Experts in network security monitoring and network forensics

NETRESEC

RawCap

» **Download RawCap.exe** «

RawCap is a free command line network sniffer for Windows that uses raw sockets.

Properties of RawCap:

- Can sniff any interface that has got an IP address, including 127.0.0.1 (localhost/loopback)
- RawCap.exe is just 23 kB
- No external libraries or DLL's needed other than .NET Framework 2.0
- No installation required, just download RawCap.exe and sniff
- Can sniff most interface types, including WiFi and PPP interfaces
- Minimal memory and CPU load
- Reliable and simple to use

Usage

You will need to have administrator privileges to run RawCap.

```
F:\Tools>RawCap.exe --help
NETRESEC RawCap version 0.1.5.0
http://www.netresec.com

Usage: RawCap.exe [OPTIONS] <interface_nr> <target_pcap_file>

OPTIONS:
 -f          Automatically flush data to file after each packet (no buffer)
 -c <count>  Stop sniffing after receiving <count> packets
 -s <sec>    Stop sniffing after <sec> seconds

INTERFACES:
 0.     IP        : 192.168.0.17
        NIC Name  : Local Area Connection
        NIC Type  : Ethernet

 1.     IP        : 192.168.0.47
        NIC Name  : Wireless Network Connection
        NIC Type  : Wireless80211

 2.     IP        : 90.130.211.54
        NIC Name  : 3G UMTS Internet
        NIC Type  : Ppp

 3.     IP        : 192.168.111.1
        NIC Name  : VMware Network Adapter VMnet1
        NIC Type  : Ethernet

 4.     IP        : 192.168.222.1
        NIC Name  : VMware Network Adapter VMnet2
        NIC Type  : Ethernet

 5.     IP        : 127.0.0.1
        NIC Name  : Loopback Pseudo-Interface
        NIC Type  : Loopback

Example: RawCap.exe 0 dumpfile.pcap
```

An alternative to supplying the interface number is to supply the IP address of the prefered interface instead, i.e. like this:

```
RawCap.exe 127.0.0.1 localhost_capture.pcap
```

Interactive Console Dialog

You can also start RawCap without any arguments, this will leave you with an interactive dialog:

```
F:\Tools>RawCap.exe
Network interfaces:
0.     192.168.0.17    Local Area Connection
1.     192.168.0.47    Wireless Network Connection
2.     90.130.211.54   3G UMTS Internet
3.     192.168.111.1   VMware Network Adapter VMnet1
4.     192.168.222.1   VMware Network Adapter VMnet2
5.     127.0.0.1       Loopback Pseudo-Interface
Select network interface to sniff [default '0']: 1
Output path or filename [default 'dumpfile.pcap']:
Sniffing IP : 192.168.0.47
File        : dumpfile.pcap
Packets     : 1337
```

Raw sockets limitations (OS dependent)

IPv6

RawCap cannot capture packets from IPv6 interfaces. This also include the localhost IPv6 interface associated with address ::1. Unfortunately the name "localhost" often resolves to ::1 rather than 127.0.0.1, which can cause confusion. Therefore, when trying to capture application traffic on localhost, make sure the monitored application is connecting to "127.0.0.1" rather than "localhost".

Sniffing localhost

Sniffing localhost/loopback (127.0.0.1) has some limitations under Windows XP. When sniffing localhost traffic in Windows XP you will only be able to capture UDP and ICMP packets, not TCP.
TCP, UDP and ICMP packets can, however, all be sniffed properly from localhost on newer operating systems like Windows Vista and Windows 7.

External interfaces

Microsoft's newer operating systems (later than WinXP) have limitations associated with raw socket sniffing of external interfaces, i.e. everything that isn't localhost. Known limitations in Windows Vista and Win7 are:

- Windows 7 - Can't capture incoming packets
- Windows Vista - Can't capture outgoing packets

Due to these limitations in the raw sockets implementations of Microsoft's current operating systems we suggest running RawCap on Windows XP if you need to capture from external interfaces.

License

RawCap is freeware and can be used by anyone, i.e. even commercial use is allowed.
You are, however, NOT allowed to:

- Re-brand RawCap under a different name or vendor
- Re-distribute RawCap from a website other than netresec.com
- Sell RawCap
- Include RawCap as part of a commercial tool

More information

You can read more about RawCap in our blog post "RawCap sniffer for Windows released".

Download RawCap

You can download RawCap.exe here.