



OUTCLASS THE HACKERS

Training In Real World Computer Security

**OSSTMM Professional Security
Testers OPST Certification Course
Sydney Australia 2007**

Register at <http://www.purehacking.com/training.php>



PureHacking
Protecting Business Intelligence



Overview:

Are you a current security tester seeking more structure to the process, or an IT professional wishing to add security testing to your skills or responsibilities?

Pure Hacking, the only dedicated, vendor neutral ethical hacking company in Australia is offering the OSSTMM Professional Security Testers (OPST) certification course to a limited number of IT professionals.

The OPST certification is the official security testing certification based on the Open Source Security Testing Methodology Manual (OSSTMM available at www.osstmm.org).

While the OSSTMM provides the structure for “What” to perform in a security test, the OPST provides the “How”. The course covers:

- which tools to use,
- how to use the tools, and most importantly,
- the methodology behind security testing.

The course builds on your existing network and systems knowledge and provides you with the skills to become a security tester or for the more experienced, the course will expand your knowledge and make your tests more complete.

The training course will support the necessary knowledge transfer for a person to be considered a capable, resourceful, and self-sufficient security tester.

The course focuses on the technical skills necessary for security testing and the business skills required in understanding contemporary business and security needs. The final certification exam is based on these two areas.

Facilitator: Ty Miller (OPSA and OPST, Certified OSSTMM Trainer)

Ty is an experienced Security Consultant with a history of delivering projects in all conditions.

Over his career he has gained knowledge and experience in multiple technologies and has been involved in developing solutions across a wide number of business processes, infrastructures, operating systems, and technologies. Ty will also be writing a chapter in the upcoming Hacking Exposed book on Web Application Testing.

Ty's daily function is penetration testing, and has tested thousands of systems and applications.

Course Outline:

The course covers the following three areas:

Business Information Security is the information security knowledge baseline for the business needs of security testing and incorporates:

- client confidentiality
- risk assessment
- testing legalities
- reporting
- the testing process
- the rules of engagement

Practical Security Testing is the technical baseline for the terms and needs in security testing based on the latest version of the OSSTMM for providing assessments and estimations.

Aggressive Security Testing is the advanced technical baseline for the terms and needs to provide a complete OSSTMM-certified security test of the Information and Internet security sections.

The course helps you understand:

- The “Why?” of the OSSTMM sections (Human and physical security, wireless communications, data networks and telecommunications)
- The “How?” for the data networks section.

This training course supports the necessary knowledge transfer for your staff to be considered a capable, resourceful, and self-sufficient security tester.

From this training, you will:

1. learn how to use the tools for security testing, including advance penetration testing techniques
2. gain an excellent foundation in testing tools functionality
3. enhance your skills and practice against a realistic Internet network
4. gain a wealth of security and networking information.

After completion you will have an understanding of how to complete various security testing techniques such as Competitive Intelligence Scouting, Privacy Review, Document Grinding, Network Surveying, Port Scanning, Services Enumeration, System Identification, Advanced System And Infrastructure Identification, Traffic Analysis and Error Detection, Vulnerability Research and Testing, Exploit Tools and Techniques, Web Application Testing, Network Manipulation and Sniffing and Password Cracking.





Prerequisites

The prospective candidate should have a good understanding of:

- TCP/IP and related protocol
- Experience of UNIX and Windows systems
- An understanding of network and systems security concepts and devices



Pure Hacking

Pure Hacking is the only security company in Australia dedicated to penetration testing. This sole focus has allowed the business to concentrate in the one area and build a reputation for quality and excellence. This experience and focus is harnessed in our training and is now available to you.

With offices in Sydney, Melbourne and Singapore, Pure Hacking services clients in 14 countries around the world. To find out more, visit: www.purehacking.com

As one of our clients recently stated:

"The team at Pure Hacking distinguish themselves by successfully communicating difficult technical concepts to all levels. They also followed through with their promise to continue support in explaining these concepts long after our contract finished."

IT Manager – Production Systems, International Business Services Corporation

Quotes such as this demonstrate our exceptional skills transfer, communication skills, focus on the client and value added long after all agreements are finished. Pure Hacking's skill and support of you, is what sets our business apart in the IT security market.

Course Outline

Day 1: OSSTMM Introduction, Implementation and Passive Testing

Theory

- Introduction
- Setup and Rules
- What is the OPST?
- Difference between OPSA and OPST
- OPST Exam Process
- What is the OSSTMM?
- Certifications
- Rules of Engagement
- 4 Point Process
- Auditors Trifecta
- Combined Method
- Security Test Types
- Error Types
- RAV Overview
- Test Error Risk Margin

Practical

- Competitive Intelligence scouting
- Privacy Review
- Document Grinding

Day 2: Understanding OSSTMM and Penetration Testing Tools

Theory

- The Security Presence
- OSSTMM Terminology
- Structure of the OSSTMM
- Modules Overview and Flow
- Modules in Detail
- Regulatory Phase
- Legislation, Regulation and Policy Compliance
- Definitions Phase
- Information Phase
- Interactive Controls Test Phase
- Security Metrics
- Applying Risk Assessment Values (RAVs)
- Operations
- Controls
- Limitations
- Actual Security
- RAVs Calculation
- OSSTMM Audit Report
- Helpful Resources

Day 2: Understanding OSSTMM and Penetration Testing Tools (cont)

Practical

- Network Surveying
- Port Scanning
- Services Enumeration
- System Identification

Day 3: Advanced Penetration Testing Techniques

Practical

- Advanced System and Infrastructure Identification
- Traffic Analysis and Error detection
- Vulnerability Research
- Vulnerability Testing
- Exploit Tools and Techniques

Day 4: Review plus Web Application and Network Manipulation

Theory

- Review of OPST course

Practical

- Web Application testing
- Network manipulation and sniffing
- Password cracking

Day 5: Open Review and OPST Exam

Theory/Practical

- Open Question and Answer Review
- Exam

Register at

<http://www.purehacking.com/training.php>

Course Information:

Duration	5 days (9am to 5:30pm)
Date	Courses commencing 26th February, 18th June, 17th September & 19th December 2007
Facilitator	Ty Miller (OPSA and OPST, Certified OSSTMM Trainer)
Cost	\$AUD3500 (x GST) – GST free for non Australian businesses
Location	Sydney, Australia
Includes	Forty (40) hours of intensive training Four (4) hour OPST Certification Exam on Day 5 A copy of course presentation materials OSSTMM Office Courseware books Bound edition of the latest Open source Security Testing Methodology Manual (OSSTMM) Lunch, morning and afternoon tea and coffee Linux systems provided NB: Windows laptops may be used at students own risk.
Examination	4 hr via Internet to remote test network
Qualification	The OPST Certification
Limitation	8 positions per course. Please book early to avoid disappointment.
Contact	To register contact Robert McAdam - 61 2 9545 7750 or visit Pure Hacking at - www.purehacking.com training@purehacking.com

PROTECTING BUSINESS INTELLIGENCE

www.purehacking.com



Head Office

SYDNEY
Chifley Tower
Level 25,
2 Chifley Square
Sydney, NSW 2000
Australia

MELBOURNE
Level 50,
101 Collins St
Melbourne, VIC 3000
Australia

POSTAL ADDRESS
GPO Box 3368
Sydney, Australia 2001

SINGAPORE
Penthouse Level
Suntec Tower Three
8 Temasek Boulevard
Singapore 038988

Tel: +61 2 9545 7750

Fax: +61 2 9545 7751

Free Call 1300 884 218

info@purehacking.com

Tel: +65 6763 6578

Fax: +65 6462 5308

Internet

B2B

Applications

VoIP

Wireless

Infrastructure

