תחילה, המשתמש יקבל קישור לאתר הגרעין האיראני וקובץ הסנפה של התקשורת בכור האיראני. בנוסף המשתמש יקבל מידע מודיעיני שפונקצית הצ'ק סמ המשתמשת לוידוא שלמות החבילות שונתה על ידי הצוות הטכני בכור, וכעת הם משתמשים בפונקציה מותאמת אישית שאתה מקבל גישה אליה. האתר של הגרעין האיראני יהיה מאובטח לכאורה, ויאפשר גישה רק מאתר אחר לא ידוע של הגרעין האיראני. אתר זה אמור להיות מאובטח מאוד ולא ניתן לגישה, ולכן המשתמש יצטרך לערוך את פקטת האיג' טי טי פי הנשלחת לשרת כך ששדה הרפרר שלה יהיה מתוך האתר.

על מנת לדעת באיזה אתר מדובר, המשתמש יצטרך לנתח את קובץ ההסנפה ולמצוא את שאילתת הדי אנ אס שנענתה עם תשובה חיובית. שאליתא זאת מכילה דומיין ניימ שרק ממנו ניתן לגשת לאתר של הכור.

בנוסף , אתר הכור לא מאפשר גישה למשתמשים לא דוברי פרסית, ולכן יהיה עליך לשנות גם את שדה השפה בפאקטת האיג טי טי פי להיות פרסית.

אחרי כל זה האתר שיתקבל יכיל שדה סיסמא. רק סיסמא נכונה תעביר לשלב הבא. כדי להבין מהי הסיסמא נצטרך לנתח את קובץ התיעוד, ולמיין מתוכו רק קבצים עם צ'ק סמ תקין, כדי להבדיל בין תקשורת מקורית של עובדי הכור לתקשורת סרק. כדי למיין , נצטרך לכתוב קוד בעזרת סקאפי, שיחשב לכל פקאטה בקובץ את הצ'ק סמ , וילסיום ידפיס רק את תוכן הפאקטות שהצ'ק סמ שלהם תקין, כלומר, שהינן חלק מהתקשורת של עובדי הכור.

אחרי מיון זה, נקבל מחרוזת מוצפנת באמצעות צופן החלפה של ויגנר. ולאחר שפותר החידה יבין באיזה צופן מדובר , הוא יוכל להשתמש בכלים אונליין כדי להשיג פענוח לצופן. הצופן המופענח יהיה שורה מהסרט הדיקטטור, שתתן רמז עבה מאוד למה היא הסיסמא.

השורה מדברת על מבנה הטיל, והבדיחה בסרט היא שהדיקטטור חושב שטיל צריך להיות פוינטי, כלומר מחודד בקצה. וזאת גם הסיסמא, והתשובה לשאלה שכתובה מתחת "מהו המבנה האידאלי עבור טיל גרעיני?",.

לאחר שהסיסמא נכונה, הפותר יקבל תמונה מצחיקה של הסרט הדיקטטור. ובתוך התמונה יהיו שני קבצי הרצה. אחד יכיל שרת מייל אס אמ טי פי שרץ על לוקל הוסט, ואחד יכיל מנגנון וידוא סיסמא. שרת המייל יביא את הדגל רק למי שישלח מייל שכתובתו היא כתובת ייחודית של הממשלה האיראנית. כדי להבין מה המייל הזה, צריך לפרוץ את מנגון וידוא הסיסמא.

קובץ וידוא הסיסמא הוא קובץ הרצה שמאמת סיסמא ומדפיס מייל אם הסיסמא נכונה. כדי להגיע לסיסמא הפותר יצטרך לעשות רברס אנג'רינג לא טריוויאלי. הקובץ מכיל כמה מנגונני אנטי דיבאג, והמייל לא יהיו מקודד ממש, וגם לא המפתח שאיתו נפענח את הכתובת המייל המוצפנת.

לאחר שהמשתמש הצליח להבין מה המייל דרך הקובץ עליו לכתוב קוד פייתון ששולח מייל בפרוטוקול אס אמ טי פי. אם המייל נשלח באופן תקין, הוא יקבל את הדגל.

נושאים: UDP protocol (custom checksum)

HTTP protocol – using it to change the Referer and language fields of the packet.

DNS – analyzing DNS traffic to get the correct domain of the referrer.

Scapy – using Scapy or similar tools to analyze the custom checksum (Wireshark can’t filter it out).

Cipher – decrypting the Vigenère cipher and understanding XOR encryption to retrieve the password during reverse-engineering.

Reverse engineering – required to get the password and find the email address.

SMTP protocol – sending the mail to the server in the correct SMTP format.

Python sockets – implementing an SMTP client using Python sockets.