# 

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

MegaCorpOne

Penetration Test Report

**Fun Times, 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** | Fun Times, LLC |
| --- | --- |
| **Contact Name** | Colin O’Donoghue |
| **Contact Title** | Penetration Tester |
| **Contact Phone** | 555.224.2411 |
| **Contact Email** | codonoghue17@gmail.com |

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 08/07/2023 | Colin O’Donoghue |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

## Introduction

In accordance with MegaCorpOne’s policies, Fun Times, LLC (henceforth known as F.T.) 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 F.T. during July of 2023.

For the testing, F.T. 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.

F.T.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

F.T. 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

F.T. 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

F.T.’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.

* It was proven that the MegaCorpOne network was impenetrable after using a number of different aspects of the Metasploit program in Kali Linux.
* We found that the MegaCorpOne’s machines were unable to connect to our back-end for penetration into the system.

### Summary of Weaknesses

F.T.’s 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.

* The passwords for users and servers proved to be weak.
* We found that Port 21 (FTP) was open and vulnerable to penetration.
* Privilege escalation was granted after the penetration was successful.
* IP Addresses were able to be viewed by the public.
* LLMNR (Link-Local Multicast Name Resolution) proved to be a weakness.

# 

## Executive Summary

F.T. had a challenging task of finding weaknesses inside the MegaCorpOne environment that proved to be successful in many ways. F.T. was ultimately able to access the network and implement root privileges that would grant us persistence within the company’s network. This was all possible mainly because of the weak passwords that were used by employees, and whenever these are compromised it is easier to maneuver through the system and gain access to sensitive information. Also, the ability to take advantage of open ports was critical in gaining access within the system. The information of the company’s servers was public as well; we were able to find the servers had vulnerabilities in plain sight. The use of LLMNR attacks proved to be successful as well. Overall, the system needs to be revamped with more security features and constant monitoring to ensure that an attacker has a much harder time gaining access to MegaCorpOne’s sensitive information. It is our recommendation that MegaCorpOne seriously considers initiating a cybersecurity team to perform these tasks and guard the company’s data from advanced threat actors.

Due to the length of this exercise, the following will provide the steps taken that F.T. used to gain complete transparency into the whole MegaCorpOne environment:

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Weak password on public web application | **Critical** |
| Open Port 21 | **Critical** |
| Privilege Escalation | **High** |
| LLMNR | **High** |
| IP Addresses available to the public | **Medium** |

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

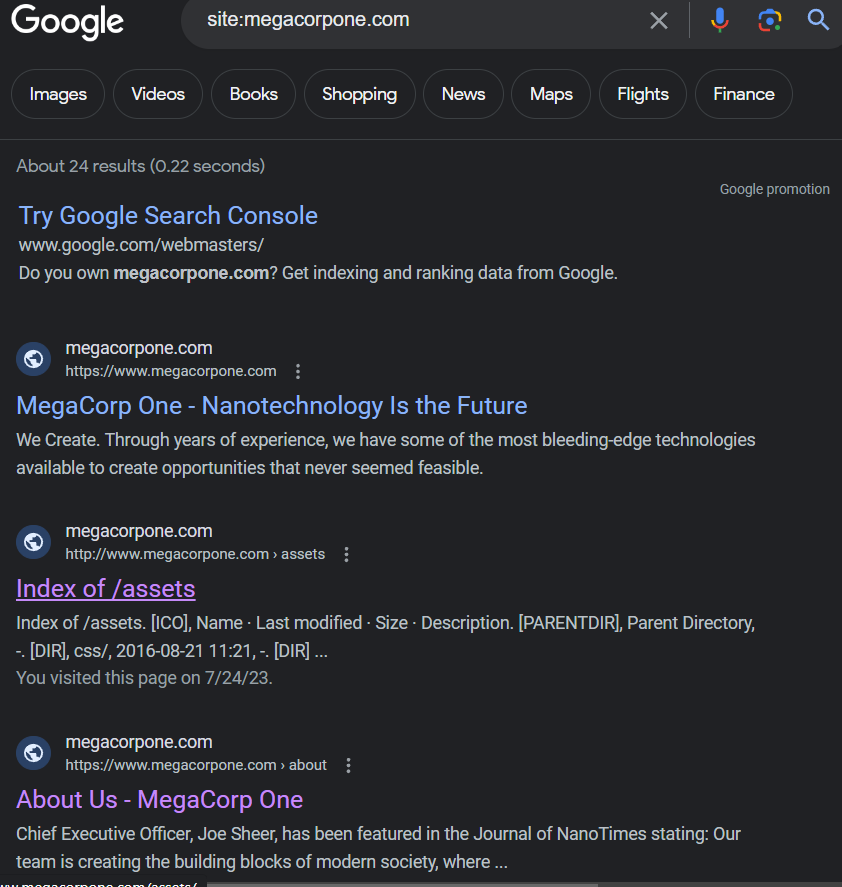
| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 194.56.244.87  172.22.117.100  172.22.117.150  172.22.117.20  172.22.117.10 |
| Ports | 21, 22, 80, 88, 443, 445, 139, 3389 |

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

## Vulnerability Findings

Reconnaissance: We used the practice of Google Dorking to see what we could find in regards to any important files or information about any of the employees within MegaCorpOne. What we found was a file that contained assets, a list of company employees with contact information and also social media account names for these employees.

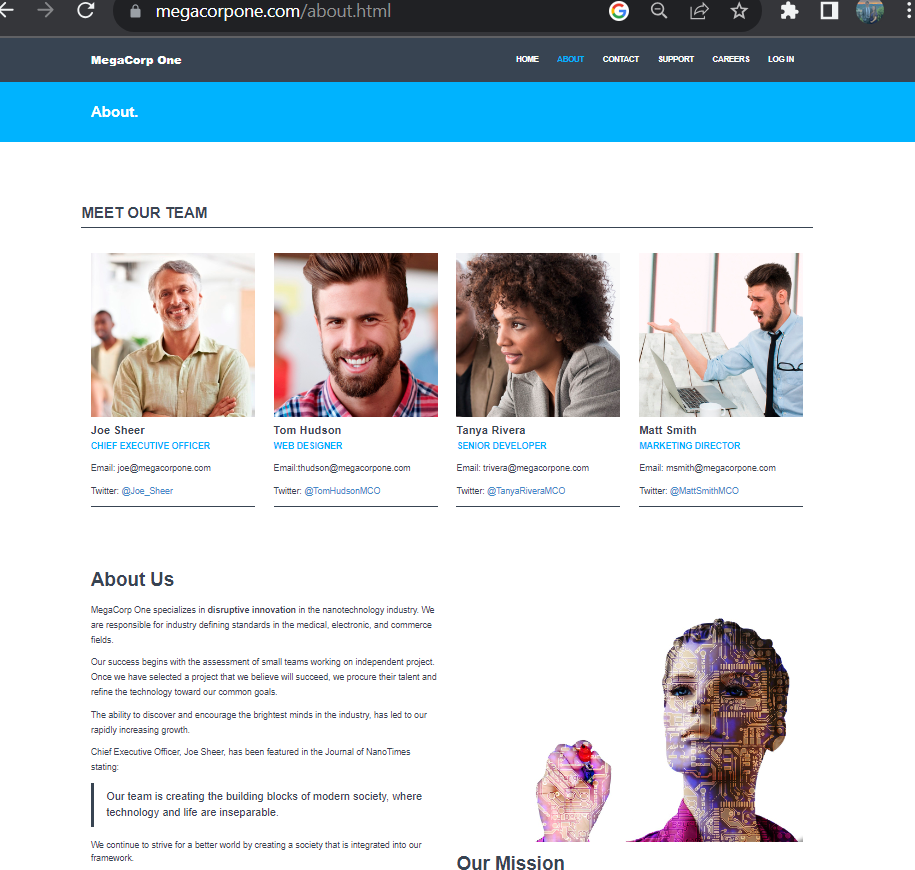
Google Dorking:



Link page to the Index of Assets:

#### 

Employee information with Social Media accounts and Email Addresses:

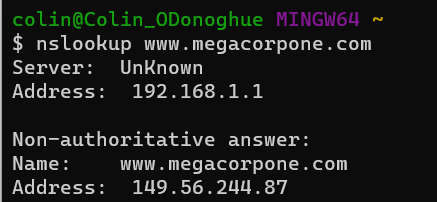


It was here that we discovered that the only employee that did not use a first initial/last name for their email address was Joe Sheer.

* Other emails found:
  + Mike Carlow (VP of Legal) [mcarlow@megacorpone.com](mailto:mcarlow@megacorpone.com)
  + Alan Grofield (IT and SEC Director) [agrofield@megacorpone.com](mailto:agrofield@megacorpone.com)
  + Human Resources [hr@megacorpone.com](mailto:hr@megacorpone.com)
  + Sales [sales@megacorpone.com](mailto:sales@megacorpone.com)
  + Shipping [shipping@megacorpone.com](mailto:shipping@megacorpone.com)

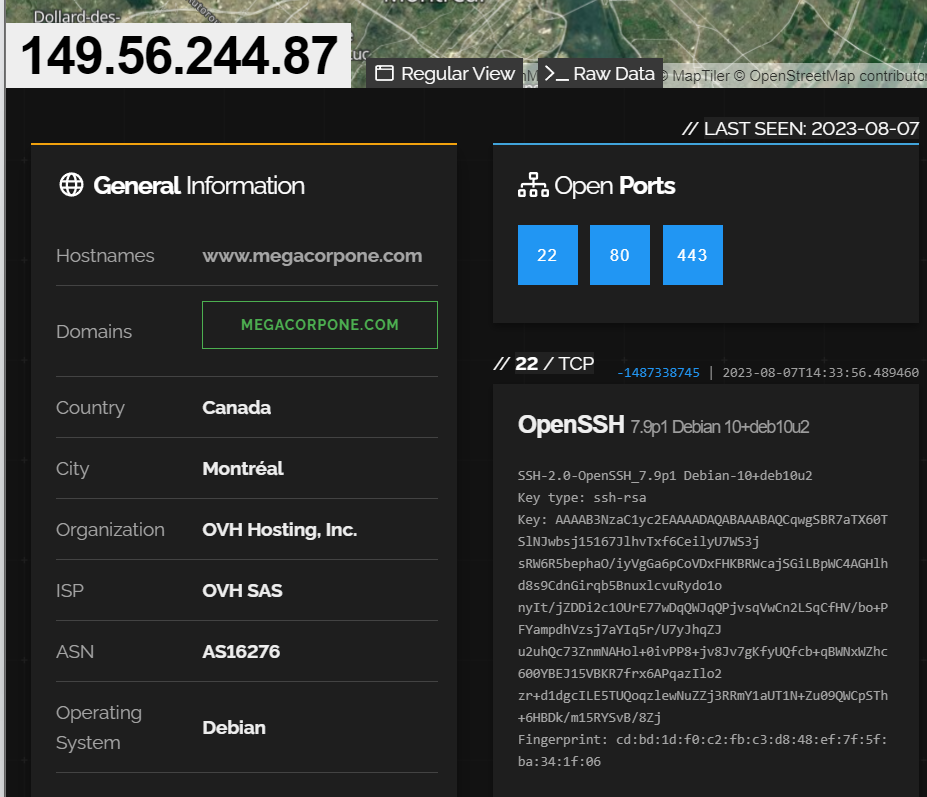
Once this was completed, NSLookup was used to obtain the IP Address for MecaCorpOne.

NSLookup:



After we obtained the IP Address, we could use the website Shodan.io to discover an array of information about the specifics of the server. It was found that ports 22, 80, and 443 were open.

Shodan Results:



\*\*\*Also, the OS system was present, as well as the web server information and the location of the server. The web server used is Apache/2.4.38 with the web server being in Montreal, Canada.

Vulnerability: IP Addresses available to the public:

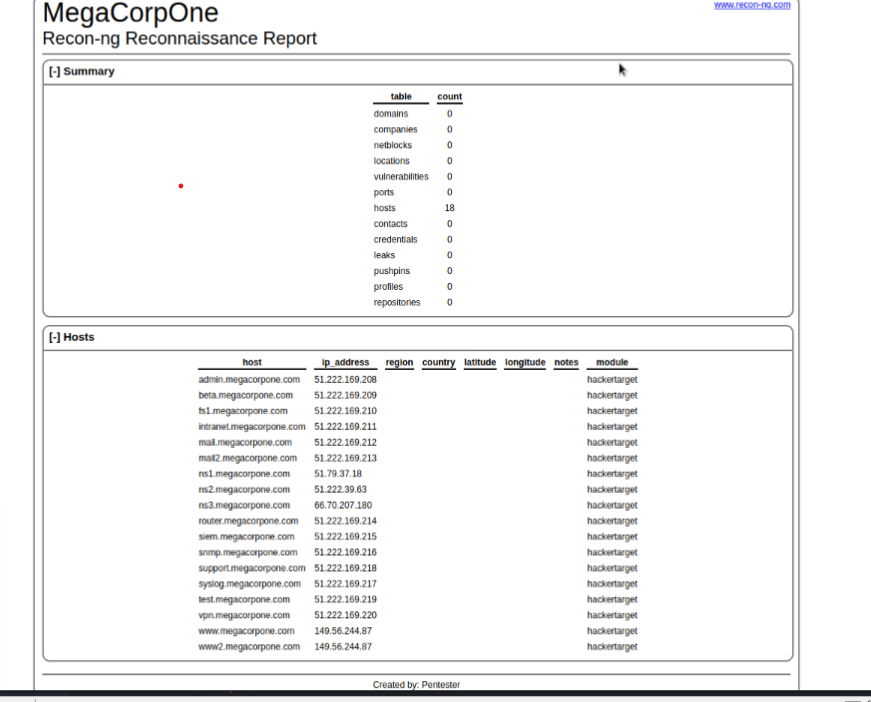
Risk Rating: Medium

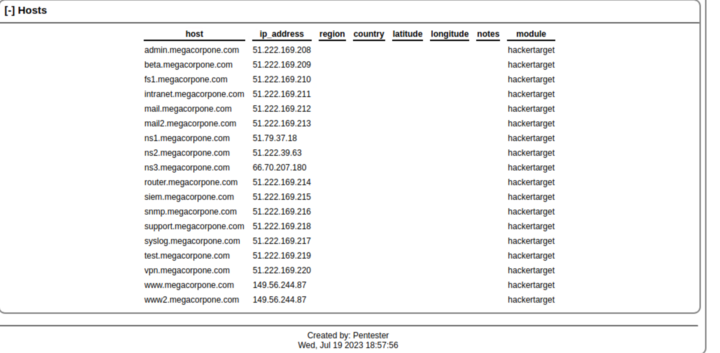
Description: Recon-ng was used to locate the IP Addresses for a number of hosts that a hacker could target, and the worst part is that Recon-ng can be used by anyone as it is a public tool. Although this is a threat, it really can only be used to find hosts, insert a faulty domain name with that IP Address like in DNS spoofing and could redirect users to sites that could cause them to now become vulnerable. In this case, users will be less likely to use a site that they do not trust, ruining a businesses’ reputation.

Affected Hosts: ns1.megacorpone.com, ns2.megacorpone.com, ns3.megacorpone.com

Remediation: Turn the public IP Addresses to private to secure the sites. Also, you could install a firewall or multiple firewalls to block any unwanted traffic to this information.

Recon-ng Report:





\*\*\*This tool generated a report and discovered hosts as well as IP Addresses.

Next, we conducted a password guessing session and compromised “thudson’s” password. We were able to gain access into the VPN due to the poor strength of the password.

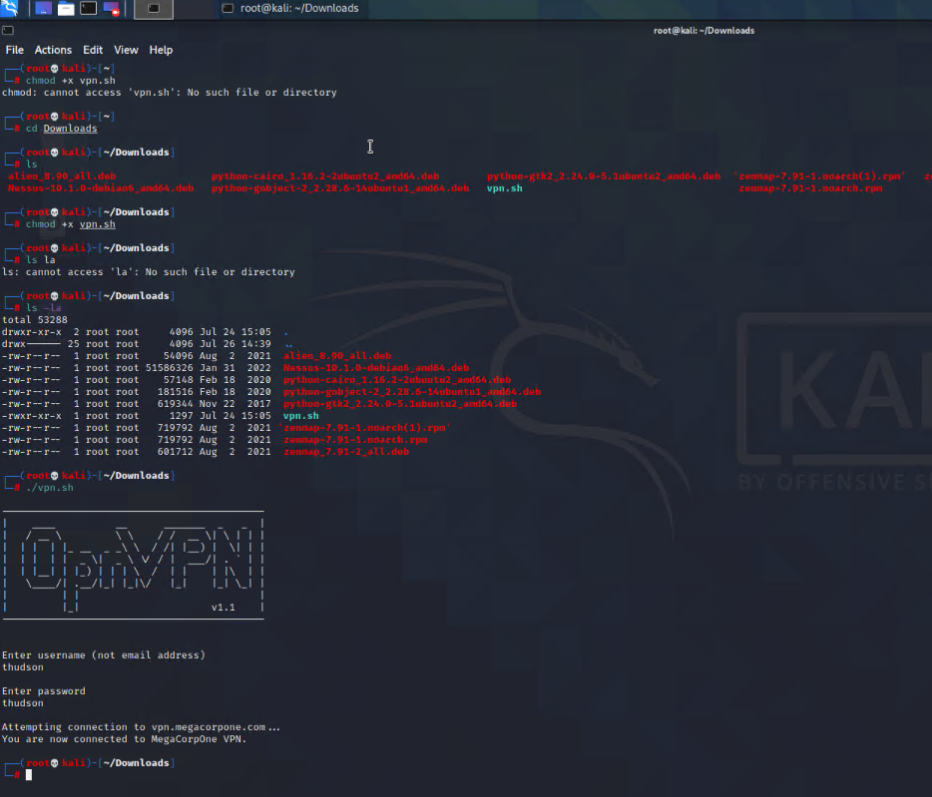
Vulnerability: Weak Passwords

Risk Rating: Critical

Description: The employees of MegaCorpOne are currently using weak passwords. This was concerning because weak passwords allow for hackers to easily gain access into a system, even with a VPN. The risk for using a weak password is critically high because having a strong password is a very simple way to combat an online attack, and having a weak password can compromise an entire company’s sensitive data.

Affected Hosts: vpn.megacorpone.com, Windows10 Machine, and WinDC01.

Remediation: Implement a rule that requires passwords to be more complex and longer. Also, make employees have to reset their passwords more often; passwords should be changed every 3 months to prevent a password spraying attack from being successful.



After this, we performed a Zenmap session to build a profile in order to do an intense scan on the network linked to the machine. Port 21 was found to be vulnerable to a backdoor exploit. Zenmap was an easier way to use Nmap due to its GUI interface. We were able to see more information that was in a structured format to easily pinpoint the information we needed to see.

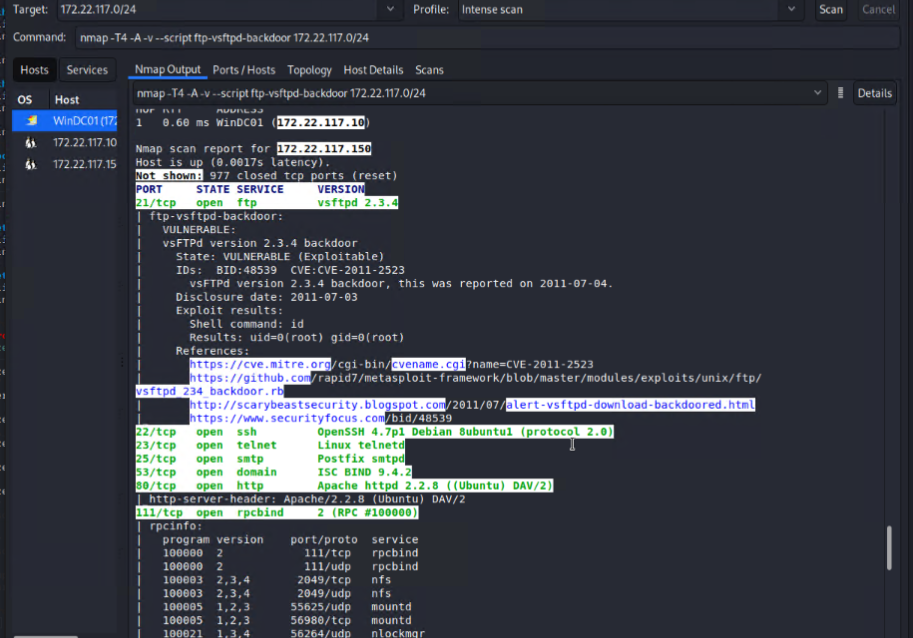
Vulnerability: Port 21 is open

Risk Rating: Critical

Description: When it comes to gaining access into a system, Port 21 is a FTP protocol that acts as a ‘front-door’ gateway into a system. It is not wise to have this open because it is considered less secure than other ports, as it transmits data like usernames and passwords in plain text. After we ran a Zenmap scan of a known IP Address, we found that the Port was open, and we used that to our advantage.

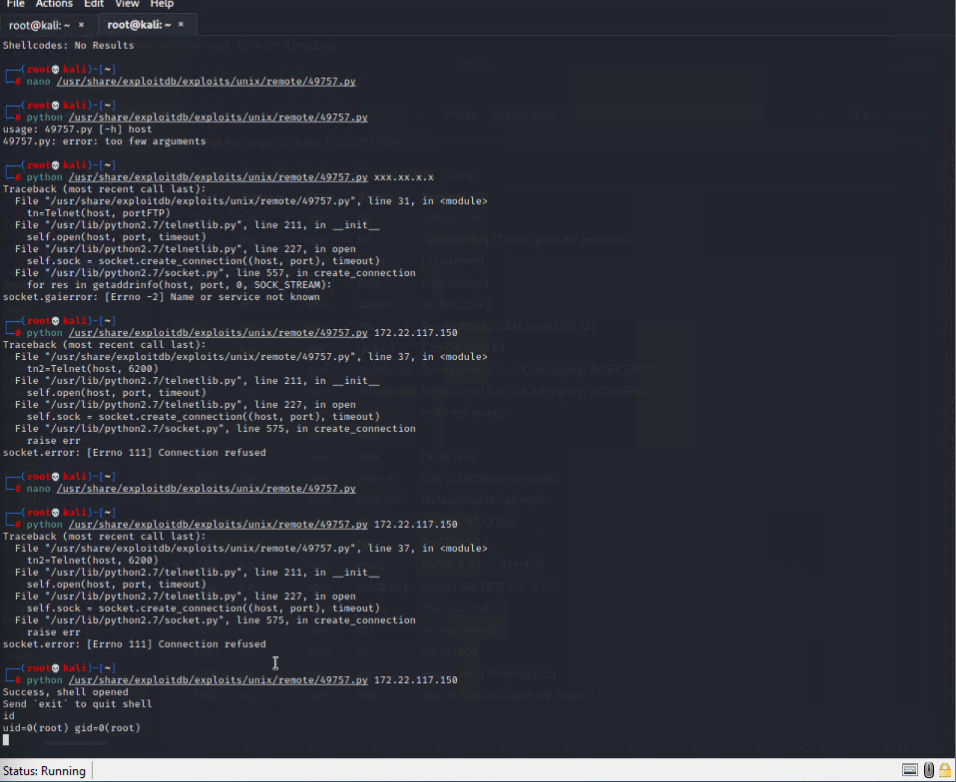
Affected Hosts: 172.22.117.20

Remediation: This Port should be closed and remain closed for the rest of the company’s operation. A firewall can also be installed to make sure that threat actors cannot easily exploit this port as well.



Exploitation:

\*\*\*In this step, we used the scan results to find a vulnerable machine called ‘Metasploitable2’ and it had a very large number of ports opened. We were looking for a specific port (Port 21) to utilize a backdoor attack without any pushback. Next, we used a script using python to configure a code that would allow us to use an IP Address to gain access into a shell within the network. The technique was successful, and we were granted root privileges as shown below:



This brings us to Privilege Escalation, as admin credentials were in a text file found when running the ‘find’ command in the shell within Metasploit.

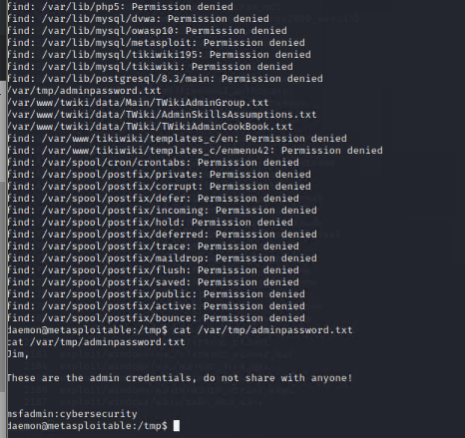
Vulnerability: Privilege Escalation

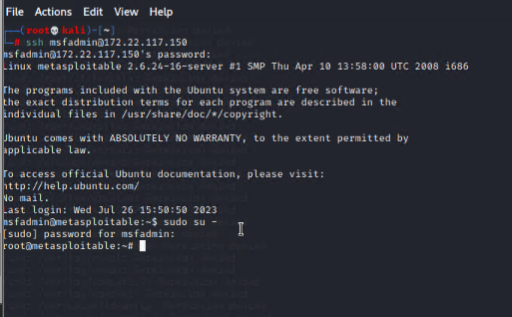
Risk Rating: High

Description: To be able to gain access into a system and escalate one’s privileges so that they are able to perform any task they want may be the most critical of all risks. Once a hacker is inside of a system, they can make it so they can do whatever they want once root or admin privileges are reached. This is another reason why strong passwords are so important.

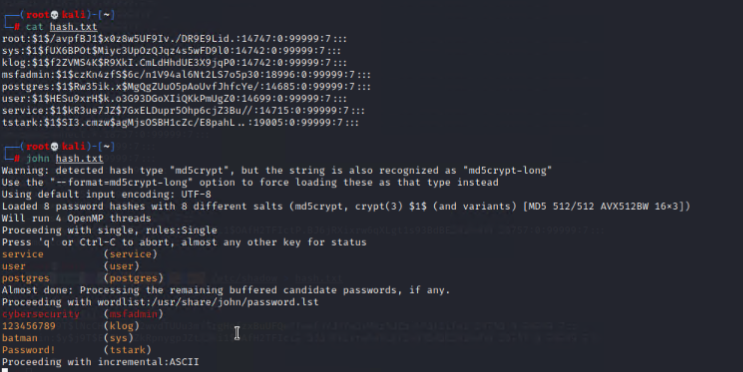
Affected Hosts: 172.22.117.150 and 172.22.117.20

Remediation: Do not grant any privileges to employees to be able to access any file or directory that they would have no business having access to in the first place. Keep employees in system groups with the files that they need public and keep everything else in admin or root security.

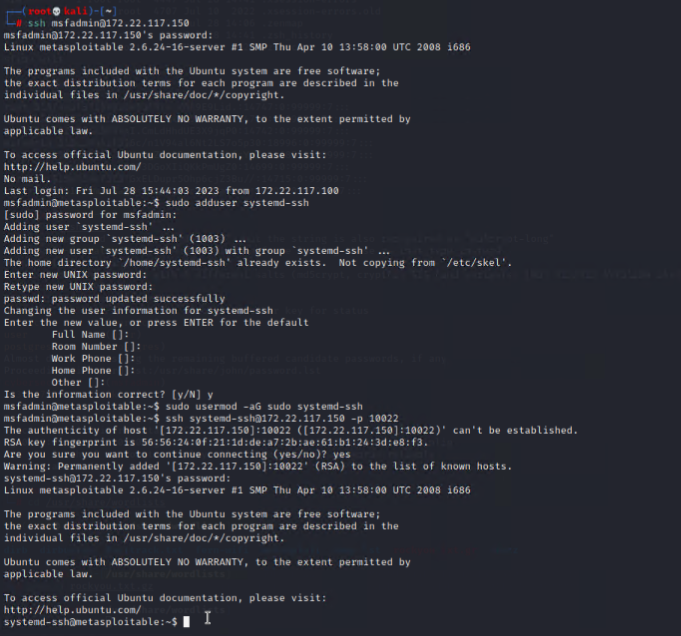




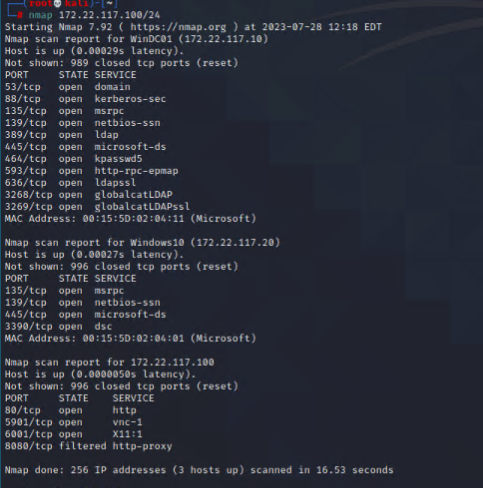
We eventually found more passwords that had been compromised when performing another password cracking method after gaining root privileges.



Also, while in root, we were able to create a new user with a verified password so that we gained persistence into the system for future infiltration:



The next thing to do was to perform an Nmap scan of the company’s network, and we found that two Windows machines were on the network with ports 445, 139, 3389, and 88 were open.



After we performed another password spraying attack, we found a set of credentials and successfully found more due to using the technique of LLMNR spoofing.

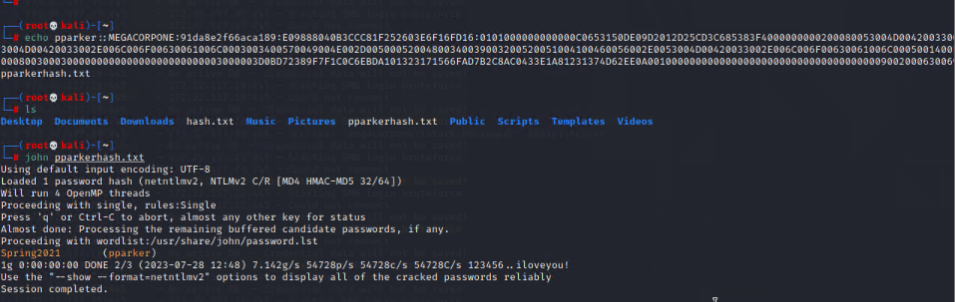
Vulnerability: LLMNR

Risk Rating: HIgh

Description: In computer networks, the LLMNR stands for Link-Local Multicast Name Resolution and it works as a protocol to serve as a backup to Domain Name Systems. When a computer wants to link to another, it needs to know the name of the machine and LLMNR helps with this process by sending out messages to machines to quickly find the right one. However, since the message gets sent out to a lot of different machines, there is a possibility of a threat actor intercepting this message and spoof the machine into thinking that they found the right one. This can lead to breaches. During this exercise, we were able to perform an attack by tricking the machine into giving us needed credentials without much pushback.

Affected Hosts: 172.22.117.20

Remediation: There needs to be one person constantly watching the traffic on the network so that the machines are connecting to the correct receiver. There is also an option to disable LLMNR completely in the group policy editor.



## MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully

Failure to perform

