# Passwörter knacken

**Dieser Beitrag ist etwas veraltet und sollte überarbeitet werden**

Seit dem Inkrafttreten des neuen Urheberrechtsgesetzes im Jahr 2003 ist es in Deutschland nicht mehr erlaubt, Kopierschutzmaßnahmen zu umgehen (§ 95 a Abs. 1 Urheberrechtsgesetz). Nicht nur der Vorgang ist strafbar, sondern bereits Herstellung, Einfuhr, Verbreitung und Verkauf von Kopierschutzknackern, ebenso wie deren Bewerbung (§ 95 a Abs. 3 Urheberrechtsgesetz).

**Nur für den Angriff auf eigene Dateien sind Hacker-Tools erlaubt.**
**Hier wird weder für diese Programme geworben noch können diese hier herunter geladen werden.**
**Sie werden auch keine Links zu diesen Programmen finden. Es handelt sich nur um Infos um sich**
**vor solchen Programmen zu schützen.**

# Überblick Passwort-Knacker

| | IE | Outlook | Office | PDF | Windows-Ameldung | WLAN | ZIP |
|---|---|---|---|---|---|---|---|
| Password-Finder 2.2 | x | x | | | | x | |
| Passware Kit Enterprise | x | x | x | x | x | | x |
| Distributed Password Recovery | | | x | x | x | x | |
| Offline NT PW & Registry Editor | | | | | x | | |
| Ophcrack | | | | | x | | |
| Protected Storage Passview | x | x | | | | | |
| Pst Password | | x | | | | | |
| PDF Unlocker | | | | x | | | |
| Aircrack-ng | | | | | | x | |

Diese Tabelle dient dem Überblick und erhebt keinen Anspruch auf Vollständigkeit.
Passwort Knack Programme dürfen nur für eigene Dateien benutzt werden

---

**Aircrack-ng 1.0-rc1**
WLANs sollte man tunlichst verschlüsseln, damit kein Fremder Schindluder treiben kann. Das alte WEP-Verfahren ist dafür allerdings ungeeignet: Die neue Version von Aircrack-ng ermittelt binnen Sekunden den Schlüssel eines WEP-geschützten Funknetzes. Schlüssel des sichereren WPA-Verfahrens kann Aircrack-ng nur durch Ausprobieren sämtlicher Buchstaben- und Zahlenkombinationen herausbekommen. Das dauert lange und ist bei komplexen Passwörtern sogar aussichtslos.

---

**Anydvd (HD) 6.4.5.0**
Anydvd klinkt sich ins Betriebssystem ein und entschlüsselt im Hintergrund Video-DVDs. In der neuen Version wurde der Knack-Algorithmus weiter verfeinert. Die HD-Variante von Anydvd unterstützt auch Blu-Ray und HD-DVD. Durch den Einsatz von Anydvd sieht es für Player-Software und Kopier-Utilities so aus, als wäre der Film unverschlüsselt. Dadurch wird es möglich, die DVD entweder 1:1 zu kopieren oder das Videomaterial von einem legal erhältlichen Recodier-Tool herunterrechnen zu lassen, etwa von der Shareware Clonedvd 2

---

**Cain & Abel 4.9.17**
Mit Cain & Abel lässt sich Datenverkehr in einem lokalen Netz belauschen. Das Tool ist in der Lage, die Zuordnungstabelle im Router oder Switch so zu ändern, dass es die Datenpakete abfangen kann. Über einen Trick lassen sich auch verschlüsselte HTTPS-Verbindungen belauschen. Cain & Abel zeigt nicht den rohen Datenverkehr an, sondern pickt sich die für Hacker relevanten Informationen heraus, zum Beispiel Benutzernamen, Passwörter und VoIP-Gespräche.

---

**DVD Shrink 3.2.0.15**
Mit DVD Shrink lassen sich manche kopiergeschützte DVDs duplizieren. Dabei umgeht die Software die unsichere CSS-Verschlüsselung und einige zusätzliche Schutzmethoden. Mit aktuellen Verfahren kommt DVD Shrink nicht zurecht, ebenso wenig wie mit HD-DVDs und Blu-Ray-Disks. Beliebt ist das Programm, weil es DVD-9-Filme auf DVD-4-Rohlingen unterbringt, indem es die Bit-Rate herunterschraubt und nicht benötigte Tonspuren sowie Extras weglassen kann. DVD Shrink entfernt auch den Regionalcode und eventuelle Restriktionen in der DVD-Benutzerführung.

---

**Distributed Password Recovery**
Elcomsoft Distributed Password Recovery 2.60.176 ist ein Hochleistungs-Tool zum Entschlüsseln von Passwörtern. Das Besondere an der Software: Sie kann die Rechenleistung von Grafikkarten mit Nvidias GPU Geforce 8 und 9 einbeziehen. Diese Graphical Processing Units sind bei Kryptografie-Berechnungen aktuellen CPUs mehrfach überlegen. Zudem ist das Programm in der Lage, die Berechnung im Netzwerk zu verteilen. Das Tool kann unter anderem Office-Dokumente und Windows-Passwörter knacken.

---

**Internet Worm Maker Thing 1.1**
Mit diesem Baukasten für Internet-Würmer kann sich ein Täter erschreckend einfach einen Schädling zusammenklicken. Damit ist das Tool eindeutig illegal. Der Täter bestimmt, welche Aktionen der Wurm durchführen soll. Dazu zählen neben harmloseren Dingen wie dem Vertauschen der Maustasten auch gefährlichere, zum Beispiel das Deaktivieren von Antiviren-Programmen und das Nachladen von Dateien. Auch die wurmtypischen Verbreitungs-Optionen sind vorgesehen. Wer einen Wurm in Umlauf bringt, muss mit ernsthaften rechtlichen Konsequenzen rechnen.

---

**Offline NT PW & Registry Editor**
Offline NT Password & Registry Editor erfüllt nur einen simplen Zweck, den aber sehr effektiv: Es

ermöglicht, das Anmelde-Passwort von Windows XP und Vista auszuhebeln. Der Rechner muss über ein CD/DVD- oder ein Diskettenlaufwerk verfügen, über das er gebootet werden kann, denn das Tool kommt in Form eines bootfähigen CD- und Disketten-Images. Darin verbirgt sich ein Mini-Linux auf Kommandozeilen-Basis. Mit ein paar Eingaben ist das XP- oder Vista-Passwort entweder geändert oder gelöscht. Das ursprünglich gesetzte Passwort lässt sich nicht ermitteln.

---

**Ophcrack Live-CD 2.0.1**
Die Ophcrack Live-CD ist eine Alternative zum Offline NT Password & Registry Editor. Der Unterschied liegt darin, dass man damit die gesetzten Passwörter nicht löschen und ersetzen, sondern ermitteln und anzeigen lassen kann. Ophcrack wird insbesondere dann eingesetzt, wenn jemand Zugang zu einem fremden PC erlangen will, ohne dass der Besitzer dies hinterher bemerkt. Das Tool nutzt die relativ neue Methode des Passwort-Knackens per Rainbow Tables.

---

**Passware Kit Enterprise 8.3**
Passwörter wiederherstellen und Dokumente entschlüsseln – darauf ist das kostenpflichtige Passware Kit Enterprise spezialisiert. Enthalten sind 25 Module, die jeweils für ein Dateiformat, eine Anwendung oder ein Software-Paket bestimmt sind. So lassen sich die Passwörter von Office-Dokumenten ebenso finden wie die von PDF-Dateien oder Datenbanken. Je nach Dokumentformat, Komplexität des Kennworts und verfügbarer Rechenleistung kann die Suche Wochen oder Monate dauern.

---

**Perfect Keylogger Lite 1.15**
Keylogger wie dieser werden benutzt, um Tastaturanschläge anderer Personen aufzuzeichnen. Dadurch lassen sich PC-Aktivitäten nachvollziehen und Passwörter ausspähen. Damit das Opfer nichts von der Abhöraktion bemerkt, lässt sich Perfect Keylogger Lite unsichtbar schalten. Nur mit dem richtigen Tastaturkürzel kann derjenige, der das Programm installiert hat, es wieder sichtbar machen und die Protokolldatei einsehen. Darin steht, in welchem Programm um welche Uhrzeit welche Tastatureingaben gemacht wurden.

---

**Protected Storage Passview 1.63**
Im Bereich Protected Storage in der Windows-Registrierdatenbank werden Benutzernamen und Passwörter von bestimmten Anwendungen verschlüsselt und zum Teil zusätzlich noch versteckt abgelegt. Die Software Protected Storage Passview kann die sehr schwache Verschlüsselung knacken, die Zugangsdaten anzeigen und sie gesammelt in eine Textdatei speichern. So macht das Programm zum einen Login-Daten sichtbar, die im Internet Explorer gespeichert sind – also Passwörter für Websites. Zum anderen zeigt es die in Outlook und Outlook Express hinterlegten Login-Daten für Mailpostfächer an.

---

**Pst Password 1.11**
Dieses Tool knackt den Passwortschutz von Outlook 97, 2000, XP, 2003 und 2007. Wenn die Mail-Software auf dem System installiert ist, ermittelt das Tool selbständig, wo die Mail-Datenbank(en) mit der Endung .PST liegen. Wenn Outlook nicht installiert ist, lässt sich eine PST-Datei, die zum Beispiel

von einem anderen Rechner stammt, manuell öffnen. Da der Passwortschutz in den aufgeführten Outlook-Versionen sehr schwach ist, benötigt das Tool keine lange Rechenzeit.

---

**Shark 3.1**
Rechner übers Internet fernsteuern – das ist der Einsatzweck von Shark. Anders als legale Remote-Desktop-Software wie Ultravnc ermöglicht Shark das aber auch ohne Kenntnis und Einwilligung des Nutzers, der vor dem entfernten PC sitzt. Die Server-Komponente von Shark tarnt sich auf vielerlei Arten, um unerkannt zu bleiben. Der Angreifer kann sie so seinen Opfern unbemerkt unterschieben, zum Beispiel per Mail oder als nützliches Programm getarnt über Web-Seiten. Die Server melden sich in regelmäßigen Abständen beim Angreifer und warten auf seine Befehle.

---

**Vista Loader 3.0.0.1**
Für Windows Vista existieren mehrere Cracks, die das Betriebssystem illegalerweise ohne gültige Lizenz nutzbar machen. Aber nur die neue Version von Vista Loader umgeht auch die Kopierschutztechniken von Vista SP1. Der Crack macht sich die Tatsache zunutze, dass Microsoft aktivierungsfreie Lizenzschlüssel an große PC-Hersteller ausgibt. Diese funktionieren aber nur, wenn Vista das jeweilige Hersteller-Bios auf dem PC vorfindet. Vista Loader täuscht daher dem Betriebssystem durch einen Treiber das passende Bios vor.

---

**Wireshark 1.0.2**
Mit Wireshark (früherer Name: Ethereal) lässt sich der komplette Netzwerkverkehr eines PCs protokollieren und analysieren. Auch andere PCs im Netz können belauscht werden, allerdings nur, wenn die Rechner über Hubs verbunden sind. Hubs kommen heutzutage eher selten vor, in aller Regel trifft man Switches an, die den Datenstrom geräteweise trennen. Wireshark zeigt jedes übertragene Paket einzeln an. Über die Kontextmenü-Funktion „Follow TCP Stream“ lässt sich die komplette TCP-Verbindung nachvollziehen, in der das gewählte Paket vorkommt.

---

**Tool Vista Loader**
Es umgeht die Kopierschutztechniken auch von Vista SP1 indem es dem Betriebssystem ein Hersteller-Bios vortäuscht. Für PC-Hersteller vergibt Microsoft nämlich aktivierungsfreie Lizenzschlüssel.

---

**Gamejack**
fertigt Kopien auch von kopiergeschützten Spielen an. Scheitert die 1:1-Kopie, bietet das Tool die Option, ein Abbild der CD/DVD auf die Festplatte abzulegen. Dieses wird dann von Gamejack als virtuelles Laufwerk eingebunden, Kopierschutzmerkmale werden emuliert. Auf diese Weise wird dem Spiel vorgegaukelt, es sei ein Original-Datenträger im Laufwerk.

---

From:
https://wiki.hennweb.de/ - **HennWeb**

Permanent link:
**https://wiki.hennweb.de/doku.php?id=allgemein:passwoerter_hacken&rev=1608749985**

Last update: **23/12/2020 19:59**