Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Tại máy attacker mở wireshark và chọn any

Ảnh có chứa bàn

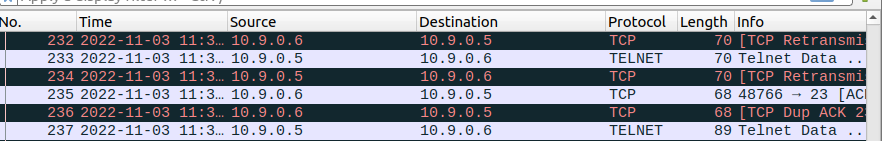
Mô tả được tạo tự động

+ Bến máy User1 ta kết nối telnet tới máy Victim

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Ta kết nối telnet thành công với máy victim



+ Bên wireshrak ta bắt được các gói gửi từ máy User1 với IP 10.9.0.6 tới Victim IP 10.9.0.5

Ảnh có chứa văn bản

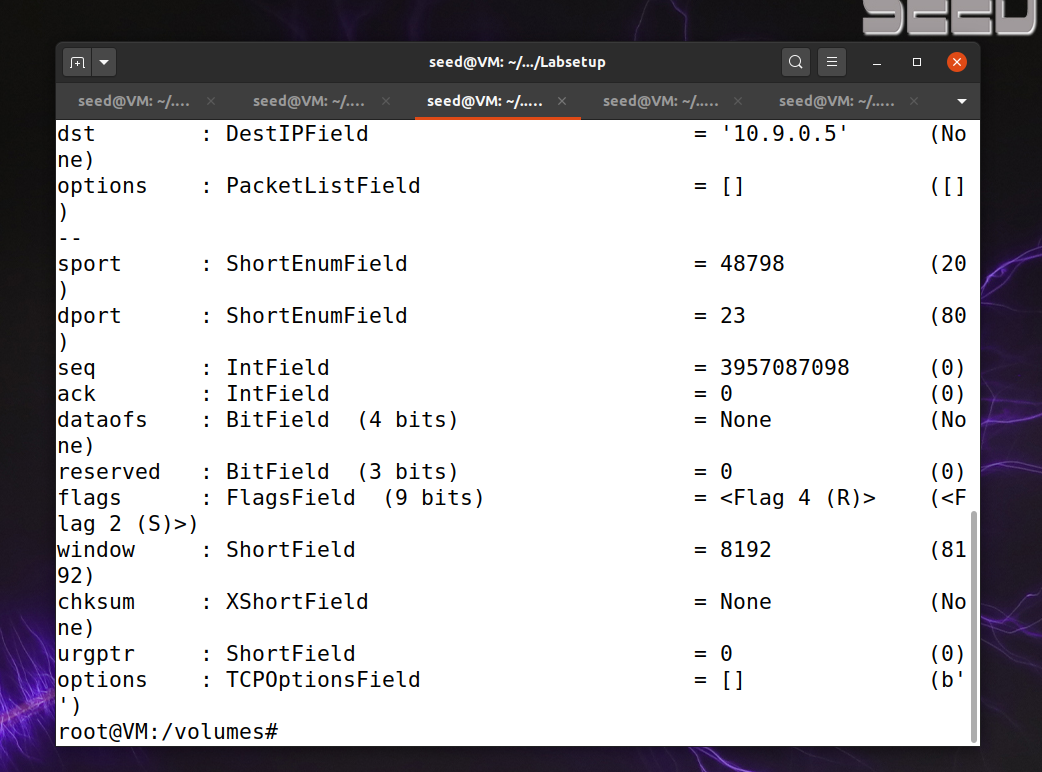
Mô tả được tạo tự động

+ Code dùng để khai thác

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Lấy lại lại trường sport cờ R để gửi gói tin Reset và seq là số next seq trong gói tin TCP ta bắt được

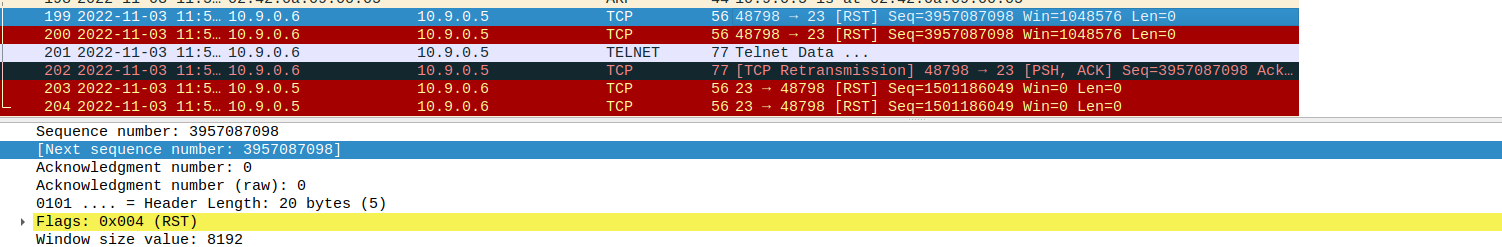


+ Kết quả sau khi thực hiện đoạn code

Ảnh có chứa văn bản

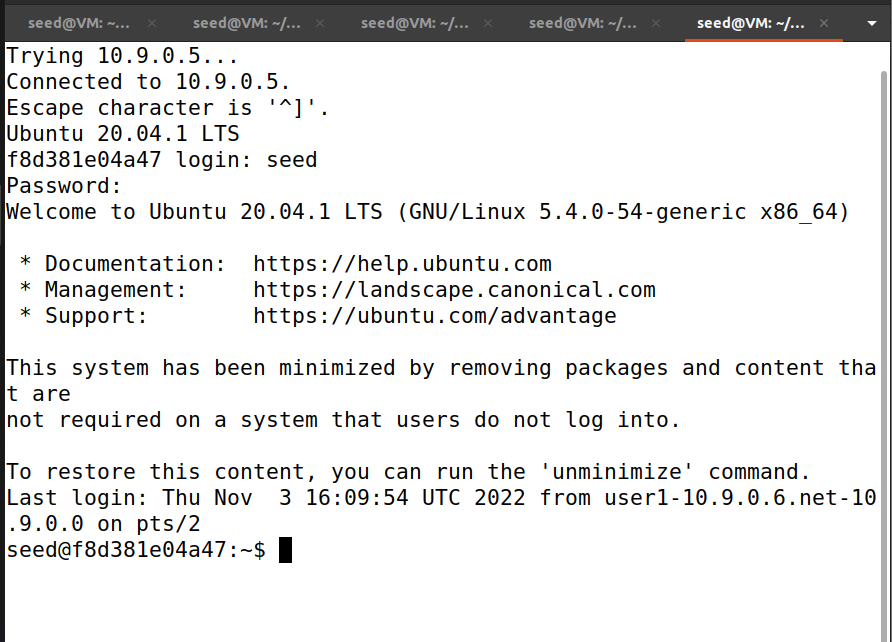
Mô tả được tạo tự động

+ Bên máy User1 ta chưa ngắt kết nối nhưng đã bị ngắt bởi attacker



+ Bên wireshrak ta có thể thấy trường flags là RST là gói tin Reset dù bên máy User1 chưa ngắt kết nối với Victim

* Auto Reset



+ Kết nối telnet giữa User1 và Victim

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Code dùng để khai thác

* Ta sẽ sniff gói tin từ iface của attacker sau đó snpoof để gửi liên tục
* Ảnh có chứa văn bản

  Mô tả được tạo tự động

+ Bên attacker gửi liên tục các gói tin

Ảnh có chứa văn bản

Mô tả được tạo tự động

+ Bên User1 mất kết nối với Victim dù chưa đóng hay exit