helion.pl
KSIĘGARNIA INTERNETOWA · WYDAWNICTWO

IDŹ DO
PRZYKŁADOWY ROZDZIAŁ
SPIS TREŚCI

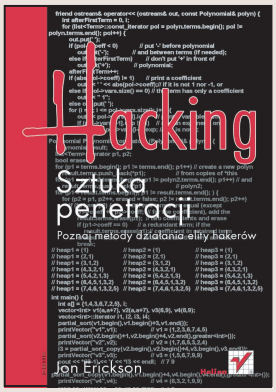
KATALOG KSIĄŻEK
KATALOG ONLINE
ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK
DODAJ DO KOSZYKA

CENNIK I INFORMACJE
ZAMÓW INFORMACJE O NOWOŚCIACH
ZAMÓW CENNIK

CZYTELNIA
FRAGMENTY KSIĄŻEK ONLINE

Hacking. Sztuka penetracji



Autor: Jon Erickson
Tłumaczenie: Bartłomiej Garbacz (rozdz. 1,2), Marcin Jędrysiak (rozdz. 3,4)
ISBN: 83-7361-418-4
Tytuł oryginału: Hacking: The Art of Exploitation
Format: B5, stron: 248

Haker kojarzy się zwykle z wrogiem publicznym, przed którym przestrzegają nas media. Najczęściej kojarzymy hakerów z włamaniami do systemów komputerowych i wielomilionowymi stratami zaatakowanych przez nich firm. Prawda jest jednak zupełnie inna. Haker to ktoś, kto potrafi w niekonwencjonalny sposób wykorzystać nieprzewidziane lub przeoczone właściwości systemów, bądź też stosuje znane wszystkim metody do rozwiązania problemów, dla których nie były one przewidziane.

Wiele osób mówi o sobie „jestem hakerem", jednak niewiele spośród nich posiada wiedzę umożliwiającą udowodnienie tego w praktyce. Tematyce hakerstwa poświęcono już wiele książek, ale żadna z nich nie wyjaśnia szczegółów technicznych metod, które stosują przedstawiciele tej grupy. Książka „Hacking. Sztuka penetracji" jest inna. Zawiera wyjaśnienie wielu zagadnień, które powinien znać każdy, kto nazywa siebie hakerem. Przedstawia zarówno teoretyczne, jak i praktyczne aspekty hackingu.

Autor książki, kryptolog i specjalista w zakresie bezpieczeństwa informacji, opisuje w niej techniki i sztuczki hakerów:

- Wykorzystywanie błędów w programach
- Tworzenie własnego kodu powłoki
- Techniki powracania do funkcji biblioteki libc
- Podsłuchiwanie i przekierowywanie ruchu w sieci
- Skanowanie portów
- Techniki łamania haseł

Wiadomości zawarte w tej książce mogą być wykorzystane przez wszystkich, którzy chcą zainteresować się hackingiem. Przyszli hakerzy dowiedzą się z niej, od czego zacząć i jak rozwinąć swoje umiejętności, a specjaliści od zabezpieczeń – na co zwrócić szczególną uwagę w swojej pracy.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Podziękowania 7

Przedmowa 8

0x100 Wprowadzenie 9

0x200 Programowanie 15

0x210 Istota programowania 16
0x220 Nadużywanie programów 19
0x230 Uogólnione techniki nadużyć 22
0x240 Uprawnienia dostępu do plików w środowiskach wieloużytkownikowych 23
0x250 Pamięć 25
0x251 Deklaracja pamięci 26
0x252 Zakończenie bajtem NULL 26
0x253 Podział na segmenty pamięci programu 27
0x260 Przepełnienia bufora 31
0x270 Przepełnienia stosowe 32
0x271 Wykorzystywanie kodu nadużycia 37
0x272 Wykorzystanie środowiska 40
0x280 Przepełnienia w przypadku segmentów heap oraz bss 49
0x281 Podstawowe przepełnienie stertowe 49
0x282 Przepełnienia wskaźników funkcyjnych 54
0x290 Ciągi formatujące 61
0x291 Ciągi formatujące i instrukcja printf() 61
0x292 Podatność ciągów formatujących na ataki 66
0x293 Odczyt spod dowolnych adresów pamięci 68
0x294 Zapis pod dowolnymi adresami pamięci 69
0x295 Bezpośredni dostęp do parametrów 76
0x296 Obejścia z użyciem sekcji dtors 79
0x297 Nadpisywanie globalnej tabeli przesunięć 85

0x2a0 Pisanie kodu powłoki ... 88
0x2a1 Podstawowe instrukcje asemblera ... 89
0x2a2 Wywołania systemowe Linuksa ... 90
0x2a3 Hello, world! ... 91
0x2a4 Kod wywołania powłoki ... 94
0x2a5 Unikanie wykorzystywania innych segmentów ... 96
0x2a6 Usuwanie bajtów zerowych ... 98
0x2a7 Dalsze zmniejszenie objętości kodu powłoki poprzez wykorzystanie stosu ... 102
0x2a8 Instrukcje w postaci drukowalnych znaków ASCII ... 106
0x2a9 Polimorficzny kod powłoki ... 107
0x2aa Polimorficzny kod powłoki z drukowalnymi znakami ASCII ... 107
0x2ab Dissembler ... 121
0x2b0 Powracanie do funkcji biblioteki libc ... 131
0x2b1 Powrót do funkcji system() ... 132
0x2b2 Wiązanie wywołań powrotnych do biblioteki libc ... 134
0x2b3 Użycie programu opakowującego ... 135
0x2b4 Zapisywanie bajtów zerowych z powróceniem do biblioteki libc ... 137
0x2b5 Zapis wielu słów w ramach pojedynczego wywołania ... 139

0x300 Sieci ... 143

0x310 Czym są sieci? ... 143
0x311 Model OSI ... 144
0x320 Szczegółowe przedstawienie niektórych warstw OSI ... 145
0x321 Warstwa sieci ... 146
0x322 Warstwa transportowa ... 147
0x323 Warstwa łącza danych ... 149
0x330 Podsłuchiwanie w sieci ... 150
0x331 Aktywne podsłuchiwanie ... 153
0x340 Przejęcie TCP/IP ... 159
0x341 Rozłączanie przy pomocy RST ... 160
0x350 Odmowa usługi ... 163
0x351 Atak Ping of Death ... 164
0x352 Atak Teardrop ... 164
0x353 Zalew pakietów ping (Ping Flooding) ... 164
0x354 Atak ze wzmocnieniem (Amplification) ... 164
0x355 Rozproszony atak DoS ... 165
0x356 Zalew pakietów SYN (SYN Flooding) ... 165
0x360 Skanowanie portów ... 166
0x361 Ukryte skanowanie SYN ... 166
0x362 Skanowanie FIN, X-mas i Null ... 167
0x363 Skanowanie z ukrycia ... 167
0x364 Skanowanie z użyciem bezczynnego komputera ... 167
0x365 Aktywne zabezpieczenie (Shroud) ... 169

0x400 Kryptologia ... 177

0x410 Teoria informacji ... 178
0x411 Bezwarunkowe bezpieczeństwo ... 178
0x412 Szyfr z kluczem jednorazowym ... 178
0x413 Kwantowa dystrybucja kluczy ... 179
0x414 Bezpieczeństwo obliczeniowe ... 180

0x420 Rozległość algorytmów ... 180
0x421 Notacja asymptotyczna ... 182
0x430 Szyfrowanie symetryczne ... 182
0x431 Kwantowy algorytm przeszukiwania ... 183
0x440 Szyfrowanie asymetryczne ... 184
0x441 RSA ... 184
0x442 Kwantowy algorytm rozkładu na czynniki ... 189
0x450 Szyfry hybrydowe ... 190
0x451 Ataki z ukrytym pośrednikiem ... 191
0x452 „Odciski palców" komputerów w protokole SSH ... 193
0x453 Rozmyte „odciski palców" ... 196
0x460 Łamanie haseł ... 201
0x461 Ataki słownikowe ... 202
0x462 Ataki na zasadzie pełnego przeglądu ... 203
0x463 Tablica wyszukiwania skrótów ... 205
0x464 Macierz prawdopodobieństwa haseł ... 205
0x470 Szyfrowanie w sieci bezprzewodowej 802.11b ... 215
0x471 Protokół Wired Equivalent Privacy (WEP) ... 215
0x472 Szyfr strumieniowy RC4 ... 217
0x480 Ataki na WEP ... 218
0x481 Ataki na zasadzie pełnego przeglądu w trybie offline ... 218
0x482 Ponowne użycie strumienia klucza ... 218
0x483 Tablice słownikowe z wektorami IV ... 220
0x484 Przekierowanie IP ... 220
0x485 Atak Fluhrera, Mantina i Shamira (FMS) ... 222

0x500 Podsumowanie ... 231

Bibliografia i dodatkowe informacje ... 232

Skorowidz ... 235

0x300

Sieci

Włamania do sieci są oparte na tych samych zasadach, co sztuczki programistyczne. Po pierwsze, należy zrozumieć reguły systemu, a następnie odkryć metodę, dzięki której będzie możliwe wykorzystanie tych reguł do osiągnięcia pożądanego wyniku.

0x350 Odmowa usługi

Inną formą ataków sieciowych są *ataki odmowy usługi* (ang. *Denial of Service*, DoS). Rozłączanie przy pomocy RST to w gruncie rzeczy forma ataku DoS. W przypadku ataku tego typu włamywacz nie próbuje ukraść żadnych informacji, ale chce zablokować dostęp do określonej usługi lub zasobu. Ataki DoS można podzielić na dwa podstawowe rodzaje — ataki powodujące zawieszanie się usług oraz ataki przepełnienia.

Ataki odmowy usługi, których celem jest jej zawieszenie, przypominają bardziej próby włamania do programów niż typowe ataki sieciowe. Nieprawidłowo przeprowadzony atak przepełnienia bufora zwykle powoduje zawieszenie całego programu docelowego zamiast przekierowania pracy systemu do własnego fragmentu kodu. Jeżeli taki program znajduje się na serwerze, żaden inny użytkownik nie będzie mógł uzyskać dostępu do tej usługi. Ataki DoS powodujące zawieszanie się usług zwykle są ściśle powiązane z konkretnymi programami, a nawet określonymi wersjami oprogramowania. Istnieje jednak kilka wyjątków od tej reguły; niektóre ataki DoS mogą zostać przeprowadzane przeciwko aplikacjom wielu producentów ze względu na podobne błędy lub strukturę kodu. Choć w większości nowoczesnych systemów operacyjnych istnieją wymagane zabezpieczenia przeciwko takim atakom, warto przyjrzeć się poszczególnym technikom włamania i metodom ich zastosowania w różnych sytuacjach.

0x351 Atak Ping of Death

Zgodnie ze specyfikacją protokołu ICMP komunikaty echa ICMP mogą zawierać maksymalnie 2^{16}, czyli 65 536 bajtów w obszarze danych pakietu. Mnóstwo osób zapomina o tym fakcie, ponieważ najważniejsze informacje znajdują się zwykle w nagłówkach takiego pakietu. Wiele systemów operacyjnych może się jednak zawiesić po odebraniu komunikatów echa ICMP, których wielkość przekracza dozwolony limit. Proces wysyłania komunikatów echa o bardzo dużej wielkości został nazwany *atakiem Ping of Death*. Jest to bardzo prosta technika ataku, ponieważ większość twórców oprogramowania nigdy nie zwracała uwagi na tę kwestię. Obecnie większość systemów operacyjnych została jednak zabezpieczona przeciwko atakom tego typu.

0x352 Atak Teardrop

Inny popularny typ ataku DoS, który powoduje zawieszenie się usługi, zyskał nazwę *ataku Teardrop*. Wykorzystuje on luki w implementacji procedur łączenia defragmentowanych pakietów, jakie są wykorzystywane przez wielu dostawców oprogramowania. W normalnej sytuacji informacje o przesunięciu fragmentów pakietu, zapisywane w przesyłanych nagłówkach, nie mogą się nakładać, co umożliwia odtworzenie pakietu. Podczas ataku Teardrop wysyłane są fragmenty pakietów z nakładającymi się przesunięciami, co powoduje zawieszanie się programów, które nie sprawdzają odbieranych pakietów pod tym względem.

0x353 Zalew pakietów ping (Ping Flooding)

Ataki przepełnienia DoS zwykle nie powodują zawieszenia się usługi lub zasobu, ale powodują ich nadmierne obciążenie, co z kolei uniemożliwia obsługę żądań użytkowników. Ataki przepełnienia są ściśle związane z zasobami sieciowymi, aczkolwiek istnieją podobne techniki ataków skierowanych przeciwko cyklom procesora i procesom systemowym.

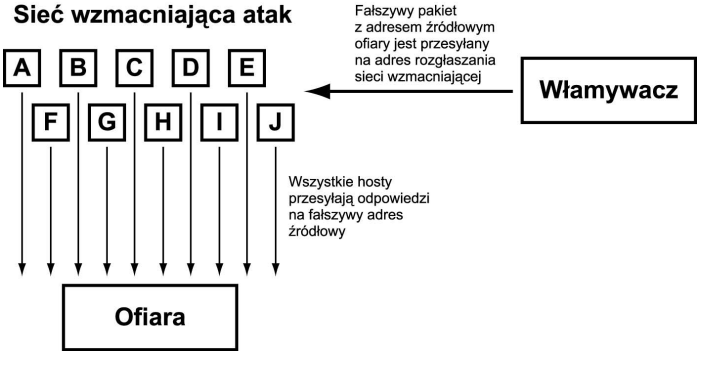
Najprostszym typem tego ataku jest *zalew pakietami ping*. Powoduje to wykorzystanie całego łącza sieciowego ofiary, przez co normalny ruch zostaje zablokowany. Haker wysyła do komputera ofiary ogromną liczbę pakietów ping o bardzo dużej wielkości, co może doprowadzić do pełnego wykorzystania dostępnej przepustowości łącza.

Atak zalewu pakietami ping nie wymaga zastosowania żadnych sprytnych sztuczek, gdyż w gruncie rzeczy jego powodzenie zależy od przepustowości łącza ofiary i napastnika. Jeżeli haker ma lepsze łącze niż ofiara, może wysyłać ogromną ilość danych, których odbiór nie będzie możliwy. Spowoduje to jednocześnie zablokowanie normalnego ruchu, jaki jest skierowany do sieci ofiary.

0x354 Atak ze wzmocnieniem (Amplification)

Należy zwrócić uwagę, że dostępne są również metody przeprowadzania ataku zalewu pakietami `ping` nawet w przypadku, gdy haker dysponuje łączem o niewielkiej przepustowości. Podczas *ataku ze wzmocnieniem* techniki fałszowania i adresy rozgłaszania

wykorzystywane są w celu wielokrotnego powiększenia pojedynczego strumienia pakietów. Aby możliwe było przeprowadzenie takiego ataku, należy najpierw znaleźć właściwy system docelowy. Zwykle jest to sieć z dużą liczbą aktywnych komputerów, pozwalająca na komunikowanie się z adresem rozgłaszania. Włamywacz wysyła duże pakiety żądania echa ICMP na adres rozgłaszania takiej sieci. Jako adres źródłowy tych pakietów podawany jest adres systemu ofiary. Pakiety zostaną rozgłoszone do wszystkich systemów w sieci wzmacniającej, co spowoduje przesłanie pakietów odpowiedzi echa ICMP na fałszywy adres źródłowy, czyli do komputera ofiary. Sposób przeprowadzenia tego ataku przedstawiono na rysunku 3.8.



Rysunek 3.8. *Atak ze wzmocnieniem*

Dzięki technice wzmacniania ruchu haker może wysłać relatywnie niewielki strumień pakietów żądania echa ICMP, natomiast ofiara zostanie zalana ogromną ilością pakietów odpowiedzi echa ICMP. Atak tego typu można przeprowadzić z użyciem pakietów ICMP (technika o nazwie *smurf*), jak również pakietów echa UDP (technika znana jako *fraggle*).

0x355 Rozproszony atak DoS

Rozproszony atak DoS (DDoS) stanowi szczególną odmianę klasycznego ataku przepełnienia. Jak już wcześniej wspomniano, atak przepełnienia jest przeprowadzany w celu całkowitego zablokowania łącza sieciowego ofiary. W przypadku ataku DDoS haker musi najpierw włamać się do wielu różnych systemów i zainstalować w nich własne demony, które będą czekały w ukryciu na sygnał do ataku. Włamywacz wykorzystuje specjalny program sterujący; po jego uruchomieniu wszystkie demony jednocześnie uderzają w ofiarę, wykonując określony typ ataku DoS. Taka technika ataku może spowodować poważne szkody, utrudniając jednocześnie próby wykrycia rzeczywistego położenia hakera.

0x356 Zalew pakietów SYN (SYN Flooding)

Ataki zalewania pakietami SYN nie powodują zablokowania łącza sieciowego, ale są skierowane przeciwko stosowi TCP/IP. Protokół TCP jest odpowiedzialny za obsługę połączeń, co oznacza konieczność śledzenia ich stanu. Za to zadanie odpowiedzialny

jest stos TCP/IP, który może jednak śledzić tylko określoną liczbę połączeń. Atak przepełnienia typu SYN Flooding wykorzystuje to ograniczenie, uniemożliwiając nawiązywanie nowych połączeń sieciowych.

Haker wysyła do systemu ofiary dużą liczbę pakietów SYN z fałszywym, nieistniejącym adresem źródłowym. Ponieważ pakiet SYN jest używany do inicjowania połączeń TCP, komputer ofiary będzie wysyłał w odpowiedzi pakiet SYN/ACK, oczekując z kolei na odpowiedź ACK. Każde takie częściowo otwarte połączenie jest umieszczane w kolejce, która ma jednak ograniczoną pojemność. Ponieważ fałszywe adresy źródłowe nie istnieją, system nigdy nie odbierze odpowiedzi ACK, które spowodowałyby usunięcie niepotrzebnych wpisów z kolejki i nawiązanie pełnego połączenia. W tym przypadku musi upłynąć czas ważności poszczególnych połączeń, co zwykle trwa dość długo.

Jeżeli haker kontynuuje zalewanie systemu ofiary fałszywymi pakietami SYN, kolejka połączeń pozostanie zapełniona, przez co prawdziwe pakiety SYN nie będą mogły przedostać się do tego systemu. Oznacza to brak możliwości tworzenia nowych połączeń TCP/IP.