Bezpieczeństwo w sieci. Lab 04. Dodatkowe zadania

Marcin Fabrykowski

14 czerwca 2012

1 Blokowanie routerów w sieci

Zwykle nie chcemy, aby w naszej były podłączane routery ani tworzone podsieci. Aby to zrobić skorzystamy z parametru TTL w pakietach, aby stacje klienckie były ostatnimi dla pakietów wchodzących do sieci.

```
/sbin/iptables -t mangle -A FORWARD -d 192.168.0.0/20 -j TTL --ttl-set 1
```

zakładamy tutaj ze naszą siecią wewnętrzną jest 192.168.0.0/20.

2 Po drugiej stronie barykady...

Lecz czasami znajdujemy sie po drugiej strony barykady, i jesteśmy użytkownikiem który chciałby sobie zrobić podsieć, aby ukryć za natem osoby które nie powinny korzystać z sieci.

```
/sbin/iptables -t mangle -A FORWARD -d 172.10.0.0/20 -j TTL --ttl-inc 1
```

Tutaj zakładamy, że 172.10.0.0/20 to nasza podsieć

3 Blokowanie stron

Inna częstą rzeczą, jaką robi administrator to blokowanie poszczególnych stron, np: megaupload.com.
Można wtedy postawić vhosta (we własnym zakresie) z informacją o powodach blokowania danej strony i przekierowywać tam wszystkie zapytania kierowane pierwotnie do blokowanego hosta.

```
iptables -t nat -D PREROUTING -p tcp -d megaupload.com -j DNAT --to 192.168.0.1:8081
```

zakładamy tutaj, że na na 192.168.0.1:8081 jest postawiony nasz vhost z informacją o blokowaniu

4 Gościnny internet

Czasami się zdarza, że udostępniamy internet niezidentyfikowanym osobą łącze. Nie chcemy wtedy, aby mieli pełnowartościowy dostęp, a jedynie do www

```
iptables -A FORWARD -s 192.168.0.0/24 -p tcp ! --dport 80 -j DROP
```

Zakładamy tutaj że 192.168.0.0/24 to nasza localna sieć publiczna.