OuiCroissant

**Penetration Testing Report**

**Month Day, Year**

**{{TEAM}}**

**Confidentiality Notice**

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to OuiCroissant or facilitate attacks against OuiCroissant. {{TEAM}} shall not be held liable for special, incidental, collateral, or consequential damages arising out of the use of this information.

**Disclaimer**

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on OuiCroissant’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

**Document Control Details**

Company: OuiCroissant

Version: 1.0

Last Edited: MONTH DAY, YEAR

Prepared By: {{TEAM}}

Classification: Confidential

**Document Recipients**

{{NAME, TITLE - MONTH DAY, YEAR}}

**Table of Contents**

Executive Summary 4

Assessment Overview 5

Scope 5

Network Topology 5

Testing Methodology 6

Engagement Narrative 7

Key Security Strengths 8

Key Findings & Recommendations 8

Compliance 9

Assessment Findings Summary 10

Assessment Findings Details 11

C1. Critical Vulnerability 11

H1. High Vulnerability 12

M1. Medium Vulnerability 13

L1. Low Vulnerability 13

I1. Info Vulnerability 15

Appendix A: Risk Matrix & Classifications 17

Risk Matrix 17

Classification Definitions & Scales 17

Impact 17

Likelihood 18

Remediation 18

Appendix B: Network Details 19

Corporate Network 19

User Network 19

Train Network 19

Guest Network 19

Appendix C: Tools Used 20

Appendix D: Reference Links 21

# Executive Summary

{{TEAM}} performed a penetration test on OuiCroissant’s network(s) on MONTH DAY, YEAR. The penetration test simulated an attack of an internal threat actor attempting to gain access to OuiCroissant network systems. The purpose of the penetration test was to discover network strengths, vulnerabilities, and suggest remediations to improve COMPANY’s cybersecurity posture.

{{TEAM}} identified strengths including STRENGTH 1, STRENGTH 2, and STRENGTH 3. These strengths improved security across various points of the tested network.

{{TEAM}} identified a total of {{NUM-VULNS}} vulnerabilities within the scope of the engagement, which are broken down by severity in the table below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Critical** | **High** | **Medium** | **Low** | **Informational** |
| **#** | **#** | **#** | **#** | **#** |

Overall risk rating summary

Paragraph about critical vulnerabilities…

Paragraph about compliance….

Key opportunities for improvement….

# Assessment Overview

## Scope

The scope of this penetration testing assessment included…

Internal testing was done during the testing window of {{TEST-DATES}}

|  |  |
| --- | --- |
| **IP Address/Host/URL** | **Description** |
|  |  |

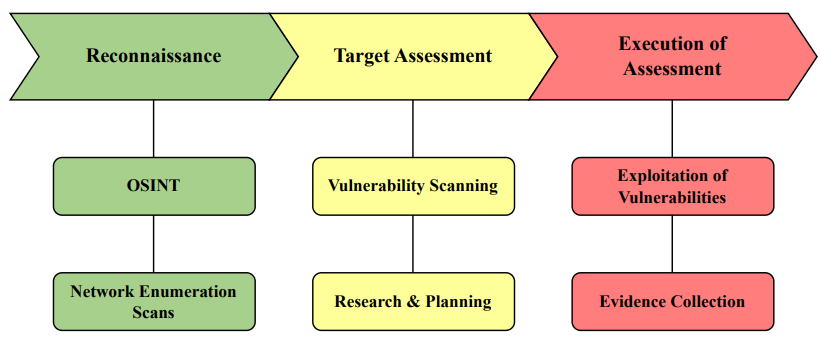
Provided Credentials

|  |  |
| --- | --- |
| **Username** | **Description** |
|  |  |

## Network Topology

## Testing Methodology

{{TEAM}}’s testing methodology had three main phases - reconnaissance, target assessment, and execution of assessment. Reconnaissance involved conducting Open-Source Intelligence (OSINT) research to gather publicly available information about OuiCroissant and network enumeration scans to gather information on available hosts and the network topology. The consultants used tools such as Nmap to identify systems and service versions of hosts and applications on the networks. Manual vulnerability scans were also conducted during the target assessment phase. For execution of assessment, the consultants used tools such as Burp Suite, Metasploit, and Hydra to find and exploit vulnerabilities. The diagram below shows a visual representation of the testing methodology the consultants followed throughout the penetration test.



## Engagement Narrative

## Key Security Strengths

1. STRENGTH 1



1. STRENGTH 2



1. STRENGTH 3

## Key Findings & Recommendations

1. FINDING 1



1. FINDING 2



1. FINDING 3

# Compliance

# Assessment Findings Summary

The risk matrix for severity level and the classification definitions and scales for likelihood, impact, and remediation can be found in Appendix A.

During the penetration test, {{TEAM}} uncovered a total of {{NUM-NON-INFO}} findings that pose a material risk to OuiCroissant’s information systems. {{TEAM}} also identified {{NUM-INFO}} informational findings that, if addressed, could further strength OuiCroissant’s overall security posture. The informational findings do not represent security vulnerabilities on their own, they are observations for areas of improvement by the organization. The below table provides a summary of the findings by severity level.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Critical** | **High** | **Medium** | **Low** | **Informational** |
| **#** | **#** | **#** | **#** | **#** |

The below table provides a high-level overview of each finding identified during testing. These findings are covered in depth in the Assessment Findings Details section of this report.

|  |  |  |  |
| --- | --- | --- | --- |
| **Identifier** | **Severity Level** | **Finding Name** | **Page #** |
| C1 | Critical |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Assessment Findings Details

This section provides a detailed description for each finding uncovered during the penetration test of OuiCroissant’s information systems. The findings are organized based on severity level (Critical, High, Medium, Low, Informational).

The risk matrix for severity level and the classification definitions and scales for likelihood, impact, and remediation can be found in Appendix A.

1. Critical Vulnerability

|  |  |
| --- | --- |
| **Critical Risk** | |
| **Likelihood** | Possible |
| **Impact** | Severe |
| **Remediation** | Medium |

Description:

Description of vulnerability

Steps to Reproduce:

*<How you determined there was a vulnerability, what you saw, proof of concept>*

Risk Assessment:

Summary of risk level

Business Impact:

Impact on business

Remediation Recommendations:

Remediation things

References:

References here

Instances:

|  |  |
| --- | --- |
| **System** | **Details** |
| DC01.example.com:445 | PetitPotam |
| WK01.example.com:445 | EternalBlue |

**Figure 1**: A php webshell uploaded to XYZ Application

!/usr/bin/python3

def meow():

print(“meow”)



**Figure 2**: A php webshell uploaded to XYZ Application

1. High Vulnerability

|  |  |
| --- | --- |
| **High Risk** | |
| **Likelihood** | Possible |
| **Impact** | Severe |
| **Remediation** | Medium |

Description:

Description of vulnerability

Steps to Reproduce:

How you determined there was a vulnerability, what you saw, proof of concept

Risk Assessment:

Summary of risk level

Business Impact:

Impact on business

Remediation Recommendations:

Remediation things

References:

References here

Instances:

|  |  |
| --- | --- |
| **System** | **Details** |
| DC01.example.com:445 | PetitPotam |
| WK01.example.com:445 | EternalBlue |

1. Medium Vulnerability

|  |  |
| --- | --- |
| **Medium Risk** | |
| **Likelihood** | Possible |
| **Impact** | Severe |
| **Remediation** | Medium |

Description:

Description of vulnerability:

Steps to Reproduce:

How you determined there was a vulnerability, what you saw, proof of concept

Risk Assessment:

Summary of risk level

Business Impact:

Impact on business

Remediation Recommendations:

Remediation things

References:

References here

Instances:

|  |  |
| --- | --- |
| **System** | **Details** |
| DC01.example.com:445 | PetitPotam |
| WK01.example.com:445 | EternalBlue |

1. Low Vulnerability

|  |  |
| --- | --- |
| **Low Risk** | |
| **Likelihood** | Possible |
| **Impact** | Severe |
| **Remediation** | Medium |

Description:

Description of vulnerability

Steps to Reproduce:

*[How you determined there was a vulnerability, what you saw, proof of concept]*

Risk Assessment:

Summary of risk level

Business Impact:

Impact on business

Remediation Recommendations:

Remediation things

References:

References here

Instances:

|  |  |
| --- | --- |
| **System** | **Details** |
| DC01.example.com:445 | PetitPotam |
| WK01.example.com:445 | EternalBlue |

1. Info Vulnerability

|  |  |
| --- | --- |
| **Informational Risk** | |
| **Likelihood** | Possible |
| **Impact** | Severe |
| **Remediation** | Medium |

Description:

Description of vulnerability

Steps to Reproduce:

*[How you determined there was a vulnerability, what you saw, proof of concept]*

Risk Assessment:

Summary of risk level

Business Impact:

Impact on business

Remediation Recommendations:

Remediation things

References:

References here

Instances:

|  |  |
| --- | --- |
| **System** | **Details** |
| DC01.example.com:445 | PetitPotam |
| WK01.example.com:445 | EternalBlue |

# 

# Appendix A: Risk Matrix & Classifications

## Risk Matrix

{{TEAM}} utilized the following 3x3 risk matrix for determining the severity level of each finding uncovered during the assessment. After determining the impact and likelihood classifications for the finding, they are used to select the appropriate severity level based on the risk matrix.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **Impact** | | |
|  |  | Severe | Moderate | Minor |
| **Likelihood** | Likely | Critical | High | Medium |
| Possible | High | Medium | Low |
| Unlikely | Medium | Low | Informational |

## Classification Definitions & Scales

{{TEAM}} utilized the following definitions and scales for classifying impact, likelihood, and remediation for each finding.

### Impact

**Definition:** With respect to security, the effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States), such as the loss of confidentiality, integrity, or availability of information or a system. With respect to privacy, the adverse effects that individuals could experience when an information system processes their PII.

|  |  |
| --- | --- |
| **Scale** | **Description** |
| Severe | Successful exploitation of the vulnerability may result in wide-spread disruption of critical business functions and significant financial damage. |
| Moderate | Successful exploitation of the vulnerability may cause significant disruptions to non-critical business functions. |
| Minor | Successful exploitation of the vulnerability may affect a few users without causing much disruption to routine functions. |

### Likelihood

**Definition:** A weighted factor based on a subjective analysis of the probability that a given threat can exploit a given vulnerability or a set of vulnerabilities.

|  |  |
| --- | --- |
| **Scale** | **Description** |
| Likely | Exploitation methods are well-known and can be performed with minimal difficulty using publicly available tools. |
| Possible | Exploitation methods are well-known and may be performed using public tools with configuration changes. Understanding of the underlying system is required for successful exploitation. |
| Unlikely | Exploitation requires deep understanding of the underlying system or advanced technical skills. Precise conditions may be required for successful exploitation. |

### Remediation

**Definition:** The act of mitigating a vulnerability or a threat.

|  |  |
| --- | --- |
| **Scale** | **Description** |
| Hard | Remediation may require extensive reconfiguration of the underlying systems and disruption of normal business functions. |
| Medium | Remediation may require minor reconfigurations or additions that may be time-intensive or expensive. |
| Easy | Remediation may be accomplished within a short amount of time and with little difficulty. |

# 

# Appendix B: Network Details

## Corporate Network

|  |  |  |  |
| --- | --- | --- | --- |
| **IP Address** | **FQDN** | **Port(s)** | **Services** |
|  |  |  |  |
|  |  |  |  |

## Guest Network

|  |  |  |  |
| --- | --- | --- | --- |
| **IP Address** | **FQDN** | **Port(s)** | **Services** |
|  |  |  |  |
|  |  |  |  |

# 

# Appendix C: Tools Used

|  |  |
| --- | --- |
| **Name** | **Description** |
| [BloodHound](https://github.com/SpecterOps/BloodHound) | Active Directory attack path visualization tool |
| [Certipy](https://github.com/ly4k/Certipy) | Tool for Active Directory Certificate Services enumeration and abuse |
| [Chisel](https://github.com/jpillora/chisel) | HTTP Tunneling tool |
| [Gobuster](https://github.com/OJ/gobuster) | Directory/File, DNS and VHost enumeration tool |
| [Gowitness](https://github.com/sensepost/gowitness) | Web interface enumeration tool |
| [Impacket](https://github.com/fortra/impacket) | Collection of Python tools for working with network protocols |
| [NetExec](http://www.netexec.wiki) | Network service exploitation tool |
| [Nmap](https://nmap.org/) | Network scanning utility |
| [PEASS-ng](https://github.com/peass-ng/PEASS-ng) | Privilege escalation enumeration scanning scripts |
| [PetitPotam](https://github.com/topotam/PetitPotam) | POC exploit for CVE-2021-36942 |
| [Responder](https://github.com/lgandx/Responder) | Network response poisoning tool |
| [Sliver](https://github.com/BishopFox/sliver) | Command and control framework |
| [SSLscan](https://github.com/rbsec/sslscan) | SSL/TLS cipher scanning tool |
| [Zerologon](https://github.com/dirkjanm/CVE-2020-1472) | POC exploit for CVE-2020-1472 |

# 

# Appendix D: Reference Links

#FF7D7D – Red

#F4B08 – Orange

#FFFF9A – Yellow

#A8D08D – Green

#D9E2F3 – Blue

<https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing>

<https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_0/home?element=IA-5>