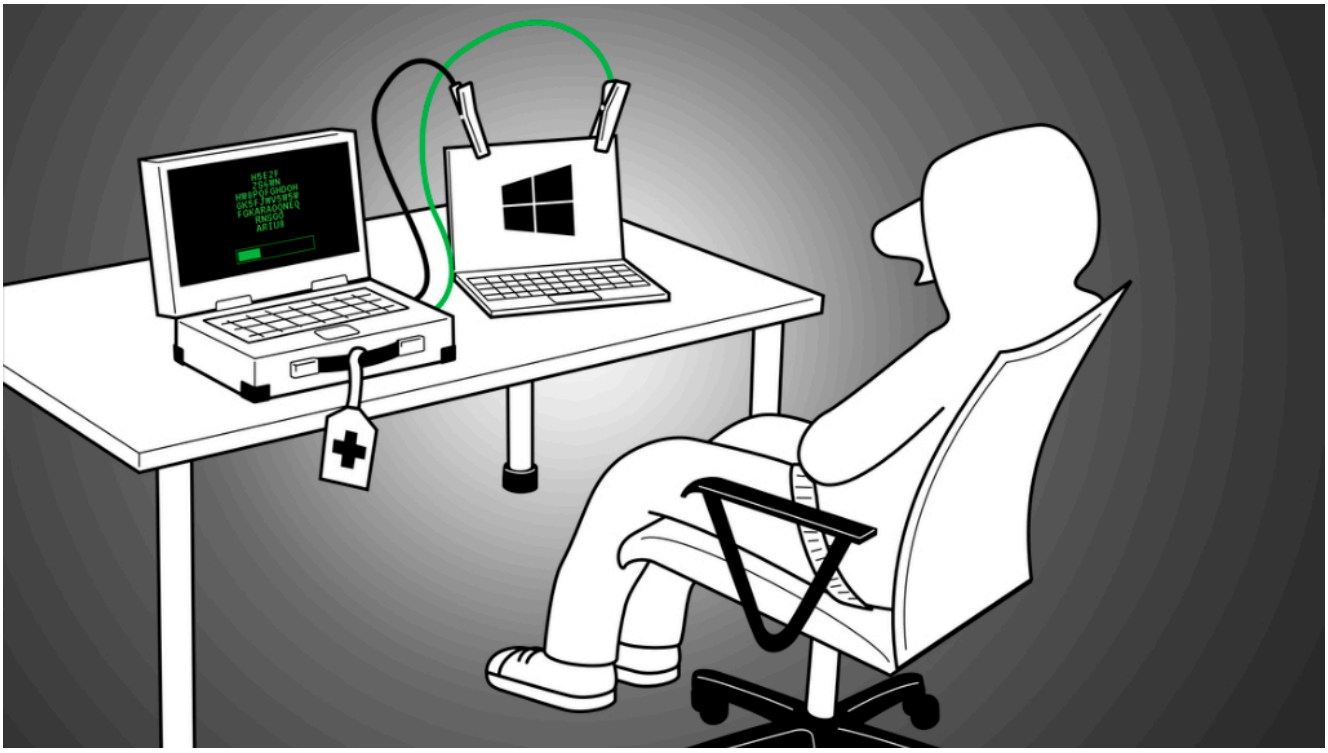
Hack Dich selbst – Nützliche Hacking-Tools für den Alltag



Hack Dich selbst

Haben Sie schon mal ein Passwort vergessen oder wichtige Dateien versehentlich gelöscht? Statt darüber zu fluchen, können Sie sich oftmals einfach selbst helfen: Schlüpfen Sie in die Rolle eines Hackers und verschaffen Sie sich wieder Zugriff auf Ihre Daten – ganz legal.
Haben Sie schon mal ein Passwort vergessen oder wichtige Dateien versehentlich gelöscht? Statt darüber zu fluchen, können Sie sich oftmals einfach selbst helfen: Schlüpfen Sie in die Rolle eines Hackers und verschaffen Sie sich wieder Zugriff auf Ihre Daten – ganz legal.

Von Ronald Eikenberg und Alexander Königstein

Hacken Sie Ihren eigenen Rechner: Was erstmal absurd klingt, kann Ihnen das Leben mit der Technik erheblich erleichtern. Denn mit den Werkzeugen der Hacker erledigen Sie nicht nur vieles schneller, Sie können damit auch echte Alltagsprobleme

lösen und sich aus der Patsche helfen. Nicht alle Hacking-Tools sind automatisch böse, oftmals handelt es sich um harmlose, aber äußerst nützliche Programme, die spezielle Aufgaben besonders gut oder effektiv lösen.

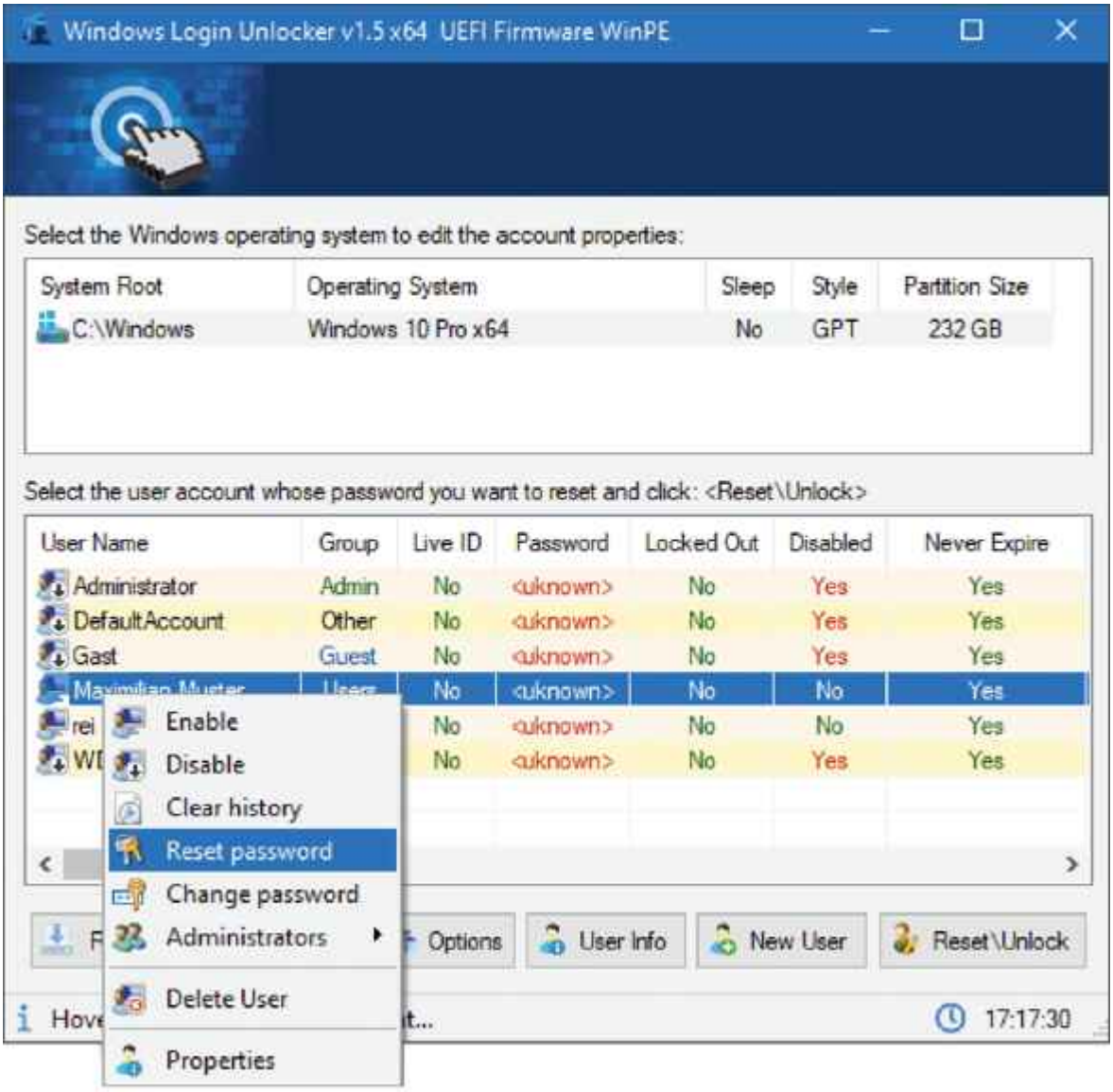
Bei Hackerangriffen ist keine schwarze Magie im Spiel, häufig sind es frei verfügbare Open-Source-Tools, die für sich genommen nicht gefährlich sind. Nach einer Infektion werden sie nachgeladen und automatisiert ausgeführt, um zum Beispiel Dateien oder Passwörter erstmal lokal einzusammeln. Ausgeleitet werden die Daten erst vom eigentlichen Schadcode (oder einem weiteren Tool). Andere Open-Source- Tools laufen direkt bei den Hackern, um zum Beispiel verschlüsselte Daten zu knacken oder gelöschte Dateien zu rekonstruieren.

Die missbräuchlich eingesetzten Werkzeuge werden von vielen Virenwächtern als „HackTool“ erkannt, weshalb den nützlichen Systemhelfern zu Unrecht ein schlechter Ruf anhaftet. Um das zu ändern, stellen wir Ihnen in diesem Artikel einige „Hacking-Tools“ vor, die sich bei uns bewährt haben. Wenn Sie sich erstmal langsam herantasten möchten, können Sie Programme gefahrlos in einer virtuellen Maschine oder auf einem ausgemusterten PC ausprobieren. Die Download-Links zu allen Tools sowie Verweise auf weiterführende c’t-Artikel finden Sie unter ct.de/y41x.

Windows-Passwort zurücksetzen

Anmelden klappt nicht, weil Windows-Passwort vergessen? Kann ja mal passieren. Wenn alle möglichen und unmöglichen Kennwörter durchprobiert sind und auch die Recovery-Fragen nicht weiterhelfen, ist guter Rat teuer. Eine Neuinstallation wäre naheliegend – ist jedoch meist gar nicht nötig. Ist die Systemplatte nicht verschlüsselt, können Sie das alte Passwort, genauer gesagt dessen Hash, einfach überschreiben. Doch Achtung: EFS-verschlüsselte Dateien lassen sich nach dieser Prozedur aus Sicherheitsgründen nicht mehr entschlüsseln (Das Encrypting File System, kurz EFS, ist die

transparente Dateiverschlüsselung von NTFS). Der Hash liegt im Registry-Zweig des Security Accounts Managers (SAM), wobei es sich letztlich nur um eine Datei auf der Platte (c:\windows\system32\config\sam) handelt. Die ist allerdings im laufenden Betrieb stets von Windows geöffnet, sodass Sie sie nicht einfach so bearbeiten können.



Windows-Passwort vergessen? Mit dem Windows Login Unlocker setzen Sie es einfach zurück.

Mit dem **Windows Login Unlocker** aus dem c’t-Notfall-Windows können Sie das Windows-Passwort dennoch zurücksetzen. Sie booten den Rechner vom Stick und der Unlocker übernimmt alle nötigen Schritte für Sie. Mit dem Tool können Sie das Passwort nicht nur zurücksetzen oder gleich ganz entfernen, sie können damit auch Konten anlegen und löschen. Der Unlocker entsperrt

sogar Accounts, die mit einem Microsoft-Konto verknüpft sind. Solche werden dabei in ein lokales Benutzerkonto umgewandelt. Einen bootfähigen USB-Stick mit dem Notfall-Windows und dem Unlock-Tool können Sie mit unserer Anleitung in c't 26/2020 leicht selbst erstellen, alle nötigen Dateien gibt es kostenlos zum Download (siehe ct.de/y41x). Sie finden das Tool im Notfall-Windows unter „Start/Datenrettung".

Die Bedienung des Unlockers erklärt sich fast von selbst: Oben listet er die gefundenen Windows-Installationen auf, zum Beispiel c:\Windows. Wählen Sie die passende und darunter das Windows-Konto, das Sie retten möchten. Nach einem Rechtsklick haben Sie diverse Möglichkeiten, von denen Sie entweder „Reset" oder „Change password" wählen. Die Änderung ist beim nächsten regulären Hochfahren ohne Stick aktiv und Sie können sich wieder einloggen. Alternativ können Sie das etablierte Open-Source-Tool „chntpw" nutzen, das auch unter Linux läuft. Es ist in Kali Linux (siehe Seite 30) bereits enthalten. Ist das Windows-Konto mit einem Microsoft-Account verknüpft, können Sie es mit chntpw jedoch nicht entsperren.

Nach der Rettungsaktion ist das Windows wieder wie gewohnt nutzbar, allerdings mit einer Ausnahme: Daten, die über die Windows-Funktion CryptProtectData() verschlüsselt gespeichert wurden, können Sie weiterhin nicht entschlüsseln, da dazu das ursprüngliche Passwort nötig ist. Hiervon sind zum Beispiel die Passwortspeicher einiger Browser und durch Windows verschlüsselte Dateien (EFS, siehe oben) betroffen, nicht aber Bitlocker.

Das Unlock-Tool demonstriert anschaulich, dass ein Windows-Konto kein wirksamer Zugriffsschutz ist. Wenn Sie unbefugte Zugriffe verhindern möchten, sollten Sie Ihre Laufwerke zum Beispiel mit BitLocker oder VeraCrypt verschlüsseln. Dann sind nur nicht Ihre Dateien geschützt, sondern auch die Windows-Installation samt Passwort-Hashes (SAM). Das Entschlüsselungskennwort sollten Sie jedoch besser nicht vergessen.

Zugangsdaten einsammeln

Im Laufe eines Windows-Lebens sammeln sich etliche Zugangsdaten im System an, zum Beispiel im Browser, Mail-Client, VPN-Programm, aber auch alle WLAN-Kennwörter. Auf diese Datenbeute haben es üble Zeitgenossen natürlich abgesehen. Sie nutzen spezielle Programme, um die gespeicherten Logins in Sekundenschnelle einzusammeln. Solche Tools sind für sich genommen völlig harmlos, denn sie übertragen die gefundenen Zugangsdaten nicht, sondern zeigen sie lediglich an und können sie in eine Datei exportieren. Das kann im Alltag sehr nützlich sein, etwa um Zugangsdaten aus einer alten Windows-Installation zu retten, bevor man das System neu aufsetzt.

Schauen Sie sich zunächst im NirSoft-Fundus um: Hier finden Sie Password-Recovery-Tools für fast jeden Zweck, darunter **WebBrowserPassView**, das die Passwortspeicher der gängigsten Browser ausliest. **Mail PassView** liest Zugangsdaten aus Mail-Clients, **VaultPasswordView** aus der Windows-Anmeldeinformationsverwaltung und so weiter. Einen interessanten Zusatznutzen hat das Tool **WirelessKeyView**: Es zeigt nicht nur die im System gespeicherten WLAN-Zugangsdaten an, es kann daraus auch QR-Codes generieren, mit denen Sie Smartphones und Tablets schnell in Ihr WLAN helfen.

Die NirSoft-Tools sind leicht zu bedienen, da ihr Funktionsumfang überschaubar ist. Möchte Sie sich einen Überblick über die Gesamtsituation verschaffen, können Sie zum Python-Tool **LaZagne** greifen, das in einem Durchgang viele Speicherorte von Betriebssystem und Anwendungen durchforstet. Es wird selbst unter Linux und macOS fündig. Laden Sie das Tool am besten als Python-Skriptsammlung (Zip-Datei) von GitHub herunter – es existiert zwar eine direkt ausführbare Windows-Datei, diese konnten wir auf unseren Systemen jedoch nicht starten.

Falls nicht vorhanden, installieren Sie zuerst den Python-

Interpreter. Unter Windows aktivieren Sie „Add Python to PATH“ und melden sich nach der Installation neu an, damit die folgenden Befehle funktionieren. Entpacken Sie das Zip-Archiv von LaZagne und installieren Sie mithilfe der Datei requirements.txt alle nötigen Python-Module: pip install -r requirements.txt. Anschließend wechseln Sie in das Verzeichnis, das zu Ihrem Betriebssystem passt (etwa „Windows“) und können dort LaZagne mit dem folgenden Befehl ausführen: python laZagne.py all Durch das „all“ führt LaZagne sämtliche vorhandenen Analysemodule aus. Wenn Sie es weglassen, erhalten Sie eine Übersicht über die möglichen Befehle.

Hat alles geklappt, liefert Ihnen das Tool eine lange Liste mit Zugangsdaten, Hashes et cetera – abhängig davon, was es auf Ihrem System zu holen gibt. LaZagne kann vieles mit den Rechten eines Standardnutzers auslesen, für manche Dinge – etwa WLAN-Passwörter – benötigt es jedoch Adminzugriff. Falls Sie das ausprobieren möchten, können Sie unter Windows die Eingabeaufforderung per Rechtsklick als Admin öffnen und anschließend LaZagne wie oben beschrieben starten.

Passwörter knacken

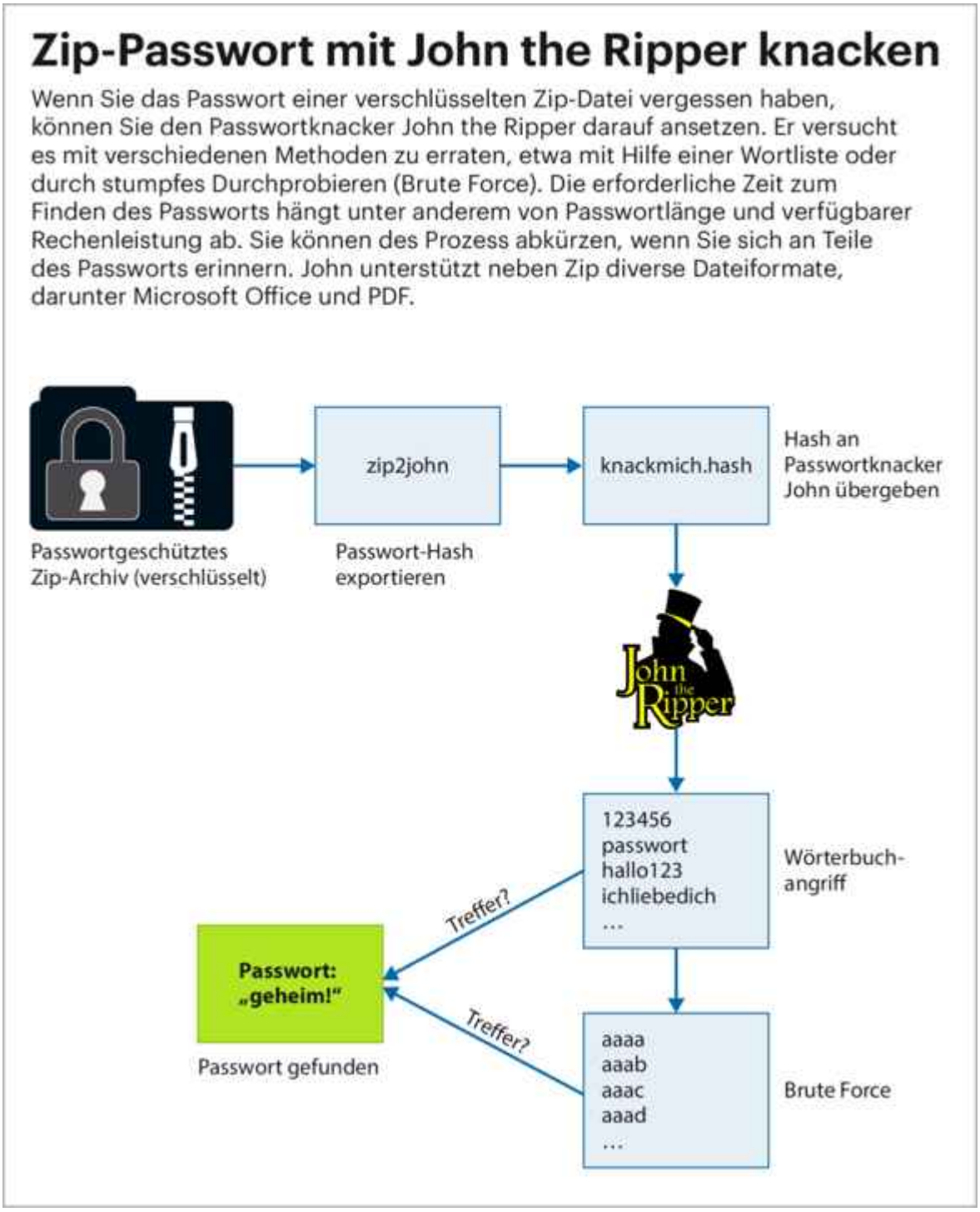
Passwortgeschützte Zip-Dateien sind ein einfaches und bewährtes Mittel, um Dateien zu verschlüsseln und so vor neugierigen Blicken zu schützen. Man kann sie fast überall mit Bordmitteln öffnen – sofern man sich noch an das richtige Passwort erinnert. Als Retter in der Not kann der legendäre Passwortknacker **John the Ripper** einspringen. Er versucht, das Passwort durch Durchprobieren zu erraten. Die Erfolgschancen stehen und fallen mit der Länge des Kennworts. Ist es recht kurz, wird John mit etwas Glück schon nach wenigen Sekunden fündig, bei sehr langen Zeichenfolgen können Millionen Jahre ins Land ziehen. Wenn Sie sich an Teile des Passworts oder zumindest an dessen Zusammensetzung erinnern, können Sie die Knackdauer jedoch deutlich reduzieren.

John gibt es für Windows, Linux und macOS, bei Kali Linux (siehe S. 30) ist er bereits an Bord. Er liest die verschlüsselten Dateien nicht selbst ein, er benötigt stattdessen eine Datei, die den zu knackenden Passwort-Hash enthält. Die können Sie mit den mitgelieferten Hilfswerkzeugen leicht selbst erstellen. Im Lieferumfang befinden sich etliche davon für diverse Dateiformate, darunter neben Zip etwa Android Backup, Bitwarden, KeePass, Office und PDF. Manche Helfer sind Python-Skripte und setzen den dazugehörigen Interpreter voraus. Die Tools liegen im Ordner „run“, Kali-Nutzer schauen indes unter /usr/share/john/.

So weit die Theorie, jetzt folgt die Praxis: Um zum Beispiel ein verschlüsseltes Zip-Archiv mit John zu knacken, extrahieren Sie zunächst den Passwort-Hash mit dem Hilfstool zip2john daraus: zip2john verschluesselt.zip > knackmich.hash. Mit anderen Formaten klappt das ebenso leicht, bei Office-Dokumenten ersetzen Sie zip2john durch office2john, bei PDF-Dokumenten durch pdf2john und so weiter.

Anschließend setzen Sie John auf die Hash-Datei an, im einfachsten Fall mit john knackmich.hash. Dann probiert er zunächst die Kennwörter aus der mitgelieferten Liste password.lst durch, die einige zehntausend der am häufigsten genutzten Passwörter aus dem englischsprachigen Raum enthält. Dabei probiert John gängige Abwandlungen aus, ein Listeneintrag „mutti“ würde deshalb auch das Passwort „Mutti!“ zutage fördern. Das Abarbeiten der Liste dauert nur wenige Sekunden. Mit etwas Glück meldet John nach kurzer Zeit einen Treffer und zeigt das gefundene Passwort auf der Konsole an.

Wird der Passwortknacker noch nicht fündig, probiert er systematisch ASCII-Zeichenkombinationen aus, was deutlich mehr Zeit frisst – und bei langen Passwörtern aussichtlos ist. In diesem Fall sollten Sie den Suchradius möglichst weit eingrenzen.



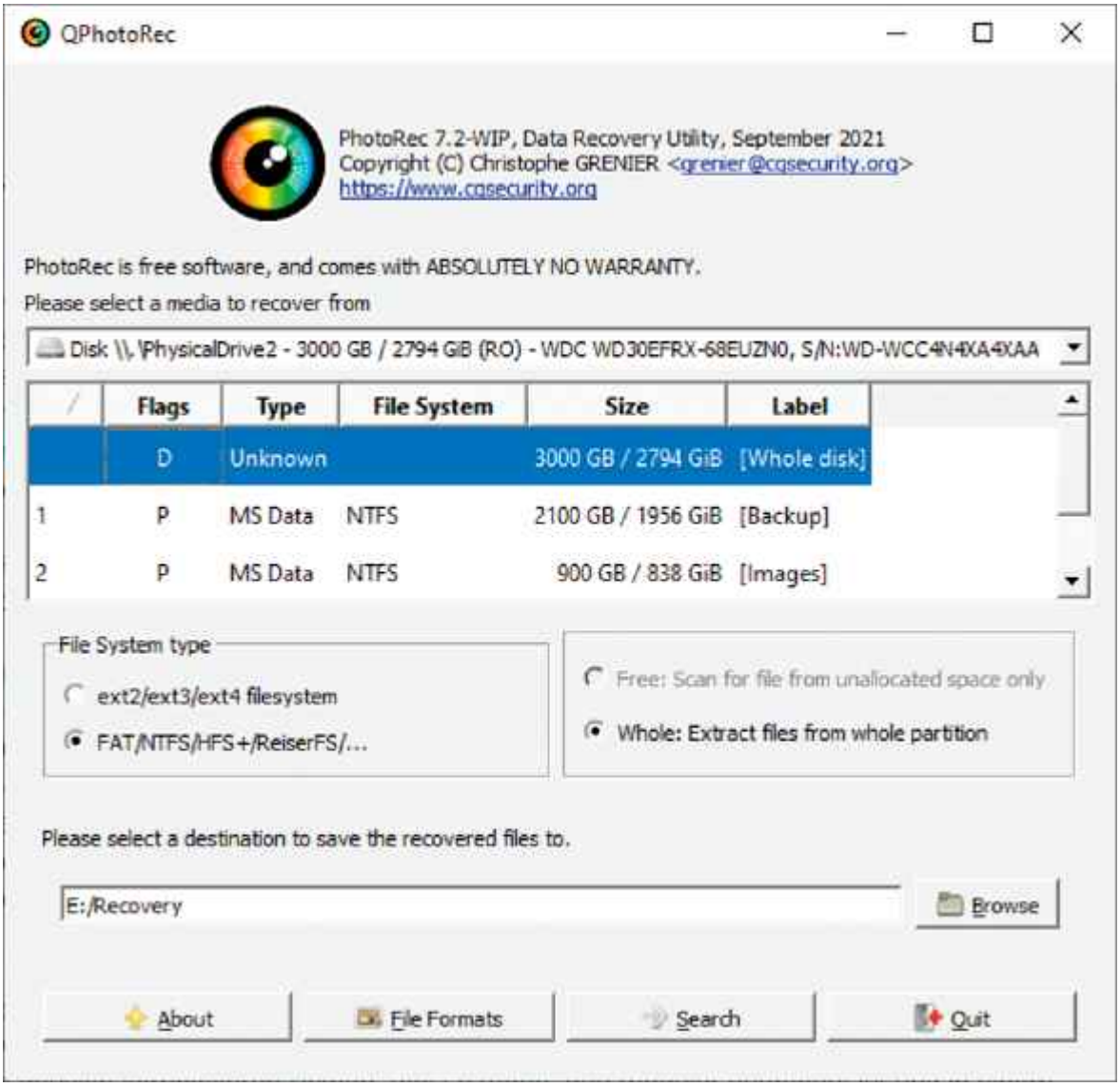
Sie können zum Beispiel eine Mindest- und Maximallänge wie 5 und 6 Zeichen vorgeben, indem Sie -min-length=5 -max-length=6 an den Befehl hängen. Mit -incremental=digits würden Sie den Suchradius auf Ziffern beschränken, um zum Beispiel ein Passwort zu finden, das aus einem Geburtsdatum besteht. Wer einen Teil seines Passworts kennt, sollte John nach einer Passwortmaske suchen lassen. Den Aufbau solcher Masken erklärt die Dokumentation en détail (siehe ct.de/y41x). Im folgenden Beispiel ist bekannt, dass das Kennwort mit „passwort“ beginnt

und darauf noch drei unbekannte Zeichen folgen: john knackmich.hash -mask=passwort?a?a?a

Probieren Sie doch mal aus, wie lange Ihre Kennwörter einem Angriff standhalten würden. Bedenken Sie aber, dass einem echten Angreifer wahrscheinlich mehr Rechenleistung zur Verfügung steht, etwa in Form eines Grafikkarten-Clusters in der Cloud. Zudem setzt er möglichweise eine andere Passwortliste ein, auf der auch Ihr Kennwort steht. Daher gilt: Wählen Sie stets möglichst lange, individuelle Kennwörter – am besten zufällig generiert oder zumindest mit absichtlichen Tippfehlern.

Dateien retten

Gelöschte Dateien sind nicht zwangsläufig unrettbar verloren. Das machen sich Hacker zunutze, um vertrauliche oder pikante Daten von achtlos entsorgten Festplatten, USB-Sticks und Speicherkarten zu kratzen. Die genutzten Tools sind natürlich auch für die Rettung eigener Daten äußerst nützlich – zum Beispiel, wenn Sie wichtige Dateien versehentlich gelöscht haben oder die Daten aus anderen Gründen plötzlich nicht mehr auffindbar sind. Auch Dateien auf SSDs lassen sich mit etwas Glück wiederherstellen, wenn das System den TRIM-Befehl noch nicht ausgeführt hat, um die Daten endgültig zu löschen.



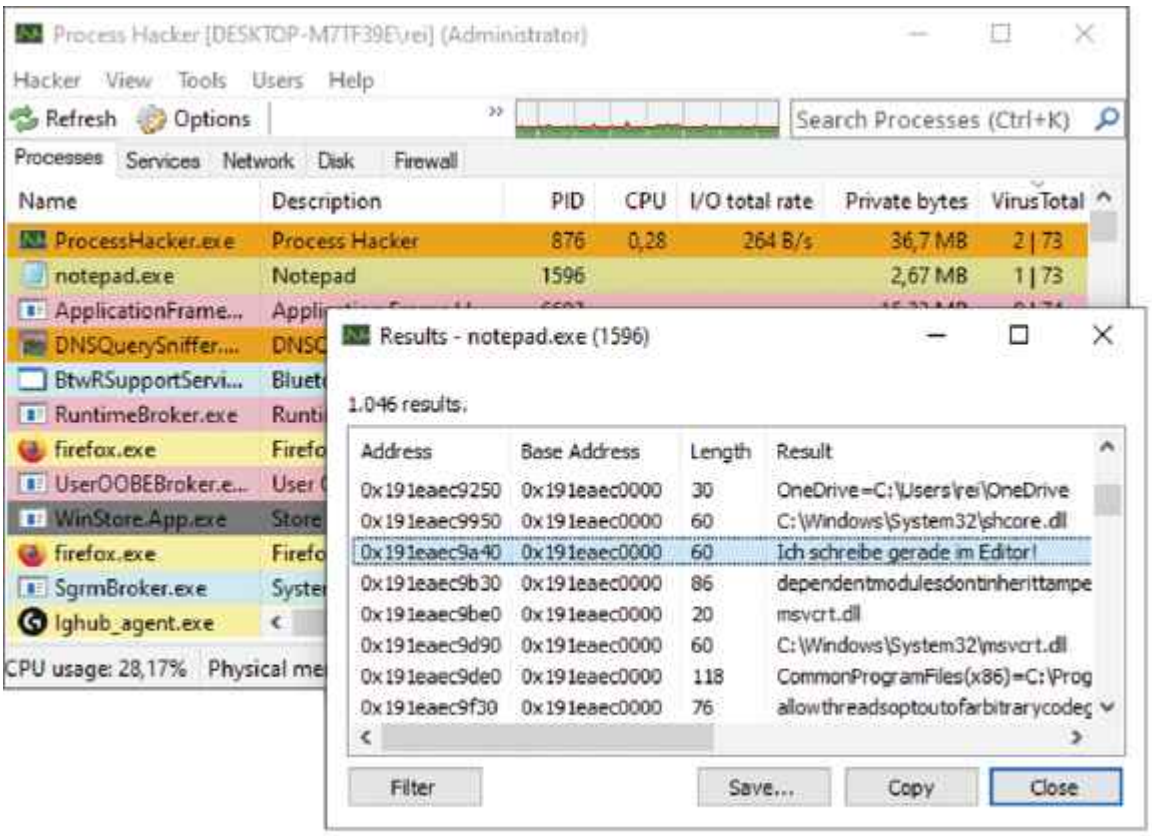
Sind Ihre Dateien noch zu retten? Mit PhotoRec finden Sie es heraus.

Ein bewährtes Werkzeug für diesen Zweck ist das Open-Source-Tool **PhotoRec**, das auf allen möglichen Betriebssystemen läuft. Es ist eigentlich auf der Kommandozeile zu Hause, mit QPhotoRec gibt es inzwischen jedoch auch eine einfache Bedienoberfläche. Nach dem Start wählen Sie oben das zu durchsuchende Laufwerk oder ein Laufwerksabbild und darunter entweder eine bestimmte Partition oder das gesamte Speichergerät. Weiter unten stellen Sie das Dateisystemformat ein und rechts daneben wählen Sie aus, ob nur die unbelegten Speicherblöcke abgesucht werden sollen („Free“) oder alles („Whole“). Zu guter Letzt geben Sie einen Zielordner für die aufgespürten Dateien an und starten die Rettungsaktion mit „Search“.

Falls Ihre Dateien nicht lesbar sind, weil Partitionen oder Dateisystem beschädigt sind, können Sie gezielte Reparaturen daran durchführen. Hierfür greifen Sie am besten zu **TestDisk**, das Sie ohnehin bereits besitzen, wenn Sie PhotoRec heruntergeladen haben. Starten Sie TestDisk über die Konsole, führt es Sie interaktiv durch die wichtigsten Fragen, ehe die Reparatur beginnt. Über die „Undelete“-Funktion können Sie mit dem Tool außerdem gezielt einzelne Dateien wiederherstellen, was schneller zum Ziel führen kann als ein groß angelegter Rettungsversuch mit PhotoRec.

Prozesse hacken

Ein Windows-System gönnt sich selten eine Pause: Prozessor, Datenträger und Netzwerk stehen niemals still. Nur ein Blick hinter die Kulissen zeigt, womit der Rechner gerade beschäftigt ist. Installiert Windows gerade fleißig Updates oder wütet ein Krypto-Trojaner, der alles verschlüsselt, was er in die Finger bekommt? Mit den richtigen Systemtools finden Sie es heraus. Die Auswahl ist riesig, und am bekanntesten sind die SysInternals-Tools, die wir schon ausführlich in c’t präsentiert haben (siehe ct.de/y41x). Im Rahmen dieser Vorstellung von Hacking-Tools möchten wir den Blick auf das Mehrzweck-Tool **Process Hacker** lenken, das einige besondere Extras enthält. Um von diesen Extras zu profitieren, benötigen Sie einen frischen Nightly-Build (3.x).



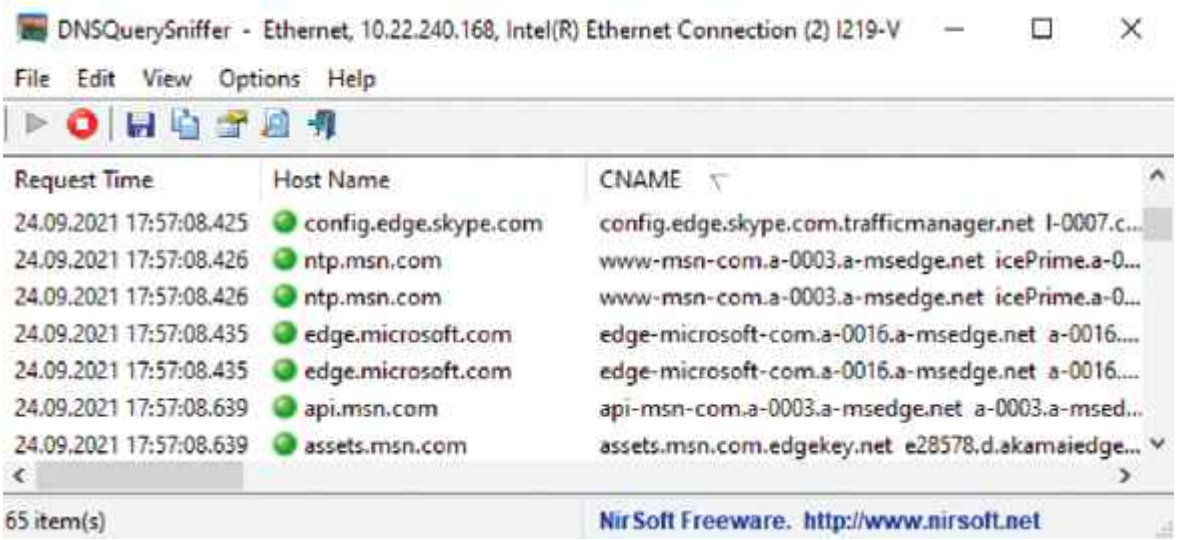
Der Process Hacker macht da weiter, wo andere Taskmanager aufhören: Das Tool erlaubt sogar Eingriffe in den Arbeitsspeicher der Prozesse.
Das Hauptfenster des Process Hacker ist in fünf Tabs unterteilt: „Processes“ zeigt, ähnlich wie der Taskmanager, Informationen über laufende Prozesse an und „Services“ listet die Dienste auf. Über den „Network“-Tab schauen Sie nach, welche Prozesse aktuell mit dem Netz kommunizieren. „Disk“ macht Dateizugriffe sichtbar und „Firewall“ lässt Sie auf die Aktivitäten der Windows-Firewall blicken. Dort sehen Sie, welche aktuellen Verbindungen auf Grundlage welcher Regeln zugelassen oder blockiert wurden. Damit sind nur die Basics beschrieben, es gibt aber noch viel zu entdecken.

Klicken Sie doppelt auf einen Prozessnamen, um ihn unter die Lupe zu nehmen. Hier können Sie zum Beispiel die geladenen Bibliotheken (Modules) einsehen, aber auch im Arbeitsspeicher des Prozesses stöbern (Memory). Klicken Sie dort auf „Options“ und „String“, listet Ihnen Process Hacker sämtliche Zeichenfolgen auf. So können Sie den Speicher zum Beispiel nach Zugangsdaten, IP-Adressen oder API-Schlüsseln

durchsuchen, die das Programm dort bereithält. Über den Tab „Windows“ der Prozesseigenschaften finden Sie heraus, welche Fenster einem Prozess zugeordnet sind und können sogar die einzelnen Fensterelemente verändern. So schalten Sie zum Beispiel – auf eigene Gefahr – gesperrte Buttons frei. Abschließend noch eine kleine Übungsaufgabe: Tippen Sie doch mal einen kurzen Text in den Editor von Windows und ändern Sie das Getippte anschließend, indem Sie den Arbeitsspeicher von notepad.exe mit dem Process Hacker manipulieren.

Netzwerkverkehr untersuchen

Wenn sich Ihr System auffällig verhält, kann sich ein Blick in den Netzwerkverkehr lohnen. Dafür ist **NetworkTrafficView** von NirSoft sehr praktisch: Es zeigt die Netzwerkverbindungen Ihres Systems an und verrät Ihnen, von welchen Prozessen die Verbindungen ausgehen. Aufschlussreich sind auch die DNS-Anfragen, denn bevor eine Verbindung zu einer bestimmten Domain aufgebaut werden kann, muss ein Prozess erstmal die dazugehörige IP-Adresse bei einem DNS-Server erfragen. Mit dem **DNSQuerySniffer**, ebenfalls von NirSoft, können Sie die Anfragen gezielt und live mitverfolgen. So können Sie auch prüfen, ob die DNS-Anfragen Ihres Systems noch im Klartext oder bereits verschlüsselt, etwa über DNS-over-HTTPS (DoH), übertragen werden. In letzterem Fall tauchen sie in dem Analyse-Tool nicht auf.



DNS-Anfragen verraten viel über das Kommunikationsverhalten des Systems. DNSQueryView macht sie sichtbar.
Mit **PacketCache** von Netresec schauen Sie bei der Analyse des Netzwerkverkehrs in die Vergangenheit: Der Dienst schreibt den IPv4-Traffic des Systems fortlaufend in den Arbeitsspeicher, wodurch Sie jederzeit herausfinden können, was in den letzten Minuten passiert ist. IPv6-Verkehr unterstützt er aktuell jedoch nicht. PacketCache wird von Hand eingerichtet, mit den Anweisungen auf der Herstellerseite (siehe ct.de/y41x) ist das jedoch schnell erledigt. Dort erfahren Sie auch, wie Sie die aufgezeichneten Daten abholen, beispielsweise mit dem Analyseprogramm Wireshark oder dem Auswertungs-Tool **NetworkMiner,** das auch von Netresec kommt. Es erlaubt einen schnellen Einblick in die Kommunikation: Wer spricht mit wem, DNS-Anfragen, TLS-Zertifikate und mehr.

Aus Klartextverkehr (HTTP) extrahiert es darüber hinaus Zugangsdaten, URL-Parameter und Bilddateien. Alles, was hier auftaucht, kann auch ein Angreifer sehen, der Ihren Datenverkehr zum Beispiel an einem Hotspot belauscht. Nutzen Sie das Tool, um Datenlecks zu erkennen und gezielt durch Verschlüsselung (etwa per VPN) zu beheben. Wenn Sie mit NetworkMiner live auf den Datenverkehr schauen möchten, sollten Sie den Capture-Treiber Npcap (WinPcap) installieren und als Netzwerkadapter für die Analyse wählen. Die zur Auswahl stehenden „Socket“-Adapter werten lediglich IPv4-Datenverkehr aus, nicht aber IPv6. Wenn Sie Wireshark installiert haben, besitzen Sie den Treiber wahrscheinlich schon.

PowerShell-Hacks

Die Windows PowerShell ist nicht nur ein fester Bestandteil des Betriebssystems, sie ist auch sehr mächtig – und das macht sie für Hacker interessant. Cyberschurken zweckentfremden die PowerShell längst für die feindliche Übernahme einzelner Rechner und ganzer Netzwerke (PowerShell Empire, siehe Seite 29). Aber sie lässt sich auch für nützliche Windows-Hacks

einspannen, etwa um das Betriebssystem individuell zu konfigurieren und seine Geschwätzigkeit zu reduzieren.

Das PowerShell-Modul **Sophia Script** erlaubt Ihnen umfassende Eingriffe ins System, die normalerweise nur sehr umständlich möglich sind. Sie können damit zum Beispiel die Telemetrie- und Diagnosefunktionen zähmen, die Bing-Suche im Startmenü loswerden und den Windows Defender aufmotzen. Die Einrichtung ist bei GitHub ausführlich dokumentiert (siehe ct.de/y41x). In der Zip-Datei befindet sich das PowerShell-Skript Sophia.ps1, das demonstriert, wie Sie die Sophia-Kommandos aneinanderreihen, zum Beispiel um eine frische Windows-Installation nach Ihren Wünschen einzurichten. Führen Sie das Skript erst aus, nachdem Sie es inspiziert und die vorgegebenen Befehle an Ihre Bedürfnisse angepasst haben.

Sie können auch einzelne Funktionen direkt aufrufen. Der folgende Befehl etwa entfernt die Bing-Suche aus dem Startmenü:

```
 . .\Functions.ps1
Sophia -Functions "BingSearch -Disable"
```

Grundsätzlich sollten Sie sich darüber im Klaren sein, was Sie tun und sich über Nebenwirkungen informieren. Wenn Sie etwa Telemetriedienste blockieren, müssen Sie beobachten, ob Windows weiterhin mit Updates versorgt wird. Es gilt die Devise: Weniger ist mehr! Falls Sie unsicher sind, was Sie mit einem Sophia-Befehl auslösen, können Sie einen Blick in den Powershell-Code werfen (Ordner „Module“).

Fazit

Das passende Hacking-Tool zur rechten Zeit kann echte Probleme lösen. Ganz gleich, ob es darum geht, ein vergessenes Passwort zu knacken, verloren geglaubte Dateien zu retten oder nervige Windows-Funktionen abzuschalten. Einigen der Helfer haftet zu Unrecht ein schlechter Ruf an – der Umstand, dass einige davon auch von Cyberschurken genutzt werden, zeigt eher, dass man

mit den Tools sehr effektiv bestimmte Dinge erledigen kann. (*rei@ct.de*)

Tools, Literaturhinweise: ct.de/y41x