

Wireless & Mobile Attack Seminar

יועץ אקדמי: מר אבי ויסמן

תוכנית לימוד ליועצים ארגוניים וליועצי אבטחת מידע

מבוא

Security-Seminar

אנו שמחים להגיש לך מתכונת של סמינרים בעלי אוריינטציה לימודית, במבחר נושאים השאובים מתוך הקורסים המתקדמים והיוקרתיים של See Security. הסמינרים נבנו במתכונת לימודית גרידא, ומאפשרים לסטודנט להמשיך לימודיו בעצמו בנושא הסמינר. מתכונת זו נועדה למבקשים להרחיב השכלתם המקצועית, אך מנועים מהיעדרות נרחבת ממקום עבודתם.

מכללת See Security הנה מכללה התמחותית למקצועות התשתיות ואבטחת המידע בלבד, ועוסקת בלעדית בתחום זה בכל זמנה, תוך שימוש במתודולוגית הדרכה שנבנתה עבור גורמים ממלכתיים, תוך שילוב תיאוריה ופרקטיקה על-בסיס חמשת עולמות אבטחת המידע. מנהל המכללה, מר אבי ויסמן, הינו ממובילי ענף אבטחת המידע בישראל, פרשן ויועץ מבוקש בערוצי השידור בישראל, יו"ר הפורום הלאומי לאבטחת מידע, IFIS וכן מנכ"ל משותף בפירמה לייעוץ אבטחת המידע ו-Cyber Warfare.

אודות הקורס

קורס מרתק זה הינו נגזרת של פרק Wireless Hacking בקורס תקיפה קיברנטית Hacking Defined Experts ("הגרסה השחורה"). הקורס חושף את הסטודנט לשיטות התקיפה הטיפוסיות לסביבת התקשורת האלחוטית וציוד נייד לאחר סקירה קלה של שיטות המודיעין והחקירה המתלווים. בין השאר, ייסרקו פרוטוקולים טיפוסיים כדוגמת 802.11 לצד גישות אלחוטיות נפוצות אחרות כדוגמת Bluetooth ו-RFID.

כל נושא מורכב מהצגה תיאורטית, ומתרגול מעשי / הדגמה, בהתאם למסגרת הזמן.

קהל היעד

מנהלי מערכות מידע בארגונים, מנהלי אבטחת מידע, יועצי אבטחת מידע, מומחי תקיפה.

מטרת התכנית

התמחות מעמיקה בתקיפה בסביבת Wireless ו-Mobile.

מידע מינהלי: אלווירה אליסייב, 03-6122831, 052-8787889, elvira@see-security.com

יועץ אקדמי: אבי ויסמן, 054-5222305, avi@see-security.com

מתודולוגיה

המסלול נבנה על-בסיס פדגוגי ודידקטי ואוריינטציה פרקטית בפיקוח אקדמי, במדרג של בעלי תארים (רמות שונות), והכרה בארגונים בעלי אתיקה דומה (ISC2, ISACA, GIAC, ISSA, SII). תשומת לב ניכרת ניתנת לדגשים הנהוגים בישראל (הפורום הישראלי לאבטחת מידע IFIS).

המתודולוגיה המתוארת מתבססת על רשימת כל המקצועות התעסוקתיים המקובלים בתעשיית אבטחת המידע ולוחמת המידע, ומולם – כל תחומי הידע הקיימים בעולם זה.

מהמטריצה נגזר הידע הנדרש לכל מקצוע, ומכאן נגזרים מסלולי הלימוד והקורסים, היקפיהם ומיקודם. מטריצה זו של הפורום הישראלי לאבטחת מידע מהווה עמוד שידרה למתודולוגיית הלימודים של See Security.

תוכנית לימודים:

1. Reconnaissance

1.1. איסוף מודיעין מקדים.

2. 802.11

2.1. חדירות וחולשות בפרוטוקול WEP.

2.2. פריצה לרשתות מוצפנות WPA1.

2.3. חדירת רשתות מוצפנות WPA2.

2.4. יצירת Rouge AP.

2.5. הרעלות KARMA.

2.6. מעקף הגנות MAC Filtering.

2.7. האזנה חיצונית לרשתות מוצפנות ומיפוי קליינטיים.

2.8. גישור רשתות.

2.9. Kismet, WiGLE, ומיפוי וניתוח רשתות מתקדם.

3. Bluetooth

3.1. גניבת ספרי טלפונים ללא חיבור קודם.

3.2. יצירת Associations ללא אישור.

3.3. חיוג מרחוק ושליטה במכשיר.

3.4. יצירת Session עמיד אל הקורבן.

4. RFID

4.1. קריאת מערכות RFID וסוגי הצפנות.

4.2. שכפול תגים.

4.3. מעבר בקרות כניסה מבוססות RFID.

4.4. קריאת מידע רגיש מרוחק.

5. Mobile Exploitation

5.1. פגיעויות ב-iOS.

5.2. פגיעויות ומחקר מערכות Android.

5.3. פגיעויות מבוססות Safari.

5.4. מחקרי פגיעויות ב-SMS ו-AppStore.

6. Mobile Spoofing

6.1. זיוף מזהה שיחה בעזרת מרכזיית Elastix.

6.2. פתיחת שיחה חסומה.

6.3. זיוף הודעות מקומיות ושליחת הודעות מזויפות.

6.4. ניהול SIP מקומי וחיבורו לרשת הטלפוניה.

סגל ההוראה במכללה:

