רשתות מחשבים בגישה מחקרית – תרגיל מסכם לסייבר עלית

ברק גונן

IPCalc

ראשת שירות הבטחון תופפה בעצבנות באצבעותיה על השולחן. "יש לנו סוכן במדינה זרה שחייב להעביר אלינו מסר באופן מיידי. לצערנו, המדינה הזרה הצליחה להגיע אל המחשב שלו ולהתקין שם תוכנת ריגול, כך שהם יכולים להאזין לכל התעבורה שלו. מה עושים?"

בחדר השתררה שתיקה עצבנית. "ממידע מודיעיני שיש לנו, תוכנת הריגול יכולה להאזין לכל מה שעובר מעל סוקטים כלשהם, בין אם TCP או UDP. נראה שהלך עליו" אמר מפקד המבצע.

לפתע נזכרתם במשהו שלמדתם פעם, מזמן. הרמתם יד ושאלתם בהיסוס "יש לסוכן אפשרות להתקין על המחשב סקאפי ופייתון?"

"כן" אמר מפקד המבצע "איך זה עוזר?"

מעודדים, הסברתם את התכנית: "אפשר לשלוח Raw data מעל IP, בלי לעשות שימוש ב-TCP או UDP. נמציא פרוטוקול משלנו שיודע לפענח מה עובר ב-Raw data, הסוכן יריץ את הלקוח ואנחנו נריץ את השרת. מי שמפלטר את תעבורת ה-TCP / UDP של הסוכן לא ימצא כלום. מה הסוכן צריך לשלוח?"

"המסר הסודי כולל מספר בן 8 ספרות" הסביר המפקד "ואנחנו צריכים למצוא דרך למסור לסוכן שהמסר שלו הגיע אלינו בהצלחה"

"אין בעיה. לאחר המסר הסודי הסוכן יוסיף את אחד התווים של פעולות החשבון הבסיסיות +,-,* או /. התשובה שנחזיר לו הפעולה החשבונית בין 4 הספרות הראשונות לבין 4 הספרות האחרונות. לדוגמה אם הסוכן שלח-

12345678+

אז נחזיר לו 6912

אם הסוכן שלח-

12345678/

אז הוא יקבל 0.217330045..."

"אוקיי הבנו אותך" אמר מפקד המבצע "מעניין מה יחשבו ארגוני המודיעין הזרים אם יעלו על המסרים שאנחנו מחליפים עם הסוכן"

ראשת שירות הבטחון השיבה בסמכותיות "הם יחשבו שלישראלים אין מה לעשות חוץ מאשר לפתח מחשבון כיס. יש לך בדיוק שעתיים לסיים את השרת והלקוח. קדימה לעבודה, צאו לי מהחדר"

<u>קובץ לקוח</u>

יש לכתוב קובץ לקוח שמקבל קלט מהמשתמש, שמונה ספרות ופעולת חשבון, שולח אותו אל השרת (לצורך הפיתוח השרת ירוץ על המחשב של הלקוח, אך אין להתבסס על כתובת IP ספציפית בשום שלב. במילים אחרות, כדי להריץ את הלקוח על מחשב אחר, כל מה שצריך לעשות הוא רק לשנות את כתובת ה-IP של היעד)

הקלט יתקבל באמצעות פרמטר לסקריפט, לא באמצעות input.

הלקוח לא צריך לבדוק את תקינות המידע שהמשתמש מזין.

הקלט חד פעמי, אין צורך לרוץ בלולאה.

<u>קובץ שרת</u>

יש לכתוב קוד שרת שמקבל את התרגיל מהלקוח פותר אותו ושלוח אל הלקוח.

<u>קובץ פרוטוקול</u>

קובץ שהן השרת והן הלקוח ישתמשו בפונקציות שלו.

יש לכתוב פילטר מתאים, שאוסף רק את הפקטות של הפרוטוקול שלנו. שימו לב- אפשר להוסיף למידע שדות כרצונכם, או לשנות שדות קיימים בפרוטוקול IP, כל עוד הדברים עובדים הכל מותר. חשוב מאד לתעד את הפרוטוקול ולהסביר את פונקציית הפילטר.

הקובץ יכלול את הפונקציה שמחשבת את התוצאה של פעולת החשבון בין 8 הספרות.

הקובץ יכלול את כל הקבועים הנדרשים בשרת ובלקוח.

<u>דגשים:</u>

1. הלקוח יידע להתמודד עם מצב שבו לא התקבלה תשובה, ולא יחכה לנצח
2. השרת לא יקרוס על שום קלט שהלקוח ישלח לו
3. הקוד יעשה שימוש בקבועים, ללא הערות PEP8, חלוקה הגיונית לפונקציות, הפרוטוקול והפילטר מתועדים היטב