**Initial Pentest Scope**

**Overview**

Our network is organized into five separate different subnets, each of which supports various parts of our

infrastructure. We are primarily a Microsoft Windows shop, with almost everything we do supported on

Windows and Azure infrastructure. This includes numerous enterprise management and security

systems, our banking infrastructure, remote systems, a DMZ, and finally workstations / branch networks.

**Summary**

The assessment will consist of the following scope:

• Five subnets, each with several (between 20 and 50) hosts

• A blockchain-based banking solution

• Several custom applications, including our core and web banking services

• A Microsoft Active Directory environment

**Contact for any concerns:** pentest@dinobank.us

**5. PENETRATION TEST METHODOLOGY AND REQUIREMENTS**

§ Web Application/Application Program Interface (API) Testing

§ Simulated Internal Attack Vectors

§ Network Testing

**5.1. INFORMATION GATHERING & DISCOVERY**

**5.1.2. WEB APPLICATION/API TESTING INFORMATION GATHERING/DISCOVERY**

**Discovery Activities:**

|  |  |  |
| --- | --- | --- |
| **Activity** | **Description** | **Findings** |
| Perform internet  searches to identify any  publicly available  information on the  target web application | Identify any publicly available documentation that can be leveraged to gain insight into  potential attack vectors of the target web application. Determine if any publicly available  vulnerability has been disclosed, which could potentially be leveraged to attack the target  web application. |  |
| Identify the target  application architecture | Identify all layers of the application including application servers, databases, middleware,  and other technologies to determine communication flow and patterns within the  application. |  |
| Identify account roles  and authorization  bounds | Identify the roles associated with the cloud service and determine access limitations. |  |
| Map all content and  functionality | Create a sitemap detailing all levels of functionality within the web application. Please  note: different account roles may have different access levels to functionality within the  target web application. |  |
| Identify all user-controlled  input entry  points | Map all areas of the application that take input from the user of the application. |  |
| Perform web  application server  configuration checks | Perform web vulnerability scanning activity to determine if common web server  configuration flaws are present that could lead to an access path. |  |

**5.2.2 NETWORK INFORMATION GATHERING/DISCOVERY**

**Discovery Activities:**

|  |  |  |
| --- | --- | --- |
| **Activity** | **Description** | **Findings** |
| Perform Open Source  Intelligence (OSINT)  Gathering Activities | Conduct an analysis of the public profile of the target system including information  disseminated about public Internet Protocol (IP) ranges, technologies implemented within  the target network or organization, and details around previous public attacks against the  target system. |  |
| Enumerate and  Inventory Live Network  Endpoints | Conduct a scan to identify active network endpoints on the network environment. |  |
| Enumerate and  Inventory Network  Service Availability | Conduct an inventory of network services to identify potential attack vectors. |  |
| Fingerprint Operating  Systems and Network | Determine service types and versions numbers. |  |
| Perform Vulnerability  Identification | Conduct network scanning activity to identify publicly available vulnerabilities. |  |

**Social Engineering ?**

**5.2.3. SIMULATED INTERNAL ATTACK INFORMATION GATHERING/DISCOVERY**

**Discovery Activities:**

|  |  |  |
| --- | --- | --- |
| **Activity** | **Description** | **Finding** |
| Perform a scoping  exercise with the CSP  to determine potential  attack vectors. | Identify valid attack chains assuming an internal CSP user was compromised by a social  engineering attack. |  |
| Perform Vulnerability  Identification | Conduct credentialed network scanning activity to identify publicly available vulnerabilities  and privilege escalation vectors. |  |

**5.3. EXPLOITATION**

**5.3.1** WEB APPLICATION/API EXPLOITATION

|  |  |  |
| --- | --- | --- |
| **Activity** | **Description** | **Finding** |
| Authentication and  Session Management | Assess the application to determine how the target application creates and maintains a  session state. Analyze account creation and management process. |  |
| Authorization | Identify issues related to role privilege enforcement across common customer roles in the  cloud service. Attempt to bypass authorization restrictions. |  |
| Application Logic | Attempt to circumvent controls to prevent bypass on intended logic patterns and  application flows. |  |
| Input Validation | Perform injection attacks against all data inputs to determine if information or files can be  inserted or extracted from the target application. Attempt to alter the backend. |  |

5.3.2. NETWORK EXPLOITATION

|  |  |  |
| --- | --- | --- |
| **Activity** | **Description** | **Findings** |
| Attack Scenarios | Present identified attack scenarios to the CSP for approval of execution. Note that if the  CSP does not approve a potential exploitation path, this must be documented in the  Penetration Test report. |  |
| Exploitation | Perform exploitation activity with the intent of gaining access to the target systems and  elevating privileges, if possible. If unsuccessful, attempt to adapt the exploitation approach  to work against the target environment. |  |
| Record Results | If exploitation attack scenarios were successful, document the results. If exploitation attack  scenarios were unsuccessful, document why the exploit failed and what protections (if any)  prevented the exploit from executing. |  |

5.3.1. SIMULATED INTERNAL ATTACK EXPLOITATION

|  |  |  |
| --- | --- | --- |
| **Activity** | **Description** | **Findings** |
| Escalate to  Administrative  Privileges | Attempt to gain administrative privileges on the CSP standard workstation image. If the  CSP provisions users as local system administrators by default, testing should still be  conducted to determine the likelihood of a successful pivot to additional workstations or  servers in the CSP environment. |  |
| Recording Results | If exploitation attack scenarios were successful, document the results. If exploitation attack  scenarios were unsuccessful, document why the exploit failed and what protections (if any)  prevented the exploit from executing. |  |

**5.4. POST-EXPLOITATION**

5.4.1. WEB APPLICATION/API POST-EXPLOITATION

|  |  |  |
| --- | --- | --- |
| **Activity** | **Description** | **Findings** |
| Unauthorized  Management Access | Use access to application to attempt to gain control of underlying infrastructure or  management systems. |  |
| Unauthorized Data  Access | Attempt to demonstrate the potential to access additional data from sources outside the  cloud service’s intended scope. |  |

5.4.2. NETWORK POST-EXPLOITATION

|  |  |  |
| --- | --- | --- |
| **Activity** | **Description** | **Findings** |
| Gain Situational  Awareness | Determine what level of access was gained following a successful exploitation attempt. |  |
| Privilege Escalation | If applicable, attempt to escalate privileges to allow for additional access on the exploited  endpoint or other endpoints within the network environment. |  |
| Lateral Movement | Perform further discovery and enumeration to identify hosts on the network that may  respond only to the compromised system. Leverage compromised systems and credentials  to pivot to additional hosts with the intent of gaining unauthorized access to management  systems or other customer systems. |  |
| Identification and  Exfiltration of Sensitive  Systems or Data | Identify sensitive or critical information that may be accessed or compromised through a  successful attack (criteria for sensitive data to be determined during the scoping phase).  Attempt to exfiltrate sensitive information undetected. |  |

**6. REPORTING FORMAT**

Penetration Test assessment activities and results must be organized and compiled into a

comprehensive Penetration Test report to be included in the Security Assessment Report (SAR). The report is required to address the following sections.

**6.1. SCOPE OF TARGET SYSTEM**

Outline the target system that was assessed and if any deviations were made from the ROE/TP

document.

**6.2. ATTACK VECTORS ADDRESSED DURING THE PENETRATION TEST**

Described the attack vector(s) tested and the threat model(s) followed for executing the Penetration Test.

**6.3. TIMELINE FOR ASSESSMENT ACTIVITY**

Document when Penetration Testing activity was performed.

**6.4. ACTUAL TESTS PERFORMED AND RESULTS**

Document the actual tests performed to address the Penetration Test requirements outlined in this document and document the results of each test.

**6.5. FINDINGS AND EVIDENCE**

Findings should include a description of the issue, the impact on the target system, a recommendation to the CSP, a risk rating, and relevant evidence to provide context for each finding.

**6.6. ACCESS PATHS**

Access paths are the chain of attack vectors, exploitations, and post-exploitations that lead to a

degradation of system integrity, confidentiality, or availability. The 3PAO must describe the access path and the Penetration Test impact if multiple vulnerabilities could be coupled to form a sophisticated attack against the CSP. The Penetration Test report should include appropriate confidentiality