**Cybersecurity Principles**

Midterm Exam

* This is a *closed* book, *closed* note exam.
* Show **ALL** your work to get full or partial credit for the problem.
* You have 75 minutes. (2 points per minute)

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |
| --- | --- | --- |
| **Problem** | **Total** | **Points** |
| 1 | 10 |  |
| 2 | 30 |  |
| 3 | 16 |  |
| 4 | 24 |  |
| 5 | 12 |  |
| 6 | 16 |  |
| 7 | 10 |  |
| 8 | 20 |  |
| 9 | 12 |  |
| **Total:** | 150 |  |

1. (10 points) Define and distinguish between integrity, confidentiality and availability.

2. (30 points) Fill in the blank (3 points each)

(i) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ can be defined as a table of subjects and objects indicating which actions individual subjects can perform on individual objects.

(ii) A/An \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to a computing system is a set of circumstances that has the potential to cause loss or harm.

(iii) Authentication mechanisms are based on: something the user knows, something the user is, and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(iv) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ tricks a client or server into executing scripted code by including the code in data inputs.

(v) In a/an \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ attack, the attacker tries all possible passwords, usually in some automated fashion.

(vi) A cipher that replaces characters of the plaintext is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(vii) The effective key length is \_\_\_\_\_\_\_ bits in triple DES.

(viii) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ are programs planted by an agent with malicious intent to cause unanticipated or undesired effects.

(ix) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is code that allows unauthorized access to a machine or program; bypasses normal access control and authentication.

(x) A virus executes in a particular way, using certain methods to spread. Each of these characteristics yields a telltale pattern, called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, that can be found by a program that looks for it.

3. (16 points) Calculations.

(a)(10 points) (Diffie-Hellman) Alice and Bob agree on *p = 23* and *g = 5*

(i) If Alice chooses her private key = 6, what is the her public key () ?

(ii) If Bob chooses his private key = 3, what is their shared secret K ?

(b) (6 points) (RSA) You are given *p = 5*, *q = 11,* if the encryption key e = 3, what is the decryption key d ?

4. (24 points) Provide a brief description of each of the following: (4 points each)

a) Trojan horse

b) Vulnerability

c) SETUID program

d) Hash collision

e) SQL injection

f) Phishing

5. (12 pts - 3pts each). **Circle** the correct answer for each of the following.

(i) Which of the following terms best describes a mathematical encryption operation that cannot be reversed?

A. One-way hash

B. DES

C. Transposition

D. Substitution

(ii) Which of the following terms best describes the assurance that data has not been changed due to an accident or malice?

A. Availability

B. Confidentiality

C. Integrity

D. Auditability

(iii) Which of the following statements is true?

A. Controls are implemented to eliminate risk and eliminate the potential for loss.

B. Controls are implemented to mitigate risk and reduce the potential for loss.

C. Controls are implemented to eliminate risk and reduce the potential for loss.

D. Controls are implemented to mitigate risk and eliminate the potential for loss.

(iv) The elements within the information system that are protected from use or access are defined as \_\_\_\_\_\_\_\_\_\_\_\_.

A. Subjects

B. Objects

C. Labels

D. All of the above

6. (16 points) Suppose that Bob wants to send a message to Alice. Digital signatures can be used to authenticate the sender of a message.

(i) (6 points) Explain how digital signatures work.

(ii) (4 points) Do digital signatures protect integrity of the message? Do digital signatures protect confidentiality of the message?

(iii)(6 points) Explain how digital signature generation would be different for private key (e.g., DES) versus public key (e.g., RSA) style encryption. Which one makes more sense to use for digital signatures?

7. (10 points) Identify all of the problem lines in the code, and explain what the problems are.

(i) (5 points)

u\_char \*make\_table(unsigned int width, unsigned int height, u\_char \*init\_row)

{

unsigned int n;

int i;

u\_char \*buf;

n = width \* height;

buf = (char \*)malloc(n);

if (!buf) return (NULL);

for (i=0; i< height; i++)

memcpy(&buf[i\*width], init\_row, width);

return buf;

}

(ii) (5 points)

int main(int argc, char \*argv[])

{

char user\_input[100];

int \*secret;

int int\_input;

secret = (int \*) malloc(2\*sizeof(int));

secret[0] = 38; secret[1] = 52;

printf("Please enter a decimal integer\n");

scanf("%d", &int\_input); /\* getting an input from user \*/

printf("Please enter a string\n");

scanf("%s", user\_input); /\* getting a string from user \*/

printf(user\_input);

printf("\n");

return 0;

}

8. (20 points) Recall the lab where you worked with buffer overflow attacks.

(i) (4 points) What is a buffer overflow vulnerability?

(ii) (6 points) List two possible mitigations.

(iii) (7 points) When running in the bof() function, finish the stack layout.

(3 points) Where are \*str, buffer, return address, previous frame pointer? Mark the bof()stack frame (similar to the main() stack frame marked on the stack).

(2 points) Assume %ebp (previous frame pointer) is stored in location 0xbffff0e0, mark the address at the correct place (using “0xbffff0e0 ---->” on the left side).

(2 points) Where is the return address stored? Mark the correct address of it at the correct place (using the method same with the last question).

(iv) (3 points) Fix the code by using a safer function.

Stack grows

int bof(char \*str)

High address

{

Main()

stack frame

char buffer[24];

strcpy(buffer, str);

return 1;

}

Low address

9.(12 points) Consider a computer system with three users: Alice, Bob and Charlie. Alice owns the file alicerc, and Bob and Charlie can read it. Charlie can read and write the file bobrc, which Bob owns, but Alice can only read it. Only Charlie can read and write the file charlierc, which he owns. Assume that the owner of each of these files can execute it.

(i) (6 points) Create the corresponding access control matrix.

(ii) (6 points) What is access control in the computer system? What is the difference between a subject and an object?