

# Sniff'em 1.01 Whitepaper

---

## Brief technical Introduction

A packet sniffer is a wiretap device that plugs into computer networks; unlike telephone circuits, computer networks are shared communication channels. Sharing means that computers can receive information that was intended for other machines (HUB). To capture the information going over the network is called sniffing.

Most popular way of connecting computers is through Ethernet. Ethernet protocol works by sending packet information to all the hosts on the same segment. The packet header contains the address of the destination and source machine. Only the machine with the matching address is supposed to accept the packet. A machine that is accepting all packets, no matter what the packet header says, is said to be in promiscuous mode.

Because, in a normal networking environment, account and password information is passed along Ethernet in clear-text, it is not hard for an intruder once they obtain root to put a machine into promiscuous mode and by sniffing, compromise all the machines on the net.

Sniff'em™ uses the promiscuous mode in the NDIS driver to enable the card to listen to data traffic. NDIS is an abbreviation for the "Network Driver Interface Specification" and is a Windows device driver interface that enables a single network interface card (NIC) to support multiple network protocols. For example, with NDIS, a single NIC can support TCP/IP, IPX, and more protocols; NDIS can also be used by ISDN adapters.

These are complicated technical details, however Sniff'em™ integrates them with ease, without bothering the user with too much complicated stuff.

## Supported Protocols

Sniff'em™ detects and/or decodes following Protocols:

### High-Level Protocols

Padding Protocol, Lcc Management, Lcc Group, Sna Path I, Sna Path G, Proway Lan, Iso Net, Internet Protocol, Map Management, OSI Network Layer, Xerox NS IDP, DECnet Phase IV, AppleTalk, Novell IPX, Van Jacobson Compressed TCP/IP, Van Jacobson Uncompressed TCP/IP, Bridging PDU, Banyan Vines, Stream

Protocol (ST-II), Reserved (until 1993), AppleTalk EDDP, AppleTalk SmartBuffered, PPP Multi-link Protocol, Cisco Systems, NetBIOS Framing, Spanning Tree, Ascom Timeplex, Fujitsu Link Backup and Load Balancing (LBLB), DCA Remote Lan, PPP Serial Data Transport Protocol, SNA over 802.2, SNA, Rs 511, IP6 Header Compression, Stampede Bridging, PPP Ascend's Multilink Protocol Plus, Reserved (Control Escape) [RFC1661], X25, ARP, PPP Internet Protocol Control Protocol, PPP OSI Network Layer Control Protocol, PPP XNS IDP Control Protocol, PPP DECnet Phase IV Control Protocol, PPP AppleTalk Control Protocol, PPP IPX Control Protocol, PPP IPv6 Control Protocol and others.

### **Low-Level Protocols**

CMP, IGMP, GGP, IP in IP (encapsulation), ST, TCP, CBT, EGP, IGP, BBN-RCC-MON, NVP-II, PUP, ARGUS, EMCON, XNET, CHAOS, UDP, TMMUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, RDP, IRTP, ISO-TP4, NETBLT, MFE-NSP and others.

Note that some of these Protocols are only available on Windows 9.x systems and some only on Windows 2000 and Windows NT.

## **Requirements**

### **Hardware**

Minimum : 16mb Ram, 486 or equivalent, promiscuous mode capable NIC.

Recommended : 128mb Ram, Pentium or equivalent, promiscuous mode capable NIC.

### **Software**

Windows 95abc, 98, 98se, ME, NT4, NT5, 2000, XP.

---