דוי"ח מעבדה- תרחיש מס' _1_

פרטים:

מגישים: יגאל נאמן 300369972

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

(vulnerability שלא תוקן- מסיבה שכנראה לא עידכנו את המערכת Apt-get update)

עם ההרצה של EXPLOITE 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-

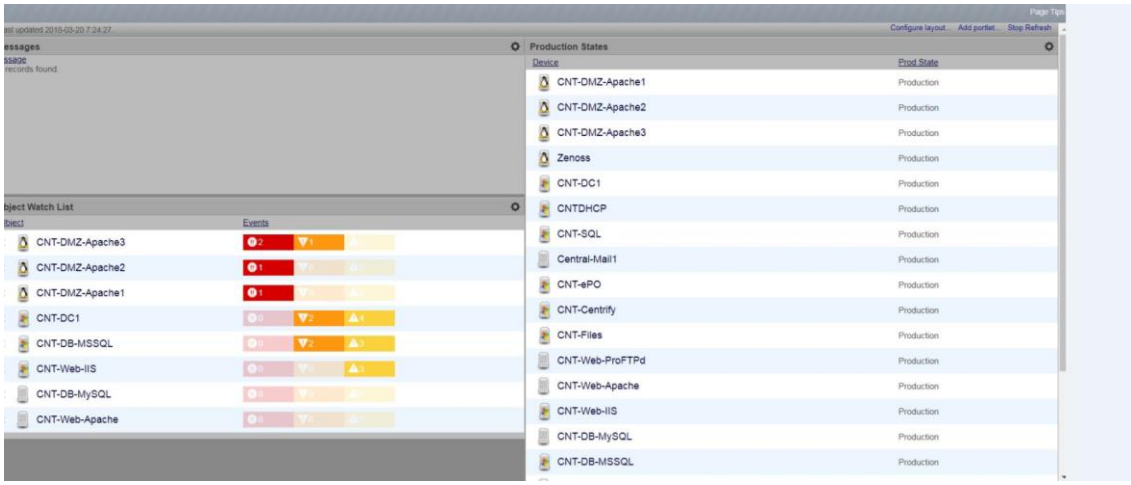
Apache1,apache2,apache3

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 מתקפה זאת נקראת גם DDOS..... כיוון שיש עומס של בקשות על השרתים

תהליך הזיהוי:

1)כניסה ל zenoss

בzenoss נמצא שרת ה apache שמספק שירותי web נפל (התמונה להמחשה בלבד)



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

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) כמובן להגדיר חוקים ב a RULS

TOP ANY*ANY with logs

THAT WILL BLOCK THE ATTACKER AND KILL THE PACKET

תהליך הגנה מונעת :

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

2)smartview tracker –בשלב זה פילטרתי את התעבורה לפי השעה שבה השרת נפל

ראיתי כי הוא קיבל פקטה אחת (מהתוקף)

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

כמובן שגדרנו את זה בתור RULS ANY ANYעם לוגים והכל.

הפרצות באבטחת הארגון

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

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

כלים שפיתחתי

בתרחיש זה עדיין לא פיתחנו איזשהו כלי

אופן עבודתי

במהלך עבודתי חילקתי תפקידים :

1)ניגשתי ל zenoss וזיהיתי כי השרת נפל

2)חיקקתי חוק (חסימה) לפאקטה ב firewall

3)נכנסתי לשרת עצמו כדי לראות שאין כניסות לשרת TOP וודאתי שאיין הרצות של אקספלוייטים נוספים ממשתמשים ברשת

חוסרים/קשיים/יתרונות

יותר מידיי סיסמאות ותוכנות הגנה, צריך לזכור כל דבר מה זה מה ולכן זה מבלבל..

יתרון שלי הוא שאני כבר יודע לעבוד עם לינוקס ואני שקצת יותר מבין בסייבר חקרתי כבר פעם כמה בוטנטים שהיו מחוברים לרשתות ה IRC