Dr Hemraj

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -1 EXAMINATION- Oct 2017

M.Tech. I[st] Semester

COURSE CODE: 10M1WCI131 MAX. MARKS:15

COURSE NAME: System and Network Security Techniques

COURSE CREDITS: 2 MAX. TIME: One Hr

Note: All questions are compulsory. Carrying of mobile phone during examinations will be treated as case of unfair means.

Que 1. ***[03 Marks]*** Ankit is building a web server that runs the following code sequence, in which `process_req()` is invoked with a user-supplied string of arbitrary length. Assume that `process_get()` is safe, and for the purposes of this question, simply returns right away.

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

Seeing the difficulty of preventing exploits with a non-executable stack, Ankit instead decides to make the stack grow up (towards larger addresses), instead of down like on the x86. Explain how you could exploit `process_req()` to execute arbitrary code. Draw a stack diagram to illustrate what locations on the stack you plan to corrupt, and where in the input string you would need to place the desired values.

Que 2. ***[03 Marks]*** Explain the following terms/statements in details-

a) Dumpster's diving
b) Covert channels
c) market place for owned machine

Que 3. ***[03 Marks]*** Explain why a capability-based system such as Hydra provides greater flexibility than the ring protection scheme enforcing protection policies.

Que 4. ***[03 Marks]*** Consider a system that generates 20 million audit records per day. Also assume that there are on average 20 attacks per day on this system and that each such attack is reflected in 40 records. If the intrusion detection system has a true-alarm rate of 0.8 and a false-alarm rate of 0.0005, what percentage of alarm generated by the system correspond to real intrusion?

Que 5. ***[03 Marks]*** Using the proper terminology represents the symmetric and asymmetric cryptography. Also provide a calculative example for both.

CI-19, MT