# Hacking-Tools-Werkzeuge für Experten-2021

## Gute Tools, böse Tools

# Hacking-Werkzeug für Fortgeschrittene

Mit den Hacking-Tools von Penetrationtestern finden Sie Sicherheitslücken in Ihren Websites, Netzwerken und Anwendungen, bevor es andere tun.

Von Ronald Eikenberg und Alexander Königstein

Hollywood weiß Hacker-Aktivitäten in Szene zu setzen: Vor unzähligen Monitoren mit monochromatischen Benutzeroberflächen sitzen Gestalten im Kapuzenpulli und brechen durch die Firewalls. In der Realität geht es weitaus nüchterner zu, denn die eigentliche Action spielt sich hinter den Kulissen ab. Das ist aber nicht weniger faszinierend, denn Hacking-Tools leisten erstaunliche Dinge, wenn man sie richtig einsetzt. Das setzt etwas Wissen und Erfahrung voraus, doch beides baut sich ganz von selbst auf, wenn Sie erst mal Feuer gefangen haben. In diesem Artikel stellen wir eine Auswahl interessanter Profi-Werkzeuge vor, die sowohl auf der dunklen als auch auf der hellen Seite der Macht genutzt werden. Stöbern Sie auch im Artikel „Hack Dich selbst“ auf Seite 18, der nützliche Problemlöser für den Alltag präsentiert.

Mit den im Folgenden vorgestellten Profi-Tools spüren Sie Sicherheitslücken in Ihren Websites, Netzwerken, Apps, IoT-Geräten und vielem mehr auf. Anschließend können Sie gezielt Schutzmaßnahmen ergreifen und die Schlupflöcher stopfen, bevor

es zu spät ist. Die meisten Hacking-Tools laufen am besten oder ausschließlich unter dem Betriebssystem Linux. Eine gute Grundlage für die ersten Schritte ist **Kali Linux**, das von Haus aus bestens auf die Bedürfnisse von Hackern zugeschnitten ist. Auf Seite 30 erfahren Sie, wie Sie sich einen Kali-USB-Stick mit persistenter Datenpartition für Ihre Experimente erstellen. Download-Links und weiterführende Informationen zu allen vorgestellten Tools finden Sie online unter ct.de/ygg5. Aber genug der Vorrede – jetzt geht es in die Vollen!

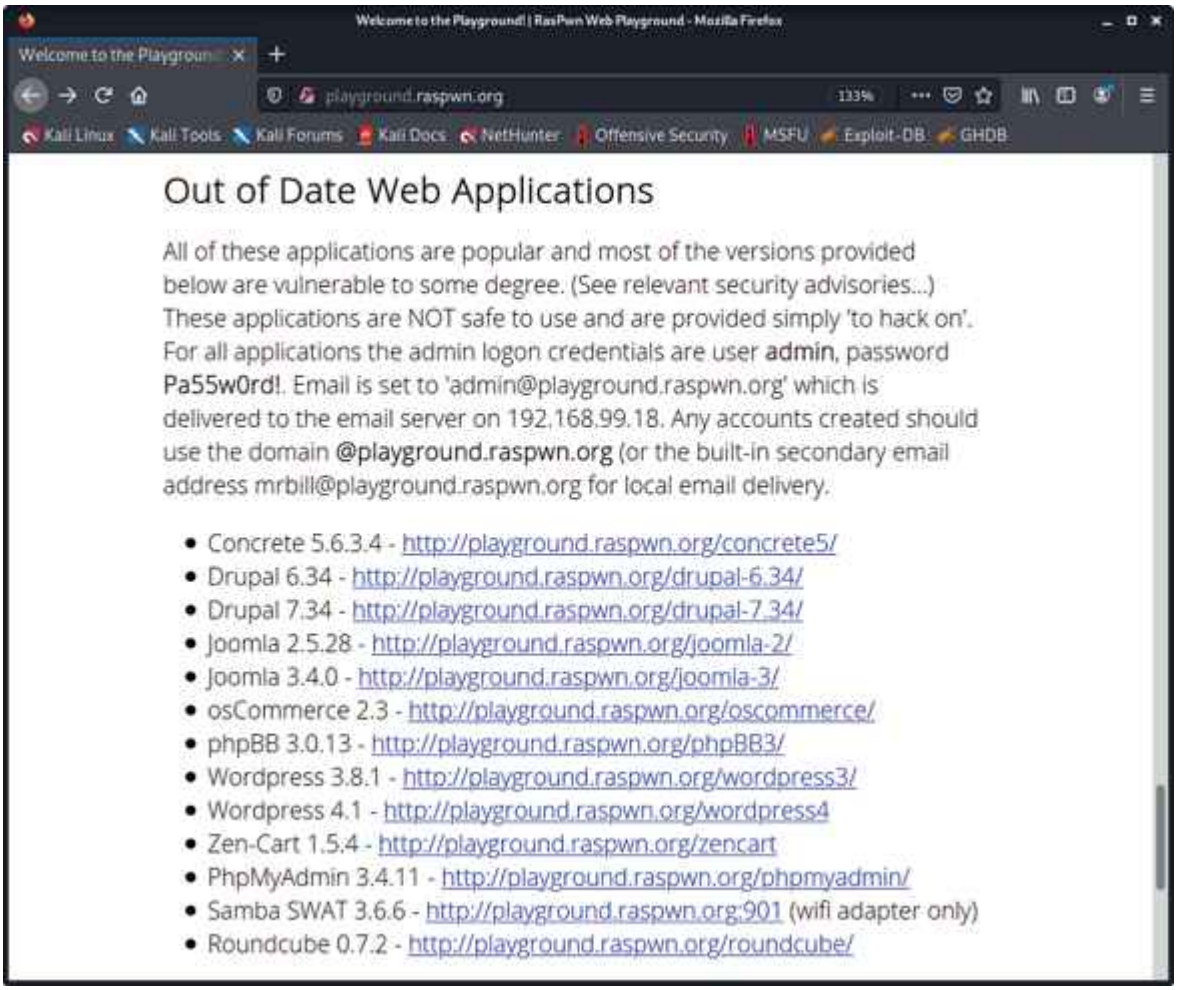
## Angreifen erlaubt

Die hier genannten Hacking-Tools sind nicht illegal, aber natürlich dürfen Sie damit nicht gegen geltende Gesetze verstoßen (siehe Seite 170). Damit Sie gar nicht erst in Versuchung kommen, die Tools unerlaubt an fremden Servern zu testen, sollten Sie sich eine geeignete Übungsumgebung schaffen – zum Beispiel ein Testnetz, in dem sich ausschließlich Systeme befinden, die Sie attackieren möchten und dürfen.

Ein geeignetes Angriffsziel ist **RasPwn**, das ein ganzes Netzwerk voller verwundbarer Server simuliert, an denen Sie sich austoben können. Sie übertragen es einfach auf eine MicroSD-Karte, die Sie anschließend in einen Raspi-Kleincomputer stecken (mindestens Raspi 2B). Nach dem Booten meldet sich ein WLAN namens „RasPwn OS“, zu dem Sie mit dem Passwort „In53cur3!“ eine Verbindung herstellen. Aus dem Netz öffnen Sie http://playground.raspwn.org mit einem Browser Ihrer Wahl, wo Sie mit allen wichtigen Informationen über das virtuelle Netzwerk und die angreifbaren Server versorgt werden. Ein Netzwerkkabel darf nicht mit dem Raspi verbunden sein, andernfalls hat das hochgradig verwundbare Image unter Umständen Zugriff auf Ihr Hauptnetzwerk und das Internet – was Sie tunlichst vermeiden sollten.

Zu den möglichen Angriffszielen zählen verwundbare WordPress-Installationen, eine steinalte Version des Webshop-Systems

osCommerce, das Datenbank-Tool phpMyAdmin, ein Mailserver, Samba und so weiter. Auch das Debian-Linux, auf dem RasPwn basiert, hat schon fast sieben Jahre auf dem Buckel und ist so löchrig wie ein Schweizer Käse. Obendrauf gibt es zahlreiche Web-Applikationen wie OWASP Bricks und Damn Vulnerable Web Application (DVWA), die nur mit dem Ziel entwickelt wurden, möglichst verwundbar zu sein, um typische Sicherheitslücken am lebenden Objekt zu demonstrieren. Viele dieser Projekte sind online dokumentiert, wodurch sie sich hervorragend zum Lernen eignen (siehe ct.de/ygg5).



Das Raspi-Image RasPwn enthält etliche verwundbare Web-Apps – und das mit voller Absicht.

## Netzwerk auskundschaften

Hat sich ein Angreifer Zugriff auf ein fremdes Netzwerk verschafft, etwa durch eine frei zugängliche Netzwerkbuchse im Aufenthaltsraum, eine per E-Mail eingeschleuste Malware oder

ein schwaches WLAN-Passwort, dann wird er sich erst mal einen Überblick über die Geräte im Netz verschaffen, um mögliche Angriffsziele auszumachen. Hierbei ist der mächtige Netzwerkscanner **Nmap** (Network Mapper) die erste Wahl. Er spürt nicht nur die Rechner, Drucker, NAS, Server, Router und vieles mehr auf, sondern auch die darauf laufenden Dienste. Durch Skripte lässt sich der Scanner beliebig erweitern, etwa um die entdeckten Clients gleich noch auf Sicherheitslücken abzuklopfen. Das alles ist nützlich, um verwundbare Geräte im eigenen Netz aufzuspüren und sie anschließend entweder abzusichern oder aus dem Verkehr zu ziehen.

Nmap läuft auf Linux, macOS und Windows, bei Kali Linux ist er inklusive. Wenn Sie auf einer Shell nmap ohne Parameter eintippen, zeigt das Tool die wichtigsten Betriebsmodi an. Um einfach und schnell die offenen Ports eines bestimmten Hosts herauszufinden, hängen Sie einfach dessen IP-Adresse an den Befehl an, etwa nmap 192.168.178.1. Das müssen Sie zwar nicht als root ausführen, es lohnt sich aber: So finden Sie mehr über die Clients heraus, im konkreten Fall die MAC-Adressen. IPv6-Adressen scannen Sie mit dem Parameter -6.

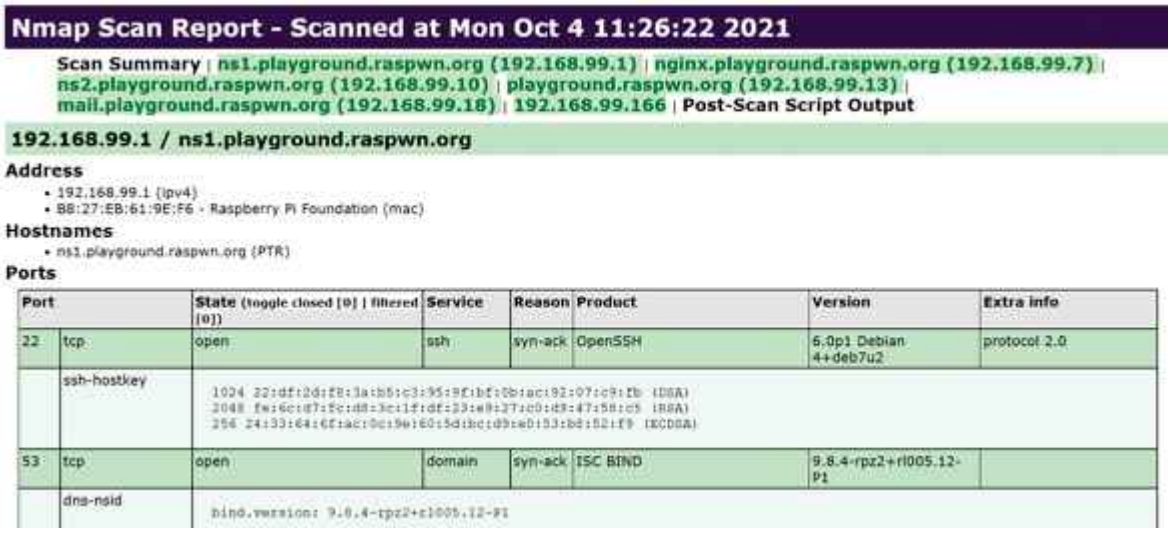
Sie können den Scan auf einen IP-Bereich ausweiten, den Sie zum Beispiel mit 192.168.178.1-50 definieren (alle IP-Adressen, die mit 192.168.178 anfangen und mit .1 bis .50 enden). Oder Sie scannen gleich das gesamte /24-Subnetz (alle bis .255): nmap 192.168.178.0/24. Ist der Scan abgeschlossen, präsentiert Ihnen Nmap die Ergebnisse auf der Shell, vorher lässt das Tool nicht von sich hören. Wer ungeduldig ist, kann mit --stats-every 10s festlegen, dass Nmap regelmäßig ein Statusupdate ausgibt.

Wirklich komfortabel lesbar ist der Bericht auf der Shell nicht. Sie können jedoch leicht einen formatierten HTML-Report erstellen, indem Sie zunächst Nmap mit -oX ergebnis.xml anweisen, einen XML-Export der Ergebnisse zu schreiben. Anschließend bauen Sie daraus mit dem unter Kali vorinstallierten Tool xsltproc eine HTML-Datei, die Sie mit

jedem Browser öffnen können: xsltproc ergebnis.xml -o ergebnis.html

Mit dem einfachen Scan kratzen Sie erst an der Oberfläche der Möglichkeiten. Mehr können Sie Nmap über verschiedene Scan-Optionen entlocken (siehe ct.de/ygg5). Sehr umfangreich ist der Modus -A, der unter anderem die Betriebssystem- und Versionserkennung (Fingerprinting) scharf schaltet. Diesen Modus sollten Sie mit sudo starten, damit Ihnen nichts entgeht. Aber aufgepasst: Nmap greift in diesem Fall aktiv auf die entdeckten Server zu, um Informationen einzuholen. Das kann zu unerwarteten Effekten führen, unser Epson-Drucker etwa spuckt bei jedem Scan eine spärlich bedruckte Seite aus. Sie sollten Ihre ersten Schritte daher besser im oben erwähnten Testnetz machen.

Eine Übersicht über die mitgelieferten Skripte finden Sie in der Dokumentation von Nmap (siehe ct.de/ygg5). Praktisch ist etwa das vulners-Skript, das zu den ermittelten Serverversionen bekannte Schwachstellen aus einer Online-Datenbank heraussucht. Eigene Skripte können Sie in der Programmiersprache Lua entwickeln.

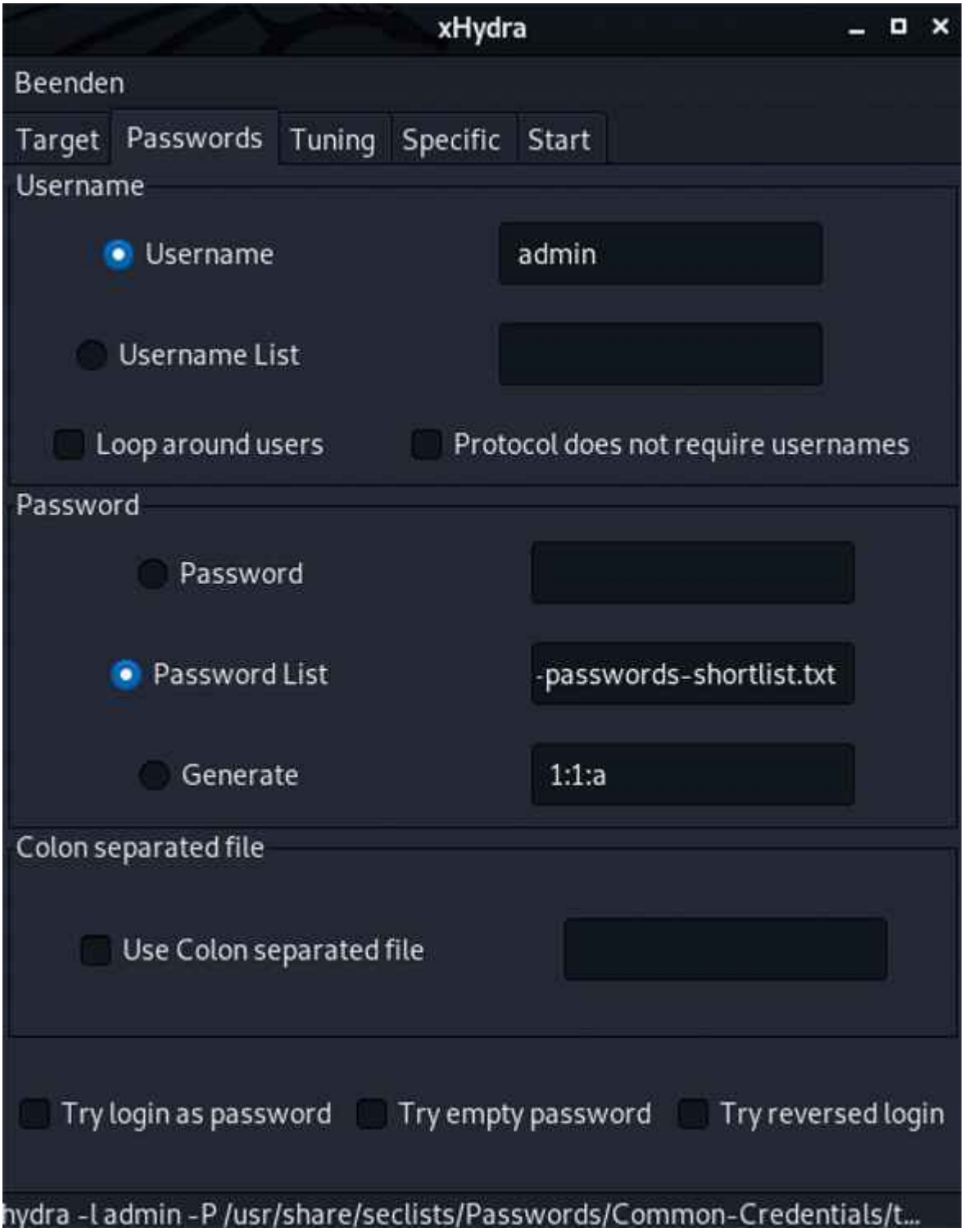


Was ist los im Netz? Der Netzwerkscanner Nmap liefert einen HTML-Bericht über alle Geräte und Dienste.

## Zugriff auf Server

Vernetzte Geräte wie WLAN-Kameras oder Smart-Home-Komponenten sind oft für eine Überraschung gut: Auf manchen Exemplaren laufen unerwartete Dienste, die im Worst Case sogar mit einem Standardpasswort für Gott und die Welt aus dem Internet erreichbar sind. Die entdecken Sie zum Beispiel mit einem Nmap-Scan (siehe „Netzwerk auskundschaften“). Doch dann stehen Sie erst mal vor verschlossener Tür, denn das Zugriffspasswort ist häufig ebenso wenig dokumentiert wie der Dienst selbst. Solche Dienste sind ein unkalkulierbares Sicherheitsrisiko.

Fehlt Ihnen das Passwort, können Sie versuchen, es zu erraten – oder Sie überlassen dem Login-Cracker **Hydra** die ganze Arbeit. Er unterstützt viele gängige Protokolle wie FTP, HTTP(S), SMB, SSH, Telnet und VNC, wodurch er universell einsetzbar ist. Sie können Hydra wahlweise auf der Shell benutzen oder mit xHydra eine grafische Oberfläche starten, um ein paar Parameter einzustellen und die Passwortsuche zu starten. Wichtig sind das Ziel, der Port und das richtige Protokoll im ersten Tab. Danach folgt die Konfiguration des Nutzernamens und einer Passwortliste. Falls Sie gerade keine zur Hand haben, können Sie unter Kali das Paket seclists installieren, das diverse Listen unter /usr/share/seclists/Passwords ablegt. Im letzten Tab ist der Output des Tools zu sehen, also im besten Fall das gesuchte Passwort.




Sesam, öffne Dich: Hydra probiert, sich mit beliebig langen Passwortlisten bei einem Server einzuloggen.

## IPv4-Traffic umleiten

ARP-Spoofing (auch ARP-Poisoning genannt) ist ein alter, aber nach wie vor effektiver Trick, um IPv4-Netzwerkverkehr umzulenken. Ein Angreifer im gleichen Netzwerk kann so den Datenverkehr anderer Teilnehmer ohne deren Zutun mitlesen und

manipulieren, etwa um sensible Daten abzugreifen oder Schadcode zu verbreiten. Das Ziel des Angriffs sind die ARP-Tabellen der Netzwerkclients. Darin ist vermerkt, unter welchen MAC-Adressen die IPs im lokalen Netz erreichbar sind. Durch gefälschte Nachrichten im Address Resolution Protocol (ARP) kann ein Angreifer die Tabellen verändern und Traffic umleiten, mitlesen und manipulieren. Eine solche Umleitung ist aber auch praktisch, um den Netzwerkverkehr einzelner Clients zu untersuchen, zum Beispiel, um herauszufinden, mit welchen Servern ein Smart-Home-Gerät spricht und ob die übertragenen Daten verschlüsselt sind.

Mit dem Sniffing-Tool **Ettercap** ist ARP-Spoofing sehr einfach, weil es alle nötigen Schritte vereint. Kali-Nutzer starten es über den Launcher („Sniffing & Spoofing/ettercap-graphical“). Wählen Sie zunächst das gewünschte Netzwerk-Interface. Anschließend müssen Sie noch die beiden IPs einstellen, zwischen denen Sie lauschen möchten, zum Beispiel Router-IP und die IP des Clients, für den Sie sich interessieren. Klicken Sie hierzu auf den Menüknopf (drei Punkte), „Targets“ und „Current Targets“. Über die Add-Buttons tragen Sie die IPs als Target 1 und 2 ein. Alternativ können Sie auch erst mal im lokalen Netz nach Clients scannen. Klicken Sie dafür im Menü unter „Hosts“ auf „Scan for hosts“. Kurz darauf können Sie die Netzwerkteilnehmer unter „Hosts/Host list“ einsehen und per Rechtsklick als Target hinzufügen.


Verkehrsumleitung: Ettercap nutzt ARP-Spoofing, um den Datenverkehr anderer Rechner über sich umzuleiten.
Jetzt müssen Sie das ARP-Spoofing nur noch auslösen: Klicken Sie oben rechts auf den Knopf, der an eine Weltkugel erinnert („MITM menu“) und auf „Arp poisoning…“. Über das Menü und „View/Connections“ können Sie live beobachten, wie die Daten durch Ihr System fließen. Sie erfahren dort unter anderem IP-Adresse, Hostname und Land der Gegenstelle, den genutzten Port und den Datenumfang. Ein Doppelklick auf eine Verbindung zeigt die übertragenen Daten an. Interessant sind zum Beispiel unverschlüsselte HTTP-Verbindungen auf Port 80, weil Sie deren Inhalt ohne weitere Hilfsmittel als Klartext lesen können.

Ettercap bringt einige interessante Plug-ins mit, die Sie im Menü unter „Plugins/Manage plugins“ durchstöbern und per Doppelklick aktivieren können. Darunter findet sich auch ein Gegengift für ARP-Spoofing: Der „arp_cop“ soll ARP-Manipulationen anzeigen. Wenn Ihnen die Analysefunktionen von Ettercap nicht ausreichen, können Sie Werkzeuge wie Wireshark nutzen, denn der angezapfte Traffic ist auf dem anfangs eingestellten Netzwerk-Interface sichtbar. Mit den Linux-Werkzeugen iptables oder nftables können Sie den Datenverkehr

zudem beliebig umleiten, zum Beispiel an einen lokalen Server.

## WLAN auf dem Prüfstand

Funknetzwerke müssen viel aushalten, denn jeder in Reichweite kann sie attackieren. Wenn Sie sich nicht darauf verlassen möchten, dass Ihr WLAN schon sicher genug sein wird, können Sie mit Hacking-Tools die Probe aufs Exempel machen. Kali hat mehrere davon an Bord, die unterschiedliche Angriffsszenarien durchspielen. Zur Nutzung benötigen Sie ein WLAN-Interface, das sich in den „Monitor Mode“ schalten lässt und zudem gut von Linux unterstützt wird. Solche gibt es als USB-WLAN-Adapter schon für weniger als 20 Euro, zum Beispiel von CSL Computer (Modell 27395) oder Alfa Network. Ob Ihr Interface den nötigen Modus unterstützt, erfahren Sie über eine Google-Suche nach dem Chipsatz, etwa „Ralink RT5572 monitor mode“.

Um die gängigsten Angriffsarten zu simulieren, können Sie zu **wifite2** greifen, das diverse WLAN-Hacking-Werkzeuge für Sie ansteuert, um Sicherheitsprobleme aufzuspüren. Sie starten es wie folgt:

```
sudo wifite --random-mac --kill
```

Die Option --random-mac sorgt dafür, dass die genutzte Geräteadresse des WLAN-Adapters zufällig ausgewürfelt wird und --kill beendet störende Prozesse, die dem Tool in die Quere kommen könnten. Wifite fragt Sie zunächst, welches WLAN-Interface genutzt werden soll und macht sich anschließend sofort an die Arbeit. Kurz darauf listet es alle Netze in Reichweite auf.


Mit wifite2 finden Sie heraus, wie sicher Ihr WLAN wirklich ist. Im ersten Schritt zeigt es alle Netze in Reichweite samt Verschlüsselung und WPS-Status an.
Sobald Sie Ihr WLAN gefunden haben, beenden Sie den Scan mit Strg+C und geben die Indexzahl des Netzes ein. Wifite testet anschließend die wichtigsten Angriffsmöglichkeiten der Reihe nach durch, allen voran WPS-Attacken (Pixie Dust und Brute Force auf die PIN), die bei anfälligen Routern am schnellsten zum Ziel führen. Danach nimmt sich das Tool WPA(2) zur Brust und schließlich das steinalte WEP-Verfahren. Gegen WPA3 kommt es derzeit nicht an.

Der WPA(2)-Angriff läuf relativ simpel ab: Zunächst zwingt wifite die Clients per Deauthentication-Paket, die Verbindung zum Router zu trennen. Bei der anschließenden Neuanmeldung zeichnet es den Handshake auf und setzt anschließend den Passwort-Cracker hashcat darauf an. Der probiert eine Reihe von Passwörtern aus einer langen Liste durch, bis er fündig wird. Die wichtigsten Schutzmaßnahmen in aller Kürze: Nutzen Sie lange WPA-Passwörter (mindestens 16 Zeichen, besser mehr), aktivieren Sie möglichst WPA2/3 (Mixed Mode) und die geschützte Anmeldung von WLAN-Geräten (Protected Management Frames, PMF).

# Datenlecks im Webserver finden

Webserver sind prinzipbedingt meist für jeden erreichbar – und damit zwangsläufig auch für Angreifer, die nach Sicherheitslücken, Datenlecks und schwachen Passwörtern suchen. Das geschieht längst nicht mehr mühsam von Hand, sondern automatisiert. So können die bösen Buben tausende Websites innerhalb kurzer Zeit auf Schwachstellen abklopfen und müssen bei der Wahl ihres Angriffsziels nicht wählerisch sein.

Wenn Sie eine Website betreiben, müssen Sie also fest mit ungebetenem Besuch rechnen. Und wenn es eine Sicherheitslücke gibt, wird diese früher oder später auch ausgenutzt. Sie können den Angreifern jedoch die Petersilie verhageln, indem Sie sich deren Tools zu eigen machen, um etwaige Schwachstellen selbst frühzeitig zu finden. Auch diese Tools dürfen Sie nur gegen eigene Server und niemals unbefugt gegen fremde Systeme einsetzen, sonst drohen juristische Konsequenzen (siehe Seite 170). Beachten Sie, dass die Werkzeuge sehr viele Anfragen und damit potenziell auch eine hohe Last erzeugen, was die Erreichbarkeit des Servers beeinträchtigen kann.

Ein einfaches, aber effektives Werkzeug zur Suche nach Datenlecks ist **DIRB**. Es probiert eine lange Liste mit gängigen Verzeichnisnamen wie /admin, /backups oder /internal durch, um Ordner zu finden, die nicht für die Öffentlichkeit bestimmt, aber trotzdem für jeden zugänglich sind. Ferner kann das Hacking-Programm Verzeichnisnamen per Brute Force erraten. Gibt es einen Treffer, versucht DIRB auch noch mögliche Unterordner zu entdecken. Die Bedienung ist einfach:

```
dirb https://ihre-website.example
```

Unzureichend geschützte Verzeichnisse sind häufig die Ursache für Datenlecks, etwa wenn darin Backups der MySQL-Datenbank oder Konfigurationsdateien mit Zugangsdaten gespeichert sind.

Diese Blindgänger sollten Sie rechtzeitig entschärfen, zum Beispiel durch einen Zugriffsschutz auf dem Verzeichnis, sofern die Daten überhaupt auf dem öffentlichen Server liegen müssen.

## WordPress-Lücken aufspüren

Das Content-Management-System WordPress ist sehr verbreitet (siehe S. 60 ff.) und bei Angreifern entsprechend hoch im Kurs. Häufig wird es in veralteten – und somit verwundbaren – Versionen betrieben oder mit anfälligen Plug-ins und Themes. Auch Konfigurationsfehler begünstigen eine Fremdübernahme. Solche Schlupflöcher aufzudecken ist inzwischen ein Kinderspiel – zum Beispiel mit dem WordPress Security Scanner **WPScan**. Der kann Ihnen gute Dienste beim Absichern Ihrer Website leisten.

Auf der GitHub-Seite des Ruby-Tools erfahren Sie, wie Sie es unter Linux, macOS und als Docker-Container an den Start bringen (siehe ct.de/ygg5). Kali-Nutzer können sich das sparen, das Programm ist vorinstalliert. Um Ihre WordPress-Installation zu scannen, füttern Sie WPScan einfach mit der URL: wpscan --url https://ihre-website.example/wordpress

Bevor die Analyse beginnt, lädt der Security Scanner eine Datenbank mit aktuellen Infos aus dem Netz. Das geschieht normalerweise automatisch, wenn Sie es jedoch auf die verwundbaren WordPress-Installationen von RasPwn loslassen möchten (siehe „Angreifen erlaubt“), haben Sie keine Internetverbindung, solange Sie mit dem Raspi-Testnetz verbunden sind. In diesem Fall sollten Sie sich zunächst mit Ihrem normalen Netz verbinden und das Update mit wpscan --update manuell starten. Trennen Sie die Verbindung danach, ehe Sie schließlich den Scan aus dem RasPwn-Netz anwerfen.

Nach und nach gibt WPScan interessante Informationen über die WordPress-Installation aus, darunter die WordPress-Version samt Erscheinungsdatum und eine Einschätzung, ob diese Ausgabe

nach aktuellem Stand der Dinge sicher ist. Weiterhin identifiziert das Tool die Versionen von Webserver und PHP sowie Themes, Plug-ins und diverse Konfigurationsfehler. Prinzipiell kann man selbst im Netz recherchieren, welche Sicherheitslücken in den identifizierten Versionen klaffen. Aber auch das kann Ihnen WPScan abnehmen. Diese Informationen fragt das Tool über ein Web-API vom Server der Entwickler ab – dafür ist eine kostenfreie Registrierung nötig (siehe ct.de/ygg5).

## Datenbank-Lecks verhindern

Die Kronjuwelen einer Website sind häufig Kunden- oder gar Nutzerdaten. Diese können Onlinegauner im Darknet leicht zu Geld machen. In der Regel bewahren Webanwendungen solche Daten in einer Datenbank auf, die natürlich gut geschützt sein sollte. Die Betonung liegt auf sollte, denn allzu oft gelingt es Cyberkriminellen, Kundendaten im großen Stil aus Datenbanken abzugreifen.

Eine häufige Ursache sind sogenannte SQL-Injection-Lücken: Dabei spricht der Angreifer nicht direkt mit dem Datenbankserver, sondern versucht stattdessen, die Webanwendung dazu zu bringen, eingeschleuste SQL-Befehle auf der Datenbank auszuführen. Das Resultat ist häufig, dass die Datenbank über die Web-Anwendung massenweise sensible Datensätze ausspuckt.

Sie ahnen es vielleicht schon: Auch für solche Lücken gibt es ein Hacking-Tool, in diesem Fall **SQLmap**. Es unterstützt zahlreiche Datenbanken, unter anderem Oracle, MySQL, MariaDB, MS SQL Server, PostgreSQL und SQLite. Je nach Datenbanktyp und Berechtigungen kann es auch Dateien auf den Webserver schreiben. Hacker können so versuchen, eine Web-Shell hochzuladen, um den Server dauerhaft fernzusteuern.

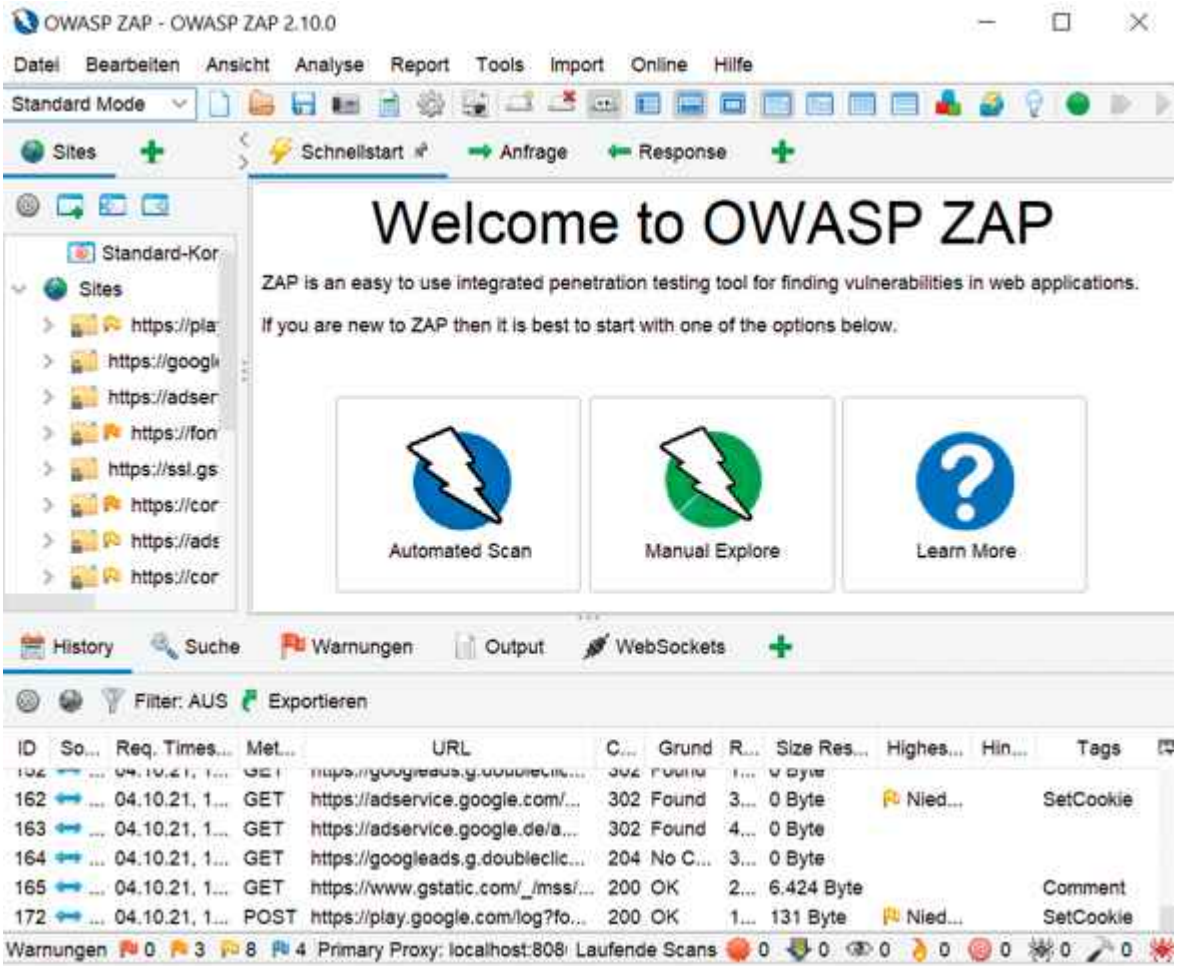
Für einen ersten Funktionstest können Sie die absichtlich anfällige „Wacko Picko“-Website von RasPwn mit SQLmap scannen.

Das Login-Formular der Website sendet beim Abschicken zwei POST-Parameter, nämlich „username“ und „password“, die der Schwachstellenscanner in diesem Beispiel in die Mangel nehmen soll. Um zu überprüfen, ob die Website bei der Auswertung dieser Parameter patzt, können Sie das Tool mit --data anweisen, genau das herauszufinden:

```
sqlmap -u "http://wackopicko.playground.raspwn.org/users/login.php" --data="username=1&password=1" --banner
```

Die Option „banner“ findet die Datenbankversion und das Betriebssystem des Servers heraus, wenn die Website verwundbar ist. Falls Sie den Datenbankinhalt gleich auslesen möchten, ersetzen Sie --banner einfach durch --dump.

Solche SQL-Injections vermeiden Sie, indem Sie Eingaben von außen konsequent überprüfen, bevor sie verarbeitet oder gar in Datenbankbefehle integriert werden. Weiterhin ist der Einsatz sogenannter „Prepared Statements“ sinnvoll, bei denen Sie zunächst den Aufbau des SQL-Befehls festlegen, ehe Sie darin einen Platzhalter mit den von außen angelieferten Werten füllen. Am besten basteln Sie die Datenbankbefehle nicht selbst zusammen, sondern setzen auf eine hinreichend getestete ORM-Bibliothek (Object-Relational Mapping), die bereits gegen alle Eventualitäten abgesichert ist.




Der Zed Attack Proxy (ZAP) macht verschlüsselten Datenverkehr im Klartext sichtbar und spürt Schwachstellen in Web-Anwendungen und APIs auf.

## Browser- und App-Traffic

Der **OWAP Zed Attack Proxy (ZAP)** ist ein universelles Werkzeug zur Analyse und Manipulation von Web-Traffic (HTTP/HTTPS). Sie können sich damit zum Beispiel zwischen Browser und Internet klemmen oder den Datenverkehr Ihres Smartphones durch den Proxy schleusen, um herauszufinden, welche Daten wohin übertragen werden. Eine Stärke des ZAP ist, dass es die identifizierten Gegenstellen, also Webanwendungen, API-Endpunkte und so weiter gleich noch auf Sicherheitsprobleme abklopfen kann. ZAP ist eine Java-Anwendung und läuft unter Windows, Linux und macOS.

Nach dem ersten Start klicken Sie am besten auf den Browser-Knopf in der Symbolleiste, um einen perfekt vorkonfigurierten

Webbrowser zu starten. Dessen Datenverkehr wird automatisch durch den Proxy geschleust. Öffnen Sie damit eine Website, um den Traffic in ZAP zu inspizieren. Wenn Sie den Browser auf diese Weise starten, schleust ZAP in die geöffneten Websites eine eigene Oberfläche namens ZAP HUD ein, über die Sie zahlreiche Funktionen direkt aus dem Browser steuern können. Klicken Sie auf den Knopf „Take the HUD Tutorial“, um eine Einführung zu erhalten und einige der nützlichen Funktionen kennenzulernen.

## Gemischtwaren

Dieser Artikel liefert Ihnen nur eine kleine Auswahl an Hacking-Tools. Das Angebot ist riesig und täglich kommen neue dazu. Einige davon sind sehr komplex oder nur für bestimmte Zielgruppen interessant. Dazu zählt das modular aufgebaute Pentesting-Framework **Metasploit**, das professionelle Penetrationtester nutzen, um einen kompletten Angriff zu simulieren: vom Aufspüren der Ziele über das Ausnutzen von Sicherheitslücken bis hin zum Ausleiten der Datenbeute. Falls Sie sich eingehender mit Hacking beschäftigen möchten, sollten Sie einen Blick darauf werfen. In eine ähnliche Kerbe schlägt **PowerShell Empire**, das Pentestern weitreichenden Rechnerzugriff verschafft, ohne verdächtigen Binärcode auf dem System zu hinterlassen – die Angriffsmodule bestehen aus Skripten für die Windows PowerShell.

Wer eine Windows-Domäne administriert, sollte Tools wie **mimikatz** kennen, das Anmeldeinformationen aus dem Arbeitsspeicher der Windows-Clients ausliest. Angreifer gelangen damit schlimmstenfalls an die Zugangsdaten eines Domänen-Administrators und können das gesamte Netzwerk übernehmen. Den Domänencontroller spüren die Eindringlinge vorher mit **AdFind** von joeware auf. Auch **PsExec** aus Microsofts SysInternals-Kollektion birgt ein gewisses Missbrauchspotenzial: Es wird genutzt, um Befehle auf anderen Rechnern im Netzwerk auszuführen. Angreifer nutzen es mit

zuvor erbeutete Anmeldeinformationen.

Das von der NSA entwickelte Reverse-Engineering-Toolkit **Ghidra** ist interessant, wenn Sie ausführbaren Code (wie EXE- und DLL-Dateien) bis ins letzte Bit auseinandernehmen und verstehen möchten. Es dekompiliert Binärdateien und kann sie auch wieder zusammenbauen, ähnlich wie der kommerzielle Disassembler IDA Pro. In c't 14/2020 haben wir Ghidra ausführlicher getestet (siehe ct.de/ygg5).

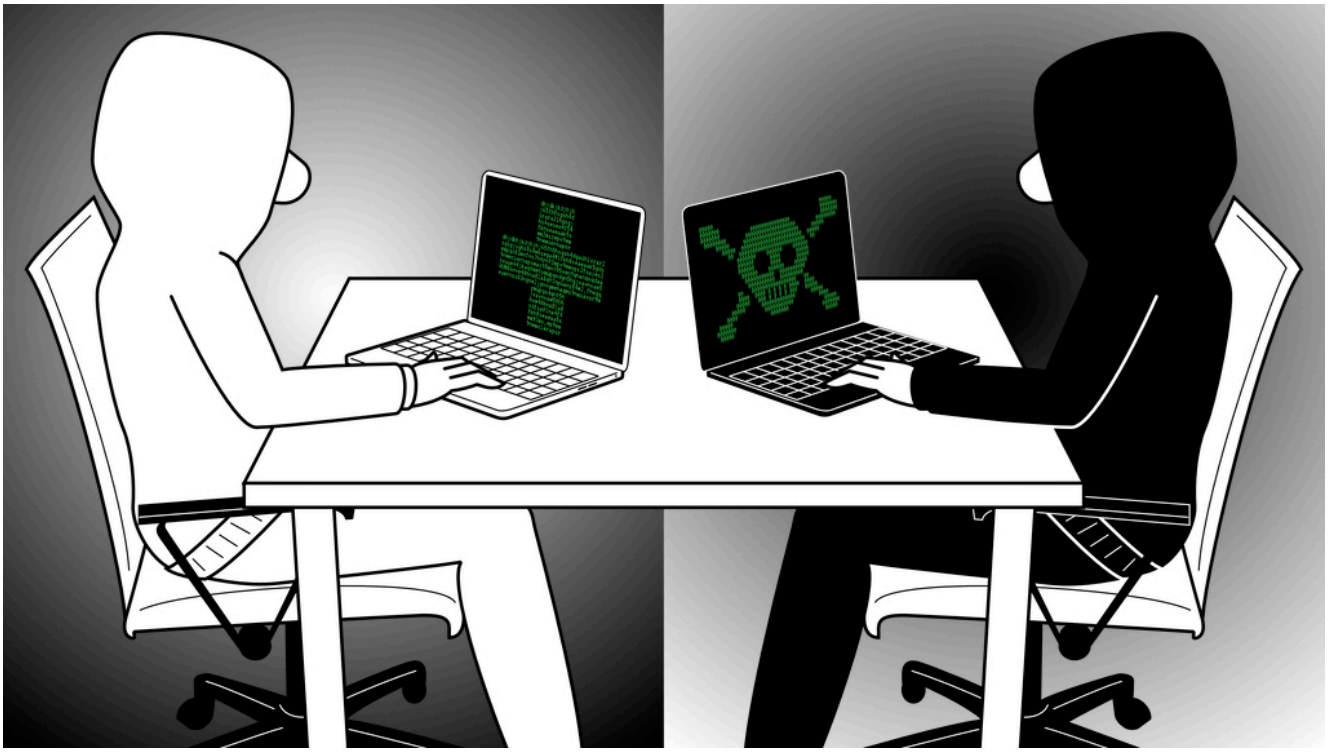
## Fazit

Die vorgestellten Hacking-Tools decken einen weiten Bereich ab. Manche Techniken sind erschreckend simpel, andere fordern viel Einarbeitung und Erfahrung. Sich damit zu beschäftigen lohnt sich aber: Sie lernen so, wie ein Angreifer zu denken und Ihre eigenen Sicherheitsprobleme und -lücken aufzuspüren. Das ist hilfreich – ganz gleich, ob Sie nur eine private WordPress-Site betreiben oder gar für die Sicherheit Ihrer Kunden verantwortlich sind. *(rei@ct.de)*

**Hacking-Tools & weitere Infos:** ct.de/ygg5

---

# Hacking-Werkzeug für Fortgeschrittene



## Gute Tools, böse Tools

Mit den Hacking-Tools von Penetrationtestern finden Sie Sicherheitslücken in Ihren Websites, Netzwerken und Anwendungen, bevor es andere tun.

# Hacking-Werkzeug für Fortgeschrittene

Mit den Hacking-Tools von Penetrationtestern finden Sie Sicherheitslücken in Ihren Websites, Netzwerken und Anwendungen, bevor es andere tun.

Von Ronald Eikenberg und Alexander Königstein

Hollywood weiß Hacker-Aktivitäten in Szene zu setzen: Vor unzähligen Monitoren mit monochromatischen Benutzeroberflächen sitzen Gestalten im Kapuzenpulli und brechen durch die Firewalls. In der Realität geht es weitaus nüchterner zu, denn die eigentliche Action spielt sich hinter den Kulissen ab. Das ist aber nicht weniger faszinierend, denn Hacking-Tools

leisten erstaunliche Dinge, wenn man sie richtig einsetzt. Das setzt etwas Wissen und Erfahrung voraus, doch beides baut sich ganz von selbst auf, wenn Sie erst mal Feuer gefangen haben. In diesem Artikel stellen wir eine Auswahl interessanter Profi-Werkzeuge vor, die sowohl auf der dunklen als auch auf der hellen Seite der Macht genutzt werden. Stöbern Sie auch im Artikel „Hack Dich selbst“ auf Seite 18, der nützliche Problemlöser für den Alltag präsentiert.

Mit den im Folgenden vorgestellten Profi-Tools spüren Sie Sicherheitslücken in Ihren Websites, Netzwerken, Apps, IoT-Geräten und vielem mehr auf. Anschließend können Sie gezielt Schutzmaßnahmen ergreifen und die Schlupflöcher stopfen, bevor es zu spät ist. Die meisten Hacking-Tools laufen am besten oder ausschließlich unter dem Betriebssystem Linux. Eine gute Grundlage für die ersten Schritte ist **Kali Linux**, das von Haus aus bestens auf die Bedürfnisse von Hackern zugeschnitten ist. Auf Seite 30 erfahren Sie, wie Sie sich einen Kali-USB-Stick mit persistenter Datenpartition für Ihre Experimente erstellen. Download-Links und weiterführende Informationen zu allen vorgestellten Tools finden Sie online unter ct.de/ygg5. Aber genug der Vorrede – jetzt geht es in die Vollen!

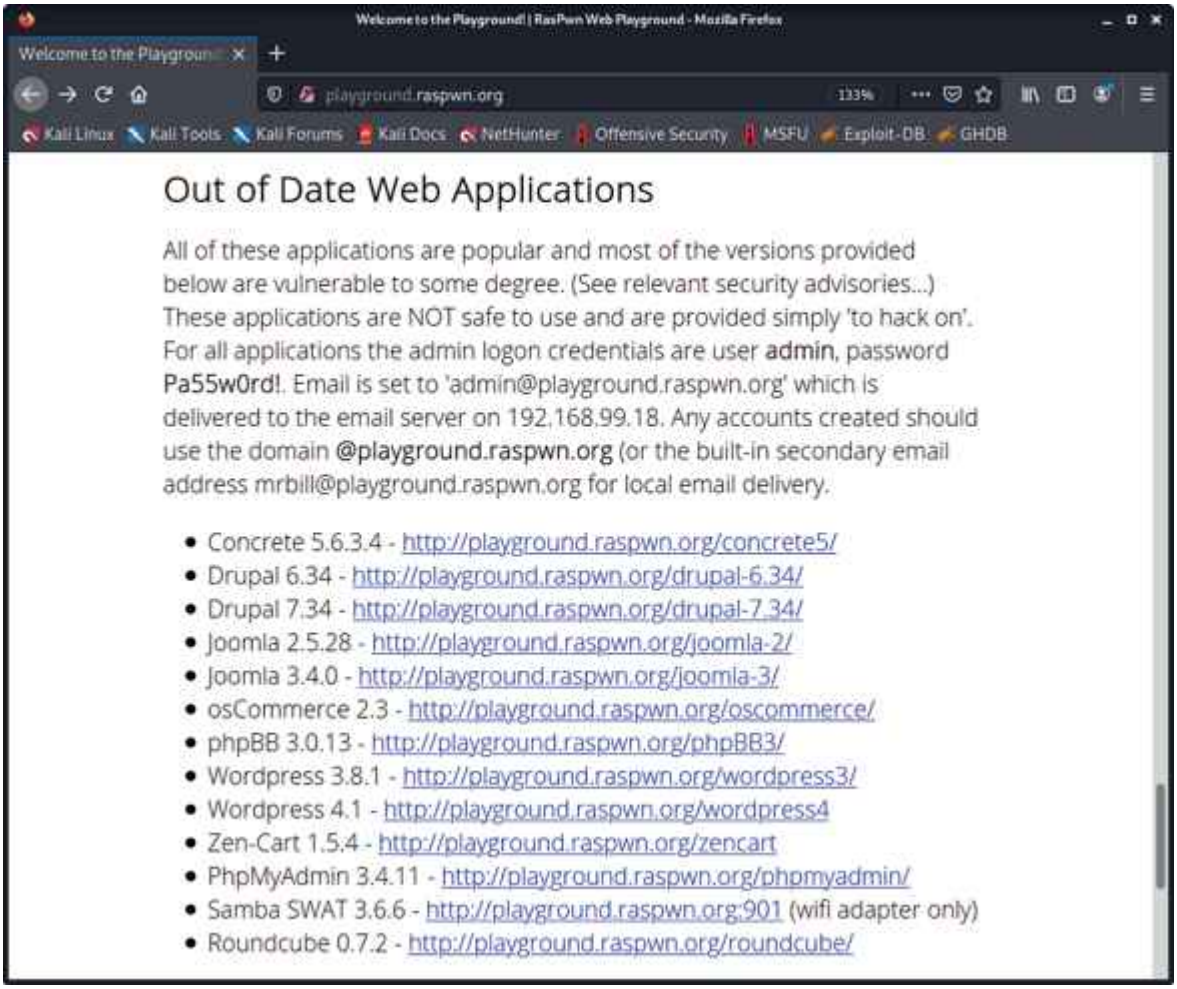
## Angreifen erlaubt

Die hier genannten Hacking-Tools sind nicht illegal, aber natürlich dürfen Sie damit nicht gegen geltende Gesetze verstoßen (siehe Seite 170). Damit Sie gar nicht erst in Versuchung kommen, die Tools unerlaubt an fremden Servern zu testen, sollten Sie sich eine geeignete Übungsumgebung schaffen – zum Beispiel ein Testnetz, in dem sich ausschließlich Systeme befinden, die Sie attackieren möchten und dürfen.

Ein geeignetes Angriffsziel ist **RasPwn**, das ein ganzes Netzwerk voller verwundbarer Server simuliert, an denen Sie sich austoben können. Sie übertragen es einfach auf eine MicroSD-Karte, die Sie anschließend in einen Raspi-

Kleincomputer stecken (mindestens Raspi 2B). Nach dem Booten meldet sich ein WLAN namens „RasPwn OS“, zu dem Sie mit dem Passwort „In53cur3!“ eine Verbindung herstellen. Aus dem Netz öffnen Sie http://playground.raspwn.org mit einem Browser Ihrer Wahl, wo Sie mit allen wichtigen Informationen über das virtuelle Netzwerk und die angreifbaren Server versorgt werden. Ein Netzwerkkabel darf nicht mit dem Raspi verbunden sein, andernfalls hat das hochgradig verwundbare Image unter Umständen Zugriff auf Ihr Hauptnetzwerk und das Internet – was Sie tunlichst vermeiden sollten.

Zu den möglichen Angriffszielen zählen verwundbare WordPress-Installationen, eine steinalte Version des Webshop-Systems osCommerce, das Datenbank-Tool phpMyAdmin, ein Mailserver, Samba und so weiter. Auch das Debian-Linux, auf dem RasPwn basiert, hat schon fast sieben Jahre auf dem Buckel und ist so löchrig wie ein Schweizer Käse. Obendrauf gibt es zahlreiche Web-Applikationen wie OWASP Bricks und Damn Vulnerable Web Application (DVWA), die nur mit dem Ziel entwickelt wurden, möglichst verwundbar zu sein, um typische Sicherheitslücken am lebenden Objekt zu demonstrieren. Viele dieser Projekte sind online dokumentiert, wodurch sie sich hervorragend zum Lernen eignen (siehe ct.de/ygg5).



Das Raspi-Image RasPwn enthält etliche verwundbare Web-Apps – und das mit voller Absicht.

## Netzwerk auskundschaften

Hat sich ein Angreifer Zugriff auf ein fremdes Netzwerk verschafft, etwa durch eine frei zugängliche Netzwerkbuchse im Aufenthaltsraum, eine per E-Mail eingeschleuste Malware oder ein schwaches WLAN-Passwort, dann wird er sich erst mal einen Überblick über die Geräte im Netz verschaffen, um mögliche Angriffsziele auszumachen. Hierbei ist der mächtige Netzwerkscanner **Nmap** (Network Mapper) die erste Wahl. Er spürt nicht nur die Rechner, Drucker, NAS, Server, Router und vieles mehr auf, sondern auch die darauf laufenden Dienste. Durch Skripte lässt sich der Scanner beliebig erweitern, etwa um die entdeckten Clients gleich noch auf Sicherheitslücken abzuklopfen. Das alles ist nützlich, um verwundbare Geräte im eigenen Netz aufzuspüren und sie anschließend entweder abzusichern oder aus dem Verkehr zu ziehen.

Nmap läuft auf Linux, macOS und Windows, bei Kali Linux ist er inklusive. Wenn Sie auf einer Shell nmap ohne Parameter eintippen, zeigt das Tool die wichtigsten Betriebsmodi an. Um einfach und schnell die offenen Ports eines bestimmten Hosts herauszufinden, hängen Sie einfach dessen IP-Adresse an den Befehl an, etwa nmap 192.168.178.1. Das müssen Sie zwar nicht als root ausführen, es lohnt sich aber: So finden Sie mehr über die Clients heraus, im konkreten Fall die MAC-Adressen. IPv6-Adressen scannen Sie mit dem Parameter -6.

Sie können den Scan auf einen IP-Bereich ausweiten, den Sie zum Beispiel mit 192.168.178.1-50 definieren (alle IP-Adressen, die mit 192.168.178 anfangen und mit .1 bis .50 enden). Oder Sie scannen gleich das gesamte /24-Subnetz (alle bis .255): nmap 192.168.178.0/24. Ist der Scan abgeschlossen, präsentiert Ihnen Nmap die Ergebnisse auf der Shell, vorher lässt das Tool nicht von sich hören. Wer ungeduldig ist, kann mit --stats-every 10s festlegen, dass Nmap regelmäßig ein Statusupdate ausgibt.

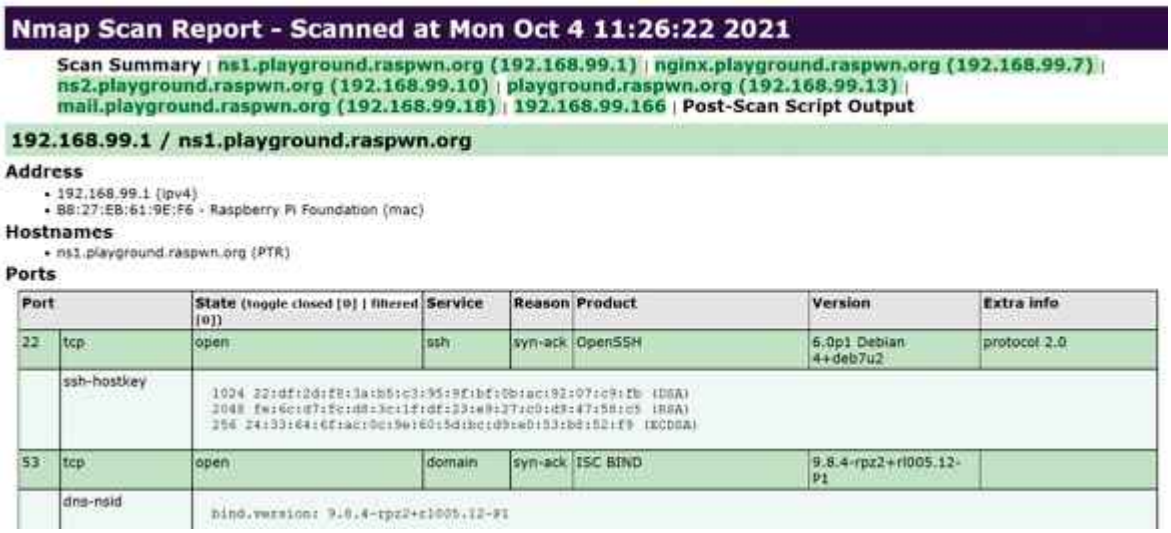
Wirklich komfortabel lesbar ist der Bericht auf der Shell nicht. Sie können jedoch leicht einen formatierten HTML-Report erstellen, indem Sie zunächst Nmap mit -oX ergebnis.xml anweisen, einen XML-Export der Ergebnisse zu schreiben. Anschließend bauen Sie daraus mit dem unter Kali vorinstallierten Tool xsltproc eine HTML-Datei, die Sie mit jedem Browser öffnen können: xsltproc ergebnis.xml -o ergebnis.html

Mit dem einfachen Scan kratzen Sie erst an der Oberfläche der Möglichkeiten. Mehr können Sie Nmap über verschiedene Scan-Optionen entlocken (siehe ct.de/ygg5). Sehr umfangreich ist der Modus -A, der unter anderem die Betriebssystem- und Versionserkennung (Fingerprinting) scharf schaltet. Diesen Modus sollten Sie mit sudo starten, damit Ihnen nichts entgeht. Aber aufgepasst: Nmap greift in diesem Fall aktiv auf die entdeckten Server zu, um Informationen einzuholen. Das kann zu unerwarteten Effekten führen, unser Epson-Drucker etwa

spuckt bei jedem Scan eine spärlich bedruckte Seite aus. Sie sollten Ihre ersten Schritte daher besser im oben erwähnten Testnetz machen.

Hardcore

Eine Übersicht über die mitgelieferten Skripte finden Sie in der Dokumentation von Nmap (siehe ct.de/ygg5). Praktisch ist etwa das vulners-Skript, das zu den ermittelten Serverversionen bekannte Schwachstellen aus einer Online-Datenbank heraussucht. Eigene Skripte können Sie in der Programmiersprache Lua entwickeln.

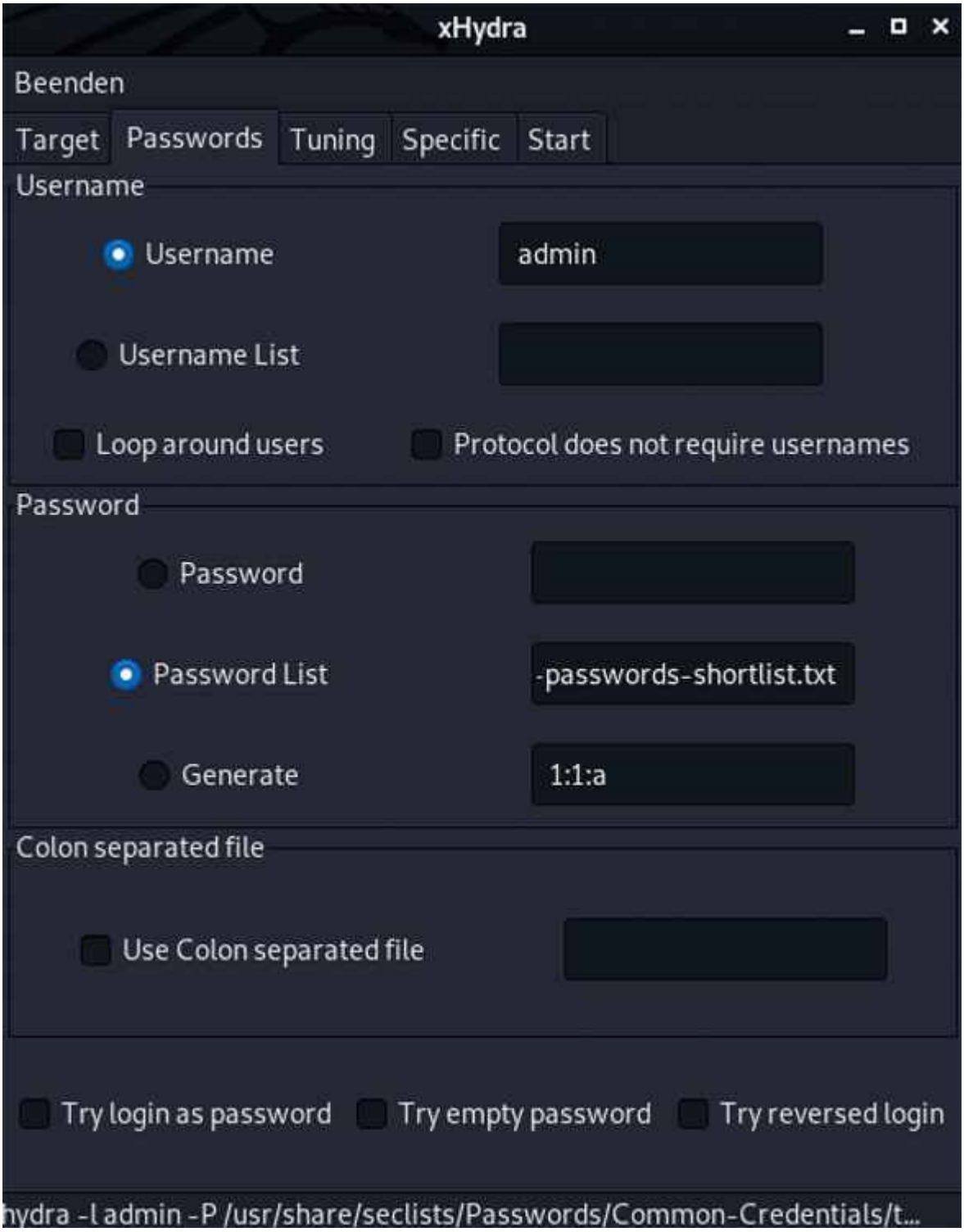


Was ist los im Netz? Der Netzwerkscanner Nmap liefert einen HTML-Bericht über alle Geräte und Dienste.

## Zugriff auf Server

Vernetzte Geräte wie WLAN-Kameras oder Smart-Home-Komponenten sind oft für eine Überraschung gut: Auf manchen Exemplaren laufen unerwartete Dienste, die im Worst Case sogar mit einem Standardpasswort für Gott und die Welt aus dem Internet erreichbar sind. Die entdecken Sie zum Beispiel mit einem Nmap-Scan (siehe „Netzwerk auskundschaften“). Doch dann stehen Sie erst mal vor verschlossener Tür, denn das Zugriffspasswort ist häufig ebenso wenig dokumentiert wie der Dienst selbst. Solche Dienste sind ein unkalkulierbares Sicherheitsrisiko.

Fehlt Ihnen das Passwort, können Sie versuchen, es zu erraten – oder Sie überlassen dem Login-Cracker **Hydra** die ganze Arbeit. Er unterstützt viele gängige Protokolle wie FTP, HTTP(S), SMB, SSH, Telnet und VNC, wodurch er universell einsetzbar ist. Sie können Hydra wahlweise auf der Shell benutzen oder mit xHydra eine grafische Oberfläche starten, um ein paar Parameter einzustellen und die Passwortsuche zu starten. Wichtig sind das Ziel, der Port und das richtige Protokoll im ersten Tab. Danach folgt die Konfiguration des Nutzernamens und einer Passwortliste. Falls Sie gerade keine zur Hand haben, können Sie unter Kali das Paket seclists installieren, das diverse Listen unter /usr/share/seclists/Passwords ablegt. Im letzten Tab ist der Output des Tools zu sehen, also im besten Fall das gesuchte Passwort.




Sesam, öffne Dich: Hydra probiert, sich mit beliebig langen Passwortlisten bei einem Server einzuloggen.

## IPv4-Traffic umleiten

ARP-Spoofing (auch ARP-Poisoning genannt) ist ein alter, aber nach wie vor effektiver Trick, um IPv4-Netzwerkverkehr umzulenken. Ein Angreifer im gleichen Netzwerk kann so den Datenverkehr anderer Teilnehmer ohne deren Zutun mitlesen und

manipulieren, etwa um sensible Daten abzugreifen oder Schadcode zu verbreiten. Das Ziel des Angriffs sind die ARP-Tabellen der Netzwerkclients. Darin ist vermerkt, unter welchen MAC-Adressen die IPs im lokalen Netz erreichbar sind. Durch gefälschte Nachrichten im Address Resolution Protocol (ARP) kann ein Angreifer die Tabellen verändern und Traffic umleiten, mitlesen und manipulieren. Eine solche Umleitung ist aber auch praktisch, um den Netzwerkverkehr einzelner Clients zu untersuchen, zum Beispiel, um herauszufinden, mit welchen Servern ein Smart-Home-Gerät spricht und ob die übertragenen Daten verschlüsselt sind.

Mit dem Sniffing-Tool **Ettercap** ist ARP-Spoofing sehr einfach, weil es alle nötigen Schritte vereint. Kali-Nutzer starten es über den Launcher („Sniffing & Spoofing/ettercap-graphical“). Wählen Sie zunächst das gewünschte Netzwerk-Interface. Anschließend müssen Sie noch die beiden IPs einstellen, zwischen denen Sie lauschen möchten, zum Beispiel Router-IP und die IP des Clients, für den Sie sich interessieren. Klicken Sie hierzu auf den Menüknopf (drei Punkte), „Targets“ und „Current Targets“. Über die Add-Buttons tragen Sie die IPs als Target 1 und 2 ein. Alternativ können Sie auch erst mal im lokalen Netz nach Clients scannen. Klicken Sie dafür im Menü unter „Hosts“ auf „Scan for hosts“. Kurz darauf können Sie die Netzwerkteilnehmer unter „Hosts/Host list“ einsehen und per Rechtsklick als Target hinzufügen.


Verkehrsumleitung: Ettercap nutzt ARP-Spoofing, um den Datenverkehr anderer Rechner über sich umzuleiten.
Jetzt müssen Sie das ARP-Spoofing nur noch auslösen: Klicken Sie oben rechts auf den Knopf, der an eine Weltkugel erinnert („MITM menu“) und auf „Arp poisoning…“. Über das Menü und „View/Connections“ können Sie live beobachten, wie die Daten durch Ihr System fließen. Sie erfahren dort unter anderem IP-Adresse, Hostname und Land der Gegenstelle, den genutzten Port und den Datenumfang. Ein Doppelklick auf eine Verbindung zeigt die übertragenen Daten an. Interessant sind zum Beispiel unverschlüsselte HTTP-Verbindungen auf Port 80, weil Sie deren Inhalt ohne weitere Hilfsmittel als Klartext lesen können.

Ettercap bringt einige interessante Plug-ins mit, die Sie im Menü unter „Plugins/Manage plugins“ durchstöbern und per Doppelklick aktivieren können. Darunter findet sich auch ein Gegengift für ARP-Spoofing: Der „arp_cop“ soll ARP-Manipulationen anzeigen. Wenn Ihnen die Analysefunktionen von Ettercap nicht ausreichen, können Sie Werkzeuge wie Wireshark nutzen, denn der angezapfte Traffic ist auf dem anfangs eingestellten Netzwerk-Interface sichtbar. Mit den Linux-Werkzeugen iptables oder nftables können Sie den Datenverkehr

zudem beliebig umleiten, zum Beispiel an einen lokalen Server.

## WLAN auf dem Prüfstand

Funknetzwerke müssen viel aushalten, denn jeder in Reichweite kann sie attackieren. Wenn Sie sich nicht darauf verlassen möchten, dass Ihr WLAN schon sicher genug sein wird, können Sie mit Hacking-Tools die Probe aufs Exempel machen. Kali hat mehrere davon an Bord, die unterschiedliche Angriffsszenarien durchspielen. Zur Nutzung benötigen Sie ein WLAN-Interface, das sich in den „Monitor Mode“ schalten lässt und zudem gut von Linux unterstützt wird. Solche gibt es als USB-WLAN-Adapter schon für weniger als 20 Euro, zum Beispiel von CSL Computer (Modell 27395) oder Alfa Network. Ob Ihr Interface den nötigen Modus unterstützt, erfahren Sie über eine Google-Suche nach dem Chipsatz, etwa „Ralink RT5572 monitor mode“.

Um die gängigsten Angriffsarten zu simulieren, können Sie zu **wifite2** greifen, das diverse WLAN-Hacking-Werkzeuge für Sie ansteuert, um Sicherheitsprobleme aufzuspüren. Sie starten es wie folgt:

```
sudo wifite --random-mac --kill
```

Die Option --random-mac sorgt dafür, dass die genutzte Geräteadresse des WLAN-Adapters zufällig ausgewürfelt wird und --kill beendet störende Prozesse, die dem Tool in die Quere kommen könnten. Wifite fragt Sie zunächst, welches WLAN-Interface genutzt werden soll und macht sich anschließend sofort an die Arbeit. Kurz darauf listet es alle Netze in Reichweite auf.


Mit wifite2 finden Sie heraus, wie sicher Ihr WLAN wirklich ist. Im ersten Schritt zeigt es alle Netze in Reichweite samt Verschlüsselung und WPS-Status an.
Sobald Sie Ihr WLAN gefunden haben, beenden Sie den Scan mit Strg+C und geben die Indexzahl des Netzes ein. Wifite testet anschließend die wichtigsten Angriffsmöglichkeiten der Reihe nach durch, allen voran WPS-Attacken (Pixie Dust und Brute Force auf die PIN), die bei anfälligen Routern am schnellsten zum Ziel führen. Danach nimmt sich das Tool WPA(2) zur Brust und schließlich das steinalte WEP-Verfahren. Gegen WPA3 kommt es derzeit nicht an.

Der WPA(2)-Angriff läuf relativ simpel ab: Zunächst zwingt wifite die Clients per Deauthentication-Paket, die Verbindung zum Router zu trennen. Bei der anschließenden Neuanmeldung zeichnet es den Handshake auf und setzt anschließend den Passwort-Cracker hashcat darauf an. Der probiert eine Reihe von Passwörtern aus einer langen Liste durch, bis er fündig wird. Die wichtigsten Schutzmaßnahmen in aller Kürze: Nutzen Sie lange WPA-Passwörter (mindestens 16 Zeichen, besser mehr), aktivieren Sie möglichst WPA2/3 (Mixed Mode) und die geschützte Anmeldung von WLAN-Geräten (Protected Management Frames, PMF).

# Datenlecks im Webserver finden

Webserver sind prinzipbedingt meist für jeden erreichbar – und damit zwangsläufig auch für Angreifer, die nach Sicherheitslücken, Datenlecks und schwachen Passwörtern suchen. Das geschieht längst nicht mehr mühsam von Hand, sondern automatisiert. So können die bösen Buben tausende Websites innerhalb kurzer Zeit auf Schwachstellen abklopfen und müssen bei der Wahl ihres Angriffsziels nicht wählerisch sein.

Wenn Sie eine Website betreiben, müssen Sie also fest mit ungebetenem Besuch rechnen. Und wenn es eine Sicherheitslücke gibt, wird diese früher oder später auch ausgenutzt. Sie können den Angreifern jedoch die Petersilie verhageln, indem Sie sich deren Tools zu eigen machen, um etwaige Schwachstellen selbst frühzeitig zu finden. Auch diese Tools dürfen Sie nur gegen eigene Server und niemals unbefugt gegen fremde Systeme einsetzen, sonst drohen juristische Konsequenzen (siehe Seite 170). Beachten Sie, dass die Werkzeuge sehr viele Anfragen und damit potenziell auch eine hohe Last erzeugen, was die Erreichbarkeit des Servers beeinträchtigen kann.

Ein einfaches, aber effektives Werkzeug zur Suche nach Datenlecks ist **DIRB**. Es probiert eine lange Liste mit gängigen Verzeichnisnamen wie /admin, /backups oder /internal durch, um Ordner zu finden, die nicht für die Öffentlichkeit bestimmt, aber trotzdem für jeden zugänglich sind. Ferner kann das Hacking-Programm Verzeichnisnamen per Brute Force erraten. Gibt es einen Treffer, versucht DIRB auch noch mögliche Unterordner zu entdecken. Die Bedienung ist einfach:

```
dirb https://ihre-website.example
```

Unzureichend geschützte Verzeichnisse sind häufig die Ursache für Datenlecks, etwa wenn darin Backups der MySQL-Datenbank oder Konfigurationsdateien mit Zugangsdaten gespeichert sind.

Diese Blindgänger sollten Sie rechtzeitig entschärfen, zum Beispiel durch einen Zugriffsschutz auf dem Verzeichnis, sofern die Daten überhaupt auf dem öffentlichen Server liegen müssen.

## WordPress-Lücken aufspüren

Das Content-Management-System WordPress ist sehr verbreitet (siehe S. 60 ff.) und bei Angreifern entsprechend hoch im Kurs. Häufig wird es in veralteten – und somit verwundbaren – Versionen betrieben oder mit anfälligen Plug-ins und Themes. Auch Konfigurationsfehler begünstigen eine Fremdübernahme. Solche Schlupflöcher aufzudecken ist inzwischen ein Kinderspiel – zum Beispiel mit dem WordPress Security Scanner **WPScan**. Der kann Ihnen gute Dienste beim Absichern Ihrer Website leisten.

Auf der GitHub-Seite des Ruby-Tools erfahren Sie, wie Sie es unter Linux, macOS und als Docker-Container an den Start bringen (siehe ct.de/ygg5). Kali-Nutzer können sich das sparen, das Programm ist vorinstalliert. Um Ihre WordPress-Installation zu scannen, füttern Sie WPScan einfach mit der URL: wpscan --url https://ihre-website.example/wordpress

Bevor die Analyse beginnt, lädt der Security Scanner eine Datenbank mit aktuellen Infos aus dem Netz. Das geschieht normalerweise automatisch, wenn Sie es jedoch auf die verwundbaren WordPress-Installationen von RasPwn loslassen möchten (siehe „Angreifen erlaubt“), haben Sie keine Internetverbindung, solange Sie mit dem Raspi-Testnetz verbunden sind. In diesem Fall sollten Sie sich zunächst mit Ihrem normalen Netz verbinden und das Update mit wpscan --update manuell starten. Trennen Sie die Verbindung danach, ehe Sie schließlich den Scan aus dem RasPwn-Netz anwerfen.

Nach und nach gibt WPScan interessante Informationen über die WordPress-Installation aus, darunter die WordPress-Version samt Erscheinungsdatum und eine Einschätzung, ob diese Ausgabe

nach aktuellem Stand der Dinge sicher ist. Weiterhin identifiziert das Tool die Versionen von Webserver und PHP sowie Themes, Plug-ins und diverse Konfigurationsfehler. Prinzipiell kann man selbst im Netz recherchieren, welche Sicherheitslücken in den identifizierten Versionen klaffen. Aber auch das kann Ihnen WPScan abnehmen. Diese Informationen fragt das Tool über ein Web-API vom Server der Entwickler ab – dafür ist eine kostenfreie Registrierung nötig (siehe ct.de/ygg5).

## Datenbank-Lecks verhindern

Die Kronjuwelen einer Website sind häufig Kunden- oder gar Nutzerdaten. Diese können Onlinegauner im Darknet leicht zu Geld machen. In der Regel bewahren Webanwendungen solche Daten in einer Datenbank auf, die natürlich gut geschützt sein sollte. Die Betonung liegt auf sollte, denn allzu oft gelingt es Cyberkriminellen, Kundendaten im großen Stil aus Datenbanken abzugreifen.

Eine häufige Ursache sind sogenannte SQL-Injection-Lücken: Dabei spricht der Angreifer nicht direkt mit dem Datenbankserver, sondern versucht stattdessen, die Webanwendung dazu zu bringen, eingeschleuste SQL-Befehle auf der Datenbank auszuführen. Das Resultat ist häufig, dass die Datenbank über die Web-Anwendung massenweise sensible Datensätze ausspuckt.

Sie ahnen es vielleicht schon: Auch für solche Lücken gibt es ein Hacking-Tool, in diesem Fall **SQLmap**. Es unterstützt zahlreiche Datenbanken, unter anderem Oracle, MySQL, MariaDB, MS SQL Server, PostgreSQL und SQLite. Je nach Datenbanktyp und Berechtigungen kann es auch Dateien auf den Webserver schreiben. Hacker können so versuchen, eine Web-Shell hochzuladen, um den Server dauerhaft fernzusteuern.

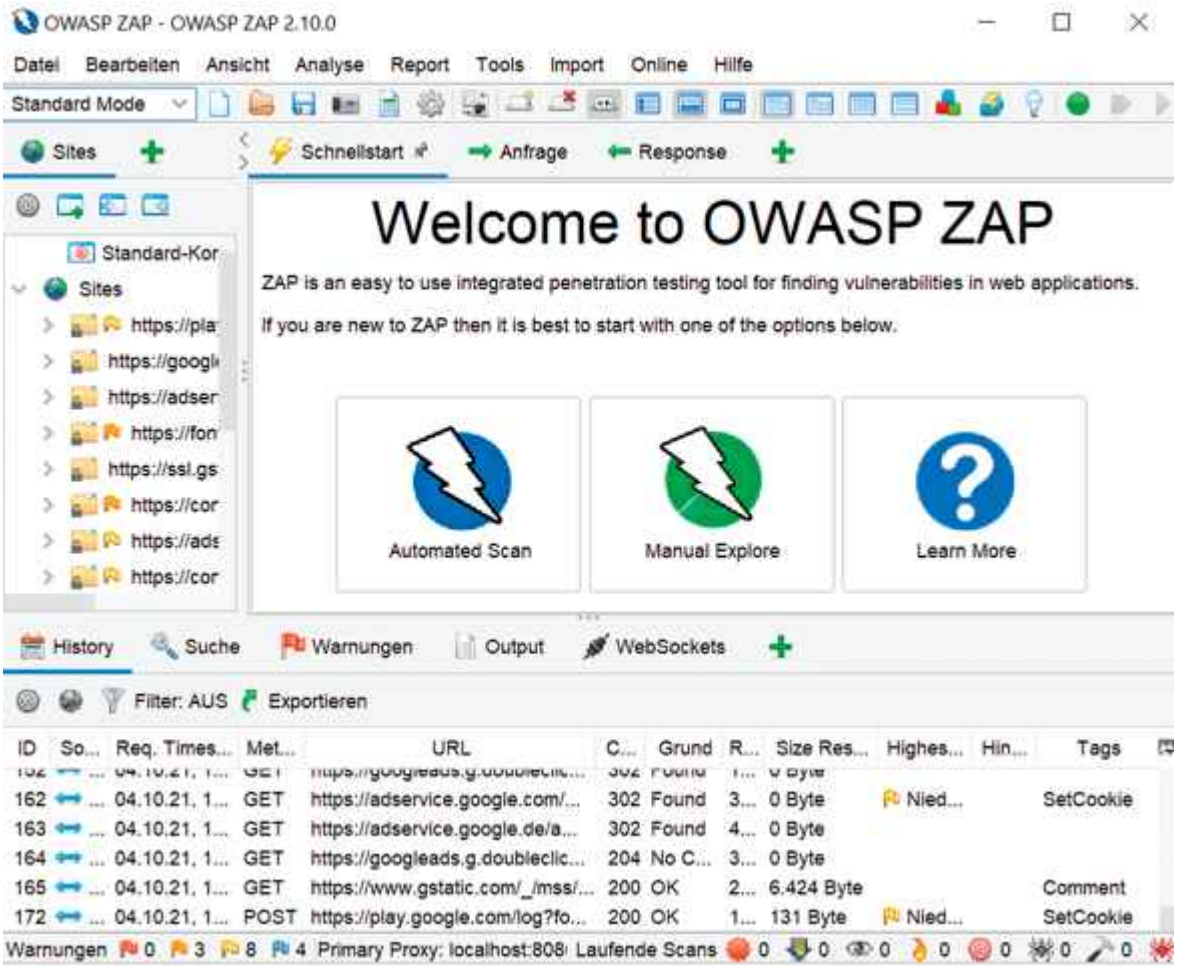
Für einen ersten Funktionstest können Sie die absichtlich anfällige „Wacko Picko“-Website von RasPwn mit SQLmap scannen.

Das Login-Formular der Website sendet beim Abschicken zwei POST-Parameter, nämlich „username“ und „password“, die der Schwachstellenscanner in diesem Beispiel in die Mangel nehmen soll. Um zu überprüfen, ob die Website bei der Auswertung dieser Parameter patzt, können Sie das Tool mit --data anweisen, genau das herauszufinden:

```
sqlmap -u "http://wackopicko.playground.raspwn.org/users/login.php" --data="username=1&password=1" --banner
```

Die Option „banner“ findet die Datenbankversion und das Betriebssystem des Servers heraus, wenn die Website verwundbar ist. Falls Sie den Datenbankinhalt gleich auslesen möchten, ersetzen Sie --banner einfach durch --dump.

Solche SQL-Injections vermeiden Sie, indem Sie Eingaben von außen konsequent überprüfen, bevor sie verarbeitet oder gar in Datenbankbefehle integriert werden. Weiterhin ist der Einsatz sogenannter „Prepared Statements“ sinnvoll, bei denen Sie zunächst den Aufbau des SQL-Befehls festlegen, ehe Sie darin einen Platzhalter mit den von außen angelieferten Werten füllen. Am besten basteln Sie die Datenbankbefehle nicht selbst zusammen, sondern setzen auf eine hinreichend getestete ORM-Bibliothek (Object-Relational Mapping), die bereits gegen alle Eventualitäten abgesichert ist.




Der Zed Attack Proxy (ZAP) macht verschlüsselten Datenverkehr im Klartext sichtbar und spürt Schwachstellen in Web-Anwendungen und APIs auf.

## Browser- und App-Traffic

Der **OWAP Zed Attack Proxy (ZAP)** ist ein universelles Werkzeug zur Analyse und Manipulation von Web-Traffic (HTTP/HTTPS). Sie können sich damit zum Beispiel zwischen Browser und Internet klemmen oder den Datenverkehr Ihres Smartphones durch den Proxy schleusen, um herauszufinden, welche Daten wohin übertragen werden. Eine Stärke des ZAP ist, dass es die identifizierten Gegenstellen, also Webanwendungen, API-Endpunkte und so weiter gleich noch auf Sicherheitsprobleme abklopfen kann. ZAP ist eine Java-Anwendung und läuft unter Windows, Linux und macOS.

Nach dem ersten Start klicken Sie am besten auf den Browser-Knopf in der Symbolleiste, um einen perfekt vorkonfigurierten

Webbrowser zu starten. Dessen Datenverkehr wird automatisch durch den Proxy geschleust. Öffnen Sie damit eine Website, um den Traffic in ZAP zu inspizieren. Wenn Sie den Browser auf diese Weise starten, schleust ZAP in die geöffneten Websites eine eigene Oberfläche namens ZAP HUD ein, über die Sie zahlreiche Funktionen direkt aus dem Browser steuern können. Klicken Sie auf den Knopf „Take the HUD Tutorial“, um eine Einführung zu erhalten und einige der nützlichen Funktionen kennenzulernen.

## Gemischtwaren

Dieser Artikel liefert Ihnen nur eine kleine Auswahl an Hacking-Tools. Das Angebot ist riesig und täglich kommen neue dazu. Einige davon sind sehr komplex oder nur für bestimmte Zielgruppen interessant. Dazu zählt das modular aufgebaute Pentesting-Framework **Metasploit**, das professionelle Penetrationtester nutzen, um einen kompletten Angriff zu simulieren: vom Aufspüren der Ziele über das Ausnutzen von Sicherheitslücken bis hin zum Ausleiten der Datenbeute. Falls Sie sich eingehender mit Hacking beschäftigen möchten, sollten Sie einen Blick darauf werfen. In eine ähnliche Kerbe schlägt **PowerShell Empire**, das Pentestern weitreichenden Rechnerzugriff verschafft, ohne verdächtigen Binärcode auf dem System zu hinterlassen – die Angriffsmodule bestehen aus Skripten für die Windows PowerShell.

Wer eine Windows-Domäne administriert, sollte Tools wie **mimikatz** kennen, das Anmeldeinformationen aus dem Arbeitsspeicher der Windows-Clients ausliest. Angreifer gelangen damit schlimmstenfalls an die Zugangsdaten eines Domänen-Administrators und können das gesamte Netzwerk übernehmen. Den Domänencontroller spüren die Eindringlinge vorher mit **AdFind** von joeware auf. Auch **PsExec** aus Microsofts SysInternals-Kollektion birgt ein gewisses Missbrauchspotenzial: Es wird genutzt, um Befehle auf anderen Rechnern im Netzwerk auszuführen. Angreifer nutzen es mit

zuvor erbeutete Anmeldeinformationen.

Das von der NSA entwickelte Reverse-Engineering-Toolkit **Ghidra** ist interessant, wenn Sie ausführbaren Code (wie EXE- und DLL-Dateien) bis ins letzte Bit auseinandernehmen und verstehen möchten. Es dekompiliert Binärdateien und kann sie auch wieder zusammenbauen, ähnlich wie der kommerzielle Disassembler IDA Pro. In c't 14/2020 haben wir Ghidra ausführlicher getestet (siehe ct.de/ygg5).

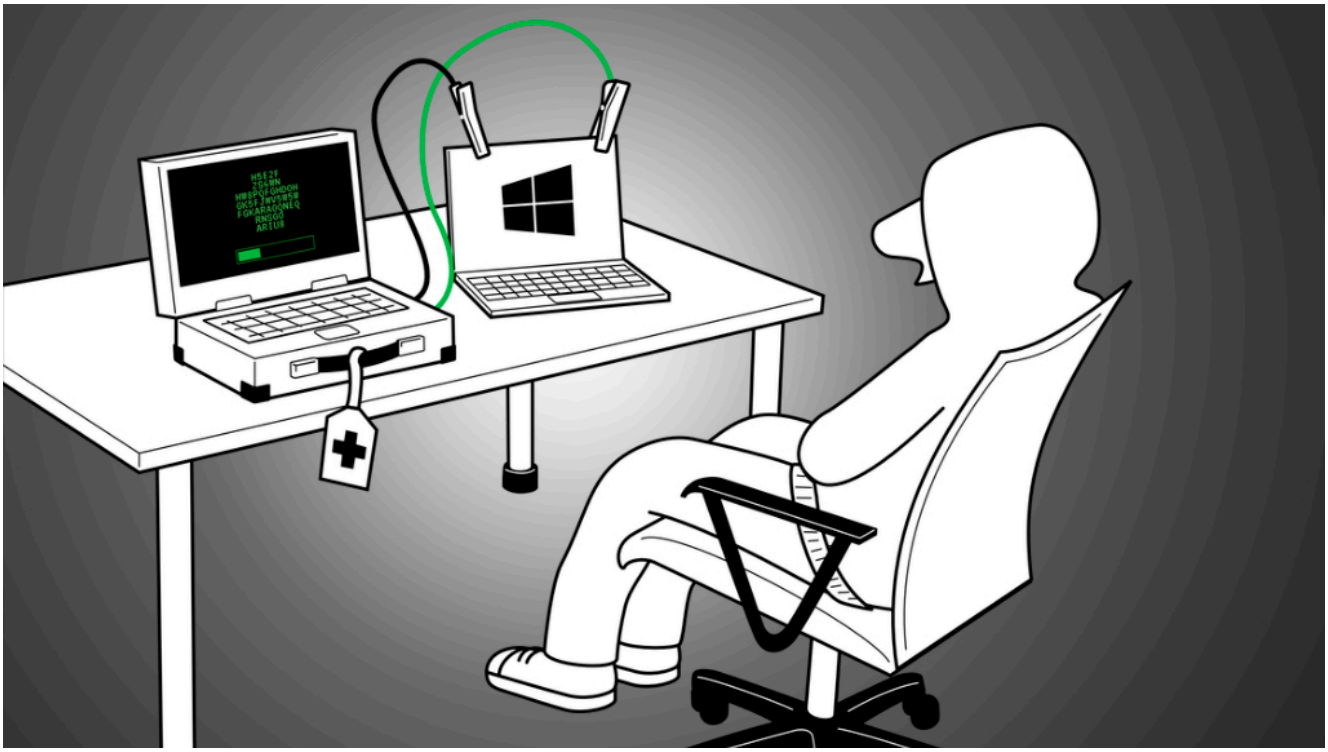
## Fazit

Die vorgestellten Hacking-Tools decken einen weiten Bereich ab. Manche Techniken sind erschreckend simpel, andere fordern viel Einarbeitung und Erfahrung. Sich damit zu beschäftigen lohnt sich aber: Sie lernen so, wie ein Angreifer zu denken und Ihre eigenen Sicherheitsprobleme und -lücken aufzuspüren. Das ist hilfreich – ganz gleich, ob Sie nur eine private WordPress-Site betreiben oder gar für die Sicherheit Ihrer Kunden verantwortlich sind. *(rei@ct.de)*

**Hacking-Tools & weitere Infos:** ct.de/ygg5

---

# 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.

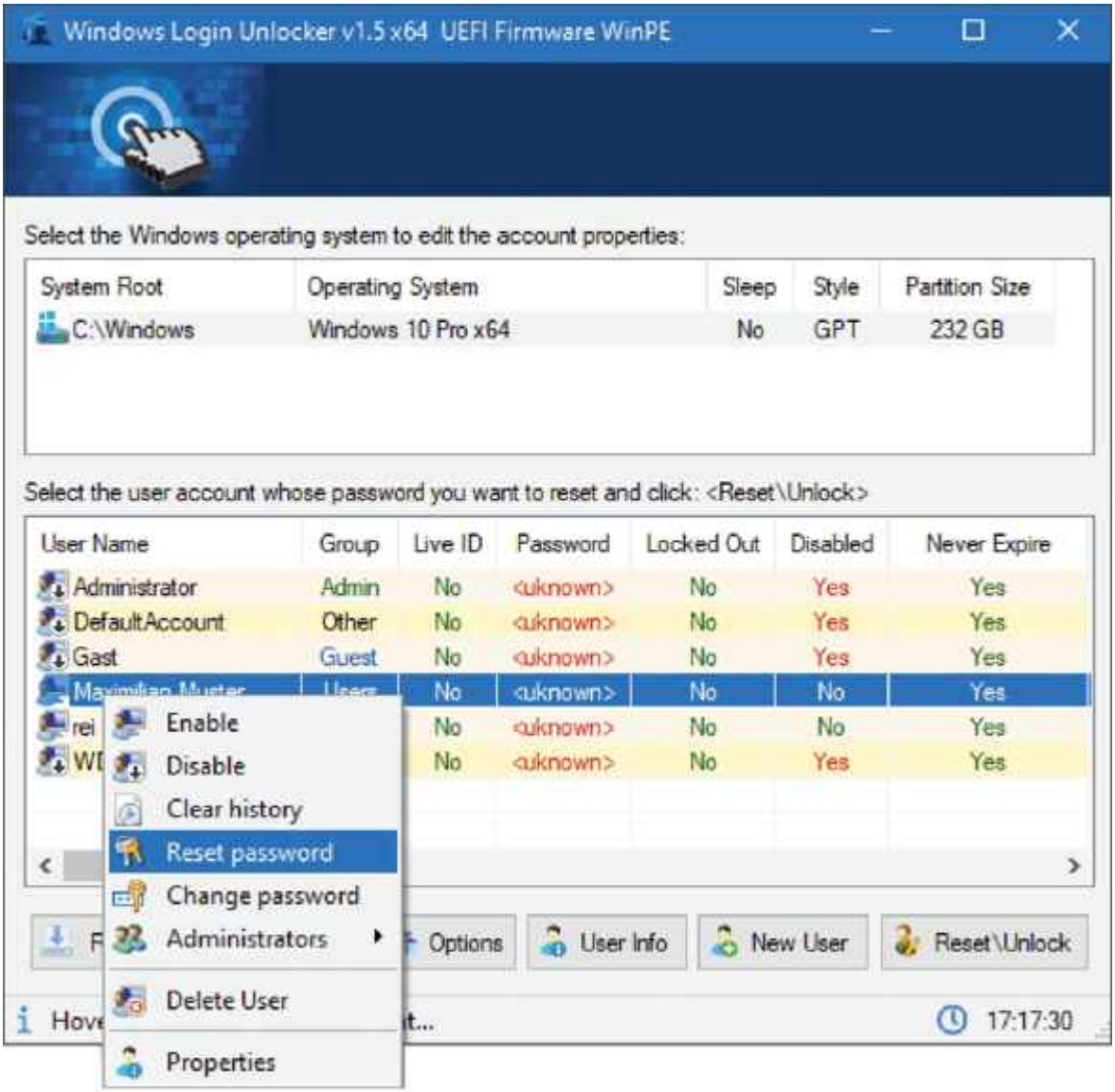
Bei Hackerangriffen ist keine schwarze Magie im Spiel, häufig sind es frei verfügbare Open-Source-Tools, die für sich genommen nicht gefährlich sind. Nach einer Infektion werden sie nachgeladen und automatisiert ausgeführt, um zum Beispiel Dateien oder Passwörter erstmal lokal einzusammeln. Ausgeleitet 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.

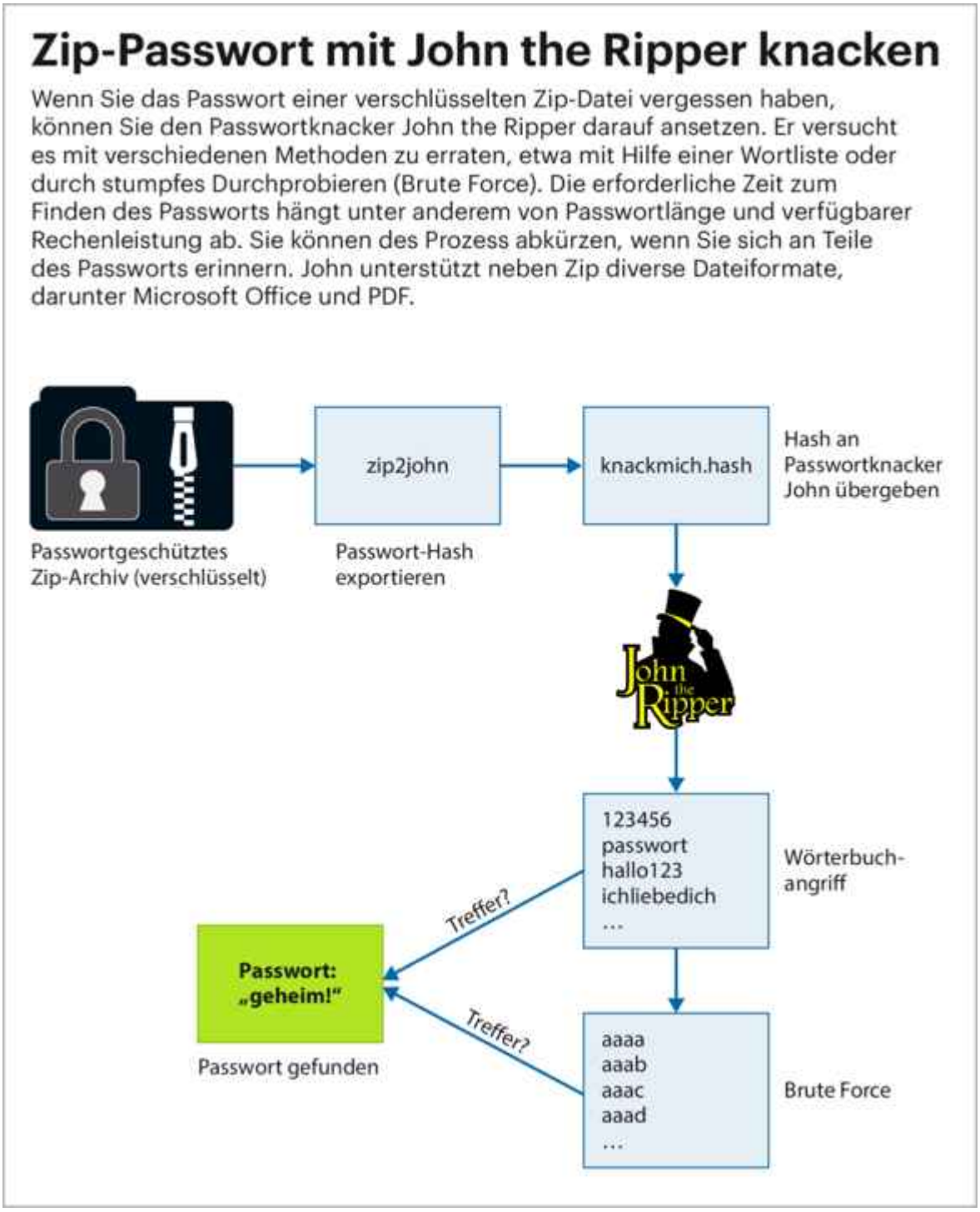
John gibt es für Windows, Linux und macOS, bei Kali Linux (siehe S. 30) ist er bereits an Bord. Er liest die verschlüsselten Dateien nicht selbst ein, er benötigt

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.



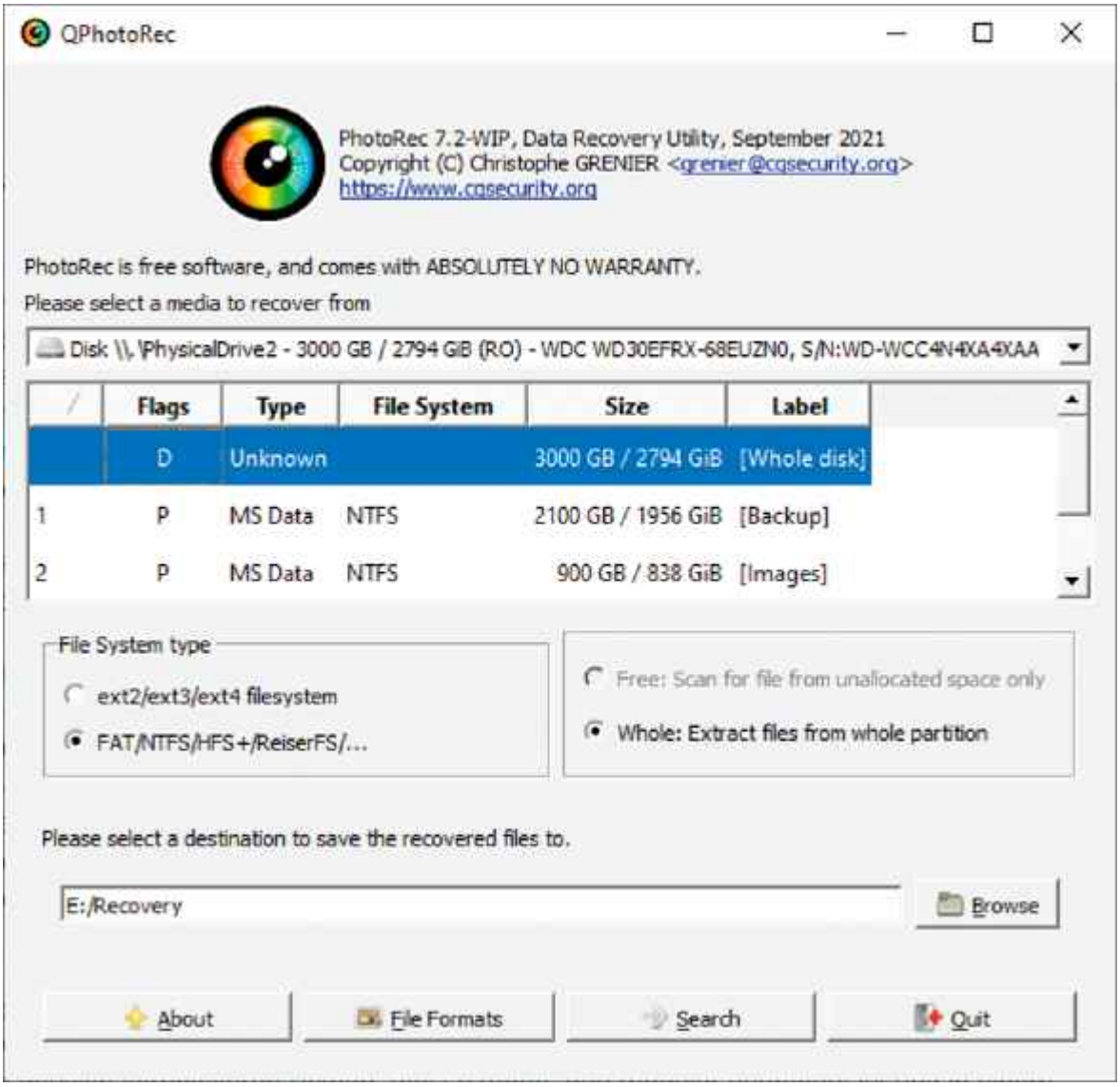

Sie können zum Beispiel eine Mindest- und Maximallänge wie 5 und 6 Zeichen vorgeben, indem Sie -min-length=5 -max-length=6 an den Befehl hängen. Mit -incremental=digits würden Sie den Suchradius auf Ziffern beschränken, um zum Beispiel ein Passwort zu finden, das aus einem Geburtsdatum besteht. Wer einen 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.



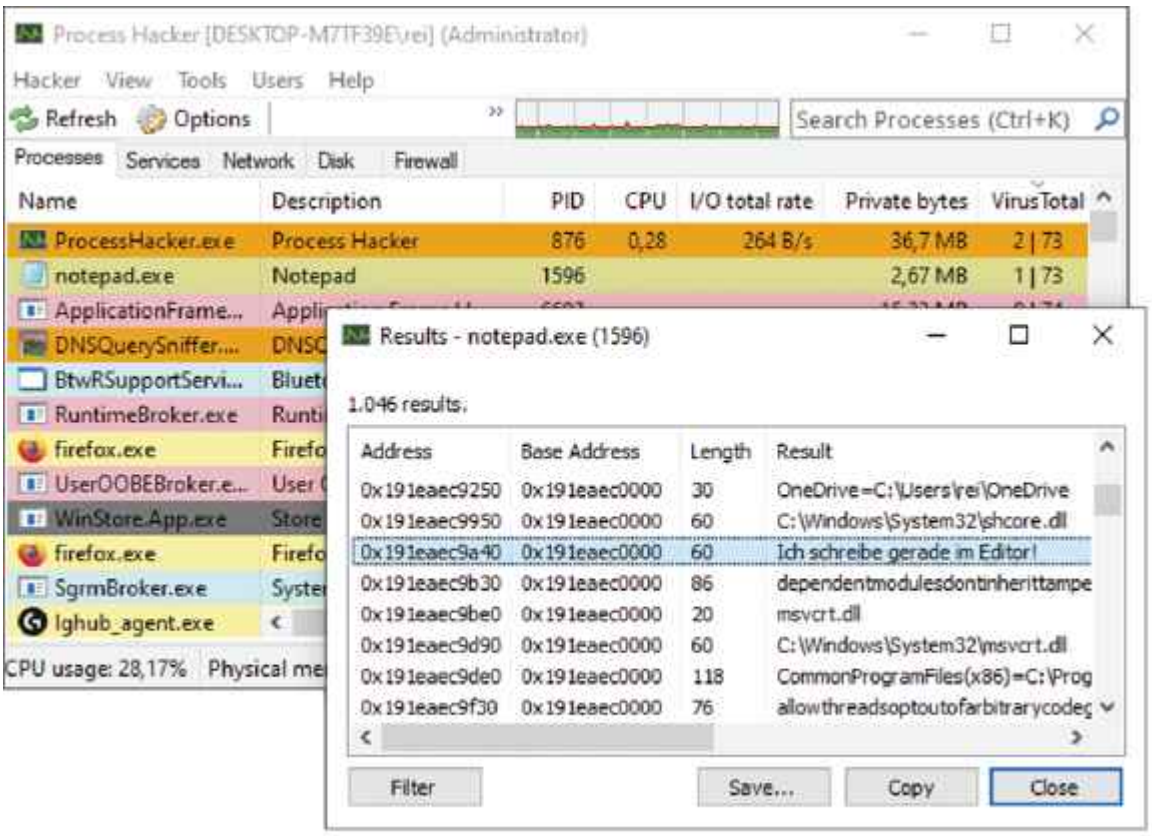

Sind Ihre Dateien noch zu retten? Mit PhotoRec finden Sie es heraus.

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).



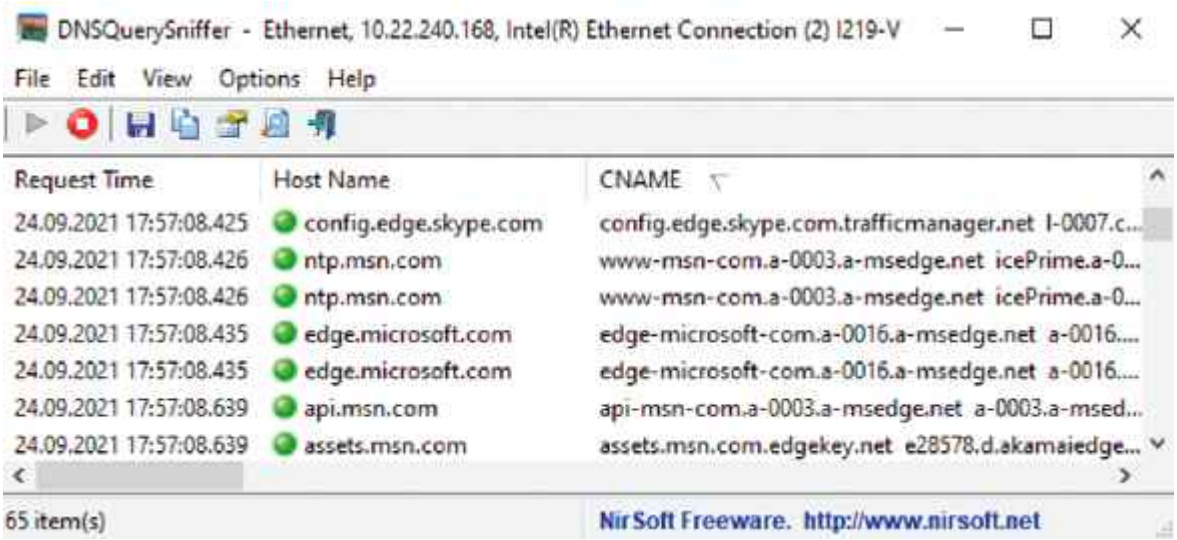

Der Process Hacker macht da weiter, wo andere Taskmanager aufhören: Das Tool erlaubt sogar Eingriffe in den Arbeitsspeicher der Prozesse.
Das Hauptfenster des Process Hacker ist in fünf Tabs unterteilt: „Processes“ zeigt, ähnlich wie der Taskmanager, Informationen über laufende Prozesse an und „Services“ 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

---

# Hacking-Tools

## Hacking-Tools

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.

# Die Werkzeuge der Hacker als Problemlöser

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 verhältnismäßig 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 **LaZagne** (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.


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

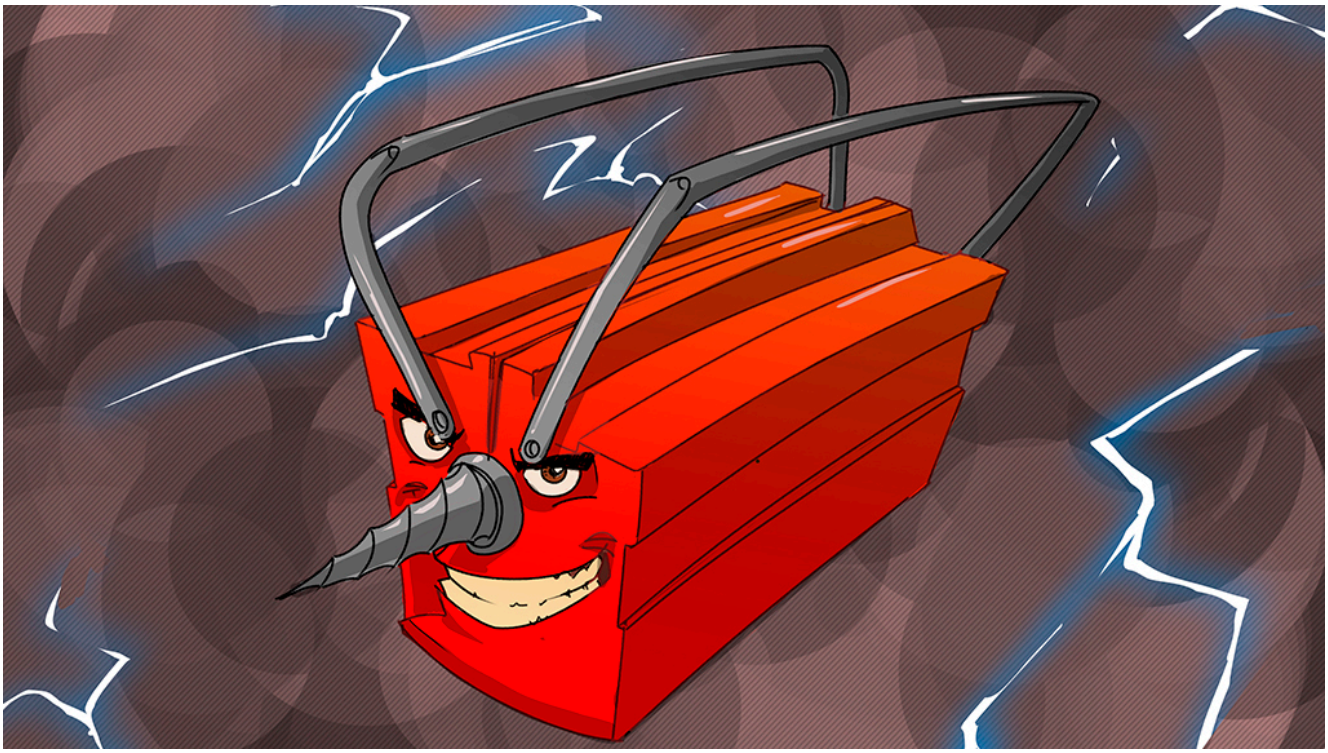
WordPress-Websites stehen unter Dauerfeuer, weil Angreifer nur zu gut wissen, dass ein verpenntes Sicherheits-Update ausreicht, um den ganzen Server zu übernehmen. Auch veraltete und verwundbare Erweiterungen sind schon vielen WordPress-Betreibern zum Verhängnis geworden. Wenn Sie das gleiche Werkzeug 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*)

---

# Rechtliche Unsicherheiten bei Hacking-Werkzeug



## Kommt drauf an, wozu

Um Schwachstellen im eigenen Netz zu suchen und Datenflüsse zu überwachen, nutzen Administratoren vielfach die gleichen Softwarehilfsmittel wie Angreifer, die illegale Ziele verfolgen. Was sagt das deutsche Recht dazu? Steht jemand, der mit trickreichen Analyse- und Spähtools arbeitet, mit einem Bei…

## Kommt drauf an, wozu

# Rechtliche Unsicherheiten bei Hacking-Werkzeug

Um Schwachstellen im eigenen Netz zu suchen und Datenflüsse zu überwachen, nutzen Administratoren vielfach die gleichen Softwarehilfsmittel wie Angreifer, die illegale Ziele verfolgen. Was sagt das deutsche Recht dazu? Steht jemand, der mit trickreichen Analyse- und Spähtools arbeitet, mit einem Bein vor Gericht?

Von Verena Ehrl

Der Theaterautor und Sprachliebhaber Hans-Joachim Haecker brachte die Dual-Use-Problematik bereits 1968 in einem Gedichtchen seines Bandes „Insonderheit“ unter dem Eindruck des internationalen Wettrüstens scherzhaft auf den Punkt:

*„Insonderheit die Abwehrwaffen*
*sind für die Abwehr wie geschaffen.*
*Auch kann man mit geschickten Händen*
*sie für den Angriff gut verwenden.“*

Die Waffen, mit denen Akteure innerhalb der IT-Welt hantieren, eignen sich zum Eindringen in Systeme, zum Überwinden von Sicherungsmaßnahmen, zum Spionieren und Manipulieren. Dieselben Werkzeuge können aber dazu dienen, unterschiedliche Ziele zu erreichen. In der Hand eines Administrators, der ein System, für das er verantwortlich ist, Penetration Tests („Pentests“) aussetzt, kann etwa das Software-Tool „Mimikatz“ legalen Einsatz finden (S. 24). Es ebnet allerdings ebenso gut Angreifern den Weg bei illegalen Aktionen, indem es ihnen Zugangsdaten für die Übernahme eines Netzwerks offenbart. Auf diese Ambivalenz bezieht sich das Schlagwort „Dual Use“ im Zusammenhang mit Hackerausrüstung.

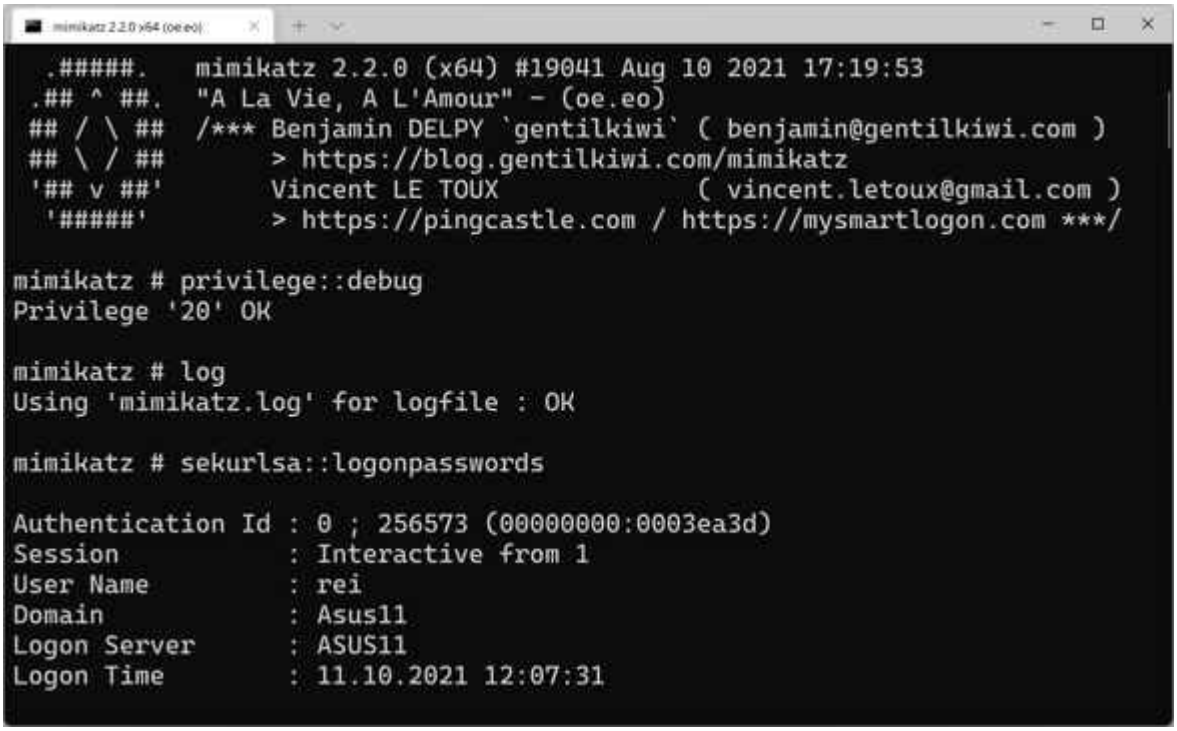
Nicht immer erscheinen die Werkzeuge, um die es geht, so spektakulär wie die Hacking-Gadget-Hardware, mit der c’t sich

in Ausgabe 18/2017 befasst hat [1]. Sehr oft steht vielmehr bloße Software im Mittelpunkt, die loggt, sucht, entschlüsselt, ausliest, analysiert und speichert (S. 16, 18, 24 und 39). Die rechtlichen Fragen, vor die ein Anwender gestellt ist, sind jedoch grundsätzlich die gleichen wie bei den Spionagegerätchen [2]: Wo liegt die rote Linie, jenseits der man sich auf illegalem Terrain bewegt? Was sagt das geltende Recht zum Umgang mit potenziell gefährlichen und schadenträchtigen Tools?

Dass es „Güter mit doppeltem Verwendungszweck“ gibt, die sich gleichermaßen für legales und illegales Tun eignen, beschäftigt nicht zuletzt den europäischen Gesetzgeber. Am 9. September 2021 ist die Neufassung der sogenannten Dual-Use-Verordnung in Kraft getreten [3].

Sie betrifft „Güter einschließlich Datenverarbeitungsprogramme (Software) und Technologie, die sowohl für zivile als auch für militärische Zwecke verwendet werden können“. Es gibt durchaus Softwareentwicklungsprojekte, die man mit etwas Fantasie in den Betrachtungshorizont der Verordnung rücken kann.

Ziel der Dual-Use-Verordnung ist die Exportkontrolle. Die kann bereits relevant werden, wenn Forschung und Produktentwicklung mit Partnerunternehmen in bestimmten außereuropäischen Ländern stattfinden und dabei schadenträchtige Software im Spiel ist.




Mimikatz ist ein typisches Beispiel für ein Hackerwerkzeug, das auch verantwortungsvollen Admins wertvolle Dienste leistet, wenn es ums Aufspüren von Schwachstellen im eigenen Netz geht.

Neu im Blick der europäischen Rechtssetzungsorgane und der zur Umsetzung verpflichteten Mitgliedsstaaten sind Länder, welche die Todesstrafe praktizieren oder in denen Menschenrechtsverletzungen wie Folter auf staatliches Geheiß stattfinden. Wer etwa potenziell gefährliche Software ins nichteuropäische Ausland transferieren will, braucht dazu eine vorherige Genehmigung des Bundesamts für Wirtschaft und Ausfuhrkontrolle (BAFA). Diese Behörde entscheidet in jedem Einzelfall, ob der Transfer zulässig ist oder nicht.

## Zweierlei Paar Schuhe

Abseits der von der Verordnung erfassten Transferproblematik sind Dual-Use-Softwarewerkzeuge rechtlich schwer zu fassen. Weder ihr Erwerb noch ihr Besitz ist grundsätzlich untersagt. Straf- und Zivilrecht melden sich erst dann, wenn jemand diese Tools einsetzt, um Rechtsbrüche zu begehen. Derjenige riskiert dann eine Strafe oder er sieht sich zivilrechtlichen Ansprüchen ausgesetzt – oft droht ihm beides.

Nicht alles, was jemand rechtswidrig tut, ist auch strafbar. Mit dem Strafrecht geht der Staat gegen von ihm untersagtes Verhalten vor, dabei sind Strafermittlungsbehörden im Spiel, es gibt Beschuldigung und Anklage. Im Zivilrecht stehen hingegen gleichberechtigte Streitparteien einander gegenüber. Dabei gibt es Kläger und Beklagte, die Gerichte entscheiden über Ansprüche, welche die Parteien gegeneinander geltend machen. Vertragspflichten und Schadenersatzansprüche sind typisches zivilrechtliches Geschäft.

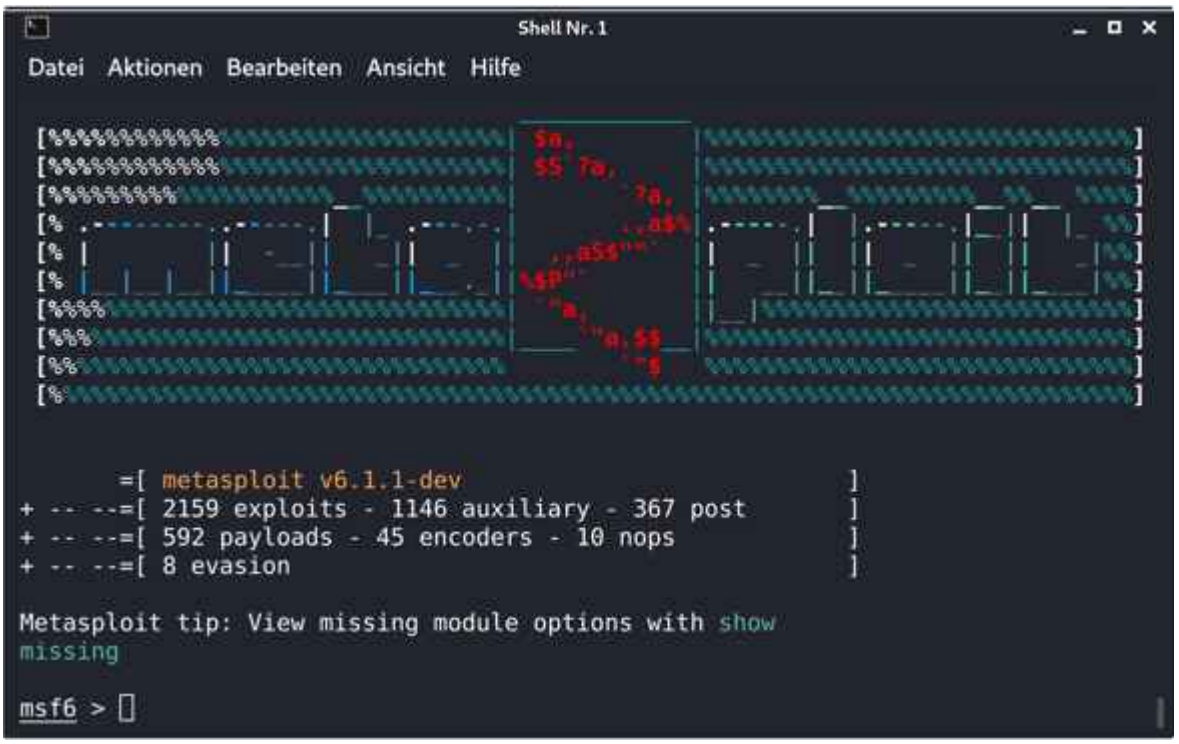
Durch Software kann ein Anwender sich Ärger in beiden Rechtsbereichen einhandeln. Ein gutes Beispiel für die rechtliche Gratwanderung dabei sind die bereits angesprochenen Pentests. Sie haben die Aufgabe, Schwachstellen in Konfiguration, Hard- und Software von Servern, Routern und Arbeitsplätzen im Netz aufzuzeigen. Ein Mitarbeiter, der einen solchen Test im Auftrag eines zuständigen Entscheiders für das betroffene Netz durchführt, bewegt sich damit auf der legalen Seite. Wenn allerdings etwa ein Cybersecurity-Dienstleister einen Pentest unaufgefordert und ohne Erlaubnis bei einem potenziellen Kunden durchführt, um diesen als Auftraggeber zu gewinnen, setzt er sich strafrechtlicher Verfolgung wegen Datenveränderung oder Computersabotage aus.

Wesentlich sind dabei die Paragrafen 303a und 303b des Strafgesetzbuchs (StGB), die sich mit virtueller Sachbeschädigung befassen. Damit hat der Gesetzgeber 1986 eine Regelungslücke beim Straftatbestand der Sachbeschädigung (§ 303 StGB) geschlossen. Die klassische Sachbeschädigung setzt einen körperlichen Gegenstand voraus – das lässt Daten und beispielsweise Festplatten, die funktionsfähig bleiben, aber deren Inhalt gelöscht oder verschlüsselt wurde, außen vor.

§ 303a StGB stellt die unbefugte Veränderung von Daten unter Strafe. Dort heißt es in Absatz 1: „Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.“

Bereits der Versuch ist strafbar; dasselbe gilt wie beim Ausspähen (§ 202a StGB) und Abfangen von Daten (§ 202b StGB) auch fürs „Vorbereiten“ einer rechtswidrigen Datenveränderung – beispielsweise durch Bereitstellen von Software, deren „Zweck die Begehung einer solchen Tat ist“ (§ 202c Abs. 1 Nr. 2 StGB).

Als Daten in diesem Sinne gelten nach § 202 StGB „nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden“, also nicht etwa Papiernotizen.




Das modulare Pentesting-Tool Metasploit ist bei Security-Experten beliebt, es lässt sich aber auch für echte Angriffe missbrauchen.

§ 303b StGB, der sogenannte Hackerparagraf, ist der Computersabotage gewidmet. Er steht in direktem Zusammenhang mit seinem Nachbarn, der die Datenveränderung betrifft, und lautet: „Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, … erheblich stört, … wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“

Wenn es um die Datenverarbeitung eines Unternehmens respektive

einer Behörde geht, stehen Freiheitsstrafen bis zu fünf Jahren im Raum. In besonders schweren Fällen riskieren Täter sogar bis zu zehn Jahren Gefängnis. Der Paragraf grenzt die Wege, auf denen die strafbare Datenverabeitungsstörung bewirkt wird, näher ein: Unter Nr. 1 fasst er die Störung durch Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten (siehe § 303a Abs. 1). Unter Nr. 2 erscheint die Dateneingabe und -übermittlung mit der Absicht, jemand anderem einen Nachteil zuzufügen. Unter Nr. 3 schließlich geht es darum, dass eine Datenverarbeitungsanlage oder ein Datenträger zerstört, beschädigt, unbrauchbar gemacht, beseitigt oder verändert wird. Auch hierbei sind wie bei der Datenveränderung bereits Versuch und Vorbereitung strafbar.

Dass es nur ums Stören von Datenverarbeitungen von „wesentlicher Bedeutung“ geht, soll Bagatellfälle aus dem Blick der Strafjustiz nehmen.

## Erpressungstrojaner vor Gericht

Im April 2021 hat der Bundesgerichtshof (BGH) einen Fall entschieden, der die Verteilung von Ransomware betraf – also das Einschleusen von Verschlüsselungstrojanern zu Erpressungszwecken [4]. Dabei stufte das Gericht unter anderem das Anbringen einer Eintragung in der Windows-Registry, die das automatische Laden einer Schadsoftware beim Rechnerstart bewirkte, als strafbare Datenveränderung ein. Zugleich sah der BGH in diesem Fall auch eine Computersabotage nach § 303b StGB.

Der Angeklagte war Mitglied einer Cybercrime-Bande mit Sitz in der Ukraine. Diese hatte mit ihren Ransomware-Angriffen von 2013 bis 2016 über 200 Millionen Rechnersysteme infiziert und von den geschädigten Computernutzern mehr als neun Millionen Euro erpressen können.

Schadsoftware ähnlicher Art mit einer vorgesehenen Entsperrmöglichkeit hätte aber auch im Rahmen eines Pentests

in einem lokalen Netz durchaus legal verwendet werden können. Ein Unternehmen hätte damit etwa seine Mitarbeiter auf deren Vorsicht testen können, was das Anklicken unbekannter Inhalte betrifft.

## Computersabotage am Arbeitsplatz

Das mutwillige Stören des Datenverarbeitungsbetriebs kann nicht nur strafrechtliche, sondern auch arbeitsrechtliche Auswirkungen haben. Mitarbeiter, die aus Wut oder infolge von Rachegedanken gegen ihren Arbeitgeber Datenvandalismus im Unternehmensnetz betreiben, riskieren eine fristlose Kündigung.

Das geschah 2019 einem als Key-Account-Manager beschäftigten Arbeitnehmer nach einer heimlichen Löschaktion auf dem Unternehmensserver seines Arbeitgebers. Nach einer Abmahnung war ihm zuvor ein Aufhebungsvertrag angeboten worden. Daraufhin löschte er 8 GByte an Daten, darunter Kalkulationssoftware, Umsatzmeldungen, Vorlagen für Preislisten und Wettbewerbsanalysen für bestimmte Produkte. Die Daten konnten später wiederhergestellt werden. Der Verdacht fiel auf ihn. Gegen die fristlose Kündigung , die er wenig später erhielt, wehrte er sich zunächst erfolgreich. In der Berufungsinstanz jedoch unterlag er vor dem Landesarbeitsgericht (LAG) Baden-Württemberg im September 2020 [5]. Sein Arbeitgeber hatte einen 93seitigen Vergleich des Datenbestands im fraglichen Verzeichnis vor und nach der Löschaktion vorgelegt.

Das Gericht sah die fristlose außerordentliche Kündigung als begründet an: Das unbefugte vorsätzliche Löschen betrieblicher Daten auf EDV-Anlagen des Arbeitgebers tauge ebenso wie das Vernichten von Verwaltungsvorgängen grundsätzlich als „wichtiger Grund“ für eine solche Kündigung im Sinne des § 626 Abs. 1 BGB. Dabei komme es nicht unbedingt darauf an, ob sich der Arbeitnehmer nach § 303a StGB oder § 303b StGB strafbar gemacht habe. Es sei auch nicht entscheidend, ob und mit

welchem Aufwand ein Teil der gelöschten Daten wiederhergestellt werden konnte oder ob der Arbeitgeber diese Daten für den weiteren Geschäftsablauf tatsächlich benötigte. Vielmehr gehöre es zu den vertraglichen Nebenpflichten eines Arbeitsverhältnisses im Sinne des § 241 Abs. 2 BGB, dass der Arbeitnehmer seinem Arbeitgeber den Zugriff auf betriebliche Dateien nicht verwehre oder unmöglich mache.


In der Hand von Angreifern kann auch der Fern Wifi Cracker, mit dem man Drahtlosnetze auf Sicherheitslücken abklopft, zum Werkzeug für eine Straftat werden.

## Wenn der Admin spioniert

Dass es bei der strafrechtlichen Bewertung von Hacker-Aktivitäten nicht so sehr um die benutzten Werkzeuge als vielmehr um Zweck und Absicht des Einsatzes geht, illustriert auch ein Fall, den 2020 der BGH in letzter Instanz entschied [5]. Zwei Männer mussten sich wegen des Ausspähens von Daten (§ 202a StGB) verantworten. Einer davon leitete die Stabsstelle eines Apothekerverbandes und betrieb daneben ein gesundheitspolitisches Informationsportal im Internet. Der zweite Angeklagte arbeitete als Systemadministrator am Berliner Standort des Bundesgesundheitsministeriums (BMG) und war nebenbei als Callboy tätig – daher rührte auch die Bekanntschaft der beiden Männer.

Der Admin hatte jahrelang Zugriffsrecht auf alle E-Mail-Accounts seiner Dienststelle und versorgte den Portalbetreiber mit so gewonnenen Interna aus dem Ministerium. Nachdem das Ministerium den unbeschränkten Mailzugriff der Administratoren im Hause als Sicherheitsmangel erkannt hatte, wurde es für den Mann schwieriger – er verlegte sich schließlich auf einen unter den Admins bekannten Notfalltrick, mit dem er sich selbst von Fall zu Fall die nötigen Zugriffsrechte verschaffte. Er lieferte dem Portalbetreiber auf Datenträger kopierte E-Mail-Inhalte nach Wunsch und kassierte dafür insgesamt rund 1000 Euro. Sein Kunde war besonders an E-Mails der Minister und Staatssekretäre sowie einiger Abteilungs- und Referatsleiter interessiert. In den weitergereichten Mails ging es unter anderem um Gesetzesvorhaben, die für das Publikum des Portals besonders interessant waren.

Das Landgericht (LG) Berlin verurteilte die Männer im April 2019 wegen gemeinschaftlichen Ausspähens von Daten nach § 202a StGB und sah in der Manipulation der Zugriffsrechte auf die einzelnen E-Mail-Konten zudem die Überwindung einer Zugangssicherung nach § 202a Abs. 1 StGB. Die gegen das landgerichtliche Urteil eingelegte Revision wies der BGH

weitgehend ab, lediglich den einzuziehenden Geldbetrag setzte er niedriger an als die Vorinstanz.

Die Bundesrichter beschäftigten sich vor allem damit, ob Daten im Sinn des §202a Abs. 1 StGB überhaupt als gesichert gelten können, wenn ein Admin mithilfe seiner Kenntnisse darauf zugreifen kann. Die Antwort: Es genüge, wenn getroffene Vorkehrungen den Zugriff auf Daten zumindest deutlich erschweren. Die Sicherung von E-Mail-Accounts durch Passwörter reiche aus. Dabei brauche der Systembetreiber nur den Zugriff Unbefugter zu berücksichtigen, aber nicht die Zugriffsmöglichkeit durch Eingeweihte oder Experten. Es sei nicht erforderlich, dass die Sicherung gerade gegenüber dem Täter wirkt – wenn dieser etwa ein Administrator ist, der den tatsächlichen Zugriff auf die Daten hat.

Als Überwinden der Zugangssicherung nach § 202a StGB können dem Gericht zufolge auch Handlungen gelten, die nicht besonders anspruchsvoll oder aufwendig sind. Wenn jemand durch Insiderkenntnisse oder Ähnliches eine Absicherung schnell und leicht ausschalten kann, zähle das rechtlich ebenso, als hätte sich jemand durch raffinierte technische Werkzeuge Zugriff verschafft. Nur wenn eine Durchbrechung des Schutzes für jedermann ohne Weiteres möglich sei, werde der Tatbestand nicht erfüllt.

## Wer den Schaden hat …

Wie bereits gesagt, ist strafrechtliche Verfolgung nicht das Einzige, was der illegale Einsatz von Hacking-Tools nach sich ziehen kann: Wenn dabei ein Schaden entsteht, hat der Geschädigte einen Anspruch auf Schadenersatz gegen den Verursacher. Schäden durch IT-Störmanöver können sehr hoch sein – wenn etwa durch den Ausfall von Unternehmensservern Arbeitsprozesse lahmgelegt werden. Auch der Ausfall der Netzkommunikation kann enorme Umsatzeinbußen und damit hohe wirtschaftliche Schäden bedeuten. Für Anspruchsteller im Zivilrecht ist wichtig, dass jede Streitpartei alles, was für

ihre Sache spricht, selbst gerichtsfest beweisen muss. Das kann bei Schäden durch Hackertools etwa den Nachweis eines Hackerangriffs und die zweifelsfreie Benennung des Angreifers betreffen. Außerdem ist auch nachzuweisen, dass der Angriff tatsächlich den geltend gemachten Schaden hervorgerufen hat.

Wenn ein Täter bereits strafrechtlich wegen einer Computerstraftat zulasten eines Geschädigten verurteilt worden ist, hat jener es anschließend vergleichsweise leicht, seine Ansprüche gegen den Verurteilten zivilrechtlich geltend zu machen: Das Urteil des Strafgerichts hat selbst bereits Indizwirkung, zudem kann der Kläger die im Strafverfahren erhobenen Beweise zu seinen Gunsten nutzen.

Ein dritter, bislang noch nicht genannter Bereich, der durch unrechtmäßigen Einsatz von Hackertools berührt werden kann, ist der Datenschutz. Wo bei einem Angriff personenbezogene Daten im Spiel sind, geht es nicht bloß um wirtschaftliche Schäden, sondern möglicherweise auch um die massenhafte Verletzung des informationellen Selbstbestimmungsrechts der Betroffenen. Wer es also als Pentester mit realen Datenbeständen zu tun hat, tut gut daran, die Bestimmungen der europäischen Datenschutzgrundverordnung (DSGVO) sorgfältig zu beachten. *(psz@ct.de)*

1. Literatur

2. Ronald Eikenberg, David Wischnjak, Böse und billig: Hacking-Gadgets, Gefahr durch angriffslustige Hardware, c’t 18/2017, S. 62 und S. 64
3. Verena Ehrl, Elektronische Übeltäter, Rechtliche Aspekte im Zusammenhang mit Spionage- und Sabotage-Gadgets, c’t 18/2017, S. 78
4. Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates vom 20.5.2021 über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung, der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck:

heise.de/s/N76o
5. BGH, Beschluss vom 8.4.2021, Az. 1 StR 78/21: heise.de/s/rmDJ
6. LAG Baden-Württemberg, Urteil vom 17.9.2020, Az. 17 Sa 8/20: heise.de/s/MXBL
7. BGH, Beschluss vom 13.5.2020, Az. 5 StR 614/19: heise.de/s/Zvpw