

Re: Class on Security Tools

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-12/0177.html>

From: GuidoZ (uberguidoz_at_gmail.com)

Date: 12/19/04

Date: Sun, 19 Dec 2004 02:42:03 -0500
To: Todd Towles <toddtowles@brookshires.com>

Nice thoughts Todd. Another open source program I've been playing with lately that may be of interest to you – Attack Tool Kit or ATK (<http://www.compute.ch/projekte/atk/>). It's currently in version 3.0 and isn't bad at all. Here's a direct copy/paste from the "Introduction"

"The acronym ATK stands for Attack Tool Kit. It was first developed to provide a very small and handy tool for Windows to realize fast checks for dedicated vulnerabilities. The special thing about ATK is that the tool is able to do the work without great interaction. But there is also always the possibility to vary and change the behaviour of the software. This concern the plugins, checking, enumeration and reporting. The user is not dependent of the ideas of the developers – If needed because of the modularity nearly every change can be done within a few seconds. ATK is absolutely free to use and distribute. The software is written in Visual Basic and underlies the General Public License (GPL)."

The plug-ins are updated frequently with newly discovered exploits. I'd recommend peeking at it just for \$hits and giggles if nothing else. ;)

--

Peace. ~G

On Wed, 15 Dec 2004 11:39:44 -0600, Todd Towles
<toddtowles@brookshires.com> wrote:

> Hey Dan,

>

> Kismet was not covered in your first class?

>

> I don't understand how much Kismet is overlooked and NetStumbler is
> shown. NetStumbler is great but it is limited, it open shows open
> networks. Close/Cloaked networks are growing and Kismet is one of the
> few software tools that will see you them along with many many other
> features.

>

> Depends on what area you mainly want to focus on, but attack tool range
> is pretty wide. Hydra, for example. I would also hit on the new trend
> of Google hacking. Google is used by hackers and pen-tester alike to
> gather huge amount of information about a target. There is even a book
> being released soon, Google hacking for Pen-Testers - I believe. Wikto

SecurityFocus Penetration: Re: Class on Security Tools

> is a Windows Nikto-like tool with Google hack features. Of course, on
> the network side you have ettercap, packet sniffers like Ethereal and
> Dsniff. It all depends on where you want to focus. There are various
> wireless attack tools that shouldn't be overlooked.
>
> I would include the EBCD in the remediation/protection tool class
> instead of the attack class. Snort, Tripwire and the MBSA are good tools
> as well. The greatest protection measure you can have is knowledge.
> Knowing what services are running and why, what version they are and if
> there are updates for them. It takes time to watch the internet for news
> and alerts and active exploit, but you will learn where and when to
> focus your software measures to optimize your security.
>
> BTW, Helix is a great LiveCD for Windows Server Forensics Analysis.
>
> Of course, this is all just my 2 cents and open for discussion. =)
>
> -Todd
>
> > -----Original Message-----
> > From: Dan Tesch [mailto:dan.tesch@comcast.net]
> > Sent: Wednesday, December 15, 2004 7:18 AM
> > To: Pen Test
> > Subject: Re: Class on Security Tools
> >
> > Certainly Nessus should be covered, you could touch on NeWT.
> > www.nessus.org
> > <http://www.tenablesecurity.com/>
> >
> > -----
> >
> > I am helping teach a class to the ISSA of Northwest Ohio,
> > here in Toledo. The next class will be the second part of a
> > series on security tools. Last class we went over scanning
> > tools such as nmap, NetStumbler, nikto, and a couple others.
> >
> > This next class will be focused on attack tools. We were
> > planning on presenting Metasploit, EBCD for password changes,
> > and a couple other tools. My question is - what (free) tools
> > should we give a brief overview of? The class is technical,
> > mostly comprised of IT directors and the like. Most are not
> > dedicated security staffers, but rather have that as part of
> > their job responsibility. We don't have to go in depth, but
> > we are demonstrating on a network we have built for this purpose.
> >
> > Next month we will be doing remediation/protection tools. I
> > was thinking about showing Snort, Tripwire, Microsoft
> > Baseline Security Analyzer, and a couple others. Any ideas on that?
> >
> > Thanks in advance,
> > Joe Traband
> > jtraband@itscomputersolutions.com
> >
> >