

RE: Exploit package analysis

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-07/0369.html>

From: Todd Towles (toddtowles_at_brookshires.com)

Date: 07/28/05

Date: Thu, 28 Jul 2005 14:04:09 -0500

To: "Erin Carroll" <amoeba@amoebazone.com>, <pen-test@securityfocus.com>

A bit off-topic, but I would look into VMWare. There are several Linux tools that will work the same as well. A separate OS environment would be very helpful in your new interest. Plus, it is very easy to go back to a fresh OS state after a malware analyzing session.

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

> From: Erin Carroll [<mailto:amoeba@amoebazone.com>]

> Sent: Thursday, July 28, 2005 11:45 AM

> To: pen-test@securityfocus.com

> Subject: Exploit package analysis

>

> All,

>

> Some of the fun of moderating this list is getting a wide
> exposure to aspects of pen-testing I have yet to tackle. One
> thing managing the list has prompted me to explore is
> exploit/code package analysis... thanks to all the spam I get
> to sift through :)

>

> In addition to worrying about my poker game, manly endowment
> & performance, and Rolex collection (once I get money from my
> friends in Nigeria), I get a lot of spams with attachments,
> usually .zip, that are obviously malware that I'd like to
> open up safely and see how they tick. I'm hoping to pick up
> some interesting pen-test techniques by looking at the
> current state of malware exploits to see how they
> work/reproduce/hide at the system level. While most of them I
> assume will be run-of-the-mill spambot or zombie generators,
> there's always a chance of running across a 0-day in the wild.

>

> My question to all of you is what are some basic sandbox
> tools you would recommend to pursue this? Does anyone work in
> a similar vein and has the experience been helpful in your
> pen-testing work?

>

>

> --

SecurityFocus Penetration: RE: Exploit package analysis

- > *Erin Carroll*
- > *"Do Not Taunt Happy-Fun Ball"*
- >
- >