	LECOCQ ARTHUR
Started on	Thursday, 15 February 2024, 9:45 AM
State	Finished
Completed on	Thursday, 15 February 2024, 9:56 AM
Time taken	11 mins 26 secs
Grade	**10.00** out of 18.00 (**55.56**%)

Question **1**

Correct

(1 point) A firewall

● Connects the internal network to a demilitarized zone and hence to external networks ✓

○ Only filters packets coming from the external network

○ Only filters packets coming from the internal network

Your answer is correct.

The correct answer is:
Connects the internal network to a demilitarized zone and hence to external networks

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:45	Saved: Connects the internal network to a demilitarized zone and hence to external networks	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Correct**	**1.00**

Question **2**

Correct

(1point) The following hook function

```
struct iphdr *iph;

struct udphdr *udph;

u32 ip_addr;

char ip[16] = "8.8.8.8";

if (iph->protocol == IPPROTO_UDP) {

    udph = udp_hdr(skb);

    if (iph->daddr == ip_addr && ntohs(udph->dest) == 53){

        printk(KERN_DEBUG "****Dropping %pI4 (UDP), port %d\n",

                     &(iph->daddr), port);

        return NF_DROP;

     }

}
```

● blocks UDP packets if their destination IP is 8.8.8.8 and the destination port is 53✓

○ allows UDP packets only if their destination IP is 8.8.8.8 and the destination port is 53

○ blocks all packets, except UDP packets if their destination IP is 8.8.8.8 and the destination port is 53

Your answer is correct.

The correct answer is:
blocks UDP packets if their destination IP is 8.8.8.8 and the destination port is 53

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:47	Saved: blocks UDP packets if their destination IP is 8.8.8.8 and the destination port is 53	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Correct**	**1.00**

Question **3**

Correct

Packet spoofing refers to the process of:

○ sending malformed packets to cause unexpected behavior at the receiver (e.g., reverse shell)

● masquerading as a known entity in the system ✓

○ passively listening to an information exchange process

Your answer is correct.

The correct answer is:
masquerading as a known entity in the system

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:48	Saved: masquerading as a known entity in the system	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Correct**	**1.00**

Question **4**

Incorrect

(1 point) The following query is performed in the back-end of a web page that allows the user to update his/her nickname and email address (the ID is automatically retrieved from the web page and it is equal to 25).

$sql = "UPDATE credential SET nickname='$input_nickname',email='$input_email' WHERE ID='$id';";

If the user inserts the following input into the nickname web field

’, salary='999999

which will be the query performed by the server?

○ $sql = "UPDATE credential SET nickname='', salary='999999', email='' WHERE ID='25';";

● $sql = "UPDATE credential SET nickname=, salary=999999, email= WHERE ID=25;";✖

○ $sql = "UPDATE credential SET salary='999999' WHERE ID='25';";

Your answer is incorrect.

The correct answer is:
$sql = "UPDATE credential SET nickname='', salary='999999', email='' WHERE ID='25';";

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:50	Saved: $sql = "UPDATE credential SET nickname=, salary=999999, email= WHERE ID=25;";	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Incorrect**	**0.00**

Question **5**

Incorrect

(1 point) In stored XSS

○ the code is stored on the user DOM before execution

● the code is stored on the user's machine before execution ✖

○ the code is stored on a database before execution

Your answer is incorrect.

The correct answer is:
the code is stored on a database before execution

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:51	Saved: the code is stored on the user's machine before execution	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Incorrect**	**0.00**

Question **6**

Correct

(1point) The following code in XSS:

investors.mega-bank.com/listing#<script>alert(document.cookie);</script>

○ prevents the attacker from getting the current session cookies

○ warns the victim about an XSS attack

● displays the current session cookies ✓

Your answer is correct.

The correct answer is:
displays the current session cookies

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:51	Saved: displays the current session cookies	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Correct**	**1.00**

Question **7**

Correct

When a script tag is interpreted as code instead of text by a DOM, we are witnessing

○ an SQL injection

○ a CSRF attack

● an XSS attack ✓

Your answer is correct.

The correct answer is:
an XSS attack

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:51	Saved: an XSS attack	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Correct**	**1.00**

Question **8**

Correct

(1 point) How can we receive packets for which we are not the intended receiver?

● enabling the promiscuous mode ✓

○ changing the MAC address in the NIC

○ turning off the NIC

Your answer is correct.

The correct answer is:
enabling the promiscuous mode

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:52	Saved: enabling the promiscuous mode	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Correct**	**1.00**

Question **9**

Correct

Which one is NOT a vulnerability that can lead to CSRF

● Improper input validation✓

○ Lack of same-origin policy enforcement

○ Lack of CSRF tokens

Your answer is correct.

The correct answer is:
Improper input validation

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:53	Saved: Improper input validation	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Correct**	**1.00**

Question **10**

Incorrect

(1 point) Assuming that a website has enabled the countermeasures against CSRF attacks. Select which cookies are transmitted in case of a POST cross-site request.

○ Normal cookie

● Normal cookie and strict cookie ✗

○ Normal cookie and lax cookie

Your answer is incorrect.

The correct answer is:
Normal cookie

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:53	Saved: Normal cookie and strict cookie	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Incorrect**	**0.00**

Question **11**

Incorrect

(1 point) An Ethereum smart contract is

○ a computer program stored in a specific node in the blockchain

○ bytecode stored in a transaction

● a computer program written in solidity that simultaneously run over the whole blockchain network ✖

Your answer is incorrect.

The correct answer is:
bytecode stored in a transaction

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:54	Saved: a computer program written in solidity that simultaneously run over the whole blockchain network	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Incorrect**	**0.00**

Question **12**

Correct

How is digital currency represented in a blockchain?

○ by a record in a centralized database

● by a transaction indicating, among the other, the sender and the receiver✓

○ by a digital token stored in the owner's machine

Your answer is correct.

The correct answer is:
by a transaction indicating, among the other, the sender and the receiver

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:55	Saved: by a transaction indicating, among the other, the sender and the receiver	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Correct**	**1.00**

Question **13**

Incorrect

(1 point) What are some best practices for secure coding to prevent buffer overflow attacks?

○ Ignore compiler warnings

● Always use dynamic memory allocation ✖

○ Validate user input against expected lengths

Your answer is incorrect.

The correct answer is:
Validate user input against expected lengths

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:55	Saved: Always use dynamic memory allocation	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Incorrect**	**0.00**

Question **14**

Incorrect

(1 point) What is the main difference between a return-to-libc attack and a format string attack?

○ They are the same type of attack with different names

● One targets stack memory, the other targets heap memory ✖

○ One relies on overflowing a buffer, the other does not

Your answer is incorrect.

The correct answer is:
One relies on overflowing a buffer, the other does not

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:55	Saved: One targets stack memory, the other targets heap memory	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Incorrect**	**0.00**

Question **15**

Incorrect

(1 point) What type of code does shellcode typically consist of?

○ Assembly instructions to open a command prompt

○ Encrypted data to bypass security measures

● Machine code to execute a specific action ✖

Your answer is incorrect.

The correct answer is:
Assembly instructions to open a command prompt

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:55	Saved: Machine code to execute a specific action	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Incorrect**	**0.00**

Question **16**

Correct

(1 point) What precautionary measure can mitigate the risk of shellcode injection?

○ Disabling system logging

○ Increasing the size of input buffers

● Implementing stack canaries✓

Your answer is correct.

The correct answer is:
Implementing stack canaries

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:56	Saved: Implementing stack canaries	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Correct**	**1.00**

Question **17**

Incorrect

(1 point) How does a format string attack exploit vulnerabilities in a program?

● By overwriting a return address on the stack ✖

○ By manipulating the format string input to access sensitive data

○ By flooding the input buffer with excessive data

Your answer is incorrect.

The correct answer is:
By manipulating the format string input to access sensitive data

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:56	Saved: By overwriting a return address on the stack	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Incorrect**	**0.00**

Question **18**

Correct

(1 point) How can an attacker leverage a format string vulnerability to gain unauthorized access?

○ By directly modifying the program's source code

○ By manipulating the inputs to reveal sensitive information

● By manipulating the format string argument to reveal sensitive information ✓

Your answer is correct.

The correct answer is:
By manipulating the format string argument to reveal sensitive information

Response history

Step	Time	Action	State	Marks
1	15/02/24, 09:45	Started	Not yet answered	
2	15/02/24, 09:56	Saved: By manipulating the format string argument to reveal sensitive information	Answer saved	
3	**15/02/24, 09:56**	**Attempt finished**	**Correct**	**1.00**