

Inhalt

Vorwort	13
Grußwort	17

TEIL I Einführung und Tools

1 Einführung	21
1.1 Hacking	21
1.2 Sicherheit	29
1.3 Exploits	41
1.4 Authentifizierung und Passwörter	48
1.5 Sicherheitsrisiko IPv6	52
1.6 Gesetzliche Rahmenbedingungen	54
1.7 Security-Organisationen und staatliche Einrichtungen	58
2 Kali Linux	61
2.1 Kali Linux ohne Installation ausprobieren	62
2.2 Kali Linux in eine virtuelle Maschine installieren	69
2.3 Kali Linux im Windows-Subsystem für Linux	77
2.4 Interna	78
2.5 Einfache Anwendungsbeispiele	81
2.6 PentestBox	85
3 Test- und Lernumgebung einrichten (Metasploitable)	87
3.1 Metasploitable 2 (Ubuntu)	88
3.2 Metasploitable 3 (Windows)	94
4 Hacking-Tools	115
4.1 nmap	116
4.2 hydra	120

4.3	nikto	126
4.4	sslyze, sslscan und testssl	129
4.5	whois, host und dig	133
4.6	Wireshark	135
4.7	tcpdump	141
4.8	Netcat (nc)	144
4.9	SPARTA	147
4.10	OpenVAS	148
4.11	Metasploit Framework	159
4.12	Metasploit Community	169
4.13	Armitage	180
4.14	Empire Framework	182
4.15	Social Engineering Toolkit (SET)	192
4.16	Burp Suite	199

TEIL II Hacking und Absicherung

5	Offline Hacking	209
5.1	BIOS/EFI-Grundlagen	209
5.2	Auf fremde Systeme zugreifen	212
5.3	Auf externe Festplatten oder SSDs zugreifen	219
5.4	Windows-Passwort zurücksetzen	220
5.5	Linux- und macOS-Passwort zurücksetzen	227
5.6	Festplatten verschlüsseln	229
6	Passwörter	239
6.1	Hash-Verfahren	240
6.2	Brute-Force Password Cracking	243
6.3	Rainbow Tables	244
6.4	Wörterbuch-Attacken	246
6.5	Passwort-Tools	248
6.6	Default-Passwörter	256
6.7	Data Breaches	257
6.8	Multi-Faktor-Authentifizierung	259
6.9	Sicheres Passwort-Handling implementieren	260

7	WLAN, Bluetooth und SDR	263
7.1	802.11x-Systeme (WiFi)	263
7.2	Bluetooth	281
7.3	Software-Defined Radios (SDR)	298
8	Angriffsvektor USB-Schnittstelle	309
8.1	USB-Rubber-Ducky	310
8.2	Digispark – ein Wolf im Schafspelz	319
8.3	Bash Bunny	329
8.4	Gegenmaßnahmen	351
9	Externe Sicherheitsüberprüfungen	355
9.1	Gründe für professionelle Überprüfungen	355
9.2	Typen von Sicherheitsüberprüfungen	356
9.3	Rechtliche Absicherung	366
9.4	Zielsetzung und Abgrenzung	368
9.5	Methodologien zur Durchführung	369
9.6	Reporting	371
9.7	Auswahl des richtigen Anbieters	374
10	Client-Side Penetration-Testing	377
10.1	Open Source Intelligence (OSINT)	377
10.2	E-Mail-Phishing-Kampagnen für Unternehmen	394
10.3	Phishing-Angriffe mit .PDF.EXE-Dateien	403
10.4	Praxisbeispiel: Phishing-Angriffe mit Office-Makros	414
10.5	Praxisbeispiel: Phishing-Angriffe mit Word-DDE-Code	418
10.6	Angriffsvektor USB-Phishing	424
10.7	Man-in-the-Middle-Angriffe auf unverschlüsselte Verbindungen	425
10.8	Man-in-the-Middle-Angriff auf SSL/TLS-Verbindungen	432
10.9	Man-in-the-Middle-Angriffe auf Remote Desktop	437
10.10	Angriffe auf Netzwerk-Hashes	443
10.11	SMB-Relaying mit der Impacket-Library (Angriff auf Administratoren)	445
10.12	SMB-Relaying mit snarf (Angriff auf normale Domänenbenutzer)	449

11	Penetration-Testing in Netzwerken	453
11.1	Externe IP-Adressen der PTA überprüfen	453
11.2	Network Access Control (NAC) und 802.1X in lokalen Netzwerken	457
11.3	Scanning von interessanten Zielen	461
11.4	Suche nach bekannten Schwachstellen mit nmap	468
11.5	Bekannte Schwachstellen mit Metasploit ausnutzen	469
11.6	Angriff auf schwache Passwörter	475
11.7	Post-Exploitation von Systemen	478
12	Windows Server absichern	495
12.1	Lokale Benutzer, Gruppen und Rechte	496
12.2	Manipulationen am Dateisystem	504
12.3	Server-Härtung	509
12.4	Windows Defender	517
12.5	Windows Firewall	520
12.6	Windows Ereignisanzeige	524
13	Active Directories	535
13.1	Was ist das Active Directory?	535
13.2	Manipulation der Active-Directory-Datenbank bzw. ihrer Daten	549
13.3	Manipulation von Gruppenrichtlinien	553
13.4	Domänenauthentifizierung (Kerberos)	559
13.5	Pass-the-Hash-Angriffe (mimikatz)	567
13.6	Golden Ticket und Silver Ticket	579
13.7	Grundabsicherung	582
13.8	Mehr Sicherheit durch Tiers (Schichten)	587
13.9	Schutzmaßnahmen gegen Pass-the-Hash und Pass-the-Ticket-Angriffe	592
14	Linux absichern	601
14.1	Installation	602
14.2	Software-Updates	605
14.3	Kernel-Updates (Live Patches)	610
14.4	SSH absichern	613
14.5	Google Authenticator	620
14.6	Fail2ban	626

14.7	Firewall	632
14.8	SELinux	642
14.9	AppArmor	649
14.10	Apache	654
14.11	MySQL und MariaDB	660
14.12	Postfix	668
14.13	Dovecot	674
14.14	Rootkit-Erkennung und Intrusion Detection	676
15	Sicherheit bei Samba-Fileservern	687
15.1	Vorüberlegungen	688
15.2	CentOS-Basisinstallation	689
15.3	Debian-Basisinstallation	693
15.4	Konfiguration des Samba-Servers	695
15.5	Samba-Server im Active Directory	699
15.6	Freigaben auf dem Samba-Server	703
15.7	Umstellung auf die Registry	708
15.8	Samba-Audit-Funktionen	712
15.9	Firewall	714
15.10	Angriffsszenarien auf Samba-Fileserver	719
15.11	Prüfen von Samba-Fileservern	722
16	Sicherheit von Webanwendungen	731
16.1	Architektur von Webapplikationen	731
16.2	Angriffe gegen Webanwendungen	734
16.3	Praktische Analyse einer Webanwendung	759
16.4	Schutzmechanismen und Abwehr von Webangriffen	778
16.5	Sicherheitsanalyse von Webanwendungen	786
17	Software-Exploitation	791
17.1	Schwachstellen von Software	791
17.2	Aufdecken von Sicherheitslücken	794
17.3	Programmausführung auf x86-Systemen	795
17.4	Ausnutzung von Buffer-Overflows	805
17.5	Structured Exception Handling (SEH)	821

17.6	Heap Spraying	823
17.7	Schutzmechanismen gegen Buffer-Overflows	825
17.8	Schutzmaßnahmen gegen Buffer-Overflows	829
17.9	Buffer-Overflows als Entwickler verhindern	835
17.10	Spectre und Meltdown	837

TEIL III Cloud, Smartphones, IoT

18	Sicherheit in der Cloud	847
18.1	Überblick	847
18.2	Amazon S3	851
18.3	Nextcloud/ownCloud	859
19	Office 365 absichern	867
19.1	Identitäten und Zugriffsverwaltung	868
19.2	Mehrstufige Authentifizierung	877
19.3	Bedingter Zugriff	883
19.4	Identity Protection	891
19.5	Office 365 Cloud App Security	893
19.6	Privileged Identities	897
19.7	Viren- und Spamschutz im E-Mail-Verkehr	905
19.8	Schadcode-Erkennung in E-Mails mit ATP	913
19.9	Sicherheit in den Rechenzentren	921
20	Mobile Security	927
20.1	Sicherheitsgrundlagen von Android und iOS	927
20.2	Bedrohungen von mobilen Endgeräten	935
20.3	Malware und Exploits	946
20.4	Technische Analyse von Apps	957
20.5	Schutzmaßnahmen für Android und iOS	966
20.6	Apple Supervised Mode und Apple Configurator	979
20.7	Enterprise Mobility Management	986

21	IoT-Sicherheit	997
21.1	Was ist das Internet der Dinge?	997
21.2	IoT-Schwachstellen finden	999
21.3	Absicherung von IoT-Geräten in Netzwerken	1016
21.4	IoT-Protokolle und -Dienste	1017
21.5	IoT-Funktechniken	1026
21.6	IoT aus Entwicklersicht	1031
21.7	Programmiersprachen für Embedded Controller	1036
21.8	Regeln für die sichere IoT-Programmierung	1039
	Index	1051
	Die Autoren	1067

Vorwort

Die Berichterstattung über Hacking-Attacken und Sicherheitslücken, die Millionen, mitunter Milliarden Geräte betreffen, ist allgegenwärtig. Sie hat die Themen »Hacking« und »IT-Security« in den vergangenen Jahren immer stärker in den Vordergrund gerückt und auch unter »Normalanwendern« ein Bewusstsein dafür geschaffen, dass die Sicherheit der IT-Infrastruktur jeden betrifft.

Viele Computer-, Smartphone- oder ganz allgemein Internetanwender drohen angesichts der vielfältigen Risiken zu resignieren. Dass man »ordentliche« Passwörter verwenden und regelmäßig Updates einspielen sollte, ist den meisten klar – aber darüber hinaus fühlen sich Anwender den Gefahren der zunehmenden Digitalisierung weitgehend schutzlos ausgeliefert.

Tatsächlich ist es primär die Aufgabe von Administratoren, IT-Verantwortlichen und Software-Entwicklern, für mehr Sicherheit zu sorgen. Immer strengere gesetzliche Rahmenbedingungen und der mit Sicherheitslücken verbundene Image-Verlust zwingen Firmen, sich mit Sicherheit intensiver auseinanderzusetzen. Es reicht nicht mehr aus, dass ein Gerät ganz einfach funktioniert, dass Software »schick« aussieht oder dass Smartphones in stylische, immer dünnere Gehäuse verpackt werden. Die Hard- und Software samt der dazugehörigen Server- und Cloud-Infrastruktur muss auch sicher sein – zumindest so sicher, wie es technisch aktuell möglich ist.

Was Hacking mit Sicherheit zu tun hat

Als »Hacking« bezeichnet man umgangssprachlich die Suche nach Wegen, die Sicherheitsmaßnahmen eines Programms oder Systems zu umgehen oder bekannte Sicherheitslücken auszunutzen. Das Ziel besteht in der Regel darin, private bzw. geheime Daten auszulesen oder zu manipulieren.

»Hacking« hat oft einen negativen Kontext, aber das stimmt so nicht: Wenn eine Firma einen sogenannten *Penetration-Test* beauftragt, um durch externe Personen die Sicherheit der eigenen IT-Infrastruktur zu überprüfen, dann bedienen sich die Penetration-Tester derselben Werkzeuge wie kriminelle Hacker. Ähnliches gilt für Sicherheitsforscher, die versuchen, neue Schwachstellen zu finden. Das erfolgt oft im Auftrag von oder in Zusammenarbeit mit großen IT-Firmen, Universitäten oder staatlichen Sicherheitsstellen. Ob ein Hacker »gut« oder »böse« ist, hängt davon ab, wie er oder sie sich nach der Entdeckung einer Schwachstelle verhält. Verantwortungsvolle

Hacker, die Schwachstellen melden und an deren Behebung mitarbeiten, gelten als »White Hats«, kriminelle Hacker als »Black Hats«.

Wenn Sie als Administrator oder IT-Verantwortlicher für die Sicherheit eines Systems zuständig sind, müssen Sie die Werkzeuge kennen, die Hacker anwenden. Damit Sie sich bzw. Ihre Firma verteidigen können, müssen Sie wissen, wie Angreifer agieren. Insofern ist es uns in diesem Buch ein großes Anliegen, Ihnen einen Überblick über die wichtigsten Hacking-Tools und -Arbeitstechniken zu geben. Allerdings machen wir an dieser Stelle nicht Schluss. Vielmehr geht es uns in der Folge darum, wie Sie sich gegen Angreifer wehren können, welche Verteidigungsmaßnahmen Sie ergreifen können, wo Sie die Konfiguration Ihrer Systeme verbessern können. Oder anders formuliert:

**Für dieses Buch ist Hacking der Weg, aber nicht das Ziel.
Das Ziel ist es, eine höhere Sicherheit zu erreichen.**

Über dieses Buch

In diesem Werk möchten wir eine breit angelegte Einführung in die Themenfelder »Hacking« und »IT-Security« geben. Angesichts von mehr als 1.000 Seiten klingt es vielleicht wie ein Understatement, wenn wir von einer »Einführung« sprechen. Tatsächlich ist es aber so, dass sowohl Hacking als auch Security unermesslich große Wissensgebiete sind.

Beinahe zu jedem Thema, das wir in diesem Buch aufgreifen, könnte man gleich ein eigenes Buch schreiben. Und dann kommen noch all die Spezialthemen hinzu, auf die wir in unserem Buch gleich gar nicht eingehen. Kurzum: Erwarten Sie nicht, dass dieses Buch allumfassend ist, dass Sie mit der Lektüre dieses Buchs bereits ein Hacking- und Security-Experte sein werden.

Dessen ungeachtet muss es einen Startpunkt geben, wenn Sie sich mit Hacking und Security auseinandersetzen möchten. Diesen Startpunkt versuchen wir hier zu geben. Konkret setzen wir uns nach einer Einführung zum Themenumfeld mit den folgenden Aspekten auseinander:

- ▶ Kali Linux (Distribution mit einer riesigen Sammlung von Hacking-Werkzeugen)
- ▶ Metasploitable (virtuelles Testsystem zum Ausprobieren von Hacking)
- ▶ Hacking-Tools (nmap, hydra, Metasploit, Empire, OpenVAS, SET, Burp, Wireshark usw.)
- ▶ Offline Hacking, Zugriff auf fremde Notebooks/Festplatten
- ▶ Passwort-Hacking, sicherer Umgang mit Passwörtern
- ▶ WLAN, Bluetooth, Funk
- ▶ USB-Hacking und -Sicherheit
- ▶ Durchführung externer Sicherheitsüberprüfungen

- ▶ Penetration-Testing (Client und Server)
- ▶ Basisabsicherung: Windows und Linux, Active Directory und Samba
- ▶ Cloud-Sicherheit: Amazon S3, Nextcloud/ownCloud, Office 365
- ▶ Hacking und Security von Smartphones und anderen Mobile Devices
- ▶ Webanwendungen angreifen und absichern
- ▶ Exploit-Grundlagen: Buffer-Overflows, Fuzzing, Heap Spraying, Mikroarchitektur-Schwachstellen (Meltdown und Spectre)
- ▶ Absicherung und sichere Entwicklung von IoT-Geräten

Die Breite der Themen erklärt, warum dieses Buch nicht einen Autor hat, sondern gleich neun. Eine kurze Vorstellung unseres Teams finden Sie am Ende des Buchs.

Zielgruppe

Wir richten uns mit diesem Buch an Systemadministratoren, Sicherheitsverantwortliche, Entwickler sowie ganz allgemein an IT-Fachkräfte, die bereits über ein gewisses Grundwissen verfügen. Um es überspitzt zu formulieren: Sie sollten zumindest wissen, was die PowerShell oder ein Terminal ist. Und Sie müssen bereit sein, betriebssystemübergreifend zu denken: Weder Hacking noch die IT-Sicherheit beschränkt sich heute noch auf Windows- oder Linux-Rechner.

Nicht im Fokus stehen dagegen reine IT-Anwender. Natürlich ist die Schulung von Computeranwendern ein unverzichtbarer Aspekt, um die IT-Sicherheit sowohl zu Hause als auch in Unternehmen zu verbessern. Eine Zusammenstellung von mehr oder weniger trivialen Regeln und Tipps, wie Computer, Smartphones und das Internet im Allgemeinen sicher und verantwortungsvoll zu nutzen sind, erscheint uns in diesem technisch orientierten Buch aber nicht zielführend.

Los geht's!

Lassen Sie sich nicht von der Größe des Themengebiets abschrecken! Wir haben versucht, unser Buch in überschaubare Kapitel zu gliedern. Die meisten davon können Sie weitgehend unabhängig voneinander lesen und sich so Schritt für Schritt einarbeiten, Hacking-Expertise gewinnen und ein besseres Verständnis dafür entwickeln, wie Sie Ihre eigenen Systeme besser absichern können. Sie werden schnell feststellen, dass eine intensivere Auseinandersetzung mit Hacking- und Security-Techniken ungemein faszinierend ist.

Wir hoffen, mit unserem Buch dazu beizutragen, die IT-Sicherheit in Zukunft besser zu managen, als dies bisher der Fall war!

Michael Kofler im Namen des gesamten Autorentams

Vorwort Klaus Gebeshuber

Die Erfahrungen aus zahlreichen Penetration-Tests zeigen, dass viele Administratoren von Computersystemen und Netzwerken kaum die Möglichkeiten und die Dreistigkeit von Hackern kennen. Ein Angreifer benötigt genau eine Schwachstelle, um in ein System einzudringen, ein Verteidiger muss viele der Möglichkeiten verhindern. Es gibt keine Regeln; kein Weg ist für einen Hacker verboten.

Persönlich haben mich die extreme Kreativität und die technischen Möglichkeiten und Varianten von Hackern schon immer fasziniert. Ich wollte schon immer wissen, was die Bösen können, um mit dem Wissen die gute Seite zu stärken. Das Buch »Die Kunst des Einbruchs« von Kevin Mitnick (mitp-Verlag 2006) entfachte damals meine Neugier für das Thema erst recht.

Es ist mir auch ein großes Anliegen, jungen Leuten einerseits die faszinierenden technischen Möglichkeiten aufzuzeigen und sie andererseits auch für ihre zukünftige Tätigkeit auf der guten Seite zu motivieren. Die *Cyber Security Challenge* mit lokalen Qualifikationen für Schüler und Studierende in mittlerweile 14 europäischen Ländern und einem Europafinale bietet hier eine schöne Möglichkeit, junge Security-Talente zu entdecken und zu fördern.

Klaus Gebeshuber

Vorwort Stefan Kania

Schon oft ist mir aufgefallen, dass bei Samba-Servern einige Aspekte hinsichtlich der Sicherheit außer Acht gelassen werden. Oft werden Samba-Freigaben mit Berechtigungen versehen, um unerlaubte Zugriffe zu vermeiden, aber die Sicherheit des Betriebssystems wird dann manchmal nicht mehr gesehen. Ein Linux-Host mit Samba als Fileserver muss immer aus zwei Blickwinkeln gesehen werden. In meinen Seminaren spreche ich das auch immer an. Schon lange wollte ich diese Sichtweise auf Samba-Systeme genauer beschreiben.

Da kam die Anfrage des Rheinwerk Verlags zu diesem Buch. Das war genau das, was ich mir vorgestellt hatte. Hier geht es nicht um die reine Konfiguration eines Samba-Servers, sondern darum, einen Samba-Server möglichst sicher aufzusetzen. Auch der Rahmen des Buches mit den verschiedenen Werkzeugen, Diensten und Geräten ist genau passend für das Thema. So ist hier ein Buch entstanden, das ich mir selbst immer gewünscht habe. Dass ich jetzt mit meinem Kapitel dazu beitragen kann, freut mich sehr. Ich hoffe, Ihnen als Leser wird dieses Buch genau so gut gefallen wie mir.

Stefan Kania

Grußwort

IT-Sicherheit ist ein Thema, an dem gegenwärtig niemand vorbeikommt. Erst Ende Februar 2018 wurde die deutsche Öffentlichkeit wieder einmal von einem Hacking-Vorfall aufgeschreckt: Digitalen Angreifern war es gelungen, in das bis zu diesem Zeitpunkt als »sicher« deklarierte Netzwerk der Bundesregierung (IVBB) einzudringen. Dies war nur der erste ernstzunehmende Cyber-Zwischenfall dieses Jahres. Es werden weitere folgen, davon bin ich überzeugt.

Die Devise heißt also: IT-Sicherheit muss auf der Prioritätenliste ganz nach oben – bei Unternehmen, Organisationen und im öffentlichen Dienst. Aber auch bei Privatanwendern sollte die IT-Sicherheit eine prominentere Rolle spielen. Angriffe auf IT-Systeme werden für entsprechende Täter in Zukunft noch attraktiver werden. Bereits heute laufen sehr viele Zahlungen oder Geschäftsprozesse über das Internet ab – ein großes Angriffsfeld, das ständig größer wird. Gleichzeitig senkt die Anonymität des Netzes die Hemmschwelle dafür, sich an entsprechenden Angriffen zu versuchen.

Wer beim Thema IT- und Datensicherheit spart, der ist schlecht beraten. Wem es dagegen gelingt, den eigenen Mitarbeitern beizubringen, wie »Hacker« denken und agieren, der ist schon einen großen Schritt näher dran an einer robust abgesicherten IT-Infrastruktur. Wer die Angreifer versteht, ist der bessere Verteidiger.

Das vorliegende Kompendium geht mit seinem Anliegen deshalb genau in die richtige Richtung: »Für dieses Buch ist Hacking der Weg, aber nicht das Ziel. Das Ziel ist es, eine höhere Sicherheit zu erreichen«, heißt es im Vorwort. Ich kann dies nur unterstützen: Als Geschäftsführer der SySS GmbH trage ich die Verantwortung für 70 IT Security Consultants, die tagtäglich nichts anderes tun, als auf Wunsch die Systeme unserer Kunden zu »hacken«. Solche Penetration-Tests spüren schnell und effizient Sicherheitslücken auf. Die IT-Verantwortlichen können diese dann beheben – bevor illegale Hacker sie ausnutzen. Gleichzeitig zeigt ein solcher Test und der dazugehörige Abschlussbericht unseren Kunden aber auch im Detail, wie wir als »White Hat Hacker« vorgehen, um Schwachstellen aufzuspüren und diese auszunutzen.

Genau solches Wissen ist von unschätzbbarer Bedeutung, wenn es darum geht, die eigenen Systeme immer sicherer zu machen. Das Buch »Hacking & Security« stellt dieses Know-how in kompakter Form für die Praxis zur Verfügung. Ich kann jedem, der beruflich mit IT-Sicherheit zu tun hat, die Lektüre nur wärmstens empfehlen. Bleiben Sie den »bösen« Hackern immer den entscheidenden Schritt voraus.

Sebastian Schreiber, Geschäftsführer SySS GmbH