IP Sniffer is a suite of IP Tools built around a packet sniffer.

The packet sniffer can work on all Windows versions using either the new raw socket implementation of Windows2000 (driverless) or WinPcap (needs to be installed) or a NDIS protocol (needs to be installed, no reboot). The sniffer has basic features like filter, decode, replay, parse...

The IP tools are:

- Bandwidth monitor.
- Adapter statistics (IP & NDIS).
- List and manage ARP entries, resolve IP to MAC, resolve MAC to IP, send a WAKEUP call.
- List and manage routes, enable & disable host as a router.
- List and manage open ports and attached processes.
- Edit network config.
- Hook winsock (winsock32.dll & ws2_32.dll).
- Spoof ARP (and do ARP cache poisoning), spoof TCP, spoof UDP, spoof ICMP, spoof DHCP Release.
- Change MAC address.
- SNMP Get & Set, List interfaces, Switch port mapper, Media Attachment Unit table.
- WINS Query.
- DNS (advanced) Query.
- Local resolver.
- DHCP Server, DHCP Discover.
- Whois Query.
- SMTP client.
- TCP tools (TCP ping, TCP half scan, Time-Daytime client/server).
- UDP tools (MSSQL Ping, SNMP ping, SSDP scan, Syslog client/server, Time-Daytime client/server).
- ICMP tools.
- TCP/UDP bounce port.
- MS Networks (enum servers by type, spoof net send, shutdown windows, remote properties, netbios names, Terminal Services process mgmt)
- Password tools :

Edit protected storage (IE, Outlook Express, ...), Decrypt Dialup Passwords, Dump XP Credentials (MSN, network shares, ...) & decrypt passwords, Decode IE history, Reveal asterisks / hidden passwords, decode RDP, Decode MSAccess passwords).

- List and manage local & remote processes.
- Tiny firewall (using Windows API).
- Test bandwidth.
- Get internet IP.

File

1. Load Single Frame

Will load a DMP file containing one network frame. It will contain the Ethernet header if you are in NDIS or WINPCAP mode.

2. Load Frames

Will load a cap file containing multiple Ethernet frames. This file is a true pcap file (compatible with ethereal for instance).

3. Save Single Frame

Will load a file containing one network frame.

4. Save Frames

Will save a cap file containing multiple Ethernet frames. Mac address will zeroed if running in RAW IP mode.

5. Exit

Terminates the application.

View

1. Autoscroll

Will autoscroll the frames listview (top panel) so that the last frames is always visible.

Can be CPU consuming.

2. Refresh

Will auto refresh the frames list view (top panel). Can be switched off to gain release CPU.

3. AutoExpand Decoder

Will auto expand the decoder treeview (right panel).

4. Display EBCDIC

Will display characters as *Extended Binary-Coded Decimal Interchange Code*. <u>IBM</u> code for representing <u>characters</u> as numbers. Mostly used on large IBM computers (AS400, etc).

5. Capture Statistics

Will display the stats for the current capture : Protocol distribution, top 10 IP's IN & Out.

6. Ethernet Protocols

Will display a list of Ethernet protocols.

7. IP Protocols

Will display a list of IP protocols.

8. Mac Address Vendor Codes

Will match a vendor to a MAC Address.

Edit

- 1. Copy selection as text Will copy selected text to the windows clipboard in the hexa editor (bottom panel)
- 2. Copy selection as hexa Will copy selected hexadecimal to the windows clipboard in the hexa editor (bottom panel)

Capture

1. Mode

Winpcap: will capture Ethernet frames using Winpcap (need to be installed)

RAW IP: will capture IP frames using Windows Native RAW IP (Win2000, XP, Win2003)

NDIS: will capture Ethernet frames using NDIS driver (need to be installed)

2. Promiscuous

Will set the promiscuous mode to true or false.

When set to true, all packets (including one that are not directed to the host running IP Tools) will be displayed (in a non switched network).

3. Start / Stop

Will start or stop the capture.

4. Clear

Will clear all panels: frames, hexa editor and decoder view.

5. Replay Selected Frame

Will replay the current selected frame.

6. Filters

Will display the filter window.

Bandwidth monitor

Locally

There, you can monitor the bandwidth in use for your adapters. Windows API IPHLPAPI, GetIfTable, is used to achive this.

Remotely

There, you can monitor the bandwidth in use on remote hosts. Microsoft WMI must be installed locally and remotely. You must be a local admin on the remote host. Note: WMI is installed by default on W2K, XP, W2K3. It must be installed manually on NT4 and W9X.

Adapter Statistics

1. Stats

Here you will retrieve all stats for IP, TCP, UDP, ICMP on your system. Windows API HLPAPI GetIpStatistics is used.

1. Protocol Distribution

Here you will get a graphical representation of network usage by TCP, UDP, ICMP.

API's used are the same as above.

Usually, most traffic should be TCP.

2. NDIS Stats

Here you will get a graphical representation of network usage by Directed, Broadcast, Multicast packets.

DeviceIOcontrole API is used to retrieve these datas.

A too high number of multicast or broadcast packets might indicate network issues.

ARP

1. ARP Entries

There you can list all ARP entries on your computer.

You can also add or delete one.

From There you can ping a host so that its MAC address will be added in your ARP entries.

From There you can also send a ARP request (resolve IP to MAC).

Doing so will not add the resolved MAC address to your ARP Entries : you then have to do it manually.

2. Send ARP

This will send an ARP Request so that you can resolve an IP address to its MAC address.

3. MAC to IP

This will resolve a MAC address to its IP address.

The entire subnet you belong to will be searched (sending ARP requests in a loop).

4. MAC Discovery

This will display all MAC addresses on your subnet, along with the IP and the MAC vendor code.

The entire subnet you belong to will be searched (sending ARP requests in a multithreaded loop).

5. Wake UP Call

Will send a Wake On Lan call

Open Ports

1. Ports by Process

This will display Process ID, Port, Protocol, and Process full path. This will work on NT4, W2K, XP, W2K3.
On NT4 and W2K, the native API NtQueryObject is used.
On XP and up, the advanced IPHLPAPI are used.

2. Netstat

The classical netstat, using IPHLPAPI. Each socket can be terminated. Process Name and PID will be displayed, if supported. Process can be terminated, or hooked.

Network Configuration

1. NDIS Properties

This will retrieve information via NDIS OID's. You can also scan wireless networks and retrieve various informations.

2. Interface Cards

This will retrieve information for the specified interface on the local computer via IPHLPAPI / GetInterfaceInfo.

3. Network Adapters

This will retrieve adapter information for the local computer via IPHLPAPI / GetAdaptersInfo.

4. Network Params

This will retrieve network parameters for the local computer via IPHLPAPI / GetNetworkParams.

5. TCP IP parameters reg key

This will open regedit and open HKEY_LOCAL_MACHINE\system\currentcontrolset\services\tcpip\parameters key.

6. ADD IP

This will add an IP on your computer via IPHLPAPI / AddIPAddress. This IP will disappear next time NIC is disabled/enabled.

Routing

1. Route Print

There you can display the routing table of your computer. You can also add, delete, modify any route.

2. Enable / Disable

There you can turn your computer into a router.

Any packet reaching your network card that is not addressed to you will be routed to the correct host.

You computer can then be use as a gateway.

You can check if routing is on in the stats windows. You should read this : forwarded datagrams : 0 (IP Forwarding ON)

Winsock Hook

Here, you can hook winsock API's for one particular process. Everytime the process will call one the winsock API's (send, recv, ...) it will be displayed in the main windows.

A DLL will be injected via CreateRemoteThread. The DLL will then hook winsock API's and inform IP tools via SendMessage.

ARP Spoof

1. Reply / Poison Cache

Here you can send forged ARP Replies.

This way you can fool a remote host with the following assertion: MAC SRC belongs to IP SRC.

The remote host will therefore modify his ARP cache accordingly.

One possible attack

Network looks like this:

Router is 192.168.1.1, MAC AAAAAA-AAAAAA

You are 192.168.1.2, MAC BBBBBB-BBBBBB

Victim is 192.168.1.3, MAC CCCCCC-CCCCC

Send the following spoof ARP Reply: MAC SRC= BBBBBB-BBBBBB, IP SRC=192.168.1.1, MAC DEST= CCCCCC-CCCCC, IP DEST=192.168.1.3

The remote host (192.168.1.3) will then think you (192.168.1.2) are the router since your MAC Addresses is resolved for the IP's router in the remote host ARP table.

2. Request

Here you can send forged / spoofed ARP requests. Same possible attack as above.

Note, to use these functionalities, you must be set to WINPcap mode or NDIS mode for you need to be able to alter layer 2.

IP Spoof

1. TCP/UDP Spoof

Here, you can forge TCP or UDP packets.

Will work with RAW sockets, WINPcap, NDIS.

In WINPcap and NDIS mode, the MAC source address will be the sending computer's one.

XP SP2 will not send forged packets with RAW sockets.

2. ICMP

Here you can forge ICMP Packets: Echo, Redirect, Mask, Timestamp request, Information request.

Echo can be use to guess the remote host operating system (playing with the code bit).

Redirect can be used to modify the route table on the remote host.

One possible attack

Network looks like this:

Router is 192.168.1.1

You are 192.168.1.2

Victim is 192.168.1.3

Remote host is 66.102.11.99

Send an ICMP redirect like this: source = 192.168.1.1, victim is 192.168.1.3, new gateway for remote host 66.102.11.99 is 192.168.1.2.

This way, next time 192.168.1.3 wants to reach 66.102.11.99, it will send packet to 192.168.1.2 (you).

3. TCP Reset

You can reset a remote connection on a remote host.

Meaning you can reset a connection between host A and host B being host C. IP tools will send spoof TCP reset frames with a SEQ number from 0 to FF FF

FF FF with a step of Window Size.

If you can guess a TCP Seq number close enough (within the window size), then you can reset a remote connection on a remote host. You also have to guess the client TCP port (> 1024).

4. NBT Name Service

You can send false windows host announcement (UDP / 138). The browser list will then display false informations.

5. DCHP Release

You can send a false DHCP release packet to a DHCP server. The server will then free the IP and offer it to somebody else. This could create IP collision.

Change MAC Address

This will change the MAC Address of your Network Interface Card. This is accomplished by modifying the windows registry.

SNMP

1. GET/SET

Can GET, Walk or SET OID for a given SNMP device.

2. Interfaces

Will walk OID 1.3.6.1.2.1.2.2.1.1 to retrieve network interfaces for a given SNMP device

3. Switch Port Mapper

Will walk OID 1.3.6.1.2.1.17.4.3.1.1 to retrieve ports for a given SNMP switch/hub.

4. MAU Table

Will walk OID 1.3.6.1.2.1.26.2.1.1.1 to retrieve information on Media Attachment Unit table for a given SNMP device.

5. Net To Media Table

Will walk OID 1.3.6.1.2.1.4.22.1.2 to retrieve the ARP table for a given SNMP device.

WINS

1. Host Query

Will query a WINS server (or any windows host) with specific records.

2. User Query

Will query a WINS server (or any windows host) for a specific user. This way one can easily locate computer(s) on which a user is logged on.

No windows API's are used. UDP frames are forged and sent over the network.

DNS

Will query a DNS server, specifying the query type. Windows Dnsapi.dll is used.

A all set of parameters can be choosen.

Hostname Resolver

Will resolve hostname to IP and IP to hostname with GetHostByName/GetHostByAddr windows API's.

DHCP

1. DHCP Server

Implements a small DHCP server. Also supports PXE DHCP options. Can turn into a PXE server using a UDP server.

2. DHCP Discover

Will send a DHCP discover UDP frame on the subnet to discover DHCP servers. Eventually display some the DHCP options sent out by DHCP servers.

No windows API used. UDP frames are forged and parsed.

WHOIS

Will query a whois server by sending a TCP frame on port 43.

SMTP Client

Will send a mail to a SMTP server. This can be used to send a mail on behalf on someone else. Mail format can be raw text and html.

TCP TOOLS

1. TCP Scan (connect)

Will perform a full connect scan (host or subnet).

This mean the scanner will send a SYN, the scan host will sent a SYN+ACK and the scanner will finally send a ACK.

2. TCP Scan (Half Connect)

Same as above but the scanner will send only a SYN, thus not establish a connection.

3. TCP Ping (Half Connect)

Will detect online host by send a SYN / FIN / XMAS (all flags set) / Null (no flag set).

Remote host will etiher send a RST+ACK / SYN+ACk depending if the choosen port is open/closed.

4. TCP Client / Server

Standard TCP client / server.

Can be used for any purpose.

5. Telnet Client / Server

Standard Telnet client / server.

Any user/pwd can be used to log in the telnet server.

6. SQL Login

Will try out a username / password against a SQL server.

7. Time Client / Server

Standard time client / server (TCP port 37).

8. DayTime Client / Server

Standard daytime client / server (TCP port 13).

UDP TOOLS

1. MSSQL Ping

Will send a UDP frame on port 1434 and retrieve basic informations on the remote MS SQL Server.

2. NTP Client

Will retrieve time via Network Time Protocol (UDP 123).

3. SNMP Ping

Will detect online host(s) running a SNMP Server and retrieve Sysinformation field.

1. SSDP Ping

Will detect online host running a SSDP server. (UDP 1900).

2. Syslog Client / Server

Basic syslog client and server. (UDP 514).

3. Time Client / Server

Basic time client and server. (UDP 37).

4. DayTime Client / Server

Basic time client and server. (UDP 13).

5. TFTP Server

Trivial FTP server with TSIZE option support. (UDP 69). Can be used in conjunction with the DHCP server to act as a PXE server.

ICMP TOOLS

1. Ping

Will ping a host or entire subnet using ICMP echo trames.

2. Tracert

Will send ICMP echo trames to a remote host, starting with a TTL=1 and then increasing it

TCP UDP Bouncer

Here you can bounce/map a loca port to remote port. Can be useful when spoofing IP.

Decoder Tools

1. Protected Storage

Will display datas stored in the protected storage.

User ids and passwords from applications such Outlook Express, Internet Explorer will be displayed in clear text.

2. Dump Credentials

Will dump credentials on XP and Windows 2003.

Credentials can be: NT user ids and passwords stored for network drives mappings, Outlook pop3 accounts, MSN messenger accounts...

3. Password Reveal

Will un hide passwords behind asterisk.

4. Dialup Password

Will display windows dialup user ids and passwords.

5. Decode IE History

Will decode the history file of Internet Explorer (History, Temprorary internet files, coockies).

6. Decode Base64

Will decode a Base64 string.

7. Decode MDB

Will retrieve the password used to lock a MS Access MDB file.

8. Decode RDP

Will decode the password stored in a MS Remode Desktop Protocol (RDP) file.

9. Hash Calculator

Will calculate the hash for MD5, SHA1, NTLM...

MS Networks

1. Enum Windows Servers

Will enum all windows by type.

A contextual menu offers many options.

A remote server can be used to retrieve the list of windows servers.

1. Netbios Names

Will retrieve windows the netbios names table (nbtstat).

2. Shutdown Windows

Will shutdown a remote windows.

3. Remote Windows Properties

Will retrieve properties from a remote windows using remote registry. Informations are system, version, environment, hotfixes, applications. The version informations contains the windows CDKEY.

4. Remote TOD

Will retrieve the remote Time Of Day of a windows server.

5. Spoof Net Send

Will send a net send message with the possibility to spoof the sender name.

6. Terminal Services

Will enumerate processes and sessions on a remote Terminal Server. Actions such as kill process, close session or disconnect user can be performed.

7. Impersonate User

Will impersonate (within the context of the current process) a windows NT account.

8. Enum Print Ports

Will retrieve the printers ports on a remote windows server.

9. Enum Print Drivers

Will retrieve the printer drivers on a remote window server.

10. Enum Drivers

Will retrieve the drivers on a remote windows server. Driver can be stopped or started.

Processes

1. Local Processes

Will display processes and modules.

There one can dump or view process memory.

One can also attach or detach a module to a process.

2. Process Monitor

Can monitor creation and deletion.

Events are displayed in the systray tooltip.

3. Remote Processes

Will display the list of processes on a remote windows thanks to WMI.

Processes can be killed or created on the remote host.

Firewall

Here you can block IP Trafic based on direction (IN or OUT), Protocol (TCP, UDP), IP, Port.

You add one or many filter.

Filters can be saved and restored later.

The PF* API's from IPHLPAPI.DLL are used.

Internet IP

Your internet IP will be retrieved, provided that you have a direct connection to Internet (no proxy).

IP is obtained via http://checkip.dyndns.org/.