# MegaCorpOne Penetration Test Summary

## Overview

This case study summarizes a hands-on penetration testing engagement performed against MegaCorpOne's simulated environment. It highlights reconnaissance, scanning, exploitation, password cracking, and persistence techniques, supported by screenshot descriptions extracted from the original report.

## Objectives

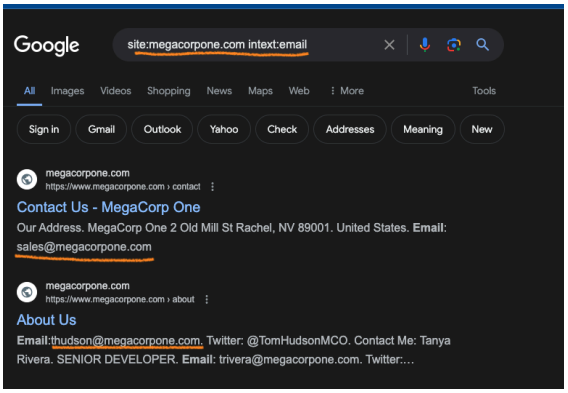
- Identify exploitable vulnerabilities within the MegaCorpOne environment.
- Compromise multiple machines.
- Escalate privileges and access sensitive information.
- Demonstrate realistic attacker methodology.

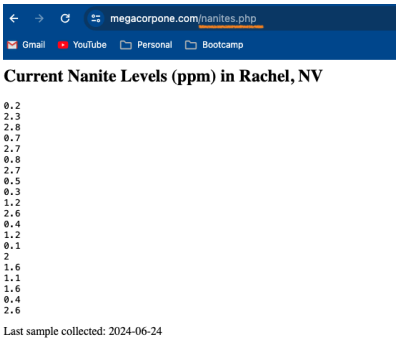
## Methodology

### 1. OSINT & Reconnaissance

Using Google dorking techniques, publicly exposed information was identified, including:

- Employee email addresses
- Internal structure references
- Public-facing server details



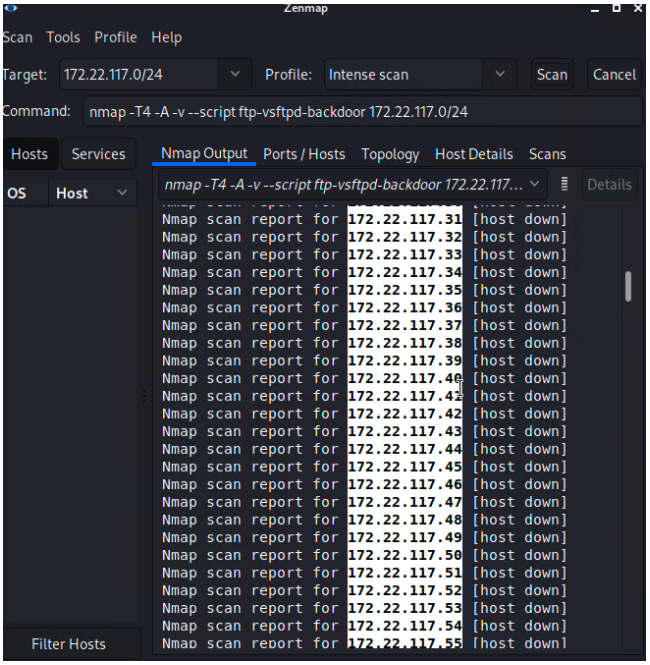



## 2. Network Scanning & Enumeration

Tools used: **Nmap**, **Zenmap**, **NSE scripts**.

Key findings:

- Open ports: 22, 80, 443
- SSH version: OpenSSH_7.9p1
- Web server: Apache 2.4.38
- OS: Debian
- Potential CVEs identified: CVE-2019-0215, CVE-2019-0220, CVE-2019-0217, and others

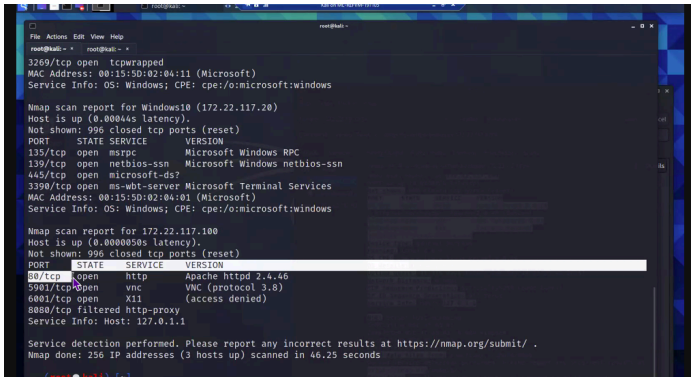


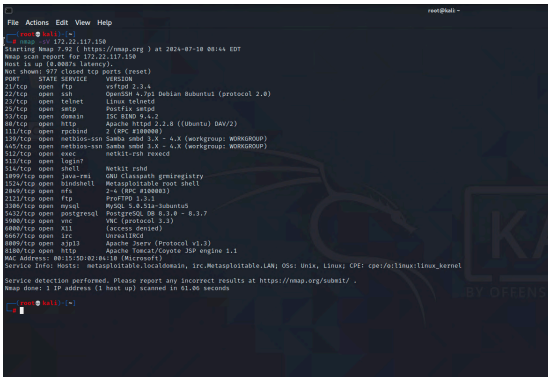

## 3. Exploitation

A critical vulnerability was discovered in **VSFTPD 2.3.4**, which contains a known backdoor.

Using Metasploit:

- Successful exploitation granted unauthorized access.
- Provided an initial foothold into the environment.



## 4. Privilege Escalation & Password Cracking

After gaining access, enumeration revealed password hashes stored in .

Using **John the Ripper**, several passwords were cracked:

- `postgres` → *postgres*
- `msfadmin` → *123456789*
- `sys` → *batman*
- `tstark` → *Password!*

These credentials enabled lateral movement and further compromise.


## 5. Persistence

A persistent SSH user was created to maintain long-term access:

- New user added:
- SSH configuration modified to allow continued access

## Key Findings

- Identified multiple critical vulnerabilities.
- Exploited a real backdoor in VSFTPD.
- Cracked several user passwords.
- Established persistent access.
- Demonstrated full attacker lifecycle: recon → exploit → escalate → persist.

## Summary

This engagement demonstrates a full attacker lifecycle and highlights several critical weaknesses within the environment. The findings highlight the importance of patching, strong credential policies, and secure service configurations.

This case study showcases real-world penetration testing methodology and hands-on offensive security capability