Cybersecurity

Penetration Test Report

MegaCorpOne

Penetration Test Report

Robust 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

Contact Information

Company Name	ROBUST SECURITY LLC
Contact Name	Stokely R. De Freitas
Contact Title	Lead Penetration Tester
Contact Phone	715.555.3543
Contact Email	stokely.defreitas@robustsecurity.com

Document History

Version	Date	Author(s)	Comments
001	07/13/2022	Stokely De Freitas	Initial Draft Report
002	07/21/2022	Stokely De Freitas	Interim Report
003	07/24/2022	Stokely De Freitas	Final Report

Introduction

In accordance with MegaCorpOne's policies, ROBUST SECURITY, LLC (henceforth known as RS LLC) 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 several systems on MegaCorpOne's network segments by RS LLC during July of 2022.

For the testing RS LLC 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 (Black Box Testing).
- 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.

RS LLC 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.
Social Engineering
Physical Penetration Testing
Wireless Security

Penetration Testing Methodology

Reconnaissance

RS LLC 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

RS LLC uses custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide MegaCorpOne with an understanding of the risks that threaten its information, and 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

RS LLC 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
172.22.117.0/24 MCO.local *.Megacorpone.com	MegaCorpOne internal domain, range and public website

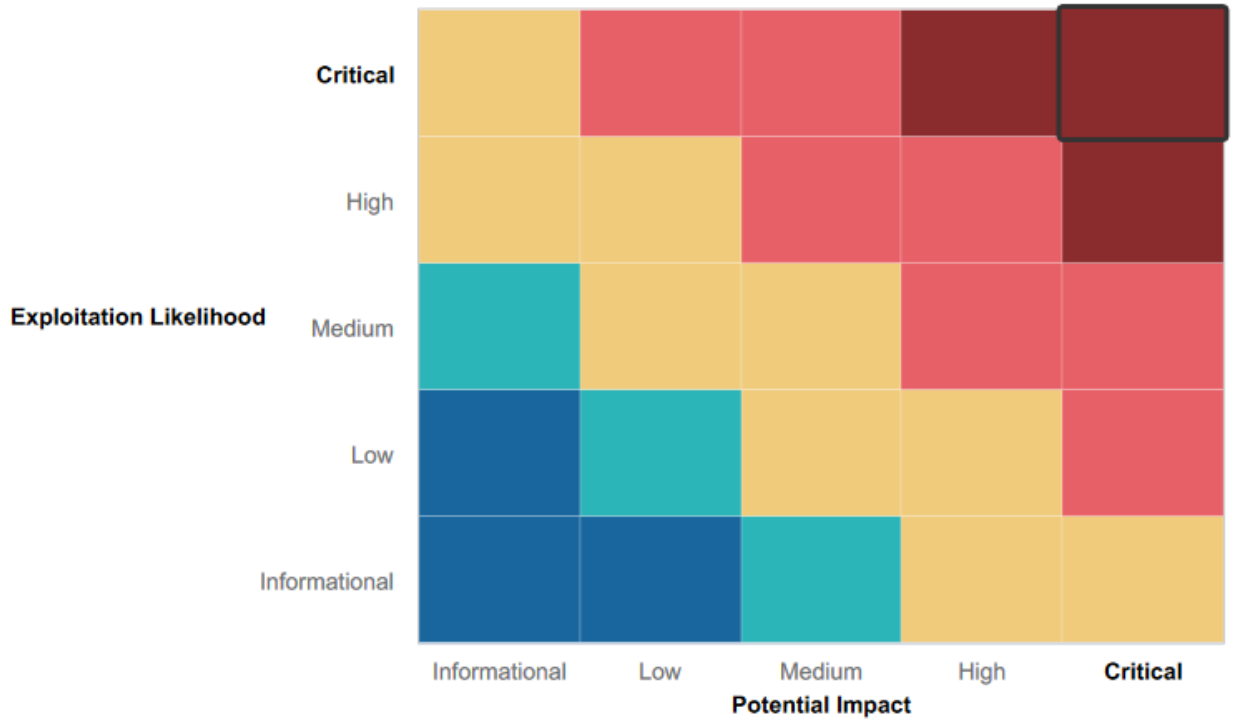
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

Critical: Immediate threat to key business processes.
High: Indirect threat to key business processes/threat to secondary business processes.
Medium: Indirect or partial threat to business processes.
Low: No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
Informational: No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within MegaCorpOne's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- The bedrock of a successful security program is the deployment and adoption of a security awareness program. MegaCorpOne security awareness program is already experiencing a measure of success in its recent implementation. All attempts to use social engineering as a means in compromising the company, failed. We were either routed to management or denied the requested information.

- Physical security was another strength of the company. Each employee is assigned a perimeter access badge with their picture. The badge must be presented on entry to the main building, and should an employee not have their badge, a form of identification must be shown at the security desk to confirm identity. Additionally, mantraps (turnstiles) are used to manage the flow of employees further into the campus. Each employee is required to use their respective badge on the turnstile to proceed further. This also prevents "piggybacking" of employees and or visitors to the building.

- Reconnaissance of the wireless networks showed only a public facing wireless SSID. Connecting to the service requires the used to create an account, using those credentials for access. It's suspected the SSID of the internal network is not being broadcast, preventing it from being visible by anyone external to the organization.

Summary of Weaknesses

RS LLC 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.

- Senior management contact details are available online to the public. Ideally, a central Point of Contact should be established, with that department's contact details publicly available.

- There was no resistance to network scanning and mapping. As a result, it was not difficult to develop or visualize the network infrastructure.

- During the reconnaissance phase several known vulnerabilities along with open ports were identified, with them being exploited during this engagement.

- Instances of login credentials were found stored within text files and obviously labeled as such. These credentials lacked complexity and took very little effort cracking.

Executive Summary

Robust Security LLC conducted a comprehensive security assessment of MegaCorpOne in order to determine existing vulnerabilities and establish the current level of security risk associated within their ecosystem and the technologies in use. This assessment harnessed penetration testing techniques to provide MegaCorpCorp management with an understanding of the risks and security posture of the corporate environment.

To test the security posture of the internal network, we began with a reconnaissance and host discovery phase during which we used port scans using Zenmap, and OSINT tools to fingerprint the operating systems, software, and services running on each target host. After fingerprinting the various targets and determining open ports and services enabled on each host, we executed a vulnerability enumeration phase, in which we listed all potential vulnerabilities affecting each host and developed a list of viable attack vectors. We attempted to exploit all vulnerabilities affecting the target hosts. After comprehensive testing, there were excessive vulnerabilities discovered within the target hosts environment. Those vulnerabilities were ultimately exploited, compromising the confidentiality, integrity and availability of resources.

The engagement highlighted multiple Critical, High and Medium severity issues impacting MegaCorpOne internal network, which required immediate remediation efforts in order to secure the company's environment against malicious threat actors. The wireless network and physical security were not in scope; however, a high-level review was performed on the infrastructure. Also performed was a physical security assessment due to it not being in scope at this time. Overall assessment shows that MegaCorpOne is not prepared to defend against an attack and should take immediate steps to remediate the findings presented within this report.

Summary Vulnerability Overview

Vulnerability	Severity
Executive Team's Business Contact Information on Company Site.	Medium
Server Details and Robots.txt file Configuration	Low
Site Profile from Shodan.io and Known Exploits	Critical
Weak Password on Public Web Application	Critical
Vulnerable Open Ports on The Network	Critical
C2 Research	N/A
Exploiting and Privilege Escalation	Critical
Password Cracking	Critical
Setting up Persistence on Compromised Machine	Critical
Windows Open Port	High
Vulnerability to Password Spraying	Medium
LLMNR Spoofing Vulnerability	Critical
Windows Management Instrumentation (WMI) Vulnerability	Medium
Reverse Shell Vulnerability	High
Privilege Escalation Exploit & Persistence	Critical
Credential Dumping & Lateral Movement	High
Compromised Server Users	Medium

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

Scan Type	Total
Hosts	172.22.117.20 172.22.117.150
Ports	172.22.117.20 135 – msrpc 139 – netbios-ssn

	445 – Microsoft-ds 3390 – ms-wbt-server 172.22.117.150 21 – ftp 22 – ssh 23 – telnet 25 – smtp 53 – domain 80 – http 111 - rpcbind

Exploitation Risk	Total
Critical	8
High	3
Medium	4
Low	1

Vulnerability Findings

Executive Team's Business Contact Information on Company Site

Risk Rating: **Medium**

Description:
The **www.megacorpone.com** displays sensitive information in the form of the executive team's full names, titles, email addresses and images. Using the Google Dorking OSINT approach, RS LLC identified the names, positions, email addresses and images of the executive team members as shown on **Fig.1** and **Fig.2** respectively. In addition to this initial information, it was revealed the web server is sitting on a Debian distro running Apache 2.4.38 on port 80 also shown on These may all seem insignificant; however, most threat actors initiate hacks weeks, months or even years prior through passive information gathering. This process is known as passive reconnaissance, where they search publicly available information (social media, company's website, government info services, etc...) building profiles of their potential victims.

Affected Hosts: www.megacorpone.com

Remediation:

- Remove the direct contact information of the executive team from the website.
- Use a single email address, where all company communication is received and then routed to the respective parties.
- The single points of contact should be as follows: -
  - hrdept@megacorpone.com – HR Department Inbox
  - prdept@megacorpone.com – Public Relations Inbox
    or
  - contactus@megacorpone.com – General Inbox

Fig.1 – Executive TM names

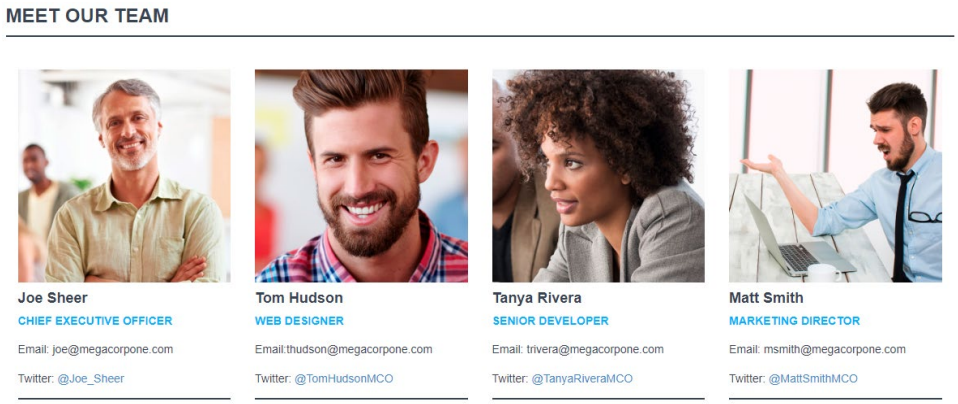


Fig.2 – Executive TM name along with Images.

Server Details and Robots.txt File Configuration

Risk Rating: Low

Description:
The **www.megacorpone.com** displays that the web server is sitting on a Debian distro running Apache 2.4.38 on port 80 also shown on **Fig.3**. A closer look at the backend server revealed the existence of a "robot.txt" file. Based on its configuration there are no restrictions for web crawlers, instead they have full access to map the structure of the website as shown in **Fig.4**. This allows an attacker to not only identify what technologies are running in your ecosystem, but also document known exploits to be leveraged later.

Affected Hosts: www.megacorpone.com

Remediation:

- The "robots.txt" file should be reconfigured to exclude specific areas of the site (e.g., User-agent: * - Disallow: /include/)

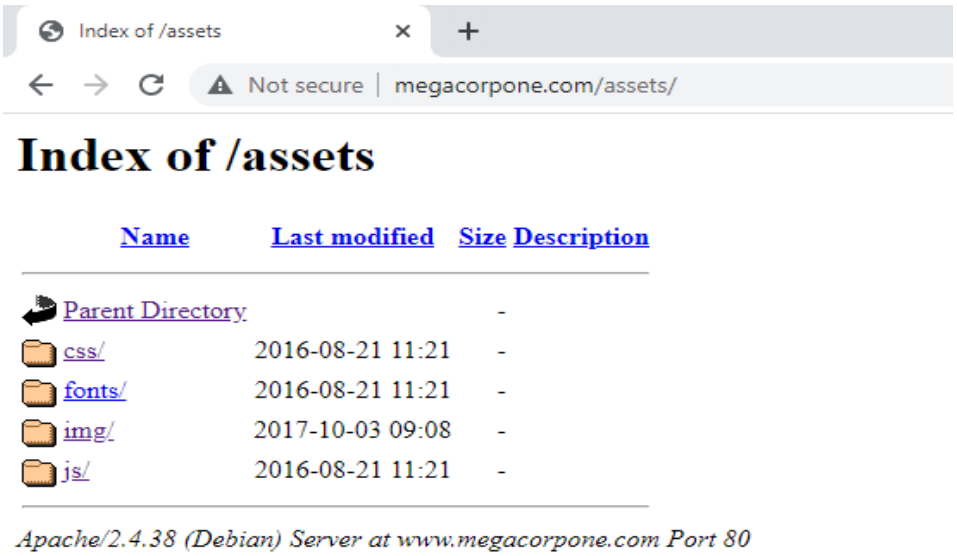


Fig.3 – OS, Web Server version and Port

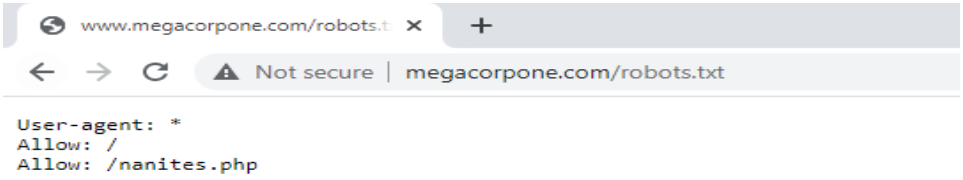


Fig.4 – Robots.txt file with no crawling restrictions

Site Profile from Shodan.io and Known Exploits

Risk Rating: Critical

Description:
The external facing IP address was obtained through a basic "nslookup" of the domain www.megacorpone.com from my workstation as shown on **Fig.5**. With the IP address and using www.shodan.io, RS LLC found the site's profile along with all associated details as shown on **Fig.6.**

The following is Shodan.io profile of the company's site:

Site Profile:

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

Known CVE Vulnerabilities:

Note: The device may not be impacted by all these issues. The vulnerabilities are implied based on the software and version.

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-2020-1934	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
CVE-2021-34798	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2020-35452	Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow
CVE-2022-29404	In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the

	parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
CVE-2022-28330	Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
CVE-2020-11993	Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.
CVE-2019-10081	HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.
CVE-2019-0217	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0196	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-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-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-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-* 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.
CVE-2019-10098	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.
CVE-2021-40438	A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2021-36160	A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).
CVE-2022-23943	Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.
CVE-2020-1927	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
CVE-2022-30522	If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort.
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-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 vulnerabilty 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 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-2019-10082	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-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-2022-28615	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 r:wsread() that point past the end of the storage allocated for the buffer.
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.

Along with shodan.io, recon-ng as shown in **Fig.7 – Fig.8**, configured for sensitive information gathering by finding files such as robot.txt, Geo-IP, Banner Grabbing, DNS Lookup, port scanning, and sub-domain information. Scanning the IP address revealed several sub-domains along with IP addresses as shown in **Fig.9**.

RS LLC generated reports for export and further analysis. This is shown in **Fig.10 – Fig.12**. See attached document "**results.html**"

Affected Hosts: www.megacorpone.com

Remediation:

- Review all known vulnerabilities and patch as required to avoid your system being exploited.

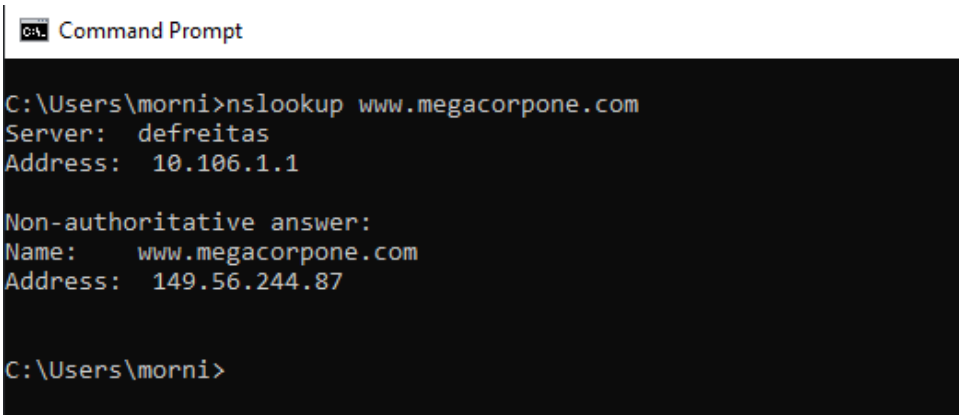


Fig.5 – Command Prompt used to obtain external facing IP address

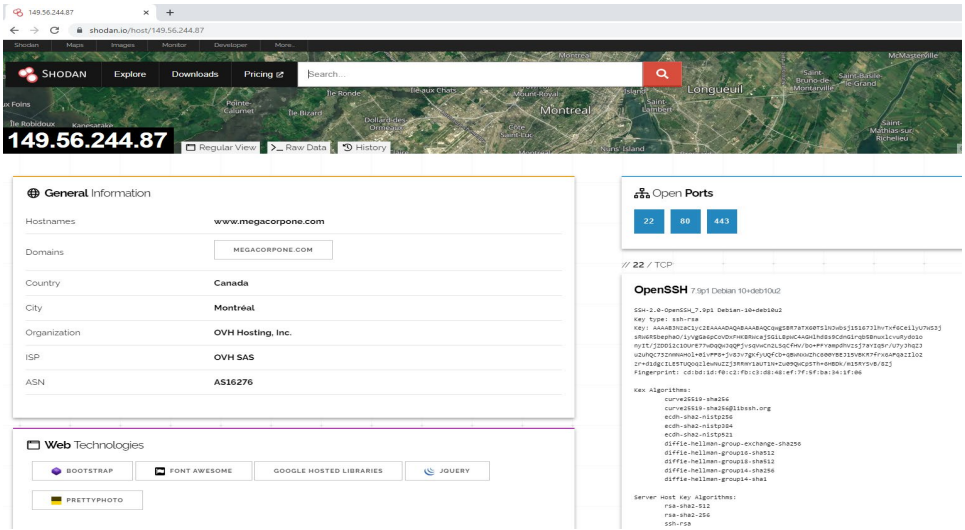


Fig.6 – Shodan.io profile for the site

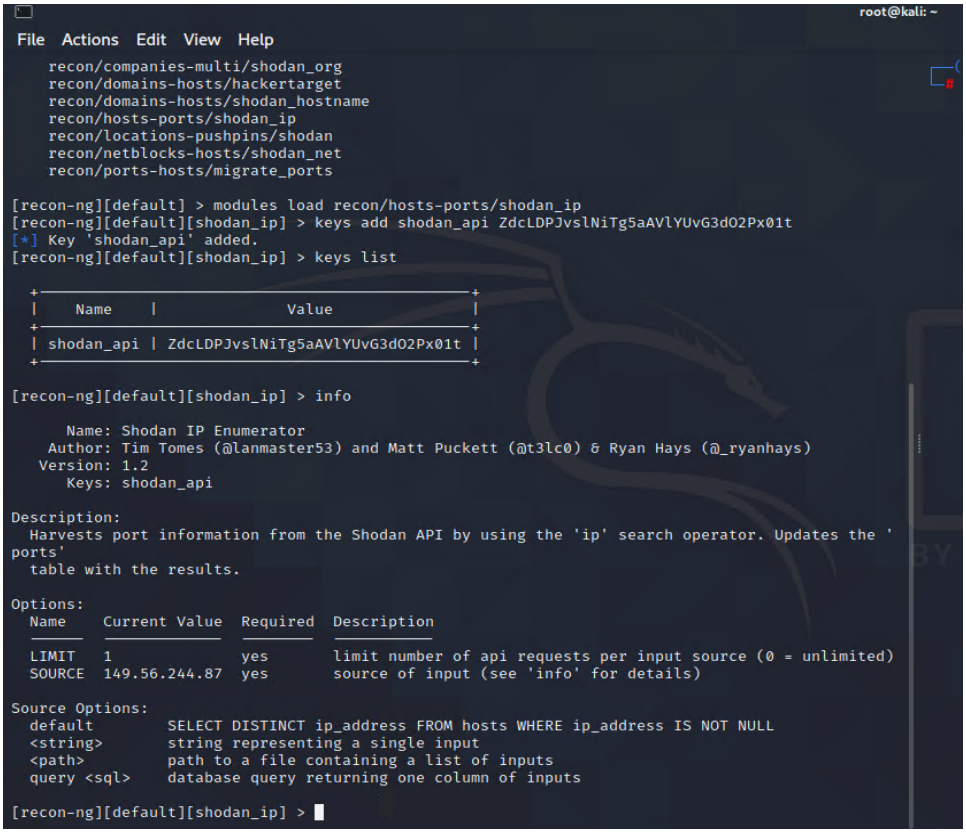


Fig.7 – Configuring recon-ng with the shodan.io API for report generation

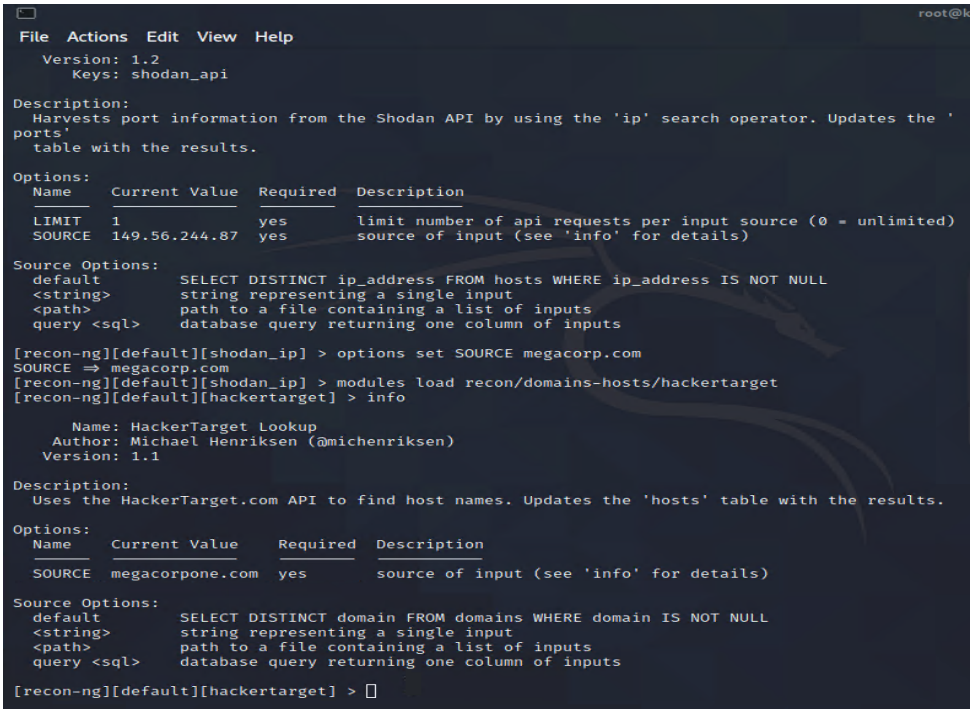


Fig.8 – Using recon-ng to scan all sub-domains and folders.

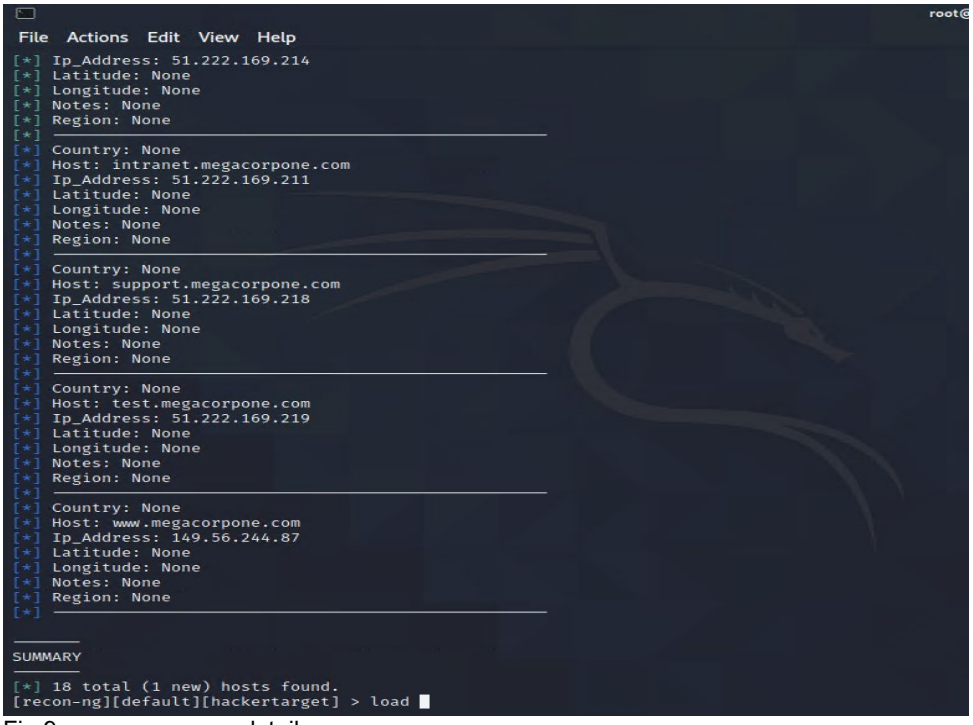


Fig.9 – recon-ng scan details

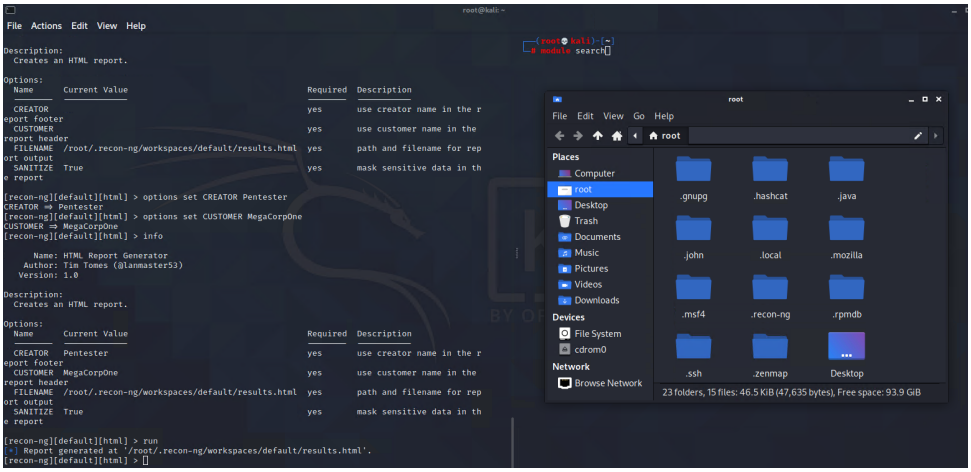


Fig.10 – Report located within the root folder

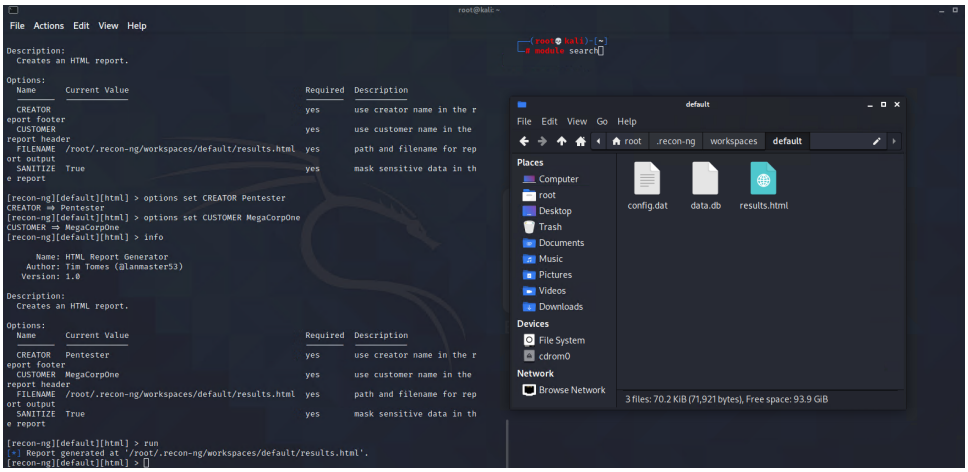


Fig. 11 – Report location within Pentester machine

MegaCorpOne

www.recon-ng.com

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	51.222.39.63						hackertarget
ns3.megacorpone.com	66.70.207.180						hackertarget
router.megacorpone.com	51.222.169.214						hackertarget
siem.megacorpone.com	51.222.169.215						hackertarget
snmp.megacorpone.com	51.222.169.216						hackertarget
support.megacorpone.com	51.222.169.218						hackertarget
syslog.megacorpone.com	51.222.169.217						hackertarget
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
Tue, Jul 05 2022 16:29:25

Fig.12 – Screeprint of recon-ng scan

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. RS LLC was able to use a username gathered from OSINT in combination with a wordlist in order to guess the user's password and access the configuration file.

Affected Hosts: vpn.megacorpone.com

Remediation:

- Set up two-factor authentication instead of basic authentication to prevent dictionary attacks from being successful.
- Require a strong password complexity that requires passwords to be over 12 characters long, upper, lower case, & include a special character.
- Reset the user **thudson**'s password.

Vulnerable Open Ports on The Network

Risk Rating: Critical

Description:
A Zenmap full network scan **Fig.13** was performed on **megacorpone.com**, in order to generate an inventory of computers. The results of the network scan showed there were vulnerable computers as shown on **Fig.14 – Fig.16** with open ports running potentially vulnerable applications. Further analysis confirmed there is a potential known exploit at **Fig.15 "21/tcp open ftp vsftpd"**. Using Searchsploit, seven (7) known exploit were found as shown at **Fig.17 "vsftpd 2.3.4 – Backdoor Command Execution Unix/remote/49757.py"**.

The exploit was reviewed as shown at **Fig.18** to determine the required parameters and arguments needed for successful execution. RS LLC successfully gained access to the machine **172.22.117.150** and was able to open a shell as shown at **Fig.19**. A "whoami" was executed to confirm "root" access. Additional resources were included to provide for information on this exploit. See **Fig.20 – Fig.21**.

Affected Hosts: megacorpone.com

Remediation:

- Perform regular vulnerability scanning for network visibility.
- Subscribe to various services that provides the latest CVE updates.
- Verify the current software is patched or replaced if necessary to maintain security.
- Close all unnecessary ports and set access rules to govern usage.

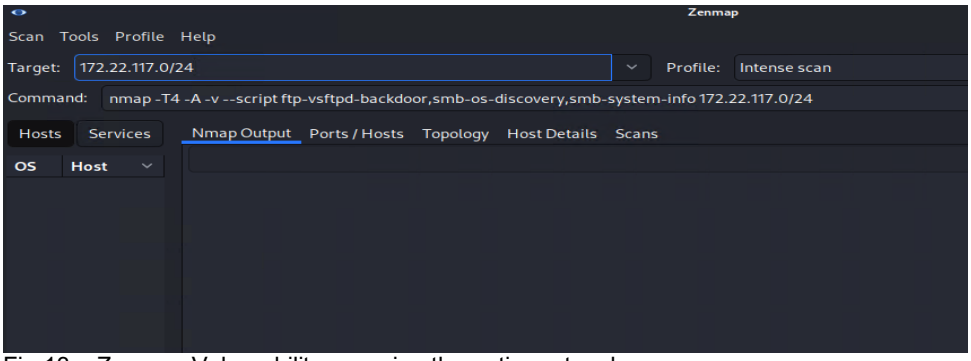


Fig.13 – Zenmap Vulnerability scanning the entire network.

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00073s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3390/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:15:5D:02:04:01 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 1909
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.73 ms Windows10 (172.22.117.20)
```
Fig.14 - Scan results for 172.22.117.20.

```
Nmap scan report for 172.22.117.150
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (reset)
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: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:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
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)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
```

Fig.15 – Scan results for 172.22.117.150

```
Nmap scan report for 172.22.117.100
Host is up (0.000069s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE     VERSION
80/tcp   open     http        Apache httpd 2.4.46
| http-server-header: Apache/2.4.46 (Debian)
5901/tcp open     vnc         VNC (protocol 3.8)
6001/tcp open     X11         (access denied)
8080/tcp filtered http-proxy
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=7/17%OT=80%CT=1%CU=32017%PV=Y%DS=0%DC=L%G=Y%TM=62D46DB
OS:D%P=x86_64-pc-linux-gnu)SEQ(SP=109%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=MFFD7ST11NW7%O2=MFFD7ST11NW7%O3=MFFD7NNT11NW7%O4=MFFD7ST11NW7%O5=MFF
OS:D7ST11NW7%O6=MFFD7ST11)WIN(W1=FFCB%W2=FFCB%W3=FFCB%W4=FFCB%W5=FFCB%W6=FF
OS:CB)ECN(R=Y%DF=Y%T=40%W=FFD7%O=MFFD7NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=
OS:A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=40%CD=S)

Uptime guess: 36.891 days (since Fri Jun 10 18:51:22 2022)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=265 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: 127.0.1.1
```

Fig.16 – Scan results for 172.22.117.100

```
┌──(root💀kali)-[~]
└─# searchsploit vsftpd
 Exploit Title                                                  |  Path
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption  | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)  | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)  | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                       | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)          | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                         | multiple/remote/49719.py
Shellcodes: No Results
┌──(root💀kali)-[~]
└─#
```

Fig.17 – Searchsploit results for the vsftpd exploit.

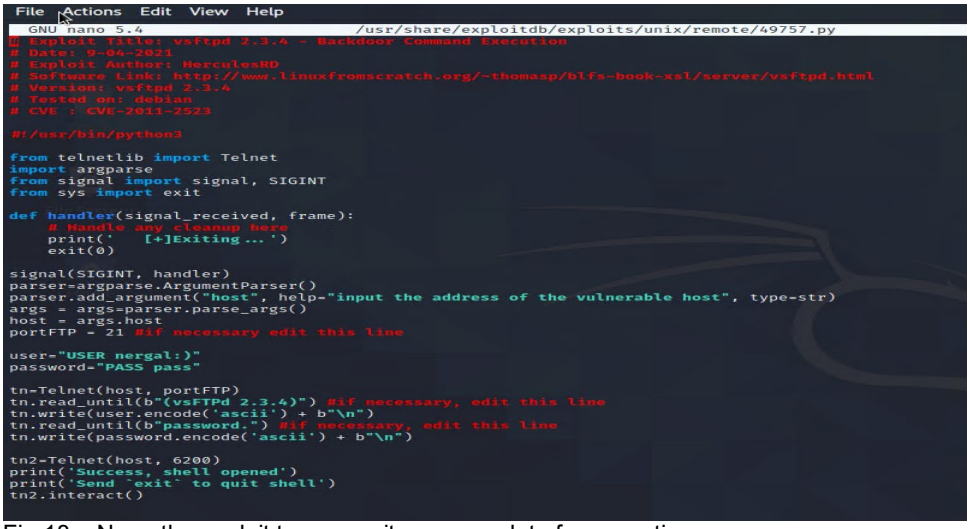


Fig.18 – Nano the exploit to ensure it was complete for execution.

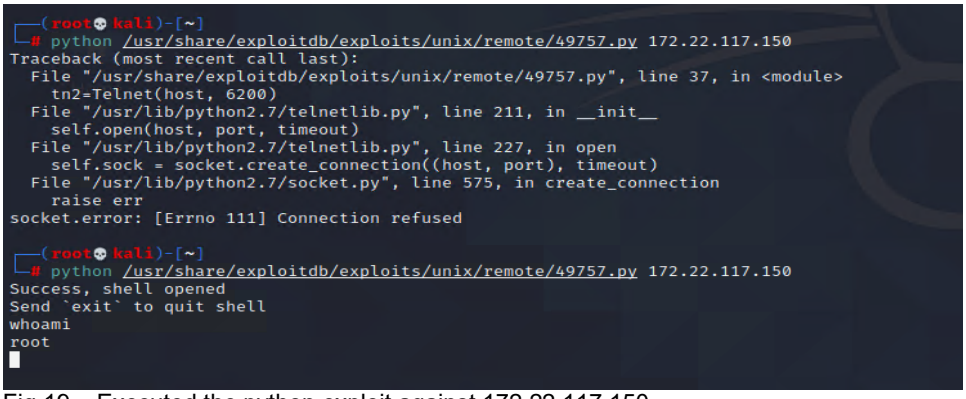


Fig.19 – Executed the python exploit against 172.22.117.150.

Fig.20 – Searchsploit vsftpd with a -w to view the exploit in html.

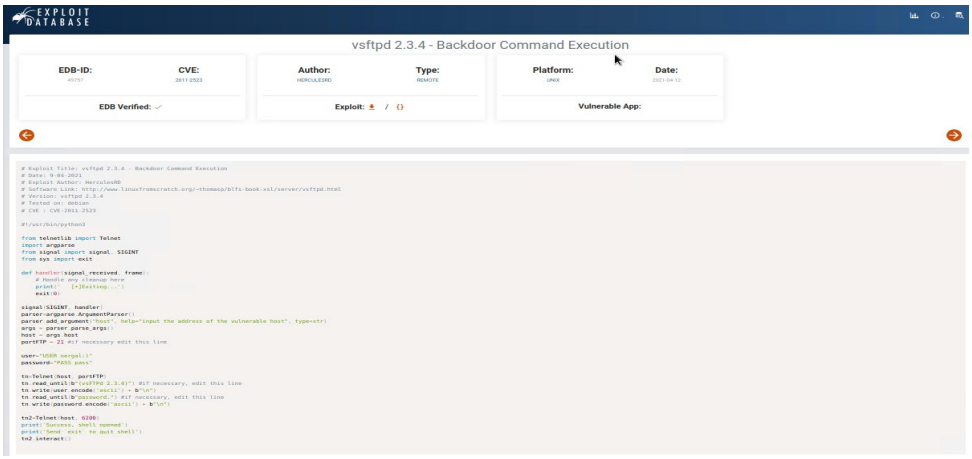


Fig.21 – Using the exploit database to understand it's full impact.

C2 Research

Risk Rating: N/A

Description:
RS LLC wanted insight into whether the network was susceptible to a Command and Controls (C2) attack. Using https://www.thec2matrix.com/matrix three (3) potential frameworks were identified based on the current infrastructure.

C2 Research:

1. What is the name of the C2 framework?
    a. Caldera ver.2
    b. Metasploit ver.5.0.62
    c. SCYTHE ver.2.5
2. What operating systems do its agents support?
    a. Caldera ver.2
        i. Windows
        ii. Linux
        iii. macOS
    b. Metasploit ver.5.0.62
        i. Windows
        ii. Linux
        iii. macOS
    c. SCYTHE ver.2.5
        i. Windows
        ii. Linux
        iii. macOS
3. What channels can the agents communicate over?
    a. Caldera ver.2
        i. HTTP
    b. Metasploit ver.5.0.62
        i. HTTP
        ii. TCP
    c. SCYTHE ver.2.5
        i. HTTP
        ii. TCP
        iii. SMB
        iv. DNS
4. What language is it written in?
    a. Caldera ver.2
        i. Python & Go
    b. Metasploit ver.5.0.62
        i. Ruby & C/java/PHP/Python
    c. SCYTHE ver.2.5
        i. Python & C
5. Is it open or closed source?
    a. Caldera ver.2
        i. Open Source
    b. Metasploit
        i. Open Source
    c. SCYTHE ver.2.5
        i. Closed Source
6. Does the developer have a Slack or Twitter link for potential support questions?
    a. Caldera ver.2
        i. Slack
    b. Metasploit ver.5.0.62

        i. Slack
    c. SCYTHE ver.2.5
        i. Twitter

Using Metaspolit several ports were scanned with the results shown below:

1. Exploit: auxiliary/scanner/ftp/anonymous/
    a. Host IP address: 172.22.117.150
    b. Port: 21
    c. Service name: FTP
    d. Service version: vsFTpD 2.3.4
    e. Exploit outcome: Success

2. Exploit: auxiliary/scanner/smtp/smtp_enum/
    a. Host IP address: 172.22.117.150
    b. Port: 25
    c. Service name: SMTP
    d. Service version: ESMTP Postfix (Ubuntu)
    e. Exploit outcome: Not sure if it was successful

3. Exploit: auxiliary/scanner/ssh/ssh_login/
    a. Host IP address: 172.22.117.150
    b. Port: 22
    c. Service name: SSH
    d. Service version:
    e. Exploit outcome: Failed

4. Exploit: exploit/unix/irc/unreal_ircd_3281_backdoor/
    a. Host IP address: 172.22.117.150
    b. Port: 6667
    c. Service name: IRC
    d. Service version:
    e. Exploit outcome: Successful

5. Exploit: exploit/aix/rpc_cmsd_opcode21/
    a. Host IP address: 172.22.117.150
    b. Port: 111
    c. Service name: RPCBIND
    d. Service version:
    e. Exploit outcome: Unsuccessful – No session was created.

Exploiting and Privilege Escalation

Risk Rating: Critical

Description:
During the reconnaissance phase of the engagement, RS LLC discovered there were poor password management practices in use. Based on this and using the previously command shell exploit, RS LLC search all files and folders using the following "**find / -type f -iname "*pass*.txt"**" command as shown at **Fig.22**. It revealed at **Fig.23** the following file **"/var/tmp/adminpassword.txt"**, which was suspected of storing login credentials, with this assumption being subsequently confirmed at **Fig.24**.

RS LLC used the credentials found and successfully SSH using the following command **"ssh msfadmin@172.22.117.150"** as shown at **Fig.25**, then escalated that initial access to a "root" shell as shown at **Fig.26**.

Affected Hosts: megacorpone.com

Remediation:

- Used an approved enterprise tool for password management.
- Create a whitelist of users and computers allowed to SSH into the server.
- Do not save files and folders on the computer with login credentials.

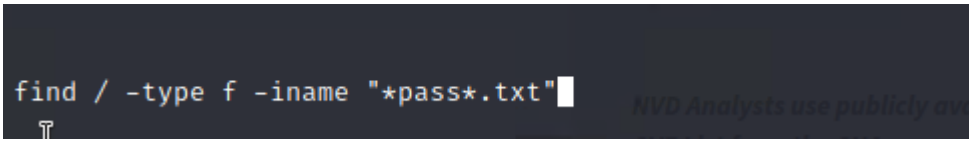


Fig.22 – Command used to locate any file with "pass" in the name coupled with wildcards.

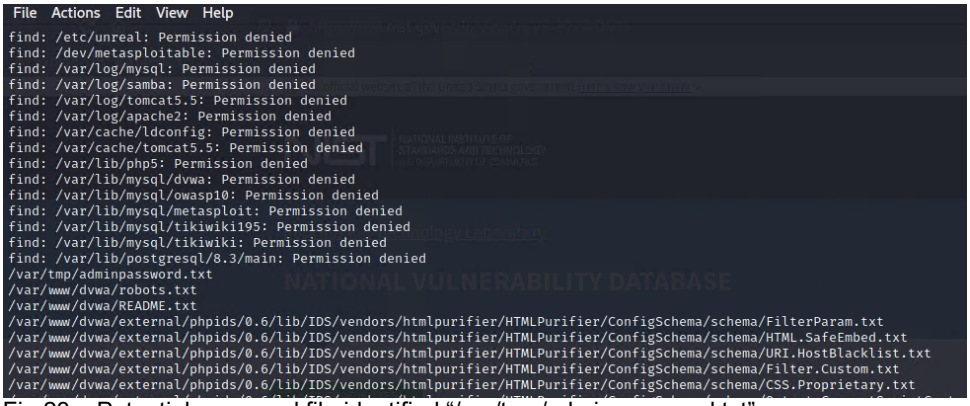


Fig.23 – Potential password file identified "/var/tmp/adminpassword.txt".

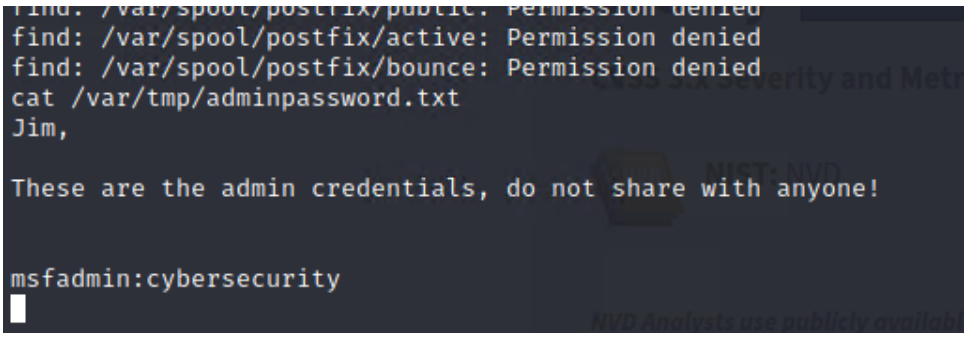


Fig.24 – File contents printed using the "cat" command.

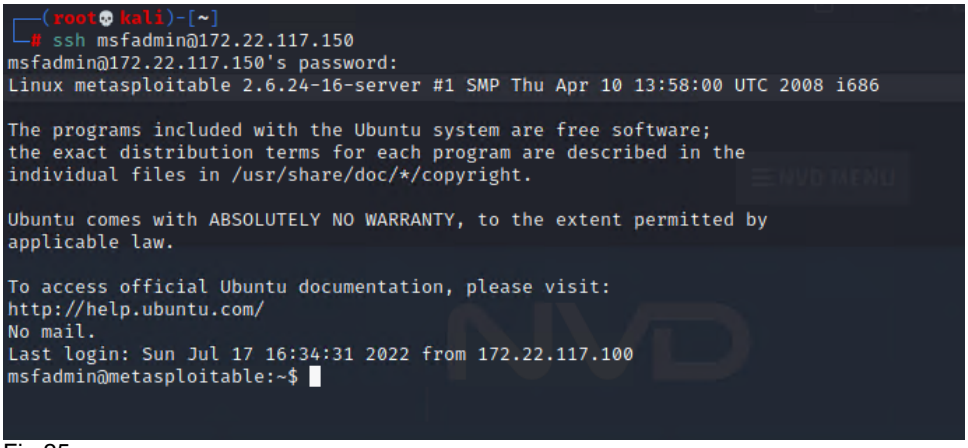

┌──(root💀kali)-[~]
└─# ssh msfadmin@172.22.117.150
msfadmin@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual 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 17 16:34:31 2022 from 172.22.117.100
msfadmin@metasploitable:~$

Fig.25

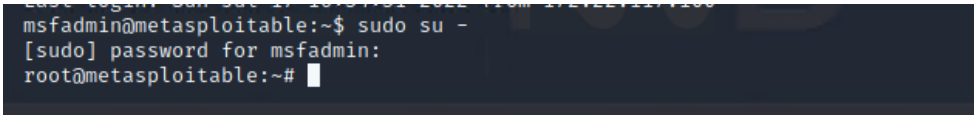

msfadmin@metasploitable:~$ sudo su -
[sudo] password for msfadmin:
root@metasploitable:~#

Fig.26

Password Cracking

Risk Rating: Critical

Description:
Exploiting the "root" shell, RS LLC logged into the machine as shown at **Fig.27**. Once in the system a search was initiated for the shadow file, using the following command "**sudo cat /etc/shadow**", with the results printed to the screen at **Fig.28**.

With all users' account identified, a new file (shadowfile.txt) was created only with valid credentials as shown at **Fig.29**. RS LLC then used "John the Ripper" password cracking tool as shown at **Fig.30** against the list. The first attempt was unsuccessful, however, subsequently the extracted list was matched against "**rockyou.txt**" and was successful. All passwords were cracked as shown at **Fig.31.** These new login credentials will be used later activities.

Affected Hosts: megacorpone.com

Remediation:

- Avoid frequently used word such as password, admin, 123456, etc…
- Passwords should consist of a combination of upper\lower case, numbers and special characters.
- Do not reuse passwords. Such as using the same password across multiple services (email, social media, etc…). The password list used in John the Ripper is a combination of compromised online credentials.
- Security awareness training to improve the tech acumen of its employees.

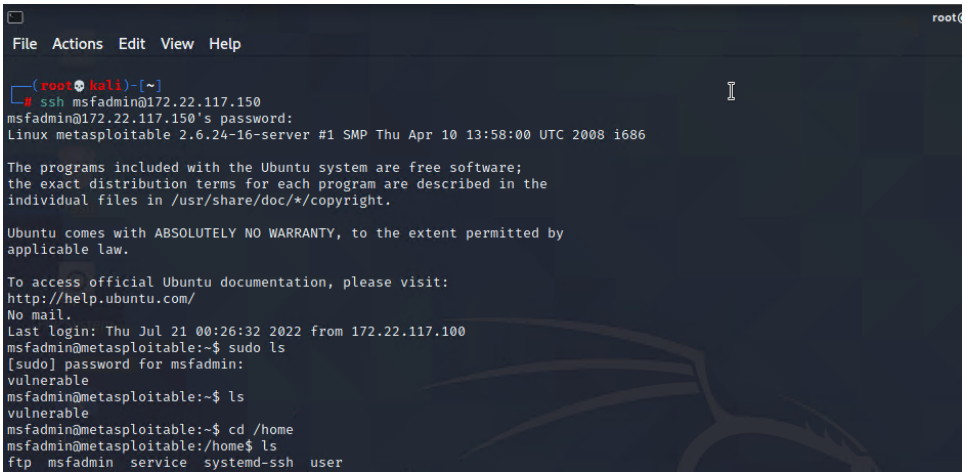


Fig.27 – SSH access to compromised system.

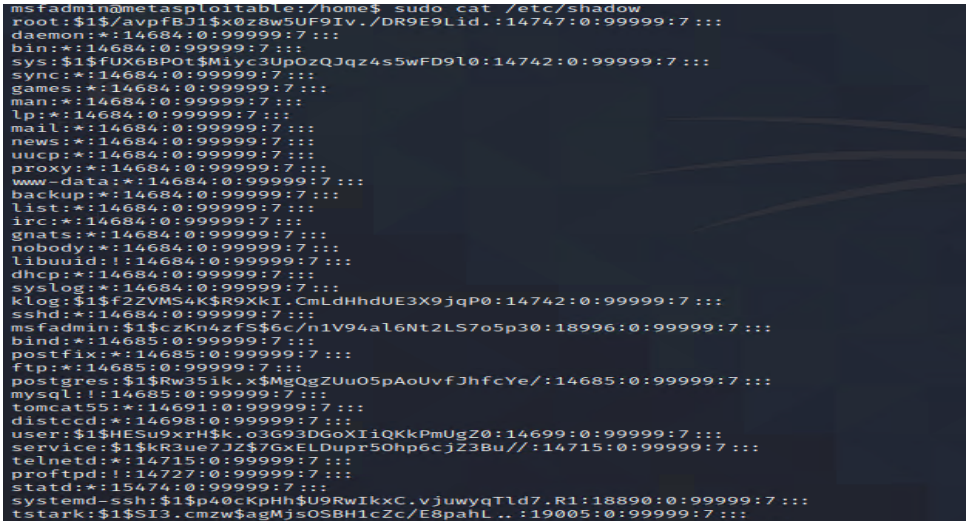


Fig.28 – The unedited etc/shadow/ file.

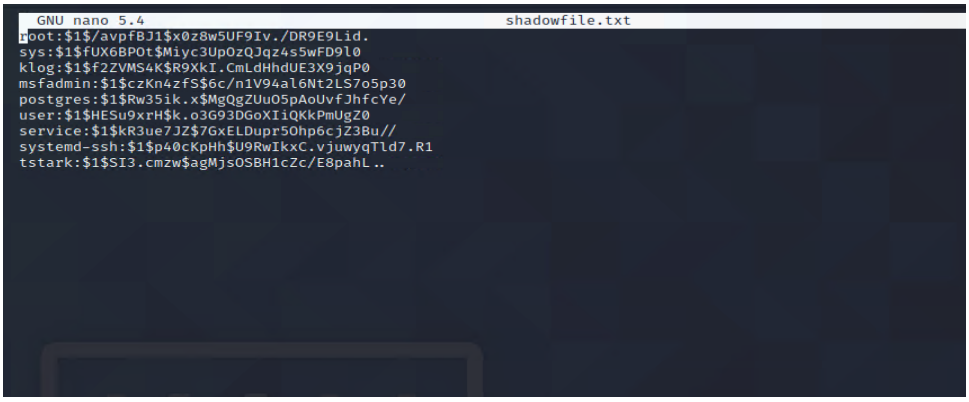


Fig.29 – Sanitized file of all users and hashed passwords.

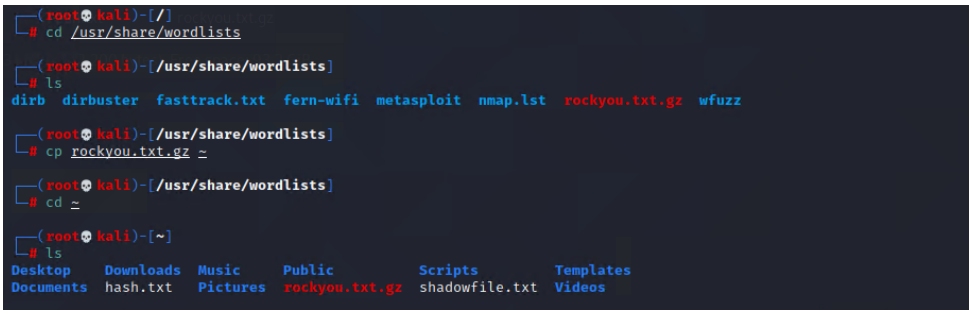


Fig.30 – Navigating to John the Ripper directory

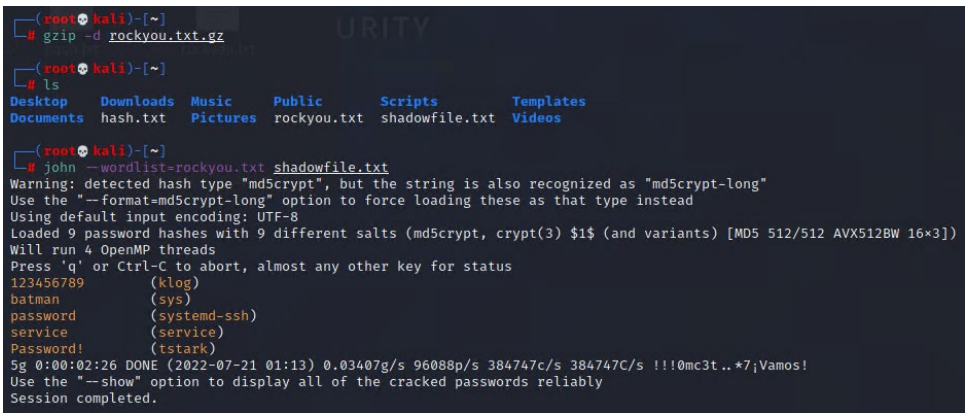


Fig.31 – John the Ripper cracked a copy of the shadow file (shadowfile.txt).

Setting up Persistence on Compromised Machine

Risk Rating: Critical

Description:
RS LLC, connected to the compromised system via SSH. Objective of this is to create a user with root access privileges and thus masked an intruder's activity. At **Fig.32** we logged back into the system and created a new account **"systemd1-ssh"** as shown at **Fig.33**. The newly created account will be used to gain access to the system without brute forcing attacks or cracking passwords.

RS LLC successfully gained access to the systems and a valid user, and this can be seen at **Fig. 34**. This will allow an intruder to traverse the company's network with very little possibility of being detected.

Affected Hosts: megacorpone.com

Remediation:

- Perform vulnerability assessments to determine accounts that can be compromised.
- Deploy a privilege access management system to manage accounts with elevated privileges.
- Configure user access policies, that will prevent all users from using their network ID to access servers. Instead expiring temporary credentials are used.
- Enable account creation and deletion logs, which are review at regular intervals.

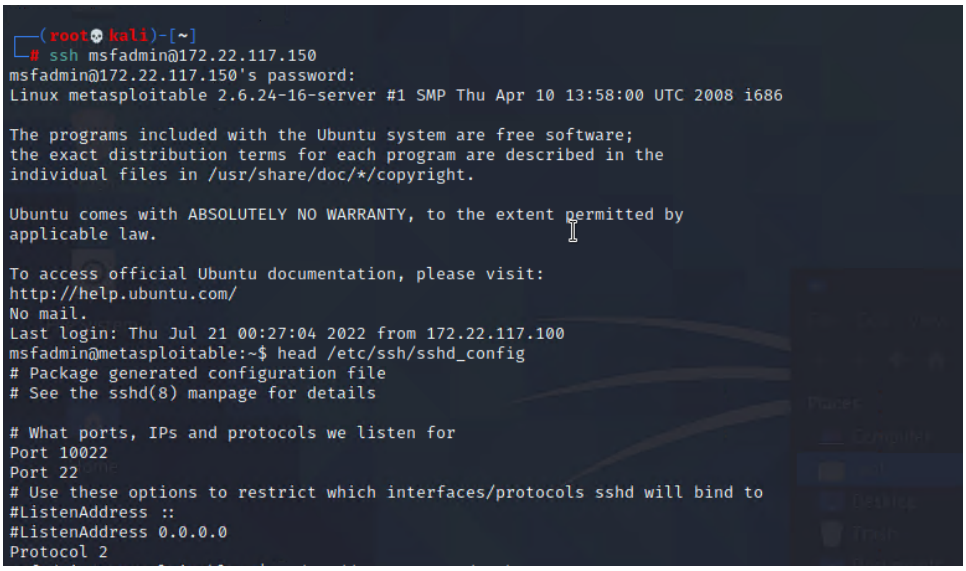


Fig.32 – SSH into compromised system

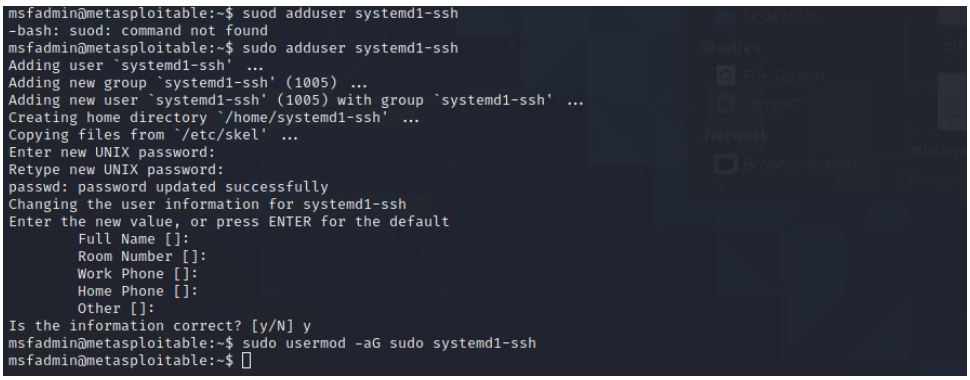


Fig.33 – Creation of an account with elevated privileges to access the system.

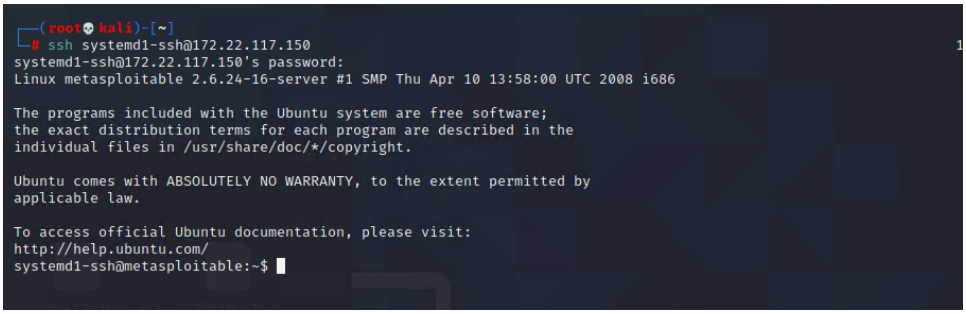


Fig.34 – Confirmation that newly created account to access system is working.

Windows Open Port

Risk Rating: High

Description:
During the reconnaissance phase of the engagement, RS LLC discovered there were two types of operating systems within the environment Linux and Windows. Moving forward we will be attempting to identify and exploit vulnerabilities within the windows environment.

The initial scan revealed there are two Windows machines as shown on **Fig.35 – Fig.36** with IP addresses and open ports. The Doman Controller (DC) is 172.22.117.10. This was easily identified primarily due to the fact it is running Kerberos requiring port 88 to authenticate. There are a total of fifteen (15) ports opened between both systems, which can become attack vectors used by a threat actor to gain access to the system\network.

Affected Hosts: megacorpone.com

Remediation:

- Close all unnecessary ports
- Regularly patch operating system for security.
- Ensure firewall rules are in place to screen traffic to the network and DC

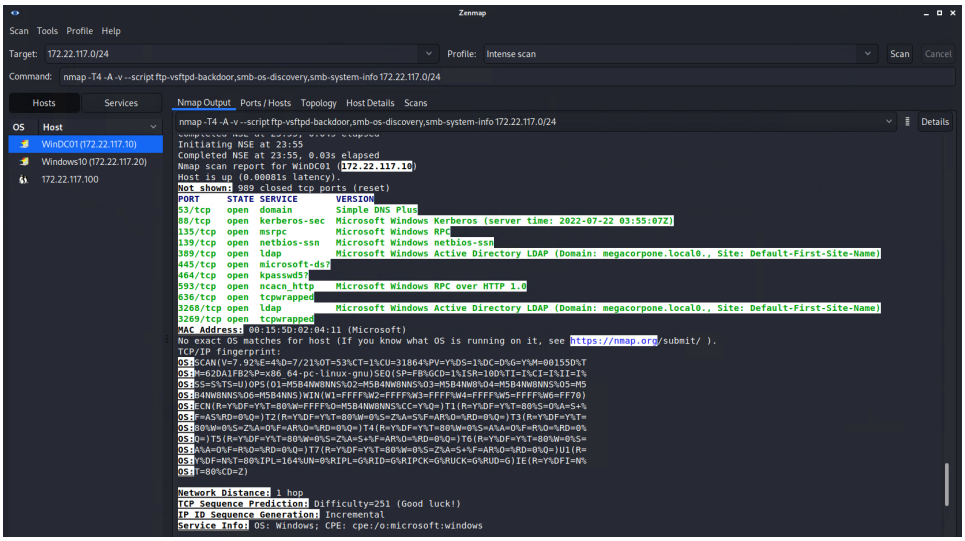


Fig.35 – This is the DC for the network

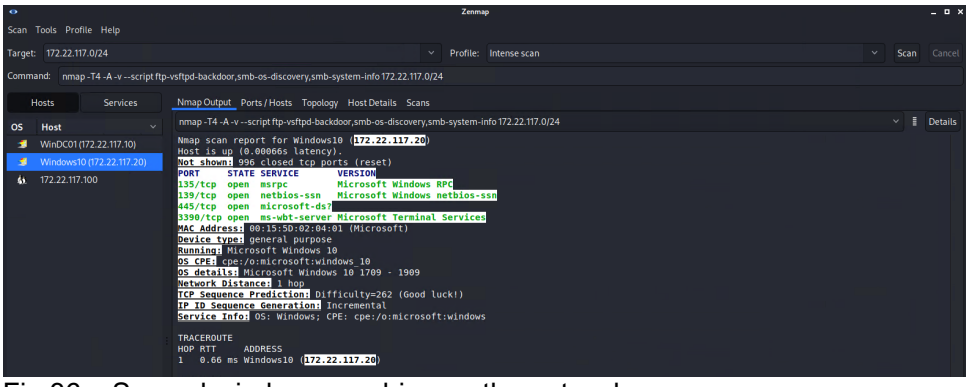


Fig.36 – Second windows machine on the network.

Vulnerability to Password Spraying

Risk Rating: **Medium**

Description:
Password Spraying is the process by which a single set of login credentials, are used against several systems to gain access. During the initial access phase of the engagement, RS LLC using John the Ripper cracked a password file and obtained several login credentials.

RS LLC used Metasploit together with **"auxiliary/scanner/smb/smb_login"** along with setting options as shown at **Fig.37 – Fig.38** to initiate the password spraying attack. At **Fig.39** the attack was successful with the following system being identified. At this point we knew the system associated to the network credentials.

Affected Hosts: megacorpone.com

Remediation:

- Set a maximum password login attempt after which the account will be locked out for a period.
- Change the default passwords for all system and web applications.
- Implement measures to detect bot activity.

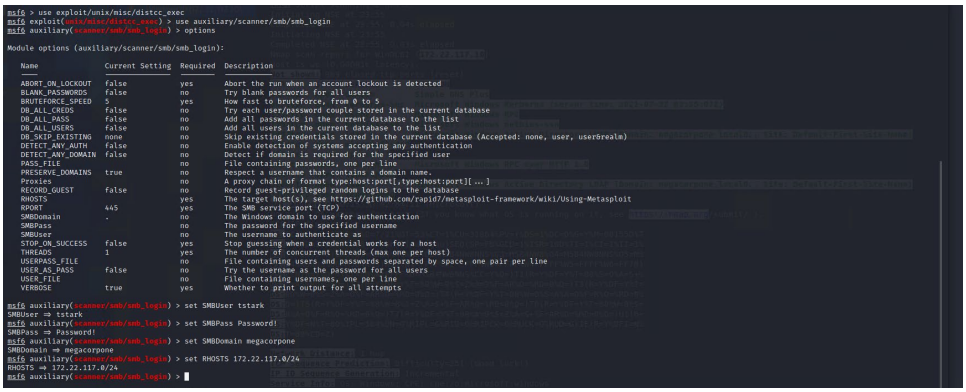


Fig.37 – Metasploit exploit used to connect login to system

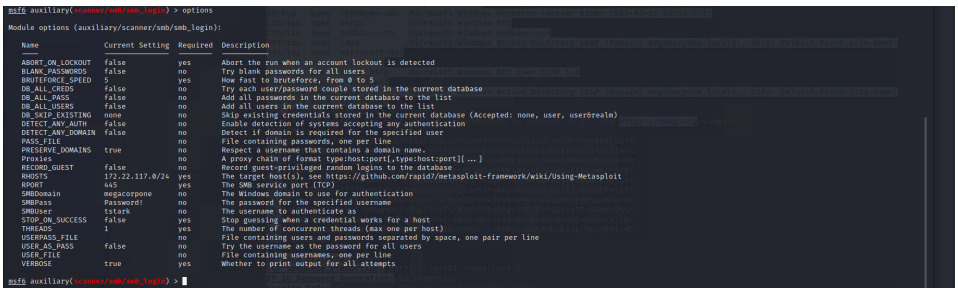


Fig.38 – Options available to narrow attack

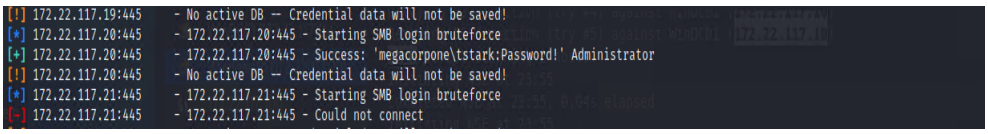


Fig.39 – Windows system found that the login credentials will work.

LLMNR Spoofing Vulnerability

Risk Rating: **Critical**

Description:
LLMNR spoofing occurs when an attacker grabs password hashes from systems off the network. RS LLC initiated a listener, spoofing password hashes as systems go through the authentication process. At **Fig.40** our attempt to grab data of the network was successful; grabbed the Client, Username and Password Hash. The hash was then moved to a text file and cracked using John the Ripper as shown at **Fig.41**. The consequence is that RS LLC was able to harvest additional valid login credentials (username: pparker - password: Spring2021) for future access.

Affected Hosts: megacorpone.com

Remediation:

- Disable the LLMNR service

Fig.40 – Listener deployed on the network waiting for an authentication process to initiate.

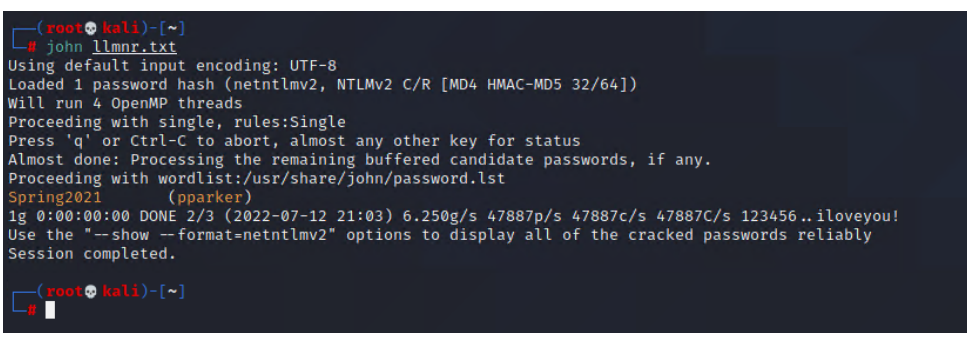


Fig.41 – Listener grabbed credential and placed into a text file to be cracked by Joh the Ripper.

Windows Management Instrumentation (WMI) Vulnerability

Risk Rating: **Medium**

Description:
Windows Management Instrumentation (WMI) is used as a Windows administrative tool but can also serve as an information gathering tool for an attacker. Using Metasploit as shown at **Fig.42** and exploit **"auxiliary/scanner/smb/impacket/wmiexec"**, RS LLC was able to retrieve the current running process as shown at **Fig.43**. The sensitive system and network data revealed at **Fig.44 – Fig.47**, provides an attacker visibility to all information processes. An attacker can then use this information to be stealthier, modify systems, achieve persistence and move laterally.

Affected Hosts: megacorpone.com

Remediation:

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

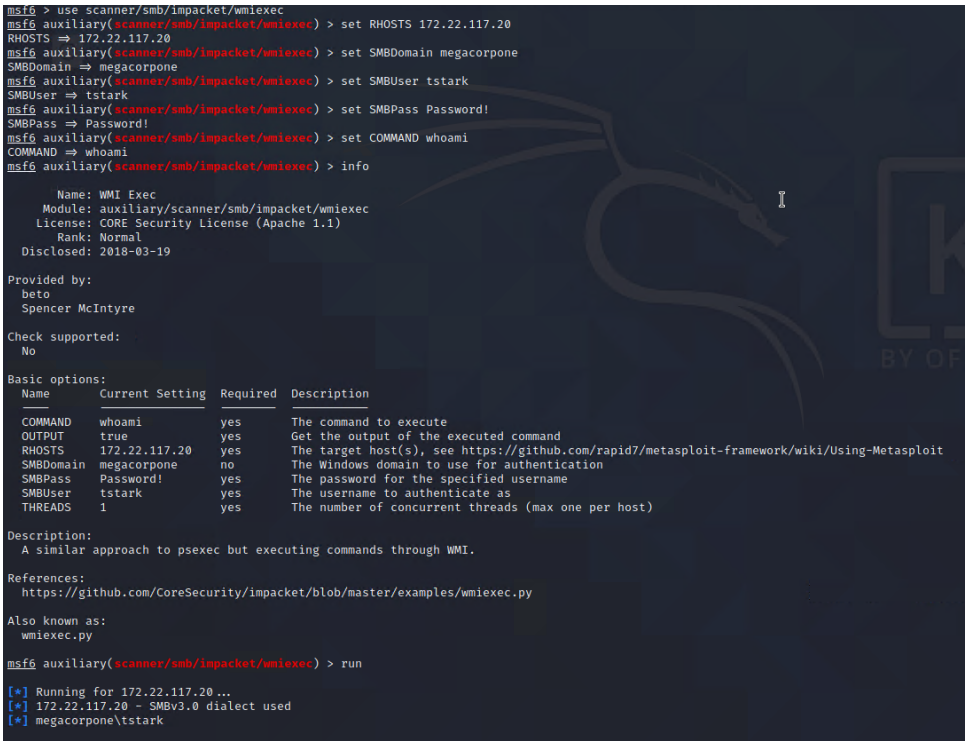


Fig.42 – Metasploit exploit used to gain access to the system

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

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        120 K
Registry                        72 Services                   0     13,584 K
smss.exe                       356 Services                   0        868 K
csrss.exe                      460 Services                   0      2,412 K
csrss.exe                      528 Console                    1      1,440 K
wininit.exe                    544 Services                   0      2,448 K
winlogon.exe                   588 Console                    1      3,464 K
services.exe                   632 Services                   0      5,640 K
lsass.exe                      672 Services                   0     13,488 K
fontdrvhost.exe                736 Console                    1        740 K
fontdrvhost.exe                744 Services                   0        952 K
svchost.exe                    808 Services                   0     11,236 K
svchost.exe                    852 Services                   0      8,200 K
LogonUI.exe                    936 Console                    1     40,812 K
svchost.exe                    968 Services                   0      8,936 K
svchost.exe                   1004 Services                   0     56,536 K
dwm.exe                        420 Console                    1     20,364 K
svchost.exe                    628 Services                   0     13,360 K
svchost.exe                   1048 Services                   0     15,676 K
svchost.exe                   1056 Services                   0     17,096 K
svchost.exe                   1064 Services                   0      4,964 K
svchost.exe                   1108 Services                   0     14,092 K
svchost.exe                   1136 Services                   0     14,092 K
svchost.exe                   1232 Services                   0      5,996 K
svchost.exe                   1360 Services                   0     12,196 K
Memory Compression            1560 Services                   0     43,440 K
VSSVC.exe                     1704 Services                   0      5,276 K
svchost.exe                   1792 Services                   0      3,808 K
svchost.exe                   1868 Services                   0      6,452 K
svchost.exe                   1948 Services                   0      3,276 K
svchost.exe                   1956 Services                   0      4,980 K
spoolsv.exe                   1604 Services                   0     11,572 K
svchost.exe                   2212 Services                   0      3,816 K
svchost.exe                   2304 Services                   0     23,876 K
MsMpEng.exe                   2328 Services                   0     80,072 K
svchost.exe                   2876 Services                   0      4,720 K
NisSrv.exe                    3184 Services                   0      8,432 K
svchost.exe                   3776 Services                   0      5,692 K
MicrosoftEdgeUpdate.exe       4064 Services                   0      3,328 K
SgrmBroker.exe                3088 Services                   0      5,560 K
uhssvc.exe                    2456 Services                   0      5,620 K
svchost.exe                   3408 Services                   0     10,100 K
svchost.exe                    552 Services                   0      8,144 K
SearchIndexer.exe             1076 Services                   0     16,056 K
svchost.exe                   2248 Services                   0      7,216 K
svchost.exe                   3884 Services                   0     15,688 K
WmiPrvSE.exe                   896 Services                   0      9,496 K
cmd.exe                        388 Services                   0      3,904 K
conhost.exe                   2196 Services                   0     11,984 K
tasklist.exe                  2228 Services                   0      8,624 K
```

Fig.43 – A list of all WMI process currently running.

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

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

Fig.44 – Windows version

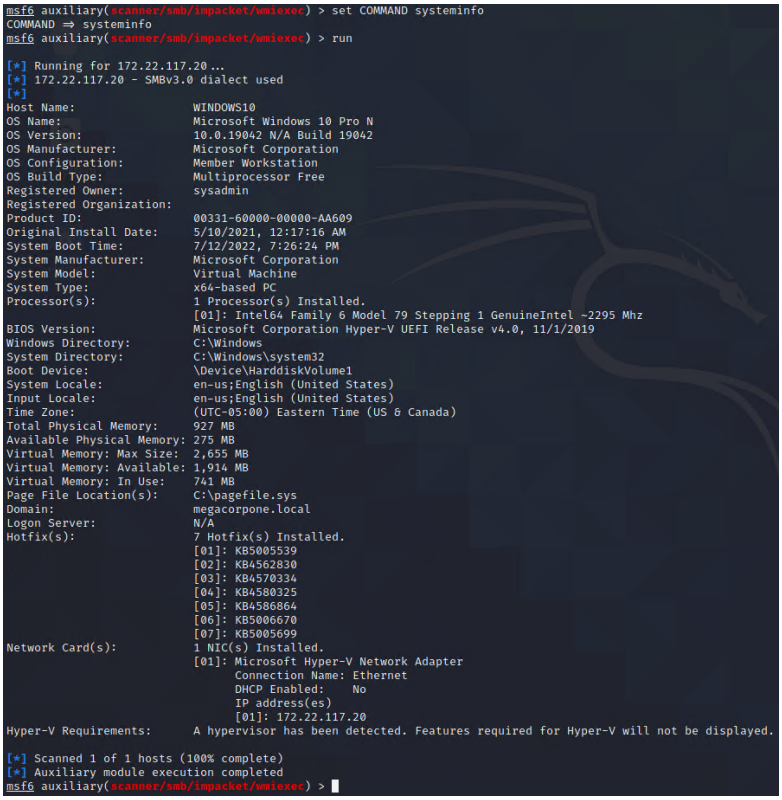


Fig.45 – Windows System Information

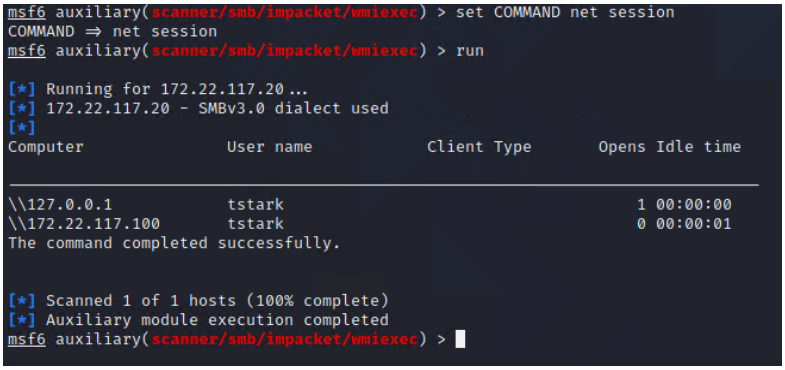


Fig.46 – Windows net session information

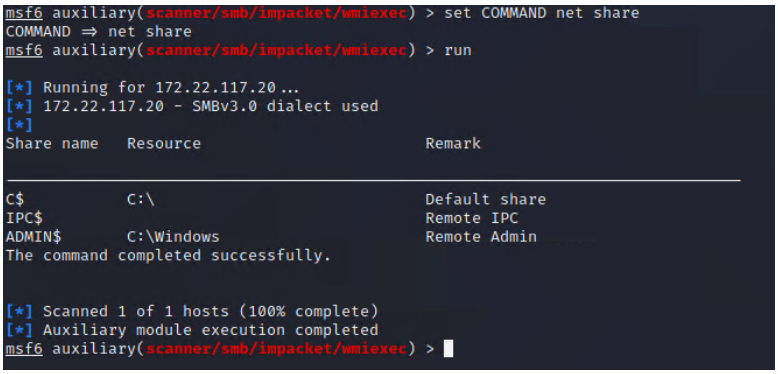


Fig.47 – Windows net share information

Reverse Shell Vulnerability

Risk Rating: High

Description:
The Reverse Shell is a crucial tool in an attacker's kit. It allows the attacker to open ports to the target machine, enabling communication and allowing for complete control of the target bypassing some firewalls. As shown at **Fig.48**, RS LLC used **"msfvenom"** to initiate a listener port for the reverse shell. Metasploit was then used with the following exploits **"exploit/multi/handler/ and payload windows/meterpreter/reverse_tcp"** creating a reverse shell on Port 4444 establishing a "meterpreter" session as shown at **Fig.49 – Fig.50**.

Affected Hosts: megacorpone.com

Remediation:

- Lock all outgoing connectivity except for specific ports and remote IP addresses needed for required services.
- Configure a proxy server as an intermediary between the external IP address and internal network.
- Remove unnecessary services, restricting the execution of reverse shell code.
- Perform scheduled patching of the web applications to limit potential vulnerabilities.

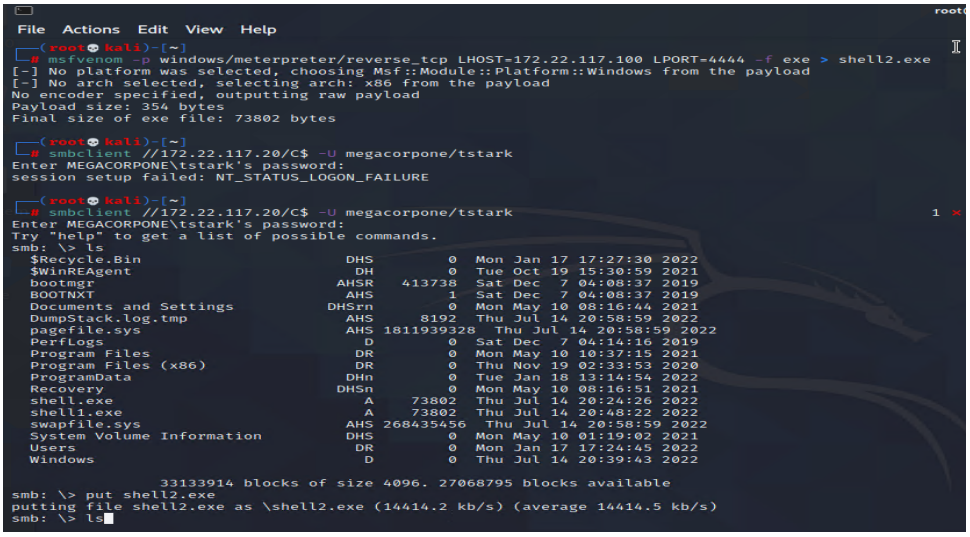


Fig.48 – Listening Port configured for communication

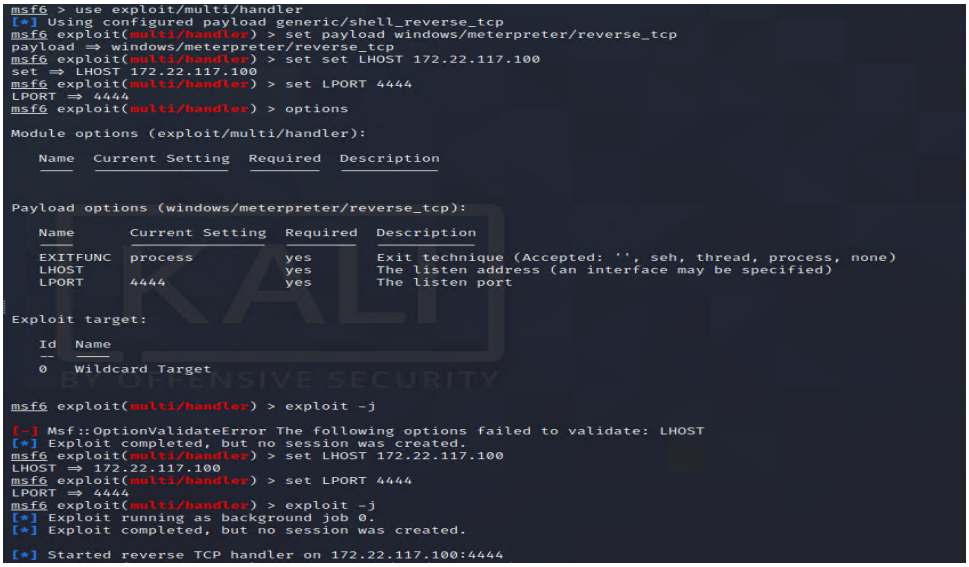


Fig.49 – Exploit initiated via the reverse TCP handler

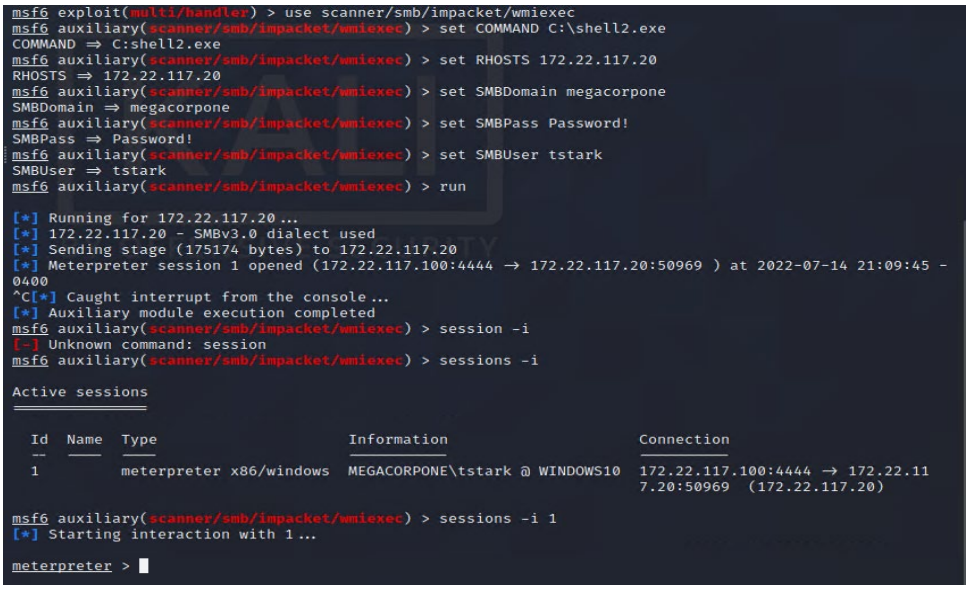


Fig.50 – Meterpreter session initiated.

Privilege Escalation Exploit & Persistence

Risk Rating: Critical

Description:
During the engagement RS LLC obtained several login accounts, however, without administrator's access. The meterpreter session previously established was "backgrounded" initiating the **"exploit/windows/local/persistence_service"**, with a persistent exploit as shown at **Fig.51 – Fig.52**. On establishing the session, the process was then migrated to an active Windows process to disguise its true nature as shown at **Fig.53 – Fig.54**.

A persistent backdoor was established into the exploited system as a shell. The task created ensures there is a consistent connection, which is re-established at 12 midnight should the process be killed as shown at **Fig.55**. The risk of a persistent threat is that once it is established, there is difficulty in detecting an intruder's presence and data can be exfiltrated from the network.

Affected Hosts: megacorpone.com

Remediation:

- Strong perimeter defenses
- Not sharing login credentials
- Security awareness training teaching employee on how to identify phishing attempts.
- Promoting safe browsing habits at work

Fig.51 – Establishing a meterpreter session

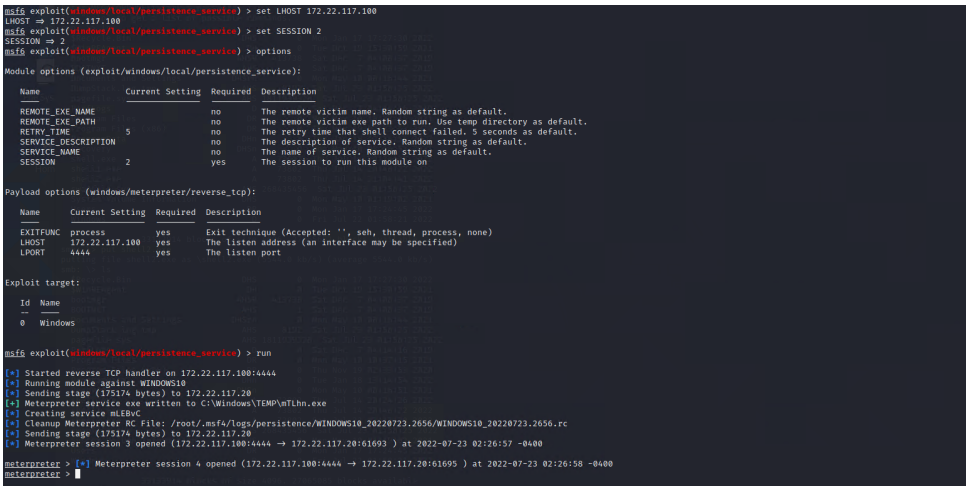


Fig.52 - Meterpreter session established

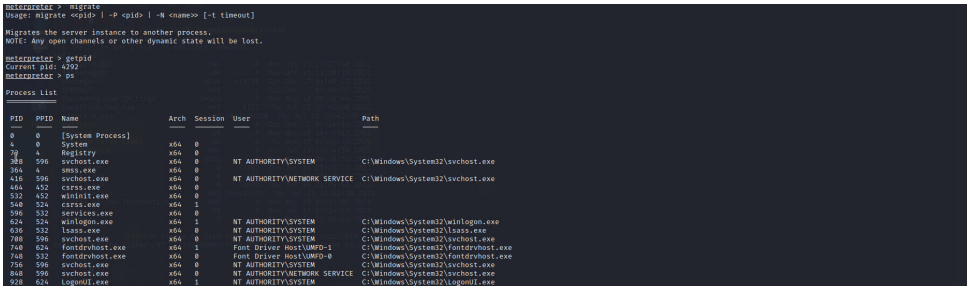


Fig.53 – Process is being migrated to blend with Windows processes

Fig.54 – Process migrated

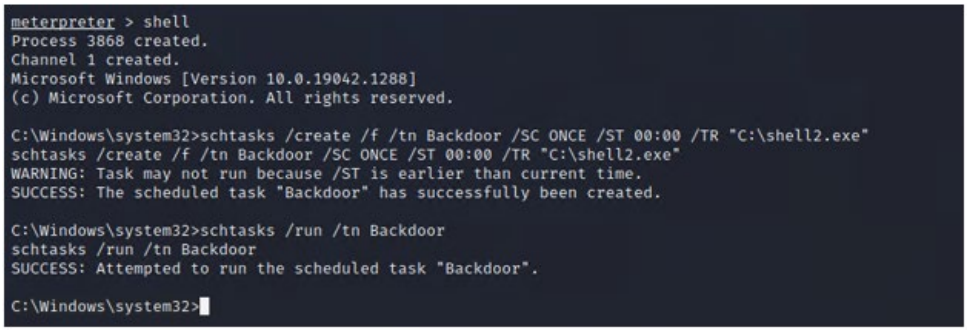


Fig.55 – Persistence established within the exploited system

Credential Dumping & Lateral Movement

Risk Rating: High

Description:
During this phase of the engagement RS LLC using Mimikatz Kiwi executed a **"kiwi_cmd lsadump::cache"** command, dumping all users residing on the Windows Domain Controller as shown at **Fig.56 – Fig.57**. The dumped credentials were echoed into **"hash.txt"** and using the John the Ripper command **"john - -format=mscash2 hash.txt"** cracked the password for the user **"bbanner"**, as shown at **Fig.58**. Lateral movement across the network is now possible as shown at **Fig.59 – Fig.60**. It is now difficult to detect it can appear to be normal network traffic. The system is now fully compromised allowing an attacker to move across the network.

Affected Hosts: megacorpone.com

Remediation:

- Update your Endpoint Security Solution
- Proactively Hunt for Advanced Threats Strong perimeter defenses
- Maintain Proper IT Hygiene by Eliminating Vulnerabilities such a Outdate or Unpatched Systems

Fig.56 – Loading kiwi to initiate credential dumping

Fig.57 – kiwi_cmd lsadump::cache dumping user credentials

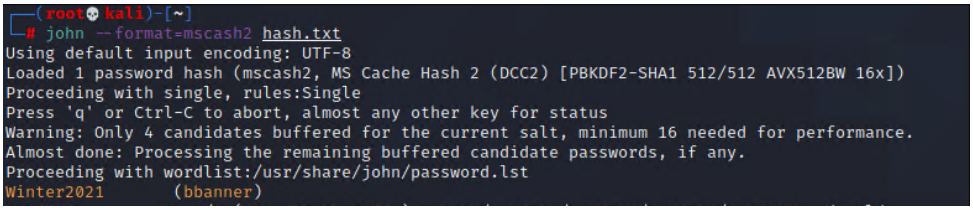


Fig.58 – "bbanner" login credentials cracked to be sued to lateral movement

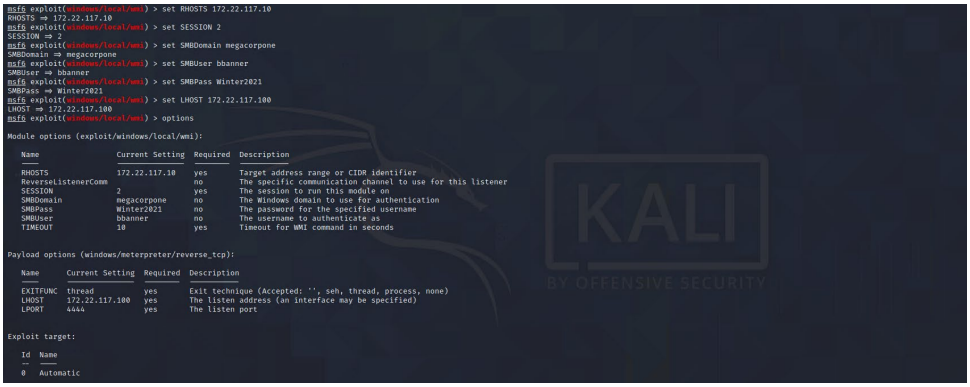


Fig.59 – Meterpreter initiated for lateral movement

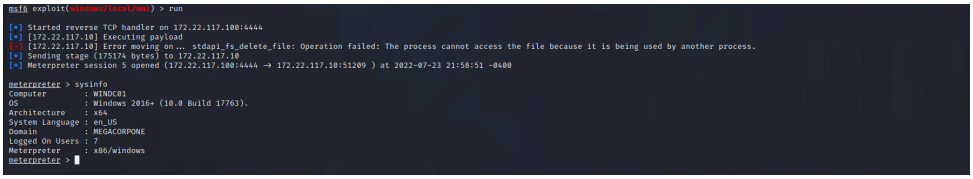


Fig.60 – Confirmation of operating from the Windows DC

Compromised Server Users

Risk Rating: **Medium**

Description:
At this finally stage of the engagement via the use of a meterpreter shell, RS LLC can now view all user accounts registered on the Domain Controller as shown at **Fig.61 – Fig.62**.

Affected Hosts: megacorpone.com

Remediation:

- Update your Endpoint Security Solution
- Proactively Hunt for Advanced Threats Strong perimeter defenses
- Maintain Proper IT Hygiene by Eliminating Vulnerabilities such a Outdate or Unpatched Systems

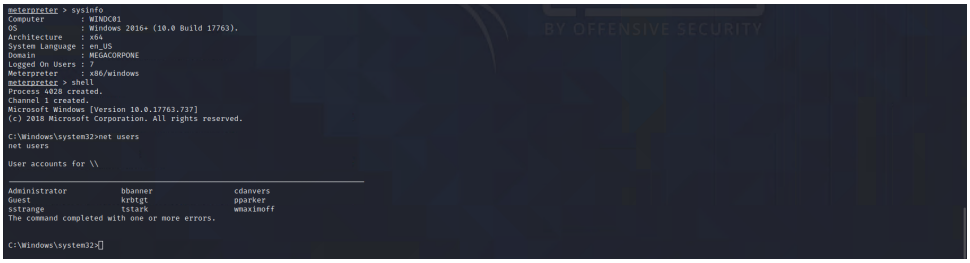


Fig.61 – All users registered on the domain controller is now accessible.

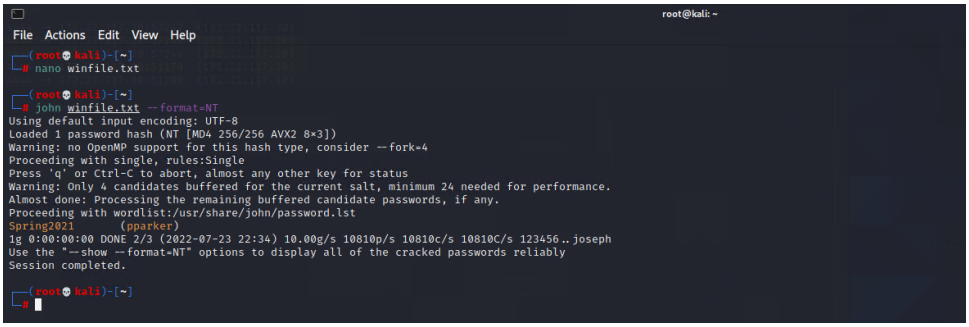


Fig.62 – The final user account was cracked

MITRE ATT&CK Navigator Map

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

Legend: Performed successfully

MITRE ATT&CK navigator map