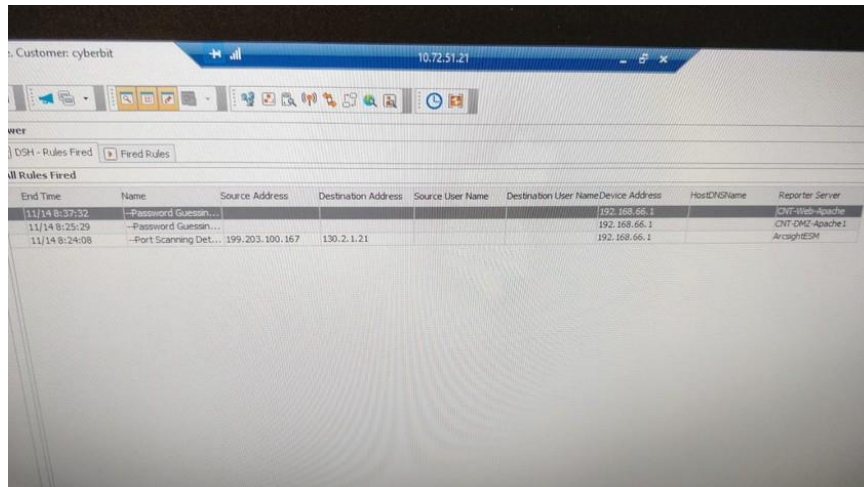


דף עזר סייבר

סדר פעולות תחילת תרחיש:

1. ניכנס ל ArcSight כדי לקבל מידע ראשוני על התקיפה.



The screenshot shows the ArcSight interface with a table titled "Fired Rules". The table has columns for End Time, Name, Source Address, Destination Address, Source User Name, Destination User Name, Device Address, Host/Engine Name, and Reporter Server. The data rows show three events: two password guessing attempts and one port scanning detection.

End Time	Name	Source Address	Destination Address	Source User Name	Destination User Name	Device Address	Host/Engine Name	Reporter Server
11/14 8:37:32	~Password Guessin...					192.168.66.1	CNT-Web-Apache	
11/14 8:25:29	~Password Guessin...					192.168.66.1	CNT-DMZ-Apache1	
11/14 8:24:08	~Port Scanning Det...	199.203.100.167	130.2.1.21			192.168.66.1		ArcsightEDM

עמודות חשובות –

Name – מהו סוג התקיפה?

Source Address – בדרך כלל תהיה הכתובת של התוקף (בעיקר אם היא מהאינטרנט [לא מופיעה במפת הרשת הארגונית])

Destination Address – בדרך כלל תהיה הכתובת של המחשב הנתקף.

2. בהתאם לסוג התקיפה - נבדוק ב ZENOSS אם נפלו שירותים או תהליכים בארגון.

3. נבצע התחברות מרוחקת למחשב הנתקף (דרך PuTTY אם הוא לינוקס, או דרך V-Sphere אם הוא ווינדוס).

4. נבדוק את קבצי הלוג החשובים:

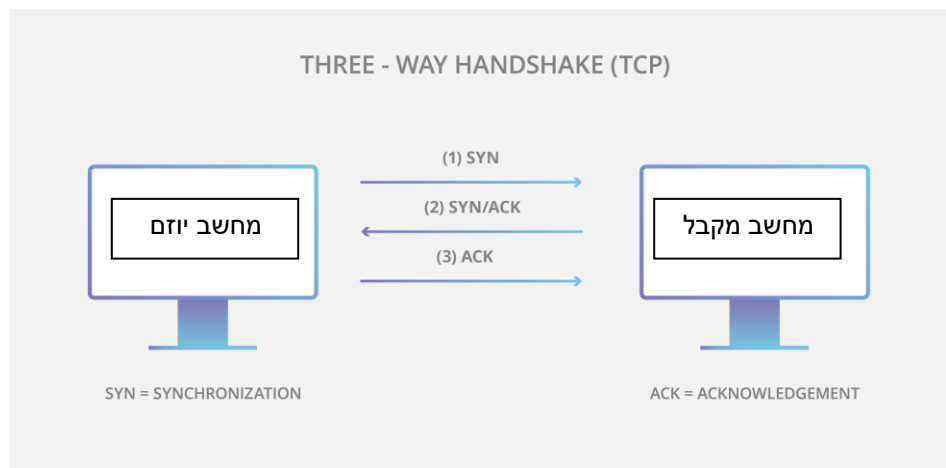
- `/var/log/auth.log` - כל ניסיונות ההתחברות המוצלחים / כושלים את המחשב.
- `/var/log/syslog` - מידע כללי על פעולות ידניות / אוטומטיות שבוצעו במערכת, במידה ונתקלים במילה CRON (מתזמן המשימות), מומלץ לבדוק אם הושטל בו סקריפט על ידי התוקף (במידה ורלוונטי לתרחיש).
- `/var/log/mail.log` - מידע על כל המיילים שנכנסו ויצאו מהמחשב.
- במידה ומדובר בתרחיש מיילים, לחפש בתיקיית `home/[user]` בשרת המיילים אם ישנם מיילים חשודים.

אחרי שקיבלנו מידע על סוג התקיפה, נמשיך לחקור בכיוון המתאים כדי לקבל כמה שיותר מידע על:

- א. מי התוקף?
- ב. איך הוא נכנס?
- ג. מה הוא עשה?
- ד. איך היה אפשר למנוע את ההתקפה? (הכל כתוב בתרחישים)

כמה דברים חשובים:

- CRON – מתזמן המשימות של לינוקס (אפשר להשתיל בו סקריפטים שירוצו אוטומטית כל זמן מוגדר).
- TCP – פרוטוקול תקשורת שנחשב אמין, תהליך ההתחברות מתבצע כך:



לאחר תהליך ההתחברות נפתחת "תעלת" תקשורת בה נשלח מידע בצורה מבוקרת בין שני המחשבים, כאשר כל הפאקטות ממוספרות כדי להבטיח את הגעתן באופן מסודר.

בנוסף, המחשב המקבל ידווח למחשב השולח שקיבל את כל המידע בשלמותו. אם המידע לא הגיע בצורה תקינה – המחשב השולח ישלח שוב את הפאקטות החסרות בצורה אוטומטית. (דוגמא לשימוש – שליחת קובץ)

- UDP – פרוטוקול תקשורת השולח את הנתונים בצורה קבועה, לא מתחשב באם הפאקטות הגיעו בשלמותן, וממשיך לשלוח את שאר המידע – לכן נחשב פחות אמין אך יותר מהיר מפרוטוקול TCP (דוגמה לשימוש – שיחת וידאו).

- על מנת להגיע לקבצים של אתר כלשהו, נכנסים לתיקיית: `/var/www`

כלים:

- Arc Sight – מוניטור של המערכת, מזהה תקשורת חשודה ומתריע.
- Smart Console – ה Firewall של המערכת. ניתן להגדיר חוקים לסינון פאקטות, חסימת פורטים וכו'.
- בין היתר ניתן לראות את התעבורה במחשב. אפשר לסנן לפי כתובת IP ולהגדיר IP – Destination IP ו- Source IP.
- Syntax example: `dst:192.168.100.13 / src:219.32.6.14`
- PuTTY – כלי לחיבור ושליטה מרחוק על מחשב מסוג לינוקס. (CLI)
- V-Sphere – כלי לחיבור ושליטה מרחוק על מחשב מסוג ווינדוס / לינוקס. (GUI)
- Zenoss – כלי לניטור שירותים בשרת. מציג סטטוס עדכני של השרתים והשירותים הרצים בהם (HTTP, apache2 וכו') בעיקר התראות.

- Snort – כלי לניתוח תעבורה הנכנסת לרשת עוד לפני שהגיעה אל ה-Firewall.

ניתן להתחבר אל שרת ה Snort דרך PuTTY ולהריץ את הפקודה `sudo tcpdump` כדי לראות את כל הפאקטות הנכנסות ויוצאות מהרשת הארגונית.

- לבדוק קבצים ששוננו לאחרונה:

- לינוקס: `ls -l` הצגת תוכן תיקייה בצורה של רשימה, אפשר לראות את תאריך השינוי האחרון.

- ווינדוס: ללכת על שדה החיפוש בתוך התיקיה, ולסנן לפי

Date Modified