# 

| Cybersecurity |
| --- |
| Penetration Test Report |

MegaCorpOne

Penetration Test Report

**John Mercer, 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](#_44sinio)

[Grading Methodology 8](#_z337ya)

[Summary of Strengths 9](#_3j2qqm3)

[Summary of Weaknesses 9](#_1y810tw)

[Executive Summary Narrative 10](#_4i7ojhp)

[Summary Vulnerability Overview 11](#_2xcytpi)

Vulnerability Findings [12](#_1ci93xb)

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

# 

## Contact Information

| **Company Name** | John Mercer, LLC |
| --- | --- |
| **Contact Name** | John Mercer |
| **Contact Title** | Penetration Tester |
| **Contact Phone** | 612-718-2935 |
| **Contact Email** | john.mercer.mn@gmail.com |

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 07/09/2022 | John Mercer | initial report |
| 002 | 07/19/2022 | John Mercer | added Windows devices |
|  |  |  |  |
|  |  |  |  |

# 

## Introduction

In accordance with MegaCorpOne’s policies, John Mercer, LLC (henceforth known as JM) 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 JM during July of 2022.

For the testing, JM 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.

JM 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

JM 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

JM 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

JM’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** |
| --- | --- |
| 172.22.117.0/16  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.

* Password complexity requirements. However, there may be issues regarding password aging or rotation.

### Summary of Weaknesses

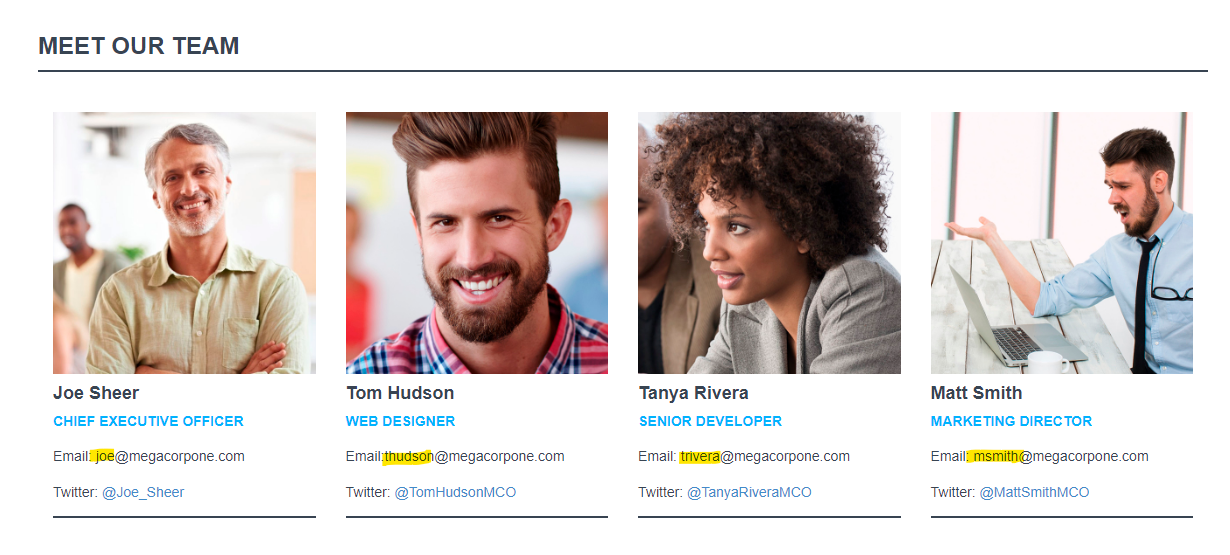
JM successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

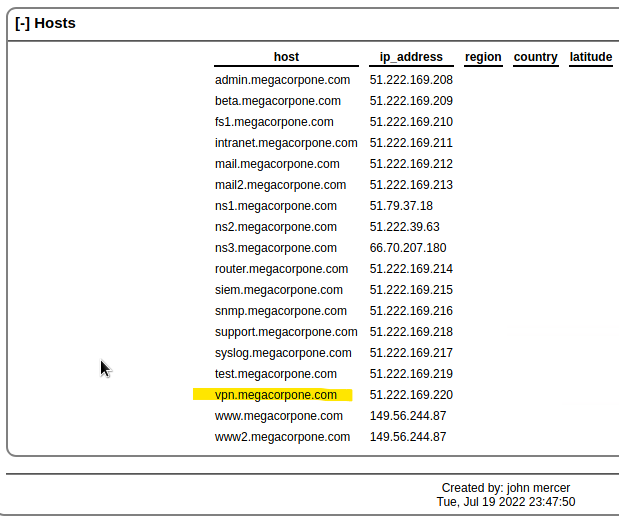
* A direct correlation between users’ email addresses and usernames.
* Lack of proper control/handling/care of administrative passwords.
* There are several vulnerabilities on metasploitable that are specific to version or port number.

# 

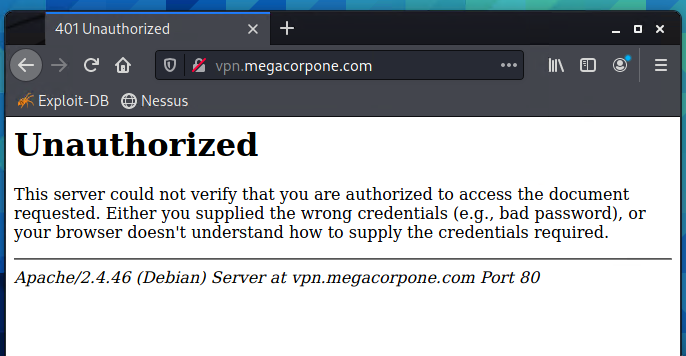
## Executive Summary

A review of public databases as well as Megacorpone’s own website revealed the names and email addresses of several members of the staff and management. While this may be desirable, the employee’s usernames were identifiable from their email addresses. It would be best if there was not a direct correlation between their username and their email address. It also revealed the existence and IP address of Megacorpone’s VPN server. Again, while this may be desirable, you should take care to make sure any externally exposed servers are well secured.



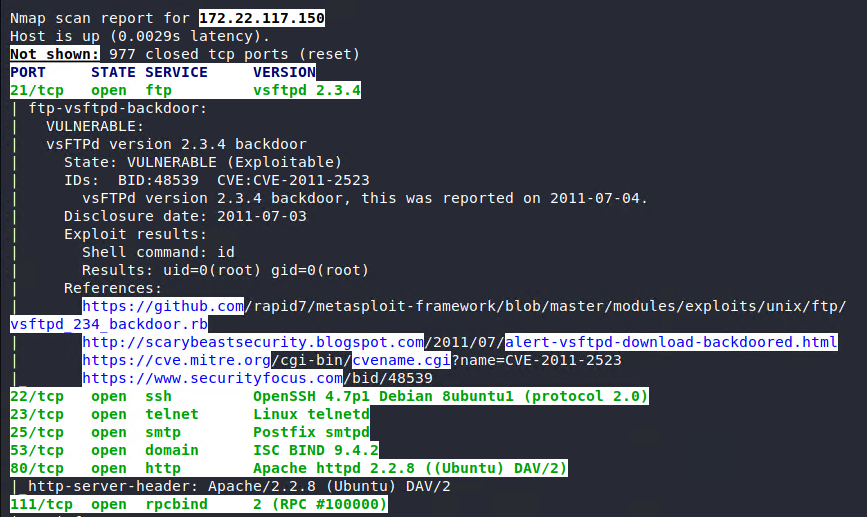


Using the VPN server and the usernames from email, we were able to guess the passwords of several users and log in as a user. It is recommended that you implement strong password complexity requirements, password again, and reuse limitations.

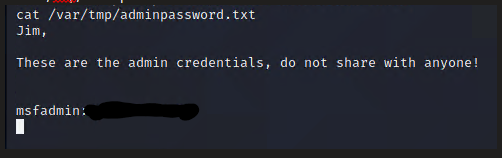


[VPN website is not functioning correctly for this exercise.]

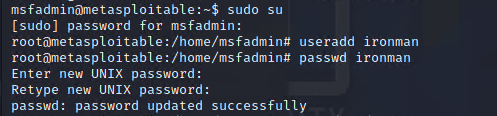
Once on the server, we were able to run scans on the network to find other systems; we identified the system metasploitable with a number of vulnerabilities (see below) that allowed us to connect to the machine and read files on it.

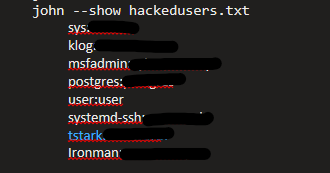


Among them was a text file listing an administrative username and password. It is highly recommended that passwords not be stored in a text file, especially passwords for accounts with administrative permissions.



Having gained admin permissions to the server, we were able to obtain the usernames and passwords of all the accounts on the system. We were also able to create a new user account and grant that new account admin permissions. While the steps performed are normal activity, it is recommended that a system be put in place to detect when accounts are added to groups that have admin permissions.



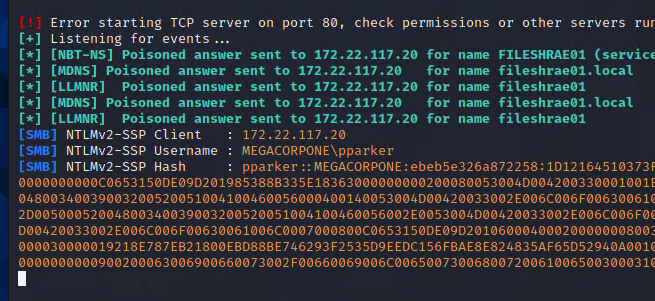


While scanning the network we also identified several Windows machines with potential vulnerabilities. Using usernames and passwords obtained from the metasploitable server, we were then able to log into the system Windows10, also with admin permissions. Note that this was a local account with only local admin rights. It is recommended that the number of local accounts we kept to a minimum and any local accounts with admin permissions be closely monitored and controlled.

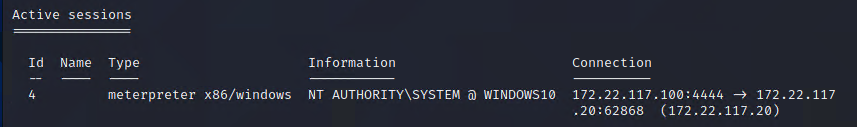


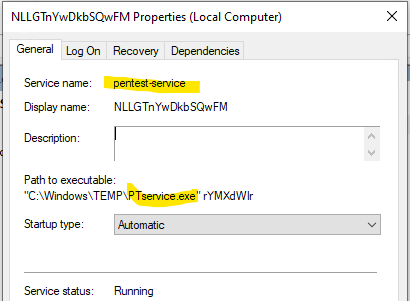


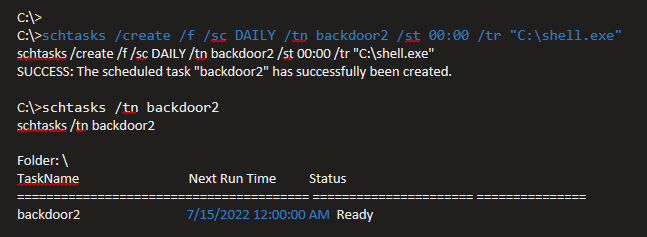
Using access to the Windows10 machine and a weakness in network protocols, we were able to obtain a domain username and password. It is recommended that the LLMNR protocol be disabled on your network via GPO.



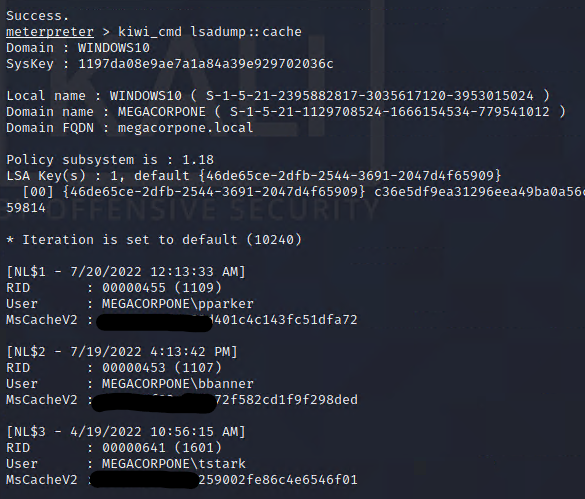
Using this local admin account, we were able to fully control the Windows10 machine as needed, including running a shell so all of our activity came from the internal machine instead of an external JM machine. This included setting up a new service to run on the Windows10 machine that we can control and is running as a system account. It is recommended that the services running on the systems be monitored and the creation of services be logged and monitored. We also set up a task on the machine to reopen the access if the system gets rebooted; so we can maintain our access.



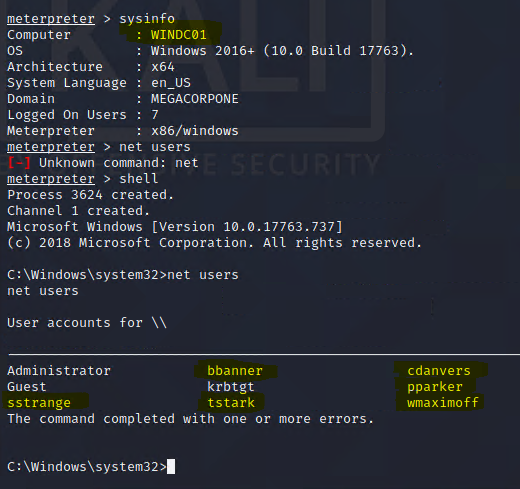




Using our access to the Windows10 machine, we were able to obtain the cached password hashes of other Megacorpone domain accounts and crack the hashes to obtain the passwords. The passwords obtained did meet most complexity requirements, they were on the shorter side and we were able to crack them in little time.



Using the newly discovered passwords, we were then able to connect to the Domain Controller server WinDC01 with domain administrator permissions. We were then able to obtain the domain’s security database and crack all the remaining user passwords. At this point you should consider all the systems and accounts on the domain as compromised.



## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Weak password on public web application | **Critical** |
| Vulnerability in vsFTPd | **Critical** |
| Vulnerability in Unreal IRC | **Critical** |
| Vulnerability in Apache Tomcat | **High** |
| Vulnerability in SMB protocol | **High** |
| Vulnerability in LLMNR protocol | **High** |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 172.22.117.20  172.22.117.10  172.22.117.150 |
| Ports | “the most commonly used 1,000 TCP ports” |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 3 |
| **High** | 3 |
| **Medium** | - |
| **Low** | - |

## 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.

**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.

### Vulnerability in vsFTPd version 2.3.4

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

**Description**:

The server metasploitable.localdomain at 172.22.117.150 is running the FTP service on port 21 using vsftpd version 2.3.4, which has a known backdoor command execution vulnerability ([CVE-2011-2523](https://nvd.nist.gov/vuln/detail/CVE-2011-2523)). Exploiting this vulnerability allows the attacker to open a command shell on the remote machine as root.

**Affected Hosts**: metasploitable.localdomain at 172.22.117.150

**Remediation**:

* Download and install a newer version of the service.
* Block outgoing traffic on port 6200/tcp.

### Vulnerability in Unreal IRC version 3.2.8.1

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

**Description**:

The server metasploitable.localdomain at 172.22.117.150 is running the Unreal engine IDC service on port 6667 using version 3.2.8.1, which has a known backdoor command execution vulnerability ([CVE-2010-2075](https://nvd.nist.gov/vuln/detail/CVE-2010-2075)). Exploiting this vulnerability allows the attacker to open a command shell on the remote machine as root.

**Affected Hosts**: metasploitable.localdomain at 172.22.117.150

**Remediation**:

* Download and install a newer version of the service, or remove is not needed.
* Block traffic on port 6667 if this service is not needed.

### Vulnerability in Apache Tomcat

**Risk Rating**: **High**

**Description**:

The server metasploitable.localdomain at 172.22.117.150 is running the Apache Tomcat service on port 8180 using version 1.1 and Apache Jserv on port 8009, which has a known vulnerability ([CVE-2020-1938](https://nvd.nist.gov/vuln/detail/CVE-2020-1938)). Exploiting this vulnerability allows the attacker to read or extract files from the web server that they may not normally have access to.

**Affected Hosts**: metasploitable.localdomain at 172.22.117.150

**Remediation**:

* Download and install a newer version of the service, or remove is not needed.
* Block traffic on ports 8180 and 8009 if this service is not needed.
* Update Apache Tomcat configuration files

### Vulnerability in SMB protocol

**Risk Rating**: **High**

**Description**:

The Windows machines (Windows10 and WinDC01) are using SMB version 2.0 which has a known vulnerability ([CVE-1999-0506](https://nvd.nist.gov/vuln/detail/CVE-1999-0506)). Exploiting this vulnerability allows the attacker to test usernames and passwords for access.

**Affected Hosts**: Windows10.localdomain at 172.22.117.20, WinDC01.localdomain at 172.22.117.10

**Remediation**:

* Apply GPO settings to block anonymous access to shares and SAM accounts.

### Vulnerability in LLMNR protocol

**Risk Rating**: **High**

**Description**:

The Windows machines (Windows10 and WinDC01) are using the LLMNR protocol which has a known vulnerability ([CVE-2011-0657](https://nvd.nist.gov/vuln/detail/CVE-2011-0657)). Exploiting this vulnerability allows the attacker to obtain usernames and passwords for access.

**Affected Hosts**: Windows10.localdomain at 172.22.117.20, WinDC01.localdomain at 172.22.117.10

**Remediation**:

* Apply GPO settings to block the LLMNR protocol.

## MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully

Failure to perform

json file: <https://drive.google.com/file/d/1xKOIw2gUZlJhFA2zxpK1ozgpacyTYeF2/view?usp=sharing>

svg file: <https://drive.google.com/file/d/11qQoWHqR1VPmpllOzQDq6pvq6EFHZToZ/view?usp=sharing>

