מעבדת סייבר – הגנה

מטלה ראשונה – חלק שני  
מגישים : עוז מעתוק -   
דניאל אלפסי - 308399542

**פעולות בסיסיות -**

1. מצא תקשורת ליעד מסויים שחוזרת או ממשיכה לפעול באופן שוטף במערכת.

כדי למצוא תנועה חוזרת או חשודה למעשה ישנם כמה דרכים.  
אופציה אחת היא לפתוח מתוך הרשת המותקפת / המחשב שנחשד כמותקף את התוכנה Wireshark ולמצוא תנועה חשודה. כלומר כתובות IP חשודות / פרוטוקולים שחוזרים על עצמם או לא אמורים כלל להופיע. בנוסף תנועה נוספת נוכל לראות באמצעות ה CheckPoint Tracker שנתן לנו מבט על ה Rule-ים והתנועה היוצאת והנכנסת שכן/לא אושרה.  
תנועה חשודה זאת ניתן יהיה גם לנטר ב ArcSight.  
  
**הערה** – רמזים למציאת המחשב בו היינו צריכים להתמקד קיבלנו מה Zenoss תחילה כאשר שמנו לב איזה שירותים נפלו.

2. חסום אותה.

בכדי לחסום התקשרות מול יעד מסויים, אנו נשתמש בכתובת ה IP שלו ובעזרתה נייצר Rule חדש בחומת האש של CheckPoint, דרך ה Dashboard, אשר תחסום את כלל הכניסות מהכתובת הנ"ל.

חשוב לשים לב מאיזה מהFirewallים אנו מבצעים את ה Rule מכיוון שיש אחד בתוך הארגון ואחד מחוץ לארגון ה "קוו הגנה הראשוני" במעבר אל העולם החיצוני (אולי נרצה רק באחד מהם להוציא לפועל Rule חדש או שבשניהם) .

3. פענח כמה נחסמו או מתי.

כמו בסעיף הקודם, ניתן דרך תוכנת ה Dashboard השולטת על ה CheckPoint Firewall לצפות בפרטי חומת האש כאשר כלולים בה גם הכתובות החסומות למעבר/לכניסה.  
בפועל ב Live יהיה אפשר לראות דרך ה Tracker תנועה שעוברת או נחסמת ולבצע סינון מתקדם לפי תאריכים ושעות.

**הכרות של השרתים.**

1. למי מחובר מחשב ה- Apache .  
(ענינו על השאלה כאשר אינינו זמינים למעבדה).  
באופן כללי ניתן להתחבר אל שרת ה Apache באמצעות PuTTY שמממש חיבור SSH או בכלי אחר המאפשר חיבור למערכת ההפעלה Ubuntu (נגיד ב VM ware).  
כאשר ניהיה מחוברים ניתן לצפות בLogים של הפעילות בשרת.  
מעבר לקח ממבנה הרשת באופן טבעי ניתן להסיק ששרת ה Apache מחובר למחשבים ב-Subnet שלו ישירות ול Database המתאים לו.

2. מי מחובר אליו ב- SSH.

בכדי לראות מי מחובר לשרת, ראשית אנו כמובן נתחבר אליו ב SSH, לאחר מכן נריץ את הפקודה netstat -tnpa | grep ESTABLISHED.\*sshd אשר תציג לנו את החיבורים לשרת בפרוטוקול הנתון עם מס' פרטים נוספים כמו כתובות.

אם נריץ את הפקודה ps auxwww | grep sshd, נוכל לקבל פרטים גם על פרטי המשתמשים אשר ביצעו את ההתחברות כמו שם המשתמש, באיזה שעה ההתחברות התבצעה וכו'.

3.פענח את הלוג.  
 - (ה Log במעבדה יפוענח ותתקבל חוות דעת מקצועים ☺ בסיכום האירוע).

4. חפש את הטקסט bad protocol.

הודעת ה bad protocol מופיעה בעקבות ניסיונות התחברות אשר אינן תואמות את פרוטוקול העבודה. לדוגמא לקוח שמנסה להתחבר לשרת FTP ע"י פרוטוקול אחר כמו SSH, לא יצליח לבצע את הכניסה וההודעה הנ"ל תופיעה בלוג.

הודעה זו מופיעה לרוב עקב ניסיונות חדירה של גורמים מזיקים (האקרים ווירוסים) אשר מנסים בצורה רחבה לפרוץ לשרת / מחשב כלשהוא. נוסיף ונאמר כי לאחר קריאה בגוגל, הודעה זו נפוצה להתקבל בניסיונות התחברות בפרוטוקול SSH בעקבות תכונותיו.