Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

Tullars Cyber Security, 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

Contact Information

Company Name	Tullars Cyber Security, LLC
Contact Name	Zackary Tullar
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	Ztullar@TCS.com

Document History

Version	Date	Author(s)	Comments
001	10/18/22	Zackary Tullar	Actions needed.

Introduction

In accordance with MegaCorpOne's policies, Tullars Cyber Security, LLC (henceforth known as TCS) 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 TCS during October of 2022.

For the testing, TCS 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.

TCS 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

TCS 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

TCS 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

TCS'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

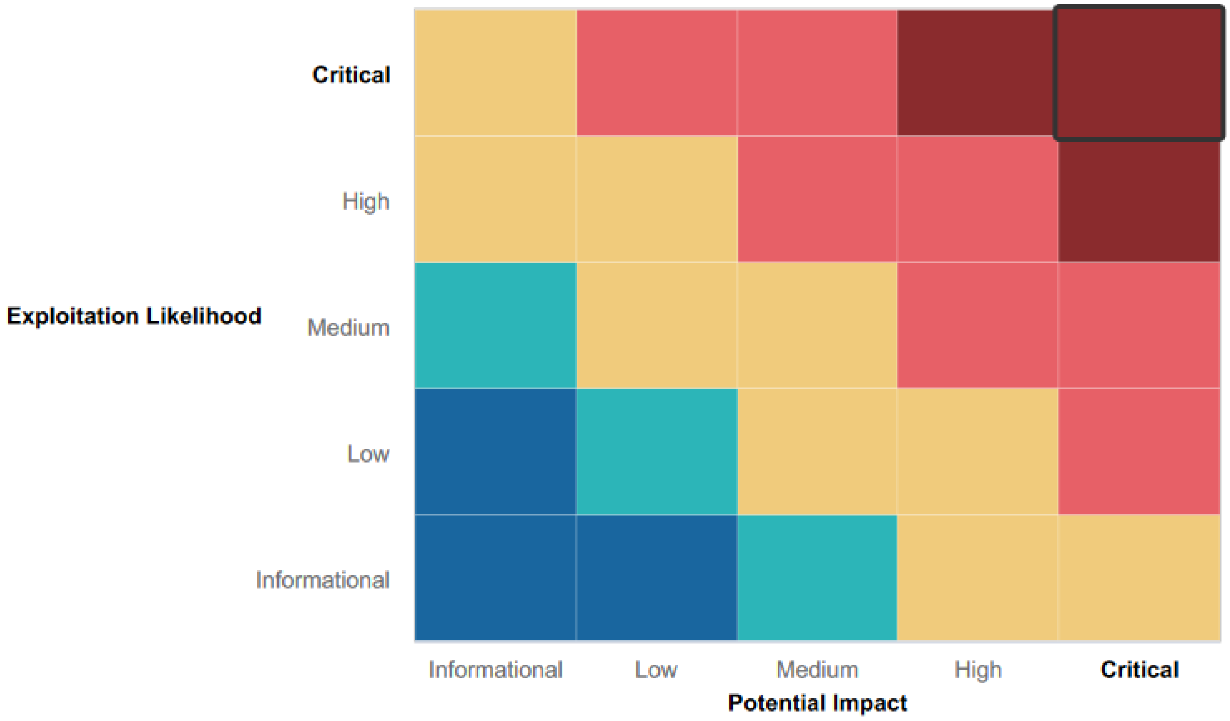
Executive Summary of Findings

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.

- During Reconnaissance we noticed there was only a public facing SSID you have to create an account in order to connect to the service. Which can prevent random people accessing the internal network.
- They have good security awareness. Each attempt to social engineer didnt work to find a weakness in their company.

Summary of Weaknesses

TCS 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.

- Higher level management has contact information available online. there should be a middle man that sets up contact with that level of management.
- Several open ports were found during reconnaissance revealing alot of vulnerabilities.
- login credentials were found within text files with no effort of hiding them. Login information was not complex and was easy to crack into.
- Network was easy to scan and there wasnt anything prohibiting it making it easy to see the network infrastructure.

Executive Summary

Starting with Google dorking we were able to find contact information for multiple employees of higher management. The public should not have information that sensitive and could possibly lead to a breach in that level of user accounts. Next we used Zenmap during reconnaissance to scan ports to map out the OS and software being used.

There was several Medium-Critical issues on MegaCorpOnes network. We were able to find and login to multiple accounts TStark, and Pparker both accounts were fairly easy to find the login information needed to access their accounts.

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
High level management contact information publicly online	Medium
known exploits from Shodan.io	Critical
Open ports on the network	Critical
Privilege Escalation	Critical
Password cracking	Critical
Open windows port	High
Password Spraying	High

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

Scan Type	Total
Hosts	172.22.117.20 172.22.117.100
Ports	21-ftp 22-ssh 53-domain 80-http 88-tcp

Exploitation Risk	Total
Critical	5
High	2
Medium	1
Low	0

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. TCS 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.

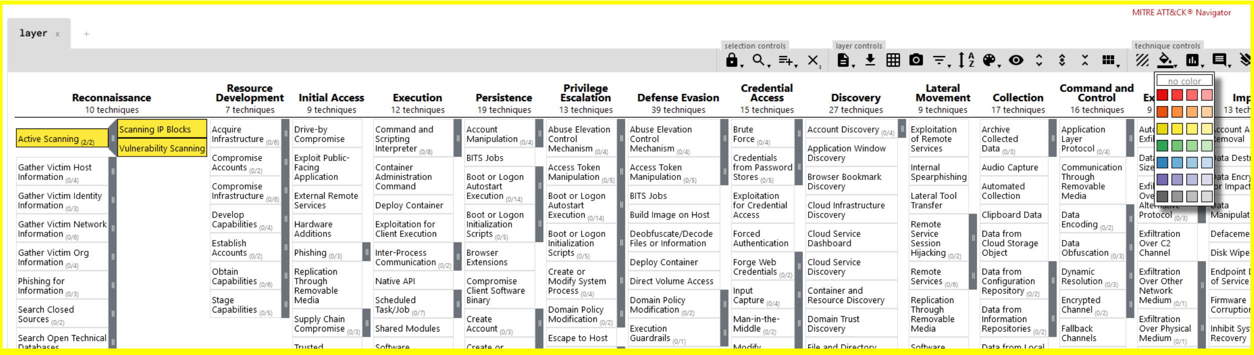
Affected Hosts: vpn.megacorpone.com

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.

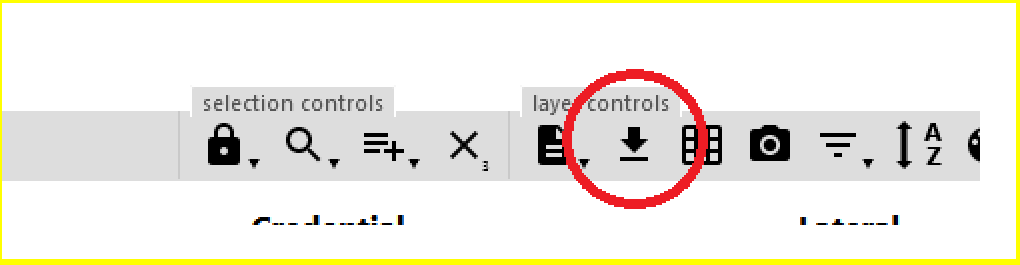
MITRE ATT&CK Navigator Map

[Using the MITRE ATT&CK 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:



Reconnaissance 10 techniques		Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Ex 9	Imp 13 tech
Active Scanning (2/2)	Scanning IP Blocks Vulnerability Scanning	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Aut Exfil	ccount A emoval
Gather Victim Host Information (0/4)		Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Dat Size	ata Destr
Gather Victim Identity Information (0/3)		Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfil Ove Alte Protocol (0/3)	ata Encry or Impact
Gather Victim Network Information (0/6)		Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulat
Gather Victim Org Information (0/4)		Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defaceme
Phishing for Information (0/3)		Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe
Search Closed Sources (0/2)		Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/7)	Create Account (0/3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (0/2)	Container and Resource Discovery	Software	Data from Information Repositories (0/2)	Fallback Channels		Endpoint of Service
Search Open Technical Databases			Trusted	Shared Modules	Create or		Domain Policy Modification (0/2)	Modify	Domain Trust Discovery		Data from Local			Firmware Corruption
				Software			Execution Guardrails (0/1)		File and Directory					Inhibit Sys Recovery

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]