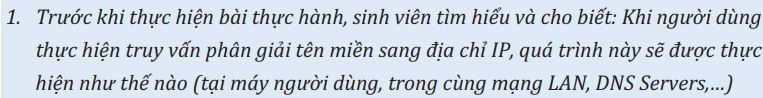
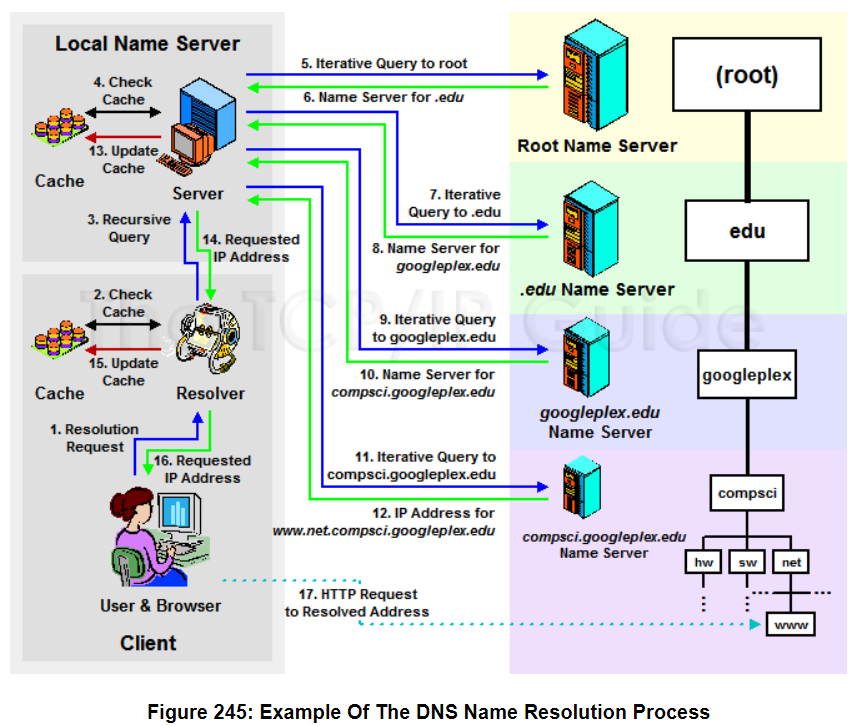
Link video youtube:



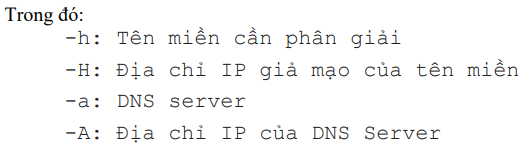


* Đầu tiên, khi người dùng nhập tên miền (ví dụ: www.example.com) vào trình duyệt hoặc ứng dụng. Hệ điều hành máy người dùng kiểm tra xem nếu địa chỉ IP của tên miền đã được lưu trong bộ nhớ cache của máy người dùng hay chưa. Nếu có, nó sẽ sử dụng địa chỉ IP từ cache mà không cần thực hiện bước tiếp theo.
* Nếu địa chỉ IP không được tìm thấy trong cache hoặc cache đã hết hạn, máy người dùng sẽ gửi một truy vấn DNS (Domain Name System) đến máy chủ DNS đầu tiên được cấu hình trong danh sách DNS của máy người dùng hoặc máy chủ DNS được cung cấp bởi ISP (Nhà cung cấp dịch vụ Internet). Máy chủ DNS trong cùng mạng LAN, nếu có, có thể trả lời truy vấn mà không cần đi xa.
* Nếu máy chủ DNS trong cùng mạng LAN không thể cung cấp địa chỉ IP, truy vấn sẽ được chuyển đến máy chủ DNS gốc (root DNS server). Máy chủ DNS gốc sẽ hướng dẫn truy vấn đến các máy chủ DNS cấp cao hơn, ví dụ như máy chủ DNS top-level domain (TLD). Quá trình này tiếp tục cho đến khi máy chủ DNS cuối cùng trả lời với địa chỉ IP của tên miền được truy vấn.
* Địa chỉ IP được trả về từ máy chủ DNS cuối cùng được chuyển về máy người dùng. Hệ điều hành và trình duyệt lưu trữ địa chỉ IP vào bộ nhớ cache để sử dụng cho các lần truy cập sau.



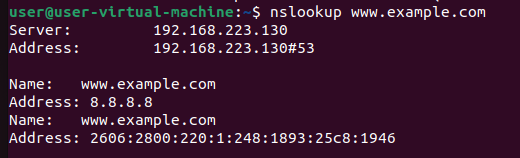
- Mục đích là tạo ra các DNS response giả mạo. Kẻ tấn công sử dụng công cụ Netwox 105 để chặn yêu cầu DNS của người dùng và phản hồi bằng phản hồi DNS giả mạo. Gói trả lời chứa địa chỉ IP sai, khiến hệ thống của người dùng tin rằng đó là IP chính xác cho trang web được yêu cầu. Do đó, người dùng được dẫn đến sai địa chỉ khi cố gắng truy cập tên miền, trang web đó.

*sudo netwox 105 -h "www.example.com" -H "8.8.8.8" -a "ns.example.com" -A "192.168.223.130" -f "src host 192.168.223.131"*

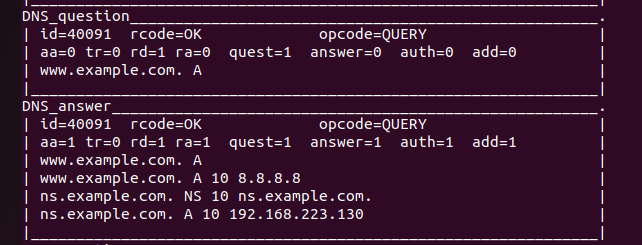


* Kết quả thực hiện:

Tại máy nạn nhân đã nhận được IP giả là 8.8.8.8 chứng tỏ tấn công thành công:

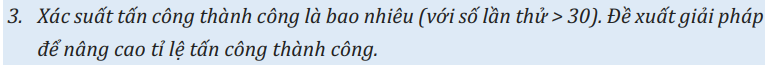


Đây là các thông số cơ bản mà DNS response giả mạo đã phản hồi về cho nạn nhân:





* Nếu không sử dụng netwox 105, thông tin này được lấy từ máy chủ DNS cục bộ trên máy tính của người dùng hoặc máy chủ DNS được cấu hình trong hệ thống của local. Ngược lại, nếu sử dụng netwox 105, kết quả có thể sẽ khác, tùy thuộc vào cách bạn thiết lập các thông số trong lệnh netwox, trên máy attacker và cách máy chủ DNS được cấu hình.



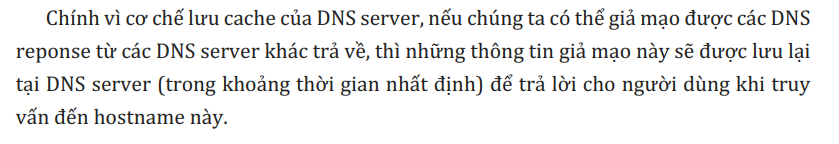
* Tỉ lệ thành công: theo như thực hiện, tỉ lệ tạm ổn, khoảng 50%, em thực hiện tổng là 7 lần tấn công, thì đa số nhập lệnh nslookup lần thứ 13-15 sẽ tấn công thành công. Có khi sẽ sớm hơn, khoảng lần thứ 5 là victim sẽ nhận được ip giả mạo.
* Để nâng cao tỉ lệ tấn công thành công:
* Đảm bảo đang sử dụng cùng mạng LAN với nạn nhân.
* Netwox 105 phải duy trì hoạt động liên tục để nhận và phản hồi request nhanh nhất có thể.



* Bật DNSSEC.
* Sử dụng tường lửa và các hệ thống phát hiện xâm nhập để giám sát và phát hiện các hành vi đáng ngờ, bao gồm cả các tấn công giả mạo DNS.
* Cập nhật hệ thống và tất cả các phần mềm liên quan thường xuyên với các bản vá bảo mật mới nhất.

**2. Tấn** **công DNS Cache Poisoning:**

* Tấn công vào DNS server.



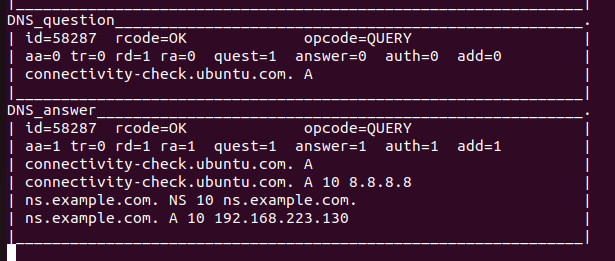
* Trong phần này sẽ thực thi với tên miền “example.org”
* Bước 1: Xóa rỗng DNS cache tại DNS server:

sudo rndc flush

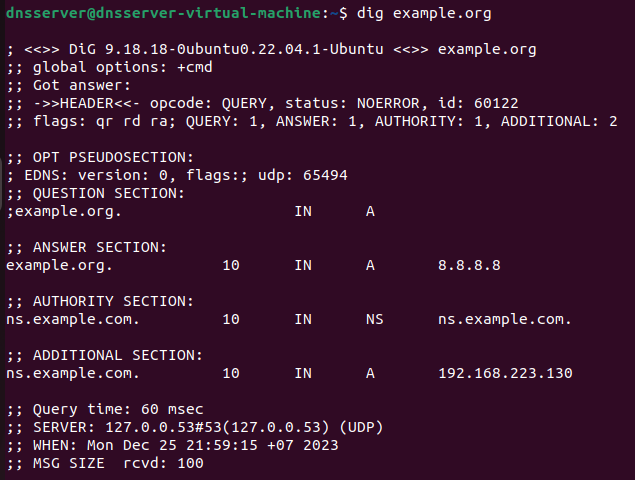
* Bước 2: Tại máy tấn công, sử dụng Netwox 105 như trong bài trước để thực hiện tấn công:

*sudo netwox 105 -h "example.org" -H "8.8.8.8" -a "ns.example.com" -A "192.168.223.130" -s raw -f "src host 192.168.223.130"*

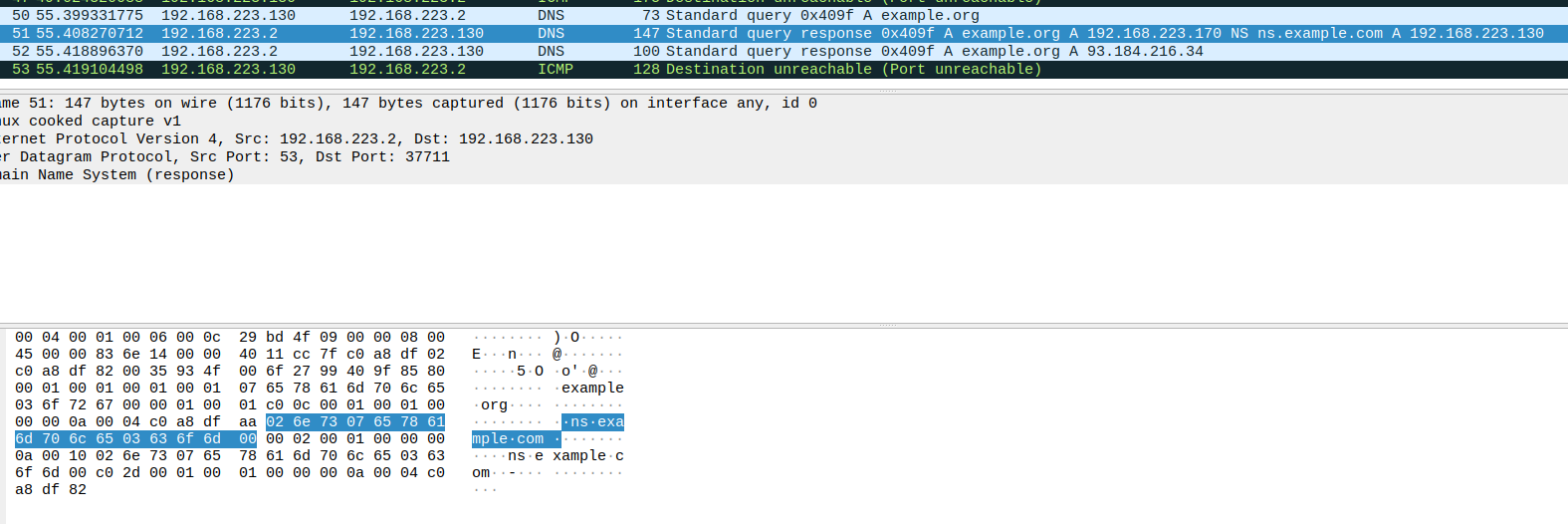
Máy tấn công:



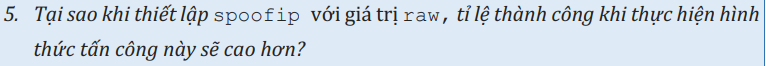
Máy DNS server: dig example.org

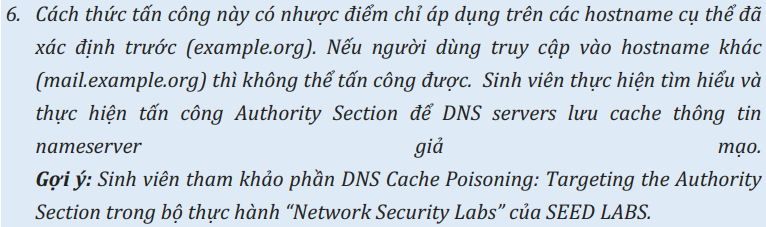


* Bước 3: Sinh viên sử dụng chương trình bắt gói tin (Wireshark, TcpDump,...) để ghi đã nhận được quá trình truy vấn giải quyết tên miền. Mô tả quá trình khảo sát được thực hiện.

Trong hình trên, DNS server có địa chỉ IP là 192.168.223.130 gửi yêu cầu truy vấn về tên miền example.org. Attacker tạo ra gói tin giả và phản hồi lại, trong nội dung gói tin thì có địa chỉ IP giả đã được đóng gói cùng là 8.8.8.8 để gửi về cho nạn nhân.

* Bước 4:

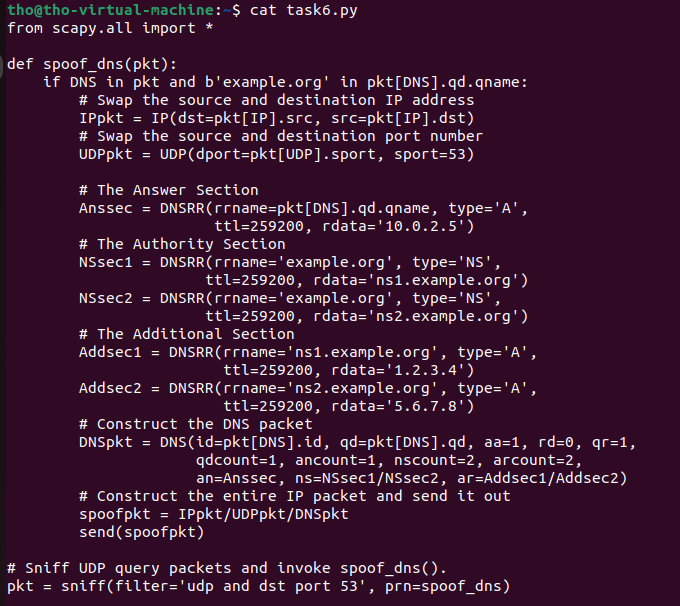
ARP request là bản tin mà máy gửi gửi broadcast để tìm địa chỉ MAC của máy nhận. Ta thiết lập spoofip với giá trị raw để che đi địa chỉ MAC và IP của máy gửi, từ đó trốn tránh được sự phát hiện của hệ thống bảo mật. Hơn nữa giả mạo IP thì sẽ gây khó khăn trong phòng ngự và phân tích bảo mật hệ thống, do đó tỉ lệ tấn công thành công sẽ cao hơn.



- Ở phần tấn công trên, chúng ta đã chỉ định chỉ một tên miền example.org tại netwox 105 để giả mạo DNS response. Nhưng nếu nạn nhân - tức là DNS server không yêu cầu phân giải tên miền example.org mà yêu cầu một tên khác như mail.example.org thì attacker khi muốn tấn công sẽ phải cấu hình lại. Do đó, chúng ta cần một giải pháp tối ưu hơn để tạo ra một cuộc tấn công toàn diện, ảnh hưởng đến toàn bộ example.org zone.

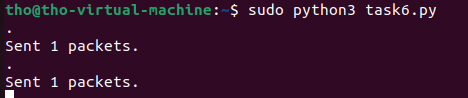
Sau khi tham khảo task 7 của seed lab, thì để giải quyết vấn đề này, cần sử dụng đến **Authority section** trong gói DNS reply. Nói đơn giản là khi tạo ra gói tin giả mạo thì sẽ thêm mục Authority section vào nội dung của gói tin giả mạo đó.Và khi mục này được lưu trữ vào bộ nhớ cache của DNS server thì những lần truy vấn tiếp theo, bất kỳ hostname nào thuộc example.org cũng sẽ bị nhận DNS reponse giả mạo từ attacker.

- Nội dung file task6.py: có chức năng tạo ra gói tin giả mạo:

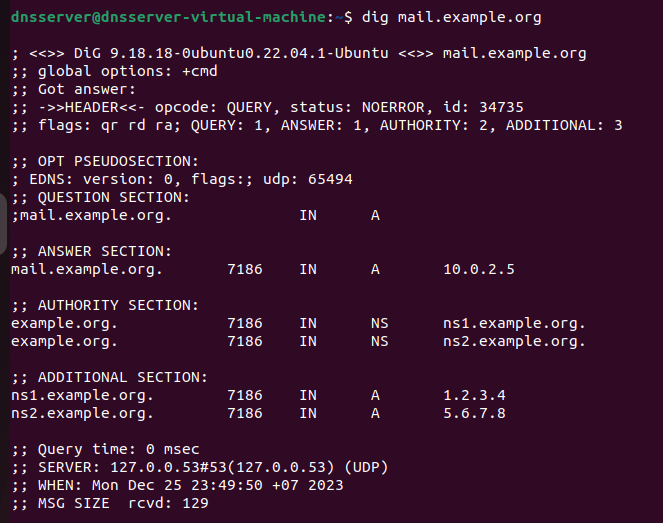


- Kết quả:

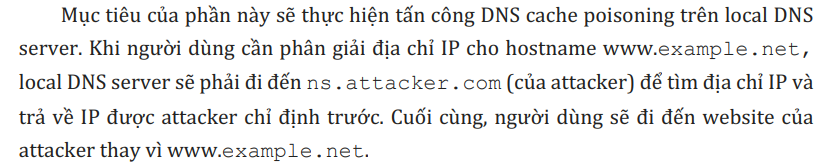
Khi thực thi file, mỗi lúc DNS server gửi yêu cầu phân giải tên miền, thì attacker sẽ gửi gói tin giả mạo, đồng thời màn hình hiển thị thông báo việc đã gửi đi thành công một packet giả đến nạn nhân:



Phía nạn nhân khi nhận được DNS response giả mạo, sau đó DNS server đã lưu vào cache nên những lần truy vấn tiếp theo, vẫn sẽ hiển thị thông tin như hình:



**3. Tấn** **công Kaminsky:**





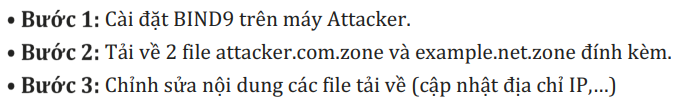
Mục tiêu của công thức tấn công Kaminsky được sử dụng trong bài thực hiện này sẽ **bắt các nạn nhân sẽ phải sử dụng ns.attacker.com làm nameserver cho example.net.** Khi đó, các truy vấn đến example.net (bao gồm phụ tên miền) sẽ được gửi đến ns.attacker.com. Trên thực tế, máy chủ DNS cục bộ sẽ cần có địa chỉ công khai IP của ns.attacker.com trước (thông qua root server, .com server, thậm chí cả kẻ attacker.com). Vấn đề phát sinh là chúng ta không phải là chủ sở hữu của tên miền trên nên không thể cấu hình máy chủ DNS trên ns.attacker.com. Để khắc phục, sử dụng bind9.

BIND9 cho phép thêm vùng chuyển tiếp trong DNS cấu hình. Trong tập tin cấu hình /etc/bind/named.conf, add nội dung sau:

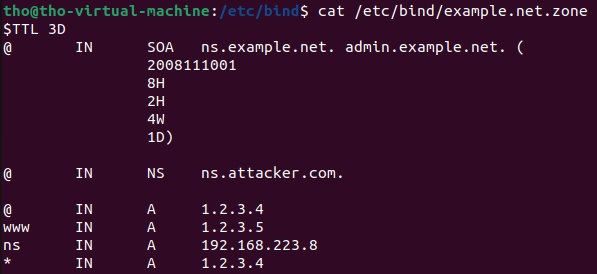
zone "attacker.com" { type forward; forwarders { 192.168.223.129; }; };

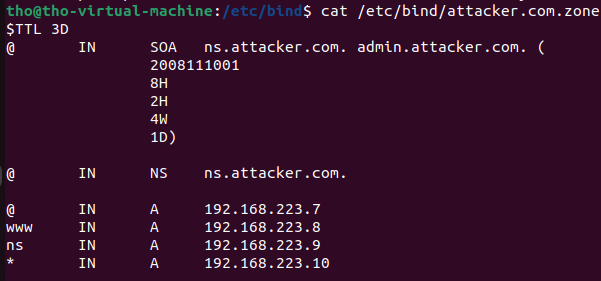
Trong đó, địa chỉ IP trên là địa chỉ của attacker. Điều này tương đương với việc sử dụng 192.168.223.129 làm nameserver cho miền attack.com. Vì vậy, với mục này, máy chủ local DNS sẽ không cố gắng tìm địa chỉ IP của nameserver của attack.com vì nó đã có địa chỉ IP rồi.

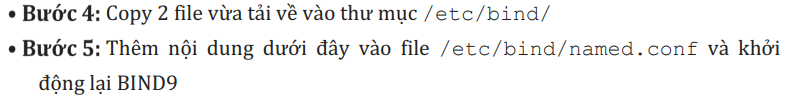


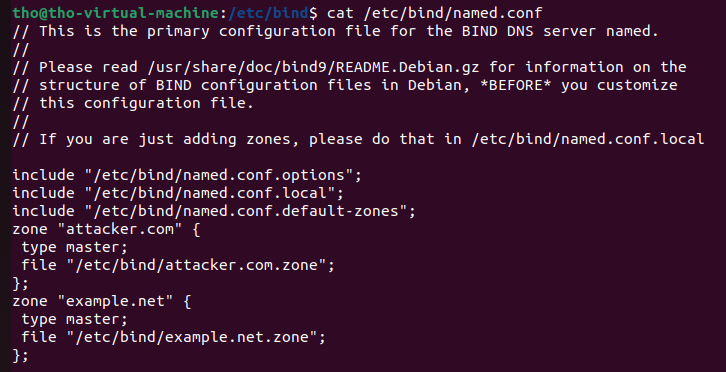


Nội dung của 2 file lần lượt như sau:



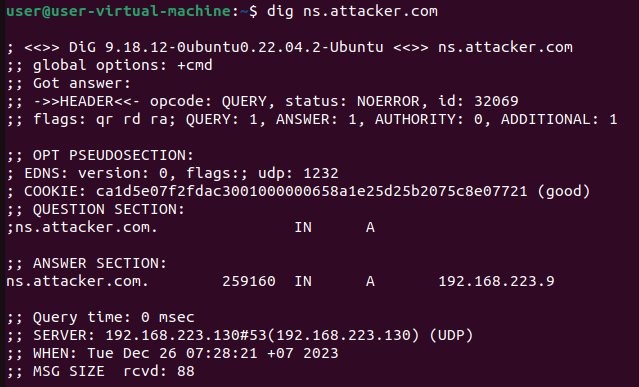






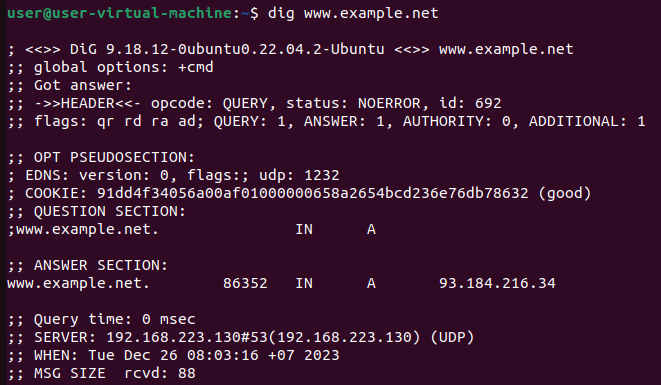


* Kiểm tra địa chỉ của ns.attacker.com: từ máy của user thực hiện lệnh truy vấn phân giải tên miền ns.attacker.com, kết quả ANWSER SECTION thu được địa chỉ IP là 192.168.223.9 giống như file đã cấu hình ở trên:



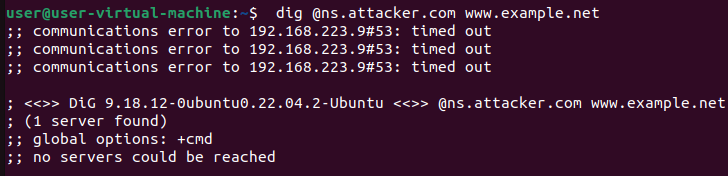
* Kiểm tra địa chỉ của [www.example.net](http://www.example.net) trong 2 trường hợp: Hai nameserver đang lưu trữ tên miền example.net, một là máy chủ tên chính thức của tên miền và cái còn lại là VM kẻ tấn công.
* TH 1: Gửi truy vấn đến local DNS server, máy chủ này sẽ gửi truy vấn tới máy chủ tên chính thức của example.net. Các địa chỉ IP xác thực của www.example.net là 93.184.216.34 và nameserver của nó được quản lý bởi Internet Corporation for Assigned Names and Numbers (ICANN):

dig [www.example.net](http://www.example.net)



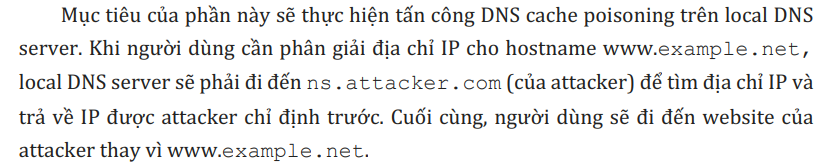
* TH 2: Gửi truy vấn trực tiếp đến ns.attacker.com:

dig @ns.attacker.com www.example.net



Ở đây user đã hỏi ns.attacker.com về địa chỉ IP của [www.example.net](http://www.example.net), tuy nhiên trong thực tế sẽ không ai làm như vậy, mà họ sẽ truy vấn trực tiếp đến namserver chính thức của example.net để tìm câu trả lời. Mục tiêu của cuộc tấn công này là để khiến nạn nhân hỏi ns.attacker.com địa chỉ IP của www.example.net. Cụ thể là, nếu cuộc tấn công của chúng ta thành công, nếu chúng ta chỉ chạy lệnh dig đầu tiên (là lệnh dig www.example.net), chúng ta sẽ nhận được kết quả giả mạo từ kẻ tấn công, thay vì nhận được kết quả xác thực từ nameserver chính thức của miền.



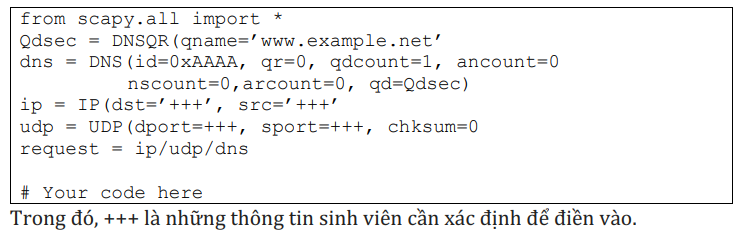




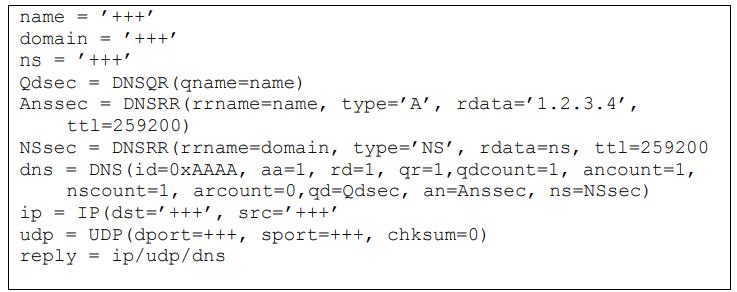
* Cần cài đặt scapy để phục vụ cho quá trình tạo ra gói tin DNS: nếu dùng cho python3 thì sử dụng lệnh sau:

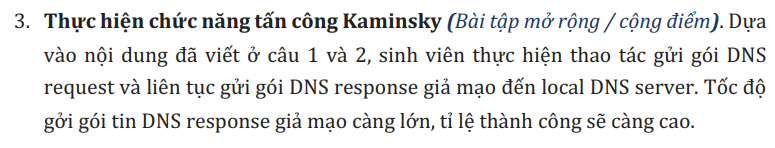
sudo pip3 install scapy

* Code tạo DNS request:









Do python tốc độ xử lý chậm nên để tạo ra gói tin giả sẽ khá tốn thời gian, do đó sẽ viết file tấn công bằng ngôn ngữ C để cải thiện tốc độ và sử dụng scapy để tạo gói tin DNS dễ dàng hơn. Vì vậy, chúng ta chỉ cần sử dụng Scapy để tạo DNS giả mạo gói và lưu nó vào một tập tin. Sau đó chúng ta tải gói vào chương trình C. Mặc dù chúng ta cần gửi rất nhiều của các gói DNS khác nhau trong cuộc tấn công Kaminsky, các gói này hầu hết đều giống nhau, ngoại trừ một số gói đặc thù. Do đó, chúng ta có thể sử dụng gói được tạo từ Scapy làm cơ sở, sau đó sẽ thay đổi (ví dụ như transaction ID) khi cần.





Chương trình Scapy sau đây tạo một gói trả lời DNS đơn giản, gói này được lưu vào một file:

* Kết quả tấn công:

Tại máy local DNS server:

