Bezpieczeństwo systemów informatycznych

SPRAWOZDANIE Z ĆWICZENIA: Zapory sieciowe

Imię Nazwisko: ..... nr albumu: .....

data ćwiczenia: ..... godzina: .....

1. Filtracja pakietów

1.1 Filtrowanie pakietów w systemie Linux (netfilter/iptables)

Pytania przygotowawcze:

Jakim poleceniem można wyświetlić wszystkie obowiązujące reguły zapory bez rozwijania wartości numerycznych (np. adresów) na nazwy i z podaniem numerów porządkowych reguł?

Zweryfikuj działanie powyższej komendy np. w zadaniu 4.

Zadania:

Wprowadź do konfiguracji zapory, przetestuj i zapisz polecenia pozwalające w efekcie:

1. ograniczyć maksymalną wielkość przyjmowanych pakietów ICMP-echo do 1 kB

- usuwać pakiety większe niż 1 kB zwracając komunikat błędu ICMP-net-unreachable

2. wykorzystać moduł pkttype w celu zablokowania przyjęcia pakietów ICMP-echo wysyłanych na adres rozgłoszeniowy. *Wcześniej należy zdjąć blokadę jądra systemu:*

```
sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=0
```

3. utworzyć statystyki odbierania pakietów ICMP-echo (*wykorzystać moduł* recent)

- *gdzie te statystyki są przechowywane*?
- zablokować odbiór pakietów ICMP-echo jeśli ich ilość osiągnie 5 w ostatnich 10 sekundach

4. wykorzystać moduł comment w celu opisania reguł utworzonych w poprzednim zadaniu
5. ograniczyć do 3 na minutę liczbę przyjmowanych pakietów ICMP-echo (*wykorzystać moduł* limit)
6. ograniczyć wychodzące nowo(!)nawiązywane połączenia TCP dla usługi WWW do 2 na minutę

- ograniczyć je do 2 na minutę dla poszczególnych adresów IP serwera z osobna

7. ograniczyć ilość jednocześnie istniejących połączeń TCP dla usługi WWW do 2
8. ograniczyć żądania GET protokołu HTTP do 500 B wielkości i do 3 na minutę

- logować pakiety, które naruszają powyższe wymagania, ale ich nie usuwać
- *jak przejrzeć log*?