Editorial

Liebe Leserin, lieber Leser,

ganz gleich, ob Sie nur die Sicherheit Ihrer eigenen Websites abklopfen möchten oder beruflich mit IT-Sicherheit zu tun haben. Es ist gut zu wissen, wie Hacker ticken. Sie sind gefragte Leute und inzwischen hat sich herumgesprochen, dass dahinter viel mehr als das düstere Hollywood-Klischee steckt. Die Grundlagen fürs Hacken sind schnell beigebracht: Alles, was Sie dazu brauchen, ist Geduld, ein Computer und dieses Büchlein. Egal, ob Sie Anfänger sind oder schon erfahren im Umgang mit der Kommandozeile: Sie lernen hier den einen oder anderen Trick kennen.

Blicken Sie mit uns hinter die Kulissen und erfahren Sie ab Seite 16, wie Sie eine abgeschottete Hacking-Umgebung mit VirtualBox und Kali Linux einrichten, etwa um anschließend Hacking-Tools auf spezielle Übungs-Webserver loszulassen. Ihr Wissen vertiefen Sie anschließend mit dem Website-Sicherheitsscanner ZAP ab Seite 24. Sollten Sie rechtliche Bedenken haben, kann der Artikel ab Seite 34 diese hoffentlich auflösen.

Das Kapitel rund um OSINT-Techniken vermittelt Ihnen alle relevanten Grundlagen, um Security-Recherchen in öffentlichen Quellen durchzuführen. Ab Seite 40 stellen wir Ihnen eine Handvoll von OSINT-Werkzeugen vor, mit denen Sie zum Beispiel Informationen über Schwachstellen abrufen und das Darknet durchforsten können. Wie wichtig OSINT-Methoden sind, zeigt der Artikel ab Seite 48, in dem ein Pentester erklärt, wie er erfolgreich ein Unternehmen hackte.

Viren, Trojaner und andere Würmer nutzen Sicherheitslücken aus, um sich am Virenschutz von Rechnern vorbeizuschleichen und sich im System einzunisten. Wer diese schmutzigen Tricks kennt, kann sich schützen und Infektionen früh erkennen. Die Artikel ab Seite 58 zeigen Grundlagen, um Schadsoftware zu analysieren.

Bereit? Der Eingabeprompt der Kommandozeile wartet auf Sie!

Wilhelm Drehling

Inhalt

HACKING AUSPROBIEREN SCHRITT FÜR SCHRITT

Am Beispiel von vorbereiteten Webservern lernen Sie, wie ein Hacker denkt, wie er vorgeht und welche Tools er benutzt. Außerdem stellen wir noch den Website-Sicherheitsscanner ZAP vor, dazu ein praktisches Beispiel aus der echten Welt, und klären rechtliche Fragen rund ums Hacking.

INFORMATIONEN GEWINNEN MIT OSINT

Informationen aus öffentlichen Quellen sammeln und auswerten ist eine der gängigsten Praktiken eines Hackers. Wir stellen unterschiedliche Tools vor sowie eine Browsererweiterung, die OSINT-Werkzeuge bündelt. Abgerundet wird das Kapitel mit einem detaillierten Hack eines Pentesters, der hierfür einige der hier vorgestellten Werkzeuge eingesetzt hat.

MALWARE-TRICKS VERSTEHEN

Trojaner, Viren und andere Bazillen gehen ähnlich vor wie Hacker: Sie nutzen eine Sicherheitslücke aus, um sich im System einzunisten. Wer diese Tricks kennt, kann sich vor ihnen effektiv schützen. Dazu erklären wir, wie Sie eine sichere Analyseumgebung einrichten und Schadcode untersuchen.

ZUM HEFT

heise Academy

Aktion: Videokurs Netzwerke absichern

Lerne praxisnah von den Angreifern und erhöhe deine Netzwerksicherheit mit den richtigen Verteidigungsstrategien. IT-Sicherheitsberater Max Engelhardt zeigt Schritt für Schritt alle Grundlagen in einem 6,5-stündigen Online-Videokurs, der für die Käufer dieser Ausgabe kostenlos ist.

In diesem Kurs lernst du, Netzwerke abzusichern, indem du dich in die Position des Angreifers begibst. Dadurch verstehst du, welche Informationen für einen Hacker wichtig sind, und erfährst, welche Einfallswege es in dein Netzwerk gibt.

Neben den üblichen Sicherungsmaßnahmen kannst du so gezielt auf deine Netzwerkumgebung zugeschnittene Maßnahmen ergreifen, um deine IT-Systeme zu schützen.

Zusätzlich geht der IT-Sicherheitsexperte Max Engelhardt speziell auf das Active Directory als häufigsten Verzeichnisdienst in Firmennetzwerken ein und erläutert dir, welche Angriffe hier in der Praxis immer wieder zu Erfolg führen und wie du sie abwehren kannst.

Max Engelhardt ist seit 2013 freiberuflicher IT-Sicherheitsberater. Dabei berät er seine Kunden in allen Aspekten der IT-Sicherheit in Form von Penetrationtests und Risikoeinschätzungen sowie beim Aufbau von SIEM/SOC-Systemen. Er hat gelernt, sich in die Position eines potenziellen Angreifers zu versetzen, um Schwachstellen in einem Computernetzwerk zu identifizieren und eine Verteidigungsstrategie zu entwickeln.

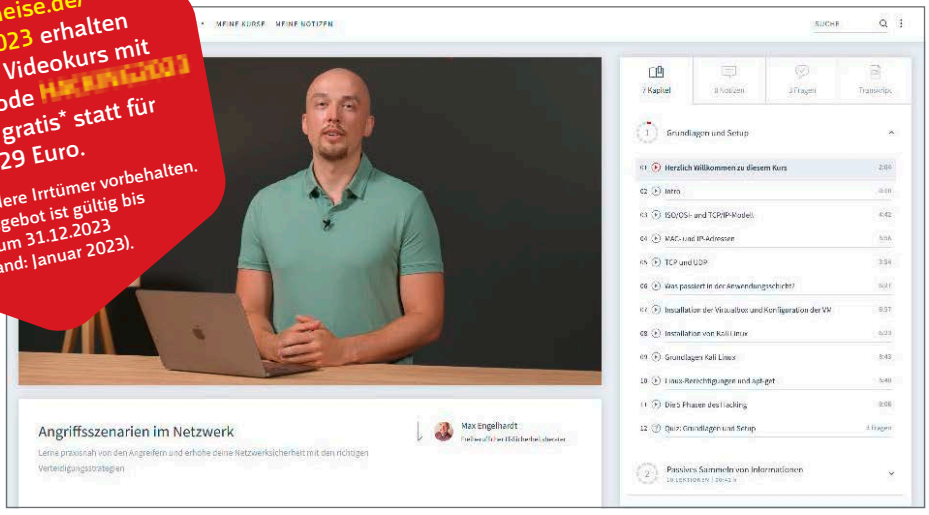
Lernen bei der heise Academy

Die IT-Fachdozenten der heise Academy präsentieren ihre Kursthemen anschaulich und verständlich. In den Videos schaust du den Experten bei der praktischen Arbeit zu und lässt dir dabei alles genau erklären. Das Wissen ist in viele kleine Lernschritte und Aufgaben unterteilt – du kannst den Kurs Lektion für Lektion durcharbeiten oder gezielt zu Themen springen, die dich interessieren.

Die persönliche Lernumgebung der heise Academy unterstützt dich mit vielen Funktionen beim Lernen, die alle in einer Ansicht schnell und einfach zugänglich sind: Du siehst deinen Lernfortschritt, kannst Lesezeichen setzen, direkt im Video Notizen speichern oder mit der Volltextsuche in den Videos konkrete Informationen wiederfinden.

Über shop.heise.de/hacking2023 erhalten Sie diesen Videokurs mit dem Rabattcode [redacted] einmalig gratis* statt für 129 Euro.

*Preis- und andere Irrtümer vorbehalten. Das Angebot ist gültig bis zum 31.12.2023 (Stand: Januar 2023).



In diesem 6,5-stündigen Videokurs zeigt Max Engelhart dir, wie Angreifer vorgehen und wie du dein Netzwerk dagegen schützt.

Alle Video-Lektionen im Überblick:

1. Grundlagen und Setup
- Grundlagen und Setup
- Herzlich willkommen zu diesem Kurs
- Intro
- ISO/OSI- und TCP/IP-Modell
- MAC- und IP-Adressen
- TCP und UDP
- Was passiert in der Anwendungsschicht?
- Installation der Virtualbox und Konfiguration der VM
- Installation von Kali Linux
- Grundlagen Kali Linux
- Linux-Berechtigungen und apt-get
- Die 5 Phasen des Hacking
- Quiz: Grundlagen und Setup

2. Passives Sammeln von Informationen
- Intro
- Wie sammelt ein Angreifer öffentliche Informationen?
- Burp Suite einrichten
- So sammelt ein Angreifer Zugangsdaten
- Subdomains als Angriffsziel
- Passives Scannen in sozialen Netzwerken
- Wie schützt man sich vor passivem Scannen?
- Sensibilisierung zum Schutz vor Angriffen
- Selbsttests zum Schutz vor passivem Scannen
- Quiz: Passives Sammeln von Informationen

3. Aktives Scannen
- Intro
- Mit Nmap offene Ports erkennen
- Scannen eines HTTP-Ports
- Schwachstellen in Software durchsuchen
- Über Protokolle SMB und SSH angreifen
- Post-Exploit Scanning
- Zum Schutz unnötige Dienste deaktivieren
- Standardfreigaben in Windows bearbeiten
- Schwachstellenmanagement
- Quiz: Aktives Scannen

4. Exploitation
- Intro
- Pentesting mit Metasploit
- Reverse Shell vs. Bind Shell
- Web Shell mit Basic Pentesting 1
- Web Exploit mit Metasploit
- Sichere Passwörter verwenden
- Präventive Maßnahmen gegen Exploits
- Reaktive Maßnahmen gegen Exploits
- Physische Sicherheit gewährleisten
- Quiz: Exploitation

5. Active Directory
- Intro
- Setup des Active Directory
- Aufbau des Active Diretory
- Authentifizierung in Active-Directory-Netzwerken
- NTLM-Relaying-Angriffe
- Poisoning und Relay-Angriffe verhindern
- mitm6-Angriff vorbereiten
- mitm6-Angriff durchführen
- Vor mitm6-Angriffen schützen
- Bloodhound-Angriff vorbereiten
- Bloodhound-Angriff durchführen
- Kerberoasting, Token und Ticket-Angriffe
- Quiz: Active Directory

6. Post-Exploitation
- Intro
- Angriffe per Datentransfer und Lateral Movement
- Rechteausweitung mit Linux Privilege Escalation
- Privilege Escalation Basic Pentesting 2
- Kritische Schwachstellen in Microsoft Windows finden
- Lateral Movement erkennen und verhindern
- Privilege Escalation erkennen und verhindern
- Persistence: Dauerhaften Zugriff erlangen
- Quiz: Post-Exploitation

7. Sicherheitslücken in Anwendungen: Buffer Overflow
- Intro
- Übersicht und Tools
- Softwaretests: Fuzzing
- Mit Shellcode Programme manipulieren
- Exploit ausführen
- Buffer Overflow verhindern
- Quiz: Sicherheitslücken in Anwendungen: Buffer Overflow
- Fazit und Kursabschluss

Zusatzaktion: Aufbaukurs zum IT-Freelancer-Einstieg

Aufbauend auf dem Kurs „Angriffsszenarien im Netzwerk“ hat Max Engelhardt eine Lernplattform geschaffen, die den Einstieg als IT-Security-Freelancer:innen ermöglicht. In diesem Kurs vermittelt er vertiefende fachliche Inhalte zu Cloudsecurity und Überwachungssystemen (SIEM) und beleuchtet alle Aspekte der Freiberuflichkeit.

Mit der Schritt-für-Schritt-Anleitung und Live-Videocalls ebnet er den Weg zu deinem ersten IT-Security-Projekt. Der Personalmangel in dieser Branche ist so groß, dass Neueinsteiger händeringend gesucht werden und mit 100 €/h beginnen! Erfahre jetzt mehr und verändere dein Leben, wie viele andere Teilnehmer:innen (siehe ct.de/wa). Als Leser dieses c’t Sonderhefts Hacking-Praxis erhältst du einen Sonderrabatt für den Aufbaukurs.

Hacking lernen in Trainingsumgebung

Wer sich vor Hackern schützen will, muss verstehen, wie diese arbeiten. Wir beschreiben den Aufbau einer virtuellen Testumgebung, in der Sie gefahrlos in die Rolle eines Angreifers schlüpfen und die Tricks der Hacker lernen.

Von **Wilhelm Drehling**

Bild: Andreas Martini

Hacking ist keine schwarze Magie, sondern eine Fähigkeit, die man sich mit etwas Erfahrung und viel Übung aneignen kann. Und es gibt viele gute Gründe, das zu tun: Wer versteht, wie ein Hackerangriff üblicherweise abläuft, kann sich davor schützen und die größten Leckagen rechtzeitig stopfen. Wer Feuer fängt und Spaß am Aufdecken von Sicherheitsproblemen hat, dem eröffnen sich berufliche Perspektiven, etwa als gut bezahlter Penetration Tester.

Mit einer virtuellen Trainingsumgebung können Sie die Angriffstechniken der Hacker in Ihrem eigenen Tempo erlernen und müssen keine juristischen Konsequenzen fürchten (siehe S. 34), da Sie Ihre Fingerübungen am virtuellen Objekt statt an fremden Rechnern machen. Als Übungsziel dienen virtuelle Maschinen, die eigens für angehende Hacker angeboten werden. Die nötigen Hacking-Tools stellt Ihnen die Linux-Distribution Kali Linux bereit. Im Sonderheft c't Security-Tipps 2021 stellten wir diese [1] sowie ein paar Hacking-Werkzeuge und Szenarien dafür bereits vor [2]. Der folgende Artikel beleuchtet weitere Möglichkeiten.

Kali Linux bringt mehr als 300 Hacking-Tools zur Schlacht mit.

Spielfeld aufklappen

Die Trainingsumgebung bauen Sie in der Virtualisierungssoftware VirtualBox auf. Die Open-Source-Software läuft unter Linux, Windows und macOS; besondere Anforderungen muss Ihr Rechner nicht erfüllen. Ein großer Arbeitsspeicher (mindestens 8 GByte) und eine SSD sind von Vorteil, aber nicht unbedingt notwendig. Falls Sie der Anleitung visuell folgen möchten, können Sie die ersten Handgriffe auch im Academy-Kurs lernen (siehe S. 6).

Laden Sie VirtualBox von der Herstellerseite herunter (siehe ct.de/wswd) und installieren Sie es. An den vorgeschlagenen Einstellungen brauchen Sie nichts zu ändern. Falls Sie VirtualBox bereits auf dem Rechner haben, sollten Sie darauf achten, dass Sie die aktuelle Version verwenden.

Nach erfolgtem Download importieren Sie die virtuelle Kali-Maschine per Doppelklick auf die OVA-Datei in VirtualBox. Die Virtualisierungssoftware fragt anschließend in einem weiteren Fenster einige Parameter der VM ab, Sie brauchen aber im Normalfall nichts zu ändern. Bestätigen Sie die Einstellungen mit Klick auf „Importieren“. Danach akzeptieren Sie noch die Software-Lizenzbestimmungen der VM (in diesem Fall die GPL v3) mit „Zustimmen“. Kurze Zeit später ist der Import abgeschlossen.

Figuren aufstellen

Jetzt fehlt nur noch ein geeignetes Angriffsziel. Verwundbare VMs bekommen Sie in Hülle und Fülle

Bild: Albert Hulm

Server-Hack Schritt für Schritt erklärt

Hacker legen nicht wild drauflos, wenn sie ein Angriffsziel im Visier haben. Stattdessen ziehen sie Fingerfertigkeit und Finesse vor. Wie genau sie vorgehen, erklären wir an einem Beispiel-Hack. Als wertvoller Komplize auf dem Weg zum Root-Zugriff soll sich ausgerechnet WordPress erweisen.

Von **Wilhelm Drehling**

Wie Sie mit wenigen Komponenten eine virtuelle Trainingsumgebung basteln und darin Hacking-Rätsel knacken, war das Thema im vorherigen Artikel (siehe S. 8). Dort beschrieben wir, wie Sie ein isoliertes Übungsnetzwerk mit der Virtualisierungssoftware VirtualBox erstellen und darin mit dem Hacker-Linux Kali verwundbare virtuelle Maschinen (VM) abtasten, die als Übungsziel dienen. Schließlich haben wir angerissen, wie Sie in die VM „Mr. Robot“ eindringen, und einige Brotkrumen gestreut, die Ihnen dabei helfen sollten, die übrigen Hacking-Aufgaben zu lösen.

Der folgende Artikel knüpft direkt daran an und liefert Ihnen eine vollständige Auflösung als Schritt-für-Schritt-Anleitung. Sie benötigen kein Vorwissen

oder besondere Hardware, um den Übungshack nachzuvollziehen, nur das auf Seite 8 beschriebene Übungsnetz. Aber auch ohne das Netz erwartet Sie im Folgenden eine interessante Lektüre.

Der gesamte Hack spielt sich in der virtuellen Testumgebung ab. Am Ende haben Sie alle drei Rätsel gelöst und als Belohnung die Flags eingesammelt, die im Server an speziellen Orten in Form von Textdateien versteckt sind, und kontrollieren den Server als Root.

Startpunkt für den Hack ist die bereits auf Deutsch gestellte Kali-Linux-VM und die virtuelle Maschine „Mr. Robot“. Beide befinden sich in dem internen Netzwerk „Hacking-Umgebung“ und erhalten eine IP-Adresse vom DHCP-Server, den VirtualBox bereitstellt. Obwohl wir bereits im letzten Artikel detailliert beschrieben haben, wie Sie zur ersten Flagge kommen, fassen wir die ersten Schritte noch mal kurz zusammen, damit Sie unserem Beispiel-Hack auch ohne Vorwissen folgen können.

Alles auf Anfang

Öffnen Sie VirtualBox und starten Sie mit Doppelklick auf Kali Linux und „Mr. Robot“ die Maschinen. Nachdem letztere hochgefahren ist, können Sie das VM-Fenster wieder verkleinern – außer einem Anmeldefenster für Root gibt es hier nicht viel zu sehen, die Zielserver laufen unsichtbar im Hintergrund. Loggen Sie sich in der Kali-VM mit „kali“ als Benutzername und Passwort ein.

Die erste Phase eines Hacks nennt sich „Enumeration“ und bedeutet nichts anderes, als den Server auszukundschaften. Die Konsole (Terminal) wird dabei Ihr treuester Begleiter sein, alle verwendeten Tools lassen sich darüber starten. Sie können das Terminal zum Beispiel über den Launcher oben links (Kali-Logo mit Drache) öffnen oder via Rechtsklick auf den Desktop und „Terminal hier öffnen“.

Zu Beginn wissen Sie nichts über Ihr Angriffsobjekt, es ruht irgendwo da draußen im Hacking-Netzwerk und läuft vor sich hin. Um die Ziel-VM zu finden, können Sie mit dem Befehl

```
sudo netdiscover -r 10.10.1.0/24
```

das Netzwerk nach aktiven Systemen scannen (die `sudo`-Abfrage bestätigen Sie mit dem Standard-Passwort „kali“). Der Befehl entdeckt unter anderem die IP-Adresse 10.10.1.3, hinter der sich Mr. Robot verbirgt. Wertvolle Informationen wie die IP-Adresse des Servers oder benutzte Befehle sollten Sie gleich mit Strg + Umschalt + C kopieren und in ein Textdokument einfügen. Das erleichtert Ihnen die folgenden Schritte und den Einstieg in weitere Übung-VMs, wenn Sie auf den Geschmack gekommen sind.

Tasten Sie sich langsam an die Maschine heran und klopfen Sie das Zielsystem auf erreichbare Ports ab, um herauszufinden, auf welchen Ports Server lauschen, die sich als Angriffsziel eignen. Dafür können Sie den Netzwerkscanner **nmap** benutzen [1]. Ein Scan mit

```
nmap 10.10.1.3
```

spuckt drei erreichbare Ports aus, darunter die Ports 80 (http) und 443 (https). Auf dem Zielsystem läuft also wahrscheinlich mindestens ein Webserver, der eine Website ausliefert. Das können Sie mit dem Browser leicht überprüfen: Öffnen Sie ihn, indem Sie oben links auf der Menüleiste den Globus anklicken und die URL http://10.10.1.3 ansteuern. Die Website

OSINT-Tools für Security-Recherchen

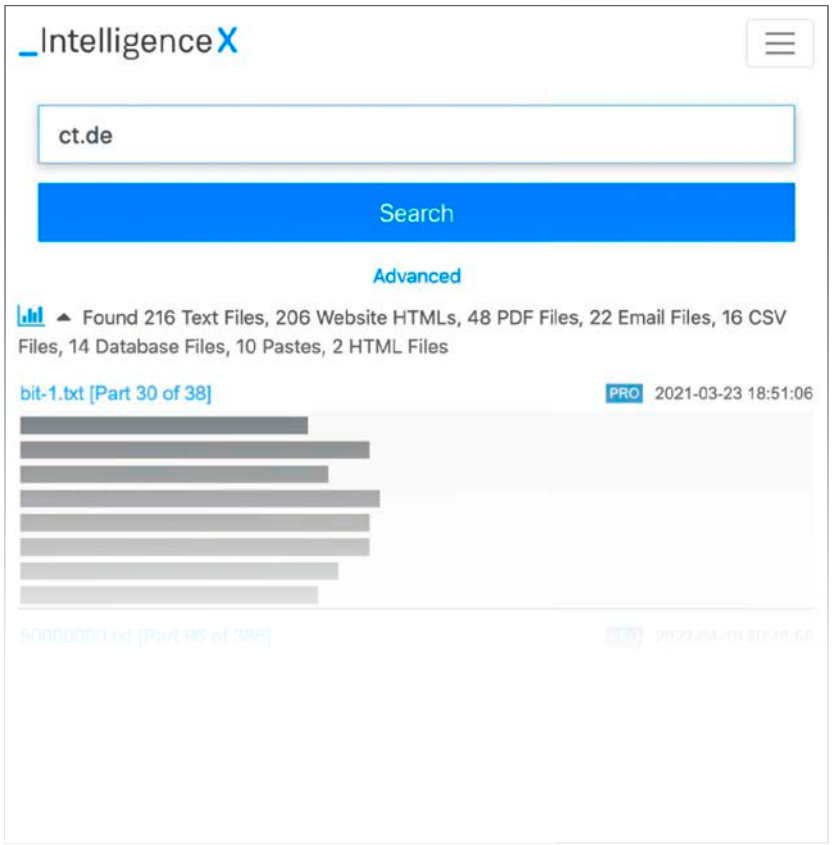
Das Netz bietet eine Fülle an Tools für Security-Recherchen, mit deren Hilfe Sie verdächtige IP-Adressen analysieren, Mailadressen überprüfen, Bitcoin-Scams aufdecken, Daten im Darknet aufspüren und vieles mehr. Wir haben eine Auswahl der nützlichsten Tools für Sie zusammengetragen.

Von **Kathrin Stoll**

Bild: Thorsten Hübner

Gerade in der IT-Sicherheit ist Open Source Intelligence (OSINT), also die Sammlung und Auswertung öffentlicher Daten, unverzichtbar. OSINT spielt längst eine wichtige Rolle bei der Informationsbeschaffung, sowohl auf Seiten von Cyber-Kriminellen als auch unter IT-Sicherheitsexperten.

Ursprünglich stammt der Begriff OSINT aus der Welt der Nachrichtendienste. Er bezeichnet das Sammeln und Analysieren von Informationen aus frei verfügbaren offenen Quellen, daher das Open Source im Begriff. Während sich die Recherchen von Nachrichtendiensten vor dem Internet weitgehend auf Printmedien, Radio und Fernsehen stützte, sind heute im Netz verfügbare Daten wichtige Anhaltspunkte für solche Nachforschungen.



So erklärt der Bundesnachrichtendienst zur Arbeit seiner OSINT-Spezialisten und -Spezialistinnen: „Meist steht am Anfang der nachrichtendienstlichen Arbeit die Auswertung von offen verfügbaren Informationen. Dazu gehören Informationen aus Fachzeitschriften wie auch aus Datenbanken. Unsere OSINT-Spezialisten können aber noch viel mehr: Mittels spezieller Recherchetools finden Sie in der Flut von offenen Informationen die für den BND relevanten Inhalte."

Doch längst nicht nur Nachrichtendienste untersuchen und analysieren offen im Internet verfügbare Daten – auch IT-Sicherheitsexperten, Rechercheverbünde, Journalisten und Menschenrechtsorganisationen setzen OSINT-Techniken ein, wenn auch zu unterschiedlichen Zwecken [1].

Mithilfe von OSINT-Tools können auch Sie öffentlich zugängliche digitale Spuren zusammentragen und sichten, zum Beispiel kompromittierte Logins und Passwörter, versehentlich im Netz gelandete Unternehmensinterna sowie Infos über Domains, Server und Mailadressen. Die Tools spüren sogar Daten aus dem Darknet, Inhalte aus sozialen Medien und bereits gelöschte Informationen auf.

Wie haben eine Auswahl nützlicher Dienste für Sie zusammengestellt. Alle genannten Tools finden Sie unter ct.de/w6e2 verlinkt.

Darknet-Recherchen

Nachforschen, ob eigene Daten und Passwörter im Darknet kursieren oder Recherchen über Dritte – all das geht mit **IntelligenceX**, einem seit 2018 bestehenden Dienst aus Tschechien, der sich als Suchmaschine und Archiv für Daten aus verschiedensten, auch schwer zugänglichen Quellen versteht.

IntelligenceX richtet sich nach Angaben des Betreibers vor allem an Regierungen und Unternehmen, aber auch an Journalisten, Recherchenetzwerke und Sicherheitsforscher. Die Bandbreite dessen, was Sie mit dem Dienst herausfinden können, ist entspre-

Malware-Analyse für Anfänger

Schadcode in einer Windows-VM Geheimnisse zu entlocken, klappt (fast) ohne Vorwissen. Mit dieser Schritt-für-Schritt-Anleitung richten Sie schnell und kostenlos eine sichere Analyseumgebung ein, in der Sie echten Schadcode untersuchen können.

Von **Olivia von Westernhagen**

Bild: solarseven/Shutterstock.com

Wer Malware analysieren will, scheint auf den ersten Blick nur zwei Optionen zu haben: Entweder er gibt sich mit Informationen zufrieden, die lokal installierte Virenwächter oder Online-Analysedienste wie etwa VirusTotal zurückliefern. Oder er wendet extrem viel Zeit auf, um Assembler zu lernen, schlecht dokumentierte Betriebssystem-Interna zu verinnerlichen und sich mit komplexen, oftmals teuren Reverse Engineering-Frameworks auseinanderzusetzen.

Sie haben auf letztere Option keine Lust, wollen sich aber ebensowenig vom Windows Defender mit Meldungen wie „Trojan:Win32/Vigorf.A“ abservieren lassen? Sie möchten die Analyse von Windows-Malware in die eigenen Hände nehmen, statt nur vorgefertigte Reports zu wälzen? Dann tun Sie das doch einfach! Windows-, Netzwerk- und idealerweise auch VirtualBox-Grundkenntnisse, eine ungefähre Vorstellung der Funktionsweise von Schadcode sowie ein gesunder Respekt vor den damit verbundenen Gefahren reichen, um als Anfänger loszulegen.

In diesem und den drei folgenden Artikeln begleiten wir Sie bei Ihren ersten Schritten. Für das Einrichten einer kostenlosen Analyseumgebung in Oracles VirtualBox verwenden wir eine frei verfügbare Windows-10-VM mit einer 90-Tage-Testlizenz. Wir erklären, wie Sie die virtuelle Maschine effektiv abschotten, um das Hostsystem vor ausbruchsfreudigen Schädlingen zu schützen. Außerdem stellen wir den Windows Defender ruhig und geben Tipps zur Tarnung der Test-VM als „normales System“ gegen Sandbox-Erkennungsmechanismen (siehe Seite 64).

Ist alles vorbereitet, lassen wir einige ausgewählte und besonders anfängerfreundliche Tools sowohl zur statischen als auch zur dynamischen Schadcode-Analyse in die frisch eingerichtete Umgebung einziehen (siehe Seite 70). Und wir erklären, wo Sie Malware-Samples herbekommen und wie Sie verantwortungsbewusst mit ihnen umgehen (siehe Seite 76).

Warum VirtualBox als Basis?

Dass es keine gute Idee ist, Schadcode direkt auf dem eigenen System (Host) auszuführen, bedarf wohl keiner weiteren Erklärung. Es gibt aber noch weitere gute Gründe für eine klare Trennung zwischen Analysesystem und normaler Arbeitsumgebung.

Indem man die Analyseumgebung als VM in einer Virtualisierungssoftware wie VMware oder eben VirtualBox als Gastsystem (Guest) auf dem Hostsystem anlegt, profitiert man von dem Konzept der Sicherungspunkte (engl. Snapshots). Zu solchen Momentaufnahmen des aktuellen Systemzustands kann man bei Bedarf jederzeit zurückkehren. Die „Systembereinigung“ im Anschluss an eine Schadcode-Ausführung ist somit innerhalb weniger Sekunden erledigt.

Ein frisch aufgesetzter Guest nebst jungfräulichem Desktop bietet zudem jede Menge Platz für die benötigten Tools. Hier lassen sie sich übersichtlich einsortieren, ohne dass diese Ordnung durch schon vorhandene „Alltags-Software“ gestört würde. Und was noch viel wichtiger ist: Weder persönliche Daten aus ebendieser Software noch der Host selbst