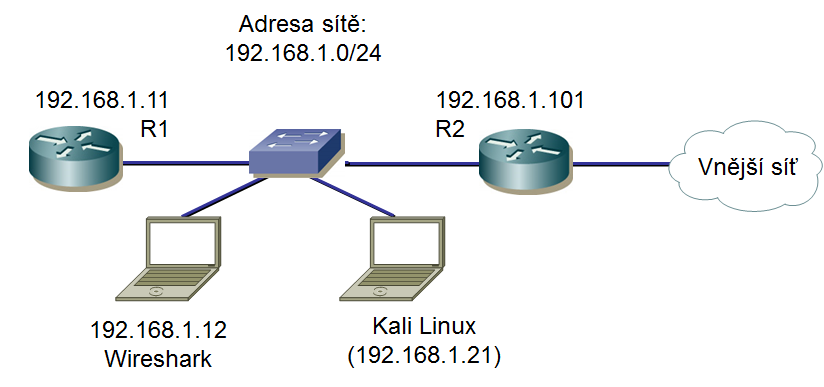
**Cvičení 3 - Útok vůči protokolu CDP a DHCP**



**Cíl:** ověřit zranitelnost síťových prvků na linkové vrstvě

**Programové vybavení:** tftpd32, Kali Linux (živá distribuce), Wireshark

**Úkoly:**

* Zapojte síť podle zadaného schématu
* Nakonfigurujte základní síťové parametry včetně stanic
  + V přepínači a směrovači ověřte čas, případně nastavte
* V levém počítači spusťte program tftpd32 a v něm
  + nakonfigurujte syslog server
  + nakonfigurujte DHCP server (počáteční adresa, počet adres - pool, výchozí brána)
* V levém počítači spusťte Program WireShark
* V pravém počítači spusťte operační systém Kali Linux
  + Ověřte, zda tento počítač získal IP adresu
* Zabezpečte síťové prvky takto
  + Zabezpečte přechod do privilegovaného režimu
    - Heslo, uloženo jako hash
  + Zabezpečte přístup přes konsolu
    - Heslo
  + Zabezpečte přístup přes virtuální terminál
    - Heslo
    - Protokol telnet
    - Bonus – protokol SSH
* V síťových zařízeních nastavte logování událostí do levého počítače (tj. kde běží tftpd32)
* Ověřte funkci protokolu syslog např. nevýznamnou změnou konfigurace rozhraní
* Ověřte viditelnost sousedních zařízení pomocí protokolu CDP
  + V síťovém zařízení příkazem show cdp neighbor detail
  + V počítači prostřednictvím programu Wireshark
* V pravém počítači (Kali Linux) spusťte program yersinia a ověřte generování falešných CDP zpráv
  + Ověřte, zda tyto zprávy registruje reálné zařízení Cisco
  + Ověřte, zda tyto zprávy zaznamenává WireShark
* V pravém počítači (Kali Linux) spusťte program yersinia a spusťte generování DHCP žádostí
  + Ověřte chování DHCP serveru (programu tftpd32 ve stanici A)
    - Pozor, může dojít k jeho zahlcení či dokonce pádu
* V přepínači nastavte funkci DHCP snooping
  + Port, ke kterému je připojena levý počítač (s DHCP serverem), označte jako důvěryhodný
* Ve pravém počítači (Kali Linux) spusťte program yersinia a opět ověřte generování DHCP žádostí
  + Port přepínače by měl být zablokován
  + Měla by být generována zpráva

**Fragmenty konfigurací pro inspiraci (neodpovídají zadání)**

Místní přístup – nastavení hesel

Switch# configure terminal

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

Switch(config)# line console 0

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

Výpis konfigurace a rozhraní a jejich nastavení

Switch# show running-config

Switch# show ip interface brief

Výpis informací o sousedech

Switch# show cdp neighbor

Zapnutí "šifrování" hesel

Switch(config)# service password-encryption

IP adresa - přepínač

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 adresa – směrovač

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

Heslo pro přechod do privilegovaného módu (uloženo jako hash)

Switch(config)# enable secret class

Ověření a nastavení času

Switch# show clock

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

Vzdálený přístup – hesla (musí být nastaveno heslo "enable")

Switch(config)# line vty 0 15

Switch(config-line)# password cisco

Switch(config-line# login

Logování událostí

Switch(config)# logging 10.0.0.253

Switch(config)# logging trap 4

Nastavení SSH

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)

Spuštění - yersinia –I

Volba síťového rozhraní

Klávesa „i“

Volba módu

Klávesa „g“

Volba typu útoku

Klávesa x

Zahájení útoku

Klávesa 1

Yersinia (DHCP)

Spuštění - yersinia –I

Volba síťového rozhraní

Klávesa „i“

Volba módu

Klávesa F2

Volba typu útoku

Klávesa x

Zahájení útoku (DHCP Discover)

Klávesa 1