



Cybersecurity

## Penetration Test Report Template

**MegaCorpOne**

### **Penetration Test Report**

**ZeroDay Cyber Assurance, 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

<b>Company Name</b>	ZeroDay Cyber Assurance, LLC
<b>Contact Name</b>	Paul Lindsay
<b>Contact Title</b>	Penetration Tester
<b>Contact Phone</b>	555.224.2411
<b>Contact Email</b>	<a href="mailto:paullindsay@zerodayvault.com">paullindsay@zerodayvault.com</a>

## Document History

Version	Date	Author(s)	Comments
001	2024-02-15	Paul Lindsay	

## Introduction

In accordance with MegaCorpOne's policies, ZeroDay Cyber Assurance, LLC (henceforth known as ZDCA) 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 ZDCA during 2024-03-02.

For the testing, ZDCA 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.

ZDCA used its proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

MegaCorpOne has outlined the following 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

ZDCA 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

ZDCA 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

ZDCA'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

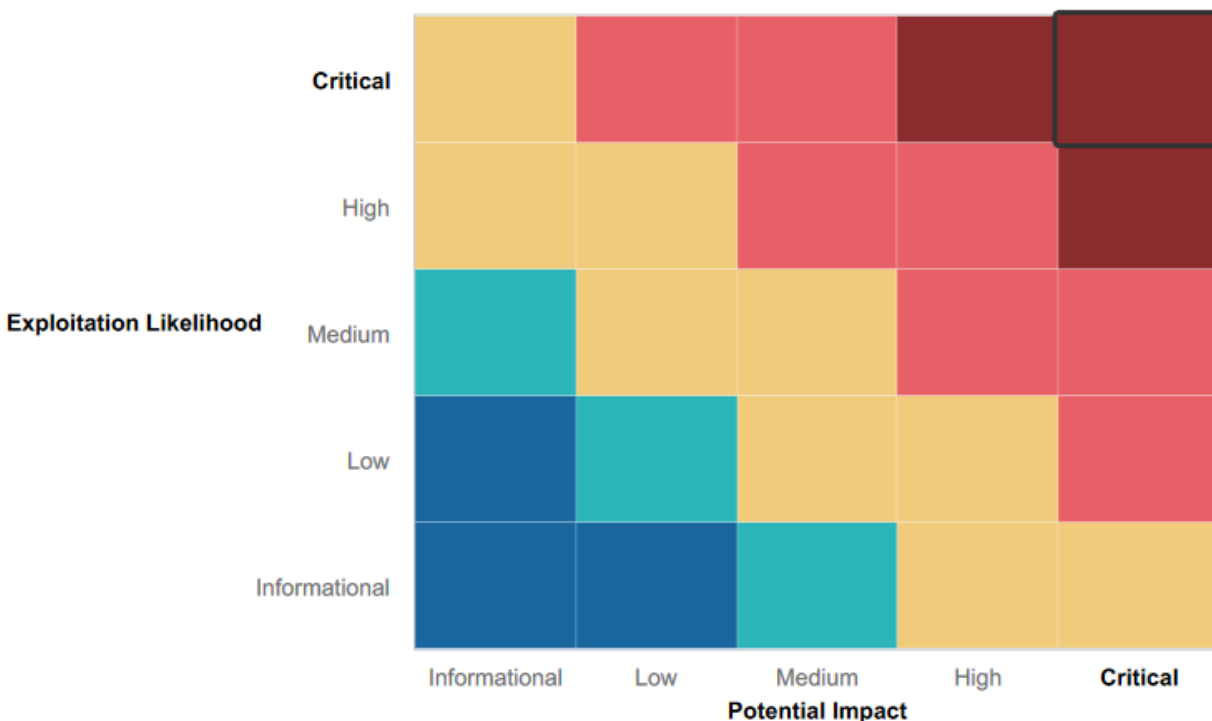
## Executive Summary of Findings

### 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

Although we are here to find and patch the weaknesses in your systems I do want to take some time here to reflect on the strengths you have already, even though we have managed to find and exploit some critical parts of the system most of our attempts were stopped which would indicate a good security scenario. Below will list some key items that outline what was not successful in creating a session or gaining unauthorized access to your systems.

### 1 - Shell Service (rshd on Port 514):

Although the exploit was attempted, no session was created, suggesting some level of resistance against unauthorized access.

### 2 - FTP Service (threectftpsvc\_long\_mode on Port 21):

The exploit was attempted, but no session was created, indicating potential security measures or configurations that prevented successful exploitation.

### 3 - FTP Service (3cdaemon\_ftp\_user on Port 21):

Similar to the previous FTP exploit, although attempted, no session was created, suggesting potential security configurations in place.

### 4 - HTTP Service (Apache httpd 2.2.8 on Port 80):

The outcome of the exploit (cayin\_xpost\_sql\_rce) is not explicitly mentioned, leaving uncertainty about the system's response to this particular attack.

### 4 - TCP Service (unreal\_ircd\_3281\_backdoor on Port 6667):

The exploit resulted in the establishment of a shell session, indicating potential vulnerabilities in the TCP service.

### 5 - MSRPC Service (Microsoft Windows RPC on Port 135):

Although the exploit was completed, no session was created, suggesting some level of resistance or security measures in place.

**6 - LDAP Service (Microsoft Windows Active Directory LDAP on Port 389):**

Similar to MSRPC, the exploit was completed, but no session was created, implying potential security measures protecting against unauthorized access.

**7 - ncacn\_http Service (Microsoft Windows RPC over HTTP 1.0 on Port 593):**

The exploit was completed, but no session was created, indicating potential security measures or configurations preventing unauthorized access.

**8 - Shell Service (Netkit rshd on Port 512):**

Similar to the previous shell exploit, the outcome was unsuccessful in creating a session, suggesting potential security measures.

**9 - FTP Service (ProFTPD 1.3.1 on Port 2121):**

The exploit was completed, but no session was created, implying potential security measures or configurations in place.

**10 - HTTP Service (Apache Tomcat/Coyote JSP engine 1.1 on Port 8180):**

Similar to other HTTP exploits, the outcome was unsuccessful in creating a session, indicating potential security measures.

Resistance or security measures that are in place already preventing successful exploitation in some cases would be considered a strength in the system and we see that a lot here. Lack of successful session creation in response to certain exploit attempts help display to us the pros in a world full of cons. It is important to not see the overwhelming amount of bad but to understand what is critical and what is already in place defending your systems.

## Summary of Weaknesses

ZDCA successfully found several vulnerabilities that should be addressed in order of severity 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 - FTP Service (vsftpd 2.3.4 on Port 21):**

2 - Vulnerability exploited successfully with a backdoor bind listener open, allowing shell access. Shell Service (rshd on Port 514):

3 - Vulnerability exploited, but no session was created.

FTP Service (threeftpsvc\_long\_mode on Port 21):

4 - Vulnerability exploited, but no session was created.

FTP Service (3cdaemon\_ftp\_user on Port 21):

5 - Vulnerability exploited, but no session was created.

HTTP Service (Apache httpd 2.2.8 on Port 80):

6 - Vulnerability (cayin\_xpost\_sql\_rce) not explicitly mentioned in terms of outcome, but the exploit was attempted.

TCP Service (unreal\_ircd\_3281\_backdoor on Port 6667):

7 - Vulnerability exploited successfully, leading to the establishment of a shell session.

MSRPC Service (Microsoft Windows RPC on Port 135):

8 - Vulnerability exploited, but no session was created.

LDAP Service (Microsoft Windows Active Directory LDAP on Port 389):

9 - Vulnerability exploited, but no session was created.

ncacn\_http Service (Microsoft Windows RPC over HTTP 1.0 on Port 593):

10 - Vulnerability exploited, but no session was created.  
Shell Service (Netkit rshd on Port 512):

11 - Vulnerability exploited, but no session was created.  
FTP Service (ProFTPD 1.3.1 on Port 2121):

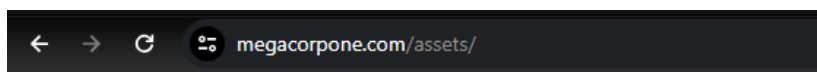
12 - Vulnerability exploited, but no session was created.  
HTTP Service (Apache Tomcat/Coyote JSP engine 1.1 on Port 8180):

13 - Vulnerability exploited, but no session was created.

The system's weaknesses include a range of vulnerabilities using services like FTP, SHELL, HTTP, TCP, MSRPC, and LDAP that have been exploited to varying degrees of success but some more critical situations which resulted in establishing a shell session giving us unauthorized access.

## Reconnaissance

- Using Google searching methods we were able to find megacorpone's Index of asset,multiple .js files as well as all information on the company and the team.



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

\*\*\*\*As you can see here we were able to access this index and then from there we can explore any of these directories\*\*\*\*\*










[Company information](#) [Email Format](#) [Management](#)




## Megacorp One

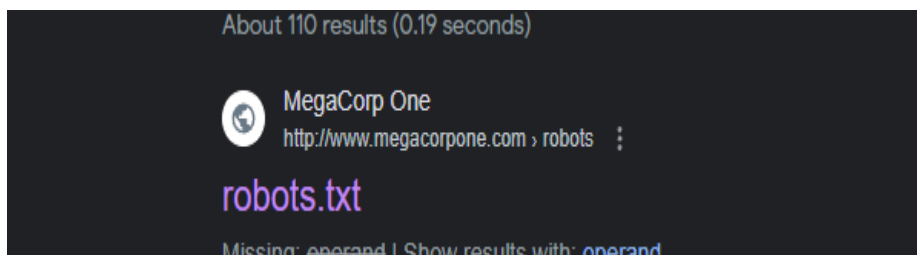
Megacorp One's email is [sales@megacorpone.com](mailto:sales@megacorpone.com) and Megacorp One's phone number is [903-883-6342](tel:903-883-6342) .  
[View all details for Megacorp One](#)

[View Top Employees for Megacorp One](#)

	<b>Website</b>	<a href="http://megacorpone.com">megacorpone.com</a>
	<b>Industry</b>	Nanotechnology
	<b>Location</b>	Rachel, Nevada, United States
	<b>Employees</b>	3
	<b>Phone</b>	903-883-6342
	<b>Email</b>	<a href="mailto:sales@megacorpone.com">sales@megacorpone.com</a>
	<b>Competitors</b>	Fei Company, Zeiss Microscopy, Qc, Hollingsworth & Vose, Sanki Global, Università Degli Stud...

 **Top Competitors for Megacorp One**

Using this same method we were also able to find a hidden file within the MegaCorpOne domain listed below,



Contents of this file :

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

- Perform nslookup on "[www.megacorpone.com](http://www.megacorpone.com)" which resulted in giving us the server ip of 172.22.117.10
- using this information we then performed NMAP/ZENMAP scan of the network 172.16.117.0/24 providing us with some information regarding the port vulnerabilities, see below for the results of this scan.

List of open ports :

```

nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery,smb-system-info 172.22.117.0/24
NSE: Script scanning 2 hosts.
Initiating NSE at 11:55
Completed NSE at 11:55, 8.07s elapsed
Initiating NSE at 11:55
Completed NSE at 11:56, 8.01s elapsed
Nmap scan report for WinDC01 [172.22.117.10]
Host is up (0.00070s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-03-02 16:53:19Z)
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)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=3/2%OT=53%CT=1%CU=40672%PV=Y%D5=1%DC=0%G=Y%M=00155D%TM
OS:6E3E35A21%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10A%TI=I%CI=I%II=I%
OS:SS=S%TS=U)OPS(O1=MSB4NW8NNS%O2=MSB4NW8NNS%O3=MSB4NW8NNS%O4=MSB4NW8NNS%O5=M5
OS:B4NW8NNS%O6=MSB4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
OS:ECN(R=Y%DF=Y%T=80%W=FFFF%O=MSB4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%W=0%A=S+%
OS:F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=RD=0%Q=)T3(R=Y%DF=Y%T=
OS:80%W=0%S=Z%A=0%F=AR%O=RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=RD=0%
OS:10%T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=
OS:1AA=0%F=R%O=RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=RD=0%Q=)U1(R=
OS:Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:I=80%CD=Z)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```

```

nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery,smb-system-info 172.22.117.0/24
References:
- https://www.securityfocus.com/bid/48539
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
- http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
- https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd\_234\_backdoor.rb
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)
|_ http.server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp    open  rpcbind      2 (RPC #100000)
rpcinfo:
  program version  port/proto service
  100000 2 111/tcp rpcbind
  100000 2 111/udp rpcbind
  100003 2,3,4 2049/tcp nfs
  100003 2,3,4 2049/udp nfs
  100005 1,2,3 34781/tcp mountd
  100005 1,2,3 53533/udp mountd
  100021 1,3,4 39313/tcp nlockmgr
  100021 1,3,4 54937/udp nlockmgr
  100024 1 40918/udp status
  100024 1 44960/tcp status
139/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp    open  exec         netkit-rsh rshcd
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 (Admin email admin@Metasploitable.LAN)
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)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux kernel:2.6
OS details: Linux 2.6.9 - 2.6.33

```

```

nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery,smb-system-info 172.22.117.0/24
1 1.59 ms 172.22.117.150

Initiating SYN Stealth Scan at 11:56
Scanning 172.22.117.100 [1000 ports]
Discovered open port 80/tcp on 172.22.117.100
Discovered open port 6001/tcp on 172.22.117.100
Discovered open port 5901/tcp on 172.22.117.100
Completed SYN Stealth Scan at 11:56, 1.23s elapsed (1000 total ports)
Initiating Service scan at 11:56
Scanning 3 services on 172.22.117.100
Completed Service scan at 11:56, 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 11:56
Completed NSE at 11:56, 0.02s elapsed
Initiating NSE at 11:56
Completed NSE at 11:56, 0.00s elapsed
Nmap scan report for 172.22.117.100
Host is up (0.000055s 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: 3.148 days (since Wed Feb 28 08:22:52 2024)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: 127.0.1.1

NSE: Script Post-scanning.
Initiating NSE at 11:56
Completed NSE at 11:56, 0.00s elapsed
Initiating NSE at 11:56
Completed NSE at 11:56, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 193.79 seconds
Raw packets sent: 3635 (156.874KB) | Rcvd: 4165 (176.803KB)

```

Version of SSH running on server: SSH-2.0-OpenSSH\_7.9p1 Debian-10+deb10u2

OS : Debian

Version of web server : Apache 2.4.38

Vulnerabilities that may be present on the server: CVE-2019-0215, CVE-2019-0220, CVE-2019-0217, CVE-2019-0197, CVE-2019-0196, CVE-2019-0211

Server Location : Montreal Canada

Recon-ng :

```

root@kali: ~
File Actions Edit View Help

MEGACORPONE.COM

[*] Country: None
[*] Host: admin.megacorpone.com
[*] Ip_Address: 51.222.169.208
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: beta.megacorpone.com
[*] Ip_Address: 51.222.169.209
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: fs1.megacorpone.com
[*] Ip_Address: 51.222.169.210
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: intranet.megacorpone.com
[*] Ip_Address: 51.222.169.211

```

```
root@kali: ~  
File Actions Edit View Help  
[*] Ip_Address: 51.222.169.211  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] Country: None  
[*] Host: mail.megacorpone.com  
[*] Ip_Address: 51.222.169.212  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] Country: None  
[*] Host: mail2.megacorpone.com  
[*] Ip_Address: 51.222.169.213  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] Country: None  
[*] Host: ns1.megacorpone.com  
[*] Ip_Address: 51.79.37.18  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] Country: None
```

```
root@kali: ~  
File Actions Edit View Help  
[*] Country: None  
[*] Host: ns2.megacorpone.com  
[*] Ip_Address: 51.222.39.63  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] Country: None  
[*] Host: ns3.megacorpone.com  
[*] Ip_Address: 66.70.207.180  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] Country: None  
[*] Host: router.megacorpone.com  
[*] Ip_Address: 51.222.169.214  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
[*]  
[*] Country: None  
[*] Host: siem.megacorpone.com  
[*] Ip_Address: 51.222.169.215  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None
```

```

root@kali: ~
File Actions Edit View Help
[*] Country: None
[*] Host: snmp.megacorpone.com
[*] Ip_Address: 51.222.169.216
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: support.megacorpone.com
[*] Ip_Address: 51.222.169.218
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: syslog.megacorpone.com
[*] Ip_Address: 51.222.169.217
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: test.megacorpone.com
[*] Ip_Address: 51.222.169.219
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*]
[*] Country: None
[*] Host: vpn.megacorpone.com
[*] Ip_Address: 51.222.169.220
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: www.megacorpone.com
[*] Ip_Address: 149.56.244.87
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: www2.megacorpone.com
[*] Ip_Address: 149.56.244.87
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]

SUMMARY
[*] 18 total (0 new) hosts found.
[recon-ng][default][hackertarget] >
[recon-ng][default] >

```

## Identification of Vulnerabilities and Services

- **Exploit:** vsftpd 2.3.4
- **Host IP address:** 172.22.117.150
- **Port:** 21
- **Service name:** FTP
- **Service version:** 2.3.4
- **Exploit outcome:** Backdoor bind listener open, shell found and created -- Success--

- 
- **Exploit:** linux/telnet/telnet\_encrypt\_keyid

- **Host IP address:**172.22.117.150
  - **Port:** 514
  - **Service name:** Shell
  - **Service version:** rshd
  - **Exploit outcome :** Exploit completed but no session was created
- 

- **Exploit:** threectftpsvc\_long\_mode
  - **Host IP address:** 172.22.117.150
  - **Port:**21
  - **Service name:**ftp
  - **Service version:**2.3.4
  - **Exploit outcome:** Exploit completed but no session was created
- 

- **Exploit:** 3cdaemon\_ftp\_user
  - **Host IP address:**172.22.117.150
  - **Port:**21
  - **Service name:** ftp
  - **Service version:**2.3.4
  - **Exploit outcome:** Exploit completed but no session was created
- 

- **Exploit:** cayin\_xpost\_sql\_rce
  - **Host IP address:**172.22.117.150
  - **Port:** 80
  - **Service name:** http
  - **Service version:** Apache httpd 2.2.8 ((Ubuntu) DAV/2)
  - **Exploit outcome:** Exploit completed, but no session was created
- 

- **Exploit:** unreal\_ircd\_3281\_backdoor
  - **Host IP address:**172.22.117.150
  - **Port:**6667
  - **Service name:** tcp
  - **Service version:** UnrealIRCd 3.2.8.1
  - **Exploit outcome:** Exploit created // Session established Shell gained \*\*\*\*\*
- 

- **Exploit:** dcerpc/ms05\_017\_msmq
  - **Host IP address:**172.22.117.10
  - **Port:**135
  - **Service name:** MSRPC
  - **Service version:** Microsoft Windows RPC
  - **Exploit outcome:** Exploit completed, but no session was created
- 

- **Exploit:**ldap/pgp\_keyserver7
- **Host IP address:**172.22.117.10
- **Port:**389
- **Service name:** ldap
- **Service version:** Microsoft Windows Active Directory LDAP (Domain:megacorpone.local0., Site: Default-First-Site-Name)



- **Exploit outcome: Exploit completed, but no session was created**

- 
- **Exploit:** msf\_rpc\_console
  - **Host IP address:** 172.22.117.10
  - **Port:** 593
  - **Service name:** ncacn\_http
  - **Service version:** Microsoft Windows RPC over HTTP 1.0
  - **Exploit outcome: Exploit completed, but no session was created**

- 
- **Exploit:** telnet\_encrypt\_keyid
  - **Host IP address:** 172.22.117.150
  - **Port:** 512
  - **Service name:** shell
  - **Service version:** Netkit rshd
  - **Exploit outcome: Exploit completed, but no session was created**

- 
- **Exploit:** netsupport\_manager\_agent
  - **Host IP address:** 172.22.117.150
  - **Port:** 2121
  - **Service name:** ftp
  - **Service version:** ProFTPD 1.3.1
  - **Exploit outcome: Exploit completed, but no session was created**

- 
- **Exploit:** tomcat\_jsp\_upload\_bypass
  - **Host IP address:** 172.22.117.150
  - **Port:** 8180
  - **Service name:** http
  - **Service version:** Apache Tomcat/Coyote JSP engine 1.1
  - **Exploit outcome: Exploit completed, but no session was created**

## Executive Summary

When completing our comprehensive assessment of Mega Corp One's network we used reconnaissance and penetration testing techniques to help us evaluate the organization's cybersecurity posture. Our objective was to identify security vulnerabilities that could potentially be exploited by malicious actors and pose a threat to Mega Corp One data security and overall business. We were asked to find and exfiltrate any sensitive information within the domain, escalate privileges to domain administrator and compromise at least 2 machines.

Our efforts revealed significant exposure in Mega Corp One's asset index, including multiple JavaScript files and critical company information. We were also able to find and identify a hidden file exposed to the public pointing to specific infrastructure weaknesses. Through nslookup and network scanning utilizing tools like NMAP/ZENMAP we were able to pinpoint several, open ports and identify the version details of critical services such as SSH and Apache, alongside the servers operating system. With this information we were able to map out potential vulnerabilities accurately.

The penetration test we executed uncovered several high-risk vulnerabilities that are directly associated with outdated and misconfigured services, for example the vsftpd 2.3.4 service allowed

backdoor access, posing a huge security risk. Other risks identified include issues in the telnet encryption, ftp services, and various service-specific exploits that would be able to gain unauthorized access or could use remote code execution.

To mitigate this, we strongly recommend immediately updating and patching all vulnerable services listed to their latest versions to protect against known exploits. Special attention should be given to critical services like vsftpd, Apache, and SSH. Replacing the use of insecure protocols, such as telnet, with secure ones like SSH to prevent any unauthorized access or eavesdropping of any kind. Firewall rules are also extremely important as the rules to restrict access to the identified vulnerable service from untrusted networks, minimizing the attack surface for attackers. Lastly enhance security awareness among staff and IP personnel to help recognize and respond to security threats proactively.

The penetration test of Mega Corp One's network has definitely uncovered multiple critical vulnerabilities that necessitate immediate attention, but that being said by addressing these vulnerabilities and implementing the recommended security measures, Mega Corp One can significantly improve its defense against potential cyber attacks, safeguarding its assets and continuing to gain the trust of their clients and stakeholders. Having a strong commitment to cybersecurity and its best practices is essential for protecting against the evolving threat landscape.

## Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
vsftpd 2.3.4	Critical
unreal_ircd_3281_backdoor	Critical
cayin_xpost_sql_rce	High
telnet_encrypt_keyid	High
dcerpc/ms05_017_msmq	Medium
ldap/pgp_keyserver7	Medium
msf_rpc_console	Medium
netsupport_manager_agent	Medium
3cdaemon_ftp_user	Low
tomcat_jsp_upload_bypass	Low

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

Scan Type	Total
Hosts	172.22.117.150 172.22.117.10
Ports	21 (FTP) 514 (SHELL) 6667 (TCP)



	135 (MSRPC) 389 (LDAP) 593 (ncacn_http) 512 (SHELL) 2121 (FTP) 8180 (HTTP)
--	---

Exploitation Risk	Total
<b>Critical</b>	3
<b>High</b>	2
<b>Medium</b>	5
<b>Low</b>	3

# 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. ZDCA 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.

## vsftpd 2.3.4

**Risk Rating:** Critical

**Description:**

This version of vsftpd is known to have a serious security vulnerability that was introduced intentionally into the code as a backdoor. This backdoor was quickly discovered and removed, but it serves as a stark reminder of the importance of maintaining security practices, including using secure sources for software and keeping software up to date.

**Affected Hosts:** 172.22.117.150

**Remediation:**

- Update vsftpd: The most critical step is to update vsftpd to a version that has patched this vulnerability. The backdoor was quickly fixed, so any version after 2.3.4 should not contain this specific vulnerability.
- Regularly Update Software: Regularly update all software to protect against known vulnerabilities.
- Use Firewalls: Configure firewalls to restrict access to necessary ports only.
- Monitor Network Traffic: Unusual network activity can indicate an attempted or successful exploit.
- Source Verification: Ensure software is downloaded from official or trusted sources to avoid tampered versions

## unreal\_ircd\_3281\_backdoor

**Risk Rating:** Critical

**Description:**

This exploit will allow an attacker to connect to the IRC server and issue a special command that gives them access to execute arbitrary commands on the server with the privileges of the user running the UnrealIRCd service. This could potentially lead to unauthorized control over the server, data theft, installation of malware, and other malicious activities.

**Affected Hosts:** 172.22.117.150

**Remediation:**

- **Update the Software:** The immediate action after the discovery of the backdoor was to download a clean version of UnrealIRCd from a trusted source. Users were urged to verify the integrity of their software using checksums or signatures provided by the developers.
- **Regularly Verify Software Integrity:** Regularly check the integrity of installed software, especially those downloaded from the internet, using cryptographic hashes or digital signatures.
- **Monitor and Restrict Access:** Implement monitoring to detect unusual activities and restrict access to what is necessary for operation.
- **Firewalls and Intrusion Detection Systems (IDS):** Use firewalls and IDS to detect and prevent unauthorized access.

## Cayin\_xpost\_sql\_rce

**Risk Rating:** High

**Description:**

An attacker could exploit this by crafting malicious SQL queries that the application executes without the proper validation. If this is successful, it could lead to unauthorized access to the database allowing the attacker to read, modify, or delete database entries. In some cases, if the SQL injection flaw is severe enough and the database server is misconfigured it could also lead to the execution of arbitrary code on the server.

**Affected Hosts:** 172.22.117.150

**Remediation:**

- **Input Validation:** Ensure all user inputs are properly validated and sanitized before processing. Use allow lists wherever possible.
- **Prepared Statements and Parameterized Queries:** Use prepared statements with parameterized queries instead of constructing SQL queries with user input directly. This effectively separates the data from the command, making it harder for an attacker to inject malicious SQL.
- **Least Privilege:** Ensure the database user used by the web application has the least privileges necessary. This minimizes the potential impact of a successful SQL injection attack.
- **Regular Updates and Patches:** Keep all software components, including web applications, databases, and server operating systems, up to date with the latest security patches.
- **Web Application Firewall (WAF):** Deploy a WAF to help detect and block SQL injection attempts and other common web attack vectors.

## telnet\_encrypt\_keyid

**Risk Rating:** High

**Description:** This is associated with a vulnerability in the telnet service, a network protocol used on the internet or local area networks to provide a bidirectional interactive text-oriented

communication facility. This appears to involve weaknesses in the encryption mechanism used by the telnet service. This will allow attackers to potentially exploit encryption keys or manipulate encryption-related parameters to compromise the security of the communication channel.

**Affected Hosts:** 172.22.117.150

**Remediation:**

- Use Secure Protocols: Whenever possible, use more secure protocols such as SSH (Secure Shell) for remote terminal access, which provides stronger encryption and authentication.
- 
- Disable Telnet: If feasible, consider disabling the Telnet service altogether in favor of more secure alternatives.
- 
- Keep Software Updated: Ensure that Telnet implementations and related software are kept up to date with the latest security patches and updates to address known vulnerabilities.
- 
- Network Segmentation: Implement network segmentation to restrict Telnet access to trusted networks or hosts, reducing the exposure to potential attackers.
- 
- Encryption Best Practices: If Telnet encryption is necessary, follow best practices for encryption, including using strong encryption algorithms, secure key management practices, and enforcing encryption for all sessions.

## **dcercpc/ms05\_017\_msmq**

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

**Description:**

This vulnerability is due to a flaw in the processing of MSMQ packets by the Distributed Component Object Model Remote Procedure Call interface. An attacker could exploit this vulnerability by sending a specially crafted MSMQ packet to the vulnerable system allowing the possible execution of code in the context of the system account.

**Affected Hosts:** 172.22.117.10

**Remediation:**

- To mitigate the risk associated with this vulnerability, Microsoft released a security update as part of Security Bulletin MS05-017. System administrators were advised to apply the appropriate patch to affected systems to remediate the vulnerability.

## **ldap/pgp\_keyserver7**

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

**Description:**

PGP key servers are used to store and distribute PGP public keys, these will be used for secure communication, encryption, and digital signatures. If a vulnerability or exploit targeting a PGP keyserver component could potentially involve security issues related to data integrity, authentication, or confidentiality or PGP keys stored on the server.

**Affected Hosts:** 172.22.117.10

**Remediation:**

- **Stay Informed:** Keep up to date with security advisories and updates from the maintainers of PGP key server software or any related software components.
- **Apply Security Patches:** Promptly apply security patches and updates provided by the software vendors to address known vulnerabilities.
- **Security Best Practices:** Implement security best practices such as proper access controls, encryption of sensitive data, and regular security audits.
- **Network Segmentation:** Implement network segmentation to restrict access to key server services and minimize the impact of potential exploits.
- **Monitoring and Logging:** Implement monitoring and logging mechanisms to detect and respond to suspicious activities or unauthorized access attempts.
- **Security Testing:** Conduct security testing, including vulnerability scanning and penetration testing, to identify and address potential security weaknesses proactively.

## msf\_rpc\_console

**Risk Rating:** Medium

**Description:**

Using the msf\_rpc\_console module, an attacker can search for and select exploit modules targeting specific vulnerabilities in RPC services. Once an appropriate exploit module is selected, the attacker can configure it with relevant options and launch the attack against the target system.

**Affected Hosts:** 172.22.117.10

**Remediation:**

- Keep systems up to date with the latest security patches and updates to address known vulnerabilities.
- Employ network segmentation and firewalls to restrict access to sensitive services and limit the impact of potential exploits.
- Implement strong authentication mechanisms and access controls to prevent unauthorized access to critical systems.
- Monitor network traffic and system logs for signs of suspicious activity that may indicate exploitation attempts.

## netsupport\_manager\_agent

**Risk Rating:** Medium

**Description:**

NetSupport Manager is a remote control and desktop management software used by IT administrators to monitor and manage computers remotely. It allows administrators to perform various tasks such as remote desktop control, file transfer, inventory management, and system diagnostics. If a vulnerability were to be discovered in the NetSupport Manager Agent, it could potentially be exploited by attackers to gain unauthorized access to systems where the agent is installed, execute arbitrary code, or perform other malicious actions.

**Affected Hosts:** 172.22.117.150

**Remediation:**

- **Keep Software Updated:** Ensure that NetSupport Manager and its components are kept up to date with the latest security patches and updates provided by the vendor.
- **Implement Access Controls:** Limit access to NetSupport Manager and its agents to authorized users only. Use strong authentication mechanisms and access controls to prevent unauthorized access.
- **Network Segmentation:** Implement network segmentation to restrict access to NetSupport Manager services to trusted networks or hosts. Use firewalls to control traffic flow and limit exposure to potential attackers.
- **Monitor for Suspicious Activity:** Monitor network traffic and system logs for signs of suspicious activity that may indicate exploitation attempts or unauthorized access to NetSupport Manager services.
- **Security Assessments:** Conduct regular security assessments and vulnerability scans to identify and address any potential weaknesses or vulnerabilities in NetSupport Manager and its agents.
- **Security Awareness Training:** Provide security awareness training to employees and users to educate them about the risks associated with remote management software and how to report any suspicious activity.

## 3dcdaemon\_ftp\_user

**Risk Rating:** Low

**Description:**

3CDaemon FTP server related to user authentication or permissions. Exploiting such a vulnerability could potentially allow an attacker to gain unauthorized access to the FTP server or perform other malicious actions.

**Affected Hosts:** 172.22.117.150

**Remediation:**

- **Keep Software Updated:** Ensure that 3CDaemon and any other FTP server software you use are kept up to date with the latest security patches and updates from the vendor.
- **Strong Authentication:** Use strong and unique passwords for FTP user accounts and consider implementing multi-factor authentication for added security.
- **Limited Permissions:** Grant minimal necessary permissions to FTP users to reduce the potential impact of a compromise.
- **Monitor FTP Logs:** Regularly monitor FTP server logs for suspicious activity and unauthorized access attempts.
- **Firewall Rules:** Implement firewall rules to restrict access to the FTP server to trusted IP addresses or ranges.
- **Encrypt Data in Transit:** Enable FTP over SSL/TLS (FTPS) or use a secure alternative like SFTP (SSH File Transfer Protocol) to encrypt data in transit.
- **Network Segmentation:** Consider placing the FTP server in a separate network segment to limit access and reduce the attack surface.
- **Regular Security Audits:** Conduct regular security audits and vulnerability scans to identify and address any weaknesses in the FTP server configuration.

## tomcat\_jsp\_upload\_bypass

**Risk Rating:** Low

**Description:**

Security vulnerability in Apache Tomcat, an open-source web server and servlet container. This vulnerability allows attackers to bypass restrictions and upload malicious JSP (JavaServer Pages) files to the server, potentially leading to remote code execution or other malicious activities.

**Affected Hosts:** 172.22.117.150

**Remediation:**

- Update Apache Tomcat: Ensure that Apache Tomcat is updated to the latest version to patch known vulnerabilities.
- Disable File Uploads: If file uploads are not necessary, consider disabling this feature in Apache Tomcat to prevent potential exploitation.
- File Upload Restrictions: Implement restrictions on file uploads, including file size limits and allowed file types, to prevent the upload of malicious files.
- Input Validation: Implement strict input validation on file uploads to detect and prevent the upload of potentially malicious files.
- Web Application Firewalls (WAF): Deploy a WAF to monitor and filter incoming HTTP requests to detect and block potential exploitation attempts.
- Regular Security Audits: Conduct regular security audits and vulnerability scans to identify and address any potential security weaknesses in Apache Tomcat and other web server components.

## MITRE ATT&CK Navigator Map

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that ZDCA used throughout the assessment. Please note that because we were able to establish a root session this is why your impact zone on the right is completely yellow indicating with root user session all of these techniques could be utilized.

Legend:

Performed successfully

Failure to perform

24