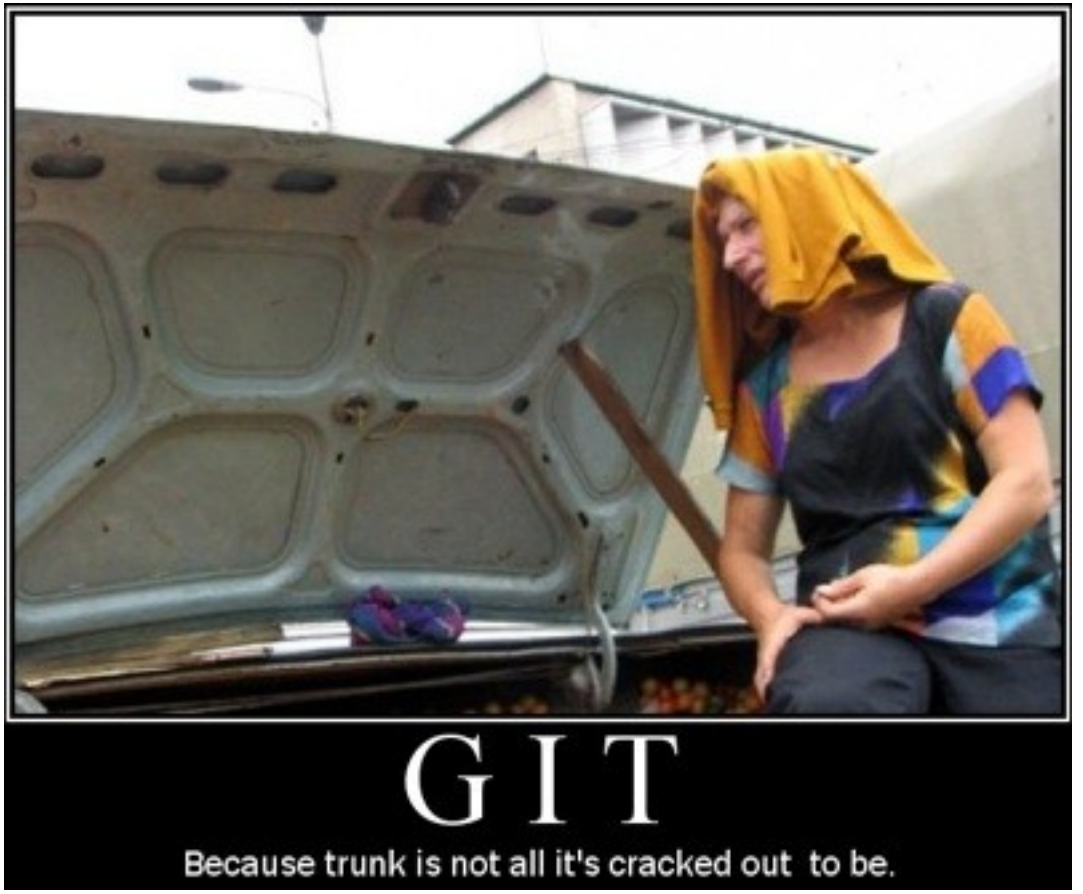
#OpenFest

Ripping web accessible .git files

(or how to get the source when its not open source)



Vlatko Kosturjak, Diverto

https://twitter.com/k0st

Agenda

- Introduction
- Finding repos
- Cloning them
- How to get the source when its not open source
- How to Profit

5 minutes

You found .git?

".git" intitle:"Index of"

About 317 results (0.20 seconds)

Index of /.git - SkullSpace
skullspace.ca/**.git**/
Index of /.**git**. Icon Name Last modified Size Description. [DIR] Parent Directory - [ ] FETCH_HEAD 20-Jun-2012 10:44 105 [ ] HEAD 13-Oct-2011 16:33 23 [ ] ...

Index of /.git - Cuddl Duds
cuddlduds.com/**.git**/
Index of /.**git**. Parent Directory · FETCH_HEAD · HEAD · ORIG_HEAD · branches/ · config · description · hooks/ · index · info/ · logs/ · objects/ · packed-refs · refs/

Index of /.git - Battle Strikers
www.battlestrikers.com/**.git**/
Index of /.**git**. [ICO], Name · Last modified · Size · Description. [DIR], Parent Directory, -. [ ], FETCH_HEAD, 12-Oct-2012 10:42, 105. [ ], HEAD, 31-Aug-2012 10:32 ...

Index of /.git
todaysspecialsapp.com/**.git**/
Index of /.**git**. Parent Directory · HEAD · branches/ · config · description · hooks/ · info/ · objects/ · refs/. Apache/2.2.22 (Unix) mod_ssl/2.2.22 ...

Want source?

- Get the repo:

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

- Get files

```
cd www.target.com
git reset --hard
```

- Profit!

http://www.skullsecurity.org/blog/2012/using-git-clone-to-get-pwn3d

Problem

Directory browsing disabled

No tool available to detect

- Most of the web/network scanners will not find this
  - No awareness
- Tools looks only this
  - .git/ => 403
- They should actually look
  - .git/logs/HEAD => 200
  - .git/config => 200
  - .git/index => 200
  - ...

Nmap NSE comes to rescue

- Have to use latest SVN version
  - Script is not in 6.01
- It looks all relevant git files
  - .git/logs/HEAD
  - .git/config
  - ...
- nmap -sS -PS80,81,443,8080,8081 -p80,81,443,8080,8081 --script=http-git <target>

```
PORT     STATE  SERVICE
80/tcp   open   http
| http-git:
|   Potential Git repository found at XX.XX.XX.XX:XX/.git/ (found 5 of 6
expected files)
```

DVCS-Pillage

- It will rip the .git files when directory browsing disabled
  - By Adam Baldwin
- Accessible from URL:
  - https://github.com/evilpacket/DVCS-Pillage
- Have few problems
  - Hmm...

Problems...

- Current methods
  - Not complete tree download method
    - Packed refs
    - git ls-files –stage method
  - No support for branches
  - No support for other than http
- Time to code my own tool
  - Want whole tree
  - Branches
  - Support old protocols

DVCS-rip

- It will rip the .git files when directory browsing disabled
- It will rip ALL files and checkout repository for you
  - Not partial
  - git fsck trick
- Support for
  - Branches
  - Any protocol (http/https/...)
- Accessible from URL:
  - https://github.com/kost/dvcs-ripper

DVCS-rip

- How to run?
- Example run:
  - rip-git.pl -v -u http://www.example.com/.git/
- It will automatically do "git checkout -f"
- Profit!

Evolving

Adam Baldwin @adam_baldwin 28 Oct

Cool alternative to my DVCS-pillage tool for git called dvcs-ripper github.com/kost/dvcs-ripp… has some new tricks that can get the whole tree!

Expand

Adam Baldwin @adam_baldwin 28 Oct

Updated DVCS-Pillage to support the 'git fsck' trick by @k0st - github.com/evilpacket/DVC…

Expand

Good example of open source collaboration between projects

Questions? Comments? Feedbacks?

@k0st

This is zero

Acknowledgements:
Adam Baldwin,
Ron Bowes,
Alex Weber,
...