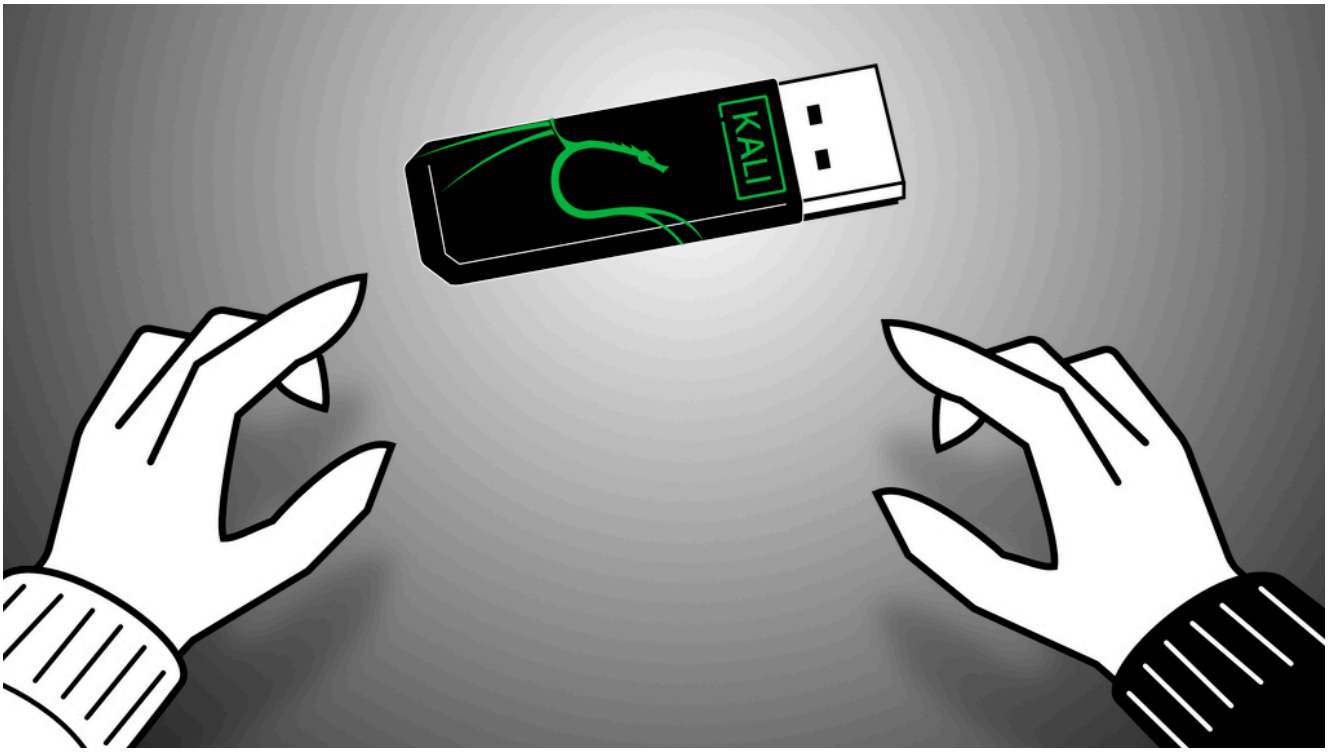
Kali Linux auf USB-Stick einrichten



Hacking-Stick

Mit Kali Linux können Sie etliche Hacking-Tools ohne Installation ausprobieren. Auf einem USB-Stick haben Sie es immer dabei.
Mit Kali Linux können Sie etliche Hacking-Tools ohne Installation ausprobieren. Auf einem USB-Stick haben Sie es immer dabei.

Von Ronald Eikenberg

Kali Linux ist in vielen Lebenslagen ein nützlicher Helfer: Es enthält etliche Hacking-Tools, die man sofort ausprobieren kann. Die oftmals umständliche Einrichtung der Programme fällt weg. Damit spüren Sie nicht nur Sicherheitsprobleme auf, die mitgelieferten Werkzeuge eignen sich auch zum Daten retten und für vieles mehr. Mit wenig Aufwand erstellen Sie sich einen bootfähigen USB-Stick, mit dem Sie sich selbst davon

überzeugen können.

Als Grundlage dient ein Debian, das perfekt auf die Bedürfnisse der Hacking-Community zugeschnitten wurde. Deshalb ist Kali genauso wie einst sein Vorgänger BackTrack Linux seit Jahren die erste Wahl bei Security-Experten und Hackern. Kali lässt sich wie jedes Betriebssystem installieren, doch das ist zum Ausprobieren gar nicht nötig. Im einfachsten Fall läuft das Hacker-Linux als Live-Betriebssystem vom USB-Stick – auf Wunsch auch mit Datenpartition, in der man dauerhaft Daten bunkern kann. Zudem gibt es allerhand virtuelle Maschinen sowie Images für Raspis und das mit Windows 10 eingeführte „Windows-Subsystem für Linux“ (WSL). Kurzum: Wer Kali testen möchte, der hat viele Optionen.

Kali-on-a-Stick

Dieser Artikel zeigt Ihnen das Einrichten eines Kali-Live-Sticks, den Sie universell einsetzen können, sowie die ersten Schritte, damit Sie komfortabel damit arbeiten können. Gegenüber einer virtuellen Maschine hat so ein Live-Stick den Vorteil, dass sein Betriebssystem direkt auf die Hardware des Rechners zugreifen kann. Das ist in Situationen wichtig, in denen ein hardwarenahes Hacking-Tool beispielsweise Direktzugriff auf Netzwerkkarte, USB-Geräte oder GPU benötigt.

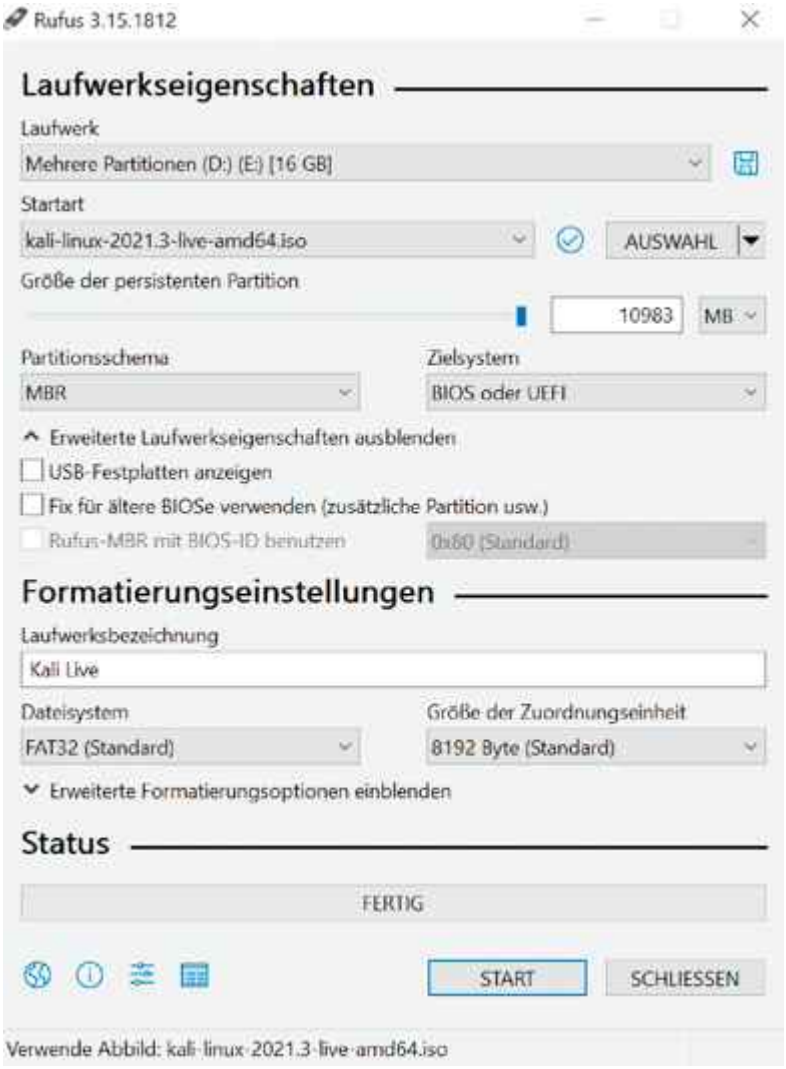
Auf der Download-Seite der „Live Boot“-Variante (siehe ct.de/ypk1) finden Sie zwei Kali-Versionen: Die stabile und getestete Snapshot-Version (etwa Kali 2021.3) und einen automatisch erstellten Weekly-Build, mit dem Sie näher am Puls der Zeit sind. Er enthält aktuellere Versionen der Komponenten, wodurch der erste Updatelauf schneller über die Bühne geht. Wenn Sie auf Nummer sicher gehen möchten, ist jedoch der Snapshot die bessere Wahl.

Live-Betriebssysteme sind üblicherweise vergesslich. Alle Änderungen am System landen lediglich im RAM und sind nach dem Herunterfahren verloren. Wenn Sie nicht jedes Mal bei Null

anfangen möchten, können Sie eine Persistence-Partition anlegen, in der Kali sämtliche Änderungen speichert, einschließlich Einstellungen, Home-Verzeichnis und Updates. Nutzen Sie am besten einen modernen USB-3-Stick, da mit der Geschwindigkeit des Speichers auch die Performance des Live-Systems steht und fällt. Ältere Stick-Semester bremsen das System unnötig aus und haben nicht selten Probleme beim Einsatz als Bootmedium. Moderne und flotte USB-Sticks bekommen Sie bei den bekannten Onlinehändlern bereits für weniger als 10 Euro. Der Stick sollte mindestens 8 GByte fassen.

Live-Linux mit Gedächtnis

Über das Anlegen der Persistence-Partition müssen Sie sich nicht den Kopf zerbrechen, denn das erledigen Sie beim Beschreiben des USB-Sticks nebenbei. Kali Linux erwartet eine ext3-Partition namens „persistence“, die sich über den gesamten überschüssigen Speicher Ihres Sticks erstrecken kann. Eine hohe Kapazität zahlt sich also aus. Bei einem 8-GByte-Stick kann sich der Speicherbereich für Ihre Daten immerhin bereits auf mehr als 3 GByte entfalten. Damit Kali die Partition erkennt, muss auf ihr eine Datei „persistence.conf“ mit dem Inhalt / union gespeichert sein.



Klick, Klick, Stick: Rufus erstellt nach ein paar Mausklicks einen bootfähigen Kali-Stick samt Persistence-Partition, in der Sie Daten dauerhaft ablegen können.
Sie könnten die Partition mit einem Partitionierer Ihrer Wahl (zum Beispiel GParted oder MiniTool Partition Wizard Free) von Hand anlegen, nachdem Sie den Stick mit dem Kali-Image bespielt haben. Doch warum kompliziert, wenn es auch einfach geht? Bei uns hat sich das Windows-Tool Rufus (siehe ct.de/ypk1) bewährt, das dem USB-Stick nicht nur das Kali-Image verpasst, sondern im gleichen Arbeitsgang auch eine geeignete Persistence-Partition.

Um einen Persistence-Stick mit Rufus zu erstellen, starten Sie das Tool und wählen ganz oben den angeschlossenen USB-Stick als Schreibziel aus. Anschließend speisen Sie über „Auswahl“ das Kali-ISO ein, zum Beispiel „kali-linux-2021.3-live-amd64.iso“. Achten Sie darauf, dass der Dateiname „live“

enthält, um sicherzustellen, dass Sie es mit der richtigen Datei zu tun haben – die „installer“-Versionen eignen sich ausschließlich zur Installation, sie enthalten keinen Livemodus.

Danach kümmern Sie sich um die Persistence-Partition. Ziehen Sie gleich darunter den Schieberegler „Größe der persistenten Partition“ ganz nach rechts, damit der Persistence-Bereich so groß wie möglich wird. Ändern Sie rechts daneben die Speichergrößeneinheit von „GB” auf „MB” und ziehen Sie den Schieberegler erneut nach rechts, um noch ein paar MByte extra herauszuquetschen. Den Rest können Sie auf den Vorgabewerten belassen. Klicken Sie auf „Start” und bestätigen Sie etwaige Rückfragen. Nach einigen Minuten, abhängig von der Schreibgeschwindigkeit Ihres USB-Sticks, ist Kali startklar.

Für Linux und macOS gibt es Rufus leider nicht, Sie können Ihr Glück mit UNetbootin versuchen (siehe ct.de/ypk1), das ähnlich funktioniert. Bei uns war es etwas wählerischer bei der Auswahl des Schreibziels, wir konnten aus ungeklärten Gründen nicht jeden USB-Stick damit bespielen. In vielen Fällen hat es jedoch erfolgreich einen bootfähigen Kali-Stick samt Persistence-Partition erzeugt. Wählen Sie unter „Abbild” einfach das Kali-ISO aus und in das Eingabefeld neben „Platz um Dateien zwischen Neustarts zu erhalten (nur Ubuntu)” tragen Sie irgendeine Zahl größer Null als Wunschgröße für die Datenpartition ein.

Die eingetippte Zahl wurde bei uns übrigens stets ignoriert, UNetbootin hat stattdessen die maximal mögliche Partitionsgröße genutzt. Abschließend starten Sie das Bespielen mit dem Ok-Knopf. Falls Sie den Stick lieber per Shell vorbereiten möchten, hilft Ihnen die offizielle Kali-Dokumentation weiter (siehe ct.de/ypk1). Dort erfahren Sie auch, wie Sie die Partition mit LUKS verschlüsseln, um sie vor unbefugten Zugriffen zu schützen.

Die Kali-Installation enthält etliche Security-Tools, die man ohne Installation ausprobieren kann.

Auf Probefahrt

Zeit für eine ersten Testfahrt! Wenn Sie ein aktuelles Windows nutzen, können Sie Ihren Rechner einfach über die erweiterten Startoptionen anweisen, vom Stick zu booten: Öffnen Sie über eine Startmenü-Suche „Optionen für den erweiterten Start ändern“ und klicken Sie unter „Erweiterter Start“ auf „Jetzt neu starten“. Nach dem Neustart wählen Sie die Option „Ein Gerät verwenden“ und anschließend den USB-Stick.

Es sollte der Grub-Bootmanager im Kali-Design erscheinen, der Ihnen diverse Startkonfigurationen anbietet. Wählen Sie „Live USB Persistence“, damit die Datenpartition des Sticks korrekt eingebunden wird. Falls Sie das nicht wünschen, wählen Sie mit dem obersten Eintrag den regulären Livemodus, der jedes Mal mit einem frischen System startet und nach der Nutzung sämtliche Änderungen vergisst.

Falls Sie den erweiterten Start nicht nutzen können, etwa weil Sie ein anderes Betriebssystem einsetzen, können Sie Ihren Rechner auch regulär vom Stick booten, indem Sie das System mit angeschlossenem Kali-Stick einschalten. Mit etwas Glück klappt der Start sofort, andernfalls müssen Sie im BIOS die Bootreihenfolge ändern oder, falls vorhanden, den Bootmanager des BIOS nutzen, um das System vom Stick zu starten.

Hierzu drücken Sie direkt nach dem Einschalten des Rechners eine bestimmte F-Taste. Welche genau, erfahren Sie in der Dokumentation des Herstellers oder über eine Google-Suche. Hier kocht jeder Hersteller sein eigenes Süppchen. Bei Asus beispielsweise öffnet sich das BIOS über die F2-Taste, mit F8 erreicht man die temporäre Auswahl des Bootmediums. Falls Sie den Rechner weiterhin nicht vom Stick starten können, probieren Sie am besten erst eine andere USB-Buchse, sonst einen anderen Stick aus.

Wenn Secure Boot in Ihrem Rechner aktiv ist, müssen Sie es zumindest vorübergehend im BIOS deaktivieren, da die Signaturüberprüfung an Kalis UEFI-Bootloader scheitert. Bei Surface-Geräten kann das Abschalten von Secure Boot dazu führen, das Sie später einmalig den Bitlocker-Wiederherstellungsschlüssel eingeben müssen, den Windows bei der Ersteinrichtung im Microsoft-Konto für Sie speichert.

Erste Schritte

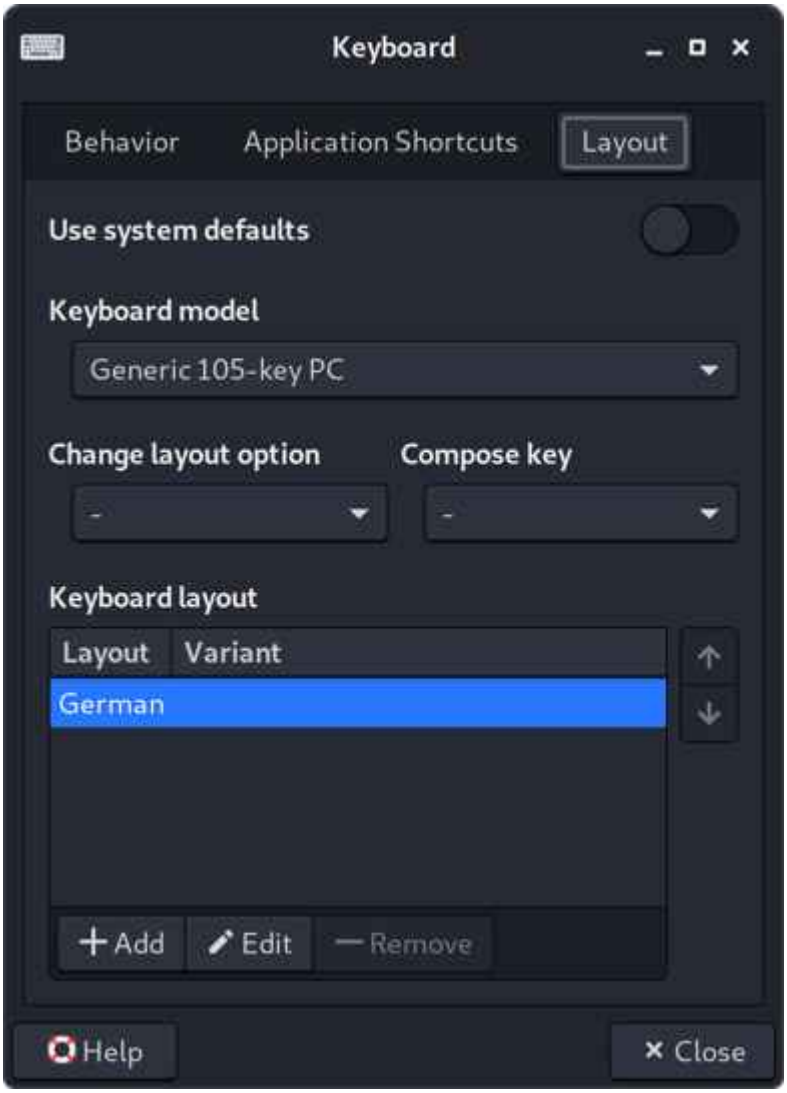
Hat alles geklappt, bootet Kali nach kurzer Zeit automatisch bis zum Desktop durch, die Eingabe eines Passworts ist nicht nötig. Falls sich Kali nach einiger Zeit der Inaktivität sperrt, erlangen Sie mit dem vorgegebenen Nutzernamen kali und dem gleichnamigen Passwort kali wieder Zugriff.

Die Xfce-Desktopumgebung macht Ihnen den Einstieg in die Kali-Welt leicht: Das Bedienkonzept unterscheidet sich nicht von anderen modernen Betriebssystemen. Ein wichtiger Dreh- und Angelpunkt ist das Kali-Menü, das Sie über das Logo oben links

und über die Windows-Taste erreichen. Hier finden Sie die Einstellungen und alle wichtigen Hacking-Tools, die bereits installiert sind. Die Kategorien wie „Password Attacks“ und „Wireless Attacks“ helfen Ihnen, sich zurechtzufinden und nützliche Werkzeuge zu entdecken.

Darunter befinden sich Klassiker wie Wireshark, Nmap, OWASP ZAP, Metasploit, aber auch exotischere Spezialtools, die nur für ganz bestimmte Aufgaben nützlich sind. Falls Sie schon wissen, wonach Sie suchen, können Sie einfach das Suchfeld ganz oben benutzen, um das gewünschte Tool aufzuspüren und zu starten. Eine Auswahl interessanter Hacking-Tools und Tipps zur Bedienung finden Sie auf Seite 24.

Nach dem ersten Start sind noch ein paar Handgriffe nötig, um komfortabel arbeiten zu können, denn das System läuft mit einer Standardkonfiguration und ist noch nicht an die hiesigen Bedürfnisse angepasst. So ist etwa das QWERTY-Tastaturlayout eingestellt, was unter anderem die Eingabe von Shell-Befehlen erschwert. Solche Einstellungen werden normalerweise während der Installation abgefragt, die Sie mit dem Livesystem gewissermaßen übersprungen haben. Doch das ist schnell korrigiert.



Erste Amtshandlung: Im Live-Modus sollte man zunächst das Tastaturlayout ändern.

Tastaturlayout ändern

Starten Sie die Tastatureinstellungen im Kali-Menü über „Settings/Keyboard“ und wechseln Sie auf den Registerreiter „Layout“. Deaktivieren Sie ganz oben den Schalter „Use system defaults“, um die darunterliegenden Einstellungen zu entsperren. Anschließend klicken Sie auf den „Add“-Button und wählen „German“ aus. Die Untervarianten hiervon können Sie ignorieren. Nach dem Hinzufügen können Sie „English“ über „Remove“ entfernen, da es nicht länger benötigt wird.

Falls Sie die Bedienoberfläche auf Deutsch umstellen möchten, öffnen Sie einfach den Terminal Emulator und tippen dort den folgenden Befehl ein: sudo localectl set-locale

LANG=de_DE.UTF-8. Sobald Sie sich über den Abmelden-Knopf in der rechten oberen Ecke des Bildschirms ausloggen („Log Out“) und wieder anmelden (mit kali/kali), spricht Kali Deutsch. Selbst die Tool-Kategorien im Kali-Menü sind übersetzt, was die ersten Schritte erleichtert. Wenn Sie mögen, ändern Sie jetzt noch das Anzeigeformat der Uhr oben rechts nach einem Rechtsklick übers Eigenschaften-Menü von 12 auf 24 Stunden. Rechts neben der Uhrzeit finden Sie das NetworkManager-Applet, über das Sie eine WLAN-Verbindung zum Router schaffen können – zum Beispiel für Updates. Dazu gleich mehr.

Falls Sie ein Notebook oder Display mit hoher Auflösung auf verhältnismäßig kleiner Fläche nutzen, zum Beispiel ein 15-Zoll-Notebook mit 4K-Display, dann wird Ihnen die dargestellte Kali-Bedienoberfläche möglicherweise winzig vorkommen. Mehr Bedienkomfort gibt es im HiDPI-Modus, der fast alles auf 200 Prozent skaliert, wie man es zum Beispiel von Windows kennt. Suchen Sie im Kali-Menü nach dem „Kali HiDPI Mode” und starten Sie ihn. Die Änderung ist sofort aktiv. Auf dem gleichen Weg können Sie auch den ursprünglichen Skalierungsmodus wiederherstellen. Auf grafische Anwendungen, die als root gestartet werden, hat der HiDPI-Modus derzeit leider keine Auswirkungen. Über das Menü „Anzeige“ können Sie die Darstellung weiter verfeinern, etwa durch Ändern der Auflösung oder individuelle Skalierungsstufen (dabei sind auch negative Werte erlaubt).

Die Shell ist Dein Freund

Auch wenn viele Tools eine grafische Oberfläche haben: Der Dreh- und Angelpunkt ist das Terminal. Mit Kali nutzen Sie die moderne Z-Shell (ZSH), mit der die Eingabe der Befehle so bequem wie möglich ist. Sie erfahren bereits beim Tippen, ob Sie auf dem richtigen Weg sind: Solange Ihre Eingabe rot gefärbt ist, würde die Ausführung zu einem Fehler führen. Bekannte Befehle erscheinen grün und mit der Tabulatortaste können Sie die aktuelle Eingabe von der Shell vervollständigen

lassen. So genügt es oft, die ersten Zeichen eines Kommandos einzugeben und Tab zu drücken. Genauso einfach hängen Sie Dateipfade an einen Befehl an, zum Beispiel, wenn Sie eine Datei mit Hashes in den Passwortknacker John the Ripper (siehe Seite 20) speisen möchten. Mit Strg+Alt+T öffnen Sie jederzeit ein neues Terminalfenster, Strg+Umschalt+T öffnet ein neues Tab in einem existierenden Terminal.

Wenn Sie Kali (oder seinen Vorfahren BackTrack) von früher kennen, wird Ihnen auffallen, dass Sie im System nicht länger als root mit uneingeschränkten Rechten unterwegs sind, sondern als „kali". Manche Tools benötigen jedoch weiterhin Superuser-Rechte, zum Beispiel bestimmte Betriebsmodi des Netzwerkscanners Nmap (siehe S. 25). Für solche Fälle starten Sie das Tool einfach mit einem vorangestellten sudo als root. Dies ist auch für viele Eingriffe ins System nötig, etwa zur Installation von Paketen und Updates. Hilfe zur Nutzung der Tools und Befehle erhalten Sie meist über man befehl oder, indem Sie -? oder --help an den Befehl anhängen.

Kali frischmachen

Mit den folgenden Befehlen bringen Sie Kali und die Tools auf den aktuellen Stand:

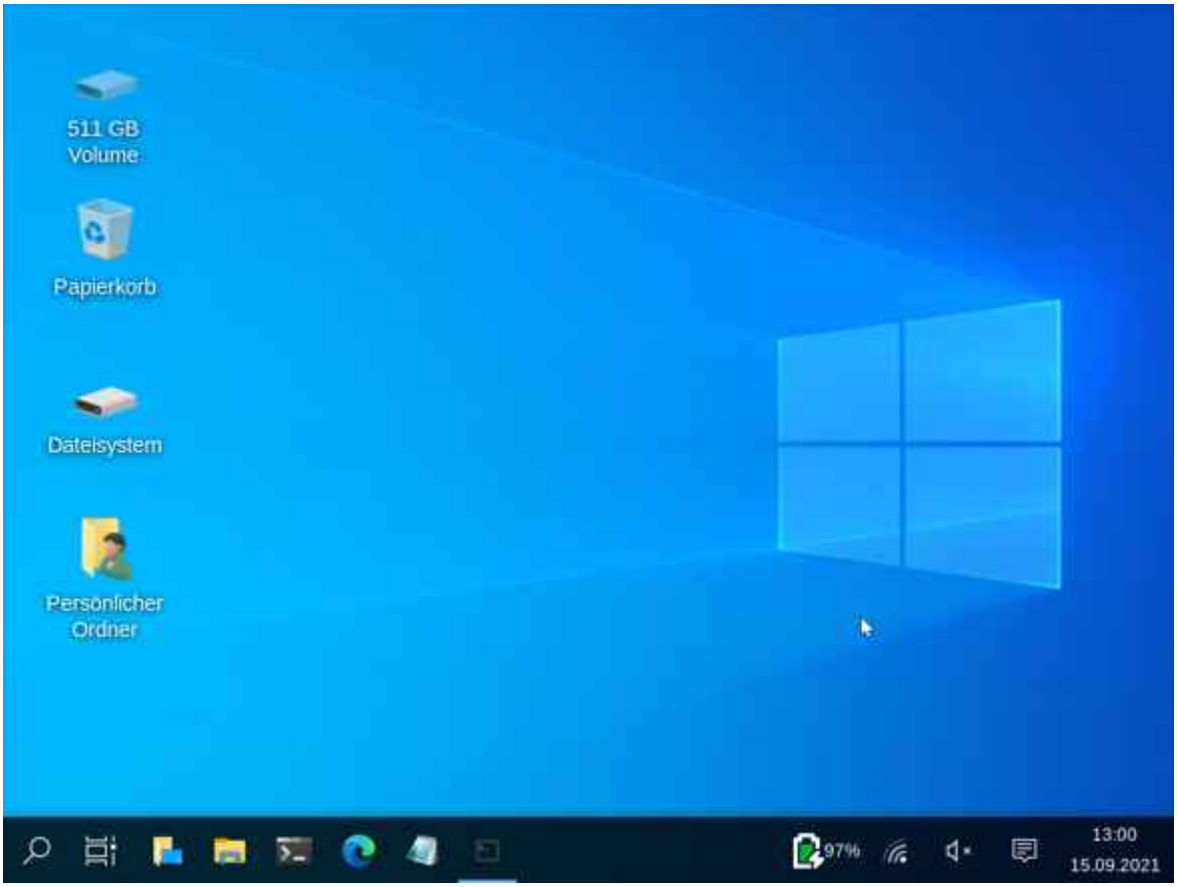
```
sudo apt update
sudo apt full-upgrade
```

Kali aktualisiert zunächst die Paketlisten und installiert anschließend die Updates. Je nachdem, wie aktuell Ihre Kali-Installation ist, kann dabei viel Zeit ins Land ziehen. Auch die Schreibgeschwindigkeit Ihres USB-Sticks spielt eine große Rolle. Möchten Sie ausschließen, dass der Upgrade-Vorgang zwischendurch darauf wartet, dass Sie Rückfragen beantworten, können Sie ein -y an den zweiten Befehl hängen, um alle Fragen im Vorfeld pauschal mit „Ja" zu bestätigen.

Tools nachrüsten

Falls Ihnen mal ein Tool fehlt, dann können Sie es wahrscheinlich aus dem Kali-Repository nachinstallieren. Sie können zum Beispiel nach Zenmap suchen, der grafischen Oberfläche für den Netzwerkscanner nmap: apt search zenmap

Danach installieren Sie den einzigen Suchtreffer zenmap-kbx mit sudo apt install zenmap-kbx. Das ist eines der ersten Tools, die als Kaboxer-Paket (Kali Applications Boxer) angeboten werden, was Sie an dem Namensbestandteil -kbx erkennen. Es handelt sich dabei um ein neues Containerformat, durch das sämtliche Abhängigkeiten in den passenden Versionen mitgeliefert werden können, ohne dass sie separat installiert werden müssen – ähnlich wie bei einem Docker-Container. Damit löst das Kali-Team das alte Problem, dass manche Tools aufgrund Ihrer Abhängigkeiten umständlich zu installieren sind oder sich mit anderen Tools in die Quere kommen. Ist der Vorgang abgeschlossen, können Sie das neue Tool über das Kali-Menü oder per Shell starten, in diesem Fall mit sudo zenmap-kbx.



Kali tarnt sich auf Wunsch als Windows 10.

Entdecke die Möglichkeiten

Mit Ihrem Kali-Stick steht Ihnen eine prall gefüllte Werkzeugtasche zur Verfügung, die Ihnen in vielen Situationen gute Dienste leistet. Die meisten Tools lassen sich zwar in die Oberkategorie „IT-Security“ einsortieren, doch Kali kann viel mehr. Wenn die Systemplatte streikt, können Sie mit TestDisk von Ihrem Stick einen Reparaturversuch starten und mit PhotoRec retten Sie verloren geglaubte Dateien. GParted ist ein leistungsfähiges grafisches Partitionierungsprogramm und Guymager erstellt Datenträgerabbilder, die sogar den Ansprüchen von Forensikern genügen. Falls Sie das Thema Forensik vertiefen möchten, sei Ihnen auch die Bootoption „forensic mode“ ans Herz gelegt: In diesem Betriebsmodus nimmt Kali keine Änderungen am System vor, was primär bedeutet, dass Laufwerke nie automatisch eingehängt werden. So kann man zum Beispiel ein Abbild der Festplatte ziehen, ohne Ihren Ist-Zustand zu verändern.

Zu guter Letzt sei noch der Undercover-Mode von Kali erwähnt, der mehr als eine Spielerei ist: Wenn Sie die Verknüpfung „Kali Undercover Mode“ über das Kali-Menü starten, verkleidet sich das Hacker-Linux kurz darauf als Windows 10. Die Taskleiste wandert Windows-typisch nach unten, als Hintergrundbild erscheint das blaue Windows-Bild. Das ist nicht nur witzig, es erlaubt Kali-Nutzern auch, im Alltag abzutauchen – und verhindert lästige Fragen neugieriger Mitmenschen.

Es gibt viel zu entdecken. Nehmen Sie sich etwas Zeit, um die zahllosen Möglichkeiten von Kali zu erkunden. Manchmal ist etwas Einarbeitung nötig, doch Sie erlernen wertvolles Hintergrundwissen darüber, wie die Dinge funktionieren und können fortan hinter die Kulissen blicken: Sorgt die neue Smart-Home-Kamera für mehr Sicherheit oder lässt sie auch Einbrecher in Ihr Wohnzimmer blicken? Wie lange hält Ihr WLAN einem Angriff stand? Ist Ihre WordPress-Installation ausreichend gegen Hacker geschützt? Mit Kali finden Sie es heraus. Inspiration liefert Ihnen der Artikel auf Seite 24, der viele wichtige und nützliche Tools detailliert vorstellt. *(rei@ct.de)*

Kali-Download & Tools: ct.de/ypk1