גירסה 1.00 - 28.8.1999
גירסה 2.00 - 29.6.2003

IRC Hack - Netsplit & Clones

מסמך זה הורד מהאתר http://underwar.livedns.co.il.
אין להפיץ מסמך זה במדיה כלשהי, ללא אישור מפורש מאת המחבר.
מחבר המסמך איננו אחראי לכל נזק, ישיר או עקיף, שיגרם עקב השימוש במידע המופיע במסמך, וכן לנכונות התוכן של הנושאים המופיעים במסמך. עם זאת, המחבר עשה את מירב המאמצים כדי לספק את המידע המדויק והמלא ביותר.

Nir Adar
Email: underwar@hotmail.com
Home Page: http://underwar.livedns.co.il

אנא שלחו תיקונים והערות אל המחבר.

הקדמה - למה בכלל לפרוץ ערוצים ב-IRC?

שרתי IRC משמשים מקומות אירוח לערוצים רבים, בהם אנשים מדברים ומכירים.
לכל חדר שיחות (=ערוץ) ישנם מספר מנהלים, אופים, השולטים בחדר, ומחליטים מי יישאר בפנים ומי בחוץ. כאשר האופים אינם מעוניינים בנוכחות שלנו בחדר שלהם, השאלה מי צריך לנהל את החדר באמת הופכת להיות שאלה אישית :).
סיבה נוספת להתעניינות בשאלה "איך פורצים" היא עניין, המתבטא בשאלה - "האם אני באמת מסוגל לעשות את זה?".

לפרוטוקול אציין שאני לא תומך בשימוש בשיטות שאתאר בהמשך כדי "לפרוץ" לשרתים באינטרנט, ובמילא הן יעבדו רק על שרתים ישנים או רשתות קטנות. הרשתות הגדולות כבר מזמן דאגו להגנה מפניהן.

כלים נדרשים

- תוכנה בשם Link-Looker, או תוכנה דומה, המאתרת Net-splits ברשת IRC.
- סקריפט IRC המותאם להתקפה שאותה רוצים לבצע.

השתלטות על ערוץ

התקפה על ערוץ מורכבת משני חלקים עיקריים:
החלק הראשון - השגת אופ.
החלק השני - שמירה עליו. השמירה על האופ נעשית על ידי הורדת האופ משאר האופים בערוץ, וכך בעצם להפוך למנהלים היחידים שלו.

השגת האופ

השיטה הראשונה להשגת אופ היא פשוט לבקש אופ מהמנהלים, ואם במקרה אחד מהם הסכים לתת לנו אופ, נתחיל בהשתלטות על הערוץ.
אפשר לנסות להשתמש בשיטה הזו, ולדעתי זו אחת השיטות היותר נחמדות.
אבל, שיטה זו לא תעבוד תמיד.
האמת, כמעט אף פעם לא.

ולכן נציג שיטה נוספת. השיטה מתבססת על Net-Splits.
מהו Net-Split?
כאשר אנחנו מתחברים אל רשת IRC, אנו מתחברים למעשה אל שרת אחד מתוך רבים המרכיבים ביחד את הרשת. בין השרתים השונים המרכיבים את הרשת ישנו קשר שוטף, באמצעותו השרתים מעדכנים אחד את השני לגבי האנשים הנמצאים בכל אחד מהערוצים, וגורמים למעשה לרשת כולה להראות כאיזור שיחות גדול אחד.
Split מתרחש כאשר אחד משרתי ה-IRC מתנתק משאר השרתים לכמה זמן. הסיבות לכך מגוונות, ובפועל מתרחשים לא מעט splits. בזמן split, אם אתה נמצא בערוץ מסוים, ואתה היחיד שמחובר לערוץ זה דרך אותו השרת שמתנתק, תמצא את עצמך לבד בערוץ ברגע ההתנתקות. כל שאר המשתמשים בערוץ ייראו כאילו עזבו אותו.
ברגע זה אנו יכולים לנצל את אחד מהעקרונות עליו מבוסס שרת IRC כדי לקבל OP. הרעיון הוא זה: המשתמש הראשון שנכנס לערוץ מקבל אופ, ונהיה המנהל שלו. לפיכך, אם אנו נמצאים לבד בערוץ עקב ה-split, ונצא ממנו ונכנס אליו מיד שוב, נמצא את עצמנו בעלי אופ. כאשר השרת יתחבר שוב אל שאר הרשת, נמצא את עצמנו ברשימת האופים של הערוץ, ומכאן שתהיה בידינו האפשרות להשתלט עליו.

מתעוררת השאלה כיצד למצוא שרת שמתנתק מהרשת לכמה זמן. אם נבחר שרת בצורה אקראית ונחכה שיתנתק, עלול לעבור זמן רב.

בעיה זו נפתרת על ידי תוכנות בסגנון התוכנה Link Looker. תוכנה זו ודומותיה מתחברות אל רשת ה-IRC ומקשיבות, מחכות לרגע שבו שרת יתפצל מהשאר.
ברגע שתוכנה כזו מוצאת שרת שהתנתק, היא מודיעה על כך למשתמש, וההתקפה יכולה להתחיל להתבצע.

שמירה על האופ

נניח שכתוצאה מפעולה כלשהי יש בידינו כעת אופ בערוץ שאנחנו רוצים להשתלט עליו.
הסכנה המיידית היא שהאופים המצויים בערוץ ישימו לב שקיבלנו את האופ, ויורידו אותו.
לפיכך, בשלב הזה דרושה מהירות. כאשר אנחנו מתכוננים להשתלט על ערוץ, נכתוב סקריפט IRC, או תוכנית ב-C שתתחבר לשרת ה-IRC, שפעולתה תהיה הורדה המונית של כל האופים בערוץ, בשניה שהשרת מדווח לנו שקיבלנו אופ. לעתים השרת מאפשר לתת או לקחת מספר אופים בו זמנית. במידה וכך, הסקריפט צריך להשתמש באפשרות זו, על מנת לטפל כמה שיותר מהר בכל האופים.
הגנה נפוצה הנהוגה בערוצים היא רובוטים המזהים התחלה של פעולת השתלטות, ומיד מורידים את האופ של התוקף. במידה וידוע שיש בערוץ רובוטים כאלו, כדאי להוריד להם את האופ במהירות האפשרית.
בנוסף ניתן לשלב שני clients שיתחברו אל השרת, ויתנו אופ אחד לשני במקרה ומורידים לאחד מהם אותו.
כתיבת סקריפט כמתואר איננה משימה קשה. אפילו אנשים שאינם מתכנתים, יכולים להשתלט למשל על שפת ה-mIRC Scripts במהירות ולכתוב סקריפט שיבצע את ההתקפה.

Clones Attack

ישנה התקפה נוספת שניתן לבצע כדי להשתלט על הערוץ, והיא מעט מורכבת יותר, אולם גם בטוחה יותר. ההתקפה מתבססת על כך שנהיה מחוברים ל-IRC בו זמנית דרך שני clients. אחד יהיה מחובר אל השרת בו קרה ה-split, והשני יהיה מחובר אל שאר הרשת.
כאשר מתרחש split, נביט מי הם האופים הנמצאים בערוץ.
נתחבר בעזרת clients נוספים אל השרת שהתפצל מהרשת, וניתן להם כינויים זהים לאלו של האופים של הערוץ.
כאשר הרשת תתחבר שוב, שרתי ה-IRC יגלו התנגשות שמות - שהיא מספר clients שונים המחוברים עם אותו הכינוי (האופים עם הכינויים שלהם, וה-clients שהפעלנו, ודאגנו שיהיה להם את אותו כינוי כמו לאופים). בתגובה לכך הרשת תנתק את כל ה-clients להם שמות כפולים - והערוץ יישאר ללא מנהליו הקודמים.
הגנה שלעיתים מופעלת כנגד התקפה כזו, היא שהאופים משנים את הכינוי שלהם (לעתים בצורה אוטומטית) מיד עם גילוי split, תוך הנחה שהתוקף ינסה להשתמש בכינויים שלהם מלפני התרחשות הפיצול. על ידי שינוי הכינוי הם מבטיחים שאם התוקף אינו נמצא בערוץ וצופה בהם, אז לא יהיה ניתן להפעיל כנגדם התקפת "התנגשות שמות".

DOS using Clones Attack

נושא שני הקשור לאבטחה של שרתי IRC הוא התקפת Clones על השרתים עצמם.
להתקפה כזו ישנן שתי מטרות עיקריות:

- ההתקפה עלולה לגרום לשרת עליו היא מופעלת לקרוס. התקפה מתוכננת היטב יכולה להפיל את הרשת.
- ההתקפה יכולה לגרום לניתוקו של השרת עליו היא מופעלת משאר הרשת. במקרה כזה מתרחש Net-Split, וניתן לנצלו למטרות כגון השתלטות על ערוץ.

ההתקפה מבוססת על Clones - מספר רב של clients המתחברים בו זמנית אל שרת ה-IRC.
כפי שצויין, השרתים השונים ברשת מעדכנים כל העת אחד את השני לגבי הקורה בהם, על מנת ליצור אשליה שכולם למעשה איזור שיחות אחד גדול (ולא מספר איזורים שיחה נפרדים).

כעת, אם נתחבר עם מספר רב של clients אל אחד השרתים, ונבצע פעולות רבות - למשל, ניכנס ונצא מערוץ ללא הפסקה, אותו שרת ידווח על כל פעולה כזו לכל שאר השרתים. אם נתחבר ונבצע מספר רב של פעולות בעזרת לקוחות רבים, השרת עלול שלא לעמוד בעומס ולקרוס. לחילופין, עקב קצב התעבורה שגדל עקב ההתקפה בצורה משמעותית, השרתים האחרים בד"כ ינתקו זמנית את השרת מהם, כדי למנוע "פקק" בהעברת המידע של שאר המשתמשים בהם. במקרה כזה השרת יפוצל מהרשת ויתרחש Net-Split.

EOF