Profesjonalne testy penetracyjne

Zbuduj własne środowisko do testów | Wydanie II

Thomas Wilhelm

Helion

Tytuł oryginału: Professional Penetration Testing, Second Edition: Creating and Learning in a Hacking Lab

Tłumaczenie: Robert Górczyński

ISBN: 978-83-246-9033-6

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/protes
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

ROZDZIAŁ 6.

Zbieranie informacji

W tym rozdziale omawiam:

- pasywne zbieranie informacji;
- aktywne zbieranie informacji.

WPROWADZENIE

Zbieranie informacji to pierwszy i bez wątpienia najważniejszy krok podczas przeprowadzania testu penetracyjnego. Po zakończeniu tej fazy powinniśmy dysponować dokładną mapą sieci celu ataku, a także znać ilość wysiłku, jaki trzeba będzie włożyć w pełne wykonanie zadania. Ponadto w trakcie tej fazy należy zidentyfikować rodzaje systemów w sieci (między innymi używane systemy operacyjne), co pozwoli na wybór odpowiedniego personelu oraz narzędzi używanych w pozostałej części projektu testu penetracyjnego. Klienci zwykle dostarczają sporo informacji dotyczących ich sieci, aby w ten sposób nieco Ci pomóc w wykonaniu zadania. Nie powinieneś się jednak zdziwić, gdy otrzymane informacje okażą się błędne. Dlatego też konieczne jest przeprowadzenie omawianej tutaj fazy niezależnie od ilości informacji otrzymanych od klienta.

Są dwa rodzaje zbierania informacji: zbieranie pasywne i zbieranie aktywne. W przypadku pasywnego zbierania informacji naszym celem jest zebranie maksymalnej ilości danych o systemach i sieci będących celem ataku, ale bez bezpośredniego łączenia się z nimi. Oznacza to również próbę zebrania wiadomości o korporacji, między innymi: kto jest jej właścicielem, gdzie mieści się siedziba, gdzie znajdują się komputery i sieć, jak jest zaprojektowana siedziba firmy (w przypadku, gdy trzeba przeprowadzić fizyczny test penetracyjny), i innych informacji, w zależności od celów projektu testu penetracyjnego.

Drugi rodzaj zbierania informacji to zbieranie aktywne. W tym przypadku następuje bezpośrednie połączenie z celem ataku. Ten rodzaj zbierania informacji ma za zadanie jedynie zapewnić lepsze rozeznanie w kwestii wysiłku koniecznego do włożenia, a także w kwestii ustalenia typu i liczby systemów, które ma objąć projekt. W dalszej części rozdziału dokładnie zostaną wymienione rodzaje gromadzonych informacji. W tym momencie najważniejsze jest, aby lepiej zrozumieć podejmowane przez nas działania.

Istnieje przekonanie, że aktywne zbieranie informacje jest bardziej użyteczne od technik pasywnych. Jednak bardzo często wymienione przekonanie jest fałszywe. Nierzadko zdarzało się, że dane wrażliwe lub o znaczeniu krytycznym wyciekły, a następnie zostały zarchiwizowane, nawet po usunięciu problemu. Podczas przeprowadzania testu penetracyjnego ten rodzaj błędów jest bardzo przydatny, zwłaszcza jeśli ujawnione informacje dotyczą atakowanej sieci. Wcale nie tak trudno znaleźć zarchiwizowane informacje o plikach konfiguracyjnych i instalacyjnych wraz z danymi poufnymi obejmującymi na przykład sekrety firmy.

W tym rozdziale skupimy się przede wszystkim na metodologii przedstawionej w dokumencie ISSAF (ang. *Information Systems Security Assessment Framework*). W wymienionej metodologii faza zbierania informacji została podzielona na kilka znacznie dokładniejszych kroków. Jednak zrealizujemy również cele przedstawione w podręczniku OSSTMM (ang. *Open Source Security Testing Methodology Manual*), w którym większość danych dotyczących zbierania informacji zawarto w module zatytułowanym *Logistics* i skoncentrowano się na wymienionych poniżej obszarach:

- framework,
- jakość sieci,
- czas.

Według podręcznika OSSTMM framework wiąże się ze wszystkim, co zostanie omówione w tym rozdziale, czyli z pasywnym i aktywnym zbieraniem informacji. Dodatkowe testy powiązane z jakością sieci i z czasem nie będą tutaj omówione, ponieważ są trudne do replikacji w laboratorium, jeśli nie zostanie wykorzystany dodatkowy osprzęt sieciowy. Test jakości sieci dotyczy utraty pakietów i współczynnika szybkości mierzonego w wielu sieciach, ale to naprawdę nie jest czynnik znaczący w małych i wielkich laboratoriach. Z kolei analiza czasu ma na celu synchronizację zegarów systemowych oraz harmonogramy pracy systemów i uczestników.

W tej fazie testu penetracyjnego będziemy zbierali wymienione informacje (a także wiele innych), ale całą operację podzielimy na dwie odmienne czynności: pasywne i aktywne zbieranie informacji, jak to zostało zasugerowane przez ISSAF. Mimo że dokument ten ma pewne istotne wady, tak naprawdę sprawdza się doskonale, dostarczając krok po kroku poleceń, jak zebrać niezbędne informacje. W tym rozdziale przeanalizujemy pewne wady nieodłącznie towarzyszące metodologii ISSAF. Jednak przedstawione tutaj sugestie mają za zadanie pomóc zrozumieć cele w wykonywanych krokach oraz wzbogacić wiedzę, aby w ten sposób zwiększyć Twoje umiejętności i efektywność podczas przeprowadzania testu penetracyjnego.

PASYWNE ZBIERANIE INFORMACJI

Jak wcześniej wspomniano, pasywne zbieranie informacji dotyczy gromadzenia danych przechowywanych w systemach, które nie znajdują się w sieci klienta. Podczas fazy zbierania informacji przeprowadzanych jest wiele rodzajów operacji wyszukiwania,

obejmujących dane niekoniecznie związane z siecią będącą celem ataku, na przykład informacje o pracownikach, o fizycznym położeniu i o działalności biznesowej. Poniżej wymieniono różne rodzaje danych, które mogą być zbierane na tym etapie.

- Ustalenie obecności celu ataku w sieci (uwaga: nie dotyczy to jedynie stron internetowych).
- Zgromadzenie zwracanych przez wyszukiwarki internetowe wyników dotyczących celu ataku.
- Wyszukanie grup internetowych zawierających komentarze pracowników firmy.
- Przeanalizowanie witryn domowych pracowników firmy.
- Zebranie informacji dotyczących zabezpieczeń oraz wszelkich danych finansowych o firmie będącej celem ataku.
- Sprawdzenie wszelkich witryn podających dane statystyczne o długości nieprzerwanego działania.
- Przejrzenie archiwalnych witryn internetowych w celu znalezienia dodatkowych informacji.
- Przeanalizowanie ofert pracy publikowanych przez cel ataku.
- Przejrzenie grup dyskusyjnych.
- Przeszukanie portali społecznościowych w celu zebrania informacji udostępnianych przez pracowników firmy.
- Sprawdzenie informacji podawanych firmie zajmującej się rejestracją i obsługą domen.
- Sprawdzenie, czy cel ataku udostępnia informacje DNS za pomocą usługi oferowanej przez firmę trzecią.

Po zakończeniu tej fazy osoba przeprowadzająca test penetracyjny będzie miała sporo informacji dotyczących celu ataku, nawet pomimo faktu, że jeszcze nie odwiedziła sieci będącej celem ataku. Wszystkie informacje zgromadzone w trakcie fazy pasywnego zbierania informacji pochodzą z zasobów firm trzecich, które zebrały dane o naszym celu ataku lub mają prawo tego rodzaju dane przechowywać.

Na końcu omawianej fazy osoba przeprowadzająca test penetracyjny może być zaskoczona ilością dostępnych w internecie informacji, nawet tych, które nie powinny być ujawniane. Po wykonaniu przedstawionych w rozdziale przykładów dotyczących gromadzenia informacji przekonasz się, jak trudno zachować prywatność i jak wiele zmieniło się w ostatnich dekadach na skutek gwałtownego rozwoju internetu.

Obecność w sieci

Ta faza bardzo często pozwala na zdobycie cennych danych dotyczących firmy klienta, na przykład informacji o pracownikach, lokalizacji fizycznej i logicznej, typów używanych systemów (między innymi marek i systemów operacyjnych), a także informacji o architekturze sieci. Na szczęście ta faza testu penetracyjnego opiera się na bardzo prostych narzędziach wymienionych w metodologii ISSAF. Są to:

- przeglądarka internetowa,
- Dogpile.com,
- Alexa.org,
- Archive.org,
- Shodanhq.com,
- dig,
- nslookup.

Do zdobycia informacji o celu wykorzystamy przede wszystkim witryny internetowe wymienione na powyższej liście, choć skorzystamy także z kilku innych witryn. Jak zwykle podręcznik OSSTMM nie zawiera żadnych zalecanych narzędzi i sugeruje oprzeć się na doświadczeniu osoby przeprowadzającej test penetracyjny i jej umiejętności wyboru najodpowiedniejszych i najbardziej użytecznych narzędzi. Witryny internetowe wymienione w dokumencie ISSAF, jak również użycie przeglądarki internetowej nie wymagają dalszych objaśnień. Prawdziwa trudność polega na zrozumieniu, jakich informacji szukamy. Odpowiedź brzmi: wszystkiego, co można znaleźć.

Poniżej przedstawiono listę sugerowanych informacji, których warto poszukać. Oczywiście lista ta na pewno nie jest kompletna. Elementy listy można dodawać (lub usuwać) w zależności od rodzaju podpisanej umowy i systemów będących celem ataku. Jednak poniższa lista stanowi dobry punkt wyjścia i powinna pomóc w określeniu innych rodzajów informacji, które mogą być dostępne w zależności od celu ataku. Im więcej informacji uda się zebrać w tej fazie, tym łatwiej będzie można wykonywać kolejne zadania.

- Adres (lub adresy) witryn internetowych.
- Typ serwera WWW.
- Położenie serwera.
- Daty, łącznie z datami ostatniej modyfikacji.
- Łącza internetowe — zarówno wewnętrzne, jak i zewnętrzne.
- Drzewo katalogów serwera WWW.
- Używane technologie (sprzęt i oprogramowanie).
- Standardy szyfrowania.
- Użyte sieciowe języki programowania.
- Pola (w tym również ukryte) formularzy sieciowych.
- Zmienne formularzy.
- Metoda przekazywania formularzy do serwera WWW.
- Informacje kontaktowe firmy.
- Znaczniki meta.
- Wszelkie komentarze na stronach internetowych.
- Możliwości w zakresie e-commerce'u.
- Oferowane usługi i produkty.

Ostrzeżenie

Informacje zebrane w tej fazie mogą nie być upublicznione. Bardzo ważne jest, aby osoba przeprowadzająca test penetracyjny traktowała te wszystkie informacje jako „zastrzeżone", nawet jeśli zostały znalezione w publicznie dostępnych witrynach internetowych.

Ze względu na to, że koncepcje znacznie łatwiej zrozumieć przez *działanie*, a nie tylko czytanie o nich, przejdziemy teraz do przykładu praktycznego. Kiedy będziesz wykonywać kroki przedstawione w książce, pamiętaj, że informacje mogły ulec zmianie od chwili jej pisania. Jednak celem ćwiczenia jest przekonanie się, dlaczego zbieramy niezbędne informacje, a nie przedstawienie kolejnych kroków do wykonania, ponieważ takie rozwiązanie okazuje się po prostu nieelastyczne i prowadzi do powstania luk w wiedzy. Dzięki zrozumieniu, *dlaczego* wykonujemy działania przedstawione w tej fazie, zyskasz większe umiejętności w zakresie przeprowadzania profesjonalnego testu penetracyjnego niż w przypadku ich wykonywania zawsze w ten sam sposób, przez powtarzanie tych samych kroków wyuczonych na pamięć.

Przyjmujemy założenie, że nigdy nie słyszeliśmy o narzędziu nmap. Jeżeli użyjemy wyszukiwarki internetowej w celu zdobycia bogatszych informacji na temat wymienionego narzędzia i jego twórcy, wtedy prawdopodobnie trafimy na trzy różne witryny internetowe powiązane z narzędziem nmap, jak pokazano na rysunku 6.1. Witryna *http://nmap.org/* wydaje się naturalnym wyborem, ale *http://insecure.org/* i *http://sectools.org/* zdają się być pośrednio powiązane ze skanerem nmap.

Insecure.Org - Nmap Free Security Scanner, Tools & Hacking resources
Network Security Tools/Software (Free Download) including Nmap Open Source Network Security Scanner; Redhat Linux,Microsoft Windows,FreeBSD,UNIX Hacking.
insecure.org/ - Similar pages

Download the Free Nmap Security Scanner for Linux/MAC/UNIX or Windows
Official Download site for the Free Nmap Security Scanner. Helps with network security, administration, and general hacking.
nmap.org/download.html - 2 hours ago - Similar pages

Chapter 8. Remote OS Detection
Chapter 8. Remote OS Detection. Table of Contents. Introduction · Reasons for OS Detection · Determining vulnerability of target hosts · Tailoring exploits ...
nmap.org/book/osdetect.html - Similar pages

Nmap: The Art of Port Scanning
The Art of Port Scanning - by Fyodor. WARNING: this page was last updated in 1997 and is completely out of date. If you aren't here for historical purposes, ...
nmap.org/nmap_doc.html - Similar pages

Top 100 Network Security Tools
Review of the top 100 network security tools (free or commercial), as voted on by 3200 Nmap Security Scanner users.
sectools.org/ - Similar pages

RYSUNEK 6.1.
Witryny internetowe zawierające informacje o narzędziu nmap

Zanim przejdziemy do kolejnego kroku, warto przypomnieć, że to dopiero połowa fazy zbierania informacji. Jak dotąd gromadzimy dane, nawet nie dotykając systemu lub sieci będącej celem ataku — oznacza to, że nie klikamy łączy wyświetlonych w wynikach wyszukiwania. Bez wątpienia pojedyncze kliknięcie i przejście na stronę internetową celu nie spowoduje wywołania alarmu — w końcu firma będąca naszym celem chce, aby jej witryna internetowa była odwiedzana i dlatego wspomniana witryna jest dostępna w internecie. Jednak bardzo ważne jest zrozumienie, jak wiele informacji można po prostu znaleźć w innych zasobach internetu. Ponadto duża ilość interesujących nas danych nie znajduje się już w witrynie internetowej celu, ale została zachowana w archiwach internetu. Inną zaletą pasywnego zbierania informacji jest to, że im później pojawisz się na radarze celu ataku, tym lepiej, zwłaszcza gdy inżynierowie odpowiedzialni za sieć klienta wiedzą o zleceniu na przeprowadzenie testu penetracyjnego. Im mniej *szumu*, tym mniejsze prawdopodobieństwo, że administratorzy systemu spróbują zabezpieczyć go przed penetracją.

W dalszej części testu penetracyjnego sprawdzimy, jak administratorzy reagują na próbę włamania. Teraz z pewnością nie chcemy, aby zaczęli dokładniej analizować dzienniki zdarzeń i blokować nasze działania już na wczesnym etapie testu penetracyjnego.

Warto pamiętać, że w trakcie omawianej fazy wreszcie dotrzemy do usług innych niż WWW, co niewątpliwie zwiększy niebezpieczeństwo wykrycia naszej działalności. Im dłużej pozostajemy niewykryci i unikamy kontaktu z siecią będącą celem ataku, tym lepiej dla nas.

Mamy więc trzy witryny internetowe związane z celem. Przystępujemy do zdobycia nieco większej ilości informacji. Z przedstawionej wcześniej listy narzędzi wybieramy teraz witrynę *http://www.alexa.com/*. Na rysunku 6.2 pokazano wyraźnie, że według Alexa.org witryny *http://nmap.org/* i *http://insecure.org/* są powiązane, ponieważ łącze *Site info* witryny *http://nmap.org/* wskazuje witrynę *http://insecure.org/*. Jeżeli wykonasz to samo zapytanie, dokonasz kolejnego interesującego odkrycia, pokazanego na rysunku 6.3. Wydaje się, że witryna *http://nmap.org/* obsługuje subdomeny, na co wskazuje istnienie jednej z nich — scanme.nmap.org. Ponadto nazwa sugeruje możliwość przeprowadzenia skanowania odkrytej subdomeny. Skoro jesteśmy na etapie pasywnego zbierania informacji i nie chcemy połączyć się z siecią będącą celem ataku, wstrzymamy się teraz z przeprowadzeniem operacji skanowania.

RYSUNEK 6.2.
Wyświetlone przez Alexa.org wyniki dla zapytania nmap

Go ahead and ScanMe!
Hello, and welcome to Scanme.Nmap.Org, a service provided by the Nmap Security Scanner Project and Insecure.Org. We set up this machine to help folks learn about Nmap and also to ...
scanme.nmap.org
Site info for insecure.org

RYSUNEK 6.3.
Informacje dodatkowe dotyczące witryny nmap.org

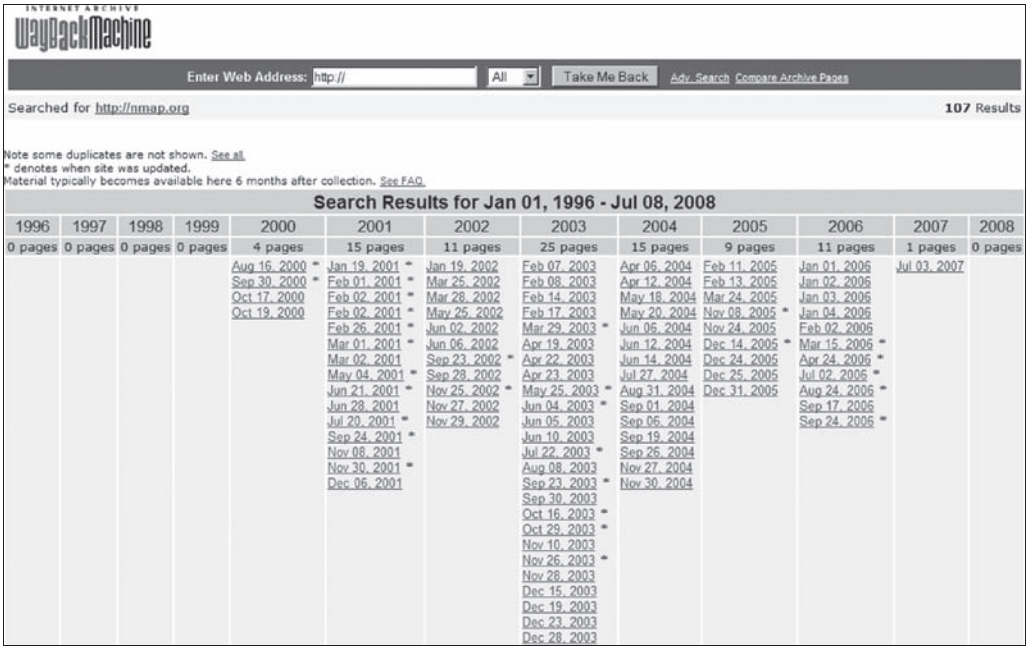
Jeżeli w witrynie Alexa.org te same zapytania wykonamy dla domen insecure.org i sectools.org, uzyskamy informacje podobne jak w przypadku witryny nmap.org, łącznie z istnieniem subdomeny scanme.insecure.org. Na tym etapie po dodaniu nowego celu do listy możemy powrócić na początek fazy zbierania informacji i dołączyć nowe adresy URL do listy witryn przeznaczonych do sprawdzenia. Gromadzenie danych to najczęściej odpowiedni krok. Jednak ostateczną decyzję pozostawiam Tobie — powtórzenie tutaj tych samych działań nie przyczyni się do lepszego zrozumienia zaprezentowanych wcześniej kroków.

Zdobyliśmy pewną ilość informacji dotyczących witryny nmap.org, a więc możemy już przystąpić do odwiedzenia samej witryny internetowej — na tym etapie także nie dotykamy bezpośrednio systemu będącego celem ataku. Istnieje kilka witryn internetowych archiwizujących bieżące i dawne strony znajdujące się w serwerze WWW naszego celu. Do wspomnianych witryn zalicza się między innymi google.com, ale rozpoczniemy od archive.org, czyli witryny pozwalającej na obserwację zmiany danej witryny internetowej w ciągu lat. Zaletą archive.org jest przechowywanie informacji, które nie są dłużej dostępne za pomocą Google'a ani obecne w bieżącej wersji docelowej witryny internetowej.

Wskazówka

Witryna archive.org nie oferuje archiwum z ostatnich sześciu miesięcy. Jeżeli potrzebujesz jednej z najnowszych migawek strony internetowej, powinieneś skorzystać z oferowanej przez Google'a funkcji buforowania strony.

Na rysunku 6.4 pokazano wyniki zapytania w witrynie archive.org. Jak możesz się przekonać, witryna nmap.org była archiwizowana przez wiele lat, począwszy od 2000 roku. Teraz zapoznamy się z jedną z ostatnich wersji witryny, wprowadzoną 24 września 2006 roku. Istnieje jeszcze nowsza wersja, ale według archive.org nie różni się zbytnio od wersji z 24 września 2006 roku. Jeżeli przeprowadzasz prawdziwy test penetracyjny, wówczas prawdopodobnie przejrzysz wszystkie dostępne łącza, aby przekonać się, jakie informacje zostały dodane lub usunięte w trakcie kolejnych uaktualnień. Witryny internetowe zmieniają się z różnych powodów. Nas najbardziej interesuje jeden z nich, czyli naprawa pomyłek związanych z ujawnieniem informacji wrażliwych o sieci, serwerze lub personelu.

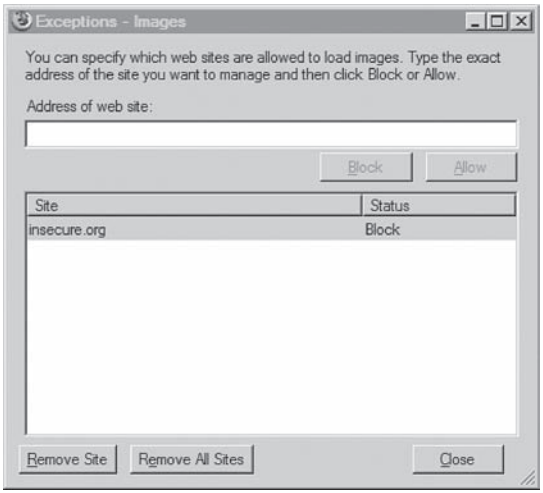


RYSUNEK 6.4.
Wyniki zapytania wykonanego w witrynie archive.org

Zanim przejdziesz dalej, powinieneś wiedzieć, że pewne zarchiwizowane strony mogą nawiązywać połączenie z serwerem WWW będącym celem ataku. Tego rodzaju połączenie jest bardzo często wykonywane w celu pobrania obrazów. Skoro jesteśmy na etapie pasywnego zbierania informacji, chcemy jak najdłużej pozostać niewykryci i dlatego powinniśmy zabronić przeglądarce internetowej pobierania obrazów z witryny insecure.org. Wprawdzie tego rodzaju rozwiązanie jest ekstremalne nawet w trakcie rzeczywistego testu penetracyjnego, ale w ten sposób zmniejszamy ryzyko choćby przypadkowego nawiązania połączenia z celem ataku. Wspomniane ograniczenie można nałożyć przez zdefiniowanie wyjątku w przeglądarce internetowej. Na przykład w przeglądarce Firefox przejdź do *Narzędzia/Opcje/Treść* i kliknij przycisk *Wyjątki…* umieszczony obok *Pobieraj obrazki automatycznie*[1]. Na rysunku 6.5 pokazano okno dialogowe, w którym widać wyjątek zdefiniowany dla witryny insecure.org. Wprawdzie nie uniemożliwi to wszelkich kontaktów z systemem będącym celem ataku, ale stanowi dodatkowy poziom kontroli. Takie rozwiązanie jest również wystarczające na potrzeby pokazania, jak zbierać informacje bez przeprowadzania bezpośredniej komunikacji z celem.

Po wybraniu wyniku z 24 września 2006 roku na ekranie zostanie wyświetlona witryna z podanego dnia (zob. rysunek 6.6). Od razu można dostrzec, że witryny insecure.org i sectools.org są ze sobą powiązane za pomocą obrazów używanych w obu tych portalach.

[1] W nowszych wersjach przeglądarki Firefox wymieniona opcja w ustawieniach została usunięta — *przyp. tłum.*



RYSUNEK 6.5.
Wyłączenie automatycznego pobierania obrazów z witryny insecure.org

Narzędzia i pułapki

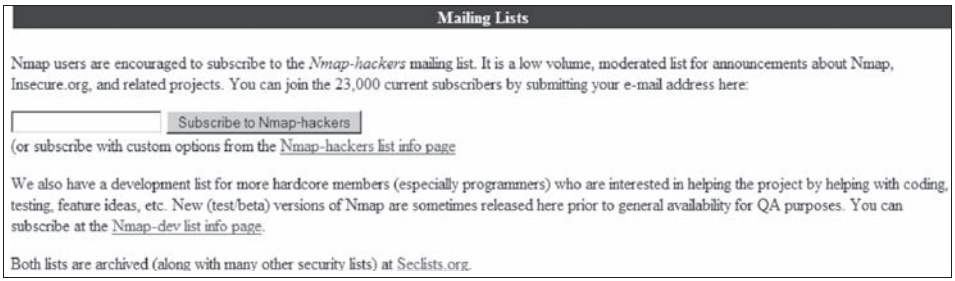
Całkowite wyłączenie dostępu do systemu będącego celem ataku

Jeżeli chcesz w maksymalnym stopniu zapewnić sobie niewykrywalność, wtedy na etapie zbierania informacji możesz zablokować wszystkie połączenia z witryną internetową celu. Pewne witryny internetowe, na przykład google.com i archive.org, będą nawiązywały połączenia z serwerem WWW celu, jeśli nie zostaną podjęte dodatkowe środki bezpieczeństwa. Oczywiście możliwość dostępu do wspomnianej witryny internetowej celu można włączyć z powrotem na dalszym etapie testu penetracyjnego. W systemie Microsoft Windows ograniczenie dostępu do systemu docelowego można przeprowadzić za pomocą przycisku *Opcje internetowe*, a dokładnie przez dodanie witryny do strefy *Witryny z ograniczeniami*.

RYSUNEK 6.6.
Buforowana przez archive.org witryna internetowa nmap.org

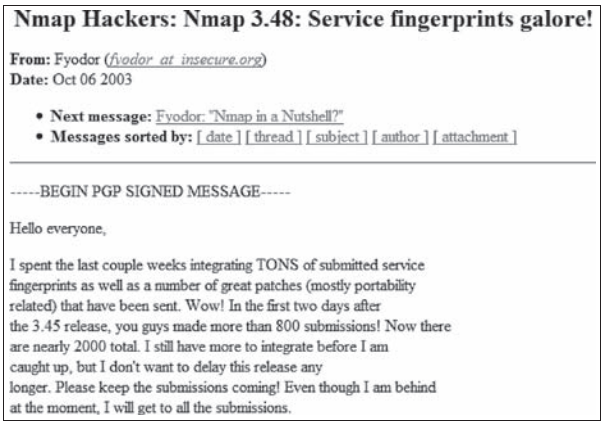
Aby zebrać maksymalną ilość informacji o witrynie będącej celem ataku, należy kliknąć wszystkie łącza wyświetlone na stronie, w szczególności te, które znajdują się w lewej kolumnie. Po kliknięciu łącza *Intro* (przenoszącego nas na stronę: *http://web.archive.org/web/20060303150420/www.insecure.org/nmap/* nadal dostępną w archiwum archive.org) odkrywamy wiele różnych informacji, w tym łącza do wiadomości o licencji, opis narzędzia nmap, łącza do dokumentacji i tak dalej.

Przewijając stronę do dołu, docieramy do list dyskusyjnych, jak pokazano na rysunku 6.7. Jeżeli analizujemy łącze seclists.org (wymienioną nazwę domeny należy dodać do listy witryn powiązanych z narzędziem nmap), odkrywamy łącza prowadzące do archiwalnych postów w różnych listach dyskusyjnych, w tym także dotyczących narzędzia nmap. Archiwum dostępne w witrynie archive.org obejmuje wiadomości z lat 2000 – 2004 i zawiera użyteczne informacje o narzędziu nmap, nawet pomimo braku wzmianki o dostępności danych sprzed roku 2004.



RYSUNEK 6.7.
Informacje dotyczące list dyskusyjnych w witrynie insecure.org

Po przeczytaniu wybranych postów odkryjemy adres e-mail autora narzędzia (Fyodora, jak się wkrótce okaże; jego prawdziwe imię i nazwisko to Gordon Lyon), co pokazano na przykładowym fragmencie na rysunku 6.8. Odkrywamy także nowe adresy e-mail, które zaczynamy dodawać do innych zebranych podczas analizy archiwum listy dyskusyjnej.



RYSUNEK 6.8.
Fragment pobrany z listy dyskusyjnej poświęconej narzędziu nmap

Zanim opuścimy kilka ostatnich rysunków, warto spojrzeć na formularz subskrypcji listy dyskusyjnej, który pokazano wcześniej na rysunku 6.7. Dzięki analizie kodu źródłowego (w witrynie archive.org) wspomnianego formularza zyskujemy wiedzę na temat sieci i systemów celu ataku. Kod źródłowy formularza przedstawia się następująco:

```
<FORM ACTION="/cgi-bin/subscribe-nmap-hackers.cgi" METHOD="GET">
<INPUT TYPE="text" NAME="emailaddy" SIZE=20>
<font color="#000000"><INPUT TYPE="submit" VALUE="Subscribe to Nmap-hackers"></font>
</FORM>
```

Nie jest to zbyt ekscytujący kod (brak ukrytych pól formularza sieciowego), ale dostarcza pewnych informacji, takich jak fakt istnienia katalogu */cgi-bin* oraz używania metody GET protokołu HTTP. W systemie docelowym znajduje się jeszcze jeden formularz sieciowy, używany do przeprowadzenia operacji wyszukiwania i łączący się z Google'em. Na tym etapie testu penetracyjnego nie jest to dla nas szczególnie interesujące. Jednak dzięki zebraniu tego rodzaju informacji można się dowiedzieć o użyciu w systemie docelowym aplikacji, która ma znane luki w zabezpieczeniach. Wykorzystywanie wspomnianych aplikacji można bardzo często odkryć tylko przez analizę kodu źródłowego stron internetowych.

Czego jeszcze możemy się dowiedzieć o naszym celu ataku? Przeanalizujmy kwestię subdomen. Dokument ISSAF sugeruje użycie witryny internetowej netcraft.com do wyszukania listy wszystkich subdomen powiązanych z daną witryną internetową. Na rysunkach od 6.9 do 6.11 pokazano subdomeny, które według netcraft.com istnieją dla naszego celu ataku.

Results for .insecure.org

Found 4 sites

	Site	Site Report	First seen	Netblock	OS
1.	cgi.insecure.org		november 2003	titan networks	linux - fedora
2.	download.insecure.org		febuary 2002	new dream network, llc	linux
3.	www.insecure.org		march 1998	titan networks	linux - fedora
4.	images.insecure.org		november 2002	titan networks	linux - fedora

RYSUNEK 6.9.
Wynik zapytania insecure.org w witrynie netcraft.com

Results for .sectools.org

Found 1 site

	Site	Site Report	First seen	Netblock	OS
1.	mirror.sectools.org		may 2007	titan networks	linux - fedora

RYSUNEK 6.10.
Wynik zapytania sectools.org w witrynie netcraft.com

Results for .nmap.org

Found 2 sites

	Site	Site Report	First seen	Netblock	OS
1.	scanme.nmap.org		october 2005	titan networks	linux - fedora
2.	www.nmap.org		may 2000	titan networks	linux - fedora

RYSUNEK 6.11.
Wynik zapytania nmap.org w witrynie netcraft.com

Podstawową witryną dla Fyodora wydaje się insecure.org — zawiera trzy subdomeny. Wracając z powrotem do archive.org, subdomena download.insecure.org wygląda na stronę z nowościami wyświetlaną na stronie głównej witryny. Niczego nowego tutaj nie znajdziemy. A co z subdomeną images.insecure.org? Jeżeli przeanalizujesz łącze, znajdziesz tekst odwołujący się do firmy VA Linux Systems, Inc, która później stała się VA Software Corporation, a następnie SourceForge, Inc. Wydaje się, że subdomena jest nadal używana, ale strona początkowa nie została zmodyfikowana od dość długiego czasu. Taka informacja może być użyteczna w przyszłości, ale teraz jest tylko interesującym drobiazgiem. Użyteczne informacje to również te dotyczące systemu operacyjnego. Wykorzystamy je na dalszym etapie testu penetracyjnego.

Wprawdzie wspomniane subdomeny mogą zawierać dodatkowe katalogi z użytecznymi dla nas informacjami, ale pobieżne przejrzenie Google'a i witryny archive.org nie wskazuje na istnienie czegokolwiek w odkrytych subdomenach. Prowadząc dalszą analizę, możemy powrócić do Google'a i wykonać zapytanie `site:cgi.insecure.org`, którego wykonanie daje 46 różnych stron, łącznie z prezentacjami przedstawianymi na konferencjach dotyczących bezpieczeństwa. (Może to być niezwykle pomocne w lepszym zapoznaniu się z działaniem narzędzia, ale niekoniecznie ma związek z przeprowadzanym przez nas testem penetracyjnym, jeśli rzeczywiście chcemy taki wykonać). W przypadku subdomen nadzieje na zdobycie większej ilości informacji dotyczących witryny i narzędzia nmap wiążemy z cgi.insecure.org, ponieważ odkryty wcześniej katalog */cgi-bin* zawiera skrypty, które ewentualnie mogą zawierać możliwe do wykorzystania luki w zabezpieczeniach.

Wyszukanie mirror.sectools.org za pomocą Google'a i witryny archive.org nie przynosi wyników. Chociaż domena może zawierać przydatne dla nas informacje, na tym etapie nie zgromadzimy większej ilości danych, dopóki nie nawiążemy połączenia z celem ataku. W przeciwnym razie niczego więcej nie znajdziemy już w archiwalnych rekordach. Warto wrócić do wspomnianej subdomeny później, gdy cel będziemy dokładniej analizować podczas testu penetracyjnego.

Wykonanie zapytania scanme.nmap.org w witrynie archive.org nie przynosi wyników. Z kolei po przejściu do Google'a możemy zobaczyć buforowaną wersję witryny. Na rysunku 6.12 pokazano, co się znajduje (a raczej *znajdowało* się) na stronie. Okazuje się, że dzięki Fyodorowi dysponujemy w internecie celem, względem którego można przeprowadzić skanowanie. Możliwość tę wykorzystamy później, w trakcie doskonalenia technik skanowania w internecie.

This is Google's cache of http://scanme.nmap.org/. It is a snapshot of the page as it appeared on Sep 22, 2008 11:29:33 GMT. The current page could have changed in the meantime. Learn more

Text-only version

Hello, and welcome to Scanme.Nmap.Org, a service provided by the Nmap Security Scanner Project and Insecure.Org.

We set up this machine to help folks learn about Nmap and also to test and make sure that their Nmap installation (or Internet connection) is working properly. You are authorized to scan this machine with Nmap or other port scanners. Try not to hammer on the server too hard. A few scans in a day is fine, but dont scan 100 times a day or use this site to test your ssh brute-force password cracking tool.

Thanks
-Fyodor

RYSUNEK 6.12.
Buforowana wersja strony scanme.nmap.org

Według Google'a z analizowaną subdomeną nie są powiązane żadne inne strony. Ponownie istnieje możliwość, że dowiemy się więcej po faktycznym nawiązaniu połączenia z atakowanym celem. Jednak teraz jesteśmy zadowoleni z poczynionych odkryć.

Dane korporacyjne

Ten krok pozwoli nam lepiej zrozumieć, kto stoi za narzędziem nmap, gdzie się znajduje, czy i jakich zatrudnia pracowników, a być może odkryjemy także jakieś informacje dotyczące sieci. W tym miejscu trzeba koniecznie zwrócić uwagę na to, jak głęboko zejdziemy na tym etapie testu penetracyjnego. Jeśli poświęcimy odpowiednią ilość czasu, istnieje duże prawdopodobieństwo odkrycia informacji osobistych, takich jak miejsca zamieszkania pracowników korporacji lub ich prywatne numery telefonów. Jeżeli nie jest wymagane przeprowadzenie działań z zakresu socjotechniki, to zbierając tego rodzaju informacje, możesz przekroczyć granice etyczne. Nawet jeśli wspomniane informacje są dostępne, nie oznacza to, że musisz je zgromadzić.

To samo dotyczy prywatnych stron internetowych pracowników korporacji, na przykład ich blogów lub witryn związanych z rodziną. Być może uda się tam znaleźć pewne użyteczne informacje, takie jak uzyskane przez inżynierów certyfikaty z zakresu systemów operacyjnych lub aplikacji. Jednak nie oznacza to, że o pracownikach korporacji powinieneś gromadzić informacje takie, jak ich znaki zodiaku lub zdjęcia bliskich (to będzie wyjątkowo podłe). Pamiętaj o zachowaniu równowagi między informacjami faktycznie użytecznymi a po prostu dostępnymi.

Spójrzmy na strony informacyjne witryn insecure.org i sectools.org (w tym przypadku mamy tylko dwie wymienione opcje, ponieważ łącze z witryny nmap.org prowadzi do witryny insecure.org). Na rysunku 6.13 pokazano informacje kontaktowe obejmujące adres siedziby, numer telefonu i adres e-mail. W przypadku witryny sectools.org informacje pozostają takie same, poza adresem e-mail. Zwróć uwagę na nazwę firmy — Insecure.com — która w ten sposób dostarcza nam jeszcze jedną nazwę domeny do sprawdzenia.

Company Info for insecure.org:

Insecure.Com Llc
370 Altair Way #113
Sunnyvale, CA
94086
US

Phone: +1 530 323 8588
hostmaster [at] insecure.org

RYSUNEK 6.13.
Informacje o firmie, które znajdziemy w witrynie insecure.org

W jaki sposób możemy wykorzystać zebrane informacje? Jeżeli mamy fizycznie sprawdzić bezpieczeństwo siedziby, więcej informacji można zdobyć za pomocą map Google'a. Na rysunku 6.14 pokazano położenie na mapie Google'a adresu widocznego na rysunku 6.13, a także informacje dotyczące budynku. Na podstawie znalezionych tutaj informacji dowiadujemy się, że firma Insecure.com do prowadzenia biznesu korzysta ze skrzynki pocztowej.

RYSUNEK 6.14.
Wynik w mapach Google'a otrzymany po podaniu adresu firmy Insecure.com

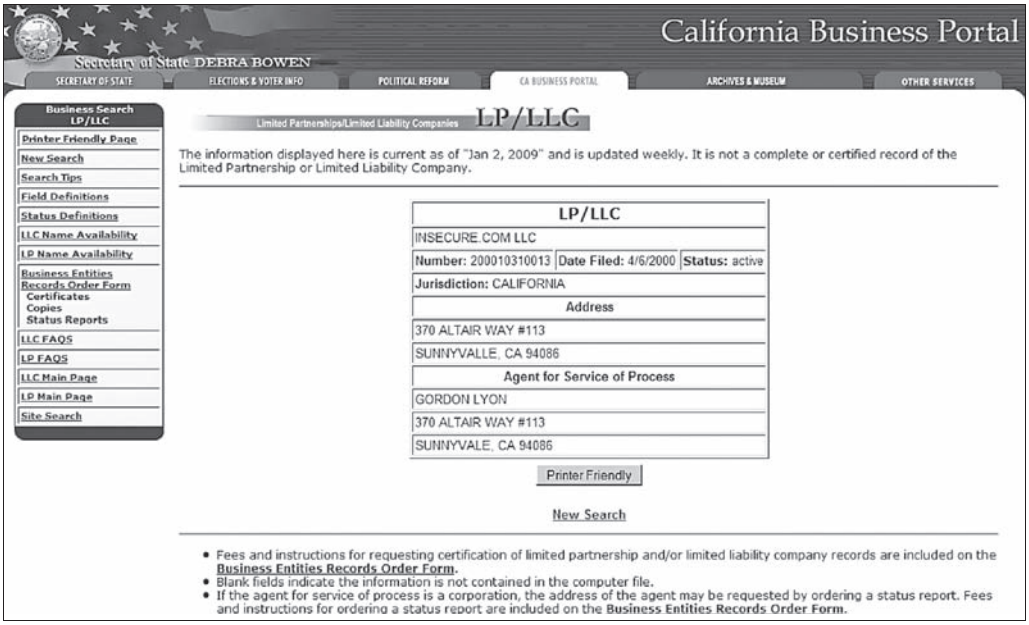
Jeżeli adres wskazywałby budynek dużej korporacji, opcja *Street View* dostarczyłaby wielu użytecznych szczegółów, takich jak budynki przyległe lub znajdujące się po drugiej stronie ulicy, położenie drzwi, okien, drogi wejścia/wyjścia, a także być może pewnych informacji dotyczących zabezpieczeń, na przykład oświetlenia, monitoringu, kontroli dostępu. Jeżeli te informacje nie są wystarczające, wtedy można wykorzystać Google Earth (*http://www.google.com/earth/*) w celu przejrzenia widoku satelitarnego okolicy, co może dostarczyć wielu informacji dodatkowych, takich jak parkingi, inne drogi i tak dalej. Użycie map Bing (*http://www.bing.com/maps/*) również może dać inny punkt widzenia, pozwalając nam na użycie wielu narzędzi do tego samego celu, a tym samym zwiększając możliwość zidentyfikowania unikalnych danych.

Analizę archiwum możemy prowadzić dalej, aby się przekonać, czy uda się zebrać jeszcze inne informacje dotyczące narzędzia nmap lub Fyodora. Jednak po przejściu do Google'a i wykonaniu zapytania „nmap fyodor palo alto" odkryjemy następujące łącze do Wikipedii: *http://en.wikipedia.org/wiki/Gordon_Lyon*. Na tym etapie już wiemy, kim jest

autor narzędzia nmap. W chwili pisania tej książki w wymienionym artykule Wikipedii znajdowało się również zdjęcie Gordona. Teraz oprócz nazwiska znamy też twarz Gordona, choć nie przekłada się to na żaden praktyczny sposób użycia. Jednak zdjęcia pracowników korporacji będącej celem ataku mogą być niezwykle użyteczne w innych projektach testów penetracyjnych, zwłaszcza w tych, które wymagają zastosowania socjotechniki.

Skoro doskonale wiemy, że informacje opublikowane w Wikipedii mogą być nieprawdziwe, warto poszukać innych źródeł informacji o właścicielu interesujących nas witryn internetowych. Powracając do rysunku 6.13, przypominamy sobie, że nazwa firmy to Insecure.com. Zaletą szukania informacji o firmie jest fakt, że firmy są rejestrowane przez organy administracji państwowej. W przypadku Insecure.com odkrywamy, że firma znajduje się w stanie Kalifornia, którego władze przygotowały portal zawierający informacje związane z firmami zarejestrowanymi w tym stanie.

Na rysunku 6.15 możesz zobaczyć wynik wykonania zapytania dotyczącego firmy Insecure.com. Według informacji dostępnych na stronie *http://www.sos.ca.gov/business/* właścicielem firmy jest Gordon Lyon, co potwierdza dane zamieszczone w Wikipedii.



RYSUNEK 6.15.
Informacje o firmie Insecure.com znajdujące się w portalu prowadzonym przez władze Kalifornii

Informacje z portalu stanowego potwierdzają także adres (Sunnyvale w Kalifornii) jako siedzibę firmy, co wcześniej zostało przez nas ustalone — tam mieści się firmowa skrzynka pocztowa. Wiemy także, kiedy został złożony wniosek o rejestrację firmy jako spółki o ograniczonej odpowiedzialności. Z powodu kosztów oraz faktu, że informacje o firmach

mają być publicznie dostępne, większość stanów prowadzi portale zawierające dane o firmach, ich właścicielach i siedzibach[2]. Dzięki temu zdobycie wiadomości dotyczących firmy stało się znacznie łatwiejsze i nie wymaga nawet połączenia z siecią sprawdzanej korporacji.

Informacje uzyskane na podstawie whois i DNS

Spójrzmy na informacje DNS dotyczące witryny internetowej nmap.org. Na rysunku 6.16 pokazano wiele informacji, przede wszystkim adres IP witryny (64.13.134.48), łącznie z dodatkowymi subdomenami (*http://mail.nmap.org/*).

NAME SERVERS

Name Server	IP	Location
ns1.titan.net	64.13.134.58	Palo Alto, CA, US
ns2.titan.net	64.13.134.59	Palo Alto, CA, US

ping nmap.org

SOA RECORD

Name Server	ns1.titan.net
Email	hostmaster@insecure.org
Serial Number	2008091400
Refresh	8 hours
Retry	1 hour
Expiry	7 days
Minimum	1 day

DNS RECORDS

Record	Type	TTL	Priority	Content
*.nmap.org	A	1 day		64.13.134.48 (Palo Alto, CA, US)
mail.nmap.org	MX	1 day	0	mail.titan.net
nmap.org	A	1 day		64.13.134.48 (Palo Alto, CA, US)
nmap.org	MX	1 day	0	mail.titan.net
nmap.org	NS	1 day		ns1.titan.net
nmap.org	NS	1 day		ns2.titan.net
nmap.org	SOA	1 day		ns1.titan.net. hostmaster.insecure.org. 2008091400 28800 3600 604800 86400
nmap.org	TXT	1 day		v=spf1 a mx ptr ip4:64.13.134.0/26 -all

RELATED DOMAINS

titan.net	insecure.org
• Whois	• Whois
• Information	• Information
• DNS Records	• DNS Records

RYSUNEK 6.16.
Informacje whois dotyczące witryny internetowej nmap.org

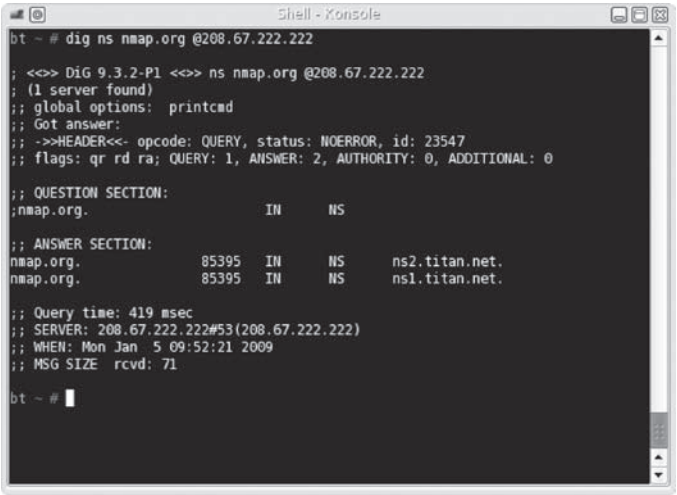
Wydaje się, że witryna nmap.org znajduje się w sieci o nazwie titan.net. Jeżeli pójdziesz za tą informacją, to odkryjesz, że titan.net jest powiązana z firmą DreamHost Web Hosting, co niewątpliwie wykracza poza nasz obszar zainteresowania, ponieważ próbujemy dowiedzieć się czegoś na temat narzędzia nmap i jego twórcy (bądź twórców). Jednak jeśli dalej będziemy prowadzić analizę, to dowiemy się nieco więcej na temat serwerów obsługujących witrynę (AMD Dual Core Opteron lub Intel Dual Processor Xeon), używanych systemów operacyjnych (Linux-VServer lub Debian Linux) oraz potencjalnych usług dostępnych dla użytkowników hostingu (między innymi MySQL,

[2] W Polsce informacje o firmie można sprawdzić w portalu Centralnej Ewidencji i Informacji o Działalności Gospodarczej (*https://prod.ceidg.gov.pl/ceidg.cms.engine/*) — *przyp. tłum.*

POP/IMAP, FTP). W ten sposób zdobędziemy większą wiedzę na temat serwerów, które mają być celem ataku. Kiedy przystąpimy do wykorzystywania luk w zabezpieczeniach systemów będących celem ataku, zdobyte teraz informacje pomogą w zawężeniu liczby potencjalnych luk w zabezpieczeniach, które mogą nas interesować.

Niektóre ze zdobytych teraz informacji będziemy wykorzystywać później, po przejściu do fazy aktywnego zbierania informacji. W ten sposób nie tylko dowiesz się, jak zbierać informacje z poziomu wiersza poleceń, ale również jak zweryfikować te, które zostały zgromadzone w fazie pasywnego zbierania informacji. Zawsze istnieje prawdopodobieństwo, że rekordy pokazane na rysunku 6.16 są nieaktualne (to kolejny powód, dla którego zawsze warto korzystać z dwóch różnych narzędzi do zbierania informacji).

Inny zestaw narzędzi zalecany przez dokument ISSAF do użycia na etapie zbierania informacji to dig i nslookup. Spójrzmy na te narzędzia i przekonajmy się, jak możemy je wykorzystać do naszych celów. Narzędzie dig pozwala na wykonywanie zapytań do serwera nazw w celu pobrania informacji o interesującym nas systemie. Wspomniane informacje mogą być pobierane z dowolnego dostępnego serwera DNS, a nie tylko z obsługującego sprawdzaną domenę. Na rysunku 6.17 pokazano wykonanie zapytania dla witryny nmap.org w celu pobrania informacji od obsługującego ją serwera. Użyty serwer nazw to 208.67.222.222 (resolver1.opendns.com), który jest serwerem dla OpenDNS, czyli firmy oferującej bezpłatną usługę DNS. Będzie to użyteczne, gdy nie jesteś pewien niezawodności działania Twojego dostawcy DNS lub jeśli chcesz po prostu mieć alternatywę.



RYSUNEK 6.17.
Wynik wykonania zapytania za pomocą narzędzia dig

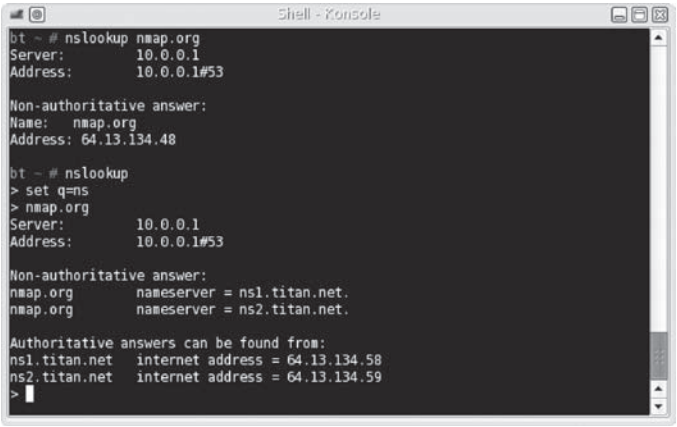
Zapiski z podziemia

OpenDNS.com

Nazwa może być nieco myląca — OpenDNS nie jest oprogramowaniem typu open source, lecz komercyjnym. Dostępne są usługi dodatkowe, o których powinieneś wiedzieć, zanim zaczniesz korzystać z bezpłatnej usługi oferowanej przez OpenDNS. Do wspomnianych usług dodatkowych należą filtry antyphishingowe, blokowanie domen i wyświetlanie odpowiedniego komunikatu podczas próby nawiązania połączenia za pomocą przeglądarki internetowej z nazwą nieistniejącej domeny. W zależności od wymagań OpenDNS może być cennym zasobem lub czymś, czego lepiej unikać.

Uzyskane przez nas informacje pokazują, że titan.net to faktycznie serwer nazw dla nmap.org. Skoro znamy serwer, możemy spróbować dowiedzieć się o nim czegoś więcej.

Kolejne narzędzie, którego użycie jest zalecane w dokumencie ISSAF, to nslookup. Użycie wymienionego narzędzia na obecnym etapie testu penetracyjnego jest bardzo uproszczone. Na rysunku 6.18 pokazano kilka poleceń wykorzystujących narzędzie nslookup zgodnie z sugestiami zamieszczonymi w dokumencie ISSAF. Jednak w wymienionym dokumencie nie ma zbyt wielu informacji dotyczących elastyczności narzędzia nslookup, a także pominięto informacje opcjonalne, które mogą być użyteczne podczas gromadzenia większej ilości danych z celu ataku. Jak wspomniano wcześniej, jest to ogólny problem związany z metodologią ISSAF — w dokumencie przedstawiono opcje narzędzi używanych w przykładach, ale nie omówiono innych możliwych scenariuszy. Niektóre inne opcje narzędzia nslookup zostaną przedstawione w dalszej części rozdziału, w fazie aktywnego zbierania informacji.



RYSUNEK 6.18.
Użycie narzędzia nslookup do zebrania informacji DNS zgodnie z sugestiami zawartymi w dokumencie ISSAF

W późniejszych przykładach wskażemy serwer DNS, z którym narzędzie nslookup ma się połączyć w celu zebrania informacji dodatkowych. Teraz po prostu skorzystamy z domyślnego serwera nazw zdefiniowanego dla analizowanej sieci. Czasami możliwość

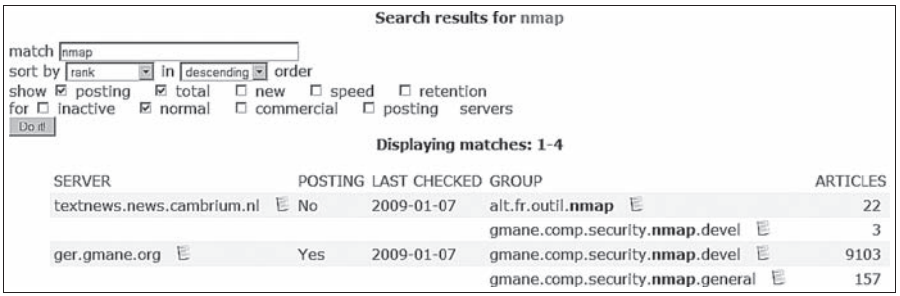
wskazania serwera DNS jest bardzo ważna, ponieważ występuje pewne opóźnienie podczas wprowadzania zmian DNS. Bieżąca faza polega na pasywnym zbieraniu informacji, więc dane nieautorytatywne są wystarczające.

Ostrzeżenie

W pewnych przypadkach bezpośrednie wykonanie zapytania do serwera nazw spowoduje złamanie założonej pasywności. Jeżeli informacje mają być naprawdę zbierane w sposób pasywny, nawiązanie połączenia z nieautorytatywnymi serwerami nazw może być kiepskim pomysłem ze względu na to, kto jest właścicielem serwera.

Dodatkowe zasoby internetowe

Dodatkowy obszar warty sprawdzenia to aktywność w grupach dyskusyjnych. Na rysunku 6.19 można zobaczyć jeden z nowszych postów zamieszczonych na grupie dyskusyjnej poświęconej narzędziu nmap. Grupę dyskusyjną można przeszukać pod kątem nazwy nmap lub adresu URL *http://insecure.org/*, aby przekonać się, co inni mają do powiedzenia na temat narzędzia nmap lub poświęconej mu witryny. Jeżeli przejrzysz grupy dyskusyjne, z reguły znajdziesz użytkowników z całego świata zamieszczających posty dotyczące narzędzia nmap. Istnieje więc realna możliwość zebrania pewnych informacji zarówno o samym narzędziu, jak i o jego witrynie domowej. Pamiętaj, że konieczne jest zebranie wielu informacji, a prawdziwe perełki można czasem znaleźć nawet w obskurnych miejscach.



RYSUNEK 6.19.
Grupa dyskusyjna przeszukana pod kątem nazwy narzędzia nmap — przykład pochodzi z witryny http://freenews.maxbaud.net/

Dokument ISSAF sugeruje także przeanalizowanie celu, aby ustalić, czy znajduje się na liście wymieniającej spam. Jeżeli cel ataku został wymieniony w bazie danych spamu, a nie powinien się w niej znajdować, może to wskazywać na włamanie do serwera poczty w przeszłości. Zgodnie z wynikami pokazanymi na rysunku 6.20 witryna insecure.org nie została dodana do bazy danych spamu, którą można przeglądać pod adresem: *http://www.dnsbl.info/*.

Spam Database Lookup Results for 64.13.134.2

The following are blacklist test results. Being listed with a DNSBL does not always indicate the IP address is a source of spam. Some DNSBL's criteria are based of the IP address' country or connection type. If you are listed with a DNSBL click on the link for removal criteria.

If you are listed with a DNSBL we *cannot* remove you. We can only try to help diagnose the problem and direct you to where you may be able to be delisted (by visiting the DNSBL's website directly.)

asiaspam.spamblocked.com	b.barracudacentral.org	bl.deadbeef.com
bl.emailbasura.org	bl.spamcannibal.org	bl.spamcop.net
blackholes.five-ten-sg.com	blacklist.woody.ch	bogons.cymru.com
cbl.abuseat.org	cdl.anti-spam.org.cn	combined.abuse.ch
combined.rbl.msrbl.net	db.wpbl.info	dnsbl-1.uceprotect.net
dnsbl-2.uceprotect.net	dnsbl-3.uceprotect.net	dnsbl.ahbl.org
dnsbl.cyberlogic.net	dnsbl.inps.de	dnsbl.njabl.org
dnsbl.sorbs.net	drone.abuse.ch	drone.abuse.ch
duinv.aupads.org	dul.dnsbl.sorbs.net	dul.ru

RYSUNEK 6.20.
Sprawdzenie, czy dana witryna została umieszczona w bazie danych spamu

Warto również przejrzeć informacje o poszukiwanych pracownikach, co często dostarcza wiadomości dotyczących sprzętu i oprogramowania używanego przez daną firmę. Poniżej przedstawiono fragment ogłoszenia, w którym firma Google szuka inżyniera (zob. odwołanie na końcu rozdziału).

Wymagania:

- licencjat z informatyki lub podobne doświadczenie;
- doświadczenie w pracy z MySQL (mile widziane doświadczenie w administracji i/lub w dostosowywaniu wydajności MySQL), a także znajomość przynajmniej dwóch z wymienionych języków: Python, Perl, SQL, powłoka;
- podstawowe umiejętności w zakresie rozwiązywania problemów w systemach operacyjnych Linux oraz związanych z siecią;
- doświadczenie w opracowywaniu i/lub obsłudze systemu ETL;
- dodatkowym atutem będzie doświadczenie w zarządzaniu ogromnym systemem z wieloma komponentami;
- kolejnym atutem będzie doświadczenie w zakresie analizy dzienników zdarzeń oraz danych.

Na podstawie powyższych wymagań dowiedzieliśmy się, że firma Google używa gdzieś systemu Linux, bazy danych MySQL oraz programów utworzonych w językach Python i Perl. Ponadto w Google'u istnieje przynajmniej jedna baza danych używająca architektury ETL. Tego rodzaju informacje będą niewątpliwie użyteczne, ponieważ pozwalają na zmniejszenie wysiłku ponoszonego w trakcie projektu, a także na dokładniejsze zdefiniowanie wymagań względem członków zespołu realizującego dany projekt.

AKTYWNE ZBIERANIE INFORMACJI

Na tym etapie testu penetracyjnego można się już mniej przejmować interakcją z siecią będącą celem ataku. Powód jest prosty: zdołaliśmy zebrać sporą ilość informacji dotyczących celu ataku, a tym samym nie ma konieczności dalszego zbierania informacji na dużą skalę. Aktywne zbieranie informacji skutkuje wynikami podobnymi do uzyskanych za pomocą technik zbierania pasywnego. Zalety zastosowania pasywnego zbierania informacji podczas testu penetracyjnego są dwie: identyfikacja informacji historycznych oraz potwierdzenie odkryć w wyniku użycia metod aktywnych.

Dodatkowa umiejętność pozwalająca na zdobycie jeszcze innych informacji to socjotechnika, ale ten temat nie zostanie omówiony w książce. Ujmując rzecz najprościej: socjotechnika oznacza uzyskanie użytecznych (i często nieautoryzowanych) informacji od pojedynczych osób związanych z celem ataku. Socjotechnika to niezwykle efektywna metoda zbierania informacji dotyczących celu — najczęściej znacznie efektywniejsza niż przeprowadzenie skanowania lub podjęcie próby wykorzystania luk w zabezpieczeniach. W tej książce nie będziemy się zajmować użyciem socjotechniki, ponieważ temu tematowi zostało poświęconych wiele innych pozycji wydanych przez Syngress. We wspomnianych pozycjach socjotechnikę omówiono znacznie lepiej, niż mógłbym to zrobić tutaj (ze względu na brak wystarczającej ilości miejsca). Ogólnie rzecz biorąc: korzystaj z dostępnych narzędzi i technik pozwalających na zebranie informacji wymaganych do przeprowadzenia testu penetracyjnego w uzgodnionym zakresie.

Zapytania DNS

Jednym z rodzajów użytecznych informacji jest poznanie wersji serwera BIND (ang. *Berkeley Internet Name Domain*) działającego w naszym celu ataku. Kierując się poleceniami sugerowanymi w dokumencie ISSAF i pokazanymi na rysunku 6.21, odkrywamy, że wersja serwera to 9.3.4. Po przeszukaniu zasobów internetu dowiadujemy się, że wymieniona wersja została wydana w styczniu 2007 roku i nie jest najnowszą wersją serwera. Tych informacji możemy użyć na dalszym etapie testu penetracyjnego w celu sprawdzenia istnienia znanych luk w zabezpieczeniach, które można by wykorzystać. Teraz jedynie zapisujemy odkryte informacje i przechodzimy dalej.

Dokument ISSAF proponuje wydanie jeszcze kilku innych poleceń dig pozwalających na zebranie informacji o serwerach poczty. Jednak tego rodzaju informacje zebraliśmy już wcześniej, o czym możesz się przekonać, ponownie spoglądając na rysunek 6.16. Bardzo ważne jest używanie dwóch różnych narzędzi do tego samego celu i tym samym weryfikacja zbieranych informacji. Zawsze istnieje ryzyko, że witryny informacyjne, takie jak na przykład pokazana wcześniej na rysunku 6.16, zawierają nieaktualne wiadomości. Użycie wiersza poleceń zdecydowanie poprawia dokładność informacji — po prostu zachowaj ostrożność i dokładnie wybieraj systemy, z którymi się łączysz, zwłaszcza jeśli chcesz pozostać niewykryty.

```
Shell - Konsole
bt ~ # dig @ns1.titan.net version.bind chaos txt

; <<>> DiG 9.3.2-P1 <<>> @ns1.titan.net version.bind chaos txt
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61387
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.3.4"

;; AUTHORITY SECTION:
version.bind.           0       CH      NS      version.bind.

;; Query time: 374 msec
;; SERVER: 64.13.134.58#53(64.13.134.58)
;; WHEN: Mon Jan  5 10:48:43 2009
;; MSG SIZE  rcvd: 62

bt ~ #
```

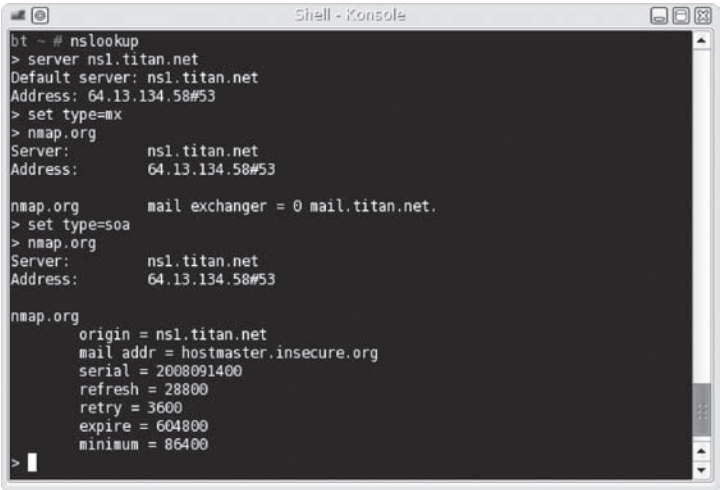
RYSUNEK 6.21.
Wykonanie zapytania w celu ustalenia wersji serwera BIND

Wskazówka

Być może będziesz musiał zapytać klienta, czy koncepcja opóźnień w uaktualnieniach DNS jest problemem, zwłaszcza gdy podstawowym zmartwieniem pozostaje dostępność serwera. Jeżeli serwer nazw zostanie zaatakowany lub przejęty, wtedy propagacja DNS powinna nastąpić jak najszybciej. Niektóre firmy oferujące usługi hostingowe bardzo wolno uaktualniają rekordy DNS.

Zawsze istnieje ryzyko, że domyślny serwer DNS (lub jakikolwiek serwer DNS niepołączony bezpośrednio z serwerem docelowym) będzie miał nieaktualne dane. Dzięki bezpośredniej komunikacji z ns1.titan.net możemy zdobyć aktualne informacje. Ponadto wspomniana komunikacja dostarczy dodatkowych informacji o serwerze poczty, jak również o witrynie nmap.org. Na rysunku 6.22 pokazano dodatkowe polecenia nslookup pozwalające na rozszerzenie naszych poszukiwań. Jak widzisz, za pomocą narzędzia nslookup można zgromadzić znacznie więcej informacji, niż zasugerowano w dokumencie ISSAF.

Narzędzia wiersza poleceń i wykorzystujące je przykłady przedstawione w dokumencie ISSAF są niezwykle użyteczne, ale nie obejmują wszystkich możliwych zapytań. Moim kursantom zalecam nie tylko wykorzystanie narzędzi i wykonanie poleceń przedstawionych w dokumencie ISSAF, ale również poznanie funkcji oferowanych przez poszczególne aplikacje, co pozwoli im w przyszłości na jeszcze lepsze przeprowadzanie testów penetracyjnych.



RYSUNEK 6.22.
Wykonanie dodatkowych poleceń nslookup w celu zebrania informacji dotyczących DNS

Konta poczty elektronicznej

Jeżeli cel ataku ma serwer poczty (jak w omawianym przykładzie), wówczas można spróbować utworzyć listę użytkowników systemu. Wspomniana lista okaże się przydatna nie tylko podczas ataku typu brute force lub podczas logowania, ale również do celów powiązanych z socjotechniką. Według dokumentu ISSAF należy nawiązać bezpośrednie połączenie z serwerem poczty i wykonać zapytania, za każdym razem podając tę samą nazwę użytkownika. Takiej operacji nie możemy przeprowadzić względem serwera poczty nmap.org, ponieważ nie mamy zezwolenia na tego rodzaju działania. Wykorzystamy więc cel ataku umieszczony na stronie internetowej poświęconej książce. Naszym celem stanie się Hackerdemia LiveCD — ta dystrybucja została na to przygotowana, celowo zawiera włączone usługi, na które można przeprowadzać ataki. Jedną z usług jest serwer sendmail. Obraz dysku z dystrybucją Hackerdemia można pobrać ze strony: *http://hackingdojo.com/pentest-media/* (odpowiedniego łącza szukaj w sekcji *Virtual Images*). W rozdziale 3. znajdziesz informacje dotyczące konfiguracji laboratorium do użycia obrazu Hackerdemia lub innej dowolnej dystrybucji LiveCD z wymienionej strony.

Na rysunku 6.23 możesz zobaczyć atak na dystrybucję Hackerdemia LiveCD przeprowadzony za pomocą poleceń zaproponowanych w dokumencie ISSAF. Udało nam się zidentyfikować niektórych użytkowników serwera (`root` i `david`) oraz wykluczyć innych (`anyone` i `michelle`).

Tego rodzaju metoda wymaga wypróbowania różnych nazw użytkowników, po jednej w każdym zapytaniu, jeśli włączone są odpowiednie opcje zachowania prywatności, na przykład pokazane na rysunku 6.23 `novrfy` i `noexpn`. Sam proces może zająć dużo czasu, w zależności od liczby użytkowników serwera oraz stanu naszej wiedzy z zakresu konwencji nazw e-mail.

```
Shell - Konsole
bt ~ # nc -vv 192.168.1.123 25
192.168.1.123: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.1.123] 25 (smtp) open
220 slax.example.net ESMTP Sendmail 8.13.7/8.13.7; Sun, 11 Jan 2009 13:45:27 GMT
EHLO heorot.net
250-slax.example.net Hello [192.168.1.10], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
VRFY root
252 2.5.2 Cannot VRFY user; try RCPT to attempt delivery (or try finger)
EXPN root
502 5.7.0 Sorry, we do not allow this operation
MAIL FROM: twilhelm@slax.example.net
250 2.1.0 twilhelm@slax.example.net... Sender ok
RCPT TO: anyone@slax.example.net
550 5.1.1 anyone@slax.example.net... User unknown
RCPT TO: root@slax.example.net
250 2.1.5 root@slax.example.net... Recipient ok
RCPT TO: david@slax.example.net
250 2.1.5 david@slax.example.net... Recipient ok
RCPT TO: michelle@slax.example.net
550 5.1.1 michelle@slax.example.net... User unknown
 sent 204, rcvd 661
bt ~ #
```

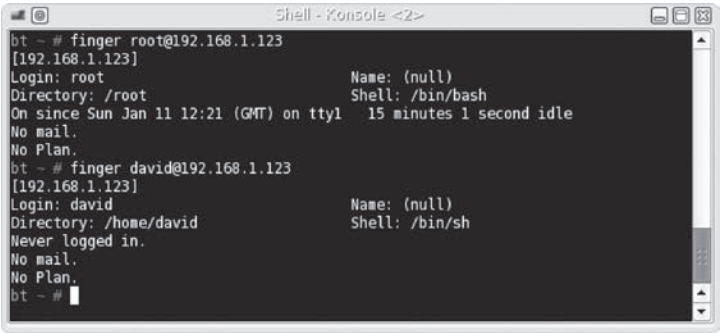
RYSUNEK 6.23.
Wykonywanie zapytań do serwera poczty dystrybucji Hackerdemia LiveCD

Uwaga

Jeżeli chcesz wyłączyć pewne zabezpieczenia dotyczące prywatności i przekonać się, jaka będzie odpowiedź po nawiązaniu połączenia z serwerem sendmail dystrybucji Hackerdemia, wtedy po prostu przeprowadź edycję pliku */etc/mail/sendmail.cf*. Modyfikacja powinna polegać na umieszczeniu komentarza na początku wiersza rozpoczynającego się od `PrivacyOptions`. Konieczne będzie również ponowne uruchomienie serwera sendmail przez wykonanie jako użytkownik `root` polecenia `/etc/rc.d/rc.sendmail restart`.

Na rysunku 6.23 widać sugestię użycia narzędzia finger względem naszego celu ataku. Zwykle trudno jest znaleźć w sieci komputer, w którym włączono możliwość użycia finger. Jednak ponieważ dystrybucja Hackerdemia została opracowana jako narzędzie szkoleniowe, włączono w niej możliwość użycia narzędzia finger. Na rysunku 6.24 pokazano, czego można się spodziewać po nawiązaniu połączenia z narzędziem finger w systemie.

Jak widzisz, narzędzie finger dostarcza znacznie więcej informacji, niż uzyskałbyś po nawiązaniu połączenia z klientem poczty. Warto w tym miejscu przypomnieć, że użycie finger rzadko będzie możliwe. Uważaj się za szczęśliwego, jeśli znajdziesz w internecie system udostępniający narzędzie finger. Upewnij się również o dezaktywacji tego narzędzia w używanym przez siebie systemie, jeśli nie masz naprawdę ważnego powodu, aby pozostawić je dostępne.



RYSUNEK 6.24.
Użycie narzędzia finger względem dystrybucji Hackerdemia LiveCD

Identyfikacja granic sieci

W ogromnych organizacjach bardzo często można się natknąć na strefy zdemilitaryzowane (ang. *Demilitarized Zones* — DMZ) znajdujące się w zakresie będącym przedmiotem testu penetracyjnego. Ujmując rzecz najprościej: strefa zdemilitaryzowana to najczęściej sieci mające bezpośrednie połączenie z internetem i stanowiące bufor między internetem i wewnętrzną siecią korporacji. Powinieneś się dowiedzieć, czy możesz penetrować strefę zdemilitaryzowaną i włamać się do sieci korporacyjnej. Dla osoby przeprowadzającej test penetracyjny problemem jest ustalenie, gdzie rozpoczyna się sieć celu ataku, oraz określenie infrastruktury łączącej cel ataku z internetem.

Wprawdzie brzmi to sensownie, ale implementacja rozwiązania jest już znacznie trudniejsza. Trzeba zachować ostrożność podczas wybierania celu, aby nie zaatakować systemu, który nie należy do klienta. Przyjmuje się założenie, że klient dostarcza listę adresów IP wszystkich systemów pozostających pod jego kontrolą. Warto pamiętać, że zdarzają się pewne przeoczenia, na przykład do sieci dodano nowe komputery, ale zapomniano uaktualnić rekordy. Jeżeli znajdziesz tego rodzaju „przeoczone" systemy, istnieje możliwość, że przeoczono je również podczas uaktualnień oprogramowania, co może ułatwić wykorzystanie luk w zabezpieczeniach sieci.

Na rysunku 6.25 pokazano wynik użycia narzędzia traceroute w sieci docelowej, czyli należącej do firmy Insecure.com. Zwróć uwagę na kilka różnych nazw domen, które warto sprawdzić: us.above.net i sv.svcolo.com. Z kolei na rysunkach 6.26 i 6.27 pokazano informacje whois dla domen above.net i svcolo.com. Od razu widać, że wymienione systemy należą do innych osób niż właściciel insecure.org. Jeżeli przeprowadzimy dalsze czynności sprawdzające, wtedy przekonamy się, że above.net zapewnia połączenie z internetem, natomiast svcolo.com — usługi w zakresie obsługiwania centrum danych.

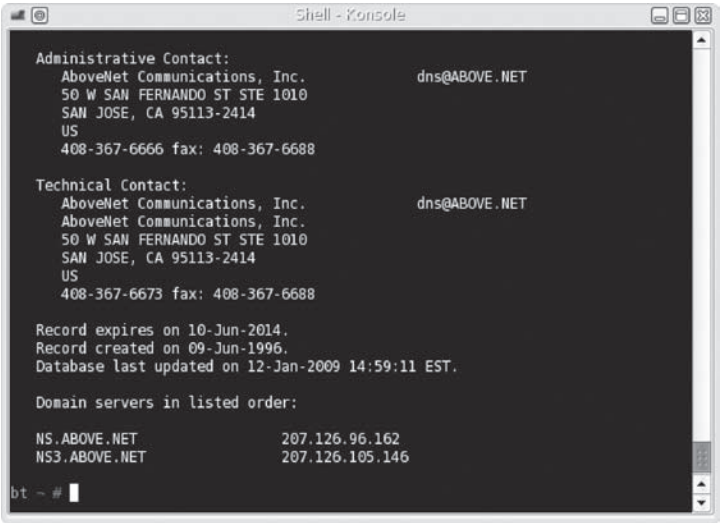
64.13.134.49 is from United States(US) in region North America

TraceRoute to 64.13.134.49 [insecure.org]

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	16	28	14	72.249.0.65	-
2	7	6	6	209.249.122.73	209.249.122.73.available.above.net
3	18	11	8	64.125.26.213	ge-2-0-0.mpr2.dfw2.us.above.net
4	11	14	17	64.125.26.134	so-1-1-0.mpr4.iah1.us.above.net
5	46	50	43	64.125.25.18	so-1-1-0.mpr4.lax9.us.above.net
6	53	53	61	64.125.26.30	so-0-1-0.mpr2.sjc2.us.above.net
7	57	53	58	64.125.31.69	xe-0-1-0.mpr2.pao1.us.above.net
8	76	56	89	208.185.168.173	metro0.sv.svcolo.com
9	62	58	53	64.13.134.49	insecure.org

Trace complete

RYSUNEK 6.25.
Wynik uruchomienia narzędzia traceroute dla sieci insecure.org



RYSUNEK 6.26.
Informacje whois dla domeny above.net

Zajmijmy się teraz znacznie bardziej interesującym aspektem, dzięki któremu jeszcze lepiej zrozumiemy, na co można się natknąć podczas identyfikacji granic sieci. Na rysunku 6.28 pokazano wynik uruchomienia narzędzia traceroute dla google.com. Po przeskoku 6 nie widzimy żadnych informacji dotyczących właściciela serwera, co wymaga przeprowadzenia dalszej analizy. Jeżeli wykonamy polecenie `whois` dla adresu IP 66.249.94.94 (jak pokazano na rysunku 6.29), wtedy dowiemy się, że właścicielem sprawdzanego systemu jest google.com. Na tym etapie możemy określić 66.249.94.94 jako granicę sieci i rozpocząć atak na ten system, pod warunkiem że mamy odpowiednie uprawnienia. (Skoro to jedynie przykład pokazujący sposób określania granic sieci, nie przeprowadzamy ataku na podany system).

```
Shell - Konsole
Domain name: SVCOLO.COM


Administrative Contact:
   Giannandrea, John  hostmaster@svcolo.com
   P.O. Box 390804
   Mountain View, CA 94039
   US
   +1.4084000550
Technical Contact:
   hostmaster, meer.net  hostmaster@meer.net
   P.O. Box 390804
   Mountain View, CA 94039
   US
   +1.8888446337    Fax: +1.6506181482



Registration Service Provider:
   Meer.net LLC, support@meer.net
   888-844-6337
   650-618-1482 (fax)
   http://www.meer.net/
   P.O. Box 390804
   Mountain View, CA 94039
   USA
```

RYSUNEK 6.27.
Informacje whois dla domeny svcolo.com

74.125.45.100 is from United States(US) in region North America

TraceRoute to 74.125.45.100 [google.com]

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	36	39	19	72.249.0.65	-
2	9	12	11	206.123.64.22	-
3	57	102	11	216.52.189.9	border4.te4-4.colo4dallas-4.ext1.dal.pnap.net
4	16	44	34	216.52.191.34	core3.tge5-1-bbnet1.ext1.dal.pnap.net
5	13	14	25	207.88.185.73	207.88.185.73.ptr.us.xo.net
6	43	51	57	207.88.185.130	207.88.185.130.ptr.us.xo.net
7	50	47	43	66.249.94.94	-
8	31	29	29	72.14.238.243	-
9	82	34	79	209.85.253.173	-
10	62	37	36	209.85.253.145	-
11	66	31	29	74.125.45.100	yx-in-f100.google.com

Trace complete

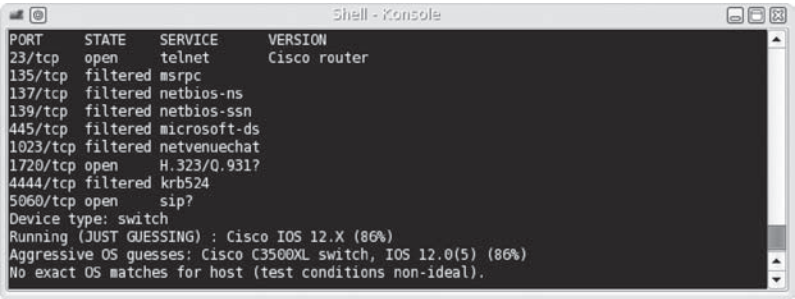
RYSUNEK 6.28.
Wynik uruchomienia narzędzia traceroute dla google.com

```
Shell - Konsole
bt ~ # whois 66.249.94.94

OrgName:    Google Inc.
OrgID:      GOGL
Address:    1600 Amphitheatre Parkway
City:       Mountain View
StateProv:  CA
PostalCode: 94043
Country:    US

NetRange:   66.249.64.0 - 66.249.95.255
CIDR:       66.249.64.0/19
NetName:    GOOGLE
NetHandle:  NET-66-249-64-0-1
Parent:     NET-66-0-0-0-0
NetType:    Direct Allocation
NameServer: NS1.GOOGLE.COM
NameServer: NS2.GOOGLE.COM
NameServer: NS3.GOOGLE.COM
```

RYSUNEK 6.29.
Informacje whois dla adresu IP 66.249.94.94

Istnieje prawdopodobieństwo, że urządzenie podane w przeskoku 7 jest routerem. Można to sprawdzić, przeprowadzając operację skanowania portów (w omawianym przykładzie jednak tego nie zrobimy). Znacznie bardziej interesująca jest liczba różnych sieci, które przeskanujemy, zanim dotrzemy do sieci docelowej — 74.125.45.100. Jeżeli wykonamy polecenia whois dla pozostałych adresów IP, wtedy dowiemy się, że ich właścicielem również jest Google. Powstaje więc pytanie: co się dzieje między przeskokami 7 i 11, które pokazano na rysunku 6.28? Na tym etapie pozorowanego testu penetracyjnego nie musimy przeprowadzać żadnych dokładniejszych operacji sprawdzających, choć naprawdę nie zaszkodzi dowiedzieć się, co można w tej sytuacji zrobić. W tym celu przeprowadzimy kilka prostych operacji skanowania, aby dowiedzieć się nieco więcej na temat wspomnianych urządzeń.

Wprawdzie nadal nie będziemy skanować żadnych elementów sieciowych firmy Google (nie mamy zezwolenia na takie działania), ale chciałbym Ci pokazać, jak może wyglądać wynik operacji skanowania sieci. Na rysunku 6.30 pokazano wynik skanowania portów routera Cisco. Na dalszym etapie testu penetracyjnego tego rodzaju informacje będą szczególnie użyteczne do identyfikacji protokołów (i prawdopodobnie systemów operacyjnych) używanych w sieci, co z kolei pomoże w sprawdzeniu ich podatności na atak. Jednak teraz tego rodzaju informacje wykorzystamy do sprawdzenia, czy połączenie nawiązano z przełącznikiem sieciowym, routerem, równoważnikiem obciążenia, przekaźnikiem, czy może zaporą sieciową. Taka wiedza pozwala czasami na lepszą identyfikację granic sieci.



RYSUNEK 6.30.
Przeprowadzone w laboratorium skanowanie sieci za pomocą narzędzia nmap

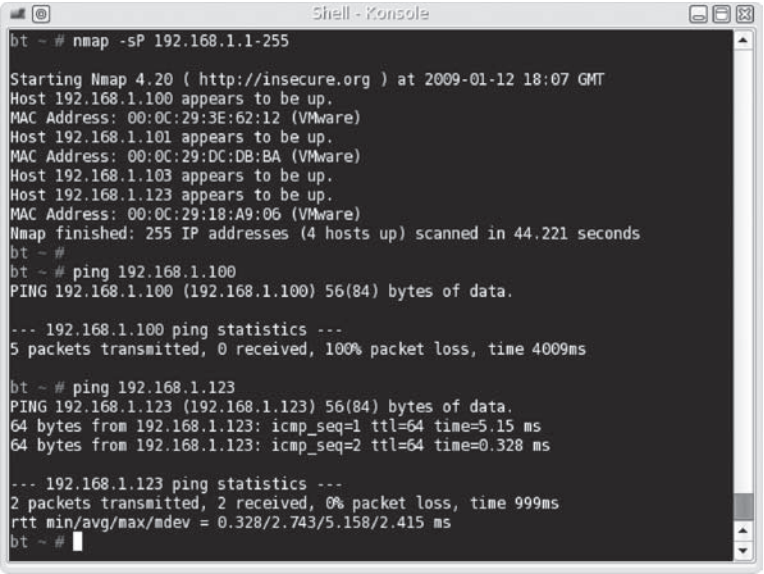
W celu identyfikacji granic sieci nie trzeba zbyt wiele robić, ale jest to krok o znaczeniu krytycznym w każdym teście penetracyjnym. Podstawowym celem tego kroku jest upewnienie się, że nie będą atakowane żadne urządzenia lub systemy, na atakowanie których nie mamy zezwolenia. Jeżeli umowa z klientem zawiera wymienione konkretne adresy IP, wówczas zadanie jest łatwiejsze, ponieważ działania można prowadzić tylko względem wymienionych adresów. Jednak jeśli zadanie polega na przeprowadzeniu testu penetracyjnego sieci, wtedy trzeba w pełni zdawać sobie sprawę, które systemy znajdują się w sieci, a które są poza zasięgiem testu penetracyjnego.

Warto również pamiętać, że systemy mogą blokować komunikaty ICMP (ang. *Internet Control Message Protocol*), aby utrudnić ich wykrycie. Inne metody wykrywania systemów zostaną omówione w rozdziale 7.

Sprawdzanie sieci

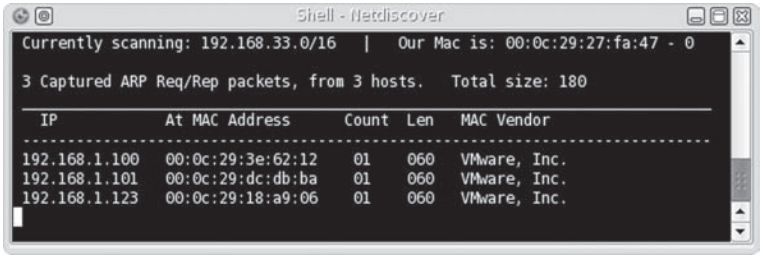
Po określeniu granic atakowanej sieci kolejnym krokiem jest identyfikacja wszystkich znajdujących się w niej urządzeń. Na tym etapie nie próbujemy ustalić rodzaju poszczególnych urządzeń (routerów, przełączników sieciowych, zapór sieciowych, serwerów i tak dalej), a jedynie określić liczbę urządzeń znajdujących się w sieci oraz powiązane z nimi adresy IP. Później przeprowadzimy skanowanie wszystkich urządzeń w celu zebrania informacji dodatkowych. Teraz wystarczy po prostu przygotować listę urządzeń sieci, aby dopracować i dostosować harmonogram działań w projekcie, jeśli zajdzie potrzeba.

Wystarczające będzie przeprowadzenie prostej operacji skanowania. Na rysunku 6.31 pokazano wynik użycia narzędzia nmap do przeskanowania jednego z laboratorium. Skaner wykrył obecność w sieci czterech komputerów, w tym także systemu przeprowadzającego skanowanie. Warto pamiętać, aby do skanowania sieci będącej celem ataku użyć co najmniej dwóch różnych narzędzi. Zdarza się, że pewne systemy nie odpowiadają na działania skanera, co jest skutkiem zastosowania mechanizmów bezpieczeństwa w takim systemie. Aby przekonać się, jak to działa, na rysunku 6.31 pokazano również wynik wydania polecenia `ping` względem dwóch systemów (o adresach IP 192.168.1.100 i 192.168.1.123.) zidentyfikowanych podczas skanowania za pomocą nmap.



RYSUNEK 6.31.
Skanowanie sieci w laboratorium za pomocą narzędzia nmap

Jeżeli przeprowadzone zostanie jedynie sprawdzenie zakresu adresów IP za pomocą polecenia `ping`, pominięte będzie co najmniej jedno urządzenie w sieci. Po raz kolejny przekonujemy się, dlaczego do wykonania danego kroku lub zadania warto używać wielu różnych narzędzi. (Czytelnicy, którzy brali udział w prowadzonych przeze mnie szkoleniach, zapewne doskonale pamiętają powtarzaną mantrę: „Zawsze bądź cyniczny — zawsze używaj więcej niż tylko jednego narzędzia do wykonania danego zadania". To naprawdę może zmienić przebieg Twojej kariery na polu przeprowadzania testów penetracyjnych). Nigdy nie możesz przewidzieć, jaka będzie reakcja systemu, gdy używasz jedynie ulubionego narzędzia. Podążając za przedstawioną powyżej radą, do sprawdzenia urządzeń w sieci wykorzystamy także narzędzie netdiscover, jak pokazano na rysunku 6.32. Wymienione narzędzie nasłuchuje ruchu ARP (ang. *Address Resolution Protocol*) w sieci i przechwytuje wszystko, co tylko może przechwycić.



RYSUNEK 6.32.
Wyniki skanowania za pomocą narzędzia netdiscover

Podobnie jak w przypadku większości narzędzi, także netdiscover ma pewne ograniczenia. Ze względu na to, że żądania ARP nie wychodzą poza router, narzędzie może wykryć jedynie systemy znajdujące się w tej samej podsieci, w której jest system przeprowadzający skanowanie. Ponadto wykryte mogą być tylko systemy aktywnie rozgłaszające swoją obecność lub wysyłające dane. Jednak w przypadku sieci znajdującej się w naszym laboratorium narzędzie netdiscover sprawdza się doskonale. Zidentyfikowane zostały wszystkie działające systemy, a odkrycia pokrywają się z wynikami skanowania przeprowadzonego za pomocą narzędzia nmap.

To jedynie niewielki fragment operacji, jaką jest skanowanie sieci. W dalszej części testu penetracyjnego dowiesz się znacznie więcej o systemach znajdujących się w sieci. Przedstawiony tutaj krok miał za zadanie jedynie przeprowadzenie prostej operacji wykrycia urządzeń znajdujących się w sieci jako fragmentu fazy zbierania informacji. Na tym etapie naszym celem nie jest zebranie wszelkich danych dotyczących urządzeń w sieci, aby sprawdzić, czy są podatne na ataki — tym zajmiemy się w rozdziałach 7. i 8.

PODSUMOWANIE

Ten pierwszy krok w profesjonalnym teście penetracyjnym wymaga dużego wysiłku. Niestety, często jest niedoceniany lub wykonywany bardzo pobieżnie. Po części wynika to z faktu, że kolejne kroki testu penetracyjnego (na przykład wykorzystywanie luk w zabezpieczeniach) są często uznawane za znacznie bardziej ekscytujące. Bywa więc, że faza zbierania informacji jest przeprowadzana szybko i niechlujnie, aby osoba przeprowadzająca test penetracyjny mogła jak najszybciej zająć się „ciekawszymi działaniami". Wprawdzie omówiona w tym rozdziale faza jest prawdopodobnie znacznie nudniejsza niż kolejne kroki testu penetracyjnego, ale jednocześnie może okazać się najcenniejsza w każdym projekcie, zarówno dla inżynierów, jak i menedżerów projektu. Stwierdzam to na podstawie własnego doświadczenia, jako osoba od wielu lat zajmująca się przeprowadzaniem profesjonalnych testów penetracyjnych.

Jeżeli faza zbierania informacji zostanie przeprowadzona prawidłowo, może zaoszczędzić ogromną ilość czasu w trakcie całego cyklu życiowego projektu. Ujmując rzecz najprościej: im więcej pracy wykonasz w fazie zbierania informacji, tym efektywniej i trafniej przeprowadzisz projekt testu penetracyjnego. Dokładne omówienie systemów, z jakimi przyjdzie Ci się zmierzyć, niewątpliwie pomoże w odrzuceniu nieefektywnych rozwiązań w zakresie wykorzystania luk w zabezpieczeniach. Ponadto zmniejszy ilość dokumentacji koniecznej do przeczytania, aby lepiej poznać aplikację lub protokół atakowany na dalszym etapie testu penetracyjnego.

Przedstawiłem tutaj różne sposoby zbierania informacji o celu ataku, zarówno w sposób pasywny, jak i aktywny. W trakcie analizy wymieniłem wiele witryn internetowych. Po lekturze tego rozdziału powinieneś zapamiętać nie nazwy witryn, które musisz odwiedzić, ale rodzaje informacji, jakie można znaleźć w internecie bez nawiązywania bezpośredniego połączenia z siecią będącą celem ataku. Dzięki wykorzystaniu publicznie dostępnych zasobów można przygotować obraz celu bez wysłania choćby jednego pakietu do sieci będącej celem ataku.

Pamiętaj, że wspomniane w rozdziale rodzaje informacji można zebrać bez nawiązywania połączenia z atakowaną siecią. Najważniejsze jednak jest to, że zgromadzone informacje — nawet jeśli pochodzą z publicznie dostępnych witryn internetowych — nie są własnością publiczną. Zachowaj szczególną ostrożność podczas pracy ze wszystkimi danymi klienta, nawet informacjami znalezionymi w internecie.

ODWOŁANIA

Google Inc. 2009. Production Engineer — Mountain View.

Skorowidz

D

E

F

G

H

I

J

K

L

Ł

M

N

O

P

R

S

Ś

T

U

V

W

Z

Ż

Twój przewodnik w testach penetracyjnych!

Trzonem każdego systemu informatycznego są dane oraz gwarancja ich bezpieczeństwa. Jest to szczególnie ważne, ponieważ codziennie w najróżniejszych systemach przetwarzane są setki informacji na temat każdego z nas. Czasami są to dane mało istotne — wpisy na portalach społecznościowych lub komentarze na popularnym portalu internetowym. Jednak obok nich przetwarzane są nasze dane medyczne, informacje o rachunkach bankowych oraz zobowiązaniach. Ich utrata lub ujawnienie to prawdziwa katastrofa! Jak zapobiegać takim sytuacjom? Jak zagwarantować klientom pełne bezpieczeństwo danych?

W celu sprawdzenia bezpieczeństwa serwisu przeprowadzane są testy penetracyjne — kontrolowane próby przełamania zabezpieczeń. Zajmują się tym najlepsi specjaliści, a pozytywny wynik testów pozwala mieć nadzieję, że włamywaczowi również nie uda się wtargnąć do serca systemu. Ta książka została w całości poświęcona takim testom. W trakcie lektury dowiesz się, jak przygotować środowisko pracy oraz jak chronić dane testu penetracyjnego. Ponadto poznasz popularne metodologie, narzędzia oraz techniki zarządzania testami. Warto zwrócić uwagę na zagadnienia prawne i zapoznać oraz zapoznać się z możliwościami kariery w tej branży. Książka ta jest obowiązkową lekturą dla wszystkich zainteresowanych bezpieczeństwem systemów informatycznych oraz prowadzeniem testów penetracyjnych.

Dzięki tej książce:

- zaznajomisz się z aspektem prawnym testów penetracyjnych
- zbudujesz środowisko pracy
- poznasz ważne luki w codziennych usługach
- odkryjesz popularne narzędzia oraz metodologie prowadzenia testów
- poznasz ścieżki kariery w branży

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

ISBN 978-83-246-9033-6

9 788324 690336

cena: 69,00 zł

Informatyka w najlepszym wydaniu