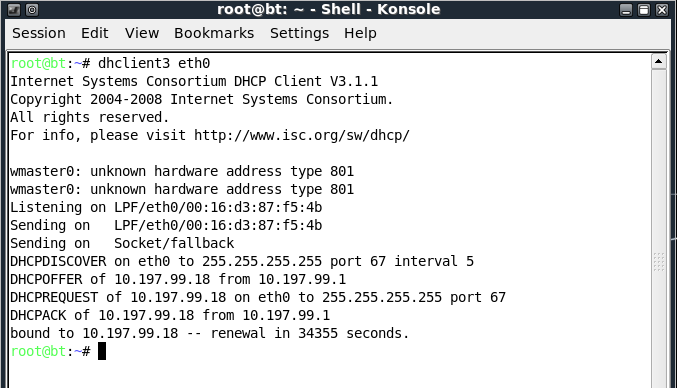
# Backtrack linux

magyar billentyű:

setxkbmap hu az X-es kornyezetben.

loadkeys hu konzolos kornyezetben

IP cím kérés Backtrack linux alatt a dhclient3 eth0 paranccsal történik.



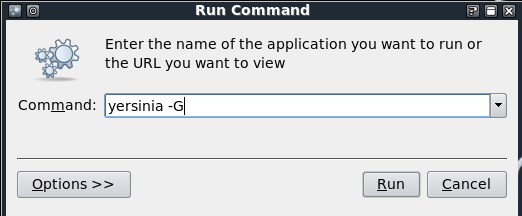
kep 1

## Yersinea

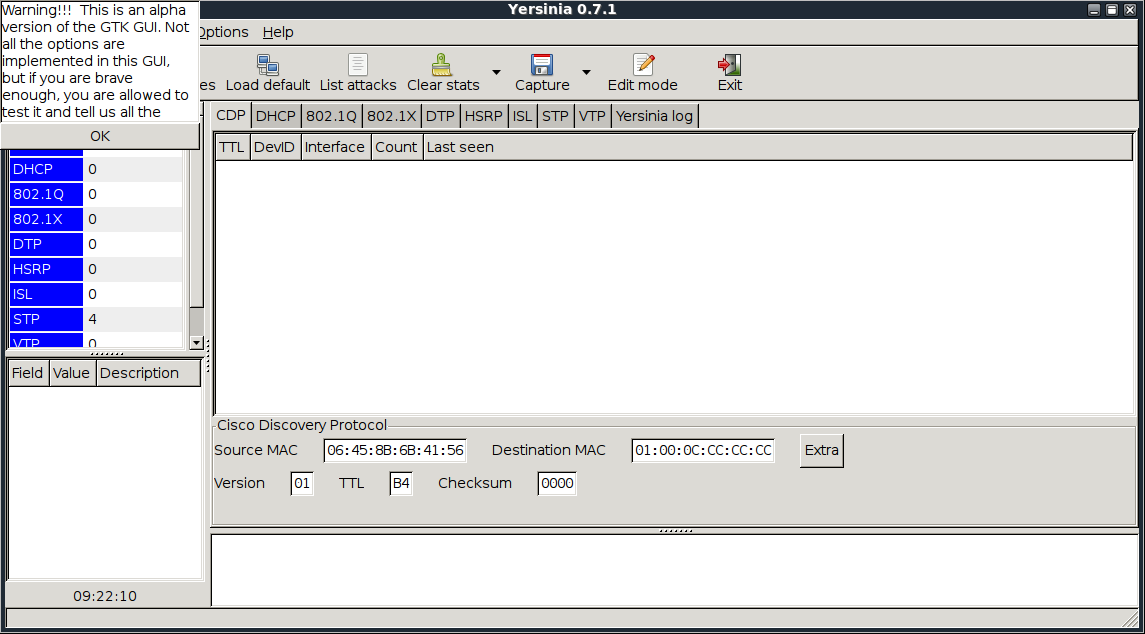
A libnet library-t használja, ez van linuxban és windows-ban is. Scapy egy másik tool, amit lehet programozni, és tetszőleges csomagot össze lehet vele állítani.

Többféle képpen indíthatjuk. csak simány yersinea, ha monitor nélkül, vagy scriptből ütemezett feladatkent indítjuk (szerver üzemmód).

-G grafikus felület. instabil. A támadás lehet, hogy a háttérben tovább fut, ha lefagy, ez problémákat okozhat, ezért lehetőleg ne használjuk.

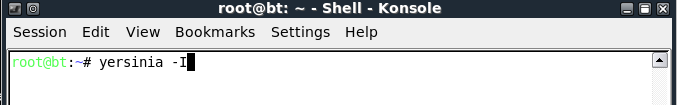


kep 2



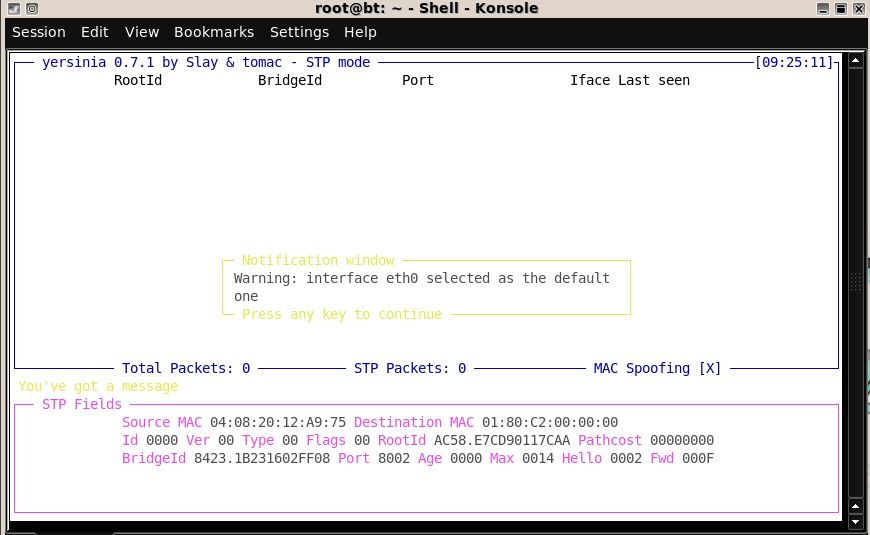
kep 3

-I interaktiv karakteresen rajzolgatja ki.



kep4

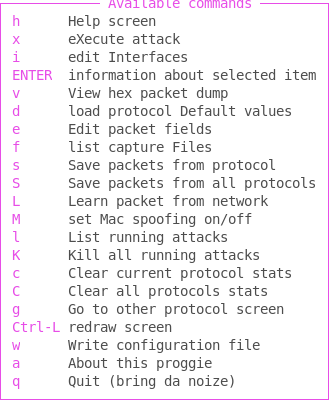
Amikor elindul az alkalmazás megmondja, hogy milyen hálókártyán fut



kep 5

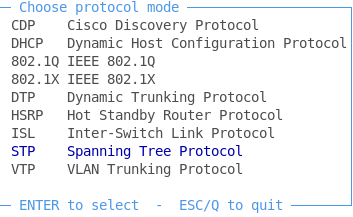
ps aux | grep yersinea fut-e, ha valami baj van. aux mindent kiír.

yersinia -I után help-et a h gomb lenyomásával kérünk.



kep 6

Következő feladat, hogy kiválasszuk, hogy milyen protokoll-t támadunk. A yersinia alapértelmezés szerint az STP protokolt támadja. A g gombot lenyomva látjuk a lehetőségeket.

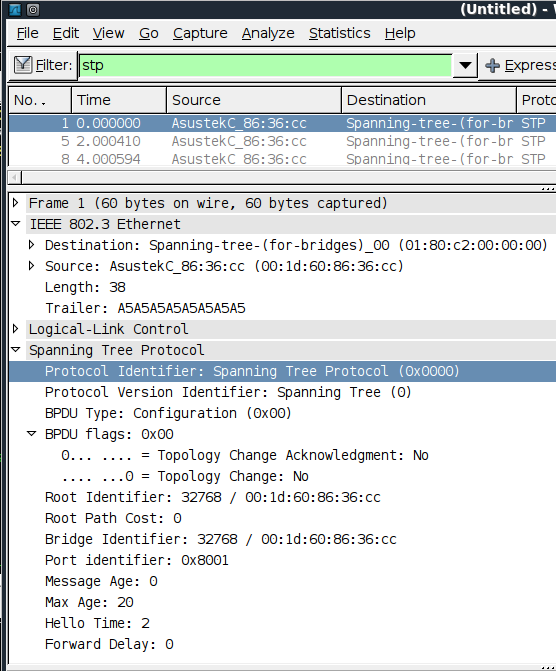


kep 7

## Spanning Tree Protokoll

Feladata, hogy biztosítsa a hurokmentes ethernet kapcsolatot. Egy fa struktúrát épít fel, ami mentes a hurkoktól. Ha valamilyen hálózati szakadás történik, akkor egy új fa struktúrát épít fel.

Előnye, hogy gyorsan lezajlik 2-10 sec. van rapid verziója is. problémái: nincsen benne semmi authentikáció illetve authorizáció nincs a protokollban beépítve. hasonlóan az ARP-hez. Nincs megszabva, hogy mennyi csomagot küldesz.



kep 8

kettő másodpercenként küldi.

célcím 01:80:C2:00:00:00 címre megy, ami egy broadcast, noha nem látszik annak.

A fa készítésének folyamata:

* Minden switch küld BPDU üzeneteket. Mindegyik switchnek van egy saját azonosítója.
* Először mindenki root akar lenni.
* Azt, hogy ki győz két érték alapján döntik el. Az első a Bridge identifier nevű szám alapértelmezés 32768 akinek kisebb, az győz.
* Ha két switchnél a Bridge identifier megegyezik, akkor a MAC address dönt. Minél alacsonyabb a MAC address, annál nagyobb a switch prioritása.
* Tehát a legkisebb Bridge identifierű és legkissebb MAC című switch fog győzni.

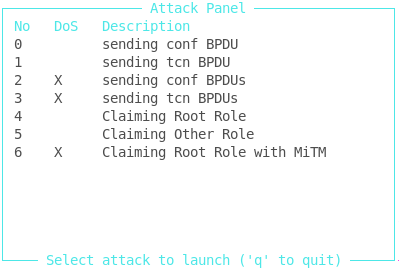
Miután kiderült ki a root csak ő küldhet BPDU-kat, két másodpercenként küldi. Azért küldi, hogy lássa minden rendben van-e. A többiek ugyanis várják. Amennyiben nem kapják meg a BPDU csomagot megfelelő időn belül úgy veszik, hogy hálózat szakadás történt, és nekilátnak, hogy újra építsék a fát az előző módszer szerint.

A switchek nem 2 sec-et várnak, hanem annyiszor 2 másodpercet, ahány hop-nyira vannak a root switchtől. Azt, hogy milyen messzire van a roottól a cost mezőben jelölik. A root switchnek 0 a költsége, amik közvetlenül a rootba vannak csatlakoztatva 1, amik ezekben vannak dugva 2… Van egy max age paraméter is, ennél tovább semmiképpen nem vár egyetlen switch sem, ha addig nem kap BPDU-t mindenképpen elkezdi az új fa kiépítését. Akkor is, ha számítás szerint még várnia kellene.

Ha hiba van Topology Change Notification üzenetet küld el.

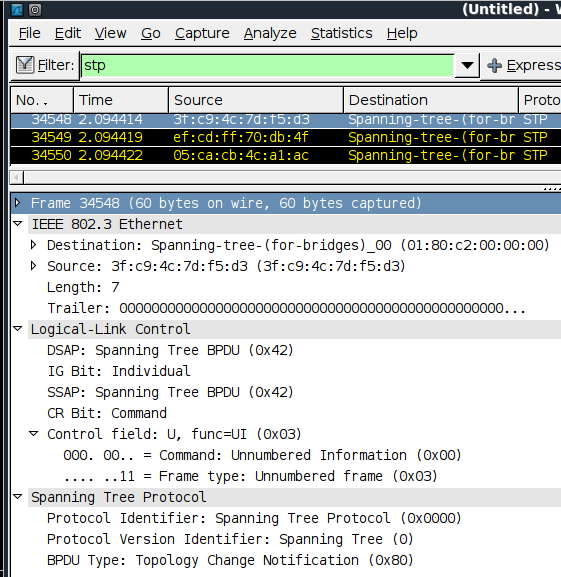
DoS támadást könnyű kivitelezni. Mivel nincs az STP protokollban semmi authentikáció.

Magát a támadást az x billentyűvel tudjuk kiválasztani.



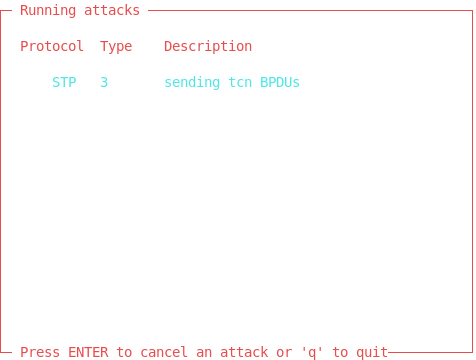
kep 9

Válasszuk a 3-as támadást. A támadás alatt change notification üzeneteket küldünk:



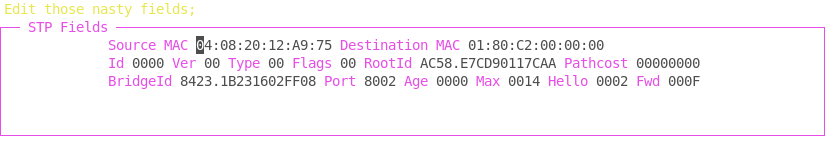
kep 10

ha elindítottuk l-el lehet listázni. a megjelenő listában kiválaszthatjuk ha több támadásunk is fut. amelyikre entert ütünk leáll.



kep 11

e billentyű lenyomásával alul szabadon szerkeszthetjük a mezőket. akkor ilyet küld a továbbiakban. Ezután ESC-cel tudunk kilépni az edit menüből.



kep 12

claiming root beáll két switch közé.

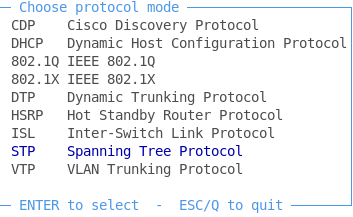
Védekezési lehetőségek:

* Megadjuk a maximálisan küldhető csomagok számát L2Rate, vagy RateLimit-nek hívják. Ezt nem csak STP-re állíthatjuk, hanem tetszőleges protokollra érvényes lehet.
* Magát az STP-t is védhetjük, hogy statikusan építjük ki. Ekkor backupra is gondolni kell, bonyolult. De lehet csak annyit megmondani, hogy melyik port a BPDU port, az csak az lehet, ami két switchet köt össze, olyan amin gép lóg nem lehet az. Tehát beállítjuk, hogy csak a switcheket összekötő porton engedem a BPDU csomagokat. Ilyenkor ügyeljünk, hogy az összes switch felé engedjük, nehogy kihagyjuk valamelyik switchet.
* BPDU filter a BPDU-t szűri, az adott portról kimenő és bejövő csomagokra is figyel. Ügyelni kell, hogy a backup portot se felejtsük engedélyezni.
* BPDUGuard csak a bejövőt forgalomban szűr.

## DHCP támadása

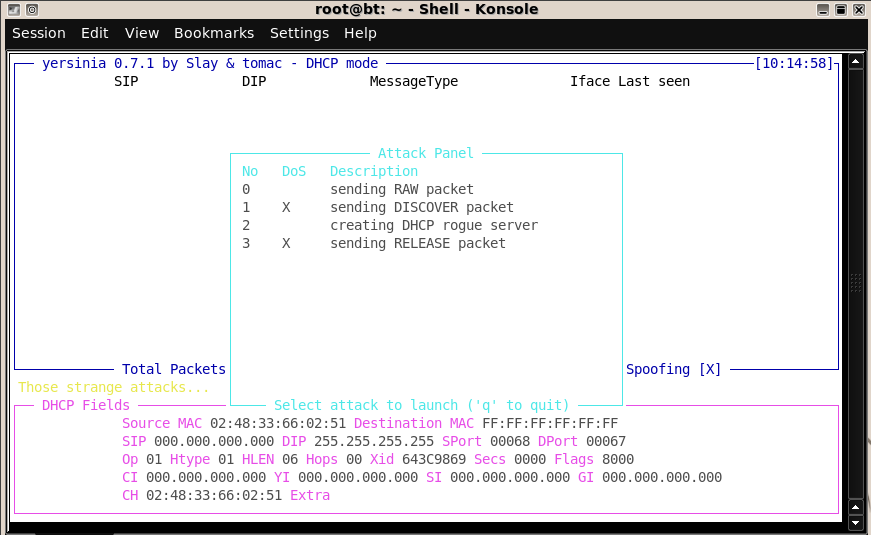
Másik tool a gobbler csak DHCP-t támad, akkor jó, ha release-nél visszakérdezhetnek a DHCP szerverek, hogy tényleg akarod-e dobni. Mert ez középre is áll, yersinea ilyet nem csinál.

A dhcp támadásához nyomjuk le a g billentyűt



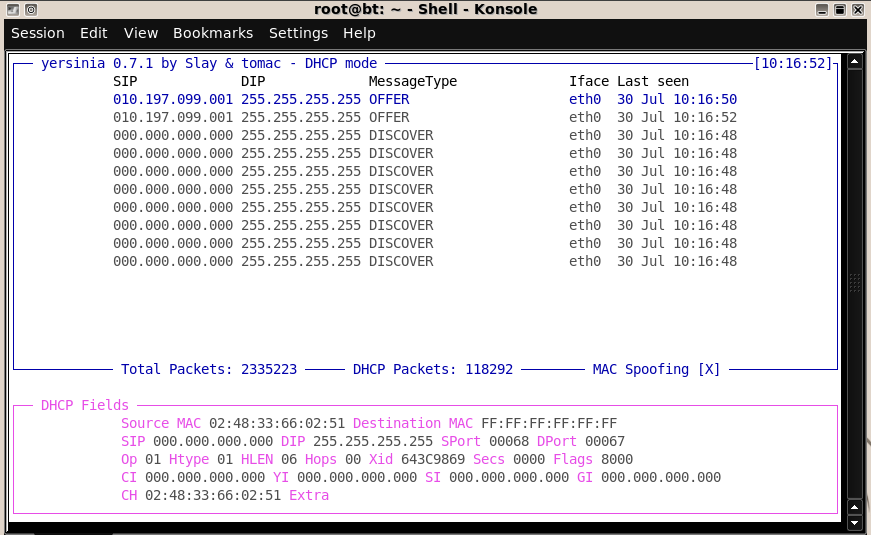
kep 13

Itt a nyilakkal válasszuk ki a DHCP protokollt, majd nyomjuk le az enter billentyűt. Ezután nyomjuk le az x billentyűt, és a megjelenő menüben:



kep 14

Itt válasszuk az 1-es parancsot, ez DHCP discover-eket küld, hamis MAC címekkel. Emiatt a DHCP szerver kiosztja az összes rendelkezésre álló IP-jét.



kep 15

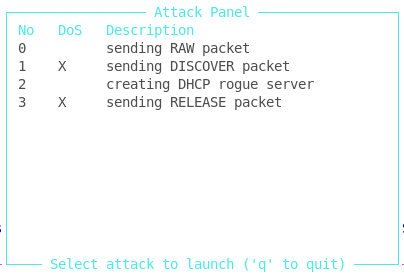
Release packet támadás. Az adott gép nevében dob egy release-t.

Védekezés:

* Be lehet kapcsolni a port security-t. ennek a szűrésére. pl. csak néhány MAC címet fogadok el. Ez nem nyújt elégséges védelmet, mert magában a BootP csomagban is van egy MAC address, és a DHCP azt nézi. Azért, mert Relay Agent sem működhetne másképpen, RFC 1542 nem működne másképpen… tehát kell. Emiatt nekem nem kell a MAC címemet hamisítani, amire a switch kidobna, hanem a BOOTP-ben lévő MAC címet változtatjuk.
* Vannak olyan megoldások (switch, gyártó függő), amik bele tudnak nézni a BOOTP-be.
* Lehet rate limiteket beállítani.

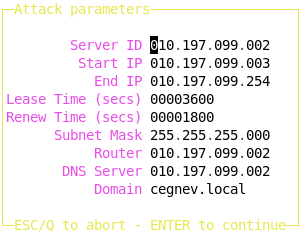
Rouge server

Ennél a támadásnál hamis DHCP-t állítok be. Így a felhasználónak én adok default Gateway-t, illetve DNS-t, így akár ARP poisoning nélkül is le lehet hallgatni a kifelé menő forgalmat. nyomjuk meg az x gombot, és válasszuk a 2-es menüpontot.



kep 16

Ez alkalommal kapunk egy új ablakot, amiben a saját hamis DHCP szerverünket feltudjuk konfigurálni:



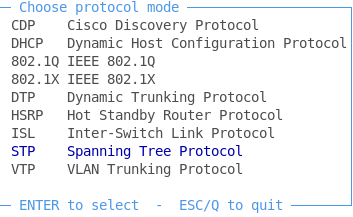
kep 17

Védekezés:

A switcheken be kell állítani, hogy melyik porton jöhet DHCP offer, ha támogat ilyet az OS-e.

## Dynamic Trunking Protokoll

Nyomjuk le a g gombot, és a megjelenő menüben válasszuk a DTP protokollt.



kep 18

A switchek portjai más-más VLAN-okba tartozhatnak.

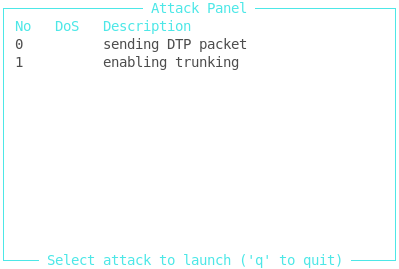
A csomagok lehetnek Tagged tehát jelölt csomagok, illetve Untagged amikor a csomagban nem jelölöm, hogy melyik VLAN-ba kell küldeni. Ilyenkor az alapértelmezett VLAN-ba tartozónak veszi.

Egy port általában egy VLAN-hoz tartozik, kivétel azok a portok, amik átjárást kell biztosítsanak a VLAN-ok között. Ezek tipikusan a switcheket összekötő portok, amiket trunk portoknak hívunk.

Illetve IP telefonoknál, ha kevés a fali csatlakozó akkor szokás, hogy telefonba dugom be a számítógépet. Ilyenkor ezeket szintén trunk portnak kell beállítani.

Manuálisan fel kell konfigurálni, hogy melyik VLAN-hoz tartozzon az adott port. Ez macerás, ezért találták ki, a DTP-t. Ez a protokoll, ha a kliens kér egy VLAN-t automatikusan definiálja a portjára. Ilyenkor annyit állítunk be, hogy milyeneket kérhet a kliens, pl. 1-3-ig lehet azon a porton. A switcheknél az szokott a DTP alap beállítás lenni, hogy bármelyiket (1-4096) kérheti a kliens, ezért ha csak bekapcsolják, akkor bármelyik portot át lehet tenni egy másik VLAN-ba.

nyomjuk le az x gombot:



kep 19

Az enabling trunking támadás olyan csomagot küld, hogy bekerüljek az összes VLAN-ba..

## VLAN

802.1q általános VLAN protokoll. ennek a régi ciscos megfelelője a ISL Inter-Switch Trunking protokoll.

Az összes portra csak sima IP csomag jöhet be. A switch portra beérkezik az IP csomag, a switch hozzátesz egy VLAN headert. A másik port mielőtt tovább küldi a gépnek a megkapott csomagot leszedi a VLAN headert.

0

Access port, ami egy VLAN-hoz tartozik. Csak olyan csomag jöhet, amiben nincs VLAN header, vagy az megegyezik a port default VLAN-jával.

az ethernet fejlécben 0x8100 jelöli a VLAN csomagot.

VLANID

12 bit

priority,

ethertype:

2 byte 0x8100

Minden switchen van egy default VLAN, ha nincs a headerben VLAN info ebbe teszi be.

default az 5-ös. default a 10-es

gép

ha a gép küld egy csomagot egy másik switchen lévő gépnek, akkor az történik, hogy a bejövő IP csomagba beteszi a default VLAN ID-t (5). Mivel másik switchen van a másik gép, ezért a trunk portra megy a csomag. Ott a VLAN ID lekerül a csomagról, mivel megegyezik a defaulttal. így megy át a másik switchre, tehát ott nem lesz VLAN fejléc. Mivel a másik switchen 10 a default VLAN, azért ezt teszi be. Ezt a konfigurációs hibát nevezzük Default VLAN Mismach-nak.

## Double encaptulation packet

Que-in-que-nak is szokták hívni, ekkor két header van egymás után:

ethertype:

2 byte 0x8100

VLANID 2

12 bit

priority,

priority

3 bit

VLANID 1

12 bit

ethertype:

2 byte 0x8100

Ha ki van javítva az előző Default VLAN Mismach hiba:

default 5 default 5

gép

ha egy másik VLAN-ban lévő gépnek akarok csomagot küldeni mit kell tennem:

az első headerbe beállítom VLAN ID-nek a defaultot, másodiknak pedik a cél VLAN-t.

Ekkor ahogy bejön a csomag a default VLAN ID-t leszedi. tehát csak a másik marad ott.

Átkerül ez a csomag a trunk portra. ott mivel már nem a default VLAN van a fejlécben nem vágja le. Így kerül át a másik switchre, ami továbbítja a cél VLAN-ba, mert azt hiszi, hogy jogosan oda való.

VOIP hopper figyeli a CDP csomagokat a hálózaton. Ezekdől ki tudja szedni a VLAN-okat. És megpróbálja engedélyezni a trunkölést a te portodra. Ha sikerül automatikusan felhúz egy interface-t, ami a többi VLAN-ba tartozik.

Védekezés, hogy semmilyen VLAN ID-t (defaultot se) szedje le.

## VTP

Egy központi switch leküldi a VLAN beállításokat a többi switchnek.

## Ettercap

Naplózás. saját napló file formátuma van, célszerű megadni, hogy logoljon, hogy később is megnézhessük mik voltak.

Az ettercap leadja a root jogosultságot alapból. nobody-ként fut. Ilyenkor nem tudunk például SSL main int he middle-t csinálni. Hogy az is sikerüljön az ettercap.conf filet, ami alapból a /etc/ettercap.conf helyen található be kell állítsuk.

EC\_UID=0

EC\_GUIR=0

kell legyen, és az iptables elől ki kell venni a komment jelet.

## Hping

adó oldal:

fogadó oldal: hping3 -1 -9 -d 1500 -r titok

## Kismet

iwconfig írja ki a létező hálókártyákat. A kártyát át kell kapcsolni monitor módba. iwconfig wlan0 mode Monitor.

Általában az lspci parancs megmondja, hogy milyen wireless kártya van a gépben.

drone az adatgyűjtést végzi, továbbítja a kismet szerverek. ehhez kapcsolódik a támadó.

kismet.conf /usr/etc/kismet.conf

ott a hálókártyát be kell állítani, leírás a <http://kismetwireless.net/> weboldalon található.

ncsource paramétert

## cowpatty