Editorial

Liebe Leserinnen und Leser,

Hacker werden in Filmen meist als Genies dargestellt, die allein mit der Kommandozeile und ihrer Kreativität jedes System knacken. Die Wirklichkeit sieht profaner aus: Selbst die besten Hacker setzen Software ein, die ihnen einen großen Teil ihrer Arbeit abnimmt. Viele der Anwendungen sind frei verfügbar – auch Sie können sie herunterladen und damit zum Hacker werden.

Wir stellen Ihnen die spannendsten Hacking-Tools vor und helfen Ihnen bei den ersten Schritten. Die Programme sind nicht nur für fragwürdige Zwecke zu gebrauchen. Sie helfen auch dann, wenn man sein Windows-Kennwort vergessen hat oder das eigene Netzwerk überwachen will. Wer einmal mit den Hacking-Tools herumgespielt hat, versteht auch besser, wie man sich vor Angriffen schützt – los geht es ab Seite 104.

Sie haben dafür gerade nicht genug Zeit? Dann empfehlen wir Ihnen unsere Security-Checklisten (ab Seite 6). Diese verzeichnen die wichtigsten Handgriffe, mit denen Sie Ihren PC, Ihr Smartphone, Ihre Online-Accounts et cetera vor Online-Gangstern und Schnüfflern schützen. Es dauert in der Regel nur wenige Minuten, die Tipps einer Liste umzusetzen.

Danach können Sie tiefer in die Materie einsteigen. In der Rubrik „Heimnetz absichern“ erklären wir ausführlich, wie man Fritzboxen und Netzwerkspeicher (NAS) einbruchsicher konfiguriert und das eigene WLAN überwacht. Warum die Zwei-Faktor-Authentifizierung für Online-Accounts nach wie vor unersetzlich ist, erfahren Sie in den Artikeln ab Seite 62. Außerdem testen wir Gadgets, die das Konzept sicher und bequem umsetzen. Ab Seite 84 erklären wir, was VPN-Dienste leisten (und was nicht!) und vergleichen elf Anbieter. Typische Sicherheitsprobleme bei Servern und in Webanwendungen wie WordPress zeigen wir ab Seite 138 – damit Sie aus den Fehlern anderer lernen können.

Christian Wölbert

Christian Wölbert

Inhalt

DIE C'T-SECURITY-CHECKLISTEN

IT-Sicherheit ganz konkret: Unsere Checklisten zeigen Schritt für Schritt, wie man PC, Smartphone, Anwendungen und Online-Konten vor Schnüfflern, Erpressern und anderen Online-Gangstern schützt.

HEIMNETZ ABSICHERN

Angreifer klopfen auch private Router automatisiert auf Schwachstellen ab. Mit unseren Tipps schottet man Fritzboxen und NAS dagegen ab und lernt, wie man das eigene WLAN auf verdächtige Aktivitäten überwacht.

ONLINE-ACCOUNTS SC

Das Mittel der Wahl gegen Daten- und Identitätsdiebstahl ist nach wie vor die Zwei-Faktor-Authentifizierung. Wir erklären das Prinzip und testen dafür geeignete Hardware wie FIDO2-Sticks.

SICHER SURFEN MIT VPN

Mit einem Virtual Private Network verschlüsselt man den Datenverkehr und surft so zum Beispiel auch in fremden WLANs sicher. Doch im VPN-Markt tummeln sich neben seriösen auch viele unseriöse Anbieter.

MIT HACKING-TOOLS PROBLEME LÖSEN

Einfach mal ein bisschen hacken: Wir haben die spannendsten Hacking-Tools für Einsteiger und Profis herausgesucht und erklären, wie man sie zu hehren Zwecken einsetzt – zum Beispiel, um das eigene Passwort zu knacken oder aus dem System auszulesen.

SERVER & WEBANWENDUNGEN SICHERN

Täglich kommen Serverbetreibern aus aller Welt persönliche Daten von Nutzern und andere heikle Informationen abhanden oder die Daten werden zwecks Erpressung verschlüsselt. Aus solchen Fällen lässt sich lernen.

ZUM HEFT

Security-Checkliste

Windows

Auf Windows haben es Hacker besonders häufig abgesehen – schlicht, weil es so verbreitet ist. Die gute Nachricht ist, dass Sie sich bereits mit Bordmitteln vor den meisten Angriffen schützen können.

Von **Ronald Eikenberg**

Bild: Andreas Martini

☑ Updates installieren

Microsoft liefert regelmäßig Updates, die offene Sicherheitslücken in Windows schließen. Den aktuellen Stand der Dinge erfahren Sie, indem Sie „Nach Updates suchen“ ins Startmenü tippen. Die letzte Überprüfung sollte nicht länger als ein paar Tage her sein. Klicken Sie dort auf den Knopf, der ebenfalls mit „Nach Updates suchen“ beschriftet ist, wenn die Versorgung klemmt, „Jetzt installieren“ startet verfügbare Updates. Sorgen Sie unter „Erweiterte Optionen“ dafür, dass Sie auch „Updates für andere Microsoft-Produkte“ über Windows Update bekommen.

Alte Windows-Versionen versorgt Microsoft nicht mehr mit Sicherheits-Patches, wodurch das Angriffsrisiko steigt. Nutzen Sie daher am besten ein Windows mit dem derzeit aktuellen Funktions-Upgrade (etwa 21H1). Halten Sie auch Anwendungen wie Browser, Mail-Client, PDF-Viewer und Video-

☑ Virenschutz überprüfen

Ein Virenschutzprogramm kann Sie zwar nicht vor allen Gefahren schützen, doch vor vielen. Bei allen aktuellen Windows-Versionen ist der Windows Defender vorinstalliert, der inzwischen mit der Konkurrenz locker mithalten kann. Stellen Sie sicher, dass er aktiv ist und mit aktuellen Virensignaturen versorgt wird. Öffnen Sie hierzu „Windows-Sicherheit“ über das Suchfeld des Startmenüs und klicken Sie anschließend auf „Viren- & Bedrohungsschutz“. Ein manuelles Signaturupdate starten Sie mit „Nach Updates suchen“ (unter Windows 11 müssen Sie vorher noch auf „Schutzupdates“ klicken).

☑ Zugriffsschutz aktivieren

Ihr Rechner muss auch vor Angriffen von Personen, die sich dem Rechner nähern, geschützt werden. Im

Lesen Sie mehr in c’t Security 2021

Bild: Sven Hauth

WLAN-Alarmanlage

WLAN ist praktisch, birgt aber auch viele Risiken: Jeder in Funkreichweite kann Router und Clients attackieren – und zwar weitgehend unbemerkt. Ein Raspi mit Nzyme schlägt Alarm, wenn sich jemand an Ihrem Netz zu schaffen macht.

Von **Tomas Jakobs**

Drahtlose Netzwerke sind vielen Gefahren ausgesetzt: Mittels Deauthentication können Angreifer WLAN-Clients beispielsweise zwingen, die Verbindung zur Basisstation zu trennen. Das geschieht entweder aus Spielerei oder um sie zu einer Verbindung mit einem Zugangspunkt unter Kontrolle der Angreifer zu animieren, der das WLAN-Netz der ursprünglichen Basisstation imitiert. Das Ziel ist, den Datenverkehr auszulesen oder zu manipulieren (Man-in-the-middle-Attacke). All das ist längst kein Hexenwerk mehr, es gibt sogar einsatzfertige Hacking-Gadgets, die Standardangriffe auf Knopfdruck ausführen [1].

Normalerweise bekommt man von WLAN-Attacken bestenfalls etwas mit, wenn die Angreifer längst ins Netzwerk eingestiegen sind. Doch Sie können vorbeugen und mit Nzyme aktiv nach auffälligen WLAN-Aktivitäten scannen. So bekommen Sie schnell mit, wenn etwa ein neues Netz in der Umgebung auftaucht, das Ihrem verdächtig ähnelt oder Ihre Geräte fremdgesteuert angewiesen werden, die Verbindung zu kappen. Die nötige Hardware kostet nur ein paar Euro und einen passenden Raspi haben Sie vielleicht sogar schon in der Schublade.

Das Open-Source-Projekt Nzyme fungiert als Wireless Intrusion Detection System (WIDS), also als Alarmanlage für Drahtlosnetzwerke. Gerade erschien die Version 1.1.1, welche die gröbsten Kinderkrankheiten hinter sich gelassen hat. Das Release bietet eine gute Gelegenheit zu erklären, wie Sie Nzyme in Betrieb nehmen und das eigene WLAN vor neugierigen Augen schützen. Entdeckt Nzyme Anomalien im Funkverkehr, warnt es in der Weboberfläche und versendet auf Wunsch E-Mails an den Administrator.

Frame-Sammler

Nzyme arbeitet im Hintergrund als Sniffer für die sogenannten WLAN-Management-Frames. Drahtlosgeräte senden Management-Frames meist unverschlüsselt, um Informationen auszutauschen. Sie machen so beispielsweise auf sich aufmerksam oder bereiten einen WPA-Handshake vor. Der Unterschied zu den bekannten Sniffern aus Pentesting-Werkzeugsammlungen liegt in der konsequenten Ausrichtung auf automatisiertes Schnüffeln und Warnen. Im Idealfall wird Nzyme stationär auf die Lauer gelegt und sich selbst überlassen. Fachkenntnisse über den Aufbau von WLAN-Paketen sind für den Betrieb von Nzyme nicht nötig. Die Software überwachte für diesen Artikel über einen Monat das heimische Netzwerk des Autors und konnte die eigenen Hackingversuche erfolgreich aufspüren.

Der Nzyme-Entwickler Lennart Koopmann hat das Tool für den Raspi konzipiert. Der Dokumentation zufolge reicht bereits ein Raspi 3 für kleine Heimnetze. Für diesen Artikel diente ein Raspi 4 mit 4 GByte Arbeitsspeicher als Testgerät. Bei Mesh-Drahtlosnetzwerken in Unternehmen empfehlen sich mehrere Raspis mit Nzyme für eine bessere Abdeckung der größeren Fläche. Diese können ihre Daten zur Auswertung an einen zentralen Log-Server im internen Netz schicken, beispielsweise an Graylog, das vom gleichen Entwickler stammt. So kann man kostengünstig auch große Netze scannen.

Für Nzyme genügt ein Raspberry Pi 3 oder neuer. Dazu brauchen Sie einen WLAN-USB-Stick, der den Monitor-Modus beherrscht.

Zur Überwachung der Funkfrequenzen ist ein WLAN-Modul nötig, das den sogenannten Monitor

WLAN-Management-Frames

Zur Überwachung des eigenen Netzes sammelt Nzyme WLAN-Management-Frames ein und meldet verdächtige Vorkommnisse, siehe dazu den Kasten „Verdächtige WLAN-Aktivitäten“ auf Seite 60. Neben Management-Frames gibt es auch weitere Arten von Frames, wie „control“, „extension“ und „data“, die für Nzyme nicht relevant sind.

- Der **Association Request** folgt auf Authentication und fragt Ressourcen an der Basisstation an.
- Darauf folgt die **Association Response**. Wenn erfolgreich, dann darf das assoziierte Gerät weitere Frame-Arten senden, beispielsweise „data“ für Datenübertragung.
- Mit **Deauthentication** verlangt ein Drahtlosgerät die

Lesen Sie mehr in c’t Security 2021

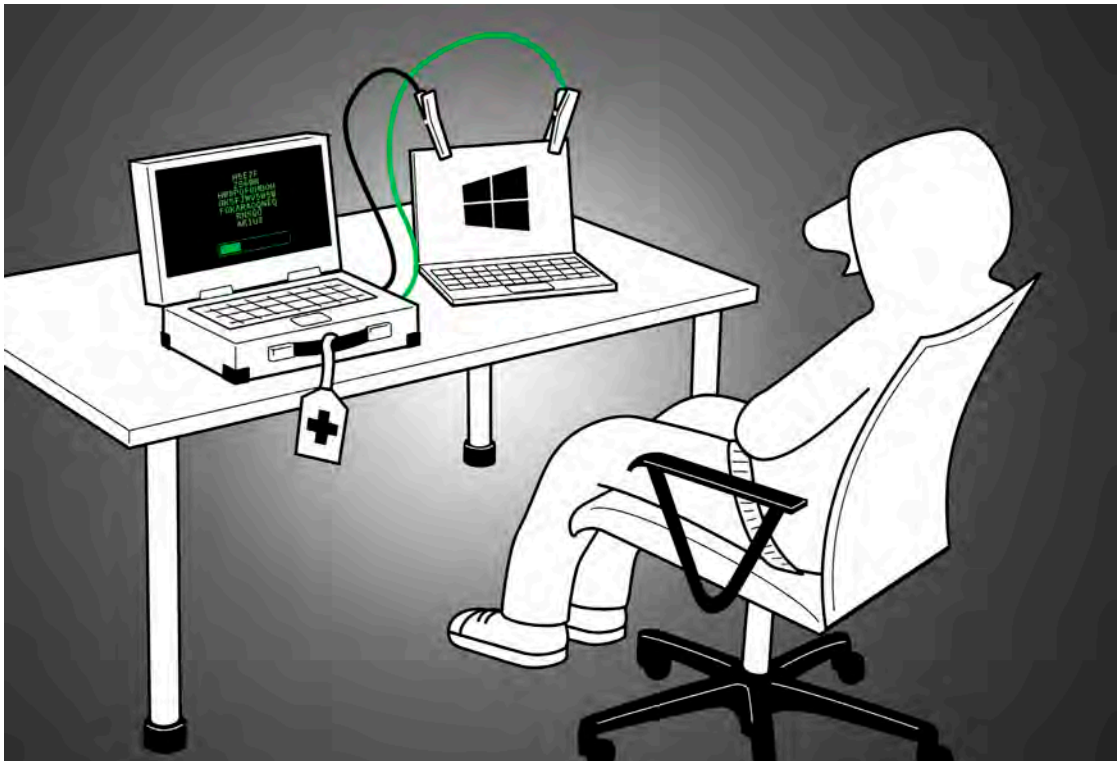


Bild: Sven Hauth

Nützliche Hacking-Tools für den Alltag

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.

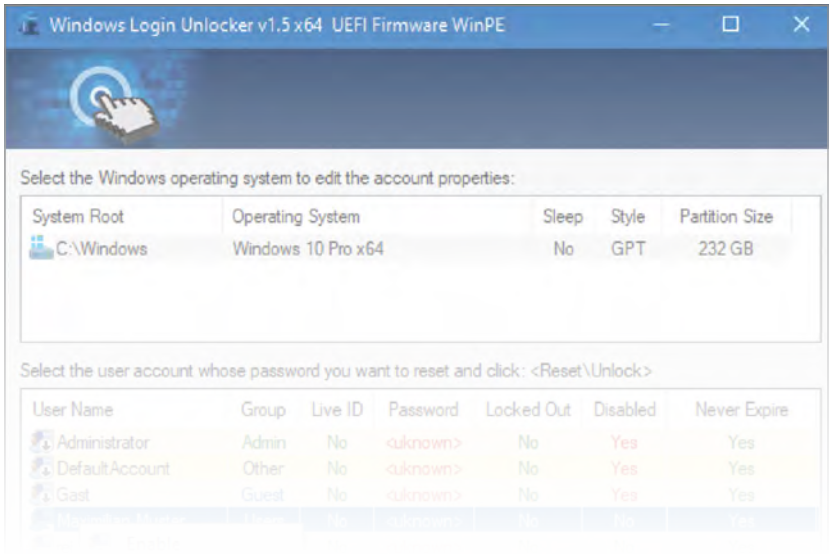
Von **Ronald Eikenberg und Alexander Königstein**

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/wn7d.



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.

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/wn7d). Sie finden das Tool im Notfall-Windows unter „Start/Datenrettung“.

Die Bedienung des Unlockers erklärt sich fast von

Bild: Andreas Martini

IoT ungesichert im Netz

Vernetzte Anlagen können in der Industrie viele Probleme lösen. Hängt man sie ungeschützt ins Internet, schafft man sich aber eine Menge neue. Bei unserer Suche nach schlampigen Konfigurationen wurden wir allzu häufig fündig.

Von **Jan Mahn**

Wenn Privatpersonen versehentlich ihr Smart-Home ungeschützt ins Internet hängen, ist der Schaden überschaubar. Schlimmstenfalls können Scherzbolde aus der Ferne das Licht abschalten oder die Rollläden schließen. Richtig unangenehm wird es aber, wenn Industrieunternehmen ihre vernetzte oder „smarte“ Fabrik mit der ganzen Welt teilen. Das Potenzial für Erpressungen und Sabotage ist riesig. Was passiert, wenn Angreifer eine Chemiefabrik oder eine Ölraffinerie fernsteuern, möchte

man sich nicht ausmalen. Eigentlich sollte man davon ausgehen, dass solche Unternehmen eigene IT-Sicherheitsexperten beschäftigen oder Expertise einkaufen und sich nach dem Stand der Technik gegen Angriffe schützen. Eigentlich.

Auf die Idee, die Sicherheit von Industrieanlagen mal systematisch zu untersuchen, brachte uns ein Tippgeber, der durch Zufall einen offenen MQTT-Server im Internet gefunden hatte. MQTT ist ein Protokoll, über das Sensoren und Aktoren einander Nachrichten schicken. Dabei läuft die Kommunikation nicht direkt von Gerät zu Gerät, sondern immer über einen MQTT-Broker, bei dem andere die Nachrichten abonnieren können. Das Protokoll haben wir bereits ausführlich vorgestellt [1] und nutzen es in Kombination mit Node-Red im c't Smart-Home (siehe ct.de/wke5). Hat man gute Gründe dafür, kann man MQTT durchaus im Internet veröffentlichen – dafür verwendet man aber unbedingt MQTT über TLS auf Port 8883 und richtet für alle Endgeräte Benutzerkonten ein. Anmelden können Sie sich entweder per Passwort oder noch besser mit einem Zertifikat.

Unseren Scanner haben wir nur auf ungeschützte Broker angesetzt. Zunächst ließen wir ihn eine Liste aller Server generieren, die auf Port 1883, also mit unverschlüsseltem MQTT antworten. Die Treffer haben wir dann darauf geprüft, ob sie Verbindungen ohne Anmeldedaten zulassen – über 10 000 Adressen landeten so in unserer Liste.

Private Freizügigkeit

Am Anfang schauten wir uns einige Treffer stichprobenartig an. Abonniert man auf einem MQTT-Broker alle Topics, kann man bereits ganz brauchbar abschätzen, für was der Server genutzt wird. Nicht gerade überraschend waren die vielen Smart-Homes, die wir rund um den Globus von Berlin bis Sidney fanden. Topics wie `livingroom/lights/center` verraten allzu eindeutig, wofür der Broker gedacht ist. Bei solchen privaten Umgebungen sahen wir häufig dasselbe zen, um die Heizung abzuschalten, wenn niemand zu Hause ist. Viele Smart-Home-Bastler wollen sich damit eine datenschutzfreundliche Alternative zu kommerziellen Location-Trackern bauen. Wer dafür aber einen ungesicherten MQTT-Server nutzt, erreicht leider genau das Gegenteil. Häufig konnte man aus den Topics leicht alle Familienmitglieder identifizieren (`peter_phone` und `marie_iphone`). Leichter kann man es Kriminellen nicht machen, den perfekten Zeitpunkt für einen Einbruch zu planen. Wo immer wir Hinweise auf den Betreiber finden konnten, informierten wir diesen. Owntracks kommt gut mit TLS und Authentifizierung klar, man muss sie nur aktivieren.

Industrielle Probleme

Die Smart-Homes waren aber nur Beifang auf der Suche nach Industrieanlagen. Um die unzähligen Treffer etwas einzugrenzen, suchten wir gezielt nach statischen IP-Adressen, die nur selten zu Privatkundenanschlüssen gehören. Heraus kam eine bunte Sammlung an „professionellen" MQTT-Brokern mit Fehlkonfigurationen – voller Lese- und Schreibzugang für alle. Ein Hersteller von Snack-Automaten aus Italien teilte die Statusinformationen mit der ganzen Welt, ein portugiesischer Hersteller von Brandmeldeanlagen ließ über 5000 Anlagen fast sekündlich den Status auf einen öffentlichen Server schreiben.

In Nordland in Norwegen fanden wir einen Server mit Live-Telemetriedaten von 70 Fahrzeugen, offensichtlich Busse, die Fahrzeugdaten und Positionen an den Server verschickten. Denselben Fehler machte auch ein Dienstleister für öffentlichen Nahverkehr aus Westdeutschland. Auf dessen Server fanden wir Telemetriedaten für Busse mehrerer Nahverkehrsunternehmen. Wir kontaktierten den Anbieter und er aktivierte nach kurzer Zeit Authentifizierung und Verschlüsselung, stattete die Geräte mit Zugangsdaten aus. Die Versuchung, für Fahrzeugtelemetrie auf Authentifizierung zu verzichten, ist groß – schließ-