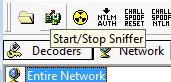
# Útok 1 – Odposlouchávání VoIP za pomocí MitM

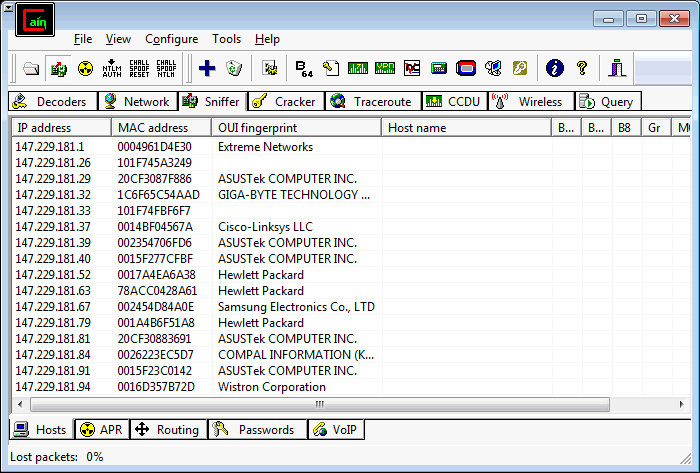
## Scénář Pomůcky

Cisco 2811 s CME (R18 a R19)  
Catalyst 3560 s PoE (S16 a S17)  
2× HW Cisco IP Phone  
PC s Cain&Abel  
PC s Cisco IP Communicatorem

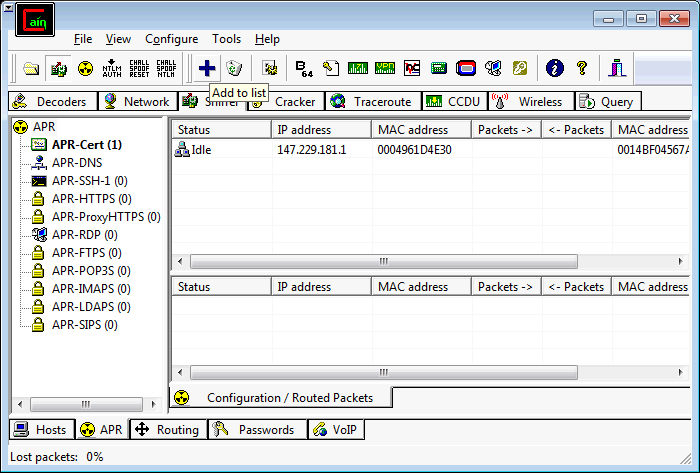


## Postup

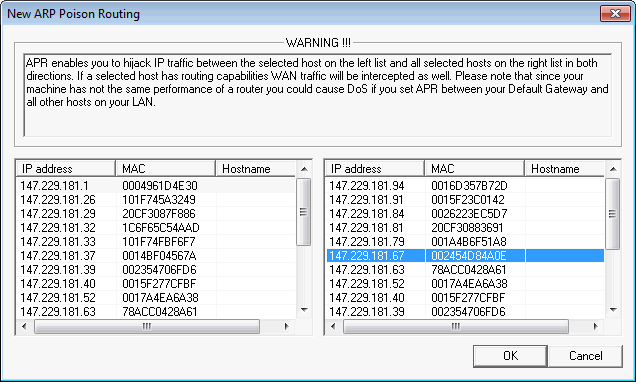
1. Catalyst 3560
   1. Ověřit, že porty, do kterých jsou připojeny telefony nejsou v rozdílných VLANách
      * show cdp neighbors
      * show vlan
2. Cisco 2811
   1. Nakonfigurovat DHCP server
      * ip dhcp pool
      * network
      * default-router
      * option 150 ip address
   2. Nakonfigurovat na telefonní ústřednu
      * set clock
      * max-ephones
      * max-dn
      * keepalive
      * telephony services
      * ip source-address <*CMERouterIP*> port 2000
      * system message
      * create cnf-files
      * ephone-dn
      * number
      * name
      * ephone
      * button
      * mac-address
3. Útočník
   1. Spustit Cain&Abel
   2. Spustit sniffování 
   3. Záložka *Sniffer*, pravé tlačítko *Scan MAC Addresses*
   4. Oscanujte všechny hosty na segmentu a zjistěte jejich MAC adresy



* 1. Z podzáložky *Hosts* na APR a pak tlačítko +

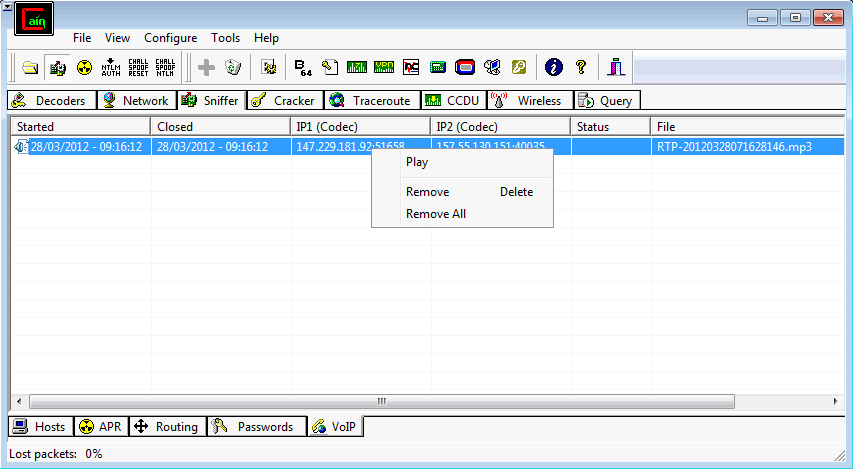


* 1. Napárovat IP adresy, vůči kterým chcete provádět MitM (mezi telefony) a *OK*



* 1. Spustit útok tlačítkem *APR* 

1. Vyzkoušet si zatelefonovat mezi uživateli
2. Přehrát si odposlechnuté hovory
   1. Záložka *VoIP*, vybrat hovor a pravým tlačítkem *Play*



# Útok 2 – Fake Google Web with MitM

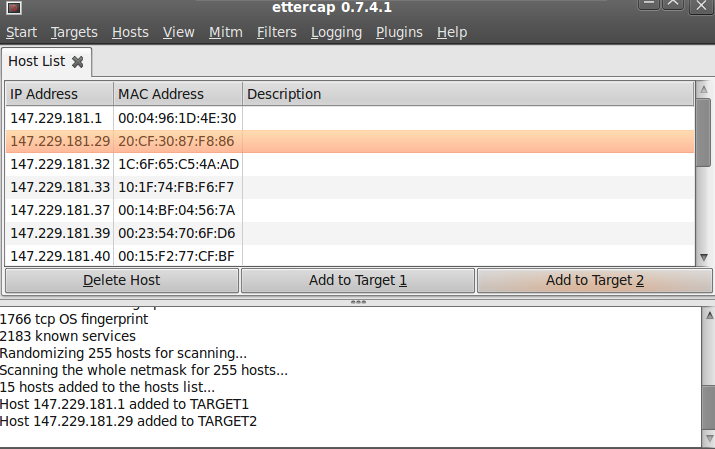
## Scénář Pomůcky

Cisco 2811 (R16 a R17)  
Catalyst 2960 (S11 a S12)  
PC s BackTrackem 5 R2  
PC

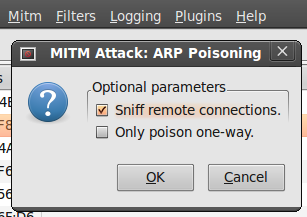


## Postup

1. Cisco 2811
   1. Nakonfigurovat interface Fa0/0, aby získával adresu skrz DHCP, a adresu na Fa0/1
      * ip address dhcp
      * no shutdown
   2. Nakonfigurovat DHCP server
      * ip dhcp pool
      * network
      * default-router
      * dns-server 8.8.8.8
   3. Nakonfigurovat NAT překlad a označit rozhraní pro NAT překlad
      * ip nat outside
      * ip nat inside
      * access-list permit 192.168.0.0 0.0.0.255
      * ip nat inside source list interface overload
   4. Nakonfigurovat statickou default route směřující do Internetu
      * ip route 0.0.0.0 0.0.0.0
2. Obnovte DHCP adresu na počítači Manželky
3. Manžel
   1. Ujistěte se, že všechny firewally i antiviry jsou vypnuté
   2. Ověřte, že typ síťovky ve VirtualBoxu je síťový most a je povolený promiskuitní mód
   3. Spusťte revertnutý BackTrack ve VirtualBoxu – login *root* heslo *toor* a nastartujte grafické rozhraní startx
   4. Zkontrolujte směrování v BackTracku
      * Soubor /etc/network/interfaces obsahuje iface eth0 inet dhcp
      * /etc/init.d/networking restart¨
      * ifconfig
   5. Spusťte Ettercap pomocí ettercap –G
   6. Menu *Sniff*, pak *Unified Sniffing* a vybrte síťovku eth0
   7. Oscanujte síť na přítomné hosty, menu *Hosts*, pak *Scan for Hosts*
   8. Zobrazte seznam hostů (*Hosts* a *Hosts list*) a označte default gateway a počítač Manželky pomocí tlačítek *Add to Target 1* a *Add to Target 2*



* 1. Nastavte MitM ARP cache poisoning kliknutím na menu *Mitm* a pak *Arp poisoning…* s tím, že budete sniffovat i vzdálená připojení



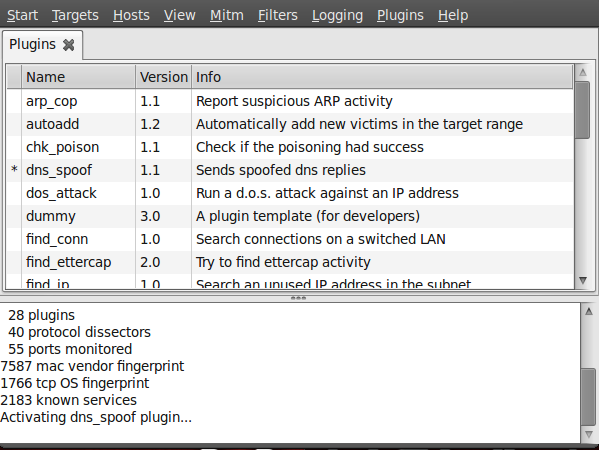
* 1. Spusťte útok *Start* a *Start sniffing*

1. Veškerá komunikace mezi Manželkou a její def. gateway chodí nyní přes Manžela
2. Vylepšete útok o kradéní hesel z Gmailu
   1. Nakonfigurujte falešný DNS překlad
      * Do souboru /usr/local/share/ettercap/etter.dns dopište:

\*.gmail.com A <*adresa manžela*>  
gmail.com A <*adresa manžela*>

www.gmail.com A <*adresa manžela*>

* 1. Z Plochy přesuňte soubory (index.html, log.txt, mail.php) falešnou Gmail stránku i s pomocnými skripty do /var/www a ověřte, že soubory mají právo spouštět a být čteny kýmkoli
     + chmod 777 index.html log.txt mail.php
  2. V Ettercapu aktivujte dns\_spoofovací plugin
     + Menu *Plugins* a pak *Manage plugins*
     + Dvakrátk klikněte na dns\_spoof, čímž by se měl aktivovat (objeví se na něm \*)



1. Vyčistí-li se i DNS cache Manželky, tak pokud se rozhodne vstoupit na Gmailý stránky, tak v adresáři /var/www/log.txt se nachází její login s heslem

## Zabezpečení

Zapnutí DHCP snoopingu a ARP inspekce, nastavení portů jako trusted a untrusted pro DHCP snooping.

ip dhcp snooping # enables DHCP snooping globally  
ip dhcp snooping vlan 1 # enables DHCP snooping for VLAN 1  
no ip dhcp snooping information option  
ip dhcp snooping trust

ip arp inspection vlan   
ip arp inspection validate src-mac dst-mac ip to

show ip arp inspection vlan   
show ip dhcp snooping binding

# Útok 3 –Double-VLAN Hopping

## Scénář Pomůcky

Catalyst 2950 (půjčený)  
Catalyst 3560 (S13)  
PC s BackTrackem   
PC pro monitorování SPAN  
PC oběti



## Postup

1. SW B
   1. Nastavit jako VTP server pro doménu LAB, pojmenovat VLAN1 a VLAN2, vypnout VTP prunning
   2. Nakonfigurovat DHCP pooly pro VLAN1 a VLAN2 a vyjměte z něj adresy switchů
      * ip dhcp pool
      * network
      * default-router
   3. Nakonfigurovat Fa0/24 jako trunk a Fa0/1 jako access port pro VLAN2
   4. Nakonfigurovat SPAN monitor session na portu Fa0/24 a replikovat jeho provoz na Fa0/10
      * monitor session source interface
      * mon ses destination interface encapsulation replicate
2. SW A
   1. Nastavit jako VTP klient pro doménu LAB, vypnout VTP prunning
   2. Nakonfigurovat Gi0/1 jako trunk a Fa0/1 jako access port pro VLAN2
3. Spustit si Wireshark na Oběti, útočníkovi a SPAN sondě
4. útočník
   1. Ujistěte se, že všechny firewally i antiviry jsou vypnuté
   2. Ověřte, že typ síťovky ve VirtualBoxu je síťový most a je povolený promiskuitní mód
   3. Spusťte BackTrack ve VirtualBoxu – login *root* heslo *toor* a nastartujte grafické rozhraní startx
   4. Zkontrolujte směrování v BackTracku
      * Soubor /etc/network/interfaces obsahuje iface eth0 inet dhcp
      * /etc/init.d/networking restart
      * ifconfig
   5. Spustit Yersinii
   6. Záložka *802.1Q*
   7. Tlačítko *Edit mode*
   8. Nastavit srcIP a dstIP podle scénáře, vnitřní tag VLAN1, vnější tag VLAN2
   9. Spustit útok *Launch attack* a v sekci 802.1Q zvolit Double-VLAN Tag

## Zabezpečení

Jako native VLAN používat VLANu, která není použita nikde jinde, vytvořte si např. VLAN3

# Útok 4 – CAM Overflow

## Scénář Pomůcky



Catalyst 2950   
PC s BackTrackem   
PC 1 a 2 (oběti)

## Postup

1. Switch
   1. Pravidelně pozorujte obsah CAM tabulky, smažte ji v případě potřeby
      * show mac-address-table
      * show mac-address-table clear
      * clear mac-address-table
2. PC 3
   1. Ujistěte se, že všechny firewally i antiviry jsou vypnuté
   2. Ověřte, že typ síťovky ve VirtualBoxu je síťový most a je povolený promiskuitní mód
   3. Spusťte BackTrack ve VirtualBoxu – login *root* heslo *toor* a nastartujte grafické rozhraní startx
   4. Zkontrolujte směrování v BackTracku
      * Soubor /etc/network/interfaces obsahuje iface eth0 inet dhcp
      * /etc/init.d/networking restart
      * ifconfig
   5. Realizujte útok CAM overflow v BackTracku, spusťte bez parametrů následující
      * macof
3. Spusťe Wireshark na všech počítačích
4. Na počítačích PC 1, PC 2 a PC 3 přidělte IP adresy
5. Pingněte mezi PC 1 a PC 2, díky zahlcení CAM tabulky dorazí ping i PC 3

## Zabezpečení

Použití port security, nastavení maximálního množství MAC address na portě a akce při jejím porušení.

switchport port-security

switchport port-security max-address

switchport port-security violation shutdown