

## Sisteminiz Elemei Geçirildi

Son Güncelleme Pazartesi, 17 Kasım 2008

Sisteminizin ele geçirildiğinden püphemleniyorsanız sisteminizde var olabilecek rootkit lere karşı sisteminizi taramalısınız, böylece saldırganın sisteminize neler kurduğunu bulabilirsiniz. Rootkit ler; ele geçirilen sistemlere kurulan ve saldırganın yaptığı işleri gizlemek için var olan programlardır. Saldırgan bu programla sisteminize başka bir zamanda tekrar girebilir. Bundan dolayı rootkitler sistemde çalışmaya devam eden programlar bırakırlar. Böylece sistem admininin haberi olmadan tekrar sisteme girilebilir. Bu işi yapabilecek bir çok rootkit programları vardır ve bundan dolayı bunların el ile tespit etmek oldukça zordur. Bunun için bu test işlemlerini otomatik olarak yapan birçok chkrootkit programları vardır. Chkrootkit i aşağıdaki link den indirebilirsiniz. Fedora nın rpm paketidir. Diğer linux uygulamaları içinde mevcuttur.

<http://rpmforge.net/user/packages/chkrootkit/>

Sisteminize kurduktan sonra yapmanız gereken sadece new terminal e (uçbirime) chkrootkit yazmak hepsi o kadar tarama işlemi baplıcağıdır ve aşağıdaki gibi çıktıyı alırsınız.

```
[root@localhost ~]# chkrootkit
ROOTDIR is '/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not infected
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not found
Checking `inetdconf'... not found
Checking `identd'... not found
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldsopreload'... not infected
Checking `login'... not infected
Checking `ls'... not infected
Checking `lsof'... not infected
Checking `mail'... not infected
Checking `mingetty'... not infected
Checking `netstat'... not infected
Checking `named'... not found
Checking `passwd'... not infected
Checking `pidof'... not infected
Checking `pop2'... not found
Checking `pop3'... not found
Checking `ps'... not infected
Checking `pstree'... not infected
Checking `rpcinfo'... not infected
Checking `rlogind'... not found
Checking `rshd'... not found
Checking `slogin'... not infected
Checking `sendmail'... not infected
Checking `ssh'... not infected
Checking `syslogd'... not tested
Checking `tar'... not infected
Checking `tcpd'... not infected
Checking `tcpdump'... not infected
```

```
Checking `top'... not infected
Checking `telnetd'... not found
Checking `timed'... not found
Checking `traceroute'... not infected
Checking `vdir'... not infected
Checking `w'... not infected
Checking `write'... not infected
Checking `aliens'... no suspect files
```

Bu arada sisteminize chkrootkit i kurun ve devamlý aralýklarla çalyptýrýn faydasýný görürsünüz