Podstawy

Obecnie bezpieczeństwo jest najważniejszym tematem każdej organizacji, niezależnie od ich wielkości czy rodzaju działalności, którą wykonują. Główną przyczyną tego jest to, że organizacje nie chcą stracić reputacji lub biznesu ponad kompromisami wpływającymi na bezpieczeństwo; po drugie, muszą spełniać wymogi prawne i regulacyjne. Jeśli chodzi o techniczne bezpieczeństwo infrastruktury, najbardziej istotną rolę odgrywa ocena podatności i test penetracyjny (PT lub PenTest). Tu pokażemy czym jest PT lub PenTest, dlaczego jest wymagany oraz jak skonfigurować i zarządzać Nessusem dla twojej organizacji. Poniżej przedstawiamy Nessus, narzędzie do oceny słabych punktów i testowania penetracji. Omówimy również następujące tematy:

• Ocena podatności

• Testy penetracyjne

• Wprowadzenie do Nessusa

• Instalowanie Nessusa na różnych platformach

• Aktualizacja wtyczek Nessus

• Zarządzanie użytkownikiem Nessus

• Konfiguracja systemu Nessus

Ocena podatności i testowanie penetracji

Ocena narażenia na ataki (VA) i testy penetracyjne (PT lub PenTest) to najczęściej stosowane typy technicznych ocen ryzyka bezpieczeństwa lub audytów technicznych przeprowadzanych przy użyciu różnych narzędzi. Narzędzia te zapewniają najlepsze wyniki, jeśli są stosowane optymalnie. Nieprawidłowa konfiguracja może prowadzić do wielu fałszywych alarmów, które mogą odzwierciedlać rzeczywiste luki lub nie. Narzędzia oceny podatności są szeroko stosowane przez wszystkich, od małych organizacji do dużych przedsiębiorstw, w celu oceny ich stanu bezpieczeństwa. Pomaga im to w podejmowaniu szybkich decyzji, aby uchronić się przed tymi lukami w zabezpieczeniach. My przedstawimy kroki związane z przeprowadzaniem oceny luk w zabezpieczeniach i PenTesty za pomocą Nessus. Nessus jest powszechnie uznanym narzędziem do takich celów. W tej sekcji przedstawiono podstawową terminologię w odniesieniu do tych dwóch rodzajów ocen. Luki w zabezpieczeniach systemów IT można zdefiniować jako potencjalne słabości w systemie / infrastrukturze, które, jeśli zostaną wykorzystane, mogą doprowadzić do realizacji ataku na system. Przykładem luki jest słabe hasło słownikowo-słowne w systemie, które może zostać wykorzystane przez atak brute force (atak słownikowy) próbujący odgadnąć hasło. Może to spowodować złamanie hasła i uzyskanie dostępu do nieautoryzowanej osoby system. System słów odnosi się do wszelkich aktywów istniejących w technologii informacyjnej lub środowisku technologii nieinformacyjnych. Ocena narażenia to etapowe podejście do identyfikowania luk w infrastrukturze. Można to zrobić za pomocą zautomatyzowanych narzędzi do skanowania, takich jak Nessus, który wykorzystuje swój zestaw wtyczek odpowiadający różnym typom znanych luk w zabezpieczeniach w infrastrukturze lub ręczne podejście oparte na liście kontrolnej, które wykorzystuje najlepsze praktyki i opublikowane luki w znanych witrynach do śledzenia luk. Podejście manualne nie jest tak kompleksowe jak podejście oparte na narzędziach i będzie bardziej czasochłonne. Rodzaj kontroli przeprowadzanych przez narzędzie oceny podatności na zagrożenia można również wykonać ręcznie, ale zajmie to znacznie więcej czasu niż zautomatyzowane narzędzie. Testy penetracyjne mają dodatkowy krok do oceny podatności, wykorzystując luki w zabezpieczeniach. Testowanie penetracyjne jest natarczywym testem, w którym personel wykonujący

test penetracyjny najpierw przeprowadzi ocenę podatności w celu zidentyfikowania luk, a następnie podejmie próbę przeniknięcia do systemu przez wykorzystanie zidentyfikowanych słabych punktów.

Potrzeba oceny podatności

Bardzo ważne jest, aby zrozumieć, dlaczego wymagana jest ocena narażenia na atak lub test penetracyjny. Chociaż tam są liczne bezpośrednie lub pośrednie korzyści dla oceny podatności lub PenTestu, kilka z nich zostało tu podane dla twojego zrozumienia.

Prewencja ryzyka

Ocena podatności odkrywa luki / słabości / luki w systemie. Przeprowadzając te skany okresowo, organizacja może zidentyfikować znane luki w infrastrukturze IT w czasie. Ocena podatności zmniejsza prawdopodobieństwo niezgodności z różnymi wymaganiami dotyczącymi zgodności i przepisami, ponieważ już znasz swoje luki w zabezpieczeniach. Świadomość takich luk w czasie może pomóc organizacji w ich naprawieniu i złagodzeniu ryzyka z góry, zanim zostaną wykorzystane. Ryzyko związane z wykorzystaniem luki obejmują:

• Straty finansowe spowodowane wykorzystaniem luk w zabezpieczeniach

• Reputacja organizacji

• Kradzież danych

• Kompromis dotyczący poufności

• Kompromis w zakresie uczciwości

• Kompromis w zakresie dostępności

Wymagania dotyczące zgodności

Znane standardy bezpieczeństwa informacji (na przykład ISO 27001, PCI DSS i PA DSS) mają wymagania kontrolne, które wymagają przeprowadzenia oceny narażenia na atak. Niektóre kraje mają określone wymogi prawne dotyczące przeprowadzania ocen podatności w niektórych określonych sektorach przemysłu, takich jak bankowość i telekomunikacja.

Cykle życia oceny podatności i testowania penetracji

W tej sekcji opisano kluczowe fazy cyklu życia VA i PenTest. Te cykle życiowe są prawie identyczne; Testy penetracyjne obejmują dodatkowy etap wykorzystania zidentyfikowanych słabych punktów. Zaleca się przeprowadzanie testów w oparciu o wymagania i biznes cele testowania w organizacji, czy to ocena podatności czy test penetracyjn. W tym cyklu życia zaangażowane są następujące etapy:

1. Ustalanie zakresu

2. Gromadzenie informacji

3. Skanowanie narażenia na atak

4. Fałszywa pozytywna analiza

5. Wykrywanie luk (test penetracyjny)

6. Generowanie raportów

Etap 1 - ustalanie zakresu

Ustalanie zakresu jest podstawowym krokiem każdej czynności oceny bezpieczeństwa. Aby wykonać test VA lub PenTest, pierwszym krokiem jest określenie zakresu oceny pod względem infrastruktury, względem której ma zostać przeprowadzona ocena, na przykład serwerów, urządzeń sieciowych, urządzeń bezpieczeństwa, baz danych i aplikacji. Ustalanie zakresu zależy od celu biznesowego oceny podatności. Podczas określania zakresu należy również uzgodnić okno skanowania. Należy również uzgodnić rodzaje ataków, które są dozwolone. Po podjęciu decyzji o zakresie oceny, faza ta obejmuje również planowanie i przygotowanie do testu, w tym decyzję o zespole, terminie i czasie testu. Innym ważnym czynnikiem, który należy uwzględnić przed rozpoczęciem zlecenia, jest podpisanie formalnej umowy o zaangażowaniu pomiędzy testerem bezpieczeństwa a stroną, na której infrastrukturze testy te będą wykonywane. Określenie zakresu powinno również obejmować określenie liczby elementów infrastruktury, które mają być testowane. Oprócz zakresu infrastruktury i innych metod zarządzania programem, należy określić dokładny zakres, podejście organizacji do celu biznesowego oraz metodologię oceny. Aby podjąć decyzję w sprawie celu biznesowego, organizacja powinna określić rodzaj ataku, który chciałby naśladować. Przykładem celu, do którego firma może dążyć, jest: "Aby dowiedzieć się, co może osiągnąć zewnętrzny atakujący, celując w zewnętrznie eksponowaną infrastrukturę, mając jedynie wiedzę o publicznie wyeksponowanym adresie IP". Ten rodzaj wymagań zostanie spełniony dzięki zewnętrznym testom penetracyjnym Blackbox na infrastrukturę i aplikacje, a podejście i metodologia powinny być zgodne z tym. W oparciu o dostępność infrastruktury od Internetu lub intranetu, testowanie można wykonać z sieci zewnętrznej lub wewnętrznej. Ponadto, w zależności od rodzaju szczegółów, testowanie infrastruktury może być Blackbox lub Greybox. W zależności od typu infrastruktury, wtyczki lub funkcje narzędzia do skanowania narażenia na atak powinny być włączone, wspomagane odpowiednimi kontrolami ręcznymi.

W testach Blackbox, tylko szczegóły, takie jak adres IP, są udostępniane testerowi. Szczegóły zapewniające wgląd w infrastrukturę, taką jak typ i wersja systemu operacyjnego, nie są udostępniane w odniesieniu do skanera Nessus; ten rodzaj testowania obejmuje skanowanie niezweryfikowane. Umożliwia to testerowi naśladowanie zewnętrznego atakującego o ograniczonej wiedzy na temat infrastruktury. Testy Greybox będą zawierały pewne szczegóły dotyczące infrastruktury, która ma być współużytkowana, na przykład typ urządzenia i wersję oprogramowania, które umożliwiają uzyskanie bardziej kompleksowych danych uwierzytelniających administratora i dostarczanych do narzędzia w celu uzyskania pełniejszych wyników. Ponadto, aby naśladować atakującego wewnętrznego z wiedzą o infrastrukturze w odniesieniu do Nessus Scanner, tego typu testowanie będzie wymagać uwierzytelnionego skanowania, dając bardziej kompleksowe wyniki.

Etap 2 - zbieranie informacji

Gromadzenie informacji jest drugim i najważniejszym etapem oceny VA-PT. Ten etap obejmuje poznanie informacji o docelowym systemie przy użyciu zarówno technicznych (WhoIS), jak i nietechnicznych metod pasywnych, takich jak wyszukiwanie czy grupy internetowe). Ten krok ma kluczowe znaczenie, ponieważ pomaga uzyskać lepszy obraz docelowej infrastruktury i jej zasobów. Ponieważ ramy czasowe oceny są na ogół ograniczone czasowo, informacje zebrane podczas tej fazy pomagają w usprawnieniu wysiłków związanych z testowaniem we właściwym kierunku, wykorzystując odpowiednie narzędzia i podejście stosowane w systemach docelowych. Ten krok staje się ważniejszy dla oceny Blackboksa, gdzie udostępniane są bardzo ograniczone informacje o systemie docelowym. Po zbieraniu informacji następuje bardziej techniczne podejście do mapowania sieci docelowej za pomocą narzędzi takich jak pingi i Telnet oraz używanie skanerów portów, takich jak NMAP. Korzystanie z takich narzędzi umożliwiłoby osobom oceniającym znalezienie hosta na żywo, usług otwartych, systemów operacyjnych i innych informacji. Informacje zebrane za pomocą mapowania

sieci dodatkowo sprawdzą informacje zebrane za pomocą innych pasywnych środków dotyczących docelowej infrastruktury, co jest ważne, aby skonfigurować narzędzie do skanowania narażenia na atak. Zapewnia to skanowanie zrobione bardziej odpowiednio.

Etap 3 - skanowanie luk w zabezpieczeniach

Ten etap obejmuje faktyczne skanowanie docelowej infrastruktury w celu zidentyfikowania istniejących usterek systemu. Odbywa się to za pomocą skanerów podatności, takich jak Nessus. Przed skanowaniem narzędzie powinno być skonfigurowane optymalnie, zgodnie z docelową informacją o infrastrukturze przechwyconą podczas początkowych faz. Należy również zadbać o to, aby narzędzie mogło dotrzeć do docelowej infrastruktury, umożliwiając dostęp poprzez odpowiednie systemy pośrednie, takie jak zapory ogniowe. Takie skanery wykonują skanowanie na protokole TCP, UDP i ICMP, aby znaleźć otwarte porty i usługi uruchomione na maszynie docelowej i dopasować je do dobrze znanych opublikowanych luk, regularnie aktualizowanych w bazie sygnatur narzędzi, jeśli istnieją one w docelowej infrastrukturze. Wyniki tej fazy dają ogólny obraz tego, jakie rodzaje luk występują w docelowej infrastrukturze, które w przypadku ich wykorzystania mogą prowadzić do kompromisu systemowego.

Etap 4 - analiza fałszywie dodatnia

Jako wynik fazy skanowania można uzyskać listę słabych punktów docelowej infrastruktury. Jedną z kluczowych czynności, które należy wykonać z danymi wyjściowymi, byłaby analiza fałszywie pozytywna, czyli usunięcie wszelkich luk w zabezpieczeniach, które są fałszywie zgłaszane przez narzędzie i nie istnieją w rzeczywistości. Wszystkie narzędzia do skanowania są podatne na zgłaszanie fałszywych trafień, a tę analizę można przeprowadzić za pomocą metod, takich jak skorelowanie słabych punktów ze sobą i wcześniej zebranych raportów dotyczących informacji i skanowania, a także sprawdzenie, czy dostęp do systemu jest dostępny. Skanery podatności nadają własną ocenę ryzyka zidentyfikowanym słabym punktom; można je ponownie przeanalizować, biorąc pod uwagę faktyczną krytyczność elementu infrastruktury (serwera lub urządzenia sieciowego) w sieci i wpływ luki.

Etap 5 - wykorzystanie luki w zabezpieczeniach (test penetracyjny)

W przypadku, gdy właściciele systemów wymagają potwierdzenia istniejących luk lub exploitów, aby zrozumieć, w jakim stopniu atakujący może zaatakować system podatny na zagrożenia, testerzy będą musieli wykazać exploity w kontrolowanym środowisku bez faktycznego udostępnienia infrastruktury, chyba że jest to wymagane. Testy penetracyjne to kolejny krok do oceny podatności, mający na celu przeniknięcie do systemu docelowego w oparciu o exploity dostępne dla zidentyfikowanych luk. Do wykorzystania możemy wykorzystać naszą własną wiedzę lub dostępne publicznie exploity o znanych lukach. Testowanie penetracyjne lub luka Eksploatacja może być w szerokim zakresie podzielona na fazy, takie jak: eksploatacja, eksploatacja i ponowna eksploatacja. Czynności w fazie przed eksploatacją są wyjaśnione w fazach od 1 do 4, tj. Wyliczanie infrastruktury i identyfikacja podatności. Gdy luka zostanie wykorzystana w celu uzyskania dostępu do systemu, osoba atakująca powinna dążyć do szczegółowego opisania sieci, wykrywając ruch, mapując sieć wewnętrzną i próbując uzyskać konto o wyższych uprawnieniach, aby uzyskać maksymalny poziom dostępu do systemu. Umożliwi to testerom przeprowadzenie kolejnych ataków na sieć, aby jeszcze bardziej zwiększyć zakres zagrożonych systemów. Etap poeksplozji będzie również obejmował usuwanie ścieżek przez wykonywanie czynności takich jak czyszczenie dzienników i wyłączanie antywirusa. Jako tester fazy poeksploatacyjnej możesz pokazać, w jaki sposób atakujący może utrzymać dostęp do systemu poprzez backdoory i rootkity.

Etap 6 - generowanie raportów

Po zakończeniu oceny zgodnie z zakresem prac należy sporządzić raport końcowy obejmujący następujące kluczowe obszary:

• Krótkie wprowadzenie do oceny

• Zakres oceny

• Podsumowanie zarządzania / wykonawcze

• Zestawienie wyników z oceną ryzyka

• Szczegółowe informacje o każdym znalezieniu wraz z ich wpływem i zalecenia dotyczące usunięcia luki

Wprowadzenie do Nessusa

Nessus jest jednym z najczęściej używanych produktów Vulnerability Assessment. Po raz pierwszy wydany w roku 1998 przez Renaud Deraison, narzędzie to jest jednym z najpopularniejszych narzędzi do skanowania luk w zabezpieczeniach wykorzystywanych w branży od 15 lat. Oficjalna strona internetowa Nessus (http://www.tenable.com) opisuje ją następująco:

"Nessus to najbardziej rozpowszechniony w branży program do oceny słabych punktów i konfiguracji, Nessus oferuje szybkie wykrywanie, kontrolę konfiguracji, profilowanie zasobów, odkrywanie poufnych danych, integrację zarządzania łatkami, i analizę podatności na zagrożenia twojej pozycji bezpieczeństwa. Napędzany przez Nessus ProfessionalFeed, stale aktualizowaną biblioteką z ponad 50 000 indywidualnych sprawdzeń luk w zabezpieczeniach i konfiguracji oraz wspierany przez specjalistyczny zespół ds. Analizy podatności na zagrożenia, Nessus zapewnia dokładność na rynku.Nessus skaluje się, aby służyć największym organizacjom i jest szybki i łatwy rozmieścić."

Z biegiem lat, Nessus ewoluował ze skanera podatności na czystą grę w celu dodania dodatkowych funkcji oceny i audytu, takich jak kontrola konfiguracji, audyt zgodności, audyt łat, audyt systemu kontroli i audyt urządzeń mobilnych. Najbardziej znany jest z łatwości i elastyczności oferowanej przez funkcję Ocena narażenia na ataki. Kluczowa infrastruktura objęta programem Nessus Vulnerability Scanner obejmuje następujące elementy:

• Urządzenia sieciowe: takie jak Juniper, Cisco, zapory ogniowe i drukarki

• Hosty wirtualne: należą do nich VMware ESX, ESXi, vSphere i vCenter

• Systemy operacyjne: obejmują systemy Windows, Mac, Linux, Solaris, BSD, Cisco iOS oraz IBM iSeries

• Bazy danych: należą do nich: Oracle, MS SQL Server, MySQL, DB2, Informix / DRDA i PostgreSQL

• Aplikacje internetowe: obejmują serwery WWW, usługi internetowe i luki OWASP

Nessus Vulnerability Scanner jest łatwym w użyciu narzędziem. Ktoś nowy w narzędziu może go łatwo nauczyć.

Początkowa konfiguracja Nessus

Szczegółowe instrukcje dotyczące instalacji Nessus zostały podane w dalszej części . Po zainstalowaniu Nessus możesz wykonać jednorazowe ustawienia dla skanera Nessus, takie jak konfiguracja kont użytkowników w celu uzyskania dostępu do skanera; ogólne ustawienia, takie jak konfiguracja SMTP lub proxy sieci, ustawienia kanałów, ustawienia mobilne i ustawienia wyników; i konfigurowanie zaawansowanych ustawień konfiguracyjnych. Ustawienia te zostały szczegółowo opisane później. Są one bardzo unikalne dla twojego środowiska skanowania, które zależy od zasad bezpieczeństwa i

preferencji twojej organizacji. Możesz również utworzyć ogólne zasady przed przystąpieniem do skanowania, w zależności od wymagań

Planowanie skanów

Nessus zapewnia elastyczność harmonogramu skanowania na docelowych hostach do przyszłego skanowania. Jest to równie dobre, jak planowanie zadań. Możesz skonfigurować i zaplanować z góry ustalony czas i zasady. Nessus automatycznie rozpocznie skanowanie w określonym czasie i wyśle wyniki e-mailem do predefiniowanych identyfikatorów e-mail. Nie wymaga to żadnego ręcznego wyzwalacza do wywoływania skanów. Możesz także zaplanować skanowanie powtórkowe, np. "Moje adresy IP skanowania powinny być skanowane w każdy czwartek o 3:00 CET". W większości przypadków duże przedsiębiorstwa napotykają wiele wyzwań związanych z identyfikacją okna skanowania. Okno skanowania jest ramką czasową dla skanowania, które określa, w jakim czasie powinno nastąpić skanowanie, i czasem, kiedy skanowanie powinno zostać zakończone. Zazwyczaj okno skanowania jest ustalane na podstawie obciążenia produkcyjnego na skanerach. Zaleca się skanowanie maszyn produkcyjnych tylko w godzinach poza godzinami szczytu. Godziny Nonpeak to czas, kiedy cel lub maszyna skanująca jest najmniej używana w ciągu dnia / tygodnia.

Wtyczka Nessus

Aby umożliwić kompleksowy zakres kontroli bezpieczeństwa, Nessus udostępnia dużą liczbę wtyczek zgrupowanych razem w celu zapewnienia podobnych kontroli bezpieczeństwa. Grupowanie umożliwia wyłączenie lub włączenie dużej liczby wtyczek opartych na komputerach docelowych za jednym razem. Przykłady głównych rodzin wtyczek to Windows, Linux, Solaris, Cisco i Database. Aby uzyskać szczegółowe informacje na temat wtyczek i różnic między kanałem domowym a rodzinami profesjonalnych pasz, zapoznaj się z oficjalną stroną Nessus na stronie https://plugins.nessus.org.

Nessus, będąc jednym z najczęściej używanych narzędzi, ma aktywną społeczność wsparcia online na stronie https://discussions.nessus.org.

Nessus jest jednym z najbardziej opłacalnych narzędzi skanujących dostępnych z funkcjami takimi jak niski całkowity koszt posiadania (TCO) i skanuje nieograniczoną liczbę adresów IP. Subskrypcje Nessus obejmują aktualizacje oprogramowania, dostęp do plików zgodności i kontroli firmy Tenable oraz wsparcie. Dodatkowo obejmuje codzienną aktualizację luki i sprawdzanie konfiguracji za pomocą automatycznej instalacji.

Zarządzanie łatkami za pomocą Nessus

Nessus odnosi sukcesy w zarządzaniu łatkami; Osiąga się to poprzez integrację Nessus z różnymi rozwiązaniami do zarządzania poprawkami. Dobrą stroną jest to, że nie potrzebujesz dostarczać Nessusowi referencji do skanowania maszyn docelowych; zamiast tego należy podać poświadczenia systemu zarządzania poprawkami. Dzieje się tak dlatego, że system zarządzania poprawkami będzie już posiadał poświadczenia do osiągnięcia hosta docelowego.

Zarządzanie, ryzyko i sprawdzanie zgodności za pomocą Nessus

Nessus dostarcza dane wyjściowe w różnych formatach, takich jak HTML, CSV i PDF. Dzięki temu jest znacznie bardziej elastyczne, aby przekazywać dane wyjściowe do różnych narzędzi do integracji. Narzędzia te mogą być narzędziami zarządzania, ryzykiem i zgodnością, takimi jak EMC RSA Archer SmartSuit lub inne podobne narzędzie.

Instalowanie Nessusa na różnych platformach

Nessus obsługuje prawie wszystkie popularne systemy operacyjne. W zależności od dostępności systemu operacyjnego można wykonać wymagane kroki instalacji podane w tej sekcji, aby zainstalować Nessus. Najnowsze informacje / kroki można również pobrać z oficjalnej strony internetowej Nessus. Platformy systemu operacyjnego:

• Microsoft Windows - XP, 2003, 2008, Vista, 2012, 7 i 8

• Linux - Debian, Red Hat, Fedora, SuSE, Ubuntu

• Solaris

• Mac

• Darmowy BSD

• Sumy kontrolne i klucze GCP

Najnowsze informacje na temat powyższej listy można znaleźć na oficjalnej stronie internetowej Tenable Nessus pod adresem http://www.tenable.com/.

Wymagania wstępne

Skaner powinien mieć 4 GB pamięci (najlepiej). Więcej informacji na temat najnowszych wymagań można znaleźć na oficjalnej stronie firmy Nessus http://www.tenable.com/. Lepszy procesor ułatwi szybkie skanowanie. Maszyna skanująca powinna zostać wybrana, zachowując zakres widoku Nessus; jeśli planujesz przeprowadzić ocenę podatności na atak dla dużego przedsiębiorstwa, zaleca się korzystanie z wysokiej klasy komputera serwera. Żadna zapora nie powinna blokować ruchu generowanego przez Nessus w celu dotarcia do systemów docelowych. Jeśli zapora jest zainstalowana, należy skonfigurować regułę zapory, aby cały ruch generowany przez komputer Nessus mógł dotrzeć do skanowanych obiektów. Nie zapomnij wyłączyć tej reguły zapory po zakończeniu działania skanowania. Jeśli sięgasz do maszyn skanujących za pomocą serwera proxy sieci Web, poświadczenia autoryzacji serwera proxy powinny być wpisane w Nessus. Jest to opcjonalne ustawienie w zależności od twojego środowisko skanowania. Powinieneś mieć uprawnienia administratora na komputerze, aby zainstalować Nessus, a kod aktywacyjny wtyczki Nessus jest wymagany do aktualizacji wtyczek.

Instalowanie Nessus na Windows 7

Aby zapoznać się z najnowszym pakietem Nessus, aby kupić lub ocenić, należy przejrzeć oficjalną stronę internetową Teness Nessus pod adresem http://www.tenable.com/:

1. Zaloguj się na stronie internetowej Nessus, aby kupić i pobrać najnowsze oprogramowanie Nessus z sekcji Produkty. Pakiet oprogramowania Nessus należy pobrać zgodnie zsystemem operacyjnym, dla którego chcesz zainstalować Nessus. Aby pobrać pakiet Nessus, należy postępować zgodnie z instrukcjami podanymi na stronie internetowej Nessus. Ważne jest, aby pamiętać, że Nessus powinien zostać pobrany zgodnie z systemem operacyjnym skanera, z którego zamierzasz skanować inne systemy, a nie systemami operacyjnymi, które zamierzasz skanować. Na przykład, jeśli chcesz przeskanować 10 maszyn Linux, jedną maszynę Solaris i pięć maszyn Windows z komputera z systemem Windows 2008, pobierz pakiet Nessus dla systemu operacyjnego Windows 2008. W zależności od liczby bitów systemu operacyjnego można wybrać pakiet 32-bitowy / 64-bitowy.

2. Po pobraniu pliku wykonywalnego Nessus (pakiet instalacyjny Nessus), kliknij go dwukrotnie, aby rozpocząć instalację. Jeśli nie masz uprawnień administratora, naciśnij Shift i kliknij prawym przyciskiem myszy plik wykonywalny; kliknij Uruchom jako, aby uruchomić instalator z kontem administracyjnym.

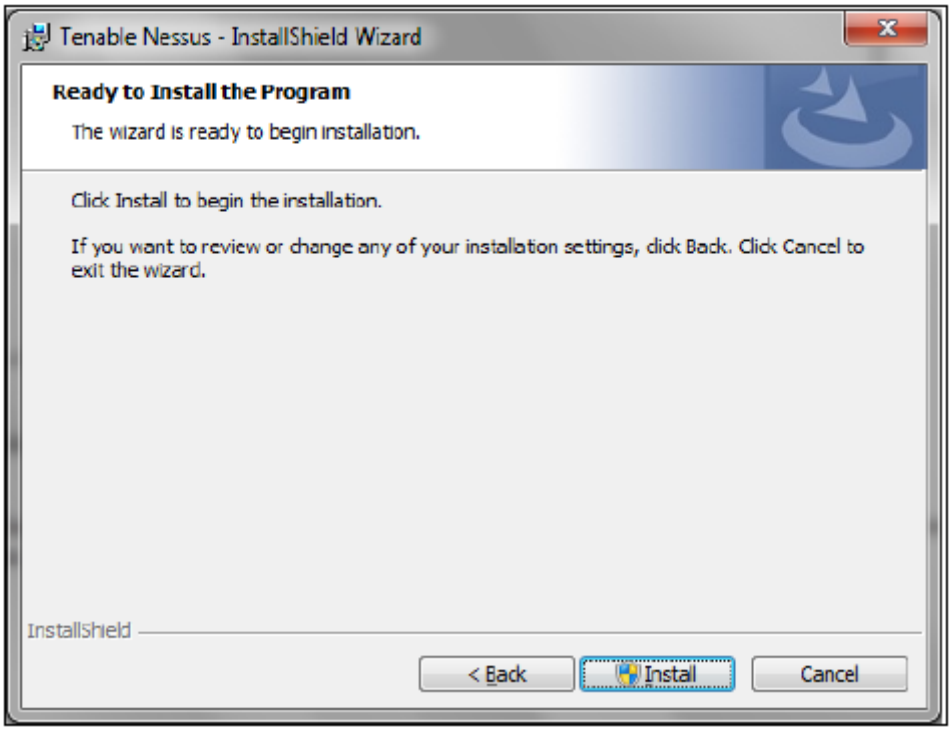
3. Możesz otrzymać ostrzeżenie o zabezpieczeniu Czy chcesz uruchomić ten plik ?. Kliknij przycisk Uruchom.

4. Po kliknięciu przycisku Uruchom instalator wyświetli okno, aby kontynuować instalację.

5. Kliknij Next, a pojawi się okno z umową licencyjną Nessus. Bardzo ważne jest, aby każdy przeczytał umowę licencyjną i przestrzegał jej

6. Aby kontynuować instalację systemu Nessus, musisz zaakceptować umowę licencyjną i kliknąć Dalej.

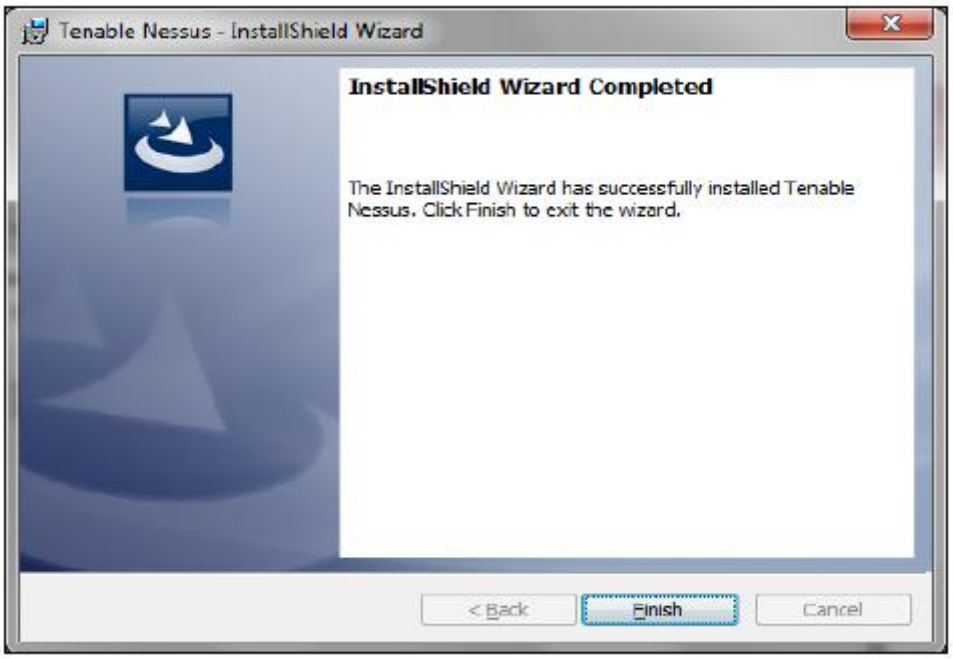
7. Masz możliwość zmiany katalogu, w którym chcesz zainstalować Nessus. Kliknij Next, aby kontynuować



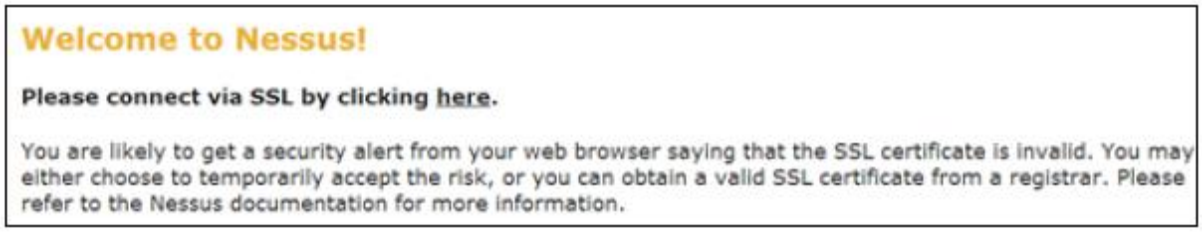
8. Kliknij Install, aby kontynuować.

9. Podczas instalacji możesz otrzymać jeszcze jeden monit z pytaniem Czy chcesz zainstalować to oprogramowanie urządzenia ?. Zaznacz pole wyboru Zawsze ufaj oprogramowaniu firmy Tenable network security Inc., jeśli chcesz zaufać wszystkim oprogramowaniu firmy Tenable. Ta opcja nie jest wymagana do wyboru. Kliknij przycisk Install w tym oknie zabezpieczeń, aby przejść dalej.

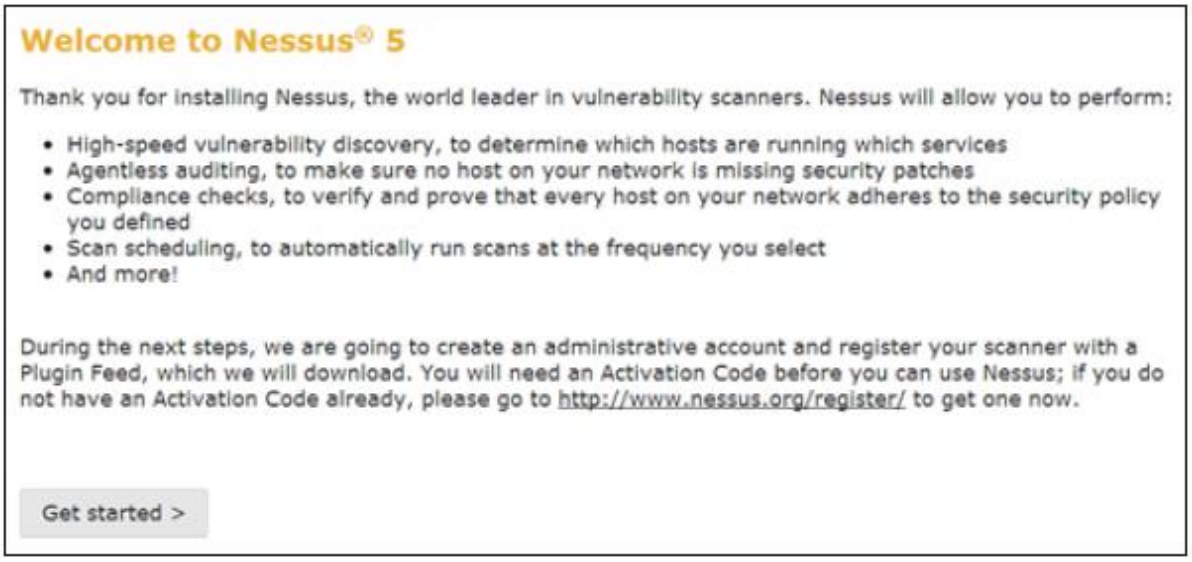
10. Poniższy zrzut ekranu pokazuje pomyślną instalację. Kliknij Finish , aby przejść dalej:



Po udanej instalacji Nessus przeniesie Cię do podstawowych konfiguracji, takich jak ustawienia domyślne, kreacje użytkownika i kod aktywacyjny. Poniższy zrzut ekranu pokazuje widok sieciowy zainstalowanego Nessus. Nessus działa domyślnie na porcie 8834:

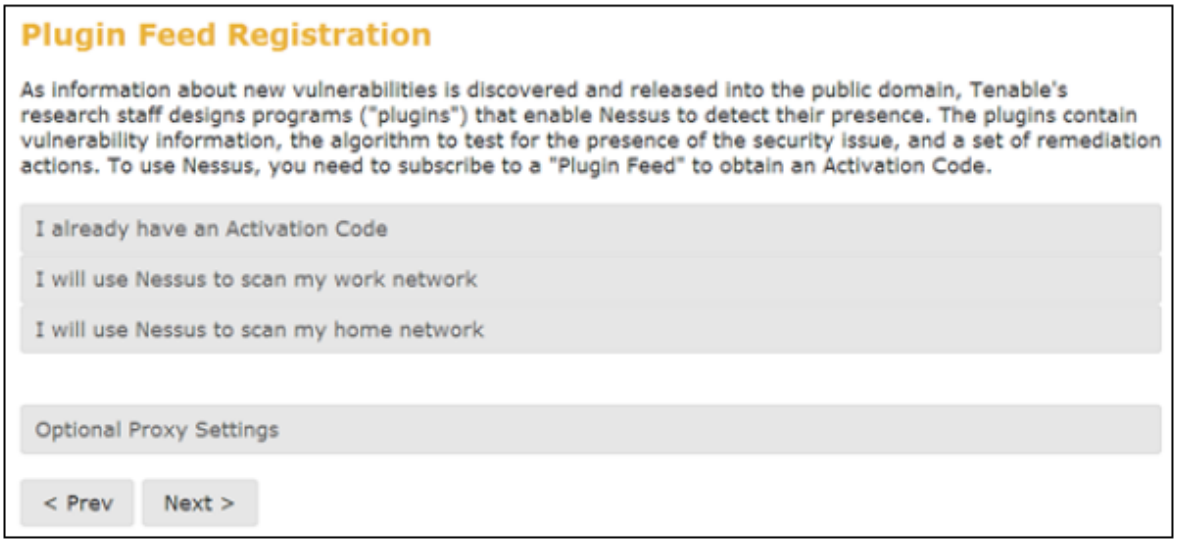


Nessus ostrzega o certyfikacie SSL. Domyślnie nie ma certyfikatu SSL. Administratorzy Nessus muszą uzyskać certyfikat SSL, aby skonfigurować Nessus z SSL. Jeśli chcesz zainstalować sam certyfikat SSL, zainstaluj go; w przeciwnym razie kliknij Proceed anywayo kontynuuj. Spowoduje to przejście do strony wstępu. Kliknij Get started, aby kontynuować.



Pierwszą rzeczą, którą musisz zrobić po tej konfiguracji konta administracyjnego. To konto jest tworzone na serwerze Nessus. To konto powinno zawsze być zapamiętane dla administracji Nessus.

Po utworzeniu konta administracyjnego Nessus poprosi o rejestrację źródła wtyczek i ustawienia proxy, co jest opcjonalne.



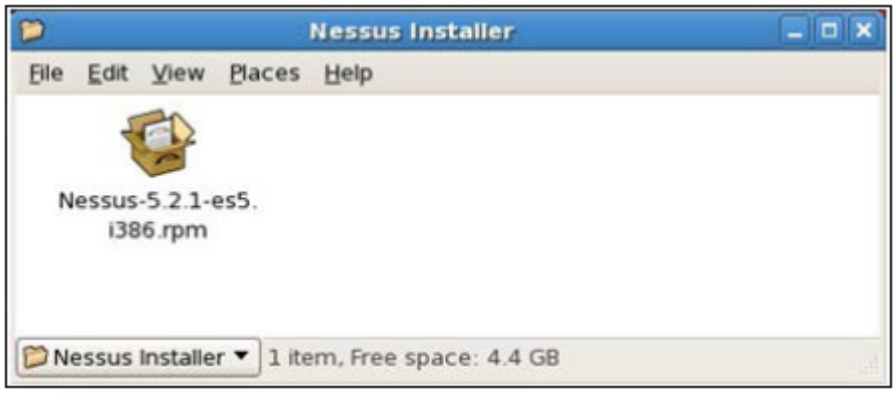
Wtyczka wprowadzania rejestracji musi być wykonana zgodnie z przewidywanym użytkowaniem. Po rejestracji otrzymasz kod aktywacyjny, którego potrzebujesz do subskrypcji wtyczki.

Instalowanie Nessusa w systemie Linux

Aby zapoznać się z najnowszym pakietem Nessus, zarówno w celu zakupu, jak i oceny, należy odwiedzić oficjalną stronę firmy Tenable Nessus pod adresem http://www.tenable.com/:

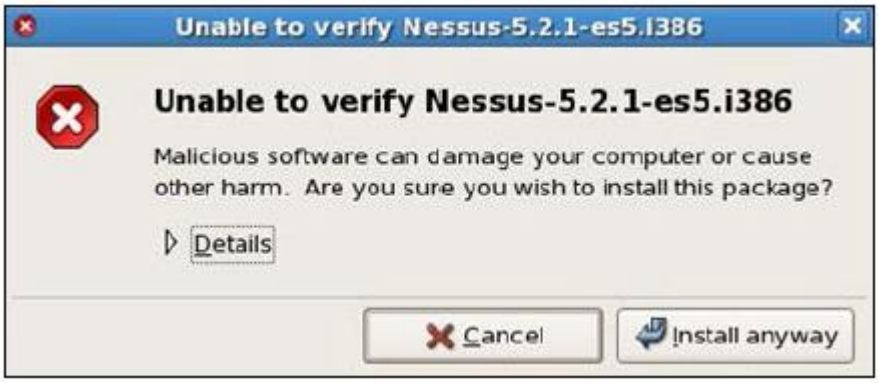
1. Zaloguj się na stronie internetowej Nessus, aby kupić i pobrać najnowsze oprogramowanie Nessus z sekcji Produkty, zgodnie z systemem operacyjnym i wersją. Kroki opisane tutaj dotyczą systemu Red Hat Linux 5.2.

2. Po pobraniu pliku wykonywalnego Nessus (pakiet instalacyjny Nessus), kliknij go dwukrotnie, aby rozpocząć procedurę instalacji. Do instalacji wymagane są uprawnienia administracyjne / root

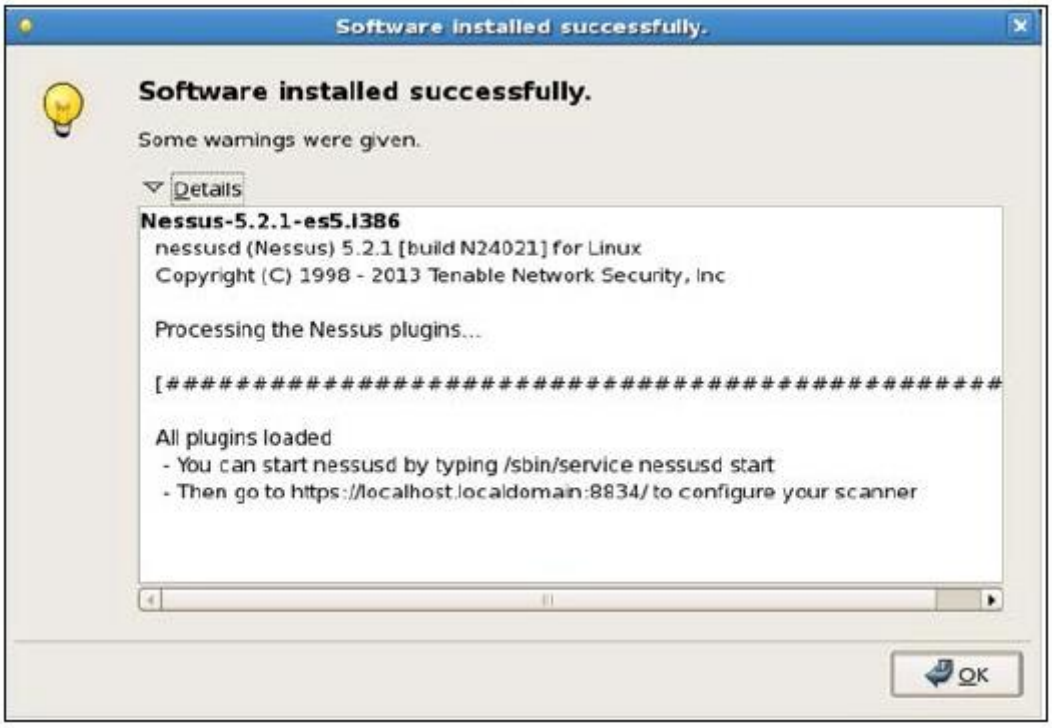


Pojawi się okno Installing packages pokazane w pliku następujący zrzut ekranu:

3. Kliknij przycisk Apply.



4. Kliknij Install anyway, aby kontynuować instalację



Powyższy zrzut ekranu pokazuje, że Nessus został pomyślnie zainstalowany w środowisku Red Hat Linux. Na początek należy uruchomić usługę Nessus.

5. Aby uruchomić usługę Nessus na terminalu Linux, należy wykonać następujące polecenie:

/ sbin / service nessusd start

Poniższy zrzut ekranu pokazuje uruchamianie usługi Nessus ze statusem OK:

6. Aby skonfigurować skaner Nessus, wpisz adres URL https: //localhost.localdomain: 8834 / w przeglądarce internetowej w systemie Linux. Ta strona wyświetla błąd bezpiecznego połączenia, który można poprawić, dodając wyjątek do przeglądarki internetowej.

7. Kliknij link Or you can add an exception

8. Kliknij Add Exception i Get Certificate. Spowoduje to aktywację przycisku Confirm Security Exception. Po kliknięciu w tę stronę przeglądarka wyświetli stronę główną skanera Nessus.

Aby dalej konfigurować, można wykonać takie same kroki, jak opisane dla instalacji systemu Windows w celu rejestracji, aktywacji, aktualizacji wtyczek, zarządzania użytkownikami i tak dalej.

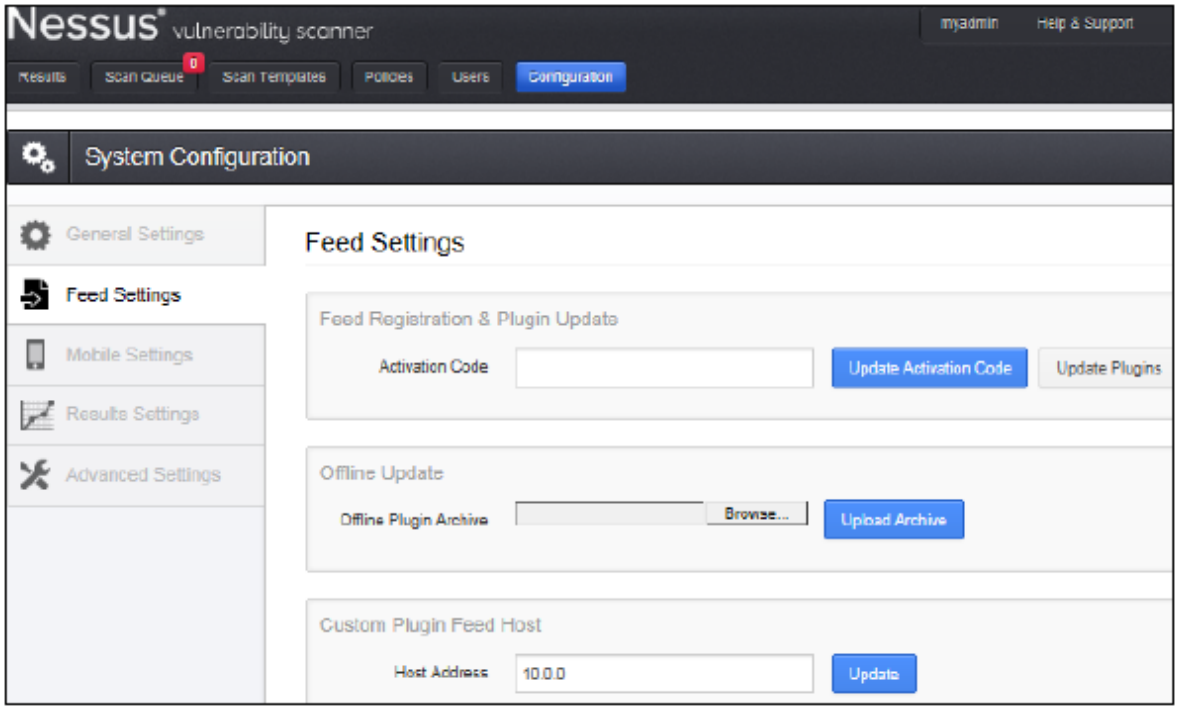
Aktualizacja definicji Nessusa (wtyczek) jest ważna, ponieważ dzięki temu Nessus jest aktualizowany i może identyfikować wszystkie najnowsze luki. Aby przeprowadzić udane skanowanie w poszukiwaniu luk w oprogramowaniu Nessus, przed rozpoczęciem skanowania należy sprawdzić i zaktualizować Nessus za pomocą najnowszych wtyczek. Aby zaktualizować Nessus na komputerze z systemem Windows, należy wykonać następujące kroki:

1. Zaloguj się do serwera Nessus przy użyciu konta administratora.

2. Kliknij kartę Konfiguracja na górnym pasku menu.

3. Po kliknięciu karty Konfiguracja, Nessus otworzy ustawienia konfiguracji systemu. To będzie miało podzakładki, mianowicie Ustawienia ogólne, Ustawienia kanału, Ustawienia mobilne, Ustawienia wyników i Ustawienia zaawansowane.

4. Kliknij kartę Ustawienia podawania na lewym panelu wyboru. Spowoduje to otwarcie strony w celu aktualizacji pliku wtyczek Nessus.



Nessus udostępnia wiele opcji pliku danych w następujący sposób:

• Aktualizacje wtyczek online

• Aktualizacje wtyczek offline

• Własne wtyczki obsługują aktualizacje hostowane

Aktualizacaje wtyczek online

Aktualizacja wtyczki online jest najpopularniejszą opcją aktualizowania wtyczek Nessus i zapewnia możliwość aktualizacji wtyczek przez Internet. Wymaga to połączenia internetowego o dość dobrej prędkości na maszynie Nessus. Po rejestracji i aktywacji Nessus wtyczki można aktualizować, klikając przycisk Aktualizuj wtyczki.

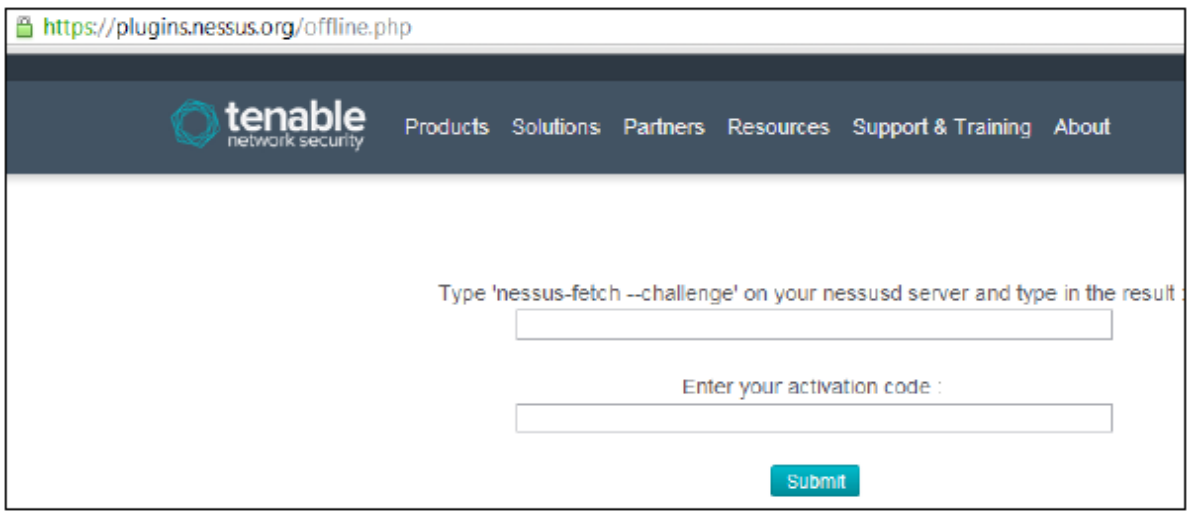
Aktualizacje wtyczek offline

Aktualizacja wtyczki offline jest używana, gdy wtyczki są archiwizowane w lokalnym katalogu, z którego Nessus może pobierać i aktualizować. To nie wymaga połączenia z Internetem w systemie Nessus. Aby skonfigurować aktualizację offline, najpierw należy uzyskać kod aktywacyjny subskrypcji Nessus, który można pobrać ze wsparcia Nessus lub zarejestrowanego identyfikatora e-mail używanego do rejestracji kanału Nessus. Następnym krokiem jest wygenerowanie kodu wyzwania, który służy do pobierania wtyczek wraz z kodem aktywacyjnym. Aby wygenerować kod wyzwania na komputerze z systemem Windows Nessus, uruchom następujące polecenie w narzędziu wiersza polecenia: \ Program Files \ Tenable \ Nessus> nessus-fetch.exe --challenge W przypadku komputera z systemem Linux Nessus polecenie jest nieco inne; następujące polecenie powinno zostać uruchomione na terminalu Linux:

/ opt / nessus / bin / nessus-fetch --challenge

Spowoduje to wygenerowanie długiego ciągu znaków, który nazywany jest kodem wyzwania. Przykładowy kod wywoławczy to 19c4ed603ac3e436a14239852c8fbf8f26f02d7b.

Aby nadal pobierać wtyczki offline, przejdź na stronę pobierania offline wtyczek Nessus pod adresem https://plugins.nessus.org/offline.php. Po załadowaniu strona wyświetla monit o kod wyzwanie i kod aktywacyjny. Wprowadź je.



Niestandardowe wtyczki obsługują aktualizacje hostowane

Niestandardowy host kanału wtyczek można skonfigurować za pomocą tej opcji. Można ustawić nazwę hosta lub adres IP hosta.

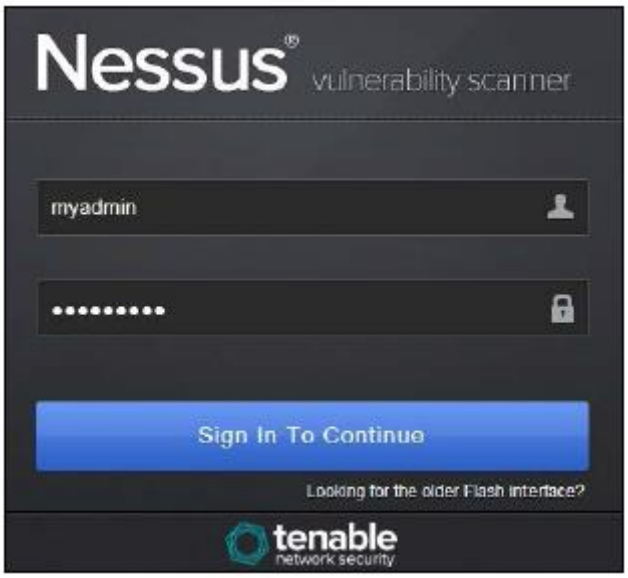
Zarządzanie użytkownikami

Zarządzanie użytkownikami to dodatkowa funkcja zapewniona przez Nessus, która jest najbardziej przydatna w dużym środowisku korporacyjnym, w którym Nessus jest używany przez wiele osób w wielu lokalizacjach. W takim środowisku funkcja ta umożliwia administratorom włączanie różnego poziomu dostępu dla wielu użytkowników na skanerze Nessus. Nessus zapewnia dwie różne role dla użytkowników w następujący sposób:

• Administrator

• Użytkownik inny niż administrator

Rola administratora ma dostęp do wszystkich funkcji Nessus, podczas gdy rola użytkownika innego niż administrator ma ograniczony dostęp. Rola nie-administratora nie zapewnia dostępu do zarządzania użytkownikami, ustawień ogólnych, ustawień kanałów i ustawień zaawansowanych. Podczas instalacji Nessus, użytkownik administracyjny jest tworzony dla administracji Nessus. Aby kontynuować zarządzanie użytkownikami Nessus, konieczne jest zalogowanie się przy użyciu tego konta ponieważ ma uprawnienia administratora. Adres URL https: // localhost: 8834 / można przeglądać na komputerze z systemem Windows.



Wprowadź nazwę użytkownika i hasło administratora, aby się zalogować. Wyświetli się strona główna programu Nessus, jak pokazano na poprzednim zrzucie ekranu. Pod logowaniem administracyjnym zostanie wyświetlonych wiele kart. Kliknij kartę Użytkownicy, aby przejść dalej za pomocą czynności zarządzania użytkownikami. W Nessusie zarządzanie użytkownikami zapewnia następujące opcje:

• Dodawanie nowego użytkownika

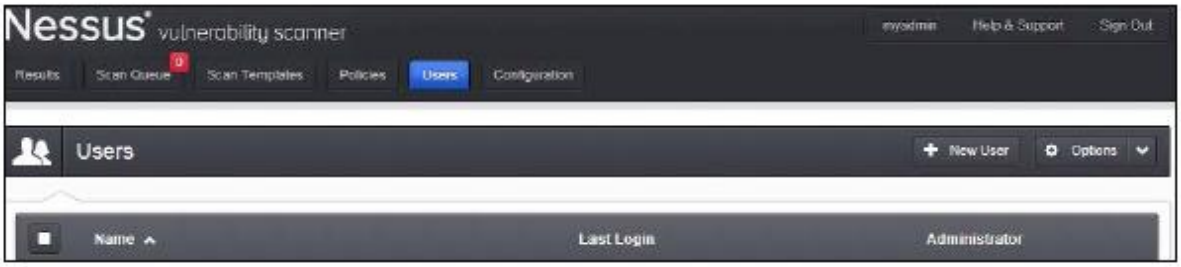
• Usuwanie istniejącego użytkownika

• Zmiana hasła dla istniejącego użytkownika

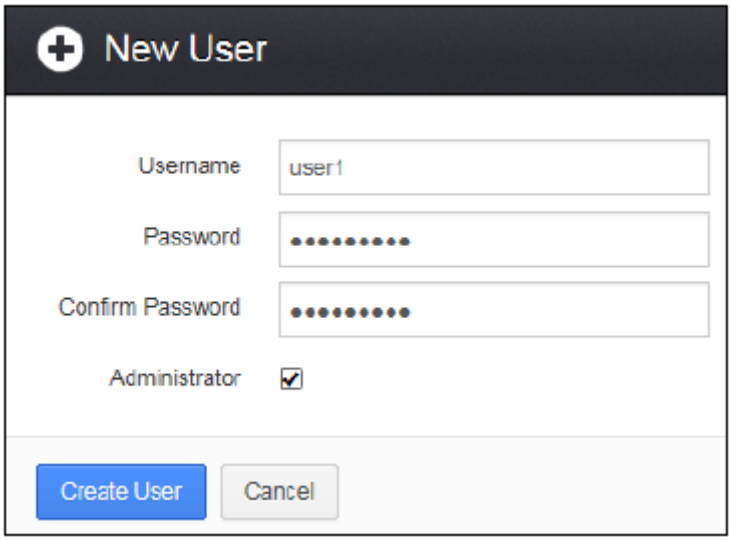
• Zmiana roli istniejącego użytkownika

Dodawanie nowego użytkownika

Kliknij przycisk New user, aby dodać nowego użytkownika.

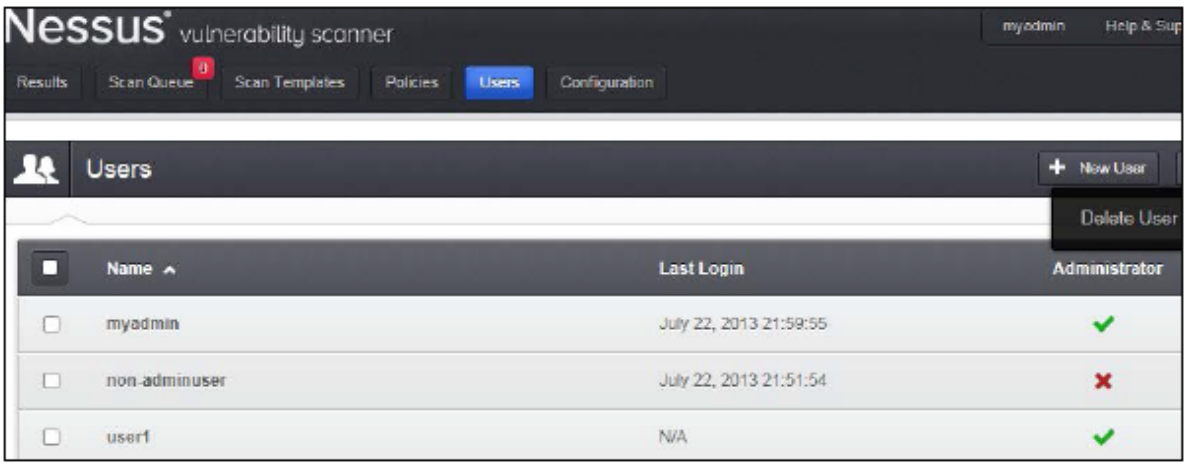


Spowoduje to wyświetlenie zachęty nowego użytkownika do ustawienia nazwy użytkownika, hasła i roli dla nowego użytkownika, jak pokazano na poniższym zrzucie ekranu:



Usuwanie istniejącego użytkownika

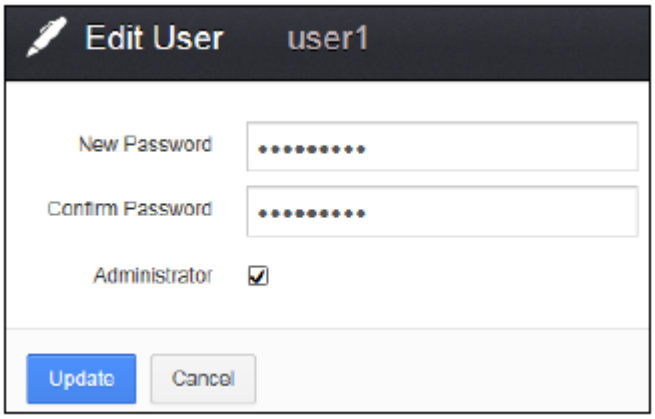
Usuń użytkownika to funkcja używana, gdy użytkownik nie jest już potrzebny w skanerze Nessus. W takich przypadkach wybierz użytkownika, który musi zostać usunięty z nagłówka Użytkownicy, i kliknij przycisk Usuń użytkownika z opcji wyświetlanych po prawej stronie.



Zmiana hasła lub roli istniejącego użytkownika

Czasami administrator otrzymuje żądania zmiany hasła dla użytkowników. Może tak być, ponieważ użytkownik zapomniał swojego hasła lub dlatego, że jego rola wymaga zmiany. W takich przypadkach

wybierz użytkownika, dla którego hasło lub rola musi zostać zmieniona, i kliknij go dwukrotnie. Spowoduje to wyświetlenie następującego okna, aby ustawić nowe hasło lub zmienić rolę:



Konfiguracja systemu Nessus

Ustawienia konfiguracji systemu Nessus można znaleźć w zakładce Konfiguracja. Ma pięć różnych grup ustawień w następujący sposób:

• Ustawienia główne

• Ustawienia kanałów

• Ustawienia mobilne

• Ustawienia wyników

• Zaawansowane ustawienia

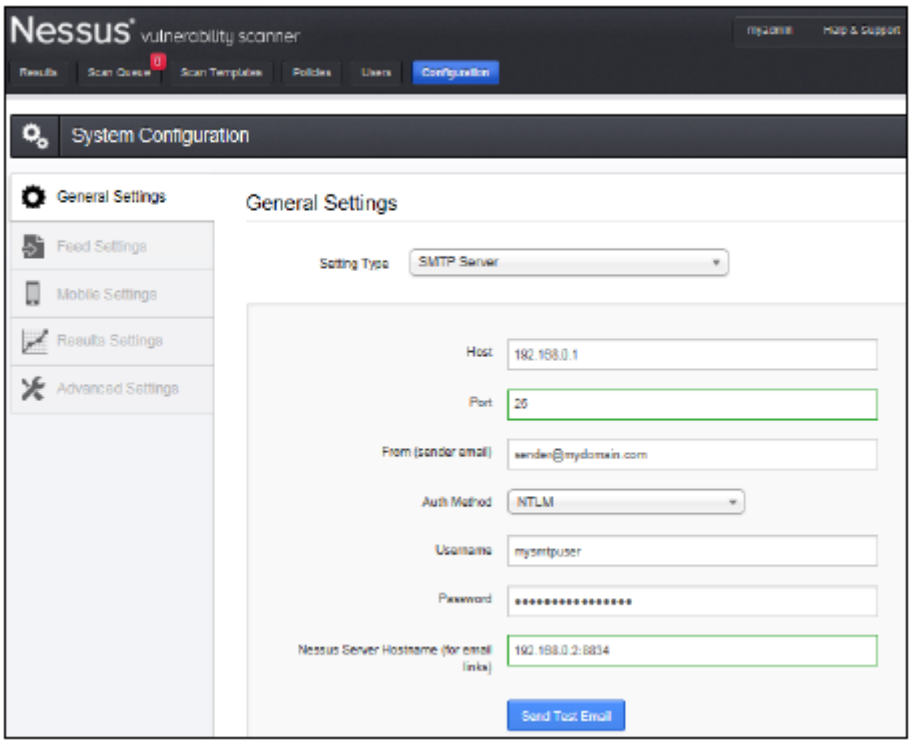
Ustawienia główne

Zakładkę Ustawienia ogólne można zobaczyć w Konfiguracji, logując się do Nessus z uprawnieniami administratora. Istnieją dwie różne opcje ustawień ogólnych, które istnieją w menu rozwijanym Typ ustawienia:

• Serwer SMTP

• Proxy

Ustawienia serwera SMTP umożliwiają skonfigurowanie serwera SMTP za pomocą serwera Nessus w celu wysyłania wyników ukończonych skanów za pomocą automatycznych wiadomości e-mail.



Ustawienia SMTP

Różne ustawienia SMTP można skonfigurować zgodnie z konfiguracją SMTP. Ustawienia SMTP wyjaśniono w poniższej tabeli:

Ustawienie SMTP	:	Opis
Host	:	Nazwa hosta lub adres IP serwera SMTP.
Port	:	Numer portu do połączenia z serwerem SMTP.
Od (E-mail nadawcy)	:	Identyfikator e-mail z e-maili z raportami powinien pojawić się jako nadawca.
Metoda uwierzytelniania	:	Metoda uwierzytelniania SMTP.
Nazwa użytkownika	:	Nazwa użytkownika do uwierzytelnienia na serwerze SMTP.
Hasło	:	Hasło odpowiadające tej nazwie użytkownika.
Nazwa hosta serwera Nessus	:	Dotyczy tylko linków do wiadomości e-mail, nazwy hosta serwera Nessus lub adresu IP s do określenia.
Wyślij testową wiadomość e-mail	:	Umożliwia testowanie przez wysłanie testowej wiadomości e-mail

Ustawienia sieci proxy

Niektóre organizacje obsługują serwer proxy sieci między zewnętrznymi i wewnętrznymi sieciami, aby przepuścić ruch. Aby zaktualizować Nessus o najnowsze wtyczki w środowisku proxy sieci, konieczne jest skonfigurowanie ustawień web proxy zgodnie z konfiguracją organizacji. Dzięki temu Nessus może uzyskać dostęp do serwera wtyczek Nessus przez Internet, aby pobrać najnowsze wtyczki. Różne

ustawienia web proxy można skonfigurować zgodnie z konfiguracją web proxy. Te ustawienia są wyjaśnione w poniższej tabeli:

Ustawienie sieci proxy	:	Opis
Host	:	Nazwa hosta lub adres IP serwera proxy.
Port	:	Numer portu serwera proxy do połączenia.
Nazwa użytkownika	:	Nazwa użytkownika do połączenia z proxy.
Hasło	:	Hasło do nazwy użytkownika do połączenia z proxy.
User-agent	:	Wymagany, jeśli serwer proxy używa specyficznych dla filtru agentów HTTP. Niestandardowy ciąg agenta użytkownika musi zostać określony.

Ustawienia kanału

Ustawienia kanałów opisano w sekcji Aktualizacja definicji w tej części.

Ustawienia mobilne

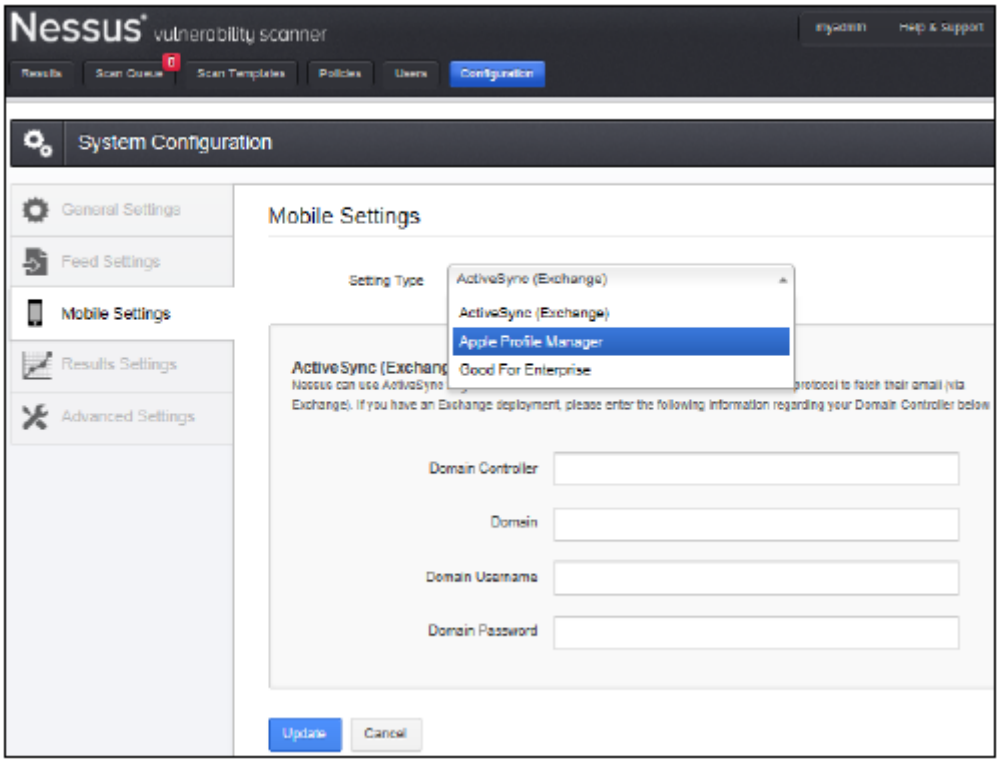
Kwestia bezpieczeństwa urządzeń mobilnych stała się w ostatnim czasie priorytetem w przypadku powszechnego korzystania z urządzeń mobilnych w domenie firmowej, w której proaktywnie wykorzystywane są koncepcje takie jak Bring Your Own Device (BYOD). Takie urządzenia, kiedy połączone z sieciami korporacyjnymi niesie ze sobą nieodłączne luki w ich platformach mobilnych. Nessus oferuje mobilną opcję skanowania bezpieczeństwa, w której informacje i luki w zabezpieczeniach urządzeń przenośnych są ostatnio połączone odpowiednie serwery są skanowane. Obecnie dołączone są wtyczki związane z urządzeniami iPhone 4, iPad, Windows Phone i Android, a Nessus ma możliwość skanowania interfejsów usługi Active Directory (ADSI) i programu Apple Profile Manager w celu identyfikacji urządzeń mobilnych podłączonych do tych serwerów oraz do zidentyfikować podatności. Karta Ustawienia mobilne zawiera opcje konfiguracji ustawień dla następującego typu:

• ActiveSync (Exchange)

• Menedżer profili Apple

• Dobry dla przedsiębiorstw

Można to zobaczyć na poniższym zrzucie ekranu:



ActiveSync (Exchange)

Nessus można skonfigurować tak, aby korzystał z ActiveSync do zbierania informacji o wszystkich urządzeniach mobilnych, które używają tego protokołu do pobierania swoich wiadomości e-mail (przez Exchange). Jeśli masz wdrożenie Exchange, możesz skonfigurować ustawienia kontrolera domeny zgodnie z poniższą tabelą:

Ustawienia mobilne ActiveSync	:	Opis
Kontroler domeny	:	Adres IP kontrolera domeny.
Domena	:	Nazwa domeny.
Nazwa użytkownika domeny	:	Nazwa użytkownika do połączenia domeny.
Hasło domeny	:	Hasło do nazwy użytkownika, z którą chcesz się połączyć.

Menedżer profili Apple

Nessus można skonfigurować tak, aby korzystał z programu Apple Profile Manager do zbierania informacji o wszystkich urządzeniach z systemem iOS. Jeśli wdrożono aplikację Apple Profile Manager, można skonfigurować ustawienia Apple Profile Manager zgodnie z poniższą tabelą:

Ustawienie mobilne Apple Profile Manager : Opis

Serwer Apple Profile Manager : Adres IP serwera menedżera Apple Profile.

Port Apple Profile Manager : Port serwera programu Apple Profile Manager do połączenia się

Apple Profile Manager nazwa użytkownika : Nazwa użytkownika, z którego można się logować.

Apple Profile Manager hasło : Hasło odpowiadające nazwie użytkownika.

SSL : Zaznacz / odznacz tę opcję w oparciu o środowisko.

Verify SSL Certificate : Zaznacz tę opcję, jeśli chcesz certyfikat SSL do zweryfikowania.

Force Device Update : Zaznacz tę opcję, jeśli chcesz aktualizować urządzenie

Device Update Timeout (Minutes) : Limit czasu aktualizacji urządzenia w ciągu kilku minut.

Dobry dla przedsiębiorstw

Nessus można skonfigurować tak, aby korzystał z zarządzania urządzeniami Good Mobile do zbierania informacji o wszystkich urządzeniach mobilnych korzystających z tego protokołu. Jeśli wdrożono produkt Good For Enterprise, można skonfigurować ustawienia wymienione w poniższej tabeli:

Ustawienie mobilne Good For Enterprise : Opis

Serwer GMC : W tym miejscu należy wspomnieć o adresie IP serwera GMC.

Port : Numer portu używany do łączenia się z serwerem GMC.

Domena : Nazwa domeny.

Nazwa użytkownika : Nazwa użytkownika, z którą chcesz się połączyć.

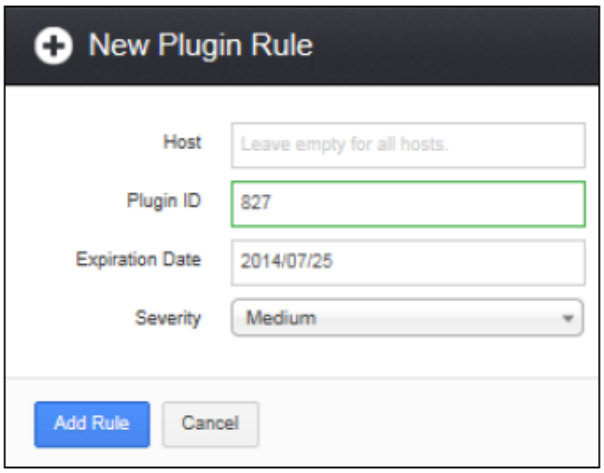
Hasło : Hasło odpowiadające nazwie użytkownika.

SSL : Zaznacz / odznacz tę opcję w zależności od środowiska.

Verify SSL Certificate : Zaznacz tę opcję, jeśli chcesz, aby urządzenie było weryfikowane.

Ustawienia wyników

Wynik Ustawienia można zobaczyć w Konfiguracjach. Pozwala to na dodanie reguł, aby wyłączyć wtyczki lub zmienić ich poziom ważności. Poniższy zrzut ekranu pokazuje, jak dodać nową regułę wtyczki:



Poniższa tabela przedstawia szczegółowo nowe opcje reguł wtyczki:

Nowa opcja reguły wtyczki : Opis

Host : Jeśli reguła wtyczki wyniku dotyczy tylko konkretnego adresu IP / hosta, hosta można wspomnieć w polu Host. Jeśli reguła ma być zastosowana dla całego zeskanowanego hosta można pozostawić to pole puste.

Identyfikator wtyczki : Identyfikator wtyczki, który należy podać, aby określić wtyczkę dla reguły.

Data ważności : Data wygaśnięcia reguły może być tu określona na wypadek, gdyby musiała wygasnąć w określonym dniu.

Poziom istotności : można ustawić z menu rozwijanego zgodnie z regułą chcesz ustawić. Może być ukryty, informacyjny, niski, średni, wysoki lub krytyczny.

Zaawansowane ustawienia

Menu konfiguracji GUI Nessus zawiera kilka konfigurowalnych opcji. Zaleca się, aby te ustawienia były odpowiednio przeglądane i modyfikowane w zależności od środowiska skanowania. Opcję można zmienić i zapisać za pomocą przycisku Zapisz lub można ją całkowicie usunąć przy użyciu znaku X obecnego obok opcji. Należy zachować szczególną ostrożność podczas modyfikowania wartości max_hosts i max_checks w nadchodzącej tabeli. Wartości te reprezentują maksymalną liczbę sprawdzeń i hostów skanowanych jednocześnie i mają bezpośredni wpływ na skanowanie, które ma zostać wykonane. Wartość max_checks, jeśli jest większa niż 5, może mieć negatywny wpływ na serwery docelowe, dlatego należy jej unikać. Podobnie wysoka wartość max_hosts może przytłoczyć system skanowania hosta i zależy od pojemności hosta, na którym jest zainstalowany Nessus. Zaleca się, aby wartość ta była utrzymywana na stosunkowo niskim poziomie (można rozpocząć od 10); może być zoptymalizowany zgodnie ze środowiskiem i możliwościami systemu. Poniższy zrzut ekranu pokazuje niektóre opcje z poniższej tabeli; opcje można dodawać lub usuwać za pomocą odpowiednio karty Dodaj ustawienia i X. Zaawansowane opcje ustawień i ich zastosowania zgodnie z dokumentacją Nessus wymienione w poniższej tabeli:

Nowe opcje reguły wtyczki : Opis : Wartość domyślna

allow_post_scan_editing : Jeśli jest włączona, możliwa jest edycja po skanowaniu. : Tak

auto_enable_dependencies : Automatycznie aktywuje wtyczki, które zależą od tego. Jeśli wyłączona, nie wszystkie wtyczki mogą działać, mimo że został wybrany w zasadę skalowania : Tak

auto_update : Kontroluje automatyczne aktualizacje wtyczek. Jeśli włączony i Nessus jest zarejestrowany, to pobiera najnowsze wtyczki z wtyczek. nessus.org automatycznie. Wyłącz, jeśli skaner znajduje się w odizolowanej sieci nie w stanie dotrzeć do Internetu. : tak

auto_update_delay : Liczba godzin do czekania między dwie aktualizacje. Cztery godziny (4) to minimalny dozwolony okres. : 24

cgi_path : Podczas testowania serwerów internetowych użyj rozdzielana dwukropkami lista ścieżek CGI : / cgi-bin: /scripts

checks_read_timeout : Pozwala określić limit czasu odczytu dla gniazda testów : 5

disable_ntp : Wyłącza stary protokół NTP : Tak

disable_xmlrpc : Wyłącza nowy XMLRPC interfejs (serwer WWW) : Nie

Dumpfile : Pozwala określić lokalizację zrzutu pliku do debugowania wyjścia, jeśli został wygenerowany : C:\Program Data\Tenable\Nessus \ nessus \logs \ nessusd. dump

global.max_hosts : Maksymalna liczba hostów, które mogą zeskanować : 130

global.max_scans : Jeśli ustawisz wartość niezerową, umożliwi to zdefiniowaie maksymalną liczbę skanów, może się to odbywać równolegle : 0

global.max_simult_tcp_session : Maksymalna liczba jednoczesnych połączeń TCP : 50

global.max_web_users : Jeśli ustawiono wartość niezerową, definiuje to maksymalną (internet) liczbę użytkowników, którzy mogą połączyć równolegle : 1024

listen_address : Adres IPv4 do nasłuchiwania przychodzących znajomości. Jeśli ustawione na 127.0.0.1, to będzie ograniczać dostęp tylko do połączeń lokalnych. : 0.0.0.0

listen_port : Port do nasłuchiwania (stary NTP protokół). Używane przed wersją 4.2 klienta NessusClient znajomości : 1241

log_whole_attack : Umożliwia rejestrowanie każdego szczegółu pliku atak i jest pomocny przy debugowaniu problemu ze skanowaniem, ale może tak być dyskiem intensywnym : Nie

Logfile : Gdzie przechowywany jest plik dziennika Nessus. : C:\ Program Data\Tenable\Nessus \ nessus\logs \ nessusd.dump

max_checks : Maksymalna liczba równoczesnych kontroli każdego testowanego hosta : 5

max_hosts : Sprawdzono maksymalną liczbę hostów w pewnym momencie podczas skanowania : 5

nasl_log_type : Kieruj typem danych wyjściowych silnika NASL w nessusd.dump : Normalna

nasl_no_signature_check : Umożliwia określenie, czy Nessus powinien rozważyć wszystkie skrypty NASL jako być podpisanym. Wybór Tak jest niebezpieczny i nie jest zalecany : Nie

non_simult_ports : Umożliwia spreparowanie tych portów które dwie wtyczki nie powinny być uruchamiane równocześnie : 139, 445, 3389

optimize_test : Pozwala zoptymalizować procedurę testową. Zmiana tego na Nie spowoduje skanowanie trwać dłużej i zazwyczaj generować więcej fałszywych alarmów : Tak

plugin_upload : Pozwala określić, czy użytkownicy administratorów mogą przesyłać wtyczki : Tak

plugins_timeout : Maksymalny czas życia wtyczek aktywność (w sekundach) : 320

port_range : Zakres portów, które będą skanery portów skandować. Może używać słów kluczowych jako domyślnych lub Wszystkie, a także listę rozdzielaną przecinkami portów lub zakresów portów : Domyślna

purge_plugin_db : Pozwala określić, czy Nessus powinien oczyść bazę danych wtyczek w każdym z nich aktualizacja. To nakazuje Nessusowi usunięcie, ponownie pobrać i odbudować wtyczkę bazy danych dla każdej aktualizacji. Wybór Tak spowoduje aktualizację znacznie wolniej : Nie

qdb_mem_usage : Powoduje, że Nessus używa mniej lub więcej pamięć podczas bezczynności. Jeśli Nessus działa na dedykowanym serwerze, ustawiając to na Wysoki użyje więcej pamięci do zwiększenia wydajność. Jeśli Nessus jest uruchomiony współdzielona maszyna, ustawiając tę wartość na Low użyje znacznie mniej pamięci, ale za umiarkowaną wydajność wpływ. : Niska

reduce_connections_on_congestion : Pozwala zmniejszyć liczbę połączeń w przypadku przekrwienia : Nie

report_crashes : Umożliwia określenie, czy anonimowo zgłasza awarie do Tenable : Tak

Reguły : Lokalizacja pliku reguł Nessus (nessusd.rules). : C:\Program Data\Tenable\Nessus\ conf \nessusd.rules

safe_checks : Bezpieczne kontrole polegają na przechwytywaniu banerów zamiast aktywnego testowania dla wrażliwości : Tak

silent_dependencies : Jeśli ta opcja jest włączona, lista wtyczek zależności i ich wyniki są nieuwzględnione w raporcie. Wtyczka może zostać wybrany jako część polityki, która zależy od innych uruchomionych wtyczek. Domyślnie Nessus uruchomi te wtyczki zależności, ale ich nie uwzględni wyniki w raporcie. Ustawianie tej opcji na Nie spowoduje obu wybranych wtyczek i wszelkie zależności wtyczki do pojawienia się w raporcie. : Tak

slice_network_address : Jeśli ta opcja jest ustawiona, Nessus nie skanuj sieć przyrostowo (10.0.0.1, następnie 10.0.0.2, a następnie 10.0.0.3 itd.) ale spróbuje obciąć obciążenie pracą w całej sieci (np. skanuje 10.0.0.1, a następnie 10.0.0.127, a następnie 10.0.0.2, a następnie 10.0.0.128, i tak dalej) : Nie

ssl_cipher_list : Zapewnia, że tylko "silne" szyfrowanie SSL używane podczas łączenia się przez port 1241. Obsługuje silne słowo kluczowe lub ogólne oznaczenia OpenSSL jako wymienione na http://www.openssl.org/docs / apps / ciphers.html : Silny

stop_scan_on_ disconnect : Pozwala zatrzymać skanowanie tego hosta wydaje się, że został rozłączony podczas skanowania : Nie

stop_scan_on_hang : Pozwala zatrzymać skanowanie, które wydaje się rozłączać. : Nie

throttle_scan : Skanowanie przepustnicy jest przeciążony dla CPU : Tak

www_logfile : Pozwala określić miejsce w sieci Nessus rejestr serwera (interfejsu użytkownika) jest przechowywany: C:\Program Data\Tenable\Nessus \ nessus \logs \ www_server.log

xmlrpc_idle_session_timeout : Limit czasu sesji bezczynności dla Nessus : 30

xmlrpc_listen_port : Port serwera Nessus do nasłuchu (nowy protokół XMLRPC) : 8834

Wszystkie te zaawansowane ustawienia muszą zostać właściwie przeanalizowane przed zastosowaniem. Zalecane ustawienia mogą się różnić w zależności od środowiska. Kilka sekcji tego rozdziału, które są specyficznymi ustawieniami konfiguracji, zostały przywołane z materiałów edukacyjnych dostępnych na stronie internetowej Nessus:

http://www.tenable.com.

Podsumowanie

W tej sekcji nauczyliśmy się podstaw oceny podatności na ataki i testowania penetracji, a także zapoznaliśmy się z Nessusem. VA i PT są kluczowymi rodzajami oceny ryzyka technicznego, w których VA koncentruje się na wykrywaniu słabych punktów lub słabych punktów infrastruktury, a PT przechodzi na kolejny poziom, aby wykorzystać te luki. Oceny takie są przeprowadzane jako kontrola prewencyjna w celu identyfikacji i złagodzenia luk w zabezpieczeniach lub spełnienia różnych wymogów zgodności. Kluczowe działania dla takich testów obejmują scoping, zbieranie informacji, skanowanie luk w zabezpieczeniach, fałszywe pozytywne analizy, wykorzystanie luki w

zabezpieczeniach (test penetracji) i generowanie raportów. Scoping obejmuje inne podejście do testowania Blackboksa (brak informacji o infrastrukturze) i Greybox (dane uwierzytelniające i szczegóły dotyczące infrastruktury są udostępniane). W tym rozdziale przedstawiliśmy również wprowadzenie do Nessusa jako jednego z powszechnie używanych skanerów podatności. Korzysta z kontroli bezpieczeństwa, zwanych wtyczkami, przeciwko którym wykryto luki podczas skanowania. Rodzina głównych wtyczek obejmuje systemy Windows, Linux, Solaris, Cisco i bazy danych. Z biegiem lat Nessus dodał funkcje, takie jak konfiguracja i kontrola zgodności, oprócz podstawowej funkcjonalności skaner podatności. Nessus może być zainstalowany na wszystkich głównych systemach operacyjnych i szczegółowych krokach instalacji Nessus na Windows 7 i Linux OS - wraz z wymaganiami są wymienione w tym rozdziale. Podczas początkowej konfiguracji tworzone jest pierwsze konto administratora, aby zalogować się do Nessus jako administrator i na podstawie tego wymogu aktywowany jest kanał domowy lub profesjonalny. Następnie aktualizuje się wtyczkę. Została również wyjaśniona opcja aktualizacji wtyczek w trybie offline. Nessus oferuje sekcję zarządzania użytkownikami do tworzenia użytkowników Nessus i przyznawania tych przywilejów do przyszłego użytku. Na koniec wprowadzono ustawienia konfiguracji systemu Nessus, takie jak Ustawienia kanału, Ustawienia mobilne i Ustawienia zaawansowane. W następnym rozdziale dowiemy się o skanowaniu infrastruktury IT za pomocą Nessusa.

Skanowanie

Skanowanie luk w zabezpieczeniach lub, innymi słowy, identyfikacja luk w docelowej infrastrukturze jest kluczową czynnością wykonywaną przez każdy skaner luk w zabezpieczeniach, taki jak Nessus. Podczas korzystania z takich skanerów w celu przeprowadzenia oceny narażenia na atak niezwykle ważne jest skonfigurowanie parametru skanowania, w sposób najbardziej efektywny, mając na uwadze utrzymanie infrastruktury docelowej. Pozwoli to uzyskać najbardziej efektywne wyniki skanowania w zoptymalizowanym czasie skanowania. W tym rozdziale przedstawimy, jak skonfigurować Nessus do skanowania luk w zabezpieczeniach. Konfiguracja skanowania w Nessus obejmuje dwa główne etapy, mianowicie konfigurację strategii skanowania i uruchomienie skanowania przy użyciu skonfigurowanej polityki. Kluczowe obszary, które zostaną omówione w tym rozdziale, są następujące:

• Wymagania wstępne skanowania

• Konfiguracja zasad

• Skanowanie poświadczeń i nieskredytowania

• Konfiguracja skanowania

• Skanuj wykonanie i wyniki

Wymagania wstępne skanowania

Pomyślne skanowanie narażenia na atak wymaga prawidłowej konfiguracji Nessus z pewnymi wymaganiami wstępnymi. Zapewni to, że wszystkie zatwierdzenia są udokumentowane, wszystkie kopie zapasowe są na miejscu, a okna skanowania zostały uzgodnione przed skanowaniem. Nessus nie może osiągnąć celu z zaporą ogniową pomiędzy blokującą ruch / pakiety. Zobaczymy teraz najczęstsze wymagania wstępne, które mają zastosowanie do większości skanów Nessus; jednak zachęcam do analizy zgodnie ze swoim środowiskiem skanowania i stosownością organizacji.

Poświadczenia administratora systemu docelowego oparte na skanach

Zawsze zaleca się uruchomienie skanowania poświadczeń w celu uzyskania lepszych wyników; oznacza to, że przed skanowaniem systemu docelowego należy uzyskać referencje systemu docelowego lub

mieć osobę, która może wprowadzić docelowe poświadczenia systemu administracyjnego w GUI Nessus bez udostępniania z Tobą przed rozpoczęciem skanowania. Pomoże to Nessusowi sondować system docelowy coraz częściej, aby odkryć maksymalne luki. Jeśli wykonujesz skanowanie Blackbox, w którym nie będziesz mieć dostępu do poświadczeń, ten szczególny warunek wstępny nie będzie mógł być zastosowany.

Bezpośrednia łączność bez zapory

Zaleca się bezpośrednią łączność Nessus z systemami docelowymi w celu uzyskania lepszych wyników; oznacza to, że nie powinno być zapory ogniowej ani żadnego innego urządzenia blokującego ruch pomiędzy Nessus a systemami docelowymi. Jeśli firewall jest pomiędzy Nessus i systemy docelowe, reguła zapory sieciowej powinna być skonfigurowana tak, aby zezwalała na cały ruch pomiędzy Nessus a systemami docelowymi. Nie zapomnij usunąć lub dezaktywować tej reguły natychmiast po zakończeniu skanowania. Jest to wymagane, ponieważ Nessus generuje wiele szkodliwych pakietów / ruchu do systemów docelowych w celu sondowania luk w zabezpieczeniach. W przypadku, gdy zapora jest zainstalowana, spowoduje to odrzucenie wszystkich takich złośliwych pakietów z systemu docelowego.

Okno skanowania do uzgodnienia

Jest to właściciel systemu docelowego, który może poinformować cię o odpowiednim czasie skanowania luki w zabezpieczeniach w zależności od obciążenia szczytowego i pozaszczytowego systemów docelowych. To odpowiednie okno czasowe nosi nazwę okna skanowania. Jeśli skanujesz systemy produkcyjne, bardzo ważne jest uzgodnienie okna skanowania, najlepiej z właścicielami systemu docelowego. Zaleca się uruchamianie skanów Nessus poza godzinami szczytu, gdy system docelowy ma minimalne obciążenie.

Skanowanie zatwierdzeń i powiązanych prac papierowych

Ważne jest, aby mieć jasną dyskusję z właścicielami systemów docelowych, aby mogli oni zrozumieć wpływ, jaki może mieć miejsce w wyniku złośliwego skanowania, które może być skanem inwazyjnym lub nie. Każda ze stron powinna zrozumieć ryzyko wykonania skanów podatności i wyrazić na to zgodę. Powinno to zostać udokumentowane do celów prawnych. Również umowa o poufności powinna być należycie podpisana przez każdą osobę z zespołu przeprowadzającego ocenę narażenia na atak lub test penetracji.

Tworzenie kopii zapasowych wszystkich systemów, w tym danych i konfiguracji

Przed wykonaniem skanowania ważne jest wykonanie pełnej kopii zapasowej systemu docelowego. Zapewni to, że jeśli coś pójdzie nie tak z maszyną docelową ze względu na skanowanie narażenia na atak, ostatnią kopię zapasową można natychmiast przywrócić, aby przywrócić komputer docelowy. Administratorzy kopii zapasowych powinni upewnić się, że wykonają pełną kopię zapasową, która obejmuje wszystkie dane, konfiguracje, informacje o integracji, kod, uwagi do wydania i specjalne konfiguracje, system IOS i inne.

Aktualizacja wtyczek Nessus

Wtyczki Nessus powinny zostać zaktualizowane o najnowsze definicje przed uruchomieniem skanowania; to sprawi, że Twój Nessus zostanie załadowany wszystkimi najnowszymi sprawdzeniami, aby odkryć najnowsze luki.

Tworzenie strategii skanowania według docelowego systemu operacyjnego i informacji

Strategię skanowania należy skonfigurować przed uruchomieniem skanowania zgodnie z docelowymi systemowymi systemami operacyjnymi i środowiskami. Zasady powinny być odpowiednio skonfigurowane w Nessus. Sposób tworzenia polityki ilustruje następna sekcja tej części.

Konfigurowanie strategii skanowania w celu sprawdzenia zgodności polityki bezpieczeństwa organizacji

Każda organizacja ma własne zasady bezpieczeństwa. Nessus zapewnia możliwość dostosowania polityki skanowania w oparciu o politykę organizacji; na przykład złożoność hasła. Podczas konfigurowania zasad Nessus należy zachować ostrożność, dostosowując zasady haseł zgodnie z zasadami haseł organizacji docelowej. Polityka haseł organizacji może oznaczać, że każde skonfigurowane hasło jest niezgodne, jeśli długość hasła jest mniejsza niż sześć znaków, podczas gdy inne organizacje mogą powiedzieć, że mniej niż osiem znaków jest niezgodnością. Nessus daje Ci elastyczność w dostosowywaniu polityki w oparciu o twoje wymagania przed uruchomieniem skanowania.

Zbieranie informacji o systemach docelowych

W poprzedniej części widzieliśmy różne fazy oceny podatności. Jedna z faz przed skanowaniem zbiera informacje, co jest ponownie warunkiem wstępnym do fazy skanowania. Powinieneś zebrać wszystkie możliwe informacje z publicznych stron internetowych, Internetu i od personelu wewnętrznego (w przypadku skanowania wewnętrznego lub skanowania w trybie greybox). Informacje te są przydatne w celu ulepszenia zasad skanowania Nessus w celu skonfigurowania lub wybrania wymaganych kontroli na podstawie informacji uzyskanych o systemie docelowym, a także pomogą w mapowaniu sieci w celu uwzględnienia adresu IP. Wystarczająca przepustowość sieci do przeprowadzenia skanowania Ważne jest, aby uruchomić skanowanie z dobrą przepustowością sieci; jeśli skanujesz przy niskiej przepustowości, istnieje ryzyko, że pakiety zostaną upuszczone pomiędzy, a twoje skanowanie może zostać przerwane pomiędzy. Aby uniknąć takich sytuacji, zawsze zaleca się uruchomienie skanowania, gdy masz dobrą przepustowość sieci. Pomoże to również w szybkim ukończeniu skanowania.

Obsługa systemu docelowego

Zaleca się, aby administratorzy systemu docelowego lub doświadczeni pracownicy pomocy technicznej analizowali kondycję i wydajność systemów docelowych. Jeśli są dostępne w oknie skanowania, mogą stale monitorować systemy docelowe i alarmy dźwiękowe. Jeśli system nie działa prawidłowo, zatrzymaj skanowanie; lub jeśli coś pójdzie nie tak, system można odzyskać.

Konfiguracja zasad

Konfiguracja zasad jest pierwszym krokiem wykonywanym przed skanowaniem. Prosta konfiguracja reguł oznacza konfigurowanie Nessus z najbardziej zoptymalizowaną konfiguracją do skanowania w oparciu o docelową infrastrukturę. Kluczowe parametry, które można skonfigurować podczas konfigurowania zasad, są następujące:

• Nazwa polisy

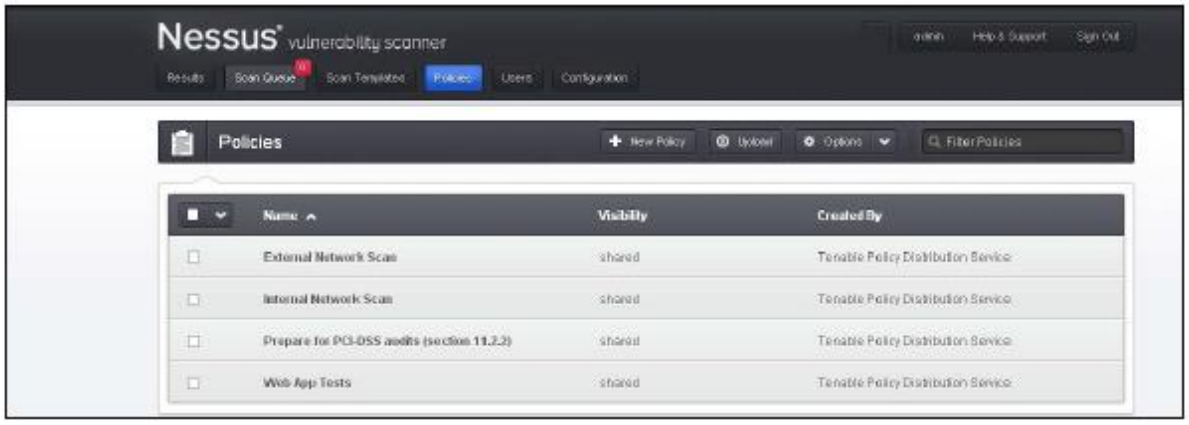
• Wymagany typ skanowania portów

• Wydajność skanowania w kategoriach maksymalnej kontroli na skanowanie równolegle i tak dalej, co decyduje o czasie skanowania

• Możliwość wprowadzania poświadczeń dla infrastruktury skanowanej lokalnie

• Opcja wyboru najbardziej odpowiednich wtyczek

• Opcja preferencji Advance, aby zapewnić różne opcje rozwijane, aby wybrać konfigurację, aby dalej dostrajać politykę w zależności od celu; na przykład sprawdzanie zgodności z bazami danych, sprawdzanie zgodności Cisco IOS i tak dalej



Nessus udostępnia opcję przesłania strategii skanowania, jeśli już ją masz. Dostępna jest również opcja eksportu i kopiowania istniejących zasad. Jeśli masz wiele systemów Nessus, możesz użyć eksportu i przesłać opcje, aby mieć te same zasady we wszystkich systemach Nessus. Możesz również usunąć zasadę, jeśli już jej nie używasz.

Domyślne ustawienia zasad

Domyślnie istnieją cztery domyślne szablony zasad, które są wstępnie załadowane w skanerze Nessus; szablony te umożliwią użytkownikowi rozpoczęcie skanowania przy użyciu tych podstawowych zasad oraz uzyskanie informacji o tym, jak będzie wyglądać typowa konfiguracja zasad lub dostosowywanie ich zgodnie z naszymi wymaganiami. Domyślne zasady są wymienione w następujący sposób:

• Zewnętrzne skanowanie sieci

• Wewnętrzne skanowanie sieci

• Zasady audytu PCI DSS

• Zasady testowania aplikacji WWW

Zasady te są oczywiste. Jeśli chcesz skanować sieć zewnętrzną, użyj zewnętrznej strategii skanowania sieci; jeśli chcesz skanować sieć wewnętrzną, użyj wewnętrznej strategii skanowania sieci; jeśli chcesz przeprowadzić skanowanie do celów PCI DSS, użyj zasad audytu PCI DSS, a na koniec, jeśli chcesz przeskanować aplikację pod kątem luk związanych z aplikacją WWW, takich jak fałszywe żądania dla wielu serwisów, cross-site scripting i zastrzyki SQL, użyj zasad testowania aplikacji WWW. Zaleca się używanie tych domyślnych zasad jako szablonów bazowych w celu tworzenia własnych dostosowanych zasad. Możesz skopiować istniejącą domyślną zasadę i zapisać ją pod nową nazwą zgodnie ze swoimi wymaganiami dotyczącymi skanowania.

Nowe tworzenie polityki

W następnej sekcji zapoznasz się z różnymi opcjami dostępnymi podczas konfigurowania strategii skanowania w Nessus. Aby rozpocząć konfigurowanie nowej zasady skanowania, kliknij opcję + Nowa

polityka na karcie Zasady. W tej zakładce dostępne są cztery opcje ustawień polityki, mianowicie Ustawienia ogólne, Poświadczenia, Wtyczki i Preferencje.

Ustawienia główne

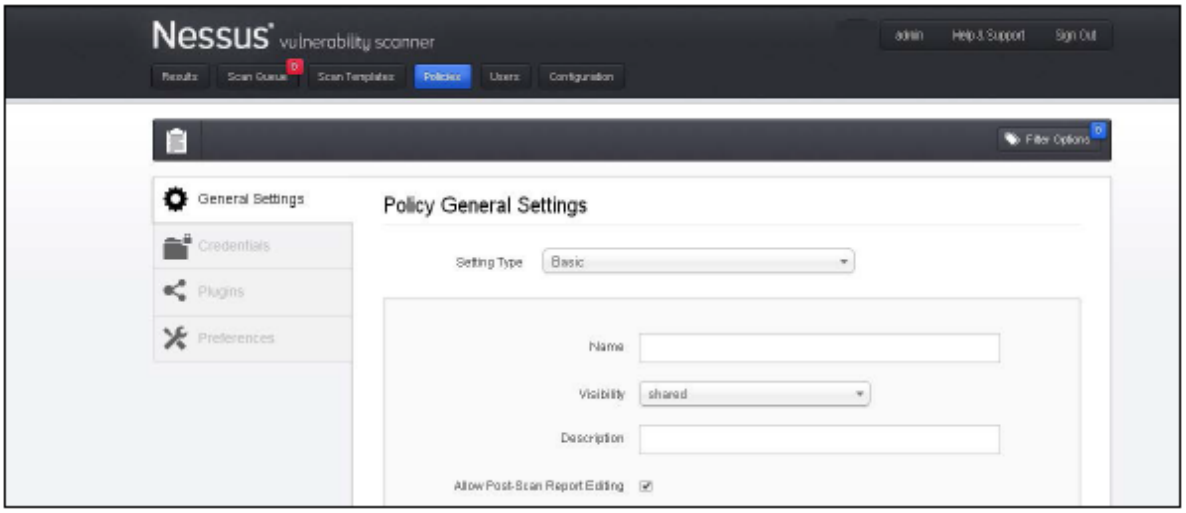
Karta Ustawienia ogólne umożliwia użytkownikowi ustawienie ogólnych informacji, takich jak nazwa skanowania, typ ustawienia skanowania i opis. Ustawienia dostępne w tym ustawieniu są podstawowe, skanowanie portów, wydajność i zaawansowane. Ustawienie Podstawowe obejmuje następujące opcje:

• Nazwa: ta opcja umożliwia przypisanie unikalnej nazwy do zasady

• Widoczność: ta opcja umożliwia udostępnianie zasad innym osobom lub przechowywanie ich do użytku prywatnego; tylko użytkownicy administracyjni mogą udostępniać te zasady

• Opis: ta opcja zapewnia opcję dodania opisu do zasad do wykorzystania w przyszłości; na przykład opis polityki skonfigurowanej do skanowania bazy danych może zostać zaktualizowany w taki sposób, aby użytkownik mógł przywołać i użyć zasady zgodnie z celem, dla którego została ustawiona.

• Zezwalaj na edycję raportu Port-Scan: ta opcja pozwala na usunięcie pozycji ze skanowania portu raportu; zazwyczaj powinno to być wyłączone podczas skanowania z perspektywy zgodności, aby pokazać, że raport nie został zmieniony, jak pokazano na poniższym zrzucie ekranu:



Ustawienie skanowania portu obejmuje następujące opcje:

• Port Scan Range: Określa liczbę portów do przeskanowania. domyślnie wskazuje 4 790 wspólnych portów znalezionych w pliku usług Nessus, WSZYSTKIE oznacza wszystkie 65 5 365 portów. Określony zakres portów można również określić za pomocą symbolu -. Również skanowanie różnych zakresów portów dla TCP i UDP w tej samej zasadzie można wykonać za pomocą t: i u: po którym następuje zakres portów. Inny zakres portów dla TCP / UDP w tej samej zasadzie można określić za pomocą znaku przecinka; na przykład T 90; 1000, U: 350-400.

• Rozważ nieskanowany port jako zamknięty: jeśli ta opcja jest zaznaczona w profilu, Nessus uzna port za zamknięty, jeśli Nessus nie będzie w stanie zeskanować portu.

• Nessus SNMP Scanner: Umożliwia Nessusowi kierowanie na usługę SNMP podczas skanowania; Jest to uzupełniane przez dodanie ustawienia SNMP w sekcji Preferencje zasad, aby uzyskać lepsze wyniki skanowania.

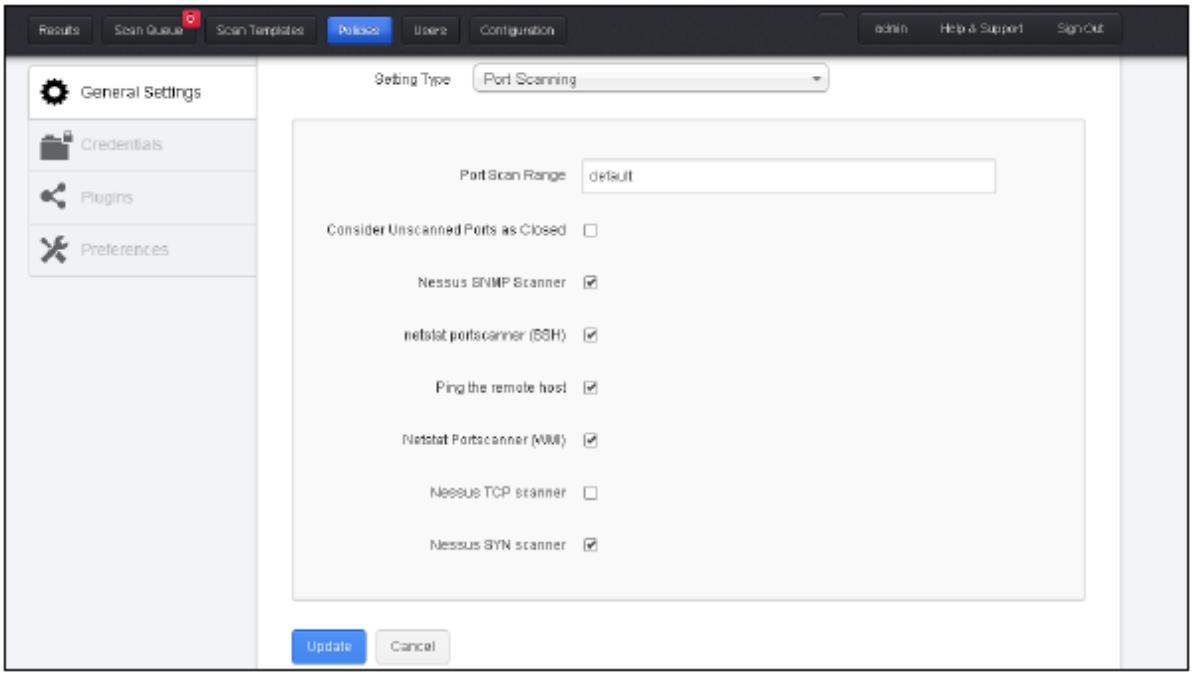
• netstat scanscanner (SSH): Ta opcja używa polecenia netstat dostępnego przez połączenie SSH, aby znaleźć otwarte porty w systemie UNIX. To polecenie wymaga poświadczeń uwierzytelniających.

• Pinguj na zdalnym hoście: ta opcja pomaga znaleźć aktywne systemy poprzez pingowanie portów. W oparciu o odpowiedź ping, Nessus zidentyfikuje ją jako otwartą.

• Netstat Port Scanner (WMI): Ta opcja używa polecenia netstat dostępnego poprzez połączenie WMI w celu znalezienia otwartych portów w systemie Windows. To polecenie wymaga poświadczeń uwierzytelniających.

• Nessus TCP Scanner: Ta opcja to wbudowana opcja Nessus do wyszukiwania otwartych portów TCP.

• Skaner Nessus SYN: Ta opcja wykorzystuje wbudowaną funkcję skanowania SYN w systemie Nessus do identyfikacji otwartego portu.



Ustawienie Wydajność obejmuje następujące opcje:

• Max. Kontrole na host: Ta opcja umożliwia Nessusowi wykonanie maksymalnej liczby kontroli, które Nessus uruchomił jednocześnie na jednym komputerze docelowym.

• Max Hosts Per Scan: Ta opcja umożliwia Nessusowi skanowanie maksymalnej liczby hostów, które Nessus będzie skanował równolegle.

• Network Receive Timeout (sekundy): Ta opcja pokazuje maksymalny czas, przez jaki Nessus będzie czekać na odpowiedź hosta. Ta wartość jest domyślnie ustawiona na 5 sekund i można ją zastąpić wartością wymienioną w konkretnej wtyczce. To może być ustawione na wyższą wartość w przypadku wolnego połączenia.

• Maksymalna liczba jednoczesnych sesji TCP na host: ta opcja ogranicza maksymalną liczbę sesji TCP do pojedynczego komputera docelowego.

• Maksymalna liczba jednoczesnych sesji TCP na skanowanie: Ta opcja ogranicza maksymalną liczbę sesji TCP dla całego okresu skanowania, niezależnie od tego, ile komputerów docelowych jest skanowanych.

• Zmniejsz równoległe połączenia z ograniczeniami: Ta opcja umożliwia Nessusowi zmniejszenie liczby pakietów wysyłanych w sieci, aby uniknąć zadławienia przepustowości sieci.

• Użyj wykrywania zatorów jądra (tylko Linux): Ta funkcja jest dostępna dla skanerów Nessus zainstalowanych w systemie Linux. Po włączeniu tej opcji Nessus będzie monitorował procesor i inne wewnętrzne parametry i odpowiednio zmodyfikuje wykorzystanie zasobów.

Ustawienie Zaawansowane obejmuje następujące opcje:

• Bezpieczne kontrole: ta opcja wyłącza wtyczki, które mogą mieć wpływ na komputer docelowy. Ważne jest, aby wybrać tę opcję, aby przeprowadzić bezpieczne skanowanie.

• Silent dependencies: Ta opcja, jeśli jest zaznaczona, zawiera listę zależności, których nie ma w raporcie.

• Szczegóły skanowania dziennika na serwerze: ta opcja rejestruje dodatkowe informacje w pliku

Dziennik serwera Nessus; pomaga to ocenić skanowanie z perspektywy wtyczki, to znaczy pomaga określić, czy konkretna wtyczka została uruchomiona i użyta.

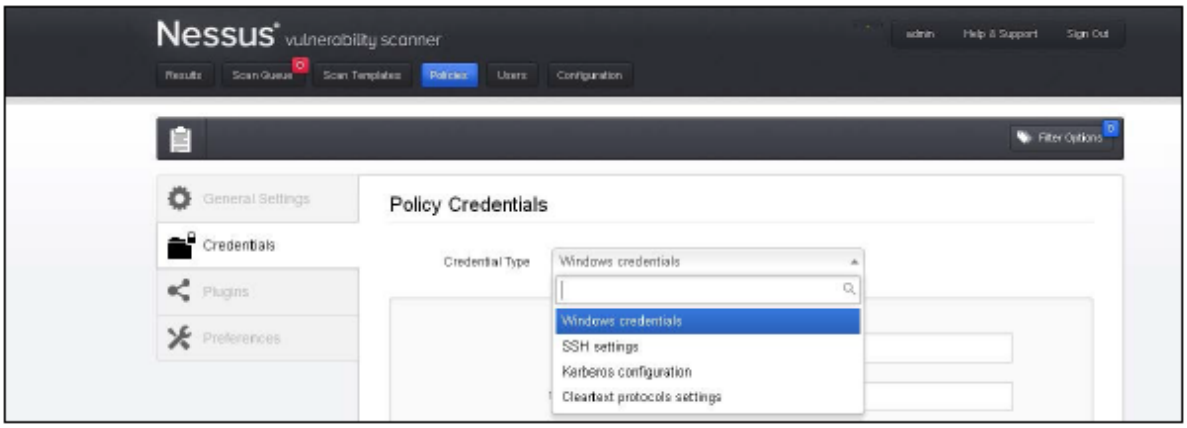
• Zatrzymaj skanowanie hosta przy rozłączaniu: jeśli ta opcja jest włączona, Nessus zatrzyma skanowanie komputera docelowego, jeśli uzna, że komputer docelowy nie odpowiada na wysłane pakiety. Może się to zdarzyć z jakiegoś powodu, na przykład gdy maszyna docelowa jest wyłączona lub ruch na maszynach docelowych jest zablokowany.

• Unikaj kolejnych skanów: Listę hostów objętych skanowaniem można podać Nessus; jeśli ta opcja jest wybrana, Nessus przeprowadzi skanowanie w sposób losowy, a nie sekwencyjnie.

• Wyznacz hosty na podstawie ich nazwy DNS: Ta opcja włącza użycie nazwy hosta w raporcie przygotowanego skanowania postów zamiast adresu IP komputera docelowego.

Skrypt z potwierdzeniem

Nessus oferuje funkcję do przeprowadzania uwierzytelnionych lub uwierzytelnionych skanów. Dzięki tej opcji Nessus może zalogować się do lokalnego systemu, aby znaleźć luki na poziomie systemu lokalnego, takie jak brakujące łatki i ustawienia systemu operacyjnego. Zazwyczaj luki te nie są wyróżniane przez Nessus w przypadku niesklarowanego skanowania w sieci. W skrócie, opcja skanowania poświadczeń pomaga znaleźć lokalne luki w zabezpieczeniach systemu po zalogowaniu się do systemu przy użyciu dostarczonych poświadczeń. Skanowanie poświadczeń wykonuje te same operacje, co lokalny użytkownik systemu; zależy to od poziomu dostępu przyznanego lokalnemu kontu użytkownika używanemu przez Nessus. Poniższy zrzut ekranu pokazuje opcję konfiguracji skanowania poświadczeń dla poświadczeń systemu Windows, ustawień SSH, konfiguracji Kerberos i ustawień protokołu Cleartext:



Opcja poświadczeń systemu Windows

W ramach opcji poświadczeń systemu Windows Nessus przechwycił szczegóły konfiguracji SMB (Server Messaging Block). SMB jest protokołem wymiany plików, który pomoże Nessusowi odkryć lokalne luki w systemie Windows. Jest zawsze zalecane używać konta z uprawnieniami administratora, aby uzyskać jak najlepsze wyniki skanu uwierzytelnionego.

Nazwy użytkowników Windows, hasła i domeny

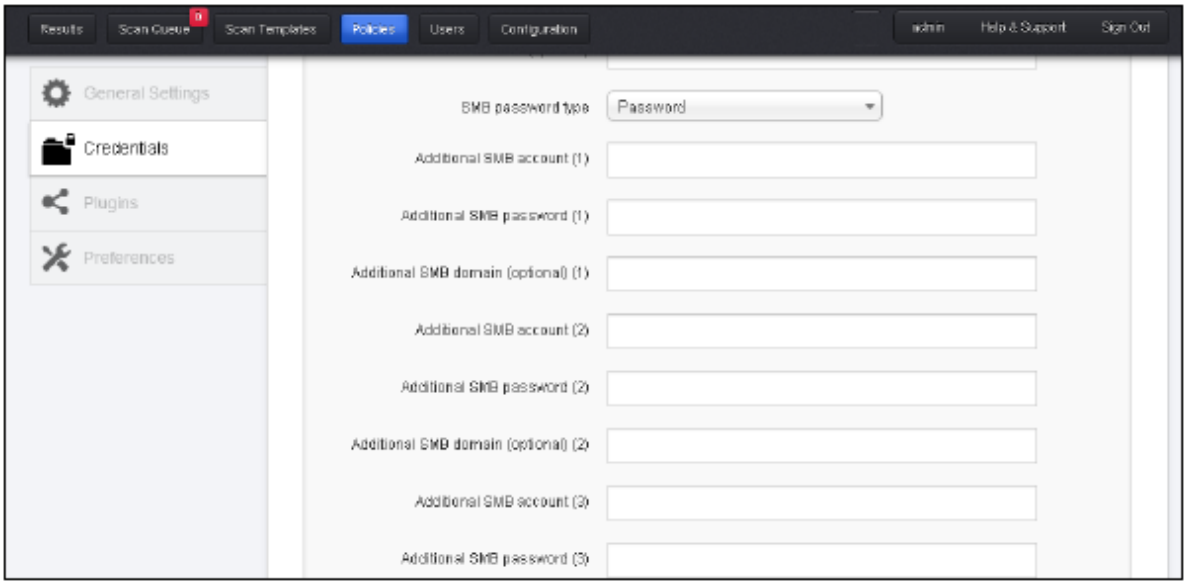
Pole domeny SMB jest opcjonalne i Nessus będzie mógł zalogować się przy użyciu poświadczeń domeny bez tego pola. Nazwa użytkownika, hasło i opcjonalna domena odnoszą się do konta, na którym znajduje się komputer docelowy. Nawet jeśli poświadczenia nie są używane, Nessus podejmie próbę zalogowania się do serwera Windows z następującymi kombinacjami:

• Administrator bez hasła

• Losowa nazwa użytkownika i hasło do testowania kont gości

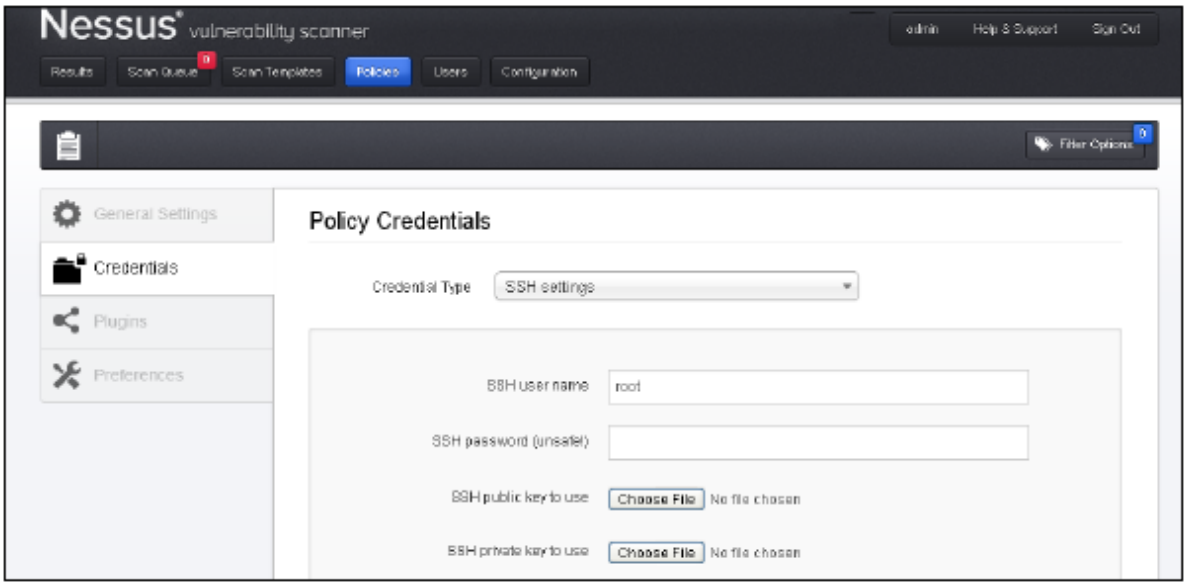
• Brak nazwy użytkownika lub hasła do testowania sesji zerowych

Nessus obsługuje kilka różnych metod uwierzytelniania dla systemów Windows. Każda z tych metod przyjmuje nazwę użytkownika, hasło i nazwę domeny (czasami opcjonalne w celu uwierzytelnienia). Opcja ustawienia pozwala określić użycie opcji NTLM lub Kerberos



Opcja ustawień SSH

Opcja ustawień SSH z rozwijanego menu umożliwia wprowadzanie danych uwierzytelniających do skanowania systemów UNIX. Poświadczenia służą do uzyskiwania informacji lokalnych ze zdalnych systemów UNIX. Zostanie wyświetlone pole do wpisania nazwy użytkownika SSH dla konta aby przeprowadzić kontrole docelowego systemu UNIX wraz z hasłem SSH lub kluczem publicznym SSH i parą kluczy prywatnych. Istnieje również pole do wpisania hasła dla klucza SSH, jeśli jest ono wymagane. Najbardziej efektywne skanowane poświadczenia to te, w których dostarczone poświadczenia mają uprawnienia root. Ponieważ wiele witryn nie zezwala na zdalne logowanie jako root, użytkownicy Nessus mogą wywoływać su, sudo, su + sudo lub dzdo z oddzielnym hasłem dla konta, które zostało skonfigurowane, aby mieć uprawnienia su lub sudo. Jeśli plik SSH known_hosts jest dostępny i dostarczony jako część strategii skanowania, Nessus spróbuje zalogować się tylko do hostów w tym pliku. Preferowany port SSH można ustawić bezpośrednio na Nessus do łączenia się z SSH, jeśli działa na porcie innym niż 22. Jeśli do eskalacji uprawnień ma być używane konto inne niż root, można o tym wspomnieć w opcji z uprawnieniami do podwyższania z opcją. Najlepsze praktyki zalecają używanie kluczy SSH do uwierzytelniania zamiast haseł SSH. Zapewni to, że ta sama nazwa użytkownika i hasło używane do inspekcji serwera SSH nie są używane do próby zalogowania się do systemu, który może nie być pod Twoją kontrolą.

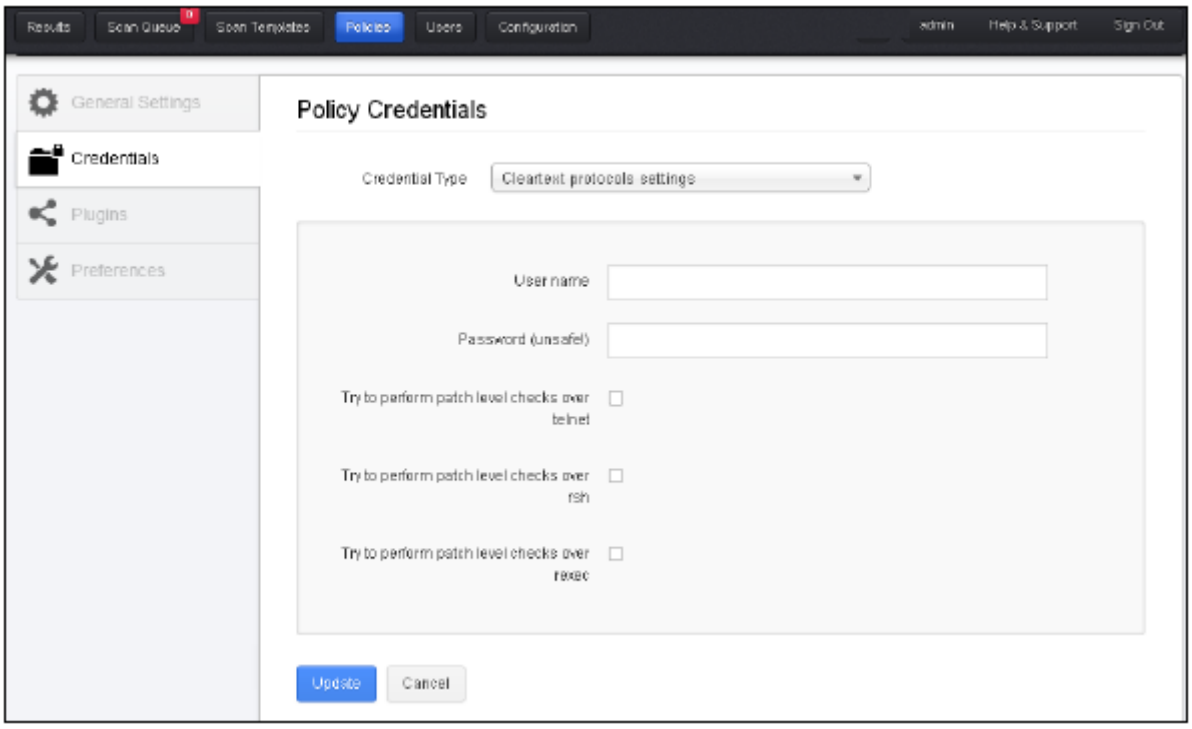


Opcja konfiguracji Kerberos

Opcja konfiguracji Kerberos umożliwia określenie poświadczeń za pomocą kluczy Kerberos z systemu zdalnego.

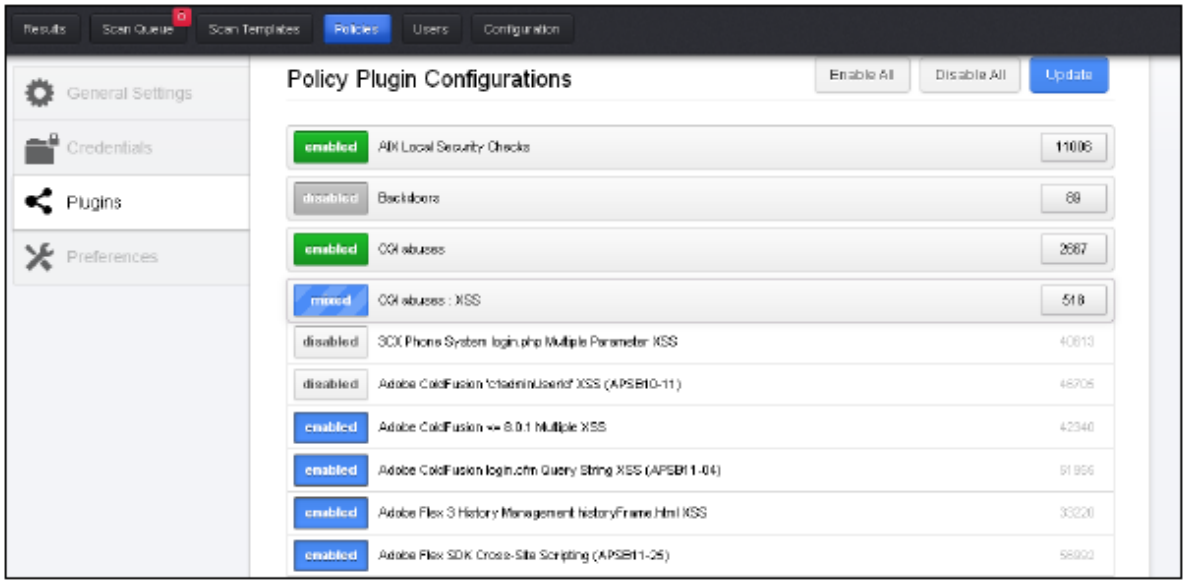
Opcja ustawień protokołu tekstowego Cleartext

W przypadku, gdy opcja bezpiecznego szyfrowania nie jest dostępna do skanowania poświadczeń, Nessus oferuje funkcję skanowania przez protokół jawnego tekstu dla telnetu, rsh, rexec. W tej opcji hasło porusza się niesatysfakcjonująco w kanale Cleartext. Ta opcja pozwala również sprawdzić poziom poprawek.



Wtyczki

Wtyczki są plikami używanymi przez Nessus do sprawdzania podatności. Te wtyczki są regularnie aktualizowane z najnowszymi sprawdzeniami luk w zabezpieczeniach, gdy tylko będą dostępne. Wtyczki są podzielone na rodziny produktów, aby umożliwić dokładne i skuteczne grupowanie podobnych wtyczek. W ten sposób, wybierając odpowiednią rodzinę wtyczek, dużą liczbę odpowiednich / niepoprawnych wtyczek można włączyć lub wyłączyć wydajnie i przy minimalnych kliknięciach. Ponadto, Nessus wydaje nowe wtyczki, gdy pojawiają się nowe luki. Poniższy zrzut ekranu pokazuje, jak będzie wyglądać okno konfiguracji wtyczek Policy:



Poniższa tabela przedstawia kolor wtyczki i ich znaczenie. Zasadniczo jest to liczba wtyczek włączonych z konkretnej rodziny wtyczek.

Znaczenie Kolorów

Zielony : Oznacza, że wszystkie wtyczki w rodzinie są włączone.

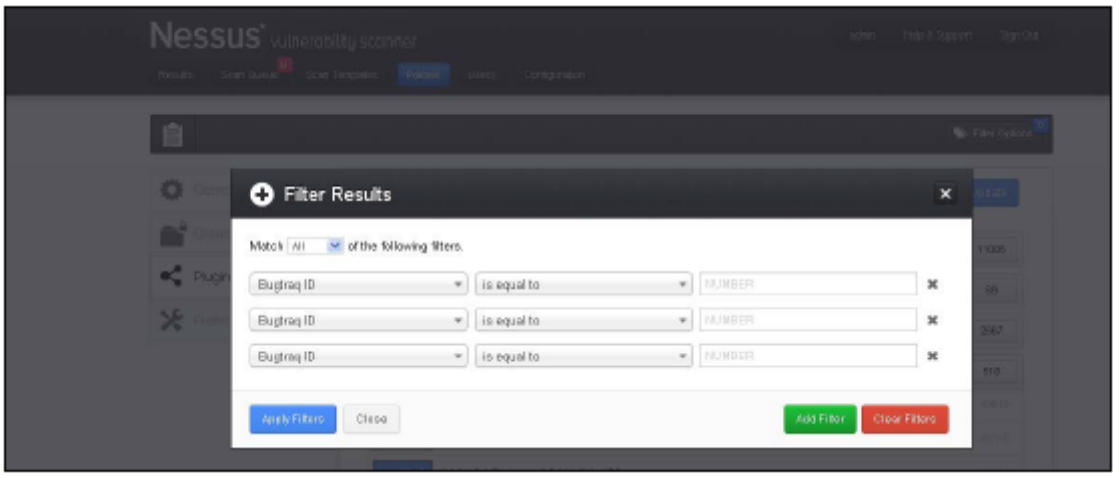
Szary : Oznacza, że wszystkie wtyczki w rodzinie są wyłączone.

Niebieski : To reprezentuje mieszany wybór, w którym w rodzinie wtyczek niektóre wtyczki są wybrane, a niektóre odznaczone.

Szczegóły wybranych wtyczek będą również reprezentowane w raporcie na podstawie znalezionej luki z powodu konkretnej wtyczki.

Filtrowanie

Na górze strony Wtyczki dostępna jest opcja filtrowania. Ta opcja umożliwia wybranie wtyczek, które są włączane za pomocą zasady, poprzez zastosowanie filtrów.



Filtry można dodawać i usuwać za pomocą odpowiednio przycisku ADD Filter i CLEAR Filters. Nessus daje również opcję Dopasuj z Dowolnym i Wszystkim. Opcja Any oznacza, że którakolwiek z podanych opcji filtrowania jest spełniona. Opcja Wszystkie oznacza, że należy podać cały wymieniony warunek filtra. Za pomocą opcji filtrowania można wybrać najbardziej zoptymalizowane wtyczki skanowania. Zaleca się także, aby najpierw wyświetlić wszystkie filtry i zastosować zasadę przy użyciu opcji filtrowania. Szczegóły różnych rodzin wtyczek i kryteriów filtrowania można znaleźć w dokumentacji Tenable:

Rodzina "Denial of Service" zawiera kilka wtyczek, które mogą powodować przerwy w sieci, jeśli opcja "Safe Checks" nie jest włączona, ale zawiera pewne przydatne kontrole, które nie spowodują szkody. Rodzina "Denial of Service" może należy używać w połączeniu z "Bezpiecznymi kontrolami", aby upewnić się, że potencjalnie niebezpieczne wtyczki nie są uruchomione. Zaleca się jednak, aby rodzina "Denial of Service" nie była używana w sieci produkcyjnej. "

Preferencje

Preferencje to głębsze ustawienia polityki Nessus, które mają charakter dynamiczny. Dynamiczne oznacza, że opcje w menu rozwijanym służące do konfigurowania ustawień preferencji mogą się różnić w zależności od wtyczek i licencji pliku danych. Te ustawienia może wybrać osoba, która tworzy strategię skanowania w zależności od wymaganie systemu docelowego. Na przykład, jeśli planujesz przeskanować bazę danych, podczas tworzenia polityki wybierz Ustawienia bazy danych z menu rozwijanego Preferencje. To szczególne ustawienie umożliwia wpisanie szczegółów bazy danych z

danymi uwierzytelniającymi bazy danych w celu dalszego sondowania bazy danych. Umożliwi to skanowanie Nessus w celu wykrycia większej podatności. Polecam stronę Nessus, http://www.tenable.com, aby uzyskać najnowsze ustawienia i ich objaśnienia.

Konfiguracja skanowania

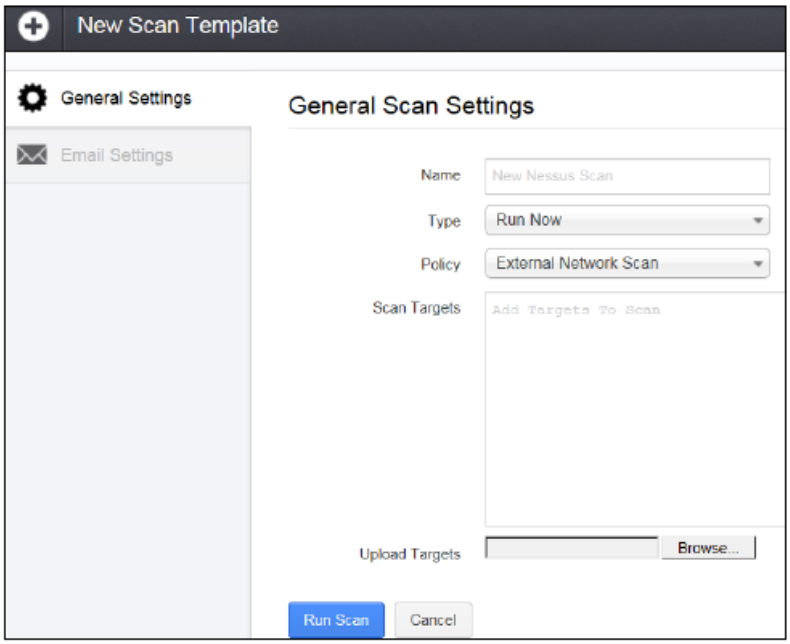
Sekwencyjne czytanie tego tekstu jest wymagane dla czytelników przed przejściem do tej sekcji. W poprzednich sekcjach wyjaśniliśmy wymagania wstępne, którymi należy się zająć przed uruchomieniem skanowania. Omówiono także sposób konfigurowania i dostosowywania polityki skanowania zgodnie z polityką bezpieczeństwa organizacji docelowych oraz różnice między uwierzytelnieniem a skanowaniem bez konieczności podawania danych.

Konfigurowanie nowego skanowania

Sposób inicjowania i uruchamiania skanowania jest zilustrowany w tej sekcji. Aby zainicjować skanowanie, zakładamy, że zostały spełnione wymagania wstępne skanowania, które zostały wcześniej wymienione w tej części. Aby rozpocząć skanowanie, zaloguj się do Nessus, używając swojego poświadczenia Nessusa i kliknij Skanuj kolejkę z najwyższego paska Nessus. Pasek kolejki skanowania ma dwa przyciski: Nowe skanowanie i Opcje, które jest menu rozwijanym, które zapewnia opcje wznowienia skanowania, wstrzymania skanowania lub zatrzymania uruchomionego skanowania. Kliknij przycisk Nowe skanowanie, aby rozpocząć nowe skanowanie. To ma dwie opcje na panelu po lewej stronie, jedną dla ustawień ogólnych i drugą dla ustawień e-mail.

Ustawienia główne

Ustawienia ogólne to ustawienia nowego skanowania, takie jak nazwa skanowania, czy chcesz go teraz uruchomić, czy zapisać jako szablon, którego skanowanie można uruchomić później, albo zaplanować skanowanie pożądany czas i na którym skanowanie to będzie automatycznie ma miejsce. Możesz także wybrać politykę, której chcesz użyć do tego nowego skanowania z menu rozwijanego zasad. Jest to również miejsce, w którym podajesz adresy IP, które chcesz przeskanować. Zapewnia to również możliwość przesłania pliku, który zawiera listę adresów IP, które mają zostać przeskanowane podczas tego nowego skanowania.



Poniższa tabela opisuje ustawienia podane na poprzednim zrzucie ekranu:

Ogólne ustawienia skanowania : Opis

Nazwa : Jak chcesz nazwać swoje skanowanie

Wpisz : To ma następujące trzy opcje w rozwijanym menu:

- Uruchom teraz: Jeśli chcesz teraz uruchomić skanowanie
- Szablon: Jeśli chcesz zapisać skan jako szablon, że możesz uruchomić później
- Zaplanowane: Jeśli chcesz zaplanować skanowanie dla żądanego czas, skanowanie rozpocznie się automatycznie

Polityka : To jest ponownie rozwijane menu, które zawiera listę wszystkich Nessus zeskanuj zasady. Dyskutowaliśmy na temat tworzenia polityki w poprzedniej sekcji. Te zasady powinny być wybrane z domeny rozwijane menu, które zostanie użyte do skanowania.

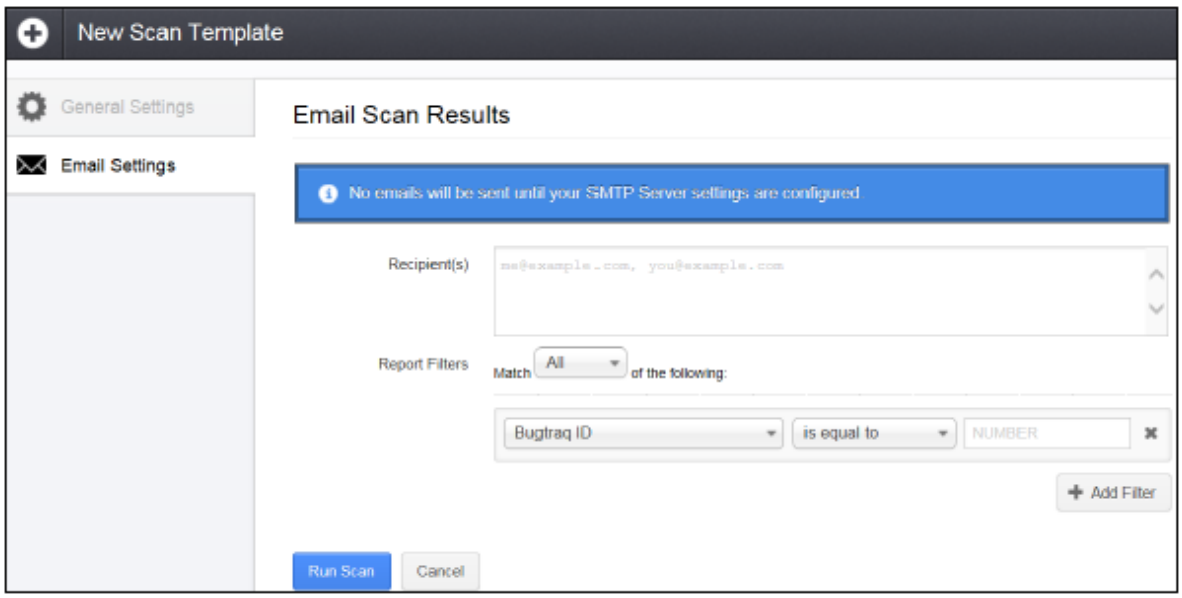
Cele skanowania : Wszystkie adresy IP, które muszą zostać zeskanowane, powinny być wymienione tutaj.

Przesyłanie celów: Jeśli masz plik tekstowy, który ma listę adresów IP do skanowania, to samo można sprowadzić tutaj w Nessus.

Na końcu masz przycisk Run scan, który zainicjuje skanowanie.

Ustawienia poczty e-mail

Ustawienia e-mail można skonfigurować do skanowania, jeśli Nessus jest skonfigurowany z serwerem SMTP. Służy do wysyłania e-mailem wyników skanowania automatycznie po zakończeniu. Identyfikatory e-mail odbiorców można wprowadzić tutaj w polu wejściowym Odbiorcy. Można również skonfigurować filtry raportów. W takim przypadku wyniki zostaną przesłane pocztą e-mail do adresatów, jeśli filtr raportu zostanie dopasowany, jak pokazano na poniższym zrzucie ekranu:



Poniższa tabela opisuje ustawienia podane na poprzednim zrzucie ekranu:

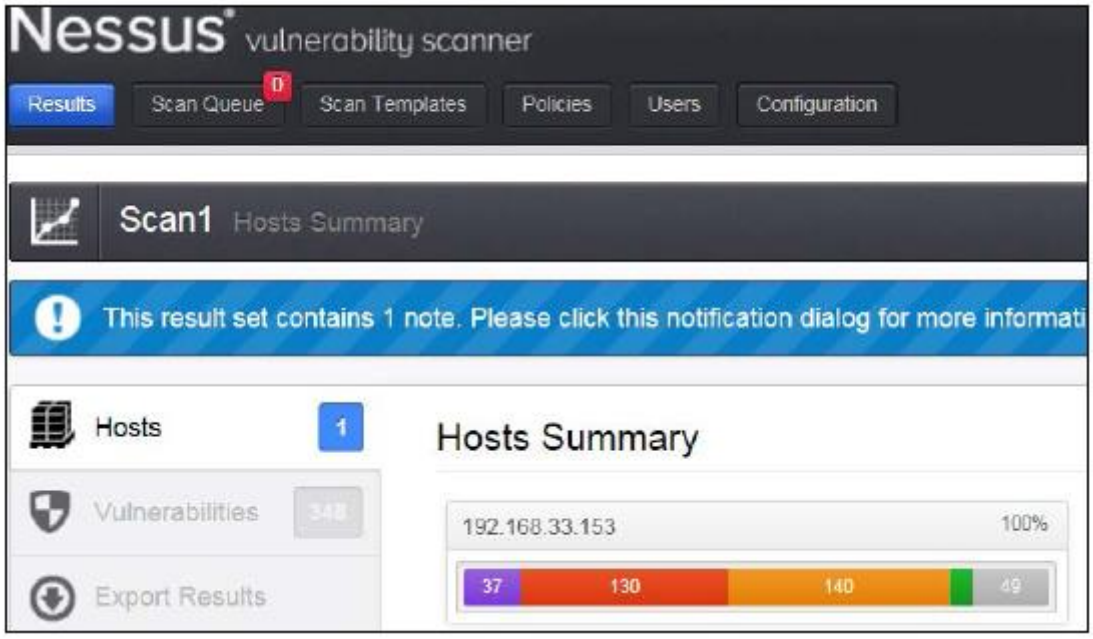
Wynik skanowania poczty e-mail : Opis

Odbiorcy : Do których chcesz wysłać zautomatyzowane wiadomości e-mail z wynikami skanowania, podaj adresy e-mail odbiorców, którzy mają być tu wysłani.

Filtry raportu : Filtry raportów można tutaj skonfigurować, aby pasowały do określonego warunku lub filtra. Jeśli to się zgadza, automatyczna wiadomość e-mail dotycząca wyniku wywoła odbiorców. Na końcu masz przycisk Uruchom skanowanie, który zainicjuje skanowanie.

Wykonanie skanowania i wyniki

W poprzedniej sekcji widzieliśmy, jak należy rozpocząć skanowanie. Po kliknięciu przycisku Uruchom skanowanie nastąpi skanowanie. Wyniki ukończonych skanów można zobaczyć na karcie Wyniki. Podwójne kliknięcie wyniku skanowania otworzy szczegółowy widok konkretnego wyniku skanowania. Ma trzy różne karty, a mianowicie hosty, luki w zabezpieczeniach i wyniki eksportu. Pod zakładką Hosty można zobaczyć podsumowanie hosta. Ma to wskaźnik ważności (krytyczny, wysoki, średni, niski i informacyjny) podatności. Poniższy zrzut ekranu pokazuje, że host jest skanowany, co ma 37 krytycznych, 130 wysokich, 140 średnich, 0 niskich i 49 informacyjnych luk w zabezpieczeniach:



Następna zakładka to Vulnerabilities; pokazuje to podsumowanie luk w zabezpieczeniach wraz z ryzykiem dotkliwości każdej luki. Podwójne kliknięcie na lukę spowoduje wyświetlenie szczegółowej informacji o tej luce, która zawiera szczegółowe streszczenie, opis, rozwiązanie, linki do luk w zabezpieczeniach, informacje o wtyczkach, informacje o zagrożeniach, informacje o usterkach, informacje o referencjach, dane wyjściowe wtyczki itd. W widoku szczegółowym dostępna jest także opcja zmiany wagi ryzyka. Ostatnia zakładka to Wyniki eksportu; zapewnia to opcję eksportu raportu wyników skanowania Nessus w różnych formatach, takich jak HTML, PDF i CSV. Można również wybrać, co jest wymagane do uwzględnienia w raporcie z następujących opcji:

- Podsumowanie gospodarza i podsumowanie
- Luki w zabezpieczeniach hosta
- Luki w zabezpieczeniach za pomocą wtyczki

• Wykonawca kontroli zgodności

• Sprawdzenie zgodności

Jedną lub wiele z tych opcji można wybrać w zależności od wymagań. Kilka sekcji tego rozdziału zostało przywołanych w materiałach edukacyjnych dostępnych na stronie internetowej Nessus: http://www.tenable.com.

Podsumowanie

W tej części dowiedzieliśmy się, jak skonfigurować Nessus do skanowania luk w zabezpieczeniach. Konfiguracja skanowania w Nessus obejmuje dwa główne etapy, mianowicie konfigurację strategii skanowania i uruchomienie skanowania przy użyciu skonfigurowanej polityki. Przeprowadzono również skanowanie wymagań wstępnych, w tym decydowania o zakresie skanowania, uzyskaniu zatwierdzenia na miejscu, decydowaniu o oknie skanowania, aktualizowaniu wtyczek, tworzeniu kopii zapasowej, właściwym otwarciu dostępu do sieci, identyfikacji punktu kontaktu i decydowaniu o skanowaniu poświadczeń lub nieskredytowania. omówione. Wśród wymagań wstępnych pierwszym kluczowym krokiem jest skonfigurowanie polityki skanowania, która będzie zawierać cztery domyślne szablony zasad (zewnętrzny, wewnętrzny, PCI DSS i aplikacja internetowa). Nessus oferuje również opcję tworzenia niestandardowych zasad przy użyciu opcji Nowa zasada. Dostępne są cztery opcje ustawień podczas tworzenia nowej polityki, a mianowicie Ustawienia ogólne i Ustawienia zaawansowane (w tym nazwa zasady, widoczność, opcje skanowania portów, wydajność skanowania i bezpieczne kontrole), skan uwierzytelniony (z tą opcją Nessus jest w stanie zalogować się do systemu lokalnego, aby znaleźć lokalny poziom systemu luki w zabezpieczeniach, takie jak brakujące poprawki i ustawienia systemu operacyjnego). Opcje dostępne w celu dodania danych uwierzytelniających dla różnych infrastruktur wyjaśniono w tej sekcji, Wtyczki (obejmuje wybór odpowiedniej rodziny sprawdzania bezpieczeństwa na podstawie rodzaj infrastruktury objętej skanowaniem, taki jak Windows, Cisco i baza danych). Wtyczkę Denial of Service należy unikać, o ile nie zostaniesz o to poproszony, ponieważ może to spowodować przestoje. Menu Preferencje obejmuje zaawansowany i głębszy poziom ustawień, które należy skonfigurować zgodnie z skanowaną infrastrukturą. Po utworzeniu polityki następuje faktyczne skanowanie; kluczowe czynności obejmują wybór nowego skanu, opcje ustawień ogólnych, które obejmują nazwę, typ i strategię skanowania, które mogą być domyślne lub dostosowane, oraz skanowanie celów, w tym adres IP infrastruktury, która ma zostać przeskanowana (można użyć pliku tekstowego za to samo). Wyjaśniono również, w jaki sposób wyniki skanowania można wysłać pocztą po zakończeniu skanowania. Na koniec wyjaśniono w skrócie opcję pobierania wyniku skanowania z karty Wynik. W następnym rozdziale dowiemy się o przeprowadzaniu analizy wyników skanowania, która obejmie analizę fałszywie pozytywną, analizę podatności na zagrożenia, wykorzystanie uciążliwości i tak dalej.

Opcje raportowania

Łatwe do zrozumienia i imponujące raportowanie jest kluczem do udanej oceny podatności. Bardzo ważne jest, aby wiedzieć, kto jest docelową publicznością, zanim napiszesz raport Ocena podatności. W większości przypadków raport oceny podatności będzie czytany przez różne grupy i przez odbiorców o różnym poziomie zaawansowania. Niektóre z nich mogą mieć bardzo silną wiedzę na temat terminów technicznych, a niektóre mogą nie rozumieć niczego technicznego; dlatego ważne jest, aby w raporcie znalazła się odpowiednia kombinacja materiałów, która dotyczy zarówno odbiorców technicznych, jak i nietechnicznych. Ważne jest wygenerowanie kompleksowego raportu dotyczącego oceny narażenia na atak, aby inni wiedzieli o lukach znalezionych w formacie tekstowym, aby był łatwy do zrozumienia dla docelowych czytelników. W tej części dowiesz się, jak napisać skuteczny raport o luce. Kluczowe obszary, które zostaną omówione w tym rozdziale, są następujące:

• Generowanie raportów

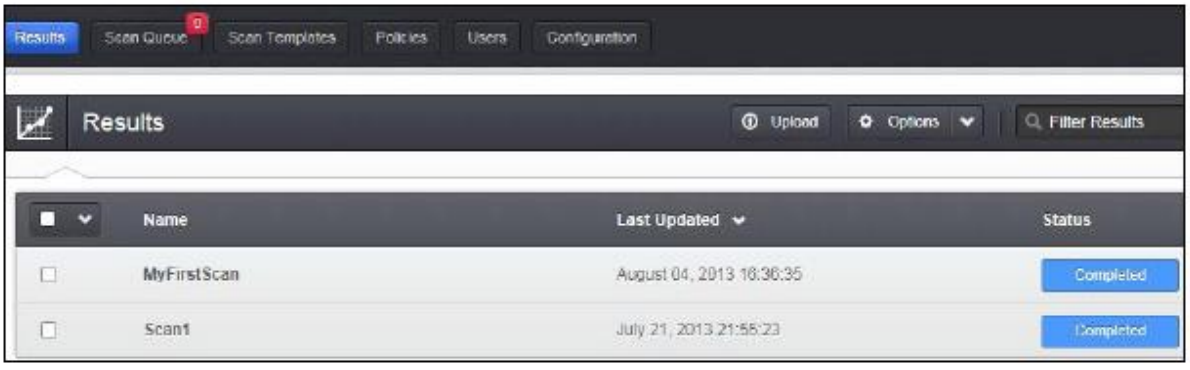
• Zgłoś dostosowanie

• Raportuj automatyzację

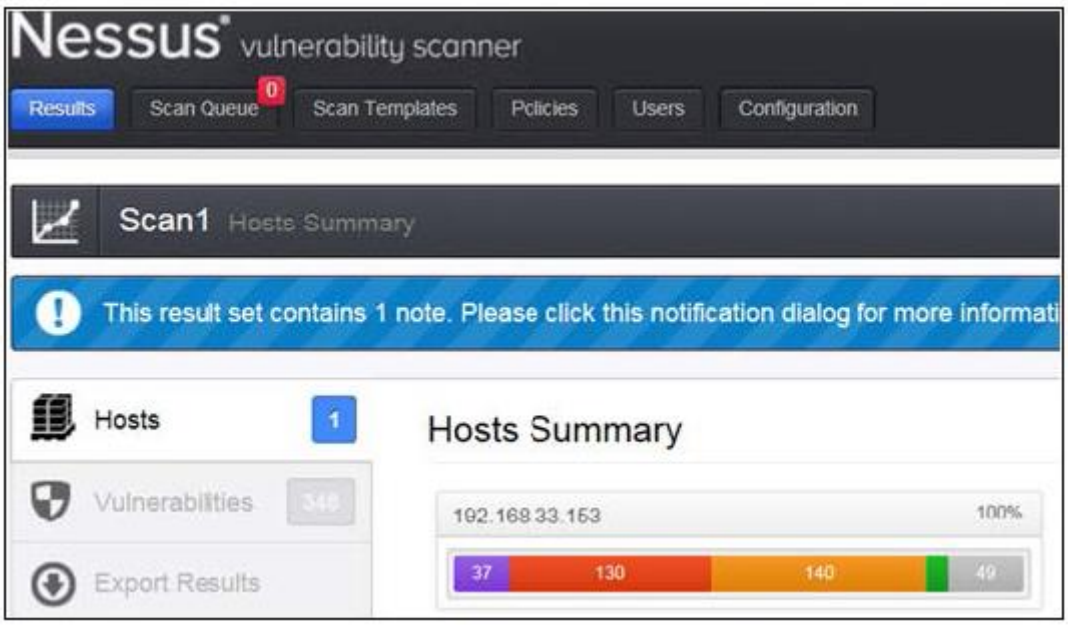
Raport oceny podatności Co należy uwzględnić, a czego nie uwzględnić w raporcie oceny podatności na ataki lub testowanie penetracji, zawsze było przedmiotem dyskusji. Ważne jest, aby zrozumieć, że ocena podatności nie osiągnie celu bez dobrego raportu. Raport powinien być napisany z myślą o odbiorcach. W większości przypadków raporty oceny podatności są przekazywane różnym zespołom w dużym przedsiębiorstwie, z różnym poziomem zrozumienia raportu. Specjalista ds. Zarządzania nie jest zainteresowany szczegółową analizą każdej luki. Wolą raczej szybko zobaczyć podsumowanie oceny jako zrzut ekranu z liczbą zidentyfikowanych luk w zabezpieczeniach, sklasyfikowanych według ich wagi; można to lepiej uchwycić w graficznej reprezentacji wraz z tekstem w sekcji pokazującej krytyczne / wysokie / średnie / niskie nasilenie luki w zabezpieczeniach. Z drugiej strony, osoba techniczna chciałaby uzyskać więcej szczegółów technicznych dotyczących raportu o luce w zabezpieczeniach i procedury krok po kroku, w przypadku gdy jest to raport z testu penetracji; to pomoże im odtworzyć lukę. Osoba techniczna również chciałaby otrzymywać rekomendacje o tym, jak naprawić lukę. Nessus generuje raport z pomyślnego skanowania, który zawiera szczegółowe informacje na temat każdej luki. W zależności od odbiorców raport można dostosować. Zaleca się wybranie i zastosowanie odpowiednich filtrów do decydowania o treści raportu, jeśli skanowanie jest wykonywane bardzo często i za każdym razem ma być generowany raport w tym samym formacie. Konsultanci bezpieczeństwa mogą tego nie chcieć, ponieważ otrzymują różne wymagania dotyczące raportowania od różnych klientów.

Generowanie raportów Nessus

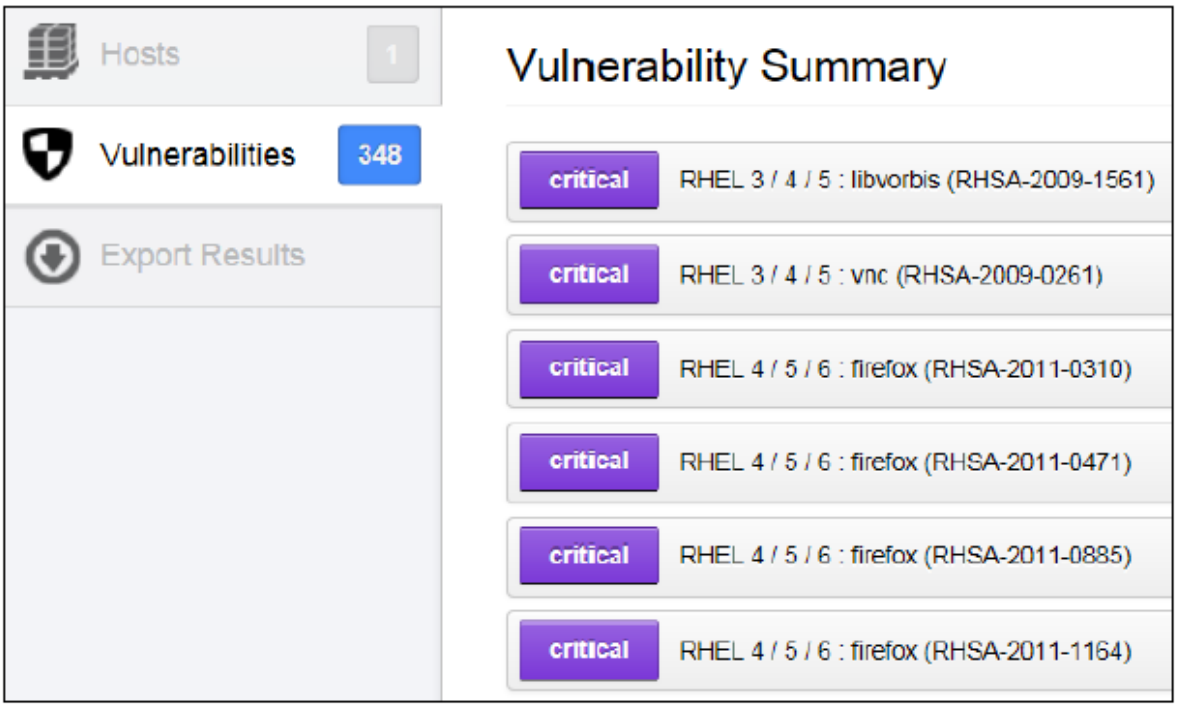
Nessus generuje raporty dla wszystkich ukończonych skanów, które można wyeksportować do systemu lokalnego i umożliwia generowanie raportów z poprzednich skanów. Wiele formatów raportu jest dostępnych w Nessusie, które można wybrać podczas generowania raportu. Po zakończeniu skanowania Nessus przechowuje wyniki skanowania. Nessus przechowuje wyniki skanowania w zakładce Wyniki, jak pokazano na poniższym zrzucie ekranu:



Podwójne kliknięcie wyniku skanowania spowoduje wyświetlenie szczegółowego widoku danego wyniku skanowania. Ten widok ma trzy różne karty: hosty, luki w zabezpieczeniach i wyniki eksportu. Pod zakładką Hosty można zobaczyć podsumowanie hosta. Ma to znaczenie (krytyczne, wysokie, średnie, niskie i informacyjne) liczby luk w zabezpieczeniach. Poniższy zrzut ekranu pokazuje, że host został zeskanowany, a ma trzydzieści siedem krytycznych, sto trzydzieści wysokie, sto czterdzieści średnie, zero niskie i czterdzieści dziewięć słabości informacyjne:



Następna zakładka to karta Vulnerabilities; pokazuje to podsumowanie podatności na zagrożenia wraz z zagrożeniem dla każdej luki. Podwójne kliknięcie na lukę prowadzi do szczegółowego widoku tej luki, która szczegółowo opisuje streszczenie, opis, rozwiązanie, linki do luk w zabezpieczeniach, informacje o wtyczkach, informacje o zagrożeniach, informacje o usterkach, informacje o referencjach, dane wyjściowe wtyczki itd. W widoku szczegółowym dostępna jest także opcja zmiany wagi ryzyka. Poniższy zrzut ekranu pokazuje widok podsumowania narażenia na atak:



Ostatnia zakładka to Export Results; zapewnia to opcję eksportu raportu wyników skanowania Nessus w różnych formatach, takich jak HTML, PDF i CSV. Możesz również wybrać, co należy uwzględnić w raporcie, korzystając z następujących opcji:

• Podsumowanie hostów (wykonawczy): ta opcja wyeksportuje raport zawierający podsumowanie wykrytych luk

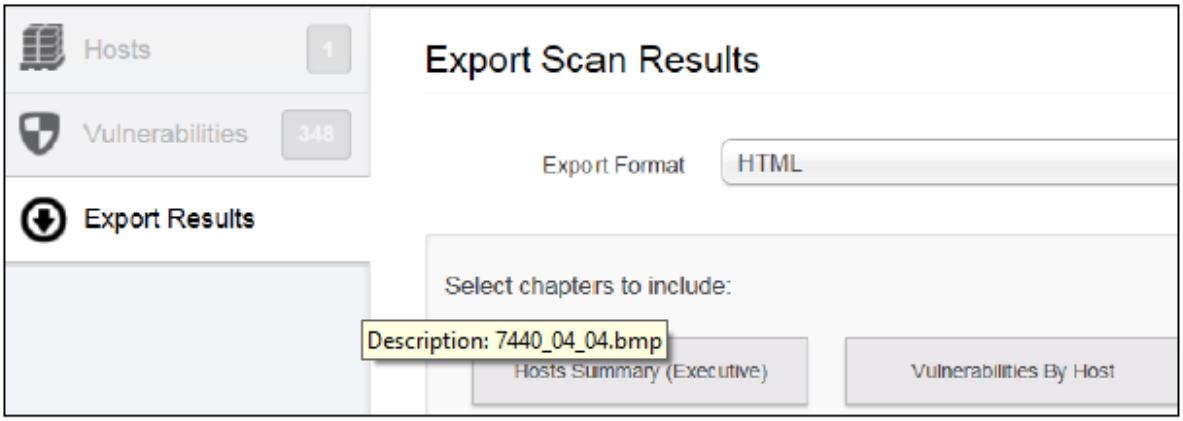
• Luki w zabezpieczeniach na podstawie hosta: ta opcja wyeksportuje raport pokazujący luki w zabezpieczeniach hosta

• Kontrola zgodności (wykonawcza): ta opcja wyeksportuje raport zawierający podsumowanie wykonawcze związane z wybranymi kontrolami zgodności

• Luki w zabezpieczeniach przez wtyczkę: Ta opcja wyeksportuje raport pokazujący luki w zabezpieczeniach przez wtyczkę

• Kontrola zgodności: ta opcja wyeksportuje raport, który pokazuje szczegóły związane z wybranymi kontrolami zgodności

Poprzednie opcje można zobaczyć na poniższym zrzucie ekranu:



W zależności od potrzeb można wybrać jedną lub więcej opcji. Nessus oferuje opcję usunięcia lub usunięcia luki przed wyeksportowaniem raportów, więc jeśli wiesz, że luka w zabezpieczeniach nie dotyczy Ciebie, możesz usunąć lub usunąć ją z listy luk w zabezpieczeniach Nessus.

Zgłoś opcję filtrowania

U góry strony wyników dostępna jest opcja filtrowania. Ta opcja umożliwia filtrowanie raportu Nessus na podstawie kilku dostępnych kryteriów wybranych z menu rozwijanego. Możesz dodać wiele filtrów naraz. Na przykład można dodać wiele filtrów, wybierając opcje z menu rozwijanego filtru, aby uzyskać raport z lukami w zabezpieczeniach, które mają wysoki współczynnik ryzyka, mogą być możliwe do wykorzystania dzięki Exploit Available w MetaSploit, a łatwość wykorzystania jest dostępna w Exploit. Poniższy zrzut ekranu pokazuje, jak dodać filtr:

Filtry można dodawać i usuwać za pomocą odpowiednio przycisków Dodaj filtr i Wyczyść filtry. Nessus daje również opcję dopasowania z dowolnymi warunkami. Warunek Dowolny wskazuje, czy została spełniona którakolwiek z podanych opcji filtrowania. Warunek Wszystkie wskazuje, że wszystkie ustawione warunki filtrowania powinny zostać spełnione. Inne opcje narzędzia do raportowania Nessus służą do porównywania wyników dwóch skanów i ścieżek audytu. Nessus pozwala również przesłać wyniki skanowania z innej maszyny, za pomocą której można generować raporty zgodnie z potrzebami.

Nessus zgłasza treść

Raport Nessus zawiera wiele szczegółowych informacji na temat skanowania i luk w zabezpieczeniach. Informacje na temat skanowania mają postać listy zeskanowanych adresów IP, czasu rozpoczęcia i zakończenia skanowania, nazwy DNS, adresu Maca, systemu operacyjnego oraz podsumowania wyników, które uwzględnia ogólną liczbę luk w zabezpieczeniach oraz rozkład pod względem ważności. luki. Poniższe informacje skanowania są przechwytywane w raportach Nessus:

• Docelowy adres IP

• Wybierz nazwę hosta

• Docelowy adres Mac

• Nazwa DNS

• Czas rozpoczęcia skanowania

• Skanuj czas zakończenia

• Docelowy system operacyjny

Niektóre pola są pokazane na poniższym zrzucie ekranu:

Raport Nessus wyszczególnia luki znalezione w skanie Nessus dla skanowanych hostów. Obejmuje to następujące informacje o każdej luce:

• Luka w zabezpieczeniach przed numerami wtyczek

• Streszczenie

• Opis

• Zobacz także link o tej luce

• Rozwiązanie

• Czynnik ryzyka

• Wynik podstawowy CVSS

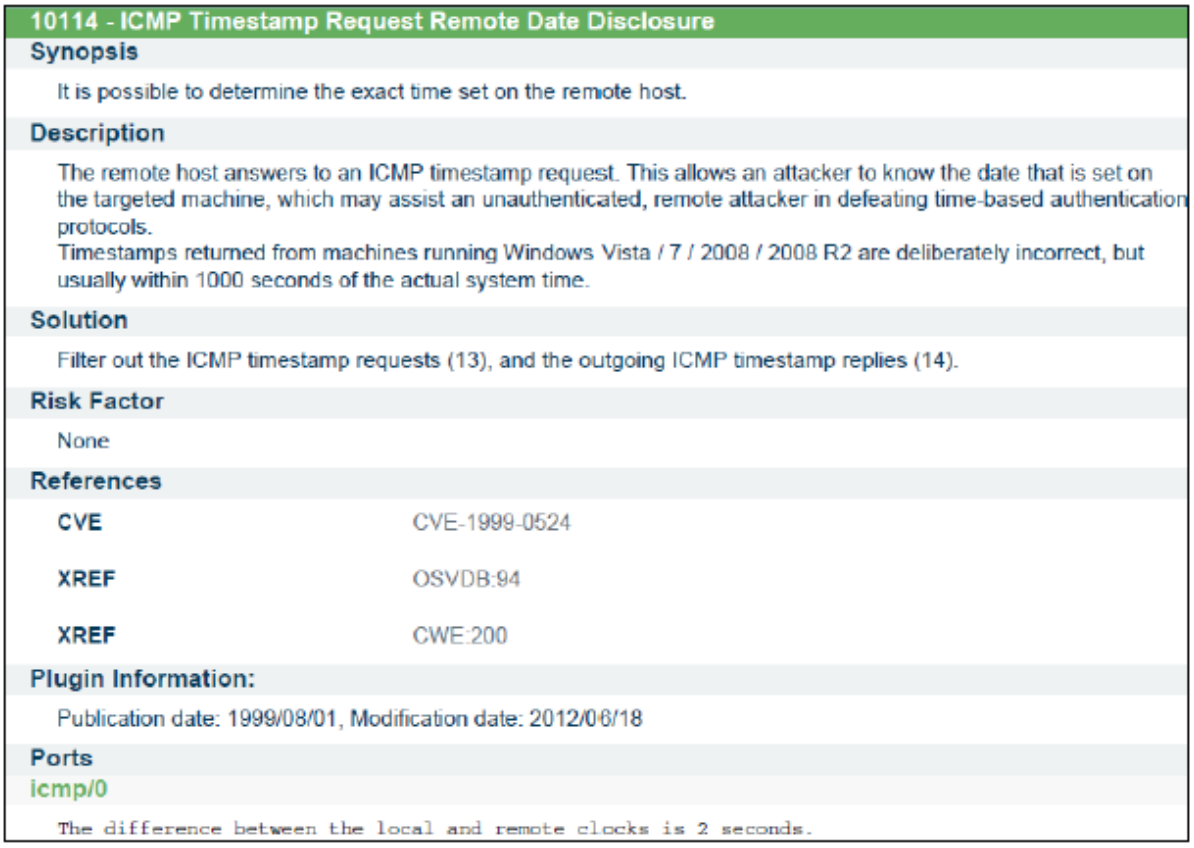
• Referencje

• Informacje o wtyczce

• Wykorzystaj za pomocą

• Porty

Poniższy zrzut ekranu pokazuje przykładową lukę w zabezpieczeniach zawierającą szczegóły luki występującej w raporcie generowanym przez Nessus:



Dostosowywanie raportu

W poprzedniej sekcji dowiedzieliśmy się, że raport Nessus zawiera wiele szczegółowych informacji na temat każdego raportu o luce. Czasami, gdy jesteś zaangażowany jako konsultant do raportu dotyczącego oceny podatności, możesz nie chcieć używać raportu wygenerowanego przez Nessus do dzielenia się z klientem, ponieważ ma on wiele szczegółów na temat każdej luki; może to być dobrze zrozumiałe i przydatne dla konsultanta bezpieczeństwa, ale nie dla końcowego klienta, który musi tylko zrozumieć, czym jest luka i co należy zrobić, aby ją naprawić. Innym przykładem może być prezentacja raportu w innym formacie dostarczonym przez klienta; w tym celu należy odpowiednio dostosować

raport. To zależy od Ciebie, jakie parametry chcesz uwzględnić w raporcie Ocena podatności. Domyślny raport wygenerowany przez Nessus jest całkiem niezły i wyczerpujący. Może się zdarzyć, że w raporcie będzie również potrzeba łatwości wykorzystania, a może wysiłek wymagany do usunięcia luki. To, co należy uwzględnić, a czego nie można uwzględnić w raporcie o luce w zabezpieczeniach, zależy wyłącznie od osoby, która tworzy raport i wymagania organizacji. Musisz dostosować raporty odpowiednio. Dostosowanie można wykonać, usuwając określone pola z domyślnego raportu Nessus i dodając do niego dodatkowe pola, które będą potrzebne oprócz domyślnych pól. Jeśli wymagane jest utworzenie raportu w formacie Microsoft Word, można kopiować i wklejać z domyślnych raportów generowanych przez Nessus. Polecam następujący format generowania imponującego raportu:

• Zgłoś pierwszą stronę:

°° Nazwa klienta

°° Przypisanie lub nazwa projektu

°° Raport przesłany przez

• Strona informacji o dokumencie:

tytuł dokumentu

°° Wersja

imię autora

°° Nazwisko recenzenta

°° Nazwa zatwierdzającego

°° Historia zmian dokumentu z datami

°° Lista dystrybucji dokumentów

°° Klasyfikacja danych dokumentu

• Nagłówek i stopka na każdej stronie z klasyfikacją danych, numerem strony, nazwą dokumentu, logo organizacji i tak dalej

• Streszczenie:

°° Krótki opis projektu oceny podatności wraz z jego zakresem

°° Luki w zabezpieczeniach są liczone z segregacją

°° Graficzna reprezentacja krytyczna, wysoka, średnia, niska,

i informacyjne luki z ich liczbą

°° Wykres liczenia adresów IP / luk w zabezpieczeniach

°° Tabela z nazwą luki w zabezpieczeniach, oceną ryzyka, wpływem na działalność i linkiem do szczegółów w tym samym raporcie

• Sekcja Szczegóły:

°° Usterki krytycznego ryzyka

Nazwa luki

Opis luki w zabezpieczeniach

Wpływ na działalność

Dotknięte IP lub nazwa aplikacji

Artefakt exploita (opcjonalnie)

Łagodzenie / zalecenie

Warunek wstępny do łagodzenia

Nazwa łatki, jeśli ma zastosowanie w celu złagodzenia

Linki do odnośnych luk w zabezpieczeniach

Odniesienia CVE

Informacje o wtyczce Nessus

Możliwość wykorzystania (Metasploit, core impact, CANVAS,

i tak dalej)

Kroki implementacji

Koszt wdrożenia

Złożoność implementacji

Wycofaj kroki, jeśli łagodzenie nie powiedzie się

°° Luki wysokiego ryzyka

Te same pola, które wymieniono w przypadku luk krytycznych

°° Zagrożenia średniego ryzyka

Te same pola, które wymieniono w przypadku luk krytycznych

°° Luki niskiego ryzyka

Te same pola, które wymieniono w przypadku luk krytycznych

°° Słabości informacyjne

Te same pola, które wymieniono w przypadku luk krytycznych

Raport z testu penetracji różni się nieco od raportu oceny podatności. Raport z testu penetracji powinien również zawierać sekcję dotyczącą wykorzystania luki w zabezpieczeniach wraz z dowodami pokazującymi, w jaki sposób została wykorzystana.

Raportuj automatyzację

Sekcja automatyzacji raportów nie jest specyficzna dla Nessus; Ogólnie rzecz biorąc, wiele narzędzi oceny luk w zabezpieczeniach dostępnych na rynku i ich starsze wersje nie obsługują generowania raportów w formatach Microsoft Excel lub PDF. Aby w pełni wykorzystać te generowane automatycznie raporty i dostosować je do preferowanych formatów raportów organizacji, głównie Excel lub Word, można zapisać skrypty w celu przekonwertowania tych domyślnych raportów w celu generowania raportów dla naszych własnych potrzeb. Inną potrzebą automatyzacji raportów Nessus

jest to, że integrując raporty Nessus za pomocą różnych narzędzi, takich jak Archer i Agiliance, które są narzędziami zarządzania ryzykiem i zgodności; informacje o bezpieczeństwie i narzędzie do zarządzania zdarzeniami; lub dowolne inne narzędzia dostępne w Twojej organizacji, za pomocą których Nessus ma generować wyniki Oceny luk w zabezpieczeniach. W takich przypadkach każde narzędzie ma wstępnie określone formaty raportów. Większość narzędzi akceptuje formaty CSV. Aby przekonwertować raporty na żądane formaty, polecam pisanie skryptów.

Podsumowanie

Niniejsza część omawia opcje raportowania w Nessus. Treść raportu dotyczącego oceny podatności powinna być dostosowana do potrzeb odbiorców raportu, od wyższej kadry kierowniczej po zespoły techniczne pracujące nad zamknięciem luk w zabezpieczeniach. Po zakończeniu skanowania dane wyjściowe są dostępne w zakładce Wynik w Nessusie. Na tej karcie znajduje się podsumowanie hostów, znalezione luki i opcja eksportu wyników. Wyniki można eksportować w różnych formatach, takich jak PDF, CSV i HTML, a Nessus oferuje pięć opcji decydowania o treści, które należy uwzględnić, a mianowicie Podsumowanie hostów (wykonawczy), Luki w zabezpieczeniach hosta, Sprawdzanie zgodności, Luki w zabezpieczeniach przez wtyczkę i Compliance Checks (Executive). Zakładka Wynik ma również filtrowanie Opcja, w której rozwijane menu filtruje wymaganą klasę i typy luk i może być filtrowana z ogólnego wyniku. Raport przechwytuje informacje o skanowaniu wraz z informacjami o luce w zabezpieczeniach, w tym streszczeniem, opisem, rozwiązaniem, zagrożeniami, wtyczkami, wynikiem CVSS i innymi ważnymi szczegółami. Niniejszy rozdział obejmuje również dostosowywanie raportów z perspektywy zewnętrznego konsultanta oraz rodzaje szczegółów, które powinny zostać uwzględnione w raporcie. Wreszcie wprowadzono koncepcję automatyzacji raportów; można to zrobić za pomocą skryptów, a także poprzez integrację z narzędziem zgodności GRC lub rozwiązaniami SIEM

Sprawdzenie zgodności

Nessus jest dobrze znany jako skaner luk w zabezpieczeniach, ale oferuje także opcję sprawdzania zgodności. Korzystając z tej opcji, można sprawdzić, czy ustawienia bezpiecznej konfiguracji infrastruktury, takie jak serwery, urządzenia sieciowe, baza danych i komputer, są zgodne z określonymi zasadami lub najlepszymi praktykami stosowanymi przez organizację. Audyt kontroli zgodności to ważna i niezbędna funkcja wymagana zgodnie z bieżącymi potrzebami bezpieczeństwa organizacji. Wszystkie organizacje odpowiedzialne za bezpieczeństwo definiują i wdrażają bezpieczne ustawienia konfiguracyjne dla swoich infrastruktur IT i sieci, aby zapobiec zagrożeniom bezpieczeństwa, które mogą zostać zrealizowane z powodu błędnej konfiguracji. Ponadto, takie wymagania dotyczące zgodności dla wzmocnienia bezpieczeństwa i kontroli wdrożenia wynikają również z wymogów regulacyjnych, gdy firma musi przestrzegać różnych przepisów dotyczących zgodności, takich jak ISO 27001 dla systemu zarządzania bezpieczeństwem informacji, HIPAA dla przemysłu medycznego i SOX dla domena finansowa. Aby sprawdzić zgodność serwerów, urządzeń sieciowych z tymi zdefiniowanymi kontrolkami lub bezpieczną konfigurację, wymagana jest regularna kontrola zgodności. Przeprowadzanie takich kontroli zgodności ręcznie, zwłaszcza gdy wielkość infrastruktury jest duża, a nawet gdy po pobraniu próbek i kontroli, które mają być sprawdzane na urządzenie są duże liczby, będzie żmudne i czasochłonne zadanie. Może to również spowodować możliwość wystąpienia błędów i czasu potrzebnego w wymianie informacji pomiędzy zespołami operacyjnymi i zespołami ds. Zgodności w celu przygotowania, zatwierdzenia i korekty artefaktów. Opcja kontroli zgodności oferowana przez Nessus pomoże w przeprowadzeniu takiego sprawdzenia w sposób zautomatyzowany. Nessus oferuje również opcje modyfikacji plików zgodności, aby były zgodne z polityką umocnienia urządzeń w organizacji.

Narzędzie Vulnerability Scan zazwyczaj rozpoznaje znane luki w zabezpieczeniach obecny w systemie, dla którego dostępna jest wtyczka, i rozpozna brakujące łatki. Inspekcja sprawdzi zgodność infrastruktury z bezpieczną konfiguracją zdefiniowaną w lokalnej polityce. Skrócenie luki w zabezpieczeniach podczas skanowania narażenia na atak nie oznacza, że system jest bezpiecznie skonfigurowany. Na przykład, jeśli polityka haseł organizacji wymaga co najmniej 10 znaków, ponieważ obsługuje poufne informacje, serwer może mieć uaktualnione łaty lub mieć stosunkowo mniejszą podatność na błędy w wynikach skanowania VA przeprowadzonego. Jest tak dlatego, że serwer nie zapewni, że skonfigurowano politykę 10 znaków. Ta funkcja jest dostępna z profesjonalnym kanałem Nessus.

Kontrole zgodności Nessus są dostępne dla głównych platform, takich jak systemy serwerowe (Windows i Unix), bazy danych, komputery stacjonarne i urządzenia sieciowe, a także standardy kontroli, takie jak PCI DSS. Ta część obejmuje następujące główne obszary:

• Kontroluj politykę

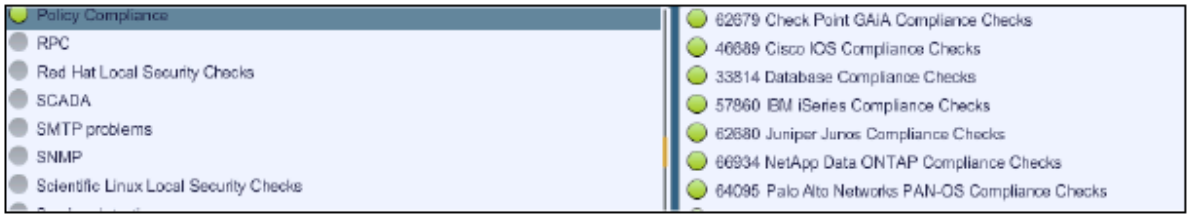
• Jak skonfigurować politykę sprawdzania zgodności Nessus

• Raportowanie zgodności w Nessus

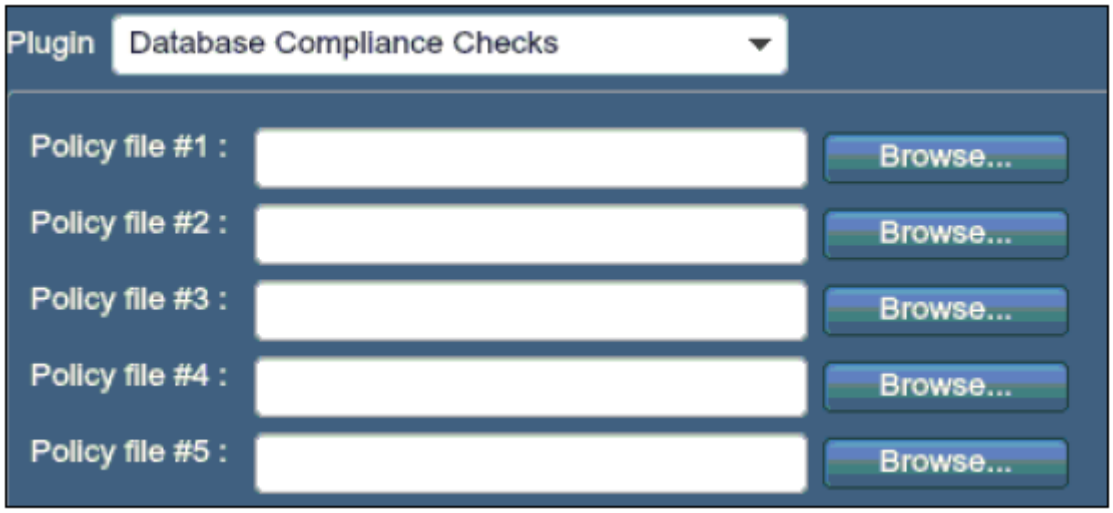
• Opcja sprawdzania zgodności dla różnych rodzajów infrastruktury

Zasady audytu

Aby przeprowadzić te kontrole zgodności, polityki są dostępne w plikach z rozszerzeniem .audit, które są dostępne dla różnych elementów infrastruktury, takich jak bazy danych, Windows i Cisco. Te pliki kontroli zawierają również wspólne punkty kontrolne objęte dobrze znanymi standardami, takimi jak SOX i PCI-DSS. Pliki te mają również rekomendacje od dobrze znanych organów ds. Bezpieczeństwa i organów doradczych, takich jak jako NIST i CERT. Te pliki kontroli można zmodyfikować zgodnie z lokalnymi zasadami lub dokumentami hartowania. Tenable oferuje opcje pobierania tych plików kontroli z witryny wsparcia i dostarcza dokumentacji, aby zrozumieć składnię tych plików, aby utworzyć je z dostosowaniami zgodnie z wymaganiami. Tenable oferuje również narzędzia do konwersji pliku zasad systemu Windows z rozszerzeniem .inf na rozszerzenie z rozszerzeniem .audit. Aby umożliwić korzystanie z opcji sprawdzania zgodności, użytkownik końcowy musi najpierw kliknąć przycisk + Dodaj politykę. Opcja sprawdzania zgodności jest dostępna w sekcji Zasady | Preferencje wtyczek. Spośród różnych dostępnych wtyczek Nessus rodzina wtyczek do sprawdzania zgodności to Zgodność z zasadami. Ta wtyczka sprawdza różne infra-komponenty, takie jak serwery i sieć. Poniższy zrzut ekranu przedstawia rodzinę wtyczek Policy Compliance:

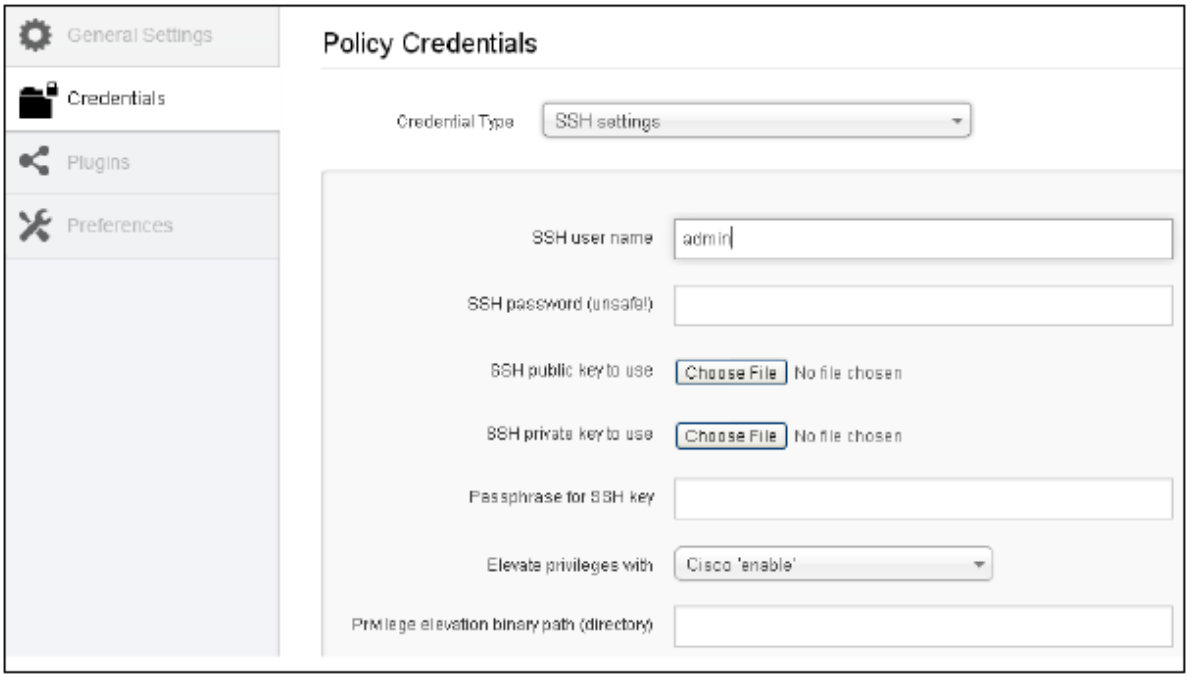


Aby użyć dostosowanych plików kontroli, użyj opcji Preferencje w obszarze Zasady. Na karcie Preferencje znajduje się menu rozwijane, w którym można wybrać różne testy zgodności, takie jak kontrole zgodności Cisco IOS i kontrole zgodności bazy danych. W tym przypadku użytkownik otrzyma również opcję wybrania i przesłania więcej niż jednego pliku kontroli, który zostanie wykorzystany do przeprowadzenia kontroli zgodności. Poniższy zrzut ekranu pokazuje wybraną opcję Database Compliance Checks:



Referencje

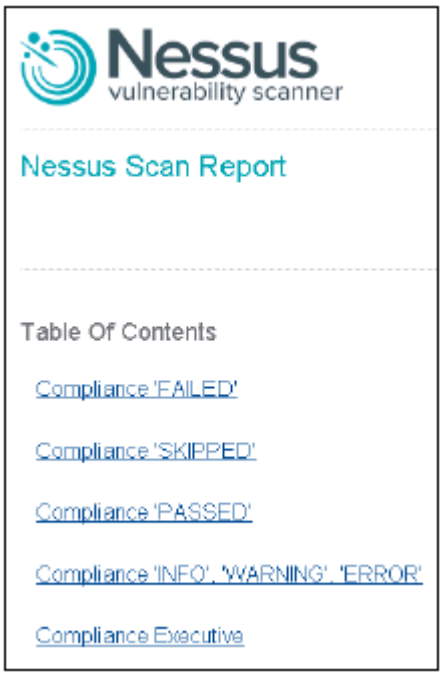
Aby Nessus mógł przeprowadzić kontrolę zgodności, należy podać poświadczenia, aby logował się do systemu w celu przeprowadzenia lokalnych kontroli. Użyte poświadczenia powinny być poświadczeniami konta uprzywilejowanego, czyli superużytkownika w przypadku konta uniksowego z uprawnieniami administracyjnymi do odczytu lokalnej polityki komputera. W przypadku sprawdzania zgodności bazy danych wymagane będą poświadczenia bazy danych. W przypadku sprawdzenia zgodności Cisco IOS, włączyć hasło jest wymagane do wykonania audytu konfiguracji. Dane uwierzytelniające można dodać w polisach | Poświadczenia, jak to miało miejsce podczas skanowania VA. Poniższy zrzut ekranu jest przykładem sposobu dostarczania referencji w przypadku audytu konfiguracji Cisco:



Raportowanie zgodności

Aby uzyskać raport dotyczący statusu zgodności danego celu, Nessus oferuje opcje takie jak Kontrola zgodności i Kontrola zgodności (Executive) podczas zapisywania raportu. Korzystając z którejkolwiek z

tych opcji, można uzyskać zgodność status systemu w stosunku do elementów sterujących obecnych w pliku .audit. Jest to reprezentowane w raporcie przez wskazanie, czy zgodność nie powiodła się, przeszła lub została pominięta wraz z podsumowaniem wykonawczym. Nieskonkurencyjne testy są zgłaszane w ramach błędów i ostrzeżeń. Poniższy zrzut ekranu prezentuje raport wygenerowany za pomocą opcji Sprawdzanie zgodności i Podsumowanie kontroli zgodności:



Inspekcja infrastruktury

Wtyczki zgodności są dostępne w ramach rodziny wtyczek Policy Compliance. Ta sekcja zawiera listę wtyczek dostępnych w tej rodzinie, które przedstawiają rodzaj infrastruktury, dla której można wykonać audyt zgodności. Dla każdego typu elementu infrastruktury, takiego jak serwery, sieci i bazy danych, należy wybrać odpowiedni plik zasad, poświadczenia i wtyczkę, jak wspomniano w poprzednich sekcjach w tej części.

Sprawdzanie zgodności Windows

Korzystając z tej wtyczki, można sprawdzić zestaw parametrów zgodności w opcji Zasady systemu Windows. Przykłady niektórych kontroli przeprowadzonych w ramach kontroli systemu Windows obejmują:

• Ustawienie rejestru

• Uprawnienia do plików

• Zasady dotyczące haseł

• Zasady blokady

• Zasady audytu

• Zasady dotyczące praw użytkownika

• Audyty serwisowe

Treść pliku Windows

Opcja Plik systemu Windows pozwala Nessusowi sprawdzać typy plików Windows (pliki Excel, Adobe lub tekstowe), które mogą zawierać poufne dane, takie jak dane osobowe umożliwiające identyfikację (PII) i dane karty kredytowej.

Sprawdzanie zgodności Unix

Nessus może sprawdzić zgodność różnych wersji Uniksa, takich jak Solaris, Red Hat, AIX, HP-UX, SUSE, Gentoo i freebsd. Kluczowe kontrole obejmują:

• Zarządzanie hasłem

• Uprawnienia do plików

• Zarządzanie plikami haseł

• Zarządzanie uprawnieniami

• Zarządzanie dostępem root

• Uruchomione procesy

Sprawdzanie zgodności Cisco IOS

Korzystając z tej wtyczki, można sprawdzić maszynę Cisco z uruchomionym plikiem konfiguracyjnym dla urządzeń Cisco IOS. Sprawdzanie zgodności można wykonać w odniesieniu do zapisanych, uruchomionych lub uruchomionych konfiguracji. Przykłady obejmują:

• Lista dostępu zastosowana do interfejsów

• Łańcuchy społeczności SNMP są chronione przez listy ACL

• Niespełnione usługi są wyłączone

• Zmieniono domyślny ciąg społeczności SNMP

Sprawdzanie zgodności bazy danych

Nessus może również sprawdzić zgodność różnych baz danych z zasadami bezpieczeństwa. Obsługiwane bazy danych to MS SQL, Oracle, MySQL PostgreSQL, IBM DB2 i Informix / DRDA. Aby zapewnić kompletność raportu, konto używane do zalogowania się do bazy danych powinno mieć uprawnienie SYSDBA lub SA. Wtyczki sprawdzania zgodności bazy danych zazwyczaj używają zapytań SELECT do pobierania konfiguracji zabezpieczeń z pliku bazy danych. Oto kilka przykładów:

• Sprawdzanie logowań bez szczegółów dotyczących wygaśnięcia

• Sprawdzanie, czy włączone są nieautoryzowane procedury składowane

Zgodność z PCI DSS

Karta płatnicza Przemysł Standard bezpieczeństwa danych (PCI-DSS) jest dobrze znanym standardem stosowanym w przypadku kart płatniczych. Nessus oferuje wtyczki zgodności PCI DSS, aby sprawdzić konfigurację zgodnie z wymaganiami tego standardu.

VMware vCenter / vSphere Compliance Check

Wtyczka VMware vCenter / vSphere Compliance Check wykorzystuje interfejs API VMware SOAP do kontroli oprogramowania wirtualizacyjnego ESX VMware, ESXi i vCenter / vSphere. Informacje uwierzytelniające do przeprowadzenia audytu można dodać do VMware vCenter SOAP

Ustawienia API w sekcji Zaawansowane zasady. Przykłady obejmują:

• Brakujące łatki

• Brakujące aktualizacje zabezpieczeń

Niektóre inne platformy uwzględnione w opcjach sprawdzania zgodności Nessus obejmują następujące elementy (sprawdź poprawioną dokumentację na oficjalnej stronie internetowej firmy Tenable, https://support.tenable.com/) Do kilku rozdziałów tego rozdziału odwołano się do materiałów szkoleniowych dostępne na stronie internetowej Nessus http://www.tenable.com:

• Sprawdzanie zgodności IBM iSeries

• Kontrole zgodności Juniper Junos

• Sprawdzanie zgodności NetApp Data ONTAP

• Sprawdzanie zgodności PAN-OS w Palo Alto Network

• Sprawdzanie zgodności Check Point GAiA

Podsumowanie

Nessus oferuje opcje przeprowadzania zautomatyzowanych kontroli zgodności za pomocą narzędzia, oprócz skanowania narażenia na atak. Korzystając z tej opcji, można sprawdzić, czy ustawienia bezpiecznej konfiguracji infrastruktury, takie jak serwery, urządzenia sieciowe i bazy danych, są zgodne ze zdefiniowanymi zasadami lub najlepszymi praktykami stosowanymi przez organizację. Wymóg zgodności wynika również z różnych standardów zgodności przestrzeganych przez organizację. Ta funkcja jest dostępna dla profesjonalnych subskrybentów kanału. Rodzina wtyczek Policy Compliance jest dostępna do skanowania sprawdzania zgodności. Rodzina wtyczek obejmuje między innymi serwery, urządzenia sieciowe i standardy, takie jak PCI DSS. Karta Wyniki Nessus oferuje także opcję zgodności, a jednocześnie zapisuje dane wyjściowe, aby wygenerować raport zgodności. Te kontrole zgodności można zmodyfikować za pomocą plików .udud. Odpowiednie referencje infrastruktury bazowej, na której przeprowadzany jest audyt zgodności, muszą zostać zaktualizowane w narzędziu.