Documentation: FloodFury Tool

Description

This tool, named floodFury.py performs a DHCP starvation attack, consuming all available IP addresses in the DHCP pool by sending DHCP discover and request packets from spoofed MAC addresses. Additionally, it can spoof DNS requests to redirect traffic to a specified IP address, effectively performing a DNS spoofing attack. The tool is useful for penetration testing and security research purposes.

Requirements

- Kali linux (or other linux flavors)
- Python 3.x
- Scapy library

Installation Dependencies

1. **Python 3.x**: Ensure Python 3.x is installed on your system. You can download it from the official Python website.
2. **Scapy**: Install Scapy using pip:

```
> pip install scapy
```

How to Use the Tool

1. Copy the python script floodFury.py to your desired location
2. **Run the Script with Appropriate Arguments**:

3. Use the following command to run the script from the linux command line:

```
> sudo python floodFury.py -i <network_interface> -t <target_ip> -p -s
<redirect_spoofed_ip>
```

Replace `<network_interface>` with your network interface (e.g., `eth0`, `wlan0`) and `<target_ip>` with the IP address of the target DHCP server.

For example, if you like to spoof DNS requests to redirect to `8.8.8.8` while performing a DHCP starvation attack on a DHCP server with the IP `192.168.100.1`, follow these steps:

```
> sudo python floodFury.py -i <network_interface> -t 192.168.100.1 -p -s
8.8.8.8
```

Replace `<network_interface>` with your network interface (e.g., `eth0`, `wlan0`).

Detailed Breakdown

1. **Network Interface**: Specify the network interface you want to use for the attack.
2. **Target IP**: Set the target DHCP server IP address to `192.168.100.1`.
3. **Persistent Attack**: Use the `-p` flag to make the attack persistent.
4. **Spoof IP**: Set the spoof IP for DNS responses to `8.8.8.8`.

Full Command

```
> sudo python floodFury.py -i eth0 -t 192.168.100.1 -p -s 8.8.8.8
```

This command will:

- Use `eth0` as the network interface.
- Target the DHCP server at `192.168.100.1`.
- Make the attack persistent.
- Spoof DNS responses to redirect to `8.8.8.8`.

How It Works

1. **DHCP Starvation**:
    - Sends DHCP discover and request packets from spoofed MAC addresses to the DHCP server at `192.168.100.1`.
    - Consumes available IP addresses in the DHCP pool, making it difficult for legitimate clients to obtain an IP address.
2. **DNS Spoofing**:
    - Intercepts DNS requests on the network.
    - Responds with spoofed DNS replies that redirect clients to `8.8.8.8`.

And the work has been accomplished!