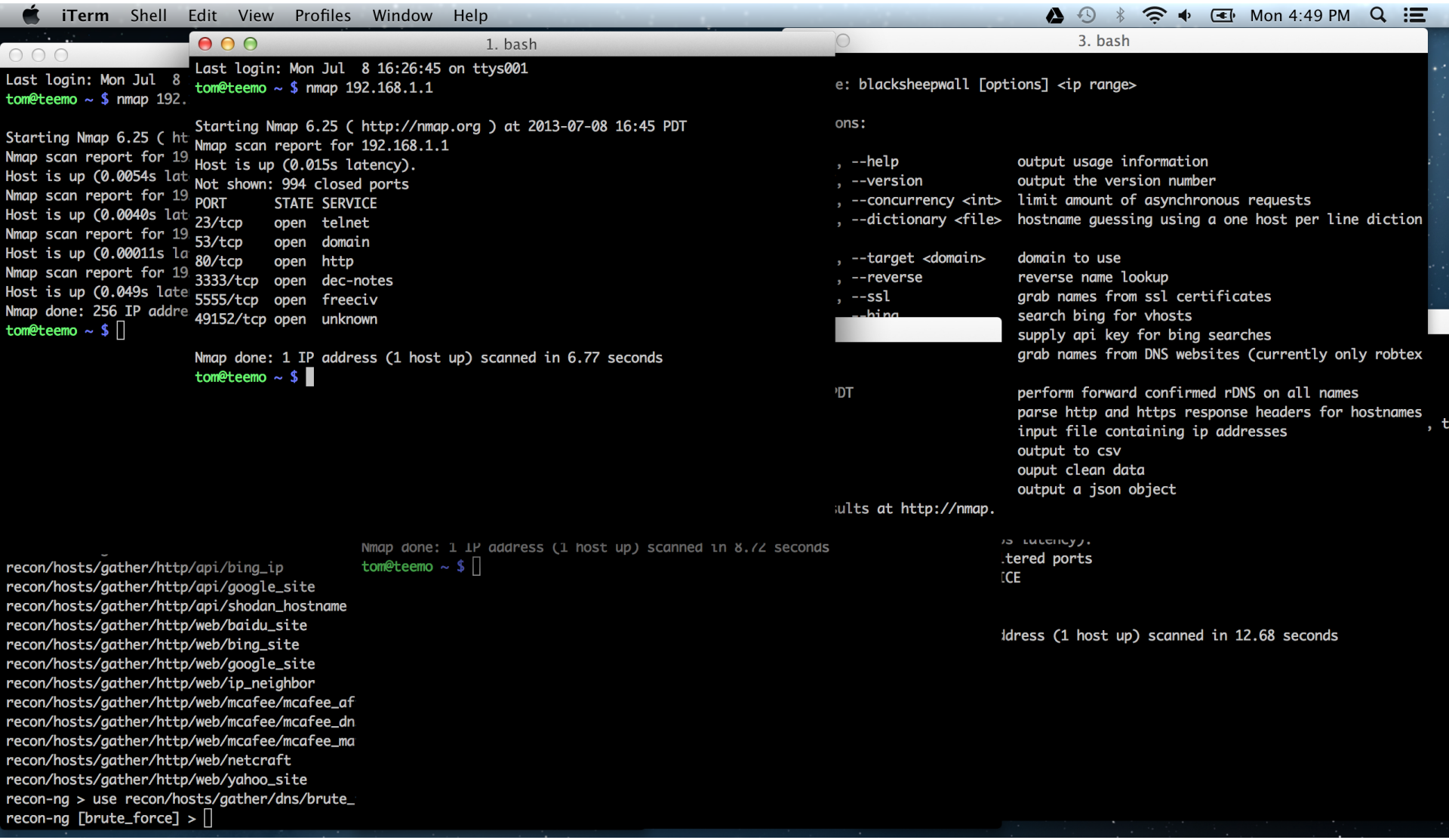
Collaborative Penetration Testing With Lair

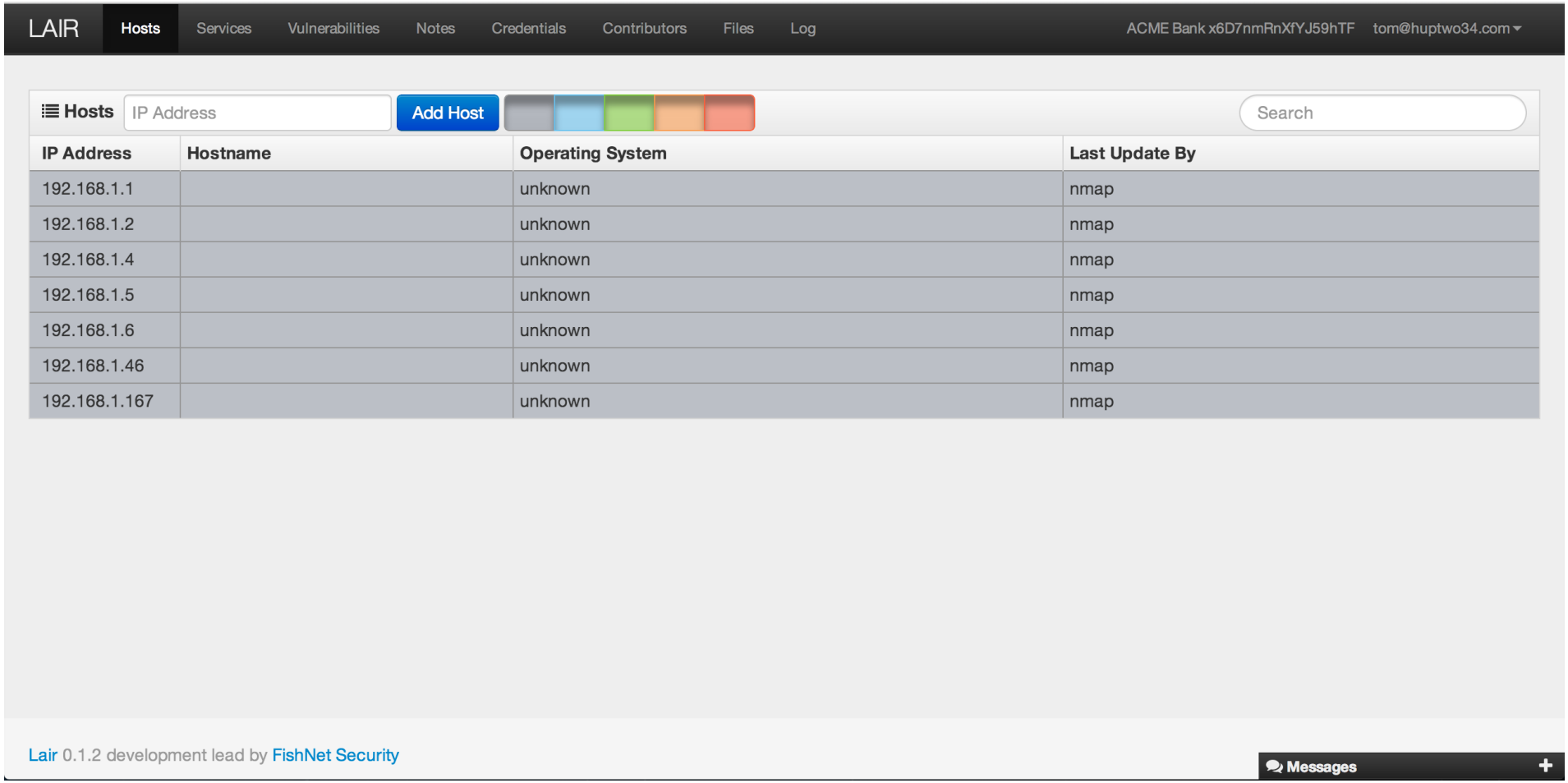
About Us

- Tom Steele
  - Consultant at FishNet Security
  - @_tomsteele
- Dan Kottmann
  - Consultant at FishNet Security
  - Security assessments
  - Hobbyist coder
  - @djkottmann

The Problem


iTerm Shell Edit View Profiles Window Help
Mon 4:49 PM
1. bash
Last login: Mon Jul 8 16:26:45 on ttys001
tom@teemo ~ $ nmap 192.168.1.1
Starting Nmap 6.25 (http://nmap.org) at 2013-07-08 16:45 PDT
Nmap scan report for 192.168.1.1
Host is up (0.015s latency).
Not shown: 994 closed ports
PORT STATE SERVICE
23/tcp open telnet
53/tcp open domain
80/tcp open http
3333/tcp open dec-notes
5555/tcp open freeciv
49152/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 6.77 seconds
tom@teemo ~ $
3. bash
e: blacksheepwall [options] <ip range>
ons:
, --help output usage information
, --version output the version number
, --concurrency <int> limit amount of asynchronous requests
, --dictionary <file> hostname guessing using a one host per line diction
, --target <domain> domain to use
, --reverse reverse name lookup
, --ssl grab names from ssl certificates
search bing for vhosts
supply api key for bing searches
grab names from DNS websites (currently only robtex
perform forward confirmed rDNS on all names
parse http and https response headers for hostnames
input file containing ip addresses
output to csv
ouput clean data
output a json object
recon/hosts/gather/http/api/bing_ip
recon/hosts/gather/http/api/google_site
recon/hosts/gather/http/api/shodan_hostname
recon/hosts/gather/http/web/baidu_site
recon/hosts/gather/http/web/bing_site
recon/hosts/gather/http/web/google_site
recon/hosts/gather/http/web/ip_neighbor
recon/hosts/gather/http/web/mcafee/mcafee_af
recon/hosts/gather/http/web/mcafee/mcafee_dn
recon/hosts/gather/http/web/mcafee/mcafee_ma
recon/hosts/gather/http/web/netcraft
recon/hosts/gather/http/web/yahoo_site
recon-ng > use recon/hosts/gather/dns/brute_
recon-ng [brute_force] >
Nmap done: 1 IP address (1 host up) scanned in 8.72 seconds
tom@teemo ~ $
.tered ports
CE
dress (1 host up) scanned in 12.68 seconds

Lair


LAIR
Hosts
Services
Vulnerabilities
Notes
Credentials
Contributors
Files
Log
ACME Bank x6D7nmRnXfYJ59hTF
tom@huptwo34.com
Hosts
IP Address
Add Host
Search
IP Address
Hostname
Operating System
Last Update By
192.168.1.1
unknown
nmap
192.168.1.2
unknown
nmap
192.168.1.4
unknown
nmap
192.168.1.5
unknown
nmap
192.168.1.6
unknown
nmap
192.168.1.46
unknown
nmap
192.168.1.167
unknown
nmap
Lair 0.1.2 development lead by FishNet Security
Messages

What is Lair

- Web application for managing and tracking the execution of network assessments
- Simplifies effort needed to execute a comprehensive, systematic pentest
- Open-source project sponsored by FishNet Security
- Imports , aggregates, and normalizes output from automated tools

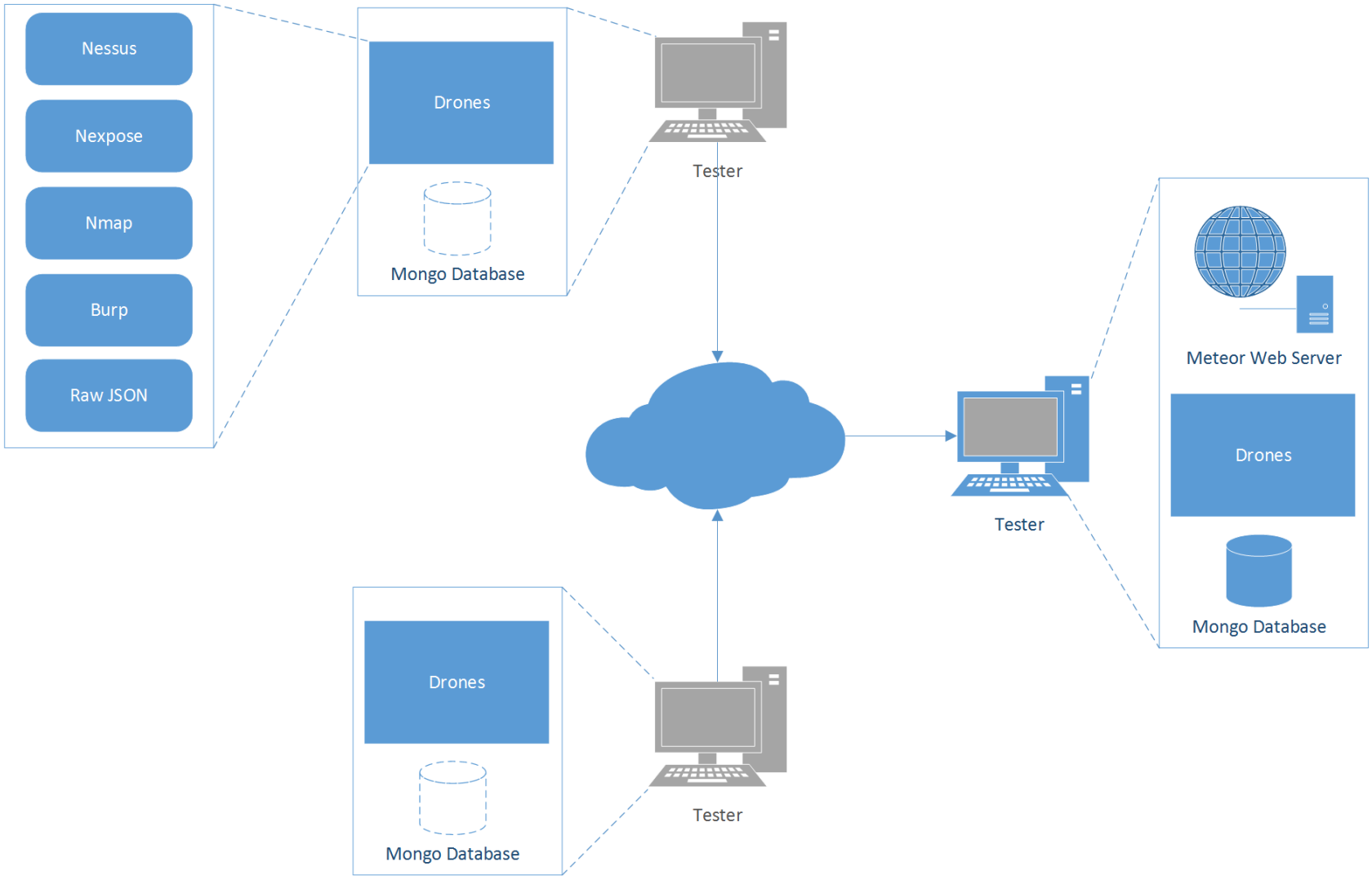
Why is it different?

- Updates pushed to distributed testers in near real-time (really real-time, no really)
  - Reduces duplication of effort
    - Workflow
    - Status tracking
  - Enhances information sharing
    - Credentials/hashes found
    - Manually identified vulnerabilities
    - Successful exploitation
    - False positives
    - Screenshots
  - Team Instant Messaging

Technology

- Web application built on Node.js and Meteor
  - Simplifies real-time synchronization of information across multiple, distributed clients
  - Pub/sub concept
  - No need to fight web sockets
- Python used for Drones
- MongoDb used for database backend

Architecture



Long Demo Now

Download it

https://bitbucket.org/fnsseca/lair