A

Tools

Dieser Anhang enthält eine Liste mit Hacking-Tools. Einige Tools erlauben die Automatisierung der Erkundung, andere helfen beim Aufspüren von Anwendungen, auf die ein Angriff lohnt. Diese Liste ist nicht vollständig, sondern enthält nur die Tools, die ich häufig nutze oder von denen ich weiß, dass sie regelmäßig von anderen Hackern genutzt werden. Denken Sie immer daran, dass diese Tools nie eigene Beobachtungen oder intuitives Denken ersetzen können. Mein Dank gilt Michiel Prins, Mitgründer von HackerOne, der bei der ersten Version dieser Liste mitwirkte und mir dabei half, diese Tools effektiv zu nutzen, als ich mit dem Hacking begann.

A.1 Web-Proxies

Web-Proxies halten Web-Traffic fest, sodass sie gesendete Requests und empfangene Responses analysieren können. Viele dieser Tools stehen kostenlos zur Verfügung, allerdings bieten die professionellen Versionen zusätzliche Features.

Burp Suite

Die Burp Suite (*https://portswigger.net/burp/*) ist eine integrierte Plattform für Sicherheitstests. Das nützlichste Tool der Plattform ist Burps Web-Proxy, und ich nutze es zu 90 Prozent der Zeit. Wie Sie aus den Bug-Reports in diesem Buch wissen, erlaubt der Proxy es Ihnen, den Traffic zu überwachen, Requests in Echtzeit abzufangen, zu modifizieren und weiterzuleiten. Burp umfasst eine ganze Reihe von Tools, doch die folgenden finde ich besonders erwähnenswert:

- einen anwendungsbezogenen Spider, der Inhalte und Funktionalitäten (passiv oder aktiv) abruft
- ein Web-Scanner zur automatischen Erkennung von Schwachstellen
- ein Repeater zur Manipulation und dem erneuten Senden (Replay) individueller Requests
- Erweiterungen, die die Plattform um zusätzliche Funktionen ergänzen

Burp ist mit eingeschränktem Funktionsumfang kostenlos verfügbar, es gibt aber auch eine Pro-Version im Jahresabo. Ich empfehle, mit der kostenlosen Version zu beginnen, bis man verstanden hat, wie sie funktioniert. Wenn Sie laufend nach Schwachstellen suchen, kann der Kauf der Pro-Version Ihre Arbeit vereinfachen.

Charles

Charles (*https://www.charlesproxy.com/*) ist ein HTTP-Proxy, ein HTTP-Monitor und ein Reverse Proxy, der es Entwicklern erlaubt, sich den HTTP- und SSL-/HTTPS-Traffic anzusehen. Damit können Sie sich Requests, Responses und HTTP-Header (die Cookies und Caching-Informationen enthalten) ansehen.

Fiddler

Fiddler (*https://www.telerik.com/fiddler/*) ist ein weiterer, leichtgewichtiger Proxy, mit dem Sie Ihren Traffic überwachen können. Die stabile Version ist allerdings nur für Windows verfügbar. Die Mac- und Linux-Versionen sind noch Beta, während diese Zeilen geschrieben werden.

Wireshark

Wireshark (*https://www.wireshark.org/*) ist ein Tool zur Analyse von Netzwerkprotokollen, mit dem Sie sich genau ansehen können, was im Netzwerk passiert. Wireshark ist besonders nützlich, wenn Sie Traffic überwachen wollen, der nicht über Burp oder ZAP abgefangen werden kann. Wenn Sie gerade einsteigen, ist die Burp Suite vielleicht die bessere Lösung, wenn die Site nur über HTTP/HTTPS kommuniziert.

ZAP-Proxy

Der OWASP Zed Attack Proxy (ZAP) ist eine freie, Community-basierte Open-Source-Plattform ähnlich Burp. Er steht über *https://www.owasp.org/ index.php/ OWASP_Zed_Attack_Proxy_Project* zur Verfügung. Auch er umfasst eine Reihe von Tools wie Proxy, Repeater, Scanner, Verzeichnis-/Datei-Brute-Forcer und so weiter. Zusätzlich unterstützt er Add-ons, sodass Sie eigene Funktionen integrieren können. Die Website enthält nützliche Informationen für Einsteiger.

A.2 Subdomain-Auflistung

Websites arbeiten häufig mit Subdomains, die man von Hand nur schwer aufspüren kann. Das Brute-Forcing von Subdomains kann Ihnen dabei helfen, zusätzliche Angriffsflächen innerhalb eines Programms zu identifizieren.

Amass

Das OWASP-Tool Amass (*https://github.com/OWASP/Amass*) ermittelt Subdomain-Namen, indem es Datenquellen abfragt, rekursives Brute-Forcing nutzt, Web-Archive durchsucht, Namen permutiert oder ändert und Reverse DNS nutzt. Amass verwendet auch die während der Auflösung gewonnenen IP-Adressen, um assoziierte Netzblöcke und ASNs (Autonomous System Numbers) zu ermitteln. Es verwendet diese Informationen dann, um die Zielnetzwerke abzubilden.

crt.sh

Die Website crt.sh (*https://crt.sh/*) erlaubt es Ihnen, die Transparenz-Logs von Zertifikaten zu durchsuchen, um die mit den Zertifikaten verknüpften Subdomains zu ermitteln. Die Zertifikats-Registrierung kann auch andere Subdomains offenlegen, die eine Site nutzt. Sie können die Website direkt verwenden oder das Tool SubFinder nutzen, das die Ergebnisse von crt.sh verarbeitet.

Knockpy

Knockpy (*https://github.com/guelfoweb/knock/*) ist ein Python-Tool, das eine Wortliste durchgeht, um die Subdomains eines Unternehmens zu identifizieren. Die Identifizierung von Subdomains führt zu einem größeren Testfeld und erhöht so die Chancen, eine Schwachstelle zu finden.

SubFinder

SubFinder (*https://github.com/subfinder/subfinder/*) ist ein in Go geschriebenes Tool zum Aufspüren von Subdomains. Es findet gültige Subdomains über die Verwendung passiver Onlinequellen. Das Programm verwendet eine einfache,

modulare Struktur und ersetzt ein ähnliches Tool namens Sublist3r. SubFinder nutzt passive Quellen, Suchmaschinen, Pastebind, Internet-Archive und so weiter, um Subdomains aufzuspüren. Findet es Subdomains, nutzt es ein Permutationsmodul (das durch aldns inspiriert ist), um Permutationen zu erzeugen, und eine leistungsfähige Brute-Forcing-Engine, um sie aufzulösen. Bei Bedarf kann auch ein reines Brute-Forcing durchgeführt werden. Das Tool lässt sich individuell anpassen, und der Code verfolgt einen modularen Ansatz, der das Einbinden neuer Funktionen erleichtert und Fehler vermeidet.

A.3 Entdeckung (Discovery)

Sobald Sie die Angriffsfläche eines Programms bestimmt haben, besteht der nächste Schritt darin, Dateien und Verzeichnisse aufzulisten. Das hilft dabei, versteckte Funktionalitäten, sensible Dateien, Zugangsdaten und so weiter zu finden.

Gobuster

Gobuster (*https://github.com/OJ/gobuster/*) ist ein Tool zum Brute-Forcing von URIs (Verzeichnissen und Dateien) und DNS-Subdomains. Es unterstützt Wildcards, ist extrem schnell, flexibel, konfigurierbar und einfach zu nutzen.

SecLists

Technisch gesehen ist SecLists (*https://github.com/danielmiessler/SecLists/*) kein Tool, sondern eine Sammlung von Wortlisten, die Sie beim Hacken nutzen können. Die Listen umfassen Benutzernamen, Passwörter, URLs, Fuzzing-Strings, gängige Verzeichnisse/Dateien/Subdomains und so weiter.

Wfuzz

Wfuzz (*https://github.com/xmendez/wfuzz/*) erlaubt es, beliebige Eingaben in beliebige Felder eines HTTP-Requests einzuschleusen. Mit Wfuzz können Sie komplexe Angriffe auf die verschiedenen Komponenten einer Webanwendung starten, etwa auf dessen Parameter, die Authentifizierung, Formulare, Verzeichnisse, Dateien, Header und so weiter. Sie können Wfuzz über entsprechende Plugins auch als Schwachstellen-Scanner nutzen.

A.4 Screenshots

In manchen Fällen ist die Angriffsfläche so groß, dass man nicht jeden Aspekt testen kann. Wenn Sie eine lange Liste von Webseiten oder Subdomains prüfen müssen, können Sie automatische Screenshot-Tools nutzen. Diese Tools erlauben eine visuelle Inspektion von Websites, ohne jede einzelne besuchen zu müssen.

EyeWitness

EyeWitness (*https://github.com/FortyNorthSecurity/EyeWitness/*) kann Screenshots von Webseiten anfertigen, Header-Informationen des Servers bereitstellen und, falls möglich, Standard-Anmeldedaten erkennen. Es eignet sich hervorragend zur Erkennung von Diensten, die auf gängigen HTTP-, oder HTTPS-Ports laufen und kann mit anderen Tools wie Nmap eingesetzt werden, um mögliche Angriffsziele aufzulisten.

Gowitness

Gowitness (*https://github.com/sensepost/gowitness/*) ist ein in Go geschriebenes Utility für Website-Screenshots. Es nutzt Chrome Headless, um Screenshots von Web-Schnittstellen über die Kommandozeile zu erzeugen. Das Projekt wurde durch EyeWitness inspiriert.

HTTPScreenShot

HTTPScreenShot (*https://github.com/breenmachine/httpscreenshot/*) ist ein Tool, um Screenshots und den HTML-Code einer großen Zahl von Websites abzugreifen. HTTPScreenShot akzeptiert IPs als Liste von URLs, von denen Screenshots angelegt werden sollen. Auch ein Brute-Forcing von Subdomains ist möglich. Diese werden dann in die Liste der Screenshot-URLs eingefügt. Die Gruppierung der Ergebnisse erleichtert die anschließende Untersuchung.

A.5 Port-Scanning

Neben dem Aufspüren von URLs und Subdomains müssen Sie auch herausfinden, welche Ports genutzt werden und welche Anwendung der Server ausführt.

Masscan

Masscan (*https://github.com/robertdavidgraham/masscan/*) behauptet, der schnellste Internet-Port-Scanner der Welt zu sein. Es kann das gesamte Internet in weniger als 6 Minuten scannen und überträgt 10 Millionen Pakete pro Sekunde. Er erzeugt Ergebnisse ähnlich Nmap, nur schneller. Darüber hinaus erlaubt Masscan den Scan beliebiger Adress- und Port-Bereiche.

Nmap

Nmap (*https://nmap.org/*) ist ein freies Open-Source-Utility für die Netzwerk-Erkennung und Sicherheitsprüfung. Nmap verwendet IP-Raw-Pakete, um Folgendes zu ermitteln:

- Welche Hosts sind im Netzwerk verfügbar?
- Welche Dienste (samt Name der Anwendung und Version) bieten diese Hosts an?
- Welche Betriebssysteme (und Versionen) laufen auf diesen Hosts?
- Welche Art Paketfilter oder Firewalls werden genutzt?

Die Nmap-Site enthält gute Installationsanweisungen für Windows, Mac und Linux. Neben dem Port-Scanning enthält Nmap Skripte für zusätzliche Funktionen. Ein Skript, das ich häufig verwende, ist `http-enum`, das Dateien und Verzeichnisse von Servern auflistet, nachdem ihre Ports gescannt wurden.

A.6 Erkundung (Reconnaissance)

Nachdem Sie URIs, Subdomains und Ports von Websites gefunden haben, die eine Untersuchung lohnen, müssen Sie etwas über die Technologien erfahren, die verwendet werden, sowie über die anderen Teile des Internet, mit denen sie verbunden sind. Die folgenden Tools helfen Ihnen dabei.

BuiltWith

BuiltWith (*http://builtwith.com/*) hilft beim Fingerprinting verschiedener Technologien, die ein Angriffsziel nutzt. Laut eigenen Angaben können mehr als 18.000 Arten von Internet-Technologien geprüft werden, einschließlich Analytics, Hosting, CMS-Typ und so weiter.

Censys

Censys (*https://censys.io/*) sammelt Daten zu Hosts und Websites über tägliche ZMap- und Zgrab-Scans im IPv4-Adressraum. Leider hat Censys jüngst ein Bezahlmodell eingeführt, das bei groß angelegten Hacks recht teuer ist, doch die kostenlose Variante kann immer noch hilfreich sein.

Google-Dorks

Google-Dorking (*https://www.exploit-db.com/google-hacking-database/*) bezeichnet die Nutzung fortgeschrittener Google-Syntax, um Informationen zu finden, die bei einem Besuch der Website nicht direkt zur Verfügung stehen. Diese Informationen umfassen gefährdete Dateien, Möglichkeiten zum Laden externer Ressourcen und andere Angriffsflächen.

Shodan

Shodan (*https://www.shodan.io/*) ist eine Suchmaschine für das Internet of Things (IoT). Shodan hilft dabei, zu ermitteln, welche Geräte mit dem Internet verbun-

den sind, wo sie sich befinden und wer sie nutzt. Das ist besonders hilfreich, wenn Sie ein potenzielles Angriffsziel erkunden und so viel wie möglich über dessen Infrastruktur erfahren wollen.

What CMS

Mit What CMS (*http://www.whatcms.org/*) können Sie einen URL eingeben und erhalten das CMS (Content-Management-System) zurück, das die Site sehr wahrscheinlich nutzt. Den CMS-Typ einer Site zu ermitteln, kann nützlich sein, weil ...

- das Wissen um das CMS einer Site Ihnen Einblick in die Code-Struktur der Site gibt.
- Sie den Code nach Schwachstellen absuchen und auf der Site testen können, wenn das CMS Open Source ist.
- die Site veraltet und für bekannte Sicherheitslücken anfällig sein könnte.

A.7 Hacking-Tools

Mit Hacking-Tools können Sie nicht nur den Entdeckungs- und Auflistungsprozess automatisieren, sondern auch das Aufspüren von Sicherheitslücken.

Bucket Finder

Bucket Finder (*https://digi.ninja/files/bucket_finder_1.1.tar.bz2*) sucht nach Buckets mit Leserechten und listet alle darin enthaltenen Dateien auf. Es kann auch schnell Buckets aufspüren, die kein Auflisten der Dateien erlauben. Finden Sie solche Buckets, können Sie die AWS-Kommandozeile nutzen wie im Bug-Report »Fehlerhafte S3-Buckets bei HackerOne" auf Seite 214.

CyberChef

CyberChef (*https://gchq.github.io/CyberChef/*) ist das Schweizer Armeemesser der Codierungs- und Decodierungs-Tools.

Gitrob

Gitrob (*https://github.com/michenriksen/gitrob/*) hilft beim Aufspüren möglicherweise sensibler Dateien, die in öffentlichen Repositories auf GitHub abgelegt wurden. Gitrob klont einem Nutzer oder einer Organisation gehörende Repositories bis zu einer konfigurierbaren Tiefe und untersucht dann die Commit-History und Flag-Dateien auf Signaturen, die auf möglicherweise sensible Daten hinweisen. Die Ergebnisse werden in einer Web-Schnittstelle präsentiert, die die Suche und Analyse vereinfacht.

Online Hash Crack

Online Hash Crack (*https://www.onlinehashcrack.com/*) versucht, Passwörter in Hash-Form, WPA-Dumps und verschlüsselten MS-Office-Dateien zu knacken.

sqlmap

Sie können das Open-Source-Penetrations-Tool sqlmap (*http://sqlmap.org/*) nutzen, um SQL-Injection-Schwachstellen zu erkennen und auszunutzen. Die Website führt eine Liste der Features auf, darunter:

- eine Vielzahl von Datenbank-Typen wie MySQL, Oracle, PostgreSQL, MS SQL-Server und andere,
- sechs SQL-Injection-Techniken und
- die Auflistung von Nutzern, Passwort-Hashes, Rechten, Rollen, Datenbanken, Tabellen und Spalten.

XSSHunter

XSSHunter (*https://xsshunter.com/*) hilft beim Aufspüren blinder XSS-Schwachstellen. Nachdem Sie sich bei XSSHunter angemeldet haben, erhalten Sie eine *xss.ht*-Kurz-Domain, die Ihr XSS identifiziert und Ihre Payload vorhält. Greift ein XSS, werden automatisch Informationen gesammelt und eine Benachrichtigung per E-Mail geschickt.

Ysoserial

Ysoserial (*https://github.com/frohoff/ysoserial/*) ist ein Tool zur Generierung von Payloads, die die unsichere Objekt-Deserialisierung von Java ausnutzen.

A.8 Mobile Apps

Zwar wurden die meisten Bugs in diesem Buch über den Webbrowser gefunden, doch manchmal müssen Sie im Rahmen Ihrer Tests auch mobile Anwendungen untersuchen. Indem Sie die Komponenten einer App aufschlüsseln und analysieren, erfahren Sie, wie sie funktioniert und wo ihre Schwachstellen liegen könnten.

dex2jar

dex2jar (*https://sourceforge.net/projects/dex2jar/*), eine Reihe von Mobile-Hacking-Tools, wandelt dalvik-Executables (*.dex*-Dateien) in Java-*.jar*-Dateien um, was das Auditing von Android-APKs deutlich vereinfacht.

Hopper

Hopper (*https://www.hopperapp.com/*) ist ein Reverse-Engineering-Tool, mit dem Sie Anwendungen disassemblieren, dekompilieren und debuggen können. Es ist für das Auditing von iOS-Anwendungen hilfreich.

JD-GUI

JD-GUI (*https://github.com/java-decompiler/jd-gui/*) hilft bei der Untersuchung von Android-Apps. Es handelt sich um ein eigenständiges, grafisches Utility, das Java-Quellcode aus *CLASS*-Dateien erzeugt.

A.9 Browser-Plug-ins

Firefox verfügt über verschiedene Browser-Plug-ins, die in Kombination mit anderen Tools genutzt werden können. Zwar nenne ich hier nur die Firefox-Versionen dieser Tools, doch vergleichbare Tools kann es auch für andere Browser geben.

FoxyProxy

FoxyProxy ist ein fortgeschrittenes Proxy-Management-Add-on für Firefox. Es verbessert die fest in Firefox integrierten Proxy-Fähigkeiten.

User Agent Switcher

User Agent Switcher fügt ein Menü und einen Toolbar-Button in den Firefox-Browser ein, der den Wechsel des User-Agents erlaubt. Mit diesem Feature können Sie bei Angriffen Ihren Browser verschleiern.

Wappalyzer

Wappalyzer hilft bei der Identifikation der Technologien, die eine Site verwendet, zum Beispiel CloudFlare, Frameworks, JavaScript-Bibliotheken und so weiter.