101 zabezpieczeń przed atakami w sieci komputerowej

Autorzy: Maciej Szmit, Marek Gusta, Mariusz Tomaszewski
ISBN: 83-7361-517-2
Format: B5, stron: 560

Chyba każda sieć komputerowa na świecie była już atakowana przez hakerów. Niektóre z ataków były skuteczne, inne nie. Efekty skutecznego ataku hakerów mogą być różne – od braku szkód, aż po utratę ważnych danych lub, co często okazuje się znacznie gorsze – wydostanie się takich danych na zewnątrz. Co sprawia, że niektóre sieci opierają się atakom hakerów, a inne nie? Sekret tkwi w zabezpieczeniach i pracy administratora.

W książce „101 zabezpieczeń przed atakami w sieci komputerowej" każdy, kto chce zabezpieczyć swoją sieć przed niepowołanym dostępem, znajdzie niezbędną do tego wiedzę. Książka przedstawia różne rodzaje ataków, sposoby ich wykrywania i metody ochrony sieci przed nimi. Opisuje ataki na różne warstwy i elementy sieci oraz zasady korzystania z zapór sieciowych.

- Wykrywanie sniffingu i ochrona przed nim
- Skanowanie portów i IP-spoofing
- Ataki typu DoS
- Wirusy, robaki i programy szpiegujące
- Zabezpieczanie procesu logowania
- Ochrona przed atakiem przez przepełnienie bufora
- Technologie i architektury zapór sieciowych
- Systemy wykrywania ataków typu IDS

Jeśli chcesz, aby administrowana przez Ciebie sieć była bezpieczna, skorzystaj ze sposobów przedstawionych w tej książce.

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

Spis treści

Rozdział 3.

Metody obrony przed atakami DoS i DDoS

Jednym z najbardziej niebezpiecznych, a zarazem popularnych, zagrożeń w sieciach komputerowych są ataki DoS (ang. *Denial of Service*, odmowa usług) w tym ich odmiana — ataki DDoS (ang. *Distributed Denial of Service*, rozproszone ataki „odmowa usługi"). Ich celem jest unieruchomienie atakowanego serwisu (na przykład serwera WWW, DNS czy całej atakowanej sieci) za pomocą różnych mechanizmów wykorzystujących zarówno luki konkretnych systemów operacyjnych, jak i niedociągnięcia stosu TCP/IP. Ataki DoS (pominąwszy pobudki czysto chuligańskie) mogą być podejmowane jako część szerszych działań mających na celu oszustwo, spenetrowanie cudzych zasobów bądź przejęcie nad nimi kontroli (na przykład zablokowanie prawdziwego DNS-a może być pomocne podczas prowadzenia ataku DNS-spoofing).

Obrona przed atakami DoS sprowadza się przede wszystkim do zainstalowania odpowiednich łat na znane luki w systemach operacyjnych oraz do odfiltrowania na zaporze sieciowej pakietów niosących atak. Do wykrycia ataków DoS i DDoS najlepiej posłużyć się analizatorami ruchu sieciowego oraz systemami IDS. W tym rozdziale zaprezentujemy szereg najpopularniejszych ataków DoS i DDoS oraz sposoby obrony przed nimi. Jako zaporę sieciową wykorzystywaliśmy linuksowy program iptables, zaś jako systemu IDS używaliśmy Snorta (odpowiednie reguły zostały wzięte z aktualnych w chwili pisania książki baz Snorta). Opis instalacji i wykorzystania obu pakietów można znaleźć w dodatkach. Zachęcamy Czytelnika, aby na podstawie niniejszego rozdziału spróbował samodzielnie skonfigurować zaporę sieciową wraz z systemem detekcji intruzów i dynamicznej reakcji (za pomocą opisanego w dodatku C. programu Guardian).

Ataki DoS

Ataki typu DoS generują duży ruch, co powoduje zaburzanie lub całkowite zablokowanie pracy normalnych aplikacji sieciowych, lub też wykorzystują słabe punkty stosu protokołów TCP/IP dla unieruchomienia atakowanego systemu lub zaburzenia jego

działania. Niektóre z nich są możliwe do przeprowadzenia, ponieważ hosty sieciowe przy uwierzytelnianiu polegają tylko na źródłowym adresie IP. Inne istnieją, dlatego że niektóre mechanizmy kontrolne i większość protokołów routingu stosuje słabe metody uwierzytelniania źródła, z którego pochodzi informacja, bądź w ogóle ich nie używa.

Ataki DOS możemy podzielić na trzy grupy:

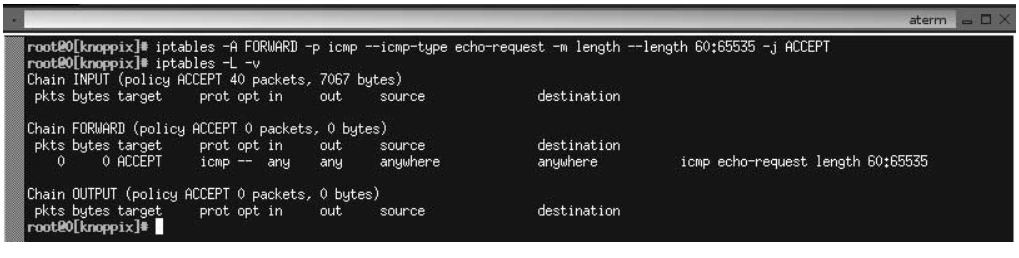
- ataki bazujące na implementacji stosu TCP/IP. Ataki tego typu wykorzystują słabości w specyfikacji TCP/IP w konkretnym systemie operacyjnym. Przykładami ataków z tej grupy jest *Ping of Death*, *Teardrop, Smbnuke*;
- ataki bazujące na standardach TCP/IP. Ataki tego typu wykorzystują słabości w samych standardach stosu TCP/IP. Przykładami ataków z tej grupy są *SYN attack* oraz *Land*;
- Ataki wykorzystujące tzw. „brutalną siłę" (ang. *brute force*). Ataki tego typu generują duży ruch, który zajmuje pasmo sieciowe. Przykładami ataków tego typu są *Smurf*, *Fraggle*.

Ping of Death

Ping of Death jest dość prostym atakiem. Standardy opisujące stos TCP/IP określają maksymalną wielkość datagramu IP na 65536 bajtów. Wiele systemów, szczególnie starsze wersje systemów uniksowych i linuksowych, może ulec uszkodzeniu, zawiesić się albo zrestartować, jeśli otrzyma datagram IP większy od możliwego maksymalnego rozmiaru. Podczas tego ataku tworzony jest i wysyłany do systemu ofiary pakiet ping przekraczający 65536 bajtów.

Zabezpieczenie nr 39. Ochrona przed atakiem Ping of Death za pomocą filtrowania na zaporze sieciowej

Jeżeli w sieci istnieją starsze wersje systemów operacyjnych, podatnych na atak Ping of Death, powinniśmy zadbać o ściągnięcie odpowiednich aktualizacji. Jeżeli z jakichś względów system taki nie może być uaktualniony do nowszej wersji, najlepszą metodą obrony jest zabezpieczenie dostępu do takiej stacji za pomocą reguły zapory sieciowej. Reguła ta może być zastosowana na routerze, przez który można uzyskać dostęp z zewnątrz do tej stacji. Regułę tej składni pokazano na rysunku 3.1.



Rysunek 3.1. *Reguła zapory sieciowej dopuszczająca pakiety ICMP Echo request o wielkości od 60 do 65535 bajtów*

Powyższa reguła przepuszcza tylko pakiety ICMP Echo Request, których rozmiary mieszczą się w zakresie od 60 bajtów do 65535 bajtów.

Teardrop

Atak *teardrop* wykorzystuje słabość w procesie składania po stronie odbiorcy datagramów IP z poszczególnych fragmentów. Podczas transmisji w sieci publicznej datagram IP przechodzi przez różne routery i sieci, w szczególności takie, w których maksymalny rozmiar ramki może być mniejszy niż rozmiar datagramu. W takim przypadku datagram może zostać podzielony na mniejsze fragmenty. Każdy fragment zawiera pole *offset field*, w którym wpisana jest informacja pozwalająca na prawidłową defragmentację pakietu. Urządzenie odbierające fragmenty składa je w oryginalny datagram IP używając do tego wartości w polu *offset field*. Podczas przeprowadzania ataku *teardrop* są wysyłane serie datagramów IP z nachodzącymi na siebie wartościami w polach *offset field*. Kiedy system odbiorcy stara się poskładać fragment w całość, zawiesza się bądź ulega uszkodzeniu.

Na rysunku 3.2 przedstawiono sposób przeprowadzenia tego ataku. W naszym przypadku pakiety były wysyłane na port 69 komputera o adresie 172.16.30.1.

Rysunek 3.2. *Przykład przeprowadzenia ataku Teardrop*

```
root@0[dos]# ./teardrop
teardrop   route|daemon9

./teardrop src_ip dst_ip [ -s src_prt ] [ -t dst_prt ] [ -n how_many ]
root@0[dos]# ./teardrop 172.16.30.13 172.16.30.1 -s 1024 -t 69 -n 113
teardrop   route|daemon9

Death on flaxen wings:
From:    172.16.30.13, 1024
  To:     172.16.30.1,   69
 Amt:   113
[ b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00
m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00
m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00
m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00
m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00m b00
m b00m b00m b00m b00m ]
root@0[dos]#
```

Na rysunku 3.3 pokazano przechwycone za pomocą sniffera pakiety generowane podczas tego ataku. Jak widać, są one pofragmentowane.

```
root@1[root]# tcpdump -vvv -i eth0 port 69
tcpdump: listening on eth0
22:18:30.388015 172.16.30.13.1024 > 172.16.30.1.tftp: [no cksum]  28 tftp-#0 (frag 242:3600+) (ttl 64, len 56)
22:18:30.411877 172.16.30.13.1024 > 172.16.30.1.tftp: [no cksum]  28 tftp-#0 (frag 242:3600+) (ttl 64, len 56)
22:18:30.431850 172.16.30.13.1024 > 172.16.30.1.tftp: [no cksum]  28 tftp-#0 (frag 242:3600+) (ttl 64, len 56)
22:18:30.447815 172.16.30.13.1024 > 172.16.30.1.tftp: [no cksum]  28 tftp-#0 (frag 242:3600+) (ttl 64, len 56)
22:18:30.472571 172.16.30.13.1024 > 172.16.30.1.tftp: [no cksum]  28 tftp-#0 (frag 242:3600+) (ttl 64, len 56)
22:18:30.492399 172.16.30.13.1024 > 172.16.30.1.tftp: [no cksum]  28 tftp-#0 (frag 242:3600+) (ttl 64, len 56)
22:18:30.512418 172.16.30.13.1024 > 172.16.30.1.tftp: [no cksum]  28 tftp-#0 (frag 242:3600+) (ttl 64, len 56)
22:18:30.532452 172.16.30.13.1024 > 172.16.30.1.tftp: [no cksum]  28 tftp-#0 (frag 242:3600+) (ttl 64, len 56)
22:18:30.552348 172.16.30.13.1024 > 172.16.30.1.tftp: [no cksum]  28 tftp-#0 (frag 242:3600+) (ttl 64, len 56)
22:18:30.572405 172.16.30.13.1024 > 172.16.30.1.tftp: [no cksum]  28 tftp-#0 (frag 242:3600+) (ttl 64, len 56)
```

Rysunek 3.3. *Pofragmentowane pakiety generowane podczas ataku Teardrop*

Zabezpieczenie nr 40. Ochrona przed atakiem teardrop za pomocą systemu Snort

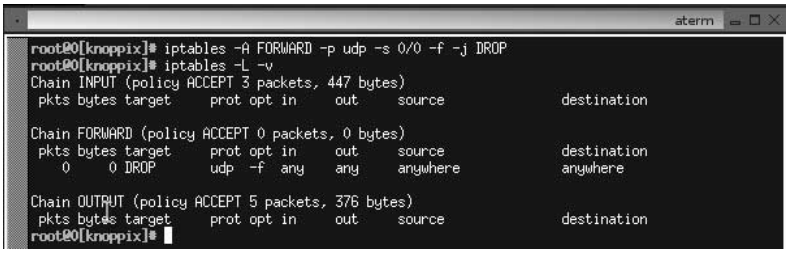
Najlepszą ochroną przeciwko temu atakowi jest sprawdzenie, czy dla naszego systemu operacyjnego istnieją aktualizacje przeciwdziałające atakowi i czy są one zainstalowane. Oczywiście można zastosować do ochrony odpowiednią regułę systemu IDS. Poniżej przedstawiono regułę wykrywającą pofragmentowane pakiety pochodzące z ataku teardrop:

```
alert udp any any -> any any (msg:"Przeprowadzono atak Teardrop"; fragbits:M;
id:242; sid:270; rev:6;)
```

Wykrycie ataku przez Snorta, a następnie dynamiczna reakcja za pomocą zapory sieciowej pozwoli na zabezpieczenie się przed tego typu pakietami. Poszczególne opcje w regule przytoczonej wcześniej oznaczają, że alarm ma być ogłoszony w przypadku wykrycia pofragmentowanego (*fragbits:M;*) ruchu UDP z dowolnego adresu na dowolny adres (*alert udp any any -> any any*). Pola *Id* oraz *Sid* wskazują indeks reguły w bazie danych Snorta (ta reguła, jak i kolejne przedstawione poniżej, zostały zaczerpnięte z najnowszej w chwili pisania książki bazy programu Snort).

Zabezpieczenie nr 41. Ochrona przed atakiem teardrop za pomocą filtrowania pakietów

Drugą metodą ochrony przed atakiem Teardrop jest odpowiednia filtracja pakietów. W celu zabezpieczenia się przed tym atakiem należy odrzucić wszystkie przychodzące do naszej sieci lub komputera pofragmentowane datagramy UDP. Odpowiednią regułę zapory sieciowej zabezpieczającą przechodzenie przez bramę do internetu pofragmentowanych datagramów UDP zaprezentowano na rysunku 3.4.



Rysunek 3.4. *Reguła zapory sieciowej zabezpieczająca przed atakiem teardrop*

Atak SYN-flood

Atak *SYN-flood* wykorzystuje moment nawiązania połączenia TCP między dwoma hostami. Kiedy klient w sieci z implementowanym stosem TCP/IP chce nawiązać połączenie z serwerem, następuje tzw. *three-way-handshake*. Składa się on z trzech faz:

1. Klient wysyła segment tcp z flagą SYN do serwera.

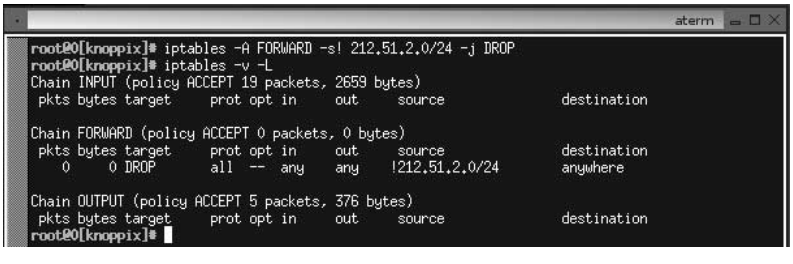
2. Serwer potwierdza odebranie segmentu SYN od klienta przez wysłanie segmentu z ustawionymi flagami SYN i ACK.
3. Klient odpowiada serwerowi segmentem z ustawioną flagą ACK.

Wykonanie tych trzech kroków powoduje ustanowienie połączenia i od tej chwili dane mogą być już wymieniane między nadawcą i odbiorcą. Każde wysłanie segmentu z flagą SYN na otwarty port u odbiorcy wymusza na nim odpowiedź przez odesłanie SYN i ACK i oczekiwanie na potwierdzenie od nadawcy flagą ACK. SYN-flood polega na zalewaniu systemu odbiorczego segmentami TCP z ustawiona flagą SYN spod fałszywych adresów IP. W tym przypadku ostateczna odpowiedź (ACK od klienta) nigdy nie nadejdzie, ponieważ odbiorca wysyła segment z flagami SYN i ACK pod fałszywy adres IP. Podczas gdy system odbiorcy czeka na potwierdzenie ACK, które nigdy nie przyjdzie, zapisuje wszystkie segmenty SYN i ACK, na które nie odpowiedział w swojej kolejce, zwykle dość małej. Po zapełnieniu tej kolejki system odbiorcy będzie ignorował wszystkie nowe próby nawiązania połączenia SYN. Segmenty z flagami SYN-ACK opuszczają kolejkę w momencie, gdy zostanie odebrane potwierdzenie ACK od nadawcy albo upłynie czas oczekiwania na to potwierdzenie — *timeout*. Przez ten czas system nie pozwoli na nawiązywanie nowych połączeń.

Zabezpieczenie nr 42. Ochrona przed atakiem SYN-flood wychodzącym z naszej sieci za pomocą zapory sieciowej

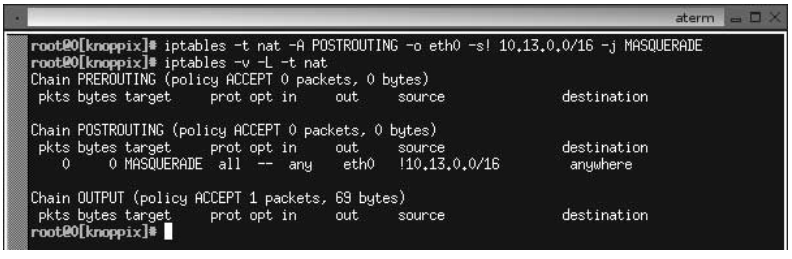
W celu przeciwdziałania tego typu atakom należy tak skonfigurować zaporę sieciową, aby pakiety opuszczające ją i wychodzące z naszej wewnętrznej sieci zawierały adres IP źródłowy pochodzący tylko z naszej wewnętrznej sieci. To spowoduje, że adresy IP nie będą mogły być *fałszowane* (podmieniane). Aby zabezpieczyć się przed wychodzeniem tego typu pakietów z wnętrza naszej sieci, przy założeniu, że w naszej sieci są adresy publiczne z sieci 212.51.2.0/24, należy zastosować na routerze regułę zapory sieciowej przedstawioną na rysunku 3.5.

Rysunek 3.5. *Reguła blokująca wychodzenie z naszej sieci pakietów ze zmienionymi adresami źródłowymi*



Znak (*!*) oznacza negację. W tym przypadku będą przepuszczane tylko pakiety z adresami źródłowymi pochodzącymi z sieci 212.51.2.0/24, pozostałe będą odrzucane.

W przypadku sieci lokalnej z prywatną pulą adresów np. 10.13.0.0/16, która jest ukryta za NAT-em, aby uchronić się przed atakiem SYN z wnętrza naszej sieci, należy dokonywać translacji tylko dla adresów z naszej sieci lokalnej. Sposób dokonywania translacji adresu źródłowego tylko dla adresów z naszej sieci przedstawiono na rysunku 3.6.



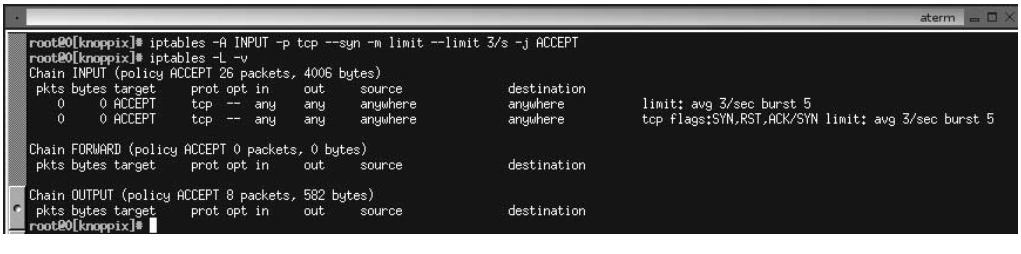
Rysunek 3.6. *Translacja adresów tylko z prywatnej puli*

W celu ograniczenia użytkownikom w sieci możliwość nawiązywania dużej liczby połączeń (segmentów tcp z ustawioną flagą SYN) możemy użyć reguły, która spowoduje, że każdy użytkownik o danym adresie IP będzie mógł nawiązać z wnętrza naszej sieci tylko 9 połączeń w ciągu 1s.

```
iptables -A INPUT -p tcp --syn -m iplimit --iplimit-above 9 -j DROP
```

Zabezpieczenie nr 43. Ochrona przed atakami SYN- flood i Naptha na usługi w naszej sieci za pomocą iptables

Jeżeli chcemy ochronić nasze serwisy dostępne z internetu przed atakami SYN-flood oraz Naptha, powinniśmy zastosować reguły filtrujące ograniczające liczbę możliwych połączeń w ciągu sekundy z naszymi serwerami. Na rysunku 3.7 pokazano regułę pozwalającą na wykonanie 3 połączeń w ciągu sekundy.



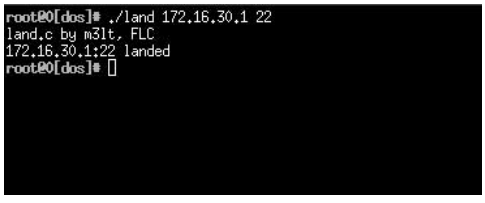
Rysunek 3.7. *Ograniczenie liczby połączeń z usługami do 3 na sekundę*

Atak Land

Atak *Land* jest podobny do ataku SYN. Tak jak w przypadku ataku SYN, wysyłane są do systemu odbiorcy segmenty z ustawioną flagą synchronizacji, jednak, podczas gdy w ataku SYN adres IP nadawcy jest nieosiągalny lub jego komputer jest wyłączony, atak Land podmienia adres źródłowy na taki sam, jak adres odbiorcy. Serwer odbierając tak spreparowany pakiet wysyła potwierdzenie (pakiet z bitem ACK) na własny adres i nawiązuje nieaktywne połączenie — zapętla swoje działanie. Likwidacja nieaktywnego połączenia następuje dopiero po upływie czasu ustalonego w systemie operacyjnym serwera dla nieaktywnych połączeń.

Na rysunku 3.8 zaprezentowano sposób przeprowadzenia tego ataku.

Rysunek 3.8. *Przeprowadzenie ataku Land*



W wyniku przeprowadzenia ataku został wysłany charakterystyczny pakiet. Jak widać, adres źródłowy i adres docelowy wskazują na ten sam komputer (rysunek 3.9).

Rysunek 3.9. *Pakiet generowany podczas ataku Land*

Zabezpieczenie nr 44. Ochrona przed atakiem Land za pomocą programu Snort

Chociaż atak tego typu nie jest stary, większość systemów operacyjnych jest wyposażona w łaty zabezpieczające przed nim. Jak w przypadku wszystkich ataków DoS, należy pamiętać o instalowaniu zawsze odpowiednich łat bądź o sprawdzeniu, czy system nie jest już wyposażony w odpowiednie zabezpieczenie. Inną metodą obrony przed atakiem Land jest ustawienie odpowiednich filtrów na zaporze sieciowej. Mają one za zadanie odrzucenie wszystkich przychodzących datagramów IP z błędnymi adresami IP, czyli przychodzących z zewnątrz do naszej zapory sieciowej datagramów, których adres źródłowy wskazuje, że pochodzą z naszej wewnętrznej sieci lokalnej. Zabezpieczeniem będzie więc odpowiednia filtracja pakietów. Wśród znanych źródłowych adresów IP powinniśmy odfiltrowywać następujące:

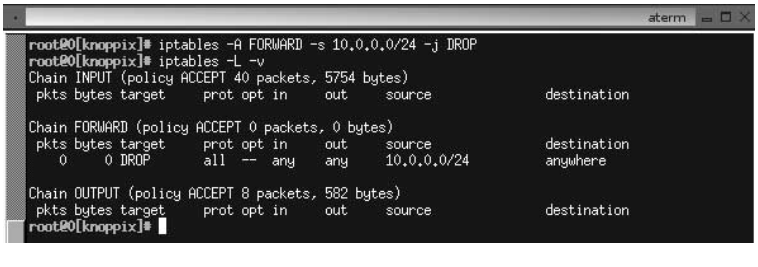
- 10.0.0.0 to 10.255.255.255,
- 172.16.0.0 to 172.31.255.255,
- 192.168.0.0 to 192.168.255.255,

czyli adresy należące do sieci prywatnych oraz

- 127.0.0.0 to 127.255.255.255 (adresy pętli zwrotnej).

Przykładową regułę odrzucającą przychodzące z zewnątrz do naszej sieci pakiety z prywatnymi adresami z klasy 10.0.0.0/8 przedstawiono na rysunku 3.10.

Rysunek 3.10. *Reguła zapory sieciowej, która nie wpuszcza do wnętrza naszej sieci pakietów z adresami IP z prywatnej sieci 10.0.0.0/8*



Zabezpieczenie nr 45. Ochrona przed atakiem Land za pomocą programu Snort (reguła systemu IDS)

Aby chronić się przed atakiem Land, możemy też wykorzystać regułę systemu IDS. Regułę tę pokazano poniżej:

```
alert tcp any any -> any any (msg:"Przeprowadzono atak Land"; flags:S; id:3868;
seq:3868; flow:stateless; sid:269; rev:9;)
```

Atak Naptha

Atak ten działa podobnie do ataku SYN-flood. Również wykorzystuje moment nawiązywania połączenia TCP między klientem i serwerem i, analogicznie do ataku SYN-flood, jego zadaniem jest zajęcie całej kolejki połączeń serwera i uniemożliwienie korzystania z danej usługi. Różnica w stosunku do zalewania segmentami SYN polega na tym, że atakujący wysyła pakiety SYN na określony port komputera ofiary i oczekuje na powracające pakiety SYN/ACK (w przypadku ataku SYN-flood atakujący wysyła tylko pakiety SYN i nic więcej nie robi). Jeśli atakujący zauważy pakiety powrotne SYN/ACK, wysyła do ofiary segment z ustawionymi flagami FIN/ACK. Powoduje to przestawienie serwera w stan tzw. pasywnego zamknięcia. Wynika on stąd, że serwer po odebraniu segmentu FIN/ACK odsyła pakiet FIN i czeka na pakiet ACK, którego nigdy nie otrzymuje. Serwer przechodzi w stan LAST_ACK i oczekuje na przyjście ostatniego segmentu ACK. W systemie Windows 98 stan ten utrzymywany jest przez około dwie minuty. W tym czasie serwer odrzuca wszelkie próby nawiązania z nim połączenia sieciowego (dopóty będzie ignorował wszystkie pakiety SYN, dopóki nie zwolni się miejsce w kolejce). Zalewając w ten sposób ofiarę sfałszowanymi segmentami SYN atakujący skutecznie blokuje możliwość korzystania z danej usługi.

Ograniczeniem tego ataku jest fakt, że napastnik musi — generując fałszywe pakiety SYN — podszywać się w nich pod adresy IP z własnej sieci. Jest to wymóg konieczny, aby powracające od zaatakowanej maszyny pakiety SYN/ACK mogły być zauważone przez napastnika i tym samym, by mógł on wysyłać poprawnie zbudowane pakiety FIN/ACK. Napastnik musi w pakiecie SYN/ACK odczytać numer sekwencyjny i na jego podstawie zbudować poprawny dla ofiary pakiet FIN/ACK. Wysyłanie pakietów FIN/ACK z ustawionym niepoprawnym numerem sekwencyjnym zakończy się niepowodzeniem, ponieważ port ofiary stwierdzi, że pakiety takie nie należą do danego połączenia.

Na poniższym listingu pokazano sposób przeprowadzania ataku:

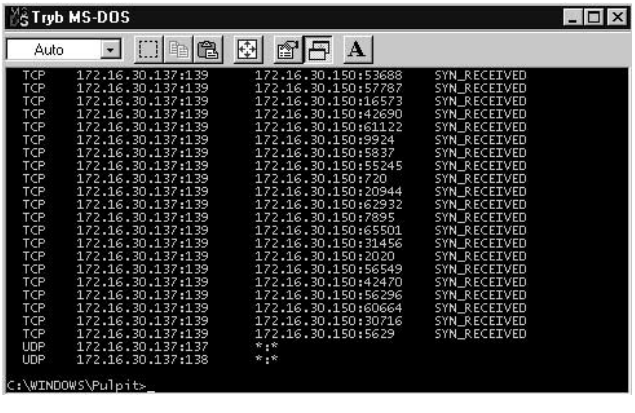
```
napastnik -> ofiara: SYN
ofiara -> napastnik: SYN/ACK
napastnik -> ofiara: ACK/FIN
```

Systemy podatne na ten atak to:

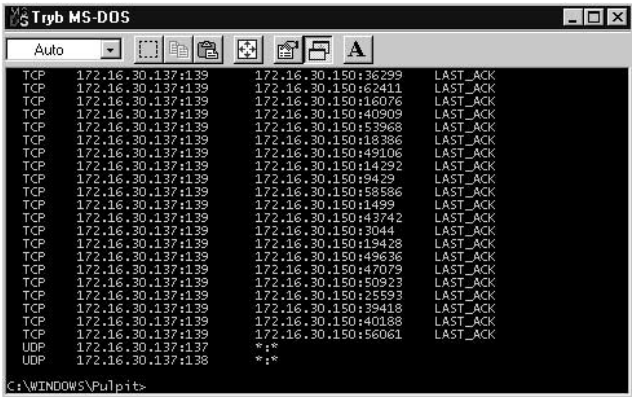
- Microsoft Windows 95,
- Microsoft Windows 98,

- Microsoft Windows 98SE,
- Microsoft Windows Millennium,
- Windows NT 4.0,
- HP-UX 11,
- IBM AIX 4.3,
- Sun Solaris 7-8,
- FreeBSD 4.0 wersja RELEASE,
- RedHat Linux 6.1 — 7.0,
- Systemy Linux oparte na jądrze z serii 2.0.

Na rysunku 3.11 przedstawiono stany połączeń na porcie 139. serwera po wykonaniu ataku SYN-flood w systemie Windows 98. Na kolejnym (rysunek 3.12) dla porównania widać stany połączeń, ale po wykonaniu ataku Naptha. Listę takich stanów uzyskano po wydaniu polecenia `netstat -na`.

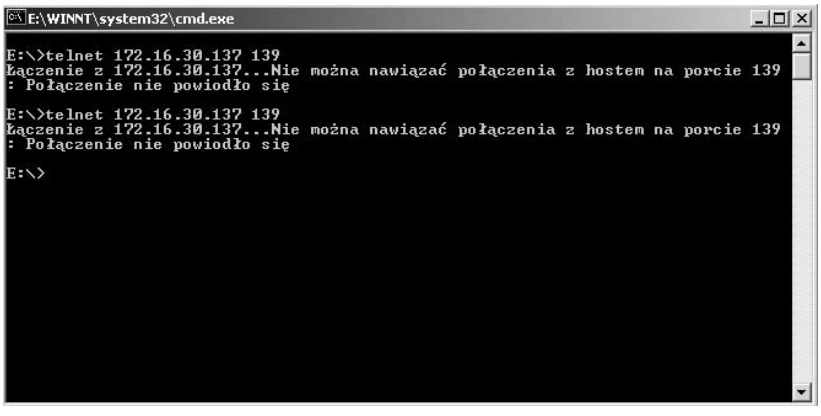


Rysunek 3.11. *Stany połączeń serwera po wykonaniu ataku SYN-flood*



Rysunek 3.12. *Stany połączeń serwera po wykonaniu ataku Naptha*

Po wykonaniu ataku Naptha próba połączenia się z usługą na porcie 139. zakończy się niepowodzeniem (rysunek 3.13).



Rysunek 3.13. *Próba ustanowienia połączenia z portem 139 ofiary po wykonaniu ataku naptha*