THE UNIVERSITY of ADELAIDE

(Draft1) Primary 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) Which of the following statements are true regarding Black Hat, Grey Hat, and White Hat hackers.

A. White Hats do not break the law, but Black Hats and Grey Hats break laws to achieve their objectives

B. White Hats generally do not break laws, but reserve the right to retaliate (attack back) against Black Hat and Grey Hat hackers

C. Grey Hats refer to those people who are White Hat hackers during the day, and Black Hat hackers outside of business hours

D. White Hat hackers are also known as Ethical Hackers

Solution: A, B and D.

[1 mark]

(b) Which of the following is NOT one of the asymmetric forces in play between black hat and white hat hackers that give the bad guys an unfair advantage?

A. Ability to work outside of laws and regulations

B. Availability of time and resources

C. Ability to work any time

D. Level of education

E. Success factor

Solution: D. Education

[1 mark]

(c) What are some important traits for becoming an effective cybersecurity specialist?

A. Solid ethical foundation

B. Sound communication skills

C. Adversarial thinking

D. Not being afraid to break the law

E. Autodidactic (self-taught)

Solution: All except D.

[1 mark]

[Total for Question 1: 3 marks]

Question 2

(a) True or False? Collecting OSINT (Open Source Intelligence) risks alerting the Blue Team.

Solution: False.

[1 mark]

(b) Spoofing the product name and version number in a network service banner (e.g., advertising IIS Web Server as Apache 2) is considered to be "security by _____".

Solution: Obscurity

[1 mark]

(c) Which of these represents the Google search syntax for looking up Excel files containing keyword 'secret', limited to the domain xyz.com, excluding the keyword 'password'?

A. `site:xyz.com inurl:excel secret AND NOT password`
B. `site:xyz.com filetype:xlsx secret -password`
C. `indomain:xyz.com inurl:excel secret AND NOT password`
D. `indomain:xyz.com filetype:xls secret -password`

Solution: B

[1 mark]

(d) Why should you configure DNS servers to allow zone transfer *only* to trusted secondary DNS servers?

A. To prevent attackers from enumerating all hosts and subdomains in the zone
B. To prevent DNS spoofing attacks against users of the DNS server
C. To prevent attackers from using brute-force techniques against the DNS server
D. To prevent attackers from creating spoofed entries in the secondary DNS server

Solution: B.

[1 mark]

[Total for Question 2: 4 marks]

Question 3

(a) Which of the following statements are true regarding the difference between vulnerability assessment and penetration testing?

A. Penetration testing is time-boxed (i.e., fixed duration), but vulnerability assessment is not

B. Penetration testing requires higher levels of skills compared to vulnerability assessment

C. Penetration testing usually results in exploiting discovered vulnerabilities, but vulnerability assessment typically just report identified vulnerabilies

D. Vulnerability assessment is more likely to report false-positives compared to penetration testing

E. Vulnerability assessment takes business context into consideration when reporting issues, but penetration testing is purely technical in nature for the purpose of reporting

Solution: B,C and D are true.

[1 mark]

(b) 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: 3 marks]

Question 4

(a) Common Vulnerability Scoring System (CVSS) is a scoring system that quantifies security weaknesses. Which of the following characteristics is/are NOT taken into consideration in the calculation of the score?

A. Complexity of the attack required to exploit
B. Whether the attack can be executed remotely or only locally
C. Whether the attack requires privileges on the target system
D. The number of affected users of the vulnerable system
E. The extent of the impact on integrity of data as the result of a successful exploitation

Solution: D - CVE does not take into consideration how widely the software is used

[1 mark]

(b) Order the CVSS score of the following CVSS strings in *increasing order* (lowest to highest)

A. `AV:N, AC:H, PR:N, UI:N, S:U, C:H, I:L, A:L`
B. `AV:L, AC:H, PR:N, UI:R, S:U, C:L, I:L, A:L`
C. `AV:N, AC:H, PR:N, UI:R, S:U, C:L, I:L, A:L`
D. `AV:N, AC:H, PR:N, UI:N, S:U, C:L, I:L, A:L`

Solution: B=>C=>D=>A

[2 marks]

(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)

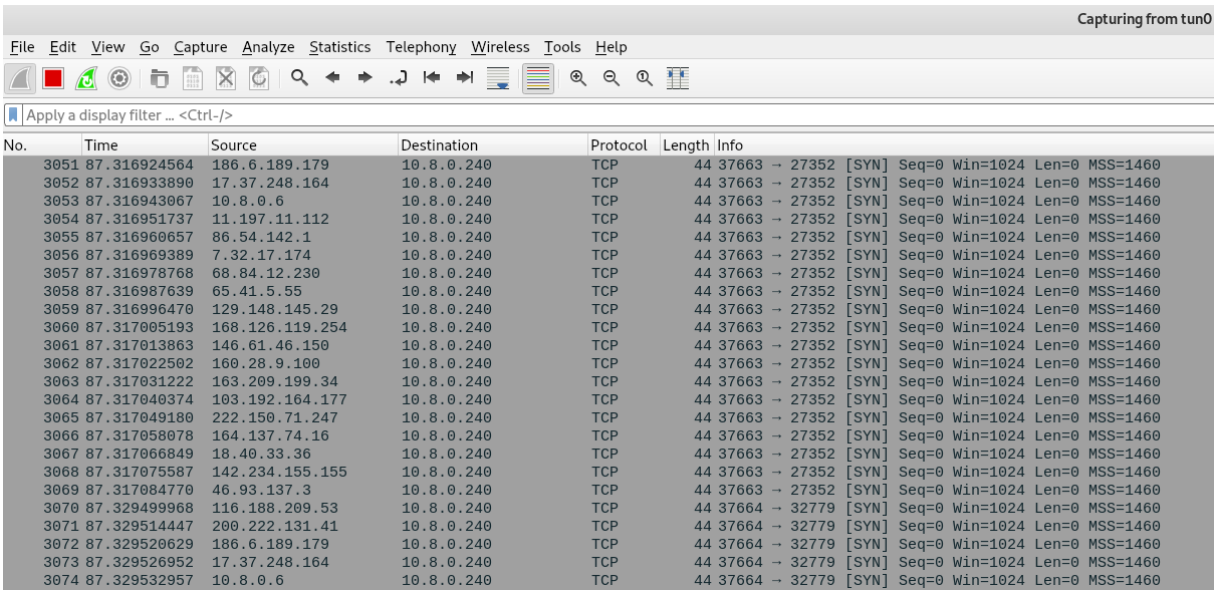
Solution: SYN ; SYN+ACK ; ACK

[3 marks]

(d) In Nmap's stealthy SYN scan (also called half-open scan, invoked by using the `-sS` flag) if the target port is open, the server returns a _____, and Nmap returns _____, without establishing a connection. If the port is closed, the server would just send _____and Nmap does not send the third packet.

Solution: 2; SYN+ACK, RST, RST

[2 marks]



No.	Time	Source	Destination	Protocol	Length	Info
3051	87.316924564	186.6.189.179	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3052	87.316933890	17.37.248.164	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3053	87.316943067	10.8.0.6	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3054	87.316951737	11.197.11.112	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3055	87.316960657	86.54.142.1	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3056	87.316969389	7.32.17.174	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3057	87.316978768	68.84.12.230	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3058	87.316987639	65.41.5.55	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3059	87.316996470	129.148.145.29	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3060	87.317005193	168.126.119.254	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3061	87.317013863	146.61.46.150	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3062	87.317022502	160.28.9.100	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3063	87.317031222	163.209.199.34	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3064	87.317040374	103.192.164.177	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3065	87.317049180	222.150.71.247	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3066	87.317058078	164.137.74.16	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3067	87.317066849	18.40.33.36	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3068	87.317075587	142.234.155.155	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3069	87.317084770	46.93.137.3	10.8.0.240	TCP	44	37663 → 27352 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3070	87.329499968	116.188.209.53	10.8.0.240	TCP	44	37664 → 32779 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3071	87.329514447	200.222.131.41	10.8.0.240	TCP	44	37664 → 32779 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3072	87.329520629	186.6.189.179	10.8.0.240	TCP	44	37664 → 32779 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3073	87.329526952	17.37.248.164	10.8.0.240	TCP	44	37664 → 32779 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3074	87.329532957	10.8.0.6	10.8.0.240	TCP	44	37664 → 32779 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Figure 1: Nmap scan example

(e) In a SYN flood attack, the sender IP address is spoofed and the third packet is never sent. Would SYN flood work if the destination server port is closed? Briefly explain your answer.

Solution: No. If the port is closed, the server returns a RST and does not consume further resource.

[2 marks]

(f) The technique to scan a target indirectly without actually sending any packets directly to the target is called _____scan.

Solution: Zombie.

[1 mark]

(g) Refer to Figure 1 for a Wireshark capture of an Nmap scan against a target. What technique (and/or flag) was used? What is the aim of using this technique?

Solution: Decoy scan (IP spoofing also accepted); evade detection.

[2 marks]

[Total for Question 4: 13 marks]

Question 5

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

Solution: False.

[1 mark]

(b) True or False? The XOR cipher is a good cipher if the key length is the same as the message length, and the key is used only once.

Solution: True. This is a one-time pad.

[1 mark]

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

Solution: Frequency.

[1 mark]

(d) Which of the following statements regarding RSA is/are true?

A. RSA is not suitable for encrypting long messages
B. RSA is typically used to exchange session keys for subsequent symmetric ciphers such as AES
C. Diffie-Hellman (DH) is used for key exchange
D. Keys are pre-shared and never exchanged over public network

Solution: A and B.

[1 mark]

(e) If two plaintext messages M_1 and M_2 are "encrypted" using the same key K using simple XOR into ciphertexts C_1 and C_2, what can you say about $C_1 \oplus C_2$?

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

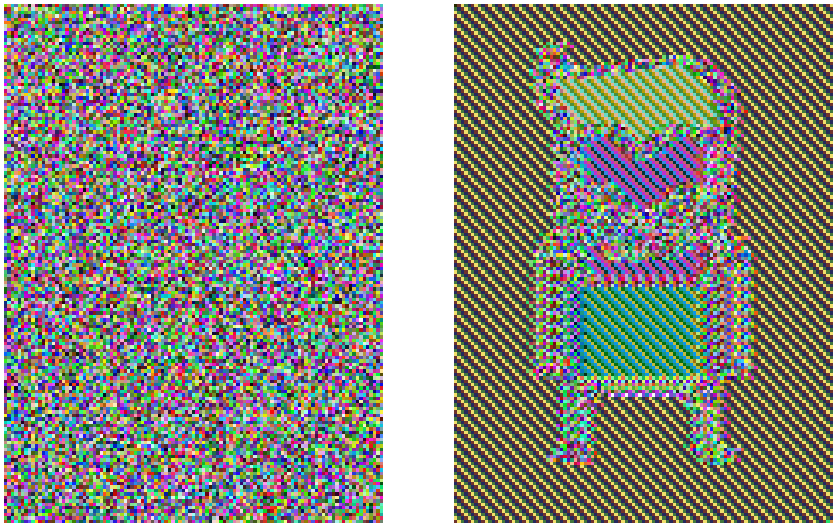
[1 mark]

(f) If two plaintext messages M_1 and M_2 are "encrypted" using the same key K using simple XOR into ciphertexts C_1 and C_2, what can you say about $M_1 \oplus C_1$?

Solution: $M_1 \oplus C_1 = K$.

[1 mark]

(g) Refer to Fig. 2. 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) (b)

Figure 2: Encrypted Images

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

Solution: B: CBC, ECB

[1 mark]

(h) 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]

(i) 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

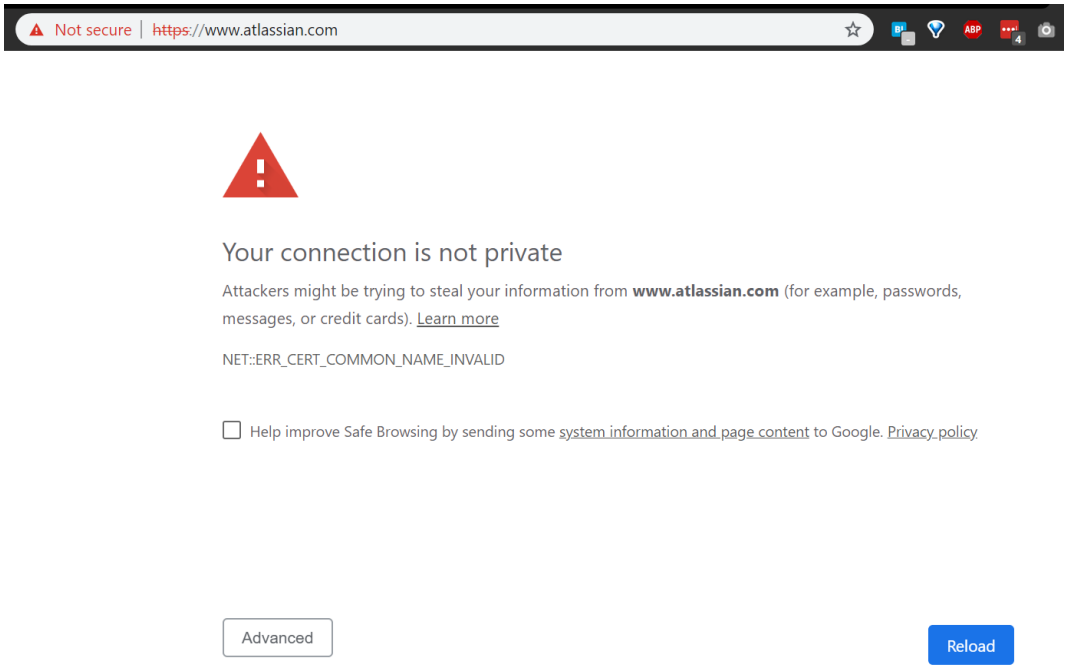


Figure 3: SSL error in Chrome

E. The CA's root certificate

Solution: B. Alice's private key

[1 mark]

(j) When browsing an SSL-protected website, you encounter the error message in Fig. 3. What could have caused this error?

A. Someone may have edited your local `hosts` file

B. You may have been a target of an ARP Cache Poisoning attack

C. Atlassian website may have been targeted with SQL injection attack

D. You may have been a target of a DNS spoofing attack

Solution: A, B and D. The error is "Common Name Invalid" meaning the CN presented in the cert does not match the URL.

[1 mark]

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

Solution: Trapdoor

[1 mark]

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

A. Key stretcihng 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 D.

[1 mark]

(m) True or False? Salting password hashes with a random string makes Rainbow Table attacks infeasible.

Solution: True.

[1 mark]

[Total for Question 5: 13 marks]

Question 6

```
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 1: Sample Code

(a) Refer to the sample code above. 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!"?

Solution: Yes. Stack protector only protects overwriting of the return address.

[1 mark]

(b) 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]

(c) When a C program is compiled using the gcc flag `-fstack-protector` a random token known as a _____is inserted into the stack frame to detect stack smashing attempts.

Solution: Canary.

[1 mark]

(d) Which of the following statements are true 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: A, B, D are true. Since program executes from lower to higher address, NOPSLED must be located at a lower address in relation to the shellcode.

[1 mark]

(e) 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]

(f) When generating a reverse shell payload using the tool `msfvenom` what are the two parameters required?

Solution: The listener's IP address (LHOST) and the listener's port number (LPORT)

[2 marks]

```
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 2: Hello World

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

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

[2 marks]

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/types.h>
#include <unistd.h>
int main(int argc, char **argv) {
  setreuid(geteuid(), getegid());
  char buff[100];
  snprintf(buff, 100, "echo␣%s", argv[1]);
  system(buff);
  return 0;
}
```

Listing 3: Echo Program

(h) Refer to listing 3, a simple program that just echos user input (`argv[1]`). Is this program vulnerable to buffer overflow? Explain why or why not.

Solution: No. `snprintf` will prevent more than 100 characters being written to the buffer.

[2 marks]

(i) Following on from the preceding question, 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`).

Solution: Providing the argument "hoge; cat /etc/shadow" is sufficient.

[2 marks]

```c
#include <stdlib.h>
#include <stdio.h>
int flag1;
int main(int argc, char **argv){
  printf(argv[1]);
  printf("The␣flag␣is:␣%d\n", flag1);
  return 0;
}
```

Listing 4: Sample Code

(j) Refer to the C program in Listing 4. Is this program vulnerable to any exploitation? On which line? What can the attacker do?

Solution: It is vulnerable to format string attack. Line 5. The attacker can read any memory location and write to (almost) any memory location.

[2 marks]

```
(gdb) x/20xw $esp
0xbffff300:     0xb7fa8000      0x41418000      0x41414141      0x41414141
0xbffff310:     0xb7fa8300      0x00000000      0xbffff338      0x004011f2
0xbffff320:     0xbffff587      0xbffff3e4      0xbffff3f0      0x004011da
0xbffff330:     0xb7fe6440      0xbffff350      0x00000000      0xb7de8b41
0xbffff340:     0xb7fa8000      0xb7fa8000      0x00000000      0xb7de8b41
(gdb) info frame
Stack level 0, frame at 0xbffff320:
 eip = 0x4011be in fun (test.c:7); saved eip = 0x4011f2
 called by frame at 0xbffff350
 source language c.
 Arglist at 0xbffff318, args: str=0xbffff587 "AAAAAAAAAA"
 Locals at 0xbffff318, Previous frame's sp is 0xbffff320
 Saved registers:
  ebx at 0xbffff314, ebp at 0xbffff318, eip at 0xbffff31c
(gdb)
```

Figure 4: Debugging with GDB

```
1  #include <stdlib.h>
2  #include <stdio.h>
3  #include <string.h>
4  void fun(char *str) {
5    char buff[10];
6    strcpy(buff, str);
7  }
8  int main(int argc, char **argv){
9    fun(argv[1]);
10   return 0;
11 }
```

Listing 5: Sample Code

(k) Refer to listing 5. The program is compiled with `-fno-stack-protector` and `-zexecstack` gcc flags. The program is run with argument `$(python -c 'print "A"*10')` and paused on line 7, just before returning to main. How many more "A"s need to be added to the argument so that the saved return address is overwritten with `0x41414141`?

Solution: 16 more characters.

[2 marks]

(l) In a typical return-to-libc attack covered in the workshop, you need to find out the memory location of the _____function and the _____function.

Solution: system() and exit(), although other libc functions can also be used.

[2 marks]

[Total for Question 6: 20 marks]

Question 7

(a) True or False? Packet sniffing is trivial in a switched network.

Solution: False. Packet sniffing is trivial in a non-switched network or open WiFi.

[1 mark]

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

A. Using SSL for all web browsing
B. Avoiding the use of plaintext protocols like FTP and TELNET
C. Using a host-based firewall to block ARP responses
D. Using VPN tunnel to a trusted gateway

Solution: All except (C).

[1 mark]

(c) Which of the following is/are true 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: A,B,C. D is wrong, as you can still do DHCP spoofing if the switch does not implement snooping

[1 mark]

(d) Which of the following techniques allow an adversary to sniff network traffic of others?

A. ARP Cache Poisoning
B. DHCP Spoofing
C. Snifing wireless traffic on open WiFi
D. Cross-Site Scripting (XSS) attack on victim's machine

Solution: A, B, C

[1 mark]

(e) True or False? You can sniff network traffic of a computer that is connected to a different VLAN using an ARP Cache Poisoning Attack.

Solution: False. ARP is only sent in the same broadcast network.

[1 mark]

(f) True or False? You can sniff network traffic packets sent from a machine connected to a different VLAN by using a DNS cache poisoning attack.

Solution: True. If you can poison the DNS cache either on the victim or the DNS server, you can still intercept traffic.

[1 mark]

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

Solution: MAC Address

[1 mark]

(h) 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	11:22:33:44:55:66:77
Victim	10.1.1.100	aa:aa:aa:aa:aa:aa:aa
Attacker	10.1.1.200	bb: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]

(i) Following on from the preceding question, what does the ARP cache 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:bb	C	eth0

B.

Address	HWtype	HWaddress	Flags Mask	Iface
10.1.1.200	ether	11:22:33:44:55:66:77	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	11:22:33:44:55:66:77	C	eth0

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

[1 mark]

[Total for Question 7: 9 marks]

Question 8

(a) Refer to the PHP code below. What string would you try to inject into the "file" 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 $file = $_POST['file'];
3 $result = shell_exec('cat ./' . $file );
4 echo 'cat output: <pre>'.$result.'</pre>';
5 ?>
```

Listing 6: Sample Code

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

[2 marks]

(b) True or False. The PHP code in the preceding question is vulnerable to both command injection and XSS.

Solution: True.

[1 mark]

(c) Suppose you find a "blind" command injection vulnerability in a web application POST parameter, where you are able to execute arbitrary command, but cannot see the output from the commands. Only the web server ports (80 and 443) are open on the firewall, and the only outbound traffic allowed are DNS (TCP and UDP port 53) and ICMP. The `www-data` user runnig the HTTP server has write access to the /uploads/ folder. Describe two ways the attacker can gain shell access to the server.

Solution: Revese shell through port 53, or writing a web shell to the /uploads/ folder.

[2 marks]

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

```
1 <?php
2 $ua = $_SERVER["HTTP_AGENT"];
3 echo "<h1>Your␣User␣Agent:" . $ua . "</h1>"
4 ?>
```

Listing 7: Sample Code

A. Reflected XSS
B. Stored XSS

C. Neither
D. Both

Solution: A. Reflected XSS

[1 mark]

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

```
1 <?php
2 $q = $_GET['QUERY'];
3 echo "<h1>Your␣Query␣was:" . htmlspecialchars($q) . "</h1>"
4 ?>
```

Listing 8: Sample Code

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

Solution: A. Neither

[1 mark]

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

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 flags during Set-Cookie

Solution: B and C.

[1 mark]

(g) True or False? Cross-site request forgery (CSRF) attack can typically be used to steal the victim's session cookie for session hijacking.

Solution: False.

[1 mark]

(h) 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]

(i) True or False? CSRF attack can only succeed if the victim has an active 'live' session with the target website.

Solution: True

[1 mark]

(j) Write a proof-of-concept payload for the "color" parameter that will display a browser `alert()` pop-up in the PHP code below.

```
1  <?php
2  $color = $_POST['color'];
3  $html = "<span style='{color:";
4  $html .= $color;
5  $html .= "}'>Hello World!</span>";
6  echo $html;
7  ?>
```

Solution:
`red'}>$<$script$>$alert(1)</script>`
Need to close the style string with ' first. Zero otherwise.

[2 marks]

(k) Refer to the PHP code below. Is this vulnerable to SQL injection? If yes, what value would you inject into the `id` parameter so that it will display the entire products table? If no, explain why.

```
1  <?php
2  // Get input
3  $id = $_GET[ 'id' ];
4  $qry = "select id,name, sku from products where id=" . $id;
5  $result = $conn->query($qry);
6
7  // Get results and output
8  while($row = $result->fetch_assoc()) {
9    $product = $row["name"];
10   $html = "<pre>ID: " . $id;
11   $html .= "/Product: $name</pre>";
12   echo $html;
13 }
14 ?>
```

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

[2 marks]

(l) Following on from the preceding question, what value would you inject into the `id` parameter to display the MySQL database server version using the `@@version` function?

Solution: Inject something like this is sufficient.

```
1 UNION SELECT 1, @@version, 3#
```

Note that you need to have 3 columns.

[2 marks]

(m) One of the most effective ways to prevent SQL injection is to use _____statements instead of building SQL strings manually.

Solution: Prepared

[1 mark]

[Total for Question 8: 18 marks]

Question 9

(a) Webpage defacing affects which security attribute(s)?

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

Solution: Integrity

[1 mark]

(b) TLS/SSL protects which of the following information security attribute(s)?

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

Solution: Confidentiality and Integrity

[1 mark]

(c) Information security risk refers to a possible event or events wherein a _____can exploit _____to compromise the _____of _____. Choose from: information assets, security, threat actor, vulnerabilities, exploit.

Solution: (a) Threat actor (b) vulnerability (c) security (d) information assets

[1 mark]

(d) In what situations would an organisation typically decide to *avoid* a risk rather than trying to mitigate it?

A. When the cost of mitigation to an acceptable level is greater than the benefits of partaking in the activity
B. When the benefits of partaking in the activity is greater than the cost of mitigation
C. When there is no practical means to mitigate the risk to an acceptable level
D. When the impact of the risk is greater than EXTREME and likelihood is VERY LIKELY

Solution: A and C only. B is clearly wrong, and there may be possible mitigations in D.

[1 mark]

(e) What are the other three approaches to addressing risks besides *avoid*?_____, _____, and _____.

Solution: transfer, accept, mitigate

[1 mark]

(f) 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]

(g) 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]

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) Which of the following are considered to be work performed by a computer forensic expert?

A. Forensic investigation as part of criminal investigation
B. Performing vulnerability assessment on a computer system
C. Incident response after a major data breach caused by hacking
D. eDiscovery in response to freedom-of-information act disclosure request and others

Solution: A, C, D

[1 mark]

(c) True or False? Forensics investigators often use disk duplicator with write-block function to prevent accidental over-writing of evidence.

Solution: True

[1 mark]

(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) In which of the following would you find text copied to the clipboard?

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

Solution: A - memory dump

[1 mark]

[Total for Question 10: 5 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) True or False? "Threat Hunting" in the security operations centre (SOC) is the act of hunting down the attacker and 'hackin back' gainst the threat actor.

Solution: False

(c) True or False? Honeypot servers are useful for both deterrence and for attribution.

Solution: True

[Total for Question 11: 3 marks]

End of exam