טכנו"צ סייבר - תרגיל 4 - "Tr0j4n"

סוס טרויאני + אינטגרציה

מבוא

נסקור בזריזות את מה שעשינו עד כה בתרגילים 1-3:

1. **תרגיל 1** - התממת קוד Python זדוני בתוך משחק מחשב.
2. **תרגיל 2** - מימוש מודול הצפנה (בו נשתמש בתרגיל הזה).
3. **תרגיל 3** - מימוש מודול תקשורת (בו גם כן נשתמש בתרגיל הזה).

כרגע יש לנו מערכת שמריצה פיקודים על גבי ממשק תקשורת, ומחזירה את הפלט בחזרה לתוקף. בתרגיל זה היא **נבנה פיקודים** לממשק התקשורת שבניתם בתרגיל 3, בנוסף להוספת **שכבת ההצפנה** מתרגיל 2.

שלב 1 - הוספת שכבת ההצפנה

נרצה להפריד בין שכבת התקשורת לשכבת ההצפנה, גם ברמת הקוד. לשם כך ניצור שתי פונקציות חדשות שעוטפות את המודול התקשורתי במודול ההצפנה.

צרו שתי פונקציות חדשות:

1. לקובץ commander/main.py הוסיפו פונקציה: encrypted_send_payload. הפונקציה מקבלת פרמטר יחיד (data) המייצג את התוכן של ההודעה שברצונו של התוקף לשלוח. הפונקציה מצפינה את המידע, שולחת אותו באמצעות send_payload, מפענחת את המידע החוזר ומחזירה אותו.

2. לקובץ malware/main.py הוסיפו פונקציה: encrypted_handle_receive. הפונקציה מקבלת פרמטר יחיד (enc_command) המייצג פיקוד מוצפן שהתקבל על הsocket. הפונקציה תפענח את הפיקוד, תריץ אותו ואת הפלט שלו תצפין ותחזיר.

בצעו את ההצפנה באמצעות הפונקציות שמימשתם בתרגיל 2, כלומר השתמשו בפונקציות encrypt_data וdecrypt_and_validate_data שכבר מימשתם. על המפתח להיות בקובץ ה settings של הפרויקט, תחת השם RSA_KEY (במחשב הפיקוד יהיה המפתח הפרטי, אצל הנוזקות יהיה המפתח הציבורי). בקובץ הsettings שלכם השתמשו בצמד המפתחות:

תוקף (פרטי) - (d, n) = (90687, 57101017)
נוזקה (פומבי) -(e, n) = (10013807, 57101017)

בדקו שהכל עובד כמו שצריך, ובואו נתחיל לכתוב פיקודים!

טכנו"צ סייבר - תרגיל 4 - "Tr0j4n"

שלב 2 - פיקודים

בשלב זה נבנה מספר פיקודים שימושיים אותם נוכל לשלוח לנוזקה שלנו. נכון לברגע הקוד שלנו מניח שהפיקוד שלנו הוא קוד Python שעלינו להריץ. על גבי זה נבנה ארבעה פיצ'רים נחמדים:

1. הוסיפו לתוקף פונקציה ששמה dir_list, שמקבלת פרמטר אחד המייצג שם של תיקיה. הפונקציה תשלח פיקוד לנוזקה. הפיקוד יבדוק אילו קבצים נמצאים בתיקיה, וישלח לתוקף את רשימת הקבצים בתיקיה. הפונקציה dirlist תחזיר את רשימת הקבצים שהתקבלה.

2. הוסיפו לתוקף פונקציה ששמה get_file, שמקבלת פרמטר אחד המייצג שם של קובץ אותו על הנוזקה להדליף. הפונקציה תשלח פיקוד לנוזקה. הפיקוד יפתח את הקובץ (לאו דווקא קובץ טקסט), ויקרא את התוכן של הקובץ למשתנה. המשתנה יעבור קידוד base64 (כדי שבמידה ובמדובר במידע בינארי זה לא ייראה כמו זבל), ויישלח לתוקף. לכשהפונקציה תקבל בחזרה את התוכן של הקובץ, היא תקודד בחזרה את המידע ותחזיר אותו. התוקף ישמור את הקובץ על המחשב שלו תחת אותו השם.

3. הוסיפו לתוקף פונקציה ששמה take_screenshot. הפונקציה תשלח פיקוד לנוזקה. הפיקוד יבצע צילום מסך על המחשב הנתקף, ישמור את המידע הבינארי שלו במשתנה, ויפעיל על המידע הבינארי קידוד base64 (כדי שזה לא ייראה כמו זבל). את המידע הזה הפיקוד יעביר בחזרה לתוקף. לכשהפונקציה take_screenshot תקבל את פלט הפיקוד בחזרה, היא תקודד בחזרה את המידע ותשמור אותו לקובץ screenshot.jpg על המחשב התוקף.

4. הוסיפו לתוקף פונקציה ששמה my_command. הפונקציה תשלח פיקוד לנוזקה. החליטו בעצמכם איזה פיקוד אתם רוצים לשלוח ומה אתם רוצים שהוא יעשה, וצרפו לREADME הסבר על הפיקוד שכתבתם. נסו לכוון לפיקוד שמעניין בתרחיש המבצעי, שמרגיש לכם שונה מהשלושה האחרים.

בונוסים מעשיים

בשלב זה נוסיף מספר פיקודים נוספים (כל אחד מהם הוא בונוס נפרד, מוזמנים לעשות מה שמעניין אותכם)

1. Persistence - הוסיפו פיקוד אשר גורם לכך שהווירוס שלכם ידלק כל פעם שהמחשב המותקף ידלק
2. Tunnel - הוסיפו אופציה להדליק פורט TCP כך שכל ההודעות TCP שמגיעות בפורט הזה, יעברו למחשב יעד (שגם יהיה כלול בפיקוד) בשם המחשב המותקף.

טכנו"צ סייבר - תרגיל 4 - "Tr0j4n"

3. Encrypt - הוסיפו פיקוד אשר מאפשר לכם להצפין למחשב המותקף את אחד הקבצים. הצפינו את הקובץ באמצעות מפתח ראנדומלי והצפנת בלוקים כלשהי, הצפינו את המפתח הראנדומלי באמצעות המפתח הפומבי והצמידו אותו ליד הקובץ
4. Proxy - כתבו פיקוד אשר מאפשר לכם לגשת לאתר אינטרנט באמצעות המחשב המותקף (כלומר התעבורה תעבור דרכו)
5. Shell - כתבו פיקוד אשר מדליק Batch אינטראקטיבי
6. Troll - שנו את תמונת הרקע של המחשב המותקף לתמונה של כלב כלשהו (עדיפות על ויסלה)

ממשק פיקוד - שנו את ה main של ה commander כך שהוא יאפשר לבחור להתחבר לכתובת IP נתונה מהמשתמש, הוסיפו לו תפריט והסבירו עליו ב README.

בונוסים על הבונוסים

זה חלק שהוא באמת לחלוטין סתם לכיף, שלבו את תרגיל 1 ואת תרגיל 4. בשלב זה יש לכם ווירוס שעובד. הרימו VM והדגימו שימוש של הווירוס שלכם על ה VM הזה (**צלמו סרטון וצרפו להגשה**)

השלמה MiniNet

עקבו אחר ההוראות לתרגול MiniNet ועקבו אחריהן, הוסיפו את התשובות לשאלות לקובץ ה README.

הגשה

הגישו קובץ zip שעוטף את כל תיקיית התרגיל שלכם (התיקיות commander, malware, global וקבצי main) בשם ex4_FullName.zip. שימו לב שגם קוד ההצפנות צריך לשבת בתוך הzip. אל ה zip צרפו README שבו תסבירו על הפיקוד הרביעי שיצרתם בעצמכם ועל הבונוסים שעשיתם במידה ועשיתם.

בהצלחה!