

# Courses, lectures and seminars

Security6.net has years of experience which make us a suitable partner when it is time for courses, workshops, seminars or otherwise created awareness about subjects such as security, networks and UNIX systems.

Below are short descriptions of some of the lectures and courses, which Security6.net has given. The courses can be adapted as desired. Suggestions for duration is noted in parentheses after the description.

## Protect yourself - learn hacking

Penetration testing is the technique used when acting like a hacker trying to break into your own networks. By learning the same methods used to break security as used by hackers and apply those in a structured way makes it possible to close down security holes in ones own network.

(2 day workshop) [more information](#)

## Computer Forensics

Computer Forensics involves the preservation, identification, extraction, documentation and interpretation of computer data.

Definition from the book Computer Forensics: Incident Response Essentials, Warren G. Kruse II og Jay G. Heiser, Addison-Wesley, 2002

Most computer professionals dont use Computer Forensics, but learning about the ways an attack is carried out and the traces left behind can help when running computers in a secure way. Further getting back to a reliable and clean system after an incident is also paramount for organisations today!

This course shows some of the tools of the trade and help ordinary computer professionals clean up after incidents, by showing the places to look and clean.

(2 dage) [more information](#)

## Modern Firewalls and Internet Security

Modern firewalls are obstinate creatures, which are expected to protect the network from all exterior threats. On this course "Modern Firewalls and Internet Security" the threats and scenarios will be treated in a half day full of practical examples and concrete advice to the building of a modern firewall to securing the perimeter of network and Internet connections.

(2 day workshop) [more information](#)

## UNIX security

The Internet and UNIX is closely related and today UNIX is one of the most important platforms for Internet. Most UNIX systems are being installed in an open and insecure default configuration which must be hardened and maintained to secure data and availability of the system.

In this courses we will go through UNIX security and scenarios with a lot of hands-on examples and exercises.

(3 day workshop) [more information](#)

## IPv6 - Internet Protocols version 6

The Internet has through more than 20 years been through radical changes, and this success has caused the technology to show aging signs in several areas. IPv6 which is expected to replace the current technology contains many new and exciting new promises. This workshop will cover the history, technology and scenarios with real-life examples and practical exercises.

(one day workshop) [Further info](#)

## **Wireless Technologies and Security**

Wardriving in developed areas reveals in a short time a wealth of unprotected wireless networks which anyone can use freely. If the company doesn't discuss the use of wireless networks there is a risk that the network security is compromised through the use of unauthorized equipment which is connected. This course uses 802.11b and compatible as a starting point to grasp the problem and recommend concrete solutions to the security problems inherent in these wireless networks. The course is targeted at companies that consider implementing wireless networks without accepting unnecessary high risks.

(2 day workshop) [Further info](#)

## **Buffer Overflows and Exploit Programs**

One of the most important security problems of the time is buffer overflows and accompanying exploit programs. A vulnerable service on a server can today often be compromised by the use of a few network packets with harmful instructions to take over the control. In this course the problems with buffer overflows are treated and some proactive solutions to counter the threats from exploit programs are shown. The course is specifically well suited to all developers of software and web solutions.

(one day workshop) [Further info](#)

## **Security Awareness for web developers**

Those involved in building and maintaining our systems has an extremely great influence on the security level. Through examples and discussion the awareness is increased in those critical areas, where the security level can be improved in

typical installations. The participants will after the workshop be prepared better for identifying weak points and choose to implements stronger security measures.

(2 day workshop)[Further info](#)

## Security Tendency Seminars

In this seminar the security incidents and tendencies from the previous quarter will be reported and linked to an actual demonstration. By participating once each quarter on these seminars will update the participants knowledge with the most important incidents and enable them to take active part in securing the network and their company with firm base in the focus recommendations which the concludes the seminar.

(half day seminar held once each quarter)

## Security Policy - Developing and Communicating It

Threats against companies are today tangible and direct, and the cost of reducing risks can be hard to control. One of the tools to reach a balanced investment in information security is a security policy, which lay down the rules for the use of IT-systems and related information assets. This course is for everybody that wants an updated information security policy to be incorporated into the company. The participants will be able drive the development and implementation of an IT security policy in their own environment. This course is takes of using the SecureAware Policy product from Neupart A/S as a starting point.

(2 day course)

## Partners

## Default Publication

Many of the courses offered are held through other education partners and can also be held at your company for a small group.