



Welcome to

# Nmap Hackerworkshop

## An evening with Nmap

Henrik Lund Kramshøj [hlk@zecurity.com](mailto:hlk@zecurity.com)

Slides are available as PDF, [kramse@Github  
nmap-workshop.tex](https://github.com/kramse/security-courses/tree/main/nmap-workshop.tex) in the repo `security-courses`

# Goal



Don't Panic!

Try different scan types from graphical Zenmap and command line

Try different tools like Nping, Ndifff

Practice real-life scenarios - enabling 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 software in 1995 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 überettiget 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/>
- 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 ?

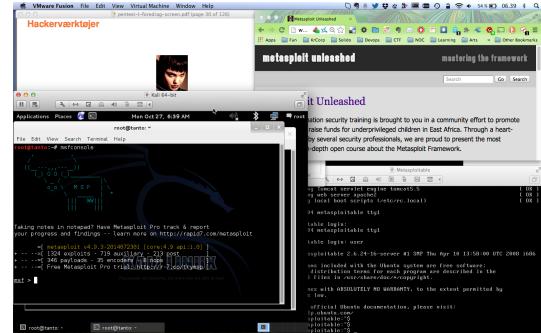
**KALI LINUX**  
"the quieter you become, the more you are able to hear"

**PENETRATION TESTING,  
REDEFINED.**

A Project By Offensive Security

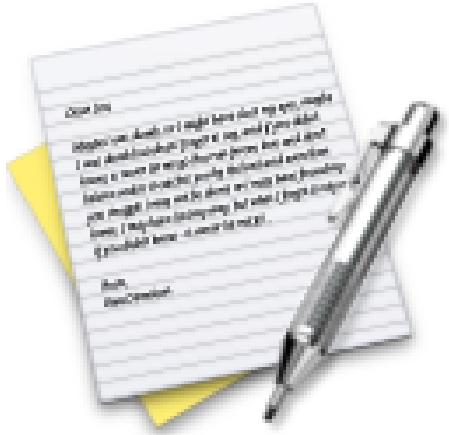
Kali <http://www.kali.org/> brings together 100s of tools  
100.000s of videos on youtube alone, searching for kali and \$TOOL  
Also versions for Raspberry Pi, mobile and other small computers

# Hackerlab setup



- Hardware: most modern laptops has CPU with virtualization  
May need to enable 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

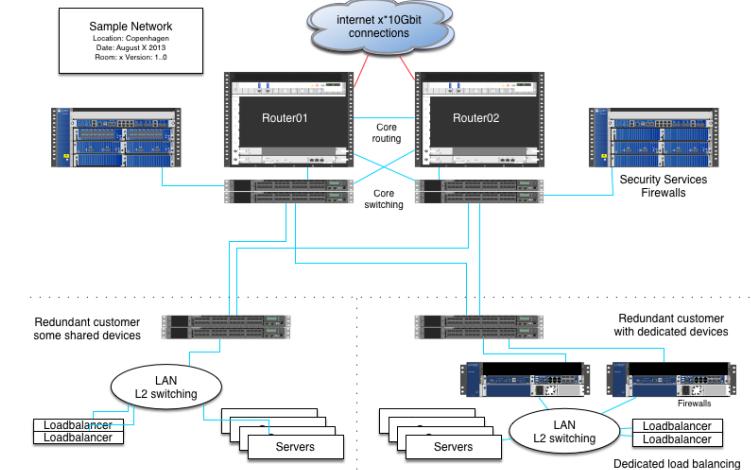


Now lets do the exercise

## Nmap install

which is number **2** in the exercise PDF.

# Scope: select systems for testing



- 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?



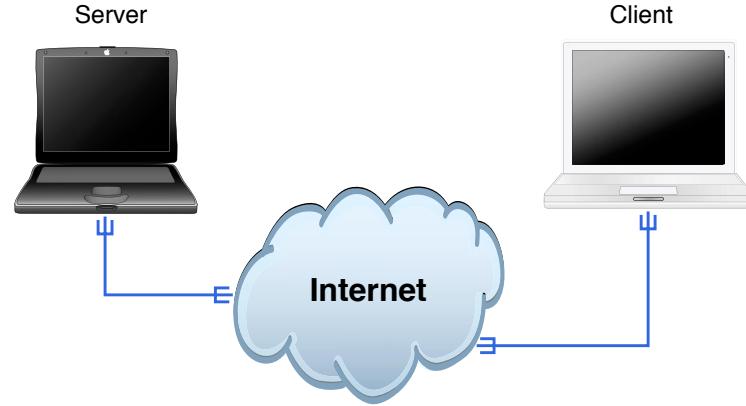
Think like a hacker

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 today



Clients and servers

Roots in academia

Protocols more than 20 years old

HTTP is becoming encrypted, but a lot other traffic is not

# Trinity breaking in



```
80/tcp      open     http  
81/tcp      open     hosts2-nc  
10 [mobile]  
11 # nmap -v -sS -O 10.2.2.2  
11  
13 Starting nmap 0.2.54BETA25  
13 Insufficient responses for TCP sequencing (3), OS detection is  
13 inaccurate  
14 Interesting ports on 10.2.2.2:  
14 (The 1539 ports scanned but not shown below are in state: clo  
51 Port      State    Service  
51 22/tcp    open     ssh  
58  
68 No exact OS matches for host  
68  
24 Nmap run completed -- 1 IP address (1 host up) scanned  
50 # sshnuke 10.2.2.2 -rootpw="Z10H0101"  
   Connecting to 10.2.2.2:ssh ... successful.  
Re Attempting to exploit SSHv1 CRC32 ... successful.  
IP Resetting root password to "Z10H0101".  
System open: Access Level <9>  
Hn # ssh 10.2.2.2 -l root  
root@10.2.2.2's password: ■
```

RTF CONTROL  
ACCESS GRANTED

Nmap has been featured in twelve movies:

<https://nmap.org/movies/>

[https://youtu.be/511GCTgqE\\_w](https://youtu.be/511GCTgqE_w)

## 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! Includes other tools!

Lets check release notes, 7.70 pt.

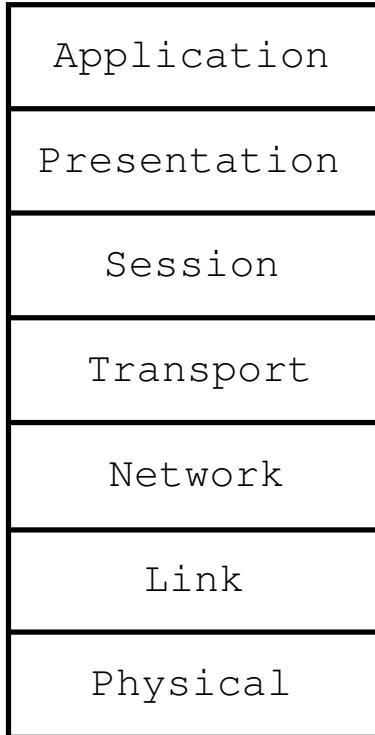
<http://seclists.org/nmap-announce/2018/0>

Bonus info: you can help Nmap by submitting fingerprints

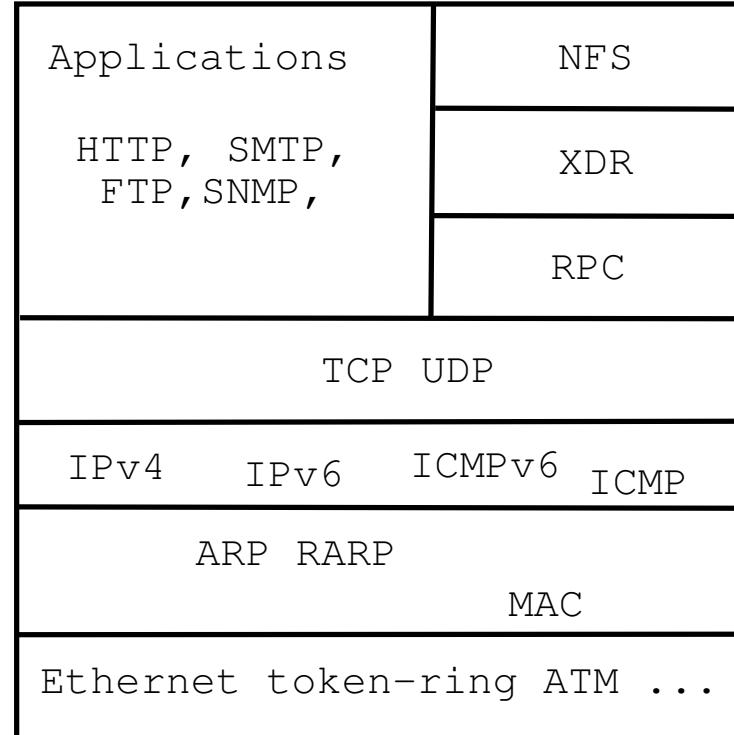
# OSI og Internet modellerne



OSI Reference Model



Internet protocol suite



# Wireshark – capture and dissect network packets



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 ▶](#)

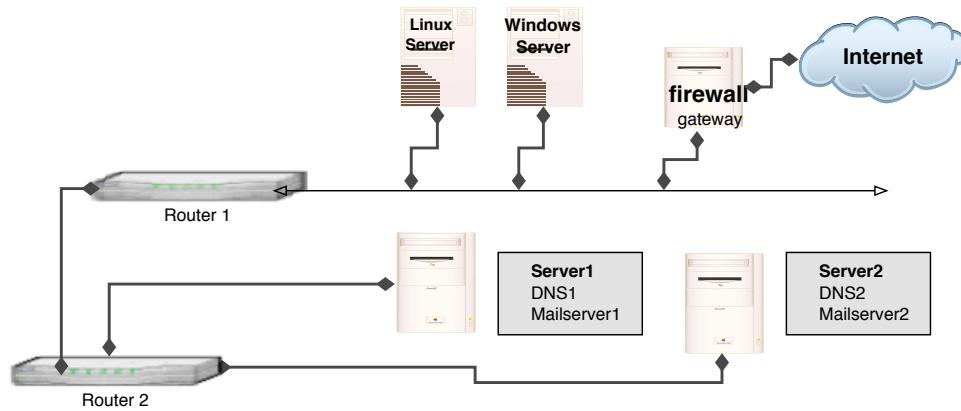
<https://www.wireshark.org>

# Using Wireshark



Filtering is a basic but advanced function

# Network mapping



Using traceroute and similar programs it is often possible to make educated guess to network topology

Time to live (TTL) for packets are decreased when crossing a router

when it reaches zero the packet is timed out, and ICMP message sent back to source

Default Unix traceroute uses UDP, Windows tracert use ICMP

# traceroute – 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
```

Low TTL, UDP, high ports above 33000 = Unix traceroute signature

# Basic port scanning



What is a port scan

Testing all values possible for port number from 0/1 to 65535

Goal is to identify open ports, listening and vulnerable services

Most often TCP og UDP scan

TCP scanning is more reliable than UDP scanning

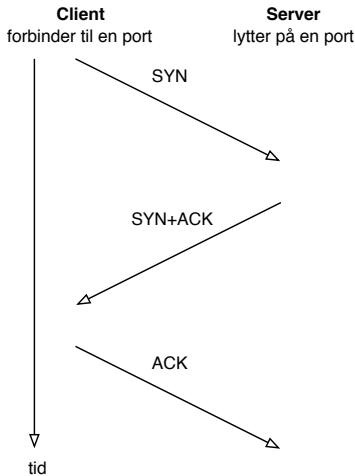
TCP handshake must respond with SYN-ACK packets

UDP applications respond differently – if they even respond

so probes with real requests may get response, no firewall they respond with ICMP on closed ports

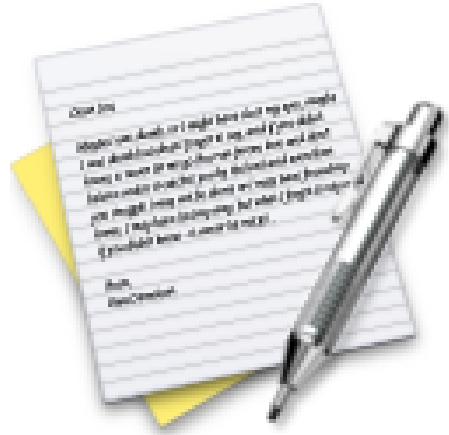
Use the GUI program Zenmap while learning Nmap

# TCP three-way handshake



- **TCP SYN half-open** scans
- in the old days systems would only log a full TCP connection – so it was a *stealth*-scans
- Today system and IDS intrusion detection can easily monitor for this
- Sending a lot of SYN packets can create a Denial of Service – **SYN-flooding**

# Exercise

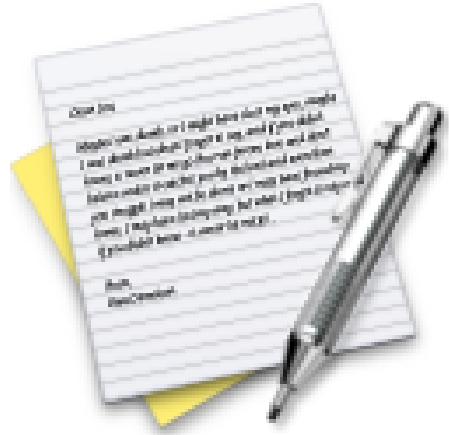


Now lets do the exercise

## 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 and port sweep



Scans across the network are named sweeps

Ping sweeps using ICMP Ping probes

Port sweep trying to find a specific service, like port 80 web

Quite easy to see in network traffic:

- Selecting two IP-addresses not in use
- Should not see any traffic, but if it does, its being scanned
- If traffic is received on both addresses, its a sweep – if they are a bit apart it is even better, like 10.0.0.100 and 10.0.0.200

Pro tip: a Great network intrusion detection engine (IDS), is Suricata [suricata-ids.org](http://suricata-ids.org)

# Nmap port sweep for web servers



```
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 for 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
```

More reliable to use Nmap script with probes like `--script=snmp-info`

# 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).

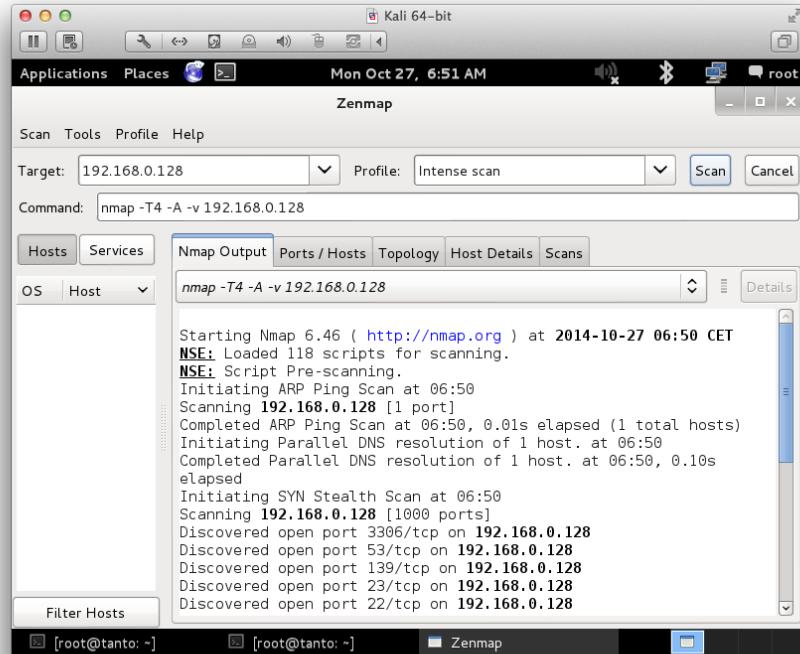
PORT      STATE      SERVICE VERSION
80/tcp    open       http      Apache httpd 2.2.26 ((Unix) DAV/2 mod_ssl/2.2.26 OpenSSL/0.9.8zc)
|_http-title: Site doesn't have a title (text/html).

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/
```

- Low-level way to identify operating systems, also try/use `nmap -A`
- Send probes and observe responses, lookup in table of known OS and responses
- Techniques known since at least: *ICMP Usage In Scanning* Version 3.0, Ofir Arkin, 2001

# Portscan using Zenmap GUI



Zenmap included in the full Nmap package <https://nmap.org>

# Exercise

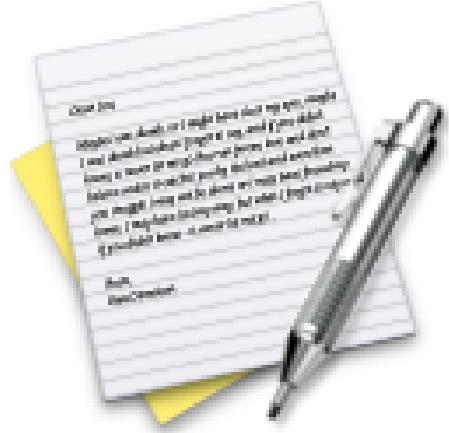


Now lets do the exercise

## Discover active systems ping sweep

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

# Exercise

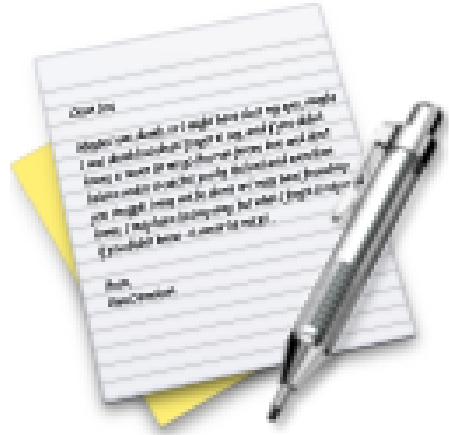


Now lets do the exercise

## 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

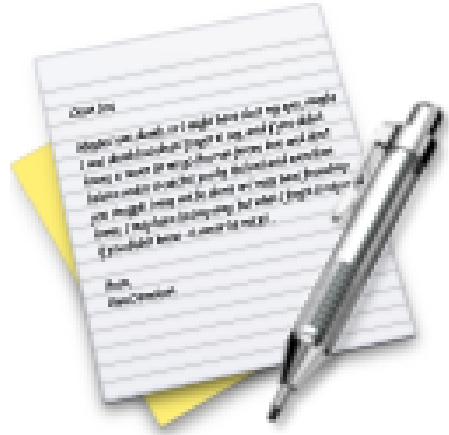


Now lets do the exercise

## 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.

## Experiences gathered



Lots of information

Reveals a lot about the network, operating systems, services etc.

I use a template when getting data

- Respond to ICMP:  echo,  mask,  time
- Respond to traceroute:  ICMP,  UDP
- Open ports TCP og UDP:
- Operating system:
- ... (banner information )

Beware when doing scans it is possible to make routers, firewalls and devices perform badly or even crash!

# Exercise

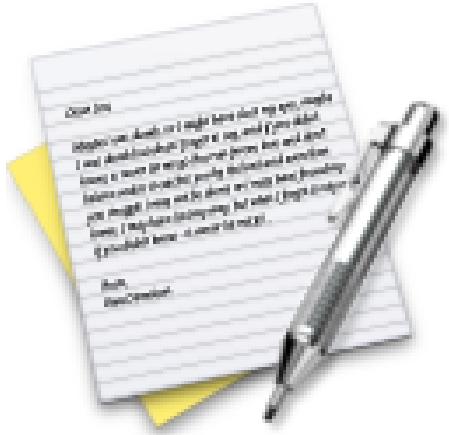


Now lets do the exercise

## Reporting HTML

which is number **10** in the exercise PDF.

# Exercise



Now lets do the exercise

## Nping check ports

which is number **11** 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 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 09.1...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

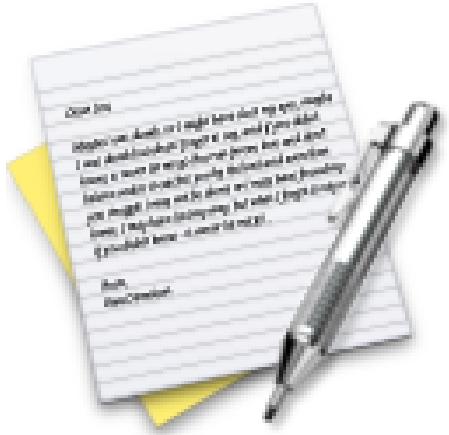


Now lets do the exercise

## Nmap Scripting Engine NSE scripts

which is number **12** in the exercise PDF.

# Exercise

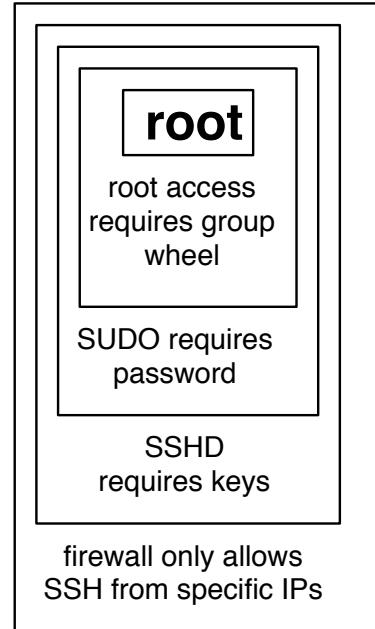


Now lets do the exercise

## Bonus: write NSE script

which is number **13** in the exercise PDF.

# Defense in depth - multiple layers of security



Multiple layers of security!

# The Exploit Database



**EXPLOIT DATABASE**

Verified Has App

Show 15 ▾

Search:

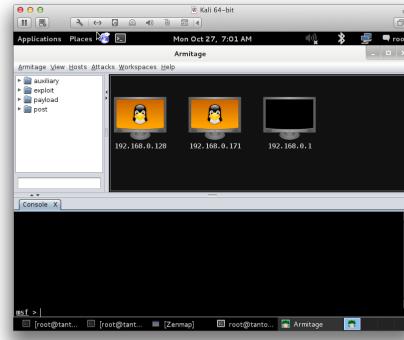
Date	D	A	V	Title	Type	Platform	Author
2019-02-25	1	2	3	Drupal < 8.6.9 - REST Module Remote Code Execution	WebApps	PHP	leonjza
2019-02-25	1	2	3	Xlight FTP Server 3.9.1 - Buffer Overflow (PoC)	DoS	Windows	Logan Whitmire
2019-02-25	1	2	3	Advance Gift Shop Pro Script 2.0.3 - SQL Injection	WebApps	PHP	Mr Winst0n
2019-02-25	1	2	3	News Website Script 2.0.5 - SQL Injection	WebApps	PHP	Mr Winst0n
2019-02-25	1	2	3	PHP Ecommerce Script 2.0.6 - Cross-Site Scripting / SQL Injection	WebApps	PHP	Mr Winst0n
2019-02-25	1	2	3	zzzphp CMS 1.6.1 - Remote Code Execution	WebApps	PHP	Yang Chenglong
2019-02-25	1	2	3	Jenkins Plugin Script Security 1.49/Declarative 1.3.4/Groovy 2.60 - Remote Code Execution	WebApps	Java	wetw0rk
2019-02-23	1	2	3	Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution	WebApps	PHP	Charles Fol
2019-02-22	1	2	3	Teracue ENC-400 - Command Injection / Missing Authentication	WebApps	Hardware	Stephen Shkardo0n
2019-02-22	1	2	3	Micro Focus Flir 3.4.0.217 - Path Traversal / Local Privilege Escalation	WebApps	Linux	SecureAuth
2019-02-22	1	2	3	Nuuo Central Management - Authenticated SQL Server SQL Injection (Metasploit)	Remote	Windows	Metasploit
2019-02-22	1	2	3	WebKit JSC - reifyStaticProperty Needs to set the PropertyAttribute::CustomAccessor flag for CustomGetterSetter	DoS	Multiple	Google Security Research
2019-02-22	1	2	3	Quest NetVault Backup Server < 11.4.5 - Process Manager Service SQL Injection / Remote Code Execution	WebApps	Multiple	Chris Anastasio
2019-02-21	1	2	3	AirDrop 2.0 - Denial of Service (DoS)	DoS	Android	s4vitar
2019-02-21	1	2	3	MikroTik RouterOS < 6.43.12 (stable) / < 6.42.12 (long-term) - Firewall and NAT Bypass	Remote	Hardware	Jacob Baines

Showing 1 to 15 of 40,914 entries

FIRST PREVIOUS 1 2 3 4 5 ... 2728 NEXT LAST

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

# Metasploit and Armitage Still rocking the internet



<http://www.metasploit.com/>

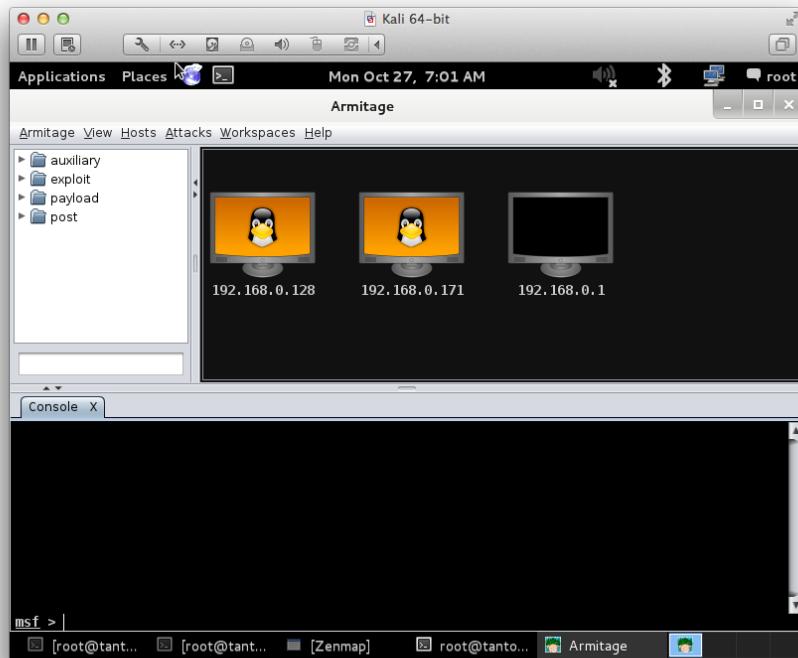
Armitage GUI fast and easy hacking for Metasploit

<http://www.fastandeasyhacking.com/>

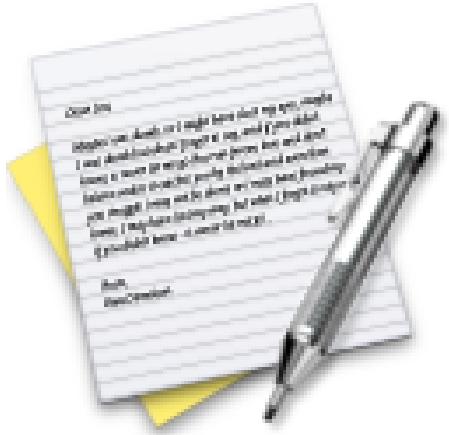
Recommended training Metasploit Unleashed

[http://www.offensive-security.com/metasploit-unleashed/Main\\_Page](http://www.offensive-security.com/metasploit-unleashed/Main_Page)

# Demo: Metasploit Armitage



# Exercise



Now lets do the exercise

## 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! So many libraries and programs that can help, maybe solve 90% of your problem, and you can glue the rest together

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@zecurity.com](mailto:hlk@zecurity.com)

Need help with infrastructure security or pentesting, ask me!

You are always welcome to send me questions later via email