**Identifies a Brute Force attack**

:Executive summary

דוח זה מציג את הפיתוח והיישום של סקריפט פייתון המיועד לזיהוי התקפות Brute Force מתוך נתוני לוגים של שרת. המטרה המרכזית של הפרויקט היא לחזק את אבטחת המערכות על ידי זיהוי ניסיונות כניסה מרובים וכושלים בזמן קצר, אשר עלולים להעיד על ניסיונות פריצה. באמצעות ניתוח ניסיונות הכניסה הכושלים והמצליחים, הסקריפט מאפשר זיהוי מוקדם של איומים פוטנציאליים ומתן התראה בזמן אמת לצוותי האבטחה.

:TECHNICAL OVERVIEW

הסקריפט נכתב בפייתון ומשתמש בספריות csv, datetime, re ו-pprint. הנתונים מאוחסנים בקובץ CSV הכולל עמודות כמו כתובת IP, קוד סטטוס, סוג הבקשה וזמן האירוע. הסקריפט מבצע את השלבים הבאים:

**קריאת הנתונים:** פתיחת קובץ ה-CSV וקריאת השורות באמצעות csv.DictReader.

**סיווג ניסיונות הכניסה**:  
ניסיונות כושלים: זיהוי שורות עם קוד סטטוס 401 ובקשה המכילה את המילה "login".  
ניסיונות מוצלחים: זיהוי שורות עם קוד סטטוס 200 או 201 ובקשה המכילה את המילה "login".

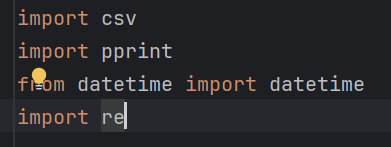
**זיהוי התקפות Brute Force:** עבור כל כתובת IP עם מספר ניסיונות כושלים, הסקריפט מחפש שלושה ניסיונות עוקבים שהתרחשו בתוך חלון זמן של חמש דקות.

**הפקת דוח:** איסוף הנתונים המזוהים והצגתם בצורה מסודרת באמצעות pprint.

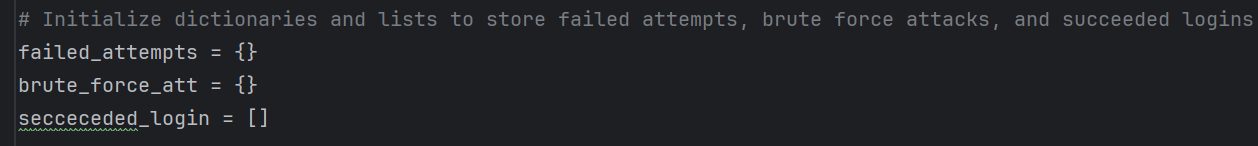
:TECHNICAL DIVE

הקוד מורכב מהשלבים הבאים:

1. **ייבוא ספריות:**

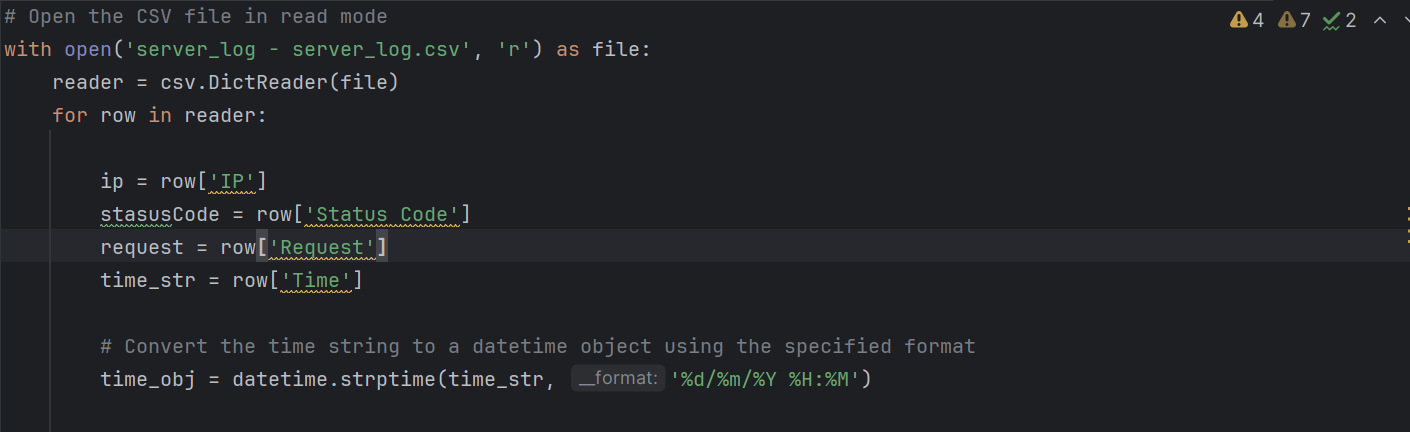


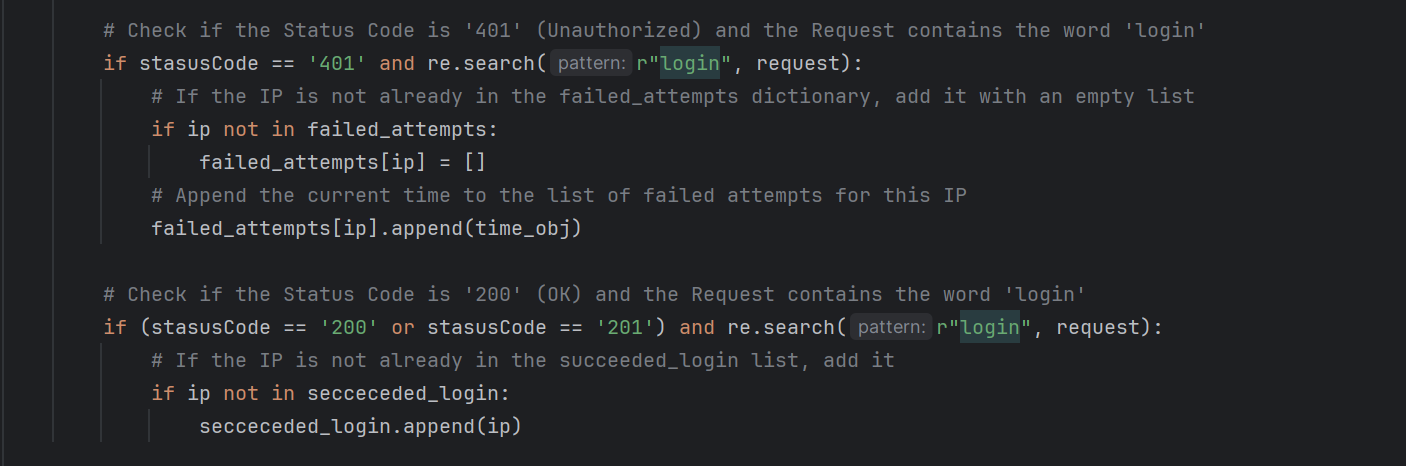
1. **אתחול מבני נתונים**:



1. **קריאת קובץ ה-CSV והכנסת הנתונים הרלוונטים למבני הנתונים:**

במידה ויש נסיון התחברות עם שגיאה 401 ו זהו נסיון login נכניס את את הפרטים לfailed\_attempts  
במידה ו- IP מסויים מצליח לעשות login - כלומר סטטוס 200/201 נכניס אותו לרשימת secceded\_login

****

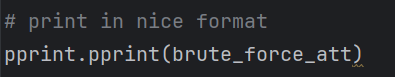
****

1. **הפללת הIP החשודים וסידור שלהם במילון אחד עם כל הפרטים:**

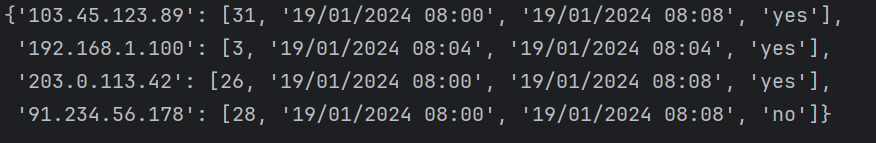
בתוך המילון מסודר לנו הIP של התוקף,כמה פעמים ניסה להיכנס, זמן התחלה, זמן נסיון פריצה אחרון, והאם הצליח להיכנס או לא.

****

1. **הדפסה של הנתונים:**

****

**הפלט:**

****

CONCLUSIONS AND SUMMARY:

הסקריפט יעיל לזיהוי התקפות Brute Force מתוך נתוני לוגים של שרת. באמצעות ניתוח ניסיונות הכניסה הכושלים, הסקריפט מאפשר זיהוי מוקדם של ניסיונות פריצה מרובים ומנגיש בצורה מסודרת את הנתונים על IP ספציפי.

הסקריפט שפיתחתי חשוב משום שהוא מסייע בזיהוי מוקדם של התקפות Brute Force, אשר מהוות איום משמעותי על אבטחת המערכות והנתונים של חברות וארגונים. התקפות אלו עלולות להוביל לדליפות מידע, פגיעה באמינות החברה ואובדן אמון הלקוחות, מה שעלול לגרום להפסדים כלכליים ונזק במוניטין. באמצעות הסקריפט, ניתן לזהות ולנטר ניסיונות כניסה כושלים מרובים בזמן קצר, ולאפשר תגובה מהירה למניעת גישה בלתי מורשית. הפרויקט הזה לא רק פותר בעיה ממשית בתחום האבטחה, אלא גם משפר את הידע הטכני שלי ומחזק את עמידת הקהילה בסייבר. המטרה הייתה להעמיק את ההבנה שלי בניתוח לוגים ובזיהוי איומים, ולתרום לכלים שמסייעים בשמירה על סביבה דיגיטלית בטוחה יותר.

**נכתב על ידי:**רועי כהן  
SOC Analyst

**תאריך:**26.01.2025