CS742 Lab Viva, Nov 08, 2017 (8.30am to 9.10am) **[10 Marks]**

Your Name: _____ Your Roll Number: _____

Code of Honour: I hereby declare that I will not cheat (or have not cheated) in this examination. _____ (signature)

Q1	Q2	Total

General Instructions:

- It is a closed book exam.
- State any assumptions clearly (they should make sense) and to the point in your answers.
- **No marks for answers without explanation**

Question 1: TCP Attacks [7 Marks]

1. In the TCP SYN flood attack, when you typed "sysctl –q net.ipv4.tcp_max_syn_backlog" what was output (quantity and its meaning) [1 Mark]

   It is the system queue size setting of max number of TCP connections that can be in SYN received state. It gave a value of 512.

2. In the TCP SYN flood attack with SYN cookies turned on, did you observe any RST packets during the attack? Who sent these packets, explain with relevant background details? Why do you think these packets were sent? [2 Marks]

   Yes. These RST packets had source IP as the spoofed IP address and the destination as the web server (on whom attack was launched). These packets were sent by the attacker machine itself. Likely because it is not able to handle the whole lot of SYN+ACK generated by the web server (victim).

3. In the TCP RST attack, what did you specify as arguments for the command "netwox 78 –d device –f filter –s spoofed ? Explain along with relevant background details. [2 Marks]

   Telnet is established between 10.0.0.2 and 10.0.0.3. The attacker (on say 10.0.0.1) can type

   netwox 78 –d eth0 –f "dst host 10.0.0.3 and dst port 23" –ips " 10.0.0.2"

   where the filter identifies the connection to reset. The –ips argument sends the RST to machine 10.0.0.2.

4. Explain in steps, how you performed the TCP session hijacking attack? The detail should include among other things, how you determined sequence numbers, what application payload you used etc. [2 Marks]

Telnet is established between 10.0.0.2 and 10.0.0.3. The attacker is on 10.0.0.1.
As part of the attack, say the attacker wants to create a directory called "attack" on 10.0.0.3 acting as 10.0.0.2

The attacker first needs to capture a packet sent by 10.0.0.2 to 10.0.0.3. From this packet, the attacker can figure out TCP seq (=s) and ack no (=a) as well as the port numbers.

The attacker then will use the netwox command (mode 40), where he will specify src as 10.0.0.2, port as observed, destination as 10.0.0.3 and port 23 (telnet). The seq number is set to s+1 and ack no to a+1. Importantly the payload of this tcp packet should include the command "mkdir attack \n". For this the attacker needs to determine the hexadecimal equiavelnt of this (e.g. 6D6B6469….)

Question 2: IP Tables [3 Marks]

1. To drop ping packets, how many iptable rules had to be installed? Why?

   Two.

   iptables -I INPUT -j DROP -p icmp --icmp-type echo-request #incoming ping
   iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP #outgoing ping

   (you don't have to specify the exact syntax)

2. What does the command "`iptables -F` INPUT" do?

   This command flushes the IP tables.

3. What does the command "`iptables -I INPUT -s 10.196.7.233 -p tcp -dport ssh -j ACCEPT`" do?

   This command allows ssh connection from IP address 10.196.7.233 to this machine.