# Tema 3 - ARP Cache Poisoning

**Securitatea Informației - 7 Ianuarie, 2022**

Burcă D.D. Paul, grupa B4, anul III

## 1 Despre

În orice rețea de calculatoare este foarte important ca datele sa fie transmise corect la destinație și să nu poată fi interceptate de persoane neautorizate (posibili atacatori). Cel mai întâlnit atac este **ARP cache poisoning** sau numit și **ARP spoofing**. ARP poisoning presupune folosirea de tabla ARP pentru redirectionarea transferului de date dintre 2 calculatoare prin intermediul acesuia (de la asta si numele de atac **"Man in the middle"**).

În cadrul unui atac de obiecei are loc și sniffing. **Sniffing-ul** reprezintă procesul de capturare (într-un fișier) și analizare a traficului cu scopul de a detecta diverse informații trimise printr-o rețea. Utilitarele folosite pentru sniffing se numesc sniffere sau analizatoare de protocoale, deoarece prin intermediul lor sunt analizate pachetele transmise prin rețea, apoi sunt capturate parolele, sau alte date confidențiale.

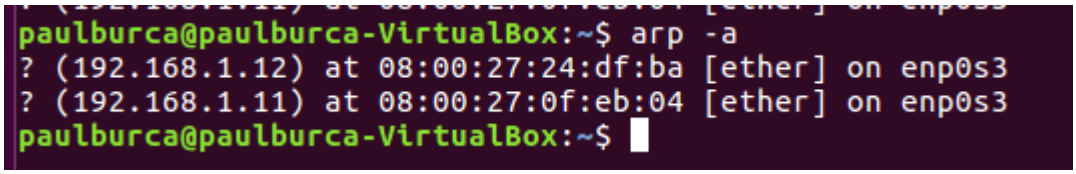
O metodă de a limita capacitatea atacurilor ce folosesc un packet sniffer de a obţine informaţii din reteaua interna este prin intermediul **switch-urilor**, dar atacul ARP poisoning tot reușește sa capteze datele dintre 2 calculatoare.

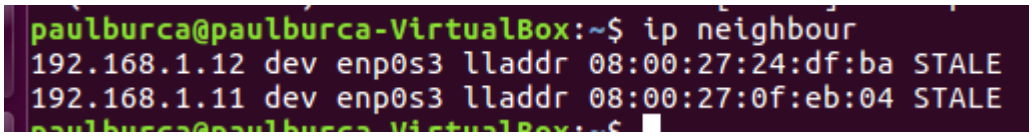
Acest atac se folosește de **ARP**. **ARP** reprezintă **Address Resolution Protocol**. Scopul acestui protocol este acela de a permite fiecărui sistem din reţea să-şi construiască o tabelă de mapări între adresele de IP şi cele fizice. Acest set de mapări este cunoscut sub numele de ARP cache sau tabela ARP.

Dacă un sistem doreşte să transmită un pachet către un alt sistem aflat în aceeaşi reţea, acesta va verifica în primul rând tabela ARP. Dacă nu este gasită maparea dorită, sistemul va trebui să invoce protocolul ARP şi va face acest lucru prin transmiterea unei cereri ARP prin reţea (prin difuzare). Această cerere conţine adresa IP dorită. Fiecare sistem receptionează această cerere şi verifică dacă se potriveşte cu propria adresa IP. Dacă se potriveşte, sistemul implicat va trimite un mesaj de răspuns care conţine adresa de nivel legatură de date. Sursa cererii va adăuga şi această informaţie în propria tabelă ARP.

Există două tipuri de înregistrări ARP: statice şi dinamice. De cele mai multe ori, se folosesc intrările dinamice ARP. Asta înseamnă că înregistrarea ARP (MAC-IP) este păstrată pe un

dispozitiv atât timp cât acesta este utilizat. O înregistrare statică ARP presupune introducerea manuală a legăturii dintre adresa MAC şi adresa IP. Cache-ul ARP poate fi vizualizat prin folosirea comenzii "**arp −a**" sau "**ip neighbour**" din linie de comandă. Ieşirea comenzii va fi asemănătoare cu cea de mai jos:




# 2 Atacul în sine

## 2.1 Detalii despre rețea

Rețeaua este structurata astfel:

**Atacatorul (C1):**

**IP:** 192.168.1.12

**MAC:** 08:00:27:24:df:ba

**Victima 1 (C2):**

**IP:** 192.168.1.13

**MAC:** 08:00:27:32:f1:fd

**Victima 2 (Router)[Gateway]:**

**IP:** 192.168.1.13

**MAC:** 08:00:27:0f:eb:04

## 2.2 Ce se întâmplă și cum afectează victimele

Staţia C1 va trimite două pachete ARP de tip răspuns fals: o dată pentru staţia C2 în care se specifică că adresă MAC a staţiei Router este 08:00:27:24:df:ba, şi o dată pentru staţia Router, în care se specifică faptul că adresa MAC a staţiei C2 este tot 08:00:27:24:df:ba. Astfel, atunci când staţia C2 doreşte să transmită un pachet staţiei Router, îl va transmite staţiei C1. La fel,

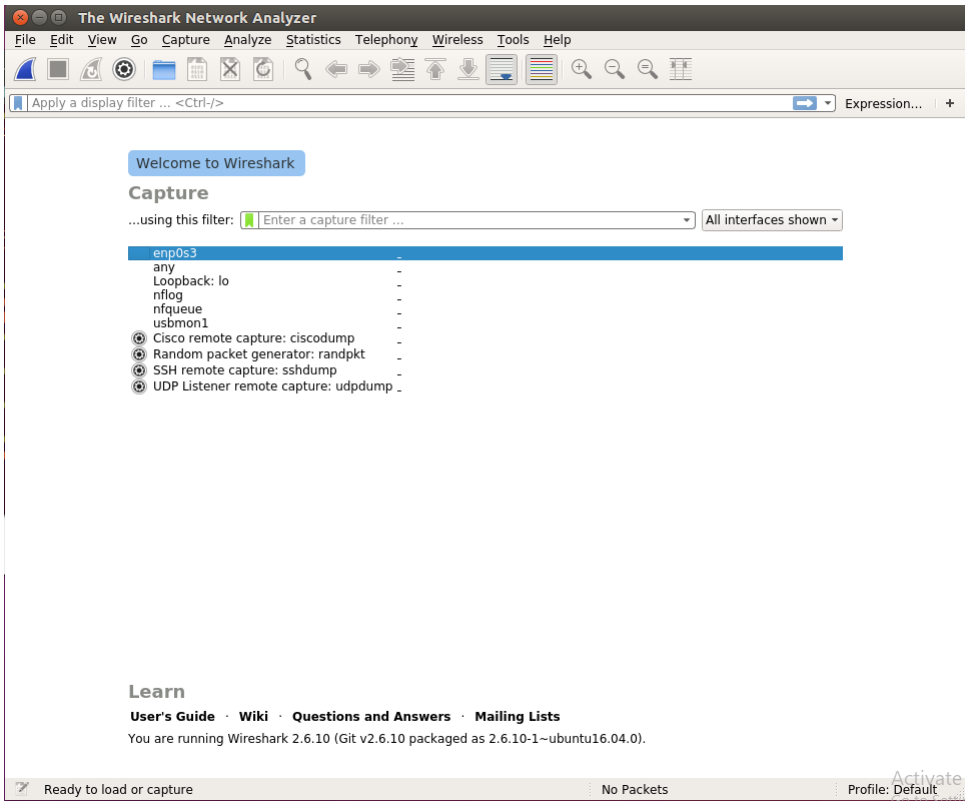
atunci când staţia Router doreşte să transmită un pachet staţiei C2, îl va transmite tot staţiei C1.

Pentru ca procesul să funcţioneze, staţia C1 va trebui să trimită pachetele primite staţiilor care sunt adresate. În plus, C1 trebuie să retrimită pachetele ARP false la intervale regulate. Aceasta pentru că intrările din tabela ARP sunt evacuate după un timp, caz în care staţia va trimite un pachet ARP de interogare. Dacă staţia interogată răspunde, intrarea din tabela ARP va fi actualizată şi traficul nu va mai ajunge la C1.

## 2.3 Pașii acestui atac într-un sistem Linux Debian (Ubuntu în cazul meu)

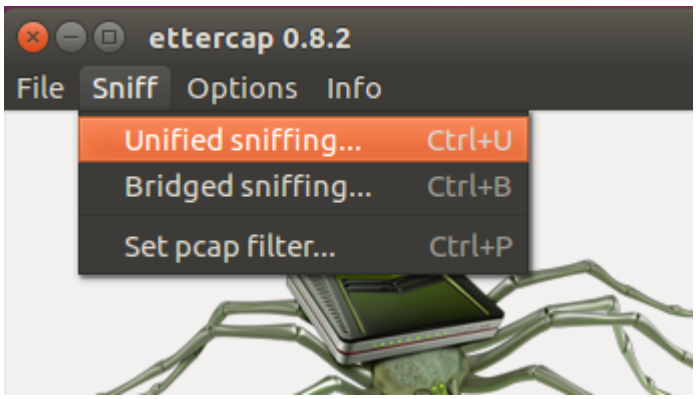
Pentru acest atac m-am folosit de Ettercap-graphical (pentru sniffing și atacul în sine):

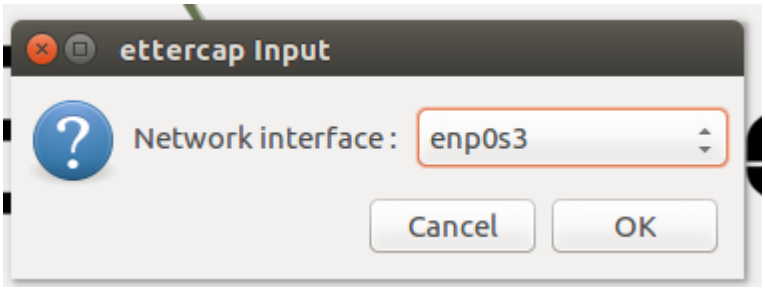

și Wireshark (pentru monitorizarea traficului și observarea efectului atacului asupra rețelei):




### 2.3.1 Pornirea sniffing-ului

După ce pornim utilitarul Ettercap-graphical, apasăm tab-ul Sniff, alegem Unified Sniffing și alegem adaptorul de rețea care facea conexiunea la rețeaua locală.



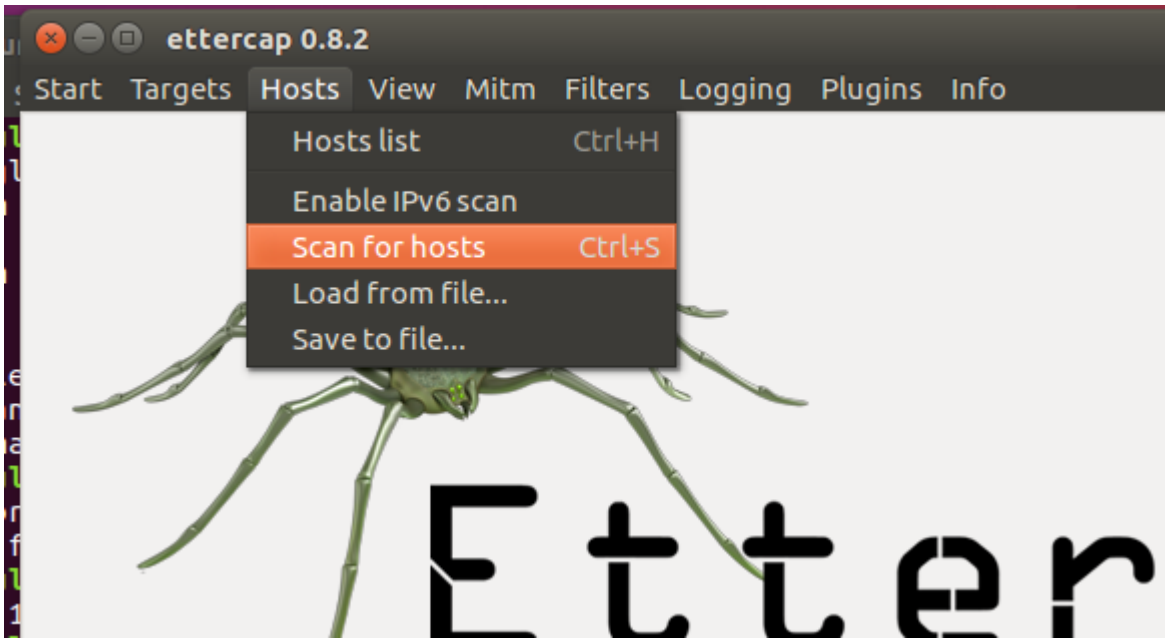



După aceea vom avea anumite detalii afișate în casuța din partea de jos:

```
Listening on:
enp0s3 → 08:00:27:24:DF:BA
        192.168.1.12/255.255.255.0
        fe80::a00:27ff:fe24:dfba/64
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/all/use_tempaddr is not set
to 0.
Privileges dropped to EUID 65534 EGID 65534...
  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

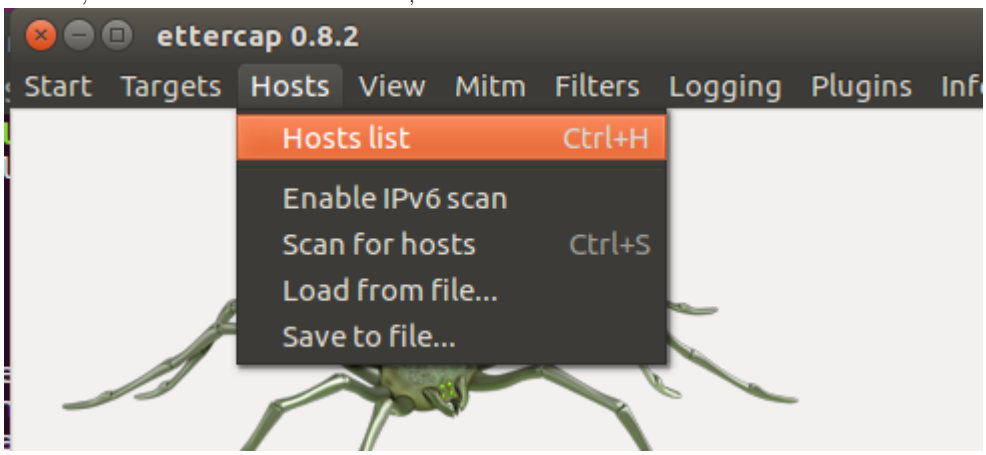
### 2.3.2 Selectarea calculatoarelor către vor face atacul

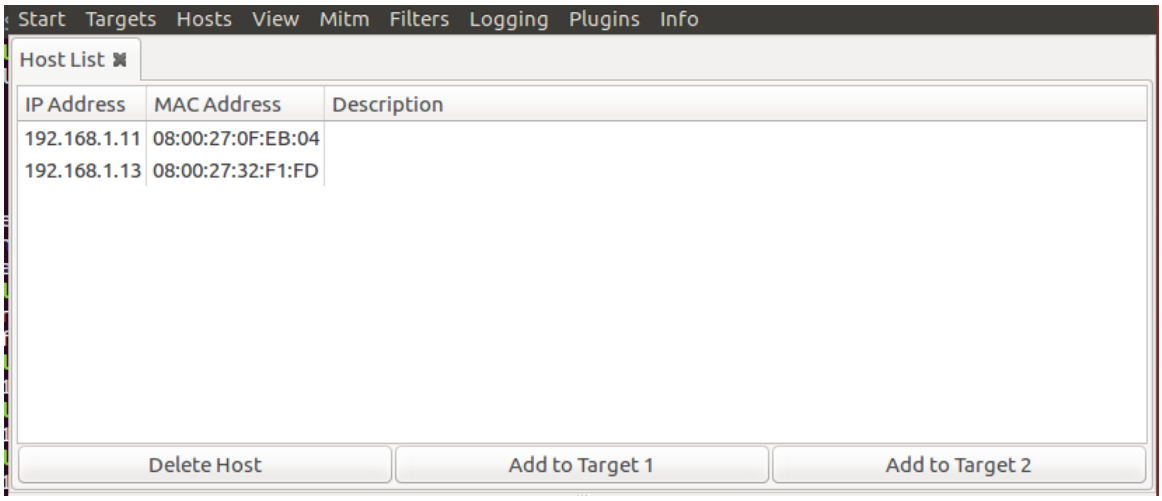
În tab-ul Hosts, vom alege "Scan for hosts" pentru decoperirea tutoror calculatoarelor din rețea.




| |
|---|
| Randomizing 255 hosts for scanning... |
| Scanning the whole netmask for 255 hosts... |
| 2 hosts added to the hosts list... |

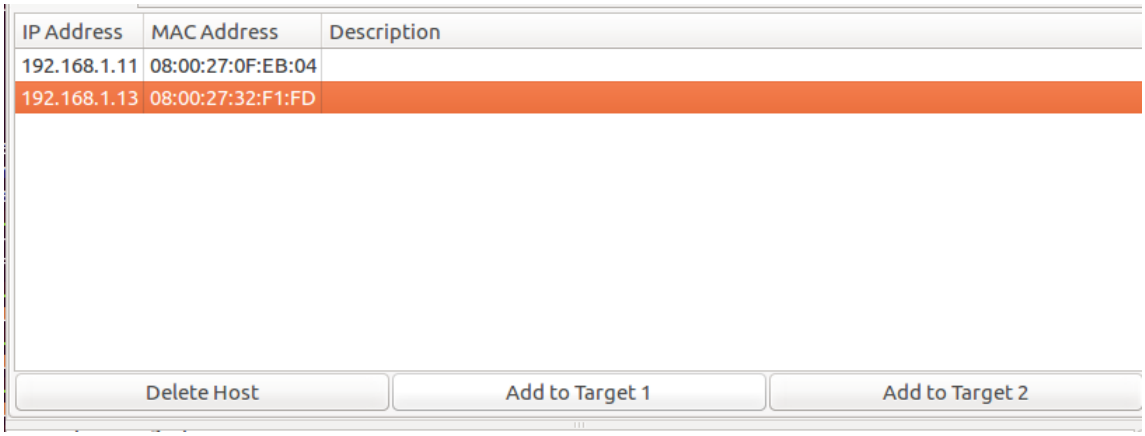
După aceea, to în acel tab vom avea și "Hosts list".

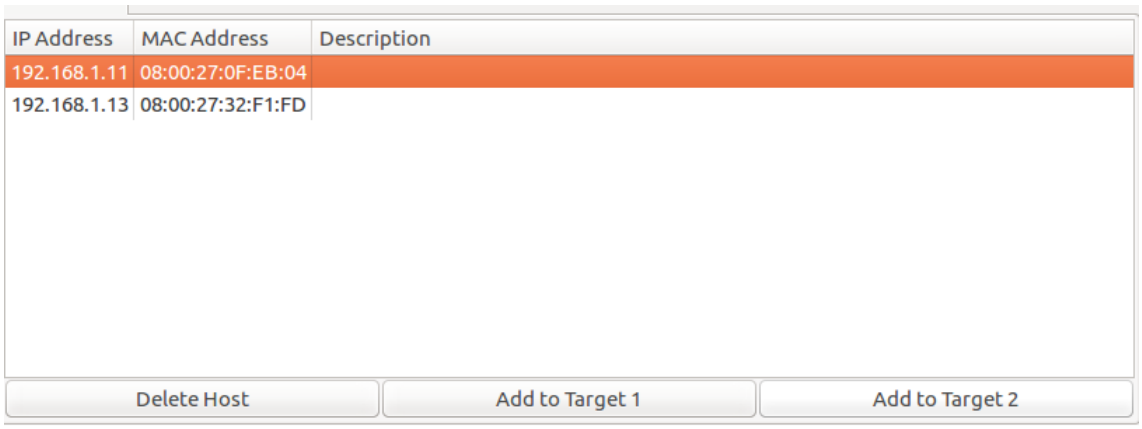





În acest meniu vom selecta ca Target1 și Target2 victimile noaste.

În cazul meu 192.168.1.11 și 192.168.1.13:



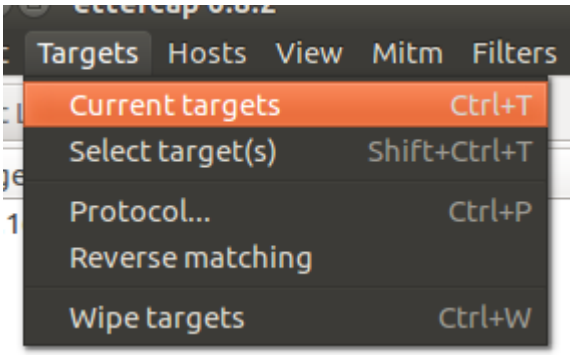



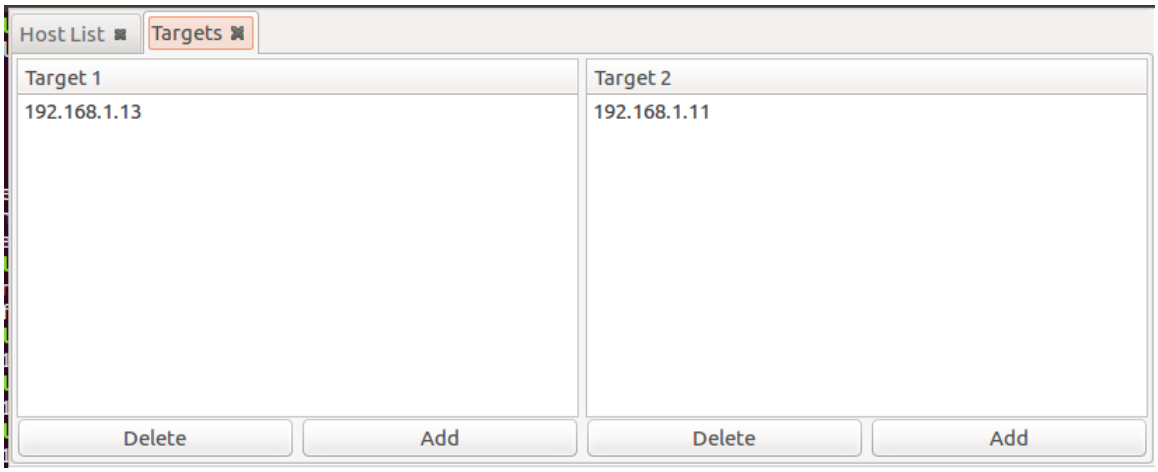

Mesaj ettercap:

| |
|---|
| Host 192.168.1.13 added to TARGET1<br>Host 192.168.1.11 added to TARGET2 |

Pentru a putea vedea toate victimele, vom merge la meniul Targets și vom selecta ”Current

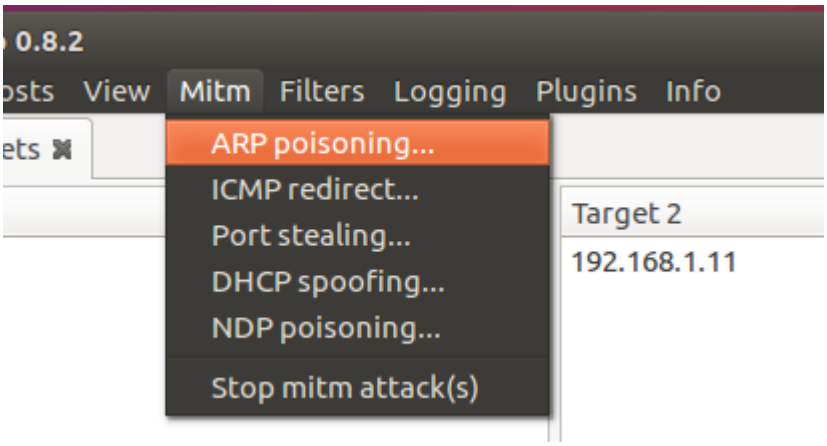
targets”:

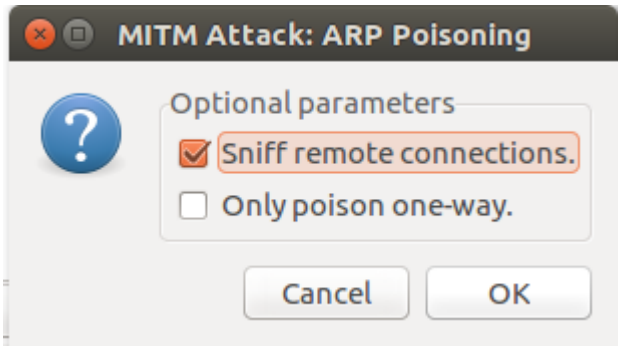



### 2.3.3 Pornirea atacului

În tab-ul Mitm selectam ARP poisoning, după bifăm opțiunea de ”Sniff remote connections” și apăsăm Ok. În acest moment atacul a început.



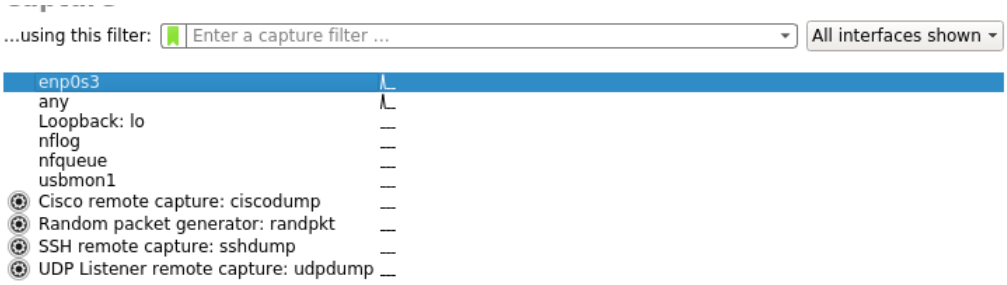


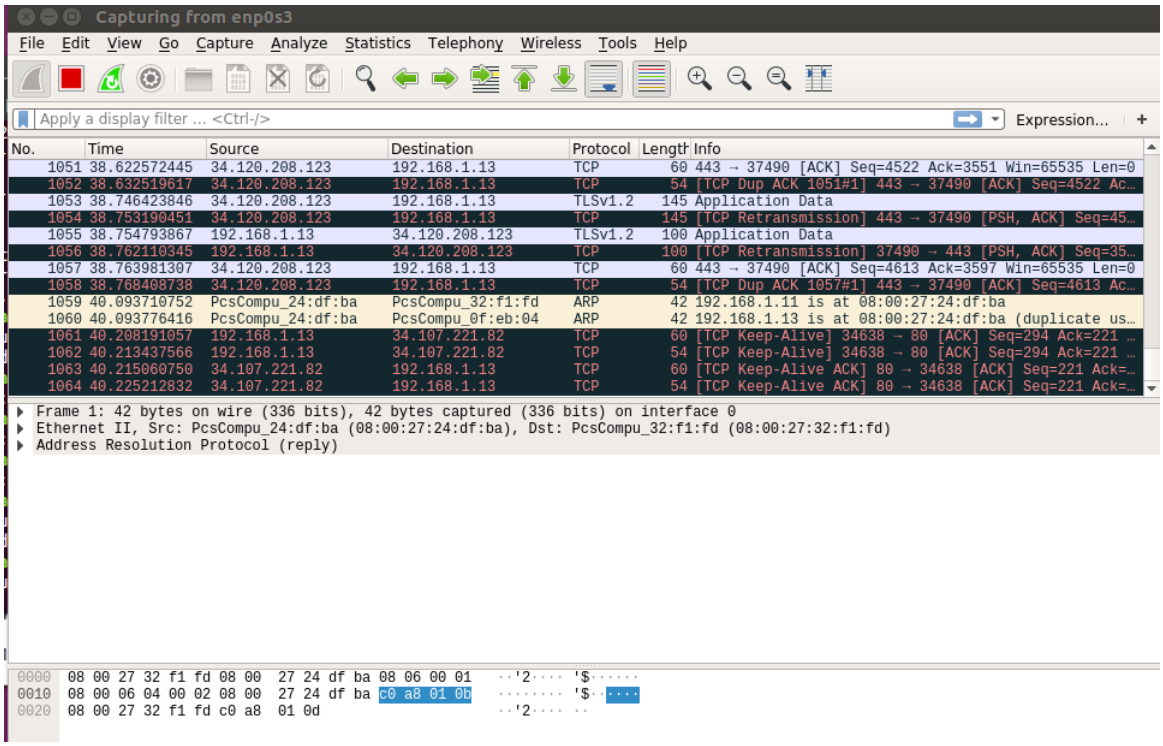

Mesaj ettercap:

| ARP poisoning victims: |
| --- |
| GROUP 1 : 192.168.1.13 08:00:27:32:F1:FD |
| GROUP 2 : 192.168.1.11 08:00:27:0F:EB:04 |

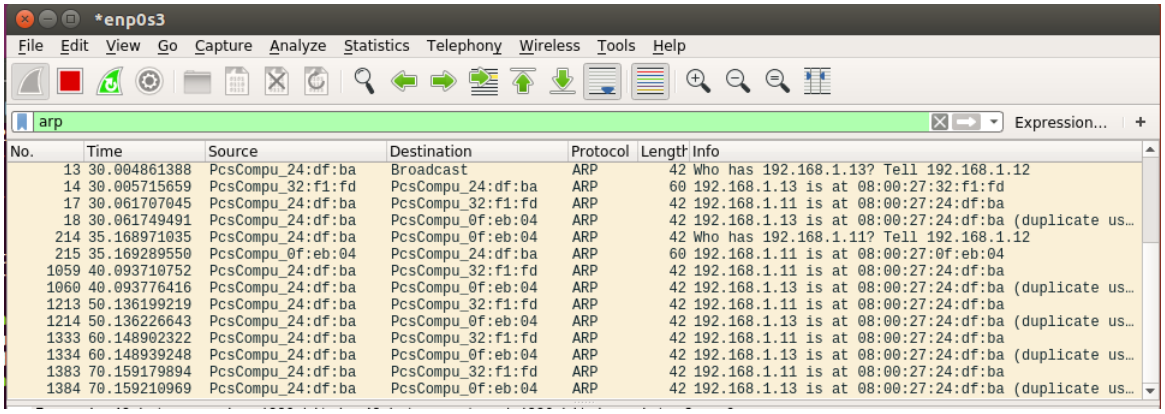
## 2.4 Vizalizarea efectului asupra retelei

Ori în cadrul unei victime ori în cadrul atacatorului putem folosi Wireshark pentru a vedea efectul. După ce am pornit utilitarul Wireshark (de preferat ca root), vom selecta adaptorul de rețea care face conexiune la rețeaua locală și vom începe observarea în cadrul rețelei respective a diferitelor procese.

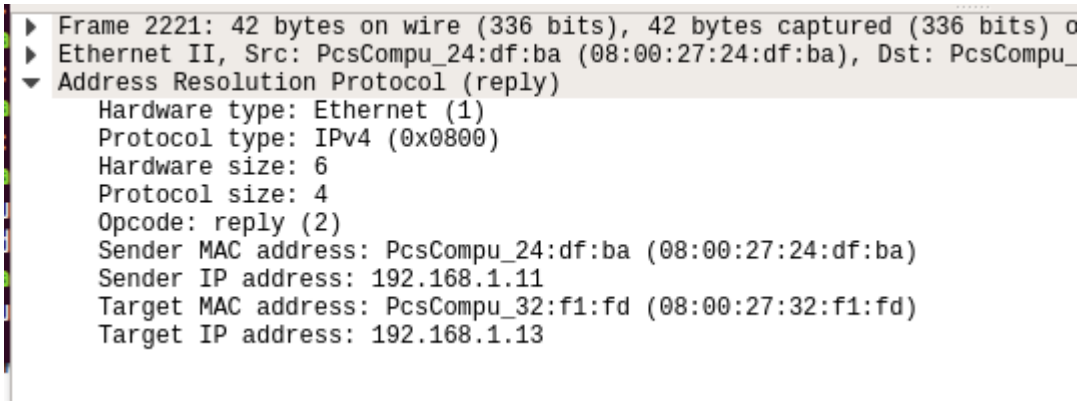




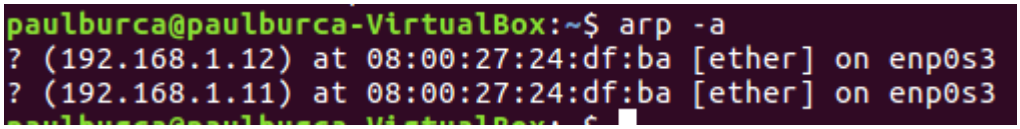

Pentru a vedea mai bine ce se întamplă putem scrie ”arp” în bara de sus (bara de filtrare) și toate procesele vor fi doar la request-uri și răspunsuri ARP:




Un lucru se il putem observa dupa o perioada e faptul ca request-urile ARP catre C2 vor fi trimise pe adresa MAC a lui C1, dar IP-ul fiind cel al router-ului.



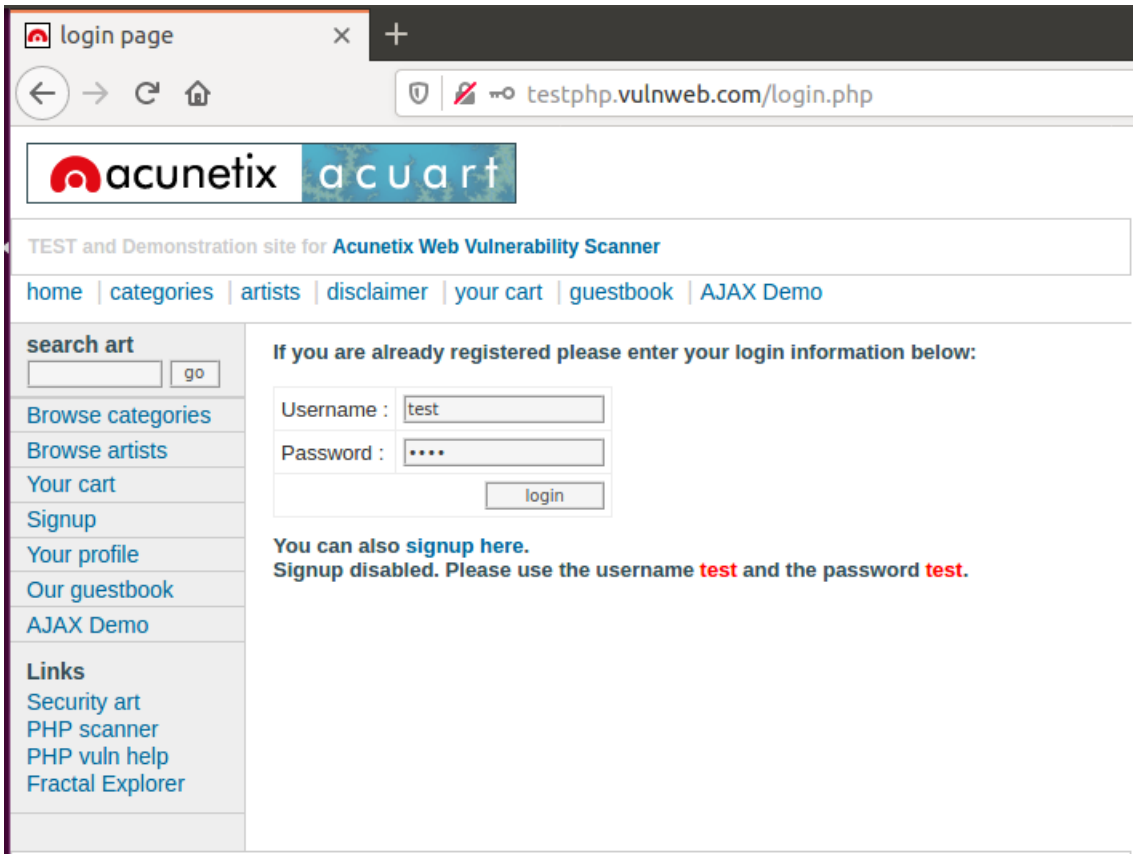

Un alt efect este ca în cadrul tabelei ARP, Router-ul este trecut cu adresa MAC a lui C1.




## 2.5 Capturarea datelor transmise

Se poate observa că în cazul în care ne vom loga online pe un site care nu folosește un protocol sigur (folosește http), acele date de conectare vor fi salvate și afisate in utilitar de Ettercap (sniffer-ul acestuia), iar în cazul în care folosește un protocol sigur (https), nu se va afișa nimic.

Pentru a demonstra acest lucru, am intrat pe site-ul `http://testphp.vulnweb.com/login.php` (site special făcut pentru teste și care ne dă posibilitatea de a testa cazul anterior amintit) pe mașina virtuală C2.




Vom vedea ca imediat după ce ne logăm sau vom încerca să ne logăm, în utilitarul ettercat din C1 se afișează datele referitoare la logare, așa cum am zis anterior.

```
HTTP : 44.228.249.3:80 -> USER: test  PASS: test  INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test
```

# 3 Concluzii

## 3.1 Realitatea despre acest atac

În ziua de azi acest atac este puțin folosit, deoarece datele pe care le-am putea obține sunt cel mai probabil criptate sau pur și simplu atacul nu va putea funcționa din cauza diverselor măsuri luate atât la nivelul stațiilor respective cât și în cadrul rețelei. Dacă am fi într-o rețea care nu are implementate niciun fel de măsuri contra acestui atac și victima ar accesa site-uri nesecurizate (http - datele transmise nu ar fi criptate), ar fi fost ușor să obținem o cantitate mare de informații de la victima noastră și acest atac ar fi fost și greu detectabil.

### 3.2 Cum ne putem proteja

Una dintre metodele de prevenire a acestui tip de atac o reprezintă criptarea traficului. Dacă se foloseşte o criptare cu cheie partajată, se obţine un oarecare grad de securitate. În schimb, dacă se foloseşte o criptare fără cheie partajată şi fără autentificare, în care cheia de criptare se derivă prin schimbul de informaţii între cele două staţii, gradul de securitate este zero (atacatorul va stabili două canale de comunicaţie, cu fiecare dintre cele două staţi, şi chiar dacă acele canale sunt criptate, atacatorul are toate informaţiile necesare pentru decriptare). Pentru prevenirea unui atac de tip ARP poisoning trebuie monitorizat tot traficul ARP din reţeaua locală atât la nivelul dispozitivelor de interconectare folosind switch-uri ce implementeaza ARP inspection (interceptează şi validează cererile şi răspunsurile ARP), cât şi la nivelul staţiilor folosind programe de genul ARP Watch pentru a detecta eventualele schimbări în asocierile IP - MAC. În acelaşi timp, pentru destinaţiile importante (pentru gateway) se recomandă folosirea de asocieri statice în tabela ARP.

### 3.3 Cazul de eșec

Atacul poate să eșueze dacă luăm în considerare măsurile de protejare contra acesui atac amintite anterior. Dacă traficul este criptat, teoretic atacul încă funcționează, dar nu putem folosi datele, iar în celelalte cazuri în care folosim tool-uri referitoare la ARP, în acest caz, atacul chiar eșuează, atacatorul nereușind să modifice tabela ARP a victimelor, datele nefiind transmise prin atacator, astfel rezultând ca în cadrul rețelei datele să fie transmise în mod normal (ca înainte de încercarea de atac) și atactorul să nu fie capabil să obțină date.

## 4 Bibliografie


- `https://profs.info.uaic.ro/~liliana.cojocaru/LUMINITA_DEFTA.pdf`
- `https://profs.info.uaic.ro/~liliana.cojocaru/Lab11.pdf`
- `https://www.youtube.com/watch?v=3UD738uE7T`
- `https://www.youtube.com/watch?v=A7nih6SANYs`