

מסמך אפיון ל- CTF

בשmachה ובהודיה אני מתכבד להציג את המסמך אפיון לעבודות גמר של קורס : "רשתות מתקדמות".
ארצה להתחילה עם הכרת תורה לברק גנון וככל המרצים שעזרו ופעלו ללימוד החומר, ממש הוריגש שהלימוד לא היה בשבייל לסמן "וii", אלא ממש מתוך שליהוחת של הקניית החומר לתלמידים, תורה הרבה, זה לא ברור מליין.

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

השלבים של ה-CTF:

שלב ראשון:

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

שלב שני:

לאחר פריצת הזיפ מתגלים לו שני קבצים, אחד http-server בצורה של .py, והשני : קובץ .exe.
כשהוא מרים את הקובץ .py הוא רואה שהוא פשוט מבקש סיסמה ואומר על איזה פורט ו IP הוא.
עם הקובץ .exe הוא רואה שהוא גם מבקש סיסמה.
על הפטור לפרוץ את הקובץ .exe ב ida, למרות שיש על הקובץ ,antibug, הפעלה ניתנת לפרוץ את הקוד בלי
לעשות דיבאג, אבל אפשר לפרוץ עמו.
לאחר פריצת הקוד, והרכתו, הקוד ייצא קובץ .pyc.

שימוש ב : http post , רברסינג (אנטי דיבאג + פצוף), הפעלה (הקובץ פיתון מוצפן בתוך ה .exe)

שלב שלישי:

המשתמש יבין שעליו להריץ את הקוד ולהסתכל עליו ב wire shark , לאחר שהוא מסניף את הפקודות, הוא
ראה שהקוד שולח פקודות ל IP מסוים ומזכה לתשובות. על המשתמש לכתוב קוד שיענה לשאלות של
הקליננט זהה, והוא יראה שהקליננט מזכה לתשובה דזוקא מאותו IP וכן על הפטור להשתמש ב
שביל להתחזות לאותו IP. לאחר שליחת כל התשובות הנכוניות, או אותו הקליננט ידפיסرمز לסיסמה
של ה http server של ההתחלה.

שימוש ב : ip , wire shark ,scapy ,udp

שלב רביעי ואחריו :

על הפטור לכתוב קוד אשר יפרוץ את הסיסמה של ה http-server, על פי אותן רמזים שננתנו לאחר השלב
הקדם. ולאחר פריצת הסיסמה, השרת ידפיס את ה FLAG שצריך להגיע אליו.
שימוש ב : http post (אותו דבר כמו שבשלב השני).