NAME

blackhole - a sysctl(8) MIB for manipulating behaviour in respect of refused SCTP, TCP, or UDP connection attempts

SYNOPSIS

sysctl net.inet.sctp.blackhole[={0 | 1 | 2}]
sysctl net.inet.tcp.blackhole[={0 | 1 | 2}]
sysctl net.inet.tcp.blackhole_local[={0 | 1}]
sysctl net.inet.udp.blackhole[={0 | 1}]
sysctl net.inet.udp.blackhole_local[={0 | 1}]

DESCRIPTION

The **blackhole** sysctl(8) MIB is used to control system behaviour when connection requests are received on SCTP, TCP, or UDP ports where there is no socket listening.

The blackhole behaviour is useful to slow down an attacker who is port-scanning a system in an attempt to detect vulnerable services. It might also slow down an attempted denial of service attack.

The blackhole behaviour is disabled by default. If enabled, the locally originated packets would still be responded to, unless also *net.inet.tcp.blackhole_local* (for TCP) and/or *net.inet.udp.blackhole_local* (for UDP) are enforced.

SCTP

Setting the SCTP blackhole MIB to a numeric value of one will prevent sending an ABORT packet in response to an incoming INIT. A MIB value of two will do the same, but will also prevent sending an ABORT packet when unexpected packets are received.

TCP

Normal behaviour, when a TCP SYN segment is received on a port where there is no socket accepting connections, is for the system to return a RST segment, and drop the connection. The connecting system will see this as a "Connection refused". By setting the TCP blackhole MIB to a numeric value of one, the incoming SYN segment is merely dropped, and no RST is sent, making the system appear as a blackhole. By setting the MIB value to two, any segment arriving on a closed port is dropped without returning a RST. This provides some degree of protection against stealth port scans.

UDP

Enabling blackhole behaviour turns off the sending of an ICMP port unreachable message in response to a UDP datagram which arrives on a port where there is no socket listening. It must be noted that this behaviour will prevent remote systems from running traceroute(8) to a system.

WARNING

The SCTP, TCP, and UDP blackhole features should not be regarded as a replacement for firewall solutions. Better security would consist of the **blackhole** sysctl(8) MIB used in conjunction with one of the available firewall packages.

This mechanism is not a substitute for securing a system. It should be used together with other security mechanisms.

SEE ALSO

ip(4), sctp(4), tcp(4), udp(4), ipf(8), ipfw(8), pfctl(8), sysctl(8)

HISTORY

The TCP and UDP **blackhole** MIBs first appeared in FreeBSD 4.0.

The SCTP **blackhole** MIB first appeared in FreeBSD 9.1.

AUTHORS

Geoffrey M. Rehmet