

הדגמה OpenDLP

מאת שחף אלקסלסי

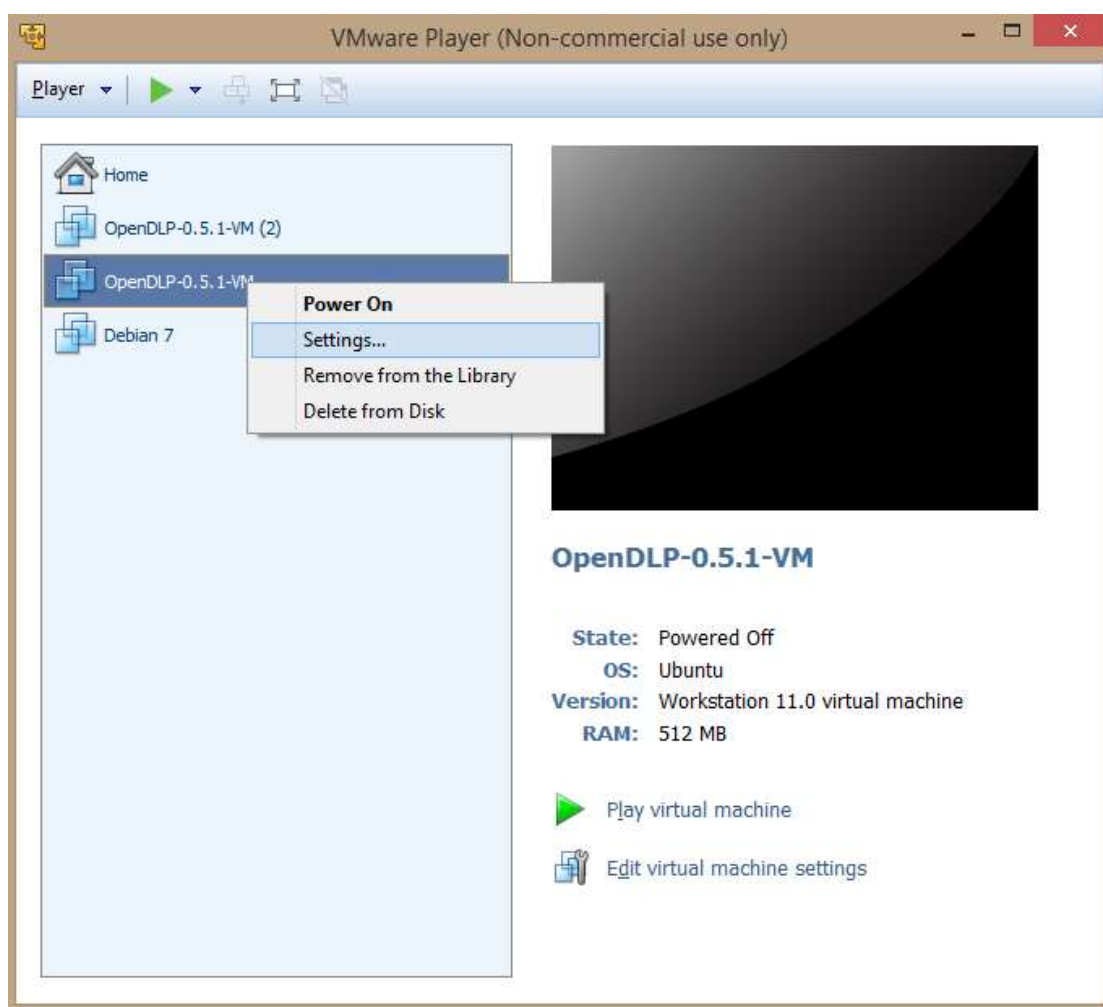
כיצד להתקין OpenDLP

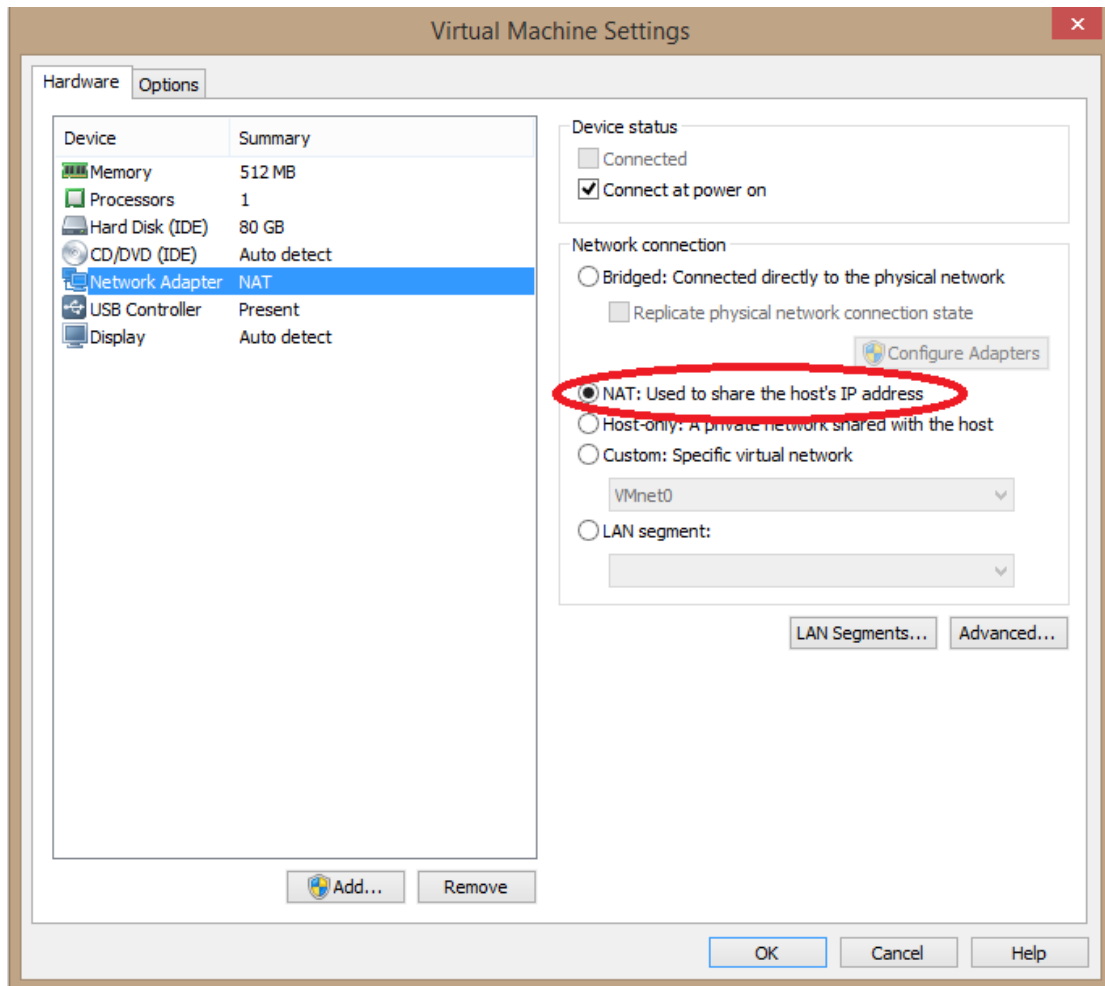
הגדרת המכונה הוירטואלית

הורדת הפצת Linux Ubuntu 11 עליה מותקנת תוכנת OpenDLP מהאתר הרשמי של OpenDLP.

נא לשים לב כי זוהי גרסה טקסטואלית בלבד. היא מהווה שרת עברנו, אליו ניגש בהמשך באמצעות ממשק UI בדפדפן המחשב האישי שלנו.

בעת התקנת המכונה הוירטואלית יש לשים לב להגדיר לה כתובת IP קבועה שאינה מסתמכת על נתב אליו עשוי להיות מחובר המחשב אלא מדמה את המחשב כנתב בפני עצמו.





לאחר התקנת המכונה הוירטואלית והגדרת כתובת ה-IP יש להריץ את המכונה.

שם משתמש וסיסמה להתחברות: `opendlp`

יש להקיש את הפקודה

`ip addr`

ולראות מהי כתובת ה-IP שהמכונה קיבלה.

```
OpenDLP-0.5.1-VM - VMware Player (Non-commercial use only)
Player
Ubuntu 11.04 opendlp tty1
opendlp login: opendlp
Password:
Last login: Sun Dec 28 04:18:50 EST 2014 on tty1
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-generic i686)

* Documentation:  https://help.ubuntu.com/

System information as of Sun Jan  4 11:45:16 EST 2015

System load:  0.08          Processes:            78
Usage of /:   1.4% of 77.97GB Users logged in:     0
Memory usage: 8%          IP address for eth0: 192.168.110.129
Swap usage:   0%

Graph this data and manage this system at https://landscape.canonical.com/
opendlp@opendlp:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:94:2b:88 brd ff:ff:ff:ff:ff:ff
    inet 192.168.110.129/24 brd 192.168.110.255 scope global eth0
    inet6 fe80::20c:29ff:fe94:2b88/64 scope link
        valid_lft forever preferred_lft forever
opendlp@opendlp:~$
```

עלול לצוץ צורך בהסרת רכיבי תקשורת מליבת הלינוקס במכונה הוירטואלית. לשם כך יש לכתוב את הפקודות הבאות:

```
cd /etc/udev/rules.d
sudo rm 70-persistent-cd.rules
sudo rm 70-persistent-net.rules
sudo reboot now
```

בשל בעיות חוקיות, להפצה לא מצורף קובץ אשר קיים בווינדוס. יש למצוא מחשב עליו מותקן Windows Vista/7 32bit ולהעתיק את הקובץ C:\Windows\System\sc.exe אל תיקיית /var/www/OpenDLP/bin ניתן לעשות זאת על-ידי העתקת הקובץ ל-USB והדבקתו או העלאת הקובץ ל-FTP והורדתו אל התיקייה המתאימה במכונה הוירטואלית.

הגדרת מכונה וירטואלית נוספת לאחסון קבצים רגישים

נגדיר באותה דרך מכונה וירטואלית נוספת, עליה נשמור קבצים רגישים.

יש צורך לשמור את כתוב ה-IP של המכונה בדיוק כמו שנעשה עבור המכונה הוירטואלית של ה-OpenDLP.

מצורף להסבר קובץ זיפ בשם PenFiles.zip המכיל קבצים לבחינת התוכנה.

בין הקבצים בקובץ הזיפ:

- קבצים תקינים
- קבצים עם מספרי כרטיס אשראי
- קבצים עם מספרי ביטוח לאומי
- וכן קבצים לשם הדגמה כיצד לעבוד על OpenDLP - קובץ השמורים בתוך דחיסה כפולה (זיפ בתוך זיפ), וקובץ עם מספרי ביטוח לאומי בפורמט של סימני קריאה ! במקום מקפים -.

הגדרת ממשק UI בדפדפן Firefox

יש להריץ את הדפדפן Firefox ולהכנס לחלון ההגדרות (Tools->Option)

לגשת ללשונית Advanced

תת הלשונית Certificate

ללחוץ על הכפתור View Certificates

בחלון שנפתח Certificate Manager יש לבחור בלשונית Your Certificates

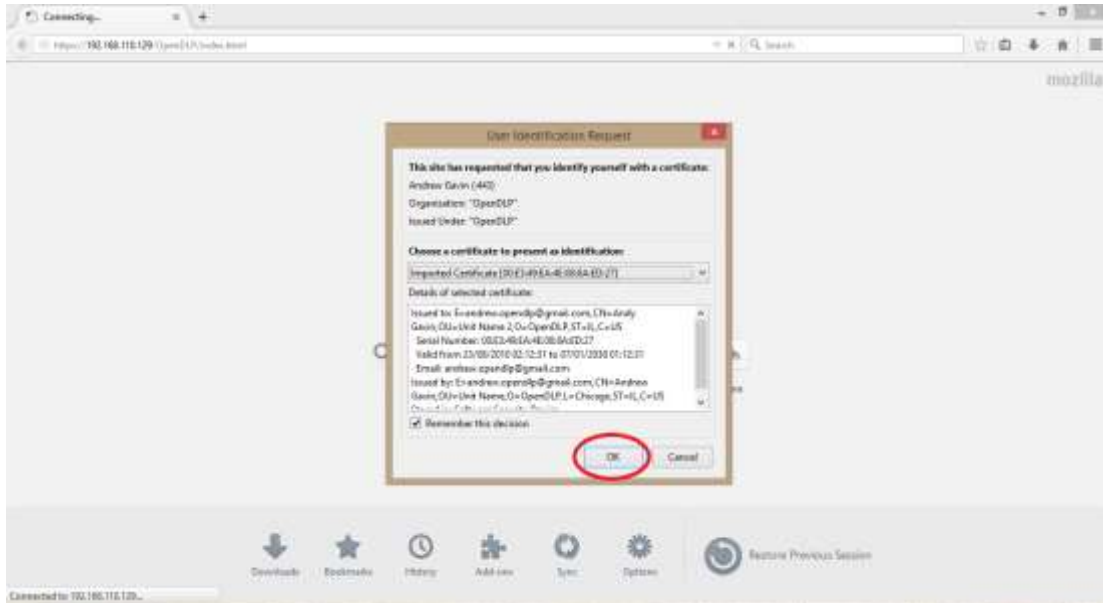
ללחוץ על הכפתור Import ולטעון את הקובץ client.p12 שמגיע עם הפצת Ubuntu 11 שהורדנו עבור התקנת המכונה הוירטואלית

הפעלת ממשק ה-UI

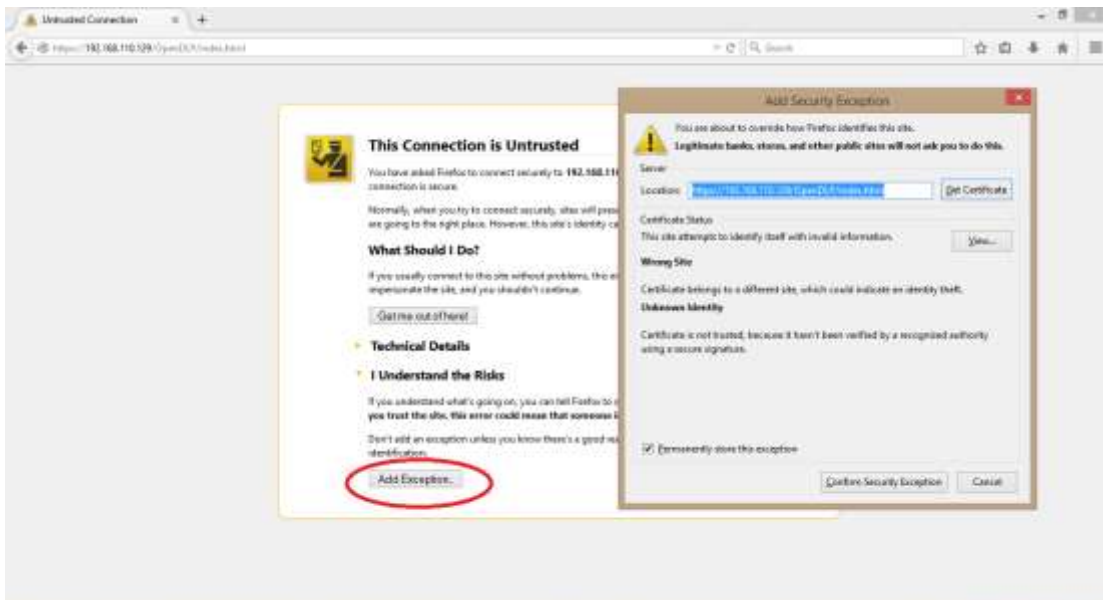
יש להכנס בדפדפן Firefox לכתובת המכונה הוירטואלית שהגדרנו עבור OpenDLP.

<https://192.168.110.129/OpenDLP/index.html>

ללחוץ OK כדי לבחור להשתמש ב-Certificate שהגדרנו



באזהרה שהאתר מסוכן יש ללחוץ על הקישור Understand the Risks, ללחוץ על הכפתור Add Exceptions ולאשר בלחיצה על Confirm Security Exception את הוספת הכלל יוצא דופן לשימוש באתר.



בחלון שיפתח Authentication Required יש לספק פרטי התחברות:

שם משתמש: dlpuser

סיסמה: OpenDLP

כעת ניתן להשתמש בממשק ה-UI של OpenDLP

OpenDLP 0.5.1

OpenDLP 0.5.1

OpenDLP is a free and open source, agent-based, centrally-managed, massively distributable data loss prevention tool released under the GPL. OpenDLP can identify sensitive data at rest on thousands of systems simultaneously. OpenDLP has two components:

Web Application

- Automatically deploy and start agents over SMB
- When done, automatically stop, uninstall, and delete agents over SMB
- Pause, resume, and forcefully uninstall agents in an entire scan or on individual systems
- Concurrently and securely receive results from hundreds or thousands of deployed agents
- Create Perl-compatible regular expressions (PCREs) for finding sensitive data at rest
- Create readable profiles for scans that include whitelisting or blacklisting directories and file extensions
- Review findings and identify false positives
- Export results as XML
- Manage Windows and UNIX agentless OS scans, Windows Metasploit agent scans, Windows agentless share scans, and database scans

Windows Agent

- Runs on Windows 2000 and later systems
- Written in C with no .NET Framework requirements
- Runs as a Windows Service at low priority so users do not see or feel it
- Recovers automatically upon system reboot with no user interaction
- Securely transmit results to web application at user-defined intervals
- Uses PCREs to identify sensitive data inside files
- Performs additional checks on potential credit card numbers to reduce false positives

Metasploit Agent

Everything the Windows Agent scan does, plus:

- Completely integrated with Metasploit through Messagepack RPC
- Removes list of exploited machines from Metasploit and displays in OpenDLP GUI
- Deploys OpenDLP directly from Metasploit to exploited machines of your choosing
- Domain credentials not required, if you can "get system" on the target from a metasploit console, you can deploy OpenDLP.

Agentless Database Scans

Starting with OpenDLP 0.3, you can now perform agentless data discovery against the following databases:

- Microsoft SQL server databases. Supports authenticating to databases either with SQL server credentials (the "sa" account, for example) or with Windows OS (domain) credentials.
- MySQL.

Agentless OS and Share Scans

הדגמה

יצירת פרופיל חדש

ראשית יש ליצור פרופיל חדש, בתפריט יש לבחור Profiles וללחוץ על Create New Profile

The screenshot shows the 'Create a new scan profile' form in the OpenDLP web interface. The form is titled 'Create a new scan profile' and contains the following fields and options:

- Profile Name:** agendless_example
- Scan Type:** UNIX Filesystem (agentless over SSH)
- Mask Sensitive Data?:**
- Username:** openalp
- Password:** *****
- Memory Limit:** 25% (as percent of target system's total RAM)
- Directories:** Scan all directories, Scan all directories except these (recursive), Only scan the following directories (recursive). Below this are input fields for /tmp, /var, /var/lib.
- File Extensions:** Scan all files, Scan all files except files with the following extensions, Only scan files with the following file extensions.

Profile Name – שם הפרופיל, לזיהוי הפרופיל הנבחר בהמשך

Scan Type – סוג הסריקה. עבור ההדגמה נבחר בבדיקה מסוג UNIX Filesystem

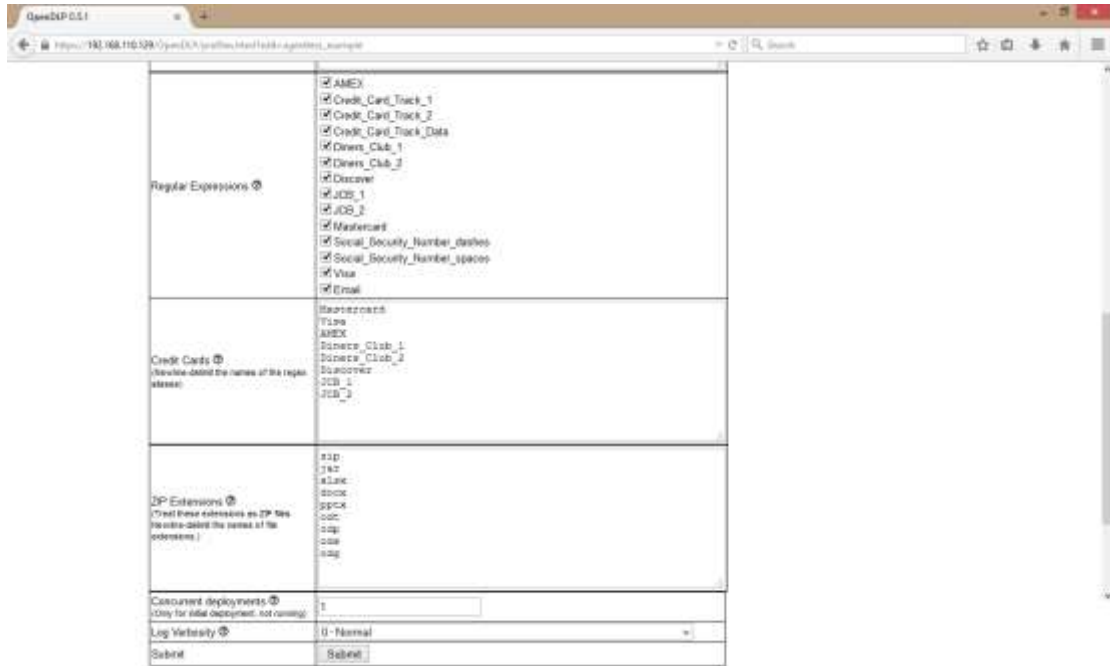
Mask Sensitive Data – האם להסתיר או לחשוף את המידע הרגיש שעשוי להתגלות בסריקה

Username+Password – פרטי ההתחברות של חשבון מנהל Root

Memory Limit – מהי מגבלת הזיכרון בה נשתמש לשם הרצת הסריקה של OpenDLP אחר קבצים רגישים

Directories – ניתן להזין רשימה של תיקיות ולבחור על סמך הרשימה האם לסרוק את כל התיקיות במחשב, רק את התיקיות ברשימה, או את כל התיקיות מלבד אלו שברשימה

File Extensions – ניתן להזין רשימה של סיומות לקבצים (סוגי קבצים) ולבחור על סמך הרשימה האם לסרוק את כל סוגי הקבצים, רק את סוגי הקבצים שברשימה, או את כל סוגי הקבצים מלבד אלו שברשימה



Regular Expressions – הביטויים הרגולים לפיהם הסריקה תחפש קבצים רגישים. בחירה מתוך רשימת ביטויים רגולריים שהוגדרו מראש

Credit Cards – אימות של סוגי כרטיסי אשראי בנוסף להתאמתם על סמך הביטוי הרגולרי

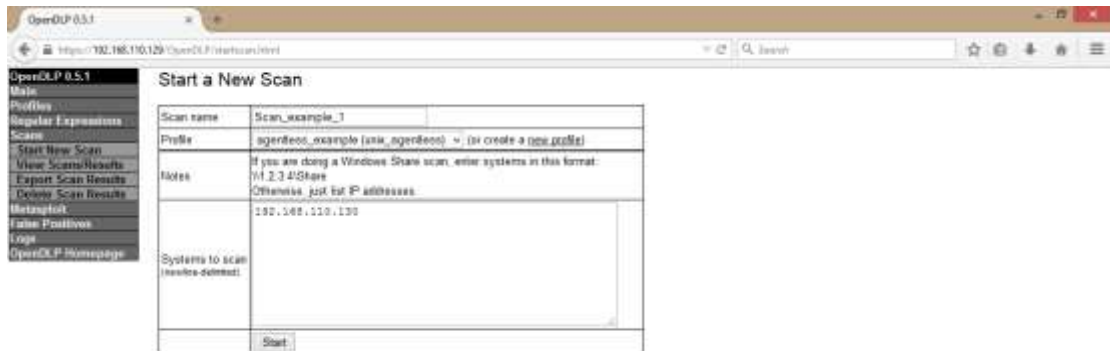
Zip Extensions – לאילו סיומות קבצים להתייחס כקבצים דחוסים אותם תנסה התוכנה לפתוח ולסרוק את הקבצים שבתוכם

Concurrent Deployments – כמות התחלתית של סוכנים שיפרשו במקביל בתחילת הסריקה

Log Verbosity – מידת הפירוט של ה-Log

יצירת סריקה חדשה

בתפריט יש לבחור Scan וללחוץ על Start New Scan



Scan Name – שם הסריקה, לזיהוי הסריקה בהמשך

Profile – בחירה בפרופיל מתאים מבין הפרופילים שיצרו

Systems to scan – רשימת כתובות ה-IP של המערכות שרוצים לסרוק

וכעת לחיצה על הכפתור Start תחל את הסריקה



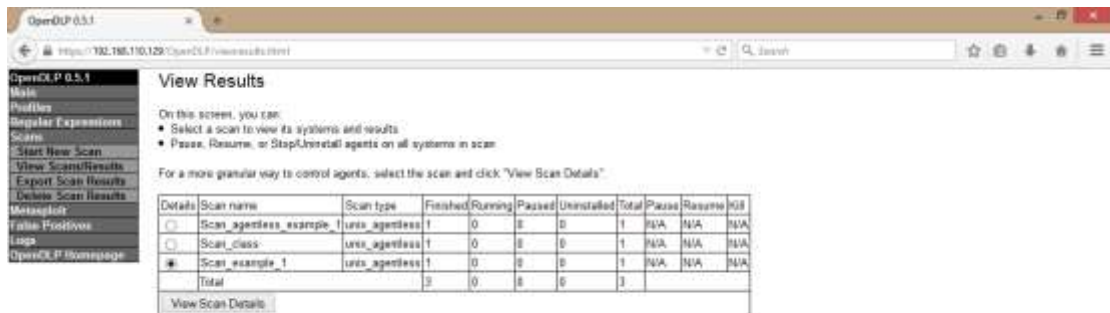
ניתן לראות חלונית General scan information עם פרטים בסיסיים אודות הסריקה

השורות שמתחת לחלונית ישנן שורות הסבר על הפעולות שמתבצעות, במקרה של הדוגמה שלנו ניתן לראות ש-OpenDLP מנסה להריץ את הסריקה על המערכת שבכתובת ה-IP 192.168.110.130 ובהמשך מודיע שהסריקה החלה.

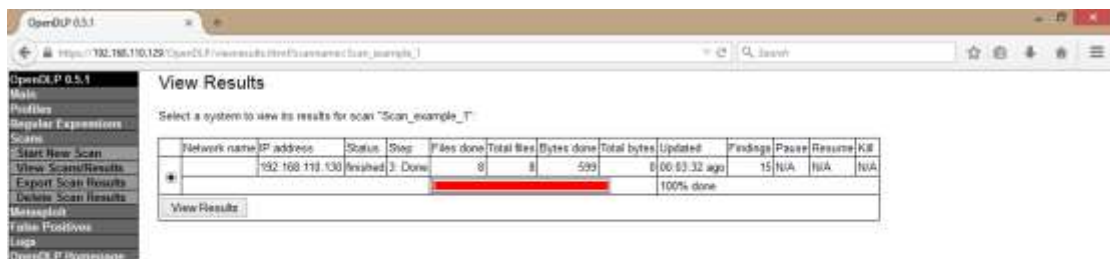
במידה והיו נבחרות מערכות נוספות לסריקה היו מופיעות שורות נוספות המעידות על נסיון הרצת הסריקה ובהמשך האם היא החלה.

תוצאות הסריקה

בכל שלב בסריקה (גם אם לא הסתיימה) ניתן לגשת לחלון הצגת תוצאות הסריקה באמצעות לחיצה על View Scans/Results ולצפות בממצאים עבור כל סריקה שבוצעה באמצעות התוכנה.



לחיצה על הכפתור View Scan Details תוך סימון הסריקה המתאימה תציג לנו חלון עם תקציר ממצאי הסריקה



ולחיצה על הכפתור View Results יציג לנו את ממצאי הסריקה בפירוט

OpenDLP 0.5.1

View Results

Results for 192.168.110.130

Profile	openDLP_eocorp1e
Status	Finished
Step	3. Done
Files Done	0
Files Total	0
Bytes Done	699
Bytes Total	0
Progress	<div style="width: 100%; background-color: red;"></div>
Percentage	100%
Completion Time	
Total Findings	15
False Positives	0
Valid Findings	15
Updated	00:05:07 ago
Pause	N/A
Resume	N/A
Kill	N/A

#	Regex	Pattern	File (click to download)	Byte offset	False?
1	AMEX	371449631398421	/var/www/PastFiles/amex.txt	0	<input type="checkbox"/>
2	Social_Security_Number_dashes	003-18-1123	/var/www/PastFiles/false_ssn_2	0	<input type="checkbox"/>
3	Social_Security_Number_dashes	400-41-2234	/var/www/PastFiles/false_ssn_2	12	<input type="checkbox"/>
4	Social_Security_Number_dashes	219-34-3345	/var/www/PastFiles/false_ssn_2	25	<input type="checkbox"/>
5	Social_Security_Number_dashes	003-18-3425	/var/www/PastFiles/amex.txt	0	<input type="checkbox"/>
6	Social_Security_Number_dashes	400-41-5325	/var/www/PastFiles/amex.txt	12	<input type="checkbox"/>
7	Social_Security_Number_dashes	219-34-5346	/var/www/PastFiles/amex.txt	25	<input type="checkbox"/>
8	Visa	4444444444444444	/var/www/PastFiles/amex.txt	0	<input type="checkbox"/>

כפי שניתן לראות בדוגמה, נסרקו 8 קבצים ובתוכם נמצאו 15 פרטי מידע רגישים בינהם מספר כרטיס אשראי מסוג American Express ומסוג Visa ומספרי ביטוח לאומי.

ניתן לסמן ממצאי פרטי מידע ספציפיים כתוצאות False Positive, מה שאומר שאמנם התוכנה OpenDLP זיהתה את הפריט כמידע רגיש אך אנו, כבני אדם, מחליטים שהוא אינו כזה.

ולבסוף בלחיצה על Export Scan Results אפשר לייצא את פירוט הסריקה וממצאיה לקובץ XML.