**פרויקט סיום קורס מגן**

|  |  |
| --- | --- |
| מגיש | ירון קרן |
| תאריך | 29.09.2020 |
| מטרת המסמך | המסמך מלווה למעבדה המציגה תרחיש תקיפה מסוג MITM (Men in the middle) במערכת פנים ארגונית.  ההתקפה במעבדה זו תתבצע על ידי גניבת זהות הלקוח ( CLIENT) באיזור ה,LEN אזור המוגדר למשתמשי הקצה בארגון, וגניבת זהות ה- Firewall Gateway שמבצע מעבר לאפליקציית ה- WEB שמותקנת על Web Application Server באזור הSERVERS , אזור המוגדר לשרתי האפליקציה והDB בארגון.  גניבת הזהויות תביא למעבר התקשורת דרך שרת התוקף (Attcker) שיוכל לנצל זאת לטובתו. |
| מבנה המסמך | * אופן תקיפה מסוג MITM בעזרת ARP Spoofing * הגדרת הרכיבים להקמת המעבדה ותפקידם בתרחיש * שרטוט טופולוגית הרשת לביצוע התרחיש * הגדרת שלבים בתקיפה (הסבר כללי) |

**אופן תקיפה מסוג MITM בעזרת ARP Spoofing**

תקשורת בשכבה 2

תקשורת בין מחשבים ורכיבי התקשורת ברשת התקשורת המקומית ,LAN, מתבצעת בשכבה 2, שכבת ה-DATA LINK.שכבה זו עוסקת באופן מעבר הנתונים ברשת הפנימית ומבצעת זאת על ידי איתור מחשב היעד על פי הכתובת הפיזית שלו ,כתובת הMAC ( Media Access Control) ומטפלת ברמת הFRAME בה נארז המידע עם הכתובות הפיזיות של המקור והיעד.

ARP

על מנת לבצע תקשורת ברמה זו, רכיבי התקשורת (שרתים, תחנות קצה, מתגים..) מנהלים את המידע על כתובות רכיבי התקשורת האחרים באותה הרשת בטבלה ייעודית, טבלתARP Address Resolution Protocol)) ,המכילה את הקשר בין כתובות הIP לכתובות הMAC.

במידה רכיב המקור אינו יודע את כתובת ה MAC של רכיב היעד, הוא משתמש בפרוטוקול הנקרא ARP כדי לגלות את כתובת ה MAC של רכיב היעד באותה רשת מקומית.

ARP מתבצע בשלושה שלבים:

1. הרכיב המבקש שולח הודעה מסוג ה BROADCASTהמכילה את כתובת ה- IP של היעד.
2. כל רכיב ברשת המקבל את שידור ה- BROADCAST משווה את כתובת ה- IP שנשלחה בהודעה, עם כתובת ה-IP של עצמו.

הרכיב בעל הכתובת הזהה, שולח הודעה מסוג Unicast בה כתובת ה MAC שלו בחזרה לשולח המקורי.

1. הרכיב המבקש מקבל את ההודעה ושומר את כתובת ה- MAC וכתובת ה- IP בטבלה הנקראת:ARP Table.
2. כעת יש ל הרכיב המבקש את כתובת ה- MAC בטבלת ה- ARP והוא יכול לתקשר עם היעד

MITM בעזרת ARP Spoofing

בתקיפה מסוג זה התוקף יבצע התחזות מול רכיב המקור ורכיב היעד כך שהתקשורת בין שני הצדדים תעבור דרכו ללא ידיעתם. התוקף "יציג" את עצמו מול רכיב המקור ככתובת היעד (כתובת הMAC שלו) , ומול רכיב היעד ככתובת המקור (כתובת הMAC שלו). הדבר יבוצע ע"י שליחת פקטות ARP אל שני רכיבים אלו.התוקף משייך את כתובת הMAC שלו למול היעד ככתובת הIP של המקור ומשייך את כתובת הMAC שלו למול המקור ככתובת הIP של היעד ובכך מבצע שינוי בטבלת הARP של כל אחד מהרכיבים.

על מנת שמעבר התקשורת תהיה דרכו ללא ידיעת המקור והיעד ,התוקף צריך להוות ראוטר בין הרכיבים ולבצע העברה של הפקטות ביניהם.

לאחר שתהליך זה מתבצע התוקף יכול להאזין ל"שיחה" בין שני הרכיבים ובמידה והיא לא מוצפנת יכול למעשה לקרוא את המידע ולבצע בו שימוש לטובתו.

**שרטוט טופולוגית הרשת לביצוע התרחיש**

SRV 10.10.1.1

LEN 10.10.0.1

FIREWALL

IP 10.10.0.10

SM 255.255.255.0

GW 10.10.0.1

IP 10.10.0.20

SM 255.255.255.0

GW 10.10.0.1

ATTACKER

CLIENT

IP 10.10.1.20

SM 255.255.255.0

GW 10.10.1.1

WEB APP SERVER

בתרחיש זה מחשב הCLIENT שנמצא באיזור הLAN מבצע התקשרות אל שרת ה -WEB APPLICATION SERVER שנמצא באיזור אחר ברשת (איזור SERVERS) דרך רכיב FIREWALL לביצוע כניסה לאתר ה- WEB דרך מסך LOGIN ייעודי בו הCLIENT מקיש את שם המשתמש והסיסמא שלו.

התקשורת בין הרכיבים הינה HTTP כלומר אינה מוצפנת והמידע מועבר ב Clear text - בין שני הרכיבים.

מחשב הATTACKER יבצע מניפולציה על טבלת הARP של מחשב הCLIENT ושל שרת ה FIREWALL ויגרום לכך שמחשב הCLIENT ישייך את כתובת הMAC של מחשב הATTACKER לכתובת ה-IP של רגל הLAN- של שרת ה, FIREWALL ושרת ה FIREWALL ישייך את כתובת הMAC של מחשב הATTACKER לכתובת הIP של מחשב הCLIENT.

בצורה זו ה"שיחה" בין הCLIENT לבין ה- FIREWALL תעבור דרך מחשב ה-ATTACKER שיאזין לשיחה בעזרת WIREshark ,יחלץ את שם המשתמש והסיסמא של הCLIENT לאתר ה- WEB ויוכל להתחזות אליו.

**הגדרת הרכיבים להקמת המעבדה ותפקידם בתרחיש**

התרחיש מתבצע בסביבת העבודה ORACLE VM VIRTUAL BOX MANAGER כאשר כל רכיב במערכת ניתן להעלות למעבדה זו מקובץ OVA ייעודי באמצעות פעולת IMPORT.

להלן רכיבי המעבדה:

1. : **LAB-Pfsense**

שרת FIREWALL מסוג PFSENSE שאליו מוגדרים שלושת הרגלים הבאות :

1. רגל הWEN- ,בעלת כתובת דינמית, לניהול ממשק משתמש ל FIREWALL כאשר שם המשתמש הינו admin והסיסמא pfsense.
2. רגל ה-LAN ,בעלת כתובת קבועה (10.10.0.1), לניהול העברת/חסימת המידע מרשת הLAN לרשתות האחרות.
3. רגל ה-SRV ,בעלת כתובת קבועה (10.10.1.1), לניהול העברת/חסימת המידע מרשת הSRV לרשתות האחרות.

על לאפשר את התקשורת בין הרכיבים הוגדרו ב LAB-Pfsense החוקים הבאים :

(1) WAN - פתיחת תקשורת בפורט 443 HTTPS

(2) WAN - פתיחת תקשורת בפורט 22 SSH

(3) LAN - פתיחת תקשורת מרשת הLAN בפורט 80 HTTP לכיוון שרת ה WAB APPLICATION SERVER שנמצא באיזור הSERVERS (SRV)

**להקמת רכיב זה על יש לייבא את קובץ LAB - PFSENSE.ova**

1. **LAB-WEB Server:**

שרת לינוקס עליו הוגדרו התוכנת הבאות:

1. Ubuntu 64bit
2. MYsql DB
3. Apache2
4. Wordpress

לאחר התקנת התוכנות הרלוונטיות הוגדרו ברמה האפליקטיבית הרכיבים הבאים:

1. הגדרת דף LOGIN – בוצע במהלך ההתקנה
2. הגדרת משתמש אדמיניסטרטור, שם משתמש וסיסמא– בוצע במהלך ההתקנה

(3)הגדרת מיפוי REDIRECT לדפי האפליקציה בDB האפליקטיבי בעזרת הפקודות הבאות:

(1) sudo mysql

(2) use wordpress;

(3)Update wp\_options

SET option\_value =" <http://10.10.1.20> "

Where option\_value =" <http://127.0.0.1> "

(4) exit

השרת הוגדר באיזור הSRV בכתובת 10.10.1.20

**להקמת רכיב זה על יש לייבא את קובץ LAB – WEB Server.ova**

1. **LAB- Client:**

שרת לינוקס עליו הוגדרו התוכנת הבאות:

)1) Debian 64bit

(2) KALI

- חיבור לאפליקציה יבוצע באמצעות תוכנת FIREFOX

- השרת הוגדר באזור הLAN בכתובת 10.10.0.10

**להקמת רכיב זה על יש לייבא את קובץ LAB – Client.ova**

1. **LAB-Attacker:**

שרת לינוקס עליו הוגדרו התוכנת הבאות:

)1) Debian 64bit

(2) KALI

- הרצת הפקודות לביצוע התרחיש יבוצע בעזרת שלושה מסכי TERMINAL

- קריאה וניתוח התקשורת בין הClient ל- APPLICATION SERVER יבוצע בעזרת תוכנת WIRESHARK

- חיבור לאפליקציה יבוצע באמצעות תוכנת FIREFOX

השרת הוגדר באיזור הLAN בכתובת 10.10.0.20

**להקמת רכיב זה על יש לייבא את קובץ LAB – Attacker.ova**

**יישום MITM**

להלן סדרת הפעולות לביצוע תקיפת MITM על פי השלבים הבאים:

**שלב 1:**

מחשב הPFSENSE

1. נבצע העלאה של שרת LAB-Pfsense

המקשר בין רשת ה- LEN לרשת ה SERVERS -(SRV)

**שלב 2:**

מחשב הWEB:

1. העלאה של שרת LAB-WEB SERVER

יש להמתין מספר דקות עד לעליית השרת.

User: eliot

Password: 159357

1. בדיקת כתובת השרת 10.10.1.20

ע"י הפקודה ifconfig ב- TERMINAL

במידה ולא מקבלים את הכתובת מבוקשת יש להקיש את הפקודה הבאה ולבדוק שוב

sudo service networking restart

1. נבצע בדיקת עליית מסך LOGIN דרך ה Firefox

<http://10.10.1.20/wp-admin>

**שלב 3:**

מחשב התוקף LAB-Attacker:

1. העלאה של שרת LAB-Attacker

User: eliot

Password: kingartur

1. נפתח מסך Terminalונפעיל את יכולת העברת הפאקטות (כלומר המחשב יהיה מעין ראוטר)לשם כך נשתמש בפקודה הבאה (במצב SUDO):

**sysctl -w net.ipv4.ip\_forward=1**

1. נפתח מסך Terminalנוסף ונבצע arpspoofing ונייצר העברת פאקטות מקורבן (10.10.0.10) אל הרגל הPFSENSE דרך מחשב התוקף על ידי שימוש בפקודה הבאה

**arpspoof –i eth0 –t 10.10.0.10 10.10.0.1**

בעזרת פקודה זו אנו מבצעים מניפולציה על מחשב הקורבן ומשנים את טבלת הARP אצלו כך שלכתובת הpfsense (רגל הLEN ) אנו משייכים את כתובת הMAC של התוקף.

1. נפתח מסך Terminalשלישי ונבצע arpspoofing ונייצר העברת פאקטות מרגל הPFSENSE אל הקורבן (10.10.0.10) דרך מחשב התוקף על ידי שימוש בפקודה הבאה

**arpspoof -i eth0 -t 10.10.0.1 10.10.0.10**

בעזרת פקודה זו אנו מבצעים מניפולציה על מחשב הpfsense ומשנים את טבלת הARP אצלו כך שלכתובת הCLIENT (10.10.0.10) אנו משייכים את כתובת הMAC של התוקף.

1. נפעיל את ה- WIREshark במחשב כאשר הוא מאזין על eth0
2. ניישם פילטר על בקשות HTTP בלבד

**שלב 4:**

מחשב הקורבן LAB-Client:

1. נגלוש אל אתר שאינו מאובטח (כלומר, HTTP בלבד) דרך תוכנת הfirefox

<http://10.10.1.20/wp-admin>

1. נבצע התחברות עם יוזר וסיסמה

User : eliot

Password : 159357

1. נגלוש באתר כרגיל

**שלב 5:**

מחשב התוקף LAB-Attacker:

1. לאחר סקירת הפאקטות ב- WIREshark נחלץ את כתובת האתר, היוזר והסיסמה.
2. מכאן התוקף יכול להתחבר לאתר ולהתחזות לClient

<http://10.10.1.20/wp-admin>

1. נבצע התחברות ממחשב התוקף עם יוזר וסיסמה של הCLIENT

User : eliot

Password : 159357