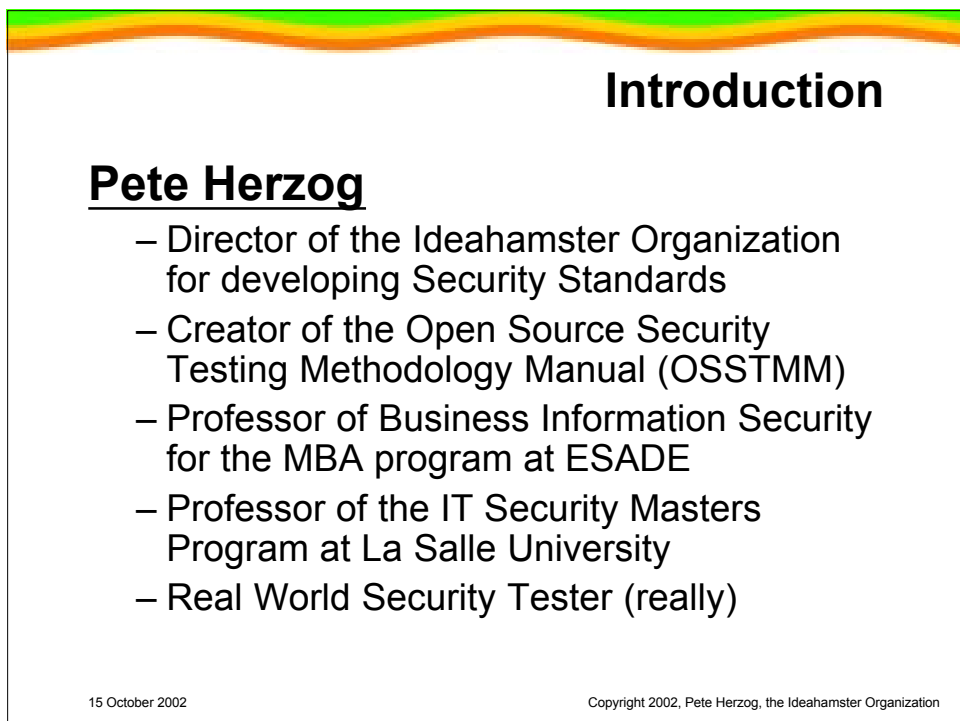


15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



Introduction

Pete Herzog

- Director of the Ideahamster Organization for developing Security Standards
- Creator of the Open Source Security Testing Methodology Manual (OSSTMM)
- Professor of Business Information Security for the MBA program at ESADE
- Professor of the IT Security Masters Program at La Salle University
- Real World Security Tester (really)

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



The Ideahamster Organization

- Established in January 2001.
- Dedicated to the development of security standards.
- Uses an open, peer-review process.
- An independent, non-political, non-profit, third party.
- Hosting 5 projects currently with 4 more in process.

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

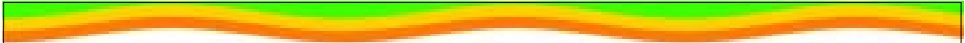


Current International Projects

- SPSMM
- OSSTMM
- OPRP
- OPST
- OPSA
- Applied OSSTMM
- OSSTMM Cheat sheet

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



Current Spain-Only Projects

- OSSTMM Internals
- Hacker High school
- Testing Data Center

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



The OSSTMM Project

- First and most widely accepted standard in development for the security testing.
- It has been downloaded over 1 million times worldwide since March 2001.
- Over 300 collaborators.
- Translation into 8 different languages underway.

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



The OSSTMM Difference

- **Worldwide Security Testing Standard**
 - No competitors
- **Open Methodology**
 - Contributors from over 20 Different Countries
 - Peer Review
 - Subject for a Masters and PhD thesis
- **Free to Implement**
 - Licensed under the Open Source License - GNU General Public License
 - Available for free download from www.osstmm.org

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



Compliance

- **Local / National Laws**
 - Spanish LOPD Ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal Art.15 LOPD -. Art. 5
 - Health Insurance Portability and Accountability Act of 1996 (HIPAA).
 - UK Data Protection Act 1998
- **Private Groups**
 - ISO 17799-2000 (BS 7799)
 - SET (Secure Electronic Transaction Compliance Testing Policies and Procedures)
- **Government Groups**
 - GAO and FISCAM
 - NIST (National Institute of Standards and Technology)

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

When nothing seems to help, I go and look at a stonecutter hammering away at his rock perhaps a hundred times without as much as a crack showing in it. Yet at the hundred and first blow it will split in two, and I know it was not that blow that did it, but all that had gone before.

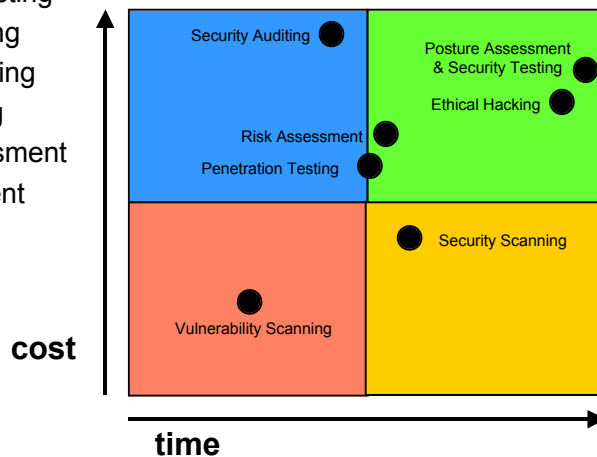
Jacob Riis

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Understanding Security Testing

- Vulnerability Scanning
- Penetration Testing
- Security Auditing
- Security Scanning
- Ethical Hacking
- Posture Assessment
- Risk Assessment



15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



The Security Testing Profession

- Helpdesk Support Person
 - communication and support
- Statistician
 - risk assessments and metrics (ROI)
- Safety Officer
 - disaster control
- Trainer
 - knowledge transfer
- Privacy Officer
 - policy and legal conditions

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



The Professional

SECURITY

- 
- Network Architect
 - Software Tester
 - Safety Inspector
 - Business Development
 - Operations
 - Marketing
 - Human Resources
 - Incident Management
 - Forensics

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



Defining Security Testing

- Quantifiable
- Consistent and repeatable
- Valid beyond the "now" timeframe
- Based on merit of the tester and analyst not on brands
- Thorough
- Compliant to individual and local laws and the human right to privacy

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



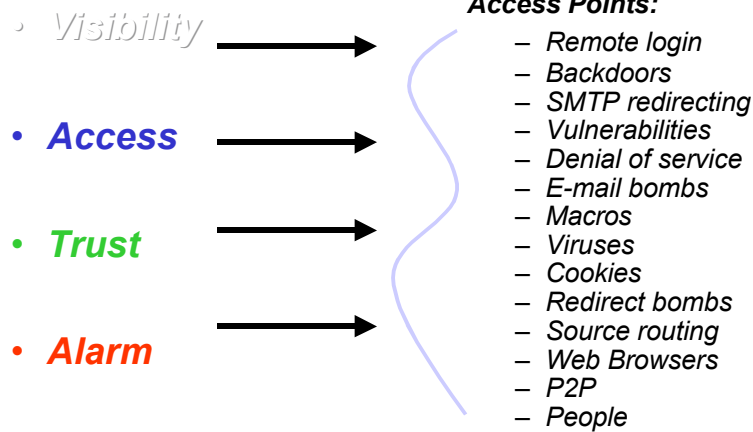
Security Testing in Practice

- Defining usable security
- Determining business justifications
- Reviewing internal processes and policies
- Complying to the various laws
- Building trust
- Promoting freedom not paranoia

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Defining the Security Presence



15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Visibility

- What can be seen in the security presence?
 - Open and filtered ports, types of systems, architecture, applications, email addresses, employee names, the skills of the new sys admin being hired through a job search online, circulation of your software products, websites visited by employees, everything employees download, chat programs employees use, etc...

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



Access

- Why do people enter your security presence?
 - Web pages, an e-business, a P2P server, DNS server, streaming video, anything in which a service or application supports the definition of quasi-public; where an outside person/computer interacts with another person/computer within your organisation.
 - Limiting access means denying all except what is expressly justified in the business plan and/or security policy.

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



Trust

- How much can you depend on what is in your security presence?
 - Trust depends on the kinds of, and amount of authentication, non-repudiation, access control, accountability, data confidentiality, data integrity employed by the system(s).

Sometimes trust is the basis for a service...

- Whenever one computer links to another, examples of trust 'partnerships' being VPNs, PKIs, HTTPS, SSH, B2B connections, database to server connections, e-mail, employee web surfing, any communication between two computers which causes interdependency between two computers whether server/server, server/client, or P2P.

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Alarm

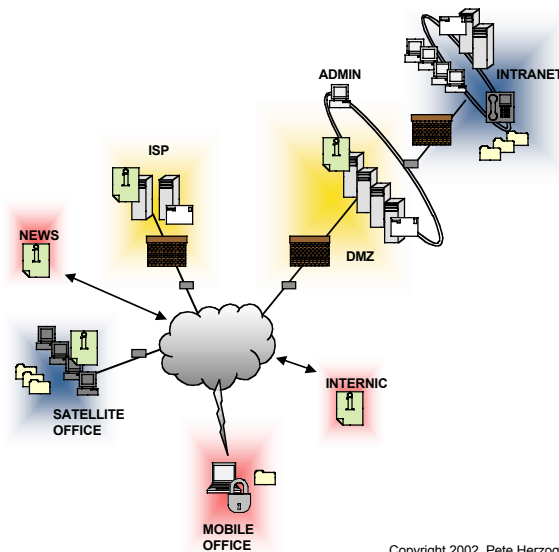
- How can you be timely and appropriately notified of activities that violate or attempt to violate **Visibility, Access or Trust?**
 - Log file analysis, port watching, traffic monitoring, intrusion detection systems (IDS), sniffing/snooping.

Alarm is often the weakest link in appropriate security measures.

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Internet Security Presence



15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

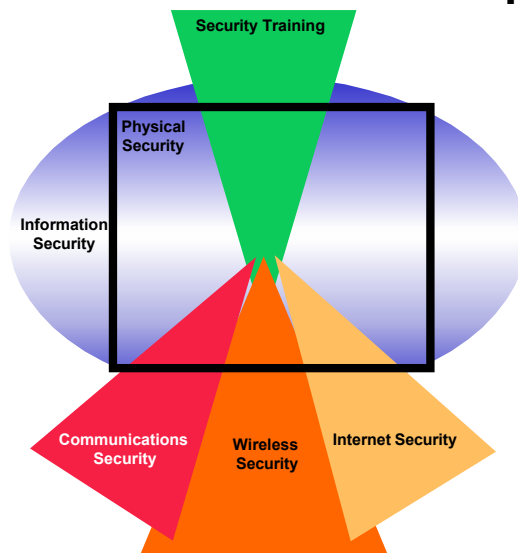
Security Map

- The security map is a visual display of the security presence.
- The security presence is the environment of an organization which affects security.
- It is comprised of six sections:
 - » Internet Security
 - » Information Security
 - » Physical Security
 - » Communications Security
 - » Wireless Security
 - » Security Training

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

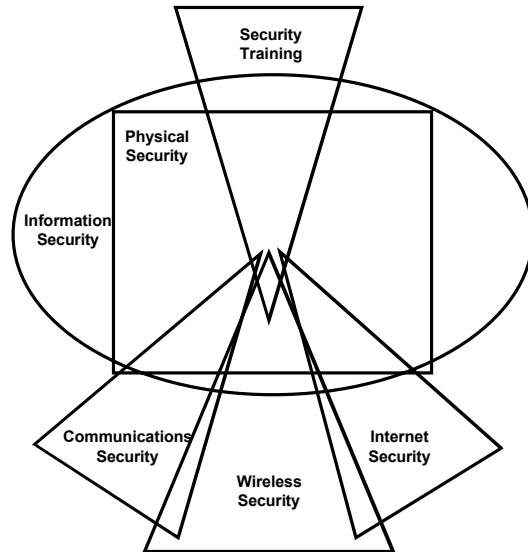
Mapped



15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Connected



15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Internet Security

- Visible Network Design and Architecture
- Open and Unfiltered Ports
- Available Services
- Available Systems
- System and Service Vulnerabilities
- Available Internet Applications
- Routers
- Trusted Systems
- Firewalls and IDS
- Intrusion Detection Systems
- Containment Measures
- Internal Clients



15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Physical Security



- Access Control Measures
- Perimeter Security
- External Perimeter Monitoring
- Alarm Requirements
- Alarm Reaction Measures
- Location Requirements
- Environmental Requirements



15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Information Security



- Business Information
- Public and Internal Privacy Requirements
- Information Leaks
- Login Information and Passwords
- System and Network Information
- Internal Processes and Procedures



15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Communications Security

- The Phone Exchange (PBX)
- Voicemail
- FAX
- Modems
- SMS
- WAP



15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Security Training

- External Requests
- Forged Internal Requests
- Guided Suggestions
- Reversed Request



15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Wireless Security

- Wireless Networks
- Cordless Communications
- Public and Private Privacy Requirements
- Infrared Systems
- Visible Light Systems



15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Goals for Security Test

- Assess IT and Information Security Vulnerabilities and Threats
- Recognize Security Best Practices
- Recognize the Business Risks
- Recognize Privacy Issues both Internal and External
- Suggest / Implement Practical Security Solutions

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Limits of Security Test

- Loss of business (down time)
- Wasted resources (employee reactions to alarm states)
- False sense of Security
- Superficial
- Process failures
- Politics

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

OSSTMM Requirements

- Overview (Executive Summary)
- Network and Domains tested
- Online Information Collected
- Persons
- Technologies
- Postings
- Containment Measures Tested
- Vulnerabilities Discovered
- Packet Response Details
- Services Discovered
- Systems Identified (Fingerprinted)
- Privacy Policies and Laws Reviewed and Results
- Firewall Tests and Responses
- IDS Tests and Responses
- Social Engineering Tests and Responses
- Vulnerable Internet Applications Discovered
- Competitive Intelligence Info Analyzed
- Vendors
- Partners
- Future Planning
- Trust Analysis
- Password Cracking

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

The Methodology

- Designed for parallel input
- Provides precise data extraction and testing points in the Internet presence
- Does not restrict creativity
- Provides consistency
- Open to new technology
- Built on complex relationships between modules and tasks
- Not limited to the Internet.



15 October 2002

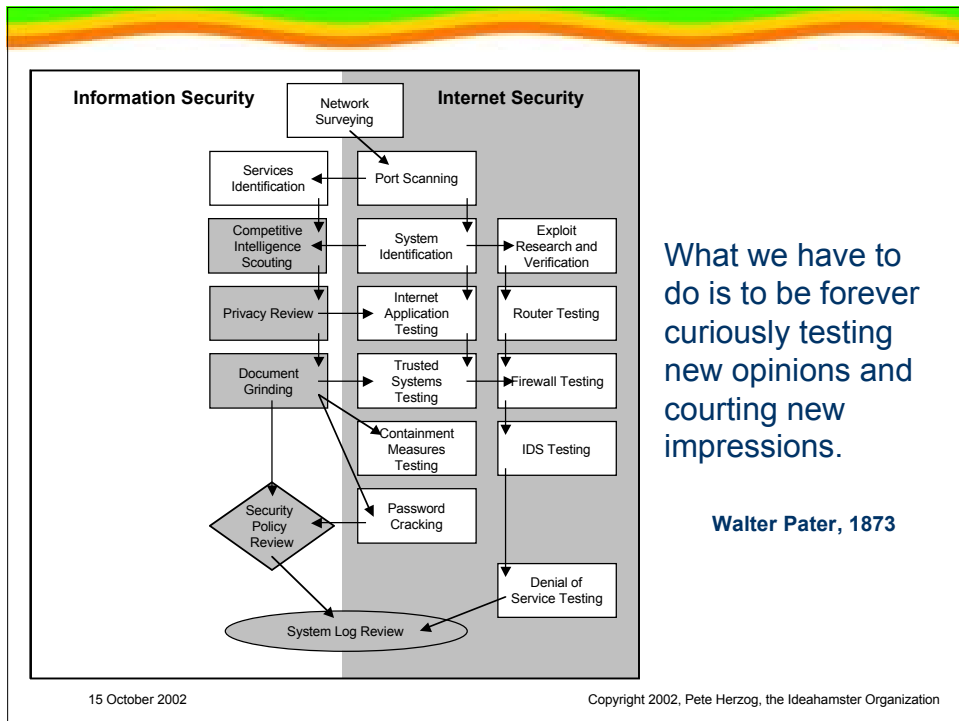
Copyright 2002, Pete Herzog, the Ideahamster Organization

Modules

- The methodology is broken down into modules and tasks.
- The modules are the flow of the methodology from one Internet Presence Point to the other.
- Each module has an input and an output.
- The input is the information used in performing each task.
- The output is the result of completed tasks.

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



What we have to do is to be forever curiously testing new opinions and courting new impressions.

Walter Pater, 1873

Module Without Output?

1. The tasks were not properly performed.
2. The tasks revealed superior security.
3. The task result data has been improperly analysed.
4. The task was not applicable.

Dissecting the Module

Module Example

Module Name		tools link
Section Name	RAV cycle	RAV description
Description of the module.		
Expected Results:	Item Idea Concept Map	
Tasks to perform for a thorough		
Group task description.		
<ul style="list-style-type: none">• Task 1• Task 2		

15 October 2002

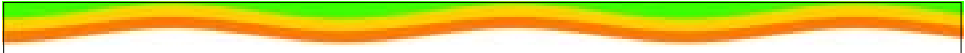
Copyright 2002, Pete Herzog, the Ideahamster Organization

To win without risk is to triumph without glory.

Pierre Corneille, 'The Cid,' 1636

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization


$$\text{RAV} = \frac{\text{degradation}}{\text{cycle}}$$

RAVs

Determined mathematically by three factors:

- The degrees of degradation of each separate module from point of optimum health measured from a theoretical maximum of 100% for risk management purposes,
- The cycle which determines the maximum length of time it takes for the degradation to reach zero based on security best practices for regular testing,
- Weights based on the process areas of Alarm, Trust, Visibility, and Access

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



RAVs

- Solves a business problem:
 - How secure am I and compared to what?
- Answers the questions:
 - How often do I need to do a security test?
 - How deep?
 - How do I compare to others?
 - What is the baseline?
 - So what percentage is realistically secure for me?
 - What about my industry?

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

RAVs

- Based on “Analog” or “Shades of Gray” defined as processes and interactions
- While sec testing is really testing configuration and policy
- Timeliness plays a part
- Size generally doesn't matter (to some point)

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Using RAVs

- Enumerate
- Designate
- Calculate

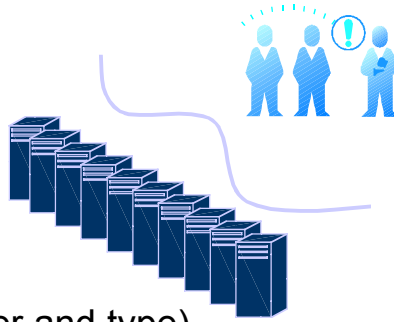
$$RAV_{var} = \left(1 - \left(\frac{\text{deg} / 100}{\text{cycle}} \right) \right)^{\text{days}} \times RAV$$

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

Planning an OSSTMM Security Test

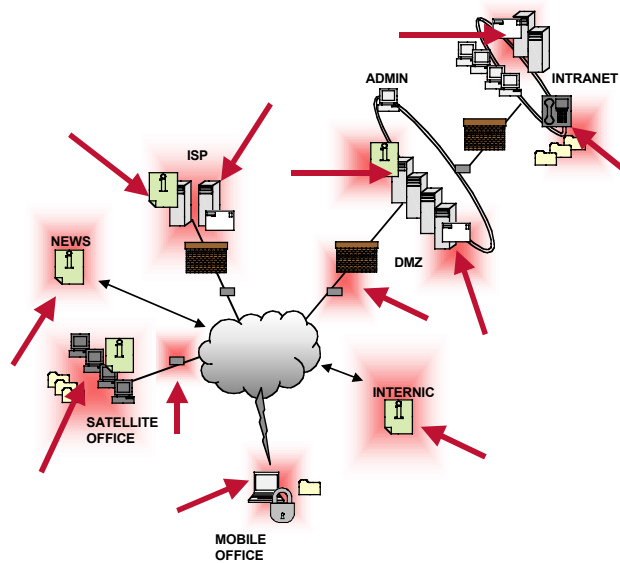
- Time
- Man Hours
- Place
- Target
 - services
 - systems (number and type)
- Presence



15 October 2002

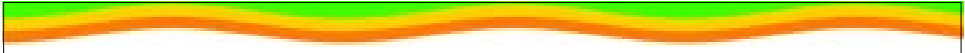
Copyright 2002, Pete Herzog, the Ideahamster Organization

Scope



15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



Where a calculator on the ENIAC is equipped with 18,000 vacuum tubes and weighs 30 tons, computers in the future may have only 1,000 vacuum tubes and perhaps weigh 1.5 tons.

unknown, **Popular Mechanics**, March 1949

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



The Future

- Business Integrity Testing Methodology
 - security testing for personnel, systems, and data.
- OSSTMM Internal
 - a solutions-based internal assessment to reduce audit and consultancy time

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



The Future

- OSSTMM Professional Security Testing certification (OPST)
 - *Aggressive Security Testing 1*
 - *Aggressive Security Testing 2*
 - *Business Security Bootcamp*

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization

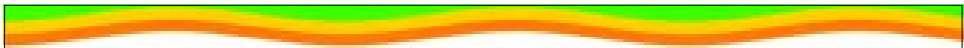


The Future

- OSSTMM Professional Security Analysis certification (OPSA)
 - *Professional Security Analysis*
 - *Redteam Strategies*
 - *Security Project Management*

15 October 2002

Copyright 2002, Pete Herzog, the Ideahamster Organization



pete@ideahamster.org



Questions?