CDPSnarf(Cisco Discovery Protocol Sniffer)

CDPSnarf全称("思科协议发现嗅探器,Cisco Discovery Protocol Sniffer")是一个专门用于提取的网络嗅探器来自CDP信息包的信息。它提供了"显示cdp邻居详细信息"的所有信息。命令会在Cisco路由器上返回,甚至更多。

——Tasos"Zapotek"Laskos

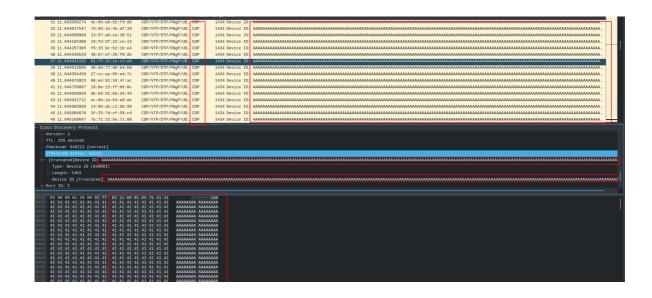
一,帮助手册

- -i 定义要嗅探的接口
- -w 写数据包到PCAP转储文件
- -r 从PCAP转储文件中读取数据包
- -d 显示调试信息
- -h 显示帮助信息并退出
- -i define the interface to sniff on
- -w write packets to PCAP dump file
- -r read packets from PCAP dump file
- -d show debugging information
- -h show help message and exit

二,命令实例

cdpsnarf -i wlan0

嗅探网卡wlan0响应的CDP包[^首先你要有一个CDP包来请求]



cdpsnarf -i wlan0 --w cdp

嗅探wlan网卡中的数据,并将数据保存至名为cdp的PCAP转储文件[^名字你可以自定义]

```
TTL: 255 ms
Checksum: 0x8211
<u>^</u>
<u>^</u>
Port ID: F
×]-[root@parrot]-[/home/kun]
#ls
cdp Desktop Documents Downloads Music Pictures Public temp Templates Videos
-[root@parrot]-[/home/kun]
```

cdpsnarf -r cdp

查看名为cdp的PCAP格式转储文件

Port ID: F
[#59] Sniffed CDP advertisement with a size of 1434 bytes. 0 seconds since last advertisement.
Source MAC address: 09:4C:E1:EE:1B:A5
CDP Version: 1
TTL: 255 ms
Checksum: 0x8211
Device ID: ААААААААААААААААААААААААААААААААААА
<u> </u>
<u> </u>
<u> </u>
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
<u> </u>
<i>\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\</i>
<u> </u>
<u> </u>
<i><b>AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</b></i>

#### cdpsnarf -d -i wlan0 192.168.0.102

## 显示调试信息