Network Security – CSE 550

Assignment 1

Total points: 35

Due: September 18, 2016 23:59 hours.

Description:

This assignment would require you to write a kernel module that would involve using the netfilter framework (like what was described in the class). You would require to write a netfilter kernel module to intercept packets and log them in the kernel logs. You should be able to detect any four different kinds of TCP based reconnaissance packets that can be generated using ‘nmap’. The module should detect these packets them to kernel logs. You do not have to filter the packets, merely identify them and log them.

Some useful resources:


https://www.digitalocean.com/community/tutorials/a-deep-dive-into-iptables-and-netfilter-architecture


What you are supposed to submit:

1. C source code for the aforementioned shell server and client programs.
2. Makefile through which one could compile these programs.
3. A write up of what your system does, what all assumptions you made, the inputs that you used to test your program and all the errors that you handled.

How you would be graded:

1. Successful compilation using Makefile – 10 points.
2. Demonstration of detection of the TCP reconnaissance packets – 20 points.
3. Description of how you are detecting the packets etc. – 5 points.