

מסמך אפיון ל - CTF

בשמחה ובהודיה אני מתכבד להגיש את המסמך אפיון לעבודת גמר של קורס: "רשתות מתקדמות".
 ארצה להתחיל עם הכרת תודה לברק גונן וכלל המרצים שעזרו ופעלו ללימוד החומר, ממש הורגש שהלימוד לא היה בשביל לסמן
 "וי", אלא ממש מתוך שליחות של הקניית החומר לתלמידים, תודה רבה, זה לא ברור מאליו.

תודה נוספת ו"בבלוד" לבודקים, להיות בודק זה לא פשוט, תודה.

השלבים של ה CTF:

שלב ראשון:

הפותר מקבל קובץ זיפ נעול עם רמזים על תבנית הסיסמה, והוא צריך לכתוב קוד שיפצח את הקובץ זיפ.
 שימוש ב: 7-zip של פייתון.

שלב שני:

לאחר פריצת הזיפ מתגלים לו שני קבצים, אחד http-server בצורה של pyc, והשני: קובץ exe.
 כשהוא מריץ את ה קובץ pyc הוא רואה שהוא פשוט מבקש סיסמה ואומר על איזה פורט ו IP הוא.
 ועם הקובץ exe הוא רואה שהוא גם מבקש סיסמה.
 על הפותר לפרוץ את הקובץ exe ב ida, למרות שיש על הקובץ antibug, יהיה ניתן לפרוץ את הקוד בלי
 לעשות דיבאג, אבל אפשר לפרוץ עם.
 לאחר פריצת הקוד, והרצתו, הקוד ייצא קובץ pyc.
 שימוש ב: http post, רברסינג (אנטי דיבאג +פצפוצ), הצפנה (הקובץ פייתון מוצפן בתוך ה exe)

שלב שלישי:

המשתמש יבין שעליו להריץ את הקוד ולהסתכל עליו ב wire shark, לאחר שהוא מסניף את הפקטות, הוא
 רואה שהקוד שולח פקטות ל IP מסוים ומצפה לתשובות. על המשתמש לכתוב קוד שעונה לשאלות של
 הקליינט הזה, והוא יראה שהקליינט מצפה לתשובות דווקא מאותו IP וכן על הפותר להשתמש ב scapy
 בשביל להתחזות לאותו IP. לאחר שליחת כל התשובות הנכונים, אז אותו הקליינט ידפיס רמז לסיסמה
 של ה http server של ההתחלה.
 שימוש ב: ip, udp, scapy, wire shark

שלב רביעי ואחרון:

על הפותר לכתוב קוד אשר יפרוץ את הסיסמה של ה http-server, על פי אותם רמזים שנתנו לאחר השלב
 הקודם. ולאחר פריצת הסיסמה, הסרבר ידפיס את ה FLAG שצריך להגיע אליו.
 שימוש ב: http post (אותו דבר כמו שבשלב השני).