Welcome to

IT-sikkerhed 2015

PROSA Superhelteseminar

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

Slides are available as PDF, kramshoej@Github

Goals of today

How to become a super hero at work

Offer input to what things to look into

Hodge-podge of security related things - inspiration

Please give feedback and join me in discussions, dialogue ☺

Plan for today

Kl 17:30-19:30 with a break

Less presentation, more talk

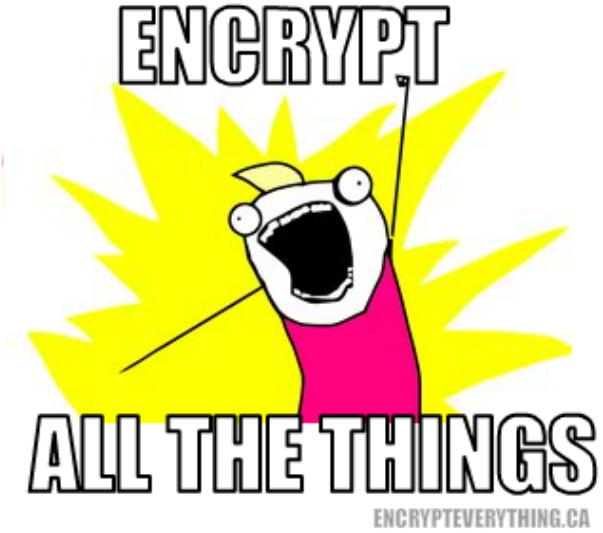
Less me talking (only) and more 2.0 social media interaction

Trying to fit in demo and workshop-like stuff

Generic advice

SOLIDO NETWORKS

Recommendations



- Lock your devices, phones, tables and computers
- Update software and apps
- Do NOT use the same password everywhere
- Watch out when using open wifi-networks
- Multiple browsers: one for Facebook, one for banking apps?
- Multiple laptops? One for private data, one for work?
- Think of the data you produce - where is it stored
- Use pseudonyms and aliases, do not use your real name everywhere
- Enable encryption: IMAP**S**, POP3**S**, HTTP**S** and full disk encryption
- Use Tor `http://torproject.org/`

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

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

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

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 kneep 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

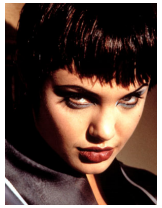
Latest backup from November (currently we are in April!)

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://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/`

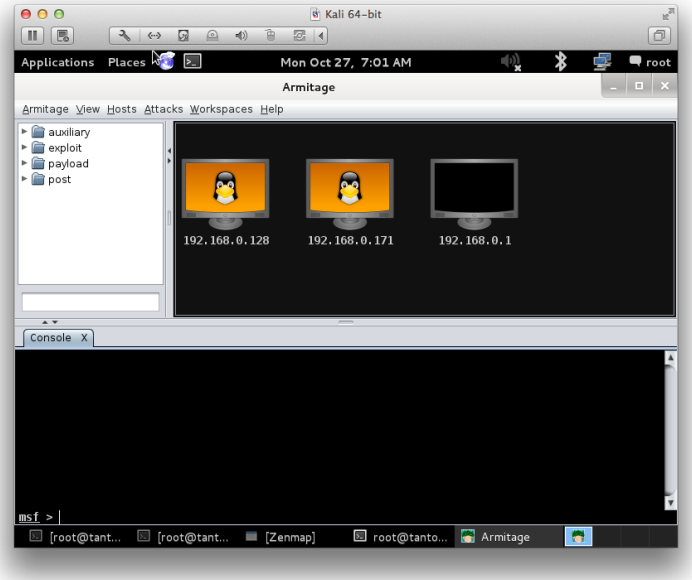
Kali Linux the pentest toolbox

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

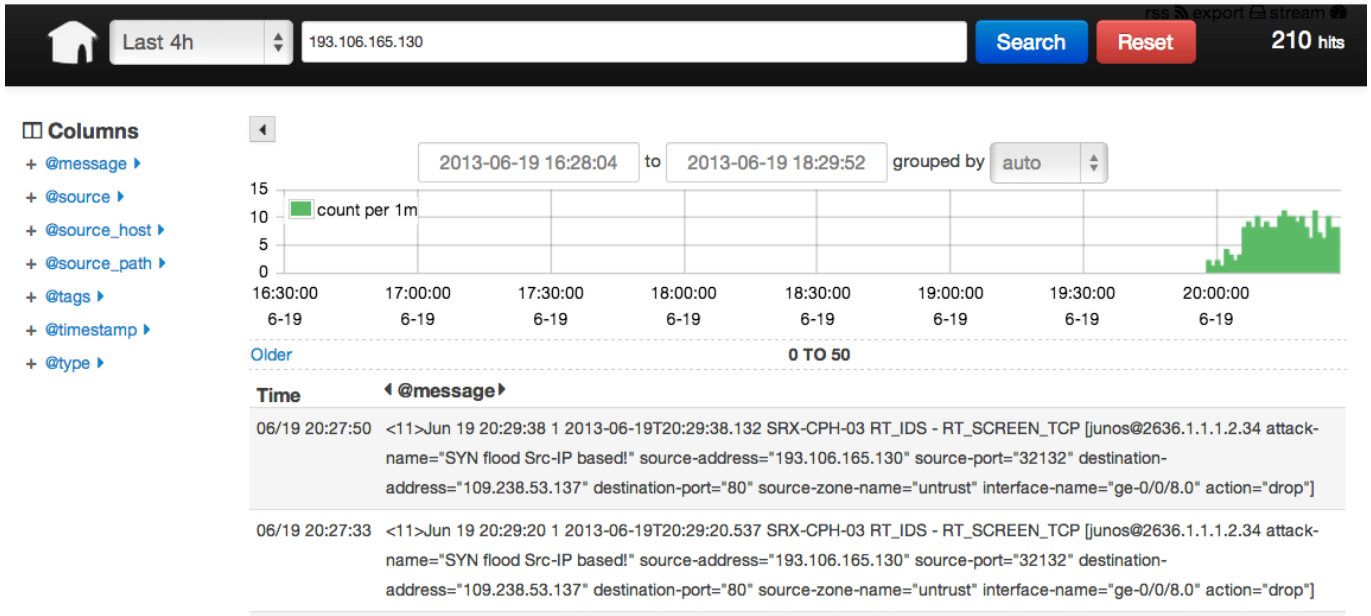


http://www.metasploit.com/

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

Kursus Metasploit Unleashed
http://www.offensive-security.com/metasploit-unleashed/Main_Page

Big data 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

Collect and present data more easily - non-programmers

Security devops

SOLIDO NETWORKS

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

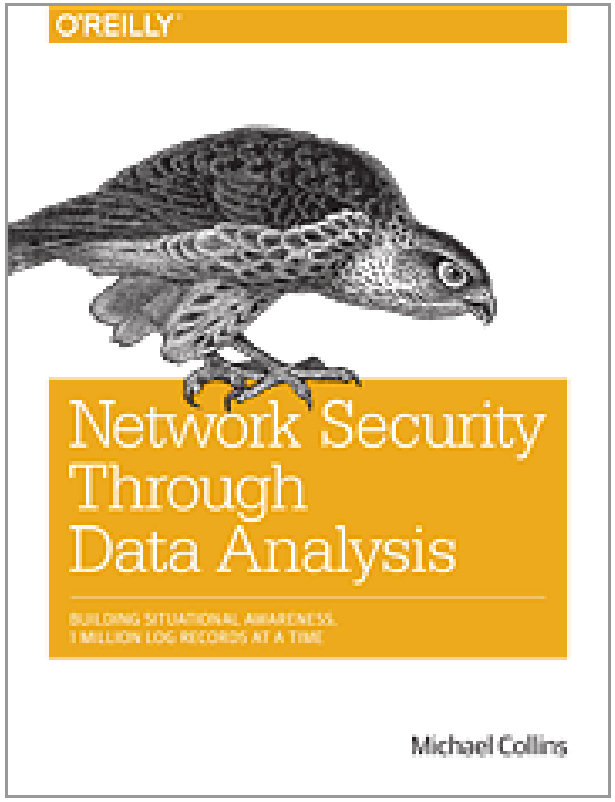
Example introductions:

- 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

SOLIDO NETWORKS

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.

`http://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

Security Onion

- Security Onion is a Linux distro for IDS, NSM, and log management
- `http://securityonion.blogspot.dk`
- `http://blog.securityonion.net/p/securityonion.html`

Nice starting point for researching dashboards/network packets

February and March 2015, Security Onion updates

SOLIDO NETWORKS

- Security Onion 12.04.5.1 ISO image now available
- Suricata IDS engine 2.0.7 updated packages for SO released
- Learn NSM with Security Onion today - its free

http://blog.securityonion.net/2015/03/suricata-207.html
http://blog.securityonion.net/2015/02/security-onion-120451-iso-image-now.html

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/blob/master/elk/Vagrantfile

Questions?

SOLIDO NETWORKS

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

You are always welcome to send me questions later via email

Did you notice how a lot of the links in this presentation use HTTPS - encrypted