|  |  |  |  |
| --- | --- | --- | --- |
| **Các các tấn công DNS Server** | | | |
| **Type** | **Test-Case** | **Exploit** | **Example** |
| DNS spoofing | Là một phương pháp tấn công máy tính nhờ đó mà dữ liệu được thêm vào hệ thống cache của các DNS server. Từ đó, các địa chỉ IP sai (thường là các địa chỉ IP do attacker chỉ định) được trả về cho các truy vấn tên miền nhằm chuyển hướng người dùng tư một website này sang một website khác | Attacker lợi dụng lỗ hổng của phần mềm DNS, do các DNS responses không được xác nhận để đảm bảo chúng được gửi từ các server được xác thực, các bản ghi không đúng đắn sẽ được cache lại và phục vụ cho các user khác. | Attacker thay thế địa chỉ IP cho một bản ghi DNS trên DNS server thành địa chỉ IP của server mà attacker đang có quyền điều khiển. Trên server này, attacker có triển khai một số phần mềm mã độc để khi người dùng bị chuyển qua sẽ dễ dàng bị nhiễm mã độc. |
| **DNS Amplification Attack** | Đây là một trong những phương pháp được sử dụng để tấn công từ chối dịch vụ, thuộc vào lớp reflection attack. | – Địa chỉ tấn công được che giấu nhờ ánh xạ sang một bên thứ ba (Reflection)  – Traffic mà người bị hại nhận được sẽ lớn hơn traffic gửi từ attacker (Amplification) |  |
| **Giả mạo máy chủ DNS** | Là cách một số phần mềm quảng cáo hay trojan thường hay thực hiện. Đầu tiên, chúng dựng lên các DNS server, giống với chức năng DNS server thông thường. Tuy nhiên, các DNS server này có khả năng điều khiển được để thêm, bớt hay chỉnh sửa các bản ghi DNS nhằm chuyển hướng người dùng tới các địa chỉ IP không chính xác với mục đích: gia tăng quảng cáo, cài mã độc, thay đổi kết quả tìm kiếm | Các phần mềm độc hại sau khi được cài vào máy tính người dùng, chúng sẽ tìm cách để thay đổi cấu hình DNS của người dùng thành địa chỉ DNS của phần mềm đã thiết lập từ trước. Qua đó, các truy vấn DNS của người dùng thay vì đi qua các DNS server của ISP hoặc do người dùng thiết lập thì lại đi qua các DNS server của attacker.  Một biến thể của hình thức này chính là việc các phần mềm độc hại thay đổi file host (Trên hệ điều hành Windows) để chỉ định địa chỉ IP cho một số website mà attacker mong muốn. | Giả mạo máy chủ DNS của Google để thực hiện tấn công DDOS thông qua SNMP |
| DNS Hijacking (còn được gọi là DNS Redirection) | Là loại tấn công độc sẽ ghi đè máy tính TCP/IP đến điểm máy chủ DNS giả mạo, do đó hủy bỏ hiệu lực các thiết lập DNS mặc định. Nói cách khác, khi kẻ tấn công kiểm soát máy tính để thay đổi các thiết lập DNS, để nó chỉ đến máy chủ DNS giả mạo, quá trình này được gọi là DNS Hijacking. | Pharming: Đây là loại tấn công mà lưu lượng truy cập của trang web được chuyển hướng đến trang web khác là giả. Ví dụ, khi người dùng cố gắng truy cập vào trang web mạng xã hội như [Facebook.com](https://Facebook.com/), nó sẽ được chuyển hướng đến trang web khác với cửa sổ pop-up và quảng cáo. Điều này thường được thực hiện bởi các tin tặc để tạo ra doanh thu quảng cáo.  Phishing: Đây là loại tấn công mà người dùng được chuyển hướng đến trang web độc. Ví dụ, khi người dùng cố gắng đăng nhập vào tài khoản ngân hàng, nó osẽ chuyển hướng đến trang web độc với việc đánh cắp thông tin đăng nhập của người dùng. |  |