

Kod szkolenia: **ANDROID/SEC**

Tytuł szkolenia: **Bezpieczeństwo i odzyskiwanie danych na platformie Android**

Dni: 3

Opis:

Adresaci szkolenia:

Szkolenie dedykowane wszystkim, którzy chcą wiedzieć więcej na temat bezpieczeństwa, wewnętrznej architektury i sposobu działania platformy Android.

Cel szkolenia:

- Poszerzenie wiedzy na temat architektury i wewnętrznych mechanizmów platformy Android
- Wskazanie potencjalnych zagrożeń w kontekście bezpieczeństwa aplikacji mobilnych
- Przedstawienie sposobów weryfikacji bezpieczeństwa
- Zademonstrowanie sposobów dostępu i odzyskiwania danych z urządzenia

Mocne strony szkolenia:

Wszystkie poruszane zagadnienia mają istotne znaczenie z punktu widzenia bezpieczeństwa aplikacji mobilnych. Szkolenie ma charakter typowego warsztatu dzięki czemu przekazywana wiedza ma ogromną wartość merytoryczną, a poruszane zagadnienia mimo wysokiego poziomu trudności dają się łatwo przyswoić.

Wymagania:

Od uczestników szkolenia wymagana jest praktyczna umiejętność programowania w języku Java, a także podstawowa znajomość platformy Android.

Parametry szkolenia:

3*8 godzin (3*7 godzin netto) wykładów i warsztatów (z wyraźną przewagą warsztatów).

Program szkolenia:

1. Rooting
 - Zasada działania / korzyści / konsekwencje
 - Boot loaders
 - System recovery i fastboot



- Wykorzystanie adb
- Procedura rootowania
- Instalacja niestandardowego obrazu ROM
- 2. Analiza systemu plików
 - Partycje - rozkład i przeznaczenie
 - Systemy plików
 - Struktura systemu plików
 - Pozyskiwanie i analiza apk
 - Budowanie plików dex
 - ART
 - Sandboxing
- 3. Podstawy bezpieczeństwa
 - Typy aplikacji (native, web, hybrid)
 - Najczęściej spotykane luki (OWASP 10 ten)
 - Testowanie bezpieczeństwa
 - Dozer
 - Identyfikowanie podstawowych zagrożeń
 - QARK (Quick Android Review Kit)
- 4. Bezpieczeństwo w praktyce
 - Dostęp do danych
 - Komunikacja z backend
 - Komponenty
 - Techniki analizy statycznej i dynamicznej
 - Typy najczęstszych ataków
 - Malware
 - MitM
 - Exploits
 - Omijanie blokady ekranu
 - Dostęp do karty SD
- 5. Ekstrakcja danych
 - Logiczny vs. fizyczny odczyt danych
 - Wykorzystanie adb
 - Dostęp do statystyk systemu
 - Omijanie / łamanie blokady ekranu
 - Wykorzystanie DD i nanodump
 - Analiza obrazu ROM
 - Analiza pamięci RAM
 - Data recovery
 - Analiza na poziomie popularnych aplikacji
 - Przegląd narzędzi (ViaExtract, Autopsy, ViaLab)

