Analiza podatności

W dzisiejszym świecie organizacje w dużym stopniu polegają na technologii informacyjnej w zakresie ochrony ważnych informacji. Informacje te są powiązane z obszarami finansów, badań i rozwoju, personelu, legalności i bezpieczeństwa. Oceny podatności skanują sieci w poszukiwaniu znanych słabych punktów bezpieczeństwa. Atakujący przeprowadzają analizę podatności na ataki w celu zidentyfikowania luk w zabezpieczeniach sieci docelowej organizacji, infrastruktury komunikacyjnej i systemów końcowych. Zidentyfikowane luki są wykorzystywane przez osoby atakujące do dalszego wykorzystywania docelowej sieci. Ocena podatności odgrywa ważną rolę w zapewnianiu bezpieczeństwa zasobów i infrastruktury każdej organizacji przed różnymi zagrożeniami wewnętrznymi i zewnętrznymi. Aby zabezpieczyć sieć, administrator musi zarządzać poprawkami, instalować odpowiednie oprogramowanie antywirusowe, sprawdzać konfiguracje, rozwiązywać znane problemy w aplikacjach innych firm oraz rozwiązywać problemy ze sprzętem z domyślnymi konfiguracjami. Wszystkie te czynności razem składają się na ocenę podatności. Ten moduł rozpoczyna się od wprowadzenia do koncepcji oceny podatności na zagrożenia. Omówiono również różne systemy oceny podatności, bazy danych podatności, cykl życia zarządzania podatnościami oraz różne podejścia i narzędzia wykorzystywane do przeprowadzania oceny podatności. Ten moduł zapewni wiedzę na temat narzędzi i technik wykorzystywanych przez osoby atakujące do przeprowadzenia jakościowej analizy podatności. Kończy się analizą raportów oceny podatności, które pomagają etycznemu hakerowi naprawić zidentyfikowane luki. Pod koniec tego modułu będziesz w stanie:

o Zrozumieć podatności, badania podatności, oceny podatności i systemów punktacji podatności

o Opisać cykl życia zarządzania podatnościami (fazy oceny podatności)

o Zrozumieć różne rodzaje podatności i technik oceny podatności

o Zrozumieć różne podejścia do rozwiązań do oceny podatności na zagrożenia

o Opisać różne cechy dobrych rozwiązań do oceny podatności

o Wyjaśnić różne rodzaje narzędzi do oceny podatności oraz kryteria ich wyboru

o Korzystać z różnych narzędzi do oceny podatności na zagrożenia

o Generować i analizować raporty oceny podatności

Koncepcje oceny podatności na zagrożenia

Ta sekcja zawiera przegląd podatności i jej przykładów, ocenę podatności, systemy oceny podatności, bazy danych podatności oraz cykl życia oceny podatności.

Co to jest podatność?

Luka odnosi się do słabości w projekcie lub implementacji systemu, którą można wykorzystać do naruszenia bezpieczeństwa systemu. Często jest to luka w zabezpieczeniach, która umożliwia atakującemu wejście do systemu z pominięciem uwierzytelniania użytkownika. Zasadniczo istnieją dwie główne przyczyny podatności systemów w sieci: błędna konfiguracja oprogramowania lub sprzętu oraz złe praktyki programistyczne. Atakujący wykorzystują te luki do przeprowadzania różnego rodzaju ataków na zasoby organizacji.

Typowe przyczyny występowania luk w zabezpieczeniach

Błędna konfiguracja sprzętu lub oprogramowania

Niepewna konfiguracja sprzętu lub oprogramowania w sieci może prowadzić do luk w zabezpieczeniach. Na przykład błędna konfiguracja lub użycie niezaszyfrowanego protokołu może prowadzić do włamań do sieci, co skutkuje wyciekiem poufnych informacji. Podczas gdy błędna konfiguracja sprzętu może umożliwić atakującemu uzyskanie dostępu do sieci lub systemu, błędna konfiguracja oprogramowania może umożliwić atakującemu uzyskanie dostępu do aplikacji i danych.

Niepewny lub zły projekt sieci i aplikacji

Niewłaściwa i niepewna konstrukcja sieci może narazić ją na różne zagrożenia i potencjalną utratę danych. Na przykład, jeśli zapory ogniowe, IDS i technologie wirtualnej sieci prywatnej (VPN) nie zostaną bezpiecznie zaimplementowane, mogą narazić sieć na liczne zagrożenia.

Nieodłączne słabości technologii

Jeśli sprzęt lub oprogramowanie nie jest w stanie obronić sieci przed określonymi typami ataków, sieć będzie narażona na te ataki. Niektóre urządzenia, aplikacje lub przeglądarki internetowe są zwykle podatne na ataki typu DoS lub ataki typu „man-in-themiddle". Na przykład systemy ze starymi wersjami przeglądarek internetowych są podatne na ataki rozproszone. Jeśli systemy nie są aktualizowane, mały atak trojana może zmusić użytkownika do przeskanowania i wyczyszczenia całej pamięci w komputerze, co często prowadzi do utraty danych.

Nieostrożność użytkownika końcowego

Nieostrożność użytkownika końcowego znacznie wpływa na bezpieczeństwo sieci. Ludzkie zachowanie jest dość podatne na różnego rodzaju ataki i może zostać wykorzystane do spowodowania poważnych skutków, w tym utraty danych i wycieku informacji. Intruzi mogą uzyskać poufne informacje za pomocą różnych technik socjotechnicznych. Udostępnianie informacji o koncie lub danych logowania przez użytkowników potencjalnie złośliwym podmiotom może prowadzić do utraty danych lub wykorzystania informacji. Podłączanie systemów do niezabezpieczonej sieci może również prowadzić do ataków ze strony osób trzecich.

Zamierzone działania użytkownika końcowego

Byli pracownicy, którzy nadal mają dostęp do dysków współdzielonych, mogą ich nadużywać, ujawniając poufne informacje firmy. Takie działanie nazywane jest umyślnym działaniem użytkownika końcowego i może prowadzić do znacznych strat danych i finansowych dla firmy.

Przykłady luk w zabezpieczeniach

Poniższe tabele podsumowują przykłady luk w zabezpieczeniach technologicznych i konfiguracyjnych:

Luki technologiczne: Opis

Luki w protokole TCP/IP: HTTP, FTP, ICMP, SNMP, SMTP są z natury niebezpieczne

Luki w systemie operacyjnym: system operacyjny może być podatny na ataki, ponieważ:

- To jest z natury niepewne

- Nie jest załatany najnowszymi aktualizacjami

Luki w zabezpieczeniach urządzeń sieciowych: Różne urządzenia sieciowe, takie jak routery, zapora ogniowa i przełączniki mogą być podatne na ataki z powodu:

- Brak ochrony hasłem

- Brak uwierzytelnienia

- Niebezpieczne protokoły routingu

- Luki w zaporze sieciowej

Luki w zabezpieczeniach konta użytkownika : wynikające z niezabezpieczonej transmisji danych konta użytkownika, takich jak nazwy użytkownika i hasła, przez sieć

Luki w zabezpieczeniach konta systemowego: Pochodzące z ustawienia słabych haseł do kont systemowych

Błędna konfiguracja usług internetowych: Błędna konfiguracja usług internetowych może stanowić poważne zagrożenie dla bezpieczeństwa. Na przykład włączenie JavaScript i błędna konfiguracja IIS, Apache, FTP i usług terminalowych może stworzyć luki w zabezpieczeniach sieci

Domyślne hasło i ustawienia : pozostawienie urządzeń/produktów sieciowych z ich domyślnymi hasłami i ustawieniami

Błędna konfiguracja urządzenia sieciowego: Błędna konfiguracja urządzenia sieciowego

Badania podatności na zagrożenia

Badanie luk w zabezpieczeniach to proces analizy protokołów, usług i konfiguracji w celu wykrycia luk w zabezpieczeniach i wad projektowych, które narażą system operacyjny i jego aplikacje na wykorzystanie, atak lub niewłaściwe użycie. Administrator potrzebuje zbadania luk w zabezpieczeniach:

• Gromadzenie informacji o trendach w zakresie bezpieczeństwa, nowo odkrytych zagrożeniach, powierzchniach ataków, wektorach i technikach ataków

• Wykrywanie słabych punktów w systemie operacyjnym i aplikacjach oraz ostrzeganie administratora sieci przed atakiem sieciowym

• Aby zrozumieć informacje, które pomagają zapobiegać problemom z bezpieczeństwem

• Wiedzieć, jak odzyskać siły po ataku sieciowym

Etyczny haker musi nadążać za ostatnio odkrytymi lukami w zabezpieczeniach i exploitami, aby być o krok przed atakującymi dzięki badaniom podatności, które obejmują:

• Wykrywanie wad i słabości projektu systemu, które mogą umożliwić atakującym złamanie zabezpieczeń systemu

• Bycie na bieżąco z nowymi produktami i technologiami oraz czytanie wiadomości związanych z obecnymi exploitami

• Sprawdzanie podziemnych witryn hakerskich (stron Deep i Dark) pod kątem nowo odkrytych luk w zabezpieczeniach i exploitów

• Sprawdzanie nowo wydanych alertów dotyczących istotnych innowacji i ulepszeń produktów dla systemów bezpieczeństwa

Eksperci ds. bezpieczeństwa i skanery luk w zabezpieczeniach klasyfikują luki w zabezpieczeniach według:

• Poziom ważności (niski, średni lub wysoki)

• Zakres eksploatacji (lokalny lub zdalny)

Etyczni hakerzy muszą przeprowadzić intensywne badania z pomocą informacji zdobytych w fazie footprintingu i skanowania w celu znalezienia luk w zabezpieczeniach.

Zasoby do badania luk w zabezpieczeniach

Poniżej przedstawiono niektóre witryny internetowe wykorzystywane do badania luk w zabezpieczeniach.

Centrum reagowania na zabezpieczenia firmy Microsoft (MSRC)

Centrum Microsoft Security Response Center (MSRC) bada wszystkie zgłoszenia dotyczące luk w zabezpieczeniach produktów i usług firmy Microsoft i dostarcza informacji w ramach ciągłych wysiłków mających na celu pomoc specjalistom ds. bezpieczeństwa w zarządzaniu zagrożeniami bezpieczeństwa i zapewnianiu ochrony systemów organizacyjnych.

• Packet Storm (https://pocketstormsecurity.com)

• Dark Reading (https://www.dorkreoding.com)

• Trend Micro (https://www.trendmicro.com)

• Security Magazine (https://www.securitymogozine.com)

• PenTest Magazine (https://pentestmog.com)

• SC Magazine (https://www.scmogozine.com)

• Exploit Database (https://www.exploit-db.com)

• Help Net Security (https://www.helpnetsecurity.com)

• HackerStorm (http://www.hockerstorm.co.uk)

• Computerworld (https://www.computerworld.com)

• D'Crypt (https://www.d-crypt.com)

Co to jest ocena podatności na zagrożenia?

Ocena podatności to dogłębne badanie zdolności systemu lub aplikacji, w tym obecnych procedur bezpieczeństwa i kontroli, do przeciwstawienia się wykorzystaniu. Skanuje sieci w poszukiwaniu znanych słabych punktów bezpieczeństwa oraz rozpoznaje, mierzy i klasyfikuje luki w zabezpieczeniach systemów komputerowych, sieci i kanałów komunikacyjnych. Identyfikuje, określa ilościowo i klasyfikuje możliwe podatności na zagrożenia w systemie. Ponadto pomaga specjalistom ds. bezpieczeństwa w zabezpieczaniu sieci, identyfikując luki w zabezpieczeniach lub luki w obecnym mechanizmie bezpieczeństwa, zanim atakujący będą mogli je wykorzystać. Ocena podatności może być wykorzystana do:

• Zidentyfikuj słabości, które można wykorzystać

• Przewiduj skuteczność dodatkowych środków bezpieczeństwa w ochronie zasobów informacyjnych przed atakiem

Zazwyczaj narzędzia do wykrywania luk w zabezpieczeniach przeszukują segmenty sieci w poszukiwaniu urządzeń obsługujących protokół IP i wyliczają systemy, systemy operacyjne i aplikacje

w celu zidentyfikowania luk w zabezpieczeniach wynikających z zaniedbań dostawców, działań związanych z administrowaniem systemem lub siecią lub codziennych czynności. Oprogramowanie do wykrywania luk w zabezpieczeniach skanuje komputer pod kątem indeksu wspólnych luk i zagrożeń (CVE) oraz biuletynów zabezpieczeń dostarczonych przez dostawcę oprogramowania. Skanery luk w zabezpieczeniach są w stanie zidentyfikować następujące informacje:

• Wersja systemu operacyjnego działająca na komputerach lub urządzeniach

• Porty IP i Transmission Control Protocol/User Datagram Protocol (TCP/UDP), które nasłuchują

• Aplikacje zainstalowane na komputerach

• Konta ze słabymi hasłami

• Pliki i foldery ze słabymi uprawnieniami

• Domyślne usługi i aplikacje, które mogą wymagać odinstalowania

• Błędy w konfiguracji zabezpieczeń typowych aplikacji

• Komputery narażone na znane lub zgłoszone publicznie luki w zabezpieczeniach

• Informacje o oprogramowaniu EOL/EOS

• Brakujące poprawki i poprawki

• Słabe konfiguracje sieci i źle skonfigurowane lub ryzykowne porty

• Pomoc w weryfikacji spisu wszystkich urządzeń w sieci

Istnieją dwa podejścia do skanowania pod kątem luk w zabezpieczeniach sieci:

Aktywne skanowanie: osoba atakująca wchodzi w bezpośrednią interakcję z siecią docelową w celu znalezienia luk w zabezpieczeniach. Aktywne skanowanie pomaga w symulowaniu ataku na sieć docelową w celu wykrycia luk, które mogą zostać wykorzystane przez atakującego.

Przykład: osoba atakująca wysyła sondy i specjalnie spreparowane żądania do docelowego hosta w sieci w celu zidentyfikowania luk w zabezpieczeniach.

Skanowanie pasywne: osoba atakująca próbuje znaleźć luki w zabezpieczeniach bez bezpośredniej interakcji z siecią docelową. Atakujący identyfikuje luki w zabezpieczeniach na podstawie informacji ujawnionych przez systemy podczas normalnej komunikacji. Skanowanie pasywne identyfikuje aktywne systemy operacyjne, aplikacje i porty w sieci docelowej, monitorując aktywność w celu określenia jej słabych punktów. Takie podejście dostarcza informacji o słabościach, ale nie zapewnia ścieżki do bezpośredniego zwalczania ataków.

Przykład: osoba atakująca odgaduje informacje o systemie operacyjnym, aplikacje oraz wersje aplikacji i usług, obserwując konfigurację i zerwanie połączenia TCP.

Atakujący skanują w poszukiwaniu luk za pomocą narzędzi takich jak Nessus Professional, Qualys, GFI LanGuard i OpenVAS.

Ograniczenia oceny podatności na zagrożenia

Oto niektóre ograniczenia oceny podatności na zagrożenia:

• Oprogramowanie do wykrywania luk w zabezpieczeniach ma ograniczone możliwości wykrywania luk w zabezpieczeniach w określonym momencie punktu w czasie.

• Oprogramowanie do wykrywania luk w zabezpieczeniach musi być aktualizowane po wykryciu nowych luk w zabezpieczeniach lub po wprowadzeniu ulepszeń do używanego oprogramowania.

• Oprogramowanie jest tak skuteczne, jak jego konserwacja wykonywana przez dostawcę oprogramowania i administratora, który z niego korzysta.

• Ocena podatności nie mierzy siły kontroli bezpieczeństwa.

• Oprogramowanie do wykrywania luk w zabezpieczeniach nie jest odporne na błędy inżynierii oprogramowania, które mogą prowadzić do przeoczenia poważnych słabych punktów.

• Do analizy danych po zeskanowaniu i zidentyfikowaniu fałszu wymagana jest ludzka ocena dodatnie i fałszywie ujemna.

• Oprogramowanie do wykrywania luk w zabezpieczeniach nie może określić wpływu zidentyfikowanej luki w zabezpieczeniach w różnych operacjach biznesowych.

• Raporty z oceny podatności na zagrożenia nie zawsze są łatwe do zrozumienia i oceny pod kątem ryzyka czynników i odpowiedź segregacyjna.

• Narzędzia do skanowania luk w zabezpieczeniach mają wąski zakres i nie obejmują wektorów ataków, takich jak Inżynieria społeczna.

• Oprogramowanie do wykrywania luk w zabezpieczeniach ma ograniczone możliwości przeprowadzania testów na żywo w Internecie , aplikacje do wykrywania błędów lub nieoczekiwanego zachowania.

Zastosowana metodologia może mieć wpływ na wyniki badań. Na przykład oprogramowanie skanujące luki w zabezpieczeniach działające w kontekście zabezpieczeń administratora domeny da inne wyniki niż oprogramowanie działające w kontekście zabezpieczeń uwierzytelnionego lub nieuwierzytelnionego użytkownika. Podobnie różne pakiety oprogramowania do wykrywania luk w zabezpieczeniach w różny sposób oceniają bezpieczeństwo i mają unikalne funkcje. Może to wpłynąć na wyniki oceny.

Systemy oceny luk w zabezpieczeniach i bazy danych

Ze względu na rosnącą dotkliwość cyberataków badanie luk w zabezpieczeniach stało się krytyczne, ponieważ pomaga zmniejszyć ryzyko ataków. Badanie luk w zabezpieczeniach zapewnia wiedzę na temat zaawansowanych technik identyfikacji wad lub luk w oprogramowaniu, które mogą zostać wykorzystane przez atakujących. Systemy oceniania luk w zabezpieczeniach i bazy danych luk w zabezpieczeniach są wykorzystywane przez analityków bezpieczeństwa do oceniania luk w systemie informatycznym i dostarczania łącznej oceny ogólnej dotkliwości i ryzyka związanego ze zidentyfikowanymi lukami w zabezpieczeniach. Bazy danych o lukach w zabezpieczeniach gromadzą i przechowują informacje o różnych lukach w zabezpieczeniach obecnych w systemach informatycznych. Poniżej przedstawiono niektóre z systemów oceny luk w zabezpieczeniach i baz danych:

• Wspólny system oceny podatności na zagrożenia (CVSS)

• Typowe luki w zabezpieczeniach i zagrożenia (CVE)

• Krajowa baza danych o lukach w zabezpieczeniach (NVD)

• Wspólne wyliczanie słabych punktów (CWE)

Wspólny system oceny podatności na zagrożenia (CVSS)

CVSS to opublikowany standard, który zapewnia otwarte ramy do komunikowania charakterystyki i wpływu luk w zabezpieczeniach IT. Model ilościowy systemu zapewnia powtarzalne i dokładne pomiary, jednocześnie umożliwiając użytkownikom przeglądanie podstawowych charakterystyk podatności, które zostały wykorzystane do wygenerowania ocen. W związku z tym CVSS dobrze nadaje się jako standardowy system pomiarowy dla branż, organizacji i rządów, które potrzebują dokładnych i spójnych ocen wpływu podatności na zagrożenia. Dwa typowe zastosowania CVSS to ustalanie priorytetów działań zaradczych związanych z lukami w zabezpieczeniach oraz obliczanie wagi wykrytych w systemie luk w zabezpieczeniach. National Vulnerability Database (NVD) dostarcza oceny CVSS dla prawie wszystkich znanych luk w zabezpieczeniach. CVSS pomaga uchwycić główne cechy luki w zabezpieczeniach i tworzy wynik liczbowy odzwierciedlający jej dotkliwość. Ten wynik liczbowy można następnie przełożyć na reprezentację jakościową (taką jak niska, średnia, wysoka lub krytyczna), aby pomóc organizacjom we właściwej ocenie i ustaleniu priorytetów procesów zarządzania podatnościami na zagrożenia. Ocena CVSS składa się z następujących trzech metryk służących do pomiaru podatności.

Podstawowa metryka: reprezentuje nieodłączne cechy luki w zabezpieczeniach.

Metryka czasowa: reprezentuje cechy, które zmieniają się w trakcie istnienia luki.

Metryka środowiskowa: reprezentuje luki w zabezpieczeniach, które są oparte na określonym środowisku lub implementacji.

Metryka waha się od 1 do 10, przy czym 10 jest najpoważniejsze. Wynik CVSS jest obliczany i generowany przez ciąg wektorowy, który reprezentuje wynik liczbowy dla każdej grupy w formie bloku tekstu. Kalkulator CVSS klasyfikuje luki w zabezpieczeniach i dostarcza użytkownikowi informacji o ogólnej wadze i zagrożeniach związanych z luką.

Dotkliwość: Podstawowy zakres wyników

Brak: 0,0

Niski: 0,1-3,9

Średni : 4,0-6,9

Wysoki: 7,0-8,9

Krytyczne: 9,0-10,0

Typowe luki w zabezpieczeniach i zagrożenia (CVE)

CVE® to publicznie dostępna i bezpłatna lista lub słownik standardowych identyfikatorów typowych luk w zabezpieczeniach oprogramowania i zagrożeń. Korzystanie z identyfikatorów CVE lub „identyfikatorów CVE", które są przypisywane przez CVE Numbering Authorities (CNA) z całego świata, zapewnia zaufanie między stronami podczas omawiania lub udostępniania informacji o unikatowych lukach w oprogramowaniu lub oprogramowaniu układowym. CVE zapewnia podstawę do oceny narzędzi i umożliwia wymianę danych w celu automatyzacji cyberbezpieczeństwa. Identyfikatory CVE stanowią punkt odniesienia do oceny zakresu narzędzi i usług, dzięki czemu użytkownicy mogą określić, które narzędzia są najbardziej skuteczne i odpowiednie dla potrzeb ich organizacji. Krótko mówiąc,

produkty i usługi zgodne z CVE zapewniają lepszy zasięg, łatwiejszą interoperacyjność i zwiększone bezpieczeństwo.

Czym jest CVE:

• Jeden identyfikator dla jednej luki w zabezpieczeniach lub narażenia

• Jeden znormalizowany opis dla każdej luki w zabezpieczeniach lub narażenia

• Słownik zamiast bazy danych

• Metoda, dzięki której różne bazy danych i narzędzia „mówią" tym samym językiem

• Droga do interoperacyjności i lepszego zabezpieczenia

• Podstawa oceny usług, narzędzi i baz danych

• Bezpłatne do publicznego pobrania i używania

• Zatwierdzone przez branżę przez CVE Numbering Authorities, CVE Board oraz liczne produkty i usługi, które obejmują CVE

Krajowa baza danych o lukach w zabezpieczeniach (NVD)

NVD to repozytorium rządu Stanów Zjednoczonych zawierające oparte na standardach dane dotyczące zarządzania lukami w zabezpieczeniach. Wykorzystuje protokół Security Content Automation Protocol (SCAP). Takie dane umożliwiają automatyzację zarządzania lukami w zabezpieczeniach, pomiaru bezpieczeństwa i zapewniania zgodności. NVD zawiera bazy danych odniesień do list kontrolnych bezpieczeństwa, luk w oprogramowaniu związanych z bezpieczeństwem, błędnych konfiguracji, nazw produktów i wskaźników wpływu. NVD przeprowadza analizę CVE, które zostały opublikowane w Słowniku CVE. Personel NVD ma za zadanie analizę CVE poprzez agregację punktów danych z opisu, dostarczonych referencji i wszelkich dodatkowych danych, które są publicznie dostępne. Wynikiem tej analizy są metryki wpływu powiązań (Common Vulnerability Scoring System — CVSS), typy luk w zabezpieczeniach (Common Weakness Enumeration — CWE) i oświadczenia dotyczące stosowalności (Common Platform Enumeration — CPE), a także inne istotne metadane. NVD nie przeprowadza aktywnie testów podatności; opiera się na dostawcach, zewnętrznych badaczach bezpieczeństwa i koordynatorach luk w zabezpieczeniach, którzy dostarczają informacje używane do przypisania tych atrybutów.

Wspólne wyliczanie słabych punktów (CWE)

Common Weakness Enumeration (CWE) to system kategorii luk i słabości oprogramowania. Jest sponsorowany przez National Cybersecurity FFRDC, którego właścicielem jest The MITRE Corporation, przy wsparciu US-CERT i National Cyber Security Division Departamentu Bezpieczeństwa Flomeland USA. Najnowsza wersja 3.2 standardu CWE została wydana w styczniu 2019 r. Zawiera ponad 600 kategorii słabych punktów, co daje CWE możliwość skutecznego wykorzystania przez społeczność jako punkt odniesienia dla działań związanych z identyfikacją słabych punktów, ich łagodzeniem i zapobieganiem. Posiada również zaawansowaną technikę wyszukiwania, w której osoby atakujące mogą wyszukiwać i wyświetlać słabe punkty w oparciu o koncepcje badawcze, koncepcje rozwojowe i koncepcje architektoniczne.

Cykl życia zarządzania lukami w zabezpieczeniach

Cykl życia zarządzania lukami w zabezpieczeniach to ważny proces, który pomaga identyfikować i korygować słabe punkty zabezpieczeń, zanim będą mogły zostać wykorzystane. Obejmuje to

zdefiniowanie postawy i zasad ryzyka dla organizacji, utworzenie kompletnej listy zasobów systemów, skanowanie i ocenę środowiska pod kątem słabych punktów i zagrożeń oraz podejmowanie działań w celu złagodzenia zidentyfikowanych słabych punktów. Wdrożenie cyklu życia zarządzania lukami w zabezpieczeniach pomaga uzyskać strategiczną perspektywę dotyczącą możliwych zagrożeń dla cyberbezpieczeństwa i sprawia, że niezabezpieczone środowiska komputerowe są bardziej odporne na ataki. Zarządzanie podatnościami powinno zostać wdrożone w każdej organizacji, ponieważ ocenia i kontroluje ryzyko i podatności w systemie. Proces zarządzania stale bada środowiska IT pod kątem podatności i zagrożeń związanych z systemem. Organizacje powinny utrzymywać odpowiedni program zarządzania podatnościami, aby zapewnić ogólne bezpieczeństwo informacji. Zarządzanie podatnościami zapewnia najlepsze rezultaty, gdy jest wdrażane w sekwencji dobrze zorganizowanych faz.

Fazy związane z zarządzaniem podatnościami to:

• Faza oceny wstępnej

o Zidentyfikuj aktywa i stwórz plan bazowy

• Faza oceny podatności

o Skanowanie luk w zabezpieczeniach

• Faza oceny końcowej

o Ocena ryzyka

o Naprawa

o Weryfikacja

o Monitorowanie

Faza oceny wstępnej

Zidentyfikuj aktywa i utwórz plan bazowy

Faza oceny wstępnej jest fazą przygotowawczą, która obejmuje zdefiniowanie polityk i standardów, wyjaśnienie zakresu oceny, zaprojektowanie odpowiednich procedur ochrony informacji oraz identyfikację i uszeregowanie krytycznych zasobów w celu stworzenia dobrej podstawy dla zarządzania słabymi punktami oraz zdefiniowania opartego na ryzyku krytyczności i wartości każdego systemu. Ta faza obejmuje gromadzenie informacji o zidentyfikowanych systemach w celu zrozumienia zatwierdzonych portów, oprogramowania, sterowników i podstawowej konfiguracji każdego systemu w celu opracowania i utrzymania linii bazowej systemu. Poniżej przedstawiono kroki związane z tworzeniem planu bazowego:

1. Zidentyfikuj i zrozum procesy biznesowe

2. Zidentyfikuj aplikacje, dane i usługi, które obsługują procesy biznesowe i przeprowadzają przeglądy kodu

3. Zidentyfikuj zatwierdzone oprogramowanie, sterowniki i podstawową konfigurację każdego systemu

4. Stwórz inwentaryzację wszystkich zasobów i określ priorytety lub uszereguj krytyczne zasoby

5. Zrozumieć architekturę sieci i sporządzić mapę infrastruktury sieciowej

6. Zidentyfikuj już istniejące kontrole

7. Zrozumieć wdrażanie zasad i praktykować zgodność ze standardami w procesach biznesowych

8. Określ zakres oceny

9. Stwórz procedury ochrony informacji wspierające skuteczne planowanie, harmonogramowanie, koordynację i logistykę

Klasyfikuj zidentyfikowane aktywa zgodnie z potrzebami biznesowymi. Klasyfikacja pomaga zidentyfikować wysokie ryzyka biznesowe w organizacji. Nadaj priorytet ocenianym aktywom na podstawie wpływu ich awarii i ich niezawodności na biznes. Ustalanie priorytetów pomaga:

• Oceń i zadecyduj o rozwiązaniu konsekwencji awarii aktywów

• Zbadaj poziom tolerancji ryzyka

• Zorganizuj metody ustalania priorytetów zasobów

Faza oceny podatności

Ta faza jest bardzo ważna w zarządzaniu podatnościami. Faza oceny podatności odnosi się do identyfikacji luk w infrastrukturze organizacji, w tym w systemie operacyjnym, aplikacjach internetowych i serwerze WWW. Pomaga zidentyfikować kategorię i krytyczność podatności w organizacji oraz minimalizuje poziom ryzyka. Ostatecznym celem skanowania pod kątem luk w zabezpieczeniach jest skanowanie, badanie, ocena i zgłaszanie luk w systemie informatycznym organizacji. Skanowanie luk w zabezpieczeniach można również przeprowadzić na odpowiednich szablonach zgodności, aby ocenić słabości infrastruktury organizacji pod kątem odpowiednich wytycznych dotyczących zgodności. Faza oceny obejmuje badanie architektury sieci, ocenę zagrożeń dla środowiska, wykonanie testów penetracyjnych, badanie i ocenę bezpieczeństwa fizycznego, analizę zasobów fizycznych, ocenę bezpieczeństwa operacyjnego, przestrzeganie polityk i procedur oraz ocenę współzależności infrastruktury.

Etapy fazy oceny:

1. Zbadaj i oceń bezpieczeństwo fizyczne

2. Sprawdź, czy nie występują błędne konfiguracje i błędy ludzkie

3. Uruchom skanowanie w poszukiwaniu luk za pomocą narzędzi

4. Wybierz typ skanowania w oparciu o wymagania organizacji lub zgodności

5. Zidentyfikuj i uszereguj luki w zabezpieczeniach

6. Zidentyfikuj wyniki fałszywie dodatnie i fałszywie ujemne

7. Zastosuj kontekst biznesowy i technologiczny do wyników skanowania

8. Przeprowadź zbieranie informacji OSINT w celu zweryfikowania luk w zabezpieczeniach

9. Utwórz raport ze skanowania narażenia na atak

Faza oceny końcowej

Faza po ocenie, zwana również fazą rekomendacji, jest przeprowadzana po ocenie ryzyka i na jej podstawie. Charakterystyka ryzyka jest kategoryzowana według kluczowych kryteriów, co pomaga nadać priorytet liście zaleceń. Zadania realizowane w fazie pooceny obejmują:

• Stworzenie listy priorytetów dla rekomendacji ewaluacyjnych na podstawie analizy wpływu

• Opracowanie planu działania w celu wdrożenia proponowanych środków zaradczych

• Wyciąganie wniosków w celu udoskonalenia całego procesu w przyszłości

• Prowadzenie szkoleń dla pracowników

Ocena końcowa obejmuje ocenę ryzyka, środki zaradcze, weryfikację i monitorowanie.

Ocena ryzyka

W fazie oceny ryzyka ryzyka są identyfikowane, charakteryzowane i klasyfikowane wraz z technikami stosowanymi do kontrolowania lub ograniczania ich skutków. Jest to ważny krok w kierunku identyfikacji słabych punktów bezpieczeństwa w architekturze IT organizacji. na tym etapie wszystkie poważne niepewności, które są związane z systemem, są oceniane i ustalane priorytety oraz planowane są środki zaradcze w celu trwałego wyeliminowania wad systemu. Ocena ryzyka podsumowuje podatność na zagrożenia i poziom ryzyka zidentyfikowany dla każdego z wybranych aktywów. Określa, czy poziom ryzyka dla danego składnika aktywów jest wysoki, umiarkowany czy niski. Działania naprawcze planowane są na podstawie ustalonego poziomu ryzyka. Na przykład luki w zabezpieczeniach sklasyfikowane jako wysokie ryzyko są atakowane w pierwszej kolejności, aby zmniejszyć szanse na wykorzystanie, które mogłoby niekorzystnie wpłynąć na organizację.

Zadania realizowane w fazie oceny ryzyka obejmują:

o Przeprowadź kategoryzację ryzyka na podstawie rankingu ryzyka (na przykład krytyczne, wysokie, średnie i niskie)

o Oceń poziom wpływu

o Określić poziom zagrożenia i ryzyka

Remediacja

Naprawa to proces stosowania poprawek w systemach podatnych na ataki w celu złagodzenia lub zmniejszenia wpływu i wagi luk w zabezpieczeniach. Obejmują one takie kroki, jak ocena luk w zabezpieczeniach, lokalizowanie zagrożeń i projektowanie reakcji na luki w zabezpieczeniach. Ważne jest, aby proces naprawczy był konkretny, mierzalny, osiągalny, odpowiedni i określony w czasie. Ta faza jest inicjowana po pomyślnym wdrożeniu etapu podstawowego i etapu oceny. Zadania realizowane w fazie remediacji obejmują:

o Priorytetyzacja środków zaradczych w oparciu o ranking ryzyka

o Opracuj plan działania w celu wdrożenia zalecenia lub środków zaradczych

o Wykonaj analizę pierwotnej przyczyny

o Zastosuj poprawki i poprawki

o Przechwytywanie wyciągniętych wniosków

o Przeprowadź szkolenie uświadamiające

o Wykonaj obsługę wyjątków i akceptację ryzyka dla luk w zabezpieczeniach, których nie można naprawić

Weryfikacja

W tej fazie zespół ds. bezpieczeństwa przeprowadza ponowne skanowanie systemów, aby ocenić, czy wymagane środki zaradcze zostały zakończone i czy poszczególne poprawki zostały zastosowane w zasobach, których dotyczy problem. Ta faza obejmuje weryfikację środków zaradczych zastosowanych w celu ograniczenia ryzyka. Zapewnia przejrzysty wgląd w firmę i pozwala zespołowi ds. bezpieczeństwa sprawdzić, czy wszystkie poprzednie fazy zostały doskonale wykorzystane, czy nie. Weryfikację można przeprowadzić za pomocą różnych środków, takich jak systemy biletowe, skanery i raporty. Zadania wykonywane w fazie weryfikacji obejmują:

o Ponowne skanowanie systemów w celu określenia, czy zastosowana poprawka skutecznie usuwa lukę

o Przeprowadzanie analizy dynamicznej

o Przegląd powierzchni ataku

Monitorowanie

Organizacje muszą przeprowadzać regularne monitorowanie w celu utrzymania bezpieczeństwa systemu. Ciągłe monitorowanie identyfikuje potencjalne zagrożenia i wszelkie nowe luki, które wyewoluowały. Zgodnie z najlepszymi praktykami w zakresie bezpieczeństwa, wszystkie fazy zarządzania lukami w zabezpieczeniach muszą być przeprowadzane regularnie. Ta faza obejmuje monitorowanie incydentów przy użyciu narzędzi, takich jak IDS/IPS, SIEM i zapory ogniowe. Wdraża ciągłe monitorowanie bezpieczeństwa, aby udaremniać stale ewoluujące zagrożenia. Do zadań realizowanych w fazie monitoringu należą:

o Okresowe skanowanie i ocena podatności

o Terminowe usuwanie zidentyfikowanych luk w zabezpieczeniach

o Monitorowanie dzienników wykrywania włamań i zapobiegania włamaniom

o Wdrażanie polityk, procedur i kontroli

Typy klasyfikacji i oceny podatności na zagrożenia

Każda luka występująca w systemie może być niebezpieczna i spowodować poważne szkody dla organizacji. Ważne jest, aby etyczni hakerzy posiadali wiedzę na temat różnych rodzajów podatności, które mogą wykorzystać, wraz z różnymi technikami oceny podatności. W tej sekcji modułu omówiono różne rodzaje luk w zabezpieczeniach i oceny podatności.

Klasyfikacja podatności

Luki obecne w systemie lub sieci są podzielone na następujące kategorie:

Błędne konfiguracje/słabe konfiguracje

Błędna konfiguracja jest najczęstszą luką w zabezpieczeniach i jest spowodowana głównie błędem ludzkim. Umożliwia atakującym włamanie się do sieci i uzyskanie nieautoryzowanego dostępu do systemów. Błędne konfiguracje mogą wystąpić zarówno celowo, jak i nieumyślnie, i wpływają na serwery WWW, platformy aplikacji, bazy danych i sieci. Atakujący mogą wykrywać błędne konfiguracje

za pomocą różnych technik skanowania, a następnie wykorzystywać systemy zaplecza. Dlatego administratorzy muszą zmienić domyślną konfigurację urządzeń i zoptymalizować ich bezpieczeństwo.

Błędne konfiguracje sieci

Częste zmiany w urządzeniach sieciowych i zabezpieczających są nieuniknione i niezbędne do usprawnienia działalności firmy. Jednak administratorzy powinni upewnić się, że wszystkie komponenty sieci są odpowiednio skonfigurowane, ponieważ wszelkie pętle we wprowadzanych zmianach mogą powodować niekorzystne skutki dla sieci, takie jak obniżenie wydajności, przerwy w działaniu usług i włamania do sieci. Poniżej przedstawiono kilka przykładów słabych konfiguracji sieciowych.

- Niepewne protokoły

Niezabezpieczone protokoły przesyłają informacje lub dane w postaci zwykłego tekstu bez implementacji jakichkolwiek technik szyfrowania w celu zabezpieczenia danych. Korzystanie z wrażliwych protokołów powoduje problemy z uwierzytelnianiem i integralnością, ponieważ osoby atakujące mogą wykorzystać niezaszyfrowane pliki lub transmisję danych i manipulować przesyłanymi danymi. Atakujący mogą również uzyskać zdalny dostęp do podatnego na ataki systemu po przechwyceniu poświadczeń udostępnianych w postaci zwykłego tekstu. Tej luki można uniknąć, usuwając urządzenia działające na niezabezpieczonych protokołach i wdrażając scentralizowany węzeł główny w celu aktualizacji protokołów.

- Otwarte porty i usługi

Komunikacja użytkownika z aplikacją lub usługą może odbywać się za pośrednictwem numerów portów TCP lub UDP, które przyjmują i przesyłają informacje w postaci pakietów. Adresy źródłowe i docelowe można zidentyfikować za pomocą przypisanych im unikalnych adresów IP. Oprócz tego wiele portów działa w sieci dla określonych usług. Serwery często działają z niektórymi otwartymi portami, ale wszystkie otwarte porty nie są niebezpieczne, chyba że są źle skonfigurowane, niezałatane lub zaimplementowane ze słabymi regułami bezpieczeństwa. Jednak otwarte porty muszą być ograniczone i wykorzystywane tylko do ważnych usług. Pozostawienie otwartych portów dla niepotrzebnych usług może spowodować pojawienie się w sieci nowych zagrożeń. Otwarte porty i usługi mogą prowadzić do utraty danych lub ataków typu „odmowa usługi” (DoS) i umożliwić atakującym przeprowadzanie dalszych ataków na inne podłączone urządzenia. Administratorzy muszą stale sprawdzać niepotrzebne lub niezabezpieczone porty i usługi, aby zmniejszyć ryzyko dla sieci.

- Błędy

Niewłaściwa konfiguracja aplikacji lub usług może generować raporty o błędach podczas ładowania stron. Takie raporty o błędach mogą dostarczyć szczegółowych informacji atakującym poszukującym luk w zabezpieczeniach, luk w zabezpieczeniach aplikacji, błędów programistycznych lub innych exploitów. Używanie przestarzałego oprogramowania może również generować błędy bezpieczeństwa, które mogą być podatne na zdalne ataki przy użyciu technik takich jak wstrzykiwanie kodu w celu manipulowania aplikacją. Aby zapobiec tej luce, należy zastosować wykwalifikowane praktyki programistyczne w taki sposób, aby aplikacja nie ujawniała krytycznych informacji, które mogłyby pomóc atakującym w wykorzystaniu serwera aplikacji.

- Słabe szyfrowanie

Wdrożenie odpowiednich metod szyfrowania może zabezpieczyć dane przesyłane w sieci oraz dane zapisywane na urządzeniach pamięci masowej. Dostęp do zaszyfrowanych plików można uzyskać tylko

za pomocą odpowiedniego odszyfrowanego klucza posiadanego przez klienta lub aplikację. Słabe szyfrowanie może umożliwić atakującym przeprowadzanie ataków typu man-in-the-middle, wąchanie ruchu w celu modyfikowania danych, a następnie podszywanie się pod legalną usługę w celu komunikowania się z użytkownikami końcowymi za pomocą fałszywych informacji. Oto niektóre przyczyny słabego szyfrowania:

• Używanie słabego algorytmu szyfrowania

• Generowanie klucza z możliwymi do odgadnięcia danymi uwierzytelniającymi

• Niepewna dystrybucja kluczy

Błędne konfiguracje hosta

Atakujący mogą wykorzystać luki w konfiguracji serwera hosta, aby manipulować zasobami i uzyskać zdalny dostęp administratora. Funkcje debugowania mogą zostać aktywowane, a nieznani użytkownicy mogą uzyskać uprawnienia administracyjne. Luki te mogą umożliwić atakującym obejście mechanizmów uwierzytelniania i dostęp do krytycznych informacji, prawdopodobnie z podwyższonymi uprawnieniami. Poniżej przedstawiono kilka przykładów słabej konfiguracji hosta.

- Otwórz uprawnienia

Nadanie użytkownikowi lub grupie użytkowników zbędnych uprawnień dostępu do aplikacji lub plików może prowadzić do problemów związanych z bezpieczeństwem, takich jak wyciek danych lub uszkodzenie funkcjonalności systemu. Zarządzanie uprawnieniami to skomplikowane zadanie, w którym administratorzy lub użytkownicy mogą potencjalnie popełniać błędy, takie jak zezwalanie nieznanym gościom na odczyt i zapis krytycznych plików. Osoba atakująca może również zwiększyć uprawnienia, używając niepotrzebnie utworzonych kont w celu uzyskania dostępu do niezabezpieczonych plików lub uruchamiania poleceń w systemie operacyjnym (OS).

- Niezabezpieczone konta root

Używanie przypisanych przez producenta domyślnych poświadczeń konta administracyjnego dla bazy danych lub aplikacji może prowadzić do problemów z bezpieczeństwem systemu. Niewdrożenie bezpiecznej polityki prywatności haseł może pozwolić atakującym na odgadnięcie poświadczeń przy użyciu różnych technik brute-force.

Wady aplikacji

Wady aplikacji to luki w zabezpieczeniach aplikacji, które są wykorzystywane przez atakujących. Aplikacje powinny być zabezpieczone za pomocą walidacji i autoryzacji użytkownika. Wadliwe aplikacje stwarzają zagrożenia dla bezpieczeństwa, takie jak manipulowanie danymi i nieautoryzowany dostęp do magazynów konfiguracji. Jeśli aplikacje nie są zabezpieczone, poufne informacje mogą zostać utracone lub uszkodzone. Dlatego programiści muszą rozumieć anatomię typowych luk w zabezpieczeniach i opracowywać wysoce bezpieczne aplikacje, zapewniając odpowiednią weryfikację i autoryzację użytkownika. Poniżej przedstawiono niektóre wady aplikacji, które mogą zostać wykorzystane przez osoby atakujące.

Przepełnienia bufora

Przepełnienia bufora to typowe luki w oprogramowaniu wynikające z błędów w kodowaniu, które umożliwiają atakującym uzyskanie dostępu do systemu docelowego. W ataku z przepełnieniem bufora atakujący podważa działanie programów i próbuje przejąć kontrolę nad systemem poprzez zapisywanie treści poza przydzielonym rozmiarem bufora. Główną przyczyną tej luki jest

niedostateczne sprawdzanie granic w programie. Bufor nie może obsłużyć danych poza swój limit, powodując przepływ danych do sąsiednich lokalizacji pamięci i nadpisywanie ich wartości danych. W przypadku przepełnienia bufora systemy często ulegają awariom, stają się niestabilne lub wykazują błędne zachowanie programu.

Wycieki pamięci

Wyciek pamięci lub wyciek zasobów to niezamierzona klasa zużycia pamięci, która występuje, gdy programista nie usunie przypisanego bloku pamięci, gdy nie jest już potrzebny. Jest to spowodowane wyjątkowymi okolicznościami, błędami i niepewnością, która część kodu jest odpowiedzialna za zwolnienie pamięci. Warunki te zależą od konsekwencji aplikacji w przypadkach takich jak krótkotrwałe aplikacje użytkownika, długotrwałe aplikacje użytkownika i procesy jądra. Wyciek pamięci powoduje obawy związane z niezawodnością oprogramowania i zachęca złośliwego aktora do przejęcia kontroli nad zaatakowanym systemem w celu przeprowadzenia ataków, takich jak DoS w celu awarii systemu, wstrzyknięcia złośliwego kodu w celu zmiany zachowania aplikacji i przejęcia kontroli nad programem. Narzędzia takie jak Valgrind, który jest kompatybilny ze środowiskiem Unix/Linux, śledzą wycieki pamięci i wyświetlają stan środowiska oprogramowania.

Wyczerpanie zasobów

Atak polegający na wyczerpaniu zasobów uszkadza serwer, wysyłając wiele żądań zasobów z różnych lokalizacji w celu wykorzystania błędów oprogramowania, co powoduje zawieszenie systemu i serwera lub awarię systemu. W aplikacjach zarządzanie pamięcią zawiera błąd wycieku pamięci, który może być łatwo wykorzystany przez zdalnych atakujących. Jest podobny do ataku DoS, ponieważ może skompromitować lub wyczerpać zasoby dostępne dla systemu w sieci. Z powodu błędów projektowych lub kodu każda interakcja lub połączenie ustanowione między klientem a serwerem może marnować zasoby lub zużywać więcej zasobów niż jest to wymagane.

Przepełnienia całkowitoliczbowe

Przepełnienie liczb całkowitych występuje, gdy funkcja arytmetyczna generuje i próbuje zapisać wartość całkowitą większą niż maksymalna wartość, jaką może przechowywać przydzielona przestrzeń pamięci. Te warunki przepełnienia mogą prowadzić do niepożądanego zachowania oprogramowania. Brak wcześniejszego wykrycia stanu przepełnienia może spowodować problemy z bezpieczeństwem i niezawodnością programu. Oprócz uzyskiwania niedokładnych wyników i powodowania niestabilności oprogramowania, przepełnienia liczb całkowitych mogą również prowadzić do przepełnień bufora i otwierać drzwi dla atakujących do manipulowania wartościami, co ostatecznie prowadzi do losowego lub złośliwego wykonania kodu.

Wyłuskanie wskaźnika/obiektu zerowego

Znany również jako odwołanie zerowe, wskaźnik zerowy to wartość przechowywana w celu wskazania, że wskaźnik nie jest wyznaczony do żadnego prawidłowego obiektu; wskazuje również nieprawidłową lokalizację pamięci. Większość problemów ze wskaźnikiem zerowym prowadzi do typowych problemów z niezawodnością oprogramowania, ale gdy osoba atakująca celowo uruchomi wyłuskanie wskaźnika zerowego, może być w stanie wykorzystać wynikowy wyjątek do obejścia logiki bezpieczeństwa i ujawnienia przez aplikację szczegółów debugowania, które mogą pomóc w opracowywaniu strategii kolejnych ataków. Programy na ogół wykorzystują te wskaźniki zerowe do wskazania warunku, takiego jak ostatni punkt

nieokreślona długość i niekompetencja do wykonywania niektórych operacji; ten typ użycia wskaźnika zerowego jest porównywalny z typami zerowalnymi i bez wartości w typie opcji. Wyłuskanie wskaźnika zerowego może uniemożliwić wykonanie programu lub spowodować jego awarię i zamknięcie.

Wstrzykiwanie DLL

Gdy aplikacja uruchamia kod innej firmy lub niezaufany kod, który ładuje zestaw lub plik DLL, osoba atakująca może wykorzystać tę lukę w celu wstrzyknięcia złośliwej biblioteki DLL do aktualnie uruchomionego procesu i wykonania złośliwego kodu. Ponadto ładowanie plików DLL bez określenia pełnej ścieżki lokalizacji pliku może umożliwić atakującym utworzenie złośliwej biblioteki DLL i umieszczenie jej w lokalizacji poprzedzającej ścieżkę prawidłowego pliku DLL. W rezultacie aplikacja wykonuje szkodliwą bibliotekę DLL. Aby zapobiec takim lukom w zabezpieczeniach, programiści nigdy nie mogą ładować niezaufanych bibliotek DLL z danych wprowadzonych przez użytkownika i muszą zawsze wywoływać biblioteki DLL, określając pełną ścieżkę lokalizacji pliku.

Warunki wyścigu

Sytuacja wyścigu to niepożądany incydent, który ma miejsce, gdy oprogramowanie lub program systemowy jest zależny od wykonywania procesów w sekwencji i od czasu programów. Ten warunek występuje, gdy system, który obsługuje zdarzenia w formacie sekwencyjnym, jest zmuszony do wykonywania wielu operacji jednocześnie. Warunek skutkuje nieprawidłowym wykonaniem programu lub błędami w oprogramowaniu. Typowa sytuacja wyścigu występuje, gdy wiele wątków jest zależnych od udostępnionego zasobu. Większość warunków wyścigu wpływa na bezpieczeństwo związane z systemem. Osoba atakująca może przeprowadzić ataki typu DoS lub eskalację uprawnień, uzyskując dostęp do udostępnionego zasobu zaufanego procesu.

- Czas sprawdzenia / Czas użytkowania

Czas sprawdzenia lub czas użycia (TOC/TOU) to błąd oprogramowania, który występuje z powodu wyścigu, który występuje po sprawdzeniu stanu określonego segmentu systemu w określonym czasie i przed czasem wykorzystania wyników sprawdzania. Mówiąc prościej, definiuje się ją jako zmianę stanu systemu od momentu sprawdzenia predykcji do czasu podjęcia działań na jej podstawie. Jest to luka związana z synchronizacją, która występuje, gdy system przyznaje uprawnienia dostępu do żądania zasobu. Na przykład, gdy użytkownik chce przelać kwotę z jednego konta na drugie, ryzyko ataku istnieje w trakcie transakcji między TOC a TOU, tj. od momentu sprawdzenia, czy żądana kwota jest dostępna dla czas przekazania tej kwoty.

Niewłaściwa obsługa danych wejściowych

Obsługa danych wejściowych jest zdefiniowana jako weryfikacja funkcjonalności aplikacji, takich jak walidacja, filtrowanie, oczyszczanie, szyfrowanie i deszyfrowanie danych wejściowych. Brak weryfikacji danych wejściowych skutkuje podatnościami. Walidacja danych wejściowych jest obowiązkowa w celu zapewnienia integralności przychodzących danych poprzez sprawdzanie i porównywanie danych z typem oczekiwanych danych. Dane pochodzące zarówno z zaufanych, jak i niezaufanych źródeł są narażone na ryzyko uszkodzenia przez atakujących przy użyciu takich technik, jak iniekcja SQL, cross-site scripting i przepełnienie bufora. Implementacja walidacji zarówno po stronie klienta, jak i po stronie serwera zapewnia skuteczne uwierzytelnianie danych.

Niewłaściwa obsługa błędów

Niewłaściwa obsługa błędów ma miejsce, gdy osoba atakująca wykorzystuje system bezpieczeństwa, wykorzystując informacje o błędach. Większość aplikacji internetowych lub serwerów ujawnia

szczegółowe informacje o błędach, takich jak zrzuty bazy danych i ślady stosu. Mogą również generować szczegółowe błędy, które obejmują informacje o stanie systemu, takie jak błąd wywołania systemowego, przekroczenie limitu czasu, wyjątki i dostępność danych, co może pomóc atakującemu w analizie i zaatakowaniu systemu. Fail-open jest jednym z problemów bezpieczeństwa spowodowanych niewłaściwą obsługą błędów. Fail-open definiuje się jako przyznanie dostępu po awarii systemu lub odmowie dostępu.

Słabe zarządzanie poprawkami

Łatka to niewielka część oprogramowania zaprojektowana w celu naprawienia problemów, luk w zabezpieczeniach i błędów, a także poprawy użyteczności lub wydajności programu komputerowego lub danych pomocniczych. Dostawcy oprogramowania dostarczają łatki, które zapobiegają nadużyciom i zmniejszają prawdopodobieństwo zagrożeń wykorzystujących określoną lukę w zabezpieczeniach. Niezałatane oprogramowanie może narazić aplikację, serwer lub urządzenie na różne ataki. Poniżej przedstawiono kilka przykładów złego zarządzania poprawkami.

Niepatchowane serwery

Serwery są niezbędnym elementem infrastruktury każdej organizacji. Było kilka przypadków, w których organizacje korzystały z niezałatanych i źle skonfigurowanych serwerów, które zagrażały bezpieczeństwu i integralności danych w ich systemie. Hakerzy wyszukują te luki w zabezpieczeniach serwerów i wykorzystują je. Te niezałatane serwery służą jako centrum atakujących lub punkt wejścia do sieci. Może to prowadzić do ujawnienia prywatnych danych, strat finansowych i przerwania działalności. Regularne aktualizowanie oprogramowania i prawidłowe utrzymywanie systemów poprzez łatanie i naprawianie błędów może pomóc w łagodzeniu luk w zabezpieczeniach powodowanych przez niezałatane serwery.

Niepoprawione oprogramowanie układowe

Niezałatane oprogramowanie układowe może prowadzić do powstania luk, przez które osoba atakująca może łatwo dostać się do sieci korporacyjnej i ukraść krytyczne informacje lub uszkodzić krytyczne zasoby. Luki w oprogramowaniu sprzętowym umożliwiają atakującym wstrzykiwanie złośliwego kodu, infekowanie legalnych aktualizacji, usuwanie danych przechowywanych na dysku twardym, a w niektórych przypadkach nawet sterowanie sprzętem systemowym ze zdalnej lokalizacji. Aby złagodzić takie luki, specjaliści ds. bezpieczeństwa muszą regularnie sprawdzać i aktualizować oprogramowanie układowe.

Niepoprawiony system operacyjny

Atakujący wykorzystują systemy, których systemy operacyjne nie zostały załatane, jako źródło wektora infekcji, aby zainfekować inne systemy lub urządzenia podłączone do tej samej sieci. Atakujący skanują systemy z niezałatanymi systemami operacyjnymi i wykorzystują te systemy do rozprzestrzeniania złośliwego oprogramowania na inne systemy podłączone do sieci. Jeśli osoba atakująca zidentyfikuje lukę w pliku jądra systemu operacyjnego lub w bibliotece współdzielonej, może ją wykorzystać do próby eskalacji uprawnień przy użyciu złośliwego oprogramowania, które uzyskuje dostęp na poziomie systemu lub administratora. Specjaliści ds. bezpieczeństwa muszą włączyć funkcję automatycznej aktualizacji, aby automatycznie i regularnie aktualizować systemy operacyjne.

Niepoprawione aplikacje

Niezałatane luki w zabezpieczeniach aplikacji umożliwiają atakującym wstrzyknięcie i uruchomienie złośliwego kodu poprzez wykorzystanie znanego błędu oprogramowania. Ogólnie rzecz biorąc, żadne

oprogramowanie ani aplikacje nie są bezbłędne. Dostawcy oprogramowania często publikują łatki usuwające zidentyfikowane luki w zabezpieczeniach. Niezałatane aplikacje torują drogę atakującym do wykorzystywania i naruszania bezpieczeństwa systemów i oprogramowania. Dlatego ważne jest, aby organizacje regularnie stosowały łaty luk w zabezpieczeniach i aktualizowały aplikacje.

Wady projektowe

Luki wynikające z wad projektowych są uniwersalne dla wszystkich urządzeń i systemów operacyjnych. Luki projektowe, takie jak nieprawidłowe szyfrowanie lub słaba weryfikacja danych, odnoszą się do błędów logicznych w funkcjonalności systemu, które atakujący wykorzystują do obejścia mechanizmu wykrywania i uzyskania dostępu do bezpiecznego systemu.

Ryzyka osób trzecich

Osoba trzecia może stać się kolejnym potencjalnym zagrożeniem dla przedsiębiorstw. Usługi lub produkty stron trzecich mogą mieć dostęp do uprzywilejowanych systemów i aplikacji, za pośrednictwem których można naruszyć informacje finansowe, dane klientów i pracowników oraz procesy w łańcuchu dostaw przedsiębiorstwa. Strona trzecia może być godna zaufania, ale przedsiębiorstwa zwykle nie sprawdzają, czy zachowują odpowiednie standardy i środki bezpieczeństwa; ostatecznie mogą stać się zagrożeniem dla sieci korporacyjnej. Główne zagrożenia związane z podmiotami zewnętrznymi obejmują kradzież tożsamości, kradzież własności intelektualnej, naruszenia danych, implantację złośliwego oprogramowania bez plików oraz włamania do sieci. Organizacja powinna być świadoma zagrożeń związanych z podmiotami zewnętrznymi i prowadzić ciągłe procesy zarządzania ryzykiem w środowisku w czasie rzeczywistym. Poniżej przedstawiono różne rodzaje ryzyka związane z zależnością od osób trzecich.

Zarządzanie dostawcami: Jest to czynność polegająca na wyborze dostawców i ocenie ryzyka związanego z usługami i produktami osób trzecich. Obejmuje wszystkie podstawowe programy i procesy wymagane przez organizację do obsługi i zarządzania operacjami i komunikacją z zewnętrznymi dostawcami. Organizacje często polegają na zewnętrznych dostawcach, aby zaoszczędzić na wydatkach, odeprzeć rywalizację rynkową, zwiększyć produktywność i uzyskać większe zyski przy mniejszym wysiłku. Jeśli jednak dostawca zewnętrzny nie jest zaufany lub nie przestrzega wymaganych standardów, może stanowić zagrożenie dla danych lub informacji organizacji. Organizacja może być zmuszona do poniesienia wszelkich konsekwencji w przypadku naruszenia. Najlepsze podejście do wykrywania ryzyka związanego z podmiotami zewnętrznymi obejmuje stosowanie najlepszych praktyk zarządzania dostawcami wraz z egzekwowaniem systemów zarządzania ryzykiem dostawców zewnętrznych.

- Integracja systemu: Jest to proces polegający na korzystaniu z usług stron trzecich lub zatrudnianiu dostawców zewnętrznych do prowadzenia operacji biznesowych. Gdy strona trzecia hostuje usługi lub tworzy oprogramowanie dla firmy, integratorzy systemów potrzebują pełnego dostępu do systemów/aplikacji. Ponieważ integratorzy pracują wewnątrz firmy, mogą łatwo omijać zapory ogniowe i rozwiązania bezpieczeństwa oraz instalować w sieci złośliwe oprogramowanie lub oprogramowanie szpiegujące. Integratorzy mogą również zastosować techniki skanowania portów w celu uzyskania pakietów danych bezpośrednio z sieci. Organizacje muszą nadzorować działania dostawców zewnętrznych i postęp projektów.

- Brak wsparcia ze strony dostawców: Organizacje często polegają na zewnętrznych dostawcach w zakresie zarządzania bezpieczeństwem systemów w sieci. W takich przypadkach sprzedawcom powierza się wykrywanie i naprawianie problemów, zanim zostaną one wykorzystane, i stają się członkami środowiska pracy organizacji. Ponieważ mają do czynienia ze złożoną infrastrukturą

sieciową, niewystarczająca wiedza w zakresie obsługi systemów bezpieczeństwa lub identyfikowania zagrożeń może otworzyć drogę do nowych cyberataków. Dostawcy powinni być biegli w znajdowaniu problemów i powinni być zachęcani do utrzymywania wysokiej jakości pracy oraz zapewniania bezpieczeństwa i aktualizacji systemów.

Ryzyko związane z łańcuchem dostaw: Większość urządzeń i systemów sieciowych w organizacji jest często kupowana od strony trzeciej. Korzystanie z takiego sprzętu w każdym segmencie wzdłuż łańcucha dostaw może potencjalnie stwarzać zagrożenie bezpieczeństwa z powodu niewłaściwej konserwacji lub konfiguracji. Należy wdrożyć odpowiednie środki kontroli bezpieczeństwa dla sprzętu/urządzeń lub oprogramowania, które organizacje kupują lub wypożyczają od strony trzeciej. Na przykład oprogramowanie lub sprzęt zakupione od strony trzeciej mogą nie zostać odpowiednio oczyszczone. W takich przypadkach złośliwe oprogramowanie ukryte wewnątrz wcześniej dostarczonego sprzętu może zainfekować nowe systemy wdrożone w organizacji i rozprzestrzenić się na wszystkie inne urządzenia podłączone do sieci.

Tworzenie kodu na zewnątrz: W niektórych przypadkach przedsiębiorstwa nie dysponują wszystkimi zasobami wymaganymi do tworzenia produktów w swoim środowisku. W takich przypadkach organizacje zatrudniają strony trzecie w celu opracowania produktów lub oprogramowania. W takich przypadkach organizacje powinny stworzyć bezpieczne środowisko, w którym projektanci zewnętrzni będą mogli opracowywać i oceniać tworzony kod. Organizacje powinny również określić, gdzie kod ma być przechowywany i umieścić odpowiednie zabezpieczenia w przestrzeni magazynowej, ponieważ kod może zostać skradziony w celu opracowania podobnych projektów. Po zakończeniu procesu kodowania produkt wymaga dokładnych testów, a programiści powinni zadbać o to, aby uniemożliwić nieautoryzowany dostęp do zasobów aplikacji. Ważne jest również, aby zasoby, do których aplikacja uzyskuje dostęp, były przechowywane w chronionym środowisku, a dane były szyfrowane przed przesłaniem przez sieć.

System Sprawl/nieudokumentowane aktywa

Podatność na rozprzestrzenianie się systemu powstaje w sieci organizacji z powodu zwiększonej liczby połączeń systemowych lub serwerowych bez odpowiedniej dokumentacji lub zrozumienia ich obsługi. Zasoby te są często zaniedbywane z biegiem czasu, co czyni je podatnymi na ataki. Może to również prowadzić do kosztownych konserwacji, ponieważ każdy wrażliwy zasób będzie uwzględniony w kosztach konserwacji za każdym razem, gdy wymagana jest skuteczna konserwacja lub konieczne jest zaplanowanie najnowszych aktualizacji sprzętu lub oprogramowania. Ponadto nieudokumentowane zasoby nie obsługują multipleksowanych kopii zapasowych baz danych ani szybkiego przesyłania strumieniowego, co zmusza zespoły IT do wyboru między szybkim tworzeniem kopii zapasowych a optymalizacją pojemności.

Niewłaściwe zarządzanie certyfikatami i kluczami

Niewłaściwe zarządzanie certyfikatami i kluczami może prowadzić do wielu luk w zabezpieczeniach, które umożliwiają atakującym przeprowadzanie ataków polegających na łamaniu haseł i eksfiltracji danych. Klucze przechowywane na serwerach są podatne na ataki. Specjaliści ds. bezpieczeństwa muszą upewnić się, że klucze są przechowywane w zaszyfrowanym formacie i są odszyfrowywane tylko w chronionym, bezpiecznym środowisku. Przechowywanie lub zachowywanie starszych lub nieaktualnych kluczy również stanowi poważne zagrożenie dla organizacji. Klucze prywatne używane z certyfikatami muszą być przechowywane w wysoce zabezpieczonym środowisku; w przeciwnym razie osoba nieupoważniona może przechwycić klucze i uzyskać dostęp do poufnych danych lub krytycznych systemów.

Rodzaje oceny podatności

Poniżej podano różne rodzaje oceny podatności:

* Aktywna ocena

Rodzaj oceny podatności, w której skanery sieciowe identyfikują hosty, usługi i luki obecne w sieci. Aktywne skanery sieciowe mogą zmniejszyć inwazyjność przeprowadzanych przez siebie kontroli.

* Ocena pasywna

Oceny pasywne analizują ruch obecny w sieci, aby zidentyfikować aktywne systemy, usługi sieciowe, aplikacje i luki w zabezpieczeniach. Oceny pasywne dostarczają również listę użytkowników, którzy aktualnie uzyskują dostęp do sieci.

* Ocena zewnętrzna

Ocena zewnętrzna polega na zbadaniu sieci z punktu widzenia hakera w celu zidentyfikowania exploitów i luk w zabezpieczeniach dostępnych dla świata zewnętrznego. Tego typu oceny wykorzystują urządzenia zewnętrzne, takie jak zapory ogniowe, routery i serwery. Zewnętrzna ocena szacuje zagrożenie atakami na bezpieczeństwo sieci spoza organizacji. Określa poziom bezpieczeństwa sieci zewnętrznej i zapory sieciowej. Poniżej przedstawiono niektóre z możliwych etapów przeprowadzania oceny zewnętrznej:

o Określ zestaw reguł dla konfiguracji firewalla i routera dla sieci zewnętrznej

o Sprawdź, czy zewnętrzne urządzenia serwerowe i urządzenia sieciowe są mapowane

o Zidentyfikuj otwarte porty i powiązane usługi w sieci zewnętrznej

o Sprawdź poziomy poprawek na serwerze i zewnętrznych urządzeniach sieciowych

o Przejrzyj systemy wykrywania, takie jak IDS, zapory ogniowe i systemy ochrony warstwy aplikacji

o Uzyskaj informacje o strefach DNS

o Przeskanuj sieć zewnętrzną za pomocą różnych zastrzeżonych narzędzi dostępnych w Internecie

o Sprawdzaj aplikacje internetowe, takie jak oprogramowanie do handlu elektronicznego i koszyków zakupowych, pod kątem luk w zabezpieczeniach

* Ocena wewnętrzna

Wewnętrzna ocena obejmuje analizę sieci wewnętrznej w celu znalezienia exploitów i luk w zabezpieczeniach. Poniżej przedstawiono niektóre z możliwych etapów przeprowadzania oceny wewnętrznej:

o Określ otwarte porty i powiązane usługi na urządzeniach sieciowych, serwerach i systemach

o Sprawdź konfiguracje routera i zestawy reguł zapory

o Wymień wewnętrzne luki systemu operacyjnego i serwera

o Przeskanuj w poszukiwaniu trojanów, które mogą być obecne w środowisku wewnętrznym

o Sprawdź poziomy poprawek na wewnętrznych urządzeniach sieciowych, serwerach i systemach organizacji

o Sprawdź, czy nie ma złośliwego oprogramowania, programów szpiegujących i wirusów oraz udokumentuj je

o Oceń bezpieczeństwo fizyczne

o Zidentyfikuj i przejrzyj proces i zdarzenia zdalnego zarządzania

o Ocena mechanizmów udostępniania plików (na przykład udziały NFS i SMB/CIFS)

o Sprawdź implementację i zdarzenia antywirusowe

Ocena oparta na Floście

Oceny oparte na Flost to rodzaj kontroli bezpieczeństwa, która polega na przeprowadzeniu kontroli na poziomie konfiguracji w celu zidentyfikowania konfiguracji systemu, katalogów użytkowników, systemów plików, ustawień rejestru i innych parametrów w celu oceny możliwości naruszenia bezpieczeństwa. Oceny te sprawdzają bezpieczeństwo określonej sieci lub serwera. Skanery oparte na technologii Flost oceniają systemy w celu zidentyfikowania luk w zabezpieczeniach, takich jak natywne tabele konfiguracji, nieprawidłowe uprawnienia do rejestru lub plików oraz błędy konfiguracji oprogramowania. Oceny oparte na Flost wykorzystują wiele komercyjnych i otwartych narzędzi do skanowania.

Ocena oparta na sieci

Oceny sieci określają możliwe ataki bezpieczeństwa sieci, które mogą wystąpić w systemie organizacji. Oceny te wykrywają zasoby sieciowe i mapują porty i usługi działające w różnych obszarach sieci. Ocenia system organizacji pod kątem luk, takich jak brakujące poprawki, niepotrzebne usługi, słabe uwierzytelnianie i słabe szyfrowanie. Specjaliści od oceny sieci używają zapór ogniowych i skanerów sieciowych, takich jak Nessus. Skanery te identyfikują otwarte porty, rozpoznają usługi działające na tych portach i wykrywają związane z nimi luki w zabezpieczeniach tych usług. Oceny te pomagają organizacjom identyfikować punkty wejścia i ataku do sieci, ponieważ podążają ścieżką i podejściem hakera. Pomagają organizacjom określić, w jaki sposób systemy są podatne na ataki z Internetu i intranetu oraz w jaki sposób osoba atakująca może uzyskać dostęp do ważnych informacji. Typowa ocena sieci obejmuje następujące testy sieci:

o Sprawdza topologie sieci pod kątem niewłaściwej konfiguracji zapory

o Sprawdza reguły filtrowania routera

o Identyfikuje niewłaściwie skonfigurowane serwery bazodanowe

o Testuje poszczególne usługi i protokoły, takie jak HTTP, SNMP i FTP

o Przegląda kod źródłowy HTML pod kątem niepotrzebnych informacji

o Wykonuje sprawdzanie granic zmiennych

Ocena aplikacji

Ocena aplikacji koncentruje się na transakcyjnych aplikacjach internetowych, tradycyjnych aplikacjach typu klient-serwer i systemach hybrydowych. Analizuje wszystkie elementy infrastruktury aplikacji, w tym wdrożenie i komunikację w obrębie klienta i serwera. Ten rodzaj oceny polega na sprawdzeniu infrastruktury serwera WWW pod kątem błędnej konfiguracji, nieaktualnej zawartości lub znanych luk w zabezpieczeniach. Specjaliści ds. bezpieczeństwa używają do przeprowadzania takich ocen zarówno narzędzi komercyjnych, jak i narzędzi typu open source.

Ocena bazy danych

Ocena bazy danych to dowolna ocena skoncentrowana na testowaniu baz danych pod kątem występowania jakichkolwiek błędnych konfiguracji lub znanych luk w zabezpieczeniach. Oceny te koncentrują się głównie na testowaniu różnych technologii baz danych, takich jak MYSQL, MSSQL, ORACLE i POSTGRESQL, w celu zidentyfikowania luk w zabezpieczeniach związanych z narażeniem danych lub wstrzyknięciem. Specjaliści ds. bezpieczeństwa używają do przeprowadzania takich ocen zarówno narzędzi komercyjnych, jak i narzędzi typu open source.

Ocena sieci bezprzewodowej

Ocena sieci bezprzewodowej określa luki w sieciach bezprzewodowych organizacji. W przeszłości sieci bezprzewodowe wykorzystywały słabe i wadliwe mechanizmy szyfrowania danych. Obecnie standardy sieci bezprzewodowych ewoluowały, ale wiele sieci nadal korzysta ze słabych i przestarzałych mechanizmów bezpieczeństwa i jest narażonych na ataki. Oceny sieci bezprzewodowych próbują zaatakować mechanizmy uwierzytelniania bezprzewodowego i uzyskać nieautoryzowany dostęp. Ten rodzaj oceny testuje sieci bezprzewodowe i identyfikuje nielegalne sieci, które mogą istnieć w granicach organizacji. Oceny te kontrolują określone przez klienta lokalizacje z siecią bezprzewodową. Wąchają ruch w sieci bezprzewodowej i próbują złamać klucze szyfrujące. Audytorzy testują dostęp do innych sieci, jeśli uzyskają dostęp do sieci bezprzewodowej.

Ocena rozproszona

Ten typ oceny, stosowany przez organizacje posiadające zasoby, takie jak serwery i klienci w różnych lokalizacjach, obejmuje jednoczesną ocenę rozproszonych zasobów organizacji, takich jak aplikacje klienckie i serwerowe, przy użyciu odpowiednich technik synchronizacji. Synchronizacja odgrywa kluczową rolę w tego typu ocenie. Dzięki synchronizacji przebiegów testów wszystkie oddzielne zasoby znajdujące się w wielu lokalizacjach mogą być testowane w tym samym czasie.

Potwierdzona ocena

Ocena uwierzytelniona jest również nazywana oceną uwierzytelnioną. W tego typu ocenie haker etyczny posiada dane uwierzytelniające wszystkich maszyn znajdujących się w ocenianej sieci. Szanse na znalezienie luk w zabezpieczeniach związanych z systemami operacyjnymi i aplikacjami są większe w ocenie poświadczeń niż w ocenie bez poświadczeń. Ten rodzaj oceny stanowi wyzwanie, ponieważ nie jest jasne, kto jest właścicielem poszczególnych aktywów w dużych przedsiębiorstwach, a nawet jeśli etyczny haker zidentyfikuje rzeczywistych właścicieli aktywów, dostęp do danych uwierzytelniających tych aktywów jest bardzo trudny, ponieważ właściciele aktywów na ogół nie udostępniają takich poufnych informacji. Ponadto, nawet jeśli etyczny haker pomyślnie uzyska wszystkie wymagane dane uwierzytelniające, utrzymanie listy haseł jest ogromnym zadaniem, ponieważ mogą wystąpić problemy ze zmienionymi hasłami, błędami w pisowni i uprawnieniami administracyjnymi. Chociaż jest to najlepszy sposób oceny docelowej sieci korporacyjnej pod kątem luk w zabezpieczeniach i jest wysoce niezawodny, jest to złożona ocena, która stanowi wyzwanie.

Ocena bez poświadczeń

Ocena bez poświadczeń, zwana także oceną nieuwierzytelnioną, zapewnia szybki przegląd słabych punktów poprzez analizę usług sieciowych ujawnionych przez hosta. Ponieważ jest to ocena bez poświadczeń, etyczny haker nie wymaga żadnych poświadczeń, aby aktywa mogły przeprowadzić ich oceny. Ten rodzaj oceny generuje krótki raport dotyczący słabych punktów; nie jest jednak niezawodny, ponieważ nie zapewnia głębszego wglądu w luki w zabezpieczeniach systemu operacyjnego i aplikacji, które nie są ujawniane przez hosta w sieci. Ta ocena nie jest również w stanie

wykryć luk w zabezpieczeniach, które potencjalnie są objęte zaporami ogniowymi. Jest podatny na fałszywie pozytywne wyniki i nie jest niezawodnie skuteczny w porównaniu z oceną opartą na poświadczeniach.

Ocena ręczna

Po wykonaniu footprintingu i skanowaniu sieci oraz uzyskaniu kluczowych informacji, jeśli etyczny haker przeprowadza ręczne badania w celu zbadania luk w zabezpieczeniach, ręcznie klasyfikuje luki i ocenia je, odnosząc się do standardów oceny luk, takich jak CVSS i baz danych luk, takich jak CVE i CWE. Taka ocena jest uważana za ręczną.

Zautomatyzowana ocena

Ocena, w której etyczny haker używa narzędzi do oceny podatności, takich jak Nessus Professional, Qualys lub GFI LanGuard, do przeprowadzenia oceny podatności celu, nazywana jest oceną automatyczną. W przeciwieństwie do ocen ręcznych, w tego typu ocenie etyczny haker nie wykonuje footprintingu ani skanowania sieci. Wykorzystują zautomatyzowane narzędzia, które mogą wykonywać wszystkie takie czynności, a także są w stanie identyfikować słabe punkty i wyniki CVSS, uzyskiwać krytyczne informacje CVE/CWE związane z luką w zabezpieczeniach oraz sugerować strategie naprawcze.

Ocena oparta na chmurze

Ten rodzaj oceny koncentruje się na ocenie ogólnego bezpieczeństwa infrastruktury chmury zgodnie z najlepszymi praktykami lub wytycznymi dostawcy usług w chmurze. Ocena ta obejmuje identyfikację słabych punktów infrastruktury chmurowej i łagodzenie ich poprzez mechanizmy kontroli dostępu i odpowiednie środki bezpieczeństwa zgodne ze standardami. Ten typ oceny jest często przeprowadzany w celu zidentyfikowania zagrożeń związanych z zasobami wdrożonymi w chmurze. Pomaga również specjalistom ds. bezpieczeństwa w wykrywaniu słabych punktów wejścia w chmurze, przez które osoby atakujące mogą przedostać się do sieci organizacji.

Ocena aplikacji mobilnych

Ocena aplikacji mobilnych ma na celu ochronę prywatności danych w aplikacjach mobilnych i interfejsach API. Jest to obowiązkowa praktyka bezpieczeństwa dla każdej organizacji, która hostuje publicznie dostępne aplikacje. Ten rodzaj oceny obejmuje badanie kodu źródłowego i wewnętrznych kontroli bezpieczeństwa aplikacji mobilnych. Specjaliści ds. bezpieczeństwa muszą przeprowadzać tego typu oceny, aby ocenić i poprawić ogólną wytrzymałość aplikacji na znane i przyszłe zagrożenia w celu ochrony wrażliwych danych. Skuteczna ocena może zminimalizować ryzyko i pomóc we włączeniu odpowiednich środków bezpieczeństwa w celu zwiększenia bezpieczeństwa aplikacji mobilnych.

Narzędzia oceny podatności

Rozwiązania do oceny podatności na ataki są ważnymi narzędziami do zarządzania bezpieczeństwem informacji, ponieważ identyfikują wszystkie potencjalne słabe punkty bezpieczeństwa, zanim atakujący będzie mógł je wykorzystać. Dostępne są różne podejścia i rozwiązania do przeprowadzania oceny podatności na zagrożenia. Wybór odpowiedniego podejścia do oceny odgrywa ważną rolę w łagodzeniu zagrożeń, przed którymi stoi organizacja. W tej sekcji opisano różne podejścia, rozwiązania i narzędzia używane do przeprowadzania oceny podatności na zagrożenia.

Porównanie podejść do oceny podatności na zagrożenia

Istnieją cztery rodzaje rozwiązań do oceny podatności na zagrożenia: rozwiązania oparte na produktach, rozwiązania oparte na usługach, ocena oparta na drzewie i ocena oparta na wnioskach.

Rozwiązania oparte na produktach

Rozwiązania produktowe są instalowane w wewnętrznej sieci organizacji. Są one instalowane w przestrzeni prywatnej lub nierutowalnej lub w adresowalnej przez Internet części sieci organizacji. Jeśli są zainstalowane w sieci prywatnej (za zaporą ogniową), nie zawsze mogą wykryć ataki z zewnątrz.

Rozwiązania oparte na usługach

Rozwiązania oparte na usługach są oferowane przez strony trzecie, takie jak firmy audytorskie lub konsultingowe w zakresie bezpieczeństwa. Niektóre rozwiązania są hostowane w sieci, podczas gdy inne są hostowane poza siecią. Wadą tego rozwiązania jest to, że atakujący mogą skontrolować sieć z zewnątrz.

Ocena oparta na drzewie

W ocenie opartej na drzewie audytor wybiera różne strategie dla każdej maszyny lub komponentu systemu informatycznego. Na przykład administrator wybiera skaner dla serwerów z systemem Windows, baz danych i usług internetowych, ale używa innego skanera dla serwerów z systemem Linux. Podejście to polega na tym, że administrator zapewnia początkowy element analizy, a następnie rozpoczyna ciągłe skanowanie bez uwzględnienia jakichkolwiek informacji znalezionych w czasie skanowania.

Ocena oparta na wnioskach

W przypadku oceny opartej na wnioskach skanowanie rozpoczyna się od sporządzenia spisu protokołów znalezionych na komputerze. Po znalezieniu protokołu rozpoczyna się proces skanowania w celu wykrycia, które porty są podłączone do usług, takich jak serwer poczty e-mail, serwer WWW lub serwer bazy danych. Po znalezieniu usług wybiera luki w zabezpieczeniach na każdej maszynie i rozpoczyna wykonywanie tylko odpowiednich testów.

Charakterystyka dobrego rozwiązania do oceny podatności na zagrożenia

Organizacje muszą wybrać właściwe i odpowiednie rozwiązanie do oceny podatności na zagrożenia, aby wykrywać, oceniać i chronić swoje krytyczne zasoby IT przed różnymi zagrożeniami wewnętrznymi i zewnętrznymi. Cechy dobrego rozwiązania do oceny podatności są następujące:

• Zapewnia prawidłowe wyniki poprzez testowanie sieci, zasobów sieciowych, portów, protokołów i systemów operacyjnych

• Stosuje dobrze zorganizowane podejście do testowania oparte na wnioskowaniu

• Automatycznie skanuje i sprawdza stale aktualizowane bazy danych

• Tworzy krótkie, praktyczne, konfigurowalne raporty, w tym raporty o lukach w zabezpieczeniach według poziomu istotności oraz analizę trendów

• Obsługuje wiele sieci

• Sugeruje odpowiednie środki zaradcze i obejścia w celu usunięcia luk w zabezpieczeniach

• Naśladuje zewnętrzny widok atakujących, aby osiągnąć swój cel

Działanie rozwiązań do wykrywania luk w zabezpieczeniach

Każda organizacja musi obsługiwać i przetwarzać duże ilości danych, aby prowadzić działalność. Te duże ilości danych zawierają uprzywilejowane informacje o tej konkretnej organizacji. Atakujący próbują zidentyfikować luki w zabezpieczeniach, które mogą wykorzystać, a następnie wykorzystują je do uzyskania dostępu do krytycznych danych w celach niezgodnych z prawem. Analiza podatności analizuje i wykrywa obszary podatne na ryzyko w sieci organizacyjnej. W analizie tej wykorzystywane są różne narzędzia i raporty dotyczące luk występujących w sieci. Rozwiązania do wykrywania luk w zabezpieczeniach wykonują testy penetracji luk w sieci organizacyjnej w trzech krokach:

Lokalizowanie węzłów: Pierwszym krokiem w skanowaniu luk w zabezpieczeniach jest zlokalizowanie aktywnych hostów w sieci docelowej przy użyciu różnych technik skanowania.

Wykonywanie na nich wykrywania usług i systemów operacyjnych: po wykryciu aktywnych hostów w sieci docelowej następnym krokiem jest wyliczenie otwartych portów i usług wraz z systemem operacyjnym w systemach docelowych.

Testowanie tych usług i systemu operacyjnego pod kątem znanych luk: Wreszcie, po zidentyfikowaniu otwartych usług i systemu operacyjnego działającego na węzłach docelowych, są one testowane pod kątem znanych luk.

Rodzaje narzędzi do oceny podatności na zagrożenia

Istnieje sześć rodzajów narzędzi do oceny podatności: narzędzia do oceny podatności na hosty, narzędzia do oceny podatności w warstwie aplikacji, narzędzia do oceny głębokości, narzędzia do oceny zakresu, narzędzia aktywne i pasywne oraz narzędzia do lokalizacji i badania danych.

Narzędzia do oceny luk w zabezpieczeniach oparte na hoście

Narzędzia do skanowania oparte na hoście są odpowiednie dla serwerów, na których działają różne aplikacje, takie jak Internet, krytyczne pliki, bazy danych, katalogi i zdalny dostęp. Te skanery oparte na hoście mogą wykrywać luki w zabezpieczeniach o wysokim poziomie i dostarczać wymaganych informacji o poprawkach (poprawkach). Oparte na hoście narzędzie do oceny podatności na zagrożenia identyfikuje system operacyjny działający na określonym komputerze hosta i testuje go pod kątem znanych braków. Wyszukuje również popularne aplikacje i usługi.

Narzędzia oceny głębokości

Narzędzia oceny głębokości służą do wykrywania i identyfikowania nieznanych wcześniej luk w zabezpieczeniach systemu. Ogólnie rzecz biorąc, narzędzia takie jak fuzzery, które dostarczają dowolne dane wejściowe do interfejsu systemu, są używane do identyfikowania luk w zabezpieczeniach o niestabilnej głębokości. Wiele z tych narzędzi wykorzystuje zestaw sygnatur luk w zabezpieczeniach w celu sprawdzenia, czy produkt jest odporny na znaną lukę, czy nie.

Narzędzia oceny luk w zabezpieczeniach warstwy aplikacji

Narzędzia do oceny podatności na zagrożenia w warstwie aplikacji zostały zaprojektowane z myślą o potrzebach wszelkiego rodzaju systemów operacyjnych i aplikacji. Różne zasoby stwarzają różne zagrożenia bezpieczeństwa i są identyfikowane przez narzędzia zaprojektowane do tego celu. Obserwacja słabych punktów systemu przez Internet przy użyciu zewnętrznego routera, zapory sieciowej lub serwera WWW nazywana jest zewnętrzną oceną słabych punktów. Luki te mogą dotyczyć zewnętrznych zagrożeń typu DoS/DDoS, przechwytywania danych sieciowych lub innych problemów. Analityk przeprowadza ocenę podatności i odnotowuje wrażliwe zasoby. Informacje o lukach w zabezpieczeniach sieci są regularnie aktualizowane w narzędziach. Narzędzia do oceny podatności warstwy aplikacji są skierowane na serwery sieciowe lub bazy danych.

Narzędzia oceny zakresu

Narzędzia do oceny zakresu zapewniają ocenę bezpieczeństwa poprzez testowanie luk w aplikacjach i systemie operacyjnym. Narzędzia te zapewniają standardowe kontrole i interfejs raportowania, który pozwala użytkownikowi wybrać odpowiedni skan. Narzędzia te generują standardowy raport na podstawie znalezionych informacji. Niektóre narzędzia do oceny są przeznaczone do testowania określonej aplikacji lub typu aplikacji pod kątem luk w zabezpieczeniach.

Narzędzia aktywne i pasywne

Aktywne skanery sprawdzają luki w zabezpieczeniach funkcji sieciowych zużywających zasoby w sieci. Główną zaletą aktywnego skanera jest to, że administrator systemu lub kierownik IT ma dobrą kontrolę nad czasem i parametrami skanowania luk w zabezpieczeniach. Tego skanera nie można używać w krytycznych systemach operacyjnych, ponieważ wykorzystuje zasoby systemowe, które wpływają na przetwarzanie innych zadań.

Skanery pasywne to takie, które nie wpływają znacząco na zasoby systemowe, ponieważ jedynie obserwują dane systemowe i wykonują przetwarzanie danych na oddzielnej maszynie analitycznej. Pasywny skaner najpierw otrzymuje dane systemowe, które dostarczają pełnych informacji o uruchomionych procesach, a następnie ocenia te dane pod kątem zestawu reguł.

Narzędzia do badania lokalizacji i danych

Poniżej wymieniono niektóre narzędzia do lokalizacji i badania danych:

- Skaner sieciowy: Skanery sieciowe to takie, które współdziałają tylko z rzeczywistą maszyną, na której się znajdują, i wysyłają raport do tej samej maszyny po skanowaniu.

- Skaner oparty na agentach: Skanery oparte na agentach znajdują się na jednym komputerze, ale mogą skanować kilka komputerów w tej samej sieci.

- Skaner proxy: Skanery proxy to skanery sieciowe, które mogą skanować sieci z dowolnego komputera w sieci.

- Skaner klastrowy: Skanery klastrowe są podobne do skanerów proxy, ale mogą jednocześnie wykonywać dwa lub więcej skanów na różnych komputerach w sieci.

Wybór narzędzia do oceny podatności na zagrożenia

Zaprojektowane przez dostawców narzędzia do oceny podatności na zagrożenia mogą być używane do testowania hosta lub aplikacji pod kątem luk w zabezpieczeniach. Istnieje kilka dostępnych narzędzi do oceny podatności, które obejmują skanery portów, skanery podatności na ataki i skanery do oceny podatności systemu operacyjnego. Organizacje muszą wybrać odpowiednie narzędzia na podstawie swoich wymagań testowych. Wybierz narzędzia, które najlepiej spełniają następujące wymagania:

• Narzędzia muszą umożliwiać testowanie od kilkudziesięciu do 30 000 różnych luk w zabezpieczeniach, w zależności od produktu

• Wybrane narzędzie powinno mieć solidną bazę danych luk w zabezpieczeniach i często aktualizowane sygnatury ataków

• Wybierz narzędzie, które pasuje do środowiska i wiedzy

• Regularnie aktualizuj silnik skanowania, aby mieć pewność, że narzędzie jest świadome najnowszych znanych luk w zabezpieczeniach

• Zweryfikuj, czy wybrane narzędzie do oceny podatności ma dokładne mapowanie sieci, mapowanie aplikacji i testy penetracyjne. Nie wszystkie narzędzia mogą znaleźć uruchomione protokoły i przeanalizować wydajność sieci.

• Upewnij się, że narzędzie ma kilka regularnie aktualizowanych skryptów luk w zabezpieczeniach dla skanowanych platform

• Upewnij się, że zostały zastosowane wszelkie poprawki; nieprzestrzeganie tego może prowadzić do fałszywych alarmów

• Dowiedz się, ile raportów jest zwracanych, jakie zawierają informacje i czy można je wyeksportować

• Sprawdź, czy narzędzie ma różne poziomy penetracji, aby zapobiec blokowaniu

• Koszty konserwacji narzędzi można zrekompensować poprzez ich efektywne wykorzystanie

• Upewnij się, że narzędzie do oceny luk w zabezpieczeniach może szybko i dokładnie przeprowadzać skanowanie

• Upewnij się, że narzędzie może wykonywać skanowanie przy użyciu wielu protokołów

• Sprawdź, czy narzędzie może zrozumieć i przeanalizować topologię sieci, aby przeprowadzić ocenę

• Ograniczenia przepustowości są głównym problemem w przypadku dużych sieci. Zapewnić

narzędzie do oceny podatności ma dużą alokację przepustowości

• Upewnij się, że narzędzie do oceny podatności posiada doskonałe funkcje ograniczania zapytań

• Upewnij się, że narzędzie może również oceniać wrażliwe systemy i nietradycyjne zasoby

Kryteria wyboru narzędzia do oceny podatności na zagrożenia

Kryteria, którymi należy się kierować przy wyborze lub zakupie dowolnego narzędzia do oceny podatności na zagrożenia, są następujące:

Rodzaje ocenianych podatności: Najważniejszą informacją w momencie oceny dowolnego narzędzia jest ustalenie, ile rodzajów podatności wykryje.

Testowanie możliwości skanowania: Narzędzie do oceny podatności musi mieć możliwość wykonania całego wybranego testu i musi przeskanować wszystkie systemy wybrane do skanowania.

Umiejętność dostarczania dokładnych raportów: Umiejętność przygotowania dokładnego raportu jest niezbędna. Raporty o lukach w zabezpieczeniach powinny być krótkie, jasne i powinny zapewniać łatwą metodę ograniczania wykrytej luki w zabezpieczeniach.

Wydajne i dokładne skanowanie: Dwoma istotnymi aspektami wydajności skanera są czas pracy pojedynczego hosta i wymagane zasoby oraz utrata usług w czasie skanowania. Ważne jest zapewnienie dokładności i świadomość dokładności wyników.

Zdolność do inteligentnego wyszukiwania: to, jak sprytni są w momencie skanowania, jest również kluczowym czynnikiem przy ocenie dowolnego narzędzia do oceny podatności na zagrożenia.

Funkcjonalność pozwalająca na pisanie własnych testów: gdy nie ma sygnatury dla niedawno znalezionej luki, pomocne jest, jeśli narzędzie do skanowania podatności pozwala na użycie testów opracowanych przez użytkownika.

Planowanie uruchamiania testowego: Ważna jest możliwość planowania uruchamiania testowego, ponieważ umożliwia to użytkownikom przeprowadzanie skanowania, gdy ruch w sieci jest niewielki.

Najlepsze praktyki dotyczące wyboru narzędzi do oceny podatności na zagrożenia

Niektóre z najlepszych praktyk, które można zastosować przy wyborze narzędzi do oceny podatności na zagrożenia, to:

• Narzędzia do oceny podatności służą do zabezpieczania i ochrony systemu lub sieci organizacji. Upewnij się, że nie uszkodzą one sieci ani systemu podczas pracy.

• Przed użyciem jakichkolwiek narzędzi do oceny podatności na zagrożenia ważne jest, aby zrozumieć ich funkcję i zdecydować, jakie informacje są potrzebne przed rozpoczęciem

• Mechanizmy bezpieczeństwa dla dostępu z wewnątrz iz zewnątrz sieci są nieco inne, więc zdecyduj o lokalizacji skanowania na podstawie żądanych informacji

• W czasie skanowania włącz rejestrowanie i upewnij się, że wszystkie wyniki i metodologie są opatrzone adnotacjami za każdym razem, gdy skanowanie jest przeprowadzane na dowolnym komputerze

• Użytkownicy powinni często skanować swoje systemy w poszukiwaniu luk i regularnie monitorować je pod kątem luk i exploitów

Narzędzia oceny podatności

Osoba atakująca przeprowadza skanowanie pod kątem luk w zabezpieczeniach, aby zidentyfikować luki w zabezpieczeniach w sieci docelowej, które może wykorzystać do przeprowadzenia ataków. Analitycy bezpieczeństwa mogą korzystać z narzędzi do oceny podatności na zagrożenia, aby identyfikować słabe punkty w zabezpieczeniach organizacji i korygować zidentyfikowane luki, zanim atakujący je wykorzysta. Skanery podatności sieci pomagają analizować i identyfikować luki w sieci docelowej lub zasobach sieciowych za pomocą oceny podatności i audytu sieci. Narzędzia te pomagają również w przezwyciężaniu słabych punktów w sieci, sugerując różne techniki naprawcze. Oto niektóre z najskuteczniejszych narzędzi oceny podatności:

Qualys Zarządzanie lukami w zabezpieczeniach

Qualys VM to usługa oparta na chmurze, która zapewnia natychmiastowy, globalny wgląd w miejsca, w których systemy IT mogą być narażone na najnowsze zagrożenia internetowe oraz sposoby ich ochrony. Pomaga w ciągłym identyfikowaniu zagrożeń i monitorowaniu nieoczekiwanych zmian w sieci, zanim przekształcą się one w naruszenia.

Cechy:

- Wykrywanie oparte na agentach

Współpracuje również z Qualys Cloud Agents, rozszerzając zasięg sieci na zasoby, których nie można przeskanować.

- Stałe monitorowanie i alerty

Gdy maszyna wirtualna jest połączona z ciągłym monitorowaniem (CM), zespoły InfoSec są proaktywnie ostrzegane o potencjalnych zagrożeniach, dzięki czemu można rozwiązywać problemy, zanim przerodzą się w naruszenia.

- Kompleksowy zasięg i widoczność

Nieustannie skanuje i identyfikuje luki w zabezpieczeniach w celu ochrony zasobów IT w siedzibie firmy, w chmurze i na mobilnych punktach końcowych. Jego pulpit nawigacyjny wyświetla przegląd stanu bezpieczeństwa i zapewnia dostęp do szczegółowych informacji o środkach zaradczych. VM generuje niestandardowe, oparte na rolach raporty dla wielu interesariuszy, w tym automatyczną dokumentację bezpieczeństwa dla audytorów zgodności.

- VM dla świata bez granic

Gdy przedsiębiorstwa wdrażają przetwarzanie w chmurze, mobilność i inne przełomowe technologie do transformacji cyfrowej, Qualys VM oferuje zarządzanie lukami nowej generacji dla tych hybrydowych środowisk IT, których tradycyjne granice zostały zatarte.

- Odkryj zapomniane urządzenia i uporządkuj zasoby hosta

Qualys może pomóc szybko określić, co działa w różnych częściach sieci — od sieci obwodowej i korporacyjnej po zwirtualizowane maszyny i usługi w chmurze. Może również identyfikować nieoczekiwane punkty dostępu, serwery WWW i inne urządzenia, które mogą narazić sieć na atak.

- Skanuj w poszukiwaniu luk wszędzie, dokładnie i wydajnie

Skanuj systemy w dowolnym miejscu z tej samej konsoli, w tym na obrzeżach, w sieci wewnętrznej i w środowiskach chmurowych.

- Zidentyfikuj i uszereguj ryzyka

Qualys, korzystając z analizy trendów, prognoz wpływu dnia zerowego i poprawki, może zidentyfikować największe zagrożenia biznesowe.

- Napraw luki w zabezpieczeniach

Zdolność Qualys do śledzenia danych o lukach w zabezpieczeniach w różnych hostach i czasie tworzy interaktywne raporty, które zapewniają lepsze zrozumienie bezpieczeństwa sieci.

Nessus Professional

Nessus Professional to rozwiązanie do oceny służące do identyfikowania luk w zabezpieczeniach, problemów z konfiguracją i złośliwego oprogramowania, które atakujący wykorzystują do penetracji sieci. Wykonuje ocenę podatności, konfiguracji i zgodności. Obsługuje różne technologie, takie jak systemy operacyjne, urządzenia sieciowe, hiperwizory, bazy danych, tablety i telefony, serwery WWW i infrastrukturę krytyczną. Nessus to platforma do skanowania podatności dla audytorów i analityków bezpieczeństwa. Użytkownicy mogą planować skanowanie w wielu skanerach i używać kreatorów do łatwego i szybkiego tworzenia zasad, planowania skanowania i wysyłania wyników pocztą elektroniczną.

Cechy:

o Szybkie wykrywanie zasobów

o Ocena podatności

o Wykrywanie złośliwego oprogramowania i botnetów

o Audyt konfiguracji i zgodności

o Skanowanie i audyt platform zwirtualizowanych i chmurowych

GFI LanGuard

GFI LanGuard skanuje, wykrywa, ocenia i usuwa luki w zabezpieczeniach sieci i podłączonych do niej urządzeń. Odbywa się to przy minimalnym wysiłku administracyjnym. Skanuje systemy operacyjne, środowiska wirtualne i zainstalowane aplikacje za pomocą baz danych sprawdzających luki w zabezpieczeniach. Umożliwia analizę stanu bezpieczeństwa sieci, identyfikuje zagrożenia i proponuje rozwiązania, zanim dojdzie do włamania do systemu.

Cechy:

o Zarządzanie poprawkami dla systemów operacyjnych i aplikacji firm trzecich

o Ocena podatności

o Internetowa konsola raportowania

o Śledź najnowsze luki w zabezpieczeniach i brakujące aktualizacje

o Integracja z aplikacjami zabezpieczającymi

o Sprawdzanie podatności urządzeń sieciowych

o Audyt sieci i oprogramowania

o Wsparcie dla środowisk wirtualnych

OpenVAS

OpenVAS to platforma kilku usług i narzędzi, które oferują kompleksowe i wydajne rozwiązanie do skanowania i zarządzania lukami w zabezpieczeniach. Platforma jest częścią komercyjnego rozwiązania do zarządzania lukami w zabezpieczeniach firmy Greenbone Network, którego rozwój jest wnoszony do społeczności open source od 2009 roku. Rzeczywistemu skanerowi bezpieczeństwa towarzyszy regularnie aktualizowany kanał testów podatności sieci (NVT), w sumie ponad 50 000 .

Nikto

Nikto to skaner serwerów sieciowych Open Source (GPL), który przeprowadza kompleksowe testy serwerów sieciowych pod kątem wielu elementów, w tym ponad 6700 potencjalnie niebezpiecznych plików lub programów, sprawdza przestarzałe wersje ponad 1250 serwerów i sprawdza problemy związane z wersjami na ponad 270 serwerach . Sprawdza również elementy konfiguracji serwera, takie jak obecność wielu plików indeksu i opcje serwera HTTP, i próbuje zidentyfikować zainstalowane serwery WWW i oprogramowanie.

Cechy:

o Obsługa SSL (Unix z OpenSSL lub może Windows z Perl/NetSSL ActiveState)

o Pełna obsługa proxy HTTP

o Sprawdza przestarzałe komponenty serwera

o Zapisuje raporty w postaci zwykłego tekstu, XML, HTML, NBE lub CSV

o Silnik szablonów do łatwego dostosowywania raportów

o Skanuje wiele portów na serwerze lub wiele serwerów za pośrednictwem pliku wejściowego

o Techniki kodowania IDS firmy LibWhisker

o Identyfikuje zainstalowane oprogramowanie za pomocą nagłówków, ikon ulubionych i plików

o Uwierzytelnianie hosta za pomocą Basic i NTLM

o Zgadywanie subdomeny

o Apache i cgiwrap wyliczanie nazw użytkowników

o Dostrajanie skanowania w celu uwzględnienia lub wykluczenia całych klas sprawdzania luk w zabezpieczeniach

o Zgaduje poświadczenia dla obszarów autoryzacji (w tym wiele domyślnych kombinacji identyfikatora i hasła)

Poniżej wymieniono niektóre z dodatkowych narzędzi do oceny podatności na zagrożenia:

• Qualys FreeScan (https://www.quolys.com)

• Acunetix Web Vulnerability Scanner (https://www.ocunetix.com)

• Nexpose (https://www.ropid7.com)

• Network Security Scanner (https://www.beyondtrust.com)

• SAINT (https://www.corson-soint.com)

• beSECURE (AVDS) (https://www.beyondsecurity.com)

• Core Impact Pro (https://www.coresecurity.com)

• N-Stalker Web Application Security Scanner (https://www.nstalker.com)

• ManageEngine Vulnerability Manager Plus (https://www.manageengine.com)

• Nipper Studio (https://www.titania.com)

Narzędzia do oceny luk w zabezpieczeniach dla urządzeń mobilnych

Skaner luk w zabezpieczeniach

Skaner luk w zabezpieczeniach to aplikacja na Androida, która wykonuje pasywne wykrywanie luk w zabezpieczeniach na podstawie odcisku palca wersji oprogramowania. Ponieważ jest to pasywna metoda oceny podatności, tej aplikacji można używać wyłącznie do identyfikacji luk; nie jest skuteczny w przeprowadzaniu kontroli zgodności.

SecurityMetrics Mobile

SecurityMetrics Mobile to mobilne narzędzie obronne, które pomaga identyfikować słabe punkty urządzeń mobilnych w celu ochrony poufnych danych klientów. Pomaga unikać zagrożeń związanych z mobilnym złośliwym oprogramowaniem, kradzieżą urządzenia, łącznością Wi-Fi, wprowadzaniem danych, użytkowaniem osobistym i biznesowym, nieuprawnionymi uprawnieniami do aplikacji, przechowywaniem danych i urządzeń, dostępem do danych konta, Bluetooth, podczerwienią (IR), technologią Near- komunikacja terenowa (NFC) oraz karty SIM i SD. SecurityMetrics MobileScan jest zgodny z wytycznymi PCI SSC (Payment Card Industry Security Standards Council), aby zapobiegać kradzieży danych mobilnych. Po zakończeniu skanowania wygenerowany raport zawiera łączną ocenę

ryzyka, podsumowanie wykrytych luk w zabezpieczeniach oraz zalecenia dotyczące usuwania zagrożeń.

Raporty z oceny podatności na zagrożenia

W procesie oceny podatności, po zakończeniu wszystkich faz, zespół ds. bezpieczeństwa dokona przeglądu wyników i przetworzy informacje w celu przygotowania raportu końcowego. W tej fazie zespół ds. bezpieczeństwa spróbuje ujawnić wszelkie zidentyfikowane luki w zabezpieczeniach, udokumentować wszelkie zmiany i ustalenia oraz uwzględnić to wszystko w raporcie końcowym wraz z krokami zaradczymi w celu złagodzenia zidentyfikowanych zagrożeń. Raport oceny podatności ujawnia zagrożenia wykrywane podczas skanowania sieci. Do oceny podatności wykorzystywane są narzędzia takie jak Nessus Professional, GFI LanGuard i Qualys Vulnerability Management. Narzędzia te zapewniają kompleksowy raport z oceny w określonym formacie. Raport ostrzega organizację przed możliwymi atakami i sugeruje środki zaradcze. Raport zawiera szczegółowe informacje na temat wszystkich możliwych luk w zabezpieczeniach polityki bezpieczeństwa firmy. Luki są podzielone na trzy poziomy w zależności od wagi: Wysokie, Średnie i Niskie ryzyko. Luki wysokiego ryzyka to te, które mogą umożliwić nieautoryzowany dostęp do sieci. Luki te muszą zostać usunięte bezpośrednio przed narażeniem sieci. Raport opisuje różne rodzaje ataków, które są możliwe, biorąc pod uwagę zestaw systemów operacyjnych, komponentów sieciowych i protokołów organizacji. Raport z oceny narażenia musi zawierać między innymi następujące punkty:

• Nazwa luki i jej zmapowany identyfikator CVE

• Data odkrycia

• Wynik oparty na bazach danych Common Vulnerabilities and Exposures (CVE).

• Szczegółowy opis luki

• Wpływ luki w zabezpieczeniach

• Szczegóły dotyczące systemów, których dotyczy problem

• Szczegóły dotyczące procesu potrzebnego do usunięcia luki, w tym poprawki informacyjne, poprawki konfiguracji i porty, które mają zostać zablokowane.

• Weryfikacja koncepcji (PoC) podatności systemu (jeśli to możliwe)

Składniki raportu oceny podatności na zagrożenia

Raport oceny podatności zawiera szczegółowe informacje dotyczące luk wykrytych w środowisku komputerowym. Raport pomaga organizacjom określić poziom bezpieczeństwa systemów komputerowych (takich jak serwery WWW, zapory ogniowe, routery, poczta e-mail i usługi plików) oraz zapewnić rozwiązania zmniejszające liczbę awarii systemu. Etyczny haker musi zachować ostrożność podczas analizowania raportów z oceny podatności na zagrożenia, aby uniknąć fałszywych alarmów. Raport z oceny pomaga organizacjom podejmować kroki ograniczające ryzyko w celu proaktywnego unikania ryzyka poprzez identyfikowanie, śledzenie i eliminowanie luk w zabezpieczeniach. Raporty oceny podatności dzielą się na dwa typy:

• Raporty o lukach w zabezpieczeniach

• Podsumowania luk w zabezpieczeniach

Raport o lukach w zabezpieczeniach

Jest to połączony raport wszystkich przeskanowanych urządzeń i serwerów w sieci organizacji. Raport o lukach w zabezpieczeniach zawiera następujące szczegóły:

• Nowo wykryte luki w zabezpieczeniach

• Otwarte porty i wykryte usługi

• Sugestie dotyczące środków zaradczych

• Linki do poprawek

Podsumowanie luk w zabezpieczeniach

Ten raport jest tworzony dla każdego urządzenia lub serwera po skanowaniu. Zawiera podsumowanie wyniku skanowania, które obejmuje następujące elementy:

• Bieżące luki w zabezpieczeniach

• Kategorie podatności

• Nowo wykryte luki w zabezpieczeniach

• Dotkliwość luk w zabezpieczeniach

• Usunięte luki w zabezpieczeniach

Raport z oceny podatności obejmuje następujące elementy:

Podsumowanie wykonawcze

o Zakres i cele oceny

• Cel skanowania pod kątem luk w zabezpieczeniach

• Zakres skanowania

o Testowanie narracji

• Systemy operacyjne, w których przeprowadzane jest skanowanie

• Adresy IP, na których wykonywane jest skanowanie

• Rodzaje wykonanych skanów

• Data i godzina (w tym początek, koniec i czas trwania skanowania)

o Podsumowanie wyników

• Zidentyfikowane krytyczne luki w zabezpieczeniach (wyróżnienia na podstawie poziomu ryzyka)

- Liczba luk w oparciu o wagę (graficzna reprezentacja)

• Zidentyfikowane systemy operacyjne

• Wydajność systemów i aplikacji podczas skanowania

• Ogólny poziom ryzyka

Krytyczne problemy, które należy rozwiązać

o Podsumowanie działań naprawczych

Przegląd oceny

o Metodologia oceny

o Informacje o skanowaniu: informacje takie jak typ przeprowadzonego skanowania, użyte narzędzia, wersje i przeskanowane zasoby.

o Informacje o celu: Informacje o nazwie i adresie systemu docelowego.

Wyniki

o Zeskanowane hosty, w tym szczegółowe informacje o każdym hoście

• <Węzeł>: Nazwa i adres hosta

• <OS>: Typ systemu operacyjnego

• <Data>: Data testu

• Usługi wrażliwe: Usługi sieciowe według ich nazw i portów,

o Rodzaje zidentyfikowanych luk w zabezpieczeniach

o Szczegółowe informacje na temat zidentyfikowanych podatności (w tym identyfikator CVE, wynik CVSS,

opis zagrożenia, wywołany wpływ, środki zaradcze i możliwości wykorzystania)

o Uwagi opisujące dodatkowe szczegóły wyników skanowania

Ocena ryzyka

o Klasyfikacja podatności w oparciu o poziom ryzyka: krytyczny, wysoki, średni lub niski

o Potencjalne luki w zabezpieczeniach, które mogą zagrozić systemowi lub aplikacji

o Krytyczne hosty z poważnymi lukami

Zalecenia

o Priorytetyzacja środków zaradczych w oparciu o ranking ryzyka

o Plan działania w celu wdrożenia zaleceń/środków zaradczych dla każdej zidentyfikowanej luki w zabezpieczeniach

o Analiza przyczyn źródłowych

o Stosowanie łat/poprawek

o Wyciągnięte wnioski

o Trening świadomości

o Wdrożenie okresowej oceny podatności

o Wdrożenie polityk, procedur i kontroli

Podsumowanie modułu

W tym module omówiono badania podatności, ocenę podatności oraz cykl życia zarządzania podatnościami. Omówiono również system oceniania podatności CVSS i bazy danych oraz różne rodzaje podatności i techniki oceny podatności. Opisano różne rozwiązania do oceny podatności wraz z ich charakterystyką oraz opisano różne narzędzia do oceny podatności, które są używane do testowania hosta lub aplikacji pod kątem luk, wraz z kryteriami i najlepszymi praktykami wyboru narzędzia. Moduł ten zakończył się szczegółowym omówieniem, jak analizować raport z oceny podatności i w jaki sposób ujawnia on zagrożenia wykryte po przeskanowaniu sieci. Następny moduł pokaże, w jaki sposób osoby atakujące, a także etyczni hakerzy i pen testerzy próbują zhakować system na podstawie informacji zebranych o celu w fazach śledzenia, skanowania, wyliczania i analizy podatności.