Slaton Security Services, LLC
Professional Information Security Services

Penetration Test Report

MegaCorp One

April 5, 2023

Slaton Security Services, LLC

101 Peachtree St.
Suite 100
Atlanta, GA 30318
United States of America

Tel: 1-404-999-1000
Fax: 1-404-999-1001
Email: info@hivesec.com
Web: https://www.Slatonsecurity.com

Table of Contents

Confidentiality Statement 4
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

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.

Contact Information

Company Name	Slaton Security Services, LLC
Contact Name	Anesha Slaton
Contact Title	Penetration Tester
Contact Phone	404-999-1000
Contact Email	anesha@slatonsecurity.com

Document History

Version	Date	Author(s)	Comments
001	31-Mar-2023	Anesha Slaton	First Draft
002	04-Apr-2023	Anesha Slaton	Initial Review
003	05-Apr-2023	Anesha Slaton	Final Review

Introduction

In accordance with MegaCorpOne's policies, Slaton Security, LLC (henceforth known as Slaton Security) 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 Slaton Security during March 2023.

For the testing, Slaton Security 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.

Slaton Security 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 the domain administrator.
Compromise at least two machines.

Penetration Testing Methodology

Reconnaissance

Slaton Security 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

Slaton Security 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

Slaton Security'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

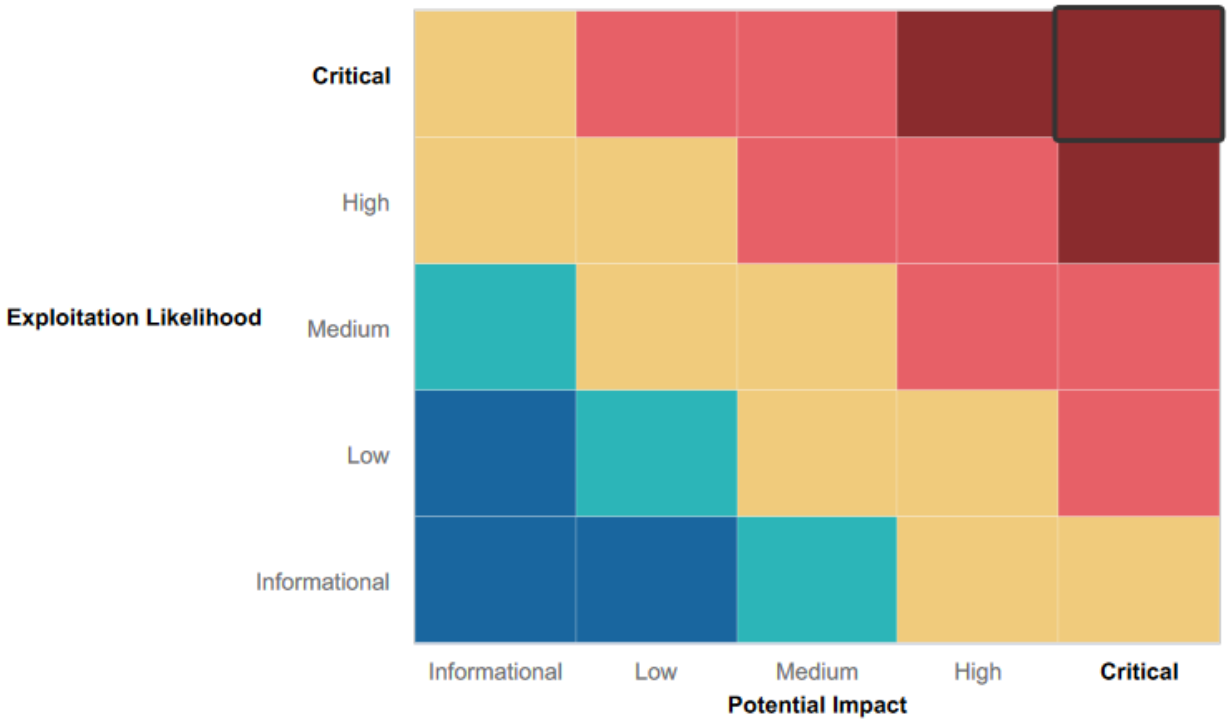
Executive Summary of Findings

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.

- MegaCorp One's cybersecurity strength is fortified by their robust password encryption practices, which provide a high level of protection to their sensitive data. This demonstrates their commitment to safeguarding against unauthorized access and maintaining the confidentiality of their information
- MegaCorp One's robust cybersecurity posture is evident in the successful implementation of a Virtual Private Network (VPN), which enhances their defenses against potential cyber attacks, demonstrating a proactive approach to safeguarding their network and data.
- During the reconnaissance of the wireless networks, it was observed that only a public facing wireless SSID was detected. Access to this service is granted through the creation of a user account with specific credentials. It is suspected that the SSID for the internal network is not being broadcast, rendering it invisible to external entities, presumably to enhance security measures within the organization.

Summary of Weaknesses

Slaton Security 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.

- During the reconnaissance phase, multiple known vulnerabilities were identified, along with open ports that were subsequently exploited as part of this engagement.
- Contact information for senior management is publicly accessible online. It is recommended to establish a central Point of Contact with the department's contact details made available to the public, ensuring streamlined and consistent communication channels.
- During the assessment, it was observed that login credentials were stored in text files with obvious labels, making them easily identifiable. Additionally, these credentials were found to lack complexity, making them vulnerable to cracking with minimal effort.

Executive Summary

Slaton Security Services, LLC performed a comprehensive security assessment on MegaCorp One to identify vulnerabilities and security risks within their approved network infrastructure, as outlined in the agreed scope of work. The assessment utilized penetration testing techniques to provide MegaCorp One's management with an understanding of the current risks and security posture of their corporate environment.

The assessment began with reconnaissance and host discovery of the internal network infrastructure using tools such as Zenmap for port scanning and OSINT (Open Source Intelligence) techniques to fingerprint the operating systems, software, and services running on each target host. Subsequently, the identified targets, open ports, and enabled services on each host were listed, followed by vulnerability enumeration to identify potential vulnerabilities affecting each host and develop a list of possible attack vectors.

The comprehensive testing revealed multiple vulnerabilities within the target host environment, which were exploited, resulting in compromise of the confidentiality, integrity, and availability of MegaCorp One's resources. The vulnerability testing uncovered Critical, High, and Medium severity issues impacting MegaCorp One's internal network, necessitating immediate remediation efforts to secure the company's environment against malicious threats.

The overall assessment of MegaCorp One indicates that they are not adequately prepared to defend against current attacks and should take prompt measures to address the findings presented in this report.

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
Open Ports on the Network	Critical
Exploiting and Privilege Escalation	Critical
Password Cracking	Critical
LLMNR Spoofing	Critical
Remote Access to compromised machines	Critical
Credential Dumping	High
Reverse Shell Vulnerability	High
Open Ports on Windows	High
Executive Level Contact Information on Company Website	Medium
Configuration Details within an Accessible File	Low

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

Scan Type	Total
Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.20 172.22.117.10 172.22.117.50
Ports	21 110 22 80 106 110

Exploitation Risk	Total
Critical	6
High	3
Medium	1

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. Slaton Security 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:

- Reset the user **thudson**'s password
- Set up MFA instead of basic authentication
- Set up strong password requirements such that there must be at least 10 characters that include upper+lower case, & include a special character.

Executive Level Contact Information on Website

Risk Rating: Medium

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. Slaton Security 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.

MEET OUR TEAM

Joe Sheer
CHIEF EXECUTIVE OFFICER
Email: joe@megacorpone.com
Twitter: @Joe_Sheer

Tom Hudson
WEB DESIGNER
Email:thudson@megacorpone.com
Twitter: @TomHudsonMCO

Tanya Rivera
SENIOR DEVELOPER
Email: trivera@megacorpone.com
Twitter: @TanyaRiveraMCO

Matt Smith
MARKETING DIRECTOR
Email: msmith@megacorpone.com
Twitter: @MattSmithMCO

Open Ports on Network

Risk Rating: Critical

Description:
A Zenmap scan showed vulnerable workstations with open ports that have potentially vulnerable applications running. Exploits include "21/tcp open ftp vsftpd".

CTK successfully gained access to the machine 172.22.117.150 and was able to open a shell to access the workstation.

Affected Hosts: megacorpone.com

Remediation:

- Close all unnecessary ports and set access rules
- Subscribe to various services that provide the latest CVE updates
- Perform regular vulnerability scanning
- Verify the current software is patched or replaced

Exploiting and Privilege Escalation

Risk Rating: Critical

Description:
Password management was insecure and vulnerable to exploits.

Affected Hosts: megacorpone.com

Remediation:

- Use an approved enterprise tool for password management.
- Create a whitelist of users and computers allowed to SSH into the server.
- Do not save files and folders on the computer with login credentials

LLMNR Spoofing

Risk Rating: Critical

Description:
A listener was initiated to spoof passwords. Additional credentials were captured.

Affected Hosts: megacorpone.com

Remediation:

Disable the LLMNR service

Remote Access to Compromised Machines

Risk Rating: Critical

Description:
Password management was insecure and vulnerable to exploits.

Affected Hosts: megacorpone.com

Remediation:

- Enable account creation and deletion logs
- Perform vulnerability assessments
- Configure strict user access policies

Open Ports on Windows

Risk Rating: High

Description:
There were two types of operating systems in play, Linux and Windows OS. The first scan showed 2 machines with open ports where there was a combined total of 15 open ports.

Affected Hosts: megacorpone.com

Remediation:

- Enable account creation and deletion logs
- Perform vulnerability assessments
- Configure strict user access policies

Reverse Shell Vulnerability

Risk Rating: High

Description:
A listener was initiated for the reverse shell to establish a Meterpreter session to exploit.

Affected Hosts: megacorpone.com

Remediation:

- Perform scheduled patching of the web applications
- Remove unnecessary services

Credential Dumping

Risk Rating: High

Description:
A listener was initiated for the reverse shell to establish a Meterpreter session to exploit.

Affected Hosts: megacorpone.com

Remediation:

- Eliminate any old or unpatched systems
- Update the Endpoint Solution

Configuration Details with Accessible File

Risk Rating: Low

Description:
The access allowed for an attacker to identify which technology is running and exploits can be performed.

Affected Hosts: megacorpone.com

Remediation:

- Files should be configured to not allow specific access.

MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully
Failure to perform