Welcome to

Hacking - protect yourself

Henrik Lund Kramshøj hlk@zencurity.com

Slides are available as PDF, kramse@Github

hacking-protect-yourself-short.tex in the repo security-courses

Goal of this presentation

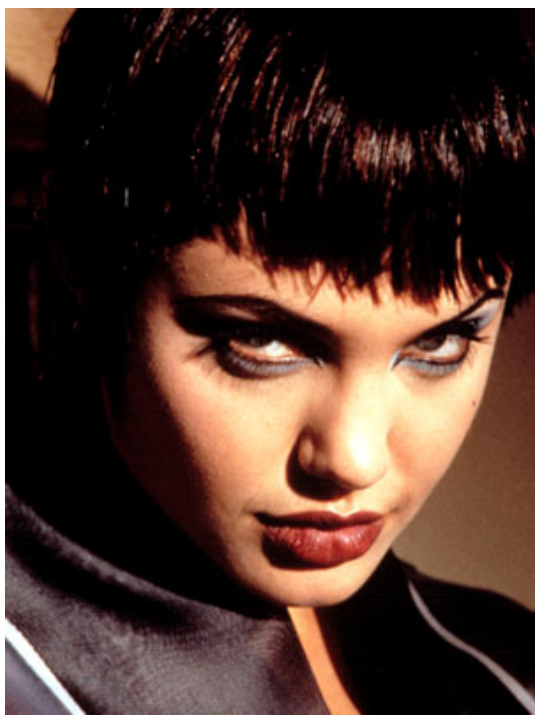
Don't Panic!

Introduce hacking and a couple of hacker tools

List some tools that can be used to protect your computer and data

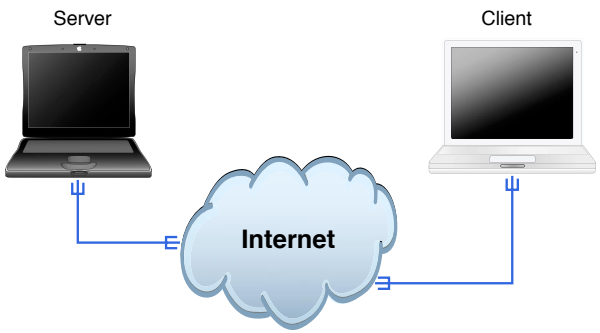
PS Sorry about the many TLAs ... og danglish

Introduktion til hacking



http://www.imdb.com/title/tt0113243/ Hackers (1995)

Internet today



Clients and servers

Rooted in academic networks

Protocols which are more than 20 years old, moved to TCP/IP in 1981

Trying to migrate to IPv6 - a lot of hacking opportunities here

Hackers don’t give a shit

Your system is only for testing, development, ...

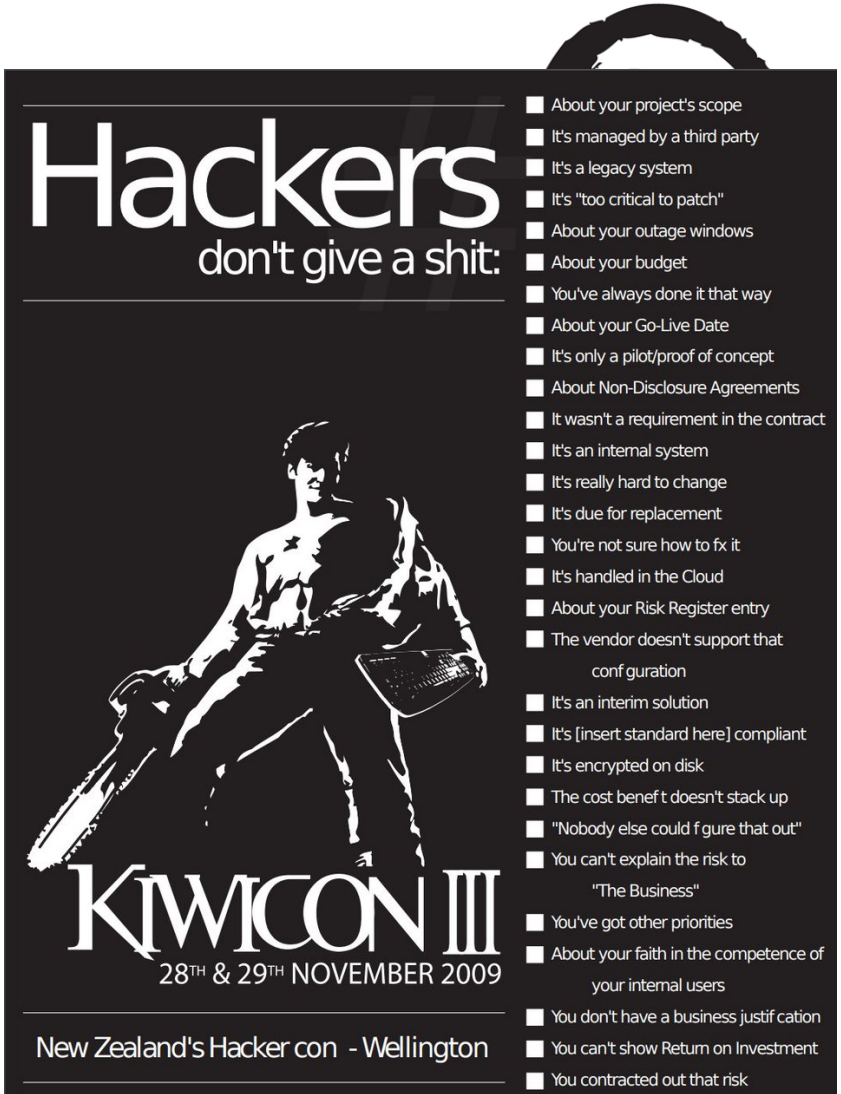
Your network is a research network, under construction, being phased out, ...

Try something new, go to your management

Bring all the exceptions, all of them, update the risk analysis figures - if this happens it is about 1mill DKK

Ask for permission to go full monty on your security

Think like attackers - don’t hold back



Hacker - cracker

Det korte svar - drop diskussionen

Det havde oprindeligt en anden betydning, men medierne har taget udtrykket til sig - og idag har det begge betydninger.

Idag er en hacker stadig en der bryder ind i systemer!

ref. Spafford, Cheswick, Garfinkel, Stoll, ... - alle kendte navne indenfor sikkerhed

- *Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Clifford Stoll
- *Hackers: Heroes of the Computer Revolution*, Steven Levy
- *Practical Unix and Internet Security*, Simson Garfinkel, Gene Spafford, Alan Schwartz

Internet er åbne standarder!

We reject kings, presidents, and voting.
We believe in rough consensus and running code.
– The IETF credo Dave Clark, 1992.

Request for comments - RFC - er en serie af dokumenter

RFC, BCP, FYI, informational
de første stammer tilbage fra 1969

Ændres ikke, men får status Obsoleted når der udkommer en nyere version af en standard

Standards track:
Proposed Standard $\rightarrow$ Draft Standard $\rightarrow$ Standard

Åbne standarder = åbenhed, ikke garanti for sikkerhed

Hacking seems like magic

Hacking looks like magic

Hacking is not magic

- Hacking only requires some ninja training
- We have been doing this since at least 1995 when SATAN was released
- Listen, Plan, Act, Do hacking

The Internet Worm 2. nov 1988

Udnyttede følgende sårbarheder

- buffer overflow i fingerd - VAX kode
- Sendmail - DEBUG
- Tillid mellem systemer: rsh, rexec, ...
- dårlige passwords

Avanceret + camouflage!

- Programnavnet sat til 'sh'
- Brugte fork() til at skifte PID jævnligt
- password cracking med intern liste med 432 ord og /usr/dict/words
- Fandt systemer i /etc/hosts.equiv, .rhosts, .forward, netstat ...

Lavet af Robert T. Morris, Jr.

Medførte dannelsen af CERT, `http://www.cert.org`

God sikkerhed

Gå efter ensartet sikkerhed på tværs istedet!

Aftale om test af netværk

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

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
- Frit efter: `http://www.stophacking.dk` lavet af Det Kriminalpræventive Råd
- Frygten for terror har forstærket ovenstående - så lad være!

Gode råd til jer

Brug teknologien

Lær teknologien at kende - læs manualen!

Tænk på følsomheden af data I gemmer og overfører

- Slå ting fra som I ikke bruger
- Slå bluetooth fra når I ikke bruger den
- Opdater softwaren på enheden
- Slå kryptering til hvor I kan: IMAP**S**, POP3**S**, HTTP**S** og over bluetooth
- Brug låsekode fremfor tastaturlås uden kode på mobiltelefonen
- Stol ikke for meget på fingertryksaflæsere

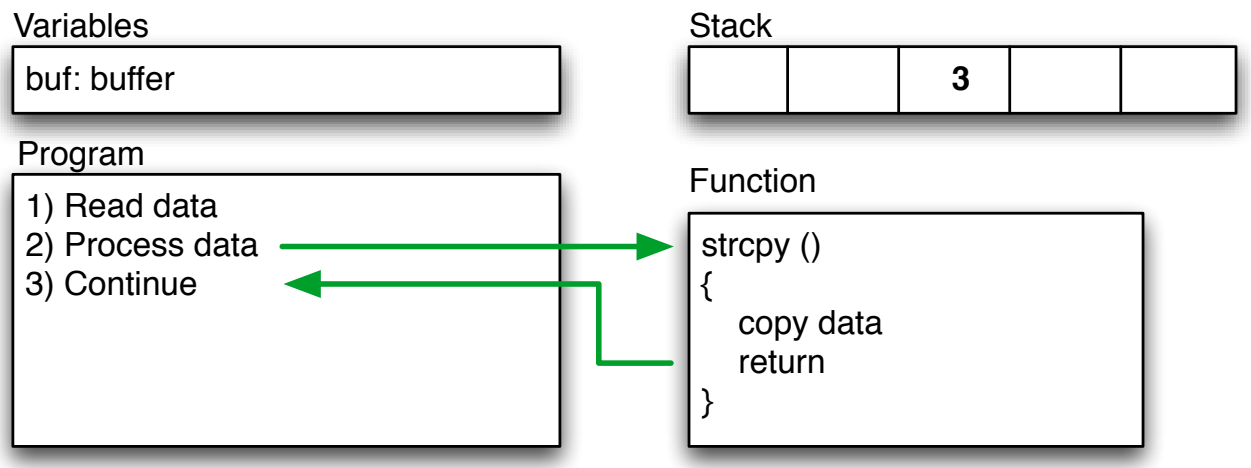
Teknisk hvad er hacking

buffer overflows et C problem

Et buffer overflow er det der sker når man skriver flere data end der er afsat plads til i en buffer, et dataområde. Typisk vil programmet gå ned, men i visse tilfælde kan en angriber overskrive returadresser for funktionskald og overtage kontrollen.

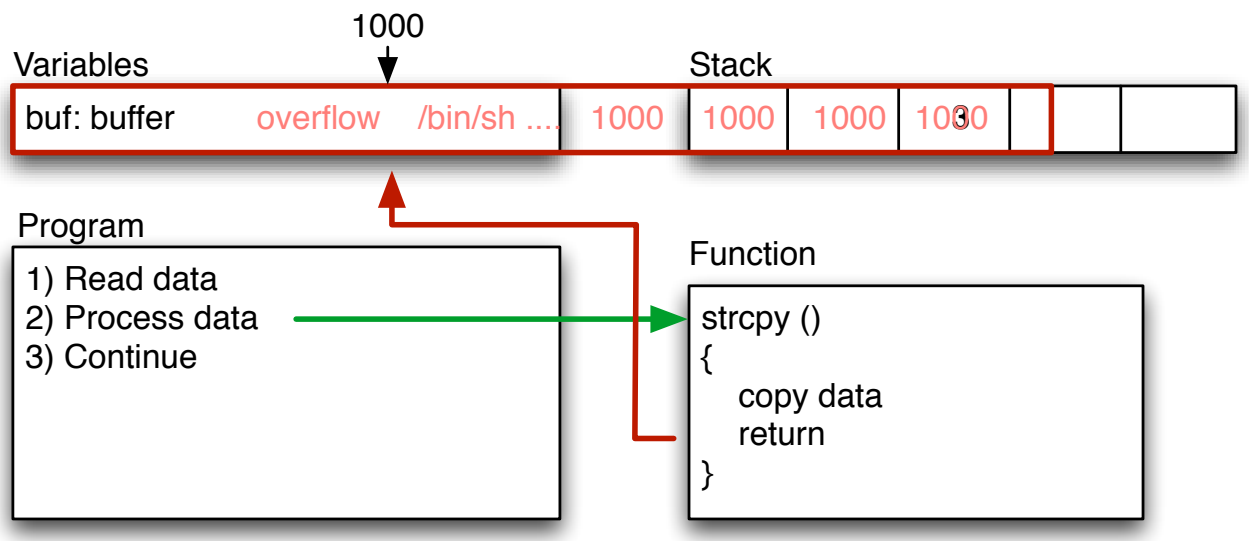
Stack protection er et udtryk for de systemer der ved hjælp af operativsystemer, programbiblioteker og lign. beskytter stakken med returadresser og andre variable mod overskrivning gennem buffer overflows. StackGuard og Propolice er nogle af de mest kendte.

Buffer og stacks




```
main(int argc, char **argv)
{       char buf[200];
         strcpy(buf, argv[1]);
         printf("%s\n",buf);
}
```

Overflow - segmentation fault



Bad function overwrites return value!

Control return address

Run shellcode from buffer, or from other place

Exploits

```
$buffer = "";
$null = "\x00";
$nop = "\x90";
$nopsize = 1;
$len = 201; // what is needed to overflow, maybe 201, maybe more!
$the_shell_pointer = 0xdeadbeef; // address where shellcode is
# Fill buffer
for ($i = 1; $i < $len;$i += $nopsize) {
    $buffer .= $nop;
}
$address = pack('l', $the_shell_pointer);
$buffer .= $address;
exec "$program", "$buffer";
```

Demo exploit in Perl

Hvordan finder man buffer overflow, og andre fejl

Black box testing

Closed source reverse engineering

White box testing

Open source betyder man kan læse og analysere koden

Source code review - automatisk eller manuelt

Fejl kan findes ved at prøve sig frem - fuzzing

Exploits virker typisk mod specifikke versioner af software

The Exploit Database - dagens buffer overflow

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

Metasploit

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.

Idag findes der samlinger af exploits

Udviklingsværktøjerne til exploits er idag meget raffinerede!

`http://www.metasploit.com/`

`http://www.fastandeasyhacking.com/` Armitage GUI til Metasploit

`http://www.offensive-security.com/metasploit-unleashed/`

Forudsætninger

Bemærk: alle angreb har forudsætninger for at virke

Et angreb mod Telnet virker kun hvis du bruger Telnet

Et angreb mod Apache HTTPD virker ikke mod Microsoft IIS

Kan du bryde kæden af forudsætninger har du vundet!

Eksempler på forudsætninger

Computeren skal være tændt

Funktionen der misbruges skal være slået til

Executable stack

Executable heap

Fejl i programmet

alle programmer har fejl

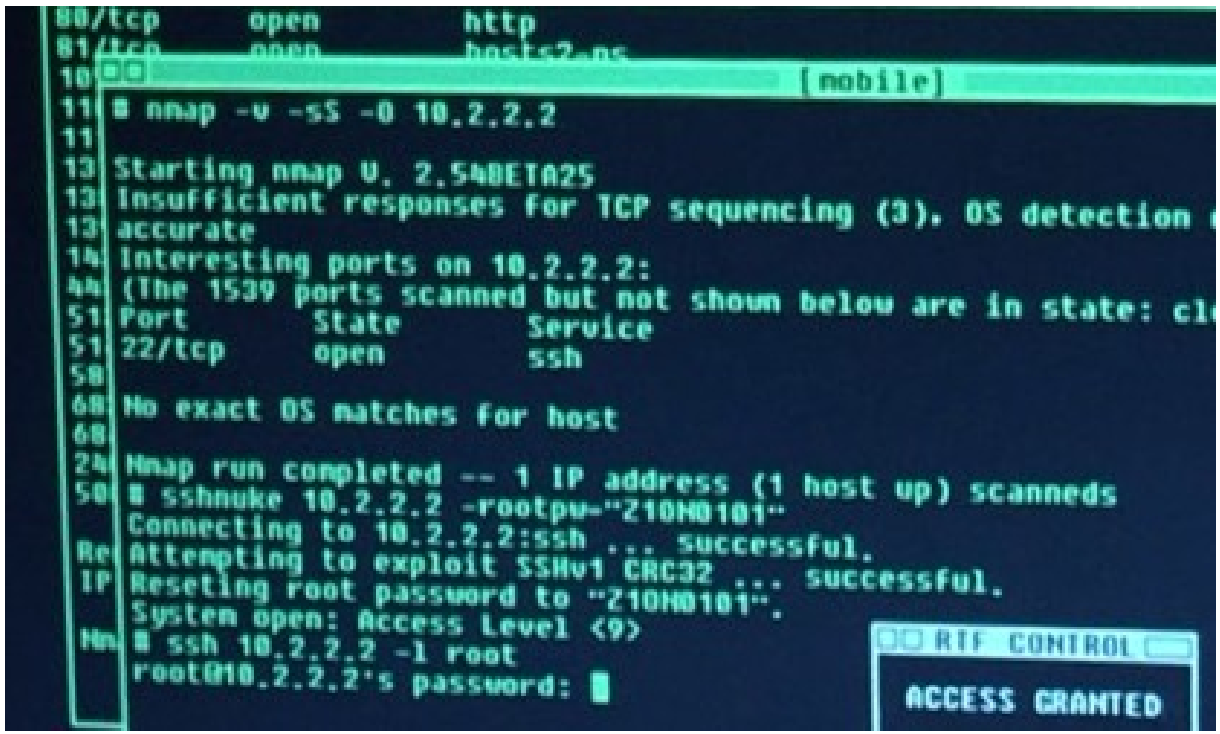
Kali Linux the pentest toolbox

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

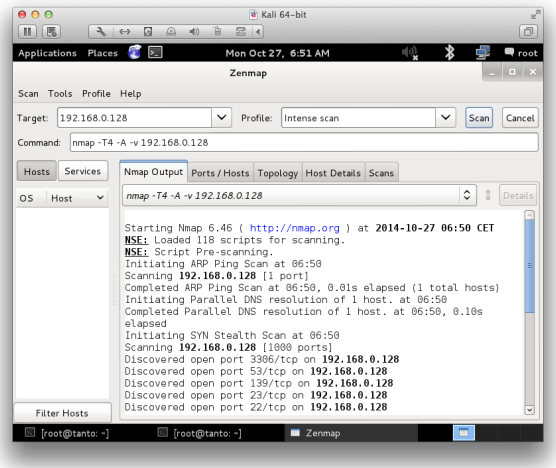
Trinity breaking in



http://nmap.org/movies.html

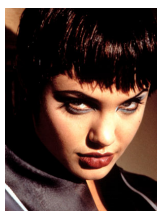
Meget realistisk http://www.youtube.com/watch?v=51lGCTgqE_w

Really do Nmap your world



- Nmap is a port scanner, but does more
- Finding your own infrastructure available from the guest network?
- See your printers having all the protocols enabled AND a wireless?

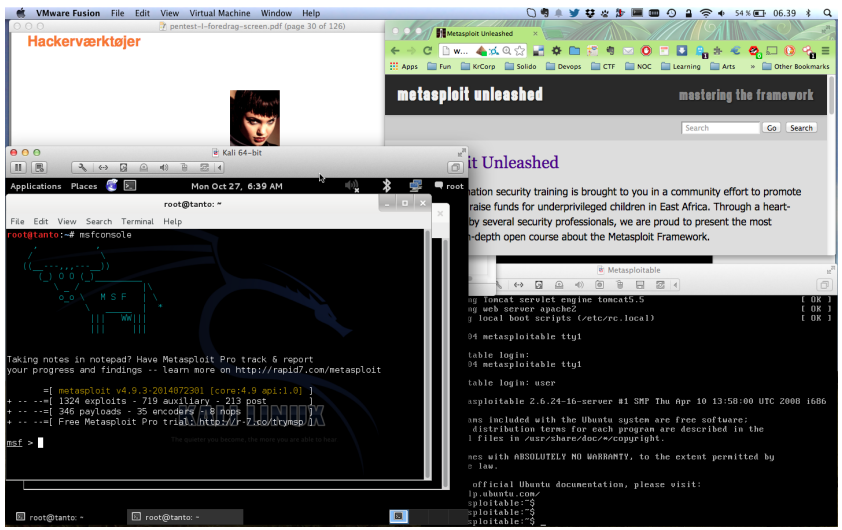
Hackertools are for everyone!



- 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`

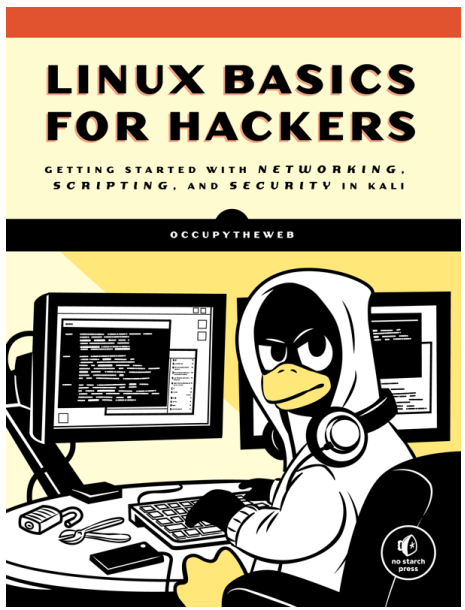
Most popular hacker tools `http://sectools.org/`

Hackerlab setup



- Create hacker labs, encourage hacker labs!
- Software Host OS: Windows, Mac, Linux
- Virtualisation software: VMware, Virtual box, HyperV pick your poison
- Hackersoftware: Kali Virtual Machine `https://www.kali.org/`

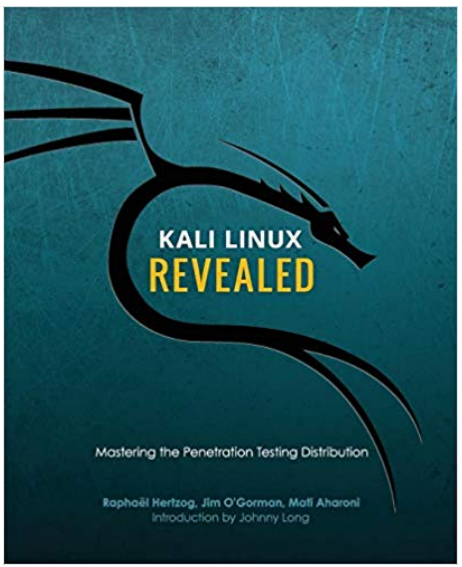
Book: Linux Basics for Hackers (LBhf)



Linux Basics for Hackers Getting Started with Networking, Scripting, and Security in Kali by OccupyTheWeb December 2018, 248 pp. ISBN-13: 9781593278557

`https://nostarch.com/linuxbasicsforhackers`

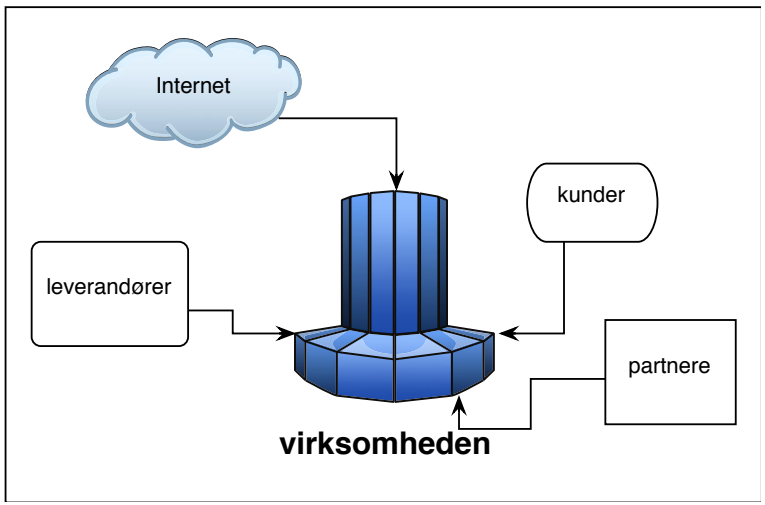
Book: Kali Linux Revealed (KLR)



Kali Linux Revealed Mastering the Penetration Testing Distribution

`https://www.kali.org/download-kali-linux-revealed-book/`
explains how to install Kali Linux

Fokus 2019: Firewalls og segmentering

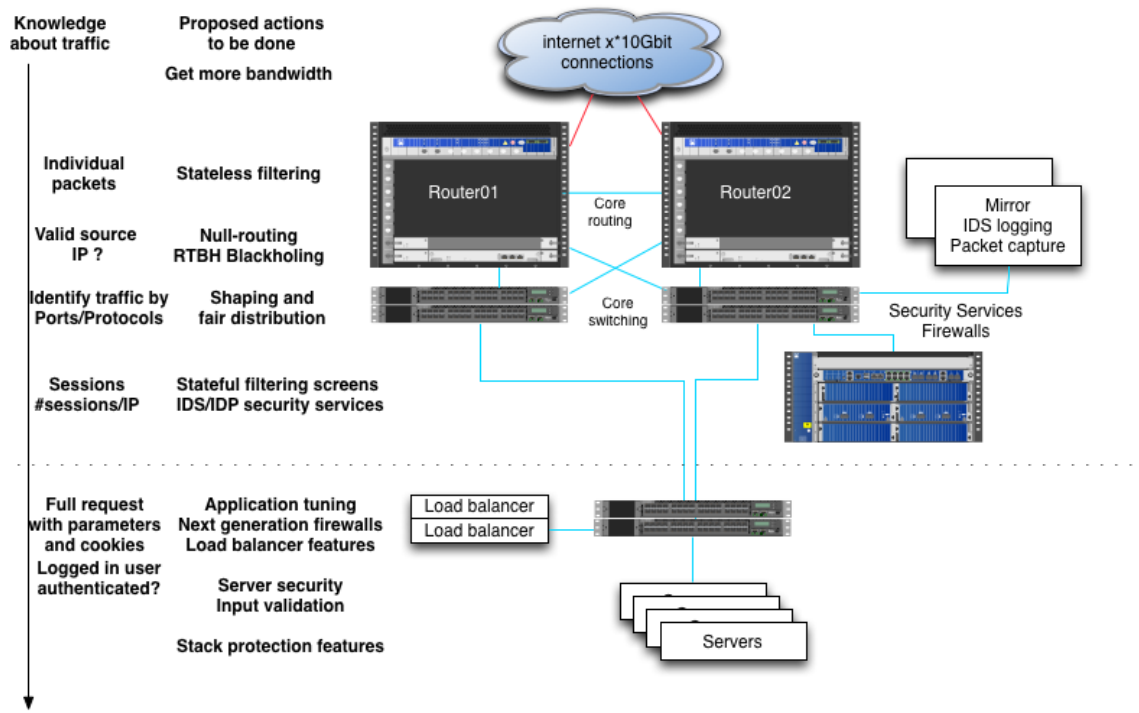


- Hvis du har et netværk, så bør du have en firewall
- En firewall tillader autoriseret trafik og blokerer resten
- Hvornår har du sidst set din løsning efter?
- Hvor lang tid tager det at se en 5.000 linier Cisco ASA config igennem?

Imagine Attacks from the Inside

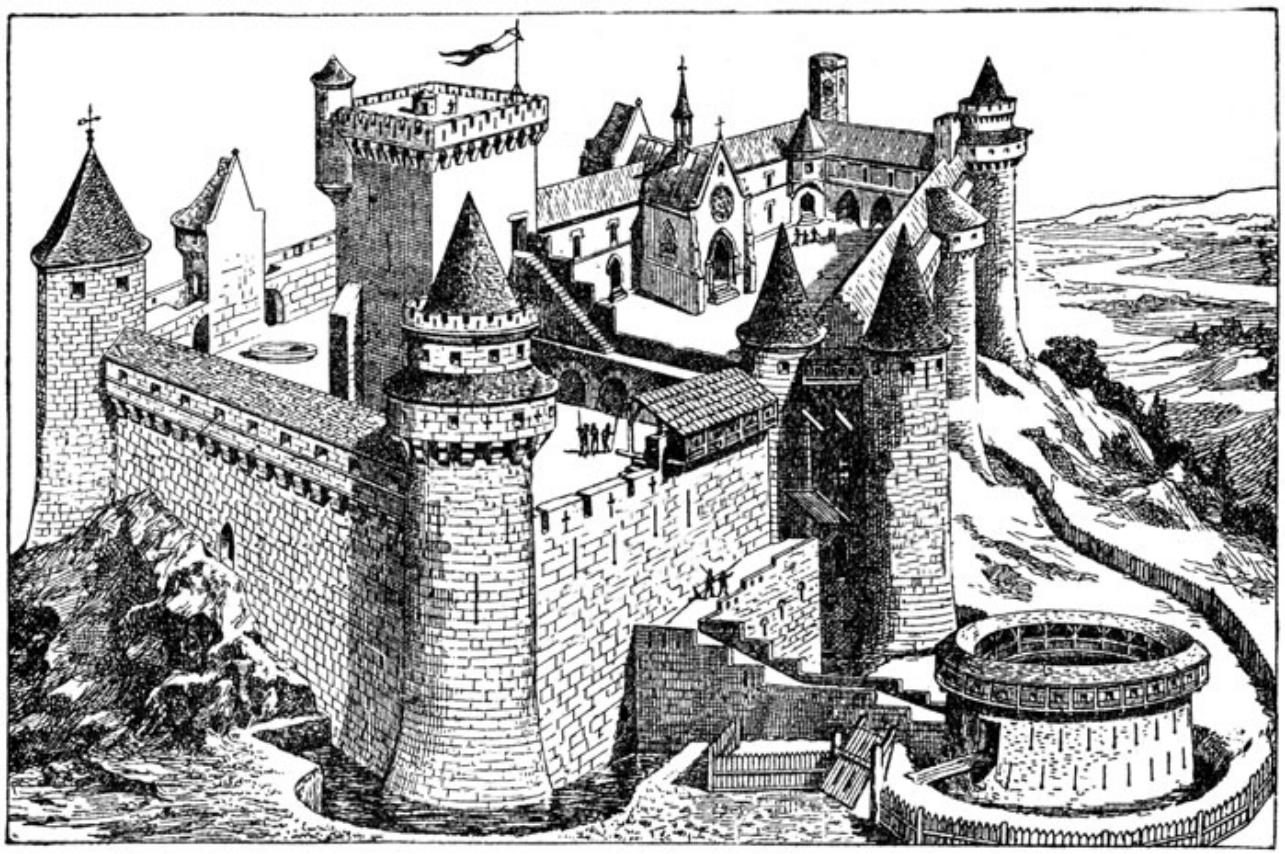
- Now imagine you were in control of a company laptop
- Do you have a large internal world wide network?
  NotPetya cost Maersk about 1.9 billion DKK
- entry thought to be via software update of M.E.Doc [uk] an Ukrainian tax preparation program
- Attackers are very creative and have a large attack surface to most companies

Big firewalls



Big firewalls are not a single device

Enhance and secure runtime environment



Gode operativsystemer

Nyere versioner af Microsoft Windows, Mac OS X og Linux distributionerne inkluderer:

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

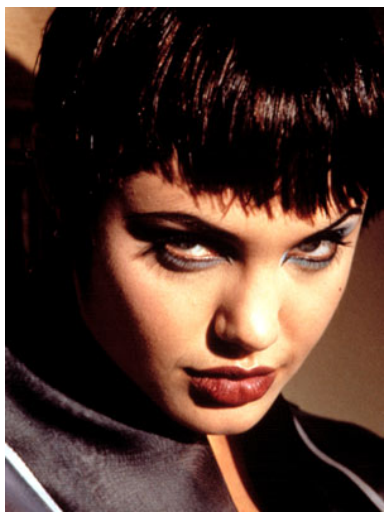
Vælg derfor hellere:

- Windows 10, end Windows Xp
- Mac OS X nyeste versioner
- Linux sikkerhedsopdateringer, sig ja når de kommer

Det samme gælder for serveroperativsystemer

NB: meget få embedded systemer har beskyttelse!

Hackertyper anno 1995



Lad os lige gå tilbage til hackerne

Hackertyper anno 2008

Lisbeth laver PU, personundersøgelser ved hjælp af hacking

Hvordan finder man information om andre

Fra mønstre til person

Først vil vi finde nogle mønstre

Derefter vil vi søge med de mønstre

Nogle giver direkte information

Andre giver baggrundsinformation

Hvad er offentligt og hvad er privat? (googledorks!)

Eksempler på mønstre

Navn, fulde navn, fornavne, efternavne, alias'es

Diverse idnumre, som CPR - tør du søge på dit CPR nr?

Computerrelaterede informationer: IP, Whois, Handles

Øgenavne, kendenavne

Skrivestil, ordbrug mv.

Tiden på din computer?

Tænk kreativt ☺

Hvor finder du informationerne

Email

DNS

Gætter

Google

Alt hvad du ellers har adgang til - eller som Lisbeth tilraner sig adgang til

Google for it

Google som hacker værktøj?

Googledorks `http://johnny.ihackstuff.com/`

Questions?

Henrik Lund Kramshøj hlk@zencurity.com

Need help with infrastructure security or pentesting, ask me!

You are always welcome to send me questions later via email

Reklamer: kursusafholdelse

Følgende kurser afholdes med mig som underviser

- Nmap workshop - 4 timer
  Nmap for blue team, forsvaret. En workshop med Nmap pakken af værktøjer som gør dig istand til at beskytte dit netværk bedre, fordi du effektivt kan undersøge det. Vi gennemgår almindelig portscanning, som sættes i system, samt andre værktøjer som Nping til verifikation af forbindelser mellem enheder og igennem filtre og firewalls.

- Suricata, Bro og DNS opsamling - 4 timer
  Workshop: Suricata, Zeek og DNS opsamling Netværk idag er ofte blevet uoverskuelige, men kritiske for vores IT-brug. Denne workshop ser på applikationer til automatisk at afkode netværkstrafik med øvelser. Vi laver øvelser med Suricata, Zeek (tidligere Bro) og passiv DNS opsamling som eksempler på at kunne logge og gå tilbage i tiden. Niveauet er introduktion til værktøjerne og øvelserne bliver udført på Linux.