KERNEL MODULE USING NETFILTER FRAMEWORK

What the system does?

The kernel module can detect the TCP based reconnaissance packets that can be generated using ‘nmap’ and logs them to the kernel log.

It can detect the following TCP based reconnaissance packets:

1. SYN packet
2. FIN packet
3. NULL packet
4. XMAS packet
5. ACK packet

How i am detecting the packets?

I am detecting the above mentioned packets by looking for the flags that are set in the TCP header.

1. SYN packet: only **SYN** flag is set in a SYN packet

2. FIN packet: only **FIN** flag is set in a FIN packet

3. NULL packet: no flag is set in a NULL packet

4. XMAS packet: **FIN**, **PSH** and **URG** flags are set in an XMAS packet

5. ACK packet: only **ACK** flag is set in an ACK packet

Inputs i used to test my program

Following are the inputs that i used to test my program to detect the above mentioned reconnaissance packets :

1. SYN packet: sudo nmap -A -T4 -sS 127.0.0.1

2. FIN packet: sudo nmap -A -T4 -sF 127.0.0.1

3. NULL packet: sudo nmap -A -T4 -sN 127.0.0.1

4. XMAS packet: sudo nmap -A -T4 -sX 127.0.0.1

5. ACK packet: sudo nmap -A -T4 -sA 127.0.0.1