Assignment 1

Networks and Systems Security (CSE554)

Winter 2022

Deadline: Feb 21, 2022 (2359hrs)

Linux Kernel Netfilter Framework Module (total points: 35)

You have read about the Linux/Netfilter framework. This assignment requires you to write a loadable kernel module that can detect specific packets and drop them. More specifically, you know by now that the netfilter framework provides hook functions (kernel call back functions) that user modules could access and obtain the detail of packets.

You need to write a kernel firewall module that you may test using two VMs

[VM1](interface 1) ←→ (interface 1) [VM2](interface 2)

On VM1 you should use the network reconnaissance tool nmap that sends crafted reconnaissance packets to the VM2 (e.g. TCP half-open scan packets, TCP connect packets, UDP packets etc.).

You would require reading the manpage of the nmap tool to identify atleast three different reconnaissance methods and the packets they send. E.g. the TCP half open scan sends only a single TCP SYN packet, expecting a SYN/ACK, RST or at worst no response.

On VM2 you require to load the kernel module that should use the Netfilter hook functions to obtain packets and identify the three reconnaissance scans. Once identified you need to log these into `syslog`

The following link may be a good starting point:

https://medium.com/bugbountywriteup/linux-kernel-communication-part-1-netfilter-hooks-15c07a5a5c4e

What to submit:

1. Write up describing your module, how it works, how it identifies packets, and how it blocks them. Also, which specific recon packets it identifies.
2. A Makefile to compile the module.
3. Sample script to test the module. This script may contain commands that are to

Grading rubric:

1. Module that compiles and correctly identifies the recon packets (20 points).
2. Test scripts (10 points).
3. Write-up (5 points).