BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 17, 2002

Badanie możliwości przenikania firewalli atakami w tunelach kryptograficznych

Marek KWIATKOWSKI, Adam PAŁASZ
Adam E. PATKOWSKI, Maciej RYCHTER, Radosław RYŃSKI
Marcin STAWORKO, Konrad TRUBAS, Fryderyk WRÓBEL

Instytut Automatyki i Robotyki WAT
ul. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: Artykuł wprowadza w problematykę badań pewnej klasy teleinformatycznych ataków na systemy komputerowe chronione zaporą sieciową (firewallem). Przedstawiono odpowiednią procedurę badawczą. Do artykułu dołączono dwa wybrane protokoły z opisywanych badań.

1. Wstęp

Firewalle są obecnie szeroko reklamowanym i stosowanym, a w wielu sieciach jedynym, mechanizmem zabezpieczającym. Rozpoznanie słabości firewalli jest zatem niezwykle ważne. Możliwość tunelowania bywa instalowana (np. SSH) jako niezwykle skuteczny mechanizm ochronny przed podsłuchem (w szczególności tzw. *sniffingiem*), pożądane jest zatem określenie, czy i jakie ryzyko wprowadza to dla systemu. W Instytucie Automatyki i Robotyki w tym roku prowadzone są badania, zmierzające do znalezienia odpowiedzi na to pytanie.

Przedmiotem badań są możliwości wykonywania ataków na podsieci strzeżone przez rozbudowane filtry pakietowe, w szczególności firewalle, być może instalowane na samodzielnych bastionach. Istotą rozpatrywanych ataków jest przenikanie przez firewalle za pomocą tunelowania kryptograficznego

między komputerami spoza i wewnątrz sieci. Celem jest ocena zagrożeń i znalezienie sposobów detekcji oraz przeciwdziałania tego rodzaju atakom.

2. Podstawy

Zakłada się, że firewall jest **oprogramowaniem** osadzonym na komputerze wyposażonym w co najmniej dwa interfejsy (karty) sieciowe, rozdzielającym dwa obszary sieci, między którymi to obszarami nie istnieje alternatywna droga pakietów. Zadaniem firewalla jest poddawanie analizie informacji przebiegającej między rozdzielonymi sieciami i jej przekazywanie lub nie. Informacja nieprzekazana może zostać po prostu zgubiona (*drop* albo *deny*) lub odrzucona (*reject*). W tym ostatnim przypadku nadawca zostanie poinformowany o tym, że komunikacja jest zabroniona.

Firewalle zwykle poddają analizie informację w pewnym, wybranym protokole – np. analizują pakiety IP (są to firewalle działające w warstwie trzeciej modelu ISO/OSI) lub jednostki informacji wymieniane w ramach usług wyższego poziomu (firewalle działające w warstwie aplikacji; dodatkowo zdolne są one zwykle do buforowania informacji – są to tzw. proxy). Firewall musi skompletować pojedynczą jednostkę przesyłanej informacji, aby następnie poddać ją analizie. Dla protokołów wysokopoziomowych jednostki te mogą być znacznych i różnych rozmiarów: np. w protokole FTP taką jednostką będzie cały przesyłany plik. W przypadkach analizy porcji informacji dużych rozmiarów, firewalle mogą powodować znaczne zahamowania w transmisji, wynikające z wstrzymania przekazywania pakietów przez firewall do chwili skompletowania jednostki informacji protokołu wysokiego poziomu i podjęcia jej przesyłania dopiero po zakończeniu analizy. W praktyce firewalle nie kompletują jednak każdej jednostki informacji, ale po prostu zapamiętują pewne wybrane cechy przebiegających pakietów (protokołu IP4 – jednostek informacji w warstwie trzeciej). Dzięki temu mogą „wyrabiać sobie pogląd" na własności protokołu wyższej warstwy (np. TCP) w trakcie przebiegania pakietów, bez drastycznego spowalniania ich ruchu. Tę umiejętność nazywa się „*stateful analysis*" lub „*stateful inspection*". W efekcie wyposażenie firewalla działającego w warstwie IP w mechanizmy *stateful analysis* powoduje, że zaczyna on działać w warstwie wyższej.

Jak już wspomniano firewalle działające w warstwie IP praktycznie analizują tylko zawartość nagłówka każdego pakietu, dodanie im własności *stateful* rozszerza zakres analizy na nagłówki jednostek informacji warstwy wyższej i pewne dodatkowe możliwości analizy poprawności strumienia pakietów warstwy IP: np. odrzucone zostaną pakiety z flagą kontynuacji, gdy nie było poprzedzających je pakietów, podobnie traktowane są pakiety ACK nie

poprzedzone przez SYN itd. Wykryte również zostaną niewłaściwe konstrukcje pofragmentowanych pakietów warstw wyższych. Jest to istotnie nowa jakość praktycznie eliminująca tzw. skaning typu *stealth*. Nie zmienia to faktu, że zawartość pakietów każdej z warstw w przytłaczającej większości pozostanie nieanalizowana przez typowe firewalle.

Głównym elementem konfiguracji każdego firewalla jest uporządkowany zbiór reguł. Każda z reguł składa się warunku i zalecenia. Reguły stosowane są do każdej jednostki informacji (np. pakietu IP, jeśli w tej warstwie działa firewall) zgodnie z porządkiem zbioru reguł. Jeśli warunek pierwszej reguły nie jest spełniony dla tej jednostki informacji, to sprawdzana jest druga reguła i tak dalej, aż do wyczerpania zbioru lub do napotkania reguły, której warunek jest spełniony. Jeśli zaś warunek reguły jest spełniony, to do jednostki informacji stosuje się zalecenie owej spełnionej reguły. Zalecenie jest zwykle ze zbioru: *przepuścić* (pakiet), *zgubić* lub *odrzucić*. W przypadku *stateful analysis* reguły dodatkowo uwzględniają stan i manipulują czymś w rodzaju pamięci podręcznej stanów transmisji.

Obecnie firewalle (w każdym razie te produkcji czołowych firm) mogą współpracować z systemami wykrywania włamań (*IDS – Intruder Detection Systems*): na podstawie informacji z IDS, że nastąpiła próba ataku z komputera o pewnym adresie IP, firewall tworzy natychmiast odpowiednią dynamiczną regułę blokującą, rozszerzając tym samym zbiór reguł.

Firewalle stosowane są najczęściej z intencją ochrony pewnej podsieci komputerowej przed niepożądaną działalnością użytkowników spoza tej sieci, ale znane są, choć rzadsze, rozwiązania separujące dwa segmenty sieci korporacyjnej, przy czym nie rozstrzyga się, w której z podsieci są zasoby cenniejsze czy bardziej warte ochrony. Celem jest „kategoryzacja" zasobów: rozdzielenie zasobów podsieci. Pozwala to na uniemożliwienie licznych ataków wewnątrz korporacji.

W opisywanych dalej badaniach chronione zasoby nie są istotne – doskonale można się obejść bez tego pojęcia. Określeń „sieć wewnętrzna" i „sieć zewnętrzna" używa się tylko dla wygody. Należy zauważyć, że dotychczas opisane funkcje firewalla są w pełni symetryczne i nie wymagają preferowania którejś ze „stron" (inna rzecz, że mogą tego wymagać konkretne zastosowania firewalla). Jednak w rzeczywistych instalacjach firewalli filtrowaniu pakietów towarzyszą jeszcze inne funkcje, dla których opisana symetria nie występuje. Komputer-nosiciel firewalla, z racji zainstalowanych kilku interfejsów sieciowych pełni zwykle jednocześnie rolę bramy sieciowej (*gateway*), a w przypadku więcej niż dwóch interfejsów – także routera. Jako *gateway*, firewall najczęściej realizuje funkcję translacji adresów (*NAT – Network Address Translation*), a ta funkcja jest zdecydowanie asymetryczna – jeden z interfejsów jest zawsze „zewnętrzny". Podobnie w przypadku rozszerzenia firewalla o sensor IDS również wyróżnia się jedną ze stron – tę

mianowicie, po której wszystkie pakiety są analizowane przez IDS, co czyni tak uzupełniony firewall asymetrycznym. Wbrew pozorom wybór „strony" firewalla, po której zostanie zainstalowany sensor, wcale nie jest prosty. Upraszczając argumentacje: rozsądne jest zainstalowanie IDS po stronie „zewnętrznej" firewalla, bo chociaż w przypadku realizacji NAT analiza jest znacznie utrudniona, zmniejszając czułość IDS, to jednak, po wykryciu ataku i zablokowaniu ruchu przez firewall, IDS może nadal analizować działania napastnika, co daje pewne korzyści.

Dla opisywanych badań istotne jest to, że podlegające badaniu ataki komputerowe realizowane są „poprzez" firewall, co w skrócie oznacza, że system komputerowy, który jest narzędziem napastnika znajduje się po jednej stronie firewalla, zaś system komputerowy, który jest celem ataku („komputer ofiary") znajduje się po przeciwnej stronie firewalla. Można się rozsądnie umówić, że strona wewnętrzna to ta, po której znajdują się cele ataków.

Tunelem kryptograficznym nazywa się mechanizm zapewniający przesyłanie na pewnym odcinku trasy w sieci teleinformatycznej pakietów w postaci zaszyfrowanej. Tunel kryptograficzny tworzony jest zwykle dla jednego z podstawowych protokołów warstwy trzeciej lub czwartej. Początkiem tunelu może być komputer (najczęściej router szyfrujący lub stacja robocza) a dokładniej pewna warstwa oprogramowania sieciowego tego komputera. Nie zawsze jest to związane z dodaniem nowej warstwy protokołów (drogą kapsułkowania); w niektórych rozwiązaniach nagłówek pakietu pozostaje bez zmian, zaś szyfrowana jest tylko treść pakietu. O tunelowaniu mówi się, gdy szyfrowanie związane jest z wybranym protokołem a nie wyróżnia się explicite aplikacji, której komunikacja jest szyfrowana. W przypadku szyfrowania informacji przez aplikację lub system informatyczny pozostaje się przy określeniu szyfrowanie, unikając określenia „tunelowanie".

Mechanizmy tunelowania wykorzystywane są do realizacji VPN (*Virtual Private Networks*), w tym również małych VPNów tworzonych drogą „uzgodnień bilateralnych" między komputerami, jak np. w oprogramowaniu PGP firmy NAI. Znanym mechanizmem tunelującym jest SSH (*Secure SHell*). Typowe szyfrowanie na trasie klient-serwer w protokołach SSL (*Secure Socket Layer*) lub HTTPS może, co prawda przy niezbyt ortodoksyjnym zastosowaniu definicji, również zostać uznane za formę tunelowania. W wersji 6 protokołu IP szyfrowanie jest znacznie łatwiej dostępne niż w wersji 4 i należy się spodziewać rozpowszechnienia zjawiska tunelowania.

Przez „przenikanie" firewalla rozumieć należy przedostanie się przezeń pakietów, które, najogólniej rzecz biorąc, przedostać się nie powinny. Innymi słowy: bez tunelowania pakiety owe, w postaci niezaszyfrowanej, nie zostałyby przez firewall przepuszczone: zostałyby wykryte i zablokowane przez którąś

ze statycznych reguł lub po rozpoznaniu sygnatury ataku przez sensor IDS powstałaby dynamiczna reguła blokująca.

Tunelowanie jest skuteczną metodą przenikania firewalli, jeśli ukrywa przed firewallem tę część oryginalnego pakietu, którą wykorzystują reguły firewalla (np. oryginalny nagłówek pakietu IP), w tym także reguły *stateful analysis*, lub ukrywa przed sensorem IDS firewalla sygnatury ataków zawarte w treści pakietu.

3. Badania

Badania prowadzone były w laboratoriach Instytutu Automatyki i Robotyki. Do tej pory przedmiotem badania było oprogramowanie firm Symantec (dawniej Axent), CheckPoint oraz darmowe firewalle filtrujące dla systemu Linux i BSD:

- Symatec Enterprise Firewall (Axent Raptor 6.5) z rozszerzeniem NetProwler 3.5.1;
- CheckPoint Firewall 1 v. 4.1;
- CheckPoint Firewall Next Generation z rozszerzeniem SNORT 1.8.6 FlexResp;
- Ip Filter dla FreeBSD 4.4;
- PGP E-ppliance100 (firewall sprzętowy).

Sprawdzane techniki ataku wymagają starannego wyboru. Najogólniej muszą one spełniać kilka warunków:

- Technika ataku powinna być użyteczna samodzielnie lub w ramach scenariusza ataku kombinowanego.
- Atak powinien być blokowany przez firewall.
- Dzięki szyfrowaniu (w ramach tunelu) powinna istnieć możliwość ukrycia przed firewallem tej części przesyłanej informacji, która stanowi podstawę rozstrzygania warunku reguły blokującej.

Przykładami wybranych ataków są: różne formy ataków z agresywnych stron WWW, ataki przez tunel SSH lub ataki z wykorzystaniem połączenia ustanawianego przez VPN między stacjami wyposażonymi w PGP Corporate Desktop.

Dla osiągnięcia celów badań sformułowano procedurę badawczą, jako wzorzec postępowania w trakcie badań. Protokoły badań stanowią podstawę do heurystycznych analiz w ocenach zagrożeń, poszukiwaniu środków

zaradczych, możliwości ochrony i wykrywania ataków. **Pamiętać jednak należy, że badane techniki ataków mają pośredni związek z celem głównym poznawczym badań: przede wszystkim chodzi o określenie uogólnionej oceny zagrożeń powstających w wyniku wykorzystywania jednocześnie dwóch środków ochrony – firewalli i szyfrowania transmisji**.

4. Procedura badawcza i wybrane protokoły

Dla zilustrowania metodyki badań w Dodatku 1 przedstawiono wykorzystywaną procedurę badawczą, zaś w Dodatkach 2 i 3 zaprezentowano dwa protokoły badań firewalli różnych typów, rozszerzonych o sensory IDS. Zaniechano prezentacji technicznych dokumentów szczegółowych (jak plany sieci, czy wykazy elementów) – są one wymienione w protokołach i dostępne w IAiR.

Pierwsze z przedstawionych badań to próba przeniknięcia firewalla atakiem z agresywnej strony WWW. Klientem usługi jest komputer ofiary ataku, rozpoczynający połączenie z serwerem WWW komputera-napastnika. Z serwera nadsyłane są informacje, które powodują naruszenie bezpieczeństwa na komputerze ofiary. Oczywiście, aby naruszenie bezpieczeństwa (incydent) miało miejsce, oprogramowanie atakowanego komputera muszą cechować pewne podatności. Sposób wykorzystania podatności jest zwykle dobrze znany i można znaleźć lub określić dla niego tzw. sygnaturę ataku. Sygnatura ataku to pewne charakterystyczne cechy przesyłanej informacji, na podstawie których można ów atak rozpoznać. Sygnatury formułowane są tak, aby rozpoznanie ataku na podstawie zawartości przesyłanych pakietów było możliwie łatwe. Sygnatury opracowywane są przez zespoły specjalistów firm produkujących oprogramowanie IDS (Symantec, ISS, NAI) lub przez pospolite ruszenie entuzjastów (np. grupy związane z rozwojem i utrzymaniem aktualności oprogramowania Snort). Z reguły sygnatury ataków z agresywnych stron WWW zawarte są gdzieś wewnątrz pakietów TCP, co oznacza, że typowy firewall filtrujący w warstwie IP musi zostać dodatkowo wyposażony w mechanizmy rozpoznawania sygnatur wewnątrz pakietów. W opisywanym badaniu Symantec Enterprise Firewall rozszerzono o sensor NetProwler.

W zależności od podatności, które reprezentuje oprogramowanie atakowanego komputera, dalszy przebieg ataku może mieć bardzo różny przebieg: od zatrzymania działania (atak *Denial of Service – DoS*) po skryte osadzenie na komputerze ofiary oprogramowania monitorującego. Różne rodzaje „podrzuconych" tak programów otwierają możliwości bardzo różnych ataków. Co więcej: w zależności od tego, jakie skutki przyniesie użycie tego

oprogramowania zależy dalsze działanie napastnika, a więc i kwalifikacja ataku kombinowanego.

Jako przykład ataku kombinowanego, którego elementem składowym jest opisywana technika, można podać atak na dobrze zabezpieczoną sieć dużej firmy, z wykorzystaniem podatności występującej w domyślnej instalacji programu Internet Explorer w wersji 5.5 i wcześniejszych. Podatność ta pozwala na skryte dostarczenie programu do komputera ofiary, a następnie uruchomienie tego programu. Za sukces opisywanej techniki należy uznać właśnie przekazanie i zainstalowanie programu. W przypadku ataku na dobrze zabezpieczoną sieć firmy celem zastosowania tej techniki jest „zdobycie przyczółka" – zainstalowanie programu szpiegowskiego wewnątrz atakowanej sieci. Sam atak musi być przygotowany przez zwabienie możliwie dużej liczby potencjalnych ofiar na agresywną stronę WWW – np. przez wysłanie powiadomień pocztą elektroniczną o jakiejś niezwykle atrakcyjnej zawartości tej strony. W rezultacie na każdym podatnym komputerze, łączącym się z serwerem, zostanie osadzony program szpiegujący. Funkcje takiego programu to np. przeszukanie wszelkich dostępnych zasobów komputerów sieci firmowej dla znalezienia pewnego dokumentu lub też systematyczne, długookresowe monitorowanie wszelkiej aktywności użytkowników w oczekiwaniu uzyskania tą drogą atrakcyjnych informacji. Za szczególną cechę tego rodzaju ataku należy uznać przewidywaną wysoką skuteczność w ataku na duże sieci zawierające systemy pracy biurowej: im większa liczba zwabionych komputerów, tym większe prawdopodobieństwo natrafienia na system o niedoskonałej konfiguracji lub niezaaplikowanych aktualizacjach.

Atak z agresywnych stron WWW jest wykrywany przez sensor firewalla i zostaje powstrzymany przez zablokowanie wszelkiej komunikacji przez firewall z komputerem napastnika. Na skutek pewnej bezwładności systemu, wynikającej z konieczności komunikacji sensor-firewall, blokada następuje dopiero po pewnym czasie. Na szczęście jest to czas wielokrotnie krótszy od czasu transmisji programu szpiegowskiego, co oznacza, że instalacja tego programu na komputerze ofiary nie ma szans powodzenia.

Dla uniknięcia wykrycia ataku wystarczy zaszyfrowanie sygnatur ataków podczas ich przebiegania przed sensorem firewalla. Do tego celu może zostać wykorzystany dowolny mechanizm szyfrujący, jednak w dobrze zabezpieczonej sieci praktycznie możliwe jest tylko wykorzystanie protokołu HTTPS. Brak wyboru rekompensowany jest skutecznością – jest mało prawdopodobne, aby możliwość użycia tego protokołu została zablokowana na granicy sieci, a jest to jedyny sposób uniknięcia ukrycia sygnatur ataku.

Przeprowadzone badanie pozwoliło sformułować wniosek, że **w przy-**

Za interesujący wynik należy uznać rozpoznanie wielkości opóźnienia reakcji firewalla na rozpoznanie ataku przez zewnętrzny sensor: od chwili nadejścia pakietu z sygnaturą ataku, do chwili efektywności odpowiedniej dynamicznej reguły blokującej. Właściwą, bo użyteczną, miarą tego opóźnienia, jest liczba pakietów przepuszczonych przez firewall do chwili osiągnięcia efektywności przez regułę. Liczba ta pozwala na wyznaczenie największej agresywnej przesyłki, której nie zdoła zablokować firewall. W przypadku badanego ataku pozwala to wnioskować o maksymalnych rozmiarach programu, który ma szanse się przemknąć przez firewall i zostać wykonany w atakowanym systemie.

Drugie z przedstawionych badań to próba nawiązania kontaktu (z zewnątrz sieci) z serwerem zdalnego sterowania zainstalowanym wewnątrz sieci. Jest to badanie zupełnie podstawowe – sygnatura ataku zlokalizowana jest w nagłówku pakietu IP: jest to po prostu numer portu docelowego, charakterystyczny dla serwera zdalnego sterowania. Z tego powodu zdolność rozpoznawania i blokowania tego rodzaju ataków posiadają nawet najprostsze firewalle. Dla tego, aby istniały techniczne możliwości przeprowadzenia ataku, musi istnieć szansa połączenia z zewnątrz (z inicjatywy komputera atakującego) ze znajdującym się wewnątrz sieci komputerem, na którym jest osadzone oprogramowanie pozwalające na ustanowienie tunelu kryptograficznego. Istotą mechanizmu pozwalającego na ukrycie połączenia jest ustanowienie tunelu „przebijającego" firewall i skierowanie pakietów (opuszczających tunel) do komputera docelowego. Do badań użyto oprogramowania NetBus, jako najbardziej znanego konia trojańskiego, oraz oprogramowania SSH, zapewniającego pożądane własności: tunelowanie oraz tzw. *port forwarding*".

Sukcesem jest w tym przypadku nawiązanie połączenia. Wykorzystywaną podatnością jest obecność na atakowanym komputerze serwera zdalnego sterowania oraz możliwość nawiązania połączenia z zewnątrz sieci z wewnętrznym komputerem z zainstalowanym serwerem SSH. Dla powodzenia ataku konieczna jest jednak autentykacja po połączeniu z serwerem SSH, co znakomicie ogranicza szanse. W przypadku ataku kombinowanego zakłada się zdobycie danych do autentykacji (identyfikatora i hasła albo klucza) inną techniką. Można także wyobrazić sobie działanie użytkownika uprawnionego do połączeń przez SSH. Podobnie wcześniejsze skryte osadzenie serwera zdalnego sterowania na komputerze docelowym nie wydaje się przedsięwzięciem łatwym.

Badanie wykazało skuteczność przenikania firewalla, czego zresztą należało się spodziewać. Wniosek podstawowy jest ten, że ustanowienie połączenia SSH przez firewall należy w ogólnym przypadku uznać za błąd konfiguracyjny.

5. Obserwacje i wnioski

Tunelowanie jest zawsze skutecznym sposobem przenikania firewalli: każdy atak, który jest identyfikowany przez oprogramowanie analizujące przesyłaną informację, może być ukryty dzięki systematycznemu zniekształcaniu tej informacji. W szczególności efektywne okazuje się zniekształcanie przez szyfrowanie.

Dla powodzenia ukrycia ataku przez tunelowanie konieczne jest istnienie tunelu. Tunel może być ustanowiony inną techniką ataku w ramach ataku kombinowanego albo zostać utworzony w dobrej wierze w ramach budowy lub modernizacji sieci. Obecnie w sieciach akceptowane jest praktycznie tylko tunelowanie kryptograficzne i tylko takie oprogramowanie można zastać albo jego osadzenie będzie technicznie dozwolone. Tunel nie musi prowadzić od napastnika do ofiary – wystarczy tylko ten odcinek trasy pakietów, nad którym czuwa sensor firewalla. Co więcej, typowe oprogramowanie tunelujące oferuje zwykle dodatkowe funkcje, w tym np. mechanizm *port forwarding*, dzięki któremu możliwe jest osiągnięcie z zewnątrz połączenia z serwerami usług osadzonych na komputerach skutecznie maskowanych przez *Network Address Translation* i nieosiągalnych z zewnątrz sieci normalną drogą. *Port forwarding* jest istotną funkcją implementacji, ale mimo wszystko od efektu tunelowania niezależną. Nie sposób oprzeć się wrażeniu pewnej symetrii: podobnie maskowanie adresów przez mechanizm *NAT* jest funkcją bramy sieciowej (*gateway'a*) zwykle z firewallem występującą, ale również odeń niezależną.

Na koniec – na podstawie przeprowadzonych badań można również sformułować pewne zalecenia dla personelu zajmującego się bezpieczeństwem sieci teleinformatycznej:

1. Wszelkie techniki ochrony powinny być połączone w niesprzeczny system tak, aby ich skutki nie pozostawały w kolizji. Nieuniknione przypadki powinny być starannie przemyślane.
2. Należy eliminować możliwości ustanawiania tuneli kryptograficznych „przechodzących przez firewall".

Ponieważ nie wszystkie tunele dadzą się wyeliminować, należy oczekiwać pojawienia się sensorów „*host based*": zainstalowanych na komputerach w sieci wewnętrznej programów-agentów, analizujących ruch tylko do macierzystego komputera i sygnalizujących atak firewallowi.

DODATEK 1. PROCEDURA BADAWCZA

Metoda badania firewalli na przenikanie ataków teleinformatycznych za pomocą tunelowania kryptograficznego

1. Cel procedury

Celem procedury jest przedstawienie metody badania firewalli na przenikanie ataków teleinformatycznych za pomocą tunelowania kryptograficznego.

2. Definicje

Firewall (zapora sieciowa) – oprogramowanie osadzone zwykle na komputerze wyposażonym w dwa lub więcej interfejsów sieciowych, przekazujące ruch pakietów między interfejsami, zdolne do filtrowania tego ruchu na podstawie zawartości pakietów. Firewalle mogą uwzględniać historię ruchu (przez pamiętanie cech poprzednich pakietów) w regułach filtrowania (*stateful analysis*).

Filtrowanie – działanie elementu przełączającego (gateway'a, routera, firewalla) polegające na selektywnym przekazywaniu pakietów między interfejsami sieciowymi. Dla każdego nadchodzącego pakietu decyzja o przekazaniu podejmowana jest na podstawie **uporządkowanego zbioru reguł**. Każda z reguł zastosowana do pojedynczego pakietu generuje wynik w logice trójwartościowej: przepuścić, odrzucić (nie przekazywać), poddać sprawdzeniu następną regułą. Pakiet sprawdzany jest kolejnymi regułami w ustalonym porządku do chwili, gdy jedna z nich da wynik rozstrzygający: przekazać albo odrzucić. Ostatnia reguła w zbiorze powinna dawać wyłącznie wyniki rozstrzygające; może być również bezwarunkowa, np.: pozostałe odrzucić.

Ruch sieciowy – zbiór wszystkich przesłań pakietów między elementami przełączającymi i końcówkami sieciowymi.

Tunelowanie kryptograficzne – przesyłanie pakietów między dwoma punktami w sieci, polegające na zaszyfrowaniu treści pakietów w jednym z punktów, a następnie za pomocą zabiegu kapsułkowania przesłanie owej

zaszyfrowanej informacji (być może przez wiele pośrednich punktów sieciowych) do drugiego punktu sieciowego, gdzie informacja zostaje odszyfrowana i odtworzona zostaje dokładnie pierwotna postać (taka jak dotarła do punktu pierwszego) pakietów i pakiety zostają przekazane dalej. Protokół transmisji między punktem pierwszym a drugim nie jest dla definicji istotny, musi tylko zapewniać poprawne przekazanie do punktu drugiego w wybranej sieci.

Kapsułkowanie – zabieg przekształcenia informacji w pakiet przez wygenerowanie nagłówka i fragmentu końcowego. Zwykle określenie to stosowane jest do zabiegu przekształcania pakietu pewnego protokołu (np. TCP) w jeden lub kilka pakietów protokołu niższej warstwy (np. IP) według modelu ISO/OSI.

Szyfrowanie – zabieg przekształcenia informacji do postaci, w której treść tej informacji staje się niedostępna bez posiadania specjalnej informacji dodatkowej nazywanej kluczem i bez znajomości sposobu przekształcenia do postaci pierwotnej (algorytmu deszyfrowania). Sposób szyfrowania nazywany jest algorytmem szyfrowania i również wymaga klucza – niekoniecznie identycznego z kluczem służącym do odszyfrowywania.

Punkt sieciowy lub **element sieciowy** – końcówka sieciowa: serwer lub stacja robocza, albo element przełączający – urządzenie służące do przekazywania pakietów.

Atak teleinformatyczny – dowolne działanie podjęte środkami teleinformatycznymi (**przesyłanie informacji** lub **uruchamianie programów**) w sieci teleinformatycznej nie angażujące innych mediów do transmisji informacji, powodujące zmiany stanu elementów sieci (w tym stanu danych i programów), które to zmiany nie zostały uznane za dopuszczalne przez dysponentów tych elementów sieciowych, których owe zmiany dotyczą.

Dysponent (administrator) elementu sieciowego – osoba prawna lub fizyczna umocowana prawnie do formułowania zasad użycia sprzętu lub oprogramowania. Dysponent działa w imieniu właściciela lub na podstawie uregulowań prawnych.

Przenikanie firewalla – zjawisko przekazania przez firewall takich informacji (w tym informacji pełniących rolę sterującą), które, zgodnie z przyjętymi przez instytucję zarządzającą zasadami, powinny zostać zablokowane.

Przekazanie informacji – wysłanie przez jeden z interfejsów sieciowych informacji nadeszłej wcześniej na inny interfejs sieciowy.

3. Zakres stosowania procedury

Procedurę stosuje się do sprawdzania odporności na przenikanie tunelami kryptograficznymi firewalli osadzanych na mikrokomputerach IBM PC.

4. Wymagane wyposażenie

- 6 stacji roboczych sieciowych: komputerów zgodnych z IBM PC, z pełnym ukompletowaniem standardowym, z interfejsami sieciowymi 100 MB/s;
- 1 komputer-nosiciel oprogramowania firewalli: zgodny z IBM PC, z pełnym wyposażeniem standardowym, z trzema interfejsami sieciowymi 100 MB/s i wymiennym dyskiem;
- 1 komputer przenośny, co najmniej dwusystemowy z Windows NT i Windows 2000, z interfejsem sieciowym 100 MB/s – do wykorzystania jako przenośny komputer pomiarowy;
- 3 huby, co najmniej czteroportowe z pełnym ukompletowaniem standardowym, 100 MB/s;
- 1 switch, co najmniej czteroportowy z pełnym ukompletowaniem standardowym, 100 MB/s;
- analizator stanów logicznych;
- kable połączeniowe sieciowe RJ45 min. 5 szt.;
- kable połączeniowe sieciowe skrzyżowane RJ45 min. 3 szt.

Licencjonowane oprogramowanie wykorzystywane w procedurze badawczej:

- *Windows NT workstation* w wersji polskiej: 6 licencji;
- *Windows 2000 Proffesional* w wersji polskiej: 6 licencji;
- *Windows 98 SE* w wersji polskiej: 3 licencje;
- *Windows XP Home Edition* w wersji polskiej: 3 licencje;
- *Windows 2000 Server* w wersji polskiej: 2 licencje;
- *Windows XP Professional* w wersji polskiej: 1 licencja;
- *Windows NT Server*: 2 licencje;
- *Solaris*: 1 licencja;
- *Sniffer Pro v.4.5* (Network Associations): 1 licencja;
- *Internet Information Server* (Microsoft): 1 licencja;
- *SiSoft Sandra Professional* (Catalin-Adrian Software, distributed by Si-Software): 4 licencje;
- *Visio Professional v. 5.0a for Midrosoft Windows* (Visio Corporation): 1 licencja;

- *MS Office XP* lub *MS Office 2000* (min. Word, Excell i PowerPoint): 1 licencja;
- Linux *Red Hat*;
- Linux *Mandrake*;
- Linux *Suse*.

5. Wymagania dotyczące personelu, środków ostrożności i środowiska

5.1. Minimalne kwalifikacje pracownika instalującego i konfigurującego sieć testową: inżynier informatyk z doświadczeniem w zakresie instalacji i konfiguracji oprogramowania sieciowego.

5.2. Minimalne kwalifikacje zawodowe pracownika realizującego badanie: technik informatyk.

5.3. Szczególne środki ostrożności:
- obowiązuje przestrzeganie zapisów wewnętrznego dokumentu laboratorium „*Przepisy BHP*" [3] (powinien być wywieszony w pomieszczeniu);
- obowiązuje przestrzeganie zapisów wewnętrznego dokumentu laboratorium „*Instrukcja przeciwpożarowa dla laboratorium*" [2] (powinien być wywieszony w pomieszczeniu);
- obowiązują ogólne przepisy BHP.

5.4. Warunki środowiska:
- temperatura w pomieszczeniu od +10 do +35 °C;
- wilgotność względna 40÷80 %.

6. Opis procedury

Dla każdego badania wstępnie powinny być przygotowane dokumenty:
- plan połączeń sieci testowej (dla badania) [4];
- wykaz inwentaryzacyjny sieci testowej (dla badania) [5];
- opis oprogramowania i konfiguracji oprogramowania elementów sieciowych (może być w postaci zbioru raportów automatycznych [6]); w tym szczególne warunki oprogramowania (np. zakładane słabości atakowanego systemu) i oprogramowanie specjalne [7];
- opis ataku, w tym definicję kryterium skuteczności [8];
- opis atakowanego firewalla;
- opis reguł blokujących atak [9];

na ich podstawie przeprowadzane powinny być kolejne działania:

6.1. Czynności wstępne.

Czynności wstępne wykonywane są w warunkach środowiska zgodnie z punktem 5.4 niniejszej procedury. Należy sprawdzić:

- zgodność połączeń w sieci z planem połączeń sieci testowej do badania;
- czy w gniazdach na dyski wymienne osadzone są właściwe dyski;
- czy kable zasilające są podłączone do właściwych gniazd zasilających.

6.2. Przygotowanie sieci do badań.

Instalacje realizowane są tylko według potrzeb.

- sprawdzenie konfiguracji i oprogramowania stacji pomiarowych na zgodność z opisem do badania;
- osadzenie właściwych systemów operacyjnych na stacjach roboczych;
- osadzenie oprogramowania testowego do ataku na stacjach roboczych;
- osadzenie systemu operacyjnego i oprogramowania firewalla (w przypadku firewalla sprzętowego włączenie go i sprawdzenie konfiguracji ze stacji pomiarowej).

6.3. Przeprowadzenie ataku wzorcowego:

- wyłączyć firewall przez wyłączenie funkcji filtrowania lub całkowite wyłączenie oprogramowania firewalla i pozostawienie funkcji gateway'a; w skrajnym wypadku (np. dla słabo konfigurowalnych firewalli sprzętowych) komputer-firewall można zastąpić hubem lub switchem;
- przeprowadzić atak;
- odnotować uwagi o skuteczności;

w przypadku nieskuteczności ataku na tym etapie procedura zostaje zakończona, ze względu na zły dobór metody ataku (nieskuteczność).

6.4. Sprawdzenie realizowalności ataku przez tunel kryptograficzny:

- wyłączyć firewall przez wyłączenie funkcji filtrowania lub całkowite wyłączenie oprogramowania firewalla i pozostawienie funkcji gateway'a; w skrajnym wypadku (np. dla słabo konfigurowalnych firewalli sprzętowych) komputer-firewall można zastąpić hubem lub switchem;
- posadowić na stacjach roboczych po obu stronach firewalla oprogramowanie do tworzenia tunelu kryptograficznego i odpowiednio je skonfigurować;
- przeprowadzić atak;
- odnotować uwagi o skuteczności.

W przypadku nieskuteczności ataku na tym etapie procedura zostaje zakończona, ze względu na zły dobór metody ataku (niemożliwość realizacji przez tunel kryptograficzny).

6.5. Sprawdzenie skuteczności działania firewalla:
- włączyć firewall i zdefiniować reguły blokujące atak;
- przeprowadzić atak;
- odnotować uwagi o skuteczności.

W przypadku skuteczności ataku na tym etapie procedura zostaje zakończona, ze względu na niewłaściwy dobór metody ataku dla firewalla (nieskuteczność firewalla).

6.6. Sprawdzenie skuteczności tunelowania:
- włączyć firewall i zdefiniować reguły blokujące atak;
- przeprowadzić atak;
- odnotować uwagi o skuteczności.

Na koniec należy opracować protokół badania [10].

Wykaz dokumentów związanych:

[1] Rozporządzenie Ministra Spraw Wewnętrznych z dnia 3 listopada 1992 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów. Na podstawie art. 13 ust. 1 pkt 2 i art. 5 ust. 2 ustawy z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz. U. Nr 81, poz. 351).

[2] *Instrukcja przeciwpożarowa dla laboratorium* – wewnętrzny wyciąg z [1], opracowany dla laboratorium.

[3] *Przepisy BHP* – wewnętrzny wyciąg z ogólnych przepisów bezpieczeństwa i higieny pracy, opracowany dla laboratorium.

[4] *Plan połączeń sieci testowej* – wykonany w Microsoft Visio.

[5] Wykaz inwentaryzacyjny elementów sieci testowej – wykonany w formie tabeli w Microsoft Word.

[6] *Raport automatyczny z konfiguracji komputera* – generowany przez program testujący SiSoft Sandra lub podobny

[7] *Opis oprogramowania specjalnego i jego konfiguracji*; w tym szczególne warunki oprogramowania: oprogramowanie do ataku, oprogramowanie do tunelowania, zakładane słabości atakowanego systemu, firewall.

[8] *Opis ataku*, w tym definicja kryterium skuteczności

[9] Opis ustawień szczególnych firewalla – m.in. reguł blokujących atak

[10] *Protokół badania* – może zawierać treści [4], [5], [7], [8], [9] jeśli nie jest rozsądne wytwarzanie ich jako oddzielnych dokumentów.

DODATEK 2.

Możliwości przenikania firewalla Symantec Enterprise Firewall atakiem z agresywnych stron WWW za pomocą tunelu kryptograficznego w protokole HTTPS

PROTOKÓŁ BADANIA nr 02/08/01

1. Dane ogólne

Data: 29.08.2002 r.

Miejsce badania: Instytut Automatyki i Robotyki Wydziału Cybernetyki WAT.

Wykonawcy: Marek Kwiatkowski, Marcin Staworko, Konrad Trubas.

2. Badany firewall

W badaniach wykorzystano jako podstawowy obiekt badań Symantec Enterprise Firewall (nazwa handlowa firmy Symantec) opatrzony identyfikatorem "Raptor Firewall". Firewall został rozbudowany o realizującego funkcję sensora agenta systemu wykrywania włamań NetProwler 3.5.1. Pakiet dystrybucyjny został udostępniony do badań przez firmę Symantec, zaś pakiet dystrybucyjny sensora został pobrany z witryny internetowej tej firmy (http://www.symantec.com.pl).

2.1. Identyfikatory oprogramowania firewalla:

Product Type: Raptor Firewall
Platform: NT
Version: 6.5.0
Build: International
License Information:
Type= Evaluation

Expires= Wed Sep 18 02:00:00 2002
Users Limit = Unlimited
Supported Features:
Gateway
DES Encryption

2.2. Identyfikatory pakietu dystrybucyjnego:

RaptorFW w/PowerVPN 6.5 NT Eval I (RFVE-06726),
Serial: 2222033403,
Passcode: *[usunięto przed publikacją]*,
Dodatkowe oznaczenie: 001.257K11.ENG.

2.3. Wybrane cechy firewalla:

Przedstawione poniżej cechy firewalla Symantec Enterprise Firewall zostały wybrane ze względu na rolę tego oprogramowania w badaniach. Firewall ten charakteryzuje się następującymi cechami:

- filtruje pakiety w warstwie trzeciej siedmiowarstwowego modelu ISO/OSI, na podstawie analizy nagłówka pakietu DoD IP,
- realizuje funkcję translacji adresów sieciowych (NAT – Network Address Translation), która umożliwia ukrycie wewnętrznych adresów sieci chronionej.
- posiada zdolność współpracy z systemami wykrywania włamań (np.: NetProwler),

W skład firewalla wchodzi konsola RMC (Raptor Management Console) upraszczająca ustalanie reguł i zarządzanie dzięki zastosowaniu mechanizmu MMC (Microsoft Management Console). Symantec Enterprise Firewall wykorzystuje MMC do administrowania na komputerach z Windows NT.

Opis szczegółowy firewalla znajduje się w [18].

2.4. Identyfikatory oprogramowania sensora:

- NetProwler Console, NetProwler 3.5.1, Build Date Aug 28 2000, 14:25:11.
- NetProwler Agent, NetProwler 3.5.1, Build Date Aug 28 2000, 14:16:57.
- NetProwler Manager, NetProwler 3.5.1, Build Date Aug 28 2000, 14:30:11.
- Plik dystrybucyjny o nazwie: NetProwler351Setup.exe (75298482B) z dnia 07.12.2000 r.

2.5. Wybrane cechy sensora:

W skład systemu NetProwler firmy Symantec wchodzą:

Konsola – główny interfejs graficzny programu NetProwler, pozwalający na centralną konfigurację i zarządzanie agentami zainstalowanymi w sieci. Konsola m.in. umożliwia: tworzenie nowych sygnatur ataków, monitorowanie stanu agentów, generowanie i przegląd raportów bezpieczeństwa.

Manager - punkt w którym przechowywane są dane o konfiguracji, lokalizacji definicji sygnatur ataków i informacji o atakach. Na podstawie instrukcji otrzymywanych z konsoli zarządza agentami.

Agent - program monitorujący ruch w sieci, wychwytujący wybrane zachowania i w czasie rzeczywistym odpowiednio reagujący na nie.

NetProwler monitoruje ruch w sieci, analizując każdy przebiegający pakiet w dostępnym segmencie sieci (lub VLANie), przez porównanie zawartości pakietu z predefiniowanymi przez producenta sygnaturami ataków. Produkt ten posiada również tzw. kreator, służący do zadawania własnych sygnatur ataku. Sensor udostępnia możliwości automatycznej reakcji: rejestrowanie sesji, przerywanie, przechwytywanie, raportowanie, alarmowanie oraz „utwardzanie" (*hardening*) czy raczej „umacnianie" zapory sieciowej. Przez umacnianie zapory sieciowej rozumie się powiadomienie zapory o wybranych cechach napastnika (zwykle przez podanie adresu IP), co pozwala zaporze na włączenie dynamicznej reguły blokującej ruch od napastnika. Rozległe możliwości IDS obejmują także funkcje zgłaszania informacji na własną konsolę zdarzeń oraz przekazywanie informacji o ataku na pager, przez SNMP lub e-mail.

Dokumentacja producenta znajduje się w [21] i [22].

3. Środowisko badania – konfiguracja sieci testowej:

Plan sieci testowej znajduje się w [17].
Wykaz poszczególnych elementów sieci testowej ujęto w [16].
Opisy współpracy i synchronizacji sensora z firewallem znajdują się w [19], [20] i [23]

4. Badana technika ataku:

4.1. Atakowane systemy

Do przeprowadzenia ataku na stacji roboczej ofiary musi działać jeden z systemów operacyjnych firmy Microsoft: Windows 9x, Me, NT lub 2000 z zainstalowaną przeglądarką Internet Explorer w wersji 5.01 lub 5.5 (bez aktualizacji ServicePack2). Microsoft nie udostępnia informacji co do obecności opisanej dalej podatności we wcześniejszych wersjach IE.

4.2. Wykorzystywana podatność

Wykorzystywana w przeprowadzonym ataku podatność polega na tym, że Internet Explorer w wersjach 5.01 i 5.5, może odczytywać i otwierać binarne załączniki poczty elektronicznej w sposób właściwy dla ich typu MIME. Jeśli agresor stworzy plik poczty elektronicznej (dla Outlook Express w postaci pliku eml) formatu HTML zawierający wykonywalny załącznik i zmodyfikuje zapis typu MIME w nagłówku tak, aby załącznik ten był akceptowany do bezwarunkowej obsługi (np. prezentacji audio) przez IE, załącznik zostanie obsłużony według swego właściwego typu: automatycznie uruchomiony (więcej szczegółów na temat podatności w [11] i [26]).

4.3. Sposób przeprowadzenia ataku

W celu przeprowadzenia ataku należy spreparować stronę www z automatycznym odwołaniem do przygotowanego pliku typu eml. Wykorzystana w opisywanych niniejszym protokołem badaniach strona WWW o nazwie Index.htm (kod) znajduje się w [24], wykorzystany plik demo.eml załączono osobno [25].

Dla samego ataku rodzaj programu sprowadzanego w pliku eml na komputer ofiary (tu Netbus Pro) nie ma żadnego znaczenia. Istotna jest tylko sygnalizacja obecności po uruchomieniu, świadcząca o powodzeniu ataku. Netbus Pro Server został wybrany tylko z tego powodu, że oczekiwano, że w przypadku rzeczywistych ataków prowadzonych badaną techniką, zostanie użyty program o zbliżonych cechach (głównie rozmiarach). Sygnałem świadczącym o jego uruchomieniu (i powodzeniu ataku) jest wyświetlenie okna ustawień.

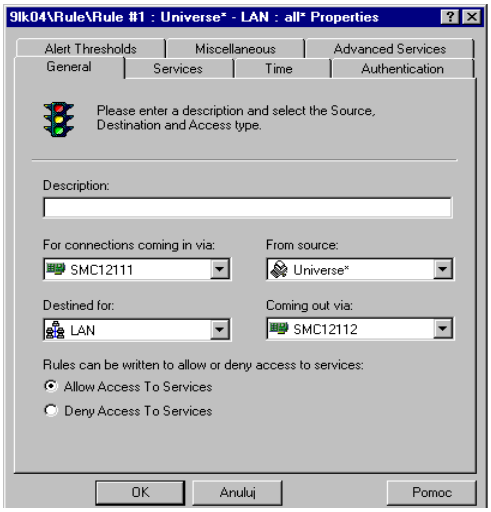
4.4. Sukces ataku

Atak uznaje się za udany tylko w przypadku poprawnego wykonania się na atakowanej stacji roboczej programu stanowiącego binarną zawartość pliku demo.eml.

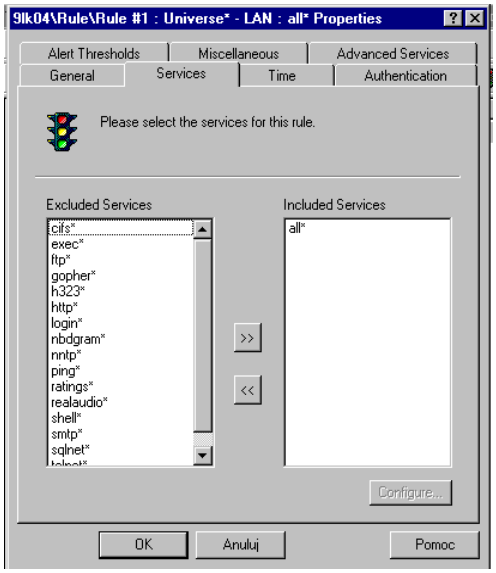
5. Wykorzystywane reguły blokujące:

W przeprowadzonym badaniu na firewallu nie zostały ustawione żadne szczególne reguły blokujące, ruch pakietów w obie strony odbywał się bez ograniczeń. Konfiguracja wykorzystywanych w badaniach reguł (o nazwach Rule#1, Rule#2) została przedstawiona na rysunkach 1, 2, 3 i 4.

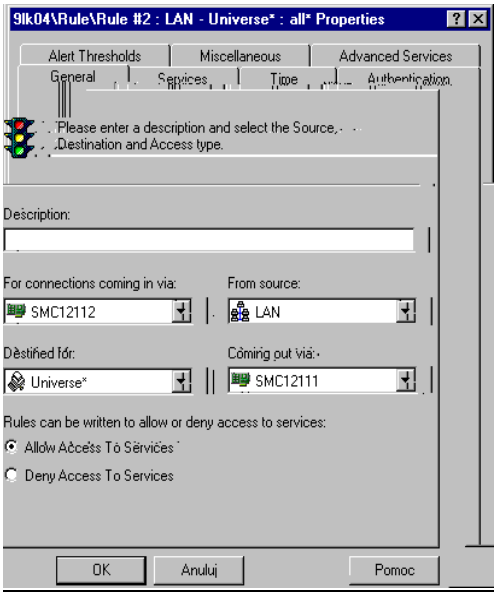
Zablokowanie ataku zostało oparte na działaniu sensora, którego zadaniem było wykrycie ataku i powiadomienie firewalla. Ponieważ zestaw sygnatur dostarczany w pakiecie dystrybucyjnym NetProwler nie przewiduje ataku wykonywanego w trakcie badania, konieczne było wprowadzenie własnej sygnatury tego ataku. NetProwler umożliwia tworzenie i dodawanie sygnatur, za pomocą tego mechanizmu wprowadzono sygnaturę wykorzystywanego ataku, nadając jej nazwę NaszaSygnatura. W celu sprawdzenia skuteczności tej sygnatury w doświadczalnym sensorze dezaktywowano wszystkie inne sygnatury ataków. Szczegółowy opis tworzenia sygnatury NaszSygnatura znajduje się w [15].



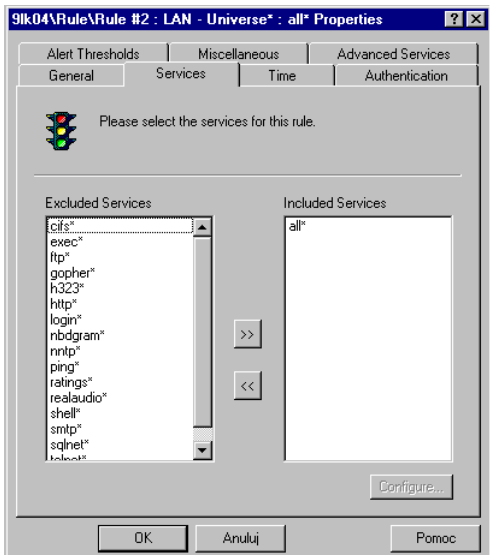
Rys. 1. Zakładka General dla reguły Rule#1



Rys. 2. Zakładka Services dla reguły Rule#1

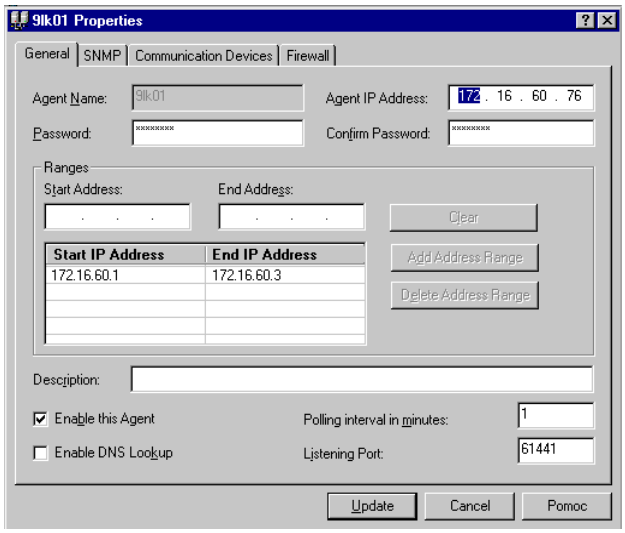


Rys. 3. Zakładka General dla reguły Rule#2

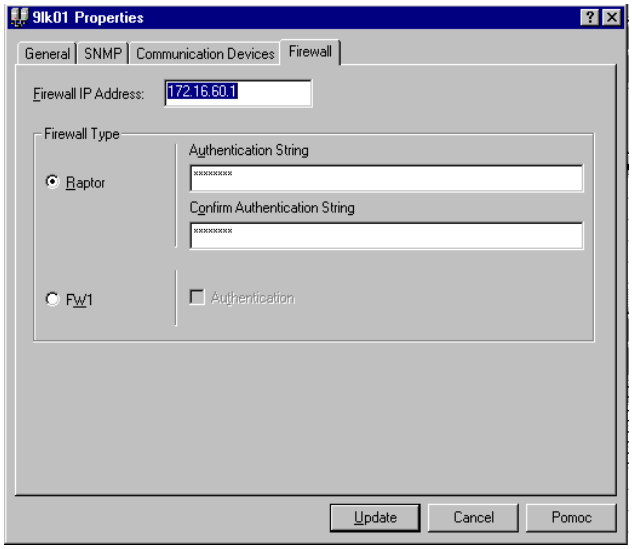


Rys. 4. Zakładka Services dla reguły Rule#2

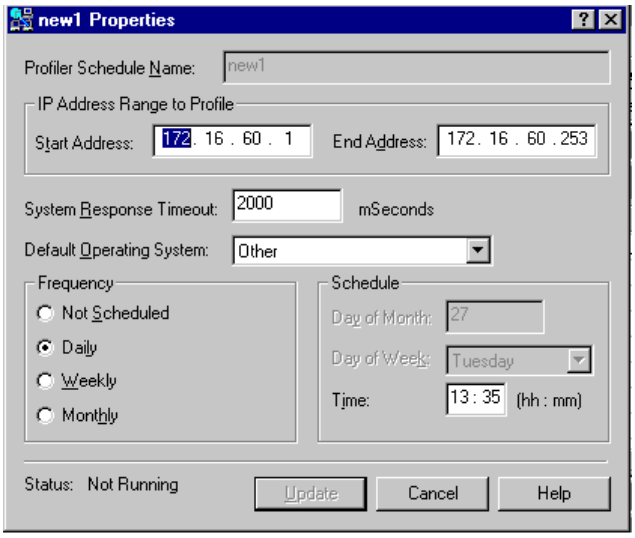
Szczegóły konfiguracji NetProwlera istotne ze względu na przeprowadzane badania przedstawiono na rysunkach 5, 6 i 7.



Rys. 5. Ustawienia agenta w NetProwler Console - zakładka General



Rys. 6. Ustawienia agent w NetProwler Console - zakładka Firewall. Dotyczy ustawień współpracy sensora z FW Raptor



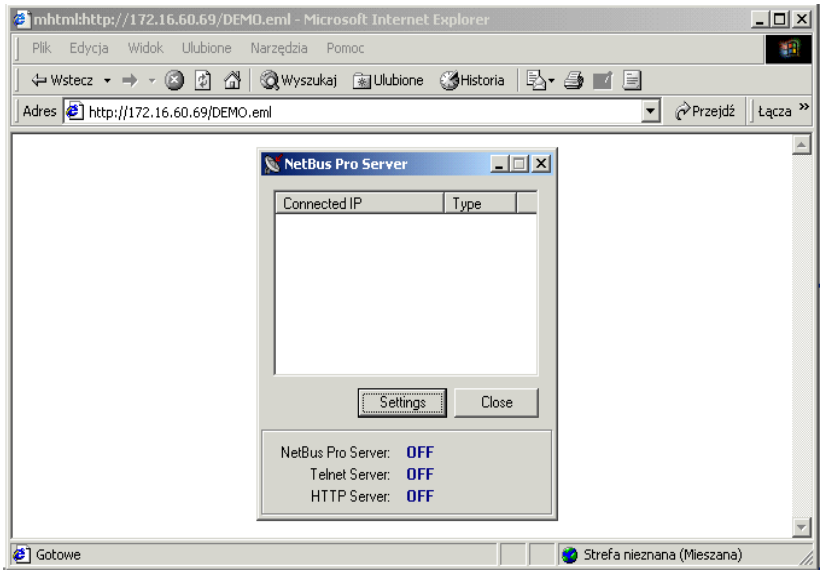
Rys. 7. Ustawienia funkcji Profiler w NetProwler Console. Profiler służy do cyklicznego odświeżania wiedzy sensora o otaczającej go sieci

6. Przebieg badania:

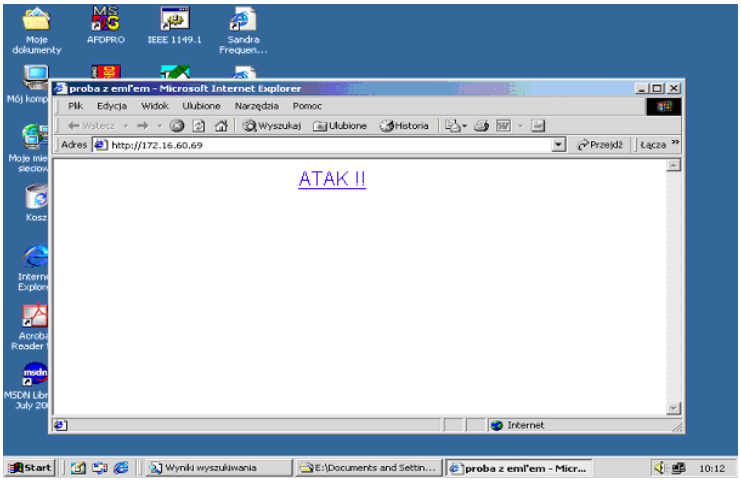
6.1. Raport z ataku wzorcowego

Badanie to, jak i wszystkie następne, przeprowadzono w sieci testowej [17]. Badanie polegało na ustanowieniu połączenia, w protokole HTTP, komputera (o nazwie 9lk08) z sieci wewnętrznej z komputerem z sieci zewnętrznej (o nazwie 9lk09) przy użyciu przeglądarki Internet Explorer w wersji 5.01. Na komputerze 9lk09 uruchomiony był serwer stron internetowych Apache, prezentujący agresywną stronę www o nazwie INDEX.HTML, przygotowaną zgodnie z opisem przedstawionym w rozdziale 4.3: kod strony Index.html znajduje się w [24], zaś wykorzystany plik demo.eml załączono osobno [25].

Atak poprzedzono usunięciem wszystkich tymczasowych plików internetowych. Po połączeniu z serwerem wyświetlana była strona prowadząca (rys. 9). Właściwy atak następował po uruchomieniu łącza znajdującego się na tej stronie. Atak został przeprowadzony i zakończył się sukcesem. O powodzeniu ataku świadczyło pojawienie się okna ustawień programu Netbus Pro Server na ekranie atakowanego komputera (rys.8), co świadczy o sprowadzeniu z serwera i uruchomieniu programu zakodowanego w pliku Demo.eml.



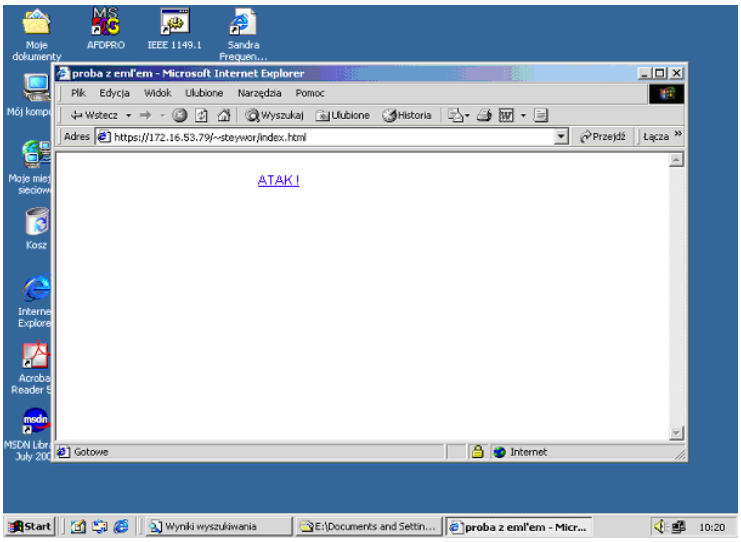
Rys. 8. Efekt ataku wzorcowego



Rys. 9. Prowadząca strona www

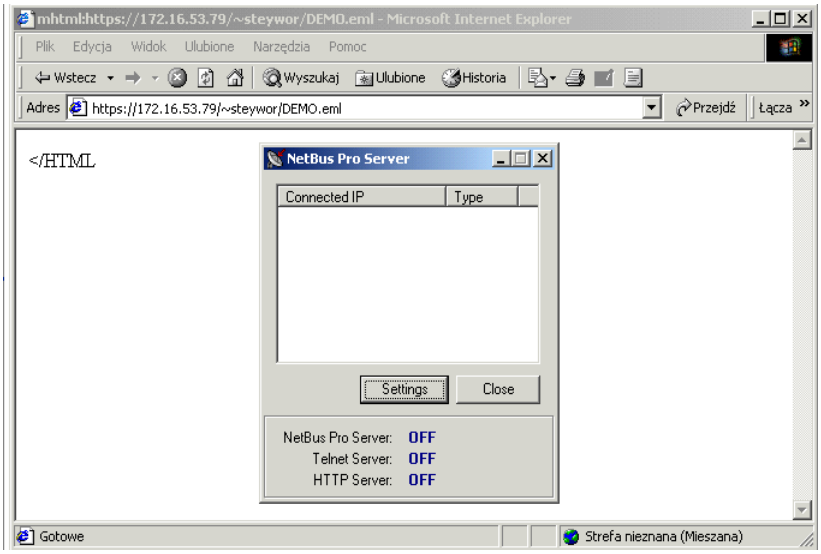
6.2. Raport z ataku przez tunel kryptograficzny bez firewalla

Badanie polegało na ustanowieniu połączenia, w protokole HTTPS między komputerem ofiary (o nazwie 9lk08) a serwerem stron WWW na komputerze o adresie 172.16.53.79 przy użyciu przeglądarki Internet Explorer w wersji 5.01.



Rys. 10. Agresywna strona www, połączenie z wykorzystaniem serwera HTTPS

Po połączeniu z tą samą stroną umieszczoną na serwerze HTTPS (rys. 10), z komputera 9lk08 i uruchomieniu łącza atak wykonał się pomyślnie, o czym świadczy pojawienie się okna ustawień programu Netbus Pro Server na ekranie atakowanego komputera (rys. 11).



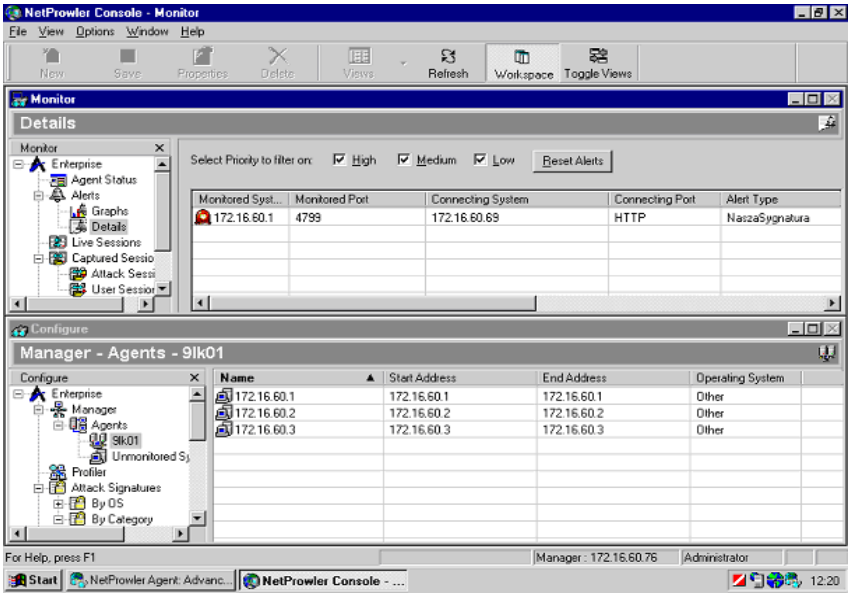
Rys. 11. Efekt ataku przeprowadzonego wykorzystaniem serwera HTTPS

6.3. Raport z ataku na firewall bez tunelowania

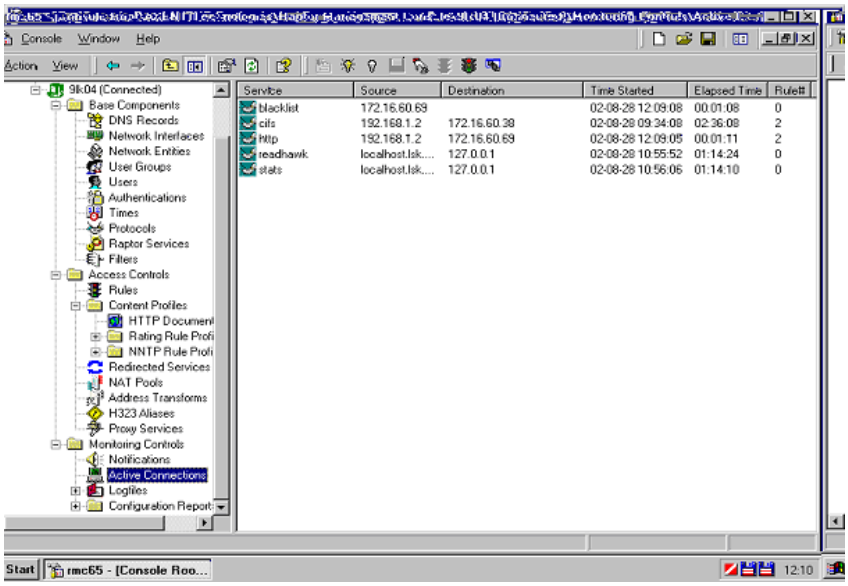
W przebiegu tego badania wykorzystano zaporę sieciową Firewall Raptor, którą uruchomiono na komputerze 9lk04 i sensor NetProwler działający na komputerze 9lk014. Przed badaniem dokonano sprzężenia firewalla i sensora zgodnie z [19], [20] i [23]. Dokonano połączenia w protokole HTTP z komputera 9lk08 (ofiary) z serwerem Apache, znajdującym się na komputerze 9lk09. Po wyświetleniu strony uruchomiono łącze umieszczone na stronie agresywnej (por. rys. 10).

Atak się nie powiódł, NetProwler zasygnalizował pojawienie się zagrożenia i powiadomił o tym zaporę sieciową (por. rys. 12).

Oba urządzenia zareagowały prawidłowo, zapora wygenerowała listę zabronionych adresów sieciowych (por. rys. 13) i połączenie z serwerem Apache zostało zablokowane.



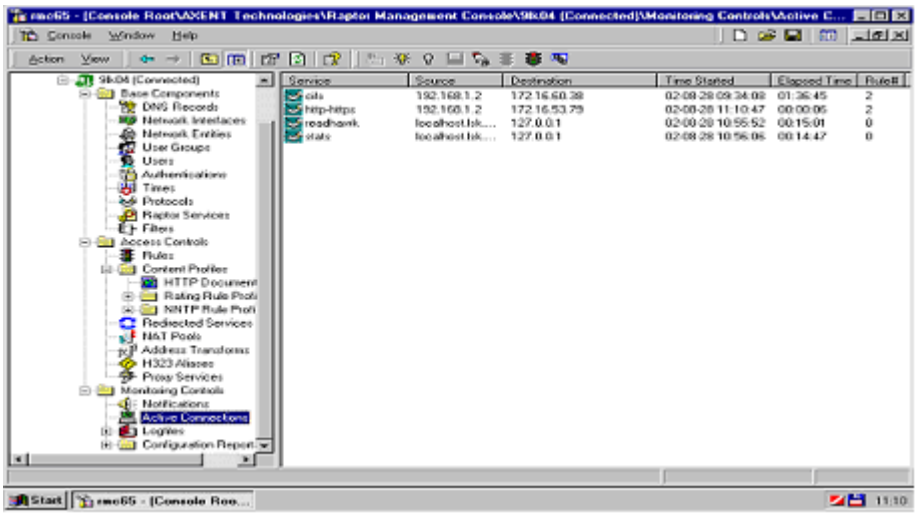
Rys. 12. Reakcja NetProwlera na atak



Rys. 13. Reakcja firewalla na atak

6.4. Raport z ataku wykorzystującego tunel kryptograficzny przez firewall

W przebiegu tego badania wykorzystano zaporę sieciową Firewall Raptor, którą uruchomiono na komputerze 9lk04 i sensor NetProwler działający na komputerze 9lk014. Przed badaniem dokonano sprzężenia firewalla i sensora zgodnie z [19], [20] i [23].



Rys. 14. Reakcja firewalla na atak , połączenie https

Po połączeniu komputera o nazwie 9lk08 z serwerem HTTPS znajdującym się na komputerze o numerze IP 172.16.53.79 na którym znajdowała się agresywna strona WWW uruchomiono znajdujące się na tej stronie łącze. Atak wykonał się prawidłowo. Zapora sieciowa odnotowała jedynie połączenie z serwerem HTTPS (por. rys 14). Sensor nie był jednak w stanie poprawnie rozpoznać zaszyfrowanej zawartości pakietów.

7. Podsumowanie wyników

Przeprowadzony atak był atakiem wielopakietowym i ten fakt w przypadku opisanym w 6.3 (bez tunelowania) pozwalał sensorowi odszukać sygnatury w pierwszym pakiecie ataku i zablokować sesję, jak również powiadomić zaporę sieciową. Kolejne pakiety ataku już nie przedostały się do

sieci chronionej, co zapobiegło powodzeniu ataku. W tym przypadku do sieci chronionej przedostało się 30 pakietów, co stanowi 4% pliku demo.eml. W przypadku tunelowania sensor nie jest w stanie analizować pakietów i atak kończy się powodzeniem – wszystkie pakiety przedostają się przez zaporę.

Wykaz dokumentów związanych:

[11] Opis źródłowy podatności (w pliku opispodatności.doc).

[12] Raport automatyczny z konfiguracji stacji roboczej 9LK01.(w pliku 9lk01Sandra.doc).

[13] Raport automatyczny z konfiguracji stacji roboczej 9LK04.(w pliku 9lk04Sandra.doc).

[14] Raport automatyczny z konfiguracji stacji roboczej 9LK08.(w pliku 9lk08Sandra.doc).

[15] Tworzenie nowej sygnatury IDS NetProwler (znajduje się w pliku tworzniewlasnejsyg.doc).

[16] Wykaz inwentaryzacyjny użytych elementów sieci.

[17] Plan sieci testowej (w pliku plansiecitestowej.doc).

[18] Reference Guide. Raptor Firewall and PowerVPN V6.5. AXENT Technologies, Inc. Rockville, 2000. (w pakiecie dystrybucyjnym w pliku RefGuideNT65.pdf).

[19] Site Preparation and Instalation Guide for NT. Raptor Firewall and PowerVPN V6.5. AXENT Technologies, Inc. Rockville, 2000.
(w pakiecie dystrybucyjnym w pliku InstalGuideNT65.pdf).

[20] Configuration Guide for NT. Raptor Firewall and PowerVPN V6.5. AXENT Technologies, Inc. Rockville, 2000. (w pakiecie dystrybucyjnym w pliku ConfigGuideNT65.pdf).

[21] User's Guide. NetProwler™ Versions 3.5 and 3.5.1. AXENT Technologies, Inc. 2000. (w pakiecie dystrybucyjnym w pliku NP35user.pdf).

[22] Release Notes NetProwler™ Versions 3.5 and 3.5.1 GA Release. AXENT Technologies, Inc. 2000. (w pakiecie dystrybucyjnym w pliku NP35ReleaseNotes.pdf).

[23] Getting Started. NetProwler™ Versions 3.5 and 3.5.1. AXENT Techn.logies, Inc. 2000. (w pakiecie dystrybucyjnym w pliku GetStart.pdf).

[24] Kod źródłowy strony www (w pliku zrodlo.doc).

[25] Plik demo.eml z katalogu www serwera Apache.

[26] Plik Microsoft Security Bulletin (MS01-020).htm

DODATEK 3.

Możliwości przenikania firewalla IP Filter atakiem oprogramowania typu spyware przez tunel kryptograficzny SSH

PROTOKÓŁ BADANIA nr 02/09/02

1. Dane ogólne

Data: 11.09.2002 r.

Miejsce badania: Instytut Automatyki i Robotyki Wydziału Cybernetyki WAT.

Wykonawcy: Fryderyk Wróbel, Adam Pałasz, Maciej Rychter, Radosław Ryński.

2. Badany firewall

W badaniach wykorzystano jako podstawowy obiekt badań Ip Filter sprzężony z systemem wykrywania włamań Snort. Oba produkty zostały pozyskane z Internetu w ramach licencji OpenSource. Ip Filter pozyskany w postaci źródeł z witryny http://coombs.anu.edu.au/~avalon/, zaś Snort z http://www.snort.org. Dokumentacja do firewalla znajduje się na [27]. Dokumentacja do systemu operacyjnego na którym został uruchomiony Ip Filter znajduje się pod adresem: http://www.freebsd.org Istotne pliki konfiguracyjne systemu FreeBSD 4.4 to [29] i [30].

2.1. Identyfikatory oprogramowania firewalla

Product Type: Ip Filter
Platform: FreeBSD 4.4
Version: 3.4.28
License Information: Open Source

2.2. Identyfikatory pakietu dystrybucyjnego

Ip Filter został pozyskany w postaci plików źródłowych z Internetu, bez szczególnych cech identyfikacyjnych.
Licencja: Open Source.

2.3. Wybrane cechy firewalla

Przedstawione poniżej cechy firewala IP FILTER zostały wybrane ze względu na rolę tego oprogramowania w badaniach. Firewall:

- filtruje pakiety w warstwie trzeciej i czwartej siedmiowarstwowego modelu ISO/OSI, na podstawie analizy nagłówka pakietu DoD IP oraz nagłówków ramek TCP/UDP,
- realizuje funkcję translacji adresów sieciowych (NAT – Network Address Translation), która umożliwia ukrycie wewnętrznych adresów sieci chronionej.

W skład firewalla wchodzą następujące narzędzia:

- **ipf** – narzędzie do zarządzania listą reguł polityki bezpieczeństwa. Odczytuje reguły z pliku bądź ze standardowego wejścia I umieszcza je na liście przetwarzania filtra;
- **ipfstat** – zbiera statystyki związane z przetwarzaniem pakietów przez filtr;
- **ipftest** – odczytuje reguły z pliku reguł I generuje odpowiednie pakiety testujące odczytane reguły;
- **ipmon** – czyta buforowane dane z urządzenia logowanie (domyślnie */dev/ipl*) i wysyła je:
  - na ekran (standardowe wyjście);
  - do pliku;
  - do syslog;
- **ipsend** – generuje dowolne pakiety i wysyła je do określonego hosta;
- **ipresend** – wczytuje dane z pliku zachowanych pakietów i wysyła je z powrotem w sieć;
- **iptest** – generuje niekonwencjonalne pakiety do testowania firewalla;
- **ipnat** - narzędzie do zarządzania listą reguł translacji adresów.

Plik z konfiguracją reguły firewalla znajduje się w [31], natomiast plik z konfiguracją reguł translacji adresów znajduje się w [32].

2.4. Identyfikatory oprogramowania sensora

Jako sensora użyto pakietu Snort 1.8.6 FlexResp. Został on pobrany z witryny internetowej http://www.snort.org w postaci źródeł i skompilowany na platformie docelowej. Snort jest udostępniany w ramach licencji Open Source.

2.5. Wybrane cechy sensora

Snort monitoruje ruch w sieci poprzez analizę wszystkich przychodzących pakietów w dostępnym segmencie sieci. Pakiety porównuje z sygnaturami predefiniowanymi przez producenta oraz utworzonymi przez użytkownika. Sensor udostępnia możliwości automatycznej reakcji, min: przerywanie połączenia, raportowanie oraz alarmowanie. W celu „utwardzenia" czyli umocnienia ściany ogniowej (powiadomienie zapory o wybranych cechach napastnika (zwykle przez podanie adresu IP)).

Snort udostępnia trzy tryby, w których może być uruchamiany:
sniffer mode – analizuje ruch w sieci a odebrane pakiety wyświetla na ekran (konsolę);
packet logger mode – odebrane pakiety zapisuje na dysk w postaci logów;
network intrusion detection mode – pozwala na określenie odpowiedniej reakcji na przychodzący pakiet według zadanych wcześniej reguł.

3. Środowisko badania – konfiguracja sieci testowej

Plan sieci testowej znajduje się w [17]. Wykaz poszczególnych elementów sieci testowej ujęto w [16].

4. Badana technika ataku

4.1. Atakowane systemy

Do przeprowadzenia ataku na stacji roboczej ofiary musi zostać zainstalowany i działać program pozwalający na przejęcie zdalnego sterowania stacją, zapewne skrycie instalowany; w opisywanym badaniu użyto oprogramowania NetBus (tzw. koń trojański) w wersji 1.7; ogólnie rzecz biorąc na komputerze atakowanym osadzony jest serwer usługi zdalnego sterowania.

Na pewnym komputerze w sieci lokalnej powinien znajdować się osiągalny z sieci zewnętrznej (spoza firewalla) program pozwalający na

utworzenie tunelu kryptograficznego oraz tzw. „*port forwarding*”; w opisywanym badaniu użyto SSH w wersji 2.4 (build 163).

Wykorzystywana w przeprowadzonym ataku podatność polega na obecności serwera zdalnego sterowania na komputerze ofiary.

4.2. Sposób przeprowadzenia ataku

W celu przeprowadzenia ataku należy zainstalować odpowiednie oprogramowanie:

na komputerze-hoście – klienta programu NetBus oraz klienta SSH,

na komputerze-ofierze – serwer programu NetBus,

na wybranym komputerze-pośredniku – serwer SSH z możliwością tunelowania.

Przeprowadzenie ataku polega na połączeniu z komputera znajdującego się w sieci zewnętrznej tunelem kryptograficznym przez firewall z komputerem-pośrednikiem zlokalizowanym w tej samej sieci wewnętrznej co komputer-ofiara, a stamtąd, przez port forwarding do komputera-ofiary. Zakłada się, że funkcja network address translation firewalla uniemożliwia wywołanie przez klienta z zewnątrz serwera jakiejkolwiek usługi na komputerze ofiary; niemożliwy jest kontakt z zewnątrz sieci lokalnej z komputerami wewnątrz sieci na porty właściwe oprogramowaniu spyware; sensory IDS są w stanie wykryć sygnatury komunikacji spyware.

4.3. Sukces ataku

Udane ustanowienie połączenia z serwerem NetBus na komputerze ofiary jest równoznaczne z udanym przeprowadzeniem ataku, co jest sygnalizowane przez klienta NetBus stosownym komunikatem:

Connected to *nr_ip_komputera_ofiary* – w przypadku połączenia się z komputerem ofiary (udanego ataku);

No connection – w przypadku braku możliwości ustanowienia połączenia z komputerem ofiary (braku sukcesu ataku).

Ustanowienie połączenia komputera atakującego z serwerem NetBus komputera-ofiary jest warunkiem wystarczającym do zakwalifikowania tej akcji jako udanego ataku. Po udanym połączeniu z serwerem NetBus atakujący ma możliwość przejęcia zdalnego sterowania zaatakowanym komputerem.

5. Wykorzystywane reguły blokujące

Dla zablokowania ataku połączenia z serwerem usługi zdalnego sterowania całkowicie wystarczy jedna z trzech własności firewalla:

włączona funkcja *NAT* *(network address treanslation)* bez stałego odwzorowania adresu komputera-ofiary w adres w sieci zewnętrznej (ta własność uniemożliwia połączenie do serwera usługi zdalnego sterowania z zewnątrz sieci);

zablokowane połączenia z zewnątrz do komputerów w sieci wewnętrznej na porty właściwe oprogramowaniu szpiegowskiemu;

ustawienie w IDS (*Intruder Detection Systems*) stanowiącym zewnętrzne rozszerzenie (sensor) firewalla **reguł wykrywania** (sygnatur) charakterystycznych dla komunikacji z serwerem NetBus.

W trakcie przeprowadzonych badań na firewallu nie zostały ustawione żadne szczególne reguły blokujące, ruch pakietów w obie strony odbywał się bez ograniczeń. Plik zawierający reguły przetwarzania (/etc/pass.all) firewalla zawierał następujące wpisy:

```
pass in all
pass out all
```

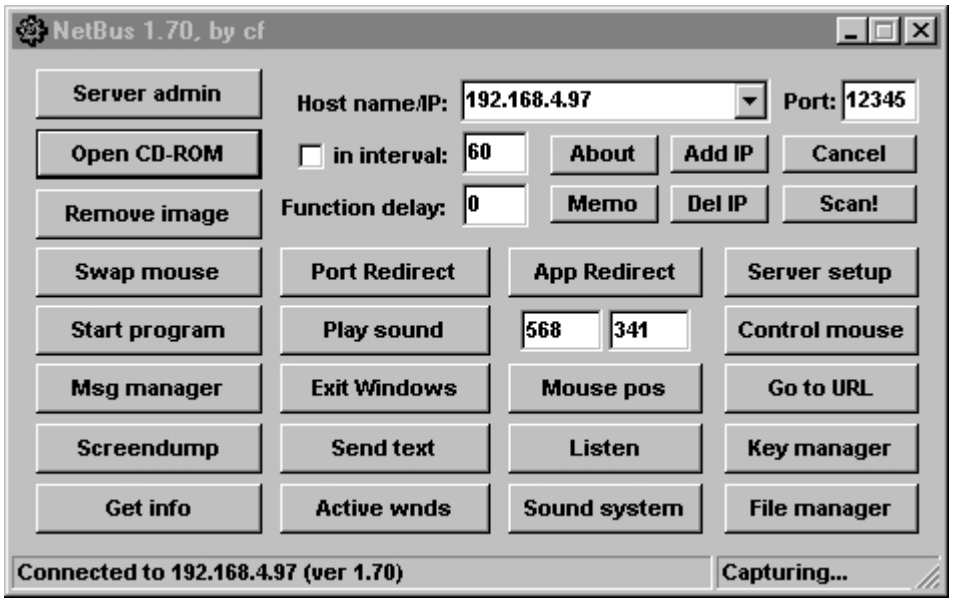
Firewall zapewniał jednoznaczne odwzorowanie wewnętrznego adresu IP komputera-pośrednika w adres zewnętrzny. W badaniu wykorzystywana była tylko zdolność połączenia z komputera z zewnątrz (spoza firewalla) z serwerem SSH (na port 22) uruchomionym na komputerze-pośredniku.

6. Przebieg badania

Badania przeprowadzono w sieci testowej [17]. Przeprowadzenie ataku polegało na ustanowieniu połączenia między komputerem znajdującym się w sieci zewnętrznej tunelem kryptograficznym przez firewall z komputerem-pośrednikiem znajdującym się w tej samej sieci wewnętrznej, co komputer-ofiara, a stamtąd do komputera-ofiary. Żadne pakiety nie były przesyłane między komputerami napastnika i ofiary z pominięciem komputera pośredniczącego. Wszystkie pakiety na tej trasie biegły zaszyfrowane w tunelu SSH niepodatne na analizę firewalla, również adresacja tych pakietów (w nagłówkach IP) była zmieniona: adresowane były one do komputera-pośrednika, na port 22 (SSH) i przekierowywane przez funkcję *port forwarding* serwera SSH. Te własności ruchu pakietów można z łatwością obserwować za pomocą snifferów włączonych w sieci wewnętrznej i zewnętrznej.

Trzeba podkreślić, że jedyny atak, jaki został przez przeprowadzony, odbył się od razu przez tunel kryptograficzny przechodzący przez firewalla z włączonym programem Snort stanowiącym zewnętrzny sensor firewalla (pominięto dokumentowane ataki wzorcowe zalecane przez procedurę badawczą).

Atak ten zakończył się pełnym sukcesem – udało się ustanowić połączenie z atakowanym komputerem, co objawiło się stosownym komunikatem klienta NetBus.



Rys. 155. Pomyślne nawiązanie połączenia (efekt ataku)

Dodatkowo przeprowadzono test wybranych funkcji oprogramowania spyware (m.in. wysunięto podajnik napędu CD-ROM komputera-ofiary, wysłano komunikat na ekran). Wszystkie funkcje działały poprawnie, co oznaczało, że firewall nie wykrywał ataku w (przechodzących przez firewall) pakietach wysyłanych z komputera atakującego do komputera ofiary.

7. Podsumowanie wyników

Przeprowadzony atak przez tunel kryptograficzny powiódł się, co jest wynikiem spodziewanym zważając na fakt, iż specyficzne dla tego programu

sygnatury zawarte w przesyłanych pakietach zostały zaszyfrowane. Skutkiem tego jest niewrażliwość firewalla na badany rodzaj ataku. Można stwierdzić, że atak ten jest praktycznie nie do wykrycia tradycyjnymi sposobami wyszukiwania sygnatur w pakietach podejrzanych przenoszenie ataku. Sposobem na zmniejszenie tej wrażliwości może być zastosowanie wyspecjalizowanego oprogramowania deszyfrującego pakiety przechodzące tunelem SSH i bieżące sprawdzanie ich zawartości przy przechodzeniu przez firewall.

Wykaz dokumentów związanych:

[27] Dokumentacja i przewodnik konfiguracji firewalla Ip Filter – w pliku ip_filter.doc lub w internecie pod adresem:

[28] http://mr0vka.eu.org/docs/tlumaczenia/ipf/ipf.html

[29] Plik konfiguracyjny jądra systemu (KAZIK)

[30] Plik konfiguracyjny uruchamiania systemu (rc.conf)

[31] Plik konfiguracyjny reguł firewalla Ip Filter (ipf.conf)

[32] Plik konfiguracyjny reguł translacji adresów (ipnat.conf)

[33] Plan sieci testowej (w pliku plansiecitestowej.doc).

[34] Wykaz inwentaryzacyjny użytych elementów sieci.

[35] Raport automatyczny Sisoft Sandra komputera 9lk03 (9lk03Sandra.doc)

[36] Raport automatyczny Sisoft Sandra komputera 9lk10 (9lk10Sandra.doc)

Recenzent: prof. dr hab. inż. Włodzimierz Kwiatkowski

Praca wpłynęła do redakcji 21.10.2002