



Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

ShadowSecurity, 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
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	11
Vulnerability Findings	12
MITRE ATT&CK Navigator Map	13

Contact Information

Company Name	ShadowSecurity, LLC
Contact Name	EMILY RAPP
Contact Title	Penetration Tester
Contact Phone	530.588.1381
Contact Email	emilyrapp200@shadowsecuritycom

Document History

Version	Date	Author(s)	Comments
001	07/17/2023	EMILY RAPP	

Introduction

In accordance with MegaCorpOne's policies, ShadowSecurity, LLC (henceforth known as S.S) 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.S during June of 2021.

For the testing, S.S 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.S 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.S 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.S 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.S'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

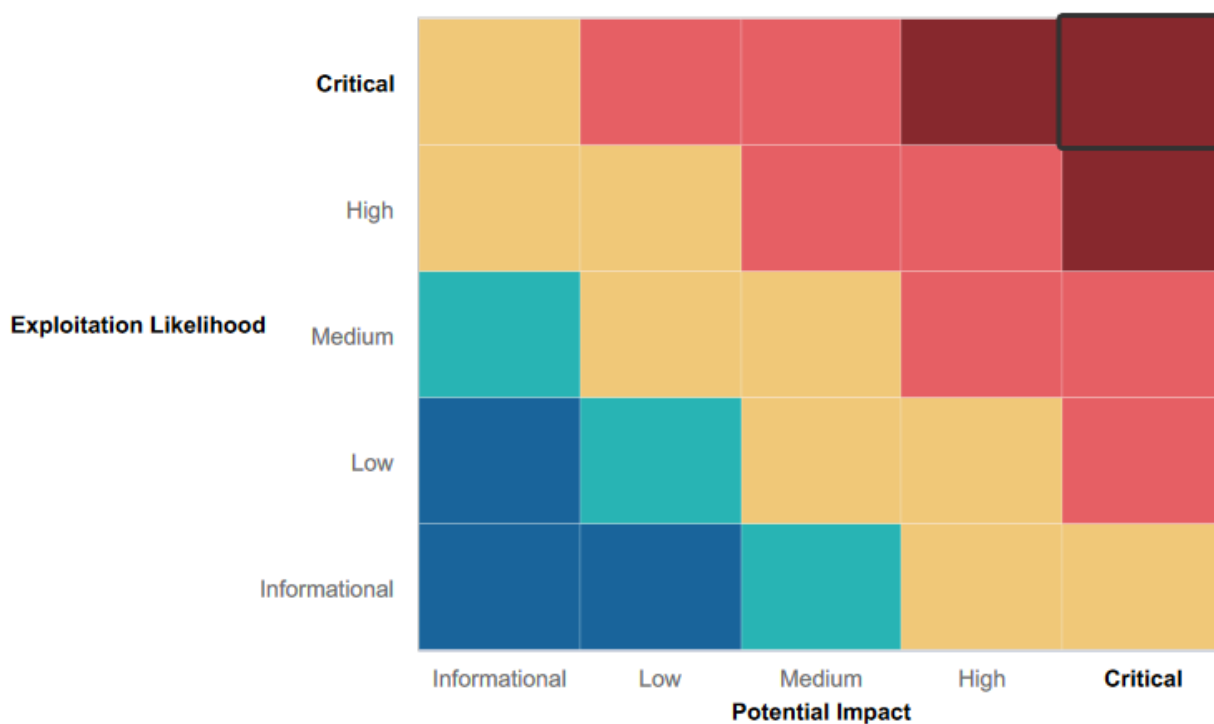
Executive Summary of Findings

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:



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.

- Hired PenTester
- Firewall in use

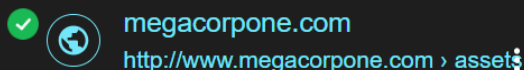
Summary of Weaknesses

S.S 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.

- Open ports
- Weak passwords/unsafe user accounts
- /assets file accessible by public

Executive Summary


Several critical weaknesses were found in my examination of the MegaCorpOne network. I used a process known as Google Dorking in order to find sensitive information regarding MegaCorpOne. Using the same technique allowed me to find user accounts (handles) of employees. From this, we can conclude that the OS is Debian, and it is running Apache version 2.4.38, which is not information that should be publicly available.



Index of /assets

Index of /assets. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [DIR], css/, 2016-08-21 11:21, -. [DIR] ...

Index of /assets

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 css/	2016-08-21 11:21	-	
 fonts/	2016-08-21 11:21	-	
 img/	2017-10-03 09:08	-	
 js/	2016-08-21 11:21	-	

Apache/2.4.38 (Debian) Server at www.megacorpone.com Port 80

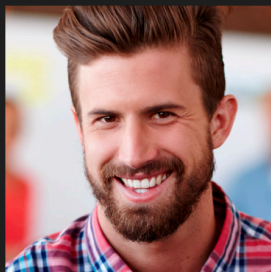
MEET OUR TEAM



Joe Sheer
CHIEF EXECUTIVE OFFICER

Email: joe@megacorpone.com

Twitter: [@Joe_Sheer](https://twitter.com/Joe_Sheer)



Tom Hudson
WEB DESIGNER

Email: thudson@megacorpone.com

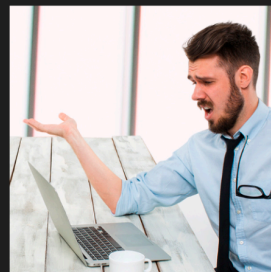
Twitter: [@TomHudsonMCO](https://twitter.com/TomHudsonMCO)



Tanya Rivera
SENIOR DEVELOPER

Email: trivera@megacorpone.com

Twitter: [@TanyaRiveraMCO](https://twitter.com/TanyaRiveraMCO)



Matt Smith
MARKETING DIRECTOR

Email: msmith@megacorpone.com

Twitter: [@MattSmithMCO](https://twitter.com/MattSmithMCO)

It is possible to retrieve the IP address of the MegaCorpOne website via Nmap

```
$ nslookup www.megacorpone.com
Server: UnKnown
Address: 100.64.100.1

Non-authoritative answer:
Name: www.megacorpone.com
Address: 149.56.244.87
```

Using this IP address, I used the service Shoden.io in order to view the websites open ports, location, OS, etc.

149.56.244.87 Regular View Raw Data

General Information	
Hostnames	www.megacorpone.com
Domains	MEGACORPONE.COM
Country	Canada
City	Beauharnois
Organization	OVH Hosting, Inc.
ISP	OVH SAS
ASN	AS16276

Ports 21 (SSH)[found on recon-ng], 80 (HTTP) and 443 (HTTPS) are open
 Passwords & Usernames

Tstark Password!
 Pparker Spring2021
 Bbanner Winter2021-domain admin

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
Port 21 Open	Critical

Stored Admin Credentials	Critical
CVE	Medium
IP Address Exposure	Medium

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

Scan Type	Total
Hosts	Windows10: 172.22.117.20 Kali: 172.22.117.100 WinCD10: 172.22.117.10 www.megacorpone.com : 194.56.244.87
Ports	22, 80, 443, 445, 139, 3389, 21

Exploitation Risk	Total
Critical	3
High	-
Medium	2
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. **S.S** 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.

Port 21 Open

Risk Rating: Critical

Description:

Zenmap scans shows port 21 open on the Windows Machine. Known backdoor vulnerabilities via port 21 make this threat critical, hackers are able to establish ongoing access.

Affected Hosts: Windows Machine

Remediation:

- Close Port 21

Admin Credential Storage

Risk Rating: Critical

Description:

Using de-hashing software and lateral movement, we were able to locate the hashed passwords of admin level users. The passwords were extremely weak, allowing for quick cracking.

Affected Hosts: Linux Machine

Remediation:

- Improve password quality
- Password protect hashes

IP Address Exposure

Risk Rating: Medium

Description:

Via Recon-ng, we were able to reveal 3 NS IP's. This information is publicly accessible, and leaves the website vulnerable to hackers.

Affected Hosts: ns1, ns2, ns3.megacorpone.com

Remediation:

- Make IP's private, or ensure strong firewall protection

CVE

Risk Rating: Medium

Description:

Shoden.io allows us to see all of the CVE vulnerabilities on the apache servers.

<https://www.shodan.io/host/149.56.244.87#22>

Affected Hosts: Apache Servers

Remediation:

- Recommend hiring a professional to fix these publicly known vulnerabilities, as there are many, and while they are simple to find, we are not testing for them specifically.

MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully - Yellow

Failure to perform - Red

MITRE ATT&CK navigator map

