Vulnerability Management.

Zarządzanie bezpieczeństwem to proces, który musi być nieustannie zasilany wiedzą o aktualnym stanie bezpieczeństwa wszystkich systemów informatycznych organizacji. Wiedza ta wykorzystywana jest do oceny sytuacji, oraz podejmowania decyzji o działaniach zaradczych. Niezbędna jest świadomość ryzyk związanych z lukami w systemach bez względu na to, czy dotyczą one aplikacji WEB, systemów baz danych, czy pojedynczych stacji roboczych.

Vulnerability Assessment

Wykrywanie i identyfikacja hostów i usług w sieci. Badanie i ocena luk bezpieczeństwa i podatności zidentyfikowanych zasobów to Vulnerability Assessment - niezbędny element procesu zarządzania bezpieczeństwem. Proces ten jest skuteczny tylko wtedy, gdy w jego wyniku stale otrzymujemy aktualne informacje wzbogacające wiedzę o stanie bezpieczeństwa. Wiedza ta może być wykorzystywana w procesie zarządzania bezpieczeństwem. Nawet najlepiej przeprowadzony audyt przestaje być aktualny natychmiast po zakończeniu pracy audytora, ponieważ od tej pory w badanej sieci pojawiły się już nowe luki bezpieczeństwa. Zarządzanie bezpieczeństwem w oparciu o nieaktualne dane nie może być skuteczne. Dlatego Vulnerability Assessment to zadanie, które powinno być powtarzane tak często, jak jest to możliwe.

Greenbone GSM

GSM firmy Greenbone to unikalne rozwiązanie łączące w sobie funkcję systemu wykrywania, identyfikacji i oceny podatności (Vulnerability Assessment), oraz systemu zarządzania wiedzą o wykrytych lukach (Vulnerability Management).

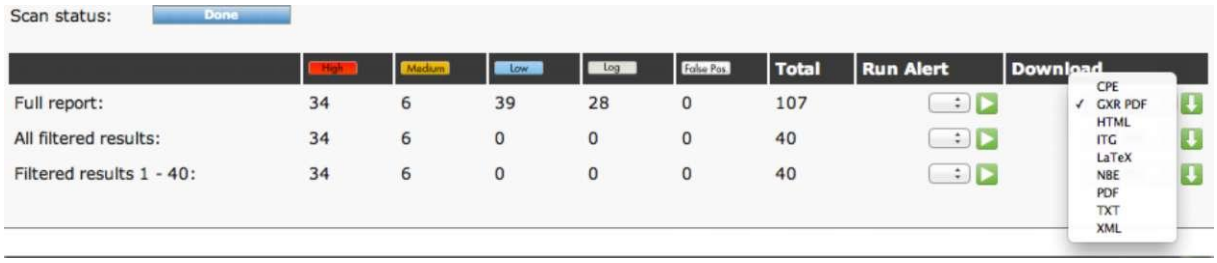
Niezwykle skuteczny skaner podatności wykrywa i identyfikuje hosty i usługi w sieci a następnie wykonuje testy w celu wykrycia podatności i luk bezpieczeństwa wynikających z konfiguracji. Testy dzielą się na dwie grupy:

- zewnętrzne oparte na skanowaniu sieciowym (black-box scanning),
- wykonywane na hostach z wykorzystaniem uwierzytelnień (white-box scanning).

System wyposażony jest w procedury testowe (obecnie ok. 30 000), które są codziennie aktualizowane przez producenta.

Raportowanie

Wyniki skanowania prezentowane są w formie przejrzystego raportu. Raport zawiera opis każdej wykrytej podatności, odnośniki do zewnętrznych źródeł informacji, oraz wskazuje działania zaradcze. Raporty mogą być filtrowane, a następnie eksportowane w wielu formatach (PDF Executive, PDF Detailed, CPE, HTML, ITG, LaTeX, NBE, TXT, XML). Wbudowany system powiadamiania może automatycznie wysyłać raporty w wybranym formacie w wiadomości e-mai. Wysyłanie raportów można uzależnić od poziomu krytyczności wykrytych podatności, lub od zmiany trendu w stanie bezpieczeństwa skanowanych obszarów sieci.



Trendy bezpieczeństwa

System Greenbone GSM wykonując kolejne skanowania automatycznie porównuje ich wyniki i wskazuje zmiany w postaci trendów dla każdego skanowanego obszaru.

Delty wyników skanowania

Oprócz pełnych raportów z każdego skanowania system Greenbone GSM umożliwia analizowanie wyników skanowań w postaci delty. Raport różnicowy zawiera jedynie te informacje, które nie znalazły się w poprzednich wynikach skanowania. Funkcjonalność ta ogranicza do minimum czas poświęcany na analizę nowych raportów. Delty mogą być filtrowane i eksportowane podobnie jak pełne raporty.

Notatki

Każda wykryta podatność może być opatrzona notatką. Notatka zostanie dołączona do opisu wykrytej podatności w wynikach skanowania i eksportowanych raportów. Do każdego wyniku można dodać nieograniczoną ilość notatek. W zależności od decyzji użytkownika notatki mogą być uwzględniane w kolejnych skanowaniach:
- zawsze, bądź przez określony okres czasu,
- zawsze dla wszystkich hostów, lub tylko dla konkretnego hosta,

- dla wszystkich użytkowników systemu, lub dla użytkownika, który umieścił notatkę,
- zawsze w przypadku wystąpienia tej podatności niezależnie od obszaru skanowania. Powyższe warunki mogą być dowolnie ze sobą łączone.
Umieszczanie notatek po przeanalizowaniu podatności umożliwia lepsze zarządzanie wiedzą o stanie bezpieczeństwa i ułatwia analizę podatności w przyszłości.

Zmiana klasyfikacji podatności

Użytkownik systemu Greenbone GSM może zmienić klasyfikację każdej z wykrytych podatności. Dostępne klasyfikacje to: Critical, Medium, Low, Log. Szczególną klasyfikacją jest False-Positive. Oznaczone tak podatności nie pojawiają się w wynikach skanowań. Każda zmiana klasyfikacji podatności może być dodatkowo opatrzona notatką. W zależności od decyzji użytkownika zmiany klasyfikacji mogą być umieszczane w kolejnych wynikach skanowania:
- zawsze, bądź przez określony okres czasu,
- zawsze dla wszystkich hostów, lub tylko dla konkretnego hosta,
- dla wszystkich użytkowników systemu, lub dla użytkownika, który umieścił notatkę,
- zawsze w przypadku wystąpienia tej podatności niezależnie od obszaru skanowania. Powyższe warunki mogą być dowolnie ze sobą łączone.
Zmiany klasyfikacji podatności, a w szczególności oznaczanie podatności jako „false- positive" ułatwiają przyszłą analizę wyników skanowań i zdecydowanie ograniczają czas i zasoby niezbędne do przeprowadzenia kolejnych analiz.

Skanowanie aplikacji WEB

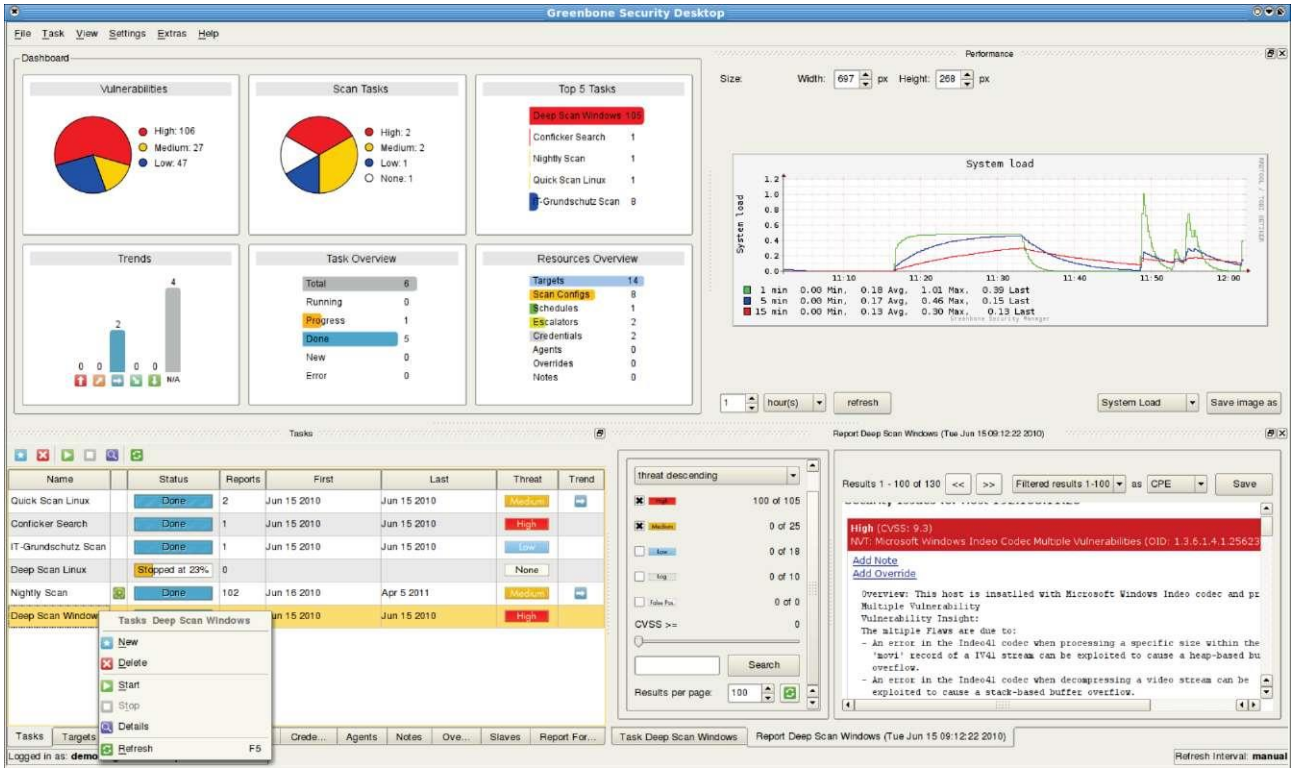
System Greenbone GSM wyposażony jest we wzorce skanowań dedykowane dla testów aplikacji WEB. Wzorce skanowań można powielać i dostosowywać do konkretnych aplikacji wskazując m.i. wirtualne hosty, adresy URL i uwierzytelnienia do logowania.

Wzorce skanowań dostosowane do potrzeb

System Greenbone GSM wyposażony jest w zestaw wzorców skanowań, które można dostosować do potrzeb organizacji, lub wykorzystywać bez zmian. W zależności od sytuacji skanowania mogą być nieinwazyjne, lub dopuszczać możliwość agresywnego atakowania usług i systemów, które mogą doprowadzić do ich niedostępności. Wybrane zestawy testów mogą uwzględniać zgromadzone wcześniej informacje, lub je ignorować. System umożliwia również łatwe importowanie wzorców dedykowanych do konkretnych zastosowań. Nowe wzorce skanowań mogą być przygotowane przez producenta, lub użytkownika systemu.

Interfejsy zarządzania i dostęp wielu użytkowników

System Greenbone GSM może być zarządzany za pośrednictwem interfejsu WEB, dedykowanej aplikacji - Greenbone Security Suite (Windows, Linux), interfejsu CLI (SSH, konsola), lub dobrze udokumentowanego API. System zapewnia jednoczesny dostęp dla nieograniczonej ilości użytkowników bez względu na stosowaną przez nich metodę dostępu i posiadaną wersję/licencję.



Licencjonowanie niezależne od ilości adresów IP i ilości użytkowników

Licencjonowanie systemów Greenbone GSM nie jest związane z ilością skanowanych adresów IP, anni z ilością użytkowników systemu. Poszczególne rozwiązania Greenbone są ograniczone pod względem maksymalnej ilości adresów IP, które można skanować w jednym zadaniu skanowania. Ilość zdefiniowanych zadań skanowania jest dowolna. Ilość równocześnie uruchamianych zadań skanowania ograniczona może być jedynie możliwościami sprzętowymi wybranego modelu urządzenia GSM. Dlatego wybór konkretnego rozwiązania Greenbone GSM powinien być podyktowany potrzebami wydajnościowymi związanymi z ilością równocześnie analizowanych hostów, ograniczonym czasem, który jest potrzebny na wykonanie zadań skanowania, oraz ilością interfejsów sieciowych potrzebnych do skanowania różnych obszarów sieci.

Licencjonowanie systemów Greenbone jest przejrzyste i przewidywalne. W ramach subskrypcji (1, 3, lub 5 lat) producent zapewnia stałą aktualizację procedur testowych, pomoc w rozwiązywaniu problemów, wsparcie dla sprzętu i oprogramowania, wsparcie przy tworzeniu wzorców skanowania i dodatkowych raportów. Dlatego subskrypcja jest jedynym stałym kosztem związanym z eksploatacją systemu.

Otwartość i przejrzystość

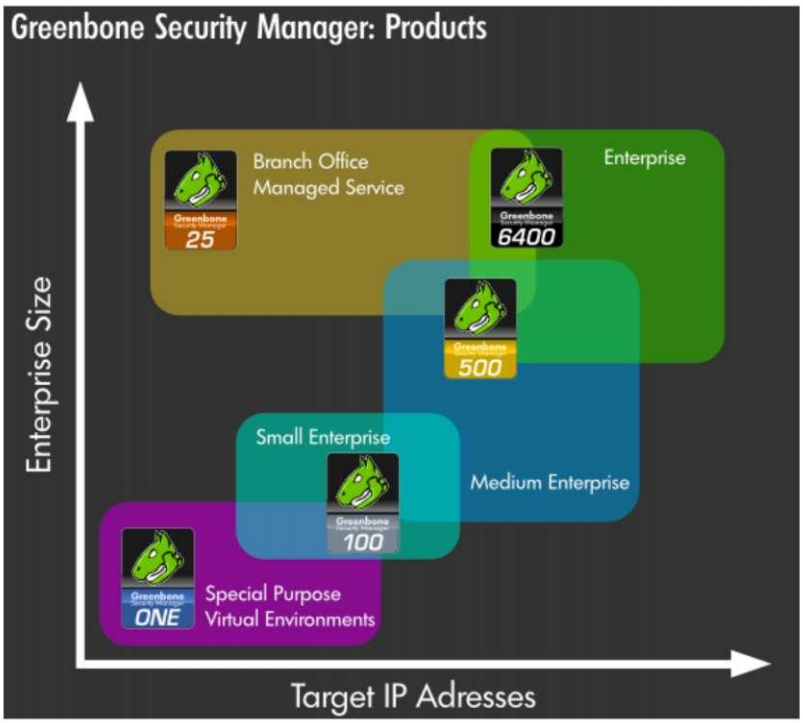
Systemy Greenbone GSM oparte są wyłącznie na otwartych standardach. Producent udostępnia pełną dokumentację systemu, dokumentację interfejsu API, oraz wiedzę niezbędną do zarządzania systemem. To unikalne podejście ma pozytywny wpływ na koszty wdrożenia, utrzymania i dostosowania systemu do wymagań użytkownika. Mechanizmy wykrywania, analizy i klasyfikacji podatności w całości oparte są na standardach:

- SCAP (Security Content Automation Protocol)
- CVE (Common Vulnerabilities and Exposure)
- CPE (Common Platform Enumeration)
- CVSS (Common Vulnerability Scoring System)
- OVAL (Open Vulnerability and Assessment Language)

Zastosowanie standardów powoduje, że wyniki skanowań są miarodajne i porównywalne. Odwołania do standardów zapewniają wysoką jakości analizy i możliwość odniesienia wyników do zewnętrznych, niezależnych źródeł. Zastosowanie standardów tworzenia procedur testowych pozwala na ich modyfikowanie oraz tworzenie własnych.

Skalowalność

Systemy Greenbone GSM oferowane są w konfiguracjach dostosowanych do potrzeb każdej organizacji. Dostępne są modele ekonomiczne przeznaczone dla samodzielnych audytorów, oraz wydajne systemy przeznaczone do pracy w dużych organizacjach sektora enterprise.Modele GSM 510, oraz GSM 6400 mogą być stosowane w architekturze rozproszonej z centralnym zarządzaniem. Systemy te są przystosowane do zarządzania wieloma skanerami GSM 25 i GSM 100. Łączenie wielu skanerów Greenbone w jeden system o rozproszonej architekturze oznacza możliwość dostosowania systemu do potrzeb organizacji w miarę jej rozwoju.



Błyskawiczne wdrożenie

Systemy Greenbone GSM to w pełni funkcjonalne platformy sprzętowe, lub wirtualne maszyny.

Greenbone Security Manager 6400	Large Enterprise IT Control of upto 50 scan sensors* **5,000 - 50,000 IPs*** **GSM 5300:** 3,000-30,000 IPs*, upto 30 scan sensors*	0-24 Port GbE Base-TX 0-24 Port GbE SFP 0-6 Port 10GbE XFP Redundant: HDD, Power, Fans Hot-Swap: HDD, Power, Fans Greenbone OS with SSH, OMP, HTTPS, Backup	 Price on application
Greenbone Security Manager 510	Medium to large enterprise IT Control of upto 12 scan sensors* Major branch offices **500 - 6,000 IPs*** **GSM 500:** 500-5,000 IPs*, upto 10 scan sensors*	4 Port GbE Base-TX 4 Port SFP Greenbone OS with SSH, OMP, HTTPS, Backup	 Price on application
Greenbone Security Manager 100	Small and medium enterprise IT Medium branch offices Scan sensor for GSM from GSM 500 **50 - 500 IPs***	4 Port GbE Base-TX Greenbone OS with SSH, OMP, HTTPS	 Appliance: from 2,990 €** Subscription: 1 year: from 2,700 € 3 years: from 6,480 € 5 years: from 9,450 €
Greenbone Security Manager 25	Scan sensor for GSM from GSM 500 Small branch offices **20 - 300 IPs***	4 Port GbE Base-TX Greenbone OS with SSH, OMP	 Appliance: from 2,490 €** Subscription: 1 year: from 2,100 € 3 years: from 5,040 € 5 years: from 7,350 €
Greenbone Security Manager ONE	Virtualised environments Special purpose **20 - 300 IPs*** Only in combination with a project solution	OVA VM Snapshot 1 (virtual) Port Greenbone OS with SSH, OMP, HTTPS	 Virt.Appliance: from 390 €** Subscription: 1 year: from 1,900 € 3 years: from 5,016 € 5 years: from 7,600 €

Urządzenia GSM są gotowe do pracy natychmiast po podłączeniu. Wdrożenie i utrzymanie systemów GSM nie wymaga instalacji ani utrzymania żadnych dodatkowych aplikacji, ani systemów operacyjnych.