Unix/Linux rootkits 101

By *srlinuxx*
Created *31/07/2007 - 5:18am*
Submitted by srlinuxx on Tuesday 31st of July 2007 05:18:35 AM Filed under Security [1]

The term rootkit originated with a reference to the root user account on Unix systems. Rootkits are not limited to Unix, however, or even to administrative user accounts like the Unix root account. No matter what operating system you use, you should be familiar with good practices for detecting and dealing with the threat of rootkits.

What is a rootkit?

As Mike Mullins explained in Windows rootkits 101, rootkits are not exploits. They are not the means of cracking security and accessing your system in the first place. Instead, rootkits are inserted into your system after it has already been compromised for the first time. Rootkits then cover the malicious security cracker?s tracks when he or she revisits the system later, or the tracks of other malicious software left behind. A rootkit may also include a ?back door? allowing the security cracker to gain access at any time in the future.

On Unix systems such as Solaris or FreeBSD, and on Unix-like systems such as Linux, a number of different means may be employed to cover the security cracker?s tracks. Common tactics include replacing system utility binaries such as ls and diff so that when they are used they will hide changes to the system and files on it from the user. The key point to keep in mind when dealing with the threat of rootkits is that once a rootkit has been installed on your system, you are no longer able to trust any of the tools installed on that system to give you accurate information.

This can make accurate detection of rootkits and other changes to a system by malicious security crackers a challenge.

Rootkit detection [2]

Also:

Like a lot of people, I use the free anti-virus program Clamav on my mail server. Last week, I was seriously impressed with its performance.

It started last wednesday, 25 July. At about noon, I received a mail by amavisd-new that it had blocked an e-mail containing a virus, Trojan.Downloader-11827. What was strange, is that I received this message on an e-mail account which is protected by my ISPs proprietary anti-virus solution. So it had not caught this virus, while Clamav did. Then I submitted the file to virustotal.com, and apparently only a few (about five) anti-virus programs detected the virus.

Amongst others, Kaspersky, F-Secure, NOD32, Bitdefender, Symantec and of course Clamav. In the clamav-virusdb mailing list archives, I found that Clamav had detection for this virus since 7h21 CEST, so it was really amongs the first to detect this virus.

Clamav is great [3]

Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] http://blogs.techrepublic.com.com/security/?p=264
[3] http://artipc10.vub.ac.be/serendipity/archives/34-Clamav-is-great.html