**שאלה 1:**

* **חלק 1:**

תיעוד של ה דגלים שהשתמשנו בהן ב command:

כדי להשתמש בסריקת TCP SYN כפי שנדרש נוסיף את הדגל

וכדי לאפשר את OS detection, version detection, script scanning ו-traceroute נוסיף הדגל:

כדי לבצע סריקה מהירה, נוסיף את הדגל:

כדי לסרוק את כל הפורטים נוסיף את הדגל:

*דגלים אלו מהתיעוד שצורף לתרגיל הבית.*

1. *הפקודה המלאה היא:*

*שהיא מכילה nmap כדי להפעיל אותו, הדגלים אשר הסברנו עליהם ואת שם השרת שרוצים לעשות לו scan שבמקרה שלנו הוא .*

1. *כתובת ה IP של שרת היא: כפי שניתן לראות מפלט nmap.*
2. *נציין בטבלה הבאה את הפורטים הפתוחים והשירות המתאים לכל אחד מהם:*

|  |  |
| --- | --- |
| *Service* | *Port* |
| *Ssh* | *22* |
| *http* | *80* |
| *nping-echo* | *9929* |
| *tcpwrapped* | *31337* |

*בטבלה כתבנו את כל הפורטים הפתוחים, השירות שמספקים והאפליקציה שמשתמשת בו כמו שצריך.*

1. *קודם כל, נציין שבדרך כלל משתמשים בפורט 80 כדי להריץ שרת רשת ונתייחס כאן כאילו זה המקרה. ולפי הפלט של nmap נראה שהתוכנה שרצה היא: Apache httpd עם גרסה 2.4.7*
2. *כפי שציינתי למעלה בהסהבר על הדגלים, דגל זה הוא והחסרון בשימוש בו שהוא מאפשר סריקה אגרסיבית ולכן עלול להיתפס כפולשני על ידי ה system administrator או להפעיל מנגנון אבטחה כלשהו שיקשה על ההתקפה אשר רצינו לבצע, בדרך כלל נעדיף שההתקפה לא תזוהה בשלבים הראשונים ודגל זה עלול לפגוע בזה.*
3. *נציין הפלט כאשר במקום הדגל מריצים עם כל אחד 3 הדגלים המתאימים:*
   1. *Script scanning עם דגל*

*חלק מהפלט המתקבל:*

*|\_http-title: Go ahead and ScanMe!*

*|\_http-favicon: Nmap Project*

*ומשמעותו: שכותרת שרת ה web שרץ על פורט 80 הינו: “Go ahead and ScanMe!” כפי שניתן לראות ואת ה Http-favicon הוא “Nmap Project!” וכמובן מידע זה התקבל לאחר ביצוע script scanning. מידע זה יכול לתת לנו מידע על הסיבה ששרת ה web רץ, במקרה זה ניתן לראות מהשם שזה לצורך ביצוע סריקות לצרכי למידה.*

* 1. *Version detection עם דגל*

*חלק מהפלט המתקבל:*

*PORT STATE SERVICE VERSION*

*22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)*

*80/tcp open http Apache httpd 2.4.7 ((Ubuntu))*

*9929/tcp open nping-echo Nping echo*

*31337/tcp open tcpwrapped*

*Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel*

*Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .*

*ומשמעותו: קיבלנו מידע על הגרסה של השירותים שרצים על הפורטים הפתוחים למשל אפשר לראות זה באופן ברור בשתי השורות הראשונות, וזה עלול לתת לנו מידע על איך אנחנו יכולים לתקיף גרסאות ספציפיות של שירות במקרה והתגלתה חולשה יבור גרסה ישנה שבמקרה רצה בשרת כי עוד לא ביצעו עדכון! נציין שלא כל המידע שמופיע הוא בזכות הדגל הזה אך לצורך נוחות הצגה והבנה של מה מתווסף צירפנו את כל הטבלה.*

* 1. *OS detection עם דגל*

*חלק מהפלט המתקבל:*

*Aggressive OS guesses: Linux 5.0 - 5.4 (96%), Linux 4.15 - 5.8 (94%), Linux 5.0 - 5.5 (93%), Linux 5.1 (93%), Linux 2.6.32 - 3.13 (93%), Linux 5.0 (92%), Linux 2.6.22 - 2.6.36 (92%), Linux 3.10 - 4.11 (92%), Linux 3.10 (91%), Linux 2.6.32 (91%)*

*No exact OS matches for host (test conditions non-ideal).*

*Network Distance: 24 hops*

*OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .*

*ומשמעותו: ש Nmap ניסה לגלות מה מערכת ההפעלה שרצה בשרת שעשינו לו סריקה ולמרות שעשינו ניחוש אגרסיבי, לא התקבל match מדויק למערכת ההפעלה שרצה בשרת אך כן קיבלנו הסתברויות שונות לזה שמערכת ההפעלה היא Linux עם גרסאות שונות. אפשר להבין מזה שאולי בשרת היעד הוא מקונפג בצורה שהוא מנסה להסתיר את מערכת ההפעלה שהוא מריץ.*

* **חלק 2:**

1. המשמעות של פורט סגור בשרת היא שהפורט נגיש אך אין מי שמאזין על הפורט הזה ולכן כאשר מגיעה חבילת SYN לפורט סגור. ובמקרה כזה נשלחת TCP RST Packet כדי לציין שהפורט הינו סגור.
2. המשמעות של פורט שהוא “filtered” בשרת היא שנסיון שלנו לגשת לפורט הזה מסוננת או נזרקת על ידי ה firewall. ובמקרה כזה לא נשלחת חבילה בחזרה כיוון שהחבילה ששלחנו לשרת נזרקת על ידי ה firewall ולכן לא מגיעה לפורט היעד ומזה נובע גם שלא מקבלים תגובה בחזרה.

**שאלה 2:**

1. הנדסה חברתית היא מושג רחב ומתאר שימוש של עקרונות פסיכולוגיים וסוציולוגיים שיהפוך פעולה כלשהיא למתאימה יותר, אחד מהיישומים של הנדסה חברתית בחיי היומיום אפשר לראות אותו כאשר הולכים לעשות קניה בסופר! למשל מוצרי יסוד נמצאים בקצי החנות כך שכדי לקנות אותם נצטרך לעבור את כל החנות ואולי לקנות עוד כמה דברים בדרך. בנוסף לכך ממתקים וקניות מזדמנות יהיו קרובות לקופה כך שלא יהיה לנו זמן להתחרט על האימפולסיביות שלנו כדי שנקנה אותם. מדוגמאות אלו אפשר לראות שבחיי היומיום, הנדסה חברתית משמשת כדי לגרום לנו לבזבז כמה שיותר כסף בסופר.
2. בהקשר של אבטחת מחשבים, הנדסה חברתית היא הדרך שבה תוקף יכול לתמרן, להשפיע ולהטעות אדם שהוא בעל גישה למידע מסווג בחברה, כדי שימסור לידיו מידע שהתוקף מעוניין בו. התוקף עשוי לשלב מגוון של טכניקות הונאה, התחזות ושכנוע כדי להגיע אל המידע האסור.
3. וירוס I Love You הופץ באמצעות הדואר האלקטרוני על ידי ניצול של פרצת אבטחה מוכרת של תוכנת Outlook. הוירוס הדביק אנשים על ידי פרצת אבטחה בשירות הדואר Outlook אשר בעזרת מייל שנשלח למישהו עם הכותרת I Love You וקובץ זדוני שהיה מצורף למייל כך שאחרי שמי שקיבל המייל והיה מספיק סקרן כדי לדעת מה שלח לו האיש שאוהב אותו, פתח את הקובץ המצורף למייל זה ובעצם פעולה זאת הדביקה אותו בוירוס. ואז אחרי ההדבקה, נשלח מייל מהקורבן (על ידי שימוש בפרצת אבטחה) לכל אנשי הקשר שלו עם אותה כותרת וקובץ זדוני. מה שהפך הוירוס לכל כך יעיל היא העובדה שהקורבנות קיבלו מייל ממישהו שהם מכירים עם כותרת I Love You ולכן הם סמכו יותר על תוכן המייל כי הרי הם מכירים השולח וזה נתן להם בטחון בלפתוח את הקובץ, בנוסף לכך היו סקרנים לדעת מה יש בקובץ שנשלח על ידי מישהו שהם חשבו שאוהב אותם. הוירוס הזה היו לו השפעות רחבות מאוד ולכן, כדי להגן על עצמן ממשלות היו צריכים להשבית את מערכות הדואר האלקטרוני שלהן.
4. ההתקפה שהובילה להפצת מידע מהטלפון של פריס הלטון התחילה בהנדסה חברתית של אחד מהעובדים במוקדי השירות של חברת T-Mobile אשר על ידי התחזות להיות איש תמיכה טכנית, התוקף הצליח לקבל את פרטי המשתמש ו הסיסמא של אחד מעובדי החברה בתירוץ שהוא יעזור לו לפתור את בעיית האיטיות באינטרנט אצלו. לאחר קבלת פרטי המשתמש והסיסמא של העובד, לתוקף הייתה גישה אל החשבונות של כל לקוחות T-Mobile. ביום אחד הוא מצא את פרטיה של פריס הלטון אך כדי לגשת למידע על הטלפון של פריס הלטון הוא היה צריך את הסיסמא שלה, ולמרבה מזלו ניתן לשחזר סיסמא במקרה שמישהו שוכח אותה אם הוא יוכל לענות על שאלת אבטחה שהלקוח קבע מראש. ולכן שוב הוא התחזה להיות פריס וביקש לשחזר הסיסמא. כיוון שפריס בחרה בשאלה קלה שהיא: "מה שם חיית המחמד האהובה עליה?" והיא פרסמה לכל העולם על הכלב שלה אז היה קל לתוקף לדעת מה התשובה הנכונה שהיא שם הכלבה של פריס. ומכאן הוא איפס את סיסמת הטלפון ונעל את פריס מחוץ לטלפון "סייד קיק" שלה ויכל לגשת למידע על הטלפון שלה דרך האתר של T-Mobile וכך הוא הצליח להדליף את המידע מהטלפון של פריס הלטון!
5. הטעות של פריס הלטון הייתה שהיא בחרה בשאלת אבטחה אשר תשובתה הייתה מוכרת להרבה אנשים, שהיא בעצם מה שם חיית המחמד האהובה עליה בזמן שהיא פרסמה לכל העולם על הכלב שלה ולכן כאשר התוקף רצה לגשת לחשבון שלה וגילה שזאת היא השאלת אבטחה שלה הוא ידע מה התשובה בקלות בגלל שפריס פרסמה את התשובה בכל מקום אפשרי והיה קל לו לאפס את הסיסמא שלה! כדי למנוע את זה היא יכלה להשתמש בשאלת אבטחה אחרת שתשובתה אינה מוכרת לכל העולם, בעיקר היא הייתה צריכה להימנע מלפרסם דברים שעלולים לגלות את התשובה לשאלת האבטחה שלה.
6. היתרון של הנדסה חברתית בתקשורת דיגיטלית היא שבדרך כלל אנשים שמתקשרים זה עם זה לא מכירים אחד את השני, במיוחד בארגונים גדולים שיש בהם הרבה עובדים ובגלל שהתקשורת היא לא פנים אל פנים אז התוקף יכול לנסות את מזלו שוב ושוב עד שהוא מגיע למישהו שיתן לו את המידע שהוא מחפש. בהתקפה מהסעיפים הקודמים ראינו שהתוקף התקשר לאיש שירות בחברת T-Mobile והתחזה להיות איש תמיכה טכנית בחברה וכיוון שהתקשורת הייתה דיגיטלית, העובד בחברה לא יכל לזהות שמי שמתקשר אליו הוא בעצם תוקף זדוני בן 17. בחיי היומיום גילו לבד של התוקף היה מקשה על שכנוע העובד למסור את פרטיו לנער בן 17 וגם העובד היה דורש לראות תג עובד או פרט מזהה אחר. אך כיוון שהתקשורת ביניהם הייתה דיגיטלית, התוקף ניצל את זה והצליח להתחמק מהצגת תג עובד וגם יכל להסתיר את גילו הצעיר שהיה מקשה עליו בביצוע ההתקפה בחיי היומיום.
7. התקפת Phishing היא התקפה שבה נשלח מייל מטעה להרבה אנשים כך שהמייל הזה נראה כמו מייל רשמי מגורם מוכר ומכיל קישור לאתר זדוני בעל שם דומה ומראה דומה לאתר המקורי שבדרך כלל מוכר לאנשים ולכן הם עלולים לחשוב שזה מייל אמיתי וילחצו על הלינק הזדוני ויזינו את פרטיהם האישיים באתר הזדוני. למרבה הצער, אתר זה הוא אתר שנשלט על ידי התוקף וכאשר האנשים מזינים את פרטיהם באתר הם בפועל מסרו את פרטים אלו לתוקף ועכשיו הוא יכול לעשות מה שהוא רוצה עם המידע הזה, וסביר להניח שאין לו כוונות טובות. דוגמה: מייל שנשלח ממישהו שמתחזה להיות חברת אשראי עם מייל כתוב בשפה פורמלית, עם הלוגו של החברה אשר דורש כניסה דחופה כדי להסדיר משהו אך כאשר מישהו נכנס לאתר הוא מוסר את פרטי האשראי לתוקף שעכשיו יכול לנצל את הכסף שנמצא בכרטיס למשל.

התקפת Spear Phishing או בשמה האחר Whaling, היא התקפה שבה הקורבנות הם מישהו ספציפי שנבחר בקפידה והמייל המטעה נשלח אליהם בלבד, בדרך כלל אלו אנשים במעמדים בכירים כאלה שיש להם גישה לחשבונות בננק של הארגון או גישה למידע חשוב. התוקף עושה חקר מקדים על הקורבן כדי למצוא מידע עליו ואז הוא שולח לו מייל שמותאם לו אישית בנסיון להפיל אותו ולקבל שם משתמש וסיסמא שלו. וכייון שאנשים משתמשים באותה סיסמא להרבה אתרים אז יכול להיות שהתוקף יקבל גישה להרבה חשבונות או אתרים שהקורבן רשום בהן ומכאן לתוקף תהיה גישה למידע חשוב או משאבים יקרים. ההתקפה עובדת כפי שתיארנו מקודם אך ההבדל העיקרי הוא שהקורבן כאן הוא איש ספיצפי שנעשה עליו חקר מקדים כדי שיהיה יותר קל לרמות אותו.

1. הסיבה העיקרית שהתקפות של הנדסה חברתית עלולות להיות יעילות במקרים שהתקפות דיגיטליות אחרות ייכשלו הוא זה שבהרבה מהמקרים, יש מנגנוני אבטחה טובות נגד ההתקפות הדיגיטליות האחרות אך עבור התקפות של הנדסה חברתית יותר קשה להגן, צריך עובד אחד שיכניס דיסק און קיי שכתוב עליו משכורות למחשב ברשת הפנימית כי הוא היה סקרן מה המשכורות של עמיתיו בחברה, או מישהו שילחץ על Link זדוני וכך לתוקף תהיה גישה למידע חשוב. בעצם התקפות של הנדסה חברתית מצליחות בזמן שהרבה מתקפות אחרות נכשלות כיוון שאנשים הם בדרך כלל הם החולייה החלשה בשרשרת ההתקפות האפשריות וכדי "לתקוף" אנשים, עושים להם הנדסה חברתית.
2. יש כמה דרכים לטפל בהתקפות מסוג הנדסה חברתית, אולי החשובה מביניהן היא חינוך. חשוב לחנך אנשים כדי שיוכלו לזהות התקפות מסוג הנדסה חברתית, במיוחד אלו שנמצאים בקשר עם העולם החיצוני כך שכל מי שיוצר קשר שלא נותן מספיק מידע כדי לזהות אותו, או שואל שאלות עמומות או משונות בטון שמצביע על דחיפות הוא חשוד, וחשוב להבהיר גם שלא מוסרים סיסמאות דרך הטלפון! וגם, אם אנחנו חושדים במישהו אז צריך לבקש את מספר הטלפון שלו ולהתקשר אליו בחזרה, וזה עלול להרתיע חלק מהתוקפים. בנוסף לכן, בארגונים חייבים ליישם מידור של המידע כך שלא כל עובד צריך לדעת את כל הסיסמאות והיכן נמצא המידע המסווג. צריך גם לשמור על המידור ברמה הפיסית כך שיהיה מידור בין רשתות מחשבים בדרגות סיווג שונות, אישורי כניסה לאיזורים מסויימים בקומה רק למי שיש לו הרשאות לכך. כאשר עושים דברים אלו, אז המערכת תוכל לזהות במקרים מסוימים שיש התקפה עליה ולהדליק נורות אבטחה שיקשו על התוקפים.