NAME

mac_ddb - Restricted kernel debugger interface policy

SYNOPSIS

To compile the ddb policy into your kernel, place the following lines in your kernel configuration file:

```
options MAC
options MAC_DDB
```

Alternately, to load the ddb module at boot time, place the following line in your kernel configuration file:

```
options MAC
```

and in loader.conf(5):

```
mac_ddb_load="YES"
```

DESCRIPTION

The **mac_ddb** policy module implements a MAC policy which restricts the set of commands that can be used at the ddb(4) command prompt. The subset of permitted commands is limited to those which do not read or write to arbitrary memory locations. This is done to deter the possible extraction of system secrets while still allowing enough debugger functionality to diagnose a kernel panic. For example, the **trace** or **show registers** commands are allowed by this policy, but **show buffer** *addr* is not.

All debugger commands that are declared with the *DB_CMD_MEMSAFE* flag are allowed by **mac_ddb**. The policy provides validation functions to conditionally allow some additional commands, based on the user provided arguments.

When loaded, the **mac_ddb** policy also ensures that only the ddb(4) debugger backend may be executed; gdb(4) may not.

Label Format

No labels are defined for **mac_ddb**.

SEE ALSO

ddb(4), mac(4), mac_biba(4), mac_bsdextended(4), mac_ifoff(4), mac_lomac(4), mac_mls(4), mac_none(4), mac_partition(4), mac_portacl(4), mac_seeotheruids(4), mac_test(4), mac(9)

BUGS

While the MAC Framework design is intended to support the containment of the root user, not all attack channels are currently protected by entry point checks. As such, MAC Framework policies should not be relied on, in isolation, to protect against a malicious privileged user.