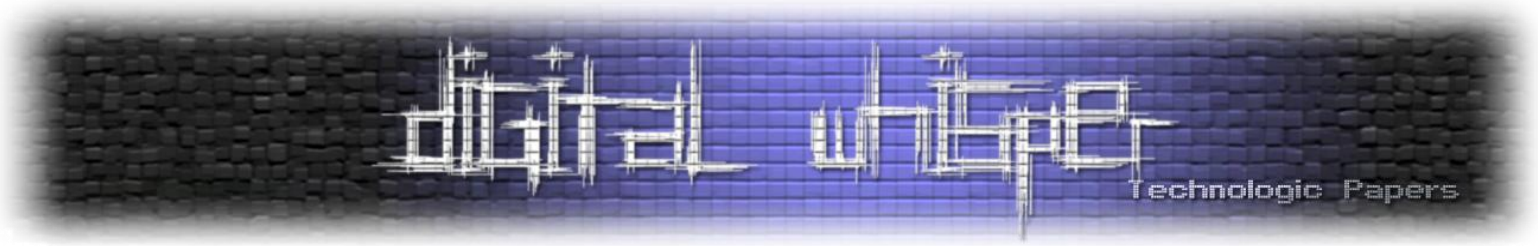


HoneyPots

מאת נתנאל שיין

הקדמה

"Suppose," he said to Piglet, "you wanted to catch me, how would you do it?"
"Well," said Piglet, "I should do it like this. I should make a Trap, and I should put a Jar of Honey in the Trap, and you would smell it, and you would go in after it."
- Winnie The Pooh.

"**מלכודת דבש**- דבר מפתה שיש בו יתרון מיידי, אבל בטווח הארוך הוא עתיד לפגוע במקבלו. במקור: כינוי מעולם הריגול לנערת פיתוי (המופעלת לרוב לשם סחיטה)."
(לקוח ממילון השפה העברית- http://www.safa-ivrit.org).

כידוע, ישנן הקבלות רבות בין העולם האמיתי לווירטואלי, והקבלה זו של מלכודות הדבש היא לטעמי אחת המוצלחות. בטרמינולוגיה של מחשבים, מלכודות דבש או Honeypots הן מלכודות המוקמות על מנת להבחין, לשנות ובמובן מסוים לנטרל ניסיונות לשימוש לא מורשה במערכות מידע. בדומה ל-"נערת פיתוי", המלכודת בנויה כך שהיא מצטיירת בתור מחשב או מיקום ברשת המכילים מידע אטרקטיבי לתוקף, אך למעשה היא מבודדת, מוגנת ומנוטרת. שיטת פעולה זו "מפתה" את התוקף לפרוץ למלכודת ומאפשרת לגורם שהציב אותה לנטר ולנתח את כל פעולותיו של התוקף ברשת. מלכודת הדבש היא כלי מאוד גמיש עם אפליקציות מגוונות, המלכודות לא מספקות מענה לבעיה בודדת אלא בעלות שימושים מרובים כגון מניעה, זיהוי או איסוף של מידע.

ישנן כמה סוגים של מלכודות הדבש, אך לכולן עיקרון משותף- הקמת מלכודות דבש ברשת לא צריכה להשפיע על אפליקציות ושירותים אחרים ברשת. החשיבות של מלכודות הדבש טמונה בעובדה שהן צריכות להיות מועדות לפריצה, לתקיפה או לסכנות אחרות.

מטרת המאמר לסקור, לתאר, לנתח ולהסביר את מנגנון מלכודות הדבש ואת השימוש בו, על כל זוויותיו החשובות ביותר.

הצורך

הצורך לפתח מלכודות דבש התפתח עקב הרצון שלנו לבסס ולשכלל את ההגנה על המידע שלנו. מדובר באחת משכבות רבות המשמשות לריבוד והגנה מיטבית על כל מידע עליו נרצה להגן.

האינטרנט הוא אחד המשאבים הכי חשובים לנו כיום- זהו מאגר הידע הגדול ביותר בעולם, הוא משמש לתקשורת ושיתוף מידע, לביצוע קניות ורכישות, הכרויות, צרכים בטחוניים וכן הלאה. אי לכך, מספר המשתמשים בו גדל באופן משמעותי מדי שנה. יחד עם הקדמה והתפתחות החשיבות של האינטרנט, התפתחו גם האיומים על המידע העצום המשותף, מועבר ומאוחסן מדי יום ברשת. על מנת להתמודד עם איומים אלו התפתחו פתרונות אבטחה שונים ומגוונים כדוגמת מערכות אנטי ווירוס, חומות אש, ומערכות IDS. פתרונות אלו מספקים מענה יפה לבעיות שאנו נתקלים בהן באינטרנט, אך האם הן מספיקות? האם אנחנו מכירים מספיק טוב את האויב מולו אנו עומדים? האמת היא שמערכות אלה יהיו תמיד במרדף אחרי הכובעים השחורים, ולצערנו הרב, תמיד צעד אחד מאחוריהם.

בדיוק למטרה זו פותחה מערכת ה-Honeypot, על מנת שתהיה צעד אחד לפני האויב. זו מערכת מחשב שנועדה להיות מטרה "מפתה" להאקרים ומטרת העל שלה היא איסוף מידע אודות התוקף ועל תהליך ההתקפה, דבר המסייע בהבנה של המניע, ההתנהגות ואת דרך האירגון של אותה התקפה על מנת ליצור הגנה טובה יותר ולמנוע התקפה זו בעתיד. בהשוואה למערכות IDS, למערכת Honeypot יש יתרון אחד גדול- היא לא מייצרת התרעות שווא על תעבורה חשודה מכיוון שאין שום רכיב פעיל שרץ במערכת. עובדה זו עוזרת למערכת לתעד כל ביט של מידע שעובר במערכת ולהצליבו עם מקורות מידע אחרים, על מנת לצייר תמונה אחת אודות ההתקפה והתוקף.

מערכות Honeypots מספקות מידע רב יותר מהנצפה, ולרוב משמשות אף לזיהוי התקפות ותולעים חדשות. הדבר המיוחד ב-Honeypot הוא שמדובר בטכנולוגייה המבוססת על כך שקיימים אנשים בעלי כוונות זדוניות. כל המערכות מסוג זה עובדות על אותו עיקרון- אף אחד לא אמור לגשת אל המערכת, וברגע שמישהו יוצר חיבור- זה מדובר בפעולה ללא אישור.

סוגי מלכודות הדבש

סיווג מלכודות דבש על פי מטרתן

מערכות ה-Honeypot לא יודעות לעשות הכל- וגם אין בכך צורך. ישנם כמה סוגים של מערכות דבש, אשר מחולקות לקטגוריות שונות לפי מטרתן: מטרת הגנה, מטרת מחקר, Honeytokens- מלכודות שאינן מהוות מחשב.

1. Production Honeypots- מלכודת למטרת הגנה

סוג זה הוא הנפוץ ביותר ביותר מבין מלכודות הדבש. מלכודת זו נמצאת בשימוש של אירגונים ובסביבות עבודה שונות, על מנת להגן על האירגון ולסייע בהקטנת הסיכונים. מערכת זו מועילה ביותר משום שהיא מספקת הגנה מידית למשאבי האתר. היות ומדובר במערכת קלה יחסית לתפעול מאשר מערכת למטרות מחקר, קל להטמיעה באירגונים שונים. מכאן גם נובע החיסרון- למרות שהמערכת מסוגלת לזהות תבניות התקפה, היא תספק פחות מידע אודות התוקפים. ישנה אפשרות ללמוד מאיזו מערכת התוקפים באים ובאיזה אקספלוייטים הם משתמשים על מנת לנסות ולפרוץ למערכת, אבל לא לגלות מידע על התוקפים ואיך הם מאורגנים.

מלכודות מסוג זה נועדו על לפתות את התוקפים ליצור קשר ולחשוף את הפירצות ברשת מראה של האירגון (רשת שאינה הרשת האמיתית, אלא רשת דמי שמטרתה לפתות את התוקף לפרוץ אליה). בעקבות חשיפת הפרצות דרך רשת הדמי, ניתן להתמגן טוב יותר ולאבטח את הרשת האמיתית.

2. Research Honeypots- מלכודת למטרת מחקר

מלכודות דבש למטרות מחקר נועדו לאסוף כמה שיותר מידע אודות קהילת הכובעים השחורים, ולא מספקות שום ערך מוסף ישיר לארגונים. השימוש הישיר למערכת שכזו הוא לספק לאירגון מידע על הסיכונים בפניהם הוא עלול לעמוד, ולאפשר לארגון ללמוד אודות מניעת ההתקפות, זיהוי ההתקפות ובכלל לבנות ולתכנן הגנה טובה יותר מול איומים שכאלו. אופן פעולת מלכודת זו עוזר להבין טוב יותר את פעולות ואירגון ההתקפה. החיסרון במלכודת מסוג זה הוא שהיא מסובכת להטמעה, לשימוש ולתחזוקה, ושומרת כמות אדירה של מידע. הגנות מסוג זה לרוב משומשות על ידי אירגונים כמו אוניברסטאות ממשלות או חברות גדולות שמעוניינות ללמד עוד אודות איומים אלו

במערכת זו אנו למדים מידע על התוקף ברמה גבוהה ביותר. כל פעולה שהתוקף נוקט נקלטת במערכת מרגע התקיפה ועד רגע הכנעת המערכת, דבר שהמאפשר איסוף מידע יחודי למדי. כמו כן, מערכת זו יכולה לזהות איומים חדשים (כמו תולעים שרק נוצרו וכן הלאה).

3. מלכודת Honeytokens

מלכודת זו הינה מלכודת מהסוג הרגיל. Honeytokens בקצרה, היא כל מה שמגדיר מלכודת דבש רגילה- חוץ מזה שהיא אינה מחשב. הבלבול הגדול ביותר בנוגע למלכודות דבש הוא שהן לא חייבות להיות מחשב- משאב פיזי כלשהו שהתוקף יצור איתו קשר.
הנה ההגדרה המקורית של Honeypot:

"A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource". – Wikipedia.org

אם נשים לב, לא רשום בפירוש שמלכודת דבש חייבת להיות מחשב, היא פשוט חייבת להיות משאב כלשהו שנרצה שהכובעים השחורים יצרו איתו קשר. Honeytokens באים בצורות וגדלים שונים, כמו ממתקים, אבל כולם מוגדרים כקונספט אחד- משאב מערכת דיגיטלי או משאב מערכת מידע שמתבסס על גישה לא מורשית מחוץ למקור. דוגמה לכך תוכל להיות חשבון משתמש מזוייף ואפילו תוכן בתוך מסד נתונים. לא משנה באיזו צורה ניצור את המלכודת, אף אחד לא אמור לגשת אליה. דבר המספק למלכודת זו את אותם יתרונות וחסרונות של מלכודת דבש רגילה (בהמשך) ואפילו מרחיב את יכולתה מעבר לגבולות המחשב.

סיווג מלכודות על פי רמת אינטראקציה

מלבד חלוקה לפי סוגים, אפשר לחלק את מלכודות הדבש לפי רמת אינטראקציה, כלומר על פי רמת המעורבות המותרות האפשרית בין התוקף לבין המערכת.

מלכודות ברמת אינטראקציה נמוכה

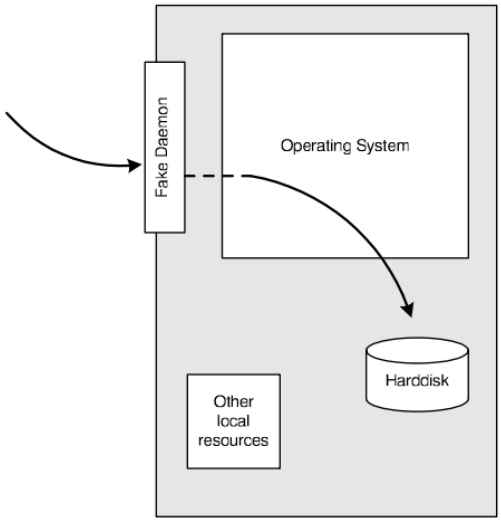
מלכודת דבש המאפשרת אינטראקציה נמוכה, רק מדמה כמה שירותים מזוייפים שלא יכולים להיפרץ ולספק גישה מלאה במלכודת. במלכודת ברמה כזו אין מערכת הפעלה שהתוקף יכול לבצע בה שינויים. במערכת זו ניתן לפענח ספאמרים והתמודדות מול תולעים. המטרה היחידה עבור הטמעת מערכת שכזו היא זיהוי התקפות פשוטות- התקפות חדשות יכולות להיחשף ולספק מידע אודות הפורצים. בנוסף, היא ניתנת להטמעה באופן פשוט ותחזוקה קלה.

לדוגמה: שימוש פשוט ב:

```
netcat -l -p 80 > /log/honeypot/port_80.lpg
```

יתן לנו האזנה על פורט 80 (HTTP) ואפשרות לתעד את כל התעבורה הנכנסת אל קובץ תיעוד מיוחד. בדרך שכזו כל התעבורה הנכנסת יכולה להיות מזוהה באופן פשוט למדי. במערכת שכזו לא ניתן לתעד תקשורת של פרוטוקולים מסובכים יותר מבחינה טכנית, לדוגמה לחיצת יד ב-SMTP לא תוביל לשום מידע מועיל מכיוון שאין שום שירות שיענה.

העובדה שבמלכדות זו אין מערכת הפעלה מהווה את החיסרון שלה- לא ניתן יהיה ללמוד אודות האופן בו התוקף מתקשר עם המערכת- דבר שיכול להיות מאוד מעניין ובעל חשיבות בהתמודדות מול התוקף. אפשר לדמות מערכות אלה למערכות בעלות חיבור אחד- יש אפשרות רק להקשיב, אבל לא לשאול שאלות.



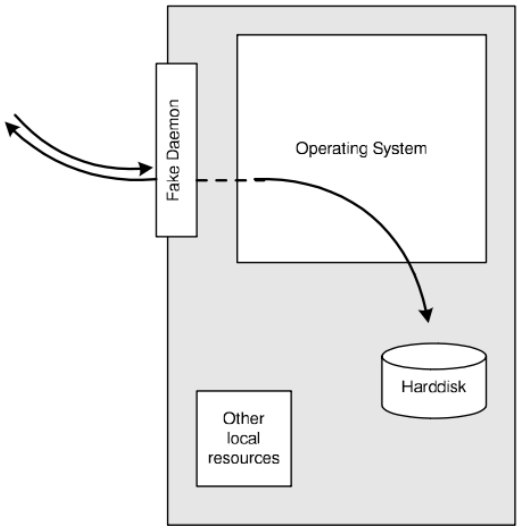
תרשים מס' 1: מלכודת דבש באינטראקציה נמוכה- פעילות נמוכה של מלכודת דבש מורידה את הסיכונים למינימום אבל גם מורידה את יכולת הלמידה אודות הפורץ לאותה רמה.

(התרשים נלקח מ-White Paper: Honeypots- Reto Baumann, Christian Plattner)

ניתן להשוות את המערכת ברמת אינטראקציה נמוכה למערכת IDS פאסיבית, מכיוון שהיא לא משנה את התעבורה ולא יוצרת קשר עם התוקף. השימוש במערכות אלו כיום נעשה ליצירת לוגים והתראות מפאקטים נכנסים, המזוהים כחלק מתבניות התקפה.

מלכודות ברמת אינטראקציה בינונית

אפעל פי שמלכודת מסוג זה מעט משוכללת מקודמתה, גם בה אין מערכת הפעלה. היא מדמה שירותים שיותר מתוחכמים טכנית. למרות שהסיכויים שהתוקף ימצא פירצת אבטחה גדלים עקב רמת התיחכום הגבוהה במערכת זו, הבעייתיות בה היא שאין הגבלות אבטחה ומערכות שיתעדו ויתריעו מה קורה במקרים של התקפה. למרות הכל, בגלל שמדובר ברמת אינטראקציה גבוהה יותר, המאפשרת שכלול מסוים לעומת המלכודות ברמת אינטרקציה נמוכה, היא גם מאפשרת התקפות יותר מסובכות שניתנות לתיעוד ולניטור. לתוקף ישנה אשליה יותר טובה אודות מערכת הפעלה תקנית ויש לו יותר אפשרויות לתקשר איתה.

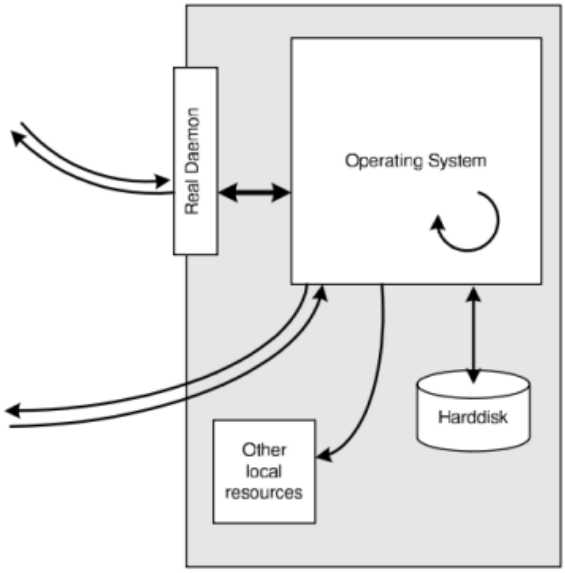


תרשים מס' 2: מלכודת דבש באינטראקציה בינונית מאפשרת "מגע" עם התוקף בדרך מינימלית.
(התרשים נלקח מ-White Paper: Honeypots- Reto Baumann, Christian Plattner)

פיתוח מערכת בעלת אינטראקציה בינונית היא תובענית יותר מבחינת זמן ותכנון, זאת משום שחייבים לקחת בחשבון מקרים מיוחדים וכל השירותים המזוייפים חייבים להיות מאובטחים כראוי. הגרסאות המפותחות לא אמורות לסבול מאותם פגמים באבטחה כמו במערכות האמיתיות- היות והמטרה האמיתית היא לשבש את אלו עם משתנים מזוייפים. הידע לפיתוח מערכת מסוג זה הוא גבוה יחסית משום שכל פרוטוקול ושירות חייב להיות מפורט לפרטים.

אינטראקציה גבוהה

הסוג המתקדם ביותר של מלכודות הדבש. אלו המערכות המסובכות ביותר ומבחינת פיתוח הן דורשות הכי הרבה זמן ומשאבים לתיכנון ועיצוב, ומשלבות את הכמות הגבוהה ביותר של סיכונים היות והן מערבות מערכות הפעלה אמיתיות עם שירותים אמיתיים, וכמובן עם חולשות אבטחה אמיתיות, על מנת לפתות את הפורץ להכנס ולאסוף מידע אודותיו. מערכת זו מספקת לפורץ מערכת הפעלה אמיתית שניתן לתקשר איתה ושום דבר לא מדומה או מוגבל. פורץ יכול לקבל גישת root ולקבל גישה מלאה למכונה המחוברת לרשת האינטרנט כל הזמן (מה שמספיק מסוכן בפני עצמו). מכאן ניתן להבין כי הסיכויים לקבלת מידע גדלים, היות ובסוג זה של מלכודת דבש, כל הפעולות מתועדות ומפוענחות. לצערנו (וזה בעצם מהווה את החסרון של המערכת) הפורץ חייב להכניע את המערכת על מנת לקבל רמה כזו של חופש, אך ברגע שיכניע הוא יקבל גישת root במערכת- כפי שהיא, ויוכל לעשות כל דבר שעולה על רוחו. משלב זה המערכת לא מאובטחת יותר וכל המכונה לא נחשבת יותר למאובטחת. אין חשיבות לעובדה אם המערכת נמצאת תחת מערכת וירטואלית היות ותמיד יימצאו דרכים לחרוג ממגבלות התוכנה.



תרשים מס' 3: במלכודת דבש ברמת אינטרקציה גבוהה יש יותר סיכון שהפורץ יוכל להכניע את המערכת ולהשתמש במשאביה.

(התרשים נלקח מ-White Paper: Honeypots- Reto Baumann, Christian Plattner)

מכיוון שלפורץ יש יותר מקורות מנקודת מבטו לפריצה ויצירת קשר, יש לשים לב במיוחד במערכת מסוג זה, על מנת לוודא שהיא לא הופכת לסכנה או לפירצת אבטחה בעצמה (הפורץ יכול לנצל את המערכת עבור בסיס להתקפות אחרות שלו). דבר חשוב במערכת הוא להגביל אותה לגישת אינטרנט מקומית בלבד, על מנת שהמערכת לא תשמש את הכובעים השחורים לצרכיהם. מכיוון שזו מערכת הפעלה מתפקדת, התוקף יכול לעשות בה שינויים על פי רצונו החופשי- זהו בעצם החלק המעניין. ניתן לקבל תמונה מלאה אודות פעולותיו, העדפותיו וכדומה. מערכת זו מאפשרת איסוף מידע יעיל ואמין לגבי קהילת הכובעים השחורים ומאפשרת לנו לאבטח את המערכות שלנו ולהתמגן מפני התקפותיהם ביעילות יתרה.

לסיכום, ניתן לומר שבמלכודות דבש העיקרון הפועל הוא שאיסוף המידע הטוב והאמין ביותר הוא גם המסוכן ביותר. יש קשר ישיר בין אמינות המידע והפירוט שנקבל לסיכון שאנו מוכנים לקחת בהתקנת מלכודת דבש.

בפרקים הקודמים דיברנו על סיווג המלכודות על פי מטרות ועל פי רמות אינטראקציה. דרך נוספת לסווג אותן היא על פי הסוגים המיושמים בתעשיית אבטחת המידע בימינו. מדובר בסיווג על פי התפקוד שמבצעת המלכודת, בגינו היא נבחרה להיות מיושמת בתעשיית האבטחה.

- **מערכות ניטור פורטים**

זוהי מלכודת הדבש הפשוטה ביותר שנמצאת כיום בשימוש. ניטור פורט הוא בעצם סוקט מבוסס תוכנה שפותח ומאזין לפורט. ההגדרה ל-סוקט היא הכמות המינימלית של מידע הנחוצה עבור תקשורת ברשת, מקורו מה-TCP/IP. סוקט מכיל בתוכו את המקור והיעד של כתובת ה-IP, את פורט המקור והיעד ואת פרוטוקול ההעברה (UDP או TCP).

מלכודת דבש של ניטור פורטים תאזין לתעבורה בפורטים שלרוב נסרקים על ידי פורצים. מערכת זו תפעל להפלת הפורט מיד לאחר קבלת החיבור, דבר שירתיע את התוקף. מצב בו חיבור נופל בפתאומיות מדליק "נורה אדומה" אצל הפורץ ומתריע על האפשרות שקיימת מערכת IDS שרצה על פורט זה.

- **מערכות הונאה**

מדובר במערכת הנמצאת שלב אחד מעל המערכות לניטור פורטים והייחוד שלה הוא שהיא יוצרת קשר עם הפורץ. בניגוד למערכת ניטור פורטים, מערכת הונאה תגיב לסריקת פורט כאילו היא שרת אמיתי. דוגמה לאחד השכלולים במערכת- היא מצויידת במסך פתיחה על מנת לשטות בתוקפים פוטנציאליים.

- **מערכת הונאה בריבוי פרוטוקולים**

מערכת הונאה בריבוי פרוטוקולים היא מערכת בעלת האפשרות להשתמש בכמה פרוטוקולים ומשתמשת במסכי כניסה, על מנת לחקות חבילות עבור מערכות הפעלה שונות.

- **מערכות מלאות**

מערכת מלאה לוקחת את נושא מלכודות הדבש שלב אחד מעבר למלכודת פשוטה והופכת מערכת פועלת עם כל האפשרויות הנלוות ולרוב נקבעת להתריע רק לגבי כללים מאוד מסויימים. מערכת מלאה זו בשילוב עם מערכת IDS כוללת מערכת התראה מלאה, ומהווה את מערכת הניטור והתיעוד האולטימטיבית.

מיקום ואסטרטגיה

מלכודת דבש אינה דורשת שום סביבה מיוחדת, בדיוק כפי ששרת אמיתי לא צריך תנאים מיוחדים על מנת לפעול. מלכודת זו יכולה לפעול ממקום בכל מקום שבו שרת אמיתי יכול, אך כמובן- מקומות מסויימים עדיפים על פני מקומות אחרים. מלבד זאת- ישנן טקטיקות ושיטות שונות לשימוש ב-Honeypot, הכל תלוי בצרכי מנהל המערכת.

מכיוון שבאמת אין דרך יחידה להקמת Honeypot והיא עשויה לשמש לתפקידים רבים, יש להתאים את התנאים הקיימים אל דרך הפעולה שבה נרצה שהמלכודת תפעל.להלן כמה דוגמאות:

- **מערכת הונאת פורטים**

דוגמה למערכת זו יהיה שרת FTP שלא באמת מספק את השירות הזה. שירותי רשת וירטואלים יכולים להיות מותקנים על מלכודות דבש, אך למעשה הם מציעים רק את תעבורת הרשת (כמובן שהשירות חייב להיראות אמיתי על מנת שלא לגרום לתוקף לעלות על התרמית).

- **מערכת שדה מוקשים**

מיקום מספר יחסית גבוה של Honeypot בקידמת הרשת על מנת להוות את המטרה הראשונית של התוקפים. מהלך זה נועד לבזבז את זמנם של התוקפים על מערכות ושירותים שלא באמת קיימים ובכך להסיח את דעתם מהמערכת האמיתית.

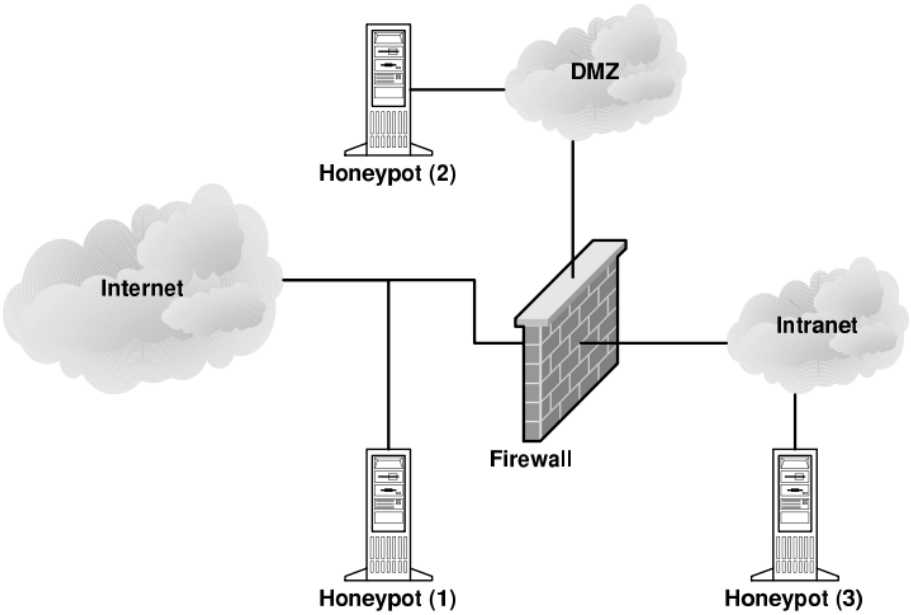
- **מערכת קורבן**

זוהי מערכת honeypots הממוקמת במיקום שאין בו שום חיבור למערכת אמיתית.

- **מערכת מגן**

בטקטיקה זו, חומת האש, או הראוטר, משתמשים בפניית פורטים בכדי להפנות תעבורה שנועדה להגיע במקור אל שירותים לא מורשים. תעבורה זו מופנית אל ה-Honeypot. לדוגמה, אם ננסה להתחבר באמצעות telnet לשרת אינטרנט כזה או אחר, נופנה אל Honeypot שהיא בעצם העתק של השרת המקורי.

בנוסף להאסטרטגיות אלה, אפשר להשתמש במלכודת על גבי רשת האינטרנט וגם על גבי רשת האינטרה-נט, הכל תלוי בשירותים שהיא נועדה לספק. לצורך הענין, אם נרצה לתפוס עובדים מהרשת המקומית באינטרה-נט, הקמת מלכודת דבש ברשת זו תהיה המועילה ביותר.



(התרשים נלקח מ-White Paper: Honeypots- Reto Baumann, Christian Plattner)

חסרונות

יש חשיבות עליונה למודעות לפרצות שקיימות במערכת אבטחה, על מנת להוסיף לה רבדים ומנגנונים נוספים שיתמודדו עם פרצות אלה, לכן פרק זה יעסוק בחסרונות של מערכת זו.

1. אם מערכת Honeypot הותקפה בהצלחה, היא יכולה לשמש כקרש קפיצה עבור התוקף אל מערכות מחשב ורשתות אחרות. ככל הנראה, זו הסכנה הגדולה ביותר במלכודות דבש. על מנת לצמצם את הסיכון, רצוי למקם את מלכודת הדבש מאחורי חומת האש. זוהי פעולה שעשויה להקשות על התוקף להגיע אל המלכודת ובנוסף לכך היא מסוגלת לצמצם את התעבורה החיצונית ומקנה למערכת צורה אמינה יותר.

2. מלכודות דבש גוזלות המון זמן יקר בהקמה ובתחזוקה (תלוי ברמת הסיבוך שלהן). באופן כללי, בגלל שמערכות אלו גוזלות המון משאבים מצד האירגון, יש אפשרות שיגיע מצב שמנהלי האבטחה באירגון פשוט יכבו אותן על מנת לשחרר משאבים.

Honeynet

A honeyfarm is a centralized collection of honeypots and analysis tools.
The concept of the honeynet first began in 1999 when Lance Spitzner, founder of the Honeynet Project, published the paper "To Build a Honeypot":
"A honeynet is a network of high interaction honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discretely regulated." – Wikipedia.org

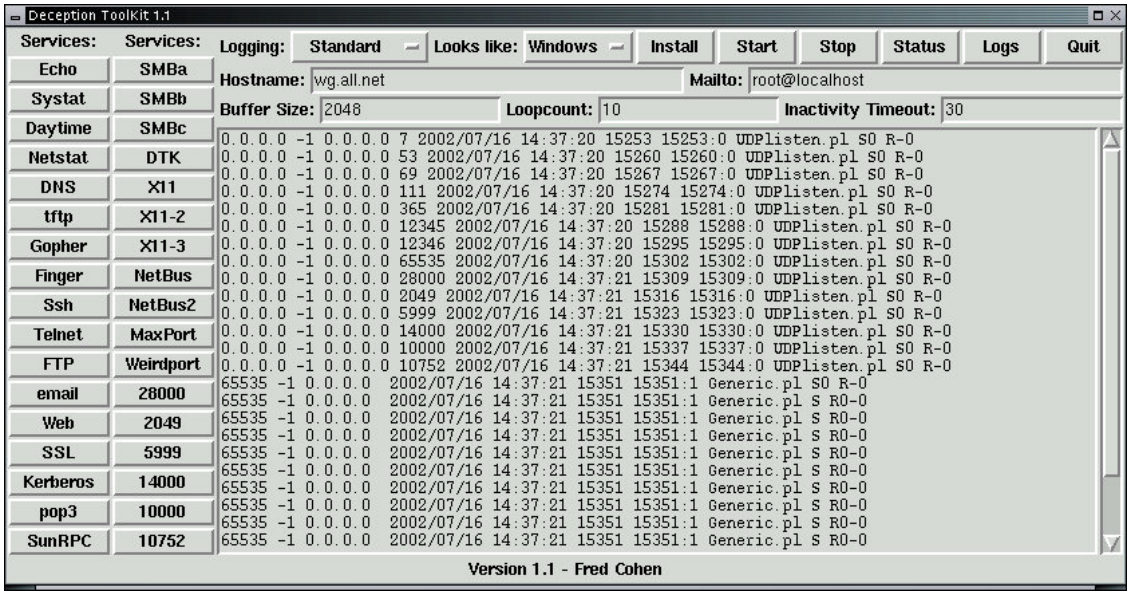
בהגדרתה, Honeypot היא שתיים או יותר מלכודות דבש (Honeypots) המחוברות ביניהן ברשת. רשתות שכאלו הן יעילות בניטור רשתות גדולות ומגוונות יותר,איתן מלכודת דבש בודדת מתקשה להתמודד ביעילות. בדרך כלל, ה-Honeypot הן מערכות המכילות מספר יגבוה יחסית של מלכודות דבש רגילות , חומות אש (על מנת להגביל ולתעד את תעבורת הרשת) ומערכות IDS שונות (על מנת לצפות ולפענח התקפות אפשריות). השילוב של מערכות אלו יחד יוצר מערכת משוכללת ומורכבת שמטרתה העיקרית היא לאסוף מידע נרחב ביותר אודות איומים מצד הכובעים השחורים, אודות אופי התקפותיהם וסכנות צפויות. הגדרה יותר מתקדמת היא ה-HoneyFarm, שמהווה אוסף מרוכז של מלכודות דבש וכלים אנליטיים שונים.
קונספט ה-Honeypot התפתח ב-1999 עקב פרסום המאמר "To Build a Honeypot" על ידי לאנס ספיטצנר, מייסד של ה-Honeynet Project

ייחודה של מערכת זו מתבטא בכך שהיא רשת של מחשבים אמיתיים שניתנת להתקפה. המחשבים ברשתהנם גמישים במיוחד, הם עוטים צורה של מה שהמתכנן רוצה, הכוח שלהם הוא בגמישות. לדוגמה: שרת Apache על CentOS.

בעקבות העובדה ש-Honeynet הינה רשת של כמה מחשבים, נוצרת בעיה בעיה אחרת- ככל שאנו מגדילים רשת שכזו, אנו זקוקים ליותר חומרה, משמע שעלות המערכת עולה ויש להשקיע יותר כסף בפיתוח ותחזוקה. פיתרון אפשרי לכך יכול להיות שימוש ב-VMWare על מנת להרים ולהריץ מערכותוירטואליות שונות (מלכודות דבש אחרות) על מחשב אחד. דבר נוסף שניתן לעשות הוא להקים חומת אש על אותו מחשב בדיוק כמו שאר מלכודות הדבש. פתרון זה מעלה בעיה מסוג שונה, היות וזוהי רק תוכנה שמדמה סביבה וירטואלית אחרת, הפורץ יוכל לפרוץ החוצה אל המכונה עצמה וזה מעמיד אותנו ואת המערכת, עליה אנו מנסים להגן, בפני בעייה אמיתית וגדולה.

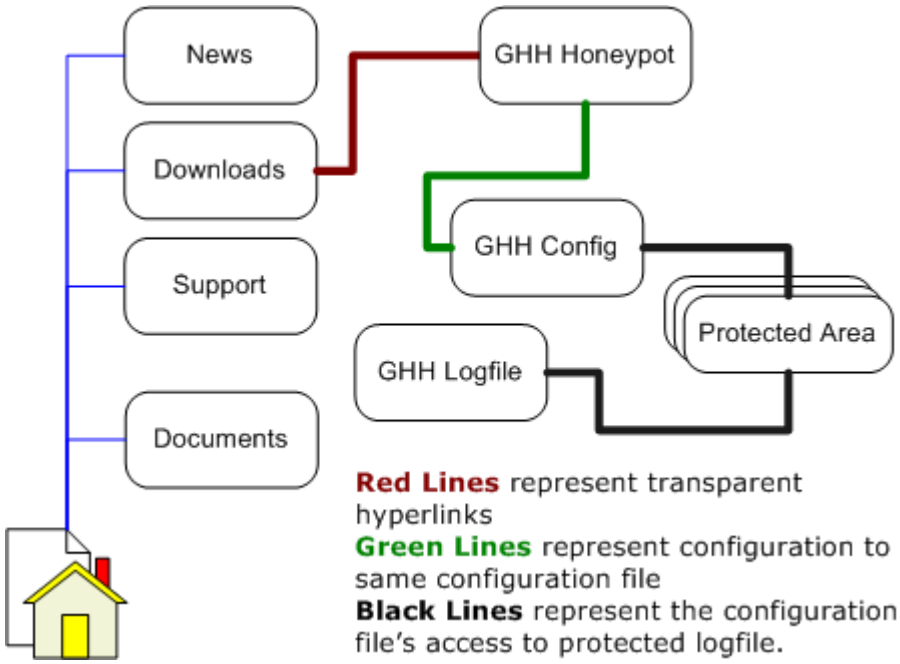
כיום ישנן מספר מערכות קיימות המשוחררות לציבור הרחב (קוד פתוח וגם מערכות מסחריות) המאפשרות להקים מלכודות דבש ברמות שונות ובשליטה שונה. בחלק זה אפרט על כמה מהן.

1. **DTK**- סט של כלים חופשיים (רובם כתובים ב-Perl) שנועדו לתת לצד אשר מנהל את המערכת להגן עליה בצורה טובה יותר ולתת לה יתרונות על התוקפים. הרעיון הכולל הוא להטעות את התוקפים על ידי כך שאם המערכת מריצה DTK, למערכת יש יותר פירצות זמינות אפשריות עבורו. מה שבאמת קורה הוא שהמערכת מגבילה את הקשר עם התוקף בצורה גבוהה, אך מדמה את כל התהליך של הפירצה ומחזירה תגובות כאילו היה מדובר במערכת אמיתית בעלת חולשות אמיתיות.



2. **Honeyd**- דימון יחסית פשוט וקטן שרץ גם על מערכות UNIX וגם על מערכות Windows. הוא מאפשר ליצור מכונות וירטואליות שונות על מחשב אחד. ניתן להגדירו להריץ שירותים כמו FTP או SMTP ומעבר לכך, מאפשר למשתמש לדמות מערכת הפעלה.

3. **GHH**- או בשמו המלא: Google Hack Honeypot. נועד לטפל בבעיית התוקפים שמשתמשים במנועי החיפוש ככלי פריצה, היות ומנוע החיפוש של חברת גוגל מאפשר חיפוש מיידי בכמות אדירה של מידע. ככל שהאינטרנט גדל, החלו להופיע גם ישומי רשת כגון פורומים וכלי ניהול מרחוק, דבר שהוביל לתוכנות לא מוגדרות כראוי להציג חולשות אלו לכולם. GHH מדמה ישום רשת אמיתי ומאפשר לו להצטרף אל מנועי החיפוש הרבים. מלכודת דבש זו מחוברת אל קובץ ההגדרות שרושם ומתעד כל דבר שהוגדר בקובץ הגדרות של המערכת. כאשר תוקף מנסה לתקוף את היישום (שלא באמת קיים), קובץ התיעוד מתחיל להתמלא במידע אודות התוקף שכולל בתוכו מידע רב כמו User Agent ואת כתובות ה-IP.



פרוייקט בנושא Honeypots

מלכודות הדבש הן נושא מעניין שניתן לחקור ולפתח עוד ועוד. כחלק מהעניין, הן מהוות נושא לפיתוח פרוייקטים רחבי אופקים וארוכי טווח, במאמר זה אביא דוגמה לאחד הפרוייקטים המפורסמים בנושא.

פרוייקט NoAH הינו רשת אירופאית של מלכודות דבש המקושרות ביניהן. מדובר בפרוייקט בן 3 שנים שמטרתו לאסוף מידע על טבע ההתקפות ברשת. מטרתו הנוספת היא לפתח תשתית שתזהה ותספק אזהרות לגבי התקפות אלה, על מנת שנוכל לנקוט באמצעים בהתאם לכך.
בשנים האחרונות נרשמה עליה חדה בהתקפות כגון וירוסים, תולעים, סוסים טרויאניים וכדומה ברחבי רשת האינטרנט. התקפות אלו מורידות את היעילות שבשימוש באינטרנט, פוגעות בתשתיות IT ועלולות להשתלט על חלקים נרחבים ברשת תוך דקות ספורות. לעתים קרובות הדבר קורה באופן מהיר מהתגובה האנושית ומהווה צורך לפיתוח מנגנון אוטומטי שיגיב באמצעי נגד במצבים אלה.

הפרוייקט מבוסס על עיצוב ופיתוח של תשתית, שנועדה לנטר ולאבטח, המבוססת על טכנולוגיית ה-Honeypots. הפרויקט משתמש במלכודות דבש המפוזרות במקומות שונים ככלי לאזהרה מוקדמת וניטור, מעבד את הנתונים שמתקבלים מהמלכודות ומתכנת אותן להגיב באמצעים מסוימים נגד התראות מסוימות.

סיכום

אז.. מי מפחד ממלכודות הדבש? כמו נערות הפיתוי בסיפורי הריגול, הן מפתות, אטרקטיביות, שקטות, נראות לחלוטין תמימות וכביכול לא טומנות בחובן שום סכנה. הן מהוות את הפיתוי המושלם לתוקף "רעב" לפריצה מוצלחת. חשוב לזכור שלמטבע שני צדדים, צד אחד טומן את הפח והשני נופל בפח שטמנו לו. אחד העקרונות המובילים בנושא אבטחת המידע הוא להיות מודע לכל האפשרויות ולאסוף את כל המידע האפשרי על מנת להמנע מלהיות זה שנופל בפח.

על הכותב

נתנאל שיין עוסק בפיתוח ובאבטחת מידע בפרט, מעורב בפרוייקטים שונים בנושא הקוד הפתוח, בעיקר בהתנדבות, חבר בעמותת המקור, כיום עובד בהייטק וסטודנט למדעי המחשב באוניברסיטה הפתוחה.

עוד דבר שהייתי חייב להכניס:

מקורות:

1. http://en.wikipedia.org/wiki/Honeypot_%28computing%29
2. http://www.honeypots.net/honeypots/links
3. http://www.projecthoneypot.org
4. drunkgeisha.noblogs.org (מכאן בא אחד התרשימים)
5. honeynet.org
6. holcroft.org
7. isoc.org
8. http://www.honeynet.org
9. http://www.ukhoneynet.org
10. Honeypots by Reto Baumann and Christian Plattner.
11. The Use of Honeypots and Packet Sniffers for Intrusion Detection by Michael Sink, P.E.
12. A Guide to the Honeypot Concept Mark Pickett
14. http://www.christianplattner.net
15. http://all.net/dtk/index.html
16. http://ghh.sourceforge.net/index.php