THE UNIVERSITY OF HONG KONG
FACULTY OF ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE

COMP 7904 Information Security: Attacks and Defense

Date: 23 May 2021 – 24 May 2021 **Time: 24 hours (from 9:30am 23 May 2021)**

Please write your university number clearly at the beginning of your answer script. Do NOT write down your name.

***** This is an open-book examination. *****

You can either write your answers on papers or type them with a computer. At the end of the examination, you should submit a *single* pdf file to Moodle.

Only approved calculators as announced by the Examinations Secretary can be used in this examination. It is candidates' responsibility to ensure their calculator operates satisfactorily, and candidates must record the name and type of the calculator used on the front page of the examination script.

Note that you can download the virtual machine for Part B while you are working on Part A.

The information for downloading the virtual machine is available on Moodle.

The total mark is 100.

Answer ALL questions in this paper.

Moodle Course Website:

https://moodle.hku.hk/course/view.php?id=80074

Part A.

[20%] Multiple choice questions. (Questions A.1 – A.10)
For each of the following questions, select ONLY ONE answer. Each CORRECT answer will have 2 marks. But 2 marks will be deducted for each WRONG answer. No marks will be deducted for UNANSWERED questions.

1.		6.	
2		7.	
3.		8.	
4.		9.	
5.		10.	

1. Which of the following statement(s) is (are) CORRECT?

   I. A cryptographic hash function takes a fixed length of input and produces a variable length of output in which the length of the output depends on a random number.
   II. It is computationally easy to compute a message's cryptographic hash value.
   III. If a cryptographic hash function is not strong collision resistant, then it cannot be weak collision resistant.

   A. I only.
   B. II only.
   C. II and III only.
   D. I and III only.
   E. All of the above.

2. Which of the following statement(s) is (are) INCORRECT about password cracking attacks?

   I. Phishing attack can be considered as a kind of social engineering attacks.
   II. If we can launch an online password attack, we should be able to launch an offline password attack.
   III. Let R1 and R2 be two reduction functions used in a rainbow table, it is required that given any hash value h, R1(h) cannot be equal to R2(h).

   A. I only.
   B. II only.
   C. III only.
   D. I and III only.
   E. All of the above.

3. Which of the following statement(s) is (are) CORRECT?

I. When you create a bootable USB for Kali Linux, setting it to the "persistent" mode can write-protect the USB to avoid corrupting the system.
II. The regular expression: ab(a|b|c)*(b|c)* represents the set of strings that starts with "ab" and ends with either "b" or "c".
III. Passive reconnaissance attempts to collect useful information for a later attack while trying not to alert the victim.

A. I only.
B. II only.
C. III only.
D. All of the above.
E. None of the above.

4. Which of the following statement(s) is (are) INCORRECT?

I. Using web.archive.org to retrieve old versions of a webpage for a victim can be regarded as a kind of active reconnaissance.
II. From https://haveibeenpwdned.com, one can obtain a database of hacked passwords in plaintext for research purposes.
III. Using this "plagiarism examination site:cs.hku.hk" in Google search will retrieve all pages from the website: cs.hku.hk that contain both "plagiarism" and "examination".

A. I and II only.
B. I and III only.
C. II and III only.
D. All of the above.
E. None of the above.

5. Which of the following statement(s) is (are) CORRECT?

I. Two devices in the world can have the same private IP address at the same time.
II. Public IP cannot be dynamic.
III. There always exists at least one DNS server in the world that can map all domain names to IP addresses.

A. I only.
B. II only.
C. I and II only.
D. I and III only.
E. II and III only.

6. Which of the following statement(s) is (are) INCORRECT?

   I. Both a full TCP scan and TCP SYN scan will complete the three-way handshake.
   II. Idle scan requires the use of a zombie.
   III. An ethical hacker does not need to conduct reconnaissance as he/she is authorized to hack the system.

   A. I and II only.
   B. I and III only.
   C. II and III only.
   D. All of the above.
   E. None of the above.

7. Which of the following(s) is (are) INCORRECT?

   I. TOR makes use of encryption technique.
   II. Snort rules are used to define the access rights of legitimate users in a system.
   III. POP3 is a protocol that will encrypt your email.

   A. I and II only.
   B. I and III only.
   C. II and III only.
   D. All of the above.
   E. None of the above.

8. Consider the following protocol using bilinear map. Let P be a generator of a cyclic group, known to the public. Alice holds <a, aP> as her private key and public key respectively, where a is an integer. Bob holds <b, bP> as his private key and public key respectively, where b is an integer.
   Step 1. Alice comes up with a random integer r.
   Step 2. Alice sends <rP> to Bob.

   Which of the following statement(s) is (are) CORRECT about this protocol.

   I. Both can compute brP and abP.
   II. If an attacker knows the private key of Bob: b and can obtain all packets going through the communicate, then he can compute both brP and abP.
   III. They can use "abP||arP" as their common session key.

   A. I and II only.
   B. I and III only.
   C. II and III only.
   D. All of the above.
   E. None of the above.

9. Which of the followings is (are) CORRECT about buffer overflow attack?

   I. Snort rules can be set to avoid buffer overflow attack.
   II. A major objective of buffer overflow attack is to overwrite the IP register to change the flow of control.
   III. Allowing data to be written outside the boundary of an allocated memory is a main cause of buffer overflow attack.

   A. I and II only.
   B. I and III only.
   C. II and III only.
   D. All of the above.
   E. None of the above.

10. Which of the following(s) is (are) CORRECT?

    I. It is not possible to have two nearby wifi routers having the same SSID.
    II. Plausibly deniable encryption allows a user to create a hidden encrypted partition within a normal partition in a harddisk such that any verifier cannot prove the existence of the hidden encrypted partition unless being disclosed by the owner.
    III. PBKD2 can help to strengthen a weak password.

    A. I only.
    B. II only.
    C. III only.
    D. I and III only.
    E. II and III only.

[10%] Answer the following short questions. (Questions A.11 – A.13)

11. [4%] Figure (a) shows a rainbow table for password cracking. Figure (b) shows some hash function values (of course, assume that you cannot obtain the password from the hash), Figure (c) shows some values for the reduction function R1, Figure (d) shows some values for the reduction function R2, and Figure (e) shows some values for the reduction function R3.

Figure (a): Rainbow Table

Start of Chain	End of Chain
kate	lugirl
lein	gboy
alice	Attic
imini	succes

Figure (b): hash function

Password	Hash
kate	gfi479
hoco	comp79
snofi	dte345
lein	eo4cg1
imini	d89qwf
mexia	yy456z
alice	cyb410
xuey	i63gt7
notes	2sjlp
succes	st456h

Figure (c): R1 reduction function

Hash	Password
gfi479	hoco
eo4cg1	imini
cyb410	xuey
i63gt7	Lugirl
d89qwf	alice

Figure (d): R2 reduction function

Hash	Password
comp79	snofi
d89qwf	mexia
i63gt7	notes
cyb410	succes
st456h	succes

Figure (e): R3 reduction function

Hash	Password
dte345	lugirl
st456h	gboy
2sjlp	attic
comp79	great
cyb410	Heiut
yy456z	gboy

(a) Assume that the given hash value is "i63gt7", find the password. Please list all steps in searching this password, until the password is found, or when you can conclude that you cannot find the password.

(b) Repeat part (a) with hash value equals "st456h".

12. [2%] Provide the commands to do the followings: (i) to locate DNS servers that are hosting HKU records; and (ii) to test if unauthorized zone transfer is allowed?

13. [4%] (T/F questions): For each of the following statements, state whether it is true (T) or false (F). No need to provide explanations. Each CORRECT answer will have 1 mark. <u>But 1 mark will be deducted for each WRONG answer.</u> No marks will be deducted for UNANSWERED questions.

(a)	(b)	(c)	(d)

(a) The reason why adding salt to passwords will make the rainbow table attack more is because that it will make the hash function not unique.

(b) PBKDF2 can strengthen a weak key (or password) while it also increases the time for the authentication process.

(c) The main idea of the FMS attack for RC4 is based on the small size of the key and the brute-force attack approach.

(d) Deep packet inspection is the key technique for a system to identify if an incoming or outgoing encrypted network pack is malicious or not.

Part B.

In this part, you are required to download the virtual machine at the location specified on Moodle.

[70%] Practical examination.

The objective of this part is to penetrate a provided vulnerable virtual machine, it requires multiple exploitation steps, resulting in getting low-level local access, and then perform privilege escalation to gain root or administrative privilege. You are required to **write a penetration testing report** describing your exploitation process for the target virtual machine. You must document all the details of your attacks including all steps, commands issued, and console output in the form of a penetration test report. Your documentation should be thorough enough that your attacks can be replicated step-by-step by a technically competent reader.

The **report requirements** are very strict. Failing to provide sufficient proofs as shown below will result in reduced or zero points being awarded.

- The detailed information of target VM (e.g. IP address, open ports, services, application, version numbers, etc.)
- Reference links of vulnerabilities
- The modified exploit code
- The URL to the original exploit code
- The command used to generate any shellcode (if applicable)
- Highlighted changes you have made to the exploit code
- An explanation of why those changes were made
- Recommendations

Main Objectives:

- Identify and verify the vulnerabilities on the machine (>=4 vulnerabilities)
- Reconnaissance methodology and research capability
- Get remote shell access to machine
- Get remote root shell on machine
- Crack / guess the users' passwords
- Provide written step-by-step documentation of the exploits and resulting shells.

Note:

- There are 4 FLAGs in different locations (e.g. home folders, databases) of the target to guide you to finish the exam.
- Attach the FLAGs as an appendix to your report. Zero points will be awarded if only the FLAGs are provided.

***** End of the paper *****