



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
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	[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

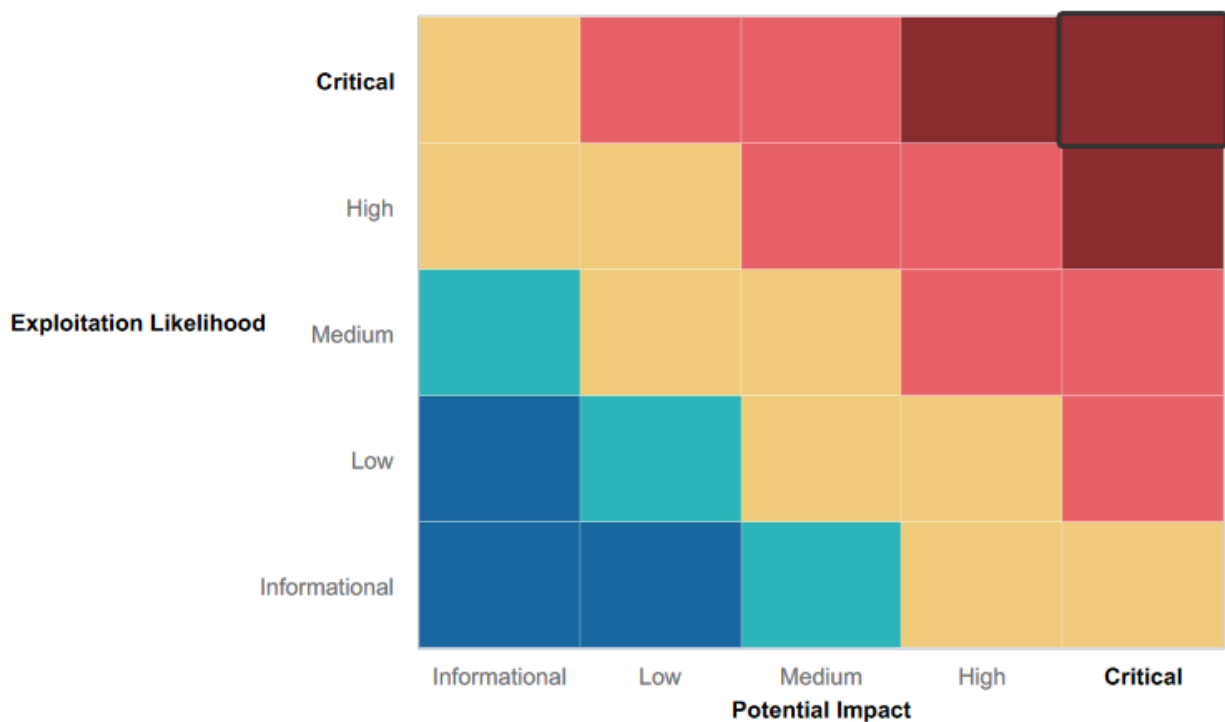
Executive Summary of Findings

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:



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.

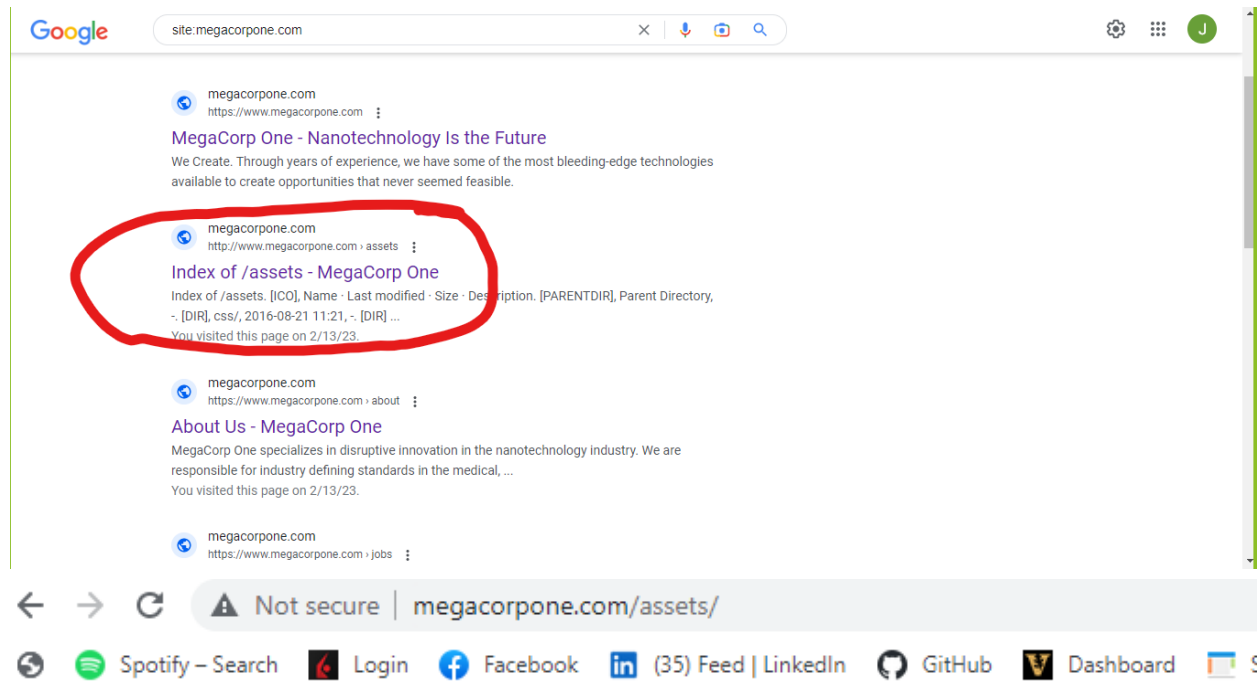
- Users and Servers have weak passwords
- Open Ports/Bind shell Backdoor

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:







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

Socials Handles & Email Addresses:

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
---	--	--	--

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

```
13127@LAPTOP-VRNGS6PV MINGW64 ~  
$ nslookup www.megacorpone.com  
Server: cdns01.comcast.net  
Address: 2001:558:feed::1  
  
Non-authoritative answer:  
Name: www.megacorpone.com  
Address: 149.56.244.87
```

Next I used a public tool called [Shodan.io](https://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:

149.56.244.87 Regular View Raw Data History

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

Open Ports

80 443

// 80 / TCP

Apache httpd 2.4.38

HTTP/1.1 200 OK
Date: Sun, 12 Feb 2023 21:41:30 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390b-596aedca79780"
Accept-Ranges: bytes
Content-Length: 14603
Vary: Accept-Encoding
Content-Type: text/html

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 "adminpassword.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.

[illegible]

	Performed successfully	Failure to perform
1. The patient was able to follow instructions.	Yes	No
2. The patient was able to understand the information provided.	Yes	No
3. The patient was able to complete the task without assistance.	Yes	No
4. The patient was able to maintain focus throughout the activity.	Yes	No
5. The patient was able to demonstrate appropriate social interaction skills.	Yes	No
6. The patient was able to manage emotions during the activity.	Yes	No
7. The patient was able to communicate effectively with others.	Yes	No
8. The patient was able to handle frustration or setbacks gracefully.	Yes	No
9. The patient was able to work independently or collaboratively as required.	Yes	No
10. The patient was able to adhere to rules and guidelines.	Yes	No
11. The patient was able to show respect for others' personal space and belongings.	Yes	No
12. The patient was able to engage in conversation appropriately.	Yes	No
13. The patient was able to express their needs and desires clearly.	Yes	No
14. The patient was able to listen actively to others.	Yes	No
15. The patient was able to take turns during group activities.	Yes	No
16. The patient was able to resolve conflicts peacefully.	Yes	No
17. The patient was able to show empathy towards others.	Yes	No
18. The patient was able to demonstrate self-control and impulse management.	Yes	No
19. The patient was able to show initiative and creativity.	Yes	No
20. The patient was able to persevere through challenges.	Yes	No
21. The patient was able to seek help when needed.	Yes	No
22. The patient was able to show gratitude and appreciation.	Yes	No
23. The patient was able to follow safety protocols.	Yes	No
24. The patient was able to show responsibility for their actions.	Yes	No
25. The patient was able to participate willingly in all activities.	Yes	No
26. The patient was able to show leadership qualities.	Yes	No
27. The patient was able to adapt to changes in the environment.	Yes	No
28. The patient was able to show resilience in the face of adversity.	Yes	No
29. The patient was able to show respect for cultural differences.	Yes	No
30. The patient was able to show respect for authority figures.	Yes	No
31. The patient was able to show respect for personal boundaries.	Yes	No
32. The patient was able to show respect for intellectual property rights.	Yes	No
33. The patient was able to show respect for environmental conservation.	Yes	No
34. The patient was able to show respect for animal welfare.	Yes	No
35. The patient was able to show respect for community resources.	Yes	No
36. The patient was able to show respect for public spaces.	Yes	No
37. The patient was able to show respect for digital privacy.	Yes	No
38. The patient was able to show respect for online communication norms.	Yes	No
39. The patient was able to show respect for workplace safety.	Yes	No
40. The patient was able to show respect for professional conduct.	Yes	No
41. The patient was able to show respect for academic integrity.	Yes	No
42. The patient was able to show respect for research ethics.	Yes	No
43. The patient was able to show respect for legal regulations.	Yes	No
44. The patient was able to show respect for contractual obligations.	Yes	No
45. The patient was able to show respect for financial responsibilities.	Yes	No
46. The patient was able to show respect for tax laws.	Yes	No
47. The patient was able to show respect for intellectual property rights.	Yes	No
48. The patient was able to show respect for patent laws.	Yes	No
49. The patient was able to show respect for trademark laws.	Yes	No
50. The patient was able to show respect for copyright laws.	Yes	No
51. The patient was able to show respect for trade secret laws.	Yes	No
52. The patient was able to show respect for contract law.	Yes	No
53. The patient was able to show respect for tort law.	Yes	No
54. The patient was able to show respect for criminal law.	Yes	No
55. The patient was able to show respect for civil law.	Yes	No
56. The patient was able to show respect for family law.	Yes	No
57. The patient was able to show respect for probate law.	Yes	No
58. The patient was able to show respect for estate planning laws.	Yes	No
59. The patient was able to show respect for bankruptcy law.	Yes	No
60. The patient was able to show respect for consumer protection laws.	Yes	No
61. The patient was able to show respect for labor laws.	Yes	No
62. The patient was able to show respect for employment contracts.	Yes	No
63. The patient was able to show respect for non-compete clauses.	Yes	No
64. The patient was able to show respect for confidentiality agreements.	Yes	No
65. The patient was able to show respect for intellectual property laws.	Yes	No
66. The patient was able to show respect for patent infringement laws.	Yes	No
67. The patient was able to show respect for trademark infringement laws.	Yes	No
68. The patient was able to show respect for copyright infringement laws.	Yes	No
69. The patient was able to show respect for trade secret laws.	Yes	No
70. The patient was able to show respect for contract law.	Yes	No
71. The patient was able to show respect for tort law.	Yes	No
72. The patient was able to show respect for criminal law.	Yes	No
73. The patient was able to show respect for civil law.	Yes	No
74. The patient was able to show respect for family law.	Yes	No
75. The patient was able to show respect for probate law.	Yes	No
76. The patient was able to show respect for estate planning laws.	Yes	No
77. The patient was able to show respect for bankruptcy law.	Yes	No
78. The patient was able to show respect for consumer protection laws.	Yes	No
79. The patient was able to show respect for labor laws.	Yes	No
80. The patient was able to show respect for employment contracts.	Yes	No
81. The patient was able to show respect for non-compete clauses.	Yes	No
82. The patient was able to show respect for confidentiality agreements.	Yes	No
83. The patient was able to show respect for intellectual property laws.	Yes	No
84. The patient was able to show respect for patent infringement laws.	Yes	No
85. The patient was able to show respect for trademark infringement laws.	Yes	No
86. The patient was able to show respect for copyright infringement laws.	Yes	No
87. The patient was able to show respect for trade secret laws.	Yes	No
88. The patient was able to show respect for contract law.	Yes	No
89. The patient was able to show respect for tort law.	Yes	No
90. The patient was able to show respect for criminal law.	Yes	No
91. The patient was able to show respect for civil law.	Yes	No
92. The patient was able to show respect for family law.	Yes	No
93. The patient was able to show respect for probate law.	Yes	No
94. The patient was able to show respect for estate planning laws.	Yes	No
95. The patient was able to show respect for bankruptcy law.	Yes	No
96. The patient was able to show respect for consumer protection laws.	Yes	No
97. The patient was able to show respect for labor laws.	Yes	No
98. The patient was able to show respect for employment contracts.	Yes	No
99. The patient was able to show respect for non-compete clauses.	Yes	No
100. The patient was able to show respect for confidentiality agreements.	Yes	No