Testy Penetracyjne

Skanowanie podatności

Arkadiusz Chrobot

Katedra Systemów Informatycznych

27 marca 2024

Plan

Wstęp

Automatyczne skanowanie podatności ma na celu identyfikację luk bezpieczeństwa w systemach operacyjnych i aplikacjach. Jest to część testów penetracyjnych, pozwalająca ustalić cele do późniejszego zbadania i ewentualnej eksploatacji, a także ocenić stan zabezpieczeń (ang. *security posture*) weryfikowanej infrastruktury informatycznej. Ten rodzaj skanowania może być także przeprowadzany przez zespoły bezpieczeństwa w podmiotach, których systemy informatyczne mogą stać się potencjalnymi celami ataków. W takim przypadku ich wykonanie powinno być regulowane zapisami w *polityce zarządzania podatnościami* (ang. *vulnerabilities management program*), definiującej procedury wykrywania, określania ważności i przeciwdziałania lukom bezpieczeństwa, zanim zostaną one wykorzystane przez intruzów.

Wymagania dla zarządzania podatnościami

Konieczność przeprowadzania skanowania podatności i testów penetracyjnych może wynikać z polityki firmowej przedsiębiorstwa, jeśli posiada ono systemy informatyczne przechowujące i przetwarzające informacje wrażliwe lub o szczególnym znaczeniu.
Również regulacje prawne lub standardy mogą wprowadzać taki wymóg. Część z nich zawiera go w formie niejawnej. Przykładem może być RODO/GDPR. Inne, jak Narodowe Standardy Cyberbezpieczeństwa jedynie zawierają sugestię, że testy penetracyjne/skanowanie podatności są zalecane (▸ NSC-800-53).

Wymagania dla zarządzania podatnościami

W polskich realiach najbardziej szczegółowe wymagania odnośnie skanowania podatności zawiera międzynarodowy standard PCI DSS, zobowiązujący instytucje mające pieczę nad systemami obsługującymi płatności kartami do:

- przeprowadzania zewnętrznego i wewnętrznego skanowania podatności;
- wykonywania tej czynności co najmniej kwartalnie i po każdej znaczącej zmianie w systemie (np. modyfikacja reguł zapory sieciowej, topologii sieci);
- zatrudnienia wykwalifikowanego personelu do przeprowadzania skanowania wewnętrznego;
- usuwania wykrytych luk dużego ryzyka i powtarzania skanowania, aż do uzyskania w raporcie informacji o braku podatności;
- zlecania wykonania skanowania zewnętrznego wskazanemu przez PCI SSC podmiotowi (ang. *Approved Scanning Vendor*).

Wymagania dla zarządzania podatnościami

Wymagania odnośnie do skanowania podatności są w większości zbieżne dla zespołów przeprowadzających testy penetracyjne i zajmujących się ochroną systemów informatycznych. Mogą jednak wystąpić pewne różnice.

Zespoły testujące mogą przeprowadzać dokładne (ang. *in-depth*) skanowanie całego weryfikowanego systemu, aby wykryć potencjalne wektory ataku.

Zespoły ochraniające mogą dla odmiany zawęzić skanowanie podatności do określonych elementów systemu, np. takich, które zostały niedawno dodane lub których konfiguracja uległa zmianie.

Planowanie

Skanowanie rozbudowanych systemów informatycznych może być kosztowne i czasochłonne. Jeśli nie nakazują tego żadne regulacje, to decyzję o tym, które jego elementy powinny być poddane tej czynności można podjąć kierując się następującymi przesłankami:

- klasyfikacją danych transmitowanych, przechowywanych i przetwarzanych w systemie,
- ekspozycją systemu w sieciach zewnętrznych,
- usługami oferowanymi przez system,
- rodzajem systemu (rozwojowy, testowy, produkcyjny).

Niektóre narzędzia do skanowania podatności oferują funkcję automatycznego wykrywania i inwentaryzowania aktywów dostępnych w systemie. Ten wykaz może być manualnie uzupełniony o informację, które z nich mają znaczenie krytyczne, a które nie.

Planowanie

Ustalanie częstotliwości

Zespoły zajmujące się cyberbezpieczeństwem mogą ustalić częstotliwość, z jaką powinno być wykonywane skanowanie podatności, biorąc pod uwagę:

- poziom tolerancji dla ryzyka (ang. *risk appetite*) podmiotu, dla którego pracują;
- regulacje prawne i standardy;
- ograniczenia techniczne, np. stosowanych narzędzi;
- ograniczenia biznesowe — skanowanie nie powinno zakłócać normalnej pracy systemów informatycznych;
- ograniczenia licencyjne,
- ograniczenia operacyjne, wpływające na zdolność zespołu do monitorowania i reagowania na wyniki skanowania.

Planowanie

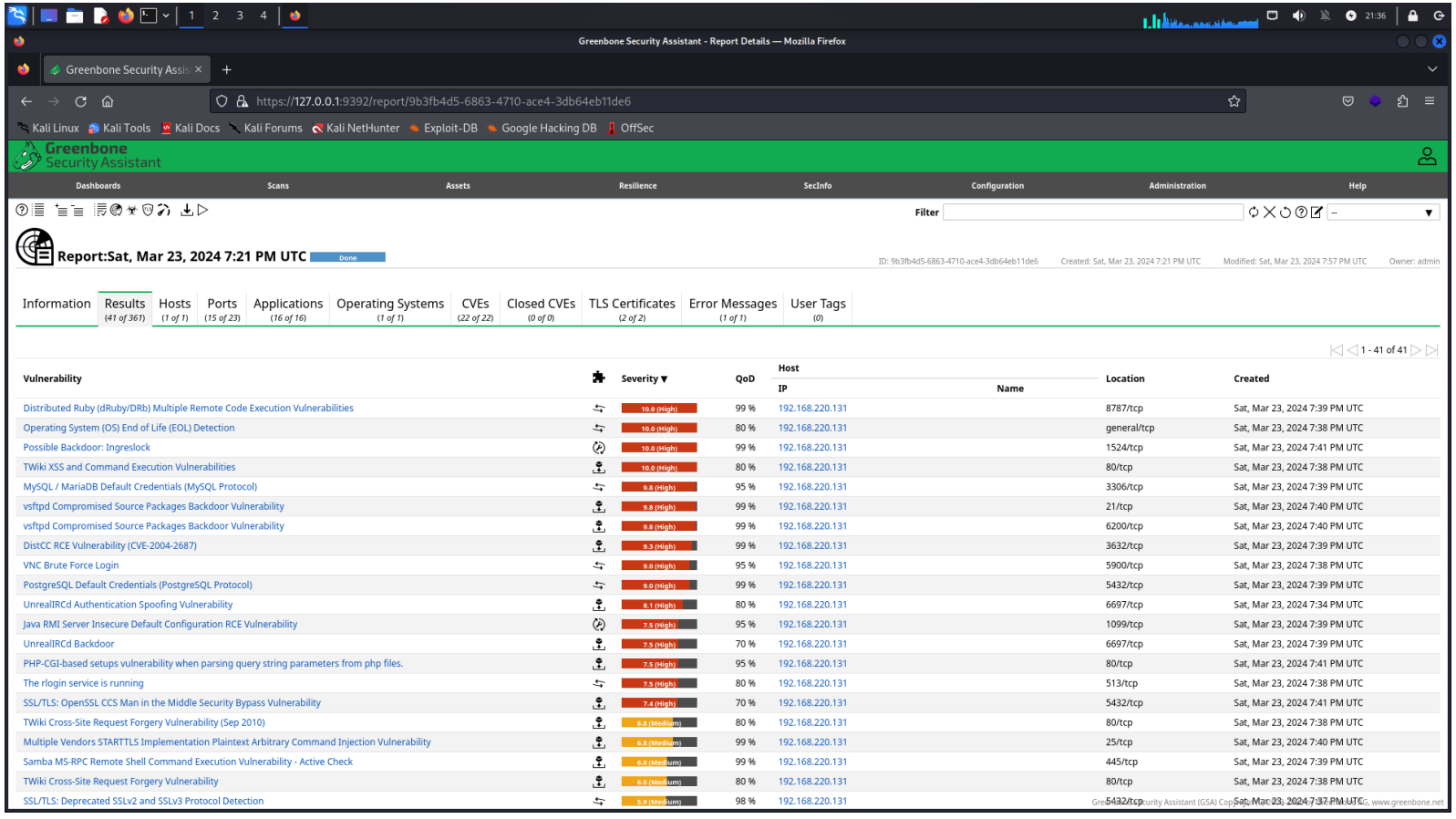
Warto zwrócić uwagę, że zespoły cyberbezpieczeństwa w firmach i organizacjach zazwyczaj preferują *wsadowy* sposób przeprowadzania skanów podatności. Nie ingerują w jego przebieg, jedynie konfigurują narzędzia, aby wysyłały raporty z uzyskanymi wynikami.
Testerzy penetracyjni wolą bardziej interaktywny sposób skanowania, dzięki któremu mogą porównywać bieżące wyniki z rezultatami skanowania innych systemów lub zmienić listę skanowanych urządzeń.
Jeśli zespoły przeprowadzające testy penetracyjne otrzymają wyniki skanowania podatności uzyskane przez zespoły cyberbezpieczeństwa, to muszą także poznać czynniki, które wpłynęły na decyzję o takim a nie innym wyborze celów.

Konfigurowanie i wykonywanie

Narzędzia

Istnieje wiele narzędzi, które służą do skanowania podatności. Należą do nich również Nmap i Metasploit, wykorzystywane w testach penetracyjnych. Jest również oprogramowania specjalistyczne, przeznaczone tylko do wykonywania tej czynności. Pierwszym narzędziem z tej drugiej kategorii było *Security Administrator Tool for Analyzing Networks* — SATAN — jego rozwój został jednak wstrzymany. Historycznie kolejnym było SAINT, a potem Nessus. Oba narzędzia są do dziś rozwijane. Nessus początkowo był narzędziem darmowym, dostępnym na licencji GPL, jednak od trzeciej wersji stał się oprogramowaniem własnościowym. Innym komercyjnym skanerem podatności jest Qualys. Na bazie darmowej wersji Nessusa powstał OpenVAS, który jest darmowym, ale profesjonalnym narzędziem. Przykład raportu ze skanowania maszyny wirtualnej *Metasploitable 2* przy użyciu tego skanera znajduje się na Rysunku 1.

Konfigurowanie i wykonywanie



Rysunek: Raport ze skanowania maszyny *Metasploitable 2* przy użyciu OpenVAS

Konfigurowanie i wykonywanie

Rodzaje skanowania

Podobnie, jak w przypadku zbierania informacji, skanowanie podatności może być *aktywne* i *pasywne*. Większość narzędzi skanuje aktywnie, wchodząc w interakcję z celem, identyfikując otwarte usługi i wyszukując ich podatności. To daje wysokiej jakości wyniki, ale:

- generuje duży ruch w sieci, ułatwiając wykrycie skanowania, co może nie być pożądane w testach penetracyjnych;
- może przypadkowo zablokować lub uszkodzić skanowany system,
- może pominąć niektóre systemy, jeśli zostanie zablokowane przez mechanizmy zabezpieczające.

Uzupełnieniem, lecz nie alternatywą, dla skanowania aktywnego jest skanowanie pasywne, które bada ruch sieciowy, starając się wychwycić sygnatury świadczące o niezabezpieczonym sprzęcie i oprogramowaniu.

Konfigurowanie i wykonywanie

Zakres

Ustalając zakres skanowania podatności, należy uwzględnić:

- Które systemy, sieci, usługi, aplikacje i protokoły będą mu podlegały?
- Jakie środki techniczne zostaną zastosowane w celu ustalenia obecności celu skanowania w sieci?
- Jakie testy zostaną przeprowadzone na systemach odkrytych podczas skanowania?

Członkowie zespołów bezpieczeństwa muszą uzgodnić zakres skanowania z innymi pracownikami technicznymi i kierownictwem, aby nie zakłócić działania przedsiębiorstwa. Testerzy penetracyjni powinni z kolei opierać się na dokumentach definiujących obszar prac.

Konfigurowanie i wykonywanie

Ustawienia

Narzędzia do skanowania podatności oferują wiele ustawień. Jednym z najistotniejszych jest *poziom czułości*, który określa rodzaje przeprowadzanej weryfikacji i pozwala osiągnąć kompromis między jakością otrzymanych wyników, a niebezpieczeństwem zakłócenia pracy badanych systemów. Oprogramowanie do skanowania może oferować pewne ustalone schematy ustawień, ale tester lub członek zespołu d.s. bezpieczeństwa może tworzyć własne, np. blokując wtyczki (ang. *plug-ins*) skanujące nieużywane w systemie urządzenia lub protokoły. Z punktu widzenia testerów penetracyjnych przydatna jest opcja pozwalająca zmniejszyć wykrywalność (ang. *stealth*) skanowania.

Konfigurowanie i wykonywanie

Uzupełnienie

Tradycyjnie skanowanie podatności polega na zdalnym wykrywaniu luk w systemach. Jednakże ten rodzaj skanowania może być wykryty, zablokowany lub zakłócony przez mechanizmy zabezpieczające. Ponadto może on być nieskuteczny w środowiskach stosujących wirtualizację i/lub konteneryzację. W takich wypadkach skanowanie przez sieć musi zostać uzupełnione danymi o konfiguracji serwerów, aby wyeliminować błędy, takie jak fałszywie dodatnie wyniki. Te informacje, mogą być uzyskane poprzez *uwierzytelnione skanowanie* (ang. *credentialed scanning*), albo przez *skanowanie z użyciem agentów* (ang. *agent-based scanning*). W pierwszym przypadku administratorzy serwerów udostępniają osobom skanującym konta tylko do odczytu na skanowanych serwerach. W drugim przypadku instalują pomocnicze oprogramowanie, które pomaga zebrać wymagane informacje. Po zakończonych testach warto je usunąć.

Konfigurowanie i wykonywanie

Perspektywa skanowania

Skanowanie powinno być wykonywane z kilku różnych punktów w topologii sieci. Dzięki temu uzyskane wyniki pozwalają lepiej poznać stan bezpieczeństwa weryfikowanej infrastruktury. Przykładowo skanowanie zewnętrzne pozwala sprawdzić, co będzie widoczne w systemie dla zewnętrznego przeciwnika, a wewnętrzne, jaką perspektywę będzie miał intruz znajdujący się w sieci wewnętrznej.

Konfigurowanie i wykonywanie

Aktualizacja narzędzi

Okresowe aktualizowanie narzędzi do skanowania podatności jest istotną sprawą z dwóch powodów. Skanery także mogą zawierać luki, które mogą być wykorzystane przez potencjalnych intruzów. Nawet wyciek informacji może być w tym przypadku bardzo groźny, bo poinformuje atakującego o słabościach systemu. Z drugiej strony, informacje o istniejących podatnościach często się zmieniają i dlatego powinny być uaktualniane. Powstał protokół o nazwie SCAP (ang. *Security Content Automation Protocol*), którego celem jest uspójnienie wymiany informacji związanych z bezpieczeństwem. Jest on obsługiwany przez większość skanerów i zawiera elementy wymienione na następnym slajdzie.

Konfigurowanie i wykonywanie

Aktualizacja narzędzi

Common Configuration Enumeration — CCE definiuje terminologię do opisywania problemów z konfiguracją systemu,

Common Platform Enumeration — CPE określa terminologię opisu nazw i wersji produktów,

Common Vulnerabilities and Exposures — CVE definiuje terminologię opisu luk w oprogramowaniu,

Common Vulnerability Scoring System — CVSS definiuje standard oceny podatności,

Extensible Configuration Checklist Description Format — XCCDF język do tworzenia list kontrolnych i wyników,

Open Vulnerability and Assessment Language — OVAL język opisu niskopoziomowych procedur testów używanych w listach kontrolnych.

Testy oprogramowania

Firmy wytwarzające oprogramowaniem powinny rozważyć wprowadzenie testów bezpieczeństwa. Mogą one być zautomatyzowane przy użyciu zarówno *analizatorów statycznych*, jak i *analizatorów dynamicznych*. W tym ostatnim przypadku interesujące mogą okazać się narzędzia do testów rozmytych (ang. *fuzz testing*). Przykładem może być *American Fuzzy Lop* — ▸ AFL — opracowany przez Michała Zalewskiego. Inną przydatną kategorią, również w testach penetracyjnych, są specjalizowane narzędzia wykrywające podatności w określonych typach oprogramowania. Dla aplikacji internetowej mogą to być narzędzia *Nikto* i *Wapiti*. Automatyczne lub ręczne znajdywanie podatności umożliwiają *przechwytujący pośrednicy* (ang. *intercept proxy*), tacy jak OWASP ZAP, *Fiddler*, *Burp Suite*. Specjalnie dla systemu zarządzania treścią *WordPress* opracowano *WPScan*. Z kolei luki w systemach zarządzania bazami danych, które używają języka SQL znajduje *SQLmap*.

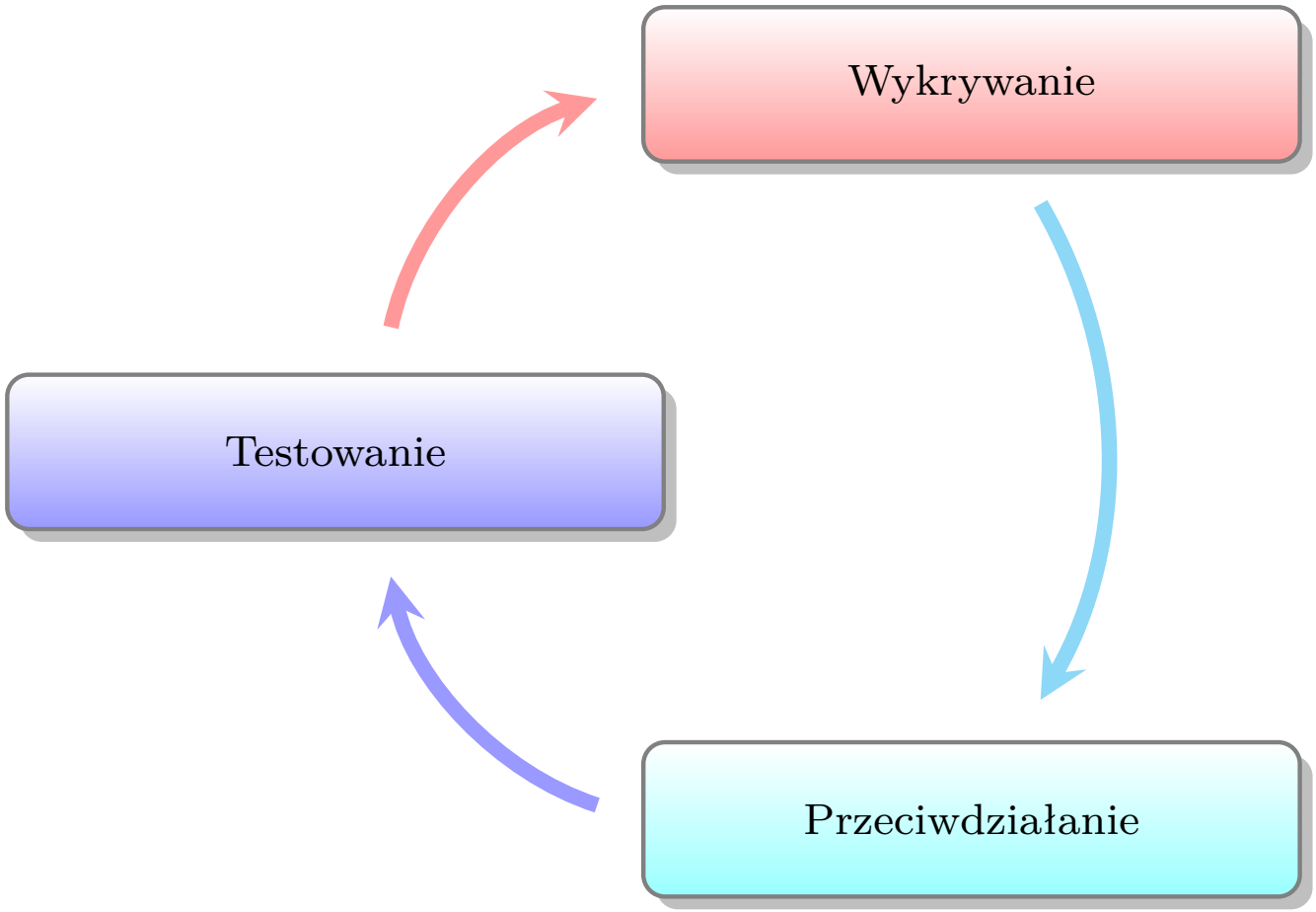
Opracowanie polityki napraw

Skanowanie podatności powinno być cyklicznym, a najlepiej ciągłym, procesem, nie jednorazową czynnością. Zbierane w ten sposób informacje powinny być analizowane w celu określenia istotności odkrytych luk i wskazania środków zapobiegawczych. Wprowadzone poprawki powinny być poddane testom. Ten cykl przedstawiony jest na Rysunku 2. Podmiot będący właścicielem skanowanych systemów musi opracować procedury, według których lukom będą nadawane priorytety i będą prowadzone prace naprawcze. Pierwsza z tych czynności może być przeprowadzona w oparciu o następujące czynniki:

- krytyczność systemu i informacji dotkniętych luką,
- trudność naprawy,
- istotności luki,
- ekspozycji luki.

Zanim poprawki zostaną wprowadzone do systemu produkcyjnego, powinny być przetestowane w izolowanym środowisku, celem sprawdzenia, czy nie powodują nieprzewidzianych efektów ubocznych.

Opracowanie polityki napraw



Rysunek: Zarządzanie podatnościami

Rozwiązywanie problemów

Skanowanie podatności może wiązać się z szeregiem problemów. Jeśli istnieje niezerowe prawdopodobieństwo, że obniży ono jakość usług dostarczanych przez system, to należy tak dobrać porę jego przeprowadzania, aby negatywny wpływ był minimalny. Jeśli te usługi są objęte umowami typu SLA, to może się okazać konieczne uzyskanie zgody na skanowanie również klienta, będącego stroną takiej umowy. Wdrożenie skanowania może wymagać także przekonania i zaangażowania kierownictwa wyższego szczebla. W końcu skanowanie systemów krytycznych, np. przeznaczonych do zastosowań medycznych, może pociągnąć za sobą konieczność stworzenia środowisk testowych z ich kopiami i przeprowadzenia najpierw na nich tej czynności. Po upewnieniu się, że nie spowoduje ona nieprzewidzianych problemów, można ją wykonać na środowisku produkcyjnym.

Pytania

?

Koniec

Dziękuję Państwu za uwagę!