DENIAL OF SERVICE ATTACK

מסמך זה הינו משותף לאתר http://underwar.livedns.co.il ולאתר http://www.ihfb.org.
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.
אין במידע האמור במסמך זה להביע על הלגיטימציה שנותן המחבר לנושאים הנדונים.
הערה: מסמך זה נכתב בשנת 1999 – ולכן יתכן שאינו מעודכן לגמרי.

כל הזכויות שמורות ל**ניר אדר**

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

אנא שלחו תיקונים והערות אל המחבר.

DENIAL OF SERVICE ATTACK אלו התקפות על שרתים, במטרה לגרום להם ליפול.
במסמך זה נסקור מספר שיטות להפלת שרתים. המסמך מתבסס ברובו על מסמך אנגלי באותו נושא.
עבור חלק מהשיטות תצטרך Linux או Unix Shell.

קשה לומר בבירור אילו שרתים יותר מוגנים מ-DENIAL OF SERVICE ATTACK (מעכשיו אקרא לזה בקיצור DOS). זה תלוי מאוד במנהל המערכת ובמה שהוא עושה על מנת להגן על המערכת שלו. בד"כ שרתי Unix עמידים יותר בפני התקפות מבפנים משרתי Windows NT או Windows 95, אולם שרתי Windows NT ושרתי Windows 95 עמידים יותר להתקפות מאנשים מבחוץ (מכיוון ששרתים אלו מריצים בד"כ פחות שירותים על הערוצים השונים).

אם תתקיף שרת, ותרצה לבדוק לאחר מכן האם הוא עדיין פעיל, השתמש ב-Ping.
מ-Unix Shell או DOS Shell כתוב:

ping <HostName>

כאשר <HostName> הוא השרת אותו אתה מנסה להפיל.

<u>התקפות מבחוץ</u>

<u>התקפה בעזרת Finger</u>

חלק מ-Finger Demons מאפשרים הכוונה של ה-Finger.
ראה לדוגמא את השורה הבאה:

$ finger @system.two.com@system.one.com

אתה בעצם מבצע Finger על system.two.com. system.two.com חושבת שבעצם system.one.com היא זאת שביצעה את ה-Finger.

שיטה זו יכולה לעזור לך להסתיר את עצמך, אבל גם יכולה לעזור לך לעשות התקפה על השרת.
הבט בשורה הבאה:

$ finger @@@@@@@@@@@@@@@@@@@@@@@@@@@@@host.we.attack

אנו גורמים לhost.we.attack לעשות לעצמו Finger שוב ושוב. התוצאה של פעולה זאת היא עומס לשרת, מילוי הזכרון הפנוי של השרת, מילוי ה-HD שלו (כתוצאה מכל ה-child processes הנוצרים).

ניתן להתגונן מהתקפה זו על ידי התקנת Finger Demon שלא תומך בהכוונה.

SunOS 4.1.3

ב-SunOS 4.1.3 ישנו באג שגורם למערכת להיתקע אם UDP Packet עם header לא תקין נשלח אל המערכת.
הפתרון לבעיה זו הוא להתקין תיקון מתאים למערכת.

X-WINDOWS

אם שרת מאפשר גישה לערוץ של X-WINDOWS (בדרך כלל הערוץ הוא בין 6000 ל6025), ניתן לגרום ל-X-WINDOWS לקרוס.
ניתן לעשות זאת על ידי התחברויות מרובות לערוץ של ה-X-WINDOWS.
הפתרון הוא לא לאפשר גישה לערוץ זה.

התקפה על שרת HTTPD

בשרתים המריצים httpd, נפתח process נוסף של httpd על כל קליינט שמתחבר למערכת. אם יוצרים הרבה קשרים לערוץ 80, המערכת עלולה להאט עקב בעיות זיכרון, ואף לקרוס.
בצד השרת ניתן לגלות את ההתקפה על ידי הפקודה netstat.

נעילת חשבונות

אם אתה רוצה לנעול חשבון מסוים במערכת מסוימת, כלומר לגרום לכך שאי יהיה אפשר להשתמש באותו חשבון (עד שמנהל המערכת יסדר מחדש את החשבון), ניתן להשתמש בשיטה הבאה.
נסה להתחבר אל אותו החשבון פעמים רבות, ולהקיש סיסמאות שגויות. בהרבה מקרים, לאחר מספר פעמים, המשתנה בין מערכת למערכת, החשבון ינעל לשימוש.

Novells Netware FTP server

שרת FTP זה ידוע בכך שהוא גורם למחשב המריץ אותו לרדת לרמה מסוכנת של זיכרון, אם מספר קליינטים מתחברים אליו בו זמנית.

EMAIL BOMBING

גם בעזרת שיטה זו אפשר להזיק לשרתים.
שולחים לאתר מסוים כמות גדולה של EMAIL.
אם השרת אינו מוגדר בצורה נכונה, הדיסק הקשיח של השרת יכול להתמלא לחלוטין, ולגרום לנפילת השרת.
פתרון ñ במערכת מבוססות UNIX לעשות מחיצה מיוחדת (partition) בדיסק שתכיל את הדואר המתקבל, כך שגם אם מחיצה זו תתמלא לחלוטין עדיין ה-Hard Disc של המחשב לא יוכל להתמלא לחלוטין.

SunOS KERNEL PANIC

דרך נוספת להפיל חלק משרתי SunOS היא להתחבר ולהתנתק מהם במהירות. חלק מהשרתים יתקעו עם הודעת KERNEL PANIC.

ANONYMOUS FTP ABUSE

לעיתים ניתן להעלות קבצים לשרת דרך ANONYMOUS FTP. במצבים כאלו ניתן להעלות קבצים כך שהדיסק הקשיח של השרת יתמלא, והשרת ייפול.
ניתן להתגונן מהתקפה זו על ידי כך שמבטלים את האפשרות של משתמשים אנונימיים להעלות קבצים אל השרת.

PING FLOODING

שיטת הצפת Ping יעילה על מנת להפיל או להאט שרתים.
בUNIX ניתן לנסות את הפקודה:

```
$ ping -s host
```

ב-windows 95 אפשר לנסות:

```
PING -T -L 256 xxx.xxx.xxx.xx
```

אם פותחים יותר מחלון אחד לעשות איתו את הPING, ההתקפה תהיה יעילה יותר.