



Hacking-Lab – das mobile Sicherheitslabor

Hacking-Lab ist eine der kreativsten mobilen Lernumgebungen für Security-Consultants, Security-Analysten, Administratoren und Software-Entwickler – ein Security-Labor zum Anfassen mit Sicherheitspraxis anstatt endloser Power-Point-Präsentationen. Hacking-Lab erlaubt es legal individuelle Hacking-Angriffe zu testen, ohne öffentliche Systeme zu schädigen. Ein Erfahrungsbericht von Sicherheitspezialist Benjamin Mejri, der am letzten Hacking-Lab-Event nach dem Motto »Hack & Learn« teilgenommen hat.

Hacking-Lab basiert auf einem Konzept, das von der Schweizer Firma Compass Security AG entworfen wurde. Die Idee besteht darin, dass man die Methoden und Verfahren der Hacker kennen muss, um sich adäquat schützen zu können. Dafür steht ein umfangreiches mobiles Security-Labor zur Verfügung, mit dessen Hilfe der Teilnehmer nach seinen eigenen Bedürfnissen und Wünschen Security-Themen kennen lernen und vertiefen kann. Dazu wählt man ein bestimmtes Thema aus und versucht ei-

nen so genannten Case, auch Wargame, Security-Rätsel, Fälle oder Hacking-Challenge genannt, zu lösen. Durch den praktischen Bezug lernt man die realen Schwachstellen und Gegenmaßnahmen kennen.

Die Art der Wargames ist breit gefächert, so dass jeder Teilnehmende seinem Know-how entsprechend in verschiedenen Schwierigkeitsgraden die vorgegebenen Fälle durchspielen und lösen kann. Ein Case ist eine Aufgabe im Hacking-Lab, welche aus drei Teilen besteht, die dem

Teilnehmenden das zu lösende Wargame erläutert. Zu jedem Case gibt es eine Beschreibung der Aufgabenstellung und eine Definition der entsprechenden Umgebung. Danach folgen die »Requirements«, welche die Voraussetzungen für die Absolvierung des Wargames festlegen. Meist benötigt man lediglich Basis-Software wie Browser, Sniffer, Web-Proxies aber auch Vmware-Player oder die Backtrack-Live-CD, um im Hacking-Lab zu arbeiten.

Der letzte und wichtigste Bereich eines Cases ist das Goal. Hier wird klar definiert, wann ein Wargame als gelöst gilt. Die Lösung wird den Betreuern mitgeteilt, wofür man Bewertungspunkte bekommt, die sich im aktuellen Event-Ranking darstellen. Die Punktevergabe dient vorrangig dem eigenen Ansporn und dem Erwerb des Zertifikats. Aber auch denjenigen, die sich mit den anderen Teilnehmenden messen wollen und als Tagessieger beziehungsweise als Top 10 für den Meisterschafts-Event qualifizieren wollen.

Punkte und Schwierigkeitsgrade

Die Punktevergabe orientiert sich nach dem Schwierigkeitsgrad der Aufgabe und liegt zwischen 5 und 30 Punkten pro Case. Nach dem Absolvieren eines Cases bekommt der Teilnehmende die Punkte über eine QR-Code-Plakette (Ausweis) auf seinen Account gutgeschrieben. Dazu wird die Plakette mit einem Mobiltelefon gescannt und so die Punkte in das Rankingsystem

2310 Web Security: SQL-Injection with UNION

You probably already read about SQL-Injection in security journals. Web applications which are bound to databases use Standard Query Language to access the database. These queries are often built depending on the users' input. However, if the input is not properly validated then a client may modify the dynamically created statement and influence the result set or even inject commands.

Requirements

Web Browser (Firefox)

Goal

Inject SQL code into the search form and try to gain full access to confidential customer data which is stored in the database (e.g. credit card numbers, passwords).

Wargame SQL-Injection: Vorgabe des Hacking-Labs

übertragen. Die aktuelle Rankinglist der Top 50 wird laufend auf Videowänden angezeigt.

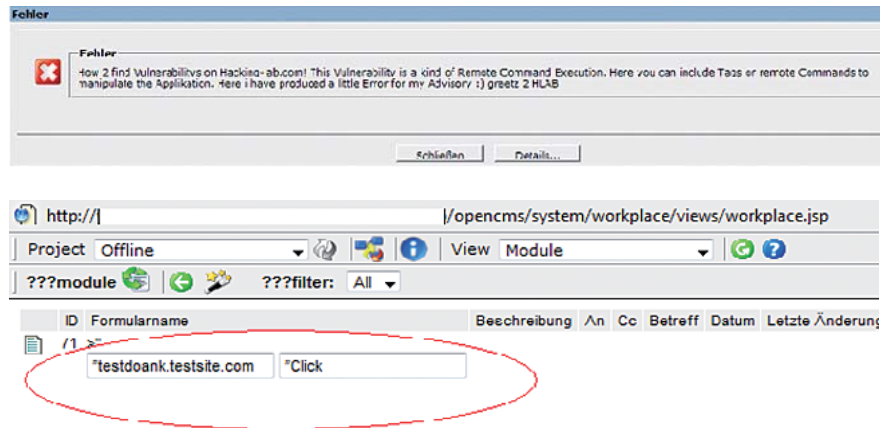
Die einzelnen Schwierigkeitsgrade sind klar definiert: so kann man sich an Aufgaben von leicht über mittel bis hin zu schwer wagen. Als Beispiel für eine leichte Aufgabe würde ich den Case »Passwortgeschützte ZIP-Dateien« bezeichnen. Dabei geht es darum an den Inhalt einer Passwort-geschützten ZIP-Datei zu gelangen. Da sich diese Aufgabe in Minuten oder Sekunden lösen lässt, ist sie für Anfänger ein komfortabler Einstieg. Als Cases mittleren Niveaus würde ich SQL-Injection-Attacken oder Cross-Site-Lücken empfehlen. Hier kann man über kombinierte Angriffe schnell und gut Punkte holen, die einen dann im Ranking nach oben katapultieren. Interessant ist auch der Lock-Picking-Bereich, bei dem es Schlösser in drei verschiedenen Schwierigkeitsgraden zu knacken gilt. Für die einfache Variante bekommt man bereits 10 Punkte, für das schwerste Schloss 30 Punkte.

Doch zurück zum eigentlichen Hack & Learn. Die Experten von Compass haben in diesem Jahr zahlreiche neue Wargames dazu entwickelt. Mit den unterschiedlichsten Taktiken versuchten die Probanden die Wargames zu lösen und manchmal war auch einen Compass-Experte sehr erstaunt über neue Lösungswege, an welche bisher noch niemand gedacht hat. Der Gedankenaustausch und die Team-orientierte Vorgehensweise (Teams lassen sich jederzeit bilden) unterstreicht das Lernen und den Erfolg als Gruppe.

Auch für die absoluten Cracks haben die Entwickler des Hacking-Lab einige Spielereien in petto: Nur mit einer Goal-Vorgabe galt es, die Internetseite des Hacking-Lab auf Sicherheitslücken zu untersuchen. Bei dieser Aufgabe gibt es keine Tipps oder Tricks und keine Hilfestellung der Betreuer. Um Punkte zu erbeuten, musste der Teilnehmende intuitiv vorgehen und aktiv mit »Research«-Methoden versuchen, die Umgebung auszukundschaften. Auch diese Aufgabe wurde gelöst: schlussendlich über ein Command-Execution im CMS vom Hacking-Lab mit netten Grüßen vom Finder der Lücke in der entsprechenden Fehlermeldung.

Ein weiteres Beispiel für eine schwierige Challenge ist die Domain-Admin-Privilege-Aufgabe. Hierbei geht es darum innerhalb eines Microsoft-Active-Directory die Rechte auf Enterprise-Admin zu erhöhen. Der Schwierigkeitsgrad dieser Challenge ist um einiges höher als bei anderen Aufgaben.

Wie man sieht ist für Jeden etwas dabei und die Erweiterung des eigenen Know-how ist oberstes Ziel. Von Authentication-Bypass über Request-Forgery bis hin zu Manipulationen von schnurlosen Telefonen sind die Cases so kreativ



Gelöst: mit den besten Grüßen ans Hacking-Lab

und umfangreich, dass jeder Teilnehmer mehrmals auf seine Kosten kommt. Durch die große Auswahl an Hacking-Wargames ist sichergestellt, dass sich die Teilnehmer dort weiterbilden können, wo deren Interessen oder Handlungsbedarf besteht.

Denkweisen und Techniken

Wer sich ausschließlich mit Level-3-Aufgaben auseinandersetzt, hat insgesamt einen größeren Freudentaumel, wenn die Aufgabe gelöst ist, aber es besteht natürlich auch die Gefahr von Frustration oder Misserfolg. Trotz längerem Suchen und Stöbern, dem Ausprobieren von diversen Angriffen kann ein Wargame trotzdem nicht gelöst werden. In solchen Fällen sollte man die Hacking-Lab-Betreuer aufsuchen. Sie geben zwar keine Step-by-Step-Anleitungen ab, sondern wichtige Inputs, um wieder in die richtige Richtung gelenkt zu werden.

Das ist auch mit ein Grund, warum so viele Administratoren und IT-Verantwortliche die Security-Wargames von Hacking-Lab besuchen, weit über die Grenzen der Schweiz hinaus. Entweder sie kommen wegen den Wargames oder aber auch wegen der zahlreichen Vorträge und Workshops, die parallel im Hacking-Lab laufen. Schlussendlich entsteht so für den Teilnehmenden eine Lernumgebung, die einen schneller voran bringt als konventionelle Methoden. Selbst Security-Neulinge konnten durch die vermittelten Inhalte der Vorträge und Workshops einige Level-1-Cases lösen und wussten danach sehr genau, wo sie in ihrem Netzwerk die Löcher stopfen müssen.

Lerneffekte und Bildung

Mittlerweile sind wir im Jahr 2009 der Technik angekommen und die Zeit der konventionellen Lernmethoden auf diesem Gebiet stoßen an ihre Grenzen. Um diese Grenze sauber zu passieren, gibt es nur wenige Möglichkeiten. Wenn ein Unternehmen beispielsweise einen

Chemiker ausbilden möchte, schickt er diesen in ein Labor, damit er in einer sicheren Umgebung lernen, forschen und produktiv arbeiten kann. Gleiches sollte auch für einen Sicherheitsverantwortlichen im Unternehmen gelten. Denn »Schulbank-Know-how« ohne Praxis und Erfahrung reicht in punkto Sicherheit gegen eine Vielzahl kreativer Gegner und Gefahrenpotenziale nicht.

Genau hier kommt das Hacking-Lab zum Einsatz. Durch die spielerische Herangehensweise, klar definierten Aufgaben bei den Wargames, hochkarätigen Vorträgen und Workshop ist der Lerneffekt um ein Vielfaches höher als bei konventionellen Schulungen. Der Teilnehmende hat hinterher meist schon ganz klare Vorstellungen, wo es auch in seinem Netzwerk brennt und vor allem welche Maßnahmen er einleiten muss.

Außerdem sind Events wie der »Swiss Cyber Strom« oder auch künftig die »Attack & Defense«-Veranstaltungen keine Szene-Events im Dunklen, sondern im Licht: Man hat den Eindruck, als sitze man in einer Universität in einem neuen Lernfach voll mit Sicherheitstechnikern. Der Lerneffekt eines solchen Events ist für mich persönlich sehr erstaunlich und ich kann nur jedem empfehlen, es selber einmal auszuprobieren.

*Benjamin Mejri ist seit einigen Jahren als Security-Analyst und Penetrationstester für öffentliche Sicherheitsunternehmen tätig. Seine Spezialgebiete sind technische Sicherheitsprüfungen, Malware-Analysen, Vorträge und Workshops zum Thema IT-Sicherheit. Durch seine Arbeit als Penetrationstester und Analyst wurden viele Open- & Closed-Source-Applikationen sowie -Services sicherer gestaltet.
E-Mail: x01445@gmail.com*