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 ל ROOT ובכך הסיסמא נפרצה והצליח לגשת לשרת.

לאחר הפריצה ה״האקר״ השתיל קבצים בתוך השרת שהם

קובץ – Bash

קובץ – Python

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

באופן סדור כל דקה.

- Stop service apache
- הפעיל את קובץ ה – Bash.sh

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

ביצע העתקה של קבצי Shadow & password לתוך תיקיית tmp ומיד לאחר מכן

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.

ה- ArcSight התריע על שני מקרים

1. Port-scanning
2. Password guessing detected

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

לאחר מכן ניסיון גישה לאתר לא התאפשר.

כשאר ניגשנו לכלי ה Zenoss ממשק אינטרנט המאפשר למנהלי מערכת לפקח על זמינות, מלאי / תצורה, ביצועים ואירועים בשרת.

קיבלנו התראה על אי פעילות של שירות Apache2 שזהו שירות המפעיל/נותן גישה לאתר.

ניגשנו לשרת Apache וביצענו סריקת רקורסיבית אחר IP של התוקף.

הממצאים הראו כי התוקף הפעיל את מתזמן המשימות שביצע באופן סדור כל דקה הפסקה של פעילות השירות Apache2 ובנוסף הושתלו שתי קבצים בשרת.

תהליך הגנה :

תהליך ההגנה הראשוני באירוע מסוג זה הוא חקיקת חוק חדש למניעת תקשורת בין "האקר" לשרת הארגון.

זאת עושים באמצעות תוכנת Smart view Tracker של חברת צ'ק פוינט.

חוק ראשון שנחקק הוא אי מתן גישה לכתובת הIP לתוך הארגון.

חוק שני שנחקק חסימת כל היציאות של השרתים לתקשורת עם התוקף.

לאחר מכן מצאנו שתי קבצים שהתוקף השתיל בשרת אותם העברנו לתיקייה Do_not_open על מנת לעצור את התקיפה ולשם חקירתם בהמשך.

תהליך הגנה מונעת :

לשם הגנה על הארגון עליו לחקור את הקובץ שהושתל לתוכה תוך כדי שינוי סיסמאות הארגון והפקת הלקחים.

- חסימת גישה ב SSH(22) מחוץ לארגון.
- הרשאות גישה לצוות הארגון בלבד
- חסימת משתמש לאחר מספר ניסיונות
- מתן הרשאות לתיקיות מערכת לעובדי הארגון בלבד

הפרצות באבטחת הארגון

פורט SSH (22) שהייה פתוח ואפשר לתוקף גישה לשרת וביצוע Brute Force ל ROOT

- גישה ב SSH(22) מחוץ לארגון.
- אי חסימת משתמש לאחר מספר ניסיונות
- הרשאות לתיקיות מערכת שלא לעובדי הארגון

אופן עבודת הצוות

הצוות חווה קושי בשיתופי פעולה למיגור התקיפה וזאת בשל חוסר ידע, ניסיון והכרות עם התוכנות השונות.
על הצוות ללמוד לעבוד בשיתוף פעולה יחד עם מתפעל האירוע וכמובן לצבור ניסיון וידע בתוכנות השונות על מנת לעצור את התקיפה הבאה.
הצעות ייעול – על הצוות בזמן תקיפה לשבת ולחלק עבודה כדי לייעל את תהליך ההגנה.

חוסרים/קשיים

הקשיים הבולטים באירוע מסוג זה הוא חוסר היכרות עם מצבים אלו, סנכרון בין כל עובדי הארגון ובעיקר חוסר ניסיון וידע בתפעול אירועים מסוג זה.