מבוא לתקשורת נתונים - תרגיל תכנות

(האקתון) - גירסה 1.0

מבוא

מטרת הפרוייקט היא להשתלט על רשת של מחשבים נגועים (botnet) ולהשתמש בה כדי להפיל קורבנות באמצעות התקפת distributed denial of service (DDoS).
כדי לממש את המערכת הזו תידרשו לממש שלוש אפליקציות מבוזרות:

1. שרת שליטה ובקרה (שו"ב או C&C). השרת הזה מתקשר עם המשתמש, אוסף כתובות של מחשבים נגועים ולבסוף משתמש בהם כדי לתקוף את הקורבן שהמשתמש בחר.
2. מחשב נגוע (bot). הבוט יפרסם את קיומו ברשת, ובמידת הצורך יענה לפקודה של שרת השו"ב ויתקוף את הקורבן. אתם אמורים להריץ 10 עותקים או יותר של התוכנה הזו במקביל על המחשב שלכם או על מחשבים אחרים ברשת.
3. הקורבן (victim) ידפיס את הכתובת בה הוא עלה למסך, ואם מתחברים אליו יותר מ-10 בוטים באותה השנייה הוא ידמה קריסה ע"י הדפסת הודעה.

תיאור אינטראקציה

V1: הקורבן עולה, בוחר באקראי סיסמא (מחרוזת בת 6 ספרות בין a ל-z), פורט TCP להאזין לו ומדפיס למסך "Server listening on port xxxx, password is xxxxxx"
B1: הבוט עולה, בוחר באקראי פורט UDP להאזין לו, מדפיס למסך "Bot is listening on port xxxx".
B2: הבוט שולח הודעת bot announcement בה הוא מציין מה הפורט אליו הוא מאזין (ראו סעיף הבא). הבוט ישלח הודעה כזו פעם ב-10 שניות.
C1: שרת השו"ב עולה ומדפיס "Command and control server nnnn active", כאשר nnnn הוא השם המקורי שבחרתם.
C2: שרת השו"ב מאזין ברקע להודעות bot announcement, ומרכיב לו מבנה נתונים עם ה-IP וה-port של כל הבוטים שראה.
C3: שרת השו"ב צריך לקלוט מהמשתמש את הפרמטרים של הקורבן: IP, port, password.

C4: שרת השו"ב מדפיס למסך "attacking victim on IP xxxx, port xxxx with n bots", כאשר n הוא כמות הבוטים שהשרת מצא
C5: שרת השו"ב שולח הודעת bot activate לכל אחד מהבוטים שהוא שמע מהם bot announcement, בה הוא רושם את הפרמטרים: IP, port, password וכן את השם המקורי של שרת השו"ב
B3: הבוט מקבל הודעת bot activate ומתחבר ב-TCP לקורבן בפורט ובכתובת ה-IP המצויינת
V2: הקורבן שולח לבוט את המחרוזת "Please enter your password\r\n"
B4: הבוט שולח לקורבן את הסיסמה שקיבל משרת השו"ב ואחריה \r\n) ENTER)
V3: הקורבן בודק את הסיסמא. אם היא לא נכונה הוא מנתק מייד. אם היא נכונה הוא רושם "Access granted".
B5: הבוט שולח לקורבן את השורה "Hacked by nnnn\r\n", כאשר nnnn הוא השם המקורי של השו"ב
V4: הקורבן בודק אם היו 10 התחברויות מוצלחות בשנייה האחרונה (תכל'ס, שומר במבנה נתונים את השעה הנוכחית ובודק מה יש במבנה עד עכשיו). אם לא הוא שומר את הזמן הנוכחי ברשימה שלו. אם כן, הוא מדפיס למסך את השורה שהבוט שלח לו. בשני המקרים הקורבן מנתק מייד ומתכונן לחיבור הבא.

מבנה הודעות

<u>bot announcement</u>:
Destination IP = broadcast (255.255.255.255)
Transport protocol = UDP
Destination port = 31337
Message contents: Listening port (16-bit value in net order)
Total application protocol message size: 2 bytes

<u>bot activate:</u>
Destination IP = IP address of bot
Transport protocol = UDP
Destination port = Listening port of bot
Message contents: IP address of victim (4 bytes), port of victim (2 bytes), password (6 bytes), name of C&C server (32 bytes exactly)
Total application protocol size: 44 bytes

<u>bot-victim communications (over TCP)</u>:
B (connects to V)
V->B: Please enter your password\r\n
B->V: blabla\r\n
V->B: Access granted\r\n
B->V: Hacked by SuperCyberFragilistic
V (disconnects)

המלצות למבני נתונים

שרת שו"ב: רשימה של בוטים שזוהו ברשת, כל אחד עם IP ופורט. UDP socket לצורך האזנה לפירסומות של הבוטים ולצורך משלוח הוראות לבוטים.
בוט: UDP socket לצורך משלוח פרסומות וקבלת הוראות. TCP client socket לצורך תקשורת עם הקורבן.
קורבן: רשימה של כמה זמני התחברויות המוצלחים האחרונים. TCP server socket לצורך תקשורת עם הבוטים.

הנחיות כלליות

1. כמובן שהכל בכאילו, בבקשה אל תפילו את הרשת של האוניברסיטה או של הפנטאגון.
2. שרתי השו"ב של כל הצוותים צריכים לעבוד עם הבוטים של כל הצוותים ולתקוף את הקורבנות של כל הצוותים.
3. ה"בוט" ,"קורבן" ו"שוב" צריכים להיות "פרוייקטים" שונים של C#, כך שניתן יהיה להפעיל כל אחד בנפרד בלי תלות אחד בשני. כמו כן, כל הפרוייקטים צריכים לדעת לפעול על אותו המחשב - לא צריך שלושה מחשבים!
4. כדי לקבל ניקוד מלא, על הקוד להיות באיכות גבוהה: שימוש נכון בהערות וב-whitespace, מתן שמות הגיוניים לקבצים, לפונקציות ולמשתנים, טיפול בערכי שגיאה וכו'.
5. האפליקציות שלכם אמורות להתמודד בחינניות עם מצבים קיצוניים בממשק המשתמש וברשת, כגון: הודעות בפורמט לא נכון שנשלחות בשם השו"ב, בשם הבוט או בשם הקורבן, קורבן שמנתק באמצע, משתמש שנותן קלט שגוי וכו'. אל תאמינו לאף אחד!
6. ההגשה היא בזוגות בלבד!
7. שפת ההגשה היא C#
8. אתם מוזמנים לתת לשרת השו"ב שלכם שם יצירתי ככל העולה על רוחכם. אנחנו נעניק פרס לשם היצירתי ביותר.

בונוס על השתתפות בניסוי

במהלך ההאקתון תוזמנו להשתתף בניסוי שעורכים תלמידים משנה ד' במסגרת פרוייקט הגמר. ההשתתפות הינה רשות ומזכה בנקודת בונוס אחת לציון הסופי בקורס.

פצחנות נעימה!