Bài: 8.3 Nghe trộm - Giới thiệu Wireshark, Biện pháp đối phó & kỹ thuật phát hiện nghe trộm

Xem bài học trên website để ủng hộ Kteam: 8.3 Nghe trộm - Giới thiệu Wireshark, Biện pháp đối phó & kỹ thuật phát hiện nghe trộm

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

Lab 8-2: Giới thiệu Wireshark

Quy trình

Mở **Wireshark** để thu thập gói tin.

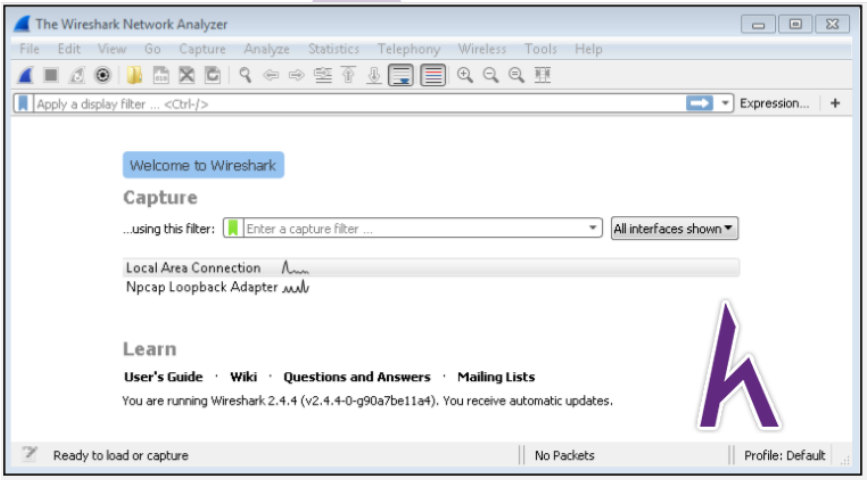

Figure 8-22 Wireshark Network Analyzer

Click **Capture** > **Options** để chỉnh sửa những lựa chọn thu thập.

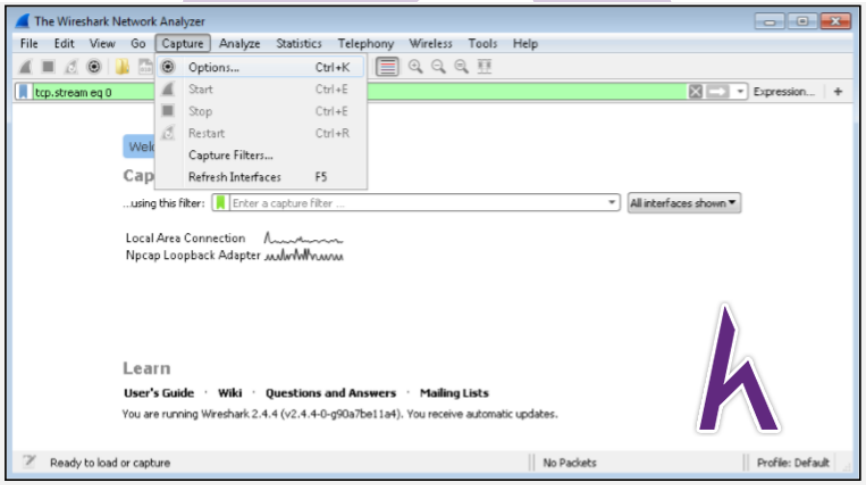

Figure 8-23 Wireshark Network Analyzer

Ở đây, bạn có thể kích hoạt hay vô hiệu hóa chế độ hỗn tạp trên giao diện. Thiết lập **Capture Filter** và chọn **Start**.

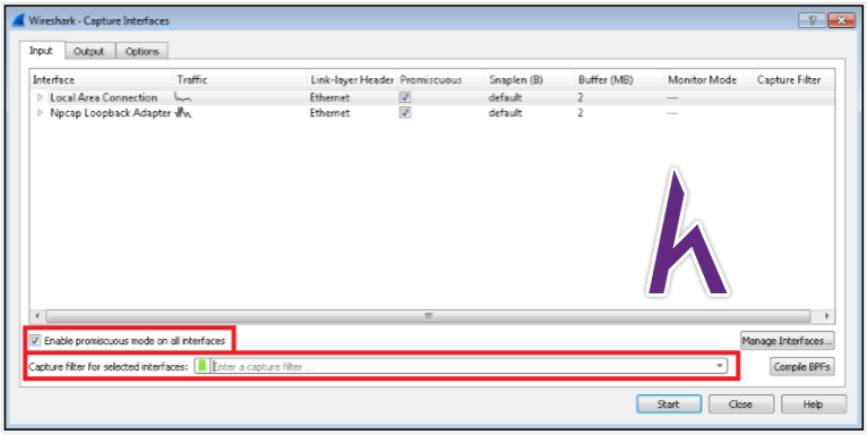

Figure 8-24 Wireshark Network Analyzer

Click **Capture** > **Capture Filter** để chọn những bộ lọc xác định. Bạn có thể thêm bộ lọc bằng cách click vào nút **Add** bên dưới.

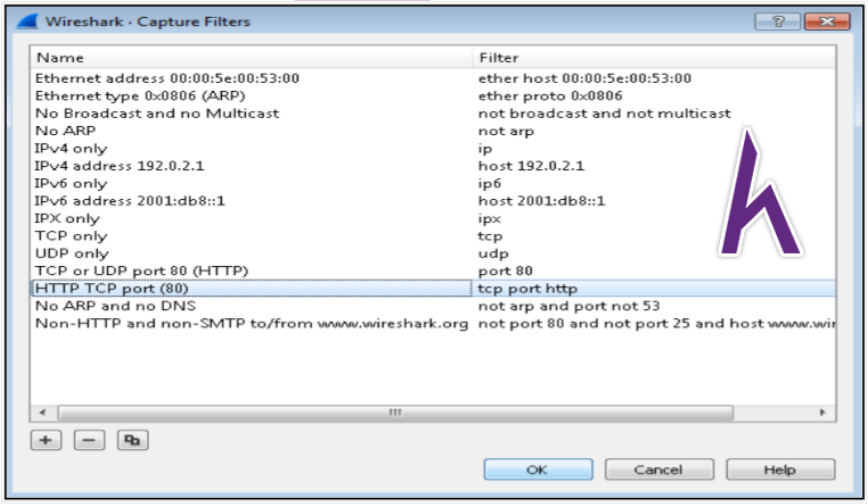

Figure 8-25 Wireshark Network Analyzer

Theo sát TCP Stream trong Wireshark

Làm việc trên giao thức dựa vào TCP có thể rất hữu ích bằng cách sử dụng tính năng theo sát **TCP stream** để kiểm tra dữ liệu từ TCP stream bằng phương pháp mà layer ứng dụng có thể quan sát. Ví dụ trong trường hợp bạn đang tìm mật khẩu trong một **Telnet stream**.

Kiểm tra dữ liệu từ gói tin thu thập như hình dưới.

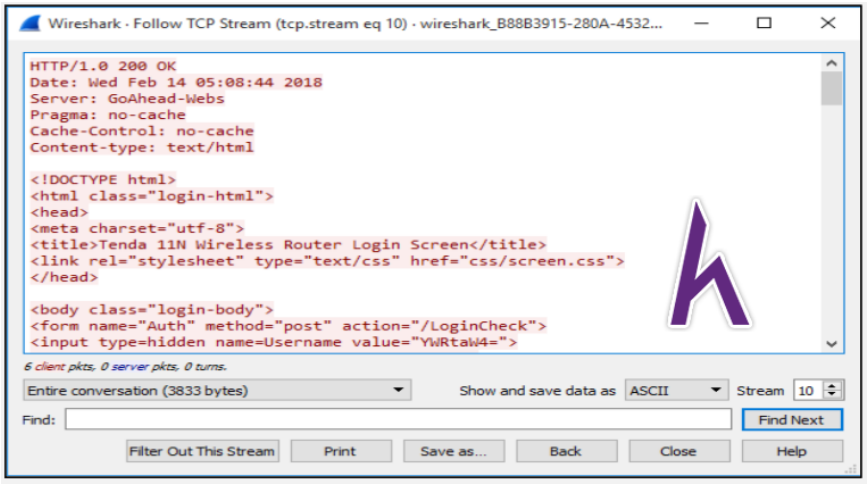

Figure 8-27 Wireshark Network Analyzer

Bộ lọc của Wireshark

Bảng dưới đây liệt kê những bộ lọc của Wireshark để lọc đầu ra.

Operator	Ý nghĩa	Ví dụ
==	Bằng	ip.addr == 192.168.1.1
eq	Bằng	tcp.port eq 23
!=	Không bằng	ip.addr != 192.168.1.1
ne	Không bằng	ip.src ne 192.168.1.1
contains	Chứa giá trị định rõ	http contains "http://www.ipspecialist.net"

Biện pháp đối phó

Ngăn chặn nghe trộm

Những kĩ thuật tốt nhất để bảo vệ giao thông mạng được liệt kê dưới đây:

- Sử dụng HTTPS thay vì HTTP
- Sử dụng SFTP thay vì FTP
- Sử dụng Switch thay cho hub
- Thiết lập bảo mật port
- Thiết lập DHCP Snooping
- Thiết lập thăm dò APR động
- Thiết lập bảo vệ nguồn
- Sử dụng công cụ phát hiện nghe trộm để phát hiện NIC trong chế độ hỗn tạp
- Sử dụng những giao thức giải hóa mạnh

Kĩ thuật phát hiện nghe trộm

Kĩ thuật phát hiện phần mềm nghe trộm

Phương pháp ping

Kĩ thuật ping được sử dụng để phát hiện phần mềm nghe trộm. Một yêu cầu ping sẽ được gửi đến địa chỉ IP đáng ngờ cùng với một địa chỉ MAC giả. Nếu NIC không hoạt động trong chế độ hỗn tạp, nó sẽ không phản hồi lại gói tin. Nếu phần mềm nghe trộm đang chạy thì nó sẽ phản hồi lại gói tin. Đây là một kĩ thuật cũ và không đáng tin cậy.

Phương pháp APR

Phần mềm nghe trộm sẽ bị phát hiện bằng **bộ nhớ đệm APR**. Bằng cách gửi một gói tin APR không truyền tin đến kẻ đáng ngờ, địa chỉ MAC sẽ được ghi vào bộ nhớ đệm nếu NIC đang chạy trong chế độ hỗn tạp. Bước tiếp theo là gửi bản truyền tin ping với địa chỉ MAC giả. Nếu máy đang chạy chế độ hỗn tạp, nó chỉ có thể phản hồi gói tin nếu nó đã ghi nhớ địa chỉ MAC thật từ gói tin APR không truyền tin đã nghe trộm.

Công cụ phát hiện chế độ hỗn tạp

Các công cụ như **PromqryUI** hay **Nmap** được dùng để phát hiện card giao diện hệ thống chạy trong chế độ hỗn tạp. Đây là những phần mềm ứng dụng **GUI based**.