THE UNIVERSITY of ADELAIDE

Replacement Examination, Semester 1, 2019

Cyber Security Fundamentals
COMPSCI 3308, 7308

Official Reading Time:	10 mins
Writing Time:	120 mins
Total Duration:	130 mins

Questions	Time	Marks
Answer all 11 questions	120 mins	100 marks 100 Total

Instructions

- Begin each answer on a new page in the answer book.
- Examination material must not be removed from the examination room.

Materials

- No calculators allowed.
- Foreign language paper dictionaries permitted.

DO NOT COMMENCE WRITING UNTIL INSTRUCTED TO DO SO

Question 1

(a) What are some of the motives behind threat actors engaging in illegal cyber activities?

A. Reconnaissance
B. Political influence
C. Curiosity
D. Profit
E. Vengeance

Solution: All except A.

[1 mark]

(b) Are activities of a "Grey Hat" hacker considered legal?

A. Yes, because they are only finding weaknesses, not actively exploiting them
B. Yes, because they will inform weaknesses to the company, not sell them on the dark web
C. No, because any on-line security testing requires written approval of the system owner
D. No, because it is unethical to break into other people's computer systems

Solution: C.

[1 mark]

(c) Name three (3) asymmetric forces at play in between blackhat and whitehat hackers that makes the bad guys generally more successful.

Solution: time, time-of-day, resource (money), being able to break the law, success factor (what constitutes success)

[3 marks]

[Total for Question 1: 5 marks]

Question 2

(a) True or False? Reconnaissance is the first step of a hacking project, and is used by both black hat hackers and white hat hackers.

Solution: True.

[1 mark]

(b) OSINT is generally uses _____techniques.

A. Active
B. Passive

Solution: B. Passive.

[1 mark]

(c) True or False? Not displaying a server product and version in the banner helps to limit disclosure to hackers performing reconnaissance.

Solution: True.

[1 mark]

(d) Which of these represents the Google search syntax for looking up PDF files containing keyword 'confidential', limited to the domain xyz.com?

A. `site:xyz.com inurl:pdf confidential`
B. `site:xyz.com filetype:pdf confidential`
C. `indomain:xyz.com ext:pdf secret -confidential`
D. `indomain:xyz.com filetype:xls confidential`

Solution: B

[1 mark]

[Total for Question 2: 4 marks]

Question 3

(a) What type of control/countermeasure can Penetration Testing be classified as?

A. Administrative
B. Preventive
C. Detective
D. Responsive

Solution: B. Preventive. Pentest finds and fixes weaknesses before the bad guys do.

[1 mark]

(b) True or False? The Lockheed Martin Cyber Kill Chain model includes a step to install a persistent back-door into an organisation.

Solution: True

[1 mark]

(c) Which of the following is the second step of the Lockheed Martin Cyber Kill Chain?

A. Actions on Objectives
B. Command & Control
C. Delivery
D. Exploitation
E. Installation
F. Reconnaissance
G. Weaponisation

Solution: G. Weaponisation.

[1 mark]

(d) Name one advantage and one disadvantage of 'black box' testing over 'white box' testing.

Solution: Advantages: Simulates real hacking, cheaper and quicker
Disadvantages: May not find all weaknesses. May not be able to put findings into context.

[2 marks]

[Total for Question 3: 5 marks]

Question 4

(a) Common Vulnerability Scoring System (CVSS) is a scoring system that quantifies security weaknesses. Whether it requires user interaction to exploit the vulnerability is a factor that is taken into consideration when calculating the score. Name three other factors.

Solution: Network vs Local, Complexity, C/I/A impact, Privige Required, Scope Changed

[3 marks]

(b) Is a Tomcat server running with a default "admin" password is considered a vulnerability?

A. No. Vulnerabilities generally refer to software bugs.
B. No. Simple human errors are not considered vulnerabilities in computer security.
C. Yes. Misconfiguration such as default passwords are one of the most common vulnerabilities.
D. Yes. Tomcat is an insecure software with many vulnerabilities, and should not be used in production. environments.

Solution: C.

[1 mark]

(c) There are 6 (or 8 including the extended ones) TCP flags. Which flag(s) are set in each phase of the TCP three-way handshake?

1. _____(client to server)
2. _____(server to client)
3. _____(client to server)

Solution: SYN ; SYN+ACK ; ACK

[3 marks]

(d) In a Nmap decoy scan, what is spoofed to hide the attacker?

A. Source MAC address
B. Source port number
C. Source IP address
D. Source sequence number

Solution: C. IP addressed.

[1 mark]

(e) True or False? The Nmap $-O$ option or the OS fingerprinting scan is a handy way of identifying the target's operating system.

Solution: True

[1 mark]

(f) The security-by-obscurity technique to hide a network service behind a port that only opens after accessing a predetermined (Secret) sequence of other ports is called port _____.

Solution: Knocking.

[1 mark]

(g) Briefly explain why Meltdown and Spectre, CPU bugs that affected billions of computers around the world, only have a CVSS base score of 5.6.

Solution: (1) It only affects confidentiality (2) CVSS base score does not take into consideration the number computers affected

[2 marks]

[Total for Question 4: 12 marks]

Question 5

(a) If a symmetric encryption like AES is used to uniquely secure communication between Alice, Bob, Charles, Deb, and Elena, how many shared secrets do you need?

Solution: 10

[1 mark]

(b) Following on from the preceding question, if you used asymmetric encryption like RSA to securely communicate between the same five people, how many private/public key pairs do you need?

Solution: 5 pairs

[1 mark]

(c) True or False? The XOR cipher is an example of a symmetric cipher.

Solution: True.

[1 mark]

(d) Substitution ciphers such as Caesar Cipher can be broken using _____analysis.

Solution: Frequency.

[1 mark]

(e) Which of the following statements are TRUE regarding the Diffie-Hellman protcol?

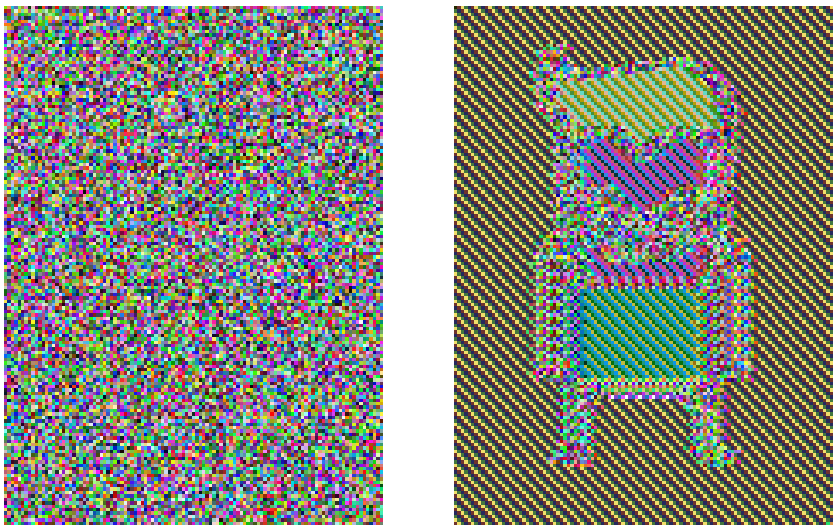
A. It is a symmetric encryption algorithm
B. It is a protocol for securely exchanging secret keys
C. It is part of the RSA cipher suite
D. It requires that both parties publicly agree on a modulus and a prime

Solution: B and D

[1 mark]

(f) Refer to Fig. 1. Both are graphic representations of the same image encrypted with AES, but using different modes. The picture on the left was encrypted with _____and the one on the right using _____.

A. ECB, CBC
B. CBC, ECB
C. AES, AES
D. ECB, AES



(a) (b)

Figure 1: Encrypted Images

Solution: B: CBC, ECB

[1 mark]

(g) If Alice wants to send a short encrypted message to Bob using RSA, which key does she use?

A. Alice's public key
B. Alice's private key
C. Bob's public key
D. Bob's private key
E. The root certificate of the Certificate Authority (CA)

Solution: C. Bob's public key.

[1 mark]

(h) If Alice wants to send a digitally signed document to Bob, which key does she use to sign the document hash?

A. Alice's public key
B. Alice's private key
C. Bob's public key
D. Bob's private key
E. The CA's root certificate

Solution: B. Alice's private key

[1 mark]

(i) The RSA encryption relies on the use of a _____function that is easy to compute in one direction, but difficult in the other direction, unless a certain secret is known.

Solution: Trapdoor

[1 mark]

(j) What operation does RSA assume to be computationally hard such that the encryption method is made safe?

Solution: Anything that is similar to "Given a big number n, calculating two primes p and q such that p * q = n".

[2 marks]

(k) Which statements below are true regarding 'key stretching' in the context of password hashing.

A. Key stretching involves repeatedly applying cryptographic hash thousands of times
B. Key stretching can make offline brute-force and dictionary attack infeasible by requiring significant computational effort for each attempt to guess a password
C. Key stretching, when used in conjunction with salt, is vulnerable to the Rainbow Table attack
D. Key stretching is an effective countermeasure against social engineering attacks aimed at credential theft
E. Excessive key stretching can negatively impact user logon experience

Solution: A, B and E.

[1 mark]

(l) Kerckhoff's principle suggests not to rely on security by obscurity. What does that mean?

Solution: Example: It means security shouldn't be achieved by making the encryption method a secret, but keeping the private key secret.

[1 mark]

[Total for Question 5: 13 marks]

Question 6

(a) Refer to the code below. What is most likely to happen when you try to compile and run the program?

```
1 #include <stdio.h>
2 #include <stdlib.h>
3 int main(int argc, char **argv) {
4   printf("The␣secret␣number␣is␣%d\n");
5   return 0;
6 }
```

Listing 1: Sample Code

A. The program will cause a segmentation fault
B. The program will not compile due to the error in line 4.
C. The program will print `The secret number is`
D. The program will print `The secret number is 0`
E. The program will print `The secret number is -1073744844`

Solution: E

[1 mark]

(b) Refer to the sample code below. Suppose the code was compiled using the `-fstack-protector` gcc flag (i.e., stack protector is enabled). Can you craft a malicious input to run arbitrary code? Briefly explain why or why not.

```
1  #include <stdio.h>
2  #include <stdlib.h>
3
4  int main(int argc, char **argv) {
5    char name[256];
6    printf("Please␣enter␣your␣name:\n");
7    gets(name);
8    printf("Hello␣%s!!\n", name);
9    return 0;
10 }
```

Listing 2: Sample Code

Solution: No. The stack protector will place a canary that will detect stack smashing.

[2 marks]

(c) In a buffer overflow attack involving shellcode injection, the saved return address of a function stack frame must be overwritten to point to _____.

A. The address of the `system()` function

B. Somewhere in middle of the NOPSLED
C. Beginning of the stack frame
D. End of the stack frame

Solution: B. Middle of NOPSLED

[1 mark]

(d) True or False? If a C program that is vulnerable to stack buffer overflow is compiled with the `gcc` flag `-z noexecstack`, then an attacker can no longer exploit the software. Briefly explain why.

Solution: False. You can still change program flows or launch return to libc attack.

[2 marks]

(e) Which of the following statements is/are FALSE regarding NOPSLED during shellcode execution?

A. NOPSLED comprises 'No-Operation' CPU instructions repeated many times
B. NOPSLED is not required for a successful shellcode execution if the exact memory location of the shellcode is known
C. NOPSLED must exist at a higher address location in the stack than the shellcode
D. NOPSLED must be adjacent to the shellcode

Solution: C is FALSE. A, B, D are true. Since programs execute from lower to higher address, NOPSLED must be located at a lower address in relation to the shellcode.

[1 mark]

(f) Which function is safer, `strcpy` or `strncpy`?

A. `strncpy` is safer, because you can specify the number of characters to copy.
B. `strcpy` is safer, because it will only copy up to the NULL (0) character.

Solution: A.

[1 mark]

(g) Suppose a socket program is vulnerable to buffer overflow and shellcode injection, and there is no firewall blocking egress/ingress to the server, but the attacker is behind a NAT router with no port forwarding. What kind of shellcode can the attacker use?

A. Only forward (bind) shell will work
B. Only reverse shell will work

C. Either forward or reverse shell will work
D. Neither forward nor reverse will work

Solution: A.

[1 mark]

(h) Suppose a system was completely compromised due to a vulnerable server program running as `root`. What engineering principle was violated?

A. Defence in depth
B. Least privilege
C. The "KISS" principle
D. Segregation of duties

Solution: B. Least privilege.

[1 mark]

(i) Refer to the code below. Suppose this program owned by `root` and the `SETUID` bit is set. How would you attack this program to run arbitrary code as `root`?

```
1  #include <stdio.h>
2  #include <stdlib.h>
3  #include <string.h>
4  #include <sys/types.h>
5  #include <unistd.h>
6  int main(int argc, char **argv) {
7    setreuid(geteuid(), getegid());
8    system("echo␣'Hello␣World!'");
9    return 0;
10 }
```

Listing 3: Hello World

Solution: Modify the PATH environmental variable and create a malicious program named "echo".

[2 marks]

(j) Refer to the code below. Suppose this program owned by `root` is compiled, and the `SETUID` bit is set. How would you attack this program to run arbitrary code as `root`?

```
1  #include <stdlib.h>
2  #include <unistd.h>
3  // This program simply prints the current date and time
4  int main(int argc, char **argv) {
5    setreuid(geteuid(), getegid());
6    system("date");
7    return 0;
```

```
8 }
```

Listing 4: Hello World

Solution: Modify the PATH environmental variable and create a malicious program named “date”.

[2 marks]

(k) Following on from the preceding question, how can you modify listing 4 to make it safe?

Solution: Replace line 8 with `/usr/bin/date` specifying the absolute path to the `date` program.

[2 marks]

(l) Refer to the code below. Where would you place the payload to exploit its weakness?

```
1 #include <stdlib.h>
2 int main(int argc, char **argv) {
3   char buffer[12];
4   char *secret_code= getenv("flag");
5   strcpy(buffer, secret_code);
6   return 0;
7 }
```

Listing 5: Sample Code

Solution: In the environmental variable flag

[1 mark]

(m) Refer to the code below. What would be the payload to force the program to print the content of the file `/etc/passwd`?

```
1 #include <stdlib.h>
2 #include <stdio.h>
3 int main(int argc, char **argv) {
4   char cmd[64];
5   char *target= getenv("f");
6   snprintf(cmd, sizeof(cmd),"file␣%s", target);
7   system(cmd);
8   return 0;
9 }
```

Listing 6: Sample Code

Solution: Example would be `export f="; cat /etc/passwd"`

[2 marks]

(n) True or False? Return-to-libc attack can be successful even if a program is compiled with `-z noexecstack` `gcc` flag.

Solution: True.

[1 mark]

[Total for Question 6: 20 marks]

Question 7

(a) Briefly explain why packet sniffing is not trivial in a switched network.

Solution: The switch maintains a mapping between MAC address and network switch, only sending packets destined for the MAC address to the associated port.

[2 marks]

(b) Which of the following is/are FALSE about DHCP spoofing

A. DHCP spoofing is not possible if DHCP snooping is enabled on all switches
B. DHCP starvation attack is a useful technique before executing DHCP spoofing
C. MITM is possible through DHCP spoofing by forging the default route IP address
D. DHCP spoofing is not possible in a switched network

Solution: D. D is wrong, as you can still do DHCP spoofing if the switch does not implement snooping

[1 mark]

(c) True or False? ARP cache poisoning is only effective if the attacker is on the same broadcast domain as the victim.

Solution: True.

[1 mark]

(d) ARP Cache Poisoning poisons the victim's ARP cache table with a spoofed _____.

Solution: MAC Address

[1 mark]

(e) Refer to the following table for the current IP addresses and MAC addresses of the Gateway, the Victim, and the Attacker. What are the correct `arpspoof` commands to execute in order to perform man-in-the-middle (MITM) attack?

	IP Address	MAC Address
Gateway	10.1.1.254	11:22:33:44:55:66
Victim	10.1.1.100	aa:aa:aa:aa:aa:aa
Attacker	10.1.1.200	bb:bb:bb:bb:bb:bb

A. `arpspoof -t 10.1.1.100 10.1.1.254` and
`arpspoof -t 10.1.1.254 10.1.1.100`

B. `arpspoof -t 10.1.1.200 10.1.1.254` and
`arpspoof -t 10.1.1.200 10.1.1.100`

C. `arpspoof -t 10.1.1.100 10.1.1.200` and
`arpspoof -t 10.1.1.254 10.1.1.200`

D. `arpspoof -t 10.1.1.200 10.1.1.100` and
`arpspoof -t 10.1.1.100 10.1.1.254`

Solution: A.

[1 mark]

(f) Following on from the preceding question, what does the ARP cache table of the victim machine look like after a successful attack?

A.

Address	HWtype	HWaddress	Flags Mask	Iface
10.1.1.254	ether	bb:bb:bb:bb:bb:bb	C	eth0

B.

Address	HWtype	HWaddress	Flags Mask	Iface
10.1.1.200	ether	11:22:33:44:55:66	C	eth0

C.

Address	HWtype	HWaddress	Flags Mask	Iface
10.1.1.254	ether	bb:bb:bb:bb:bb:bb	C	eth0

D.

Address	HWtype	HWaddress	Flags Mask	Iface
10.1.1.200	ether	11:22:33:44:55:66	C	eth0

Solution: A. The gateway address has the attacker's MAC address

[1 mark]

[Total for Question 7: 7 marks]

Question 8

(a) Refer to the PHP code below. What string would you try to inject into the `ip` parameter to list all the files including hidden ones in the `/root` directory? Assume the PHP page exists in the `/var/www/html` directory.

```
1 <?php
2 $ip = $_GET['ip'];
3 $result = shell_exec('ping ' . $ip );
4 echo 'Ping Result: <pre>'.$result.'</pre>';
5 ?>
```

Listing 7: Sample Code

Solution:
`xxx; ls -a /root OR xxx & ls -a /root`

[2 marks]

(b) Following on from the preceding question and the same PHP code, what payload would you inject into the `ip` parameter to get the browser to display a pop-up alert that shows the domain cookie?

Solution:
`xxx; echo </pre><script>alert(document.cookie)</script>`
Note that you have to close the `pre` tag for this to succeed. This is a requirement to get full points.

[2 marks]

(c) Following on from the preceding question and the same PHP code, what is the best strategy for preventing both kinds of injection attacks?

A. using a regular expressions to ensure the `ip` parameter conforms to IPv4 format
B. using parameterised queries instead
C. using black list of dangerous characters such as `$` and `;`
D. disabling javascript on the browser

Solution: A.

[1 mark]

(d) Refer to the PHP code below. Is this vulnerable to reflected or stored XSS (or both or neither)?

```
1 <?php
2 $name = htmlspecialchars($_GET["name"]);
3 echo "<h1>Hello " . $name . "!!!</h1>"
4 ?>
```

Listing 8: Sample Code

A. Reflected XSS
B. Stored XSS
C. Neither
D. Both

Solution: C. Neither, due to the htmlspecialchars function

[1 mark]

(e) Which of the following statements about XSS are FALSE?

A. You can only perform reflected XSS attack using GET requests, whereas both POST and GET requests can be used to perform stored XSS attack
B. Reflected XSS attack requires that the victim is tricked into clicking on a link or visiting a malicious website
C. Both stored and reflected XSS can be prevented by escaping special characters '>', '<', '"', ''' and '&' with HTML entity code.
D. Both reflected and stored XSS can be defeated by setting the `HttpOnly` and `Secure` cookie flags during Set-Cookie

Solution: A and D.

[1 mark]

(f) Which of the following statement(s) is/are FALSE regarding Cross-site request forgery (CSRF) attacks?

A. It can be defeated by setting the 'samesite' attribute on session cookies
B. It can only work with `GET` requests
C. It is typically used to steal the victim's session cookie
D. It relies on the victim having an active and valid session with the target service

Solution: B and C.

[1 mark]

(g) True or False? Session hijacking via cookie theft will not work if the user has already logged out of the service.

Solution: True

[1 mark]

(h) Refer to the PHP code below, which is vulnerable to SQL injection attacks. Write a proof-of-concept exploit code for the `id` parameter so that it will display the entire `user` table.

```
1  <?php
2  // Get input
3  $id = $_GET[ 'id' ];
4  $qry = "select id,name from users where id=" . $id;
5  $result = $conn->query($qry);
6
7  // Get results and output
8  while($row = $result->fetch_assoc()) {
9      echo "User Name is " . $row["name"];
10 }
11 ?>
```

Solution: Inject something like this.

```
1 OR 1=1#
```

[2 marks]

(i) Following on from the preceding question, suppose the `user` table also contains additional fields `password` and `dob` containing each user's password and date of birth, respectively. Write a proof-of-concept payload for the `id` parameter to extract and display these fields (i.e., passwords and birthdates) of all users by using MySQL function `concat(str1, str2, str3, ...)`.

Solution:

```
1 UNION SELECT 1,
  concat(name, '|', password, '|', dob)
  from users#
```

[4 marks]

[Total for Question 8: 15 marks]

Question 9

(a) Theft of intellectual properties such as research data is deemed a loss of

A. Confidentiality
B. Availability
C. Integrity
D. Non-Repudiation

Solution: A. Confidentiality

[1 mark]

(b) Updating systems with latest security patches is considered what kind of control?

A. Administrative
B. Preventative
C. Detective
D. Responsive

Solution: B. Preventative

[1 mark]

(c) What are the other three approaches to addressing risks besides *avoid*?

Solution: transfer, accept, mitigate

[3 marks]

(d) What is the difference between inherent risk and residual risk?

Solution: Inherent risk refer to the level of risk before implementing any controls; residual risk refers to level of risk after controls are implemented.

[1 mark]

(e) Name three security engineering principles (or rules of thumb)

Solution: Any of the 10 mentioned in the lecture

[3 marks]

[Total for Question 9: 9 marks]

End of exam

Question 10

(a) A forensics investigator discovers a PNG image file that appears unusually large. Suspecting that another file may be embedded in the image, `binwalk` is used to analyse the file. Tools like `binwalk` rely on a short binary sequence known as _____to identify beginning of file types such as PE (portable executable) or ZIP files.

Solution: Magic Number

[1 mark]

(b) True or False? Tools like Autopsy and Encase can recover files that have been deleted and purged from trash in a Windows operating system.

Solution: True

[1 mark]

(c) What are the three main file time stamps that investigators examine on a Windows file system?

Solution: Created, Modified, Last Accessed

[3 marks]

(d) In which of the following would you find "recently opened files" in Windows?

A. Memory dump
B. Windows registry
C. C:\temp directory
D. Browser history

Solution: B - Windows Registry

[1 mark]

(e) *Volatility* is a tool for analysing:

A. Hard disk or SSD
B. Windows registries
C. Memory dump
D. Machine logs

Solution: C. Memory dump.

[1 mark]

[Total for Question 10: 7 marks]

Question 11

(a) Which of the following are considered potential indicators of compromise (IOC)?

A. Login by an administrative user at unusual hours
B. A user logging in from multiple countries simultaneously
C. Multiple login failures for different user accounts from the the same IP address
D. A server communicating to a known C2 server.

Solution: A, B, C, and D.

[1 mark]

(b) What is "Threat Hunting" in the security operations centre (SOC)?

A. Act of implementing 'traps' that will alert the Blue Team in the event of a compromise
B. Act of 'hunting' down the attacker and 'hacking back' against the threat
C. Act of searching through logs for signs of anomalies that may indicate a compromise
D. Act of hunting for new and innovative countermeasures against hacking attempts

Solution: C.

[1 mark]

(c) Honeypot servers are useful for:

A. Both deterrence and for attribution
B. Deterrence only
C. Attribution only
D. Neither deterrence nor attribution

Solution: A. Both deterrence and for attribution

[1 mark]

[Total for Question 11: 3 marks]