Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

FeelSafe, 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	**FeelSafe**, LLC
Contact Name	Omar Rayo
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	omarrayo@feelsafecom

Document History

Version	Date	Author(s)	Comments
001	04/04/2023	Omar Rayo	The only contributer

Introduction

In accordance with MegaCorpOne's policies, [**FeelSafe**], LLC (henceforth known as FS 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 FS during April of 2023.

For the testing, FS 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.
FS 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

FS 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, ZENMAP, GOOGLE DORKING.

Identification of Vulnerabilities and Services

FS uses custom, private, and public tools such as Metasploit, John The Ripper, Zenmap, recon-ng, 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

FS'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
172.16.117.0/24 MCO.local *.Megacorpone.com	MegaCorpOne internal domain, range and public website

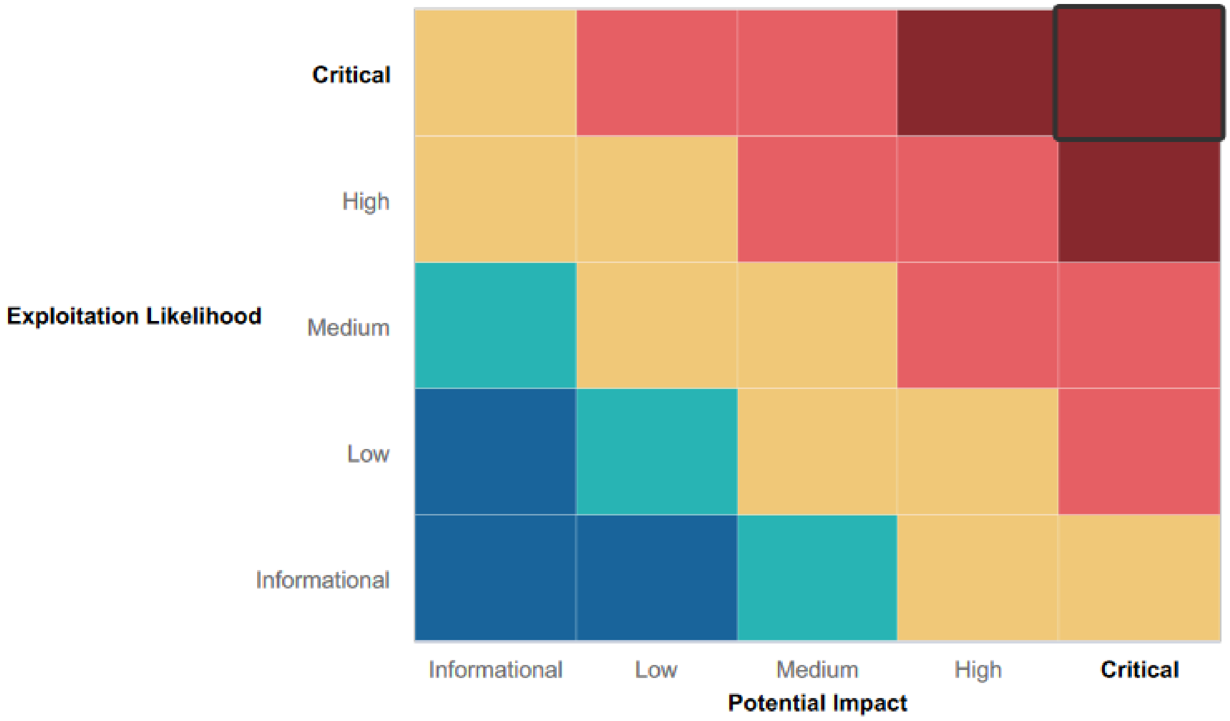
Executive Summary of Findings

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.

- While using metasploit and using ssh_login and ssh_login_publickey. Our testers were not able to enumerate information.
- MegaCorpOne had a layered approach for security which is a strong place to start
-

Summary of Weaknesses

FS 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.

- Known vulnerabilities related to Apache HTTP Server
- Known open ports to public 22, 80, 443
- Found unsecure network point
- Administrative and Entrepreneur passwords are weak and simple to guess.
- Able to known exploits to deliver payloads in system and gain access to root
- We were able to create user and create a persistent connection
- Passwords of all users
- hidden users

Executive Summary

To begin we began our investigation doing reconnaissance using open source tools like google. By Google Docking megacorpone.com we were able to find email addresses and names of people in the company. We were able to find hidden directories and files that are public through google dorking. After google dorking and using ZenMap to map out the IP of the network we were able to find many open ports that have known exploits. Using recon-ng we created a summary of ports and IP's used to carry out our pentest. Throughout exploits we were able to carry out back door exploits. After collecting the information of Megacorpone we then transitioned our focus on using the metasploit tools. While using metasploit we were able to backdoor into msfadmin and gain root privileges. After gaining root privileges we were able to add users and change passwords and also open more ports for further back door uses and hiding our activity. I was unable to make a persistent backdoor with a time scheduled command but with more time our team could have set a scheduled task that is malicious.

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions	High
A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.	Medium
Open ports with weak configuration. Was able to repeatedly attack the company without my IP being banned.	High
Being able to establish a reverse shell	High

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

Scan Type	Total
Hosts	19
Ports	SSH 22, Http 80, HTTPS 443

Exploitation Risk	Total
Critical	1
High	3
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. FS 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.

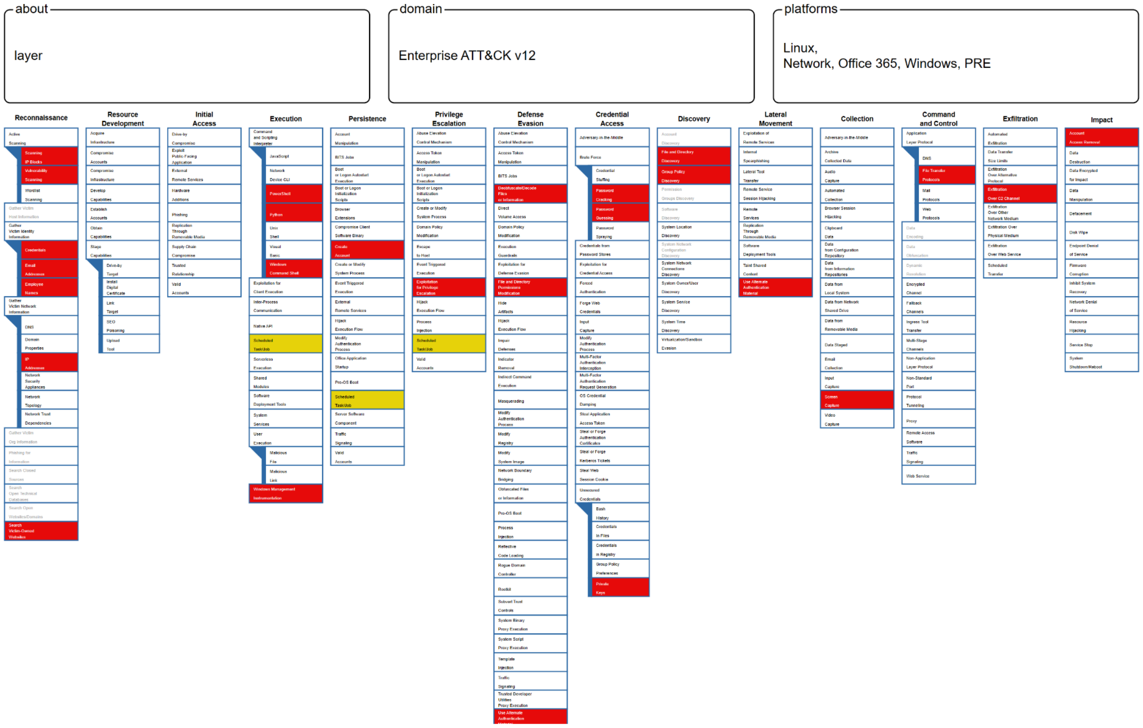
Affected Hosts: vpn.megacorpone.com

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.
- Ban IP's that repeatedly trying to brute force users passwords
- Have port moderating tools and configure UFW to not accept incoming traffic unless from an authorized user.
- Delete unused accounts.
- Have trainings on phishing and requiring passwords to be changed every 6 months

- While using nslookup on www.megacorpone.com (nslookup www.megacorpone.com) : finding the open ports 22, 80, 443. We also found the ssh server and version, the server type Debian, the version of the web server Apache 2.4.38 and along with Shodan, we found known vulnerabilities on the server.The servers location was in Montreal Canada.
- When navigating to vpn.megacorpone.com our team attempted to password guess some users on the server. We were able to guess the passwords of 6 users. When logged in we were able to download a shell script and then change the permissions of the file.
- Using Zenmap we were also able to find IP's with open ports that are open and with account access we would be able to exploit and add, change, and take files off the network.
- **Exploit**: https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/
- **Host IP address**: 172.22.117.150 **Port**: 21**Service name**: FTP **Service version**: VSFTPD 2.3.4 **Exploit outcome**: Success
- On the linux machine we were able to establish persistence and add a user system-ssh and add that user to the sudo group.
- When scanning the windows machine we were able to find two machines on the network 172.22.117.20 and .10 with the fallowing ports open 445, SMB, 139,RPC/SMB, 3389, RDP, 88, Kerberos.
- Using the tools auxiliary/scanner/smb/smb_login in metasploit were able to password spray all ips 172.22.117.0/24 with the Credentials tstark:Password!
- While using msfvenom we were able to create a meterpreter/reverse_tcp shell and up load a .exe file. Then going going to metasploit we are able to execute a payload that allows us to gain a shell in metasploit.

MITRE ATT&CK Navigator Map



about

layer

domain

Enterprise ATT&CK v12

platforms

Linux,
Network, Office 365, Windows, PRE

Reconnaissance
- Active Scanning
  - 🟥 Scanning IP Blocks
  - 🟥 Vulnerability Scanning
  - Wordlist Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
  - 🟥 Credentials
  - 🟥 Email Addresses
  - 🟥 Employee Names
- Gather Victim Network Information
  - DNS
  - Domain Properties
  - 🟥 IP Addresses
  - Network Security Appliances
  - Network Topology
  - Network Trust Dependencies
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- 🟥 Search Victim-Owned Websites

Resource Development
- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities
- Stage Capabilities
  - Drive-by Target
  - Install Digital Certificate
  - Link Target
  - SEO Poisoning
  - Upload Tool

Initial Access
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
- Command and Scripting Interpreter
  - JavaScript
  - Network Device CLI
  - 🟥 PowerShell
  - 🟥 Python
  - Unix Shell
  - Visual Basic
  - 🟥 Windows Command Shell
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- 🟨 Scheduled Task/Job
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
  - Malicious File
  - Malicious Link
- 🟥 Windows Management Instrumentation

Persistence
- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- 🟥 Create Account
- Create or Modify System Process
- Event Triggered Execution
- External Remote Services
- Hijack Execution Flow
- Modify Authentication Process
- Office Application Startup
- Pre-OS Boot
- 🟨 Scheduled Task/Job
- Server Software Component
- Traffic Signaling
- Valid Accounts

Privilege Escalation
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Domain Policy Modification
- Escape to Host
- Event Triggered Execution
- 🟥 Exploitation for Privilege Escalation
- Hijack Execution Flow
- Process Injection
- 🟨 Scheduled Task/Job
- Valid Accounts

Defense Evasion
- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- 🟥 Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification
- Execution Guardrails
- Exploitation for Defense Evasion
- 🟥 File and Directory Permissions Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
- Indicator Removal
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- Obfuscated Files or Information
- Pre-OS Boot
- Process Injection
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls
- System Binary Proxy Execution
- System Script Proxy Execution
- Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- 🟥 Use Alternate Authentication Material

Credential Access
- Adversary-in-the-Middle
- Brute Force
  - Credential Stuffing
  - 🟥 Password Cracking
  - 🟥 Password Guessing
  - Password Spraying
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- Modify Authentication Process
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- OS Credential Dumping
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Unsecured Credentials
  - Bash History
  - Credentials In Files
  - Credentials in Registry
  - Group Policy Preferences
  - 🟥 Private Keys

Discovery
- Account Discovery
- 🟥 File and Directory Discovery
- 🟥 Group Policy Discovery
- Permission Groups Discovery
- Software Discovery
- System Location Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- 🟥 Use Alternate Authentication Material

Collection
- Adversary-in-the-Middle
- Archive Collected Data
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- 🟥 Screen Capture
- Video Capture

Command and Control
- Application Layer Protocol
  - DNS
  - 🟥 File Transfer Protocols
  - Mail Protocols
  - Web Protocols
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Software
- Traffic Signaling
- Web Service

Exfiltration
- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- 🟥 Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer

Impact
- 🟥 Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

🟨 Failure to Perform

🟥 Successful attack