דו"ח מעבדה- תרחיש מס' 2

פרטים:

מגיש: מירב בוים 206489155

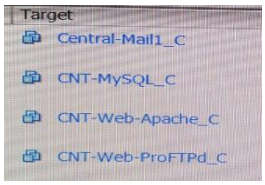
תאריך: 30.4.2018

שם התרחיש:

תהליך ההתקפה:

עובד בחברה הוריד קובץ מיוטיוב player.jar

בקובץ זה הייתה נוזקה שלא הצלחנו לזהות מה היה בה כי הקובץ מחק את עצמו (קובץ זמני). הנוזקה הפילה לחברה מספר שרתים.



בנוסף גם zenoss נפל

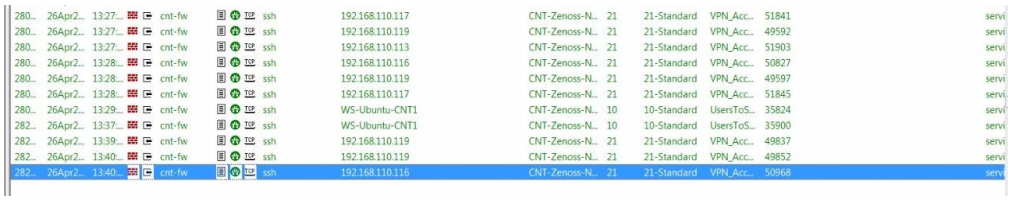
בנוסף על מנת לבלבל אותנו התוקף שינה את התאריכים של קבצים רלוונטים לתחקיר כדי שלא נסתכל עליהם כחשודים.

תהליך הזיהוי:

ראינו שה zenoss נפל. הלכנו לכלי vmware כדי להרים אותו, הרמנו אותו ואז ראינו ב zenoss שנפלו לנו עוד שרתים.

הרמנו את השרתים ואז התחלנו לחקור את התחנות שנפלו.

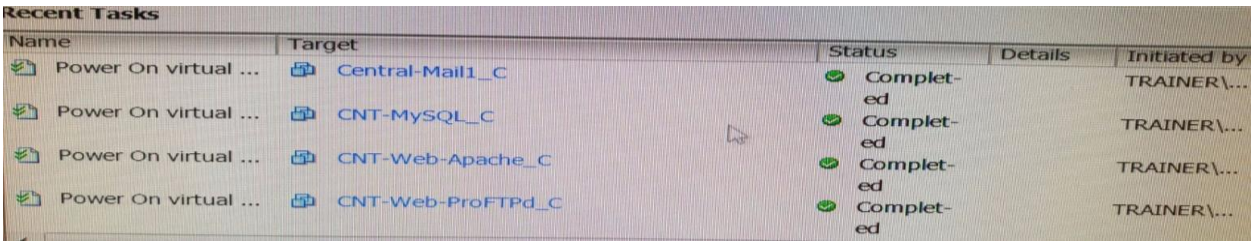
חיפשנו חיבורים חשודים לתחנות ב tracker וגילינו שיש מחשב בחברה שמחובר דרך SSH לשרתים שנפלו.



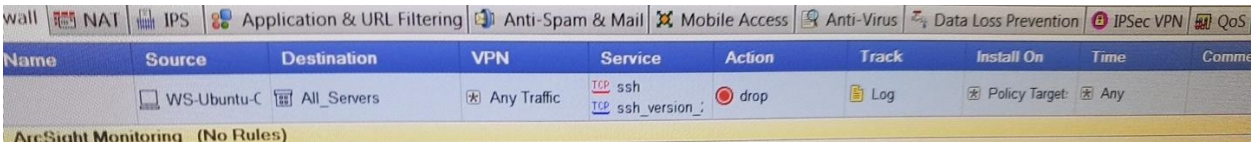
נכנסו למחשב זה דרך ה vmware והתחלנו לחקור אותו. זיהינו שהוא הוריד תיקיה לאחרונה, חקרנו את התיקיה וגילינו שהיא מכילה קבצים חשודים כמו metasploit

תהליך הגנה:

לאחר זיהוי נפילת השרתים הרמנו אותם.



לאחר הזיהוי של המחשב שגרם לנפילת השרתים חסמנו אותו ב firewall



נכנסנו לשרתים שנפלו ושינינו בהם סיסמאות

תהליך הגנה מונעת:

ניהול מדיניות סיסמאות

לא לתת הרשאות למחשבי קצה להתחבר ב SSH לשרתים שאינם אמורים לגשת אליהם.

התקנת אנטי וירוס ובדיקת קבצים במחשבי קצה.

הפרצות באבטחת הארגון

SSH פתוח
מחשבי קצה לא מוגנים
תקשורת חופשית בתוך הארגון ללא מידור

כלים שפיתחנו

לא פיתחנו

אופן עבודת הצוות

מישהו אחד ניהל את האירוע וכתב דברים על הלוח, מישהו היה אחראי לכתוב את החוקים ב firewall .
שאר הזמן כל אחד עשה מה שהיה צריך לעשות כגון בדיקת שרת מסויים שהיה צריך לבדוק או תחנה מסויימת., הרמת השרתים וכו.

חוסרים/קשיים

זיהוי איך עבד הקוד הזדוני