Welcome to

Heartbleed bug

Netværket om Procesorienteret IT-sikkerhed

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

`http://www.solidonetworks.com`

In part based on

`http://www.version2.dk/blog/openssl-er-doed-laenge-leve-libressl-57640`

`http://www.version2.dk/blog/opdater-openssl-og-dit-os-nu-57202`

Planen idag

Don’t Panic!

Kl 13:00-14:45 - med pause

Mindre enetale, mere foredrag 2.0 med sociale medier, informationsdeling og interaktion

Send gerne spørgsmål senere

The current situation

Internet security sucks

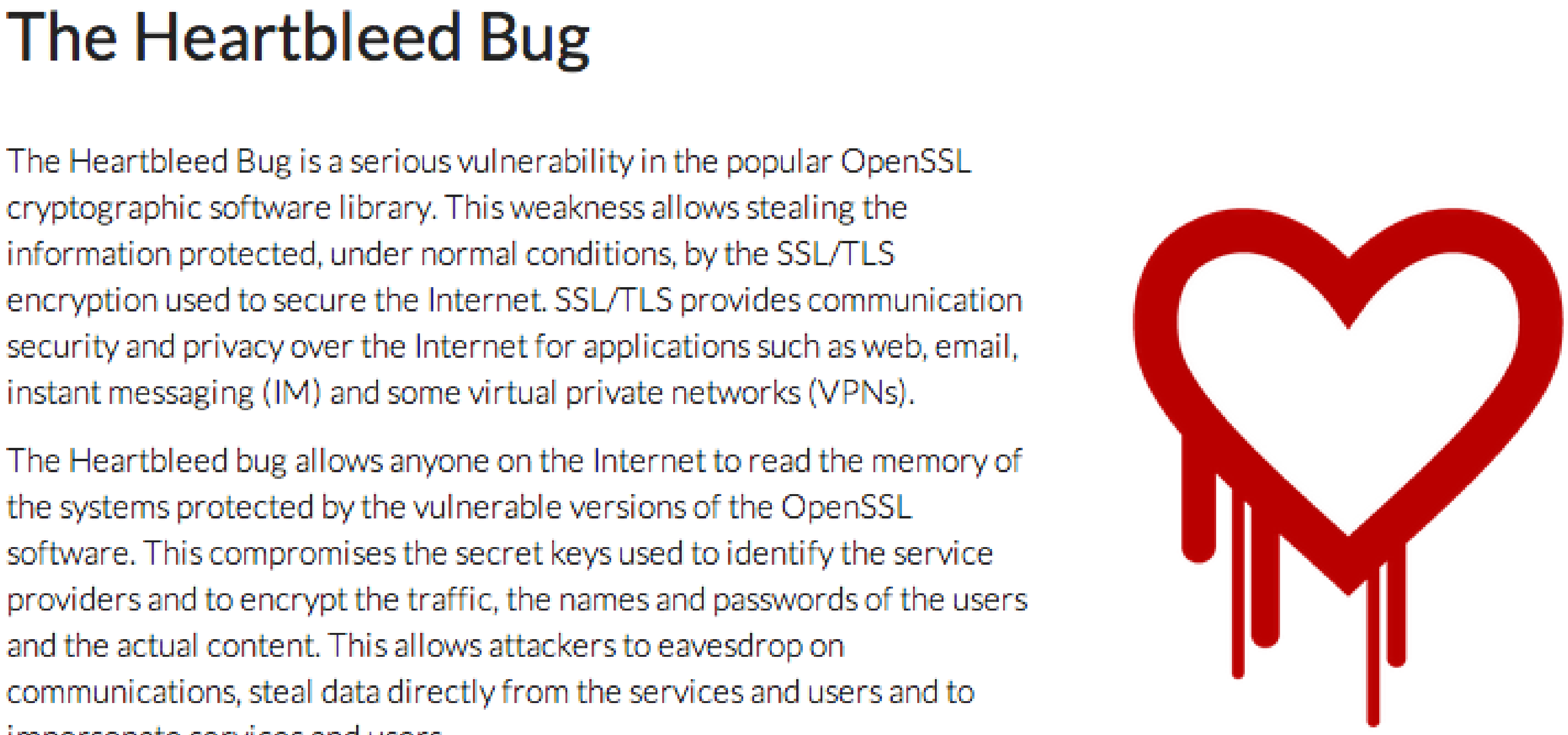
We depend on cloud services and underfunded infrastructure - OpenSSL

We depend on others and the whole internet - DDoS

Personal computers like laptops suck at security

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

Heartbleed CVE-2014-0160



The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

Source: `http://heartbleed.com/`

Heartbleed is yet another bug in SSL products

```
What versions of the OpenSSL are affected?
Status of different versions:

* OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
* OpenSSL 1.0.1g is NOT vulnerable
* OpenSSL 1.0.0 branch is NOT vulnerable
* OpenSSL 0.9.8 branch is NOT vulnerable

Bug was introduced to OpenSSL in December 2011 and has been out
in the wild since OpenSSL release 1.0.1 on 14th of March
2012. OpenSSL 1.0.1g released on 7th of April 2014 fixes the bug.
```

It’s just a bug - but a serious one

Why is heartbleed different?

Great PR, name, web site, logo

OpenSSL is very widespread

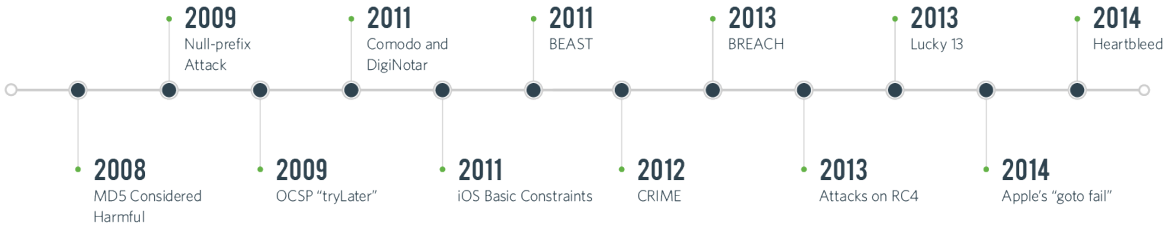
OpenSSL has been criticized before

The spotlight is now on a lot of products, infrastructure

BOTH Open Source products and Proprietary products hurt by this

TL;DR
OpenSSL is everywhere and an example of our dependency on weak components

Key points after heartbleed



Source: picture source

`https://www.duosecurity.com/blog/heartbleed-defense-in-depth-part-2`

- Writing SSL software and other secure crypto software is hard
- Configuring SSL is hard
  check you own site `https://www.ssllabs.com/ssltest/`
- SSL is hard, finding bugs "all the time" `http://armoredbarista.blogspot.dk/2013/01/a-brief-chronology-of-ssltls-attacks.html`
- Rekeying is hard - slow, error prone, manual proces - Automate!
- Proof of concept programs exist - god or bad?

Proof of concept programs exist - god or bad?

Some of the tools released shortly after Heartbleed announcement

- `https://github.com/FiloSottile/Heartbleed` tool i Go site `http://filippo.io/Heartbleed/`
- `https://github.com/titanous/heartbleeder` tool i Go
- `http://s3.jspenguin.org/ssltest.py` PoC
- `https://gist.github.com/takeshixx/10107280` test tool med STARTTLS support
- `http://possible.lv/tools/hb/` test site
- `https://twitter.com/richinseattle/status/453717235379355649` Practical Heartbleed attack against session keys links til, `https://www.mattslifebytes.com/?p=533` og "Fully automated here " `https://www.michael-p-davis.com/using-heartbleed-for-hijacking-user-sessio`
- Metasploit er også opdateret på master repo `https://twitter.com/firefart/status/453758091658792960` `https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliar` `scanner/ssl/openssl_heartbleed.rb`

Security is magic

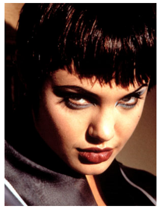
.

Think security always appropriate paranoia

Follow news about software security

Support communties, join and learn

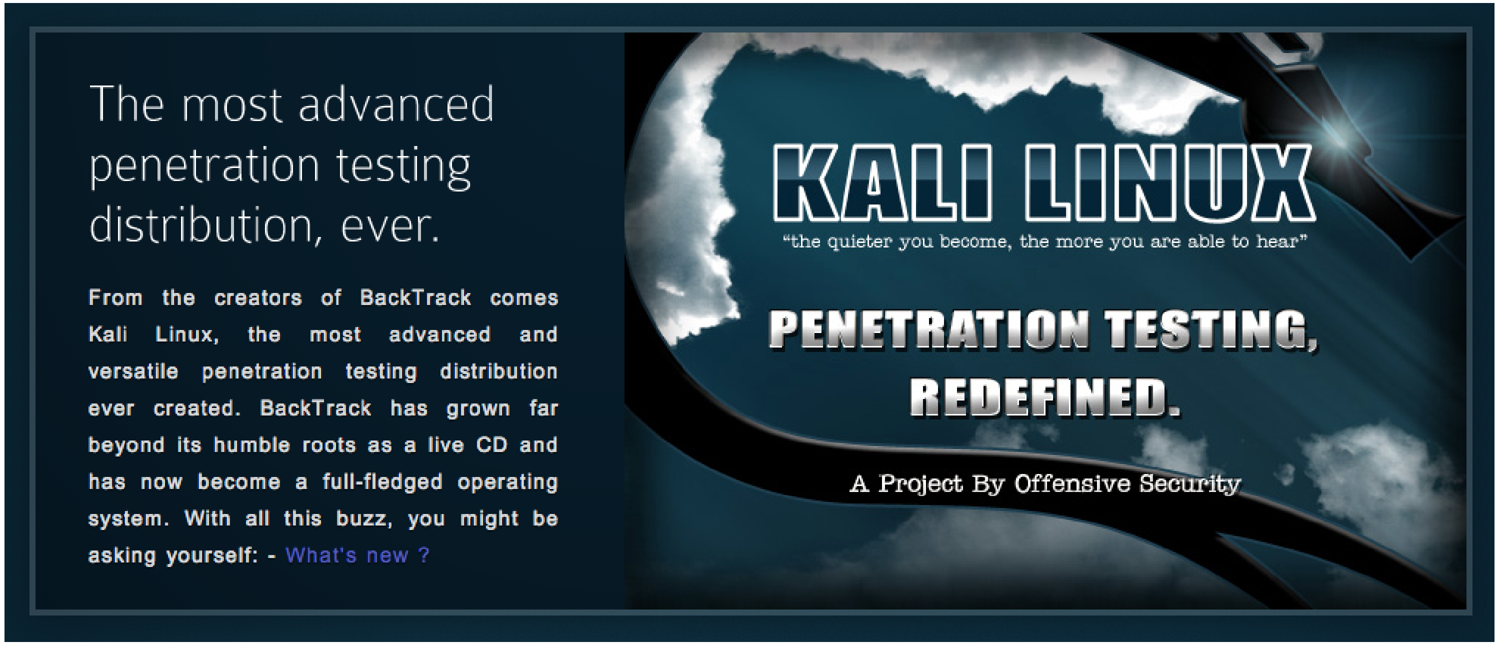
Hackerværktøjer er også til dig!



- 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 new backtrack



The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - What's new ?

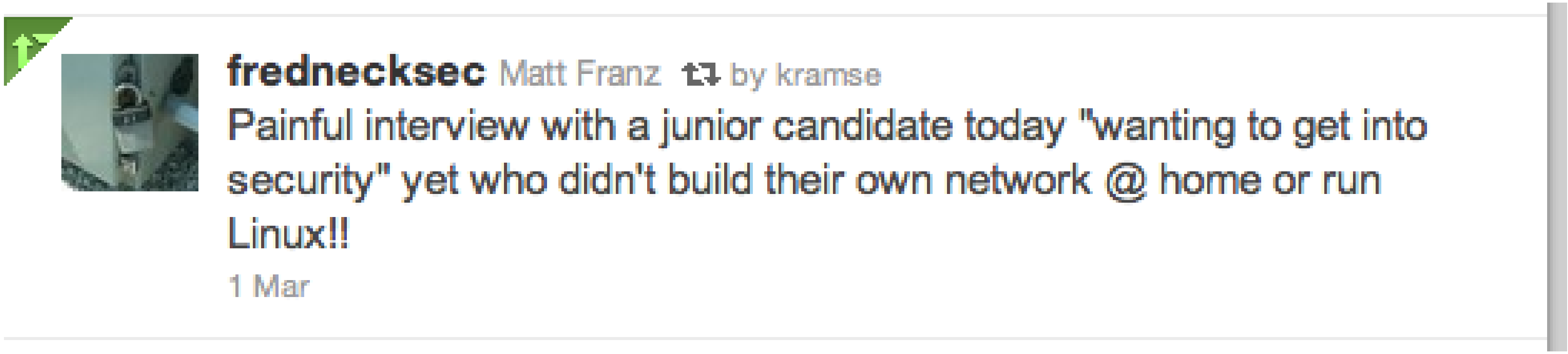
KALI LINUX
"the quieter you become, the more you are able to hear"
PENETRATION TESTING, REDEFINED.
A Project By Offensive Security

BackTrack `http://www.backtrack-linux.org`

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

100.000s of videos on youtube: "kali hack" 60.000, "backtrack hack" 125.000

it’s a Unix system, I know this



fredneckssec Matt Franz ⇄ by kramse

Painful interview with a junior candidate today "wanting to get into security" yet who didn't build their own network @ home or run Linux!!

1 Mar

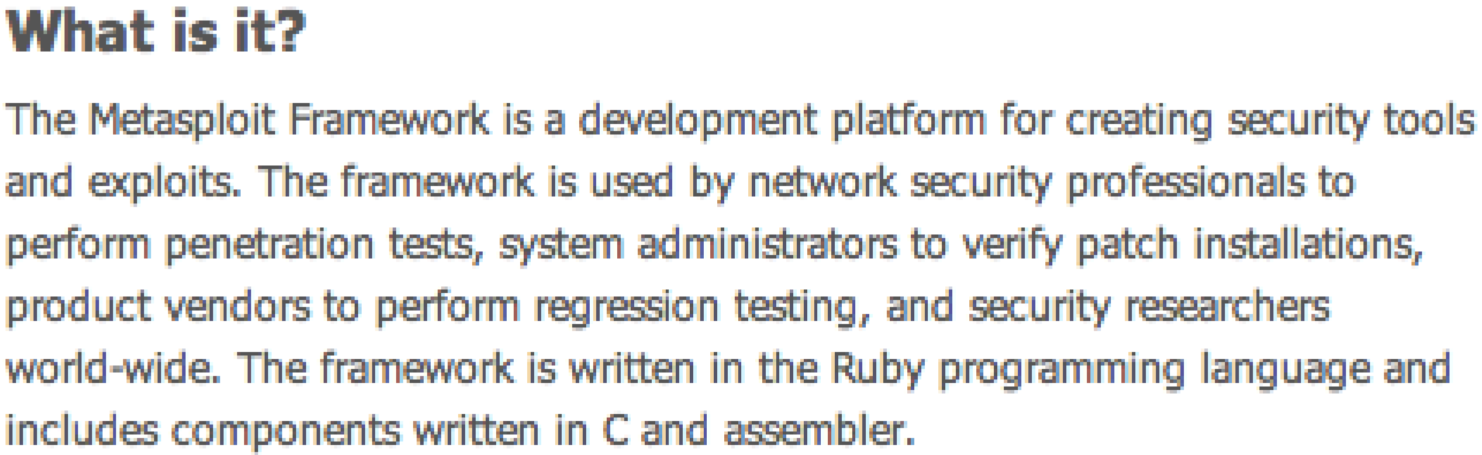
Skal du igang med sikkerhed?

Installer et netværk, evt. bare en VMware, Virtualbox, Parallels, Xen, GNS3, ...

Brug BackTrack, se evt. youtube videoer om programmerne

Quote fra Jurassic Park `http://www.youtube.com/watch?v=dFUlAQZB9Ng`

Metasploit and Armitage Still rocking the internet



What is it?

The Metasploit Framework is a development platform for creating security tools and exploits. The framework is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers world-wide. The framework is written in the Ruby programming language and includes components written in C and assembler.

`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`

Bog: Metasploit: The Penetration Tester's Guide, No Starch Press
ISBN-10: 159327288X

Fri adgang til hackerværktøjer

I 1993 skrev Dan Farmer og Wietse Venema artiklen
Improving the Security of Your Site by Breaking Into it

I 1995 udgav de softwarepakken SATAN
Security Administrator Tool for Analyzing Networks

> We realize that SATAN is a two-edged sword - like many tools, it can be used for good and for evil purposes. We also realize that intruders (including wannabees) have much more capable (read intrusive) tools than offered with SATAN.

Se `http://sectools.org` og `http://www.packetstormsecurity.org/`

Kilde: `http://www.fish2.com/security/admin-guide-to-cracking.html`

Heartbleed hacking

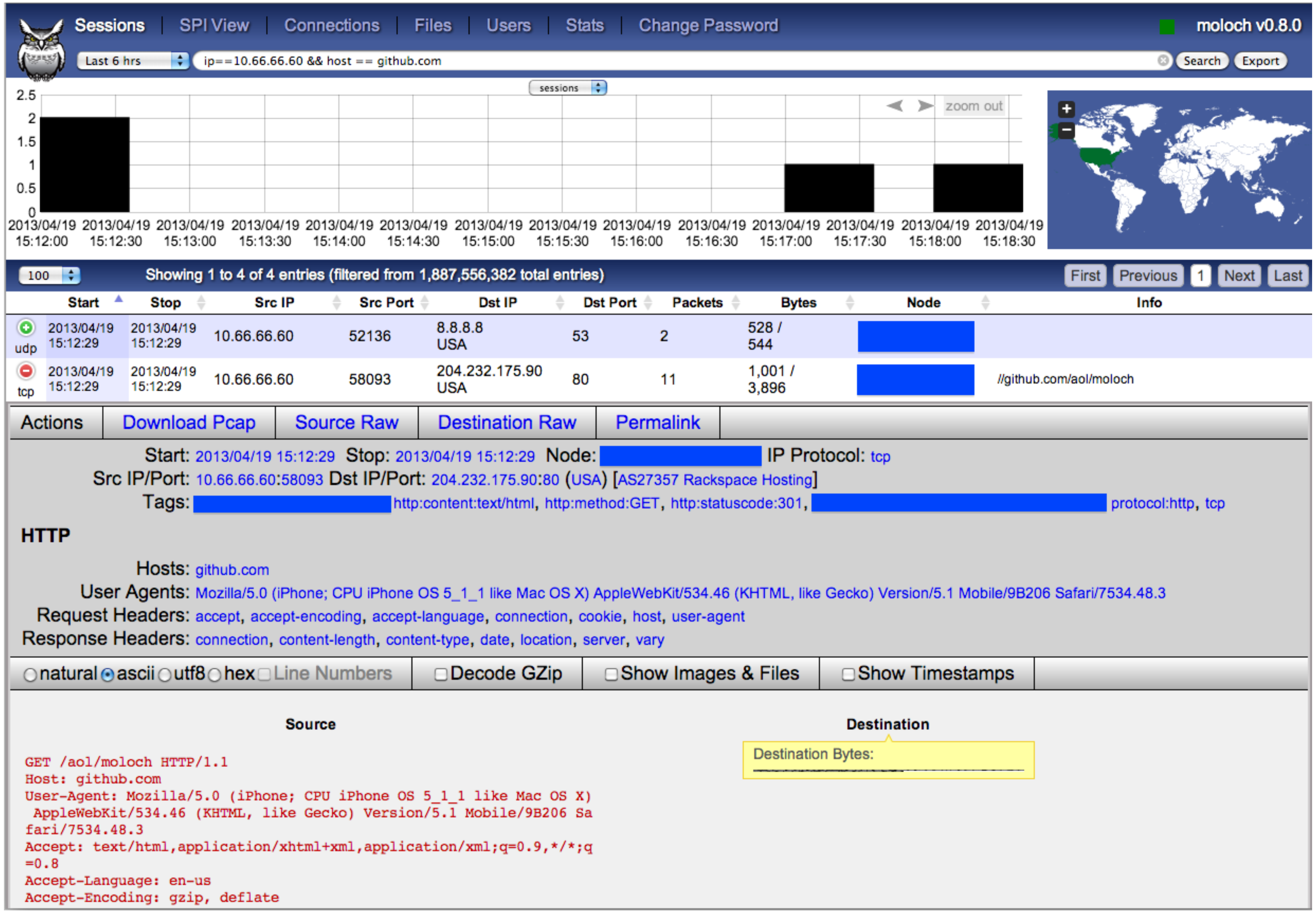
```
06b0: 2D 63 61 63 68 65 0D 0A 43 61 63 68 65 2D 43 6F  -cache..Cache-Co
06c0: 6E 74 72 6F 6C 3A 20 6E 6F 2D 63 61 63 68 65 0D  ntrol: no-cache.
06d0: 0A 0D 0A 61 63 74 69 6F 6E 3D 67 63 5F 69 6E 73  ...action=gc_ins
06e0: 65 72 74 5F 6F 72 64 65 72 26 62 69 6C 6C 6E 6F  ert_order&billno
06f0: 3D 50 5A 4B 31 31 30 31 26 70 61 79 6D 65 6E 74  =PZK1101&payment
0700: 5F 69 64 3D 31 26 63 61 72 64 5F 6E 75 6D 62 65  _id=1& card˙numbe
0710: XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX   r=4060xxxx413xxx
0720: 39 36 26 63 61 72 64 5F 65 78 70 5F 6D 6F 6E 74   96&card˙exp˙mont
0730: 68 3D 30 32 26 63 61 72 64 5F 65 78 70 5F 79 65   h=02&card˙exp˙ye
0740: 61 72 3D 31 37 26 63 61 72 64 5F 63 76 6E 3D 31   ar=17&card˙cvn=1
0750: 30 39 F8 6C 1B E5 72 CA 61 4D 06 4E B3 54 BC DA   09.l..r.aM.N.T..
```

- Obtained using Heartbleed proof of concepts - Gave full credit card details
- ”can XXX be exploited” - yes, clearly! PoCs ARE needed
  without PoCs even Akamai wouldn’t have repaired completely!
- The internet was ALMOST fooled into thinking getting private keys
  from Heartbleed was not possible - scary indeed.

Analysis of the heartbleed bug

- analyse af problemet i koden `http://blog.existentialize.com/diagnosis-of-the-openssl-heartbleed-bug.html`
- IDS regler Detecting OpenSSL Heartbleed with Suricata `http://blog.inliniac.net/2014/04/08/detecting-openssl-heartbleed-with-suric`
- god beskrivelse af hvordan man kan fixe hurtigere hvis man har automatiseret infrastruktur `https://www.getpantheon.com/heartbleed-fix`
- Mange blogindlæg om emnet - eksempelvis `http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/`
- ”nse script ssl-heartbleed.nse committed to nmap as rev 32798. ”
- You can now use Masscan to scan the whole internet for the Hearbleed vulnerability in under 6 minutes `https://twitter.com/jedisct1/status/453679529710460928` og `https://github.com/robertdavidgraham/masscan/commit/23497c448b0a1c7058e84`

Moloch



ip==10.66.66.60 && host == github.com

Showing 1 to 4 of 4 entries (filtered from 1,887,556,382 total entries)

	Start	Stop	Src IP	Src Port	Dst IP	Dst Port	Packets	Bytes	Node	Info
udp	2013/04/19 15:12:29	2013/04/19 15:12:29	10.66.66.60	52136	8.8.8.8 USA	53	2	528 / 544	[redacted]	
tcp	2013/04/19 15:12:29	2013/04/19 15:12:29	10.66.66.60	58093	204.232.175.90 USA	80	11	1,001 / 3,896	[redacted]	//github.com/aol/moloch

Actions | Download Pcap | Source Raw | Destination Raw | Permalink

Start: 2013/04/19 15:12:29 Stop: 2013/04/19 15:12:29 Node: [redacted] IP Protocol: tcp
Src IP/Port: 10.66.66.60:58093 Dst IP/Port: 204.232.175.90:80 (USA) [AS27357 Rackspace Hosting]
Tags: [redacted] http:content:text/html, http:method:GET, http:statuscode:301, [redacted] protocol:http, tcp

HTTP

Hosts: github.com
User Agents: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3
Request Headers: accept, accept-encoding, accept-language, connection, cookie, host, user-agent
Response Headers: connection, content-length, content-type, date, location, server, vary

○natural ●ascii ○utf8 ○hex □Line Numbers | □Decode GZip | □Show Images & Files | □Show Timestamps

Source

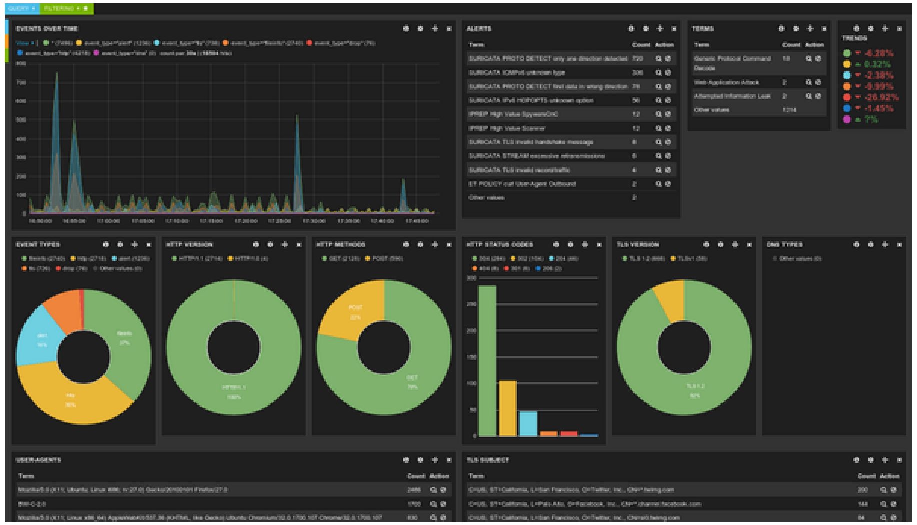
```
GET /aol/moloch HTTP/1.1
Host: github.com
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1_1 like Mac OS X)
 AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Sa
fari/7534.48.3
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q
=0.8
Accept-Language: en-us
Accept-Encoding: gzip, deflate
```

Destination

Destination Bytes:

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

Suricata with Dashboards



ALERTS

Term	Count	Action
SURICATA PROTO DETECT only one direction detected	720	
SURICATA ICMPv6 unknown type	308	
SURICATA PROTO DETECT first data in wrong direction	78	
SURICATA IPv6 HOPOPTS unknown option	56	
IPREP High Value SpywareCnC	12	
IPREP High Value Scanner	12	
SURICATA TLS invalid handshake message	8	
SURICATA STREAM excessive retransmissions	6	
SURICATA TLS invalid record/traffic	4	
ET POLICY curl User-Agent Outbound	2	
Other values	2	

TERMS

Term	Count	Action
Generic Protocol Command Decode	18	
Web Application Attack	2	
Attempted Information Leak	2	
Other values	1214	

USER-AGENTS

Term	Count	Action
Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:27.0) Gecko/20100101 Firefox/27.0	2486	
BW-C-2.0	1700	
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/32.0.1700.107 Chrome/32.0.1700.107	830	

TLS SUBJECT

Term	Count	Action
C=US, ST=California, L=San Francisco, O=Twitter, Inc., CN=*.twimg.com	200	
C=US, ST=California, L=Palo Alto, O=Facebook, Inc., CN=*.channel.facebook.com	144	
C=US, ST=California, L=San Francisco, O=Twitter, Inc., CN=si0.twimg.com	84	

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/`

Security devops

We need devops skillz in security

automate, security is also big data

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

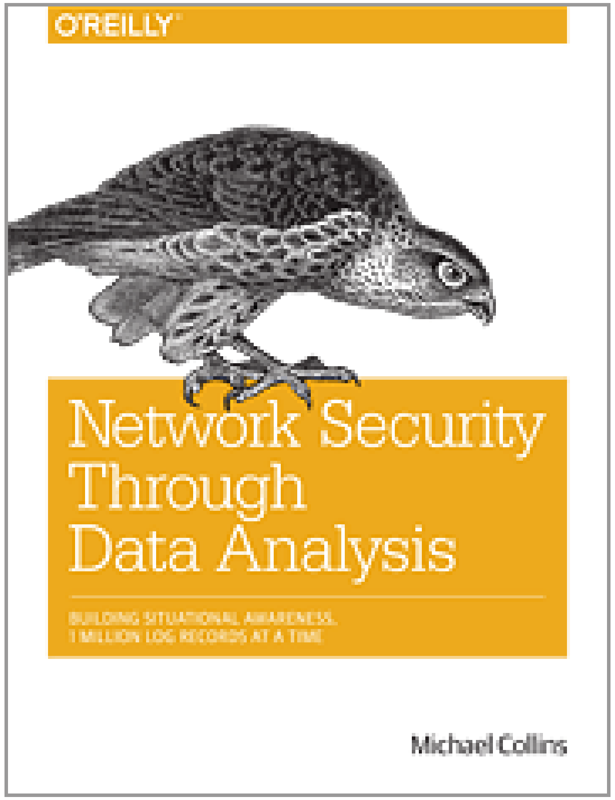
tools, languages, databases, protocols, data formats

Example introductions:

- Seven languages/database/web frameworks in Seven Weeks
- Elasticsearch the definitive guide `http://www.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!

Network Security Through Data Analysis


O'REILLY
Network Security Through Data Analysis
BUILDING SITUATIONAL AWARENESS, 1 MILLION LOG RECORDS AT A TIME
Michael Collins

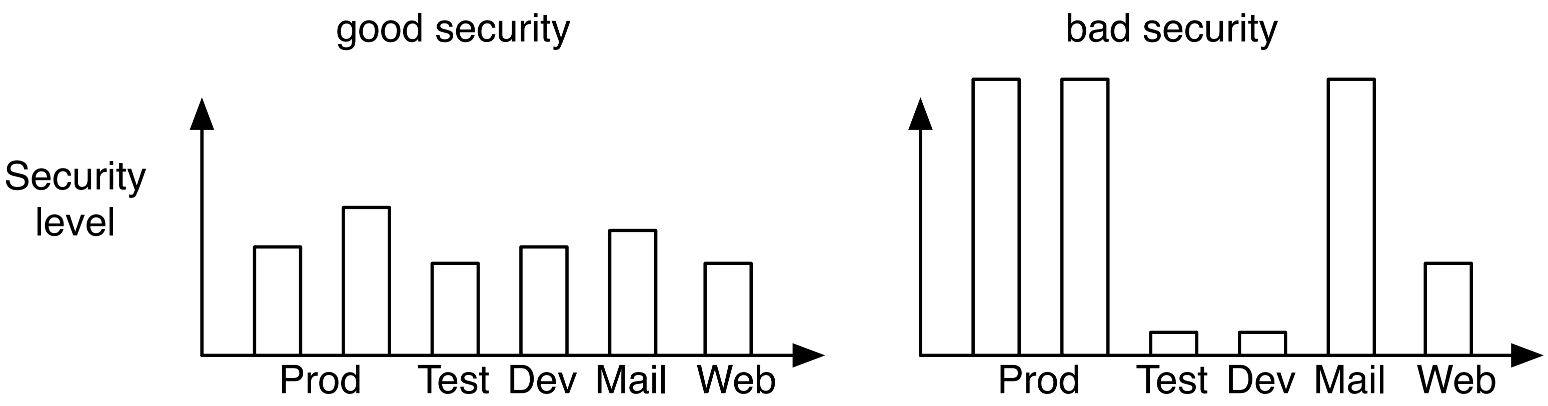
Low page count, but high value! Recommended.

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

Security Onion

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

Afbalanceret sikkerhed



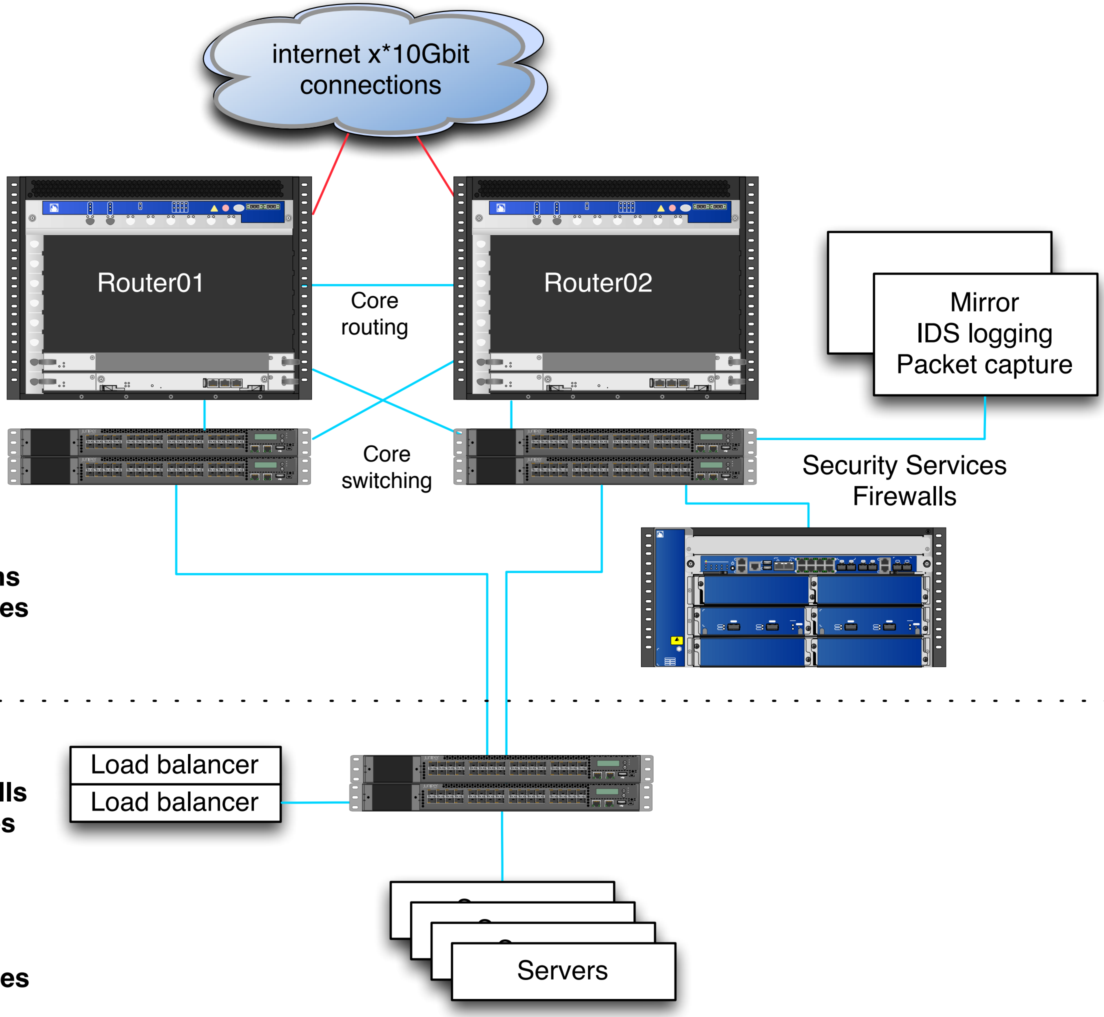
Det er bedre at have et ensartet niveau

Hvor rammer angreb hvis du har Fort Knox et sted og kaos andre steder

Hackere vælger ikke med vilje den sværeste vej ind

Defense in depth - multiple layers of security

Knowledge about traffic	Proposed actions to be done
	Get more bandwidth
Individual packets	Stateless filtering
Valid source IP ?	Null-routing RTBH Blackholing
Identify traffic by Ports/Protocols	Shaping and fair distribution
Sessions #sessions/IP	Stateful filtering screens IDS/IDP security services
Full request with parameters and cookies	Application tuning Next generation firewalls Load balancer features
Logged in user authenticated?	Server security Input validation
	Stack protection features



internet x*10Gbit connections

Router01

Router02

Core routing

Core switching

Mirror
IDS logging
Packet capture

Security Services
Firewalls

Load balancer

Load balancer

Servers

Quick conclusions

- 100.000vis af servere er sårbare overfor dette, se blandt andet listerne på `https://github.com/musalbas/heartbleed-masstest`
- Store sites som Yahoo.com, Flickr, FBI osv. er ramt
- Har du haft en server som var sårbar bør du skifte private key på SSL og få et nyt certifikat
  NB: reklame konkurrencedygtige priser på https://www.digitaltcertifikat.dk/ potentielt sparer du 10.000vis af kroner!
- NB: med DNSSEC/DANE implementeret ville det kun koste dine egne ressourcer at skifte certs!
- I Norge er der aktiv scanning igang og både HTTPS sites og mail servere har været ramt, dagens stat siger (tweet ca kl 8) "I've now completed checking STARTTLS mail servers: 11% still vulnerable." https://twitter.com/einaros/status/453773598172663808
- Yes, OpenSSL has lots of problems

Heartbleed Conclusions

Nothing new, but more focus on problems?
Really is there something new in this?

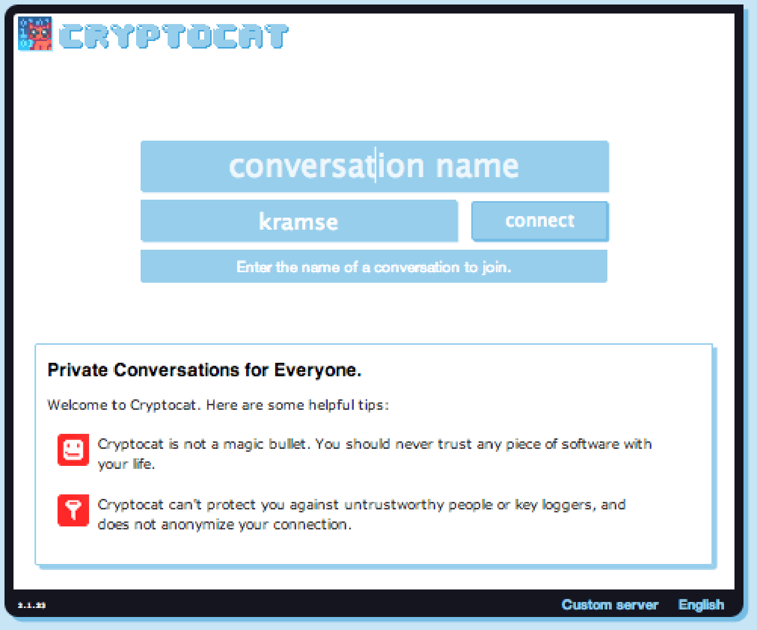
Software has bugs - stay vigilant, implement defense in depth

Software need funding - especially software used in our critical systems

Security needs proof of concepts and open communication
Akamai fix that wasn't good enough!

TL;DR Fund more security audits, stop using untested/unaudited software

Audits



Private Conversations for Everyone.

Welcome to Cryptocat. Here are some helpful tips:

Cryptocat is not a magic bullet. You should never trust any piece of software with your life.

Cryptocat can't protect you against untrustworthy people or key loggers, and does not anonymize your connection.

Truecrypt audit

`https://isecpartners.github.io/news/2014/04/14/iSEC-Completes-Truecrypt-Audit.html`

Cryptocat audit

`https://blog.crypto.cat/2013/02/cryptocat-passes-security-audit-with-flying-colors/`

Compare SSL

```
/* Read type and payload length first */
  if (1 + 2 + 16 > s->s3->rrec.length)
      return 0; /* silently discard */
  hbtype = *p++;
  n2s(p, payload);
  if (1 + 2 + payload + 16 > s->s3->rrec.length)
      return 0; /* silently discard per RFC 6520 sec. 4 */
  pl = p;
```

Ditch OpenSSL - write our own?

SSL implementations compared - above code from OpenSSL copied from this:
`http://tstarling.com/blog/2014/04/ssl-implementations-compared/`

LibreSSL announced, OpenBSD people
`http://www.libressl.org/` and `http://opensslrampage.org/`

Udviklingsstandarder

Hvad gør I for at undgå problemer som de her nævnte? - kan man gøre mere?

Man børe være klar over hvilke teknologier man bruger

Standardiser på et mindre antal produkter, biblioteker, sprog

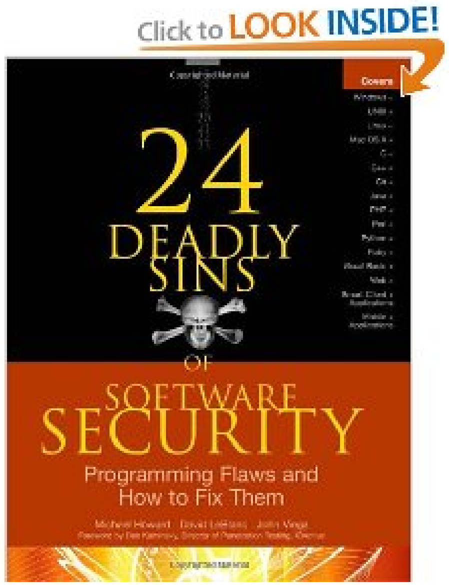
Regler og procedurer skal hele tiden opdateres:

- Kvalitetssikring - høj kvalitet er generelt mere sikker

Ved at fokusere på antallet af produkter kan man måske indskrænke mulighederne for fejl, høj kvalitet er ofte mere sikkert

nye produkter kan være farlige til man lærer dem at kende!

Deadly sins bogen



24 Deadly Sins of Software Security Michael Howard, David LeBlanc, John Viega 2. udgave, første hed 19 Deadly Sins

OWASP top ten

> The OWASP Top Ten provides a minimum standard for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

The Open Web Application Security Project (OWASP)

OWASP har gennem flere år udgivet en liste over de 10 vigtigste sikkerhedsproblemer for webapplikationer

`http://www.owasp.org`

OWASP WebGoat

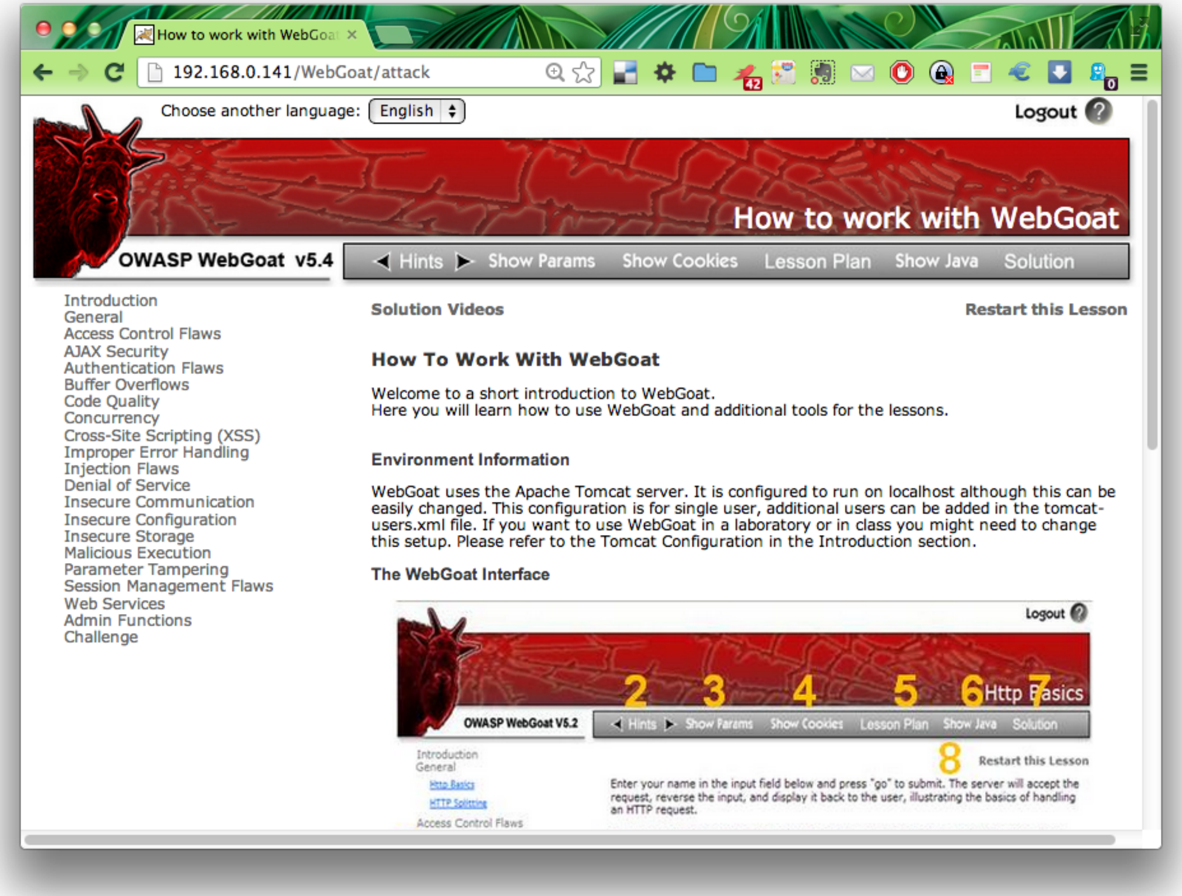
WebGoat fra OWASP, `http://www.owasp.org`

Træningsmiljø til webhacking

Downloades som Zipfil og kan afvikles direkte på en Windows laptop

`https://www.owasp.org`

WebGoat overview



How To Work With WebGoat

Welcome to a short introduction to WebGoat.
Here you will learn how to use WebGoat and additional tools for the lessons.

Environment Information

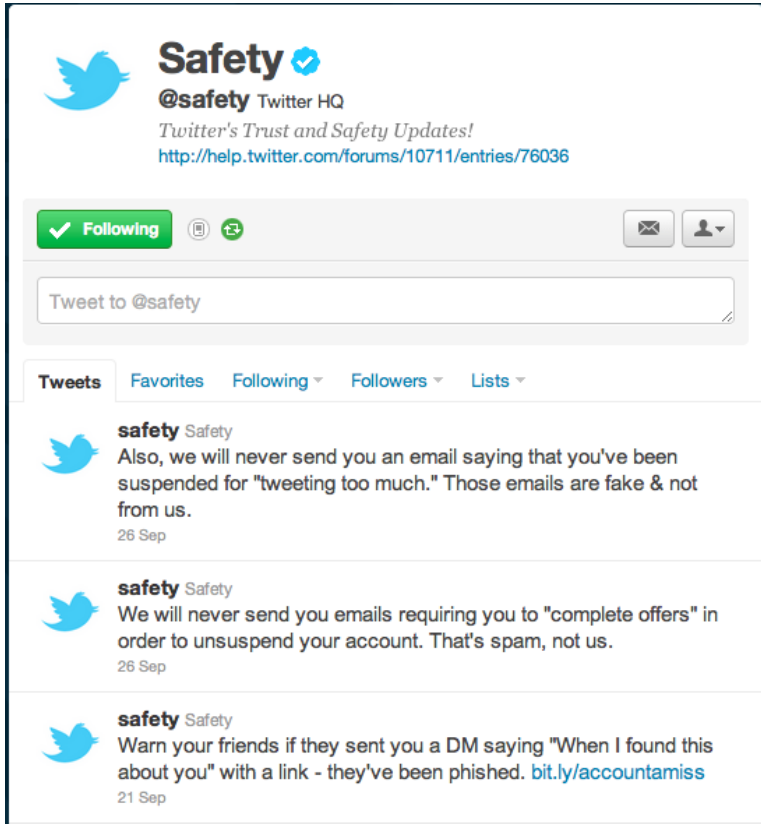
WebGoat uses the Apache Tomcat server. It is configured to run on localhost although this can be easily changed. This configuration is for single user, additional users can be added in the tomcat-users.xml file. If you want to use WebGoat in a laboratory or in class you might need to change this setup. Please refer to the Tomcat Configuration in the Introduction section.

The WebGoat Interface

Enter your name in the input field below and press "go" to submit. The server will accept the request, reverse the input, and display it back to the user, illustrating the basics of handling an HTTP request.

Perfect for learning web hacking/protection

Følg med Twitter news



Safety
@safety Twitter HQ
Twitter's Trust and Safety Updates!
http://help.twitter.com/forums/10711/entries/76036

safety Safety
Also, we will never send you an email saying that you've been suspended for "tweeting too much." Those emails are fake & not from us.
26 Sep

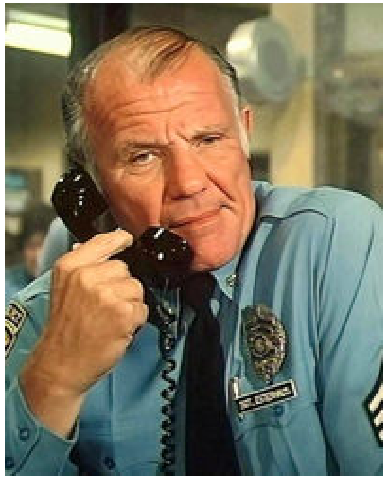
safety Safety
We will never send you emails requiring you to "complete offers" in order to unsuspend your account. That's spam, not us.
26 Sep

safety Safety
Warn your friends if they sent you a DM saying "When I found this about you" with a link - they've been phished. bit.ly/accountamiss
21 Sep

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

Be careful - spørgsmål?

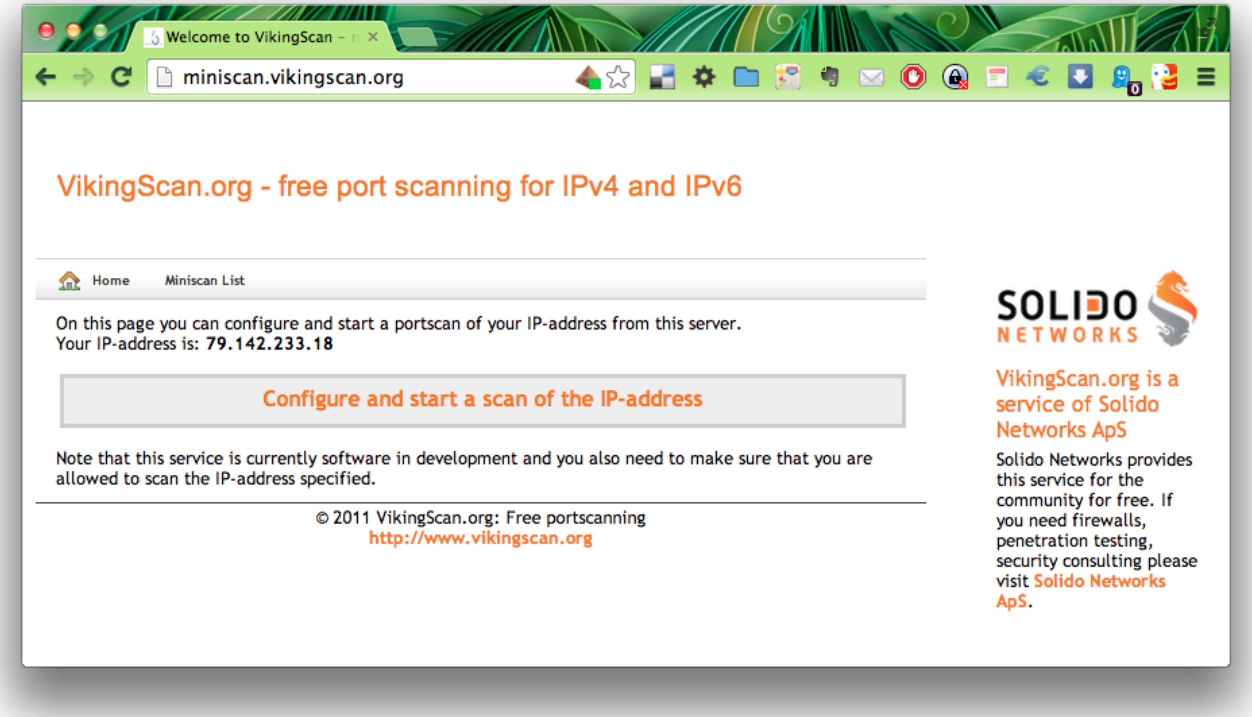


Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

Billede: Michael Conrad `http://www.hillstreetblues.tv/`

VikingScan.org - free portscanning



VikingScan.org - free port scanning for IPv4 and IPv6

On this page you can configure and start a portscan of your IP-address from this server.
Your IP-address is: 79.142.233.18

Configure and start a scan of the IP-address

Note that this service is currently software in development and you also need to make sure that you are allowed to scan the IP-address specified.

© 2011 VikingScan.org: Free portscanning
http://www.vikingscan.org

VikingScan.org is a service of Solido Networks ApS

Solido Networks provides this service for the community for free. If you need firewalls, penetration testing, security consulting please visit Solido Networks ApS.