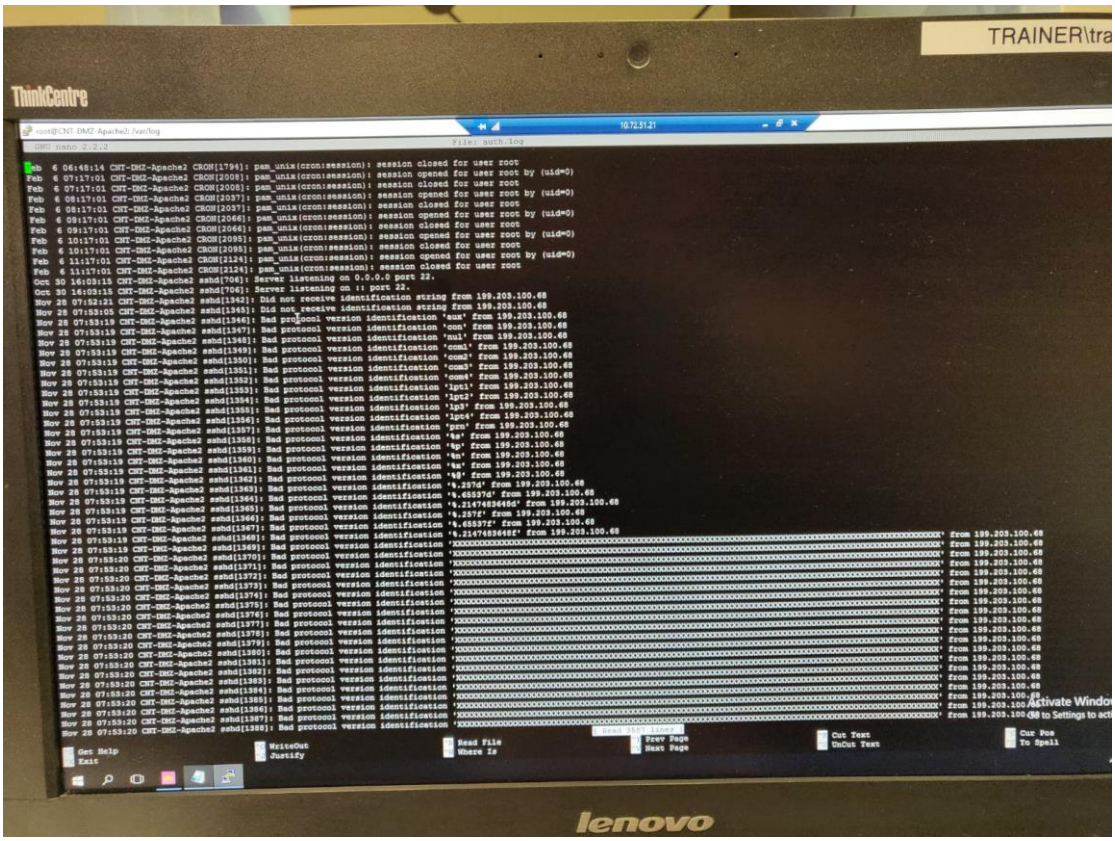
# דוח אירוע-2

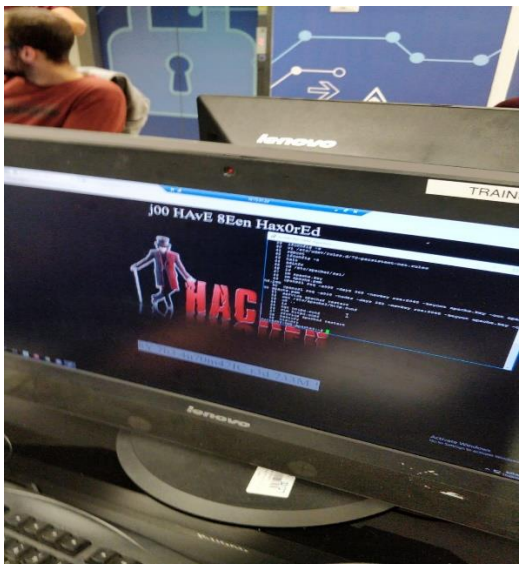
מגיש: דור לבקוביץ

שם התרחיש: פריצה לאתר bbc.

תהליך התקפה: בתאריך 28.11.2019 בשעה 10:20 בבוקר התקבלה התראה על ניסיון port scanning מסרבר apache2 מ- IP (199.203.100.68)



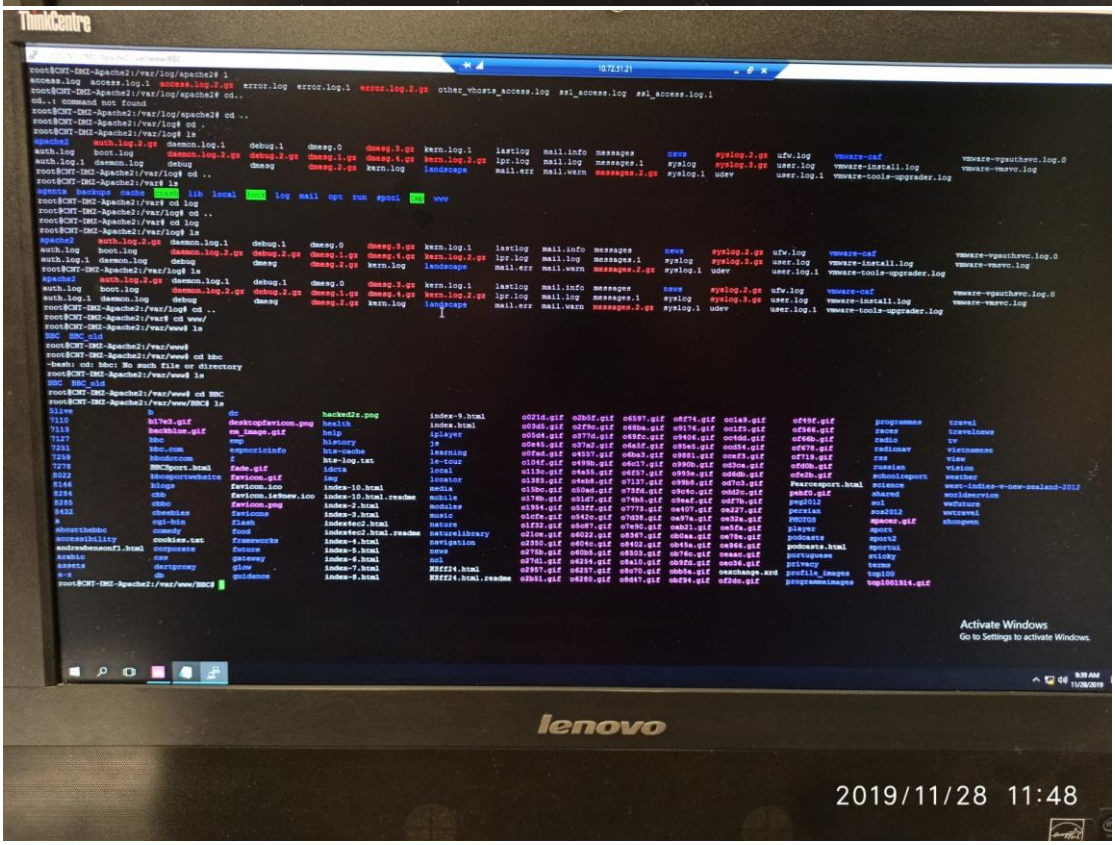

תהליך הזיהוי: לאחר בדיקה מעמיקה במערכת הarkSight הגענו למסקנה שהפורץ חדר לקבצים של האתר BBC ולאחר בדיקה נוכחנו לגלות שהוא נפל והושחט.



תהליך ההגנה ראשוני: בדיקת לוגים ובדיקת התחברויות ולאחר מכן ניגשנו תיקייה שם נמצאים כל הקבצים של האתר וראינו שהקבצים שונו.

```
7251                bbc.com          espnpricinfo     hts-cache        learning         c0fad.gif
7259                bbcdotcom        f                hts-log.txt      le-tour          c104f.gif
7278                BBCSport.html    fade.gif         idcta            local            c113c.gif
8022                bbcsportwebsite  favicon.gif      img              locator          c1383.gif
8146                blogs            favicon.ico      index-10.html    media            c15bc.gif
8284                cbb              favicon.ie9new.ico index-10.html.readme mobile    c176b.gif
8285                cbbc             favicon.png      index-2.html     modules          c1954.gif
8432                cbeebies         favicons         index-3.html     music            c1cfe.gif
a                   cgi-bin          flash            index4ec2.html   nature           c1f32.gif
aboutthebbc         comedy           food             index4ec2.html.readme naturelibrary c21ce.gif
accessibility       cookies.txt      frameworks       index-4.html     navigation       c2350.gif
andrewbensonf1.html corporate        future           index-5.html     news             c275b.gif
arabic              css              gateway          index-6.html     nol              c27d1.gif
assets              dartproxy        glow             index-7.html     N5ff24.html      c2957.gif
a-z                 db               guidance         index-8.html     N5ff24.html.readme c2b51.gif
root@CNT-DMZ-Apache2:/var/www/BBC# cat index.html
<html>
        <head>
                <title>YoU HaVe BeEn HaCeD !!!</title>
        </head>
        <body bgcolor="Black">
                <p style="text-align: center; ">
                        <font align="middle" color="#DDDDDD" size="10">j00 HAvE 8Een HaxOrEd</font></p>
                <p>
                         </p>
                <p>
                         </p>
                <p style="text-align: center; ">
                        <img alt="" src="hacked2z.png" style="width: 650px; height: 500px; " /></p>
                <p>
                         </p>
                <p>
                         </p>
                <p style="text-align: center; ">
                        <font align="middle" color="#DDDDDD" size="10">8Y 7h3 4u70m47IC r3d 733M !</font></p>
        </body>
</html>
root@CNT-DMZ-Apache2:/var/www/BBC#
```

2019/11/28 11:50




2019/11/28 11:48

תהליך הגנה מונעת: לאחר בדיקה נמצא שהפורץ חדש דרך פורט 22 (SSH) ואין סיבה שפורט זה יהיה פתוח כל הזמן ודבר שני זה להוריד את כמות הניחושים (הפורץ חדר ע"י ניחוש סיסמאות)

הסבר מפורט על אופן ההתקפה (התמקדות בחולשות): הפורץ עשה port scanning ומצא שיש גישה לפורט 22 (ssh) ומשם פשוט שלח פרטים שגויים על מנת לקבל את הגירסה הנכונה ואת הפרטים על מנת להמשיך את הפריצה ולאחר מכן השיג את השם משתמש וסיסמה ונכנס לקבצי האתר ושינה אותם.

כלים חדשים שפיתחתם/השתמשתם: ArcSight, zennos, putty.

אופן עבודת הצוות: שוב היה חוסר סינכרון בין אנשי הצוות שכל אחד לא ידע מה השני עשה וזה ממש האט את הדרך לפיתרון.

חוסרים/קשיים/בעיות: הפעם לקח לנו די הרבה זמן להבין ולהגיע לשורש הבעיה גם מחוסר ידע וגם מחוסר סינכרון בין אנשי הצוות.

**יש לשלב לוח זמנים, ותמונות בתהליכים שאתם מפרטים(כמובן, היכן שרלוונטי).**