דו"ח מעבדה - תרחיש מס' 1

פרטים:

מגיש: דביר ברזילי

תאריך: 12.4.18

שם התרחיש: Apache shut down

תהליך ההתקפה:

התוקף ביצע סריקת פורטים וניחוש סיסמאות לשרת Apache1. הפורץ הצליח להתחבר לשרת והחל להעביר לתוך השרת נוזקה שתפקידה גם להפיל את השרת כל דקה מחדש, וגם לשלוח לפורץ את הקבצים passwd ו-shadow.

תהליך הזיהוי:

בשעה 13:11 התחילה מערכה נוספת שבה כתובת IP 199.203.100.30 ביצעה Password guessing לשרת Apache3. בדקנו את קבצי הלוגים בשרת זה וראינו שהפורץ לא התחבר לשרת.

בשעה 13:16 התחילה מערכה נוספת שזיהינו בעזרת ה-ArcSight. ראינו שכתובת IP חיצונית 199.203.100.178 מבצעת סריקת פורטים על המחשב (FoxNews) Apache1 אחרי זה (בשעה 13:18) מבצעת Password guessing. ראינו בקבצי הלוגים שבדקה זו הפורץ הצליח לחדור לשרת דרך שירות SSH. בנוסף כשבדקנו את שרת הZenoss הופיע לנו שהסרוויס Apache2 בשרת Apache1 נפל.

בשעה 13:19 זיהינו בArcSight שהשרת Apache1 מנסה ליצור תקשורת עם הפורץ בפורט 80 (199.203.100.194) .

בנוסף זיהינו ב- CRON (מתזמן תהליכים בלינוקס) שיש קובץ שרץ כל דקה מחדש על השרת.

תהליך הגנה:

כשזיהינו מי התוקפים ומה היעד שלהם ראשית כל חוקקנו חוקים חדשים בFireWall שיחסמו כל תעבורה נכנסת ויוצאת בין הרשת שלנו לפורצים. בנוסף שינינו את הסיסמה לשרת כדי למנוע נסיון חדירה נוסף דרך כתובת שונה. ניסינו להרים חזרה את השרת אך הוא נפל כל פעם מחדש. הבנו שכנראה מדובר בנוזקה שמפילה את השרת באופן אוטומטי. משם התחלנו לחפש בתוך השרת Apache1 אחר שינויים שנעשו בעקבות הפריצה ונסיון להבין מה הנוזקה שגורמת לנפילת השרת. זיהינו ב- CRON (מתזמן תהליכים בלינוקס) שיש קובץ שרץ כל דקה מחדש עם שתי פקודות, ואחת מהן אחראית על נפילת השרת. הפקודה השנייה אחראית על הרצת קובץ נוסף בשם bd_bash שגם אחראי על הרצת קובץ פייתון. זיהינו שמטרת התוקף בקבצים אלו הייתה לגנוב את קבצי ה- passwd ו- shadow. בגניבת קבצים אלו המשתמש השיג את דרך הצפנת הסמאות של הארגון, וע"י כך יכול לפענח את כל הסמאות בארגון.

תהליך הגנה מונעת:

שינוי סיסמאות בארגון. אילולא סיסמאות כאלו פשוטות (פריצה לאחר ניחוש חמישי!) הפורץ לא היה מצליח להחדיר ולגנוב קבצים ממחשבי הארגון. בנוסף כדאי לסגור את פורט 20 לפחות לתקשורת חיצונית, ובאופן כללי להיות בביקורת עליו ולאפשר גישות באופן נקודתי בעת הצורך. הגנה נוספת אפשרית היא לא ליצור הרשאות גישה (read only למי שאינו root וכדומה), למרות שבמקרה שלנו הפורץ הגיע להרשאת root.

הפרצות באבטחת הארגון

סיסמאות פשוטות מידי. הרשאות לשינוי כתיבה וקריאה לכל אדם. פורט 20 פתוח בשרתי הארגון.

אופן עבודת הצוות

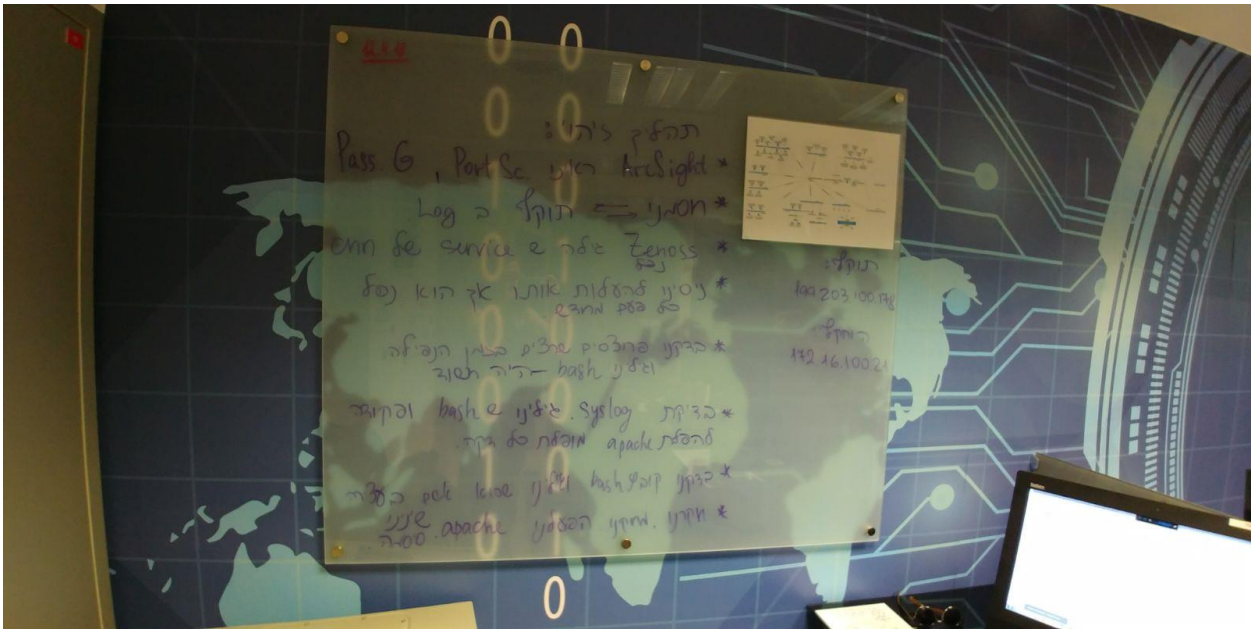
הייתה עמדת "מחוקק" שדאגה לחסום את התוקפים ב-Firewall לאחר שזיהינו אותם. באופן כללי היינו כל הזמן בביקורת על הכלים השונים ודאגנו לפקח ולאתר ארועים חשודים. לאחר שנטרלנו את התוקף וחסמנו

אותו, נרתמנו לאיתור הבעייה שגורמת לשרת ליפול ע"מ לטפל בנזק שנגרם. החיפוש לקח זמן רב יחסית ודרש גם קריאה ולמידה של דברים חדשים באינטרנט שלא ידענו את משמעותם קודם לכן. דאגנו לעדכן אחד את השני על כל פיסת מידע חדשה שהבנו ותיעדנו את מהלכי התרחיש על הלוח כדי שיהיה לנו נוח לעקוב אחרי מה שקורה.

חוסרים/קשיים

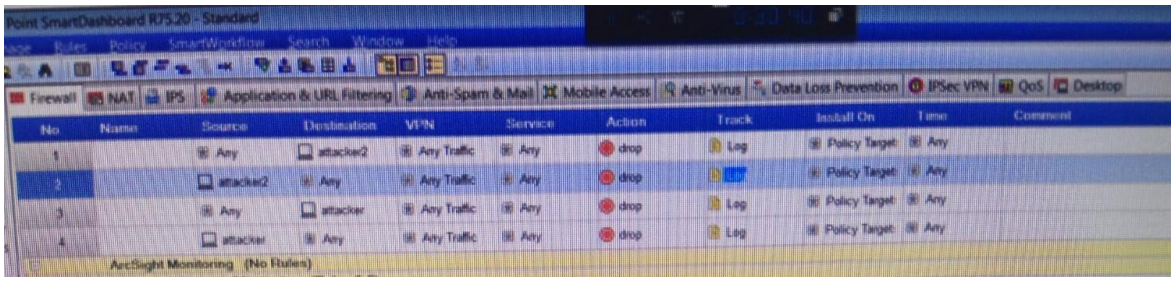
קושי בזיהוי מטרת הפורצים ומה בדיוק הם ניסו לעשות בתוך השרתים.
בנוסף אחרי שהשירות HTTP בשרת Apache1 נפל התקשנו להעלות אותו מחדש, אנו חשדנו שיש ווירוס שמפיל את השרת כל פעם מחדש וזה לא אירוע חד פעמי.
קושי נוסף היה שהפורץ עשה "רעש" וניסה לפרוץ גם לשרת Apache3.

תמונות למזכרת

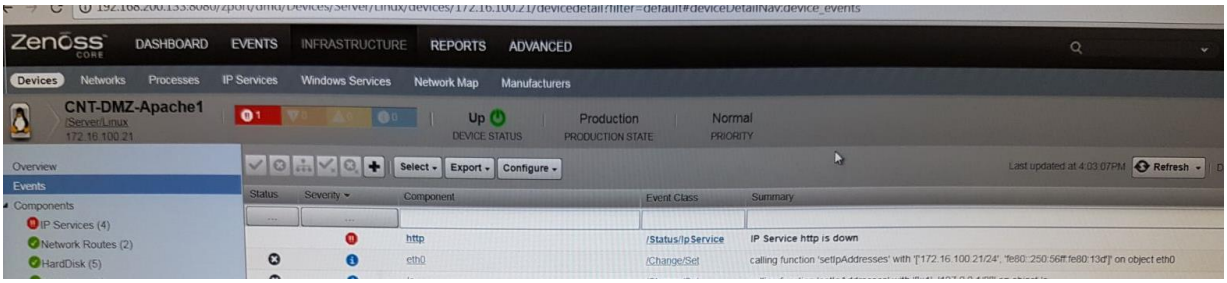


תיעוד על הלוח

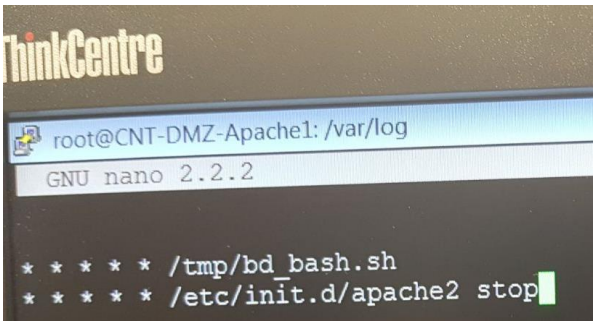
בס"ד



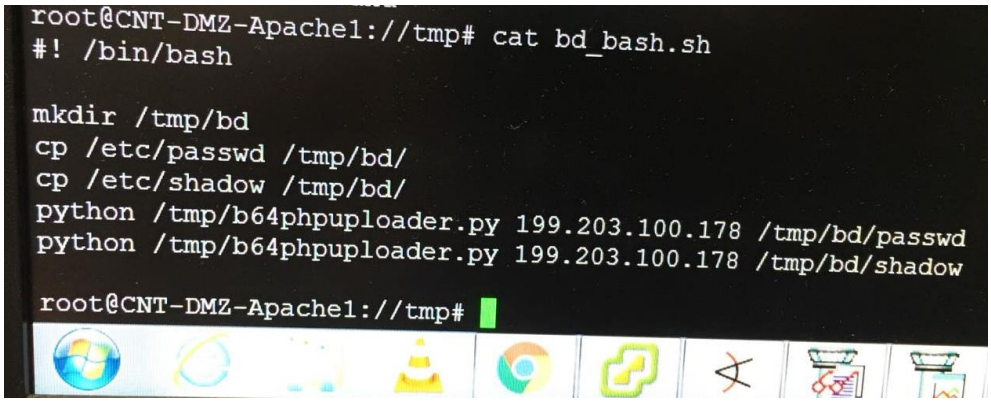
חסימת תקשורת עם הפורצים



נפל Apache1



הקובץ שרץ כל דקה. הפיל את השרת והעביר קבצים עם מידע רגיש לפורץ.



גנב קבצים עם מידע רגיש: passwd & shadow