Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

CYBER GUARD, 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	CYBER GUARD, LLC
Contact Name	Evan Boroff
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	evanboroff@cyberguard.com

Document History

Version	Date	Author(s)	Comments
001	07/11/2023	Evan Boroff	

Introduction

In accordance with MegaCorpOne's policies, Cyber Guard, LLC (henceforth known as "C.G."]) 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 C.G. during July of 2023.

For the testing, C.G. 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.

C.G. 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

C.G. 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

C.G. 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

C.G.'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

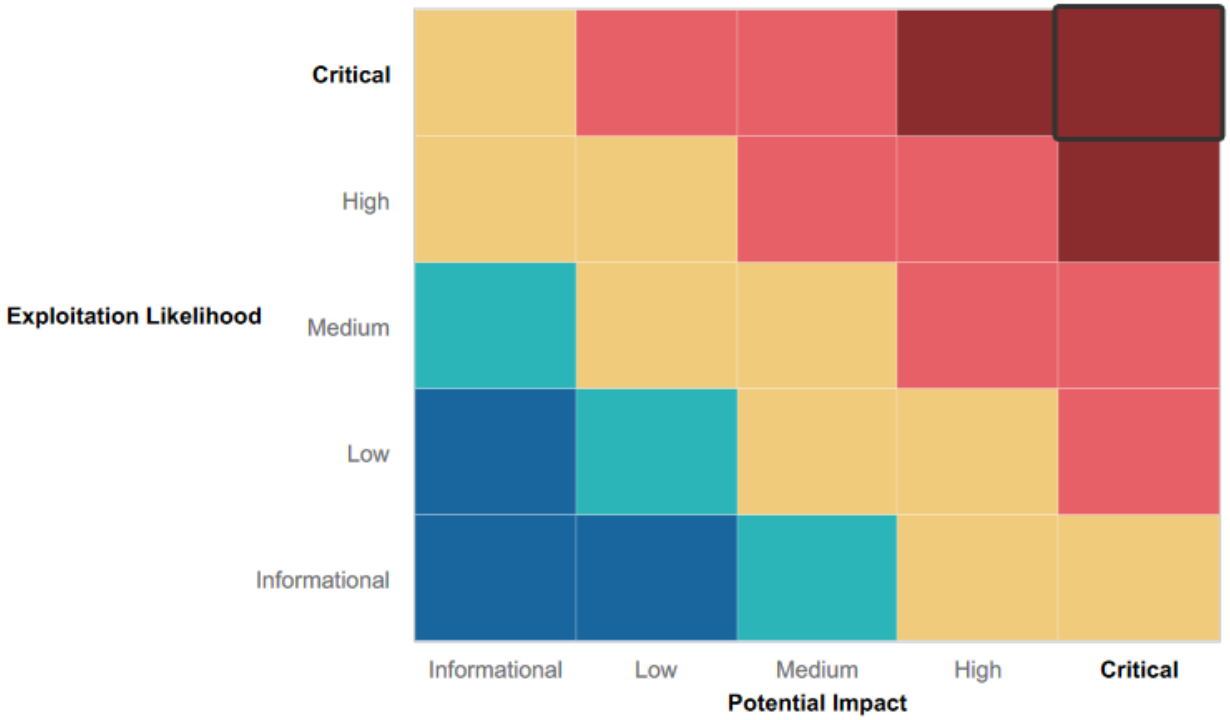
Executive Summary of Findings

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 has a firewall in place
-

Summary of Weaknesses

C.G. 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.

- All passwords on file are weak and could be hacked easily.
-

Executive Summary

C.G. found numerous weaknesses with MegaCorpOne that should be tended to as soon as possible to prevent infiltration into the company network and the contents within. We were able to crack on weak passwords, which allowed easy access to MegaCorpOne's network and then we were able to escalate privileges to root level, highest available privileges.

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
VSFTPD Backdoor	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 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, 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. C.G. 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 uses a Metasploit Module. 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 or update version vsftpd from 2.3.4.
- Change the passwords of all user accounts on the system.

Weak Stored Password Policy

Risk Rating: Critical

Description:
Once C.G. accessed a shell on the company network, the "adminpassword.txt" file was located in the var/tmp directory. This easily accessible file makes it easy to anyone trying to access the network and, therefore, will have access to passwords

Remediation:

- Implement individuals with clearance to access these sensitive files.
- Hash the passwords so they aren't readable to just anyone.

SSH-Key Exchange

Risk Rating: Low

Description:
SSH-Key Exchange can be exploited if there are any vulnerabilities in the implementation of the protocol or in the encryption algorithm.

Remediation:

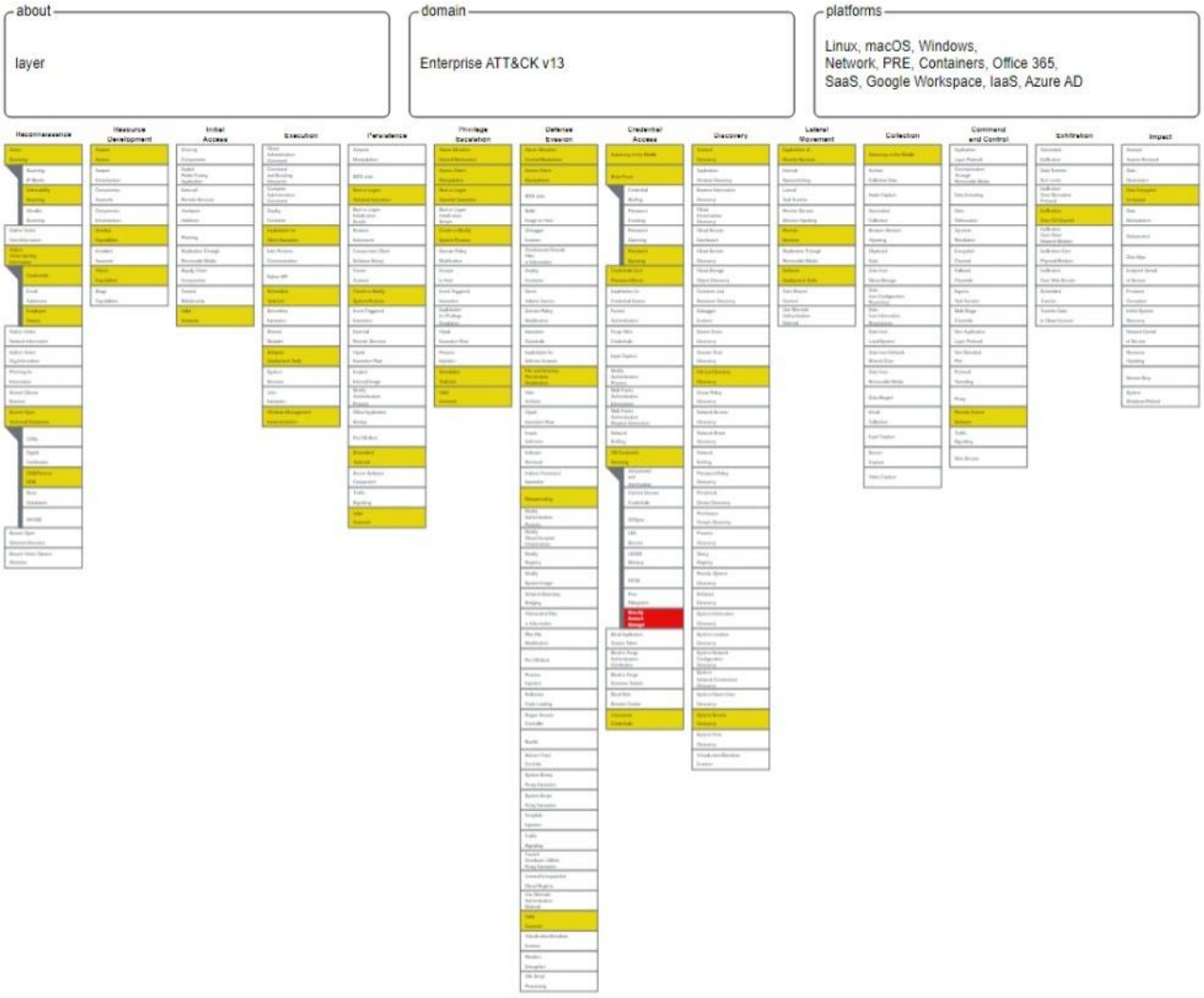
- Regenerate keys.
- Disable or restrict SSH access.

MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully
Failure to perform


about
layer
domain
Enterprise ATT&CK v13
platforms
Linux, macOS, Windows,
Network, PRE, Containers, Office 365,
SaaS, Google Workspace, IaaS, Azure AD
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact