(1 point) Stack canaries prevent

- data-oriented bof attacks
- any type of bof attacks (i.e., both data-oriented and control-flow-oriented bof attacks) ✖
- control-flow-oriented bof attacks

(1 point) What is the purpose of a return-to-libc attack?

- Return-to-libc attacks aim to bypass ASLR and execute predefined sequences of existing library functions to carry out specific actions.
- Return-to-libc attacks involve redirecting the program's execution flow to arbitrary memory addresses, allowing the execution of malicious code. ✖
- Return-to-libc attacks exploit vulnerabilities in the computer's memory management system to gain arbitrary code execution privileges.

(1 point) Which countermeasure is effective against return-to-libc attack?

- Control Flow Integrity, which enforce strict control over the program's execution flow, preventing deviations or unauthorized jumps to non-intended locations.
- Address Space Layout Randomization ✖
- Stack canaries

(1 point) When you perform a shellcode attack, you have to make the program jump:

- to any address before the location of the shellcode cause the stack pointer will move along the stack until it finds the shellcode ✖
- to any address before the location of the shellcode, but after the return address, cause the stack pointer will move along the stack until it finds the shellcode
- exactly at the address where the shellcode has been placed

(1 point) Select the appropriate role of the eax, ebx and ecx registers when performing a shellcode attack:

- eax contains the zero value; ebx points to argv[0]; ecx points to argv
- eax contains the system call number; ebx points to argv[0]; ecx points to argv ✔
- eax contains the system call number; ebx points to argv; ecx points to argv[0]

(1 point) Gadgets used to perform a Return Oriented Programming (ROP) attack

- are assembly instructions that the attacker makes the program jump to in order to change its runtime behavior ✔
- are source code instructions that the attacker makes the program jump to in order to change its runtime behavior
- are assembly instructions that the attacker injects intro the victim program

(1 point) Packet sniffing refers to the process of:

- Overhearing live communications between legitimate network entities ✔
- Changing sensitive information in a packet to trick the receiver
- Intercepting communication between two hosts to manipulate packets

(1 point) In a Smurf attack, the attacker:

- Spoofs an ICMP packet using as sender address the victim's address ✔
- Spoofs an ICMP packet using as receiver address the victim's address
- Spoofs an TCP packet using as sender address the victim's address

(1 point) A reflected XSS attack:

- the attacker exploits a link sent to the victim
- the attacker stores the malicious code on a server
- the attacker stores and executes the code direclty on the browser ✖

(1 point) In a DOM-based XSS attack, the sink:

- executes the script to e.g., display sensitive information
- sanitizes the input to prevent the execution of the attack
- interacts with a server to retrieve the attacker's code ✖

(1 point) What is the most generic set of pre-requisites for an attacker to complete a CRSF attack?

- Crafting a cross-site request; making the victim send the cross-site request crafted by the attacker (e.g., by visiting a malicious web page); appending the victim session cookie to the cross-site request
- Having the victim under an active session on the target website; crafting a cross-site request; making the victim send the cross-site request crafted by the attacker (e.g., by visiting a malicious web page) ✔
- Having the victim under an active session on the target website; crafting a cross-site request; making the victim click on the link crafted by the attacker which will send the cross-site request

(1 point) Select which is the main vulnerability that leads to a CSRF attack among the following ones:

- Browsers attaching session cookies indiscriminately to any request towards the target website ✔
- Victim having an active session on the target website
- Cross-site requests

(1 point) In a SYN flooding attack

- The attacker always modifies the sender IP address
- The attacker overloads the receiver's packet buffer causing a denial of service ✔
- The attacker takes control of an existing connection

(1 point) Select which information is mandatory to be known by the attacker in order to successfully perform a SQL injection attack, assuming he can only interact with the web page of the victim website.

- The exact structure of the SQL query performed against the SQL database on the server ✖
- The exact structure of the SQL database on the server
- The website sanitizers applied on the client side

(1 point) XSS takes advantage of

- the fact that web applications execute scripts in a distributed fashion
- the fact that web applications execute scripts on remote servers
- the fact that web applications execute scripts on the users' browser ✔

(1 point) Select the option that holds true for TCP Hijacking

- The attacker takes control of an existing connection ✔
- The attacker causes a denial of service to an existing connection
- The attacker creates a new connection impersonating another user

(1 point) A transaction in a blockchain is

- a list of multiple exchanges that needs to be validated via a consensus algorithm
- a string in a list of records including, among the others, the sender and receiver addresses, and the amount exchanged ✔
- a pointer to a digital currency (e.g., Bitcoin) exchanged among users

(1 point) An Ethereum smart contract is

- bytecode stored in a transaction
- a computer program stored in a specific node in the blockchain
- a computer program written in solidity that simultaneously run over the whole blockchain network ✖