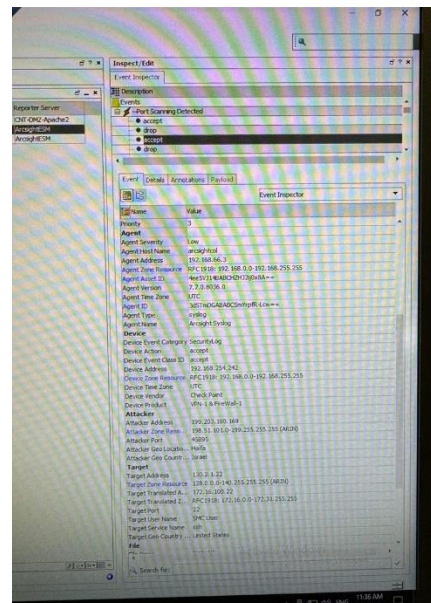
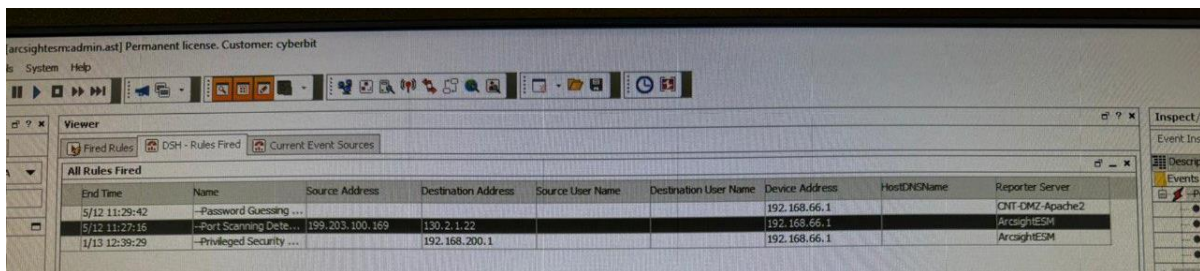


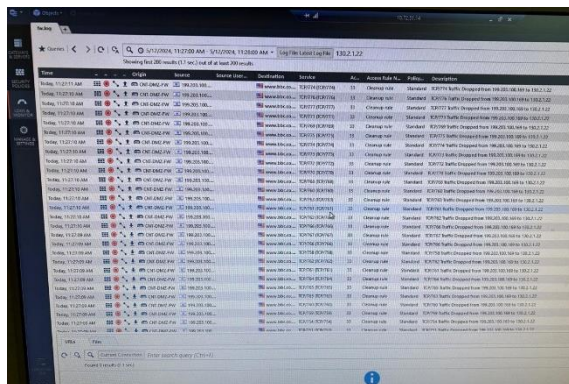
דו"ח תרחיש 1

1. לוגיסטיקה :
 - a. שם מלא : אליהו פרידמן
 - b. תעודת זהות : 211691159
 - c. שם התרחיש : Web Defacement
2. תהליך זיהוי התקיפה :

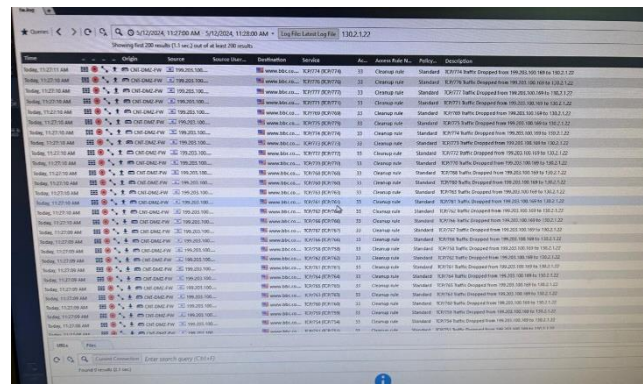
בשעה 11:27 ה ArcSight-התריע על סריקת פורטים של מכונה 130.2.1.22 . ממכונה 199.203.100.169 שלפי מפת הרשת נמצאת מחוץ לארגון.



בלשונית בצד ימין של הממשק, תחת הכותרת, אנו רואים פירוט יותר מורחב של ההתראה שזוהתה .
נוכל לראות אילו פורטים זהו כפתוחים – accept (הבקשה לפורט מסוים התקבלה – הפורט פתוח)
ומנגד אילו פורטים זהו כסגורים – drop (הבקשה לפורט מסוים נדחתה – הפורט סגור). כמובן שזוהי
רק דגימה שלפיה ה-ArcSight- זיהה התנהגות חשודה וכדי לראות את התמונה המלאה אנו יכולים
להתבונן ברשומות של חומת האש :



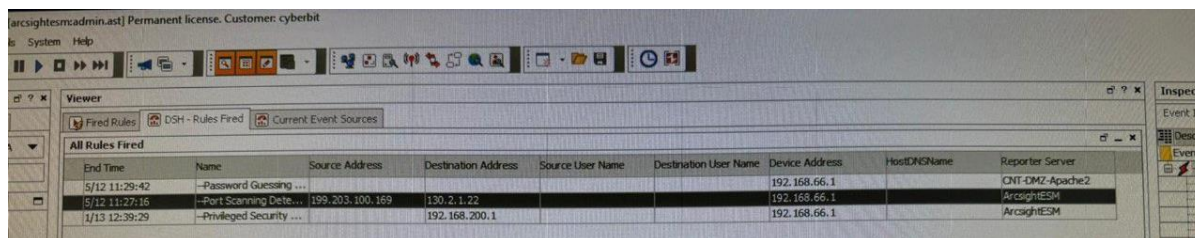
Time	Action	Source	Destination	Description
5/12/2024 11:27:00 AM	Standard	192.168.100.22	192.168.100.1	Standard: KSNIT Traffic Disposed from 192.168.100.22 to 192.168.100.1
5/12/2024 11:27:00 AM	Standard	192.168.100.22	192.168.100.1	Standard: KSNIT Traffic Disposed from 192.168.100.22 to 192.168.100.1
5/12/2024 11:27:00 AM	Standard	192.168.100.22	192.168.100.1	Standard: KSNIT Traffic Disposed from 192.168.100.22 to 192.168.100.1



Time	Action	Source	Destination	Description
5/12/2024 11:27:00 AM	Standard	192.168.100.22	192.168.100.1	Standard: KSNIT Traffic Disposed from 192.168.100.22 to 192.168.100.1
5/12/2024 11:27:00 AM	Standard	192.168.100.22	192.168.100.1	Standard: KSNIT Traffic Disposed from 192.168.100.22 to 192.168.100.1
5/12/2024 11:27:00 AM	Standard	192.168.100.22	192.168.100.1	Standard: KSNIT Traffic Disposed from 192.168.100.22 to 192.168.100.1

נוכל לראות שסריקת הפורטים הייתה רחבה בהרבה ממה שראינו בדגימה של ה- ArcSight רואים את תיאום הזמנים (11: 27) והסריקה שמתחילה מפורטים נמוכים עד פורט 790. המכונה שהתוקף סרק הינה: CNT-DMZ-Apache2

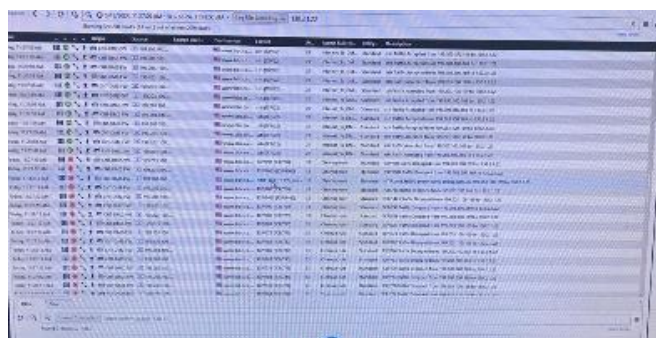
זמן קצר לאחר מכן (11: 29) אנו רואים התראה נוספת ב- ArcSight הפעם של ניחוש סיסמאות מאותו מקור, שקודם לכן ביצע את סריקת הפורטים על אותה המכונה שהיא: Apache-DMZ-CNT.2



End Time	Name	Source Address	Destination Address	Source User Name	Destination User Name	Device Address	HostName	Reporter Server
5/12 11:29:42	--Password Guessing ...	199.203.100.169	130.2.1.22			192.168.66.1		CNT-DMZ-Apache2
5/12 11:27:16	--Port Scanning Dete...	199.203.100.169	130.2.1.22			192.168.66.1		ArcsightESM
1/13 12:39:29	--Privileged Security ...		192.168.200.1			192.168.66.1		ArcsightESM



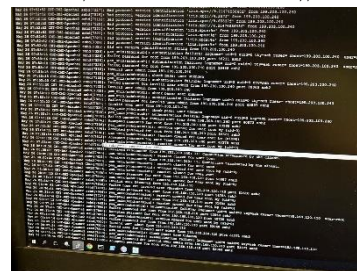
ניתן לראות שישנם חמישה ניסיונות כושלים של הכנסת הסיסמה בחלונות ה- Events מהמקור- 199.203.100.169 ליעד 172.16.100.22. ניסיונות כושלים אינם מספקים לנו אינדיקציה לשאלה האם בסוף התהליך התוקף הצליח להיכנס ועל כן נצטרך לבדוק את הנושא יותר לעומק.



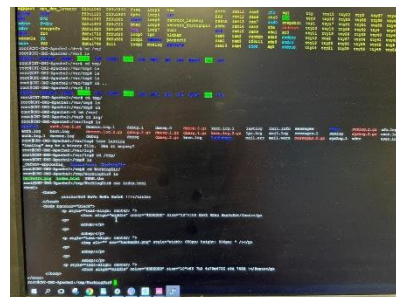
Time	Action	Source	Destination	Description
5/12/2024 11:27:00 AM	Standard	192.168.100.22	192.168.100.1	Standard: KSNIT Traffic Disposed from 192.168.100.22 to 192.168.100.1
5/12/2024 11:27:00 AM	Standard	192.168.100.22	192.168.100.1	Standard: KSNIT Traffic Disposed from 192.168.100.22 to 192.168.100.1
5/12/2024 11:27:00 AM	Standard	192.168.100.22	192.168.100.1	Standard: KSNIT Traffic Disposed from 192.168.100.22 to 192.168.100.1

אנו רואים שהתוקף עדיין מחובר (נמצא בסטטוס established) ונרצה להוציא אותו מהמערכת. נרצה לחקור מה התוקף עשה ואיד, על כן נתבונן ב- auth.log

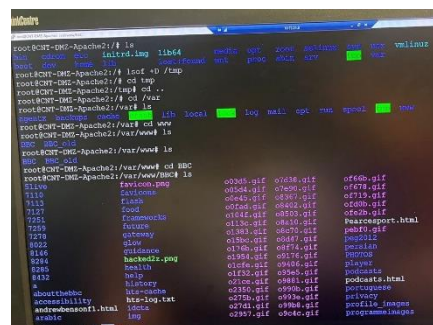
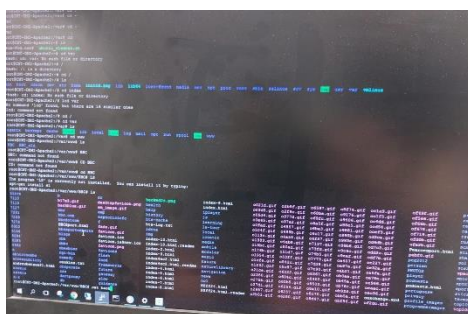
התוקף השתמש בפרוטוקול SFTP להעברת קבצים. הצילום מסך לא מראה את כל השימוש.



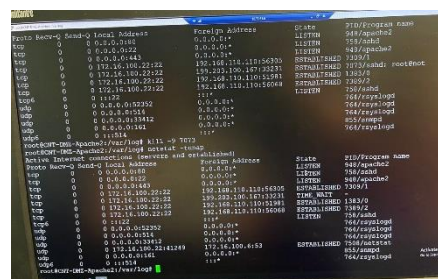
נשים לב שבתיקיית tmp בתוך workingdir נמצאים שני קבצים שהתוקף העביר לתוך הארגון



ניכנס לתיקייה שמחזיקה את BBC ונשים לב כי ישנם 2 תיקיות .
תיקיית 'BBC' שבה יש את הקבצים החדשים שהתוקף שתל, ותיקיית 'BBC_old' בה נמצאים הקבצים הישנים שהתוקף העביר .



בכדי להוציא את התוקף מהמערכת נשתמש בפקודת kill (הצילום מסך טיפה שונה כי לא מצאתי צילום מסך של הקבוצה שלי).



לאחר שהוצאנו את התוקף מהארגון נעביר את הקבצים שהושגו לבדיקה ובחינה, ובו זמנית נשיב את הדף לעבוד. נעשה זאת על ידי העברת הקבצים חזרה לתיקייה והעברת הקבצים הנגועים משם.

3. פירוק ווקטור התקיפה לשלבים לפי [MITRE](https://mitre.org) :

כאן נבצע פירוק של ווקטור התקיפה לתבנית MITRE ATT&CK.

: [Reconnaissance](https://mitre.org)

התוקף ביצע סריקת פורטים פתוחים על הכתובת 130.2.1.22. התוקף מגלה שפורט
80,443,21,5322 פתוחים

: [Resource Development](#)

התוקף העלה למכונה שני קבצים זדונים. אחד hacked2z.png שזוהי התמונה ואת
html.index שמריץ את התמונה של התוקף באתר BBC.

: [Initial Access](#)

התוקף מנסה להתחבר ב SSH- לשרת ה- Apache 2 שנמצא ב-DMZ (בכתובת
172.16.100.22). לאחר מספר ניסיונות כושלים, הוא מצליח לקבל גישה למכונה ומתחבר
כמשתמש root.

: [Execution](#)

התוקף מעביר בפרוטוקול SFTP קובץ לתוך תיקיית WorkingDir/tmp במכונת
Apache2. קבצים בשם png.z2hacked ו-html.index. שמטרתם היא לשנות את תוכן
האתר BBC, ב-html.index ישנו פקודה שמריצה את התמונה png.z2hacked.

: [Persistence](#)

אין

: [Privilege Escalation](#)

אין. הוא מראש התחבר למשתמש בעל הרשאות גבוהות.

: [Defense Evasion](#)

אין-האתר נתקף ושונתה תמונה, וכן לא נמחקו הלוגים

: [Credential Access](#)

אין. לא התבצעה גניבת סיסמאות.

: [Discovery](#)

אין. התוקף לא ניסה לקבל מידע על הסביבה שבה הוא נמצא

: [Lateral Movement](#)

אין. התוקף לא זז בין מכונות או בין רשתות בארגון.

: [Collection](#)

אין

: [Command and Control](#)

אין. התוקף כבר מחובר ב SSH-אין לו שרת שו"ב

: [Exfiltration](#)

אין

: [Impact](#)

האתר BBC נפרץ ועולה עם התמונה ששתל התוקף. בנוסף, יש לתוקף גישה מלאה למכונה
ועליה הרשאות מנהל מערכת (root –), יכול להיות שבעתיד לתוקף תהיה גישה למכונות
נוספות בארגון.

לא היה צד תקשורתי משמעותי בהתקפה, התקשורת היוותה רק כאמצעי ולא הייתה זו שהובילה את הנזק הישיר, התקיפה בפועל אינה מבוססת ומושגת על תקשורת. הפרוטוקולים שהתוקף השתמש בהם היו SSH עבור החיבור למכונות SFTP, עבור העלאת הקבצים לשינוי תוכן האתר של BBC והעלאת התמונה במקום.

5. פעולות לוקאליות :

- a. המשתמש שדרכו נכנס התוקף :
התוקף נכנס למשתמש root במכונה Apache-DMZ2. ראינו ב-ArcSight שהתוקף ניסה להתחבר 5 פעמים ואז הפסיק לנסות - לאחר חקירה נוספת, הבנו שהניסיונות הכושלים הובילו להצלחה בהתחברות. (אין לנו דרך מפורשת לדעת כיצד הוא גילה את הסיסמה, ניתן להניח שזו הייתה התקפה על פריצת הסיסמה, שהצליחה בהסתברות גבוהה).
קבצים שנפגעו/שונו/הועתקו/הושטלו :
- b. בתיקית var/www/bbc התוקף העביר את תיקיית BBC לתקיית OLD_BBC ובתיקיית BBC השתיל 2 קבצים זדוניים : index.html ו-hacked2z.png ובכך שינה את דף הבית של אתר BBC
מסקנות נוספות :
- c. הגישה של התוקף למכונה הזו מסוכנת מאוד, גם בהפלת האתר (הלקוחות לא יכולים לגשת = הארגון מאבד כסף) וגם בעתיד הארגון כי יכול להיות שבעתיד הוא ינצל את הגישה הזו כ-Backdoor ויוכל לתקוף את הארגון מבפנים ולהשתלט על מכונות נוספות. חוץ מאיבוד הכסף עלולה להיות פגיעה תדמיתית במותג וכן פחד של אנשים להיכנס לאתר בעתיד מחשש שהאתר עדיין נגוע.

6. הגנה :

- a. הגנה ראשונית :
ראשית אמצעי ההגנה שנקוט הוא לנתק את התוקף. לחסום כל תקשורת עם הכתובת של התוקף בחומת האש. לשנות את הסיסמה שהתוקף גילה והצליח לפרוץ. להחזיר את האתר של השרת לפעילות בהקדם
הגנה מניעתית :
- b. בכדי לסק[ק הגנה מניעתית, יש להשתמש בסיסמאות חזקות יותר, להוסיף מנגנוני MFA (למשל, קוד לאישור ההתחברות בטלפון). לבחון אפשרות חסימת חיבורים מרחוק מחוץ לארגון או "להחביא" את הפורטים עבור הפרוטוקולים האלו. למשל ניתן לסגור לצמיתות את פורט 22 עבור SSH ולעדכן את כלל העובדים שמעתה החיבור ב-SSH יהיה בפורט 34534 שימוש ב-p-forwarding.

7. הערות נוספות :

- a. אופן עבודת הצוות :
אני חושב שיחסית לסטודנטים שבתחילת דרכם היה בסדר. אם כי ניכרים חוסר ההבנה בנושא. יש לציין לטובה את ראש הצוות שלמרות שזוהי מבין המעבדות הראשונות עשה את עבודתו בצורה מקצועית
מגבלות העבודה :
- b. היה קושי בהבנה, אך המדריכים עזרו לנו מאוד.