructure**

By the end, you'll not only understand how to penetrate AWS environments, but also how to build a solid defense strategy to protect your cloud assets.
Let's dive into the cloud—and take full control of its security.

Course duration- 40 Hours



AZURE PENETRATION TESTING & SECURITY SYLLABUS

Module 01- Introduction to Azure and Cloud Computing

1. What is Microsoft Azure?
2. Azure vs AWS vs GCP overview
3. Understanding cloud service models: IaaS, PaaS, SaaS
4. Key concepts: Regions, Availability Zones, Resource Groups
5. Azure portal, CLI, PowerShell & Resource Manager (ARM)
6. Compute (VMs, App Services, Functions)
7. Storage (Blob, Table, File)
8. Networking (VNet, NSG, Azure Firewall)
9. Identity (Azure AD)
10. Database (SQL Database, Cosmos DB)

Module 02- Identity and Access Management in Azure

1. Azure Active Directory (Azure AD) fundamentals
2. Role-Based Access Control (RBAC)
3. Azure AD Conditional Access Policies
4. Multi-Factor Authentication (MFA)
5. Azure AD Privileged Identity Management (PIM)
6. Just-In-Time (JIT) access and Just-Enough-Access (JEA)

Module 03- Azure Security Services Overview

1. Microsoft Defender for Cloud
2. Azure Sentinel (SIEM and SOAR)
3. Microsoft Defender for Identity
4. Azure Key Vault
5. Azure Policy and Blueprints
6. Azure Information Protection (AIP)
7. DDoS Protection Plans

Module 04- Azure Networking and Network Security

1. Virtual Network (VNet) architecture
2. Subnets, Route Tables, and Network Security Groups (NSGs)
3. Azure Firewall and Application Gateway
4. Private Endpoints and Service Endpoints
5. Azure Bastion Host
6. VPN Gateway and ExpressRoute

Module 05- Data Security and Encryption in Azure

1. Data classification and protection
2. Encryption at rest & in transit
3. Customer-Managed Keys (CMKs) vs Microsoft-Managed Keys
4. Azure Disk Encryption
5. Secure Access to Blob Storage and SAS tokens
6. Azure Purview for data governance

Module 06- Securing Azure Compute and Applications

1. Hardening Azure Virtual Machines
2. Secure deployment pipelines (CI/CD) using DevOps and GitHub Actions
3. Web application security (App Service, Function Apps)
4. Container security in Azure Kubernetes Service (AKS)
5. API security with Azure API Management
6. Azure App Gateway WAF (Web Application Firewall)

Module 07- Incident Detection and Response

1. **Threat detection with Microsoft Defender**
2. **Setting up Azure Sentinel for centralized threat hunting**
3. **Creating custom detection rules and analytics**
4. **Automated response using Logic Apps and Playbooks**
5. **Forensics in Azure: log collection, evidence isolation**

Module 08- Introduction to Azure Penetration Testing

1. **Microsoft's cloud pen-testing policy**
2. **Scoping and legal considerations in Azure pentests**
3. **Penetration Testing vs Red Teaming in cloud**
4. **Cloud vs traditional pen-testing methodology**
5. **Permitted activities and rules of engagement**

Module 09- Reconnaissance and Enumeration in Azure

1. **Discovering Azure subdomains and services (AzureFront, *.cloudapp.net)**
2. **Identifying exposed resources (VMs, endpoints, blobs)**
3. **Tools: Azucar, MicroBurst, ScoutSuite, CloudFox**
4. **Enumerating Azure AD objects and roles**
5. **Detecting misconfigured public storage and secrets**

Module 10- Attacking Azure Resources

1. Exploiting misconfigured IAM and role assignments
2. Privilege escalation via role chaining and token abuse
3. Accessing unsecured blobs, functions, databases
4. Exploiting Azure AD Connect misconfigurations
5. Metadata API exploitation in Azure VMs (Managed Identity abuse)
6. SSRF & RCE in Azure-hosted apps

Module 11- Post-Exploitation and Pivoting in Azure

1. Lateral movement techniques in Azure environments
2. Extracting credentials from Key Vault and storage accounts
3. Abusing Azure automation and Logic Apps for persistence
4. Access token reuse and session hijacking
5. Dumping AzureAD logs, subscriptions, keys

Module 12- Defending and Hardening Azure

1. Secure Azure AD tenant configuration
2. Secure score analysis and improvement
3. Conditional Access and Identity Protection best practices
4. Hardening VMs and app services
5. Secure DevOps with security gates and dependency scanning
6. Logging and alerting for security events

Note: Please confirm payment details via our official WhatsApp +91-9318492128 before making any payment. Ensure the Payment Account name is 'CyberiumX' only.