**LAB 7**

**LOCAL DNS ATTACK LAB**

Nhóm 13:

Trương Đăng Quý\_0850080039

Nguyễn Thị Ngọc Hiền\_0850080072

Châu Tú Hoa\_0850080073

**Bài làm:**

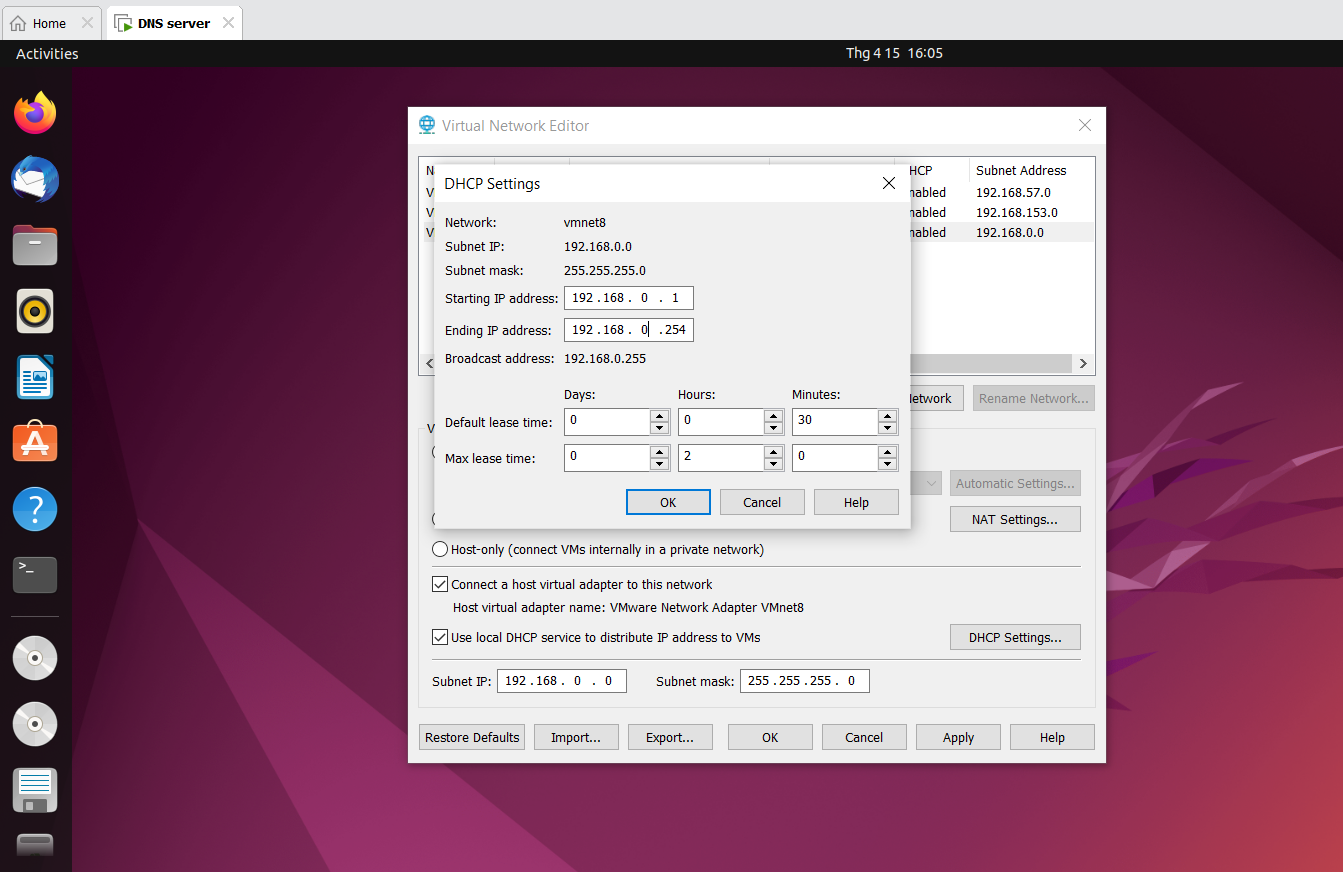
**Môi trường:**

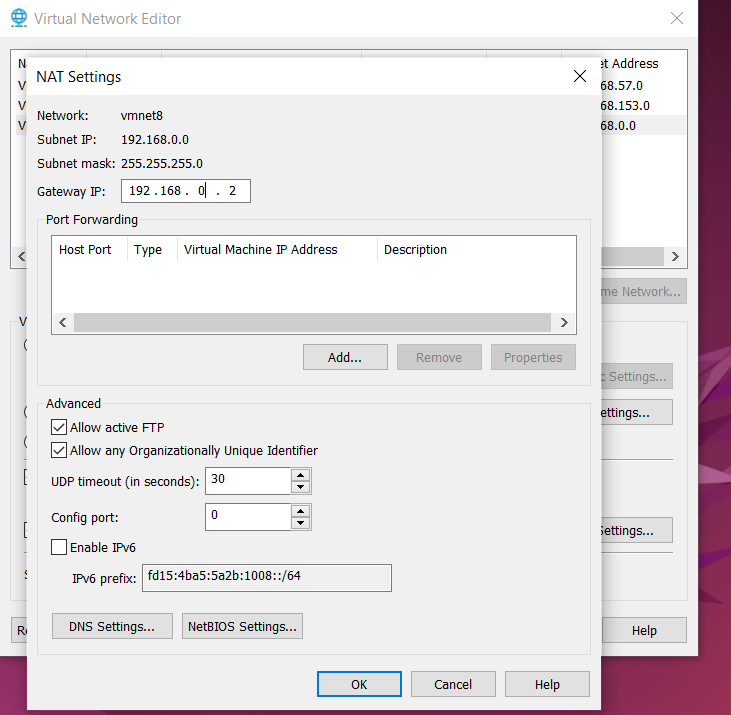
* Máy ảo Vmware Ubuntu 22.04.2 làm DNS server
* Máy ảo Vmware Ubuntu 22.04.2 làm User
* Máy ảo Vmware Ubantu 22.04.2 làm Attacker

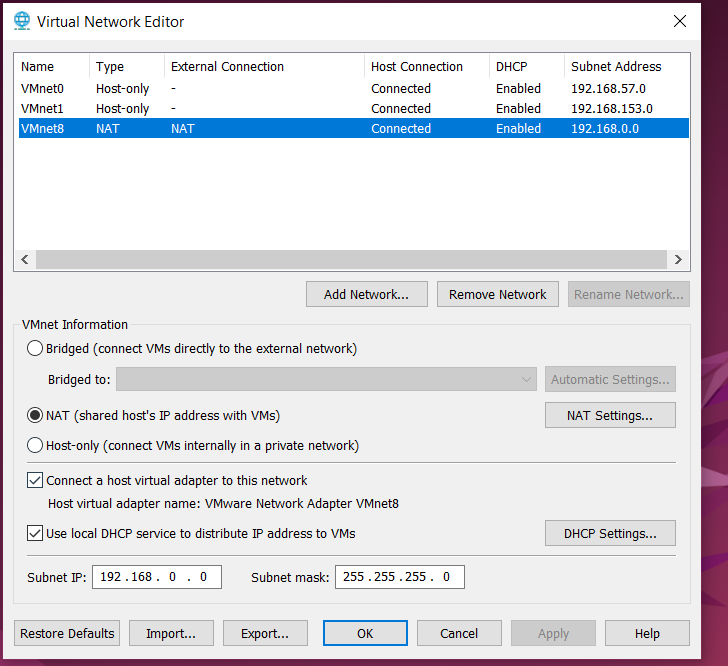
**Thiết lập IP tĩnh cho cả 3 máy**

* DNS server: 192.168.0.10/24
* User: 192.168.0.100/24
* Attacker: 192.168.0.200/24

Trước tiên, cần thiết lập vùng mạng NAT trước, vì có thể máy ảo không thuộc lớp mạng 192.168.0.0/24.

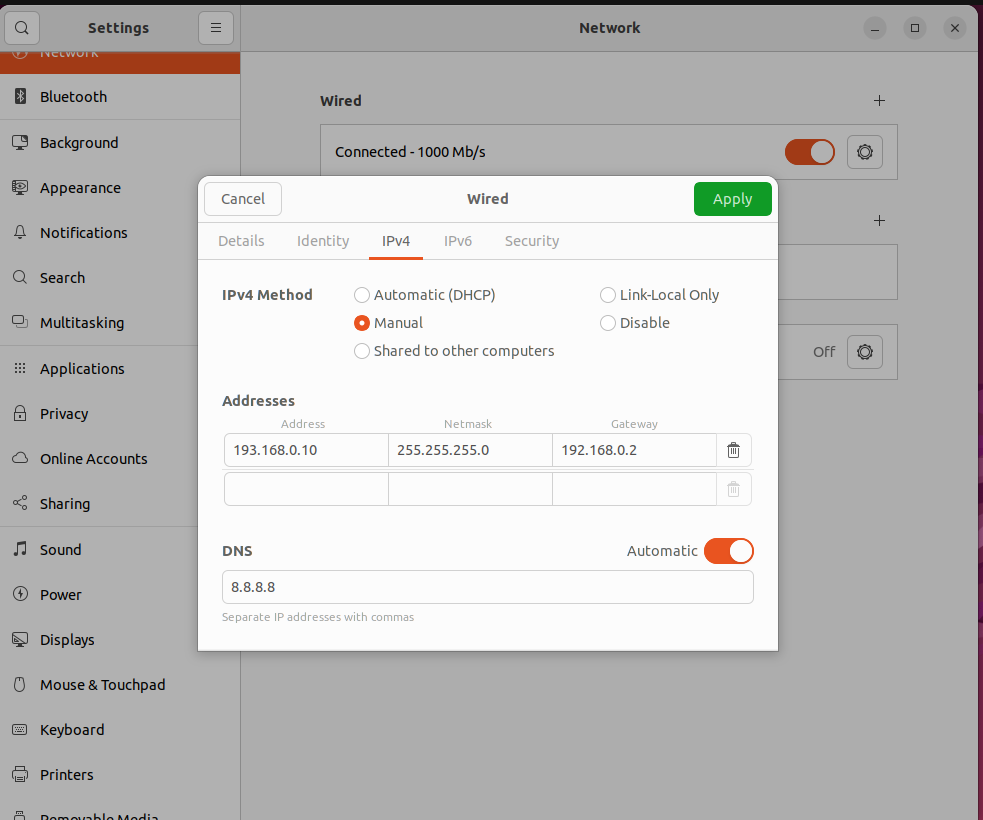


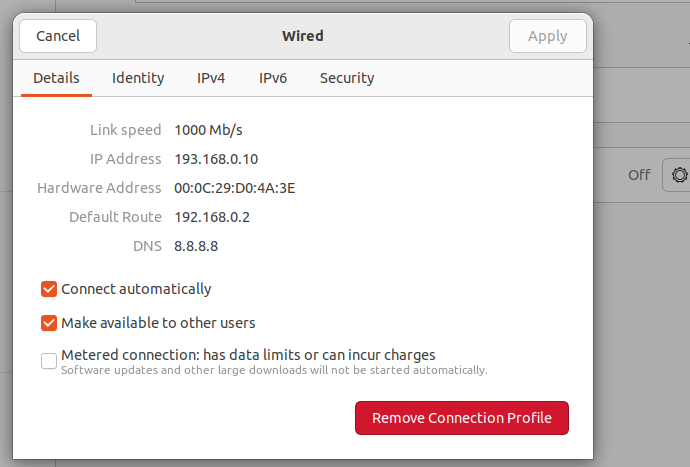




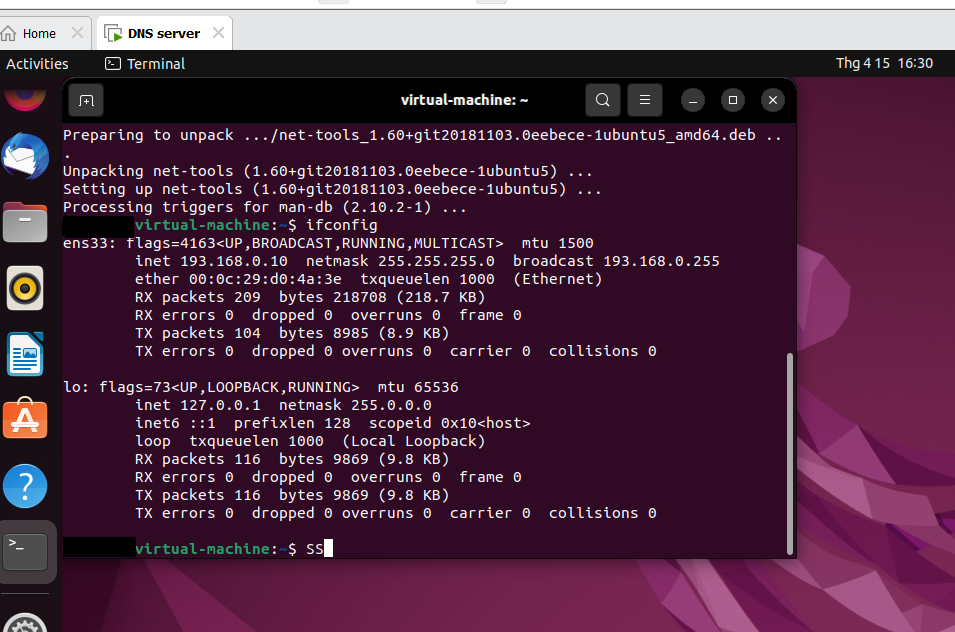
2.1. Install and configura the DNS server

Sau đó ta thiết lập IP tĩnh cho DNS server như sau:

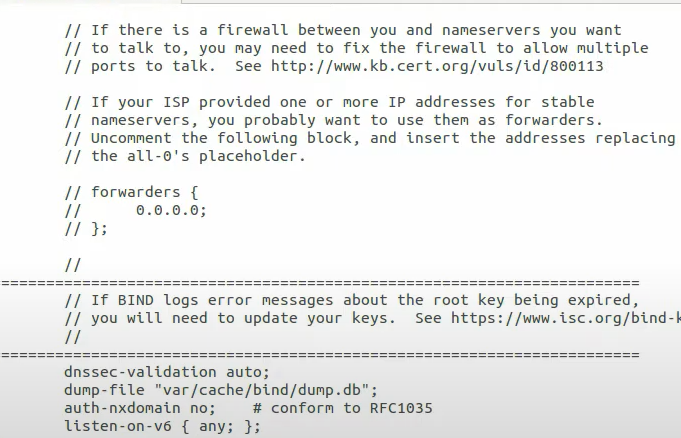




Và sau đó restart lại máy để apply vào. Sau đó vào terminal để kiểm tra bằng lệnh: ifconfig.



Và kiểm tra tốc đọ mạng google: ping google.com



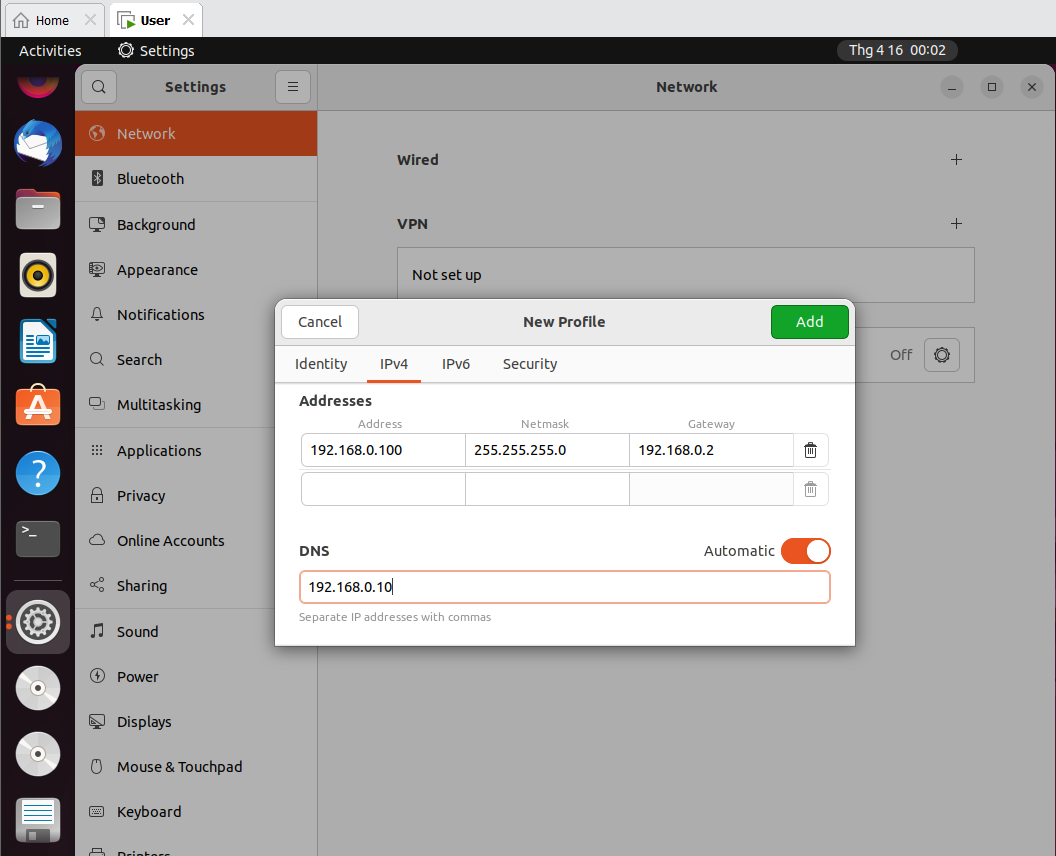
Step 3: Tạo zone

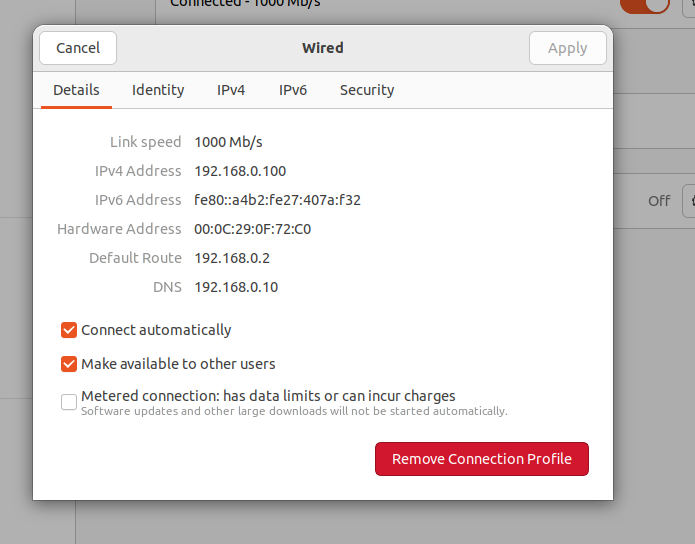
Ta sử dụng một domain là example.com

Và đườn dẫn /etc/bind/ để tạo file named.conf với nội dung như trên

2.2. Cấu hình máy User

Bên máy này cũng thiết lập IP tĩnh 192.168.0.100





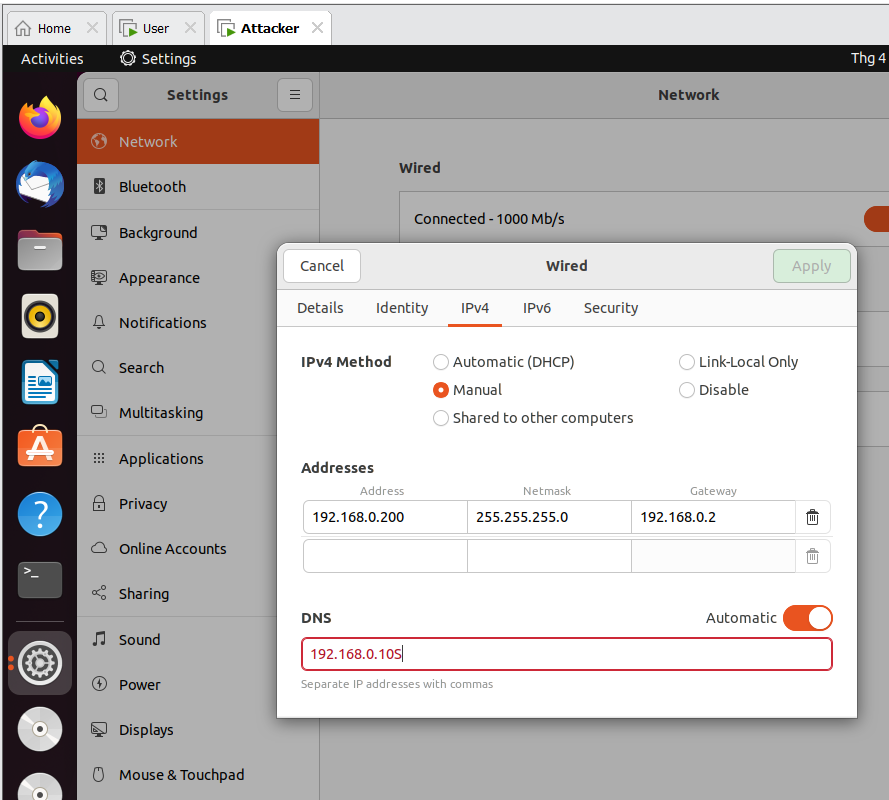
Và ta chỉnh sửa file /ect/resolv.conf để chỉ ra khi cần phân giải tên miền thì phải thông qua máy nào (IP).

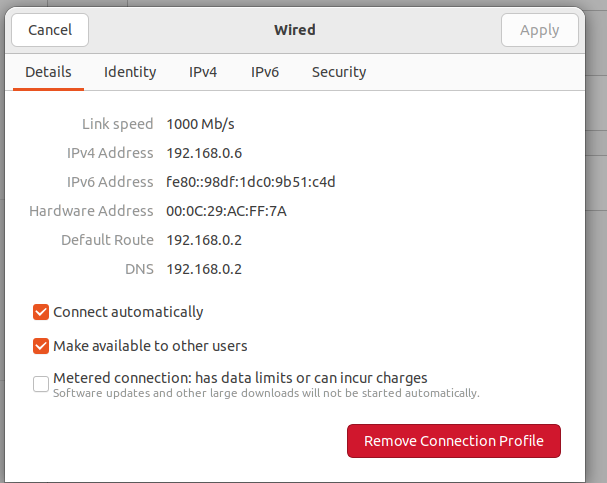
Ở đây ta thiết đặt là nameserver 192.168.0.10

Restart lại để apply nó

2.3. Attacker

Ta không cần cấu hình gì nhiều- chỉ đạt mỗi IP cho nó như mặc định của mô hình: 192.168.0.200





2.4. Ta sử dụng lệnh dig [www.example.com](http://www.example.com) trên máy User để xem một vài thông tin về domain [www.example.com](http://www.example.com)

ANSWER SECTION chứa bảng ánh xạ DNS. Ví dụ [www.example.com](http://www.example.com) là 192.168.0.101

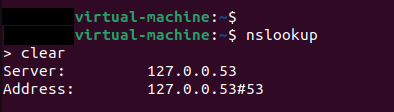
3.2. Task 1 – Attacker have alrealy compromised the victim’s machine

Trong tấn công này, attacker xân nhập máy người dùng có quyền chỉnh sửa file/etc/host để chuyển hướng truy cập của người dùng đến địa chỉ độc hại

Ví dụ như trường hợp attacker có thể telnet đến máy user và có quyền chỉnh sửa file host đó.

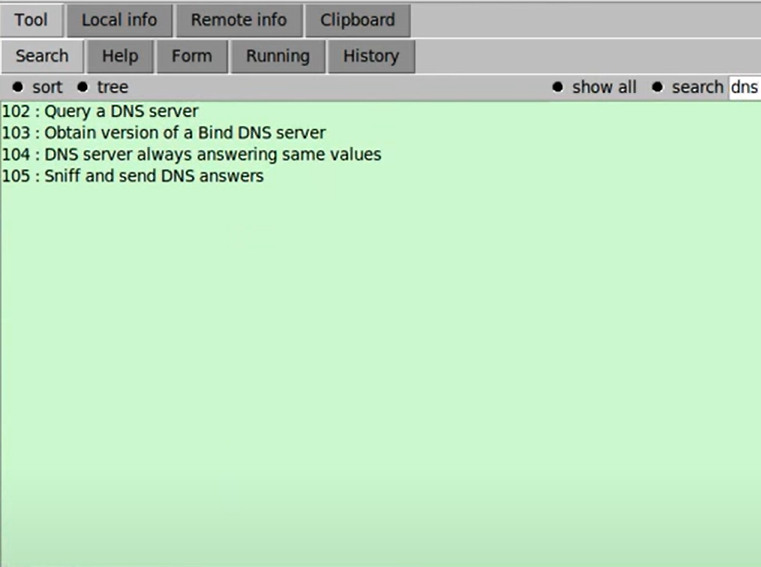
Attacker chuyển hướng tên miền [www.example.com](http://www.example.com) vốn được maping đến 192.168.0.101, thì đổi thành 192.168.0.200 [www.example.com](http://www.example.com) (địa chỉ Attacker)

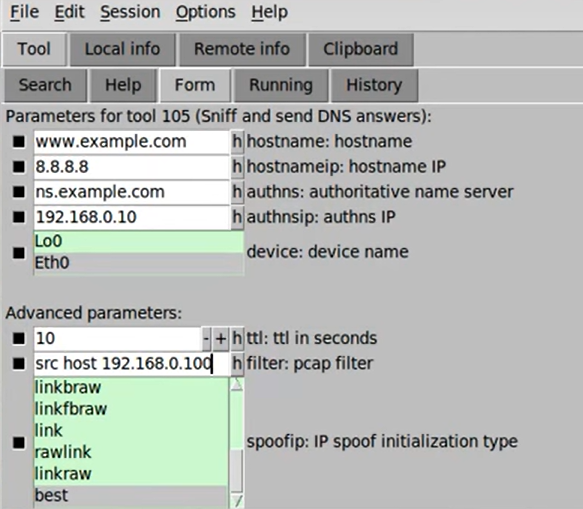
Đối với nslookup thì có vẻ nó không khả quang, như lệnh ping hoặc truy cập bằng web browser thì được



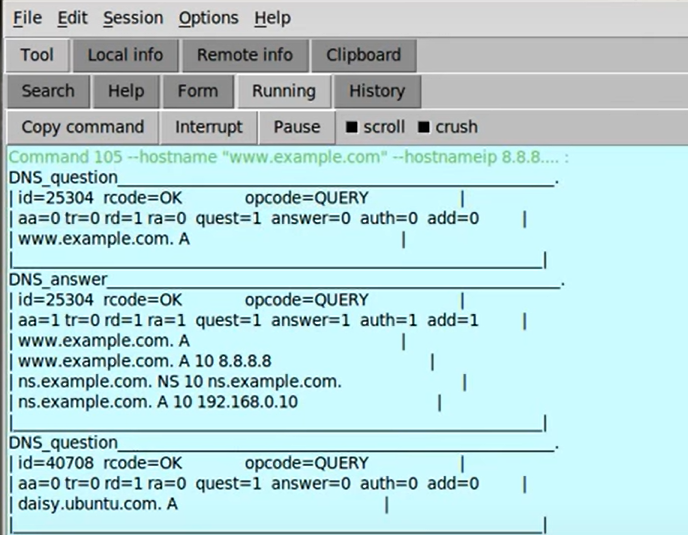
3.2- Dicrectly Spoof Response to User

Trong phần này, khi User truy vấn tên miền, thì nó sẽ gửi một gói tin DNS request đến DNS server. Lúc này, Attacker sniff được, lấy thông tin từ gói tin đó và giả mạo một gói tin phản hồi DNS response đáp ứng đầy đủ các yêu cầu của một gói DNS response thật, nhưng trong gói này Attacket đã đổi IP domain cần truy vấn thành IP độc hại của mình mong muốn.





Trong này, Attacker sử dụng công cụ Netwag để thực hiện điều này. Và trong trường hợp filter gõ src host <địa chỉ ip user> để chỉ tấn công mỗi ip user này



3.3-Task 3- DNS server Cache Poisoning

Trong phần tấn công, Attacker tấn công vào máy server thay vì máy người dùng để đạt hiệu quả. Vì khi user truy vấn 1 tên miền không nằng trong DNS server (Apollo), thì DNS server này sẽ truy vấn một Root DNS server ở a nằm ngoài mạng local. Lợi dụng điểm này, Attacker sẽ gởi một tin giả mạo đến DNS server trước khi gói tin từ Root DNS server phản hồi về sẽ giống như tấn công ở Task 2 nhưng lần này nhằm vào DNS server.

Cuộc tấn công này sẽ lâu dài, vì kết quả của gói tin giả mạo sẽ được lưu trên DNS cache của server. Từ đó, mà nhiều user khi truy cập tên miền đó thông qua DNS server sẽ cũng bị ảnh hưởng.

Trước khi làm phần này nên configure một số thứ bên DNS server để các máy mà thiết lập DNS đến server 192.168.0.10 đều có thể truy vấn được

Cấu hình của forwarding DNS server

Bên máy user và attacker thì trong file /ect/resolv.còn phải chỉ ra nameserver 192.168.1.10 – là địa chỉ của DNS server

Giờ thì truy cập thử bằng nslookup trên máy user. User đã truy xuất thành công và tiếp tục trên attacker sẽ tấn công vào DNS server.