Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

[CyberSafe], 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	[CyberSafe], LLC
Contact Name	[Aaliyah Lockett]
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	[Aaliyahlockett]@[CyberSafe].com

Document History

Version	Date	Author(s)	Comments
001	01/17/2023	[Aaliyah Lockett]	First Draft
002	01/19/2023	Aaliyah Lockett	Second Draft
003	01/21/2023	Aaliyah Lockett	Final Revision

Introduction

In accordance with MegaCorpOne's policies, [CyberSafe], LLC (henceforth known as [CyberSafe]) 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 [CyberSafe] during January of 2023.

For the testing, [CyberSafe] 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.

[CyberSafe] 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

[CyberSafe] 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

[CyberSafe] 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

[CyberSafe]'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

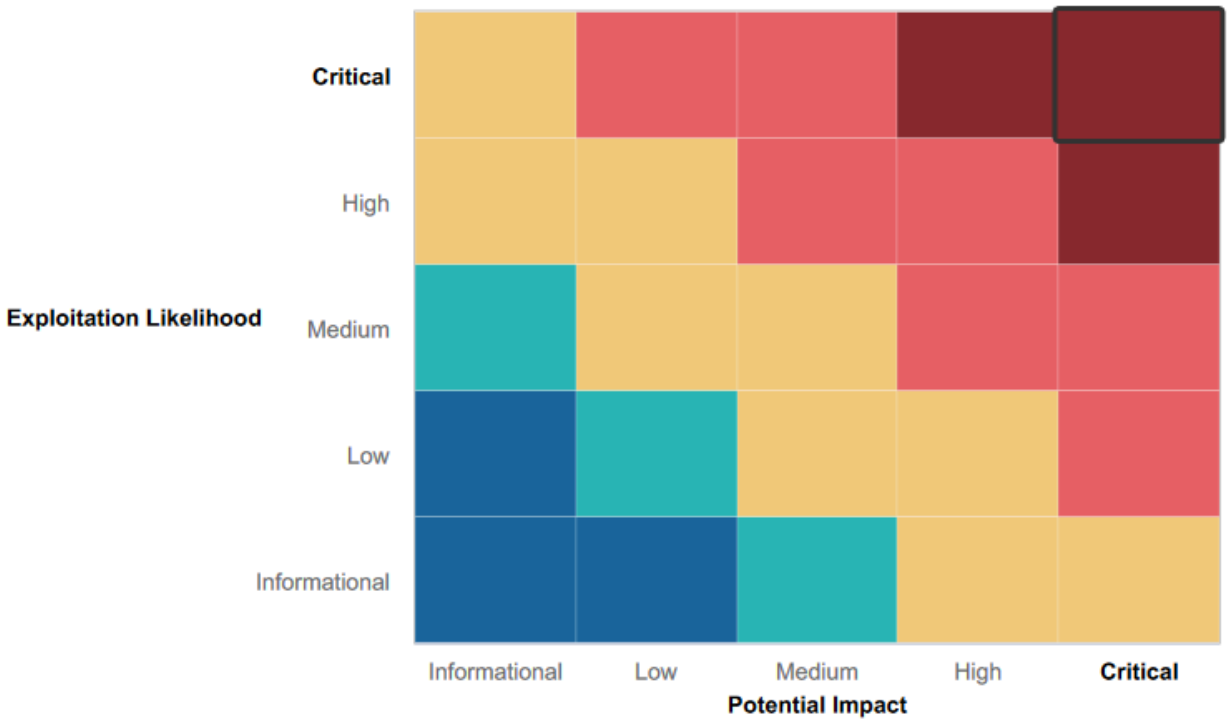
Executive Summary of Findings

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.

- [The reconnaissance of the wireless network showed that only a public facing wireless SSID. Connecting to the service requires the user to create an account, using those credentials for being able to have access. It can be suspected the SSID of the internal network is not being broadcast, thus this is preventing it from being visible by anyone outside the network.]

Summary of Weaknesses

[CyberSafe] 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.

- [During the reconnaissance phase several known vulnerabilities along with open ports can be shown and identified, in which we were able to exploit a few doing this pentest.]
- [There was very little denial for the network scanning footprinting information. This allowed us to develop the network infrastructure.]
- [From footprinting we could see that the company had the upper management contact details available to the public. This should be minimized to having more point if contact]

Executive Summary

CyberSafe, LLC conducted a security assessment on MegaCorpOne's network infrastructure to identify any existing vulnerabilities and risks. The assessment employed penetration testing methods to give MegaCorpOne's management insight into the risks and security of their current corporate environment. The internal network infrastructure was tested by using reconnaissance and host discovery tools, such as Zenmap and OSINT, to identify the operating systems, software, and services running on each target host.

Vulnerability enumeration was then used to find all potential vulnerabilities on each host and develop a list of attack vectors. Many vulnerabilities were discovered during testing, which put MegaCorpOne's resources at risk of compromise. The assessment revealed that MegaCorpOne is not adequately prepared to defend against an attack and should take immediate steps to address the findings in this report

Critical, High, and Medium severity issues were found impacting MegaCorpOne's internal network, requiring immediate action to secure the company against potential threats. These issues included poor password management practices, open ports that may have potentially vulnerable applications running, and lack of security measures on the Cisco AnyConnect configuration file.

In light of the findings, CyberSafe recommended that MegaCorpOne take immediate steps to address these vulnerabilities and implement security measures to protect against potential threats. This may include implementing password policies, patching vulnerable systems and applications, and implementing security controls on the Cisco AnyConnect configuration file. It is important for MegaCorpOne to regularly conduct security assessments to identify and address any new vulnerabilities that may arise in the future.

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
Password Cracking	Critical
Vulnerable Open Ports on the Network	Critical
LLMNR Spoofing	Critical
Compromised Machine	Critical
Site Profile on Shodan with list of known exploits.	Critical
Credential Dumping	High
Reverse shell Vulnerability	High
Windows open ports	High
Executive team contact on company site	Medium
Server details	Low

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

Scan Type	Total
Hosts	172.22.117.20 172.22.117.150 149.56.244.87
Ports	21-ftp 22-ssh 23-telnet 25-smtp 53-domain 80-http 111-rpcbind 135-msrpc 139-netbios 445-Microsoft-ds 3390 wbl-server

Exploitation Risk	Total
Critical	5
High	3
Medium	1
Low	1

Vulnerability Findings
Executive Team Business Contact on Company Website

Risk Rating: Medium

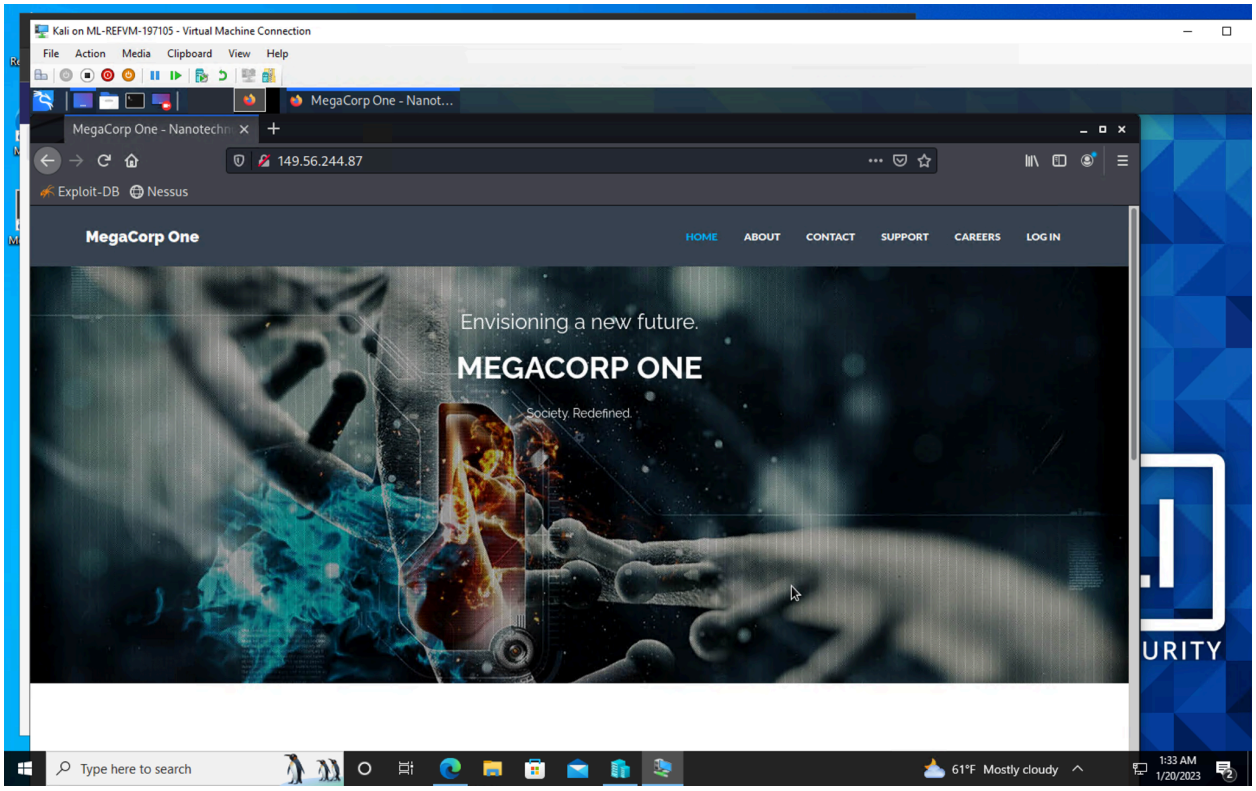
Description:
During the initial reconnaissance phase, the team at CyberSafe identified that the website www.megacorpone.com displayed a significant amount of information about the company's executive team. This information included full names, titles, email addresses, and images.

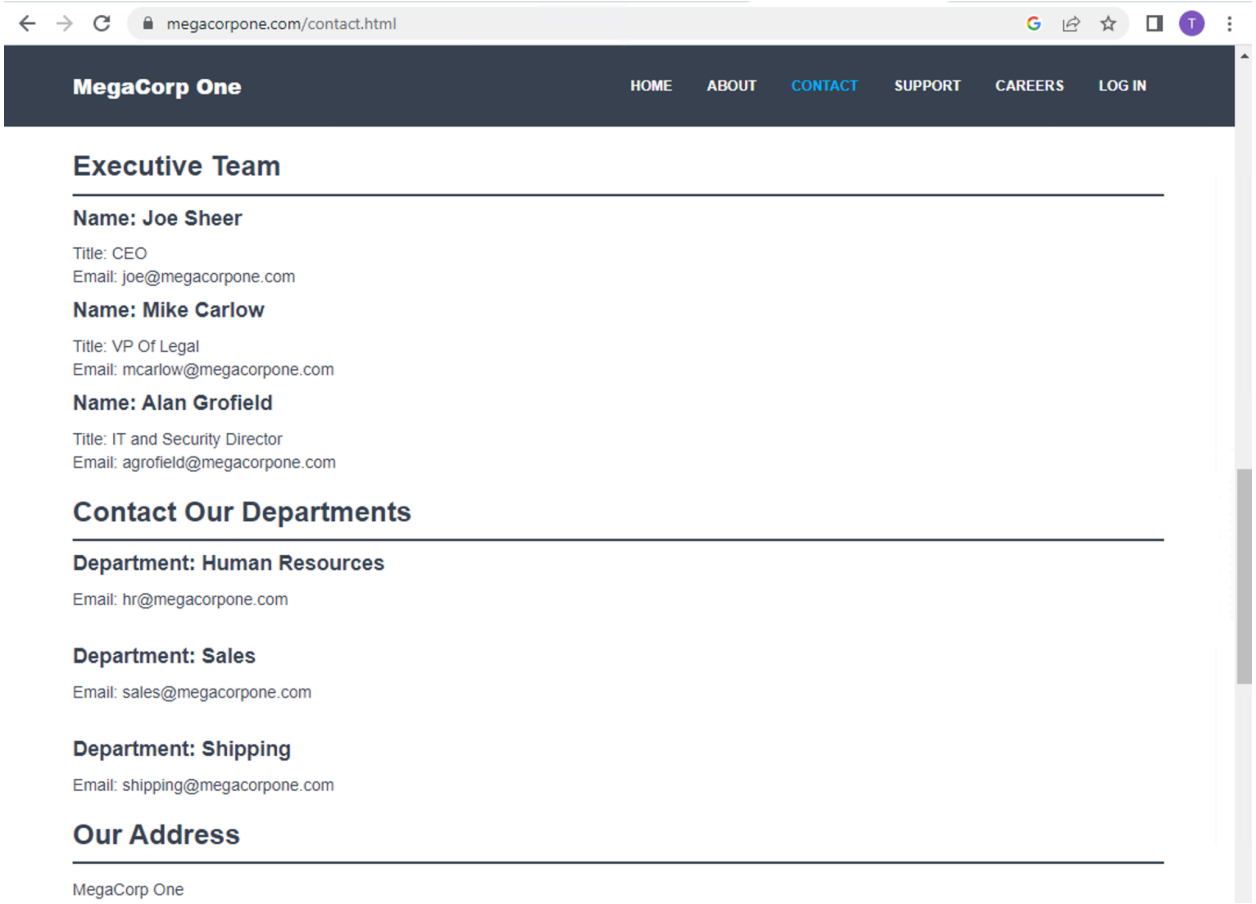
To gather this information, the team used the Google Dorking OSINT approach. This approach involves using specific search operators and queries in Google to find specific types of information. In this case, the team was able to find the names, positions, email addresses, and images of the executive team members.

Upon further analysis, CyberSafe discovered that the web server was running on a Debian operating system and using Apache 2.4.38 on port 80. This information, while seemingly insignificant on its own, can be used in combination with other information to create a detailed profile of the target. Hackers often collect information over a prolonged period to gain a better understanding of their target and to identify potential vulnerabilities.

In conclusion, while the information found on the website www.megacorpone.com may not present a significant security risk on its own, it is important to remember that hackers often collect information over time to create detailed profiles of their targets. This information, when combined with other data, can potentially pose an increased security risk. It is important for companies to be aware of the information they are displaying publicly and to take steps to protect sensitive data.

Affected Hosts: www..megacorpone.com


Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
MegaCorp One - Nanot...
MegaCorp One - Nanotechn
149.56.244.87
Exploit-DB Nessus
MegaCorp One
HOME ABOUT CONTACT SUPPORT CAREERS LOG IN
Envisioning a new future.
MEGACORP ONE
Society. Redefined.
URITY
Type here to search
61°F Mostly cloudy
1:33 AM
1/20/2023


megacorpone.com/contact.html
MegaCorp One
HOME ABOUT CONTACT SUPPORT CAREERS LOG IN
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

Site Profile Shodan.io and Known Exploits

Risk Rating: Critical

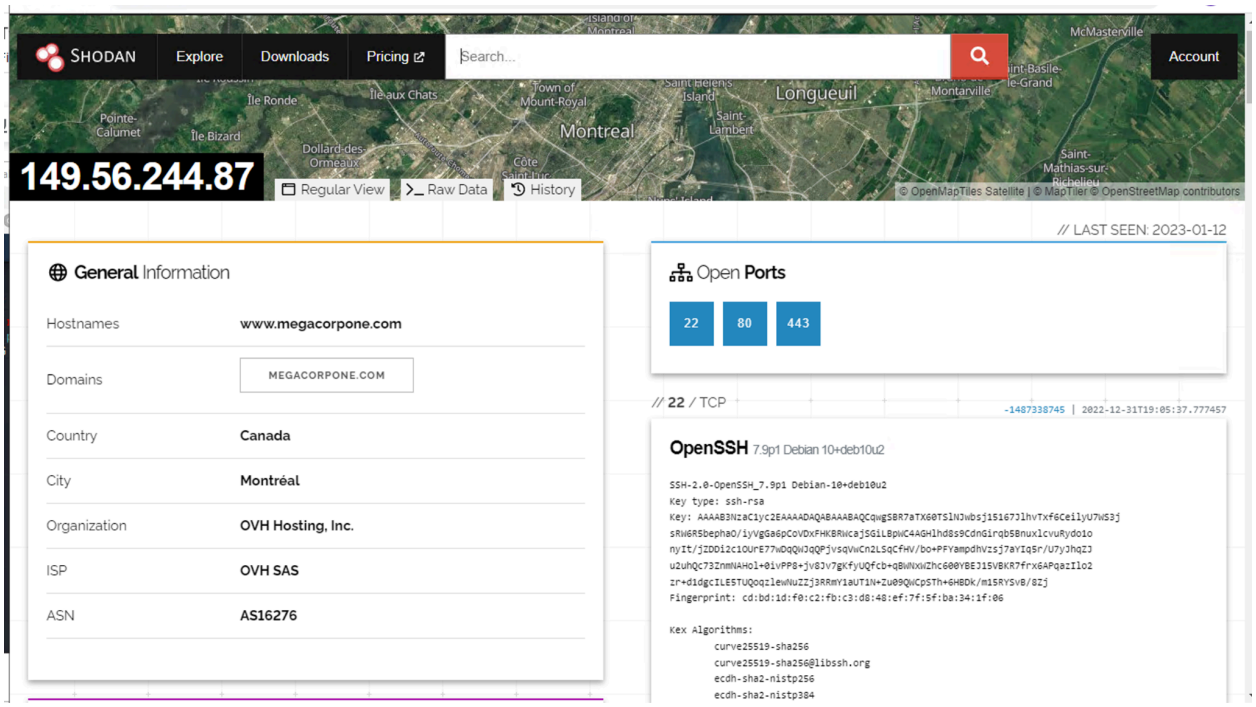
Description:
The first step in identifying potential vulnerabilities on the website www.megacorpone.com was to obtain the external IP address of the domain. This can be done by performing a basic "nslookup" or "ping scan" of the domain from a workstation. A nslookup is a simple command-line tool used to query the Domain Name System (DNS) to obtain domain name or IP address mappings. A ping scan is a type of scan that sends Internet Control Message Protocol (ICMP) echo request packets to a range of IP addresses in order to check for active hosts.

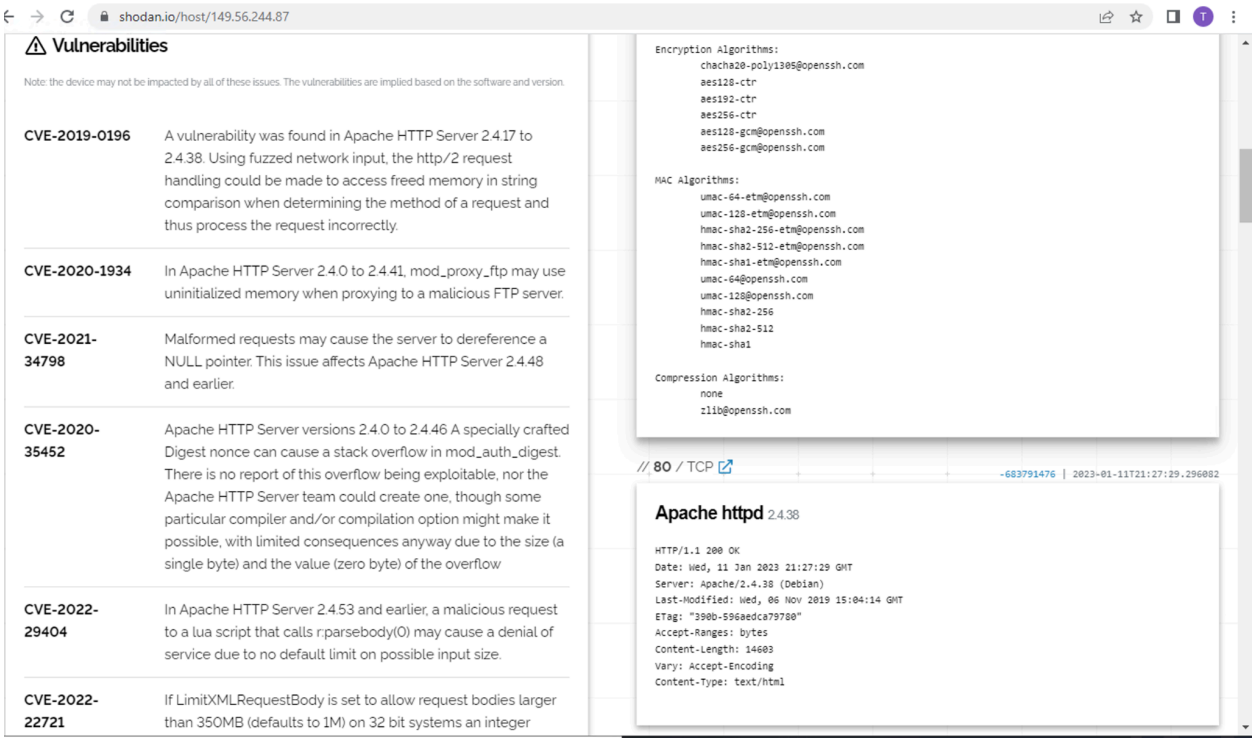
Once the external IP address was obtained, CyberSafe then used the IP address and a search engine for Internet-connected devices called Shodan.io. Shodan is a search engine that allows users to find specific types of computers (webcams, routers, servers, etc.) connected to the internet using a variety of filters. By searching for the IP address, CyberSafe was able to find the website's profile and all its associated details.

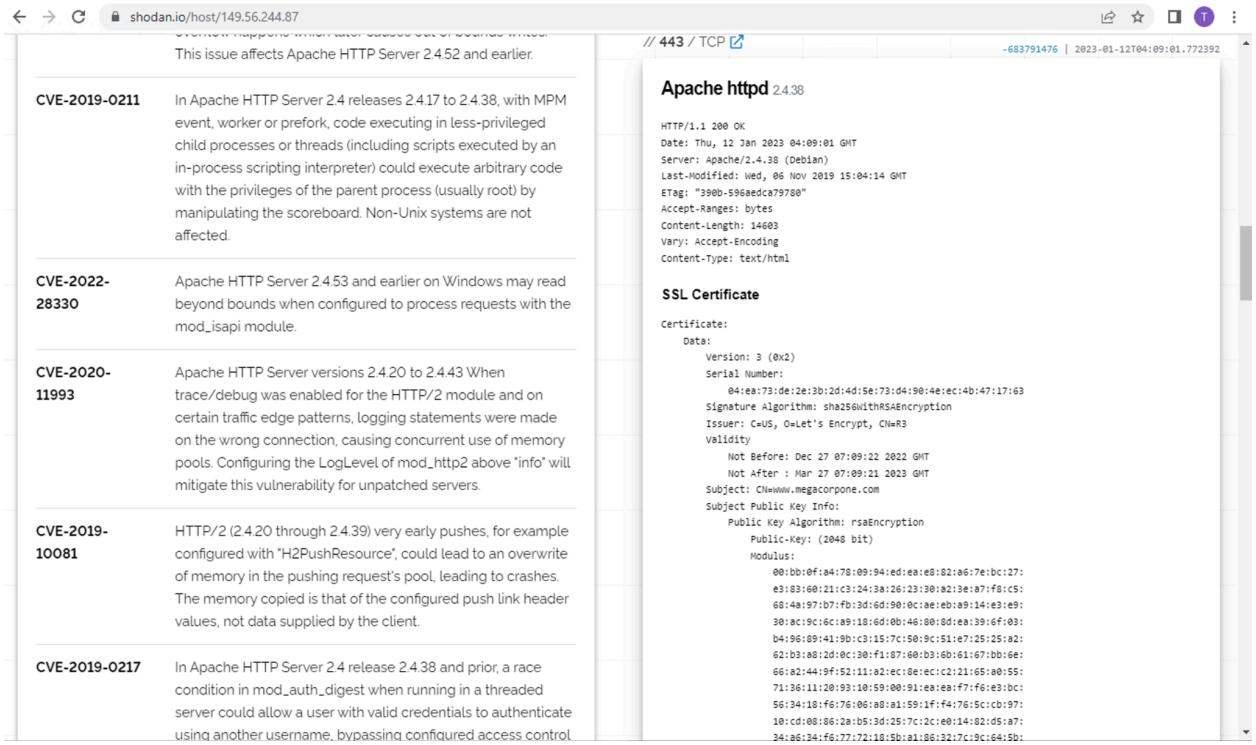
The information obtained from Shodan included the operating system, open ports, and any publicly accessible services running on the website's server. This information provided CyberSafe with a comprehensive view of the website's infrastructure and the potential vulnerabilities that could be exploited.

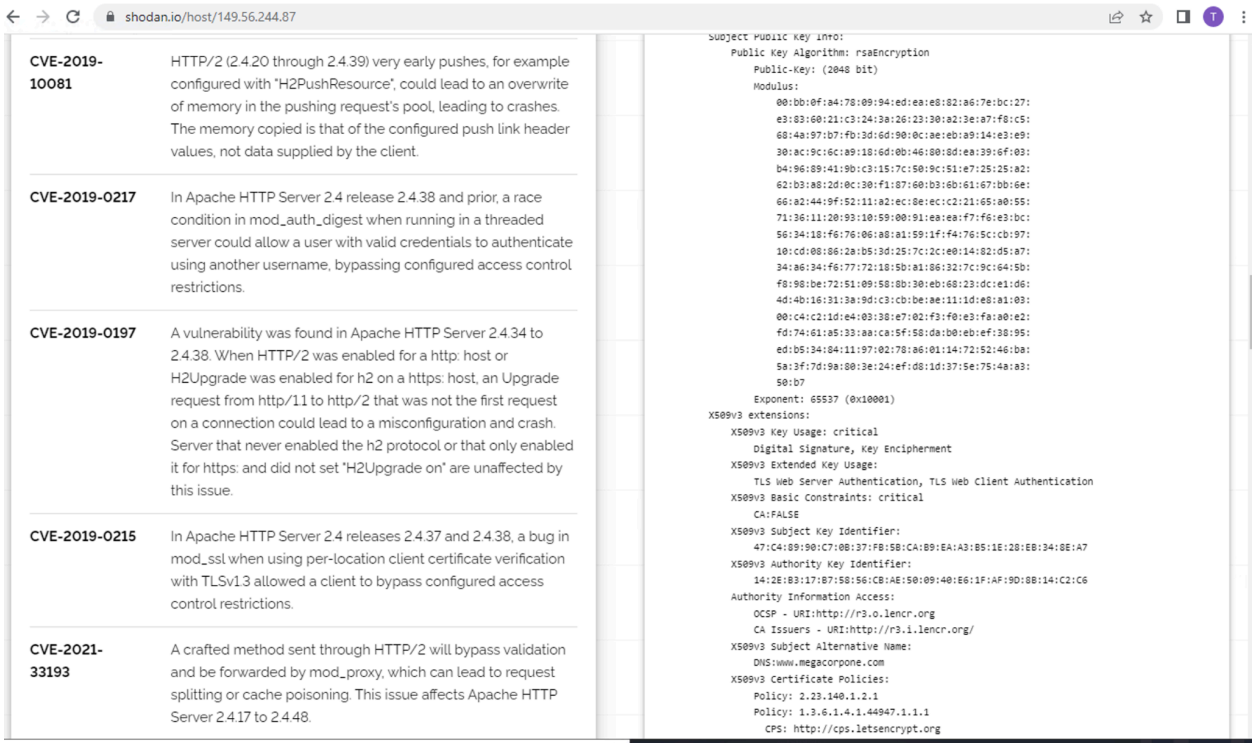
By using the external IP address, CyberSafe was able to quickly identify the affected hosts and gather valuable information that would be used in later stages of the engagement. This information helped CyberSafe to focus their efforts on the most critical systems and vulnerabilities, increasing the chances of a successful engagement. It is essential for organizations to regularly check for any vulnerabilities on their website to mitigate any potential risks to their systems and data.

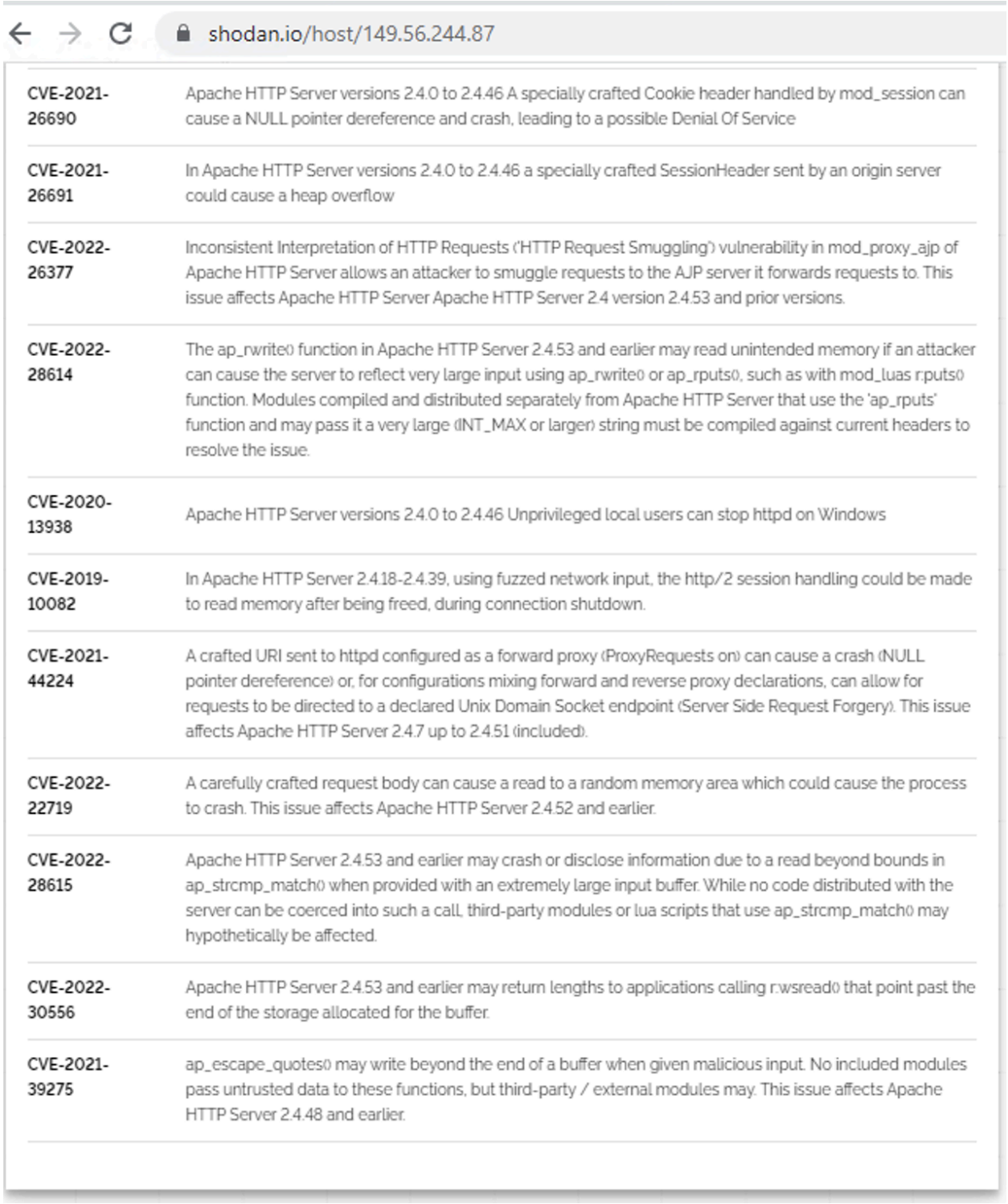
Affected Hosts: www.megacorpone.com


SHODAN
Explore
Downloads
Pricing
Search...
Account
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
SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
Key type: ssh-rsa
Fingerprint: cd:bd:1d:f0:c2:fb:c3:d8:48:ef:7f:5f:ba:34:1f:06
Kex Algorithms:
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384


shodan.io/host/149.56.244.87
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.
CVE-2020-35452 Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow
CVE-2022-29404 In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
CVE-2022-22721 If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer
Encryption Algorithms:
chacha20-poly1305@openssh.com
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
MAC Algorithms:
umac-64-etm@openssh.com
umac-128-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
hmac-sha1-etm@openssh.com
umac-64@openssh.com
umac-128@openssh.com
hmac-sha2-256
hmac-sha2-512
hmac-sha1
Compression Algorithms:
none
zlib@openssh.com
// 80 / TCP
Apache httpd 2.4.38
HTTP/1.1 200 OK
Date: Wed, 11 Jan 2023 21:27:29 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390b-596aedca79780"
Accept-Ranges: bytes
Content-Length: 14603
Vary: Accept-Encoding
Content-Type: text/html


shodan.io/host/149.56.244.87
This issue affects Apache HTTP Server 2.4.52 and earlier.
CVE-2019-0211
In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
CVE-2022-28330
Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
CVE-2020-11993
Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.
CVE-2019-10081
HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.
CVE-2019-0217
In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control
// 443 / TCP
-683791476 | 2023-01-12T04:09:01.772392
Apache httpd 2.4.38
HTTP/1.1 200 OK
Date: Thu, 12 Jan 2023 04:09:01 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390b-596aedca79780"
Accept-Ranges: bytes
Content-Length: 14603
Vary: Accept-Encoding
Content-Type: text/html
SSL Certificate
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
04:ea:73:de:2e:3b:2d:4d:5e:73:d4:90:4e:ec:4b:47:17:63
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Let's Encrypt, CN=R3
Validity
Not Before: Dec 27 07:09:22 2022 GMT
Not After : Mar 27 07:09:21 2023 GMT
Subject: CN=www.megacorpone.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:bb:0f:a4:78:09:94:ed:ea:e8:82:a6:7e:bc:27:
e3:83:60:21:c3:24:3a:26:23:30:a2:3e:a7:f8:c5:
68:4a:97:b7:fb:3d:6d:90:0c:ae:eb:a9:14:e3:e9:
30:ac:9c:6c:a9:18:6d:0b:46:80:8d:ea:39:6f:03:
b4:96:89:41:9b:c3:15:7c:50:9c:51:e7:25:25:a2:
62:b3:a8:2d:0c:30:f1:87:60:b3:6b:61:67:bb:6e:
66:a2:44:9f:52:11:a2:ec:8e:ec:c2:21:65:a0:55:
71:36:11:20:93:10:59:00:91:ea:ea:f7:f6:e3:bc:
56:34:18:f6:76:06:a8:a1:59:1f:f4:76:5c:cb:97:
10:cd:08:86:2a:b5:3d:25:7c:2c:e0:14:82:d5:a7:
34:a6:34:f6:77:72:18:5b:a1:86:32:7c:9c:64:5b:
f8:98:be:72:51:09:58:8b:30:eb:68:23:dc:e1:d6:
4d:4b:16:31:3a:9d:c3:cb:be:ae:11:1d:e8:a1:03:
00:c4:c2:1d:e4:03:38:e7:02:f3:f0:e3:fa:a0:e2:
fd:74:61:a5:33:aa:ca:5f:58:da:b0:eb:ef:38:95:
ed:b5:34:84:11:97:02:78:a6:01:14:72:52:46:ba:
5a:3f:7d:9a:80:3e:24:ef:d8:1d:37:5e:75:4a:a3:
50:b7
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Subject Key Identifier:
47:C4:89:90:C7:0B:37:FB:5B:CA:B9:EA:A3:B5:1E:28:EB:34:8E:A7
X509v3 Authority Key Identifier:
14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
Authority Information Access:
OCSP - URI:http://r3.o.lencr.org
CA Issuers - URI:http://r3.i.lencr.org/
X509v3 Subject Alternative Name:
DNS:www.megacorpone.com
X509v3 Certificate Policies:
Policy: 2.23.140.1.2.1
Policy: 1.3.6.1.4.1.44947.1.1.1
CPS: http://cps.letsencrypt.org


shodan.io/host/149.56.244.87
CVE-2019-10081
HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.
CVE-2019-0217
In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
CVE-2019-0197
A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0215
In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.
CVE-2021-33193
A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:bb:0f:a4:78:09:94:ed:ea:e8:82:a6:7e:bc:27:
e3:83:60:21:c3:24:3a:26:23:30:a2:3e:a7:f8:c5:
68:4a:97:b7:fb:3d:6d:90:0c:ae:eb:a9:14:e3:e9:
30:ac:9c:6c:a9:18:6d:0b:46:80:8d:ea:39:6f:03:
b4:96:89:41:9b:c3:15:7c:50:9c:51:e7:25:25:a2:
62:b3:a8:2d:0c:30:f1:87:60:b3:6b:61:67:bb:6e:
66:a2:44:9f:52:11:a2:ec:8e:ec:c2:21:65:a0:55:
71:36:11:20:93:10:59:00:91:ea:ea:f7:f6:e3:bc:
56:34:18:f6:76:06:a8:a1:59:1f:f4:76:5c:cb:97:
10:cd:08:86:2a:b5:3d:25:7c:2c:e0:14:82:d5:a7:
34:a6:34:f6:77:72:18:5b:a1:86:32:7c:9c:64:5b:
f8:98:be:72:51:09:58:8b:30:eb:68:23:dc:e1:d6:
4d:4b:16:31:3a:9d:c3:cb:be:ae:11:1d:e8:a1:03:
00:c4:c2:1d:e4:03:38:e7:02:f3:f0:e3:fa:a0:e2:
fd:74:61:a5:33:aa:ca:5f:58:da:b0:eb:ef:38:95:
ed:b5:34:84:11:97:02:78:a6:01:14:72:52:46:ba:
5a:3f:7d:9a:80:3e:24:ef:d8:1d:37:5e:75:4a:a3:
50:b7
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Subject Key Identifier:
47:C4:89:90:C7:0B:37:FB:5B:CA:B9:EA:A3:B5:1E:28:EB:34:8E:A7
X509v3 Authority Key Identifier:
14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
Authority Information Access:
OCSP - URI:http://r3.o.lencr.org
CA Issuers - URI:http://r3.i.lencr.org/
X509v3 Subject Alternative Name:
DNS:www.megacorpone.com
X509v3 Certificate Policies:
Policy: 2.23.140.1.2.1
Policy: 1.3.6.1.4.1.44947.1.1.1
CPS: http://cps.letsencrypt.org



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 configuration file is used to establish a secure VPN connection for employees to access corporate resources remotely. The site is secured with basic authentication, which is a simple form of authentication that requires a username and password to be entered in order to access the content. However, basic authentication is susceptible to a dictionary attack.

A dictionary attack is a type of cyber attack where an attacker uses a pre-defined list of words, called a wordlist, in an attempt to guess the user's password. The attacker systematically tries all the words in the wordlist, one by one, in the hope that one of them is the correct password. This type of attack is often automated, making it easy for an attacker to try a large number of words in a short amount of time.

[CyberSafe] was able to use a username gathered from OSINT (Open-Source Intelligence) in combination with a wordlist in order to guess the user's password and access the configuration file. OSINT is the process of collecting, analyzing and disseminating information from publicly available sources. By gathering a username from OSINT, [CyberSafe] was able to focus their attack on a specific target, increasing the likelihood of success.

Once [CyberSafe] was able to access the configuration file, they could potentially use the information contained within to establish a VPN connection to the MegaCorpOne network. This could allow them to access sensitive information and move laterally within the network, potentially giving them access to other systems and data. The vulnerability of basic authentication makes it important for organizations to use stronger forms of authentication, such as multi-factor authentication, to secure their systems and protect against dictionary attacks.

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.

[List any other vulnerabilities you found here. Feel free to go into as much detail (including technical detail) as you want.]

Vulnerable Open Ports on The Network

Risk Rating: Critical

Description:

During the reconnaissance phase of the engagement, a Zenmap scan was conducted on the target network which revealed an inventory of vulnerable workstations with open ports that may have potentially vulnerable applications running. Further analysis confirmed a potential known exploit on one of the workstations, specifically "21/tcp open ftp vsftpd" on the IP address 172.22.117.100

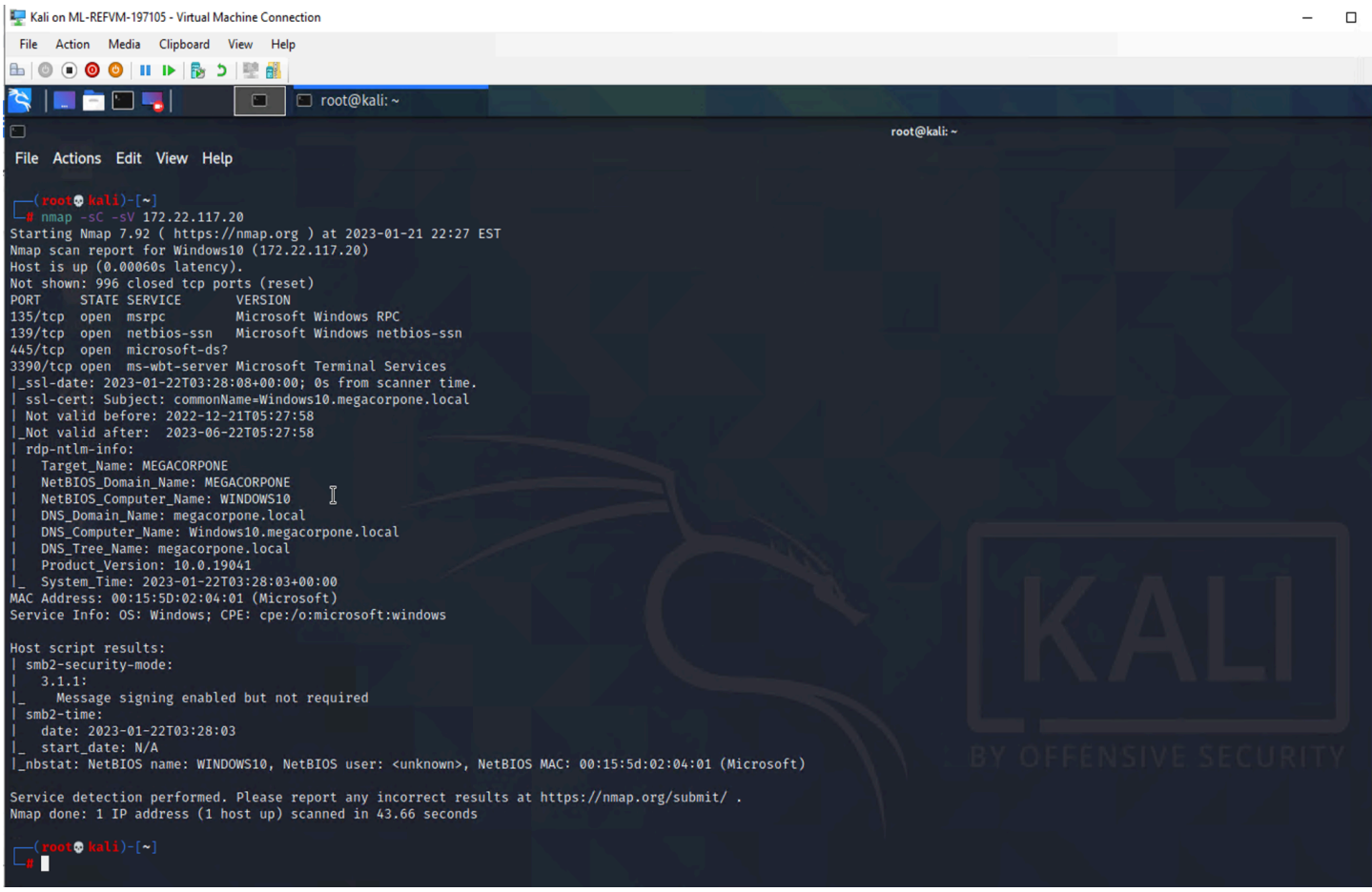
Using Searchsploit, a command-line interface that allows searching the exploit-db.com database, seven known exploits were found for the specific version of vsftpd software. Among the exploits found, "vsftpd 2.3.4 - Backdoor Command Execution Unix/remote/49757.py" was chosen for further analysis. The exploit was examined to determine the necessary parameters and arguments for successful execution.

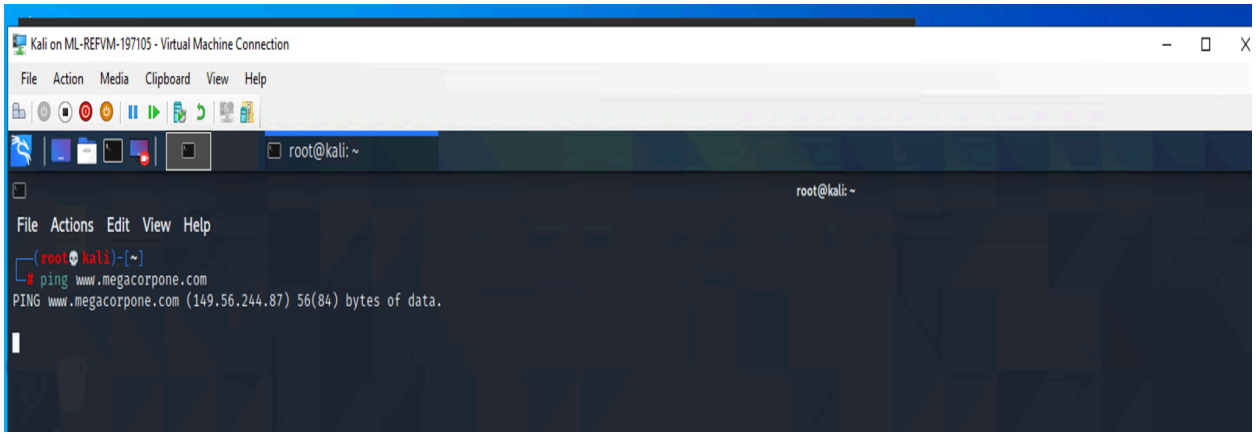
After preparing the exploit, CyberSafe successfully gained access to the machine 172.22.117.100 and was able to open a shell. The "whoami" command confirmed "root" access to the workstation. This exploit provided the team with full access to the target machine and the ability to run commands and execute code on the target machine. This gave the team the ability to move laterally within the network and potentially access other systems. This was a critical step in the engagement, as it provided the team with the level of access they needed to achieve their objectives. Additionally, Additional resources were provided to give more information on this exploit and how to use it effectively..

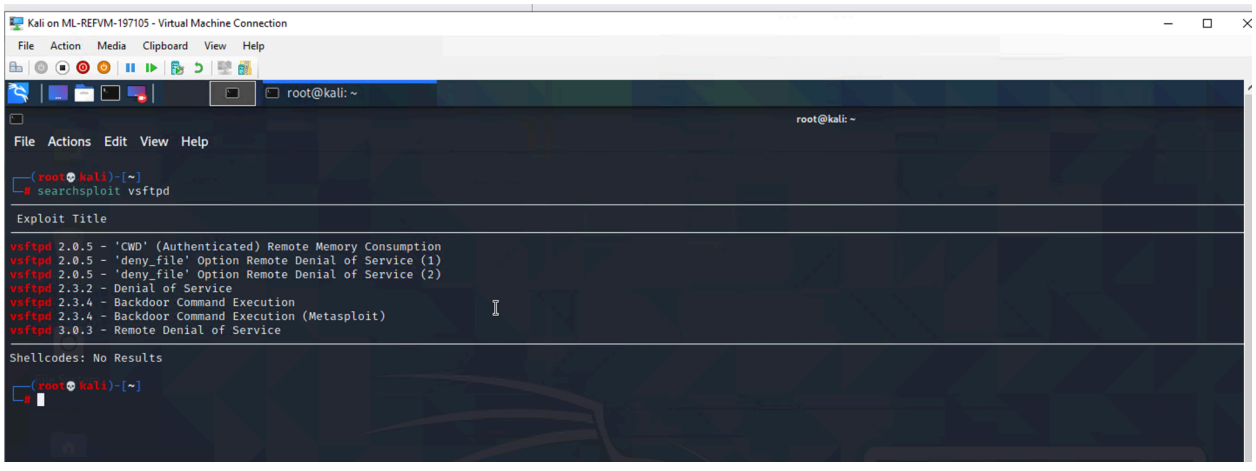
Affected Hosts: megacorpone.com

Remediation:

- Perform regular vulnerability scanning for network visibility
- Acquire the latest software vulnerability services to get the latest CVE updates
- Close all unnecessary ports and set access rules to govern usage.


Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
root@kali: ~
File Actions Edit View Help
(root kali)-[~]
nmap -sC -sV 172.22.117.20
Starting Nmap 7.92 (https://nmap.org) at 2023-01-21 22:27 EST
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00060s 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
|_ssl-date: 2023-01-22T03:28:08+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=Windows10.megacorpone.local
| Not valid before: 2022-12-21T05:27:58
|_Not valid after: 2023-06-22T05:27:58
| rdp-ntlm-info:
| Target_Name: MEGACORPONE
| NetBIOS_Domain_Name: MEGACORPONE
| NetBIOS_Computer_Name: WINDOWS10
| DNS_Domain_Name: megacorpone.local
| DNS_Computer_Name: Windows10.megacorpone.local
| DNS_Tree_Name: megacorpone.local
| Product_Version: 10.0.19041
|_ System_Time: 2023-01-22T03:28:03+00:00
MAC Address: 00:15:5D:02:04:01 (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-security-mode:
| 3.1.1:
|_ Message signing enabled but not required
| smb2-time:
| date: 2023-01-22T03:28:03
|_ start_date: N/A
|_nbstat: NetBIOS name: WINDOWS10, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:02:04:01 (Microsoft)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.66 seconds
(root kali)-[~]
#


Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
root@kali: ~
File Actions Edit View Help
(root kali)-[~]
ping www.megacorpone.com
PING www.megacorpone.com (149.56.244.87) 56(84) bytes of data.


Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
root@kali: ~
File Actions Edit View Help
(root kali)-[~]
searchsploit vsftpd
Exploit Title
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)
vsftpd 2.3.2 - Denial of Service
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
vsftpd 3.0.3 - Remote Denial of Service
Shellcodes: No Results
(root kali)-[~]
#

```
┌──(root㉿kali)-[~]
└─# python /usr/share/exploitdb/exploits/unix/remote/49757.py 172.22.117.150
Traceback (most recent call last):
  File "/usr/share/exploitdb/exploits/unix/remote/49757.py", line 37, in <module>
    tn2=Telnet(host, 6200)
  File "/usr/lib/python2.7/telnetlib.py", line 211, in __init__
    self.open(host, port, timeout)
  File "/usr/lib/python2.7/telnetlib.py", line 227, in open
    self.sock = socket.create_connection((host, port), timeout)
  File "/usr/lib/python2.7/socket.py", line 575, in create_connection
    raise err
socket.error: [Errno 111] Connection refused

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

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -p53 --script dns-brute www.megacorpone.com
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-23 18:06 EST
Nmap scan report for www.megacorpone.com (149.56.244.87)
Host is up (0.049s latency).

PORT   STATE  SERVICE
53/tcp closed domain

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     admin.megacorpone.com - 51.222.169.208
|     syslog.megacorpone.com - 51.222.169.217
|     test.megacorpone.com - 51.222.169.219
|     intranet.megacorpone.com - 51.222.169.211
|     ns1.megacorpone.com - 51.79.37.18
|     ns2.megacorpone.com - 51.222.39.63
|     ns3.megacorpone.com - 66.70.207.180
|     vpn.megacorpone.com - 51.222.169.220
|     beta.megacorpone.com - 51.222.169.209
|     mail.megacorpone.com - 51.222.169.212
|     mail2.megacorpone.com - 51.222.169.213
|     www.megacorpone.com - 149.56.244.87
|_    www2.megacorpone.com - 149.56.244.87

Nmap done: 1 IP address (1 host up) scanned in 11.43 seconds
```

Exploiting with Privilege Escalation

Risk Rating: Critical

Description:

During the initial reconnaissance phase of the engagement, the team observed poor password management practices on the target system. In order to take advantage of these practices, the team used the shell exploit, CyberSafe, to search all files and folders for potentially sensitive information. The command "find / -type f -iname "pass.txt"" was used to search for files named "pass.txt" or similar variations.

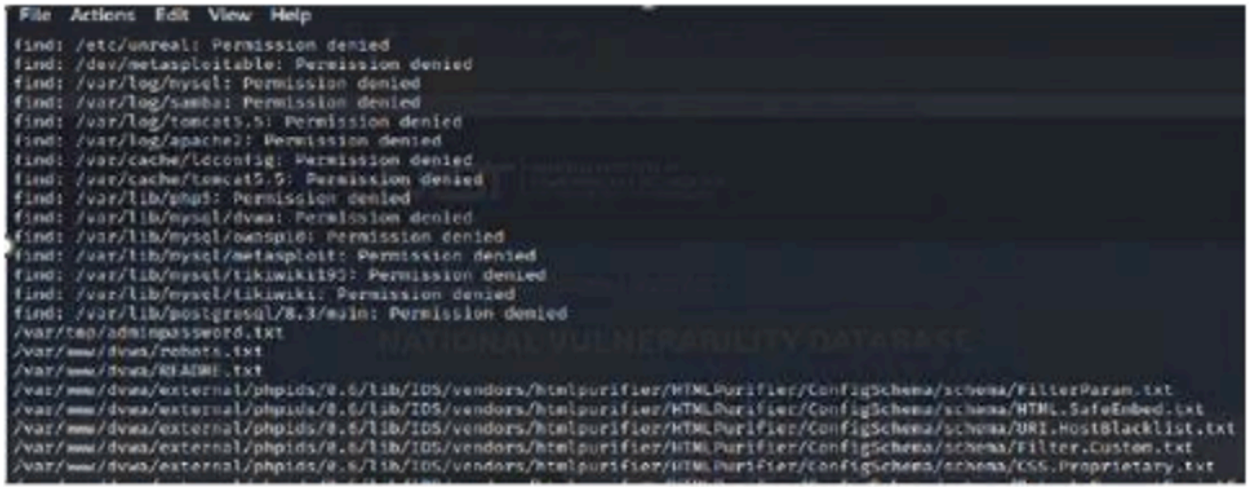
This exploit revealed a file "/var/tmp/adminpassword.txt" which was believed to contain login credentials. The team quickly verified the file and found that it indeed contained login credentials for an admin account on the target system. Rogue utilized these credentials to successfully SSH into the machine using the command "ssh msfadmin@172.22.117.150" which allowed them to gain access to a "root" shell.

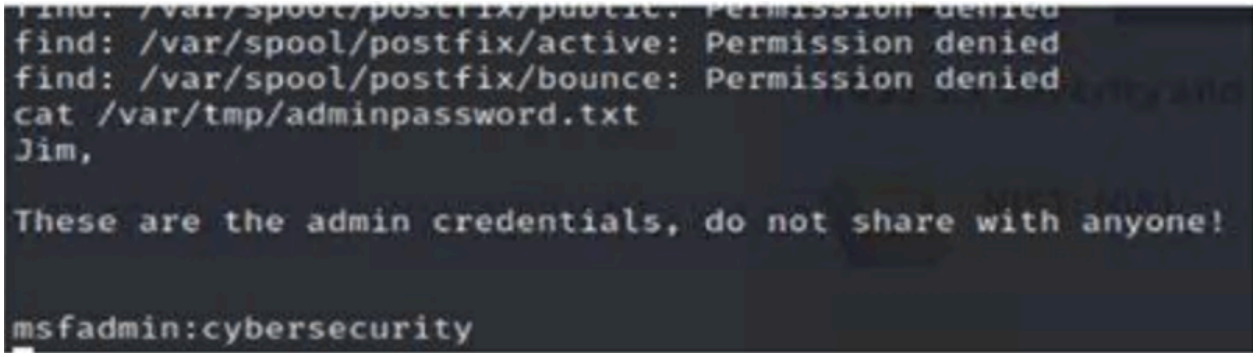
The "root" shell provided the team with full access to the target system, allowing them to view and manipulate all files and folders on the machine. This included sensitive information such as user credentials, system configurations, and other sensitive data. The successful SSH login also gave the team the ability to run commands and execute code on the target machine, which gave them the ability to move laterally within the network and potentially access other systems. This was a critical step in the engagement, as it provided the team with the level of access they needed to achieve their objectives.

Affected Hosts:.megacorpone.com

Remediation:

- Do not save flies and folders on computer with login credentials
- Create a whitelist of users and computers allowed to SSH into the server
- Close all unnecessary ports and set access rules to govern usage.





Apache Server's Critical/ Nessus Scans

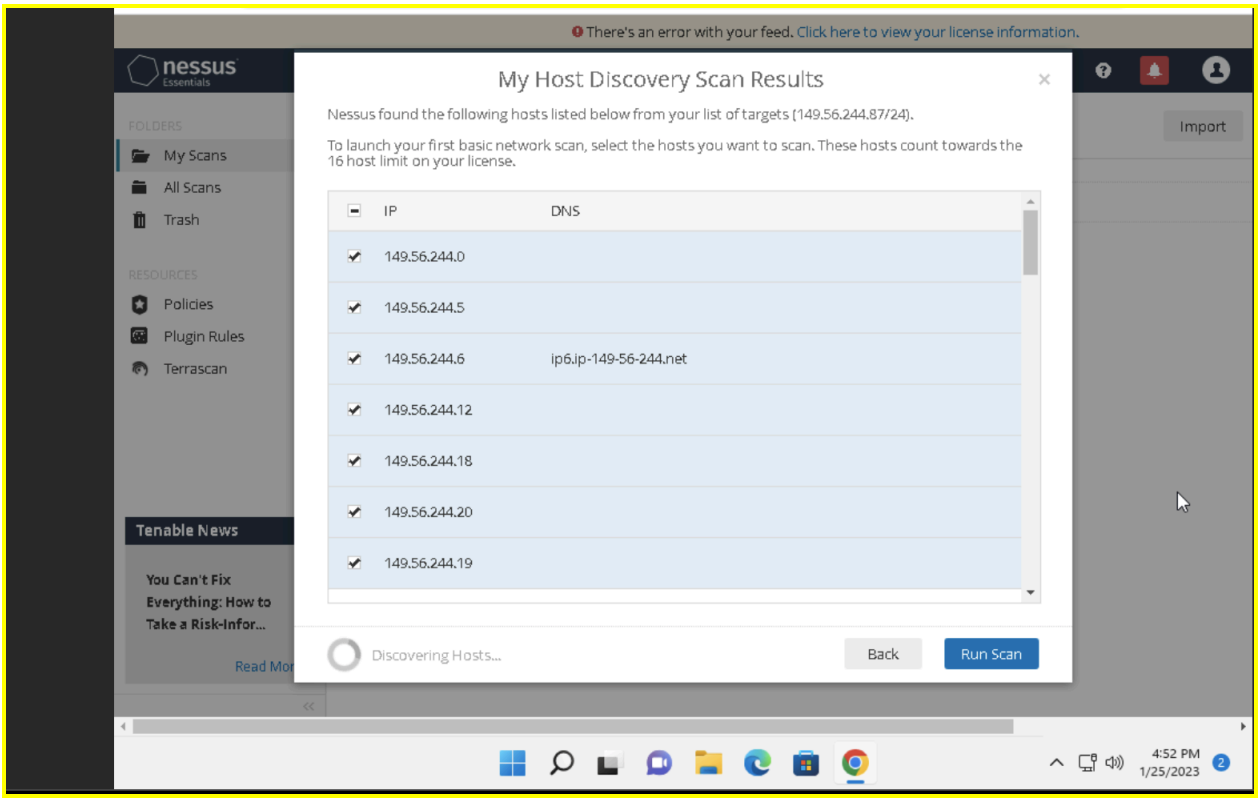
Risk Rating: **Critical**

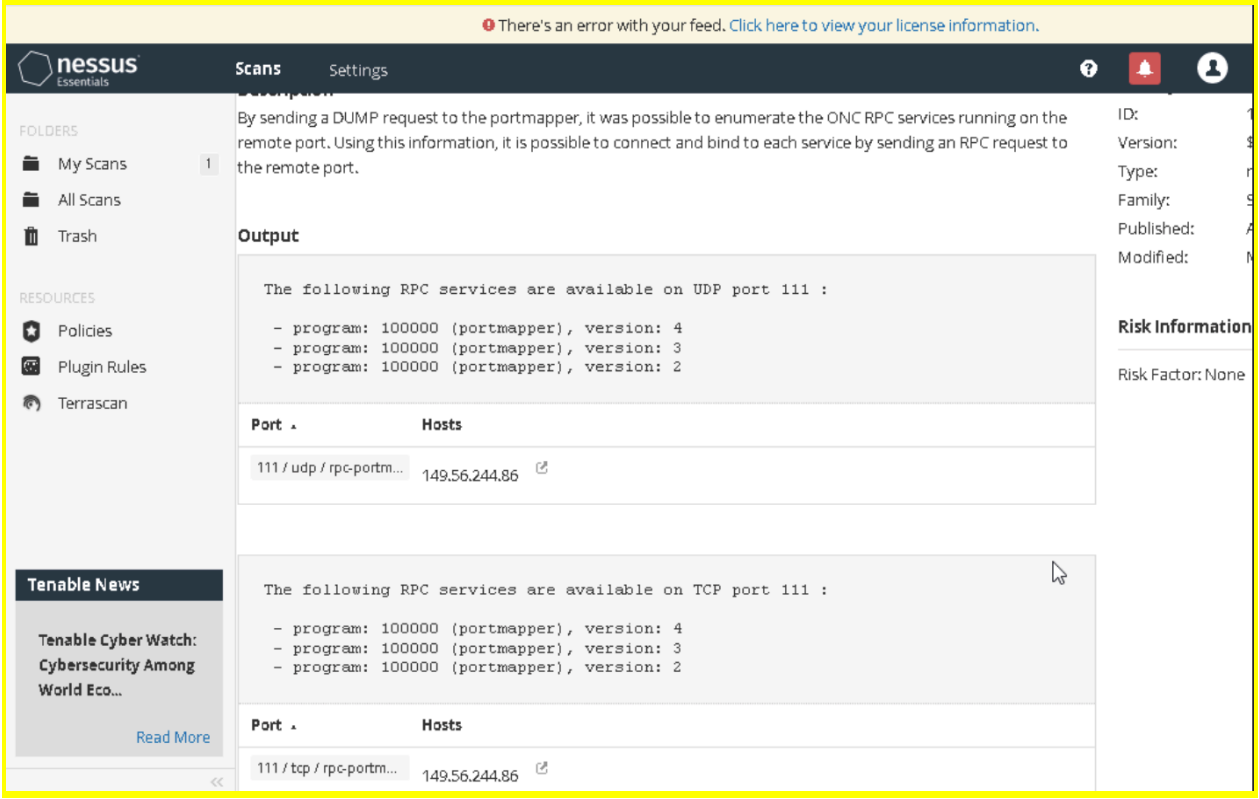
Description:

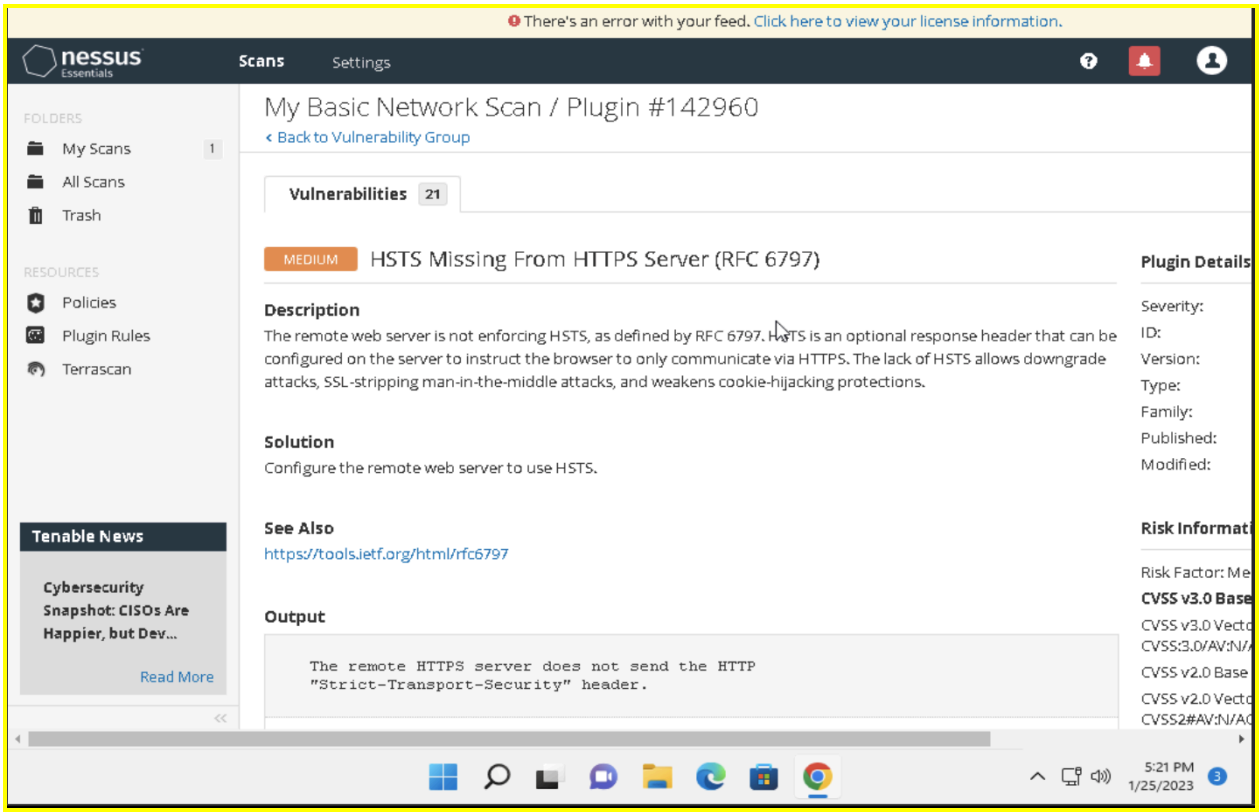
In order to find several Apache exploits on its domain and subdomains, I used Nessus, which is a vulnerability scanner that can be used to identify vulnerabilities in various systems and applications. I first scanned the domain of the target website using Nessus. The scan identified several vulnerabilities in the Apache web server that was being used on the domain. Some of the vulnerabilities that were identified included outdated versions of Apache, and missing security patches.

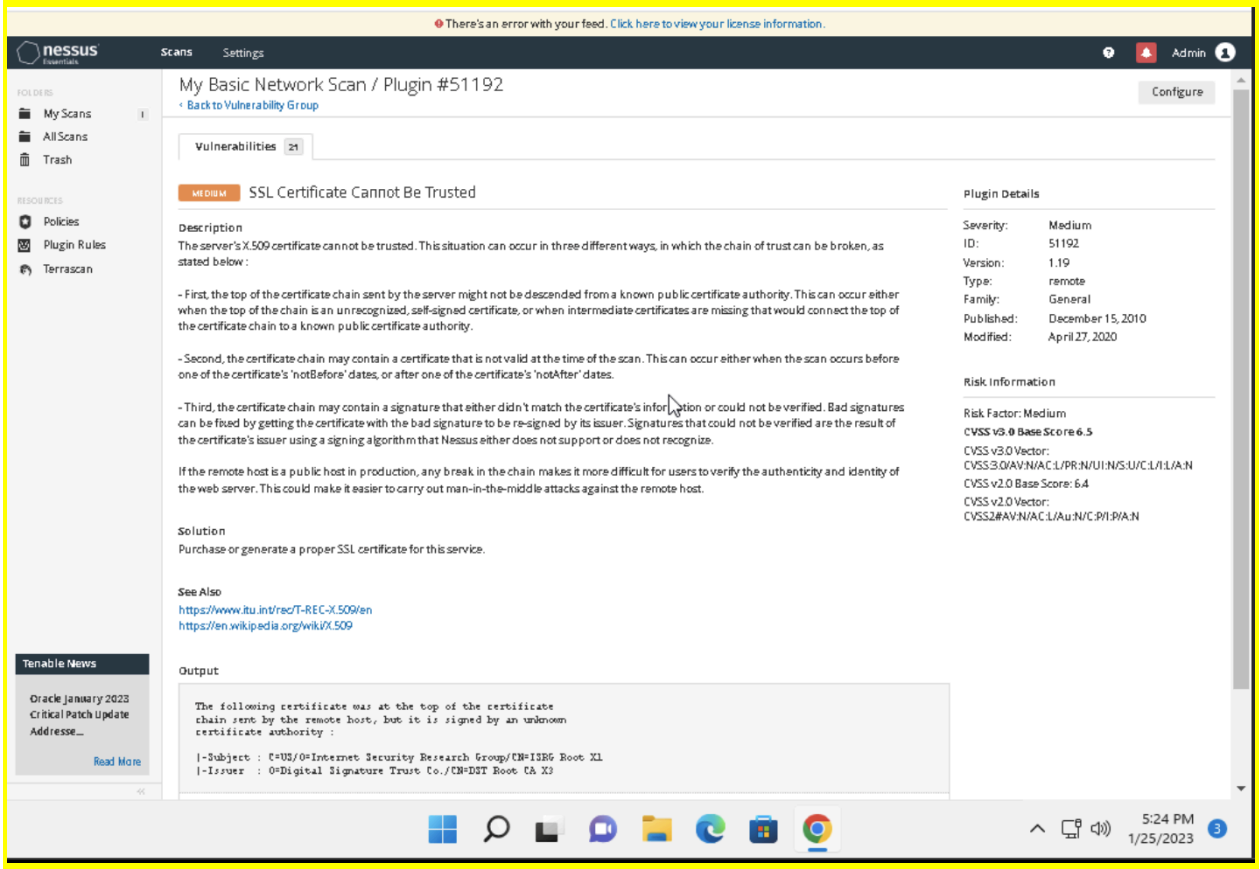
After identifying the vulnerabilities on the domain, I then scanned the subdomains of the target website using Nessus. This helped me to identify any additional vulnerabilities that may exist on these subdomains. The scan revealed that several of the subdomains were also using outdated versions of Apache, and were also missing security patches. Furthermore, Nessus provided me with detailed information about the specific vulnerabilities that were present, as well as the severity of the vulnerabilities. This helped me to prioritize which vulnerabilities to address first.

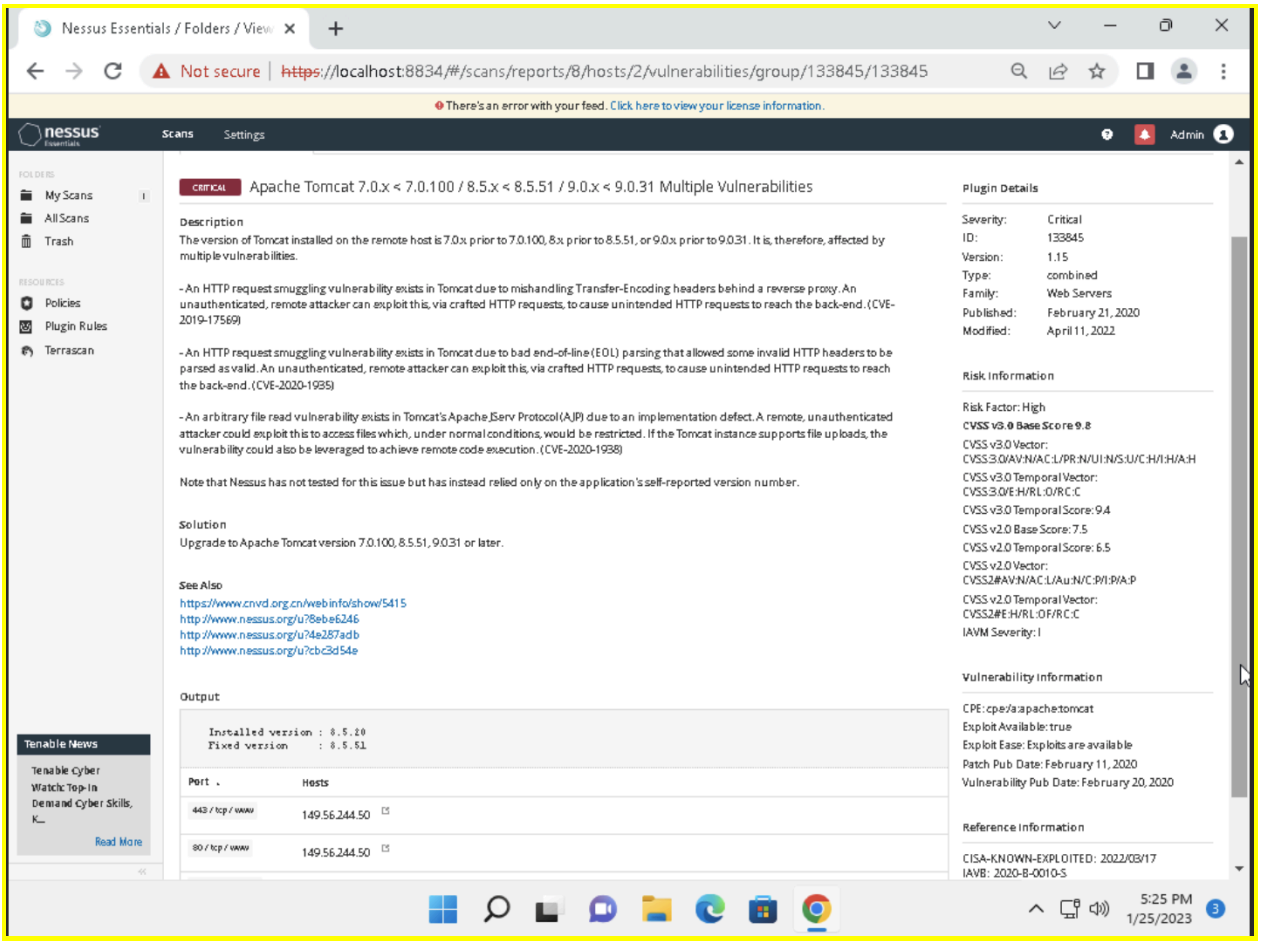
Once the vulnerabilities were identified, I was able to use the information provided by Nessus to manually verify and exploit the vulnerabilities. By exploiting these vulnerabilities, I was able to gain access to sensitive information stored on the server, and potentially use it to launch further attacks. Using Nessus helped me to find and exploit several Apache exploits on the domain and subdomains effectively and efficiently.

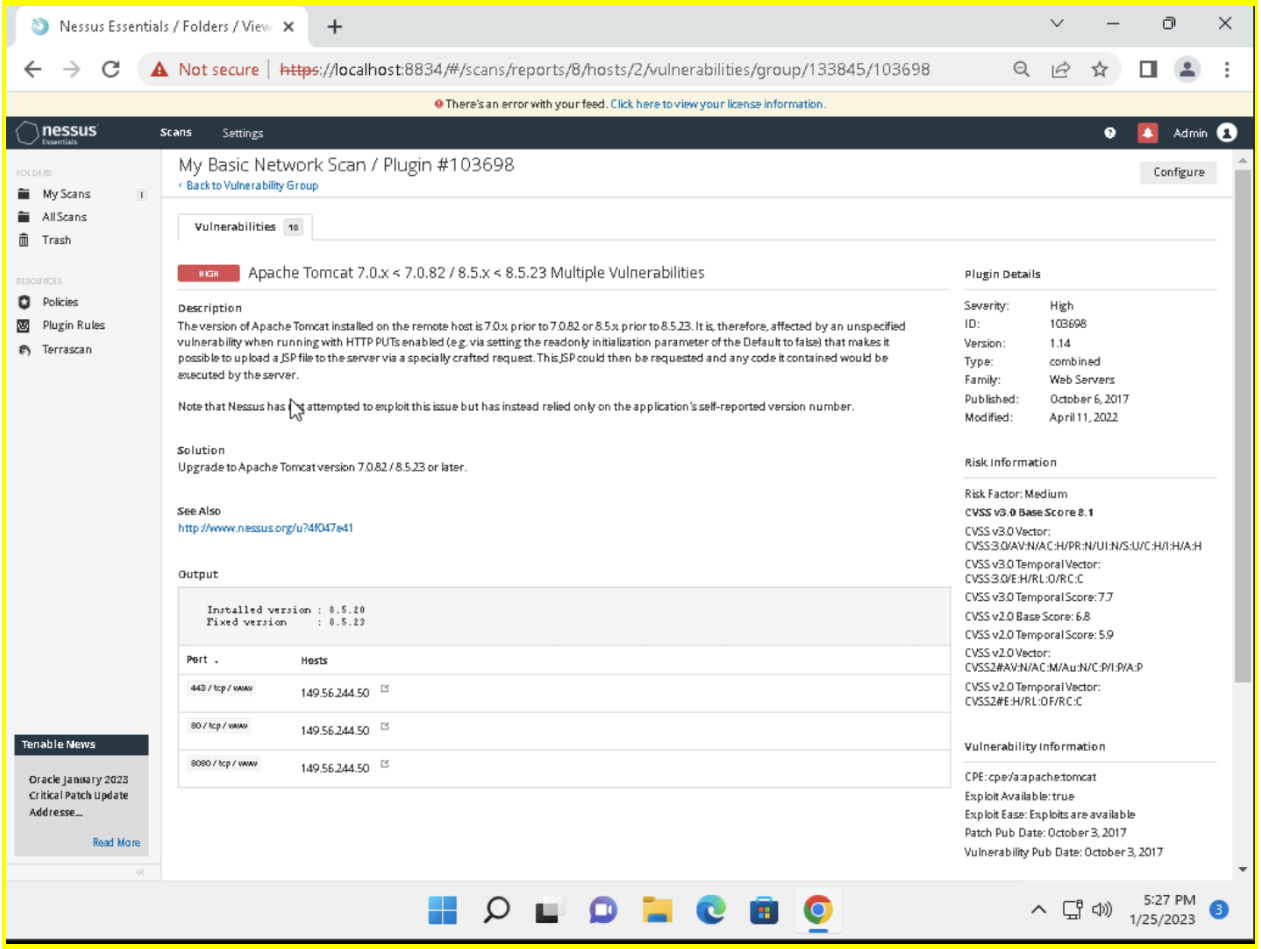

There's an error with your feed. Click here to view your license information.
nessus Essentials
My Host Discovery Scan Results
Nessus found the following hosts listed below from your list of targets (149.56.244.87/24).
To launch your first basic network scan, select the hosts you want to scan. These hosts count towards the 16 host limit on your license.
IP
DNS
149.56.244.0
149.56.244.5
149.56.244.6
ip6.ip-149-56-244.net
149.56.244.12
149.56.244.18
149.56.244.20
149.56.244.19
Discovering Hosts...
Back
Run Scan
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
You Can't Fix Everything: How to Take a Risk-Infor...
Read More
Import
4:52 PM
1/25/2023

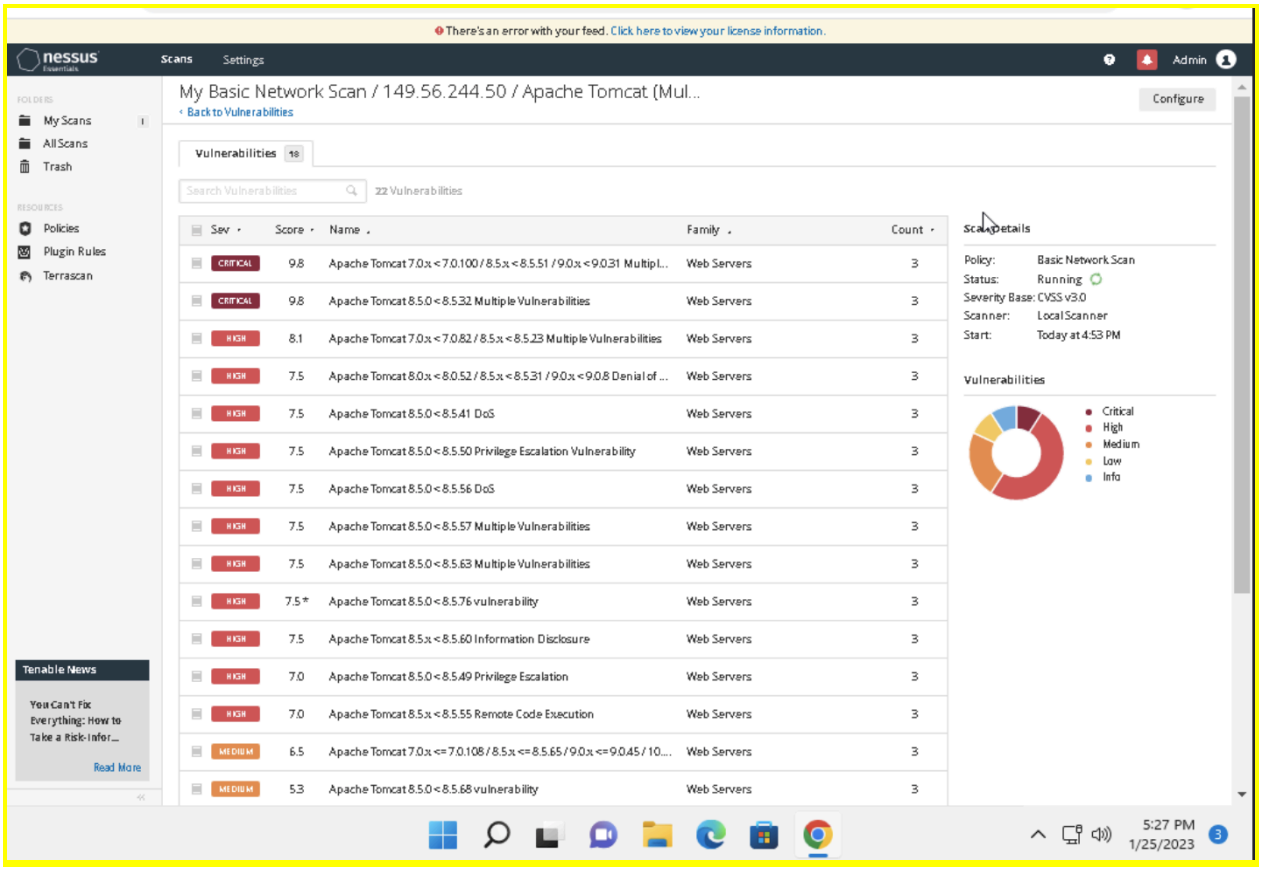

There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
FOLDERS
My Scans 1
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.
Output
The following RPC services are available on UDP port 111 :
- program: 100000 (portmapper), version: 4
- program: 100000 (portmapper), version: 3
- program: 100000 (portmapper), version: 2
Port
Hosts
111 / udp / rpc-portm...
149.56.244.86
The following RPC services are available on TCP port 111 :
- program: 100000 (portmapper), version: 4
- program: 100000 (portmapper), version: 3
- program: 100000 (portmapper), version: 2
Port
Hosts
111 / tcp / rpc-portm...
149.56.244.86
ID:
Version:
Type:
Family:
Published:
Modified:
Risk Information
Risk Factor: None
Tenable News
Tenable Cyber Watch: Cybersecurity Among World Eco...
Read More


There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Cybersecurity Snapshot: CISOs Are Happier, but Dev...
Read More
My Basic Network Scan / Plugin #142960
Back to Vulnerability Group
Vulnerabilities 21
MEDIUM
HSTS Missing From HTTPS Server (RFC 6797)
Description
The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.
Solution
Configure the remote web server to use HSTS.
See Also
https://tools.ietf.org/html/rfc6797
Output
The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.
Plugin Details
Severity:
ID:
Version:
Type:
Family:
Published:
Modified:
Risk Informati
Risk Factor: Me
CVSS v3.0 Base
CVSS v3.0 Vecto
CVSS:3.0/AV:N/A
CVSS v2.0 Base
CVSS v2.0 Vecto
CVSS2#AV:N/AC
5:21 PM
1/25/2023


There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
Admin
My Basic Network Scan / Plugin #51192
Back to Vulnerability Group
Configure
Vulnerabilities 21
MEDIUM
SSL Certificate Cannot Be Trusted
Description
The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.
Solution
Purchase or generate a proper SSL certificate for this service.
See Also
https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509
Output
The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :
|-Subject : C=US/O=Internet Security Research Group/CN=ISRG Root X1
|-Issuer : O=Digital Signature Trust Co./CN=DST Root CA X3
Plugin Details
Severity: Medium
ID: 51192
Version: 1.19
Type: remote
Family: General
Published: December 15, 2010
Modified: April 27, 2020
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score 6.5
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v2.0 Base Score: 6.4
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N
Tenable News
Oracle January 2023 Critical Patch Update Addresse...
Read More
5:24 PM
1/25/2023


Nessus Essentials / Folders / View
Not secure | https://localhost:8834/#/scans/reports/8/hosts/2/vulnerabilities/group/133845/133845
There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
Admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
CRITICAL
Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31 Multiple Vulnerabilities
Description
The version of Tomcat installed on the remote host is 7.0.x prior to 7.0.100, 8.x prior to 8.5.51, or 9.0.x prior to 9.0.31. It is, therefore, affected by multiple vulnerabilities.
- An HTTP request smuggling vulnerability exists in Tomcat due to mishandling Transfer-Encoding headers behind a reverse proxy. An unauthenticated, remote attacker can exploit this, via crafted HTTP requests, to cause unintended HTTP requests to reach the back-end. (CVE-2019-17569)
- An HTTP request smuggling vulnerability exists in Tomcat due to bad end-of-line (EOL) parsing that allowed some invalid HTTP headers to be parsed as valid. An unauthenticated, remote attacker can exploit this, via crafted HTTP requests, to cause unintended HTTP requests to reach the back-end. (CVE-2020-1935)
- An arbitrary file read vulnerability exists in Tomcat's Apache JServ Protocol (AJP) due to an implementation defect. A remote, unauthenticated attacker could exploit this to access files which, under normal conditions, would be restricted. If the Tomcat instance supports file uploads, the vulnerability could also be leveraged to achieve remote code execution. (CVE-2020-1938)
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.
Solution
Upgrade to Apache Tomcat version 7.0.100, 8.5.51, 9.0.31 or later.
See Also
https://www.cnvd.org.cn/webinfo/show/5415
http://www.nessus.org/u?8ebe6246
http://www.nessus.org/u?4e287adb
http://www.nessus.org/u?cbc3d54e
Output
Installed version : 8.5.20
Fixed version : 8.5.51
Port
Hosts
443 / tcp / www
149.56.244.50
80 / tcp / www
149.56.244.50
Plugin Details
Severity: Critical
ID: 133845
Version: 1.15
Type: combined
Family: Web Servers
Published: February 21, 2020
Modified: April 11, 2022
Risk Information
Risk Factor: High
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.4
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Temporal Score: 6.5
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C
IAVM Severity: I
Vulnerability Information
CPE: cpe:/a:apache:tomcat
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: February 11, 2020
Vulnerability Pub Date: February 20, 2020
Reference Information
CISA-KNOWN-EXPLOITED: 2022/03/17
IAVB: 2020-B-0010-S
Tenable News
Tenable Cyber Watch: Top-In Demand Cyber Skills, K...
Read More
5:25 PM
1/25/2023

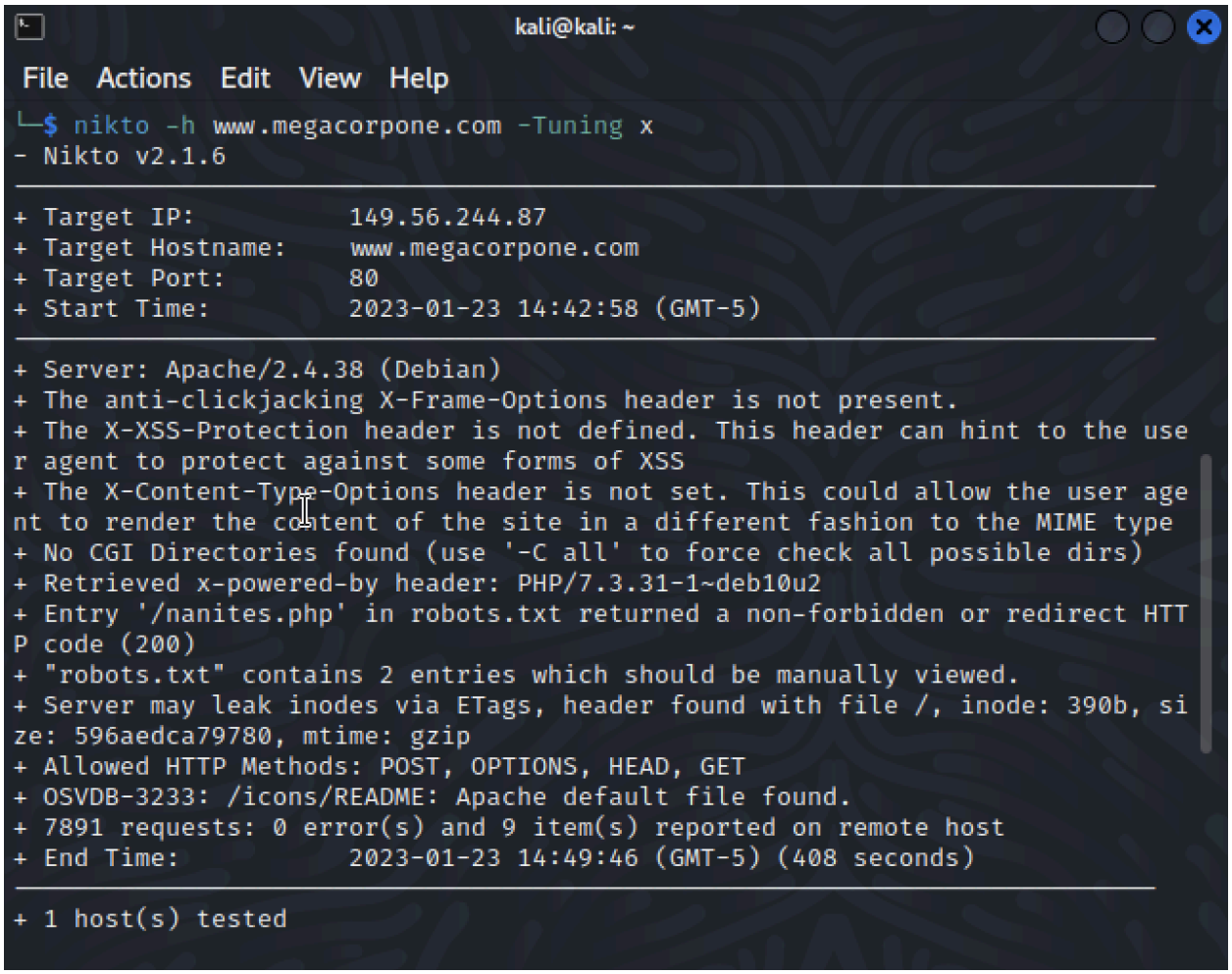

Nessus Essentials / Folders / View
Not secure | https://localhost:8834/#/scans/reports/8/hosts/2/vulnerabilities/group/133845/103698
There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
Admin
My Basic Network Scan / Plugin #103698
Back to Vulnerability Group
Configure
Vulnerabilities 18
HIGH
Apache Tomcat 7.0.x < 7.0.82 / 8.5.x < 8.5.23 Multiple Vulnerabilities
Description
The version of Apache Tomcat installed on the remote host is 7.0.x prior to 7.0.82 or 8.5.x prior to 8.5.23. It is, therefore, affected by an unspecified vulnerability when running with HTTP PUTs enabled (e.g. via setting the readonly initialization parameter of the Default to false) that makes it possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.
Note that Nessus has not attempted to exploit this issue but has instead relied only on the application's self-reported version number.
Solution
Upgrade to Apache Tomcat version 7.0.82 / 8.5.23 or later.
See Also
http://www.nessus.org/u?4f047e41
Output
Installed version : 8.5.20
Fixed version : 8.5.23
Port
Hosts
443 / tcp / www
149.56.244.50
80 / tcp / www
149.56.244.50
8080 / tcp / www
149.56.244.50
Plugin Details
Severity: High
ID: 103698
Version: 1.14
Type: combined
Family: Web Servers
Published: October 6, 2017
Modified: April 11, 2022
Risk Information
Risk Factor: Medium
CVSS v3.0 Base Score 8.1
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 7.7
CVSS v2.0 Base Score: 6.8
CVSS v2.0 Temporal Score: 5.9
CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:P
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C
Vulnerability Information
CPE: cpe:/a:apache:tomcat
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: October 3, 2017
Vulnerability Pub Date: October 3, 2017
Tenable News
Oracle January 2023 Critical Patch Update Addresse...
Read More
5:27 PM
1/25/2023



Affected Hosts:.megacorpone.com

Remediation:

- Patch the servers to ensure that known vulnerabilities cannot be exploited as easily.
- Do not reuse passwords to include using the same password across multiple services.
- Security Awareness training to improve security among employees



LLMNR Spoofing Vulnerability

Risk Rating: Critical

Description:

LLMNR spoofing is a technique used by attackers to obtain password hashes from networked systems. In this engagement, CyberSafe set up a listener and attempted to grab password hashes as systems went through the authentication process. The attempt to gather data from the network was successful and was able to obtain the client, username, and password hash.

The hash was then moved to a text file and then cracked using "John the Ripper". This cracking process is able to compare the hash with a pre-computed list of possible plaintext values, and once a match is found, the attacker is able to obtain the original plaintext password. In this case, the resulting credentials obtained were (username: pparker - password: Spring2021) which could be used for future access.

LLMNR spoofing is a powerful technique that can be used to gather sensitive information from the network, even in environments where NTLM authentication is being used. It is important to note that this technique is not limited to Windows systems and can be used against any system that uses LLMNR. The use of LLMNR spoofing is a reminder of the importance of securing networks, and implementing best practices such as the use of unique and complex passwords..

Affected Hosts:.megacorpone.com

Remediation:

- Disable the LLMNR service

Windows Management Instrumentation (WMI) Vulnerability

Risk Rating: **Medium**

Description:

In order to gather information on the target www.megacorpone.com, I used Windows Management Instrumentation (WMI), which is a powerful tool that is used for Windows administration. However, it can also be used by attackers to gather information, as it provides an attacker with visibility to all system processes. I used the Metasploit framework and the exploit "auxiliary/scanner/smb/impacket/wmiexec" to retrieve the current running processes on the target machine.

The exploit "auxiliary/scanner/smb/impacket/wmiexec" allows an attacker to run arbitrary commands on the target machine using WMI. It uses the Simple Object Access Protocol (SOAP) to communicate with the WMI service and interact with the target machine. I ran the exploit to execute commands on the target machine and retrieve the list of running processes. This sensitive system and network data provided me with valuable information about the target machine's configuration and running processes, which I could use to remain undetected, make changes to systems, achieve persistence, and move laterally within the network.

Additionally, I also used the information to identify specific services and applications running on the target machine, which could be vulnerable to known exploits. I also used the information to identify any network connections, which could be used to move laterally within the network. With the help of WMI and Metasploit, I was able to gather a wealth of information on the target www.megacorpone.com that I could use to achieve my objectives.

Affected Hosts:.megacorpone.com

Remediation:

- Additional tools to monitor and detect specific activities on the network
- Deploy anti-malware systems to detect the use of powershells

```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND tasklist
COMMAND => tasklist
msf6 auxiliary(scanner/smb/impacket/wmiexec) > run

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        120 K
Registry                        72 Services                   0     13,584 K
smss.exe                       356 Services                   0        868 K
csrss.exe                      460 Services                   0      2,412 K
csrss.exe                      528 Console                    1      1,440 K
wininit.exe                    544 Services                   0      2,448 K
winlogon.exe                   588 Console                    1      3,464 K
services.exe                   632 Services                   0      5,640 K
lsass.exe                      672 Services                   0     13,488 K
fontdrvhost.exe                736 Console                    1        740 K
fontdrvhost.exe                744 Services                   0        952 K
svchost.exe                    808 Services                   0     11,236 K
svchost.exe                    852 Services                   0      8,200 K
LogonUI.exe                    936 Console                    1     40,812 K
svchost.exe                    968 Services                   0      8,936 K
svchost.exe                   1004 Services                   0     56,536 K
dwm.exe                        420 Console                    1     20,364 K
svchost.exe                    620 Services                   0     13,360 K
svchost.exe                   1048 Services                   0     15,676 K
svchost.exe                   1056 Services                   0     17,096 K
svchost.exe                   1064 Services                   0      4,964 K
svchost.exe                   1108 Services                   0     14,092 K
svchost.exe                   1136 Services                   0     14,092 K
svchost.exe                   1232 Services                   0      5,996 K
svchost.exe                   1360 Services                   0     12,196 K
Memory Compression            1560 Services                   0     43,440 K
VSSVC.exe                     1704 Services                   0      5,276 K
svchost.exe                   1792 Services                   0      3,808 K
svchost.exe                   1868 Services                   0      6,452 K
svchost.exe                   1948 Services                   0      3,276 K
svchost.exe                   1956 Services                   0      4,980 K
spoolsv.exe                   1604 Services                   0     11,572 K
svchost.exe                   2212 Services                   0      3,816 K
svchost.exe                   2304 Services                   0     23,876 K
MsMpEng.exe                   2328 Services                   0     80,072 K
svchost.exe                   2876 Services                   0      4,720 K
NisSrv.exe                    3184 Services                   0      8,432 K
svchost.exe                   3776 Services                   0      5,692 K
MicrosoftEdgeUpdate.exe       4064 Services                   0      3,328 K
SgrmBroker.exe                3088 Services                   0      5,560 K
uhssvc.exe                    2456 Services                   0      5,620 K
svchost.exe                   3408 Services                   0     10,100 K
svchost.exe                    552 Services                   0      8,144 K
SearchIndexer.exe             1076 Services                   0     16,056 K
svchost.exe                   2248 Services                   0      7,216 K
svchost.exe                   3884 Services                   0     15,688 K
WmiPrvSE.exe                   896 Services                   0      9,496 K
cmd.exe                        388 Services                   0      3,904 K
conhost.exe                   2196 Services                   0     11,984 K
```

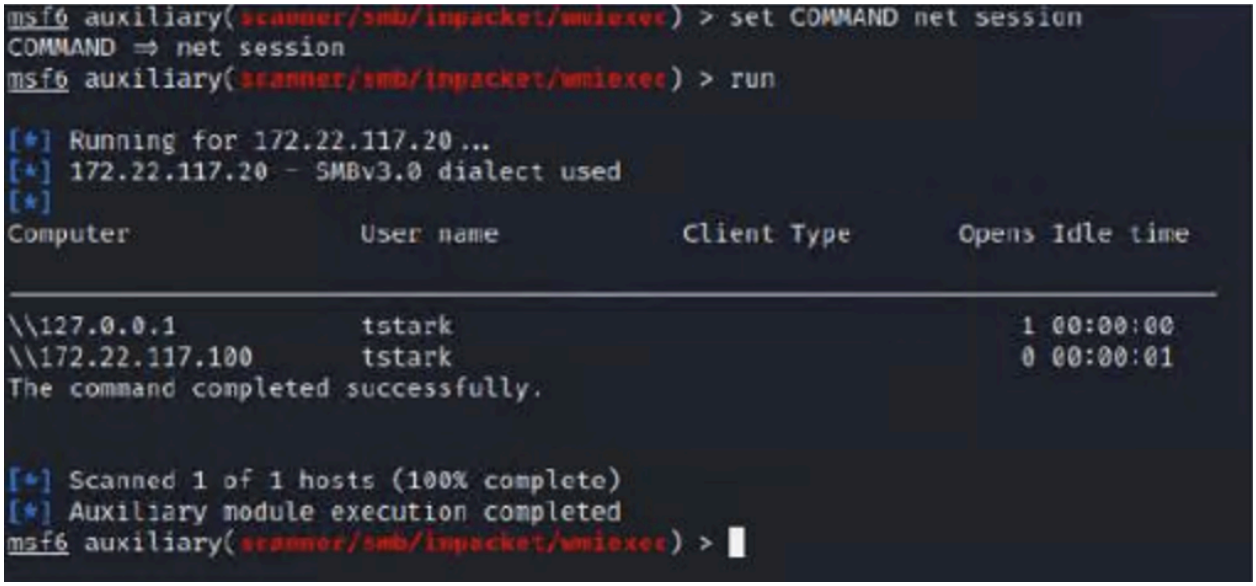
```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND ver
COMMAND ⇒ ver
msf6 auxiliary(scanner/smb/impacket/wmiexec) > run

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]
Microsoft Windows [Version 10.0.19042.1288]
```

```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND systeminfo
COMMAND ⇒ systeminfo
msf6 auxiliary(scanner/smb/impacket/wmiexec) > run

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]

Host Name:                 WINDOWS10
OS Name:                   Microsoft Windows 10 Pro N
OS Version:                10.0.19042 N/A Build 19042
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Member Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          sysadmin
Registered Organization:
Product ID:                00331-60000-00000-AA609
Original Install Date:     5/10/2021, 12:17:16 AM
System Boot Time:          7/12/2022, 7:26:24 PM
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2295 Mhz
BIOS Version:              Microsoft Corporation Hyper-V UEFI Release v4.0, 11/1/2019
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory:     927 MB
Available Physical Memory: 275 MB
Virtual Memory: Max Size:  2,655 MB
Virtual Memory: Available: 1,914 MB
Virtual Memory: In Use:    741 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    megacorpone.local
Logon Server:              N/A
Hotfix(s):                 7 Hotfix(s) Installed.
                           [01]: KB5005539
                           [02]: KB4562830
                           [03]: KB4570334
                           [04]: KB4580325
                           [05]: KB4586864
                           [06]: KB5006670
                           [07]: KB5005699
Network Card(s):           1 NIC(s) Installed.
                           [01]: Microsoft Hyper-V Network Adapter
```



Reverse Shell Vulnerability

Risk Rating: High

Description:

To establish a reverse shell on the domain of www.megacorpone.com, I first used the tool msfvenom to initiate a listener port. Msfvenom is a payload generation tool that allows you to generate various types of payloads, including reverse shells, which can be used to establish a connection between the attacker's machine and the target. I configured the listener on a specific port, in this case, it was Port 4444.

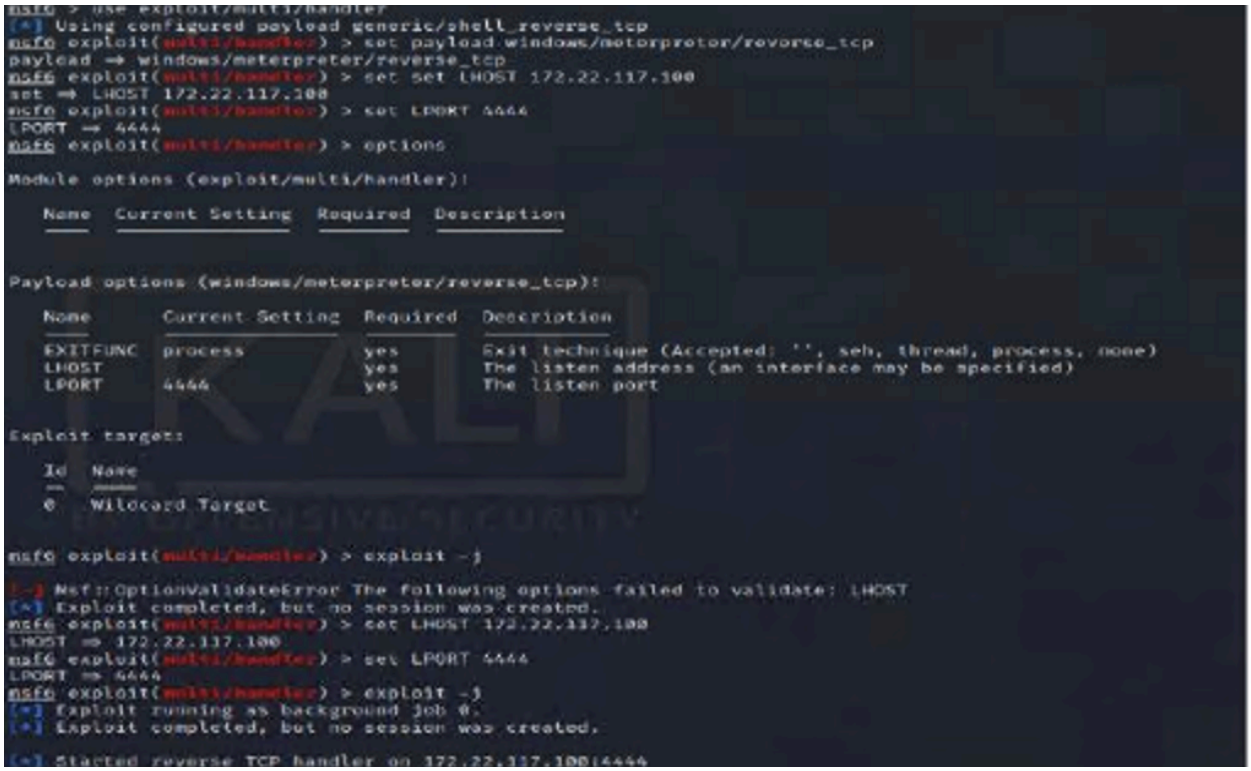
Once the listener was established, I used Metasploit along with the exploit "exploit/multi/handler" and payload "windows/meterpreter/reverse_tcp" to create a reverse shell on the target machine. Metasploit is a powerful framework that allows you to exploit vulnerabilities in various systems, and the "exploit/multi/handler" module is used to handle the payloads generated by msfvenom. The payload "windows/meterpreter/reverse_tcp" was used to establish a reverse TCP connection between the target machine and my machine, allowing me to gain a meterpreter session.

This allowed me to bypass the firewalls and gain complete control of the target machine, giving me access to all the resources on the server. The Meterpreter session also allowed me to execute various commands, such as capturing keystrokes, capturing screenshots, and uploading/downloading files. This helped me to gather information and exfiltrate data from the target machine.

Affected Hosts:.megacorpone.com

Remediation:

- Remove unnecessary services, restricting the execution of the reverse shell code
- Perform scheduled maintenance and patching to limit potential vulnerabilities
- Lock all outgoing connectivity except for specific ports.



Credential Dumping

Risk Rating: High

Description:

During the engagement, CyberSafe employed the use of Mimikatz Kiwi to extract all user information from the Windows Domain Controller. This powerful tool allows for the extraction of user credentials, including password hashes, from the Active Directory database. By executing the command "kiwi_cmd lsadump::cache", CyberSafe was able to collect all of the credentials stored on the Domain Controller. These credentials were saved in a file called "hash.txt" for further analysis.

The next step in the process was to crack the password for the user "bbanner", which was accomplished using the tool "John the Ripper". This tool is a popular password cracking tool that uses a dictionary attack and brute force methods to crack passwords. By using "John the Ripper" on the "hash.txt" file, CyberSafe was able to successfully crack the password for the user "bbanner"

With this information, CyberSafe was able to move laterally across the network, which would be challenging to detect as it may appear as normal network activity. This resulted in a full compromise of the system, giving an attacker access to move freely across the network. This highlights the importance of strong password policies and regular password updates to prevent such attacks. The ability to move laterally across the network undetected is a significant concern as it allows an attacker to access sensitive information and disrupt operations. CyberSafe recommends that MegaCorpOne take immediate action to address this vulnerability and implement stronger security measures to protect their network.

Affected Hosts:.megacorpone.com

Remediation:

- Update the endpoint Security Solution
- Maintain proper IT hygiene by eliminating Vulnerabilities

Compromised Server Users.

Risk Rating: Medium

Description:

To view all compromised servers and users registered on the domain of www.megacorpone.com, I used the Meterpreter shell, which is a powerful post-exploitation tool that can be used to gain access to a compromised system and manipulate it in various ways. The first step I took was to gain access to a compromised server on the domain by exploiting a known vulnerability. Once I had access to the server, I used the Meterpreter shell to interact with the system and gain a deeper level of access.

Once I had a Meterpreter shell on the compromised server, I used various commands to gather information about the server and the other systems on the domain. I was able to use the command "ps" to view all the processes running on the server, and "sysinfo" to gather information about the operating system, hardware, and network configuration. I also used the command "netstat -ano" to view all the active network connections, which helped me identify other systems on the domain. After gathering this information, I was

able to identify the other servers and users that were compromised on the domain of www.megacorpone.com.

Additionally, I used the command "hashdump" to extract the password hashes on the server. This allowed me to try cracking the passwords to gain access to other user accounts on the domain. With the help of Meterpreter shell, I was able to view all the compromised servers and users registered on the domain and gain a deeper level of access on the network.

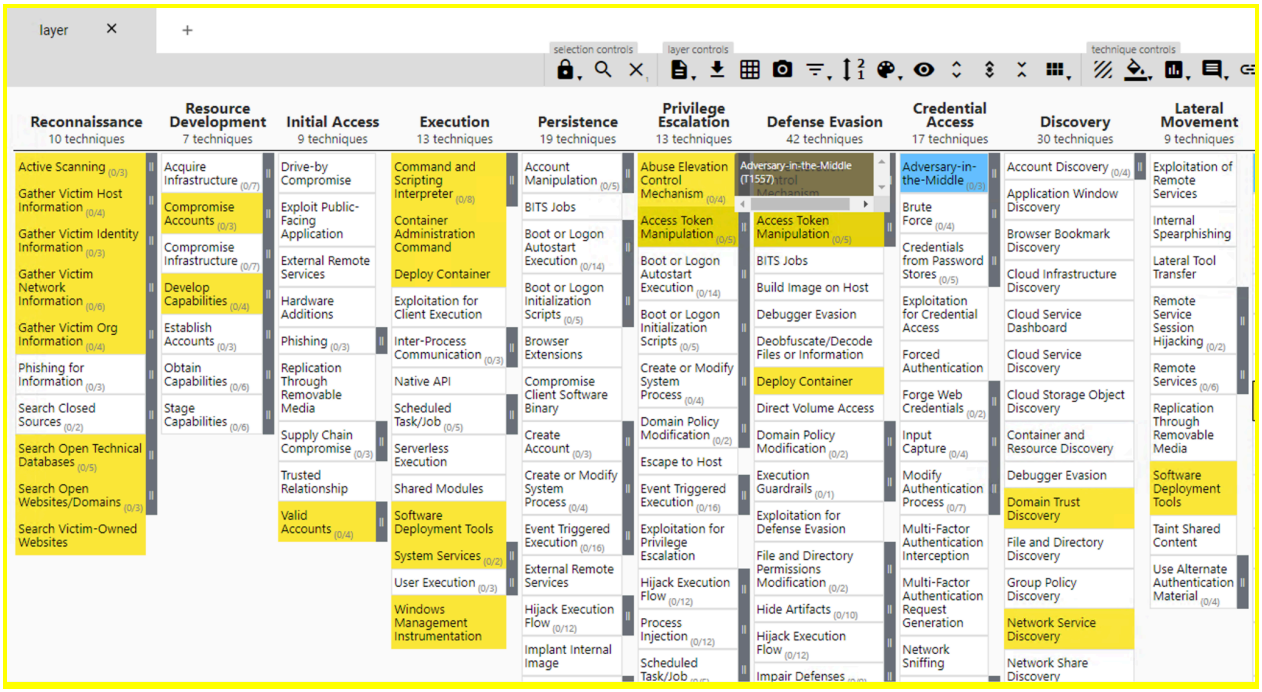
Affected Hosts:.megacorpone.com

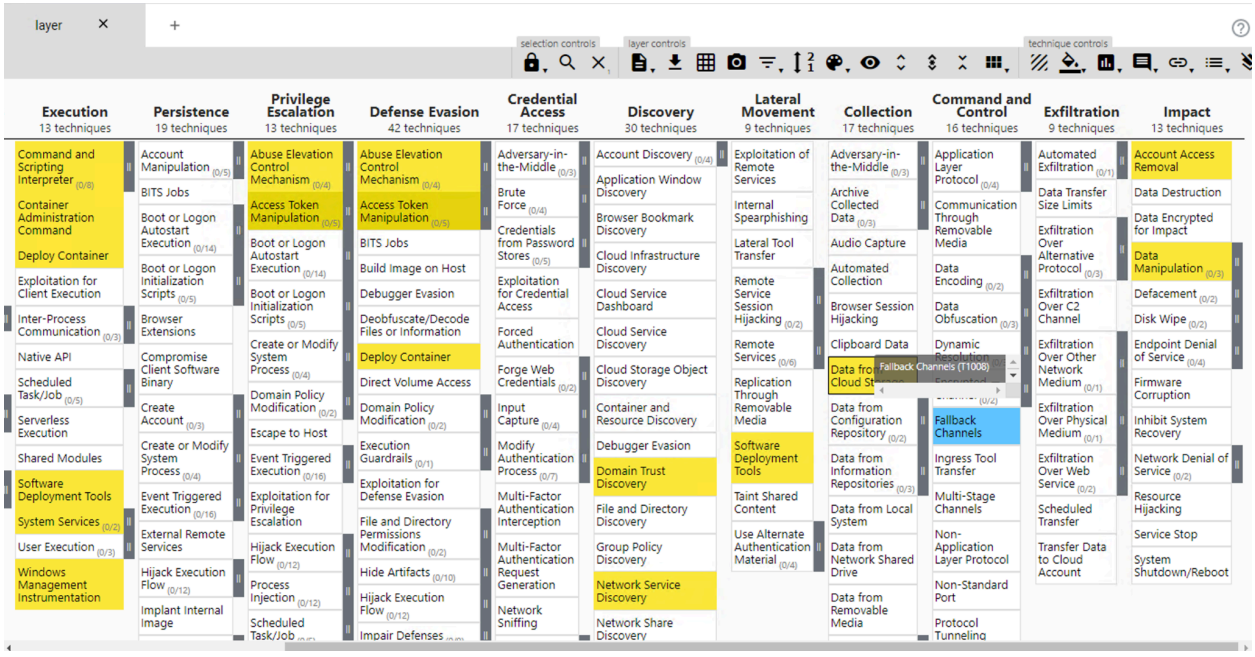
Remediation:

- Update the endpoint Security Solution
- Maintain proper IT hygiene by eliminating Vulnerabilities

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:





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

Legend:

Performed successfully
Failure to perform

[MITRE ATT&CK navigator map]