THE UNIVERSITY of ADELAIDE

Replacement Examination, Semester 1, 2018

Cyber Security Fundamentals
COMPSCI 3308, 7308

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

Questions	Time	Marks
Answer all 9 questions	120 mins	120 marks 120 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

Security Assessment

Question 1

(a) What is the first stage in a typical ethical hacking assignment according to PTES?

A. Pre-Engagement
B. Intelligence Gathering
C. Network Scanning
D. Social Engineering

Solution: A.

[1 mark]

(b) Which of the following is NOT true about "Black Box" testing?

A. It is usually time-boxed
B. It has the advantage of simulating a real attack
C. It is likely to find more weaknesses compared to White Box testing
D. It is considered cost-effective as it discovers weaknesses that are likely to be found

Solution: C. White Box testing usually reveals more issues.

[1 mark]

(c) Which testing method most closely simulates a real attack scenario, Penetration Testing, or Red Teaming?

A. Red Teaming
B. Penetration Testing
C. They are comparable
D. Neither

Solution: A. Red Teaming.

[1 mark]

(d) Why are vulnerability assessments more likely to produce false positives compared to penetration testing?

Solution: Vulnerability assessment relies on version numbers and finger prints for software/service versions, which can lead to false positives. Pentests positive proves exploitability, which means virtually no false positives.

[2 marks]

(e) The planning or pre-engagement phase of a penetration testing includes which of the following?

A. Agreeing on the scope and exceptions
B. Agreeing on communication methods, including emergency contacts
C. Agreeing on time frame and fees
D. Signing an engagement letter formally giving permission to test

Solution: A, B, C, and D.

[2 marks]

(f) In a Red Teaming exercise, what is the role of the Blue Team?

A. Supporting the Red Team to find weaknesses
B. Detecting and responding to attempts at exploiting weaknesses by the Red Team
C. Reporting incidents to the police when attacks are detected
D. Blocking ports on the perimeter firewall to prevent the Red Team from accessing critical systems

Solution: B. Detecting and responding to exploits and exploit attempts.

[1 mark]

(g) Which of the following statements are true about a vulnerability with CVSS 3.0 vector string: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H (Score 5.9)?

A. You can exploit this remotely
B. The attack complexity is high
C. Has High impact on Integrity
D. Has High impact on Availability
E. User Interaction is not required

Solution: A, B, C, D, E (all are true)

[2 marks]

(h) Meltdown and Spectre are what kind of attack?

A. Ransomware
B. Denial of service
C. Brute-force
D. Side-channel

Solution: D. Side-channel attack.

[1 mark]

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

A. No. Vulnerabilities generally refer to bugs in software systems.

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]

[Total for Question 1: 12 marks]

Security Engineering

Question 2

(a) The security engineering principle used when malware is scanned at the email gateway using one antivirus engine, then by the email client by another antivirus engine is called _____.

Solution: Defence in depth

[2 marks]

(b) What security engineering principle is applied when a developer is prevented from accessing UAT and Production systems, thereby preventing uploading of untested code?

Solution: Least Privilge OR Segregation of Duties

[2 marks]

(c) In a sound security engineering, the cost (including implementation and any negative impact on productivity) of a control must be commensurate with the _____of the asset.

A. Integrity
B. Value
C. Availability
D. Confidentiality

Solution: B. Value of the asset.

[1 mark]

(d) What has traditionally been the problems with biometric-based authentication?

A. False rejection (Type I errors)
B. False acceptance (Type II errors)

Solution: A False rejection, which is a Type I error.

[1 mark]

(e) True of False. In a Mandatory Access Control (MAC) the owners of objects can modify who can access the objects.

Solution: False

[1 mark]

(f) True or False. Linux operating system implements Discretionary Access Control for its file system security.

Solution: True

[1 mark]

[Total for Question 2: 8 marks]

Information Security and Risk Management

Question 3

(a) When you mitigate a risk, the residual risk is typically becomes

A. Higher than the inherent risk
B. Lower than the inherent risk
C. Unchanged from the inherent risk
D. Negligible

Solution: B. Lower.

[1 mark]

(b) In ISO/IEC 27001, what artefact is used to document the subset of normative controls applicable to the organisation?

A. List of Application of Controls
B. Statement of Applicability
C. Organisational Control Enumeration
D. RIsk Assessment Report

Solution: B. Statement of Applicability

[1 mark]

(c) Refer to the matrix in Figure 1. Suppose the Risk Severity of DDoS is rated Hazardous (4) for this company. If the company wishes to bring the residual risk to "Acceptable", mitigations must be implemented so that the Risk Likelihood becomes _____.

Solution: Extremely Improbable(1)

[2 marks]

(d) Ensuring all systems are up-to-date with security patches is is a type of which kind of control?

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

Solution: A. Preventive

[1 mark]

(e) Ransomware causes impact on which attribute of information security?

A. Confidentiality
B. Availability

Risk Likelihood	Risk Severity				
	Catastrophic 5	Hazardous 4	Major 3	Minor 2	Negligible 1
Frequent 5	Unacceptable	Unacceptable	Unacceptable	Tolerable	Tolerable
Occasional 4	Unacceptable	Unacceptable	Tolerable	Tolerable	Tolerable
Remote 3	Unacceptable	Tolerable	Tolerable	Tolerable	Acceptable
Improbable 2	Tolerable	Tolerable	Tolerable	Acceptable	Acceptable
Extremely Improbable 1	Tolerable	Acceptable	Acceptable	Acceptable	Acceptable

Figure 1: Risk Matrix

C. Integrity
D. Non-repudiation

Solution: B. Availability

[1 mark]

(f) An email platform where a person cannot deny having sent an email by requiring digital signature on all emails protects which of the following security attribute?

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

Solution: D. Non-Repudiation

[1 mark]

(g) A ransomware attack threatens which of the following security attributes?

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

Solution: B. Availability

[1 mark]

(h) In information security, terms RPO and RTO are used in which of the following activities?

A. Business Continuity Planning
B. Disaster Recovery Planning
C. Penetration Testing
D. Red Teaming

Solution: A and B.

[1 mark]

[Total for Question 3: 9 marks]

Reconnaissance

Question 4

(a) What Google search modifier can you use to search for the keyword "password" but only instances where the keyword appears in the URL of the webpage?

Solution: inurl:password

[1 mark]

(b) What Google search modifier can you use to search for the keyword "password" but only instances where it appears in a file with extension "bak"?

Solution: password ext:bak

[1 mark]

(c) Which of the following techniques can be used to find out hosts and subdomains of spotify.com? Select all that are applicable.

A. Using the Google or Bing search string site:spotify.com
B. Attempting to perform zone transfer from the Spotify name servers
C. Performing brute-force DNS lookup using dnsenum
D. Using online intelligence tools such as censys.io, shodan.io, and Netcraft
E. Using nmap to scan for hosts in network ranges owned by spotify.com and performing reverse DNS lookup

Solution: A, B, C and D and E. All these are useful techniques.

[1 mark]

(d) Which of these techniques are active (NOT passive) reconnaissance?

A. Using nmap to scan for open ports and services
B. Using Google search techniques to find information
C. Looking up Facebook and LinkedIn pages of employees
D. Going to a pub near a headquarter and become chummy with an employee
E. Calling up the company's Helpdesk and phishing for information
F. Sitting in the company's car park and identify WiFi SSIDs

Solution: A, D, E are active reconnaissance. B, C, F are passive.

[1 mark]

(e) What tool(s) can be used to find out the technologies used by a company several years in the past?

Solution: Wayback machine (Internet Archives) and or Netcraft

[2 marks]

[Total for Question 4: 6 marks]

Web Application Security

Question 5

(a) Which function in Burp Suite would you use to perform a dictionary attack on an input field?

A. Spider
B. Cluster Bomb
C. Repeater
D. Intruder

Solution: D. Intruder

[1 mark]

(b) Which of the following statements about reflected vs stored XSS are TRUE? Select all that apply.

A. Reflected XSS require the attacker to entice the victim into clicking on a link or visiting a malicious site
B. Stored XSS is also known as persistent XSS and reflected XSS is also known as non-persistent XSS
C. Reflected XSS can be prevented by input validation, but stored XSS require output validation
D. Both reflected and stored XSS can be defeated by setting the HttpOnly and Secure flags during Set-Cookie

Solution: A and B. C: both can be thwarted by input or output validation. D: this will prevent access to cookie, but does not stop script running.

[2 marks]

(c) Refer to the PHP code below. Is this vulnerable to XSS? If yes, write a sample payload for the "id" parameter that will display a browser pop-up.

```
1 <?php
2 $id = $_GET['id'];
3 echo "<script> var id=" . $id . ";</script>"
4 ?>
```

Solution: 1; alert(1)

[2 marks]

(d) What can you inject into the 'color' parameter to get the browser to display a JavaScript alert() popup?

```
1 <?php
2 $color = $_GET['color'];
```

```
3 echo "<h1 style='color:" . $color . "'>Hello World</h1>"
4 ?>
```

Solution:

```
red'><script>alert(1);</script>
```

[2 marks]

(e) How would you modify the code from the previous question to make it immune to XSS using the function htmlspecialchars()?

Solution: For example, change line 3 to
$color = htmlspecialchars($_GET['color']);

[2 marks]

(f) If you suspect that there exists a file name with a '60s movie title, how would you combine the tools *cewl* and *dirb* to find the folder?

Solution: Use cewl to build a word list, then brute-force using dirb

[2 marks]

(g) A web application sets a cookie using the Set-cookie HTTP response header with the following key-value pair: "logged_in=true" upon logon, and set it to "logged_in=false" when the user clicks on the logout button. Is this a safe practice?

Solution: No. Cookie values can easily be manipulated by the client and should not be used for determining an active session.

[2 marks]

(h) Refer to the code below. What string would you try to inject into the "file_name" parameter to get (1) content of the */etc/passwd* file? (2) list all the files in the current directory,including hidden ones in the /root directory? Assume the PHP page exists in the */var/www/html/tools/* directory.

```
1 <?php
2 $file = $_REQUEST['file_name'];
3 $result = shell_exec('cat ./' . $file );
4 echo 'CAT output: <pre>'.$result.'</pre>';
5 ?>
```

Solution:

```
(1) ../../../../etc/passwd
(2) xxx; ls -a /root OR xxx & ls -a /root
```

[4 marks]

(i) Refer to the code below. Is this vulnerable to SQL injection? If yes, what value would you inject into the "id" parameter so that you will get it to display the entire users table, remembering that "#" comments out SQL statement.

```
1  <?php
2  // Get input
3  $id = $_REQUEST[ 'id' ];
4
5  // Check database
6  $query  = "SELECT first_name, last_name FROM users WHERE
       user_id = '$id';";
7  $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query )
8
9  // Get results
10 while( $row = mysqli_fetch_assoc( $result ) ) {
11     // Get values
12     $first = $row["first_name"];
13     $last  = $row["last_name"];
14
15     // Feedback for end user
16     $html .= "<pre>ID: {$id}<br />First name: {$first}<br />
           Surname: {$last}</pre>";
17 }
18 ?>
```

Solution: Inject something like this is sufficient.

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

[4 marks]

(j) Continuing from the same code in the previous question, suppose the user table contains two additional columns: $password$ and tfn (Tax File Number) and you want to retrieve value from them as well. What value would you inject into the id column?

Solution: Inject something like the following. Give partial points if UNION and CONCAT are mentioned.

```
1' UNION SELECT id, CONCAT(password, tfn) from users#
```

[4 marks]

(k) While testing for SQL injection, the tester encounters the error shown in Fig. 2. What SQL syntax would have generated this error? How would the attacker proceed to fix this error?

Solution: UNION request.Try changing the number of columns by trial and error.

[2 marks]

(l) True or False. Cross-Site Request Forgery (CSRF) is an attack against the web application server, and do not require user interaction.

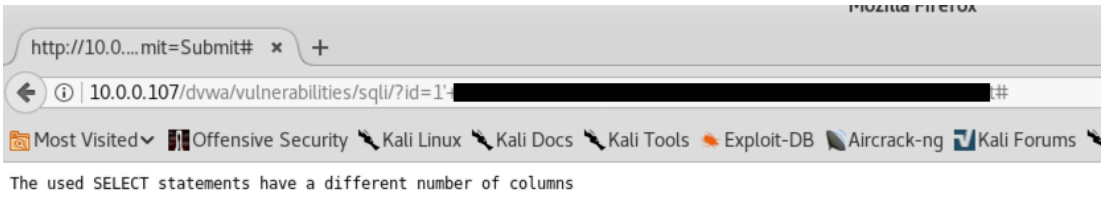

Figure 2: SQLi Error

Solution: False.

[1 mark]

(m) For a Cross-Site Request Forgery (CSRF) attack to succeed, the victim user must _____.

A. Have the web application displayed on the browser
B. Have JavaScript enabled on the browser
C. Actively click on a malicious link crafted by the attacker.
D. Have an active logged-in session with the web application

Solution: D.

[1 mark]

(n) What are two of the recommended countermeasure to CSRF? Choose two from below.

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

Solution: A and D.

[1 mark]

(o) The code below is vulnerable to SQL injection on the parameter 'id', but the page does not return actual results from SQL queries. Is this page vulnerable to SQL injection?

```
1 <?php
2 $id = $_GET[ 'id' ];
3
4 // Check database
5 $getid  = "SELECT first_name, last_name FROM users WHERE
      user_id = '$id';";
6 $result = mysqli_query($GLOBALS["___mysqli_ston"],  $getid )
      ;
7
```

```
8  // Get results
9  $num = @mysqli_num_rows( $result ); // The '@' character
       suppresses errors
10 if( $num > 0 ) {
11     // Feedback for end user
12     $html .= '<pre>User ID exists in the database.</pre>';
13 }
14 else {
15     // User wasn't found, so the page wasn't!
16     header( $_SERVER[ 'SERVER_PROTOCOL' ] . ' 404 Not Found'
           );
17     // Feedback for end user
18     $html .= '<pre>User ID is MISSING from the database.</
           pre>';
19 }
20 ?>
```

A. Yes, it is vulnerable to normal SQL injection
B. Yes, it is vulnerable to blind SQL injection
C. Yes, it is vulnerable to speculative SQL injection
D. No, it is not vulnerable to SQL injection

Solution: B. Yes, it is vulnerable to blind SQL injection

[1 mark]

(p) For the code in the previous question, compose a payload for the id parameter that helps to determine if the $first\_name$ of the user with $id = 1$ starts with "A". Note: The MySQL function to get the nth character of a string is $substr(str, n, 1)$.

Solution:

```
1' AND substr(first_name,1,1) = "A"#
```

[2 marks]

(q) What are some common methods for preventing SQL injection attacks? Select all that apply.

A. Using the htmlchars() function to escape dangerous characters in the user input
B. Using an intrusion detection system on the firewall
C. Using prepared statements or parameterised queries
D. Using a safe database API available on the server-side framework, such as PDO for PHP

Solution: C and D.

[1 mark]

[Total for Question 5: 34 marks]

```
39 7.129726582   217.59.53.41        10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
40 7.129730167   106.35.56.249       10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
41 7.129734499   199.66.74.199       10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
42 7.129737372   92.90.69.148        10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
43 7.129741213   92.209.86.238       10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
44 7.129744700   1.135.168.94        10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
45 7.129747519   95.8.182.58         10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
46 7.129750755   35.103.176.232      10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
47 7.129753581   69.254.49.247       10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
48 7.129756497   134.145.240.208     10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
49 7.129761842   186.18.16.210       10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
50 7.129764437   184.189.248.40      10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
51 7.129767804   146.101.52.165      10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
52 7.129771302   194.161.47.152      10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
53 7.129775214   175.35.215.179      10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
54 7.129777881   129.66.6.81         10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
55 7.129780682   209.182.94.226      10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
56 7.129783242   223.15.150.58       10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
57 7.129786626   90.23.190.101       10.0.0.134          TCP        44 61682 → 22 [SYN] Seq=0 Win=10
```

Figure 3: Wireshark capture of an Nmap scanning

Network Security and Remote Exploitation

Question 6

(a) Refer to figure Fig.3 showing a Wireshark capture of an Nmap scan in progress. Which of the following Nmap commands could have resulted in this packet capture?

A. nmap -sS -Pn -p 22 -SPOOF=RND 100 10.0.0.134
B. nmap -sX -Pn -D 217.59.53.41 10.0.0.134
C. nmap -sV -Pn -D 217.59.53.41 10.0.0.134
D. nmap -sS -Pn -p 22 -D RND:100 10.0.0.134

Solution: D

[1 mark]

(b) Describe two (2) ways you can execute DNS poisoning.

Solution: (1) Change local hosts file, (2) intercept and poison DNS response to a client (3) poison response sent back to a DNS server.

[2 marks]

(c) Refer to Figure 4. If the attacker wants to intercept all traffic between the two victim computers A and B, he needs to poison the ARP cache as follows:

A. On Computer A: point 192.168.0.125 to 192.168.0.111; on Computer B: point 192.168.0.123 to 192.168.0.111
B. On Computer A: point 192.168.0.125 to aa:bb:cc:66:66:66; on Computer B: point 192.168.0.123 to aa:bb:cc:66:66:66
C. On Computer A: point 192.168.0.125 to aa:bb:cc:11:22:55; on Computer B: point 192.168.0.123 to aa:bb:cc:66:66:66
D. On Computer A: point 192.168.0.125 to aa:bb:cc:66:66:66; on Computer B: point 192.168.0.123 to aa:bb:cc:11:22:44

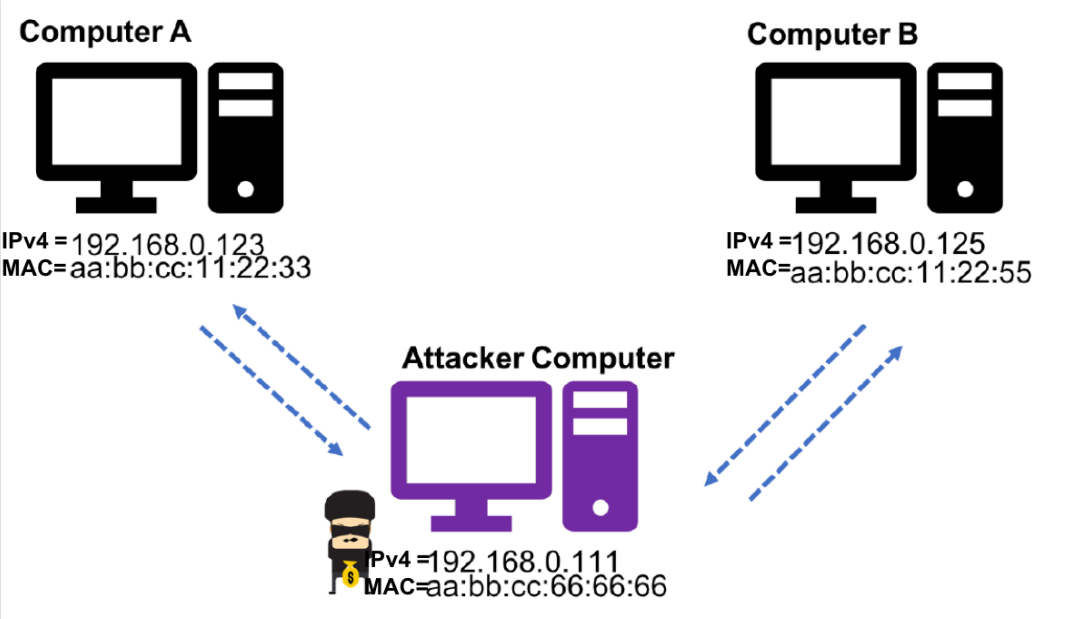

Figure 4: ARP Cache Poisoning

Solution: B. Both computer A and B ARP caches must be poisoned so that respective IPs map to the attackers's MAC address.

[1 mark]

(d) You found a vulnerability that is exploitable over the network on a server, but there is a firewall in front of the server that prevents you from opening any ports. Which of the following payloads should you use to gain remote shell?

A. Reverse shell
B. Forward (bind) shell
C. Either may work
D. Neither will work

Solution: A. Reverse shell

[1 mark]

(e) Suppose an attacker successfully launches ARP Cache Poisoning and is able to intercept and listen to all traffic between the victim computer and the gateway. If the victim computer connects to https://gmail.com/ and login using user name and password, can the attacker steal the password? Why or why not?

Solution: No. TLS protects the HTTP traffic, and the attacker is unable to sniff traffic without presenting with a false TLS certificate,

which would cause a certificate error. You may be able to steal if the user accepts the fake certificate...

[2 marks]

[Total for Question 6: 7 marks]

Cryptography

Question 7

(a) In digital signature, the document's message digest is encrypted with

(b) True or False. In Public Key Cryptography, the public key of the recipient is typically used to encrypt the entire messages that the sender would like to deliver to the recipient.

Solution: False. The public key is typically used to encrypt and agree on a temporary secret key.

[1 mark]

(c) In RSA public-key cryptography, what is the relationship between p, q, n, d, e, (the first prime, the second prime, the modulus, the private exponent, and the public exponent respectively)? Select all choices that are true.

A. $message = \{message\}^{d*e}\ mod(n)$
B. $plaintext = \{ciphertext\}^{d}\ mod(n)$
C. $d * e = 1\ mod\{(p-1)(q-1)\}$
D. $n = (p-1)(q-1)$

[1 mark]

(d) In cryptography, what is a trap door function?

Solution: Trap door is a function that is computationally easy to calculate in one direction, but difficult in the reverse without knowing a secret.

[2 marks]

(e) Cryptographic hash function provides which aspects of information security? Choose ll choices that apply.

A. Availability
B. Integrity
C. Confidentiality
D. All of the above

Solution: B only. Hash function does not provide any means to protect availability or confidentiality.

[1 mark]

(f) If two $A = B\ \oplus\ K$ and $C = D\ \oplus\ K$ what can you say about $A \oplus C$?

Solution: $A \oplus C = B\ \oplus\ D$

[2 marks]

(g) The Enigma Machine used a kind of a:

A. Block cipher
B. Stream cipher
C. Polygraphic Substitution cipher
D. Monographic Substitution cipher

Solution: C. Polygraphic substitution cipher

[1 mark]

(h) What is an effective attack against monographic substitution cipher?

Solution: Frequency analysis

[2 marks]

[Total for Question 7: 11 marks]

Memory Attacks

Question 8

(a) Uninstantiated static variables and global variables are stored in which memory segment?

A. The Stack
B. The Heap
C. The BSS
D. The TEXT
E. None of the above

Solution: C. BSS

[1 mark]

(b) Which one of these statements are true about the STACK and the HEAP in the x86 architecture?

A. The Stack "grows" from lower memory address to higher, and the Heap grows from higher to lower memory address.
B. The Stack "grows" from higher memory address to lower, and the Heap grows from lower to higher memory address.
C. Both the Stack and the Heap goes from low to high address space.
D. Both the Stack and the Heap goes from high to low address space.
E. None of the above

Solution: B. The stack grows "down" from higher to lower; the heap grows from lower address to higher.

[1 mark]

(c) What is a shellcode?

A. A small piece of code that is injected into a program to launch a shell
B. A small piece of code that is injected into a program to execute commands
C. A type of shell that causes a buffer overflow to occur on the STACK
D. A type of shell that causes a program to crash
E. None of the above

Solution: B. Although called "shell"code it's an arbitray set of instructions that is embedded as payload when attacking a vulnerable program

[1 mark]

(d) How can you attack the vulnerable C code below so that it will print out "Yay!"? Assume that this is compiled with the -fno-stack-protector gcc switch.

```
1  #include <stdio.h>
2  #include <stdlib.h>
3
4  int main(int argc, char** argv){
5      char[] grade = "F";
6      char buf[68];
7      gets(buf);
8
9      if (0 == strcmp(grade, "HD") {
10         printf("Yay!");
11     }
12     else {
13         printf("Noooooo!");
14     }
15     return 0;
16 }
```

Solution: Run, for example, with argument 'python -c 'print "A"*68 + "HD\x00"' Can also do printf or inline perl

[4 marks]

(e) Briefly explain what happens to the compiled binary when you add the compile option -$fstack\text{-}protector$ in the gcc compiler.

Solution: The compiler inserts a canary near the top of the stack frame to detect stack smashing.

[2 marks]

(f) How does ASLR help to prevent buffer overflows?

Solution: ASLR randomises memory allocation during each program execution to make it harder for the attacker to craft an attack.

[2 marks]

(g) Briefly explain what a NOP Sled is and how it can be useful for exploiting a vulnerable program.

Solution: The NOP sled is a series of no-operations (
90) instructions that can be used as a "landing pad" for exploits. When the exact location of the exploit code is not know, you can point to an area of NOP instructions.

[2 marks]

(h) Which memory segment can be attacked in the following code in order to get the program to print "Yay!"? Indicate the line number where the overflow will occur.

```
1  #include <stdlib.h>
2  #include <stdio.h>
3
4  struct data {
5      int flag;
6      char name[64];
7  };
8
9  int main(int argc, char **argv) {
10     struct data *d;
11     d = calloc(sizeof(struct data));
12     strcpy(d->name, argv[1]);
13     if (flag) {
14         printf("Yay!");
15     }
16     return 0;
17 }
```

Solution: The HEAP. Line 11.

[1 mark]

(i) Which memory segment can be attacked in the following code so that the program will print "Cowanbanga!"? Which line does the exploit take place?

```
1  #include <stdlib.h>
2  #include <stdio.h>
3
4  int target;
5
6  void vuln(char *string) {
7      printf(string);
8
9      if(target) {
10         printf("Cowanbanga!\n");
11     }
12 }
13 int main(int argc, char **argv) {
14     vuln(argv[1]);
15 }
```

Solution: Any memory segment can be attacked. Line 7.

[1 mark]

(j) Even if you compile a C program using Stack Execution Prevention ($-noexecstack$) option enabled, buffer overflow can still lead to code

execution. Give an example of an attack method that circumvents these countermeasures.

Solution: (1) Executing code in libc, (2) executing code in the heap.

[1 mark]

(k) What are the safer versions of the C functions $gets$ and $strcpy$?

Solution: fgets and strncpy

[2 marks]

(l) Refer to the code below. Which line is vulnerable to buffer overflow? What argument would you provide it to overflow the buffer and overwrite the variable x?

```
1  #include <stdlib.h>
2  #include <stdio.h>
3  #include <string.h>
4
5  void fn(char *str)
6  {
7      volatile int x;
8      char buffer[2020];
9
10     x = 0;
11
12     sprintf(buffer, str);
13
14     if(x) {
15         printf("Yes!");
16     }
17 }
18
19 int main(int argc, char **argv)
20 {
21     char buffer[12];
22     strncpy(buffer,argv[1],sizeof(buffer));
23     fn(buffer);
24     return 0;
25 }
```

Solution:

`%02020xa`

[4 marks]

[Total for Question 8: 22 marks]

Miscellaneous

Question 9

(a) Which of the following personal characteristics are deemed important for an ethical hacker? Select all that apply.

A. Lateral thinking, or thinking outside of the box
B. Being able to think like the bad guys
C. Persistence and patience
D. Good communication skills
E. Sound ethical principles

Solution: All of the above

[1 mark]

(b) If you discover a critical "0-day" security vulnerability in a popular software or an online service you should:

A. Post it on Twitter and Facebook so that everyone can take appropriate precautions
B. Inform the vendor/service provider and plan on a responsible disclosure
C. Go to a dark web market and sell the vulnerability to the highest bidder
D. Create a proof-of-concept (POC) exploit code and publish on Github

Solution: B.

[1 mark]

(c) The phenomenon whereby the consumer opts to buy cheaper but less secure software due to asymmetry of information (i.e., the buyer does not know which software is more secure) is known as the:

A. Market for Oranges
B. Market for Bananas
C. Market for Kiwis
D. Market for Lemons

Solution: D. Market for Lemons

[1 mark]

(d) What can help consumers decide on which software or services are secure?

Solution: Certification schemes like Common Criteria as well as independent audit reports such as SOC reports based on SSAE16.

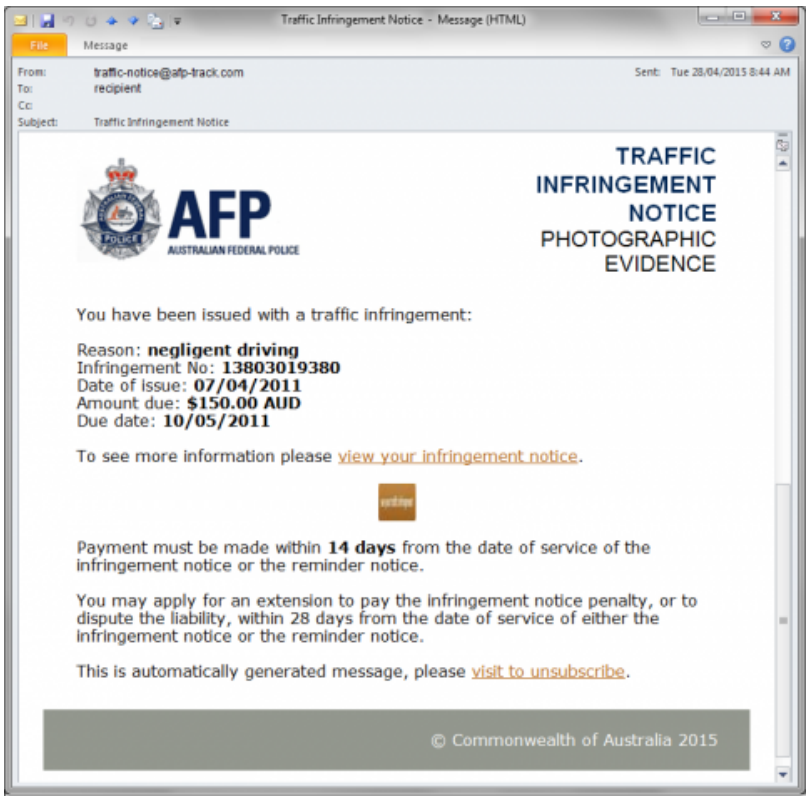

Figure 5: AFP Phishing

[1 mark]

(e) Refer to the phishing email in Fig.5. Which of Caldini's "Six Principles of Persuasion" is used in this phishing?

A. Liking
B. Consistency
C. Emergency
D. Scarcity
E. Social Proof
F. Authority

Solution: F. Authority

[1 mark]

(f) What is the name of the model developed by Lockheed Martin that helps to portray an end-to-end malicious attack using malware?

A. Cyber Exploit Chain
B. Cyber Kill Chain
C. Cyber Malware Chain
D. Cyber Attack Chain

Solution: B. Cyber Kill Chain

[1 mark]

(g) Bcrypt uses hash _____to increase computational effort required for calculation.

A. Stretching
B. Salting
C. Substitution
D. Reverse Engineering

Solution: A. Stretching

[2 marks]

(h) True or False? "Salting" SHA512 password hashes makes it considerably harder to crack the password of a single user.

Solution: False. For a single user, it does not significantly increase computational effort. It is computationally hard to launch an off-line attack or create a rainbow table.

[1 mark]

(i) In security, a Rainbow Table is a _____table used for reversing _____.

Solution: precomputed; password hashes (or just hashes)

[1 mark]

(j) Metasploit is a framework written in the _____language. The two main types of modules are Exploits and _____.

Solution: Ruby, Payloads

[1 mark]

[Total for Question 9: 11 marks]

End of exam