# 

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

MegaCorpOne

Penetration Test Report

**[ShadowEntity], 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** | [ShadowEntity], LLC |
| --- | --- |
| **Contact Name** | [John Wallace] |
| **Contact Title** | Penetration Tester |
| **Contact Phone** | 555.224.2411 |
| **Contact Email** | JohnWallace@ShadowEntity.com |

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 03/06/2023 | John Wallace |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

## Introduction

In accordance with MegaCorpOne’s policies, ShadowEntity, LLC (henceforth known as S.E) 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 S.E during March of 2023.

For the testing, S.E 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 access 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.

S.E 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

S.E 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

S.E uses custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain 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

S.E’s normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the 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

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.

* Megacorpone hired ShadowEntity to perform a pentest to find weaknesses.
* Megacorpone does have a firewall in place.

### Summary of Weaknesses

S.E 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.

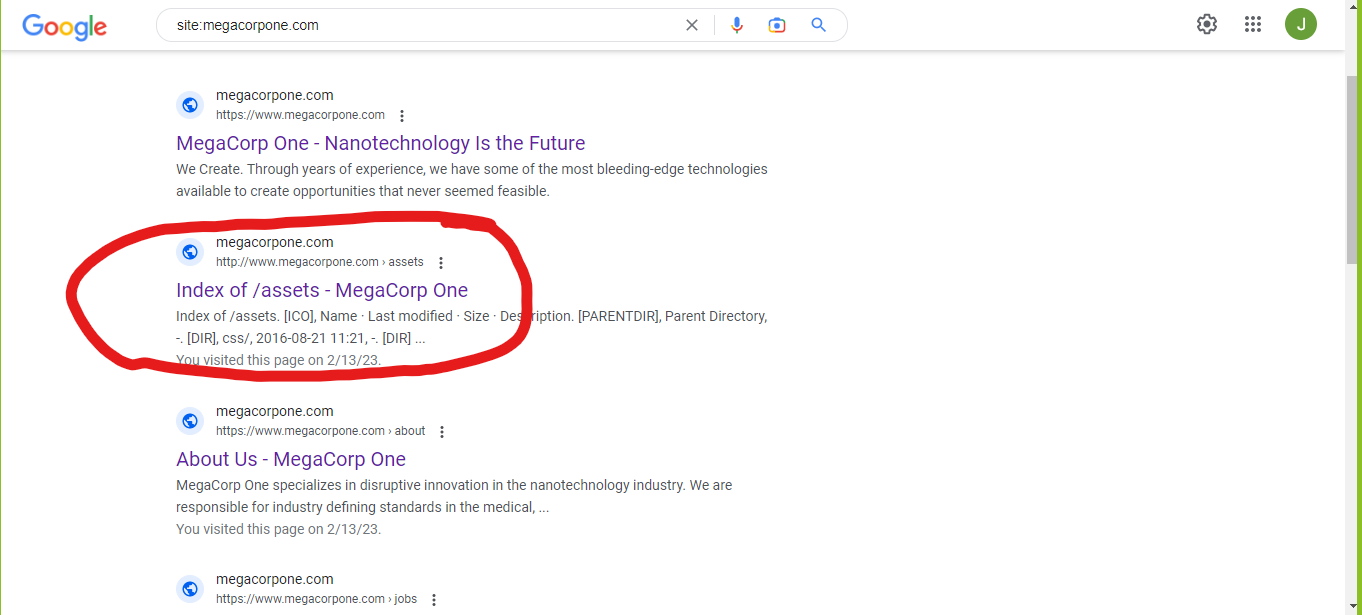
* Users and Servers have weak passwords
* Open Ports/Bind shell Backdoor

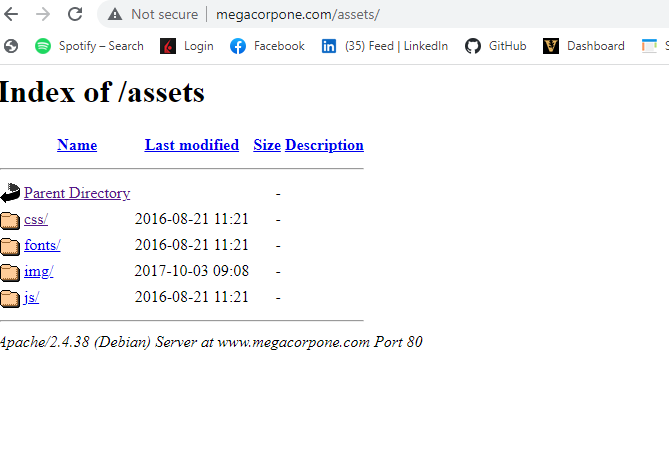
# 

## Executive Summary

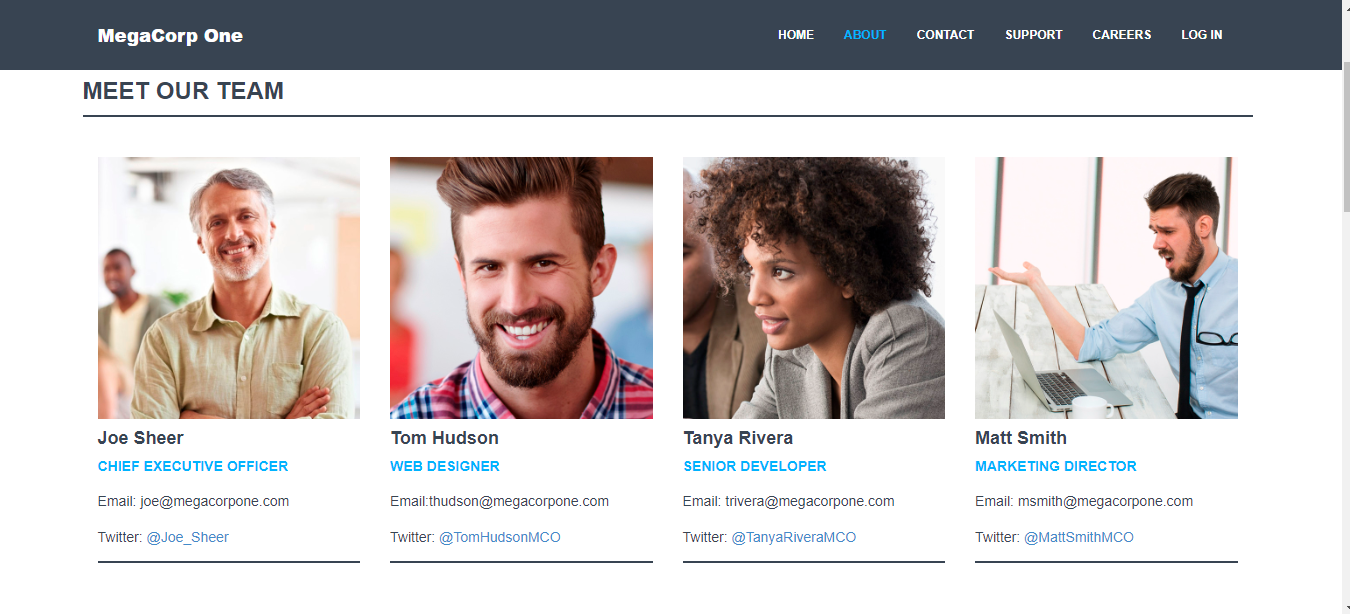
S.E has found several weaknesses within MegaCorpOne that need to be immediately remediated to prevent an attacker from gaining access to the network and its contents. We (S.E) were successfully able to scan for open ports and crack weak passwords, after which we used to gain initial access to Megacorpone’s network and then successfully escalated our privileges to the highest level (root).

**Reconnaissance**: **Google Dorking:**  I utilized Google specifically a technique called google dorking to unveil specific information about MegaCorpOne such as the assets file and Social Media handles of some of Megacorpone employees.

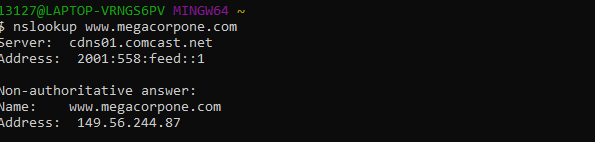
Assets file: 



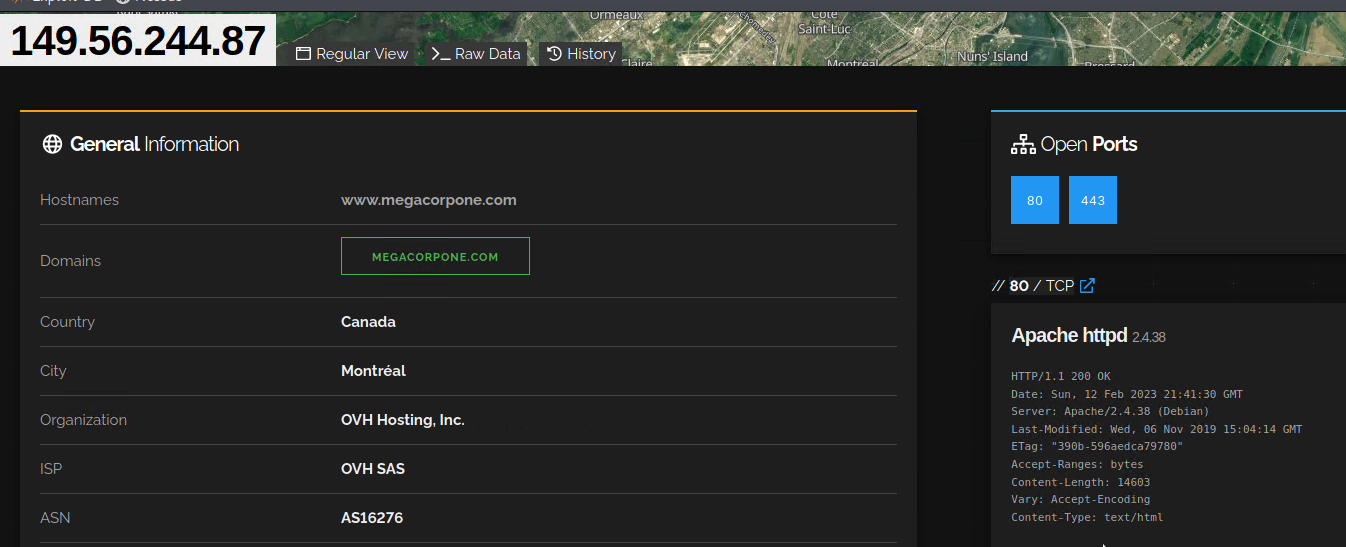
Socials Handles & Email Addresses:



Next I used **NSLOOKUP** to get the IP Address of MegaCorpOne shown below:



Next I used a public tool called [**Shodan.io**](https://www.shodan.io/) to reveal which ports are open, which Server and OS is being used, and the geolocation of the server. See image below for more details:



# Ports 80 and 443 are open.

# Server OS is Debian

# The webserver running is Apache version 2.4.38

# The server is located in Montreal, Canada

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Weak Password on Public Web Application | **Critical** |
| VSFTPD Bckdoor | **Critical** |
| Weak-Stored Password Policy | **Critical** |
| SSH-Key exchange | **Low** |
|  |  |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | Linux: 172.22.117.100  Windows: 172.22.117.20  WinDC10: 172.22.117.10 |
| Ports | Linux: 80, 5901, 6001, 8080  Windows: 135, 139, 445, 3390  WinDC10: 53, 88, 135, 139, 389, 445, 463, 493, 636, 3268, 3269 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 3 |
| **High** | 0 |
| **Medium** | 0 |
| **Low** | 1 |

## 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. S.E 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**:

* Set up two-factor authentication instead of basic authentication to prevent dictionary attacks from being successful.
* Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
* Reset the user **thudson**’s password.

**VSFTPD Backdoor**

**Risk Rating: Critical**

**Description:**

This attack utilizes a Metasploit Module (exploit/unix/ftp/vsftpd\_234\_backdoor). This module exploits a backdoor in vsftpd version 2.3.4 that allows an attacker to gain a reverse shell on the server.

**Remediation:**

* Replace/Update version vsftpd from 2.3.4.
* Change the passwords of all user accounts on the system, especially those that have FTP access.

**Weak Stored Password Policy**

**Risk Rating: Critical**

**Description:**

Upon gaining access to a shell on the company network, the “adminpasswork.txt” readable file was found inside the var/tmp directory. This isn’t necessarily an exploit but a lack of digital hygiene executed by the system administrators. Anyone who gains access to the network will be able to read this file thus gaining passwords.

**Remediation:**

* Implement security groups so that only people with the right credentials can access sensitive files.
* Hash the passwords so they aren’t human readable and add ‘salt’ to make them harder to crack.

**SSH-Key Exchange**

**Rating: Low**

**Description:**

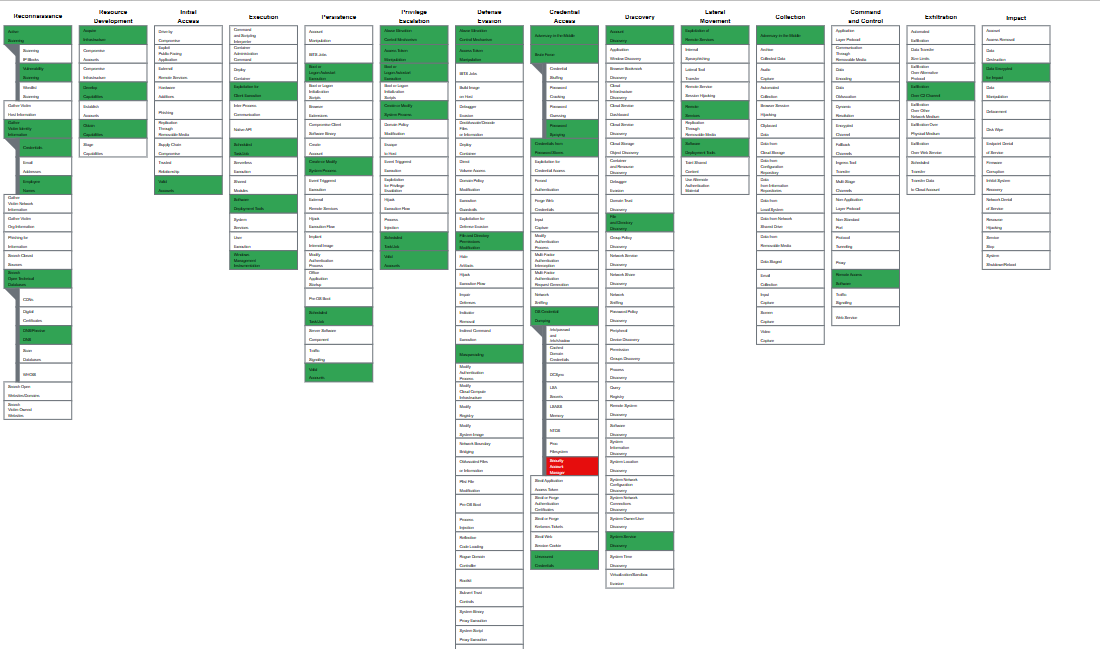
SSH Key Exchange can be exploited if there are vulnerabilities in the implementation of the protocol or if the encryption algorithm.

**Remediation:**

* Regenerate keys
* Disable/Restrict SSH access.

# 

## MITRE ATT&CK Navigator Map



Legend:

Performed successfully

Failure to perform