back to dashboard

Monitor Mode Basics

EXPIRED

Monitor wireless traffic and filter out useful information

15-45 Minutes 250 Points 3/10 Difficulty

Start Stop

You have already completed this exercise.

Mission Statement Verify Flags

Entering into monitor mode is one of the first few steps required to start Wireless Penetration Testing. No matter which toolset you use or which framework you go with. The wireless NIC has to be put into monitor mode to look for interesting packets in the air.

There are many types of packets, but you'll find the most useful ones to be the Management frames.

There are 12 management frame subtypes defined by 802.11-2007 standard. To complete this lab you'd need to use/identify a few Mgmt. Frames using aircrack-ng suite of tools. Frames like:

1. Probes Request/Response
2. Beacon
3. Association
4. Authentication

To actually look at the packet level of the Management frames you can use the following Wireshark filter after putting your card into monitor mode (`iwconfig wlan0 mode monitor`)

```
wlan.fc.type_subtype == 4
```

This filter will help you see only the Probe request packets in Wireshark. To see Probe Response you can change `4` to `5`

For a handy list of Wireshark filters, follow here:
https://www.semfionetworks.com/uploads/2/9/8/3/29831147/wireshark_802.11_filters_-_reference_sheet.pdf