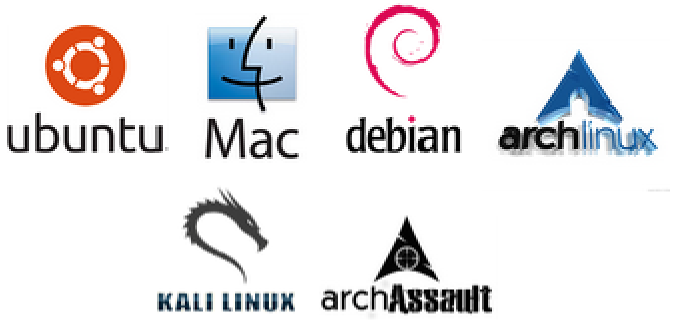
Installation

The following platforms are supported:



Read more about this.

Quick install

For many OSes, you can quickly install Faraday by either downloading the latest tarball or cloning the Faraday Git Project, and running:

```
$ git clone https://github.com/infobyte/faraday.git faraday-dev
$ cd faraday-dev

$ pip2 install -r requirements_server.txt
$ ./faraday-server.py

$ pip2 install -r requirements.txt
$ ./faraday.py
```

Read more about the installation process.

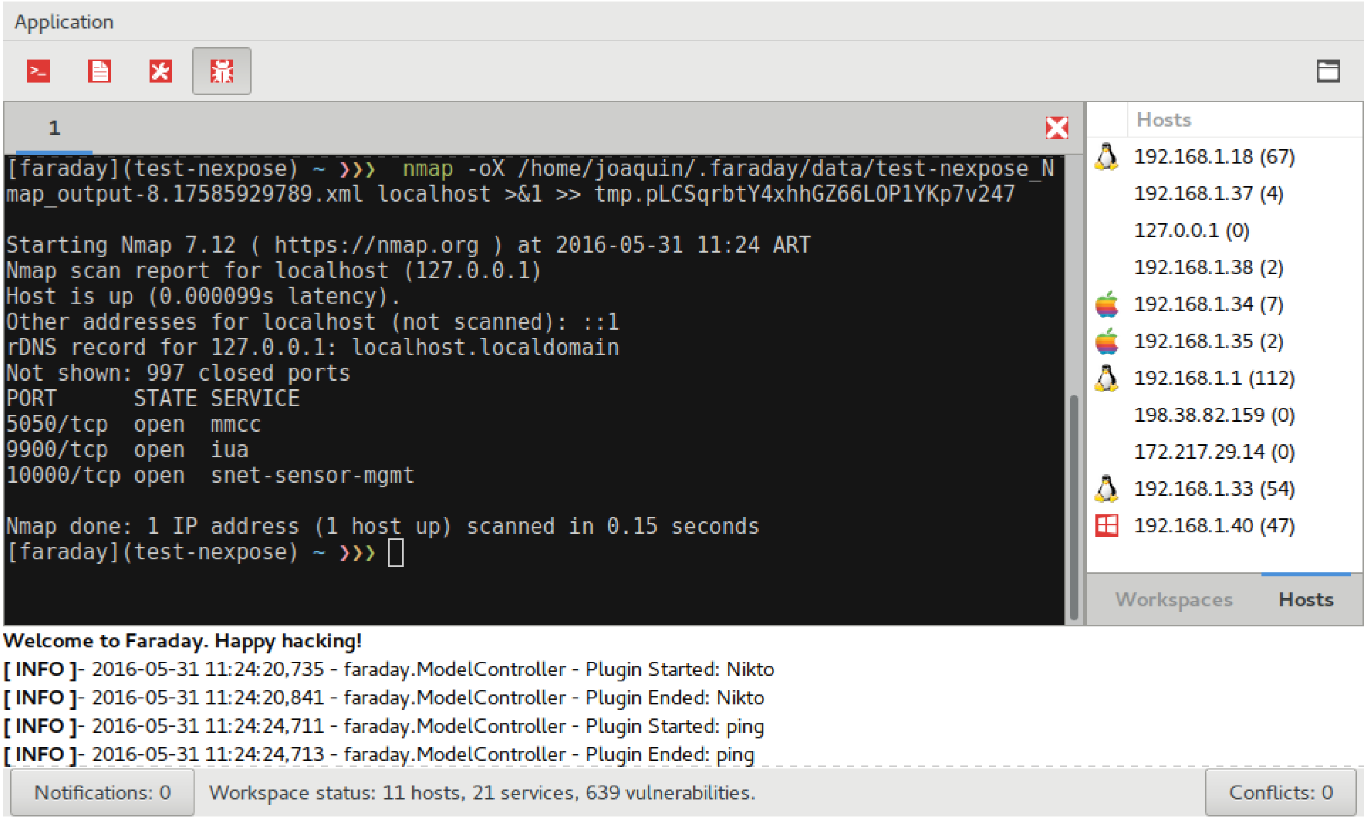
About

Faraday introduces a new concept - IPE (Integrated Penetration-Test Environment) a multiuser Penetration test IDE. Designed for distributing, indexing, and analyzing the data generated during a security audit.

> Made for true pentesters!

Faraday was made to let you take advantage of the available tools in the community in a truly multiuser way.

Designed for simplicity, users should notice no difference between their own terminal application and the one included in Faraday. Developed with a specialized set of functionalities, users improve their own work. Do you remember the last time you programmed without an IDE? What IDEs are to programming, Faraday is to pentesting.



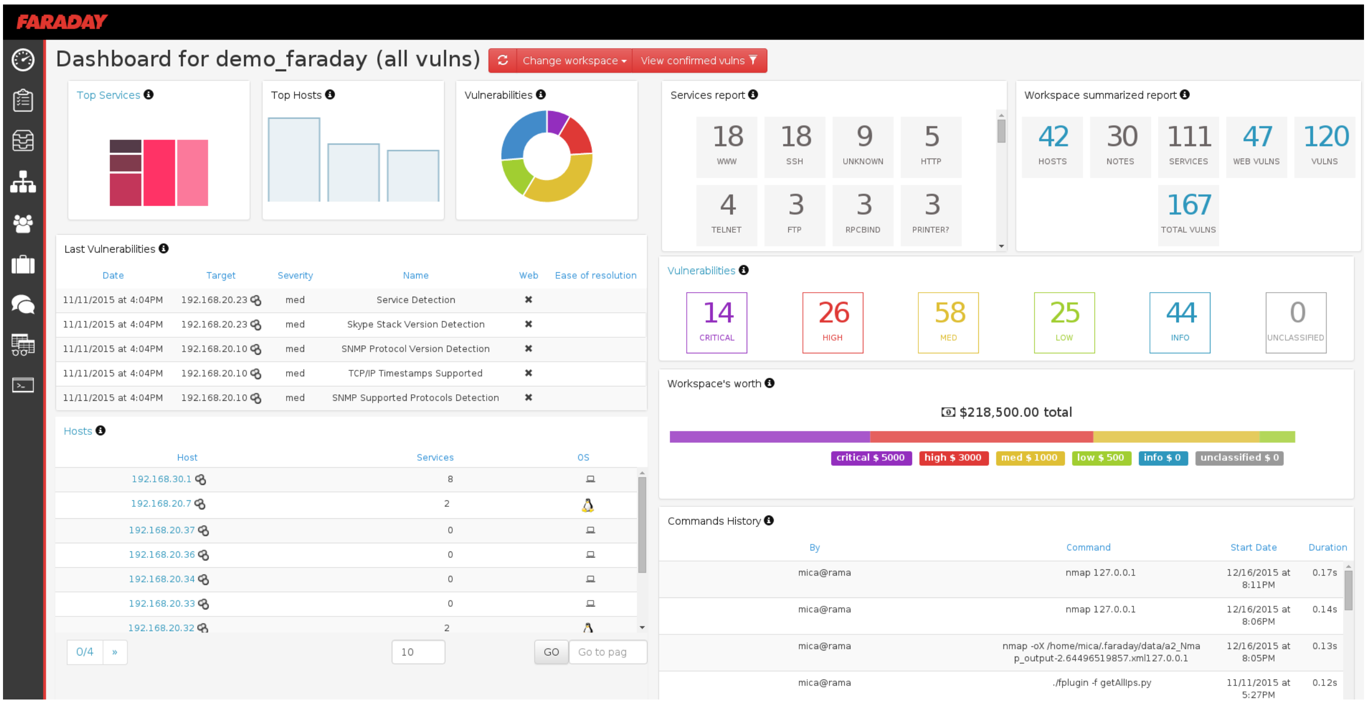
```
[faraday](test-nexpose) ~ ››› nmap -oX /home/joaquin/.faraday/data/test-nexpose_N
map_output-8.17585929789.xml localhost >&1 >> tmp.pLCSqrbtY4xhhGZ66LOP1YKp7v247

Starting Nmap 7.12 ( https://nmap.org ) at 2016-05-31 11:24 ART
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000099s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 997 closed ports
PORT      STATE SERVICE
5050/tcp  open  mmcc
9900/tcp  open  iua
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
[faraday](test-nexpose) ~ ›››
```

192.168.1.18 (67)
192.168.1.37 (4)
127.0.0.1 (0)
192.168.1.38 (2)
192.168.1.34 (7)
192.168.1.35 (2)
192.168.1.1 (112)
198.38.82.159 (0)
172.217.29.14 (0)
192.168.1.33 (54)
192.168.1.40 (47)

```
Welcome to Faraday. Happy hacking!
[ INFO ]- 2016-05-31 11:24:20,735 - faraday.ModelController - Plugin Started: Nikto
[ INFO ]- 2016-05-31 11:24:20,841 - faraday.ModelController - Plugin Ended: Nikto
[ INFO ]- 2016-05-31 11:24:24,711 - faraday.ModelController - Plugin Started: ping
[ INFO ]- 2016-05-31 11:24:24,713 - faraday.ModelController - Plugin Ended: ping
```

Notifications: 0 | Workspace status: 11 hosts, 21 services, 639 vulnerabilities. | Conflicts: 0

Faraday crunches the data you load into different visualizations that are useful to managers and pentesters alike.



Dashboard for demo_faraday (all vulns)

Services report

18	18	9	5
WWW	SSH	UNKNOWN	HTTP
4	3	3	3
TELNET	FTP	RPCBIND	PRINTER?

Workspace summarized report

42	30	111	47	120
HOSTS	NOTES	SERVICES	WEB VULNS	VULNS
		167		
		TOTAL VULNS		

Last Vulnerabilities

Date	Target	Severity	Name	Web	Ease of resolution
11/11/2015 at 4:04PM	192.168.20.23	med	Service Detection	✖	
11/11/2015 at 4:04PM	192.168.20.23	med	Skype Stack Version Detection	✖	
11/11/2015 at 4:04PM	192.168.20.10	med	SNMP Protocol Version Detection	✖	
11/11/2015 at 4:04PM	192.168.20.10	med	TCP/IP Timestamps Supported	✖	
11/11/2015 at 4:04PM	192.168.20.10	med	SNMP Supported Protocols Detection	✖	

Vulnerabilities

14	26	58	25	44	0
CRITICAL	HIGH	MED	LOW	INFO	UNCLASSIFIED

Hosts

Host	Services	OS
192.168.30.1	8	💻
192.168.20.7	2	🐧
192.168.20.37	0	💻
192.168.20.36	0	💻
192.168.20.34	0	💻
192.168.20.33	0	💻
192.168.20.32	2	🐧

0/4 » 10

Workspace's worth

$218,500.00 total

critical $ 5000 | high $ 3000 | med $ 1000 | low $ 500 | info $ 0 | unclassified $ 0

Commands History

By	Command	Start Date	Duration
mica@rama	nmap 127.0.0.1	12/16/2015 at 8:11PM	0.17s
mica@rama	nmap 127.0.0.1	12/16/2015 at 8:06PM	0.14s
mica@rama	nmap -oX /home/mica/.faraday/data/a2_Nmap_output-2.64496519857.xml127.0.0.1	12/16/2015 at 8:05PM	0.13s
mica@rama	./fplugin -f getAllIps.py	11/11/2015 at 5:27PM	0.12s

To read about the latest features check out the release notes!

Plugins list

You feed data to Faraday from your favorite tools through Plugins. Right now there are more than 60+ supported tools, among which you will find:

There are three Plugin types: **console** plugins which intercept and interpret the output of the tools you execute, **report** plugins which allows you to import previously generated XMLs, and **online** plugins which access Faraday's API or allow Faraday to connect to external APIs and databases.

Read more about Plugins.

Features

Workspaces

Information is organized into various **Workspaces**. Each Workspace contains a pentest team's assignments and all the intel that is discovered.

Conflicts

If two plugins produce clashing information for an individual element, a conflict that the user will have to resolve is generated. An example is if **user1** incorporates host *127.0.0.1 OS:Linux* and **user2** incorporates *127.0.0.1 OS: Linux Ubuntu 13.10*.

On our GTK interface there's a button on the bottom right corner of the main window displaying the number of conflicts in the current workspace. To resolve them, just click on the button and a window will open where you can edit the conflicting objects and select which one to keep.

Faraday plugin

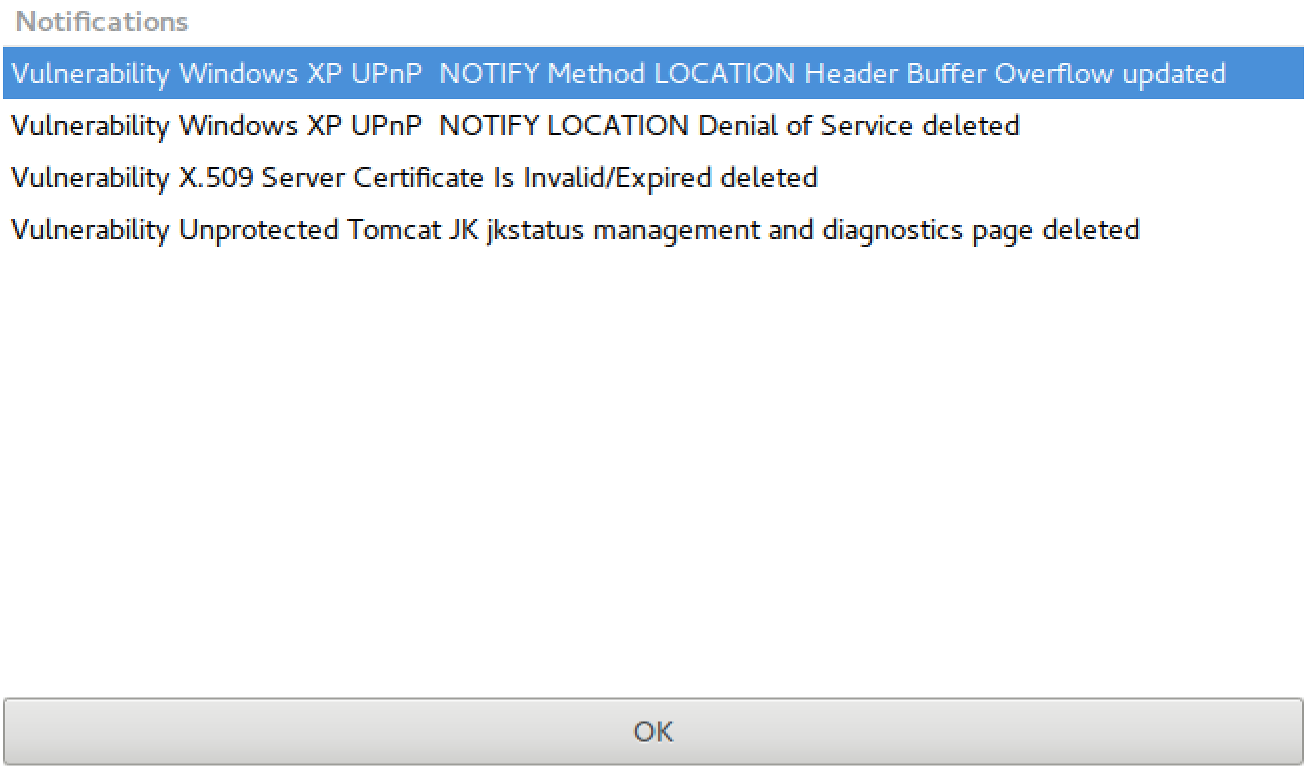
Using our plugin you can perform various actions using the command line, for example:

```
$ cd faraday-dev/bin/
$ ./fplugin create_host 192.154.33.222 Android
1a7b2981c7becbcb3d5318056eb29a58817f5e67
$ ./fplugin filter_services http ssh -p 21 -a
Filtering services for ports: 21, 22, 80, 443, 8080, 8443

192.168.20.1     ssh      [22]    tcp open    None
192.168.20.1     http     [443]   tcp open    None
192.168.20.7     ssh      [22]    tcp open    Linux
192.168.20.7     http     [443]   tcp open    Linux
192.168.20.11    ssh      [22]    tcp open    Linux
```

Read more about the Faraday Plugin.

Notifications

Updating objects on other Faraday instances result in notifications on your Faraday GTK Client.



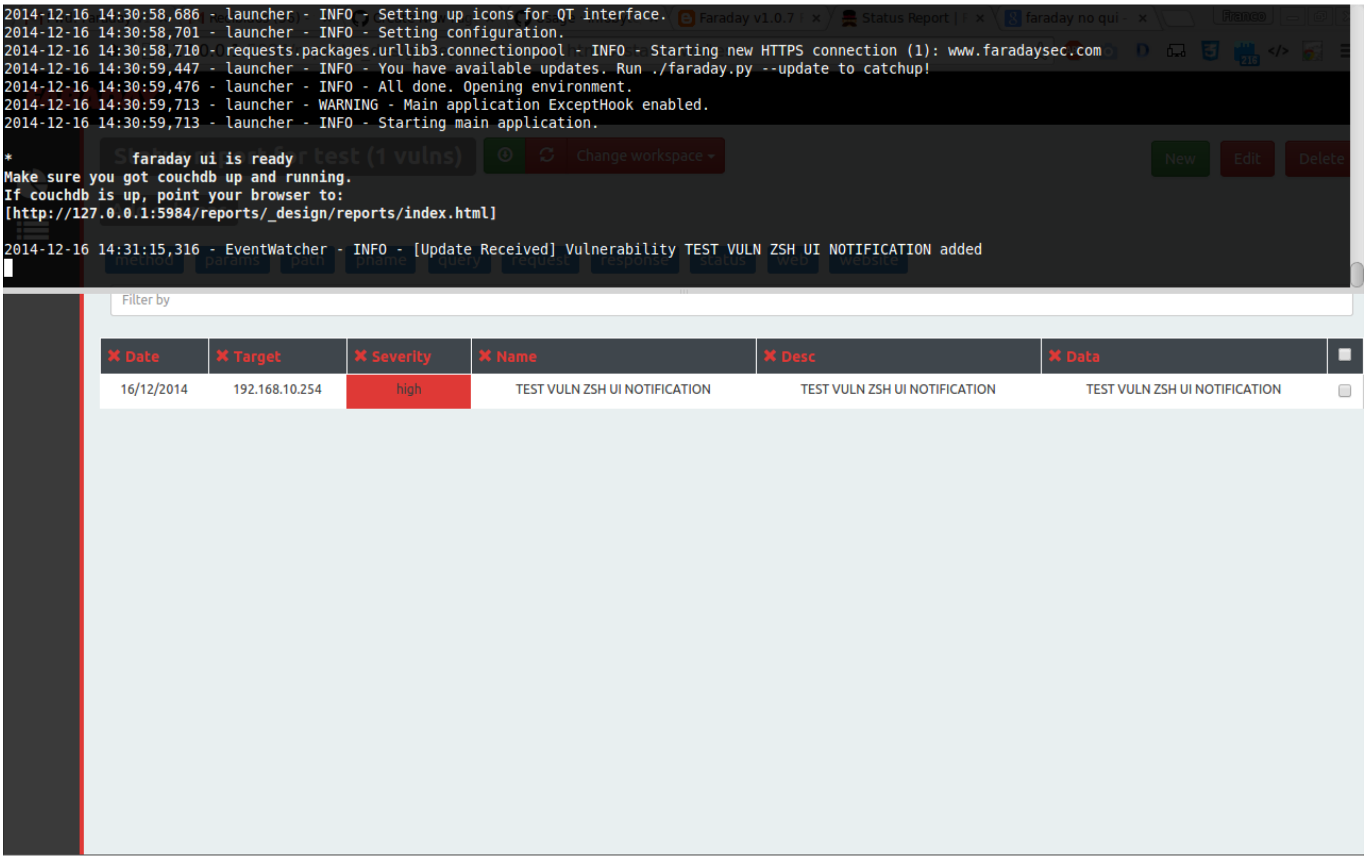
Vulnerability Windows XP UPnP NOTIFY Method LOCATION Header Buffer Overflow updated

Vulnerability Windows XP UPnP NOTIFY LOCATION Denial of Service deleted

Vulnerability X.509 Server Certificate Is Invalid/Expired deleted

Vulnerability Unprotected Tomcat JK jkstatus management and diagnostics page deleted

ZSH UI no-gui notifications



```
2014-12-16 14:30:58,686 - launcher - INFO - Setting up icons for QT interface.
2014-12-16 14:30:58,701 - launcher - INFO - Setting configuration.
2014-12-16 14:30:58,710 - requests.packages.urllib3.connectionpool - INFO - Starting new HTTPS connection (1): www.faradaysec.com
2014-12-16 14:30:59,447 - launcher - INFO - You have available updates. Run ./faraday.py --update to catchup!
2014-12-16 14:30:59,476 - launcher - INFO - All done. Opening environment.
2014-12-16 14:30:59,713 - launcher - WARNING - Main application ExceptHook enabled.
2014-12-16 14:30:59,713 - launcher - INFO - Starting main application.

*    faraday ui is ready
Make sure you got couchdb up and running.
If couchdb is up, point your browser to:
[http://127.0.0.1:5984/reports/_design/reports/index.html]

2014-12-16 14:31:15,316 - EventWatcher - INFO - [Update Received] Vulnerability TEST VULN ZSH UI NOTIFICATION added
```

✖ Date	✖ Target	✖ Severity	✖ Name	✖ Desc	✖ Data	□
16/12/2014	192.168.10.254	high	TEST VULN ZSH UI NOTIFICATION	TEST VULN ZSH UI NOTIFICATION	TEST VULN ZSH UI NOTIFICATION	□

CSV Exporting

More information

Links

- Homepage: https://www.faradaysec.com
- User forum: https://forum.faradaysec.com
- User's manual: https://github.com/infobyte/faraday/wiki
- Download: .tar.gz
- Commits RSS feed: https://github.com/infobyte/faraday/commits/master.atom
- Issue tracker: https://github.com/infobyte/faraday/issues
- Frequently Asked Questions (FAQ): https://github.com/infobyte/faraday/wiki/FAQ
- Mailing list subscription: https://groups.google.com/forum/#!forum/faradaysec
- Twitter: @faradaysec
- Demos
- IRC: ircs://irc.freenode.net/faraday-dev WebClient
- Screenshots: https://github.com/infobyte/faraday/wiki/Screenshots
- Send your ideas and suggestions here: https://www.faradaysec.com/ideas

Presentations

- Ekoparty Security Conference - 2017:
  - http://blog.infobytesec.com/2017/10/ekoparty-2017-review_23.html
- Black Hat Arsenal Asia - 2017:
  - https://www.blackhat.com/asia-17/arsenal.html#faraday
- Zero Nights - 2016
  - https://www.slideshare.net/AlexanderLeonov2/enterprise-vulnerability-management-zeronights16
- AV Tokio - 2016:
  - http://en.avtokyo.org/avtokyo2016/event
- Black Hat Arsenal USA - 2016:
  - https://www.blackhat.com/us-16/arsenal.html#faraday
- Black Hat Arsenal Europe - 2016
  - https://www.blackhat.com/eu-16/arsenal.html#faraday
- SecurityWeekly - 2016:
  - http://securityweekly.com/2016/08/02/security-weekly-475-federico-kirschbaum/
- Bsides Latam - 2016:
  - http://www.infobytesec.com/down/Faraday_BsideLatam_2016.pdf

- Black Hat Arsenal Asia - 2016:
  - https://www.blackhat.com/asia-16/arsenal.html#faraday
- Black Hat Arsenal Europe - 2015:
  - https://www.blackhat.com/eu-15/arsenal.html#faraday
- Black Hat Arsenal USA - 2015:
  - https://www.blackhat.com/us-15/arsenal.html#faraday
  - http://blog.infobytesec.com/2015/08/blackhat-2015_24.html
- RSA - 2015:
  - http://www.rsaconference.com/events/us15/expo-sponsors/exhibitor-list/1782/infobyte-llc
  - http://blog.infobytesec.com/2015/05/infobyte-en-la-rsa-2015.html
- Ekoparty Security Conference - 2014:
  - https://www.youtube.com/watch?v=_j0T2S6Ppfo
- Black Hat Arsenal - 2011
  - http://www.infobytesec.com/down/Faraday_BH2011_Arsenal.pdf
- Ekoparty Security Conference - 2010:
  - http://prezi.com/fw46zt6_zgi8/faraday/
  - http://vimeo.com/16516987