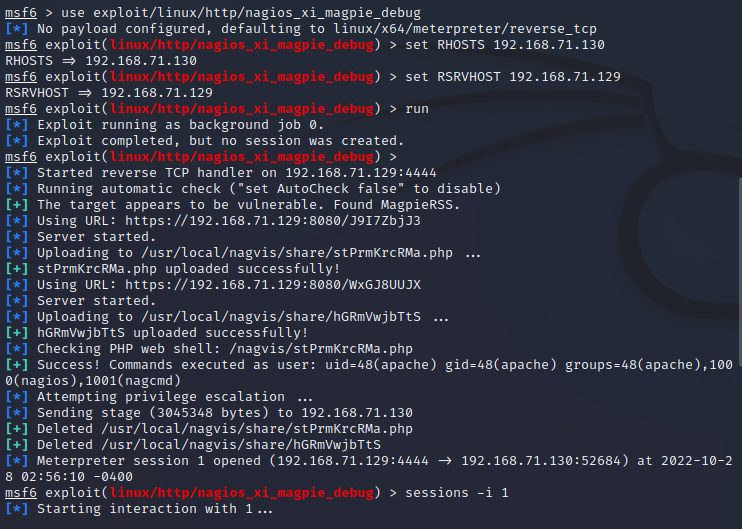
**Tiểu luận môn học: Phân tích và xác định mẫu dữ liệu tấn công CVE-2018-15708**

**Họ và tên: Lê Khánh Duy**

**MSSV: N18DCAT014**

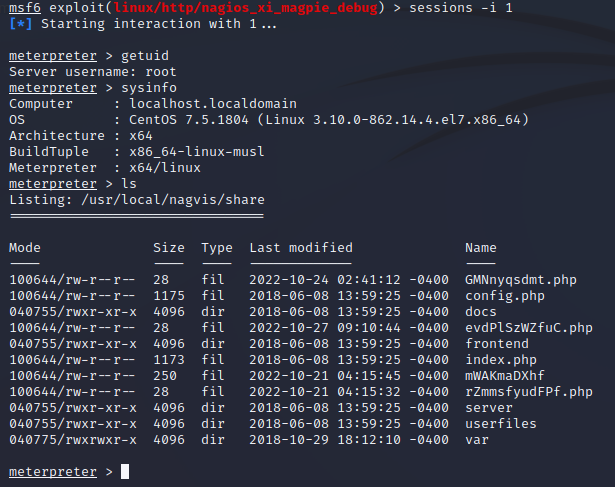
Tiến hành tấn công với payload có sẵn của **metasploit** với:

* RHOSTS: là địa chỉ ip của máy Victim
* RSRVHOST: là địa chỉ server để upload file php đến server Victim

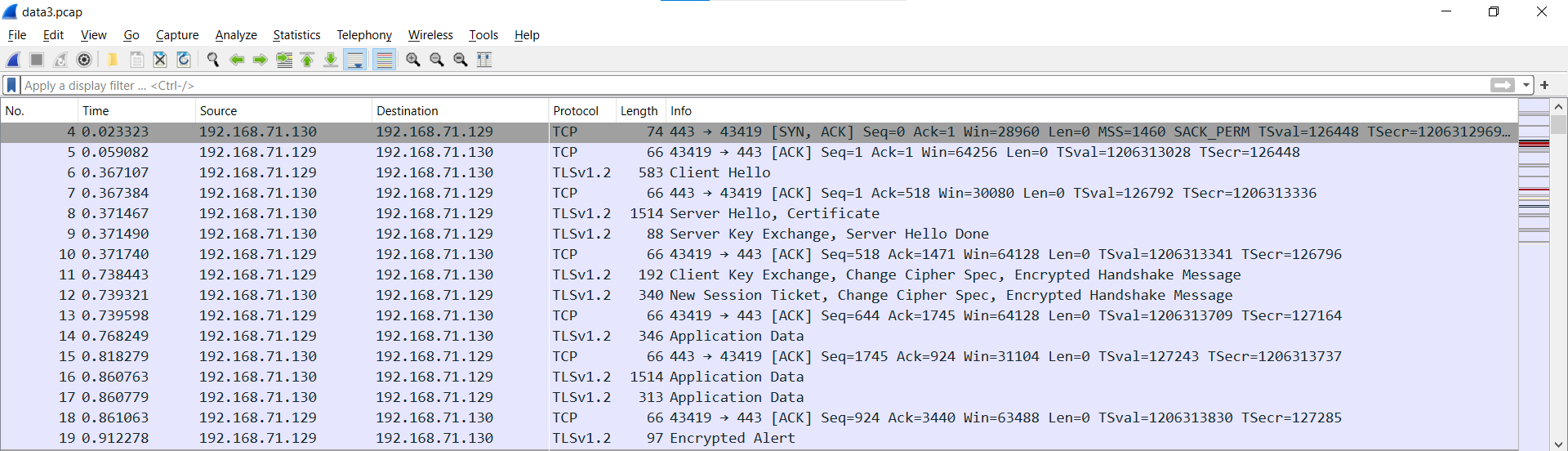


Sửng dụng 1 URL từ máy Actacker để upload file .php lên server Victim, có 2 file được tải lên với URL khác nhau. Sau khi hoàn thành sẽ tạo 1 session để kết nối vào máy Victim

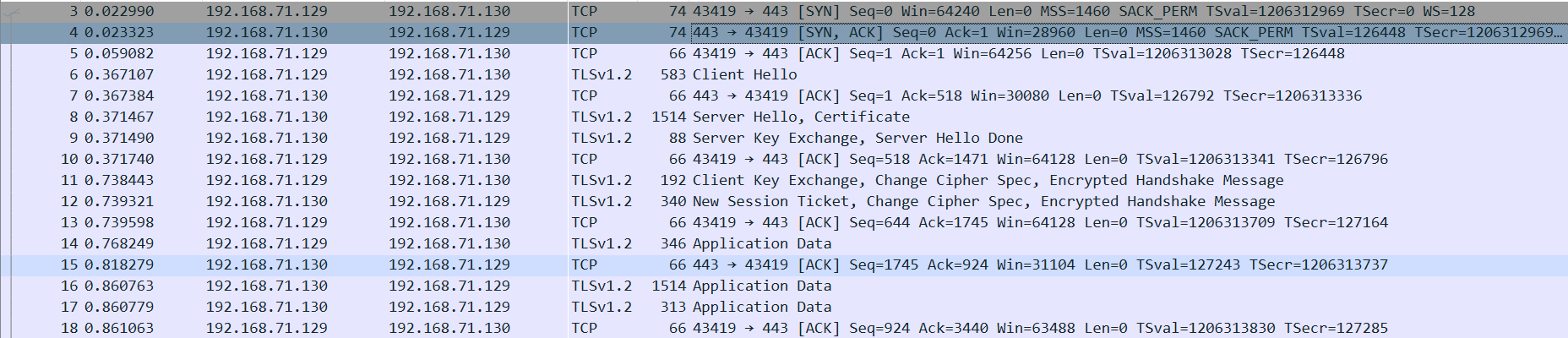
**Thực hiện thử các lệnh**



Sử dụng Wireshark để bắt các gói trong quá trình tấn công

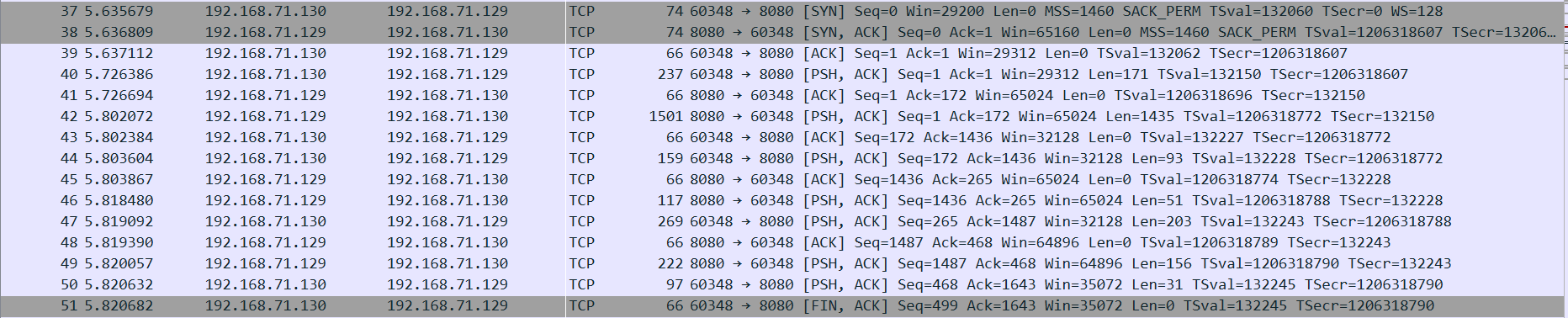


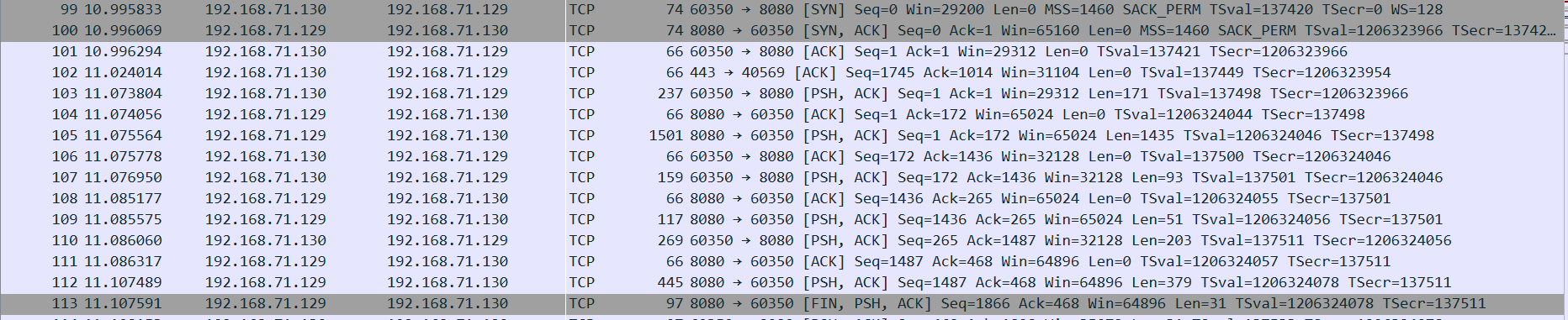
**Phân tích các gói**



Đầu tiên máy Atacker sẽ truy cập đến domain của server Victim qua port 443 (https) và Actacker sẽ tạo port ngẫu nhiên để tránh phát hiện

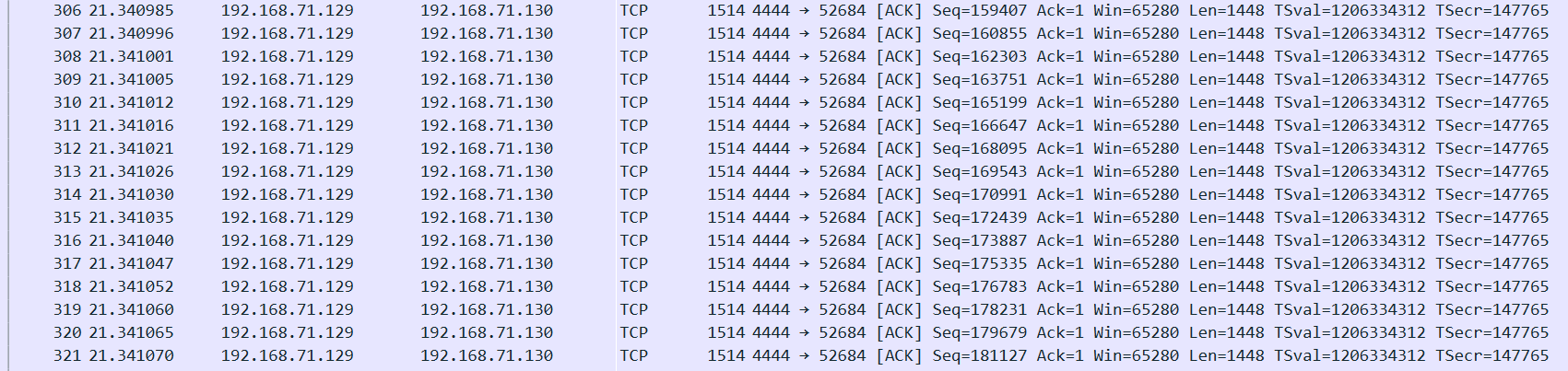
Các gói upload file .php





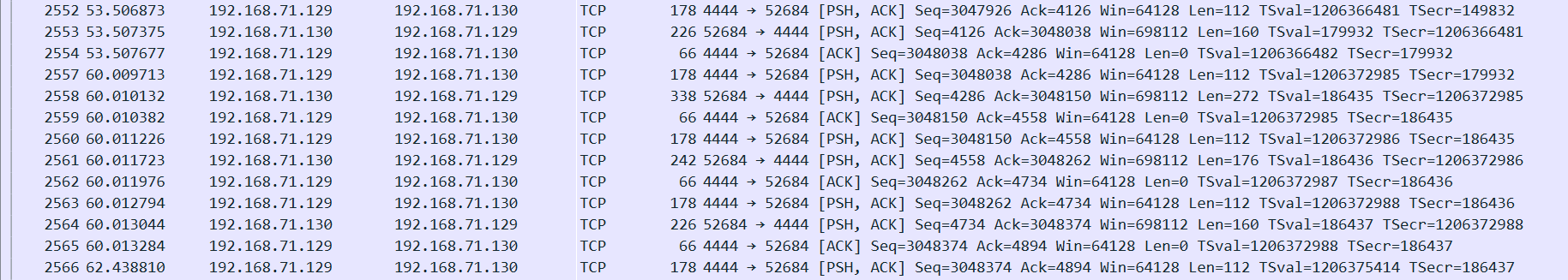
Các gói sinh ra trong quá trình tải lên file .php từ máy Actacker đến máy Victim, do có 2 file .php đc gởi nên sinh ra 2 phần. Máy Actacker sẽ tải từ port 8080 đến port ngẫu nhiên của máy Victim, port Actacker có thể thay đổi

Cái gói sinh ra trong quá trình kết nối 2 máy



Máy Atacker sẽ kết nối từ port 4444 đến port ngẫu nhiên trên máy Victim, có từ 1000-2000 gói được gửi.

Các gói sinh ra từ các lệnh test cmd



**Xác định signature**

* Trong mỗi lần gửi file .php đều sinh ra gói

[SYN] và win=64240 từ máy Actacker -> Victim

Victim -> Atacker sẽ trả ra gói [SYN, ACK] và win=28960

Gửi file .php từ Actacker->Victim qua port 8080 nhưng port này có thể thay đổi nên không chọn làm key, chọn [SYN] và win=29200

Victim -> Atacker sẽ trả ra gói [SYN, ACK] và win=65160

* Trong quá trình tạo session sẽ gửi 1000-2000 từ máy Actacker->Victim

[ACK] và win=65280