

Cooperative Infrastructure for Security and CTF Teams

By Dan Borges



whoami

- Casual CTF Player and Host
- CCDC Red Teamer
- Ex-Mandiant Consultant
- CEO of a startup
- <http://attack.tools>



This is not an intro, this is for ctf teams

 GitHub, Inc. [US] https://github.com/ctfs

CTFs

 CTFs

[Repositories](#) [People 3](#)

[Filters](#) Find a repository...

write-ups-tools
A collection of tools used to maintain and create CTF writeup folders
Updated 14 hours ago

write-ups-2015
Wiki-like CTF write-ups repository, maintained by the community. 2015
Updated 16 hours ago

write-ups-2013
Wiki-like CTF write-ups repository, maintained by the community. 2013
Updated 28 days ago

write-ups-2014
Wiki-like CTF write-ups repository, maintained by the community. 2014
Updated on Sep 27

trailofbits.github.io/ctf/

CTF Field Guide

"Knowing is not enough; we must apply. Willing is not enough; we must do." - Johann Wolfgang von Goethe

Welcome!

We're glad you're here. We need more people like you.

If you're going to make a living in defense, you have to think like the offense.

So, learn to win at Capture The Flag (CTF). These competitions distill major disciplines of professional computer security work into short, objectively measurable exercises. The focus areas that CTF competitions tend to measure are vulnerability discovery, exploit creation, toolkit creation, and operational tradecraft.

Whether you want to succeed at CTF, or as a computer security professional, you'll need to become an expert in at least one of these disciplines. Ideally in all of them.

That's why we wrote this book.

In these chapters, you'll find everything you need to win your next CTF competition.

xx.blogspot.com/2013/08/bootcamp-project-ctf-primer.html

LOCKBOXX

A CONSTANTLY EVOLVING SECURITY BLOG

MONDAY, AUGUST 19, 2013

Bootcamp Project: CTF Primer

So you want to play in a digital Capture The Flag (CTF)?!

The first step is always finding and registering in the CTF you want to play in. After that, this guide is here to help you prepare for your first CTF, aka expect the unexpected.

First, look for local CTFs or register for some Online CTFs.

Think CTFs are over your head? Think again:

If You Can Open The Terminal, You Can Capture T

```
-$ grep "ctf" /etc/group | formatgroup.sh
admin
dth0m
j3mmy
j3p0stl3ch
kenneth
m3rc3p0nt3r
n3t3n3
polym
polyst0r
polyst0r_san
she3ll3
sand1
stango
{and many more! <3 you, #missctf!
-$
```

Breaking the CTFs down we have three styles to look at: Jeopardy, Offensive-Scenario, Offense-Defense.

Offensive-Scenario: Typically involves either attack scenarios or live systems to attack. These types of CTFs will emulate penetration testing over other forms of hacking.

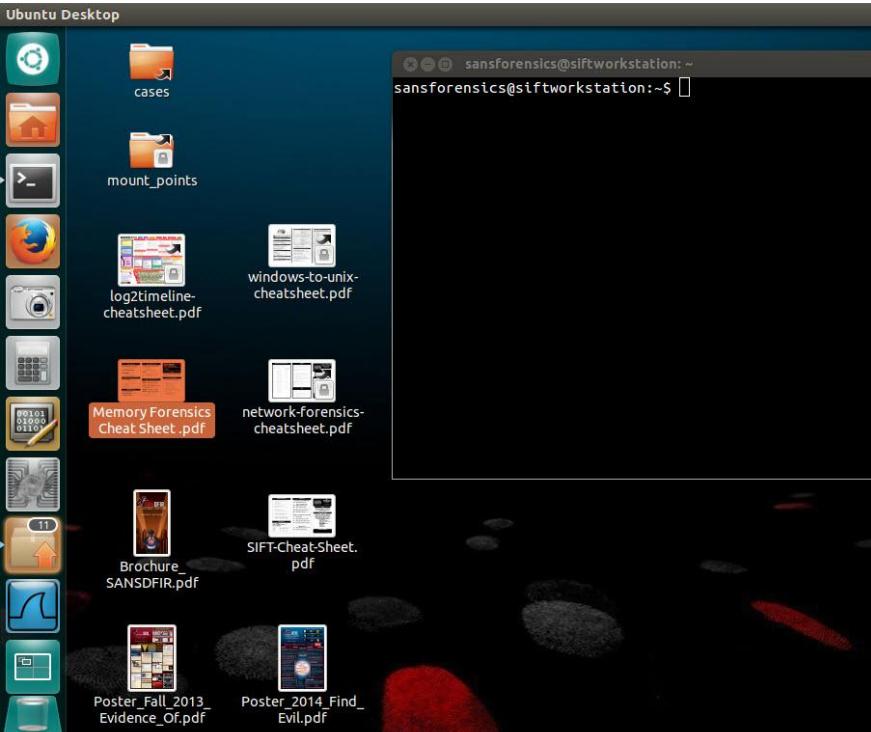


010110
110011
101000
0001

OpSec basics: don't use public / indexed services



Have your tools ready and updated!



KALI LINUX

WHAT IF I TOLD YOU
TO UPDATE SQL MAP

Mobile security, forensics & analysis with Santoku

VIAFORENSICS

© Copyright 2013 viaForensics, LLC. Proprietary Information.

This advertisement for Kali Linux features a large red 3D-style dragon head on a dark textured background. Below it is a large, sharp stainless steel Santoku knife. A black banner across the middle contains the text 'WHAT IF I TOLD YOU TO UPDATE SQL MAP'. Another banner below the knife says 'Mobile security, forensics & analysis with Santoku'. The bottom left corner has the 'VIAFORENSICS' logo. The bottom right corner shows a green-toned portrait of a man wearing sunglasses.

Pure Funky Magic



Input: Hide input No file chosen

Output:

00000000: 41 48 41 48 41 48 41

AHAHAHA

Module descriptions

Note: Slicing is now enabled to trim data before and/or after processing by a specific module. This feature is based on the Python slicing notation preceded by an "a" before ("b") you send data to a PFM module or after ("a") it has been processed. For example, adding "b0:128 a64:-32" as module arguments will cause PFM to only send and return only the 64th through whatever byte is 32 bytes from the end of the processed data for that module. Similarly, "b18: a:256" will suppress the first 18 byte first 256 bytes of processed data. Stepping and other advanced slicing features are not supported however. The script checks for arguments beginning with an "a" or "b" as slicing arguments. To override this for a specific argument (like a zip password that happens to match that pattern) prepend it with "--".

from_b64: Base64 decodes the input.
from_bplist: Converts a binary plist to XML (default) or JSON format.
- optional arg(s): "json" for JSON format.
from_bz2: Inflates bz2 compressed data.
from_deflate: Inflates a deflate compression stream.
from_gzip: Inflates a gzip stream.
from_hex: Converts a hex dump to raw data. Supported formats include xxd, Wireshark, hexdump and plain hex with no spacing.
from_unix_epoch: Converts unix epoch timestamp to human formatted time (GMT).
from_url: URL decodes the input (including encoded spaces).
from_wide: Converts two-byte wide characters (UTF-16 unicode) to one-byte characters.
from_zip: Expands a zip file.

- optional arg(s): Zip archive password
from_zlib: Inflates a zlib stream.

to_b64: Base64 encodes input.
to_bz2: Bz2 compresses data.
to_deflate: Creates a deflate compression stream.
to_gzip: Creates a gzip stream.
to_hex: Provides a hexdump of the input.
- optional arg(s): "stream" will convert to hex stream
to_url: URL encodes input (including spaces).
to_zip: Zip compresses input data.
to_zlib: Creates a zlib stream.

do_byte_spread: Quick byte frequency analysis of input. Also performs a Shannon entropy check - the closer to 1.0 the more random the data (possibly indicating encryption).

do_pkt_payloads: Extracts data payloads from all TCP, UDP & ICMP packets in a pcap. No ordering or defrag.

do_rc4: Applies RC4 crypto key to input.

- required arg(s): A key in hex format (no spaces or Leading 0x) is required.

do_strip_HTTP_header: Strips the HTTP header from a dumped TCP stream.

do_xor: Performs an XOR against the input using a supplied key.

- required arg(s): A single or multi-byte XOR key in plain hex (no spaces, no Leading 0x) is required.

00:54 GMT

from_b64
to_hex

FROM
TO
DO

Args:
or "b" to allow you to slice data
the first 128 bytes of data to a module
of data to the Target: webpage
that contain a Do the thing(s) expects them

What if I sold you



Slack / Github / Google Docs integration for chat-ops



ahhh

CHANNELS (14)

[REDACTED]

DIRECT MESSAGES (21)

ahhh 11:02 AM yupp

ross 11:02 AM sweet

ahhh 11:03 AM [REDACTED]

ross 11:04 AM okay

github BOT 1:14 PM [wisp:master] 1 new commit by Ross Ragsdale:
cd2810b: Create sense-state.py - Ross Ragsdale

[wisp:master] 1 new commit by Ross Ragsdale:
faf2fc7: Create unroot.sh - Ross Ragsdale

ross 3:14 PM Added a Shell snippet: wireless!

github BOT 3:16 PM [wisp:master] 1 new commit by Ross Ragsdale:
f29eabb: Update unroot.sh - Ross Ragsdale

+ [REDACTED]

6 Search

About wisp

Channel Details

Pinned Items

No items have been pinned yet! Click the icon on important messages or files and choose Pin to wisp to stick them here.

1/6 Members



Shared Files

Notification Preferences

Using Quip for file sharing, interactive docs, and chat-ops



Back

http://tasks.asis-cf.ir/tera_85021482a68d6ed21892ea99b
hacker@lubuntu-64:~/Downloads/as
Please wait until my job be done
%0.0002528
http://darksky.slac.stanford.edu/simulator

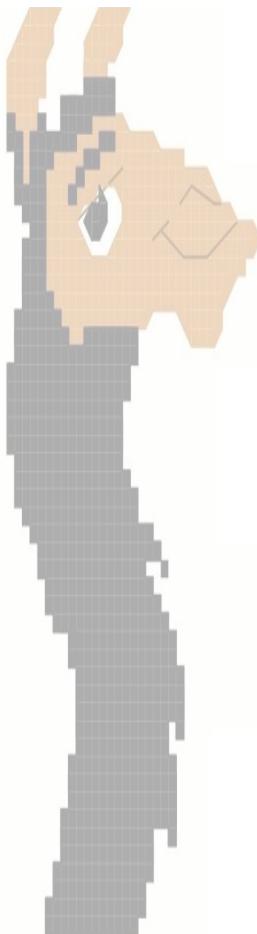
renamed the document to Tera - May 9
May 9 · 13 · 13
HAAAH this thing goes to grab
<http://darksky.slac.stanford.edu/simulator>
...
which is a 31TB file

May 9 · Like
Everyone - w00t w00t!
May 9 · Like
nice
good job

renamed Tera to Tera (SOLVED) - May 9
edited the document · May 9 · Like · Revert

Tera (SOLVED)

✓ Read by [REDACTED]



ASIS{3149ad5d3629581b17279cc889222b93}

```
import requests
import struct

url = "http://darksky.slac.stanford.edu/simulations/ds14_a/ds14_a_1.0000"

def chunks(l, n):
    for i in xrange(0, len(l), n):
        yield l[i:i+n]

def xor(data, key):
    return bytearray(a^b for a, b in zip(*map(bytearray, [data, key])))

with open('tera.elf', 'rb') as f:
    data = f.read()

# Extracted with IDA :
memory_locations = data[0x1480:0x1480+0x130]
# Extracted with IDA :
xor_key = data[0x1680:0x1680+0x98]

# Get all memory locations
mem_chunks = [struct.unpack("<Q", x)[0] for x in chunks(memory_locations, 8)]

xor_chunks = "".join([chr(struct.unpack("<L", x)[0]) for x in chunks(xor_key, 4)])

encrypted_string = ""

for chunk in mem_chunks:
    print "Fetched byte at %08x..." % chunk
    res = requests.get(url, headers={"range": "bytes=%d-%d" % (chunk, chunk)})

    encrypted_string += res.content

print xor(encrypted_string, xor_chunks)
```

Etherpad for a private interactive doc application



B I U S

≡ ≡ ▷ ▷

↶ ↷



⚙ ⭐

↔ </>

🕒



In lot of char fields, there is a useless size. List here char where we could remove the size (business logic)

- Remove size everywhere , do not update it.
 - Keep only size in bar code (ean13) field in product form
 - QDP: are you sure?

Specification:

- Remove size attribute from all modules, keeps with special cases
 - Special cases like, (ean13, journal code*,....)
 - **Note:** Special cases are managed during the development of task.
- Report: Manage function 'ellipsis(size, value)' that crop a <value> to display only <size 3>
 - return value + '...'
 - `_ellipsis(char, size=100, truncation_str='...')` , Feature already there within report so no need to create new function.
 - check all reports to see if, with normal values, it's still ok otherwise use the `_ellipsis()` method
 - *: journal code has been arbitrary set to stay 3 letters long because otherwise it's a mess in reports (e.g: general ledger..), in move names... and it's usually enough.
 - Here use function:ellipsis(size, value)'.

Branch:

- Addons:

OSINT cooperation with Maltego or Spiderfoot



MALTEGO

Share Graph

SpiderFoot New Scan Scans Settings

Complete the details below to share a graph or connect to a graph

Session Server Encryption

Paterva (Public) Use the public Paterva Communication Server.

Paterva (Private) Use your own private Paterva Communication Server.

Server Name or IP

Other Use a different XMPP (Jabber) server by completing the fields below.

Server DNS Name

Port Auto detect Attempt to detect the default port.
 Default Uses TLS encr.
 Old style SSL
 HTTP Bind
 HTTPS Bind

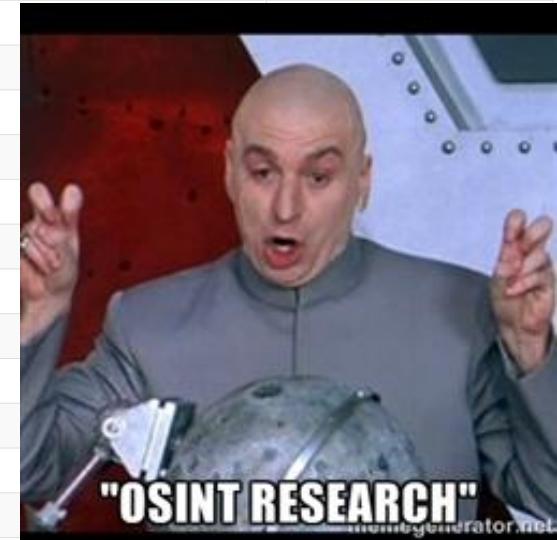
Username

Password Save password

Status Browse * Graph Scan Settings Log

Search...

Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Internet Name	3	5	2015-11-08 03:00:18
Affiliate - Web Content	3	5	2015-11-08 03:00:50
Affiliate Description - Abstract	2	2	2015-11-08 03:00:19
Affiliate Description - Category	34	41	
HTTP Headers	1	1	
HTTP Status Code	1	1	
Human Name	1	1	
Internet Name	1	1	
Junk File	9	9	
Linked URL - External	14	14	
Linked URL - Internal	53	54	
Malicious Affiliate	3	3	
Non-Standard HTTP Header	1	1	
Raw File Meta Data	1	1	
SSL Certificate - Issued by	1	1	



"OSINT RESEARCH" generator.net

Metasploit master server and connecting clients



```
Player Applications Places Terminal Sat 03:11 1
File Edit View Search Terminal Help
Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit
[= metasploit v4.11.4-2015092301 ]
+ --=[ 1485 exploits - 857 auxiliary - 250 post
+ --=[ 432 payloads - 37 encoders - 8 nops
+ --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > db_connect msf: [REDACTED].220/msf
[*] Rebuilding the module cache in the background...
msf > db_status
[*] postgresql connected to msf
msf > hosts

Hosts
=====
address mac name os_name os_flavor os_sp purpose info comm
----- --- --- -----
[REDACTED] .43 [REDACTED] firewall
[REDACTED] .97 WIN-[REDACTED] Windows 2012 client

msf >
```

```
Command Prompt - ssh -i seasoned_security.pem ubuntu@[REDACTED]
[*] Time: 2015-08-02 06:26:52 UTC Note: host=[REDACTED].43 type:host.nat.server data={:info=>"This device is a
[*] Time: 2015-08-02 06:26:52 UTC Note: host=[REDACTED].97 type:host.nat.client data={:info=>"This device is tr
msf > chosts
[-] Unknown command: chosts.
msf > notes
[*] Time: 2015-08-02 06:26:51 UTC Note: host=[REDACTED].43 type:host.os.session_fingerprint data={:name=>"WIN-
[*] Time: 2015-08-02 06:26:52 UTC Note: host=[REDACTED].97 type:host.nat.server data={:info=>"This device is ac
[*] Time: 2015-08-02 06:26:52 UTC Note: host=[REDACTED].97 type:host.nat.client data={:info=>"This device is tr
msf > hosts

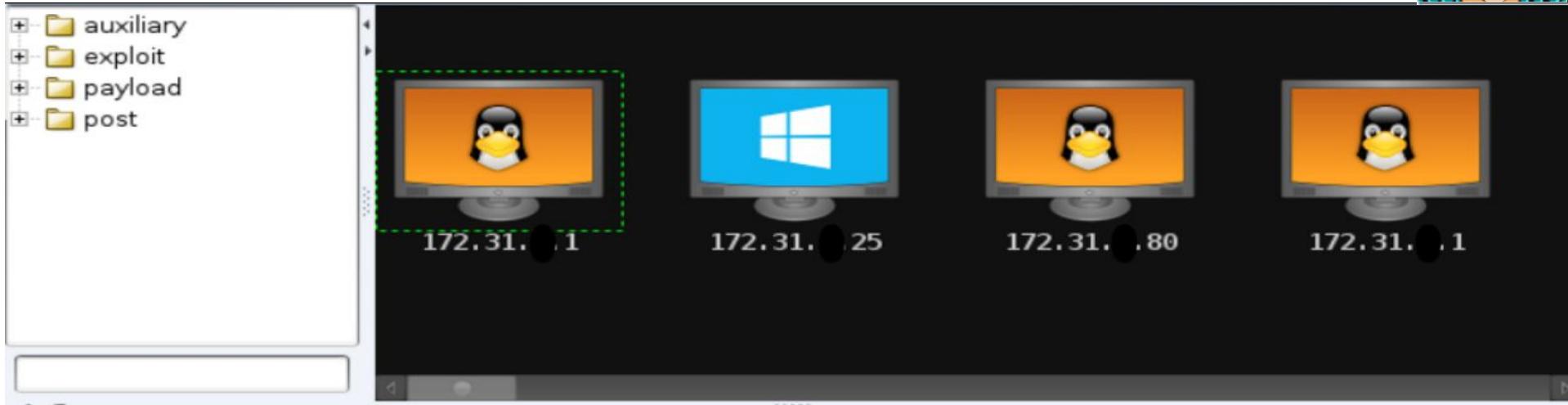
Hosts
=====
address mac name os_name os_flavor os_sp purpose info comm
----- --- --- -----
[REDACTED] .43 [REDACTED] firewall
[REDACTED] .97 WIN-[REDACTED] Windows 2012 client

msf > curl icanhazip.com
[*] exec: curl icanhazip.com

% Total % Received % Xferd Average Speed Time Time Current
          Dload Upload Total Spent Left Speed
100 15 100 15 0 0 175 0 --:--:-- --:--:-- 176
[REDACTED] .220

msf > db_status
[*] postgresql connected to msf
msf >
```

Cobalt Strike / Armitage Team-servers



The image shows the Armitage interface, a graphical user interface for the Cobalt Strike red team platform. On the left, a sidebar lists categories: auxiliary, exploit, payload, and post. The main pane displays four team-servers represented by computer monitors. The first monitor (IP 172.31.1.1) has a Linux Tux icon and is highlighted with a dashed green border. The other three monitors (IPs 172.31.1.25, 172.31.1.80, and 172.31.1.1) show Windows icons. Below the monitors is a horizontal bar with various icons.

Event Log X		Console X			nmap X		
Scan X	Scan X	Scan X	Services X	Services X	Services X	Services X	
host	name	port	proto	info			
172.31.1.1	ssh	22	tcp	SSH-2.0-OpenSSH_5.5p1 Debian-6+squeeze5			
172.31.1.1	telnet	23	tcp	Welcome to VyOS x0a x0dvyos login:			
172.31.1.1	mysql	3306	tcp	5.5.41-Ubuntu0.12.04.1			
172.31.1.1	ms-wbt-server	3389	tcp	Microsoft Terminal Service			

Everyone loves cracking hashes - have them on demand



```
sudo echo "/usr/local/cuda/lib" | sudo tee -a  
/etc/ld.so.conf.d/cuda.conf  
sudo ldconfig  
cd /usr/local/cuda/samples/1.Utilities/deviceQuery  
sudo make  
sudo ./deviceQuery  
cd ~  
wget http://us.download.nvidia.com/XFree86/Linux-x86_64/340.32/NVIDIA-Linux-x86_64-340.32.run  
chmod +x NVIDIA-Linux-x86_64-340.32.run  
sudo ./NVIDIA-Linux-x86_64-340.32.run  
wget http://hashcat.net/files/cudaHashcat-1.21.7z  
7za x cudaHashcat-1.21.7z
```

Finally you should be able to bench mark it using:
./cudaHashcat64.bin -b

You will probably want some wordlists for your cracking, I've assembled a collection of wordlist collections [here](#), with a little bit on creating customized wordlists.

And best of all, it works :) Here's cracking some MD5(Unix) passwords, and here's to cracking more!

```
./cudaHashcat64.bin -m 500 -a 0 ~/hashes/md5.unix.txt  
~/wordlists/rockyou.txt
```

```
Session.Name....: cudaHashcat  
Status.....: Exhausted  
Input.Mode.....: File (/home/ubuntu/wordlists/rockyou.txt)  
Hash.Target....: File (/home/ubuntu/hashes/md5.unix.txt)  
Hash.Type.....: md5crypt, MD5(Unix), FreeBSD MD5, Cisco-IOS MD5  
Time.Started...: Sat Aug 16 01:59:39 2014 (3 mins, 26 secs)  
Time.Estimated.: 0 secs  
Speed.GPU.#1...: 75697 H/s  
Recovered.....: 4/9 (44.44%) Digests, 4/9 (44.44%) Salts  
Progress.....: 129089664/129089664 (100.00%)  
Skipped.....: 55538172/129089664 (43.02%)  
Rejected.....: 9/129089664 (0.00%)  
HwMon.GPU.#1...: 0% Util, 64c Temp, -1% Fan
```

Command Prompt - ssh -i seasoned_security.pem ubuntu@[REDACTED]

```
Speed.GPU.#1..: 683.6 MH/s  
Hashtype: SHA256  
Workload: 1024 loops, 256 accel  
Speed.GPU.#1..: 290.5 MH/s  
Hashtype: SHA384  
Workload: 256 loops, 256 accel  
Speed.GPU.#1..: 71960.0 kH/s  
Hashtype: SHA512  
Workload: 256 loops, 256 accel  
Speed.GPU.#1..: 71907.4 kH/s  
Hashtype: SHA-3(Keccak)  
Workload: 128 loops, 256 accel  
Speed.GPU.#1..: 58364.7 kH/s  
Hashtype: SipHash  
Workload: 1024 loops, 256 accel  
Speed.GPU.#1..: 3105.0 MH/s  
Hashtype: RipeMD160  
Workload: 1024 loops, 256 accel  
Speed.GPU.#1..: 481.6 MH/s  
Hashtype: Whirlpool  
Workload: 512 loops, 32 accel  
Speed.GPU.#1..: 43914.4 kH/s
```



© DISNEY

Fixed Disks
Fixed Disk 0
Disk IO
C: (VH
r=0, w=

Cooperative disassembly with a radare2 webserver



10.0.0.139:8008 39 :

10.0.0.139:8008

" -- Change your fortune types with 'e cfg.fortunetype = fun,tips,nsfw' in your ~/.radare2rc "

Current Project

CurrentProject: CurrentFile: asm_arm_gnu.dll OtherProjects: Layout: panels (desktop) ▾

Delete Save As Save Open

Files

Open File ...

Choose File No file chosen Upload

?

Disassembler Hex Dump Strings Entropy Types Settings Projects

Information

type DLL (Dynamic Link file asm_arm_gnu.dll fd 3 size 0x9e31f blksz 0x0 mode r-- block 0x100 format pe pic false canary false nx false crypto false va true bintype pe class PE32 arch x86 bits 32 machine i386 os windows subsys Windows CUI endian little stripped true static false linenum true lsyms false relocs false binsz 647967 compiled Wed Apr 29 09:49:3 guid 723684D4ABB6FBBA

EVERYBODY'S OUT PARTYING

AND I'M SITTING HERE REVERSE ENGINEERING

memegenerator.net

CloudShark.com for pcap collaboration in browser



mDNSResponder - 11-5-15 at 7.32 PM.pcapng 42.7 kb · 241 packets · more info

 Analysis Tools ▾  Graphs ▾  Download  Profile

Type: A (Host Address) (1)
Class: IN (0x0001)

▼ Answers

- ```
us-courier.push-apple.com.akadns.net: type A, class IN, addr 17.110.227.83
us-courier.push-apple.com.akadns.net: type A, class IN, addr 17.110.229.80
us-courier.push-apple.com.akadns.net: type A, class IN, addr 17.110.224.215
us-courier.push-apple.com.akadns.net: type A, class IN, addr 17.110.229.140
us-courier.push-apple.com.akadns.net: type A, class IN, addr 17.110.228.17
us-courier.push-apple.com.akadns.net: type A, class IN, addr 17.110.224.20
us-courier.push-apple.com.akadns.net: type A, class IN, addr 17.110.229.91
us-courier.push-apple.com.akadns.net: type A, class IN, addr 17.110.226.73
```

A cartoon illustration of Mr. Burns from The Simpsons. He is wearing his signature straw hat and vest, and has a determined or angry expression on his face. He is holding a white spray paint can with a yellow label that appears to have a small American flag on it. The background shows a landscape with hills and a blue sky with clouds.

# Private BitBucket or GitHub to work on exploit or challenge code together

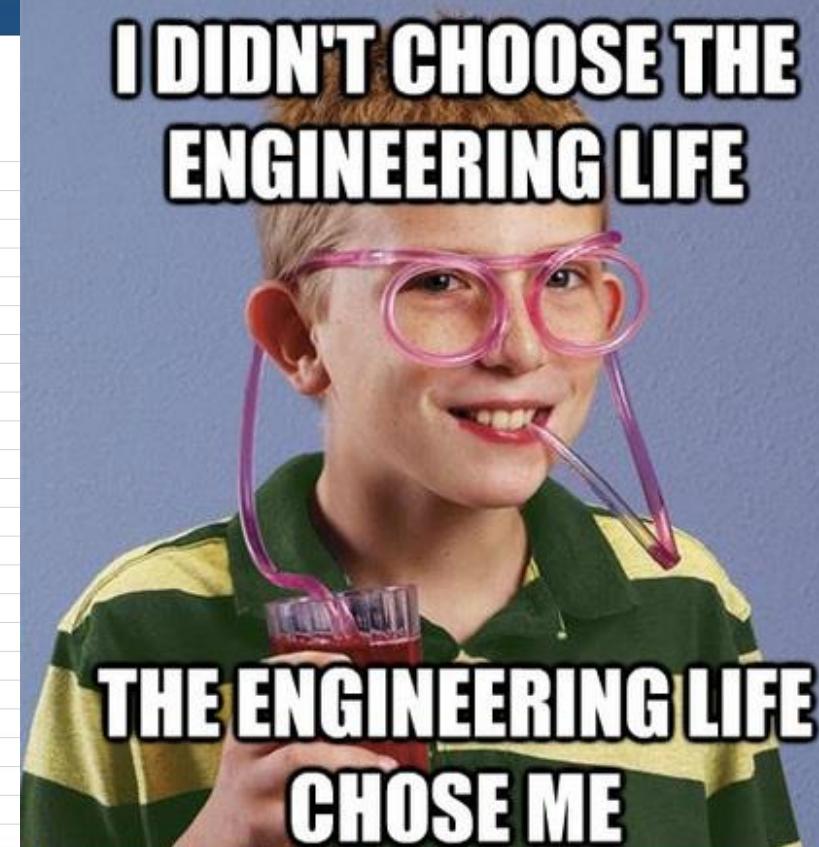


Bitbucket Dashboard Teams Repositories Snippets Create

Commits

master Show all

| Author     | Commit   | Message                                                      |
|------------|----------|--------------------------------------------------------------|
| [Avatar]   | 16bb32f  | Fix crashes.                                                 |
| [Avatar]   | 3e7d0b3  | TrafficLights                                                |
| [Avatar]   | b25c698  | Arm binary: Disarmed.                                        |
| [Avatar]   | bb398e3  | Add new OTV challenge.                                       |
| [Avatar]   | 98cc29c  | Scripty challenge.                                           |
| [Avatar]   | b05dae2  | Add NYNEX Challenge.                                         |
| [Avatar]   | 510ad01  | Added /bin/bash# to the unicode stego chall                  |
| [Avatar]   | d5fb340  | unserialize.php deleted online with Bitbucket                |
| [Avatar]   | e8c217f  | Added unserialize challenge                                  |
| [Avatar]   | b055d80  | unserialize.php web challenge                                |
| [Avatar]   | 2a32ee4  | More changes to unicode chall.                               |
| [Avatar]   | 63a7d56  | New Unicode Stego Challenge (still needs work)               |
| [Avatar]   | 0152d0e  | Fix subnet and debug flag.                                   |
| [Avatar] M | 952d58f  | Merge branch 'master' of bitbucket.org:shadowcats/bsites2015 |
| [Avatar]   | ff84751  | Web challenge. Personnel Info                                |
| [Avatar]   | c7f7198  | Delete the binary I accidentally committed.                  |
| [Avatar]   | 09fd603b | Add Chris's OTV challenge.                                   |
| [Avatar]   | ff1e544  | Build an RSA-based challenge, Account.Padding.               |
| [Avatar]   | 0434db6  | Mark distributables.                                         |
| [Avatar]   | fb0e0b1  | Support ratelimiting incoming connections in the runner.     |
| [Avatar]   | f1f6e01  | Add README for garbage.                                      |
| [Avatar]   | 055993b  | Enable whitespace.                                           |
| [Avatar]   | c87d9b2  | Initial checkin of a couple of draft challenges & notes.     |



# Start a wiki or blog for notes and lessons learned



https://shadowcats.info

Shadow Cats Home About

Shadow Cats

## Shadow Cats

View

### CTFs

- CTF Practice
- CTF Writeups
- Our CTF Library

### Security Research

- Brainstorming
- Inspiration
- Tools

I Am Devloper  
@iamdevloper

Following

[a man is choking]

waiter: quick is anyone a doctor?

vim user: i'm a vim user

RETWEETS 755 FAVORITES 875



3:10 AM - 11 Aug 2015



https://systemoverlord.com/blog/csaq-quals-2015-sharpturn-aka-forensics-400/

System Overlord System engineering, security, and CTFs. Home Blog Portfolio About

Search Everything Go

## CSAW Quals 2015: Sharpturn (aka Forensics 400)

Posted by: David Tomaschik 2015/09/21 21:33 (0 comments) 0 2

The text was just:

I think my SATA controller is dying.

HINT: `git fsck -v`

And included a tarball containing a git repository. If you ran the suggested `git fsck -v`, you'd discover that 3 commits were corrupt:

```
Checking HEAD link
Checking object directory
Checking directory ./objects/2b
Checking directory ./objects/2e
Checking directory ./objects/35
Checking directory ./objects/4a
Checking directory ./objects/4c
Checking directory ./objects/7c
Checking directory ./objects/a1
Checking directory ./objects/cb
Checking directory ./objects/d5
Checking directory ./objects/d9
Checking directory ./objects/e5
Checking directory ./objects/ef
Checking directory ./objects/f8
Checking tree 2bd4c81f7261a0eccd9bae3027a46b9746fa4f
Checking commit 2e5d53f41522fc9036bacce1398c87c2483cd5
error: sha1 mismatch 354ebf392533dce06174f9c8c093036c138
error: 354ebf392533dce06174f9c8c093036c138935f3: object
Checking commit 4a2f359e042db12cc32a68482/c79cf7c97fe0b
Checking tree 4c0555b27c05dbf0e44598a0601e5c8e28319f67
Checking commit 7c9ba838ff5ce6912c69e7171befc64da12d4c
Checking tree a1607d81984206648265fd23a4af5e13b289f83
Checking tree cb6c9498d7f33305f32522f862bce592ca4becd5
Checking commit d57aaaf773b1a8c8e79b6e515d3f92fc5cb332866
error: sha1 mismatch d961f81a588fcfde57bbea7e171daea85e61333: object
error: d961f81a588fcfde57bbea7e171daea85e61333: object
Checking blob a5a5f634b467ac6a13b6c01f4f076fa74d0251a6f22f
```

Recent Posts

- ▶ CSAW Quals 2015: Sharpturn (aka Forensics 400)
- ▶ What the LastPass CLI tells us about LastPass Design
- ▶ So, is Windows 10 Spying On You?
- ▶ Blue Team Player's Guide for Pros vs Joes CTF
- ▶ Hacker Summer Camp 2015: DEF CON

Archive

2015  
2014  
2013

What if I never find out who's a good boy?



cd Questions ??



THIS COULD B US...

