DOCUMENTATION- AND CODING-GUIDELINES

SECURITY WORKBENCH WS 2016/17

Inhaltsverzeichnis

Änderungshistorie

Version	Tätigkeit	Name	Datum
1.0	Initiale Erstellung	Nadine Zaffrahn	26.10.2016

1. Vorwort

Die Security-Workbench besteht im Kern aus zwei Elementen:

- Dokumentation als PDF-Dokument.
  In der Dokumentation werden zum einen fachliche Grundlagen für ausgewählte Angriffsszenarien auf IT-Systeme vermittelt und zum anderen die Benutzung der Security-Workbench (Installation und Starten der Workbench sowie Arbeiten mit den Tools und Skripten) detailliert beschrieben.
- Skripte und Tools in einer Kali-Linux-Maschine
  Innerhalb einer virtuellen Kali-Linux-Maschine sind verschiedene Tools und Skripte hinterlegt. Mithilfe dieser Tools und Skripte können die in der PDF-Dokumentation erklärten Angriffsszenarien durchgespielt werden.

Ziel der Security-Workbench ist es, Interessierten und Anfängern einen Einstiegspunkt zum Thema IT-Security zu geben. Daher ist es notwendig, die Bedienung und Dokumentation an den zu erwartenden Vorkenntnissen auszurichten.

2. Layout der PDF-Dokumentation

Das grundlegende Layout der PDF-Dokumentation ist durch die zugrundeliegende LaTeX-Vorlage (siehe document.tex bzw. document.pdf) weitestgehend vorgegeben.

Fachliche Themen sind i.d.R. in 4 Teilbereiche untergliedert. Zunächst werden Grundlagen im Abschnitt „Erklärung“ vermittelt. Dazu gehört die Art der Attacke theoretisch zu erklären.

Im anschließenden Kapitel „Vorbereitungen“ werden alle notwendigen Maßnahmen beschrieben, die vor der Durchführung der Beispielskripte abgeschlossen sein müssen (Tools, zusätzliche Einstellungen, Hardware, Anzahl beteiligter Rechner, …). Hier ist auch auf eventuelle Risiken einzugehen (z.B. DNS-Spoofing im eigenen Netzwerk auszuprobieren ist ok, in öffentlichen Netzwerken (Cafés etc.) oder Hochschul- bzw. Firmennetzwerken ist dies jedoch illegal und daher nicht empfehlenswert).

Der Abschnitt „Ablauf“ erklärt dem Leser, wie er den beschriebenen Angriff selbst durchführen kann. Zu beschreiben ist dabei die Ausgangslage, alle notwendigen Schritte (z.B. Ausführung des Skriptes) mit genauen Beschreibungen der Aufrufparameter und den dadurch ausgelösten Aktionen.

Der Abschnitt „Gegenmaßnahmen“ enthält Hinweise zum Erkennen des beschriebenen Angriffs und der Absicherung des Systems.

Alle praktischen Beispiele sollten mit möglichst ausführlichen Screenshots der notwendigen Aufrufe (z.B. in der Konsole oder in Tools) hinterlegt werden. Werden während der Ausführung Ausgaben erzeugt oder Oberflächen der verwendeten Tools geöffnet, sollten diese ebenfalls als Screenshot aufgenommen und die Ausgaben detailliert erklärt werden.

3. Layout der Skripte

An den Stellen, wo es technisch möglich und sinnvoll ist, kann ein Angriffsszenario als Skript hinterlegt werden. Ziel ist es, am Ende eine integrierte Anwendung zu erhalten, in der alle Themen der PDF-Dokumentation enthalten sind, sofern der Angriff in einem Skript darstellbar ist.

Aus diesem Grund ist es notwendig, ein einheitliches Layout und einen einheitlichen Aufbau innerhalb der Unterpunkte zu definieren.

Jedes Skript sollte mit einer Einleitung beginnen, in dem das Szenario kurz beschrieben ist. Nachfolgend sind Beispiele bzw. Templates für Inhalte der Workbench zu finden.

3.1. Einheitliche Befehle innerhalb der Workbench

- Auswahlmöglichkeiten (fix)
  Einsatz z.B. im Inhaltsverzeichnis
  Durchnummerieren der Möglichkeiten und Auswahl durch Ziffer + ENTER
- Auswahlmöglichkeiten (variabel)
  Kann die Anzahl der Auswahlmöglichkeiten nicht vorhergesagt werden (z.B. Anzahl und Bezeichnung der Netzwerkadapter), erfolgt die Auswahl durch das Abtippen der angezeigten Möglichkeiten und ENTER
- Beenden der gesamten Workbench
  STRG + c
- Beenden eines Skripts und Rücksprung ins Inhaltsverzeichnis
  x + ENTER
- Explizite Hilfe-Menüs
  Alle Erklärungen (was muss ich machen, was sehe ich gerade) sind direkt beim jeweiligen Step im Skript anzugeben, d.h. keine expliziten Hilfe-Menüs, wie sie in der alten Version der Workbench realisiert wurden. Sind detaillierte Infos in der PDF-Dokumentation verfügbar, ist auf die jeweiligen Kapitel zu verweisen. Dies gilt vor allem bei Inhalten der Kapitel „Fachbegriffe“, „Vorbereitung“, „Verwendete Tools“ oder wenn das Skript ein Tool mit zusätzlicher Benutzeroberfläche startet.

3.2. Begrüßung in der Workbench

In dieser Anwendung - die übrigens in der Programmiersprache python geschrieben wurde :-) - findest du den Großteil der Angriffsszenarien, die in der zughörigen PDF-Dokumentation der Security Workbench beschrieben sind. Um dir den Einstieg in die IT-Security und das Hacken zu erleichtern, führen wir dich mittels dieser Anwendung durch die verschiedenen Einzelschritte eines Angriffs. Trotzdem sollst du das Hacking als so real wie möglich erleben. Deshalb gibt es anstelle einer grafischen Benutzeroberfläche ein für Linux typisches Kommandozeilentool (Shell).

Für alle Schritte eines Angriffs ist beschrieben, welche Parameter zum Aufruf benötigt werden und was genau im Hintergrund passiert. In einzelnen Fällen ist es aber möglich, dass auch außerhalb dieser Shell-Anwendung Programme gestartet und deren Oberflächen angezeigt werden. Eine genaue Erklärung mit Screenshots dieser Oberflächen findest du in der PDF-Dokumentation.

Außerdem findest du alles, was hier im Skript erklärt ist, mindestens genauso ausführlich und mit Screenshots im dazugehörigen Kapitel der PDF-Dokumentation.

Wir – die Studenten des Informatik-Masters – wünschen dir viel Spaß und Erfolg beim Hacken.

> Mit ENTER geht es weiter zum Inhaltsverzeichnis…

3.3. Inhaltsverzeichnis

Was möchtest du tun?

1 ARP-Spoofing

2 DNS-Spoofing

3 …

> Bitte gib nachfolgend die Ziffer des gewählten Angriffs an und drücke ENTER…

3.4. Beispiel für den Inhalt/Aufbau eines Szenarios (hier: ARP-Spoofing)

Mithilfe des ARP-Spoofings kannst du den Netzwerkverkehr von fremden Rechnern überwachen und manipulieren.

! Achtung ! Führe dieses Skript nur aus, wenn du in deinem privaten Netzwerk angemeldet bist!

Du kannst das Skript jederzeit beenden und zum Inhaltsverzeichnis zurückkehren, indem du “x“ eingibst und ENTER drückst. Das komplette Programm kannst du durch „STRG + c“ beenden.

Step 1: Vorbereitungen

Stelle sicher, dass die Security Workbench (Kali Linux) direkten Zugriff auf das Host-Netzwerk hat. Wie das geht, kannst du in der PDF-Dokumentation im Kapitel „Tunneln von Netzwerkadaptern“ nachlesen.

> Mit ENTER geht es weiter…

Step 2: Auswählen des Netzwerkadapters

Nachfolgend sind die Netzwerkadapter aufgelistet, die auf deinem Rechner verfügbar sind. Wähle den Adapter aus, den du in Step 1 konfiguriert hast (i.d.R. eth0), indem du den Namen des Adapters abtippst und ENTER drückst.

> gewählter Netzwerkadapter:

Step 3: …