Akademia Handlowa Nauk Stosowanych w Radomiu

Bezpieczeństwo systemów komputerowych Laboratorium 3

Radom 2021/2022

1. Cel zadania

Zapory sieciowe to jedne z podstawowych narzędzi do zarządzania ruchem sieciowym. Ich największym atutem jest filtracja ruchu sieciowego oraz częściowa ochrona przed atakami z zewnętrznych sieci. Celem laboratorium jest zapoznanie się z ich możliwościami.

2. Potrzebne narzędzia.

- kompletny zestaw komputerowy
- systemem operacyjnym Windows/Windows Server (minimum 10/2019)
- system Linux (dowolna wersja)

LUB

- kompletny zestaw komputerowy z dowolnym system operacyjnym
- oprogramowanie do wirtualizacji (VMWare, Hyper-B, VirtualBox, kvm)
- systemy Windows jak wykazano wcześniej
- system Linux jak wskazano wcześniej

3. Informacje wstępne

Obecnie każdy system operacyjny, zarówno z rodziny Windows, jak i Unix-like, posiada wbudowaną zaporę sieciową. Pierwotnie natywnie tego typu narzędzie posiadały jedynie systemy Unix-like, które domyślnie zawsze były i są systemami czysto sieciowymi.
W przypadku systemów Unix-like zapora sieciowa została zintegrowana bezpośrednio z jądrem systemu. W przypadku systemów z jądrem Linux jest to iptables. Z kolei w systemach FreeBSD/OpenBSD to pf, ipfw oraz ipfilter. Systemy z rodziny MacOS posiadają zaś aplikację Firewall lub narzędzie linii poleceń znane z FreeBSD – pf.
Windows od wersji XP SP2 także otrzymał usługę zapory sieciowej. Dzięki temu rozwiązaniu system zyskał ochronę przed ewentualnymi atakami i niepożądanym ruchem sieciowym już od piewszego uruchomienia. Przed wspomnianą wersją posiadacze systemów Windows byli zmuszeni do instalacji i konfiguracji aplikacji firm trzecich, często płatnych.
Zapory sieciowe spełniają następujące role:

- Filtrują ruch na podstawie wskazanych reguł wejścia/wyjścia
- Przekierowują pakiety na podstawie określonych reguł do innych części sieci
- Umożliwiają przekierowywanie usług sieciowych z sieci NAT/PAT
- Umożliwiają podstawową obronę przez atakami pojemnościowymi (np. DoS/DDoS)
- Pozwalają kierować/blokować ruch z części/całych podsieci
- Zapobiegają podkładaniu transmisji w ramach niektórych ataków (np. sekwencji TCP)

Powyżej zostały wskazane tylko najważniejsze funkcjonalności zapór. Często działanie zapory systemowej łączy się z działaniem zapory sprzętowej celem lepszej filtracji ruchu. Znane są bowiem przypadki, gdy zapora systemowa mogła zostać zneutralizowana przez szkodliwe oprogramowanie (zainstalowane przez użytkownika). Zapory sprzętowe zaś nadal będą filtrowały ruch pochodzący z sieci zewnętrznych, przez co urządzenie docelowe nadal będzie chronione (chociaż może być już podatne na takie ataki jak człowiek w środku).

4. Przebieg.

Podczas laboratorium należy sprawdzić następujące elementy zapór sieciowych:

- Sposób działania reguł blokujących/zezwalających w wybranych zaporach sieciowych
- Sposób konfiguracji przekierowania danych na inne urządzenie niż docelowe
- Sposób konfiguracji przekierowania danych na inny port docelowy niż port, na który przyszedł pakiet (przekierowanie wewnętrzne)
- Sposób na przerwanie podejrzanego ruchu (przykładowo od klientów wysyłających zbyt dużo podejrzanych pakietów)
- Sposób na podtrzymanie już rozpoczętego ruchu, który może generować dużą ilość ruchu pakietów
- Filtrowanie ruchu na podstawie zawartości danych (filtracja warstwy siódmej)
- Manipulacja ruchem sieciowym w taki sposób, by usługi dostępne w systemie były możliwe do uruchomienia jedynie po stronie localhost. Jaką usługę trzeba w tym wypadku połączyć z zaporą by można było w ten sposób korzystać z zasobów serwera?

Wskazane jest by zadania wykonać na co najmniej dwóch różnych zaporach sieciowych. Jeżeli jakiegoś polecenia nie da się wykonać na wybranej zaporze należy wskazać, dlaczego jest to niemożliwe (ograniczenie oprogramowania, ograniczenie systemu, ograniczenie obu wymienionych itp.).

5. Zakończenie

Rozwiązanie należy przesłać w postaci PDF (NIE MUSI MIEĆ FORMY SPRAWOZDANIA!) zawierający zrzuty ekranowe dokumentujące działanie określonej funkcjonalności i/lub krótki opis wskazanej funkcjonalności (nawet w postaci listowej jakie przynosi korzyści dla bezpieczeństwa) na adres piotr_dobosz@int.pl, w temacie wiadomości zawierając frazę [AHNS_BSK].

6. Dodatki

http://planetatechnika.pl/ASSO/Linux/netfilter.pdf
https://www.howtogeek.com/205108/your-mac%E2%80%99s-firewall-is-off-by-default-do-you-need-to-enable-it/
https://www.maketecheasier.com/how-to-set-up-port-forwarding-windows-10/
https://superuser.com/questions/1365179/advanced-port-redirection-windows-firewall