# 

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

MegaCorpOne

Penetration Test Report

**CYBROS, 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** | CYBROS, LLC |
| --- | --- |
| **Contact Name** | OMAR SANCHEZ |
| **Contact Title** | Penetration Tester |
| **Contact Phone** | 555.224.2411 |
| **Contact Email** | OMARSANCHEZ@CYBROS.com |

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 09/01/2024 | OMAR SANCHEZ | V.1 TEST ONE |
| 002 | 10/01/24 | OMAR SANCHEZ | FINALIZED |
|  |  |  |  |
|  |  |  |  |

# 

## Introduction

In accordance with MegaCorpOne’s policies, CYBROS, LLC (henceforth known as [CB) 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 [CB

] during SEPTEMBER of 2024..

For the testing, [CB] 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.

CB] 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

CB 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

CB 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

CB’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.

* Email Security Awareness: User email formats were found, but no personal information or sensitive data was exposed through them.
* Limited Public Data Exposure: MegaCorpOne has taken steps to restrict sensitive information online. Many pages retrieved through targeted searches lacked exploitable data, showing efforts to control publicly accessible content.
* Server Location: Although the server is located in Montreal, Canada, MegaCorpOne uses generic naming conventions for its assets, making it harder for attackers to deduce sensitive infrastructure details.
* Segmentation of Hidden Pages: The hidden /nanites.php page appeared isolated from the main web infrastructure.

### Summary of Weaknesses

CB 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.

* Outdated Apache Web Server: The Apache version 2.4.38 used on MegaCorpOne’s website is outdated and has several known vulnerabilities.These issues could allow for remote code execution or privilege escalation if exploited.
* Unsecured SSH Version: The server's SSH version, OpenSSH\_7.9p1, is also outdated, with known security issues. This increases the risk of attackers exploiting these vulnerabilities to gain unauthorized access to the server.
* Exposed Usernames: The naming for emails they used first initial and last name and that makes it relatively easy for an attacker to guess the email addresses of other users within the organization. This could lead to targeted phishing campaigns or brute-force attempts on login portals.
* Hidden Directories Accessible Without Authentication: The robots.txt file exposed the existence of hidden directories, including /nanites.php. The lack of authentication on these directories could allow unauthorized access and further information gathering by an attacker.

# 

## Executive Summary

[Provide a narrative summary of your findings, step by step. Include screenshots. It’s fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A–Z summary of your assessment.]

Google Hacking Techniques: Our team used Google search techniques to gather information on MegaCorpOne's domain. megacorpone.com query revealed that the website runs Apache 2.4.38 on Debian, with known vulnerabilities like CVE-2019-0215. Some additional queries uncovered employee emails and a consistent naming convention.

Shodan Analysis: A DNS lookup and Shodan scan revealed open ports 22 (SSH), 80 (HTTP), and 443 (HTTPS). The server runs OpenSSH\_7.9p1 on Debian, with vulnerabilities such as CVE-2019-0220, and is located in Montreal, Canada.

Discovery of Hidden Directories: Searching for megacorpone.com led to a robots.txt file, exposing a hidden /nanites.php directory. While it did not contain sensitive data, its existence suggests other directories could be accessible.

Recon-ng Scans: Using Recon-ng, the team identified 151 hosts associated with MegaCorpOne, offering a deeper view of their network. Results were compiled into an HTML report.

Report and Documentation: All findings were documented with actionable recommendations, supported by screenshots of key steps like hidden directory discovery, Shodan results, and Recon-ng outputs.

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Weak password on public web application | **Critical** |
| EMPLOYEE DATA(EX: EMAILS) | **HIGH** |
| OLD SYSTEM DATA(USING OUTDATED SSH) | **HIGH** |
| OUTDATED APACHE SERVERS | **Critical/HIGH** |
|  |  |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 151 |
| Ports | 3 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 3 |
| **High** | 2 |
| **Medium** | 1 |
| **Low** | - |

## 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. [YOUR COMPANY NAME ABBREVIATED] 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.

[List any other vulnerabilities you found here. Feel free to go into as much detail (including technical detail) as you want.]

# 

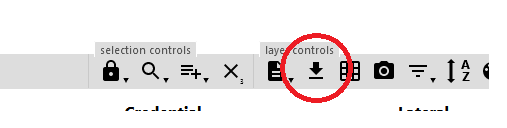
## MITRE ATT&CK Navigator Map

[Using the [MITRE ATT&CK Navigator](https://mitre-attack.github.io/attack-navigator/), build out a map showing what techniques you’ve used so far. To do so, on the MITRE ATT&CK Navigator page, click “Create New Layer,” then “Enterprise,” and select each technique that you’ve used. Change the color of each selected technique to highlight it in yellow if it was successful, or in red if it was unsuccessful, as the following image shows:

A picture containing text

Description automatically generated

When you’re done, be sure to download the chart as JSON by clicking the download icon, as the following image shows:



Remember, this report is not yet complete—we will finish it in the next module.

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

Legend:

Performed successfully

Failure to perform

[MITRE ATT&CK navigator map]