

Hacking-Tools

Die Werkzeuge der Hacker als Problemlöser



Überblick	Seite 16
Hacking-Tools als Windows-Helfer	Seite 18
Werkzeuge für Experten	Seite 24
Hacking-Stick mit Kali Linux	Seite 30
Was erlaubt ist – und was nicht	Seite 170

Gefährlich, nützlich – oder beides? c't hat Hacking-Tools ausprobiert, um diese Frage zu klären. Viele entpuppten sich als Problemlöser und können auch Ihnen gute Dienste leisten, etwa um vergessene Passwörter zu knacken, Dateien zu retten oder das Netzwerk auf Sicherheitslücken abzuklopfen.

Von Ronald Eikenberg

Wer Hacker sagt, meint häufig Kriminelle, die unberechtigt Daten kopieren und veröffentlichen. Diese Black-Hats, benannt nach den bösen Cowboys mit schwarzen Hüten aus alten Wildwestfilmen, handeln mit gestohlenen Daten oder betrügen auf Kosten ihrer Mitmenschen. Doch es gibt auch Hacker, die ihr Know-how legal und moralisch einwandfrei einsetzen. Diese White-Hats sind gefragte Leute, sie spüren zum Beispiel als gut bezahlte Penetrationstester (Pentester) Sicherheitslücken für Unternehmen auf.

Allen Hackern gemein ist, neben ihrem technischen Know-how, dass sie sich die Arbeit oft mit speziellen Programmen erleichtern, um viele Aufgaben überhaupt erst erledigen zu können. Viele dieser Hacking-Tools sind frei verfügbar und völlig legitim einsetzbar – es besteht daher kein Grund, sie zu verteufeln. Es spricht sogar vieles dafür, die Tools selbst zu benutzen und damit die Sicherheit der eigenen Rechner, Router & Co. zu untersuchen – oder die eines Auftraggebers. Wer damit jedoch gegen geltende Gesetze verstößt und fremde Systeme attackiert, macht sich natürlich strafbar. Eine fundierte Einordnung der rechtlichen Lage finden Sie auf Seite 170.

Retter in der Not

Wir haben zahlreiche Hacking-Tools ausprobiert und stellen in dieser Ausgabe eine Auswahl der interessantesten Programme vor, die sogar das Zeug zum Retter in der Not haben. Viele der Hacking-Tools starten direkt unter Windows und sind dank einer grafischen Bedienoberfläche ver-

hältnismäßig leicht bedienbar, während andere alle Klischees erfüllen und nur auf der textbasierten Linux-Shell laufen. Wir möchten Ihnen die ganze Bandbreite zeigen: Im folgenden Artikel finden Sie nützliche Helfer für den Windows-Alltag mit konkreten Tipps zur Verwendung. Ist zum Beispiel die Abgabe der Bachelorarbeit gefährdet, weil Sie das Passwort der Word-Datei vergessen haben, setzen Sie doch mal den Passwortknacker **John the Ripper** darauf an. Mehr dazu lesen Sie auf Seite 20. Haben Sie sich aus Ihrem Windows ausgesperrt, setzen Sie das Passwort mit dem **Windows Login Unlocker** einfach zurück. Auf Seite 18 erfahren Sie wie.

Sie helfen Ihren Schwiegereltern beim Umstieg auf einen neuen PC, aber das vor Jahren eingerichtete WLAN-Passwort ist nicht mehr auffindbar? Mit Tools wie **La-Zagne** (S. 19) lesen Sie es vom alten Rechner aus und exportieren dabei gleich noch viele andere Zugangsdaten, die sich dort im Laufe der Zeit angesammelt haben und den Umzug beschleunigen. Auf Seite 22 zeigen wir außerdem, wie Sie vermeintlich

unrettbar verlorene Dateien wieder ans Tageslicht befördern.

Security-Check

Ab Seite 24 geht es etwas härter zur Sache mit Spezialtools, mit denen zwar nicht jeder etwas anfangen kann, die jedoch erstaunliche Fähigkeiten haben. Mit dem vielseitigen Netzwerkscanner **Nmap** (S. 25) verschaffen Sie sich schnell einen Überblick über die Situation in Ihrem Netzwerk und entdecken vielleicht auch den Nachbarn, der seit der letzten Party immer noch im WLAN mitsurft. Im gleichen Durchgang können Sie Ihre Geräte auf Sicherheitsprobleme abklopfen.

WordPress-Websites stehen unter Dauerfeuer, weil Angreifer nur zu gut wissen, dass ein verpenntes Sicherheits-Update ausreicht, um den ganzen Server zu übernehmen. Auch veraltete und verwundbare Erweiterungen sind schon vielen WordPress-Betreibern zum Verhängnis geworden. Wenn Sie das gleiche Werkzeug wie die Angreifer nutzen, spüren Sie etwaige Sicherheitslücken rechtzeitig auf und können Gegenmaßnahmen ergreifen, bevor Ihre Daten im Darknet gehandelt werden. Blättern Sie hierfür zu **WPScan** auf Seite 27.

Last, but not least, zeigen wir Ihnen ab Seite 30, wie Sie sich einen bootfähigen Hacking-Stick erstellen. Als Grundlage dient **Kali Linux**, das etliche Security-Tools enthält, die Sie direkt ausprobieren können. Alles, was Sie brauchen, ist ein USB-Stick mit mindestens 8 GByte und etwas Zeit. Manche der Tools sind zwar etwas unhandlich, von dem gewonnenen Fachwissen können Sie jedoch lange profitieren. Genau das Richtige für verregnete Herbsttage. *(rei@ct.de) ct*

Machen Sie Bekanntschaft mit Hydra, Medusa und John the Ripper: Hacking-Tools mit gefährlich klingenden Namen sind, richtig eingesetzt, echte Problemlöser.

