

**<Project Name>**

**Penetration Testing Report v1.0**

27th July, 2024

**Prepared By**

**<Author Name>**

<Email>

<Mobile>

<City, Country>

Table of Contents

[Confidentiality Statement 3](#_Toc173003981)

[Disclaimer 3](#_Toc173003982)

[Contact Information 3](#_Toc173003983)

[Executive Summary 4](#_Toc173003984)

[Risk Rating 5](#_Toc173003985)

[1. STRIDE 5](#_Toc173003986)

[2. DREAD 5](#_Toc173003987)

[Severity Legend 5](#_Toc173003988)

[Scope 6](#_Toc173003989)

[Assessment Timelines 6](#_Toc173003990)

[Key Strengths & Weaknesses 7](#_Toc173003991)

[1. Strengths 7](#_Toc173003992)

[2. Weaknesses 7](#_Toc173003993)

[Observed Vulnerabilities 8](#_Toc173003994)

[Assessment Details 9](#_Toc173003995)

[Open Source Intelligence Gathering (OSINT) 9](#_Toc173003996)

[1. Vulnerability Name 1 INFO 9](#_Toc173003997)

[2. Vulnerability Name 2 MEDIUM 10](#_Toc173003998)

[External Penetration Testing 11](#_Toc173003999)

[1. Vulnerability Name 1 MEDIUM 11](#_Toc173004000)

[2. Vulnerability Name 2 HIGH 12](#_Toc173004001)

[Internal Penetration Testing 13](#_Toc173004002)

[1. Vulnerability Name 1 HIGH 13](#_Toc173004003)

[2. Vulnerability Name 2 HIGH 14](#_Toc173004004)

# **Confidentiality Statement**

This document is the sole property of **<CLIENT NAME>** and **<Project KillChain>**. This document contains proprietary and confidential information. Duplication, Distribution, or Use in whole, in parts, or in any form requires due consent from both of the parties involved during the time of the engagement and creation of this report.

The **<CLIENT NAME>** can share this document internally within their organization based on the data classification policy, and SOD matrix provided with due care and due diligence.

# **Disclaimer**

This assessment was a time-bound activity with explicit (**<TESTING DATE>**). The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagement does not allow a full evaluation of all security controls. **<Project KillChain>** prioritized the assessment to identify the weakest security controls an attacker would exploit. **<Project KillChain>** recommends conducting similar assessments on an annual basis/continual basis by internal or third-party assessors to ensure the continued success of the controls.

# **Contact Information**

|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **Contact Information** |
| <CLIENT NAME> | | |
| <CLIENT POC> | <TITLE> | Email:email@client.client |
| <PROJECT KILL-CHAIN> | | |
| <TESTER POC> | <TITLE> | Email:killchain@projectkillchain.chain |

# **Executive Summary**

**<Client Name>** Penetration Testing Team was hired to conduct a full fledge security assessment of “**<PROJECT NAME>**” to uncover all potential security vulnerabilities which can potentially provide an advantage to the threat actors to successfully compromise the organization, exfiltrate the sensitive data, add backdoor for long term access. **<Project KillChain>** Penetration Testing Team equipped with the start of the art tools and team conducted this assessment end to end and found several vulnerabilities.

The methodology included the following.

1. Open Source Intelligence Gathering – OSINT
2. External Penetration Testing
3. Internal Penetration Testing

**<Project KillChain>** Penetration Testing Team conducted this assessment in 3 phases, starting from Open-Source Intelligence gathering and utilizing the same information to compromise the organization externally and gain access to internal system with the final goal of taking over the domain controller in which **<Project KillChain>** proved to be successful.

**<ADD A SUMMARY OF YOUR FINDINGS HERE>**

All of the issues observed and being provided in this report are required to be fixed while most of them require immediate fixing. **<Project KillChain>** team recommends fixations on priority basis.

# **Risk Rating**

The vulnerability risk rating is based on the STRIDE and DREAD framework.

# **STRIDE**

|  |  |  |
| --- | --- | --- |
| **S. No** | **Threat** | **Security Property** |
| 1. | Spoofing | Authentication |
| 2. | Tampering | Integrity |
| 3. | Repudiation | Non-Repudiation |
| 4. | Information Disclosure | Confidentiality |
| 5. | Denial of Service | Availability |
| 6. | Elevation of Priviliges | Authorization |

# **DREAD**

|  |  |  |
| --- | --- | --- |
| **S. No** | **Risk Analysis** | |
| 1. | Damage | Impact of an attack |
| 2. | Reproducibility | How easy the attack can be reproduced |
| 3. | Exploitability | How easy can an attack be launched |
| 4. | Affected Users | How many users will be affected |
| 5. | Discoverability | How easy can this vulnerability be found |

# **Severity Legend**

This section includes the color schemes used to represent the severity of the vulnerabilities throughout this report.

|  |  |  |
| --- | --- | --- |
| **S. No** | **Severity** | **Legend** |
| 1. | Critical |  |
| 2. | High |  |
| 3. | Medium |  |
| 4. | Low |  |
| 5. | Informational |  |

# **Scope**

The scope for this assessment was limited to the following assets only and did not include DOS/DDOS, Social Engineering, and Physical Security Assessment activities, Public Facing infrastructure other than the provided internet facing asset.

|  |  |  |  |
| --- | --- | --- | --- |
| S. No | Assessment Type | Asset Name/Details | Asset Location |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
| 4. |  |  |  |

# **Assessment Timelines**

The agreed assessment timelines for this assessment covering the above provided scope is provided in the below table.

|  |  |  |  |
| --- | --- | --- | --- |
| S. No | Assessment Type | Days | Hours |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

No additional days were taken except the client briefing after the conclusion of the assessment.

# **Key Strengths & Weaknesses**

# **Strengths**

* Strength 1
* Strength 2
* Strength 3
* Etc.

# **Weaknesses**

* Weakness 1
* Weakness 2
* Weakness 3
* etc.

# **Observed Vulnerabilities**

Following is a list of vulnerabilities that have been identified during the assessment.

|  |  |  |
| --- | --- | --- |
| **S. No** | **Observation** | **Severity** |
| **Open Source Intelligence Gathering** | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| **External Penetration Testing** | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| **Internal Penetration Testing** | | |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

The above section includes the observations and vulnerabilities in the order they were observed to provide mode value to the client in case of having in-house security assessment team replicate the issues in the order they occurred. However, it is not necessary to follow the order, each observation/vulnerability can be treated separately and independent of each other as well.

# **Assessment Details**

# **Open Source Intelligence Gathering (OSINT)**

This section includes all the observations **<Project-KillChain>** team has observed when performing Open-Source Intelligence gathering on the single public facing application. The observations details in this section might not be a vulnerability inherently, however, can lead to several vulnerabilities when combined. Thus, it is recommended to follow the recommendations as provided for each observation.

# **Vulnerability Name 1 INFO**

<Add Description Here>

**Recommendation**

* <Add Recommendation Here>

# **Vulnerability Name 2 MEDIUM**

<Add Description Here>

**Recommendation**

* <Add Recommendation Here>

# **External Penetration Testing**

This section includes all the observations/vulnerabilities **<Project-KillChain>** team has observed and exploited as a single or in combination externally to gain authorized/unauthorized access to the public facing assets within the scope (**<IP Address/CIDR Scope>**).

# **Vulnerability Name 1 MEDIUM**

<Add Description Here>

**Recommendation**

* <Add Recommendation Here>

# **Vulnerability Name 2 HIGH**

<Add Description Here>

**Recommendation**

* <Add Recommendation Here>

# **Internal Penetration Testing**

This section includes all the observations/vulnerabilities **<Project-KillChain>** team has observed and exploited as a single or in combination after gaining access to the internal system, pivoting and exploiting interconnected systems as the system exploited in external penetration testing was observed to be connected to internal network over “**<SCOPE>**”.

# **Vulnerability Name 1 HIGH**

<Add Description Here>

**Recommendation**

* <Add Recommendation Here>

# **Vulnerability Name 2 HIGH**

<Add Description Here>

**Recommendation**

* <Add Recommendation Here>