FIoS

1

Roll Number:_____

Thapar Institute of Engineering and Technology, Patiala

Department of Computer Science and Engineering

Auxiliary Exam	Course Code: UCS534
B.E. COE/CSE (Third Year): Semester-V	Course Name: Computer and Network Security
August 16, 2022, MM:50	Name of Faculty: Dr. Tarunpreet Bhatia

Note: Attempt all parts of a question at one place. Assume missing data, if any, suitably.

Q.1 a) List out the steps to launch a DNS cache poisoning attack, in which an attacker (IP 192.168.3.300) intercepts a communication channel between a client (IP 192.168.1.100) and a server computer belonging to the website www.estores.com (IP 192.168.2.200). **(6)**

b) Discuss 4 ways to protect your organization from DNS poisoning attacks? **(4)**

Q.2 Write the rules using a Linux command line firewall for the following: **(2*5)**

a) Accept packets from a trusted IP Address (say 192.168.0.7)
b) Deny ssh service
c) Accept tcp packets on destination port 6881 (bittorrent)
d) Block connections on ports 23 and 80 on a computer whose local IP address is 192.168.0.6
e) List all the rules applied on your system and delete all the rules

Q.3 TLS is a cryptographic services protocol based upon public-key certificates, and is commonly used on the Internet.

a) What port is reserved for HTTP over TLS? Briefly explain the purpose of the TLS Handshake protocol. **(2)**
b) Identify the security services provided to TLS connections by the TLS Record Protocol. **(2)**
c) How are the TLS Handshake Protocol and the TLS Record protocol connected? **(3)**
d) As part of the Handshake Protocol the client and server negotiate which 'cipher suite' to use. In what circumstances is this negotiation useful? Why can this negotiation lead to potential security weaknesses **(3)**

Q.4 Set-UID is an important security mechanism in Linux operating systems. When a Set-UID program runs, it assumes the owner's privileges. **(5+5)**

a) What risks such privileged programs face and how they can be attacked if there are mistakes in the code. Explain with the help of an example.
b) How to improve the security of privileged programs?

Q.5 Explain with an example how ASLR and Stack Guard can be used as a defence against buffer overflow attacks? Is it possible to bypass ASLR and Stack Guard? Justify your answer. **(10)**