

Ataki sieciowe – spoofing

- ▶ Komputery znajdujące się w sieci lokalnej z reguły darzone są większym zaufaniem niż pozostałe.
- ▶ Dostęp do niektórych usług oparty jest często na nazwach łączących się komputerów, np. weryfikacji, czy należą do „lokalnej” domeny.
- ▶ W celu znalezienia tłumaczenia nazwa – adres IP używany jest system DNS (mapy „zwykłe” i „odwrotne”).
- ▶ Mapy „odwrotne” związane są z adresami IP i należą do właścicieli odpowiednich klas adresowych.
- ▶ Nie ma sposobu, by powstrzymać kogoś przed rozgłaszaniem fałszywych informacji, na przykład:

```
1.3.0.63.in-addr.arpa.      IN PTR sun1000.pwr.wroc.pl.
```

- ▶ Jak w takim przypadku zachowa się komputer, którego użytkownik dopisał swoje konto i nazwę „sun1000.pwr.wroc.pl” do pliku `~/.rhosts` albo odpowiednich skryptów IRC, dających na podstawie nazwy IP dodatkowe uprawnienia?
- ▶ Jedynym sposobem weryfikacji tej informacji jest sprawdzenie „zwykłej” mapy:

```
sun1000.pwr.wroc.pl      IN A    156.17.1.33
                          IN A    156.17.250.100
```

- ▶ Jeśli adres użyty do tłumaczenia IP-nazwa nie zostanie znaleziony wśród adresów uzyskanych po przetłumaczeniu nazwy na IP – ktoś się bawi w spoofing DNS.