UNIVERSITY OF APPLIED SCIENCES

Fachbereich Informatik

Seminararbeit

IT - Security – POST Exploitation

Wintersemester 2016/2017

Eingereicht am:

30 November 2016

Eingereicht von:
Simon Nimmerjahn
Student Wirtschaftsinformatik
E-mail: winf100615@fh-wedel.de

Betreuer:
Prof. Dr. Gerd Beuster
Fachhochschule Wedel
Feldstraße 143
22880 Wedel
Tel.: 04103 - 80 48 - 38
E-Mail: gb@fh-wedel.de

Inhaltsverzeichnis

1 Einführung

1.1 Begriffserklärung

Wenn man über das Thema „IT - Security“ spricht, geht es in der Regel darum wie ein System durch einen Angriff von außen abgesichert werden kann. Aber diese Sichtweise reicht in den meisten Fällen nicht aus, da jedes System Sicherheitslücken hat und daher bei jedem System die Gefahr besteht, dass dieses von einem Angreifer übernommen wird. Die Verantwortlichen müssen sich daher auch mit der Frage beschäftigen, welches Risiko besteht wenn ein Angreifer ein System übernommen hat. In diesem Fall muss dafür sorge getragen werden, dass selbst wenn ein System infiltriert wurde, der Schaden gering bleibt. Allerdings können die Risiken vielseitig sein. Die meisten Angriffe gegen Firmennetzwerke verfolgen nicht mehr primär das Ziel Systeme zu zerstören, vielmehr sollen die Systeme nach Möglichkeit ungehindert weiterlaufen, damit der Angreifer so viele Informationen wie möglich sammeln kann.

Bereits im Jahre 2014 wurde der Schaden aufgrund von Wirtschaftsspionage laut dem Verein Deutscher Ingenieure auf jährlich 100 Milliarden Euro geschätzt. (vgl. nifis) Vor dem Hintergrund dieser Summen, erkennt man schnell das es für einen Angreifer wesentlich lukrativer ist, unbemerkt zu bleiben und die gesammelten Informationen zu nutzen oder weiter zu verkaufen.

Auch im politischen Umfeld sind solche Angriffe inzwischen angekommen. Auch hier ist das Sammeln von Informationen über die Politik eines Landes ein wichtiges Instrument um frühzeitig über politische Entwicklungen informiert zu sein. Bei dem sogenannten „Bundestag-Hack“ (vgl. heise) konnte zwar nicht zweifelsfrei ein Schuldiger ausfindig gemacht werden, es ist aber zu vermuten das dieser Angriff politisch motiviert war. Bei diesem Angriff wurden alle Arten von „Post Exploitation“, welche im nächsten Abschnitt beschrieben werden, verwendet um sich im Netz des Bundestages zu bewegen. In diesem Fall wurden als Abwehrmaßnahme alle Systeme im Bundestag ersetzt um den Angreifer so zu eliminieren.

Wie bereits angedeutet, beschreibt der Begriff „Post Exploitation“ Methoden mit denen sich ein Angreifer Zugriff auf das gesamte Unternehmensnetzwerk verschaffen kann, nachdem er einmal in das System eingedrungen ist. In dem Fall vom deutschen Bundestag ist dieses erste Eindringen durch das versenden einer Phishing Mail geschehen, wodurch der Angreifer einen einzelnen Rechener gekapert hat von dem aus er sich dann weiterbewegen konnte.

2

Arten von Post Exploits

In den folgenden Abschnitten werden die verschiedenen Arten von Post Exploits erläutert. Zur Erklärung wird hierfür auf Linux Server Systeme in Unternehmen verwiesen. Natürlich sind alle Angriffe, soweit nicht anders beschrieben, auch auf Windows Server Systemen und Clients möglich. Der Root User unter Linux ist vergleichbar mit dem Administrator unter Windows und hat die Möglichkeit auf alle Bereiche des Systems zuzugreifen. Daher ist dieser Benutzer besonders zu schützen.

2.1 Local Privilege Escalation

Nachdem ein System infiltriert wurde, hat der Angreifer in den meisten Fällen einen sehr begrenzten Handlungsspielraum, da die lokalen Systemrechte für den Angreifer minimal sind. Das hängt heutzutage damit zusammen, dass in modernen Betriebssystemen die Anwendungen standardmäßig nicht mit Root – Rechten laufen. Auf einem aktuellen Ubuntu Server wird z.B. der Webserver von dem Benutzer "www-data" ausgeführt. Dieser Benutzer hat auf dem System minimale Rechte, sodass dieser keinen Systemweiten Schaden anrichten kann.

Ein Angreifer möchte allerdings weitgehende Rechte auf einem System erlangen um größtmöglichen Zugriff auf alle Daten zu bekommen. Um dieses Ziel zu realisieren, ist der Angreifer auf Sicherheitslücken angewiesen mit denen ein lokaler Benutzer die Rechte eines anderen Benutzers, in der Regel die des Root Users, erlangen kann. In diesem Fall spricht man von einer "Local Privilege Escalation". Durch dieses Vorgehen kann der Angreifer alle weiteren Aktionen als Root User ausführen und so auf alle Bereiche des Systems zugreifen. Wenn es der Angreifer erst einmal soweit geschafft hat, hilft auch eine lokale Firewall nicht mehr weiter. Ein kluger Angreifer wird die Firewall zwar nicht komplett deaktivieren, allerdings kann er sich einen zusätzlichen Kommunikationskanal aufbauen mit dem er weiterhin auf das System zugreifen kann, obwohl das übersprüngliche Einfallstor bereits gepatcht wurde.

Beispiele für Angriffspunkte dieser Art gibt es viele und es werden regelmäßig Sicherheitslücken gefunden, durch die es für einen Benutzer möglich ist erweiterte Rechte zu erlangen. Das Problem bei diesen Sicherheitslücken ist allerdings, dass zum Schließen einer solchen Lücke der Kernel gepatcht werden muss und das geht aktuell noch nicht immer zur Laufzeit obwohl hier aktuell große Fortschritte gemacht werden. Durch den zwingenden Neustart eines Servers und der damit verbundenen Downtime werden diese Sicherheitslücken speziell auf internen Systemen häufig erst spät oder gar nicht geschlossen. Das ist zum Schutz gegen Angriffe von außen auch deutlich weniger relevant als das Patchen der Server welche direkt im Internet stehen, allerdings sollte dieser Punkt bzgl. eines internen Angriffs beachtet werden.

Hierbei ist allerdings zu beachten, dass jegliche Sicherheitspatches im Vorwege auf deren Funktionalität getestet werden müssen. Patches jeglicher Art sollten immer zuerst auf Test- und Entwicklungsmaschinen installiert werden bevor diese auf produktiven Systemen zum Einsatz kommen.

2.2 Local Information Gathering

Nachdem der Angreifer Zugriff auf das System hat und sich gegebenenfalls mittels „Privilege Escalation“ die notwendigen Rechte verschafft hat, verfolgt dieser beim „Local Information Gathering“ das Ziel, so viele Informationen wie möglich von dem gekaperten System zu beschaffen. Insbesondere Passwörter sind für das weitere Vorgehen von hohem Interesse. Hierbei kommt es auch nicht darauf an ob diese gehasht sind oder im Klartext vorliegen, da auch gehashte Passwörter zu einem späteren Zeitpunkt geknackt werden können. Dieses Vorgehen konnte in der jüngsten Vergangenheit bei dem LinkedIn Leak (vgl. urfas) beobachtet werden. Die Passwörter wurden bereits im Jahre 2012 entwendet und sind erst 2016 als Klartext Passwörter wieder aufgetaucht. Das Problem an diesem Leak ist, dass viele Nutzer auch noch ca. 4 Jahren immer noch das gleiche Passwort verwendet haben.

Ein einfaches Vorgehen um Passwörter auf einem System zu finden, ist es nach Dateinamen oder Zeichenketten zu suchen. Dateien dieser Art lassen sich unter Linux mit den Befehlen

```
$ find / -name '*passwd*' -o -name '*password*'
$ grep -iR password /*
```

auf dem System finden. Diese Befehle sollen hier nur als Beispiel dienen und lassen sich natürlich beliebig erweitern und modifizieren. Mit dieser einfachen Suche ist der Angreifer in vielen Fällen sehr erfolgreich, da in einfachen Skripten die Passwörter häufig im Klartext stehen. Auf Windows Systemen wurden beispielsweise die Passwörter für FTP Logins, welche man in der Anwendung FileZilla hinterlegt hat, immer im Klartext gespeichert. Dadurch hatte der Angreifer automatisch Zugriff auf alle FTP Konten.

Wenn der Angreifer über die Suche nach Passwörtern nicht erfolgreich war, ist es für ihn allerdings ein einfaches einen Keylogger zu aktivieren und damit alle Eingaben des Benutzers aufzuzeichnen. Das ist besonders auf Client Systemen eine sehr effektive Maßnahme. Insbesondere die Systeme der Administratoren sind hier gefährdet, da der Angreifer durch die eingegebenen Benutzer und Passwort Kombinationen schnell Zugriff auf das gesamte Unternehmensnetzwerk bekommen kann.

Eine weitere Informationsquelle ist die Bash History unter Linux. In dieser werden nach dem Abmelden alle Eingaben geschrieben die der Nutzer während der Session getätigt hat. Häufig finden sich daher in dieser Datei Passwörter die z.B. als Parameter übergeben wurde. Des Weiteren sind auch Benutzer Accounts und Gruppenzugehörigkeit interessante Informationen um sich ein Bild über das angegriffene Unternehmen zu verschaffen. Hierüber können detaillierte Informationen über den Aufbau und die Struktur eines Unternehmens gesammelt werden. Mit diesen gesammelten Informationen kann der Angreifer im nächsten Schritt versuchen weitere Systeme eines Unternehmens zu infizieren.

2.3 Lateral Movement

Nachdem zuvor notwendige Informationen und im besten Fall auch Passwörter gesammelt wurden, geht es jetzt darum den Angriff auf weitere Systeme auszuweiten. Die meisten Anwender haben den gleichen Benutzer und das gleiche Passwort auf allen Systemen. Dabei ist es unerheblich ob es sich um eine Unternehmensweite Domäne handelt oder nicht. Wenn der Angreifer nun Benutzer und Passwort kennt, kann er sich auf weitere Systeme einloggen. Es ist sehr wahrscheinlich das die Systeme einen ähnlichen Patchstand haben wodurch jedes System die gleichen Sicherheitslücken aufweist. Alternativ zu dem Passwort reicht es dem Angreifer in einigen Fällen auch, wenn er nur den Hash kennt. Unter Windows wird bei der Authentifizierung via SMB nur der Hash übertragen. Das Remote – System geht in dem Fall davon aus, dass der User den Hash nur haben kann wenn dieser auch das Passwort kennt. Diesen Hash kann der Angreifer allerdings durch "Local Information Gathering" in Erfahrung bringen und muss sich in diesem Fall nich mal mehr die Mühe machen das Klartext Passwort zu ermitteln. Das selbe Prinzip gilt auch bei der Verwendung von Token mit denen sich Windows Systeme und Prozesse untereinander authentifizieren, damit der Benutzer nicht jedesmal wieder sein Passwort eingeben muss. Wenn es dem Angreifer gelingt diesen Token in seinen Besitz zu bringen, kann er ohne Kenntnis von Benutzer und Passwort auf weitere Systeme zugreifen.

Auch auf Linux Systeme kann der Angreifer ohne Kenntnis des Passwortes gelangen. Viele Linux Benutzer nutzen einen SSH Key zur Authentifizierung. In dem Fall liegt auf dem Remote Server der Public Key und auf dem Client der Private Key. Wenn der Angreifer nun in den Besitz des Private Keys gelangt, kann er auf alle Systeme Zugreifen auf denen der entsprechende Public Key hinterlegt ist. Daher ist der Private Key bestmöglich zu schützen und sollte auf jeden Fall durch ein Passwort gesichert werden. Wenn der Angreifer allerdings einen Keylogger verwendet hilft diese Sicherheitsmaßnahme auch nicht weiter.

2.4 Pivoting

Häufig befindet sich der Angreifer auf Web- oder Email-Servern, da diese direkt aus dem Internet erreichbar sind. Wenn sich der Angreifer also auf einem Email Server befindet, hat er ggf. bereits einen großen Datenpool um Informationen über das Unternehmen zu erhalten. In der Regel werden solche Informationen allerdings nicht auf Servern gespeichert welche direkt in der DMZ stehen und dadurch aus dem Internet erreichbar sind. Vielmehr werden diese Daten auf internen Systemen gespeichert. Der Angreifer steht daher vor der Herausforderung auf interne Systeme Zugreifen zu können. Ein direkter Zugriff sollte immer durch eine externe Firewall abgesichert sein, sodass der Angreifer nicht ohne weiteres auf interne Netze Zugreifen kann. Der Angreifer ist daher gezwungen Sicherheitslücken in den Applikationen zu finden welche aus der DMZ mit internen Anwendungen kommunizieren.

Damit der Angreifer die externe Firewall nicht umgehen kann, sollte man bei der Konfiguration eines Servers immer darauf achten, dass sich das System nicht in unterschiedlichen Netzen befindet. Falls das doch der Fall sein sollte, kann der Angreifer dieses System nutzen um auf das andere Netzsegment zugreifen zu können. Das gilt aber nicht nur für Server sondern auch für Clients. Auch diese sollten nicht vollumfänglich auf alle Netzsegmente Zugreifen dürfen. Wenn der Client z.B. auf die Intranet Seite Zugreifen soll und diese sich in einem anderen Netzsegment befindet, sollte in der Firewall auch nur der Port 80 bzw. 443 freigegeben werden. Dieses Vorgehen erschwert es den Angreifer auf die Systeme zugreifen zu können.

2.5 Persistence

Der Angriff findet in der Regel nur im Speicher statt. Sprich sobald das System heruntergefahren wurde verliert der Angreifer seine Session und hat keinen Zugriff mehr auf das System. Durch das "Lateral Movement" hat der Angreifer zwar die Möglichkeit auf mehreren Systemen aktiv zu sein, es bleibt aber das Risiko das er seine Session verliert. Daher muss er sich überlegen inwiefern er auch zu einem späteren Zeitpunkt wieder Zugriff erlangen kann. Besonders auf Client Systemen welche in der Regel am Ende des Arbeitstages heruntergefahren werden, ist es das für den Angreifer enorm wichtig. Eine Möglichkeit ist es daher, einen Task zu bauen welcher beim Starten des Systems ausgeführt wird. Dieser kann automatisch eine Session zum System des Angreifers aufbauen damit dieser wieder Zugriff hat.

Ein weiteres Problem für den Angreifer besteht darin, dass der Benutzer seine Passwörter ändert. Um dieses Problem zu umgehen muss sich der Angreifer einen eigenen Benutzer erstellen um sich dauerhaft auf dem System einloggen zu können. Wie man allerdings gerade feststellen kann, muss der Angreifer das erste mal Änderungen an dem System vornehmen und riskiert dadurch entdeckt zu werden. Da er das unter allen Umständen verhindern möchte, wird der Angreifer versuchen möglichst viele Sessions zu unterschiedlichen Systemen aufzubauen um beim Verlust einer Session nicht den Zugriff auf das Unternehmen zu verlieren. Eine sehr effiziente Abwehrmaßnahme für Systemverantwortliche ist es daher den Strom abzuschalten und danach alle Systeme wieder hochzufahren.

3 Gegenmaßnahmen

3.1 Allgemein

Angriffe dieser Art abzuwehren ist sehr schwer, denn jede Software die eigesetzt wird hat Sicherheitslücken. Es kann daher fast nie ausgeschlossen werden, dass ein System gehackt wird. Es gilt für ein Unternehmen daher die Anforderung, dass solche Angriffe frühstmöglich entdeckt werden. Besonders in großen Unternehmen ist dieses eine Herausforderung und es vergehen oft Wochen oder Monate bis ein Angriff entdeckt wird. Nachdem ein Angriff festgestellt wurde hilft es allerdings nicht mehr das infizierte System abzuschalten, häufig hat der Angreifer durch "Lateral Movement" und "Pivoting" viele weitere Systeme in unterschiedlichen Netzsegmenten infiziert.

So geschehen bei Thyssen Krupp (vgl. Ber16), die den Angriff und ihr Verhalten öffentlich gemacht haben. Hier hat sich ein Angreifer im Februar 2016 Zugriff auf das Unternehmensnetzwerk verschafft und wurde im März von der IT Security Abteilung der Firma entdeckt. In dem von der Wirtschafts Woche veröffentlichten Bericht ist sehr gut zu erkennen, wie ein Angreifer vorgeht und wie schwer es ist ihn ausfindig zu machen. Entdeckt wurde der Angreifer aufgrund eines ungewöhnlichen Dateinamens welcher verwendet wurde um beim "Lateral Movement" weitere Systeme zu infizieren. Der Angreifer hat in diesem Fall durchaus Spuren auf den Systemen hinterlassen, diese aber beim verlassen dieser sofort wieder gelöscht. Daran sieht man, dass ein Angreifer gar kein Interesse hat jederzeit auf jedes System zugreifen zu können und sich darauf permanent einzunisten, vielmehr ist sein wichtigstes Anliegen möglichst lange unentdeckt zu bleiben.

Abgewehrt wurde dieser Angriff erst im Oktober 2016, nachdem das ganze Unternehmensnetzwerk kontinuierlich gescannt und der Angreifer beobachtet wurde. Die Verantwortlichen bei Thyssenkrupp hatten sich bewusst gegen offensive Maßnahmen entschieden, da so der Angreifer gewarnt worden wäre und sich ggf. versteckt hätte. In dem Fall wäre das Unternehmen nicht in der Lage gewesen abschließend sicher zu sagen ob sie den Angriff eliminiert haben.

In dem Artikel wird weiterhin deutlich, dass IT-Security viel Geld kostet. Zwar steigen die Ausgaben der Unternehmen in diesem Bereich, aber die wenigsten Unternehmen leisten sich eigene Abwehrzentren (vgl. Ber16). Der Angriff bei Thyssenkrupp zeigt wie wichtig es besonders für große Unternehmen ist, Geld und Personal in eine effiziente IT - Security Abteilung zu investieren.

3.2 Regeln

Der Blogger Brian Krebs hat in seinem Blog Regeln aufgestellt (vgl. Kre) um das Risiko eines erfolgreichen Angriffs möglichst gering zu halten. Diese Regeln gelten nicht explizit für "Post Exploition" sondern sind Regeln die jeder beherzigen sollte. Dabei ist es irrelevant ob er sich in einem Unternehmen oder Privat in seinen eigenen vier Wänden aufhält.

Die Regeln lauten wie folgt:

"If you didn't go looking for it, don't install it!"
Mit der ersten Regel sagt Krebs, dass man keine Software installieren sollte, die einem auf einer Website zum Download angeboten wird um diese Seite nutzen zu können. Zum Beispiel einen Codec um ein Video abzuspielen. Jegliche dieser Software sollte wenn möglich direkt von der Herstellerseite heruntergeladen werden. Generell gilt bei dieser Regel, wenn man nicht nach der Software expliziet gesucht hat und zum Beispiel eine Webseite sie trotzdem anbietet, sollte man diese nicht installieren.

"If you installed it, update it."
Diese Regel ist vermutlich eine der wichtigsten. Angreifer nutzen Sicherheitslücken aus. Das heißt sobald eine Sicherheitslücke bekannt ist wird diese auch ausgenutzt. Es ist daher zwingend erforderlich das jegliche Software die eingesetzt wird schnellstmöglich gepatcht wird.

"If you no longer need it, remove it"
Wenn man diese Regel befolgt verringert sich das Risiko eines Angriffs aufgrund einer geringen Anzahl von Angriffspunkten. Jegliche Software die nicht mehr verwendet wird sollte umgehend deinstalliert werden. Denn nur in Software welche auf dem System vorhanden ist können Sicherheitslücken ausgenutzt werden. Durch dieses Vorgehen verringert sich außerdem die Anzahl der Software welche gepatcht werden muss.

4

Intern / Extern

4.1 Interner Angriff

Unter einem externen Angriff versteht man den Angriff von außen, sprich von jemandem der nicht direkten Zugriff auf das Unternehmensnetzwerk hat. Bei allen Sicherheitsplanungen sollte allerdings auch immer ein Angriff von intern bedacht werden. Ein Mitarbeiter welcher das Unternehmen wechseln möchte oder jemand der gekündigt werden soll, stellt ein potentielles Sicherheitsrisiko für ein Unternehmen dar. Durch Zugriffsrechte auf Unternehmensinterna kann es hier zu einem erheblichen Schaden in Form von Wirtschaftsspionage kommen. Daher ist darauf zu achten das auch Mitarbeiter mit möglichst wenig Rechten ausgestattet werden und das diese nur Zugriff auf Systeme bekommen die sie für ihre tägliche Arbeit zwingend benötigen. Ein regelmäßiges Audit der Rechte aller Benutzers ist zwingend erforderlich.

Als Beispiel wird an dieser Stelle gerne der Benutzeraccount eines Auszubildenden herangezogen. Dieser wechselt während seiner Ausbildung mehrmals die Abteilung und wird jedesmal mit den entsprechenden Rechten versorgt. Das führt häufig dazu, dass der Auszubildende am Ende der Ausbildung mehr Rechte hat als jeder andere Mitarbeiter.

Durch ein "minimale – Rechte – Prinzip" können diese Probleme gelöst werden und durch Anwendung dieses Prinzips wird es auch einem externen Angreifer erschwert sich innerhalb des Unternehmensnetzwerkes zu bewegen.

5 Beispiele

5.1 Dirty Cow

Ende Oktober wurde eine Local Privilege Escalation Lücke im Linux Kernel gefixt. Diese Lücke bestand seit über 9 Jahren, konnte aber erst durch die Weiterentwicklung des Kernels in den letzten Jahren einfacher ausgenutzt werden. Bei dieser Sicherheistlücke kann ein Benutzer nicht direkt die Rechte des Root Benutzers erlangen, allerdings hat er die Möglichkeit alle Dateien zu überschreiben für die er Leserechte besitzt. (vgl. Sch)

Unter Linux ist das Rechte System zwar einfach aber sehr effizient gebaut. Ein Benutzer kann für eine Datei Leserechte, Schreibrechte und das Recht zum ausführen dieser Datei haben. Das gleiche gilt auch für Verzeichnisse. Es wird zusätzlich zwischen dem Benutzer, der Gruppe oder allen Benutzer auf dem System. Für unsere Sicherheitslücke bedeutet dies, dass sobald eine Datei Leserechte für alle Benutzer auf dem System besitzt kann diese von jedem Benutzer auch bearbeitet werden. Dieses gilt z.B. für die Datei "/etc/group" in der die Gruppenzugehörigkeit der Benutzer geregelt wird. Durch das bearbeiten dieser Datei kann der Angreifer seinem aktuellen Benutzer Root – Rechte verschaffen.

Zusätzlich zu den oben genannten Datei- und Verzeichnisrechten ist es möglich Access Listen für hierfür zu hinterlegen. Damit kann man die Rechte für Dateien und Verzeichnisse granularer gestalten um so die Sicherheit zu erhöhen. Es ist mit ACLs zum Beispiel möglich zwei Benutzern volle Rechte an eine Datei zu geben, ohne das die Gruppe irgendwelche Rechte besitzt.

Quellenverzeichnis

[Ber16] Jürgen Berke. Im Auge des Sturms. *Wirtschafts Woche*, 51, 2016.

[Hei] Heise.de. Bundestags-Hack. Website. Online erhältlich unter https://www.heise.de/thema/Bundestags_Hack; abgerufen am 11. Dezember 2016.

[Kre] Brian Krebs. Krebs's 3 Basic Rules for Online Safety. Website. Online erhältlich unter https://krebsonsecurity.com/2011/05/krebss-3-basic-rules-for-online-safety; abgerufen am 11. Dezember 2016.

[NIF] NIFIS. Wirtschaftsspionage: 100 Milliarden Euro Schaden bringt Bundesregierung in Zugzwang. Website. Online erhältlich unter http://http://www.nifis.de/veroeffentlichungen/news/datum/2014/08/01/wirtschaftsspionage-100-milliarden-euro-schaden-bringt-bundesregierung-in-zugzwang; abgerufen am 03. Dezember 2016.

[Sch] Fabian A. Scherschel. Dirty Cow: Linux-Rechteausweitung wird für Angriffe missbraucht. Website. Online erhältlich unter https://www.heise.de/security/meldung/Dirty-Cow-Linux-Rechteausweitung-wird-fuer-Angriffe-missbraucht-3356639.html; abgerufen am 10. Dezember 2016.

[UR] Fabian A. Scherschel Uli Ries. Linkedin-Hack: 117 Millionen Passwort-Hashes zum Download aufgetaucht. Website. Online erhältlich unter https://www.heise.de/security/meldung/LinkedIn-Hack-117-Millionen-Passwort-Hashes-zum-Download-aufgetaucht-3224212.html; abgerufen am 12. Dezember 2016.

[Wei14] Georgia Weidman. *Penetration Testing.* no starch press, 2014.