1)

(1 point) A firewall

- Only filters packets coming from the internal network
- Only filters packets coming from the external network
- Connects the internal network to a demilitarized zone and hence to external networks ✔

2)

(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

3)

Packet spoofing refers to the process of:

- passively listening to an information exchange process
- masquerading as a known entity in the system
- sending malformed packets to cause unexpected behavior at the receiver (e.g., reverse shell) ✖

Your answer is incorrect.

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

4)

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

Your answer is incorrect.

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

---

5)

6)

7)

8)

9)

Which one is NOT a vulnerability that can lead to CSRF

- Lack of same-origin policy enforcement
- Improper input validation ✔
- Lack of CSRF tokens

10)

(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 and lax cookie
- Normal cookie and strict cookie
- Normal cookie ✔

---

11)

12)

13)

14)

15)

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

- Assembly instructions to open a command prompt
- Machine code to execute a specific action ✗
- Encrypted data to bypass security measures

Your answer is incorrect.

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

16)

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

- Implementing stack canaries ✓
- Disabling system logging
- Increasing the size of input buffers

17)

18)