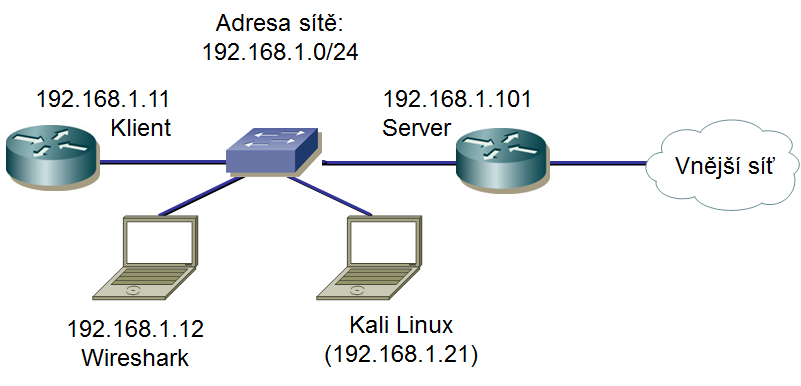
**Cvičení 5: útok typu zaplnění MAC tabulky (MAC flooding)**



**Cíl:** nastavit malou experimentální síť a ověřit útok typu MAC flooding

**Programové vybavení:** Kali Linux

* nástroj macof
* Emulátor terminálu v Kali Linuxu – program minicom  
  # dmesg | grep tty (zjištění sériových portů, např. adaptér na USB0 )  
  # minicom –b 9600 –D /dev/ttyUSB0 -8 (spuštění programu minicom)

**Popis:** Záměrem útočníka je zachytit relaci telnet a získat tak přístupové údaje k serveru. Zaplní proto CAM (Content Addressable Memory) tabulku přepínače falešnými MAC adresami, takže se přepínač začne chovat jako rozbočovač.

Poznámka: útok bude úspěšný jen při splnění určitých podmínek. Klíčové je, aby útok nastal dříve, než se přepínač naučí MAC adresy klienta a serveru. Pokud by je přepínač znal, útokem by došlo k zaplnění pouze zbytku tabulky a vůči uvedeným adresám by se přepínač choval korektně. Údaje z CAM tabulky sice jsou po stanovené době nečinnosti odstraněny, ale v praxi je málo pravděpodobné, že by klient či server byly dostatečně dlouho neaktivní. CAM tabulku lze také vymazat – buď příkazem, nebo restartem (vypnutím/zapnutím) přepínače – toto předpokládá fyzický přístup k němu.

**Úkoly:**

* Uveďte síťová zařízení do výchozí konfigurace (ověřte, případně resetujte)
* Zapojte síť podle zadaného schématu
* Nakonfigurujte základní síťové parametry všech uzlů
* Nakonfigurujte základní síťové parametry síťových zařízení pro vzdálený přístup
* Zabezpečte síťová zařízení takto
  + Zabezpečte přechod do privilegovaného režimu
    - Heslo uloženo jako hash
  + Zabezpečte přístup přes konsolu
    - Heslo
  + Zabezpečte přístup přes virtuální terminál
    - Heslo
    - Protokol telnet

**Realizace útoku typu zaplnění MAC tabulky (MAC flooding)**

* Kali Linux – veškeré úkony budou prováděny prostřednictvím příkazů (tj. v grafickém rozhraní otevřete jako okno terminálu, případně přejděte z grafického prostředí do čistě textového relace - Ctrl+Alt+F1; dále pak mezi relacemi Alt+Fn). (Tento počítač nemusí mít IP adresu.)
* V dalším počítači spusťte Wireshark a aktivujte monitorování - je vhodné nastavit zobrazovací filtr na telnet
* V přepínači ověřte stav MAC tabulky (která MAC adresa uzlu je za kterým portem, plus členství ve VLAN)

Switch# show mac address-table

* V přepínači ověřte stav MAC tabulky (její velikost, tj. počet použitých a volných záznamů)

Switch# show mac address-table count

* V přepínači smažte obsah MAC tabulky

Switch# clear mac address-table dynamic

* Kali Linux – zahajte útok (co nejrychleji!) – vyvolejte zaplnění MAC tabulky falešnými rámci (parametry jsou odchozí rozhraní a vyslaný počet rámců)

#macof –i eth0 –n 99999

* Ze směrovače-klienta se přihlaste ke směrovači–serveru

Router# telnet 192.168.1.101 nebo jen  
Router# 192.168.1.101

* Wirehark by měl nyní ukazovat zachycené pakety. Zastavte monitorování, umístěte kursor na první zachycený paket a volbami Analyze/Follow/TCP Stream zobrazte zachycenou relaci
* Pokud nedojde zachycení relace, přepínač pravděpodobně stihl ještě před útokem MAC adresy směrovačů (klienta, serveru). Toto lze ověřit v MAC tabulce (příslušný záznam by měl být prázdný)

Switch#show mac address-table interface fastEthernet 0/1

Mac Address Table

-------------------------------------------

Vlan Mac Address Type Ports

---- ----------- -------- -----

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

Výchozí konfigurace směrovače (při výzvě NEUKLÁDAT konfiguraci)

erase startup-config

reload

Výchozí konfigurace přepínače (při výzvě NEUKLÁDAT konfiguraci)

erase startup-config

delete flash:vlan.dat

reload

Místní přístup přes konsolu přepínače nebo směrovače – nastavení hesel

Switch> enable

Switch# configure terminal

Switch(config)# enable password class

Switch(config)# line console 0

Switch(config-line)# password cisco

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 (rovněž nastavit heslo "enable", jinak nelze přejít do privilegovaného módu)

Switch(config)# line vty 0 15

Switch(config-line)# password cisco

Switch(config-line# login

Výpis konfigurace a stavu rozhraní přepínače

Switch# show running-config

Switch# show mac-address-table

Switch# show interface trunk

Router# show ip interface brief

Výpis informací o sousedech

Switch# show cdp neighbor

Zapnutí "šifrování" hesel

Switch(config)# service password-encryption

Nastavení IP adresy u přepínače (slouží pouze pro jeho vzdálenou správu)

Switch(config)# interface vlan 1

Switch(config-if)# ip address 192.168.1.100 255.255.255.0

Switch(config-if)# exit

Switch(config)# ip default-gateway 192.168.1.101

Nastavení IP adres u směrovače, překladu adres/portů (NAT/PAT) a statické cesty

Router(config)#interface GigabitEthernet 0/0

Router(config-if)# ip address 192.168.1.101 255.255.255.0

Router(config-if)# ip nat inside

Router(config)# interface GigabitEthernet 0/1

Router(config-if)# ip address 10.0.0.137 255.255.255.0

Router(config-if)# ip nat outside

Router(config)# access-list 10 permit any

Router(config)# ip nat inside source list 10 interface  
 GigabitEthernet 0/1 overload

Router(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.254

Ověření funkce překladu adres

show ip nat translations

Konfigurace DHCP

ip dhcp excluded-address 192.168.1.1 192.168.1.29

ip dhcp excluded-address 192.168.1.100 192.168.1.254

…

Router(config)ip dhcp pool INTERNALNET-1

Router(dhcp-config)# network 192.168.1.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.1.101

Router(dhcp-config)# dns-server 8.8.8.8 147.251.6.10

Router(dhcp-config)# domain-name test.cz

Router(dhcp-config)# lease 5

Ověření funkce DHCP

show ip dhcp bindings

Aktivace HTTP(S) serveru

username admin privilege 15 password cisco

ip http server

ip http secure-server

ip http authentication local