F107

1

Roll Number:

Thapar Institute of Engineering and Technology

Department of Computer Science and Engineering

B.E. CoE 3rd year EST UCS534: Computer and Network Security

Time: 02 Hours; MM: 50 Name of Faculty: Dr. Maninder Singh/Dipto Barman

Note: **1.** Attempt all Questions in a sequence. **2.** Start each question (but not each part of a question) on a new page. **3.** Attempt 5 out of 7 questions. **4.** All questions carry equal marks.

Q1. Stack buffer overflow bugs are caused when a program writes more data to a buffer located on the stack than what is actually allocated for that buffer. Study the following C code and draw program stack in foo() with various inputs:

i) before data is copied

ii) "hello" is provided as command line argument

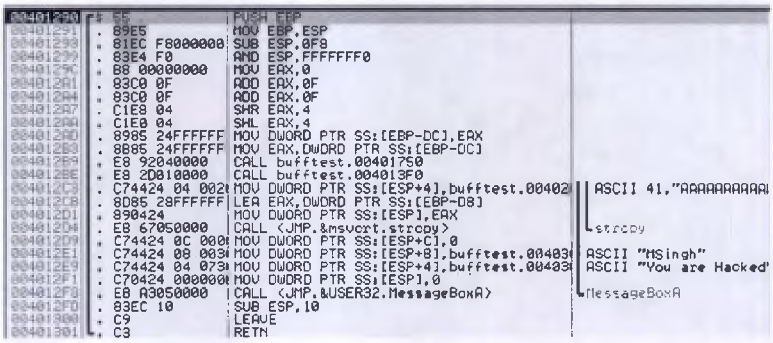
iii) AAAAAAAAAAAAAAAAAAA\x0A\xAF\xD8\x77 is provided as command line argument.

```
#include <string.h>
 void foo (char *bar)
{
  char  c[12];
  strcpy(c, bar);

 int main (int argc, char **argv)
{
  foo(argv[1]);
}
```

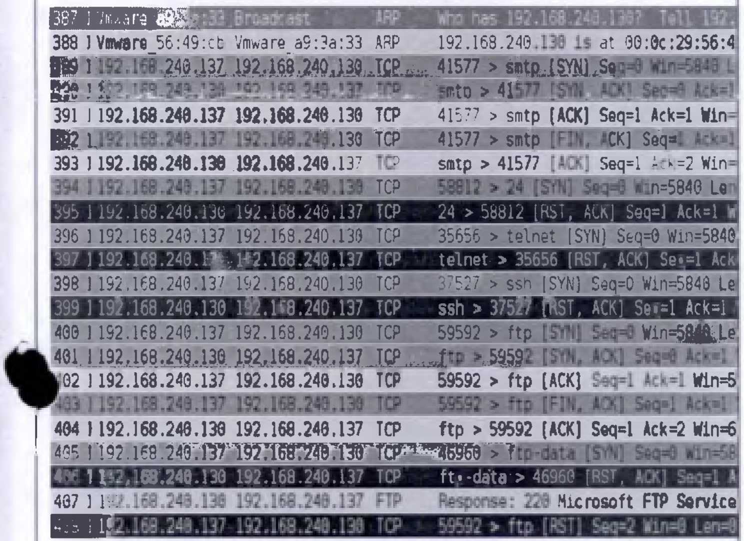
iv) What does \x0A\xAF\xD8\x77 indicates? What happens when EIP is filled with this address?

v) Study the following Ollydbg output and explain calls to strcpy and MessageBoxA functions.



```
00401290 r$ 55              PUSH EBP
00401291 .  89E5            MOV EBP,ESP
00401293 .  81EC F8000000   SUB ESP,0F8
00401299 .  83E4 F0         AND ESP,FFFFFFF0
0040129C .  B8 00000000     MOV EAX,0
004012A1 .  83C0 0F         ADD EAX,0F
004012A4 .  83C0 0F         ADD EAX,0F
004012A7 .  C1E8 04         SHR EAX,4
004012AA .  C1E0 04         SHL EAX,4
004012AD .  8985 24FFFFFF   MOV DWORD PTR SS:[EBP-DC],EAX
004012B3 .  8B85 24FFFFFF   MOV EAX,DWORD PTR SS:[EBP-DC]
004012B9 .  E8 92040000     CALL bufftest.00401750
004012BE .  E8 2D010000     CALL bufftest.004013F0
004012C3 .  C74424 04 002   MOV DWORD PTR SS:[ESP+4],bufftest.00402  ASCII 41,"AAAAAAAAAA
004012CB .  8D85 28FFFFFF   LEA EAX,DWORD PTR SS:[EBP-D8]
004012D1 .  890424          MOV DWORD PTR SS:[ESP],EAX
004012D4 .  E8 67050000     CALL <JMP.&msvcrt.strcpy>                strcpy
004012D9 .  C74424 0C 000   MOV DWORD PTR SS:[ESP+C],0
004012E1 .  C74424 08 003   MOV DWORD PTR SS:[ESP+8],bufftest.00403  ASCII "MSingh"
004012E9 .  C74424 04 073   MOV DWORD PTR SS:[ESP+4],bufftest.00403  ASCII "You are Hacked'
004012F1 .  C70424 000000   MOV DWORD PTR SS:[ESP],0
004012F8 .  E8 A3050000     CALL <JMP.&USER32.MessageBoxA>           MessageBoxA
004012FD .  83EC 10         SUB ESP,10
00401300 .  C9              LEAVE
00401301 L. C3              RETN
```

Q2. Study following data captured by Wireshark and answer:



```
387 ] Vmware_a9:3a:33 Broadcast       ARP  Who has 192.168.240.130?  Tell 192.
388 ] Vmware_56:49:cb Vmware_a9:3a:33 ARP  192.168.240.130 is at 00:0c:29:56:4
389 ] 192.168.240.137 192.168.240.130 TCP  41577 > smtp [SYN] Seq=0 Win=5840 L
390 ] 192.168.240.130 192.168.240.137 TCP  smtp > 41577 [SYN, ACK] Seq=0 Ack=1
391 ] 192.168.240.137 192.168.240.130 TCP  41577 > smtp [ACK] Seq=1 Ack=1 Win=
392 ] 192.168.240.137 192.168.240.130 TCP  41577 > smtp [FIN, ACK] Seq=1 Ack=1
393 ] 192.168.240.130 192.168.240.137 TCP  smtp > 41577 [ACK] Seq=1 Ack=2 Win=
394 ] 192.168.240.137 192.168.240.130 TCP  58812 > 24 [SYN] Seq=0 Win=5840 Len
395 ] 192.168.240.130 192.168.240.137 TCP  24 > 58812 [RST, ACK] Seq=1 Ack=1 W
396 ] 192.168.240.137 192.168.240.130 TCP  35656 > telnet [SYN] Seq=0 Win=5840
397 ] 192.168.240.130 192.168.240.137 TCP  telnet > 35656 [RST, ACK] Seq=1 Ack
398 ] 192.168.240.137 192.168.240.130 TCP  37527 > ssh [SYN] Seq=0 Win=5840 Le
399 ] 192.168.240.130 192.168.240.137 TCP  ssh > 37527 [RST, ACK] Seq=1 Ack=1
400 ] 192.168.240.137 192.168.240.130 TCP  59592 > ftp [SYN] Seq=0 Win=5840 Le
401 ] 192.168.240.130 192.168.240.137 TCP  ftp > 59592 [SYN, ACK] Seq=0 Ack=1
402 ] 192.168.240.137 192.168.240.130 TCP  59592 > ftp [ACK] Seq=1 Ack=1 Win=5
403 ] 192.168.240.137 192.168.240.130 TCP  59592 > ftp [FIN, ACK] Seq=1 Ack=1
404 ] 192.168.240.130 192.168.240.137 TCP  ftp > 59592 [ACK] Seq=1 Ack=2 Win=6
405 ] 192.168.240.137 192.168.240.130 TCP  46960 > ftp-data [SYN] Seq=0 Win=58
406 ] 192.168.240.130 192.168.240.137 TCP  ftp-data > 46960 [RST, ACK] Seq=1 A
407 ] 192.168.240.130 192.168.240.137 FTP  Response: 220 Microsoft FTP Service
408 ] 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.

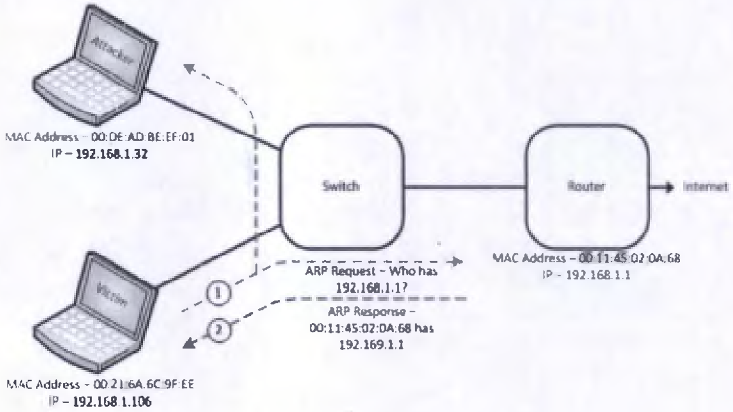
Q3. Study the given topology and show

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 command in this context.

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

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


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
1
ARP Request – Who has 192.168.1.1?
2
ARP Response – 00:11:45:02:0A:68 has 192.169.1.1
Victim
MAC Address – 00:21:6A:6C:9F:EE
IP – 192.168.1.106

Q4.

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

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

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.

Q5.

i) What are the benefits of stateful firewalls that support connection-based firewall rules? Please use examples to illustrate the benefit.

ii) The UDP and ICMP protocols are not connection-based protocols, how do firewalls know whether a UDP or ICMP packet is part of an existing "connection"?

iii) Add a rule in iptables to accept packets from a trusted network 192.168.10.0/2

iv) A machine has an IP address 10.0.20.5. On this machine, you need to block incoming connections to its ports 22, 23, 80, and 443. What will you do?

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

iv) 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?

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

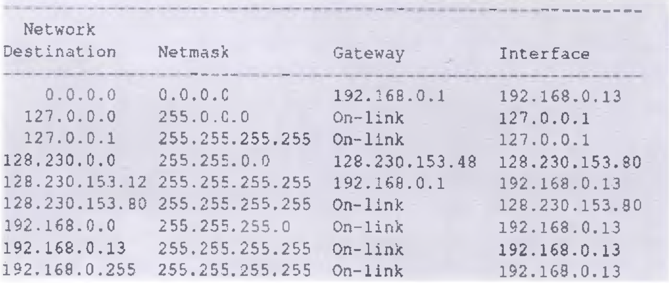
v) For the Shellshock vulnerability to be exploitable, two conditions need to be satisfied, What are these two conditions?

v) A TCP server is running on a remote machine called sirius using "nc -lv 9090". This machine is on a planet outside the Solar system. An alien named Alice living on the Earth wants to communicate with the TCP server on sirius, but unfortunately, Earth has a firewall that prevents all computers on the Earth from accessing any machine outside the Solar system. Alice does have a computer on Mars, which does not have such a restrict firewall rule. Alice's computer on Mars is called mars, and her account name is called alien. (1) Please describe how Alice can use an SSH tunnel to bypass Earth's firewall, so she can talk to sirius. (2) Without the firewall, if Alice wants to communicate with the TCP server on sirius, she can use the "nc sirius 9090" command. Now, with the SSH tunnel and the Firewall, what command should Alive run to access the server?

Q6.

i) What are the main differences between SSH tunnel and VPN tunnel?

ii) To log into TIET network, Bob needs to use a TLS-based VPN. After he has established a VPN tunnel between his machine and TIET network (128.230.0.0/16), he checks the routing table on his computer. Here is what routing table shows:



```
------------------------------------------------------------------
  Network
Destination     Netmask          Gateway         Interface
------------------------------------------------------------------
    0.0.0.0     0.0.0.C          192.168.0.1     192.168.0.13
  127.0.0.0     255.0.C.0        On-link         127.0.0.1
  127.0.0.1     255.255.255.255  On-link         127.0.0.1
128.230.0.0     255.255.0.0      128.230.153.48  128.230.153.80
128.230.153.12  255.255.255.255  192.168.0.1     192.168.0.13
128.230.153.80  255.255.255.255  On-link         128.230.153.80
192.168.0.0     255.255.255.0    On-link         192.168.0.13
192.168.0.13    255.255.255.255  On-link         192.168.0.13
192.168.0.255   255.255.255.255  On-link         192.168.0.13
```

From the above routing information, please answer the following questions (you need to explain your answer).

(a) What is the IP address of the TUN interface on Bob's machine?

(b) What is the IP address of TIET's VPN server?

(c) What is the computer's real IP address, i.e., the IP address assigned to the machine's physical network interface card?

(d) Assume that Bob is behind a firewall that blocks him from accessing a web site (assume that the IP address of the web site is 8.8.8.8). Please describe how Bob can use TIET's VPN to bypass the firewall. If changes need to be made to this routing table, please show exactly what changes Bob needs to make?

iii) When we use VPN to reach Facebook, which is blocked by our firewall, we route our Facebook-bound packets towards the TUN interface to reach the VPN server via the tunnel. The VPN server will route our packets towards Facebook (via the Internet). When Facebook sends reply to us, will the packet be sent directly to us (i.e., without going through the tunnel), or to the VPN server (and then go through the tunnel)? Please explain why.

Q7.

i) When browsing a web site, we see the following message. What does it mean that the certificate is not issued by a trusted CA? What is considered as a trusted CA?

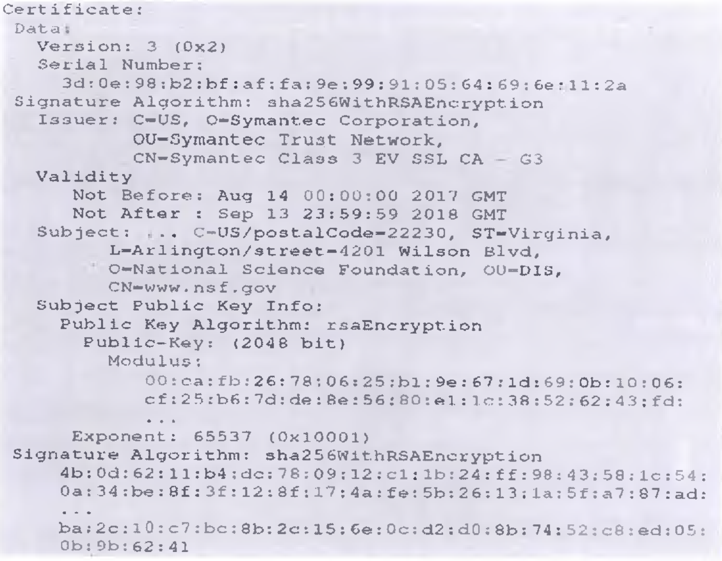
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.

ii) A bank recently changed its website name from www.bank32.com to www.bank48.com so users have to use this new name to access the bank's online services. To cut the cost, the bank wants to use the same certificate, instead of getting a new one. Would that be possible and why?

iii) An attacker has created a self-signed certificate, and he somehow gets a victim to add this certificate to the trusted certificate list of the victim's browser. What could be the damage?

iv) Are HTTPS and HTTP two different protocols? What are their differences and what do they have in common?

v) The following is an X.509 certificate.



```
Certificate:
 Data:
   Version: 3 (0x2)
   Serial Number:
     3d:0e:98:b2:bf:af:fa:9e:99:91:05:64:69:6e:11:2a
 Signature Algorithm: sha256WithRSAEncryption
   Issuer: C=US, O=Symantec Corporation,
           OU=Symantec Trust Network,
           CN=Symantec Class 3 EV SSL CA - G3
   Validity
      Not Before: Aug 14 00:00:00 2017 GMT
      Not After : Sep 13 23:59:59 2018 GMT
   Subject: ... C=US/postalCode=22230, ST=Virginia,
         L=Arlington/street=4201 Wilson Blvd,
         O=National Science Foundation, OU=DIS,
         CN=www.nsf.gov
   Subject Public Key Info:
     Public Key Algorithm: rsaEncryption
       Public-Key: (2048 bit)
         Modulus:
             00:ca:fb:26:78:06:25:b1:9e:67:1d:69:0b:10:06:
             cf:25:b6:7d:de:8e:56:80:e1:1c:38:52:62:43:fd:
             ...
      Exponent: 65537 (0x10001)
 Signature Algorithm: sha256WithRSAEncryption
     4b:0d:62:11:b4:dc:78:09:12:c1:1b:24:ff:98:43:58:1c:54:
     0a:34:be:8f:3f:12:8f:17:4a:fe:5b:26:13:1a:5f:a7:87:ad:
     ...
     ba:2c:10:c7:bc:8b:2c:15:6e:0c:d2:d0:8b:74:52:c8:ed:05:
     0b:9b:62:41
```

(a) Who issues the certificate?

(b) Who is the owner of the certificate?

(c) Who generated the signature on this certificate, and how can this signature be verified?

(d) The public key contained in this certificate is based on the RSA algorithm. Using the RSA algorithm, to encrypt a message M, we calculate M^e mod n. What is the value of e and n in this public key, if the number is too large, you only need to write first four bytes.