Sniff'em 1.01

Whitepaper

Technical Introduction

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" 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 Requirement: 16mb Ram, 486 or equivalent, promiscuous mode capable NIC.
Recommended Requirement: 128mb Ram, Pentium or equivalent, promiscuous mode capable NIC.

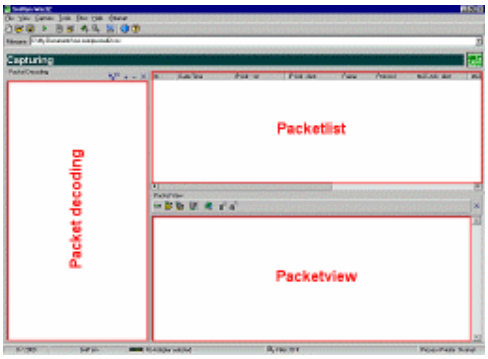
Software

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

Graphical user Interface

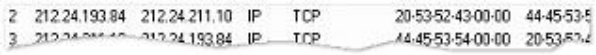
Main Graphical user interface

Sniff'em™ uses a simple Graphical User interface, which allows simple usage while conserving powerful user manipulation. The main Graphical User Interface (GUI) is divided into three parts: The *Packet list*, *Packet view* and *Packet decoding* view.



Packet List

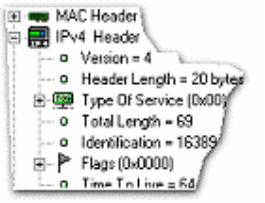
The Packet list pane displays incoming and outgoing Network packets in Chronological order.



Additionally a right-click menu offers flexible options to Save, Edit Select, Remove, Invert, Export, Find, Refresh.

Packet Decoding

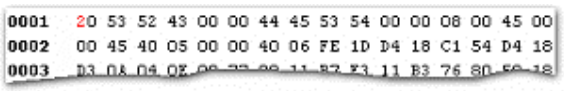
In the Packet Decoding view Packets are decoded and displayed in a Tree based structure. The main nodes are the different protocol Headers and Field values. These 3 panes interoperate based on User input, if you select a value from the Tree it will automatically show you where that value is located inside the raw Packet data in the Packet View by colouring the data parts of the packet in Blue.



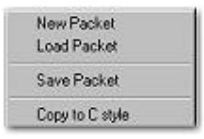
Double clicking a Tree view entry allows you to change the value of the selected field, which will immediately mirror the changes in the raw packet data and as such in the Packet view.

Packet View

The raw packet data will be represented in the Packet View, and Hexadecimal as well as an ASCII view on the packet data. The selected Data part will be displayed as RED and is browsable by using your direction keys on your keyboard. BLUE values are displayed if a correspondent Packet Decoding Value has been selected. These values can be changed on the fly, by simply selecting the Packet view and typing on your keyboard, as such you are able to immediately change the contents of captured Network packets, even more, you are able to send them over the ether in the changed or original state.



Again, a right-click menu offers flexible options such as *New packet, Load packet, Save packet, Copy C style, Copy Packet style*. The two copy options will copy to the raw packet data to the Clipboard, for further interaction.

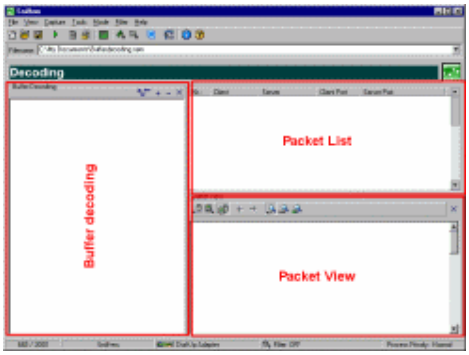


Graphical user Interface

Buffer Decoding

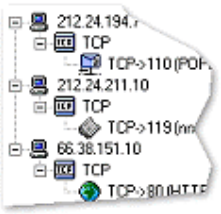
While the main Graphical user interface is a real-time display, the Buffer Decoding view does additional clustering, reassembly and decoding routines to offer a broad overview over the Network usage and Network captures currently within the Buffer.

The Buffer Size can be adjusted in the Settings menu, the more available RAM your PC configuration has the more Packets the Buffer can hold. Note that Sniff'em™ offers a way to open saved projects that has more packets than the Buffer can hold.



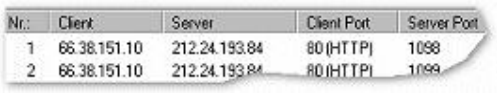
Buffer Decoding Tree

Buffer decoding is like the Packet decoding view Tree based structure representing the Source IP (Hostname or equivalent) together with the correspondent decoded protocols. Contrary to the Packet decoding view these protocols are session reassembled. As such, you are able to browse a whole Telnet session done by a host; you can follow exactly what they typed, in either ASCII, HEX or Packet data. The same goes for POP3, SMTP, IRC, IDENT, NETBEUI, DNS, HTTP and many more.



Packet List

The Packet List within the Buffer Decoding View shows the connections between Client and Server based on the protocol chosen, for instance if you choose POP3 for it is going to list all captured Network packets that were send from the selected IP to that Host using POP3 as Protocol. Furthermore it offers yet another right-click menu that lets you access the tagging feature of Sniff'em™ which is described in a paragraph at the bottom of this page.



Nr.:	Client	Server	Client Port	Server Port
1	66.38.151.10	212.24.193.84	80 (HTTP)	1098
2	66.38.151.10	212.24.193.84	80 (HTTP)	1099

Packet View

This view displays the content of the decoded Packets, as example, for HTTP, it shows all GET, POST requests and their response, for Telnet every command send and received. Note that you may choose if you only want to see the Received data, the Send data, or both, additionally you may view the content as plain ASCII or HEX or structured packet data.

Handy Feature

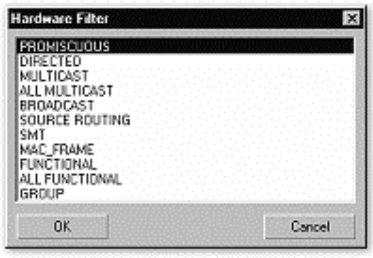
Tagging

Right clicking on the Packet list within the Buffer Decoding view gives you the possibility to tag Session reassembled by Sniff'em™ and made visible inside the Main Graphical user interface. The example shows a HTTP tagged packet and the result in the Main Graphical User Interface, note that you may tag five different Sessions which will have attributed five different coloured icons. Easy to spot these sessions within the Main graphical User Interface Packet List using this small feature.

Filter facility

Hardware Filter

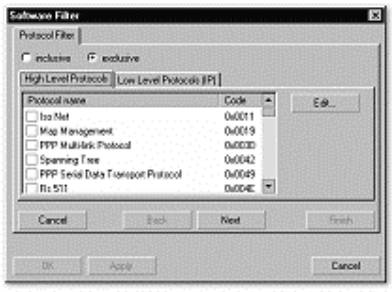
Sniff'em™ is able to make use of several advanced Hardware filter modes, these modes include:



1. Promiscuous: captures all Packets.
   All Functional: All functional address packets, not just the ones in the current functional address.
2. All Multicast: All multicast address packets, not just the ones enumerated in the multicast address list.
3. Broadcast: Broadcast packets.
4. Directed: Directed packets. Directed packets contain a destination address equal to the station address of the NIC.
5. Functional: Functional address packets sent to addresses included in the current functional address.
6. Group: Packets sent to the current group address.
7. Mac Frame: NIC driver frames that a Token Ring NIC receives.
8. Multicast: Multicast address packets sent to addresses in the multicast address list. A protocol driver can receive Ethernet (802.3) multicast packets or Token Ring (802.5) functional address packets by specifying the multicast or functional address packet type. Setting the multicast address list or functional address determines which multicast address groups the NIC driver enables.
9. SMT: SMT packets that an FDDI NIC receives.
10. Source Routing: All source routing packets. If the protocol driver sets this bit, the NDIS library attempts to act as a source routing bridge.

Software Filter

Additionally to the Hardware filters Sniff'em™ offers very flexible and advanced Software Filters, these sometimes complex filters can be integrated with ease using the foolproof Graphical User interface. Software filters are able to Filter based on:



1. High-Level protocol (IP, X75, X25..)
2. Low-Level protocol (ICMP, IGMP, TCP..)
3. IP Source (Wildcards supported)
4. IP Destination (Wildcards supported)
5. Source Port (Port ranges supported)
6. Destination Port (Port ranges supported)
7. MAC Destination
8. MAC Source
9. ASCII Packet data
10. TCP State (SYN, ACK, RST) and Size

Exclusive Filters

Available for all filters, these settings will capture and display packets that are NOT selected. It will exclude the selected Protocol, Port, Mac address, etc.

Inclusive Filters

Available for all filters, this settings will only capture and display protocols, which are selected and ignore the others.

Practical uses for Filter

1. Filter out the Packet valuable for Network analysis. (Broadcast, ICMP error)
2. Monitor internet usage (Filter HTTP traffic and words like Porn, sex, etc)
3. Special Events (Trigger Mode) Capture traffic immediately AFTER a special predefined event occurred (ftp login, smtp message)

Filter facility

Filter Modes (introduced in version 1.1)

Tagging Filter
Using this Filter mode Sniff'em™ will capture and display all the Traffic and takes in consideration the Filters that were set. The difference here is that if given *Tag filter* is hit by an Network packet; Sniff'em™ will tag it by assigning a special value to the Tag index, this features allows users to immediately see the packets they wanted to get hold of while still capturing the whole data traffic crossing the network.

Normal Filter
Only Packets that are specified in the Filter settings (In case of the inclusive filter set) will be captured others will be "dropped". (Vice versa for the Exclusive filter)

Action Filter (introduced in version 1.1)

Execute (Shell)
Action filter allow special action to be done when a predefined filer is hit, as example if a predefined packet hits the network Sniff'em is able to spawn "trace.exe %ip.source >> %ip.source.txt". Note that the executable that is spawned supports dynamic parameters and that MS-DOS batch files may be called too and as such you are able to shell an unlimited number of Applications with dynamic parameters.

Net Message
The Net message will send a Net message to a machine over a network once the Filter was hit, this is ideal for Intrusion Detection as well as special events, break-ins, policy infringement (Games, surfing)

Generalities

Usage Modes

Normal Mode
Real-Time display of captured packets, incoming Network packets will be immediately decoded and added to the Packet list, this eats up a whole lot of resources, this is why we introduced the *Logging only* mode.

Logging Only
Logging only mode will disable the graphical display of incoming packets temporarily and capture the packets by logging them to the hard disc with a minimum of CPU usage, this is a real performance boost and recommended for heavy loaded networks.

Trigger mode
The Trigger mode is another nifty feature of Sniff'em™, it uses a predefined Filter to set it's Trigger event. As example: a Trigger filter is set to port 110 (POP3) and ASCII data "Password: superjemp", once such a packet is found (i.e. a user logs in) Sniff'em™ will start capturing subsequent traffic be it filtered or not.

Buffer Size

Limits
The Buffer size can be adjusted in the Settings menu, it directly scales with free memory, when using Normal mode the display will be cleared once the limit set has been reached, if *Logging Only* mode is activated the Buffer Size is ignored. However when you open a saved Project which is bigger then Buffer size, a new Window will pop-up and give you the possibility to select the range of Packets to load into the Buffer. You may also change the Size of the Buffer to hold the whole Project.