Security: How to keep my port scanning tool from crashing my head node?

If you find that using a port scanning tool like Nessus or nmap causes your head node to crash or temporarily become unresponsive, then make the following changes on your head node.

First, in /etc/shorewall/policy, replace every mention of REJECT with DROP on your head node. For example, change this:

```
# THE FOLLOWING POLICY MUST BE LAST
all all REJECT info
```

to this:

```
# THE FOLLOWING POLICY MUST BE LAST
all all DROP info
```

And restart shorewall:

```
# systemctl restart shorewall
```

Now shorewall will not be burdened with having to send back rejection responses to every host that tries to connect to an unopened port.

Next, add the following line to /etc/sysctl.conf:

```
kernel.printk = 4 4 1 7
```

And to apply that setting now:

```
# sysctl -p /etc/sysctl.conf
```

That will inform your logging daemon (i.e. syslogd, rsyslogd, etc.) to only send shorewall messages regarding error conditions, critical conditions, alerts requiring immediate responses, and system-wide emergencies to your head node's console; thus, the system will not hang up due to the flood of informational messages coming from shorewall during a port scan.

Unique solution ID: #1401
Author: Sean Eubanks
Last update: 2018-01-09 18:58