Automatyzacja skanów bezpieczeństwa w tym integracja weryfikacji bezpieczeństwa w funkcjonalnych testach automatycznych. Bardzo przydatna podczas kilku iteracji testów.

Przykładowy opis etapów i obszarów poddawanych testom:

1. **Ocena ryzyka – Risk assessment**
   Proces przeglądu i analizy potencjalnych obszarów ryzyka. Nadawany jest priorytet i określane możliwe sposoby zapobiegania. Efektem tego etapu jest propozycja punktów kontroli wykrywania prób ataku i implementacji mechanizmów minimalizacji następstw ataku. Warta wspomnienia w tym przypadku jest technika zwana modelem oceny ryzyka (Threat modeling). Umożliwia ona określenie poziomu ryzyka dla poszczególnych elementów pośrednio pozwalając na stworzenie metod zmniejszenia jego wystąpienia oraz wykorzystania niewątpliwie ograniczonych zasobów na obszarach najbardziej potrzebujących uwagi. Model taki powstaje w oparciu o standard NIST 800-30, jego wynikiem są zazwyczaj kolekcje list i diagramów, główne etapy uwzględniają:

   - Dekompozycję aplikacji – w procesie inspekcji zbierana jest wiedza na temat działania aplikacji, jej składowych, funkcjonalnościach i sposobu komunikacji.
   - Określenie i klasyfikacja składowych – podział na zasoby namacalne i nieprzeliczalne oraz ich ocena pod kątem wagi biznesowej.
   - Wyszukiwanie potencjalnych podatności – mogą wywodzić się z problemów technicznych, operacyjnych lub zarządzania.
   - Wyszukiwanie potencjalnych zagrożeń – przy pomocy technik scenariuszy lub „drzew” ataku, tworzony jest model opisujący potencjalne miejsca ataku z perspektywy włamywacza.
   - Tworzenie/wypracowanie strategii zapobiegania – przygotowanie punktów kontroli i procedur ograniczania wpływu włamania.

2. **Security auditing – audyt bezpieczeństwa**
   Procedura definiowania błędów bezpieczeństwa w poszczególnych aplikacjach, które składają się na środowisko ataku. Może być to manualna weryfikacja polityk, procedur, procesów jak i samych pracowników lub ról. Uwzględniana jest konfiguracja systemu i środowiska pracy, czyli czynniki, dla których wybrano daną technologię albo jaki był powód zaprojektowania elementu w ten, a nie w inny sposób. Na tej podstawie tester ustala prawdopodobieństwo wystąpienia problemu w danym elemencie. Jest to również jeden z nielicznych etapów pozwalający wykryć problemy w samym cyklu życia oprogramowania (SDLC) i upewnić się, że wdrożono odpowiednią politykę i jest ona rozumiana, czy też zweryfikować poziom kompetencji. Często podczas tej fazy testów wykonywany jest przegląd kodu aplikacji. Istnieje możliwość sprawdzenia pojedynczych linii. Pozwala to odnaleźć niskopoziomowe mechanizmy pozwalające na niezamierzoną interakcję z systemem, które są niezmiernie trudne do znalezienia przy użyciu innych metod. Poza problemami wynikającymi ze złych intencji, odnajdywane są w tym przypadku różnego rodzaju komentarze, nieaktualne wersje modułów, problemy ze współdzieleniem, wadliwa logika biznesowa, niepoprawna kontrola dostępu, podatności algorytmu szyfrowania, obejścia ułatwiające pracę czy różnego rodzaju złośliwy kod (trojany, backdory). W celu zmniejszenia nakładu pracy wymaganego do przeglądu kodu źródłowego pokaźnych rozmiarów używane są automatyczne skanery, jako uzupełnienie wykonywany jest manualny przegląd aby zniwelować ograniczenie w postaci braku możliwości zrozumienia przez skaner kontekstu, zależności wynikających z przepływów pomiędzy elementami programu.

3. **Test penetracyjny – Penetration testing**
   Test ma na celu imitowanie złośliwego ataku zewnętrznego znany również pod nazwą testów czarnoskrzynkowych (black box). Wykonywany w celu oceny bezpieczeństwa systemu. Podczas testu używana jest działająca wersja aplikacji a audytor nie posiada dogłębnej wiedzy o zasadach jej działania. Często grupa testowa jest w posiadaniu podstawowego konta z dostępowego. Następuje próba

uzyskania nieautoryzowanego dostępu do systemu wykonywana przez wykwalifikowanego specjalistę w sposób w jaki działałby potencjalny napastnik.Etapy:

- Rekonesans,
- identyfikacja luk,
- wykorzystanie podatności,
- analiza ryzyka,
- zacieranie śladów.

4. **Ocena postawy/polityki – Posture assessment**
   Zestawienie trzech weryfikacji w celu oceny pełnego obrazu podejścia do bezpieczeństwa w organizacji. Składowe to: ocena ryzyka, test penetracyjny, skanowanie bezpieczeństwa.

5. **Security scanning**
   Charakteryzuje się identyfikacją słabości sieci i systemu, do których później przedstawia się propozycje sposobu redukcji ryzyka. Skanowanie tego typu wykonywane jest manualnie jak również za pomocą automatycznych narzędzi.

6. **Szukanie wrażliwych punktów – Vulnerability scanning**
   W fazie tej identyfikowane są zagrożenia, które faktycznie mogą wystąpić w testowanym środowisku, weryfikowana jest także skuteczność wykorzystania znanych luk w zabezpieczeniach poszczególnych składowych środowiska np. programów i ich konkretnych wersji. Skan tego typu wykonywany jest za pomocą automatycznych narzędzi, przeszukujących środowisko pod kątem znanych obszarów podatności.