Dradis Framework

Information Security Inc.

iSEC
information security inc.

Contents

- About Dradis
- Dradis Architecture
- Features
- Dradis Goals
- Testing Environment
- Required packages
- Installing Dradis
- Using Dradis
- References

About Dradis

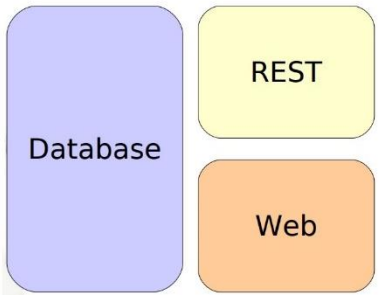
- Dradis is an open-source collaboration framework, tailored to InfoSec teams

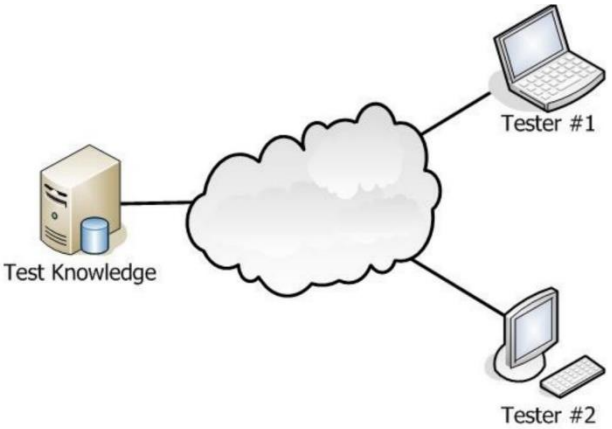
About Dradis

- Two editions of Dradis Framework:

- Dradis Framework Community Edition (CE): open-source and available freely under the GPLv2 license
- Dradis Framework Professional Edition (Pro): includes extra features that are more useful for organizations dealing with bigger teams and multiple projects at a time

Dradis Architecture





Features

- Platform independent
- Markup support for the notes: text styles, code blocks, images, links, etc.

Features

- Integration with existing systems and tools:

Brakeman
Burp Suite
MediaWiki
Metasploit
Nessus
NeXpose
Nikto
Nmap
OpenVAS
….. Full list (https://dradisframework.com/ce/addons/)

Dradis Goals

- Share the information effectively
- Easy to use, easy to be adopted. Otherwise it would present little benefit over other systems
- Flexible: with a powerful and simple extensions interface

Testing Environment

- Kali Linux 2017

```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.2"
VERSION_ID="2017.2"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Required packages

- apt-get install libsqlite3-dev
- apt-get install libmariadbclient-dev-compat
- apt-get install mariadb-client-10.1
- apt-get install mariadb-server-10.1
- apt-get install redis-server

Installing Dradis

- Installing Dradis on Kali Linux
- Installing required packages

```
root@kali2017:~# cat ForSed
libsqlite3-dev  libmariadbclient-dev-compat   mariadb-client-10.1  mariadb-server-10.1   redis-server
root@kali2017:~# apt-get install $(cat ForSed)
Reading package lists... Done
Building dependency tree
Reading state information... Done
libsqlite3-dev is already the newest version (3.20.1-1).
mariadb-client-10.1 is already the newest version (10.1.26-1).
mariadb-client-10.1 set to manually installed.
mariadb-server-10.1 is already the newest version (10.1.26-1).
mariadb-server-10.1 set to manually installed.
redis-server is already the newest version (4:4.0.2-2).
The following additional packages will be installed:
  libmariadbclient-dev
The following NEW packages will be installed:
  libmariadbclient-dev libmariadbclient-dev-compat
0 upgraded, 2 newly installed, 0 to remove and 159 not upgraded.
Need to get 1,103 kB of archives.
After this operation, 6,679 kB of additional disk space will be used.
```

Installing Dradis

- Update “bundler”

```
The latest bundler is 1.16.0.pre.3, but you are currently running 1.15.1.
To update, run `gem install bundler --pre`
root@kali2017:~/dradis-ce#
root@kali2017:~/dradis-ce#
root@kali2017:~/dradis-ce#
root@kali2017:~/dradis-ce#
root@kali2017:~/dradis-ce# gem install bundler --pre
Fetching: bundler-1.16.0.pre.3.gem (100%)
Successfully installed bundler-1.16.0.pre.3
Parsing documentation for bundler-1.16.0.pre.3
Installing ri documentation for bundler-1.16.0.pre.3
Done installing documentation for bundler after 4 seconds
1 gem installed
```

Installing Dradis

- Installing from GitHub

```
root@kali2017:~# git clone https://github.com/dradis/dradis-ce.git
Cloning into 'dradis-ce'...
remote: Counting objects: 7288, done.
remote: Compressing objects: 100% (4/4), done.
remote: Total 7288 (delta 1), reused 4 (delta 1), pack-reused 7283
Receiving objects: 100% (7288/7288), 1.25 MiB | 1.29 MiB/s, done.
Resolving deltas: 100% (4765/4765), done.
```

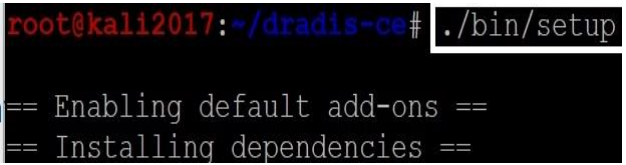
Installing Dradis

- Installing from GitHub

```
root@kali2017:~# cd dradis-ce/
root@kali2017:~/dradis-ce# bundle install --path /root/dradis-ce/
Fetching https://github.com/dradis/dradis-calculator_cvss.git
Fetching https://github.com/dradis/dradis-calculator_dread.git
Fetching https://github.com/dradis/dradis-csv.git
Fetching https://github.com/dradis/dradis-html_export.git
Fetching https://github.com/dradis/dradis-acunetix.git
Fetching https://github.com/dradis/dradis-brakeman.git
Fetching https://github.com/dradis/dradis-burp.git
Fetching https://github.com/dradis/dradis-metasploit.git
Fetching https://github.com/dradis/dradis-nessus.git
Fetching https://github.com/dradis/dradis-nexpose.git
Fetching https://github.com/dradis/dradis-nikto.git
Fetching https://github.com/dradis/dradis-nmap.git
Fetching https://github.com/dradis/dradis-ntospider.git
Fetching https://github.com/dradis/dradis-openvas.git
Fetching https://github.com/dradis/dradis-qualys.git
Fetching https://github.com/dradis/dradis-zap.git
Fetching https://github.com/dradis/dradis-projects.git
Fetching https://github.com/dradis/dradis-plugins.git
Fetching gem metadata from https://rubygems.org/.........
Fetching version metadata from https://rubygems.org/..
Fetching dependency metadata from https://rubygems.org/.
Resolving dependencies...
Fetching rake 12.0.0
```

Installing Dradis

- Installing from GitHub



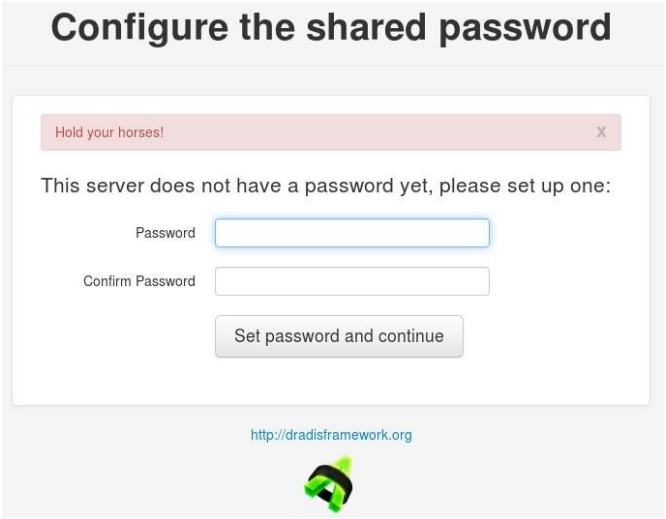
Installing Dradis

- Setting up the app
- Fire up the server by running the following command

```
root@kali2017:~/dradis-ce# bundle exec rails server
=> Booting Thin
=> Rails 5.1.3 application starting in development on http://localhost:3000
=> Run `rails server -h` for more startup options
Thin web server (v1.6.3 codename Protein Powder)
Maximum connections set to 1024
Listening on localhost:3000, CTRL+C to stop
```

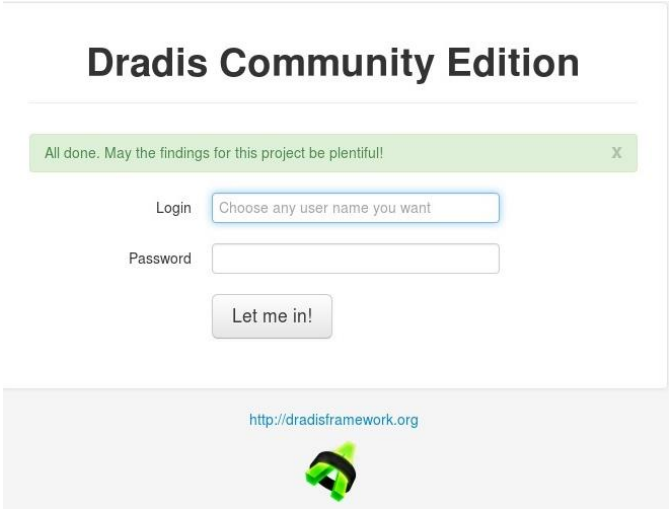
Installing Dradis

- Point your browser to: http://localhost:3000
- Configure the shared password by entering it and confirming it:



Installing Dradis

- Create a username, then enter the password you created above:

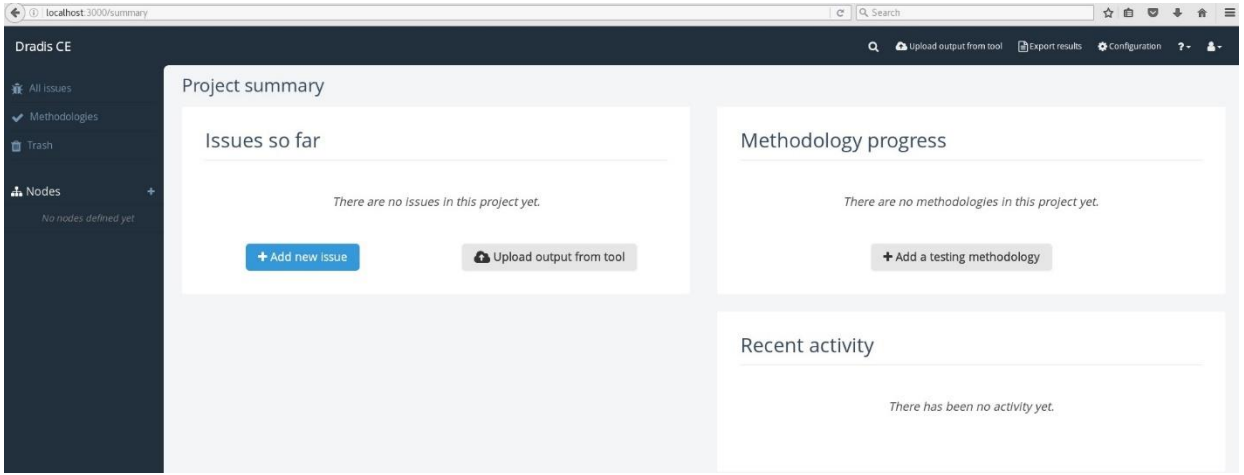


Installing Dradis

- In a new tab in your terminal, start the Background worker that is needed to upload and parse tool output

Using Dradis

- The installation process is completed



Using Dradis

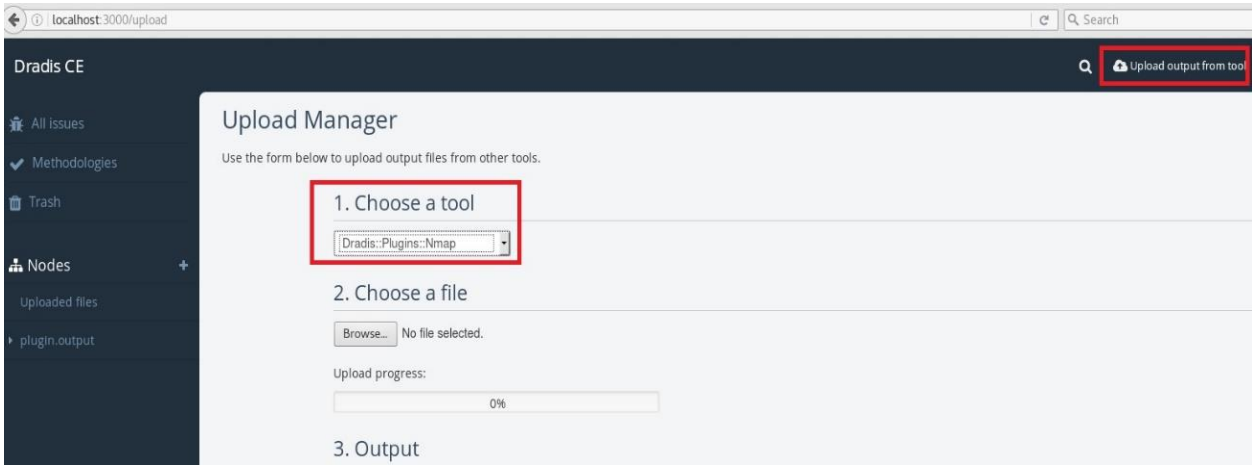
- Importing nmap results
- Nmap scan saving output to Dradis.xml

```
root@kali2017:~# nmap -T3 -A -v -sS -oX Dradis.xml 192.168.10.95

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-16 22:12 EDT
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
Initiating NSE at 22:12
Completed NSE at 22:12, 0.00s elapsed
Initiating ARP Ping Scan at 22:12
Scanning 192.168.10.95 [1 port]
Completed ARP Ping Scan at 22:12, 0.23s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:12
Completed Parallel DNS resolution of 1 host. at 22:12, 0.01s elapsed
Initiating SYN Stealth Scan at 22:12
Scanning 192.168.10.95 [1000 ports]
Discovered open port 3389/tcp on 192.168.10.95
Discovered open port 445/tcp on 192.168.10.95
```

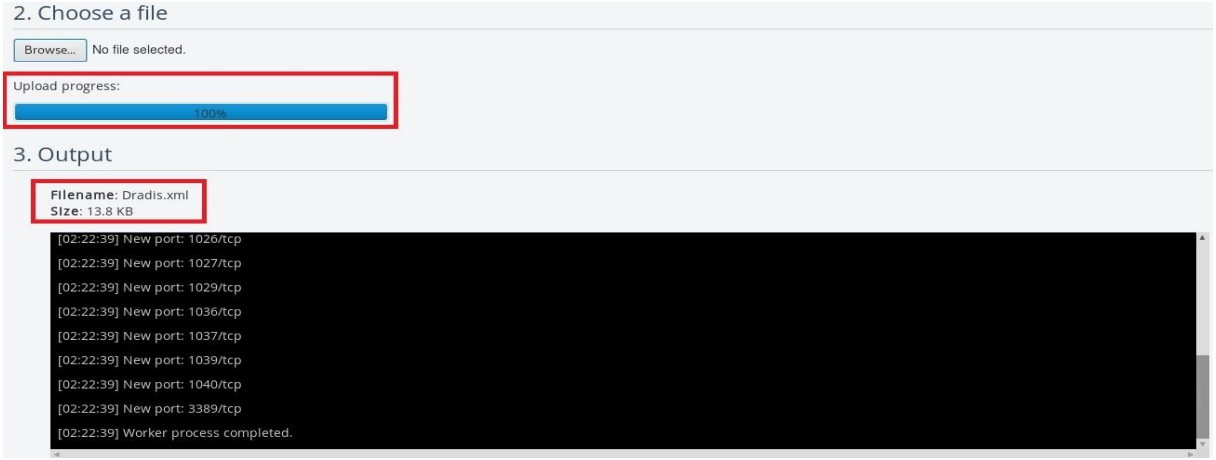
Using Dradis

- Importing Dradis.xml



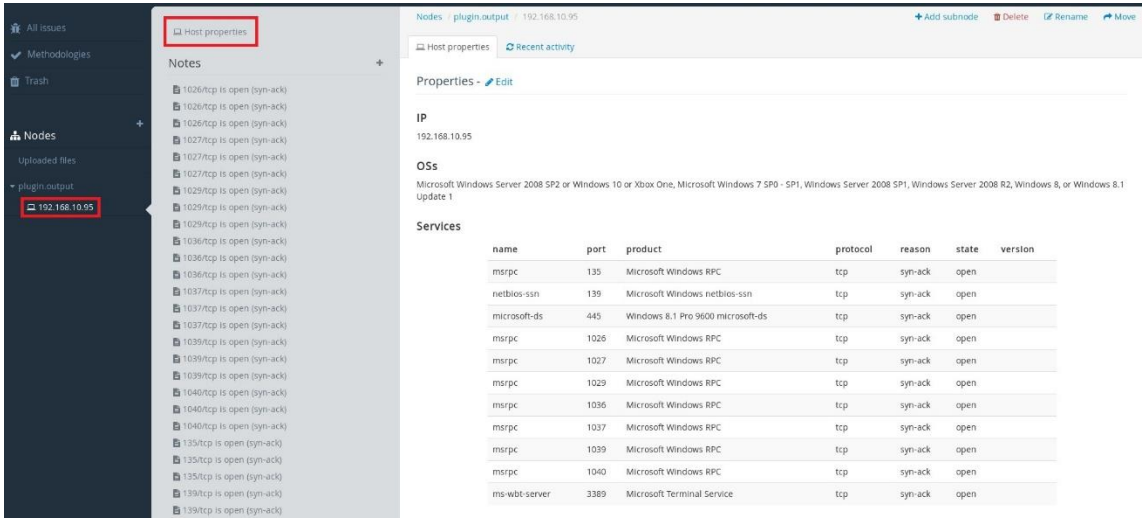
Using Dradis

- Importing Dradis.xml



Using Dradis

- Host properties



References

- Kitploit
http://www.kitploit.com/2017/10/dradis-framework-collaboration-and.html

- Kali Linux
https://www.kali.org/downloads/

- Dradis CE (Community Edition)
https://dradisframework.com/ce/

- Installing Dradis on Kali Linux
https://dradisframework.com/ce/documentation/install_kali.html

- Installing Dradis from GitHub
https://dradisframework.com/ce/documentation/install_git.html