

RE: Pen test courses

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-05/0114.html>

From: Roger Bou-Aoun (*roger.bouaoun_at_ndu.edu.lb*)

Date: 05/29/03

To: "'JC'" <security-focus@resnulus.net>, "'Cox, Michael'" <msox@ti.com>, <pen-test@securityfocus.com>
Date: Thu, 29 May 2003 08:33:13 +0200

Hi All,

The difference between them is that the first one is Technical and the other one is Business oriented, it should be the next step after OSPT, CISSP, CISA...

Kind Regards

Division of Computing Services

Roger Bou-Aoun, Head
Information Security & Internetworking Department
Notre Dame University
Tel: 961-9-218-950 ext 2266
e-mail: roger.bouaoun@ndu.edu.lb

-----Original Message-----

From: JC [mailto:security-focus@resnulus.net]
Sent: Wednesday, May 28, 2003 7:54 AM
To: Cox, Michael; pen-test@securityfocus.com
Subject: Re: Pen test courses

Hi Michael,

I can't really give you a good comparison between the Isecom OPST and OPSA trainings without having much details about the SANS training courses...

What I can tell you is that the OPST and OPSA courses are based on the OSSTMM (Open Source Security Testing Methodology Manual). Isecom developed the OSSTMM, this methodology has evolved with the feedback from many security professionals, it is a living document that is in constant progress. Isecom has other open-source projects that all seem very interesting! You can download the OSSTMM from www.isecom.org. If you have ideas, you can feed them back to Isecom and your enhancements might make it in the official document! That is what I like about the

SecurityFocus Penetration: RE: Pen test courses

OSSTMM, its quality enhancements can be made by all of us!

There is no such reference on the SANS website I could find, maybe somebody that followed that training can give some more feedback on the source of the methodology used there.

For the technical side, the Isecom classes focus on getting the job done with open source tools first of all, avoiding automatic tools to make sure that you understand what exactly the various tests are meant to achieve and how to validate them as being successful. This is meant to enhance your insight on the subject.

I don't know for sure what the SANS courses concentrate on product-wise, here again, people who followed that training will be able to give you more details!

Cheers,
Martin

----- Original Message -----

From: "Cox, Michael" <mscox@ti.com>
To: "JC" <-none-@resnilius.net>; <pen-test@securityfocus.com>
Sent: Tuesday, May 27, 2003 3:43 PM
Subject: RE: Pen test courses

> *Can anyone comment on the OPST training vs. the SANS "Hacker
> Techniques, Exploits and Incident Handling" track or the SANS
> "Auditing Networks, Perimeters and Systems" track?*

>
> *Thanks!*
> *Michael*

>
> > -----Original Message-----
> > *From: JC [mailto:-none-@resnilius.net]*
> > *Sent: Monday, May 26, 2003 2:48 PM*
> > *To: Petr Ruzicka; pen-test@securityfocus.com*
> > *Subject: Re: Pen test courses*

> >
> >
> > *Petr,*
> >
> > *There are 2 very interesting courses from Isecom.org*
> > *(<http://www.isecom.org>):*
> > *These classes focus on the right methodology, ethics, law,*
> > *understanding of the tests, lifecycles of security tests,*
> > *organisational aspects, etc... In*
> > *other words, more than just using the tools, but*
> > *understanding how to use*
> > *them in the best way possible. These courses are based on the*
> > *Open Source*
> > *Security Testing Methodology Manual (OSSTMM) that is an open source*

RE: Pen test courses

SecurityFocus Penetration: RE: Pen test courses

> > *methodology to perform professional and complete security tests.*
> >
> > – *OSSTMM Professional Security Analyst (OPSA):*
> > " *The premise of the training course is to provide a variety of hard*

> > *and soft skills to the security professional. The training course*
> > *focuses on the*
> > *analytical skills and security knowledge necessary for*
> > *security and risk*
> > *analysis and the business skills required for successful*
> > *security team and*
> > *project management. This course is not about just passing the*
> > *exam. This*
> > *course is about bringing the combined, international knowledge and*
> > *experiences of security team leaders and security consultants*
> > *to bring depth*
> > *and insight to the training. "*
> >
> > – *OSSTMM Professional Security Tester (OPST):*
> > " *The premise of the training course is to support the necessary*
> > *knowledge transfer for a person to be considered a capable,*
> > *resourceful, and self-sufficient security tester. The training*
> > *course focuses on the technical skills necessary for security*
> > *testing and the business skills*
> > *necessary for providing justification, efficiency, and understanding*
> > *contemporary business and security needs. "*
> >
> > *Cheers,*
> > *Martin*
> >
> >
> > ----- *Original Message* -----
> > *From: "Petr Ruzicka" <pruzicka@openbsd.cz>*
> > *To: <pen-test@securityfocus.com>*
> > *Sent: Monday, May 26, 2003 11:37 AM*
> > *Subject: Pen test courses*
> >
> >
> > > *Hi,*
> > > *could you recommend me some valuable PenTest training ?*
> > > *I know already how to use nmap, ping/traceroute, nessus,*
> > > *hping, nemesi,*
> > > *tcpdump/etereal, ettercap, I know how to do passive fingerprint of*
> > > *OS, use various honeypots etc. etc.*
> > > *However, there is always something new to learn, I'm sure.*
> > > *I did some*
> > > *research of available training courses on the Internet and I'm not*
> > > *sure which could be valuable to me, as I do not need to spend time*
> > > *learning 'nmap -vv -sS -PO x.x.x.x'.*
> > > *Besides programming skills and researching new*
> > > *vurnabilities (and keep*

RE: Pen test courses

SecurityFocus Penetration: RE: Pen test courses

> > *running on learning track), is there any good training out there ?*

> > > *Thanks a lot*

> > >

> > > *Petr Ruzicka*

> >

>
