# 

| Cybersecurity |
| --- |
| Penetration Test Report Template |

MegaCorpOne

Penetration Test Report

**[Juice Full of Security], LLC**

# 

## Confidentiality Statement

This document contains confidential and privileged information from MegaCorpOne Inc. (henceforth known as MegaCorpOne). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

## Table of Contents

[Confidentiality Statement 2](#_30j0zll)

[Contact Information 4](#_1fob9te)

[Document History 4](#_3znysh7)

[Introduction 5](#_2et92p0)

[Assessment Objective 5](#_3dy6vkm)

[Penetration Testing Methodology 6](#_2s8eyo1)

[Reconnaissance 6](#_17dp8vu)

[Identification of Vulnerabilities and Services 6](#_3rdcrjn)

[Vulnerability Exploitation 6](#_26in1rg)

[Reporting 6](#_lnxbz9)

[Scope 7](#_35nkun2)

[Executive Summary of Findings 8](#_44sinio)

[Grading Methodology 8](#_z337ya)

[Summary of Strengths 9](#_3j2qqm3)

[Summary of Weaknesses 9](#_1y810tw)

[Executive Summary Narrative 10](#_4i7ojhp)

[Summary Vulnerability Overview 11](#_2xcytpi)

Vulnerability Findings [12](#_1ci93xb)

[MITRE ATT&CK Navigator Map 13](#_3whwml4)

# 

## Contact Information

| **Company Name** | [Juice Full of Security ], LLC |
| --- | --- |
| **Contact Name** | [Josh Welch] |
| **Contact Title** | Penetration Tester |
| **Contact Phone** | 555.224.2411 |
| **Contact Email** | [JoshWelch]@[juicesecurity].com |

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| Day 1 | 07/12/2022 | [Josh Welch] | Attacking the Web Application CTF |
| Day 2 | 07/14/2022 | [Josh Welch] | Attacking Rekall's Linux Servers |
| Day 3 | 07/16/2022 | [Josh Welch] | Attacking Rekall's Windows Servers |

# 

## Introduction

In accordance with MegaCorpOne’s policies, [Juice Full of Security], LLC (henceforth known as [JFS] conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks’ and systems’ security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices. The project was conducted on a number of systems on MegaCorpOne’s network segments by [JSF] during July of 2022.

For the testing, [JSF] focused on the following:

* Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
* Attempting to exploit vulnerabilities found and accessing confidential information that may be stored on systems.
* Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

### Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in MegaCorpOne’s web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

[JSF] used its proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

MegaCorpOne has outlined the following objectives:

Table 1: Defined Objectives

| **Objective** |
| --- |
| Find and exfiltrate any sensitive information within the domain. |
| Escalate privileges to domain administrator. |
| Compromise at least two machines. |

# 

## Penetration Testing Methodology

### Reconnaissance

[JSF] begins assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

### Identification of Vulnerabilities and Services

[JSF] uses custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain a perspective of the network security from a hacker’s point of view. These methods provide MegaCorpOne with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

### Vulnerability Exploitation

[JSF]’s normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. The exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or sensitive data.

### Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

### Scope

Prior to any assessment activities, MegaCorpOne, and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the MegaCorpOne POC to determine which network ranges are in-scope for the scheduled assessment.

It is MegaCorpOne’s responsibility to ensure that IP addresses identified as in-scope are actually controlled by MegaCorpOne and are hosted in MegaCorpOne-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

| **IP Address/URL** | **Description** |
| --- | --- |
| 172.16.117.0/16  MCO.local  \*.Megacorpone.com | MegaCorpOne internal domain, range, and public website |

# 

## Executive Summary of Findings

## 

### Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to 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 or partial threat to business processes.

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

Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:

Chart

Description automatically generated with medium confidence

## 

### Summary of Strengths

[JFS] While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within MegaCorpOne’s environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

* Rekall's Linux Servers
  + Website/ IP Scan
    - Strength: The Linux server shows minimal information that requires multiple scans, and even uses an outside port scan to get all information needed. This can make it harder for less skilled users to gain useful information to advance in the penetration assault.
  + Strut - CVE-2017-5638
    - The Strut file does contain sensitive information but to access this information one must have already gained access to the Linux Server admin account. even if a person does gain access to the account the must reroot the IP address that is connected to the server and gain root access to display the sensitive information.

### Summary of Weaknesses

[JFS] successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

* Web Application

Brute force attack

* + - Weakness: Password and login on Rekall Corporation website for “User” and “Admin” were both simple and repetitive to simple brute force. Site had no requirement on password’s character limit or character requirement when creating account.
    - Fix: Require a character limit and character requirement when making password and login info. Prohibit any user or admin to use the same login name as their password. Eliminate login for admin users on public websites and create a separate site/method for admins to log in.

Sensitive data exposure

* + - Weakness: Rekall Corporation website main site page that had sensitive data/information easily available to access with little to no work or security protecting it. Pages like “Robot.txt,” “About-Rekall.php,” and “Disclaimer.php” were easily accessible from either ‘Google searches,’ ‘Directory traversal,’ and even a ‘Curl Command.’
    - Fix: Detach the aforementioned page from being accessible from any page on the open website. If pages are unneeded in any respect, it is best to delete them all together to prevent any information being exposed.

XSS reflected

* + - Weakness: On every text field for Rekall Corporations website alouds easy XSS reflected commands and scripts to either access login information or load malicious code to gain control of functions/observe user. These commands can bring down the website to give the website malware that mined information from users and adminations.
    - Fix: Update the HTML of the website to secure these text fields and have at least industry standards for XSS protections. Also reduce the amount of text fields the Rekall Corporation website has to reduce the potential breach you may have on multiple web pages.
* Rekall's Windows Servers

Sensitive data exposure

* + - Weakness: The Rekall github page exposes password information that is accessible to anyone on the web. A simple google search alouds any person with to find a hash password that can be easily broken with any password cracker. This gives them access to MegaCorpone’s Windows server and allows them to pivot to other servers on the system.
    - Fix: Take down the Rekall github page from being accessible from the internet. it would be best to delete the page all together and change the password that is exposed.

## Executive Summary

Juice Full of Security conducted a comprehensive security assessment of MegaCorpOne’s, in order to determine existing vulnerabilities and establish the current level of security risk associated with the environment and the technologies in use. This assessment harnessed penetration testing techniques to provide MegaCorpOne’s management with an understanding of the risks and security posture of their corporate environment.

TEST SCOPE

The test scope for this engagement included three main components that were stress tested as if a real breach had occurred. The Web Application, Rekall's Linux Servers, and Rekall's Windows Servers were all tested to discover any insecure protocols, unsecured networks, or related security issues. Testing was performed July 12 – July 16, 2022. Additional days were utilized to produce the report. Testing was performed using industry-standard penetration testing tools and frameworks, including Burp Suite, Fierce, the Metasploit Framework, Nmap, Nessus Scan, OpenVAS, SQL Injections, Wireshark, and WPScan.

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Web Application: (Sensitive data exposure) | **Critical** |
| Web Application: (XSS reflected) | **Critical** |
| Web Application: (Brute force attack) | **High** |
| Rekall's Windows Servers: (Sensitive data exposure) | **Medium** |
| Rekall's Linux Servers: (Website/ IP Scan) | **Low** |
| Rekall's Linux Servers: (Strut - CVE-2017-5638) | **Low** |

The following summary tables represent an overview of the assessment findings for this penetration test:

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | (192.168.13.0/24), (172.22.117.0/24) |
| Ports | (Port 25/tcp), (Port 110tcp) |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical - 5** | 10 |
| **High - 4** | 4 |
| **Medium - 3** | 3 |
| **Low - 2** | 2 |

## Vulnerability Findings

### Weak Password on Public Web Application

**Risk Rating**: **Critical**

**Description**:

The site **vpn.megacorpone.com** is used to host the Cisco AnyConnect configuration file for MegaCorpOne. This site is secured with basic authentication but is susceptible to a dictionary attack. [JSF] was able to use a username gathered from OSINT in combination with a wordlist in order to guess the user’s password and access the configuration file.

**Affected Hosts**: vpn.megacorpone.com

**Remediation**:

* Fix: Require a character limit and character requirement when making password and login info. Prohibit any user or admin to use the same login name as their password. Eliminate login for admin users on public websites and create a separate site/method for admins to log in.
* Fix: Detach the aforementioned page from being accessible from any page on the open website. If pages are unneeded in any respect, it is best to delete them all together to prevent any information being exposed.
* Fix: Update the HTML of the website to secure these text fields and have at least industry standards for XSS protections. Also reduce the amount of text fields the Rekall Corporation website has to reduce the potential breach you may have on multiple web pages.

1. Web Application
   1. Brute force attack
      1. Weakness: Password and login on Rekall Corporation website for “User” and “Admin” were both simple and repetitive to simple brute force. Site had no requirement on password’s character limit or character requirement when creating account.
      2. Method: simply think of the most common password/phrases will allow access to users and admin accounts. Ex: A user username was [melina] this also was the user password as well. These simple passwords were also for the admin accounts as well.
   2. Sensitive data exposure
      1. Weakness: Rekall Corporation website main site page that had sensitive data/information easily available to access with little to no work or security protecting it. Pages like “Robot.txt,” “About-Rekall.php,” and “Disclaimer.php” were easily accessible from either ‘Google searches,’ ‘Directory traversal,’ and even a ‘Curl Command.’
      2. Method: Any person that has a common understanding of Google Dorking and what the inspect tool is can gain valuable information that is left on the website. Ex: search Site;Rekall Corporation robots.txt will return a text file that is still connected to the website.
   3. XSS reflected
      1. Weakness: On every text field for Rekall Corporations website alouds easy XSS reflected commands and scripts to either access login information or load malicious code to gain control of functions/observe user. These commands can bring down the website to give the website malware that mined information from users and adminations.
      2. Method: On any text field that is on the Rekall Corporation website entering a simple ‘scripted’ payload will give a pop-up alert. Ex [<script>alert("hi")</script>]. If a simple payload like this can get the desired response then a more complex and malicious payload can be entered to take down the website.

## MITRE ATT&CK Navigator Map

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that [JSF] used throughout the assessment.

Legend:

| **Critical - Red** |
| --- |
| **High - Orange** |
| **Medium - Yellow** |
| **Low - Green** |

Performed successfully

Failure to perform

[Pen-Testing Report Diagram](https://drive.google.com/file/d/1bUvyLwIOKCnFIdMb1MJ6DBSBfAiMh1Hh/view?usp=sharing)