דו"ח מעבדה- תרחיש מס' \_01\_

# פרטים:

מגיש: ברק שרעבי

תאריך: 01/11/18

שם התרחיש: Apache shutdown

# תהליך ההתקפה:

תהליך ההתקפה התבצע באמצעות Port-Scanning התוקף ביצע סריקה לכל הפורטים הקיימים ולכל אחד מהם שלח בקשה לבדיקה האם יקבל איזשהו תשובה, בכך התוקף הצליח למצוא פרצה לאחד מן הפורטים שהוא פורט הSSH (22) ומצא "אוזן קשבת"

לאחר מכן הפורץ עשה Brute Force לROOT ובכך הסיסמא נפרצה והצליח לגשת לשרת.

לאחר הפריצה ה"האקר" השתיל קבצים בתוך השרת שהם

קובץ – Bash

קובץ – Python

ובנוסף פעל עם הCronTab - (מתזמן המשימות) שהוא הפעיל באופן מתוזמן שני משימות

באופן סדור כל שניה.

* Stop service apache
* הפעיל את קובץ ה – Bash

כל פעם שהמשימה המתוזמנת פעלה מה שקרה זה ששירות apache נפל וקובץ ה – Bash

הפעיל את קובץ ה – Python שאחראי על העברת קבצי ה Shadow & password בסטרינג הישר לתוקף ובכך הצליח התוקף לראות את קבצי האש והסיסמאות.

# תהליך הזיהוי:

תהליך הזיהוי הראשוני התבצע באמצעות תוכנת ה- ArcSight שיודעת לנתח לוגים מכמות גדולה של שרתים ובהתאם לחוקים שהוגדרו מתריע על חריגות.

בשעה 7:13 UTC לערך התראה ראשונית התקבלה בתוכנה והתריעה על כתובת IP 199.203.100.231 המנסה לגשת למקום אסור 130.2.1.21 שזוהי כתובת IP של שרת אפצ'י האחראי על אתר FOXNEWS.

זאת התבצע על פי תוכנת ה Nmap למיפוי פורטים פתוחים ולחדירה דרכם

ARCSIGHT

ZENUS

גישה לאתר לא התאפשרה.

# תהליך הגנה:

# תהליך הגנה מונעת:

החלפת סיסמאות בכלל הארגון

# הפרצות באבטחת הארגון

האפשרות לעשות סריקת פורטים וbrute force גישה ב SSH מחוץ לארגון

# אופן עבודת הצוות

# חוסרים/קשיים