Dradis Framework
Importing informations will you get root

Theofanis Kasimis
CEO Audax Cybersecurity
CCNA, CCNA Security, CEH, OSCP
Email: fkasimis@audax.gr
Twitter: @_fkasimis_

The Dradis Project

Το Dradis Project είναι μια πλατφόρμα open source και χρησιμοποιείται από ερευνητές ασφάλειας & τμήματα IT για την υποβολή εκθέσεων & αναφορών & παρέχει μια κεντρική αποθήκη πληροφοριών για να παρακολουθούμε τι έχει γίνει μέχρι στιγμής αλλά και μεταγενέστερα.

/dradis/social

- Dradisframework.org
- info@dradisframework.org
- IRC
- Forum
- Dradis Academy
- Github
- Twitter: @dradisfw

Τεχνογνωσία

- Ruby
- Linux (Kali 2.0), Mac, Windows
- Συλλογή & αποθήκευση πληροφοριών
- Εύκολο στη χρήση & την προσαρμογή
- Παραμετροποιήσιμο
- Μικρό & φορητό
- Προγραμματισμένες εργασίες

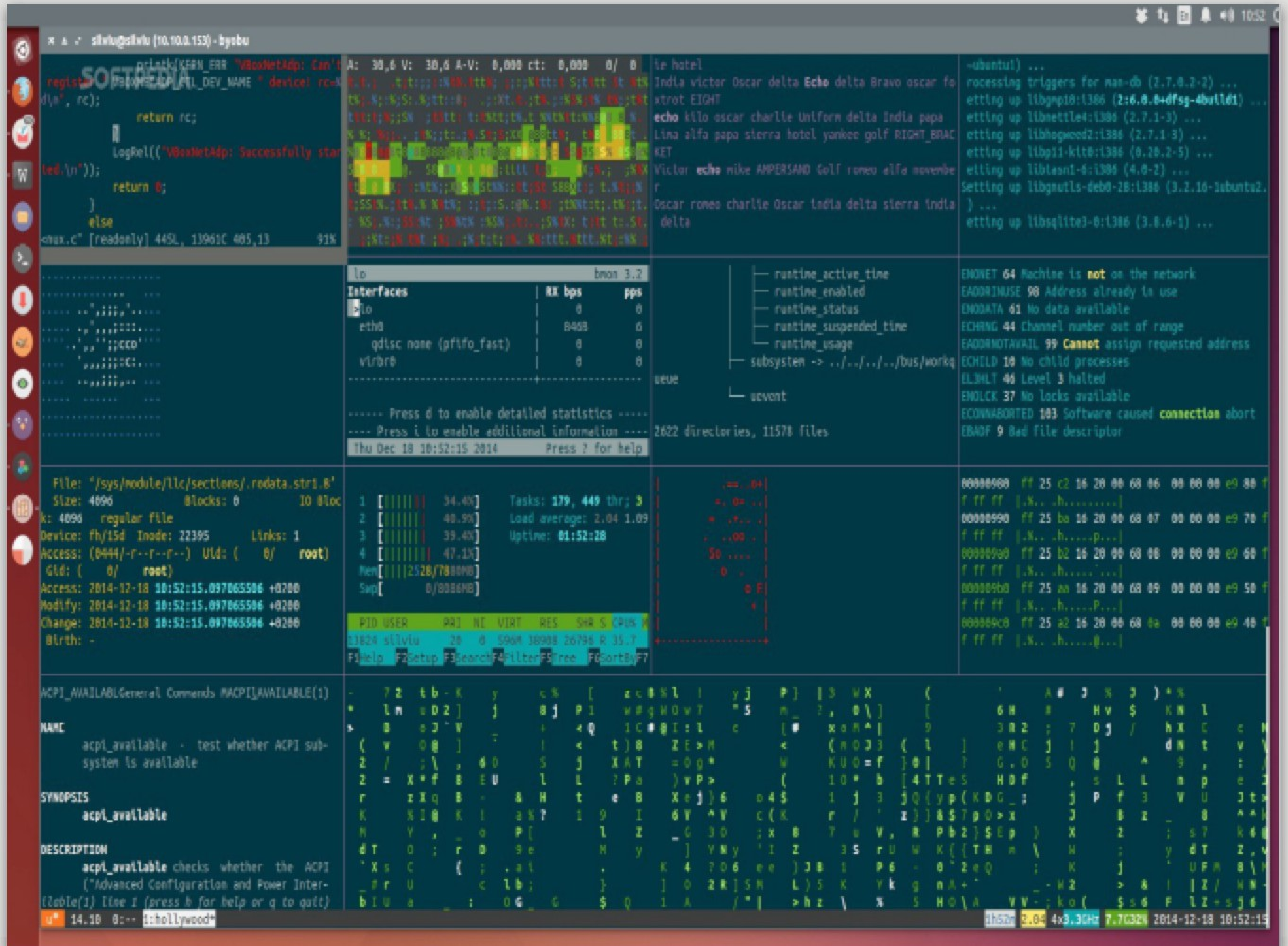
/dradis/tools..

- Import XML Files
- Plugins Vulnerability Scanners
- Export Report Files from reporting tools of Dradis


PORTSWIGGER
WEB SECURITY
MediaWiki
tenable
network security
nexpose
Nmap
OpenVAS
osvdb
QUALYS
w3af
SecureCheck

Παράδειγμα No1

* Ερευνητές Ασφάλειας / Penetration Testers



silviu@silviu (10.10.0.153) - byobu
return rc;
return 0;
else
Interfaces
RX bps
pps
lo
eth0
qdisc none (pfifo_fast)
virbr0
Press d to enable detailed statistics
Press i to enable additional information
Thu Dec 18 10:52:15 2014
Press ? for help
2622 directories, 11578 files
runtime_active_time
runtime_enabled
runtime_status
runtime_suspended_time
runtime_usage
uevent
ENONET 64 Machine is not on the network
EADDRINUSE 98 Address already in use
ENODATA 61 No data available
ECHRNG 44 Channel number out of range
EADDRNOTAVAIL 99 Cannot assign requested address
ECHILD 10 No child processes
EL3HLT 46 Level 3 halted
ENOLCK 37 No locks available
ECONNABORTED 103 Software caused connection abort
EBADF 9 Bad file descriptor
File: '/sys/module/llc/sections/.rodata.str1.8'
Size: 4096
Blocks: 0
regular file
Device: fh/15d Inode: 22395 Links: 1
Access: (0444/-r--r--r--) Uid: (0/ root)
Gid: (0/ root)
Access: 2014-12-18 10:52:15.097065506 +0200
Modify: 2014-12-18 10:52:15.097065506 +0200
Change: 2014-12-18 10:52:15.097065506 +0200
Birth: -
Tasks: 179, 449 thr; 3
Uptime: 01:52:28
NAME
acpi_available - test whether ACPI subsystem is available
SYNOPSIS
acpi_available
DESCRIPTION
acpi_available checks whether the ACPI ("Advanced Configuration and Power Inter-
14.10
1:hollywood*
2014-12-18 10:52:15

Παράδειγμα No2

* Τμήματα IT


DROIDS FRAMEWORK
EST.
2007
CRAFTED IN LONDON

How do I run it?

```
$ tar -xzf dradis-3.1.0.rc2-linux-x86.tar.gz
$ cd dradis-3.1.0.rc2-linux-x86/
$ ./dradis-webapp  && ./dradis-worker
```

Then point your browser to http://127.0.0.1:3000.

Remember: you'll need to have Redis up and running:

In Linux:

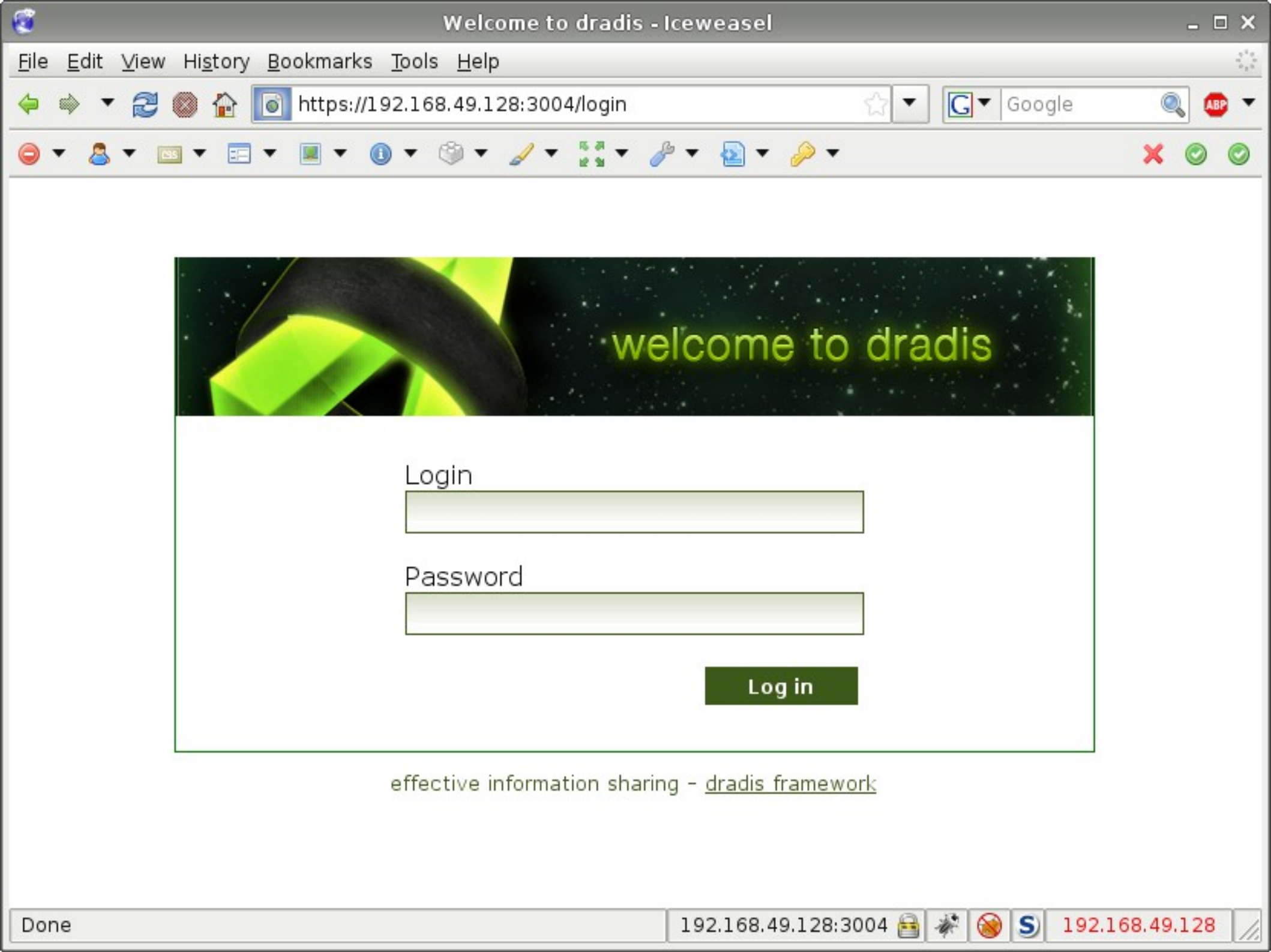
```
$ apt-get install redis-server
```

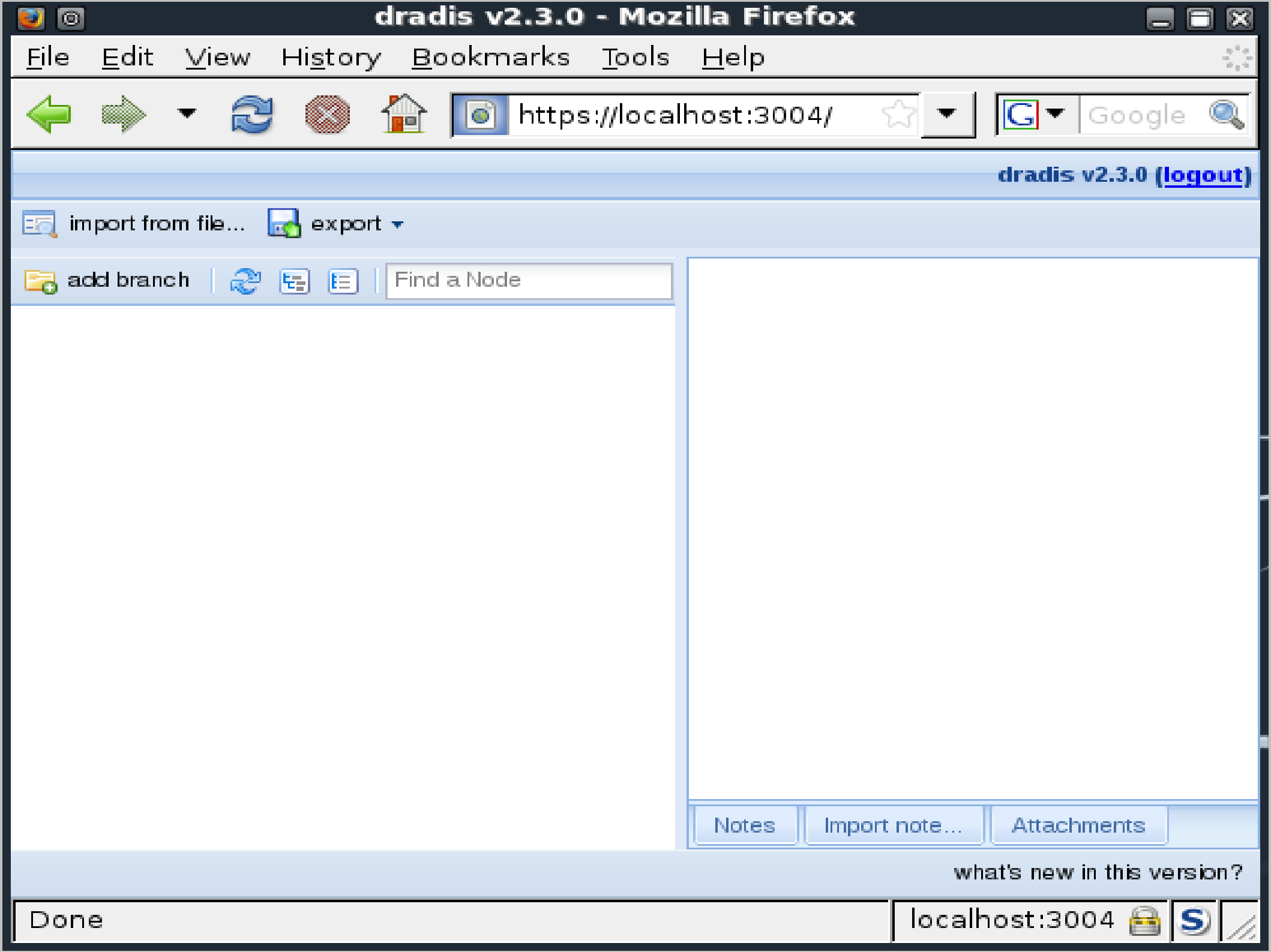
In MacOS:

```
$ brew install redis
$ redis-server /usr/local/etc/redis.conf
```

This isn't working, help!

Calm down, it will all be fine (eventually), please head to the Community Forums and tell us what went wrong.


Welcome to dradis - Iceweasel
File Edit View History Bookmarks Tools Help
https://192.168.49.128:3004/login
Google
welcome to dradis
Login
Password
Log in
effective information sharing - dradis framework
Done
192.168.49.128:3004
192.168.49.128


dradis v2.3.0 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://localhost:3004/
Google
dradis v2.3.0 (logout)
import from file...
export
add branch
Find a Node
Notes
Import note...
Attachments
what's new in this version?
Done
localhost:3004

Upload Manager

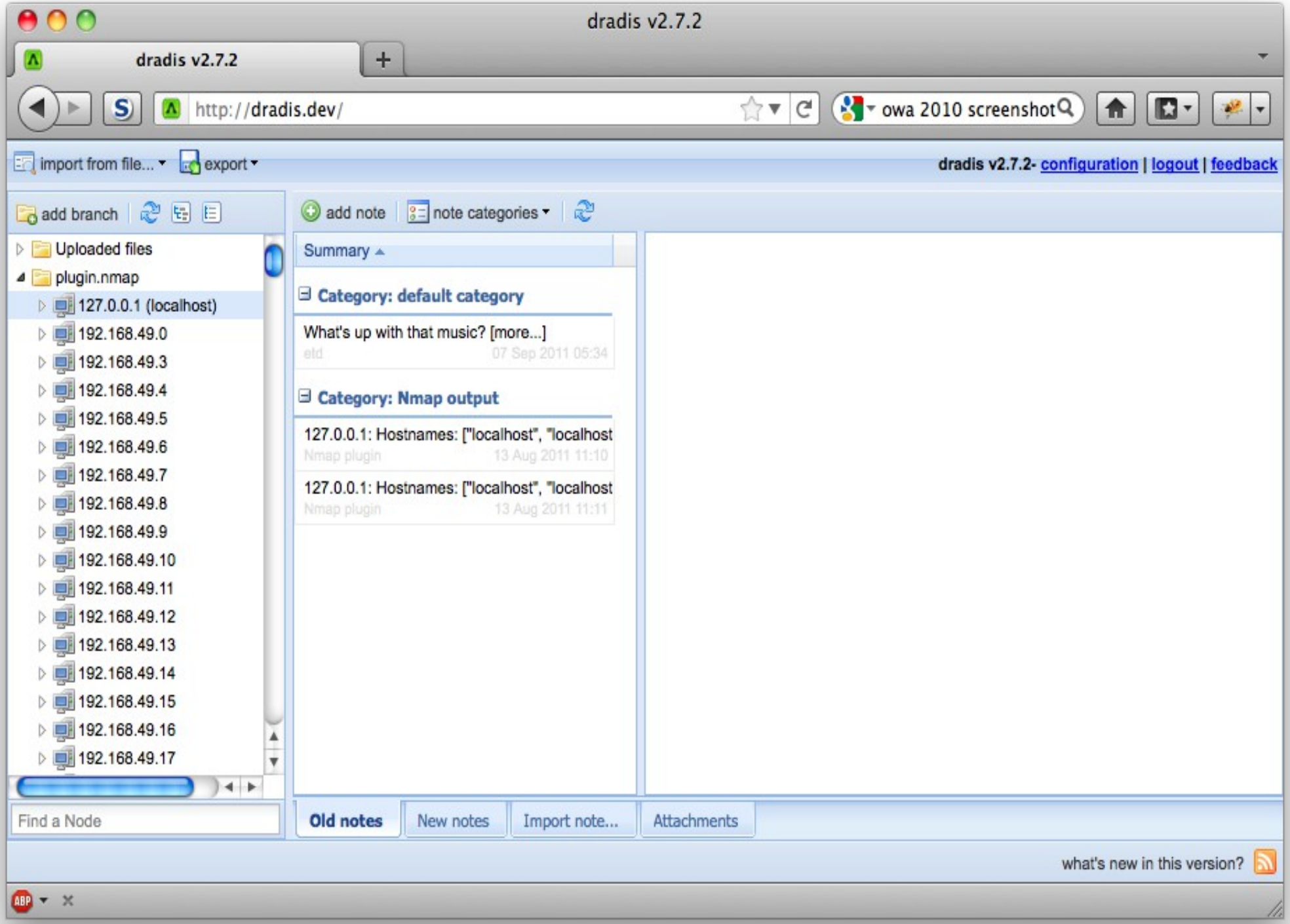
Use the form below to upload output files from other tools. Once you have uploaded them you can process with the different plugins available.

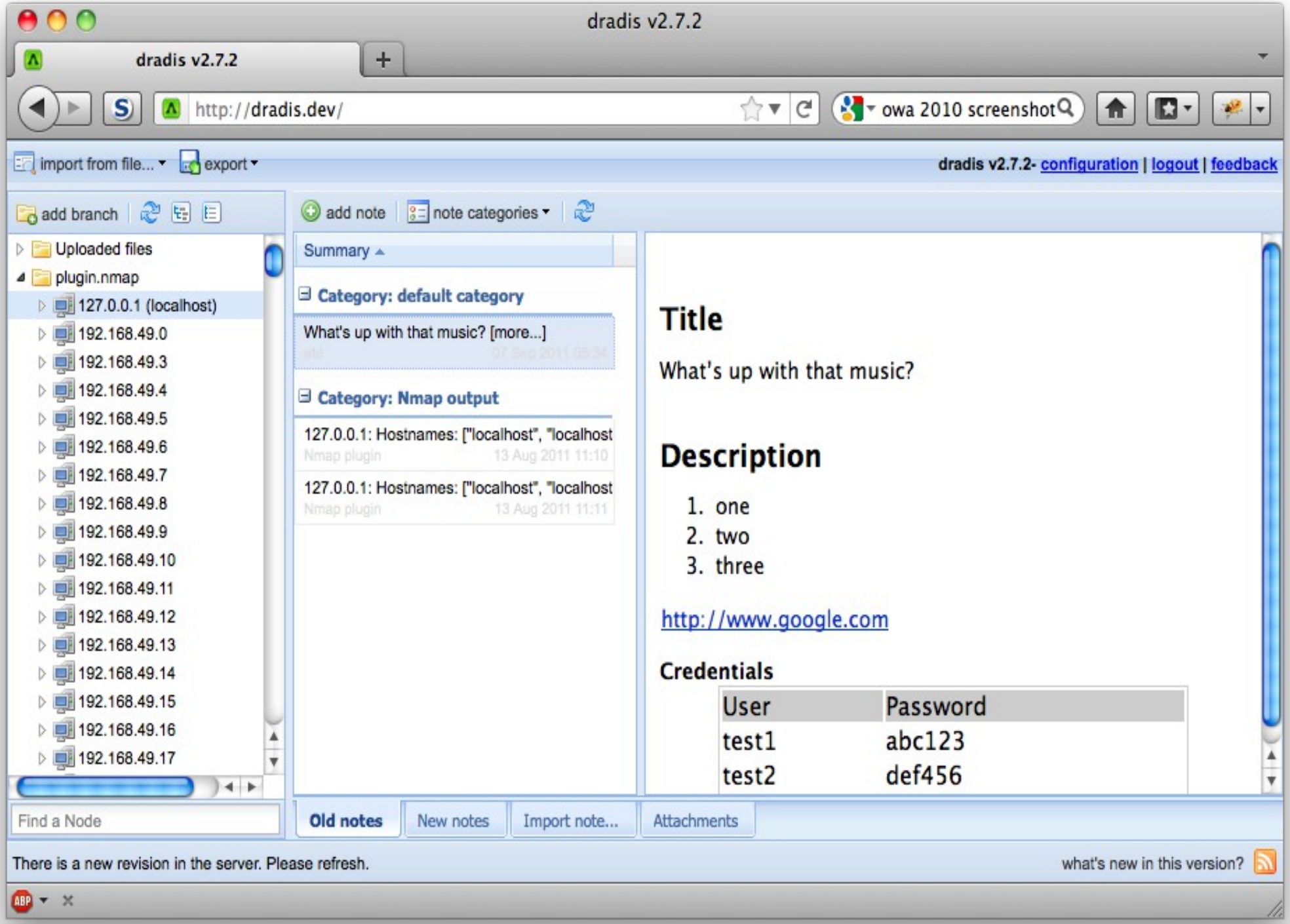
Upload file

NmapUpload | Browse... | metasploitable2.xml

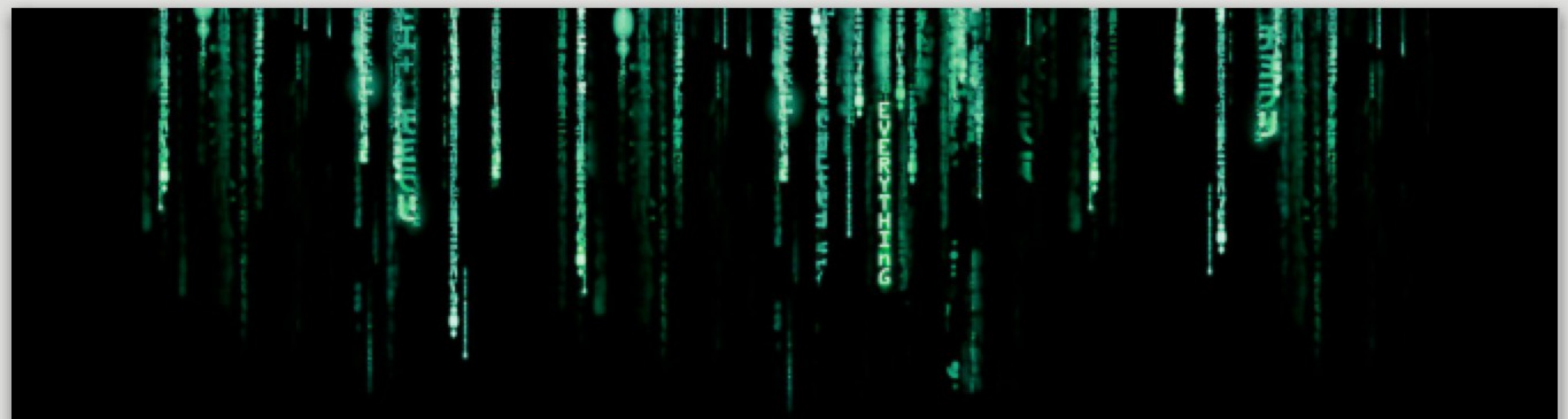
Filename: metasploitable2.xml
Size: 18.5 KB

```
[16:22:55] Small attachment detected. Processing in line.
[16:22:55] Validating Nmap upload...
[16:22:55] Parsing Nmap output...
[16:22:55] Done.
[16:22:56] Worker process completed.
```


dradis v2.7.2
dradis v2.7.2
http://dradis.dev/
owa 2010 screenshot
import from file...
export
dradis v2.7.2- configuration | logout | feedback
add branch
Uploaded files
plugin.nmap
127.0.0.1 (localhost)
192.168.49.0
192.168.49.3
192.168.49.4
192.168.49.5
192.168.49.6
192.168.49.7
192.168.49.8
192.168.49.9
192.168.49.10
192.168.49.11
192.168.49.12
192.168.49.13
192.168.49.14
192.168.49.15
192.168.49.16
192.168.49.17
Find a Node
add note
note categories
Summary
Category: default category
What's up with that music? [more...]
etd
07 Sep 2011 05:34
Category: Nmap output
127.0.0.1: Hostnames: ["localhost", "localhost
Nmap plugin
13 Aug 2011 11:10
127.0.0.1: Hostnames: ["localhost", "localhost
Nmap plugin
13 Aug 2011 11:11
Old notes
New notes
Import note...
Attachments
what's new in this version?


dradis v2.7.2
dradis v2.7.2
http://dradis.dev/
owa 2010 screenshot
import from file...
export
dradis v2.7.2- configuration | logout | feedback
add branch
add note
note categories
Uploaded files
plugin.nmap
127.0.0.1 (localhost)
192.168.49.0
192.168.49.3
192.168.49.4
192.168.49.5
192.168.49.6
192.168.49.7
192.168.49.8
192.168.49.9
192.168.49.10
192.168.49.11
192.168.49.12
192.168.49.13
192.168.49.14
192.168.49.15
192.168.49.16
192.168.49.17
Summary
Category: default category
What's up with that music? [more...]
Category: Nmap output
127.0.0.1: Hostnames: ["localhost", "localhost
Nmap plugin 13 Aug 2011 11:10
127.0.0.1: Hostnames: ["localhost", "localhost
Nmap plugin 13 Aug 2011 11:11
Title
What's up with that music?
Description
1. one
2. two
3. three
http://www.google.com
Credentials
User
Password
test1
abc123
test2
def456
Find a Node
Old notes
New notes
Import note...
Attachments
There is a new revision in the server. Please refresh.
what's new in this version?

Τι πετύχαμε;;;;;



- Συγκέντρωση πληροφοριών ανα τερματικό
- Κατηγοριοποίηση Κενών ασφάλειας ανα τερματικό
- Κατηγοριοποίηση βαθμού επικινδυνότητας (green, orange, red)
- Αποθήκευση αποτελεσμάτων για έλεγχο αργότερα ανα ημέρα/τερματικό
- Προγραμματισμένες εργασίες ανα τερματικό

Βίντεο / Demo

ΤΕΛΟΣ ΠΑΡΟΥΣΙΑΣΗΣ

ΣΑΣ ΕΥΧΑΡΙΣΤΩ ΠΟΛΥ

2ΗΜΕΡΟ ΣΥΝΕΔΡΙΟ

Infocom SECURITY

Upgrade your Knowledge
Protect your Business

ethical hacking