IOT and Network Security from device to core

Rashid Khan,
Director, Networking

Red Hat

UML Alum EE ‘96

You made the right choice going here

Red Hat

Agenda

- Background
- Internet Stats
- IOT and Stats
- DDOS
- MITM
- DNS
- Common Sense mitigations
- CVE
- Open Source
- Q&A

Red Hat

We sell free SW, and IBM acquired us for ~34B

RH runs in 90% of Fortune 500 companies

Annual Rev of approx ~4B

Some Internet stats

Most users access the Internet with	**Chrome browser** (64.45%) than any other browser. (*statcounter*)
Most users access the Internet with an	**Android device** (38.9%) than any other desktop or mobile device. (*statcounter*)
The average Internet user spends	**6.5 hours online every day**. (*We Are Social Global Digital Report 2019*)
For every second of the day there is	**88,555 GB** of Internet traffic. (*Internet live stats*)

https://hostingfacts.com/internet-facts-stats

Red Hat

https://www.internetlivestats.com/

4,532,128,565

Internet Users in the world

1,763,824,437

Total number of Websites

127,546,191,619

Emails sent today

3,470,383,943

Google searches today

3,320,219

Blog posts written today

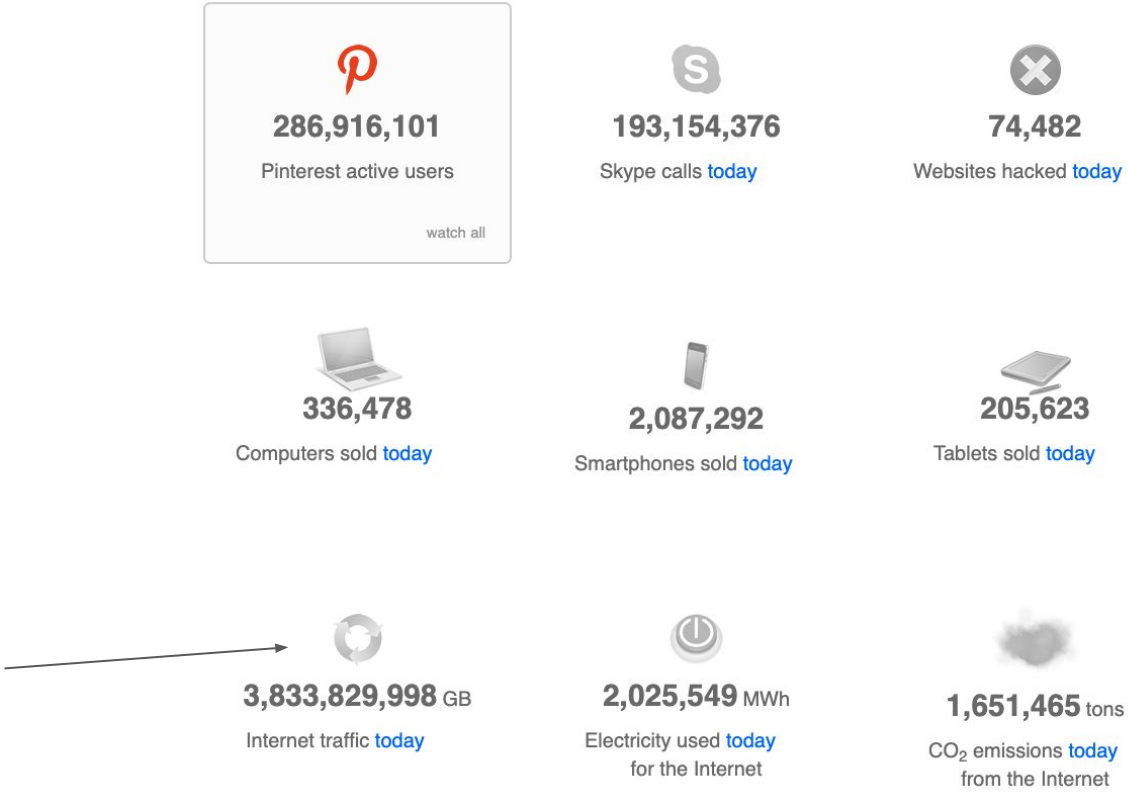
377,582,048

Tweets sent today

Red Hat

https://www.internetlivestats.com/

Internet Traffic Today?



Red Hat

What is an IOT device?

In a very general sense, IoT refers to a broad range of internet-connected devices that are capable of communicating with other devices and networks. They can perform a variety of functions but are most often used to gather information and perform specific actions. While many of them have the ability to process data, some are only intended to gather and transmit data elsewhere for processing.

Security cameras
Smart Sprinklers
Subaru
Locks
Lenscrafters
Sephora

Mirror.co
Toilets on Boeing
Industrial lighting

https://www.vxchnge.com/blog/iot-statistics

Some IOT stats

Next 7 years how many IOT devices will be there?	**41 Billion**
How many years is 1B seconds	**31.75 years**
How many new IOT devices come online every sec	**127**
Total Economic Impact of IoT by 2025	**4T - 11T$ (12 zeros) US Budget is ~4T**

https://www.vxchnge.com/blog/iot-statistics

Red Hat

Netflix Anyone?

netstat

```
tcp4       0      0  rashids-air-37.h.62811 s3-1.amazonaws.c.https ESTABLISHED
tcp6       0      0  2601:18f:802:972.62810 2620:149:a41:103.https ESTABLISHED
tcp4       0      0  rashids-air-37.h.62805 ec2-18-221-40-48.19997 ESTABLISHED
tcp4       0      0  rashids-air-37.h.62801 server-13-35-87-.https ESTABLISHED
tcp6       0      0  2601:18f:802:972.62794 2607:f8b0:4004:c.5228  ESTABLISHED
tcp6       0      0  2601:18f:802:972.62783 2620:149:a41:102.https ESTABLISHED
tcp6       0      0  2601:18f:802:972.62751 2620:149:a41:102.https ESTABLISHED
tcp4       0      0  rashids-air-37.h.62723 ec2-18-204-85-51.https ESTABLISHED
tcp4       0      0  rashids-air-37.h.62703 ec2-52-14-94-164.19997 FIN_WAIT_2
tcp4       0      0  rashids-air-37.h.62561 ec2-3-18-81-55.u.19997 FIN_WAIT_2
tcp4       0      0  rashids-air-37.h.62537 ec2-18-223-183-1.19997 FIN_WAIT_2
tcp4       0      0  rashids-air-37.h.61628 eap.redhat.com.https   ESTABLISHED
tcp4       0      0  rashids-air-37.h.60249 ec2-18-215-36-24.https ESTABLISHED
tcp4       0      0  rashids-air-37.h.49152 rkrkrk.hsd1.ma.c.56922 ESTABLISHED
tcp4       0      0  rashids-air-37.h.59536 google-home.hsd1.8009  ESTABLISHED
tcp4       0      0  rashids-air-37.h.54788 niya-airport-cap.afpov ESTABLISHED
tcp4       0      0  rashids-air-37.h.52741 niya-airport-cap.afpov ESTABLISHED
tcp6       0      0  rashids-macbook-.49134 fe80::2133:4b61:.1025  ESTABLISHED
tcp6       0      0  rashids-macbook-.1024  fe80::2133:4b61:.1024  ESTABLISHED
tcp4       0      0  rashids-air-37.h.52387 17.57.144.52.5223      ESTABLISHED
tcp6       0      0  rashids-macbook-.ias-r fe80::988:e573:e.1025  ESTABLISHED
tcp6       0      0  rashids-macbook-.1024  fe80::988:e573:e.1024  ESTABLISHED
tcp6       0      0  rashids-macbook-.19004 fe80::dbef:e09d:.1025  ESTABLISHED
tcp6       0      0  rashids-macbook-.1024  fe80::dbef:e09d:.1024  ESTABLISHED
tcp6       0      0  rashids-macbook-.black fe80::eb2f:5abe:.15505 ESTABLISHED
tcp6       0      0  rashids-macbook-.1024  fe80::eb2f:5abe:.1024  ESTABLISHED
udp4       0      0  *.*                    *.*
udp6       0      0  2601:18f:802:972.63432 lga25s60-in-x03..https
udp6       0      0  2601:18f:802:972.64680 lga25s55-in-x0a..https
udp4       0      0  *.*                    *.*
udp4       0      0  *.bootpc               *.*
udp4       0      0  rashids-air-37.h.60599 lga25s55-in-f227.https
udp4       0      0  *.mdns                 *.*
udp6       0      0  2601:18f:802:972.52256 lga34s16-in-x0e..https
udp6       0      0  2601:18f:802:972.53445 2607:f8b0:400d:c.https
```

670 sessions / connections

718 after netflix session

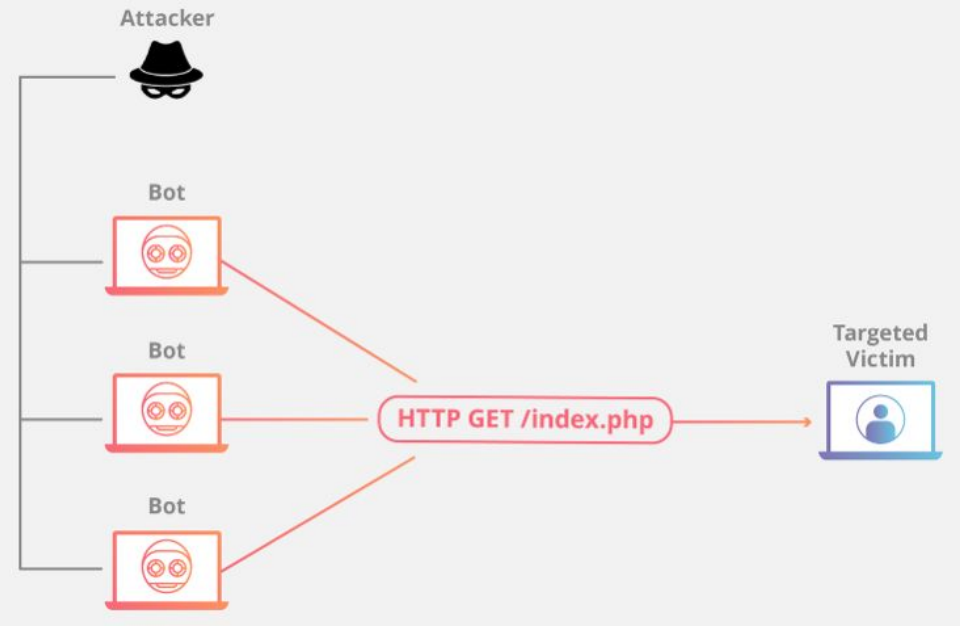
Red Hat

What is DDOS?

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic

https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

What is DDOS?



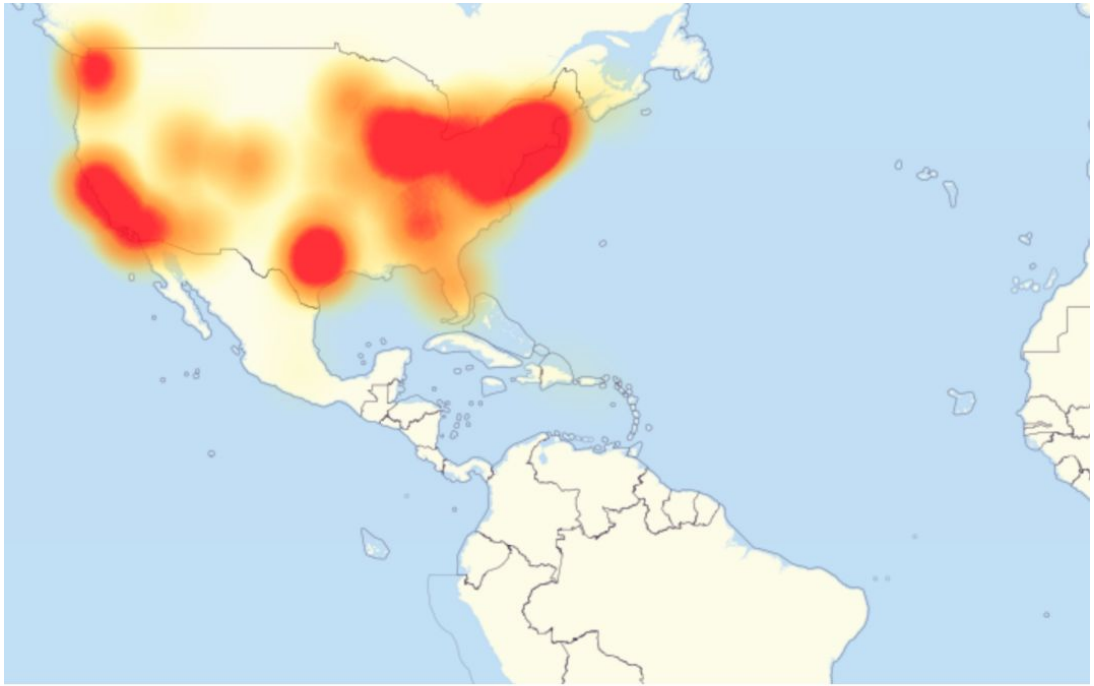
Red Hat

2016 Dyn cyberattack

The **2016 Dyn cyberattack** was a series of distributed denial-of-service attacks (DDoS attacks) on October 21, 2016, targeting systems operated by Domain Name System (DNS) provider Dyn. The attack caused major Internet platforms and services to be unavailable to large swathes of users in Europe and North America

https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

2016 Dyn cyberattack



A map of internet outages in Europe and North America caused by the Dyn cyberattack (as of 21 October 2016 1:45pm Pacific Time).

Red Hat

2 Million IoT Devices Vulnerable to Complete Takeover

Millions of security cameras, baby monitors and “smart” doorbells are open to hijack – and no solution is currently available.

Over 2 million IP security cameras, baby monitors and smart doorbells have serious vulnerabilities that could enable an attacker to hijack the devices and spy on their owners — and there’s currently no known patch for the shared flaws.

https://threatpost.com/iot-devices-vulnerable-takeover/144167/

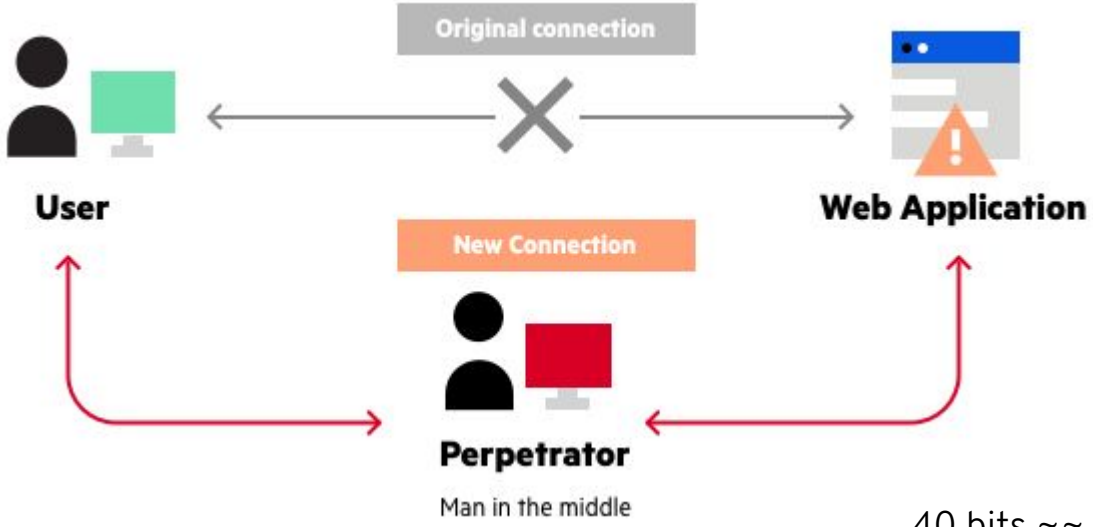
Red Hat

What is Man in the middle attack?

A man-in-the-middle attack requires three players. There's the victim, the entity with which the victim is trying to communicate, and the "man in the middle," who's intercepting the victim's communications. Critical to the scenario is that the victim isn't aware of the man in the middle.

https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

What is a man in the middle attack?



40 bits ~~ 9 minutes

Lock symbol

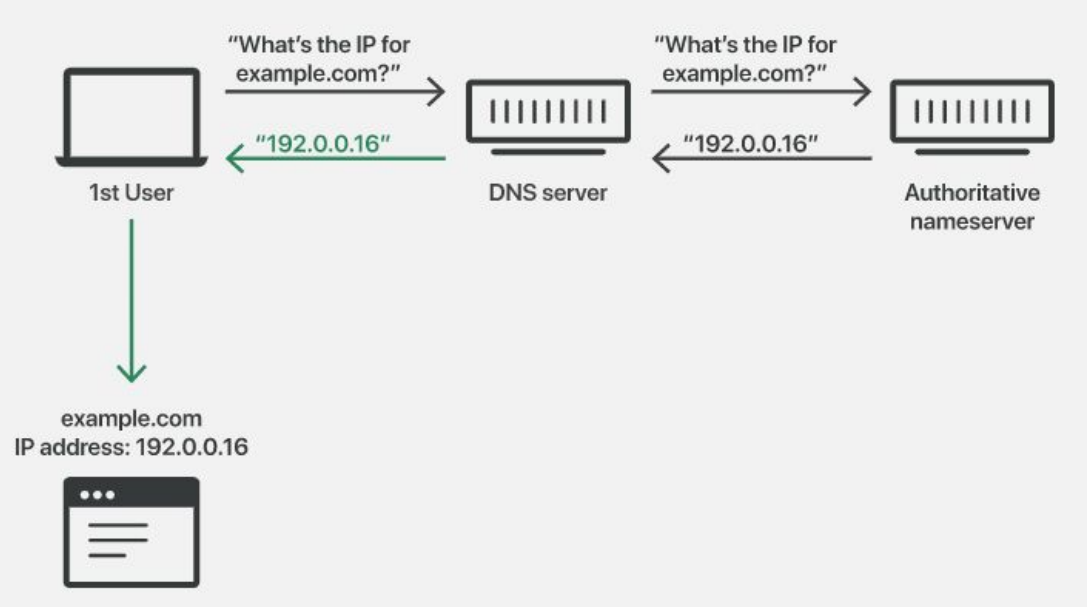
Red Hat

What is DNS spoofing?

DNS cache poisoning is the act of entering false information into a DNS cache, so that DNS queries return an incorrect response and users are directed to the wrong website

https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

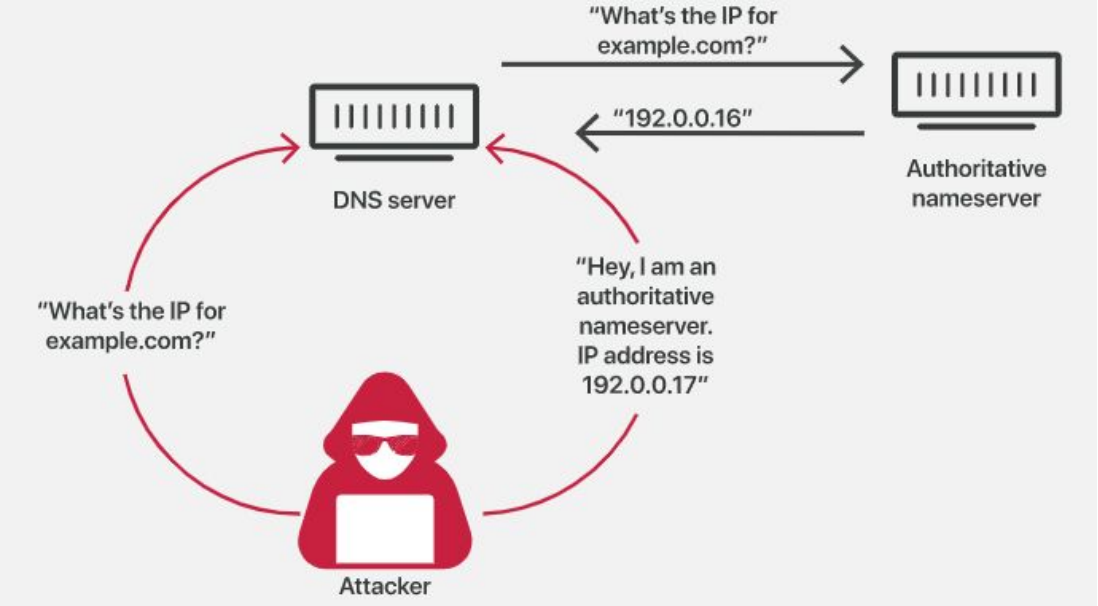
DNS Spoofing



https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

Red Hat

DNS Spoofing



https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

Red Hat

What is the biggest problem in network security?

Red Hat

What is the biggest problem in network security?

As secure as the weakest link

Red Hat

What is the biggest problem in network security?

As secure as the weakest link

Red Hat

What is the biggest problem in network security?

- admin admin, password, pa$$w0rd, golf
- Default (manufacturing, vs end use)
- Sudo
- Running privileged services as root
- Leaving troubleshooting tasks in place
- Being lax about patches

https://www.infoworld.com/article/3003634/10-dumb-security-mistakes-sys-admins-make.html

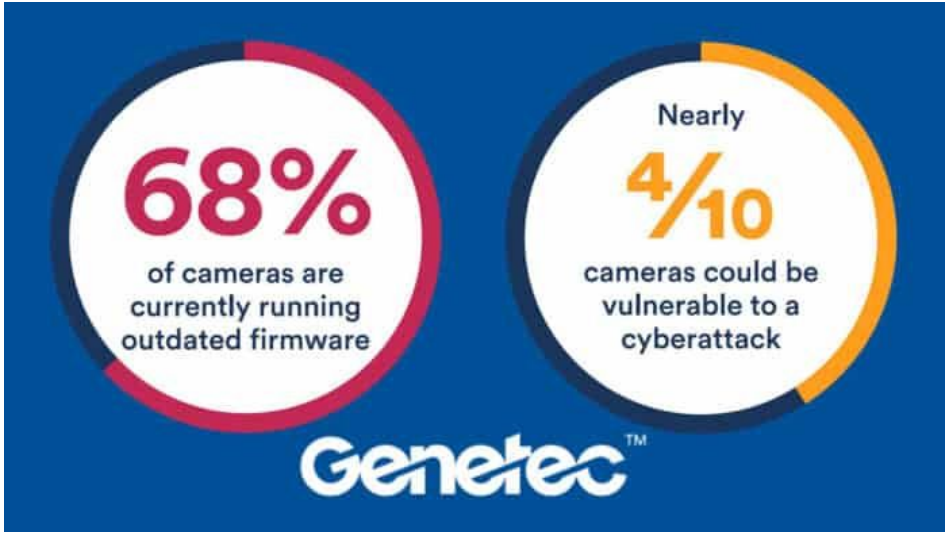
Red Hat

What is the biggest problem in network security?

The vast amounts of video data generated by the cameras flow through the network to be analyzed at servers (e.g., cloud). The Cisco Visual Networking Index [14] (Cisco VNI) predicts that the IP video traffic will be 82% of the consumer Internet traffic by 2020 from 70% in 2015. Following this trend, we assume that the IP video traffic will be more than
95% of the Internet traffic by 2030

https://engineering.purdue.edu/HELPS/Publications/papers/2017ISCAS.pdf

What is the biggest problem in network security?



Admin admin
Manufacturing

https://lossprevention media.com/4-in-10-security-cameras-can-be-at-risk-of-cyber-attack-due-to-outdated-firmware/

Red Hat

What is a CVE?

Common Vulnerabilities and Exposures

https://cve.mitre.org/

Spectre Meltdown?

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

https://meltdownattack.com/

CVE-2019-11477

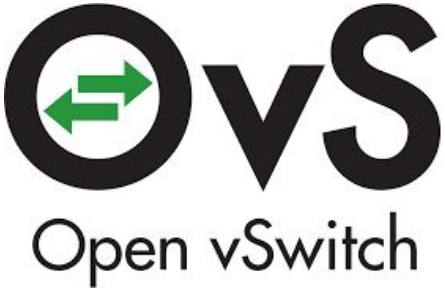
1. tcp: tcp_fragment() should apply sane memory limits
2. tcp: refine memory limit test in tcp_fragment()
3. tcp: be more careful in tcp_fragment()

https://cve.mitre.org/about/faqs.html#what_is_cve_id

What is Open Source?

Open Source Benefits?

Opportunities (Challenges) with Open Source?



What can YOU do?

Red Hat

Home work

How do public and private key pairs work?

https://www.redhat.com/en/open-source-stories

Questions?

Thank You!

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat