Helion

HACKING I TESTY PENETRACYJNE PODSTAWY

Lektura obowiązkowa
dla każdego pentestera!

Patrick Engebretson

Tytuł oryginału: The Basics of Hacking and Penetration Testing:
Ethical Hacking and Penetration Testing

Tłumaczenie: Robert Górczyński

ISBN: 978-83-246-6653-9

Syngress is an imprint of Elsevier. 225 Wyman Street, Waltham, MA 02451, USA

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

Printed in Poland.

Spis treści

ROZDZIAŁ 3.

Skanowanie

Informacje zawarte w rozdziale:

- Narzędzie ping i przeczesywanie sieci za jego pomocą
- Skanowanie portów
- Skanowanie systemu pod kątem jego podatności na atak

WPROWADZENIE

Po zakończeniu pierwszego kroku testu penetracyjnego powinieneś doskonale znać wybrany cel ataku oraz mieć zebrane dokładne informacje na jego temat. Wspomniane informacje to będzie przede wszystkim zbiór adresów IP. Przypomnij sobie, że jednym z ostatnich zadań w fazie rekonesansu jest przygotowanie listy adresów IP, które należą do celu i na których zaatakowanie masz zezwolenie. Ta lista ma znaczenie kluczowe podczas przechodzenia z kroku pierwszego do drugiego. W kroku pierwszym zebrane informacje zostały zamienione na adresy IP możliwe do zaatakowania. Z kolei w kroku drugim adresy IP będą mapowane na otwarte porty i usługi.

Musisz koniecznie zrozumieć, że zadaniem większości sieci jest zezwolenie na przynajmniej częściową komunikację i dwukierunkowy przepływ danych. Sieci działające w całkowitej izolacji, pozbawione połączenia z internetem oraz usług takich jak poczta elektroniczna i WWW są obecnie rzadkością. Każda usługa, połączenie lub potencjalne połączenie z inną siecią dostarczają kolejnych możliwości przeprowadzenia ataku. Skanowanie to proces wyszukiwania funkcjonujących systemów i oferowanych przez nie usług.

Krok drugi, jakim jest skanowanie, można podzielić na trzy oddzielne fazy:

2.1. Określenie, czy system działa.
2.2. Skanowanie portów systemu.
2.3. Skanowanie systemu pod kątem jego podatności na atak.

W dalszej części rozdziału zostaną przedstawione narzędzia pozwalające na połączenie trzech wymienionych powyżej faz w pojedynczy proces. Aby jednak ułatwić opanowanie nowego materiału, najlepiej, jeśli te fazy będą omówione oddzielnie.

Krok 2.1 to proces prowadzący do określenia, czy wybrany cel jest systemem włączonym i posiadającym możliwość komunikacji oraz interakcji z Twoim komputerem. Ten krok charakteryzuje się najmniejszą niezawodnością, dlatego też niezależnie od jego wyniku zawsze należy wykonać kolejne kroki, czyli 2.2 i 2.3. Pamiętaj, że przeprowadzenie kroku 2.1 jest bardzo ważne i powinieneś dokładnie zanotować informacje o komputerach, które udzieliły odpowiedzi na zapytanie i okazały się dostępne.

Krok 2.2 to proces identyfikacji portów i usług działających w określonym komputerze.

Ujmując to najprościej, port umożliwia oprogramowaniu i sieci przeprowadzenie komunikacji z innym urządzeniem sprzętowym, np. komputerem. Port to rodzaj połączenia pozwalającego komputerowi na wymianę danych z innymi komputerami, oprogramowaniem lub urządzeniami. Przed połączeniem komputerów w sieci dane były wymieniane pomiędzy poszczególnymi komputerami za pomocą fizycznych nośników, np. dyskietek. Odkąd komputery zostały połączone w sieci, konieczne stało się opracowanie sposobu pozwalającego im na prowadzenie efektywnej komunikacji. Odpowiedzią na wspomnianą potrzebę stały się porty. Użycie wielu portów pozwala na jednoczesne prowadzenie wielu rodzajów komunikacji bez konieczności oczekiwania.

Aby jeszcze bardziej obrazowo przedstawić koncepcję portów i ich użycie w komputerach, pomocne może być przeanalizowanie następującej analogii: potraktuj komputer jak dom. Istnieje wiele różnych sposobów, w jakie można dostać się do domu. Każdy ze sposobów wejścia do domu (komputera) przypomina port w komputerze. Podobnie jak w przypadku portów w komputerze, drzwi w domu pozwalają zarówno na wejście do środka, jak i wyjście na zewnątrz.

Wyobraź sobie dom z pewną liczbą drzwi. Większość osób będzie korzystać z drzwi frontowych (głównych), ale właściciele mogą używać także bocznych, garażowych itd. Czasami mieszkańcy wchodzą do domu tylnymi drzwiami lub przez drzwi balkonowe. Niekonwencjonalnie zachowująca się osoba może po prostu wspiąć się do okna i spró-

bować przez nie wejść lub nawet wślizgnąć się przez otwór w drzwiach przeznaczony dla psa lub kota.

Niezależnie od sposobu, w jaki osoba próbuje wejść do domu, każdy z wymienionych przykładów to doskonała analogia do komputera i portów. Przypomnij sobie, że porty to rodzaje drzwi wejściowych do komputera. Niektóre z portów są powszechnie stosowane i przyjmują ogromną ilość ruchu sieciowego (podobnie jak w przypadku drzwi frontowych w domu), inne pozostają mniej znane i rzadziej używane (podobnie jak otwór w drzwiach przeznaczony dla zwierzaka).

Wiele najczęściej spotykanych usług sieciowych działa, korzystając ze standardowych numerów portów, co może dostarczyć atakującemu wskazówek dotyczących przeznaczenia atakowanego systemu. W tabeli 3.1 wymieniono listę najczęściej używanych portów oraz udostępniane przez nie usługi.

TABELA 3.1.
Najczęściej używane numery portów i odpowiadające im usługi

Numer portu	Usługa
20	Transfer danych FTP
21	Kontrola FTP
22	SSH
23	Telnet
25	SMTP (e-mail)
53	DNS
80	HTTP
443	HTTPS

Oczywiście istnieje znacznie więcej portów i usług, niż wymieniono w powyższej tabeli. Jednak przedstawiona lista ma Ci jedynie dostarczyć podstawowych informacji na temat najczęściej obecnie używanych portów w komputerach firmowych. Kiedy rozpoczniesz skanowanie portów wybranych celów, bardzo często będziesz spotykał usługi wymienione w tabeli 3.1.

Szczególną uwagę powinieneś zwrócić na odkrycie wszelkich otwartych portów w skanowanym systemie. Twórz szczegółowe notatki i zapisuj dane wyjściowe generowane przez wszystkie narzędzia używane w kroku 2.2. Pamiętaj, otwarty port to potencjalne drzwi pozwalające na dostanie się do atakowanego systemu.

Ostatnim krokiem w fazie skanowania jest krok 2.3, czyli skanowanie systemu pod kątem jego podatności na atak. Jest to proces polegający na wyszukiwaniu i identyfikowaniu wszelkich znanych słabych punktów w usługach oraz oprogramowaniu działającym w atakowanym komputerze. Odkrycie znanych luk w atakowanym systemie można porównać do znalezienia skrzyni złota. Obecnie wystarczy wykryć znaną lukę w zabezpieczeniach, by można było z powodzeniem zaatakować wiele komputerów działających

w internecie, mając jedynie niewielkie umiejętności w tym zakresie lub nie mając praktycznie żadnych.

Warto w tym miejscu wspomnieć o różnym poziomie niebezpieczeństwa wynikającego z istnienia poszczególnych luk w zabezpieczeniach. Pewne luki mogą dostarczać atakującemu niewielkich możliwości, podczas gdy inne — wręcz przeciwnie, mogą pozwolić na zdobycie pełnej kontroli nad komputerem. Wspomniane różne poziomy niebezpieczeństwa wynikającego z istnienia luk w zabezpieczeniach zostaną dokładniej omówione w dalszej części rozdziału.

W przeszłości miałem wielu klientów proszących mnie o podjęcie próby uzyskania dostępu do pewnych ważnych serwerów w sieci lokalnej. Oczywiście we wspomnianych przypadkach ostateczny cel ataku nie jest bezpośrednio dostępny w internecie. Niezależnie od tego, czy próbujesz uzyskać dostęp do supertajnego komputera znajdującego się w sieci wewnętrznej, czy po prostu dostać się do sieci, pierwszym podejmowanym krokiem jest najczęściej skanowanie urządzeń brzegowych. Powód jest prosty: rozpoczynamy od urządzeń brzegowych, ponieważ właśnie ich dotyczy większość informacji zebranych w fazie rekonesansu. Ponadto, przy obecnie stosowanych technologiach i architekturach, nie zawsze istnieje możliwość bezpośredniego *dostania się* do sieci. Dlatego też często stosowana metoda polega na przejściu przez serię komputerów, aby wreszcie dotrzeć do wybranego celu. W pierwszej kolejności trzeba zdobyć urządzenie brzegowe, a następnie dopiero można ruszyć w kierunku urządzeń wewnętrznych.

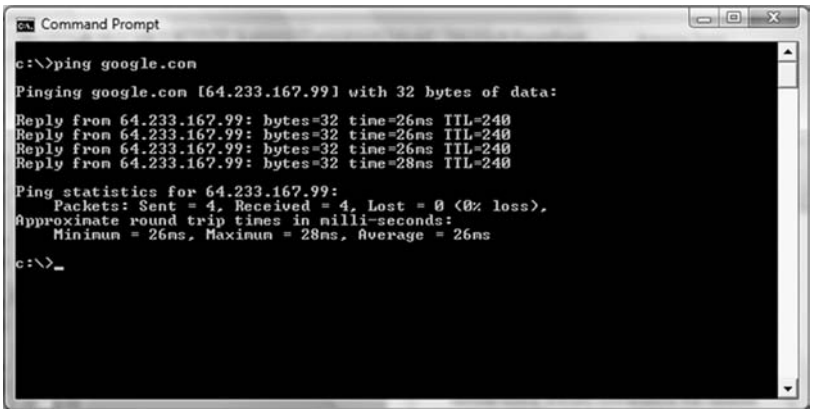
Urządzenia brzegowe to komputery, serwery, routery, zapory sieciowe i inne wyposażenie znajdujące się na zewnętrznych krawędziach chronionej sieci. Wspomniane urządzenia działają na zasadzie pośrednika pomiędzy chronionymi zasobami wewnętrznymi oraz sieciami zewnętrznymi, takimi jak internet.

Jak już wcześniej wspomniano, pierwszym krokiem jest najczęściej skanowanie urządzeń zewnętrznych w poszukiwaniu ich słabych punktów lub luk w zabezpieczeniach, które można wykorzystać, aby dostać się do wewnątrz. Po uzyskaniu dostępu do wewnątrz (to będzie tematem rozdziału 4.) proces skanowania można powtórzyć z poziomu nowo zdobytego urządzenia i wyszukać kolejne cele ataku. Tego rodzaju cykliczny proces pozwala na utworzenie bardzo szczegółowej mapy sieci wewnętrznej i wykrycie infrastruktury o znaczeniu krytycznym ukrytej za zaporą sieciową.

NARZĘDZIE PING I PRZECZESYWANIE SIECI ZA JEGO POMOCĄ

Ping to specjalny typ pakietu sieciowego nazywany pakietem ICMP. Jego działanie polega na wysyłaniu określonych typów ruchu sieciowego (pakietów ICMP Echo Request) do wskazanego interfejsu w komputerze bądź urządzeniu sieciowym. Jeżeli urządzenie (i dołączona karta sieciowa) otrzymujące pakiet ping jest włączone i może udzielać odpowiedzi na te pakiety, nadawca otrzyma pakiet Echo Reply. Poza informacją, że adresat pakietu jest włączony i akceptuje ruch sieciowy, można dzięki pakietom ping uzyskać inne cenne informacje, między innymi czas trwania podróży pakietu do systemu

adresata i z powrotem. Dzięki ping można poznać także poziom strat w trakcie komunikacji, co pozwala na określenie stopnia niezawodności połączenia. Na rysunku 3.1 pokazano przykład wykonania polecenia `ping`.



RYSUNEK 3.1.
Przykład działania polecenia ping

Wiersz pierwszy na rysunku 3.1 pokazuje wydanie polecenia `ping`. Zwróć uwagę, że rysunek pochodzi z systemu Windows. Wszystkie nowoczesne wersje systemów Linux i Windows mają wbudowane polecenie `ping`. Podstawowa różnica pomiędzy wersjami znajdującymi się w systemach Linux i Windows polega na tym, że domyślnie polecenie `ping` w Windows wysyła cztery pakiety Echo Request i automatycznie kończy działanie, podczas gdy w systemie Linux polecenie będzie nieustannie wysyłało wspomniane pakiety aż do chwili, gdy zakończysz działanie narzędzia ping. W systemie Linux przerwanie działania narzędzia ping następuje po naciśnięciu klawiszy *Ctrl+C*.

Skoncentrujmy uwagę na wierszu trzecim, rozpoczynającym się od słów `Reply from`. Wspomniany wiersz informuje nas o dostarczeniu pakietu ICMP Echo Request na adres IP 64.233.167.99 oraz o otrzymaniu odpowiedzi z podanego adresu. Fragment `bytes=32` wskazuje na wielkość wysłanego pakietu. Z kolei `time=26ms` informuje o czasie trwania podróży pakietu w obie strony. Fragment `TTL=240` przedstawia wartość TTL (ang. *Time To Live*) używaną do określenia maksymalnej liczby „przeskoków" pakietu, zanim zostanie on uznany za nieważny.

Skoro znasz już podstawowy sposób działania polecenia `ping`, przekonajmy się, jak może ono zostać wykorzystane przez hakera. Ponieważ pakiet ping może być bardzo użyteczny w określaniu dostępności sprawdzanego systemu, wykorzystamy polecenie `ping` w celu wykrywania komputerów. Niestety wysyłanie pakietów ping do wszystkich potencjalnych komputerów nawet w małej sieci będzie wysoce nieefektywne. Na szczęście dla nas istnieje kilka narzędzi pozwalających na przeczesywanie sieci za pomocą pakietów ping (ang. *ping sweep*). Przeczesanie sieci za pomocą pakietów ping polega na wysłaniu serii tych pakietów do pewnego zakresu adresów IP zamiast ręcznego podawania adresu IP poszczególnych komputerów.

Najprostszym sposobem przeczesania sieci za pomocą pakietów ping jest użycie narzędzia o nazwie FPing. Wymienione narzędzie jest wbudowane w dystrybucję BackTrack i działa z poziomu powłoki. Narzędzie FPing można pobrać także dla systemu Windows. Najłatwiejszym sposobem użycia narzędzia FPing jest przejście do aplikacji Terminal i wydanie polecenia `fping –a –g 172.16.45.1 172.16.45.254>hosts.txt`. Opcja `-a` powoduje uwzględnienie w danych wyjściowych jedynie dostępnych komputerów. W ten sposób otrzymane dane wyjściowe będą znacznie czytelniejsze i łatwiejsze do odczytu. Opcja `-g` pozwala na podanie przeczesywanego zakresu adresów IP — musisz podać zarówno początkowy, jak i końcowy adres IP zakresu. W omawianym przykładzie skanowane są wszystkie adresy IP od 172.16.45.1 do 172.16.45.254. Z kolei znak > oznacza potokowanie danych wyjściowych do pliku o nazwie *hosts.txt*. Oprócz użytych w przedstawionym przykładzie istnieje jeszcze wiele innych opcji pozwalających na zmianę sposobu działania narzędzia FPing. Możesz się z nimi zapoznać w dokumentacji narzędzia wyświetlanej po wydaniu w powłoce polecenia:

```
man fping
```

Po wykonaniu omówionego powyżej polecenia możesz wyświetlić zawartość nowo utworzonego pliku *hosts.txt* zawierającego listę komputerów, które udzieliły odpowiedzi na wysłany im pakiet ping. Zebrane w ten sposób adresy powinieneś dodać do listy potencjalnych celów. Musisz pamiętać o jednej bardzo ważnej rzeczy: nie wszystkie komputery udzielają odpowiedzi na pakiety ping. Niektóre komputery mogą być schowane za zaporą sieciową, inne z kolei mogą mieć zablokowaną możliwość udzielania odpowiedzi na pakiety ping.

SKANOWANIE PORTÓW

Posiadając listę celów ataku, możesz kontynuować ich analizę poprzez przeskanowanie portów we wszystkich urządzeniach o odkrytych adresach IP. Przypomnij sobie, że celem skanowania portów jest wykrycie wszystkich otwartych portów i ustalenie usług udostępnianych przez dany system. Wspomniana usługa to określona praca lub zadanie wykonywane przez komputer, np. obsługa poczty elektronicznej, serwera FTP, serwera wydruku, dostarczanie stron internetowych itd. Skanowanie portów można porównać do pukania w kolejne drzwi i okna domu, aby przekonać się, kto z mieszkańców zareaguje. Przykładowo po odkryciu otwartego portu 80 można podjąć próbę nawiązania z nim połączenia, a w efekcie otrzymać dość szczegółowe informacje na temat serwera WWW nasłuchującego na tym porcie.

W każdym komputerze istnieje w sumie 65 536 portów (o numerach od 0 do 65 535). Port może być typu TCP lub UDP, w zależności od wykorzystującej go usługi oraz natury prowadzonej przez niego komunikacji. Operacja skanowania ma nam dostarczyć informacji, które z portów są otwarte lub pozostają w użyciu. W ten sposób otrzymujemy lepszy ogólny obraz celu ataku, co z kolei pomaga w wyborze jak najskuteczniejszego sposobu przeprowadzenia ataku.

Jeżeli miałbyś wybrać tylko jedno narzędzie do przeprowadzenia operacji skanowania portów, bez wątpienia powinno być to narzędzie Nmap. Zostało ono utworzone przez Gordona „Fyodora" Lyona; jest dostępne bezpłatnie na witrynie *http://www.insecure.org/*, a także wbudowane w wiele obecnych dystrybucji systemu Linux, w tym również BackTrack. Wprawdzie istnieje możliwość uruchomienia narzędzia Nmap wraz z graficznym interfejsem użytkownika (ang. *Graphical User Interface*), ale w rozdziale skoncentrujemy się na jego wykorzystaniu z poziomu powłoki.

Osoby, które dopiero rozpoczynają pracę na polu zapewniania bezpieczeństwa i hackingu, bardzo często zadają pytania o powód nauki narzędzia działającego z poziomu powłoki, skoro można wykorzystać wersję danego narzędzia wyposażoną w graficzny interfejs użytkownika. Jednocześnie te same osoby często narzekają na trudność w używaniu powłoki. Odpowiedź jest bardzo prosta. Po pierwsze, korzystając z wersji narzędzia działającej w powłoce, będziesz mógł poznać opcje pozwalające na zmianę jego zachowania. W ten sposób zyskujesz znacznie większą elastyczność i dokładniejszą kontrolę oraz lepiej zrozumiesz używane narzędzie. Po drugie (i prawdopodobnie znacznie ważniejsze), hakerzy rzadko działają w sposób, jaki jest pokazywany w filmach. Wreszcie, narzędzia powłoki można wykorzystywać w skryptach. Możliwość zastosowania skryptów i automatyzacji zyskuje kluczowe znaczenie, gdy chcesz podnieść poziom swoich umiejętności.

Pamiętasz film zatytułowany *Kod dostępu*, w którym Hugh Jackman tworzył wirusa? Tańczył, popijał wino i jednocześnie tworzył wirusa, korzystając z narzędzi wyposażonych w graficzny interfejs użytkownika. To naprawdę wygląda nierealistycznie. Większość początkujących hakerów jest przekonana, że narzędzia ich pracy będą wyposażone w graficzny interfejs użytkownika, a po przejęciu kontroli nad komputerem zobaczą jego ekran i będą mogli poruszać się po nim kursorem myszy. Wprawdzie taka ewentualność istnieje, ale naprawdę bardzo rzadko. W większości przypadków celem jest uzyskanie dostępu do powłoki z uprawnieniami administratora lub wejście do systemu dzięki tylnym drzwiom. Powłoka to narzędzie pozwalające na kontrolowanie komputera z poziomu wiersza poleceń. Wygląda i działa jak okno aplikacji Terminal, w której często pracujesz, z wyjątkiem tego, że wydajesz polecenia na swoim komputerze, ale wykonywane są one na zdalnym. Poznanie narzędzi w ich wersjach działających z poziomu powłoki ma więc znaczenie krytyczne, ponieważ po zdobyciu kontroli nad zaatakowanym komputerem będziesz musiał umieścić w nim własne narzędzia i korzystać z nich za pomocą powłoki, a nie graficznego interfejsu użytkownika.

Przyjmijmy założenie, że nadal odmawiasz nauki używania powłoki. Ponadto załóżmy, że dzięki użyciu kilku narzędzi byłeś w stanie uzyskać dostęp do zaatakowanego komputera. Po uzyskaniu dostępu do zaatakowanego komputera zobaczysz powłokę, a nie graficzny interfejs użytkownika. Jeżeli nie wiesz, w jaki sposób kopiować pliki, dodawać użytkowników, modyfikować dokumenty i wprowadzać inne zmiany z poziomu powłoki, Twoja praca w celu uzyskania dostępu pójdzie na marne. Będziesz zablokowany, podobnie jak Mojżesz, który mógł zobaczyć Ziemię Obiecaną, ale nie mógł na nią wejść.

Podczas przeprowadzania skanowania portów wykorzystywane narzędzie dosłownie tworzy pakiet, a następnie wysyła go do każdego portu w skanowanym komputerze. Celem jest ustalenie rodzaju odpowiedzi otrzymywanej z każdego sprawdzanego portu. Różne rodzaje operacji skanowania portów dostarczają odmiennych wyników. Bardzo ważne jest pełne zrozumienie stosowanego rodzaju skanowania, jak również oczekiwanych danych wyjściowych tej operacji.

Procedura nawiązania połączenia

Kiedy dwa urządzenia w danej sieci chcą się ze sobą komunikować poprzez TCP, w pierwszej kolejności muszą przeprowadzić procedurę nawiązania połączenia (ang. *Three-Way Handshake*). Ten proces jest bardzo podobny do rozmowy telefonicznej, przynajmniej przed nastaniem czasu, gdy każdy ma w telefonie włączoną identyfikację dzwoniącego. Kiedy chcesz z kimś porozmawiać przez telefon, bierzesz aparat do ręki i wykręcasz numer. Osoba, u której dzwoni telefon, podnosi słuchawkę, nie wiedząc, kto do niej telefonuje, i mówi „Halo". Wtedy osoba dzwoniąca przedstawia się, np. „Halo, mówi Janek". Jeżeli obie osoby się znają, dzwoniący może w odpowiedzi usłyszeć np. „A, witaj, Janku". Na tym etapie obie osoby mają wystarczającą ilość informacji, aby w zwykły sposób prowadzić konwersację.

Komputery działają w bardzo podobny sposób. Kiedy dwa komputery chcą się ze sobą komunikować, muszą przejść przez proces podobny do przedstawionego powyżej. Pierwszy komputer łączy się z drugim poprzez wysłanie pakietu SYN do portu o określonym numerze. Jeżeli drugi komputer nasłuchuje na tym porcie, udziela odpowiedzi, wysyłając pakiet SYN/ACK. Gdy pierwszy komputer otrzyma ten pakiet, odpowiada pakietem ACK. Na tym etapie oba komputery mogą już prowadzić zwykłą komunikację. W omówionym wcześniej przykładzie rozmowy telefonicznej osoba dzwoniąca działa jak wysyłający pakiet SYN. Osoba odbierająca telefon i mówiąca „Halo" działa jak pakiet SYN/ACK wysyłany dzwoniącemu, natomiast dzwoniący przedstawia się poprzez pakiet ACK.

Użycie narzędzia Nmap do przeprowadzenia skanowania TCP

Pierwsze analizowane przez nas skanowanie nosi nazwę skanowania TCP. Ta operacja jest bardzo często uznawana za najbardziej podstawowe i stabilne skanowanie wszystkich portów, ponieważ narzędzie Nmap próbuje przeprowadzić pełny proces nawiązania połączenia ze wszystkimi portami podanymi w wywołaniu narzędzia Nmap. Skoro skanowanie w rzeczywistości przeprowadza pełny proces nawiązywania połączenia, a następnie elegancko zamyka dane połączenie, istnieje niewielkie niebezpieczeństwo zalania żądaniami atakowanego systemu i doprowadzenia go do awarii.

Jeżeli w wywołaniu narzędzia nie podasz zakresu portów, przeskanowany zostanie tysiąc najczęściej używanych portów. O ile nie masz czasu do stracenia, zawsze zaleca się przeprowadzenie skanowania wszystkich portów. Powód jest prosty: administratorzy

często próbują chronić usługę poprzez jej uruchomienie na niestandardowym porcie. Przeskanowanie wszystkich portów następuje po użyciu opcji `-p` w wywołaniu narzędzia Nmap. Z kolei opcja `-PN` informuje narzędzie Nmap, że zalecane jest przeprowadzenie skanowania wszystkich urządzeń. Użycie wymienionej opcji może doprowadzić do wyłączenia wykrywania komputerów i zmuszenia narzędzia do przeskanowania każdego systemu, tak jakby był włączony. To niezwykle użyteczna możliwość podczas wykrywania systemów i portów, które wcześniej mogły zostać przeoczone.

Aby przeprowadzić skanowanie TCP, z poziomu powłoki wydaj polecenie:

```
nmap –sT -p- -PN 172.16.45.135
```

Warto poświęcić chwilę na przeanalizowanie powyższego polecenia. Pierwsze słowo `nmap` powoduje uruchomienie narzędzia Nmap, opcja `-sT` nakazuje przeprowadzenie skanowania TCP. Tę opcję jednak rozbijemy na czynniki pierwsze: `-s` pozwala na wskazanie rodzaju wykonywanego skanowania, natomiast `-T` oznacza skanowanie typu TCP. Opcja `-p` została użyta w celu przeprowadzenia skanowania wszystkich portów, a nie domyślnego tysiąca. Opcji `-PN` użyto w celu pominięcia fazy wykrywania komputerów i przeprowadzenie skanowania wszystkich adresów, tak jakby systemy były włączone i odpowiadały na żądania ping. Wreszcie, w poleceniu podajemy adres IP skanowanego komputera. Oczywiście adres, którego użyjesz, powinien być inny niż podany w przykładzie! Na rysunku 3.2 pokazano proces przeprowadzenia skanowania TCP przez narzędzie Nmap i wygenerowane w jego wyniku dane wyjściowe.

RYSUNEK 3.2.
Skanowanie TCP i otrzymane w jego wyniku dane wyjściowe

Czasami proces skanowania trzeba przeprowadzić względem całej podsieci lub pewnego zakresu adresów IP. W takim przypadku narzędziu Nmap należy zlecić przeprowadzenie skanowania ciągłego zakresu adresów IP poprzez dołączenie ostatniego oktetu końcowego adresu IP, np.:

```
nmap –sT -p- -PN 172.16.45.1-254
```

Wydanie powyższego polecenia spowoduje przeskanowanie przez narzędzie Nmap wszystkich komputerów o adresach IP od 172.16.45.1 do 172.16.45.254. Podobnie jak w przypadku przeczesywania sieci za pomocą pakietów ping, także powyższe rozwiązanie to potężna technika, dzięki której możesz znacznie poprawić swoją wydajność podczas skanowania.

Jeżeli musisz przeprowadzić skanowanie serii komputerów o niekolejnych adresach IP, możesz utworzyć plik tekstowy i umieścić w nim listę adresów IP do przeskanowania, po jednym adresie w każdym wierszu. Następnie w wywołaniu narzędzia Nmap użyj opcji `-iL ścieżka_dostępu_do_pliku`. W ten sposób wszystkie wymienione w pliku komputery zostaną przeskanowane po wydaniu pojedynczego polecenia. Kiedy istnieje możliwość, zawsze staraj się tworzyć pojedynczy plik tekstowy zawierający adresy IP wszystkich komputerów, które są Twoimi celami. Większość omawianych w książce narzędzi posiada opcję lub mechanizm pozwalający na wczytanie tych danych z pliku tekstowego, co oszczędza Twój czas poprzez uniknięcie konieczności nieustannego wprowadzania tych samych danych. Co ważniejsze, im mniej razy wprowadzasz adres IP, tym mniejsze niebezpieczeństwo popełnienia pomyłki i przeskanowania niewłaściwego komputera.

Użycie narzędzia Nmap do przeprowadzenia skanowania SYN

Skanowanie SYN to bezsprzecznie najpopularniejszy rodzaj skanowania portów przeprowadzany przez narzędzie Nmap. Istnieje wiele powodów jego popularności, a jeden z nich to fakt, że ten rodzaj skanowania jest domyślnie przeprowadzany przez narzędzie Nmap. Jeżeli uruchomisz narzędzie Nmap bez wskazania rodzaju skanowania (za pomocą opcji `-s`), to Nmap domyślnie przeprowadzi skanowanie SYN.

Pomijając aspekt ustawienia skanowania SYN jako domyślnego, jego popularność wynika także z szybkości działania — jest znacznie szybsze niż skanowanie TCP, a przy tym pozostaje stosunkowo bezpieczne i minimalizuje niebezpieczeństwo doprowadzenia do awarii skanowanego komputera lub uznania skanowania za atak typu DOS. Większa szybkość skanowania SYN wiąże się z tym, że zamiast pełnego procesu nawiązania połączenia przeprowadza tylko jego dwa pierwsze kroki.

W skanowaniu SYN komputer przeprowadzający operację skanowania wysyła pakiet SYN, na który skanowany komputer odpowiada pakietem SYN/ACK (oczywiście przy założeniu, że port jest używany i niefiltrowany), podobnie jak ma to miejsce w skanowaniu TCP. Jednak na tym etapie zamiast odpowiedzieć tradycyjnym pakietem ACK, komputer skanujący wysyła pakiet RST (zerowania). Wspomniany pakiet nakazuje skanowanemu komputerowi zignorowanie poprzednich pakietów i zamknięcie połączenia pomiędzy dwoma komputerami. Jak widać, większa szybkość skanowania SYN w porównaniu ze skanowaniem TCP wynika z mniejszej liczby przesyłanych pakietów pomiędzy komputerami. Wprawdzie kilka pakietów mniej nie kojarzy się ze zbyt dużą oszczędnością, ale ta liczba może szybko się zwiększyć podczas skanowania wielu komputerów.

Jeżeli zechcemy porównać proces nawiązywania połączenia z rozmową telefoniczną, skanowanie SYN można przedstawić następująco: dzwoniący wykręca numer do osoby, czeka, aż ona odbierze telefon i powie „Halo”, a wtedy odkłada słuchawkę bez słowa.

Inną zaletą skanowania SYN jest to, że w pewnych sytuacjach oferuje określony poziom anonimowości. Z tego powodu ten rodzaj skanowania jest często określany mianem

skanowania stealth. Ponieważ proces nawiązania połączenia nigdy nie zostaje w pełni przeprowadzony, oficjalnie połączenie nigdy nie zostaje nawiązane w 100%. Pewne aplikacje i systemy zapisu informacji w plikach dzienników zdarzeń wymagają pełnego nawiązania połączenia, aby informacje na ten temat zostały zarejestrowane. Ponieważ w plikach dzienników zdarzeń będą rejestrowane tylko w pełni nawiązane połączenia, a skanowanie SYN nigdy oficjalnie nie nawiąże ani jednego połączenia, przez wiele aplikacji pozostanie ono niezauważone. Pamiętaj o wyjątkach od przedstawionej reguły. Wszystkie nowoczesne zapory sieciowe i używane obecnie systemy wykrywania włamań są w stanie wykryć i zgłosić skanowanie SYN!

Ponieważ skanowanie SYN to domyślny rodzaj skanowania przeprowadzany przez narzędzie Nmap, nie ma konieczności jego wskazywania za pomocą opcji `-s`. Jednak w tej książce koncentrujemy się na podstawach, więc warto wyrobić sobie nawyk wyraźnego wskazywania wybranego rodzaju skanowania.

Aby przeprowadzić skanowanie typu SYN, z poziomu powłoki wydaj przedstawione poniżej polecenie:

```
nmap –sS -p- -PN 172.16.45.135
```

Samo polecenie jest dokładnie takie samo jak użyte w poprzednim przykładzie, ale z jednym wyjątkiem: zamiast opcji `-sT` została użyta opcja `-sS`. W ten sposób narzędzie Nmap otrzymało polecenie przeprowadzenia skanowania SYN, a nie TCP. Rodzaj skanowania bardzo łatwo zapamiętać: litera `T` wskazuje TCP, natomiast litera `S` wskazuje SYN. Pozostałe opcje użyte w powyższym poleceniu zostały dokładnie omówione w poprzednim przykładzie. Jeśli zapomniałeś ich znaczenia, powróć do punktu „Użycie narzędzia Nmap do przeprowadzenia skanowania TCP”, w której znajdziesz ich objaśnienie. Na rysunku 3.3 pokazano dane wyjściowe wygenerowane przez operację skanowania SYN wskazanego komputera.

RYSUNEK 3.3.
Skanowanie SYN i otrzymane w jego wyniku dane wyjściowe

Poświęć chwilę na porównanie całkowitego czasu przeprowadzenia poszczególnych operacji skanowania TCP i SYN. Wspomniane czasy zostały pokazane na rysunkach 3.2 i 3.3. Nawet w tak prostym przypadku skanowania pojedynczego komputera wyraźnie widać, że skanowanie SYN zostało przeprowadzone w krótszym czasie.

Użycie narzędzia Nmap do przeprowadzenia skanowania UDP

Podczas skanowania portów jeden z błędów najczęściej popełnianych przez nowicjuszy zajmujących się testami penetracyjnymi to zlekceważenie UDP. Aspirujący do miana hakerów bardzo często uruchamiają narzędzie Nmap, przeprowadzają pojedyncze skanowanie (najczęściej typu SYN) i przechodzą do operacji skanowania pod kątem podatności systemu na atak. Nigdy nie powinieneś lekceważyć wagi skanowania portów UDP! Rezygnację z przeprowadzenia skanowania UDP można porównać do opuszczenia czytania wskazówek lub przypisów w książce. Wprawdzie prawdopodobnie dobrze zrozumiesz temat, ale może Ci umknąć wiele szczegółów.

Trzeba koniecznie zrozumieć, że oba rodzaje skanowania — typu TCP i SYN — opierają się na komunikacji TCP. Wspomniany TCP to akronim *Transmission Control Protocol*, natomiast UDP to akronim *User Datagram Protocol*. Komputery mogą się między sobą komunikować za pomocą TCP lub UDP, a pomiędzy wymienionymi protokołami występuje wiele kluczowych różnic.

Protokół TCP jest uznawany za „protokół zorientowany pod kątem połączenia", ponieważ wymaga, aby komunikacja pomiędzy nadawcą i odbiorcą pozostała zsynchronizowana. Ten proces gwarantuje, że pakiety przekazywane pomiędzy komputerami pozostaną nietknięte i będą dostarczane w kolejności ich wysyłania. Z drugiej strony protokół UDP jest uznawany za „bezpołączeniowy", ponieważ nadawca po prostu wysyła pakiety do odbiorcy bez stosowania jakiegokolwiek mechanizmu gwarantującego ich dostarczenie. Każdy z wymienionych protokołów ma swoje wady i zalety w kategoriach szybkości działania, niezawodności i sprawdzania pod kątem występowania błędów. Aby w pełni opanować sztukę skanowania portów, powinieneś w pełni zrozumieć wymienione protokoły. Ich poznanie wymaga czasu.

Przypomnij sobie, jak porównaliśmy proces nawiązywania połączenia do rozmowy telefonicznej. Wspomniany proces nawiązania połączenia to kluczowy komponent komunikacji TCP pozwalający na zachowanie synchronizacji pomiędzy nadawcą i odbiorcą. Ponieważ protokół UDP jest bezpołączeniowy, ten rodzaj komunikacji można porównać do wrzucenia listu do skrzynki pocztowej. W większości przypadków nadawca po prostu umieszcza na kopercie adres odbiorcy, nakleja znaczek, a następnie wrzuca list do skrzynki pocztowej. Pracownik poczty zbiera listy, poczta wysyła do odpowiednich miejscowości, a na końcu listonosz dostarcza je adresatom. W tym przykładzie nadawca nie otrzymuje potwierdzenia dostarczenia listu adresatowi. Odkąd pracownik poczty wyjmie list ze skrzynki pocztowej, nie ma żadnej gwarancji dostarczenia listu do adresata.

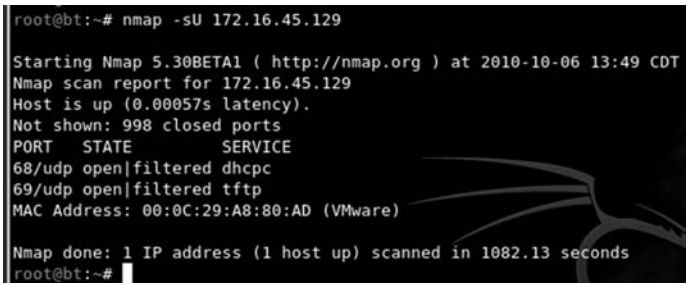
Skoro poznałeś podstawowe różnice pomiędzy protokołami TCP i UDP, musisz teraz zapamiętać, że nie każda usługa korzysta z protokołu TCP. Niektóre z ważniejszych usług wykorzystujących protokół UDP to między innymi DHCP, DNS (do poszczególnych zapytań), SNMP i TFTP. Jedną z najważniejszych cech osoby przeprowadzającej testy penetracyjne powinna być dokładność. Przeoczenie lub niedostrzeżenie usługi na

skutek braku przeprowadzenia skanowania UDP testowanego komputera może się okazać dla Ciebie bardzo kłopotliwe.

Zarówno skanowanie TCP, jak i SYN opiera się na protokole TCP. Jeżeli chcesz wykryć usługi wykorzystujące protokół UDP, musisz przeprowadzić skanowanie UDP za pomocą narzędzia Nmap. Na szczęście narzędzie znacznie ułatwia to zadanie. Aby przeprowadzić skanowanie UDP wybranego celu ataku, z poziomu powłoki wydaj następujące polecenie:

```
nmap –sU 172.16.45.129
```

Zwróć uwagę na różnice pomiędzy powyższym poleceniem i poleceniami przedstawionymi w poprzednich przykładach. W pierwszej kolejności nakazujemy narzędziu Nmap przeprowadzenie skanowania UDP, na co wskazuje opcja `-sU`. Bystry Czytelnik od razu zauważy brak opcji `-p` i `-PN` w poleceniu. Powód ich braku jest bardzo prosty: skanowanie UDP jest bardzo wolne. Przeprowadzenie nawet podstawowego skanowania UDP domyślnego tysiąca portów może zająć 20 – 30 minut. Możesz również zauważyć zmianę adresu IP. W omawianym przykładzie skanowany jest komputer działający pod kontrolą systemu Linux wraz z uruchomioną usługą TFTP. Dzięki temu będziesz mógł zobaczyć wyniki skanowania. Na rysunku 3.4 pokazano uruchomienie skanowania UDP i dane wyjściowe wygenerowane w jego wyniku.



RYSUNEK 3.4.
Skanowanie UDP i otrzymane w jego wyniku dane wyjściowe

Musisz koniecznie zapamiętać, że komunikacja UDP nie wymaga otrzymania odpowiedzi od adresata pakietu. Skoro komputer docelowy nie udziela odpowiedzi informującej o otrzymaniu pakietu, jak narzędzie Nmap może odróżnić port otwarty od portu chronionego przez zaporę sieciową? Innymi słowy, jeżeli usługa jest dostępna i przyjmuje pakiety UDP, normalne jej zachowanie polega po prostu na akceptacji pakietu, ale bez wysyłania nadawcy odpowiedzi w stylu „Otrzymałem pakiet". Podobnie jest w przypadku zapór sieciowych: często ich strategia polega na akceptacji pakietu i niewysyłaniu żadnej odpowiedzi do jego nadawcy. W omawianym przykładzie nawet jeśli jeden pakiet przejdzie, a drugi zostanie zablokowany przez zaporę sieciową, to z powodu braku udzielenia nadawcy odpowiedzi nie ma możliwości określenia, czy pakiet został zaakceptowany przez usługę, czy odrzucony przez zaporę sieciową.

Z tego powodu narzędzie Nmap ma bardzo utrudnione zadanie podczas ustalania, czy dany port jest otwarty, czy filtrowany. Dlatego też w przypadku braku odpowiedzi na operację skanowania UDP narzędzie Nmap wyświetla dla danego portu wiadomość o treści „open | filtered". Trzeba w tym miejscu koniecznie wspomnieć, że w rzadkich przypadkach usługa UDP będzie wysyłała odpowiedź do nadawcy pakietu. Wówczas narzędzie Nmap jest wystarczająco inteligentne, aby określić działającą usługę i opisać dany port jako otwarty („open").

Jak już wcześniej wspomniano, osoby dopiero rozpoczynające pracę polegającą na przeprowadzaniu testów penetracyjnych bardzo często nie doceniają wagi skanowania UDP. Prawdopodobnie wynika to z faktu, że większość zwykłych operacji skanowania UDP nie dostarcza zbyt wielu informacji, a niemal każdy port zostaje określony jako „open | filtered". Po przejrzeniu przykładowych danych wyjściowych uzyskanych w wyniku przeskanowania kilku komputerów bardzo łatwo można poczuć się rozczarowanym wynikami skanowania UDP. Jednak nie wszystko stracone! Twórcy narzędzia Nmap dostarczyli nam sposobu na otrzymanie znacznie bardziej użytecznych wyników skanowania UDP.

Aby otrzymać znacznie dokładniejsze wyniki ze skanowania UDP komputera, w poleceniu inicjującym skanowanie umieść opcję `-sV`. Opcja ta jest przeznaczona do przeprowadzania skanowania wersji, ale w omawianym przypadku pomaga również w zawężeniu wyników skanowania UDP.

Po włączeniu skanowania wersji narzędzie Nmap wysyła dodatkowe próbki do każdego portu określonego w wynikach skanowania UDP jako „open | filtered". Te dodatkowe próbki podejmują próbę identyfikacji usług poprzez wysłanie specjalnie przygotowanych pakietów. Dzięki wspomnianym specjalnie przygotowanym pakietom znacznie częściej można osiągnąć sukces w prowokowaniu adresata do udzielenia odpowiedzi. Bardzo często prowadzi to do zmiany wyniku oznaczenia portu z „open | filtered" na „open".

Jak już wcześniej wspomniano, najprostszy sposób dodania skanowania wersji do skanowania UDP polega na użyciu opcji `-sV`. Zwróć uwagę, że ponieważ wcześniej użyta została opcja `-sU`, wskazująca rodzaj skanowania, to dużą literę `V` można dodać do istniejącej opcji `-sU`. W ten sposób powstaje poniższe polecenie:

```
nmap –sUV 172.16.45.135
```

Użycie narzędzia Nmap do przeprowadzenia skanowania Xmas

W świecie komputerów RFC jest dokumentem zawierającym specyfikację techniczną opisującą daną technologię bądź standard. Dokument RFC może zawierać ogromną ilość szczegółowych informacji dotyczących wewnętrznego sposobu działania określonego systemu. Ponieważ dokument ten zawiera szczegóły techniczne dotyczące tego, jak system *powinien* działać, atakujący i hakerzy często przeglądają dokumentację w poszukiwaniu potencjalnych słabości lub dziur. Skanowanie typu Xmas i Null pozwala na wykorzystanie tego rodzaju dziur.

Nazwa skanowania Xmas bierze się z faktu włączenia flag FIN, PSH i URG pakietu. W wyniku tego pakiet ma włączonych tak dużo flag, że często jest określany mianem „świecącego jak choinka[2]". Ponieważ wcześniej omówiliśmy już komunikację TCP i proces nawiązywania połączenia, powinno być dla Ciebie jasne, że pakiet Xmas jest bardzo nietypowy z powodu braku włączonej flagi SYN lub ACK. Wspomniana nietypowość pakietu ma swój cel. Jeżeli implementacja TCP w skanowanym systemie działa zgodnie z założeniami przedstawionymi w odpowiednim dokumencie RFC, jeden z nietypowych pakietów można wysłać w celu określenia stanu portu.

Zgodnie z informacjami przedstawionymi w dokumencie RFC dotyczącym protokołu TCP: jeśli zamknięty port otrzyma pakiet nieposiadający włączonych flag SYN, ACK lub RST (czyli np. pakiet utworzony przez skanowanie Xmas), to port powinien udzielić odpowiedzi w postaci pakietu wraz z włączoną flagą RST. Co więcej, według tego samego dokumentu RFC jeśli port jest włączony i otrzyma pakiet bez ustawionej flagi SYN, ACK lub RST, pakiet powinien być zignorowany. Poświęć chwilę na ponowne przeczytanie dwóch poprzednich zdań, ponieważ mają one znaczenie krytyczne do zrozumienia odpowiedzi, którą będziemy otrzymywać w wyniku przeprowadzenia skanowania Xmas.

Jeśli przyjmiemy założenie o pełnej zgodności atakowanego systemu operacyjnego ze specyfikacją przedstawioną w dokumencie RFC TCP, narzędzie Nmap ma możliwość określenia stanu portu bez przeprowadzania pełnego połączenia z atakowanym komputerem, a nawet bez inicjowania takiego połączenia. Użyte zostało wyrażenie „jeśli przyjmiemy założenie", ponieważ nie każdy dostępny obecnie na rynku system operacyjny jest w pełni zgodny z RFC. Ogólnie rzecz biorąc, skanowanie Xmas i Null sprawdza się w odniesieniu do komputerów działających pod kontrolą systemu UNIX i Linux, ale nie Windows. Dlatego też wymienione rodzaje skanowania są nieefektywne, jeśli atakowany komputer posiada system operacyjny firmy Microsoft.

Aby przeprowadzić skanowanie Xmas, wystarczy po prostu w przedstawionym poprzednio poleceniu zastąpić opcję `-sU` opcją `-sX`. Wykonanie pełnego skanowania następuje więc po wydaniu z poziomu powłoki poniższego polecenia:

```
nmap –sX -p- -PN 172.16.45.129
```

Na rysunku 3.5 pokazano uruchomienie skanowania Xmas względem komputera działającego pod kontrolą systemu Linux.

Użycie narzędzia Nmap do przeprowadzenia skanowania Null

Skanowanie Null, podobnie jak Xmas, wykorzystuje pakiety niezgodne ze zdefiniowanymi założeniami komunikacji TCP. Pod wieloma względami skanowanie Null jest całkowitym przeciwieństwem skanowania Xmas, ponieważ wykorzystuje pakiety, które są pozbawione jakichkolwiek flag (czyli są zupełnie puste).

[2] Słowo *Xmas* oznacza w języku angielskim święta Bożego Narodzenia — *przyp. tłum.*

RYSUNEK 3.5.
Skanowanie Xmas i otrzymane w jego wyniku dane wyjściowe

Zaatakowany system odpowiada na skanowanie Null w dokładnie taki sam sposób jak w przypadku skanowania Xmas. Otwarty port w skanowanym systemie nie będzie udzielał żadnej odpowiedzi narzędziu Nmap, podczas gdy zamknięty port odpowie pakietem RST. Warto w tym miejscu przypomnieć, że tego rodzaju skanowanie jest niezawodne jedynie w przypadku systemu operacyjnego, który pozostaje w pełni zgodny ze specyfikacją RFC TCP.

Jedną z największych zalet stosowania skanowania Xmas i Null jest w pewnych sytuacjach możliwość ominięcia prostych filtrów i list kontroli dostępu (ang. *Access Control List* — ACL). Niektóre z prymitywnych filtrów działają poprzez blokowanie przychodzących pakietów SYN. Osoba stosująca tego rodzaju filtry sądzi, że odrzucanie pakietów SYN przez system uniemożliwi przeprowadzenie procesu nawiązania połączenia. Jeżeli nie dojdzie do procesu nawiązania połączenia, nie wystąpi strumień komunikacji TCP pomiędzy systemami, a dokładniej: żadna komunikacja TCP nie będzie mogła zostać zainicjowana poza tak chronionym komputerem.

Trzeba koniecznie zrozumieć, że celem skanowania Xmas i Null nie jest utworzenie jakiegokolwiek kanału komunikacji, lecz jedynie określenie, czy dany port jest otwarty, czy zamknięty.

Mając na uwadze dwa powyższe akapity, rozważmy następujący przykład. Przyjmujemy założenie, że administrator sieci w osobie Bena Owneda zainstalował prostą zaporę sieciową, która ma uniemożliwić inicjowanie z zewnątrz jakichkolwiek połączeń z jego systemem. Wspomniana zapora sieciowa działa po prostu poprzez odrzucanie całego nadchodzącego ruchu sieciowego, na początku którego znajduje się pakiet SYN. Ben zatrudnił swojego przyjaciela (etycznego hakera) do przeskanowania jego systemu. Etyczny haker przeprowadza skanowanie TCP, które nie przynosi żadnych wyników. Ponieważ jest doświadczonym hakerem, przeprowadza kolejne operacje skanowania, tym razem UDP, Xmas i Null. Na twarzy etycznego hakera pojawia się uśmiech, gdy dostrzega, że skanowanie Xmas i Null ujawniło w systemie Bena otwarte porty.

Powyższy scenariusz można zrealizować za pomocą narzędzia Nmap, ponieważ pozwala ono na utworzenie pakietów bez włączonej flagi SYN. Skoro filtr odrzuca jedynie pakiety przychodzące, które zawierają flagę SYN, to pakiety wygenerowane przez ska-

nowanie Xmas i Null są przepuszczane. Aby przeprowadzić skanowanie Null, należy z poziomu powłoki wydać następujące polecenie:

```
nmap –sN -p- -PN 172.16.45.129
```

Podsumowanie skanowania portów

Po omówieniu podstaw skanowania portów warto jeszcze wspomnieć o kilku opcjach, które możesz uznać za użyteczne po zdobyciu większego doświadczenia w zakresie przeprowadzania testów penetracyjnych.

Jak już wcześniej wspomniano, opcja `-sV` powoduje przeprowadzenie skanowania wersji. W trakcie tego skanowania narzędzie Nmap wysyła próbki do otwartych portów i próbuje ustalić pewne informacje o usłudze nasłuchującej na danym porcie. O ile to możliwe, narzędzie Nmap dostarczy szczegółowych informacji o usłudze, jak na przykład numer wersji. Tego rodzaju informacje powinieneś zachować w swoich notatkach. Używanie opcji `-sV` jest zalecane w każdej sytuacji, gdy tylko jest możliwe, zwłaszcza w przypadku nietypowych lub nieoczekiwanych portów — przecież przebiegły administrator mógł przenieść obsługę serwera WWW na port 34567, aby spróbować ją w ten sposób dodatkowo ochronić.

Narzędzie Nmap zawiera opcję `-T`, pozwalającą na zmianę szybkości skanowania portu. Wartość liczbowa wymienionej opcji mieści się w zakresie od `0` do `5`, gdzie `0` oznacza najwolniejsze skanowanie, natomiast `5` — najszybsze. Zastosowanie wspomnianej opcji będzie użyteczne w sytuacji, w której będziesz próbował uniknąć wykrycia operacji skanowania poprzez jej spowolnienie. Inny przykład: masz do przeskanowania ogromną liczbę adresów IP, a jednocześnie ilość czasu jest ograniczona, rezygnujesz więc z pełnego skanowania na rzecz szybszego. Musisz pamiętać, że w przypadku najszybszej operacji skanowania narzędzie Nmap może dostarczać mniej dokładnych wyników.

Wreszcie, opcja `-O` może być użyteczna podczas ustalania systemu operacyjnego używanego w skanowanym komputerze. Przydaje się, gdy chcesz sprawdzić, czy atakujesz komputer działający pod kontrolą systemu operacyjnego Windows, Linux, a może jeszcze innego. Poznanie rodzaju systemu operacyjnego w atakowanym komputerze zaoszczędzi Ci czasu, ponieważ pozwala skoncentrować się na atakowaniu znanych słabych punktów tego systemu. Nie ma żadnego sensu próba wykorzystania słabych punktów systemu Linux, jeśli atakowany komputer działa pod kontrolą Windows.

Po zakończeniu skanowania portów w atakowanym komputerze powinieneś posiadać listę otwartych portów i działających na nich usług. Te informacje trzeba zachować, a następnie dokładnie przeanalizować. Podczas analizy danych wyjściowych dostarczonych przez narzędzie Nmap poświęć chwilę na próbę zalogowania się do usług zdalnego dostępu, które mogłeś wykryć podczas skanowania. W kolejnym rozdziale będą przedstawione narzędzia pozwalające na przeprowadzenie ataku typu brute force w celu zalogowania się. Na obecnym etapie możesz spróbować się zalogować z użyciem domyślnych nazw użytkowników i haseł. Ponadto spróbuj się zalogować, używając informacji, nazw

użytkowników i adresów e-mail zebranych w fazie rekonesansu. Istnieje możliwość ukończenia testu penetracyjnego po prostu poprzez odkrycie otwartego zdalnego połączenia i zalogowanie się do systemu za pomocą domyślnej nazwy użytkownika i hasła. Telnet i SSH to doskonałe przykłady usług zdalnego dostępu, do których zawsze powinieneś spróbować się zalogować. Poniżej przedstawiono polecenia pozwalające na zalogowanie się do wymienionych usług:

```
telnet docelowy_adres_ip
ssh root@docelowy_adres_ip
```

W powyższych poleceniach `docelowy_adres_ip` oznacza adres atakowanego komputera. W większości przypadków te próby okażą się nieudane, ale niekiedy zakończą się powodzeniem.

SKANOWANIE SYSTEMU POD KĄTEM JEGO PODATNOŚCI NA ATAK

Mając listę adresów IP, otwartych portów i usług działających w atakowanym komputerze, można przystąpić do jego przeskanowania w poszukiwaniu luk w zabezpieczeniach. Luka to słaby punkt w oprogramowaniu lub konfiguracji systemu, umożliwiający przeprowadzenie ataku. Luki mogą występować w wielu różnych postaciach i odmianach, ale najczęściej są powiązane z niezainstalowaniem odpowiednich poprawek. Producenci oprogramowania często wydają poprawki, w których usuwane są znane problemy bądź luki w zabezpieczeniach. Oprogramowanie i system bez zainstalowanych poprawek bardzo często stają się celem ataku penetracyjnego, ponieważ niektóre luki pozwalają na zdalne wykonywanie kodu. Wspomniane zdalne wykonywanie kodu to niewątpliwie Święty Graal hakera.

Trzeba koniecznie zrozumieć, że operacja skanowania pod kątem podatności systemu na atak — i otrzymane dzięki niej wyniki — prowadzi bezpośrednio do trzeciego kroku testu penetracyjnego, którym jest uzyskanie dostępu do atakowanego systemu. Aby przeskanować system pod kątem wykorzystania jego luk w zabezpieczeniach, musisz użyć odpowiedniego skanera. Do dyspozycji masz wiele dobrych skanerów, ale w niniejszej książce skoncentrujemy się na narzędziu Nessus.

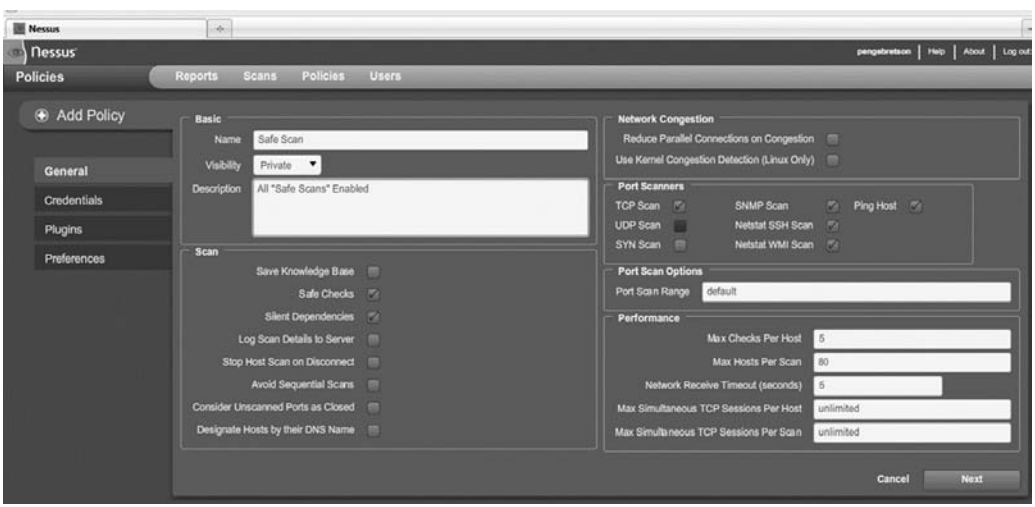
Nessus to doskonałe narzędzie dostępne bezpłatnie dla użytkowników domowych. Na witrynie producenta możesz je pobrać i otrzymać bezpłatnie klucz rejestracyjny. Jeżeli chcesz używać Nessusa w firmie, będziesz musiał pobrać wersję Professional (a nie Home) i za nią zapłacić. Obecnie opłata wynosi 1500 dolarów rocznie. W książce będziemy korzystali z narzędzia w wersji dla użytkowników domowych (bezpłatnej).

Narzędzie Nessus działa zarówno w systemie Linux, jak i Windows, a jego instalacja jest bardzo łatwa. Nessus działa na zasadzie klient-serwer. Po zakończeniu konfiguracji serwer działa niewidocznie w tle, natomiast Ty komunikujesz się z nim za pomocą przeglądarki internetowej. Aby zainstalować narzędzie Nessus w systemie, wykonaj przedstawione poniżej kroki.

1. Pobierz plik instalacyjny z witryny *http://www.tenable.com/products/nessus*.
2. Na podanej witrynie zarejestruj się (podając adres e-mail) w celu otrzymania bezpłatnego klucza. Producent wygeneruje dla Ciebie unikalny klucz, który wykorzystasz do odblokowania narzędzia Nessus.
3. Zainstaluj aplikację.
4. Utwórz użytkownika Nessus, aby uzyskać dostęp do systemu.
5. Uaktualnij wtyczki.

Jednym z kluczowych komponentów narzędzia Nessus są wtyczki. Wspomniana wtyczka to niewielki blok kodu wysyłany do atakowanego komputera w celu sprawdzenia, czy występuje w nim znana luka w zabezpieczeniach. Narzędzie Nessus ma dosłownie tysiące wtyczek. Trzeba je pobrać z internetu po pierwszym uruchomieniu narzędzia. Domyślna instalacja Nessusa spowoduje, że będzie on automatycznie uaktualniał wtyczki.

Po zainstalowaniu serwera Nessus możesz uzyskać do niego dostęp, uruchamiając przeglądarkę internetową i podając adres *https://127.0.0.1:8834* — o ile próbujesz uzyskać dostęp do Nessusa na tym samym komputerze, na którym został zainstalowany jego serwer. Nie zapomnij o podaniu protokołu `https`, ponieważ Nessus używa bezpiecznego połączenia podczas komunikacji z serwerem. Na ekranie zobaczysz ekran logowania — musisz tutaj podać nazwę użytkownika i hasło utworzone podczas instalacji narzędzia. Po zalogowaniu się zobaczysz ekran podobny do pokazanego na rysunku 3.6.



RYSUNEK 3.6.
Sesja z narzędziem Nessus

Zanim będziesz mógł używać Nessusa, musisz zdefiniować politykę skanowania stosowaną przez to narzędzie. W tym celu kliknij łącze *Policies* widoczne w górnym menu wyświetlonej strony internetowej. Konfiguracja polityki wymaga określenia jej nazwy. Jeżeli zamierzasz przygotować kilka rodzajów polityki, powinieneś także utworzyć ich

opisy. Poświęć chwilę na analizę rysunku 3.6 i zwróć uwagę na zaznaczenie pola wyboru *Safe Checks*.

W trakcie pierwszej konfiguracji narzędzia Nessus powszechnie stosowane rozwiązanie polega na utworzeniu dwóch rodzajów polityki, po jednej z zaznaczoną i niezaznaczoną opcją *Safe Checks*. Powód jest bardzo prosty: niektóre wtyczki i operacje sprawdzania są uznawane za niebezpieczne, ponieważ polegają na rzeczywistej próbie wykorzystania luki w zabezpieczeniach sprawdzanego systemu. Musisz mieć świadomość, że usunięcie zaznaczenia pola wyboru *Safe Checks* może potencjalnie doprowadzić do zaburzeń działania sieci i systemu, a nawet do jego całkowitego wyłączenia. Poprzez zdefiniowanie dwóch rodzajów polityki z włączoną i wyłączoną opcją *Safe Checks* możesz uniknąć wprowadzenia niezamierzonych zaburzeń w działaniu sieci.

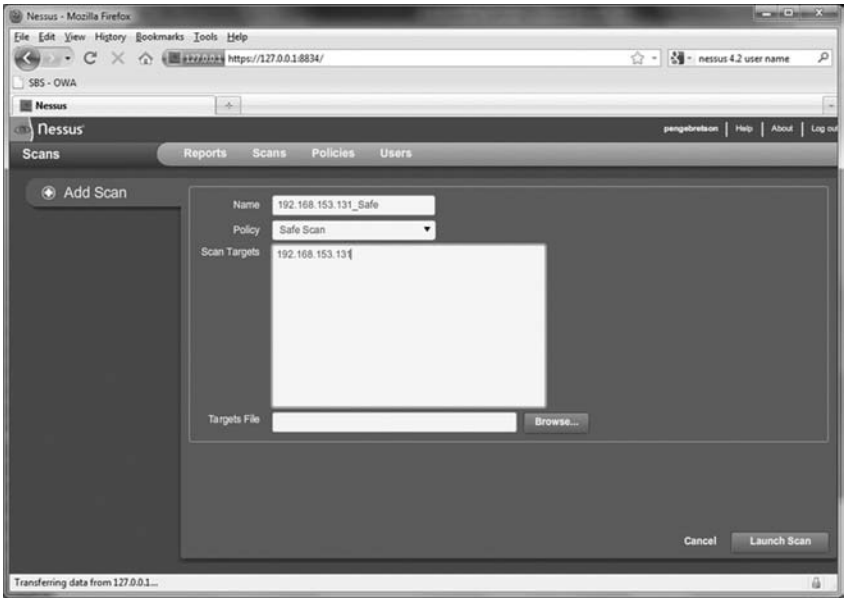
Istnieje wiele opcji, dzięki którym operację skanowania możesz dostosować do własnych potrzeb. Na potrzeby przykładów omawianych w książce będziemy stosowali konfigurację domyślną. Poświęć chwilę na przejrzenie różnych opcji. Klikając przycisk *Next* wyświetlany w prawym dolnym rogu, przejdziesz przez wszystkie opcje dodatkowe, które można ustawić dla skanowania.

Po skonfigurowaniu skanowania zapisz opcje, klikając przycisk *Submit*, który zostanie wyświetlony po przejrzeniu wszystkich dostępnych opcji konfiguracyjnych. Politykę skanowania musisz skonfigurować tylko jednokrotnie. Po zapisaniu opcji będziesz mógł korzystać z tak przygotowanej polityki do przeprowadzania operacji skanowania systemu pod kątem podatności na atak.

Kiedy polityka została zdefiniowana i zapisana, możesz rozpocząć skanowanie wybranego celu. Aby rozpocząć operację, kliknij łącze *Scans* znajdujące się w górnym menu. Możesz podawać pojedyncze adresy w celu przeskanowania poszczególnych systemów lub listę adresów IP określających wiele systemów do przeskanowania. Zawartość strony Scans została pokazana na rysunku 3.7.

Podaj nazwę dla skanowania, wybierz politykę i adres IP celu. Jeżeli chcesz przeskanować pojedynczy system, podaj jego adres IP w polu *Scan Targets*. Jeśli natomiast adresy IP celów zapisałeś w pliku tekstowym, możesz go wczytać po kliknięciu przycisku *Browse…*. Gdy wszystko będzie przygotowane, kliknięcie przycisku *Launch Scan* znajdującego się w prawym dolnym rogu rozpoczyna operację skanowania. W trakcie skanowania narzędzie Nessus wyświetla informacje o jego przebiegu.

Kiedy narzędzie Nessus zakończy skanowanie, jego wyniki możesz przejrzeć po kliknięciu przycisku *Reports* znajdującego się w menu głównym. Wyświetlony raport zawiera szczegółową listę wszystkich luk w zabezpieczeniach znalezionych przez Nessusa. Szczególnie powinieneś się zainteresować znaleziskami oznaczonymi jako *High*. Poświęć nieco czasu na dokładną analizę raportu i sporządzenie szczegółowych notatek o przeskanowanym systemie. Przygotowane tutaj informacje wykorzystasz w kolejnym kroku testu penetracyjnego, czyli podczas próby uzyskania dostępu do systemu.



RYSUNEK 3.7.
Przygotowanie do rozpoczęcia skanowania za pomocą narzędzia Nessus

Po zakończeniu skanowania portów w celu znalezienia luk w zabezpieczeniach względem wszystkich wyznaczonych celów masz zebraną wystarczającą ilość informacji, aby przystąpić do ataku na system.

JAK ĆWICZYĆ SKANOWANIE PORTÓW?

Najłatwiejszym sposobem ćwiczenia operacji skanowania portów jest przygotowanie dwóch komputerów lub użycie maszyn wirtualnych. Powinieneś wypróbować wszystkie opcje i typy skanowania omówione w rozdziale. Zwróć szczególną uwagę na dane wyjściowe wygenerowane przez każdą operację skanowania. Operacje skanowania przeprowadź względem komputerów działających pod kontrolą zarówno systemu Windows, jak i Linux.

Na skanowanych komputerach powinieneś włączyć pewne usługi lub zainstalować oprogramowanie dodatkowe, aby mieć pewność, że system będący przedmiotem skanowania będzie miał otwarte porty. Dobrym rozwiązaniem jest instalacja i uruchomienie FTP, serwera WWW, telnetu lub SSH.

W przypadku osoby, która po raz pierwszy spotyka się ze skanowaniem portów, jednym z najlepszych sposobów doskonalenia umiejętności jest wybór podsieci i ukrycie adresu IP w sieci. Po ukryciu celu w podsieci zadaniem uczącego się jest jego zlokalizowanie. Po odszukaniu celu kolejnym zadaniem jest przeprowadzenie pełnego skanowania systemu.

Aby pomóc w zastosowaniu przedstawionego powyżej rozwiązania, utworzyłem prosty skrypt odpowiedzialny za ukrycie systemu w danej podsieci. Kod jest przeznaczony do uruchomienia w systemie Linux. Oczywiście możesz go dowolnie zmodyfikować i zmienić adres IP, aby działał w Twojej sieci. Skrypt generuje dowolną liczbę z zakresu od 1 do 254, która następnie będzie użyta jako ostatnia liczba w adresie IP komputera. Po wygenerowaniu losowo wybranego adresu IP zostaje on przypisany komputerowi.

Dzięki uruchomieniu przedstawionego skryptu będziesz mógł przećwiczyć pracę z narzędziami i technikami omówionymi w rozdziale. Kod skryptu wprowadź w dowolnym edytorze tekstów, a następnie zapisz plik pod nazwą *ip_gen.sh*.

```
#!/bin/bash
echo "Konfiguracja komputera ofiary, to może chwilę potrwać..."
ifconfig eth0 down
ifconfig eth0 172.16.45.$((( $RANDOM %254) ! 1)) up
# Usunięcie znaku # z początku poniższych wierszy powoduje uruchomienie usług w komputerze
ofiary.
# Pamiętaj, w zależności od używanej dystrybucji może wystąpić potrzeba zmiany ścieżek
dostępu.
#/etc/init.d/ssh start
# Uwaga, może wystąpić konieczność wygenerowania klucza SSH za pomocą sshd-generate.
#/etc/init.d/apache2 start
#/etc/init.d/atftpd start
echo "Komputer ofiary został skonfigurowany."
echo "Adres IP komputera należy do sieci 172.16.45.0/24."
echo "Możesz już zamknąć to okno i rozpocząć atak... Powodzenia!"
```

Następnie otwórz okno aplikacji Terminal i przejdź do katalogu, w którym zapisałeś plik skryptu. Przed uruchomieniem skryptu trzeba nadać plikowi uprawnienia do jego uruchamiania. W tym celu wystarczy wydać następujące polecenie:

```
chmod 755 ip_gen.sh
```

Aby uruchomić skrypt, w oknie aplikacji Terminal wydaj polecenie:

```
./ip_gen.sh
```

Skrypt powinien wyświetlić komunikat informujący o zakończeniu konfiguracji komputera ofiary. Dzięki użyciu skryptu takiego jak przedstawiony powyżej masz możliwość doskonalenia umiejętności w zakresie wyszukiwania systemu i jego skanowania.

CO DALEJ?

Po opanowaniu podstaw używania Nmap i Nessus powinieneś zagłębić się w bardziej zaawansowane opcje dostępne w obu narzędziach. W tym rozdziale przedstawiono zaledwie ułamek oferowanych przez nie możliwości. Witryna *http://insecure.org/* to doskonały zasób wiedzy dotyczącej narzędzia Nmap. Naprawdę powinieneś poświęcić nieco czasu na poznanie opcji wbudowanych w narzędzie Nmap. Nessus posiada także mnóstwo funkcji dodatkowych, które nie zostały omówione w rozdziale.

Kiedy już będziesz swobodnie korzystał z zaawansowanych funkcji narzędzi Nmap i Nessus, powinieneś skierować swoją uwagę ku innym dostępnym skanerom. Obecnie dostępne są dziesiątki dobrych skanerów. Wybierz kilka, zainstaluj je i poznaj ich funkcje. Na rynku znajdziesz także kilka produktów komercyjnych, które powinieneś znać. Nie są one opracowane wyłącznie jako skanery wyszukujące luki w zabezpieczeniach, ale oferują znacznie więcej możliwości. Narzędzia Core Impact i Saint doskonale sprawdzają się w ocenie luk w zabezpieczeniach, choć wymagają wyłożenia prawdziwych pieniędzy na ich zakup.

PODSUMOWANIE

W rozdziale skoncentrowaliśmy się na drugim kroku testu penetracyjnego, czyli przede wszystkim na skanowaniu. Na początku przedstawione zostało ogólne omówienie działania polecenia `ping`, a dopiero potem właściwe zagadnienie skanowania. Sam temat skanowania został podzielony na dwie odrębne części: skanowanie portów oraz skanowanie w poszukiwaniu luk w zabezpieczeniach. Narzędzie Nmap przeznaczone do skanowania portów pozwala na przeprowadzenie różnych typów skanowania, które zostały omówione w rozdziale. Ponadto zademonstrowano rzeczywiste przykłady i dane wyjściowe różnych operacji skanowania, a także sposób interpretacji danych wyjściowych generowanych przez narzędzie Nmap. Koncepcję skanowania w poszukiwaniu luk w zabezpieczeniach przedstawiono poprzez użycie narzędzia Nessus. W rozdziale znalazły się praktyczne przykłady wykorzystania wymienionego narzędzia.

Skorowidz

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z

Kompendium wiedzy na temat testów penetracyjnych!

Współczesne systemy informatyczne przetwarzają gigantyczne ilości niezwykle wrażliwych danych — osobowych, medycznych czy finansowych. Ich utrata lub przejęcie przez niepowołane osoby może oznaczać katastrofę dla firmy. Dlatego etyczny hacking i testy penetracyjne to coś, co może przynieść dużo satysfakcji i pożytku, a przy tym jest opłacalne finansowo!

W jaki sposób zostać specjalistą? Jakie narzędzia będą Ci potrzebne oraz na co zwrócić szczególną uwagę? Na te i wiele innych pytań odpowiada ta wyjątkowa książka. W trakcie lektury dowiesz się, jak korzystać z nowoczesnych narzędzi oraz jak interpretować otrzymane wyniki. W kolejnych rozdziałach znajdziesz informacje na temat różnych form ataków oraz metod utrzymania dostępu po udanym ataku. Na koniec nauczysz się przygotowywać raport dla zleceniodawcy – taki, który będzie zrozumiały nawet dla laika. Książka ta jest obowiązkową lekturą dla wszystkich pasjonatów bezpieczeństwa systemów informatycznych. Warto ją mieć pod ręką!

Dowiedz się, jak:

- przeprowadzić rekonesans
- skanować oraz odkrywać strukturę sieci
- wykorzystywać luki w zabezpieczeniach
- utrzymywać dostęp do maszyny
- przygotowywać przejrzyste i czytelne raporty z testów penetracyjnych

helion.pl
księgarnia internetowa

Nr katalogowy: 13758

Księgarnia internetowa
http://helion.pl

Zamówienia telefoniczne:
0 801 339900
0 601 339900

Helion

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

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

Informatyka w najlepszym wydaniu

ISBN 978-83-246-6653-9

9 788324 666539

cena: 39,00 zł