Vorstellung des Tools: Rootkithunter

von Karsten Kurtze

Kategorie: Sicherheit
Autor: Michael Boelen

Einsatzgebiet:

Rootkit Hunter scannt Linux- und BSD-Systeme auf Befall durch Rootkits und Backdoors, mit denen Angreifer die Kontrolle über infizierte Systeme übernehmen können. Existieren unter Linux derzeit auch keine ernst zu nehmenden Viren, so existiert sehr wohl die Bedrohung durch Rootkits und Backdoors. Diese kann man sich z.B. durch die Installation von Softwarepaketen aus fragwürdiger Quelle einfangen, die durchaus den Schädling enthalten können und durch die Installation mit Rootrechten in das System eingeschleppt werden. Von dem dann unbemerkten Austausch einwandfreier Systemdateien gegen infizierte bis hin zu manipulierten Kernelmodulen, die bereits beim Systemstart geladen und aktiviert werden: Solche Bedrohungen sind möglich, wenn auch nicht an der Tagesordnung. Eine Hysterie empfiehlt sich natürlich nicht, sehr wohl aber eine gesunde Vorsicht. Rootkit Hunter ist ein Hilfswerkzeug, das diese Mentalität unterstützt.

Um sich genauere Informationen über Rootkits zu verschaffen, empfiehlt sich die Lektüre der folgenden Texte:
http://de.wikipedia.org/wiki/Rootkit
http://www.heise.de/security/artikel/38057

Bezugsquelle: kostenlos von:
http://www.rootkit.nl/projects/rootkit_hunter.html

ROOTKIT HUNTER wird in regelmäßigen Abständen aktualisiert (Update), von daher ist es ratsam, die Seite in regelmäßigen Abständen aufzusuchen oder die Updateabfrage von ROOTKIT HUNTER zu verwenden (siehe "Bequeme Methode").

Informationen zum Projekt, über die verschiedenen Suchtechniken des Scanners sowie eine Übersicht über unterstützte OS unter:

http://www.rootkit.nl/projects/rootkit_hunter.html

Installationsanleitung

Von der o.g. Downloadseite (ganz unten) ist die aktuelle Version als tar-Archiv herunterzuladen, am besten in das eigene Homeverzeichnis.Nach dem Herunterladen öffnen wir am einfachsten den Konqueror, wechseln in unser Homeverzeichnis, und lassen das Archiv an Ort und Stelle via einfachem Rechtsklick mit der Maus und Auswahl der zutreffenden Option entpacken. Es taucht ein neues Verzeichnis mit dem Titel "rkhunter" auf. Wir klicken uns mit dem Konqueror in dieses Verzeichnis, und öffnen mit erneutem Rechtsklick und Auswahl von "Aktionen / Terminal öffnen" eine Konsole. Nun werden wir zunächst Root (Eingabe von "su" nebst Passworteingabe) und starten die Installation durch Eingabe des Befehls "./installer.sh".

Nach der Installation liegt die ausführbare Datei rkhunter im Verzeichnis / usr/local/bin.

Es gibt nun zwei Möglichkeiten, ROOTKIT HUNTER zu starten und auf die Suche zu schicken.

Konventionelle Methode
Konsole öffnen, Root werden (das ist zwingend erforderlich!)

a) Um ROOTKIT HUNTER das gesamte System prüfen zu lassen, folgendes eingeben:

/usr/local/bin/rkhunter --checkall

b) Um zu erreichen, daß ROOTKIT HUNTER zusätzlich ein Aktions- und Ergebnisprotokoll erstellt, folgendes eingeben

/usr/local/bin/rkhunter --createlogfile --checkall

c) Um zu überprüfen, ob eine neue Version von ROOTKIT HUNTER vorliegt, folgendes eingeben:

/usr/local/bin/rkhunter --versioncheck

Bequeme Methode
Man kann sich die Sache vereinfachen und nur einmal tippen, wenn man für den Scan mit Logfile sowie die Updateüberprüfung jeweils ein Icon auf den Desktop legt.

Desktop-Icon für Scan mit Logfile:
Rechtsklick auf freie Desktopstelle, Auswahl von "Neu erstellen / Datei", Verknüpfung zu Programm", im aufklappenden Fenster folgende Einstellungen vornehmen: Im Reiter "Allgemein" Programmname (z.B. RKH) sowie passendes Icon wählen, im

Reiter "Programme" in der Zeile Befehl eingeben: /usr/local/bin/rkhunter --createlogfile --checkall
Anschließend im gleichen Reiter unten "Erweiterte Optionen" wählen und hier die folgenden Optionen aktivieren: "in Terminal starten", "Terminal nach Programmende geöffnet lassen", "als anderer Benutzer ausführen" (und dort diesen Benutzer mit "root") benennen. Zweimal mit OK bestätigen, fertig.

Desktop-Icon für Updateabfrage:
Gleicher Vorgang wie für Scan mit Logfile, im Reiter Programme in der Zeile Befehl jedoch eingeben:
/usr/local/bin/rkhunter --versioncheck

Klick auf das erste Icon öffnet ein Terminal und fragt nach dem Root-Passwort. Nach korrekter Eingabe startet der Scan. Die Scanergebnisse werden im Terminal angezeigt. Nach Abschluß des Scans muß das Terminal per Mausklick geschlossen werden.

Klick auf das zweite Icon öffnet ein Terminal und fragt nach dem Root-Passwort.
Nach korrekter Eingabe nimmt ROOTKIT HUNTER Kontakt mit der Homepage auf und prüft, ob ein Update vorhanden ist. Das Ergebnis der Prüfung wird im Terminal angezeigt. Danach muß man das Terminal per Mausklick schließen.

ROOTKIT HUNTER aktualisieren

Liegt eine neue Version vor, ist das Update sehr einfach. Man muß lediglich das Archiv mit der neuen Version von der o.g. Seite herunterladen, dies am besten wieder in das eigene Homeverzeichnis. Danach löscht man im Konqueror zunächst das alte Verzeichnis namens rkhunter, anschließend entpackt man das neue Archiv, das wiederum ein eigenes Verzeichnis mit Namen "rkhunter" hinterläßt. Man wechselt erneut in dieses Verzeichnis und installiert wie bereits oben genannt die neue Version. Die ausführbare Datei befindet sich wieder in / usr/local/bin und heißt "rkhunter".

Hat man sich Desktop-Icons angelegt, ändert sich nichts. Nach Einspielen der neuen Version startet mit Klick auf die Desktop-Icons auch das aktualisierte Programm mit dem Scan. Zu überprüfen ist dies mit Klick auf das Icon, das die Updateabfrage startet, es wird hier angezeigt werden, daß die aktuell installierte und im Einsatz befindliche Version identisch mit der Version ist, die auf dem Homeserver von RKH als die aktuelle ausgewiesen ist.

Hinweis: Wie auch bei einem herkömmlichen Virenscanner unter Windows gilt auch bei ROOTKIT HUNTER, daß nicht jeder Alarm auf einem echten Infekt basieren muß. Zu empfehlen ist auch die Übersicht über die unterstützten OS (siehe oben): Nur bei unterstützten Distributionen ist der Einsatz wirklich anzuraten.