STUDIA INFORMATICA 2002
Volume 23 Number 3 (50)

Jacek LACH
Politechnika Śląska, Instytut Informatyki

SPOSOBY UZYSKIWANIA INFORMACJI O SIECI I WYBRANE METODY PRZECIWDZIAŁANIA

Streszczenie. W artykule przedstawiony został przegląd technik stosowanych przez komputerowych włamywaczy, umożliwiających uzyskanie informacji na temat atakowanej sieci. Techniki te stosuje inżynier bezpieczeństwa w celu oceny jakości zabezpieczeń systemu. Przedstawione zostały kolejne etapy początku procesu włamania: wywiad środowiskowy, rekonesans sieci, identyfikacja systemu, a także podstawowe sposoby unikania związanych z tym zagrożeń.

METHODS OF COLLECTING NETWORK INFORMATION AND SELECTED COUNTERMEASURES

Summary. This article describes methods of collecting information on network configuration that are frequently used by attackers to get the overall view of its security. Introductory steps to breaking into the system were presented: social engineering, network mapping, operating system identification as well as some countermeasures that should be taken to reduce the risk.

1. Wstęp

Jedną z najbardziej skutecznych metod badania zabezpieczeń systemów komputerowych jest przeprowadzenie symulowanego ataku wykorzystującego wszystkie techniki stosowane zwykle przez włamywacza. Podejście takie nazywane jest testem penetracyjnym. Test taki wykonuje specjalista od zabezpieczeń podczas badań związanych z oceną podatności systemu na określone techniki włamania. Testy penetracyjne mogą być wykonywane zarówno przez firmowych specjalistów, jak i przez zewnętrzne firmy (tzw. włamanie na zamówienie). Wykonywanie testu penetracyjnego ma dwa podstawowe cele:

- Weryfikacja działających zabezpieczeń oraz ewentualnie wykrycie luk w zabezpieczeniach istniejących w ramach aktualnie prowadzonej polityki bezpieczeństwa. Prowadzenie testu w sposób zbliżony do zachowania się potencjalnego włamywacza ma na celu ocenę rzeczywistego poziomu zabezpieczeń systemu komputerowego.
- Weryfikacja poprawnego działania (identyfikacja incydentów oraz ich rejestracja w celu późniejszej identyfikacji intruza oraz lokalizacji zniszczeń) systemów identyfikacji włamań.

Wykonywanie testu penetracyjnego wiąże się z pewnym ryzykiem dla testowanego systemu, np. test podatności na atak typu DoS może skutecznie unieruchomić badany serwer. Z tego powodu należy dokładnie zaplanować przebieg wykonywania testu (czas wykonania, sposób gromadzenia wyników, kolejność wykonywania testów). W przypadku systemów o kluczowym znaczeniu może być konieczne pominięcie części testów mogących zakłócić ich poprawną pracę lub odłożenie ich do czasu, gdy chwilowa przerwa w działaniu będzie dopuszczalna. Przed wykonaniem całości testów należy zapewnić wykonanie uaktualnienia kopii zapasowej systemu, w zależności od rodzaju przeprowadzanego testu może bowiem dojść nawet do utraty ważnych danych przechowywanych w badanym systemie.

Wykonywanie testu penetracyjnego można podzielić na kilka etapów, które zostaną przedstawione w kolejnych punktach artykułu.

2. Wywiad środowiskowy

Etap ten jest często pomijany w przypadku rutynowych testów bezpieczeństwa, jednak jest równie często wykorzystywany przez włamywaczy dla zdobycia podstawowych informacji na temat badanego systemu. Etap ten polega m.in. na analizie zawartości stron WWW znajdujących się na serwerze pod kątem informacji mogących ułatwić włamywaczowi uzyskanie podstawowych informacji na temat serwera (pracujący system operacyjny, wersja systemu, zainstalowane oprogramowanie), podobne informacje można próbować uzyskać z nadmiarowych rekordów umieszczanych w strukturze DNS przez nieświadomych (niebezpieczeństwa) administratorów. Do technik wykorzystywanych przez bardziej zdeterminowanych włamywaczy należy również śledzenie zawartości stron administratorów systemu oraz list dyskusyjnych, w których administratorzy docelowego systemu biorą aktywny udział.

3. Rekonesans sieci

Rekonesans sieci jest pierwszym etapem badania zabezpieczeń, w którym włamywacz podejmuje aktywne działanie. Operacja ta ma na celu ustalenie działających w sieci komputerów, jak również struktury połączeń wewnątrz sieci, aby możliwe było skuteczne przeprowadzenie kolejnych etapów ataku.

Do standardowych metod badania dostępności hosta należy użycie pakietów ICMP typu *ECHO Request/ECHO Replay*. Narzędzie umożliwiające ich użycie jest dostępne pod postacią polecenia ping:

```
$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) from 10.0.0.2 : 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=0 ttl=255 time=501 usec
64 bytes from 10.0.0.1: icmp_seq=1 ttl=255 time=497 usec
64 bytes from 10.0.0.1: icmp_seq=2 ttl=255 time=491 usec

--- 10.0.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.491/0.496/0.501/0.018 ms
```

Modyfikacja działania tego programu polegająca na skanowaniu równoległym całej podsieci nosi nazwę omiatania (*ang. ping sweep*).

Prostszym sposobem, w przypadku wielu wersji systemu UNIX (Linux, Solaris, HP-UX), uzyskania informacji o działających hostach w sieci jest jednak wysłanie pakietu *Echo request* na adres rozgłoszeniowy lub adres sieci. Spowoduje to uzyskanie odpowiedzi od wszystkich aktywnych komputerów w sieci za pomocą jednego tylko wysłanego pakietu. Ponieważ zgodnie z RFC 1122 ignorowanie żądań ICMP *Echo Request* skierowanych na adresy rozgłoszeniowe jest dopuszczalne, dobrze jest zablokować reakcje systemów na tego typu zdarzenia. Jest to konfiguracja domyślna w systemach z rodziny Windows oraz *BSD.

Innymi typami komunikatów ICMP używanymi przy wykrywaniu dostępności hosta są:

- *Timestamp Request* - umożliwia odpytanie zdalnego hosta o aktualny czas, uzyskanie odpowiedzi wskazuje na działanie hosta, cecha ta zgodnie z RFC 1122 nie musi być implementowana, jednak większość systemów ją obsługuje.
- *Information Request* - przeznaczona dla systemów samokonfigurujacych się. Zgodnie z wytycznymi z RFC 1812 routery nie powinny generować tego typu komunikatów ani na nie odpowiadać, hosty nie powinny mieć zaimplementowanej obsługi. Słuszne jest więc blokowanie tego rodzaju komunikatów przez urządzenie filtrujące.

- *Address Mask Request* - przeznaczona do konfiguracji urządzeń bezdyskowych. Obsługa tego komunikatu nie jest wymagana, można wiec całkowicie te komunikaty zablokować.

Do bardziej zaawansowanych technik wykrywania dostępności hosta należą techniki wykorzystujące:

- wymuszanie komunikatów ICMP o błędach w niepoprawnych pakietach IP skierowanych do usług, do których dostęp nie jest blokowany przez urządzenia filtrujące,
- nietypowe ustawienia typu protokołu, powodujące generacje komunikatu ICMP *Destination Unreachable* wskazującego na brak obsługi wymaganego protokołu,
- nadużycie fragmentacji: po wysłaniu pewnego tylko podzbioru pofragmentowanego pakietu, host docelowy po pewnym czasie odrzuci niekompletne fragmenty zwracając komunikat ICMP *Fragment Reassembly Time Exceeded*,
- nieprawidłowości w konfiguracji sieci: jeżeli routery wewnętrzne mają wartość MTU mniejszą niż router zewnętrzny, to skierowanie do sieci pakietu o wielkości przekraczającej MTU routerów wewnętrznych z ustawioną flagą DF spowoduje generację komunikatu *Fragmentation Needed and Don't Fragment Bit was Set.*

Wszystkie wymienione metody w większości przypadków umożliwiają również detekcję urządzenia filtrującego na drodze pakietów.

W przypadku gdy badana sieć jest chroniona za pomocą urządzeń filtrujących, możliwe jest wykorzystanie techniki nazywanej mapowaniem odwrotnym (*ang. inverse mapping*). Wykorzystuje ona komunikaty routera o niedostępności hosta docelowego (*Host Unreachable*) do oceny sytuacji w badanej sieci. Technika ta umożliwia określenie hostów niedostępnych, pozostałe hosty są dostępne lub filtrowane.

Metody wcześniej omówione służą do sprawdzenia, czy konkretne hosty w badanej sieci są dostępne. Inną informacją, często poszukiwaną przez włamywacza, jest informacja dotycząca struktury sieci. Informację taką można uzyskać za pomocą polecenia *traceroute*. Metoda ta cechuje się jednak małą skutecznością. Przyczyny niskiej skuteczności tej metody leżą w filtrowaniu ruchu UDP w chronionej sieci. Wykonanie polecenia z opcją -I wymusza użycie pakietów ICMP *Echo Request* w miejsce datagramów UDP. Częściowo informacje te można również uzyskać przy użyciu polecenia *ping*, jednak z powodu ograniczonego rozmiaru nagłówka pakietu, w którym przechowywane są informacje o trasie pakietu, informacje te mogą nie być tak obszerne. Skuteczne przebadanie struktury sieci jest również niemożliwe w przypadku istnienia dodatkowych zabezpieczeń w badanej sieci.

W przypadku badania sieci zabezpieczonej za pomocą urządzenia filtrującego używana jest technika o nazwie *Firewalking*. Umożliwia ona określenie reguł filtrowania oraz

dostępności hostów za urządzeniem filtrującym, opierając swoje działanie na ruchu pakietów imitujących ruch dopuszczany przez urządzenie filtrujące.

4. Skanowanie portów

Skanowanie portów (*ang. port scanning*) jest jedną z najpopularniejszych metod stosowaną do określenia usług działających na badanym systemie w celu wykorzystania dobrze znanych luk w ich zabezpieczeniach. Określenie to odbywa się poprzez sprawdzenie, na którym z dobrze znanych portów nasłuchuje proces demona/serwisu. Następnie możliwe jest określenie typu świadczonej usługi na podstawie numeru portu.

W programach umożliwiających skanowanie portów można spotkać następujące metody:

- Skanowanie proste (*TCP connect() scanning*) jest najprostszą metodą, wykorzystującą wywołanie systemowe. Jest to metoda szybka (możliwość równoległego tworzenia połączeń), nie wymagająca specjalnych uprawnień w systemie, jednak łatwo wykrywalna, nawet w systemie bez jakichkolwiek zabezpieczeń.
- Skanowanie półotwarte (*TCP SYN scanning*) polega na rozpoczęciu poprawnego połączenia poprzez wysłanie pakietu SYN. Jeżeli na badanym porcie nasłuchuje usługa, podejmie ona połączenie poprzez odesłanie SYN|ACK, w przeciwnym razie w odpowiedzi uzyskamy RST. Metoda ta jest monitorowana przez mniejszą liczbę systemów (połączenie TCP zostaje zerwane przed nawiązaniem pełnego, poprawnego połączenia), jednak każdy przyzwoity system detekcji włamań potrafi taką próbę zidentyfikować.
- Skanowanie ukryte (*TCP FIN scanning*) bazuje na odpowiedzi uzyskanej po wysłaniu pakietu z ustawioną flagą FIN (port otwarty - w odpowiedzi pakiet z ustawioną flagą RST). Pakiety takie są czasem przepuszczane przez filtry pakietowe, gdy odpowiadający pakiet z flaga SYN jest blokowany. Metoda ta ma kilka odmian (Xmas, Ymas, Null), w których ustawione są inne flagi pakietu, jednak wykorzystują tę samą zasadę.
- Skanowanie fragmentami polega na wykorzystaniu omówionych technik przy podzieleniu pakietu próbkującego na małe fragmenty. Fragmenty takie mogą być przepuszczane przez urządzenia filtrujące, nie dokonujące składania fragmentów. Ustawienia takie zdarzają się, gdy urządzenie filtrujące jest mocno obciążone i składanie fragmentów zostało wyłączone ze względu na wydajność.
- Skanowanie z włączoną flagą ACK umożliwia uzyskanie informacji na temat urządzenia filtrującego (prosty filtr pakietowy lub filtr stanowy).

- Skanowanie UDP wykorzystuje fakt, że większość systemów wysyła komunikat ICMP *Port unreachable* przy próbie wysłania pakietu do zamkniętego portu UDP.

Wśród różnych metod skanowania poniższe nie tylko mają dać obraz badanego systemu, ale jednocześnie mają pozwolić na ukrycie adresu, z którego atak następuje:

- Skanowanie *dumb host* - wykorzystuje możliwość przewidywania sekwencji numeracji pakietów w celu określenia dostępności portów atakowanego systemu poprzez fałszowanie pakietów i monitorowanie hosta wykorzystywanego do skanowania.
- *FTP bounce attack* wykorzystuje cechę protokołu FTP udostępniającą połączenia proxy. Metoda skuteczna nawet przy nowych wersjach serwerów FTP, niektóre z nich umożliwiają przeprowadzenie tego typu ataku na nieuprzywilejowane porty.
- *Decoy scanning* - metoda ta to skanowanie przeprowadzone dowolną z wyżej wymienionych metod z modyfikacją polegającą na wysyłaniu dodatkowo dużej liczby pakietów ze sfałszowanymi adresami źródłowymi w celu ukrycia faktycznego adresu, z którego odbywa się atak.

Bardziej szczegółowy opis można znaleźć w [1] [2] i [3].

5. Identyfikacja systemu

Identyfikacja systemu operacyjnego to etap, podczas którego dokonywane jest ustalenie rodzaju działającego systemu operacyjnego wraz z jak najdokładniejszym ustaleniem jego wersji. Rozpoznanie to może odbywać się przy wykorzystaniu błędów w konfiguracji badanego systemu lub przy zastosowaniu zaawansowanych technik nazywanych technikami badania odcisku palca (*ang. OS fingerprinting*). Techniki powyższe mają swoje odmiany w postaci technik aktywnych (włamywacz kieruje odpowiedni ruch do badanego systemu) i pasywnych (włamywacz skupia się na obserwacji i analizie ruchu pochodzącego z badanego systemu). Dokładna prezentacja technik identyfikacji systemu wykracza poza ramy tego artykułu i została przeprowadzona w [7].

6. Próba przełamania zabezpieczeń systemu

Po ustaleniu wersji działającego na atakowanym hoście systemu operacyjnego oraz utworzeniu listy dostępnych usług możliwe jest zastosowanie przeciw nim dostępnego w sieci oprogramowania (*ang. exploit*), wykorzystującego znane luki w ich bezpieczeństwie. Oprogramowanie to w zależności od rodzaju luki w zabezpieczeniach umożliwia dostęp do

zasobów serwera bądź też jego zablokowanie. Dostęp do zasobów serwera nawet z poziomu zwykłego użytkownika umożliwia przegląd pewnego podzbioru systemu plików, co zwiększa zagrożenie rozszerzania uprawnień. Eliminacja działającego serwera nie stanowi strat jedynie w postaci braku dostępności pewnych usług. Dodatkowym zagrożeniem jest ułatwienie podszywania się pod unieruchomiony serwer, co może zostać wykorzystane w celu przejęcia uprawnień wynikających z zastosowanych w sieci relacji zaufania.

7. Podsumowanie

Po wykonaniu poprzednio opisanych etapów potencjalny włamywacz (osoba przeprowadzająca test penetracyjny) powinien przekonać się, że ma do czynienia z bezpiecznym systemem, w którym:

- nie ma uruchomionych zbędnych, łatwych do przełamania usług,
- nie można bez zwiększonego nakładu pracy i ryzyka pozostawienia śladu w logach uzyskać informacji na temat działającego oprogramowania,
- uruchomione usługi są aktualnymi wersjami (dla których nie istnieją ogólnodostępne programy wykorzystujące luki w bezpieczeństwie),
- próba wykrycia wszystkich działających usług zostanie odnotowana w logach systemowych.

Przeprowadzenie powyższych testów umożliwia ocenę systemu pod względem dostępności informacji umożliwiających znaczne przyspieszenie procesu łamania systemu. Prace te powinny więc być przeprowadzone z należytą dokładnością, a wyniki testów skrupulatnie przeanalizowane. Nie stanowi to oczywiście zabezpieczenia przed istniejącymi lukami (te powinny być eliminowane za pomocą udostępnianych poprawek na programy bądź instalacji nowych wersji), jednak może w znaczący sposób utrudnić włamywaczowi dostęp do systemu, a co za tym idzie wydłużyć czas potrzebny do włamania. Powinno to dać czas administratorowi na odnalezienie w logach informacji o zaistniałej nienaturalnej sytuacji.

LITERATURA

1. The Art of Port Scanning by Fyodor (http://www.insecure.org/nmap/nmap_doc.html).
2. Port Scanning without the SYN flag, Uriel Maimon (Phrack Magazine #49) 1996.
3. http://www.kyuzz.org/antirez/papers/dumbscan.html 1998.
4. Remote OS detection via TCP/IP Stack FingerPrinting by Fyodor (http://www.insecure.org/nmap/nmap-fingerprinting-article.html) 1999.

5. ICMP Usage in Scanning - The Complete Know How, Ofir Arkin Sys-Security Group, 2000-2001.
6. Passive System Fingerprinting using Network Client Applications, Jose Nazario, crimelabs research, 2001.
7. Lach J.: Identyfikacja systemu operacyjnego w teście penetracyjnym, Seminarium Sieci Komputerowe, Studia Informatica vol. 23.
8. Stawowski M.: Badanie zabezpieczeń sieci komputerowych. ArsKom, Warszawa 1999.

Recenzent: Dr inż. Krzysztof Nałęcki

Wpłynęło do Redakcji 17 kwietnia 2002 r.

Abstract

The article describes methods of collecting information on network configuration that are frequently used by attackers to get overall view of its security. Introductory steps to breaking into the system were presented. Social engineering was briefly described focusing on most common sources of information. More descriptive information was given on network mapping – the process of building map of the network with some of the methods of checking hosts availability. The presented methods are: using ping and traceroute utilities, advanced techniques using ICMP messages. Chapter 3 focuses on port mapping which is the process of getting list of available services on the running system. Both traditional methods were presented as well as the latest one. Some basic countermeasures that should be taken against those methods were given. Operating system fingerprinting was later described. This action is taken by an intruder to examine the target system and identify the kind and version of the operating system that the machine runs. Along with listing the services the system is running, the attacker narrows the list of potential vulnerabilities that can be abused. System fingerprinting can be made using both TCP and ICMP protocols. Operating system fingerprinting can be made active and passive way. Active OS fingerprinting is made by sending some packets to probed systems. Passive OS fingerprinting is done through sniffing traffic from the probed host. Methods presented in the article are widely used by the community of hackers, they should be used with the same frequency by security administrators to give them the exact view of real security level of their systems.