Atacul ARP cache poisoning

ARP reprezintă Address Resolution Protocol. Scopul acestui protocol este acela de a permite fiecărui sistem din rețea să-și construiască o tabelă de mapări între adresele IP și cele MAC. Dacă un sistem dorește să transmită un pachet către un alt sistem aflat în aceeași rețea, acesta va verifica în primul rând tabela ARP. Dacă nu este găsită maparea dorită, sistemul va trebui să invoce protocolul ARP și va face acest lucru prin transmiterea unei cereri ARP prin rețea. Această cerere conține adresa IP dorită. Fiecare sistem recepționează această cerere și verifică dacă se potrivește cu propria adresa IP. Dacă se potrivește, sistemul implicat va trimite un mesaj de răspuns care conține adresa MAC. Acest set de mapări este cunoscut sub numele de ARP cache sau tabela ARP.

Atacul ARP cache poisoning se bazează pe faptul că protocolul ARP nu face autentificare, astfel că poate să primească replay-uri ARP (este „bombardat” cu astfel de replay-uri), fără ca acesta să le fi făcut și prin urmare să actualizeze cache-ul ARP cu informația primită. Astfel folosind ARP poisoning, traficul dintre două calculatoare poate fi interceptat. Această metodă este cunoscută ca Attack-Man-The-Middle. Prin acest tip de atac, stațiile afectate dintr-o rețea vor ajunge să aibă intrări eronate în tabela ARP, iar atacatorul dacă a reușit să-și conecteze adresa MAC la o adresă IP autentică, va începe să primească orice date care pot fi accesate de acea adresă IP.

1. Configurarea mediului de lucru

Pentru implementarea atacului ARP cache poisoning am clonat 3 mașini virtuale ce rulează pe Lubuntu 14.04.6 LTS, pe care le-am numit astfel: Router (observatorul), C1(atacatorul) și C2(victima). Mașini virtuale care au fost configurate după cum a fost specificat în documentul [config\_retea.pdf](https://profs.info.uaic.ro/~nica.anca/is/config_retea.pdf).

|  |  |  |  |
| --- | --- | --- | --- |
| Tipul mașinii | IP address | MAC address | Rol |
| VM Router | 192.168.1.11 | 08:00:27:df:21:ed | Observator |
| VM C1 | 192.168.1.12 | 08:00:27:b5:cb:2d | Victima |
| VM C2 | 192.168.1.13 | 08:00:27:fb:ab:b5 | Atacator |

Aplicații/utilitare folosite:

* wireshark: pentru observarea traficului din rețea

sudo apt-get install wireshark-qt

113 sudo apt-get install libqt5gui5

114 sudo apt-get install libqt5gui5-gles

115 sudo apt-get install libqt5multimedia5

116 sudo apt-get install libqt5printsupport5

117 sudo apt-get install libqt5widgets5

118 sudo apt-get install libqt5multimedia5-plugins

119 sudo apt-get install wireshark-qt

120 sudo apt-get install wireshark

* ettercap: pentru inițializarea atacului

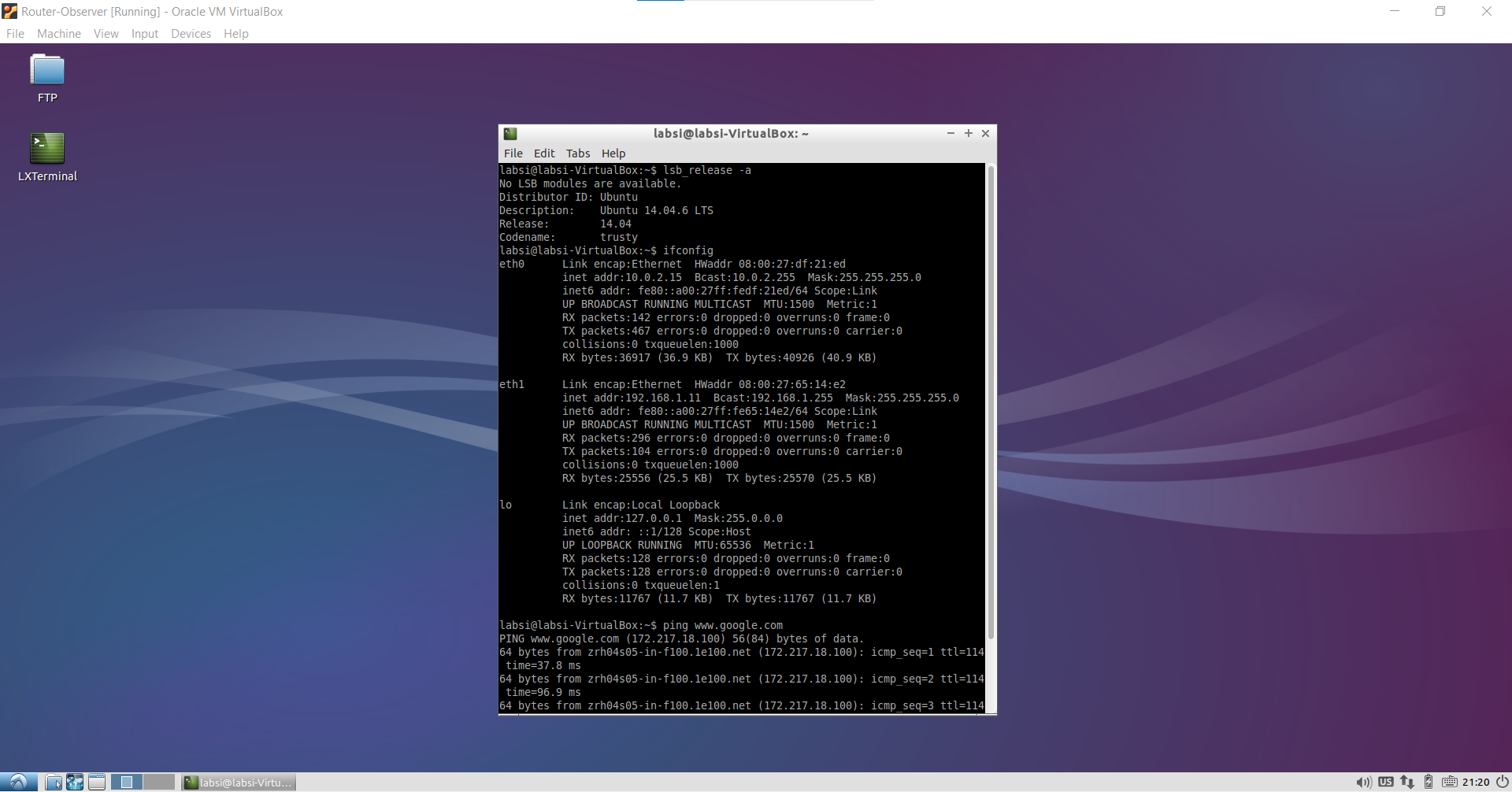
sudo apt-get install ettercap ettercap-gtk

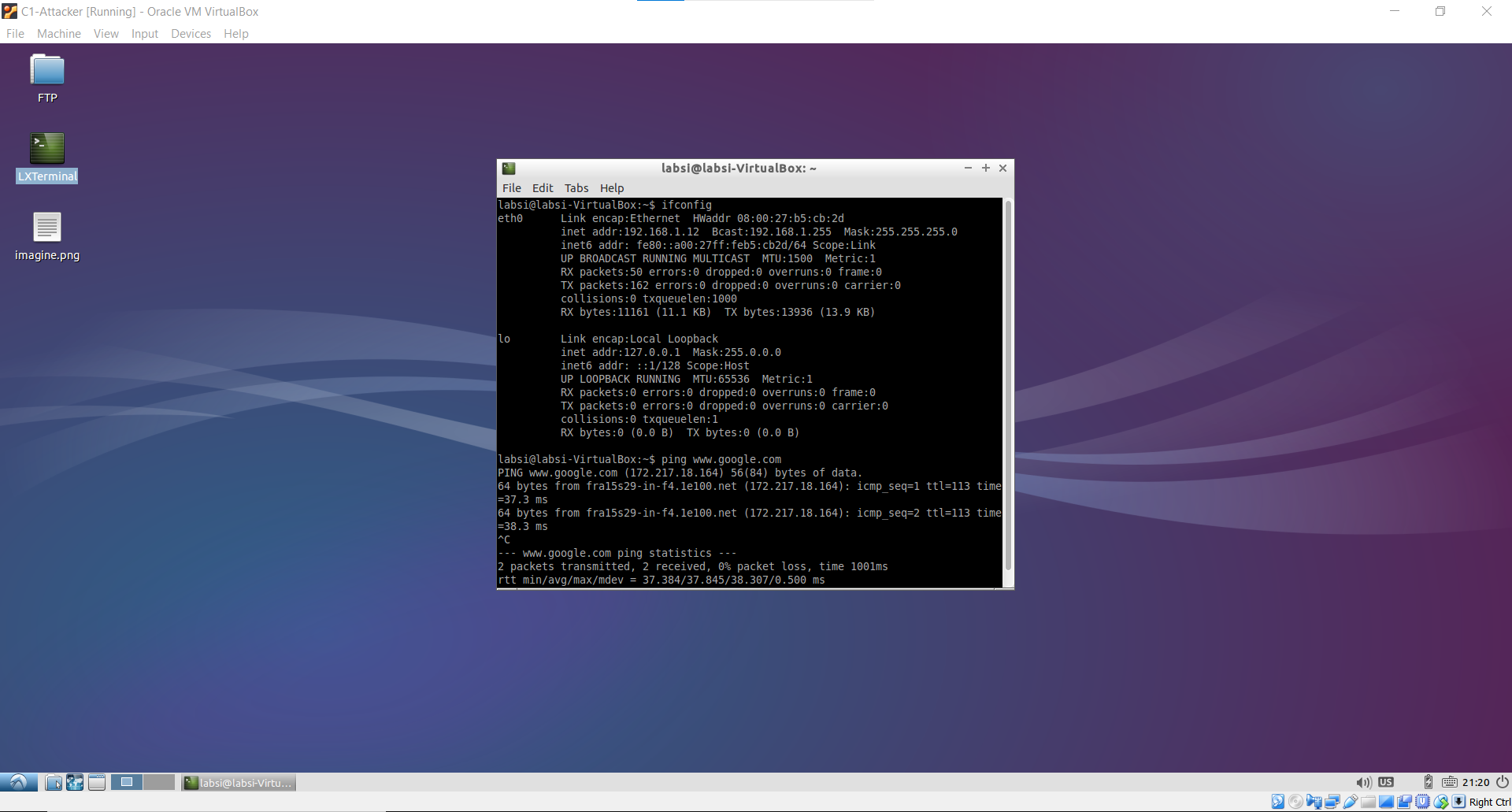
188 sudo apt install ettercap-common

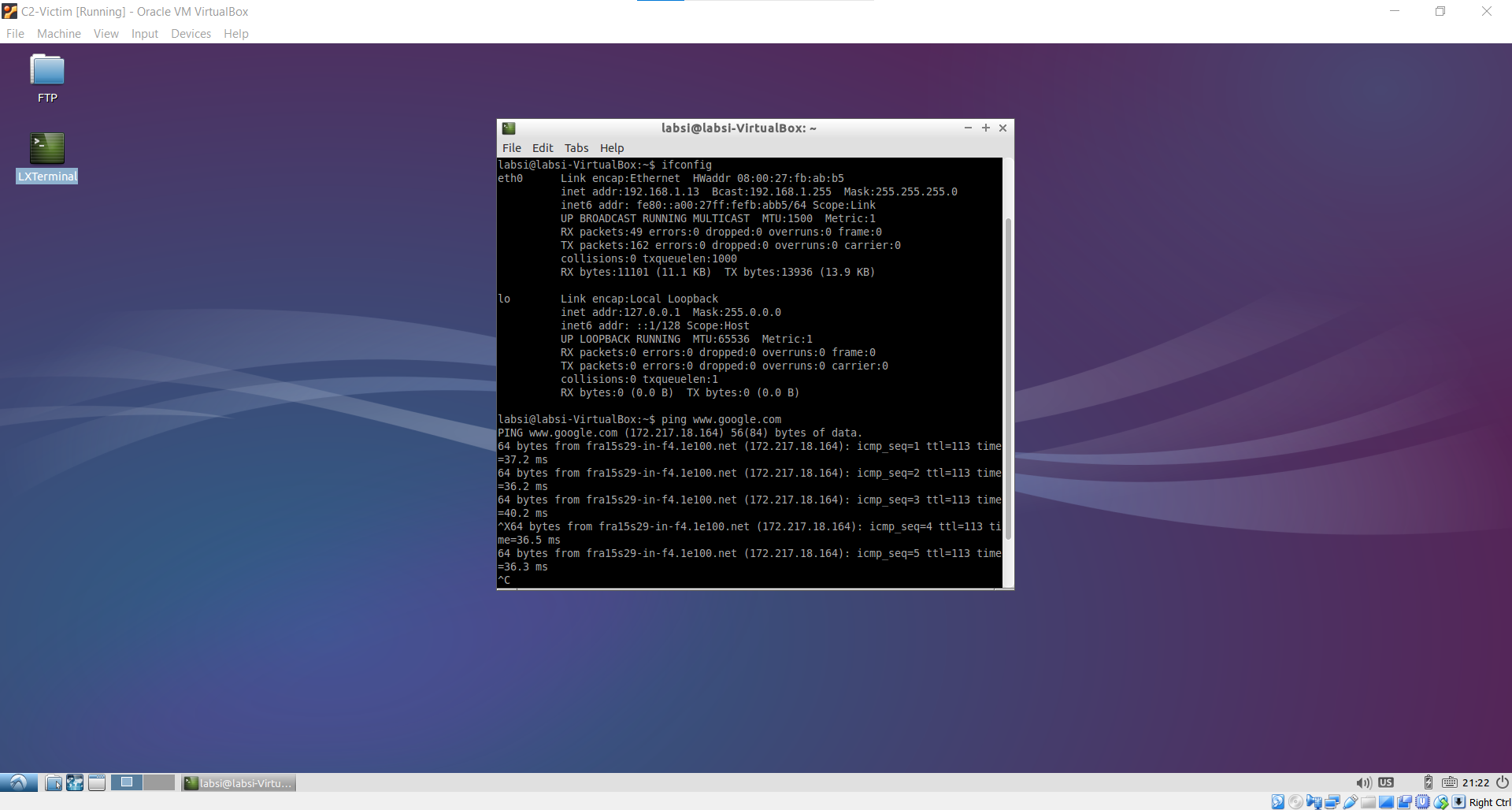
189 ettercap -g

190 ettercap -G

* vsftpd: crearea unui server FTP și transmiterea de fișiere între mașini







1. Configurația serverului FTP

FTP (File Transfer Protocol) este un protocol utilizat pentru accesul la fișiere aflate pe servere din rețele de calculatoare particulare sau din Internet.

Prima dată vom actualiza sistemul prin comanda:

sudo apt-get upgrade

Apoi vom instala framework-ul FTP astfel:

sudo apt-get install vsftpd

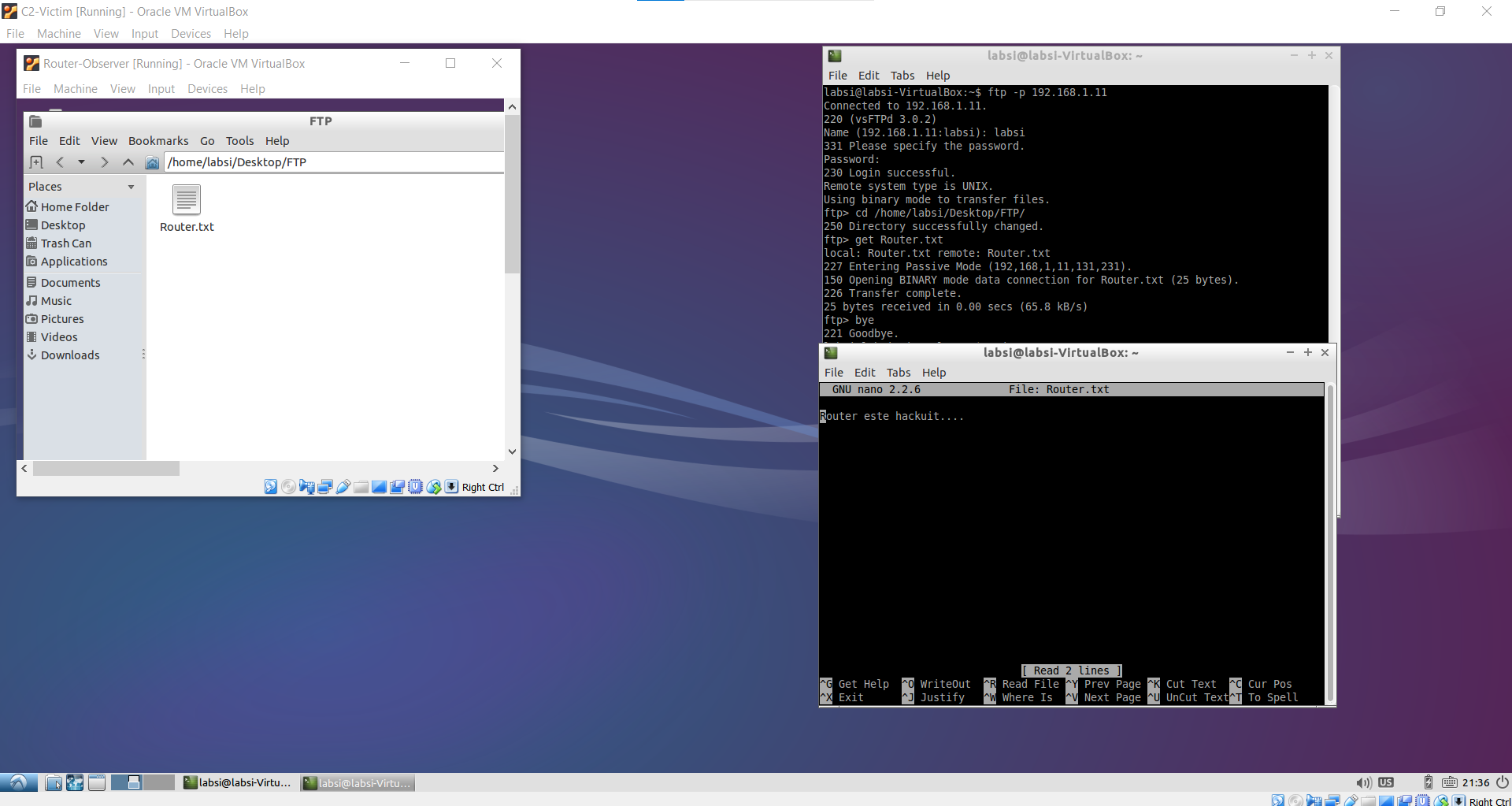
Și vom edita fișierul vsftpd.conf pentru a activa sau dezactiva unele caracteristici astfel:

sudo apt-get install vsftpd

Caracteristici care sa ne permită de exemplu, configurarea accesului la server a utilizatorilor sau ca utilizatori locali să poată să se conecteze la serverul ftp, să urce fișiere, să nu acceseze directoare ce nu le sunt permise sau configurarea accesului la server a utilizatorilor.

Pentru a ne conecta la server și a lua un fișier, de exemplu de pe Router vom folosi urmatoarele comenzi: ftp -p 192.168.1.1

La server ne vom conecta cu user-ul: labsi și parola: labsi. Ne vom situa în directorul de unde dorim sa luam fisierul și cu comanda: get Router.txt se va copia fisierul respectiv pe mașina victima.



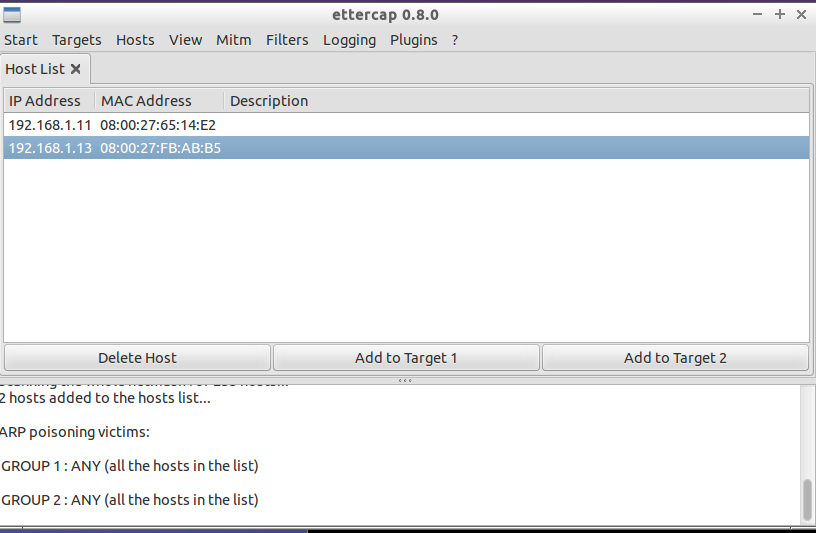
1. Pașii efectuați în realizarea atacului

* După ce am pornit cele 3 mașini virtuale vom deschide pe Router aplicatia Wireshark cu care vom putea observa traficul de internet

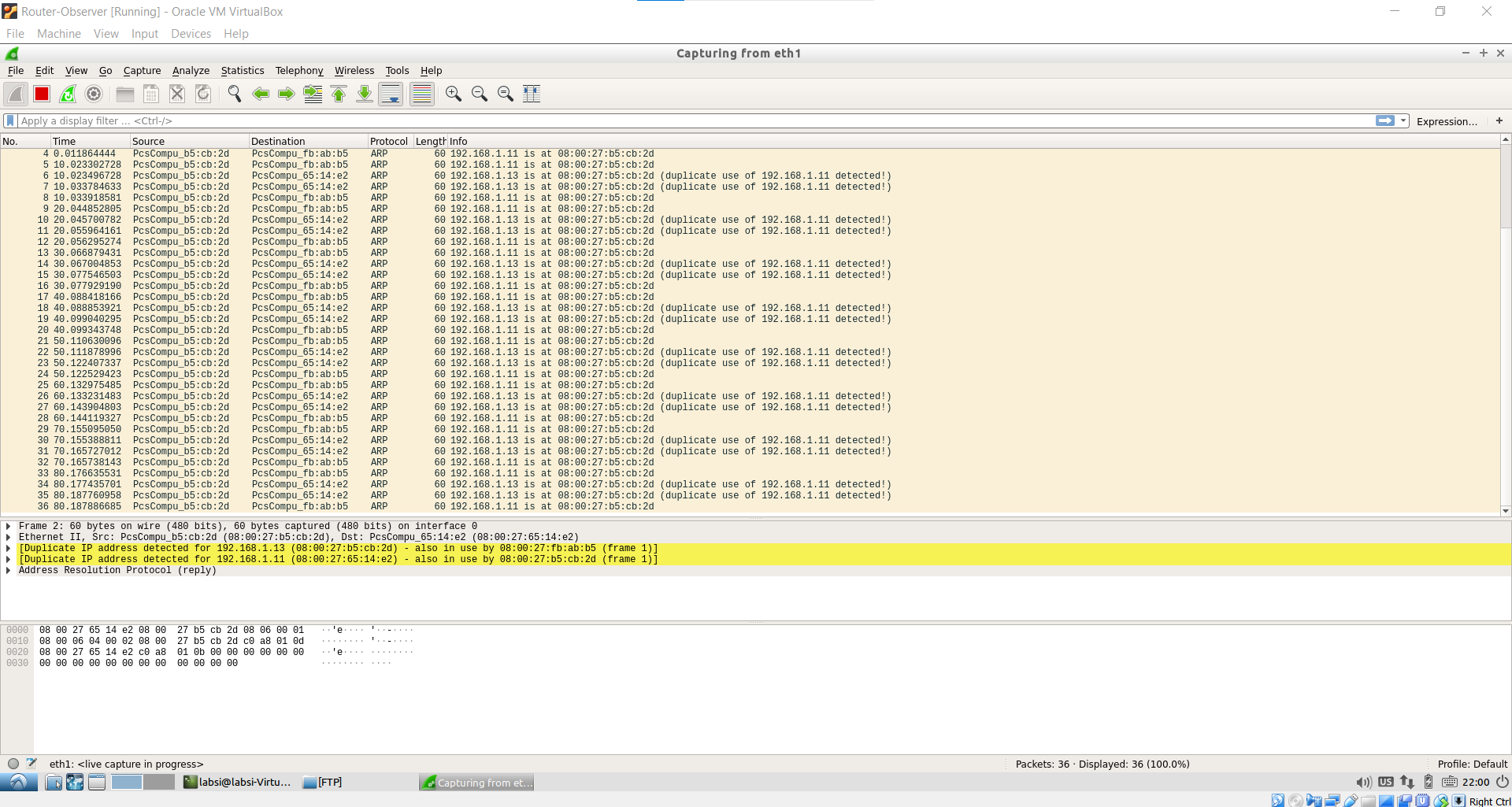
sudo wireshark

* Pe mașina virtuală a atacatorului vom deschide aplicatia ettercap cu care vom iniția atacul ARP cache poisoning

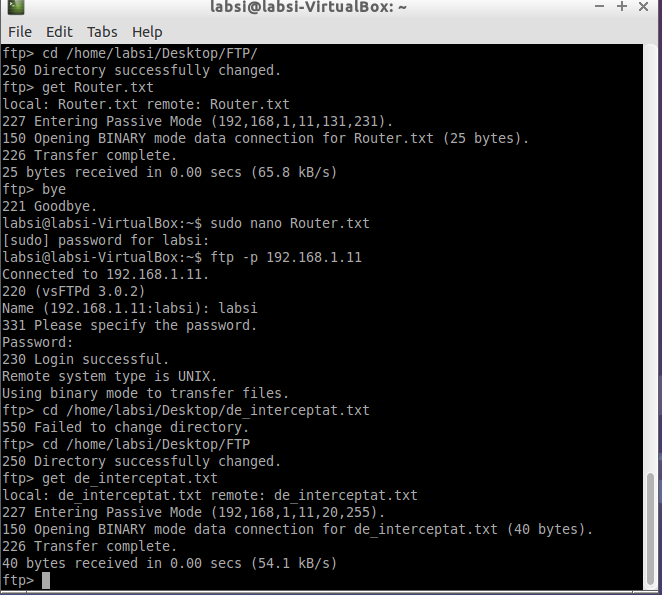
sudo ettercap -G



* În ettercap vom iniția atacul astfel: selectăm din bara de sus Sniff, apoi Uniffied Sniffing, alegem interfata eth0, tot din bara de sus apasam pe Start, Start Sniffing. Apasam pe Hosts din bara de sus, pe Scan for hosts, List of hosts și alegem adresa IP a masini virtuale victimă(192.168.1.13). Apoi in bara de sus este o optiune pentru felul de atac MITM pe care îl dorim, noi vom alege ARP Poisoning, va aparea o fereastra in care vom bifa Sniff remote connections și apasam Ok. Astfel se va începe „bombardarea” masini victimă cu reply-uri nesolicitate, după cum se poate observa în poza de mai jos

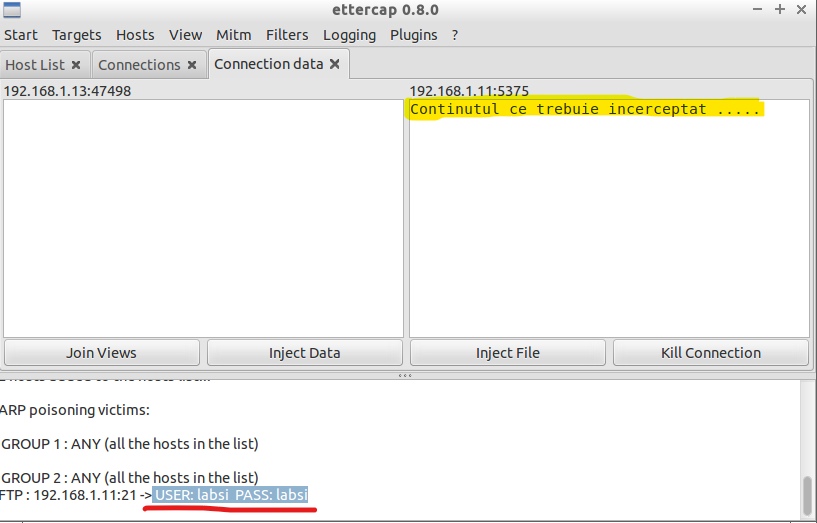


* Apoi vom face o demonstrație unde victima încearcă din nou să preia un fișier prin ftp de la Router.

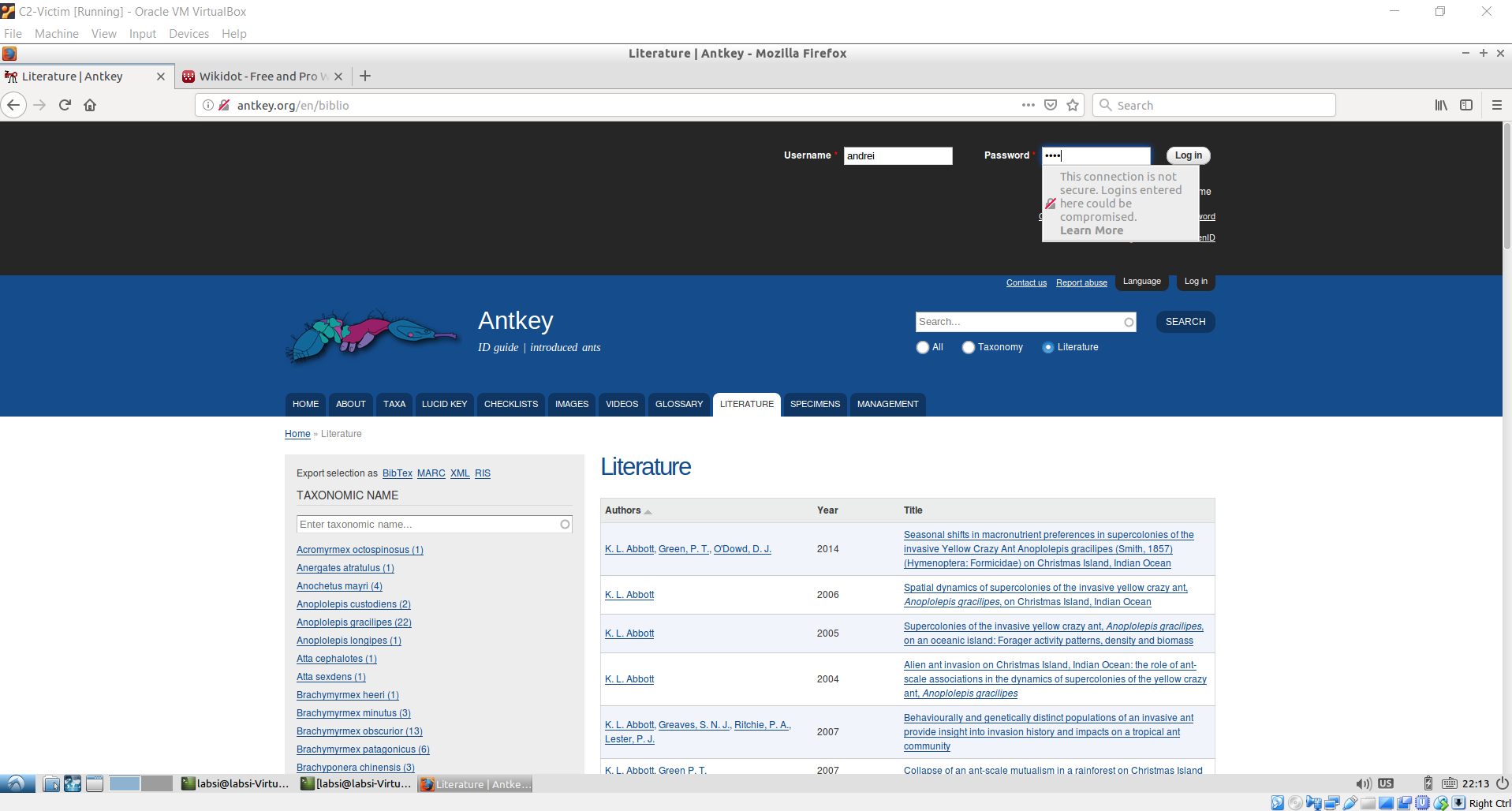


1. Rezultatul atacului

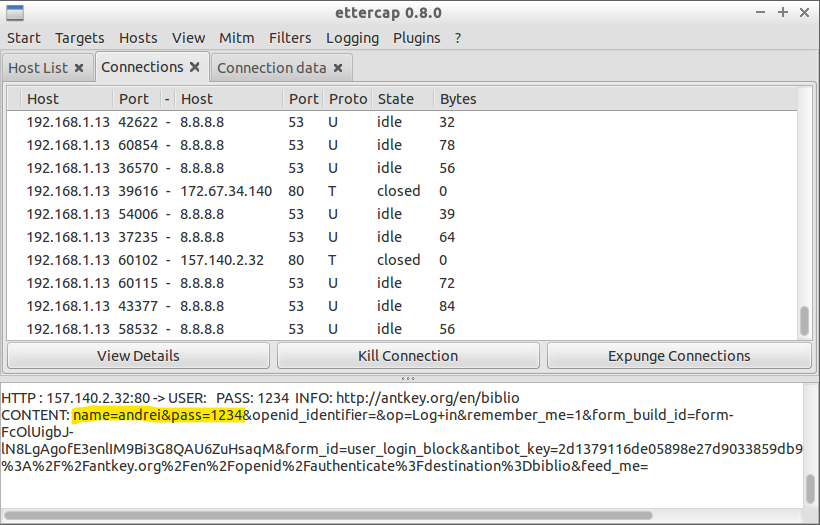
* În ettercap vom putea observa că datele de conectare și fișierul au fost interceptate de către atacator:



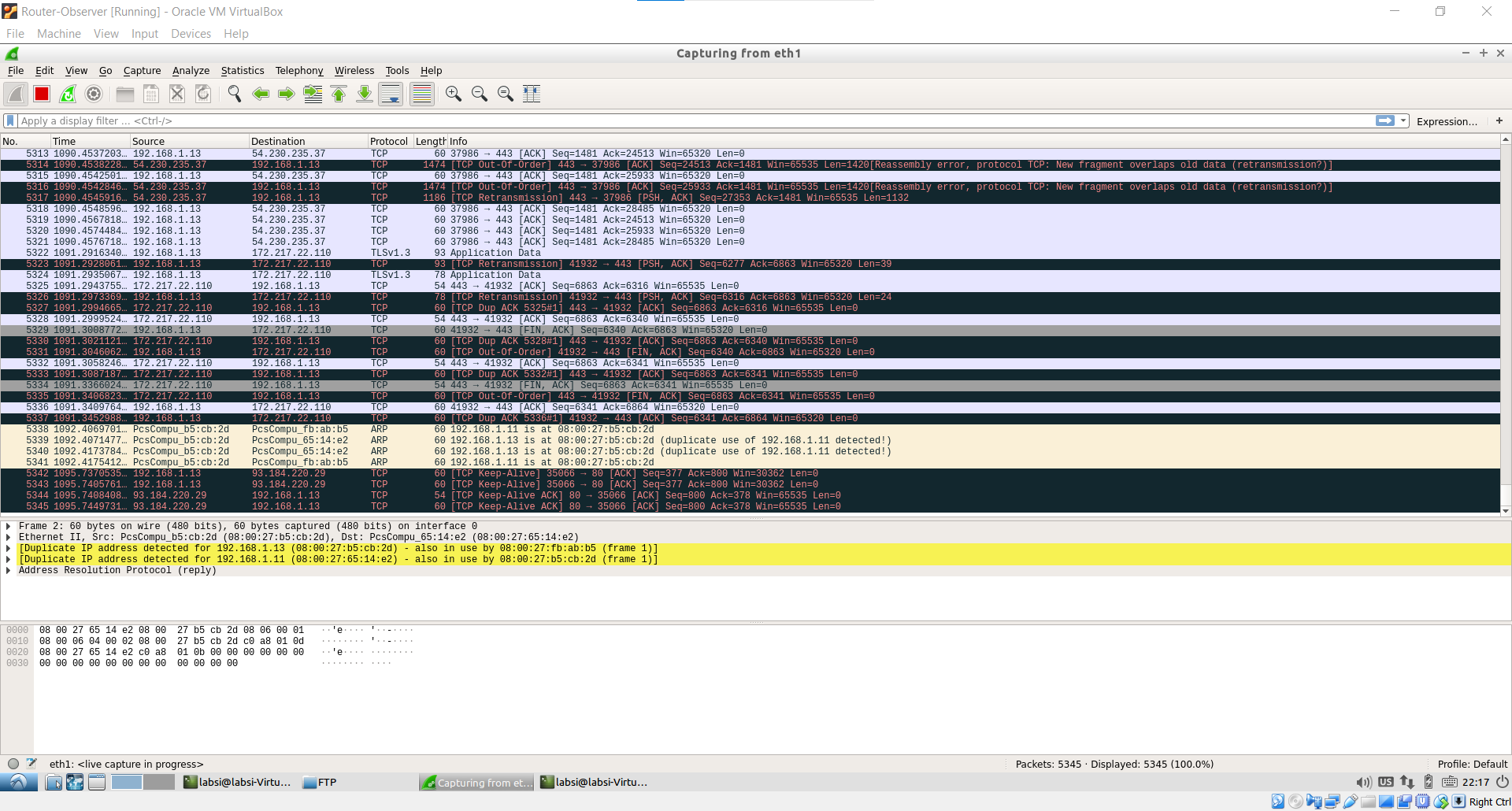
* De asemenea putem încerca sa luăm și datele de conectare de pe un site care nu folosește HTTP:



* Putem observa că ettercap a luat datele de logare pentru site-ul de mai sus



-La sfârșit traficul de rețea de pe router arată așa:

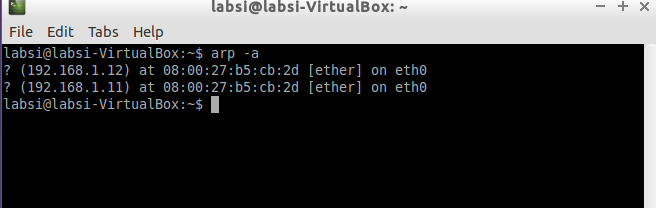


1. Detectarea unui astfel de atac

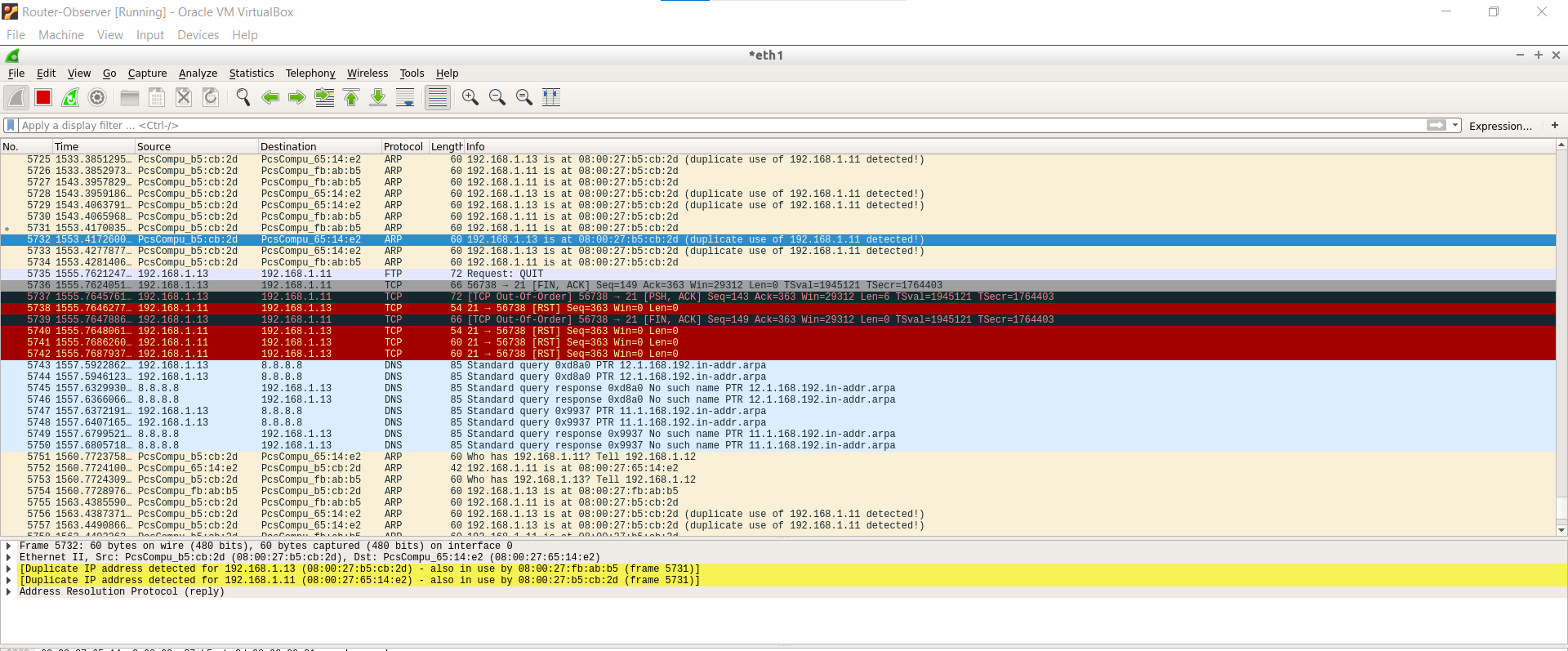
* O modalitate de detectare a unui astfel de atac este folosirea comenzi

arp -a

Unde daca la rezultat avem adrese IP cu aceleași adrese MAC înseamnă că am fost supuși unui astfel de atac



* De asemenea wireshark ne avertizează când cineva face un astfel de atac



1. Prevenire

* Folosirea de VPN
* În fișierul vsftpd.conf să avem ssl\_enable=YES pentru a cripta datele de conectare
* Folosirea de intrari ARP statice
* Instalarea unui tool, de exemplu, XArp, care sa detecteze dacă suntem atacați
* Set-Up Packet Filtering

Bibliografie:

* <https://www.utgjiu.ro/revista/ec/pdf/2010-04.I/16_LUMINITA_DEFTA.pdf>
* <https://www.punctpc.com/ce-este-otravire-arp-sau-atac-arp-spoofing-si-cum-functioneaza/>
* <https://www.digitalocean.com/community/tutorials/how-to-set-up-vsftpd-for-a-user-s-directory-on-ubuntu-18-04>
* <https://www.tecmint.com/install-ftp-server-in-ubuntu/>
* <https://openmaniak.com/ro/ettercap_arp.php>
* <https://www.indusface.com/blog/protect-arp-poisoning/>
* <https://en.wikipedia.org/wiki/ARP_spoofing>
* <https://www.imperva.com/learn/application-security/arp-spoofing/>