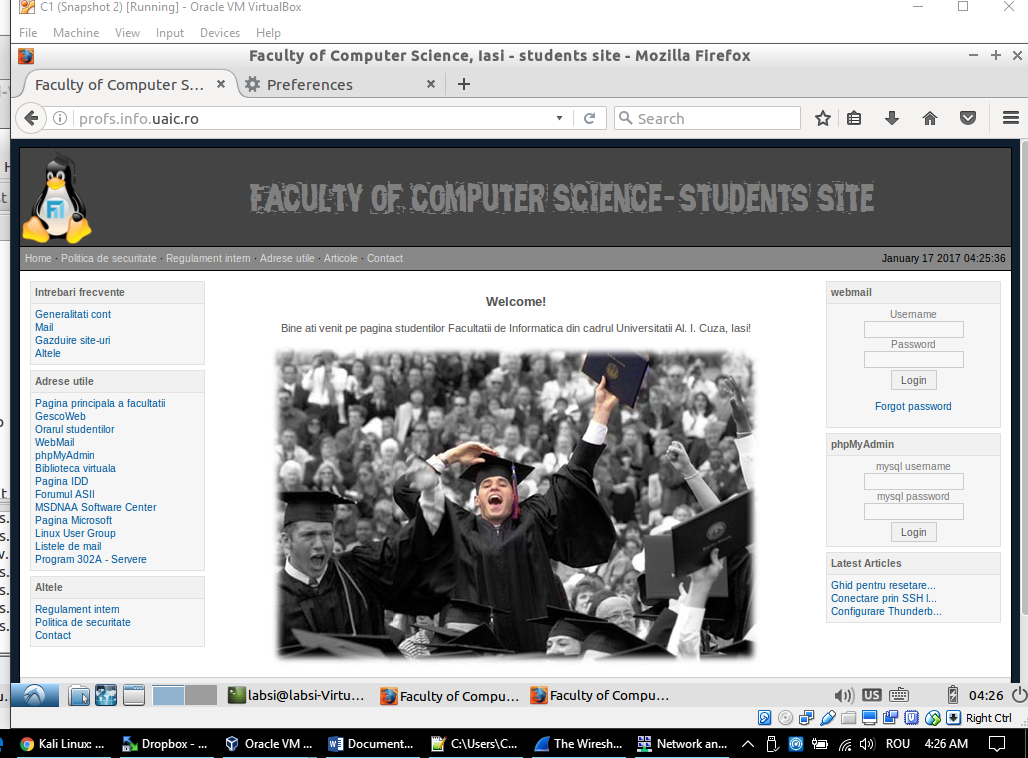
[A3] DNS Server Cache Poisoning

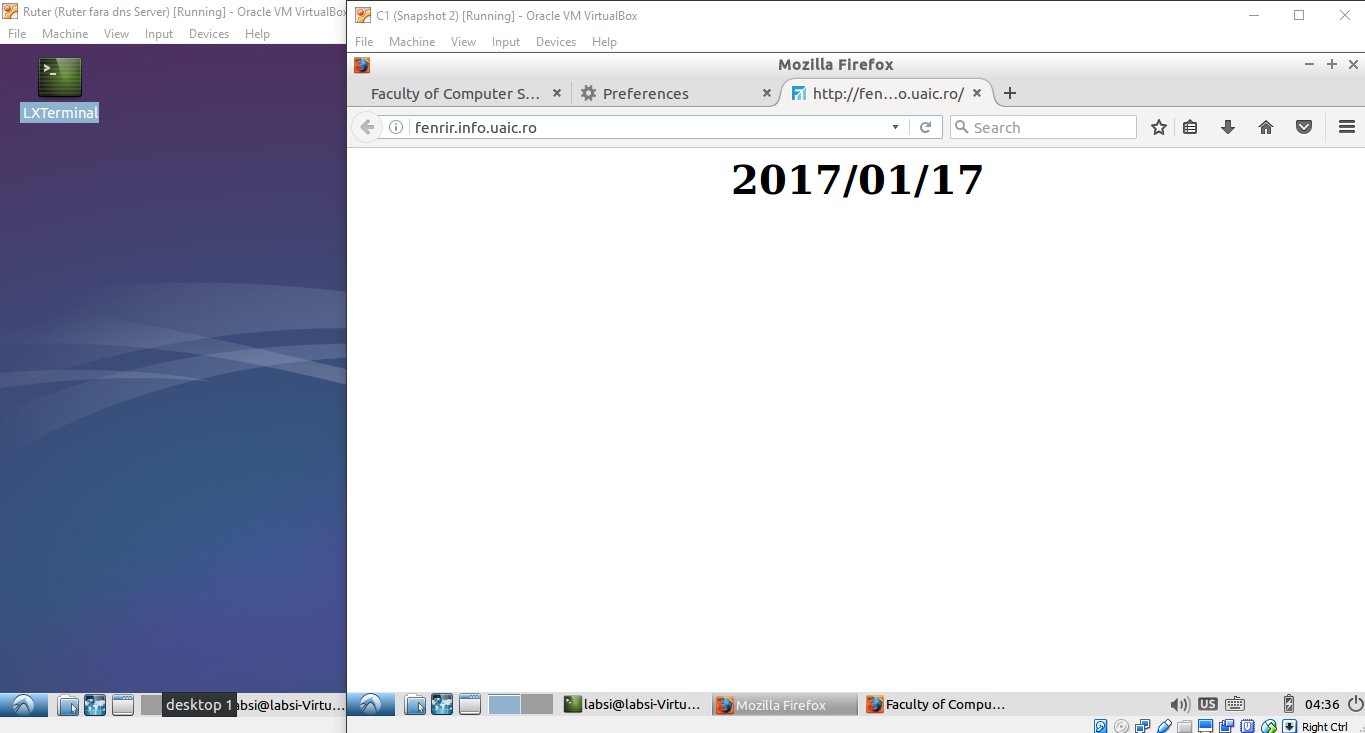
# Strategia aleasa pentru atac și implementarea atacului:

Cand un client va vrea sa intre pe profs.info.uaic.ro = 85.122.23.20 va fi redirectat pe fenrir.info.uaic.ro = 85.122.23.145.

**OBS.** Am incercat initial cu redirecate situri populare precum microsoft.com , facebook.com dar acestea nu au functionat acesta mergand cu https.

Solutie : dezactivarea unor optiuni de securitate din browser. Sau folosirea unor site-uri nesecurizate : profs si Fenrir.





# Mediu de lucru :

3 Masini virtuale : Ruter –local DNS , C1 , C2 -Atacator

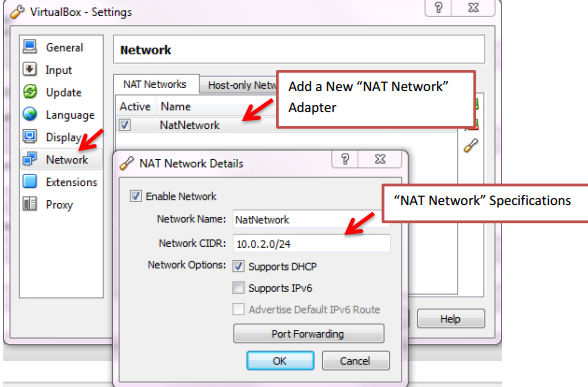
# Configurare mediu de lucru:

Am configurat respectand indicatiiile de [aici](http://profs.info.uaic.ro/~olgai/si2016/config_retea.pdf) **cu diferenta ca la C1 am modificat** potrivit atacului lista dns-nameservers 192.168.1.11 care este adresa ruterului (severului DNS local).

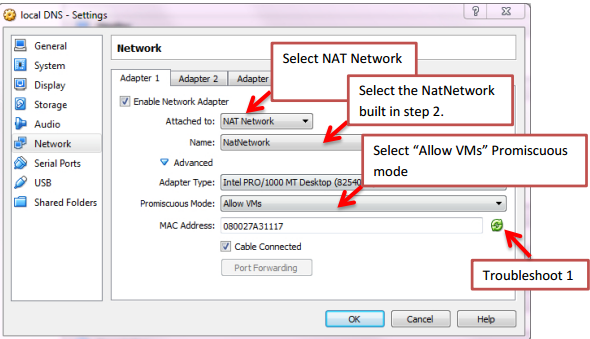
**OBS.** Atacatorului (C2) i-au ramas adresele serverelor DNS la care interogheaza si ruterul, altfel s-ar ataca pe el insusi.

Am configurat virtual box astfel:

1. Am creat din File > Preferences un **NatNetwork**



1. Am configurat ruterul cu eth0 (Adaptor1) atasat la **NatNetwork** si cu eth1(Adaptor2) atasat la **Internal Network.**



1. Am configruat MV C1, apoi prin clonare cu C1 am creat C2, **attached to Internal Network.**
2. **Configurare mediu de lucru:**

|  |  |  |
| --- | --- | --- |
| **Ruter** | **C1** | **C2** |
| **traceroute dnsutils** | **traceroute dnsutils** | **traceroute dnsutils** |
|  |  |  |
| **Instalare Server DNS bind9**  **Configurare server DNS** | **Config client schimbare NS** | **Instalare ettercap** |
|  |  | **Ettercap -G** |

## Configurare server DNS:

Am realizat-o după aceste linkuri

<https://help.ubuntu.com/14.04/serverguide/dns-configuration.html#dns-caching-configuration>

Si am verificat setarile cu

<https://help.ubuntu.com/14.04/serverguide/dns-troubleshooting.html#dns-testing-dig>

# Comenzi:

## Ruter:

Ifconfig

Nslookup

Dig -x addr

sudo rndc flush

sudo rndc dumpdb -cache

sudo cat /var/cache/bind/dump.db

## C1(client victima):

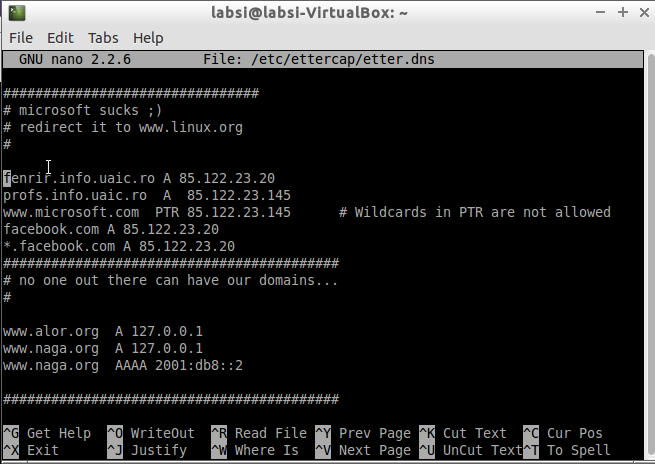
arp

Ping 192.168.1.13

firefox

## C2(atacator):

sudo nano /etc/ettercap/etter.dns



**OBS.** Aici se seteaza numele pentru care se va inlocui IP-ul prin Spoofing

sudo ettercap –G

**Pași de urmat cu ettercap –G:**

Start sniffing pe eth0

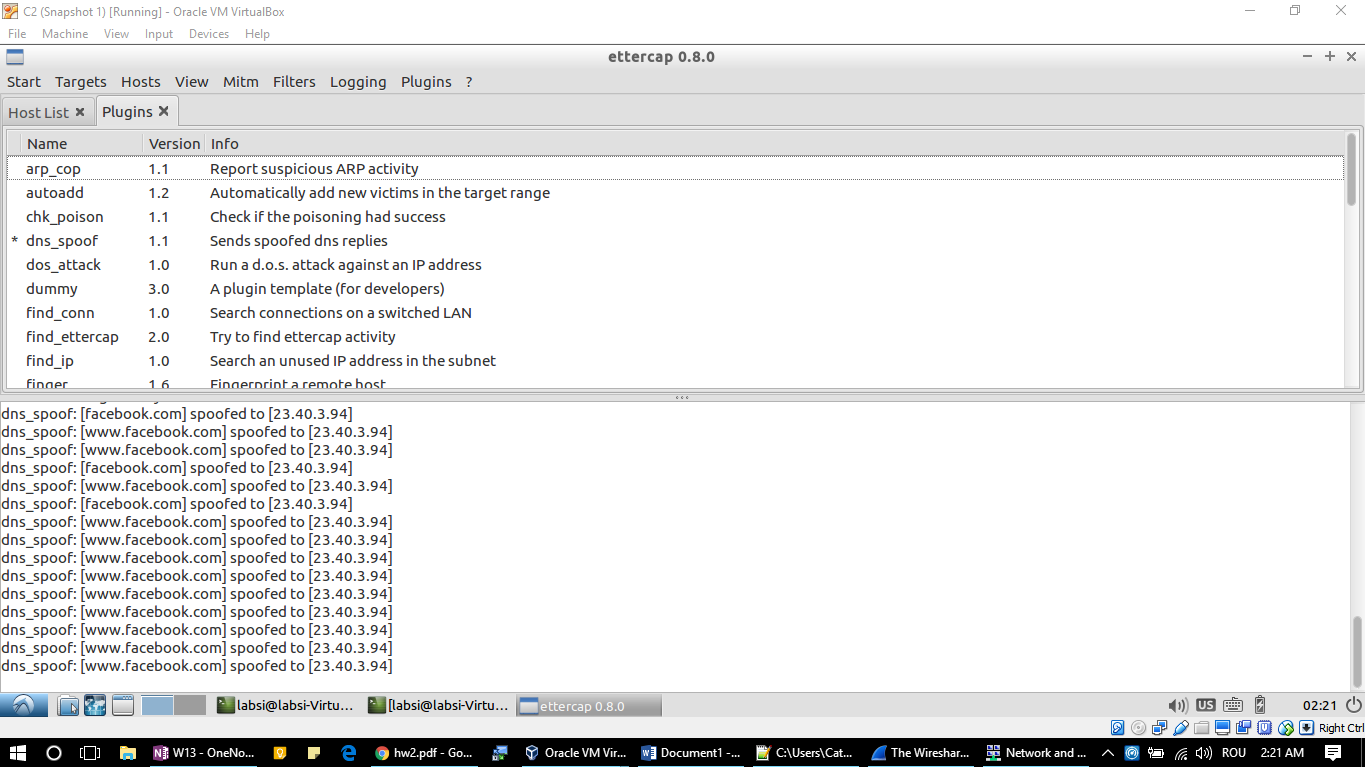
Scan host

Add target 1 192.168.1.11

Add target 2 192.168.1.12

Select from Plugins DNS spoofing

Arp poisoning

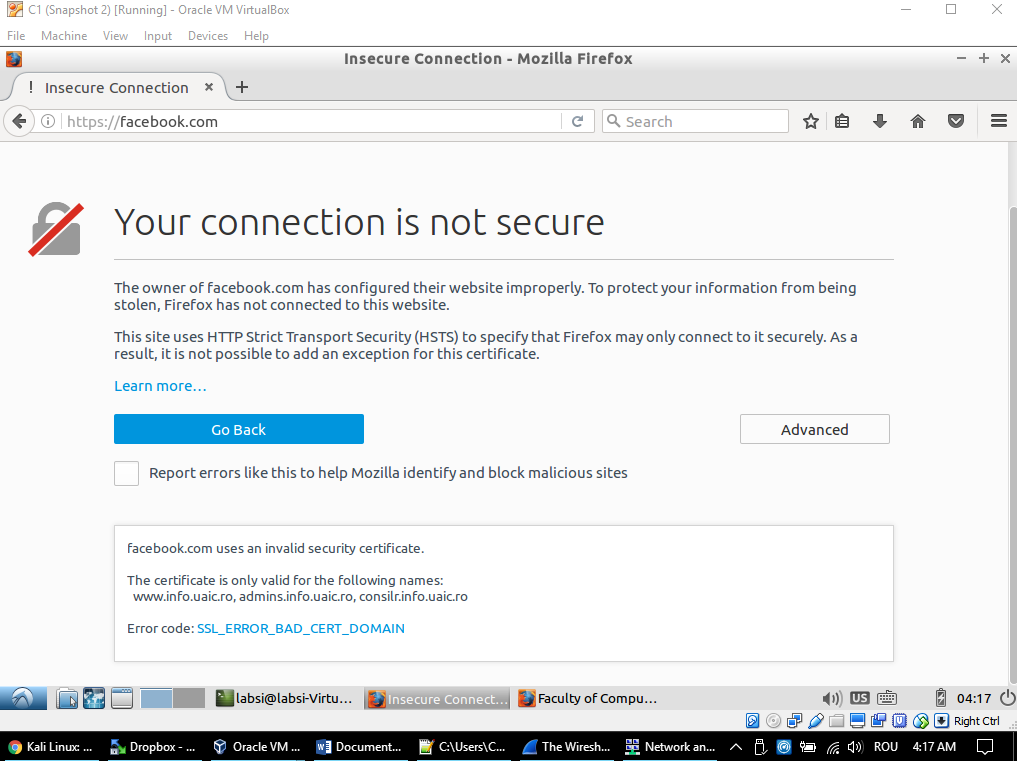


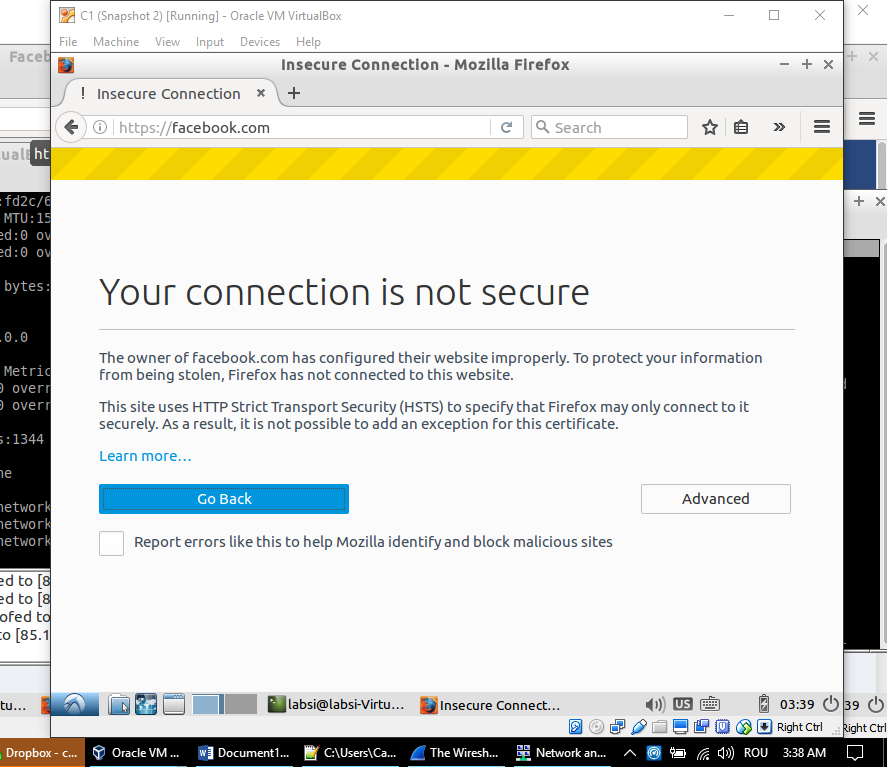
# Metode de prevenire

**Foarte important**: Ideal este folosirea protocolului/extensiilor de securitate DNS-sec astfel atacatorul nemaiputand sa falsifice un raspuns de la un alt server DNS.

Alte recomandari ar fi un TTL( time to live ) mic la cache. Iar pe partea de client optiunile de securitate la browser avtive.

Nu ar trebui sa ne dam credentialele pe un un server web **http ci https** cum este de exemplu facebook.





Char daca **acest atac poate trece peste acest detaliu** ar fi o masura de securitate inplus care ne apara si ingreuneaza efectuarea atacului.

# Referinte:

Configurare:

<http://profs.info.uaic.ro/~olgai/si2016/hw2.pdf>

http://profs.info.uaic.ro/~olgai/si2016/config\_retea.pdf

[**http://www.cis.syr.edu/~wedu/seed/Documentation/VirtualBox/VirtualBox\_NATNetwork.pdf**](http://www.cis.syr.edu/~wedu/seed/Documentation/VirtualBox/VirtualBox_NATNetwork.pdf)

[**https://help.ubuntu.com/14.04/serverguide/dns-configuration.html**](https://help.ubuntu.com/14.04/serverguide/dns-configuration.html)

[**https://help.ubuntu.com/14.04/serverguide/dns-configuration.html#dns-primarymaster-configuration**](https://help.ubuntu.com/14.04/serverguide/dns-configuration.html#dns-primarymaster-configuration)

**https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-caching-or-forwarding-dns-server-on-ubuntu-16-04**