Jonathan Lee

CSC Sacramento State

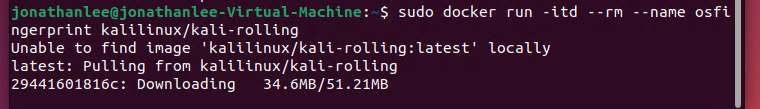
Summer Researching

6-2-2023

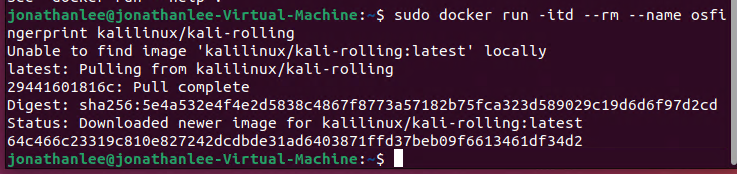
**Fingerprinting Docker’s Kali Container with p0f**

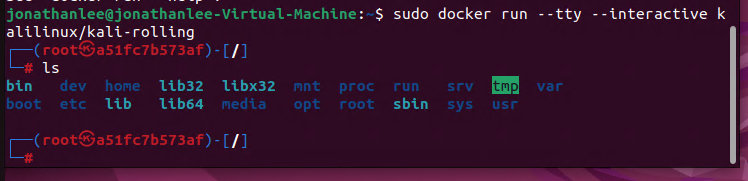
1. Install docker

sudo apt install docker.io -y

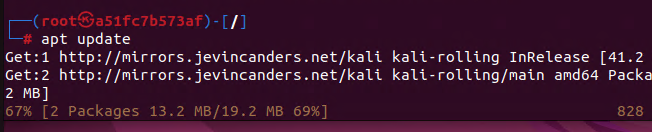


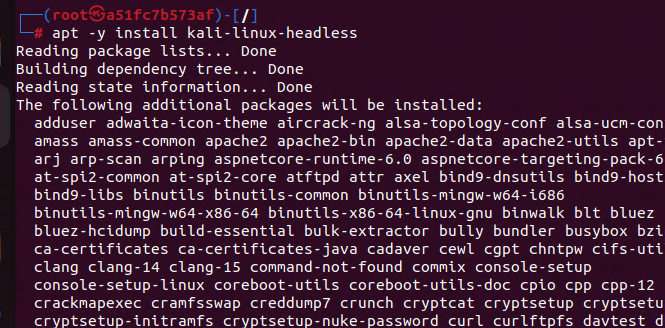
1. install Kali Docker container



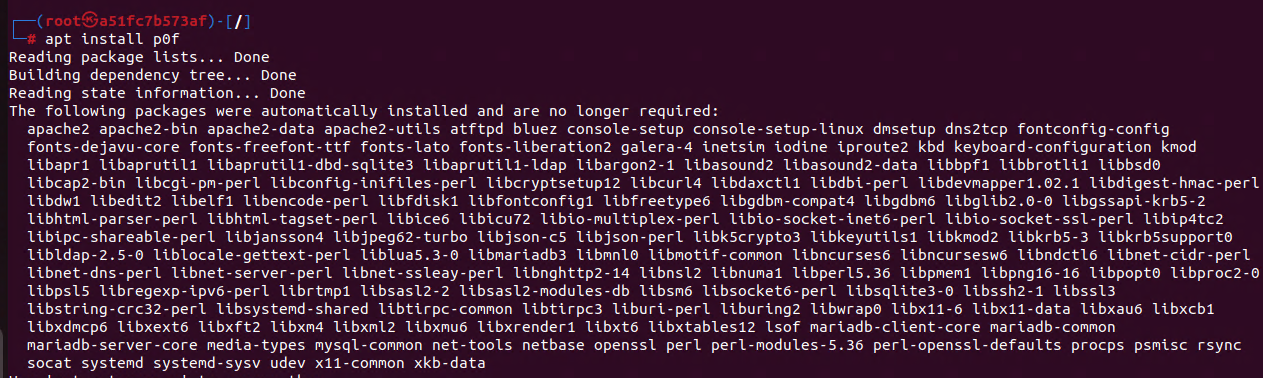


1. run a container or just run interactive

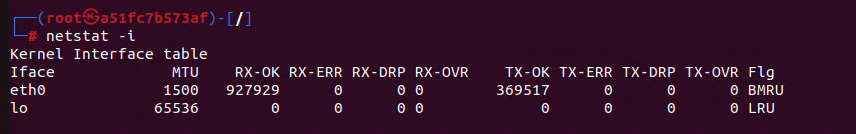




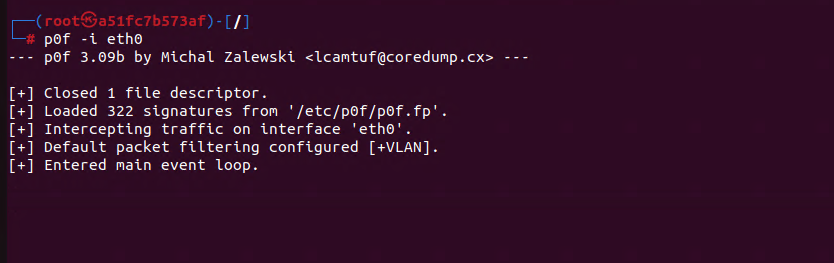
1. apt update
2. apt -y install kali-linux-headless



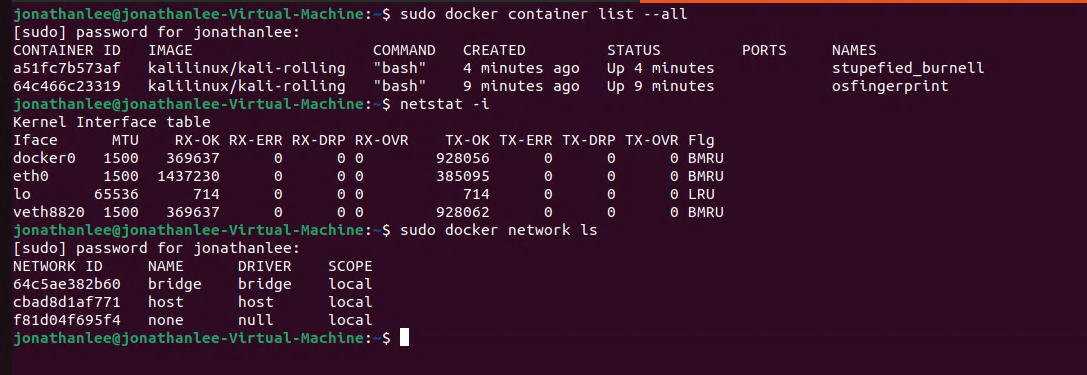
1. apt install p0f



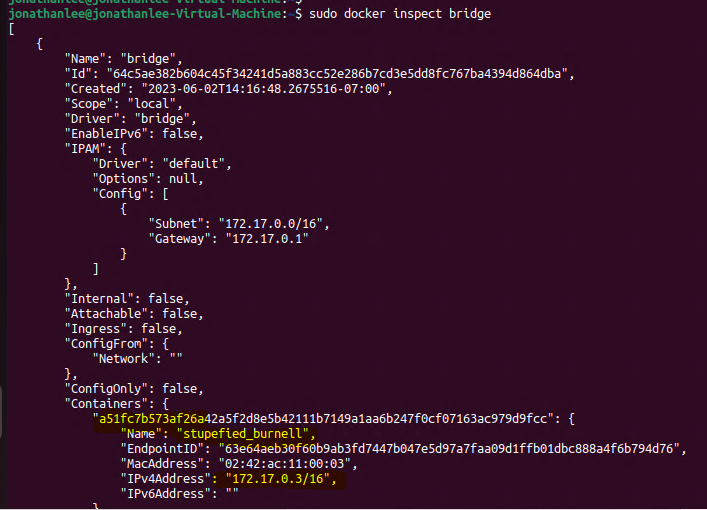
1. get the network interface name



1. now run p0f -I eth0



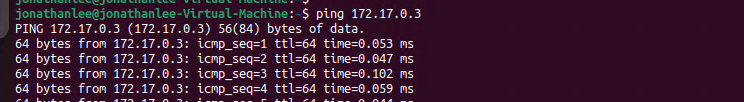
1. Open a new window in Ubuntu check check what container you are running kali in for this version I am using a51fc7b57af as seen in the root@ section



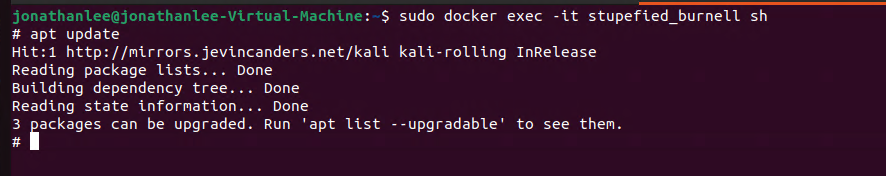
1. Sudo docker inspect bridge shows ip of kali



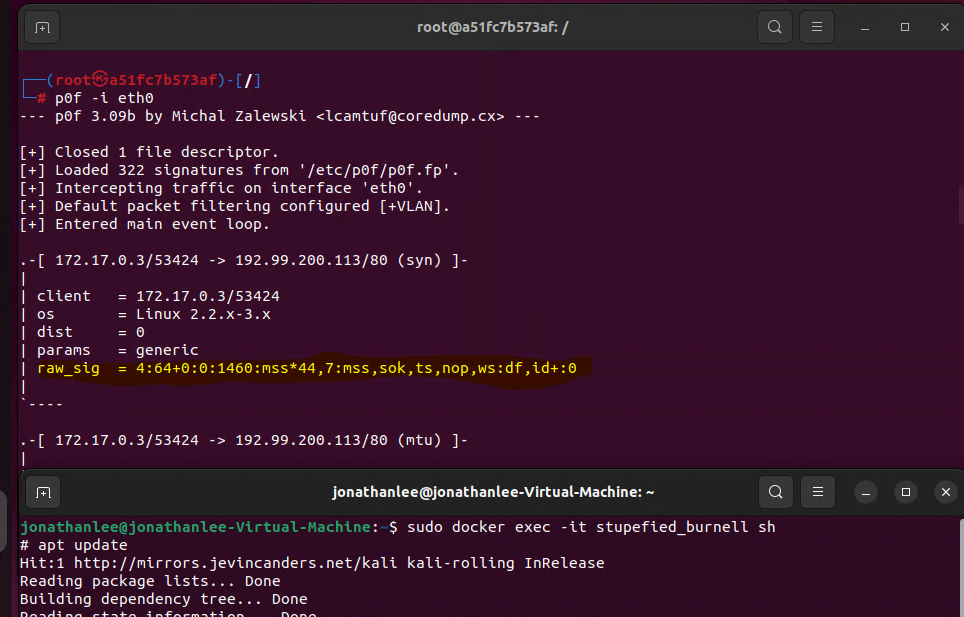
1. Sudo docker ps



1. These match so start pings to get traffic going on this address if it pings move to next step cancel ping

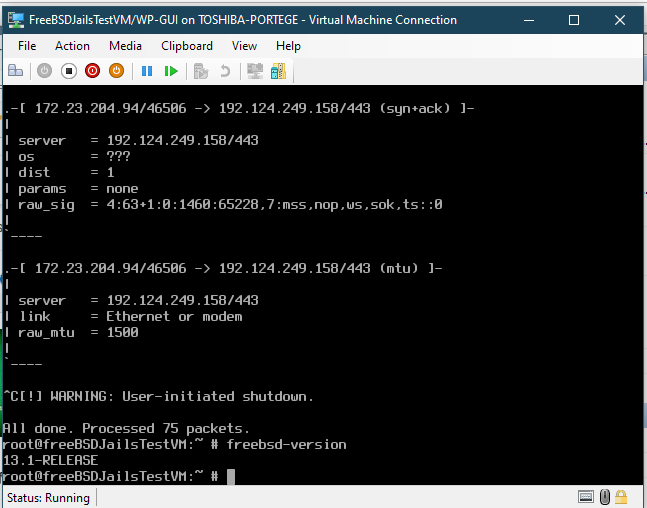


1. Login to the container in the other window while still running p0f in the other

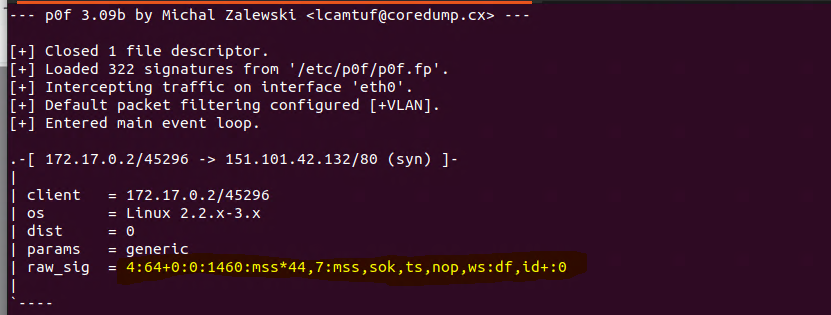


Docker’s Kali Container is 4:64+0:0:1460:mss\*44,7:mss,sok,ts,nop,ws:df,id+:0

This signature is the OS fingerprint



Here is it again in FreeBSD



Here it is again for a Debian docker container.

Works Cited:

“Using Kali Linux Docker Images: Kali Linux Documentation.” *Kali Linux*, 6 Mar. 2023, www.kali.org/docs/containers/using-kali-docker-images/.

“P0F: Kali Linux Tools.” *Kali Linux*, 5 Aug. 2022, www.kali.org/tools/p0f/.

“You Need to Learn Docker Right Now!! // Docker Containers 101.” *YouTube*, 2 Apr. 2020, www.youtube.com/watch?v=eGz9DS-aIeY.