מבחן מסכם באבטחת מידע והגנת הסייבר — נוסח ב'

נושאי הבחינה: קריפטוגרפיה, פונקציות Hash, ארכיטקטורת רשת, פרוטוקולים מוגנים

משך ריצה מוקצב: 120 דקות

שם המועמד/ת: _____

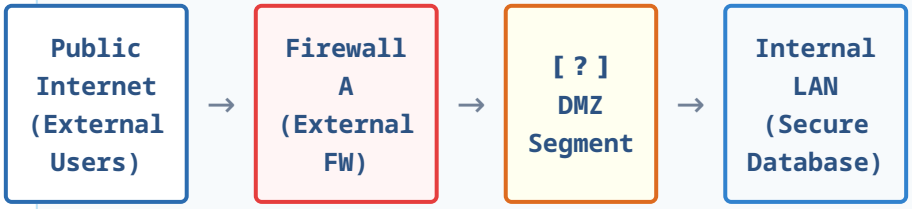
מזהה אישי (ת.ז): _____

SECTION 0x01 פרק א': ניתוח ארכיטקטורה ושאלות פתוחות (30 נקודות)

ענו בהרחבה ובפירוט על השאלות הבאות על בסיס העקרונות הנלמדים. (15 נקודות לשאלה)

שאלה 1 [ניתוח ויזואלי של ארכיטקטורת רשת מאובטחת - DMZ]:

לפניכם תרשים זרימה לוגי (משמאל לימין) המציג את חלוקת האזורים ברשת ארגונית מוגנת המכילה שרת אינטרנט ציבורי ושרת בסיס נתונים פנימי:



איור 1: מבנה פריסת אזורי הגנה ברשת הארגונית

על בסיס עקרונות הגנת הרשת והפרדת אזורים, ענו על שני הסעיפים הבאים:

1. מהו המונח המקצועי המדויק המחליף את סימן השאלה (?) בתוך איור 1? אילו סוגי שרתים (לדוגמה: שרת אפליקציה, שרת DB, שרת Web) חובה למקם באזור זה ואיזה שרת אסור בתכלית האיסור למקם בו?
2. הסבירו כיצד מבנה זה מונע מתוקף חיצוני שהצליח לפרוץ לשרת האינטרנט הציבורי להשיג גישה מיידית וחופשית למידע הרגיש של הארגון.

שאלה 2 [ניהול ססמאות והתקפות קריפטוגרפיות - Rainbow Tables & Salting]:

הסבירו מהי התקפת "טבלאות קשת" (Rainbow Tables Attack) על בסיס נתונים של ססמאות מוצפנות מונע Hash-לפני ביצוע ה **(Salting) וכיצד שימוש בטכניקת **המלחת ססמאות ,(Hashed Passwords) התקפה זו לחלוטין ברמה הארכיטקטונית:

SECTION 0x02 פרק ב': שאלות ברירה מרובה - אמריקאי (40 נקודות)

לכל שאלה תשובה אחת בלבד. סמנו את האפשרות הנכונה ביותר. (20 נקודות לשאלה)

שאלה 3 [אלגוריתמי הצפנה סימטרית - Block Ciphers]:
בעבודה עם אלגוריתם הצפנה סימטרי מבוסס בלוקים (כמו AES), מהו תפקידו של ה-**Initialization Vector וכיצד הוא משפיע על פלט ההצפנה, (CBC Mode כמו) במצבי הצפנה מתקדמים **(IV)?

- א. ה-IV משמש כמפתח ההצפנה הראשי של המערכת ומחליף את הצורך במפתח סודי.
- ב. ה-IV מבטיח שבלוקים זהים של טקסט מקור (Plaintext) יפיקו בלוקים שונים לחלוטין של טקסט מוצפן (Ciphertext) בכל הרצה, ובכך מונע התקפות סטטיסטיות.
- ג. ה-IV פועל רק בשלב הפענוח כדי לאמת שלא בוצע שינוי בנתונים במהלך ההעברה.
- ד. תפקידו היחיד של ה-IV הוא לקבוע את אורך הבלוק המקסימלי (לדוגמה 128 סיביות).

שאלה 4 [הצפנה אסימטרית ואלגוריתם RSA]:
באלגוריתם ההצפנה האסימטרי המוכר **RSA**, על איזו בעיה מתמטית קשה (Computational Hardness) מבוססת רמת הבטיחות והקושי לפרוץ את המפתח הפרטי מתוך המפתח הציבורי הנגיש?

- א. קושי בחישוב לוגריתם דיסקרטי במרחב סופי (Discrete Logarithm Problem).
- ב. בעיית פירוק לגורמים ראשוניים של מספרים גדולים מאוד (Prime Factorization Problem).
- ג. חישוב מהיר של עקומות אליפטיות מעל שדות סופיים (Elliptic Curve Discrete Log).
- ד. קושי בביצוע פעולות היפוך בינאריות רציפות (XOR Cascade Complexity).

SECTION 0x03 פרק ג': היגדי קביעה - נכון / לא נכון (30 נקודות)

קבעו עבור כל היגד האם הוא נכון מתמטית או שגוי. (15 נקודות לשאלה)

שאלה 5 [פונקציות האש ועמידות בפני התנגשויות]:

תכונת ה-"עמידות בפני התנגשויות" (Collision Resistance) בפונקציית האש פירושה שמבחינה חישובית, בלתי אפשרי למצוא שני קלטים שונים לחלוטין (X ≠ Y) שיפיקו בדיוק את אותו פלט האש (Hash(X) = Hash(Y)).

[ ] היגד נכון | [ ] היגד שגוי

שאלה 6 [אבטחת תקשורת ופרוטוקול DNSSEC]:

פרוטוקול האבטחה DNSSEC מיועד להצפין את כל תעבורת שאילתות ה-DNS של המשתמש מפני ציתות ואיסוף נתונים (Eavesdropping), אך הוא אינו מספק אימות לזהות מקור המידע או הגנה מפני זיוף תשובות.

[ ] היגד נכון [ ] היגד שגוי

-- סוף טופס הבחינה (נוסח ב') - בדקו היטב את תהליכי ההצפנה וההגנה שלכם --