Red IRIS

TOPERA v0.2

IPv6 and Slow HTTP Attacks

Daniel Garcia a.k.a CrOhn (twitter.com/ggdaniel)
Rafa Sánchez - (twitter.com/r_a_ff_a_e_ll_o)

buguroo
offensive security

RedIRIS

Qué vamos a contar

IDS --> SNORT --> Topera v0.1 -->

DEMO --> Topera v0.2--> DEMO

buguroo offensive security

IDS/IPS

Sistema de Detección/Prevención de Intrusos

buguroo offensive security

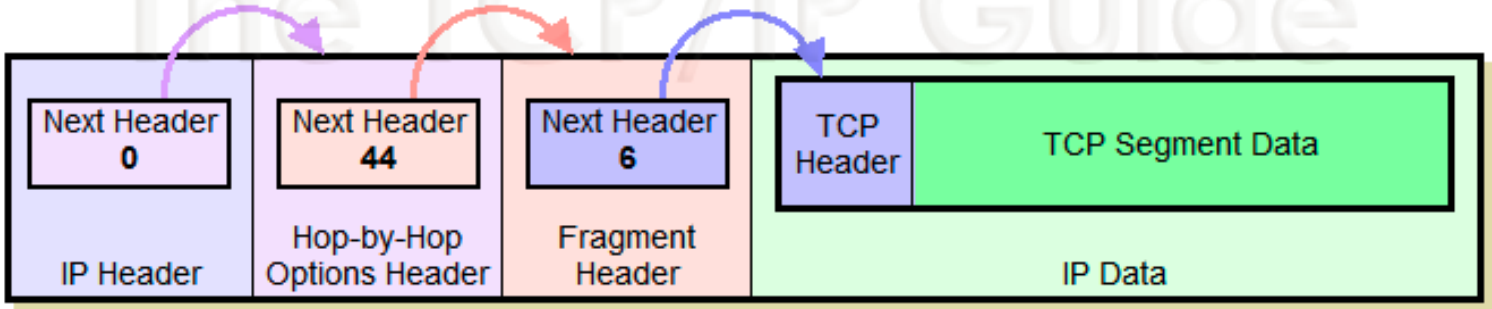
Red IRIS

SNORT

No se lleva muy bien con IPv6

SNORT

Extension Headers



http://www.tcpipguide.com/

RedIRIS

IETF

Rfc2460 -> IPv6 nodes must accept and attempt to process extension headers in any order and occurring any number of times in the same packet [...]

Dec. 1998

buguroo offensive security

IETF

A Uniform Format for IPv6 Extension Headers

[...]furthe ome issues
that a document
include umber of
extension headers [...]

IETF

Securit[illegible] Implications of the Use of IPv6 Extensi[illegible] [illegible]bor Discovery [...] this [illegible] [illegible]osts silently ignore N[illegible] [illegible]s that use IPv6 [illegible]]

(F. Gont) - IPv6 maintenance Working Group (6man)

No.	Time	Source	Destination	Protocol	Length	Info
39	140.5401570(	2003:444:555::8	fe80::a00:27ff:fe41:e!	ICMPv6	134	Echo (ping) request id=0x
40	143.9236940(	::	ff02::16	ICMPv6	90	Multicast Listener Report
42	144.6960230(	::	ff02::1:fff3:eae	ICMPv6	78	Neighbor Solicitation for
43	145.6955330(	fe80::a00:27ff:fef3	ff02::2	ICMPv6	70	Router Solicitation from

```
+ Frame 39: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
+ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 6, Src: 2003:444:555::8 (2003:444:555::8), Dst: fe80::a00:27ff:fe41:e52
  + 0110 .... = Version: 6
  + .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 80
    Next header: IPv6 destination option (60)
    Hop limit: 64
    Source: 2003:444:555::8 (2003:444:555::8)
    Destination: fe80::a00:27ff:fe41:e52 (fe80::a00:27ff:fe41:e52)
    [Destination SA MAC: CadmusCo_41:0e:52 (08:00:27:41:0e:52)]
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  + Destination Option
  + Destination Option
  + Destination Option
  + Destination Option
  + Destination Option
  + Destination Option
  + Destination Option
  + Destination Option
  + Destination Option
+ Internet Control Message Protocol v6
```

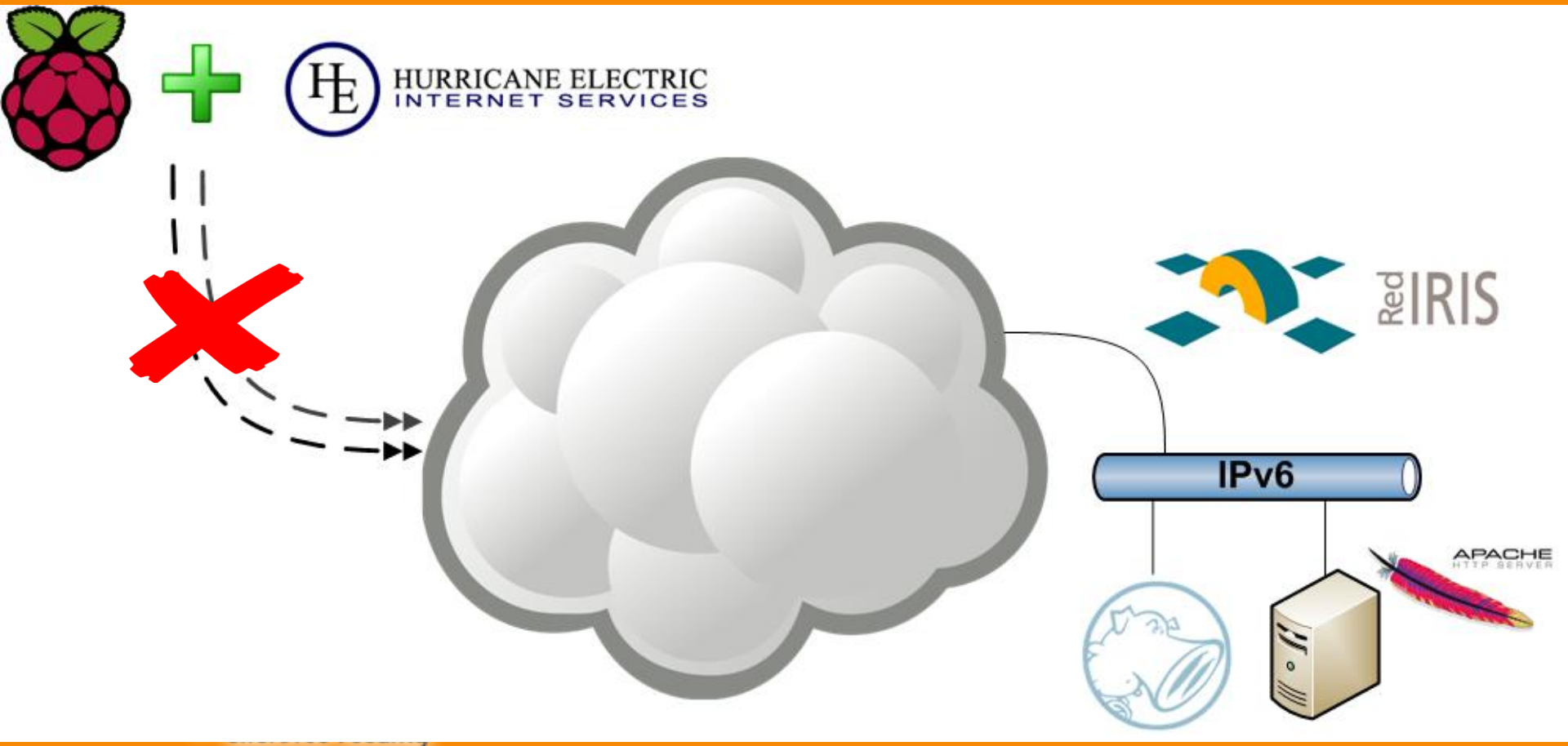
RedIRIS

Topera v0.1

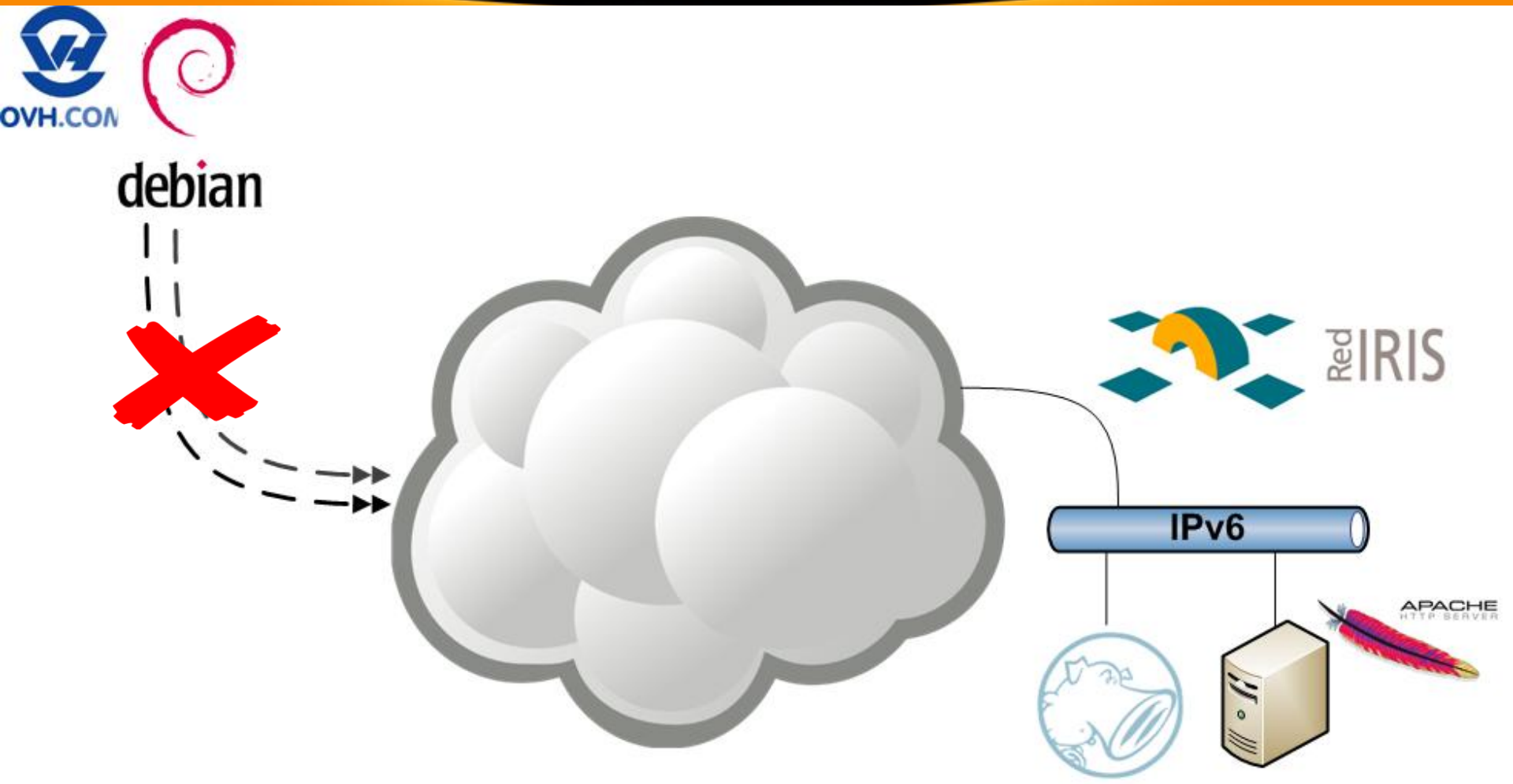
CONSECUENCIAS de TOPERA...

buguroo offensive security

Topera v0.1


HURRICANE ELECTRIC
INTERNET SERVICES
RedIRIS
IPv6
APACHE

Topera v0.1



Snort mailing list archives

By Date By Thread Search

Re: Interesting

From: Joel Esler <jesler () sourcefire com>
Date: Tue, 11 Dec 2012 20:33:04 -0500

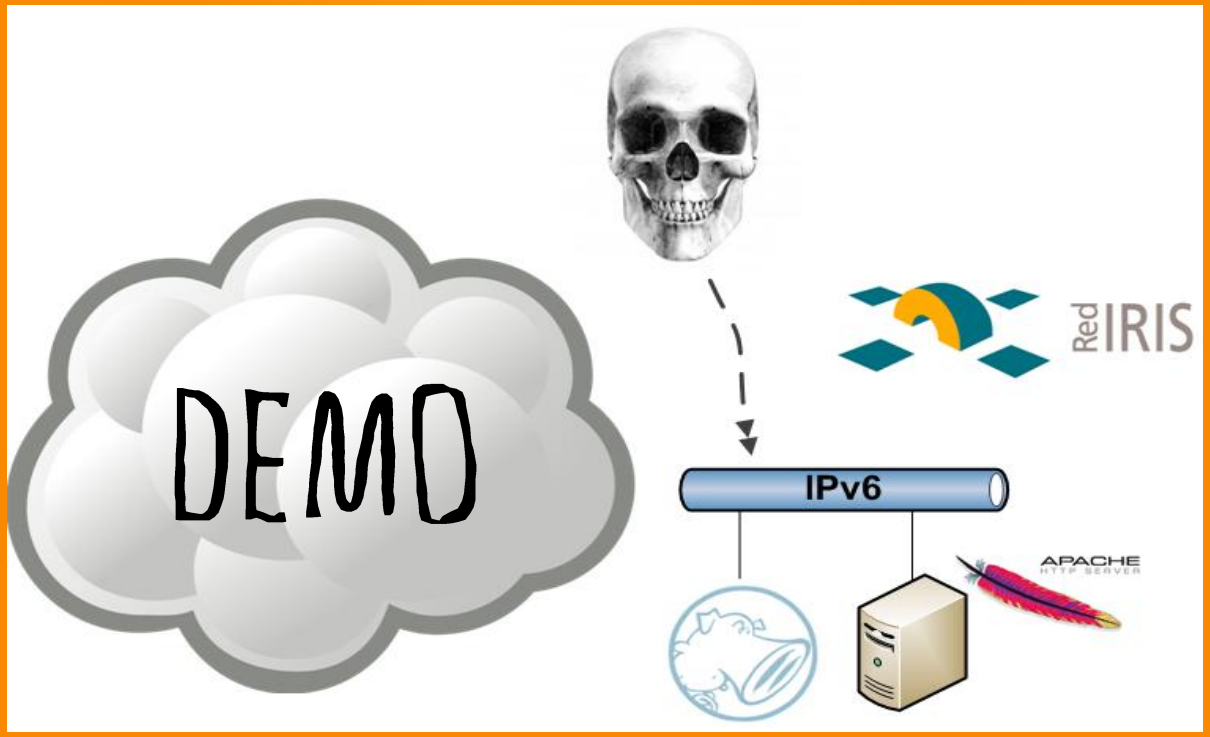
We're looking into it as well. Sorry I haven't responded sooner.

--
Joel Esler
Sent from my iPhone □

On Dec 11, 2012, at 5:02 PM, "Lay, James" <james.lay () wincofoods com> wrote:

> Thanks Elz…nice to know someone is looking at it J
>
> James
>
> From: beenph [mailto:beenph () gmail com]
> Sent: Tuesday, December 11, 2012 10:10 AM
> To: Lay, James
> Cc: snort-users () lists sourceforge net
> Subject: Re: [Snort-users] Interesting
>
>
> On Tue, Dec 11, 2012 at 9:59 AM, Lay, James <james.lay () wincofoods com> wrote:
>
> > http://code.google.com/p/topera/

Topera v0.1



http://code.google.com/p/topera/

buguroo offensive security

Nuevos Ataques

TOPERA evoluciona...

buguroo offensive security

Red IRIS

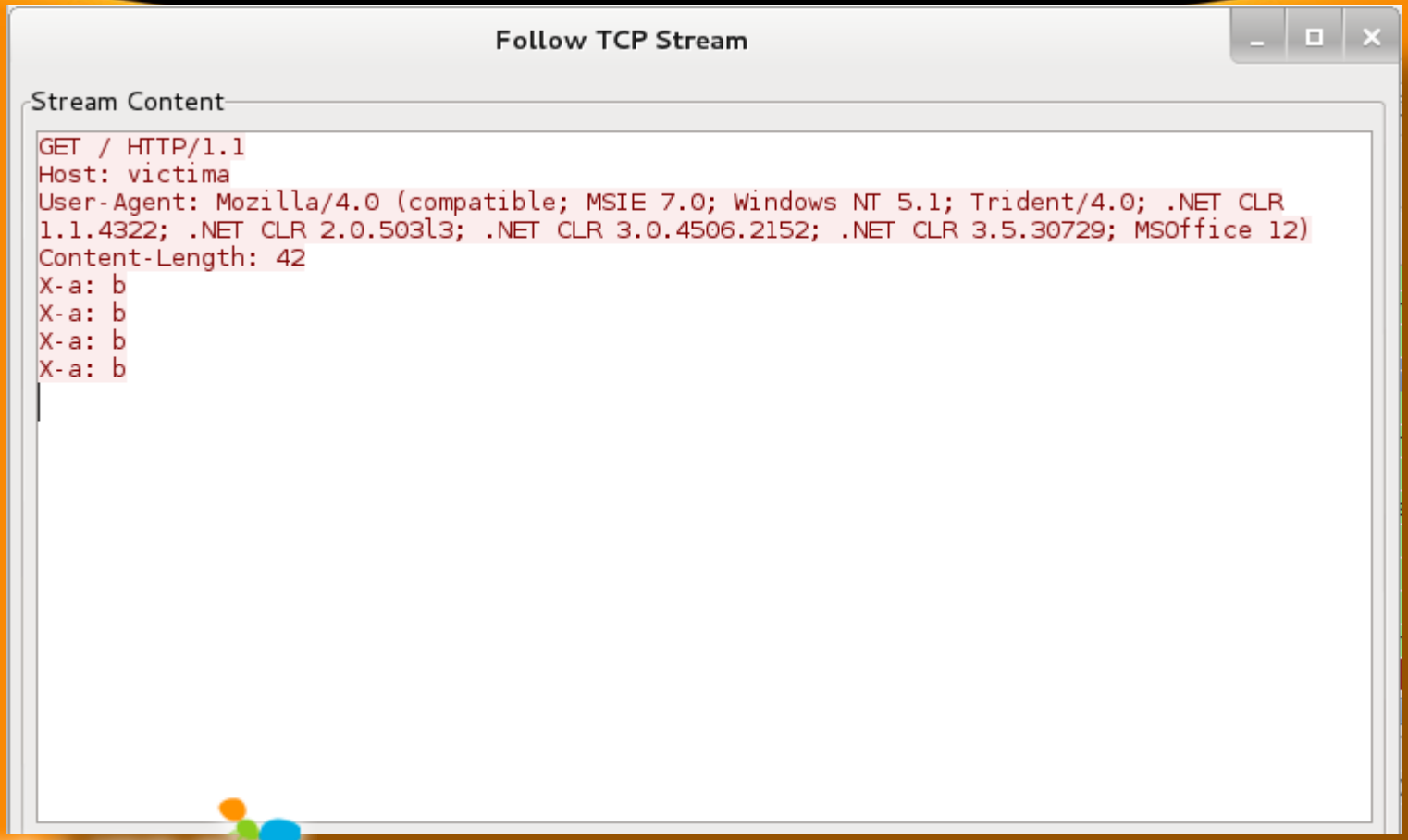
Slow HTTP

Denial Of Service Attack

buguroo
offensive security

Red IRIS

Slowloris



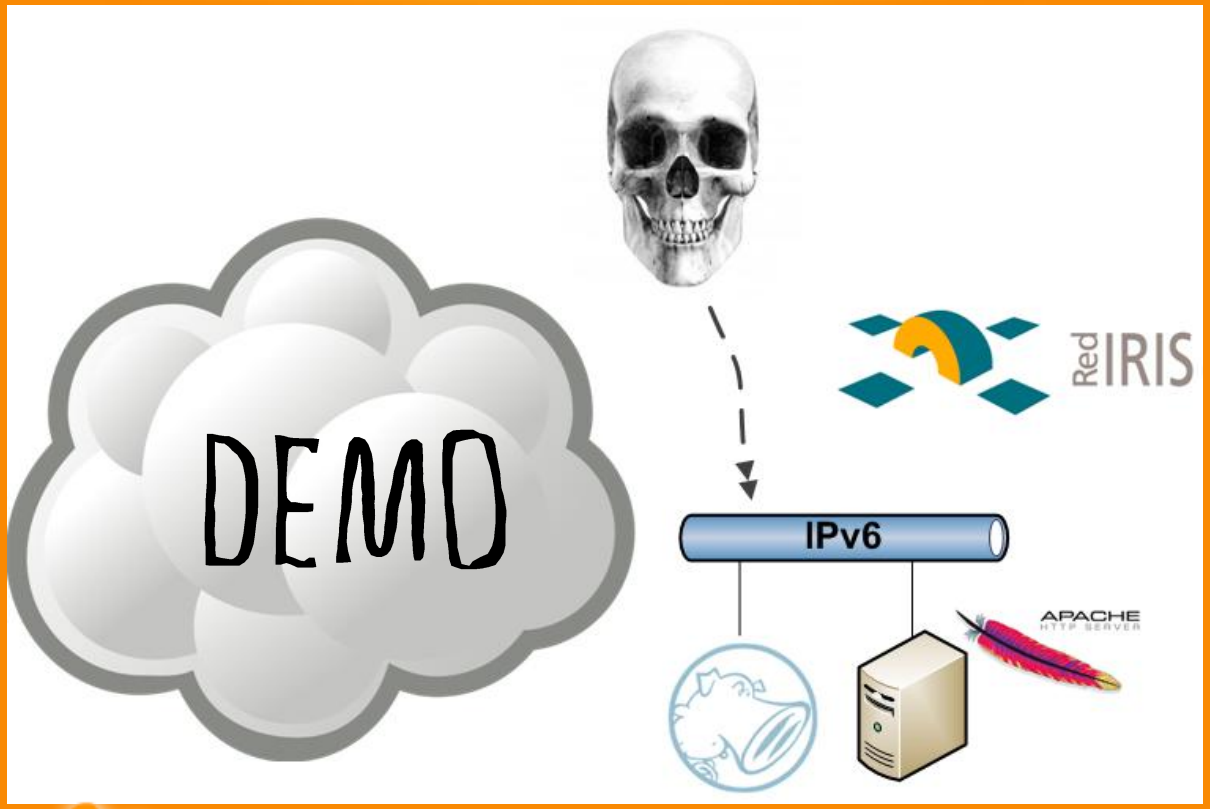
TOPERA v0.2

Y si mezclamos todo?

buguroo offensive security

http://securityreactions.tumblr.com/

Topera v0.2



buguroo
offensive security

RedIRIS

Topera v0.2

https://github.com/toperaproject/topera/

buguroo offensive security

Es un Riesgo Real??

cias Ralli, Fran!!

RedIRIS

Es un Riesgo Real??

SOURCEfire®

ABOVE SECURITY™ DEPUIS/SINCE 1999

INDUSTRIAL DEFENDER®

BT

ALTOR NETWORKS

OPTENET Get optimal internet

astaro internet security

DIGITAL SECURITY true+ assurance | clarity | insight

BRCONNECTION

SAVVIS℠

buguroo® offensive security

Gracias!!