NET FILTER KERNEL MODULE

Description

This kernel module captures the packet and identifies the type of TCP reconnaissance performed. Following type of TCP reconnaissance are detected

1. Xmas Scan
2. Null Scan
3. Syn Scan
4. Ack Scan
5. Fin Scan

Get Started

Compilation

```
make
```

Installation

To install the netfilter kernel module, type the following on shell

```
sudo make install
```

Remove

To uninstall the netfilter kernel module, type the following on shell

```
sudo make remove
```

Kernel Log

To see the live kernel log, type following on shell

```
sudo cat /proc/kmsg
```

Examples NMAP

Examples to perform various nmap reconnaissance

```
sudo nmap -sX 20.0.0.5
sudo nmap -sS 20.0.0.5
sudo nmap -sN 20.0.0.5
```

Implementation

Init

A hook function is registered at the *prerouting* hook. This function would be then called each time a packet is captured at the prerouting hook. The priority for this function as marked first so that it is the first function called at the prerouting hook.

Hook Function

This function checks if the packet is a TCP packet. If it is a TCP packet then the *flags* from tcp header are checked. Various combination of flags are checked to detect the type of reconnaissance.

- NULL: All flag bits are 0
- XMAS: Urg, Fin, Psh flag bits are set
- SYN: only Syn bit is set
- ACK: only Ack bit is set
- Fin: only Fin bit is set

Exit

If the module is to be uninstalled, the previosuly (in init) registered hook function is unregistered.

Author: Sushant Kumar Singh