

Re: Pentesting tool – Commercial

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2008-03/msg00018.html>

- *From:* "Andre Girona" <andreg@xxxxxxxx>
 - *Date:* Tue, 4 Mar 2008 10:54:29 -0700
-

On Tue, Mar 4, 2008 at 4:47 AM, Trygve Aasheim <trygve@xxxxxxxxxxxxxxx> wrote:

Trygve,

Thank you for walking into my strawman argument / trap.

So the results from your fuzzers can be implemented into modules in these tools and tested

You used the secret word! "Fuzzers"! Woohoo!

The framework can then run the exploits for you continuously while you test different configurations and version of the target software.

Exciting. I bet that will work wonders.

What type of weakness are you attempting to exploit in this example? Stack-based buffer overflows? While I understand the issues behind the need to verify the system state's properties per stack-based buffer overflow exploit (and this is getting rather complicated thanks to /GS, SSP, SafeSEH, ASLR, et al) – making a reliable overwrite on EIP (and/or several other registers) is far more complicated than these tools can even handle.

Not to mention that stack-based buffer overflows aren't the popular software weakness that they used to be. It's more difficult to find them and exploit them than ever before.

What about the other 642 software weaknesses?

Also it helps if you are looking at exploiting an infrastructure more than just running one exploit against one target

Re: Pentesting tool – Commercial

"Exploiting an infrastructure" is funny to me. I bet you are talking about network-based IPS. Or maybe host-based?

First question: What's the best thing about IPS?

<Awkwardly long pause>

Answer: NOTHING!

Second question: What's the best thing about pen-testing?

<Insanely long pause>

Like HD Moore and Val Smith's speech at Black Hat 2007, where they showed how to use the output from one module as input into another module – and then achieve your goals

Achieve your goals! Fight to win!

Btw – they're called `mixins'. It's a programming language thing.

(WPAD -> HASH -> login into Windows Domain example)

I knew about the problems with WPAD 10 years ago, and so did everyone I knew at the time. This sort of thing doesn't magically become possible thanks to Ruby.

The same approach are used by malware developers now, and mpack is a good example

What approach? You mean programming?

We're also seeing more and more fuzzingtools being implemented directly into these frameworks, like lorcon in Metasploit and the web attack modules in Impact

Lorcon is a driver. Web attack modules use fault-injection.

So then the tools can search for new vulnerabilities more than just act on the pre-loaded exploits.

I think we're going to have to redefine terminology if people really think this is true.

Re: Pentesting tool – Commercial

What does one do about the vulnerabilities that these tools don't find?

So I don't understand your limited view on these tools...
It's like asking "if this car is so damn good, why can't it drive me to work...!?".

Lulz!@#! I don't understand your limited view on the vulnerability problem. Your opinion on pen-testing tools is like responding with "It's a floor wax; it's a cereal; it cleans your pipes!".

But that might be the difference here...you wanna exploit your iPhone, while these tools are made to test the security level of company infrastructures...

No, I don't want to exploit anything. I don't want anybody exploiting anything. I want people to find vulnerabilities and fix them, usually without tools. I want developers to instinctively avoid writing vulnerabilities thanks to some simple processes and workflow. I want formal specification and verification.

I don't want people to use penetration-testing tools to test the security level of their company. I don't care how secure that they are in this way. I want them to acquire secure software and use it securely. I want developers to write code securely.

How secure is Core Impact? Is it unbreakable? Can I write a listener that gets scanned and launches a shell through the scanner? Can I take control of the pseudo-worm?

Cheers,
Andre

This list is sponsored by: Cenzic

Need to secure your web apps NOW?
Cenzic finds more, "real" vulnerabilities fast.
Click to try it, buy it or download a solution FREE today!

<http://www.cenzic.com/downloads>
