

Re: Heavyweight Network Mapping Tools

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-11/0105.html>

From: Andy Cuff [Talisker] (talisker_at_securitywizardry.com)

Date: 11/29/03

To: "Robert E. Lee" <robert@isecom.org>, <pen-test@securityfocus.com>

Date: Sat, 29 Nov 2003 21:59:46 -0000

Hi Robert,

Thanks a lot for such a comprehensive reply

> <http://www.lumeta.com/ipsonar.html>

>> *The Lumeta stuff is very good, but costly and mostly closed. It is*

> *leveraging work from William Cheswick and Hal Burch.*

I've come across this before and to my knowledge and largely confirmed by the site case studies they run the discovery themselves, whilst this is ok it tends to be expensive furthermore subsequent updates get expensive. I'd look for the ability to schedule the scan for the quiet hours and have multiple threads so as not to adversely effect any individual sub network too greatly. As soon as the initial scan is complete the process starts over, highlighting changes from the initial baseline. The output from this is then used to drive the active OS fingerprinting.

The visualisation is perfect

>

> <http://www.opte.org>

The OPTE project has Barret Lyon of Network Presence (main developer) and

> *Dan Kaminsky of Avaya's Enterprise Security Practice (Author of*

> *Paketto/scanrand) behind it. The goals for the OPTE project are slightly*

> *different than what you've described, but could easily be adapted to your*

> *needs.*

The code is only 70% complete, though the data is very interesting, where do I find the base?

>

>> *Mandatory*

>> *Hosts alive through ICMP*

> *Fyi, I plan on taking the OPTE project base and modifying it for uses such*

> *as what you've described. However, instead of using ICMP I plan on*

> *implementing automated scans/system finding based on an abbreviated*

Section

> *C, Modules 1-3 of the OSSTMM (<http://www.osstmm.org> pages 45-48). This is*

> *far more complete for flushing out live systems and works equally well on*

SecurityFocus Penetration: Re: Heavyweight Network Mapping Tools

> *internal and external systems alike. I'll have all of this stuff logging*