BRAIN-MEDIA.DE

PROFESSIONELLES INTERNET- UND OPEN-SOURCE-KNOW-HOW

Holger Reibold

Cain & Abel kompakt

Security.Edition

Einstieg in das Penetration Testing mit dem Windows-Klassiker

Holger Reibold

Cain & Abel kompakt

BRAIN MEDIA

© 2015 Brain-Media.de

Herausgeber: Dr. Holger Reibold

Umschlaggestaltung: Brain-Media.de

Satz: Brain-Media.de

Coverbild: Brain-Media.de

Korrektur: Theresa Tting

Inhaltsverzeichnis

Vorwort

Fast täglich kann man in den Medien von erfolgreichen Hacker-Attacken hören. Prominentes Opfer war im Sommer 2015 das Netzwerk des Bundestages, das – vermeintlich aus Russland – gehackt wurde. Das BSI, das für die Wartung und die Sicherheit dieses Netzwerks zuständig ist, blamierte sich in diesem Zusammenhang, weil man weder in der Lage war, das Netzwerk ausreichend zu schützen, noch zeitnah eine sichere Umgebung herzustellen.

Solch prominente Geschehnisse sind nur die Spitze eines Eisbergs. Tag für Tag werden Millionen Hacker-Attacken gefahren. Manchmal sind es nur Skript-Kiddies, die ihre erworbenen Hacker-Fähigkeiten testen, doch die überwiegende Anzahl der Attacken dürfte einen kriminellen Hintergrund haben. Oftmals geht es um Wirtschaftsspionage.

Wenn auch Sie für die Sicherheit eines Netzwerks zuständig sind, müssen Sie dieses kontinuierlich auf Sicherheitslücken und sonstige Schwachstellen hin überprüfen. Fachleute sprechen von Penetrationstests. Sie dienen dazu, Netzwerkkomponenten auf bekannte Schwächen hin zu überprüfen.

Ihr Ziel muss es sein, potenziellen Hackern zuvorzukommen. Das Zauberwort lautet dabei: Waffengleichheit. Nur dann, wenn Sie wissen, wie Hacker vorgehen und welche Tools sie dabei einsetzen, sind sie in der Lage, ihnen mit gleichen Mitteln zu begegnen. Dabei sind Sie potenziellen Angreifern gegenüber klar im Vorteil, denn Sie kennen die kritischen Infrastrukturkomponenten, die Netzwerk-Topologie, potenzielle Angriffspunkte, die ausgeführten Services und Server etc.

Um Ihre eigene Infrastruktur so sicher wie möglich zu machen, müssen Sie immer und immer wieder folgende Schritte ausführen:

1. Identifizierung von Schwachstellen und deren Risiko.
2. Praktische Ausnutzung und Testen der Schwachstellen in einer gesicherten Umgebung.
3. Tests in einer realen Umgebung.
4. Schließen von gefundenen Schwachstellen.

Wenn Sie bei Punkt 4 angelangt sind, fängt alles wieder von vorne an – ein permanenter Kreislauf. Wenn Sie diese Schritte verinnerlichen und kontinuierlich die

Sicherheit kritischer Systeme im Blick haben, wird Ihre Umgebung mit jeder Maßnahme sicherer. Das wiederum spart Ihnen langfristig viel Zeit und Ärger, denn Sie geben Hackern kaum eine Chance, ihr Unwesen zu treiben.

Sie können das Ganze auch sportlich betrachten und als Spiel sehen. Jeder hat dabei seine Mittel: Mitspieler, technische Geräte und Techniken. Am Ende ist nur wichtig, dass Sie als Sieger vom Platz gehen.

In diesem Buch lernen Sie eines der beliebtesten Hacker-Tools kennen: Cain & Abel. Es handelt sich dabei um ein Windows-Programm, das verschiedenste Aufgaben beim Penetration Testing übernehmen kann – angefangen beim Knacken von Passwörtern bis hin zu Attacken auf WLANs.

Bleibt mir nur noch, Ihnen viel Spaß und Erfolg beim Einstieg in die Welt der Penetrationtests mit Cain & Abel zu wünschen!

Herzlichst,

Holger Reibold

(September 2015)

1 Penetration Testing mit Cain & Abel

Genug der Vorrede! Sie wollen loslegen. Am liebsten jetzt direkt. Wie aber können die ersten Schritte aussehen? Und wo soll man beginnen? Noch bevor Sie sich Gedanken darüber machen, welche Systeme zuerst einer Sicherheitsanalayse unterzogen werden, müssen Sie zunächst ein Penetration Testing-System aufsetzen und sich mit bewährten Vorgehensweisen vertraut machen.

In der Praxis kommt dabei ein handlicher Werkzeugkasten zum Einsatz, der alle notwendigen Tools zur Verfügung stellt. Deren Einsatz ist in der Regel längst nicht so kompliziert, wie viele meinen. Wenn Sie die Grundtechniken drauf haben, sind Sie bereits ein guter Penetration-Tester und können sich auch an harte Nüsse herantrauen.

In diesem Einstieg dreht sich alles um den Sicherheitsspezialisten Cain & Abel. Das von Massimiliano Montoro entwickelte Programm wird häufig als Tool für die Passwortrettung für Windows-Betriebssysteme betrachtet, doch damit wird man dem Programm nicht gerecht. Vielmehr handelt es sich um ein Multifunktionswerkzeug.

Cain & Abel erlaubt beispielsweise das einfache Auslesen aller Passwörter, die im Browser gespeichert wurden und das Knacken von verschlüsselten Passwörtern mit Wörterbücher- und Brute-Force-Attacken. Das Programm kann dabei insbesondere Rainbow Tables verwenden.

Eine weitere Besonderheit, die Cain & Abel für das Penetration Testing so interessant macht, sind die Sniffing-Funktionen, mit denen Sie Traffic aufzeichnen können. Per ARP-Spoofing können Sie Man-in-the-Middle-Angriffe gegen eine Reihe von SSL-basierten Diensten und RDP durchführen. Cain & Abel kann auch verschiedene Informationen von Windows-Systemen auslesen und sogar Routing-Prozesse analysieren.

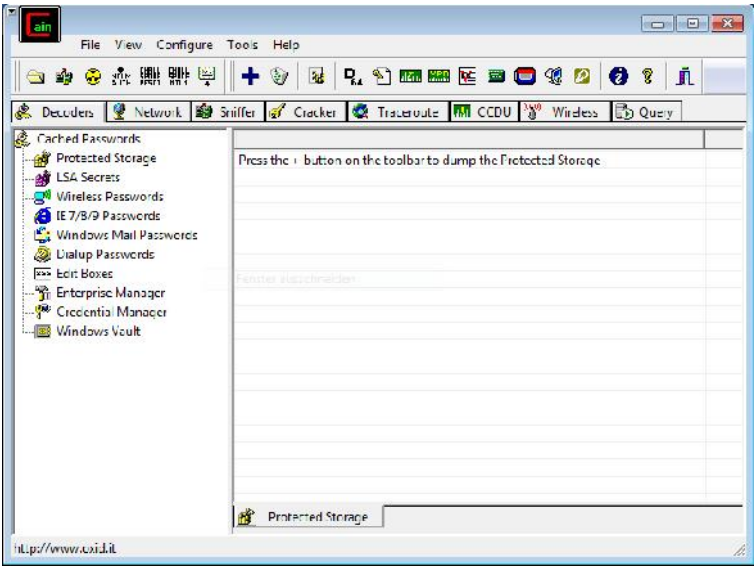
Wie Sie der Programmbezeichnung entnehmen können, besteht Cain & Abel aus zwei Komponenten. Bei Abel handelt es sich um ein Client-Programm, das ferngesteuert über das Windows-Netzwerk installiert werden kann und TCP/UDP-Tabellen, die LSA-Secrets und die Hashwerte der Benutzerkonten auslesen kann. Für die Cain-Komponente kann Abel den Remote-Konsolenzugriff ermöglichen.

Damit Cain & Abel auf tiefe Netzwerkschichten und den dort übermittelten Traffic zugreifen kann, benötigt das Programm spezielle Treiber, insbesondere die WinPcap-Treiber und den AirPcap-Adapter. Letztgenannter ermöglicht das passive

Mitlesen von Datenverkehr in WLANs und Angriffe auf WEP-geschützte Netzwerke. Auch Attacken gegen einen WPA-Handshake und WPA-PSK gesicherte WLANs können mit Cain & Abel durchgeführt werden.

Immer dann, wenn das Programm an seine Grenzen stößt, können Sie zu anderen Hilfsmitteln greifen. So können Sie beispielsweise die von Cain aufgezeichneten Passwort-Hashes mit Programmen wie John the Ripper knacken. Cain selbst kann Aufzeichnungen von Netzwerkverkehr im Datenformat von LibPcap/WinPcap lesen und extrahiert dann automatisch Passwörter bzw. deren Hashwerte.

Das Praktische an Cain & Abel ist die Tatsache, dass dieses Tool so viele Funktionen unter einer Benutzeroberfläche zusammenfasst, die für Penetration Tester relevant sind.



Der Klassiker für MitM-Attacken: Cain & Abel.

1.1 Typischer Einsatzbereich

Bevor wir uns der Inbetriebnahme, der Konfiguration und dem genaueren Kennenlernen des Programms widmen, möchte ich Ihnen kurz einige typische Anwendungsbereiche im Schnelldurchlauf vorstellen. Alle für die Netzwerksicherheit verantwortlichen Personen müssen tief in ein Netzwerk, seine Struktur und seine

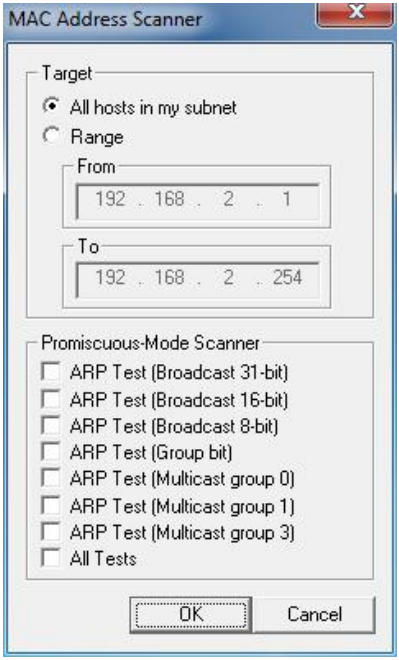
Anwendungen eindringen, um etwaige Schwachstellen zu identifizieren. Auch Hacker machen prinzipiell nichts anderes. Nur die Intension ist eine andere. Um tiefe Einblicke in den Netzwerk-Traffic zu erhalten, müssen Sie Daten abfangen, mit denen Sie irgendwie weiterkommen. Dabei sind ARP-Spoofing-Methoden sehr hilfreich, und hierbei insbesondere die sogenannten Man-in-the-Middle-Angriffe, kurz MitM. Sie werden auch als Janusangriffe (in Anspielung auf den doppelgesichtigen Janus der römischen Mythologie) bezeichnet.

ARP-Spoofing ist eine spezielle Man-in-the-Middle-Attacke. Dabei befindet sich der potenzielle Angreifer entweder physikalisch oder logisch zwischen den beiden Kommunikationspartnern, hat dabei mit seinem System vollständige 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 vortäuscht, das jeweilige Gegenüber zu sein.

Beim ARP-Spoofing werden gefälschte ARP-Pakete an das Ziel übermittelt. Dabei wird beim Zielrechner die ARP-Tabelle überschrieben, wodurch der gesamte Netzwerkverkehr des Zielrechners auf den Penetration-Rechner umgeleitet wird. Hier kommt Cain & Abel ins Spiel, denn das Multifunktionswerkzeug erlaubt nicht nur das einfache Auslesen aller Passwörter, sondern eben auch das Sniffing, die Durchführung von Brute-Force-Attacken und noch viel es mehr.

Nach der Installation müssen Sie zunächst die Netzwerkkonfiguration anpassen. Dazu klicken Sie in der Symbolleiste auf das zweite Symbol von links (*Start/Stop Sniffer*). Wählen Sie den Netzwerkadapter aus, den Sie für die Aufzeichnung verwenden wollen. Dann aktualisieren wir im Hauptfenster die Host-Liste. Öffnen Sie die Registerkarte *Sniffer* und dort das Unterregister *Hosts*.

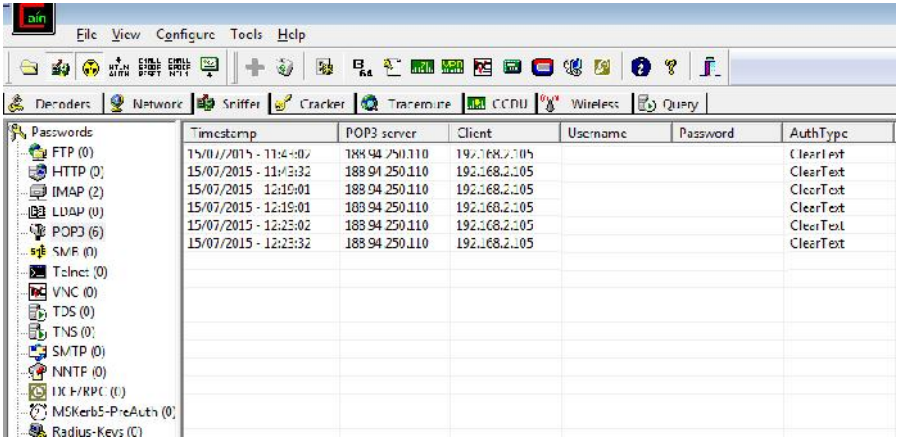
Anschließend bestimmen Sie den Adressbereich, der für Sie von Interesse ist. Dazu klicken Sie auf das Pluszeichen, bestimmen den Bereich oder wählen alle Hosts des Subnetzes, in dem Sie sich befinden. Mit einem Klick auf *OK* wird die Liste aktualisiert. Das Tool durchkämmt das Netzwerk und stellt Ihnen die gefundenen Hosts in einer Tabelle zur Auswahl.



Die Konfiguration des Adressbereichs.

Wählen Sie das Ziel aus. Dazu wechseln Sie zur Registerkarte *ARP*. Markieren Sie in der linken Spalte zunächst den Haupteintrag *ARP*. Es öffnet sich rechts ein zweigeteilter Bereich. Mit einem Klick in den oberen Bereich erscheint in der Symbolleiste das blaue Pluszeichen. Cain & Abel präsentiert Ihnen den Dialog *ARP Poison Route*. Dort wählen Sie links beispielsweise Ihren DSL-Router und rechts einen Zielrechner. Mit Cain & Abel können Sie sich dann zwischen diesen beiden Komunikationspartnern einhängen.

Um den eigentlichen Angriff zu starten, klicken Sie den Radioaktiv-Button (*Start/Stop ARP*). Wenn Sie parallel dazu den Traffic mit Wireshark aufgezeichnet haben, können Sie diesen mitlesen.



Die Registerkarte *Passwords* verrät Ihnen nun, welche Passwörter zwischen den beiden Zielen ausgetauscht wurden.

Wenn Sie nun die Registerkarte *Passwords* öffnen, können Sie dort Informationen (Benutzername/Passwort) abrufen, die zwischen den beiden Rechnern übermittelt wurden, zwischen die Sie sich mit Cain & Abel gesetzt haben. Wenn das Passwort dann auch noch im Klartext übermittelt wird, haben Sie den Zugang zum jeweiligen Dienst.

Für den Betrieb von Cain & Abel müssen Sie außerdem die Windows-eigene Firewall oder die eines Drittanbieters deaktivieren. Damit haben Sie einen ersten Eindruck von der Leistungsfähig- und Benutzerfreundlichkeit des Sicherheitsspezialisten.

1.2 Installation

Wie bereits erwähnt, handelt es sich bei Cain & Abel um ein Programm, das aus den beiden Komponenten Cain und Abel besteht. Die sind im Installationsprogramm *ca_setup.exe* enthalten, das über die Website der Entwickler unter der URL *http://www.oxid.it* bereitsteht.

Die Komponente Cain (*Cain.exe*) ist das GUI-Hauptprogramm, Abel ein Windows-Service, der auf den beiden Dateien *Abel.exe* und *Abel.dll* bzw. *Abel64.exe* and *Abel64.dll* besteht.

Die Systemanforderungen von Cain & Abel sind ansonsten minimal. Es genügt ein Windows-System ab Windows 2000 mit ca. 10 MB freiem Speicherplatz. Dabei

nicht berücksichtigt ist der Speicherplatz für etwaige Traffic-Aufzeichnungen, Rainbow Tables etc.

Sie benötigen außerdem den WinPcap-Pakettreiber. Der ist allerdings in dem Cain & Abel-Installationspaket enthalten. Die aktuellste Version dieses Treibers finden Sie auf der WinPcap-Projektsite (*http://www.winpcap.org*).

Wenn Sie mit Cain & Abel auch drahtlosen Traffic unter die Lupe nehmen wollen, benötigen Sie hierfür den AirPcap-Treiber. Der erlaubt beispielsweise das passive Sniffen von WLAN-Traffic. Den AirPcap-Treiber müssen Sie sich manuell herunterladen, denn er ist nicht Bestandteil des Installationspakets. Die Download-URL:

https://support.riverbed.com/content/support/software/steelcentral-npm/airpcap.html

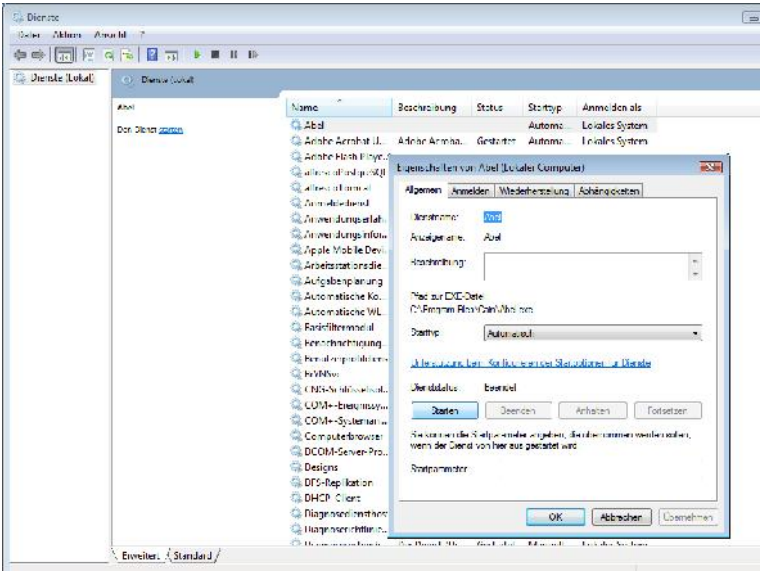
Die Installation von Cain & Abel ist ansonsten einfach: Starten Sie das Installationsprogramm mit einem Doppelklick auf die Installationsdatei und folgen Sie den Anweisungen am Bildschirm. Das Setup bietet keine besonderen Auswahlmöglichkeiten.

Das Installationsprogramm installiert eine Fülle von Dateien im Standardverzeichnis *C:\Programme\Cain*:

- Cain.exe – das Hauptprogramm
- Cain.exe.sig – PGP-Signatur des Entwicklers für die Datei *Cain.exe*
- CA_UserManual.chm – Windows-Hilfe für Cain & Abel
- Abel.exe – ausführbare EXE des Windows-Dienstes Abel
- Abel.exe.sig – PGP-Signatur zu *Abel.exe*
- Abel.dll - DLL, die für die Ausführung von *Abel.exe* benötigt wird
- Abel.dll.sig – PGP-Signatur für *Abel.dll*
- Abel64.exe – Exectuable für 64-Bit-Windows-Systeme
- Abel64.exe.sig – PGP-Signature für *Abel64.exe*
- Abel64.dll – DLL für die Ausführung von *Abel.exe* unter 64 Bit-Windows
- Abel64.dll.sig – PGP-Signatur für *Abel64.dll*
- Uninstal.exe – Deinstallationsprogramm
- Wordlist.txt – kurze Wortliste

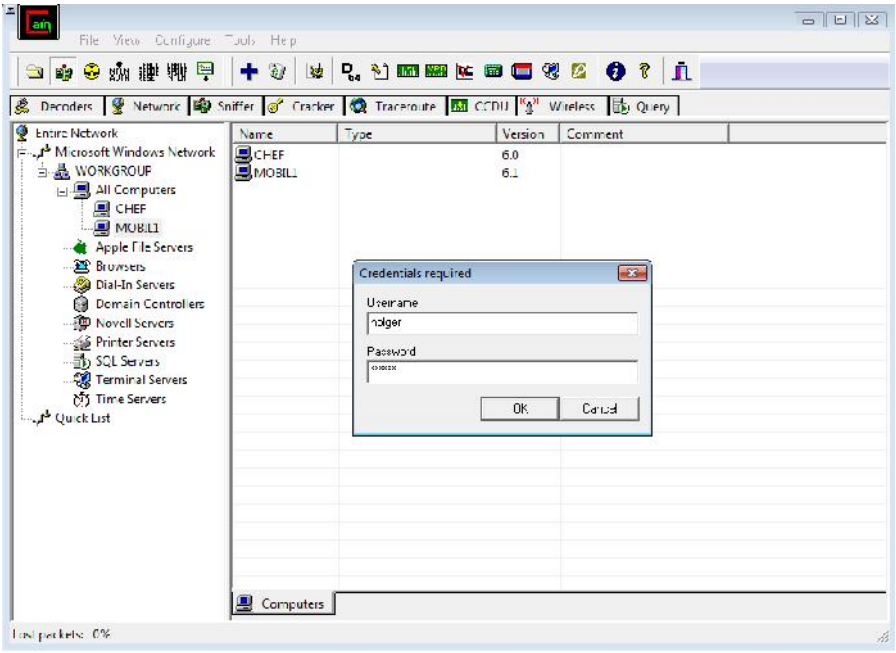
- Install.log – Protokoll der Installationsdatei
- Whatsnew.txt – Neuigkeiten zum Programm
- oui.txt – Herstellerinformationen über MAC-Adressen
- \cain\winrtgen\winrtgen.exe – Winrtgen, kleines Windows-Programm für das Erzeugen von Rainbow Tables
- \cain\winrtgen\winrtgen.exe.sig – PGP-Signatur von Winrtgen
- \cain\winrtgen\charset.txt – Beispieldatei, die Charset-Definitionen für *Winrtgen.exe* und Attacken mit Cain enthält
- \cain\Driver\WinPcap_4_1_3.exe – WinPcap-Treiber

Das Client-Programm Abel ist ein Windows-Dienst, der wie bereits erwähnt, aus den beiden Dateien *Abel.exe* und *Abel.dll* besteht. Beachten Sie, dass diese beide Dateien zwar in das Installationsverzeichnis kopiert, nicht aber als Windows-Dienst eingerichet werden. Sie können Abel lokal oder mit Hilfe von Cain auch remote installieren. In beiden Fällen sind administrative Berechtigungen notwendig.



Abel ist als Windows-Dienst eingerichtet.

Um Abel lokal als Dienst zu installieren, führen Sie einfach einen Doppelklick aus. Anschließend wird Abel beim nächsten Systemstart automatisch ausgeführt.



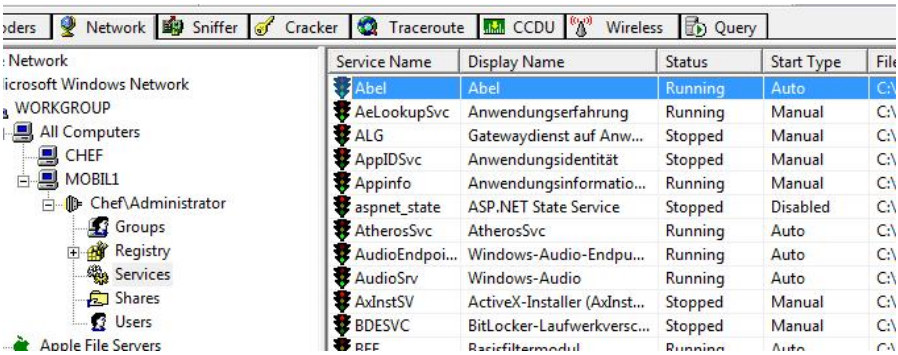
Die Remote-Installation von Abel auf einem Windows-Netzwerk-Client.

Sie können Abel auch auf einem entfernten Windows-Client installieren. Einzige Voraussetzung: Der Client muss zur Arbeitsgruppe gehören und Sie müssen einen administrativen Account besitzen.

Ist das der Fall, öffnen Sie in Cain die Registerkarte *Network* und wählen den Rechner aus, auf dem Sie Abel installieren wollen. Markieren Sie den Rechner mit der rechten Maustaste und führen Sie aus dem Kontextmenü den Befehl *Connect As* aus.

Geben Sie die Zugangsdaten an und stellen Sie die Verbindung her. In Cain werden zu dem Remote-Client verschiedene Untermenüs eingeblendet. Markieren Sie das Service-Icon und führen Sie mit einem Rechtsklick den Befehl *Install Abel* aus. Fertig! Das funktioniert übrigens auch dann, wenn es sich beim dem Cain-System um ein 32-Bit- und bei dem Remote-Rechner um ein 64-Bit-System handelt. Das

Programm installiert in diesem Fall die 64-Bit-Variante auf dem Remote-Rechner. Nach der Remote-Installation können Sie Abel von Cain aus steuern.



Abel wurde erfolgreich auf dem Remote-System installiert.

Damit Cain korrekt ausgeführt werden kann, benötigt das Programm folgende Bibliotheken: Abel.dll, Crypt32.dll, Pstorec.dll, Kernel32.dll, Advapi32.dll, Comctl32.dll, Comdlg32.dll, Gdi32.dll, Iphlpapi.dll, Mpr.dll, NetApi32.dll, Odbc32.dll, Ole32.dll, Oleaut32.dll, Packet.dll (Winpcap), Rasapi32.dll, Rpcrt4.dll, Shell32.dll, User32.dll, Wpcap.dll (Winpcap), Airpcap.dll (AirPcap), Ws2_32.dll, Wsnmp32.dll.

Abel.exe benötigt entsprechend folende Bibliotheken: Abel.dll, Kernel32.dll, Advapi32.dll, Iphlpapi.dll, User32.dll, Ws2_32.dll.

Ist die Installation von Cain & Ábel abgeschlossen, richtet der Sicherheitsspezialist weitere Dateien in dem Installationsverzeichnis ein. Für die Cracker-Funktionen werden folgende Dateien angelegt:

- APOP-MD5.LST – enthält die Zugangsdaten für APOP-MD5
- CRAM-MD5.LST – enthält die Zugangsdaten für CRAM-MD5
- PIX-MD5.LST – enthält die Zugangsdaten für Cisco PIX
- IOS-MD5.LST – enthält die Zugangsdaten für iOS
- PWLS.LST – enthält die List der PWL-Daten und Zugangsdaten
- NTLMv2.LST – enthält die Zugangsdaten für NTLMv2
- LMNT.LST – enthält die Zugangsdaten für LM und NTLMv1

- CACHE.LST – enthält die Zugangsdaten für MS-CACHE
- OSPF-MD5.LST – enthält die Zugangsdaten für OSPF-MD5
- RIP-MD5.LST – enthält die Zugangsdaten für RIPv2-MD5
- VRRP-HMAC.LST – enthält die Zugangsdaten für VRRP-HMAC
- VNC-3DES.LST – enthält die Zugangsdaten für VNC Triple DES
- MD2.LST – enthält die Zugangsdaten für MD2
- MD4.LST – enthält die Zugangsdaten für MD4
- MD5.LST – enthält die Zugangsdaten für MD5
- SHA-1.LST – enthält die Zugangsdaten für SHA-1
- SHA-2.LST – enthält die Zugangsdaten für SHA-2
- RIPEMD-160.LST – enthält die Zugangsdaten für RIPEMD-160
- K5.LST – enthält die Zugangsdaten für MS-Kerberos PreAuth
- RADIUS_SHARED_HASHES.LST – enthält die Zugangsdaten für RADIUS PreShared Key
- IKEPSKHashes.LST – enthält die Zugangsdaten für IKE-PSK
- MSSQLHashes.LST – enthält die Zugangsdaten für MS SQL
- MySQL.LST – enthält die Zugangsdaten für MySQL
- ORACLE.LST – enthält die Zugangsdaten für ORACLE
- TNS-HASHES.LST – enthält die Zugangsdaten für ORACLE-TNS
- 80211.LST – Liste der IEEE 802.11-Capture-Dateien
- SIPHASHES.LST – Liste der Hash-Werte, die das SIP-Protokoll verwendet
- TOKENS.LST – Liste der RSA-Zeichen
- WPAPSK.LST – Liste der WPA-PSK-Werte
- CHAP.LST – Liste der CHAP-MD5-Werte

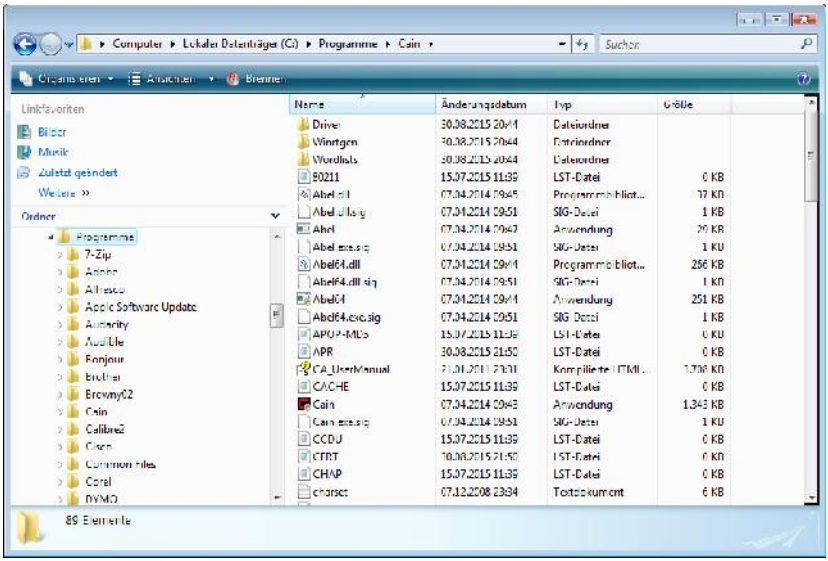
Die Sniffer-Funktionen verwenden folgende Dateien:

- HOSTS.LST – Liste mit Host-Informationen wie MAC- und IP-Adresse sowie Hostnamen
- APR.LST – Liste mit Hosts, die in APR verwendet werden
- DRR.LST – Liste mit Host-Namen und IP-Adressen, die von APR-DNS verwendet werden
- SSH-1.LST – Referenzen zu Dateien, die durch den SSH-1 Sniffer-Filter erzeugt wurden
- CERT.LST – Referenzzertifikatdateien, die von APR-HTTPS genutzt werden
- HTTPS.LST – Referenz zu Dateien des APR-HTTPS Sniffer-Filters
- FTPS.LST – Referenz zu Dateien des APR-FTPS Sniffer-Filters
- IMAPS.LST – Referenz zu Datieen des APR-IMAPS Sniffer-Filters
- LDAPS.LST – Referenz zu Dateien des APR-LDAPS Sniffer-Filters
- POP3S.LST – APR-POP3S-Sniffer-Filter
- RDP.LST - APR-RDP-Sniffer-Filter
- FTP.LST – Zugangsdaten, die der FTP-Sniffer-Filter aufgezeichnet hat
- HTTP.LST – Zugangsdaten, die der HTTP-Sniffer aufgezeichnet hat
- IMAP.LST – Zugangsdaten, die der IMAP-Sniffer aufgezeichnet hat
- POP3.LST – Zugangsdaten, die der POP3-Sniffer aufgezeichnet hat
- SMB.LST – Zugangsdaten, die der SMB-Sniffer aufgezeichnet hat
- TELNET.LST – Zugangsdaten, die der Telnet-Sniffer aufgezeichnet hat
- VNC.LST – Zugangsdaten, die der VNC-Sniffer aufgezeichnet hat
- TDS.LST – Zugangsdaten, die der TDS-Sniffer aufgezeichnet hat
- SMTP.LST – Zugangsdaten, die der SMTP-Sniffer aufgezeichnet hat
- NNTP.LST – Zugangsdaten, die der NNTP-Sniffer aufgezeichnet hat
- KRB5.LST – Zugangsdaten, die der Kerberos-Sniffer aufgezeichnet hat
- DCERPC.LST – Zugangsdaten, die der DCE/RPC-Sniffer aufgezeichnet hat

- RADIUS.LST – Zugangsdaten des RADIUS-Sniffers
- ICQ.LST – Zugangsdaten des ICQ-Sniffers
- IKE-PSK.LST – Zugangsdaten des IKE-PSK-Sniffers
- MySQL.LST – Zugangsdaten des MySQL-Sniffers
- SNMP.LST – Community-String des SNMP-Sniffers
- VoIP.LST – VoIP-Konversionen, die der VoIP-Sniffer ausgezeichnet hat
- WPAPSKAUTH.LST – Zugangsdaten des WPAPSK-Sniffers
- TNS.LST – Zugangsdaten des ORACLE-TNS-Sniffers
- GRE_PPP.LST – Zugangsdaten des GRE/PPP-Sniffers
- PPPoE.LST – Zugangsdaten, die der PPPoE-Sniffer gesammelt hat

Cain & Abel legt einige weitere Dateien an bzw. greift auf diese bei der Verwendung verschiedener Funktionen zurück:

- RT.LST – Enthält eine Liste von Rainbow Tables
- QLIST.LST – Liste der Host, die auf der Registerkarte *Network* aufgeführt wird
- CCDU.LST – Enthält Informationen über den Cisco Config Downloader
- HTTP_USER_FIELDS.LST – Liste der Benutzernamenfelder, die der HTTP-FORM- und HTTP-COOKIE-Sniffer verwendet
- HTTP_PASS_FIELDS.LST – Passwortfelder, die der HTTP-FORM- und HTTP-COOKIE-Sniffer verwendet
- DUMP.IVS – Liste der WEP IVs in einem Aircrack-ng kompatiblen Format

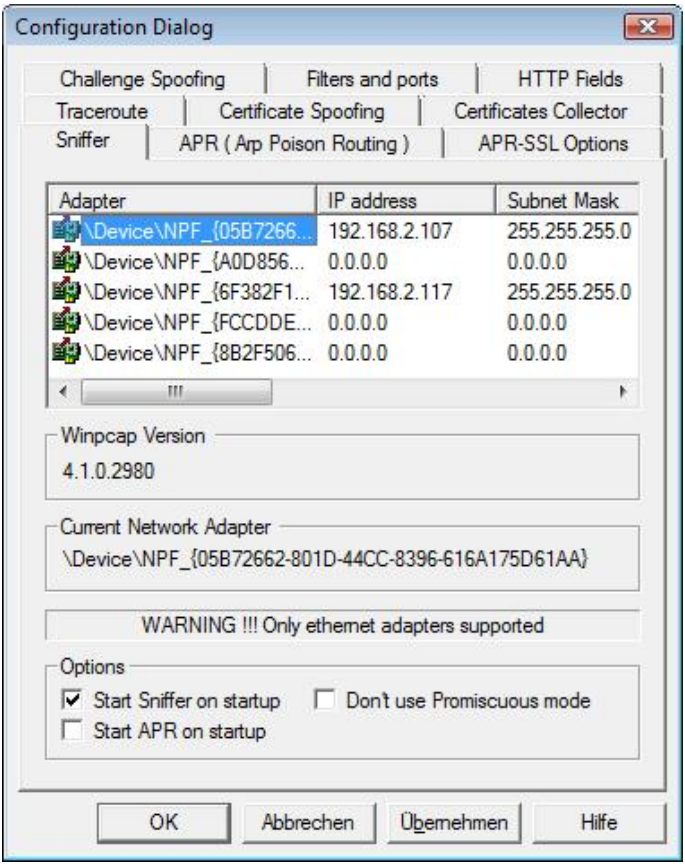


Ein Blick in das Installationsverzeichnis von Cain & Abel.

Cain & Abel verwendet außerdem verschiedene Unterverzeichnisse bzw. legt diese an – je nachdem, welche Funktionen Sie verwenden:

- \cain\Certs\ – enthält Fake-Zertifikate mit der Dateierweiterung *CRT*, die für das APR SSL-Spoofing verwendet werden
- \cain\HTTPS\ – enthält die APR-HTTPS-Aufzeichnungen
- \cain\FTPS\ – enthält die APR-FTPS-Aufzeichnungen
- \cain\POP3S\ – enthält die APR-POP3S-Aufzeichnungen
- \cain\IMAPS\ – enthält die APR-IMAPS-Aufzeichnungen
- \cain\LDAPS\ – enthält die APR-LDAPS-Aufzeichnungen
- \cain\SSH-1\ – enthält die APR-SSH-1-Aufzeichnungen
- \cain\Telnet\ – enthält die Telnet-Aufzeichnungen
- \cain\VoIP\ – enthält die VoIP-Aufzeichnungen im WAV-Format
- \cain\CCDU\ – enthält die Aufzeichnungen von CISCO-Devices

Wenn Sie Cain & Abel aus irgendeinem Grund wieder von Ihrem System entfernen wollen, so verwenden Sie hierfür das Deinstallationsprogramm der Cain-Programmgruppe oder den Software-Manager. Beachten Sie, dass das Deinstallationsprogramm den Abel-Service nicht entfernen kann.



Ein erster Blick auf die Cain & Abel-Konfiguration.

1.3 Cain & Abel konfigurieren

Um ein Maximum aus Cain & Abel herauszuholen, müssen Sie die Umgebung optimal an Ihre Bedürfnisse anpassen. Das Programm stellt Ihnen umfangreiche Anpassungs- und Konfigurationsmöglichkeiten zur Verfügung. Diese sind über das

Menü *Configure* oder mit einem Klick auf das *Configure*-Icon in der Symbolleiste (das mit dem Zahnrad) verfügbar.

Beim Öffnen der Cain & Abel-Konfiguration wird standardmäßig die Registerkarte *Sniffer* geöffnet. Auf dieser Registerkarte werden zunächst die erkannten Netzwerkschnittstellen aufgeführt. Zu jeden Adapter können Sie der tabellarischen Übersicht folgende Informationen entnehmen:

- Adapter
- IP-Adresse
- Netzmaske
- Gateway
- MAC-Adresse
- Typ
- Geschwindigkeit
- Beschreibung

Als Nächstes erfahren Sie, welche WinPcap-Version auf Ihrem System installiert ist.

Im Feld *Options* können Sie durch Aktivieren der Option *Start Sniffer on Startup* dafür sorgen, dass der Sniffer bei jedem Programmstart aktiviert wird. Der Sniffer ist mit dem WinPcap-Driver Version 2.3 (oder höher) kompatibel. Allerdings ist ein Sniffing, also eine Aufzeichnung des Traffics, nur über eine Ethernet-Schnittstelle möglich.

Auf der Registerkarte *APR* können Sie das sogenannte ARP Poison Routing konfigurieren. Cain verwendet einen gesonderten Thread, der alle 30 Sekunden ARP-Poison-Pakete an das Opfer übermittelt. Das ist notwendig, da der ARP-Cache auf den Remote-Systemen häufig geleert wird, wenn kein Traffic vorhanden ist.

In diesem Dialog können Sie die Spoofing-Adresse und das Zeitintervall konfigurieren. Im Bereich *Spoofing options* definieren Sie die Adressen, die Cain in das Ethernet ARP-Header der Poison-Pakete und die Rückgabe-Pakete schreibt. Mit einer solchen Konfiguration ist die ARP-Poison-Attacke vollständig anonym, da die reale IP-Adresse nicht über das Netzwerk übermittelt wird.

Wenn Sie diese Option aktivieren, sollten Sie einige Dinge beachten. Adressen-Spoofing, also das Fälschen der eigenen Adresse, ist nur dann möglich, wenn das Penetration Testing-System mit einem Netzwerk-HUB oder -Switch verbunden ist, bei dem die Funktion Port-Sicherheit nicht verwendet wird.

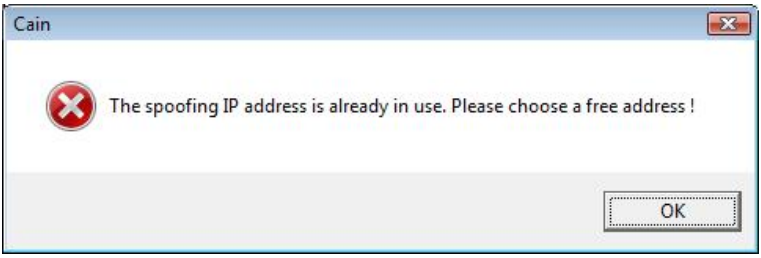
Ist die Port-Sicherheit aktiviert, wird die Quell-MAC-Adresse, die in jedem Ethernet-Frame enthalten ist, mit einer Liste gültiger MAC-Adrssen auf dem Switch verglichen. Da die gefälschte Adresse nicht in dieser Liste aufgeführt ist, wird die Verbindung unterbrochen.

Die gefälschte Adresse muss außerdem eine freie Adresse des aktuell verwendeten Subnetzes sein. Das ARP-Protokoll kann nicht Router oder VLAN mit anderen Adressen als denen des Subnetzes passieren. Es darf auch keine bereits verwendete Adresse zum Einsatz kommen, da es andernfalls zu einem Adressenkonflikt kommt.

Hier einige Beispiele für gültige Spoofing-Adressen:

Reale IP-Adresse	Subnetzmaske	Gültiger Bereich für die Spoofing-Adresse
192.168.0.1	255.255.255.0	Unbenutzte Adresse des Bereichs 192.168.0.2 - 192.168.0.254
10.0.0.1	255.255.0.0	Unbenutzte Adresse des Bereichs 10.0.0.2 - 10.0.255.254
172.16.0.1	255.255.255.240	Unbenutzte Adresse des Bereichs 172.16.0.2 - 172.16.0.14
200.200.200.1	255.255.255.252	Unbenutzte Adresse des Bereichs 200.200.200.2 - 200.200.200.3

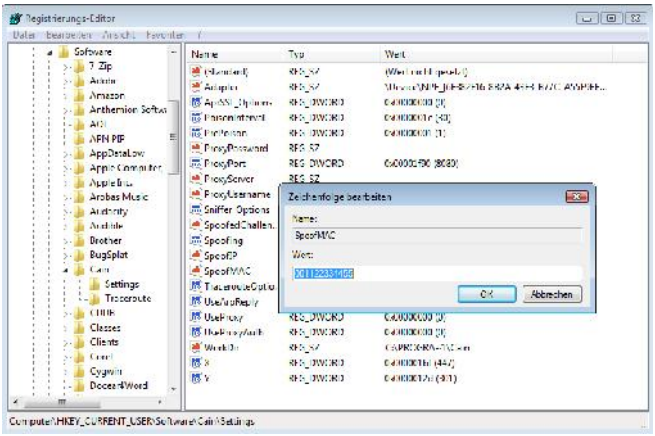
Wenn Sie eine Spoofing-Adresse verwenden wollen, führt Cain & Abel automatisch einen Test durch, wenn Sie auf *Apply* klicken, ob die Adresse bereits verwendet wird. Wird sie bereits verwendet, wird eine entsprechende Warnung ausgegeben.



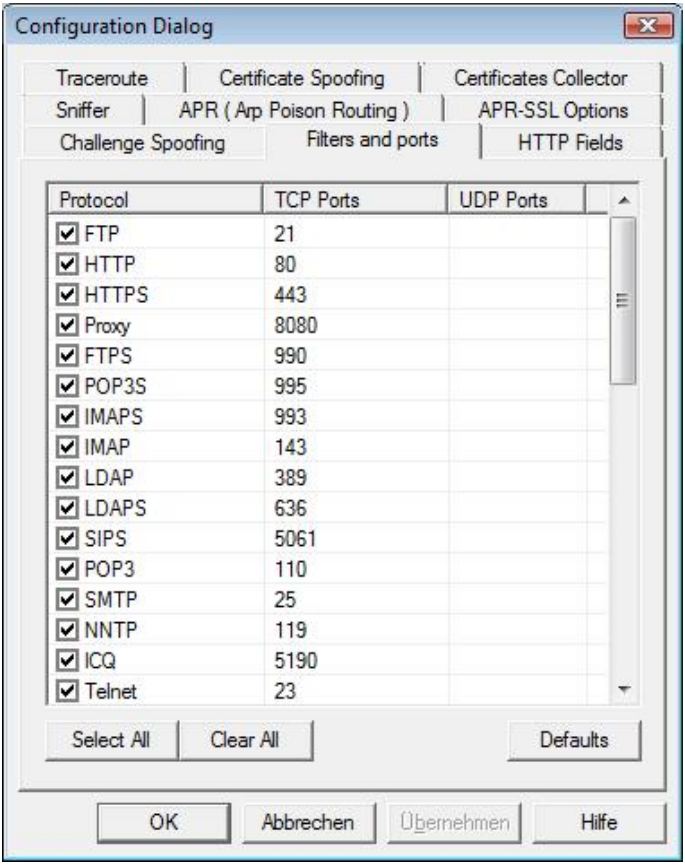
Die gewünschte Spoofing-Adresse ist bereits in Verwendung. Sie müssen eine andere Adresse verwenden.

Auch die von Ihnen verwendete MAC-Adresse darf bislang noch nicht in dem Netzwerk zum Einsatz kommen. Die Existenz von zwei identischen MAC-Adressen im gleichen Layer 2-LAN kann auf Seiten der Switches zu Verarbeitungsproblemen führen.

Daher müssen Sie beim Spoofen auch darauf achten, dass Sie eine noch nicht verwendete MAC-Adresse nutzen. Cain & Abel sieht hierfür standardmäßig den Wert *001122334455* vor. Allerdings kann diese Konfiguration nicht über die Cain-GUI geändert werden. Wenn Sie diesen Wert ändern wollen, ist das nur mit einem Eingriff in die Windows-Registry möglich. Ändern Sie im Schlüssel *HKEY_CURRENT_USER\Software\Cain\Settings* den Wert *SpoofMAC*.



Die gefälschte MAC-Adresse kann nur mit einem Eingriff in die Windows Registry geändert werden.



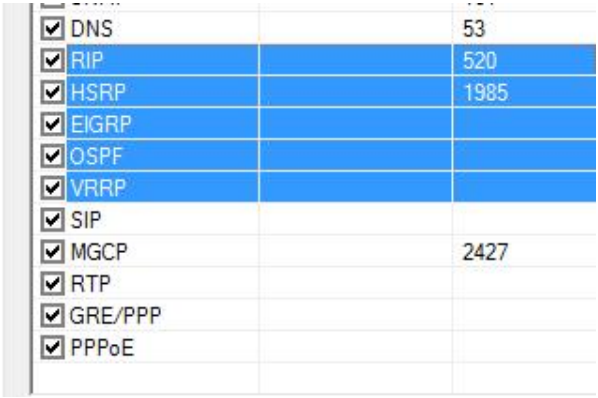
Die Filter- und Port-Konfiguration.

Sie können in der Cain & Abel-Konfiguration auch festlegen, welche Filter und welche Anwendungsprotokolle verwendet werden. Im Unterschied zu Sniffern wie Wireshark zeichnet Cain nicht den gesamten Traffic auf, sondern nur die Authentifizierungsinformationen. Wenn Sie dennoch an allen Daten interessiert sind, können Sie das mit Hilfe eines Telnet-Filters erzielen.

Die Sniffer-Filter sind so konzipiert, dass sie auch in Netzwerken, die gerade einer ARP-Poison-Attacke oder ähnlichen ausgesetzt sind, weiter korrekt arbeiten. Dazu verwendet Cain verschiedene Hilfsmittel, um all die relevanten Informationen im Klartext zu extrahieren, die für eine Analyse notwendig sind.

Verschiedene Authentifizierungsmechanismen verwenden einen Challenge-Response-Austausch. In diesem Fall muss der Austausch von verschiedenen Parametern analysiert werden, die vom Client an den Server und vom Server an den Client übermittelt werden.

Im unteren Dialogbereich können Sie auch die Analyse von verschiedenen Routing-Protokollen aktivieren und deaktivieren, beispielsweise von HSRP, VRRP, EIGRP, OSPF und RIP.



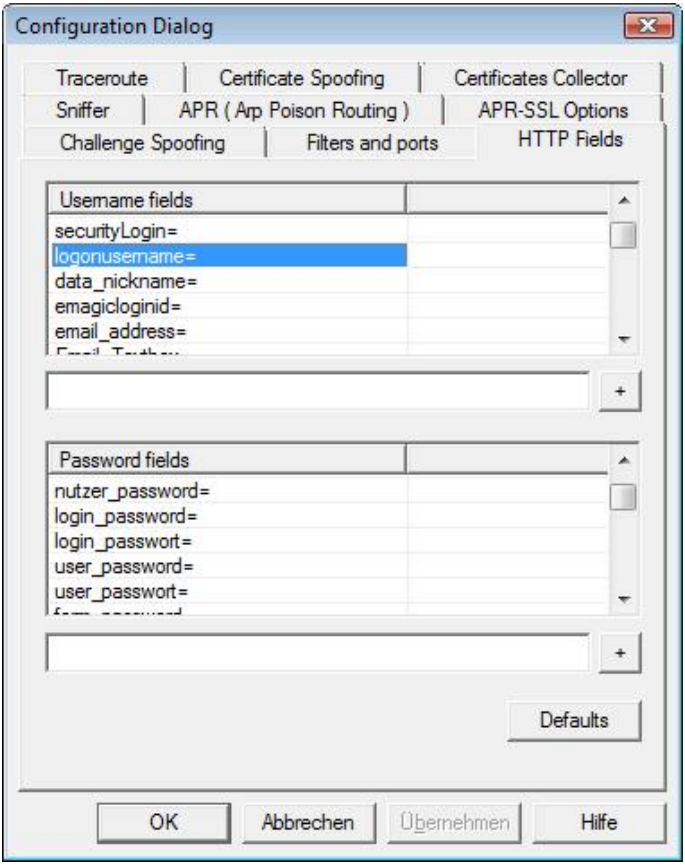
Die Filter für die Analyse der Routing-Protokolle sind standardmäßig aktiviert.

Cain & Abel kann sogar den Traffic analysieren, den in Verbindung mit einer typischen Web-Applikation entsteht. Für den Penetration Tester sind dabei insbesondere die Verarbeitung von Formulareingaben von Interesse. Die Verarbeitung und Übermittlung von Cookies und HTML-Formulareingaben kann mit diesen Filtern analysiert werden.

Cain & Abel prüft dabei alle Konfigurationen, die Sie hier hinterlegt haben bzw. die, die bereits angelegt sind. Für jedes Benutzernamenfeld werden alle Passwortfelder geprüft und die Eingaben auf dem Bildschirm ausgegeben.

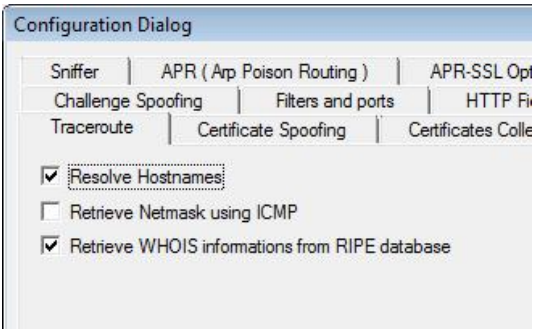
Anhand eines Beispiels wird deutlicher, was dabei konkret passiert. Die folgende Cookie-Konfiguration verwendet die beiden Felder *logonusername=* und *userpassword=* für die Authentifizierung. Wenn Sie diese beiden Felderkonfigurationen nicht auf der Registerkarte *HTTP Fields* hinterlegen, kann der Sniffer auch keine Zugangsdaten prüfen und extrahieren:

```
GET /mail/Login?domain=xxxxxx.xx&style=default&plain=0
HTTP/1.1

Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-excel, application/vnd.ms-powerpoint, app-
lication/msword, application/x-shockwave-flash, */*

Referer: http://xxx.xxxxxxx.xx/xxxxx/xxxx

Accept-Language: de

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; SV1; (R1 1.3); .NET CLR 1.1.4322)

Host: xxx.xxxxxx.xx

Connection: Keep-Alive

Cookie: ss=1; logonusername=user@xxxxxx.xx; ss=1; srclng=de;
srcdmn=de; srctrg=_blank; srcbld=y; srcauto=on; srcclp=on;
srcsct=web; userpassword=password; video=c1; TEMPLA-
TE=default;
```



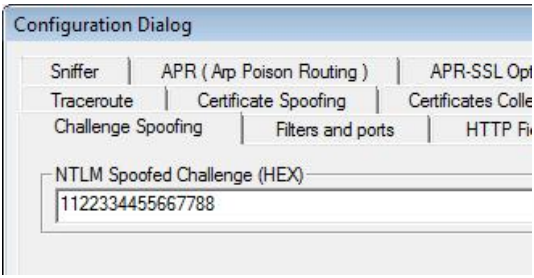
Die Konfiguration der HTTP-Feldeingaben.

Sie können eigene Feldkonfigurationen anlegen, indem Sie den Code in das Eingabefeld tippen und anschließend auf das Pluszeichen klicken. Sie können neue Felder für die Eingabe von Benutzernamen- und Passworteingaben hinzufügen.



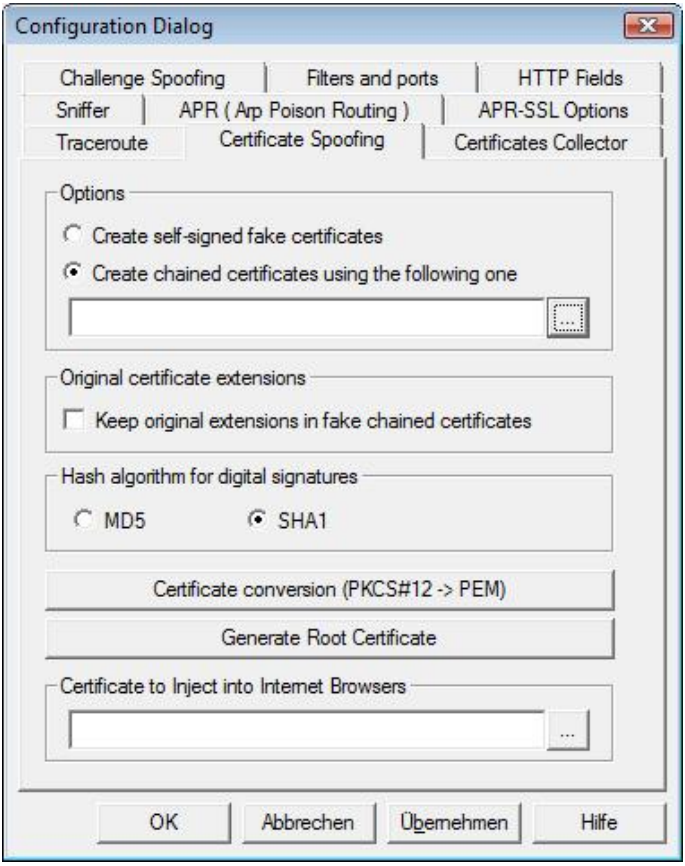
Die Traceroute-Einstellungen.

Auf der Registerkarte *Traceroute* können Sie drei Einstellungen vornehmen. Standardmäßig sind die Auflösung des Hostnamens (Resolve Hostnames) und das Einlesen von WHOIS-Daten zu jedem Hop aktiviert. Sie können zusätzlich auch die Netzmaske einlesen.



Die Konfiguration des NTLM Challenge-Wertes.

Auf der Registerkarte *Challenge Spoofing* können Sie den Wert für die NTLM-Authentifizierungspakete ändern. Diese Konfiguration ist für APR-Attacken relevant. Damit können Sie NTLM-Hashwerte in Verbindung mit Rainbow Tables knacken.



Die Funktionen für das Fälschen von Zertifikaten.

Die Funktionen auf der Registerkarte *Certificate Spoofing* machen das, was man anhand der Bezeichnung vermuten würde: Sie dienen dem Fälschen von Zertifikaten bzw. können auf Grundlage von bestehenden Zertifikaten abgewandelte generieren. Diese können dann beispielsweise für Man-in-the-Middle-Attacken oder für Browser-Injektionen verwendet werden. Mit der Konvertierungsfunktion können Sie außerdem eine Zertifikatdatei von PKCS#12 (PFX, P12) nach PEM (CRT) konvertieren.

Damit kennen Sie die wichtigsten Funkionen und Anpassungsmöglichkeiten, die das Programm Cain & Abel zu bieten hat. Als Nächstes schauen wir uns an, wie Sie konkret mit dem Sicherheitsspezialisten arbeiten.

Index

H

I

J

K

L

M

N

O

P

R

S

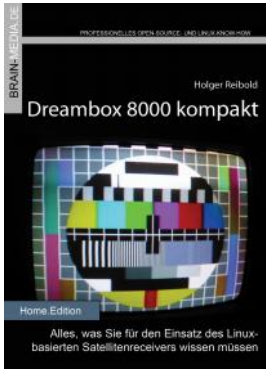
T

V

W

Z

Weitere Brain-Media.de-Bücher



Dreambox 8000 kompakt

Die Dreambox 8000 stellt ihre Vorgänger allesamt in den Schatten. Was Sie alles mit der Dreambox 8000 anfangen können, verrät Ihnen die Neuauflage unseres Dreambox-Klassikers. Mit einem Vorwort des Dream Multimedia-Geschäftsführers Karasu.

Umfang: 450 Seiten plus CD
ISBN: 978-3-939316-90-9
Preis: 29,80 EUR

X-Plane 10 kompakt

Der Klassiker unter den Flugsimulatoren geht in die zehnte Runde. Viele neue Funktionen und verbessertes Handling warten auf die Anwender. Kein Wunder also, dass die Fangemeinde wächst und wächst. Unser Handbuch beschreibt alles, was Sie für das Fliegen mit X-Plane wissen sollten.

Umfang: 430 Seiten
ISBN: 978-3-939316-96-1
Preis: 24,80 EUR

Audacity 2.0 kompakt

Audacity ist zweifelsohne das beliebteste freie Audioprogramm. Vom anfänglichen Geheimtipp hat sich der Editor zum Standard für die Aufzeichnung und Bearbeitung von Audiodaten gemausert. Das Vorwort steuert der ehemalige Core-Entwickler Markus Meyer bei.

Umfang: 306 Seiten
ISBN: 978-3-95444-027-6
Preis: 24,80 EUR

Evernote kompakt

Bei der alltäglichen Informationsflut wird es immer schwieriger, Wichtiges von Unwichtigem zu trennen, Termine und Kontakte zu verwalten. Mit Evernote können Sie diese Flut bändigen und Ihren Alltag optimieren. "Evernote kompakt" vermittelt das notwendige Know-how für den Einsatz von Evernote auf Ihrem Desktop, Smartphone und online.

Umfang: 320 Seiten
ISBN: 978-3-95444-098-6
Preis: 22,80 EUR

Fire TV kompakt

Mit Fire TV hat Amazon eine tolle kleine Box für das Online-Entertainment auf den Markt gebracht, die für wenig Geld die gesamte Palette der Internet-basierten Unterhaltung abdeckt. In diesem Handbuch erfahren Sie, was Sie alles mit der kleinen Box anstellen können.

Umfang: 182 Seiten
ISBN: 978-3-95444-172-3
Preis: 16,80 EUR

Magento SEO kompakt

Magento ist die Standardumgebung für den Aufbau eines Online-Shops. Doch damit Sie mit Ihren Shop-Angebot auch im Internet wahrgenommen werden, müssen Sie ein wenig die Werbetrommel rühren und den Shop für Google & Co. optimieren. Mit wenigen Handgriffen machen Sie Ihren Online-Shop SEO-fest und maximieren Ihre Verkäufe.

Umfang: 100 Seiten
ISBN: 978-3-95444-098-6
Preis: 14,80 EUR

Wireshark kompakt

Wireshark ist der mit Abstand beliebteste Spezialist für die Netzwerk- und Protokollanalyse. In diesem Handbuch lernen Sie, wie Sie mit dem Tool typische Administratoraufgaben bewältigen. Das Buch beschränkt sich dabei auf die wesentlichen Aktionen, die im Admin-Alltag auf Sie warten, und verzichtet bewusst auf überflüssigen Ballast.

Umfang: 170 Seiten
ISBN: 978-3-95444-176-1
Preis: 16,80 EUR

Scribus 1.5 kompakt

Scribus ist längst ein ebenbürtiger Gegenspieler von InDesign & Co. In unserem Handbuch erfahren Sie alles, was Sie für den erfolgreichen Einstieg wissen müssen.

460 Seiten Praxis-Know-how. Dazu viele Tausend ClipArts und Schriften zum kostenlosen Download.

Umfang: 460 Seiten
ISBN: 978-3-95444-124-2
Preis: 27,80 EUR

Weitere Titel in Vorbereitung

Wir bauen unser Programm kontinuierlich aus. Aktuell befinden sich folgende Titel in Vorbereitung:

- Android Forensik
- Android Security
- Alfresco 5.0 kompakt
- WordPress 4.x kompakt
- Smart Home kompakt
- Das papierlose Büro

Plus+

Plus+ − unser neues Angebot für Sie ... alle E-Books im Abo. Sie können 1 Jahr lang alle Brain-Media-Bücher als E-Book herunterladen und diese auf Ihrem PC, Tablet, iPad und Kindle verwenden − und das ohne irgendwelche Einschränkungen. Das Beste: Plus+ schließt auch alle jene Bücher ein, die in diesem Jahr noch erscheinen.

Und das zum Sonderpreis von 29 Euro! Ein unschlagbares Angebot!

Auf unserer Website steht ein detaillierter Überblick aller Titel im PDF-Format zum Download bereit (ca. 6,2 MB), der bereits zu Plus+ gehörende Titel aufführt und die in naher Zukunft hinzukommen.