

DNS Spoofing

DNS („domain name system”) reprezintă un standard folosit cu scopul administrării adreselor IP ale site-urilor web. Asignarea unui DNS pe un server ne permite accesarea serverului fără să cunoaștem IP-ul.

Exemplu:

fmi.unibuc.ro - IP 193.226.51.15

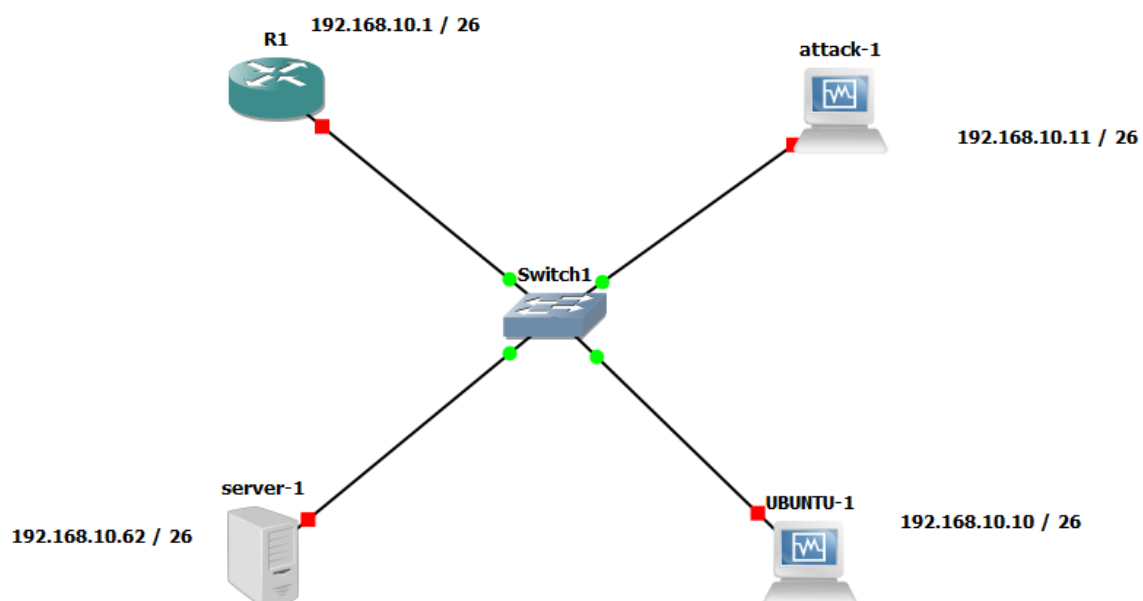
Existența DNS-ului reprezintă un necesar în acest moment, întrucât reținerea IP-urilor pentru fiecare server web ar fi fost incomod, putând face astfel asemănarea cu o carte de telefoane.

Principiul de funcționare este relativ simplu. De fiecare dată când accesăm un site web, se realizează o succesiune de interogări în funcție de complexitatea site-ului, pentru a fi redirecționat către serverul web care are IP-ul assignat cu numele de domeniu accesat.

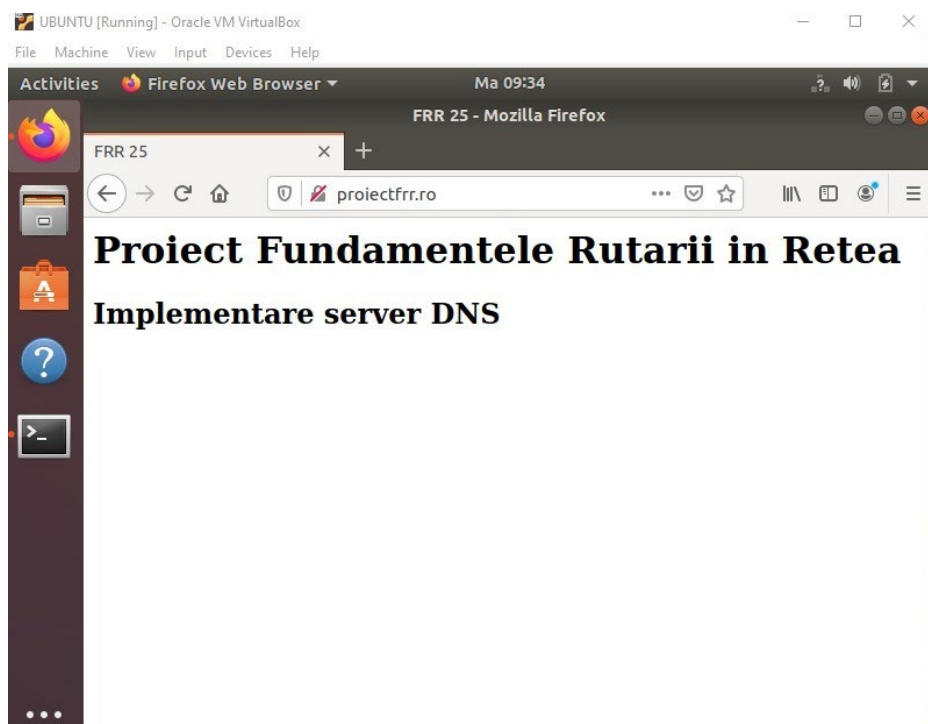
DNS-ul, ca orice alt serviciu de altfel, are diverse vulnerabilități în funcție de soluțiile de securitate alese. În cadrul acestui proiect, am implementat un tip de atac „Man in the Middle”, denumit DNS Spoofing. Acest tip de atac afectează hosturile dintr-o rețea, schimbând redirecționarea inițială a DNS-ului către un alt server web de unde se realizează diverse operațiuni frauduloase.

Acest tip de atac se realizează accesând serverul DNS al rețelei de unde se schimbă adresa serverului către cea frauduloasă.

Pentru implementarea acestei operațiuni, am utilizat programul GNS3, unde am simulat următoarea topologie:



Serverul are setat ca DNS următorul domeniu: `proiectfrr.ro`. Acest server web are următoarea interfață:



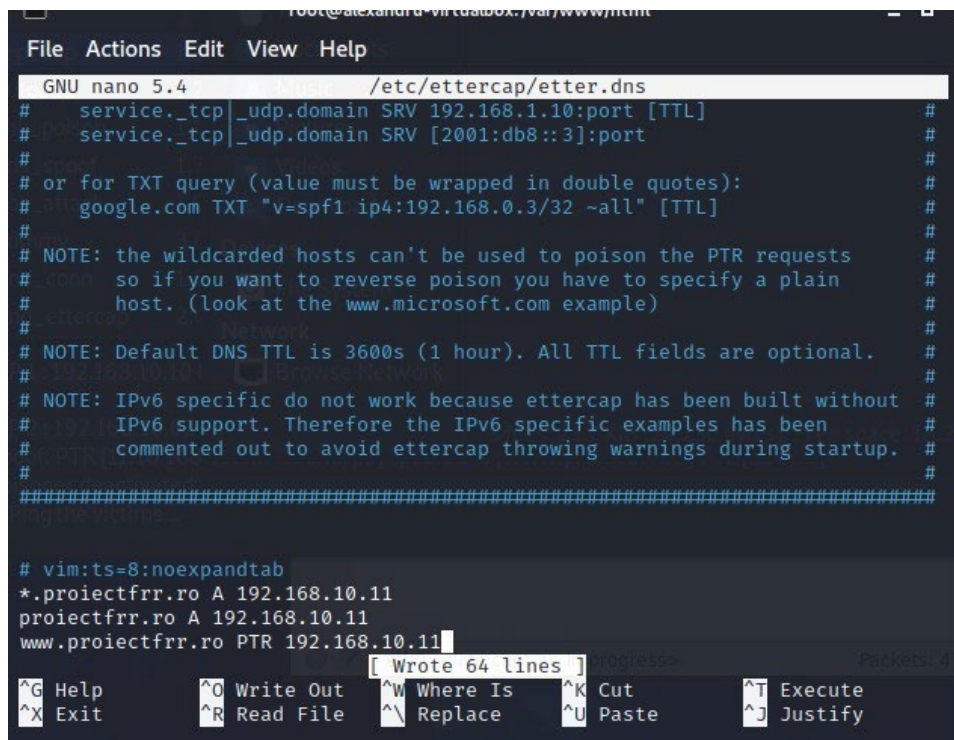
Este configurat și pentru www.proiectfrr.ro

```
GNU nano 2.5.3      File: db.proiectfrr.ro
;
; BIND data file for local loopback interface
;
$TTL 604800
@      IN      SOA      proiectfrr. root.proiectfrr.ro. (
                        2      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@      IN      A        192.168.10.62
;
@      IN      NS       ns.proiectfrr.ro.
@      IN      A        192.168.10.62
www    IN      A        192.168.10.62
ns     IN      A        192.168.10.62
```

Serverul este hostat pe Ubuntu Server, hostul Ubuntu cu sistemul de operare Ubuntu 18.04, iar hostul attack cu sistemul de operare Kali Linux, sistem de operare făcut special pentru testarea atacurilor.

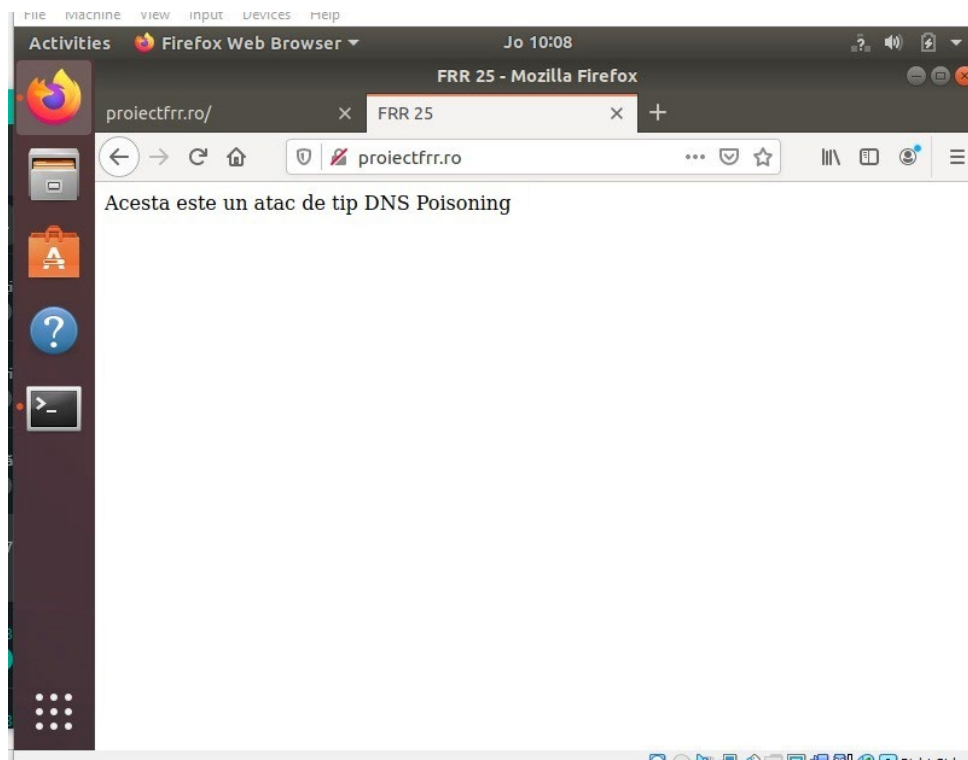
Unealta necesară pentru atac este „ettercap”, instalat odată cu sistemul de operare Kali Linux. Acest program are un plugin numit „dns spoof” care realizează acest tip de atac. Configurarea acestuia se realizează simplu, accesând fișierul `etter.dns` din `/etc/ettercap/`, unde se adaugă datele domeniului și IP-ul către serverul unde se redirecționează.

În cadrul testului, serverul web este chiar IP-ul atacatorului, întrucât nu pot rula mai mult de 3 mașini virtuale simultan din cauza limitării sistemului.



```
File Actions Edit View Help
GNU nano 5.4 /etc/ettercap/etter.dns
# service._tcp._udp.domain SRV 192.168.1.10:port [TTL]
# service._tcp._udp.domain SRV [2001:db8::3]:port
#
# or for TXT query (value must be wrapped in double quotes):
# google.com TXT "v=spf1 ip4:192.168.0.3/32 ~all" [TTL]
#
# NOTE: the wildcarded hosts can't be used to poison the PTR requests
# so if you want to reverse poison you have to specify a plain
# host. (look at the www.microsoft.com example)
#
# NOTE: Default DNS TTL is 3600s (1 hour). All TTL fields are optional.
#
# NOTE: IPv6 specific do not work because ettercap has been built without
# IPv6 support. Therefore the IPv6 specific examples has been
# commented out to avoid ettercap throwing warnings during startup.
#
#####
# vim:ts=8:nowrap:
*.projectfrr.ro A 192.168.10.11
projectfrr.ro A 192.168.10.11
www.projectfrr.ro PTR 192.168.10.11
[ Wrote 64 lines ] progress> Packets: 47
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
```

În momentul în care rulăm softul, pagina web devine:



Bibliografie:

<https://www.cloudflare.com/learning/dns/what-is-dns/> - accesat la data de 25.03.2021.

<https://www.imperva.com/learn/application-security/dns-spoofing/> - accesat la data de 25.03.2021.