דוי״ח מעבדה- תרחיש מס׳ _1_

פרטים :

מגישים : יגאל נאמן

תאריך :11.11.18

שם התרחיש :מתקפת Apache Shutdown

תהליך ההתקפה :

תהליך שבו התוקף חודר לשרת האפצי שלי

מתקין עליו אקספלוייט שנכתב בפייתון, אותו אקספלוייט(וירוס) מה שהוא בעצם עושה זה

מתקין עצמו על ה- ROOTב- /var/tmp/ שם כל משמש יכול לקבל גישה (VULNIRABILEשלא תוקן כביכול)

עם ההרצה של האקספלוייט הוא מעתיק (שולח לכתובת התוקף) את כל הסיסמאות שיש ב Shadow ובעוד מקום נוסף ששייך גם כן למשתמש ה- ROOT

לאחר מכן מבצע הוירוס פעולת כיבוי של השרת אפצי , זאת אומרת מכבה את הסרביס

Apache service stop

כל זה קורה כאשר תחת האקספלוייט שרץ.

דבר נוסף שייתכן שקורה הוא ושצריך לבדוק זאת :

בשרתי ה-

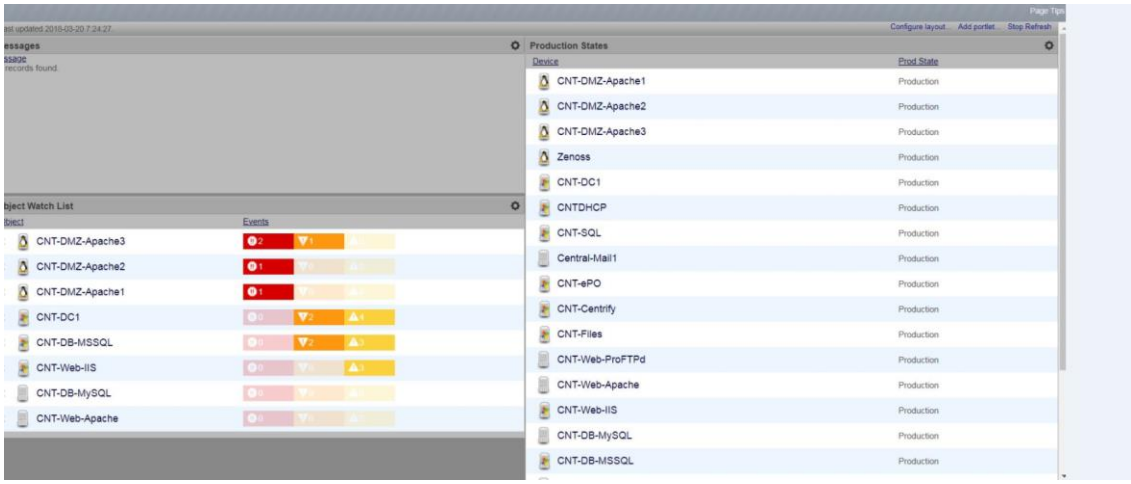
Apache1,apache2,apache3

במהלך ההתקפה התוקף שולח בקשת PASSWORD GUSSING לאחד משרתי apache וה apache מחזיר לו בתגובה ack כלומר הוא מצפה לתשובה בחזרה ack אך הוא איננו מקבל תשובה בחזרה כתוצאה מכך הפורט תפוס והתוקף שולח הרבה בקשות בזמן קצר וכתוצאה מכך נופלים השרתים ואינם מספקים את השירותים קבלת דף html

תהליך הזיהוי:

1)כניסה ל zenoss

בzenoss נמצא שלושת שרתי ה apache שמספקים שירותי web נפלו



לאחר מכן נכנסתי לבדוק את הזמנים של נפילת השרתים שהזמנים משמשים לי

נכנסתי בעקבות זאת לשרת ה APACHE

ל- לוגים של המערכת /LOGS/TMP/VAR

עשיתי CATלקובץ

ואז ראיתי בקובץ הלוג שהיה בתאריך ובשעה 11.11.18 שיש התקנה של קובץ בתקייה

בשביל לבדוק מה קרה – ואז גליתי שיש אקספלוייט שמותקן התקייה

:/~ROOT@:/var/tmp/Apacche_shutdown.py

2)smartview tracker –בשלב זה פילטרתי את התעבורה לפי השעה שבה השרתים נפלו ראיתי כי הוא קיבל פקטה אחת (מהתוקף)

חיקקתי חוק שמבצע DROP לכתובת האייפי של התוקף זאת אומרת שהוא יחסום את התוקף והתוקף לא יוכל לשלוח בקשות יותר לשרתי האפצי

כמובן שגדרנו את זה בתור RULS ANY ANY עם לוגים והכל.

תהליך הגנה:

מניעה עכשווית-במידה ואנו מזהים בזמן קצר הרבה בקשות יש למנוע זאת ולהגביל את כמות הבקשות בזמן קצר (פיקוח על בקשות בזמן קצר)

תהליך הגנה מונעת:

מניעה לטווח הארוך – במידה והשרת רואה זמן המתנה ארוך מהמשתמש יעשה יסגור את ה socket (חיבור)

הפרצות באבטחת הארגון

1)לא היה חוק שמגביל את כמות הבקשות בזמן קצר \ או את כתובת התוקף \ ואו את ה-CLASS שלו

2)לא הוגדר חוק ב ARCSIGH FIREWALL ולכן הפרצת אבטחה יצאה לפועל

כלים שפיתחנו

בתרחיש זה עדיין לא פיתחנו איזשהו כלי

אופן עבודת הצוות

במהלך עבודתנו חילקנו תפקידים :

1)ניגש ל zenoss וזיהה כי השרתים נפלו

2)חקר את הפאקטות ב firewall

3)נכנס לשרתים עצמם כדי לראות שאין כניסות לשרתים

4)ניהול התרחיש וחילוק תפקידים יגאל

חוסרים/קשיים