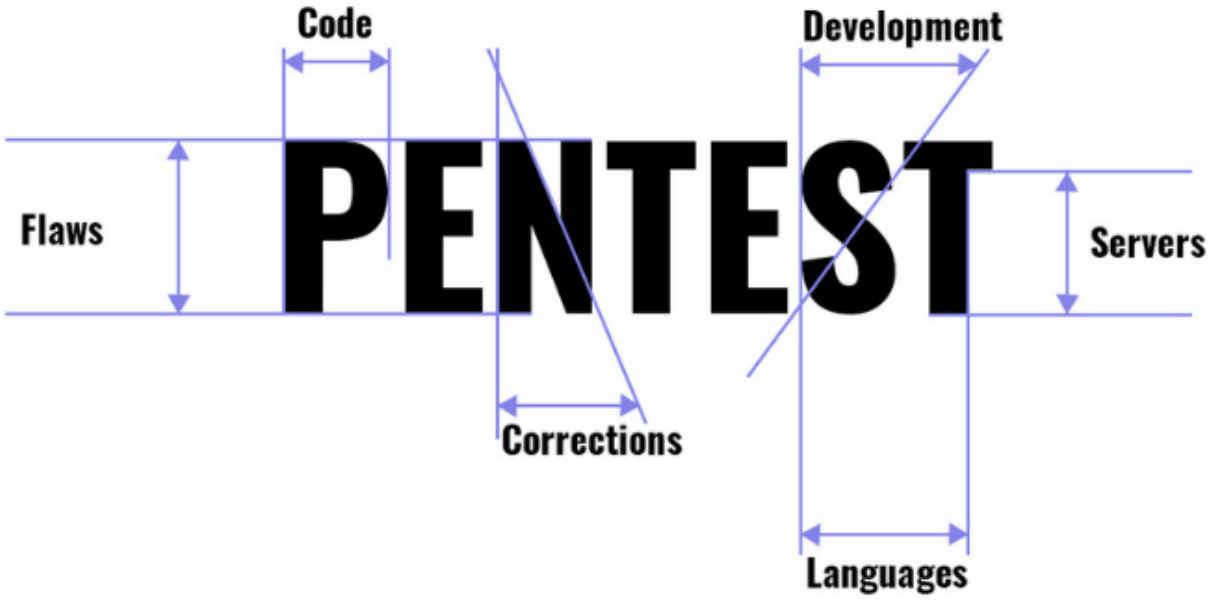
Awesome Azure Penetration Testing



A curated list of useful tools and resources for penetration testing and securing Microsofts cloud platform **Azure**.

Table of Contents

Tools

Enumeration

- o365creeper - Enumerate valid email addresses
- CloudBrute - Tool to find a cloud infrastructure of a company on top Cloud providers
- cloud_enum - Multi-cloud OSINT tool. Enumerate public resources in AWS, Azure, and Google Cloud
- Azucar - Security auditing tool for Azure environments
- CrowdStrike Reporting Tool for Azure (CRT) - Query Azure AD/O365 tenants for hard to find permissions and configuration settings
- ScoutSuite - Multi-cloud security auditing tool. Security posture assessment of different cloud environments.
- BlobHunter - A tool for scanning Azure blob storage accounts for publicly opened blobs
- Grayhat Warfare - Open Azure blobs and AWS bucket search
- Office 365 User Enumeration - Enumerate valid usernames from Office 365 using ActiveSync, Autodiscover v1 or office.com login page
- CloudFox - Automating situational awareness for cloud penetration tests
- Monkey365 - Conduct Microsoft 365, Azure subscriptions and Azure Active Directory security configuration reviews
- Azure-AccessPermissions - PowerShell script to enumerate access permissions in an Azure AD environment
- Prowler - Perform AWS and Azure security best practices assessments, audits, incident response, continuous monitoring, hardening and forensics readiness

Information Gathering

- o365recon - Information gathering with valid credentials to Azure
- Get-MsolRolesAndMembers.ps1 - Retrieve list of roles and associated role members
- ROADtools - Framework to interact with Azure AD
- PowerZure - PowerShell framework to assess Azure security
- Azurite - Enumeration and reconnaissance activities in the Microsoft Azure Cloud
- Sparrow.ps1 - Helps to detect possible compromised accounts and applications in the Azure/M365 environment
- Hawk - Powershell based tool for gathering information related to O365 intrusions and potential breaches

- Microsoft Azure AD Assessment - Tooling for assessing an Azure AD tenant state and configuration
- Cloud Katana - Unlocking Serverless Computing to Assess Security Controls
- SCuBA M365 Security Baseline Assessment Tool - Automation to assess the state of your M365 tenant against CISA's baselines

Lateral Movement

- Stormspotter - Azure Red Team tool for graphing Azure and Azure Active Directory objects
- AzureADLateralMovement - Lateral Movement graph for Azure Active Directory
- SkyArk - Discover, assess and secure the most privileged entities in Azure and AWS
- omigood (OM I GOOD?) - Scanner to detect VMs vulnerable to one of the "OMIGOD" vulnerabilities

Exploitation

- MicroBurst - A collection of scripts for assessing Microsoft Azure security
- azuread_decrypt_msol_v2.ps1 - Decrypt Azure AD MSOL service account
- Microsoft-Teams-GIFShell - Microsoft Teams can be leveraged by an attacker, to execute a reverse shell between an attacker and victim piped through malicious GIFs sent in Teams messages

Credential Attacks

- MSOLSpray - A password spraying tool for Microsoft Online accounts (Azure/O365)
- MSOLSpray.py - A Python version of the MSOLSpray password spraying tool for Microsoft Online accounts (Azure/O365)
- o365spray - Username enumeration and password spraying tool aimed at Microsoft O365
- MFASweep - A tool for checking if MFA is enabled on multiple Microsoft Services Resources
- adconnectdump - Dump Azure AD Connect credentials for Azure AD and Active Directory

Resources

Articles

- Abusing Azure AD SSO with the Primary Refresh Token
- Abusing dynamic groups in Azure AD for Privilege Escalation
- Attacking Azure, Azure AD, and Introducing PowerZure
- Attacking Azure & Azure AD, Part II

- Azure AD Connect for Red Teamers
- Azure AD Introduction for Red Teamers
- Azure AD Pass The Certificate
- Azure AD privilege escalation - Taking over default application permissions as Application Admin
- Defense and Detection for Attacks Within Azure
- Hunting Azure Admins for Vertical Escalation
- Impersonating Office 365 Users With Mimikatz
- Lateral Movement from Azure to On-Prem AD
- Malicious Azure AD Application Registrations
- Moving laterally between Azure AD joined machines
- CrowdStrike Launches Free Tool to Identify and Help Mitigate Risks in Azure Active Directory
- Privilege Escalation Vulnerability in Azure Functions
- Azure Application Proxy C2
- Recovering Plaintext Passwords from Azure Virtual Machines like It's the 1990s
- Forensicating Azure VMs
- Network Forensics on Azure VMs
- Cross-Account Container Takeover in Azure Container Instances
- Azure Active Directory password brute-forcing flaw
- How to Detect Azure Active Directory Backdoors: Identity Federation
- Azure App Service vulnerability exposed hundreds of source code repositories
- AutoWarp: Cross-Account Vulnerability in Microsoft Azure Automation Service
- Microsoft Azure Synapse Pwnalytics
- Microsoft Azure Site Recovery DLL Hijacking
- FabriXss (CVE-2022-35829): Abusing a Custom Role User Using CSTI and Stored XSS in Azure Fabric Explorer
- Untangling Azure Active Directory Principals & Access Permissions
- How to Detect OAuth Access Token Theft in Azure
- How to deal with Ransomware on Azure
- How Orca found Server-Side Request Forgery (SSRF) Vulnerabilities in four different Azure Services
- EmojiDeploy: Smile! Your Azure web service just got RCE'd
- Bounce the Ticket and Silver Iodide on Azure AD Kerberos

Lists and Cheat Sheets

- List of all Microsoft Portals

- Azure Articles from NetSPI
- Azure Cheat Sheet on CloudSecDocs
- Resources about Azure from Cloudberry Engineering
- Resources from PayloadsAllTheThings
- Encyclopedia on Hacking the Cloud
- Azure AD - Attack and Defense Playbook
- Azure Security Resources and Notes
- Azure Threat Research Matrix

Lab Exercises

- azure-security-lab - Securing Azure Infrastructure - Hands on Lab Guide
- AzureSecurityLabs - Hands-on Security Labs focused on Azure IaaS Security
- Building Free Active Directory Lab in Azure
- Aria Cloud Penetration Testing Tools Container - A Docker container for remote penetration testing
- PurpleCloud - Multi-use Hybrid + Identity Cyber Range implementing a small Active Directory Domain in Azure alongside Azure AD and Azure Domain Services
- BlueCloud - Cyber Range system with a Windows VM for security testing with Azure and AWS Terraform support
- Azure Red Team Attack and Detect Workshop
- SANS Workshop – Building an Azure Pentest Lab for Red Teams - The link in the description contains a password-protected OVA file that can be used until 2nd March 2024

Talks and Videos

- Attacking and Defending the Microsoft Cloud (Office 365 & Azure AD
  - Presentation Slides
- TR19: I'm in your cloud, reading everyone's emails - hacking Azure AD via Active Directory
  - Presentation Slides
- Dirk Jan Mollema - Im In Your Cloud Pwning Your Azure Environment - DEF CON 27 Conference
  - Presentation Slides
- Adventures in Azure Privilege Escalation Karl Fosaaen
  - Presentation Slides
- Introducing ROADtools - Azure AD exploration for Red Teams and Blue Teams

Books

- Pentesting Azure Applications

Tips and Tricks

- Replace COMPANYNAME with the company name of your choice to check if they use Azure. If the **NameSpaceType** indicates *"Managed"*, then the company is using Azure AD:

```
https://login.microsoftonline.com/getuserrealm.srf?login=username@COMPANYNAME.onmicrosoft
```