@espreto

Pentesting in SDN

Owning the controllers

CONVISO®
APPLICATION SECURITY

Who Am I?

Roberto Soares

Information Security Consultant

Conviso Application Security

@espreto

- Network (traditional)
- SDN Overview
- Threat Vectors
- Pentesting
- Defense
- Future

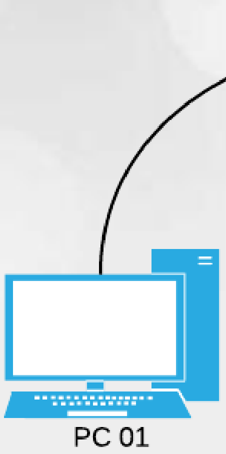
Traditionally...

- Specific Vendors;
- Scalability;
- Complexity;
- Hardware Focus;
- Interoperability;
- etc...

https://33.media.tumblr.com/tumblr_m8gl3iiTk51qjve0go1_500.gif

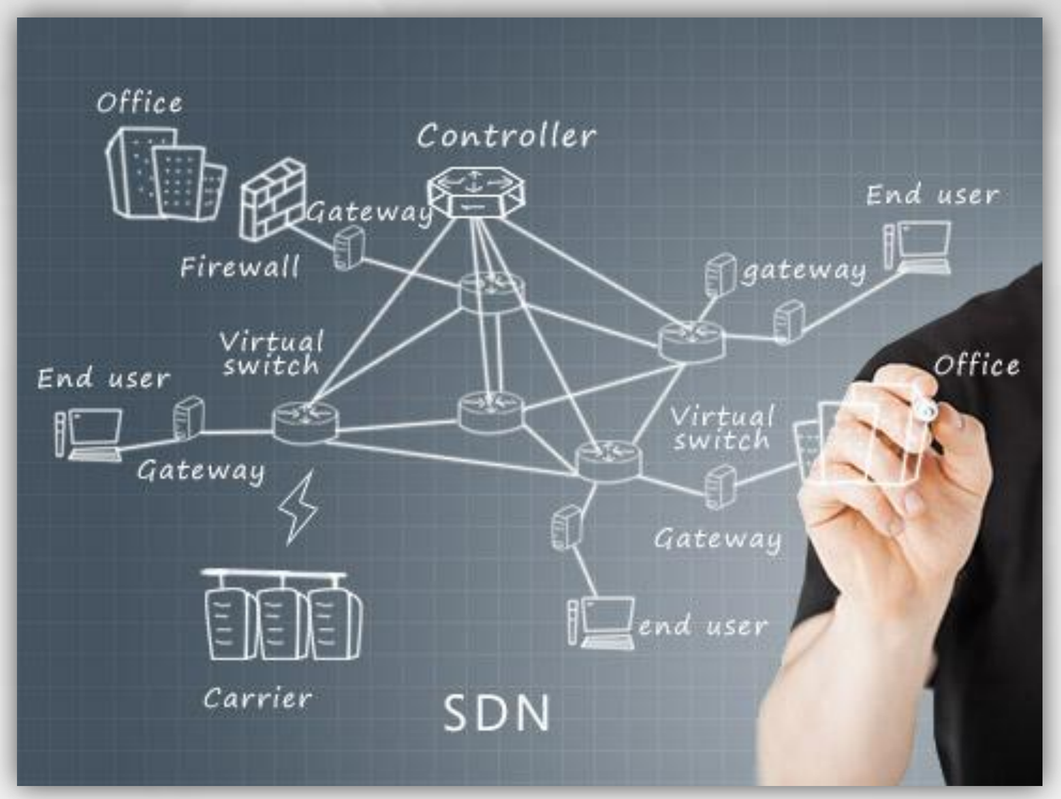
CONVISO® APPLICATION SECURITY

Classical Model



1. Package sent to the switch.
2. Switch looks in their polices.
3. Switch forwards the packet to the server.

SDN (Software Defined Network)



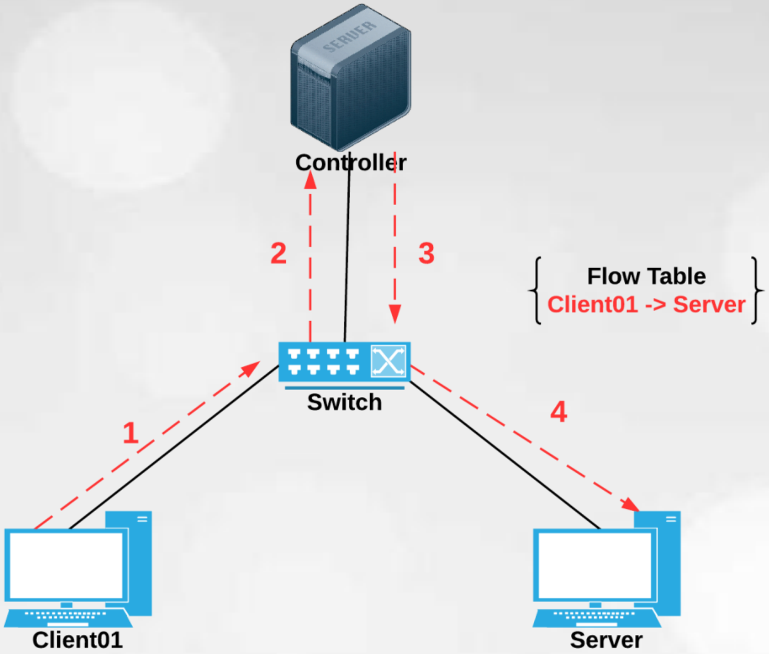
http://www.algoblu.com/en/image/sdn_1.jpg

SDN: Architecture

Data Plane & Control Plane

“SDN isn’t a technology, it’s a architecture”.

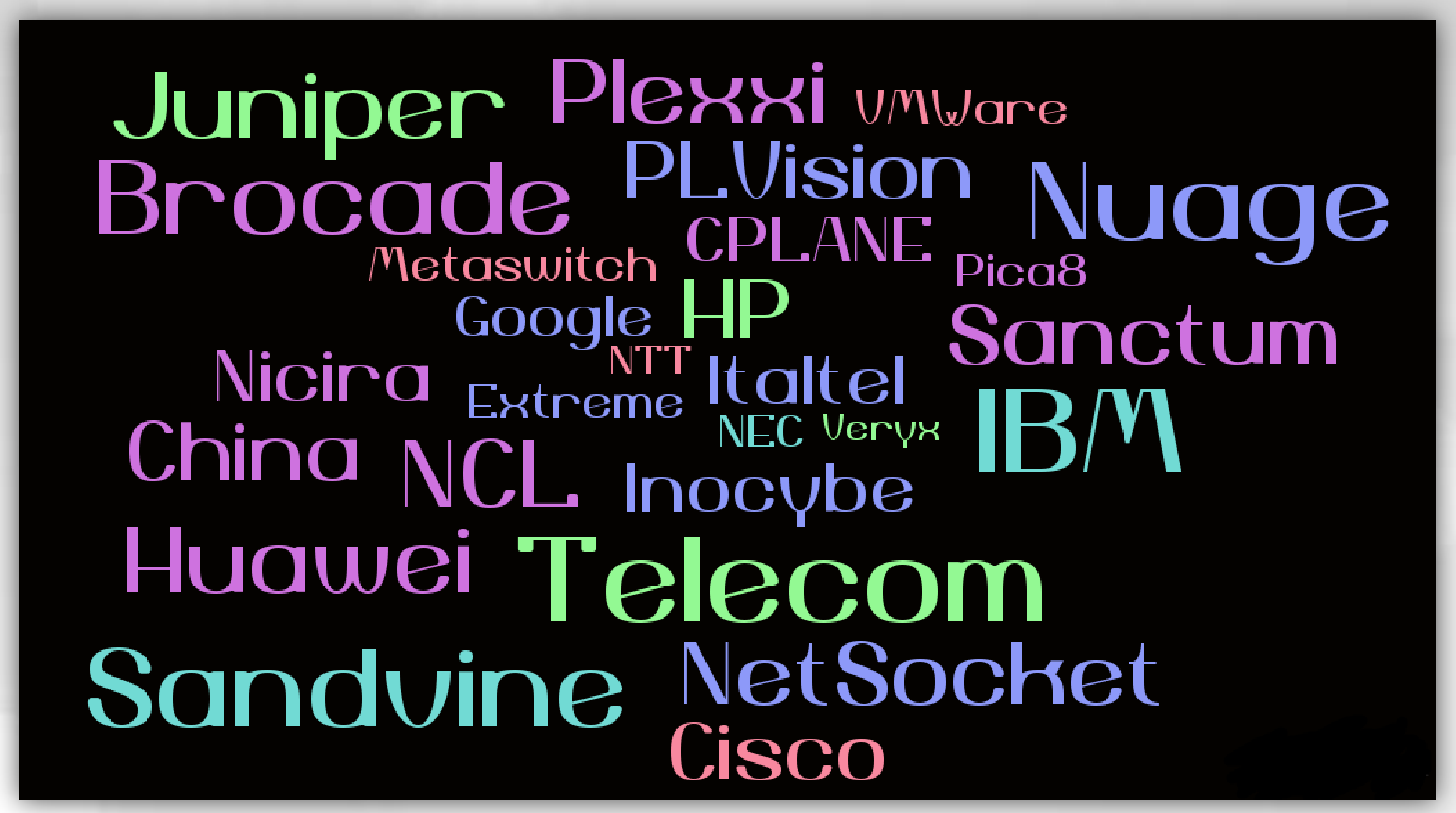
SDN: Technical



1. Packet is sent to the switch.
2. Packet header is extracted and sent to the controller.
3. Controller (check) adds a new flow in the switch table.
4. Switch forwards the packet to the server.

CONVISO®
APPLICATION SECURITY

Vendors



"SDN is just a fad..."

CONVISO® APPLICATION SECURITY

Controllers

- Commercial
  - HP VAN SDN
  - Juniper Contrail
  - Oracle SDN
  - Cisco XNC
  - Huawei POF

- Open-Source
  - Mininet
  - OpenDayLight
  - FloodLight
  - Juniper OpenContrail

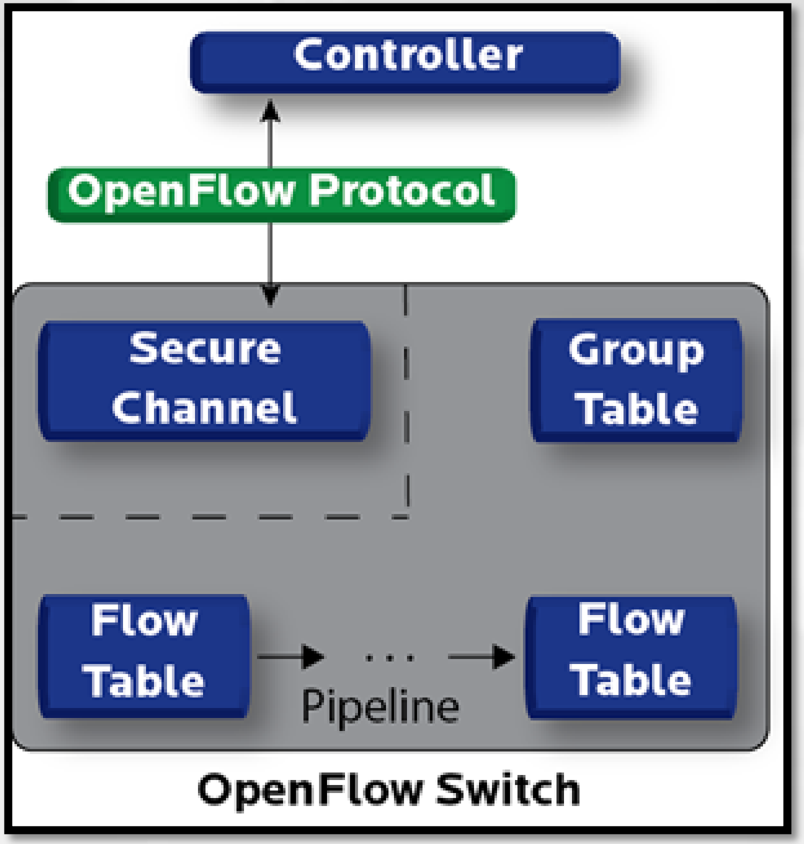
OpenFlow

- Communication between the controller and the switch (logical/physical).
- Routing flow based.
- Secure channel for transmission.
- Allows for programming “Flows“ (traffic type);
- Allows for switching different network layers to be combined;
- Not limited by the platform or be enforced by the protocols.

“SDN != OpenFlow”

CONVISO®
APPLICATION SECURITY

OpenFlow (internal)



https://www.sdncentral.com/wp-content/uploads/2013/04/figure1.png

It's time for revision!

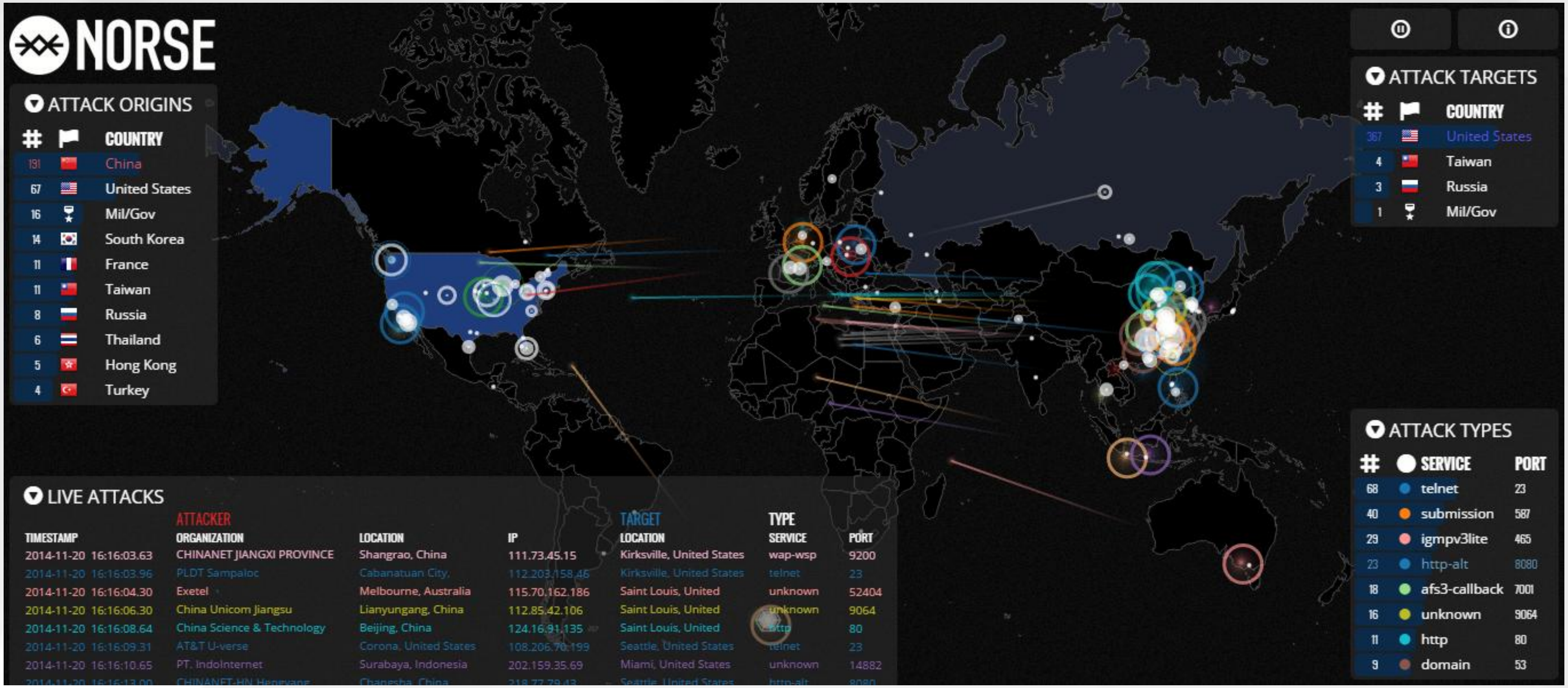
DEMO 1

SDN overview with mininet

"Why set up your network if you can program it?"

CONVISO® APPLICATION SECURITY

Threat Vectors



NORSE

ATTACK ORIGINS

#	COUNTRY
191	China
67	United States
16	Mil/Gov
14	South Korea
11	France
11	Taiwan
8	Russia
6	Thailand
5	Hong Kong
4	Turkey

ATTACK TARGETS

#	COUNTRY
367	United States
4	Taiwan
3	Russia
1	Mil/Gov

ATTACK TYPES

#	SERVICE	PORT
68	● telnet	23
40	● submission	587
29	● igmpv3lite	465
23	● http-alt	8080
18	● afs3-callback	7001
16	● unknown	9064
11	● http	80
9	● domain	53

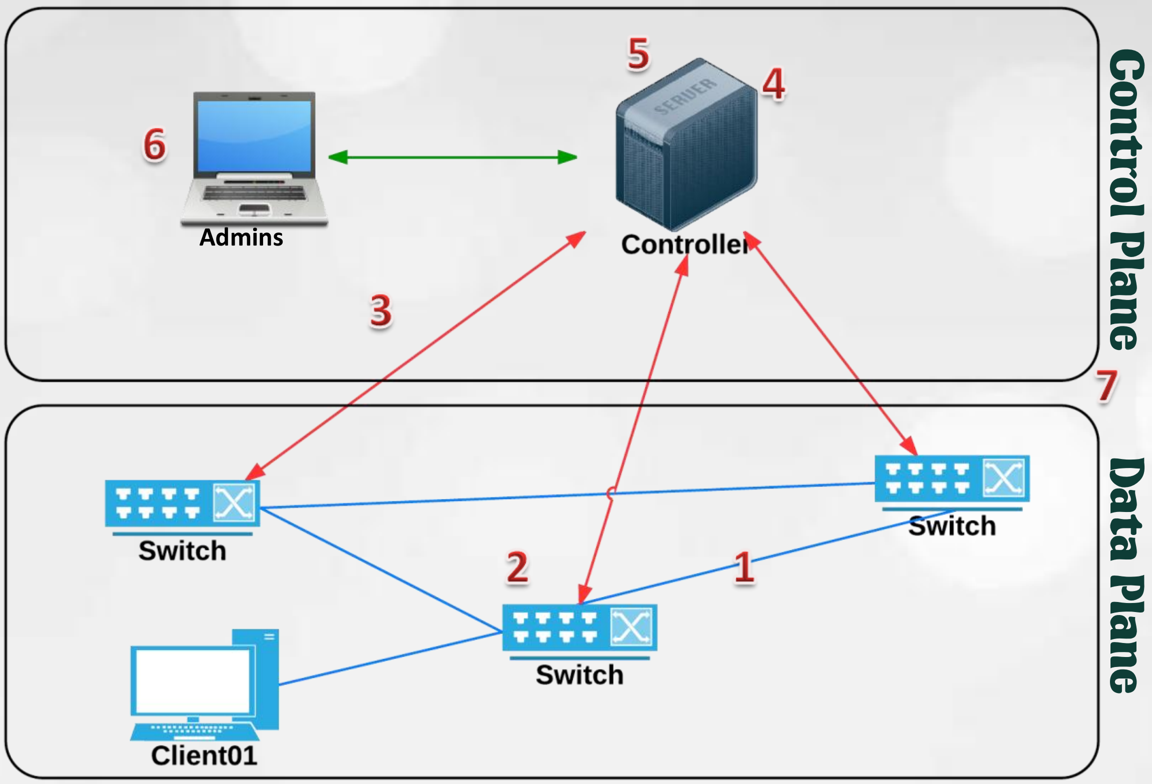
LIVE ATTACKS

	ATTACKER			TARGET	TYPE	
TIMESTAMP	ORGANIZATION	LOCATION	IP	LOCATION	SERVICE	PORT
2014-11-20 16:16:03.63	CHINANET JIANGXI PROVINCE	Shangrao, China	111.73.45.15	Kirksville, United States	wap-wsp	9200
2014-11-20 16:16:03.96	PLDT Sampaloc	Cabanatuan City,	112.203.158.46	Kirksville, United States	telnet	23
2014-11-20 16:16:04.30	Exetel	Melbourne, Australia	115.70.162.186	Saint Louis, United	unknown	52404
2014-11-20 16:16:06.30	China Unicom Jiangsu	Lianyungang, China	112.85.42.106	Saint Louis, United	unknown	9064
2014-11-20 16:16:08.64	China Science & Technology	Beijing, China	124.16.91.135	Saint Louis, United	http	80
2014-11-20 16:16:09.31	AT&T U-verse	Corona, United States	108.206.70.199	Seattle, United States	telnet	23
2014-11-20 16:16:10.65	PT. IndoInternet	Surabaya, Indonesia	202.159.35.69	Miami, United States	unknown	14882
2014-11-20 16:16:13.00	CHINANET-HN Hengyang	Changsha, China	218.77.79.43	Seattle, United States	http-alt	8080

map.ipviking.com

CONVISO® APPLICATION SECURITY

Vectors!



↔ Admins Management (SSH!?)

↔ Control Plane (OpenFlow)

↔ Data Plane (logical/physical connections)

Attacks!

1. Fake/Hijacked traffic flows.
2. Switch vulnerabilities.
3. Vulnerabilities on Control Plane communications.
4. Controller vulnerabilities.
5. Untrusted apps/plugins on controller.
6. Vulnerabilities on admin computer.
7. Lack of resources for security analysis.

Specific to SDN

CONVISO® APPLICATION SECURITY

Attacks!

1. Fake/Hijacked traffic flows.
2. Switch vulnerabilities.
3. Vulnerabilities on Control Plane communications.
4. Controller vulnerabilities.
5. Untrusted apps/plugins on controller.
6. Vulnerabilities on admin computer.
7. Lack of resources for security analysis.

CONVISO®
APPLICATION SECURITY

Pentesting...

1. Identify controllers.
2. Enumerate configs.
3. Owning the controller.

Default Ports

Controllers:

- FloodLight/Mininet/Pox/POF/HP VAN port 6633.
- Oracle SDN port 6522.

Management Interface:

- FloodLight port 8080.
- OpenDayLight Web Interface port 8080.
- HP VAN SDN & IBM SDN-VE port 8443.
- Cisco XNC HTTP (8080) and HTTPS (8443).

It's time for revision!

DEMO 2

sdn_enum_controllers.rb

https://github.com/espreto

CONVISO APPLICATION SECURITY

Authentication

Default passwords:

FloodLight = floodlight:<null>

OpenDayLight = admin:admin

HP VAN SDN = admin:skyline

Juniper Contrail = admin:contrail123

IBM SDN-VE = admin:admin

Cisco XNC = admin:admin

REST APIs

- FloodLight port 8080
  - (http://localhost:8080/wm/core/controller/switchs/json)
- OpenDayLight port 80/8080
  - (http://localhost/rest/v1/model/controller-node)
- HP VAN SDN port 35357/8443
  - (https://localhost:8443/sdn/v2.0/auth)
- Juniper Contrail port 8081/8082
  - (http://localhost:8081/analytics/uves)
- IBM SDN-VE port 8443
  - (http://localhost:8443/one/nb/v2)
- Cisco XNC port 8080
  - (http://localhost:8080/controller/nb/v2/monitor)

CONVISO® APPLICATION SECURITY

It's time for revision!

DEMO 3

sdn_enum_configs_api.rb

https://github.com/espreto

CONVISO®
APPLICATION SECURITY

It's time for revision!

DEMO 4

sdn_hp_change_pass.rb

https://github.com/espreto

CONVISO APPLICATION SECURITY

It's time for revision!

DEMO 5

sdn_hp_rce.rb

https://github.com/espreto

CONVISO®
APPLICATION SECURITY

It's time for revision!

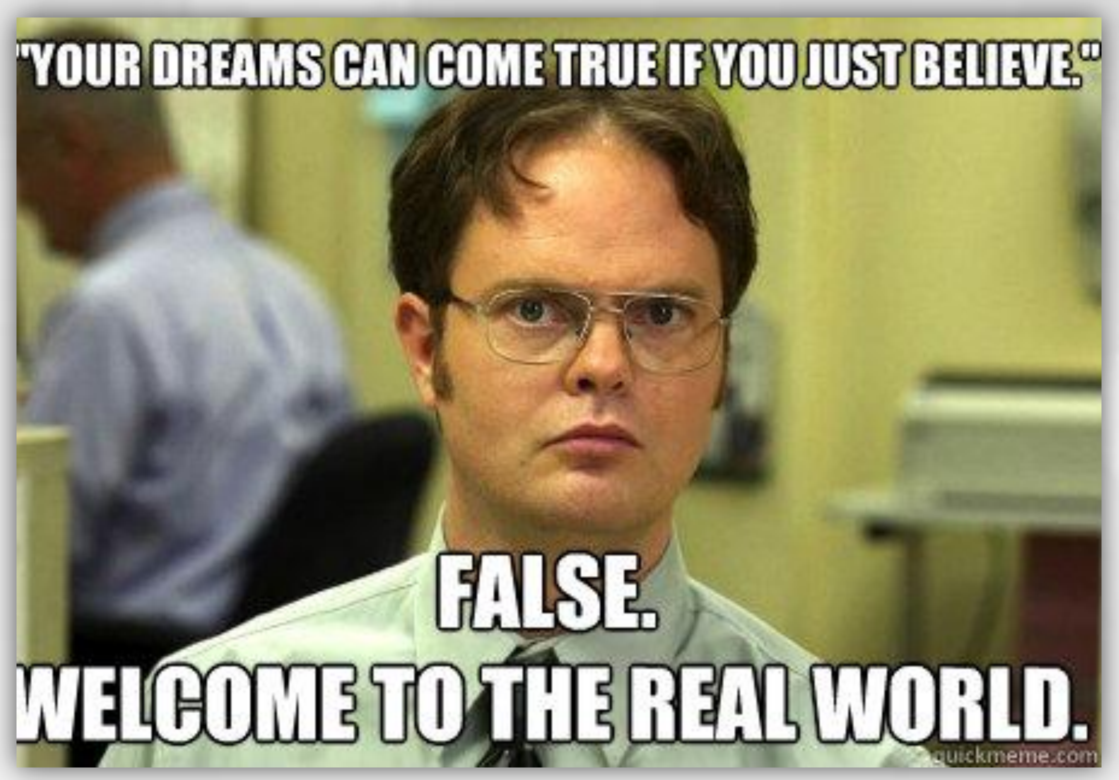
DEMO 6

sdn_contrail_read_file.rb

https://github.com/espreto

CONVISO®
APPLICATION SECURITY

Real World...


"YOUR DREAMS CAN COME TRUE IF YOU JUST BELIEVE."
FALSE.
WELCOME TO THE REAL WORLD.
quickmeme.com

http://cdn.business2community.com/wp-content/uploads/2014/08/real_world_dwight_meme.jpg

CONVISO®
APPLICATION SECURITY

Try Hard

- VLANs?
- IDS/IPS?
- NAC?
- Etc, etc, etc...

Look:
idle_timeout, hard_timeout, rtt values, etc.

“Packet Analysis is your best friend”.

Defense

- Apply controls in CP and DP;
- Restrict access APIs;
- Audit internal malicious activity;
- Plugins/Applications that add levels of security;
- Hardening;
- Secure Development Lifecycle (SDLC);
- Specialized intrusion tests;
- Others...

"Security must not be optional".

CONVISO®
APPLICATION SECURITY

Future...

...of this research:

- Coordination of CVEs with vendors; \o/
- Advanced research with SDN;
- Donations of Switches (OpenFlow supported); ☺
- Create a group to share information;
- And...

"Opportunities are usually disguised as hard work, so most people don't recognize them".
Ann Landers.

CONVISO® APPLICATION SECURITY

Questions?

@espreto

rsoares[at]conviso.com.br

robertoespreto[at]gmail.com

iwantshell.com

CONVISO®
APPLICATION SECURITY