Netstat -vat by Sean Michael Kerner (bio)
A command line view of IT

« Fedora 15 will not be going to Vegas | Sean Michael Kerner Blog | Firefox hit with 0day Nobel Peace Prize vuln »

Fuzzing proprietary protocols not that hard #sectorca

By Sean Michael Kerner on October 26, 2010 1:48 PM

From the '*Fuzzing Fun*' files:

TORONTO. I'm a fan of fuzzing, which is basically a way to throw garbage input at an application to see if it will break.

At the SecTOR security conference currently underway in Toronto, Dr. Thomas Proll of Siemens explained how he goes about fuzzing proprietary protocols.

Proll explained that in his job as a penetration tester he has to fuzz proprietary protocol frequently and he usually doesn't have enough to reverse engineer protocols either. The types of tech that he is testing is often infrastructure like electricity, oil & gas and transportation system.

> **"Fuzzing is breaking the communication protocol," Proll said. "Unfortunately I can't show you how to break a power plant."**

There are a couple of approaches that Proll uses for fuzzing. The first approach is to do a port scan and find an open port. Once an open port is found he throws some very basic junk input as his initial fuzzing attempt.

> **cat /dev/urandom | nc 192.168.0.1 1234**

With the above simple command, Proll said that he has been able to break all kinds of systems. He added that it only works if the service being tested doesn't have any input validation.

The other method he takes is by capturing traffic over the wire using wireshark and then inserts random error with editcap (part of wireshark). Then he replays the packet with tcpreplay.

Wow - garbage in, garbage out.

Permalink | Comments (0) | TrackBacks (0) | Share

0 TrackBacks

Listed below are links to blogs that reference this entry: Fuzzing proprietary protocols not that hard #sectorca.

TrackBack URL for this entry: https://swarm.internet.com/mt-tb.cgi/16309

Leave a comment

Name

Email Address

- Email address required for verification only; it will not be displayed and will not be added to any marketing lists -

URL

Remember personal info?

Comments (You may use HTML tags for style)

Recent Entries

- Firefox hit with 0day Nobel Peace Prize vuln
- Fuzzing proprietary protocols not that hard #sectorca
- Fedora 15 will not be going to Vegas
- OpenLogic joins the Linux Foundation - Why now?
- Mozilla goes chromeless so you can build your own browser
- Pidgin 2.7.4 secures open source IM
- Interop saves IPv4 for another day
- Novell openSUSE Build Service 2.1 released
- IPv4 addresses fall below 5 percent. Is it time for IPv6 yet?
- Is Facebook Anti-Social if they're not OpenSocial?

Archives

Preview Submit