DIRECTORATE OF DISTANCE EDUCATION
NALSAR UNIVERSITY OF LAW, HYDERABAD

Advanced Diploma in Cyber Security & Data Protection Laws

Academic Year: 2021-2022

Second Semester –End Semester

Take Home Examination (July 1-4, 2022)

Paper II – 1.2.5. Cyber Security and Forensics
Lab Sessions: Digital Evidence Retrievals and Analysis Systems (DERAS)

TOTAL MARKS: 50

INSTRUCTIONS TO CANDIDATES

a) **Read the instructions for Take Home Examination carefully and adhere to the same.**
b) ***Please mention your name, ID No., subject name and total number of pages on the Answer Sheet.***
c) ***Clearly indicate the question numbers while answering them.***
d) ***Since this is a take home exam, we expect your answers to be analytical rather than straight answers.***
e) **Copying from any source including from other students is strictly prohibited. Plagiarism is considered as a serious academic mis-conduct and the University will take action as it deems fi**

---

1. Explain the concept of Application Layer Protocol: What is it and what is it not? And Issues Solved by the Application Layer with Application Layer protocol examples. **(15 marks)**

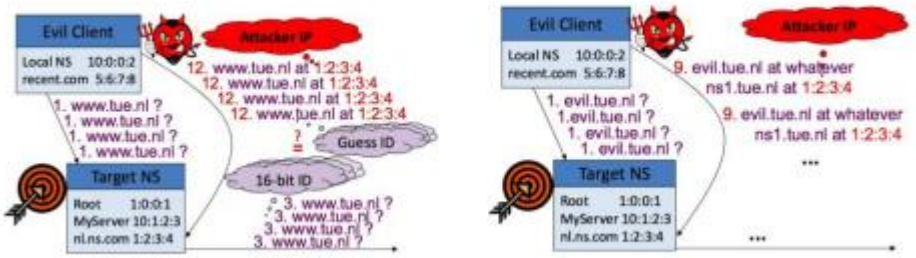
2. Explain the following Cyber Crimes with a real-time example **(15 marks)**

1. SQL Injection
2. XSS Cross Site Scripting
3. XSRF Cross-Site request forgery (XSRF)

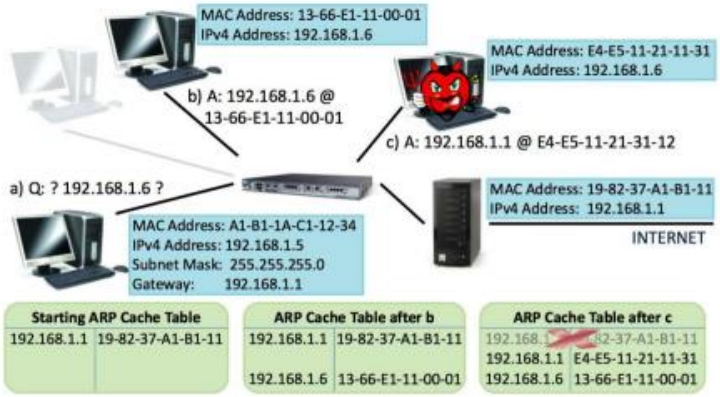
3. Case studies **(20 Marks)**

Scenario A. Illustrate the cybercrimes in the TCP/IP Protocol in the below tables (T1, T2, T3) with a real-time example

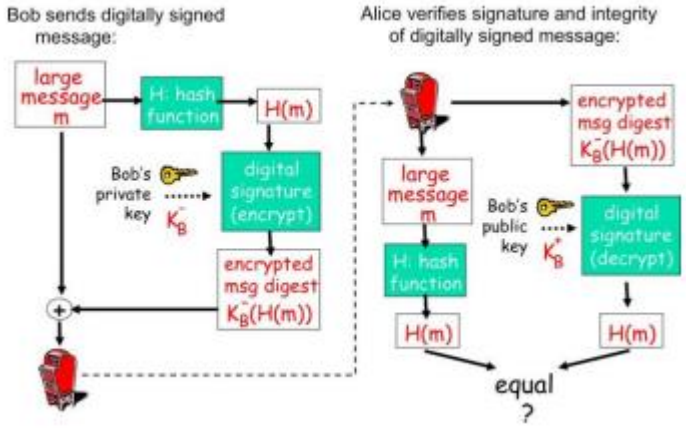
T1.



T2.



T3



Scenario B.

Premise: Wireshark is a Network Forensic Analysis Tool (NFAT) for Windows that can detect the OS, hostname and open ports of network hosts through packet sniffing or by parsing a PCAP file. Wireshark can also extract transmitted files from network traffic
Download Link: https://www.wireshark.org/download.html
Video Reference: https://vimeo.com/700699765
Password: nalsar123
PCAP Files:
https://drive.google.com/file/d/16NNECefVxPZ9xhbQ9HD5qcQi1D6e1tiH/view?usp=sharing

Objective: Analysing PCAP Files

Actions to be performed:

1. The observed hosts, including their DNS names, IP addresses and ports used during the monitored period
2. HTTP parameters sent to web servers as part of the observed session
3. Clear-text ASCII contents extracted from the network streams, including a separate tab for any captured credentials
4. The files exchanged between the hosts during the monitored period