
התקפת Brute-Force



CYBER SCHOOL



שיעור זה מספק תובנה לתוך עולמו של ההאקר על ידי הצגת כלים לפיצוח סיסמאות וכיצד משתמשים בהם בשיטות מקוונות ולא מקוונות. גם הגנות שונות נגדן מכוסות בשיעור זה.

היסודות 





CYBER SCHOOL

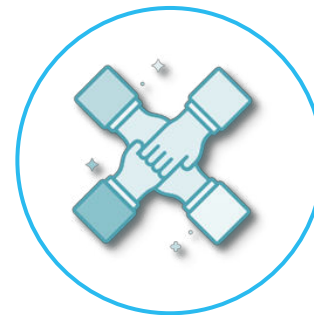
היסודות



סיסמאות - מחרוזת של תווים מוצפנים ומשמשים לאימות משאבים דיגיטליים.



Hashes - מזהים ייחודיים המחושבים על ידי יישום פונקציות מתמטיות על ערכים נתונים.



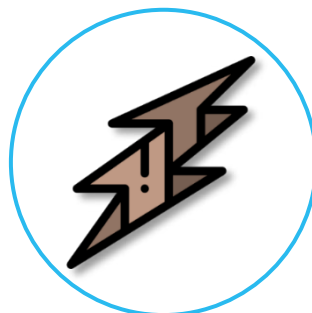
צירופים - לעתים קרובות משתמשים בסיסמאות וב-hashes יחד כדי להגן על נתונים.



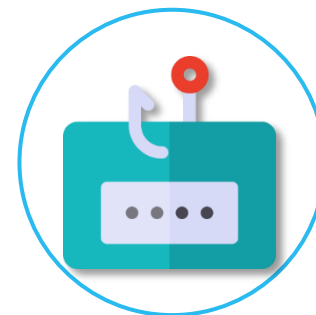
ניחוש
סיסמאות



סיסמאות
ברירת מחדל



פיצוח

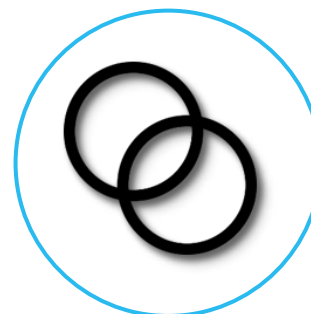


פישינג

חולשות סיסמה



סיסמאות חלשות - סיסמאות שקל לזכור הן הראשונות שהאקרים ינסו.



סיסמאות בשימוש חוזר - שימוש באותה סיסמה במספר חשבונות.



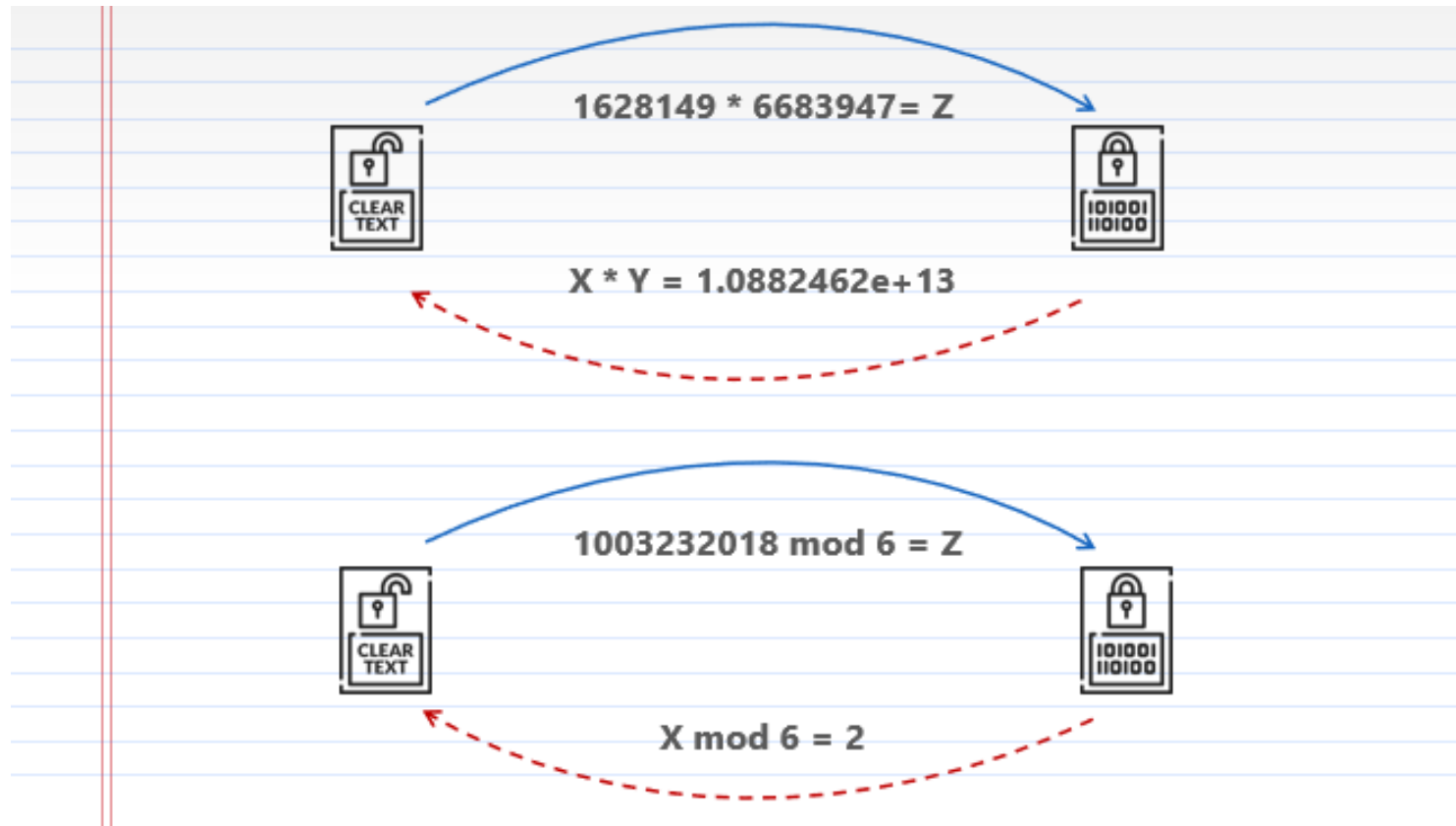
חולשת Hash - פיצוח אלגוריתמים ישנים של Hash לאורך זמן.



פונקציות חד כיווניות



ערך מגובב על ידי אלגוריתם hashing וניתן להשוות אותו לצורך זיהוי. שימוש בשני אלגוריתמים שונים לתהליך ה-hashing יקשה על הזיהוי של הערך.



סוגי Hash




מאפיינים	Hash
hash קריפטוגרפי של 128 סיביות. נחשב פגיע מאז 2012.	MD5
hash קריפטוגרפי של 160 סיביות. מתקפת ההתנגשות הראשונה בוצעה בשנת 2017.	SHA-1
hash קריפטוגרפי של 256 סיביות. משתמשים בו בעיקר ב-SSH ו-SSL.	SHA-256
טקסט מקודד מחדש בקבוצות ה-hash עם MD4. משמש במערכת הפעלה Windows OS.	NTLM
גרסה משופרת של NTLM. משתמשת ב-salting וחותמות זמן נגד PTH.	NetNTLM
נחשב לחזק מאד. משתמש בחתימה דיגיטלית אסימטרית.	RSA



תרגול קצר - Hashes של קבצים



15-20 דקות 

המשימה

יש להשיג את ה-hash של קובץ טקסט באמצעות שירות מקוון.

השלבים

- יש ליצור שני קבצים עם אותו תוכן ושמות שונים.
- יש ליצור קובץ אחד עם תוכן שונה.
- יש להעלות את הקבצים אל:
<https://md5file.com/calculator>
- יש לחקור את התוצאות.

כלים

קבצים קשורים



CYBER SCHOOL

סוגי מתקפות סיסמה



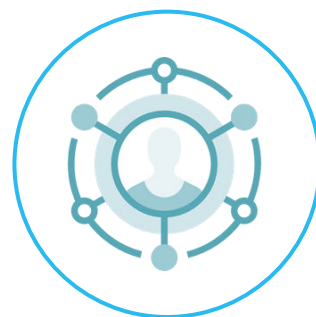
Brute-Force



טבלת
Rainbow



מילון



מילון שעבר
מוטציה



פיצוח
RAR/Zip





ססמאות חזקות - סיסמאות מורכבות ולא נפוצות.



מגבלות ניסיונות כניסה - יכולות למנוע מתקפות
.Brute-Force



Ban2Fail - בוחן יומני מערכת וניסיונות כניסה
בושלים, ומאפשר סינון.



מעבדה: הצפנה ופענוח של Hashes



15-20 דקות

המשימה

יש להשתמש באלגוריתם MD5 כדי ללמוד על החולשה של hashes מיושנים.

השלבים

יש ליצור ערך ואת ה-hash שלו ולהשוות ביניהם.

קבצים קשורים

מסמך מעבדה

כלים

Kali Linux

Firefox

עורך טקסט



CYBER SCHOOL



שאלות?

