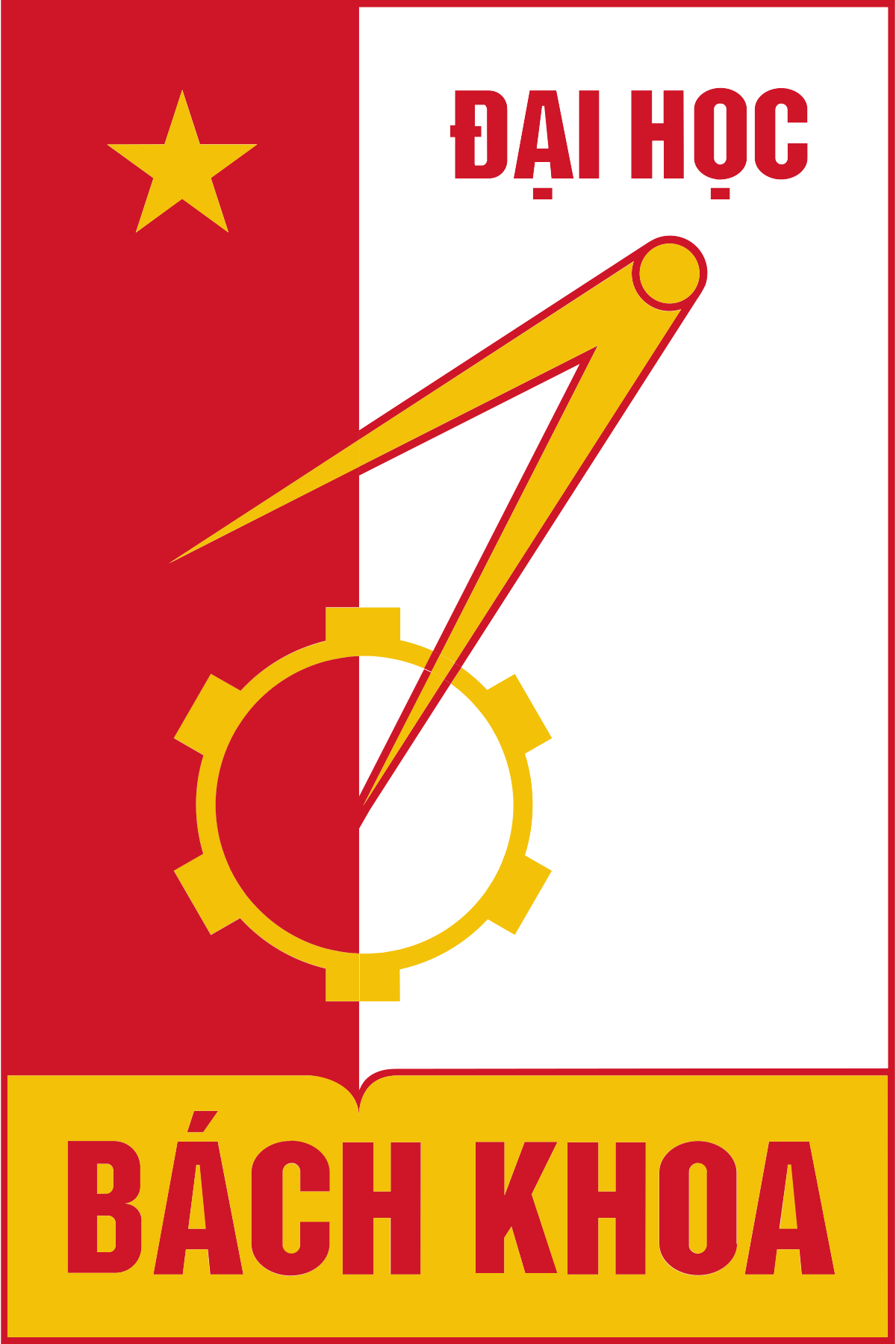
**ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

**─────── \* ───────**

****

**BÁO CÁO TUẦN 3**

Môn học: Project II (IT - 3931)

Đề tài: Network Security with IDS/IPS: Detection and Prevention of Network Attacks in a Virtualized Environment

|  |  |
| --- | --- |
| **Sinh viên thực hiện:** | **Ngô Trung Hiếu - 20225316**  **Kỹ thuật máy tính 04 – K67** |
| **Giảng viên hướng dẫn:** | **Nguyễn Quốc Khánh** |

**Hà Nội – 2025**

**Mục lục**

[I. Truy cập website dvwa từ máy ảo attacker 4](#_Toc210829080)

[II. Tạo Snort rule cơ bản 9](#_Toc210829081)

[III. Mô phỏng Brute force attack 15](#_Toc210829082)

[a. Cài đặt foxyproxy và burp suite 15](#_Toc210829083)

[b. Viết snort rule chống lại brute force 19](#_Toc210829084)

## Truy cập website dvwa từ máy ảo attacker

Đặt địa chỉ IP tĩnh

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

NAT rule trên pfsense cho phép gói tin ICMP đi từ máy ảo attacker (10.0.2.4) đi đến máy ảo victim (192.168.1.101)

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

Tải snort cho pfsense, ta vào System 🡪 Package Manager 🡪 Available Packages. Sau đó ta tìm kiếm snort package để tải về.

A screenshot of a computer

AI-generated content may be incorrect.

Sau đó ta có thể kiểm tra kết quả download ở Installed Packages

A screenshot of a computer

AI-generated content may be incorrect.

Tạo thêm rule cho phép máy ảo attacker truy cập website dvwa trên máy ảo victim. Ta vào Firewall 🡪 NAT 🡪 Port Forward, vào thêm 2 rule cho phép máy ảo attacker gửi gói tin TCP cổng 80 (http) và 443 (https) truy cập đến DVWA trên máy ảo victim.

A screenshot of a computer

AI-generated content may be incorrect.

Truy cập website DVWA trên máy ảo attacker với url: <http://192.168.1.101/dvwa>, trong đó 192.168.1.101 là địa chỉ IP của máy ảo victim. Tài khoản và mật khẩu truy cập lần lượt là *dvwa* và *password*

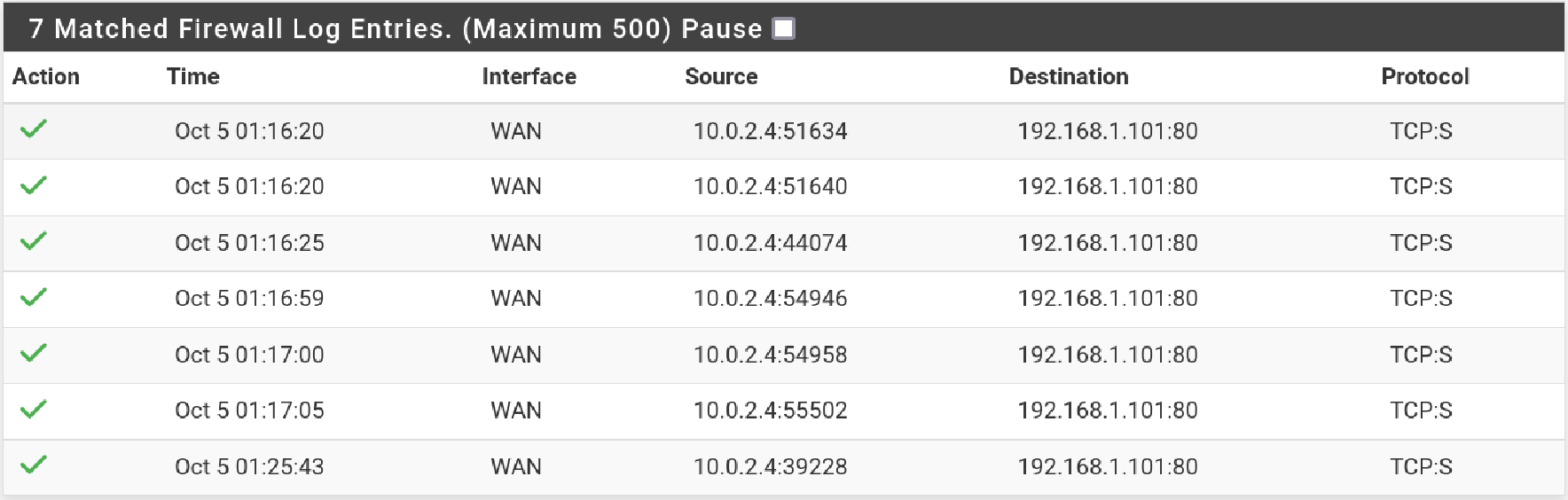
A screenshot of a computer

AI-generated content may be incorrect.

Màn hình chính

A screenshot of a computer

AI-generated content may be incorrect.



## Tạo Snort rule cơ bản

Snort package là tập hợp đầy đủ các thành phần giúp phát hiện, cảnh báo và ngăn chặn tấn công mạng. Trong đó:

Snort Engine: lõi xử lý, phân tích gói tin mạng.

Rules: tập luật phát hiện tấn công (community, registered, ET).

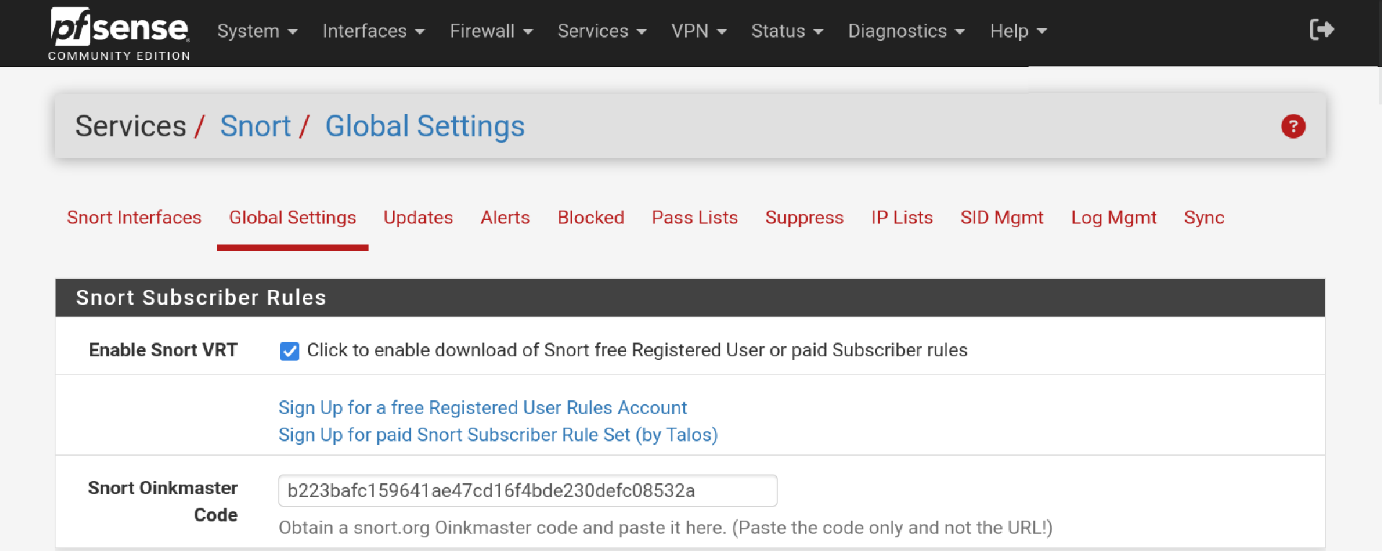
Preprocessors: tiền xử lý gói tin, phát hiện bất thường như port scan, HTTP lỗi.

Detection Engine: so khớp gói tin với rules để phát hiện hoặc chặn tấn công.

Output Plugins: ghi log, cảnh báo hoặc xuất dữ liệu ra giao diện.

Giao diện quản lý (GUI): trên pfSense giúp cấu hình, xem alert và cập nhật rules dễ dàng.

Vì nó bao gồm các tập luật sẽ có ích trong việc thử nghiệm các tấn công mà không phải viết lại tự đầu, nên ta sẽ cài Snort package trên pfSense và cấu hình global. Ta chọn Service 🡪 Snort 🡪 Global Settings. Chọn *Enable Snort VRT* để cho phép tải xuống các tập luật miễn phí, và chọn một số Snort package của community.



A screenshot of a computer

AI-generated content may be incorrect.

Sau khi lựa chọn các package xong ta chọn *Save* để Snort có thể bắt đầu tải về. Ta có thể xem tình trạng tải xuống ở Services 🡪 Snort 🡪 Updates.

A screenshot of a computer

AI-generated content may be incorrect.

Để có thể tạo luật cho chế độ IDS Snort, ta sẽ sang Services 🡪 Snort 🡪 Interfaces.

A screenshot of a computer

AI-generated content may be incorrect.

Em sẽ tạo luật phát hiện gói tin ICMP của máy ảo attacker gửi cho máy ảo victim với thông điệp *“ICMP detected 10.0.2.4”*. Sau đó, để kiểm tra luật có hoạt động thành công không, ta thử ping từ attacker sang victim, rồi qua phần Services 🡪 Snort 🡪 Alerts.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Ta kiểm tra tương tự với gói tin TCP khi đăng nhập trang web dvwa trên máy ảo victim được máy ảo attacker gửi đi.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Ngoài ra, ta có thể xuất file .pcap từ pfsense để có thể lấy gói tin đó cho Wireshark phân tích nội dung. Đầu tiên, ta vào Diagnostics 🡪 Packet Capture và chọn *Start* để pfsense bắt đầu lắng nghe.

A screenshot of a computer

AI-generated content may be incorrect.

Sau đó ta đăng nhập vào dvwa từ máy attacker.

A screenshot of a computer

AI-generated content may be incorrect.

Cuối cùng chọn chọn *Stop* để có thể xuất gói .pcap và mở nó bằng Wireshark.

A screenshot of a computer

AI-generated content may be incorrect.

## Mô phỏng Brute force attack

### Brute force attack

Brute force (còn gọi là tấn công vét cạn hoặc thuật toán vét cạn) là phương pháp thử-sai có hệ thống để tìm ra giải pháp bằng cách kiểm tra tất cả các khả năng có thể có một cách có phương pháp. Trong an ninh mạng, đây là kỹ thuật tin tặc sử dụng phần mềm tự động để thử liên tục tất cả các tổ hợp tên đăng nhập và mật khẩu, hoặc khóa mã hóa, để truy cập trái phép vào hệ thống.

### Cài đặt foxyproxy và burp suite

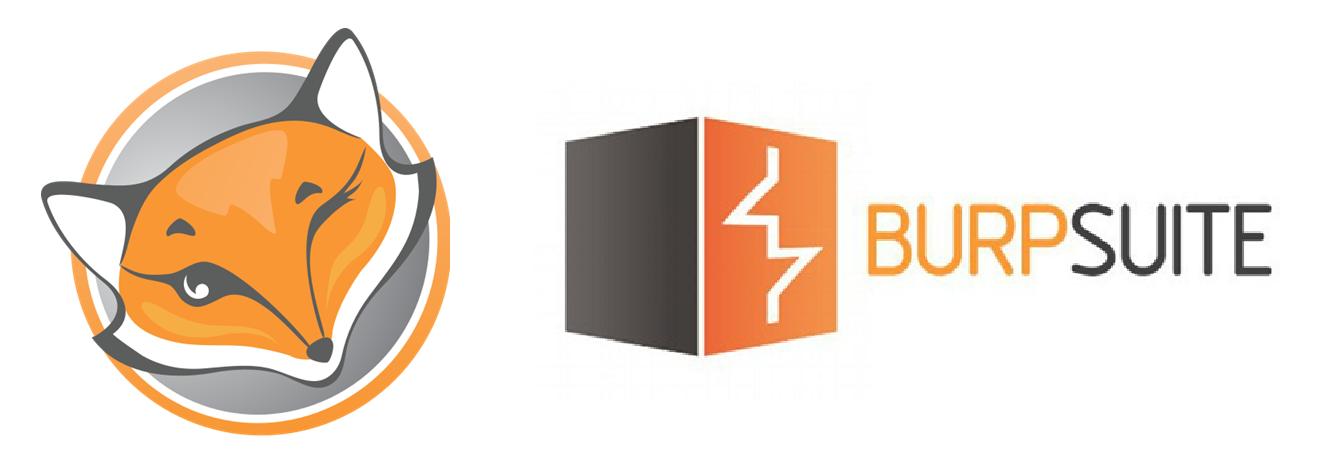
Trước khi mô phỏng, ta sẽ tải foxyproxy và burp suite để có thể bắt được gói tin gửi từ attacker 🡪 victim (dvwa).

FoxyProxy

* Là một extension/plug-in cho trình duyệt (Firefox/Chrome) để chuyển hướng traffic trình duyệt qua proxy theo profile/luật (theo domain, theo URL, theo thời gian...).
* Công dụng chính: bật/tắt nhanh proxy, dùng nhiều profile proxy khác nhau và áp dụng rules để chỉ gửi một số request qua proxy mà bạn muốn kiểm tra.

Burp Suite

* Bộ công cụ testing web phổ biến (intercepting proxy) gồm nhiều module: Proxy (chặn/hiện nội dung request-response), Repeater (thử thủ công), Intruder (tự động gửi nhiều biến thể request để kiểm thử), Decoder, Comparer, Scanner (ở bản chuyên nghiệp), và các tính năng quản lý session / extraction.
* Cho phép xem/hiệu chỉnh HTTP(s) request-response realtime, ghi lại lịch sử, tái phát (replay), tự động hoá các payload, và thao tác với token/cookie/session.



Cấu hình foxyproxy, để chuyển tiếp các gói tin đến cho localhost:port mà burp suite đang lắng nghe (127.0.0.1:8080)

A screenshot of a computer

AI-generated content may be incorrect.

Bật chế độ Intercept ON, burp suite sẽ bắt được gói tin trước khi chuyển tiếp, với việc này ta có thể mô phỏng brute force attack bằng cách thay đổi các tham số (vd username, password, cookie,…) trong gói tin request. Sau đó, ta có thể gửi gói tin đăng nhập ở */dvwa/vulnerabilities/brute* để xem burp suite bắt gói tin.

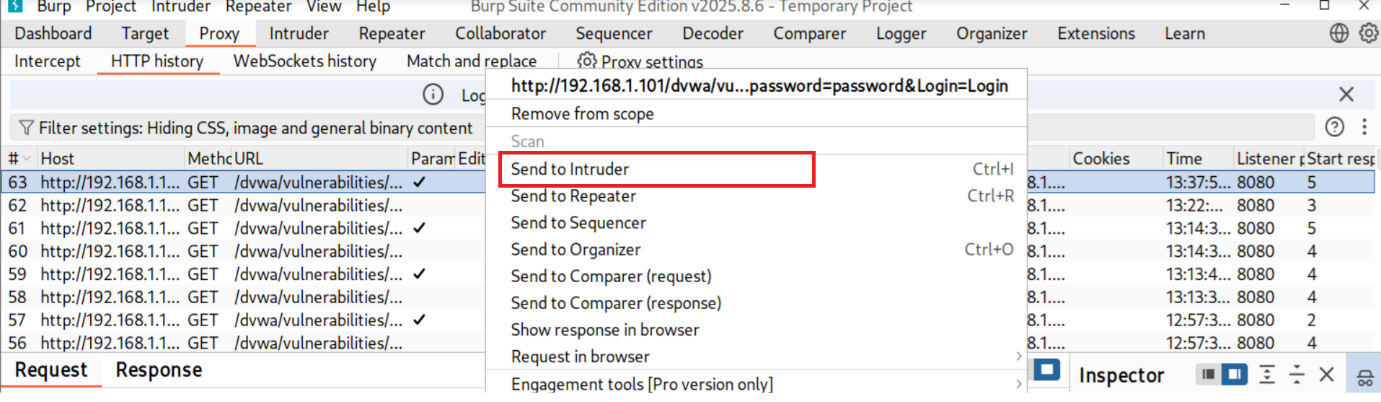
A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Ta sẽ gửi gói tin này sang cho Intruder - là module tự động hoá gửi nhiều biến thể (thay đổi các tham số) của một HTTP request để kiểm thử (brute-force, fuzzing, thử tham số).



Để có thể thay đổi được tham số cho từng request, ta phải đánh dấu tham số muốn thay đổi. Ở đây ta sẽ thử đánh dấu *giá trị của tham số* *password*, và sử dụng kiểu tấn công *Sniper attack -* thay 1 vị trí một lần, duyệt từng payload, dùng để test từng giá trị riêng lẻ.

A screenshot of a computer

AI-generated content may be incorrect.

Sang tab Payloads, ở phần Payload configuration, ta sẽ thêm vào một số các mật khẩu phổ biến để thử.

A screenshot of a computer

AI-generated content may be incorrect.

Ngoài ra để nhận biết được trong số các mật khẩu cái nào là chính xác, ta sẽ đánh dấu các gói tin response, bằng một chuỗi ký tự được lấy từ nội dung của gói tin thông báo mật khẩu sai.

A screenshot of a computer

AI-generated content may be incorrect.

Ta sẽ lấy chuỗi “incorrect” để phân biệt giữa mật khẩu đúng và mật khẩu sai. Nhập chuỗi này vào Grep – Match để Intruder có thể đánh dấu giúp ta.

A screenshot of a match

AI-generated content may be incorrect.

Hoàn tất công việc chuẩn bị, bây giờ sẽ mô phỏng tấn công

A screenshot of a computer

AI-generated content may be incorrect.

Ta có thể dễ dàng thấy mật khẩu *password* là chính xác và không được đánh dấu.

### Viết snort rule chống lại brute force

alert tcp any any -> 192.168.1.101 80 (msg:"DVWA BRUTE (/dvwa/vulnerabilities/brute)"; flow:to\_server,established; uricontent:"/dvwa/vulnerabilities/brute"; http\_uri; uricontent:"username="; http\_uri; uricontent:"password="; http\_uri; threshold:type threshold, track by\_src, count 5, seconds 5; sid:1000303; rev:1;)

**Mục đích:** Rule này cảnh báo khi có nhiều request đến endpoint /dvwa/vulnerabilities/brute trên web server 192.168.1.101:80 có chứa tham số username= và password= ,tức là cố gắng brute-force form đăng nhập của DVWA. Nếu cùng 1 nguồn gửi ≥ 5 request trong 5 giây thì rule sẽ alert.

**Giải thích một số tham số:**

* flow:to\_server,established;

Chỉ xét các gói đi tới server trên một kết nối đã được thiết lập (giảm false positives từ các gói không liên quan).

* uricontent:"/dvwa/vulnerabilities/brute"; http\_uri;

Tìm chuỗi đường dẫn trong phần URI của HTTP request (ví dụ GET /dvwa/vulnerabilities/brute?...).

* uricontent:"username="; http\_uri; và uricontent:"password="; http\_uri;

Yêu cầu URI có cả username= và password= (tức là request truyền thông tin đăng nhập trong query string).

* threshold:type threshold, track by\_src, count 5, seconds 5;

Cho ta biết giới hạn sinh ra 1 alert: theo dõi mỗi IP (by\_src), nếu gặp 5 lần trong 5 giây thì sinh alert (tức phát hiện hành vi lặp lại như brute-force).

**Kết quả:** phát hiện thành công brute force

**A screenshot of a computer

AI-generated content may be incorrect.**

## Mô phỏng tấn công Command Injection

### Tổng quan về command injection

Mục đích của tấn công chèn lệnh (command injection) là chèn và thực thi các lệnh do kẻ tấn công chỉ định trong ứng dụng có lỗ hổng.

Trong tình huống này, ứng dụng thực thi các lệnh hệ thống không mong muốn, hoạt động như một vỏ lệnh hệ thống giả (pseudo system shell), và kẻ tấn công có thể sử dụng nó như bất kỳ người dùng hệ thống được ủy quyền nào.

Tuy nhiên, các lệnh được thực thi với các đặc quyền và môi trường giống như dịch vụ web đang có.

Các cuộc tấn công chèn lệnh xảy ra trong hầu hết các trường hợp là do thiếu xác thực dữ liệu đầu vào chính xác, vốn có thể bị kẻ tấn công thao túng (các trường biểu mẫu, cookie, tiêu đề HTTP, v.v.).

Cú pháp và các lệnh có thể khác nhau giữa các Hệ điều hành (OS), chẳng hạn như Linux và Windows, tùy thuộc vào hành động mong muốn của kẻ tấn công.

Cuộc tấn công này cũng có thể được gọi là "Thực thi lệnh từ xa (Remote Command Execution - RCE)".

Từ xa, tìm ra người dùng của dịch vụ web trên hệ điều hành, cũng như tên máy chủ (hostname) thông qua RCE.

### Mô phỏng tấn công với các mức bảo mật

1. Bối cảnh

Dvwa yêu cầu nhập một địa chỉ IP, server dùng giá trị đó làm đối số cho một lệnh hệ điều hành, cụ thể ở đây là lệnh ping đến địa chỉ IP được người dùng nhập. Vấn đề ở đây là ứng dụng không kiểm soát/escapе giá trị người dùng trước khi đưa vào lệnh shell.

A screenshot of a login box

AI-generated content may be incorrect.

1. Ý tưởng khai thác:

Thoát khỏi ngữ cảnh tham số, bằng cách chèn ký tự/tổ hợp dùng để tách lệnh hoặc thực thi lệnh con (ví dụ các ký tự phân tách lệnh, subshell, backtick, v.v.), kẻ tấn công phá rời phần tham số ban đầu.

Ký tự & chuỗi tách/chạy nhiều lệnh

* ; — separator: cmd1; cmd2 ⇒ chạy cmd1 rồi cmd2.  
  Ví dụ: 381; echo pwned
* && — chỉ chạy tiếp khi lệnh trước thành công: cmd1 && cmd2.
* || — chỉ chạy tiếp khi lệnh trước thất bại.
* & — có thể là chạy background hoặc separator tuỳ shell: cmd1 & cmd2.
* | — pipe: output lệnh trái được truyền sang cho input lệnh phải (ls | grep x).

1. Dấu hiệu nhận biết khi tấn công thành công:

Response có xuất hiện chuỗi/chuỗi ngẫu nhiên mà bạn không mong đợi (do lệnh chèn in ra).

Lỗi bất thường từ chương trình (do tham số bị thay đổi).

1. Tấn công với các mức an toàn (low, medium, high)

* Security level: Low

A screenshot of a computer

AI-generated content may be incorrect.

Như đã nói ở trên, ta có thể khai thác lỗ hổng này bằng cách nối thêm các ký tự cho phép chạy nhiều lệnh. Thay vì nhập địa chỉ IP không, ta sẽ nối thêm “&& ls” ở cuối.A screenshot of a computer

AI-generated content may be incorrect.

Kết quả: sau khi được server sử dụng input này mà không kiểm tra (validation), lệnh được thực hiện trong shell thực chất

*Ping 192.168.1.101 && ls*

Ping 192.168.1.101 sẽ chạy trước; nếu nó trả về thành công thì shell sẽ chạy tiếp lệnh ls. Kết quả ls là danh sách file trong thư mục hiện thời của quá trình thực thi — chính là thư mục mà tiến trình web (dvwa) đang chạy.

Ta sẽ xem source code để hiểu cách xử lý dữ liệu sau khi gửi input cho server.

A screenshot of a computer code

AI-generated content may be incorrect.

Ta có thể dễ thấy, với mức độ bảo mật *low*, server hoàn toàn không *validate* dữ liệu.

* Security level: Medium

A screenshot of a computer

AI-generated content may be incorrect.

Với mức độ medium, ta nhìn source code trước.

A screenshot of a computer program

AI-generated content may be incorrect.

Server đã có thêm một chút kiểm tra đầu vào, bằng xóa các ký tự “*&&”, “ ;”* trong input để tránh việc chèn vào cuối. Nhưng như thế là không đủ, ta có thể sử dụng ký tự *“&”* – có tác dụng phân tách thành hai lệnh chạy độc lập với nhau.

A screenshot of a computer

AI-generated content may be incorrect.

www-data là tên user đặc biệt mà các service web như Apache sử dụng để chạy các ứng dụng (dvwa) và xử lý các yêu cầu của khách truy cập.

Chạy Dịch vụ: Khi ta cài đặt máy chủ web và các ứng dụng PHP/HTML, tất cả các tiến trình đó không chạy dưới quyền của ta (tài khoản đăng nhập) mà chúng được chuyển sang chạy dưới danh nghĩa của www-data.

Cho phép web server chạy với quyền hạn rất hạn chế (không phải root), nên nếu web server bị khai thác, kẻ tấn công chỉ có quyền của www-data thay vì toàn quyền hệ thống — giảm thiểu nguy hại.

* Security level: High

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

Với mức bảo mật *high*, rõ ràng dvwa đã xử lý với nhiều ký tự hơn, nhưng vẫn chưa đủ. Nếu để ý, ta có thể thấy “| ” có một dấu cách (space), vậy thì đơn giản ta chỉ cần nối địa chỉ IP với “|” mà không có dấu cách

A screenshot of a computer screen

AI-generated content may be incorrect.

Ký tự “|” có tác dụng lấy output của lệnh trước truyền vào input cho lệnh hiện tại. Và vì hostname không lấy input mà nó chỉ tìm kiếm thông tin trong hệ thống và trả về hostname tương ứng.

### Viết snort rule phát hiện tấn công command injection