דוח אירוע - 3

מגיש: עוז מעתוק 305181158

שם התרחיש: Web Defacement

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 משהו משהו. בעקבות הפסקת התהליך הנ"ל, לא ניתן היה לגשת לאתרים שנפגעו בשרת ה Apache.

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 לה שמנו לב במערכת הייתה על 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 הנתקף Apache בכדי לברר על פרטים נוספים אודות התקיפה. גם שם ראינו לוגים המתאימים להתקפת ה BrutForce וניחוש הסיסמאות. לאחר ניסיונות התחברות לדפים האינטרנט עליהם השרת הנ"ל אחראי, גילינו כי אתר ה BBC נפרץ וטוען לנו תמונת מסך "Hacked". בשלב הזאת הגענו למסקנה כי ההתקפה כיוונה לפגוע בדפי האינטרנט של שרתי ה Apache שלנו. בעקבות כך עלו לנו שתי חשדות, האחת כי קיימת הפנייה מתוך כתובת אתר ה BBC שלנו לאתר אחר (של התוקף) והשנייה כי בוצעה עריכת קבצי מקור אתר האינטרנט BBC. האפשרות הראשונה בוטלה לאחר חקירה קצרה על שרת ה Apache והמסקנה כי אנו על המחשבים שלנו לא יכולנו לטעון דף אשר אינו ממוקדם על הרשת המוגדרת, אך את הדך של התוקף אכן הצלחנו לטעון. מכך ניגשנו לתיקיית מקור הקבצים עבור אתר ה BBC ושם באמת גילינו כי הקבצים השתנו והוחלפו, בנוסף לכך מצאנו תיקייה "odl BBC" ובה נשמרו קצבי אתר ה BBC המקורי שלנו.

<u>תהליך ההגנה ראשוני:</u> כתגובה הראשנית להתקפה מסוג BrutForce וחדירה של גורם זר הזנו חסימה לכתובתו של הפורץ ע"י הגדרת חוק מתאים בחומת האש של הרשת ע"י תוכנת ה Dashboard של Checkpoint. בהמשך לחסימת התוקף, על אחריותינו הייתה להחזיר את כלל השירותים (אתר האינטרנט) לקדמותם. בזכות כך כי קבצי אתר ה BBC המקורי נשמרו על שרת ה Apache, ביצענו החלפה של הקבצים (התיקיות בעצם) ובכך המצב חזר לקדמותו ובפנייה לאתר ה BBC באמת באתר הנדרש עלה.

<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).

- 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. לאחר עיון במצגת התרחיש היתגלה כי התוקף השתמש ב Protocol Fuzzing על מנת לחדור אל תוך שרת ה Apache שלנו, זאת ניתן להבחין בקבצי הלוג על גבי פרוטוקול ה SSH אשר משרת את התוקפים שלנו כבר שלושה תרחישים. (להוסיף על מי יודע לסיסמא ואיך והאם ה brutforce היה מוצלח? מוצלח....)

<u>כלים חדשים שפיתחתם/השתמשתם:</u> פקודות לינוקס הקשורות בחיפוש מלל בקבצי השרת, פקודות עריכת קבצים, חקירת שרת Apache והכרת המבנה שלו המערכת ההפעלה Linux. במהלך התרחיש השתמשנו בפקודות כמו VIM בכדי לקרוא קבצי לוגים, rm, cp, mv לניהול קבצים בשרת ה Apache, ופקודות נוספות כמו find המפורטות בלינקים למטה אשר כלולות בסיבת ה Bash של מערכת ה Linux. שימוש נרחב בתוכנת ה CheckPoint SmartView Tracker (SIEM app) וכמובן (לא חדש) ב Zenoss.

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. גם הפעם שיתוף הפעולה כלל גם עבודה בזוגות על כל מימצא מפני שנדרש מאיתנו לגלות הבנה רבה יותר בכדי לפענח את המתרחש ברשת. בעקבות כך שהצוות כבר מנוסה יותר התרחיש התנהל בצורה חלקה יותר כאשר כל חברי הצוות לגלות הבנה ולהתחבר למתרחש בתרחיש גם אם זה לא חלק מהעמדה שלהם.

חוסרים/קשיים/בעיות: קושי עיקרי 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. בנוסף, נדרש התמצאות בקבצי שרת ה Apache ועירנות יתר לפעולות אשר אינן מנותרות ע"י הכלים אשר עומדים לרשותינו.

ציון זמנים וצעדי התקדמות של הצוות:

1. 7:37-> 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. 7:40-> Password guessing.

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

3. 7:45-> Getting inside Apache1 server, investegaiting the Log of autentication, searche and found for attacker autenticate and IP.

4. 7:50-> Adding new rule to Check Point Dashboard from Apache to Block the attacker IP

5. 7:52-> Verify policyS

6. 7:55-> notice that the BBC website was Hacked! And we are getting "Hacked Background" when loading it.

7. 7:57-> discover changes in BBC folder at the Apache server, and existing an "old BBC" folder there too. understanding want files in those two folders, the first one is the hacker work ans the second is our original BBC website files.

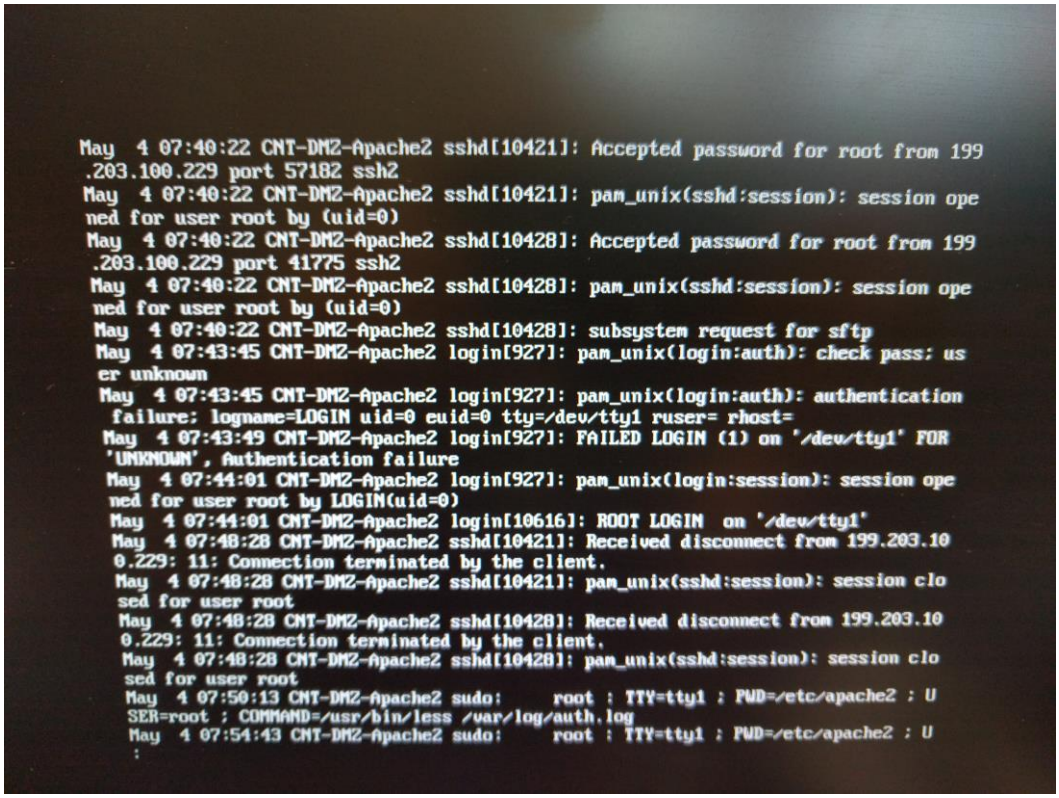
8. 8:00-> switching the paths, then BBC website back to original.

תמונות:

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	TCP 759	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	44073
1040...	13Apr2016	6:43:29	cnt-fw-dmz	TCP 766	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	38648
1040...	13Apr2016	6:43:29	cnt-fw-dmz	TCP 761	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	34340
1040...	13Apr2016	6:43:29	cnt-fw-dmz	TCP 765	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	48761
1040...	13Apr2016	6:43:29	cnt-fw-dmz	TCP 762	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	39839
1040...	13Apr2016	6:43:29	cnt-fw-dmz	TCP 760	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	44847
1040...	13Apr2016	6:43:29	cnt-fw-dmz	TCP 758	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	52056
1040...	13Apr2016	6:43:29	cnt-fw-dmz	TCP 767	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	35797
1040...	13Apr2016	6:43:30	cnt-fw-dmz	TCP 771	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	41640
1040...	13Apr2016	6:43:30	cnt-fw-dmz	TCP 770	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	47313
1040...	13Apr2016	6:43:30	cnt-fw-dmz	TCP 775	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	34878
1040...	13Apr2016	6:43:30	cnt-fw-dmz	TCP 777	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	41610
1040...	13Apr2016	6:43:30	cnt-fw-dmz	TCP 772	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	53104
1040...	13Apr2016	6:43:30	cnt-fw-dmz	TCP 774	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	36755
1040...	13Apr2016	6:43:30	cnt-fw-dmz	TCP 773	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	37869
1040...	13Apr2016	6:43:30	cnt-fw-dmz	TCP 769	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	42248
1040...	13Apr2016	6:43:30	cnt-fw-dmz	TCP 776	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	59464
1040...	13Apr2016	6:43:30	cnt-fw-dmz	TCP 768	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	39785
1040...	13Apr2016	6:43:32	cnt-fw-dmz	TCP 784	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	49925
1040...	13Apr2016	6:43:32	cnt-fw-dmz	TCP 781	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	54424
1040...	13Apr2016	6:43:32	cnt-fw-dmz	TCP 778	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	43673
1040...	13Apr2016	6:43:32	cnt-fw-dmz	TCP 780	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	51840
1040...	13Apr2016	6:43:32	cnt-fw-dmz	TCP 786	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	52797
1040...	13Apr2016	6:43:32	cnt-fw-dmz	TCP 782	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	44870
1040...	13Apr2016	6:43:32	cnt-fw-dmz	TCP 783	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	49282
1040...	13Apr2016	6:43:32	cnt-fw-dmz	TCP 785	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	54565
1040...	13Apr2016	6:43:32	cnt-fw-dmz	TCP 779	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	46056
1040...	13Apr2016	6:43:32	cnt-fw-dmz	TCP 787	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	54250
1040...	13Apr2016	6:43:33	cnt-fw-dmz	TCP 789	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	44181
1040...	13Apr2016	6:43:33	cnt-fw-dmz	TCP 1443	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	60247
1040...	13Apr2016	6:43:33	cnt-fw-dmz	TCP 788	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	56701
1040...	13Apr2016	6:43:33	cnt-fw-dmz	TCP socks	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	50835
1040...	13Apr2016	6:43:33	cnt-fw-dmz	TCP 790	199.203.100.231		130.2.1.21	29	29-Standard	Any_Any	44741
1040...	13Apr2016	6:43:33	cnt-fw-dmz	TCP 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	TCP 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	TCP 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	TCP 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	TCP 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	TCP 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	TCP 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	TCP 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	TCP 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	TCP ssh	199.203.100.231		130.2.1.21	23	23-Standard	Internet_To_DMZ_External	42251

BrutForce Attack for getting into server, in the Apache server logs.

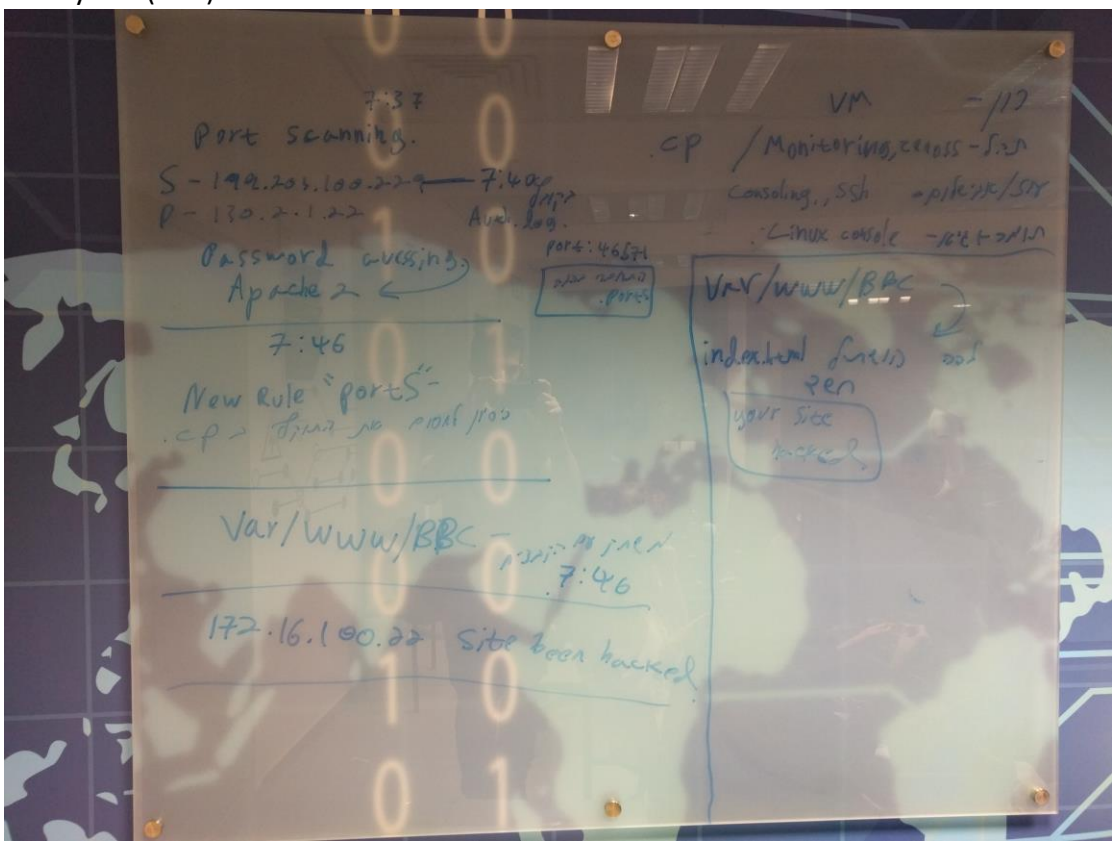


```
May  4 07:40:22 CNT-DMZ-Apache2 sshd[10421]: Accepted password for root from 199
.203.100.229 port 57182 ssh2
May  4 07:40:22 CNT-DMZ-Apache2 sshd[10421]: pam_unix(sshd:session): session ope
ned for user root by (uid=0)
May  4 07:40:22 CNT-DMZ-Apache2 sshd[10428]: Accepted password for root from 199
.203.100.229 port 41775 ssh2
May  4 07:40:22 CNT-DMZ-Apache2 sshd[10428]: pam_unix(sshd:session): session ope
ned for user root by (uid=0)
May  4 07:40:22 CNT-DMZ-Apache2 sshd[10428]: subsystem request for sftp
May  4 07:43:45 CNT-DMZ-Apache2 login[927]: pam_unix(login:auth): check pass; us
er unknown
May  4 07:43:45 CNT-DMZ-Apache2 login[927]: pam_unix(login:auth): authentication
 failure; logname=LOGIN uid=0 euid=0 tty=/dev/tty1 ruser= rhost=
May  4 07:43:49 CNT-DMZ-Apache2 login[927]: FAILED LOGIN (1) on '/dev/tty1' FOR
'UNKNOWN', Authentication failure
May  4 07:44:01 CNT-DMZ-Apache2 login[927]: pam_unix(login:session): session ope
ned for user root by LOGIN(uid=0)
May  4 07:44:01 CNT-DMZ-Apache2 login[10616]: ROOT LOGIN  on '/dev/tty1'
May  4 07:48:28 CNT-DMZ-Apache2 sshd[10421]: Received disconnect from 199.203.10
0.229: 11: Connection terminated by the client.
May  4 07:48:28 CNT-DMZ-Apache2 sshd[10421]: pam_unix(sshd:session): session clo
sed for user root
May  4 07:48:28 CNT-DMZ-Apache2 sshd[10428]: Received disconnect from 199.203.10
0.229: 11: Connection terminated by the client.
May  4 07:48:28 CNT-DMZ-Apache2 sshd[10428]: pam_unix(sshd:session): session clo
sed for user root
May  4 07:50:13 CNT-DMZ-Apache2 sudo:     root : TTY=tty1 ; PWD=/etc/apache2 ; U
SER=root ; COMMAND=/usr/bin/less /var/log/auth.log
May  4 07:54:43 CNT-DMZ-Apache2 sudo:     root : TTY=tty1 ; PWD=/etc/apache2 ; U
:
```

Find –cmin output for checking changed files

```
783619   12 drwxr-xr-x 106 root     root      12288 May  4 07:48 /var/www/BBC
784745    4 -rw-r--r--   1 root     root        563 May  4 07:46 /var/www/BBC/
index.html
786343   68 -rwxr-xr-x   1 root     root      68256 May  4 07:48 /var/www/BBC/
hacked2z.png
783838    4 drwxr-xr-x   2 snmp     snmp       4096 May  4 08:03 /var/lib/snmp
786322    4 -rw-------   1 snmp     snmp       1073 May  4 08:03 /var/lib/snmp
/snmpd.conf
782033    4 drwxr-xr-x   2 root     root       4096 May  4 08:03 /var/lib/uran
dom
781846    4 -rw-------   1 root     root       4096 May  4 08:03 /var/lib/uran
dom/random-seed
783486    4 drwxr-xr-x   2 root     root       4096 May  4 07:40 /var/lib/upda
te-manager
781920    0 -rw-r--r--   1 root     root          0 May  4 07:40 /var/lib/upda
te-notifier/release-upgrade-available
781917    0 -rw-r--r--   1 root     root          0 May  4 08:03 /var/lib/plym
outh/boot-duration
  2859    0 drwxrwxrwt   5 root     root        100 May  4 08:04 /var/lock
  4711    0 drwxr-xr-x   2 root     root         60 May  4 08:04 /var/lock/sub
sys
  4712    0 -rw-r--r--   1 root     root          0 May  4 08:04 /var/lock/sub
sys/vmware-tools
  4117    0 drwxr-xr-x   2 www-data root         40 May  4 08:03 /var/lock/apa
che2
  3492    0 drwx------   2 root     root         40 May  4 08:03 /var/lock/lvm
  2848    0 drwxr-xr-x   9 root     root        420 May  4 08:04 /var/run
  4737    4 -rw-r--r--   1 root     root        589 May  4 08:04 /var/run/motd
  4702    4 -rw-r--r--   1 root     root          5 May  4 08:04 /var/run/vmto
blaa
```

Finally the (non)whiteBaord



להרחבה / קישורים נוספים:

Protocol Fuzzing –

Fuzzing בגדול, היא טכניקה אשר הומצאה בכדי לבצע בדיקות על שירותים / אפליקציות בצורה יותר מודרנית. הרי שהיום הקלט העובר אשר משתמש מסויימת פונה לשירות או תוכנה אינו בהכרח תקין או רלוונטי ולפלעמים יכול לפגוע בביצועי השירות. בנוסף לקח בעקבות התפתחות עולם הסייבר, הידע והכלים המסתובבים ברשת, ניתן לשם לב כי קיימות אין ספור שיטות לפריצות אבטחה או הפלת תוכנות / תהליכים / שירותים ע"י הזרקת קוד (לא בהכרח ספציפי ובעל משמעות אלא סתם הצפה או שיבוש) או העמסת בקשות כבדות וכו' ליעד הנתקף. כאשר נתמקד ב Protocol Fuzzing נשם לב כי מדובר בשיטה לשיבוש והפלת שירותי פרוטוקולים על גבי שרתים או מחשבים פרטיים וזאת בעזרת הזרקת קוד "משבש" לשירות הפרוטוקול.

BruteForce –

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

Password Gussing by BrutForce –

ע"י שימוש בשיטת התקיפה BrutForce נוצר כלי לפריצת סיסמאות בצורה ברוטלית. הרעיון הוא להתאים מאגר של סיסמאות / לנחש סיסמאות בהתאם וע"י יכולות ה BrutForce, להציף ולנסות את הסיסמאות הרלוונטיות עד שמתקיימת הצלחה.

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.

ArcSight SEIM by HPE

Zenoss

Vmware vSphare

Checkpoint smartView Tracker

תוכנת בקרת רשת מבית checkpoint המספקת ממשק נוח ויעיל לאיתור אירועים ברשת. התוכנה מספקת כלים מאוד משמעותיים בסינון פעולות אשר מעניין את העוקב. התוכנה בנוסף מציגה לוגים רלוונטים לפעולות ברשת ומנתחת את תעבורת הרשת.