

דו"ח מעבדה- תרחיש מס' 1

פרטים:

מגיש: מירב בויס 206489155

תאריך: 12.4.2018

שם התרחיש:

תהליך ההתקפה:

סריקת פורטים ל Apache1 ו Apache3, ניחוש סיסמאות ל Apache1 והתחברות. הפעלת תהליך שמריץ כל דקה תוכנית שמפילה את הסררויס Apache2 ושולח לעצמו את הקבצים shadow, passwd.

תהליך הזיהוי:

זיהינו ב ArcSight שכתובת חיצונית 199.203.100.30 מבצעת סריקת פורטים על Apache3, וכתובת חיצונית 199.203.100.178 מבצעת סריקת פורטים וניחוש סיסמאות על Apache2.

ראינו ב Zenoss שהסררויס Apache2 נפל. נכנסנו ל Apache1 עם putty והעלנו את הסררויס (ע"י הפקודה service Apache2 start) וגילינו שהוא שוב נפל (ע"י הפקודה service -status-all).

```
root@CNT-DMZ-Apache1:/# service apache2 start
* Starting web server apache2
root@CNT-DMZ-Apache1:/# service -status-all
[ - ] apache2
```

בדקנו log וגילינו שכל דקה רצה פקודה להפלת Apache2 והפעלת ה bash.

```
root@CNT-DMZ-Apache1:/var/log# tail lastlog
d@2pts/5192.168.110.122root@CNT-DMZ-Apache1:/var/log# tail syslog
pr 12 14:20:01 CNT-DMZ-Apache1 CRON[10421]: (root) CMD (/tmp/bd_bash.sh)
pr 12 14:21:01 CNT-DMZ-Apache1 CRON[10449]: (root) CMD (/tmp/bd_bash.sh)
pr 12 14:21:01 CNT-DMZ-Apache1 CRON[10450]: (root) CMD (/etc/init.d/apache2 stop)
```

עשינו חיפוש ב Apache1 ומצאנו את הקובץ bs_bash.sh וחקרנו אותו. ראינו שיש בו פקודות שמריצות קובץ python שמעתיק את הקבצים passwd, shadow.

```
b64phpuploader.py bd bd_bash.sh vgauthsvclog.txt.0 vmware-root  
root@CNT-DMZ-Apache1:/tmp# nano bd_bash.sh
```

הגענו ל cron וגילינו שיש שתי פקודות שרצות כל דקה, פקודה שמפילה את הסרוויס Apache2 ופקודה שמריצה את bs_bash.sh.

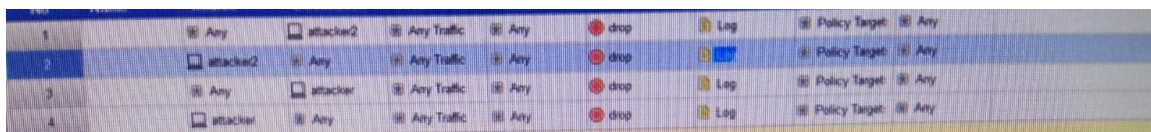
```
root@CNT-DMZ-Apache1:/var/log# env EDITOR=nano crontab -e
```

```
* * * * * /tmp/bd_bash.sh  
* * * * * /etc/init.d/apache2 stop
```

קראנו ובדקנו מה אלה הקבצים passwd, shadow.

תהליך הגנה:

חסמנו את התקשורת פנימה והחוצה עם 199.203.100.178 ב firewall



1	Any	attacker2	Any Traffic	Any	drop	Log	Policy Target	Any
2	attacker2	Any	Any Traffic	Any	drop	Log	Policy Target	Any
3	Any	attacker	Any Traffic	Any	drop	Log	Policy Target	Any
4	attacker	Any	Any Traffic	Any	drop	Log	Policy Target	Any

מחקנו את הקובץ bs_bash.sh והשבתנו את המשימות ב cron.

הרמנו את הסרוויס Apache2.

שינינו סיסמא.

תהליך הגנה מונעת:

סגירת פורט 20

ניהול הרשאות גישה לכתיבה וקריאה לתקיות וקבצים.

שינוי סיסמאות בארגון לסיסמאות חזקות יותר

הפרצות באבטחת הארגון

ssh היה פתוח.

סיסמאות פשוטות וקלות לניחוש.

כלים שפיתחנו

לא פיתחנו

אופן עבודת הצוות

חלוקת העבודה בין כולם, כל אחד בדק מה שהיה יכול והיה צורך בכך.
כל אחד שקרא על דבר מסויים באינטרנט שיתף והסביר לשאר חברי הקבוצה.

חוסרים/קשיים

קושי לזהות את מטרת התוקף.
קושי לעלות את השרת שנפל ולהבין מה גורם לנפילתו מחדש.