



Welcome to

Basic hacking - black/white hat

Dark Net og personlige oplysninger

Henrik Lund Kramshøj hk@zencurity.dk

Slides are available as PDF, [kramshoej@Github](https://github.com/kramshoej)

Formålet med foredraget



Don't Panic!

Skabe en forståelse for hackerværktøjer hacking historie

The Darknet: hvad er det for en størrelse?

skal vi være bekymrede for vores personlig oplysninger?

Aftale om test af netværk

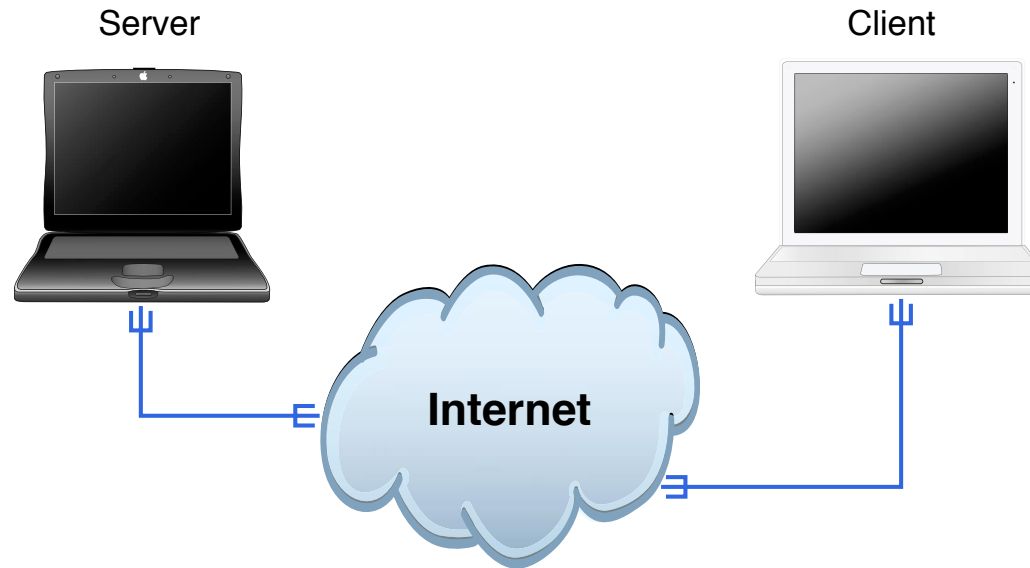


Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling.

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> Det Kriminalpræventive Råd, siden er væk
- Frygten for terror har forstærket ovenstående - så lad være!

Internet idag




Klienter og servere

Rødder i akademiske miljøer

Protokoller hvor nogle er mere end 20 år gamle

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

Teknisk hvad er hacking



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

Trinity breaking in



```
80/tcp    open     http
81/tcp    open     hosts2-ns
10.2.2.2  [ nobile]
11 # nmap -v -ss -O 10.2.2.2
11
13 Starting nmap V. 2.540ETA25
13 Insufficient responses for TCP sequencing (3). OS detection
13 accurate
14 Interesting ports on 10.2.2.2:
44 (The 1539 ports scanned but not shown below are in state: cl
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 -rootpu-"210N0101"
Connecting to 10.2.2.2:ssh ... successful.
Re Attempting to exploit SSHv1 CRC32 ... successful.
IP Resetting root password to "210N0101".
System open: Access Level <9>
Hw # ssh 10.2.2.2 -l root
root@10.2.2.2's password: 
```

<http://nmap.org/movies.html>

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

Hacking er magi



Hacking ligner indimellem magi

Hacking er ikke magi



Hacking kræver blot lidt ninja-træning



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>



Konsulentens udstyr - vil du være sikkerhedskonsulent

Sikkerhedskonsulenterne bruger typisk Open Source værktøjer på Linux og enkelte systemer med Windows - jeg bruger helst Windows 7 idag

Laptops, gerne flere, men een er nok til at lære!

- *A Hands-On Introduction to Hacking* by Georgia Weidman, June 2014
<http://www.nostarch.com/pentesting>
- *Metasploit The Penetration Tester's Guide* by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni
<http://nostarch.com/metasploit>
- Metasploit Unleashed - gratis kursus i Metasploit
<http://www.offensive-security.com/metasploit-unleashed/>

Hackerværktøjer

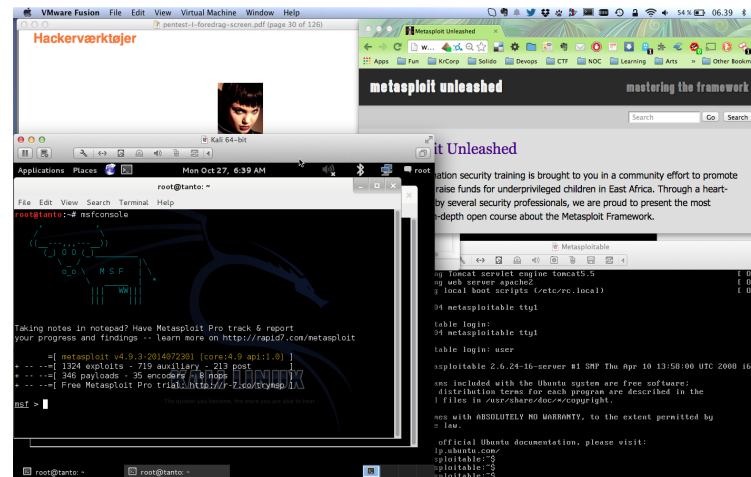


- Nmap, Nping - tester porte, godt til firewall admins <http://nmap.org>
- Metasploit Framework gratis på <http://www.metasploit.com/>
- Wireshark avanceret netværkssniffer - <http://http://www.wireshark.org/>
- Burpsuite <http://portswigger.net/burp/>
- OpenBSD operativsystem med fokus på sikkerhed <http://www.openbsd.org>

Kilde: billedet er Angelina Jolie fra Hackers 1995

Kræver en mere struktureret

Hackerlab opsætning



- Tænk som en hacker, rekognoscering, angreb, udnyt
- Hardware: en moderne laptop med CPU der kan bruge virtualisering
Husk at slå virtualisering til i BIOS
- Software: Windows, Mac, Linux og virtualiseringssoftware: VMware, Virtual box, vælg selv
- Hackersoftware: Kali Linux som en virtuel maskine
- 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 <http://www.kali.org/>

Wireshark - <http://www.wireshark.org> avanceret netværkssniffer

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 ...	

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
- Fandt systemer i /etc/hosts.equiv, .rhosts, .forward, netstat ...
- Password cracking med intern liste med 432 ord og /usr/dict/words

Lavet af Robert T. Morris, Jr.

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

1980'erne - det er vel fixet så?

2016 botnets Internet of things (IoT)



This is bad news for cybersecurity as the IoT devices market heats up as people buy into the smart, automated systems. Gartner Inc. projects connected devices to rise to 6.4 billion worldwide in 2016 with almost 5.5 million devices being connected daily.

2016: Mirai Botnet Internet of things (IoT), 60 common factory default usernames and passwords

"Mirai was used in the DDoS attack on 20 September 2016 on the Krebs on Security site which reached 620 Gbps."

2016: Currently, "Bashlight" is creating an army of a million IoT devices.
Eeen million enheder!

Sources: [https://en.wikipedia.org/wiki/Mirai_\(malware\)](https://en.wikipedia.org/wiki/Mirai_(malware))

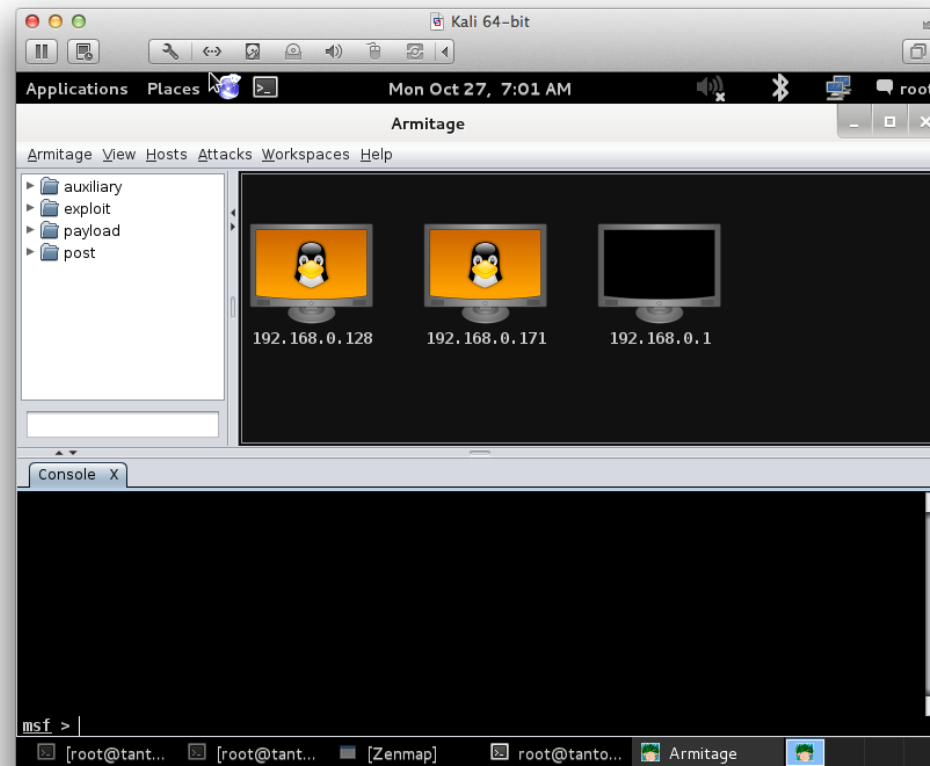
<http://heavy.com/tech/2016/10/mirai-iot-botnet-internet-of-things-ddos-attacks-internet-outage>

Real life bruteforce? Found in on real server



```
root:admin:87.x.202.63
admin:admin:91.x.104.207
admin:0767390145:x.72.110.84
admin:0767390145:89.xx.163.73
admin:0767390145:89.x.142.153
root:root:186.x.39.228
admin:admin:189.x.160.98
root:dumn3z3u:189.x.216.232
admin:0767390145:189.x.36.247
root:admin:169.x.34.145
root:default:66.x.33.138
root:default:66.x.33.138
root:111111:213.x.89.250
admin:admin:91.x.52.114
admin:0767390145:195.x.246.131
admin:0767390145:195.x.246.131
```

Demo: Metasploit Armitage



Armitage GUI fast and easy hacking for Metasploit

<http://www.fastandeasyhacking.com/> og lidt wireshark

Informationsindsamling



Det vi har udført er informationsindsamling

Indsamlingen kan være aktiv eller passiv indsamling i forhold til målet for angrebet

passiv kunne være at lytte med på trafik eller søge i databaser på Internet

aktiv indsamling er eksempelvis at sende netværkspakker og portscanne

Darknet / dark web / deep web



As of 2015, "The Darknet" is often used interchangeably with the dark web due to the quantity of hidden services on Tor's darknet. The term is often used inaccurately and interchangeably with the deep web due to Tor's history as a platform that could not be search indexed.

- The dark web is the World Wide Web content that exists on darknets,
- The deep web, invisible web, or hidden web are parts of the World Wide Web whose contents are not indexed by standard search engines for any reason
- Indhold på darknet/dark web er ofte ikke lettilgængeligt, kræver speciel software eller direkte links
- Populære Darknets Freenet, I2P, and Tor, Kendt deep web site: det lukkede narko m.m. Silk Road
https://da.wikipedia.org/wiki/Silk_Road

Advarsel: Der ER grimme ting på Darknets/Deep web

Source: <https://en.wikipedia.org/wiki/Darknet> https://en.wikipedia.org/wiki/Deep_web

Tor project anonym web browsing



Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

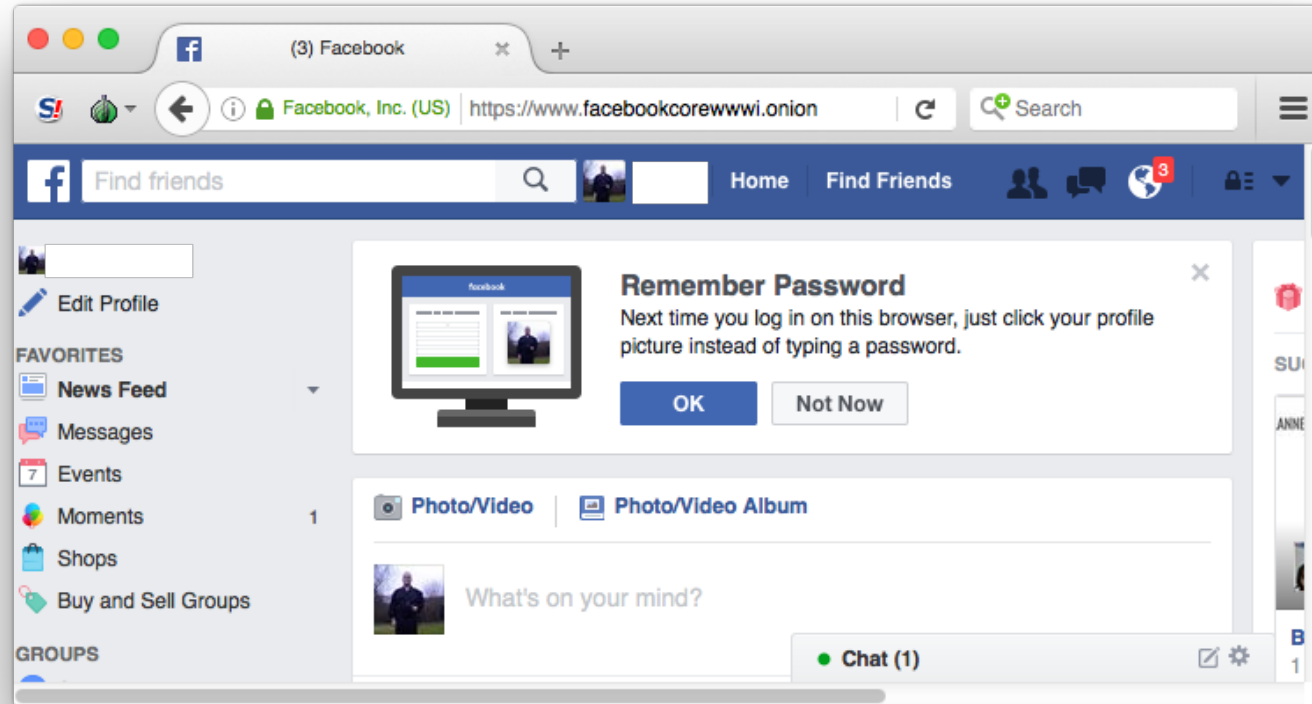
[Download Tor](#)

- ➔ Tor prevents anyone from learning your location or browsing habits.
- ➔ Tor is for web browsers, instant messaging clients, remote logins, and more.
- ➔ Tor is free and open source for Windows, Mac, Linux/Unix, and Android

<https://www.torproject.org/>

Der findes alternativer, men Tor er mest kendt

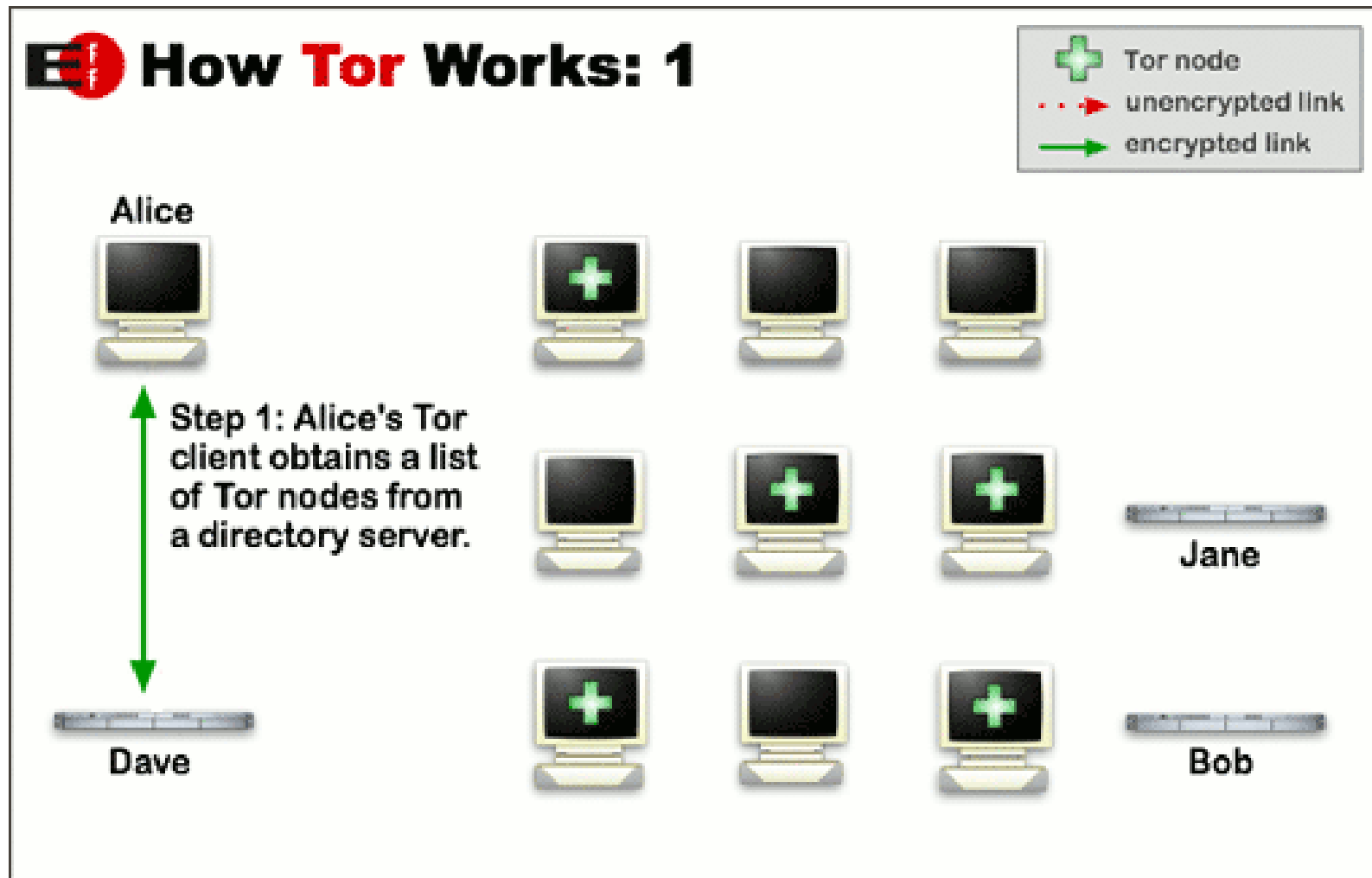
Facebook over Tor



Eksempel site: Facebook over Tor

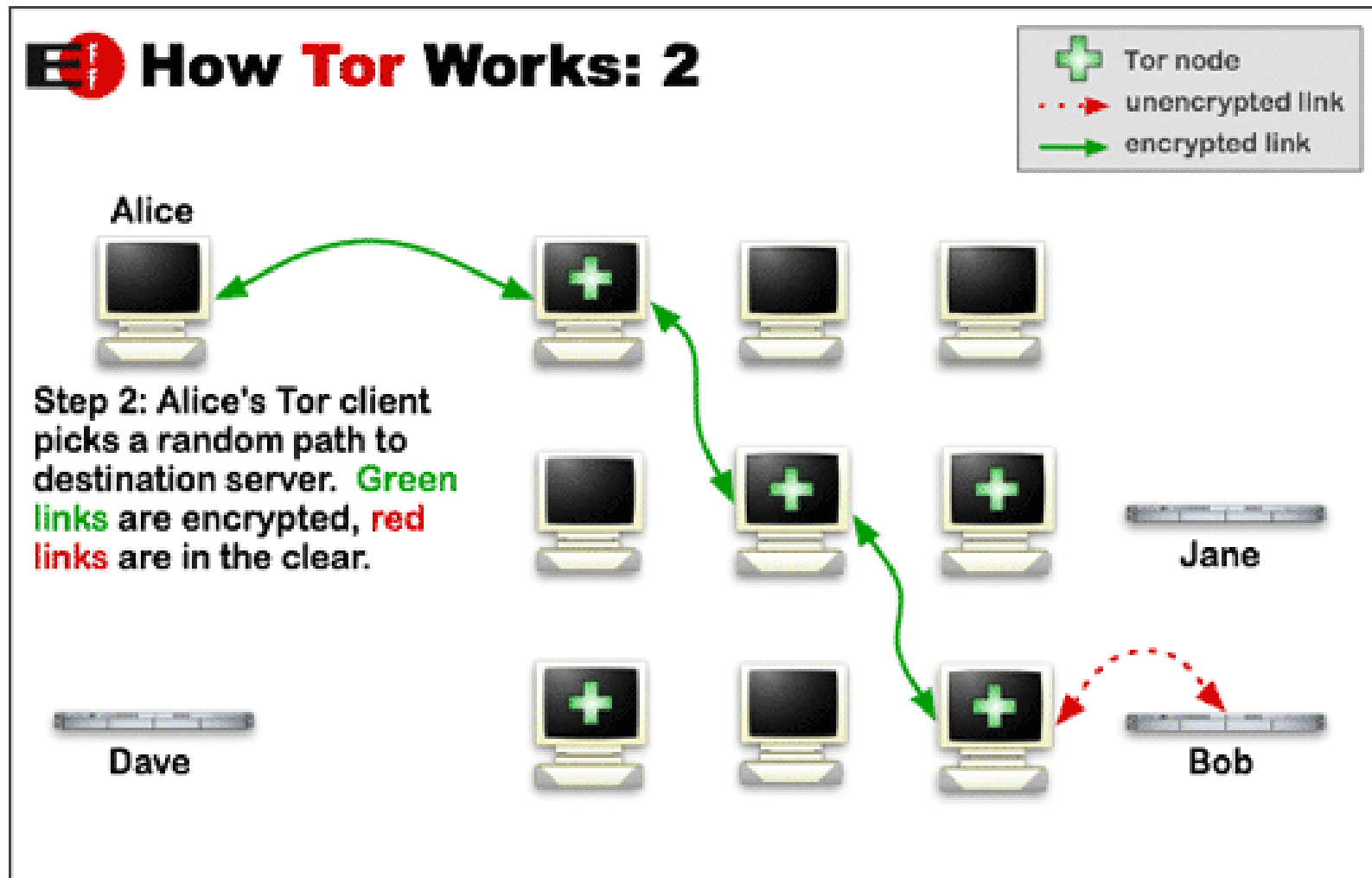
<https://facebookcorewwi.onion/>

Tor project - how it works 1



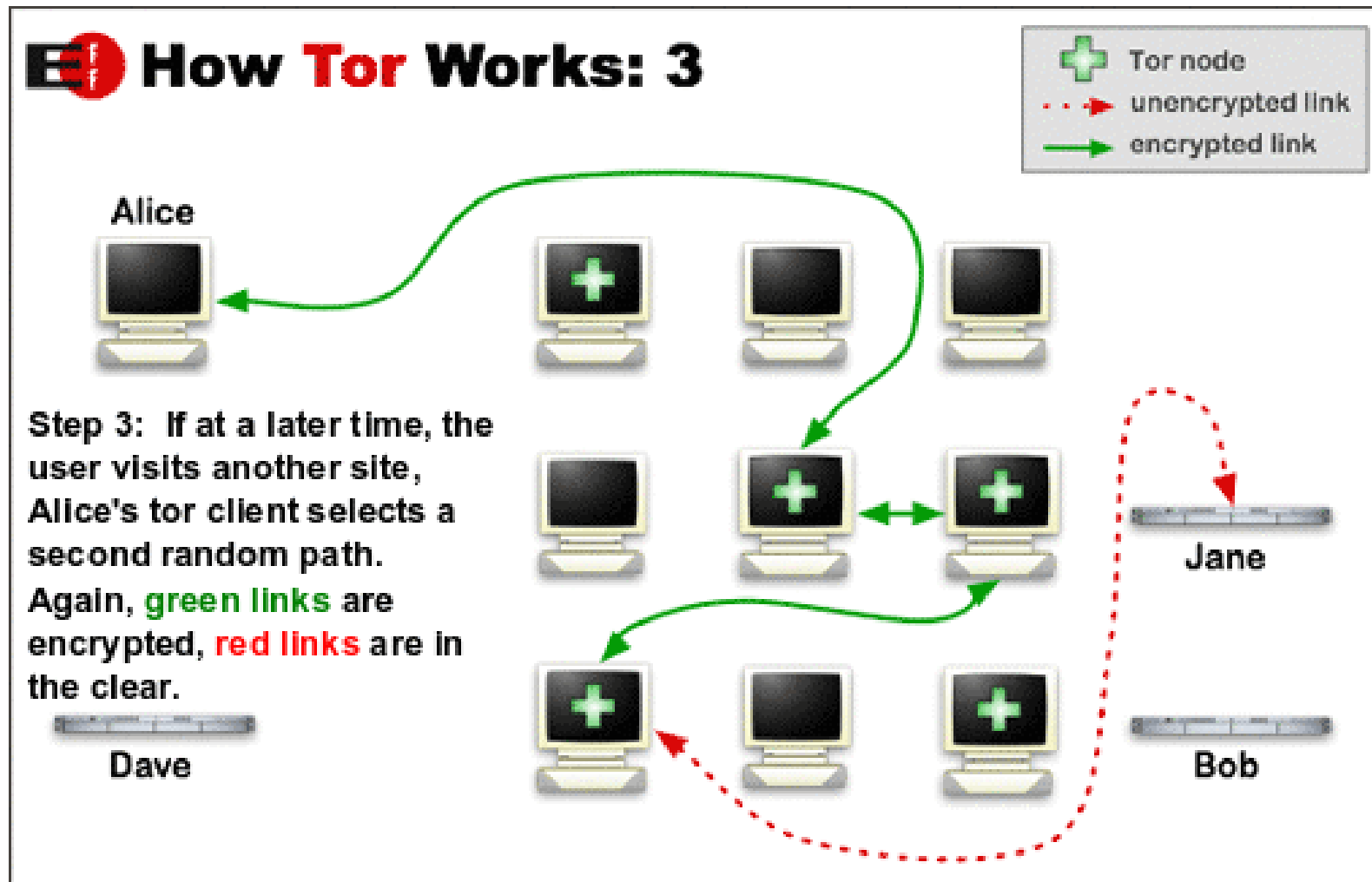
pictures from <https://www.torproject.org/about/overview.html.en>

Tor project - how it works 2



pictures from <https://www.torproject.org/about/overview.html.en>

Tor project - how it works 3



pictures from <https://www.torproject.org/about/overview.html.en>

Why use Tor?



- Your public IP is **Red Information**, often lead directly to you
- You like to browse things, without telling your ISP, the government, your teacher, ... everyone, Avoid censorship
- You want to avoid stalkers
- You are an investigative journalist or high school student researching Al Qaeda, Daesh, ISIS for school
- Consider getting the book *The Smart Girl's Guide to Privacy*
<http://smartprivacy.tumblr.com/>

Shameless plug: we are starting up danish information page and more <https://www.torserver.dk/>

Pic from <https://www.torproject.org/>

Who Uses Tor?



Internet.

Family & Friends

People like you and your family use Tor to protect themselves, their children, and their dignity while using the



accountability.

Businesses

Businesses use Tor to research competition, keep business strategies confidential, and facilitate internal



on corruption.

Activists

Activists use Tor to anonymously report abuses from danger zones. Whistleblowers use Tor to safely report



Media

Journalists and the media use Tor to protect their research and sources online.



gathering online.

Military & Law Enforcement

Militaries and law enforcement use Tor to protect their communications, investigations, and intelligence

Smart Girl's Guide to Privacy



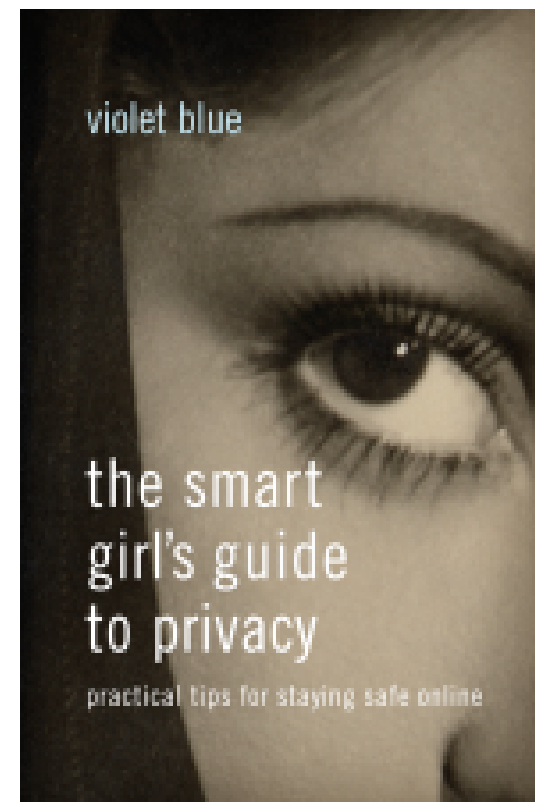
<https://www.nostarch.com/smartgirlsguide>

Practical Tips for Staying Safe Online by Violet Blue

August 2015, 176 pp. ISBN: 978-1-59327-648-5

Kan varmt anbefales!

Søg også på Emma Holten



Fuld Disk Kryptering: Bitlocker



- Microsoft tilbyder Bitlocker fuld disk kryptering
- Åbnes med dit Windows kodeord
- Meget transparent - data krypteres når det skrives ned
- Nedsætter ikke hastigheden mærkbart, ofte forbedres den endda
- Genetableringsnøgle - er slået til på FT computere
Giver mulighed for at IT-afd kan åbne din computer hvis du glemmer koden
- Fungerer på både roterende diske og SSD,
men pas på SSD kan have data fra før kryptering slået til

Kilde: mere information om Bitlocker

<http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview>



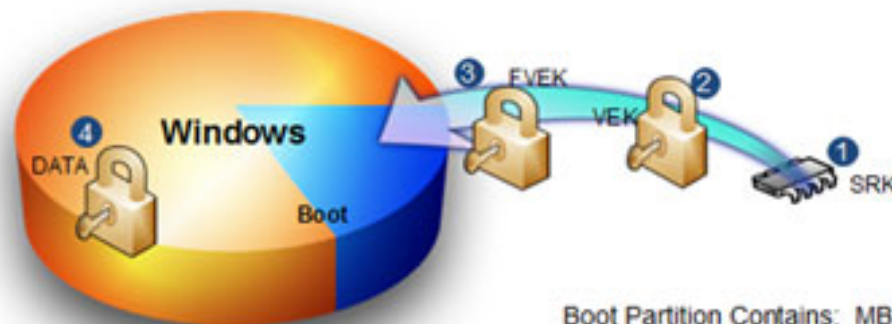
Disk Layout & Key Storage

Windows Partition Contains

- Encrypted OS
- Encrypted Page File
- Encrypted Temp Files
- Encrypted Data
- Encrypted Hibernation File

Where's the Encryption Key?

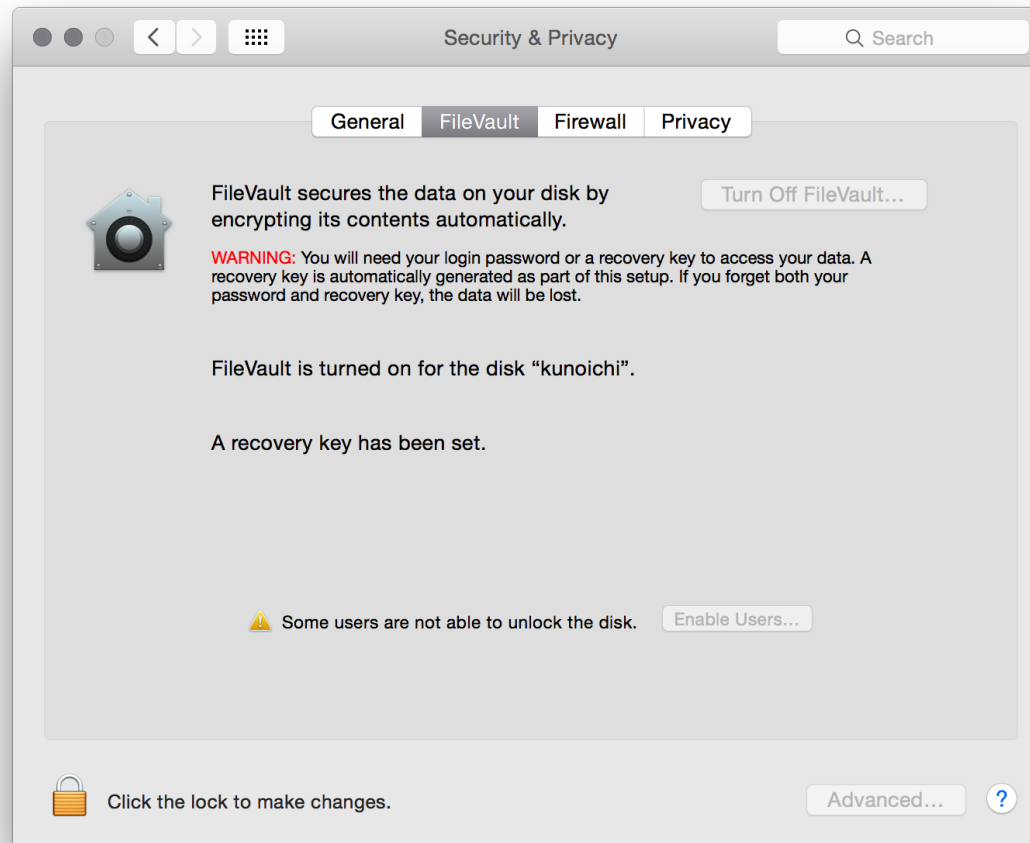
1. SRK (Storage Root Key) contained in TPM
2. SRK encrypts VEK (Volume Encryption Key) may also by PIN/Startup key
3. VEK stored (encrypted by SRK) in volume metadata
4. VEK encrypts an internal key (FVEK) used to encrypt the data. FVEK is stored in the volume metadata.



Boot Partition Contains: MBR, Loader, Boot Utilities (Unencrypted, small)

Kilde: <https://technet.microsoft.com/en-us/library/cc512654.aspx>

Bonus: Full Disk Encryption Mac OS X



Indbygget, gratis, stærk - slå det til når I kommer hjem

Brug flere browsere



Firefox



chrome



TorProject.org



Allow active content to run
only from sites you trust



ScriptBlock 1.0

A smart extension that controls javascript, iframes, and plugins



HTTPS Everywhere

whonix
PRIVACY & ANONYMITY OS

Fordele ved flere browsere



Flere browsere giver højere sikkerhed

Data kan ikke flyde mellem flere browsere, cookies m.m.

Mit forslag:

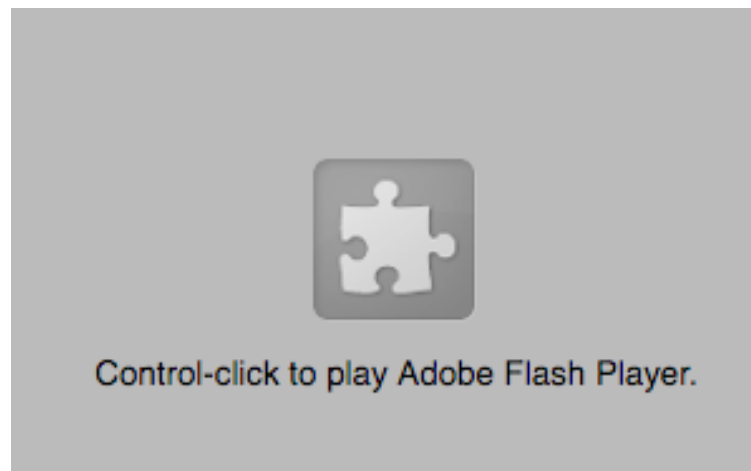
- En browser til *sikre sites* banken, intranet
- En browser til generel internet surfing
- En browser med alle mulige plugins, web udvikling eksempelvis

Installer gerne plugins til højere sikkerhed i allesammen:
HTTPS Everywhere, NoScript/ScriptBlock m.fl.

Det anbefales at disse installeres og vedligeholdes fra IT-afdelingen

Alle browsere har mange fejl!

Chrome en rimeligt sikker browser



Generelt er internet browsing en risikofyldt aktivitet

Drive-by-download hacking er reel trussel

Opdaterer sig selv løbende

Egen Sand-box til Flash

Denne browser kan indstilles rimeligt sikkert

Generelt indstillinger for browsere

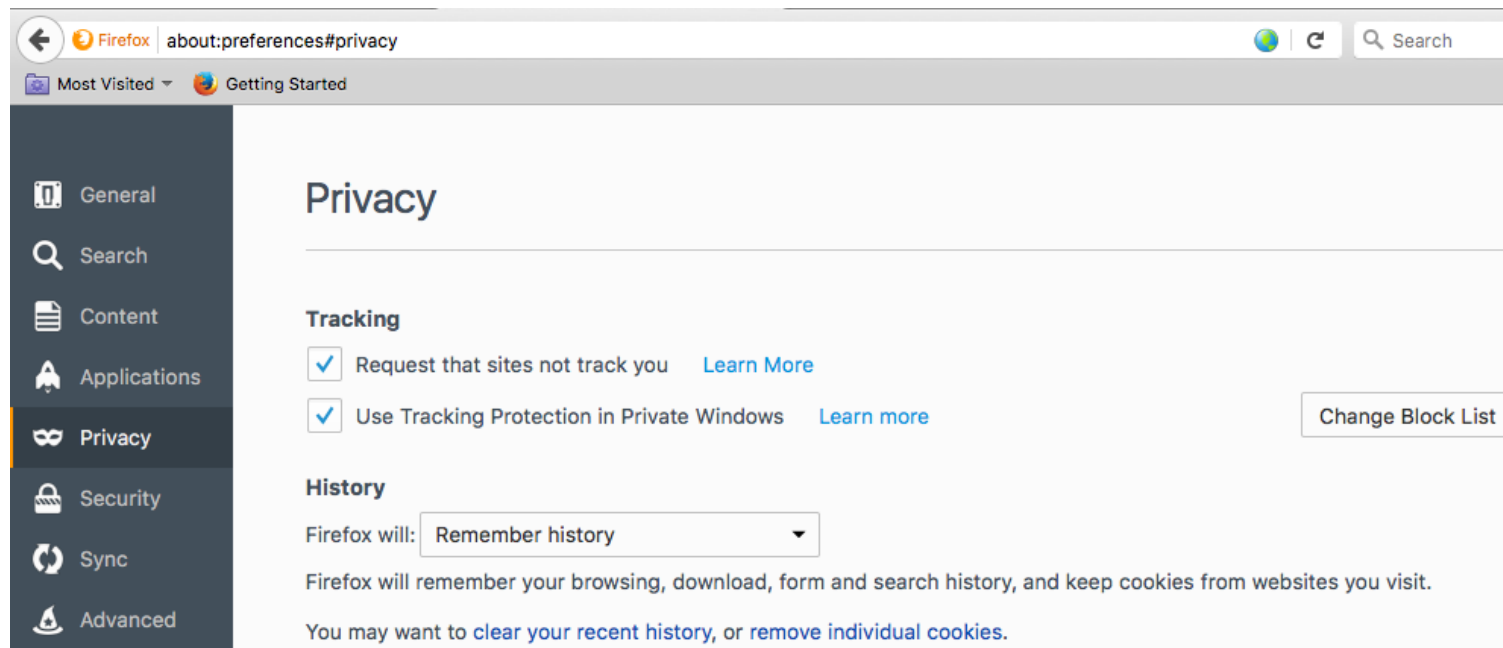


Skal være indstillet på den sikre browser til generel surf

- Slå JavaScript fra generelt med NoScript/ScriptBlock
- Slå click-to-play til for aktivt indhold
- Slå "Do Not Track" til
- Slå Java helt fra, afinstaller evt. Java helt fra computeren
- Installer en AdBlocker - jeg bruger AdBlock

Vigtigt: servere der viser reklamer er ofte mål for hacking

Hvor ændrer man indstillingerne



De fleste findes under:

- Chrome `chrome://settings/` og `chrome://extensions/`
- Firefox Indstillingerne og for enkelte ting: `about:config`

Kig også gerne på Safari eller Internet Explorer indstillingerne

HTTPS Everywhere



HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

`https://www.eff.org/https-everywhere`

Also in Chrome web store!

Opsummering



Husk følgende:

- Husk: IT-sikkerhed er ikke kun netværkssikkerhed!
- God sikkerhed kommer fra langsigtede initiativer
- Hvad er informationssikkerhed?
- Data på elektronisk form, USB drev
- Data på fysisk form, køb en makulator
- Lav backup af data I vil gemme! Køb en ekstern USB disk til offline
3-2-1 backup 3 kopier i 2 programmer med 1 offline/slukket

Informationssikkerhed er en proces

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

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

Hvis man vil vide mere kan man starte med:

- *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

Definition af hacking, oprindeligt



Eric Raymond, der vedligeholder en ordbog over computer-slang (The Jargon File) har blandt andet følgende forklaringer på ordet hacker:

- En person, der nyder at undersøge detaljer i programmerbare systemer og hvordan man udvider deres anvendelsesmuligheder i modsætning til de fleste brugere, der bare lærer det mest nødvendige
- En som programmerer lidenskabeligt (eller enddog fanatisk) eller en der foretrækker at programmere fremfor at teoretiserer om det
- En ekspert i et bestemt program eller en der ofte arbejder med eller på det; som i "en Unixhacker".

Kilde: Peter Makholm, <http://hacking.dk>

Benyttes stadig i visse sammenhænge se <http://labitat.dk>