

Forum:[Hack Forums](#)

Thread: [REMnux - A Linux Distribution for Reverse Engineering Malware](#)

Yin - July 16, 2010, 9:32 pm

I guess this could go in here.

I stumbled upon this distro earlier today. No, I don't use Linux, but I found it and it seemed interesting. I researched it for a little bit, and here's what I found out -

REMnux is a Linux distro, as you already know, that assists malware analysts in reverse engineering "malicious" programs. It's based on Ubuntu. I found that it's designed for running services that are useful when performing malware analysis. In the process of that, the analyst USUALLY infects another computer, or system (VMware, etc). It directs potentially (so things that COULD be infected) malicious connections to the system that's listening on the right ports.

I also found that it's useful for web based malware, like Javascript, java programs, etc (like drivebys, and what not), and flash files. A good bonus is that it has tools for documents that have been infected recently (exploit for like exe to PDF, etc), so that it can analyze Word and PDF files. The malware can be loaded onto the REMnux and analyzed directly on that without other systems.

However, don't assume that REMnux has all the malware analysis tools you can dream of. Many of the tools it has are apparently designed to work on Windows. If you want to use the Windows analysis tools on a Linux platform, then you can always look at Wine (most of you know what that is I hope..?)

That's all I pretty much found out. I decided to sum it up in a few paragraphs, easier for me then just typing in a list what it has, and what it doesn't.

The download link if you're interested -

<http://sourceforge.net/projects/remnux/>

Enjoy. I'm kind of bored, so I decided to write something quick here and share something I thought was interesting.

v0lt4g3 - July 17, 2010, 12:14 pm

Cool man! I was just chatting about RE a few minutes ago, & now this!

Thanks!