IN DIESEM KAPITEL

- Das Pentest-Universum erforschen
- Welche Tests und Zertifizierungen brauchen Sie?
- Verstehen, was Pentester können müssen
- Cyberkriminalität
- Ihr erster Penetrationstest

Kapitel 1
Die Rolle von Pentests in der IT-Sicherheit

Penetrationstests – oder kurz Pentests – sind eine der heißesten Fertigkeiten, die ein IT-Profi braucht. Während Hightech immer größere Teile der Welt bestimmt, wird die Frage nach ihrer Sicherheit immer dringlicher. Firmen und Organisationen suchen händeringend nach Fachleuten mit Cybersecurity-Hintergrund, die in der Lage sind, Pentests durchzuführen.

Als Pentester brauchen Sie ein solides Verständnis davon, wie ein krimineller Hacker Zugang zu Ihrem System bekommen kann und wie er seine Attacken ausführt. Keine Angst, ich begleite Sie auf diesem Weg durch Angriffsszenarien und die Vorstellungswelt der Hacker. Sie müssen tatsächlich genauso wie ein Hacker denken lernen, um ein guter Pentester zu werden, weshalb diese auch White Hats (»weiße Hüte«) oder Ethical Hackers genannt werden. Wenn jemand vielleicht doch keine ganz blütenweiße Weste hat, aber auch keine wirkliche kriminelle Energie entwickelt, spricht man auch von einem Grey Hat (»grauer Hut«). Mehr dazu in Kapitel 2.

Ich werde Ihnen auch alles nahebringen, was Sie über Sicherheitslücken wissen müssen sowie über die Tools, Techniken und Skills, welche die heutige Elite der Penetrationstester Tag für Tag einsetzt, um das Vermögen ihrer Unternehmen oder Auftraggeber zu schützen.

All dies und mehr wird in diesem Buch an die Reihe kommen, doch in diesem Kapitel beginne ich zunächst einmal buchstäblich bei null: Zuerst betrachten wir die Rolle, die ein Pentester in einer Firma spielen kann. Dann kommen wir zur Wichtigkeit von Zertifizierungen und was man dafür können muss. Zum Schluss gibt es noch ein paar Abschnitte

darüber, wie Sie es am geschicktesten anstellen, ein kompetenter und nachgefragter Pentester zu werden.

Die Rolle von Penetrationstests

In der Cybersecurity gibt es eine Unmenge von Namen für alle, die dort mit guten oder bösen Absichten unterwegs sind. Wenn Sie neu auf dem Gebiet sind, kann das mehr als verwirrend werden. Um alle Unklarheiten zu beseitigen, widme ich diesen Abschnitt der Beschreibung der guten Leute, die die Pentests durchführen, und deren Aufgaben. (In Kapitel 2 kommen dann die Bösen dran.)

Die primäre Aufgabe eines Penetrationstesters ist es, kontrolliert beziehungsweise »ethisch« in Computersysteme einzudringen. Der Rahmen wird zuvor im sogenannten *Scope* abgesteckt. In ihm wird festgehalten, was der Pentester sich genau anschauen darf, wie er vorgehen darf und vor allem, was er nicht darf. Ein professioneller Pentester versucht dabei aktiv, die vorhandenen Sicherheitsvorrichtungen und -einstellungen zu umgehen. Auf diese Weise kann er zeigen, wie verwundbar ein Betriebssystem, eine Webanwendung oder ein Unternehmensnetzwerk sind. Zwar wird es letztendlich in die Verantwortung anderer Leute fallen, mit den gefundenen Problemen umzugehen. Aber der Tester wird zum Abschluss seiner Untersuchung auf jeden Fall einen umfassenden Bericht schreiben, in dem er jeden seiner Schritte und seine Ergebnisse detailliert dokumentiert. So werden dann seine Auftraggeber von ihm auch entsprechend fundierte Vorschläge erwarten. Damit beschäftigen wir uns in Kapitel 12.

Sie benötigen unbedingt eine offizielle Erlaubnis, um einen Penetrationstest durchzuführen. Selbst wenn Sie extra engagiert wurden, um für Ihren Auftraggeber Pentests zu machen, brauchen Sie möglicherweise Extragenehmigungen für einige besonders kritische Aktivitäten. Kapitel 9 beschäftigt sich mit diesem Thema.

Crowdsourcing

In dem Maße, wie Big Data als Konzept an Bedeutung gewinnt und die IT-Systeme immer größer und komplexer werden – besonders wenn immer mehr Unternehmen in die Cloud wandern und Lösungen outsourcen –, wird es dringlicher und dringlicher, so viele Ressourcen wie möglich für die Systemsicherheit zu mobilisieren, um den immer neuen Risiken und Bedrohungen begegnen zu können. Und weil die Konzerne immer mehr auf massiv parallele Rechnerverbünde und virtualisierte Systeme mit neuartigen Architekturen setzen, gibt es eine große Menge an Gelegenheiten, in denen die globale Community der guten Ritter, das heißt, die der White-Hat-Hacker, ihre segensreiche Tätigkeit entfalten kann.

Crowdsourcing ist grundsätzlich eine Form der Zusammenarbeit von (IT-)Experten, bei der gruppenbasierte Teams von Enthusiasten (die durchaus gleichzeitig Experten sein können) gemeinsam Aufgaben lösen, die traditionell firmenintern bearbeitet werden. Das funktioniert

in der Regel über das Internet und kommt auch im Bereich der IT-Sicherheit vermehrt zum Einsatz. Mithilfe von Pentests können Experten die Firmensysteme dann in gemeinsamer Arbeit in ganz ähnlicher Weise untersuchen, wie es herkömmliche Security-Teams tun würden. Eine crowdgesourcte Pentestergruppe könnte mit der gleichen Art von Probeangriffen beauftragt werden wie ein konventioneller Consultant.

Crowdgesourctes Pentesting läuft im Prinzip genauso wie jedes andere Crowdsourcing: Sie setzen eine große und sehr vielfältige Basis von Ressourcen, Wissen und Fähigkeiten ein, um ein besseres Ergebnis zu bekommen. Wenn Sie hierbei allerdings Bedenken wegen Ihrer Privatsphäre oder juristischen Problemen haben, wenden Sie sich besser an den Cybersecurity-Consultant Ihres Vertrauens.

Crowdsourcer finden Sie zum Beispiel auf Websites wie `www.hackerone.com`. Dort können Sie entweder Ihre Fähigkeiten in die Schwarmintelligenz der weißen Hüte einfließen lassen oder aber deren Hilfe selbst in Anspruch nehmen.

Firmeneigene Sicherheitsprofis

Sie haben als Unternehmen grundsätzlich zwei Optionen: Entweder verlassen Sie sich auf Ihre eigenen IT-Sicherheitsleute oder Sie heuern externe Consultants an (auf diese gehe ich im nächsten Abschnitt ein). Firmeneigene Profis finden Sie in der Regel in Konzernen und staatlichen Institutionen, die eigene Abteilungen mit erfahrenen Pentestern beschäftigen. Für kleinere Einheiten ist so etwas oft entweder zu teuer oder ihre Systeme sind nicht komplex genug, um eigene Experten auszulasten. Manchmal werden dort Pentests und andere Sicherheitsmaßnahmen von einem Systemadministrator, einem Network Engineer oder anderen IT-Kräften nebenher erledigt.

Ein Angestellter, der speziell für die (Cyber-)Sicherheit von Vermögen, Interessen und Ansehen einer Firma verantwortlich ist, wird oft Security Analyst genannt. Dies ist dann in der Regel ein Vollzeitjob. Das Aufgabenprofil kann im Detail eine sehr große Bandbreite an Security-Funktionen, Fähigkeiten und eingesetzten Tools abdecken.

Je nach Organisation und ihrer konkreten Stellung darin können Security Analysts auch andere Berufsbezeichnungen führen:

- ✔ Chief Information Security Officer (CISO)
- ✔ Security Architect
- ✔ Security Engineer
- ✔ Security Operations Staff
- ✔ Risikoanalyst
- ✔ Forensics Technician
- ✔ Security Practitioner

Es gibt ganz offensichtlich eine ganze Menge von verschiedenen Tätigkeiten und Aufgaben in der IT-Sicherheit, aber alle beschäftigen sich auf irgendeiner Ebene mit der Analyse von Sicherheitsproblemen.

Allgemein gesprochen ist ein guter Security Analyst jemand, der dazu in der Lage ist, sich in viele Gebiete einzuarbeiten und einen ganzheitlichen Blick auf die Firma oder Organisation zu entwickeln, für deren Sicherheit er verantwortlich ist. Hierauf gehe ich später im Abschnitt »Wie Sie sich die Grundlagen aneignen« noch näher ein.

Security Consultants

Wie oben bereits gesagt, können Sie auch externe Experten damit beauftragen, Pentests an Ihrer Unternehmens-IT durchzuführen. Dies können entweder freiberufliche Einzelunternehmer sein oder aber Angestellte von darauf spezialisierten Beratungsfirmen. Mit einem solchen Schritt können Sie viel Geld und Zeit sparen.

Security Consultants arbeiten sowohl remote (also extern) als auch von innerhalb Ihrer Firma aus. Auf letztere Weise können Sie noch intensivere Testmethoden anwenden. So oder so, mit externen Experten erhalten auch kleine Unternehmen zu einem vernünftigen Preis Top-Expertise für ihre Cybersicherheit. Gleichzeitig bietet dieses Modell gerade Pentesting-Neulingen die Gelegenheit, erste Erfahrungen und Aufträge zu sammeln.

Zertifizierungen

Sowohl berufliche Organisationen als auch große kommerzielle Anbieter betreiben generalisierte Zertifizierungsprogramme nach Industriestandard, ebenso gibt es Zertifizierungen für den Einsatz von dedizierten beziehungsweise proprietären Tools und auch Mischformen aus beiden Ansätzen.

Eines der am weitesten verbreiteten Pentesting-Zertifikate auf dem Markt ist beispielsweise »CompTIA PenTest+«. Obwohl dieses Programm eine Reihe von allgemeinen Themen rund ums Pentesting abdeckt, geht es bei den gebräuchlichsten Tools ziemlich in die Tiefe. Weitere wichtige Zertifizierungen sind CEH (Certified Ethical Hacker Certification), die SANS GIAC Penetration Testing Certification und ISC2 CISSP (mehr hierzu in Kapitel 16).

Es empfiehlt sich übrigens für jeden angehenden Pentester, sich möglichst frühzeitig mit dem Schreiben, Einreichen und Präsentieren von Reports anzufreunden. Darauf gehe ich im Detail in Teil IV ein.

Wie Sie sich die Grundlagen aneignen

Ihre künftige Pentester-Karriere wird Ihnen ein breites Spektrum an Fähigkeiten abverlangen. Doch die größte (und wichtigste) Aufgabe ist es, sich in die Sicherheit von Netzwerken und Computersystemen allgemein einzuarbeiten, worauf ich im Folgenden eingehen möchte.

Ein ganzheitliches Security-Konzept

Nur wenn Sie das Geschäftsmodell und die Mission einer Organisation verstehen, können Sie einen ganzheitlichen Ansatz zu deren Cybersecurity formulieren. Dazu müssen Sie sich unter Umständen mit ganz unterschiedlichen Dingen wie Programmierung, Network/System Engineering, Endknoten, Desktop-Rechnern, Lagerhaltung, Logistik und vielen anderen Subsystemen und Services beschäftigen. Das soll nicht heißen, dass Sie nicht auch Gutes für die Security tun können, wenn Sie nicht die ganze aufgeführte Bandbreite beherrschen. Doch es macht definitiv einen Unterschied, wenn Sie Ihre Aufgabe strategisch und proaktiv angehen und dadurch Angriffen und Sicherheitslücken mit optimaler Effizienz begegnen.

Ein solches ganzheitliches Sicherheitskonzept ist auch unter dem Namen *Defense in Depth* bekannt. Die drei englischen Schlagworte Confidentiality, Integrity und Availability (Abkürzung: CIA, übersetzt: Vertraulichkeit, Integrität und Verfügbarkeit) beschreiben als unerlässliches Dreigestirn die Datenstrategie einer Organisation, Defense in Depth und Pentesting sichern diese gegen äußere und innere Bedrohungen ab – dies ist im Wesentlichen der ganzheitliche Ansatz der Cybersicherheit.

Um einen auch nur einigermaßen aussagekräftigen Pentest durchzuführen, sollten Sie so viel über IT-Security und Netzwerkarchitektur wissen wie möglich. Ein ganz einfaches Beispiel: Bereits für einen Basis-Pentest müssen Sie in Ihrem Scanning-Tool zumindest eine Netzwerkadresse und/oder einen Subnetzbereich eingeben.

Sie müssen auch den Unterschied zwischen einem Vulnerability Scan und ganzheitlichem Pentesting kennen – und warum diese beiden Maßnahmen einander ähneln und worin sie differieren. Abbildung 1.1 zeigt, wie Sie in der sehr gebräuchlichen Software Nessus einen IP-Adressbereich eingeben, den Sie scannen und auf Schwachstellen untersuchen wollen. Wenn Sie die Risiken und Sicherheitslücken kennen, können Sie einen Schritt weiter gehen und pentesten – also diese Lücken gezielt als Exploit ausnutzen. Dringen Sie dabei durch, wissen Sie und Ihr Auftraggeber, dass es beim Sicherheitskonzept Luft nach oben gibt.

Es ist entscheidend, dass Sie wissen, was IP-Adressen, Protokolle, Netzwerke und ähnliche Technologien für die Risikoanalyse bedeuten (und auch weniger ähnliche!). Auf diese Weise können Sie beim Pentesting gefundene Lücken unabhängig von der konkret eingesetzten Methode ausnutzen (Datenbanken, Mainframes, virtualisierte Systeme und anderes).

In den folgenden Abschnitten stelle ich Ihnen das Grundwissen vor, das Sie als (zukünftiger) erfolgreicher Pentester unbedingt brauchen.

Ein Pentester lässt keinen Stein auf dem anderen und er rechnet immer mit allem. Wenn Sie das System testen, testet es genauso auch Sie. Darüber hinaus beschränken sich virtuelle kriminelle Aktivitäten nicht auf Computersysteme. Das Internet of Things (IoT) breitet sich immer weiter aus und verbindet netzfähige Anlagen von Tablets, Smartphones und Sensoren bis hin zu Smarthome-Geräten wie intelligenten Tiefkühltruhen und TV-Geräten. Nicht alles davon

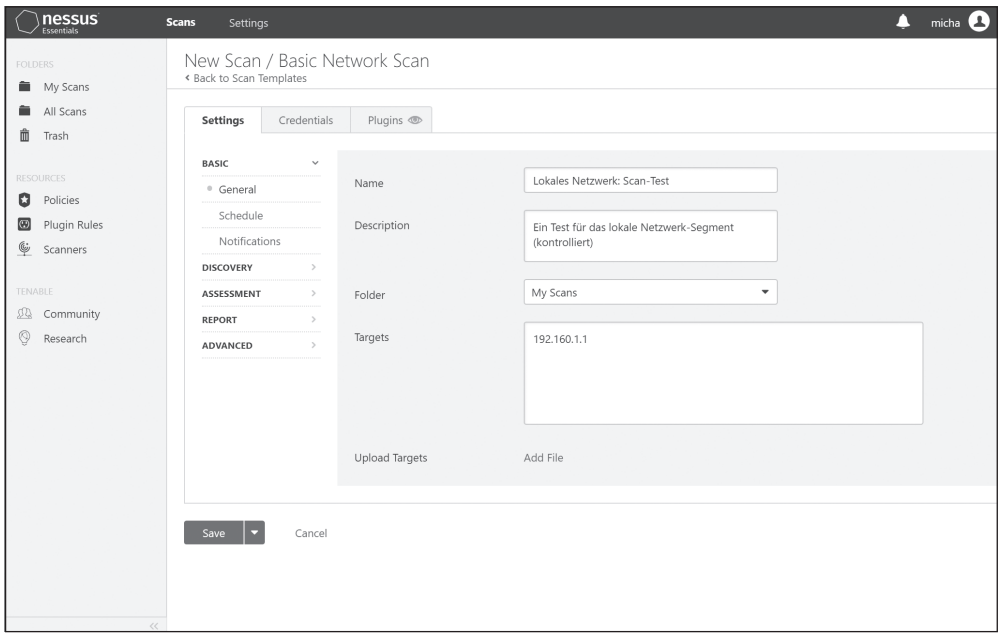

Abbildung 1.1: Wie Sie im Tool Nessus einen IP-Bereich eingeben, den Sie scannen möchten

kommt Ihnen als professioneller Pentester in der Geschäftswelt vor die Flinte, aber Sie müssen immer mit ungewöhnlichen Geräten rechnen, welche mit dem zu untersuchenden System verbunden sind. Nehmen Sie sich die Zeit, genau zu analysieren, was für ausgefallene mobile Geräte beispielsweise die Außendienstmitarbeiter des Unternehmens durch die Welt spazieren tragen könnten.

Beachten Sie auch die Reconnaissance der Hacker, also die Aktivitäten, mit denen sie im Vorfeld auskundschaften, wo sich ein Angriff lohnen könnte. Hacker starten oft mit ganz allgemeinen Recherchen, etwa einer Internetsuche, die sie auf eine vielversprechende Spur bringen könnte. So könnte eine simple Suche über das Protokoll »Whois« bereits eine interessante Adresse ausspucken. Auch eine DNS-Suche beziehungsweise -Anfrage dürfte wertvolle Hinweise liefern. Google-Suchen können auf potenzielle Angriffspfade, URLs, Domain-Namen, IP Adressen, E-Mail-Adressen und mehr führen. In Kapitel 2 erfahren Sie mehr über Reconnaissance.

Basic Networking

Basic Networking schließt das OSI(Open Systems Interconnect)-Modell ein (ist aber natürlich nicht darauf beschränkt). Sie müssen wissen, wie Daten von einem Ort (dem Sender) zu einem anderen (dem Empfänger) gelangen, um nachzuvollziehen, wie eine Cyberattacke abläuft.

Natürlich müssen Sie auch wissen, wie die ganzen Blackboxes im Netz wie Router, Switches, Hubs, Load Balancers, Firewalls oder Intrusion Prevention Devices funktionieren. (Der

Begriff *Blackbox Security Testing* bezieht sich auf Sicherheitstests »von außen nach innen«. In der Regel bekommt der Tester gar keine Informationen dazu, wie die internen Systeme arbeiten.) Wenn Sie einen Router pentesten, müssen Sie dessen Funktionsweise verstehen.

Das TCP/IP-Protokoll fällt ebenfalls unter »Netzwerk-Grundwissen«. Das Transmission Control Protocol (TCP) und das Internet Protocol (IP) kontrollieren zusammen, wie sich Computer mit dem Internet verbinden. Sie enthalten wesentliche Teile der sieben Layer des OSI-Modells (siehe Abbildung 1.2). Dieses definiert als logischer Rahmen, wie Daten von der Quelle zum Zielort und zurück gelangen, wobei eine Vielzahl von Netzwerktechnologien, Systemen und Applikationen involviert sind.

Anwendung
Darstellung
Sitzung
Transport
Vermittlung
Verbindungsebene/ Sicherungsschicht
Bitübertragung

Abbildung 1.2: Das OSI-Modell

Die in einer Suite wie TCP/IP zusammengefassten Protokolle beziehen sich auf verschiedene Schichten des Modells und üben unterschiedliche Funktionen aus. Beispielsweise operiert FTP auf einem höheren Layer des Modells als TCP oder IP. Die Idee dahinter ist, dass im Fall, dass die unteren Ebenen nicht funktionieren, die höheren Ebenen nicht korrekt arbeiten werden. Das OSI-Modell erlaubt es Ihnen dann, etwaige Probleme im vernetzten System in einem transparenten Workflow abzuarbeiten.

In Abbildung 1.3 sehen Sie eine Wire Packet Capture, also abgefangene Datenpakete, die einen großen Informationsschatz darstellen, den Sie beim Pentesting mit einem Tool wie Wireshark verwenden können, indem sie die abgefangenen Datenpakete dort im Detail analysieren.

Ihr umfangreiches Wissen über diese Protokolle, wie und wo sie operieren und was sich in den Frames, Headers und im Inneren der Datenpakete verbirgt, wird Sie zu einem großartigen Pentester machen. Wenn Sie zum Beispiel bei einem Pentest die Meldung erhalten, dass es eine Schwachstelle in Telnet gibt, über die Datenpakete im Klartext hin- und hergeschickt werden, müssen Sie herausfinden, welchen Angriffsweg ein Hacker wählen würde. Dies ist wesentlich einfacher, wenn Sie wissen, wie die Protokolle gestrickt sind und wie sie sich verhalten sollten, wenn sie *nicht* manipuliert oder von Software-Bugs betroffen sind.

Ich empfehle Ihnen dringend, sich wirklich ausführlich mit TCP/IP zu beschäftigen, denn es ist bis heute die global wichtigste Protokoll-Suite. Als es vor vielen, vielen Jahren eingeführt wurde, hatte es eine ganze Menge Macken. Insbesondere

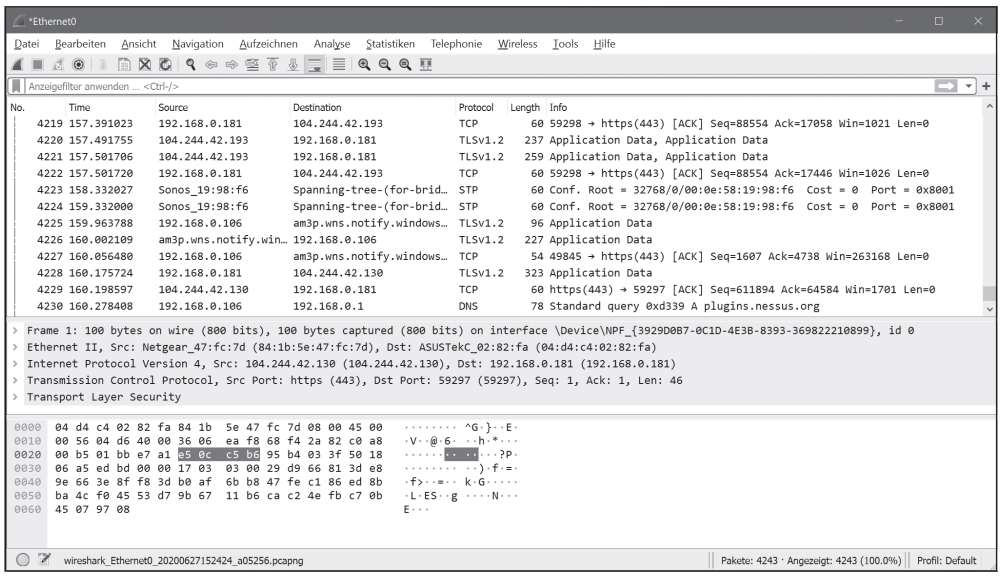

Abbildung 1.3: Ein Blick in mit dem Tool Wireshark abgefangene Datenpakete, die einen großen Informationsschatz darstellen

zählten dazu die einfache Anwendbarkeit und dass damals Sicherheit weit hinter Nutzbarkeit rangierte. Angesichts dessen können heutige Netzwerke und Systeme zwar auf all diese mittlerweile nur zu gut bekannten Macken eingehen, doch es lauert immer noch Gefahr im Verborgenen. Studieren Sie TCP/IP und alle seine Subprotokolle in allen Details, um die Sicherheitslücken Ihres Unternehmens bestmöglich aufspüren zu können.

Allgemeine Sicherheitstechnologie

Zu den allgemeinen digitalen Sicherheitstechnologien zählen Firewalls. Ein Scan gegen eine Firewall ergibt in der Regel wenig bis keine Informationen. Teilweise können die Informationen auch alternieren, abhängig davon, wie »aggressiv« man beim Scannen vorgegangen ist. Es hilft zu wissen, warum das so ist, wenn Sie einen Sicherheitsbericht erstellen sollen. Wenn Sie etwa ein Ping an das Interface senden, erhalten Sie gar nichts zurück, weil die Firewall das Antwortprotokoll deaktiviert hat (oder haben sollte).

Abbildung 1.4 zeigt das Log einer Cisco-Router-Firewall, welches die IP-Adressen und Ports von Quellen und Empfängern auflistet, die bei Verbindungen benutzt wurden.

Ein anderes Beispiel wäre, dass Sie bei einem Scan auf einem Webserver in einer Demilitarized Zone (DMZ, auch Screened Subnet) hinter einer Firewall offene Ports finden, die es dort nicht geben sollte. Wenn Sie nun im Log der Firewall nach diesem Server suchen und seine Einträge finden, erkennen Sie, welche Quellen-IP-Adressen versuchen, eine Verbindung dorthin aufzubauen. So etwas sollten Sie als einen aktiven Angriff notieren und mit hoher Priorität mit Gegenmaßnahmen behandeln.

Severity	Date	Time	Syslog ID	Source IP	Source Port	Destination IP	Destination Port
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016
6	Jan 11 2010	06:14:52	338301	128.107.241.185	53	192.168.45.4	47016

Abbildung 1.4: Das Log einer Cisco-Router-Firewall, das IP-Adressen und Ports auflistet

Andere allgemeine und wichtige Sicherheitstechnologien sind Dinge wie Intrusion Prevention/Detection Systems, Load Balancers, Access Control Lists (ACLs) auf Routern und Wireless Access Points, Controller und Mobile Extenders. Jedes Einzelne davon kann für einen Angreifer zum Exploit werden – und je mehr Sie darüber wissen und aus den entsprechenden Logs herauslesen können, desto eher können Sie die damit verbundenen Risiken erkennen und erfolgreiche Ethical Hacks starten.

Systeminfrastruktur und Applikationen

Sie müssen auch mit allen IT-Systemen Ihrer Firma vertraut sein, also Server, Speicher, Telekommunikation und den darauf installierten Applikationen. Dies schließt die Betriebssysteme und die von ihnen bereitgestellten Dienste mit ein (Name Resolution Services, Remote Access Gateways und IP Address Leasing). Wenn Sie ein Profi sind, wird Ihr Report Pentests auf allen diesen Einheiten enthalten.

Wenn Sie ein Domain Name System (DNS) scannen, stellen Sie vielleicht fest, dass dort Patches installiert werden müssen. Handelt es sich um ein Microsoft-Windows-Server-System, können Sie diese wahrscheinlich ziemlich einfach downloaden und Ihrem Report entsprechend installieren. Vielleicht arbeiten Sie auch unter Unix beziehungsweise Linux, wo der DNS Name Daemon (Dienst) BIND läuft. In beiden Fällen könnten Sie dort Probleme entdecken, die Ihre Aufmerksamkeit erfordern. Wenn Sie wissen, worum es sich dabei handelt, erkennen Sie nicht nur, wie das Problem zu beheben ist, sondern auch wie die dazu nötigen Aufgaben zu priorisieren sind.

Web-Applikationen sind naturgemäß anfällig für Sicherheitslücken, da Sie ja nach Möglichkeit ständig zugänglich sein sollten. Datenbank-Server unter der Structured Query

Language (SQL) können zum Beispiel mit einer Injection Attack angegriffen werden. Eingabefelder, die Nutzereingaben gar nicht oder nur mangelhaft auf den Inhalt und die Form überprüfen, können genutzt werden, um eigene Skripte auszuführen, auch bekannt als *Cross Site Scripting (XSS)*. Auch die Betriebssysteme von Webdiensten und -applikationen sind Einfallstore für kriminelle Aktivitäten, die ständig überwacht und gepflegt werden müssen.

Mobile Systeme und die Cloud

Mobile Technologien ersetzen in zunehmendem Maße Desktop-Rechner und andere Geräte als Endknoten in Firmennetzwerken. Sie bewegen sich rund um die Welt von Ort zu Ort – ein Must-know für angehende Security-Experten! Ob es sich dabei um Betriebsvermögen handelt oder private Geräte benutzt werden, sie transportieren Firmensoftware und zum Teil hochsensible Daten durch die Gegend. Die damit verbundenen Herausforderungen für die IT-Sicherheit adressieren Lösungen des Mobile Device Managements (MDM).

Natürlich möchten Sie auch Ihr MDM selbst einem Sicherheitstest unterziehen. Das machen Sie genau wie mit allen anderen Systemen: Scannen, Pentesten, Report erstellen und erkannte Risiken behandeln.

Die Cloud ist eine weitere potenzielle Quelle von Herausforderungen für Security- und Pentesting-Profis. Da Cloud-Technologien jedoch in den Zuständigkeitsbereich der Cloud-Anbieter fallen, sind Sie erst einmal auf der sicheren Seite, wenn Sie vertrauensvoll mit deren Security-Teams zusammenarbeiten. Solange diese gute Pentester sind, haben Sie dasselbe erreicht, als wenn Sie selbst aktiv geworden wären.

Hinweis: Sie sollten darauf vorbereitet sein, dass auch beim Cloud-Anbieter Fehler passieren können, die sich unmittelbar auf Ihre eigene Security auswirken.

Cyberkriminalität

Cyberkriminalität bedeutet kriminelle Aktivitäten – wie Datendiebstahl, Zerstörung von Information und Identitätsdiebstahl –, die mithilfe von Computersystemen und -netzen und ähnlichen Technologien begangen werden. Hacking dreht sich zu einem großen Teil um Cyberaktivitäten und Cyberkriminalität. Jeder Zugang zu irgendeinem System, der *nicht* ausschließlich zur Recherche erfolgt, insbesondere auch das Sammeln von Informationen über solche Zugangsmöglichkeiten und mögliche anzurichtende Schäden, ist ungesetzlich. Seit den anarchischen Anfängen in den frühen 1990er Jahren sind mehr und mehr gesetzliche Regelungen zum Schutz von Daten und digitalen Besitztümern erlassen worden.

Die folgenden Überlegungen zur Cyberkriminalität sollten Sie besonders beherzigen, bevor Sie mit Penetrationstests beginnen:

- ✔ Wer cyberkriminelle Handlungen begeht, tut dies in der Regel, um Informationen, Zugriff oder Einflussmöglichkeiten zu erhalten, die einen Wettbewerbsvorteil bieten oder direkt Geld wert sind.

- ✔ Die wesentliche Aktivität von Cyberkriminellen ist der unablässige Versuch, Informationssysteme anzuzapfen.
- ✔ Der einzige Weg, um herauszufinden, wie anfällig Sie für cyberkriminelle Angriffe sind, besteht darin, dass Sie Ihr System selbst angreifen, das heißt pentesten. Dies erlaubt es Ihnen, den Angreifern eine Nasenlänge voraus zu bleiben und so Ihre Ressourcen zu schützen und etwaige Risiken abzumildern.
- ✔ Sie müssen vom Besitzer der Daten oder Systeme angestellt oder beauftragt sein und über eine explizite Erlaubnis verfügen, um Ethical Hacking, Pentesting, Vulnerability Scans oder andere Tools einzusetzen, bei denen Sie selbst Sicherheitslücken ausnutzen, um die Systemsicherheit zu überprüfen.

Pentesting kann sehr leicht selbst als ein Akt von Cyberkriegsführung aufgefasst werden – wenn Sie Systeme und Netze testen, ohne dafür eine explizite Erlaubnis zu haben. Aus Ethical Hacking wird dadurch ganz schnell unethischer Gesetzesbruch!

- ✔ Wenn Sie Sicherheitslücken gefunden haben, können Sie diese mit den entsprechenden Tools als Exploit nutzen. Sie müssen allerdings aufpassen, was für andere Probleme sich daraus ergeben könnten. Wenn Sie zum Beispiel einen Buffer auf einer Netzkarte zum Überlaufen bringen, um zu testen, ob sich auf diese Weise ins System eindringen lässt, dürfte dies Ihr gesamtes Netzwerk lahmlegen. Das kann besonders dann problematisch sein, wenn der beauftragte Pentest in der produktiven Umgebung des Auftraggebers stattfindet. Deswegen ist es immer wichtig, Rücksprache mit dem Auftraggeber zu halten!
- ✔ Sie sollten sich im Vorhinein überlegen, welche möglicherweise irreparablen Schäden bei einem Pentest entstehen könnten, und für diesen Fall Vorkehrungen treffen. Wenn etwa die Gefahr eines Ausfalls des Betriebssystems besteht, sollten Sie dieses vorher sichern, damit Sie es anschließend wiederherstellen können. Generell sollten Sie von allen wichtigen Daten vorher Backups gemacht haben!
- ✔ Sie könnten Kollegen unbeabsichtigt auf von Ihnen gefundene Sicherheitslücken aufmerksam machen, wodurch die Gefahr von nicht-digitalen Informationslecks entsteht. Sie sollten niemanden hinzuziehen, der das gefundene Wissen nicht unbedingt benötigt.
- ✔ Wenn Sie der Security Incident Handler sind (etwa als Teil des Incident Response Teams, das ich Ihnen in Kapitel 2 vorstellen werde) und gerade einem Cyberkriminellen auf der Spur sind, dann achten Sie darauf, dass alle erfassten Daten und Belege auch gerichtsfest sind.
- ✔ Das Darknet ist der Ort, von wo die meisten Angreifer ihre Tools und Ressourcen beziehen, da dieser Bereich des Internets normalerweise nicht mit Suchmaschinen erfasst werden kann. Die meisten dieser Tools finden sich in Peer-to-Peer-Netzwerken und ähnlichen Konstruktionen. »Script-Kiddies«, Low-Level-Hacker, Cyberkriminelle, Elite-Hacker und Cyberterroristen rüsten sich dort für ihre gesetzwidrigen Handlungen aus.

Die Grenze zu Cyberterrorismus und Cyberkriegsführung

Je nach Schwere der Tat (und Auftraggeber) spricht man bei massiver Cyberkriminalität auch von *Cyberterrorismus* und *Cyberkriegsführung*. Stehen Regierungs- oder Militärbehörden eines fremden Staates hinter einem solchen Angriff, kann man ihn als kriegerischen Akt ansehen, stecken nicht staatliche Gruppe dahinter, geht es in Richtung Cyberterrorismus.

Dabei geht es nicht nur darum, Informationen zu stehlen oder Einfluss auf Entscheidungen zu gewinnen. Cyberattacken auf die Stromversorgung oder die militärische Infrastruktur eines Landes können desaströse Konsequenzen haben. Dies macht kontinuierliches Pentesting zu einer Frage der nationalen Sicherheit.

Was Sie brauchen, um anfangen zu können

Es ist Ihnen vielleicht noch nicht klar, aber man fängt nicht einfach irgendwie mit Pentesting an. Sie sollten unbedingt die folgenden Schritte befolgen, wenn Sie zum Kern des Pentestens vordringen wollen:

- ✔ Stellen Sie sicher, dass Sie die **Grundlagen der Informationstechnologie (IT)** beherrschen, insbesondere Computersysteme und Netzwerke.
- ✔ **Testen Sie Systeme auf Sicherheitslücken und mögliche Angriffsvektoren,** dies ist eine grundlegende Aufgabe beim Pentesting. Solch ein Test erkennt bereits im Voraus potenzielle Bedrohungen – Stellen, an denen ein Hacker attackieren könnte. Ein Beispiel für eine Sicherheitslücke ist ein Software-Bug, mit dessen Hilfe sich Zugriffsberechtigungen manipulieren lassen. Ein *Angriffsvektor* wiederum ist eine Methode oder ein Pfad, wodurch ein Hacker Zugang zum Zielsystem finden kann; Hacker suchen so lange in Ihrem System herum, bis sie eine schwache Stelle gefunden haben. Vektoren diskutiere ich im Detail in Kapitel 4.

  Nach dem Test erstellen Sie Reports über erkannte Sicherheitslücken mit Framework-Tools wie Metasploit, in denen Sie detailliert auflisten, welche Risiken alle behandelt werden müssen. Anschließend führen Sie weitere Tests durch, um festzulegen, was alles im konkreten Einzelfall zu tun ist, oder um zu prüfen, ob die Risiken beseitigt wurden.

Die Suche nach Sicherheitslücken wird exponentiell effizienter, wenn Sie sie in Kombination mit anderen Tests einsetzen. Das sind etwa Systemüberprüfungen (zum Beispiel die Auswertung von Log-Dateien) oder Performance-Tests, welche ungewöhnlich hohe CPU- oder Festplattenaktivitäten anzeigen, oder generell alles, was darauf hindeutet, dass ein unerwünschter Gast eingedrungen ist und vielleicht sogar Code hinterlassen hat.

- ✔ **Planen Sie, wann Sie Ihre Scans durchführen.** Es scheint eine Selbstverständlichkeit zu sein, aber es ist sehr wichtig, wann und wie oft Sie prüfen. Um potenzielle Einfallstore so fest verschlossen wie möglich zu halten, brauchen Sie Schedules mit regelmäßigen Testintervallen, die alle relevanten Teile Ihres Unternehmens berücksichtigen.
- ✔ **Wählen Sie die passenden Tools aus.** Abbildung 1.5 zeigt Metasploit (mehr dazu in Kapitel 4), womit Sie unter anderem Scans durchführen können. Es gibt sehr viele Management- und Monitoring-Tools, Logs und andere nützliche Software, womit sich Ihr Pentest-Toolkit optimieren lässt, damit es Ihnen einen möglichst vollständigen Überblick über alle Lücken in Ihrer Cybersicherheit verschafft. Vieles davon behandle ich in Kapitel 3, einige andere später in Teil 2.
- ✔ **Testen Sie in einer sicheren Umgebung.** Sie tun gut daran, alle neuen Tools, Scans und sonstigen Prozeduren erst in einer »*Sandbox*« oder Lab-Umgebung auszuprobieren, bevor Sie damit auf die sicherheitsrelevanten Teile Ihres Produktivsystems losgehen. Auf diese Weise wissen Sie, was Sie tun, bevor Sie es tun.

Abbildung 1.5: Mit dem Framework Metasploit können Pentester auch Scans durchführen.

Pentest – wie und wann?

Bei jedem Pentest, den Sie unternehmen, sollten Sie sich vorher eine Strategie überlegen. Natürlich können Sie blind herumsuchen und dann schauen, ob Sie etwas finden. Dies ist okay, wenn Sie es wöchentlich oder monatlich, also wirklich regelmäßig machen. Dabei sollten Sie aber darauf achten, dass sie die »*Security Posture*«, das heißt den allgemeinen Sicherheitszustand von Hardware, Software, Netzwerken, Diensten und Daten Ihres Unternehmens erfassen. Bei der zeitlichen Planung sollten Sie auch darauf achten, dass Sie die Ressourcen haben, um auf etwaige Notfälle schnell und erfolgreich reagieren zu können.

Manchmal wollen Sie aber auch tiefer graben und Ihrer Sicherheitslage wirklich auf den Zahn fühlen, etwa mit Penetrationstests, Stealth Operations, Destroy Attacks und Überlaufangriffen. Wenn Sie beispielsweise Grund zur Annahme haben, dass ein Hacker externen Zugang auf Files innerhalb Ihres Netzwerks sucht, sollten Sie genau diesen Pfad mit allen Ihnen zur Verfügung stehenden Mitteln untersuchen.

Sie sollten außerdem nach Möglichkeit sowohl interne als auch externe Tests ausführen. Sie wissen nie, von wo aus der nächste Angriff starten könnte.

Sie müssen gut darüber Bescheid wissen, von wo überall ein Angriff starten könnte – sowohl von innerhalb Ihres Trusted Networks (also von eigentlich überprüften Trusted Usern) als auch von außerhalb des Sicherheitsgürtels. Eine externe Attacke von nicht überprüften (untrusted) Usern könnte von einem externen Besucher einer Website gestartet werden, welche Sie in einer Demilitarized Zone (DMZ) Ihres Netzwerks hosten. Dort versteckt sich vielleicht eine Sicherheitslücke, die es dem Hacker erlaubt, ins Innere des Netzes zu gelangen und dort Schaden anzurichten. Eine interne Attacke wiederum ist genau das, wonach es klingt: Unbehelligt von Firewalls und anderen Schutzmaßnahmen gegen externe Eindringliche startet ein treuloser Trusted User sein unheilvolles Tun direkt vor Ihren Augen.

So oder so können Sie die nötigen Scans zum Beispiel mit Nessus durchführen (Abbildung 1.6) und damit testen, ob einer dieser Vektoren unerwünschte Resultate produziert, nämlich einem Hacker unerkannt Zugriff auf Ihr System zu verschaffen.

Wie Sie die passenden Tools für solche Scans auswählen, bespreche ich in Teil 2.

Sie müssen die richtige Balance zwischen Security und Assessment finden. Möglicherweise finden Sie einen Hack, dürfen ihn aber trotzdem nicht beheben. Ein zu hundert Prozent sicheres, perfektes System ist komplett unzugänglich und daher für alle Beteiligten unbrauchbar. Netzwerke und vernetzte Systeme leben davon, dass sie (für die richtigen Leute) zugänglich sind, also müssen bestimmte Ports notwendigerweise offen bleiben. Internetzugang erfordert zum Beispiel im Allgemeinen, dass Port 80 (HTTP) offen bleibt.

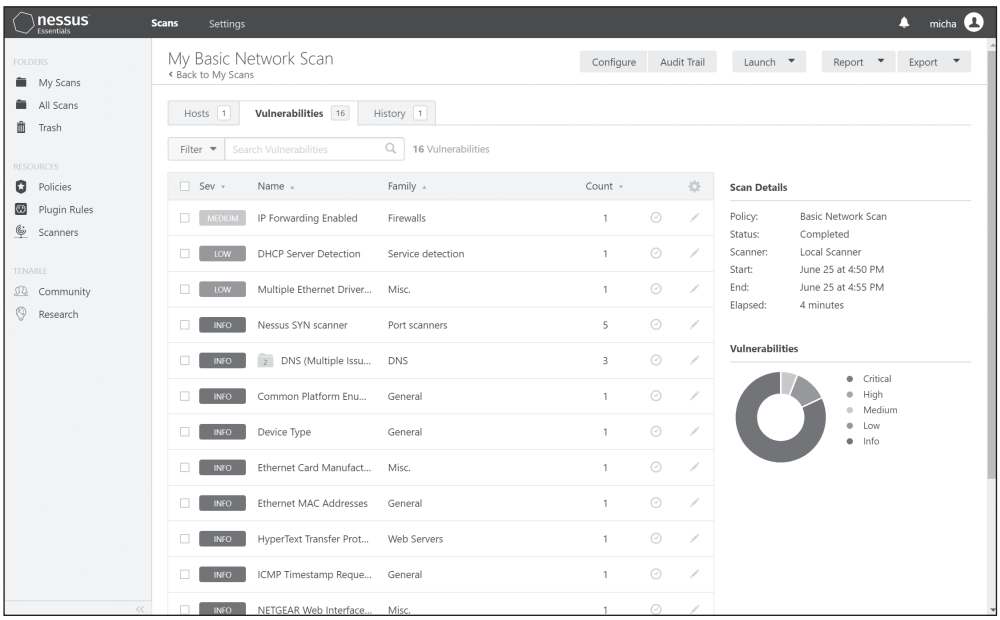

Abbildung 1.6: So können Sie Nessus bei der Bewertung von Sicherheitsmaßnahmen einsetzen.

Die ersten Schritte

Wenn Sie bereit für Ihren ersten Pentest sind, gehen Sie dabei sinnvollerweise folgendermaßen vor:

1. **Downloaden und installieren Sie ein Pentest-Tool in einer sicheren Umgebung wie Ihrem Heimnetzwerk.**

Einen Pentest in Produktivumgebungen durchzuführen, der dann zum Systemausfall führt, entspricht einem Denial-of-Service-Angriff und verhindert, dass Kunden und andere Menschen Ihr System nutzen können. Stellen Sie sicher, dass Sie so sicher und kontrolliert wie möglich vorgehen, damit Sie Risiken aufdecken und nicht selbst ein Risiko sind! Mehr zu Denial-of-Service-Angriffen lesen Sie in Kapitel 6.

2. **Downloaden Sie ein freies Tool und beginnen Sie Ihre Untersuchungen.**

   Ich diskutiere eine Vielzahl von verfügbaren Tools in Kapitel 3, doch für den Anfang würde ich zunächst einen Vulnerability Scan auf Sicherheitslücken empfehlen. Verschiedene Sicherheitsfirmen bieten dafür Testversionen ihrer Software an, die Sie in der Regel 30 Tage kostenlos nutzen können. Dazu gehört beispielsweise Vulnerability Manager Plus von ManageEngine (`www.manageengine.com`) oder die Qualsys Community Edition (`www.qualys.com`), eine Cloud-Lösung, die als freie Version verfügbar ist. Mit einer solchen Software können Sie Scans laufen lassen, die Ihnen zeigen, wo ein Host angreifbar ist und welchen Bedrohungen er ausgesetzt ist.

3. **Scannen Sie einen einzelnen Host anhand seiner IP-Adresse oder ein ganzes IP-Subnetz mit allen enthaltenen Hosts.**

   Dieser Schritt hilft Ihnen, Zielsysteme zu identifizieren, die aufgrund der generierten Berichte näher in Augenschein genommen werden sollten.

4. **Dokumentieren Sie den oder die getesteten Hosts sowie die Attacken, die Sie aufgrund der erhaltenen Informationen ausprobieren möchten.**

   Ihr Ziel ist dabei, Sicherheitslücken aufzudecken.

5. **Penetrieren Sie!**

   Dies ist der Teil eines Pentests, bei dem der geplante Hack tatsächlich ausgeführt wird und Sie sehen, ob Sie damit durchkommen oder nicht.

6. **Bereiten Sie Ihre Erkenntnisse auf.**

   Stellen Sie einen Report zusammen, beheben Sie die Schwachstellen, überwachen Sie Problembereiche, die sich nicht grundsätzlich lösen lassen, blockieren Sie Zugänge und so weiter, und so fort.