



Welcome to

White Hat Hacking, protect your network

Bella Center 2019

Henrik Lund Kramshøj hlk@zencurity.com

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

We are all part of security

Hackers don't give a shit

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

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

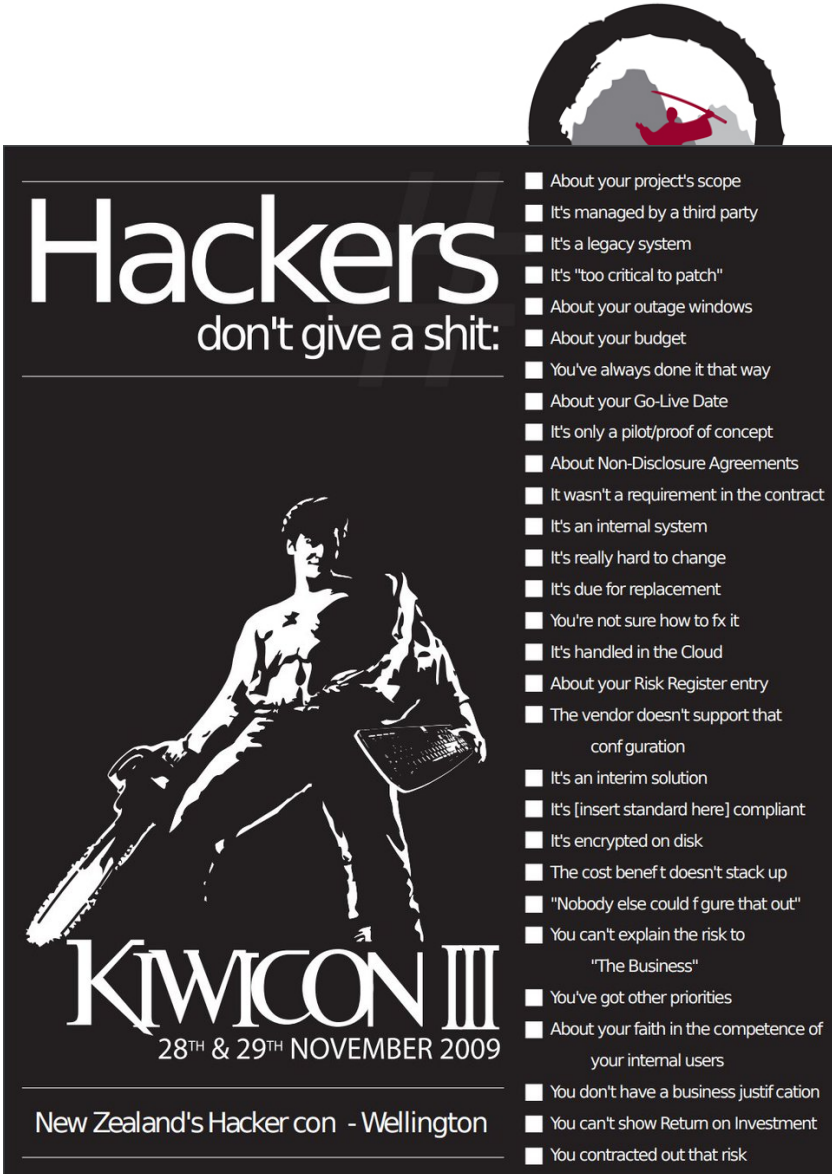
Try something new, stay aware

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

Make sure to alert someone if something is strange

if something can become a threat

May need to repeat this multiple times, until fixed



Hackers
don't give a shit:

- ☐ About your project's scope
- ☐ It's managed by a third party
- ☐ It's a legacy system
- ☐ It's "too critical to patch"
- ☐ About your outage windows
- ☐ About your budget
- ☐ You've always done it that way
- ☐ About your Go-Live Date
- ☐ It's only a pilot/proof of concept
- ☐ About Non-Disclosure Agreements
- ☐ It wasn't a requirement in the contract
- ☐ It's an internal system
- ☐ It's really hard to change
- ☐ It's due for replacement
- ☐ You're not sure how to fix it
- ☐ It's handled in the Cloud
- ☐ About your Risk Register entry
- ☐ The vendor doesn't support that configuration
- ☐ It's an interim solution
- ☐ It's [insert standard here] compliant
- ☐ It's encrypted on disk
- ☐ The cost benefit doesn't stack up
- ☐ "Nobody else could figure that out"
- ☐ You can't explain the risk to "The Business"
- ☐ You've got other priorities
- ☐ About your faith in the competence of your internal users
- ☐ You don't have a business justification
- ☐ You can't show Return on Investment
- ☐ You contracted out that risk

KIWICON III
28TH & 29TH NOVEMBER 2009

New Zealand's Hacker con - Wellington

Data found in Network data



Lets take an example, DNS

Domain Name System DNS breadcrumbs

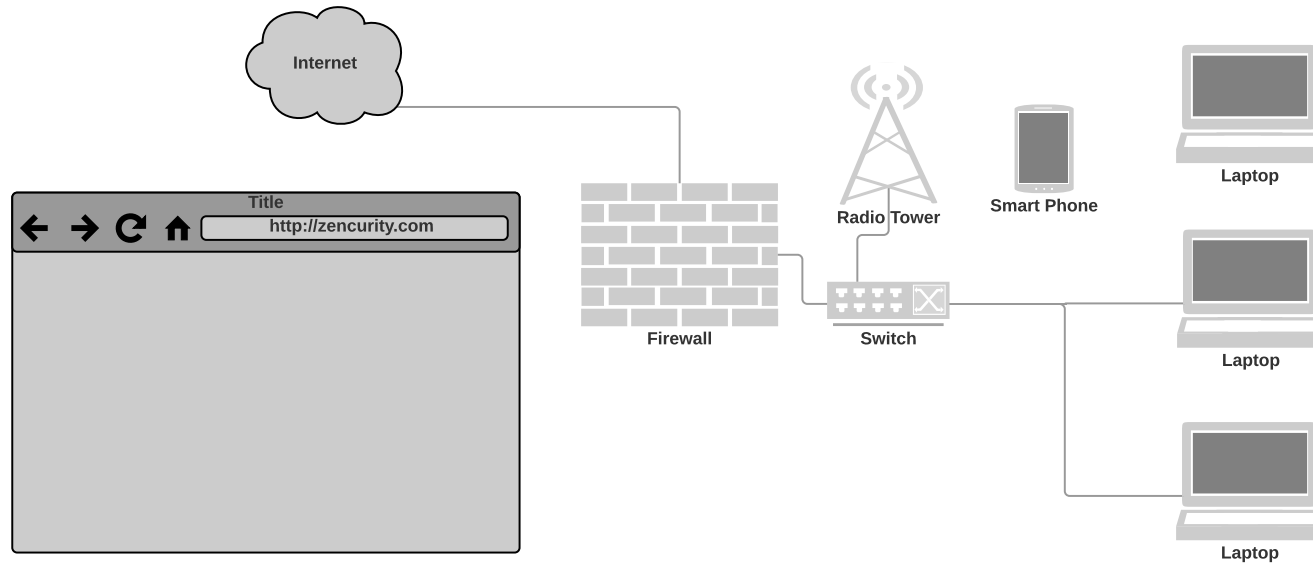
- Your company domain, mailservers, vpn servers
- Applications you use, checking for updates, sending back data
- Web sites you visit
- Privacy issue - how to monitor company without invading employee privacy

Advice show your users,ask them to participate in a experiment

Join this Wireless network SSID and we will show you who you are on the internet

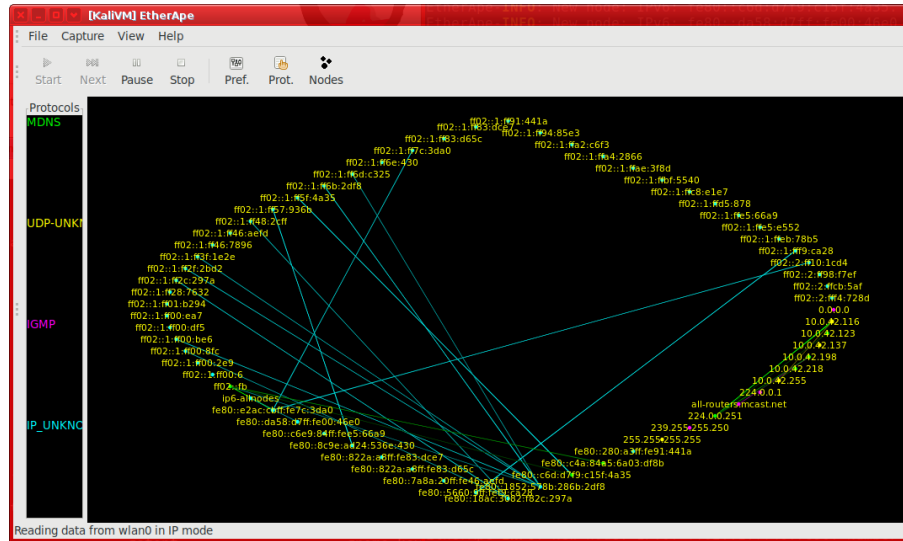
Maybe use VPN more - or always!

Your Privacy under Attack



- Your data travels far
- Often crossing borders, virtually and literally
- Many technologies are old and insecure

Demo Attacks fun with DNS and routing



- Now imagine you were in control of a network
- Everyone uses DNS, DNS is not secure
- HTTPS is nice, but how do you get to HTTPS? (PS hsts for 8mins?!)

No real sites are hurt in the process!