דו"ח מעבדה- תרחיש מס' 6

פרטים:

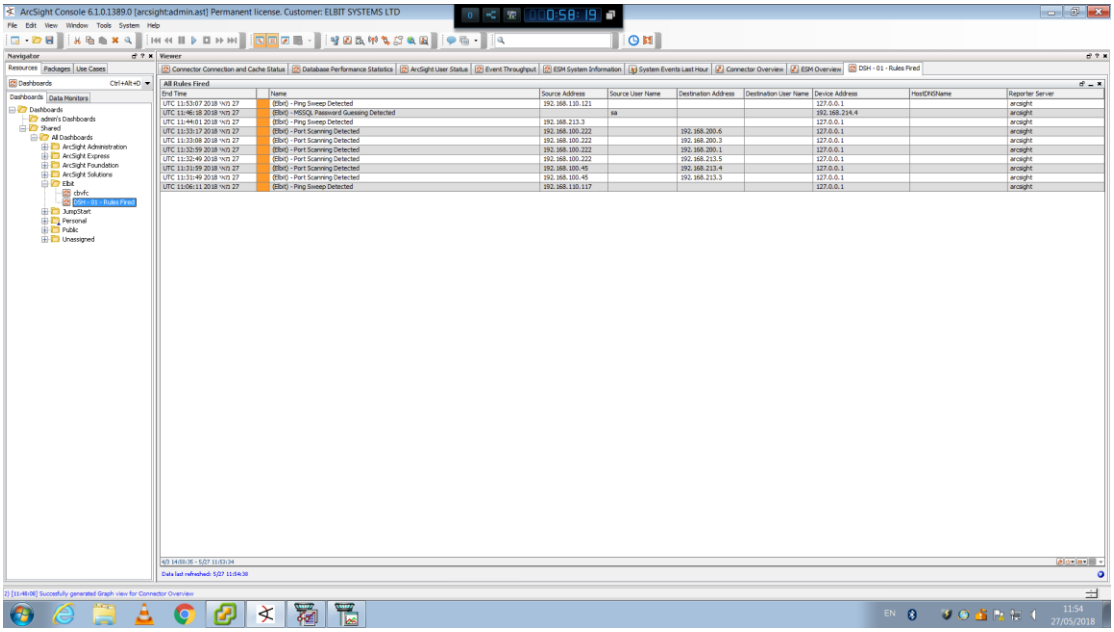
מגיש: שגיא סעדה

תאריך: 27/05/2018

שם התרחיש: תקיפת הארגון באמצעות פרצת אבטחה Backdoor Command Execution בשרת ה- FTP ושאיבת מידע משרת ה- Database שלנו.

תהליך ההתקפה:

בתהליך ההתקפה זוהו התראות ב- ArcSight.



<u>התראה ראשונה – Ping sweep</u>

מה- IP – 192.168.110.117

כתובת זו, נמצאת ב- Subnet של ה- VPN Segment.

התראה שנייה – Port Scanning

מה- IP – 192.168.100.45 ובנוסף, 192.168.100.222

כתובת אלו, נמצאות ב- Subnet של העובדים בארגון אך אינן מוכרות.

סריקת הפורטים בוצעה על השרתים –

CNT-Web-ProFTPd

CNT-WEB-Apache

CNT-DC

CNT-Mail

CNT-Files

התראה שלישית – Ping Sweep

מה- IP – 192.168.213.3

כתובת זו, היא הכתובת של השרת – CNT-Web-ProFTPd

התראה רביעית – MSSQL Password Guessing

עם sa – Source User Name

ו- 192.168.214.4 – IP – Device Address

כתובת זו, היא הכתובת של השרת – CNT-DB-SQL

ולבסוף, התראה חמישית – Ping Sweep

מה- IP – 192.168.110.121

כתובת זו, נמצאת ב- Subnet של ה- VPN Segment.

תהליך ההתקפה בקצרה -

1 – מישהו ביצע Ping Sweep ברשת שלנו.

2 – לאחר מכן, סריקת פורטים מתוך ה- Subnet של העובדים לשרתים בארגון.

3 – מישהו ביצע Ping Sweep מהשרת ProFTPd.

4 – ניסיון לפריצת סיסמא לשרת ה- DB-SQL.

5 – מישהו ביצע Ping Sweep ברשת שלנו.

מכאן, ניתן להסיק להמשך –

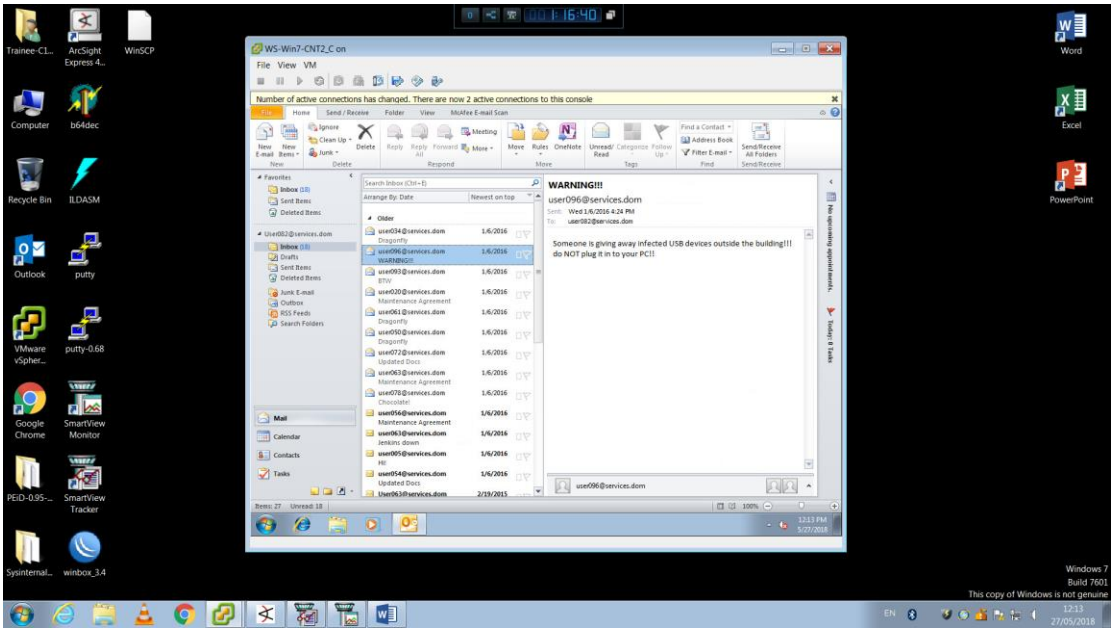
ניסיון לפריצה באמצעות מכונה וירטואלית הנמצאת ב- Subnet של העובדים ולאחר מכן התחברות לשרת ה- ProFTPd (משם היה Ping Sweep) ואז, ניסיון כניסה ל- DB-SQL.

תהליך הזיהוי:

בתהליך הזיהוי, התחברנו לעמדות העובדים מתוך חשד לתקיפה.

ב- 2 עמדות עם מערכת ההפעלה Win ראינו מייל שהתקבל וכתוב בו –

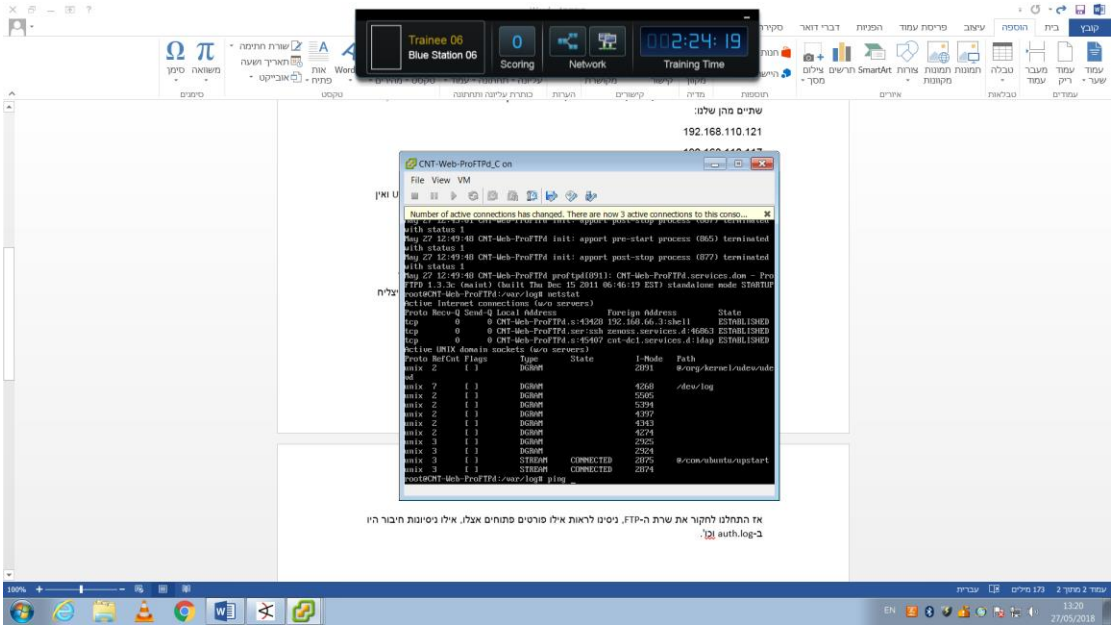
"מישהו נתן התקן USB מחוץ לבניין, אל תחבר אותו למחשב!"



מכאן, נעבור לחקירת העמדות על מנת לבדוק אולי הן חיברו התקן USB ונפגעו מהתקפה.

אך לא מצאנו מידע שיכול לעזור לנו.

לאחר מכן, התחלנו לחקור את שרת ה- ProFTPd, נרצה לראות איזה פורטים פתוחים אצלו, אילו ניסיונות חיבור היו ב- Auth.log וכדומה.



ניתן לראות באמצעות הפקודה Netstat שהשרת- ProFTPd מחובר ל-
Zenoss ו- ArcSight ובנוסף, שרת CNT-DC1.

<u>הסבר על ProFTPd</u> –

שרת FTP, תוכנה חופשית וקוד פתוח, התואמת למערכות דמויי יוניקס ול- Microsoft Windows.
בין שרתי ה- FTP הפופולריים ביותר בסביבות יוניקס היום.
המטרה העיקרית של השרת הוא להעברת קבצים.

<u>פרוטוקול FTP</u> – הוא פרוטוקול תקשורת מבוסס TCP להעברת קבצים בין מחשבים.

באמצעות פרוטוקול זה, תוכנת לקוח FTP מתקשרת עם תוכנת שרת FTP, לשם לקיחת קובץ מהשרת או הוספת קובץ אליו.

מקור - https://he.wikipedia.org/wiki/File_Transfer_Protocol

מכאן, עצרנו לחשוב שוב איך ניתן לבצע Ping Sweep מתוך ה- ProFTPd בלי שראינו חיבור וודאי לשרת.

שאלנו את עצמנו, אם מתחברים לשרת ה- FTP עצמו כ- Client האם ניתן לעשות Ping Sweep? לא.

ה- Client זה בעצם שימוש לקוח בשרת, כלומר – תוכנה שמאפשרת למשתמש בגישת לקוח לעשות מה שרלוונטי ללקוח, וחיבור לשרת כשרת, כלומר – לא לקוח, אפשר לבצע שאילתות כמו Ping ברשת.

שימוש ב- Terminal ככל הנראה על מנת לעשות Ping Sweep.

ולכן, הסקנו שצריכים שליטה מלאה אליו כדי לבצע שאילתות כאלה ברשת.

אך, איך הושגה שליטה על שרת ה- ProFTPd? הוא אומנם כן מאזין על SSH אך לא ראינו חיבור - יש סיכוי שמדובר על Shell כלשהו על השרת.

- אם לא מתאמתים דרך SSH, מישהו פרס Shell, ככל הנראה משתמש שכבר היה ברשת – היה מחובר למערכת.
- Command Injection ב- Web לא רלוונטי למקרה זה.
- SQL Injection – לא רלוונטי למקרה זה.

הפורטים שפתוחים בשרת ה- ProFTPd הם – 21 (FTP) ו- 22 (SSH).

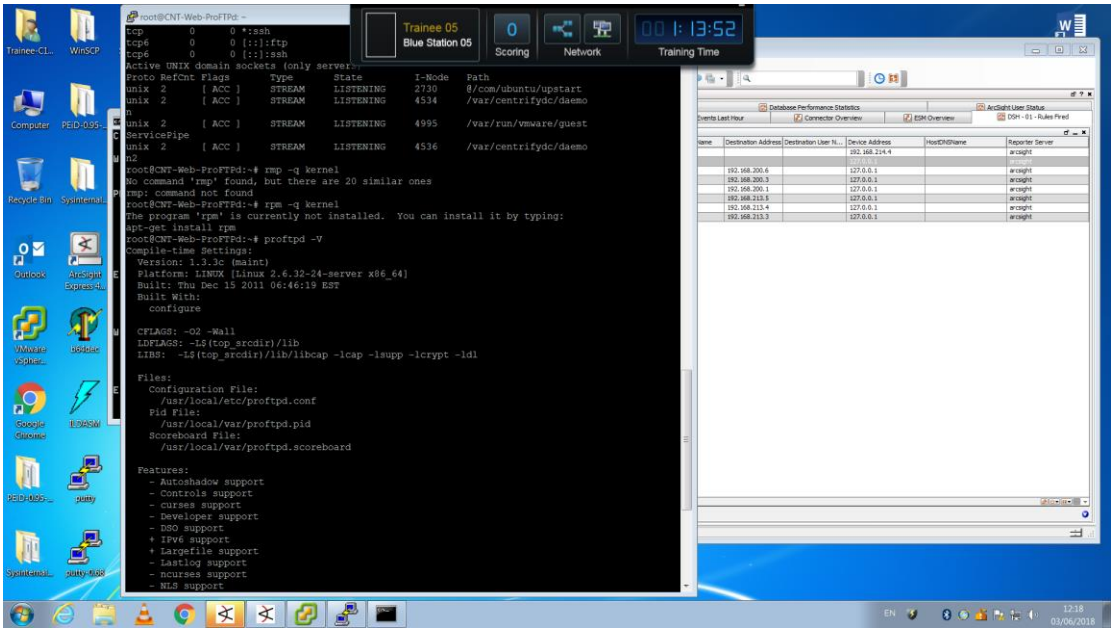
FTP כמו שצוין קודם, זה פרוטוקול ויש הרבה שירותים שמממשים אותו, כמו HTTP.

לאחר שקיבלנו רמז, חיפשנו ב- Google על צירוף של Buffer Overflow עם ProFTPd.

מצאנו שיש פרצת אבטחה בגרסאות 1.3.0/1.3.0a של שרתי ProFTPd.

מכאן, חיפשנו איזה גרסה יש לנו בארגון – ומצאנו שהגרסה שלנו היא 1.3.3c, חיפשנו Exploit שקיים על הגרסה זו וראינו Backdoor Command Execution, באתר Exploit Database.

קישור לאתר - https://www.exploit-db.com/exploits/16921/



עכשיו, הכל ברור יותר – מה שמצאנו בעצם זו פרצת אבטחה המאפשרת הרצה מרוחקת של פקודות על המחשב, דרך Socket.

הסבר על Socket –

Socket הוא נקודת קצה עבור זרם נתונים בתקשורת בין תהליכים על גבי רשת מחשבים.

מקור -
https://he.wikipedia.org/wiki/%D7%A9%D7%A7%D7%A2_(%D7%AA%D7%A7%D7%A9%D7%95%D7%A8%D7%AA_%D7%9E%D7%97%D7%A9%D7%91%D7%99%D7%9D)

Socket מאפשר Remote Command Execution, ולכן מה שקורה זה שבחיבור ה- Socket נשלחות פקודות אל השרת, וה- Buffer שמקבל את הפקודות והמידע, אשר הגודל שלו אינו קבוע, מקבל את המידע וניתן לשלוח מידע גדול וכך ליצור Buffer Overflow על השרת, ולגרום לו להריץ קוד שהשתילו דרך ה- Buffer Overflow הזה.

אז איך ניתן לדעת את ה- Return address מרחוק?

על מנת לדעת לתקוף מרחוק – לעיתים זה תלוי בגרסת מערכת ההפעלה ועדכונים שלה, וכן בשירות שנעשה בו שימוש.
אז תוקפים משתמשים בזה, מתקינים אצלם את הכלי הרצוי ועושים בדיקות על יבש על מנת למצוא את הדרך הטובה ביותר לתקוף ולהצליח בתקיפה. (כך מזהים את הנקודה של ה- Return Address).
מכיוון שהכלי נופל ברגע שיש הרצה מרחוק ודורסים את ה- Return Address, חשוב בתור תוקף לבצע ניסיונות אלו.
בנוסף, נהוג לדמות את המצב של הרשת במדויק על מנת לוודא שהדרך אכן עובדת.

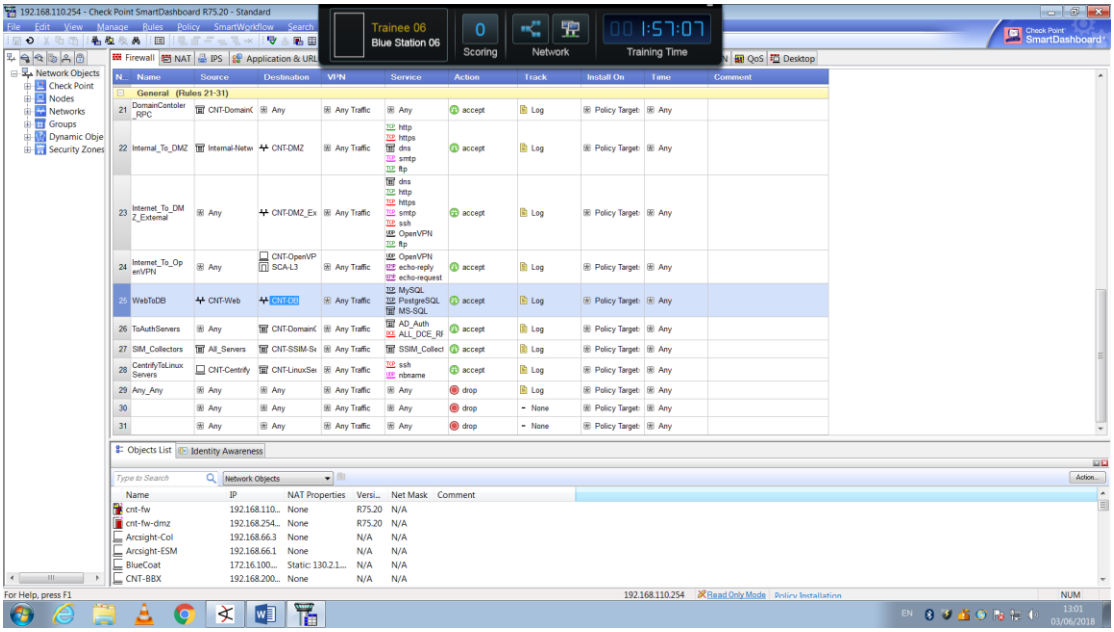
בגלל שראינו שהקוד הזה קיים באינטרנט כנראה שזה עובד, וכבר מישהו עשה את כל העבודה הזו.

ה- Remote Command Execution קורה דרך פורט 21, אז הייתה פתיחת קשר מול ה- ProFTPd כדי לבדוק מהי גרסאת ה- ProFTPd וכך התוקף השיג מידע על הכלי ויודע בדיוק איך לתקוף. (פתיחת ה- Socket מאפשרת הרצת פקודות מרחוק, באמצעות Shell).

התוקף מקבל את ההרשאות של מי שהריץ את השירות.
כלומר, ה- Owner של ה- Service, מי שהפעיל את התוכנה שדרכה התוקף מבצע את התקיפה.

מכאן, נרצה לבדוק איך התקשורת בדיוק עוברת, ומדוע התוקף לא הלך ישירות לשירותי ה- DB מסגמנט העובדים – אימות דרכי הפעולה של התוקף.
לשם כך נצטרך לבדוק את החוקים ב- Firewall ולהכיר לעומק את מבנה הארגון שלנו.

<u>הסבר על ה- Firewall –</u>
ראינו ברשימת החוקים של ה- Firewall שאין חוק שמאפשר תקשורת מהסגמנט של המשתמשים לסגמנט של ה- DB.
אך כן יש חוק שמאפשר תקשורת בין ה- CNT-DB ל- CNT-Web.

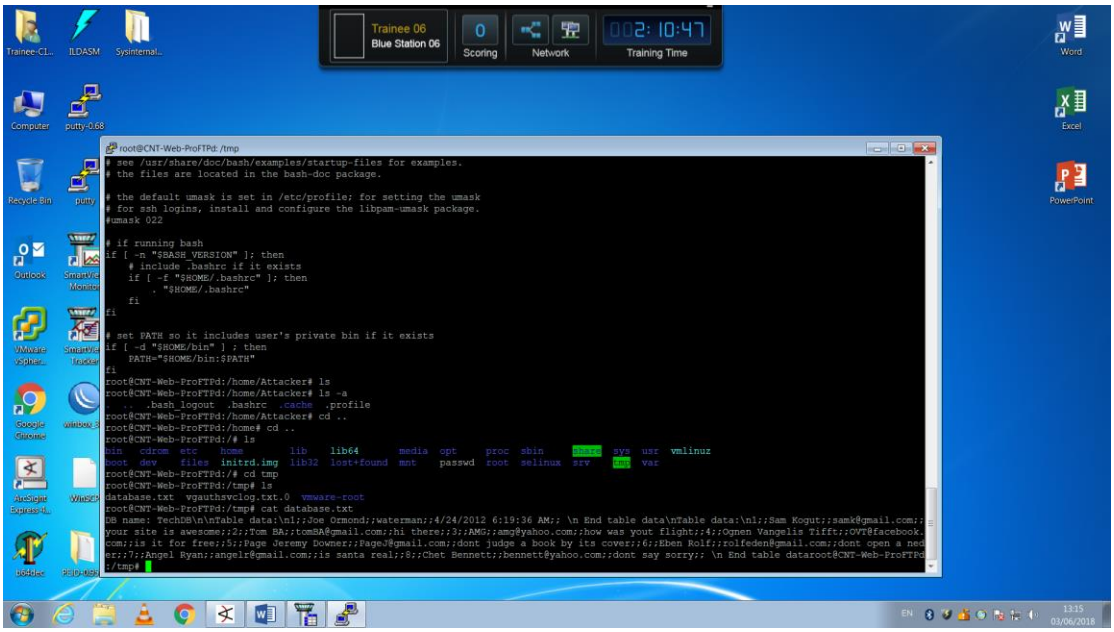


בהנחה שהתוקף מחפש את ה- DB בארגון, הוא מנסה לגשת דרך ה- User Segment, לבצע Port Scanning ולמצוא איזשהו קשר בפורט המתאים.
ברגע שהוא לא מצליח למצוא, הוא ניגש לסגמנטים אחרים שקיימים ברשת ומסתכל עליהם.
כך בעצם מצא את ה- Web Segment ואת שרת ה- FTP.
משם הוא מבצע Ping Sweep וכך מוצא את כל מי שכן יש לו גישה ל- DB, כך מוצא את סגמנט ה- DB ומבצע לשם ניחוש סיסמאות.

לאחר מכן, נחקור את אירוע ה- Password Guessing שהופיע לנו ב- ArcSight ואנו רואים שאין Source IP ו- Destination IP, אך יש Device Address והוא של השרת CNT-DB- SQL.

לכן, התחברנו בהתחלה לשרת ProFTPd דרך Putty באמצעות SSH, והתחלנו לחקור את השרת.

נכנסו לתיקייה tmp וראינו שם קובץ בשם Databases.txt.



כפי שניתן לראות, יש שם מידע כלשהו שככל הנראה התוקף שם בקובץ Text ודרכו הוא רוצה לשאוב מידע משרת ה- DB-SQL.

התוקף מנסה לתקשר עם מערכת DB-SQL דרך מערכת של לינוקס ב ProFTPd.

אך, DB-SQL זה של Windows.

הסבר על DB-SQL –

Microsoft SQL Server – מערכת לניהול בסיס נתונים במודל היחסי של חברת מיקרוסופט.

שפת הפיתוח שבאמצעותה מועברות הפקודות למערכת היא Transact-SQL שהיא מימוש תקן ANSI של שפת SQL משמשת לתשאול וטיפול בנתונים, יצירת טבלאות והיחסים ביניהן ותחזוקת המערכת תוך שימוש בתוכניות שירות שונות.

מקור - https://he.wikipedia.org/wiki/Microsoft_SQL_Server

מסקנות –

התוקף מנסה להשיג מידע מה- DB-SQL אשר נמצא על מערכת Windows אך אין באפשרותו לתקשר ישירות משרת ה- ProFTPd אשר נמצא על מערכת Linux לכן, אנו יודעים שלתוקף הייתה גישה גם לעמדות של העובדים – User Segment, ושם יש לנו מערכות Windows ולכן עמדות קצה יכולות לדבר באותה שפה עם שרת ה – DB-SQL אך אין לו הרשאות, ולשרת ProFTPd יש את ההרשאות הנדרשות.

מכאן, ב- User Segment התוקף פתח לקוח של SQL וכתב שם את הבקשה, מעביר ל- ProFTPd וה- ProFTPd מעביר ל- DB-SQL עם ההרשאות הרלוונטיות.

תהליך זה נקרא SSH Tunneling –

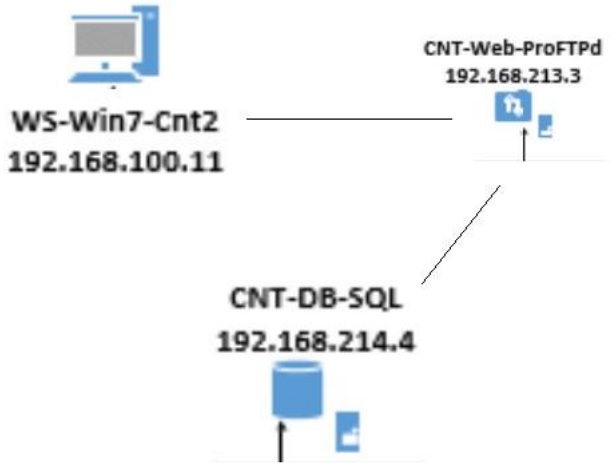
מנהרת SSH היא תעלה מוצפנת הנוצרת על ידי פרוטוקול SSH בה מוכמס פרוטוקול אחר, לרוב פרוטוקול שאיננו מוצפן.

לדוגמא, מחשבים מרוחקים המשתפים קבצים באמצעות פרוטוקול SMB דרך רשת לא מאובטחת, נדרשים להצפין את תעבורת פרוטוקול ה- SMB בחלק הלא מאובטח של הנתיב בו עוברים הנתונים.

פרוטוקול SSH מאפשר יצירת תעלה מוצפנת שכזו, דרכה מועברות הודעות SMB.

בהנחה שרשת המקור והיעד מאובטחות, מושגת בכך אבטחה מלאה של כל חלקי הרשת בהם מתבצע שיתוף הקבצים ללא כל שינוי במימוש פרוטוקול SMB.

מקור - https://he.wikipedia.org/wiki/%D7%9E%D7%A0%D7%94%D7%95%D7%A8_(%D7%AA%D7%A7%D7%A9%D7%95%D7%A8%D7%AA_%D7%A0%D7%AA%D7%95%D7%A0%D7%99%D7%9D)



במקרה שלנו, כפי שניתן לראות –

התוקף משתמש ב- Win7-Cnt2 על מנת לתקשר עם שרת ה- DB-SQL דרך ProFTPd.

תהליך זה מתבצע על פורט 21, פורט זה נותן אפשרות לדבר בתוך הרשת, באמצעות שרת ה- ProFTPd דרך שינוי מקדים של התוקף.

התוקף הפיל את שירות ה- FTP שהיה בפורט 21 והחליף אותו ל- SSH.

יש הסוואה של תעבורה שמתאימה ל- DB-SQL, על פורט 21 וכך ה- Firewall מאפשר את התעבורה כי הוא לא בודק את תוכן התעבורה אלא רק את נתוני המסגרת, כלומר, בודק את ה- Headers עד השכבה הרביעית (TCP/IP) ולכן אינו יודע שברמת ה- Application יש לנו תעבורה של SQL. (ה- Firewall מאפשר שימוש בפורט 21 בין סגמנט העובדים ל- ProFTPd).

זו חולשה של ה- Firewall – פירוט בתהליך הגנה מונעת.

תהליך הגנה:

התהליך ההגנה, הבנו שאכן שרת ה- DB-SQL נפגע ונשאב ממנו מידע דרך שרת ה- ProFTPd באמצעות עמדת עובד- Win7-Cnt2.

לכן נצטרך לנתק את החיבור של התוקף באמצעות ניתוק של המשתמשים שמחוברים ל- ProFTPd ותיקון בעיות בפרצות האבטחה בארגון.

תהליך הגנה מונעת:

1- תדרוך העובדים בארגון – לעשות מדי פעם תרחישי תקיפה ולראות איך יגיבו העובדים ומשם להסיק מסקנות שיעזרו בהמשך (כמובן, אזהרות מפני מתקפות מסוג זה).
2- יש לשמור על מערכת הפעלה, תוכנות ואפליקציות מעודכנות – ישנם פרצות אבטחה ידועות במוצרי תוכנה ומצליחים באמצעותם לחדור למחשבים בקלות.
כאשר מתגלה פרצה בתוכנה כלשהי, לרוב היצרן דואג להפיץ תיקון (באמצעות עדכון), אך כל עוד התוכנה המותקנת במחשב לא עודכנה, הפרצה עדיין קיימת.
במקרה שלנו, שרת ה- ProFTPd לא היה מעודכן ולכן פרצת האבטחה הייתה קיימת.
3- חוק שימנע קבלת IP חדש בארגון, זאת אומרת, התוקף קיבל כתובת IP כאשר הצליח לחדור לסגמנט העובדים – מה שנתן לו להיות חופשי ברשת הארגון ולסרוק אותה.
4- חולשת ה- Firewall –
יש Firewalls שהם New Generation / Deep pattern inception שיודעים להשוות את תוכן החבילה אל נתוני המסגרת שלה, וכך דברים כאלה נמנעים.
חשוב לשים לב שאמנם זה מעולה, אך נמנעים לעיתים להשתמש בהם בגלל שזה מאט את התעבורה וגם יקר יותר.
נשים לב שבכל רשת צריך לאזן בין נוחות המשתמש לבין הגנת הרשת.
פתיחה עד רמה שביעית ובדיקות, יצור צוואר בקבוק באזור ה- Firewall ברשת ועלול לעקב את התעבורה.
5- התקנת אנטי וירוס הסורק את תוכן ההתקנים החיצוניים שמתחברים למחשב וחסימתם במידת הצורך.

הפרצות באבטחת הארגון:

ראה סעיף "תהליך הגנה מונעת" ובנוסף,

פרצת האבטחה בשרת ProFTPd 1.3.3c –

קיימת פרצת אבטחה של – Backdoor Command Execution (Metasploit) בשרת.

מקור - https://www.exploit-db.com/exploits/16921/

כלים שפיתחנו

אין ברשותנו כרגע את הידע לפתח כלים.

אופן עבודת הצוות

בתרחיש זה, מתן ניהל את האירוע.

כיוון שההתראות שקיבלנו היו רבות, התחלקנו למשימות שונות.

חקירת עמדות העובדים, חקירת שרת ה- ProFTPd, חקירת שרת ה- DB-SQL.

בנוסף, בעזרת חיפושים ב- Google מצאנו את פרצת האבטחה של ProFTPd 1.3.3c.

חוסרים/קשיים

-