Wstępna specyfikacja systemu IPS

Marcin TORGiren Fabrykowski

10 września 2012

Spis treści

1 Opis problemu

1.1 Co to jest IPS

System IPS (Intrusion Prevention System) jest to system wykrywania i blokowanie ataków sieciowych. Jego zadaniem jest analiza ruchu sieciowego wchodzącego do serwera oraz przechodzącego przez niego, oraz odpowiednie reagowanie w przypadku wykrycia **podejrzanych** zachowań.

1.2 Schemat działania

1. Analiza ruchu sieciowego
2. Wykrycie zachowań pasujących do reguł bezpieczeństwa
3. Reakcja na niebezpieczne zachowanie
4. Poinformowanie administratora o próbie ataku
5. Zapisanie podjętych działań w bazie danych

2 Analiza ruchu sieciowego

2.1 Używane narzędzie

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

2.2 Jak działa iptables

TODO

3 Wykrywanie zagrożeń

3.1 Ataki typu SSH BruteForce

3.1.1 Opis

Atak ten polega na ciągłej próbie połączenia się z usługą SSH z różnymi hasłami.

3.1.2 Obrona

Zastosuję ograniczenie liczby połączeń z usługą SSH w ciągu minuty do 4. Dodatkowo przy liczbie połączeń przekraczającej 10 na godzinę zostanie wygenerowane ostrzeżenie.

3.1.3 Implementacja

TODO

3.2 Ataki typu SYN Flood

3.2.1 Opis

Atak ten jest jednym z ataków DoS i polega na wysyłaniu ciągłej dużej ilości pakietów SYN do atakowanego hosta.

W normalnym przypadku, klient wysyła pakiet SYN do serwera deklarując chęć nawiązania połączenia. Serwer odpowiada pakietem SYN-ACK potwierdzając gotowość do nawiązania połączenia, po czym klient wysyła pakiet ACK, co jest równoznaczne z ustanowieniem połączenia.

W przypadku ataku SYN Flood, atakujący wysyła dużą ilość pakietów SYN. Serwer odpowiada na każde takie żądanie połączenia pakietami SYN-ACK. Jednakże atakujący nie wysyła pakietów ACK. Serwer w oczekiwaniu na odpowiedzi, przechowuje informacje o nawiązywanych połączeniach w tablicy stanów połączeń. Przed usunięciem wpisu z tej tablicy z powodu braku odpowiedzi ACK od klienta, serwer musi odczekać czas ustalony przez TIMEOUT.

Jeżeli pakietów SYN było odpowiednio dużo, mogą one zapełnić całą tablicę połączeń serwera. Spowoduje to, że w przypadku próby nawiązania połączenia przez normalnego użytkownika, jego żądanie zostanie odrzucone z powodu przepełnionej tablicy stanów. W efekcie, serwer przestanie odpowiadać na żądania użytkowników.

3.2.2 Obrona

Aby zabezpieczyć się przed atakami SYN Flood możemy limitować ilość przychodzących pakietów SYN od jednego odbiorcy.

3.2.3 Implementacja

TODO

3.3 Ataki typu ICMP Flood

3.3.1 Opis

Kolejny atak DoS. Wykorzystywany, gdy atakujący ma większe łącze niż ofiara. Polega na wysyłaniu znacznej liczby pakietów ICMP Request. Serwer odpowiadając na każde zapytanie szybko **nasyca** swoje łącze, powodując iż staje się niedostępny dla zwykłych klientów.

3.3.2 Obrona

Obroną na atak ICMP Flood jest limitowanie akceptowanych pakietów ICMP Request w ciągu sekundy.

3.3.3 Implementacja

TODO

3.4 Atak niepoprawnymi pakietami

3.4.1 Opis

Otrzymanie niepoprawnego pakietu, np: zawierającego jednocześnie flagi SYN i FIN, może spowodować nieprzewidywalne zachowanie w niektórych implementacjach obsługi sieci.

3.4.2 Obrona

Ignorowanie wszystkich niepoprawnych pakietów

3.4.3 Implementacja

TODO

3.5 Zbieranie informacji poprzez ICMP Address Mask Request

3.5.1 Opis

ICMP type 17. Pozwala atakującemu na poznanie ustawień sieci. Informacje takie pozwalają na ataki **broadcastowe** oraz ułatwiają **wpięcie** się do sieci.

3.5.2 Obrona

Większość dzisiejszych systemów nie odpowiada na zapytania o maskę sieci, jednak **dla pewności** lepiej zabezpieczyć się przed takim atakiem. Pozwoli to nam również wysłać ostrzeżenie do administratora, że ktoś interesuje się serwerem

3.5.3 Implementacja

TODO

3.6 Zbieranie informacji poprzez ICMP Timestamp Request

3.6.1 Opis

ICMP type 13. Pozwala atakującemu na poznanie dokładnego czasu na serwerze. Może to prowadzić do ataków opartych na liczbach pseudolosowych bazujących na czasie serwera.

3.6.2 Obrona

Ignorowanie żądań typu 13, oraz informacja do administratora.

3.6.3 Implementacja

TODO

3.7 Skanowanie portów metodą SYN

3.7.1 Opis

Skanowanie to polega na wysyłaniu pakietów SYN do skanowanego hosta. Jeżeli port jest otwarty, serwer odpowiada, zgodnie ze standardem, pakietem SYN ACK, na to skaner odpowiada pakietem RST.
Natomiast, jeżeli port jest zamknięty, skanowany host odpowiada pakietem RST ACK.
W przypadku kiedy port jest filtrowany na firewallu, skanowany host nie odsyła żadnej odpowiedzi.
Daje to pełen przegląd stanu portów, co może być bardzo niebezpieczne.

3.7.2 Obrona

Limitowanie ilości akceptowanych pakietów SYN w jednostce czasu. W przypadku wykrycia skanowania, przekazanie informacji do administratora.

3.7.3 Implementacja

TODO

3.8 Skanowanie portów funkcjami systemowymi

3.8.1 Opis

Skanowanie to jest bardzo podobne do poprzedniego, jednak wykorzystuje funkcje systemowe zamiast niskopoziomowych gniazd surowych. W tym przypadku następuje pełne nawiązanie połączenia TCP.

Rozpoznanie stanu portu jest takie samo jak w skanowaniu pakietami SYN: Jeśli udało się nawiązać połączenie, to znaczy, że port jest otwarty, jeżeli otrzymaliśmy RST ACK, to znaczy że port jest zamknięty, a jeżeli brak odpowiedzi, znaczy to że port jest filtrowany

3.8.2 Obrona

Metoda identyczna jak w pakietach SYN, gdyż użycie metod systemowych jest jedynie wydłużoną wersją użycia gniazd surowych i pakietów SYN

3.8.3 Implementacja

TODO

3.9 Skanowanie pakietami ACK

3.9.1 Opis

Polega na wysyłaniu pakietów ACK na poszczególne porty. W przypadku gdy port jest filtrowany, nie zostaje wysłana żadna odpowiedź, natomiast jeżeli port jest **otwarty na firewallu** dostaniemy odpowiedź w postaci pakietu RST niezależnie czy port jest otwarty czy zamknięty.

3.9.2 Obrona

Filtrowanie pakietów ACK mających równocześnie **state NEW**

3.9.3 Implementacja

```
iptables -A INPUT -p tcp -m state --state NEW -tcp-flags ALL ACK -j DROP
```

3.10 IP spoofing z wewnątrz

3.10.1 Opis

Metoda ataku polegająca na podszywaniu się pod innego użytkownika sieci poprzez zmianę adresu IP.

3.10.2 Obrona

Stworzenie bazy MAC -IP, a następnie sprawdzanie za pomocą modułu IPSET obecności pary MAC-IP pakietu w bazie zarejestrowanych stacji roboczych.

3.10.3 Implementacja

TODO

3.11 IP spoofing z zewnątrz

3.11.1 Opis

Metoda polega na wysyłaniu z sieci zewnętrznej pakietów ze zmienionym adresem źródłowym.

3.11.2 Obrona

Blokowanie pakietów pochodzących *z zewnątrz* z adresami źródłowymi należącymi do adresów prywatnych

3.11.3 Implementacja

TODO

3.12 Wirusy

3.12.1 Opis

Jednym z objawów obecności wirusów w naszej sieci jest duża ilość wysyłanych wiadomości z zainfekowanych komputerów. Nie jest to bezpośredni atak na nasz serwer, ale obecność wirusów w sieci może doprowadzić w przyszłości do ataków.

3.12.2 Obrona

Po wykryciu dużej liczby wysłanych maili w krótkim czasie, zainfekowany komputer zostanie odcięty od sieci.
Należy tutaj uważać na sytuację w której użytkownik rzeczywiście wysyła dużą ilość maili - np: wysyłanie CV

3.12.3 Implementacja

TODO

4 Analiza

4.1 Logowanie z iptables

Zapis logowania z iptables do pliku będzie realizowany przy odpowiedniej konfiguracji programu **syslog-ng**.

4.1.1 Konfiguracja syslog-ng

TODO

4.2 Analiza logów

Analiza będzie przeprowadzana w minutowych odstępach. Skrypt będzie analizował wycinek logów z poprzedniej minuty w poszukiwaniu oznak ataku.

W przypadku wykrycia ataku zostanie wysłana wiadomość do administratora o wykrytym ataku oraz dodanie do bazy danych informacji o zajściu.

5 Raportowanie

5.1 Na automatycznie

5.1.1 Alerty

Wysyłane drogą mailową informacje o wystąpieniu próby ataku. Najpóźniej minutę po wystąpieniu zajścia. Analiza logów IPSa co minutę za pomocą CRON-a.

5.1.2 Raport dzienny

Wysyłany drogą mailową raport sporządzany raz dziennie również za pomocą CRON-a. Zawierać będzie informacje o przeprowadzonych atakach, *podejrzanych* zachowaniach oraz podjętych krokach.

5.2 Na żądanie

Za pośrednictwem protokołu HTTP, dostępny będzie interface pozwalający na przeglądanie raportów z konkretnych dni oraz przeglądanie dokładnych logów na których podstawie zostały rozpoznane próby ataków.

System zarządzania raportami zostanie stworzony w Pythonie, przy użyciu frameworku Django.

6 Zapis do bazy danych

6.1 Baza danych

Jako bazy danych będę używał bazy PostreSQL.
Po wstępnym zapoznaniu się z danymi dostępnymi w internecie, uznałem że PostreSQL jest wydajniejszy przy bazach z dużą ilością rekordów oraz porównywalny z MySQL przy mniejszych bazach.

6.2 Struktura logów

Dane jakie będą zapisywane:

- Data i godzina
- Nazwa serwera na którym wystąpiła akcja
- Typ zagrożenia
- Podjęte działania
- Wyciąg z logów pokazujący pakiet powodujący uruchomienie alarmu

Typy zagrożeń będą definiowały poziom niebezpieczeństwa, potrzebę wysyłania wiadomości mailowej
W bazie będą również zapisane dane klientów w naszej podsieci.

6.3 Zapisywanie do bazy

Zapisywanie będzie dokonywane przez skrypty analizujące logi co minutę przy użyciu CRONa.

7 Zarządzanie systemem

Planowany jest również prosty interface webowy do zarządzania systemem. Pozwalać on będzie włączać i wyłączać poszczególne moduły, dodawać nowych klientów do bazy danych - pary MAC-IP, konfigurować limity dla częstotliwości połączeń.

System będzie również napisany w Pythonie i Django.