opendlp
Data Loss Prevention

Security Tool Demonstration

OpenDLP: Data Loss Prevention

Presented by :
A1 - Group 3

OVERVIEW & INSTALLATION

What is DLP

Data loss prevention (DLP) refers to the software tools and processes used to **protect data and detect the presence of malicious actors**.

Data loss can be categorized in the following types

- Accidental Data loss:
  - Employees unfamiliar with the company policies
  - Insecure handling of sensitive materials (employees' lack of proper training)
- Internal Attacks:
  - Malicious attacks by a person with authorized system access.
- External Attacks:
  - An external attack is an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to physical or logical resources

How DLP software works

- Data loss prevention products allow organizations to establish policies for how data should be protected in the following circumstances:
  - at rest (e.g., data stored on a hard drive)
  - in motion (e.g., data traveling on a network)
  - in use (e.g., data being used by someone who is accessing and modifying files)
- If any of those violations are identified, DLP enforces remediation with alerts, encryption, and other protective actions to prevent end users.
- DLP also provides reporting to meet compliance and auditing requirements and identify areas of weakness and anomalies for forensics and incident response.

opendlp

Data Loss Prevention

OpenDLP, an open source data loss prevention tool.

- ★ Scan databases for sensitive information.
- ★ OpenDLP is capable of searching for regular expressions found in cleartext.
- ★ OpenDLP is an example of a simplified DLP tool that has a subset of the capabilities of a COTS tool set.

Background

- The user can configure the tool to search documents for specific phrases that may identify sensitive information.
- The user can also create different scanning profiles to search for specific phrases.
- OpenDLP can identify basic Microsoft Office documents and other zip files containing sensitive information.
- The reports generated from this tool can be used to further mitigate insider threat through the use of access control lists (ACLs) and auditing.

OpenDLP and Regular Expressions

- OpenDLP contains built-in regular expressions (RegExs) for all major credit cards and social security numbers.
- Any number of regular expressions can be crafted for a specific need within the organization.
- The implementer only needs to have a basic understanding of regular expressions to create new expressions.

Keywords	Regular Expression
Company Confidential	`(?ism)COMPANY\sCONFIDENTIAL`
Company Proprietary	`(?ism)COMPANY\sPROPRIETARY`

Requirements for OpenDLP

Oracle's VirtualBox

OpenDLP VM image files

Source Code

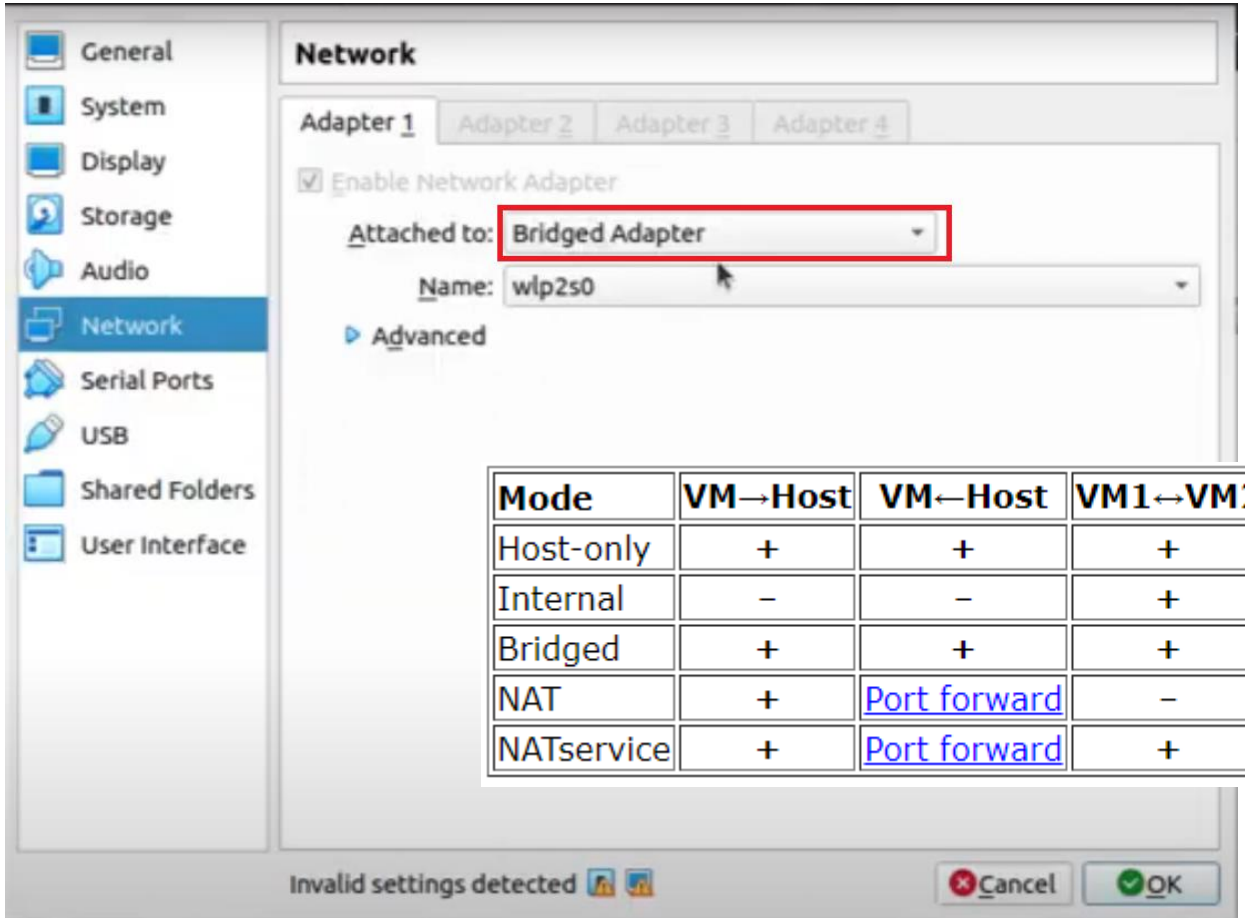
README-VM.txt

- Source code is also available to download and install
- README-VM.txt file that is bundled with the virtual machine images contains instructions that should be followed to configure the software properly

Installation

- Download all the 7zip files from this link: Google Code Archive - Long-term storage for Google Code Project Hosting.
- In Ubuntu, install 7zip and run the following commands: 7za OpenDLP-0.5.1-VM.7z.001
- Import “ova” file on VirtualBox.
- To connect to openDLP from the host machine, configure networking in “Bridge mode”.
- To connect to VM: username-opendlp, password-opendlp
- For details information: openDLP/README.md at main · cloudsecuritylabs/openDLP (github.com)

Installation



Mode	VM→Host	VM←Host	VM1↔VM2	VM→Net/LAN	VM←Net/LAN
Host-only	+	+	+	–	–
Internal	–	–	+	–	–
Bridged	+	+	+	+	+
NAT	+	Port forward	–	+	Port forward
NATservice	+	Port forward	+	+	Port forward

Installation

```
File  Machine  View  Input  Devices  Help
[    7.088234] intel8x0: measure - unreliable DMA position..
[    7.448017] intel8x0: measure - unreliable DMA position..
[    7.808034] intel8x0: measure - unreliable DMA position..

Ubuntu 11.04 opendlp tty1

opendlp login: opendlp
Password:
Last login: Mon Aug 27 15:32:16 EDT 2012 on tty1
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-8-generic i686)

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

 System information disabled due to load higher than 1.0
opendlp@opendlp:~$
opendlp@opendlp:~$
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: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 08:00:27:58:82:6e brd ff:ff:ff:ff:ff:ff
opendlp@opendlp:~$ sudo vi /etc/network/interfaces
[sudo] password for opendlp: _
```

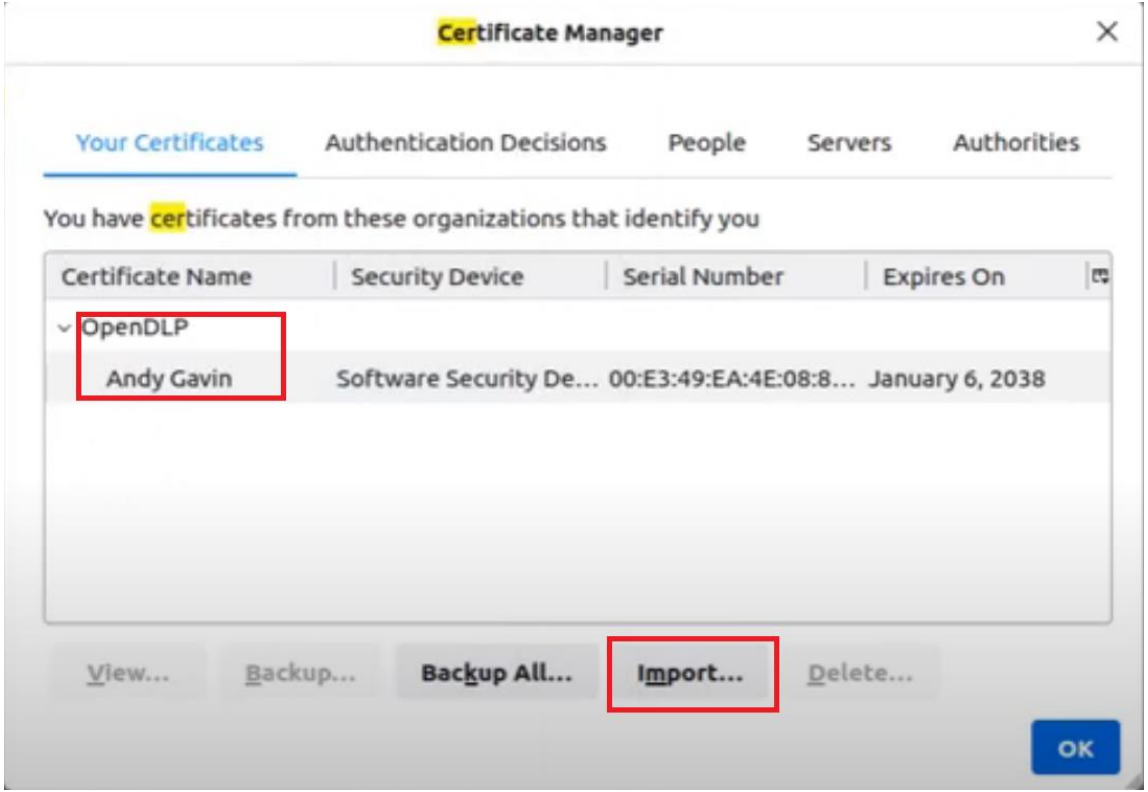
```
File  Machine  View  Input  Devices  Help

"/etc/network/interfaces" 10L, 268C written
opendlp@opendlp:~$
opendlp@opendlp:~$
opendlp@opendlp:~$
opendlp@opendlp:~$ ifdown eth1
ifdown: failed to open statefile /var/run/network/ifstate: Permission denied
opendlp@opendlp:~$ sudo ifdown eth1
ifdown: interface eth1 not configured
opendlp@opendlp:~$ sudo ifup eth1
ssh stop/waiting
ssh start/running, process 1148
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: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
en 1000
    link/ether 08:00:27:58:82:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.28/24 brd 192.168.0.255 scope global eth1
    inet6 2601:c2:d00:aa0:a00:27ff:fe58:826e/64 scope global dynamic
       valid_lft 272636sec preferred_lft 272636sec
    inet6 fe80::a00:27ff:fe58:826e/64 scope link
       valid_lft forever preferred_lft forever
opendlp@opendlp:~$
```

Installation

https://192.168.0.28

Secure Connection Failed



TECHNICAL DETAILS & PROFILE CREATION

Technical Design & System Architecture

OpenDLP has two types of basic components:

- ❑ A web application to manage Windows agents, Windows/UNIX/database agentless scanners and scan results.
- ❑ A microsoft windows agent used to perform accelerated scans of up to thousands of systems simultaneously.

Technical Design & System Architecture

- The agent is written in C programming language.
- The agents resumes automatically upon system reboots without any interaction from the user.
- Securely transmits results to central management web application at user defined intervals over two-way-trusted SSL connections.
- To identify sensitive data, it uses Perl Compatible Regular Expressions(PCREs) and can read inside compressed file.
- Limits itself to a percent of physical memory of the machine running it.

Working Principle

OpenDLP is a flexible tool that can be used in different, creative ways, but the basic workflow is as follows:

- ❑ Review the provided Regular Expressions for data to look for
- ❑ Create a profile with authentication credentials and policy settings
- ❑ Start a scan by providing a list of IPs.
- ❑ Review the scan results and mark false positives
- ❑ Report any suspect business sensitive or compliant data found
- ❑ Work with the information owners and Office of Information Security to develop a remediation plan

OpenDLP's Main Interface

- OpenDLP 0.5.1
- Main
- Profiles
- Regular Expressions
- Scans
- Metasploit
- False Positives
- Logs
- OpenDLP Homepage

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 reusable 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
- Resumes 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 integreated with Metasploit through Messagepack RPC
- Retrieves list of exploited machines from Metasploit and displays in OpenDLP GUI
- Deploys OpenDLP directly from Metasploit to exploied machines of your choosing
- Domain credentials not required, if you can "get system" on the target from a metasploit ponsole, 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
Starting with OpenDLP 0.4, you can now perform agentless data discovery against the following systems:
- Microsoft Windows operating systems over SMB
- UNIX operating systems over SSH
- Microsoft Windows network shares over SMB

To Get Started
Assuming the README has been followed and OpenDLP is properly installed on the web server, you can:
- Review existing PCREs and add your own
- Create a profile with PCREs, appropriate authentication credentials, and other policy settings
- Start a scan by providing a list of Windows systems
- Review results and mark false positives
- Export the scan as XML and use the data offline

OpenDLP is maintained by Andrew Gavin at http://opendlp.googlecode.com.

Review the provided Regular Expressions for data to look for

OpenDLP 0.5.1 | OpenDLP 0.5.1

https://192.168.0.7/OpenDLP/regex-delete.html

- OpenDLP 0.5.1
- Main
- Profiles
- Regular Expressions
  - Create New Regex
  - Delete Regex
- Scans
- Metasploit
- False Positives
- Logs
- OpenDLP Homepage

Delete an existing regular expression

Delete	Regex Name	Regex
☐	AMEX	(\D|^)(34|37)[0-9]{2}(\ |\-|)[0-9]{6}(\ |\-|)[0-9]{5}(\D|$)
☐	card	1234*
☐	Credit_Card_Track_1	(\D|^)\%?[Bb]\d{13,19}\^[\-\/\.\w\s]{2,26}\^[0-9][0-9][01][0-9][0-9]{3}
☐	Credit_Card_Track_2	(\D|^)\;\d{13,19}\=(\d{3}|)(\d{4}|\=)
☐	Credit_Card_Track_Data	[1-9][0-9]{2}\-[0-9]{2}\-[0-9]{4}\^\d
☐	Diners_Club_1	(\D|^)30[0-5][0-9](\ |\-|)[0-9]{6}(\ |\-|)[0-9]{4}(\D|$)
☐	Diners_Club_2	(\D|^)(36|38)[0-9]{2}(\ |\-|)[0-9]{6}(\ |\-|)[0-9]{4}(\D|$)
☐	Discover	(\D|^)6011(\ |\-|)[0-9]{4}(\ |\-|)[0-9]{4}(\ |\-|)[0-9]{4}(\D|$)
☐	JCB_1	(\D|^)3[0-9]{3}(\ |\-|)[0-9]{4}(\ |\-|)[0-9]{4}(\ |\-|)[0-9]{4}(\D|$)
☐	JCB_2	(\D|^)(2131|1800)[0-9]{11}(\D|$)
☐	Mastercard	(\D|^)5[1-5][0-9]{2}(\ |\-|)[0-9]{4}(\ |\-|)[0-9]{4}(\ |\-|)[0-9]{4}(\D|$)
☐	Social_Security_Number_dashes	(\D|^)[0-9]{3}\-[0-9]{2}\-[0-9]{4}(\D|$)
☐	Social_Security_Number_spaces	(\D|^)[0-9]{3}\ [0-9]{2}\ [0-9]{4}(\D|$)
☐	Visa	(\D|^)4[0-9]{3}(\ |\-|)[0-9]{4}(\ |\-|)[0-9]{4}(\ |\-|)[0-9]{4}(\D|$)

Delete

Create a profile with authentication credentials

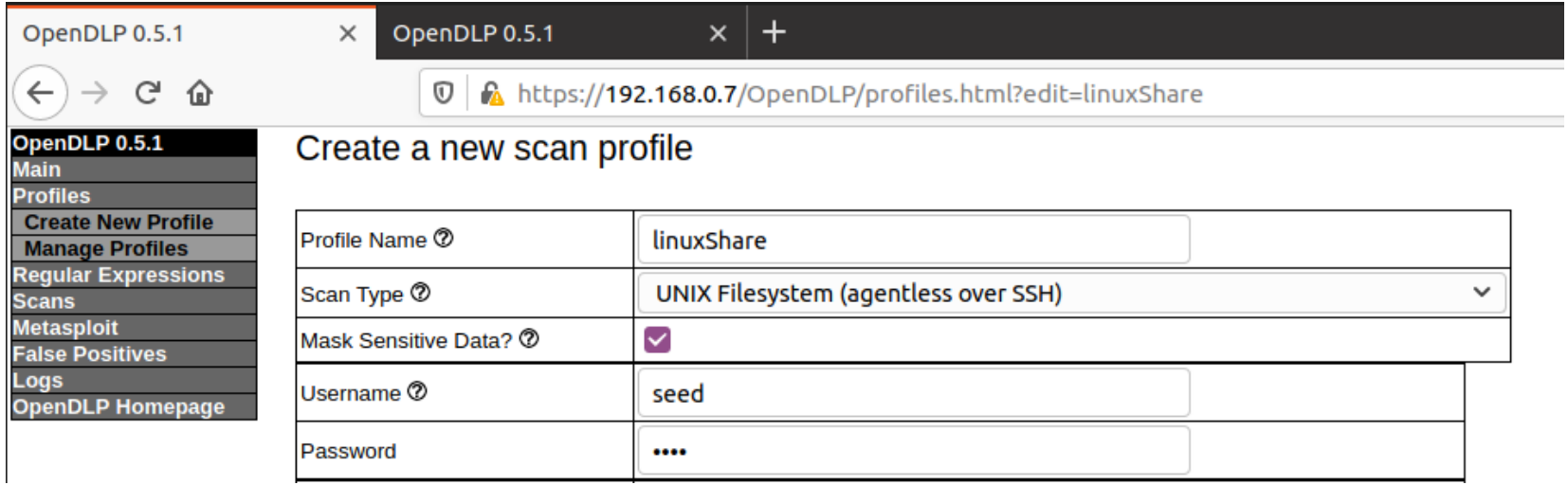
- ❑ Enter a profile name in the “Profile Name” field.
- ❑ Set the scan type to “Linux Filesystem (agentless over SSH).”
- ❑ Select whether or not you want to mask the sensitive data in the scan results.
- ❑ Enter the administrator’s username for the targets of the scan and corresponding password.

Profiles

Profiles are used to define the scan types to be done as well as to provide and store the credentials necessary to perform the scan. OpenDLP uses the following profile types:

- ❑ Windows Filesystem(agent)
- ❑ Windows Filesystem(agentless over SMB)
- ❑ Windows File Network Share(agentless SMB)
- ❑ UNIX Filesystem(agentless over SSH)
- ❑ Microsoft SQL server(agent)
- ❑ Mysql(agentless)

Create a profile with authentication credentials (contd.)



Create a profile with authentication credentials (contd.)

- ❑ Limit the percent of physical memory of the machine running to a certain value.
- ❑ Indicate which client directories to scan(e.g., /home/seed/Share).
- ❑ Set the File Extensions option accordingly.

Create a profile with authentication credentials (contd.)

Memory Limit (as percent of target system's total RAM)	20%
Directories (Newline-delimit the file extensions in this list)	○ Scan all directories ○ Scan all directories except these (recursive) ◉ Only scan the following directories (recursive) /home/seed/Share
File Extensions (Newline-delimit the file extensions in this list)	○ Scan all files ◉ Scan all files except files with the following extensions ○ Only scan files with the following file extensions 323 386 3g2 3gp 3gp2 3gpp 7z aac aca ace aif

Create a profile with authentication credentials (contd.)

- ❑ Select the regular expressions to include in the scan(include RegExs for Top Secret, Secret, and Confidential).
- ❑ Set the concurrent deployments to a number between 1 and 100. Depending on -
  - ❑ Environment
  - ❑ The system resources available to the OpenDLP virtual machine.
  - ❑ The options selected in the scan.
- ❑ Click the “Submit” button to save the scanning profile

Create a profile with authentication credentials (contd.)

Regular Expressions	AMEX Credit_Card_Track_1 Credit_Card_Track_2 Credit_Card_Track_Data Diners_Club_1 Diners_Club_2 Discover JCB_1 JCB_2 Mastercard Social_Security_Number_dashes Social_Security_Number_spaces Visa card
Credit Cards (Newline-delimit the names of the regex aliases)	Mastercard Visa AMEX Diners_Club_1 Diners_Club_2 Discover JCB_1 JCB_2
ZIP Extensions (Treat these extensions as ZIP files. Newline-delimit the names of file extensions.)	zip jar xlsx docx pptx odt odp ods odg
Concurrent deployments (Only for initial deployment, not running)	2
Log Verbosity	1 - More Verbose (Not recommended for large (100+) deployments)
Submit	Submit

SCANNING & RESULT ANALYSIS

Content Analysis Techniques

- ❑ Content Analysis using Regular Expressions.
- ❑ Fingerprinting.
- ❑ Partial Document Matching.
- ❑ Statistical Analysis.
- ❑ Conceptual/Lexicon
- ❑ Categories

Agent Vs Agentless Scanning

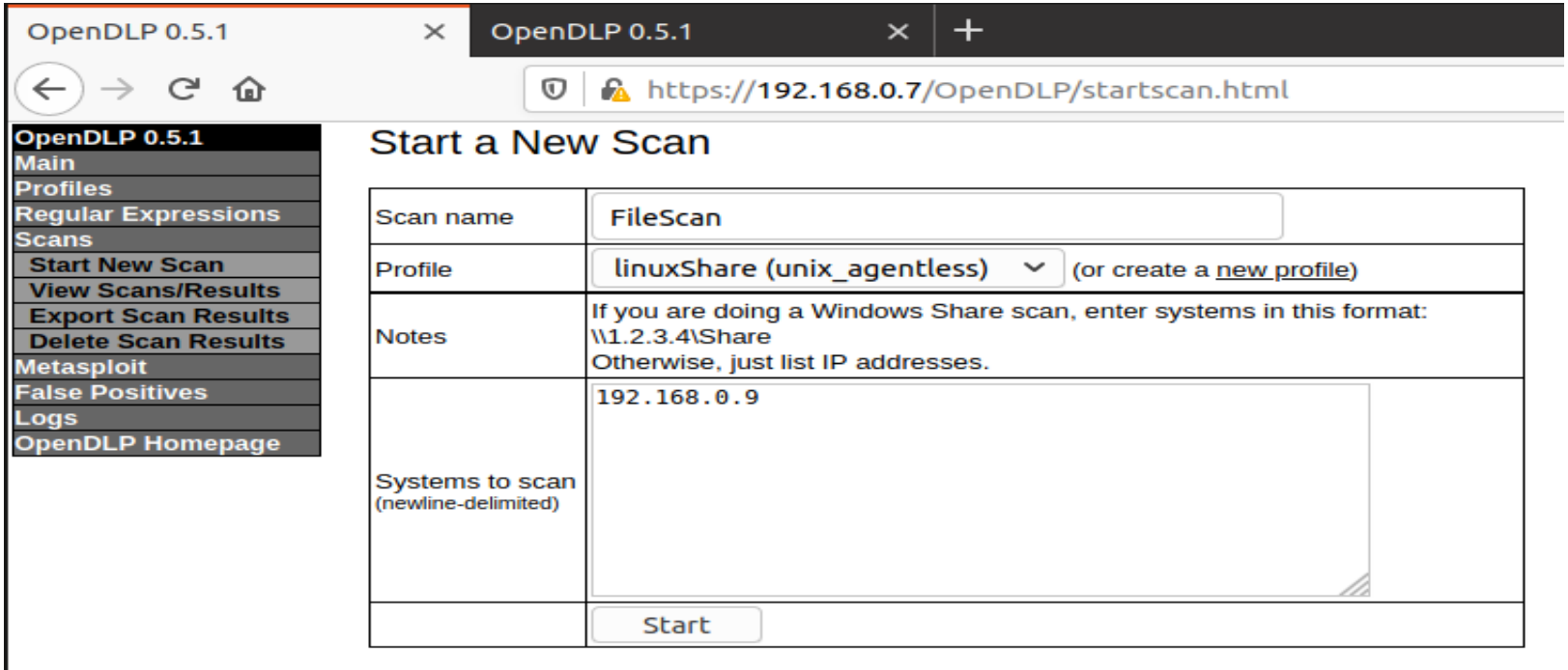
An agent-based scan deploys a software package to a client that searches for sensitive data and returns the results to the OpenDLP server.

Agentless scans are conducted by the OpenDLP server, where the results are processed and stored.

Start a scan by providing a list of IPs

- ❑ Enter a scan name in the “Scan Name” field.
- ❑ Select the appropriate scanning profile.
- ❑ Enter the IP address(es) to include in the scan.
- ❑ Click the Start button.

Start a scan by providing a list of IPs(contd.)



Review the scan results and mark false positives

OpenDLP 0.5.1 | OpenDLP 0.5.1

https://192.168.0.7/OpenDLP/logs.html?scanname=FileScan&system=02E72338C8AC6772FC9EC8

- OpenDLP 0.5.1
- Main
- Profiles
- Regular Expressions
- Scans
- Metasploit
- False Positives
- Logs
- OpenDLP Homepage

View Logs

Logs for 192.168.0.9:

Profile	linuxShare
Status	finished
Step	3: Done
Files Done	2
Files Total	2
Bytes Done	2,030
Bytes Total	0
Total Findings	25
False Positives	0
Valid Findings	25
Updated	00:00:29 ago

#	Timestamp	Log Entry
1	Thu Jul 28 12:01:26 2022	Attempting to start discovery
2	Thu Jul 28 12:01:26 2022	Retrieved all profile information
3	Thu Jul 28 12:01:26 2022	Ignore dirs option: allow
4	Thu Jul 28 12:01:26 2022	Ignore file extensions option: ignore
5	Thu Jul 28 12:01:26 2022	Total system memory is 520187904; limiting memory usage to 104034304
6	Thu Jul 28 12:01:26 2022	Starting to enumerate files and directories
7	Thu Jul 28 12:01:27 2022	Processing this directory on 192.168.0.9: /home/seed/Share (aka /tmp/OpenDLP/4/home/seed/Share)
8	Thu Jul 28 12:01:27 2022	Searching files for regular expressions
9	Thu Jul 28 12:02:12 2022	Done with UNIX agentless file system scan

Review the scan results and mark false positives (contd.)

OpenDLP 0.5.1 | OpenDLP 0.5.1

https://192.168.0.7/OpenDLP/vie

- OpenDLP 0.5.1
- Main
- Profiles
- Regular Expressions
- Scans
  - Start New Scan
  - View Scans/Results
  - Export Scan Results
  - Delete Scan Results
- Metasploit
- False Positives
- Logs
- OpenDLP Homepage

View Results

Results for 192.168.0.9:

Profile	linuxShare
Status	finished
Step	3: Done
Files Done	2
Files Total	2
Bytes Done	2,030
Bytes Total	0
Progress	
Percentage	100%
Completion Time	
Total Findings	25
False Positives	0
Valid Findings	25
Updated	00:01:08 ago
Pause	N/A
Resume	N/A
Kill	N/A

#	Regex	Pattern	File (click to download)	Byte offset	False?
1	AMEX	XXXXXXXXXXXXX126?	/home/seed/Share/secret.txt	72	
2	AMEX	XXXXXXXXXXXXX005?	/home/seed/Share/secret.txt	113	
3	Discover	XXXXXXXXXXXXXX009?	/home/seed/Share/secret.txt	273	
4	JCB_1	XXXXXXXXXXXXXX410?	/home/seed/Share/secret.txt	322	
5	JCB_1	XXXXXXXXXXXXXX000?	/home/seed/Share/secret.txt	376	
6	Mastercard	XXXXXXXXXXXXXX903?	/home/seed/Share/secret.txt	432	
7	Mastercard	XXXXXXXXXXXXXX903?	/home/seed/Share/secret.txt	480	
8	Mastercard	XXXXXXXXXXXXXX118?	/home/seed/Share/secret.txt	1318	
9	Visa	XXXXXXXXXXXXXX299?	/home/seed/Share/secret.txt	628	
10	Visa	XXXXXXXXXXXXXX299?	/home/seed/Share/secret.txt	697	
11	Visa	XXXXXXXXXXXXXX299?	/home/seed/Share/secret.txt	766	
12	Visa	XXXXXXXXXXXXXX107?	/home/seed/Share/secret.txt	835	
13	Visa	XXXXXXXXXXXXXX193?	/home/seed/Share/secret.txt	891	
14	Visa	XXXXXXXXXXXXXX454?	/home/seed/Share/secret.txt	942	
15	card	XXX	/home/seed/Share/secret.txt	350	
16	Discover	XXXXXXXXXXXXXX818?	/home/seed/Share/mastercard.txt	561	
17	Visa	XXXXXXXXXXXXXX019?	/home/seed/Share/mastercard.txt	66	
18	Visa	XXXXXXXXXXXXXX008?	/home/seed/Share/mastercard.txt	115	
19	Visa	XXXXXXXXXXXXXX005?	/home/seed/Share/mastercard.txt	164	
20	Visa	XXXXXXXXXXXXXX000?	/home/seed/Share/mastercard.txt	211	
21	Visa	XXXXXXXXXXXXXX026?	/home/seed/Share/mastercard.txt	258	
22	Visa	XXXXXXXXXXXXXX564?	/home/seed/Share/mastercard.txt	307	
23	Visa	XXXXXXXXXXXXXX409?	/home/seed/Share/mastercard.txt	354	
24	Visa	XXXXXXXXXXXXXX026?	/home/seed/Share/mastercard.txt	401	
25	Visa	XXXXXXXXXXXXXX417?	/home/seed/Share/mastercard.txt	450	

Mark Selected as False Positives

Mark False Positives

#	Regex	Pattern	File (click to download)	Byte offset	False?
1	AMEX	XXXXXXXXXXXXX126?	/home/seed/Share/secret.txt	72	☐
2	AMEX	XXXXXXXXXXXXX005?	/home/seed/Share/secret.txt	113	☐
3	Discover	XXXXXXXXXXXXXX009?	/home/seed/Share/secret.txt	273	☑
4	JCB_1	XXXXXXXXXXXXXX410?	/home/seed/Share/secret.txt	322	☑
5	JCB_1	XXXXXXXXXXXXXX000?	/home/seed/Share/secret.txt	376	☑
6	Mastercard	XXXXXXXXXXXXXX903?	/home/seed/Share/secret.txt	432	☐
7	Mastercard	XXXXXXXXXXXXXX903?	/home/seed/Share/secret.txt	480	☐

OpenDLP 0.5.1
Main
Profiles
Regular Expressions
Scans
Metasploit
False Positives
Logs
OpenDLP Homepage

View False Positives

On this screen, you can:

- Select a scan to view the false positives associated with its systems
- After selecting a scan, reverse false positives so they display in results

Details	Scan name	False Positives
○	Scan101	3
○	tanvirscan2	1

View False Positives

OpenDLP 0.5.1
Main
Profiles
Regular Expressions
Scans
Metasploit
False Positives
Logs
OpenDLP Homepage

View False Positives

Select a system in scan "Scan101" to view its detailed false positives:

	Network name	IP address	False Positives
◉	192.168.0.9	192.168.0.9	3

View False Positives

OpenDLP 0.5.1
Main
Profiles
Regular Expressions
Scans
Metasploit
False Positives
Logs
OpenDLP Homepage

View False Positives

Select a false positive to clear for system 192.168.0.9 in scan "Scan101":

#	Regex	Pattern	File	Byte offset	False?
1	Discover	XXXXXXXXXXXXXX009?	/home/seed/Share/secret.txt	273	☐
2	JCB_1	XXXXXXXXXXXXXX410?	/home/seed/Share/secret.txt	322	☐
3	JCB_1	XXXXXXXXXXXXXX000?	/home/seed/Share/secret.txt	376	☐

Mark Selected as NOT False Positives

Mark False Positives

#	Regex	Pattern	File (click to download)	Byte offset	False?
1	AMEX	XXXXXXXXXXXXX126?	/home/seed/Share/secret.txt	72	☐
2	AMEX	XXXXXXXXXXXXX005?	/home/seed/Share/secret.txt	113	☐
3	Mastercard	XXXXXXXXXXXXXX903?	/home/seed/Share/secret.txt	432	☐
4	Mastercard	XXXXXXXXXXXXXX903?	/home/seed/Share/secret.txt	480	☐
5	Mastercard	XXXXXXXXXXXXXX118?	/home/seed/Share/secret.txt	1318	☐
6	Visa	XXXXXXXXXXXXXX299?	/home/seed/Share/secret.txt	628	☐
7	Visa	XXXXXXXXXXXXXX299?	/home/seed/Share/secret.txt	697	☐
8	Visa	XXXXXXXXXXXXXX299?	/home/seed/Share/secret.txt	766	☐
9	Visa	XXXXXXXXXXXXXX107?	/home/seed/Share/secret.txt	835	☐
10	Visa	XXXXXXXXXXXXXX193?	/home/seed/Share/secret.txt	891	☐
11	Visa	XXXXXXXXXXXXXX454?	/home/seed/Share/secret.txt	942	☐
12	card	XXX	/home/seed/Share/secret.txt	350	☐
13	Discover	XXXXXXXXXXXXXX818?	/home/seed/Share/mastercard.txt	561	☐
14	Visa	XXXXXXXXXXXXXX019?	/home/seed/Share/mastercard.txt	66	☐
15	Visa	XXXXXXXXXXXXXX008?	/home/seed/Share/mastercard.txt	115	☐
16	Visa	XXXXXXXXXXXXXX005?	/home/seed/Share/mastercard.txt	164	☐
17	Visa	XXXXXXXXXXXXXX000?	/home/seed/Share/mastercard.txt	211	☐
18	Visa	XXXXXXXXXXXXXX026?	/home/seed/Share/mastercard.txt	258	☐
19	Visa	XXXXXXXXXXXXXX564?	/home/seed/Share/mastercard.txt	307	☐
20	Visa	XXXXXXXXXXXXXX409?	/home/seed/Share/mastercard.txt	354	☐
21	Visa	XXXXXXXXXXXXXX026?	/home/seed/Share/mastercard.txt	401	☐
22	Visa	XXXXXXXXXXXXXX417?	/home/seed/Share/mastercard.txt	450	☐
					Mark Selected as False Positives

Limitations

- No advanced content analysis – regex only.
- Unable to scan non-plain-text or compressed files (including current versions of Office).
- Can be defeated by encryption.
- Requires NetBIOS, which some environments ban (Backdated, not used anymore).
- Complicated codebase.

References

- openDLP/README.md at main · cloudsecuritylabs/openDLP (github.com)
- (244) Install OpenDLP Virtual Machine - Download, Import to Virtual Box, Configure Networking, manage UI - YouTube
- (244) OpenDLP: How To Perform Scan-Create Scan Profile, Perform Scan, Review Results, Update Regex (Part2) - YouTube

Thank You