

SeekerKit

A Multi-purpose toolkit

By Guy Bruneau, GSEC, GCIA, GCUX

Version 0.5 beta – 19 April 2002

SeekerKit is written to be self-contained. It boots to a fully functional command line workstation all running in RAM disk. All packages contained on this CD have been compiled statically to ensure they run without the need of dynamic libraries.

This program can be downloaded at:

<http://www.whitehats.ca/downloads/forensics/SeekerKit.iso>

Mounting drives

If the primary master is running Windows NT/2000, the drive can be mounted read-only this way on the /ntfs partition:

```
mount /ntfs
```

If the primary master is running Windows 95/98/ME, the drive can be mounted read-only this way on the /dos partition:

```
mount /dos
```

The CD-ROM drive will be mounted automatically if located on the primary slave, secondary master/slave on the /cdrom.

The floppy drive can be mounted in VFAT format by issuing the following command:

```
mount /floppy
```

Kernel modules

If you require to mount a device module that is not running, find the module in /root/rc.modules and issue the command likewise:

```
modprobe eepr100
```

Networking

If you would like to connect to the network to use some of the tools on this CD, you can modify the /root/rc.network file after the system is booted or copy the following to a diskette and run it as a script:

```
#!/bin/sh
#
# Put any local setup commands in here:
echo "Starting local network..."
/sbin/ifconfig eth0 192.168.30.10
/sbin/ifconfig eth0 netmask 255.255.255.0
/sbin/route add default gw 192.168.30.1 netmask 0.0.0.0 metric 1
```

Known issues:

This version hasn't been fully tested on laptops.

SeekerKit is comprised of the following binaries:

Utilities

Snort
Tepdump
Tethereal
Nemesis
Dsniff
Tcpreplay
Xprobe
Hping2
Netcat
Nmap

Communication Utilities

Ssh
Scp
Sftp

Forensic

Lsof
Script