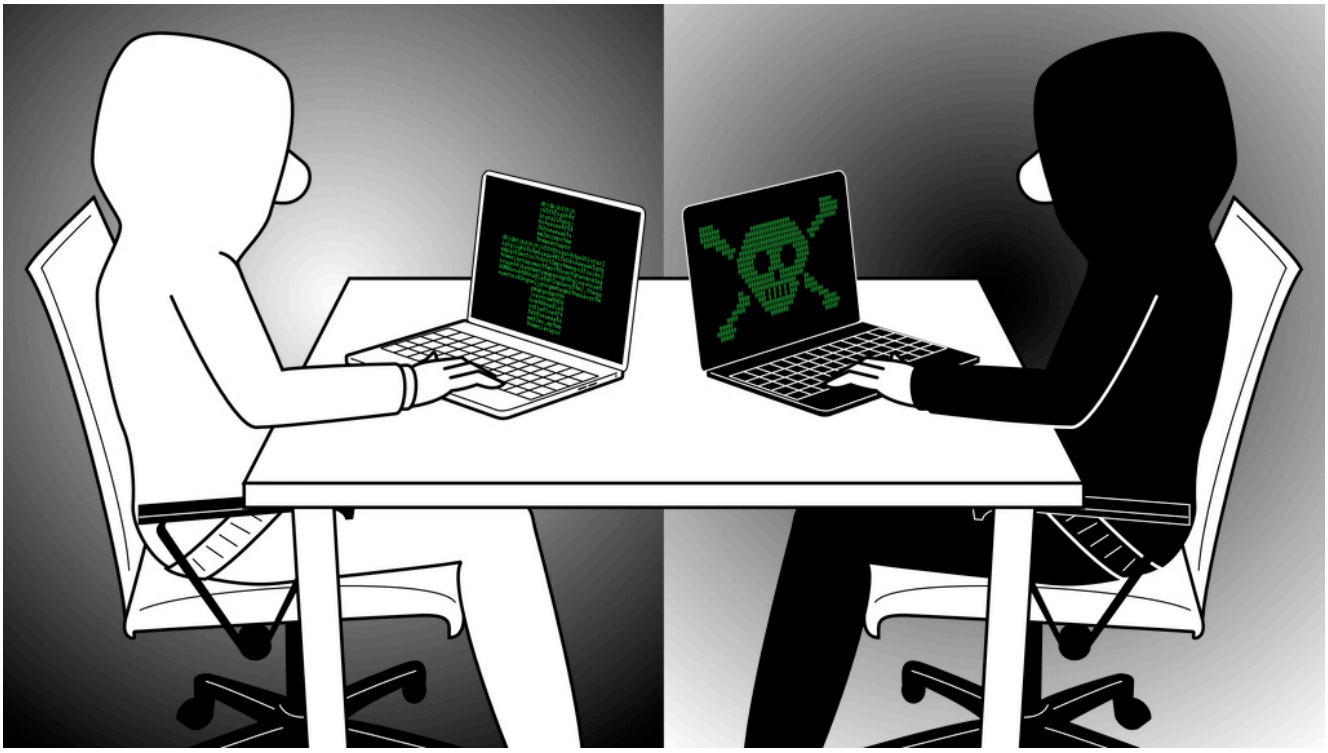
Hacking-Werkzeug für Fortgeschrittene



Gute Tools, böse Tools

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

Hacking-Werkzeug für Fortgeschrittene

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

Von Ronald Eikenberg und Alexander Königstein

Hollywood weiß Hacker-Aktivitäten in Szene zu setzen: Vor unzähligen Monitoren mit monochromatischen Benutzeroberflächen

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

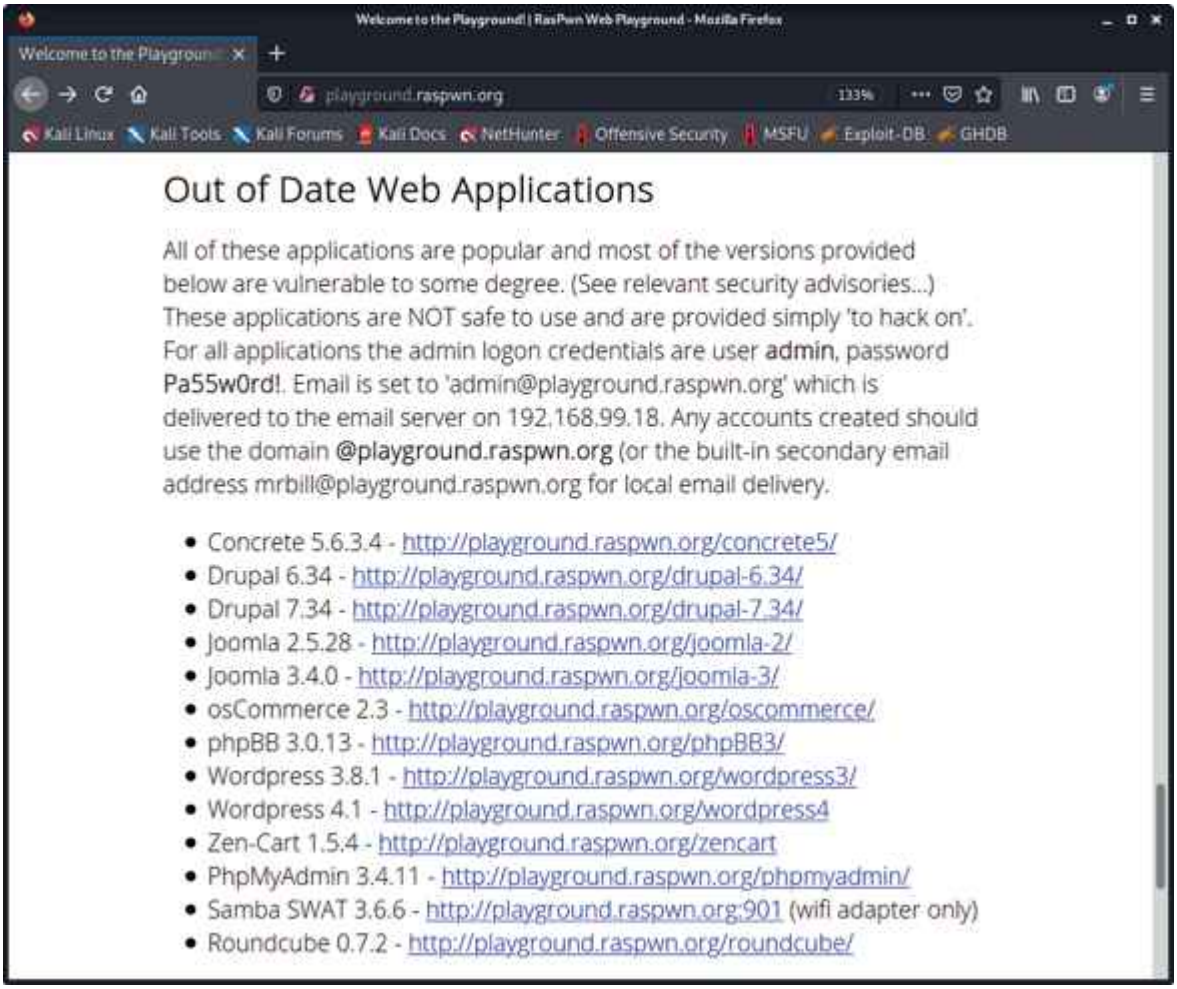
Mit den im Folgenden vorgestellten Profi-Tools spüren Sie Sicherheitslücken in Ihren Websites, Netzwerken, Apps, IoT-Geräten und vielem mehr auf. Anschließend können Sie gezielt Schutzmaßnahmen ergreifen und die Schlupflöcher stopfen, bevor es zu spät ist. Die meisten Hacking-Tools laufen am besten oder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

Angreifen erlaubt

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

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

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



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

Netzwerk auskundschaften

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

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

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

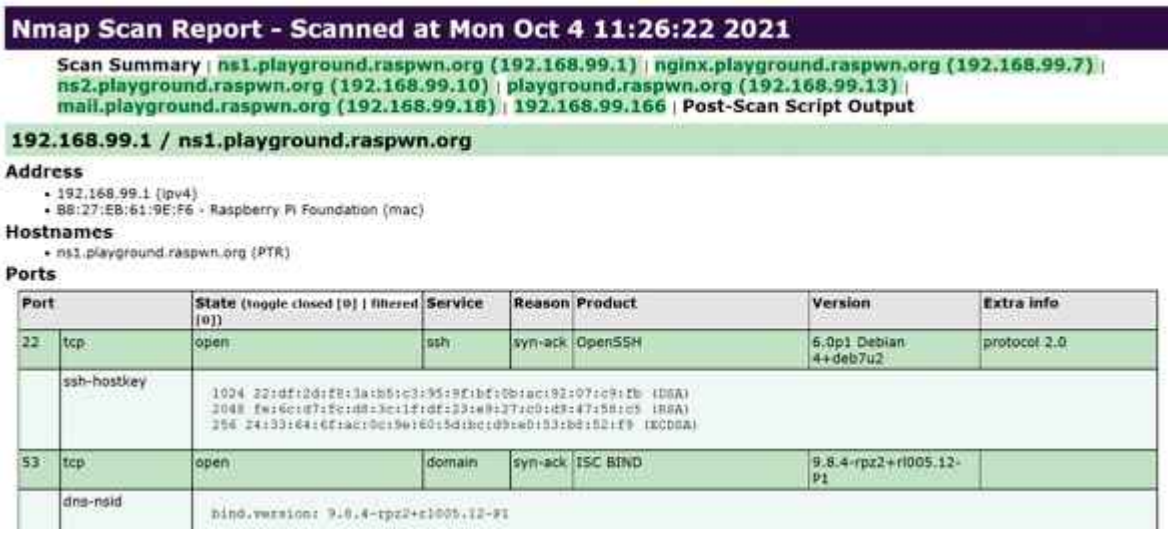
Wirklich komfortabel lesbar ist der Bericht auf der Shell nicht. Sie können jedoch leicht einen formatierten HTML-Report erstellen, indem Sie zunächst Nmap mit -oX ergebnis.xml anweisen, einen XML-Export der Ergebnisse zu schreiben. Anschließend bauen Sie daraus mit dem unter Kali vorinstallierten Tool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

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

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

Hardcore

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

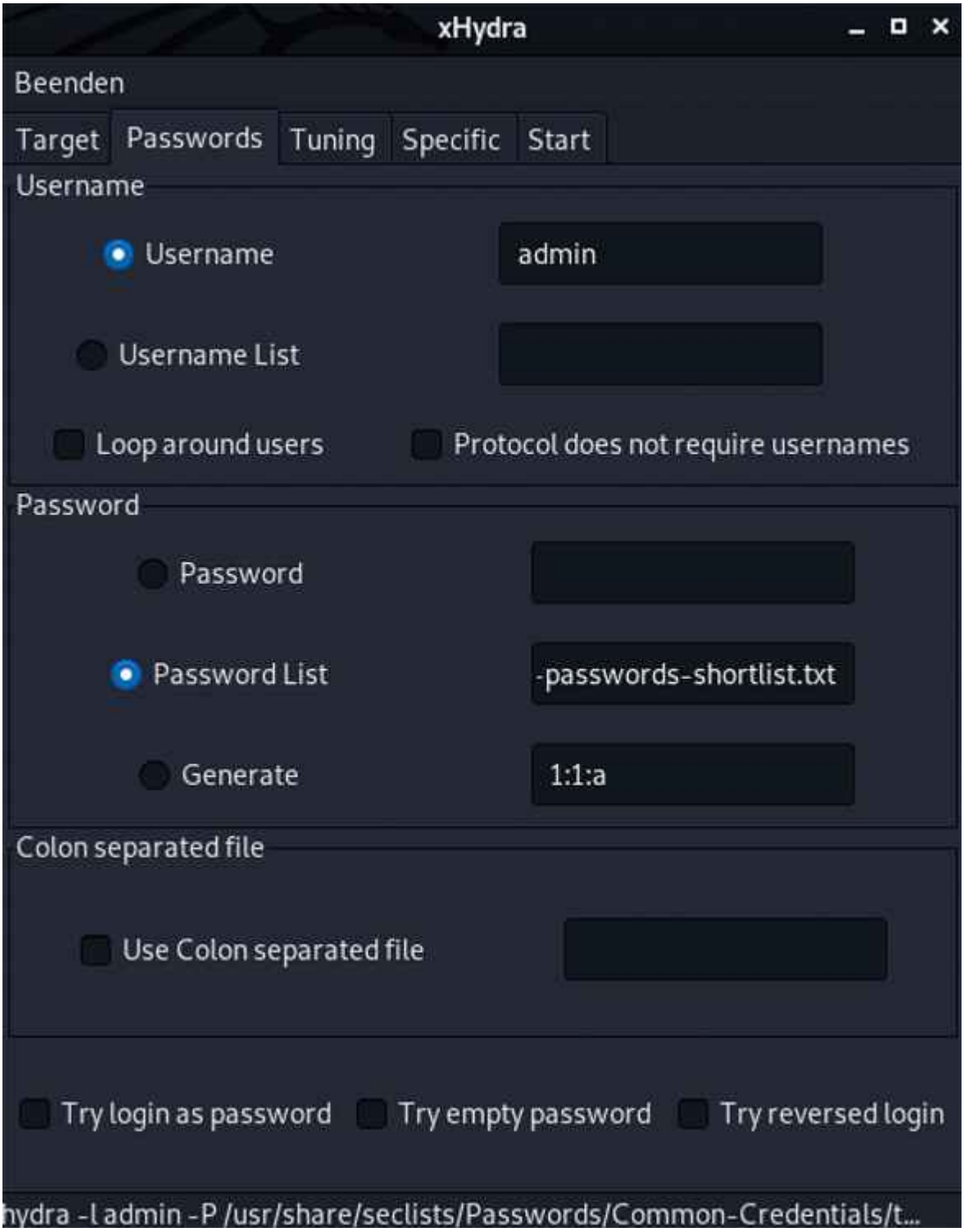


Was ist los im Netz? Der Netzwerkscanner Nmap liefert einen HTML-Bericht über alle Geräte und Dienste.

Zugriff auf Server

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

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



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

IPv4-Traffic umleiten

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

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

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

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

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

zudem beliebig umleiten, zum Beispiel an einen lokalen Server.

WLAN auf dem Prüfstand

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

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

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

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

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

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

Datenlecks im Webserver finden

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

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

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

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

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

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

WordPress-Lücken aufspüren

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

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

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

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

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

Datenbank-Lecks verhindern

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

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

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

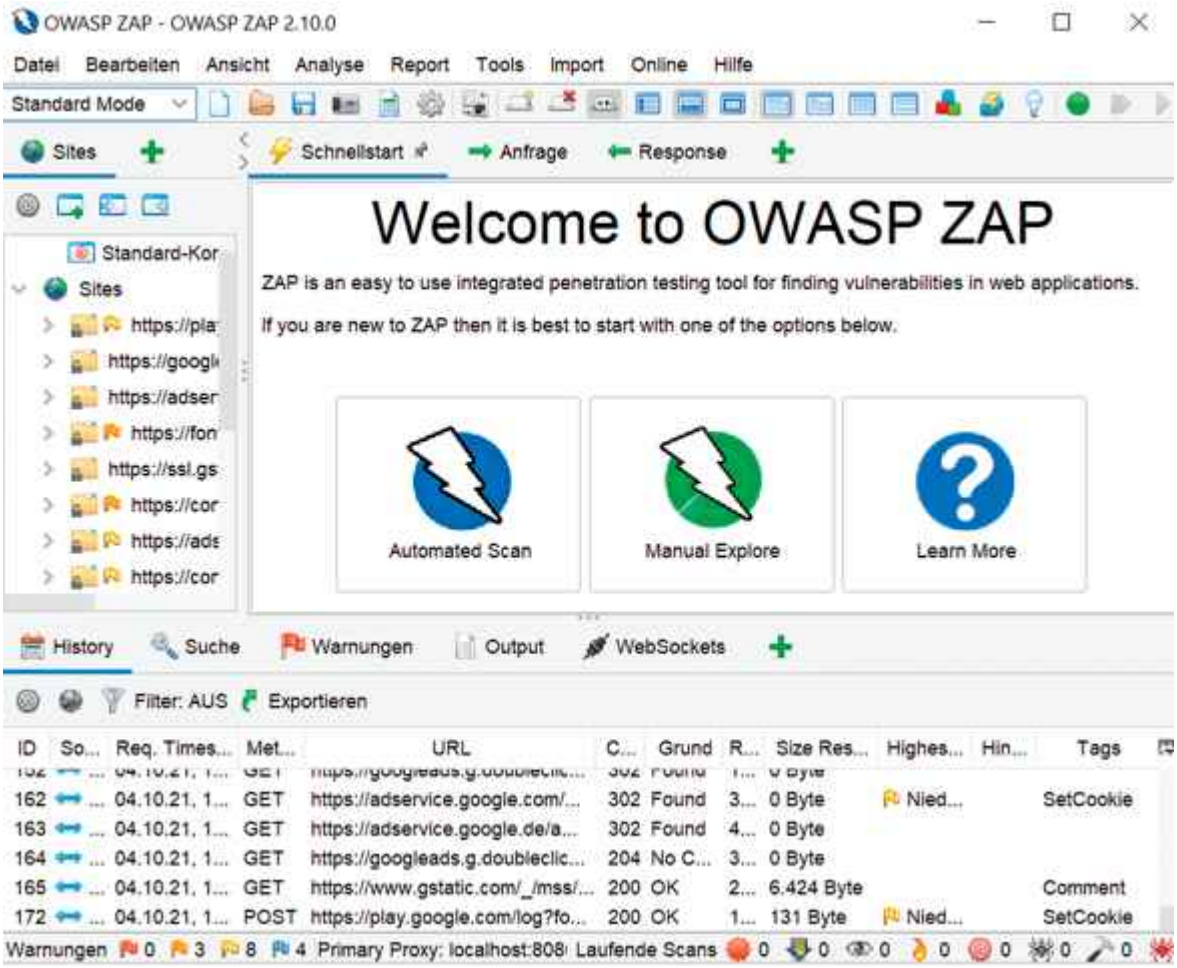
Für einen ersten Funktionstest können Sie die absichtlich anfällige „Wacko Picko“-Website von RasPwn mit SQLmap scannen.

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

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

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

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



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

Browser- und App-Traffic

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

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

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

Gemischtwaren

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

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

zuvor erbeutete Anmeldeinformationen.

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

Fazit

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

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