Indian Institute of Information Technology Sri City, Chittoor

End Semester Examination – December 2021

Introduction to Cyber Security

SET - 1

Maximum Marks: 30 Time Duration: 1.5 hr.

Instructions

1. This is a **closed book online proctored** exam.
   a. You should not refer to books, notes or online resources.
   b. You should not discuss questions or answers with anyone (including outsiders)
   c. You should have your camera and microphone **ON** at all times and no headphones
2. Write the solutions clearly and legibly in A4 sheets, using pen (NOT pencil) and at the end of the exam you should submit the scanned copy of your solutions as explained by the faculty
3. **The name of the scanned copy should be Roll No + '_' + Set No.pdf (e.g. S20190010XYZ_Set1.pdf).**
4. **Write your name, roll no. and set number on each page of the answer sheets.**
5. **Answer questions in brief and to the point only**.
6. Follow all other instructions given by the faculty during the exam

Descriptive Questions (6 marks each)

1. Assume that you are building a web server that runs the following code sequence. Assume that do _work() is safe, and simply returns right away.

```
void process_request(char *input)
{
        char buf[256];
        strcpy(buf, input);
        if (!strncmp(buf, "GET ", 4))
        {
                do_work(buf);
                return;
        }
}
```

   a. Is this function susceptible to buffer overflow attacks? Explain your answer in 1-2 sentences. Also point out the line(s) where the overflow occurs, if any. [2 marks]
   b. Your security analyst tells you that you can simply make your stack non-executable and you need not worry about buffer overflows. Is he/she

correct? Explain in 1-2 sentences. [2 marks]

c. Your security analyst tried to make your system stack non-executable, but he failed (apparently he is not very good at his job!!). He said he had heard about something called canaries that can detect buffer overflows, but he cannot recollect what it is. Can you explain the concept to him in 1-2 sentences? [2 marks]

2. You are trying to book an airline ticket. You see on the website that only one ticket is left, and you book it. At the airport, you realize that there is another person with a reservation for the same seat! The airline staff are insisting that their system is perfect and there are no flaws.
   a. Can you suggest one possible error that might have led to this situation? [2 marks]
   b. Give a simple example that demonstrates this error. [2 marks]
   c. Suggest one way in which you can fix this problem. [2 marks]
3. What is a honeypot. Discuss various locations where honeypots can be deployed. [2+4 marks]
4.
   a. Compare and contrast between the signature-based and anomaly-based intrusion detection systems? Discuss their advantages and disadvantages. [3 Marks]
   b. What is the difference between a false positive and a false negative in the context of an IDS? How these are helpful to evaluate the accuracy of an IDS. [3 Marks]
5. What do you understand by the Cyber Incident Response and also discuss its need? [3+3 Marks]