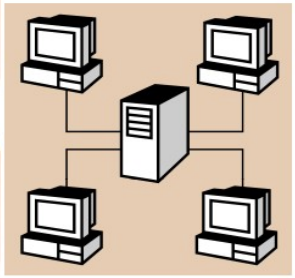
SnniffingAttack

Dr. Ravi Verma

SNIFFING

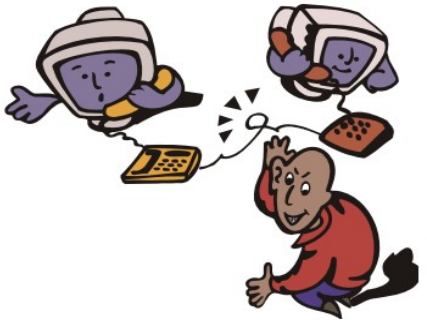
Sniffing is a data interception technology



Sniffer is a program or device that captures the vital information from the network traffic specific to a particular network

The objective of sniffing is to steal:

- Passwords (from email, the web, SMB, ftp, SQL, or telnet)
- Email text
- Files in transfer (email files, ftp files, or SMB)

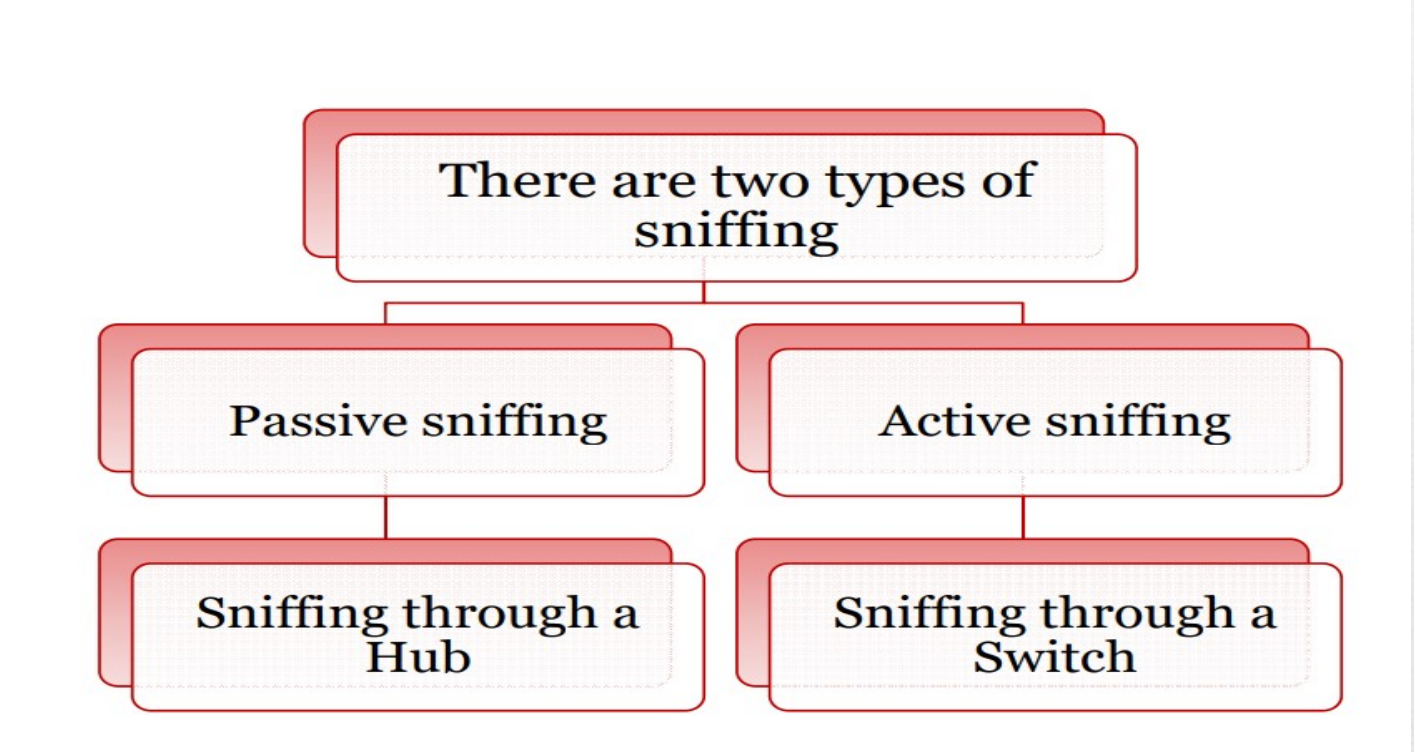


PROTOCOLS VULNARABILTIES

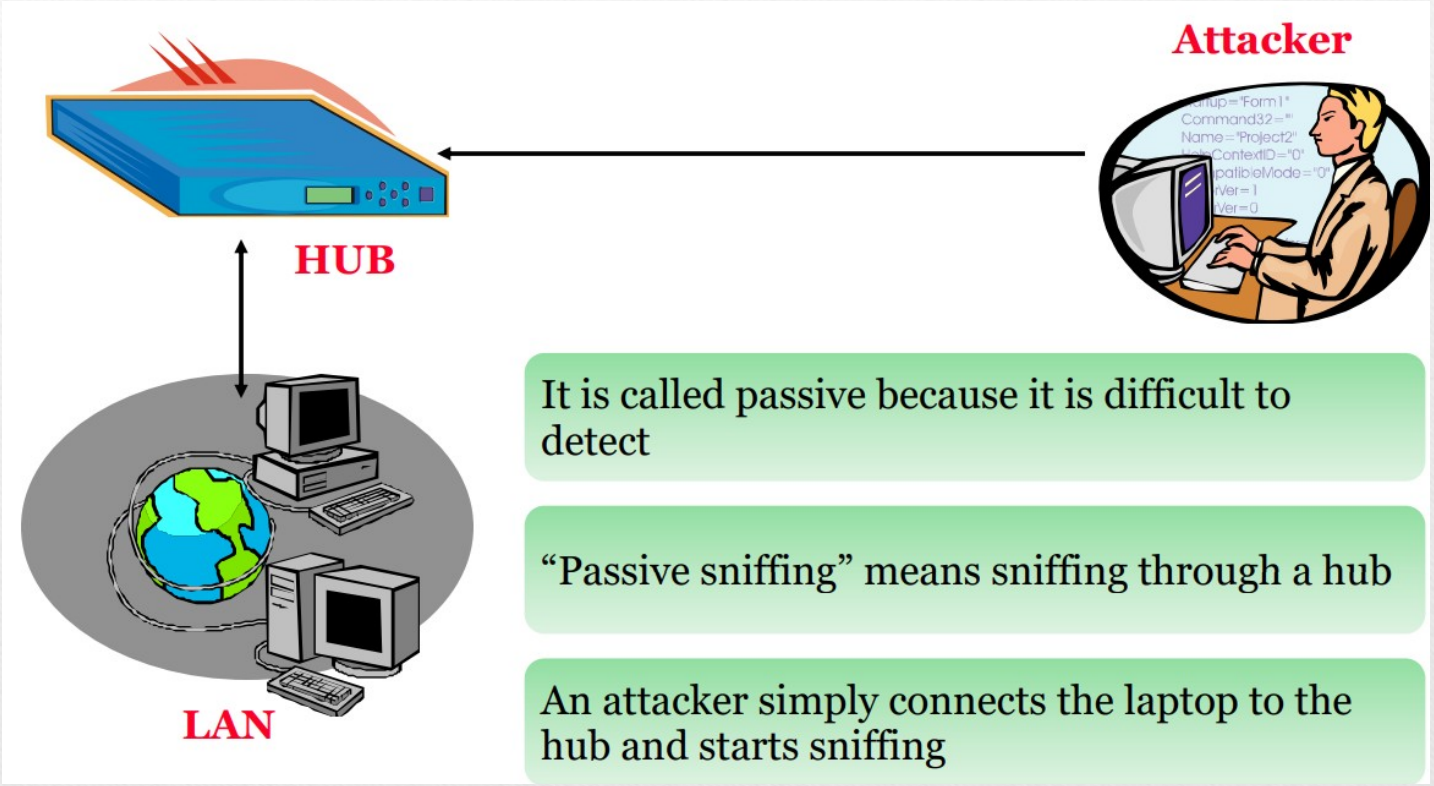
Protocols that are susceptible to sniffers include:

- Telnet and Rlogin: Keystrokes including user names and passwords
- HTTP: Data sent in the clear text
- SMTP: Passwords and data sent in clear text
- NNTP: Passwords and data sent in clear text
- POP: Passwords and data sent in clear text
- FTP: Passwords and data sent in clear text
- IMAP: Passwords and data sent in clear text

TYPES


There are two types of sniffing
Passive sniffing
Active sniffing
Sniffing through a Hub
Sniffing through a Switch

PASSIVE SNIFFING

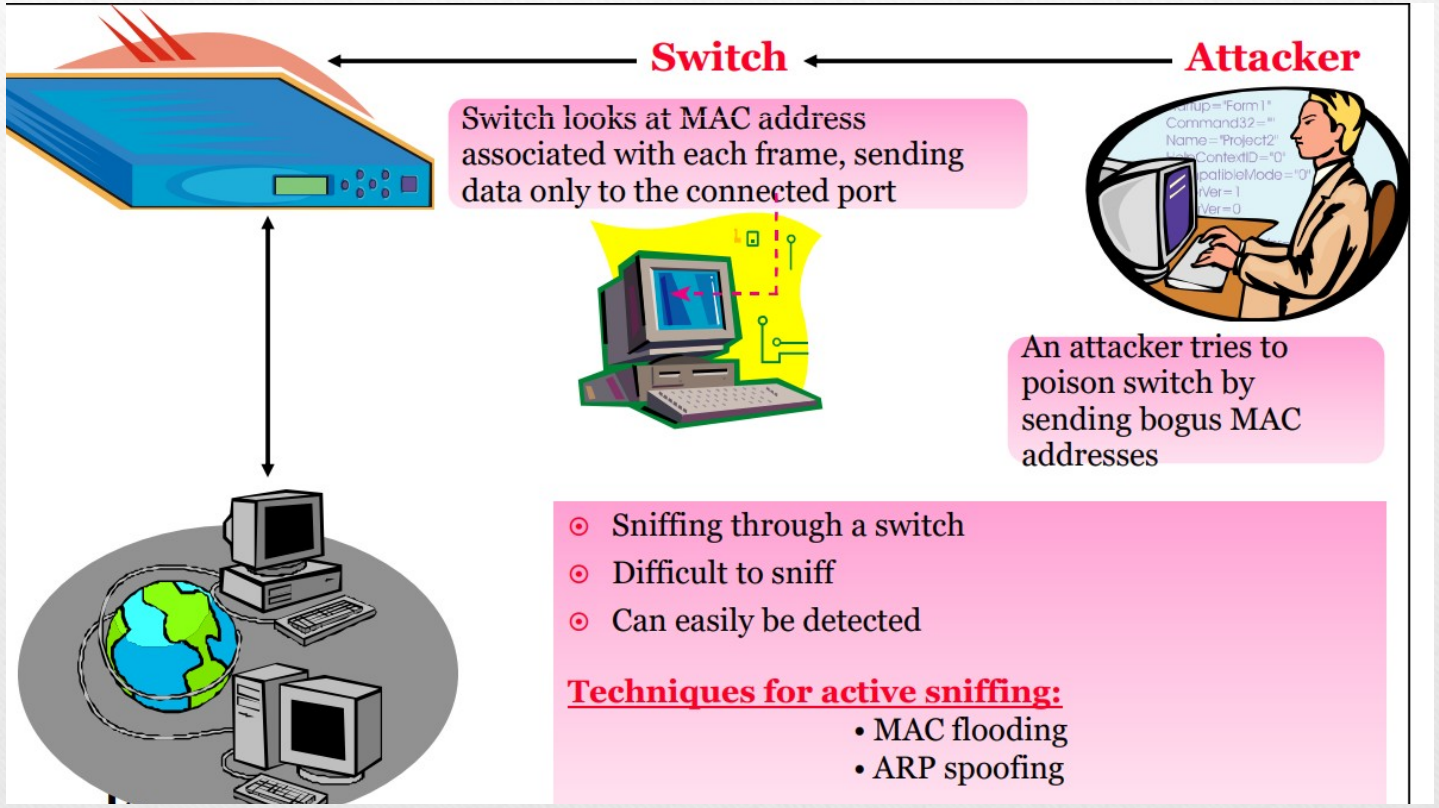


It is called passive because it is difficult to detect

"Passive sniffing" means sniffing through a hub

An attacker simply connects the laptop to the hub and starts sniffing

ACTIVE SNIFFING



Dude Sniffers

Developed by Mikro Tik, the Dude network monitor is a new application which can improve the way you manage your network environment

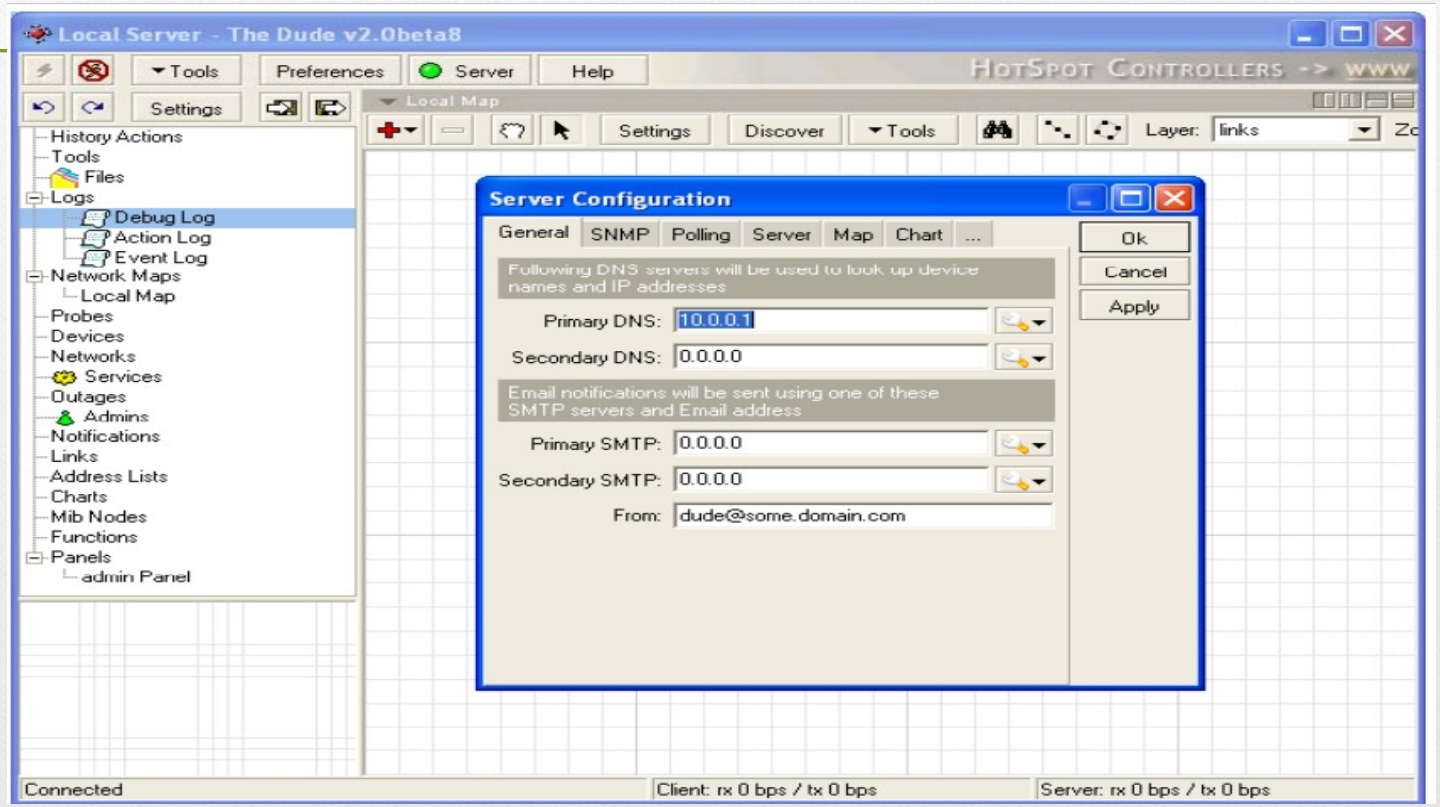
Functions:

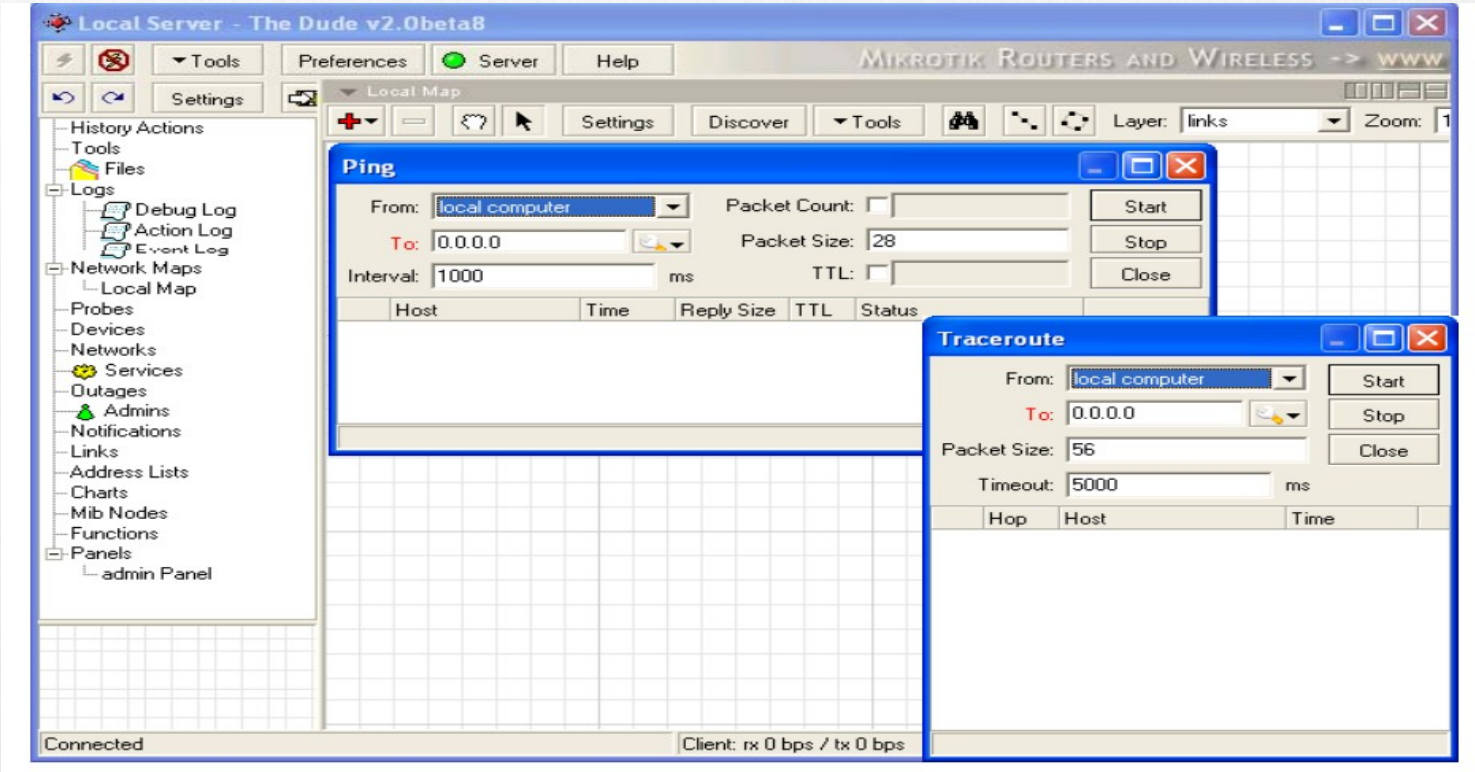
- Automatically scans all devices within the specified subr
- Draws and lays out a map of your networks
- Monitors services of your devices
- Alerts you in case some service has problems

It is written in two parts:

- Dude Server, which runs in a background
- Dude Client, which may connect to local or remote dude server

DUDE TOOLS


Local Server - The Dude v2.0beta8
Tools
Preferences
Server
Help
HotSpot Controllers -> www
Settings
Local Map
Settings
Discover
Tools
Layer:
links
History Actions
Tools
Files
Logs
Debug Log
Action Log
Event Log
Network Maps
Local Map
Probes
Devices
Networks
Services
Outages
Admins
Notifications
Links
Address Lists
Charts
Mib Nodes
Functions
Panels
admin Panel
Server Configuration
General
SNMP
Polling
Server
Map
Chart
...
Ok
Cancel
Apply
Following DNS servers will be used to look up device names and IP addresses
Primary DNS:
10.0.0.1
Secondary DNS:
0.0.0.0
Email notifications will be sent using one of these SMTP servers and Email address
Primary SMTP:
0.0.0.0
Secondary SMTP:
0.0.0.0
From:
dude@some.domain.com
Connected
Client: rx 0 bps / tx 0 bps
Server: rx 0 bps / tx 0 bps

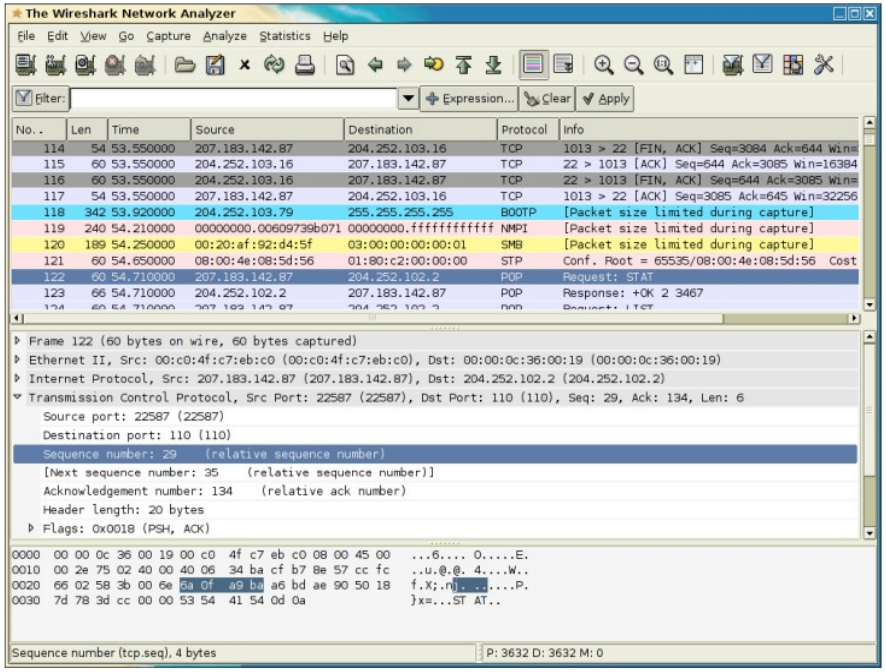

Local Server - The Dude v2.0beta8
Tools
Preferences
Server
Help
MIKROTIK ROUTERS AND WIRELESS -> WWW
Settings
Local Map
Settings
Discover
Tools
Layer:
links
Zoom:
History Actions
Tools
Files
Logs
Debug Log
Action Log
Event Log
Network Maps
Local Map
Probes
Devices
Networks
Services
Outages
Admins
Notifications
Links
Address Lists
Charts
Mib Nodes
Functions
Panels
admin Panel
Ping
From:
local computer
To:
0.0.0.0
Interval:
1000
ms
Packet Count:
Packet Size:
28
TTL:
Start
Stop
Close
Host
Time
Reply Size
TTL
Status
Traceroute
From:
local computer
To:
0.0.0.0
Packet Size:
56
Timeout:
5000
ms
Start
Stop
Close
Hop
Host
Time
Connected
Client: rx 0 bps / tx 0 bps

WIRESHARK

Wireshark is a network protocol analyzer for UNIX and Windows

It allows user to examine data from a live network or from a capture file on a disk

User can interactively browse captured data, viewing summary, and detailed information for each packet captured



Display Filters in Wireshark

Display filters are used to change the view of packets in captured files

Display Filtering by Protocol

- Example: Type the protocol in the filter box
- arp, http, tcp, udp, dns

Filtering by IP Address

•ip.addr == 10.0.0.4

Filtering by multiple IP Addresses

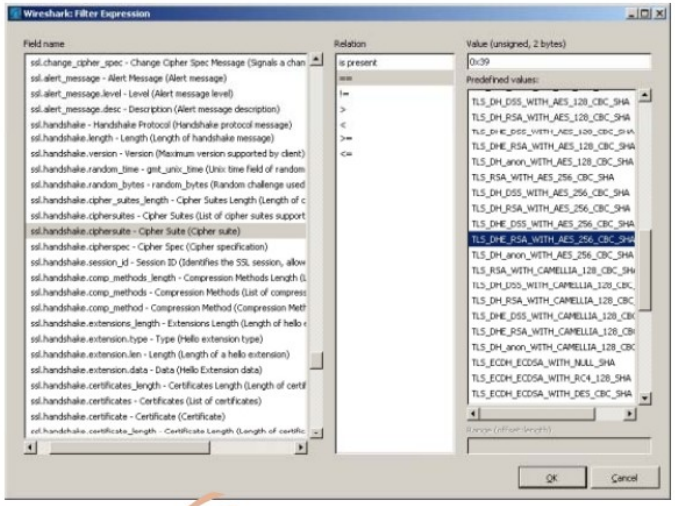
•ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5

Monitoring Specific Ports

•tcp.port==443
•ip.addr==192.168.1.100 machine
ip.addr==192.168.1.100 && tcp.port=443

Other Filters

•ip.dst == 10.0.1.50 && frame.pkt_len > 400
•ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30
•ip.src==205.153.63.30 or ip.dst==205.153.63.30



TCP Stream in Wireshark

Wireshark reassembles all packets in a TCP conversation and displays ASCII in an easy-to-read format

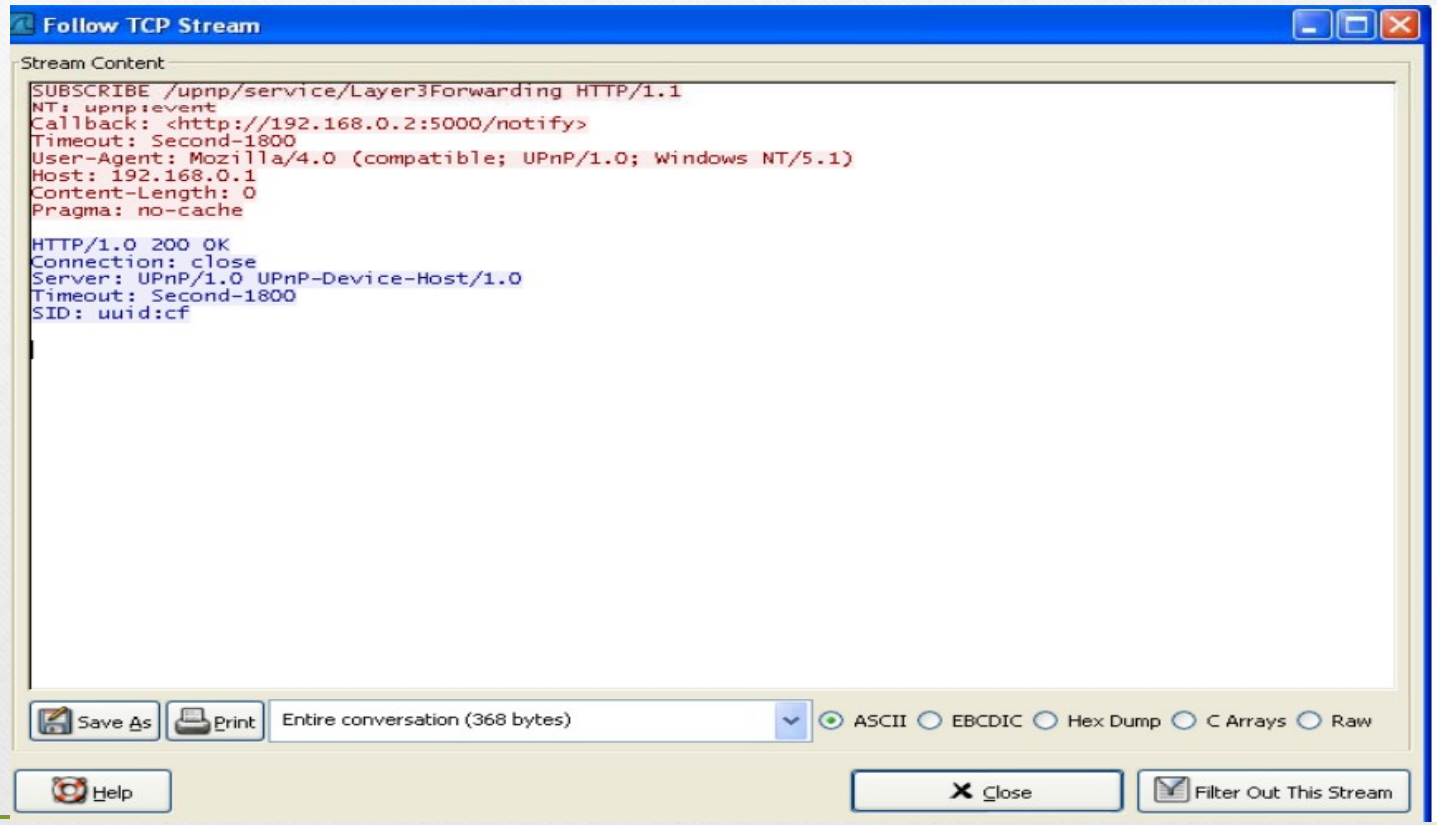
This makes it easy to pick out usernames and passwords from the insecure protocols such as Telnet and FTP

Example: Follow the stream of HTTP session and save the output to a file.

Command: Selecting a TCP packet in Summary Window and then selecting **`Analyze -> Follow TCP Stream`** from menu bar will display "Follow TCP Stream window"

You can also right-click on a TCP packet in Summary Window and choose "Follow TCP Stream" to display window

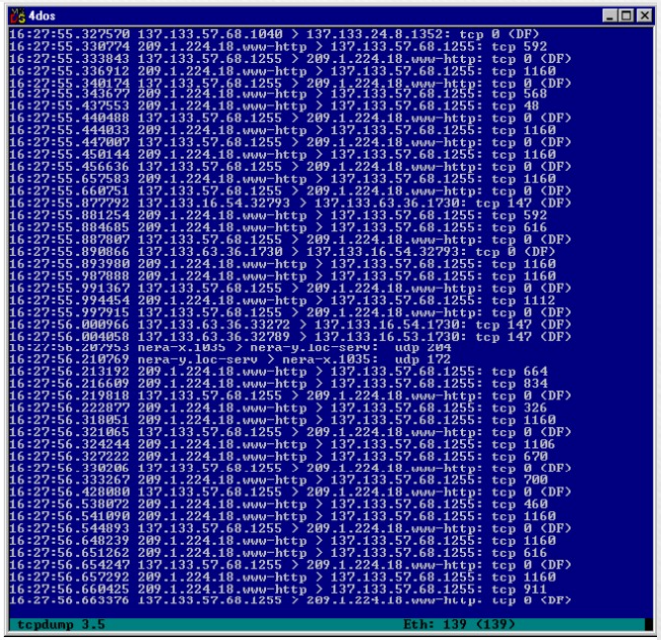
TCP Streaming



TCP dump commands

Tcpdump is a common computer network debugging tool that runs under command line

It allows user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached



TCP dump commands

Exporting tcpdumps to a file

- `# tcpdump port 80 -l > webdump.txt & tail -f webdump.txt`
- `# tcpdump -w rawdump`
- `# tcpdump -r rawdump > rawdump.txt`
- `# tcpdump -c1000 -w rawdump`
- `# tcpdump -i eth1 -c1000 -w rawdump`

Captures traffic on a specific port

- `# tcpdump port 80`

You can select several hosts on your LAN and capture the traffic that passes between them

- `# tcpdump host workstation4 and workstation11 and workstation12`

TCP dump Commands Cont..

Capture all the LAN traffic between workstation4 and the LAN, except for workstation11

- # tcpdump -e host workstation4 and workstation11 and workstation13

Capture all packets except those for certain ports

- # tcpdump not port 110 and not port 25 and not port 53 and not port 22

Filter by protocol

- # tcpdump udp
- # tcpdump ip proto OSPFIGP

Capture traffic on a specific host and restrict by protocol

- # tcpdump host server02 and ip
  # tcpdump host server03 and not udp
  # tcpdump host server03 and ip and igmp and not udp

Linux Sniffing Tools

Linux Sniffing Tools (cont'd)

sshmitm
- SSH monkey-in-the-middle

tcpkill
- Kills TCP connections on a LAN

tcpnice
- Slows down TCP connections on a LAN

urlsnarf
- Sniffs HTTP requests in Common Log Format

webspy
- Displays sniffed URLs in Netscape in real time

webmitm
- HTTP/HTTPS monkey-in-the-middle

Sniffing Atools

Sniffer hacking tools (These tools are available on the Lin

arpspoof
- Intercepts packets on a switched LAN

dnsspoof
- Forges replies to DNS address and pointer queries

dsniff
- Password sniffer

filesnarf
- Sniffs files from NFS traffic

mailsnarf
- Sniffs mail messages in Berkeley mbox format

msgsnarf
- Sniffs chat messages

How to Detect Sniffing

You will need to check which machines are running in promiscuous mode

Run ARPWATCH and notice if the MAC address of certain machines has changed (Example: router's MAC address)

Run network tools like HP OpenView and IBM Tivoli network health check tools to monitor the network for strange packets

Countermeasures

Restriction of physical access to network media ensures that a packet sniffer cannot be installed

The best way to be secured against sniffing is to use encryption. It would not prevent a sniffer from functioning but will ensure that what a sniffer reads is not important

ARP Spoofing is used to sniff a switched network, so an attacker will try to ARP spoof the gateway. This can be prevented by permanently adding the MAC address of the gateway to the ARP cache

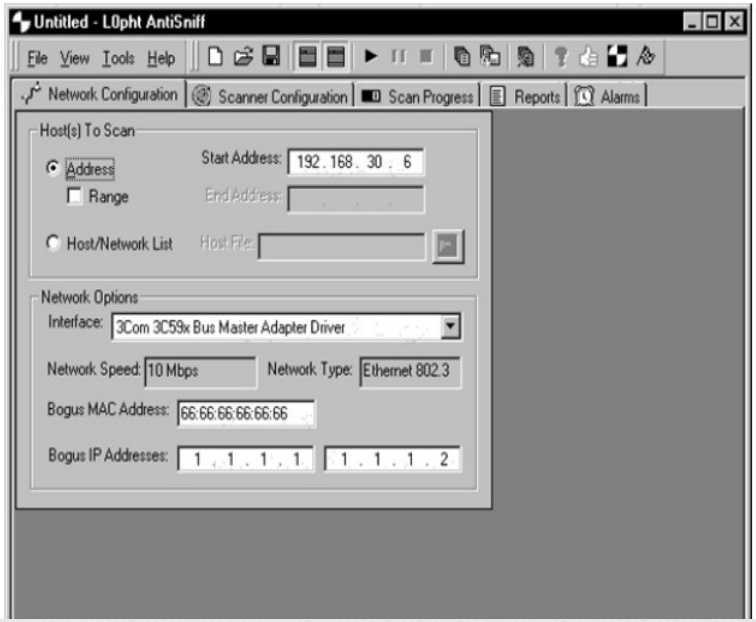
Countermeasures

There are various tools to detect a sniffer in a network:

- ARP Watch
- Promiscan
- Antisniff
- Prodetect

Anti-sniff Tool

AntiSniff tool can detect machines on the network that are running in the promiscuous mode



- Question ? Please