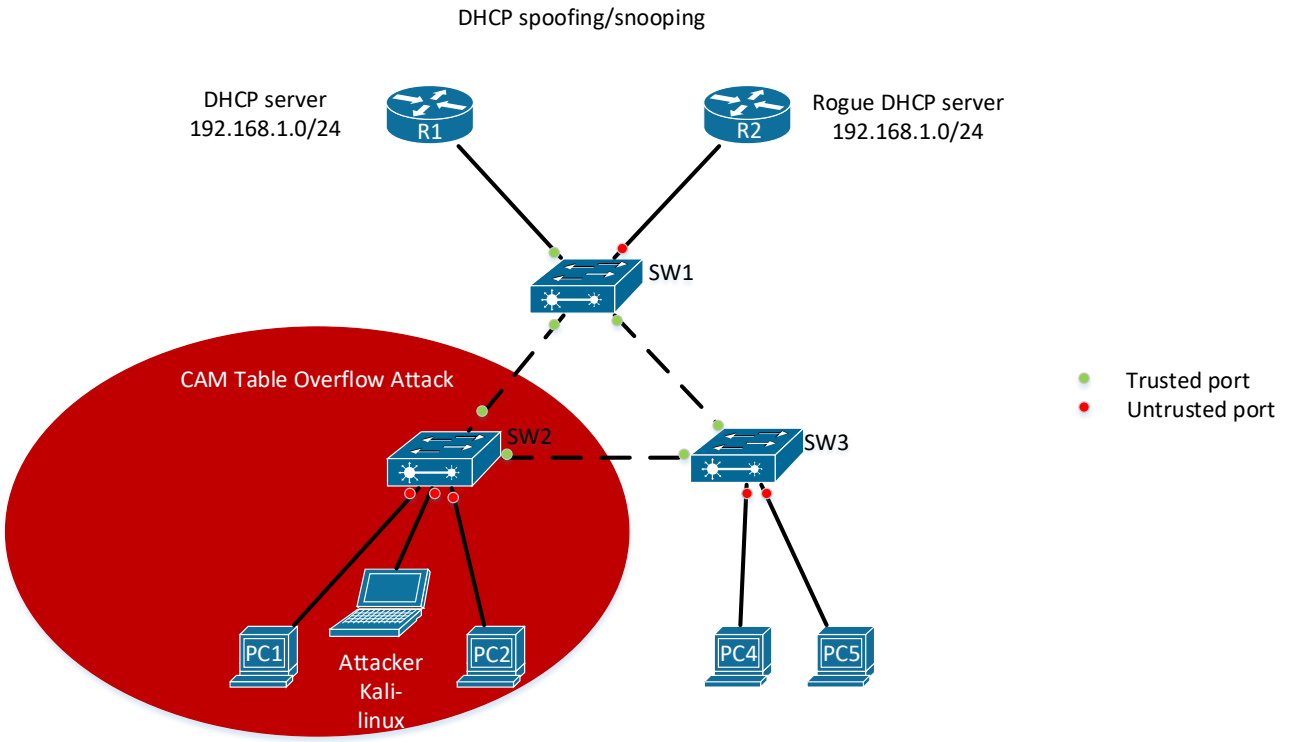
PS1/ Cvičenie 11 / **DHCP starvation/spoofing/snooping, CAM table Overflow**

Topológia



Inštrukcie a scenár

- V GNS3 pracujete každý samostatne
- V reálnom laboratórií sa pracuje v „dvojiciach“, každá „dvojica“ má dve smerovače, tri prepínače (2960) a tri počítače
    - pokiaľ nie je dostatok počítačov (3 na dvojicu), tak použi dva pre legitímnych hostov, a tretí bude útočník, na ktorom zároveň budete cez Wireshark odchytávať komunikáciu 2 legitímnych hostov – toto môže byť na celom cvičení iba jedno PC, ktoré si skupiny budú „požičiavať“
    - na konci cvičenia SW2 vymeníte za prepínač 2950 (ktorý donesie vyučujúci)
- Pre toto cvičenie bude potrebné pripraviť si virtuálny stroj s Kali-linuxom (bude nižšie). V GNS3 ho už máme pripravený.
- Kde sa robí s Wiresharkom, sprav screenshot aj z pohľadu na hlavičky pri odchytení ICMP správy
- Vrchné smerovače potrebujú min. 1 ethernetové rozhranie
- Pre toto cvičenie sú potrebné image:
    - vios_l2-adventerprisek9-m.03.2017.qcow2
    - c7200-adventerprisek9-mz.155-2.XB.image
    - kali-linux-2018.4-amd64.iso

CAM Table Overflow Attack

1. **Káblovanie**
   a. Topológiu si zapoj podľa obrázku vyššie, ale **odpojte káble z PC1 a PC2**
   KALI LINUX PRIHLASOVACIE MENO JE root A HESLO JE gns.
2. **Základná konfigurácia:**
   a. V reálnom laboratórií : Vo Virtual-boxe vytvor nový virtuálny stroj s použitím ISO obrazu Kali-linuxu
      i. Image si môžete stiahnuť napr. tu: ....
   b. Skontroluj či má prepínač prázdnu CAM tabuľku, ak nie vymaž všetky záznamy (`sh mac add-table, clear mac add-table *`)
   c. Na **všetkých** prepínačoch zapnite **RSTP**
      spanning-tree mode rapid-pvst
   d. Nastav IP adresy počítačom z rozsahu 172.16.0.0/24, kde posledný oktet bude číslo PC z obrázka vyššie
3. **ÚTOK: Spusti útok CAM Table Overflow a sleduj správanie**
   a. Spusti útok
      i. Pripoj útočníka kálbom do prepínača
      ii. Skontroluj, že v CAM tabuľke sa nachádza len jediná naučená MAC adresa poprípade ešte MAC adresy susedných switchov (adresa útočníka)
         - **Pozor!** nepripájaj zvyšných klientov! Nesmú byť pripojený skôr kým nebude CAM tabuľka plná!
           Su tam naozaj len mac adresy switchov a utocnikova
   b. Cez terminál útočníka spusti príkaz `macof` a na prepínači zadaj príkaz `show mac address-table count`, aby si zistil kapacitu – max. počet záznamov, zisti koľko adries sa prepínač aktuálne už naučil, a koľko mu ešte ostáva do dosiahnutia maxima a tento príkaz opakuj pokým nezistíš, že je tabuľka plná (count = 0).
   Asi nie je dobre cakat kym bude count = 0 lebo switch Cisco vIOS L2 v GNS3 ma cca 70 miliónov voľných mac adries. Tento test sa nedá vykonať v reálnom čase pretože by zaplnenie tabuľky trvalo cca 151 hodín v GNS3.

   c. Pripoj PC1 a PC2 k prepínaču.
      i. Na útočníkovi si spusti Wireshark, nastav filter iba na icmp.
      Na Kali Linuxe spustia zadaním príkazu wireshark v terminale.
      ii. Z PC1 over konektivitu k PC2 (ping)
         - Odchytil útočník s Wireshrakom komunikáciu týchto dvoch klientov?
            - Prečo je to tak?
            - Čo sa s prepínačom udialo?
              Konektivita je v poriadku len vo wiresharku kali linuxu nevidím žiadne ICMP pretože sa nezaplnila MAC tabuľka switchu generovanými MAC adresami.
4. **OCHRANA: Nakonfiguruj na prepínači Port Security a od sleduj ochranu pred týmto typom útoku**
   a. Na porte útočníka nakonfiguruj port security s obmedzenou kapacitou na 5 MAC adries (sticky)
   b. Nastav akciu na restrict

c. Znova zopakuj útok podľa postupu z bodu 3, a over na prepínači status portu na ktorom je útočník, obsah CAM tabuľky (koľko a aké MAC tam sú?).

Nastavte na SW2 v obrázku na porte útočníka:

```
switchport mode access
switchport port-security
switchport port-security maximum 5
switchport port-security violation restrict
switchport port-security mac-address sticky
```

Keď spustím macof následne ked mam nastavený port security tak v mac address table mam aj static mac adresy a vidím aj restrict reakciu ale switch sa naučí dynamic adresy od kali linuxu.

DHCP spoofing/snooping + DHCP starvation

1. **Nakonfiguruj DHCP server na R1**
   a. Vytvor dhcp pool:
      i. názov crypto
      ii. default gateway: 192.168.1.254
      iii. DNS server: 192.168.1.253
      iv. Rozsah: 192.168.1.0/24, a vyjmi z prideľovania posledné dve IP adresy (gateway a DNS server)

Na R1 zadajte:

```
conf t
interface fastEthernet 0/0
no shutdown
ip address 192.168.1.254 255.255.255.0
exit
ip dhcp pool crypto
default-router 192.168.1.254
dns-server 192.168.1.253
network 192.168.1.0 255.255.255.0
exit
ip dhcp excluded-address 192.168.1.253 192.168.1.254
```

2. **Na klientoch nastav nech si získajú automaticky IP adresu od DHCP servera**
   - Over, či funguje

Funguje na klientoch stačí zmeniť prideľovanie IP adresy na automaticky.

3. ÚTOK: Použi Kali-linux pre DHCP starvation

Na reálnych zariadeniach je postup nasledovný :

- Otvor Terminal, potom použi príkaz `yersinia -G`, tým otvoríš útočný nástroj
- V nástroji zaklikni `Launch attack`, vyber útok `DHCP` a následne `sending Discover Packet`, klikni na `ok`
    i. Sleduj generovanie
    ii. Zisti na R1, koľko je prenajatých IP adries? (`show ip dhcp pool`)
    iii. Zisti na ako dlho sú prenajaté IP adresy? (`show ip dhcp bindings`)
    iv. Na klientovi požiadaj o znovu pridelenie IP adresy. (`release/renew`)
        a. Čo znamená pridelená adresa `169.254.x.x`?

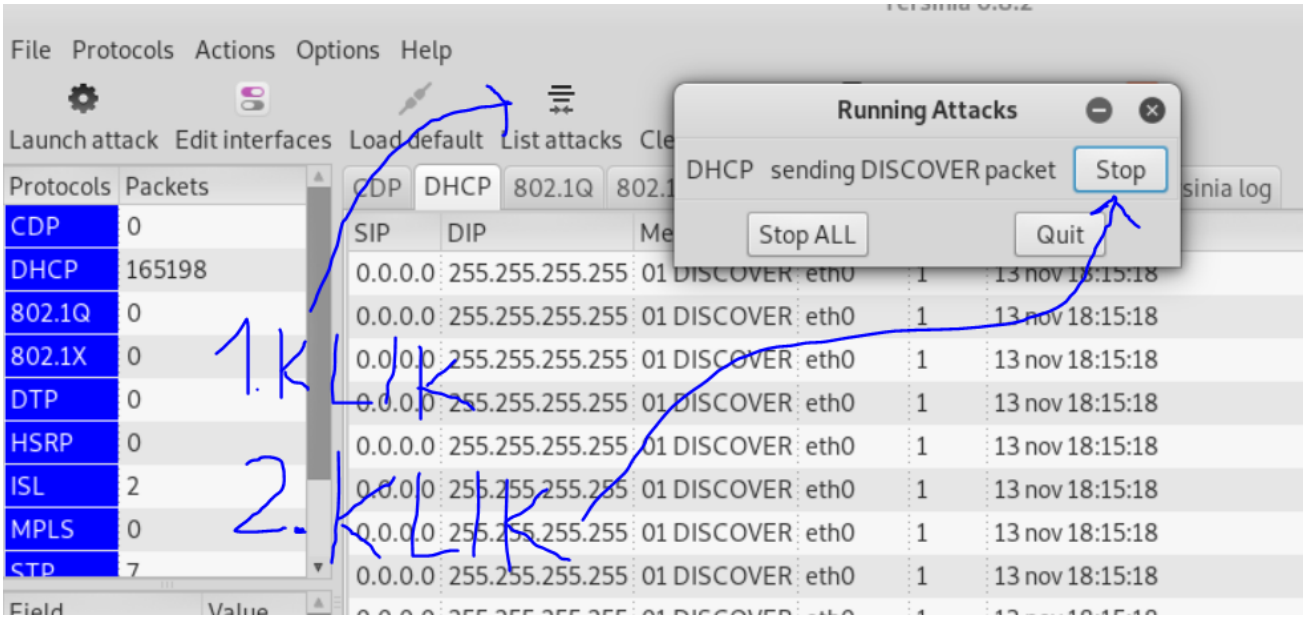
V GNS3 je postup nasledovný:

- V GNS3 útok nefunguje ako by mal.
- Útok treba urobiť nasledovne:
    v. Odpojiť všetky káble klientov zo switchu alebo vymazať klientov.
    vi. Na R1(dhcp serveri) je potrebné zadať príkaz `clear ip dhcp binding *`.
    vii. Pripojiť Kali Linux a získať s ním IP adresu cez dhcp.
    viii. Spustiť na Kali linuxe v terminály `yersinia -G`, tým sa otvorí útočný nástroj
    ix. V nástroji je potrebné zakliknúť `Launch attack` a vybrať útok `DHCP` a `sending Discover Packet`.
    x. Počkať kým DHCP server požičia všetky adresy.
    xi. Overenie pomocou príkazu `show ip dhcp pool`
    xii. Pripojiť Lubuntu PC káblom do switchu a získať automaticky IP adresu.
    xiii. Malo by ukázať chybu a namiesto 192.168.1.x adresy ktorú by ste mali získať od DHCP servera nezískate žiadnu IP adresu.
    xiv. Overte pomocou príkazu `ip a` na Lubuntu.
- Počas spusteného útoku alebo po ňom treba zadať na routeri `show ip dhcp pool`, `show ip dhcp binding`.
- Príkaz `release` uvoľni používanú adresu a PC sa bude snažiť získať novú adresu od DHCP servera.
    xv. Vo windowse by získal 169.254... v linuxe nezíska žiadnu IP adresu keď mu dhcp server nemá čo ponúknuť.
    xvi. V linuxe je obdoba release : príkaz `sudo dhclient -r ens3` na lubuntu a `sudo dhclient -r eth0` na kali linuxe. Renew je `sudo dhclient ens3` alebo len `sudo dhclient`.
    xvii. Okrem toho je potrebné aj reaktivovať rozhranie na koncovom zariadení. Na ploche v `IP config`, `activate connection` a zvoliť `deaktivovať` a následne hneď `aktivovať`.

```
R1#show ip dhcp pool

Pool crypto :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 252
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 0.0.0.0              192.168.1.1      - 192.168.1.254     252
R1#show ip dh
R1#show ip dhcp bind
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.1         0cfa.46b5.e200          Nov 14 2019 04:52 PM    Automatic
192.168.1.2         0cfa.462c.2f00          Nov 14 2019 04:55 PM    Automatic
192.168.1.3         7987.817e.79ad          Nov 13 2019 05:12 PM    Automatic
192.168.1.4         f961.1d4d.f671          Nov 13 2019 05:12 PM    Automatic
192.168.1.5         090d.164f.aa39          Nov 13 2019 05:12 PM    Automatic
192.168.1.6         8d0d.c472.64c2          Nov 13 2019 05:12 PM    Automatic
192.168.1.7         27df.b77b.0a75          Nov 13 2019 05:12 PM    Automatic
192.168.1.8         b36a.d902.2389          Nov 13 2019 05:12 PM    Automatic
192.168.1.9         f3b7.251d.b8eb          Nov 13 2019 05:12 PM    Automatic
192.168.1.10        a587.4a6e.53bc          Nov 13 2019 05:12 PM    Automatic
192.168.1.11        e305.cc7e.36e5          Nov 13 2019 05:12 PM    Automatic
192.168.1.12        bd7d.3867.97b5          Nov 13 2019 05:12 PM    Automatic
192.168.1.13        55ca.d847.0c14          Nov 13 2019 05:12 PM    Automatic
192.168.1.14        198c.741b.403e          Nov 13 2019 05:12 PM    Automatic
192.168.1.15        bbd2.502b.ad03          Nov 13 2019 05:12 PM    Automatic
192.168.1.16        0514.0c32.0deb          Nov 13 2019 05:12 PM    Automatic
192.168.1.17        8fde.cc65.ee43          Nov 13 2019 05:12 PM    Automatic
192.168.1.18        a3eb.5656.3c1f          Nov 13 2019 05:12 PM    Automatic
192.168.1.19        b328.4510.87af          Nov 13 2019 05:12 PM    Automatic
 --More--
```

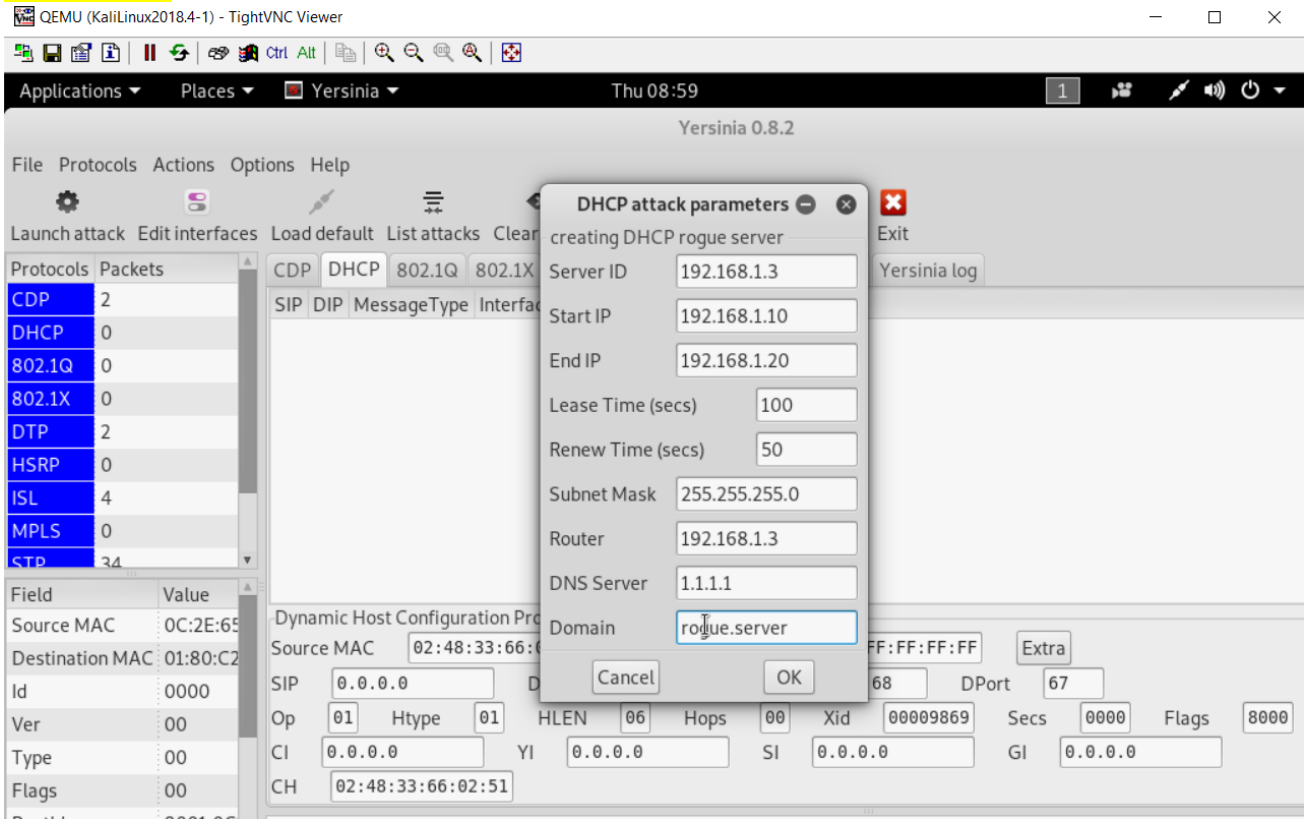
UTOK ZASTAVIME POSTUPOM NA NASLEDUJUCOM OBRAZKU



4. ÚTOK (pokračovanie): Nakonfiguruj falošný DHCP server

V realite by útočník nakonfiguroval falošný dhcp server priamo u seba. Funguje to tak, že útok *Sending DHCP discover packet* stále beží (tým má útočník zaručené, že si vyžiada všetky IP adresy od legitímneho DHCP servera) a vytvorí zo seba falošný DHCP server (viď. Obr. nižšie).

Ukážka reality



Toto však zaberá príliš veľa RAM pamäte, čo si ani v podmienkach laboratória (4GB RAM na PC), ani v podmienkach GNS3 servera nemôžeme dovoliť, preto tento útok predčasne vypneme:

a. Najprv vypni útok `sending discover DHCP packet`.
b. Následne **nakonfiguruj falošný DHCP** server na **smerovači R2** (efekt bude podobný ako v realite).
    i. Rovnako ako v bode 1, vytvor pool s tým istým rozsahom, ale **zmeň** default gateway na .252 (útočník)

Na R2(rogue router) zadajte :

```
conf t
interface fastEthernet 0/0
no shutdown
ip address 192.168.1.252 255.255.255.0
exit
ip dhcp pool rogue
default-router 192.168.1.252
dns-server 192.168.1.253
network 192.168.1.0 255.255.255.0
exit
ip dhcp excluded-address 192.168.1.252 192.168.1.253
```

5. **Na klientoch požiadaj o obnovenie dynamicky získanej IP adresy**
    a. Release/renew
    b. Nezabudni aj reaktivovať rozhranie na Lubuntu PCs.
    c. Akú IP adresu sa klienti naučili?
        i. Podľa default gateway vieš overiť, že adresy sú naučené od falošného DHCP servera?

        Na klientoch zadajte :
        dhclient -r ens3.
        Aby som to vedel musel by som poznať default gateway predošlého skutočného DHCP servera a porovnať ich. Na Lubuntu zistíš default gateway príkazom route -n

6. **OCHRANA: Na prepínačoch nastav dhcp snooping**
    a. Zapni dhcp snooping príkazom `ip dhcp snooping`
    b. Priraď do snoopingu vlan, kde sa defaultne nechádzajú všetky porty (vlan1) (`ip dhcp snooping vlan 1`)
    c. Porty, na ktorých sa očakáva legitímny DHCP server, nastav ako dôveryhodné, rovnako aj **všetky porty medzi prepínačmi** musia byť nastavené ako **trusted**!
    d. Over nastavenie DHCP snooping príkazom `show ip dhcp snooping`
    e. Dostaň všetko do pôvodného stavu a zopakuj útok, ktorý by teraz už nemal byť úspešný:
        i. Na legitímnom DHCP servery R1 vyčistiť pool (`clear ip dhcp binding *`) alebo (`clear ip dhcp pool <názov poolu> binding`)
        ii. Zopakuj útok z bodu 3:
            - Otvor Terminal, použi príkaz `yersinia -G`, vyber `Launch attack`, následne útok `DHCP` a `sending Discover Packet`, potvrď `ok`.

- Sleduj generovanie
- Over na R1, že žiadnu IP neprenajal útočníkovi (`show ip dhcp binding`)

iii. Na klientovi PC1 požiadaj o znovu pridelenie IP adresy (`release/renew`)

- Nezabudni reaktivovať rozhranie na Lubuntu PCs
- Je potrebné zastaviť útok, aby mohli byť pridelené IP adresy koncovým staniciam a taktiež je potrebné počkať dlhší čas kým DHCP server pridelí IP adresy.
- Over funkčnosť, mali by získať správnu IP adresu z legitímneho DHCP servera

Na switchoch zadajte :

conf t

ip dhcp snooping

ip dhcp snooping vlan 1

Na rozhraniach ktorymi su spojene switche a na rozhraniach veducich od switchov ku klientom ktorým dôverujeme zadajte ip dhcp snooping trust.

Over dhcp snooping prikazom show ip dhcp snooping

Vypnite rogue dhcp server router a na legitímnom zadajte clear ip dhcp binding *

Môžete zatiaľ na klientoch na ktorých očakávate že dostanú IP adresu vypnúť v edit connection ich connection a následne spustiť yersinia -G a útok sending Discover Packet. Ak vám to funguje správne tak v termináli každého switchu uvidíte správu nekalej činnosti a čo je hlavné keď si zobrazíte reálny dhcp server a dáte show ip dhcp binding alebo show ip dhcp pool tak by ste mali vidieť že neprenajal žiadnu IP adresu. Následne môžete požiadať na klientoch o pridelenie IP adresy automaticky.