JA110 Penetration Testing Java

Kurzbeschreibung:

Der Kurs Java für Penetration Tester soll Pentester in Java-spezifische Exploitation-Techniken einführen. Es werden die gängigsten Schwachstellen-Klassen behandelt und wie man sie ausnutzt. Hierbei wird spezieller Fokus auf die Praxis und Verständnis der Funktionsweise von Angriffswerkzeugen gelegt:

- Wie funktioniert ysoserial und was kann ich damit machen?
- Wie genau funktioniert die JNDI-Injection bei der log4jv2-Schwachstelle?

Der Kurs versetzt den Pentester in die Lage, Java-Produkte zu erkennen, effektiv Fingerprinting durchzuführen, ggf. frei verfügbare Exploits zu modifizieren und Schwachstellen abseits der ausgetreteten Pfade aufzuspüren und auszunutzen. Java-Vorwissen ist zwar hilfreich, aber nicht erforderlich.

Zielgruppe:

Penetration Tester

Voraussetzungen:

Die Teilnehmer sollten Erfahrung im Pentesting mitbringen und grundlegende Programmierkenntnisse in Java oder zumindest einer anderen Programmiersprache besitzen.

Sonstiges:

Dauer: 5 Tage

Preis: 2690 Euro plus Mwst.

Ziele:

Der Kurs versetzt den Pentester in die Lage, Java-Produkte zu erkennen, effektiv Fingerprinting durchzuführen, Schwachstellen auszunutzen und ggf. frei verfügbare Exploits zu modifizieren.

Inhalte/Agenda:

- Kurze Einführung in Java
  - Java und Bytecode
  - Virtuelle Maschine und Laufzeitbibliothek
  - ClassLoader
  - Protokolle, APIs und Frameworks

- XML External Entity Injection
  - Angriffsschema und Beispiel
  - Exfiltration von Dateien über HTTP/FTP/...
  - Exfiltration von Dateien über Fehlermeldungen

- Unsicherer Datei-Upload
  - Ein alter Bekannter
  - Falsches Prozessieren von Archiven
  - Beispiel: Spring4Shell

- JNDI-Injection
  - Kurze Einführung in JNDI
  - JNDI-Referenzen
  - Die verschiedenen Techniken zur Ausnutzung
  - Beispiel: Log4j

- Unsichere Deserialisierung
  - Kurze Einführung in (De)-Serialisierung
  - Was ist ein Gadget?
  - Ein komplexeres Beispiel
  - RMI
  - Andere Formate: JSON, XML und YAML
  - Verwundbare Bibliotheken

- Java Management Extensions
  - Information Leakage
  - Die verschiedenen Wege zur RCE
  - Deserialisierungs-Angriffe auf JMX
  - Andere Protokolle für JMX

- Andere Themen
  - Spring Boot Actuator
  - Jolokia
  - Leaks durch schlechte Fehlerbehandlung

- Injection-Angriffe
  - EL-Injection in PrimeFaces
  - EL-Injection in Struts2
  - Template-Injection

- Fortgeschrittene Themen
  - Benutzung des Java Decompilers
  - Benutzung des Debuggers
  - Ausblick auf statische und dynamische Code-Analyse