Welcome to

Security Update

End of 2018

Henrik Lund Kramshøj hlk@zencurity.dk

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

Security areas to look into when 2019 comes around.

Very short presentation intended to create security awareness by listing some of the security problems we face. Then listing some ideas, methods and tools to improve the situation.

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Goals for today

Discuss IT-security

Create Awareness

Client security

Server security

Short pentest introduction

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Paranoia defined

par·a·noi·a

/ˌparəˈnoiə/

noun

noun: **paranoia**

1. a mental condition characterized by delusions of persecution, unwarranted jealousy, or exaggerated self-importance, typically elaborated into an organized system. It may be an aspect of chronic personality disorder, of drug abuse, or of a serious condition such as schizophrenia in which the person loses touch with reality.
   synonyms: persecution complex, delusions, obsession, psychosis More
   - suspicion and mistrust of people or their actions without evidence or justification.
     "the global paranoia about hackers and viruses"

Origin

GREEK

para
irregular

GREEK

noos
mind

→ GREEK

paranoos
distracted

→ MODERN LATIN

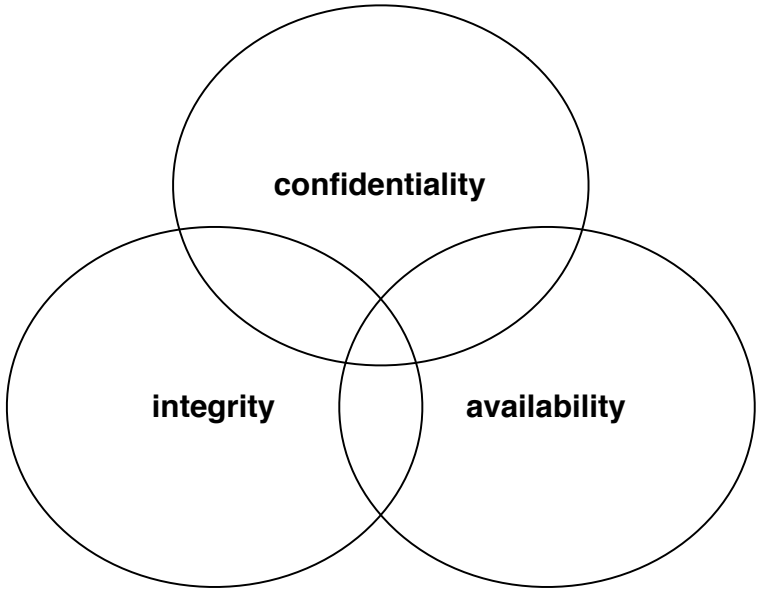
paranoia
early 19th cent.

More

Source: google paranoia definition

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Confidentiality Integrity Availability



We want to protect something

Confidentiality - data holdes hemmelige

Integrity - data ændres ikke uautoriseret

Availability - data og systemet er tilgeængelig når de skal bruges

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

What is data?

Personal data you dont want to loose:

- Wedding pictures
- Pictures of your children
- Sextapes
- Personal finances

Source: picture of my son less than 24 hours old - precious!

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

The current situation

Internet security sucks, 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

New vulnerabilities, while we are already dealing with those from yesterday

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

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/`

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

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.

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Exploits og sårbarheder

Exploits som Heartbleed udnytter sårbarheder

Kræver nogle forudsætninger

Sårbarheder i software

Sårbarheder pga dårlige indstillinger

Dårlige passwords

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Clients

Vores client systemer er idag oftest:

Laptops

Mobile enheder

Delte stationære

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Malware charateristics

Malware is advanced and sophisticated

Modular frameworks

Use strong cryptography to hide, and hide your data ransomware

Use 0-day exploits - unknown to others

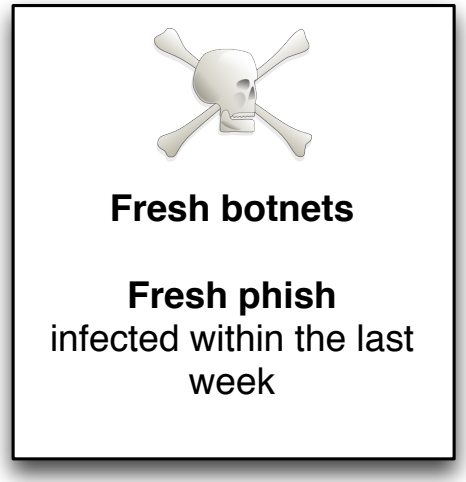
Use rootkits to stay under radar and avoid anti-virus

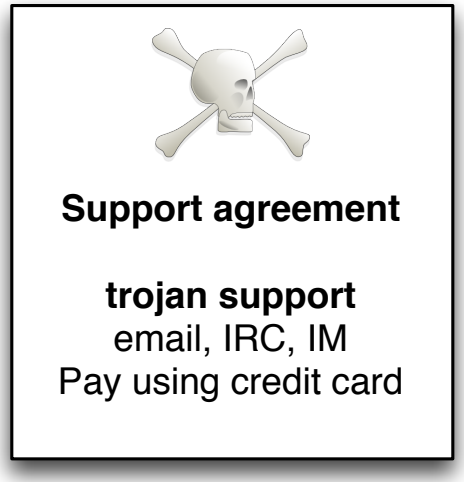
Mutate and change to avoid detection

In general less noisy

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Botnets and malware sold with support





Malware programmers act like software houses

"Buy this version with updates and support"

Rent a bot net with 100.000 computers

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Phishing - Receipt for Your Payment to mark561@bt.....com

Mark Willson
145 Church Lane East
Aldershot, Hampshire, GU11 3ST
United Kingdom

Important Note: Mark Willson has provided an Unconfirmed Address. If you are planning on shipping items to Mark Willson, please check the Transaction Details page of this payment to find out whether you will be covered by the PayPal Seller Protection Policy.

Note:

If you haven't authorized this charge ,click the link below to cancel transaction

Cancel Transaction:

https://www.paypal.com/cgi-bin/webscr/cgi-bin/webscr?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

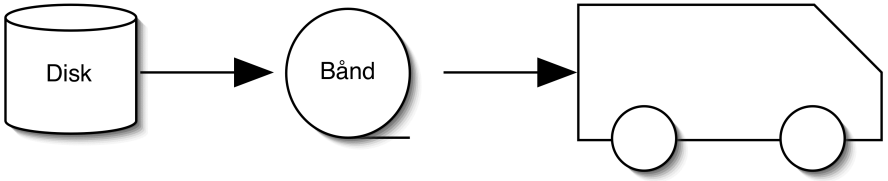
*SSL connection:
PayPal automatically encrypts your confidential information in transit from your computer to ours using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available)
---

http://paypal-co.uk.dt6.pl/?login-run.webscrcmd=_account-run.CaseIDNumberPP-046-631-789

Do you recognize Phishing?

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Client sikkerhed - Back to basics



opbevaring af sikkerhedskopi væk fra systemer

Opdateringer er altid nødvendige, vi skal opfordre til opdateringer

Firewall aktiveret altid

Phishing og exploits via email - spearphishing er stor risiko

Procedurer og rapportering, gør det nemt

Backups gør at vi kan opdatere uden risiko, genskabe data

PS Måske bruges en cloud service istedet for bånd, men offline er godt

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Risk management defined

Information Risk Management

Life is full of risk.

Risk is the possibility of damage happening and the ramifications of such damage should it occur. ***Information risk management (IRM)*** is the *process* of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. There is no such thing as a 100 percent secure environment. Every environment has vulnerabilities and threats to a certain degree. The skill is in identifying these threats, assessing the probability of them actually occurring and the damage they could cause, and then taking the right steps to reduce the overall level of risk in the environment to what the organization identifies as acceptable.

Source: Shon Harris *CISSP All-in-One Exam Guide*

We all take risks every day - sometimes even calculated risk

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Server sikkerhed

Vi mener servere, og tilhørende infrastruktur

Servere - server OS og applikationer

KVM: IPMI, Dell DRAC, HP ILO, adskilte management netværk

Netværksenheder brug VPN til at tilgå alle administrative interfaces

Firewalls - naturligvis, men flere zoner, DMZ

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Solutions

Automate your job, Ansible is our preferred tool

Backup your life, help others backup, Duplicity is my choice

Use hackertools to detect and identify

Categorise, sort, prioritize, group problems - solve more

Measure, collect and present - make it pretty

Learn from devops, Elasticsearch Logstash Kibana, Grafana

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

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Daily operations

Asset ownership Routers, servers, network devices, services

User management Lots of things, including Active Directory

Patch management

Host and services ownership, who owns the services

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Monthly and quarterly checks

Crypto stuff HTTPS certificates, TLS in general, use 4k keys, TLS 1.2+, `https://www.ssllabs.com/`

VPN settings: IPsec, VPN, L2TP, key lengths, roll shared PSK

Routing, internet service provider contacts, whois

Firewall review - read all rules, disable unneeded

Review DNS and mail settings, DMARC, DNSSEC, DKIM

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Use standard to take Charge of Your Security

Multiple standards:

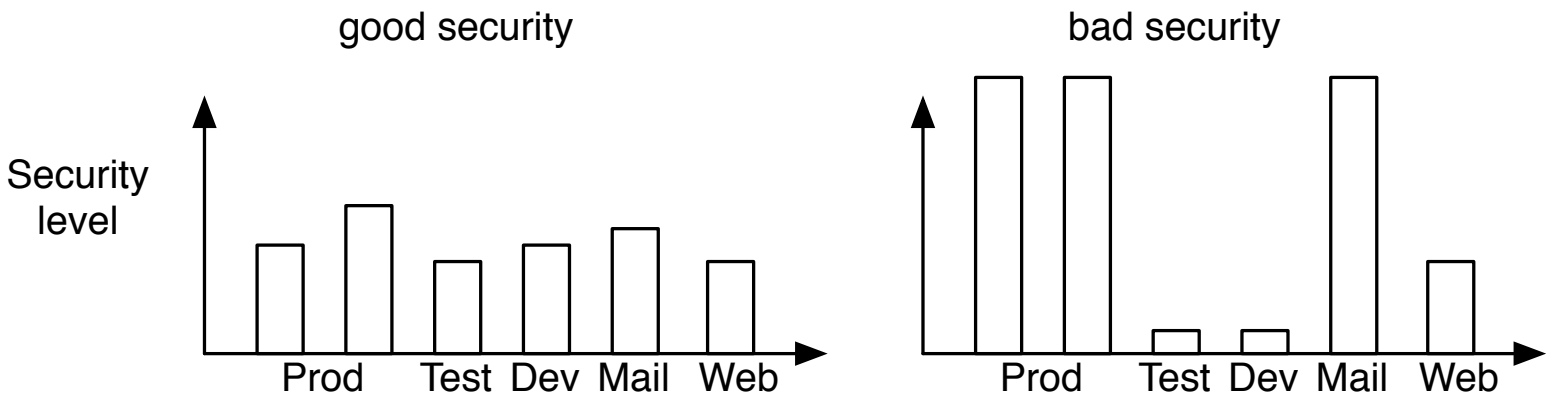
- ISO/IEC 27001 - information security management system standards
  `http://en.wikipedia.org/wiki/ISO/IEC_27001`
- SSAE 16 No. 16, Reporting on Controls at a Service Organization
  Statement on Standards for Attestation Engagements (SSAE) `http://ssae16.com/`
- ISAE 3402 Assurance Reports on Controls at a Service Organization
  International Standard on Assurance Engagements (ISAE) `http://isae3402.com/`
- Independent assessment from a trusted security firm - which must often also be certified
- Physical Security, power, HVAC - trusted partners reviewing security
- Implementing standards is also security

Over the years organisations have become more mature with regards to security

Implementing security controls were easier when you owned all resources

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Balanced security



Better to have the same level of security

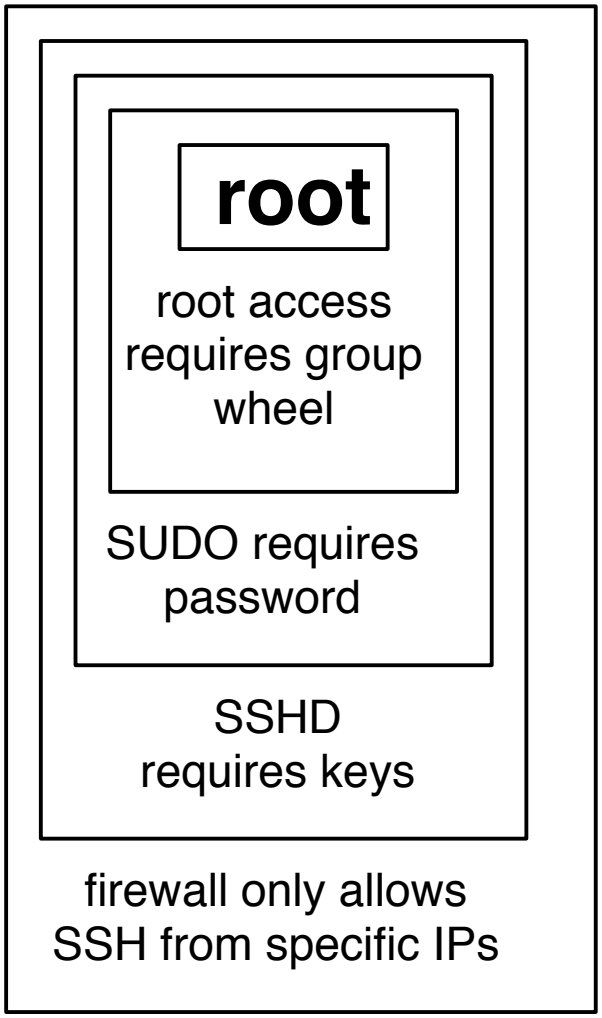
If you have bad security in some part - guess where attackers will end up

Hackers are not required to take the hardest path into the network

Realize there is no such thing as 100% security

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Defense in depth - layered security



Multiple layers of security! Isolation!

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

First advice use the modern operating systems

Newer versions of Microsoft Windows, Mac OS X and Linux

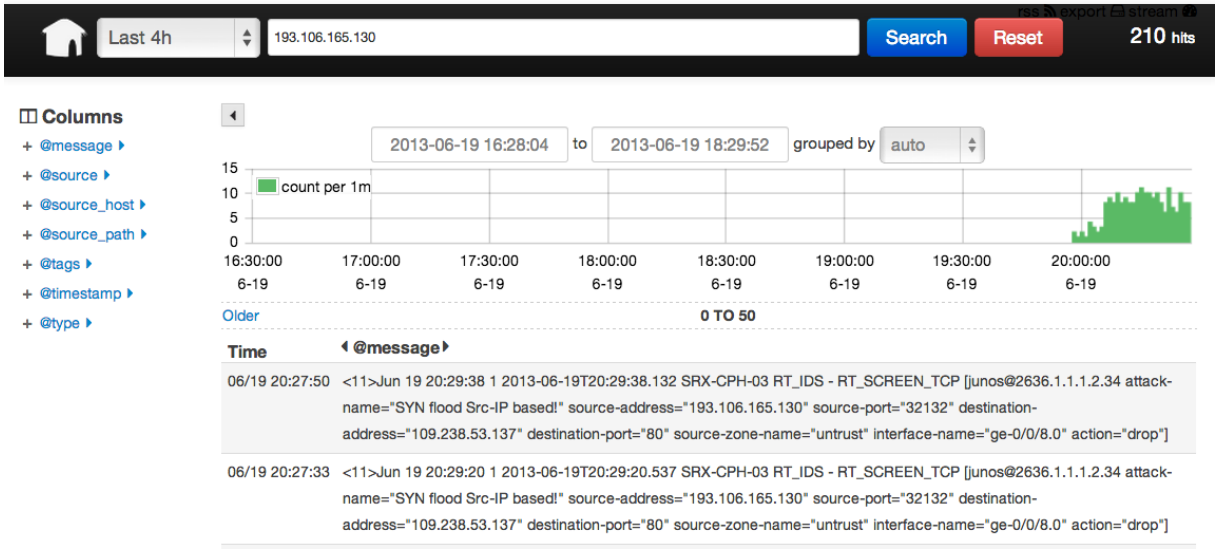
- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

Note: these still have errors and bugs, but are better than older versions

Always try to make life worse and more costly for attackers

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Network 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, called ELK stack or Elastic stack

Packetbeat `https://www.elastic.co/products/beats/packetbeat`

Collect and present data more easily - non-programmers

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Security engineering som job rolle

On any given day, you may be challenged to:

Create new ways to solve existing production security issues
Configure and install firewalls and intrusion detection systems
Perform vulnerability testing, risk analyses and security assessments
Develop automation scripts to handle and track incidents
Investigate intrusion incidents, conduct forensic investigations and incident responses
Collaborate with colleagues on authentication, authorization and encryption solutions
Evaluate new technologies and processes that enhance security capabilities
Test security solutions using industry standard analysis criteria
Deliver technical reports and formal papers on test findings
Respond to information security issues during each stage of a project's lifecycle
Supervise changes in software, hardware, facilities, telecommunications and user needs
Define, implement and maintain corporate security policies
Analyze and advise on new security technologies and program conformance
Recommend modifications in legal, technical and regulatory areas that affect IT security

Source: https://www.cyberdegrees.org/jobs/security-engineer/
also https://en.wikipedia.org/wiki/Security_engineering

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Pentesting as example

Penetration testing

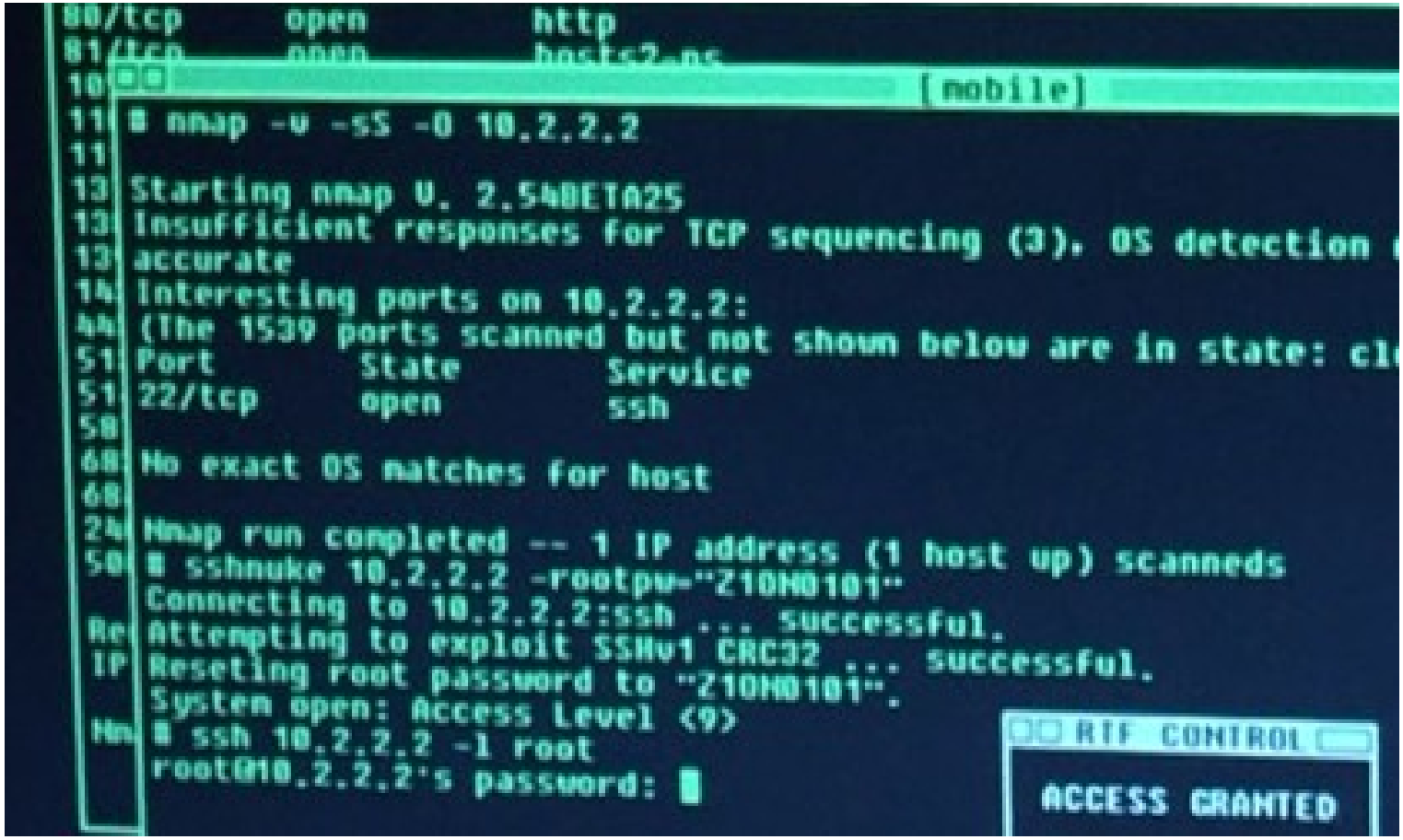
Kontrol af sikkerheden

Bruger aktive værktøjer

Brug Nmap pakken til at checke åbne porte

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Trinity breaking in

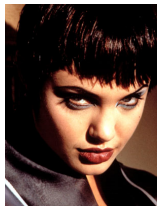


http://nmap.org/movies.html

Meget realistisk https://www.youtube.com/watch?v=0PxTAn4g20U

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

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/`

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

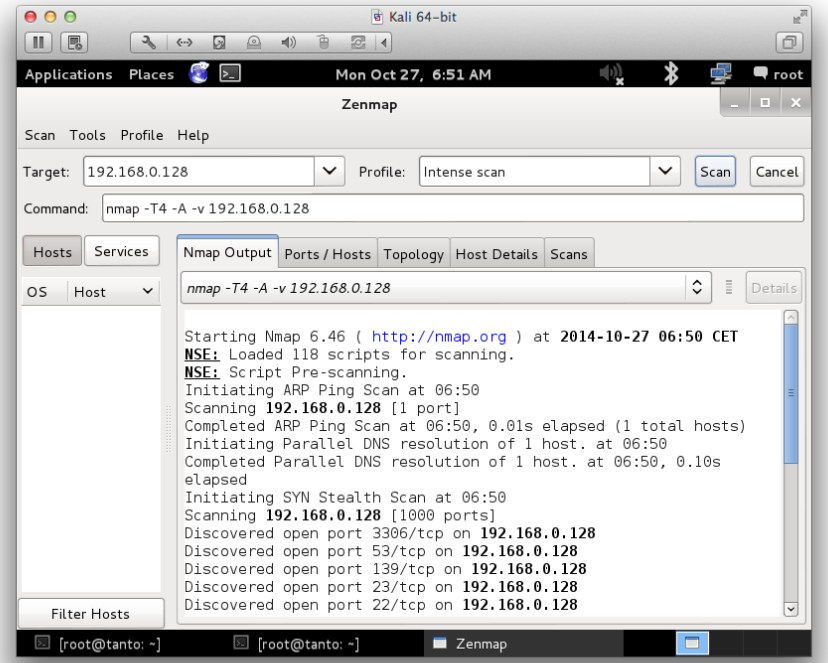
Nping - ligesom ping, blot med flere protokoller

```
root@KaliVM:~# nping --tcp -p 80 www.zencurity.com

Starting Nping 0.7.70 ( https://nmap.org/nping ) at 2018-09-07 19:06 CEST
SENT (0.0300s) TCP 10.137.0.24:3805 > 185.129.60.130:80 S ttl=64 id=18933 iplen=40  seq=2984847972 win=1480
RCVD (0.0353s) TCP 185.129.60.130:80 > 10.137.0.24:3805 SA ttl=56 id=49674 iplen=44  seq=3654597698 win=1638
SENT (1.0305s) TCP 10.137.0.24:3805 > 185.129.60.130:80 S ttl=64 id=18933 iplen=40  seq=2984847972 win=1480
RCVD (1.0391s) TCP 185.129.60.130:80 > 10.137.0.24:3805 SA ttl=56 id=50237 iplen=44  seq=2347926491 win=1638
SENT (2.0325s) TCP 10.137.0.24:3805 > 185.129.60.130:80 S ttl=64 id=18933 iplen=40  seq=2984847972 win=1480
RCVD (2.0724s) TCP 185.129.60.130:80 > 10.137.0.24:3805 SA ttl=56 id=9842 iplen=44  seq=2355974413 win=16384
SENT (3.0340s) TCP 10.137.0.24:3805 > 185.129.60.130:80 S ttl=64 id=18933 iplen=40  seq=2984847972 win=1480
RCVD (3.0387s) TCP 185.129.60.130:80 > 10.137.0.24:3805 SA ttl=56 id=1836 iplen=44  seq=3230085295 win=16384
SENT (4.0362s) TCP 10.137.0.24:3805 > 185.129.60.130:80 S ttl=64 id=18933 iplen=40  seq=2984847972 win=1480
RCVD (4.0549s) TCP 185.129.60.130:80 > 10.137.0.24:3805 SA ttl=56 id=62226 iplen=44  seq=3033492220 win=1638

Max rtt: 40.044ms | Min rtt: 4.677ms | Avg rtt: 15.398ms
Raw packets sent: 5 (200B) | Rcvd: 5 (220B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 4.07 seconds
```

Byg pakkerne med kommandolinien

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Nmap GUI - Zenmap



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

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

Aktiv testing 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

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

Kali Linux the pentest toolbox

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

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

Also versions for Raspberry Pi, mobile and other small computers

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)
```

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

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
```

© license CC BY 3.0. 2018 Henrik Lund Kramshøj

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