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

COMP 7904 Information Security: Attacks and Defense

Date: 23 May 2020 – 24 May 2020 **Time: 24 hours (from 9:30am 23 May 2020)**

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 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 from Moodle for Part B while you are working on Part A.

The total mark is 100.

Answer ALL questions in this paper.

Part A.

[30%] Multiple choice questions. 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.		11.	
2		7.		12.	
3.		8.		13.	
4.		9.		14.	
5.		10.		15.	

1. Which of the following statement(s) is (are) CORRECT about a cryptographic hash function?

   I. A hash function which is strong collision resistant must also be weak collision resistant.
   II. A hash function which is one-way must also be weak collision resistant.
   III. Given two different documents D1 and D2, it is possible that the hash values of both documents are the same.

   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.

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

   I. Rainbow table can be used to crack all passwords of a system.
   II. Using salt can make rainbow table attack more difficult to succeed.
   III. Brute-force attack is always successful given unlimited amount of time and space.

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

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

   I. Offline password attacks are easier to be discovered by the victim than online password attacks.
   II. Two factor authentication refers to the case that if the first authentication fails, the user is given another chance to go through the second authentication.
   III. PBKD2 can help to strengthen a weak password.

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

4. Which of the following regular expression represents the set of all non-empty strings of even length assuming that the alphabet is {a, b}?

A. (a|b)(a|b)*
B. (aa|bb)*
C. ab(a|b)*
D. (aa|ab|ba|bb)*
E. None of the above.

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

I. Conducting a google search is considered as an activity of passive recon.
II. censys.io allows you to search for all ftp hosts in Hong Kong.
III. By checking the website https://haveibeenpwdned.com, I can be sure that my account has not been hacked.

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

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

I. All DNS servers support iterative query.
II. 172.30.1.1 is a private IP.
III. DNSSEC is a standard protocol to be installed in all DNS servers.

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 statement(s) is (are) INCORRECT?

I. SQL injection is a man-in-the-middle attack between an SQL server and a web application server.
II. Sniffing is to modify the content of a packet on a network.
III. Analyzing a press release of a target company (website) is considered as an active reconnaissance.

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. Which of the following is NOT a correct description of ethical hacking?

A. Ethical hacking involves the same tools, tricks, and techniques that hackers use except that ethical hacking will not use "social engineering" to hack into a system.
B. Ethical hackers are security professionals.
C. It is legal to conduct ethical hacking.
D. Ethical hacking will produce a report to convey the findings to the customer.
E. None of the above.

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

I. A zone file has only one SOA.
II. By default, a network interface controller is not in promiscuous mode.
III. tcpdump is one of the eavesdropping tools.

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. Proxy hijacking is a man-in-the-middle attack.
II. DNS spoofing tries to alter a DNS server's records.
III. ARP spoofing can be considered as a sniffer 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.

11. 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, id> to Bob, where id is the id of Alice.

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

I. Both Alice and Bob are able to compute a common key.
II. The common key is "abP || brP".
III. If an attacker knows Bob's private key, he can launch a compromised key 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.

12. Which of the followings can be used to avoid buffer overflow attack?

I. By setting filtering rules in the firewall.
II. Check the source code if available.
II. Try to test the program with all possible inputs.

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

13. Which of the following(s) is (are) INCORRECT for cross-site scripting (XSS) attack?

I. In a reflected XSS attack, the victim is cheated to download the malicious code.
II. In a persistent XSS attack, the malicious code comes from website database that the victim accesses.
III. XSS attack is not a man-in-the-middle 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.

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

I. WPA has been cracked already.
II. By hiding SSIDs, attackers are not able to discover your router.
III. Using the MAC filtering property in a router can avoid nodes whose MAC addresses not in the white list to connect to the router.

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

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

I. By launching a DDOS attack, an attacker can create a backdoor in the target system.
II. Encrypting network traffic is critical so that it is not possible to infer anything from the traffic.
III. One should always apply patches, when available, to an operating system to protect 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.

Part B.

[70%] Practical examination.

The objective of this examination is to penetrate a provided vulnerable virtual machine, it requires multiple exploitation steps, resulting in getting low-level local access, and then performing 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 **documentation requirements** are very strict and failure to provide sufficient proof shown as 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 the vulnerabilities on the machine
- Reconnaissance methodology and research capability
- Get shell access to machine
- Get root shell on machine
- Crack / guess the users' passwords
- Provide written step-by-step documentation of the exploits and resulting shells.

*** End of the paper ***