OWASP-NL Meeting announcement

September 24th 2008: Unauthorized Access

Summary
The main goal of the upcoming OWASP-NL meeting is to provide information to managers, architects, designers, developers and security and risk professionals. The speakers will give specific examples and there will be time to ask questions.

Please register before September 18th because of the necessary catering arrangements.

Location
The location and catering is provided by the sponsor of this meeting:

Sofitel Cocagne
Eindhoven
Vestdijk 47
5611 CA Eindhoven

For the route by car or public transport please visit:
www.sofitel.com

Madison Gurkha

Madison Gurkha ondersteunt organisaties met kwalitatief hoogwaardige diensten bij het efficiënt identificeren, verminderen en voorkomen van (technische) ICT security-risico's.
Madison Gurkha is de volstrekt onafhankelijke specialist op het gebied van technische ICT security audits, ICT security consultancy en tailor-made opleidingen , zoals secure programming, applied hacking en forensics light.
Madison Gurkha werkt voornamelijk voor grote (beursgenoteerde) organisaties die veel waarde hechten aan

ICT-beveiliging en die op dat gebied alleen met topspecialisten genoegen nemen.
Lees meer op: www.madison-gurkha.com of www.itsx.com

Program

18.00 - 18.30 **Check-In** (catering included)

18.30 – 18:45 **Introduction** (OWASP organization, projects, sponsor)

18.45 - 19.45 **Unauthorized Access**

Wil Allsopp

Physical Penetration Testing and Social Engineering have been conducted by testing organisations for some time but there has been very little discussion within the industry regarding the use of formal approaches ensuring a consistently high quality and repeatability of the testing lifecycle.

This was a problem I attempted to address in the book Unauthorized Access and is the focus of this discussion.

We will look at the following:

- What is physical penetration testing and what does it aim to achieve?
- Tactical approaches to Social Engineering in testing.
- The advantages and disadvantages of deploying SE.
- Training operators and building operating teams - what skill sets should you deploy?
- What are the legal aspects involved, how do these vary between jurisdictions?
- How should you plan a physical penetration test at strategic, tactical and operational levels?
- How do you gauge risk i.e. Contractual, Operational, Legal and Environmental?

The biggest problem currently facing physical penetration testing teams is that it's hard to prove a negative i.e. a failed test by no means guarantees the security of the client. By ensuring your team is trained and prepared you can mitigate this problem to a large degree.

19.45 – 20.00 **Break**

20. 00 – 20.30 **Mini Meetings: Time- Box testing & Test Tools**

Barry van Kampen en Dave van Stein

20.30 – 21.00 **Education Project (NNTB)**

Martin Knobloch

21.00 – 21:30 **Discussion, questions and social networking**

Registration

If you want to attend, please send an email to:
netherlands-board@lists.owasp.org

Please register before September 18th, because of the necessary arrangements.

All OWASP chapter meetings are free of charge and you don't have to be an OWASP member to attend. There are never any vendor pitches or sales presentations at OWASP meetings.

NOTE TO CISSP's: OWASP Meetings count towards CPE Credits.

More information on the OWASP Dutch Chapter can be found on: http://www.owasp.org/index.php/Netherlands