THE UNIVERSITY of ADELAIDE

Primary Examination, Semester 1, 2022

Cyber Security Fundamentals
COMPSCI 3308

Writing Time: 120 mins

Questions	Time	Marks
Answer all 25 questions	120 mins	100 marks
		100 Total

Instructions

- Begin each answer on a new page.
- Examination material must not be removed from the examination room.
- This is an open book exam.

Materials

- Simple, Non-programmable Calculators Allowed.
- Lecture notes, Personal notes (handwritten or printed), Foreign language dictionary (paper), English language dictionary (paper) Allowed.

DO NOT COMMENCE WRITING UNTIL INSTRUCTED TO DO SO

Question 1 **3 marks**

Please briefly describe the differences between black hat, white hat, and grey hat hackers.

Question 2 **2 marks**

After executing the bash script in Listing 1, there will be a number [f] of files created. In each file there will be [n] random number(s) in range of [min] and [max]. Calculate the values of [f], [n], [min] and [max].

```
#!/bin/bash
rm -rf output
mkdir -p output
for k in {1..50}
do
    filename=$(printf output/%06d $k)
    for j in {1..50}
    do
        num=$((RANDOM % 50 ))
        echo $num > $filename
    done
done
```

Listing 1: numbers.sh

Question 3 **2 marks**

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

Question 4 **3 marks**

What is the key space of the encryption function in Listing 2?

Note:

- ord() function calculates the character code (e.g. ord('A') = 65)
- chr() function is the reverse (e.g., chr(65) = 'A')

```
#!/usr/bin/env python3
def crypt(plain, key):
    output = ''
    for c in plain:
        if(c.isalpha() and c.isupper()):
            x = ord(c) + key
            while (x > 100):
                x -= 36
            output += chr(x)
        else:
            output += c
    return output
```

Listing 2: crypt.py

1. black hat - malicious actors engaging in illegal hacking for personal gain
white hat - defending against black hat using security engineering
grey hat - might engage in illegal activities, but to find faults / other ethical reasons.

2. f: 50
n: 50
min: 0
max: 49

3. advantage - cost / time effective
disadvatage - can miss weaknesses easily

4. 95^n

Question 5

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

A. Alice's public key
B. Bob's public key
C. Alice's private key
D. Bob's private key

[2 marks]

(b) 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. Bob's public key
C. Alice's private key
D. Bob's private key

[2 marks]

[Total for Question 5: 4 marks]

Question 6 **4 marks**

Write the Google search syntax to look for a website where:

- The page body contains the keyword "cybersecurity fundamentals"
- The page title contains "course"
- The page is NOT using "http"
- The page is in the "edu.au" domain

Question 7 **2 marks**

Name two techniques that can be used to force the victim to browse to a malicious website when it tries to browse google.com.

Question 8 **3 marks**

What TCP flags are set in each phase of the TCP three-way handshake?

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

5 a) bob's public key

b) alices private key

6. intext: "Cybesecurity Fundamentals" intitle: "course" - inurl: "http" site: "edu.au"

7. DNS spoofing
   ARP cache poisoning

8. 1. syn
   2. syn-ack
   3. ack

Question 9

You have the network 20.22.2.0/22.

(a) What is the netmask of this network?

[2 marks]

(b) How many hosts are able to be allocated in this network?

[2 marks]

(c) You want to create subnets on this network and the subnets need to support up to 55 hosts each. How many bits would you allocate for the host part of the subnets?

[2 marks]

(d) How many such subnets can you support?

[2 marks]

[Total for Question 9: 8 marks]

Question 10 **5 marks**

Take a look at the C program in Listing 3. Determine if it is vulnerable to Buffer overflow or Format String (or both), and briefly explain why.

```
#include <stdlib.h>
#include <stdio.h>

int main(int argc, char** argv)
{
    char buff[128];
    char result[] = "+";
    printf("Enter your name: ");
    gets(buff);
    printf("Hello %s! Your covid test result is %s.\n", buff,
       result);
    return 0;
}
```

Listing 3: vulnerable.c

Question 11 **4 marks**

Refer to the program in Listing 3 (as same as the one in Question 10).

Is it possible to change the value of 'result' by injecting several '-'s into the memory (to cause a buffer overflow and overwrite the 'result' as '-')? Briefly explain why.

9. a) first 22 bits

1111 1111 1111 1111 1111 1100 0000 0000

255. 255. 252. 0

b. 10 bits left

2^{10} = 1024 addresses

−2 for broadcast, network interface

= 1022 hosts

c. $2^x > 55$

$x = 6$

$2^6 = 64$

∴ 6 bits for hosts

d) 4 bits remaining

$2^4 = 16$ subnets.

10. Buffer overflow - No. result comes before buff in stack and cannot be written into from gets

format string - Yes. specifying %n into buff will overrite result with # characters so far - could do Hello + 94 characters + %.n to get result of +99.

11. no it's not, a buffer overflow is not possible, because the only other variable (buff) is located beneath result in stack. Since we write top-down, result cannot be overwritten.

Question 12 **2 marks**

In which of the following scenario(s) is DHCP spoofing attack possible?

A. Victim's machine is on the same subnet as the Attacker, connected to a switched (Layer 2 switch) network

B. Victim's machine is on the same subnet as the Attacker, connected to a non-switched (hub) network

C. Victim's machine is on a different subnet from the Attacker

Question 13 **3 marks**

Refer to the code in Listing 4. Suppose the code was compiled using the `-fstack-protector` **gcc** flag (i.e., stack protector is enabled). Is it possible to get the program to print "Yes!"? Briefly explain why or why not.

```
1  #include <stdio.h>
2  #include <stdlib.h>
3
4  int main(int argc, char **argv) {
5    char ans[] = "N";
6    char buf[12];
7    gets(buf);
8    if (0 == strcmp(ans, "Y")) {
9      printf("Yes!");
10   }
11   return 0;
12 }
```

Listing 4: fstack-protector.c

Question 14 **3 marks**

Take a look at the code in Listing 5. 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 5: hello-world.c

12. A and B - must be on same subnet

13. Yes it is. Stack protector stops execution of code from stack. This is a buffer overflow vulnerability from gets. ans comes after buf in the stack and since we write from high to low addresses, ans can get overwritten.

14. ~

Question 15

Refer to the code in Listing 6, a simple program that just echos user input (`argv[1]`).

```
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    char buff[100];
9    snprintf(buff, 100, "echo %s", argv[1]);
10   system(buff);
11   return 0;
12 }
```

Listing 6: echo.c

(a) Is this program vulnerable to buffer overflow? Explain.

[2 marks]

(b) What malicious input could be provided to run arbitrary code as `root`, if the SETUID bit is set, and the owner is `root`? Write a proof-of-concept exploit that prints the content of the shadow file (/etc/shadow).

[2 marks]

[Total for Question 15: 4 marks]

Question 16

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

[1 mark]

15. a) no its not, snprintf is a safe function

b) ~

16 a) MQE address

(b) 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 10.1.1.200 10.1.1.254` and
`arpspoof -t 10.1.1.200 10.1.1.100`

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

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

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

[2 marks]

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

A.

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

B.

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

[2 marks]

(d) Which of the following is/are effective countermeasures against MITM attacks?

A. Using a host-based firewall to block ARP responses

B. Using VPN tunnel to a trusted gateway

C. Using SSL for all web browsing

D. Avoiding the use of plaintext protocols like FTP and TELNET

[2 marks]

[Total for Question 16: 7 marks]

b) option B - change gateway and victim to attacker

c) option C - gateway IP is now associated with attacker MAC address

d) B, C, D.

Question 17 **2 marks**

Refer to the PHP code in Listing 7, which is vulnerable to SQL injection attacks. Write a proof-of-concept exploit code for the id parameter so that it will display all the students grades (the entire grades table).

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

Listing 7: inject.php

Question 18

Take a look at the PHP code in Listing 8.

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

Listing 8: ping.php

(a) 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.

[3 marks]

(b) What payload would you inject into the IP parameter to get the browser to display a pop-up alert that shows the domain cookie?

[3 marks]

(c) What is the best strategy for preventing these kind of injection attacks?

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

[2 marks]

[Total for Question 18: 8 marks]

17. " ' OR ' 1 ' = ' 1 '

18. a) " ; ls -a /root "

b) " ; </pre> <script> alert (document. cookie) </script>

c) All 4 are viable . A only works client side
C, D are good, but can be worked around.
Combine B, C, D for best result.

Question 19

(a) True or False? For a Cross-Site Request Forgery (CSRF) attack to succeed, the victim must have an active (logged-in) session with the target application.

[2 marks]

(b) True of False. An application that is vulnerable to GET type CSRF can be exploited simply by tricking the victim to load an image on the browser.

[2 marks]

(c) Which of the following mitigation strategies are effective against CSRF attacks?

A. Use the Secure flag in the Set-cookie response header
B. Using randomised tokens to validate each request
C. Use the HttpOnly flag in the Set-cookie response header
D. Use the Referrer http request header to check for same-origin

[2 marks]

[Total for Question 19: 6 marks]

Question 20

(a) Having services running as non-root is an example of which security engineering principle?

[2 marks]

(b) List other three security engineering principles.

[2 marks]

[Total for Question 20: 4 marks]

Question 21 **4 marks**

Calculate the annualised loss expectancy (ALE) in the following scenario describing the risk of fire damaging the University's Data Center.

- Data Center is worth $5 million dollars
- Fire takes place every 10 years
- 40% of the equipment is damaged beyond repair before the fire is put out.

Question 22 **5 marks**

In the scenario of a global pandemic, it is almost certain that the University is impacted by having a significant reduction in student enrolment. Against this threat, the University has adopted online teaching methodology, which decreased the impact to moderate reduction in student enrolment. Make a qualitative risk analysis for this scenario and calculate the inherent risk and residual risk.

19. a) true

b) true.

c) B and D

20. a) least privelage

b) 1. keep security simple

2. make security useable

3. fail securely

21. 5 mil total

40 %. needs to be replaced

5,000,000 x 40 %.

= 2,000,000 every 10 years

= 200,000 per year = ALE

22. threat - pandemic

impact (before) = significant (4)

mitigation - online teaching

impact (after) = moderate (3)

likelihood : almost certain (5)

inherent risk = 4 x 5 = 20

residual risk = 3 x 5 = 15

Question 23 **4 marks**

What kind of controls are the following:

1. Card access to the datacenter: _____
2. Developers should use the Hungarian notation in their code: _____
3. Users login using 2-factor authentication: _____
4. Snort installed in the DMZ: _____

Question 24 **4 marks**

Determine if the following are a threat, a vulnerability or a risk:

1. SQL injection: _____
2. Unpatched OS: _____
3. Black hat hacker: _____
4. Computer infected by a black hat hacker: _____

Question 25

(a) Which Information Security Management framework privides certification?

A. ISO 27001
B. ISO 27002
C. NIST Cyber Security Framework
D. CIS Critical Security Controls

[2 marks]

(b) How many mitigation strategies are recommended to be implemented as a baseline by the Australian Cyber Security Center (ACCS)?

[2 marks]

[Total for Question 25: 4 marks]

End of exam

23. 1. physical - preventive
2. technical - preventive
3. administrative - preventive
4. technical - detective

24. 1. risk - unparamterisation (vulnerability) + hacker (threat)
2. vulnerability
3. threat
4. vulnerability

25 a) A.

b) 8.