Packet Sniffers

Packet sniffing is listening (with software) to the raw network device for packets that interest you. When your software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like "login" or "password."

To do packet sniffing, you will have to obtain or code a packet sniffer that is capable of working with the type of network interface supported by your operating system:

Network interfaces include:

- LLI
- NIT (Network Interface Tap)
- Ultrix Packet Filter
- DLPI (Data Link Provider Interface)
- BPF (Berkeley Packet Filter)

LLI was a network interface used by SCO, which has been augmented with DLPI support as of SCO OpenServer Release V.

NIT was a network interface used by Sun, but has been replaced in later releases of SunOS/Solaris with DLPI.

Ultrix supported the Ultrix Packet Filter before Digital implemented support for BPF.

DLPI is supported under current releases of System V Release 4, SunOS/Solaris, AIX, HP/UX, UnixWare, Irix, and MacOS. DLPI is partially supported under Digital Unix. Sun DLPI version 2 supports Ethernet, X.25 LAPB, SDLC, ISDN LAPD, CSMA/CD, FDDI, Token Ring, Token Bus, and Bisync as data-link protocols. The DLPI network interface provided with HP/UX supports Ethernet/IEEE 802.3, IEEE 802.5, FDDI, and Fibre Channel.

BPF is supported under current releases of BSD and Digital Unix, and has been ported to SunOS and Solaris. AIX supports BPF reads, but not writes. A BPF library is available for Linux.

Packet Sniffers

Commercial, bundled, and free packet sniffers are available for most operating systems:

Free Packet Sniffers

Ethereal
Platform(s): Most
License: Open Source GPL

Ethereal is used by network professionals around the world for troubleshooting, analysis, software and protocol development, and education. It has all of the standard features you would expect in a protocol analyzer, and several features not seen in any other product. Its open source license allows talented experts in the networking community to add enhancements. It runs on all popular computing platforms, including Unix, Linux, and Windows.

tcpdump
Platform(s): Most
License: BSD License

Tcpdump prints out the headers of packets on a network interface that match the boolean expression. It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -b flag, which causes it to read from a saved packet file rather than to read packets from a network interface. In all cases, only packets that match expression will be processed by tcpdump.

Natas
Platform(s): Windows
License: Free

Natas is a free Windows 2000 network packet sniffer with several options. Sourcecode (C++) included.

nfswatch/
Platform(s): Unix
License: Open Source

nfswatch is a packet sniffer which is dedicated to sniffing NFS (Network File System) traffic. nfswatch lets you monitor NFS requests to any given machine, or the entire local network. It mostly monitors NFS client traffic (NFS requests); it also monitors the NFS reply traffic from a server in order to measure the response time for each RPC.

Web Packet Sniffer
Platform(s): Unix
License: Open Source

Web Packet Sniffer is a pair of Perl scripts that together will:

- Listen to all TCP/IP traffic on a subnet.
- Intercept all outgoing requests for Web documents and display them.
- Intercept all incoming requests for Web documents and display them.
- Decode the Basic authentication passwords, if any.

Sniffit
Platform(s): Linux, SunOS, Solaris, FreeBSD and Irix
License: Open Source

sniffit is a packet sniffer for TCP/UDP/ICMP packets. sniffit is able to give you very detailed technical info on these packets (SEQ, ACK, TTL, Window, ...) but also packet contents in different formats (hex or plain text, ...).

Bundled Packet Sniffers

Microsoft Network Monitor
Platform(s): Windows

License: Bundled with Microsoft Windows

Microsoft Network Monitor is the packet sniffer which is bundled with Microsoft Windows.

Network Monitor is a component of Microsoft? Systems Management Server (SMS) that enables you to detect and troubleshoot problems on LANs, WANs, and serial links running the Microsoft? Remote Access Server (RAS). Network Monitor provides real-time and post-capture modes of network data analysis.

In real-time analysis, network traffic is examined by real-time monitors. These monitors test network traffic for a specific set of conditions, and when those conditions are detected, display events, which may prompt end-user action. For example, a monitor can detect conditions that indicate a SYN attack and aid a network administer to respond to the potential attack.

In post-capture analysis, network traffic is saved in a proprietary capture file so that the captured data can be analyzed later. In this case, analysis can be in the form of protocol parsers picking out specific network frame types and displaying the frame data in the Network Monitor UI; or analysis can be in the form of experts examining the network data and displaying a report (experts may also manipulate the network data).

Network Monitor provides the following types of functionality:

- Captures network data in real-time or delayed mode.
- Provides filtering capabilities when capturing data.
- Uses monitors for real-time analysis and security.
- Uses experts and parsers for detailed post-capture analysis.

snoop
Platform(s): Solaris
License: Bundled with Solaris

snoop is the packet sniffer which is bundled with the Solaris Operating System.

snoop captures packets from the network and displays their contents. snoop uses both the network packet filter and streams buffer modules to provide efficient capture of packets from the network. Captured packets can be displayed as they are received, or saved to a file for later inspection.

snoop can display packets in a single-line summary form or in verbose multi-line forms. In summary form, only the data pertaining to the highest level protocol is displayed. For example, an NFS packet will have only NFS information displayed. The underlying RPC, UDP, IP, and ethernet frame information is suppressed but can be displayed if either of the verbose options are chosen.

nettl / netfmt
Platform(s): HP-UX

License: Bundled with HP-UX

The nettl and netfmt packet sniffing utilities are bundled with the HP-UX operating system.

Commercial Packet Sniffers

LanWatch
Platform(s): DOS/Windows
License: Commercial

LANWatch is a software-based network packet analyzer. Easy to install and use, LANWatch monitors traffic in real time and displays a wide range of statistics. With LANWatch, network administrators can quickly identify problems and keep networks running at peak performance. Support and QA Personnel can determine the origin of network problems. Network Application and Protocol Developers can easily monitor, examine and verify network protocols in both hexadecimal and formatted views.

Etherpeek
Platform(s): Windows, Macintosh
License: Commercial

EtherPeek is an Ethernet network traffic and protocol analyzer designed to make the complex tasks of troubleshooting and debugging mixed-platform, multi-protocol networks easy. EtherPeek sets the industry standard for ease-of-use while delivering all the superior diagnostic and analysis capabilities expected of a full-featured analyzer at an affordable price.

Sniff'em
Platform(s): Windows
License: Commercial

Sniff'em captures, monitors and analyzes network traffic, detecting bottlenecks and other network related problems. Using this information, a network manager can keep traffic flowing efficiently. The Sniff'em packet sniffer can also be used legitimately or illegitimately to capture data being transmitted over a network.

Sniff'em is a competitively priced, performance minded Windows based Packet sniffer, Network analyzer and Network sniffer, a revolutionary new network management tool designed from the ground up with ease and functionality in mind.

Source: http://www.go4expert.com/articles/packet-sniffers-t3686/