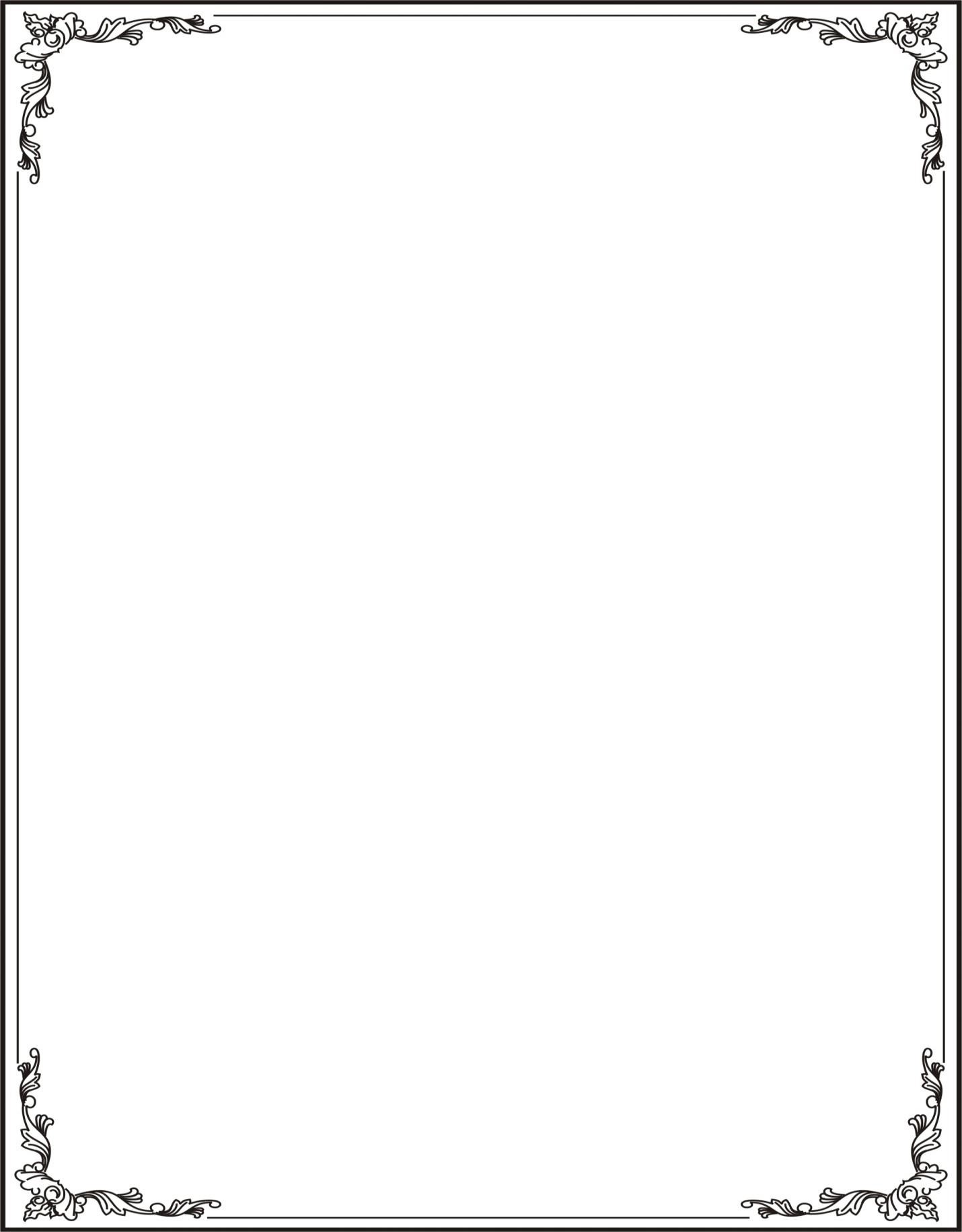
**Xây dựng chương trình phát hiện tấn công mã lỗ hổng CVE-2019-0708**

**Đề tài:**

**Chuyên Đề An Ninh Mạng**

**BÁO CÁO CUỐI KỲ**



**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN 2**

**-------oO🖎🕮✍Oo-------**

**Giảng viên : Nguyễn Hồng Sơn**

**Sinh viên thực hiện: Trần Quốc Trượng**

**MSSV: N18DCAT100**

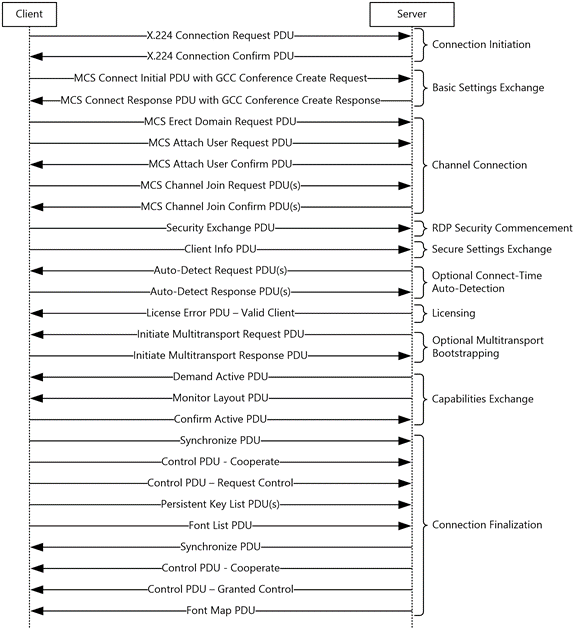
**TP.HCM, tháng 11/2022**



# 1. Cơ sở lý thuyết

## 1.1. RDP

* RDP: Dịch vụ Máy tính Từ xa của Microsoft (trước đây gọi là Dịch vụ Đầu cuối) cho phép người dùng mở các phiên Windows tương tác từ xa. Dịch vụ Máy tính Từ xa cung cấp các chức năng tương tự như các chức năng của môi trường dựa trên thiết bị đầu cuối, nơi nhiều thiết bị đầu cuối (máy khách) có thể được kết nối với một máy chủ (máy chủ) duy nhất. Người dùng từ xa có thể đăng nhập vào máy chủ từ xa và truy cập dữ liệu, chạy ứng dụng, v.v. trên máy tính chủ. Kết nối máy tính để bàn từ xa mặc định giao tiếp với máy chủ từ xa bằng Giao thức Máy tính Từ xa (RDP) qua cổng 3389/TCP.
* Các giai đoạn của kết nối RDP

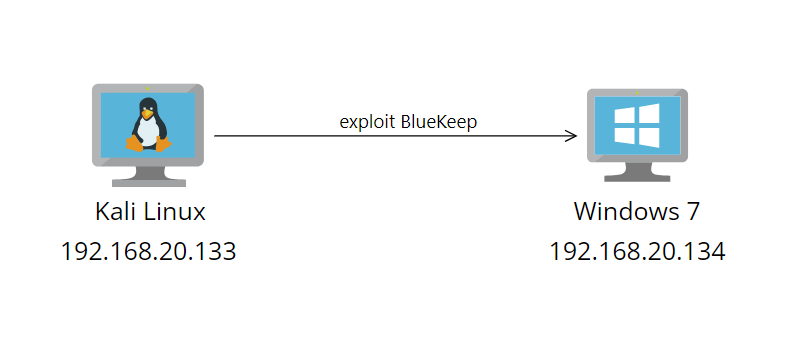


## 1.1.2. BlueKeep

* BlueKeep (CVE-2019-0708) là một lỗ hổng RCE trong máy chủ RDP của Microsoft, ảnh hưởng đến các máy Windows từ Windows 2000 đến Windows 7 và Windows Server 2008 R2. Nó đã được tìm thấy và vá vào tháng 2019 năm XNUMX. Lỗ hổng này là một use-after-free đã có trong trình điều khiển nhân Windows xử lý các kết nối RDP - termdd.sys.
* Lỗ hổng này có thể bị khai thác trong giai đoạn khởi tạo kết nối của RDP. Trong quá trình trao đổi cài đặt cơ bản, máy khách và máy chủ thương lượng kênh ảo tĩnh nào để khởi tạo cho kết nối và có các kênh sẽ được phân bổ cho kết nối bất kể yêu cầu của máy khách, bao gồm cả kênh MS\_T120.
* termdd.sys tạo một bảng chứa con trỏ đến cấu trúc kênh cho mọi kênh đã tạo. Bảng này chứa tối đa 32 (0x20) Kênh. Kênh ảo tĩnh MS\_T120 được tạo theo mặc định và nó luôn ở 0x1F chỉ mục. Điều này xảy ra ngay cả trước khi chuỗi kết nối bắt đầu.
* Để kích hoạt lỗ hổng này, cần tạo một máy khách RDP tùy chỉnh, sẽ yêu cầu một kênh ảo tĩnh có tên MS\_T120 trong Trao đổi cài đặt cơ bản. Nếu kênh đó được yêu cầu, máy chủ RDP sau đó sẽ cố gắng tìm hiểu xem kênh này đã được tạo cho kết nối này chưa. Nếu vậy, nó sẽ trả con trỏ về cấu trúc điều khiển kênh hiện có thay vì tạo một cấu trúc mới. Tại thời điểm này, sẽ có hai con trỏ trỏ đến một cấu trúc dữ liệu.
* Để kích hoạt lỗi, máy khách RDP phải gửi một gói sẽ khiến máy chủ đóng kênh MS\_T120 (hành vi hợp pháp và được ghi lại). Sau khi đóng kênh, máy chủ sẽ tiếp tục và giải phóng cấu trúc điều khiển kênh của MS\_T120 và con trỏ đến nó trong mảng kênh kết nối, nhưng chỉ có một kênh được tạo do yêu cầu của máy khách (không phải do máy chủ tạo tự động). Bây giờ có một con trỏ lủng lẳng và lần sau khi máy chủ sẽ cố gắng truy cập kênh MS\_T120 (điều này xảy ra thường xuyên vì đây là kênh quan trọng đối với hoạt động của RDP), hệ thống sẽ kiểm tra lỗi.

# 2. Thực hiện

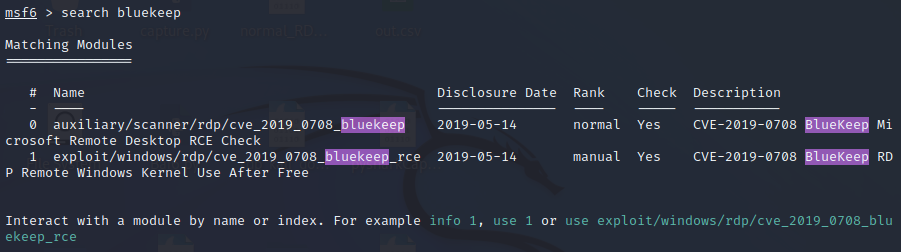
## 2.1. Mô hình



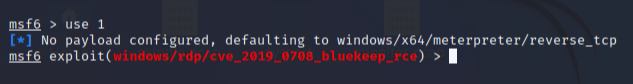
|  |  |  |  |
| --- | --- | --- | --- |
| Tên thiết bị | Thông tin |  | Interface |
| Kali Linux | Máy ảo VMWare, sử dụng metasploit thực thiện khai thác | Ip address | 192.168.20.133 |
| Netmask | /24 |
| Default Gateway | 192.168.20.2 |
| DNS |  |
| Windows 7 | Máy ảo VMWare, windows 7 sp1, chứa lỗ hổng BlueKeep, RDP port 3389 | Ip address | 192.168.20.134 |
| Netmask | /24 |
| Default Gateway | 192.168.20.2 |
| DNS |  |

## 2.2. Tấn công

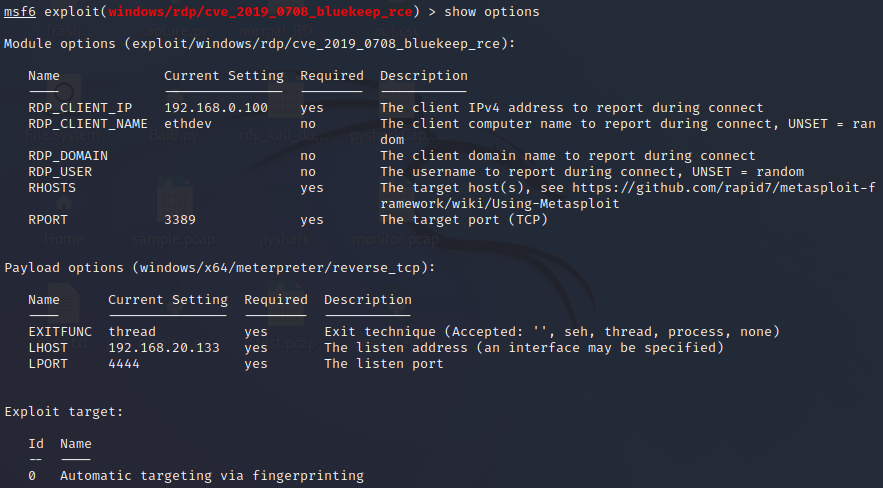
* Bước 1: Trên máy Kali mở metasploit và tìm kiếm module bluekeep



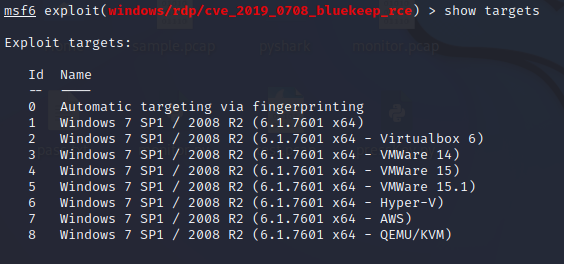
* Bước 2: Chọn module 1



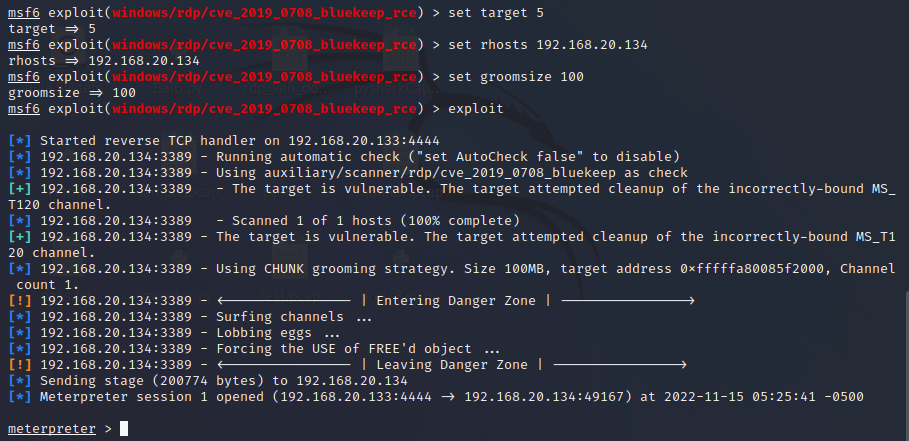
* Bước 3: show options



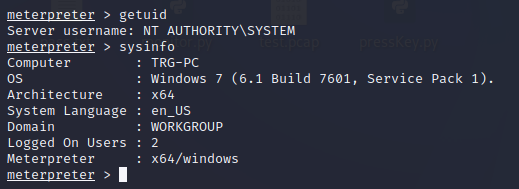
* Bước 4: show targets



* Bước 5: Chọn mục tiêu, đặt các tham số cần thiết và thực hiện khai thác



* Bước 6: Khai thác thành công



## 2.3. Phân tích và phát hiện

### 2.3.1. Kết nối RDP có mã hoá mức độ thấp

Khi mã hóa cấp thấp được định cấu hình, các giai đoạn đầu tiên của giao tiếp RDP xảy ra trong văn bản rõ ràng cho đến giai đoạn Security Exchange PDU. Giám sát và phân tích các giai đoạn trước đó là đủ để phát hiện khai thác.

Mô-đun khai thác gửi yêu cầu đàm phán với chuỗi 7 ký tự cookie ngẫu nhiên(gói RDP Cookie). Sau đó máy RDP mục tiêu chấp nhận đàm phán (gói RDP Negotiate Respone)

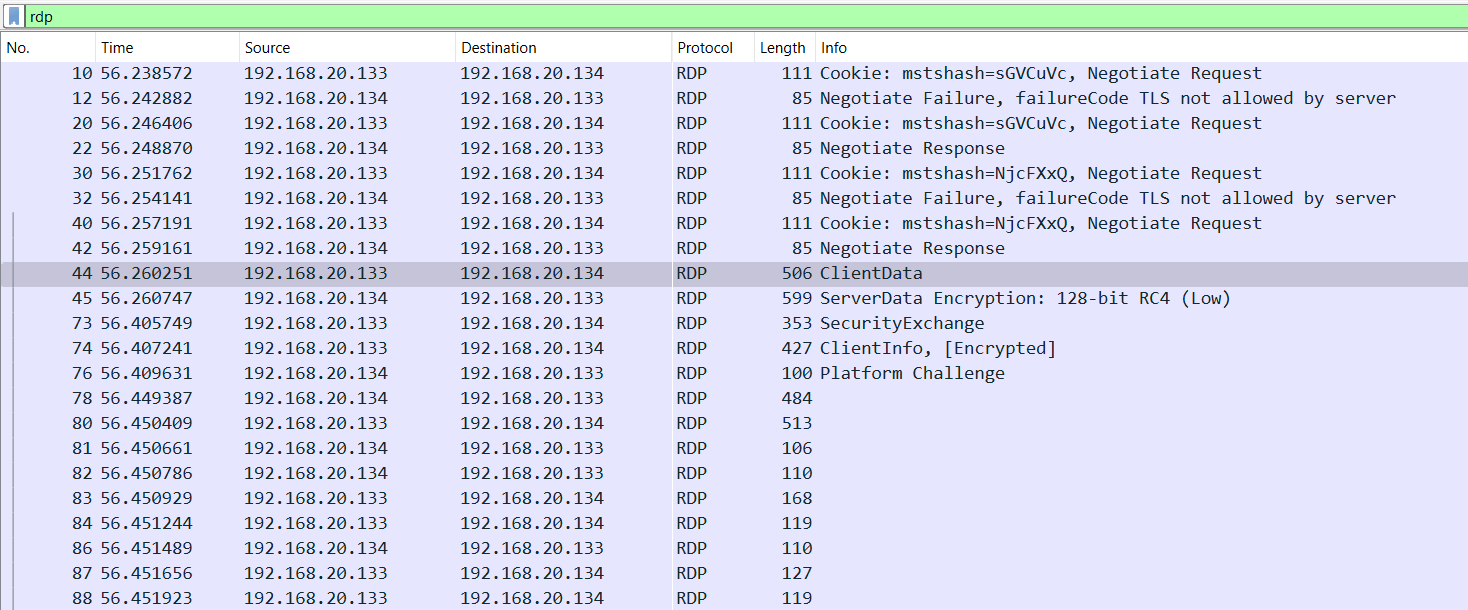


Figure 1. Lưu lượng mạng của khai thác bắt được từ wireshark

Máy tấn công tiếp tục gửi yêu cầu (gói RDP ClientData) gồm nhiều kênh ảo đến mục tiêu, gồm có MS\_T120 và những kênh khác bắt đầu bằng MS\_XXX.

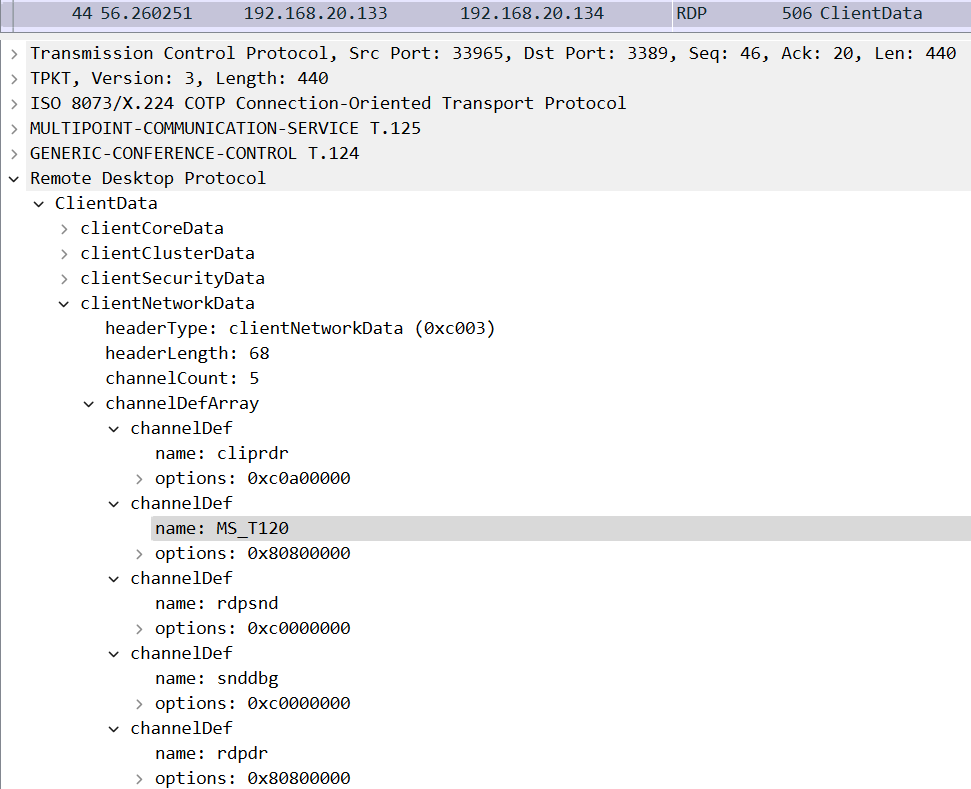


Figure 2. Kênh MS\_T120 có trong yêu cầu gửi đến mục tiêu

Tên kênh “MS\_T120” là kênh trong kết nối RDP được Microsoft sử dụng nội bộ và không có trường hợp hợp lệ nào được sử dụng ở Client khi kết nối RDP

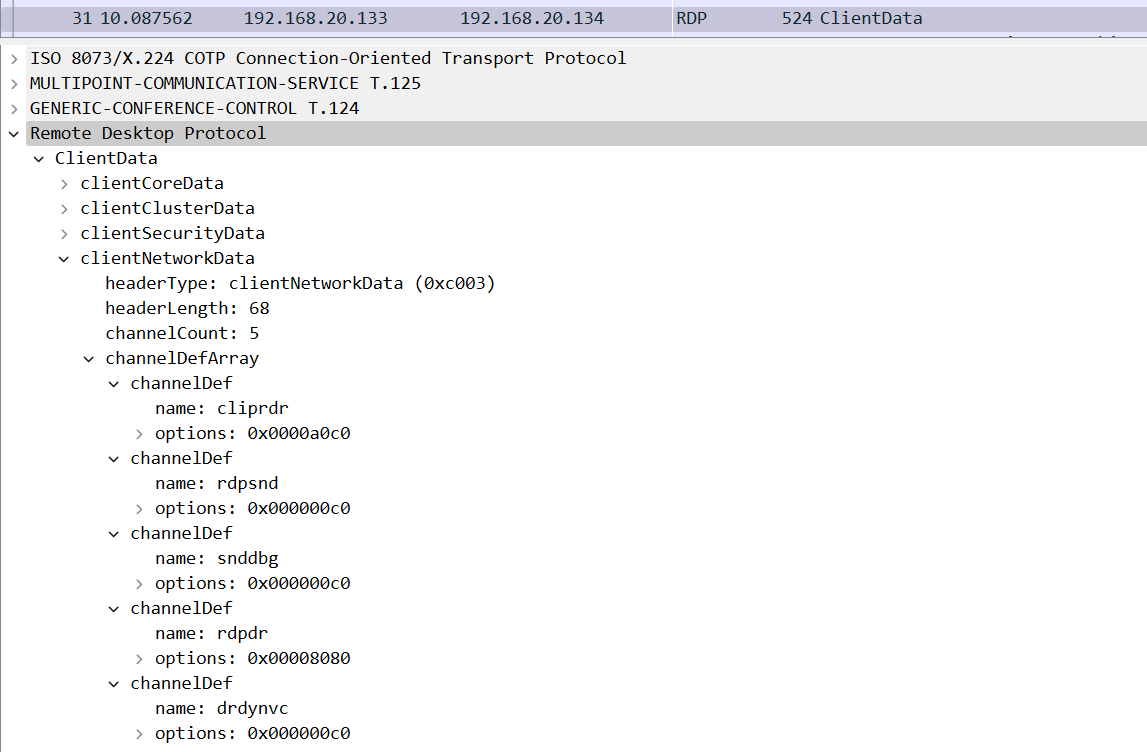


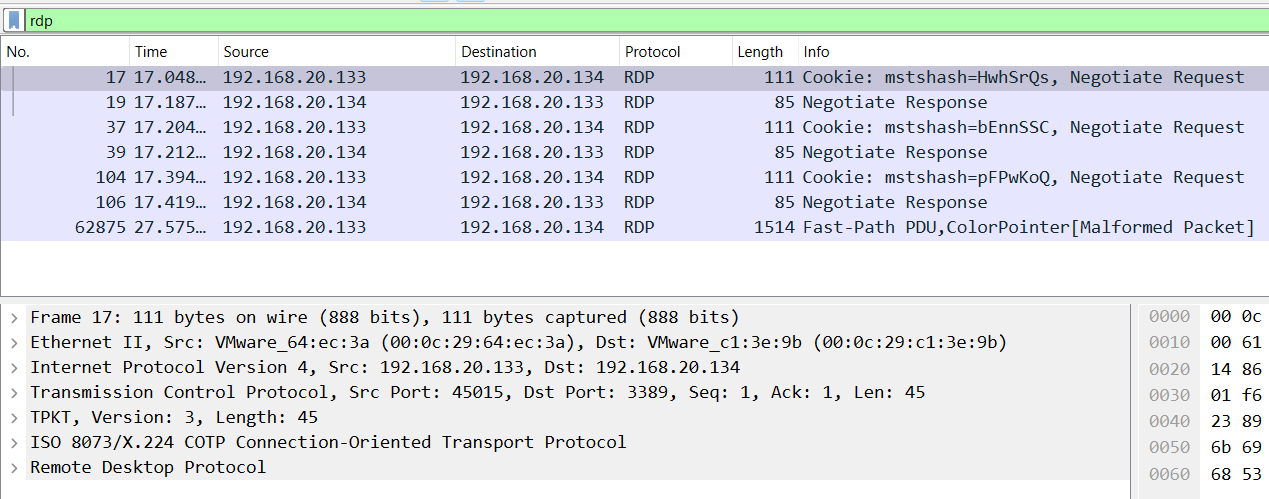
Figure 3. Yêu cầu cầu kênh của kết nối RDP bình thường

Như vậy có thể xác định dấu hiệu để phát hiện nỗ lực khai thác là bất kỳ kết nối RDP nào cố gắng kết nối với MS\_T120 được coi là 1 kết nối đáng ngờ.

### 2.3.2. Kết nối RDP có mã hoá mức độ cao

Khi mã hóa cấp cao được định cấu hình, tất cả các giao tiếp sau khi kết nối xác nhận PDU được mã hóa bằng TLS. Chỉ có các gói ở giai đoạn “Connection Initiation” được nhìn thấy.

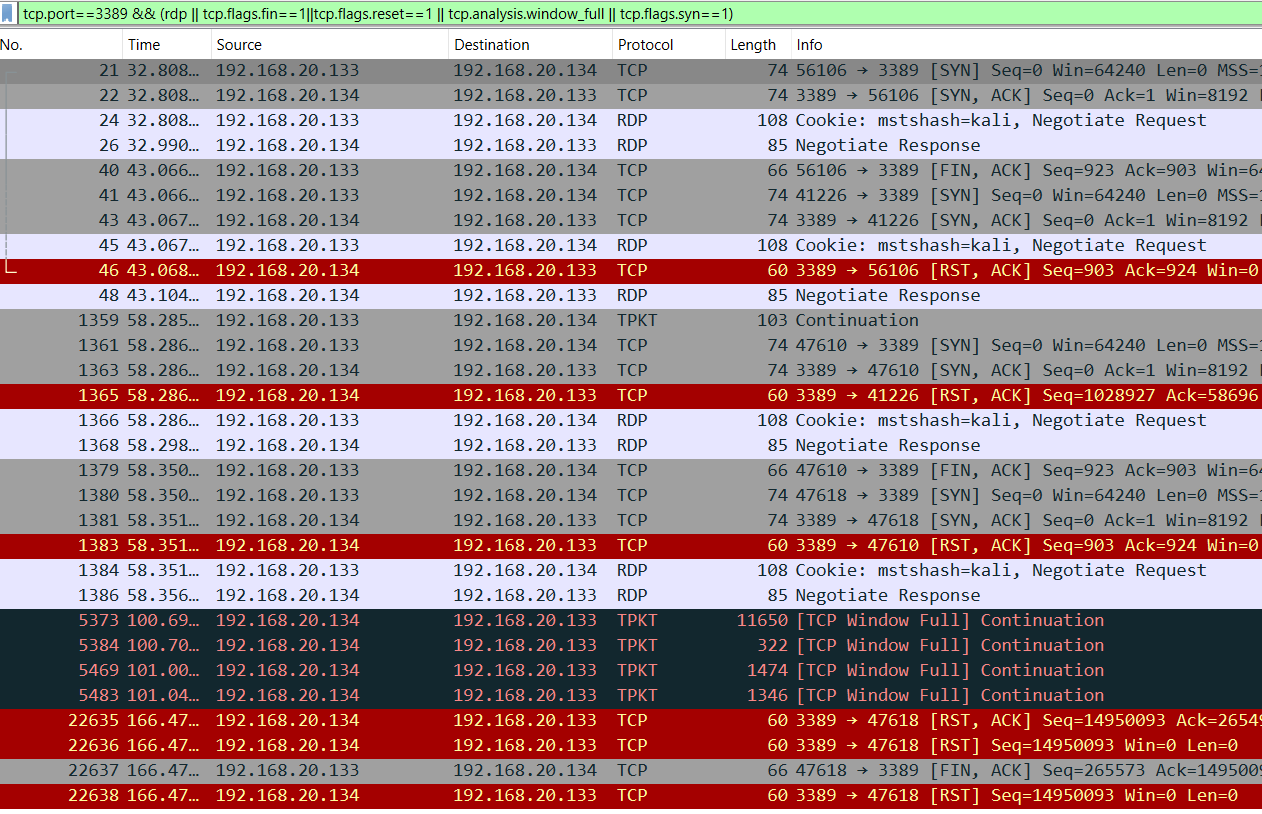
Máy tấn công gửi yêu cầu đàm phán với cookie ngẫu nhiên:



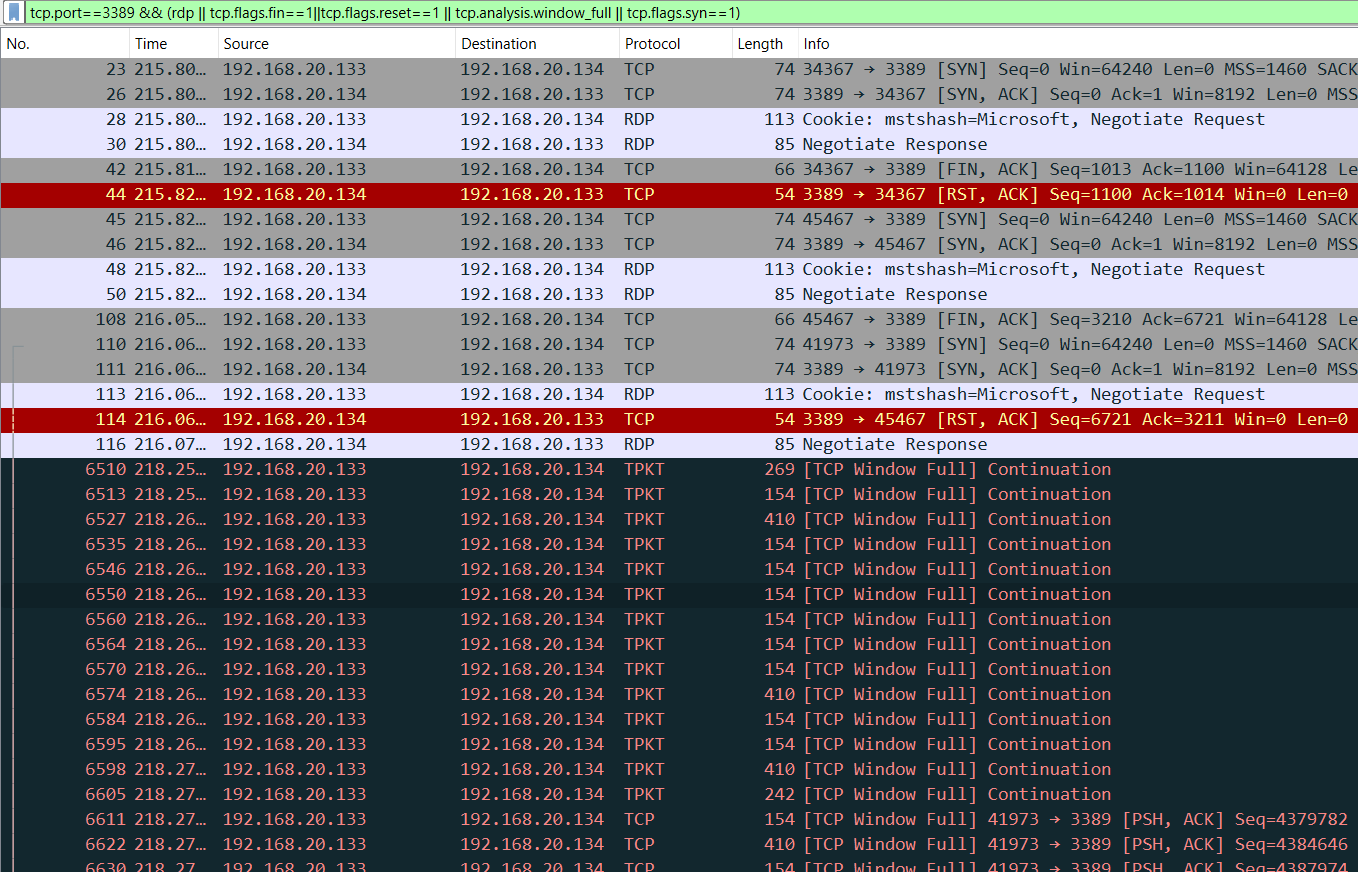
Nếu module metasploit không chỉ định user name nó sẽ sử dụng giá trị cookie ngẫu nhiên. Có thể dựa vào đó để phát hiện dấu hiệu khai thác.

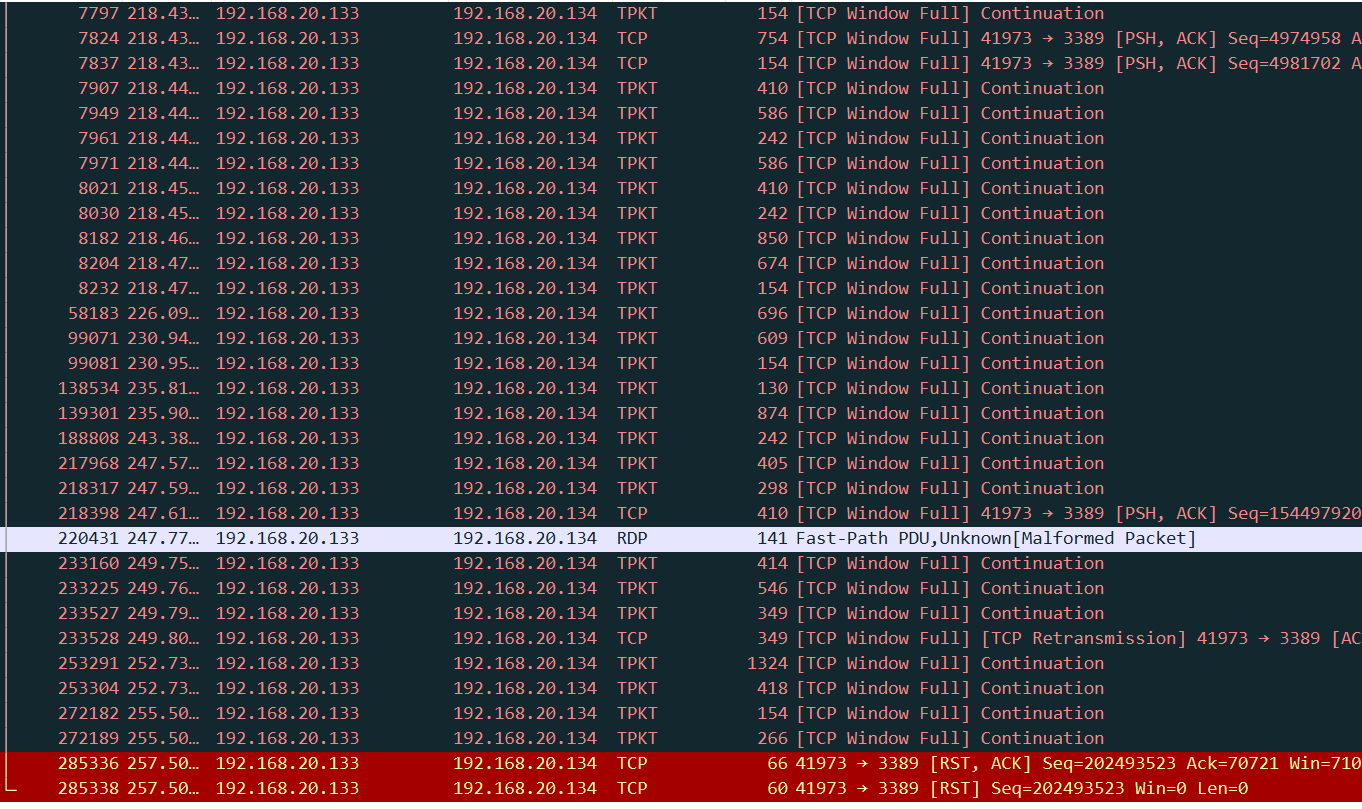
Kết nối được mã hoá nên không có nhiều dữ liệu để xác định khai thác. Vì thế sẽ chuyển qua phân tích hành vi của khai thác sau khi kết nối tới máy mục tiêu.

Tiến hành thu thập lưu lượng mạng của một kết nối RDP bình thường:

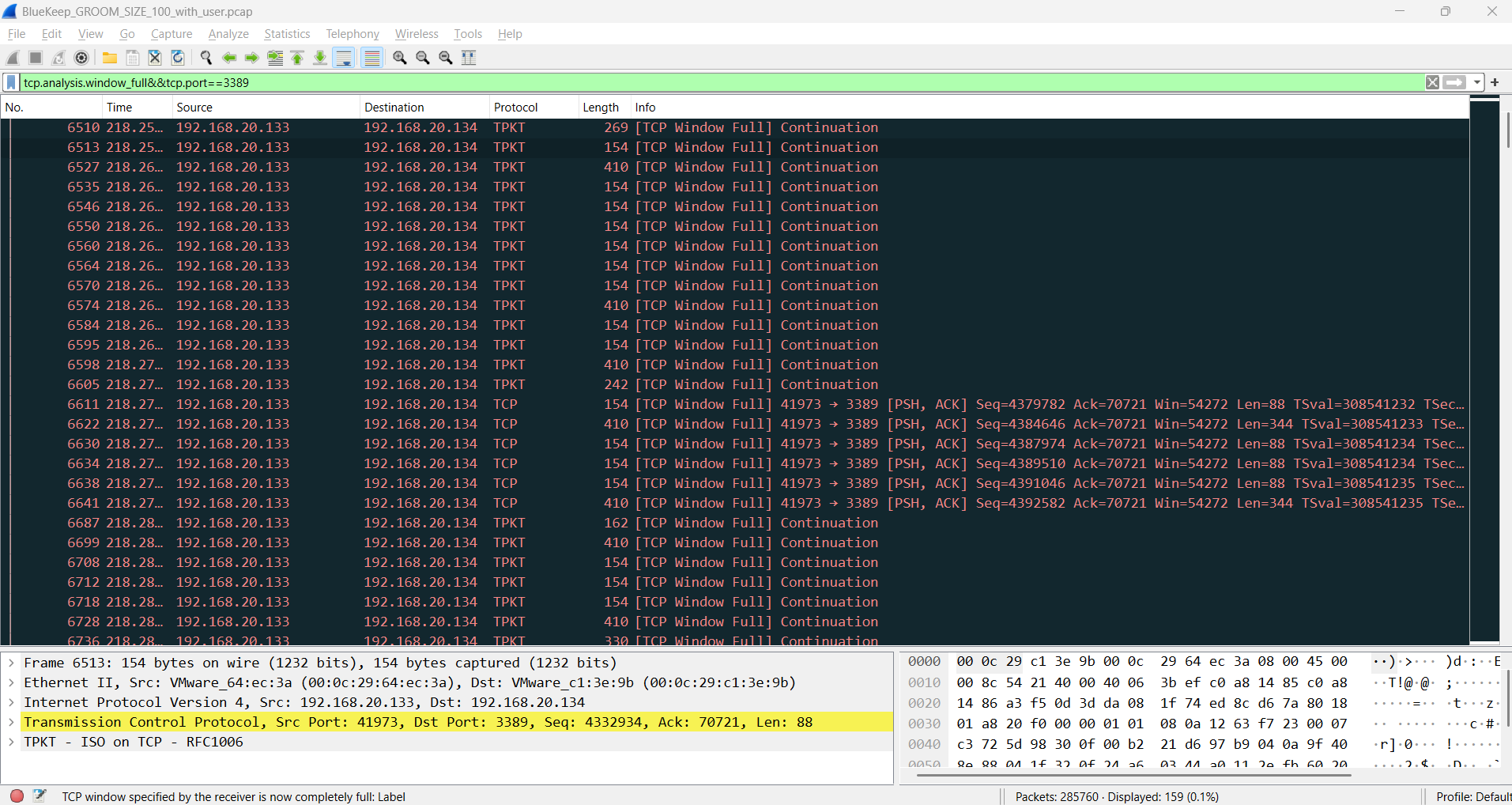


Tiến hành thu thập lưu lượng mạng từ module khai thác:

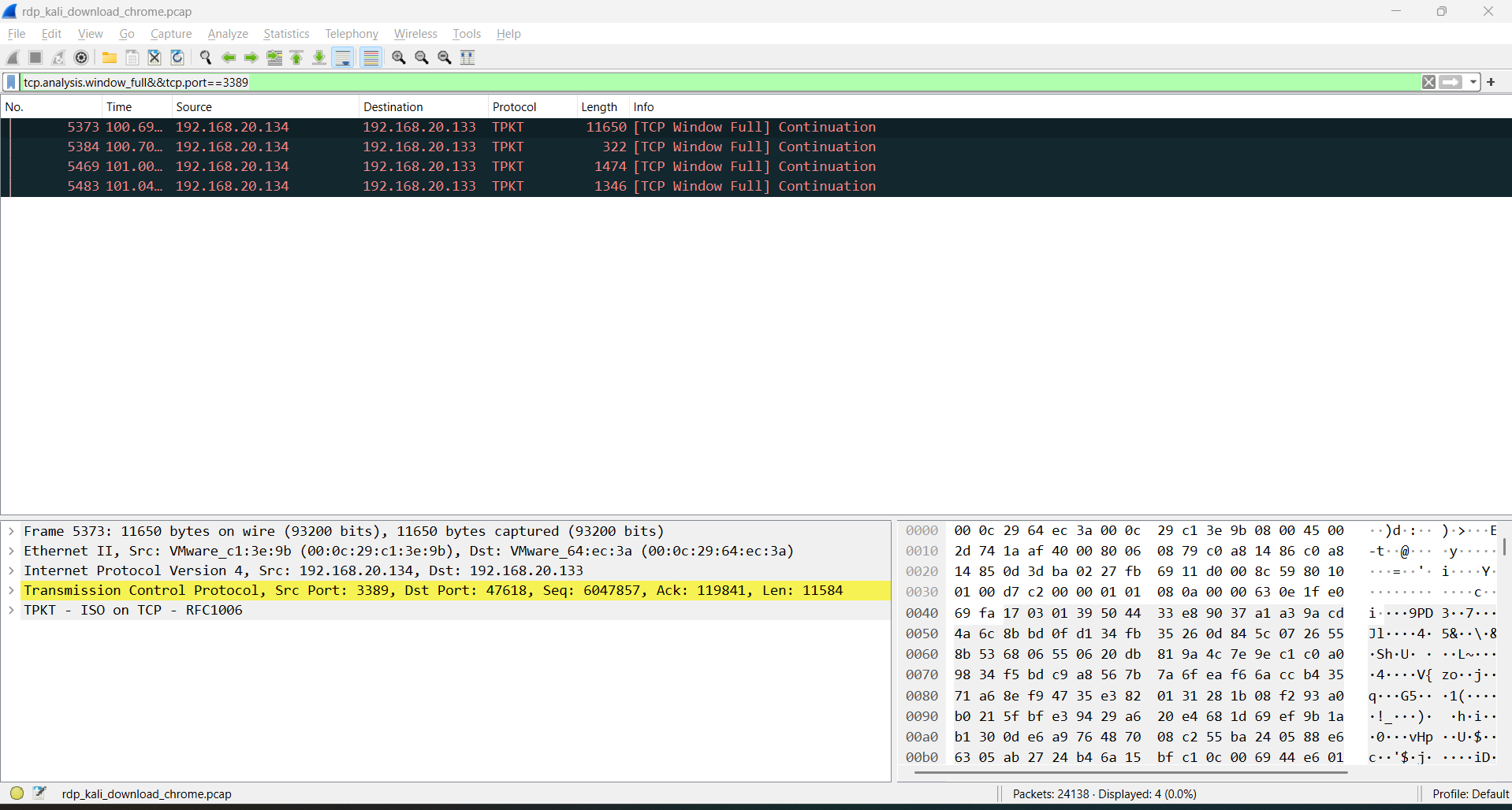




Nhận thấy rằng module metasploit sau khi kết nối RDP tới máy mục tiêu đã gửi rất nhiều đoạn dữ liệu đến máy mục tiêu, làm cho bộ đệm máy mục tiêu bị tràn:



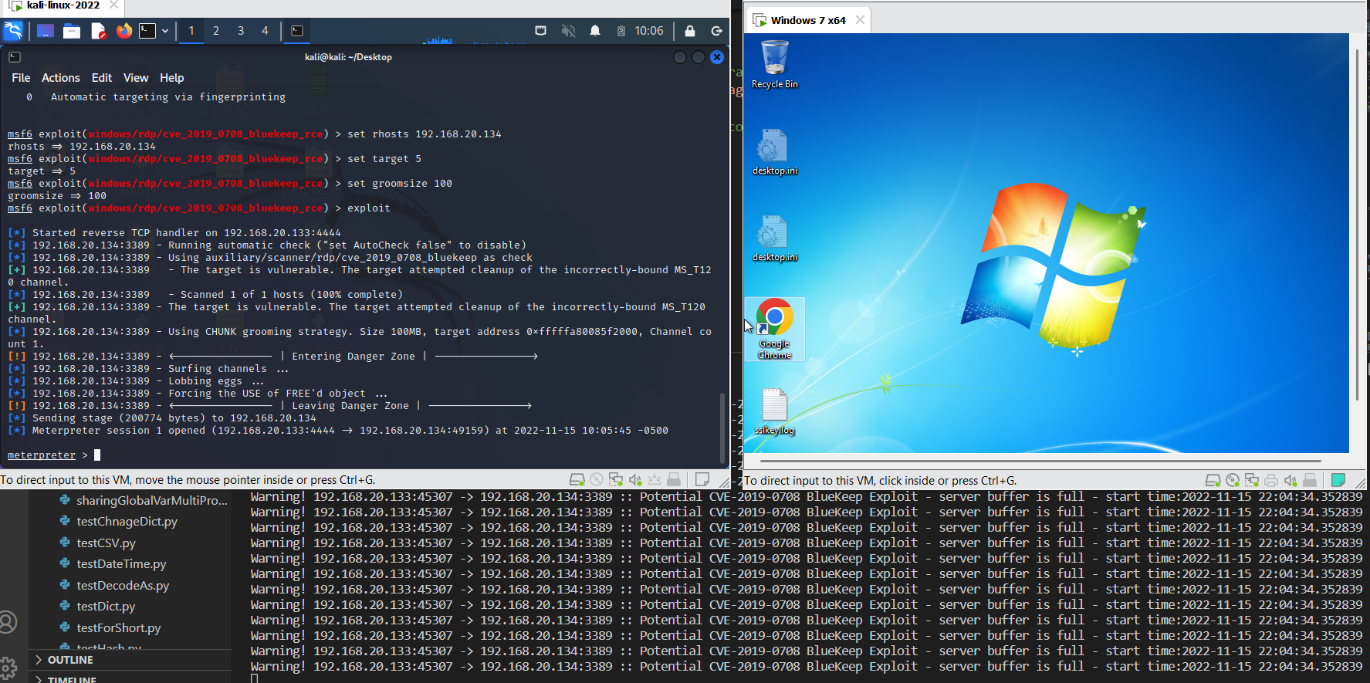
Trong khi kết nối RDP bình thường không có hành vi này.



Kết luận: Khi kết nối được mã hoá mức độ cao có thể xác định dấu hiệu của khai thác dựa vào hành vi gửi các cookie ngẫu nhiên và làm đầy bộ nhớ của máy mục tiêu (các gói TCP windows full có source từ máy tấn công và destination là máy mục tiêu)

## 2.4. Chương trình python phát hiện khai thác

Chương trình sử dụng pyshark để bắt gói, tìm và so khớp các gói tin với các dấu hiệu của khai thác đã xác định ở trên. Sau khi thu thập đủ dữ liệu so khớp với khai thác, chương trình sẽ phát ra cảnh báo.



Chương trình hỗ trợ ghi log

