Wydział Fizyki i Informatyki Stosowanej

Praca inżynierska

Marcin Fabrykowski

kierunek studiów: **informatyka stosowana**

System IPS oparty o iptables

Opiekun: **dr inż. Krzysztof Rzecki**

Kraków, styczeń 2013

Oświadczam, świadomy(-a) odpowiedzialności karnej za poświadczenie nieprawdy, że niniejszą pracę dyplomową wykonałem(-am) osobiście i samodzielnie i nie korzystałem(-am) ze źródeł innych niż wymienione w pracy.

.....
(czytelny podpis)

Na kolejnych dwóch stronach proszę dołączyć kolejno recenzje pracy popełnione przez Opiekuna oraz Recenzenta (wydrukowane z systemu MISIO i podpisane przez odpowiednio Opiekuna i Recenzenta pracy). Papierową wersję pracy (zawierającą podpisane recenzje) proszę złożyć w dziekanacie celem rejestracji.

Spis treści

Wstęp

Rozdział 1

Opis problemu

Nazwa rozdziału do zmiany. Czekam na propozycje :P

1.1 O IPS

1.1.1 Co to jest IPS

System IPS (ang. Intrusion Prevention System) jest to system wykrywania i blokowania ataków sieciowych. Jego zadanie polega na analizie ruchu sieciowego wchodzącego do oraz przechodzącego przez niego oraz odpowiednie reagowanie w przypadku wykrycia nienormalnych zachowań sieci.

1.1.2 Schemat działania

1. Analiza ruchu sieciowego
2. Wykrycie zachowań pasujących do zdefiniowanych reguł bezpieczeństwa
3. Reakcja na wykryte niebezpieczne zachowanie
4. Poinformowanie administratora o próbie ataku oraz podjętych działaniach
5. Zapisanie danych o ataku oraz podjętych działaniach do bazy danych
6. Udostępnienie administratorowi wglądu w historię ataków

1.2 Analiza ruchu sieciowego

1.2.1 Używane narzędzie

Jako systemu analizującego ruch sieciowy wykorzystam pakiet Netfilter konfigurowany za pomocą iptables.

1.2.2 Netfilter

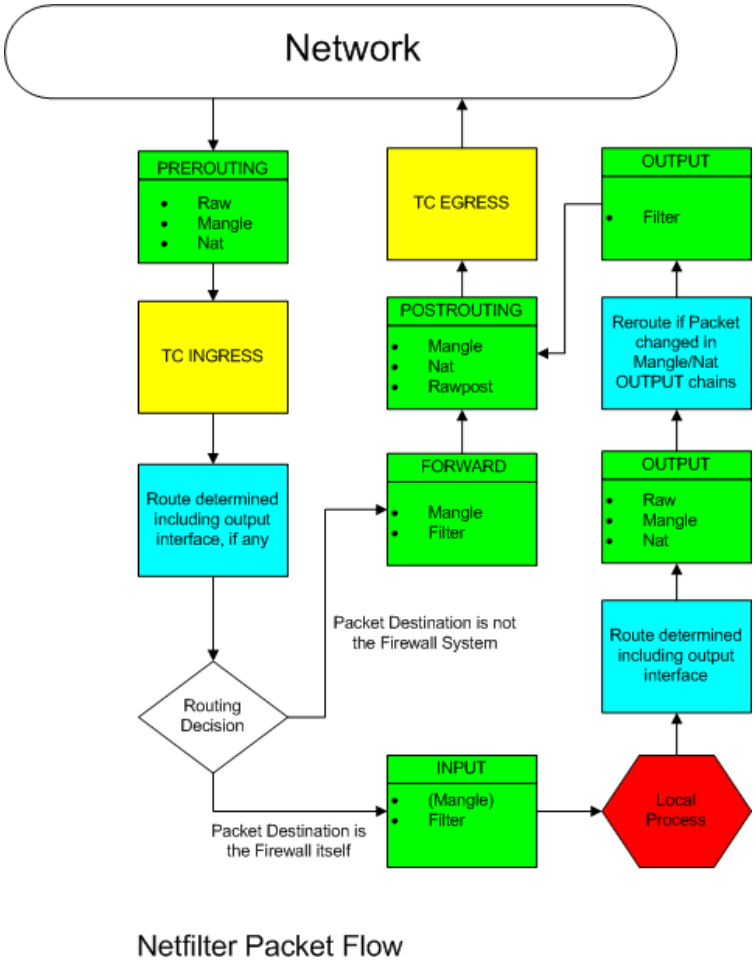
1.2.2.1 Ogólny zarys

Netfilter jest oprogramowaniem pozwalającym na filtrowanie pakietów, ich translacje (NAT) oraz inne manipulację. Od wersji jądra 2.4.x, pakiet netfilter jest umieszczony wewnątrz niego. Potrafi on dopasowywać analizowane pakiety ze względu na szeroką gamę kryteriów, jak również przeprowadzić szereg operacji na danych pakietach.

1.2.2.2 Zasada działania

Netfilter posiada 4 zdefiniowane tablice: raw, mangle, nat, filter, oraz 5 łańcuchów: PREROUTING, INPUT, FORWARD, OUTPUT, POSTROUTING. Kolejność przechodzenia pakietu przez tabele i łańcuchy obrazuje rys. 1.1.
Gdy pakiet dochodzi do komputera na którym jest netfilter, zostaje on przekazany do łańcucha PREROUTING. Następnie, następuje decyzja o routowaniu pakietu, i w zależności czy pakiet jest kierowany do lokalnego komputera, jest kierowany do łańcucha INPUT, bądź w przypadku gdy ma zostać przekazany dalej, do łańcucha FORWARD oraz POSTROUTING.
W przypadku, gdy pakiet jest generowany przez nasz komputer, zostaje on przejęty przez łańcuch OUTPUT, a następnie POSTROUTING.

Pierwszą tablicą przez którą przechodzi pakiet, jest tablica *raw*. W tym miejscu możemy oznaczyć pakiet targetem TRACE, który spowoduje logowanie każdej reguły do której pakiet będzie pasował. Wykorzystywane jest to przy debugowaniu sieci bądź firewalla. Inna opcją która może pojawić się jedynie w tablicy raw, jest



Rysunek 1.1: Przepływ pakietów w netfilter

target NOTRACK. Spowoduje on nieoznaczenie pakietu przez moduł *conntrack*, który rejestruje pakiety i rozpoznaje je jako istniejące połączenia.

Następna tablicą do której zostaje przekazany pakiet, jest tablica *mangle*. W tablicy tej możemy manipulować wartościami TTL.

Kolejną tablicą przetwarzającą pakiet, jest tablica *nat*. W tablicy tej możemy manipulować adresami pakietowymi. W zależności, czy naszym celem jest SNAT cz DNAT, używamy do tego odpowiednich łańcuchów PREROUTING i POSTROUTING

Ostatnią tablicą, która przetwarza pakiety, jest tablica *filter*. Jest to tablica

w której powinno się umieszczać wszystkie reguły dotyczące filtrowania pakietów. Jeżeli nie zostanie jawnie podana tablica, domyślną tablicą jest tablica *filter*.

Jeżeli pakiet zostanie przetworzony przez całą ścieżkę w firewallu i nie zostanie podjęta decyzja o zaakceptowaniu bądź odrzuceniu pakietu, zostaje zastosowana polityka odpowiedniego dla tego pakietu łańcucha głównego, tj. INPUT, OUTPUT, FORWARD. Politykami mogą być TARGET-y terminujące, tj. ACCEPT, REJECT, DROP.

1.2.2.3 Najważniejsze kryteria dopasowania

Netfilter posiada bogaty wachlarz możliwości dopasowywania pakietów

--source, --src, -s *<adres>*
dopasowuje adres źródłowy pakietu do podanego jako *adres*

--destination, --dst, -d *<adres>*
dopasowuje adres docelowy pakietu do podanego jako *adres*

--protocol, -p *<protocol >*
dopasowuje protokół używany przez pakiet.
Najczęściej używane protokołu to: *tcp*,*udp*,*icmp*

--source-port, --sport *<port >*
dopasowuje port źródłowy pakietu.
Aby użyć tego dopasowania należy zdefiniować protokół.

--destination-port, --dport *<port >*
dopasowuje port docelowy pakietu.
Aby użyć tego dopasowania należy zdefiniować protokół.

--tcp-flags *<maska ><flagi >*
DO POPRAWY STYLISTYCZNEJ
dopasowuje pakiet, jeżeli wszystkie *flagi* są ustawione, oraz wszystkie flagi wymienione w *masce* oraz niewymienione w *flags* są nieustawione

--mac-source *<mac-adres >*

dopasowuje pakiet na podstawie źródłowego adresu sieciowego. Adres podawany jest w formacie: AA:BB:CC:DD:EE:FF.

--in-interface, -i *<interface>*

dopasowuje pakiet ze względu na interface sieciowy na którym dany pakiet się pojawił

--out-interface, -o *<interface>*

dopasowuje pakiet ze względu na interface sieciowy przez który pakiet będzie wysyłany

--limit *<ilość>/<czas>*

dopasowuje pakiety, jeśli ich ilość nie przekracza *ilość* w okresie *czas*.
Czas może przyjmować wartości: second, minute, hour, day.

1.2.2.4 Najważniejsze działania

Jeżeli pakiet zostanie dopasowany, netfilter może wykonać jedną ze zdefiniowanych akcji a pakiecie. W przypadku niezdefiniowania akcji, pakiet przechodzi do kolejnych reguł w firewallu a w firewallu zostaje zwiększony licznik dopasowanych pakietów dla danej reguły.
Dopasowany pakiet zostaje wysłany do wybranego targetu poprzez opcję -j, np: -j ACCEPT.

ACCEPT

dany pakiet zostaje zaakceptowany i nie przechodzi przez dalszą filtrację

REJECT

odrzucenie pakietu z wysłaniem informacji do adresata. Domyślna wartość odpowiedzi to icmp-port-unreachable.
Istnieje możliwość ustawienia odpowiedzi wysyłanej do adresata poprzez atrybut --reject-with *<type>*, gdzie *type* jest jednym z zdefiniowanych komunikatów:

- icmp-net-unreachable
- icmp-host-unreachable
- icmp-port-unreachable
- icmp-prot-unreachable
- icmp-net-prohibited
- icmp-host-prohibited
- icmp-admin-prohibited.

DROP

odrzucenie pakietu, bez wysyłani informacji zwrotnej do adresata. Pakiet zostaje "upuszczony".

LOG

pakiet zostaje wysłany do systemu logowania jądra. Jest to nieterminatorowy target, to znaczy, że po dopasowaniu pakietu, zostaje on zalogowany, a następnie przechodzi przez dalszą część firewalla.
Najczęściej jest on stosowany wraz z opcją --log-prefix, który dodaje prefix w systemie logowania. Pozwala on na późniejsze odróżnienie poszczególnych logów od siebie.

TTL

pozwala na manipulację wartościami TTL. Zalecane jest niezmienianie tej wartości, jednak w praktyce, są sytuacje w których zmiana wartości TTL jest potrzebna.
Możliwe opcje przekazywane do tego targetu:

--ttl-set *<wartość>*

ustawia wartość ttl na podaną

--ttl-inc *<wartość>*

zwiększa wartość ttl o podaną wartość

--ttl-dec *<wartość>*

zmniejsza wartość ttl o podaną wartość

REDIRECT

target ten przekierowuje pakiet na siebie. Istnieje również możliwość możliwość zmiany portu w danym pakiecie poprzez opcję: --to-ports *<port>*. Aby użyć opcji --to-ports, należy określić protokół -p *<protokół>*

SNAT

pozwala zmienić adres źródłowy dopasowanego pakietu. Określenie nowego adresu źródłowego dokonujemy za pomocą opji:
--to-source *<adres>* [:*port*[-*port*]]
gdzie *port* jest opcjonalnym parametrem określającym port, bądź zakres portów. Aby zdefiniować port(y) należy zdefiniować protokół.

DNAT

pozwala zmienić adres docelowy oraz port dopasowanego pakietu. Określenie nowego adresu docelowego dokonujemy za pomocą opji:
--to-source *<adres>* [:*port*]
Aby móc zdefiniować port, należy określić protokół.

1.2.3 Iptables

1.2.3.1 Zarys ogólny

Iptables jest konsolowym interfejsem dla netfilter-a. Pozwala on na tworzenie łańcuchów, dodawanie oraz usuwanie reguł, oraz wyświetlanie statystyk. Często nazwa iptables używana jest wymiennie z netfilter. Wynika to z faktu braku innych interfejsów do obsługi netfilter.

1.2.3.2 Polecenia iptables

Najczęściej wykorzystywane polecenia iptables to:

-t *<tablica>*

opcjonalny parametr, który możemy przekazać do każdej poniżej opisanej opcji, definiujący tablicę na której będziemy wykonywać operacje. Jeżeli ten parametr nie zostanie zdefiniowany, domyślną tablicą jest tablica *filter*.

-A *<łańcuch> <reguła>*

dodawanie nowej reguły na koniec łańcucha.

-I *<łańcuch>* **[nr]** *<reguła>*

wstawienie nowej reguły do łańcucha. Jeżeli zostanie podany parametr *nr*, reguła zostaje wstawiona na pozycję *nr*. Jeżeli parametr nie zostanie podany, domyślną wartością jest 1, czyli początek łańcucha.

-D *<łańcuch> <reguła>*

usuwa z łańcucha regułę podaną przez specyfikację.

-D *<łańcuch> <nr>*

usuwa z łańcucha regułę podaną przez numer porządkowy, liczony od 1.

-N *<łańcuch>*

tworzy nowy łańcuch o nazwie *łańcuch*.

-F [*łańcuch***]**

usuwa wszystkie reguły z zadanego łańcucha. Jeżeli nie zostanie podany łańcuch, wyczyszczone zostaną wszystkie łańcuchy.

-X *<łańcuch>*

usuwa zadany łańcuch. Aby móc usunąć łańcuch, musi on być wcześniej wyczyszczony.

-P *<łańcuch> <polityka>*

ustawia politykę dla łańcucha.

-L [*łańcuch***]**

wypisuje reguły w łańcuchu. Jeżeli wartość *łańcuch* nie zostanie podana, zostają wypisany wszystkie łańcuchy.

Często używane opcje polecenia -L, to:

-n

nie zamienia adresów ip na nazwy domenowe - często przyśpiesza wypisywanie wyników, gdyż nie oczekujemy na odpowiedzi od revdns-a.

-v

tryb gadatliwy. Wypisuje statystyki ilościowe i objętościowe dla wypisywanych reguł