

Imię	Nazwisko

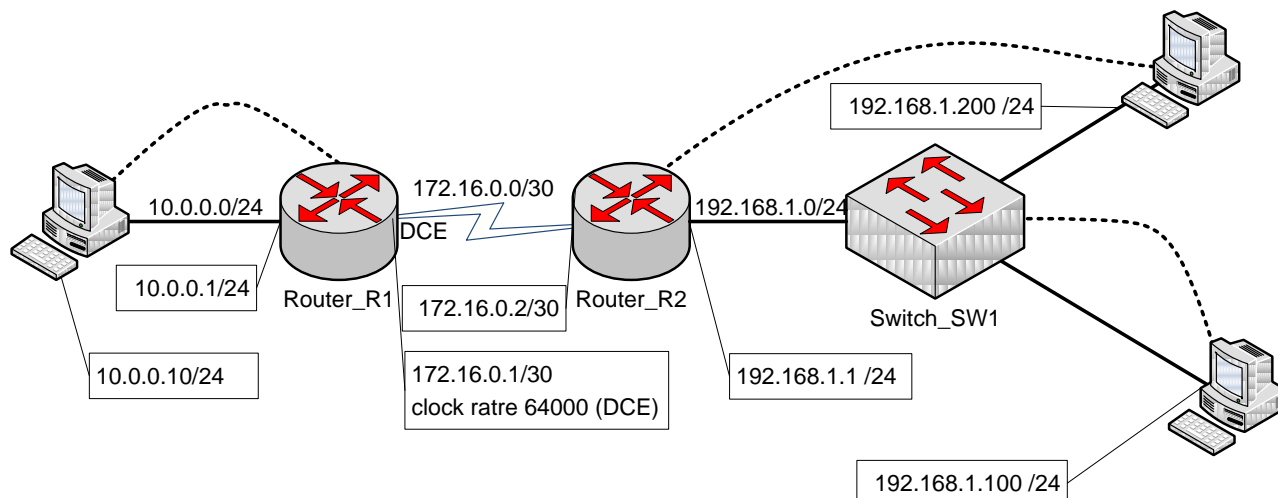
# ZADANIE.02

## Analiza danych w sieci

**Przechwytywanie sesji telnet, analiza sesji SSH,  
podsluchiwanie zapytań WWW, przechwytywanie  
przesyłanych treści, stron**

## 1. Budowa sieci laboratoryjnej

- Zbudować sieć laboratoryjną zgodnie z przedstawioną poniżej topologią i adresacją.



## 2. Środowisko audytu.

- Na komputerze o adresie 192.168.1.100 zainstalować usługę WWW (Apache lub IIS lub inne).
- Na komputerze o adresie 192.168.1.100 zainstalować usługę FTP (dowolny).
- Na komputerze o adresie 192.168.1.200 zainstalować usługę snifera pakietów (Wireshark lub Pakietyzer lub inny).
- Na komputerze o adresie 192.168.1.200 zainstalować NMAP - tryb tekstowy (lub ZENMAP -graficzny).

## 3. Przekierowanie pakietów na przełączniku.

```
SW1(config)# monitor session 1 source interface fastethernet0/1
SW1(config)# monitor session 1 destination interface fastethernet0/6
```

lub

```
SW1(config)# monitor session 1 source vlan 1
SW1(config)# monitor session 1 destination interface fastethernet0/6
```

- Na komputerze o adresie 192.168.1.200 uruchomić snifera pakietów i zebrać ruch pakietów. Zlokalizować adresy IP urządzeń i określić rodzaj ruchu.
- Na komputerze o adresie 192.168.1.200 uruchomić NMAP - przetestować otwarte porty na hoście 10.0.0.10

## 4. Konfiguracja sesji telnet/SSH

- Ustawić hasło konsoli (na obu routerach)
  - R2(config)#line console 0
  - R2 (config-line)#login
  - R2 (config-line)#password cisco
- Ustawić hasło wirtualnego terminala (sesja telnet) (na obu routerach)
  - R2 (config)#line vty 0 4
  - R2 (config-line)#login
  - R2 (config-line)#password cisco
- Z komputerów o adresie 192.168.1.100 oraz 10.0.0.10 uruchomić sesje telnet z routerem R2 (adres 192.168.1.1)
- Na komputerze o adresie 192.168.1.200 uruchomić snifera pakietów i zebrać ruch pakietów. Przeanalizować ruch telnet (możliwość podsłuchania hasła).

\* \* \*
- Ustawić hasło wirtualnego terminala (sesja SSH) (na obu routerach)
  - R2 (config)#username cisco password class
  - R2 (config)#ip domain-name ala.ma.kota.pl
  - R2 (config)#crypto key generate rsa
  - R2 (config)#line vty 0 4
  - R2 (config-line)# transport input ssh
  - R2 (config-line)#login local
- Z komputerów o adresie 192.168.1.100 oraz 10.0.0.10 uruchomić sesje SSH z routerem R2 (adres 192.168.1.1)
- Na komputerze o adresie 192.168.1.200 uruchomić snifera pakietów i zebrać ruch pakietów. Przeanalizować ruch SSH (możliwość podsłuchania hasła).

## 5. Przechwytywanie sesji WWW i FTP

- Z komputera o adresie 10.0.0.10 uruchomić sesje WWW oraz FTP do o adresie 192.168.1.100
- Na komputerze o adresie 192.168.1.200 uruchomić snifera pakietów i zebrać ruch pakietów. Przeanalizować ruch WWW, FTP (możliwość pobranie całego przesyłanego pliku).

## 6. Zakończenie pracy

- Koniec zajęć - wyczyszczenie konfiguracji urządzeń, przywrócenie właściwych parametrów urządzeń sieciowych i komputerów.