Logging in LXC

Logging

One problem I ran into is that access to kernel logging is limited or unavailable from inside of a LXC container. For some usecases (like *netfilter*'s `LOG` action) any logging that happens in a LXC container will be blackholed and not recorded anywhere without a change on the host. Most often the solution to these permission/security problems is to find a way to allow access to these things from userspace.

ulogd2

I solved the *netfilter* `LOG` problem by simply using *ulogd2* to replace kernel logging with userspace logging. After installing and configuring *ulogd2* I just replaced any references to `LOG` with `NFLOG` in my *netfilter/iptables* rules. Don't worry if this doesn't make sense right now I'll talk about this more in the Firewall Setup section.

> ulogd is a userspace logging daemon for netfilter/iptables related logging. This includes per-packet logging of security violations, per-packet logging for accounting, per-flow logging and flexible user-defined accounting.

Installation

```
apt install ulogd2
```

Configuration

To get the output I wanted I had to edit the *ulogd2* config...

```
# /etc/ulogd2.conf
- stack=log1:NFLOG,base1:BASE,ifi1:IFINDEX,ip2str1:IP2STR,print1:PRINTPKT,emu1:LOGEMU
+ #stack=log1:NFLOG,base1:BASE,ifi1:IFINDEX,ip2str1:IP2STR,print1:PRINTPKT,emu1:LOGEMU
...
```

```
+ stack=log1:NFLOG,base1:BASE,ifi1:IFINDEX,ip2str1:IP2STR,print1:PRINTPKT,firewall:LOGEMU
+ stack=log2:NFLOG,base1:BASE,ifi1:IFINDEX,ip2str1:IP2STR,print1:PRINTPKT,firewall:LOGEMU
+ stack=log3:NFLOG,base1:BASE,ifi1:IFINDEX,ip2str1:IP2STR,print1:PRINTPKT,firewall:LOGEMU
+
+ [firewall]
+ file="/var/log/ulog/firewall.log"
+ sync=1
```

Connection Tracking

Similarly to *netfilter* logging connection tracking in a LXC container is more limited due to not having access to the host's `/proc/` filesystem. But I can install *conntrack* to provide a way to see connection tracking from userspace.

conntrack

> The conntrack utilty provides a full featured userspace interface to the Netfilter connection tracking system that is intended to replace the old /proc/net/ip_conntrack interface. This tool can be used to search, list, inspect and maintain the connection tracking subsystem of the Linux kernel.

Installation

```
apt install conntrack
```

Revision #4
Created 24 March 2021 12:15:51 by dustin@swigg.net
Updated 8 April 2021 12:40:06 by dustin@swigg.net