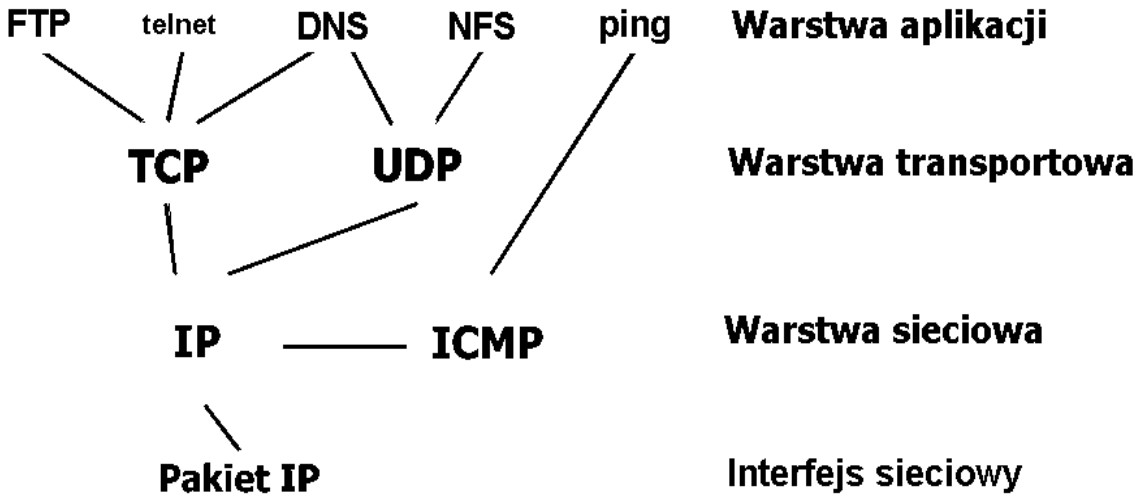
Firewall cz. II

Poprzednio poznawaliśmy zasady projektowania i wdrażania firewalli. Dziś spróbujemy powrócić do tematu filtrowania pakietów nieco „od kuchni”. Postaram się przedstawić główne zjawiska zachodzące podczas przetwarzania pakietów przez rutery i hosty, starając się zasygnalizować mogące wystąpić zagrożenia. Wszelkie informacje zawarte w poniższym tekście z założenia mają charakter informacyjno-edukacyjny, dlatego nie zamierzam podawać konkretnych „patentów” na włamywanie się za pomocą opisywanych metod do własnej lub obcej sieci czy serwera. Jest to nielegalne i przede wszystkim nieetyczne. Niemniej czasami warto przetestować zabezpieczenia własnego systemu pod kątem włamań przy użyciu zmodyfikowanych pakietów danych. Zainteresowanym polecam witrynę internetową www.astalavista.box.sk, gdzie dostępne są różnego rodzaju narzędzia do monitorowania i analizowania bezpieczeństwa sieci opartych na TCP/IP. Do najciekawszych należą m.inn. pakiet SATAN oraz program netcat. Oba działają w środowisku unixowym. Teraz zajmijmy się teoretyczną stroną potencjalnych włamań przy pomocy zmodyfikowanych pakietów IP.

Budowa pakietu

Aby móc zgłębiać problematyką związaną z analizowaniem i filtrowanie pakietów trzeba najpierw zapoznać się z ich budową oraz hierarchią warstw TCP/IP. Wygląda ona następująco :

- warstwa Aplikacji (np. telnet)
- warstwa Transportowa (UDP lub TCP)
- warstwa Internetu (IP)
- warstwa dostępu (medium) sieciowego (np. Ethernet)



Konstrukcja pakietów polega na tym, że każda kolejna warstwa używanego protokołu opakowuje pakiet. Występuje tu analogia do wkładania listu do kolejnych kopert.
Na każdym, oprócz warstwy Aplikacji, poziomie w budowie pakietu możemy wyróżnić dwie części : nagłówek i dane. W nagłówku zawarte są informacje istotne dla aktualnej warstwy, a pole danych zawiera najczęściej cały pakiet z warstwy poprzedniej. Innymi słowy każda warstwa traktuje informacje , które dostała z warstwy poprzedniej (nasz przykładowy list w kopercie), jako dane i dodaje do nich własny nagłówek (wkłada całośc do kolejnej koperty). Proces ten nazywa się **enkapsulacją.**
Powyżej opisane przetwarzanie ma miejsce podczas „przechodzenia” od warstwy aplikacji „w dół” do warstwy dostępu do sieci. W druga stronę, podczas przekazywania pakietu do warstw wyższych, ma miejsce procedura odwrotna, czyli „rozrywanie kopert”. W czasie przekazywania „w górę” każdy nagłówek jest obcinany przez odpowiednią warstwę. Np. warstwa transportowa usuwa przed przekazanie do warstwy aplikacji nagłówek warstwy internetowej itd.

Z punktu widzenia analizy pakietów najważniejsze informacje umieszczone są właśnie w nagłówkach różnych warstw. Z racji tematyki jaką się zajmujemy skupimy się na analizowaniu pakietów w warstwie Internetu czyli IP.

IP stanowi podstawę Internetu. Może mieć pod sobą wiele warstw i protokołów. Większość pakietów IP stanowią zwykłe pakiety, przeznaczone dla jednego konkretnego hosta (transmisja typu unicast). Pakiety IP

mogą być również wysyłane do grupy hostów (transmisja multicast) lub też mogą być pakietami rozgłoszeniowymi przeznaczonymi dla wszystkich hostów w danej podsieci (transmisja broadcast).
Idea rozsyłania grupowego miała na celu zwiększenie efektywności. Przypomina trochę system notatek służbowych. Zamiast wysyłać po jednym pakiecie do każdego hosta (np. z informacja „Chętni na piwo proszeni są o zgłaszanie się do kierownika administracyjnego") wysyła się jeden pakiet do grupy zainteresowanych hostów. Natomiast pakiety rozgłoszeniowe przypominają ogłoszenia w stylu „Proszę natychmiast opuścić budynek" i są skierowane do wszystkich. W praktyce używa się ich również w przypadku, gdy nadawca nie potrafi określić dokładnego miejsca przeznaczenia, ale uważa że odbiorca zorientuje się, że informacja przeznaczona jest dla niego (np. „Mały Jasio czeka na mamę w punkcie obsługi klienta")

W przeciwieństwie do notatki służbowej pakiet rozsyłania grupowego jest pojedynczym obiektem. Jeśli kilka, kilkanaście lub kilkadziesiąt hostów potrzebuje tej samej informacji, to pakiet grupowy pozwala znacznie zmniejszyć obciążenie sieci. Użycie pakietu rozgłoszeniowego dałoby podobną oszczędność, ale jednocześnie wprowadziłoby efekt uboczny w postaci marnowania czasu komputerów, których dany komunikat by nie dotyczył.

Pamiętać należy, że zarówno adresy rozgłoszeniowe jak i rozsyłania grupowego powinny być tylko i wyłącznie adresami docelowymi. Jedynym odstępstwem od tej reguły jest przypadek, gdy host korzystający z dynamicznego przydzielania adresu (DHCP) usiłuje go uzyskać. W pozostałych przypadkach użycie adresu typu broadcast lub multicast jako adresu źródłowego oznaczać będzie próbę naruszenia bezpieczeństwa poprzez atak typu **DoS (Denial of Service**) czyli blokadę usług. Host docelowy odpowiadając na taki pakiet powoduje wysłanie komunikatów do wszystkich hostów których adresy pasują do adresu rozgłoszeniowego czy grupowego.
Teoretycznie używając zwykłego polecenia *ping* do wysłania spreparowanego w ten sposób pakietu możemy spowodować zalanie naszej ofiary setkami komunikatów zwrotnych. Na podobnej zasadzie działa tzw. smerf, czyli programik używany zwłaszcza przez młodsze pokolenie interneutów do wszelkiego rodzaju „cyberwojen". Nie muszę chyba dodawać, że stosowanie podobnych praktyk jest w świetle nowego prawa karalne.
Opisany atak wygląda na banalny, ale tylko teoretycznie. Jest to trudny rodzaj ataku, ze względu na to, że większość ruterów i firewalli odfiltrowuje tego typu pakiety. Dlatego często stosuje się go np. w połączeniu z odpowiednią fragmentacją pakietów.

Nasz firewall powinien blokować pakiety z docelowym adresem rozgłoszeniowym oraz z grupowymi lub rozgłoszeniowymi adresami źródłowymi.

Opcje IP

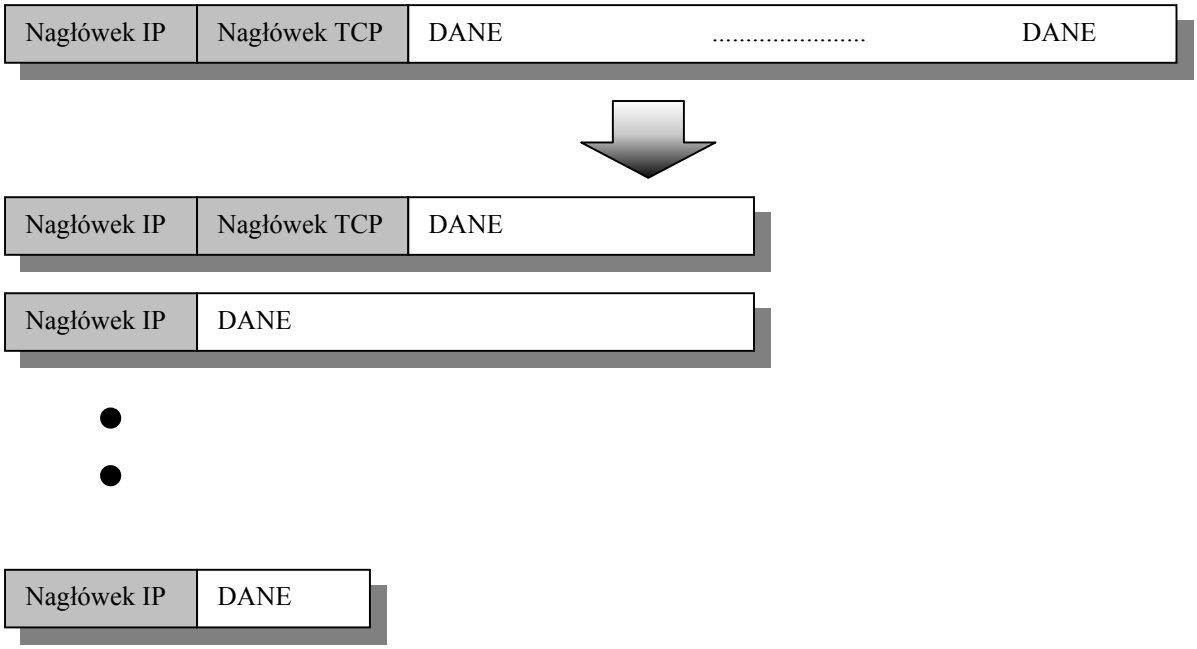
Jednym z istotniejszych dla nas elementów nagłówka IP, obok adresu źródłowego i docelowego, jest pole opcji. Jest ono zazwyczaj puste. W praktyce wykorzystywane jest najczęściej właśnie do prób włamań.
Najczęściej spotykaną opcją jest trasowanie źródłowe (***source routing***). Określa ona trasę jaką pakiet ma być przesyłany. Pozwala na pominięcie danych zawartych w tablicach trasowania ruterów przekazujących pakiet. Jest to korzystne w przypadku, gdy podejrzewamy, że któryś z ruterów pośredniczących zawiera błędne dane. W praktyce opcja ta jest stosowana do wymuszania konkretnych, z reguły niespodziewanych dróg w celu ominięcia zabezpieczeń. Jest to poważny problem, gdyż trasowanie źródłowe posiada wiele zalet, które możnaby wykorzystywać do optymalizacji połączeń. Niestety jest ono w większości przypadków zablokowane jako używane tylko do ataków. Sytuacja ta powoduje m. inn. problemy z rozpowszechnianiem rozwiązań mobilnego IP, czyli przenoszenia się z miejsca na miejsce bez konieczności zmieniania adresu IP.

Ze względów bezpieczeństwa powinniśmy wyłączyć trasowanie źródłowe na ruterach oraz odfiltrowywać na firewallu pakiety z ustawionymi opcjami IP. W większości przypadków nie powinno to wywołać żadnych problemów.

Fragmentacja IP

Jest to również bardzo istotna z punktu bezpieczeństwa oraz wydajności transmisji właściwość IP. Duży pakiet może zostać podzielony na mniejsze, dzięki czemu można go przesłać przez sieci, gdzie występuje ograniczenie wielkości pakietów. Taki podział nazywa się fragmentacją, a powstałe podczas niego kawałki – fragmentami.
Tak podzielony pakiet przesyłany jest przez kolejne odcinki. Dopiero po dotarciu do hosta docelowego fragmenty są składane w oryginalnej wielkości pakiet.

Fragmentacja danych



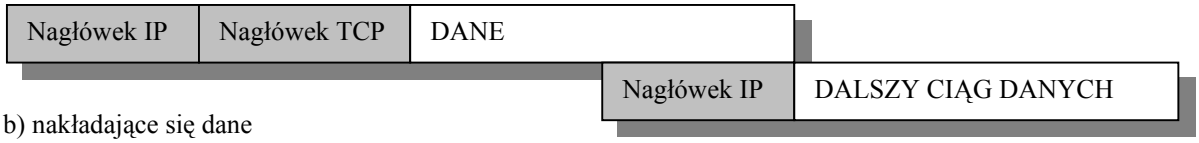
Decyzja o fragmentacji pakietu może zostać podjęta przez jeden z ruterów w dowolnym punkcie trasy pakietu. Można wykorzystać znacznik w nagłówku IP, aby zabronić fragmentacji pakietu. Wiąże się to jednak z ryzykiem odrzucenia go, jeśli wartość MTU (*Maxiumum Transmission Unit*) jest mniejsza niż wielkość pakietu. Istnieje jednak funkcja systemowa pozwalająca określić maksymalną wartość MTU, która używa znacznika zabezpieczającego przed fragmentacją.
Dla systemu określenie ścieżki MTU stanowi sposób na zdefiniowanie maksymalnej wielkości pakietu. Bardziej wydajne są duże, niepodzielone pakiety. Jednakże jeśli w dalszej części procesu przekazywania pakietu musiałby on ulec fragmentacji, znacznie zmniejszy to prędkość transmisji.
Najprostszą metodą na określenie maksymalnej wielkości pakietu jest wysłanie na początku transmisji pakietu ze znacznikiem „nie fragmentuj" i sprawdzenie czy nie został on odrzucony. Zwiększając wielkość kolejnych pakietów do momentu aż otrzyma komunikat o błędzie, system jest w stanie w sposób doświadczalny ustalić maksymalną dopuszczalną wielkość pakietu na danej trasie. Powoduje to straty na początku połączenia, ale są one rekompensowane w przypadku większej ilości przesyłanych danych.
Rozwiązanie to ma pewną poważną wadę : w przypadku nieprawidłowego przekazywania komunikatów ICMP, np. poprzez ich odfiltrowywanie na firewallu, niemożliwe jest poprawne określenie MTU.

Z punktu widzenia bezpieczeństwa problem z fragmentacją pakietów polega na tym, że tylko pierwszy fragment, jako zawierający nagłówek TCP, jest analizowany przez filtry firewalla. Pozostałe fragmenty były przepuszczane bez analizowania. Rozwiązanie to jest teoretycznie jest bezpieczne, gdyż w przypadku zatrzymania pierwszego fragmentu pakietu system docelowy nie jest w stanie złożyć oryginalnego pakietu.
Nie da się jednak do końca przewidzieć, jak na taki niekompletny pakiet zareaguje host docelowy. Będzie on przechowywać w pamięci otrzymane fragmenty czekając na brakujący. Może to zostać wykorzystane do ataku typu DoS.

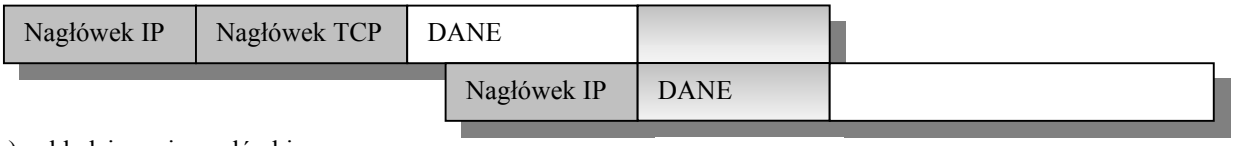
Podzielony na fragmenty pakiet mogą być też swojego rodzaju koniem trojańskim. Teoretycznie każdy pakiet zawiera informację gdzie się zaczyna i gdzie się kończy. Modyfikując te dane można nakładać na siebie pakiety w taki sposób, że pakiet z akceptowalnym nagłówkiem IP będzie zawierał w sobie pakiet z nieakceptowalnym nagłówkiem, który w normalnych warunkach zostałby odfiltrowany. Jednak ze względu na to, że znajduje się w jednym z fragmentów pakietu-nosiciela, zostaje przepuszczony bez analizy, gdyż system filtrujący nie spodziewa się w tym miejscu kolejnego nagłówka.
Systemy operacyjne różnie reagują na pokrywające się fragmenty. Może nastąpić ich odrzucenie lub próba niepoprawnego poskładania prowadząca do zawieszenia się systemu. Ogólnie rzecz ujmując fragmentacja pakietów bardzo źle wpływa na wydajność połączeń i, co bardzo ważne, może spowodować zablokowanie systemu bezpieczeństwa.

Nakładanie się fragmentów

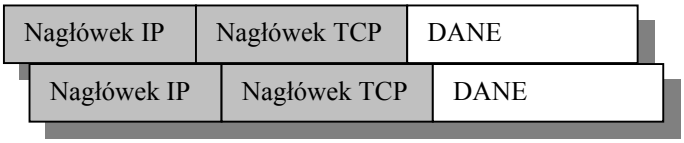
a) przypadek normalny



b) nakładające się dane



c) nakładające się nagłówki



Najlepszą metodą obrony w przypadku fragmentacji pakietów jest zastosowanie, zamiast filtrów odrzucających lub przepuszczających fragmenty pakietów, filtra ponownie składającego pakiety. Filtr taki powinien lokalnie składać pakiety, analizować je, i jeśli pakiet jest akceptowalny, wysyłać pod adres docelowy, w razie konieczności je fragmentując. Zwiększa to znacząco bezpieczeństwo systemu, niestety kosztem wydajności. Innym rozwiązaniem jest wycinanie wszystkich fragmentów. Może to zniszczyć pomyślne połączenie, ale stanowi to mniejsze zło niż ryzyko blokady systemu. Na szczęście, wraz z doskonaleniem metod określania ścieżki MTU, fragmentację pakietów w celach innych niż „nielegalne", spotyka się coraz rzadziej,

Jest to tylko kilka przykładowych zagrożeń, z jakimi możemy się spotkać podczas przetwarzania pakietów. Standardowe metody ochrony są wobec nich bezradne. Widać więc wyraźnie, że zbudowanie naprawdę skutecznego systemu zabezpieczeń to prawdziwa sztuka. Dlatego tak ważne jest częste kontrolowanie i okresowa modernizacja konfiguracji firewalla.
Zainteresowanym zagadnieniami związanymi z budową i analizą pakietów IP polecam następujące książki :

- Craig Hunt „Administrowanie sieciami TCP/IP" Wydawnictwo ReadMe
- E. D. Zwicky, S. Cooper, D.B. Chapman „ Internet Firewalls" Wydawnictwo ReadMe Warszawa 2001
- Edward Amoroso „ Wykrywanie intruzów" Wydawnictwo ReadMe Warszawa 1999

Michał Zimnicki
PUH KOMKAS s.c.