Kod szkolenia: **SEC/WEB**

Tytuł szkolenia: **Testy bezpieczeństwa nowoczesnych aplikacji internetowych**

Dni: 3

Opis:

**Adresaci szkolenia**

Szkolenie jest kierowane do testerów, programistów, administratorów aplikacji, audytorów oraz fascynatów bezpieczeństwa pragnących zdobyć całościową wiedzę z zakresu prowadzenia testów penetracyjnych oraz wykorzystania jej do weryfikacji bezpieczeństwa złożonych systemów informatycznych.

**Cel szkolenia**

Celem szkolenia jest przekazanie wiedzy, która uczyni z uczestnika nie tylko weryfikatora bezpieczeństwa na podstawie baz wiedzy i gotowych exploitów ale da podstawy do zostania researcherem bezpieczeństwa zdolnym do pracy z nieznanymi aplikacjami i protokołami oraz wyszukiwania nowych podatności w nich. Mocną stroną szkolenia są przykłady dla aplikacji .NET (stack Microsoft) i Java (stack Oracle i open source) - z dziedziny bankowości oraz aplikacje mobilne Android i iOS. Uczestnicy wykonują zadania związane z projektem testów penetracyjnych na laboratorium w formie zwirtualizowanego środowiska symulującego typowej problemy złożonej infrastruktury.

**Wymagania**

Od uczestników wymagane jest doświadczenie w pracy z aplikacjami internetowymi - najlepiej jako programista lub wdrożeniowiec albo doświadczenie z dziedziny bezpieczeństwa takich rozwiązań. Znajomość podstaw Java oraz .NET a także podstaw administracji w systemach Windows i Linux pozwoli bezboleśnie przejść przez wszystkie laboratoria.

**Parametry szkolenia**

Czas trwania: 3*8 godzin (3*7 godzin netto)

Program szkolenia:

1. Rodzaje testów penetracyjnych
    - Różnica między testem penetracyjnym a audytem
    - Metodyki prowadzenia testów penetracyjnych
    - Typy testów: whitebox, blackbox, greybox

- Fazy testów penetracyjnych
- Szacowanie zagrożeń, modelowanie zagrożeń i drzewa ataku
- Zakres testu
- Projekty R&D
- checklisty w testach penetracyjnych, standardy kodowania: CIS, CERT

2. Rodzaje podatności, typy podatności według różnych klasyfikacji
   - klasyfikacja podatności według OWASP i CWE
   - co to jest CVE? - otwarte i zamknięte bazy podatności
3. Narzędzia do analizy sieci i fazy rozpoznania, zbierania informacji o celu ataku
   - sniffery
   - narzędzia aktywne
   - narzędzia pasywne
   - weryfikacja konfiguracji
   - wykorzystanie: Foca, Massdns, subfinder, dirsearch, dirb
   - Google dorks
   - Shodan
   - użycie baz FuzzDB i Directory List
4. Ataki na aplikacje webowe
   - SQL Injection
   - różne ataki typu Injection (XPath, XML, Command, Script, LDAP)
   - Deserializacja w Javie
   - Wstrzykiwanie kodu przez JSON w usługach REST
   - Mass assignment
   - Ataki na usługi REST JAX-RS
   - XSS
   - CSRF
   - Bezpośredni dostęp do danych i obiektów (IDOR)
   - Path Traversal
   - XXE
   - Spring EL Injection, ataki na Spring Framework
   - Command Injection (Shellshock)
   - Zarządzanie sesją
   - Typowe problemy z rejestracją użytkowników i odzyskiwaniem hasła
   - Podatności w JWT
5. Narzędzia do testów manualnych typu proxy
   - wykorzystanie Burp Suite, OWASP ZAP
6. Automatyczne skanery bezpieczeństwa
   - Wykorzystanie Nessus, Nexpose, Burp Suite Scan, Skipfish, Arachni, OpenVAS
   - Narzędzia zapewniające bezpieczeństwo w trakcie developmentu: OWASP Dependency Check, Retire.js, Find-Sec-Bugs, PMD
7. Zbiory exploitów
   - wykorzystanie Metasploit
8. Skrypty i automatyzacja testów bezpieczeństwa
   - wykorzystanie ZAP i Mozilla ZEST
   - integracja OWASP ZAP z Jenkins

- wykrywanie dziurawych komponentów z OWASP Dependency Check w CI

9. Testowanie WebServices
    - XXE
    - SOAP
    - XSLT
    - BPEL
10. Kryptografia
    - weryfikacja poprawnej konfiguracji SSL
    - Man-in-the-middle
    - Słabości w implementacji kryptografii
11. Ataki DoS i DDoS
    - ataki na logikę aplikacji: ReDOS, XML Bomb, Flood
12. Cloud
    - Specyficzne zagadnienia dla cloud: AWS
    - Wykorzystanie cloud w testach: DoS, DDoS
13. Zarządzanie informacją w trakcie testu penetracyjnego
    - Budowanie bazy wiedzy i bazy ataków
    - Dradis Framework, Faraday IDE, Magic Tree
14. Tworzenie raportu
    - co powinien zawierać dobry raport z testów penetracyjnych?
    - jak formułować zalecenia i obejścia?
    - jak bezpiecznie dostarczyć raport do klienta?
    - jak opisać podatność i uzyskać CVE?
15. Planowanie i zarządzanie projektem testów penetracyjnych
    - formalności w pracy z klientem
    - zarządzanie zakresem
16. Wizerunek pentestera
    - Networking
    - Wizytówka