O/c (2)

Roll Number:

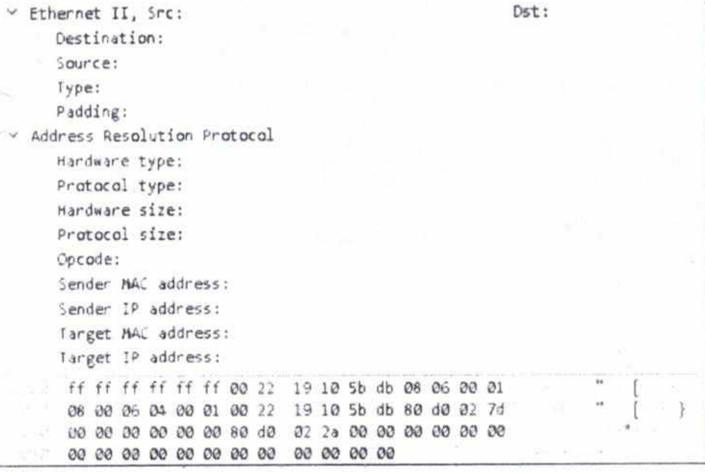
Department of Computer Science and Engineering
Thapar Institute of Engineering & Technology, Patiala

BE (3rd year) MST
Elective Focus: Cyber and Information Security
Time: 02 Hours; MM: 50

UCS534: Computer and Network Security
Dr. Maninder Singh, Dr. Ashima Anand
Oct 01, 2022

Q1.
Read the following Wireshark snippet, The "Packet Bytes" pane shows a canonical hex dump of the packet data which is shown here at the bottom of this snippet, based on your knowhow of packet bytes fill in the requisite fields on the "Packet Details Pane"

Src: Dst: Destination: Source: Type: Padding: for Ethernet II and Hardware type: Protocol type: Hardware size: Protocol size: Opcode: Sender MAC address: Sender IP address: Target MAC address: Target IP address: for Address Resolution Protocol



```
˅ Ethernet II, Src:                              Dst:
    Destination:
    Source:
    Type:
    Padding:
˅ Address Resolution Protocol
    Hardware type:
    Protocol type:
    Hardware size:
    Protocol size:
    Opcode:
    Sender MAC address:
    Sender IP address:
    Target MAC address:
    Target IP address:
   ff ff ff ff ff ff 00 22  19 10 5b db 08 06 00 01         "    [
   08 00 06 04 00 01 00 22  19 10 5b db 80 d0 02 7d         "    [    }
   00 00 00 00 00 00 80 d0  02 2a 00 00 00 00 00 00        *
   00 00 00 00 00 00 00 00  00 00 00 00
```

Q2.

i) We run "nc -l 7070" on Machine 1 (IP address is 10.0.2.6), and we then type following commands on Machine 2. Describe what is going to happen?

```
$ /bin/cat < /dev/tcp/10.0.2.6/7070 >&0
$ /bin/cat < /dev/tcp/10.0.2.6/7070 >&1
```

ii) Please describe how you would do the following: run the /bin/cat program on Machine 1; the program takes its input from Machine 2 and print out its output to Machine 3 (clearly mention where netcat will run and why)

iii) For the Shellshock vulnerability to be exploitable, two conditions need to be satisfied, what are these two conditions?

iv) Write a Bash function definition that tries to exploit the Shellshock vulnerability.

v) Instead of putting an extra shell command after a function definition, we put it at the beginning (see the following example). We then run Bash, which is vulnerable to the Shellshock attack. Will the shell command echo world be executed? Explain 'yes' or 'no'.

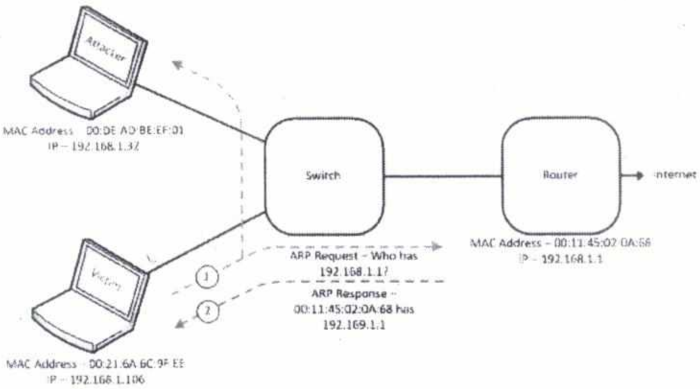
```
$ export foo='echo world; () { echo hello;}'
$ bash
```

Q3. Study the given topology and show

i) Application, Transport, Network and Data Link layer Protocol Data Units (PDUs) when Victim machine is surfing web and has opened web page www.thapar.edu mapped to (14.139.100.100).

ii) Show output generated by netstat –an on victim machine and www.thapar.edu command in this context.

iii) Initial ARP cache entries of Victim Machine & Router.


Attacker
MAC Address 00:DE AD:BE:EF:01
IP – 192.168.1.32
Switch
Router
internet
MAC Address – 00:11:45:02:0A:68
IP – 192.168.1.1
ARP Request – Who has 192.168.1.1?
1
ARP Response – 00:11:45:02:0A:68 has 192.169.1.1
2
Victim
MAC Address – 00:21:6A:6C:9F:EE
IP – 192.168.1.106

iv) ARP entries of Victim Machine & Router after attacker successfully performed ARP Man in the Middle (MITM) attack.

Q4. Consider a PHP program running as Apache module, and a CGI program.

```
-----------------------------------
The PHP program (test.php):
<?php
system("/bin/ls -l")
?>
-----------------------------------
The CGI program (test.cgi):
#!/bin/sh
/bin/ls -l
```

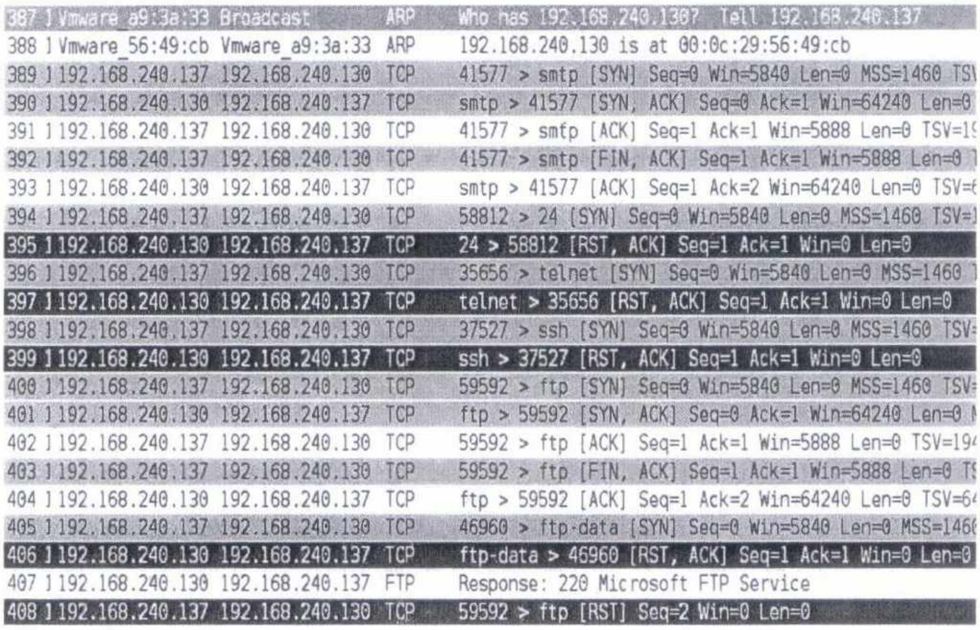
Both programs invoke /bin/ls command in a new shell process (/bin/sh points to /bin/bash). If the programs are invoked as the following, please explain the difference in effect of the Shellshock vulnerability on these two cases. What conditions are necessary to exploit shellshock in either case?

```
$ curl -A "() { echo hello; }; echo world;"
http://localhost/test.php
```

```
$ curl -A "() { echo hello; }; echo world;"
http://localhost/test.cgi
```

P.T.O

Q5. a) Study following data captured by Wireshark and answer:



```
387 1 Vmware_a9:3a:33 Broadcast       ARP   Who has 192.168.240.130?  Tell 192.168.240.137
388 1 Vmware_56:49:cb Vmware_a9:3a:33 ARP   192.168.240.130 is at 00:0c:29:56:49:cb
389 1 192.168.240.137 192.168.240.130 TCP   41577 > smtp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TS
390 1 192.168.240.130 192.168.240.137 TCP   smtp > 41577 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
391 1 192.168.240.137 192.168.240.130 TCP   41577 > smtp [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=1
392 1 192.168.240.137 192.168.240.130 TCP   41577 > smtp [FIN, ACK] Seq=1 Ack=1 Win=5888 Len=0
393 1 192.168.240.130 192.168.240.137 TCP   smtp > 41577 [ACK] Seq=1 Ack=2 Win=64240 Len=0 TSV=
394 1 192.168.240.137 192.168.240.130 TCP   58812 > 24 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=
395 1 192.168.240.130 192.168.240.137 TCP   24 > 58812 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
396 1 192.168.240.137 192.168.240.130 TCP   35656 > telnet [SYN] Seq=0 Win=5840 Len=0 MSS=1460
397 1 192.168.240.130 192.168.240.137 TCP   telnet > 35656 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
398 1 192.168.240.137 192.168.240.130 TCP   37527 > ssh [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=
399 1 192.168.240.130 192.168.240.137 TCP   ssh > 37527 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
400 1 192.168.240.137 192.168.240.130 TCP   59592 > ftp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=
401 1 192.168.240.130 192.168.240.137 TCP   ftp > 59592 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
402 1 192.168.240.137 192.168.240.130 TCP   59592 > ftp [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSV=19
403 1 192.168.240.137 192.168.240.130 TCP   59592 > ftp [FIN, ACK] Seq=1 Ack=1 Win=5888 Len=0 T
404 1 192.168.240.130 192.168.240.137 TCP   ftp > 59592 [ACK] Seq=1 Ack=2 Win=64240 Len=0 TSV=6
405 1 192.168.240.137 192.168.240.130 TCP   46960 > ftp-data [SYN] Seq=0 Win=5840 Len=0 MSS=146
406 1 192.168.240.130 192.168.240.137 TCP   ftp-data > 46960 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
407 1 192.168.240.130 192.168.240.137 FTP   Response: 220 Microsoft FTP Service
408 1 192.168.240.137 192.168.240.130 TCP   59592 > ftp [RST] Seq=2 Win=0 Len=0
```

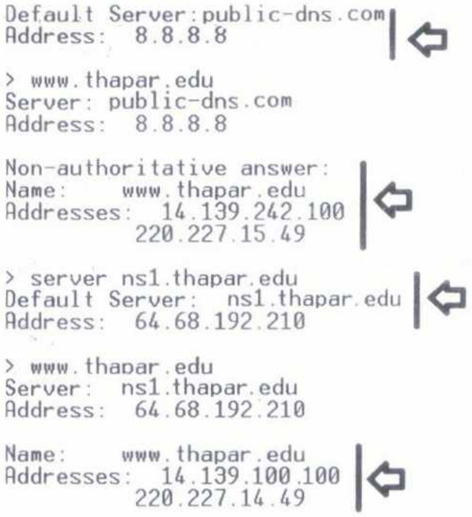
i) Explain role being performed by hosts 192.168.240.137 & 192.168.240.130

ii) What is being performed within frame range (389-408), elaborate line by line?

iii) Significance of 387-388 frames.

b)

Study the output generated by **"nslookup"** program {given on the right-hand side} while user was connected to the Internet, Give technical comments on the highlighted parts. Emphasis should be on DNS-poisoning concept.



```
Default Server:public-dns.com
Address:  8.8.8.8

> www.thapar.edu
Server: public-dns.com
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.thapar.edu
Addresses:  14.139.242.100
          220.227.15.49

> server ns1.thapar.edu
Default Server:  ns1.thapar.edu
Address:  64.68.192.210

> www.thapar.edu
Server:  ns1.thapar.edu
Address:  64.68.192.210

Name:    www.thapar.edu
Addresses:  14.139.100.100
          220.227.14.49
```