DoS Tool

Packet flooding program

Ivo Lemmen Leeuwenborgh AO 7/5/2017

Table of Contents

DoS Tool

Packet flooding program

Use Case

The form of packet flooding used in this program will enable the attacker to send different types of packets of their choice in combination with each other or not, at intervals of 1 millisecond (1000 times per second) to a specified location by IP and MAC, with the aim to at best cause the targeted internet adapter to crash or to slow it down. Additionally you can track incoming packets between your specified IP range in the built in monitor and use that information to determine if you're being attacked and / or use it to determine a target.

Functionality

First Form

This is the main form, where all the controls are. Here you can specify your attack parameters and launch an attack.

Menu bar

- The first option in the menu bar allows you to open a duplicate tab on a different thread, to strengthen the attack.
- The second option allows you to open a second form, where you can monitor incoming packet traffic.
- The third option launches the default web browser and loads the page to download WinPcap from.

Buttons

- The start button activates a timer, indicating how long the attack is running and opens a packet connection on the background process to enable sending packets.
- The stop button terminates the background process and resets the timer.
- The new button allows you to open a duplicate tab, to strengthen the attack by combining the processing power.

Textboxes

- In the IP textbox you specify the target destination's IP address.
- In the MAC textbox you specify the target destination's MAC address.
- In the Port textbox you specify the target destination's open port (only for UDP).
- In the Buffer size textbox you specify the size of the payload in bytes.

Select box

All the active internet adapters will appear as a list in the select box, you specify the one you're currently using for connecting to the internet. You will attack and listen from this adapter.

Checkboxes

The checkboxes allow toggling between the different types of attacks and also allow combining them in real time.

Second Form

This form once the background process is activated will show important information regarding incoming packets and print those in the grey window.

Buttons

- The start button begins the background process of listening to incoming packets. The important data from the packets will be printed in the grey window.
- The stop button terminates the background process.

Textbox

The source IP range textbox allows setting a range between the source IP you want to listen to, for example: if the incoming packet's source IP is 192.168.10.5 and you want to track only traffic that has a source IP between 192.168.10.0 and 192.168.10.5 and between 192.168.10.5 and 192.168.10.10, then the input string would be "192.168.10.0-192.168.10.10" without the quotation marks.

Types of attacks

ICMP flood

Rapidly send Internet Control Message Protocol ping packets over IPv4 over Ethernet with a maximum payload of 1512 bytes, without waiting for reply. Packet source IP will be set to the destination IP, causing an infinite loop that will result in a crash of the internet adapter. Over ethernet this type is best.

ARP flood

Rapidly send Address Resolution Protocol request packets over IPv4 over Ethernet with a maximum payload of 1512 bytes. Packet source IP won't be set, concealing the origin. This form will slow down the targeted internet adapter, because the machine won't know where to reply to.

UDP flood

Rapidly send User Datagram Protocol packets over IPv4 over Ethernet with a maximum payload of 1512 bytes. This packet requires a destination port to be set. This type will stress the targeted internet adapter by causing it to reply with an ICMP Destination Unreachable packet.