COMP 4632
Practicing Cybersecurity: Attacks and Counter-measures

Sample Exam Questions

(for reference only)

Instructions

1. All answers need to be written in the provided answer book during the examination.
2. The sample questions here aim to help students understand the question formats. They do not necessarily reflect the difficulties of the actual exam questions.
3. There *may* be questions with bonus marks in the examination. Students who are able to fulfill certain requirements will be given extra marks. However, the maximum marks gained for the whole exam will not exceed 100. (e.g. If student A scores 97 marks with 2 bonus marks, his/her total score will be 99; and if student B scores 99 marks with 2 bonus marks, his/her total score will be 100 only).
4. Marks *may* be deducted when wrong answers are provided in some questions. However, all questions will not carry negative marks.

Part A – Multiple Choice Questions [@1-2 marks]

Write down alphabet(s) representing the most appropriate answer in each of the following questions.

Q1. What can an attacker do on a vulnerable application via exploiting a Cross-Site Scripting (XSS) vulnerability? List all applicable answer(s). **[2 marks]**

(A) Retrieve the following cookie set in HTTP response:
`Set-Cookie: session_id=12345678; Secure`
(B) Add your selfie photo to the main page ☺;
(C) Retrieve the password hash of a user stored in the application’s database;
(D) Upload a malicious file to the application;
(E) Download a malicious file to the browser.

Answer: A, B, E

Q2. Bob claimed that he hacked the home network of his neighbor Alice. What should Alice do in order to keep her home network secure? **[1 mark]**

(A) Disconnect the network from the Internet when no one in her home need to get online.
(B) Check the password used and configurations of the Wi-Fi network;
(C) Ask for assistant from her friend who sells enterprise-grade network firewall.
(D) Call the police.

Answer: B

Part B – Short Questions [@1-5 marks]

Answer the questions according to the instructions provided.

Q3. Explain what is "salted" password hashes and the advantage of them. **[3 marks]**

Answer:

- Salted password hashes are generated from a cryptographic hash function
- A random data (i.e. salt) is used together with the password when generating the hash
- It helps to defend against pre-computed dictionary attack (e.g. rainbow table)

(deduct 0.5 for each wrong point)

Q4. Write down the Linux command to find the lines containing "answer" from the file "/home/comp4632/marking_scheme.txt". **[1 mark]**

Answer:

```
grep "answer" /home/comp4632/marking_scheme.txt
```

Part C & D – Computer-Assisted Questions

In the following two parts, you will be asked to work on some tasks using the virtual machine(s) images provided during the actual examination. You are not allowed to use tools outside the virtual machine(s) to complete the questions. Follow the instructions in the questions to answer them accordingly.

Part C – Short questions [@1-5 marks]

Q5. Illustrate what happened when you opened your browser, entered www.google.com in the URL bar, and finally saw the page hosted at https://www.google.com.hk/. Include appropriate details (e.g. IP addresses, port numbers, response codes, etc) you observed. **[5 marks + 2 bonus marks]**

Answer:

- The domain name www.google.com was translated to IP address 216.58.221.132 via DNS (or host tables, etc)
- The browser process connect to TCP 80 port of the 216.58.221.132 and sent an HTTP request for www.google.com
- The web server at 216.58.221.132 redirects the browser to a URL at http://www.google.com.hk/ with a HTTP 302 response
- Similarly, the domain name www.google.com.hk was translated to IP address 216.58.221.131 and the browser send request to TCP 80 port as instructed in the HTTP 302 response
- The web server at 216.58.221.131 redirects the browser to a URL at https://www.google.com.hk with a HTTP 302 response
- The browser sent a request over HTTPS (or SSL) to TCP 443 port of the same web server and obtained a HTML document
- The browser parsed the HTML document, request for related resources and render the page accordingly.

(1 mark for each point in appropriate order)
(deduct 0.5 for each wrong point)

Part D – Long questions [@6+ marks]

Q6. The "8 Win Online Betting System" finally goes live after 4 weeks of blood, sweat and tears. You are hoping to enjoy your fruitful university life again but things don't often go your way ☹. You were asked to take the application support role when some end users reported that the application were entirely not accessible.

You attempted to access the application from various network locations. The results were recorded in the following table:

	Network Location / Access Path	**Result / Observations**
(i)	via Internet from your Home	Entirely not accessible
(ii)	via local area network of your office, passing through the same network firewall which is used also for protect your office computers and servers from the Internet	Entirely not accessible
(iii)	Directly connect your laptop to the switch connecting the web server	20% of the access failed to connect and 80% connections were established successfully. Among the successful connections, most of them had slow responses and some even timeout.

(a) Based on the information provided up to here, make ONE educated guess on the most possible part having issues. Justify your guess with fact(s). Suggest ONE way to verify your guess. **[3 marks]**

Answer:

- The network firewall may be having issues
- It's because all access paths passing through the firewall failed
- Identify other access path(s) and test whether all those passing through firewall would fail and those not passing through would succeed.

(1 mark for each point above)
(for other reasonable guess with valid justification and verification, max 1.5 marks can be given for this part)
(mark only the 1st educated guess)

Your colleague passed you the root access to the web server so that you can have further investigate there.

(b) Suggest TWO checks that may help your investigation. Name ONE possible command or file path for each of those checks. **[2 marks + 2 bonus marks]**

Answer:

- CPU & memory utilization (command: top)
- Web server logs (/var/log/apache2/access.log, /var/log/apache2/error.log…)
- Opened ports and connections (command: netstat)
- Capture live network traffic (command: tcpdump)
- Any other valid checks & command / path

(1 mark for each, consisting of 0.5 for the check and 0.5 for command/path)
(no deduction on irrelevant checks)

The network administrator provided you a PCAP file containing the traffic passing through the Firewall captured during the incident. You can find the file at /home/comp4632/Q6/firewall.pcap inside the provided virtual machine.

(c) Analyze the PCAP file and try to identify the attack(s), and explain how they may cause the incident. List the corresponding potential attacker IP address(es). **[5 marks + 2 bonus marks]**

Answer:

- There were TCP SYN floods launched from 3 IP addresses X.X.X.X and Y.Y.Y.Y, Z.Z.Z.Z
  - Result in numerous half-open TCP connections, consuming the number of concurrent connections supported by the firewall/server
- Repeated SQL injections on a parameter on a page from the IP address A.A.A.A
  - Causing the database to sleep long time before responding the result to the application, causing the application time out.
- Others potentially involved IP address
  - B.B.B.B launched a port scan on the server
  - C.C.C.C tested the vulnerable parameter for SQL injection

(2 point for each for SYN flood / SQL injection, consisting of 1 for the type of attack, and 1 for the impact)
(0.5 point each correct potential attacker IP address)

End of Sample Questions