binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main

Abriss von Penetration Testing

Als Penetrationstester werden Sie sich der spannenden Aufgabe stellen, Sicherheitsanalysen von IT-Systemen durchzuführen. Dabei entstand unser Aufgabengebiet mehr oder weniger als eine Art Gegenmaßnahme seitens der IT-Sicherheit im Wettrüsten gegen die Angreifer. Potenzielle Auftraggeber bitten bzw. beauftragen uns mit der Identifikation der Schwachstellen ihrer IT-Systeme, um diese am Ende härten zu können. Doch welche Technologien müssen wir im Detail überprüfen?

Vorreiter in Sachen Sicherheit von Webanwendungen ist die Non-Profit-Organisation Open Web Application Security Project (OWASP). In ihrem Projekt OWASP TOP 10 listen sie die zehn häufigsten Schwachstellen in Webanwendungen auf (`https://owasp.org/www-project-top-ten/`).

Die Ergebnisse unseres Pentests sollten wir in einem abschließenden Bericht festhalten. Dieser Bericht ist letztlich das Dokument, welches unser Auftraggeber in seinen Händen halten wird. Aus diesem Grund sollte die Berichterstellung von uns einen besonderen Stellenwert erhalten. Sofern wir eine Schwachstelle identifiziert haben, wird aufseiten des Auftraggebers im Management eine Entscheidung getroffen werden müssen, wie mit dem Risiko verfahren werden soll. Im idealen Fall soll die Sicherheitslücke von Softwareentwicklern oder IT-Administratoren geschlossen werden. Folglich muss unser Bericht sowohl für die Personen mit starkem IT- als auch mit geringem IT-Hintergrund verfasst werden. Dies wird üblicherweise über die Aufteilung in eine Managementübersicht und einen technischen Bericht realisiert. Beide listen alle identifizierten Schwachstellen auf, unterscheiden sich aber in der Intention des Verfassers. In der Managementübersicht muss die Schwere der Risiken von Schwachstellen deutlich werden, wohingegen im technischen Bericht die Detailbeschreibung im Vordergrund steht, die folgende Aspekte umfassen sollte:

- Beschreibung der Schwachstelle
- Beschreibung der Auswirkungen
- Proof of Concept
- Empfehlung zur Behebung

Challenge: Identifizieren Sie zwei Schwachstellen der OWASP TOP 10 in einem ihrer verwundbaren Webanwendungen (s. `https://owasp.org/www-project-vulnerable-web-applications-directory/`), erstellen Sie einen abschließenden „Penetrationstestbericht“ und senden Sie diesen verschlüsselt via GPG per E-Mail an ds@binsec.com. Der zugehörige Public Key wurde zu diesem Zweck auf einem öffentlich erreichbaren Keyserver hinterlegt.

Hinweise:

1. Sie benötigen für das o.g. Szenario mind. 1 Angreifersystem und 1 Zielsystem.
2. Sie können alle Server mit VirtualBox erzeugen. Da die Server sich gegenseitig erreichen und weiterhin Programme nachinstalliert werden müssen, eignet sich als Netzwerkkonfiguration die VBox-Einstellung „Nat-Netzwerk“.
3. Als Angreifermaschine können Sie Kali Linux verwenden. Kali Linux ist eine kostenlose Penetration-Testing- und Security-Auditing-Linux-Distribution (Debian Derivat, basiert auf Debian Testing), welche mehr als 300 Pentest-Tools sowie vorinstallierte Dienste wie Apache beinhaltet. Die ISOs oder auch vorgefertigte VMs können unter https://www.kali.org/downloads/ heruntergeladen werden. Eine Einführung in Kali Linux fnden Sie unter `https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf`
4. Eine mögliche Gliederung könnte wie folgt aussehen:
    - Deckblatt
    - Inhaltsverzeichnis
    - Vorwort
    - Managementübersicht
    - Technischer Bericht