תרגיל בית 1 הגנה ברשתות

שאלה 1 :

2. פרוטוקול ARP הוא פרוטוקול שבו על ידי שאילתות המופצות במחשבים הנמצאים ברשת כלשהי, ניתן למצוא כתובת MAC של מכשיר מבוקש המכיל IP ידוע שבהינתן ה-IP, אנו מחפשים את כתובת ה-MAC של המכשיר.

התקפת ARP spoofing יכולה להיות התחזות להיות המכשיר בעל ה-IP המבוקש ולהחזיר למעשה את ה-MAC שלו ולא של המכשיר בעל ה-IP הנתון.

1. תוקף יכול להשיג מהתקפה זו מידע אשר לא היה מיועד אליו אלא למחשב אחר ברשת, מידע אשר יכול להיות חשוב מאוד ופרטי ובכך להיחשף למחשב זדוני המתחזה למחשב שאליו מיועד המידע.
2. בהנחה שהתוקף יודע איזה מחשב ברשת הולך לבצע שאילתת ARP, ובהינתן שהשאילתה מופצת בו זמנית לכל תתי המחשבים ברשת, על התוקף להיות כמה שיותר קרוב פיזית למחשב אשר מפיץ את שאילתות ה-ARP ולכן מגדיל את סיכוייו לקבל את השאילתה מוקדם יותר מהמחשב בעל ה-IP המיועד ולענות לפניו.
3. ראינו בהרצאה כי דרך להתמודד עם ARP spoofing יכולה להיות למשל עם cookies.
4. מומלץ להתקין במהירות security updates כיוון שהן מכילות תיקונים לחולשות קיימות שעלולות לא להיות מפורסמות למשתמשים ולכן החולשות האלה עלולות להיות מקור לתקיפה ולכן צריך להתקין במהירות עדכוני אבטחה. דוגמה לכך היא התולעת blaster אשר הופצה רק לאחר ש-microsoft פרסמו patch שמתקן את החולשה וקבוצה ביצעה reverse engineering ל-patch כדי למצוא את החולשה.
6. המחשב קרס באותו יום בגלל שנדבק בתולעת האינטרנט.
7. בממוצע, אחת מכל 7 תולעים לעולם לא הייתה מתאבדת, ולכן נוצר מצב בו כל מחשב נדבק בהרבה תולעים שלא מתאבדות ולכן זה לוקח מספר דקות עד שהזיכרון יתמלא לגמרי בתולעים.
8. הסטודנט לא היה מתחבר עם המחשב לרשת האינטרנט בחוות המחשבים.
10. חולשת buffer overflow היא חולשה שבה מקצים חוצץ ואין בדיקה על גודל המידע שממלא את החוצץ, ולכן יכול להיווצר מצב בו יש העברה של מידע בגודל כולל גדול מגודל החוצץ ולכן יש דליפה של מידע מהמקום בו הוקצה החוצץ והוא עלול לדרוס מידע אחר. תולעת יכולה לנצל חולשה זו באמצעות דריסת מידע חשוב כמו כתובות חזרה מפונקציות ובמקומן לכתוב כתובות של פונקציות שהתוקף רוצה שירוצו.
11. 2 תולעים מפורסמות שהשתמשו בחולשה זו הן תולעת האינטרנט (התולעת של מוריס) ותולעת blaster.
12. תולעת האינטרנט ניצלה את חולשת ה-buffer overflow של פקודת ה-gets שאינה מוודאה את תקינות הקלט, הוגדר חוצץ בגודל 512 בתים, ואז רצה הפקודה gets כאשר ב-socket מועברת לחוצץ הודעה גדולה יותר מגודל החוצץ ולכן יש buffer overflow וההתקפה ניצלה זאת על מנת לדרוס ערך חזרה של הפונקציה gets ולהכניס כתובת חזרה אחרת לפונקציה שהתוקף רצה שתרוץ.
13. צריך לבטל את הכשל שבו בממוצע אחד מכל 7 עותקים של התולעת לא מתאבד, ולתת לתולעים לבדוק אם יש תולעים נוספות במחשב, ובמידה שיש אז שיתאבדו (כדי לשמר חסינות התולעת אפשר להשתמש במנגנון של challenge – response כדי למנוע זיוף תגובה של תולעת ובכך להגדיל את הסיכוי שאכן קיימת תולעת נוספת ועליה להתאבד על מנת שבממוצע תהיה רק תולעת אחת במחשב.
14. התקפת syn attack היא התקפה על TCP למניעת זמינות. כאשר מתחיל TCP session מערכת הפעלה מקצה משאבים ל-session בדמות זיכרון, תורים. מערכת הפעלה משחררת את המשאבים כאשר נגמר ה-session. כלומר, פתיחה של הרבה sessions יכולה לצרוך את כלל המשאבים הזמינים למערכת ההפעלה, ובכך לפגוע במחשב ובתפקודו. התקפת syn attack היא מסוג DOS כלומר מניעת שירות, ובאה לידי ביטוי בכך שהמתקיף שולח למותקף המון חבילות ראשונות של TCP session ביחד במטרה להפיל את המותקף או להאט אותו דרסטית או למנוע ממנו לתת שירות לאחרים, וזאת באמצעות מיצוי המשאבים שלו כפי שציינתי למעלה (תורים, זיכרונות).

שאלה 2 :

2. מודל השכבות כפי שנלמד:

יש לנו את שכבת האפליקציה בראש הכוללת את האפליקציות כלומר תוכניות שרוצות לדבר אחת עם השנייה, בשכבה זו אפליקציה מגדירה את המידע אותו היא רוצה להעביר לאפליקציה אחרת, ועל מנת לבצע את הטרנזקציה של המידע, היא דורשת תמיכה משכבת התובלה.

דוגמה לפרוטוקול בשכבת האפליקציה : HTTP.

שכבת התובלה היא שכבה אחת מתחת לשכבת האפליקציה, שכבה זו יודעת לקבל מידע משכבת האפליקציה ולפרק את המידע לחבילות ועל מנת שיהיה אפשר להעביר אותן ברשת היא דורשת תמיכה משכבת הרשת.

פרוטוקול בשכבת התובלה : TCP המאפשר מעבר מידע בצורה אמינה על ידי תחזוק session של העברת מידע.

שכבת הרשת כבר מעבירה את המידע ברשת ועליה לדעת את מסלול הניתוב ברשת של המידע ויכולה להיות שישנה דרישה שהמידע יעבור בין כמה מחשבים ברשת ולכן שכבת הרשת מטפלת בזה בצורה שהיא שקופה לשכבת התובלה.

פרוטוקול בשכבת הרשת : IP.

שכבת ה-MAC מתחת לשכבת הרשת והיא השכבה שמטפלת במשלוח עצמו על ערוץ התקשורת שהוא השכבה הפיזית והתחתונה. שכבת ה-MAC היא אחראית על מעבר המידע בין מחשבים שכנים, כלומר אי אפשר לשלוח לצורך העניין מידע ממחשב בטכניון למחשב פרטי בארה"ב על שכבת הרשת בלבד אלא יש ניתוב באמצעות שכבת הרשת שנעזרת בשכבת ה-MAC כדי לנתב בין שכנים.

פרוטוקול בשכבת ה-MAC : Ethernet.

שאלה 3 :

1. יישום בחיי היומיום של הנדסה חברתית הוא למשל קנייה בסופר, שם יש נטייה לשים מוצרי יסוד בסוף הסופר ובכך יש הכרח לחצות את כל הסופר בתקווה שלקוח יקנה מספר מוצרים "על הדרך", ועוד דוגמה למשל ממתקים ליד הקופות.
2. בהקשר של אבטחת מחשבים, הנדסה חברתית היא הדרך שבה תוקף יכול לתמרן, להשפיע ולהטעות אנשים בעלי גישה למידע מסווג בחברה, ושימסור לידיו מידע שהתוקף מעוניין.
3. ממשלות נאלצו להשבית את מערכות הדואר האלקטרוני שלהן כדי למנוע את קריסתן ולהגן על עצמן מווירוס ILOVEYOU.
4. על ידי ניצול באג באתר האינטרנט של T-Mobile ניתן היה להתחבר לרשת האינטרנט הפנימית של T-Mobile ולקבל גישה לחשבונות הטלפון של הלקוחות, שזה מה שעשה התוקף, כאשר הוא קיבל גישה לחשבונות הטלפון של הלקוחות באמצעות כניסה לרשת האינטרנט הפנימית של החברה באמצעות שם משתמש וסיסמה של עובד בשירות המכירות בצורה כזו שהוא הערים עליו שהוא טכנאי שנשלח לתקן בעיות.
5. כדי לגשת לתוכן המכשיר של פאריס הילטון, צריך לתת סיסמה או לשחזר באמצעות מענה על שאלה אישית. השאלה של פאריס הייתה מה השם של חיית המחמד האהובה עליה כאשר השם היה מפורסם וידוע לכל. אם הייתה בוחרת שאלה שרק היא יודעת את התשובה עליה אז הייתה עלולה להימנע ההתקפה.
6. הכוח הנוסף של הנדסה חברתית בתקשורת דיגיטלית לעומת הנדסה חברתית בחיי היומיום היא שדרך אמצעי תקשורת דיגיטלי אין צורך בזיהוי ממשי, והתוקף ניצל זאת בכך שסביר להניח שהעובד בחברת T-Mobile בשירות המכירות לא היה מאמין לילד בן 17 שהוא טכנאי בשירות החברה, ולעומת זאת דרך הטלפון לא היה ניתן לזהות שהוא משקר. בנוסף, היה עליו לפחות ללבוש מדים של החברה או להציג איזה שהוא תג עובד. כמו כן, ארגונים גדולים המשתמשים בתקשורת דיגיטלית פגיעים הרבה יותר וחשופים לתקיפות דיגיטליות.
7. התקפות phishing הן התקפות המציפות רגשות עזים וחזקים ומהירים על מנת לגרום לפעולות פזיזות של הנתקף. לחיצה על קישור או הפנייה לעמוד הנראה זהה ועם כתובת קרובה לעמוד מקור (למשל התחזות לעמוד של בנק) הנותנת עוד יותר אמינות בלינק הנגוע מבחינת הנתקף, ועל ידי כך הנתקף עלול להכניס מידע כגון שם משתמש וסיסמאות ישר לידי התוקפים.

ההבדל בין התקפות phishing לבין התקפות spear phishing הוא שב-spear phishing ההפצה של ההתקפה היא לאנשים שנבחרו בקפידה מראש וסביר להניח בעלי יכולת וכוח כמו למשל מנהלים בכירים בארגונים, לעומת phishing שהוא מופץ בתקווה לתפוס נתקפים כלשהם.

1. התוקף יכול לקנות מראש מניות של חברה קטנה שלא נסחרת במחזורים גבוהים ולכן כל קנייה בסכום גבוה מקפיצה את שווי המנייה. לאחר פריצה לחשבון בנק של הנתקף הוא יכול לבצע רכישה בסכום גבוה של מניות החברה, מה שמקפיץ את שווי נייר הערך והוא מרוויח כסף רב, וזאת מבלי לבצע העברה מהחשבון של הנתקף לחשבונו שלו.
2. ניתן לבצע תקיפה תוך כדי זיהוי חולשה בתוכנה או בחומרה, אך בהמון מקרים התקיפות מתבצעות עקב חולשה בצורת אדם מבפנים שעלול לספק מידע כגון סיסמאות ושמות משתמשים, ולכן באמצעות שימוש בהנדסה חברתית ניתן לנצל חוליה חלשה באבטחה בצורה כזו שאדם מספק עלול לספק מידע מסווג שעוקף הרשאות.
3. הדרכים המוצעות בפודקאסט לטיפול בהתקפות הנדסת חברתית הוא חינוך בחברה – כל העובדים שיש להם ממשק עם אנשים מחוץ לחברה צריכים להכיר את השיטות והדרכים לגלות התקפות של הנדסה חברתית כמו למשל "לקוח" שלא מספק מספיק פרטים ברורים או מדבר בטון שמשדר דחיפות או לחץ אז יש לחשוד.

בנוסף, ארגון יכול להפעיל מנגנון מידור מידע, לא כל עובד חייב להיות חשוף לכל המידע בארגון. ניתן לקבוע נהלים ברורים איזה מידע אפשר לספק בלבד לגורם חיצוני.