Welcome to

Nmap Hackerworkshop

An evening with Nmap

Henrik Lund Kramshøj hlk@zencurity.dk

Slides are available as PDF, kramse@Github
nmap-workshop.tex in the repo security-courses

Don't Panic!

Spend an evening using Nmap tools, multiple tools:

Try different scan types from graphical Zenmap and command line

Try different tools like Nping, Ndiff

Practice real-life scenarios

Enable you to do quality port scans!

NOTE: please read the notes for each exercise, important information!

Hackertools

First published *Improving the Security of Your Site by Breaking Into it* Dan Farmer og Wietse Venema in 1993

Published in 1995 then a software package SATAN *Security Administrator Tool for Analyzing Networks*

Caused quite a stir and panic, *everybody can hack, the internet will break*

> 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.

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

DK Law - Aftale om test af netværk

Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem.

Hacking kan betyde:

- At man skal betale erstatning til personer eller virksomheder

- At man får konfiskeret sit udstyr af politiet

- At man, hvis man er over 15 år og bliver dømt for hacking, kan få en bøde – eller fængselsstraf i alvorlige tilfælde

- At man, hvis man er over 15 år og bliver dømt for hacking, får en plettet straffeattest. Det kan give problemer, hvis man skal finde et job eller hvis man skal rejse til visse lande, fx USA og Australien

- Frygten for terror har forstærket ovenstående – så lad være!

Use hackertools!

Hackertools – Using them already? – should use them after this course

Portscans show potential access to your network

Web test tools and scanners can crawl a site and report problems

Lots of potential weaknesses can be found proactively by using these tools regularly

Note: penetration testing is not a silverbullet

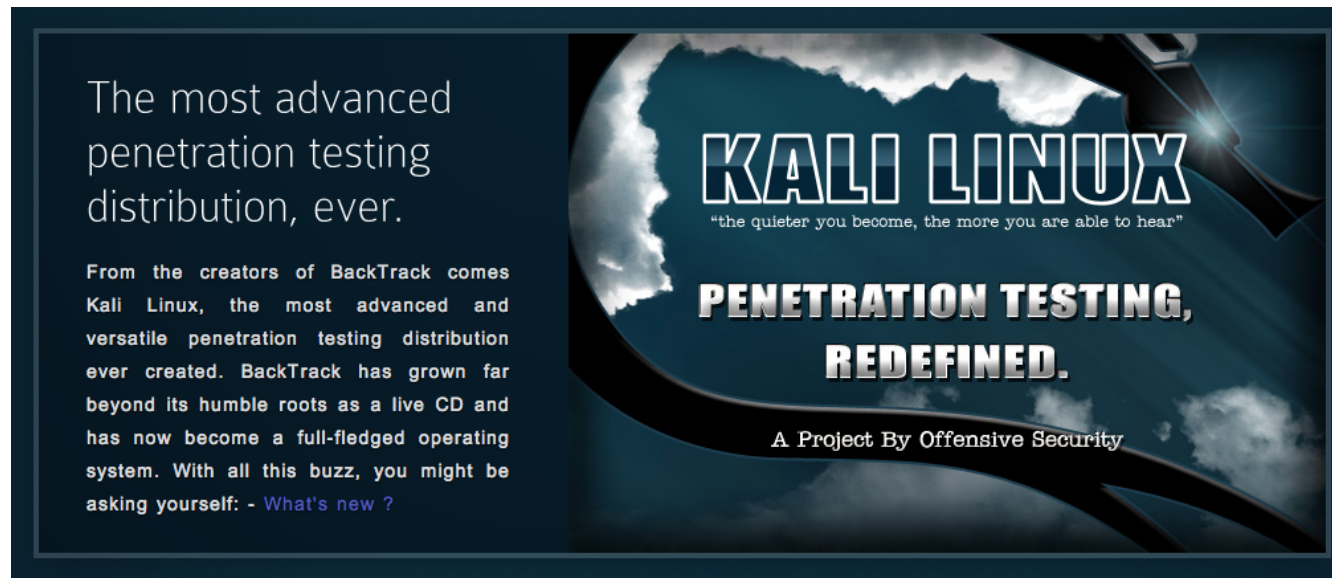Honeypots can also be used to setup traps for attackers

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

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

Kali `http://www.kali.org/` brings together 100s of tools

100.000s of videos on youtube alone, searching for kali and $TOOL

Also versions for Raspberry Pi, mobile and other small computers

Other pentesting Linux distributions exist, but Kali is very popular

Hackerlab setup
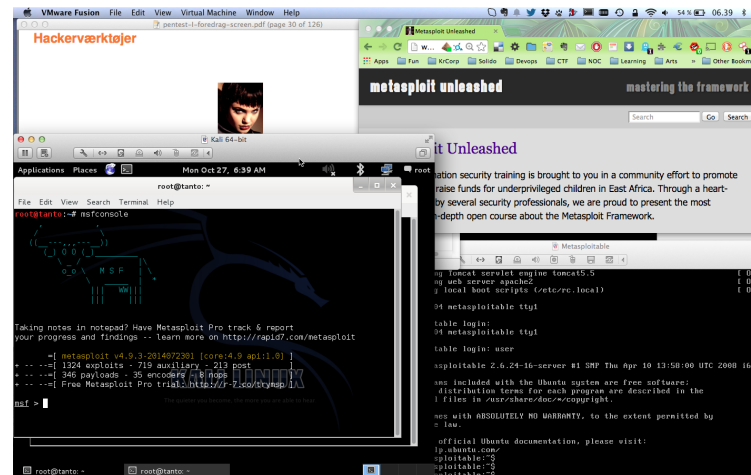
- **Hardware:** most modern laptops has CPU with virtualization
  May need to enale it in BIOS

- **Software:** use your favorite operating system, Windows, Mac, Linux

- **Virtualization software:** VMware, Virtual box, choose your poison

- **Hackersoftware:** Kali as a Virtual Machine `https://www.kali.org/`

- **Install soft targets:** Metasploitable, Windows 2000, Windows XP, ...

Exercise
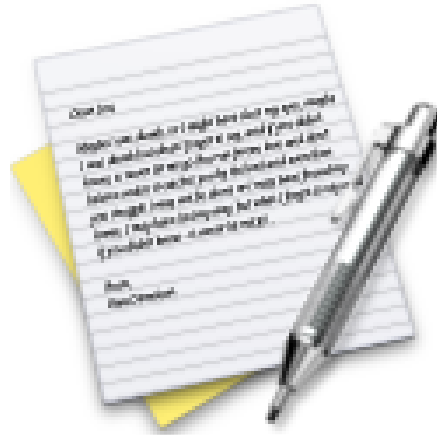
Now lets do the exercise

Wireshark install

which is number 1 in the exercise PDF.
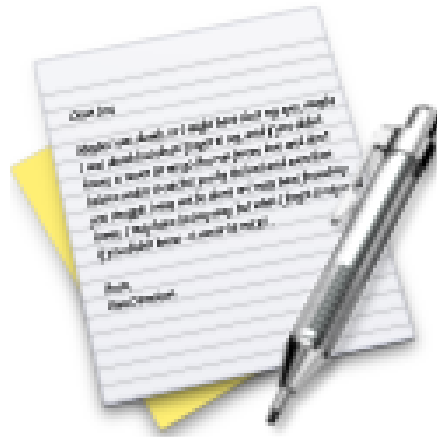
Exercise

Now lets do the exercise

Nmap install

which is number 2 in the exercise PDF.

Scope: select systems for testing

Sample Network
Location: Copenhagen
Date: August X 2013
Room: x Version: 1..0

internet x*10Gbit connections

Router01   Core routing   Router02

Core switching

Security Services
Firewalls

Redundant customer
some shared devices

Redundant customer
with dedicated devices

LAN
L2 switching

Firewalls

Loadbalancer
Loadbalancer

Servers

Servers

LAN
L2 switching

Loadbalancer
Loadbalancer

Dedicated load balancing

Typical scope targets:

- Routers in front of critical systems and networks - availability
- Firewalls – are traffic flows restricted
- Mail servers – open for relaying
- Web servers – remote code execution in web systems, data download

Halt testing – compromised servers

There can be reason for halting a penetration test

You should stop testing when:

- Breached and compromised systems are found. Dont mess up evidence
- Network is bad, testing will not show correct results

or if the customer wants to halt testing:

- Problems when performing the test
- Crashes in critical systems
- Other crises demand attention

NB: examples only! – always stop testing if customers ask!

Reporting – results

What is in a pentest report:

- Title, Table of contents, – total. 15-30 pages for 5 hosts
- Confidentiality agreement – Write "Confidential" on each page
- Executive summary – big companies always want this
- Information about the scan done, what was it
- Scope and targets
- Review of all targets – detailed information and recommendations
- Conclusion – may be more technical
- Appendices – various information, Whois info about subnets and prefixes

It is the organisation that ultimately decides which recommendations to follow

What happens now?

Think like a hacker

Recon phase – gather information reconnaissance

- Traceroute, Whois, DNS lookups
- Ping sweep, port scan
- OS detection – TCP/IP and banner grabbing
- Service scan – rpcinfo, netbios, ...
- telnet/netcat interact with services

Today focus on Nmap and processes around portscanning

Internet i dag

Server   Client

Internet
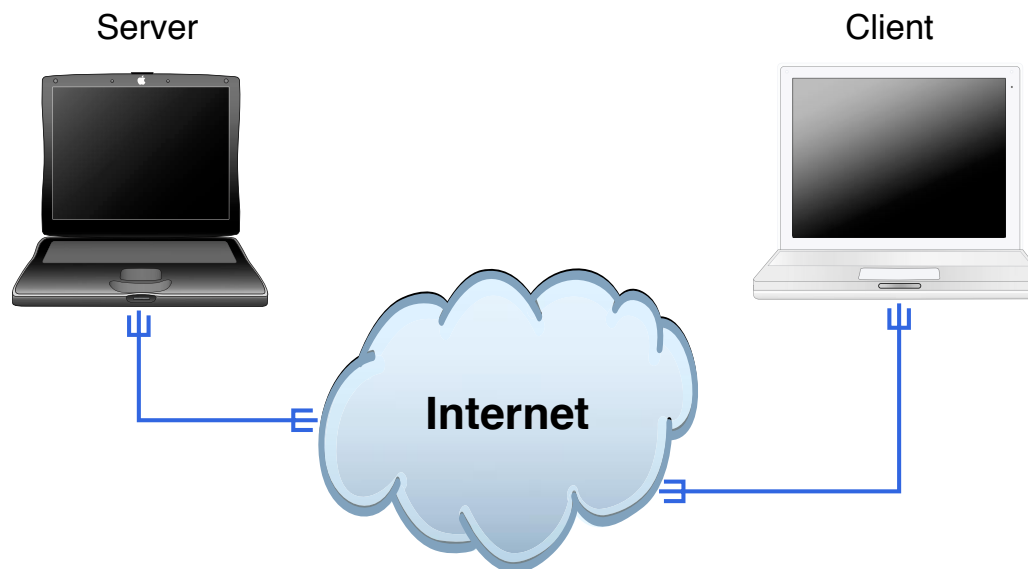
Klienter og servere

Rødder i akademiske miljøer

Protokoller der er op til 20 år gamle

Meget lidt kryptering, mest på http til brug ved e-handel

Trinity breaking in

Meget realistisk - sådan foregår det næsten:

https://nmap.org/movies/

https://youtu.be/51lGCTgqE_w

Nmap has been featured in twelve movies

what is Nmap today

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.

Initial release September 1997; 20 years ago

Today a package of programs for Windows, Mac, BSD, Linux, ... source

Flexible, powerful, and free!

Vi gennemgår seneste release notes, 7.70 pt. http://seclists.org/nmap-announce/2018/0

Bonus tal om hvordan man submitter fingerprints til Nmap

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

https://www.wireshark.org
Både til Windows og Unix

Brug af Wireshark
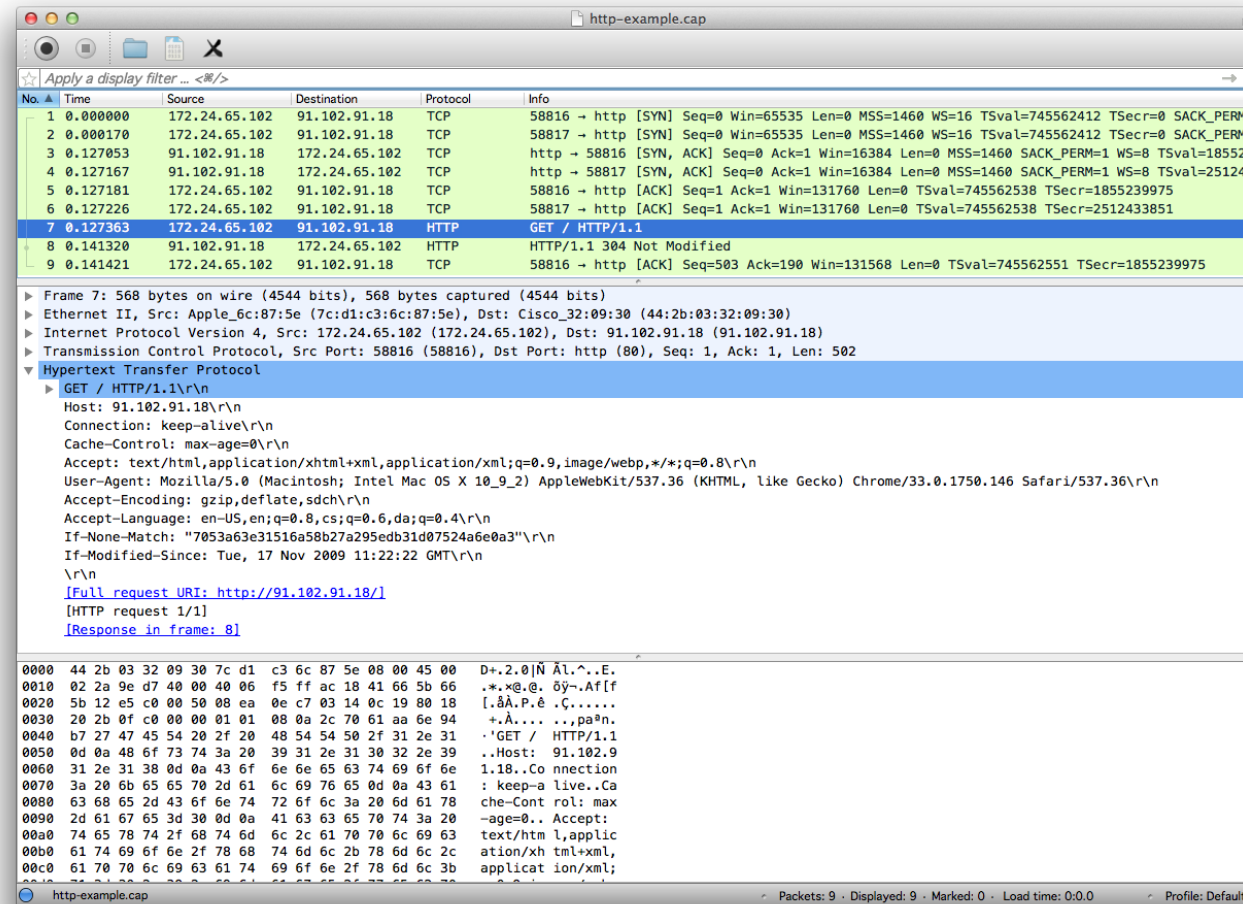
Læg mærke til filtermulighederne

Network mapping

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

Levetiden (TTL) for en pakke tælles ned på hver router, sættes denne lavt opnår man at pakken *timer ud* – besked fra hver router på vejen
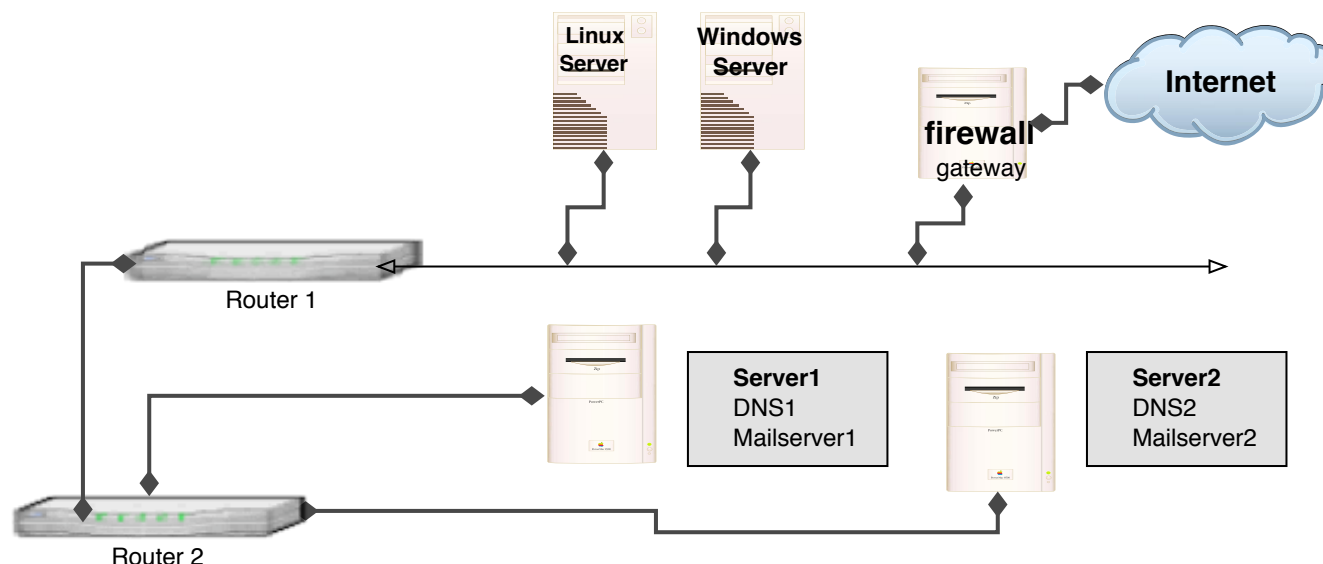
Default Unix er UDP pakker, Windows tracert ICMP pakker

traceroute – med UDP

```
 #  tcpdump -i en0 host 10.20.20.129 or host 10.0.0.11
tcpdump: listening on en0
23:23:30.426342 10.0.0.200.33849 > router.33435: udp 12  [ttl 1]
23:23:30.426742 safri > 10.0.0.200:  icmp: time exceeded in-transit
23:23:30.436069 10.0.0.200.33849 > router.33436: udp 12  [ttl 1]
23:23:30.436357 safri > 10.0.0.200:  icmp: time exceeded in-transit
23:23:30.437117 10.0.0.200.33849 > router.33437: udp 12  [ttl 1]
23:23:30.437383 safri > 10.0.0.200:  icmp: time exceeded in-transit
23:23:30.437574 10.0.0.200.33849 > router.33438: udp 12
23:23:30.438946 router > 10.0.0.200: icmp: router  udp port 33438 unreachable
23:23:30.451319 10.0.0.200.33849 > router.33439: udp 12
23:23:30.452569 router > 10.0.0.200: icmp: router  udp port 33439 unreachable
23:23:30.452813 10.0.0.200.33849 > router.33440: udp 12
23:23:30.454023 router > 10.0.0.200: icmp: router  udp port 33440 unreachable
23:23:31.379102 10.0.0.200.49214 > safri.domain:  6646+ PTR?
200.0.0.10.in-addr.arpa. (41)
23:23:31.380410 safri.domain > 10.0.0.200.49214:  6646 NXDomain* 0/1/0 (93)
14 packets received by filter
0 packets dropped by kernel
```

Basal Portscanning

Hvad er portscanning

Afprøvning af alle porte fra 0/1 og op til 65535

Målet er at identificere åbne porte – sårbare services

Typisk TCP og UDP scanning

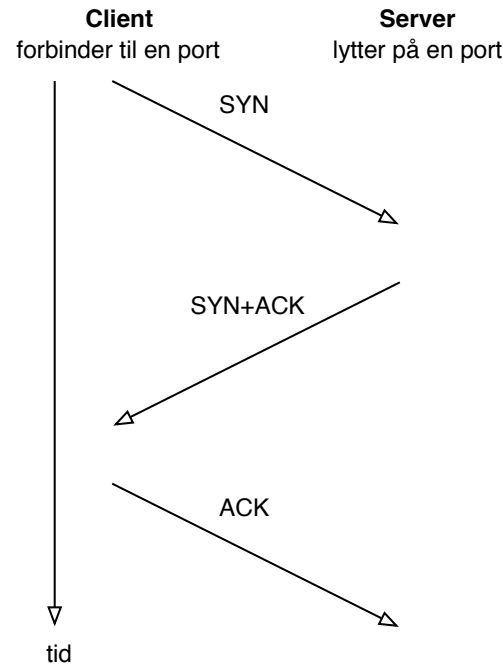TCP scanning er ofte mere pålidelig end UDP scanning

TCP handshake er nemmere at identificere, skal svare SYN

UDP applikationer svarer forskelligt – hvis overhovedet
Svarer på rigtige forespørgsler, uden firewall svares ICMP på lukkede
porte

Brug GUI programmet Zenmap mens i lærer Nmap at kende

TCP three-way handshake

- **TCP SYN half-open** scans

- Tidligere loggede systemer kun når der var etableret en fuld TCP forbindelse – dette kan/kunne udnyttes til *stealth*-scans

- Hvis en maskine modtager mange SYN pakker kan dette fylde tabellen over connections op – og derved afholde nye forbindelser fra at blive oprette – **SYN-flooding**
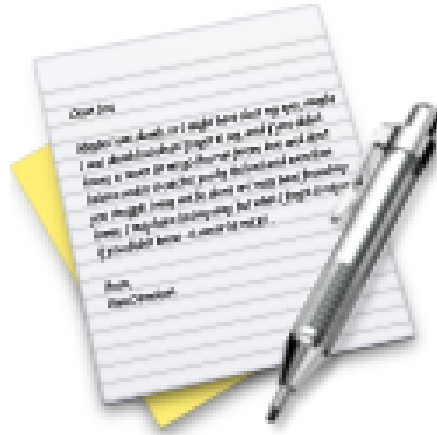
Exercise

Now lets do the exercise

Lookup Whois and DNS data

which is number 3 in the exercise PDF.

Exercise

Now lets do the exercise

Capturing network packets

which is number 4 in the exercise PDF.

Ping og port sweep

Scanninger på tværs af netværk kaldes for sweeps

Scan et netværk efter aktive systemer med PING

Scan et netværk efter systemer med en bestemt port åben

Er som regel nemt at opdage:

- konfigurer en maskine med to IP-adresser som ikke er i brug
- hvis der kommer trafik til den ene eller anden er det portscan
- hvis der kommer trafik til begge IP-adresser er der nok foretaget et sweep – bedre hvis de to adresser ligger et stykke fra hinanden

Pro tip: Hvis du leder efter et Netværks IDS, så kig på Suricata
`suricata-ids.org`

Nmap port sweep efter webservere

```
root@cornerstone:~#  nmap -p80,443 172.29.0.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:31 CET
Nmap scan report for 172.29.0.1
Host is up (0.00016s latency).
PORT     STATE     SERVICE
80/tcp   open      http
443/tcp  filtered  https
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.29.0.138
Host is up (0.00012s latency).
PORT     STATE   SERVICE
80/tcp   open    http
443/tcp  closed  https
MAC Address: 00:0C:29:46:22:FB (VMware)
```

Nmap port sweep efter SNMP port 161/UDP

```
root@cornerstone:~# nmap -sU -p 161 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:30 CET
Nmap scan report for 172.29.0.1
Host is up (0.00015s latency).
PORT       STATE           SERVICE
161/udp open|filtered snmp
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 172.29.0.138
Host is up (0.00011s latency).
PORT      STATE   SERVICE
161/udp closed snmp
MAC Address: 00:0C:29:46:22:FB (VMware)
...
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.18 seconds
```

Nmap Advanced OS detection

```
root@cornerstone:~# nmap -A -p80,443 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:37 CET
Nmap scan report for 172.29.0.1
Host is up (0.00027s latency).
PORT     STATE     SERVICE VERSION
80/tcp  open      http    Apache httpd 2.2.26 ((Unix) DAV/2 mod_ssl/2.2.26 OpenSSL/0.9.8zc)
|_http-title: Site doesn't have a title (text/html).
443/tcp filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)
Device type: media device|general purpose|phone
Running: Apple iOS 6.X|4.X|5.X, Apple Mac OS X 10.7.X|10.9.X|10.8.X
OS details: Apple iOS 6.1.3, Apple Mac OS X 10.7.0 (Lion) - 10.9.2 (Mavericks)
or iOS 4.1 - 7.1 (Darwin 10.0.0 - 14.0.0), Apple Mac OS X 10.8 - 10.8.3 (Mountain Lion)
or iOS 5.1.1 - 6.1.5 (Darwin 12.0.0 - 13.0.0)
OS and Service detection performed.
Please report any incorrect results at http://nmap.org/submit/
```
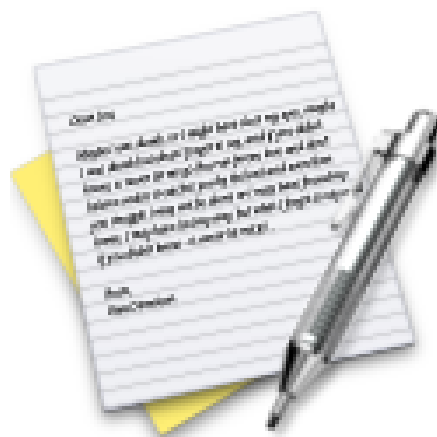
- **Lavniveau måde at identificere operativsystemer på, prøv også** nmap -A

- **Send pakker med** *anderledes* **indhold, observer svar**

- **En tidlig og detaljeret reference:** *ICMP Usage In Scanning* **Version 3.0, Ofir Arkin, 2001**

Portscan med Zenmap GUI
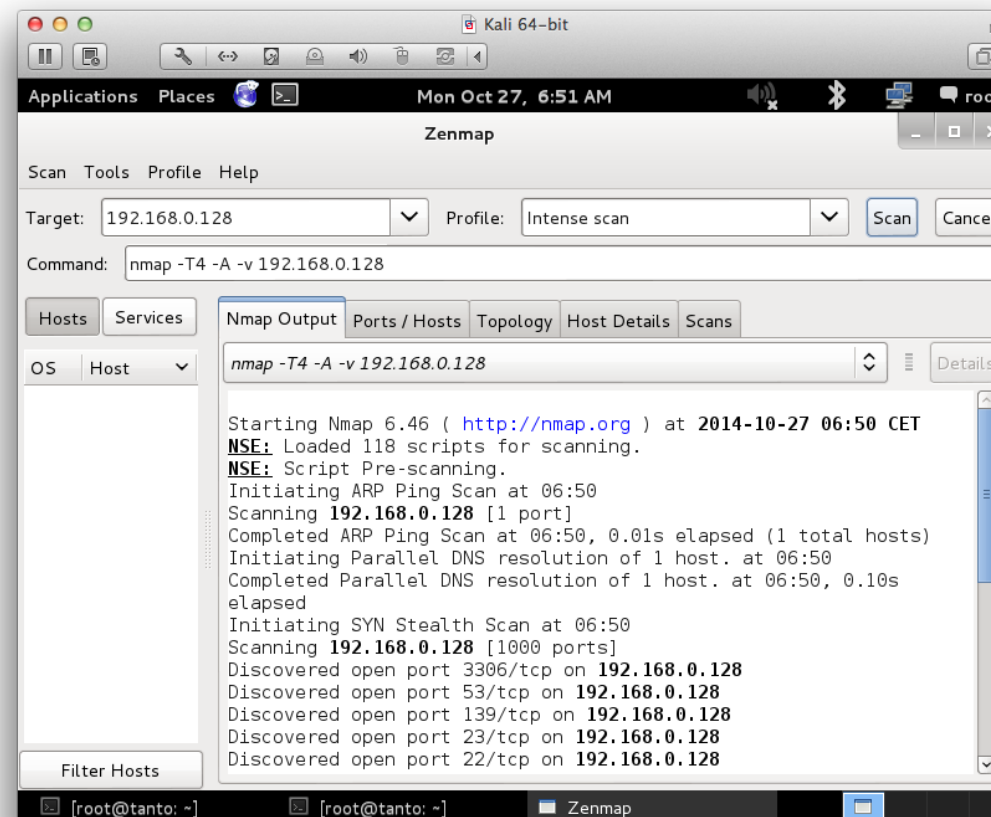
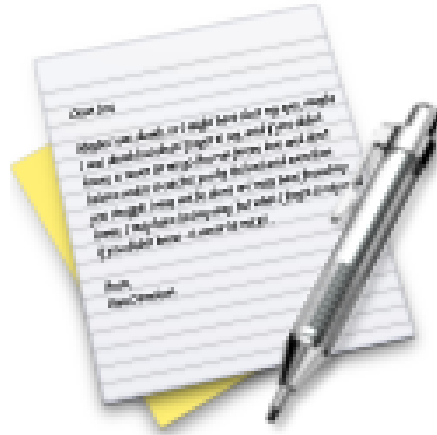**Zenmap følger med i pakken når man henter Nmap** `https://nmap.org`

Exercise

Now lets do the exercise

Discover active systems ping sweep

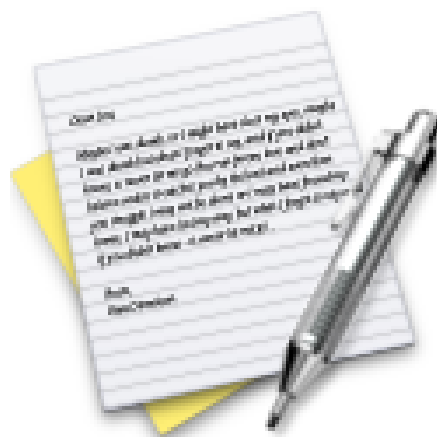which is number **5** in the exercise PDF.

Now lets do the exercise

Execute nmap TCP and UDP port scan

which is number 6 in the exercise PDF.
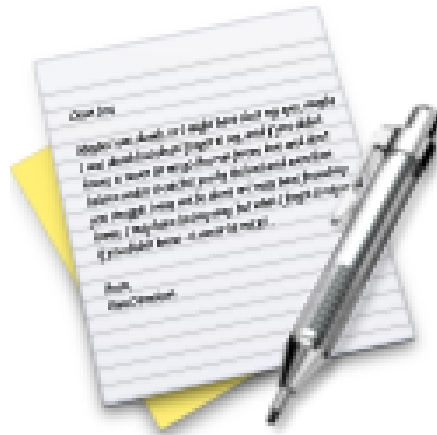
Exercise

Now lets do the exercise

Perform nmap OS detection

which is number **7** in the exercise PDF.

Exercise

Now lets do the exercise

Perform nmap service scan

which is number 8 in the exercise PDF.

Exercise

Now lets do the exercise

Nmap full scan

which is number 9 in the exercise PDF.

# Erfaringer hidtil

Mange oplysninger

Kan man stykke oplysningerne sammen kan man sige en hel del om netværket

En skabelon til registrering af maskiner er god

- Svarer på ICMP: □ echo, □ mask, □ time
- Svarer på traceroute: □ ICMP, □ UDP
- Åbne porte TCP og UDP:
- Operativsystem:
- ... (banner information m.v.)

Mange små pakker kan oversvømme store forbindelser og give proble-mer for netværk

Exercise
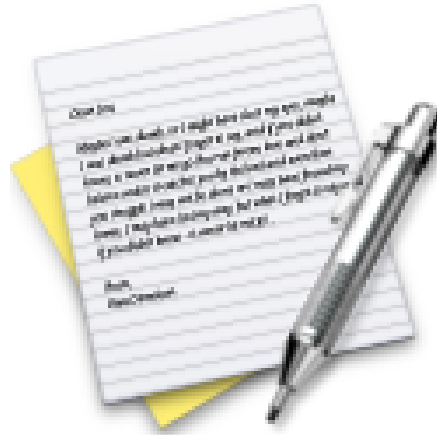
Now lets do the exercise

Reporting HTML

which is number 10 in the exercise PDF.

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

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.

Scan for Heartbleed and SSLv2/SSLv3

Example Usage

```
nmap -sV -sC <target>
```

Script Output

```
443/tcp open    https    syn-ack
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
```

```
nmap -p 443 --script ssl-heartbleed <target>
```
https://nmap.org/nsedoc/scripts/ssl-heartbleed.html

```
masscan 0.0.0.0/0 -p0-65535  --heartbleed
```
https://github.com/robertdavidgraham/masscan

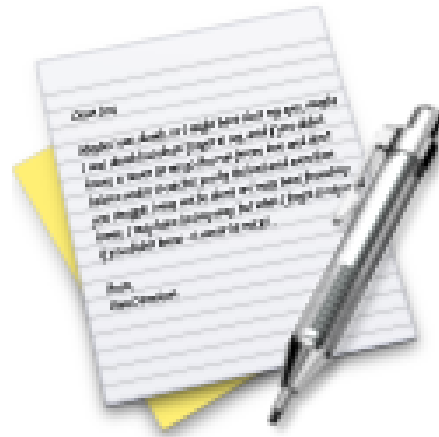### Almost every new vulnerability will have Nmap recipe

Exercise

Now lets do the exercise

Bonus: write NSE script

which is number 12 in the exercise PDF.

Exercise

Now lets do the exercise

Bonus: write NSE script

which is number 12 in the exercise PDF.

Simple Network Management Protocol

SNMP er en protokol der supporteres af de fleste professionelle netværksenheder, såsom switche, routere

hosts – skal slås til men følger som regel med

SNMP bruges til:

- *network management*
- statistik
- rapportering af fejl – SNMP traps

Sikkerheden baseres på community strings der sendes som klartekst ...

Det er nemmere at brute-force en community string end en brugerid/kodeord kombination

Brute force

Hvad betyder bruteforcing?
afprøvning af alle mulighederne

```
Hydra v2.5 (c) 2003 by van Hauser / THC <vh@thc.org>
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]]
[-o FILE] [-t TASKS] [-g TASKS] [-T SERVERS] [-M FILE] [-w TIME]
[-f] [-e ns] [-s PORT] [-S] [-vV] server service [OPT]

Options:
  -S         connect via SSL
  -s PORT    if the service is on a different default port, define it here
  -l LOGIN   or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS    or -P FILE try password PASS, or load several passwords from FILE
  -e ns      additional checks, "n" for null password, "s" try login as pass
  -C FILE    colon seperated "login:pass" format, instead of -L/-P option
  -M FILE    file containing server list (parallizes attacks, see -T)
  -o FILE    write found login/password pairs to FILE instead of stdout
...
```

Defense in depth - multiple layers of security

root

skift til root
kræver
gruppe wheel

sudo kræver
kodeord

SSHD
kræver nøgler

firewall tillader kun
SSH fra bestemte IP
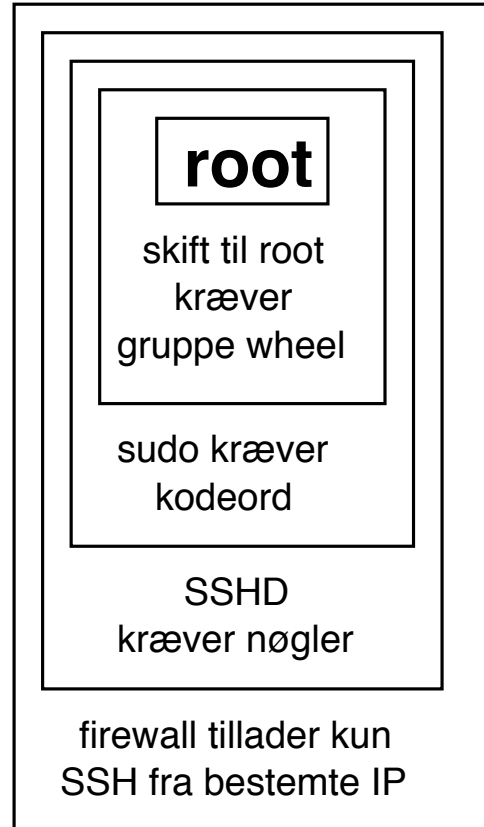
Forsvar dig selv med flere lag af sikkerhed!

Undgå standard indstillinger

Når vi scanner efter services går det nemt med at finde dem

Giv jer selv mere tid til at omkonfigurere og opdatere ved at undgå standardindstillinger

Tiden der går fra en sårbarhed annonceres på internet til den bliver udnyttet er meget kort i dag! Timer!

Ved at undgå standard indstillinger kan der måske opnås en lidt længere frist – inden ormene kommer

NB: Ingen garanti – og det hjælper sjældent mod en dedikeret angriber

Dårlige passwords og konfigurationsfejl – ofte overset

Move SSH port away from port 22/tcp

The Exploit Database – dagens buffer overflow

http://www.exploit-db.com/

Metasploit and Armitage Still rocking the internet

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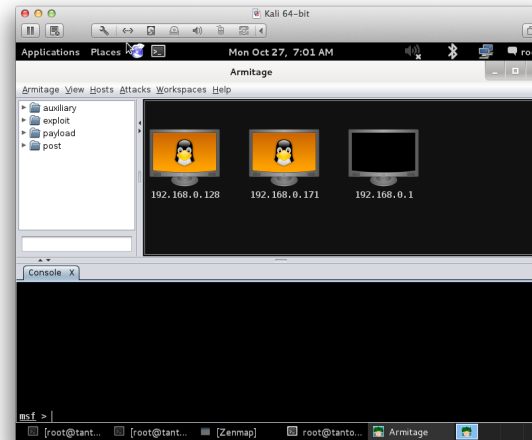
Armitage GUI fast and easy hacking for Metasploit
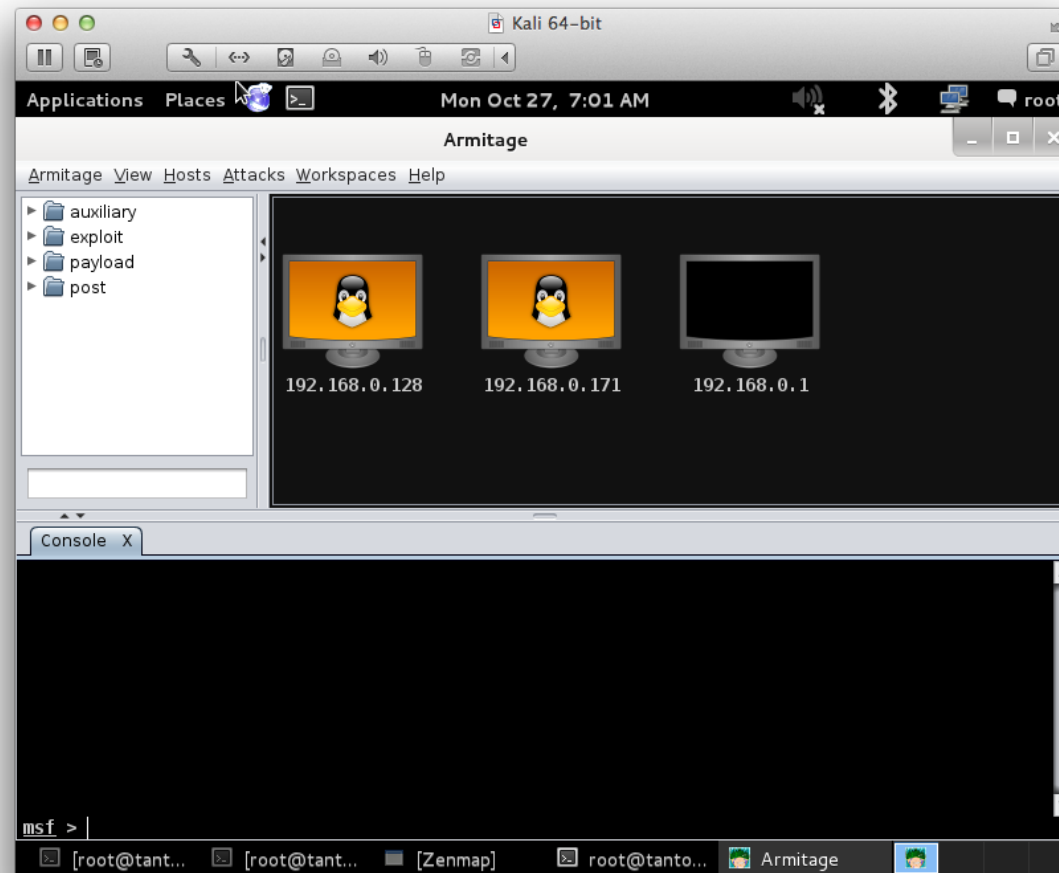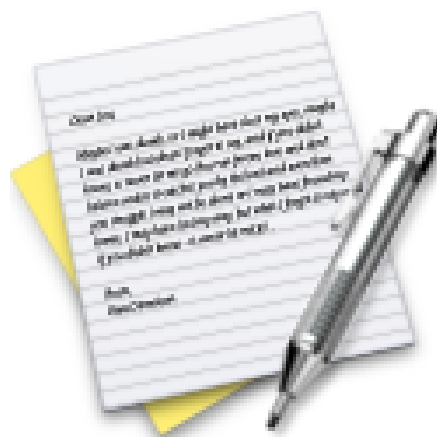`http://www.fastandeasyhacking.com/`

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

Demo: Metasploit Armitage

Exercise

Now lets do the exercise

Bonus: Try Nmap from Metasploit

which is number 14 in the exercise PDF.

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

Use Github! Der er så mange biblioteker og programmer, noget eksis-terende løser måske dit problem 90

Example introductions:

- Seven languages/database/web frameworks in Seven Weeks
- Elasticsearch the definitive guide

We are all Devops now, even security people!

Questions?

Henrik Lund Kramshøj hlk@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