BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng máy tính**

**Lab 5: DNS Attack**

*GVHD: Đoàn Minh Trung*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT140.O12.ATCL – Nhóm 03

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Bùi Hoàng Trúc Anh | 21521817 | [21521817@gm.uit.edu.vn](mailto:21521817@gm.uit.edu.vn) |
| 2 | Lê Hoàng Oanh | 21521253 | 21521253@gm.uit.edu.vn |
| 3 | Nguyễn Ngọc Trà My | 21520353 | [21520353@gm.uit.edu.vn](mailto:21520353@gm.uit.edu.vn) |
| 4 | Huỳnh Minh Tân Tiến | 21521520 | 21521520@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-2)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | Bài 1 | 100% |
| 2 | Bài 2 | 100% |
| 3 | Bài 3 | 100% |
| 4 | Bài 4 | 100% |
| 5 | Bài 5 | 100% |
| 6 | Bài 6 | 100% |
| 7 | Bài 7 | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

1. **Trước khi thực hiện bài thực hành, sinh viên tìm hiểu và cho biết: Khi người dùng thực hiện truy vấn phân giải tên miền sang địa chỉ IP, quá trình này sẽ được thực hiện như thế nào (tại máy người dùng, trong cùng mạng LAN, DNS Servers,…)**

Quá trình phân giải tên miền (DNS resolution) từ tên miền sang địa chỉ IP thường bao gồm các bước sau:

1. Máy Người Dùng:

- Người dùng nhập một tên miền vào trình duyệt hoặc ứng dụng.

- Trước hết, trình duyệt sẽ kiểm tra xem địa chỉ IP của tên miền đã được lưu trong bộ nhớ cache của nó chưa. Nếu có, quá trình phân giải có thể kết thúc tại đây và không cần thực hiện các bước phức tạp hơn.

2. Máy Người Dùng Gửi Yêu Cầu Đến DNS Resolver:

- Nếu thông tin không có trong cache hoặc cache đã hết hạn, máy người dùng sẽ gửi yêu cầu DNS đến DNS resolver. DNS resolver thường là máy chủ DNS được cấu hình trong cài đặt mạng của máy người dùng hoặc là DNS resolver của nhà mạng.

3. DNS Resolver:

- DNS resolver là máy chủ DNS trung gian giữa máy người dùng và DNS server. Nếu thông tin cần thiết không có trong cache của nó, resolver sẽ bắt đầu quá trình truy vấn.

4. Truy Vấn DNS Server:

- DNS resolver sẽ gửi yêu cầu truy vấn DNS đến một hoặc nhiều máy chủ DNS. Trong một số trường hợp, resolver có thể cần tương tác với nhiều máy chủ DNS để lấy được đáp ứng.

5. DNS Server Phụ Trách Tên Miền:

- DNS server phụ trách tên miền được yêu cầu sẽ kiểm tra xem nó có thông tin về tên miền đó trong bộ nhớ cache của mình không. Nếu có, nó sẽ trả về địa chỉ IP tương ứng mà không cần thực hiện các bước tiếp theo.

6. Truy Vấn Tới DNS Root Server (Nếu Cần):

- Nếu DNS server không biết địa chỉ IP của tên miền và không có trong cache, nó sẽ thực hiện một truy vấn tới máy chủ DNS gốc (DNS root server).

7. Truy Vấn Tới DNS Top-Level Domain (TLD) Server (Nếu Cần):

- DNS root server sẽ hướng dẫn DNS resolver tới máy chủ DNS thuộc top-level domain (TLD) của tên miền (ví dụ: .com, .org, .net).

8. Truy Vấn Tới Authoritative DNS Server Của Domain:

- DNS TLD server sẽ hướng dẫn resolver tới máy chủ DNS chịu trách nhiệm cho tên miền cụ thể mà người dùng đang truy vấn, được gọi là authoritative DNS server.

9. Địa Chỉ IP Được Trả Về:

- Authoritative DNS server sẽ trả về địa chỉ IP tương ứng với tên miền và DNS resolver sẽ chuyển thông tin này về máy người dùng.

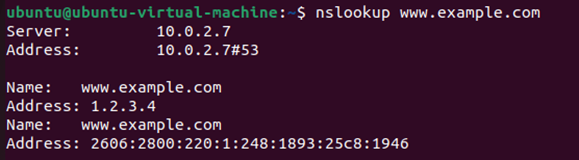
10. Máy Người Dùng Nhận Địa Chỉ IP:

- Máy người dùng nhận được địa chỉ IP và sử dụng nó để thực hiện kết nối đến máy chủ tương ứng.

Quá trình trên giúp định danh và kết nối các máy chủ thông qua tên miền, giúp người dùng dễ nhớ và sử dụng địa chỉ IP một cách thuận tiện.

1. **Mô tả kết quả nhận được từ quá trình phân giải tên miền ww.example.com khi sử dụng và không sử dụng netwox 105.**

**Khi sử dụng netwox 105**



Khi chạy lệnh netwox, máy attacker gửi một gói tin DNS giả mạo đến máy client (10.0.2.6) với thông tin như trên. Khi máy client nhận được gói tin DNS giả mạo, nó sẽ tin rằng đó là gói tin DNS hợp lệ từ máy chủ DNS (10.0.2.7) và sẽ cập nhật bảng DNS cache của nó với thông tin giả mạo đó. Do đó, khi chạy lệnh nslookup trên máy client, sẽ thấy kết quả như sau:

* Server: 10.0.2.7: Đây là địa chỉ IP của máy chủ DNS mà máy client tin rằng nó đang truy vấn.
* Address: 10.0.2.7#53: Đây là địa chỉ IP và cổng của máy chủ DNS mà máy client tin rằng nó đang truy vấn.
* Name: www.example.com: Đây là tên miền mà máy client muốn phân giải.
* Address: 1.2.3.4: Đây là địa chỉ IP giả mạo mà máy client nhận được từ gói tin DNS giả mạo. Đây là địa chỉ IP mà máy client sẽ sử dụng để kết nối với www.example.com.
* Name: www.example.com: Đây là tên miền mà máy client muốn phân giải.
* Address: 2606:2800:220:1:248:1893:25c8:1946: Đây là địa chỉ IP thực của www.example.com, được trả về bởi máy chủ DNS thật. Đây là địa chỉ IP mà máy client sẽ sử dụng để kết nối với www.example.com nếu nó hỗ trợ IPv6.

**Khi không sử dụng netwox 105**

A screenshot of a computer

Description automatically generated

Kết quả này cho thấy một truy vấn nslookup được thực hiện từ máy ảo Ubuntu để phân giải tên miền www.example.com. Máy chủ DNS có địa chỉ IP là 10.0.2.7 đã trả lời truy vấn, chỉ ra rằng địa chỉ IP của www.example.com là 192.168.0.101.

Điều này có nghĩa là, khi không sử dụng netwox, máy client sẽ nhận được thông tin DNS chính xác từ máy chủ DNS. Máy chủ DNS sẽ tra cứu tên miền www.example.com trong bảng DNS zone của nó và trả về địa chỉ IP tương ứng. Địa chỉ IP 192.168.0.101 là địa chỉ IP nội bộ của www.example.com trong mạng riêng. Đây là địa chỉ IP mà máy client sẽ sử dụng để kết nối với [www.example.com](http://www.example.com).

1. **Xác suất tấn công thành công là bao nhiêu (với số lần thử > 30). Đề xuất giải pháp để nâng cao tỉ lệ tấn công thành công.**

Ở máy attacker, ta tiếp tục sử dụng netwox. Ở máy user, ta viết file bash để thực hiện lệnh nslookup đến www.example.com 1000 lần.

A close-up of a website

Description automatically generated

Ta thực hiện file bash và nhận được nhiều kết quả không thành công.

A screenshot of a computer

Description automatically generated

Và cũng một số lần tấn công thành công.

A screenshot of a computer

Description automatically generated

Như vậy sau khi hoàn thành và thực hiện kiểm tra thống kê thì cứ 1000 lần thực hiện thì sẽ có được từ 20 đến 25 lần thành công như vậy xác suất là 2 - 2.5% tỉ lệ thành công.

Để nâng cao tỉ lệ tấn công thành công, bạn có thể thử các giải pháp sau:

* Sử dụng một tham số --spoofip khác để giả mạo địa chỉ IP nguồn. Tham số này cho phép bạn tạo liên kết để giả mạo ở cấp độ IP4/IP6 hoặc cấp độ liên kết. Bạn có thể thử các giá trị như ‘raw’, ‘link’, ‘best’, hoặc các sự kết hợp của chúng.
* Sử dụng một tham số --ttl khác để đặt thời gian sống của câu trả lời DNS. Tham số này cho phép bạn xác định thời gian mà câu trả lời DNS sẽ được lưu trong bộ nhớ cache của máy chủ DNS. Bạn có thể thử các giá trị như 0, 1, hoặc một số lớn hơn.
* Sử dụng một tham số --filter khác để lọc các gói tin DNS. Tham số này cho phép bạn hạn chế các gói tin được bắt. Bạn có thể sử dụng các yếu tố lọc như host, net, port, dst, src, ether, ip, arp, rarp, tcp, icmp, udp. Bạn có thể thử các bộ lọc khác nhau như “host 10.0.2.6 and udp”, “net 10.0.2.0/24 and dst port 53”, hoặc "ether src 00:0c:29:8a:5c:5f and icmp".

1. **Cần làm gì để hạn chế được nguy cơ tấn công của cơ chế này.**

Tuy nhiên, nếu bạn muốn giảm thiểu nguy cơ tấn công từ câu lệnh này, bạn có thể thực hiện một số biện pháp bảo mật:

1. Firewall:

Cấu hình firewall trên máy chủ của bạn để chỉ cho phép các kết nối và gói tin cần thiết.

Hạn chế truy cập vào các cổng không cần thiết để giảm khả năng bị tấn công.

1. Bảo vệ chống tấn công DDoS:

Sử dụng các giải pháp bảo vệ chống tấn công DDoS để đảm bảo rằng hệ thống của bạn có khả năng chống lại các cuộc tấn công phủ định dịch vụ.

1. Cập nhật và Patching:

Đảm bảo hệ điều hành và tất cả các ứng dụng đang chạy trên máy chủ của bạn đều được cập nhật đầy đủ và có các bản vá bảo mật mới nhất.

1. Kiểm soát quyền truy cập:

Chỉ cấp quyền truy cập cần thiết cho người dùng và quy trình hệ thống.

1. Ghi log và giám sát:

Bật chế độ ghi log chi tiết để theo dõi các hoạt động trên hệ thống.

Sử dụng giải pháp giám sát mạng để phát hiện các hoạt động không bình thường.

1. Tích hợp IDS/IPS:

Sử dụng Hệ thống Phát hiện Xâm nhập (IDS) và Hệ thống Ngăn chặn Xâm nhập (IPS) để giám sát và ngăn chặn các hành vi xâm nhập.

1. Bảo vệ DNS:

Kiểm soát quyền truy cập vào máy chủ DNS và hạn chế các loại truy vấn có thể được thực hiện.

1. Tối ưu hóa SSL/TLS:

Sử dụng phiên bản mới nhất của SSL/TLS và cấu hình chúng đúng cách để tăng cường bảo mật.

1. **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?**

“--spoofip raw” được sử dụng để đặt giá trị "raw" cho phần spoofip. Giá trị ‘raw’ có nghĩa là giả mạo ở cấp độ IP4/IP6 (nó sử dụng ngăn xếp IP của hệ thống). Tuy nhiên, lý do cụ thể khiến tỉ lệ thành công tăng cao hay thấp hơn với giá trị "raw" phụ thuộc vào môi trường cụ thể và cách mà các thiết bị mạng và hệ thống bảo vệ chống lại tấn công DNS spoofing.

Dưới đây là một số nguyên nhân có thể giải thích tại sao sử dụng giá trị "raw" có thể tăng cường khả năng tấn công:

* Bypassing Security Measures: Các hệ thống bảo mật và thiết bị tường lửa có thể kiểm tra và lọc các gói tin DNS dựa trên định dạng và cấu trúc của chúng. Sử dụng giá trị "raw" có thể giúp bypass các kiểm tra này, làm cho gói tin giả mạo trở nên khó phát hiện hơn.
* Custom Packet Crafting: Khi sử dụng giá trị "raw," bạn có thể tùy chỉnh chính xác cấu trúc và nội dung của gói tin DNS giả mạo. Điều này có thể giúp bạn tạo ra gói tin mà các hệ thống bảo mật khó nhận biết.
* Exploiting Vulnerabilities: Các giá trị raw có thể được sử dụng để tận dụng những lỗ hổng cụ thể trong cách mà các ứng dụng hoặc hệ thống xử lý gói tin DNS.

Khi thiết lập spoofip với giá trị raw, tỉ lệ thành công khi thực hiện hình thức tấn công này sẽ cao hơn vì bạn có thể lừa đảo máy chủ DNS rằng bạn là một máy chủ DNS có thẩm quyền hoặc một máy khách DNS hợp lệ. Điều này có thể gây ra các vấn đề về an ninh mạng, như tấn công từ chối dịch vụ phân tán (DDoS) hoặc chuyển hướng người dùng đến các trang web độc hại .

1. **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.**

Ta sẽ thực hiện cài đặt gói tin và gửi gói tin giả mạo khi người dùng dig example.org và với hostname khác như www.example.org thì vẫn tấn công được.

File code python:

A screenshot of a computer program

Description automatically generated

Thực thi gửi gói tin

A screenshot of a computer program

Description automatically generated

Kết quả trên máy user

A computer screen shot of a computer

Description automatically generated

Tấn công Kaminsky

Thực hiện cấu hình named.conf

A screenshot of a computer

Description automatically generated

Thực hiện cấu hình attacker.com.zone và example.com.zone

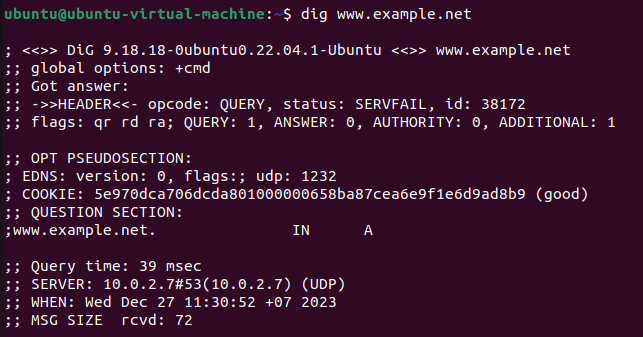
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Thực hiện kiểm tra thiết lập với dig example



Thực hiện việc tấn công

Code python để tạo ra DNS request và thực hiện gửi gói tin

A screen shot of a computer

Description automatically generated

Sử dụng Wireshark để kiểm tra, có thể thấy gói tin đã được gửi thành công

A computer screen shot of a code

Description automatically generated

A screenshot of a computer

Description automatically generated

Code python để gửi reply giả mạo

A screen shot of a computer program

Description automatically generated

Kiểm tra bằng Wireshark thì thấy đã gửi các gói tin thành công, tấn công thành công

A computer screen shot of white text

Description automatically generated

A computer screen with a blue and white line

Description automatically generated

1. **DNS - zone transfert (Viết writeup chi tết)**

**Statement**

**A not really dutiful administrator has set up a DNS service for the “ch11.challenge01.root-me.org" domain...**

**Challenge connection informations :**

* **Host: challenge01.root-me.org**
* **Protocol: DNS**
* **Port: 54011**

Với port , host, và domain đã được cung cấp, Dig với cái thông tin đã được cung cấp   
dig @challenge01.root-me.org -p 54011 ch11.challenge01.root-me.org any

Option any dùng để truy vấn tất cả các record dns của 1 tên miền

A computer screen shot of a computer code

Description automatically generated

Truy cập vào domain name challenge01.root-me.org

A screenshot of a computer

Description automatically generated

Xuất hiện yêu cầu authentic, sau khi sign up và dig lại thử thì được kết quả

A computer screen shot of a computer screen

Description automatically generated

Upload key lên web và check:

A close-up of a blue and white rectangle

Description automatically generated

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-2)