



OpenDLP

מאת שחר אלקסלסי

:DLP software - Data loss prevention software

- זיהוי דליפת נתונים פוטנציאלית ומניעה על ידי ניטור, זיהוי וחסימת מידע רגיש בזמן שימוש, בתנועה (תעבורת רשת) ובמנוחה (אחסון נתונים).
- בתקריות זליגת מידע, נתונים רגישים ייחשפו לאנשים בלתי מורשים.
- נתונים רגישים יכולים להיות:
 - מידע פרטי
 - מידע של חברות
 - קניין רוחני
 - מידע פיננסי
 - מידע על מטופלים
 - נתוני כרטיסי אשראי ועוד.

OpenDLP

- כלי חינמי המבוסס קוד פתוח
- כלי לאיתור זליגות נתונים אפשריות המשוחרר תחת רישיון GPL.
- יכול בו זמנית לזהות נתונים רגישים במנוחה על מאות או אלפי מערכות מיישום אינטרנט מרכזי, במערכות הבאות:
 - מערכת הקבצים של Windows
 - מערכת הרשת של Windows
 - מערכת הקבצים של Unix
 - מסד הנתונים Microsoft SQL Server
 - מסד הנתונים MySQL
- חיפוש המידע מתבצע בעזרת Regular Expressions.

כלים מתחרים

:MyDLP

- כלי דומה, חינמי, המזהה מידע רגיש בשימוש, תנועה, ומנוחה.
- כלי זה גם הוא מבוסס סוכנים, אך יכול לזהות נתונים רגישים רק במערכת הפעלה של Windows.

מי משתמש ב-OpenDLP?

- חברות שמאחסנות מידע רגיש, בכדי למצוא את דליפות המידע ולטפל בהן לפני שהן יגיעו לידיים הלא נכונות.
- השימוש העיקרי הוא על ידי מנהלי רשת, ובודקי חדירה.

מה אפשר לעשות עם המערכת

ישנן מערכות מידע רבות ששומרות מידע רגיש כמו פרטי כרטיסי אשראי, הכלי של OpenDLP יכול למצוא בקלות את המידע הנ"ל ברחבי הרשת בה שמורה מערכת המידע.

דורך העבודה של OpenDLP

:Agents Scan

- התוכנה מבוססת על יישום אינטרנט שמהווה פאנל ניהול, וסוכנים חכמים שמהווים כלי לחיפוש מידע רגיש.
- דורך יישום האינטרנט ניתן לשלוח פקודת להתקנת סוכנים חכמים על עמדה מרוחקת והפעלתם על העמדה.
- הסוכנים מבצעים חיפוש על העמדה ומנסים ליצור קשר עם יישום האינטרנט מדי כמה זמן כדי לעדכן אותו בהספק.
- עם סיום החיפוש הסוכנים מוחקים את עצמם מהעמדה המרוחקת והזכר היחיד לפעולה של OpenDLP בעמדה המרוחקת יכול להימצא רק ב-Log מערכת של העמדה.

דורך העבודה של OpenDLP

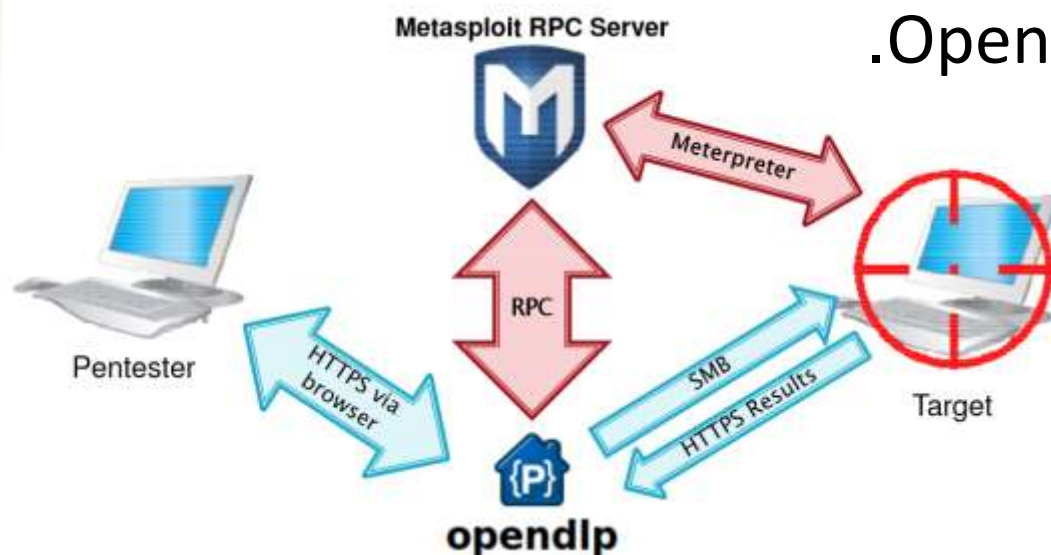
:Agentless Scan

- ל-OpenDLP יש גם מימוש של חיפוש שלא בעזרת סוכנים חכמים, למשל עבור מערכת הקבצים של Unix.
- סריקה ללא סוכנים חכמים מתבצעת על-ידי שימוש בסוכן אחד שקיים במערכת הקבצים של המערכת הנסרקת.
- ההבדל העיקרי בין סריקה עם סוכנים לסריקה ללא סוכנים הוא הזמן שלוקח לסריקה להתבצע.

דרך העבודה של OpenDLP

:Metasploit Scan

- אפשרות נוספת לפריסה של סריקת OpenDLP היא באמצעות Metasploit.
- משתמשים בפרצות אבטחה במערכת כדי להריץ את הסריקה.
- התוכנה ניגשת לשרת Metasploit אשר בוחן אקספלוויטים אפשריים למחשב הנסרק, ובהתאם לאקספלוויטים שנמצאו התוכנה מנצלת אותם לפריסת הסריקה של OpenDLP.



נקודות חולשה

- המערכת יודעת להתמודד רק עם ביטויים שמתאימים במדויק לביטוי רגולרי שהוגדר.
- במידה והנתונים הרגישים מאוחסנים באופן מוצפן היא לא תמצא אותם.
- לא פותח קבצים דחוסים (ZIP) רקורסיבית, ולכן קובץ דחוס בתוך קובץ דחוס לא יסרק כהלכה.
- עובד רק על קבצים עם סיומות (תוקן בגירסאות המתקדמות).

הדגמה

כדי להדגים את מטרתו ויכולותיו של הכלי OpenDLP נבצע התקנה של התוכנה על מכונה וירטואלית לצידה, ניצור מכונה וירטואלית נוספת ובה נשמור קבצים בעלי מידע רגיש (לדוגמה פרטי כרטיס אשראי).

נדגים כיצד ניתן לבצע חיפוש של קבצים רגישים על מחשבים מרוחקים באמצעות יישום האינטרנט, על ידי סריקה ללא סוכנים חכמים.

פעולה זו, אם תפעל כשורה, תציג לנו רשימת קבצים רגישים ומהו סוג המידע הרגיש שנמצא בכל אחד מהם.

נראה גם כיצד להסתיר קובץ כך שלא ימצא בבדיקות התוכנה, על-ידי שימוש בנקודות החולשה מהשקופית הקודמת.

- מכונה וירטואלית 1 – שרת עם OpenDLP 0.5.1: Ubuntu 11
- מכונה וירטואלית 2 – מחשב עם קבצים נגועים: Ubuntu 11
- ממשק UI של OpenDLP: Windows 8.1 ודפדפן Firefox 34.0.5
- קבצים נגועים: כרטיסי אשראי, מספרי ביטוח לאומי אמריקאי

ארכיטקטורת ההדגמה

