

3 Analyse der Informationen und Auswertung von Schwachstellen

Webquellen:

<http://www.packetstormsecurity.org>

<http://www.2600.com>

<http://www.theregister.co.uk/content/55/16725.html>

Nessus, ISS Scanner

Empfehlenswerte Seite mit Tools: <http://www.networkintrusion.co.uk/scanners.htm>

wwwscan: a Perl script that scans Web servers for more than 800 known vulnerabilities

Many whitehat/blackhat Web sites provide information on vulnerabilities and associated exploits

<http://www.packetstormsecurity.org>

3.1 Herausfinden der verwendeten Betriebssysteme und -versionen

Ziel ist es, das auf einer aktiven IP-Adresse verwendete Betriebssystem (und dessen Version) herauszufinden.

OS detection helps attackers in tailoring exploits that target OS-specific vulnerabilities. Furthermore, attackers are also interested in server software (FTP, DNS, WWW...) that are running on live IPs.

„Banner Grabbing“:

Ein Angreifer könnte auch telnet verwenden, um eine Verbindung zu aktiven Ports herzustellen:

```
telnet 192.168.10.16 25
```

In diesem Beispiel wird versucht, eine Verbindung zu einem SMTP-Service herzustellen. Auf Grund des Banners, mit dem sich der Zieldienst meldet, lassen sich Rückschlüsse auf das verwendete Betriebssystem und den verwendeten Anwendungsserver machen.

Beispiel:

```
220 SRV01.firma.at Microsoft ESMTMP MAIL Service ready at Mon, 3 Nov
2008 15:44:50 +0100
```

Das obige Beispiel ist der Standardbanner eines Microsoft-ESMTMP-Servers (etwa Exchange 2003 oder Exchange 2007).

3.1.1 NMap

Nmap unterstützt auch die Versionserkennung des Zielbetriebssystems:

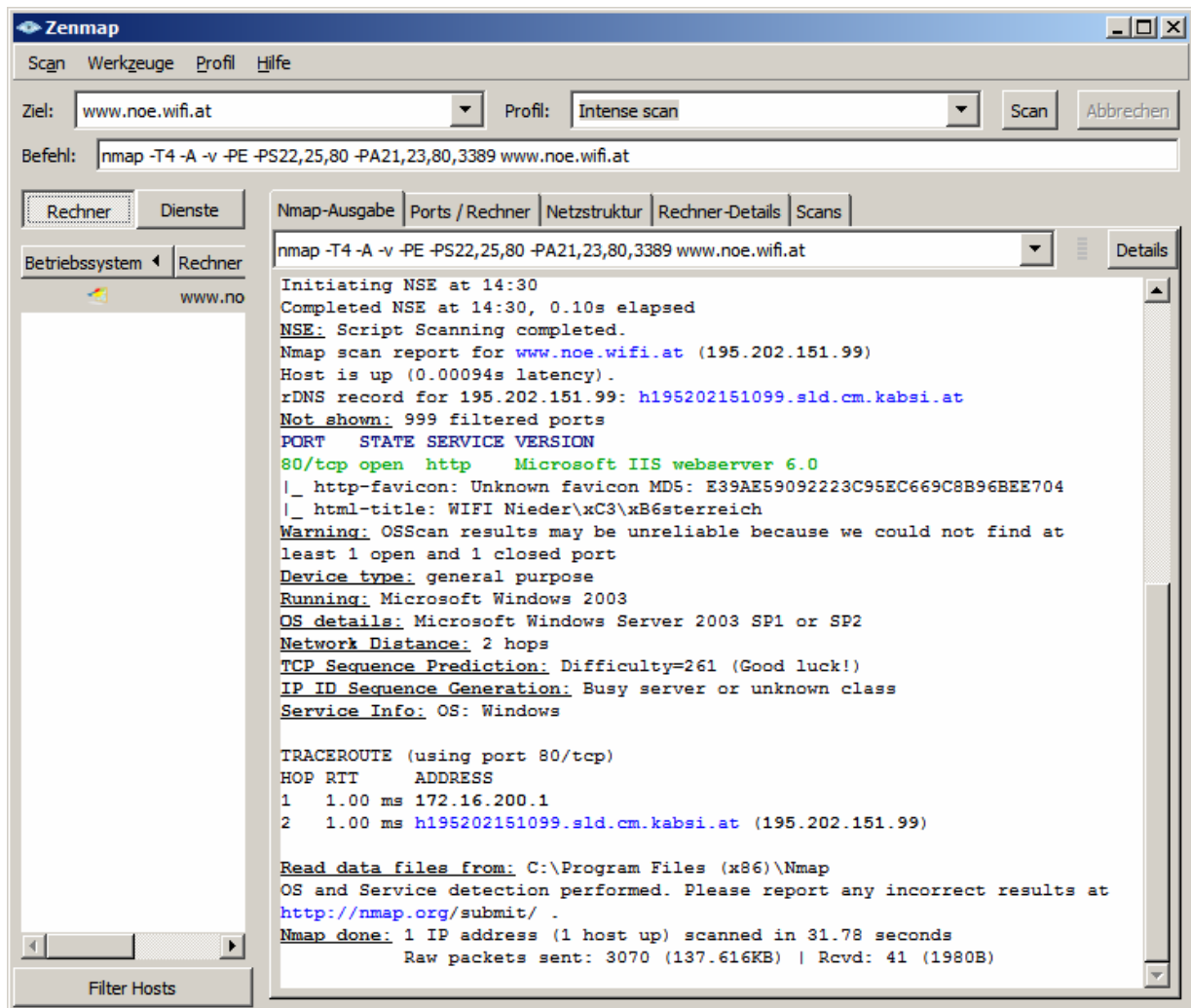
Beispiel:

```
nmap -sS -O victimIPaddress
```

NMAP verwendet dazu Unterschiede bei der Implementierung von TCP/IP, etwa:

- Windows 2000 sendet IP-Pakete mit der TTL=128, Linux verwendet hingegen TTL=64
- Die meisten TCP/IP-Implementierungen antworten nicht auf ein FIN-Paket, das an einen offenen TCP-Port gesendet wird; Windows NT antwortet hingegen.

In dem Moment, wo aktive IP-Adressen, offene TCP-/UDP-Ports und Betriebssystemversionen bekannt sind, wird ein Angreifer versuchen, die Schwachstellen dieser Systeme herauszufinden.



3.1.2 Nessus (UNIX)

Nessus ist ein bekannter Netzwerk- oder Vulnerability Scanner für Linux-, Unix- Windows- und OS X-systeme. Nessus basiert auf dem Client-Server-Prinzip. Das heißt, dass auf einem Rechner der Nessusserver (nessusd) gestartet wird und man sich anschließend mit einem oder mehreren Clients entweder vom lokalen oder einem entfernten Computer aus verbinden kann. Abgesichert wird dies durch SSL-Zertifikate und Passwörter.

Mit dem Start des Servers werden automatisch die Plug-ins geladen. Mit diesen Plug-ins lassen sich diverse Sicherheitslücken des Betriebssystems bzw. der Dienste, die auf dem zu scannenden Host laufen, finden. Die Plug-ins werden in der Nessus-eigenen Skriptsprache „Nessus Attack Scripting Language“ (NASL) erstellt.

Mit Hilfe des „Clients“ verbindet man sich darauf mit dem Server und stellt eine „Session“ ein, in welcher man die Plug-ins, den Zielhost und andere Einstellungen eintragen oder verändern kann. Wurde der Scan auf einen Host ausgeführt, gibt der Nessus-Client eine Übersicht über die offenen Ports (das Scannen der Ports macht Nessus mit nmap) und eventuell gefundene Sicherheitslücken aus.

3.2 Denial-of-Service-Attacken

Als Denial of Service (DoS, zu Deutsch etwa: Dienstverweigerung) bezeichnet man einen Angriff auf einen Host (Server) oder sonstigen Rechner in einem Datennetz mit dem Ziel, einen oder mehrere seiner

Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch Überlastung. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von Verteilter Dienstblockade bzw. DDoS (Distributed Denial of Service). Normalerweise werden solche Angriffe nicht per Hand, sondern mit Backdoor-Programmen oder Ähnlichem durchgeführt, die sich von alleine auf anderen Rechnern im Netzwerk verbreiten und dem Angreifer durch solche Botnetze weitere Wirte zum Ausführen seiner Angriffe bringen.

DoS-Angriffe wie **SYN-Flooding** oder die **Smurf-Attacke** belasten die Dienste eines Servers, beispielsweise HTTP, mit einer größeren Anzahl Anfragen, als dieser in der Lage ist zu bearbeiten, woraufhin er eingestellt wird oder reguläre Anfragen so langsam beantwortet, dass diese abgebrochen werden. Wesentlich effizienter ist es jedoch, wie bei **WinNuke**, der **Land-Attacke**, der **Teardrop-Attacke** oder dem **Ping of Death** Programmfehler auszunutzen, um eine Fehlerfunktion (wie einen Absturz) der Serversoftware auszulösen, worauf diese ebenso auf Anfragen nicht mehr reagiert.

4 Man-in-The-Middle-Angriffe (MITM-Angriffe)

Ein Man-In-The-Middle-Angriff (MITM-Angriff), auch Janusangriff (nach dem doppelköpfigen Janus der römischen Mythologie) genannt, ist eine Angriffsform, die in Rechnernetzen ihre Anwendung findet. Der Angreifer steht dabei entweder physikalisch oder – heute meist – logisch zwischen den beiden Kommunikationspartnern und hat dabei mit seinem System komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren. Die Janusköpfigkeit des Angreifers besteht darin, dass er den Kommunikationspartnern das jeweilige Gegenüber vortäuschen kann, ohne dass sie es merken.

Bekannte Möglichkeiten für MITM-Angriffe:

- ARP-Spoofing: Siehe Kapitel 4.1!
- DNS-Cache Poisoning: Der Angreifer gibt eine falsche Zieladresse für die Internet-Kommunikation vor und leitet dadurch den Verkehr durch seinen eigenen Rechner (Poison Routing).

4.1 ARP-Spoofing, ARP Poison Routing (APR)

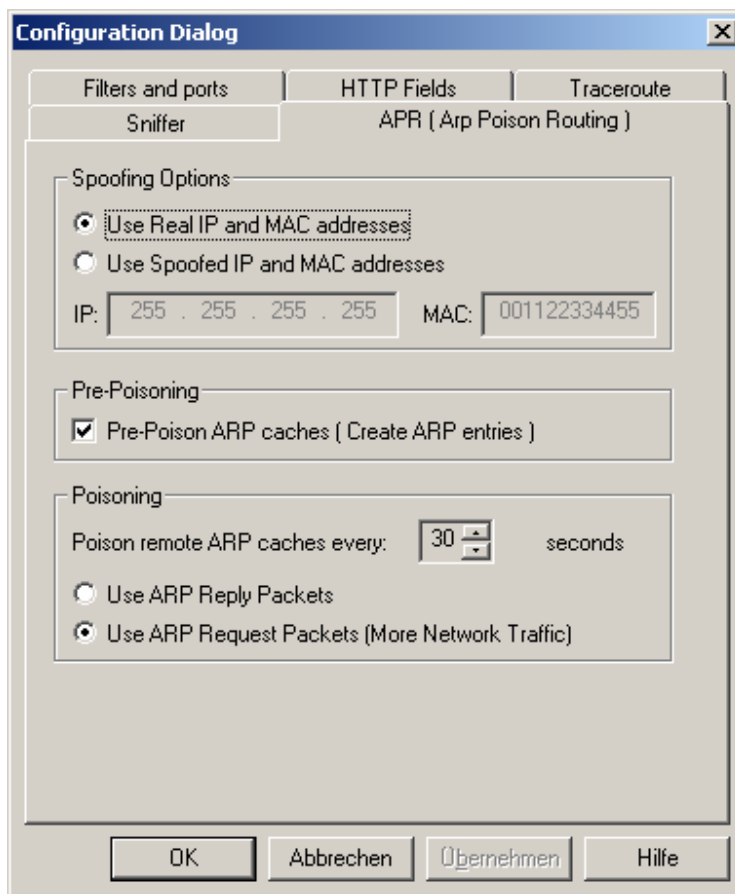
ARP-Spoofing (vom engl. to spoof – dt. täuschen, reinlegen) oder auch ARP Poison Routing (zu dt. etwa Anfrageverfälschung) bezeichnet das Senden von gefälschten ARP-Paketen. Beim ARP-Spoofing wird das gezielte Senden von gefälschten ARP-Paketen dazu benutzt, um die ARP-Tabellen in einem Netzwerk so zu verändern, dass anschließend der Datenverkehr zwischen zwei Rechnern in einem Computernetz abgehört oder manipuliert werden kann.

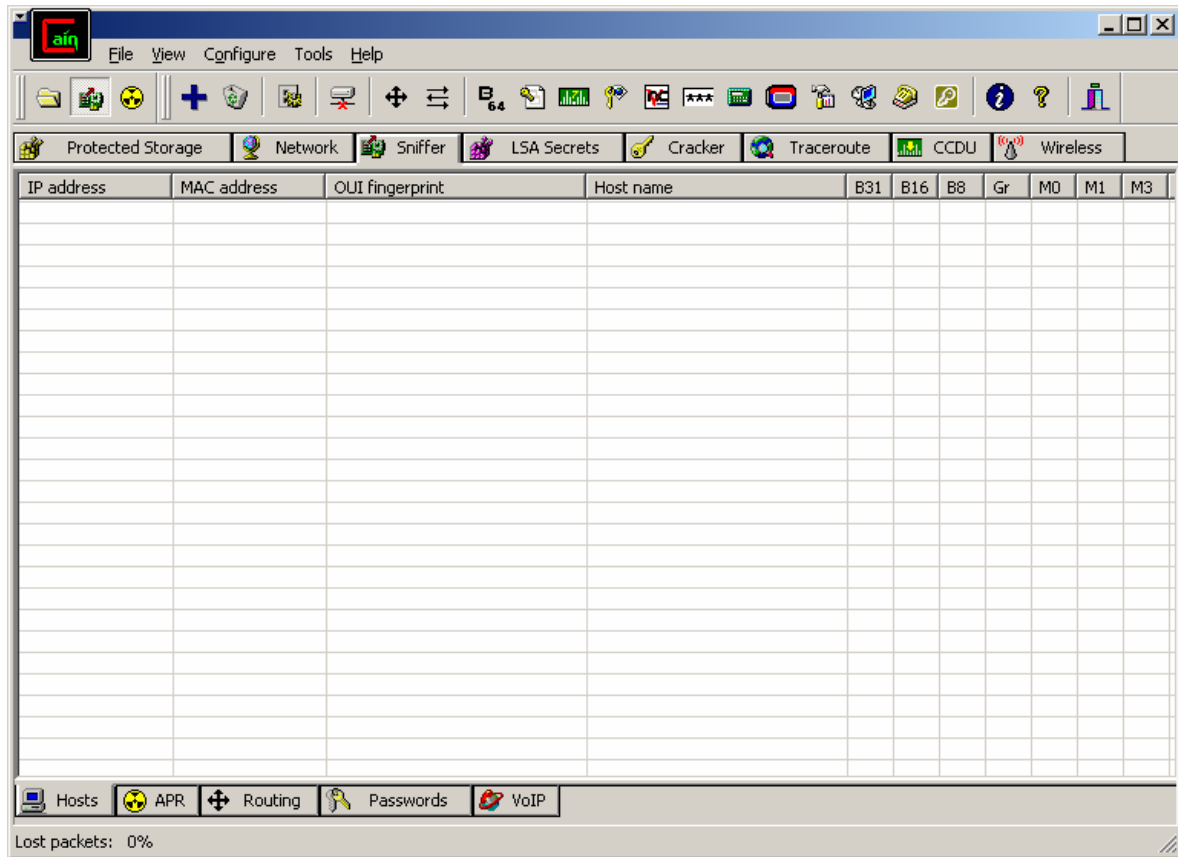
4.1.1 ARP Spoofing mit Cain & Abel

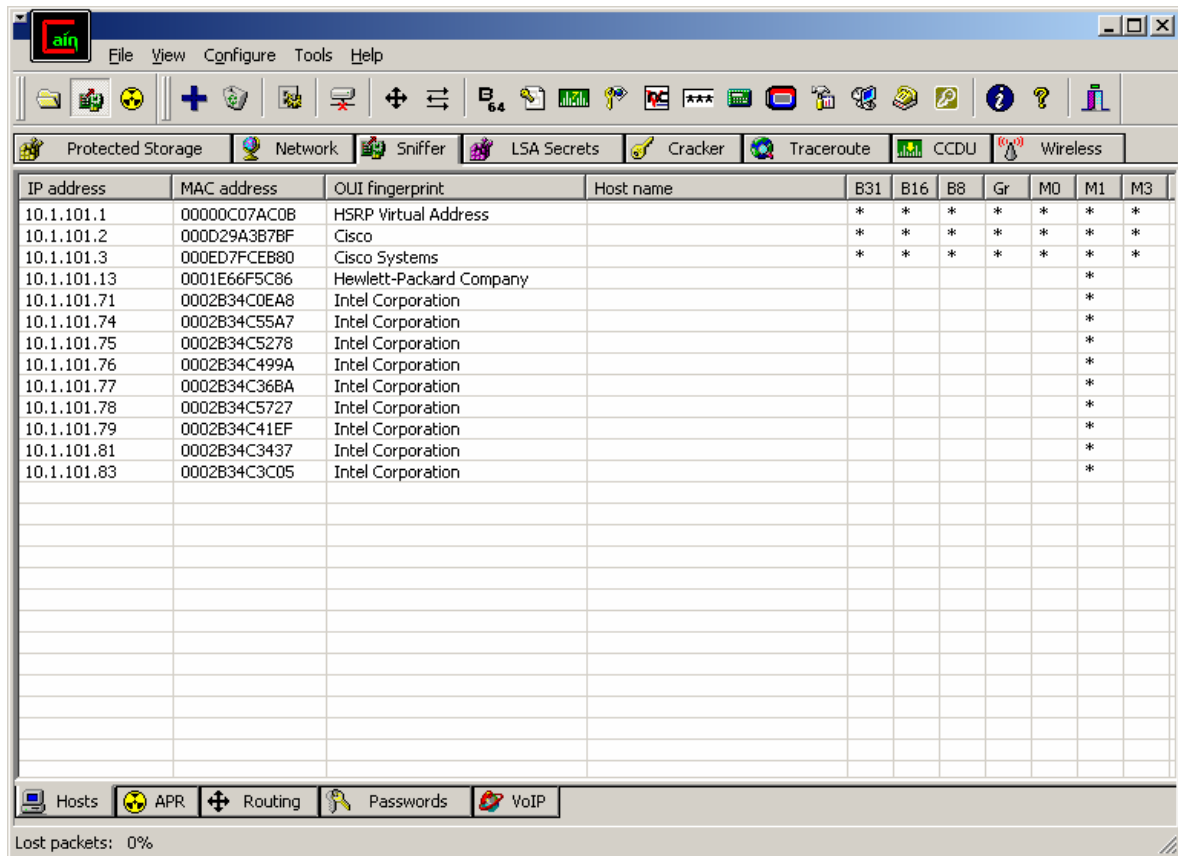
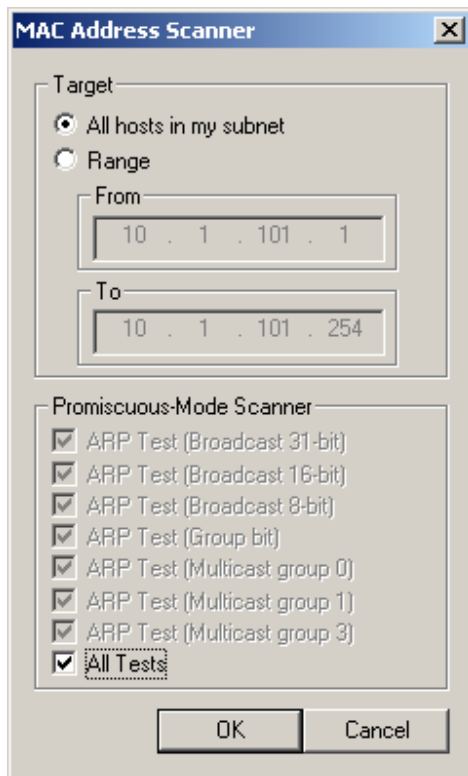
Cain & Abel (Download unter <http://oxid.it>) ist laut dem Entwicklerteam unter Massimiliano Montoro ein Passwort-Recovery-Tool für Microsoft Windows, ist aber eher ein Multifunktionswerkzeug.

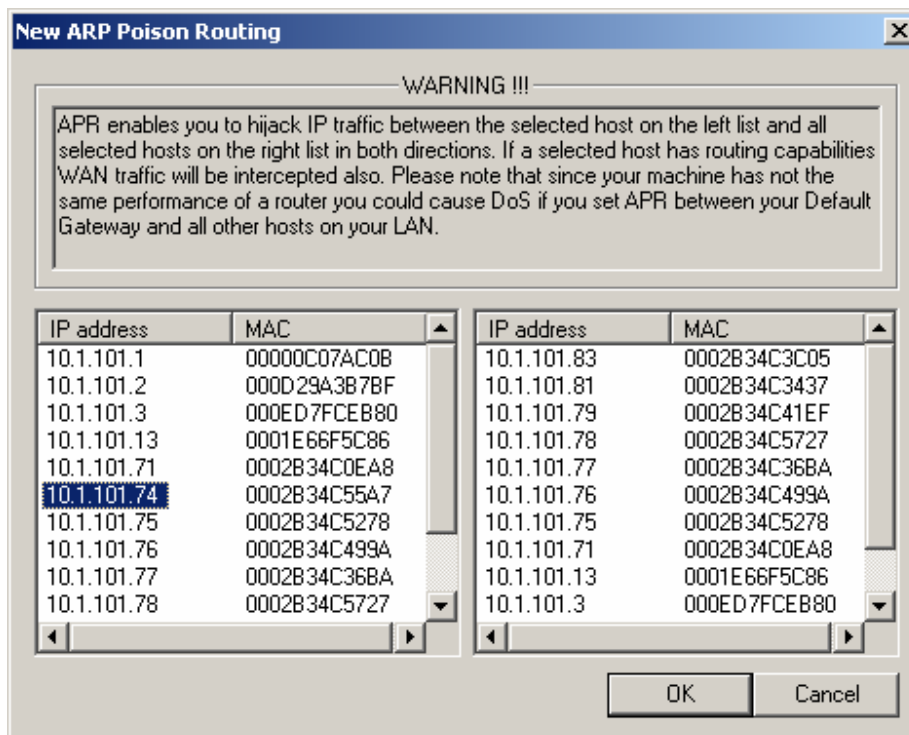
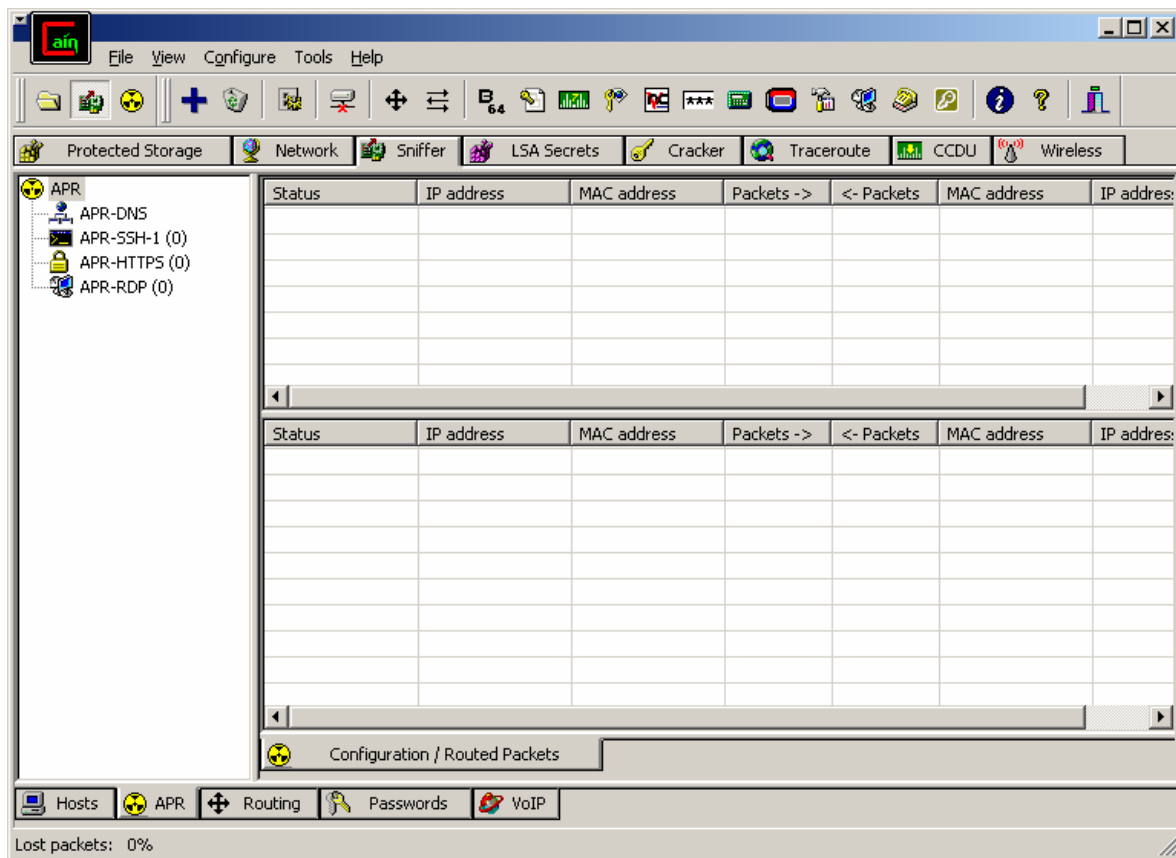
Es erlaubt das einfache Auslesen aller Passwörter, die im Browser gespeichert wurden, außerdem das Cracking verschlüsselter Passwörter (Hashes) mit Hilfe von Wörterbüchern, Brute-Force- und Rainbow-Tables sowie das Aufzeichnen von Passwörtern und VoIP-Unterhaltungen im Netz via ARP-Spoofing. Dadurch ist es ebenfalls in der Lage, Man-in-the-middle-Angriffe gegen eine Reihe von SSL-basierten Diensten und RDP durchzuführen. Außerdem können diverse Informationen von Windows-Systemen ausgelesen werden. Ebenfalls möglich ist das Analysieren von Routing-Prozessen.

Da Cain & Abel Sicherheitsvorkehrungen umgeht, muss es nach Inkrafttreten des sogenannten Hackerparagrafen (§202c StGB) in Deutschland als Computerprogramm zum Ausspähen von Daten aufgefasst werden. Somit kann **die illegale Benutzung der Software unter Strafe** gestellt werden.









The screenshot displays the main interface of Cain & Abel. The central pane shows a list of network connections. The connections are as follows:

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	10.1.101.74	0002B34C55A7			0000C07AC0B	10.1.101.
Idle	10.1.101.74	0002B34C55A7			0002B34C36BA	10.1.101.
Idle	10.1.101.74	0002B34C55A7			0002B34C3437	10.1.101.
Idle	10.1.101.74	0002B34C55A7			0002B34C5278	10.1.101.
Idle	10.1.101.74	0002B34C55A7			0002B34C3C05	10.1.101.
Idle	10.1.101.74	0002B34C55A7			000D29A3B7BF	10.1.101.
Idle	10.1.101.74	0002B34C55A7			0001E66F5C86	10.1.101.
Idle	10.1.101.74	0002B34C55A7			0002B34C499A	10.1.101.
Idle	10.1.101.74	0002B34C55A7			0002B34C41EF	10.1.101.
Idle	10.1.101.74	0002B34C55A7			0002B34C5727	10.1.101.
Idle	10.1.101.74	0002B34C55A7			0002B34C0EA8	10.1.101.
Idle	10.1.101.74	0002B34C55A7			000ED7FCEB80	10.1.101.

The interface also shows a sidebar with 'APR' and sub-items: APR-DNS, APR-SSH-1 (0), APR-HTTPS (0), and APR-RDP (0). At the bottom, there are buttons for Hosts, APR, Routing, Passwords, and VoIP. The status bar at the very bottom indicates 'Lost packets: 0%'.

The screenshot shows a network security tool interface with a menu bar (File, View, Configure, Tools, Help) and a toolbar. Below the toolbar are tabs for Protected Storage, Network, Sniffer, LSA Secrets, Cracker, Traceroute, CCDU, and Wireless. The main window displays a list of poisoning attacks and a routing table.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.1.101.74	0002B34C55A7	0	0	00000C07AC0B	10.1.101.1
Poisoning	10.1.101.74	0002B34C55A7	0	0	0002B34C36BA	10.1.101.77
Poisoning	10.1.101.74	0002B34C55A7	0	0	0002B34C3437	10.1.101.81
Poisoning	10.1.101.74	0002B34C55A7	0	0	0002B34C5278	10.1.101.75
Poisoning	10.1.101.74	0002B34C55A7	0	0	0002B34C3C05	10.1.101.83
Poisoning	10.1.101.74	0002B34C55A7	0	0	000D29A3B7BF	10.1.101.2
Poisoning	10.1.101.74	0002B34C55A7	0	0	0001E66F5C86	10.1.101.13
Poisoning	10.1.101.74	0002B34C55A7	0	0	0002B34C499A	10.1.101.76
Poisoning	10.1.101.74	0002B34C55A7	0	0	0002B34C41EF	10.1.101.79
Poisoning	10.1.101.74	0002B34C55A7	0	0	0002B34C5727	10.1.101.78
Poisoning	10.1.101.74	0002B34C55A7	186	164	0002B34C0EA8	10.1.101.71
Poisoning	10.1.101.74	0002B34C55A7	0	0	000ED7FCEB80	10.1.101.3

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	10.1.101.74	0002B34C55A7	3	3	0002B34C0EA8	172.16.200.101

Configuration / Routed Packets

Hosts APR Routing Passwords VoIP

Lost packets: 0%