logo

**Penetration Test: Final Report**

Prepared for

**<company>**

<date>

Proprietary & Confidential

# Table of Contents

[1 Table of Contents 2](#_Toc63341601)

[2 Confidentiality Statement 3](#_Toc63341602)

[3 Contact Information 4](#_Toc63341603)

[4 Document History 4](#_Toc63341604)

[5 Executive Summary 5](#_Toc63341605)

[5.1 Project Information 5](#_Toc63341606)

[5.2 Testing Methodology 5](#_Toc63341607)

[5.3 Scope 6](#_Toc63341608)

[5.4 Risk Ranking Approach 6](#_Toc63341609)

[5.5 Summary of Findings 7](#_Toc63341610)

[6 Detailed Assessment Findings and Recommendations 8](#_Toc63341611)

[6.1 Internal Penetration Test 8](#_Toc63341612)

[6.1.1 Scenario 8](#_Toc63341613)

[6.1.2 Attack Narrative 8](#_Toc63341614)

[6.1.3 Findings 9](#_Toc63341615)

[6.2 External Penetration Test 10](#_Toc63341616)

[6.2.1 Scenario 10](#_Toc63341617)

[6.2.2 Attack Narrative 10](#_Toc63341618)

[6.2.3 Findings 11](#_Toc63341619)

[6.3 Web Application Penetration Test 12](#_Toc63341620)

[6.3.1 Scenario 12](#_Toc63341621)

[6.3.2 Attack Narrative 12](#_Toc63341622)

[6.3.3 Findings 13](#_Toc63341623)

[6.4 Attack Narrative 14](#_Toc63341624)

# Confidentiality Statement

This document contains confidential and privileged information from <vendor>. The information is intended for the private use of <company> for their understanding of the current state of security and or compliance of their organization. By accepting this document, <company> agrees to keep the contents of this document in confidence and not copy, disclose, or distribute it to any parties, other than those that will provide services and/or products directly to <company> as a result of the recommendations of this document, without written request to and written confirmation from <vendor>. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

# Contact Information

|  |  |
| --- | --- |
| **Full Legal Name** | <company> |
| **Primary Contact for Notices Name, Title** |  |
| **Street Address** |  |
| **City, State/Province** |  |
| **Zip/Postal Code, Country** |  |
| **Phone Number** |  |
| **Email** |  |

|  |  |
| --- | --- |
| **Full Legal Name** | <vendor> |
| **Primary Contact for Notices Name, Title** |  |
| **Street Address** |  |
| **City, State/Province** |  |
| **Zip/Postal Code, Country** |  |
| **Phone Number** |  |
| **Email** |  |

# Document History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Comments** |
|  |  |  |  |

# Executive Summary

## Project Information

<company> (“Client”) contracted <vendor> (“VENDOR”) to perform internal, external and web application penetration tests, with the goals of:

1. Identifying if a remote or insider attacker could penetrate existing defenses
2. Determining the impact of a security breach on the:
   1. Confidentiality of the company’s private data
   2. Internal infrastructure and availability of the company’s information systems
   3. Hardiness of web applications against targeted attacks

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker or malicious insider to gain unauthorized access to organizational data. The attacks were conducted with the following levels of access:

1. A general internet user
2. A local user who compromised a networked computer that is unassociated with Client

This assessment was conducted in accordance with the recommendations outlined in NIST SP 800-115[[1]](#footnote-1), with all test and actions being conducted under controlled conditions.

## Testing Methodology

Internal Penetration Test:

A testing platform was provided to the Client for installation inside of the internal network. Internal activities against Client networks include, but are not limited to the following:

* Scanning (e.g. Nmap) to identify open ports and services
* Attempted exploitation of vulnerable programs and services using various tools, means and techniques

External Penetration Test:

External activities against the Client networks include, but are not limited to, the following:

* Open Source Intelligence Gathering (e.g. Shodan, theHarvester, Google Dorks) to identify the extent of Client’s visibility on the open web
* Scanning (e.g. Nmap) to identify open ports and services
* Web application assessments (e.g. Burp Suite Pro, ZAProxy) to identify data transmission issues between a publicly available website and a client application or browser

Web Application Assessment:

Activities against the Client applications include, but are not limited to, the following:

* Open Source Intelligence Gathering (e.g. Shodan, theHarvester, Google Dorks) to identify the extent of Client’s visibility on the open web
* Tests against OWASP Top 10 Web Vulnerabilities[[2]](#footnote-2)
* Limited form field probing/fuzzing
* Static source code analysis

## Scope

The scope of this penetration test includes the following internal and external networks and web applications:

|  |  |  |  |
| --- | --- | --- | --- |
| Internal Network/IPs | | External Networks/IPs | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Web Applications | | | |
|  | |  | |

## Risk Ranking Approach

Risk analysis was conducted over the course of the assessment as vulnerabilities were discovered. These findings were then assigned a risk category and severity level using the Process for Attack Simulation & Threat Analysis (P.A.S.T.A.) method. There are seven (7) stages to determining and assigning risk using PASTA:

|  |  |
| --- | --- |
| Stages | Description |
| 1. Define business objectives | Determine requirements for the analysis and management of web-based risks |
| 1. Define the technology scope | Define the scope of technical assets/components for which threat enumeration will occur |
| 1. Decompose the application | Identify the controls that protect high-risk applications and services |
| 1. Threat analysis | Identify and extract threat information from intelligence sources to learn about probable scenarios that might be used by malicious actors |
| 1. Weakness and vulnerabilities analysis | Analyze weaknesses and vulnerabilities of security controls |
| 1. Attacks/Exploits enumeration & modeling | Attempt to compromise security controls and gain unauthorized access to systems |
| 1. Risk and impact analysis | Impact analysis, residual risk and countermeasure development |

## Summary of Findings

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose on the business processes implemented by the application, based on the following criteria:

**Critical**: Immediate threat to key business processes.

**High**: Indirect threat to key business processes/threat to secondary business processes.

**Medium**: Indirect/partial threat to business processes.

**Low**: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.

**Info**: Useful informational data point; not a vulnerability but may become one.

The current risk level of systems tested, based on the highest risk level of findings in systems, is **<severity>**. During the testing, a total of <num> (x) **Critical**, <num> (x) **High**, <num> (x) **Medium** and <num> (x) **Low** vulnerabilities were identified.

|  |  |
| --- | --- |
| Internal Penetration Test | |
| Vulnerability | Severity |
|  |  |
|  |  |

|  |  |
| --- | --- |
| External Penetration Test | |
| Vulnerability | Severity |
|  |  |
|  |  |

|  |  |
| --- | --- |
| Web Application Penetration Test | |
| Vulnerability | Severity |
|  |  |
|  |  |

# Detailed Assessment Findings and Recommendations

## Internal Penetration Test

### Scenario

The scenario for the internal penetration test was as follows:

* Malicious Visitor: A testing platform was provided to Client for installation inside of the internal network to imitate an attacker that has compromised a machine unowned by Client with internal network connectivity without access to or using proper credentials.

### Attack Narrative

**(keep the narrative to a single page)**

Generic overview, blah blah. After scanning with Nmap, scans indicated a possible vulnerability in <service>. Using <tool>, the team was able to exploit this vulnerability and gain <permissions/accesses> to <x> machines. The team then used <tool and process> to pivot into <admin account>, which would be considered a full domain compromise, etc., etc.

### Findings

| **Vulnerability Name** | **Example Vuln** |
| --- | --- |
| **CVSS Score/Severity** | **Critical** |
| **Resolution Effort** | Medium-High |

**Description:**

The Hashcat utility was used to crack passwords collected by Responder. Using a wordlist of over 3.4 billion unique passwords, the utility hashes each “word” and compares it to the given known hash. If the resultant hash matches, then the password has been “cracked” into its plaintext value. It is possible for hash collisions to occur; however it is exceedingly rare with NTLMv2 hashing. But because of the possibility, each plaintext password is then attempted against the target to verify correctness using CrackMapExec, as seen below. The blue box highlights a successful login, signified by the “[ + ]” characters.

<image here>

**Affected Assets:**

<write affected user accounts and/or system IP/hostnames here>

**Recommendations:**

<try to give at least 2 recommendations to include the most technically effective and the most cost effective>

Domain user account password settings are controlled by the domain’s group policy settings. On a domain controller, these settings can be found using the group policy editor under Computer Configuration 🡪 Policies 🡪 Windows Settings 🡪 Security Settings 🡪 Account Policies 🡪 Password Policy. The details on what Microsoft considers a “complex password” can be found within reference 1 below. To enforce stronger password policies than those available by default, domain policy should be reconfigured with custom password rules that enforce more complexity than the default Windows policy. Details on overriding or manipulating the default password policy can be found within reference 2 below. Additionally, all user accounts specified above should be handled as compromised, and passwords should be changed immediately.

**References:**

1. https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements
2. https://docs.microsoft.com/en-us/previous-versions//ms722439(v=vs.85)?redirectedfrom=MSDN

## External Penetration Test

### Scenario

The scenario for the external penetration test was as follows:

* An attacker from within the United States is targeting Client.
* The attacker is attempting to obtain unauthorized access to non-public personnel or client data without valid credentials.

### Attack Narrative

### Findings

| **Vulnerability Name** |  |
| --- | --- |
| **CVSS Score/Severity** |  |
| **Resolution Effort** |  |

**Description:**

<write here>

**Affected Assets:**

<write here>

**Recommendations:**

<write here>

**References:**

<write here>

## Web Application Penetration Test

### Scenario

The scenario for the external penetration test was as follows:

* An attacker from within the United States is targeting Client.
* The attacker is attempting to obtain unauthorized access to the administrative functions of the application without valid credentials.

### Attack Narrative

### Findings

| **Vulnerability Name** |  |
| --- | --- |
| **CVSS Score/Severity** |  |
| **Resolution Effort** |  |

**Description:**

<write here>

**Affected Assets:**

<write here>

**Recommendations:**

<write here>

**References:**

<write here>

## Attack Narrative

The following table is a non-inclusive list of tools used during this assessment:

|  |  |  |  |
| --- | --- | --- | --- |
| Tools Listing | | | |
| Metasploit | Burp Suite Pro | Nmap | CrackMapExec |
| Responder | Impacket | testssl.sh (script) | John the Ripper |
| Hydra | Medusa | Hashcat | Sysinternals Suite |
|  |  |  |  |

The following table illustrates a selection of exploits that were attempted against internal hosts. Exploits pertaining to DNS/ARP spoofing, denials of service or brute forcing credentials were not attempted. These exploits have the potential of crashing services or locking out users and should never be used in a production environment without explicit permission of the system owners.

|  |  |  |
| --- | --- | --- |
| Attempted Exploit(s) | Targeted Host(s) | Results |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. <https://csrc.nist.gov/publications/detail/sp/800-115/final> [↑](#footnote-ref-1)
2. <https://owasp.org/www-project-top-ten/> [↑](#footnote-ref-2)