# 

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

MegaCorpOne

Penetration Test Report

**TechExpertz, 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** | TechExpertz, LLC |
| --- | --- |
| **Contact Name** | Justin Castellanos |
| **Contact Title** | Penetration Tester |
| **Contact Phone** | 555.224.2411 |
| **Contact Email** | JRCast@TecEx.com |

## Document History

| **Version** | **Date** | **Author(s)** | **Comments** |
| --- | --- | --- | --- |
| 001 | 01/26/2023 | Justin Castellanos |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

## Introduction

In accordance with MegaCorpOne’s policies, TechExpertz, LLC (henceforth known as TecEx 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 TecEx during January of 2023.

For the testing, TecEx 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.

TecEx 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

TecEx 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

TecEx 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

TecEx’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** |
| --- | --- |
| 172.22.117.0/24  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.

* Software updated to prevent known attacks
* Group policies for non-admin accounts to limit access

### Summary of Weaknesses

TecEx 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.

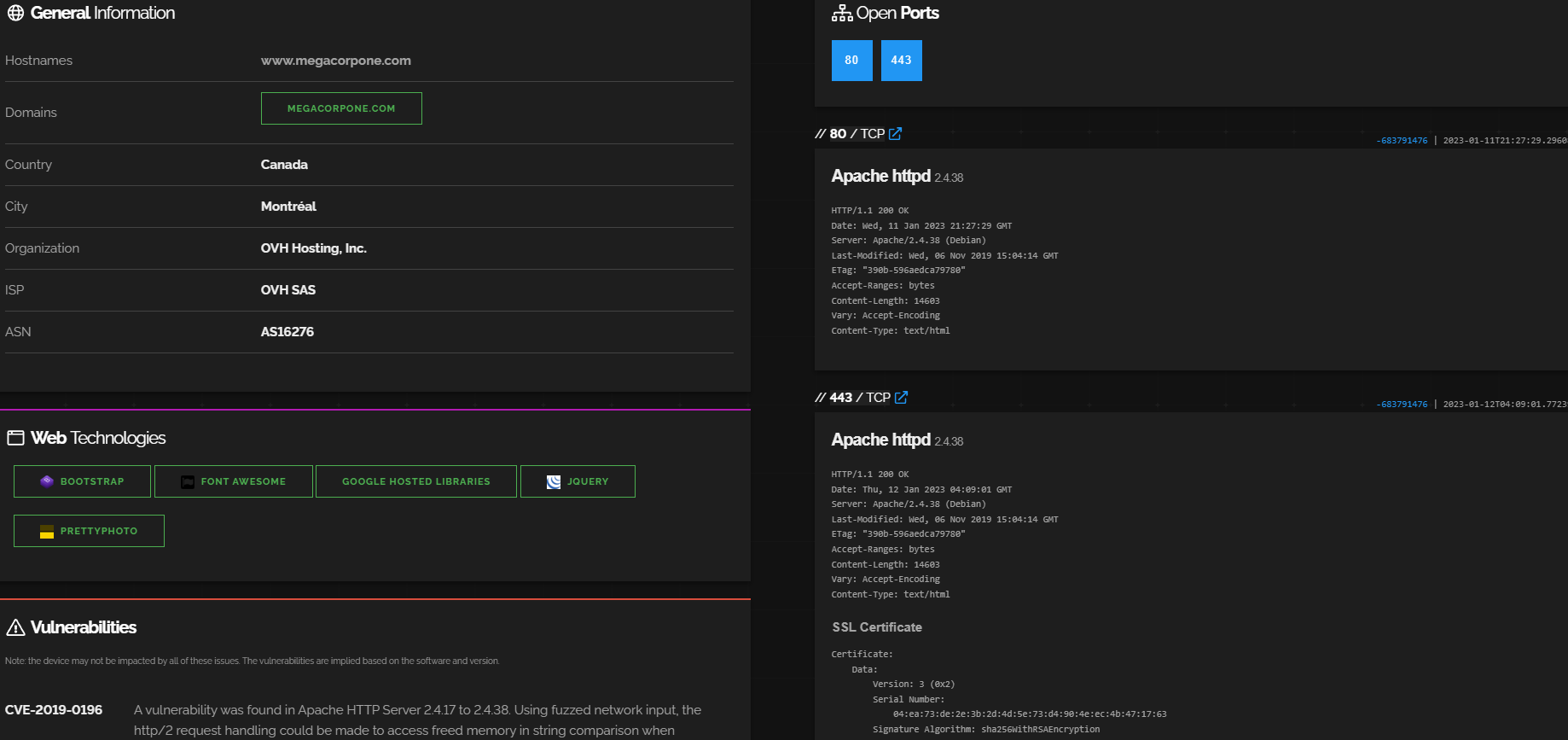
* Weak Passwords on public web application
* Weak user passwords for admin and domain accounts
* Intrusion detection and response systems not in place
* Host firewall not in place
* Privilege account managment to keep domain accounts out of host admin groups

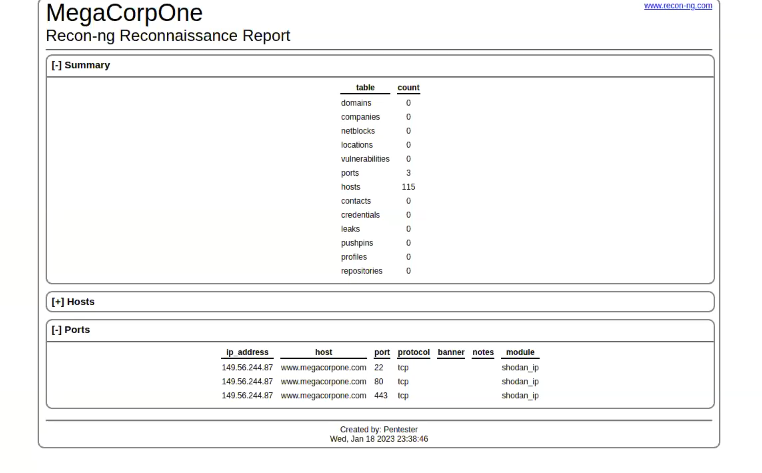
# 

## Executive Summary

Starting with open source recon using google to gather some basic information on megacorpone, we found names and emails to several personnel.

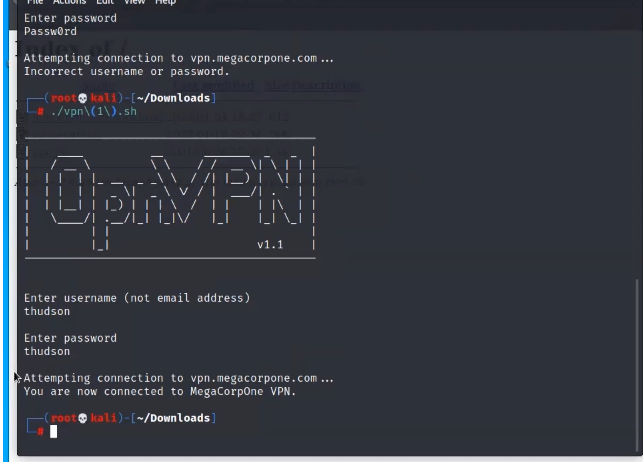
Using shodan.io, an open source scanning tool, we were able to passively scan megacorpone’s website.

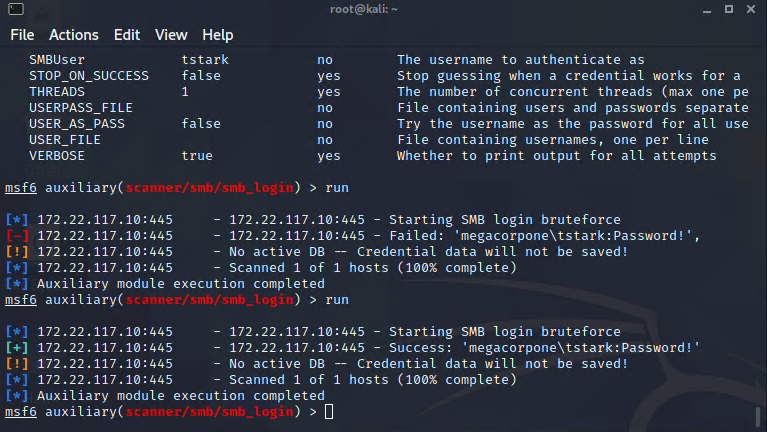


Using recon-ng we were able to scan the for subdomains with IP addresses that are being used by the megacorpone.com domain. 

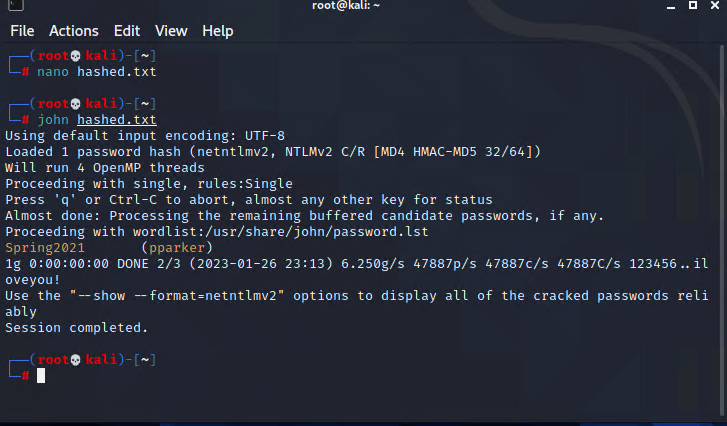
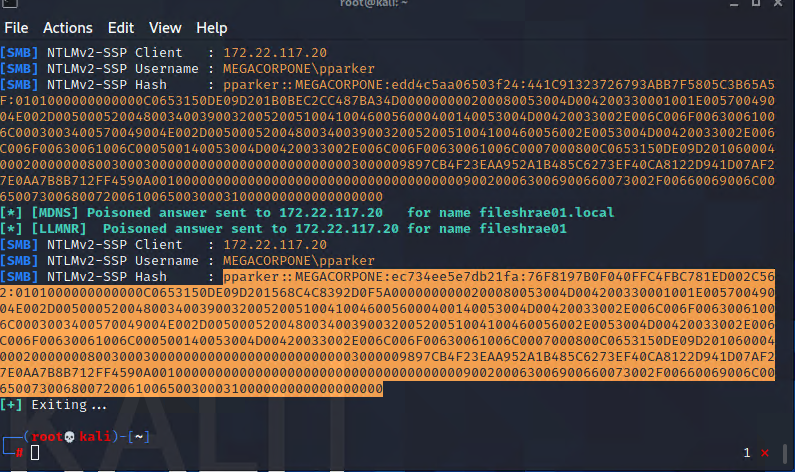
We discovered a url, vpn.megacorpone.com, that gave us access to download the password.list and vpn.sh files. Using password guessing we were able to figure out the password for user thudson.

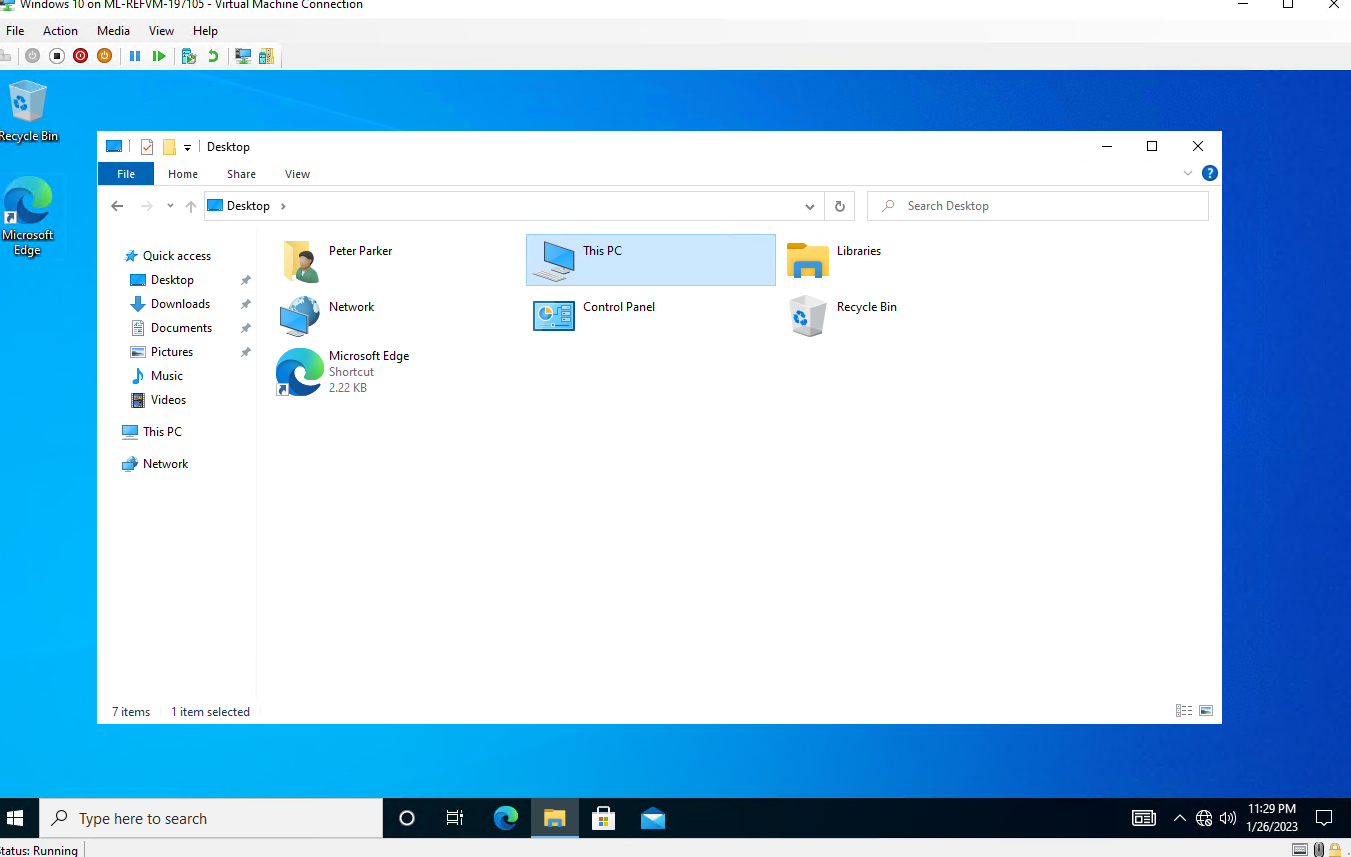
Using the vpn.sh file we were able to use the credentials to log into the megacorpone vpn service.

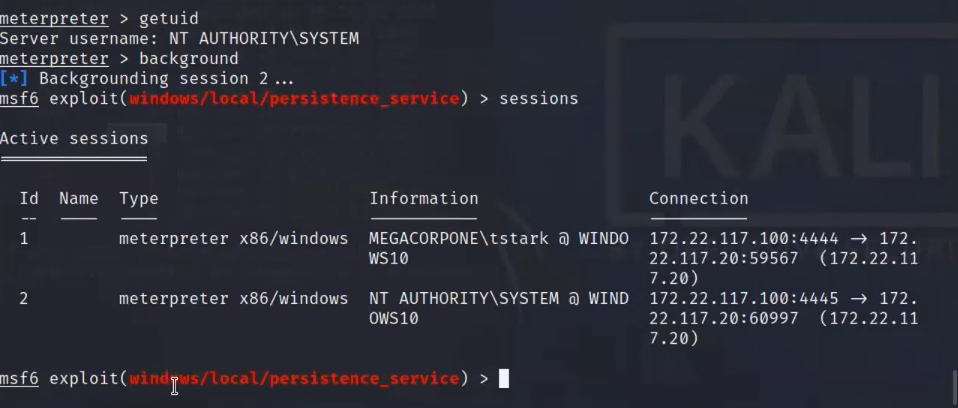


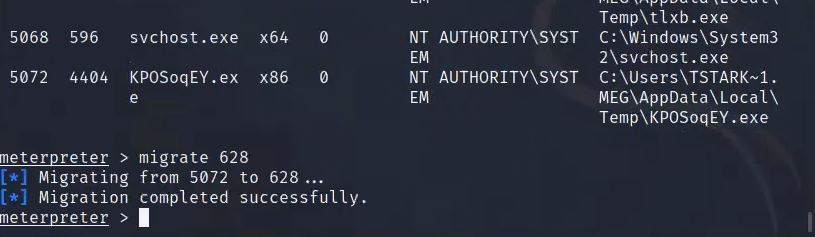
After gaining access we began to gather more information, finding the IP address for the eth0 and eth1 for the local network. Using nmap to scan the network we discovered there was a host 172.22.117.150 that had an FTP port open. We used thudson’s credentials to gain access to the targeted host 172.22.117.150 using metasploit. From there we ascertained the adminpasswords.txt file containing the credentials for msfadmin account. Once logged into the msfadmin account we were able to download the /etc/shadow file that stores password hashes. Using John the Ripper (tool for decoding password hashes) we were able to decipher the credentials for the user tstark.

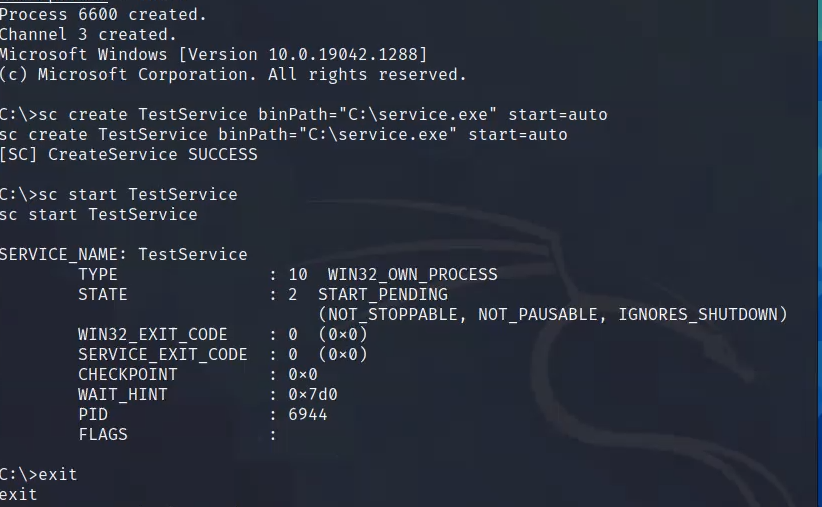
Upon further investigation of the network we discovered that host 172.22.117.20 had port 445 open for SMB services. Using tstark credentials we were able to gain access to this host using a password sprayer exploit.

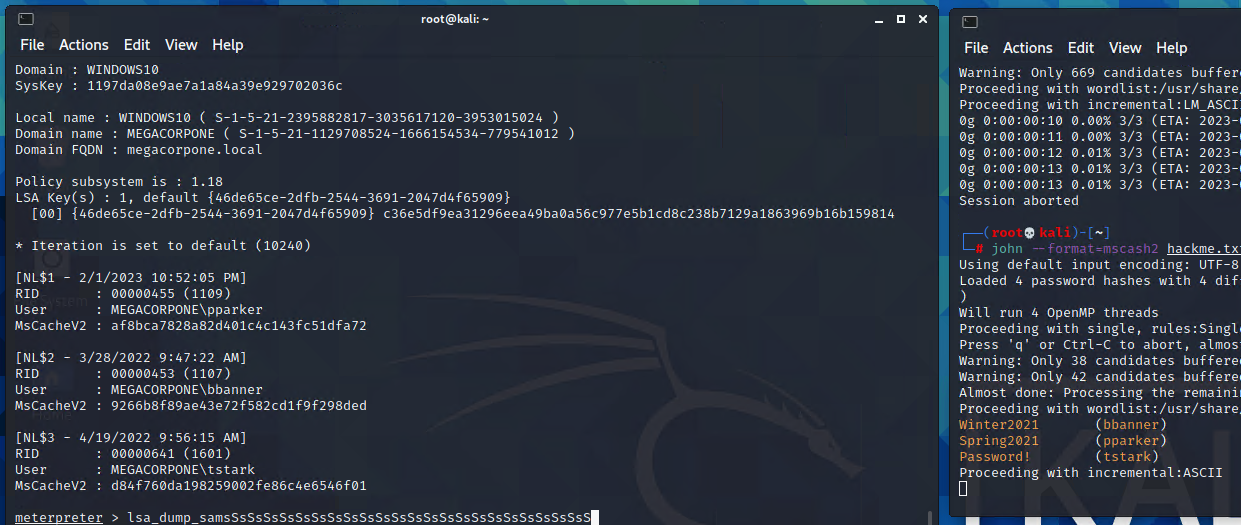
From here we utilized metasploit to listen for LLMNR requests in the network to try and steal credentials from other users. We discovered the credentials for a pparker and were able to use John the Ripper to decode the hashed password.

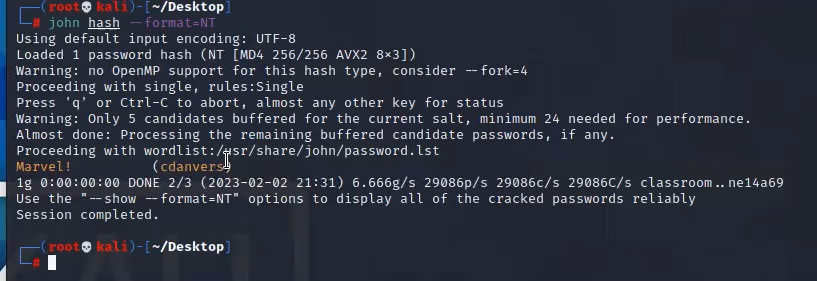
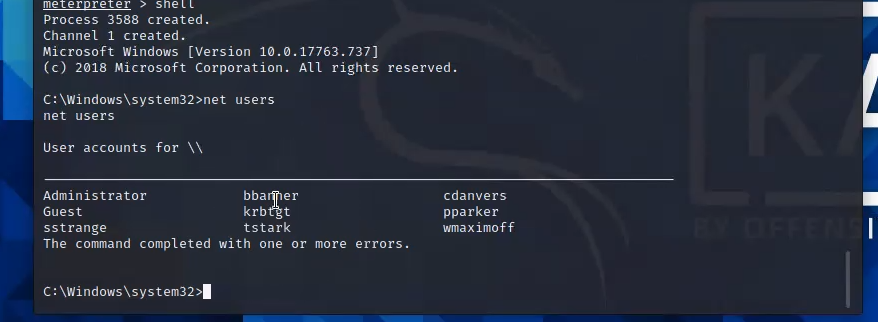
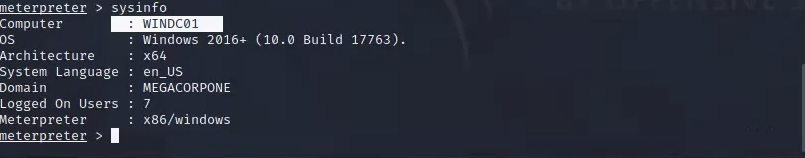


After gaining access to the target host 172.22.117.20 TecEx created a shell.exe file containing an reverse\_tcp exploit to gain backdoor access. Using Metasploit we were able to escalate our privileges which allowed TecEx to use Meterpreter on the system admin account.

To keep this persistent TecEx modified processes to hide the system admin backdoor process in the system processes. TecEx also made a service.exe file and scheduled a task to run this file on reboots.



Using Mimikatz in Metasploit TecEx was able to dump the LSASS memory and get credentials for the user bbanner. Using John the Ripper again with proper formatting TecEx was able to crack the password hashes for all 3 users. 

Using similar techniques TecEx was able to use the banner credentials and exploit SMB to gain access to the DC host 172.22.117.10. After gaining access using Meterpreter TecEx looked up the users for the DC host finding the user cdanvers. Using Meterpreter to dump the NTLM file to get the password hash for cdanvers an admin for the DC giving TecEx complete control of the network.

This Concludes the Summary of the penetration test from TecEX.

## Summary Vulnerability Overview

| **Vulnerability** | **Severity** |
| --- | --- |
| Weak password on public web application | **Critical** |
| Weak user passwords | **Critical** |
| Process Injection | **Critical** |
| OS Credential Dumping: LSASS Memory | **Critical** |
| Remote Services: SMB/Windows Admin Shares | **High** |
| [Create or Modify System Process](https://attack.mitre.org/techniques/T1543/) | **High** |
| Scheduled Task/Job | **High** |
| External Remote Services | **Medium** |
| Create Accounts | **Medium** |
| Application Layer Protocol | **Medium** |
| Exploitation for Credential Access | **Low** |
| Network Share Discovery | **Low** |

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

| **Scan Type** | **Total** |
| --- | --- |
| Hosts | 172.22.117.100,172.22.117.150,  172.22.117.10,117.22.117.20 |
| Ports | 445,135,22,443,80 |

| **Exploitation Risk** | **Total** |
| --- | --- |
| **Critical** | 4 |
| **High** | 3 |
| **Medium** | 3 |
| **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. TecEx 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.

### Weak Passwords on User Accounts

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

**Description**:

Multiple users in the private network for MegaCorpOne credentials were stolen using metasploit exploits. Gaining access to admin accounts TecEx was able to copy the /etc/shadow files and use John the Ripper with a wordlist to crack password hashes. Using Metasploit along with Kiwi TecEx was able to dump the LSASS memory and the NTLM. Using John the Ripper TecEx was able to crack all passwords.

**Affected Hosts**: 172.22.117.100 172.22.117.150 172.22.117.10 172.22.117.20

**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 **tstark**’s, **pparker**’s, **cdanvers**', and **bbanner**’s password.

### Process Injection

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

**Description**:

Using Msfvenom TecEx made a shell.exe file containing a reverse\_tcp exploit. Using the credentials for tstark we were able to login to the SMB client for host 172.22.117.20 and download the shell.exe file to the C:\ location. Using metasploit to run a WMI execution exploit through the SMB service we were able to execute the shell.exe file on the target host 172.22.117.20. Once the session was created TecEx used another exploit in Metasploit to run Meterpreter on the targeted host and gain persistence access.

**Affected Hosts**: Target:(172.22.117.20) Source:(172.22.117.100)

**Remediation**:

* Set up host firewall to restrict file sharing communications such as SMB
* Network intrusion detection and prevention systems that use network signatures to scan traffic for malware or unusual data transfer over known tools and protocols.

### 

# OS Credential Dumping: LSASS Memory

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

**Description**:

Using Metasploit TecEx loads an extension for MimiKatz called Kiwi. Kiwi allows for some additional commands that can dump the SAM. Using the Command lsa\_dump\_sam TecEx was able to reveal usernames and NTLM password hashes from host 172.22.117.20.

**Affected Hosts**: Target:(172.22.117.20)

* **Remediation**: Consider disabling or restricting NTLM.
* Consider disabling WDigest authentication.On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing.
* Ensure that local administrator accounts have complex, unique passwords across all systems on the network.

<https://attack.mitre.org/techniques/T1003/001/>

# Remote Services: SMB/Windows Admin Shares

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

**Description**:

Using Nessus to scan the target host 172.22.117.20 TecEx was able to find a vulnerability in the SMB service the target host is running. Using Nmap to scan for what ports are open TecEx found that port 445 is running SMB service. Using metasploit to run a SMB login exploit with the credentials of tstark that was decoded TecEx was able to gain a meterpreter session into the target host.

**Affected Hosts**:

**Remediation**:

* Deny remote use of local admin credentials to log into systems. Do not allow domain user accounts to be in the local Administrators group multiple systems.
* Consider disabling Windows administrative shares.
* Do not reuse local administrator account passwords across systems. Ensure password complexity and uniqueness such that the passwords cannot be cracked or guessed.
* Deny remote use of local admin credentials to log into systems. Do not allow domain user accounts to be in the local Administrators group multiple systems.

<https://attack.mitre.org/techniques/T1021/002/>

## MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully

Failure to perform

[MITRE ATT&CK navigator map]

