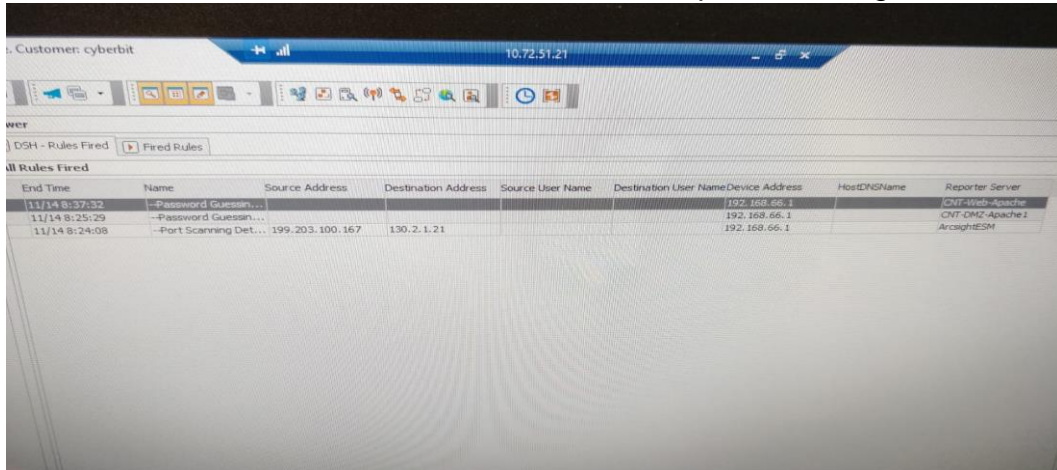


דוח אירוע-מס' תרחיש

מגיש: דור לבקוביץ

שם התרחיש: port scanning



The screenshot shows a security monitoring 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/DNS Name, and Reporter Server. The data rows show events related to password guessing and port scanning.

End Time	Name	Source Address	Destination Address	Source User Name	Destination User Name	Device Address	Host/DNS Name	Reporter Server
11/14 8:27:32	--Password Guessing...					192.168.66.1	CNT-DMZ-Apache1	ArcoSightESM
11/14 8:25:29	--Password Guessing...					192.168.66.1	CNT-DMZ-Apache1	ArcoSightESM
11/14 8:24:08	--Port Scanning Det...	199.203.100.167	190.2.1.21			192.168.66.1		

תהליך התקפה: ב – 14 לנובמבר התקבל דיווח על סריקת פורטים (PORT SCANNING) ולאחר דקה כמה ניסיונות ניחוש של סיסמאות מסרבר APACHE1 מ-IP חיצוני (199.203.100.167) לאחר מספר ניסיונות התוקף הצליח לחדור בעזרת PRUTE.FORCE.

תהליך הזיהוי: ההתראה הראשונית הגיעה דרך תוכנת ArkSight בשעה 8:24 בבוקר. לאחר מספר דקות נפל השירות (APECHE2) שנראה בעזרת תוכנת ZENNOS. בגלל ה – PORT SCANNING ובגלל ההפרש הקטן בינו לבין הניחוש סיסמה הגענו למסקנה שפרצו לנו למערכת.

תהליך ההגנה ראשוני: נכנסתי אל var/log של הסרבר על מנת לבדוק אם יש נזק כלשהו.

```
root@CNT-DMZ-Apache1:/var/log# ls
apache2      auth.log.3.gz  daemon.log.1  debug         debug.4.gz    dmesg.2.
auth.log     auth.log.4.gz  daemon.log.2.gz  debug.1       dmesg         dmesg.3.
auth.log.1   boot.log       daemon.log.3.gz  debug.2.gz    dmesg.0       dmesg.4.
auth.log.2.gz daemon.log     daemon.log.4.gz  debug.3.gz    dmesg.1.gz    kern.log
root@CNT-DMZ-Apache1:/var/log# cd tmp
-bash: cd: tmp: No such file or directory
root@CNT-DMZ-Apache1:/var/log# cd ../../..
root@CNT-DMZ-Apache1:/# cd Desktop
-bash: cd: Desktop: No such file or directory
```

לאחר בדיקה ב-auth.log נראה היה כמה ניסיונות כושלים להתחבר עד אשר צלח.

וגם בקובץ daemon.log היו דברים חשודים.

פנינו אל השרת APACHE1 כדי לראות מה גורם לנפילה וגילינו כי השירות נופל עקב תקייה בשם bd_bash ששולחת פקודת כיבוי לשירות כל דקה.

מחקנו את המשתמש שלו מהתיקיה temp ובעזרת פקודת crontab ערכנו את הקובץ והעלנו חזרה את השירות ע"י הפקודה `sudo service apache start`.

והשירות רץ בהצלחה.

תהליך הגנה מונעת: להקשיח את הסיסמאות, לבטל את החיבור ל-ssh שלא לצורך ולהוריד את כמות הניסיונות הכושלים על מנת למנוע דבר שכזה בעתיד.

הסבר מפורט על אופן ההתקפה (התמקדות בחולשות): התוקף השתמש בסריקת פורטים וככה גילה שיש גישה לפורט 22 (SSH) ומשם הצליח לחדור לשרת ולהשתיל פקודה באחד הקבצים על מנת להפיל את השירות.

כלים חדשים שפיתחתם/השתמשתם: ArcSight, zennos, putty.

אופן עבודת הצוות: היה חוסר סינכרון בין אנשי הצוות ומכך נוצר מלא בעיות וטעויות קריטיות להמשך הטיפול בבעיה.

חוסרים/קשיים/בעיות: היה חסר לנו הרבה פרטים וידע בדברים מאוד בסיסיים אבל למרות הכל הצלחנו לעמוד במשימה!

יש לשלב לוח זמנים, ותמונות בתהליכים שאתם מפרטים (כמובן, היכן שרלוונטי).