חלק א': הפסיכולוגיה של הסיסמאות (Password Psychology)

1. מלכודת המורכבות

רבים חושבים שסיסמה כמו P@ssw0rd1 היא חזקה.

הסבירו מדוע, מנקודת מבטו של מחשב פריצה, החלפת האות a ב-@ או o ב-0 כמעט ואינה מוסיפה לאבטחה:

---

2. אנטרופיה (Entropy) – אורך מול מורכבות

השוו בין שתי הסיסמאות הבאות:

1. Tr0ub4dor&3 (נראית מורכבת, קשה לזכור).
2. CorrectHorseBatteryStaple (ארבע מילים אקראיות, קלה לזכור).

מבחינה מתמטית, איזו מהן תיקח למחשב יותר זמן לפצח ולמה? (רמז: האורך).

⚔️ חלק ב': וקטורי תקיפה (Attack Vectors)

3. זהה את ההתקפה

לפניכם תיאורים של שיטות פריצה. כתבו את שם ההתקפה המתאים (Brute Force / Dictionary / Credential Stuffing):

שם ההתקפה	התיאור
_____	התוקף משתמש ברשימה של מיליון המילים הנפוצות ביותר באנגלית ובווריאציות שלהן.
_____	התוקף מנסה את כל הצירופים האפשריים: aaac, aaab, aaaa... (איטי מאוד).
_____	התוקף לקח שם משתמש וסיסמה שדלפו מ-LinkedIn בשנת 2012 ומנסה להתחבר איתם ל-Netflix ולבנק של הקורבן.

4. ריסוס סיסמאות (Password Spraying)

בהתקפה זו, התוקף בוחר סיסמה אחת נפוצה (למשל Summer2025!) ומנסה אותה כנגד כל העובדים בארגון.

מדוע הוא עושה זאת במקום לנסות הרבה סיסמאות על משתמש אחד? (איזה מנגנון הגנה הוא מנסה לעקוף?)

🛡️ חלק ג': הגנה ואחסון (Defense & Storage)

5. איך שומרים סוד?

שרתים לעולם לא צריכים לשמור סיסמאות כטקסט גלוי (Plaintext).

- **Hashing (גיבוב):** מה קורה לסיסמה כשהיא עוברת תהליך Hash? (האם ניתן להפוך אותה חזרה?)

- **Salting (המלחה):** מדוע מוסיפים מחרוזת אקראית ("מלח") לסיסמה לפני הגיבוב? (בפני איזו טבלה זה מגן עלינו?)

---

6. מדיניות נעילה (Account Lockout)

הגדרתם שחשבון יינעל אחרי 3 ניסיונות כושלים.

מהו הסיכון (או החיסרון) בהגדרה הזו אם תוקף מחליט לנסות לנעול את כל הארגון בכוונה? (סוג של התקפת DoS).

🔐 חלק ד': אימות מודרני (MFA & SSO)

7. דרגות הגנה ב-MFA

אימות רב-שלבי הוא חובה, אבל לא כל השיטות נולדו שוות. דרגו את השיטות מהחלשה ביותר (1) לחזקה ביותר (3):

- ___ מפתח חומרה פיזי (YubiKey / FIDO2).
- ___ הודעת SMS עם קוד.
- ___ אפליקציית אימות (Authenticator App).

מדוע **SMS** נחשב לשיטה הפחות בטוחה? (מה התוקף יכול לעשות לכרטיס ה-SIM?)

---

8. Single Sign-On (SSO)

מהו היתרון הגדול של SSO עבור המשתמש, ומהו הסיכון הגדול עבור הארגון אם החשבון הראשי נפרץ?

🧪 חלק ה': הכנה למעבדה (Lab Prep)

9. כלי העבודה

במעבדה נשתמש ונכיר כלים לבדיקה ופריצה. חברו בין הכלי לפעולה:

הפעולה	הכלי/האתר
כלים המשמשים תוקפים לביצוע Brute Force על שירותים וקבצי Hash.	**Hydra / John the Ripper**
אתר המחשב את הזמן התיאורטי לפיצוח סיסמה (Entropy).	**HowSecureIsMyPassword**
אתר הבודק האם המייל והסיסמה שלי דלפו בעבר לאינטרנט.	**HaveIBeenPwned**

💡 סיכום אישי

רשמו פעולה אחת שתעשו היום כדי לשפר את אבטחת הסיסמאות האישית שלכם (למשל: הפעלת MFA באינסטגרם, התקנת מנהל סיסמאות):