Firewall SPI i Filltr Pakietów

Zeroshell, stosując szkielet netfilter-a i linuxowy program sterujący pakietami (iptables) , może być skonfigurowany do działania jako firewall i chronić sieć LAN przed atakami i skanowaniem portów z sieci WAN. Zeroshell może pracować zarówno jako filtr pakietów, tj. filtrować w oparciu o warunki (zasady) ustanowione dla nagłówków pakietów, lub jako SPI (firewall sprzętowy)

Zasady te są zapisane są na listach zwanych „łańcuchami" (INPUT chain, OUTPUT chain, FORWARD chain). Zeroshell według tych zasad nadzoruje pakiety przychodzące (packets input) , wychodzące (packets output) i tranzytowe (packets in transit) . Należy zauważyć, że w tym ostatnim przypadku możliwe jest ustalenie, czy reguła ma być stosowana tylko do pakietów w routingu, tylko do pakietów mostkowanych lub dla jednych i drugich. Aby uczynić sposób konfigurowania zapory bardziej modularnym nowe listy mogą być tworzone w oparciu o listy zdefiniowane wcześniej przez administratora

Zadania jakie można wykonać na pakiecie jeżeli spełnia on określone kryteria:

- **ACCEPT:** pakiet zostaje zaakceptowany przez zaporę;
- **DROP**: pakiet jest odrzucany i nie dociera do miejsca przeznaczenia. Nadawcy nie jest wysyłany komunikat informujący o odrzuceniu pakietu;
- **REJECT**: jak DROP, tylko nadawca otrzyma komunikat ICMP informujący o niedostarczeniu pakietu
- **CHAIN**: w tym przypadku zdefiniowany przez użytkownika „łańcuch" przejmuje kontrolę. Jeśli pakiet nie spełnia kryteriów żadnej reguły z listy („łańcucha"), kontrola wraca do łańcucha wywołującego;
- **RETURN**: kontrola powraca do „łańcucha" wywołującego lub jeżeli RETURN wywołany jest przez ustawione zadanie, zachowanie pakietu jest uzależnione od tego zadania.
- Dla predefiniowanych łańcuchów akcja może przyjąć wartość ACCEPT lub DROP i stosuje się do pakietów, które nie spełniają żadnej reguły. Dla zdefiniowanych „łańcuchów" z tzw. *domyślnej polityki* może zostać ustawione ACCEPT lub DROP i będzie to zastosowane dla pakietów, które nie spełniają żadnej ustalonej reguły.

Kryteria dla typu „packet filter" obejmują:

- **Input:** reprezentuje interfejs sieciowy, z którego pakiet wchodzi do zapory. To może być interfejs Ethernet, VPN, point-to-point, bridge, bond lub standard 802.1Q VLAN stosowany do jednego z w/w interfejsów;
- **Output:** reprezentuje interfejs sieciowy, przy pomocy którego pakiet wychodzi z zapory. Interfejsy mogą być podobne jak w kryterium Input;
- **Source IP:** reprezentuje adres źródłowy IP pakietu. Może on być wyrażony w formie pojedynczego IP, podsieci lub segmentu;
- **Destination IP:** oznacza docelowy adres IP pakietu. Może on być wyrażony w formie pojedynczego IP, podsieci lub segmentu;

- **Fragments**: wskazuje, że dotyczy drugiego lub kolejnego fragmentów pakietu IP;
- **Source MAC**: wskazuje źródłowy MAC adres pakietu;
- **Protocol Matching**: są to filtry na warstwie 4 (transport) w zależności od wybranego protokołu. W szczególności w przypadku protokołu TCP są to: port źródłowy, port docelowy, opcje i flagi połączenia (SYN, ACK, FIN, RST, URG, PSH);
- **Time Matching**: reprezentuje godzinę i dzień tygodnia, w którym stosowany jest filtr;

Kryteria „Stateful Packet Inspection" obejmują:

- **NEW**: jest to pakiet należący do nowego połączenia w warstwie 4;
- **ESTABLISHED**: jest to pakiet należący do już nawiązanego połączenia;
- **RELATED**: jest to pakiet skorelowany z już nawiązanym połączeniem, zwykle jest to ICMP;
- **INVALID**: jest to uszkodzony pakiet;

Należy zauważyć, że wszystkie kryteria mogą zostać zanegowane i że „packet filter criteria" mogą działać jednocześnie jako kryteria SPI, dzięki czemu firewall jest bardzo elastyczny.