Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report
Kelp 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	[Kelp Security], LLC
Contact Name	[Raul Rodriguez]
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	[Raul]@[KelpSec].com

Document History

Version	Date	Author(s)	Comments
001	01/01/2022	[Raul Rodriguez]	

Introduction

In accordance with MegaCorpOne's policies, Kelp Security, LLC (henceforth known as Kelp Sec] 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 [Kelp] during January of 2022.

For the testing, Kelp Sec 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.

[Kelp Sec] 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

Kelp Sec 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

Kelp Sec 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

Kelp Sec'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

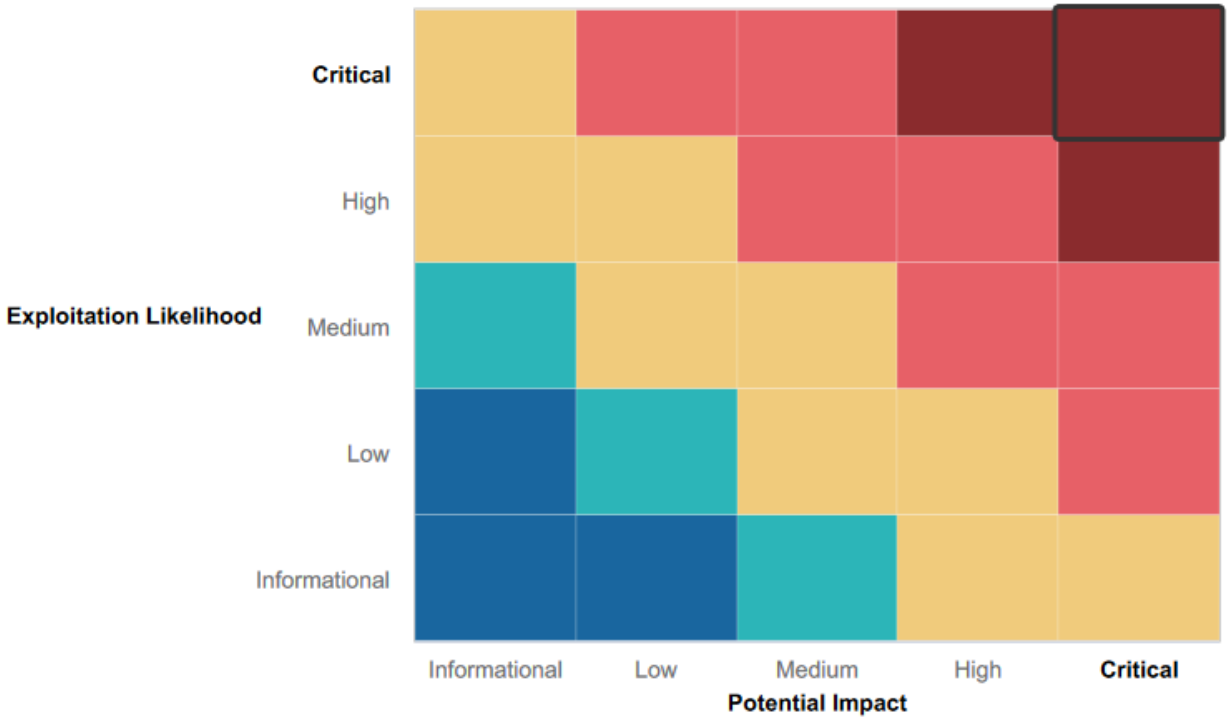
Executive Summary of Findings

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.

- [Everyone used different passwords]
- [MegaCorpOne realized it needed to hire security professionals to examine their network]

Summary of Weaknesses

Kelp Sec 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.

- [Passwords were able to be guessed using the season/year and variations of password/ usernames as the password]
- Using msfvenom show a lack of security measures such as updates and anti virus
- Password was able to be retrieved using an LLMNR attack show a weakness in the Windows OS

Executive Summary

In our assessment of the security of MegaCorpOne's network, we found several vulnerabilities that could lead to a significant financial loss if not addressed.

First, we found that many of the passwords used by the company were easily guessable. This means that an attacker could gain access to the company's systems without needing to use any sophisticated hacking techniques. This could lead to the theft of sensitive data.

Second, we found that the company's Windows servers were vulnerable to exploitation through LMMNR. This is a protocol that allows attackers to gain access to a system without needing to authenticate. Updates, disabling and antivirus would help secure the company's assets better in the future.

Third, We were able to gain access through credential dumping, basically is the dumping of sensitive information from a computer system, primarily passwords and usernames. This could be fixed with 2FA, regular password changes and active system monitoring. .

In conclusion, our assessment of MegaCorpOne's network security revealed several vulnerabilities that must be addressed to prevent potential financial and asset loss. The MegaCorpOne should implement strong password policies to prevent easily guessable passwords, apply updates and antivirus to protect against LMMNR protocol exploits, implement 2FA, regular password changes and active system monitoring to prevent credential dumping, and take adequate measures to protect their systems from potential attacks. Failure to address these issues could result in disastrous repercussions for the company.

Venom
https://drive.google.com/file/d/1ROvZlDbKwX7z5vYixW-cF5aOPd9WRc1f/view?usp=sharing
Cred Dump Results
https://drive.google.com/file/d/1r-Jtdkm7ppokK5Dh0yRpCMpf7Vv6NHHc/view?usp=sharing
Results of LMMNR
https://drive.google.com/file/d/1RjFdB9X6eIigtrlGf38q_eBMCeCPavYZ/view?usp=sharing

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
Credential Dump	High
MSF Venom	High
LMMNR	High

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

Scan Type	Total
Hosts	172.22.117.20
Ports	445 444

Exploitation Risk	Total
Critical	1
High	3
Medium	0
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. Kelp Sec 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.

LLMNR Vulnerability

Risk Rating: High

Description:
MegaCorpOne's network has a policy known as LLMNR that has an exploit that allows attackers to exploit vulnerabilities in systems. Attackers gain access by spoofing LLMNR responses to a victim's machine and tricking the victim machine into connecting to the attacker's machine instead of a legitimate one. At that point an attack can gain credentials and/ or spread malware. Using this method KelpSec was able to get an employee password and then was eventually able to look at network activity.

Affected Hosts; vpn.megacorpone.com

Remediation

- Have the sys admin disable LLMNR
- Using a more secure protocols: Instead of using LLMNR, use secure protocols like DNS-over-HTTPS and DNSSEC to resolve hostnames
- Letting the employees know about LLMNR attacks would be a great way of prevention and notification

Credential Dump

Risk Rating: High

Description:
Credential dumping is the practice of extracting sensitive information, such as passwords and usernames, from a computer system. This information can then be used to gain unauthorized access to a system or network, potentially leading to data breaches and asset loss. Kelp Sec was able to use a credential dump to obtain the information of 2 employees using this method.

Affected Host; vpn.megacorpone.com

Remediation
- Implementing Strong passwords
- Establishing a form of 2FA (two factor authentication)_
- Having passwords only last for a limited amount of time before they expire

MSF Venom

Risk Rating: High

Description:
MSFVenom is an incredibly powerful and versatile tool that is part of the Metasploit Framework (MSF). It is used by penetration testers and security professionals to generate and encode payloads, which are then delivered to a target system in order to exploit a vulnerability and gain unauthorized access.Kelp Sec was able to establish persistence and upload a reverse shell using this tool.

Remediation
- Making sure to establish an up-to-date firewall
- Actively monitoring the network and making sure no maliciou activity is happening
- Keeping software updated to prevent exploit and keep up with the cyber world