Security & Firewalls: Nach rootkits suchen

Nach einem erfolgreichen Einbruch oder auch nur bei einem verdacht auf einen Einbruch ins System sollte man auf jedenfall sich auf die Suche nach rootkits machen.
rootkit
Ein rootkit ist eine Sammlung von Programmen und Modulen, welche einem Eindringling auf einem Computersystem weiterhin einen versteckten Zugang sichern und/oder
Spuren verwischen. Je nach Qualität des rootkits, kann es sich sogar per Kernel-Patch selbst verstecken.

chkrootkit

Eins der passenden Tools ist chkrootkit. Es handelt sich um ein Shell-Script, welches die Eigenheiten bekannter rootkits kennt und danach sucht. Da es ein Shell-Script ist, kann man es auf einer Vielzahl von Linux/Unix-OSs ausführen. Es hat allerdings den Nachteil, dass es andere Systemprogramme verwendet, um seine Analysen durchzuführen. Auf einem geknackten Rechner könnten diese Programme ausgetauscht worden sein, so dass falsche Ergebnisse geliefert werden. Deshalb sind andere Tools wie z.B. Tripwire unabdinglich um sicher zustellen, welche Dateien wann geändert wurden.

rkhunter

rkhunter (Rootkit Hunter) ist ein weiteres Tool mit dem Vorteil, daß es der Update-Zyklus deutlich kürzer ist als bei chkrootkit. In der Fachwelt wird er sogar als der bessere Spürhund für Rootkits.

Eindeutige ID: #1039
huschi
2006-06-20 09:19