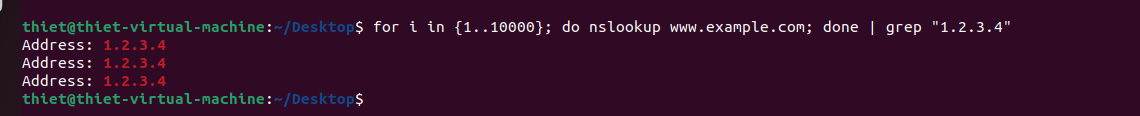
1. Tấn công giả mạo phản hồi trực tiếp đến người dùng (Directly Spoofing Response to User)



* Thực thi công cụ nslookup 10000 lần để xem số lần máy nhận địa chỉ IP giả mạo thì ta thấy có 3 lần máy nhận được ip giả mạo

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Bên máy attacker ta dùng công cụ netwox để nghe lén quá trình DNS request

1. Tấn công DNS Cache Poisoning

* Tấn công [www.example.org](http://www.example.org) và dùng grep để lọc số lần máy nạn nhân nhận địa chỉ ip của máy attacker

5. Tại sao khi thiết lập spoofip với giá trị raw, tỉ lệ thành công khi thực hiện hình thức tấn công này sẽ cao hơn?



* Xóa rỗng DNS cache tại DNS server



* Tại máy tấn công, sử dụng Netwox 105 như trong bài trước để thực hiện tấn công. Sử dụng filter với nội dung “src host 10.0.2.6” (sử dụng địa chỉ IP của DNS server). Có thể sử dụng thêm ttl (time-to-live) để chỉ định thời gian tồn tại trong bộ nhớ cache.

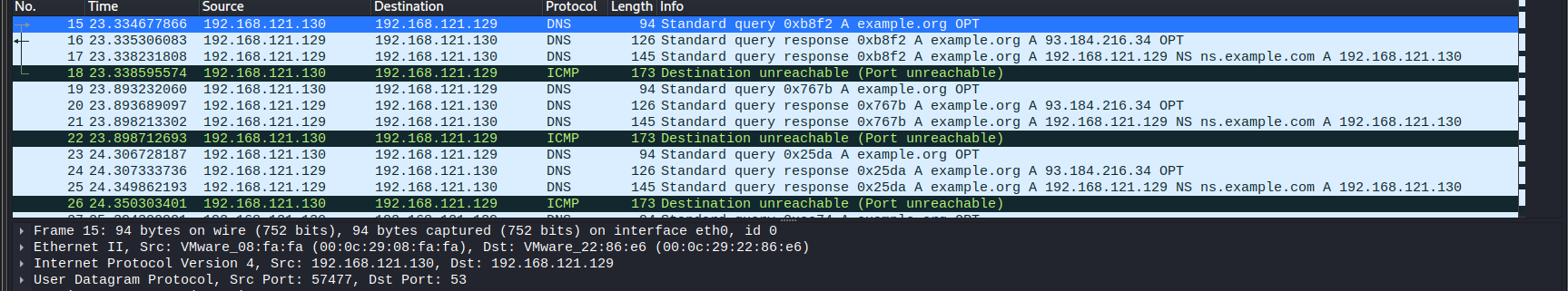
Ảnh có chứa văn bản, thiết bị điện tử

Mô tả được tạo tự động

* Kết quả sau khi thực hiện tấn công
* Ta thấy gần như lần nào máy nạn nhân cũng nhận địa chỉ ip của máy attacker



* Để nguyên trường spoofip nếu không, Netwox 105 sẽ cố gắng giả mạo địa chỉ MAC cho địa chỉ IP giả mạo. Để có được địa chỉ MAC, tool sẽ gửi một yêu cầu ARP, yêu cầu địa chỉ MAC của IP giả mạo. Địa chỉ IP giả mạo này thường là địa chỉ IP của một máy chủ DNS bên ngoài, không nằm trên cùng một mạng LAN. Do đó sẽ không có trả lời cho yêu cầu ARP. Tool sẽ đợi trả lời ARP một lúc trước khi tiếp tục mà không có địa chỉ MAC. Việc chờ đợi sẽ trì hoãn tool gửi phản hồi giả mạo. Nếu phản hồi DNS chính chủ trả sớm hơn phản hồi giả mạo thì cuộc tấn công sẽ thất bại.



* Sử dụng wireshark để bắt quá trình phân giải tên miền

6. Cách thức tấn công này có nhược điểm chỉ áp dụng trên các hostname cụ thể đã xác định trước (example.org). Nếu người dùng truy cập vào hostname khác (mail.example.org) thì không thể tấn công được. Sinh viên thực hiện tìm hiểu và thực hiện tấn công Authority Section để DNS servers lưu cache thông tin nameserver giả mạo

Ảnh có chứa văn bản

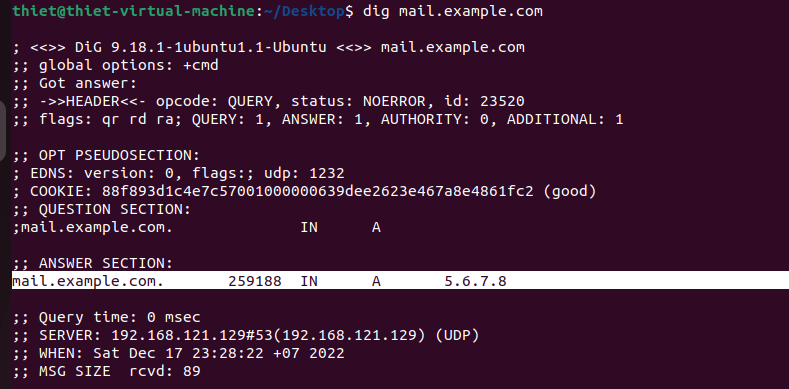
Mô tả được tạo tự động

* Source code dùng để tấn công

Ảnh có chứa văn bản

Mô tả được tạo tự động

* Bên máy attacker ta thực hiện chạy file để tấn công



* Bên máy user ta dùng dig để phân giải tên miền và thấy mail.example.com đã nhận địa chỉ IP giả

Ảnh có chứa văn bản

Mô tả được tạo tự động

* File dump cache của DNS server đã nhận và lưu namserver của giả mạo

Ảnh có chứa văn bản

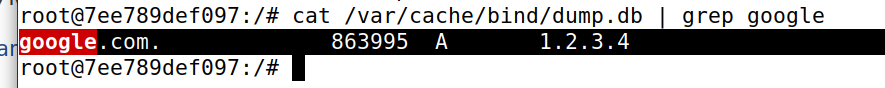
Mô tả được tạo tự động

* Ta cũng có thể tấn công domain google.com

Ảnh có chứa văn bản

Mô tả được tạo tự động

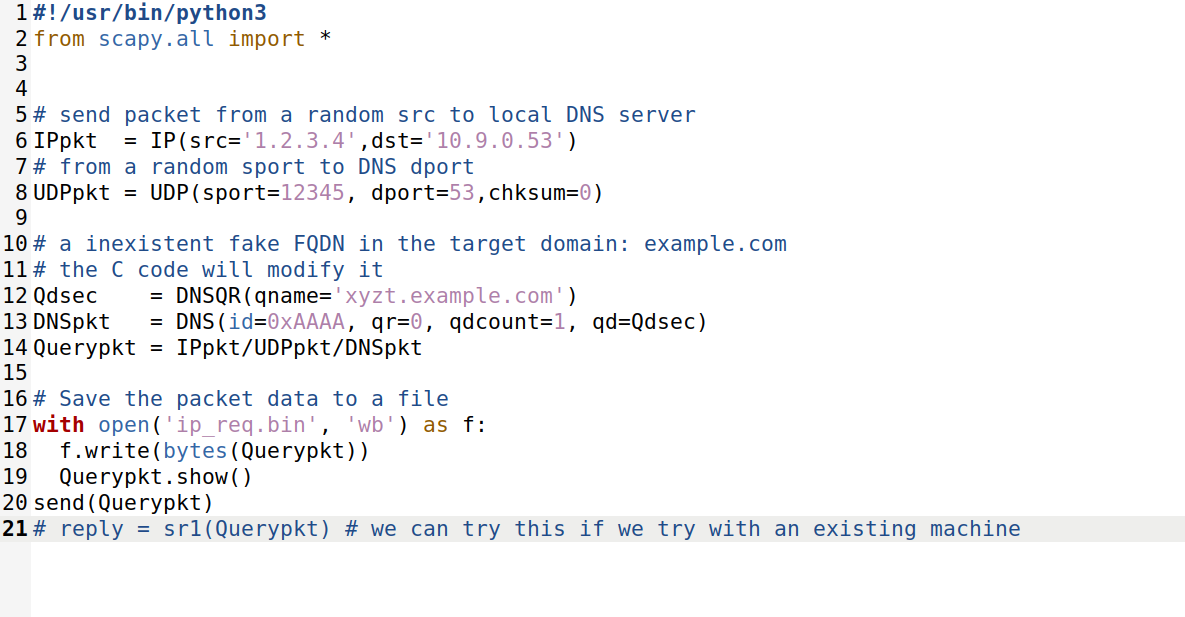
* Sau khi tấn công thì địa chỉ của google.com là ip giả mạo ta đã cài sẵn



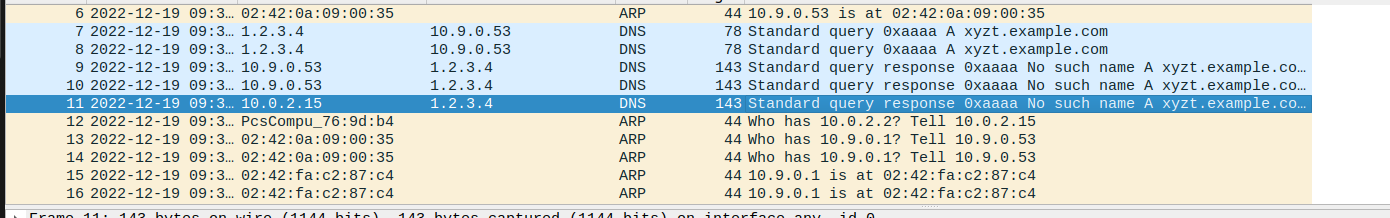
* Cache của DNS server cũng đã bị poison bởi ip giả ta đã cài sẵn

1. Tấn công Kaminsky

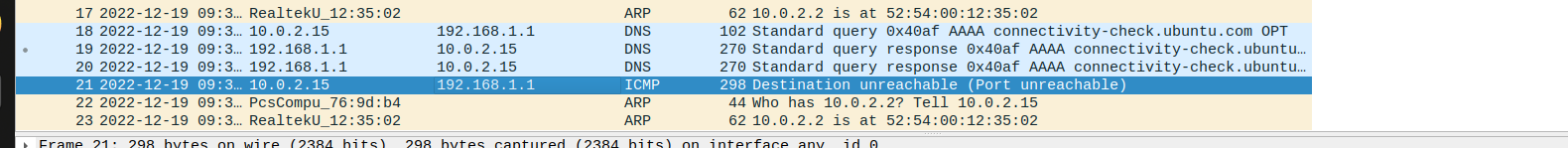
* Đầu tiên ta cần gửi các yêu cầu DNS đến một hostname không tồn tại “xyzt.example.com”
* Và khi DNS server nhận được yêu cầu truy vấn do hostname này chưa có trong cache nên local server sẽ tạo yêu cầu truy vấn đến namserver của example.com



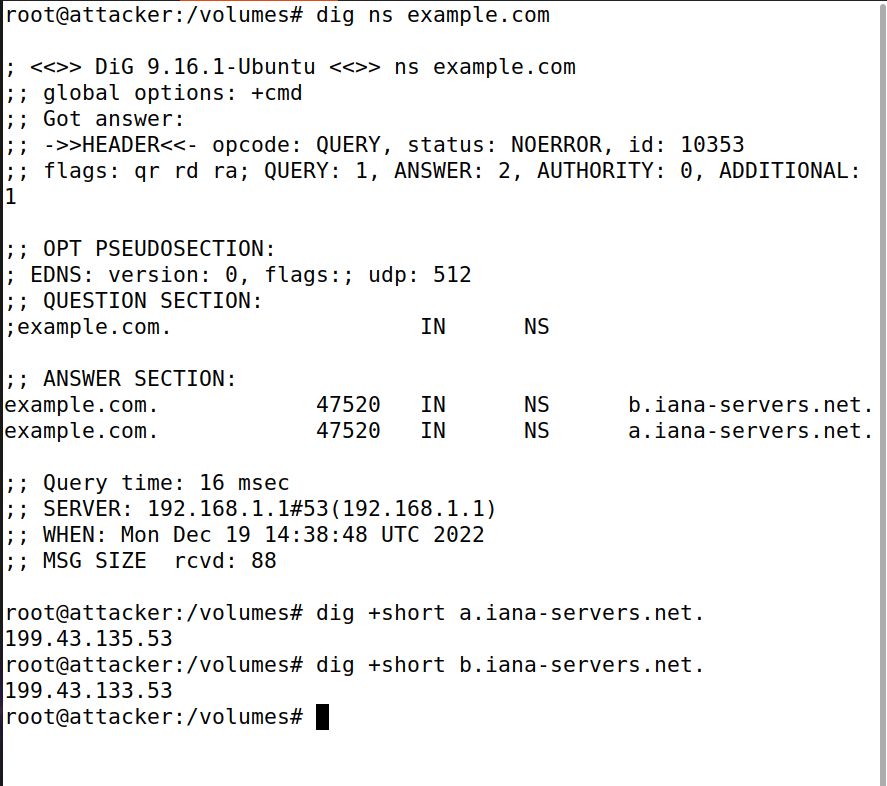
* Code dùng để tạo một truy vấn DNS server



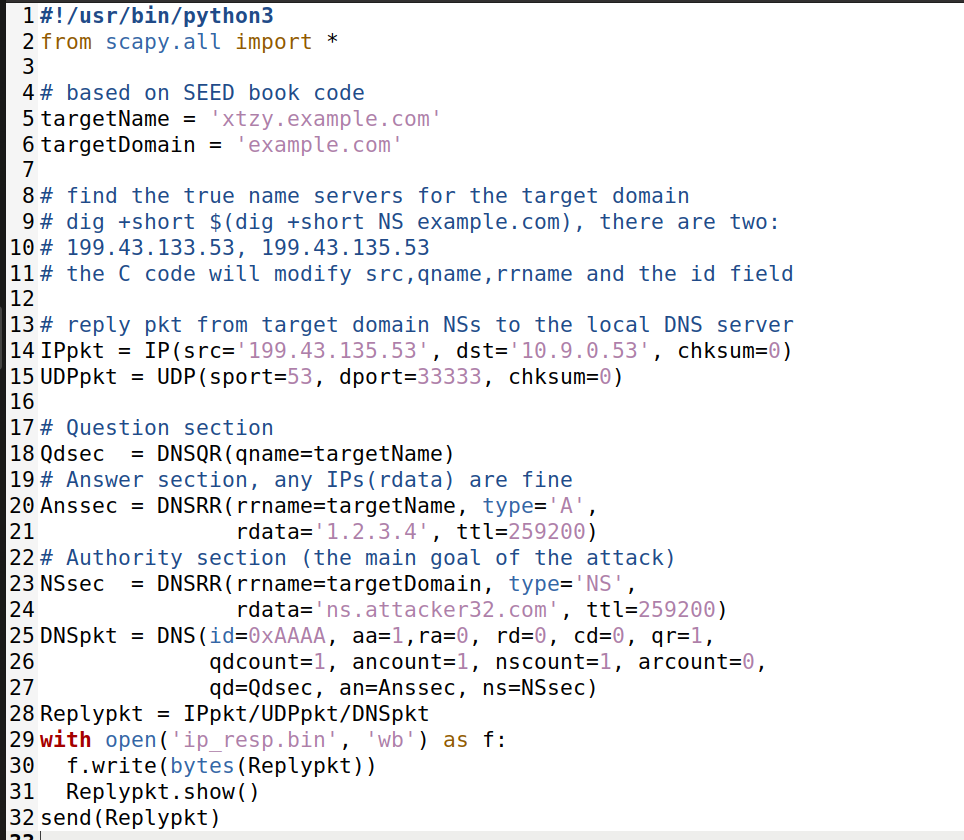
* Dùng wireshark ta thấy được gói tin DNS cho hostname “xyzt.example.com”
* Do chưa có trong cache nên khi nhân được local DNS server tạo yêu cầu truy vấn đến namserver của example.com



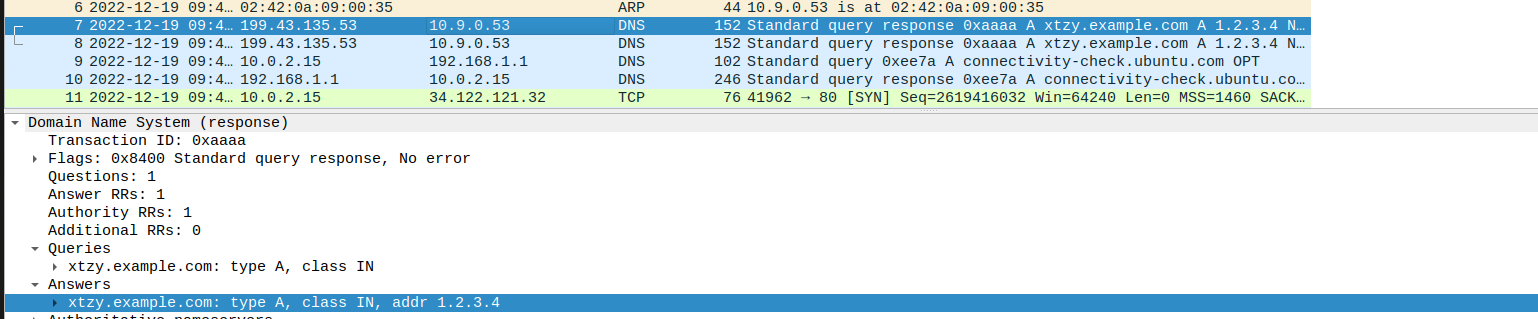
* Do đây là tên miền giả của attacker và chưa nhận được phản hồi nên sẽ có gói tin trả về là unreachable
* Tiếp theo ta sẽ cần spoof gói tin DNS để giả mạo các câu trả lời từ nameserver của domain này



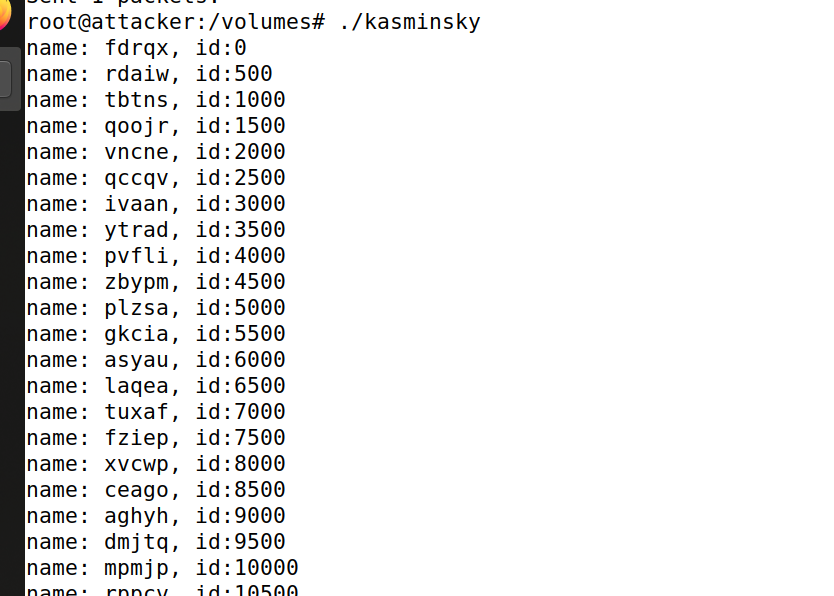
* Đầu tiên ta cần biết được IP của máy chủ định danh của example.com ở đây có 2 máy chủ cho tên miền này là “199.43.135.53” và “199.43.133.53”



* Từ IP máy chủ định danh lấy được ta dùng để viết code thực thi để giả mạo phản hồi DNS cho domain example.com



* Trong wireshark ta thấy được phản hồi DNS chứa địa chỉ IP 1.2.3.4 trong section answer dưới dạng IP của domain example.com
* Từ 2 phần trên để thực hiện tấn công ta cần gửi nhiều DNS response với transaction ID khác nhau để cung cấp IP cho xyzt.example.com và kèm theo “Authoritative Nameservers” để xác định ns.attacker.com là nameserver của tên miền example.com và nếu có 1 DNS reponse giả đúng ID và đến local DNS trước khi DNS response đúng thì DNS server sẽ chấp nhận và lưu cache thông tin này
* Trường hơp thất bại thì có thể dùng hostname khác để tiếp tục thử và nếu thành công thì tại local DNS server nameserver của exmaple.com sẽ được thay thế bằng ns.attacker.com



* Sau khi thực thi file để khai thác ta thấy nó gửi nhiều gói response với nhiều id khác nhau

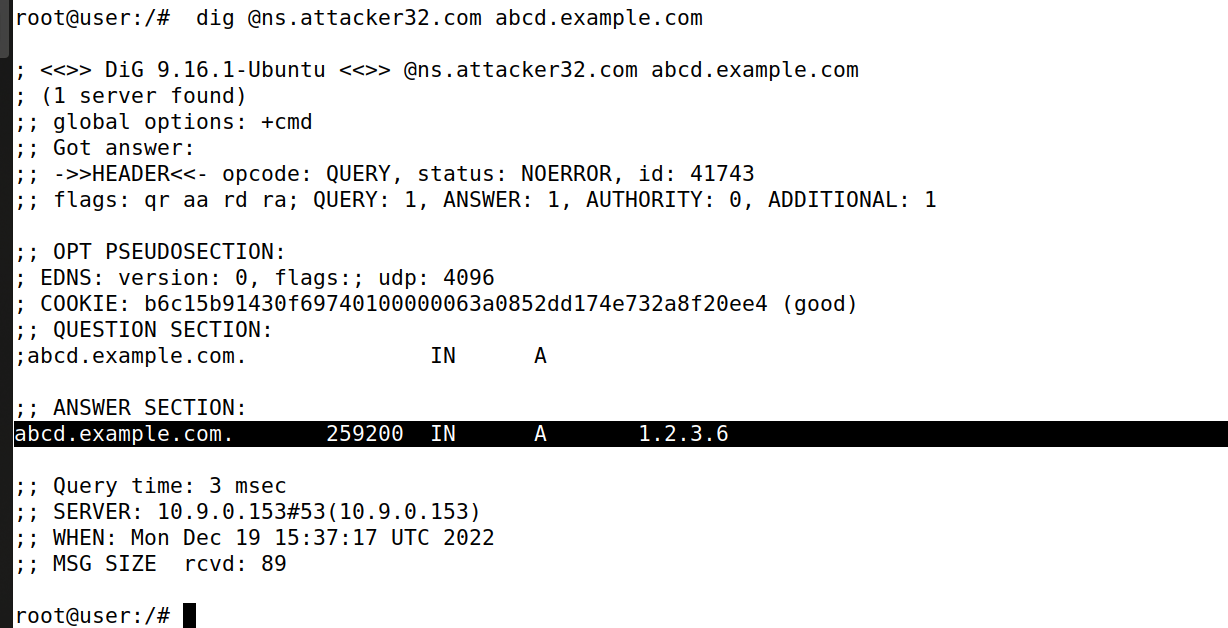
Ảnh có chứa bàn

Mô tả được tạo tự động

* Ta xem cache của local DNS thấy NS record của example.com đã thành của ns.attacker32.com và khi máy chủ nhận được truy vấn DNS cho hostname exmaple.com nó sẽ gửi đến ns.attacker32.com thay vì gửi đến máy chủ định danh hơp [háp của tên miền

Ảnh có chứa văn bản

Mô tả được tạo tự động



* Ta thấy khi truy vấn tên miền abcd.example.com với bình thường và dưới @ns.attacker32.com thì địa chỉ IP đều như nhau nghĩa là cache đã bị đầu độc bởi nameserver của attacker