# Restrict Kernel Modules

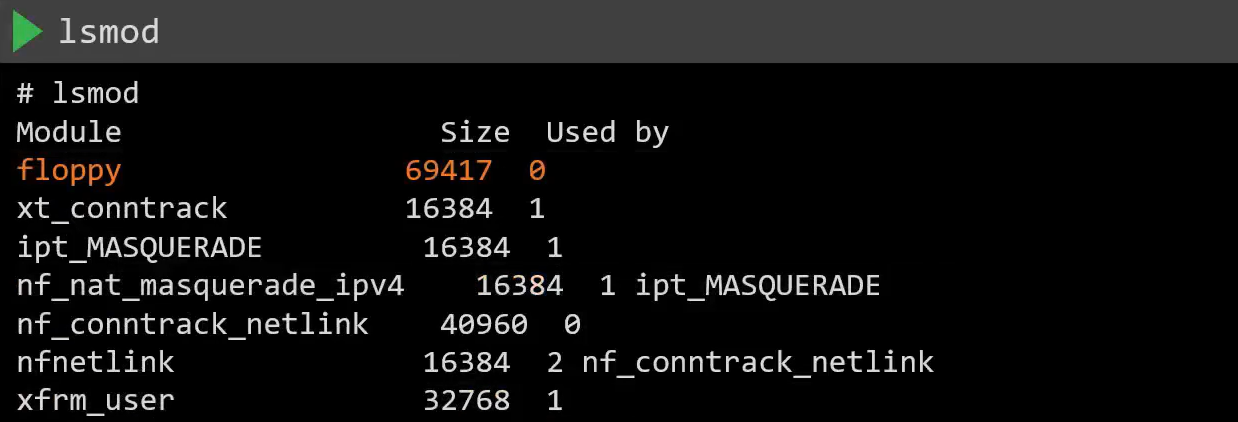
1. Loading PC Speaker module

modprobe pcspkr



1. List all the modules loaded into the kernel

lsmod



When we have k8s workloads running on the source, even an unprivileged process running on a pod can cause certain network protocol related modules to be loaded into the kernel by creating a network socket.

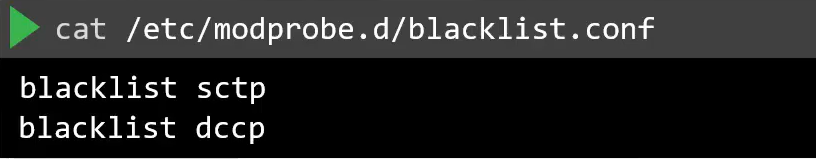
This can allow an attacker to exploit a potential vulnerability.

Solve:

Blacklist the modules on all the nodes of the cluster

Add to blacklist:

cat /etc/modprobe.d/blacklist.conf



reboot

## Disable Open Ports

<https://kubernetes.io/docs/reference/ports-and-protocols/>

Check installed packages:

apt list –installed

Check active service on the system

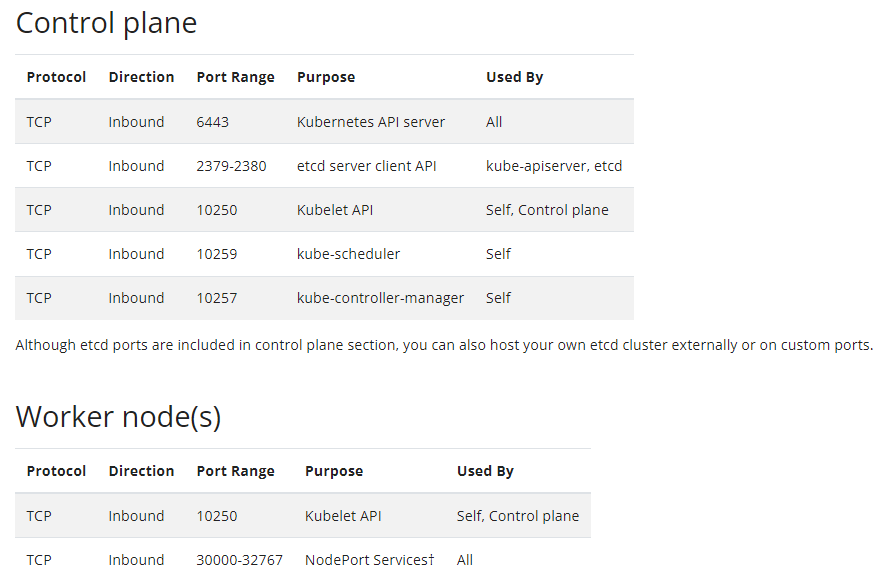
systemctl list-units –type service

Remove service

rm -f /var/lib/systemd/xxxxx.service

Remove Package

apt remove nginx -y



UFW disable useless ports

ufw default allow outgoing

ufw default deny incoming

ufw allow from xxx.xxx.xxx.xxx/xx to any(ip) port 22 proto tcp

ufw enable

ufw status

