מטלה 1 – התקפת Evil-Twin

רקע

- התקפת התאום הרשע (Evil-Twin) מהווה יישום של התקפה קלאסית לעולם הסייבר האלחוטי מסוג Rogue AP. העקרון פשוט, משתמש שרגיל להתחבר לתאום הטוב לא מצליח להתחבר אליו יותר, מנסה להתחבר ידנית לרשת היחידה שהם מסוגלים להתחבר אליה (התאום הרשע) ובגלל ששני הרשתות נראות זהות, זה מצליח... הם מנסים לגלוש באינטרנט אבל מגיעים לCaptive Portal בו הם נדרשים לספק שם משתמש וסיסמה ולאחריה הם גולשים באינטרנט...

מטרת המטלה

- פיתוח **כלי** לביצוע התקפת Evil-Twin מלאה כמתואר ברקע. כחלק מיכולות הכלי, תלמדו כיצד ניתן בקלות רבה לאסוף נתוני נקודות קצה בWLAN בלי קשר לשיוך הרשת שלהם. תלמדו על הפגיעות הגבוהה של תקן 802.11 עקב הקושי לוודא את זהות שולחי החבילות וכן כיצד להקים רשת תקשורת אלחוטית בתקן 802.11.

- מיומנות בפיתוח כלי מנע (Counter Measures)
- בנוסף תרכשו מיומנות בשפת התכנות Python וספריית SCAPY שעל יכולותיה בתחום הרשתות ובפרט WLAN עליכם לסמוך. כמו כן המטלה תקנה לכם מיומנות בפיתוח ובניית כלי תקיפה/הגנה ומיומנות בLinux Shell.

דגשים

- כאשר מתייחסים לתקיפת טכנולוגיית תקשורת אלחוטית תמיד נדרש לנהל ממד חומרתי מעבר לפן היישומי הרגיל ולכן יש צורך בפיתוח תוכנת התקיפה אשר איננה מטפלת רק במרחב היישומי אלא גם בניהול ישיר של תקשורת אלחוטית דרך חומרה תואמת. הדבר יוצר מורכבות גדולה בפעולות הנדרשות לביצוע המתקפה מה שמהווה פתח לשיבושים וטעויות שפוגעות באיכות ההתקפה/הגנה.
- הפתרון הטוב ביותר להתמודד עם מורכבות זו הינה לבנות תוכנת תקיפה אשר בתוכה יוטמעו תהליכי המתקפה השונים והיא זו שתנהל את המתקפה מתחילתה ועד סופה. עליה לאפשר למשתמש להיות כמו מנצח בתזמורת, במאמץ קטן לתזמן את הכלים השונים והמנגינה תוך כדי ניטור תמידי של מצב המערכת כפי שהמנצח שומע את המוזיקה של התזמורת.

- בקורס זה, **כלי תקיפה מוגדר כמערכת הנמצאת תחת מעטפת וממשק אחד** אשר ממנו מתבצעים כל הפעולות הנדרשות ללא צורך בהתאמת הקוד, בהקלדת פקודות מקבילות בעטיפת shell נפרדת. במושג "כלי" אנחנו מכוונים למערכת שלמה שאיש הסייבר בונה לעצמו בכדי לבצע את עבודתו ובהקשר שלנו, ביצוע התקפה. עיינו בהגדרה הנ"ל:

A complete integrated set of software utilities that are used to develop and maintain applications and databases.

- נדרש **שכל הגשות הקוד יהיו מקוריות של הקבוצות** וקבלת השראה מפתרונות וכלי תקיפה בעבר הן מומלצות. מותר להשתמש בקוד קיים כבסיס לבניית הכלי והכנתו בתנאי שהקוד הותאם ופותח למטרות ההגשה. הציון ניתן על יכולת פיתוח כלי עצמאי ומקורי ולא אחרת.
- על הקוד המוגש לעבוד! המערכת תיבדק בדרך כלל בסביבת הפעלה Linux Kali או Ubuntu, **לא כדאי להשתמש ב VM כסביבת פיתוח ובדיקה לכלי!**

אל תשכחו לקרוא את דרישות המטלה בעמוד הבא!

דרישות המטלה:

- **בניית כלי תקיפה** Evil Twin **<u>אשר איננו מצריך שינוי בקוד בכדי להפעילו</u>** לדוגמא מאפשר בחירת התקן רשת אלחוטית המסוגל לבצע את הדברים הבאים:
  - סריקת WLAN בסביבה למשך דקה והצגת הרשתות השונות שנתגלו.
  - בחירת הרשת שיש לבצע עליה את ההתקפה.
  - הצגת לקוחות של הרשת עליה נעשית ההתקפה.
  - בחירת קורבן וביצוע התקפת Evil-Twin.
  - חיווי לשלבי ההתקפה השונים דהיינו:
    - ניתוק הקורבן מהרשת הקיימת/ השבתת התאום הטוב באמצעות SCAPY.
    - העלאת הרשת הזדונית (התאום הרשע) והפעלת Captive Portal.
    - התחברות הקורבן לרשת הזדונית ופעילותו.
    - השגת המידע שהינה מטרת ההתקפה.
- **בניית כלי הגנה** אשר מזהה קיומה של התקפה על הקורבן ומונעת את הצלחת ההתקפה.

הנחיות ביצוע:

- לצורך ביצוע ההתקפה, נדרש מתאם רשת אלחוטית (WLAN Network interface controller), אשר מאפשר חישה סבילה והזרקת חבילות בתקן 802.11 (Monitor mode) . במסגרת הקורס נרכשו מספר מתאמים וניתן להשיגם באריאל וברמת-גן.
- <u>איש הקשר באריאל</u>: איליה רוזנטל, לרוב זמין בין השעות 10:00 -14:00, ימים א-ה ב-A56.0.54 החדש מול מעבדת הסייבר של עמית. נייד: 054-524-5532.
- בכדי לתאם עם איליה, המעיטו בשיחות צליל או הקלטות השתמשו כמה שיותר בתוכנת המסרים של WhatsApp.
- <u>איש הקשר ברמת-גן</u>: הוא המרצה (אני). ניתן לפנות אלי במייל, בשיעורים ובדרכים נוספות שאפרט בשיעור.

הנחיות הגשה

- יש להגיש קובץ דחוס אחד הכולל:
- קבצי קוד בדוק ומנוסה אשר ניתן להריצו במערכת הפעלה לינוקס סטנדרטית.
- תיעוד השימוש בקוד, הכנות או **דרישות קדם** ככל שיידרש.
- קובץ NFO לפי סגנונכם הכולל את **הפרטים האישיים של המגישים**, זה המקום שבו ניתן להוסיף התייחסות לעבודה או למטלה שאיננה קשורה לקוד עצמו.
- העבודה הינה לפי קבוצות העבודה שהתחלקתם אליהם במטלה 0.

כמו תמיד, אם יש ספק, אין ספק שצריך לפנות אלי...
אפשר במייל אפשר בכיתה וכדומה...

בהצלחה רבה,
אייל

נ.ב .

כתובת המייל: abard@g.ariel.ac.il