Systemy wykrywania włamań

1 Wprowadzenie

Systemy wykrywania intruzów(*ang. Intrusion detection systems*) należą do jednych z najmłodszych rozwiązań w arsenale obronnym administratorów systemów. Systemy te maja na celu wspomagać administratorów w wykrywaniu prób naruszeń polityki bezpieczeństwa. Docelowym dążeniem twórców takich rozwiązań jest pełna automatyzacja w procesie wykrywaniu różnego rodzaju nadużyć systemów informatycznych. Naturalnym dążeniem oprócz pełnej automatyzacji wykrywania intruzów jest chęć doposażenia takich systemów w możliwości udaremniania ataków. Systemy IDS dzięki temu przeobrażają się w systemy zapobiegania włamaniom(*ang. Intrusion Prevention Systems*). Takie systemy z natury rzeczy są jeszcze bardziej skomplikowane niż systemy IDS, posiadają możliwość blokowania akcji wykonywanych przez inne programy, np. dynamiczna modyfikacja firewalla i zablokowanie ruchu sieciowego. Dlatego też wymagania stawiane takim programom są bardzo wysokie.

Słowa kluczowe: IDS, IPS, Snort, wykrywanie włamań.

2 Zastosowanie systemów wykrywania włamań

Główną przyczyną stosowania rozwiązań IDS/IPS w środowiskach sieciowych jest wzrastająca liczba różnego rodzaju ataków przeprowadzanych automatycznie np. za pomocą robaków internetowych czy wirusów jak i tych groźniejszych w których intruz aktywnie pracuje nad uzyskaniem nieuprawnionego dostępu do chronionego systemu. Ochrona systemów komputerowych jest kosztowna i czasochłonna. Systemy IDS/IPS w założeniach mają pomóc obniżyć koszty takiej ochrony oraz podnieść jej efektywność poprzez automatyzację analizy zdarzeń, które mogą świadczyć o potencjalnym naruszeniu polityki bezpieczeństwa danej organizacji.

3 System Snort

Przykładem systemu IDS jest program Snort. Obecnie Snort jest uważany za najlepsze tego typu rozwiązanie Open Source. Mimo, że Snort jest darmowy okazał się na tyle dobry, że wiele firm szkoleniowych oferuje płatne profesjonalne kursy uczące zarządzania aplikacją Snort. Również firmy zajmujące się komercyjnie tworzeniem systemów IDS doceniły Snorta i oferują wsparcie dla reguł Snorta w swoich produktach.

3.1 Podstawy

Uruchomienie programu Snort w trybie wykrywania intruzów z plikiem konfiguracyjnym snort.conf. Snort będzie działał jako demon:

```
snort -c snort.conf -D
```

Możliwe jest również uruchomienie programu Snort w trybie sniffera:

```
snort -v -e -i eth0
```

Inny tryb pozwala logować pakiety:

```
snort -l /ścieżka/do/katalogu
```

W przypadku logowania pakietów możliwe jest również logowanie do formatu akceptowanego przez program tcpdump, co jest bardzo dużą zaletą tego programu Snort. Logowanie binarne o którym mowa jest o wiele szybsze i pozwala zastosować Snorta w sieciach o szybkości 100Mbit/s:

```
snort -l /scieżka/do/katalogu -b
```

Tryb wykrywania włamań można uruchomić w następujący sposób:

```
snort -c snort.conf -D
```

Snort posiada jeden plik konfiguracyjny. W domyślnej konfiguracji wystarczy zmienić kilka opcji aby uruchomić program. Plik konfiguracyjny posiada komentarze pomocne przy konfiguracji. Najważniejsze opcje to:

- HOME_NET – definiuje lokalną przestrzeń adresową, ustawić można ja na wartość $eth0_ADDRESS lub jawnie podać adres podsieci wraz z maską postaci /xx
- EXTERNAL_NET – definiuje przestrzeń adresową nie należącą do sieci HOME_NET, można ustawić na any lub podać adres lub adresy sieci.

3.2 Koncepcja preprocesorów

Aby umożliwić użytkownikom łatwe dodawanie nowych funkcjonalności do programu Snort, powstała koncepcja modułów nazywanych preprocesorami. Każdy preprocesor zawiera nową funkcjonalność wraz z możliwościami konfiguracji. Przykładowy preprocesor `portscan` loguje początek i koniec skanowania portów. Skanowanie portów w tym przypadku jest

definiowane jako próby połączeń do więcej niż `p` portów w przeciągu `t` sekund. Preprocesor `portscan` zawiera kilka parametrów:

- adres sieci dla której ma być monitorowane skanowanie portów
- ilość przeskanowanych portów w założonym czasie
- okres w sekundach w którym następuje skanowanie portów
- ścieżka do pliku w którym będą zapisywane informacje o próbach skanowania

Załączenie w snort.conf preprocesora portscan:

```
preprocessor portscan: 20.1.2.0/24 5 7 /var/llog/snort/portscan.log
```

Preprocesor `portscan-ignorehosts` pozwala ignorować niektóre hosty lub całe sieci przed wykrywaniem ich przez preprocesor `portscan`. Dzięki temu możliwe jest ograniczenie podatności preprocesora `portscan` na fałszywe komunikaty o próbach skanowania portów. Załączenie preprocesor portscan-ignorehosts:

```
preprocesor portscan-ignorehosts: 192.168.1.432
```

3.3 Moduły wyjściowe

Dzięki modułom wyjściowym użytkownik ma możliwość określić, gdzie mają trafiać informacje od systemu Snort. Ogólna postać polecenia ładującego moduł wyjściowy wygląda następująco:

```
output <name>: <options> np: output alert_syslog: log_auth
log_alert
```

Moduł `alert_fast` pozwala logować skróconą postać komunikatu bez nagłówka pakietu, który spowodował uaktywnienie reguły tworzącej zapis w logach. Inne dostępne moduły to `alert_full`, `alert_unixsock`, `log_tcpdump`. Możliwe jest również logowanie do bazy danych jak również wyłączenie logowania za pomocą modułu `log_null`.

3.4 Reguły Snorta

To, co stanowi o sile systemu Snort to tryb wykrywania włamań i systemem tworzenia reguł, dzięki którym Snort potrafi wykrywać różnego rodzaju ataki. Język tworzenia reguł Snorta jest dość skomplikowany . Zostaną tutaj zaprezentowane tylko podstawowe elementy niezbędne do wykonania ćwiczeń. Przykład kompletnej reguły:

```
alert tcp any any -> 192.168.1.0/24 111 (content: 00 01 86 a5 ;
msg: mount access ;)
```

Reguła Snorta jest podzielona na dwie logiczne części: część nagłówka i cześć z opcjami. Część nagłówkowa zawiera akcję jaką należy wykonać, rodzaj protokołu, adres ip źródła , port źródłowy oraz adres ip docelowy oraz numer docelowego portu. Możliwe jest równie użycie wieloznacznego słowa any, które symbolizuje dowolny adres ip, dowolny port. Część w nawiasach okrągłych zawiera zestaw opcji użytych dla tej reguły, Każda opcja zakończona jest średnikiem.
Po odebraniu pakietu porównuje nagłówki reguł oraz opcje zawarte w regułach z pakietem. Jeśli nastąpi porównanie wykonywana jest zapisana w regule akcja.
Możliwe do wykonania akcje to:

- alert, generuje alarm i loguje pakiet
- log, tylko loguje pasujący pakiet
- pass, przepuszcza pakiet
- activate, wywołuje alarm i uruchamia dynamiczną regułę
- dynamic, reguła pozostająca w bezczynności aż do momentu aktywacji przez regułę typu activate

3.5 Opcje w regułach programu Snort

Dzięki rozbudowanym i licznym opcjom jest możliwe wykonywanie wielu testów na pakietach. Każda opcja składa się z słowa kluczowego, po nim dwukropka i argumentu dla danej opcji. Przykładowe opcje:

Opcja: `msg: <tekst>;`

Opcja pozwala dodawać tekst do reguł, dzięki temu informacje zapisane w plikach logu są bardziej czytelne.

Opcja `flag:[!|*|+]<FSRPAU0>[,<FSRPAU0>];`

Opcja pozwala analizować nagłówek pakietu pod kątem ustawionych w nim flag:

- `F - FIN`
- `S - SYN`
- `R - RST`
- `P - PSH`
- `A - ACK`
- `U - URG`
- `0 - brak ustawionych flag`
- `+ - dopasuj do danej flagi i opcjonalnie do reszty`
- `* - dopasuj do którejkolwiek z podanych flag`
- `! - dopasuj jeśli podanej flagi nie są ustawione w pakiecie`

Np. `alert tcp any any -> any any (flags:SF;)`

4 Podsumowanie

Program Snort jest zaawansowanym narzędziem IDS/IPS. Istnieje szereg dodatkowych funkcjonalności dla programu Snort ,co sprawia, że jest to rozbudowane narzędzie którym nie łatwo zarządzać. Nauka posługiwania Snortem może zająć trochę czasu ale warto poświęcić

czas na naukę obsługi tego rozwiązania ponieważ może ono pomóc lepiej chronić środowisko sieciowe.

5 Zadania

- Uruchom program Snort w trybie sniffera.
- Uruchom program Snort w trybie logowania pakietów i sprawdź w jaki sposób Snort zapisuje pakiety.
- Uruchom program Snort w trybie wykrywania włamań z preprocesorem skanowania portów. Użyj narzędzia `nmap` do zasymulowania skanowania portów. Sprawdź czy program Snort wykryje działanie programu nmap. Sprawdź zawartość pliku logów.

6 Problemy do dyskusji

- Zapoznaj się z rozwiązaniem Snort_inline.
- Jakie niebezpieczeństwa niesie za sobą używanie programów typu IPS?

7 Bibliografia

- Strona domowa projektu Snort: http://www.snort.org
- Strona domowa projektu nmap: http://insecure.org/nmap
- „100 sposobów na bezpieczeństwo sieci" Andrew Lockhart, Wydawnictwo HELION2004
- Dokumentacja systemowa programu `tcpdump`: `man tcpdump`