Welcome to

Log analyse med Elasticsearch, Logstash og Kibana

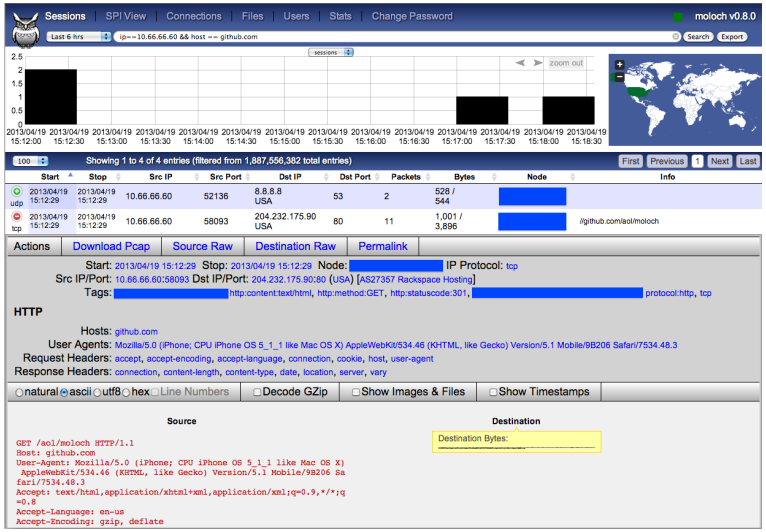
TheCamp.dk 2015

Henrik Lund Kramshøj hlk@kramse.org

THECAMP.DK - 7 open source days

Slides are available as PDF, kramshoej@Github

Goals of today



Log analysis is required today - and we have many logs

Gather logs, parse logs, explain logs - fix stuff

Google your logs with the ELK stack

Show sample logs from Suricata, Sudo, SSH, Postgresql m.fl.

Plan for today

Kl 13:30 - 16:00 with a break, or shorter

Less presentation, more talk

Less me talking (only) and more 2.0 social media interaction

Trying to fit in demo and workshop-like stuff

The current situation

Internet security sucks

Personal computers like laptops suck at security

Mobile devices suck even more at security - less CPU/MEM/storage

We depend on cloud services and underfunded infrastructure - OpenSSL

We depend on others and the whole internet - DDoS

Goals: Internet Ninjas

Real super heroes are just ninjas

By knowing the internet, technologies and possibilities

Using technology and knowledge make it seem magical

In reality preparedness and defense in depth go a looooong way

Common sense is not magic, structured methods are king

Challenges

Less resources available for IT and infosec

Lots of new malware, virus, vulnerabilities and hacking

Dataloss ransomware, theft

Loss of confidentiality, 2014: 700 million lost accounts

Infosec charlatans, hype and lies

Your boss wants: No cost, and please show us great results

Solutions

Automate your job, Ansible is our poison - demo

Backup your life, help others backup, Duplicity is my choice

Learn self-defense for yourself, practice infosec war `http://ssd.eff.org`

Use hackertools to detect and identify

Categories, sort, prioritize, group problems - solve more

Measure, collect and present - make it pretty

Learn from devops, Elasticsearch Logstash Kibana D3.js

Use your brain

A lot will seem easy and basic from the outside, but when you are knee-deep in something you loose focus. Take a step back once in a while.

Case: Aalborg Farve og Lak.

> ”Vi skulle alligevel have nyt Navision-system i maj, så vi måtte fremrykke den investering. På den måde kunne vi få tastet alt ind i det nye system. I hele sagen har vi dog tabt omkring en million kroner med de mistede ordrer, ny software og revisionsbistand,”

Medejer og salgs- og personaleansvarlig hos Aalborg Farve- og Lak, Pernille Skall

Break-in through Windows Xp

Ransomware infection - across multiple systems

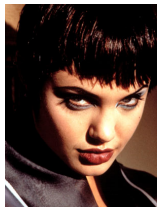
Latest backup from November (currently we are in April!)

Great that they share

Todays break-ins use yesterdays vulns, repeated and documented multiple times

`http://www.computerworld.dk/art/233684/hacker-kom-ind-via-labelprinter-tog-dans`

Hackertools are for everyone!



- Hackers work all the time to break stuff, Use hackertools:
- Nmap, Nping `http://nmap.org`
- Wireshark - `http://www.wireshark.org/`
- Aircrack-ng `http://www.aircrack-ng.org/`
- Metasploit Framework `http://www.metasploit.com/`
- Burpsuite `http://portswigger.net/burp/`
- Skipfish `http://code.google.com/p/skipfish/`
- Kali Linux `http://www.kali.org`

Most popular hacker tools `http://sectools.org/`

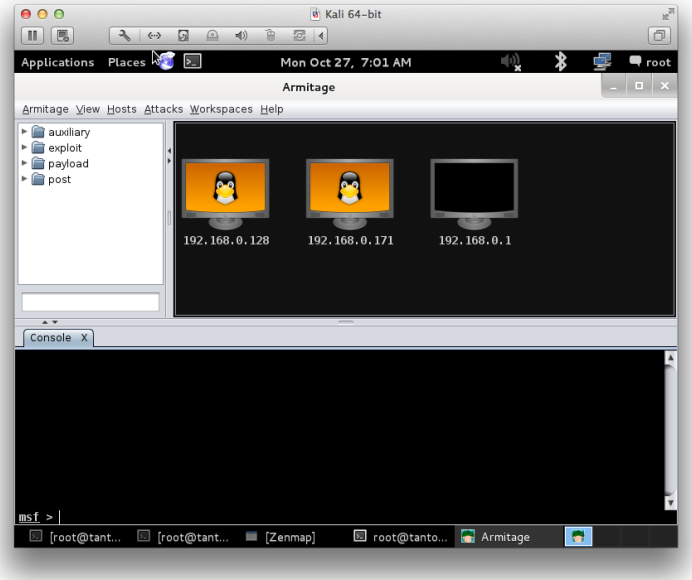
Kali Linux the pentest toolbox

Kali `http://www.kali.org/`

100.000s of videos on youtube

Also versions for Raspberry Pi, mobile and other small computers

Metasploit and Armitage Still rocking the internet

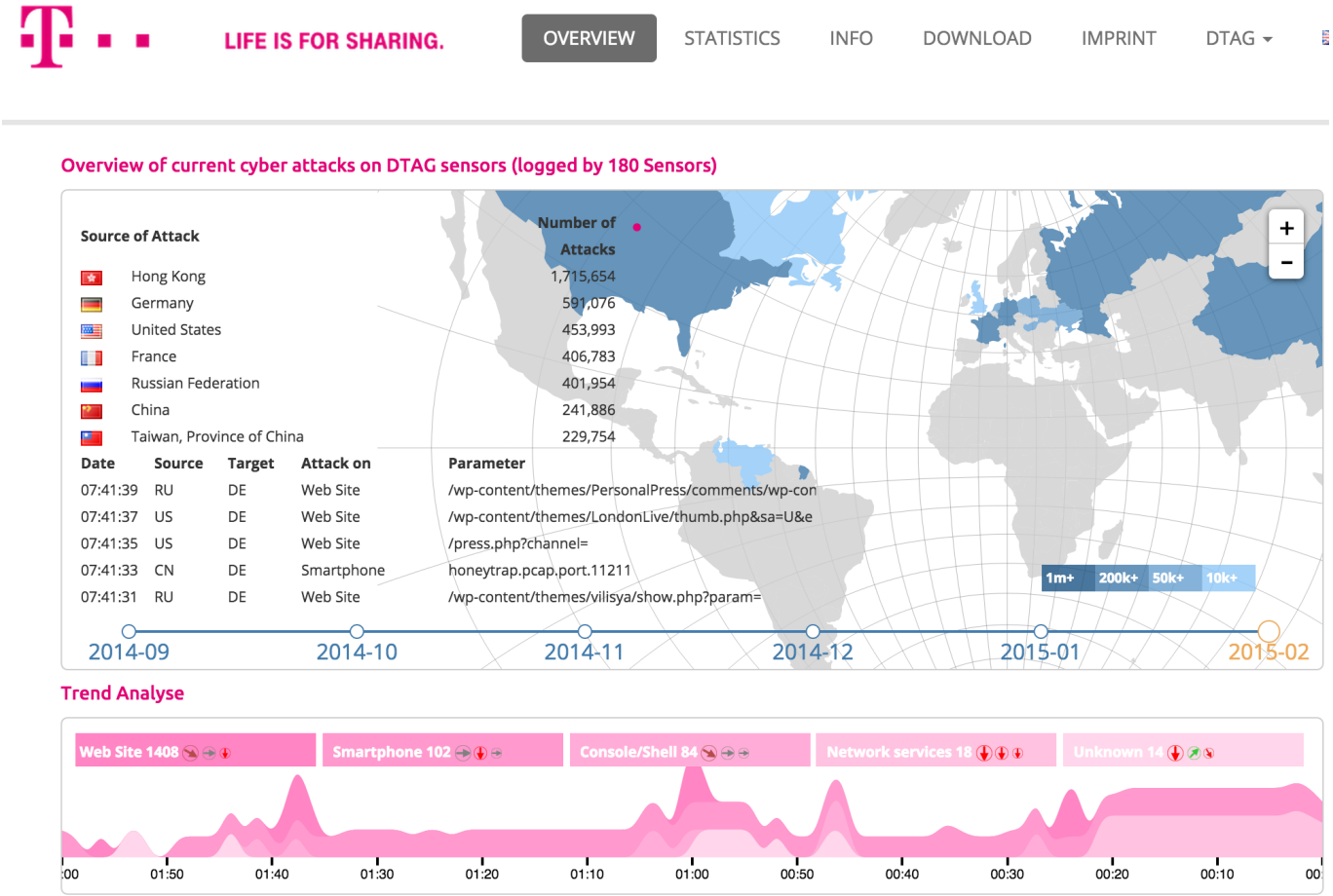


`http://www.metasploit.com/`

Armitage GUI fast and easy hacking for Metasploit
`http://www.fastandeasyhacking.com/`

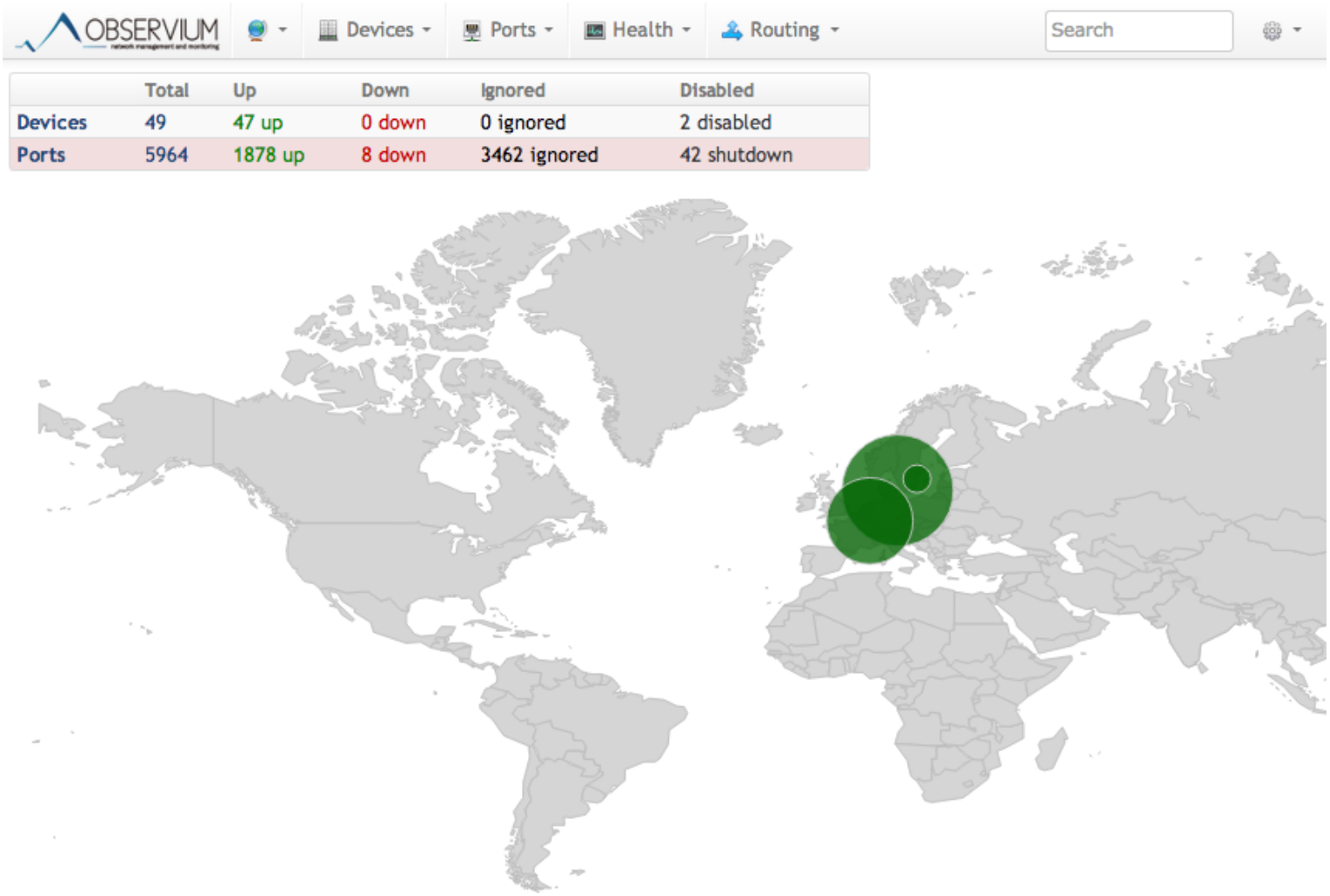
Recommened training Metasploit Unleashed
`http://www.offensive-security.com/metasploit-unleashed/Main_Page`

Defense: Attack overview



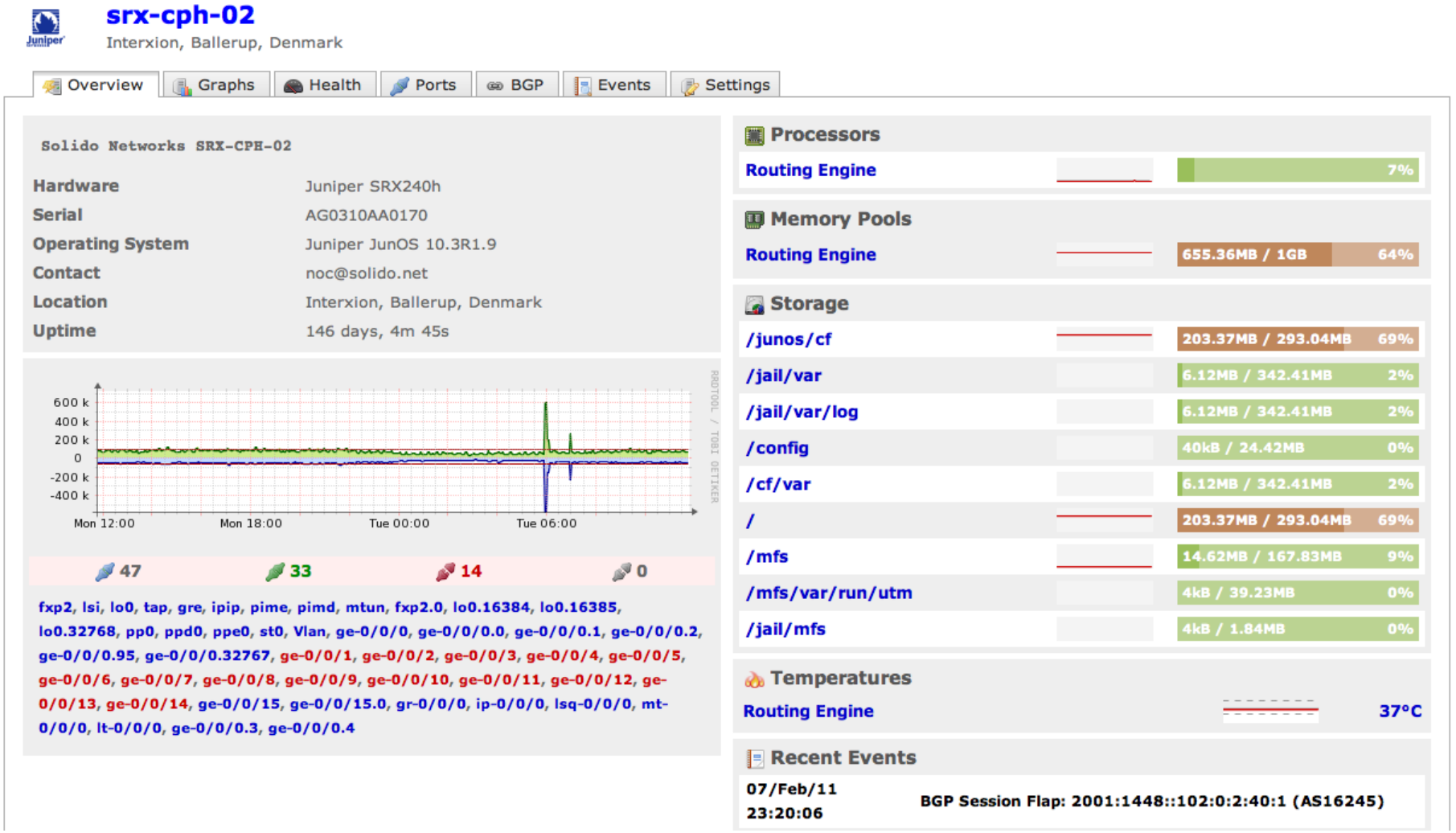
http://www.sicherheitstacho.eu/?lang=en

Graphs and Dashboards!



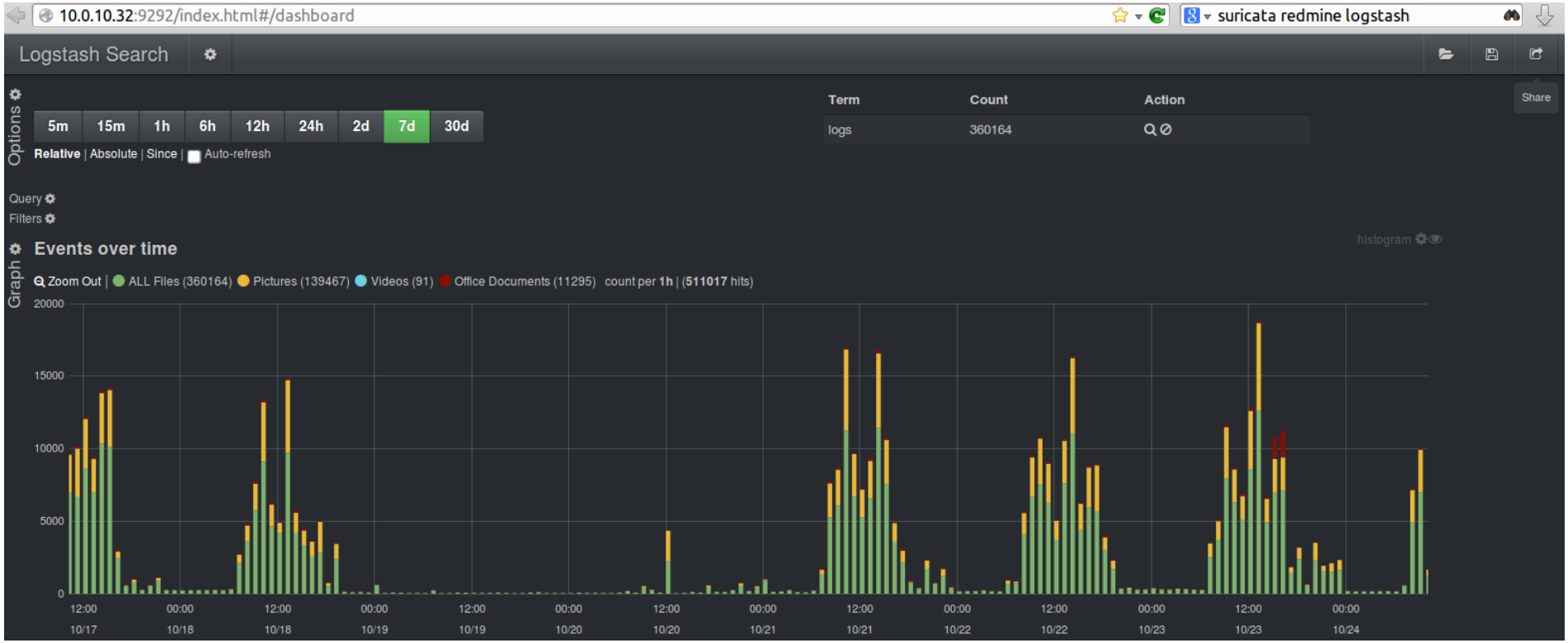
Observium

Observium example router overview



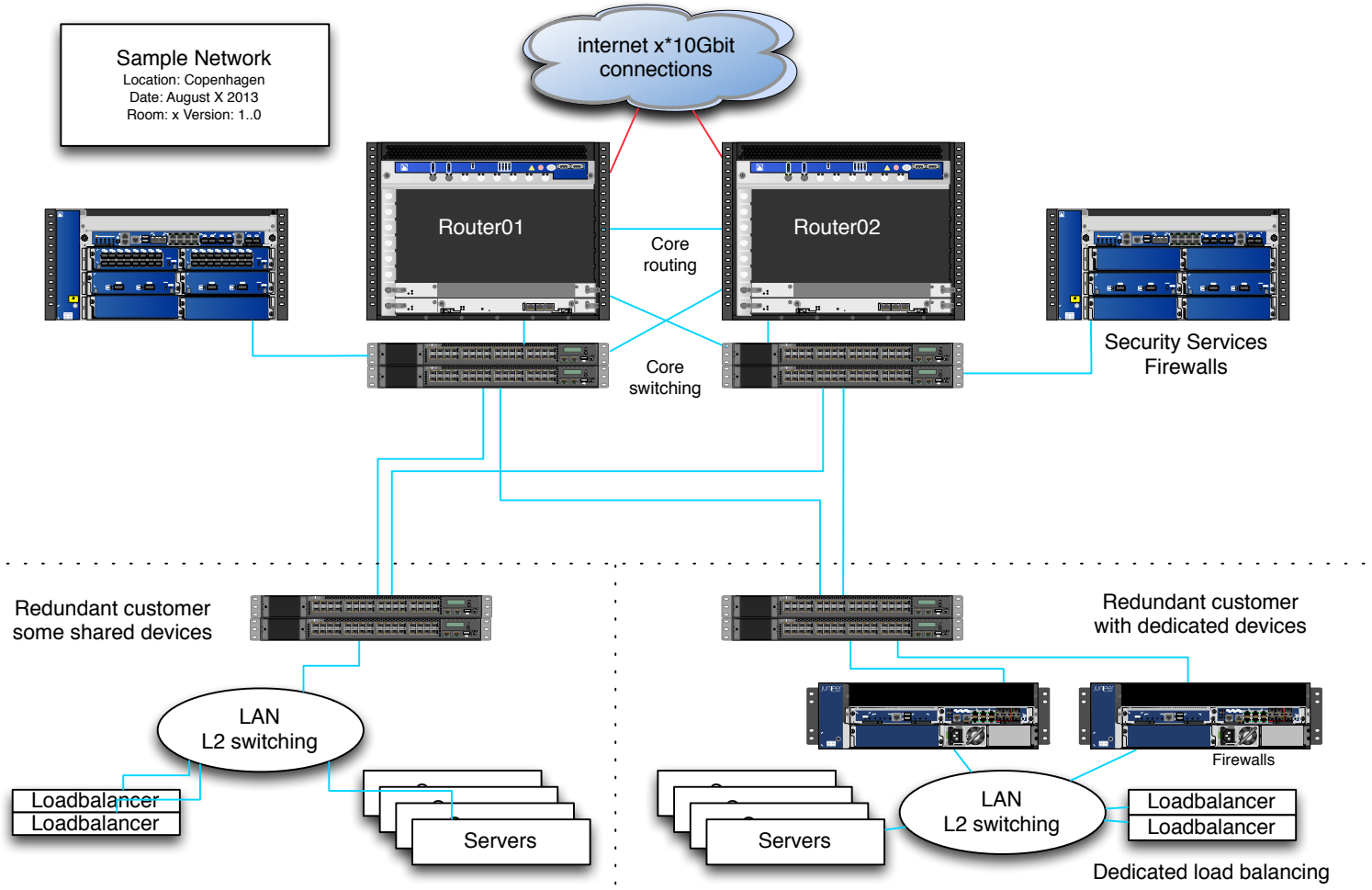
More useful information than default vendor interface! (flash)

Graphs and Dashboards!

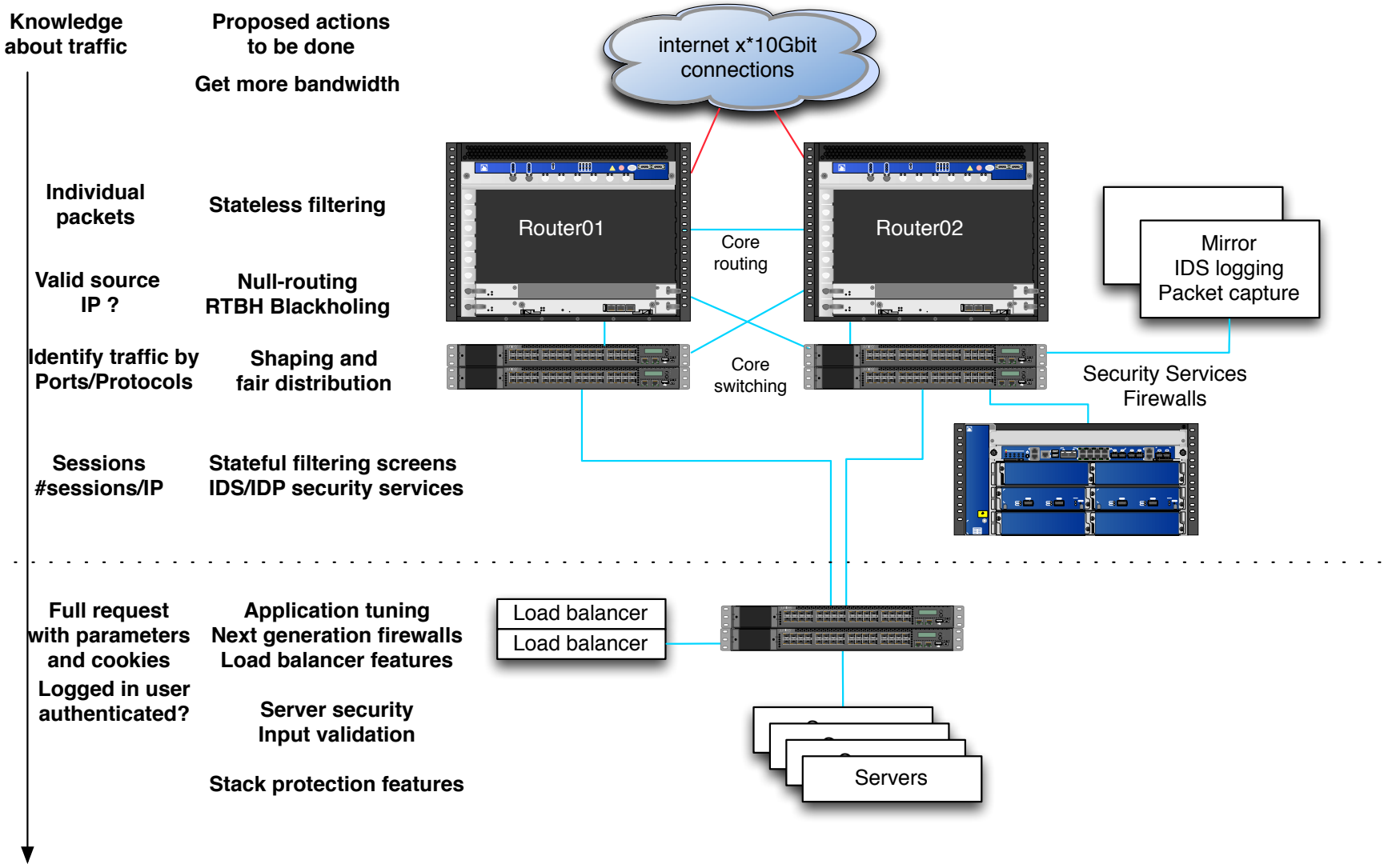


- Screenshot from Peter Manev, OISF
- Shown are Suricata IDS alerts processed by Logstash and Kibana

Networks today



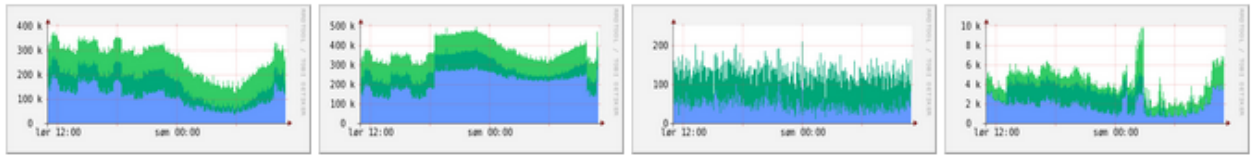
Defense in depth - multiple layers of security



Netflow NFSen

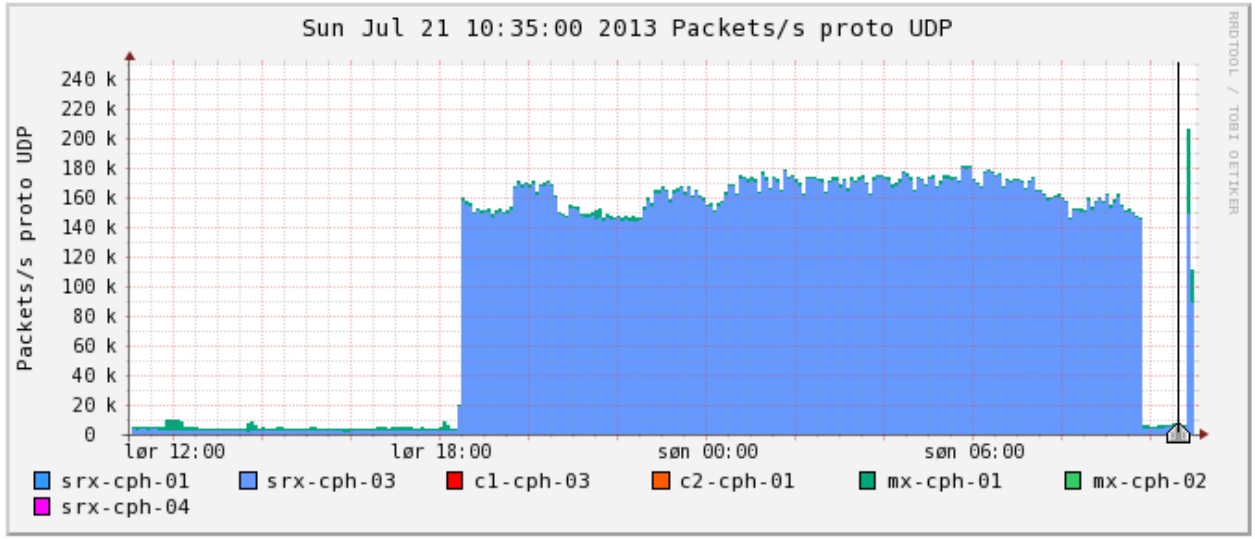
Profile: live

TCP **any** **ICMP** **other**



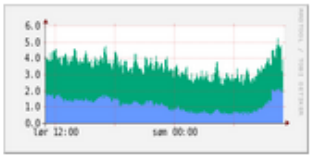
Profileinfo:

Type: live
Max: unlimited
Exp: never
Start: Jun 23 2011 - 13:10 CEST
End: Jul 21 2013 - 11:00 CEST



t_{start} **2013-07-21-10-35**
t_{end} **2013-07-21-10-35**

Flows



Traffic

Select [Single Timeslot] Display: [1 day] << < | ^ > >> >|

(•) Lin Scale (•) Stacked Graph
( ) Log Scale ( ) Line Graph

An extra 100k packets per second from this netflow source (source is a router)

How to get started

How to get started searching for security events?

Collect basic data from your devices and networks

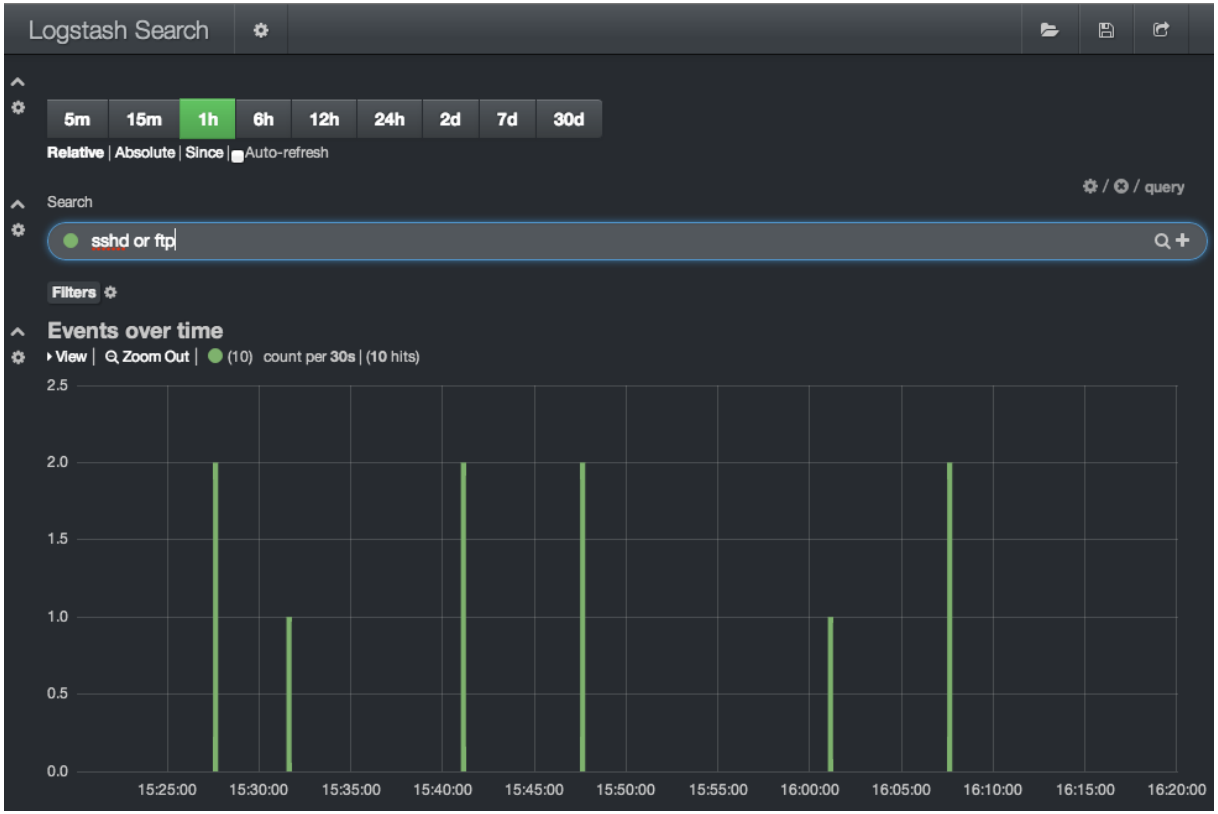
- Netflow data from routers
- Session data from firewalls
- Logging from applications: email, web, proxy systems

Centralize!

Process data

- Top 10: interesting due to high frequency, occurs often, brute-force attacks
- *ignore*
- Bottom 10: least-frequent messages are interesting

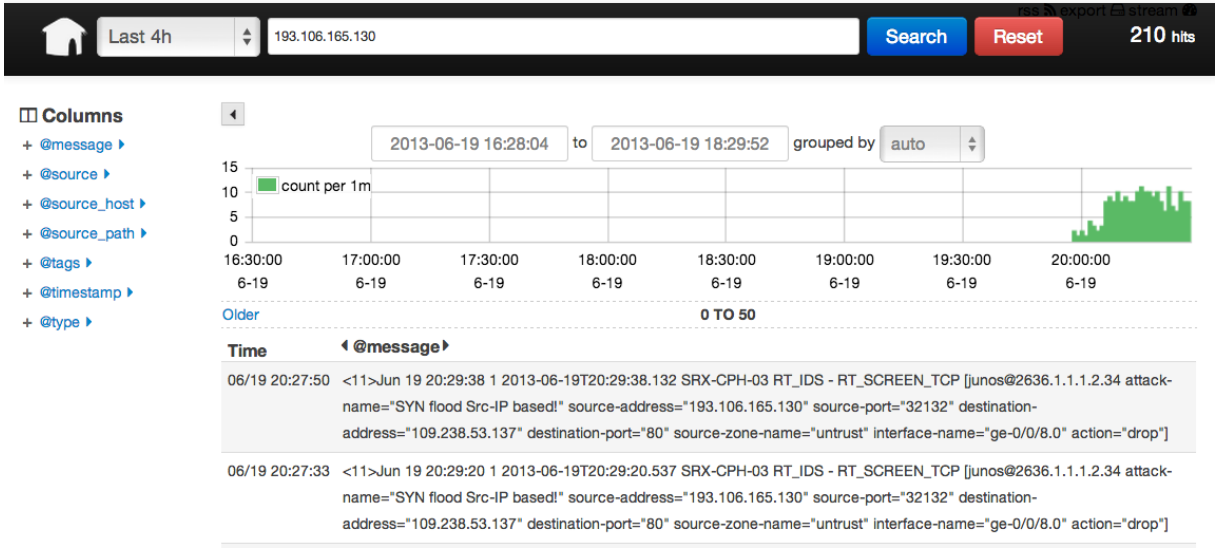
View data efficiently



View data by digging into it easily - must be fast

Logstash and Kibana are just examples, but use indexing to make it fast!

Network tools - examples



Net: Bro `http://www.bro-ids.org` Suricata `http://suricata-ids.org`

DNS: DSC and PacketQ `https://github.com/dotse/packetq/wiki`

Syslog: Elasticsearch, Logstash, and Kibana

Packetbeat `https://www.elastic.co/products/beats/packetbeat`

Collect and present data more easily - non-programmers

Security devops

We need devops skillz in security - automate, security is also big data

integrate tools, transfer, sort, search, pattern matching, statistics, ...

tools, languages, databases, protocols, data formats

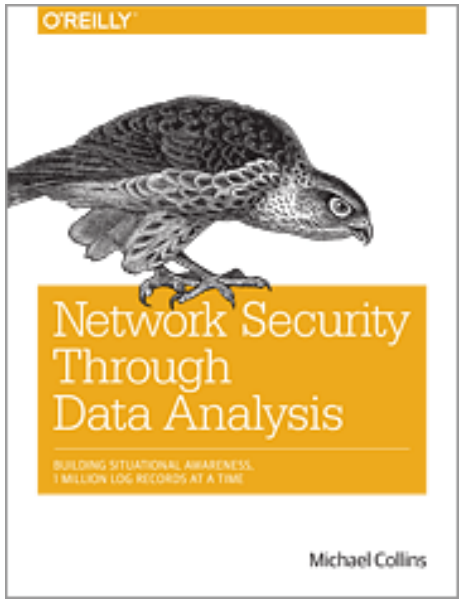
Example introductions:

- Seven languages/database/web frameworks in Seven Weeks
- Elasticsearch the definitive guide
  `http://www.elastic.co/guide/en/elasticsearch/guide/current/index.html`
- `https://www.elastic.co/products/kibana`
- `https://www.elastic.co/products/logstash`

We are all Devops now, even security people!

Do you even Github? ☺`https://github.com/stars`

Network Security Through Data Analysis



Low page count, but high value! Recommended.

Network Security Through Data Analysis: Building Situational Awareness
By Michael Collins
Publisher: O'Reilly Media Released: February 2014 Pages: 348

BRO IDS

The Bro Network Security Monitor

Bro is a powerful network analysis framework that is much different from the typical IDS you may know.

While focusing on network security monitoring, Bro provides a comprehensive platform for more general network traffic analysis as well. Well grounded in more than 15 years of research, Bro has successfully bridged the traditional gap between academia and operations since its inception.

`https://www.bro.org/`

BRO more than an IDS

> The key point that helped me understand was the explanation that Bro is a domain-specific language for networking applications and that Bro-IDS (http://bro-ids.org/) is an application written with Bro.

Why I think you should try Bro

`https://isc.sans.edu/diary.html?storyid=15259`

Bro scripts


```
global dns_A_reply_count=0;
global dns_AAAA_reply_count=0;
...
event dns_A_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr)
{
++dns_A_reply_count;
}

event dns_AAAA_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr)
{
++dns_AAAA_reply_count;
}
```

Source: dns-fire-count.bro from

`https://github.com/LiamRandall/bro-scripts/tree/master/fire-scripts`

Example, Using tools similar to PacketQ

Using PacketQ

Let's have a practical look at how PacketQ works by trying to figure out what kind of DNS ANY queries are being sent towards our name-server.

DNS ANY traffic is currently commonly abused for DNS amplification attacks (See Blog post "DDoS-Angriffe durch Reflektierende DNS-Amplifikation vermeiden" in German). The first thing I want to know is what are the IP addresses of the victims of this potential DNS amplification attack:

```
packetq -t -s "select src_addr,count(*) as count from dns where qtype=255 group
by src_addr order by count desc limit 3" lolo.20130118.070000.000179
"src_addr" ,"count"
"216.245.221.243",933825
"85.126.233.70" ,16802
"80.74.130.55" ,91
```

Are you using your brain and existing tools? Building own specialised tools? Discussion: bridging the gaps between Devops and Security? Good thing, easy?

http://securityblog.switch.ch/2013/01/22/using-packetq/

http://jpmens.net/2013/05/27/server-agnostic-logging-of-dns-queries-responses/

Storing query logs, old school or needed?

- policy/protocols/ssl/expiring-certs.bro
- policy/protocols/ssl/extract-certs-pem.bro
- policy/protocols/ssl/heartbleed.bro
- policy/protocols/ssl/known-certs.bro
- policy/protocols/ssl/log-hostcerts-only.bro
- policy/protocols/ssl/validate-certs.bro
- policy/protocols/ssl/validate-ocsp.bro
- policy/protocols/ssl/weak-keys.bro

Looking at DNS PacketQ it was an Older link, but thinking the time is now for doing:

- DNS query logs, keep it for at least a week? - with DSC and PacketQ
- SSL/TLS full logs over sessions, certs, keys - with Bro/Suricata
  `https://www.bro.org/sphinx-git/script-reference/scripts.html`
- Log and search with Elasticsearch?
  `https://www.elastic.co/guide/en/elasticsearch/guide/current/index.html`
- Even netflow session logging, full 1:1 - NFSen, Suricata Flow mode?

February 2015: Finding infected sources

”We were contacted by a client to help with their incident response in tracking down an infection on a clients machine with the new CTB-Locker ransomware (Curve-Tor-Bitcoin Locker) aka Critroni which had no signatures available at the time of infection for this variant.

LANGuardian includes a file share activity monitoring module which provided a very detailed forensic analysis of the ransomware and the paths it had taken in order to encrypt the clients system and also the fileserver in which it was connected to, the initial infection came from the opening of an attachment in an e-mail.”

It has become critical to identify vulnerable or infected ASAP!

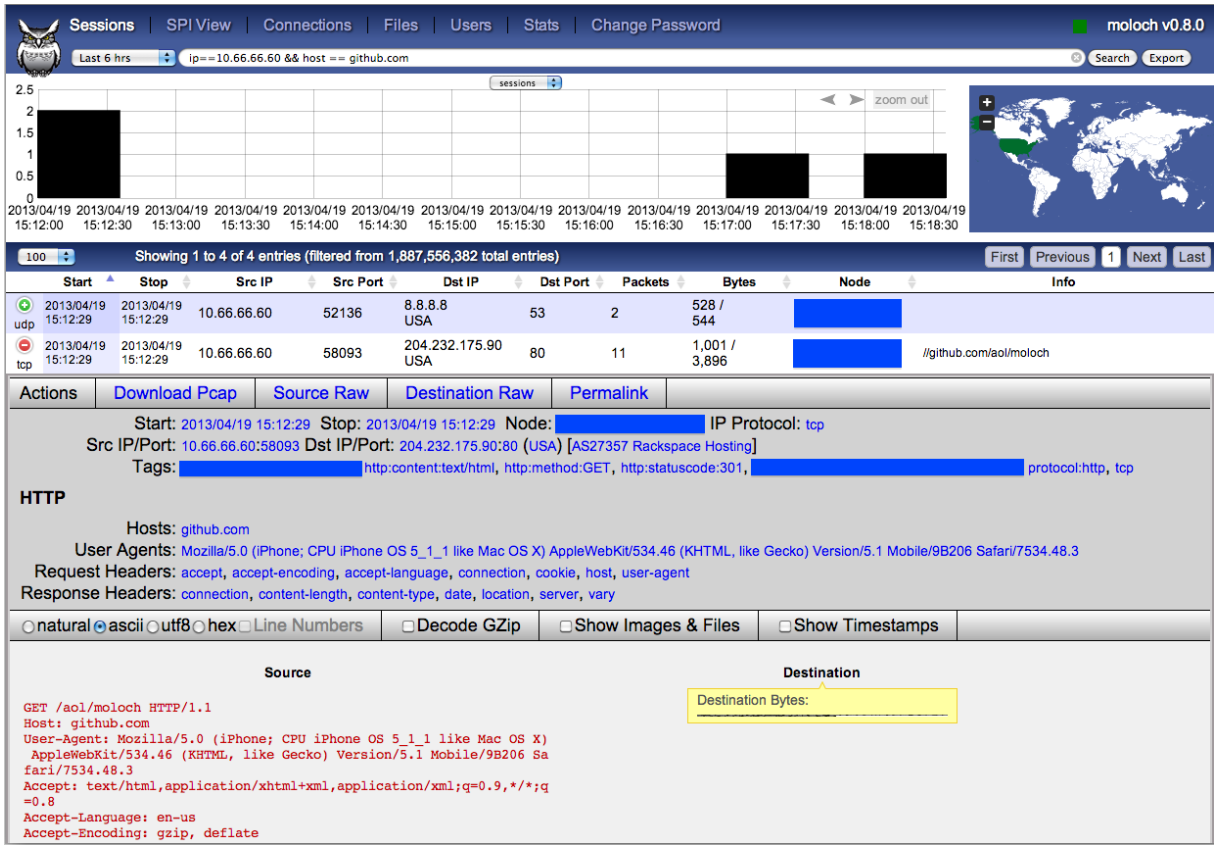
Source: `https://www.netfort.com/support-team-stories-detecting-the-source-of-ransomware/`

Security Onion

- Security Onion is a Linux distro for IDS, NSM, and log management
- Learn NSM with Security Onion today - its free

Nice starting point for researching dashboards/network packets

Moloch



Picture from `https://github.com/aol/moloch`

Suricata with Dashboards

Picture from Twitter

https://twitter.com/nullthreat/status/445969209840128000

New link March 2014: 10Gbits

http://pevma.blogspot.se/2014/03/suricata-prepearing-10gbps-network.html

http://suricata-ids.org/2014/03/25/suricata-2-0-available/

Big Data tools: Elasticsearch

elasticsearch

the definitive guide

clinton gormley zachary tong Copyright © 2014 Elasticsearch

`http://www.elasticsearch.org/guide/en/elasticsearch/guide/current/index.html`

`http://www.elasticsearch.org/overview/kibana/`

`http://www.elasticsearch.org/overview/logstash/`

We are all Devops now, even security people!

Ansible configuration management


```
- apt: name= item  state=latest
  with_items:
        - unzip
        - elasticsearch
        - logstash
        - redis-server
        - nginx
- lineinfile: "dest=/etc/elasticsearch/elasticsearch.yml state=present
  regexp='script.disable_dynamic: true' line='script.disable_dynamic: true'"
- lineinfile: "dest=/etc/elasticsearch/elasticsearch.yml state=present
  regexp='network.host: localhost' line='network.host: localhost'"
- name: Move elasticsearch data into /data
  command: creates=/data/elasticsearch mv /var/lib/elasticsearch /data/
- name: Make link to /data/elasticsearch
  file: state=link src=/data/elasticsearch path=/var/lib/elasticsearch
```

only requires SSH+python `http://www.ansible.com`

Kibana 4 february 2015

Highly recommended for a lot of data visualisation

Non-programmers can create, save, and share dashboards

Source: `https://www.elastic.co/products/kibana`

Next steps

In our network we are always improving things:

Suricata IDS `http://www.openinfosecfoundation.org/`

More graphs, with **automatic identification** of IPs under attack

Identification of **short sessions without data** - spoofed addresses

Alerting from **existing** devices

Dashboards with key measurements

Conclusion: Combine tools!

Lets get to work!

- Get Kibana working
- Get access to Kibana
- Produce some data
- Create dashboards

While demoing Ansible, and vagrant

Lots of examples
`https://github.com/geerlingguy/ansible-vagrant-examples/`

Grok expresssions

og vise hvordan man kan lave sine egne Grok expressions til at splitte loglinier til felter.

Questions?

Henrik Lund Kramshøj hlk@kramse.org

THECAMP.DK - 7 open source days