Firewall Lab

Joshua Main-Smith

2020-10-26

Contents

NFTable Implementation

Introduction

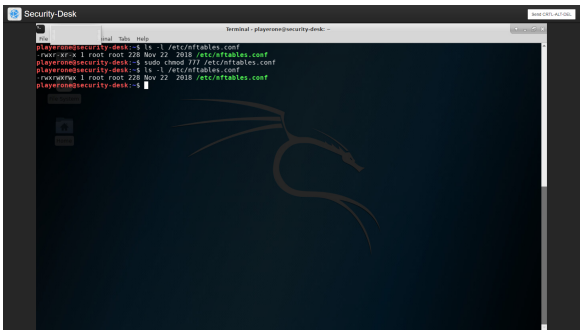
We have been tasked with replacing the outdated iptable implementation with nftables. From the manual page, iptables are used in the configuration of IPv4 and IPv6 packet filtering rules for the Linux kernel. Each table contains a list of chains, which are sets of rules used in filtering packets. The three chains are input (for inbound packets), output (for outbound packets), and forward (for connections that aren't delivered locally). Nftables are created by the same company as those who maintain iptables, but nftables were made in response to some of the insufficiencies of iptables, such as scalability and performance.

Switching from IPTables to NFTables

To get started, we first need to reinstall iptables in order to use the commands from iptables-translate. To do this, we simply issue the Linux command **sudo apt-get install iptables**. We then proceeded to install nftables with **sudo apt-get install nftables**.

We were then able to proceed with setting up an nft ruleset file. A copy of our iptable rules were located on our desktop. Relocating there, we could add our old rules to our nft file by executing **sudo iptables-restore-translate -f SecurityDesk_iptables_v4 >ruleset.nft**, where SecurityDesk_iptables_v4 is the name of file containing the iptable rules. This file is then turned into a script with **sudo nft -f ruleset.nft**.

We then needed to add these rules to the configuration file. As can be seen in the image below, we needed to change the file permission to allow us to write and execute. This is accomplished with **sudo chmod 777 /etc/nftables.conf**.



We were then able to write the script to the configuration file with **sudo nft list ruleset >/etc/nftables.conf**. And finally, to start and enable nftables we run the commands **sudo systemctl start nftables** and **sudo systemctl enable nftables**. The command systemctl is used to control system components of the

operating system and the service manager. We can then remove iptables from the system, since it is no longer needed. This is done with **sudo apt remove iptables**. We follow a similar approach on the Prod-Joomla system, with the only difference being the file name under **/home/playerone/**.

Rule Chain Discussion

Screenshots of the rules can be seen in the images below. With both the systems, the output and forward chain packets are all accepted. The input chain for the security desktop denies packets, except for ct state up to 521 bytes and tcp SSH connections up to 10 bytes. The input chain for the Joomla system is the same as the Security desktop input chain with the addition of tcp http connections of up to 2 bytes.

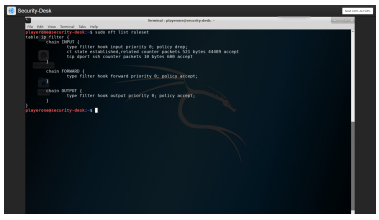


Figure 1: Security Desk Rules

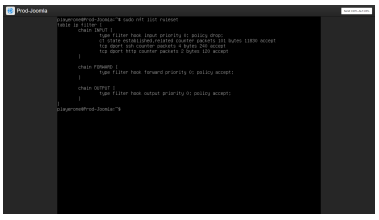


Figure 2: Joomla Desk Rules