

RE: best tool to draw attack trees ??

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-03/0085.html>

From: Mike.Ruscher@cse-cst.gc.ca

Date: 03/25/02

From: Mike.Ruscher@cse-cst.gc.ca

To: mark@curphey.com, security@luddites.ca

Date: Mon, 25 Mar 2002 11:57:29 -0500

Just a thought... there is a lot of COTS and shareware/freeware genealogical software kicking around which are tree structures and can be linked to more information and images. I would take a look at these initially.

mgr

Mike Ruscher, ITS Specialist I2, CSE/CST

mike.ruscher@cse-cst.gc.ca

Phone: +1 613 991-8040

ED/C200

<http://www.cse-cst.gc.ca>

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

From: Mark Curphey [mailto:mark@curphey.com]

Sent: Saturday, March 23, 2002 5:08 PM

To: security@luddites.ca

Cc: 'pen-test@securityfocus.com'; Kruse, Darren (DEH)

Subject: Re: best tool to draw attack trees ??

We looked at Attack Trees at OWASP (<http://www.owasp.org>) ages ago. More important things got in the way (like building Web Scarab and the Input / Output API's) but we played with UML Sequence diagrams and it certainly was a effective way of doing attack trees.

<http://www.owasp.org/pen-test-list-phf.gif> is the only old example I can find now of the classic Phone Book script.

A good Open Source freeware tool is Poseidon Commuity Edition from www.gentleware.com

Worth pointing out they seem to have been derived from earlier work by Jeff Voas and Gary McGraw in their books Software fault injection.

On Fri, 2002-03-22 at 18:22, lit sec wrote:

> *Attack Trees, eh?*

>

RE: best tool to draw attack trees ??

SecurityFocus Penetration: RE: best tool to draw attack trees ??

> I've had a look at the Java-based solution over at <http://www.amenaza.com/>
. Looks like it might suit your needs. Fairly easy to use, and does a hell
of a lot more than Visio. Here's a quote: "(Amenaza) ...the developers of
SecurITree, a risk assesment tool and methodology that can help your
organization determine possible threats to your IT systems and how to best
ward off these threats."

>
> -Luddites.Canada

> ----- Original Message -----

> From: "Kruse, Darren (DEH)" <Kruse.Darren2@saugov.sa.gov.au>

> Date: Fri, 22 Mar 2002 13:30:18 +1030

> >I'm puzzling over what is the best way to draw attack trees.
> >Attack trees provide a formal, methodical way of describing the security
of

> >systems, based on varying attacks. Basically, you represent attacks
against

> >a system in a tree structure, with the goal as the root node and
different

> >ways of achieving that goal as leaf nodes.

> >Bruce Schnier's Secrets and Lies – Digital Security in a Networked World

> ><http://www.amazon.com/exec/obidos/ASIN/0471253111/qid=1016671800/sr=8-1/ref>

=
> >sr_8_67_1/002-8209990-0206427 , in particular chapter 21 covers Attack
Trees

> >There's also a DDJ article on attack trees

> ><http://www.ddj.com/documents/s=896/ddj9912a/9912a.htm> (also by Bruce
> >Schnier) that covers virtually the same ground as the book.

> >I'm thinking that it would make a really good motivational tool for

> >management to see what all the threats are against our systems.

> >Having a documented attack tree would also help me in identifying what
holes

> >,and threats I need to worry about RIGHT NOW !

> >My first thought was to wade in, and start drawing with Visio – making
use

> >of the layers feature to distinguish between different sets of values..

> >Possible / Impossible Cost script kiddie tool released ?

> >etc..

> >But does anyone know of a more "closely-suited" tool than Visio ? I've
done

> >a google search on "attack tree" software, and come up blank.

> >There are cheaper alternatives to Visio – maybe Kivio mp

> ><http://www.thekompany.com/products/kivio/faq.php3> ?? Unfortunately, the
KDE

> >version (Kivio without the mp suffix) doesn't do layers. :-(

> >Would a web interface be better ? – certainly for navigating between

> >threats, but how about when you want to see a larger part of the tree ? ,

RE: best tool to draw attack trees ??

SecurityFocus Penetration: RE: best tool to draw attack trees ??

- *Previous message:* [Davis, Matt: "Exploits for Un-patched Windows NT SNMP vulnerability"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)