CTF – הצעת פיתוח

נכתב ע"י אליאל מונפורט

328269121

ב- CTF נעשה שימוש ב- 8 נושאים:

SMTP, Wireshark, Nmap, HTTP, תכנות סוקטים, קריפטוגרפיה, Gobuster, TLS.

מספר השלבים:

5 שלבים

פתיחה:

קובץ PDF המכיל סיפור פתיחה יצירתי... [משהו על סוכן חשאי ומשימה סודית]

בסוף הקובץ יהיה קישור להסנפת Wireshark.

שלב א – SMTP + Wireshark:

המידע הנתון – קובץ הסנפה ושם ה- Target (הניתנים בנקודת הפתיחה).

הפעולות המתבקשות – קובץ ההסנפה יכלול חבילות SMTP ו- HTTP. בעזרת השם אפשר למצוא חבילת SMTP מתאימה. בעזרת חבילת ה- SMTP נוכל למצוא בנוסף בקשת GET של תמונה.

המידע המתקבל – בחבילת ה- SMTP יהיה מסר מוצפן בהצפנה סימטרית בשיטת Xor, ובתמונה יהיה מפתח (Shared Secret) לפיענוח ההצפנה.

שלב ב – קריפטוגרפיה:

המידע הנתון – מסר מוצפן בהצפנת סימטרית בשיטת Xor ומפתח לפיענוח ההצפנה.

הפעולות המתבקשות – פיתוח קוד לפיענוח המסר בעזרת המפתח Shared Secret שמצאנו בשלב קודם (ההצפנה הסימטרית מתרגיל 6).

המידע המתקבל – במסר המפוענח יהיה קישור ל- Google Drive המאגר שרת HTTP הרץ מקומית (local host) בקובץ exe.

שלב ג – HTTP + Nmap + תכנות סוקטים:

המידע הנתון – קובץ הרצה (exe) של שרת HTTP הרץ על Local Host.

הפעולות המתבקשות – הרצת השרת. השרת יאזין לחיבור אך לא יפרט לאיזה Port. שימוש בפקודת Nmap למציאת Port -ים פתוחים ומציאת Port השרת בפרט. פיתוח קוד הלקוח המבצע בקשת GET ומדפיס את תגובת השרת.

המידע המתקבל – בקשת " \ ", עמוד בררת מחדל, ייתן קוד 302 שיפנה למיקום אחר. בקשת המיקום האחר יחזיר קישור לאתר שיצרתי.

שלב ד – Gobuster:

המידע הנתון – קישור לאתר. לאתר יש עמוד התחברות הדורש שם משתמש וסיסמא.

הפעולות המתבקשות – הרצה הפקודה Gobuster על האתר, ומציאת נתיבים מוסתרים באתר.

המידע המתקבל – מציאת מספר נתיבים מוסתרים באתר. שנים מהנתיבים חשובים, אחד יכיל כפתור ל- Google Drive שיכיל קובץ הסנפה (הסנפת TLS), והשני יכיל עמוד המכיל את ה- Client Random ואת המפתח לפיענוח ההסנפה.

שלב ה – TLS:

המידע הנתון – קובץ הסנפה המכיל חבילות TLS, וקובץ המכיל את ה- Client Random ואת המפתח לפיענוח ההסנפה.

הפעולות המתבקשות – בעזרת ה- Client Random והמפתח נפענח את ההסנפה.

המידע המתקבל – עם חקירה מעמיקה של ההסנפה ובעזרת הפילטר **Follw Stream** וגם הפילטר **"fram contains "Password**, נוכל למצוא את ה- Username וה- Password הרצויים.

סיום:

בעזרת ה- Username וה- Password שמצאנו נוכל להתחבר למערכת ונקבל את המסר הסופי המודיעה את הצלחה ה- CTF.