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... משם אפשר לפתח את הדברים בסגנונות שונים והמוכר ביותר הינו שניסיון לגלוש בדפי המרשתת מביא לCaptive Portal אשר דורש את שם המשתמש והסיסמה לרשת בכדי לגלוש...

התקפה שכזו, מאפשרת לעקוף רשת אשר מאובטחת היטב או ליצור תנאים טובים יותר להשגת מידע...

מטרת המטלה

- הבנה יסודית ברשתות תקשורת בתקן WLAN 802.11, כיצד ומה נדרש בכדי להקים רשת שכזו וכן הבנת הפגיעות הגבוהה של תקשורת בתקן 802.11 זה כמו זו הנובעת מהקושי לוודא את זהות שולחי החבילות והקלות בה ניתן ליצור רשת בשליטת התוקף.
- פיתוח **כלי תקיפה** 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.
- פיתוח **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 תכנון ותכן כלי תקיפה/הגנה ומיומנות בעבודה בLinux Shell.

דגשים

- **כל סטודנט** חייב לעבור הגנה פרונטלית/ZOOM על הגשת המטלה של קבוצתו.
- ציון המטלה בנוי **מציון בסיס וציון אישי.** ציון הבסיס ניתן להגשה עצמה והציון האישי ניתן לביצועי הסטודנט בהגנה על ההגשה.
- בהגנה על הגשת מטלה זו **כל סטודנט ייבחן** על הבנה, ידע ושליטה טובים בטכנולוגית WLAN בדגש על הנלמד בכיתה. בפרט עליו להכיר ולהבין היטב כיצד הדברים שנלמדו בכיתה ממומשים בקוד. הבנה פונקציונאלית הינה הבנה הכרחית אבל לא מספיקה בהקשר הזה.
- כדאי ומומלץ ללמוד ולקבל השראה ממקורות שונים אבל להיזהר מהבנה שטחית ופונקציונאלית החסרה את ההקשר המלא...
- **נדרש שהכלים שהוגשו יפותחו באופן עצמאי ומקורי!**
- הקוד נדרש לפעול **בגמישות** של חומרות שונות וסביבות תקשורת שאינן הסביבה בה בדקתם את ההגשה... ההגשה תיבדק בדרך כלל בסביבת הפעלה DragonOS או הפצת לינוקס דומה.
- אם משתמשים **ב VM** חייבים לקחת בחשבון שלמרות שנראה שישנה גישה מלאה לחומרת התקשורת, בפועל נדרשת לפעמים הגדרות מיוחדת שבלעדיהן נראה שהחומרה לא תקינה...

אזהרה חמורה: אין להשתמש בכלים מוכנים מראש בסגנון כלי העבודה של Aircrack...

הגשה שבה ייעשה שימוש בכלי שכזה **תיפסל מיידית**!

אל תשכחו לקרוא את דרישות המטלה בעמוד הבא!

דרישות המטלה :

- **פיתוח כלי תקיפה** המבצע את התקפת Evil Twin כפי שמפורט לעיל.
- **פיתוח כלי הגנה** המזהה את ההתקפה ומאפשר ביצוע פעולות מנע. עליכם להשתמש בידע ממה שלמדתם בכיתה ולבנות כלי שכזה... (בונוס קטן למימוש פעולות מנע אשר אינן משביתות את פעולת הרשת).

מהם שלבי התקפת Evil twin

- מציאת **כל** רשתות ה WLAN בסביבת הרכיב (דקת סריקה).
- בחירת רשת אחת מאלו שנמצאו.
- בחירת קורבן שהינו **לקוח פעיל** ברשת שנבחרה.
- ניתוק הקורבן **בלבד** מהרשת שנבחרה.
- הפעלת רשת תאומה מרושעת כולל **שירותי התקשורת** האחרים הנדרשים לפעילות תקינה.
- יצירת מנגנון ללכידת שם משתמש וסיסמה.

שימו לב!

בקורס זה, ה**כלי מוגדר כמערכת הנמצאת תחת מעטפת וממשק אחד** אשר ממנו מתבצעים כל הפעולות הנדרשות **ללא צורך נוסף בהתאמת הקוד, הקלדת פקודות מקבילות בעטיפת shell נפרדת וכדומה.** זכרו שSCAPY איננה מסוגלת לנהל את החומרה בפועל...

כלי טוב יאפשר מצד אחד תצורה (setup) מהירה של התהליך ע"י המשתמש תוך מניעת טעויות ושיבושים ומצד שני יאפשר למשתמש מודעות מצב בזמן אמת בכדי שיוכל להגיב ולהבין מה קורה בכל שלב. לכן חובה ליצור לכל שלב חיווים (משוב) מתאימים, לדוגמא הצגת אלו רכיבי חומרה יש להשתמש או הצגת מצב סריקת כל הרשתות הקיימות בסביבה ולהציג אותן כך שהמשתמש יוכל לבחור באחת מהן. קחו בחשבון שללא חיווי של הכלי לא תוכלו לדעת שמשתמש התחבר לרשת התאומה או לדעת שהמטרה הושגה וההתקפה הסתיימה...

אתם רוצים לפתח כלי התוכנה שיאפשר למשתמש לפעול כמנצח בתזמורת שמנגנת את תהליך העבודה כך שהמשתמש מפעיל במאמץ קטן את הנגנים ומסוגל לשמוע בו זמנית את המוזיקה שהם יצרו כך שידע בדיוק מה כל נגן עשה או לא...

חומרה נדרשת :

מתאם רשת אלחוטית (WLAN Network interface controller), אשר מאפשר חישה סבילה והזרקת חבילות בתקן 802.11 (Debug mode/Monitor mode) . במסגרת הקורס נרכשו מספר רב של מתאמים אשר נמצאים באריאל וניתן לשאול אותם לתקופת הקורס.

איש הקשר באריאל: איליה רוזנטל, יש לפנות אליו **רק באמצעות תוכנת המסרים WhatsApp:**
נייד: 054-524-5532

הנחיות הגשת הקבצים :

- אפשר להגיש את הקבצים כקובץ דחוס או בGITHUB.
- **כל שינוי בהגשה לאחר המועד הסופי, יפסול את ההגשה מיידית.**
- על ההגשה לכלול :
  - קבצי קוד בדוק שיעבוד תקין על מערכת הפעלה לינוקס סטנדרטית.
  - קובץ ReadMe הכולל את **פרטי הקבוצה כולל פרטי המגישים** וכל תיעוד נדרש אחר כגון הכנות או דרישות קדם.

אם יש ספק, אין ספק שצריך לפנות אלי, אם במייל, בכיתה או בשעות קבלה

בהצלחה רבה,

אייל

נ.ב .

כתובת המייל: abard@g.ariel.ac.il