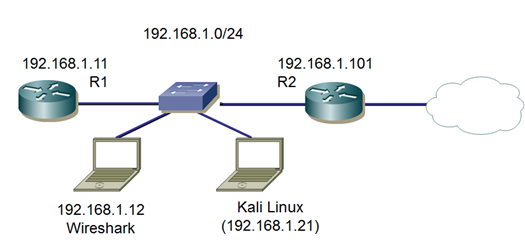
**Attack against CDP a DHCP**



**Objective**: to verify the vulnerability of network elements at the link layer

**Software:** tftpd64, Kali Linux (live distribution), Wireshark

**Tasks:**

* Connect the network according to the given scheme
* Configure basic network parameters including stations
  + Verify the time on the switch and router, if necessary set the
* On the left computer, run the tftpd64 program and
* Configure the syslog server
  + Configure the DHCP server (starting address, number of addresses - pool, default gateway)
  + On the left computer, run the WireShark program
* On the right computer, run the Kali Linux operating system
  + Verify that this computer has obtained an IP address
* Secure the network elements as follows
  + Secure the transition to privileged mode
    - Password, stored as a hash
* Secure access through the console
  + Password
* Secure access via virtual terminal
  + Password
  + Telnet protocol
  + Bonus - SSH protocol
* On network devices, set up event logging to the left computer (i.e. where tftpd64 is running)
* Verify the syslog function, e.g. by making a minor change to the interface configuration
* Verify visibility of neighbouring devices using CDP
  + On a network device, use the show cdp neighbor detail command
  + On the computer, using Wireshark
* On the right computer (Kali Linux) run yersinia and verify the generation of false CDP messages
  + Verify that these messages are registered by a real Cisco device
  + Verify that these messages are logged by WireShark
* On the right machine (Kali Linux), run the yersinia program and start generating DHCP requests
  + Verify the behavior of the DHCP server (tftpd64)
    - Caution, it may become overwhelmed or even crash
* Set the DHCP snooping function on the switch
  + Mark the port to which the left computer (with the DHCP server) is connected as trusted
* On the right computer (Kali Linux), run the yersinia program and again verify the generation of DHCP requests
  + The switch port should be blocked
  + A message should be generated

**Fragments of configurations (for inspiration - they do not fully correspond to the specification!)**

Local access via switch or router console - password settings

Switch# configure terminal

Switch(config)# enable password **class**

Switch(config)# line console 0

Switch(config-line)# password **cisco**

List configuration and interfaces and their settings

Switch# show running-config

Switch# show ip interface brief

Show information about neighbours

Switch# show cdp neighbor

Turning on password "encryption"

Switch(config)# service password-encryption

IP address - switch

Switch(config)# interface vlan 1

Switch(config-if)# ip address 10.0.0.11 255.255.255.0

Switch(config-if)# exit

Switch(config)# ip default-gateway 10.0.0.254

IP address – router

Router(config)# interface GigabitEthernet 0/0

Router(config-if)# ip address 10.0.0.12 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.254

Password to enter privileged mode (stored as a hash)

Switch(config)# enable secret class

Verify and set the time

Switch# show clock

Switch# clock set 08:55:05 May 04 2016

Remote access - passwords (the "enable" password must be set)

Switch(config)# line vty 0 15

Switch(config-line)# password cisco

Switch(config-line# login

Events loging

Switch(config)# logging 10.0.0.253

Switch(config)# logging trap 4

SSH setting

Router(config)# hostname testrouter

testrouter (config)# domain vske.cz

testrouter (config)# ip ssh version 2

testrouter (config)# crypto key generate rsa

testrouter (config)# line vty 0 1

testrouter (config-line)# transport input ssh

**Yersinia (CDP)**

Start - yersinia –I

Interface choice

Key „i“

Mode choice

Key „g“

Type of attack choice

Key x

Start of attack

Key 1

**Yersinia (DHCP)**

Start - yersinia –I

Interface choice

Key „i“

Mode choice

Key F2

Type of attack choice

Key x

Start of attack (DHCP Discover)

Key 1