# סיכום מאמן סייבר

## דברים שבודקים שנכנסים לשרת:

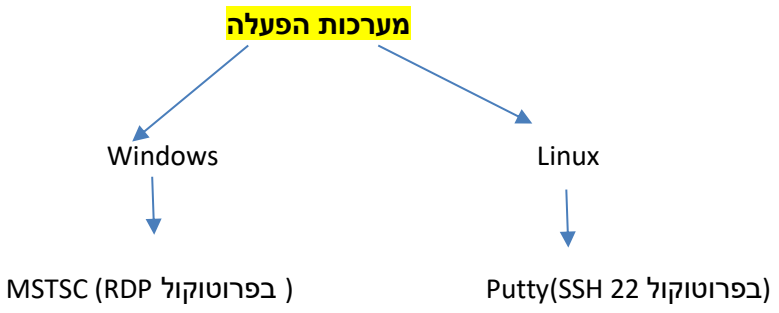
- איך נכנסים לשרת?

1. בודקים איזה מערכת הפעלה( ככה נדע לאן להתחבר)
2. מה הכתובת שאליה אנחנו מנסים להתחבר (הכוונה לאיזה מחשב נרצה להתחבר)

## דרך פעולה :

נכנסים ל- Vsphere ושמה ניתן לראות את כל השרתים הקיימים ברשת שלנו.

ניתן להניח תמיד כי שרת iis הוא באופן טבעי שרת של ווינדוס.




| דברים שנבדוק | LINUX | WIN |
|---|---|---|
| 1. LOGS (לוגים) | א) נכנס לתיקייה VAR : באמצעות הפקודה cd /var<br><br>ב) אז נכנס ל- cd log ואם נרצה לבדוק איזה קבצים נמצאים בתוך תיקיית log נרשום את הפקודה ls והוא יציג את הלוגים הקיימים בתיקייה.<br><br>• logs שנבדוק בדרך כלל הם:<br>1.system logs - syslog<br>בנוסף ע"י שימוש בפקודה grep ניתן לבצע סינון בלינוקס. | Event Viewer<br>נכנס לתיקייה windows Logs מתוך ה Event Viewer:<br>1.Application<br>2.Security<br>3.System<br><br>נשתמש ב- Filter שנמצא בשורת חיפוש (נשתמש ב 12 השעות האחרונות) |
| 2. Last Modify | כדי לרשום קבצים בספרייה ולמיין אותם תאריך ושעה שהשתנו לאחרונה ניתן לעשות זאת באמצעות הפקודה :<br>`$ ls -lt`<br>אם רוצים לעשות מיון הפוך ניתן לעשות זאת באמצעות הוספה r-: | נכנס תחילה למחשב זה(E+WINKEY), לאחר מכן בשורת החיפוש נלחץ Date modify ונסמן את היום של התקיפה. לאחר סריקה ניתן לעבור על התיקיות והקבצים ולראות איפה יש משהו חשוד |

**קרדיט: אוראל מרדכי**

| | | |
|---|---|---|
| | $ ls -ltr | |
| Network .3 | שימוש בפקודה netstat<br>Netstat -bna | שימוש בפקודה netstat<br>Netstat -bna |
| 4 . בודקים שהכל תקין | בלינוקס ניתן לבדוק Services process באמצעות שימוש הפקודה: Services - -status - all<br>כל מצב מפרט את מצב השירותים שבשליטת מערכת V.<br>+ מציין שהשירות פועל,<br>- מציין שירות שנעצר .<br>? לא ניתן לקבוע את מצב השירות (מסיבה כלשהי). | דוגמה נבדוק את המנהל משימות, Process Manager.<br><br>ניתן להוריד גם Process Explorer(אך יכול להיות שזה יתקע גם אותו).<br><br>לבדוק את ה Zenoss שאין SERVICES שנפלו. |

- **איך מרימים Service שנפל?**

1. בווינדוס ניתן לגשת דרך הComputer Management ואז לגשת ל Services Application ואז ל Services ואז ללכת לאותו שירות שנפל . ניתן גם דרך ה CMD בשימוש בפקודה:
Net stop/run ושם ה Service
2. בלינוקס באמצעות הפקודות:

```
/etc/init.d/apache2 stop

/etc/init.d/apache2 start
```

- **מה אנחנו צריכים לחפש בלוגים?**

**בווינדוס :**

logs task scheduler (ניתן דרך התיקייה גם לראות C:\Windows\Tasks\SchedLgu.txt זה נראה בווינדוס), Task category.
נרצה לבדוק דברים חריגים שמתרחשים בזמן התקיפה.
נעשה זאת באמצעות הפילטר שיעזור לנו להתמקד בחיפוש הדברים הללו.

**בלינוקס :**

הסבר קצר קודם : Cron הוא כלי קלאסי שנמצא במערכות Linux ו UNIX -להפעלת משימות בזמנים או במרווחים קבועים מראש .משימות אלה נקראות משימות Cron או עבודות Cron . Cron משתמש לתזמן עדכונים אוטומטיים, דור הדו"ח, או לבדוק עבור שטח דיסק זמין בכל יום ולשלוח לך דוא"ל אם הוא נופל מתחת לסכום מסוים.
עבודות Cron System קיימות כרשומות **בקובץ /etc/crontab .**

כדי להציג רשומות crontab של המשתמש הנוכחי להשתמש בפקודה הבאה:

**crontab -l**

- שיטה להעיף כל 20%(שמסמל רווח ב WEB ) שמופיע בקובץ:
נלחץ Ctrl+F ובלשונית REPLACE אני ארשום ב find what 20% ולחיצה על REPLACE ALL .

- איך רואים פינג בשרת?

<u>נפתח CMD נקליד את הפקודה הבאה:</u>

**Ping -t (ip Address number or dns like "google.com")**

**<u>התו "-t":</u>** כדי להציג את מצב הטעינה הנוכחי של TCP , במקום מצב TCP המוצג בדרך כלל.

## <u>פקודות לינוקס בסיסיות</u>

### <u>פקודות LS:</u>

1) הפעלת הפקודה ls מבלי לצרף ארגומנט נוסף יציג את רשימת הספריות הנוכחית של אותה תיקייה בה אנו נמצאים.

2) לרשימת התוכן של ספריה כלשהי, מבלי להיכנס ישירות לתיקייה , נרשום את הפקודה : "name of the folder"/ ls.

3) ספרייה תמיד מכילה כמה קבצים מוסתרים (לפחות שניים) , ולכן, כדי להציג את כל הקבצים בספרייה, ניתן להשתמש ב a- או flag- , רישום הפקודה נעשית כך: ls -a or ls -flag.

4) ניתן גם להדפיס מידע מפורט על כל קובץ בפלט ,ls כגון הרשאות קבצים, מספר קישורים, שם הבעלים ובעל הקבוצה, גודל הקובץ, זמן השינוי האחרון ואת הקובץ / שם ספריה. כל זה ניתן לעשות באמצעות הפקודה: ls -1 (ראינו בטבלה).

### <u>פקודות Netstat:</u>

1) Netstat הוא כלי בשימוש נרחב לשאילתה מידע על תת הרשתות של לינוקס .ניתן להשתמש בה כדי להדפיס את כל היציאות הפתוחות כך: "Sudo netstat -1tup".

### <u>הסבר על כל תו:</u>

- "-1" אומר לnetstat להדפיס את כל שקעי ההאזנה.
- "-t" מציג את כלי חיבורי ה-TCP .
- "-u" מציג את כלי חיבורי ה-UDP .
- "-p" מאפשר הדפסה של שם יישום או תוכנית האזנה ביציאה.

2) כדי להדפיס ערכים מספריים במקום שמות שירות, הוסף את הדגל n- :

"sudo nestat -1ntup".

3) ניתן גם להשתמש בפקודה **grep** כדי לברר איזה יישום מקשיב ביציאה מסוימת, למשל : "netstat -1ntup | grep "name of app. ניתן לחלופין, לציין את היציאה ולמצוא את היישום בדרך הבאה :"netstat -1ntup | grep ":port number" .

4) שימושים נוספים ב- netstat הם ע"י הפקודות **bna-** וגם **noa-** . נפרט כל תו מה אומר:

- **"a-":** בורר זה מציג חיבורי TCP פעילים, חיבורי TCP עם מצב ההאזנה, כמו גם יציאות UDP שהוקלטו.
- **"b-":** תו Netstat זה דומה מאוד לתו O- המפורט למטה, אך במקום להציג את ה - PID(Process id), יציג את שם הקובץ בפועל של התהליך .שימוש ב o- over -אולי נראה כאילו זה חוסך לך צעד או שניים, אבל באמצעות זה יכול לפעמים מאוד להאריך את הזמן שנדרש netstat לבצע באופן מלא.
- **"n-":** כדי למנוע מ netstat - לנסות לקבוע שמות מארח עבור כתובות IP זרות . בהתאם חיבורי הרשת הנוכחיים שלך, באמצעות בורר זה יכול להפחית באופן משמעותי את הזמן הדרוש כדי ש- netstat יוכל לבצע באופן מלא.
- **"o-":** אפשרות שימושית עבור משימות רבות לפתרון בעיות, מתג O- מציג את מזהה התהליך (PID) המשויך לכל חיבור מוצג .

**פרוטוקולים +פורטים + מושגים בסיסיים:**

- **Proto** - שם הפרוטוקול המשמש את החיבור בשכבת התעבורה
- **Local Address** - כתובת ה-IP של המחשב המקומי והפורט שבו משתמש החיבור (אם הפורט עדיין לא נקבע יופיע הסימן "*")
- **Foreign Address** - כתובת המחשב המרוחק
- **State** - מצב ההתקשרות:
  - **ESTABLISHED** - התקשרות פעילה
  - **TIME_WAIT** - מצב שמתחיל מיד לאחר סיום ההתקשרות ומאפשר למחשב המקומי לפרש חבילות מידע נכנסות כשאריות, שעדיין מסתובבות ברשת, מהתקשרות שהסתיימה.
  - **LISTEN** - מצב שבו תוכנית ממתינה לחבילות מידע נכנסות (לעיתים יכול להעיד על סוס טרויאני שממתין לקבלת פקודות)

- **פרוטוקול תקשורת** - אוסף חוקים שיוצרים צורת תקשורת מוסכמת כגון - TCP/IP.
- **TCP/IP** - פרוטוקול / חבילת TCP/IP היא פרוטוקול התקשורת הדומיננטי כיום, ומהווה את הבסיס עליו מושתתת רשת האינטרנט.
- **כתובת IP** (ראשי תיבות של Protocol Address Internet) - כתובת ייחודית הניתנת לכל רכיב (מחשב) ברשת מחשבים, המבוססת על פרוטוקול ה- IP.
- **רשת מקומית** (LAN - Local Area Network) - רשת מחשבים המתפרסת על אזור גיאוגרפי מוגבל (עד אלפי מטרים רבועים).
- **רשת אזורית** (Network WAN - Wide Area) - רשת מחשבים המחברת בין רשתות מקומיות על פני מרחב גיאוגרפי בלתי מוגבל.
- **FTP** - פרוטוקול להעברת קבצים בין שרת ללקוחותיו.

**קרדיט: אוראל מרדכי**

- **HTTP** (ראשי תיבות של Protocol Hyper Text Transter) - פרוטוקול להעברת דפי HTML וקבצים נלווים. משמש להעברת דפי אינטרנט בגלישה דרך הדפדפן. מרבית דפי האינטרנט פנויים מפרוטוקול זה.
- **SMTP** (ראשי תיבות של Protocol Simple Mail Transfer) - פרוטוקול לשליחה  והעברה של דואר אלקטרוני (שרת דואר יוצא).
- **POP3 -** פרוטוקול לשליפה של דואר אלקטרוני משרתי דואר אלקטרוני (דואר נכנס).
- **DHCP** (ראשי תיבות של Host Configuration Protocol Dynamic) - פרוטוקול להקצאה דינמית של כתובות IP. שרת DHCD הנו שרת המקצה כתובות IP למשתמשים המתחברים לחברת האינטרנט
- **firewall (חומת אש) -** תוכנה למניעת חדירה לא מורשית אל המחשב, וקישור לא מורשה אל האינטרנט על ידי תוכנות במחשב, או אנשים במחשבים אחרים.
- **דפדפן -** תוכנה לפתיחת דפי HTML, כגון: Internet Explorer. משמשת לניווט בין אתרי האינטרנט השונים.

- **firewall (חומת אש)** - תוכנה למניעת חדירה לא מורשית אל המחשב, וקישור לא מורשה אל האינטרנט על ידי תוכנות במחשב, או אנשים במחשבים אחרים.

- **שרת Proxy** - שרת היושב בדרך כלל בחברות האינטרנט ומושך אליו דפי האינטרנט המבוקשים בעולם. השימוש בשרת זה מתבצע על מנת לאפשר גישה מהירה לאתרים מרוחקים, להאיץ את מהירות הגלישה ולשמור על רוחב הפס הבינלאומי.
- **וירוס המחשב** - תוכנה שחודרת למחשב באופן ופוגעת בפעולה התקינה של המחשב הנפגע.
- **תולעת מחשב** - תוכנה שחודרת למחשב באופן סמוי, מפיצה את עצמה באמצעות תוכנות מסרים מידיים או באמצעות הדואר האלקטרוני, ופוגעת בפעולה התקינה של המחשב הנפגע.
- **אנטי וירוס** - תוכנה לזיהוי ואיתור וירוסים, מחיקתם ותיקון קבצים נגועים בהם.
- **תוכנת ריגול** - תוכנה שעוקבת בחשאי אחר הרגלי גלישה של המשתמש במחשב, בו היא מותקנת,  ומעבירה מידע על הרגלים אלה, או על שימוש בתוכנה שמותקנת על המחשב באופן בלתי חוקי לאתרים ששתלו אותה. התוכנה אינה מאפשרת למשתמש למחוק אותה.

| יציאות ברירת מחדל | פרוטוקול | הגדרת פרוטוקול |
|---|---|---|
| n/a | TCP\UDP | מספק חיבורים למחשבים על רשת TCP/IP. |
| 25 | SMTP | שולח דואר אלקטרוני על רשת TCP/IP |
| 53 | DNS | מתרגם URL לכתובת IP |
| 80 | HTTP | מעביר דפי אינטרנט על רשת TCP/IP |
| 67,68 | DHCP | הופך את הקצאת כתובות IP ברשת לאוטומטיות |
| 443 | HTTPS | מעביר עמודי אינטרנט בבטחה על רשת TCP/IP |
| 20,21 | FTP | מעביר קבצים על רשת TCP/IP |
| 161\162 | SNMP | ניהול ובקרת התקנים על רשת |
| 110\993 | POP\IMAP | הורדת דואר אלקטרוני משרת דואר אלקטרוני |
| 389 | IDAP | גישה לספריות מידע |
| 3389 | RDP | גישה מרחוק למחשבים (MSTSC) |
| 22 | SFTP | העברת קבצים מאובטחת |
| 445 | SMB | מספק גישה משותפת לקבצים ומדפסות |
| 137 | NETBIOS | אינו מספק גישה לאינטרנט ברשת קבוצת עבודה |

# פקודות בסיסיות משורת ההפעלה RUN

## Windows commands

| | |
|---|---|
| Terminal Server Connection (Remote Desktop Protocol) שולחן עבודה מרוחק | **MSTSC** |
| ייבוא או ייצוא הגדרות הרישום כניסה לעורך הרישום **(Registry)** | **REGEDIT** |
| Terminal Server Connection (Remote Desktop Protocol) שולחן עבודה מרוחק | **MSTSC** |
| Command Prompt | **CMD** |

# פקודות שימושיות ב- DOS:

| | |
|---|---|
| מחיקת התוכן המוצג במסך | **CLS** |
| הצגת רשימת הקבצים והספריות בדיסק | **DIR** |
| מחיקת קבצים מהדיסק . - /P יאפשר מחיקת כל התיקייה | **DEL** |
| הפנייה לספרייה הרצויה. כניסה לתיקייה. | **CD "שם התייקיה"** |
| למחוק את התיקייה | **RD** |
| חזרה לתיקיית השורש | **CD ** |
| כדי לצאת מתיקייה ולהגיע לרמה אחת מעל | **CD..** |

# פקודות רשת(Network):

| | |
|---|---|
| **ping** | פקודה זו תשמש אותנו כדי לבדוק קשר בין המחשב שעליו אנו עובדים לנקודת יעד כלשהי. |
| **ipconfig** | מאפשרת לקבל מידע אודות הגדרות Tcp/ip של העמדה, המידע מציג כתובת IP ו mask subnet Default Gateway. ניתן להוסיף את המתג all ולקבל מידע על שרת DNS. |
| **netstat** | מאפשרת לקבל מידע סטטי על תעבורת הרשת. המתגים הנפוצים netstat -e מספקים מידע על התעבורה ברשת המקומית ethernet s- netstat הפקודה מאפשרת גם מעקב אחר פורטים פתוחים (חשוב מאוד) באמצעות המתגים-n- a- |
| **nslookup** | משמשת לצורך בדיקת שרתי DNS, לוודא ששרת ה-DNS שלנו פועל כראוי |
| **tracert** | פקודה זו מאפשרת לנו למצוא את הנתיב בו יעברו נתונים מהמחשב שלנו אל יעד כלשהו |
| **ipconfig /release** | משחררת את כתובת האי פי הנוכחית שלך |
| **ipconfig /renew** | נותנת לך כתובת חדשה |
| **Ipconfig /all** | אם נרצה לראות גם את ה- Subnet Mask, DNS, MAC address. (ה- MAC נקרא שם כ- " Physical" Address). Subnet Mask יכלול רק 255 או 0. |

# מבנה של צוות SOC

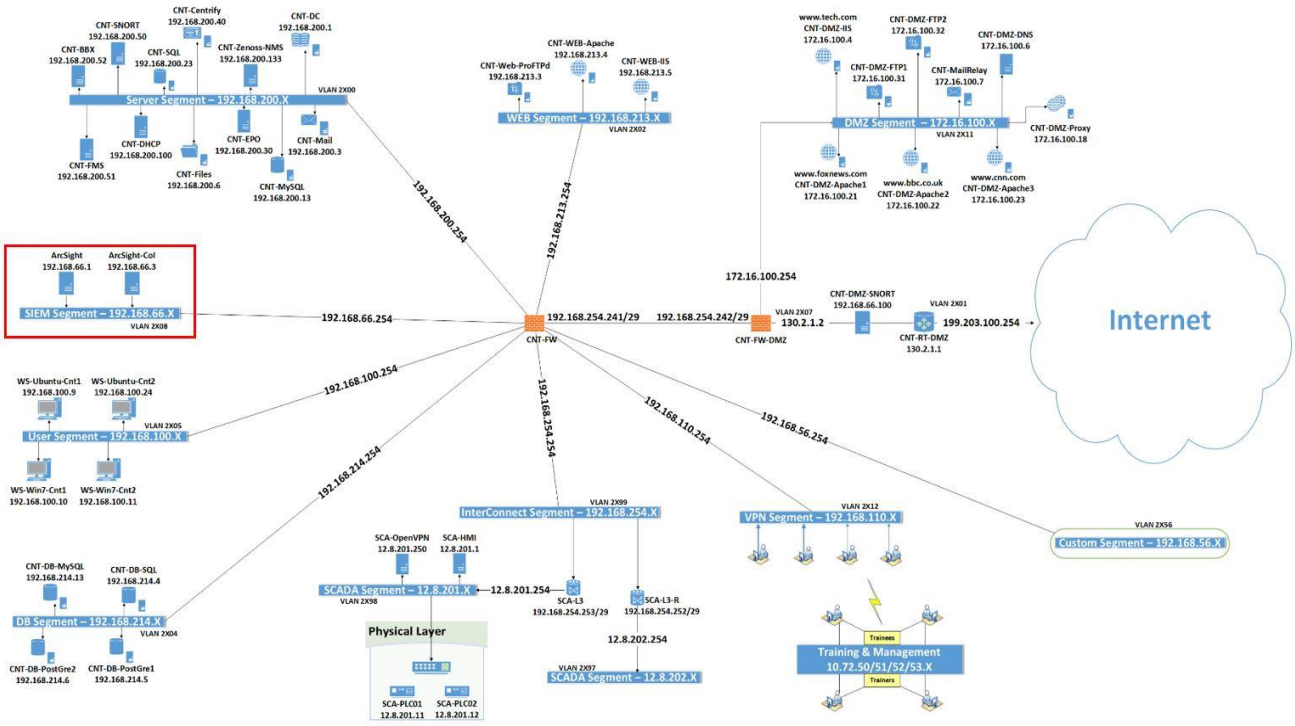
- זיהוי
- סיווג
- מניעה

**הסבר המושג DMZ (De millitrzes zone)**:

שטח מפורז , שטח שאסור שיהיה בו צבא. מבחינתו בעולם האמיתי יש באינטרנט אזור מסויים שאנו מרשים לאנשים להיכנס אליו.

**שרתי אפצ'י:** שרתי לינוקס.

**הסבר המושג Segment:** סגמנט זו קבוצה של טווח כתובות ip (שיושבת בטווח כתובות שמוגדר על ידי מנהל הרשת) ברשת הארגונית שלנו. כלומר כל קבוצה של שרתים תשב בסגמנט (מקטע) מסוים (יכול להיות גם מדפסות, שרתים, מחשבים). להלן מפת הרשת של הארגון אשר ניתן לראות כי כל קבוצה של שרתים יושבת בסגמנט מסוים:




ניתן לראות בריבוע האדום כי שרתי ה **Arcsight** יושבים תחת סגמנט (מקטע/קבוצה) הנקרא SIEM בטווח הכתובות של 192.168.66.X וכל שרת במקטע מקבל X אחר לפי טווח הכתובות.

## כלים עיקריים

**1. Arcsight**

**2. Zennos**

**3. CheckPoint Firewall**

**4. Vsphere Client ובשאר הכלים במצגת.**

## תחילת עבודה

**סיסמא לווינדוס: Aa123456**

**נתחבר תחילה לשרת ה- VPN של הארגון ולאחר מכן נפתח את הכלים הבאים.**

1) נתחבר ל- VPN CONNECTION (נמצא בגישה לאינטרנט בשורת ההתחלה).

2) לאחר מכן ,נבצע התחברות לכלי ArcSight :
   a. **משתמש**: admin
   b. **סיסמא**: P@ssw0rd

**הסבר קצר על הכלי ArcSight :** הכלי נמצא תחת סגמנט כלי "סים". הכלי אוסף לוגים מכל השרתים, וכל הזמן השרת של ה- ArcSight מקבל לוגים ,בין עם הם תקינים או אינם תקינים, ובכך הכלי מזהה כניסות חשודות שנעשות לשרתים. הכלי יודע לנתח לוגים מכמות גדולה של שרתים ובהתאם לחוקים שהוגדרו **מתריע על חריגות(הוא אינו חוסם)**.

3) **כלי Zenoss-** יודע לאתר SERVICES שנפלו בשרתים.

**כניסה למערכת:**

**כתובת** : 192.168.200.133:8080

**שם משתמש**: admin , **סיסמא**: P@ssw0rd

4) **Vmware-** מאפשר גישה לראות ולהתחבר לכל השרתים של הארגון.

IP=10.72.53.1

כלי VMWARE- תוכנה לניהול שרתים.

בהתחלה נלחץ על VMs and Templates, כאן נוכל לראות את כל השרתים של הארגון.

ניתן להתחבר גם מרחוק על השרתים ב-2 דרכים:

1) ווינדוס- באמצעות פרוטוקול RDP דרך כלי MCTSC .
2) לינוקס- באמצעות פרוטוקול SSH (22) דרך כלי putty.
מתקשרים ביניהם דרך winscp.

5) **CheckPoint Firewall-** חומת אש , נועדה לתת לנו אבטחה מתקדמת בפני איומי סייבר. המערכת עוזרת בניטור וחסימת התקשרויות בלתי רצויות לרשת התקשורת או מחשב יחיד.

הדרכה לחוקק חוקים: כאשר אנו יודעים את כתובת התוקף נרצה לבצע חסימה של התוקף על מנת שלא תהיה לו גישה נוספת לשרתים שלנו. נעשה זאת באמצעות חקיקת חוק של דרכי הכניסה והיציאה של התוקף.

**נחוקק חוק לפי סדר הפעולות הבא:**

א) נלחץ על לשונית window, ונכנס לאפשרות הראשונה smartdashboard.
ב) נפתח את כל הפלוסים על מנת לראות את כל החוקים שקיימים.
ג) בשורה של Network & Security Monitoring נלחץ על קליק ימני בעכבר ואז נפנה לאופציה הראשונה Add Rule-> above.
ד) לאחר מכן יפתח חלון ונבחר באפשרות ..New והאופציה הראשונה Host.
ה) בחלון ה HOST נרשום בשם את שם התוקף או משהו בעל משמעות עבור אותו ip שנחסום. ב- ip address נרשום את כתובת התוקף.
ו) עכשיו נפנה ל install Policies שנמצא תחת לשונית search,יפתח לנו חלון ונסמן את 2 הריבועים cnt-fw ו- cnt-fw-dmz ונלחץ OK. בשלב זה יתבצע התקנה לחקיקה שיצרנו.
ז) כעת ניתן לראות כי נוצר שורה חדשה תחת שורת ה- Network & Security Monitoring.
ח) חשוב מאוד לבדוק שהגדרנו בחסימה גם את ה destination של התוקף וגם את ה source. כלומר דרכי הכניסה והיציאה של התוקף.

## כללים חשובים שנרשום ונשאל את עצמנו

**כלל 1:** נרשום תמיד זמנים , קריטי להצלחה של מציאת הבעיה.

**כלל 2:** נבדוק דרכי תקשורת.

**כלל 3:** נרשום כל דבר שנראה לנו חשוד.

**שאלות שנשאל את עצמנו:**

- מאיפה זה מגיע?
- איך לעצור את זה?
- מה זה עושה?

# מושגים שלמדנו במהלך הקורס

**PORT SCANING:** בעצם יש מישהו שהולך ובודק פורטים אחד אחד ומחכה לראות מי יחזיר תגובה (לראות תקשורת).

**Secure Shell** בראשי תיבות **(SSH)** : הוא פרוטוקול לתקשורת מחשבים המאפשר ביצוע פעולות על מחשב מרוחק לאחר תהליך הזדהות(login) . הוא נועד להחליף את RSH, rlogin ו־ telnet ולאפשר תקשורת מאובטחת ומוצפנת בין שני מחשבים לא תלויים ברשתות לא מאובטחות. SSH פועל מעל TCP, והפורט הסטנדרטי שלו הוא 22.

SSH נועד לתעבורה ממחשב אחד למחשב אחר בצורה מאובטחת דרך תוכנות SSH. בעזרת פונקציה זו ניתן לאבטח תעבורה של תוכנה שאינה תומכת באבטחה, או שאבטחתה חלשה יחסית.

**Ping Sweep:** מטרתו למפות את הרשת, ולקבל את טווח כתובות של כל הרשת. הוא טכניקה בסיסית לסריקת רשת המשמשת לקביעת איזה טווח של כתובות IP למארחים חיים (מחשבים).

**Website Crawling**: גורם שאוסף נתונים באמצעות הורדת קבצים, יש תוכנות בלינוקס שעושות זאת באופן אוטומטי לדוגמה: WGET , HTTPCRACK ועוברות לינק לינק ומעתיקות אתרים. בעצם זה זחלן רשת שעובד דרך מנועי החיפוש השונים ואוסף מידע דרך crawling (תולעת/זחלן).

**קרדיט: אוראל מרדכי**