הגנה ברשתות 236350 אביב תשפ"ג

גיליון מספר 1

שם המגיש: עומר גרייף

ת"ז : 2082000154

תאריך הגשה: 16/4/23

שאלה 1 – סריקת פורטים

1. **הפקודה המלאה שהרצתי על מנת לעמוד בתנאים המבוקשים –**

sudo nmap -sS -T4 -A --allports scanme.nmap.org

2. **כתובת IP של scanme.nmap.org :**

45.33.32.156

3. **פורטים פתוחים**:

Port: 22 Service: SSH
Port: 80 Service: HTTP
Port: 9929 Service: NPING-ECHO
Port: 31337 Service: TCPWRAPPED

4. **תוכנה וגרסה:**

בד"כ שרת רץ מעל פורט 80 ולכן => Apache httpd 2.4.7 ((Ubuntu)) <= תוכנה: Apache
גרסה: 2.4.7

5. **דגל לאפשור "-A traceroute. ו OS detection, version detection, script scanning":**

דגל זה מבקש גישה למידע שעשוי לעזור לתוקף אח יד עם זאת מדובר במידע שלא בהכרח חיוני לתקשורת סטנדרטית של שני פורטים ועל כן המערכת המותקפת עשויה לזהות כך את כוונת התקיפה ולהגן מבעוד מועד.

6. **השפעות הדגלים**:

<= OS detection

" Aggressive OS guesses: OpenWrt 12.09-rc1 Attitude Adjustment (Linux 3.3 - 3.7) (90%), HP P2000 G3 NAS device (89%), Linux 2.6.32 (89%), Linux 2.6.32 - 3.1 (89%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (89%), Linux 3.7 (89%), Ubiquiti Pico Station WAP (AirOS 5.2.6) (88%), Linux 2.6.32 - 3.13 (88%), Linux 3.0 - 3.2 (88%), Linux 3.3 " (88%)

ייתכנות לשימוש שרת היעד בכל אחת מגרסאות מערכת ההפעלה הכתובות לעיל

<= Traceroute

TRACEROUTE (using port 5900/tcp)

HOP RTT ADDRESS

1 3.02 ms OpenWrt.lan (192.168.1.1)

משמעותו הצגת מידע על תנועת החבילות, ניתן לראות כי ההופ הראשון הוא OpenWrt.lan , IP 192.168.1.1 והRTT שלו הוא 3.02ms.

7. **פורט סגור:**

פורט סגור הוא פורט שלא מאפשר חיבור פתוח אליו, כלומר לא מאזין לבקשות של שרתים אחרים אך עדיין הוא קיים במערכת. חבילת TCP שתשלח בתגובה מהשרת לSYN תכיל דגל RST שמודיע שהתקשורת נכשלה.

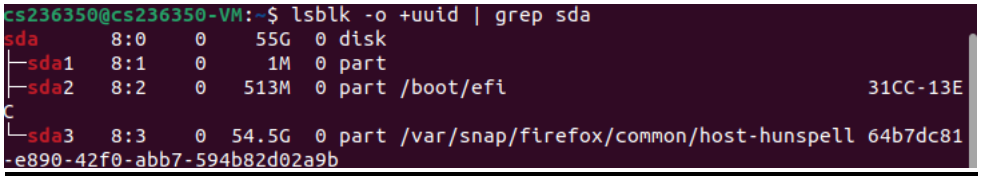
8. **פורט "filtered":**

פורט פילטרד הוא פורט שלא מצליח לענות לSYN עקב חסימה של חומת אש, סינון או כל השפעת תקשורת כלשהיא. כלומר כתגובה לSYN לא תתקבל תשובה לשולח.

9. **בקשות HTTP נוספות:**

OPTIONS , POST , PROPFIND

10. **צירוף תצלום ומוקלד:**




```
sda       8:0    0    55G  0 disk
├sda1     8:1    0     1M  0 part
├sda2     8:2    0   513M  0 part /boot/efi
31CC-13EC
└sda3     8:3    0  54.5G  0 part /var/snap/firefox/common/host-
hunspell 64b7dc81-e890-42f0-abb7-594b82d02a9b
```

שאלה 2 – הנדסה חברתית

1. **יישום בחיי היום יום להנדסה חברתית –** למשל בסופר, ניתן להבחין כי בסמוך לקופה נמצאים שוקולדים וממתקים שנועדו לנצל את העובדה שהלקוח עשוי לקבל החלטה חפוזה ולהוסיף לסל הקניות שלו מוצר שבחירתו מונעת מאימפולסיביות. כך הסופר מנצל את החולשה שלנו ומאפשר לעצמו למכור עוד מוצרים "ברגע האחרון".

2. **הנדסה חברתית בהקשר אבטחת מחשבים -** הנדסה חברתית בהיבט אבטחת מחשבים היא ניצול חולשות האדם על מנת לאפשר גישה למידע \ הכנסת וירוס שהתוקף מעוניין בו. התקיפה בעיקרה תהא מבוססת על הונאה ושכנוע של המותקף שתוביל בסופו של דבר "להפיל בפח" את המותקף ולקבל את המידע הרצוי / להכניס את הוירוס.

3. **ILOVEYOU – איך עובד , ייעלותה , הגנה של ממשלות בעקבותיה –** הפצת מייל שניצלה פרצת אבטחה מוכרת אך עיקרה וחידושה היה השימוש בהנדסה חברתית באמצעות תקשורת מרוחקת. המייל שהמותקף קיבל הכיל קובץ שנקרא ILOVEYOU שנשלח "לכאורה" ממכר של המותקף. הקובץ למעשה היווה את הוירוס והשילוב של מייל ממכר של המותקף יחד עם חיבור ריגשי של המילים ILOVEYOU ניצל את התורפה הרגשית של המותקפים ועל כן היווה יעילות משמעותית. נתן תחושה של אמינות בשילוב עניין וסקרנות של המותקף לפתוח את הקובץ שקיבל במייל. הממשלות נאלצו להשבית את מערכות הדואר שלהן על מנת למנוע את קריסתן.

4. **ההתקפה שהובילה לקבלת המידע של פריס הילטון –** ההתקפה התבססה על באג של חברת טי מוביל שאפשרה להתחבר לרשת הפנימית שלהם מרחוק באמצעות סיסמא ומשתמש שיש בידי עובדים בחברה. ההאקר הבינו כי אנשי המכירות בחברה מהווים נקודת חולשה מכיוון שלרב הם ללא רקע טכני וחושדים בדברים מסוג זה ובנוסף הם אנשים חביבים שמטרתם לעזור ללקוחות. ההאקר התקשר למוקד והציג את עצמו כטכנאי, יצר קשר עם איש המכירות ונתן לו תחושה שהוא אכן טכנאי וכך על ידי התחזות מוצלחת השיג את פרטי המשתמש וכך הצליחו להיכנס למערכת של טי מובייל, הנדסה חברתית במיטבה.

5. **הטעות של פריס הילטון איך ניתן למנוע –** כדי שההאקר יוכל להכנס לממידע של פריס הילטון הוא נדרש להכניס את הסמא שלה או לענות על שאלת שחזור. השאלה שפריס הילטון בחרה הייתה "מה שמה של חיית המחמד האוהבה עליה" ובמקרה בסמיכות לנסיון חדירה לפרטים שלה היא פרסמה שהכלבה שלה אבדה ופרסמה את שמה בציבור כך שגם התוקף הגיע למידע זה. כדי למנוע פריצה זו פריס הילטון הייתה יכולה לבחור שאלה לשחזור שאך ורק היא יודעת את התשובה עליה ולדאוג לא לפרסם זאת באף סיטואציה.

6. **כוחה של הנדסה חברתית בתקשורות דיגיטלית לעומת חיי היום יום –** ראשית העדר ממשק פנים אל פנים של התוקף עם המותקף מקשה באופן משמעותי על זיהוי הונאות. למשל במקרה שלנו אם התוקף היה צריך להגיע באופן פיזי כדי להשיג את הסיסמא הרצויה הוא כנראה היה נכשל שכן במפגש פנים אל פנים היו מצפים ממנו להראות יותר אסמכתאות שהוא אכן טכנאי, מה גם שגילו הצעיר עשוי היה להעלות חשד.

בנוסף בחברות של היום מרבית התקשורת מתבצעת באמצעים דיגיטליים כמעט ללא קשר אישי ישיר, דבר שמקל על התוקף להתחזות לעובד בחברה ולקבל פרטי מידע שהוא לא אמור לקבל כפי שראינו בדוגמה הקודמת.

7. **התקפות phishing והתקפות spear phishing -** התקפות phising הן התקפות מבוססות הנדסה חברתית בהן התוקף שולח מייל/הודעה למותקפים בהם הוא מציע להם שירות, פנייה מעסק/בנק/אוניברסיטה וכו שפונה לקבל רחב יחסית של אנשים על מנת לקבל את פרטים ולנצלם לגישה למידע שלהם. כמו למשל "הנך נדרש לעדכן את פרטי הבנק שלך" "זכית בהגרלה ייחודית וכל שעליך לעשות הוא להכנס לקישור הבא" וכו. או לחילופין יצירת אתרים שנראים זהים לחלוטין לאתרים הרגילים אך בפועל כל המידע באתר מנוהל על ידי התוקף עם כתובת URL מעט שונה מהמקורית שעין לא חדה מספיק עשויה לפספס. כל אלה מנצלים את הקושי של המותקף להבדיל בין הודעת אמת להודעת כזב (פישינג) ועל ידי כך לגזול את המידע של המותקף.
בspear phishing התקיפה מוכוונת כלפי אדם ספציפי ולכן אופי התקיפה יתבסס על תחקיר של התוקף על המותקף והתאמת הודעות פישינג בהתאם לעיסיקו/ אירועים שרלוונטים למותקף.

8. **השיטה המתוארת לגבי גישה לחשבון בנק ללא גילוי של התוקף –** התוקף קונה מבעוד מועד מניות בחברה קטנה וברגע שהוא מצליח להשיג גישה לחשבון בנק של המותקף הוא מבצע העברה בנקאית לחברה שבה הוא קנה את המניות, דבר שגורם לערך המנייה לקפוץ באופן משמעותי וכך התוקף מצליח להרוויח ללא קבלת הכסף של המותקף באופן ישיר וללא השארת עקבות.

9. **יתרונה של תקיפה מבוססת הנדסה חברתית לעומת אחרות (איפה היא מצליחה שאחרות נכשלות) -** כיום יש הרבה מערכות הגנה שמזהות תקיפות ומצליחות להגן על פניהן . יתרונה המשמעותי של תקיפה מבוססת הגנה חברתית היא שהיא מנצלת את חולשת המוח האנושי וכך גם אמצעי הגנה מורכבים עשויים להיות חסרי ערך אם הקורבן נותן מיוזמתו את פרטיו הסודיים ו/או מאפשר גישה של התוקף

10. **דרכים לטיפול בהתקפות מבוססות הנדסה חברתית -** חינוך אנשי החברה למודעות לתקיפות בדגש על נקודות התורפה של ארגונים ותשומת לב והגנה בהם, בקשה של סממני זיהוי שרק עובדי החברה יודעים, מידור של עובדי החברה כך שלא כל עובד חשוף לכל המידע, סינון של ספקיות דואר אלקטרוני שמעבירות באופן אוטומטי לספאם הודעות אשר חשודות בפישינג והכי חשוב - לא לתת סיסמאות דרך הטלפון.