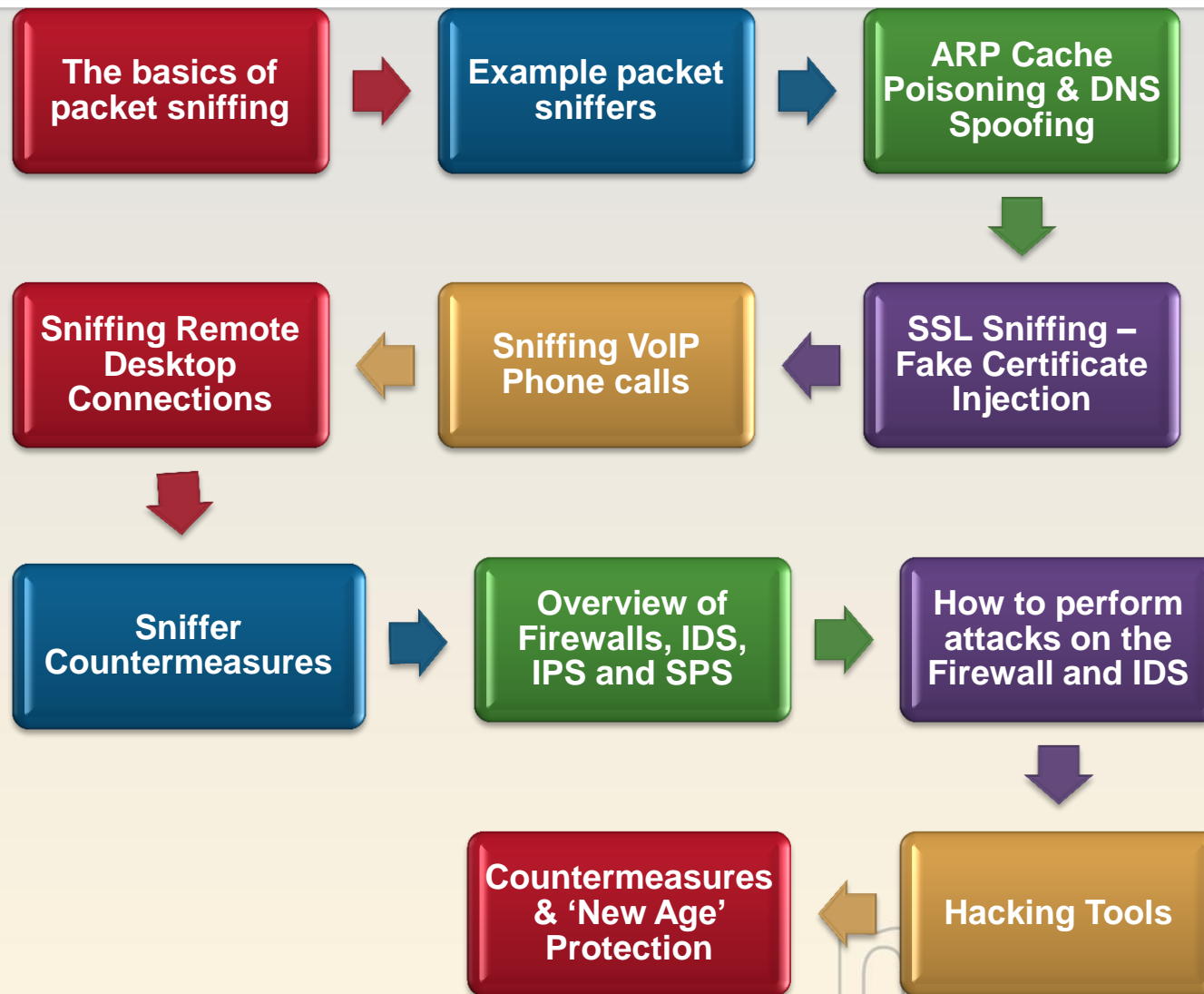


Networks, Sniffing and IDS



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.



WinPcap

Tool: Wireshark

VMware Accelerated AMD PCNet Adapter (Microsoft's Packet Scheduler) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
60	3.913148	192.168.42.104	224.0.0.22	IGMP	V3 Membership Report / Join group 2
61	3.913705	192.168.42.104	239.255.255.250	UDP	Source port: 53477 Destination port: 53477
62	3.924230	192.168.42.121	224.0.0.22	IGMP	V3 Membership Report / Join group 2
63	3.925551	192.168.42.104	224.0.0.22	IGMP	V3 Membership Report / Join group 2
64	3.963086	HonHaiPr_1e:57:07	Broadcast	ARP	who has 192.168.42.1? Tell 192.168.42.1
65	3.963662	Cisco-Li_39:8d:ed	HonHaiPr_1e:57:07	ARP	192.168.42.1 is at 00:18:f8:39:8d:ed
66	3.996573	192.168.42.121	224.0.0.252	LLMNR	Standard query ANY JMS-6400
67	3.996737	192.168.42.104	224.0.0.252	LLMNR	Standard query ANY JMS-6400
68	4.069675	192.168.42.117	208.73.181.192	TCP	csvr-sslproxy > hpvrtgrp [ACK] Seq: 3191, Win: 0, Len: 0
69	4.139297	208.73.181.192	192.168.42.117	TCP	[TCP ACKed lost segment] hpvrtgrp
70	4.144232	192.168.42.121	239.255.255.250	UDP	Source port: 53477 Destination port: 53477
71	4.144950	192.168.42.104	239.255.255.250	UDP	Source port: 53477 Destination port: 53477
72	4.196000	192.168.42.117	255.255.255.255	UDP	Source port: 1028 Destination port: 1028

Frame 68 (66 bytes on wire, 66 bytes captured)

Ethernet II, Src: Tivo_21:c1:66 (00:11:d9:21:c1:66), Dst: Cisco-Li_39:8d:ed (00:18:f8:39:8d:ed)

Internet Protocol, Src: 192.168.42.117 (192.168.42.117), Dst: 208.73.181.192 (208.73.181.192)

Transmission Control Protocol, Src Port: csvr-sslproxy (3191), Dst Port: hpvrtgrp (5223), Seq: 1, Ack: 1, Len: 0

Source port: csvr-sslproxy (3191)

Destination port: hpvrtgrp (5223)

[Stream index: 4]

Sequence number: 1 (relative sequence number)

Acknowledgement number: 1 (relative ack number)

Header length: 32 bytes

Flags: 0x10 (ACK)

0... .. = Congestion window Reduced (CWR): Not set

0... .. = ECN-Echo: Not set

..0. = Urgent: Not set

...1 = Acknowledgement: set

0000 00 18 f8 39 8d ed 00 11 d9 21 c1 66 08 00 45 00 ...9.... !.f..E.

0010 00 34 2b 0f 40 00 06 9e 8d c0 a8 2a 75 d0 49 ...4+..@..*u..I

0020 b5 c0 0c 77 14 67 ff cb 77 ac 45 4f e7 9a 80 10 ...w.g.. w.EO..

0030 1f 95 6e 7a 00 00 01 01 08 0a 06 9b 07 8b 79 a4 ...nz.... ..y.

0040 2a 7b *{

Header Length (tcp.hdr_len), 1 byte

Packets: 119 Displayed: 119 Marked: 0 Dropped: 0

Profile: Default

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

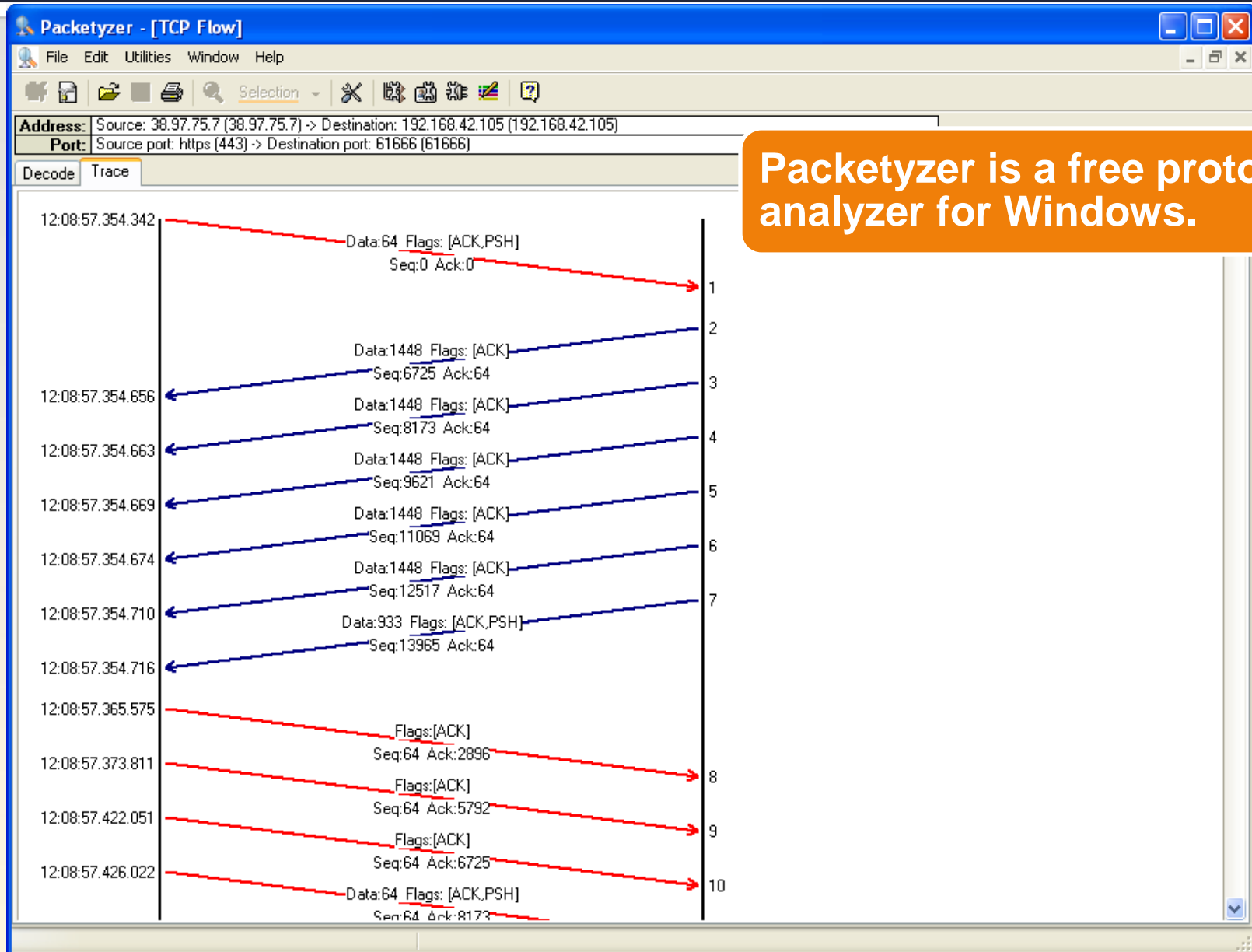
TCP Stream Re-assembling

The image displays the Wireshark network protocol analyzer interface. The main packet list shows a series of TCP segments from 192.168.42.105 to 38.97.75.7. A context menu is open over packet 7067, with 'Follow TCP Stream' highlighted. A red arrow points from this menu item to the 'Follow TCP Stream' dialog box. This dialog shows the raw data of the selected TCP stream, which appears to be a Base64-encoded string. The 'Raw' output format is selected at the bottom of the dialog.

Wireshark can re-create any TCP session.

© Mile2 All rights reserved.

Tool: Packetyzer



Packettyzer is a free protocol analyzer for Windows.

tcpdump & windump

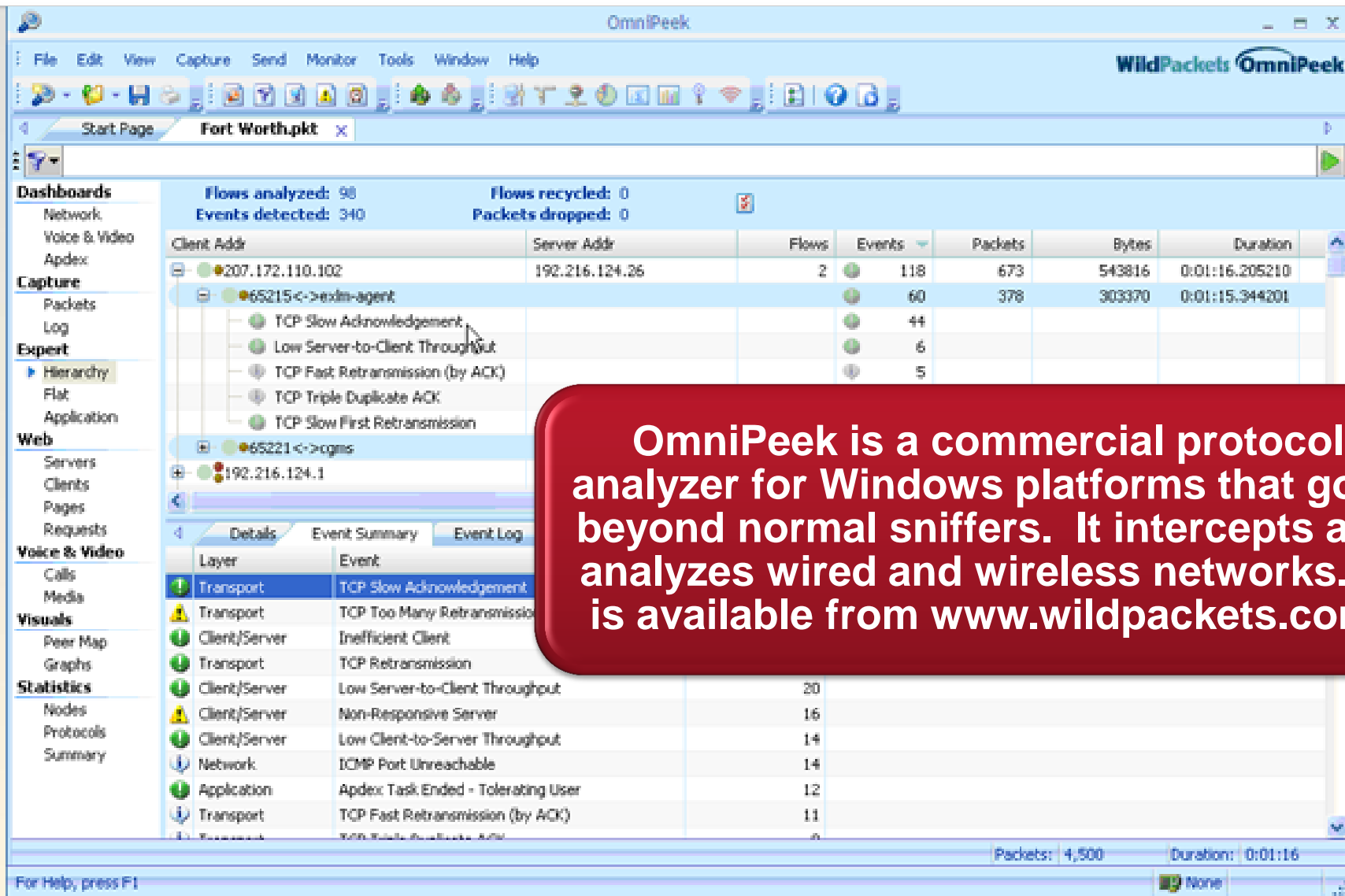
- **Tcpdump** is a popular Unix protocol analyzer, it prints out the headers of packets on a network interface that match the specified boolean expression.

```
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



The screenshot displays the OmniPeek application window. The top menu bar includes File, Edit, View, Capture, Send, Monitor, Tools, Window, and Help. Below the menu is a toolbar with various icons. The main window is titled 'Fort Worth.pkt'. On the left, a sidebar contains a 'Dashboards' section with links to Network, Voice & Video, and Apex. Below this is a 'Capture' section with links to Packets, Log, and Expert. The 'Expert' section is further divided into Hierarchy, Flat, and Application views. The 'Web' section includes Servers, Clients, Pages, and Requests. The 'Voice & Video' section includes Calls and Media. The 'Visuals' section includes Peer Map and Graphs. The 'Statistics' section includes Nodes, Protocols, and Summary. The main area shows a table of network flows and a list of events. A red callout box is overlaid on the right side of the interface.

Flows analyzed: 98
Events detected: 340
Flows recycled: 0
Packets dropped: 0

Client Addr	Server Addr	Flows	Events	Packets	Bytes	Duration
207.172.110.102	192.216.124.26	2	118	673	543816	0:01:16.205210
65215<->edm-agent			60	378	303370	0:01:15.344201
TCP Slow Acknowledgement			44			
Low Server-to-Client Throughput			6			
TCP Fast Retransmission (by ACK)			5			
TCP Triple Duplicate ACK						
TCP Slow First Retransmission						
65221<->ogms						
192.216.124.1						

Details | **Event Summary** | **Event Log**

Layer	Event	Count
Transport	TCP Slow Acknowledgement	20
Transport	TCP Too Many Retransmissions	16
Client/Server	Inefficient Client	14
Transport	TCP Retransmission	14
Client/Server	Low Server-to-Client Throughput	14
Client/Server	Non-Responsive Server	12
Client/Server	Low Client-to-Server Throughput	11
Network	ICMP Port Unreachable	11
Application	Apdex Task Ended - Tolerating User	11
Transport	TCP Fast Retransmission (by ACK)	11

Packets: 4,500 | Duration: 0:01:16

For Help, press F1

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	LAN5 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	LAN5 TECHNOLOGY CO., LTD.		*	*				*	

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

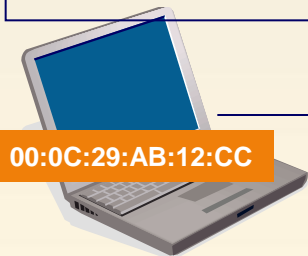
Tell 00:0C:29:AB:12:BB

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

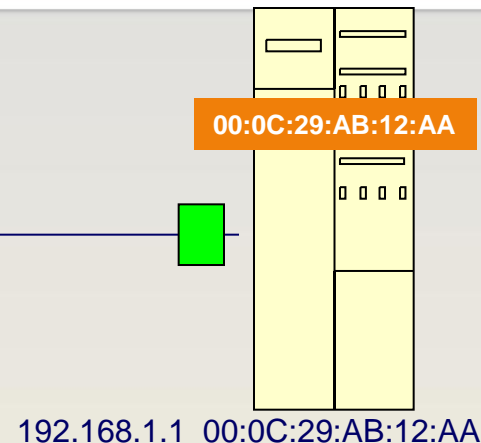
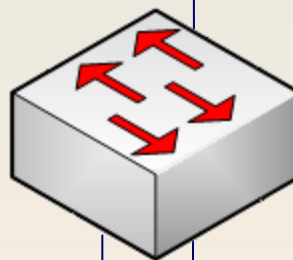
To: 00:0C:29:AB:12:BB

ARP Reply

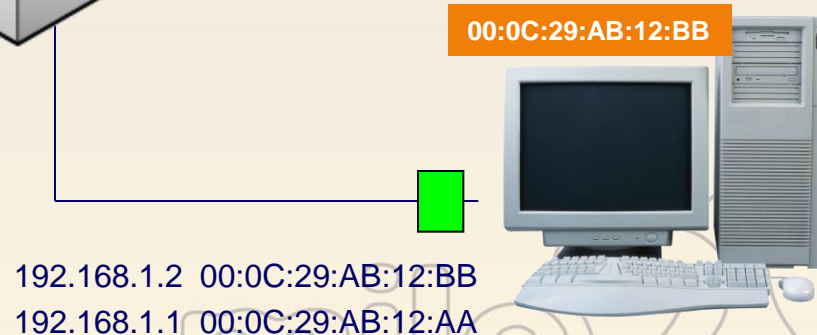
192.168.1.1 is at
00:0C:29:AB:12:AA



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

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

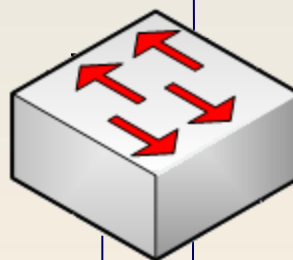
User-Andy176 Pass-Yhj28xg

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

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

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

Hacker



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

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

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

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
```


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](#)

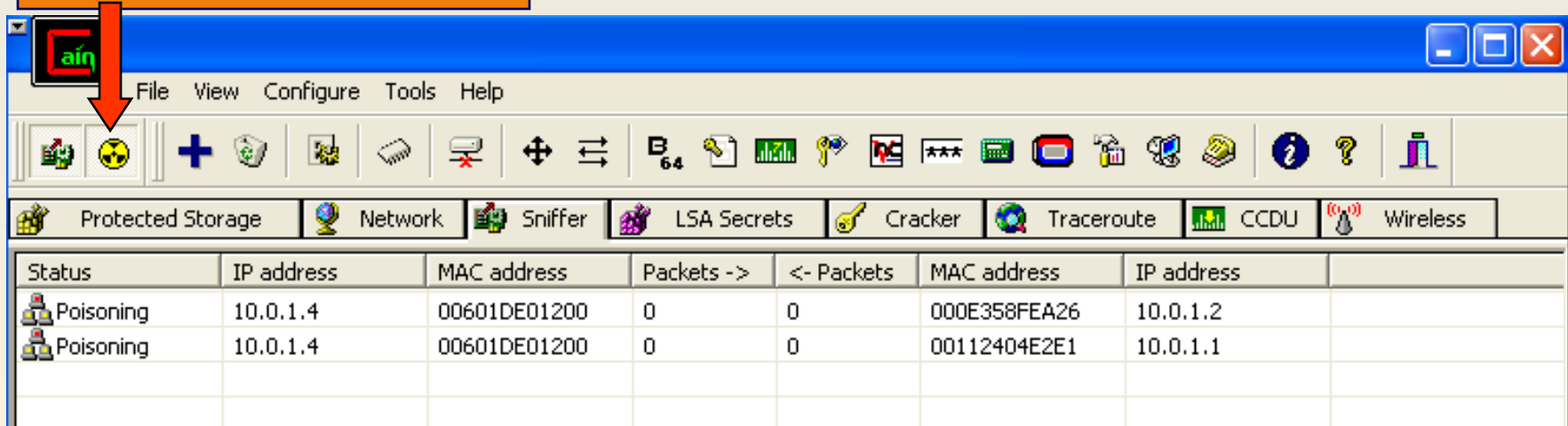


Tool: Cain and Abel

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

Start Targets Hosts View Mitm Filters Logging Plugins

Connections ✕ Profiles ✕

IP Address	Hostname
169.254.1.1	
169.254.1.30	
169.254.1.31	
X 213.140.2.█	
X 195.130.225.█	
169.254.1.40	

Purge Local
 Purge Remote

Unified sniffing was stopped.
 Starting Unified sniffing...

 POP : 213.140.2.32: █ -> USER: █ P
 POP : 195.130.225.172: █ -> USER: █
 POP : 213.140.2.32: █ -> USER: █

Start Targets Hosts View Mitm Filters Logging Plugins

Connections ✕

Host	Port	-	Host	Port	Proto	State	Bytes
64.12.24.190	5190	-	169.254.1.30	32917	TCP	idle	260
169.254.1.30	32905	-	207.46.107.58	1863	TCP	idle	13
169.254.1.30	32771	-	62.177.1.107	5222	TCP	idle	1

View Details
 Kill Connection

46 ports monitored
 6311 mac vendor fingerprint
 1542 tcp OS fingerprint
 2 known services
 Starting Unified sniffing...

 Unified sniffing was stopped.

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).

arp spoof, 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.

```
root@0[knoppix]# dsniff
dsniff: listening on eth0
-----
12/15/04 18:32:24 tcp 10.0.1.2.1038 -> 10.0.1.4.21 (ftp)
USER bigcheese
PASS pumpkin
```

NAME

dsniff - password sniffer

SYNOPSIS

```
dsniff [-c] [-d] [-m] [-n] [-i interface] [-s snaplen] [-f services]
[-t trigger[,...]] [-r|-w savefile] [expression]
```

DESCRIPTION

dsniff is a password sniffer which handles FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net, Sybase and Microsoft SQL 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.

```
root@0[knoppix]# webspay -i eth0 10.0.1.4
webspay: listening on eth0
openURL(http://66.102.7.99/)
```



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:

DNSspooof
(part of Dsniff
for Unix)

WinDNSspooof
(for Windows)

Cain and Abel
(for Windows)

DNS Hijacker
(for Unix)

Cain's DNS Spoofer

DNS Spoofer for APR

DNS Name Requested

www.cnn.com

IP address to rewrite in response packets

209 . 208 . 224 . 72

Resolve

OK

Cancel

DNSSPOOF(8)

NAME

dnsspoof - forge replies to DNS address / pointer queries

SYNOPSIS

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

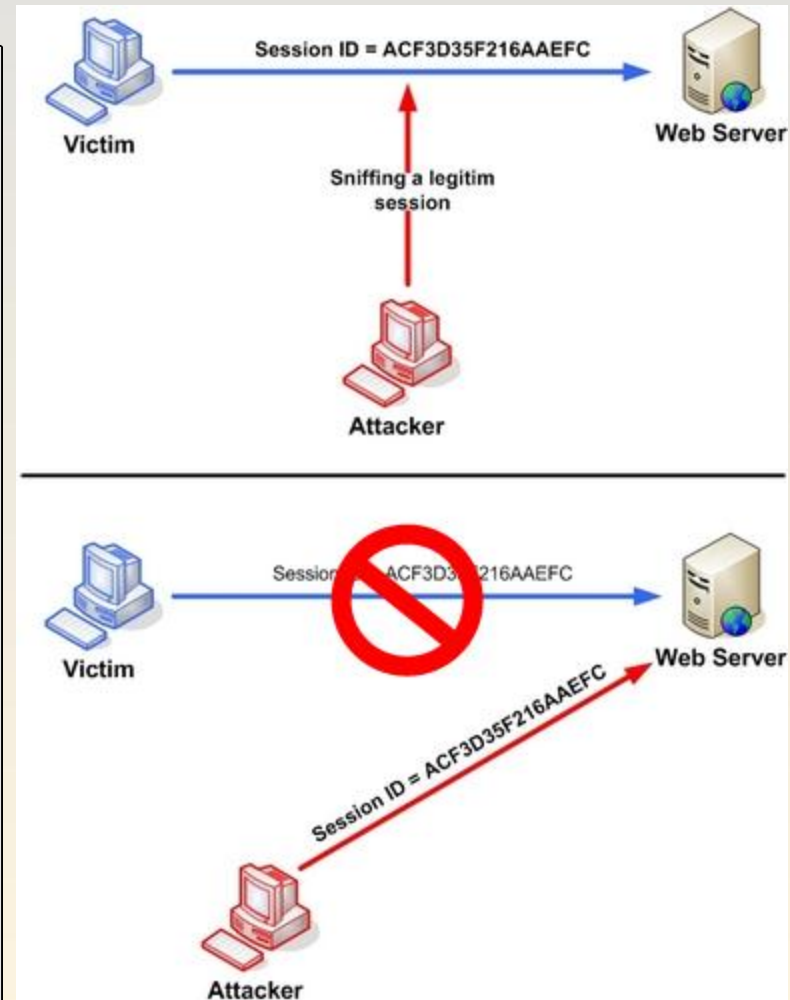
DESCRIPTION

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.

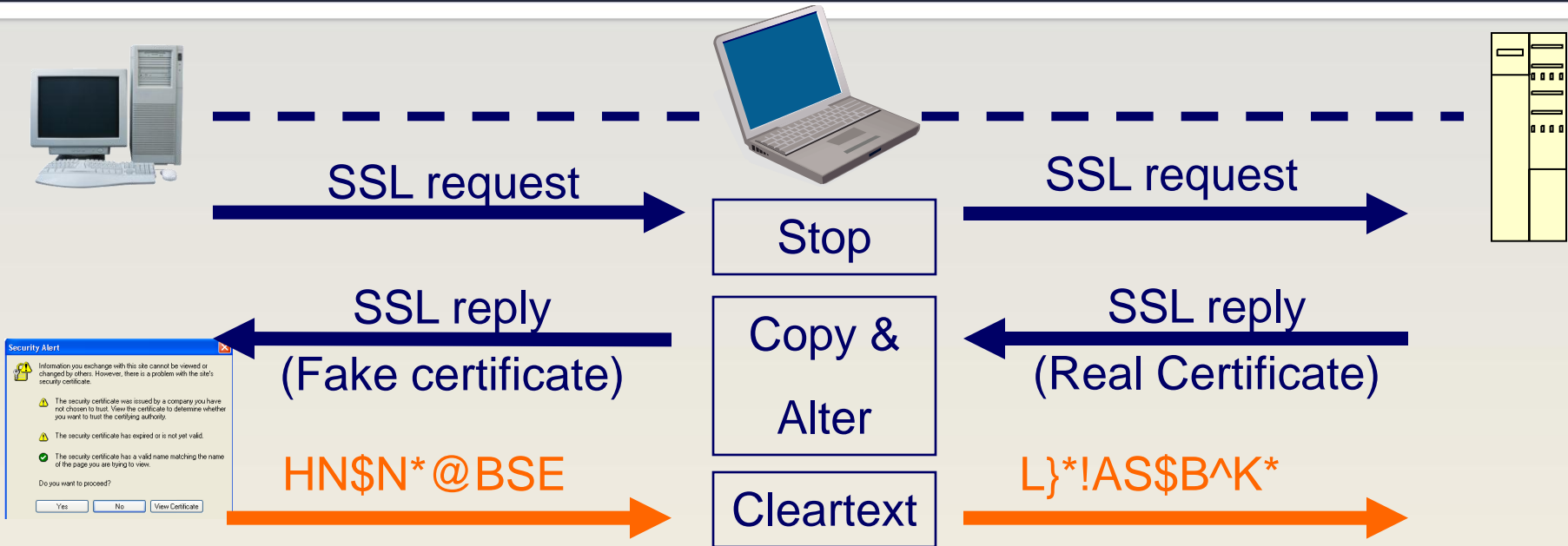
Session Hijacking

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 dnsspoofing SSH password logins, and optionally hijacking interactions. Only SSH protocol version 1 is (or ever will be) this program is far too evil already.

Security Alert



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.



The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.



The security certificate has expired or is not yet valid.



The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

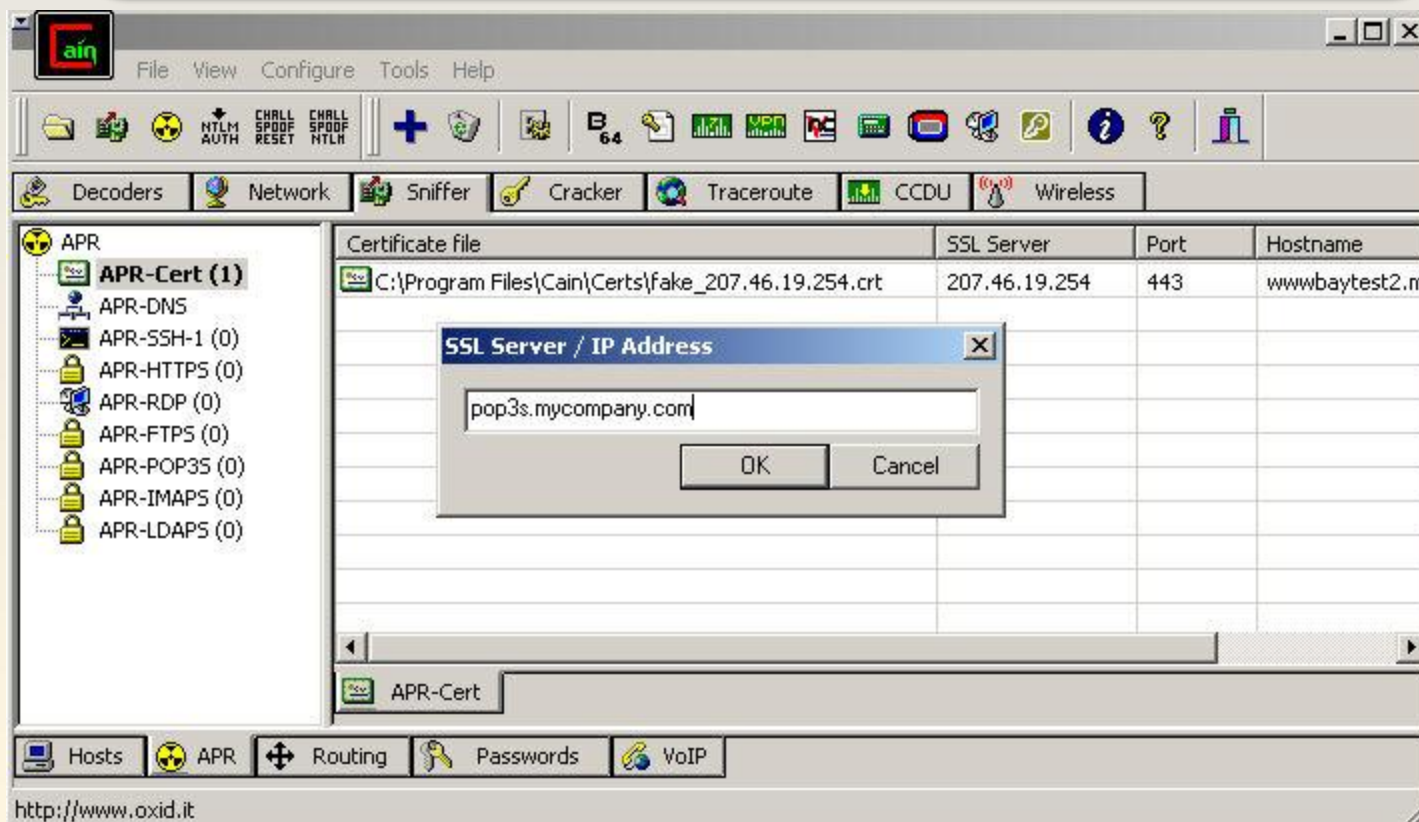
Yes

No

View Certificate

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.

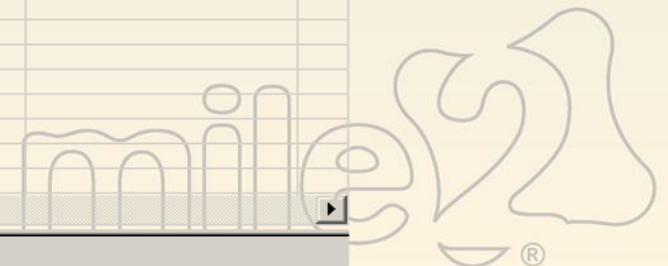
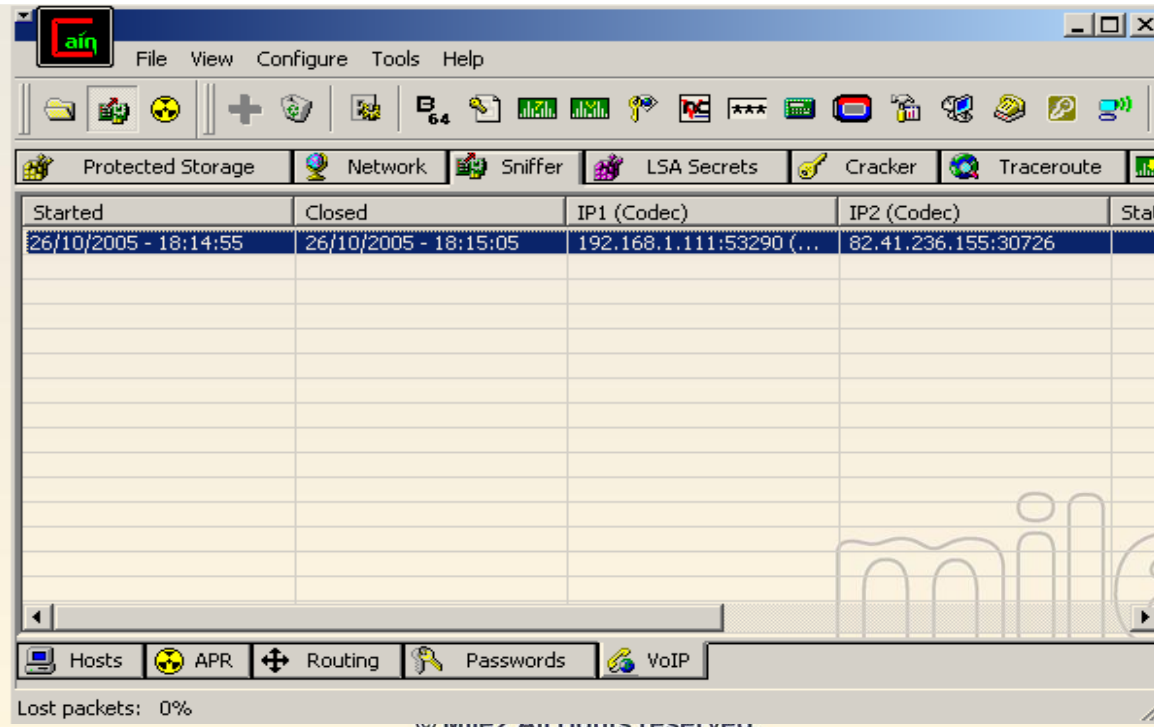
Voice over IP traffic may be deployed on any IP network, including ones lacking a connection to the rest of the Internet, for instance on a private building-wide LAN.

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)	eStera 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

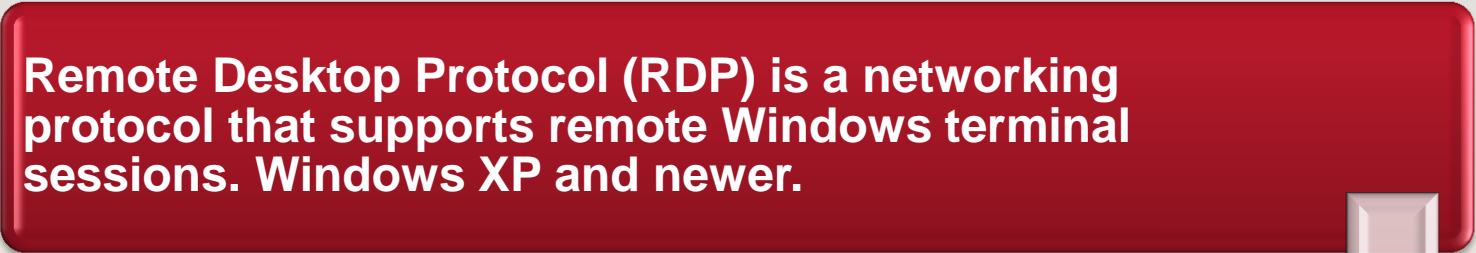
Cain & Abel is configured to intercept and decode VoIP traffic. Once decoded, C&A saves the file as a .wav ready for playback.

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.



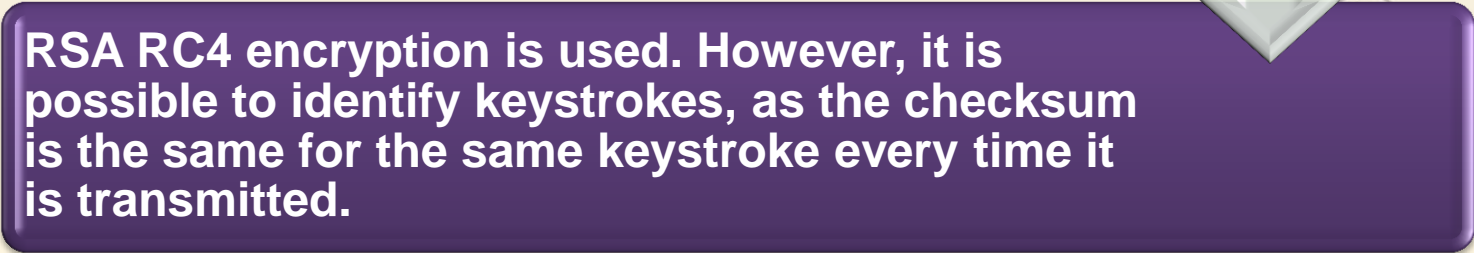
It transmits all of the information usually associated with a local console session - keystrokes, video and mouse data, and so forth.



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.

The screenshot shows the Cain & Abel network sniffing tool. On the left, a tree view shows the network topology with 'APR' as the root, containing 'APR-DNS', 'APR-SSH-1 (2)', 'APR-HTTPS (8)', and 'APR-RDP (3)'. The main window displays a table of captured RDP sessions:

Started	Closed	RDP server	Client	Status	Version	Enc.Level	Key size	Filename
01/07/2005 - 19:59:59	04/08/2005 - 14:43:31	192.168.9.208	192.168.9.164	Closed	RDPv4	medium	128 bit	RDP-2005...
20/10/2005 - 16:09:26	20/10/2005 - 16:10:13	192.168.0.129	192.168.0.159	Closed	RDPv4	medium	56 bit	RDP-2005...
20/10/2005 - 16:10:51	20/10/2005 - 16:11:33	192.168.0.129	192.168.0.159	Closed	RDPv4	medium	56 bit	RDP-2005...

Below the table, a Notepad window titled 'RDP-200571185959234.txt - Notepad' displays the following decrypted RDP traffic:

```
[client decrypted packet] - 12 bytes total; 2 bytes decrypted
0000 c4 0c 17 b8 0d bc 52 04 35 10 00 14          .....R.5...

Key pressed client-side: 0x14 - 't'

[server decrypted packet] - 92 bytes total; 82 bytes decrypted
0000 c0 5c 6e 8a d2 3b ea 4f 09 ba 1d e5 c4 60 fb 93  .\n...;o.....`..
0050 e6 c3 cd 2d 55 84 71 a8 5d ce 28 34          ...-U.q.].(4

Key released client-side: 0x14 - 't'

[client decrypted packet] - 12 bytes total; 2 bytes decrypted
0000 c4 0c 82 3d 07 58 47 0d c1 2f 01 36          ...=.XG../.6

Key released client-side: 0x36 - 'right shift'

[client decrypted packet] - 12 bytes total; 2 bytes decrypted
0000 c4 0c 36 cb 47 86 4f 4f 64 d0 00 23          ..6.G.ood...#
```


Routing Protocols Analysis

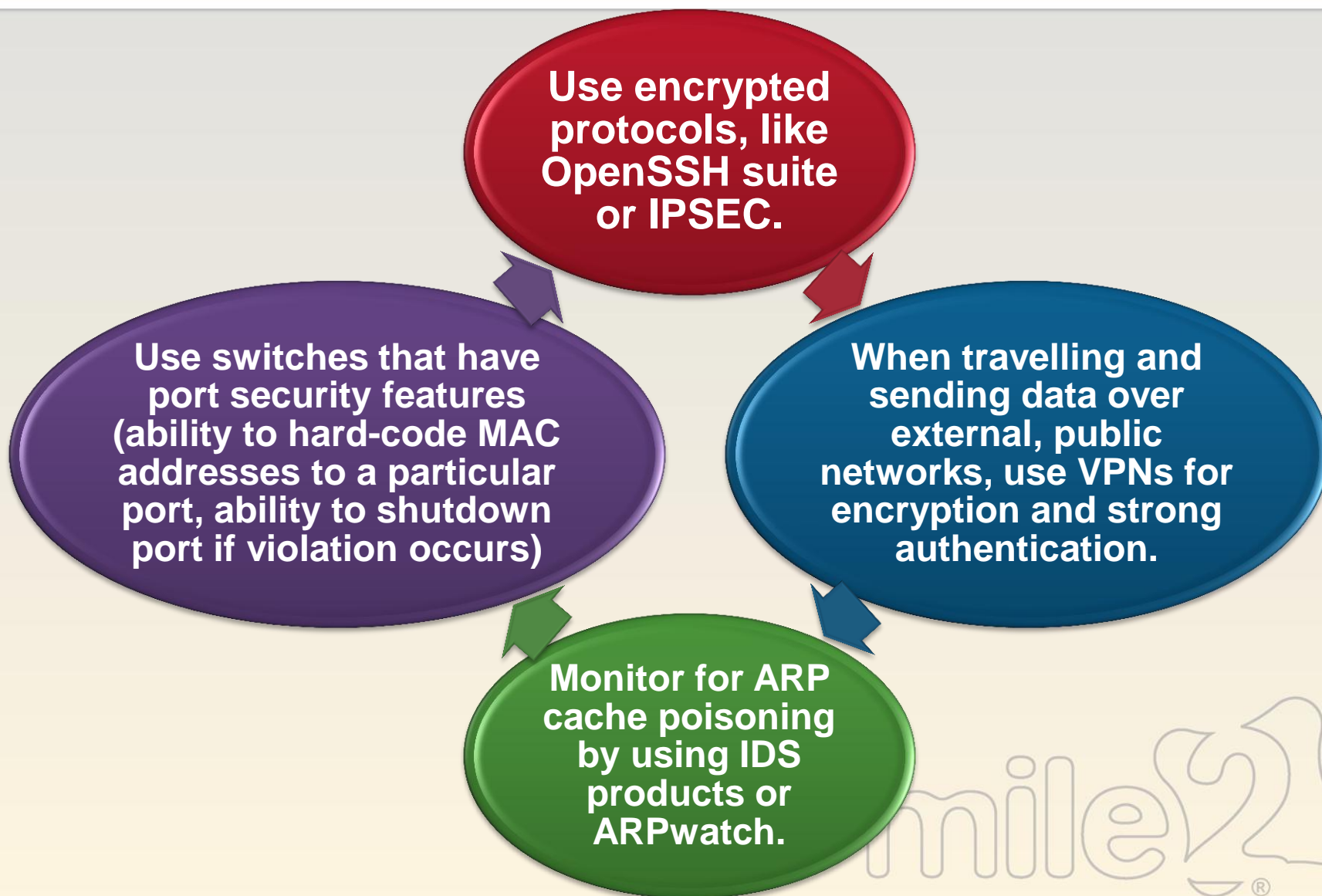
Routing protocols like VRRP, HSRP, RIP, OSPF, EIGRP are also analyzed by the program. This enables a quick identification of the subnet routing and perimeter.

Routing

Destination	Mask	Next Hop	Type	Source	Origin AS	Ext. Metric	Learned from	Bandwidth	Delay	F
10.13.1.0	255.255.255.0	0.0.0.0	External	10.49.1.2	0	0	Static	2560	256	2
10.13.11.0	255.255.255.0	0.0.0.0	External	10.49.1.2	0	0	Static	2560	256	2
10.13.12.0	255.255.255.0	0.0.0.0	External	10.49.1.2	0	0	Static	2560	256	2
10.13.13.0	255.255.255.0	0.0.0.0	External	10.49.1.2	0	0	Static	2560	256	2
10.13.14.0	255.255.255.0	0.0.0.0	External	10.49.1.2	0	0	Static	2560	256	2
10.14.1.0	255.255.255.0	0.0.0.0	External	10.49.1.2	0	0	Static	2560	256	2
10.20.0.0	255.255.0.0	0.0.0.0	External	10.49.1.2	0	0	Static	2560	256	2
10.50.0.0	255.255.0.0	0.0.0.0	External	10.49.1.2	0	0	Static	2560	256	2
10.70.0.0	255.255.0.0	0.0.0.0	External	10.49.1.2	0	0	Static	2560	256	2
10.90.0.0	255.255.0.0	0.0.0.0	External	10.49.1.2	0	0	Static	2560	256	2
10.91.0.0	255.255.0.0	0.0.0.0	External	10.49.1.2	0	0	Static	2560	256	2
10.254.254.136	255.255.255.248	0.0.0.0	External	10.49.1.2	0	0	Static	2560	256	2
10.49.0.0	255.255.252.0	10.40.254.253	Internal	10.40.254.253				2560	256	2
10.11.0.0	255.255.252.0	10.40.254.253	Internal	10.40.254.253				2560	256	2
10.42.0.0	255.255.0.0	10.40.254.253	Internal	10.40.254.253				2560	256	2
10.10.0.0	255.255.0.0	10.40.254.253	Internal	10.40.254.253				2560	256	2

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

Fragmented Packets



Evading IDS

**Fragmented
Packets**

**Malformed
Packets**

**Encrypted
Tunnels**



‘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.

F
I
R
E
W
A
L
L

Allow: 25, 53, 80, 443.

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

SYN – Port 21...

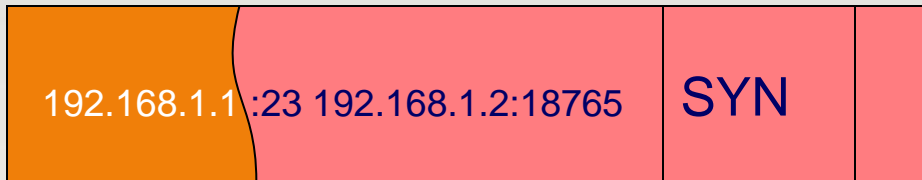
DENIED

STATE 192.168.1.1 - 192.168.1.2

UNAUTHORIZED



Evasive Technique -Example



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



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.**

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**



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



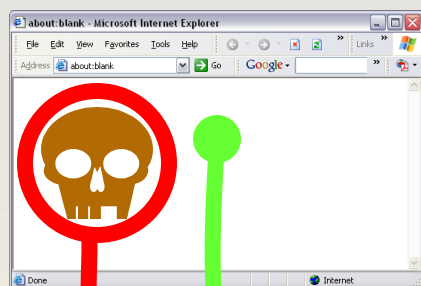
© Mile2. All rights reserved.

Spyware Prevention System (SPS)

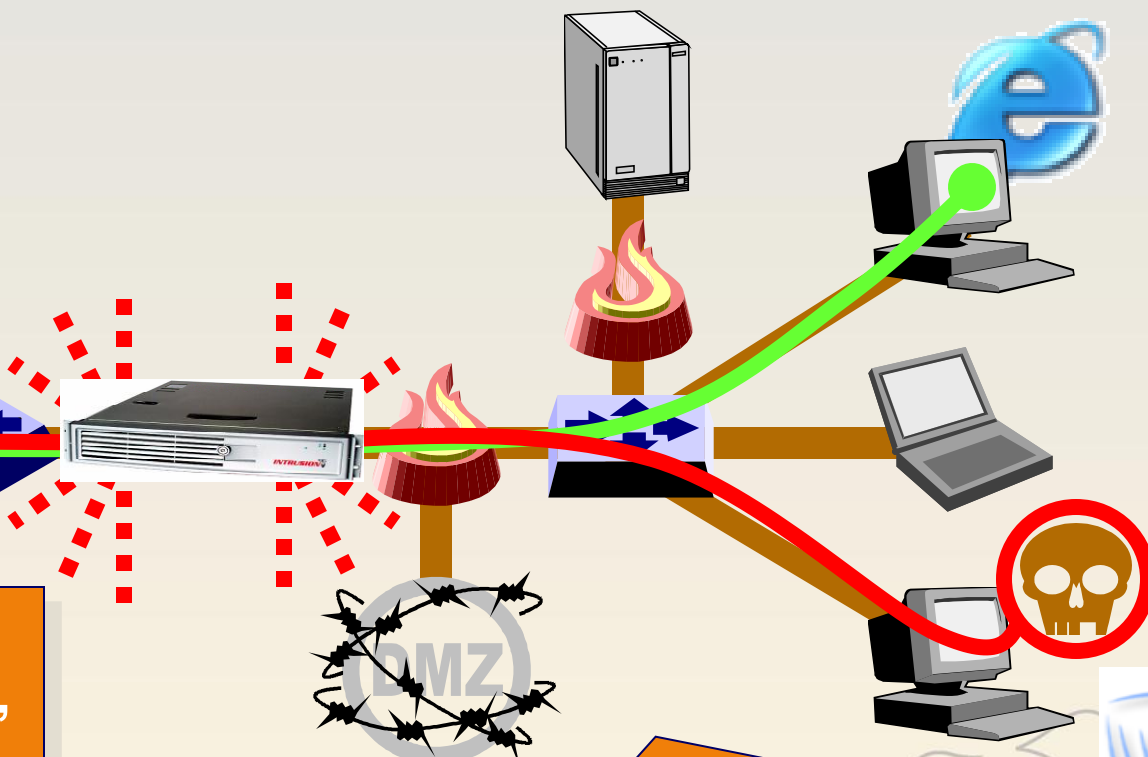


INTRUSION

SpySnare - <http://www.intrusion.com/>

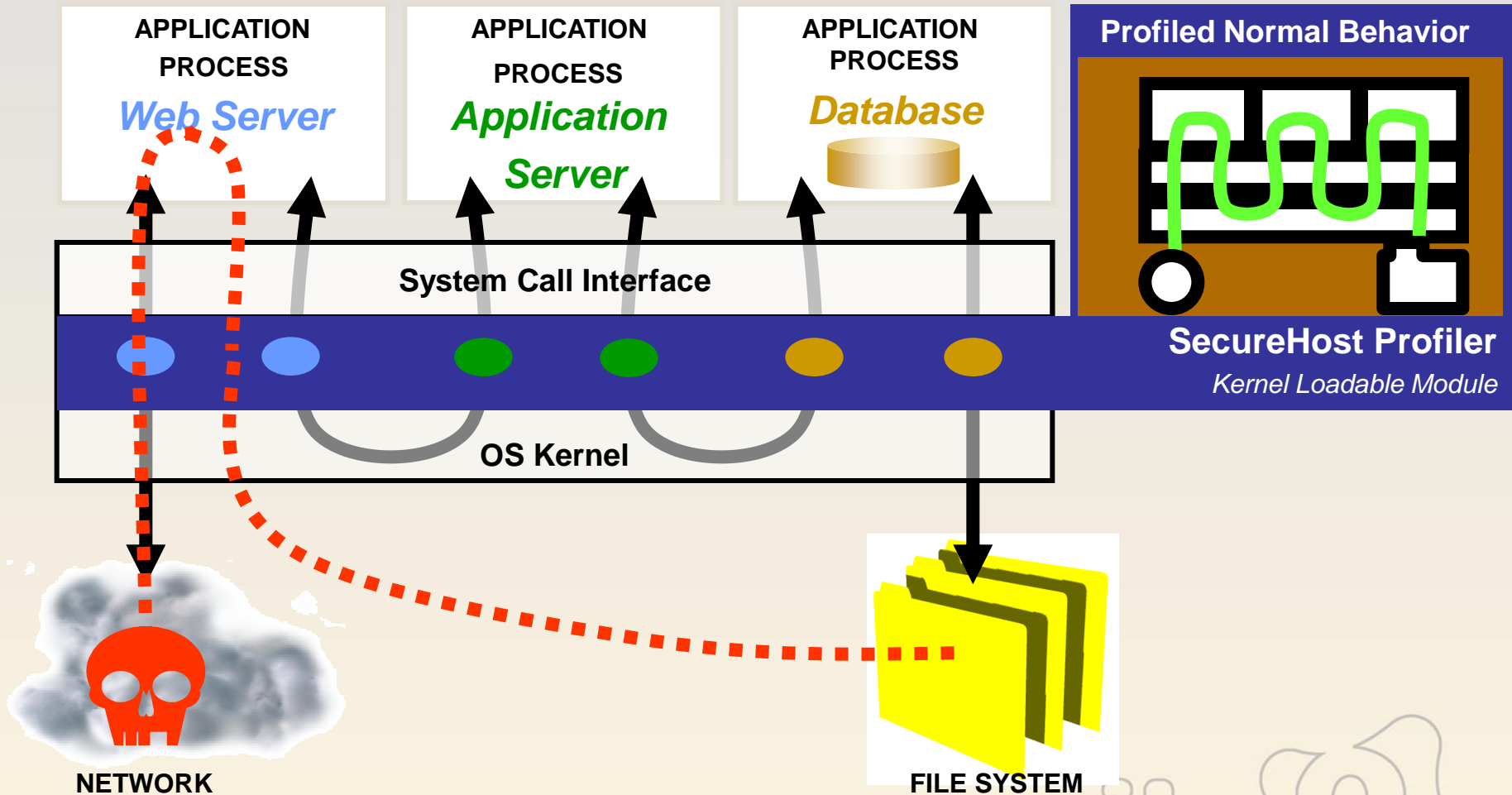


**Spyware injection,
even stealth injection,
blocked by SPS**



**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

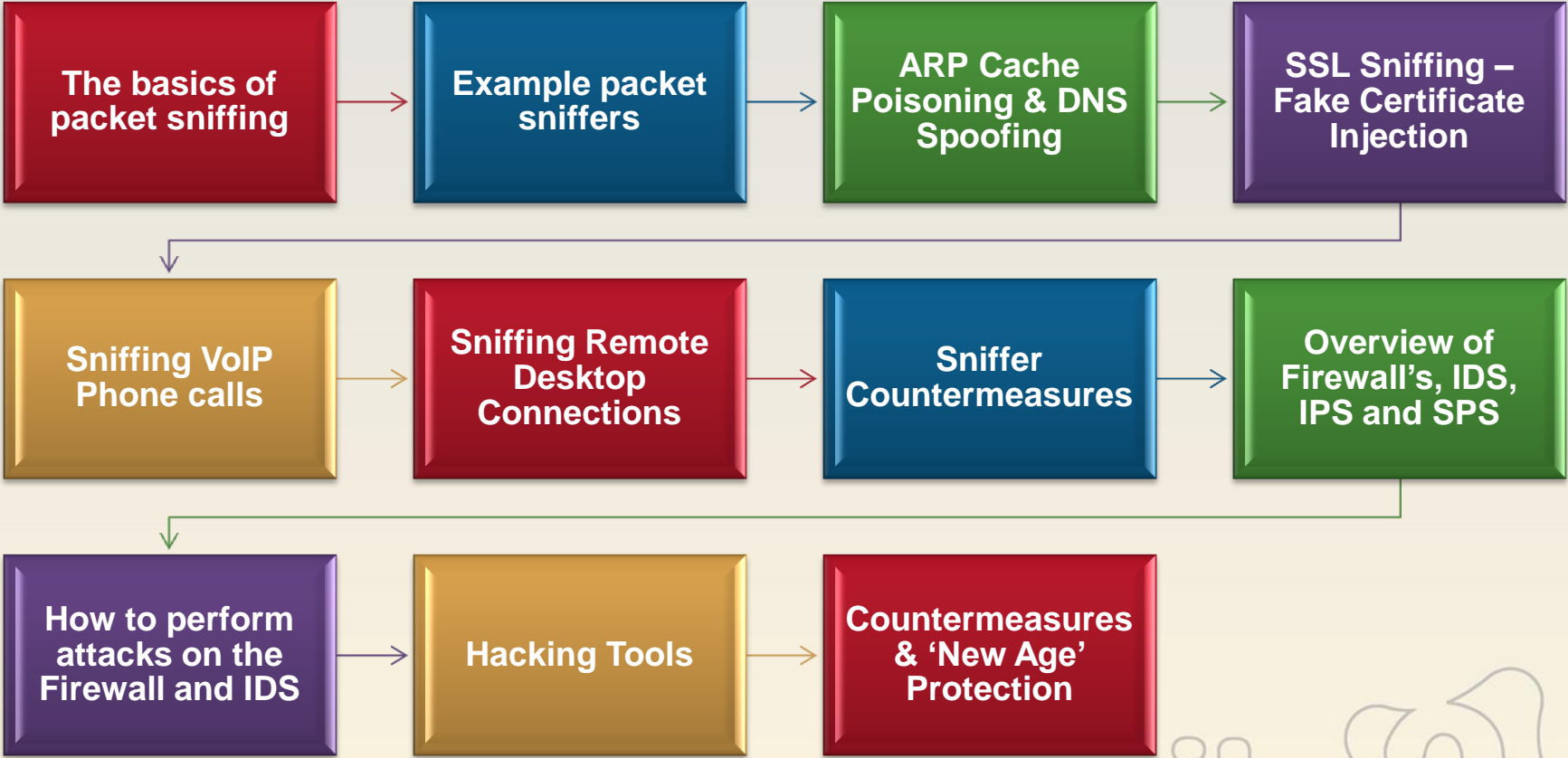
Injected code



Exploits create 'unexpected' code paths



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



Module 12 Lab

Networks-Sniffing-IDS

