



FedRAMP Penetration Test Report

22 March 2018

Prepared By:



Kratos SecureInfo, Inc.
Bridge Pointe Corporate Centre
4820 Eastgate Mall
San Diego, CA 92121

Offered through its cybersecurity division:

Kratos SecureInfo, Inc.
14130 Sullyfield Circle, Suite H
Chantilly, VA 20151
888.677.9351

Executive Summary

Background

Microsoft retained Kratos SecureInfo to perform a Federal Risk and Authorization Management Program (FedRAMP) penetration test of the Azure system. The Azure penetration test is a representation of the security posture as of the end date of penetration testing, prior to any mitigation. This report provides the results of the activities performed and serves as a permanent record of the penetration testing activities. The effort was performed offsite remotely from the Kratos SecureInfo offices in Chantilly, VA, between 2 October 2017 and 8 December 2017. The testing included automated and manual activities using the penetration testing guidance found in the “FedRAMP Penetration Test Guidance, version 1.0.1” document.

Findings

The table below represents the total findings discovered as a part of the penetration testing activities. They are organized by severity, after mitigating factors. There were no **High**, no **Moderate**, and fourteen (14) **Low** findings identified during the penetration test. The table below summarizes the findings by impact level. Detailed information about the findings is in “Table 9 - Penetration Testing Findings”.

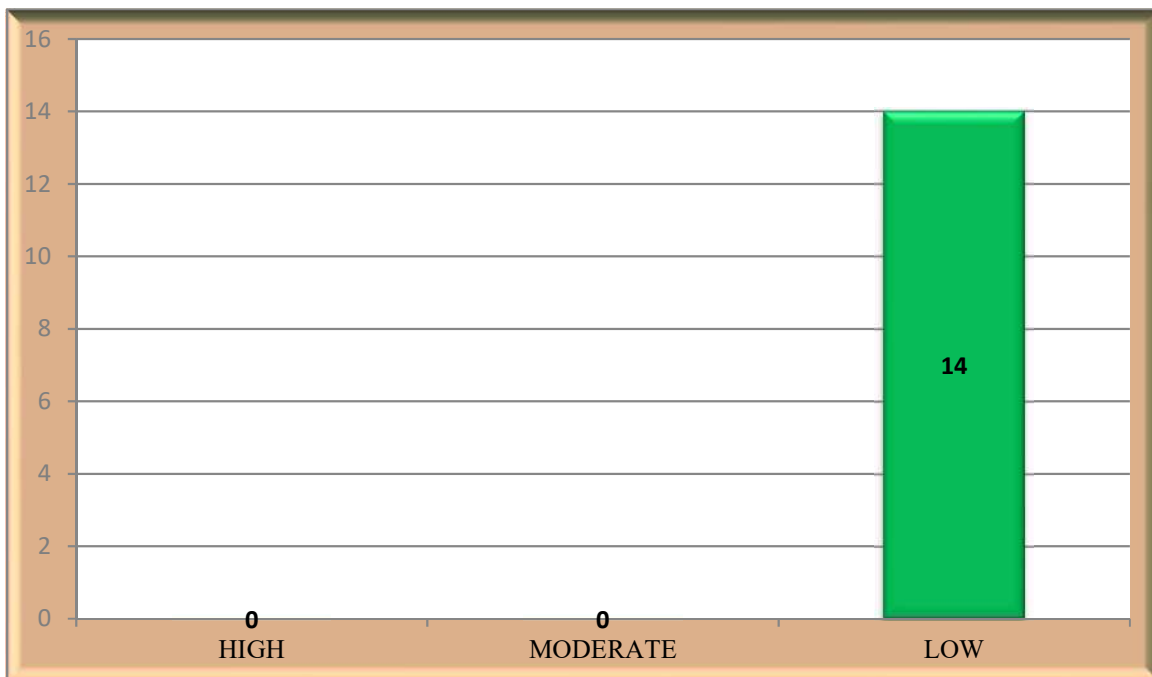


Table 1 – Penetration Test Findings by Impact Level

Document Revision History

Date	Page(s)	Description	Author
1/26/2018	All	Draft Deliverable to Microsoft	Kratos SecureInfo
22 March 2018	5.3.1, Appendix A	Final Deliverable to Microsoft Changes to final version: <ul style="list-style-type: none">• Following review of one finding, evidence of mitigations was presented. Vulnerability was removed.	Kratos SecureInfo

Table of Contents

EXECUTIVE SUMMARY	2
DOCUMENT REVISION HISTORY	3
TABLE OF CONTENTS	4
1. OVERVIEW	7
1.1. TIMELINE	9
1.2. SCOPE	9
1.3. ATTACK VECTORS	9
2. WEB APPLICATION	12
2.1. WEB APPLICATION OVERVIEW	12
2.2. WEB APPLICATION TESTING: <REDACTED>	12
2.2.1 Application Architecture	14
2.2.2 Accounts, Roles, and Authorization Bounds	14
2.2.3 Content and Functionality	14
2.2.4 User-Controlled Inputs	15
2.2.5 Server Configuration Checks	15
2.2.6 Web Application Microsoft Azure Exploitation	15
2.2.7 Web Application Microsoft Azure Post-Exploitation	38
3. NETWORK	39
3.1. NETWORK OVERVIEW	39
3.2. NETWORK DISCOVERY	39
3.2.1 Endpoint Enumeration	39
3.2.2 Service Enumeration	46
3.2.3 Operating System Fingerprinting	46
3.2.4 Vulnerability Identification	46
3.3. NETWORK EXPLOITATION	46
3.3.1 Test Case: Exploitation of Azure Boundary Service	47
3.3.2 Test Case: Credentialed Tenant Exploitation of a Secondary Tenant	47
3.3.3 Test Case: Target System to CSP Management System	48
3.4. NETWORK POST-EXPLOITATION	48
4. SOCIAL ENGINEERING	49
4.1. SOCIAL ENGINEERING OVERVIEW	49
4.2. SOCIAL ENGINEERING DISCOVERY	49
4.3. SOCIAL ENGINEERING EXPLOITATION	54
5. INTERNAL ATTACK	55
5.1. INTERNAL ATTACK OVERVIEW	55
5.2. INTERNAL ATTACK DISCOVERY	55
5.2.1 Scoping	55
5.3. INTERNAL ATTACK EXPLOITATION	56
5.3.1 Test Case: Escalation of Privileges on Workstation	56
6. PHYSICAL SECURITY	59

6.1. PHYSICAL SECURITY OVERVIEW	ERROR! BOOKMARK NOT DEFINED.
6.2. PHYSICAL SECURITY DISCOVERY.....	ERROR! BOOKMARK NOT DEFINED.
6.3. PHYSICAL SECURITY EXPLOITATION	ERROR! BOOKMARK NOT DEFINED.
6.3.1 Datacenter:<REDACTED>.....	Error! Bookmark not defined.
6.3.2 Datacenter: <REDACTED>.....	Error! Bookmark not defined.
6.3.3 Datacenter: <REDACTED>.....	Error! Bookmark not defined.
6.3.4 Datacenter: <REDACTED>.....	Error! Bookmark not defined.
6.3.5 Datacenter: <REDACTED>.....	Error! Bookmark not defined.
6.3.6 Datacenter: <REDACTED>.....	Error! Bookmark not defined.
6.3.7 Datacenter: <REDACTED>.....	Error! Bookmark not defined.
6.3.8 Datacenter: <REDACTED>.....	Error! Bookmark not defined.
6.3.9 Datacenter: <REDACTED>.....	Error! Bookmark not defined.
6.3.10 Datacenter: <REDACTED>.....	Error! Bookmark not defined.
6.3.11 Datacenter: <REDACTED>.....	Error! Bookmark not defined.
6.3.12 Datacenter: <REDACTED>.....	Error! Bookmark not defined.
6.3.13 Datacenter: <REDACTED>.....	Error! Bookmark not defined.
7. FINDINGS.....	59
7.1. FALSE POSITIVES	59
APPENDIX A - FINDINGS	65
APPENDIX B - EVIDENCE.....	65

Table of Figures

Figure 1-1: Azure Infrastructure.....	8
Figure 2-1: https://portal. <REDACTED>.us/.....	16
Figure 2-2: https:// <REDACTED>.portal.a<REDACTED>.com/	16
Figure 2-3 – Native Accounts Provided Paired with Designated Portals.....	16
Figure 2-4, Usernames designated for Web Application Testing	17
Figure 2-5 – Out of Scope Portal	18
Figure 2-6, https:// <REDACTED>.microsoftonline.us.....	18
Figure 2-7, https:// <REDACTED>.microsoftonline.com	19
Figure 4-1, Spear Phishing Results.....	54
Figure 6-1, <REDACTED> Aerial View	Error! Bookmark not defined.
Figure 6-2, <REDACTED> External Access Points.....	Error! Bookmark not defined.
Figure 6-3, <REDACTED> Aerial View	Error! Bookmark not defined.
Figure 6-4, <REDACTED> External Access Points.....	Error! Bookmark not defined.
Figure 6-5, <REDACTED> Aerial View	Error! Bookmark not defined.
Figure 6-6, <REDACTED> External Access Points.....	Error! Bookmark not defined.
Figure 6-7, <REDACTED> Aerial View	Error! Bookmark not defined.
Figure 6-8, <REDACTED> Main Entrance.....	Error! Bookmark not defined.
Figure 6-9, <REDACTED>External Access Points.....	Error! Bookmark not defined.
Figure 6-10, <REDACTED> External Access Points – Loading Dock	Error! Bookmark not defined.
Figure 6-11, <REDACTED> Aerial View	Error! Bookmark not defined.
Figure 6-12, <REDACTED> Main Entrance.....	Error! Bookmark not defined.
Figure 6-13, <REDACTED>SOC and Access Point.....	Error! Bookmark not defined.
Figure 6-14, <REDACTED> Aerial View	Error! Bookmark not defined.

Figure 6-15, <REDACTED>Main Entrance Access Point.....	Error! Bookmark not defined.
Figure 6-16, <REDACTED> Aerial View	Error! Bookmark not defined.
Figure 6-17, <REDACTED> Main Entrance	Error! Bookmark not defined.
Figure 6-18, <REDACTED> SOC and Access Point	Error! Bookmark not defined.
Figure 6-19, <REDACTED> Aerial View	Error! Bookmark not defined.
Figure 6-20, <REDACTED> Main Entrance	Error! Bookmark not defined.
Figure 6-21, <REDACTED> Aerial View	Error! Bookmark not defined.
Figure 6-22, <REDACTED> Main Entrance	Error! Bookmark not defined.
Figure 6-23, <REDACTED> Aerial View	Error! Bookmark not defined.
Figure 6-24, <REDACTED> Administration Building, Main Entrance	Error! Bookmark not defined.
Figure 6-25, <REDACTED> External Access Points.....	Error! Bookmark not defined.
Figure 6-26, <REDACTED> Aerial View	Error! Bookmark not defined.
Figure 6-27, <REDACTED> Administration Building, Main Entrance	Error! Bookmark not defined.
Figure 6-28, <REDACTED> External Access Points.....	Error! Bookmark not defined.
Figure 6-29, <REDACTED> Aerial View	Error! Bookmark not defined.
Figure 6-30, <REDACTED> Administration Building, Main Entrance	Error! Bookmark not defined.
Figure 6-31, <REDACTED> External Access Points.....	Error! Bookmark not defined.
Figure 6-32, <REDACTED> Aerial View	Error! Bookmark not defined.
Figure 6-33, <REDACTED>Administration Building, Main Entrance.....	Error! Bookmark not defined.
Figure 6-34, <REDACTED> External Access Points.....	Error! Bookmark not defined.

Table of Tables

Table 1 – Penetration Test Findings by Impact Level	2
Table 2 – FedRAMP Attack Vector Matrix	10
Table 3 - Microsoft Azure Account Roles	14
Table 4 - Azure Externally Accessible Hosts	46
Table 5 - Publicly Available Information about Azure	50
Table 6 - Publicly Available Information on Azure Personnel.....	53
Table 7 - Potential Simulated Internal Attack Vectors	55
Table 8 - Physical Penetration Testing Location Information.....	Error! Bookmark not defined.
Table 9 - <REDACTED>.....	Error! Bookmark not defined.
Table 10 - <REDACTED>.....	Error! Bookmark not defined.
Table 11 - <REDACTED>.....	Error! Bookmark not defined.
Table 12 - <REDACTED>.....	Error! Bookmark not defined.
Table 13 - <REDACTED>.....	Error! Bookmark not defined.
Table 14 - <REDACTED>.....	Error! Bookmark not defined.
Table 15 - <REDACTED>.....	Error! Bookmark not defined.
Table 16 - <REDACTED>.....	Error! Bookmark not defined.
Table 17 - <REDACTED>.....	Error! Bookmark not defined.
Table 18 - <REDACTED>.....	Error! Bookmark not defined.
Table 19 - <REDACTED>.....	Error! Bookmark not defined.
Table 20 - <REDACTED>.....	Error! Bookmark not defined.
Table 21 - <REDACTED>.....	Error! Bookmark not defined.
Table 22 - Penetration Testing Results - False Positives.....	64
Table 23 - Penetration Testing Findings	65
Table 24 - Penetration Testing Evidence and Artifacts	78

1. OVERVIEW

Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for Cloud Service Providers (CSP). Testing FedRAMP mandated security controls, specifically through penetration tests, is an integral part of the FedRAMP process. Penetration tests are mandated by the FedRAMP for initial accreditation or to maintain certification under continuous monitoring. Microsoft retained Kratos SecureInfo, an accredited FedRAMP independent third-party assessment organization (3PAO), to perform penetration testing of the Azure system using current FedRAMP penetration testing guidance. Kratos SecureInfo conducted a proactive and authorized FedRAMP penetration test to validate FedRAMP security controls implemented on Azure. The primary goal for the FedRAMP penetration test includes:

- ✓ Gaining access to sensitive information
- ✓ Circumventing access controls and privilege escalation
- ✓ Exploiting vulnerabilities to gain access to systems or information
- ✓ Confirming that remediated items are no longer a risk.

Azure is categorized as a FedRAMP Infrastructure as a Service (IaaS) / Platform as a Service (PaaS) Cloud Service Model and is offered by Microsoft to quickly build, test, deploy, and manage their applications, services, and product development across a network of Microsoft-managed datacenters within the United States. The Microsoft Azure platform exports savings to the customer by delivering the software, platform, and information technology (IT) infrastructure resources where and when it is needed via the Internet.

The following Azure architecture diagram provides a visual depiction of the system network components that constitute the portions undergoing the FedRAMP penetration test.

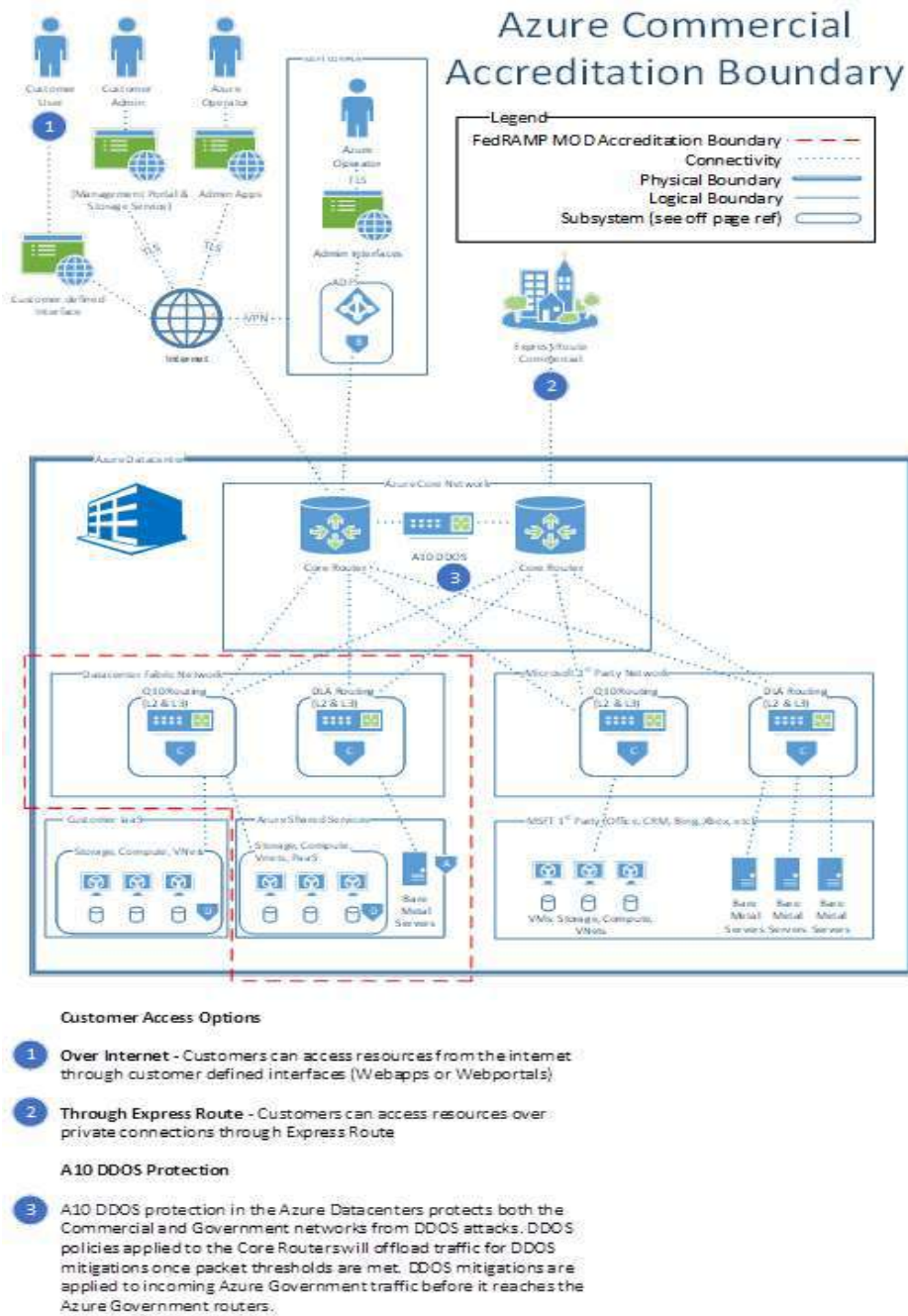


Figure 1-1: Azure Infrastructure

During the penetration test, Kratos SecureInfo identified exploitable security weaknesses of Azure including cloud service and application flaws, improper configurations, and end-user behavior to evaluate Microsoft’s security policy compliance, employees’ security awareness, and the organization’s ability to identify and respond to security

incidents. Findings were then validated, documented, and given an appropriate risk rating which can be found in the “Table 9 - Penetration Testing Findings”.

1.1. Timeline

For test vectors that required internal Azure system access, the testing was performed using an <REDACTED> laptop issued by the Azure team to the Kratos SecureInfo penetration testing team. For these vectors’ penetration testing efforts, testing was accomplished using a Microsoft-issued account and smart-card, in addition to a Microsoft-authorized/authenticated virtual private network (VPN) connection from the Kratos SecureInfo offices site.

Testing was accomplished remotely from the Kratos SecureInfo Chantilly, VA offices between 2 October 2017 and 8 December 2017.

1.2. Scope

The scope for penetration testing included the agreed upon FedRAMP attack vectors listed in Table 2 below, and authorized in the signed and approved Rules of Engagement (RoE) submitted as part of the Security Assessment Plan (SAP) for the Azure IaaS / PaaS offering. In-scope resources tested include, but were not limited to the Network infrastructure, internet facing and internal services such as web applications, social engineering efforts directed at designated corporate employees, hosts, and datacenter physical security.

During the engagement, Kratos SecureInfo did not perform any tests that would knowingly result in a denial of service (DoS) to operations, networks, servers, or telephone systems. Additional detail can be found in the Azure penetration test RoE.

1.3. Attack Vectors

Based on threat modeling, FedRAMP has defined six (6) attack vectors, in addition to a physical penetration test. The attack vectors are potential avenues of compromise that signal a degradation of system integrity, confidentiality, or availability. For the Azure penetration test, Kratos SecureInfo mapped each FedRAMP attack vector to affected technology sections based on threat perspectives, as shown in Table 2. Visually, Table 2 identifies if a particular FedRAMP attack vector is applicable for Azure, and if so, further lists the technology sections tested. For each technology section tested, a test case was created for the Azure penetration test. Using this method, both Microsoft and Kratos SecureInfo explored potential vulnerabilities, threats, and mitigation strategies.

Attack Vector	Description	Applicable?	Technology Sections Tested by Attack Vector
EXTERNAL TO CORPORATE	External Untrusted to Internal Untrusted. An internet-based attack attempting to gain useful information about or access the target cloud system through an external corporate network owned and operated by the CSP.	Yes	<input type="checkbox"/> Web Application <input type="checkbox"/> Mobile Application <input type="checkbox"/> Network <input checked="" type="checkbox"/> Social Engineering <input type="checkbox"/> Internal Attack
EXTERNAL TO TARGET SYSTEM	External Untrusted to External Trusted. An internet-based attack as an un-credentialed third party attempting to gain unauthorized access to the target system.	Yes	<input checked="" type="checkbox"/> Web Application <input type="checkbox"/> Mobile Application <input checked="" type="checkbox"/> Network <input type="checkbox"/> Social Engineering <input type="checkbox"/> Internal Attack
TARGET SYSTEM TO CSP MANAGEMENT SYSTEM	External Trusted to Internal Trusted. An external attack as a credentialed system user attempting to access the CSP management system or infrastructure.	Yes	<input checked="" type="checkbox"/> Web Application <input type="checkbox"/> Mobile Application <input type="checkbox"/> Network <input type="checkbox"/> Social Engineering <input type="checkbox"/> Internal Attack
TENANT TO TENANT	External Trusted to External Trusted. An external attack as a credentialed system user, originating from a tenant environment instance, attempting to access or compromise a secondary tenant instance within the target system.	Yes	<input checked="" type="checkbox"/> Web Application <input type="checkbox"/> Mobile Application <input type="checkbox"/> Network <input type="checkbox"/> Social Engineering <input type="checkbox"/> Internal Attack
CORPORATE TO CSP MANAGEMENT SYSTEM	Internal Untrusted to Internal Trusted. An internal attack attempting to access the target management system from a system with an identified or simulated security weakness on the CSP corporate network that mimics a malicious device.	Yes	<input type="checkbox"/> Web Application <input type="checkbox"/> Mobile Application <input type="checkbox"/> Network <input type="checkbox"/> Social Engineering <input checked="" type="checkbox"/> Internal Attack
MOBILE APPLICATION	External Untrusted to External Trusted. An attack that emulates a mobile application user attempting to access the CSP target system or the CSP's target system's mobile application.	No*	<input type="checkbox"/> Web Application <input checked="" type="checkbox"/> Mobile Application <input type="checkbox"/> Network <input type="checkbox"/> Social Engineering <input type="checkbox"/> Internal Attack
PHYSICAL PENETRATION TESTING	External Untrusted to Internal Trusted. Ensure Datacenter security doors are locked, security alarms work, and security guards are present and alert as required by the CSP organization's security policies and procedures.	Yes**	<input checked="" type="checkbox"/> Internal Untrusted Attack <input checked="" type="checkbox"/> External Untrusted Attack <input checked="" type="checkbox"/> CSP Data Centers

Table 2 – FedRAMP Attack Vector Matrix

* Kratos SecureInfo, in collaboration with Microsoft, determined that the mobile application FedRAMP attack vector is not applicable. As per the Azure System Security Plan (SSP), Azure does not provide in-scope mobile services; therefore, this vector is not applicable.

** Kratos SecureInfo, in collaboration with Microsoft, determined that the physical penetration testing is applicable due to being classified as an IaaS and Microsoft being responsible for the security controls impacting the physical environment of Azure. Physical security penetration tests will attempt to simulate an attack by an external untrusted individual, including any rogue, untrusted Microsoft employee, against each datacenter processing Azure data.

2. WEB APPLICATION

2.1. Web Application Overview

The FedRAMP penetration test of Azure included both internal (from the Microsoft corporate network) and Internet-based attacks, attempting to gain unauthorized access to Azure web applications and the underlying Application Program Interface (API). Specifically, three (3) test cases cover at a minimum:

- ✓ A simulated internet attack by an external un-credentialed entity (e.g., public) against Azure web application(s).
- ✓ A simulated internet attack by an external credentialed entity (e.g., customer) against the Azure management infrastructure.
- ✓ A simulated internet attack by an external credentialed entity (e.g., customer #1) on a primary tenant against a secondary tenant (e.g. customer #2).

2.2. Web Application Testing: <REDACTED>

Microsoft's Azure suite consists of multiple services that include web applications. A breakdown of the sites is below:

- <REDACTED>.azure.net
- <REDACTED>.core.windows.net
- <REDACTED>. <REDACTED>.core.windows.net
- <REDACTED>. <REDACTED>. <REDACTED>.core.windows.net
- portal. <REDACTED>.com
- <REDACTED>.core.windows.net.
- <REDACTED>-beta. <REDACTED>.core.windows.net (site was determined to be no different than the non-beta site)
- <REDACTED>. <REDACTED>.core.windows.net
- portal. <REDACTED>.com
- <REDACTED>. <REDACTED>. <REDACTED>.core.windows.net
- <REDACTED>. <REDACTED>.windows.net
- <REDACTED>. <REDACTED>.msft.net
- <REDACTED>-<REDACTED>. <REDACTED>.core.windows.net
- <REDACTED>.windows.net
- <REDACTED>. <REDACTED>. <REDACTED>.core.windows.net
- <REDACTED><REDACTED>-<REDACTED>. <REDACTED>.core.windows.net/<REDACTED>/
- <REDACTED>. <REDACTED>-<REDACTED>. <REDACTED>.core.windows.net/<REDACTED>/
- <REDACTED>. <REDACTED>-<REDACTED>. <REDACTED>.core.windows.net
- <REDACTED>. <REDACTED>-<REDACTED>. <REDACTED>.core.windows.net.
- <REDACTED>-<REDACTED>. <REDACTED>.windowsazure.com
- <REDACTED>. <REDACTED>.windowsazure.com
- <REDACTED>.cloudapp.net
- <REDACTED>. <REDACTED>. <REDACTED>.core.windows.net
- <REDACTED>.microsoftonline.com
- <REDACTED>.microsoftonline.com
- <REDACTED>. <REDACTED>.core.windows.net
- <REDACTED>.cloudapp.net

2.2.4 User-Controlled Inputs

User-controlled input entries on the web application were identified by reviewing application mappings and identifying the dynamic/static URLs containing sections for parameter input. User-controlled input along with the content was used to identify fuzz test points and leverage attacks against Microsoft Azure. A full listing of the web application user-controlled inputs is included in “Table 10 - Penetration Testing Evidence and Artifacts”.

2.2.5 Server Configuration Checks

The Burp Suite tool was used to identify each parameter and subsequently harvest potential vulnerabilities. Penetration tests involved automated injection of bad parameters checking for logic errors, SQL injection, etc. Detailed information about the findings is in “Table 9 - Penetration Testing Findings” and raw scan data is provided in “Table 10 - Penetration Testing Evidence and Artifacts”.

2.2.6 Web Application Microsoft Azure Exploitation

2.2.6.1. Un-credentialed exploitation of Microsoft Azure

No vulnerabilities were discovered using un-credentialed access to the Microsoft Azure web applications. No access to pages or content is available, other than the login page, without conducting authentication.

2.2.6.2. Authentication and Session Management

The Microsoft Azure system uses a username/password for its web applications. Microsoft internal domain accounts also utilize a smartcard. Either authentication method combination creates a session token along with a session cookie. The session token is used by the application to maintain an authenticated session. Sample representative screenshots of the authentication portals that were in scope are identified below. The same portal was used for both Azure and Azure Government for each account/role. Once authenticated, the user is redirected to the appropriate environment.

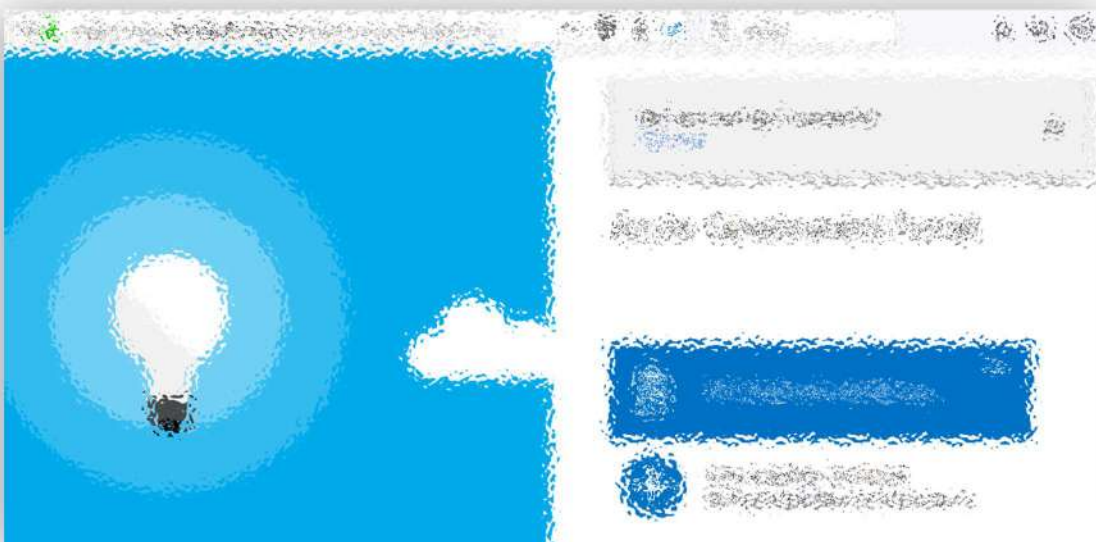


Figure 2-1: <https://<REDACTED>.azure.us/>



Figure 2-2: <https://ms.<REDACTED>.azure.com/>

Testing for this assessment was accomplished using six (6) native accounts (shown below) for login based around the two (2) portals listed above:



Figure 2-3 – Native Accounts Provided Paired with Designated Portals



Figure 2-4, Usernames designated for Web Application Testing

Many in-scope hosts redirected the testing team to an out-of-scope web page/authentication portal. Kratos verified with Microsoft that this portal is a landing page for any web application that requires authentication. The penetration testing team investigated the out of scope portal and determined that using the domain account issued to the penetration test team (<REDACTED>@microsoft.com) would enable an authenticated session to redirect back to the URL that was initially requested for testing. The penetration test team used this domain account to test the URLs required for the web application penetration test. Both <REDACTED>.microsoftonline.us and <REDACTED>.microsoftonline.com use OAuth to authorize access. The native microsoft accounts were used to verify and test proper implementation. Test results from these in-scope web applications and URLs can be found in their appropriate sections of this report. No vulnerabilities were noted during the testing of the implementation of OAuth.

While the targeted web applications were in-scope and tested, this portal/landing page was confirmed by Microsoft to be out of scope and was not listed in the ROE. Therefore, no further testing was conducted on these authentication pages. Additionally, in-scope web applications that redirected to this landing page were not accessible without the Microsoft-provided laptop, Microsoft-provisioned credentials, and multi-factor authentication via Microsoft-issued smart card, further mitigating risk associated with these out-of-scope pages.



Figure 2-5 – Out of Scope Portal



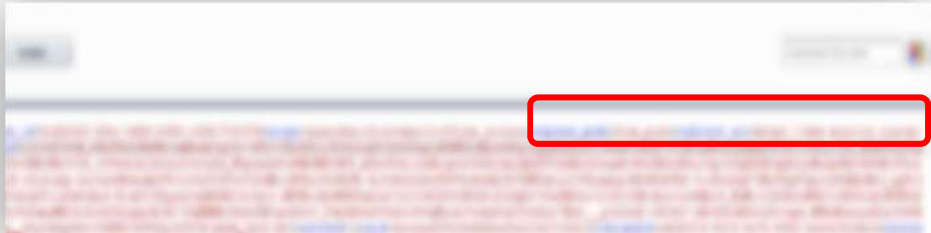

Figure 2-6, <https://<REDACTED>.microsoftonline.us>

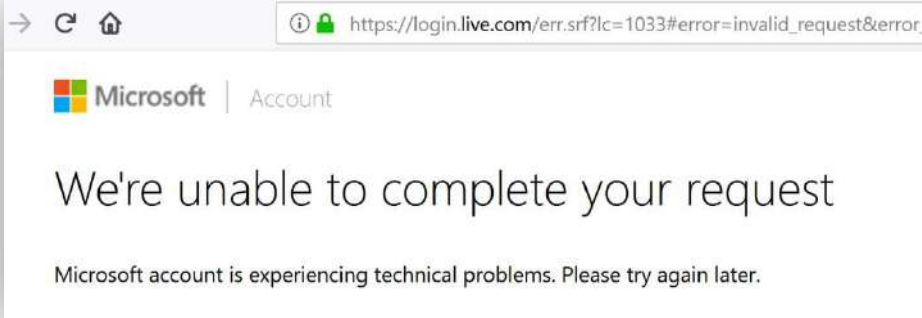


Figure 2-7, <https://<REDACTED>.microsoftonline.com>

2.2.6.2.1. Test Case: OAuth2 – Open Relay Test


Attack Vector: External to Target System - External Untrusted to External Trusted

Test Objective	OAuth2 attack: “redirect_uri” Open relay
Primary Target(s):	<REDACTED>.microsoftonline.us, <REDACTED>.microsoftonline.com
Secondary Target(s):	Azure
Severity of Findings:	None
Evidence:	<p>Manipulation of the redirect_uri parameter using both <REDACTED>.microsoftonline.com and external target URLs, all resulted in error messages.</p> <p>Example test: injecting <a href="http://www.<REDACTED>.org">www.<REDACTED>.org as the redirect_uri</p>  <p>The response:</p> 

	 <p>Reference: <a href="https://<REDACTED>.com/blogs/Attacking-the_OAuth-Protocol">https://<REDACTED>.com/blogs/Attacking-the_OAuth-Protocol</p>
--	--


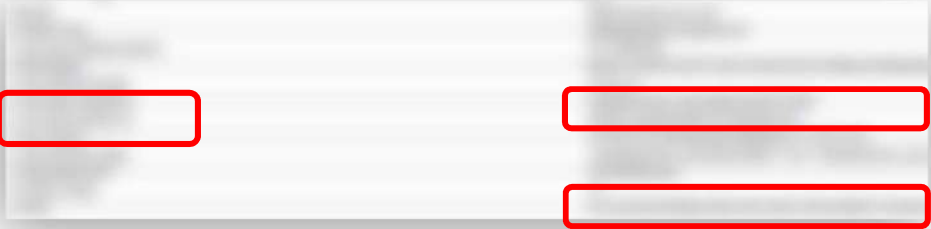
2.2.6.2.2. Test Case: OAuth2 – Cross-site Request Forgery (CSRF) Attack on Authorization Response

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	OAuth attack: CSRF on the Authorization Response
Primary Target(s):	<REDACTED>.microsoftonline.us, <REDACTED>.microsoftonline.com
Secondary Target(s):	Azure
Severity of Findings:	None
Evidence:	<p>CSRF on the authorization response is mitigated with the “state” parameter passed in the 2nd and 3rd steps of the OAuth exchange. An attacker cannot forge a malicious (CSRF) URL without knowing the ‘state’ which is session specific.</p>  <p>Reference: <a href="https://<REDACTED>.com/blogs/Attacking-the_OAuth-Protocol">https:// <REDACTED>.com/blogs/Attacking-the_OAuth-Protocol</p>


2.2.6.2.3. Test Case: Token Randomness/Complexity

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Token Complexity: Randomness
Primary Target(s):	<REDACTED>.microsoftonline.us, <REDACTED>.microsoftonline.com
Secondary Target(s):	Azure
Severity of Findings:	None
Evidence:	<p>The test team created numerous “id-tokens” by creating new sessions within the Azure Portals.</p> <p>Observation 1: Each creation results in a new, entirely different token/session ID Observation 2: Different browsers each had different browser IDs Observation 3: The length of each of token/session ID was found complex enough that a brute force attempt was mathematically unfeasible.</p> <p>“client-session-id tokens” generated for an account were drastically different every time the account was signed in. Too few keys were (manually) created to conduct a meaningful statistical analysis of the distribution of keys. The token/session ID successfully bind the user’s credentials to the traffic, the browser, and the appropriate access controls given by the web application.</p>  

2.2.6.2.4. Test Case: Token Creation

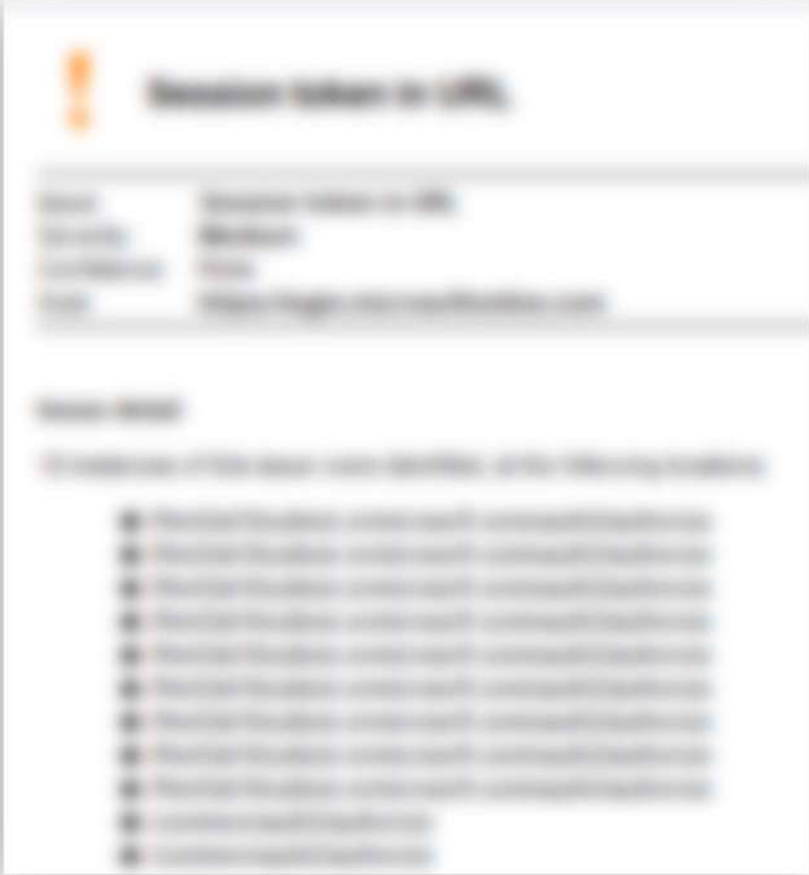
Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Token Security: Token Creation
Primary Target(s):	<REDACTED>.microsoftonline.us, <REDACTED>.microsoftonline.com
Secondary Target(s):	Azure
Severity of Findings:	None
Evidence:	<p>The “client-session-id” token was tested against known hash types to determine if the token is created from an associated string. Both MD5 hash crackers and brute force guessing tools failed to confirm that the token is based on a known, potentially predictable value.</p> <p>Several tools were used to try and reverse engineer the associated value. The password cracker “<REDACTED>” was used to check the token against known plaintext (variations of the account username associated with the hash).</p> <p>The hash was also passed to databases as a suspected MD5 to try and identify any pre-computed known values as shown below:</p> 

2.2.6.2.5. False Positive – Session Token in URL

Attack Vector: **External to Target System - External Untrusted to External Trusted**

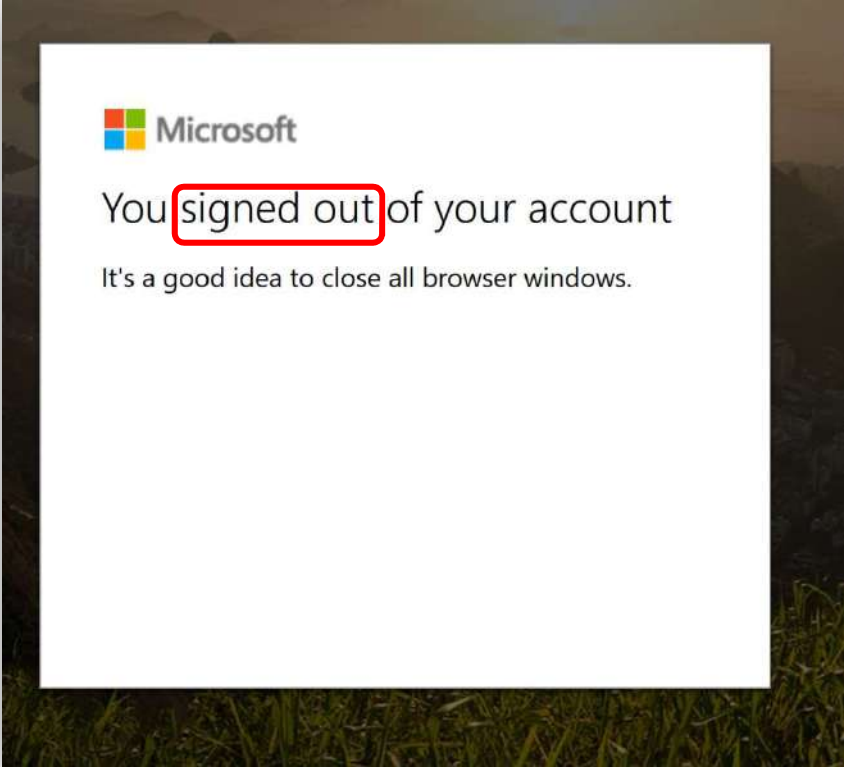
Test Case	Session Token in URL Verification
-----------	-----------------------------------

Primary Target(s):	<REDACTED>.microsoftonline.us, <REDACTED>.microsoftonline.com
Secondary Target(s):	Azure
Severity of Findings:	False Positive
Evidence:	<p>Burp Scanner identified 18 instances of session tokens being placed within the URL being passed. After inspection, these results were determined to be false positives and pose no risk to session security.</p> 

2.2.6.2.6. Test Case – Log Out

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Case	Session Expiration
Primary Target(s):	<REDACTED>.microsoftonline.us, <REDACTED>.microsoftonline.com
Secondary Target(s):	Azure
Severity of Findings:	None

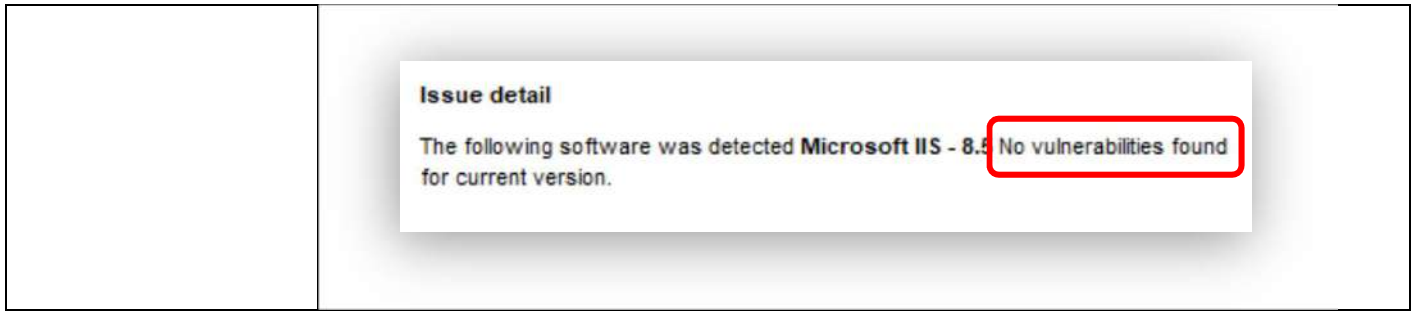
<p>Evidence:</p>	<p>Session is torn down after “log out” action. The browser “back” button does not result in a re-establishment or continuation of the authenticated session, instead it redirects to the login page. The previous tokens no longer work to re-create a session.</p> 
------------------	--

2.2.6.3. Authorization

2.2.6.3.1. Test Case – Software with Known Vulnerabilities

Attack Vector: External to Target System - External Untrusted to External Trusted

Test Objective	Software with Known Vulnerabilities
Primary Target(s):	<REDACTED>.microsoftonline.us, <REDACTED>.microsoftonline.com
Secondary Target(s):	Azure
Severity of Findings:	None
Evidence:	The implemented software, such as Microsoft IIS, Microsoft ASP.Net, and Microsoft Server version and patches are all up to date and no vulnerabilities were found.



2.2.6.3.2. Test Case: Outdated JQuery Software

Attack Vector: External to Target System - External Untrusted to External Trusted

Test Objective	Outdated JQuery Software
Primary Target(s):	<REDACTED>. <REDACTED>.windowsazure.com
Secondary Target(s):	Azure
Severity of Findings:	Low
Evidence:	The jQuery library included on the webserver is Version 1.7.2, which was released in 2012. Several newer versions have been released since then, with one Common Vulnerabilities and Exposures (CVE) related to this older version, i.e., <REDACTED>. This finding was discovered through manual analysis of the web application. The newest version is <REDACTED>. This vulnerability is outlined in PT-2017-1 of Appendix A.

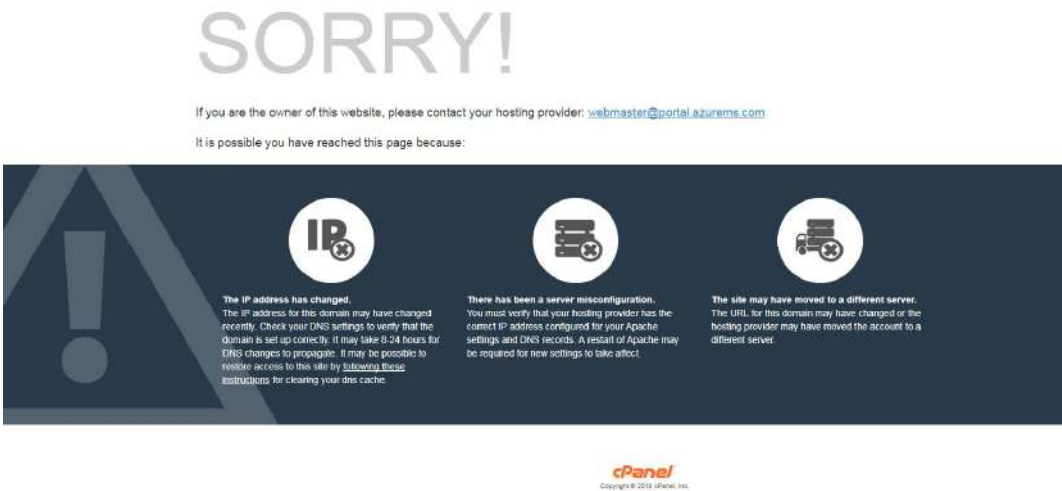
2.2.6.3.3. Test Case: Outdated Bundled JS Libraries

Attack Vector: External to Target System - External Untrusted to External Trusted

Test Objective	Outdated Bundled JS Libraries
Primary Target(s):	<REDACTED>.com
Secondary Target(s):	<REDACTED>
Severity of Findings:	Low
Evidence:	The following JavaScript libraries are included on the server which are all out of date. <REDACTED><REDACTED><REDACTED><REDACTED><REDACTED> <REDACTED><REDACTED><REDACTED><REDACTED> The newest versions are: <REDACTED><REDACTED><REDACTED><REDACTED><REDACTED><REDACTED> <REDACTED>jquery cookie plugin abandonware, now <REDACTED> <REDACTED><REDACTED> Only one CVE is related to these files, i.e., <REDACTED> (moment.js). This vulnerability was discovered through manual analysis of the web application. This vulnerability is outlined in PT-2017-2 of Appendix A.

2.2.6.3.4. Test Case: Unhandled Exception – Runtime Error

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Unhandled Exception – Runtime Error
Primary Target(s):	Portal. <REDACTED>.com
Secondary Target(s):	Azure
Severity of Findings:	Low
Evidence:	<p>When using provided login accounts, site gives an application error with the IIS default error page. This type of error is intended for debugging by developers and should be replaced by a custom and generic "error" page that is displayed to users, and that does not reveal the underlying technology.</p>  <p>This vulnerability was discovered through manual analysis of the web application. This vulnerability is outlined in PT-2017-3 of Appendix A.</p>

2.2.6.3.5. Test Case: Default <REDACTED>. <REDACTED> Errors Enabled

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Default <REDACTED>. <REDACTED> Errors Enabled
Primary Target(s):	<REDACTED>. <REDACTED>.windows.net
Secondary Target(s):	Azure
Severity of Findings:	Low
Evidence:	<p>The server is configured to display default <REDACTED>. <REDACTED> errors which are intended for debugging purposed and are used by developers. General users should be provided a generic, custom "Error" page so as not to divulge information about the technology implemented on the server. This vulnerability was discovered during manual</p>

	analysis of the web application. This vulnerability is outlined in PT-2017-6 of Appendix A.
--	---

2.2.6.3.6. HTTP Connections to Untrusted Third-Party Providers

Attack Vector: External to Target System - External Untrusted to External Trusted

Test Objective	HTTP Connections to Untrusted Third-Party Providers
Primary Target(s):	<REDACTED>.microsoft.com
Secondary Target(s):	Azure
Severity of Findings:	Low
Evidence:	<p>The third-party provider is not undergoing FedRAMP certification and security posture cannot be determined. Compromise of the provider's website could be leveraged to attack the browsers of government clients logged into portal.azure.us by hosting malicious code.</p> <p>Example Sites: <REDACTED>.log. <REDACTED>.com <REDACTED>. <REDACTED>.com <REDACTED>. <REDACTED>.net --- incorporated in UK ("LTD") <a href="http://www.<REDACTED>.com">www. <REDACTED>.com</p> <p>This vulnerability was discovered through manual analysis of the web application</p> <p>This vulnerability is outlined in PT-2017-7 of Appendix A.</p>

2.2.6.3.7. Unhandled Exception – Internal Server Error

Attack Vector: External to Target System - External Untrusted to External Trusted

Test Objective	Unhandled Exception – Internal Server Error
Primary Target(s):	<REDACTED>. <REDACTED>.windowsazure.com Main. <REDACTED>. <REDACTED>.azure.us main. <REDACTED>. <REDACTED>. <REDACTED>.azure.us
Secondary Target(s):	Azure
Severity of Findings:	Low
Evidence:	<p>The server responds with a code 500 Internal Server Error when subjected to unexpected input. This can be indicative of poor programming practices, which could entice an adversary with time and technical experience to search for more severe vulnerabilities. This vulnerability was discovered through manual analysis of the web application.</p> <p>This vulnerability is further outlined in PT-2017-8 of Appendix A.</p>

	<p>This vulnerability was discovered by <REDACTED> Web Application Scanner.</p> <p>This vulnerability is outlined in PT-2017-4 of Appendix A.</p>
--	---

2.2.6.3.10. Test Case: Default Errors Enabled

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Default Errors Enabled
Primary Target(s):	<REDACTED>. <REDACTED>. <REDACTED>. <REDACTED>.azure.us
Secondary Target(s):	Azure
Severity of Findings:	Low
Evidence:	<p>Portal. <REDACTED>.us forces the user's browser to make requests to <REDACTED>. <REDACTED>. <REDACTED>. <REDACTED>.azure.us as part of the normal HTTP interaction involving groups and users. A bad request results in a "400 Bad Request" error; however, it also provides what appears to be an application stack trace in the response packet. This data is intended for debugging by developers and should be replaced by a default "Error" message to provide to users.</p> <p>This vulnerability was discovered through manual analysis of the web application.</p> <p>This vulnerability is outlined in PT-2017-10 of Appendix A.</p>

2.2.6.3.11. Test Case: Cookie Without HTTPOnly Flag Set

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Cookie Without HTTPOnly Flag Set
Primary Target(s):	<p>https:// <REDACTED>. <REDACTED>.windows.net</p> <p>https:// <REDACTED>.microsoftonline.com</p> <p>https:// <REDACTED>. <REDACTED>. <REDACTED>.core.windows.net</p> <p>https:// <REDACTED>. <REDACTED>. <REDACTED>.core.windows.net</p> <p>https:// <REDACTED>windows.net</p>
Secondary Target(s):	Azure
Severity of Findings:	Low
Evidence:	<p>If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This vulnerability was discovered using <REDACTED> Web Application Scanner.</p> <p>This vulnerability is outlined in PT-2017-12 of Appendix A.</p>

2.2.6.3.12. Test Case: Content Type Incorrectly Stated

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Content Type Incorrectly Stated
Primary Target(s):	https:// <REDACTED>. <REDACTED>.msft.net
Secondary Target(s):	Azure
Severity of Findings:	Low
Evidence:	<p>If a response specifies an incorrect content type, then browsers may process the response in unexpected ways. If the content type is specified to be a render-able text-based format, then the browser will usually attempt to interpret the response as being in that format, regardless of the actual contents of the response. Additionally, some other specified content types might sometimes be interpreted as HTML due to quirks in particular browsers. This behavior might lead to otherwise "safe" content such as images being rendered as HTML, enabling cross-site scripting attacks in certain conditions.</p> <p>This vulnerability was discovered using <REDACTED> Web Application Scanner.</p> <p>This vulnerability is outlined in PT-2017-13 of Appendix A.</p>

2.2.6.3.13. Test Case: Cacheable HTTPS Response

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Cacheable HTTPS Response
Primary Target(s):	https:// <REDACTED>.microsoftonline.com
Secondary Target(s):	Azure
Severity of Findings:	Low
Evidence:	<p>Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time. This vulnerability was discovered using BurpSuite Web Application Scanner.</p> <p>This vulnerability is outlined in PT-2017-14 of Appendix A.</p>

2.2.6.3.14. Test Case: Software Version Numbers Information Disclosure


Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Software Version Numbers Information Disclosure
Primary Target(s):	<REDACTED>. <REDACTED>. <REDACTED>.core.windows.net portal. <REDACTED>.com <REDACTED>. <REDACTED>.windows.net
Secondary Target(s):	Azure
Severity of Findings:	Low

Evidence:	<p>The HTTP response from the application reveals <REDACTED> and <REDACTED>. <REDACTED> version numbers.</p> <p>This vulnerability was discovered using <REDACTED>Web Application Scanner</p> <p>This vulnerability is outlined in PT-2017-11 of Appendix A.</p>
-----------	--

2.2.6.3.15. Test Case – Directory Traversal/File Include

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Case	Software with Known Vulnerabilities
Primary Target(s):	<REDACTED>.microsoftonline.us, <REDACTED>microsoftonline.com
Secondary Target(s):	Azure
Severity of Findings:	None
Evidence:	<p>The testing of the privileges and Access Control Lists by testing Input Vector Enumeration and Automated Directory Traversal and File Include Tools.</p> <div style="text-align: center;">  </div> <div style="text-align: center; margin-top: 20px;"> <pre>----- END_TIME: Thu Oct 26 16:48:09 2017 DOWNLOADED: 4612 - FOUND: 0</pre> </div> <p>References: See <REDACTED> and <REDACTED> Artifacts ~</p>

2.2.6.4. Application Logic

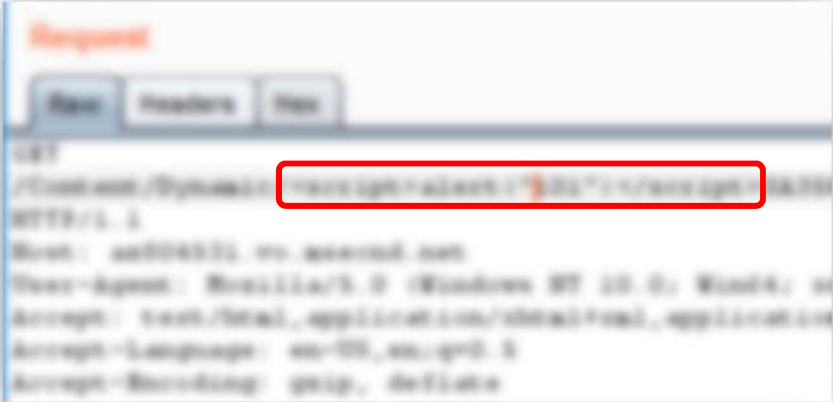

The Microsoft Azure logic patterns and application flows were tested in an attempt to circumvent security controls. No vulnerabilities were noted in this category.

2.2.6.5. Input Validation

Using data gathered previously in the user-controlled Inputs section, customized manual injection attacks were conducted against select input points of Microsoft Azure. In addition, significant amounts of automated spiders and scans were conducted validating input validation security.

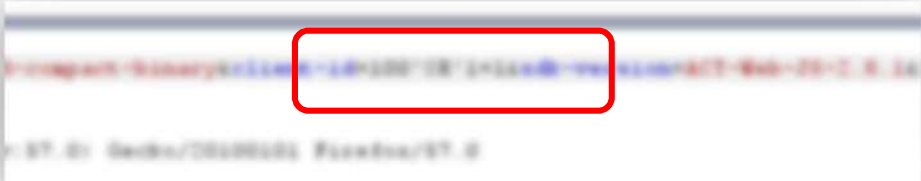
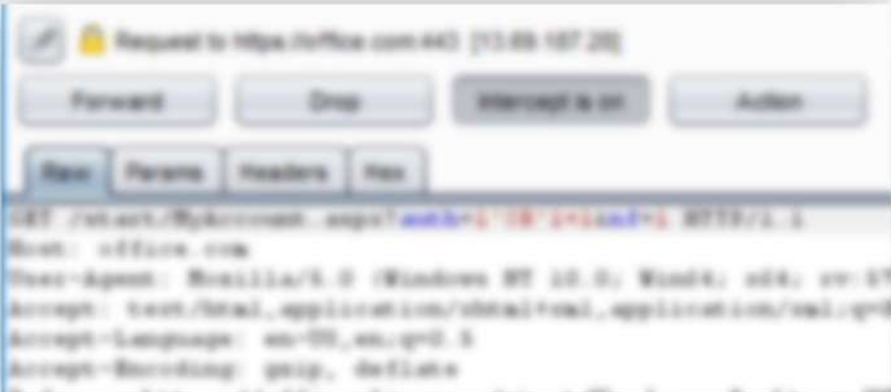
2.2.6.5.1. Test Case: Input Validation using <REDACTED> Techniques in Input Fields

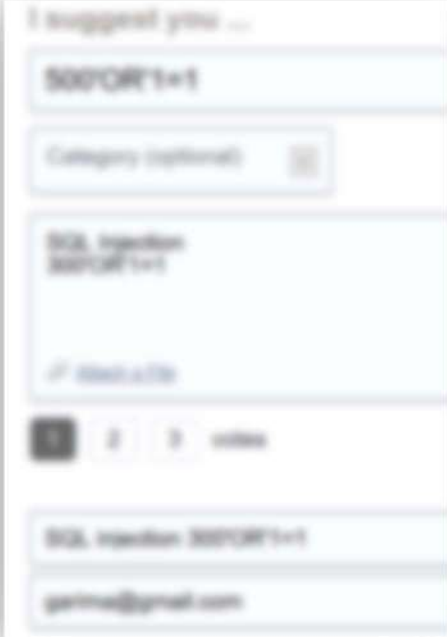

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Input Validation: Invalid data (<REDACTED>) in HTML input field
Primary Target(s):	<REDACTED> services
Secondary Target(s):	<REDACTED> services
Severity of Findings:	None
Evidence:	<p>The web application appropriately encodes malicious characters, so they do not affect server side applications and the response is an error code.</p>  

2.2.6.5.2. Test Case: Input Validation using SQL Injection


Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	SQL Injection
Primary Target(s):	<REDACTED> services
Secondary Target(s):	<REDACTED> services
Severity of Findings	None
Evidence:	<p>SQL injection attacks resulted in 'Microsoft having technical difficulties' generic error messages, this includes blind and comment SQL injection attacks.</p> <p>Example: SQL injection attempt for client_id variable in URI.</p>  

	   <p>The web Application Logic processes the data in an appropriate manner and leaves it uninitialized as is recommended for industry best practices.</p>
--	--

2.2.6.5.3. Test Case: HTTP Options

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Substitution of POST and GET Requests
Primary Target(s):	<REDACTED>.microsoftonline.us, <REDACTED>.microsoftonline.com
Secondary Target(s):	Azure
Severity of Findings:	None
Evidence:	<p>The operation of manipulating the HTTP POST request and the HTTP Get request resulted in a '411 Length Required' error, preventing the successful manipulation of these requests.</p> 


2.2.6.5.4. Test Case: Cross Site Scripting (XSS)

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Manipulation of user input with malicious data (XSS)
Primary Target(s):	<REDACTED>.microsoftonline.us, <REDACTED>.microsoftonline.com
Secondary Target(s):	Azure
Severity of Findings:	None
Evidence:	<p>The testing team attempted the manipulation of user input using several forms of malicious data. No malicious input was returned within the web applications in a manner that caused the execution of code.</p>

2.2.6.5.5. Test Case: Clickjacking/Keyjacking

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Manipulation of a web page using a frameable response
Primary Target(s):	<REDACTED>.microsoftonline.us, <REDACTED>.microsoftonline.com
Secondary Target(s):	Azure
Severity of Findings:	Low
Evidence:	<p>Using the findings from Burp Suite Pro, the testing team used the web forms, which were disclosed to use frame-able responses in order to create a clickjacking or key-jacking scenario. This vulnerability was discovered through Burp Web Application Scanner. This scenario is further outlined in PT-2017-5 in Appendix A.</p> <div data-bbox="521 758 1227 1419" style="border: 1px solid black; padding: 10px; margin: 10px auto; width: fit-content;"> <p>Website is vulnerable to clickjacking! Hey - we're giving away iPad minis!!! Just click the WIN button and it's yours!!!</p>  <p style="text-align: center; color: red;">>> WIN <<</p> </div>

2.2.7 Web Application Microsoft Azure Post-Exploitation

2.2.7.1. Unauthorized Management Access

No unauthorized access to management, root, or administrator level functionality was gained during the test.

2.2.7.2. Unauthorized Data Access

Access to unintended web applications was gained through forced browsing, but the revealed data, such as internal IP addresses and email addresses pose no threat to the Microsoft Azure web applications.

3. NETWORK

3.1. Network Overview

The FedRAMP penetration test of Azure included external public Internet testing the network infrastructure and external security posture. The focus was to gain unauthorized access to Azure via the network infrastructure. Specifically, tests simulated an external attack by an external un-credentialed entity (e.g., public) against the Azure network infrastructure, as configured in a production environment. In addition to Network penetration test case(s), FedRAMP required the following activities to be performed:

- ✓ A simulated Internet attack by an external un-credentialed entity (e.g. public) and an internal un-trusted entity (e.g. tenant) against Azure network services(s).
 - Network discovery
 - Network exploitation
 - Network post-exploitation, if exploitation was successful

Successful exploitation of the external Azure did not lead to new access path(s). FedRAMP required post-exploitation activities to explore overall risk of a vulnerability to the Azure as a whole. By performing post-exploitation, it was possible to assess confidence that any impact of the vulnerability is valid.

3.2. Network Discovery

3.2.1 Endpoint Enumeration

For this engagement, Microsoft provided the penetration testing team with a list of roughly 779,400 IPv4 addresses, of which 147,417 were unique. Of the unique addresses, 67,853 were RFC 1918 reserved IP addresses, and 78,386 were RFC 6598 shared address space. An NMAP scan was done to determine which hosts were communicating and had ports open to be able to test.

Description	Method of Scan	Result
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-082
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED> -sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-040
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-041
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-042

Description	Method of Scan	Result
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p 80,123,137-139,161,443,445,1433,8080,8443,3389 -sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-043
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED> -sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-044
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -<REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-045
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-046
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-047
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-048
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-049
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-050
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-051
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-052
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-053

Description	Method of Scan	Result
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-054
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-055
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-056
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-057
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED> -sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-032
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-033
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-034
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-035
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -<REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-036
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-037
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-038

Description	Method of Scan	Result
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-039
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-058
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-059
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-060
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-061
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-062
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-063
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-064
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-065
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-066
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-067

Description	Method of Scan	Result
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-068
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-069
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-070
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-071
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-072
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-073
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-074
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-075
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-076
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-077
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-078

Description	Method of Scan	Result
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-079
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-080
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-081
Host Discovery (Service Ping Sweep) - 10 network - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-089
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-083
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-002
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-003
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-004
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-005
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-006
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-008
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-007
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-019

Description	Method of Scan	Result
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-031
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-030
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-029
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-028
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-027
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-009
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-010
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-026
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED> -sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-011
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-025
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-012
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-024
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-013
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-014
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-015

Description	Method of Scan	Result
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-016
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-017
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-018
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-022
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-021
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-020
Host Discovery (Service Ping Sweep) - <REDACTED>	NMAP -vv -n -Pn -p <REDACTED>-sSV --max-retries 1 -iL <TARGETLIST> -oA <RESULTFILE>	SEE ARTIFACT PT-023

Table 4 - Azure Externally Accessible Hosts

3.2.2 Service Enumeration

The services offered by Azure were not mapped externally because none were identified during the host discovery portion, which also including mapping common services associated with Microsoft servers.

3.2.3 Operating System Fingerprinting

Since no open ports were detected during the endpoint enumeration phase, operating system fingerprinting phase was unnecessary and skipped.

3.2.4 Vulnerability Identification

Since no open ports were detected during the endpoint enumeration phase, vulnerability identification phase was unnecessary and skipped.

3.3. Network Exploitation

A network-level exploitation of Azure was completed to analyze the risks of identified vulnerabilities. The penetration tests focused on external attacks against Azure hosts to determine the sensitivity any information retrieved if exploitation is successful. Attack scenario(s) were created to exercise the security of Azure with the intent of gaining access to the hosts/systems and elevating privileges, if possible. If exploitation of the scenario was unsuccessful, the

scenario also discussed reasons why exploitation failed and what protections (if any) prevented the exploitation. The next section(s) cover the network exploitation of the Azure external boundary.

3.3.1 Test Case: Exploitation of Azure Boundary Service

The testing team put the supplied IP addresses and hosts through rigorous external to target testing. Through the use of numerous automated and manual methods the testing team was able to determine that the boundaries of the CSP was secure, filtered, and had no open ports in which were able to be exploited. Please see artifacts PT-002 through PT-115.

Attack Vector: **External to Target System - External Untrusted to External Trusted**

Test Objective	Attack boundary perimeter services from external domain
Primary Target(s):	Services offered at the boundary of Azure
Secondary Target(s):	Azure
Severity of Findings:	None
Evidence:	No vulnerabilities to report. Please see artifacts PT-002 through PT-115 for additional information.

3.3.2 Test Case: Credentialed Tenant Exploitation of a Secondary Tenant

While the testing team did not find any ports open to the external network, the perimeter of the CSP did not leave any availability to test a Tenant to Tenant exploitation through the Azure external boundaries presented within the RoE. However, the team was able to build out a simulated tenant environment in the portal, using virtual machines and services offered through Azure.

Attack Vector: Tenant **Tenant to Tenant - External Trusted to External Trusted**

Test Objective	Attack services and boundaries within a credentialed tenant of Azure towards a secondary credentialed tenant
Primary Target(s):	Services offered at the boundary and within a secondary tenant
Secondary Target(s):	Azure
Severity of Findings:	None
Evidence:	When a new virtual machine or service is initially deployed to the tenant environment, Azure will enable the necessary remote management port and service to allow the tenant to login remotely to finalize configuration. By default, this management service is open, and remotely accessible to the Internet. For Unix, the management port is <REDACTED>/<REDACTED> (SSH) and for Windows Server, the port is <REDACTED><REDACTED> (RDP). The tenant is responsible for managing access control to the services for their environment. While it is a best practice to avoid using default/standard ports, the usage of default ports is not a definitive vulnerability; therefore, this is not considered a finding.

3.3.3 Test Case: Target System to CSP Management System

The penetration testing team was not able to compromise any vector of the CSP management system by using the credentials of a tenant. Please see artifacts PT-002 through PT-115 for further details on exploitation attempts.

Attack Vector: Tenant **Target System to CSP Management System - External Trusted to Internal Trusted**

Test Objective	Attack services and boundaries within a credentialed tenant of Azure towards a secondary credentialed tenant
Primary Target(s):	Primary Tenant
Secondary Target(s):	Azure
Severity of Findings:	None
Evidence:	No vulnerabilities to report. Please see artifacts PT-002 through PT-115 for additional information.

3.4. Network Post-Exploitation

There were no findings within the Network Exploitation section of this Penetration Test Report.

4. SOCIAL ENGINEERING

4.1. Social Engineering Overview

The FedRAMP penetration test of Azure included an internet-based attack attempting to gain useful information about the Azure offering. The primary goal of the social engineering effort is to access the Azure through the corporate network owned and operated by Microsoft. The penetration test attempted to simulate an attack by an external untrusted entity (i.e., public) against designated in-scope Azure personnel. A comprehensive Open Source Intelligence (OSINT) discovery process along with a coordinated, but unannounced, spear phishing exercise was accomplished. The principle reasoning is to gain insight into the possibility of exploiting weaknesses in the human factor coupled leveraging corporate trust relationships to obtain an access path into Azure. Only employees, who are affiliated with the Azure and as determined by OSINT information, are targeted in this test. The vector primarily involves public information gathering of any data of value to facilitate an attack against the Azure, followed by an unannounced spear phishing campaign. During the RoE phase of this penetration test, Kratos and Microsoft mutually agreed that the sample size for social engineering testing would be 25 users with administrator access to the Azure infrastructure. This number was based on the sample size that FedRAMP has deemed acceptable in the previous penetration tests of social engineering of Microsoft Azure.

As stated in the RoE, Azure personnel were not targeted specifically to disclose Personal Identifiable Information (PII), as defined by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122. The scope of the Azure phishing reconnaissance includes Azure personnel with approved access to environments within the Azure accreditation boundary. The actual scope of the exercise was determined during the Azure Penetration Test RoE creation. During OSINT efforts, employees affiliated with Azure are identified and included in the social engineering exploitation phase. In such cases, those personnel were incorporated into social engineering spear phishing campaign. If an employee is determined to be no longer employed by the Microsoft, such personnel were removed from the scope.

4.2. Social Engineering Discovery

The penetration test began with OSINT information gathering which includes various attempts to discover key words and phrases related to the business conducted by the Microsoft, specifically Azure employees. Such employee-focused information gathering may concentrate on publicly available information based on employee relationships, email lists, website posts, and social networks. The social engineering target information that was harvested publicly from various Open Source tools found to be potentially relevant to Azure is identified in Table 5. This table details only those targets that were captured as a part of the Kratos OSINT information gathering efforts.

Source	Query	Result
Web Search Engine	Inurl: Microsoft.com Intext: @microsoft.com && intext:Azure	No relevant information was discovered using the provided query
LinkedIn Scraping	Manual searching	<p><REDACTED>@microsoft.com - <REDACTED></p> <p><REDACTED>@microsoft.com - <REDACTED></p> <p><REDACTED>@microsoft.com - <REDACTED></p> <p><REDACTED>@microsoft.com - <REDACTED></p> <p><REDACTED>@microsoft.com - <REDACTED><REDACTED>@microsoft.com - <REDACTED></p> <p><REDACTED>@microsoft.com - <REDACTED></p> <p><REDACTED>@microsoft.com - <REDACTED></p> <p><REDACTED>@microsoft.com - <REDACTED></p> <p><REDACTED>@microsoft.com - <REDACTED></p> <p><REDACTED></p>

Table 5 - Publicly Available Information about Azure

Due to the initially-collected targets either not being in-scope or the total targets not meeting the requisite sample size, Microsoft provided additional in-scope targets from which Kratos selected to meet the sample size. Table 6 details the total targets that were used for social engineering efforts. This table shows publicly available employee contact information associated with Azure. Note that the information depicted is “as harvested” and may be inaccurate. Raw data collected during Social Engineering is located in “Table 10 - Penetration Testing Evidence and Artifacts”.

Last Name	First Name	Email (as harvested)
<REDACTED>	<REDACTED>	<REDACTED>@micrososoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com

<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com
<REDACTED>	<REDACTED>	<REDACTED>@microsoft.com

Table 6 - Publicly Available Information on Azure Personnel

4.3. Social Engineering Exploitation

Attack Vector: Tenant **External to Corporate - External Untrusted to Internal Untrusted**

The spear phishing campaign is an electronic communication attempt, typically email, directed at specific individuals of Azure in order to gain/maintain access or disclose sensitive information. Kratos SecureInfo defined an acceptable email campaign based on a customized email template. See spear phishing/social engineering results in Figure 4-1.

Social engineering post-exploitation activities are not required by FedRAMP. Collection of statistics of the unannounced spear phishing campaign toward the Azure system administrators on the approved list is, however, reportable to FedRAMP. The spear phishing campaign was unannounced and launched from the Kratos SecureInfo lab on 16 November 2017 at 17:01 CDT. Spear Phishing ended on 28 November 2017 at 16:00 CDT.

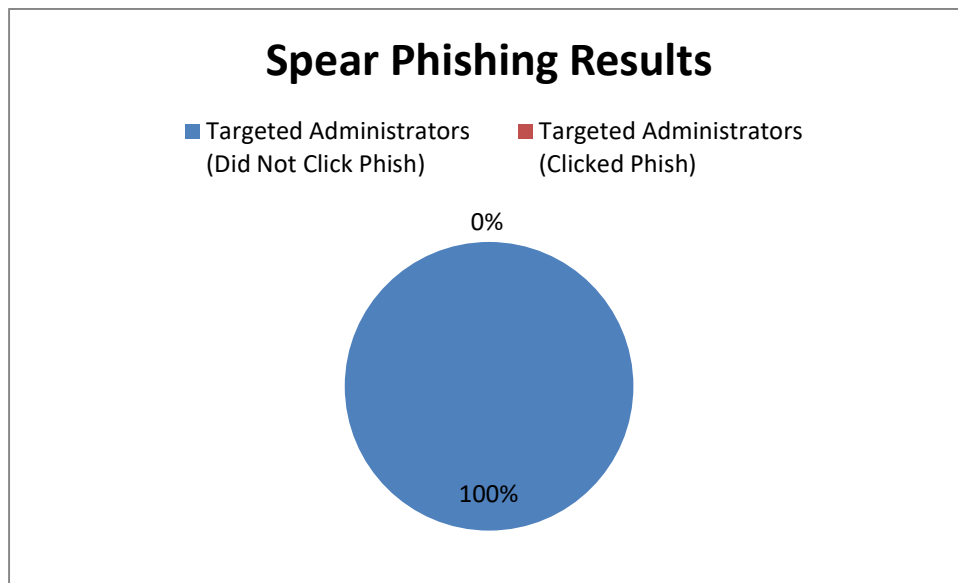


Figure 4-1, Spear Phishing Results

5. INTERNAL ATTACK

5.1. Internal Attack Overview

The FedRAMP penetration tests included representative corporate assets to determine the security posture against threats to Microsoft originating from the corporate environment. The focus was to identify and exploit vectors on corporate assets to access systems within the Azure boundary. Specifically, tests exploited any trust relationships between the Azure and corporate environment by simulating an internal attack by an internal credentialed entity (e.g., Microsoft employee or infected corporate workstation) against the Azure management infrastructure. In addition to the Internal Attack penetration test case(s), FedRAMP required the following activities to be performed:

- ✓ A simulated Internet attack by a trusted internal user (e.g. corporate user) against the CSP management system.
 - Internal Attack discovery
 - Internal Attack exploitation

Internal Attack discovery involved a scoped identification of attack chains with the assumption that an internal Azure user was compromised via social engineering attack(s). Additionally, a credentialed vulnerability scan of the representative workstation(s) was completed to identify publicly available vulnerabilities and privilege escalation vectors. Internal Attack exploitation involved testing potentially exploitable attack vulnerabilities on the representative workstation that could allow escalation and pivoting. FedRAMP does not require post-exploitation activities. Post-exploitation is not applicable under the Internal Attack vector; testing *assumes* a corporate breach with management access into the Microsoft corporate network has already occurred given that penetration testing is able to identify privilege escalation, pivoting avenues, and effective attack chains.

5.2. Internal Attack Discovery

5.2.1 Scoping

Kratos SecureInfo performed a scoping exercise to determine potential attack vectors into the Azure management environment. The scoping exercise identified possible privilege escalation, pivoting avenues, and attack chains. The attack chain(s) assume that an internal Microsoft user/employee was compromised by a successful social engineering attack. Table 7 describes various scenarios and applicable attack chains.

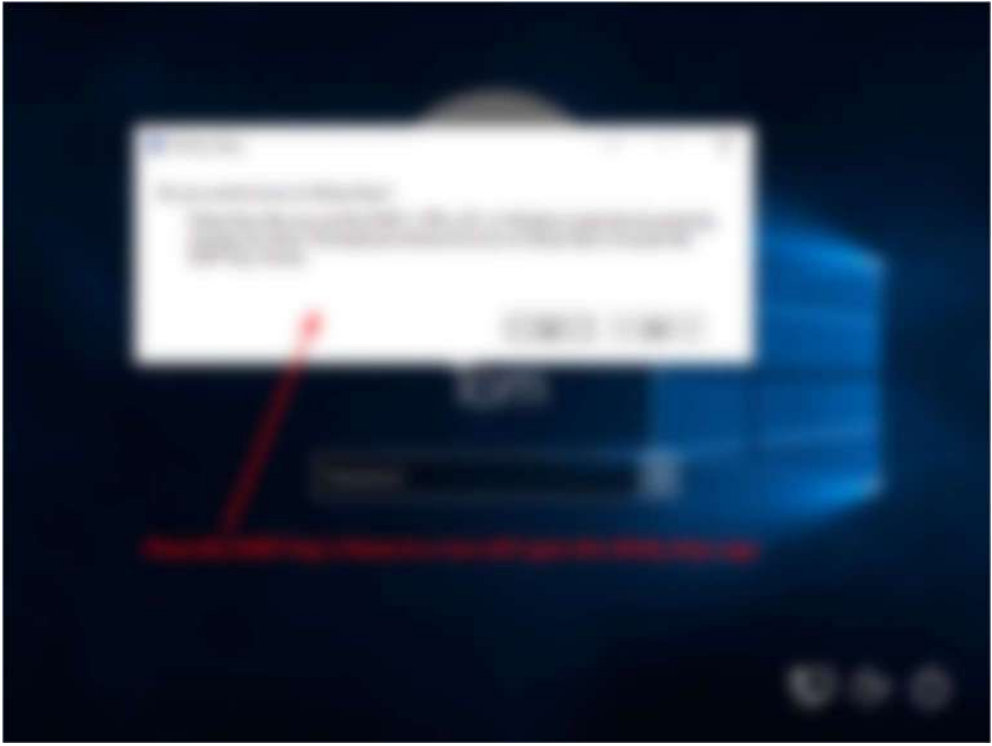
Scenario	Attack Chain
A low-level Azure account is escalated on the user workstation.	Internal Untrusted Users to Internal Trusted Users

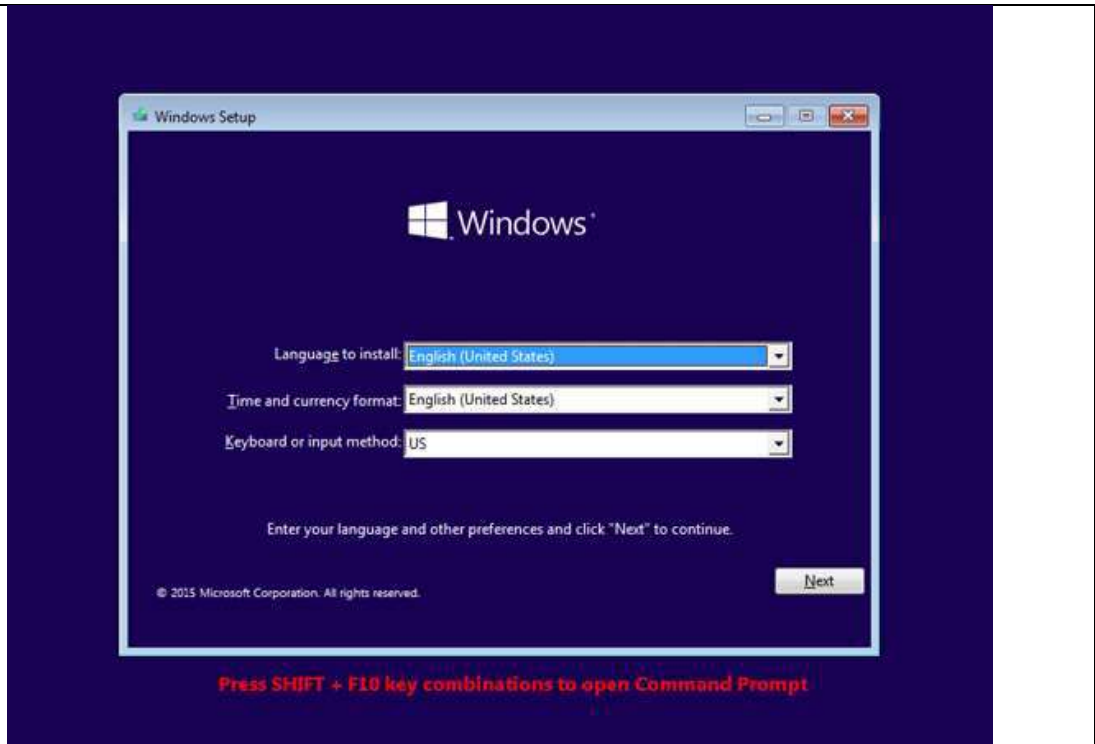
Table 7 - Potential Simulated Internal Attack Vectors

5.3. Internal Attack Exploitation

5.3.1 Test Case: Escalation of Privileges on Workstation

Attack Vector: Corporate to CSP Management System - Internal Untrusted to Internal Trusted

Test Objective	Escalate Privileges on the Corporate Workstation from standard User
Primary Target(s):	Corporate Representative Workstation
Secondary Target(s):	Azure Management Stack; Azure administrator access.
Severity of Finding:	None
Evidence:	<p>Over the course of the penetration test, one goal was to obtain administrator access on the laptop issued to the penetration testing team by the Azure team. An exploit path was discovered on the laptop that allowed the penetration testing team to obtain Administrator access using an exploit commonly known as the “sticky keys exploit.” Sticky keys are an accessibility feature built into the Windows operating system that is on by default, and is executed by pressing the Shift key five times. Once done, a prompt will appear asking if the user would like to use sticky keys.</p>  <p>This exploit is done by booting the windows machine to an installation copy of Windows 10. From the initial installation screen, by pressing Shift + F10, a Command Prompt window will appear.</p>



Once inside command prompt, the penetration test team changed directories to the internal drive "C:" and copied the executable that runs when Shift is pressed five times. This executable is named "<REDACTED>." By copying the Administrator command prompt, located at C:\<REDACTED>\<REDACTED>\<REDACTED>.exe, and replacing the "<REDACTED>" with this cmd executable, the penetration test team was able to execute an Administrator command shell from the login screen of the Windows operating system.



	<p>Once an Administrator command prompt was obtained, the penetration test team used the “<REDACTED>” commands to reset the Administrator password to “<REDACTED>” and proceeded to log in as the local Administrator on the Azure laptop.</p> <p>Without any mitigation, the above stated discovery would be considered a vulnerability; however, due to mitigations in place, risk has been eliminated. The compensating controls in this case that mitigate the risk to the method of environment access are:</p> <ul style="list-style-type: none">• Multifactor authentication is required to access the laptop• Multifactor authentication is required to access the environment (locally and remotely, whether privileged or non-privileged)• An approved VPN is required to access the environment• Just-in-time (JIT) access is required to access any asset within the environment (to include the Jump Boxes used to access anything within the boundary)• The laptop where the vulnerability was initially found is a corporate asset, which would bring down the potential impact to only include the Azure Jump Boxes (if the other mitigations were not in place)• While pass-the-hash would be a targeted exploit by a threat actor, it would not be a plausible one as the smart cards employed for the above stated multifactor authentication rely on Kerberos and are encrypted. This was proven by the fact that the penetration testing team could not break the two factor authentication. <p>Because of these controls, this does not appear to be a vulnerability within the Azure environment.</p>
--	---

6. PHYSICAL SECURITY

<SECTION REDACTED>

7. FINDINGS

Detailed information about the confirmed findings is in “Appendix A – Findings”. False positives are detailed in the below section, “False Positives”.

7.1. False Positives

Please see the following table for the list of findings deemed false positive that were discovered during penetration testing.

Discovery Source	False Positive Vulnerability	Justification
Nikto	<REDACTED>Information Disclosure Site: https://<REDACTED>.<REDACTED>.windowsazure.com/ Site: https:// <REDACTED>.<REDACTED>.windowsazure.com/<REDACTED>/	Server is unlikely to be Windows Server 2008R2 or older. Attempted exploitation via pad buster. After 86,000 and 144,000 respectively, canceled further attempts.
Burp	Xpath Injection Site: <REDACTED>.<REDACTED>.windowsazure.com	Multiple instances, however they are all simply an error page which is giving HTTP 200 responses to create a false positive.
Burp	SQL Injection Site: <REDACTED>.<REDACTED>.windowsazure.com	Multiple instances, however they are all simply an error page which is giving HTTP 200 responses to create a false positive.
Burp	Suspicious <REDACTED>data in parameter Site: <REDACTED>.<REDACTED>.windowsazure.com	Site is flagging the value of OpenIdConnect.nonce.OpenIdConnect, which were attempted be base64 decoded but the values were never legible.
Burp	CSRF Site: <REDACTED>.azure.us	Manual review found that these are merely GET request for java libraries and that no functions are being performed that would be vulnerable to a CSRF attack.
Burp	Cross Domain Scripting Site: <REDACTED>.microsoftonline.us	Manual verification revealed that the external websites are also owned by Microsoft, and therefore not truly "external" resources being included.
Burp	Cross Site Scripting Site:<REDACTED>.azure.com	The application reflects malicious user input in the OAuth "redirect_uri" variable in an error message. This would appear to be exploitable as a cross site scripting vulnerability (XSS). However, when actual script is entered, the error message no longer reflects the input, and instead announces "invalid input received from the user".

Burp	Billing API Authorization bypass Site: <REDACTED>.azure.us	False Positive: However, upon closer inspection, the data is blank and does not contain actual information about the requested subscription ID. Therefore, it appears that the request is vetted against the Authorization token to ensure the data being requested belongs to the authenticated user.
Burp	Cross Site Scripting Site: <REDACTED>.azure.us	The portal.azure.us Dashboard allows editing to include HTML Tags. The <REDACTED>tag appears to be blacklisted and now allowed. It appears that this limitation can be circumvented by adding an open <<REDACTED>before the<REDACTED>tag. However, the final HTML that is rendered on the web page still ignores the <REDACTED>tag and displays the content as an IMG tag.
Burp	File Include Site: portal. <REDACTED>	The Burp Pro scanner reported a file include vulnerability in the JavaScript file: <REDACTED> Upon manual examination, this was found to be a false positive. The requested "<REDACTED>" file was not retrieved. Instead a JavaScript file was retrieved which was confused by the scanner as the successful retrieval of the password file.

<p>Burp</p>	<p>Cross-domain Referrer leakage Site: <REDACTED>.microsoftonline.com</p>	<p>Cross Domain Referrer Leakage False Positive Explanation:</p> <p>The page was loaded from a URL containing a query string: https:// <REDACTED>.microsoftonline.com/<REDACTED>.aspx</p> <p>The response contains the following links to other domains: https:// <REDACTED>. <REDACTED>.com/<REDACTED>.aspx https:// <REDACTED>.com/ajax/jquery<REDACTED> https:// <REDACTED>.microsoft.com/<REDACTED><REDACTED> https://www.microsoft.com/<REDACTED>/<REDACTED></p> <p>All of the links contained are Microsoft links and Cross Domain Referer Leakage is not a threat. The websites linked can be trusted.</p>
<p>Burp</p>	<p>Cross-domain Referrer leakage Site: <REDACTED>.microsoftonline.com</p>	<p>Cross Domain Script Include False Positive Explanation:</p> <p>The response dynamically includes the following script from another domain: https:// <REDACTED>.com/ajax/jquery/<REDACTED></p> <p>The script from an external domain is included, however that is a Microsoft domain and the script can be trusted.</p>

Burp	Email Addresses Disclosed Site: <REDACTED>.microsoftonline.com	Email Addresses Disclosed: The following email addresses were disclosed in the response: <REDACTED>@<REDACTED>.com <REDACTED>@<REDACTED>.onmicrosoft.com These emails are used as examples and cannot be of use by an attacker.
Burp	Session token in URL Site: <REDACTED>.microsoftonline.us, <REDACTED>.microsoftonline.com	Burp Scanner identified 18 instances of session tokens being placed within the URL being passed. After inspection, these results are a false positive, and the results pose no risk to session security.
Burp	Cross-Site Scripting (Reflected) https:// <REDACTED>. <REDACTED>. <REDACTED>core.windows.net https:// <REDACTED>. <REDACTED>.msft.net	Burp scanner identified several XSS vulnerabilities, but all seem to be invalid, per manual testing. Filtering of any scripting is being done by the web application.
Burp	Out-of-band resource load (HTTP) https:// <REDACTED>. <REDACTED>.windows.net https:// <REDACTED>. <REDACTED>. <REDACTED>.core.windows.net https:// <REDACTED><REDACTED>. <REDACTED>.core.windows.net	No connections to other hosts were established using any payload.
Burp	SQL Injection https:// <REDACTED>. <REDACTED>.msft.net	No injection methods were possible on the web application. These attempts were either blocked by the web application, or sanitized in the output.
Burp	External Service Interaction https://p<REDACTED>. <REDACTED>. <REDACTED>.core.windows.net https:// <REDACTED><REDACTED>. <REDACTED>.core.windows.net	No suitable payload caused the application server to attack a separate host.
Burp	Cross-Site Request Forgery https:// <REDACTED>. <REDACTED>.core.windows.net https:// <REDACTED>. <REDACTED>.msft.net https:// <REDACTED>. <REDACTED>. <REDACTED>.core.windows.net	The application's state could not be altered by any request made by the attacker. Parameter filtering blocked any malformed request.

<p>Burp</p>	<p>XML Injection https:// <REDACTED>. <REDACTED>. <REDACTED>.core.windows.net https:// <REDACTED>. <REDACTED>. <REDACTED>.core.windows.net</p>	<p>No unauthorized actions were possible using any XML functions given to the user.</p>
<p>Burp</p>	<p>Client-side HTTP parameter pollution (reflected) https:// <REDACTED>. <REDACTED>.core.windows.net</p>	<p>No other vulnerabilities allowed the leverage of any parameter pollution, so identification of effected parameters was not possible.</p>
<p>Burp</p>	<p>Open redirection (DOM-Based) https:// <REDACTED>. <REDACTED>.core.windows.net https:// <REDACTED>-<REDACTED>. <REDACTED>.core.windows.net https:// <REDACTED>. <REDACTED>. <REDACTED>.core.windows.net</p>	<p>This vulnerability would need phishing as leverage, and thus could not be tested over the course of the penetration test.</p>

Table 8 - Penetration Testing Results - False Positives

Appendix A - Findings


Findings	File
This Excel Spreadsheet contains the Penetration Test Findings.	 Azure Commercial Pen Test Findings Tat

Table 9 - Penetration Testing Findings

Appendix B - Evidence

Evidence ID	Description	Test Section	Artifact
PT-001	This artifact contains the Rules of Engagement (RoE) signed between Kratos SecureInfo and Microsoft.	Other	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-002	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-003	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-004	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-005	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-006	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-007	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-008	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-009	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-010	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-011	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.

PT-012	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-013	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-014	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-015	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-016	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-017	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-018	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-019	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-020	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-021	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-022	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-023	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.

PT-024	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-025	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-026	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-027	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-028	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-029	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-030	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-031	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-032	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-033	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-034	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-035	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.

PT-036	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-037	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-038	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-039	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-040	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED><REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-041	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-042	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>management network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-043	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>management network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-044	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>management network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-045	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>management network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-046	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a	Network	Artifact too large to embed; evidence artifacts to be

	private 10 network remotely on the <REDACTED> management network management segment.		delivered separately and/or by request.
PT-047	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>management network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-048	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>management network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-049	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-050	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-051	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-052	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>management network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-053	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>management network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-054	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-055	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-056	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.

PT-057	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-058	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> management network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-059	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on <REDACTED><REDACTED>segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-060	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>management network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-061	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>management network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-062	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-063	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-064	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-065	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-066	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-067	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.

PT-068	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-069	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>t network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-070	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-071	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-072	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-073	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-074	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-075	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-076	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-077	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-078	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-079	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a	Network	Artifact too large to embed; evidence artifacts to be

	private 10 network remotely on the <REDACTED> network management segment.		delivered separately and/or by request.
PT-080	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-081	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-082	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on the <REDACTED> network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-083	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans on the <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-084	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP <REDACTED>. <REDACTED>.windowsazure.com.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-085	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>. <REDACTED>.windowsazure.com.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-086	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>. <REDACTED>. <REDACTED>.core.windows.net.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-087	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>. <REDACTED>.net.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-088	This artifact contains additional NMAP scans from the tenant to tenant perspective.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-089	This artifact contains the raw NMAP scanner data for External to Target CSP un-credentialed scans of a private 10 network remotely on <REDACTED>network management segment.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-092	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.

	<REDACTED>.diagnostics<REDACTED>.core.windows.net.		
PT-093	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>.core.windows.net.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-094	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of portal. <REDACTED>s.com.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-096	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>.microsoftonline.com.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-097	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of<REDACTED>.windows.net.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-098	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>.microsoftonline.com.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-100	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>.core.windows.net.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-101	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>.core.windows.net.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-102	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of icm<REDACTED>.msft.net.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-103	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>.windows.net.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-104	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>. <REDACTED>.net.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-105	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>.core.windows.net/.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.

PT-106	This artifact contains the write-up and screenshot data for the Internal Attack of the provided laptop by <REDACTED>	Internal Attack	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-107	This artifact contains the network scan data for the Azure infrastructure deployable <REDACTED>.	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-108	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>.core.windows.net.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-110	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>. <REDACTED>.core.windows.net.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-111	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>. <REDACTED>.windows.net.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-112	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>. <REDACTED>.windowsazure.com.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-113	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>.net .net. This includes: <REDACTED>.net <REDACTED>.net <REDACTED>.net <REDACTED>.net <REDACTED>.net <REDACTED>.net <REDACTED>.net <REDACTED>.net <REDACTED>.net <REDACTED>.net <REDACTED>.net <REDACTED>.net <REDACTED>.net <REDACTED>.net <REDACTED>.net	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.

	<REDACTED>.core.windows.net <REDACTED>core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net <REDACTED>.core.windows.net		
PT-115	This artifact contains the Burp Pro, Nessus, and any other web scanner data for External to Target CSP un-credentialed of <REDACTED>.windowsazure.com.	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-116	NMAP and Nessus scans from azure cloud	Network	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-117	NMAP and Nessus scans from azure DOD cloud	Web Application	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.
PT-118	Phishing logs and associated files.	Social Engineering	Artifact too large to embed; evidence artifacts to be delivered separately and/or by request.

Table 10 - Penetration Testing Evidence and Artifacts