דוח אירוע - 2

מגיש: עוז מעתוק 305181158

שם התרחיש: Apache Server Attack

תהליך התקפה: התקפה מסוג זה בנוייה בכדי לפגוע ברשתי ה web של Apache, לכן ראשית על התוקף הייתה לזהות את היעד המבוקש. פעולתו הראשונה של התוקף (לאחר מציאת הרשת עצמה) הייתה סריקת פורטים פתוחים על 130.2.1.21 זאת בכדי להסיק מה תפקידו של המחשב הנבדק וגילוי חולשותיו שהם הפורטים הפתוחים למעבר, כך ידע התוקף להתאים את פעולותיו לנק' התורפה של היעד. חשוב לציין כי סריקת הפורטים מתבצעת מחוץ למחשב המיועד להתקפה, לכן לאחר פיענוח הפורטים הפתוחים ניתן היה לתוקף לגשת על תוך היעד. כמובן שבזכות הגדרת סיסמא בכניסה לשרתי הרשת שלנו, נדרש מהתוקף לפענח את הסיסמא המתאימה, לשם כך הפעיל התוקף שיטת BruteForce אשר מנסה לבצע פעולה כניסה עבור סיסמאות מוגרלות (generate) עד מציאת הסיסמא הנכונה וביצוע החדירה לשרת. לאחר פריצתו של התוקף לשרת המיועד, בוצעה פעולת הפסקה לתהליך Ipservice אשר תומך בתחזוקת אתרי האינטרנט על הרשת. בעקבות הפסקת התהליך הנ"ל, לא ניתן היה לגשת לאתרים בשירות שרת ה Apache. הפקודה להפסת השירות הוכנסה למתזמן משימות CRON כך שתפעל בצורה אוטומטים.

תהליך הזיהוי: תחילה העמדנות תצפית בכל כלי שיכולנו, כאשר הכלים האפקטיבים היו ה – ArcSight, CheckPoint Dashboard, וה – Zenoss. הסיבה לכך שדווקא כלים אלו היו רלוונטים לתרחיש היא מפני שה ArcSight מאפשר לנו לזהות תרחישים שאינם עומדים בחוקיות המוטמעת במערכת, CheckPoint Dashboard מנטרת את תעבורת הרשמת ומתייגת מקרים לפעולות רשת מוכרות, וה – Zenoss עוקבת אחר תהליכים ושרותים אשר נמצאים בכלל הרשת. הפעולה החריגה הראשונה לב שמנו לב במערכת הייתה על חומת האש שלנו דרך תוכנת ה CheckPoint Dashboard, אשר הציגה לנו פעולה של סריקת פורטים על 130.2.1.21 שמקורה הוא כתובת IP אשר אינה מוכרת לרשת שלנו, במקביל קפצה התרעה על Password Guessing ב ArcSight. בהמשך לשתי מקרים אלו זוהתה תקיפת ה BrutForce ב CheckPoint Tracker שסיפק לנו פרטים נוספים על התוקף, בעקבות כך נכנסו לקבצי הלוג של שירות ה SSH על השרת הנתק Apache בכדי לברר על פרטים נוספים אודות התקיפה. גם שם ראינו לוגים המתאימים להתקפת ה BrutForce וניחוש הסיסמאות. לאחר מכן הבחנו בהפסקה של תהליך IP service על שרת ה Apache1 ברשת. לאחר בירור על התהליך הנ"ל ביצענו ניסיונות התחברות לדפים עליהם השרת הנ"ל אחראי, אך ללא הצלחה. בשלב הזאת הגענו למסקנה כי ההתקפה כיוונה לפגוע בשירות האינטרנט של שרתי ה Apache שלנו ברשת (יש השארה כי היא גם נועדה לגניבת מידע בנוסף לפגיעה). בתגובה להפלת התהליך, הרצנו פקודה להפעלתו בחזרה, כאשר לאחר מס' דקות הבחנו כי התהליך מופסק פעם נוספת. מכך עלה החשש כי הפעולה להפסקת התהליך אינה ידנית אלא אוטומטים. לבדיקה נכנסנו ל Log file של שרת ה Apache, וראינו פקודות על שירות ה CRON שהוא מתזמן משימות למערכות יוניקס. זה גרר אותנו לבדוק קבצים אשר קשורים ל CRON, ובתוך crontab אשר מכיל את רשימת הפעולות המתוזמנות ראינו כי קיימות שתי שורות להפעלת סקריפטים, האחת הפעלה של

הסקריפט bd_bash אשר לא הצלחנו לחקור יותר מידי מפני שביצענו בשלב מסויים הפעלה מחדש של שרת ה Apache וזה גרם למחיקה של הסקריפט הנ"ל. השנייה apache2 stop אשר עוצרת את שרת ה Apache. מאיסוף מידע על סקריפט ה bd_bash, נודע לנו כי מטרתו היית להעביר מידע בפרוטוקול HTTP מהשרת שלנו לתוקף. בפעולה זאת הבחנו ב Tracker אך לא קישרנו את המקרה. מהשלמת פערים מול קבוצות אחרון נודע לנו כי הסיסמאות אשר בהן השתמש התוקף בתקיפת ה BrutForce הן סיסמאות שהוא לקח מתוך שרת ה DC שלנו. מסתבר שהתוקף פרץ לתוך שבת ה DC אשר מנהל ומכיל את כל המידע על את כלל המשתמשים המוזנים במערכת, וזה כולל את הסיסמאות שלהם. לכן הצליח הפורץ להכנס אל תוך השרתים שלנו ע"י הכרת טווח הסיסמאות הקיים לנו ברשת.

<u>תהליך ההגנה ראשוני:</u> כמובן, כמו בתרחיש הקודם, התגובות הראשניות להפלת תהליכים ברשת שלנו וחדירה של גורם זר הן הפעלת התהליך מחדש ע"י התחברות לשרת המכיל את התהליך והרצת פקודה מתאימה להחייאתו, ולגבי החדירה בוצעה חסימת כתובתו של הפורץ ע"י הגדרת חוק מתאים בחומת האש של הרשת ע"י תוכנת ה Dashboard של Checkpoint.

- יש לציין כי לאחר הפעלת התהליך הנפגע, ביחד עם חסימת כתובת ה IP החשודה, התהליך הנ"ל נפל שוב ושוב. מתוך זו ניתן להסיק כי הפסקת התהליך אינה בוצעה בצורה ידנית אלא ע"י התמאת פקודה / סקריפט אוטומטי אשר מבצע את הפסקת התהליך בכל פעם מחדש בתירות מסויימת.

<u>תהליך הגנה מונעת:</u> כמו שצויין בתהליך ההגנה הראשוני, חסימת כתובת ה IP של התוקף היא פעולה הגנה מונעת אשר מגינה עלינו מפני התקפות נוספות מצד התוקף הספציפי (המחשב הספציפי בעצם), בנוסף את האוטומציה שנעשתה בעזרת הכנסת סקריפטים לתוכנת תיזמון התהליכים עצרו בכך שמחקנו את שורות הפעלת הסריפטים מהקובץ אשר מכיל את רשימת הפעולות לתיזמון crontab (בהמשך להסבר בתהליך הזיהוי).

- דרך נוספת למניעת התקפות מסוג זה, היא להגדיר חוק לא דווקא על כתובת האיי פי של התוקף החשוד, אלא להרכיב חוק אשר מתריע ומונע את תקיפות ה BrutForce. החוק יזהה את תקיפת ה BrutForce ע"י הכרה במאפיינים שלה, אזי הצפה של בקשות אימות סיסמא בזמן קצר.
- ניתן בנוסף לסגור את כלל הפורטים אשר אינם משמשים באופן קבוע את צרכי הרשת וכך לצמצם את היכולת הפגיעה של תוקפים.
- כמו שהוסבר על הגדרת חוק לניתור BrutForce, על אותו עיקרון ניתן להתמיע חוק לניתור Port Scanning, וכך להגן על הרשת שלנו גם ממקרים אלו.

<u>הסבר מפורט על אופן ההתקפה (התמקדות בחולשות):</u> החולשה הראשונה שבעקבותיה יכל הפורץ להתחיל את התקפתו היא האפשרות לבצע סריקת פורטים על אחד מהשרתים שלנו ללא קושי כלל, דבר שהוביל להסקת מסקנות בצד של התוקף לגבי הרשת שלנו ואפשרות ההבחנה בסוג השרת או סוג השירות אשר עליו אחראי השרת הנבדק. מרכז העניין בהפקרת הפורטים היא בעצם החולשה הגדולה ביותר! מפני שפורטים פתוחים הם כמו דלתות פתוחות לפורצים. חולשה שנייה ומאוד בולטת היא האפשרות לבצע התחברות ע"י SSH מכל משתמש בעולם אל תוך השרתים ברשת שלנו (שאמורה להיות מאובטחת), כמענה לכך ניתן להכניס חוקים אשר מאפשרים פעולות SSH אך ורק מכתובות IP ספציפיות ומוקרות למנהלי הרשת.

כלים חדשים שפיתחתם/השתמשתם: פקודות לינוקס הקשורות בניהול תהליכים, חקירת שרת Apache והכרת המבנה שלו המערכת ההפעלה Linux. במהלך התרחיש השתמשנו בפקודות כמו less בכדי לקרוא קבצי לוגים, Apache stop/restart לניהול שרת ה Apache, ps aux להצגת התהליכים הרצים על המערכת, crontab –e לצפייה ועריכה בקובץ המשימות של המזמן cron, ופקודות נוספות המפורטות בלינקים למטה להפעלה/הפסקת תהליכים במערכת ה Linux. שימוש נרחב יותר בתוכנת ה CheckPoint SmartView Tracker (SIEM app).

אופן עבודת הצוות: שוב כמו בתרחיש הקודם, עבודת הצוות התחלקה למשימה כאשר אחר מהחברים קיבל את הפיקוד לידיים, חילק את העבודה ודאג לסנכרן את חברי הצוות התוצאות ובדרישות נוספות. הפעם שיתוף הפעולה כלל גם עבודה בזוגות על כל מימצא מפני שנדרש מאיתנו לגלות הבנה רבה יותר בכדי לפענח את המתרחש ברשת.

חוסרים/קשיים/בעיות: הבעיה הראשונה שניתן להתייחס אליה כי תקלה טכנית בחלק הראשון של התרחיש, שבעקבותיה לא הופיעו לנו אזהרות בשירות ה – Zenoss עקב נפילת תהליכים ברשת. קושי נוסף אשר נגע אלינו הוא העובדה כי כאשר אחד השרתים נפגע, רק אדם אחד יכול לעבוד עליו ולחקור אותו, ואז התקדמות הקבוצה נתלת אך ורק באדם אחד. מתוך כך נדרש לנו יותר זמן מאשר שניתן לנו באותם הימים בכדי לתפעל את התרחיש. בנוסף, במהלך חקירת התרחיש, ניסנו להתחבר לתוקף בכדי לקבל עליו מידע ואולי גם לפגוע בו על מנת להגן על הרשת שלנו. ברגע שביצענו פעולה כזאת הפכנו חשופים עוד יותר לתקיפות ולחדירה לרשת הפנימית שלנו. מסקנה ממקרה זה הביא לכך שצריך להתשמש בכלי SandBox אשר יוצרת סביבה בטוחה לעבודה באיזור פגיע.

ציון זמנים וצעדי התקדמות של הצוות:

1. 9:00-> Password guessing, Port scanning.

   Password guessing: Aggregate if at least 5 matching conditions are found within 2 Minutes AND these event fields are the same.

   Port scanning: Aggregate if at least 20 matching conditions are found within 30 Seconds AND these event fields are unique (event1.Destination Port) AND these event fields are the same. Attacker: 199.203.100.231 Destenation: 130.2.1.21.

2. 9:11-> Zenoss: IP Service HTTP is down.

3. 9:15-> Getting inside Apache1 server, getting list of whole services running at server by typing: ls /etc/init.d

4. 9:20-> Adding new rule to Check Point Dashboard from Apache to 199.203.100.231

5. 9:25-> Verify policyS

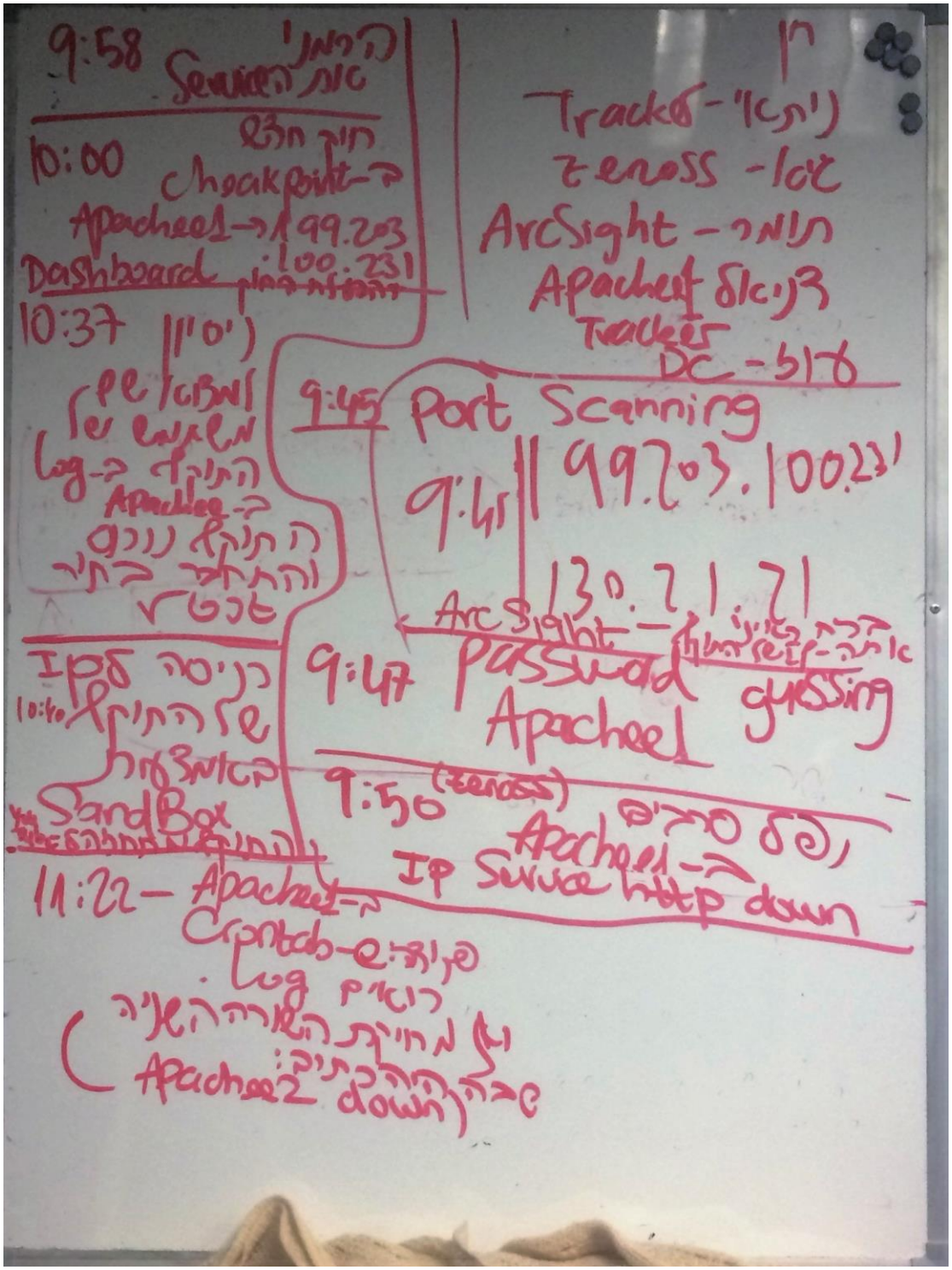
6. 9:30-> Log of autentication, searched for attacker autenticate

7. 9:40-> crontab -e, delete second line shutting down apache2

8. 9:45-> service apache2 start.

תמונות:

First of all the baord



BrutForce Attack for getting into server, using passwords that he got from DC. at Checkpoint Tracker

No.	Date	Time	Origin	Service	Source	Source User Name	Destination	Rule	Curr. Rule ...	Rule Name	Source P
1661731	6Apr2016	7:58:18	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	41535
1661741	6Apr2016	7:58:18	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	41543
1661824	6Apr2016	7:58:23	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39512
1661835	6Apr2016	7:58:23	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39521
1661923	6Apr2016	7:58:28	cnt-fw	KerbCanagePassword_TCP	WS-Ubuntu-CNT1		CNT-DC1	10	10-Standard	UsersToServers	34452
1661934	6Apr2016	7:58:28	cnt-fw	KerbCanagePassword_TCP	WS-Ubuntu-CNT1		CNT-DC1	10	10-Standard	UsersToServers	34461
1662443	6Apr2016	7:58:48	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43712
1662453	6Apr2016	7:58:48	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43720
1662598	6Apr2016	7:58:53	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39530
1662609	6Apr2016	7:58:53	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39539
1662753	6Apr2016	7:58:58	cnt-fw	KerbCanagePassword_TCP	WS-Ubuntu-CNT1		CNT-DC1	10	10-Standard	UsersToServers	34470
1662764	6Apr2016	7:58:58	cnt-fw	KerbCanagePassword_TCP	WS-Ubuntu-CNT1		CNT-DC1	10	10-Standard	UsersToServers	34479
1663476	6Apr2016	7:59:18	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43728
1663483	6Apr2016	7:59:18	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43733
1663494	6Apr2016	7:59:18	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43741
1663657	6Apr2016	7:59:23	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39548
1663668	6Apr2016	7:59:23	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39557
1663813	6Apr2016	7:59:28	cnt-fw	KerbCanagePassword_TCP	WS-Ubuntu-CNT1		CNT-DC1	10	10-Standard	UsersToServers	34490
1663824	6Apr2016	7:59:28	cnt-fw	KerbCanagePassword_TCP	WS-Ubuntu-CNT1		CNT-DC1	10	10-Standard	UsersToServers	34499
1664442	6Apr2016	7:59:48	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43749
1664452	6Apr2016	7:59:48	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43757
1664587	6Apr2016	7:59:53	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39566
1664598	6Apr2016	7:59:53	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39575
1664762	6Apr2016	7:59:58	cnt-fw	KerbCanagePassword_TCP	WS-Ubuntu-CNT1		CNT-DC1	10	10-Standard	UsersToServers	34508
1664773	6Apr2016	7:59:58	cnt-fw	KerbCanagePassword_TCP	WS-Ubuntu-CNT1		CNT-DC1	10	10-Standard	UsersToServers	34517
1665116	6Apr2016	8:00:18	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43765
1665126	6Apr2016	8:00:18	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43773
1665190	6Apr2016	8:00:23	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39584
1665201	6Apr2016	8:00:23	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39593
1665280	6Apr2016	8:00:28	cnt-fw	KerbCanagePassword_TCP	WS-Ubuntu-CNT1		CNT-DC1	10	10-Standard	UsersToServers	34528
1665291	6Apr2016	8:00:28	cnt-fw	KerbCanagePassword_TCP	WS-Ubuntu-CNT1		CNT-DC1	10	10-Standard	UsersToServers	34537
1665707	6Apr2016	8:00:48	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43781
1665714	6Apr2016	8:00:48	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43786
1665724	6Apr2016	8:00:48	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43794
1665813	6Apr2016	8:00:53	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39602
1665824	6Apr2016	8:00:53	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39611
1665959	6Apr2016	8:00:58	cnt-fw	KerbCanagePassword_TCP	WS-Ubuntu-CNT1		CNT-DC1	10	10-Standard	UsersToServers	34546
1665970	6Apr2016	8:00:58	cnt-fw	KerbCanagePassword_TCP	WS-Ubuntu-CNT1		CNT-DC1	10	10-Standard	UsersToServers	34555
1666392	6Apr2016	8:01:18	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43802
1666402	6Apr2016	8:01:18	cnt-fw	KerbCanagePassword_TCP	CNT-Web_Apache		CNT-DC1	26	26-Standard	ToAuthServers	43810
1666484	6Apr2016	8:01:23	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39620
1666495	6Apr2016	8:01:23	cnt-fw	KerbCanagePassword_TCP	192.168.100.24		CNT-DC1	10	10-Standard	UsersToServers	39629

And in the Apache server logs...

You can see the attack, included CRON commands

```
ed for user root
Apr 13 06:24:45 CNT-DMZ-Apache1 login[949]: pam_unix(login:session): session ope
ned for user root by LOGIN(uid=0)
Apr 13 06:24:45 CNT-DMZ-Apache1 login[6724]: ROOT LOGIN  on '/dev/tty1'
Apr 13 06:25:01 CNT-DMZ-Apache1 CRON[6737]: pam_unix(cron:session): session open
ed for user root by (uid=0)
Apr 13 06:43:23 CNT-DMZ-Apache1 sshd[6894]: Did not receive identification strin
g from 199.203.100.231
Apr 13 06:44:37 CNT-DMZ-Apache1 sshd[6899]: Did not receive identification strin
g from 199.203.100.231
Apr 13 06:44:50 CNT-DMZ-Apache1 sshd[6900]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.231  user=root
Apr 13 06:44:52 CNT-DMZ-Apache1 sshd[6900]: Failed password for root from 199.20
3.100.231 port 53088 ssh2
Apr 13 06:44:52 CNT-DMZ-Apache1 sshd[6902]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.231  user=root
Apr 13 06:44:54 CNT-DMZ-Apache1 sshd[6902]: Failed password for root from 199.20
3.100.231 port 59682 ssh2
Apr 13 06:44:54 CNT-DMZ-Apache1 sshd[6904]: Invalid user admin from 199.203.100.
231
Apr 13 06:44:54 CNT-DMZ-Apache1 sshd[6904]: pam_unix(sshd:auth): check pass; use
r unknown
Apr 13 06:44:54 CNT-DMZ-Apache1 sshd[6904]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.231
Apr 13 06:44:56 CNT-DMZ-Apache1 sshd[6904]: Failed password for invalid user adm
in from 199.203.100.231 port 34606 ssh2
Apr 13 06:44:57 CNT-DMZ-Apache1 sshd[6906]: Invalid user admin from 199.203.100.
231
Apr 13 06:44:57 CNT-DMZ-Apache1 sshd[6906]: pam_unix(sshd:auth): check pass; use
:_
```

and the sucssece

```
r unknown
Apr 13 06:44:57 CNT-DMZ-Apache1 sshd[6906]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.231
Apr 13 06:44:58 CNT-DMZ-Apache1 sshd[6906]: Failed password for invalid user adm
in from 199.203.100.231 port 33361 ssh2
Apr 13 06:44:58 CNT-DMZ-Apache1 sshd[6908]: Invalid user user from 199.203.100.2
31
Apr 13 06:44:58 CNT-DMZ-Apache1 sshd[6908]: pam_unix(sshd:auth): check pass; use
r unknown
Apr 13 06:44:58 CNT-DMZ-Apache1 sshd[6908]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.231
Apr 13 06:45:01 CNT-DMZ-Apache1 sshd[6908]: Failed password for invalid user use
r from 199.203.100.231 port 38435 ssh2
Apr 13 06:45:01 CNT-DMZ-Apache1 sshd[6910]: Accepted password for root from 199.
203.100.231 port 55778 ssh2
Apr 13 06:45:01 CNT-DMZ-Apache1 sshd[6910]: pam_unix(sshd:session): session open
ed for user root by (uid=0)
Apr 13 06:45:36 CNT-DMZ-Apache1 sshd[6976]: Accepted password for root from 199.
203.100.231 port 54805 ssh2
Apr 13 06:45:36 CNT-DMZ-Apache1 sshd[6976]: pam_unix(sshd:session): session open
ed for user root by (uid=0)
Apr 13 06:45:36 CNT-DMZ-Apache1 sshd[6983]: Accepted password for root from 199.
203.100.231 port 42251 ssh2
Apr 13 06:45:36 CNT-DMZ-Apache1 sshd[6983]: pam_unix(sshd:session): session open
ed for user root by (uid=0)
Apr 13 06:45:36 CNT-DMZ-Apache1 sshd[6983]: subsystem request for sftp
Apr 13 06:51:01 CNT-DMZ-Apache1 CRON[7263]: pam_unix(cron:session): session open
ed for user root by (uid=0)
Apr 13 06:51:19 CNT-DMZ-Apache1 sshd[6976]: Received disconnect from 199.203.100
:
```

Port scanning from out attacker, and ssh connection in the CheckPoint Tracker

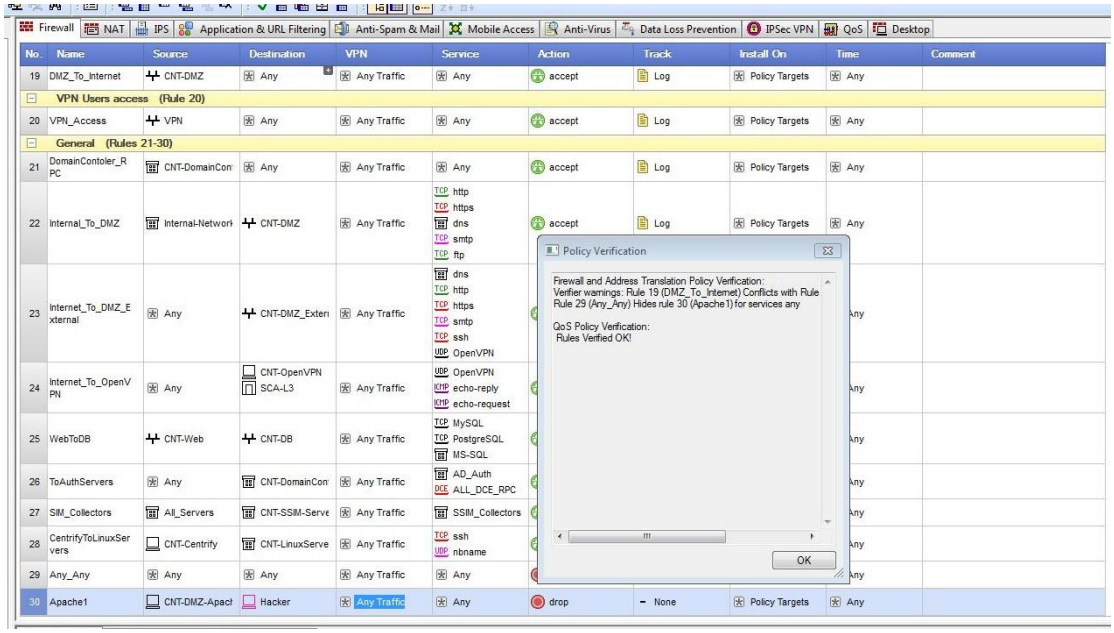
No.	Date	Time	Origin	Service	Source	Source User Name	Destination	Rule	Curr. Rule ...	Rule Name	Source Por
1040...	13Apr2016	6:43:29	cnt-fw-dmz	759	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	44073
1040...	13Apr2016	6:43:29	cnt-fw-dmz	766	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	38648
1040...	13Apr2016	6:43:29	cnt-fw-dmz	761	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	34340
1040...	13Apr2016	6:43:29	cnt-fw-dmz	765	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	48761
1040...	13Apr2016	6:43:29	cnt-fw-dmz	762	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	39839
1040...	13Apr2016	6:43:29	cnt-fw-dmz	760	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	44847
1040...	13Apr2016	6:43:29	cnt-fw-dmz	758	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	52056
1040...	13Apr2016	6:43:29	cnt-fw-dmz	767	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	35797
1040...	13Apr2016	6:43:30	cnt-fw-dmz	771	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	41640
1040...	13Apr2016	6:43:30	cnt-fw-dmz	770	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	47313
1040...	13Apr2016	6:43:30	cnt-fw-dmz	775	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	34878
1040...	13Apr2016	6:43:30	cnt-fw-dmz	777	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	41610
1040...	13Apr2016	6:43:30	cnt-fw-dmz	772	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	53104
1040...	13Apr2016	6:43:30	cnt-fw-dmz	774	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	36755
1040...	13Apr2016	6:43:30	cnt-fw-dmz	773	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	37869
1040...	13Apr2016	6:43:30	cnt-fw-dmz	769	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	42248
1040...	13Apr2016	6:43:30	cnt-fw-dmz	776	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	59464
1040...	13Apr2016	6:43:30	cnt-fw-dmz	768	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	39785
1040...	13Apr2016	6:43:32	cnt-fw-dmz	784	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	49925
1040...	13Apr2016	6:43:32	cnt-fw-dmz	781	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	54424
1040...	13Apr2016	6:43:32	cnt-fw-dmz	778	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	43673
1040...	13Apr2016	6:43:32	cnt-fw-dmz	780	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	51840
1040...	13Apr2016	6:43:32	cnt-fw-dmz	786	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	52797
1040...	13Apr2016	6:43:32	cnt-fw-dmz	782	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	44870
1040...	13Apr2016	6:43:32	cnt-fw-dmz	783	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	49282
1040...	13Apr2016	6:43:32	cnt-fw-dmz	785	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	54565
1040...	13Apr2016	6:43:32	cnt-fw-dmz	779	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	46056
1040...	13Apr2016	6:43:32	cnt-fw-dmz	787	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	54250
1040...	13Apr2016	6:43:33	cnt-fw-dmz	789	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	44181
1040...	13Apr2016	6:43:33	cnt-fw-dmz	1443	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	60247
1040...	13Apr2016	6:43:33	cnt-fw-dmz	788	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	56701
1040...	13Apr2016	6:43:33	cnt-fw-dmz	socks	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	50835
1040...	13Apr2016	6:43:33	cnt-fw-dmz	790	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	44741
1040...	13Apr2016	6:43:33	cnt-fw-dmz	HTTP_and_HTTPS_proxy	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	35551
1040...	13Apr2016	6:44:37	cnt-fw-dmz	ssh	199.203.100.231		130.2.1.21	23	23-Standard	Internet_To_DMZ_External	54398
1040...	13Apr2016	6:44:50	cnt-fw-dmz	ssh	199.203.100.231		130.2.1.21	23	23-Standard	Internet_To_DMZ_External	53088
1040...	13Apr2016	6:44:52	cnt-fw-dmz	ssh	199.203.100.231		130.2.1.21	23	23-Standard	Internet_To_DMZ_External	59682
1040...	13Apr2016	6:44:54	cnt-fw-dmz	ssh	199.203.100.231		130.2.1.21	23	23-Standard	Internet_To_DMZ_External	34606
1040...	13Apr2016	6:44:56	cnt-fw-dmz	ssh	199.203.100.231		130.2.1.21	23	23-Standard	Internet_To_DMZ_External	33361
1040...	13Apr2016	6:44:58	cnt-fw-dmz	ssh	199.203.100.231		130.2.1.21	23	23-Standard	Internet_To_DMZ_External	38435
1040...	13Apr2016	6:45:01	cnt-fw-dmz	ssh	199.203.100.231		130.2.1.21	23	23-Standard	Internet_To_DMZ_External	55778
1040...	13Apr2016	6:45:36	cnt-fw-dmz	ssh	199.203.100.231		130.2.1.21	23	23-Standard	Internet_To_DMZ_External	54805
1040...	13Apr2016	6:45:36	cnt-fw-dmz	ssh	199.203.100.231		130.2.1.21	23	23-Standard	Internet_To_DMZ_External	42251

Ip service on Apache server if shutdown by the attacker (in Zenoss)

Status	Severity	Resource	Component	Event Class	Summary
		CNT-DMZ-Apache1	http	/Status/IpService	IP Service http is down
		localhost		/Status/Snmp	SNMP agent down - no response received
		CNT-Files	DFSR	/Unknown	The DFS Replication service detected invalid msl
		CNT-DC1	zenwin	/Status/Wmi	Could not read Windows services (NT code 0x80
		CNT-DC1	zenwin	/Status/Wmi	Could not read Windows services (NT code 0xc0

Enter to the crontab filr of CRON job scheduler, and removing the commands that the attacker added

Making a rule that will block all activity from the attacker by his IP address (CheckPoint DashBoard)



<u>להרחבה / קישורים נוספים:</u>

IP service –

שירות אשר קיים בשרתים האחריים לתחזוקת אתרי אינטרנט, ותפקידו הוא לנהל ולתחזוק כתובות IP עבור האתרים אשר הוא אחראי עליהם. התהליך מבצע גם הפניות לדפים נדרשים על סמך בקשות ממשתמשים בשרת (או בדפים) ומתייג כתובות מתאימות לדפים ואתרים מתאימים.

BruteForce –

שיטה לפיצוח סיסמאות ופריצה, אשר מג'נרטת (מגרילה) סיסמאות מתאימות עבור ניסיון פריצה מסויים עד מציאת הסיסמא הנכונה.

Apache Server –

שרת האפאצ'י הוא שרת ה HTTP הנפוץ בעולם, מבוסס על פיתוח בקוד פתוח אשר מספק גמישות והתאמה למס' רב של צרכים בתחום אתרי האינטרנט. שרת זה מסוגל לעבוד על מס' מערכות הפעלה ומשמש כ שרת פרוקסי קדמי, כלומר שרת המקבל בקשות ממשתמשים ומעביר אותן הלאה, אל שרתי יישום שונים, שבהם מיושם האתר עצמו.

Port Scanning –

סריקת פורטים היא שיטה להכרת מחשב היעד (המחשב הנסרק) והפורטים אשר איתם הוא עובד ע"י שליחת בקשות במגוון פורטים וסימון התשובות המתקבלות עבור פורטים פעילים. פעולה זו מספקת מידע שמיש על המחשב/מערכת/שרת כמו אילו שירותים הוא אחראי ומספק. סריקת הפורטים משמשת מנהלי רשת לתחומי אבטחה, ותוקפי רשת לאיתור חולשות.

CRON –

כלי תוכנה אשר מבצע תיזמון משימות למערכות הפעלה על בסיס יוניקס

SendBox –

תוכנה הנועדה ליצור סביבה מנותקת מהמחב והרשת אשר אתה באמת למצא בא, כך שעליה תוכל להכנס לסביבות לא בטוחות ולבצע פעולות אשר יכולות להביא לפעיגה באבטחה שלך ושל הרשת שלך. התוכנה בצעת חלוקה של זיכרון ומקום איחסון מתוך המכונה עליה היא ריצה, עוטפת אותה בזהות אחרת וכמובן דואגת לחסימת תקשורת ופעולות בין המכונה המריצה לכלל התהליכים הרצים ב SendBox.

Linux commands for proccess menaging

Apache linux commands

Cron commands