Einstieg in Ethical Hacking

Penetration Testing & Hacking-Tools
für die IT-Security

DIE LESEPROBE

Kapitel 1

Was ist (Ethical) Hacking?

Mit diesem Buch sollten Sie in der Lage sein, Schwachstellen auf Ihren Computer und in Ihrem Netzwerk aufzuspüren und gefundene Schwachstellen zu beseitigen, bevor Cyber-Kriminelle die Möglichkeit haben, diese auszunutzen.

Da der Begriff »Ethik« häufig missverständlich gebraucht wird, schauen wir uns einmal an, wie der Begriff in Wörterbüchern definiert ist:

> *Gesamtheit sittlicher Normen und Maximen, die einer [verantwortungsbewussten] Einstellung zugrunde liegen.*

Diese Definition passt auch sehr gut zu diesem Buch und den hier behandelten professionellen Sicherheitstests und -techniken. Fachleute aus IT- und Datensicherheit sind verpflichtet, die hier vorgestellten Techniken ehrlich und nur dann durchzuführen, wenn sie **die ausdrückliche Erlaubnis der Inhaber der Systeme erhalten haben**.

1.1 Begriffserklärung

Wenn man die Medienberichte verfolgt, ist klar, dass viele bereits die Folgen von Cyber-Angriffen zu spüren bekommen. Deshalb haben viele sicher schon von Hackern und böswilligen Anwendern gehört. Aber um wen handelt es sich bei den Leuten? Was sollten Sie über diese wissen?

Um Missverständnissen in diesem Buch vorzubeugen, definieren wir hier folgende Begriffe:

- **Hacker:** Hier versucht ein externer Angreifer, Computer und sensible Daten anzugreifen, um ein illegales Ziel zu erreichen. Es werden dabei beinahe alle Systeme angegriffen, die als Angriffsziel lohnend sein können.
- **Böswillige Anwender:** Dabei handelt es sich um interne Angreifer, die als berechtigte und »vertrauenswürdige« Anwender von innen heraus Computer und sensible Daten angreifen. Ein böswilliger Anwender greift die Systeme meistens an, um sich zu rächen, aber in einigen Fällen verfolgt er auch illegale Ziele.

  Angreifer können zugleich Hacker als auch böswillige Anwender sein. Es ist einfacher, beide als Hacker zu bezeichnen und ich werde nur dann einen Unterschied zwischen beiden Begriffen machen, wenn wir uns intensiver mit deren Werkzeugen, Techniken und Denkweisen beschäftigen müssen.

- **Ethische Hacker:** Hier handelt es sich um die »Guten«, die Systeme hacken, um ihre Schwachstellen aufzudecken, um Schutzmaßnahmen gegen unberechtigte Zugriffe aufbauen zu können. Zu diesen können IT-Security-Berater als auch internes Personal zählen.

1.2 Was ist ein Hacker?

Wenn wir an einen Hacker denken, dann fällt vielen der typische Computer-Nerd im Kapuzenpullover ein. Doch was ist ein Hacker wirklich?

Die beste Beschreibung, die ich bisher gehört habe, die aber wenig mit Computern zu tun hat, lautet: Ein Hacker ist eine Person, die auf kreative Art und Weise ein Problem löst.

In der ursprünglichen Bedeutung war es noch ein Tüftler im Kontext einer verspielten, selbstbezogenen Hingabe im Umgang mit Technik und einem besonderen Sinn für Kreativität. Jedoch ist der Begriff heute meist negativ behaftet und wir verstehen darunter eine Person, die illegal in Computersysteme eindringt. Diese Person hat Spaß daran, programmierbare Systeme zu erforschen, und geht dabei bis an die Grenzen ihrer Fähigkeiten. Sie liebt die intellektuelle Herausforderung, Hindernisse auf kreative Art und Weise zu überwinden und zu umgehen. Hier versucht die Person mit dem Wissen über technische Geräte sowie das Internet, die Technik zu überlisten, zweckzuentfremden oder zu modifizieren.

Was unterscheidet Programmierer oder Informatiker von Hackern? Es ist nicht leicht, diese Frage zu beantworten, da es keine feste Definition gibt. Programmierer(in) ist ein normaler Job, den man erlernen kann, ohne automatisch ein Hacker oder eine Hackerin zu sein.

Es gibt aber einige Punkte, die Hacker von Programmierern unterscheiden: Hacker probieren neue Dinge aus. Dinge, die nicht dokumentiert sind. Sie experimentieren und testen Software oder Hardware. Sie wissen nicht unbedingt, wie alles funktioniert, und versuchen, die Software oder Hardware über ihre Tests zu verstehen. Programmierer und Programmiererinnen bleiben bei den Systemen, die sie kennen. Hacker versuchen, die Software zu einem Verhalten zu bringen, das ihrem Zweck dient. Sie versuchen, die Ecken zu finden, die nicht dokumentiert sind, was oft Trial-and-Error bedeutet. Hacker haben Freude daran, was bei anderen normalerweise Frust hervorruft. In der Regel fühlen sie sich davon herausgefordert und ruhen selten, bevor sie nicht verstanden haben, was gerade passiert.

Hacker(innen) teilen ihre Erkenntnisse häufig mit der Community, um damit für besseres Verständnis zu sorgen. Sie dokumentieren ihre Schritte, um auch andere auf diesen Punkt zu bringen. Das hilft ihnen dabei, auch über ihre Fähigkeiten hinauszukommen.

Sie können die Hacker aufgrund ihrer Tätigkeit unterschiedlichen Szenen zuordnen: Hardware Hacker, Open Source Software, Security, Hacktivismus, File Sharing und Cracking-Szene. Die Aufzählung ist bestimmt nicht vollzählig. Man hat in der Szene versucht, die illegalen Tätigkeiten von den »guten« Hackern zu trennen. Aus diesem Grund wurde versucht, den Begriff »Cracker« zu etablieren. Aber leider hat er sich nicht durchgesetzt, deshalb müssen wir akzeptieren, dass das Wort »Hacker« ein Sammelbegriff für viele Beschreibungen geworden sind.

Heutzutage wird die Bezeichnung »Hacker« meist missverstanden. Sie klingt in der allgemeinen Sprache negativ, meint aber eigentlich hochversierte Computerfreaks. Es handelt sich um Menschen, die sich mit Computersystemen beschäftigen und zugleich besonders neugierig sind. Es sind Menschen, die Herausforderungen lieben und gerne Neues erlernen. Den Hacker zeichnet es aus, kreativ zu sein, eigene Ideen zu entwickeln, Neues zu schaffen und die eigenen Fertigkeiten möglichst kreativ einzusetzen. Hacker sind bereit, harte Arbeit zu leisten, um ihre Ziele zu erreichen, und teilen ihr Wissen mit ihresgleichen. Das sind eigentlich alles positive Eigenschaften, die sich viele Unternehmen von ihren Mitarbeitern wünschen.

Wie überall gibt es auch unter den Hackern schwarze Schafe. Diese spezielle Gruppierung der Hacker sind die kriminellen Cracker: Es sind jene Freaks, die für das negative Image der Hacker verantwortlich sind. Sie dringen in Netzwerke und Computersysteme ein, stehlen Daten und knacken Passwörter.

1.3 Hackertypen und deren Motivation

Unter dem Begriff »Hacker« werden die guten Hacker in dieselbe Schublade wie die heimlich operierenden Hacker gesteckt. Aus diesem Grund spricht man auch oft von »White Hat«- und »Back Hat«-Hackern. Diese Einteilung stammt aus alten Western-Filmen, in denen die Guten immer weiße und die Bösen immer schwarze Hüte getragen haben. Trotzdem verbinden heutzutage die meisten Menschen etwas Negatives mit dem Begriff »Hacker«.

Hinweis

Viele bösartigen Hacker behaupten, es zum Wohle der Gesellschaft machen und keinen schädigen zu wollen. Achten Sie darauf, einen Sicherheitsbeauftragten nicht mit einem kriminellen Hacker zu verwechseln. Der Sicherheitsbeauftragte hackt in ehrlichen Interessen und entwickelt auch jene Werkzeuge, die uns bei der Arbeit unterstützen. Sie sind sich ihrer Verantwortung bewusst und sorgen dafür, dass ihre Ergebnisse und die Quelltexte ihrer Programme veröffentlicht werden.

1.3.1 Black Hats

Black Hats sind die bösen Hacker. Sie nutzen ihre Fähigkeiten mit krimineller und destruktiver Absicht. Sie dringen illegal in Systeme ein und stehlen Daten oder verschlüsseln diese. Sie erpressen Unternehmen, stehlen Geld oder richten Schaden an. Black Hats verändern auch fremde Software, um einen Kopierschutz aufzuheben oder unbemerkt eine Schadsoftware anzuhängen. Sie stehlen digitale Identitäten, um sich selbst Vorteile zu verschaffen, und stören zudem die Verfügbarkeit von Diensten mittels Denial-of-Service-Angriffen.

1.3.2 White Hats oder Ethical Hacker

White Hats nutzen ihre Fähigkeiten für die Verteidigung von Systemen. Es handelt sich dabei häufig um unabhängige Security-Consultants, die Sicherheitsmaßnahmen und Systeme analysieren und Maßnahmen zur Verbesserung der Sicherheit vorschlagen.

White Hats haben Freude am Hacken von Webseiten, Apps und Programmen. Sie helfen Unternehmen und Personen, alle möglichen Fehler, Schwachstellen und Bugs in ihrer Software zu finden.

1.3.3 Grey Hats

Gray Hats veröffentlichen (un)absichtlich ihre gefundenen Schwachstellen aus bekannten Betriebssystemen und Software im Internet. Die Schwachstellen können von allen, auch den Black Hats, ausgenutzt werden. Für die Unternehmen läuft die Zeit, sie müssen die Schwachstelle rasch schließen, um das Risiko eines erfolgreichen Angriffs zu reduzieren.

Gray Hats sind der Meinung, dass Software- und Hardwarehersteller für die Sicherheit der eigenen Produkte verantwortlich sind, und überlassen es dem Schicksal, ob die von ihnen veröffentlichten Informationen für gute oder schlechte Zwecke eingesetzt werden.

1.3.4 Script Kiddies

Bei den Script Kiddies handelt es sich um Jugendliche, die ein Tool im Netz finden, mit dem sie Unternehmen oder eine Privatperson angreifen und ihre Opfer gezielt zur Weißglut bringen. Selten ist hier das Ziel, Geld zu machen, sondern es geht darum, die eigenen Fähigkeiten auszutesten und das Ziel zu ärgern.

Diese Gruppe war vor allem in den frühen Jahren des Hackings noch weit verbreitet, bildet aber nur noch einen kleinen Teil der Angreifer.

1.3.5 Blue Team & Red Team

Hier handelt es sich um die zwei Seiten der Medaille für den Schutz von IT-Systemen.

Beim Red Team handelt es sich um Penetration Tester, die nach Schwachstellen in den Systemen suchen und so versuchen, in die Systeme einzudringen. Hierzu zählen auch die »Bug-Bounty-Hunter«. Diese Gruppe sucht nach Schwachstellen für Unternehmen im Rahmen eines Bug-Bounty-Programms. Viele Unternehmen, vor allem Software-Hersteller wie Microsoft, Google, Amazon, Twitter & Co., haben Bug-Bounty-Programme, die es erlauben, die Programme auf Schwachstellen zu prüfen.

Das Blue Team bilden die Cyber-Security-Analysten, die die Systeme gegen die Angriffe schützen. Es gibt auch Wettbewerbe, bei denen Blue Teams einen Server mit Demodaten vor dem Red Team schützen. Die Red Teams versuchen dabei, unbemerkt in die Systeme einzudringen.

1.4 Die Rolle des Ethical Hackers

Die Rolle des Ethical Hackers, auch als White Hat Hacker oder Sicherheitsexperte bezeichnet, ist von entscheidender Bedeutung, wenn es um die Sicherheit von IT-Systemen und Netzwerken geht. Im Gegensatz zu böswilligen Hackern, die Schwachstellen ausnutzen, um unbefugten Zugriff zu erlangen und Schaden anzurichten, hat der Ethical Hacker eine völlig andere Zielsetzung. Ethisches Hacken erfolgt in einem professionellen Umfeld mit der Genehmigung der »Opfer«. Seine Hauptaufgabe besteht darin, Sicherheitslücken und Schwachstellen in einem System zu identifizieren, bevor diese von Angreifern ausgenutzt werden können.

Der Ethical Hacker geht dabei in der Regel methodisch vor und es besteht eine gute Chance, die Auswirkungen bösartiger Angriffe bereits im Testbetrieb auszuwerten, mit dem Ziel, noch vor der Produktivstellung neuer Software oder Änderungen in der Netzwerkkonfiguration einen höheren Sicherheitsgrad zu erreichen.

Ein ethischer Hacker stellt im Rahmen eines sogenannten Audits folgende Fragen:

- Was kann ein Angreifer auf dem Zielsystem sehen?
- Welche Server und Geräte sind für ihn sichtbar?
- Welche dieser Geräte sind für ihn erreichbar?
- Wie kann der Angreifer die gewonnenen Informationen gegen das Unternehmen einsetzen?
- Sind seine Versuche und Erfolge in den Systemen nachvollziehbar?
- Welche Systeme sind im Unternehmen zu schützen?

- Gegen wen oder was muss geschützt werden?
- Welche Maßnahmen sind jeweils angemessen?
- Wie hoch ist das Budget, das das Unternehmen für einen ausreichenden Schutz bereitstellen kann?

Es ist die Aufgabe des ethischen Hackers, die Systeme von Unternehmen hinsichtlich der bekannten Cyber-Attacken abzusichern. Da es, wie bekannt ist, keinen 100%igen Schutz gibt, sind Ethical Hacker bemüht, Detect-, Alert- und Log-Mechanismen zu installieren, um eventuelle Angriffe bis zum Angreifer zurück nachvollziehen zu können.

Statt sich auf die Sicherheitsmechanismen von eingekauften Standardsystemen zu verlassen, dringt der Ethical Hacker im Auftrag des Unternehmens in dessen IT-Infrastruktur ein. Genauso hartnäckig wie ein böswilliger Angreifer penetriert der ethische Hacker das Unternehmensnetzwerk und sucht eine Lücke, über die er eindringen kann. Er scannt alle von außen und innen erreichbaren Geräte und versucht, die darauf installierten Betriebssysteme und Dienste zu ermitteln. Sobald er eine Sicherheitslücke gefunden hat, verschafft er sich einen Zugriff zu dem betroffenen System und hinterlässt dort als Beweis eine Nachricht für den Auftraggeber.

Bei diesem Vorgehen, das man auch als »Penetrationstest« bezeichnet, arbeitet der ethische Hacker vorsichtig und achtet darauf, produktiv laufende Dienste nicht zu beeinträchtigen. Angriffe, die auf die Abschaltung bestimmter Dienste abzielen, werden dabei nicht auf produktiven Systemen, sondern ausschließlich auf Testsystemen durchgeführt. Buffer-Overflows-, Denial-of-Service-(Dos-)Angriffe oder Wurmattacken werden dabei in einem abgeschotteten Testnetzwerk durchgeführt. Um aber die gleichen Bedingungen zu schaffen wie auf den produktiven Systemen, muss die gleiche Hardware und Netzwerkkonfiguration eingesetzt werden; das betrifft Firewalls, Router, Switches, Datenbanken, Webserver, Mail-Server, FTP-Server und vieles mehr.

Darüber hinaus hat ein Ethical Hacker folgende Aufgaben:

- **Autorisierte Sicherheitstests**

  Der Ethical Hacker führt Sicherheitstests nur mit ausdrücklicher Erlaubnis des Eigentümers oder Verwalters des Systems oder Netzwerks durch. Bevor ein Sicherheitstest durchgeführt wird, muss der Ethical Hacker einen schriftlichen Auftrag erhalten, der die Ziele, den Umfang und die Bedingungen des Tests festlegt. Die Autorisierung gewährleistet, dass der Ethical Hacker rechtmäßig handelt und keine rechtlichen Konsequenzen befürchten muss.

- **Identifizierung von Schwachstellen**

  Die Hauptaufgabe des Ethical Hackers besteht darin, Schwachstellen und Sicherheitslücken in einem System oder Netzwerk zu identifizieren. Hierbei

setzt er verschiedene Methoden und Techniken ein, wie zum Beispiel Penetrationstests, Vulnerability Scans und Code Reviews. Durch die Identifizierung von Schwachstellen kann der Ethical Hacker dem Unternehmen dabei helfen, proaktiv auf potenzielle Bedrohungen zu reagieren und entsprechende Sicherheitsmaßnahmen zu ergreifen.

- **Vermeidung von Sicherheitsvorfällen**

  Indem der Ethical Hacker Sicherheitslücken aufdeckt, trägt er maßgeblich dazu bei, Sicherheitsvorfälle zu verhindern. Durch die Behebung von Schwachstellen, bevor sie von böswilligen Hackern ausgenutzt werden können, schützt der Ethical Hacker das Unternehmen vor finanziellen Verlusten, Reputationsrisiken und rechtlichen Konsequenzen.

- **Beratung und Empfehlungen**

  Nach Abschluss eines Sicherheitstests erstellt der Ethical Hacker einen detaillierten Bericht mit den identifizierten Schwachstellen und Sicherheitslücken. Dieser Bericht enthält auch Empfehlungen und Vorschläge, wie die Sicherheit des Systems verbessert werden kann. Der Ethical Hacker fungiert somit als Berater für das Unternehmen und unterstützt es dabei, eine effektive Sicherheitsstrategie zu entwickeln und umzusetzen.

- **Sensibilisierung und Schulung**

  Der Ethical Hacker trägt auch zur Sensibilisierung und Schulung der Mitarbeiter bei. Durch Schulungen und Workshops können die Mitarbeiter für die Bedeutung der IT-Sicherheit sensibilisiert werden und lernen, wie sie sich vor Phishing-Angriffen, Social Engineering und anderen Sicherheitsbedrohungen schützen können.

- **Gesetzliche Aspekte und Ethik**

  Der Ethical Hacker muss sich strikt an ethische Richtlinien und gesetzliche Bestimmungen halten. Er darf nur autorisierte Tests durchführen und muss sicherstellen, dass seine Aktivitäten den geltenden Gesetzen und Vorschriften entsprechen. Der Ethical Hacker hat eine ethische Verpflichtung, die Privatsphäre und die Daten des Unternehmens zu respektieren und vertrauliche Informationen vertraulich zu behandeln.

Zusammenfassend lässt sich sagen, dass die Rolle des Ethical Hackers von großer Bedeutung für die Sicherheit von IT-Systemen und Netzwerken ist. Durch die Identifizierung von Schwachstellen und Sicherheitslücken trägt der Ethical Hacker maßgeblich dazu bei, Sicherheitsvorfälle zu verhindern und das Unternehmen vor finanziellen Schäden und Rufverlust zu schützen. Die enge Zusammenarbeit zwischen dem Ethical Hacker und dem Unternehmen ist unerlässlich, um eine effektive Sicherheitsstrategie zu entwickeln und umfassende Schutzmaßnahmen umzusetzen. Ethical Hacking ist somit ein unverzichtbarer Bestandteil eines ganzheitlichen Sicherheitskonzepts.

Es ist also durchaus möglich, dass Hacking ethisch ist!

Für viele mag es nach einem Widerspruch klingen, aber es ist eine ausgezeichnete Methode, sich gegen bösartige Angriffe abzusichern. Es schafft eine solide Basis für mehr Sicherheit, wenn man sich nicht auf die Funktionen der eingekauften Systeme verlässt, sondern die eigene Infrastruktur hinterfragt und ausreichend testet. Angreifer interessieren sich meistens nicht für das Netzwerk eines bestimmten Unternehmens, auf das sie es abgesehen haben: Sie scannen das Internet nach ihnen bekannten Schwachstellen ab und greifen dort an, wo ein schneller Erfolg mit wenig Aufwand möglich ist.

Der beste Weg, sein Netzwerk vor Hackern zu schützen, ist, selbst wie ein Hacker zu denken.

1.4.1 Hacker-Ethik

Ein Hacker, der mit einem ausdrücklichen Auftrag der Verantwortlichen eines Unternehmens arbeitet, um das Unternehmen vor Angriffen zu schützen, hat sich ethisch korrekt zu verhalten. Das bedeutet, er schadet dem Unternehmen nicht und stiehlt auch keine Informationen. Sein Anliegen ist es, die Integrität und Vertrauenswürdigkeit der Systeme eines Unternehmens zu festigen.

Bei der professionellen Durchführung von Sicherheitstests müssen ethische Hacker daher die folgenden Regeln einhalten.

Ethisch arbeiten

Das bedeutet vor allem, sich an professionellen Moralvorstellungen und Prinzipien zu orientieren, unabhängig davon, ob es sich um Tests an eigenen Systemen oder Auftragsarbeiten handelt. Die Unternehmensziele müssen dabei unterstützt werden. Dazu zählt vor allem, dass Ergebnisse immer rückhaltlos vorgelegt werden, auch wenn es für Sie ein Nachteil sein kann.

Der oberste Grundsatz lautet immer Vertrauenswürdigkeit. Diese stellt auch die beste Möglichkeit dar, um Mitarbeiter auf Dauer vom Sicherheitsprogramm zu überzeugen. Ein Datenmissbrauch ist ein absolutes No-Go. So würden nur Black-Hat-Hacker agieren.

Achtung der Privatsphäre

Sie müssen die gesammelten Daten mit allergrößtem Respekt behandeln. Alles, was Sie bei Ihren Tests erfahren, muss privat bleiben. Dazu zählen Protokolldateien von Webanwendungen, Kennwörter im Klartext, aber auch persönliche Daten. Schnüffeln Sie niemals in vertraulichen Firmendaten oder im Privatleben der Mitarbeiter des getesteten Unternehmens herum.

Tipp

Binden Sie immer andere in den Prozess mit ein und sorgen Sie für Zeugen. Wenn Sie selbst beaufsichtigt werden, sorgt das vor allem für mehr Vertrauen.

Bringen Sie keine Systeme zum Absturz

Der größte Fehler, der beim Hacken von Systemen auftritt, besteht darin, Systeme, die eigentlich geschützt werden sollten, versehentlich zum Absturz zu bringen. Das passiert vor allem bei schlechter Planung. Häufig werden die Möglichkeiten und Grenzen sowie der Nutzen der verwendeten Werkzeuge und Techniken nicht gut genug verstanden.

Die Wahrscheinlichkeit ist nicht hoch, aber durch das Testen können für die Systeme DoS-Bedingungen entstehen. Das geschieht vor allem dann, wenn zu viele und zu schnell Tests ausgeführt werden. Es kann dann zu Systemausfällen, Beschädigung von Daten, Systemneustarts und Ähnlichem kommen. Häufig kommt es beim Testen von Webseiten und -anwendungen vor.

Es kann auch passieren, dass Sie Konten versehentlich dauerhaft oder vorübergehend sperren, indem Sie jemanden veranlassen, Passwörter zu ändern, ohne dass dieser die Konsequenzen derartiger Situationen erkennt. Seien Sie immer vorsichtig und gehen Sie mit gesundem Menschenverstand an Ihre Aufgabe heran.

1.4.2 Ethical Hacking vs. Auditierung

Häufig wird Ethical Hacking mit einer Sicherheitsüberprüfung (Auditierung) verwechselt, aber es gibt hierbei Unterschiede. Bei einem Audit vergleicht man Sicherheitsrichtlinien eines Unternehmens mit den aktuell gültigen Standards. Ein Audit wird durchgeführt, um zu überprüfen, dass es Sicherheitskontrollen gibt, dabei wird üblicherweise ein risikobasierter Ansatz verfolgt, das heißt, dass Sie sich mit allen Risiken der Systeme auseinandersetzen und diese entsprechend bewerten. Bei Sicherheitsaudits werden oft auch Geschäftsabläufe überdacht, wobei die Abläufe nicht unbedingt technisch ausgerichtet sein müssen, sondern einfach nur auf Sicherheitsfragen basieren.

Beim Ethical Hacking konzentriert man sich auf potenziell nutzbare Schwachstellen. Dabei wird geprüft, ob Sicherheitskontrollen effektiv sind oder zumindest überhaupt existieren. Ethical Hacking kann einerseits sehr technisch sein, andererseits auch auf niedrigem technischem Niveau ablaufen. Auch wenn hier formale Vorgehensweisen verfolgt werden, sind diese tendenziell weniger strukturiert als bei formalen Sicherheitsaudits. Bei Unternehmensaudits (z.B. für die Zertifizierung ISP 9001 oder 27001) sollten Sie darüber nachdenken, die hier vorgestellten Techniken des Ethical Hacking auch im Auditierungsprozess einzubinden.

1.5 Wie werde ich ein Hacker oder eine Hackerin?

Um diese Frage hier im Buch auch beantworten zu können, habe ich sie in unterschiedliche Suchmaschinen eingegeben. Bei der Suche stellten sich immer drei Hauptthemen heraus:

- Grundlegende Fertigkeiten des Hackens erwerben
- Wie ein Hacker denken
- Respekt verdienen

Der erste Punkt ist leicht abzuhandeln, es ist das Grundwissen, das man sich aneignen muss. Hierbei handelt es sich vor allem um IT-Grundlagen. Dieses Wissen lässt sich auch abseits der bekannten Wege wie Ausbildung erlangen. Es ist ein wichtiger Bestandteil dieses Buches: Wie bekomme ich dieses Wissen aus dem Internet?

Ein Teil dieser Grundlagen sind:

- Verstehen, wie der Computer funktioniert
- Betriebssysteme verstehen
- Ein gutes Betriebssystem beherrschen – in der Regel Linux
- Verstehen, wie logische Abläufe funktionieren
- Programmabläufe verstehen
- Programmieren lernen
- Verstehen, wie man mit verschiedenen Datenstrukturen umgeht
- Datenbanken verstehen
- Wissen, wie Netzwerke funktionieren
- Wissen, wie das Internet funktioniert

Beim Thema, wie ein Hacker zu denken, wird es schwieriger. Es geht hierbei oft darum, sich kreative Lösungen zu überlegen oder Dinge zu verbinden, die nicht offensichtlich zusammengehören. Diese Fertigkeit steigt erst mit den technischen Fähigkeiten.

Der dritte Punkt »Respekt verdienen« ist schwerer zu erklären. Es ist hiermit nicht gemeint, ein möglichst cooler Hacker zu sein, wie es im Script-Kiddie-Bereich durchaus üblich ist. Es geht nicht um den Hack selbst, sondern um Sie als Person. Aufrichtig sein, zuhören und lernen, Empathie und Hilfe anbieten, andere respektieren und sich deren Respekt verdienen. Dabei handelt es sich um keine Einbahnstraße.

Dieses Buch, das Internet und andere Hacker und Hackerinnen sind ein guter Startpunkt, um Wissen zu sammeln, herauszufinden, was Sie besonders interessiert, und etwas damit anzufangen.

Ich möchte Sie darauf hinweisen, dass die meisten Dokumentationen auf Englisch verfasst sind, daher ist es empfehlenswert, Englisch zu können. Einzelne Fachbegriffe sind schnell nachgeschlagen, aber ohne technischen Wortschatz wird es fast unmöglich.

Tipp

Sollten Sie darüber nachdenken, für Ihre Kunden ethisch zu hacken und Tests durchzuführen, oder wenn Sie Ihre Referenzen und Leistungsnachweise um ein zusätzliches Zertifikat erweitern wollen, können Sie im Rahmen des EC-Council[1] den Certified Ethical Hacker (C|EH) erwerben oder bei Offensive Security[2] eine Zertifizierung, z.B. OSCP, machen.

1.6 Informationen zu den Tools sammeln

Grundlagen sind sehr wichtig, um das gesamte Zusammenspiel der Komponenten zu verstehen, seien es nun die Netzwerkkomponenten innerhalb der zu testenden Infrastruktur oder die der eingesetzten Tools. Generell ist die IT-Welt sehr komplex, darum spezialisieren sich viele auf einzelne Themenbereiche. Beim Hacken ist es sinnvoll, ein Generalist zu sein und ein breites Spektrum zu erlernen, aber nur, so weit es auch benötigt wird. Beim Hacking werden aber auch ganz andere Fähigkeiten notwendig. Es ist wichtig, dass Sie Informationen schnell finden sowie abstrakte oder neue Konzepte schnell verstehen und umsetzen können. Glücklicherweise haben wir das Internet zur Verfügung.

Zwei der wichtigsten Werkzeuge sind ein Browser und eine Suchmaschine. Dabei ist es egal, welche Suchmaschine benutzt wird, datenschutzfreundliche Alternativen wie DuckDuckGo liefern ähnliche Ergebnisse wie Google. Welche Suchmaschine Sie nutzen, ist das Ergebnis des Abwägens Ihrer persönlichen Wünsche.

Da viele Suchergebnisse, die wir uns erarbeitet haben, früher oder später nicht mehr erreichbar sind, empfiehlt es sich, eine persönliche Wissensdatenbank anzulegen. Das bedeutet, Sie speichern sich gute Erklärvideos, Artikel oder PDFs offline ab. Gute Artikel, Schaubilder oder Texte kopiere ich entweder direkt heraus oder drucke mir die Webseite als PDF aus. Die Druckansicht ist meistens auch schöner, übersichtlicher und ohne Werbung.

Da nicht bekannt ist, wie lange URLs noch existieren, werde ich in diesem Buch darauf verzichten, diese mit Ihnen zu teilen. Aber egal, nach welchen Begriffen ich gesucht habe, ich habe immer die gleichen oder ähnliche Inhalte gefunden.

1 https://www.eccouncil.org/
2 https://www.offensive-security.com/

Es gibt viele Blogartikel im Internet, die einzelne Themen gut erklären, aber die besten Quellen sind häufig die offiziellen Dokumentationen oder Spezifikationen, danach kommen die Wikis und Stackoverflows. Sie können sich dort gerne die eine oder andere Idee abschauen, aber Sie sollten sie immer noch einmal überprüfen, bevor Sie etwas übernehmen.

Es gibt viele Fachbücher als Open-Book-Projekt zum Herunterladen. Diese sind zum Nachschlagen auch passend, aber nur eine praktische Anleitung erklärt Ihnen die Zusammenhänge. Solche Anwendungsbeispiele lassen sich als »how to« oder »tutorial« finden.

Wenn Sie sich für ein Tool entschieden haben, können Sie auch speziell nach Bedienungsanleitungen, Blogposts und Tutorials für dieses Tool suchen, die Sie dann für Ihren Lernprozess ebenfalls dokumentieren und speichern sollten. Es gibt neben den größeren Dokumentationen häufig auch Programm-Cheat-Sheets, nach denen Sie suchen können. Dabei handelt es sich um kleine Spickzettel, die oft benutzte Beispiele oder Funktionen dokumentieren. Sie können sich auch eigene Cheat Sheets anlegen, falls es keine oder keine guten gibt, die Ihren Bedürfnissen entsprechen.

Um einen schnellen Einstieg in ein Thema zu haben, gehe ich immer gleich vor:

- Einen groben Überblick über das Thema verschaffen
- Dokumentationen lesen
- Beispiele suchen
- Prototypen entwickeln bzw. testen/üben

1.7 Richtlinien, Compliance und regulatorische Aspekte

Sollte ethisches Hacken ein Bestandteil Ihres IT-Risikomanagements werden, dann benötigen Sie unbedingt schriftliche Richtlinien für Ihre Sicherheitstests. Diese Richtlinien beschreiben,

- welche Art von ethischem Hacken ausgeführt wird,
- welche Systeme (Server, Webanwendungen, Laptops und so weiter) berücksichtigt werden und
- wie oft die Prüfung vorgenommen wird.

Sie sollten auch darüber nachdenken, eine Dokumentation der jeweils verwendeten Testwerkzeuge anzulegen, in der diese beschrieben und die Termine für die regelmäßigen Tests Ihrer Systeme vorgegeben werden. So können Sie z.B. vorgeben, dass externe Systeme vierteljährlich und interne Systeme halbjährlich getestet werden müssen.

Ihre eigenen Richtlinien schreiben vor, wie mit Sicherheitstest in Ihrem Unternehmen umgegangen wird, aber vergessen Sie nicht, dass Sie auch Gesetze berücksichtigen müssen, die speziell das Unternehmen betreffen. Diese erfordern eine ständige Anpassung der eigenen Sicherheitsanforderungen. Dadurch, dass Ihr ethisches Hacken den jeweiligen Vorgaben folgt und an die staatlichen Anforderungen angepasst wird, lässt sich Ihr eigenes Programm gewaltig aufwerten.

1.8 Warum sich selbst hacken?

Um einen Dieb zu fangen, muss man wie ein Dieb denken! Das ist auch die Grundlage des ethischen Hackens. Es ist extrem wichtig, die Feinde zu kennen. Das Gesetz des Durchschnitts (je mehr Möglichkeiten existieren, desto höher die Wahrscheinlichkeit eines erfolgreichen Treffers) arbeitet der Sicherheit entgegen. Mit der steigenden Anzahl der Hacker mit ständig wachsendem Wissen und der immer größer werdenden Zahl der Schwachstellen werden eines Tages wohl alle Computersysteme und Anwendungen irgendwie gehackt oder zumindest gefährdet. Es ist wichtig, die eigenen Systeme vor Angreifern zu schützen, und zwar nicht nur jene, die bereits bekannt sind. Mit Kenntnis der Tricks der Hacker können Sie die wirkliche Verletzbarkeit und Angreifbarkeit Ihrer Systeme ermitteln.

Hacken nutzt schlechte Sicherheitsverfahren und offene Schwachstellen aus. Firewalls, Verschlüsselung und Kennwörter können ein falsches Gefühl von Sicherheit vortäuschen. Die Sicherheitssysteme konzentrieren sich häufig nur auf die Schwachstellen der obersten Ebene wie grundlegende Zugangskontrolle, ohne die Arbeitsweise von Hackern zu berücksichtigen. Ethisches Hacken ist die einzige Möglichkeit, um die eigenen Systeme gegen Angriffe zu wappnen. Wenn Sie die Schwachstellen nicht kennen, ist es nur eine Frage der Zeit, bis diese ausgenutzt werden.

Wichtig ist, dass Sie Ihre Fähigkeiten, wie jeder Hacker, erweitern. Um die Systeme wirksam schützen zu können, müssen Sie wie Hacker denken und arbeiten. Als Ethical Hacker müssen Sie wissen, welche Tools zur Verfügung stehen und wie die Angriffe wirksam zu stoppen sind. Sobald Sie wissen, wonach Sie suchen müssen und wie Sie entsprechende Informationen nutzen, ist es für Sie ein Kinderspiel, die Bemühungen von Hackern zu durchkreuzen.

Hinweis

Sie können und müssen Ihre Systeme nicht vor allem schützen, da dies unmöglich ist. Wichtig ist der Schutz Ihrer Systeme vor bekannten Schwachstellen und den üblichen Angriffen, was in vielen Organisationen zu den am meisten übersehenen Schwachstellen zählt.

Je mehr Möglichkeiten Sie ausprobieren und je intensiver Sie ganze Systeme und nicht einzelne Geräte testen, desto wahrscheinlicher wird es, Schwachstellen zu entdecken, die Ihre kompletten Systeme gefährden.

Übertreiben Sie es aber nicht mit dem ethischen Hacken. Es ist nur wenig sinnvoll, Ihr System auch vor den unwahrscheinlichsten Angriffen zu schützen. Es ist nicht notwendig, dass Sie sich Gedanken über den Schutz eines Webservers machen, wenn Sie keinen internen Webserver betreiben. Es reicht, wenn Sie den Webzugriff auf das Notwendigste beschränken.

Zielsetzung für das ethische Hacken:

- Legen Sie Prioritäten für Ihre Systeme fest, um die Anstrengungen auf das Wichtige zu konzentrieren.
- Hacken Sie die Systeme, ohne selbst Schaden anzurichten.
- Weisen Sie auf Schwachstellen hin und weisen Sie nach, dass diese missbraucht werden können.
- Beseitigen Sie die Schwachstellen und sichern Sie Ihre Systeme besser.

1.9 Vorgehensweise und Methodik im Ethical Hacking

Das Ethical Hacking ist ein systematischer Prozess, der darauf abzielt, Schwachstellen und Sicherheitslücken in einem System oder Netzwerk zu identifizieren und zu beheben. Eine gut durchdachte Vorgehensweise und Methodik sind entscheidend, um effektive und umfassende Sicherheitstests durchzuführen. In diesem Abschnitt werde ich die wichtigsten Schritte und Phasen im Ethical-Hacking-Prozess erläutern.

1. **Informationsbeschaffung und Planung:** Der erste Schritt in jedem Ethical-Hacking-Projekt ist die Informationsbeschaffung und Planung. Hierbei werden Informationen über das Zielunternehmen oder die Zielumgebung gesammelt. Dies umfasst eine gründliche Recherche über das Unternehmen, seine IT-Infrastruktur, Mitarbeiter und öffentlich verfügbare Informationen. Basierend auf diesen Erkenntnissen wird ein detaillierter Plan für den Sicherheitstest erstellt, der die Ziele, den Umfang, die Methoden und die Zeitrahmen des Tests festlegt.
2. **Footprinting und Scanning**: In dieser Phase werden verschiedene Techniken wie Port-Scanning, Netzwerk-Scanning und Footprinting eingesetzt, um Informationen über die Zielumgebung zu sammeln. Durch das Scannen des Netzwerks werden offene Ports, erreichbare Hosts und potenzielle Schwachstellen identifiziert. Beim Footprinting werden Informationen über die Zielorganisation, ihre Subnetze, DNS-Informationen und andere relevante Daten ermittelt.

3. **Enumeration und Schwachstellenermittlung:** Nachdem relevante Informationen gesammelt wurden, beginnt die Phase der Enumeration und Schwachstellenermittlung. Hierbei werden gezielt Informationen über Benutzer, Ressourcen und Dienste im Netzwerk gesammelt. Durch diese Phase können mögliche Schwachstellen und Sicherheitslücken identifiziert werden, die ausgenutzt werden könnten, um unbefugten Zugriff zu ermöglichen.
4. **Exploitation und Penetration:** In dieser Phase werden identifizierte Schwachstellen und Sicherheitslücken ausgenutzt, um Zugriff auf das System oder Netzwerk zu erhalten. Ethical Hacker verwenden hierbei verschiedene Exploits und Hacking-Tools, um Schwachstellen zu überwinden und in das System einzudringen. Es ist wichtig zu betonen, dass Ethical Hacker ausschließlich autorisierte Exploits verwenden und nur so weit gehen, wie es für den Sicherheitstest notwendig ist.
5. **Post-Exploitation und Privilege Escalation:** Nachdem Zugriff auf das System erlangt wurde, erfolgt die Post-Exploitation-Phase. Hierbei versuchen Ethical Hacker, ihre Privilegien im System zu eskalieren und weitere Informationen zu sammeln. Ziel ist es, langfristigen Zugriff auf das System zu erhalten, um weitere Sicherheitslücken zu identifizieren und Schwachstellen zu beheben.
6. **Dokumentation und Berichterstattung:** Eine gründliche Dokumentation und Berichterstattung sind ein wesentlicher Bestandteil des Ethical-Hacking-Prozesses. Alle durchgeführten Schritte, identifizierten Schwachstellen, ergriffenen Maßnahmen und Ergebnisse sollten genau protokolliert werden. Ein detaillierter Bericht wird erstellt, der die Schwachstellen, die Auswirkungen und mögliche Gegenmaßnahmen beschreibt. Dieser Bericht wird dem Auftraggeber präsentiert, der dann die notwendigen Sicherheitsmaßnahmen ergreifen kann.
7. **Nachverfolgung und Nachprüfung:** Nach Abschluss des Ethical-Hacking-Tests ist es wichtig, den Prozess zu überprüfen und die durchgeführten Maßnahmen zu bewerten. Sicherheitsexperten sollten den Erfolg des Tests bewerten, um sicherzustellen, dass alle Schwachstellen behoben wurden und das System ausreichend geschützt ist. Gegebenenfalls können weitere Tests durchgeführt werden, um sicherzustellen, dass die empfohlenen Sicherheitsmaßnahmen effektiv sind.

Abschließend ist zu betonen, dass die Vorgehensweise und Methodik im Ethical Hacking flexibel sein sollten, um den spezifischen Anforderungen jedes Projekts gerecht zu werden. Ein strukturierter und gut geplanter Ansatz ist entscheidend, um umfassende und aussagekräftige Sicherheitstests durchzuführen. Ethical Hacker müssen in der Lage sein, sich den Gegebenheiten und Herausforderungen jedes einzelnen Projekts anzupassen und gleichzeitig sicherzustellen, dass sie alle relevanten Aspekte abdecken.

Im Ethical Hacking sind Transparenz und Zusammenarbeit von entscheidender Bedeutung. Ethical Hacker sollten immer in enger Abstimmung mit dem Auftrag-

geber arbeiten, um die Ziele des Sicherheitstests zu verstehen und sicherzustellen, dass alle Tests autorisiert und im Einklang mit den Unternehmensrichtlinien durchgeführt werden. Die Sicherheit des Systems steht immer im Vordergrund, und daher müssen Ethical Hacker äußerste Sorgfalt walten lassen, um potenzielle Schäden zu vermeiden.

Ein weiterer wichtiger Aspekt ist die kontinuierliche Verbesserung des Ethical-Hacking-Prozesses. Ethical Hacker sollten immer auf dem neuesten Stand bleiben, was Angriffstechniken, Sicherheitslücken und Gegenmaßnahmen betrifft. Die Sicherheitslandschaft ändert sich ständig, und daher ist es entscheidend, dass Ethical Hacker ihre Fähigkeiten und Kenntnisse regelmäßig aktualisieren und erweitern.

Ethical Hacking ist nicht nur ein einmaliger Sicherheitstest, sondern ein kontinuierlicher Prozess, der dazu dient, die Sicherheit des Systems langfristig zu gewährleisten. Unternehmen und Organisationen sollten Ethical Hacking als wichtigen Bestandteil ihres Sicherheitskonzepts betrachten und regelmäßige Sicherheitstests durchführen, um Schwachstellen zu identifizieren und zu beheben, bevor sie von Angreifern ausgenutzt werden können.

1.10 Gefahren verstehen

Es ist eines, zu verstehen, dass Systeme von Hackern weltweit und böswilligen Benutzern im eigenen Büro angreifbar sind. Aber es ist etwas anderes, zu wissen, dass es verschiedene Angriffsmöglichkeiten gibt. Hier werde ich einige der bekanntesten Angriffsmöglichkeiten vorstellen.

Es ist wichtig zu wissen, dass viele Schwachstellen im Bereich der Datensicherheit allein betrachtet nicht bedenklich sind, wenn aber mehrere gleichzeitig ausgenutzt werden, können diese die Systeme schwer gefährden. Die Windows-Standardkonfiguration gemeinsam mit schwachen Administrator-Kennwörtern von SQL-Servern oder drahtlos verwaltete Netzwerkserver allein stellen noch nicht unbedingt ein größeres Sicherheitsrisiko dar. Wenn Hacker aber diese verschiedenen Schwachstellen gleichzeitig ausnutzen, so gelangen sie möglicherweise an sensible Daten und mehr.

Vorsicht

Komplexität ist ein Feind der IT-Sicherheit. Die Zahl der Schwachstellen und der Angriffe nimmt immer mehr zu. Gründe dafür sind vor allem Cloud-Computing und soziale Netzwerke. Gemeinsam mit der Virtualisierung führt das zu äußerst komplexen modernen IT-Umgebungen. Je mehr Systeme zusammenspielen, desto komplexer wird die Umgebung. Man darf hier nicht vergessen, die Auswirkungen von einzelnen Sicherheitslücken auf das Gesamtgefüge zu betrachten.

1.10.1 Nicht-technische Angriffe

Sie haben sicher schon den Begriff »Exploit« gehört. Dabei handelt es sich um Programme, die Sicherheitslücken in einem Computersystem ausnutzen. Die wohl größte Schwachstelle sind Menschen – Endbenutzer und sogar Sie selbst –, die zu einem bestimmten Verhalten bewegt werden, um z.B. über Phishing-Mails Exploits herunterladen. Diese Angriffe werden »Social Engineering« genannt. In Kapitel 10 werden Sie mehr über Social Engineering erfahren.

Es gibt auch Angriffe auf IT-Systeme auf physischer Ebene. Hacker brechen in Gebäude, Computerräume oder andere Bereiche ein, um an wichtige Daten zu gelangen, indem sie Computer, Server und andere wertvolle Geräte stehlen. Zu diesen Angriffen zählt auch das sogenannte »Dumpster Diving« (übersetzt: »Mülltauchen«), also das Durchwühlen von Mülleimern nach wertvollen Daten (Kennwörtern, Netzwerkdiagrammen und anderen Informationen).

1.10.2 Angriffe auf das Netzwerk

Es ist meistens leicht, die Infrastruktur von Netzwerken anzugreifen, weil diese vielfach über das Internet weltweit erreichbar sind. Die Arten dieser Angriffe:

- Verbindung mit einem Netzwerk über einen ungesicherten drahtlosen Zugriffspunkt, der hinter einer Firewall hängt
- Die Schwächen von Netzwerkprotokollen wie TCP/IP oder SSL (Secure Sockets Layer) ausnutzen
- Ein Netzwerk mit zu vielen Anforderungen überlasten, was zu Dienstblockaden und damit der Unerreichbarkeit von Diensten für rechtmäßige Benutzer führt (DoS – Denial of Service)
- In einem Netzwerk einen Netzwerkanalysator installieren und alle Pakete, die durch das Netzwerk reisen, abfangen und auf vertrauliche Informationen im Klartext untersuchen

1.10.3 Angriffe auf Betriebssysteme

Das Lieblingsziel von Hackern ist das Betriebssystem. Der Grund liegt darin, dass alle Computer ein Betriebssystem benötigen und diese für viele Exploits anfällig sind.

Gelegentlich werden auch seltene Betriebssysteme verwendet wie das reichlich alte Novell NetWare oder OpenBSD, die sicherer wirken als andere, aber doch auch Schwachstellen aufweisen. Hacker greifen natürlich lieber verbreitete Betriebssysteme wie Windows, Linux oder macOS an, da deren Schwachstellen bekannt sind und die Auswahl der Ziele größer ist.

Beispiele für die Angriffe sind:

- Ausnutzung von Schwachstellen aufgrund fehlender Updates
- Angriffe auf Authentifizierungssysteme der Betriebssysteme
- Aushebeln von Sicherheitsfunktionen der entsprechenden Dateisysteme
- Knacken von Kennwörtern und schwachen Verschlüsselungsimplementierungen

1.11 Zusammenfassung

Ethical Hacking, auch bekannt als Penetrationstest oder White-Hat-Hacking, ist eine Methode, bei der Sicherheitsexperten versuchen, Computersysteme, Netzwerke oder Anwendungen zu hacken, um Schwachstellen zu identifizieren. Das Ziel ist, diese Schwachstellen vor bösartigen Hackern zu schützen.

Ethical Hacker verwenden dabei ähnliche Tools und Techniken wie böswillige Hacker, jedoch mit ausdrücklicher Zustimmung des Zielsystems und im Rahmen der Gesetze und ethischen Richtlinien. Sie spielen eine wichtige Rolle bei der Cybersicherheit und helfen Unternehmen und Organisationen, ihre Systeme vor böswilligen Angriffen zu schützen.