PROFESSIONELLES INTERNET- UND OPEN-SOURCE-KNOW-HOW

Holger Reibold



Security.Edition

Einstieg in das Penetration Testing mit dem Windows-Klassiker **Holger Reibold**

Cain & Abel kompakt



2

Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Verlags ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form durch Fotokopien oder ein anderes Verfahren zu vervielfältigen oder zu verbreiten. Dasselbe gilt auch für das Recht der öffentlichen Wiedergabe. Der Verlag macht darauf aufmerksam, dass die genannten Firmen- und Markennamen sowie Produktbezeichnungen in der Regel marken-, patent- oder warenrechtlichem Schutz unterliegen.

Verlag und Autor übernehmen keine Gewähr für die Funktionsfähigkeit beschriebener Verfahren und Standards.

© 2015 Brain-Media.de Herausgeber: Dr. Holger Reibold Umschlaggestaltung: Brain-Media.de Satz: Brain-Media.de Coverbild: Brain-Media.de Korrektur: Theresa Tting

Inhaltsverzeichnis

VO)	RWORT 7
1	PENETRATION TESTING MIT CAIN & ABEL9
1.1	Typischer Einsatzbereich10
1.2	Installation13
1.3	Cain & Abel konfigurieren22
2	ABEL IN DER PRAXIS
2.1	Die Konsole
2.2	Hash-Werte auslesen
2.3	Local Security Authority37
2.4	Routen inspizieren
2.5	Offene Ports40
3	CAIN KENNENLERNEN43
3.1	MAC-Adressenscanner45
3.2	Netzwerk einlesen
3.3	Einblick in die Registry48
3.4	Promiscuous-mode Scanner49
3.5	Services steuern

3.6	Benutzer und Freigaben52
3.7	Traceroute
3.8	WLANs prüfen55
4	PASSWÖRTER KNACKEN57
4.1	Angriffstypen
4.2	Wörterbuchattacke mit Cain63
4.3	Kryptografische Analyse65
4.4	LM & NTLM knacken68
4.5	PWL-Dateien knacken71
4.6	WLAN-Traffic dekodieren72
4.7	MySQL-Datenbanken74
5	SNIFFEN MIT CAIN75
5.1	APR in der Praxis79
5.2	APR-HTTPS
5.3	Certificates Collector
5.4	Voice over IP
INE	DEX

WEITERE BRAIN-MEDIA.DE-BÜCHER	93
Weitere Titel in Vorbereitung	96
Plus+	96

6

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 8

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 Win-Pcap-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.

File View Configure	Tools Help
Cached Passwords Cached Passwords LSA Secres Windows Mail Passwords Windows Mail Passwords Lialup Passwords Edit Boxes - Therboxes Credential Manager - Windows Voult	Press the + button on the toolbar to dump the Fretected Storage
tit.p://www.csi.d.it	Protected Storage

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.

		enere.		
 All host 	s in my sul	bnet		
Range				
- From-				
192	. 168 .	2	. 1	
-To-				
192	. 168 .	2	. 254	
ARP TO ARP TO ARP TO ARP TO ARP TO ARP TO ARP TO ARP TO	est (Broad est (Broad est (Broad est (Broad est (Group est (Multic est (Multic s (Multic s	canne cast 3 cast 11 cast 8- bit) ast gro ast gro ast gro	' I-bit) S-bit) bit) up 0) up 1) up 3)	

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.

Passwords Timestemp POP3 server Client Username Password # FTP (0) 15/07/2015 118/34/250110 192.1682.105 192.1682.105 192.1682.105 # HTTP (0) 15/07/2015 118/322 188/94/250110 192.1682.105 192.1682.105 # DE LUDAP (0) 15/07/2015 12.15:01 188/94/250110 192.1682.105 192.1682.105 # POP3 (6) 15/07/2015 12.15:01 188/94/250110 192.1682.105 192.1682.105 # POP3 (6) 15/07/2015 12.15:01 188/94/250110 192.1682.105 192.1682.105 # POP3 (6) 15/07/2015 12.15:01 188/94/250110 192.1682.105 192.1682.105 # SMF (0) 15/07/2015 12.23:32 188/94/250110 192.1682.105 192.1682.105 # Tok (0) FT SK (0) 15/07/2015 12.23:32 188/94/250110 192.1682.105 192.1682.105 # Tok (0) FT SK (0		🥫 📕	Wireless	📟 🚾 📾 🚍	er 🧑 Tracerout	🛊 🖳 🕂 🥹 💀	🖻 🍻 🙃 sẫi 韻筆 翻
- ↑ FTP (0) T5/07/2015 - 11:4:07 188 94 250.110 192.168.2.105 → HTTP (0) 15/07/2015 - 11:4:32 188 94 250.110 192.268.2.05 → IMAP (2) 15/07/2015 - 12:15:01 188 94 250.110 192.268.2.05 → POP3 (6) 15/07/2015 - 12:15:01 188 94 250.110 192.268.2.05 → POP3 (6) 15/07/2015 - 12:2:32 188 94 250.110 192.268.2.05 → Tainet (0) - → Tainet (0) - → TS (0) -	AuthType	Password	Username	Client	POP3 server	Timestamp	Passwords
Image: Physical Science	Clearl ext			192.168.2.105	188 94 250.110	15/07/2015 - 11:44:02	- CO (0)
IMAP (2) 15/07/2015 12:15:01 188 94 250 110 192:168.2:105 IBLDAP (0) 15/07/2015 - 12:15:01 183 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:02 183 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:02 188 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:02 188 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:32 188 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:32 188 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:32 188 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:32 188 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:32 188 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:32 188 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:32 188 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:32 188 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:32 188 94 250 110 192:168.2:105 IMAP (2) 15/07/2015 - 12:2:32 188 94 250 110	ClearText			192.168.2.105	188 94 250 110	15/07/2015 - 11:/3:32	HTTP (0)
→ □ □	ClearText			192.168.2.105	188 94 250 110	15/07/2015 12:19:01	IMAP (2)
••••••••••••••••••••••••••••••••••••	ClearText			192.168.2.105	188 94 250 110	15/07/2015 - 12:19:01	
Image: Style (in) 15/07/2015 - 12:23:32 188 94 250.110 192.168.2.105 Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in) Image: Style (in)	ClearTest			192.168.2.105	188 94 250 110	15/07/2015 - 12:23:02	(12: 0.002 (6)
Image: Second	ClearText			192.168.2.105	188 94 250 110	15/07/2015 - 12:23:32	
₩ VNC (0) ➡ TDS (0) ➡ TNS (0) ➡ SWTP (0) ♥ NNTP (0) ♥ NTP (0)							Telnet (0)
TDS (0) Image: Strate (0) Image: Strate (0) Image: Strate (0)							VNC (0)
-∰ TNS (0) -∰ SMTP (0) -∰ NNTF (0) -∰ DX F/KPC (0)							TDS (0)
SVTP (0) DX F/RPC (0)							TNS (0)
NNTF (0) NL F/RPC (0)							IN TTN E
							NINTE (0)
No second a second							
							NY NCK LE D A L (0)
With Kerbs-PreAuth (0)							() MSKerbS-PreAuth (0)

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/steelcentralnpm/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.

	a s ∐ 51 ⊧ ∎ 1 ⊪						
📮 Dienste (Lokal)	O Denis (coluit						
	Abol	Name	Baschraibung	Status	Starttyp	Anmeiden al	s
	Don Diener geneen	G Abd	Adaba Asmba	Castrates	Automa	Lokales Syste	271 C
		Gadabe Flash Playe.	Adode Armoa.	hestoner	Annoma	Treates syar	m
		🤹 allierse offerslip eSQI	Eigenscheiten vo	n Abel (Lob	aler Compu	Jea)	
		Qualities of orms!	Algemen Anny	elden Wied	enterste ung	Aphäng okeiten	1
		Anwendungserlah.	Monatmomo:	Rod			
		Anwendungsinfor.	Anzeigename.	Abel			
		Arbeitsstationsdie	Heatheritung:				-
		Aufgabenplanung		1			
		Automatische Ko.	CAProgram Bio	ete avCaln\Aba	nen		
		📮 Fasisfiltermodul	Danttyp	Automat	e.t.		•
		Economic House Benelikarian Marine		Louis and			100
		ErVNSv:	Uter Jane L	an sa huu	eren der Star	polioner ur Dier	Ritt
		CNS-Schlössehsol.	Ner ddalus	beendel	-		
		COM+-Elegnissy	Raten	Deen	den	Anhaten	Fortsetzen
		Computerbrowser Computerbrowser Computer Pro	Sie konnen die wenn der Diens	Sialparanal I von her au	er wigeben, s s gestertet wi	lie ober commerce Id	wenten waten,
		Designs	Startpartmetter				
		DHCP Client	-				
		 Diagnosed enthosy Usan according to 			ок	Abbreche	n Cosmehmen

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.

🗅 📦 😔 📩 連 明 🗎	+ @ b	R. 2	COUL 1987 Worder - 55 Ocean	
 Lentre Network Lintre Network WORKGROUF WORKGROUF All Computers CHEF MUBLI Apple File Servers Dial-In Servers Dial-In Servers Domain Controllers Novell Servers SQL Servers There Servers Time Servers Unck List 		Credentials required User ane Insiger Pastword Oxee	Version Comment 6.0 6.1 0K Carual	

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.

Network	Service Name	Display Name	Status	Start Type	File
icrosoft Windows Network	Abel	Abel	Running	Auto	C:\
WORKGROUP	SteLookupSvc	Anwendungserfahrung	Running	Manual	C:\
- All Computers	Stal G	Gatewaydienst auf Anw	Stopped	Manual	C:\
	State AppIDSvc	Anwendungsidentität	Stopped	Manual	C:\
🖻 📃 MOBIL1	Standard Appinfo	Anwendungsinformatio	Running	Manual	C:\
⊢ I Chef\Administrator	aspnet_state	ASP.NET State Service	Stopped	Disabled	C:\
Groups	StherosSvc	AtherosSvc	Running	Auto	C:\
🗄 🎯 Registry	🐺 AudioEndpoi	Windows-Audio-Endpu	Running	Auto	C:\
Services	Standio Srv	Windows-Audio	Running	Auto	C:\
- 🔂 Shares	Stanst SV 4	ActiveX-Installer (AxInst	Stopped	Manual	C:\
🛄 🕵 Users	BDESVC	BitLocker-Laufwerkversc	Stopped	Manual	C:\
Apple File Servers	8 REF	Raciefiltermodul	Running	Auto	CA

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 RA-DIUS 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

🖌 Cirganisteren 👻 🗐 Ansienten 🔹 🕘	Brennen			_	
inkfavoriten	Name	Änderungsdatum	Тур	Größe	
Bilder Musik 2 Juletzt geindert Weitere >>	Univer Winntgen Uvordists B0211	30.08.2015 20/44 30.08.2015 20:44 30.08.2015 20:44 15.07.2015 11:39 07.04.2014 09:45	Dateiordner Dateiordner Uateiordner LST-Datei Programmbibliot	0 KB 17 KD	
Danner	Abd J larg Abd J larg Abd J larg Abd J larg Abd Add Larg Abd Add Larg Abd Add Add Larg Abd Add Add Add Add Add Add Add Add	07.04.2214 0963 07.04.2214 0967 07.04.2214 0964 07.04.2214 0961 07.04.2214 0961 07.04.2214 0961 07.04.2214 0961 07.04.2214 0961 15.07.2215 11.39 07.04.2214 0963 07.04.2214 0963 07.04.2215 11.39	SIG-Detei Anwendung SIG-Detei Programmibiliotuu SIG-Detei Anwendung SIG-Detei LST-Datei Kompilierte ITMILL LST-Datei Anwendung SIG-Detei LST-Datei LST-Datei LST-Datei	1 KB 29 KR 1 KU 255 KB 1 KN 251 KB 1 KB 0 KU 0 KB 1.344 KB 1.344 KB 1 KU 0 KB 0 KB	

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.

Challenge Spooting	Filters and ports	HTTP Fields
Traceroute Certificate	Spoofing Ce	rtificates Collector
Sniffer APR (Arp Poiso	n Routing)	APR-SSL Options
Adapter	IP address	Subnet Mask
Device\NPF_{05B7266	192.168.2.107	255.255.255.0
Device\NPF_{A0D856	0.0.0.0	0.0.0.0
Device\NPF_{6F382F1	192.168.2.117	255.255.255.0
Device \NPF_{FCCDDE	0.0.0.0	0.0.0.0
Device\NPF_{8B2F506	0.0.0.0	0.0.0
4 III III		•
Current Network Adapter	1D-44CC-8396-616/	A175D61AA}
WARNING !!! Only e	ethernet adapters su	pported
Options		

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.

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

Hier einige Beispiele für gültige Spoofing-Adressen:

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.

Sniffer APR (Challenge Spoofing	Arp Poison Routing) Filters and ports	APR-SSL O	ptions Fields
Protocol	TCP Ports	UDP Ports	
FTP	21		
HTTP	80		
HTTPS	443		E
Proxy	8080		
FTPS	990		
POP3S	995		-
MAPS	993		
IMAP	143		
LDAP	389		
LDAPS	636		
SIPS	5061		
POP3	110		
SMTP	25		
NNTP	119		
	5190		
✓ Telnet	23		
Salact All	aar All	Defa	ulte

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.

27

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.

	1.7.0
✓ DNS	53
RIP	520
HSRP	1985
EIGRP	
✓ OSPF	
VRRP	
SIP	
MGCP	2427
RTP	
GRE/PPP	
PPPoE	

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, application/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.xxxxx.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=cl; TEMPLA-TE=default;

29

Traceroute Certificate Spoofing	Certificates Collector
Challenge Spoofing Filters and	ports HTTP Fields
Usemame fields	
securityLogin=	
logonusemame=	
data_nickname=	
emagicloginid=	
email_address=	
	*
Password fields	<u> </u>
nutzer_passwo <mark>rd</mark> =	
login_password=	
login_passwort=	
user_password=	
user_passwort=	
	+
	Defaults
	-

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.

Sniffer	APR (Arp	Poison Routing)	APR-SSL O
Traceroute	Certifi	cate Spoofing	Certificates Co
Challenge S	poofing	Filters and port	s HTTP
Challenge S	poofing	Filters and port	s HTT
		100 and 100 and	
NTLM Spoo	ofed Challeng	e (HEX)	

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.

31

Challenge Spoof	ing Filters and port	s HTTP Fields
Sniffer AF	R (Arp Poison Routing) Certificate Spoofing	APR-SSL Options Certificates Collector
Options		
C Create self-si	gned fake certificates	
· Create chain	ed certificates using the foll	owing one
Hash algorithm for	l extensions in fake chained or digital signatures	d certificates
C MD5	SHA1	
< MD5		
Certifi	cate conversion (PKCS#12	? -> PEM)
Certifi	cate conversion (PKCS#12 Generate Root Certificate	2 -> PEM)
Certifi Certificate to Inje	cate conversion (PKCS#12 Generate Root Certificate ct into Internet Browsers —	e
Certifi Certificate to Inje	cate conversion (PKCS#12 Generate Root Certificate ct into Internet Browsers —	e
Certifi Certificate to Inje	icate conversion (PKCS#12 Generate Root Certificate ct into Internet Browsers	e

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

Α

Abel	15,	33
Abel.exe		15
Abel-Konsole		34
Abel-Untermenü		34
Access Point		55
Adam und Eva		33
Adapter		23
Adressbereich		11
Adressenkonflikt		24
AirPcap), 14,	55
Algorithmus		57
Angriffstyp		58
Angriffsziel		80
APR-HTTPS		84
ARP	23,	75
ARP Poison Routing		23
ARP-Cache		79
ARP-Paket		45
ARP-Poison-Attacke		23
ARP-Spoofing), 11,	77
ARP-Tabelle		11
Authentifizierung		27
Authentifizierungsmechanismus .		27

В

Benutzer	52
Benutzerdaten	69
Benutzername29	9, 52
Berechtigung	15
Bibliothek	17
Boot Key	70
Brute-Force	9, 58
BSSID	72

С

Cain & Abel	9
Cain & Abel-Konfiguration	26
Cain.exe	13
Certificates Collector	86
Challenge-Response	27
Cookies	27
Cracker1	17, 37
CRT2	21, 31

D

Deinstallationsprogramm	22
Dienstmanager	50
Domain Controller	47
Drucker	47
DSN	74

Ε

F

Firewall	13
Formulareingabe	27
Freigabe	52
Full-Routing	83

G

Gateway	23
Geschwindigkeit	23
Gruppenrichtlinie	35
GUI	13

Н

Hacker	7
Half-Routing	83
Handshake	10
Hash	10
Hash-Wert	36
Hijacking	82
Нор	39
Host-Liste	11
HTML	27, 60
HTTPS	77
HUB	24

I

ICMP	54
IDS	49
Infrastruktur	7
Infrastrukturkomponente	7
Injektion	31
Installation	13
Installationsprogramm	14
Installationsverzeichnis	17
Intrusion Detection System	49
IP-Adresse	23
ipconfig	35

J

Janusangriff	11
John the Ripper	10

Κ

Klartext	13
Konfiguration	23
Konsole	34
Korek-Attacke	73
Kryptografische Analyse	65

L

LAN	View 8	2
-----	--------	---

Layer 2	25
LM	68
LM Hash	36
Local Security Authority	37
LSA-Secrets	9

Μ

MAC-Adresse	23, 24
MAC-Adressen-Scanner	45
MAC-Information	45
Man-in-the-Middle	9, 11
Metrik	
MySQL-Datenbank	74

Ν

netstat	40
Netzmaske	23
Netzwerk einlesen	47
Netzwerkadapter	11
Netzwerkanalyse	43
Netzwerkfreigabe	53
Netzwerk-Scan	47
Netzwerkziel	
NT Hash	
NT Hashes Dumper	70
NTLM	30, 68

0

ODBC-Treiber	74
Offener Port	40
OphCrack	66

Ρ

Paketfilter	76
Passwort	10
Passwort knacken	57
Passwort-Cracker	57
Passworteingabe	29
Passwortfilter	76
Passwortlänge	36

PCAP-Format	72
Penetration Testing	. 9
Performance-Monitor	35
PFX	31
PKCS	31
Poisoning	81
Port	41
Port-Konfiguration	26
Promiscuous-mode Scanner	49
Protokollfilter	76
Prozess-ID	40
PRW-Attacke	73
PWL-Dateien	71

R

Rainbow Tables-Generator	67
Rainbow Tables	9, 65
RainbowCrack	66
RDP	9
Registry	48
Registry Browser	49
Remote-Client	16
Remote-Konsolenzugriff	9
Remote-Rechner	17
Route-Konfiguration	39
Route-Manager	38
Routen inspizieren	38
Router	12
Routing	27

S

SAM-Datei	69
Schlüsselkategorie	60
Schnittstelle	39
Server	47
Servicename	51
Services steuern	50
SID	48
Sniffen	75
Sniffer-Filter	26
Sniffer-Funktionen	19
Snifferleiste	43

Software-Manager	22
Spoofing	24
SSH-1	77
Standardleiste	43
Starttyp	51
Status	41
Subnetz	11
Switch	24
Syskey Decoder	70
Systemanforderungen	13

Т

Tastenkürzel	44
TCP/UDP	9
TCP-Verbindung	40
TCPview	81
Telnet	78
Telnet-Session	78
Terminal-Server	47
Traceroute	30, 54
Traffic-Aufzeichnung	14

V

Verbindungsmanager	56
Verschlüselungsmethode	57
Verschlüsselungstyp	72
Voice over IP	86

W

WAN View	82
WAN-Traffic	82
Web-Applikation	27, 74
WEP	55
WHOIS	54
Windows DDK	55
Windows-Dienst	15
Windows-Netzwerk	9
Windows-Registry	25, 48
WinPcap	9, 14
Winrtgen	67
Wireshark	12, 78

WLAN	55
WLAN prüfen	55
WLAN-Traffic	72
Wörterbuch-Attacke	9, 63
Wörterliste	63
WPA	10, 55
WPA-PSK	10

Ζ

Zeichensatz	.59
Zertifikat31,	85
Zertifikat fälschen	.31

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

BUILDER BUILDE DE SAUSAUER FORM-ROUTE Iniger Reihouri A-Plane 10 kompakt Uniger Reihouri Builger Reihouri Builger Reihouri Builger Reihouri Builger Reihouri Builger B

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







ie in die Suchnaschinenoptimierung to ein und maximieren Ihre Verkäufe





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.