

Offensive Azure Operations and Tactics Certification (OAOTC) Lab Guide





Offensive Azure Operations & Tactics Certification (OAOTC) Lab Guide

Table of Contents

Table of Contents	2
Version Control	11
Course Outline and Setup	11
1. Introduction.....	11
2. Course Approach.....	11
3. Course Support.....	11
4. Course Requirement.....	12
5. Lab Deployment Setup	12
Creating a New User	13
Acquire a "Microsoft Entra ID P2" License	17
Assign "Microsoft Entra ID P2" License	18
Disable Security Defaults	20
Get the Pay-as-you-go Subscription	22
Assigning Owner Privileges to the New User on the Subscription	23
Create DevOps Organization	25
Deployment Script.....	26
Configure the WKL Student Portal.....	27
Increasing IPV4 Quota	28
Increase vCPU Quota	31
6. Troubleshooting.....	33
Getting an Error While Deploying Labs.....	33
Using Wrong Credentials	33
Quota Issues	36
Module 1: Introduction to Azure/Entra ID.....	37
Entra ID Components	39
Azure Service	40
Microsoft Intune	41
Core Concepts of Intune	42



Office/Microsoft 365.....	44
Microsoft Graph.....	45
Authentication & Authorization Methods	48
OAuth 2.0 and OpenID Connect Flow	48
Authentication with Az PowerShell and Azure CLI.....	57
Authentication via Az PowerShell	57
Authentication via Azure CLI.....	58
Lab - Multiple Ways of Authentication	60
Introduction	60
Solution	60
Maze of Tokens	73
Types of Security Tokens	73
Token Lifetimes.....	73
Bearer Tokens and JWTs	74
Primary Refresh Tokens (PRTs).....	74
Module 2: Azure Access Controls	76
Role-Based Access Control (RBAC).....	76
Attribute-Based Access Control (ABAC).....	79
Privileged Identity Management (PIM)	82
Lab - Enumerate Custom Roles	85
Introduction	85
Solution	85
Key Vault Access Policies.....	92
Management Plane vs. Data Plane.....	94
Module 3: Enumeration Approach	95
Unauthenticated Enumeration	95
Authenticated Enumeration	96
Lab - Resource Enum	102
Introduction	102
Solution	102
Glimpse of Security Controls.....	107
Azure Conditional Access Policies (CAP).....	107
Azure Policy	108



Module 4: Gaining Initial Foothold	110
Device Code Phishing	110
Dynamic Device Code Phishing	113
Illicit Consent Grant Attack	115
Man-in-the-Middle (MitM)	118
Exposed Services	120
Storage accounts	120
Storage Accounts SAS Token	121
Lab - Storage Account Connection String	124
Introduction	124
Solution	124
Lab - Storage Account - SAS Token	130
Introduction	130
Solution	130
Lab - Storage Account - Rest API Access	137
Introduction	137
Solution	137
Serverless Infrastructure	142
Introduction to Serverless Infrastructure	142
Lab - Managed Identity in Function App	150
Introduction	150
Solution	150
App Service	154
Exploiting Application	156
Lab - Vulnerable Web	161
Introduction	161
Solution	161
Logic Apps	164
Azure Kubernetes (K8s)	165
Exposed Credentials	167
Password Spray	168
Lab - Password Spray Attacks	170
Introduction	170



Solution	170
Module 5: Post Exploitation & Lateral Movement Approach.....	174
Hijacking Function Apps	174
Attack Techniques for Function Apps.....	176
Publish Profiles and the SCM Portal.....	176
Abusing Function App Master Key.....	178
Lab - Abusing Master Key	186
Introduction	186
Solution	186
Abusing Storage Account for Lateral Movement	201
Lab - Abusing Package Files.....	212
Introduction	212
Solution	212
Hunting for Sensitive Information.....	224
Abusing the Reader Role	224
Azure Resource Manager (ARM) Templates.....	230
Logic Apps: A Source of Hardcoded Credentials	231
Lab - Abusing Reader Role	233
Introduction	233
Solution	233
Hijacking Azure Cloud Shell.....	239
Lab - Hijacking Cloud Shell	244
Introduction	244
Solution	244
Abusing logic App	252
Lab - Sensitive Info in API Workflow	254
Introduction	254
Solution	254
Abusing Logic Apps via Managed Identity	257
Lab - Managed Identity in Logic App.....	260
Introduction	260
Solution	260
Abusing Storage Account Write Access on Blob Storage.....	268
Abusing Storage Account Write Access on Azure File Share	281



Azure Key Vault.....	284
Lab - Key Vault - Decrypt Secrets with Old Key.....	286
Introduction	286
Solution	286
Lab - Key Vault - Modify the Access Policy and Extract the Certificate.....	293
Introduction	293
Solution	293
Lab - Key Vault - Decrypt Secrets with Old Key and Restore Backup from Storage Account	304
Introduction	304
Solution	304
Azure Cosmos DB.....	315
Lab - Cosmos DB - Leverage Read only Key to gain access.....	316
Introduction	316
Solution	316
Microsoft Intune: A High-Value Target	319
Pathway 1: Application-Based Compromise.....	319
Pathway 2: Device Configuration Scripts.....	320
Attack Path: Intune To On-Prem/Employees Devices	321
Token Exchange	322
Understanding Microsoft First-Party Applications.....	322
The Token Exchange Attack.....	322
Module 6: Entra ID Misconfiguration	323
Shadow Admins	323
Lab - PIM Eligible Role.....	325
Introduction	325
Solution	325
Enterprise Apps/App Registrations.....	330
App Registration Ownership and Attack Path.....	331
Enterprise App Users & Groups.....	332
App Service Authentication with an Identity Provider	333
Lab - Abusing Shadow Admins	335
Introduction	335
Solution	335
Conditional Access Policy (CAP)	345



CAP Misconfigurations: The Attacker's Opportunity	346
Joining a Fake Device into Entra ID with AADInternals	347
Abusing CAP via Microsoft Graph API Permissions	348
Entra ID Groups and Dynamic Membership.....	350
Entra ID Group Types	350
Entra ID Membership Types	350
Security Risk: Misconfigured Dynamic Rules	351
Guest Users and Invitation Abuse	352
Lab - Weak Membership Rules	355
Introduction	355
Solution	355
Authentication Methods	363
Temporary Access Pass (TAP).....	364
Passwordless Authentication	364
Microsoft Authenticator	365
OATH Tokens	367
Phone Options	367
Email Authentication	367
Module 7: Introduction to Azure DevOps	368
Core ADO Services	369
Boards	369
Repos	369
Wiki.....	370
Pipelines.....	371
Pipelines – Library.....	372
Test Plans	373
Artifacts	374
Lab - Hunting for Leaked Credentials in DevOPS.....	375
Introduction	375
Solution	375
Exploring Project Settings	387
Permissions - Projects	388
Permissions – Pipelines	390
Agent Pools	391



Service Connections	392
Understanding Pipelines	394
Pipeline Architecture Overview	394
Pipeline Creation	395
Running Pipelines	397
Setting Up Self-Hosted Agents	400
Agent Pools	400
Azure Pipelines with GitHub	402
Pipeline Creation: Connecting to GitHub	402
YAML vs. Classic Editor Build	405
YAML Structure	405
YAML Build Configuration	405
Visual Interface for Pipeline Creation (Classic Editor)	407
Build and Release Pipelines (Classic Editor)	409
Lab - Abusing DevOPS Pipelines to extract Secrets	412
Introduction	412
Solution	412
DevOps REST APIs	432
DevOps Personal Access Token (PAT)	432
Using a PAT for Authentication	433
Getting Access Token	435
Lab - Abusing DevOPS using Rest APIs	437
Introduction	437
Module 8: Pivoting From Cloud to On-prem	438
Automation Account.....	438
Automation Account Credentials.....	438
Extracting Credentials from Runbook	439
Lab - Automation Account Credential Object	441
Introduction	441
Solution	441
Lab - Automation Account Certificate	446
Lab - Automation Account Certificate	451
Introduction	451
Solution	451



Hybrid Worker	457
Extending Automation to On-Premises.....	457
Hybrid Worker - Pivoting to On-prem.....	458
Lab - Hybrid Worker.....	460
Introduction	460
Solution	460
Azure Arc.....	463
Adding an On-Prem Server.....	464
Lab - Custom Script Extension	471
Introduction	471
Solution	471
Hybrid Connections.....	475
Run Command - Azure Arc.....	476
Function App/App Service to On-Prem.....	476
Lab - Cloud to On-prem via Function App	480
Introduction	480
Solution	480
Application Proxy	485
Application Proxy Authentication Workflow	486
Application Proxy Connector Workflow.....	488
Application Proxy Web App	489
Application Proxy Creation.....	490
Attack Path: Application Proxy to On-prem	491
Module 8: Pivoting from On-prem to Cloud	492
Hybrid Identity	492
Password Hash Synchronization (PHS)	493
Pass-Through Authentication (PTA) and Attack Paths.....	496
Azure AD Federation Integration (AD FS)	498
Single Sign-On (SSO).....	499
Stealing PRT	501
Module 9: Maintaining persistence.....	503
Service Principal Persistence: The Stealthy Backdoor.....	503
The Attack Vectors.....	503
Understanding the Key Permissions.....	503



Automation Accounts	506
Automation Account: The Cloud Command Center	506
Azure Arc: The Universal Bridge	506
Onboarding the Machine with Azure Arc for Persistence	506
The Hybrid Worker Persistence Chain	508
Hybrid Connections	511
The Core Component: Hybrid Connection Manager (HCM)	511
The Attacker's Abuse Vector	512
Exploiting Remote Access (PS Remoting)	512
Exploiting Hybrid Connections with Function Apps	513
SCM Portal Access	514
Virtual Machine Run Command and Persistence with ARC	514
Lab - Virtual Machine Run Command and Persistence with Hybrid Worker	516
Introduction	516
Solution	516
Lab - Virtual Machine Run Command and Persistence with HCM	517
Introduction	517
Solution	517
Module 10: Configuration Assessment	518
The Role of CSI Benchmarks	518
Automation and Client Context	520
Required Permissions for Assessment	520
Automated Tools for Configuration Assessment	521
Open-Source Tools	521
Commercial Tools	523
Lab – Config Review	524
Introduction	524
Solution	524