דו״ח מעבדה- תרחיש מס׳ 1

פרטים :

מגיש : שגיא סעדה

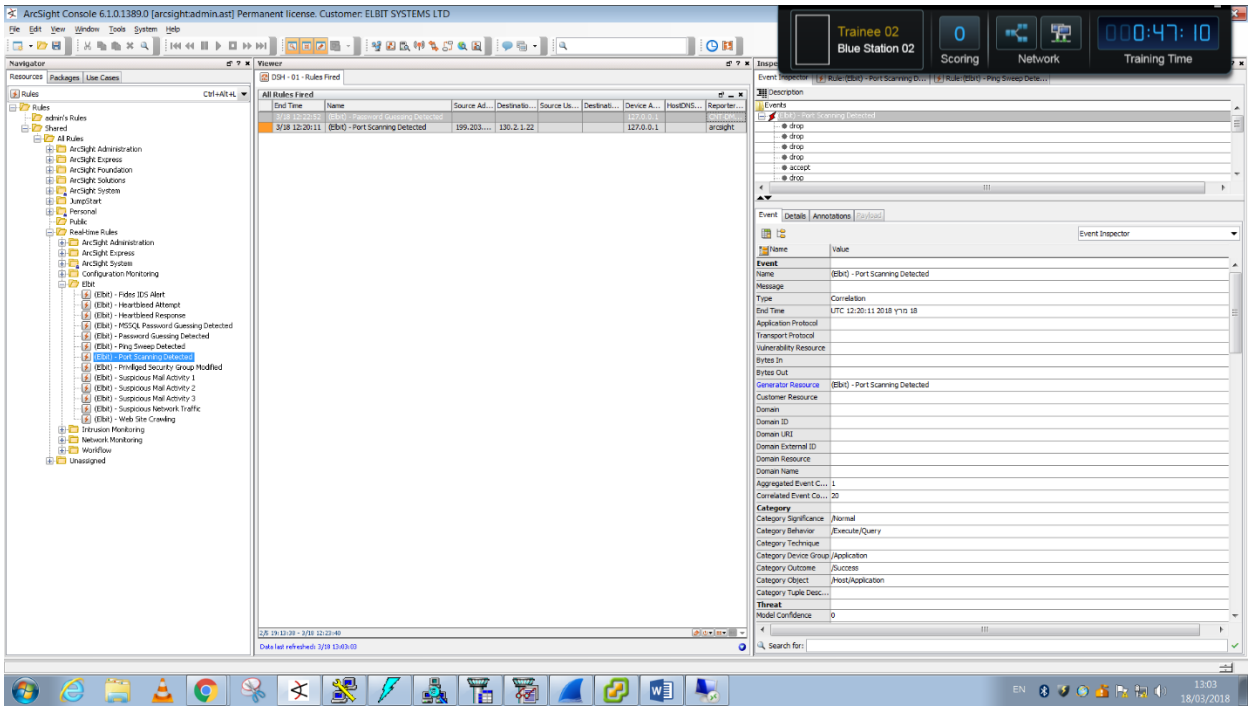
תאריך : 18/03/2018

שם התרחיש : תקיפת אתר הארגון.

תהליך ההתקפה :

התוקף סרק פורטים פתוחים בשרת הארגון – Port Scanning (אייפי של התוקף – 199.203.100.68) בשעה 12:20.

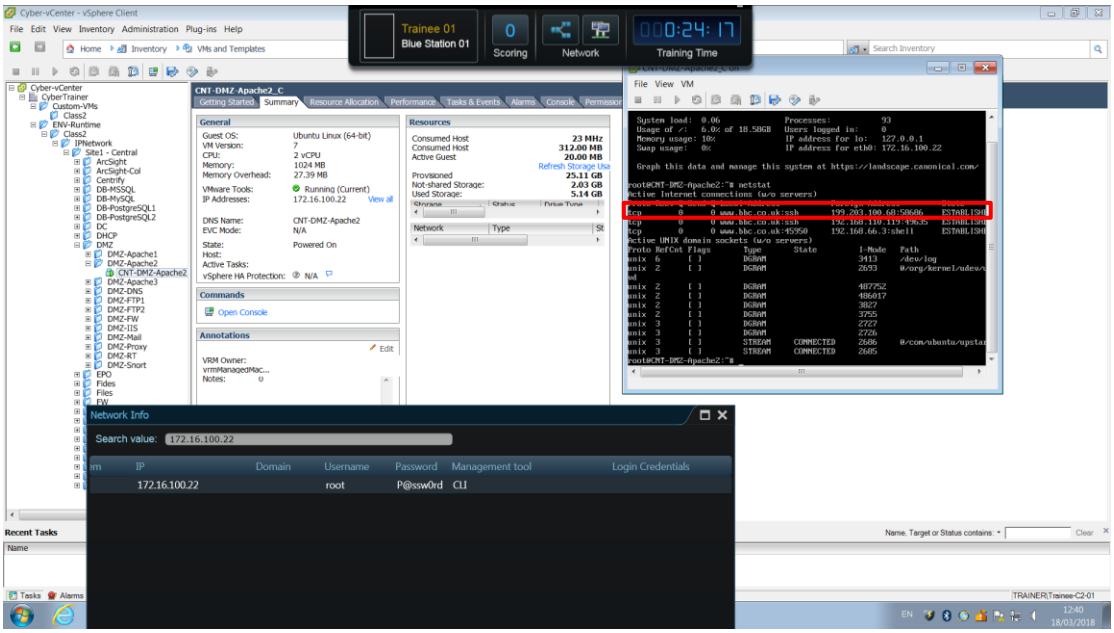
ולאחר מכן, ניסה להתחבר ל- ssh של שרת (עמדה) ה- apache2 של הארגון בשיטת – Password Cracking. (אייפי של השרת הנתקף – 172.36.100.22) בשעה 12:22. (בשלב זה איננו יודעים אם הצליח להתחבר).



תהליך הזיהוי:

בתהליך זה זיהינו את ניסיונות התוקף שצוינו קודם בכלי ARCHSIGHT ולאחר מכן התחברנו לשרת ה – apache2 של הארגון (השרת הנתקף) באמצעות Putty על מנת שנוכל לחקור את העמדה.

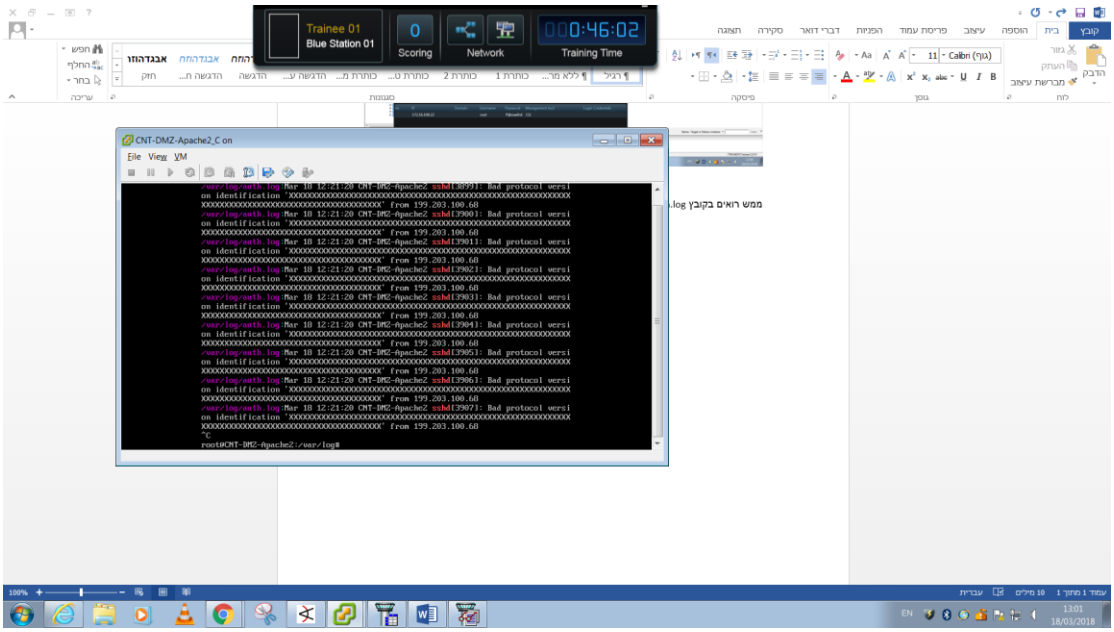
הרצנו netstat על העמדה וראינו שיש חיבור של ה- IP החשוד לשרת ביוזר פורט (שלו) : 58686.



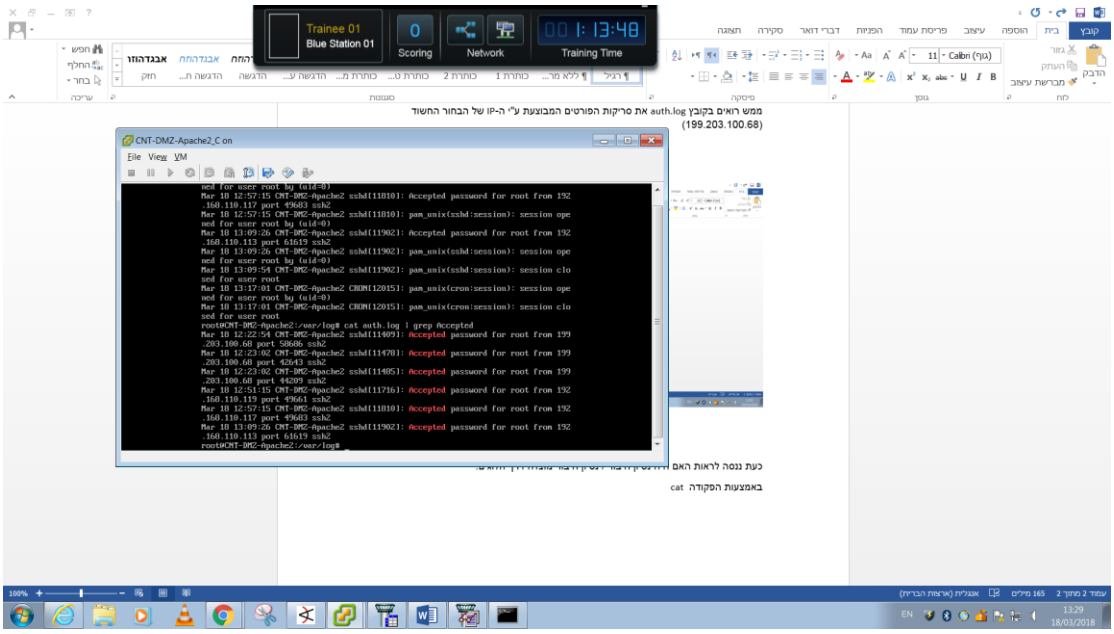
הסקנו שבאמצעות חיפוש בלוגים של המערכת נוכל לזהות את פעולות התוקף והוכחה וודאית להתחברותו וכך קרה –

הפעולה הראשונה הייתה – grep sshd /var/log/* כך ראינו את סריקות הפורטים "fuzzing".

נכנסו לתיקייה var/log ושם בקובץ auth.log ראינו את כל ניסיונות החיבור של התוקף באמצעות סיסמאות שונות ל- ssh של שרת זה.



לאחר מכן הרצנו את הפקודה cat auth.log | grep Accepted על מנת לבדוק האם היה ניסיון כניסה שצלח, ואכן מצאנו כניסה וודאית של התוקף.



מכיוון שראינו כניסה וודאית של התוקף, הסקנו שמכיוון ששרת זה הוא שרת apache2, זאת אומרת אחראי על האתר ככל הנראה לשם התוקף כיוון.

נכנסו לאתר הנתקף בכתובת 172.32.100.22 דרך הדפדפן ואכן ראינו שהתוקף שינה את קבצי האתר. (פעולה שהיינו צריכים לבדוק בהתחלה).

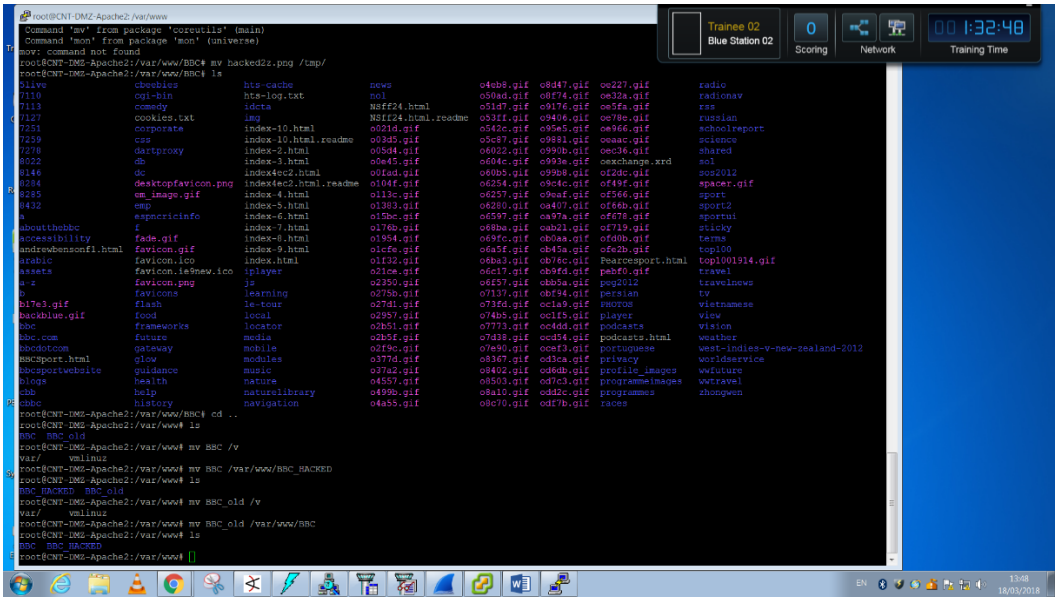
תהליך הגנה:

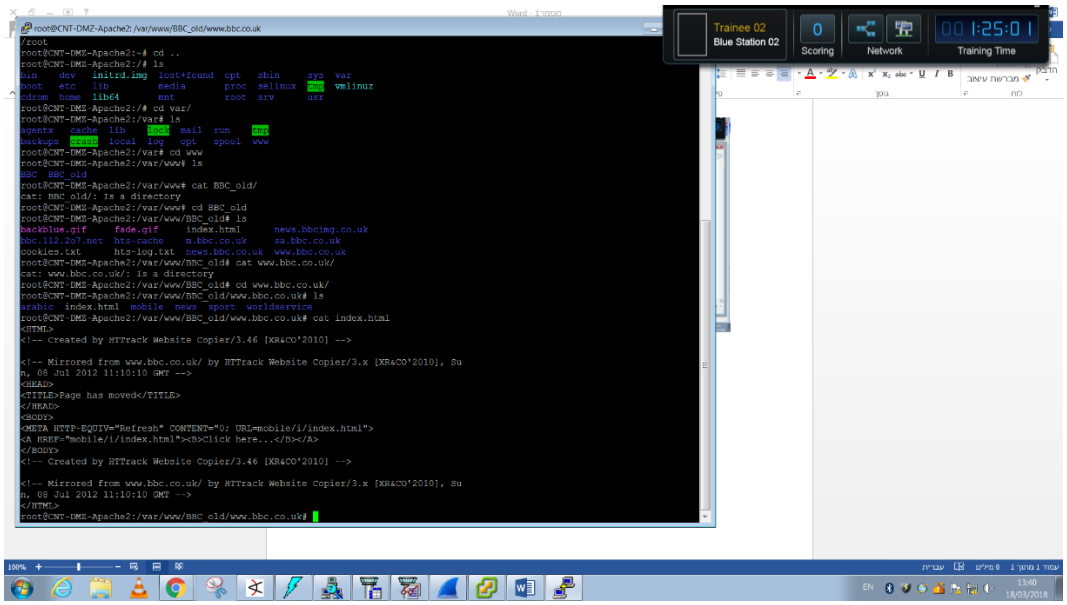
בתהליך זה קודם כל נרצה להבין בדיוק את משמעויות התקיפה:

1 – נבדוק אם התוקף עשה עוד דברים ברשת – לא נראה כך.

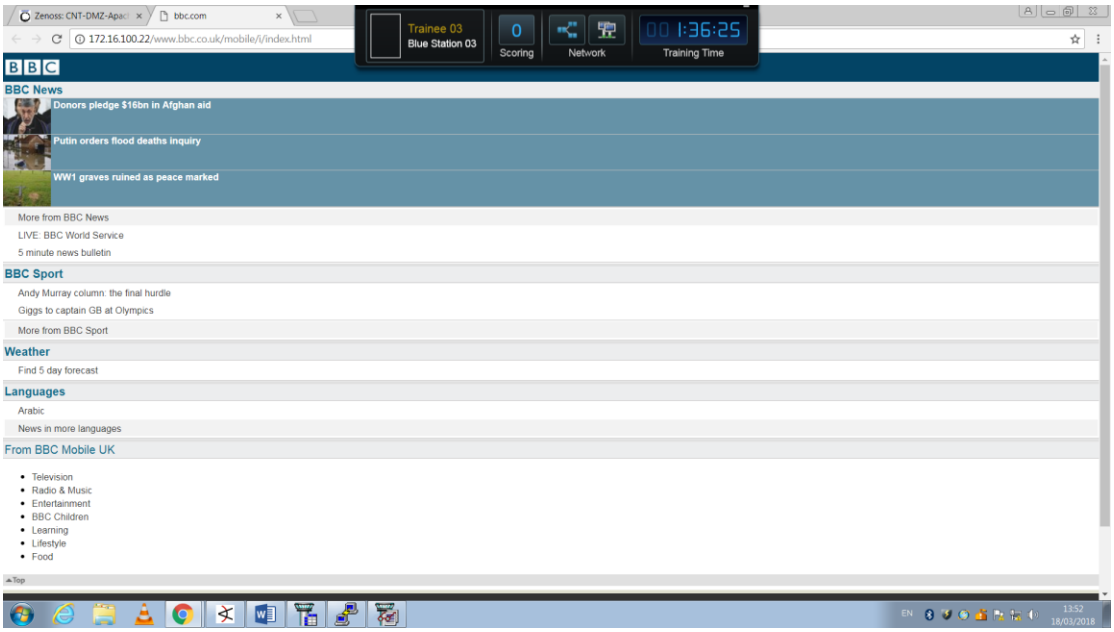
2 – נרצה לזהות היכן הקבצים שלה העמוד שהוא החליף יושבים, למחוק / לאסוף אותם לחקירה ובנוסף נרצה להחזיר את האתר המקורי לשרת.

ולכן, חיפשנו בעץ התיקיות של השרת וראינו בתיקיית www קובץ בשם BBC_OLD, מצאנו קובץ hacked2z.png, העברנו אותו תיקיה וראינו שאכן זהו הקובץ הזדוני שהופעל באתר – ככל הנראה יש עוד קבצים זדוניים בתיקייה ולכן נחזור לקבצים שיש בתיקייה BBC_OLD (ברגע שהעברנו אותו התמונה הזו לא עלתה כשגלשנו שוב אל האתר).





רצינו לחזור לנתיב המקורי של האתר ולכן שינינו את שם הקובץ BBC_OLD חזרה ל BBC וגלשנו שוב אל האתר – ואכן ראינו שהאתר עלה.



תהליך הגנה מונעת:

בתהליך זה לא בצענו פעולות אך ישנם כמה דברים שכדאי לעשות בהתאם לתקיפה –

1 – כתיבת חוק שברגע שמישהו מנסה לבצע סריקת פורטים יותר מ – X פעמים – ייחסם, כנ"ל לגבי ניסיונות באמצעות סיסמאות שונות.

2 – כדאי לחזק את הסיסמא, סיסמאות פשוטות כמו root פשוטות לפענוח.

3 – החלפת סיסמאות בארגון מדי X זמן. (שבועות/חודשים).

הפרצות באבטחת הארגון

בתהליך ההגנה עבור תרחיש זה ניתן לראות כמה פרצות אבטחה בארגון כגון:

1 – חוסר בחוק המונע סריקת פורטים ובנוסף חוק שמונע מספר ניסיונות התחברות ל- ssh באמצעות סיסמאות שונות.

2 – סיסמא פשוטה מדי – root.

3 – גישה פשוטה מדי לקבצי האתר.

כלים שפיתחנו

אין ברשותנו כרגע את הידע לפתח כלים.

אופן עבודת הצוות

מפני שזה תרחיש ראשון, בהתחלה לא כלכלך הבנו איך לחלק את העבודה בצורה יעילה.
באמצע התרחיש התחלנו לחלק עבודה בכך שכל אחד יעשה משהו אחר –

בדיקת קבצי הלוג, פיקוח על התחברויות נוספות לארגון, אפשרויות לדרכי חסימת התוקף וכו'.

חוסרים/קשיים

-