Azure Security
Penetration and Vulnerability Testing
Security As-Service

Prepared for:

Prepared by:
MDS Security Team

Maureen Data Systems

How MDS can help you achieve your security goals?

MDS have access to a pool of cybersecurity professionals that will provide you complete guidance and support so your organization can achieve the security goals.

Our resources are highly skilled and fully accredited in Microsoft Skill Certifications with full access to Microsoft engineering teams.

With almost 30 years of experience, we give you access to the security best practices and up-to-date guidance in an agile and flexible way.

Delivered, managed and governed by our elite team of cybersecurity and compliance experts, reducing risks and promoting frameworks compliant practices.

We provide the scalable solutions you need that benefit from economies of scale (OpEx) and shared resources.

It allows you to differentiate yourself and focus on your own business by harnessing the power of cloud technologies to drive innovation.

Agenda

- *Cloud Security – Azure Penetration Testing Solution*
- *Proposed Project Schedule Estimate*
- *Proposed Solution Estimated Cost*

Cloud Security – Azure Pen Testing

When creating an environment on Azure, the flexibility enablement provides organizations the ability to deploy without worrying about "racking and stacking". Still, it is necessary to perform security due diligence to secure those resources. The MDS Azure Pen testing will help your organization enhance the security of your infrastructure in the cloud providing visibility and awareness of the entire Azure ecosystem.

Our Methodology

MDS's Proven Pen testing Methodology

Scope Definition

- Rules of Engagement
- Set Objectives
- Scope Definition
- Set Timeline

Reconnaissance

- Open-Source Intelligence
- Deep Internet Scanning
- Enumeration

Vulnerability Assessment

- Vulnerability Scanning
- Manual Validation
- Analysis, Planning and Research
- Threat Modeling

Exploitation

- Automated Exploits
- Custom Exploits
- Privilege Escalation
- Lateral Movement

Reporting & Support

- Executive Report
- Technical Report
- CISO Review
- Stakeholders Meeting

Penetration Testing Frameworks & Methodologies

MDS ALIGNS THE FRAMEWORK BASED ON YOUR BUSINESS	**(NIST)** The National Institute of Standards and Technology	**(ISSAF)** Information System Security Assessment Framework
(OWASP) Open Web Application Security Project	**(PTES)** Penetration Testing Methodologies and Standards	**(OSSTMM)** Open-Source Security Testing Methodology Manual

Services within Scope

Security and Management


Azure Portal


Active Directory


Management Groups


Subscription


Automation


Key Vault

Hybrid Operations


AD Health


Identity Governance

Web and Mobile


Function App


API Apps


Web Apps

Compute


Virtual Machine


Containers

Storage


Blob Storage


Azure Files

Data

SQL Server


Cache Redis


Azure Cosmos DB

Networking


Virtual Network

DNS Zones


VPN Gateway


Express Route


Load Balancer


Firewall

Azure Penetration Testing Tools

MDS Sample Penetration Testing Tools

Reconnaissance

Intelligence work of obtaining information, either passively or actively.

Nmap

Spiderfoot

Stormspotter

Intrigue

CS Suite

Shodan

Vulnerability Assessment

I*dentifying systems that are running and the services active on them*.

Metasploit

Nessus

Invoke-Obfuscation

Veil

Gaining Access

Exploiting identifiable vulnerabilities to gain unauthorized access.

MicroBurst

Burp Suite

PowerUp

King Phisher

PowerZure

CrackMapExec

Mimikatz

Sample Report Findings

Vulnerability Instances: all and exploitable, by severity

VPR: all (exploitable)

13(10)	17(13)	104(12)
CRITICAL	HIGH	MEDIUM

CV88 v2.0: all (exploitable)

19(12)	29(10)	288(19)
CRITICAL	HIGH	MEDIUM

Top 10 Critical Vulnerabilities

The two tables in this chapter provide a top 10 vulnerabilities grouped using the critical VPR or critical CVSS. For VPR and CVSS v3.0 the rating is 9.0 - 10, for CVSS v2.0 the rating is 10. The vulnerabilities identified using VPR are the most active in the world, and based on in-depth threat analysis, are considered the most critical to mitigate. Traditionally, the method for identifying risk used most commonly with CVSS v3.0 or CVSS v2.0. While each still remains very important and should be mitigated, these vulnerabilities are not given the same context as VPR identified vulnerabilities.

Top 10 Critical Vulnerabilities: VPR

Top 10 most prevalent critical vulnerabilities

Plugin ID	Plugin Name	Plugin Family	VPR	Known Exploit?	Publication Date	Count
97833	MS17-Q10: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	Windows	8.8	Yes -	2017/03/14	3
143221	ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VNSA-2020-0026)	Misc.	9.2	-	2020/11/19	3

RS-NTC-002 PASSWORD REUSE

Critical Risk *Passwords*

Impact

If users of different access or privilege levels have the same password, an attacker who compromises the password of a lower-privilege user could reuse that password to access other higher privilege accounts with the same password. Red Siege identified users having the same password. It appears the password may be a default password set when provisioning new users.

Password set A: 16 accounts with the same leetspeak[3] version of the word "password"

- apowell
- arodgers
- hgmcclane
- hgruber
- jmcclane
- jnelson
- karl
- lbarnes
- marketing
- mbowman
- mfarrell
- nakatomi-svc-acct
- tgabriel
- wstuart
- ykomarov

Password set B: 3 accounts with the same password based on the word "password" followed by a number.

- bbulaga
- cmatthews
- rcobb

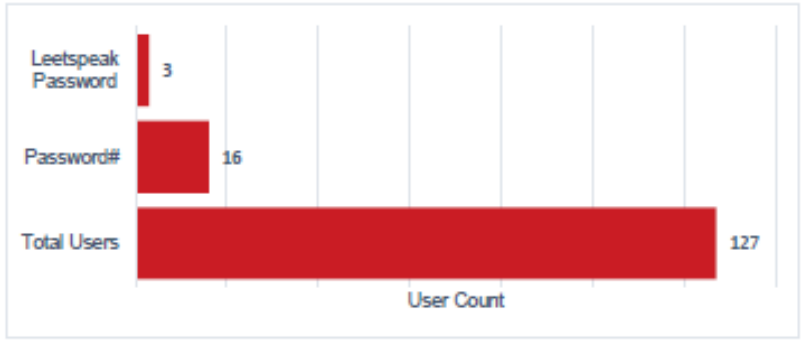

Figure 2. Number of Users with Bad Passwords

Azure Penetration and Vulnerability Assessment

- *In scope per Microsoft Azure Rules of Engagement*
  - Create several test accounts or tenants to demonstrate and test access and data transfer between accounts and tenants
  - Run port scans, fuzz testing or other vulnerability testing tools against your own Azure VMs
  - Test load on an application by generating traffic expected from a typical business process—including surge tests.
  - Tests that check security monitoring capabilities
  - Breaking out of an Azure service container like Azure Functions

Azure Penetration and Vulnerability Assessment

- *Out of Scope per Microsoft Azure Rules of Engagement*

The following acts are prohibited as part of a penetration test:

- Analyzing or testing assets of other Microsoft Cloud customers.
- Accessing or using any data that is not owned by your organization.
- Running denial of service (DoS) attacks, or any test that generates large amounts of traffic.
- Perform fuzz testing that may use extensive network bandwidth (except on your own VMs).
- Taking action after the proof of concept (POC) stage of the penetration test—for example, you can prove you have root access on a system, but not execute root commands.
- Violating any part of the Acceptable Use Policy.
- Performing phishing or other social engineering attacks against Microsoft employees.

Proposal Estimated Pricing

Activities	Price starts at:
Workstream 1: Penetration Testing and Vulnerability Testing	$12,000 -
*Price will be estimated based on the Azure ecosystem	
Total Estimate	**$12,000 -**

THANK YOU!

Maureen Data Systems