1.

a. BadStore’s cart cookie is also an encoded string with a predictable structure

XXX:YYY:... etc., and it probably contains information it shouldn’t. Which field

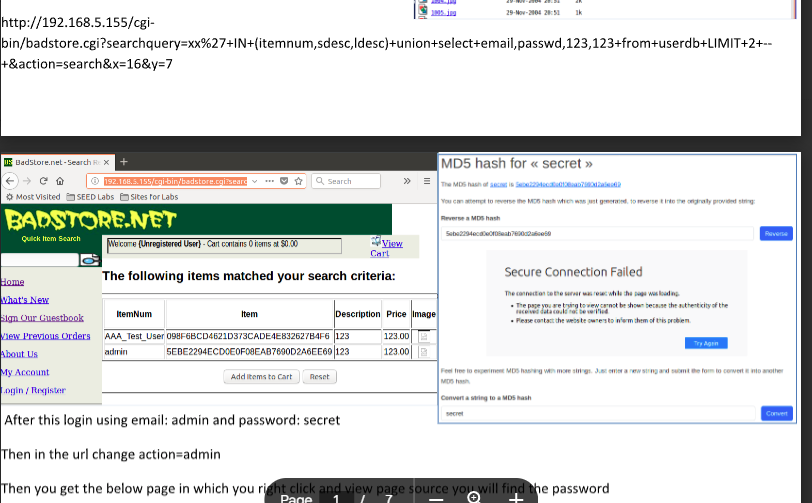
of the decoded string could an attacker change to give himself a discount on an

item’s price?

->open badstore and seed

->firefox and then login as admin

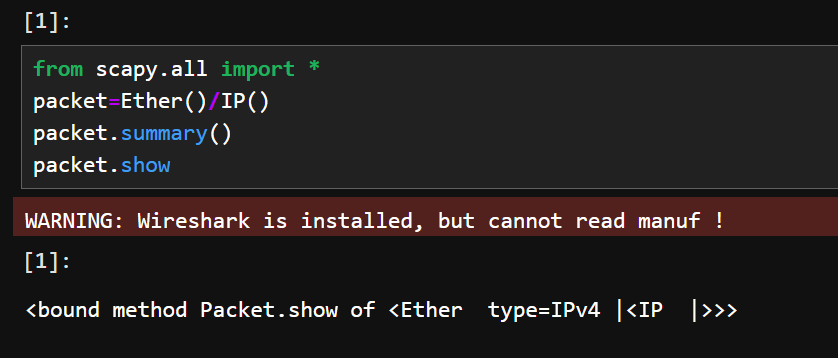
->we need to first find the password of the admin fellow



Login as supplier and then do what;’s next and then add the items to cart and next copy the card id and decode and encode it

b. Using Scapy, create a frame that consists of an Ethernet layer, with an IP layer on

top? With the show method, capture all fields of the frame.



c. Write a Shell script for port scan using NetCat.

Done in record

2.

a. Log in as joe@supplier.com to Badstore— — this is possible in a variety of ways,

including SQL injection. Then look at his previous orders and answer the

question: What credit card number did he use to make a purchase of $46.95?

Multiple answers are possible.

Once you log in as joe go to view previous orders and then get in the card numbers and decode and encode it

b. How to Sniff with Scapy (for 10 packets and show the details of all the packets).

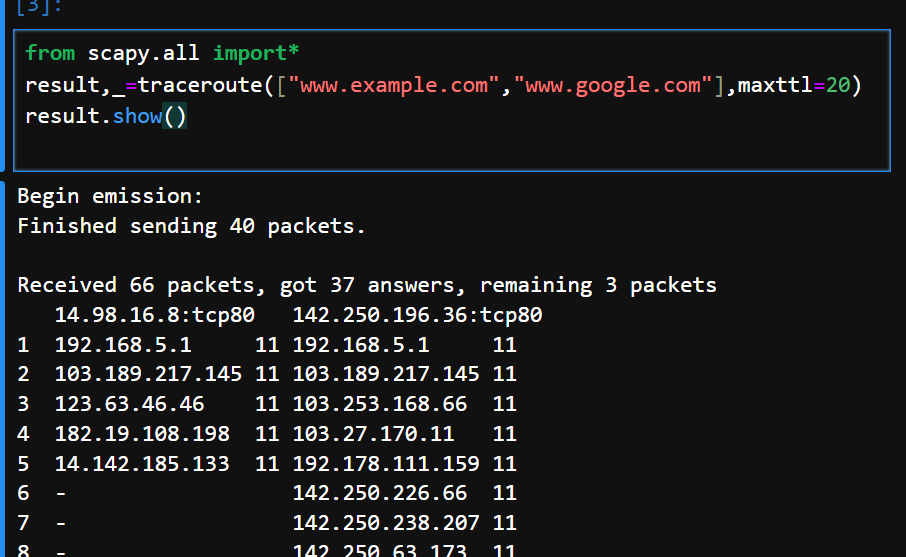
c. Using NetCat, show how to Communicate with the server using 2 terminals and

across systems

Done in record

3.

a. Demonstrate how to perform traceroute in Scapy.



b. Using NetCat, show the usage of HTML Request/Response (HEAD /GET).

Seed-> nc –lp 5000

-><http://localhost:5000>

->seed terminal and type

HTTP/1.1 200OK

Server:Nooblinux

<!doctype html>

<title>Nooblinux</title>

Content-Type:text/html

<h1>Response</h1>

->Press enter twice and then see the browser

c. Using Nmap perform Ping Scan (determine which hosts are up). Also show how

to scan a single IP.

Use nmap –sN <ip addr>

4.

a. Write a python code using Scapy for creating a Network Scanner (Hint: Create an

ARP packet using ARP() method )

from scapy.all import \*

#Define the target subnet

target\_subnet="192.168.5.0/24"

#Send ARP requests

answered,unanswered=srp(Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(pdst=target\_subnet),timeout=2,verbose=False)

for sent,recieved in answered:

print(f"Host Up:{recieved.psrc}MAC:{recieved.hwsrc}")

b. Using NetCat, show communication between browser and the server. (for plain

text)

curl one I guess

c. Using Nmap, Scan a range of IPs. Also scan an entire subnet.

>> nmap -sn 192.168.1.1-10

5.

a. Demonstrate SYN flood attack using Scapy.

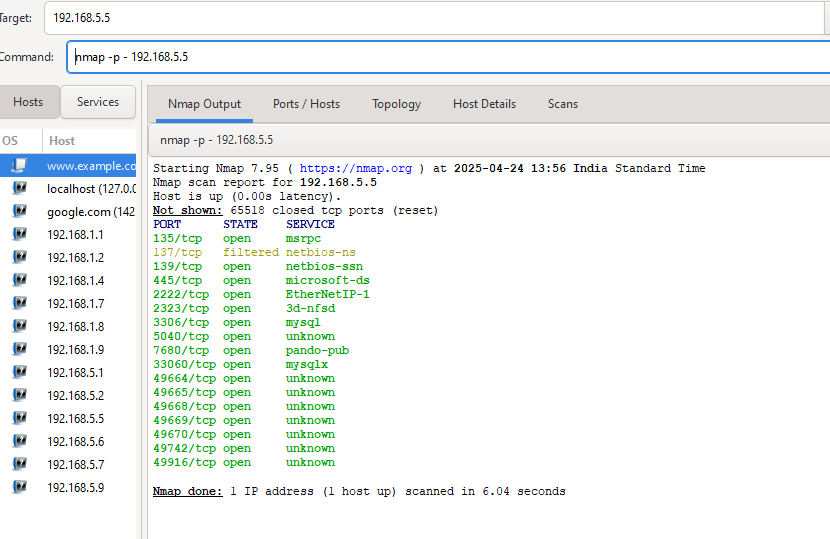
Record and the word doc

b. Using NetCat, show communication between browser and the server. (for an

image)

c. Using Nmap, Scan specific ports. Also show how to scan all 65535 ports.

nmap



6.

a. BadStore uses cookies to track the contents of the cart, once you’ve added

something to it. What is the key of the cookie used for the cart?

Key is ssoid

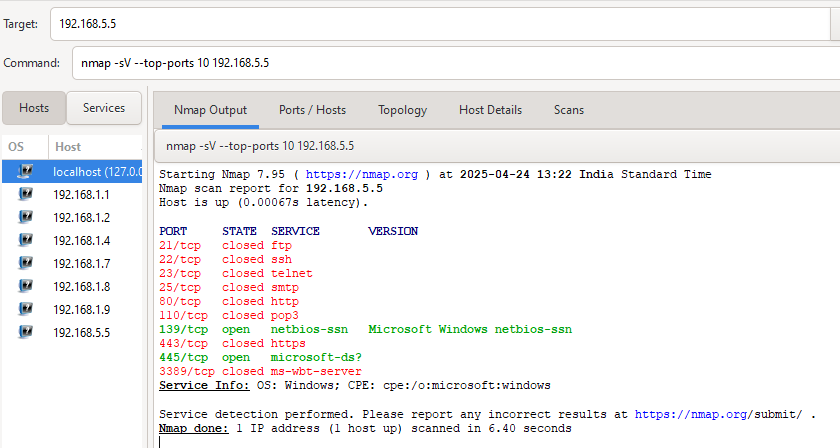
b. Write a Shell script for port scan using NetCat.

record

c. Using Nmap, scan top 1000 ports (default). Also show how to detect service

version.

nmap -sV --top-ports 1000 192.168.5.5



7.

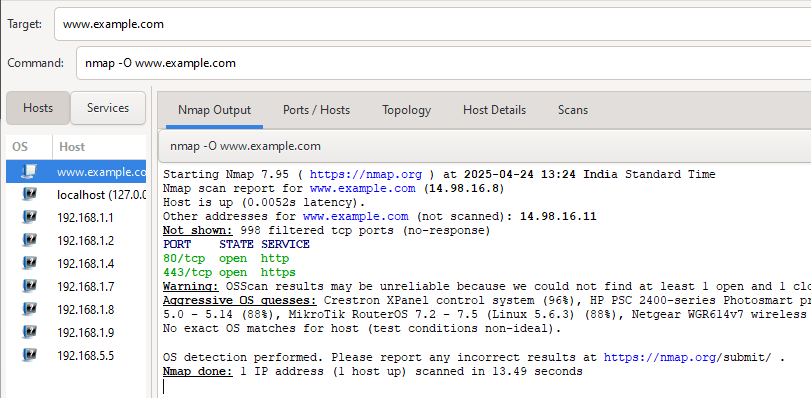
a. BadStore uses cookies to track the contents of the cart, once you’ve added

something to it. What is the key of the cookie used for the cart?

done

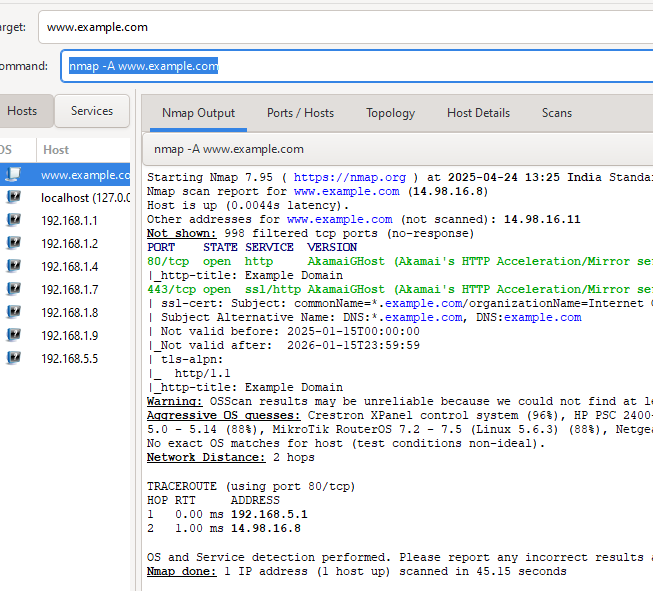
b. Using Nmap show OS detection. Also demonstrate how to perform Aggressive

scan.



nmap -A [www.example.com](http://www.example.com)

this is like a combo of p ,o,sn



c. One of the BadStore pages has a hidden form field that establishes a new user’s

privilege level. What is the name of this field?

Admin lognin ->add new user -> view page source

Type=”hidden” password

8.

a. Demonstrate how to Send ICMP packets in Scapy and show the packet captured

using Wireshark to destination 8.8.8.8.

packet=IP(dst="8.8.8.8")/ICMP()

send(packet)

#go to wireshark and apply icmp

b. Using NetCat, show communication between browser and the server (for an

image).

The image one

c. How many items for purchase are in BadStore’s database? Use SQL injection on

the quick search form field to find out.

<http://192.168.5.165/cgi-bin/badstore.cgi?searchquery=x%27+union+select+count(itemnum),count(itemnum),count(itemnum),count(itemnum)+price+from+itemdb+--+&action=search&x=11&y=9>

9.

a. Demonstrate how to Perform a Port Scan using Scapy tool on target

[www.example.com](http://www.example.com).

from scapy.all import\*

target\_ip="8.8.8.8”

ports=[22,80,443]

for port in ports:

packet=IP(dst=target\_ip)/TCP(dport=port,flags="S")

response= sr1(packet,timeout=1,verbose=0)

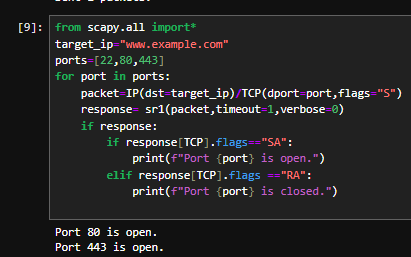
if response:

if response[TCP].flags=="SA":

print(f"Port {port} is open.")

elif response[TCP].flags =="RA":

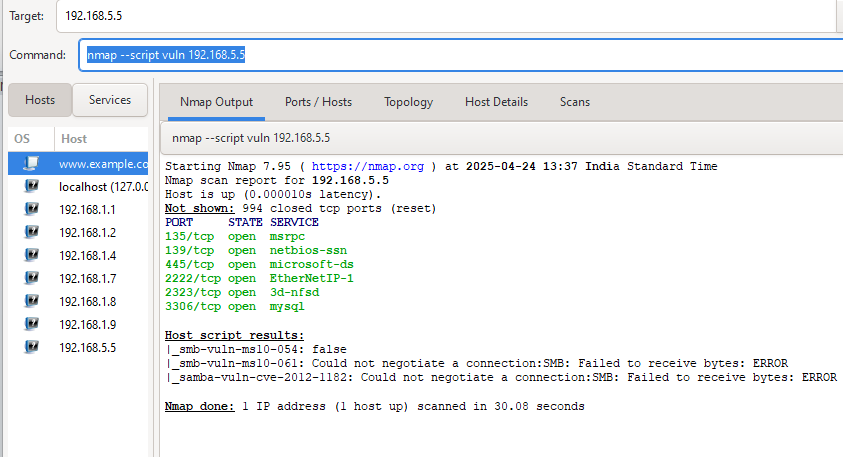
print(f"Port {port} is closed.")



b. Using Nmap, Scan for vulnerabilities. Also demonstrate how to save results to a

text file.

nmap --script vuln 192.168.5.5



c. What operations are suppliers permitted to do once they have logged into the

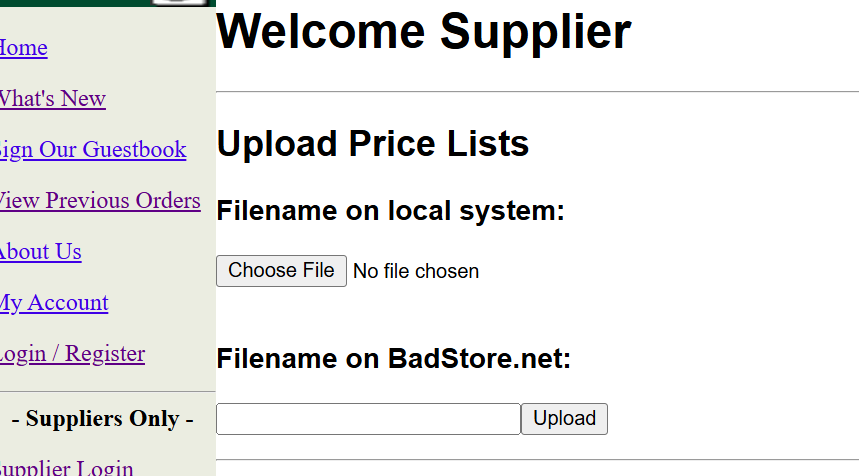
“suppliers only” area? Use SQL injection to bypass authentication, or find a way

to create an account as a supplier.

Login as supplier

Upload thing should be there

The second part here says that you need to get the password from md5 thingy



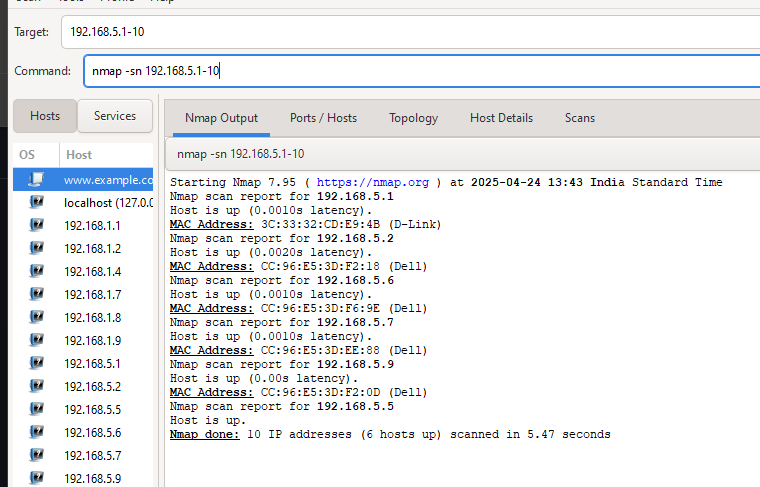
10.

a. Using NetCat, show communication between browser and the server (for an

image).

done

b. Using Nmap, Scan a range of IPs. Also scan an entire subnet.



Subnet part to be asked

c. Log in as joe@supplier.com — — this is possible in a variety of ways, including

SQL injection. Then look at his previous orders and answer the question: What

credit card number did he use to make a purchase of $46.95? Multiple answers are

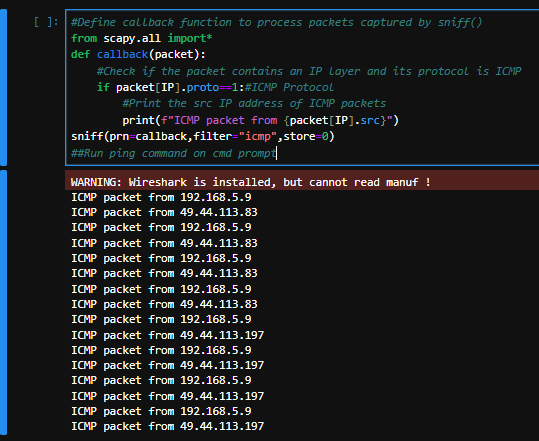
possible, but we will accept all of them.

Log in as joe ->view purchase ..

11.

a. Create a simple network monitor that watches for ICMP packets using python

function callback in Scapy.



b. Using Nmap, scan the top 1000 ports (default). Also show how to detect service

version.

done

c. Get administrator privileges and then use the admin action to look at the user

database. There are two users whose emails have the form XXX@whole.biz; what

is the XXX portion of either of the two users? For example, if one of the users is

jackie@whole.biz, the right answer is jackie. (The answer is case-sensitive.)

done

12.

a. Identify hosts that are up in a local network using Scapy (hint: ARP)

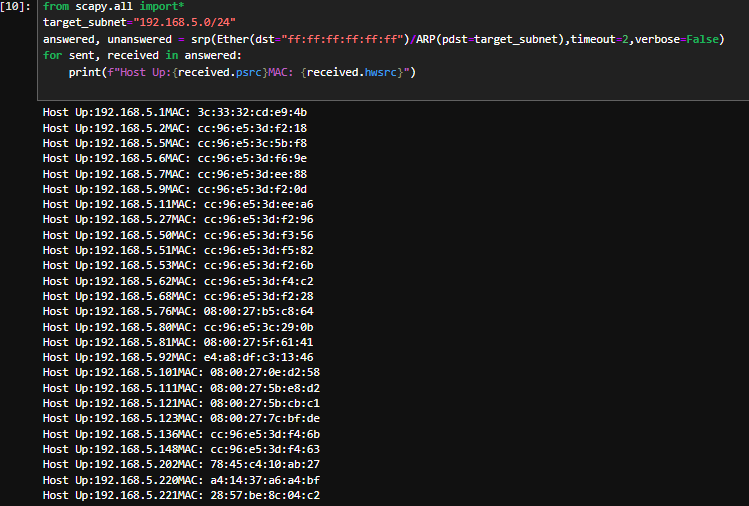
from scapy.all import\*

target\_subnet="192.168.5.0/24"

answered, unanswered = srp(Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(pdst=target\_subnet),timeout=2,verbose=False)

for sent, received in answered:

print(f"Host Up:{received.psrc}MAC: {received.hwsrc}")



b. Using NetCat show communication between browser and the server (for an

image).

done

c. BadStore uses cookies to implement a session key, once you’ve authenticated,

and for tracking the contents of the cart, once you’ve added something to it. You

can figure out the cookies in use by BadStore in various ways. What is the key of

the session cookie?

done

13.

a. Display the route and measure transit delays of packets across an IP network with

Scapy (on www.example.com, [www.google.com](http://www.google.com))

#traceroute is a common network diagnostic tool for displaying the route and measuring transit delays of packets across an IP netweok

result,\_=traceroute(["www.example.com","www.google.com"],maxttl=2)

result.show()

b. Using NetCat, show communication between browser and the server(for an

image).

done

c. BadStore uses cookies to track the contents of the cart, once you’ve added

something to it. What is the key of the cookie used for the cart?

done

14.

a. Write a scapy program to carryout SYN flooding attack.

Code and wireshark

b. BadStore’s session cookie format is poorly designed because it uses a predictable

structure. In particular, it is an encoded string (with a URL-encoded newline at

the end) of the form XXX:YYY:ZZZ:etc. Which are the fields used in the cookie?

Explain the fields in the decoded one form

c. BadStore’s cart cookie is also an encoded string with a predictable structure

XXX:YYY:... etc., and it probably contains information it shouldn’t. Which field

of the decoded string could an attacker change to give himself a discount on an

item’s price?

The price filed is the one that can be changed