



Welcome to

Kom og Hack IT-systemer

Henrik Lund Kramshøj hk@zencurity.dk



Don't Panic!

Hvordan foregår hacking?

Vi vil introducere Kali 2.0 Linux hackerplatformen og med eksempler som stiger i sværhedsgrad præsentere hacking af websystemer og sårbare virtuelle systemer.

Skabe forståelse for hackerværktøjer samt penetrationstest metoder

Du vil få mulighed for at prøve:

- hacking af websystemer gennem et sårbart website
- portscanning med Nmap sikkerhedsværktøjet
- hacking af en sårbar virtuel maskine med Metasploit



Improving the Security of Your Site by Breaking Into it af Dan Farmer og Wietse Venema i 1993

De udgav i 1995 så en softwarepakke med navnet *SATAN Security Administrator Tool for Analyzing Networks*

De forårsagede en del panik og furore, alle kan hacke, verden bryder sammen

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.

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

Brug hackerværktøjer!



Hackerværktøjer – bruger I dem? – efter dette kursus gør I

Portscannere kan afsløre huller i forsvaret

Webtestværktøjer som crawler igennem et website og finder alle forms kan hjælpe

I vil kunne finde mange potentielle problemer proaktivt ved regelmæssig brug af disse værktøjer – også potentielle driftsproblemer

Hacking er magi



Hacking ligner indimellem magi

Hacking er ikke magi



Hacking kræver blot lidt ninja-træning

Movie:Kryptonite lock - old



Just search for: kryptonite lock bic pen

<https://www.youtube.com/watch?v=LahDQ2ZQ3e0>

Hacking eksempel - det er ikke magi



MAC filtrering på trådløse netværk

Alle netkort har en MAC adresse - BRÆNDT ind i kortet fra fabrikken

Mange trådløse Access Points kan filtrere MAC adresser

Kun kort som er på listen over godkendte adresser tillades adgang til netværket ■

Det virker dog ikke 😊

De fleste netkort tillader at man overskriver denne adresse midlertidigt

Derudover har der ofte været fejl i implementeringen af MAC filtrering

MAC filtering



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 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 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!
- https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/ssl/openssl_heartbleed.rb

Most vulnerable operating systems in 2014



Operating system	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Apple Mac OS X	147	64	67	16
Apple iOS	127	32	72	23
Linux Kernel	119	24	74	21
Microsoft Windows Server 2008	38	26	12	0
Microsoft Windows 7	36	25	11	0
Microsoft Windows Server 2012	38	24	14	0
Microsoft Windows 8	36	24	12	0
Microsoft Windows 8.1	36	24	12	0
Microsoft Windows Vista	34	23	11	0
Microsoft Windows RT	30	22	8	0

An average of 19 vulnerabilities per day were reported in 2014, according to the data from the National Vulnerability Database (NVD).

Source:

<http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/>

Most vulnerable applications in 2014



Application	# of vulnerabilities	# of HIGH vulnerabilities	# of MEDIUM vulnerabilities	# of LOW vulnerabilities
Microsoft Internet Explorer	242	220	22	0
Google Chrome	124	86	38	0
Mozilla Firefox	117	57	57	3
Adobe Flash Player	76	65	11	0
Oracle Java	104	50	46	8
Mozilla Thunderbird	66	36	29	1
Mozilla Firefox ESR	61	35	25	1
Adobe Air	45	38	7	0
Apple TV	86	29	49	8
Adobe Reader	44	37	7	0
Adobe Acrobat	43	35	8	0
Mozilla SeaMonkey	63	28	34	1

Not surprisingly at all, web browsers continue to have the most security vulnerabilities because they are a popular gateway to access a server and to spread malware on the clients.

Source:

<http://www.gfi.com/blog/most-vulnerable-operating-systems-and-applications-in-2014/>

OSI og Internet modellerne



OSI Reference Model

Application
Presentation
Session
Transport
Network
Link
Physical

Internet protocol suite


Applications HTTP, SMTP, FTP, SNMP,	NFS
	XDR
	RPC
TCP UDP	
IPv4	IPv6 ICMPv6 ICMP
ARP RARP	
MAC	
Ethernet token-ring ATM ...	

Wireshark - grafisk pakkesniffer




WIRESHARK [Get Acquainted ▾](#) [Get Help ▾](#) [Develop ▾](#) [Sharkfest '15](#) [Our Sponsor](#) [WinPcap](#)

We're having a conference! You're invited!




Download

Get Started Now



Learn


Knowledge is Power



Enhance

With Riverbed Technology

News And Events



Join us at SHARKFEST '15!


SHARKFEST '15 will be held from June 22 – 25 at the Computer History Museum in Mountain View, CA.

[Learn More ▸](#)


Troubleshooting with Wireshark

By Laura Chappell
Foreword by Gerald Combs
Edited by Jim Aragon


This book focuses on the tips and techniques used to identify




Wireshark Blog




Cool New Stuff

Dec 17 | By Evan Huus 

Wireshark 1.12 Officially Released!

Jul 31 | By Evan Huus 

To Infinity and Beyond! Capturing Forever with Tshark

Jul 8 | By Evan Huus 


[More Blog Entries ▸](#)

Enhance Wireshark

Riverbed is Wireshark's primary sponsor and provides our funding. They also make great products.

802.11 Packet Capture

- WLAN packet capture and transmission
- Full 802.11 a/b/g/n support
- View management, control and data frames
- Multi-channel aggregation (with multiple adapters)



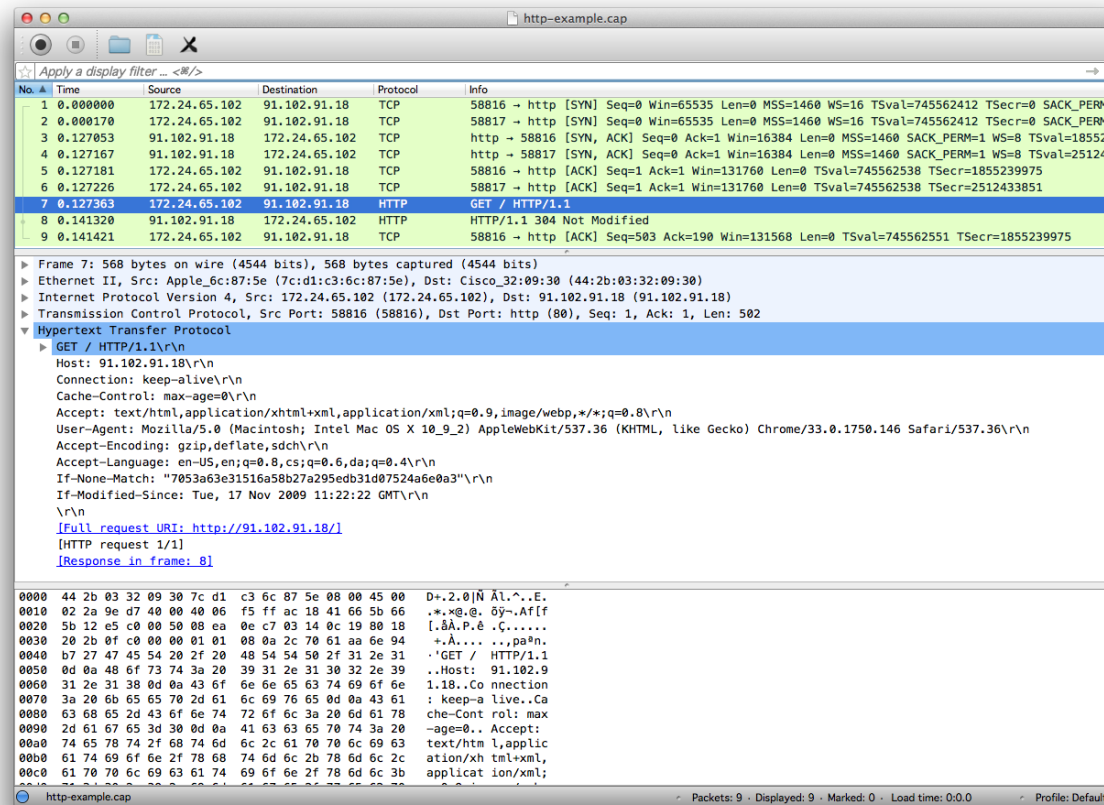
[Learn More ▸](#)

[Buy Now ▸](#)

`http://www.wireshark.org`

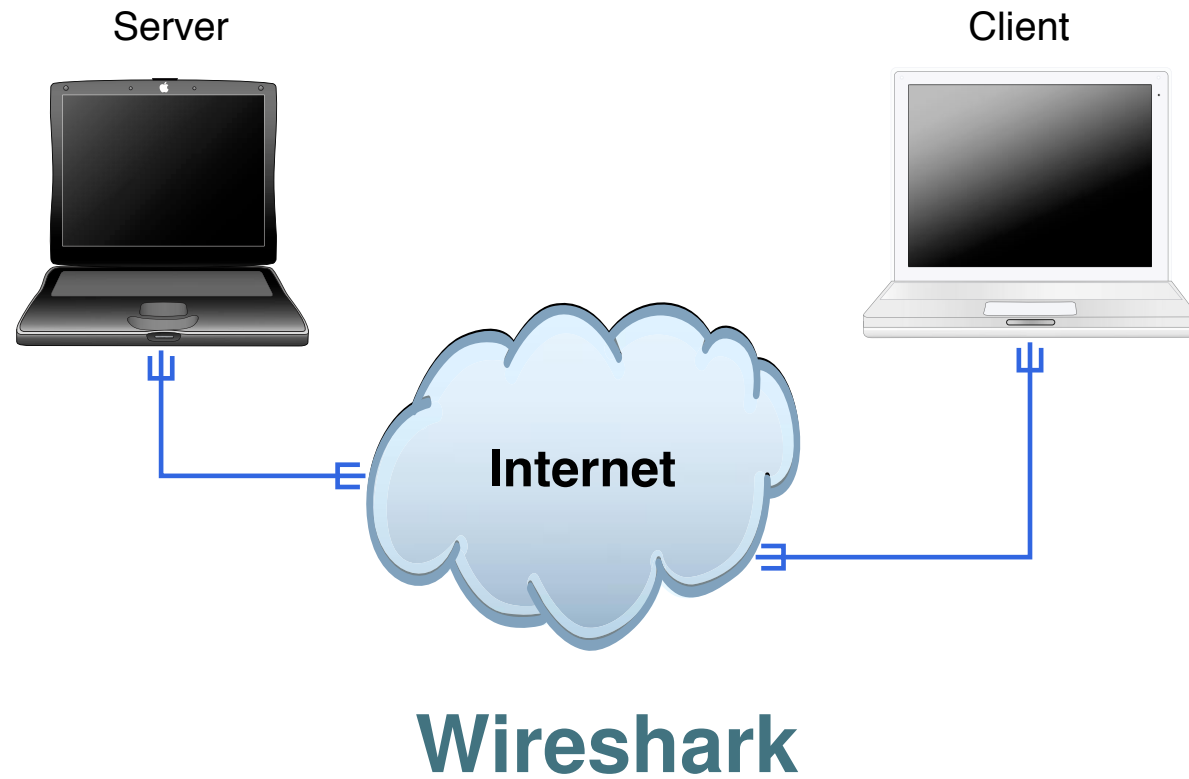
både til Windows og UNIX

Wireshark usage

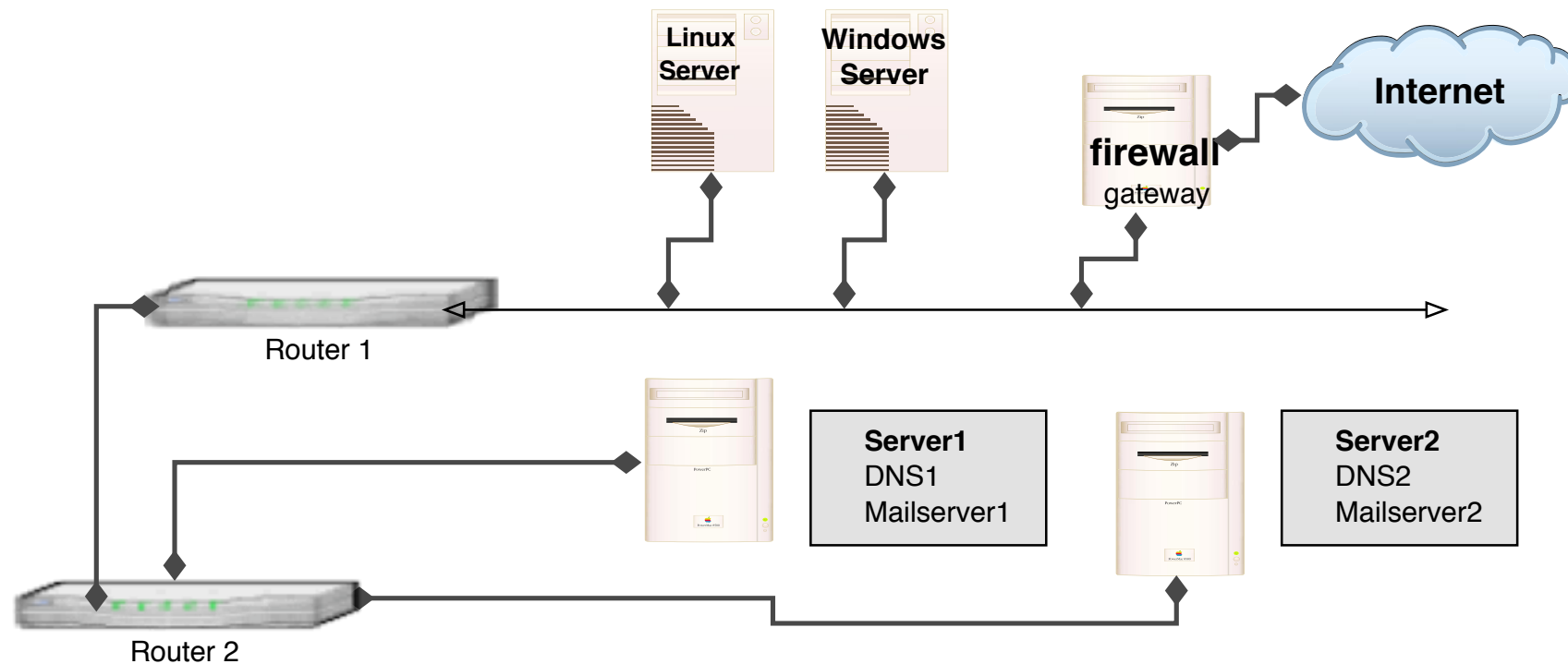


Wireshark: Filters, hexdump, protocol dissection, overview, coloring, advanced features

Demo: Wireshark

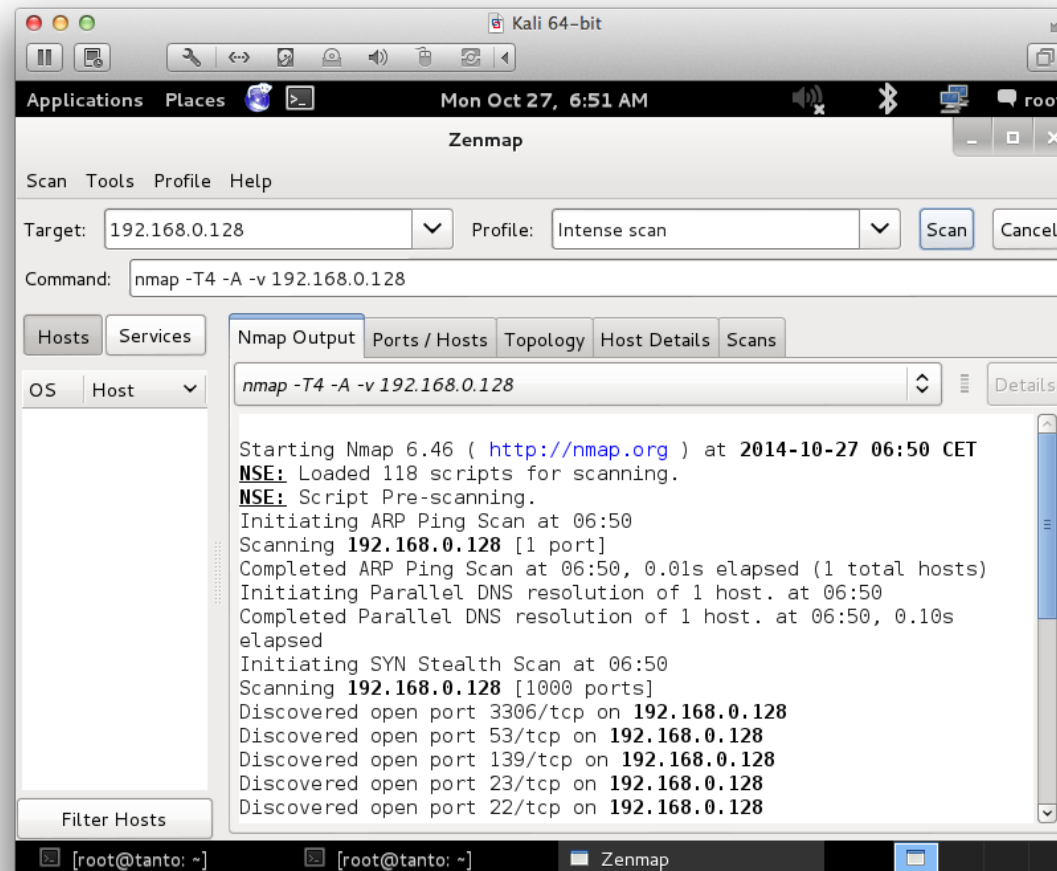


Network mapping



Ved brug af traceroute og tilsvarende programmer kan man ofte udlede topologien i det netværk man undersøger

Portscan med Zenmap GUI



Cracking passwords



- Hashcat is the world's fastest CPU-based password recovery tool.
- oclHashcat-plus is a GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.
- oclHashcat-lite is a GPGPU cracker that is optimized for cracking performance. Therefore, it is limited to only doing single-hash cracking using Markov attack, Brute-Force attack and Mask attack.
- John the Ripper password cracker old skool men stadig nyttig

Source:

<http://hashcat.net/wiki/>

<http://www.openwall.com/john/>



Henrik Kramshøj retweeted



Solar Designer @solardiz

Similarly expensive Xeon E5-2670 is 2.4x to 3.3x slower than Zynq 7045 #FPGA on this test, yet consumes ~20x more power; GPUs are way behind



Henrik Kramshøj retweeted



Solar Designer @solardiz

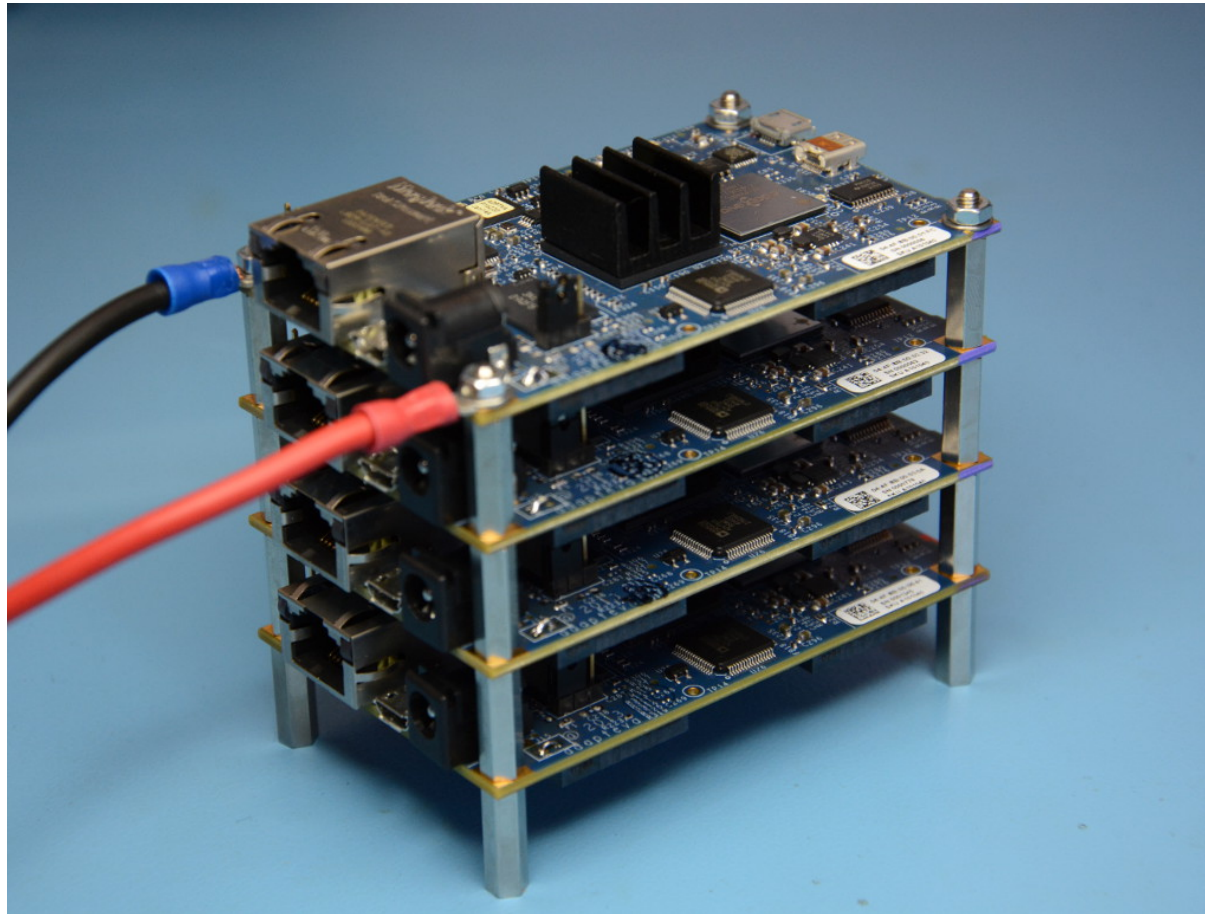
On last night to submit WOOT final paper, @kmalvoni got bcrypt \$2a\$05 to 20538 c/s, \$2a\$12 to 226 c/s on Zynq 7045 #FPGA. Not the limit yet.

15h

<https://twitter.com/solardiz/status/492037995080712192>

Warning: FPGA hacking - not finished part of presentation

Stacking Parallella boards



<http://www.parallella.org/power-supply/>



- Alle bruger nogenlunde de samme værktøjer, se også <http://www.sectools.org/>
- Portscanner Nmap, Nping – tester porte, godt til firewall admins <https://nmap.org>
- Generel sårbarhedsscanner Metasploit Framework <https://www.metasploit.com/>
- Specialscannere, eksempelvis web sårbarhedsscanner – eksempelvis Nikto, Skipfish
- Specielle scannere – wifi Aircrack-ng, web Burpsuite <http://portswigger.net/burp/>
- Wireshark avanceret netværkssniffer – <https://www.wireshark.org/>
- og scripting, PowerShell, Unix shell, Perl, Python, Ruby, ...

Billedet: Angelina Jolie fra Hackers 1995

Hvad skal der ske?



Tænk som en hacker

Rekognoscering

- ping sweep, port scan
- OS detection – TCP/IP eller banner grab
- Servicescan – rpcinfo, netbios, ...
- telnet/netcat interaktion med services

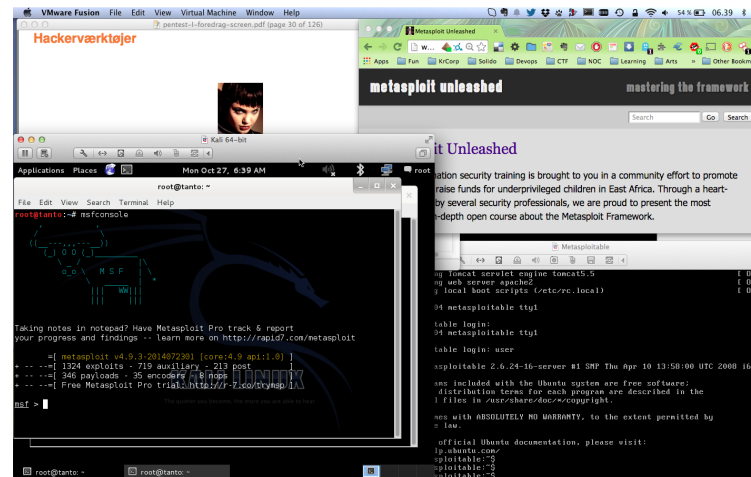
Udnyttelse/afprøvning: Metasploit, Nikto, exploit programs

Oprydning/hærdning vises måske ikke, men I bør i praksis:

- Lav en rapport
- Ændre, forbedre og hærde systemer
- Gennemgå rapporten, registrer ændringer
- Opdater programmer, konfigurationer, arkitektur, osv.

I skal jo også VISE andre at I gør noget ved sikkerheden.

Hackerlab opsætning



- Hardware: en moderne laptop med CPU der kan bruge virtualisering
Husk at slå virtualisering til i BIOS
- Software: dit favoritoperativsystem, Windows, Mac, Linux
- Virtualiseringssoftware: VMware, Virtual box, vælg selv
- Hackersoftware: Kali som Virtual Machine <https://www.kali.org/>
- Soft targets: Metasploitable, Windows 2000, Windows XP, ...

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.**

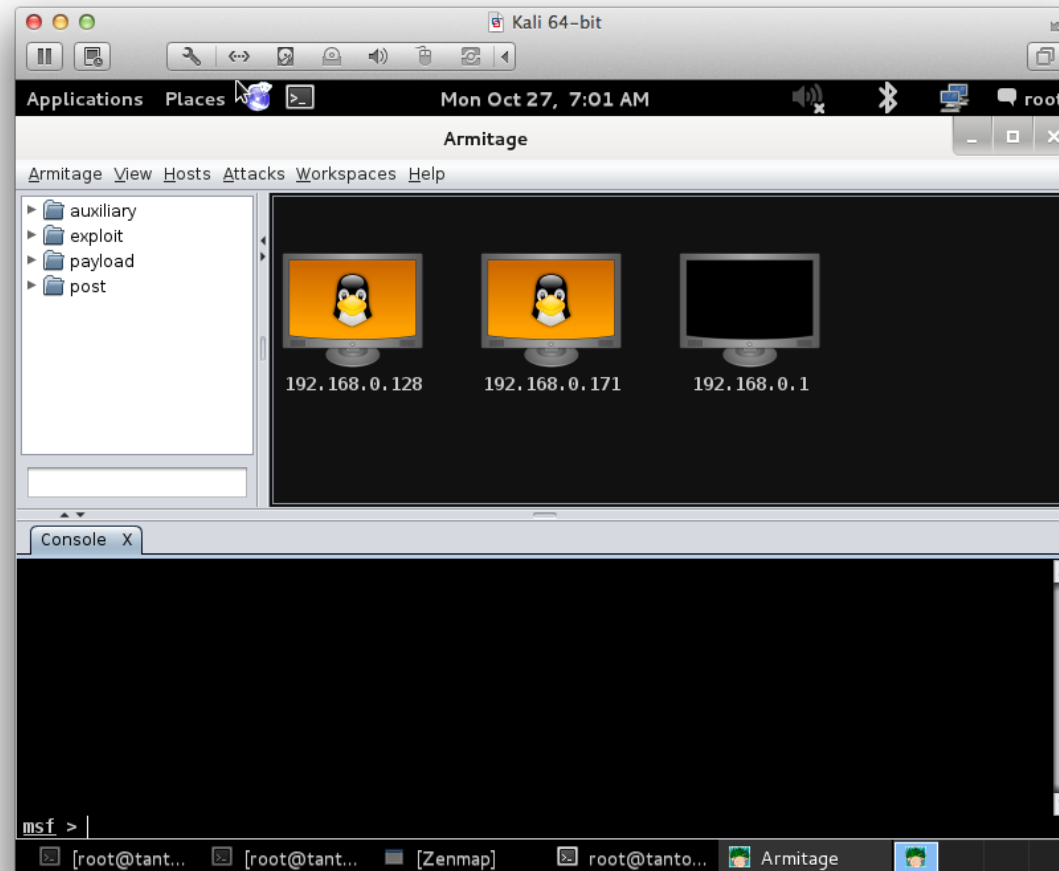
A Project By Offensive Security

BackTrack – <http://www.backtrack-linux.org>

Kali – <https://www.kali.org/> version 2.0 netop udkommet!

Wireshark – <https://www.wireshark.org> avanceret netværkssniffer

Demo: Metasploit Armitage



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.

Udviklingsværktøjerne til exploits er i dag meget raffinerede!

<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



Vi kan ikke nå alverden men prøv at gentage det jeg viste

- Wireshark
- Wireshark med FTP
- Nmap med Zenmap
- Armitage og Metasploit, husk `service postgresql start`
- Prøv også OWASP Web Goat som jeg har startet

Questions?



Henrik Lund Kramshøj hlik@zencurity.dk

Need DDoS testing or pentest, ask me!

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