



ספר קורס



התקפת Brute-Force

עמוד 1 -

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

מידע על ספר לימוד זה

מסמך זה הוא ספר לימוד עבור הקורס המלא של האקינג אתי. הוא מכיל את כל המידע שהמנחה יציג בכיתה.

ספר הלימוד מלווה את הקורס כולו, לפי סדר כרונולוגי, משלב ההתחלה ועד לחומר המתקדם של הקורס.

מקרא

קטעי טקסט צבעוניים מופיעים לאורך מסמך זה כדי להפנות את הקורא למקור ספציפי, או להעשיר אותו במידע נוסף.

קטעי הטקסט הצבעוניים כוללים את הנושאים הבאים:

משימת מעבדה



יש לעיין בקבצי המעבדה התואמים כדי לתרגל את מה שנלמד עד כה. תיבת טקסט זו כוללת גם שאלות ספציפיות לתרגול.

טוב לדעת



מידע נוסף או תובנות לגבי הנושא. מידע זה נועד לצורך העשרה בלבד ואינו חלק מהחומרים עליהם תיבחנו.

טיפ



מידע שימושי שיש בו כדי לסייע לתלמידים ללמוד את החומר או לעבוד עם כלים מסוימים.

מידע נוסף



קישורים או הפניות לחומר חיצוני שניתן להשתמש בהם כדי להרחיב את הידיעות שלכם לגבי הנושא.

מבוא

התקפות Brute-Force הן נפוצות וניתן לבצע אותן על פני ממשקים שונים. כדוגמה, יש לדמיין תוכנית שעוברת לאתר ספציפי, מקלידה את שם המשתמש שלכם, מנסה סיסמה ולוחצת על כפתור ההתחברות בעצמה. לאחר מכן היא חוזרת על תהליך זה עוד 100 פעמים.

כלים רבים המבצעים התקפות הקשורות ב-Brute-Force זמינים להורדה או לשימוש מקוון, אך ניתן לכתוב את חלקם למטרות ספציפיות.

פרק זה עוסק במה שההתקפות הללו עושות, כיצד הן מבוצעות על ידי כלים מסוגים שונים, ומה ניתן לעשות כדי להתגונן מפני התקפות כאלה.

סיסמאות הן מחרוזות של תווים המשמשים להצפנה ואימות של משאבים דיגיטליים, כגון קבצים, יישומים, חשבונות, טלפונים ניידים, מחשבים ועוד. סיסמאות חזקות מורכבות בדרך כלל משילוב של אותיות, מספרים ותווים מיוחדים.

טוב לדעת



בתחום אבטחת הסייבר, סיסמאות מורכבות הן דבר חשוב. סיסמה מורכבת כוללת אותיות גדולות, אותיות קטנות, מספרים ותווים מיוחדים.

Hashes הם מזהים ייחודיים המחושבים על ידי יישום פונקציות מתמטיות על ערכים בגודל שרירותי. בשל התכונה החד-כיוונית שלהם, הם יכולים להגן על נתונים מועברים או מאוחסנים מפני חבלה.

אלגוריתמים של Hashing מבצעים פעולות מתמטיות נוספות בסיסמה לפני שמירתה בדיסק.

לעתים קרובות משתמשים בסיסמאות וב-hashes יחד כדי להגן על נתונים. לדוגמה, ניתן ליצור hashes של סיסמאות לביצוע אימות.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# cat /etc/shadow  
root:$6$Qus/lc0s$fDzMTF8yHWMrZlF6Ja3Xh0EIyIasHFLcqwyrf8QNzlHVtAaeXD0Cv7uiGNWR  
aiTK2gdcu8kf.dcjSmJZCzXkT1:17737:0:99999:7:::  
daemon*:17633:0:99999:7:::  
bin*:17633:0:99999:7:::  
sys*:17633:0:99999:7:::  
sync*:17633:0:99999:7:::  
games*:17633:0:99999:7:::  
man*:17633:0:99999:7:::  
lp*:17633:0:99999:7:::  
mail*:17633:0:99999:7:::  
news*:17633:0:99999:7:::  
uucp*:17633:0:99999:7:::  
proxy*:17633:0:99999:7:::  
www-data*:17633:0:99999:7:::  
backup*:17633:0:99999:7:::  
list*:17633:0:99999:7:::  
irc*:17633:0:99999:7:::  
gnats*:17633:0:99999:7:::  
nobody*:17633:0:99999:7:::  
_apt*:17633:0:99999:7:::  
systemd-network*:17633:0:99999:7:::  
systemd-resolve*:17633:0:99999:7:::  
mysql!:17633:0:99999:7:::  
epmd*:17633:0:99999:7:::
```

סימאות בפורמט לינוקס שעבר Hashing

טיפ

לעיתים מתייחסים ל-Hashing בטעות כסוג של הצפנה. עם זאת, ניתן לפענח הצפנה, בעוד שאת ה-hashes לא ניתן לפענח.



שיטות מתקפה

ניחוש סימאות

רוב מתקפות הסימאות אינן כרוכות בפיצוח ממשי, ובמקום זאת מסתמכות על שיטות ניחוש ברמת המומחים. תוקפים שאין להם מושג מהי הסיסמה, יכולים לנסות לנחש אותה על סמך סימאות אקראיות ונפוצות, כגון Pa\$\$w0rd, 1234, qwerty, Aa123456 וכו'.

מידע נוסף

בכל שנה מתפרסם מאמר המתמקד בסימאות הנפוצות ביותר של השנה:
<https://rockit.cloud/2020/02/18/the-most-commonly-used-password-in-2020-is/>



סימאות ברירת מחדל

חלק מהשירותים כוללים אמצעי אבטחה שהוגדרו מראש עם סימאות ברירת מחדל שקל לנחש, או כאלה שמתפרסמות כאישורי ברירת מחדל לצורך גישה למערכת. שמירה על סימאות אלה כברירת מחדל, מבלי לשנות אותן, עלולה להוביל לגישה בלתי מורשית. אנשים רבים משתמשים באישורי ברירת מחדל עבור מצלמות, נתבים והתקנים אחרים.

מידע נוסף

Shodan הוא מנוע חיפוש למכשירים המחוברים לאינטרנט שיכול לספק מידע על מצלמות אינטרנט, נתבים וסימאות ברירת המחדל שלהם:
<https://www.shodan.io/explore>



פיצוח

פיצוח סימאות קצת מורכב יותר מכיוון שהוא דורש חומרה ותוכנה כאחד. לגבי תוכנה, קיימת תוכנית שתנסה באופן אוטומטי שילובי תווים שונים ותשווה את התוצאות עם ה-hash הידוע. מהירות הפיצוח תלויה במורכבות האלגוריתם ובחומרה המבצעת את תהליך החישוב. סיסמה שעברה hashing על ידי SHA-512 עשויה להיות בטוחה יותר מאשר סיסמה שעברה hashing על ידי SHA-256. נדון באלגוריתמים של Hashing בהמשך פרק זה. יש גם הבדל בין רכיבי חומרה של CPU ו-GPU, שגם בהם נדון בהמשך הפרק. הכדאיות של שיטה זו, לעומת זאת, תלויה ביכולת לבדוק סימאות שונות שוב ושוב, ללא הגבלה.

טוב לדעת

למחשב שיכול לפצח סיסמה בת שמונה תווים תוך 4.2 שעות ידרשו 5.7 טריליון שנים כדי לפצח סיסמה בת 16 תווים.



פישינג

כאשר פיצוח סיסמה אינו אופציה, בשל מורכבותו או דרישות קפדניות, ניתן להשתמש בשיטות אחרות, כגון פשינג. נדרש הרבה פחות מאמץ לגרום למשתמש לחשוף סיסמה באמצעות אתר מזויף מאשר ניסיון לפצח אותה.

חולשות סיסמה

ככל שמחשבים מתפתחים עם כל שנה שחולפת, כך מתפתחת היכולת של ההאקרים לפצח סיסמאות. סיסמאות של שמונה ספרות, שפעם נחשבו למאובטחות, מפוצחות היום בקלות בגלל כוח המחשוב והטכנולוגיה.

אנשים מחזיקים בחשבונות משתמש למספר שירותים, מחשבונות דוא"ל ועד חשבונות בנק, חשבונות מדיה חברתית ועוד. שימוש באותה סיסמה עבור חשבונות שונים הוא נוהג נפוץ בקרב אנשים, מכיוון שקל יותר לזכור את פרטי ההתחברות שלהם כך, והאקרים יודעים זאת. במקרים כאלה, מספיק לפצח סיסמה אחת כדי לפצח את כל סוגי חשבון המשתמש.

החולשה העיקרית של אלגוריתמים של hashes היא שעל פני זמן ממושך הם עלולים לגרום לכפילות או התנגשות. מעת לעת מפותחות שיטות חדשות שהן מורכבות ומאובטחות יותר.

אלגוריתם ה-hash של MD5 כבר אינו נחשב מאובטח, ובקרב גם ה-SHA-1 ילך בעקבותיו. באופן דומה, בקרב סיסמאות ידרשו לפחות 10 ספרות ויכללו מדיניות מורכבת יותר.

מידע נוסף

מאמר שפורסם על ידי ZDNet באמצע 2019 טען כי 25% ממערכות ה-CMS הגדולות עדיין משתמשות באלגוריתם ה-MD5 hashing:
<https://www.zdnet.com/article/a-quarter-of-major-cms-use-outdated-md5-as-the-default-password-hashing-scheme>



טוב לדעת

אתר MD5 מציע פתרון מקוון לחישוב hashes שונים. hash של ערך תמיד יהיה זהה כל עוד נעשה שימוש באותו אלגוריתם, ללא תלות בפלטפורמה.

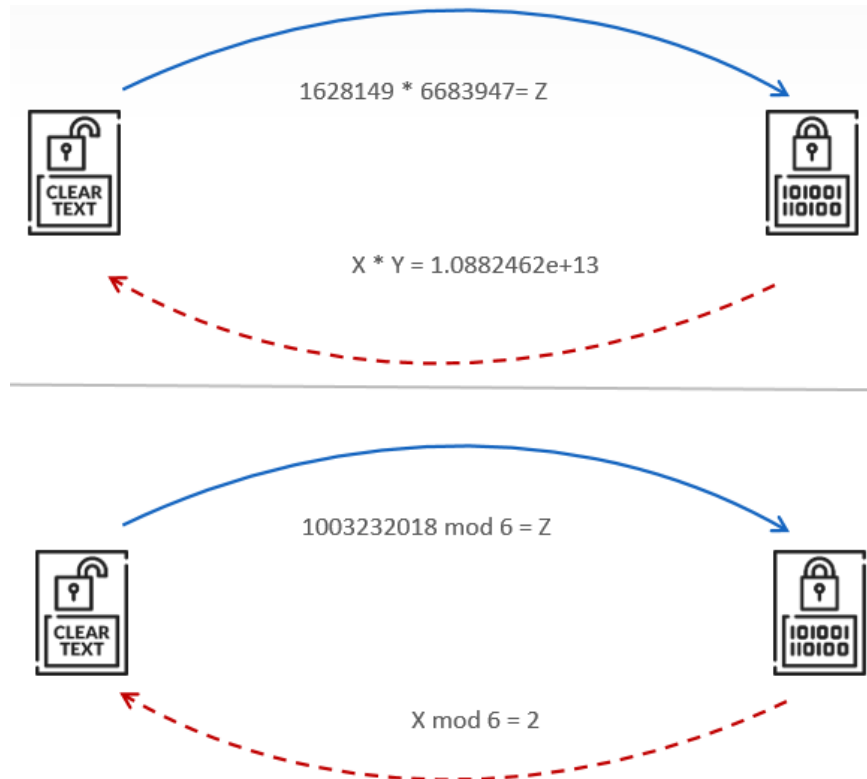




מחשבון Hash מקוון

פונקציות חד כיווניות

Hashing משתמש בחישובים בכיוון אחד, ובחישובים מורכבים יותר בצד השני. שילוב של פירוק לגורמים ראשוניים ומודולציה הופך את פונקציית ה-hash לבלתי הפיכה (או לפחות קשה להפיכה).



חישוב אלגוריתם Hash

עמוד 7 -

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

סוגי Hash

במהלך השנים פותחו סוגים שונים של פונקציות hash לשימושים שונים. ההבדלים העיקריים בין הפונקציות הם אורך ערך ה-hash שנוצר והפרמטרים והתהליך של כל אלגוריתם.

MD5: hash הצפנה של 128 סיביות שנחשבת פגיעה מאז 2013.

SHA-1: hash קריפטוגרפי של 160 סיביות. מתקפת ההתנגשות הראשונה נגד SHA-1 בוצעה בשנת 2017.

SHA-256: hash קריפטוגרפי של 256 סיביות, המשמש בעיקר בהצפנת SSH ו-SSL.

NTLM: טקסט מקודד מחדש בקבוצות ה-hash עם MD4. משמש במערכת הפעלה Windows OS.

NetNTLM: גרסה של NTLM המשתמשת ב-salting ובחותמות זמן למניעת PTH.

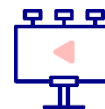
RSA: נחשב לאלגוריתם הצפנה חזק מאוד המשתמש בחתימה דיגיטלית א-סימטרית.

טיפ



כל ה-hashes שלעיל ניתנים לחישוב באמצעות מחוללי מחשבוניים ומחוללי hashes מקוונים.

תרגול קצר: Hashes של קובץ



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

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. <

סוגי מתקפות סיסמה

התקפות **מילון (Dictionary)** הן הנפוצות והקלות ביותר לביצוע באמצעות סיסמה או שירות התחברות. ההתקפה מבוססת על מספר רב של סיסמאות נפוצות ו/או מותאמות אישית היוצרות יחד מילון סיסמאות.

Brute-force כרוך בניסיון של סיסמאות בזו אחר זו עד שמתגלה הסיסמה הנכונה. אם ידועה סיסמה חלקית, התווים הידועים ייכללו בהתקפה, דבר שיוביל לרזולוציה מהירה יותר. זוהי השיטה האיטית ביותר.

התקפת מילון שעברה מוטציה משתמשת ברשימת סיסמאות מותאמת אישית, מחליפה את הסיסמאות ומוסיפה מספרים ודפוסים אקראיים.



טוב לדעת

התקפת מילון שעברה מוטציה היא ההתקפה השכיחה ביותר בה משתמשים נגד שירותים מקוונים (כניסות SSH, RDP ו-FTP).

טבלאות Rainbow הן טבלאות גדולות המכילות hashes מחושבים מראש של ערכים מסוימים. הטבלאות משמשות לביצוע הצפנה הפוכה על פונקציות hash. התקפה מסוג זה היא לרוב מהירה יותר מהתקפות אחרות של brute-force. בדרך כלל, מסדי נתונים ומתארים מקוונים משתמשים בסוג זה כדי לספק מענה מהיר.

פיצוח RAR/zip הוא שיטה להשגת גישה לקבצים המוגנים באמצעות סיסמה המצורפים בקבצי RAR או zip. כלים מקוונים, כגון rar2john, זמינים לפיצוח קבצים מסוג זה.

אמצעי הגנה

סיסמאות חזקות

אלגוריתמי הצפנה, טובים ככל שיהיו, עדיין אינם מספיקים כדי להגן לחלוטין מפני התקפות של brute-force. הגנה חזקה יותר צריכה לכלול שימוש בסיסמאות מורכבות יותר ואקראיות יותר. הסיסמאות חייבות להיות מורכבות משילובים של אותיות קטנות וגדולות, סמלים ומספרים.

מגבלות ניסיונות כניסה

הגבלת מספר ניסיונות התחברות רצופים היא הגנה מצוינת מפני התקפות מרחוק. ניתן ליישם אותה באמצעות כלים מובנים או תוכנות צד שלישי.

Fail2ban

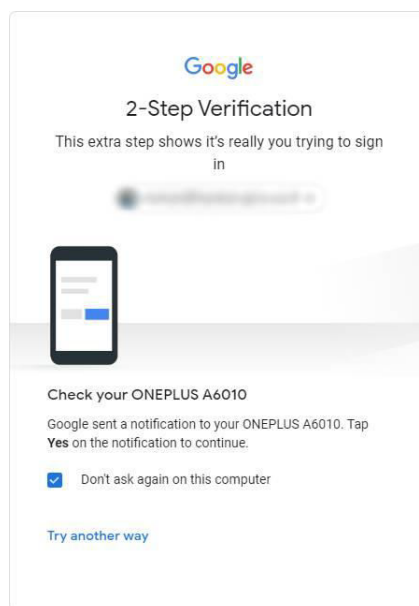
Fail2Ban פועל כ-IPS שבוחן יומני מערכת וניסיונות כניסה כושלים. הוא מאפשר סינון על בסיס כללים, כגון פסקי זמן ומספר מרבי של ניסיונות התחברות.



Fail2Ban

אימות מרובה גורמים או אימות דו-גורמי (2FA)

זוהי שיטת אימות בה ניתנת גישה למשימה ספציפית רק לאחר הצגת שני גורמים או יותר, כגון אימות SMS או אימייל, למנגנון האימות.



דוגמה לאימות דו-גורמי של Google

עמוד 10 -

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

משימת מעבדה: הצפנה ופיצוח של Hashes
השתמשו באלגוריתם MD5 כדי ללמוד על החולשות של hashes מיושנים.

