Cybersecurity

Application level security

14/1/2025

Surname: _____

Name: _____

Student ID: _____

PLEASE CAREFULLY READ THE FOLLOWING NOTES: the test lasts 1h. During the test you can't leave the room. A pen is all you need to fill this form. Use only the given space to answer the questions. For the multiple-choice questions you MUST provide a (short) motivation for your answer. At the end of the test, give back this form to your teacher. Copying or sharing information with your colleagues during the test will be considered cheating and will inevitably bring your exam to a premature and negative end.

Question 1

Which critical aspect of SMTP's store-and-forward model makes it susceptible to certain types of email threats like spoofing attacks?

[X] A) Lack of authentication for email delivery servers
[ ] B) Inability to encrypt email content during transmission
[ ] C) Reliance on proprietary email clients for compatibility
[ ] D) Dependency on multi-recipient addressing in headers

Motivation: THE ONLY PURPOSE OF SMTP IS TO TRANSFER EMAILS, SECURITY IS NOT PART OF ITS OBJECTIVES.

Question 2

What is the main limitation of SPF?

[ ] A) It does not support emails with non-ASCII characters
[X] B) It does not protect the email body or attachments
[ ] C) It mandates the use of IMAP for email reading
[ ] D) It is incompatible with encryption protocols

Motivation: SPF ONLY CHECKS IF THE SENDER IP ADDRESS IS AUTHORIZED, PREVENTING SPOOFING, BUT DOESN'T PROTECT MESSAGE'S CONTENT.

Question 3

Which intrusion detection method relies on predefined rules to detect known attack patterns?
[X] A) Signature-based detection
[ ] B) Anomaly-based detection
[ ] C) Distance-based detection
[ ] D) Statistical profiling

Motivation: THE STRATEGY IS BASED ON THE KNOWLEDGE ABOUT PREVIOUSLY ATTACKS STORED IN A DATABASE. IT'S USEFUL FOR WELL KNOW ATTACKS, BUT USELESS FOR NEW TYPE OF ATTACKS.

Question 4

What is the main limitation of network-based IDS in monitoring traffic?
[X] A) High resource usage for all traffic types
[X] B) Inability to monitor data passing through encrypted channels
[ ] C) Dependency on a specific operating system
[ ] D) Difficulty in detecting Denial of Service attacks

Motivation: IT CANNOT ANALYSE ENCRYPTED TRAFFIC WITHOUT DECRYPTING IT FIRST, LIMITING ITS ABILITY TO DETECT HIDDEN ATTACKS WITHIN HTTPS OR VPN CONNECTIONS

Question 5

What is the main goal of a hybrid disclosure policy for vulnerabilities?
[ ] A) To keep vulnerabilities entirely secret
[ ] B) To ensure transparency by immediate public disclosure
[X] C) To balance secrecy and transparency in vulnerability management
[ ] D) To allow vendors unlimited time to patch vulnerabilities

Motivation: BALANCING CONFIDENTIALITY AND TRANSPARENCY IT'S GUARANTEED THAT VENDORS HAVE TIME TO CORRECT PROBLEMS WITH PATCHES BEFORE PUBLIC DISCLOSURE.

Question 6

What is a Cross-Site Request Forgery (CSRF) attack?
[X] A) An attack that exploits the user's session to perform unauthorized actions
[ ] B) A technique to inject malicious scripts into a server-side web application
[ ] C) An attack that manipulates DNS records to redirect traffic
[ ] D) A method for brute-forcing authentication credentials

Motivation: USUALLY BROWSERS INCLUDE SESSION COOKIES IN HTTP REQUEST. THE ATTACKER PERFORM SOME MALICIOUS ACTIONS EXPLOITING USER'S SESSION, IN ORDER TO SEND REQUESTS FOR THE SEWRE WEBSITE, WHERE THE USER IS AUTHENTICATED.

Question 7

What is the main principle of the Zero Trust security model? How does this approach improve over previous ones?

USUALLY, EVERYTHING CONSIDERED TO BE INTERNAL IS TRUSTWORTHY, BUT THIS APPROACH IS A SECURITY MODEL THAT ASSUME THAT NO USERS OR DEVICES SHOULD BE CONSIDERED TRUSTWORTHY, EVEN IF INTERNAL. IT'S BETTER THAN THE PREVIOUS ONE, BECAUSE EVERY ALLESS REQUEST MUST BE AUTHENTICATED, AUTHORIZED AND CONTINUOUSLY VERIFIED, RESTRICTING USER'S PERMISSION IN ORDER TO REDUCE SURFACE ATTACK. FURTHERMORE, EACH ACTIVITY IS TRACKED TO IDENTIFY SUSPICIOUS BEHAVIOURS.

Question 8

List the key characteristics of blind SQL injection attacks.

IT'S A TYPE OF ATTACK WHERE THE ATTACKER DOESN'T RECEIVE DIRECT ERROR MESSAGES FROM THE DATABASE, MAKING IT HARDER TO IDENTIFY THE VULNERABILITY. TO BYPASS THIS LIMITATION, TECHNIQUES SUCH AS BOOLEAN-BASED ARE USED, WHERE QUERIES RETURN DIFFERENT RESPONSES DEPENDING ON WHETHER A CONDITION IS TRUE OR FALSE, AND TIME-BASED, WHICH EXPLOITS COMMANDS LIKE SLEEP(n) TO DETERMINE IF A QUERY EXECUTES SUCCESSFULLY BY ANALYZING RESPONSE TIMES.