**Bài thực hành Snort**

**Mục tiêu:**

• Sử dụng Snort để xem và phân tích gói tin

• Tạo các luật Snort bằng cách phân tích lưu lượng giao thức.

• Sử dụng Nmap để quét mạng và hệ thống, sau đó sử dụng Snort để phát hiện các tấn công quét mạng từ NMap.

**Các bước thực hiện (tham khảo file Lab7\_Snort rules.pdf)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Nội dung** | **Yêu cầu** |
| 1 | Cài đặt Snort trên Windows | Chụp ảnh nội dung lệnh ipconfig |
| 2 | Chuẩn bị máy ảo Kali với Nmap | Chụp ảnh nội dung ifconfig, ping tới máy cài Snort |
| 3 | Kiểm tra interface Snort với: C:\Snort> snort -W | Chụp ảnh nội dung |
| 4 | - Dùng Snort để bắt gói tin từ card mạng. Ví dụ: C:\Snort> snort -dev -i 3  - Test thử với lệnh ping từ máy Kali Linux tới máy Snort | Chụp ảnh nội dung |
| 5 | Cấu hình luật cho Snort để bắt lưu lượng phát sinh từ facebook.com  Vd: file luật trong c:\snort\rules\rules.txt  Nội dung: alert tcp any 80 -> any any ( \  msg:"Facebook web traffic detected"; \ content:"facebook.com"; sid:10000; )  Chạy với lệnh: snort -dev -i X -p -c rules\rules.txt -l log -K ascii -k none  Với X là interface bắt gói tin  Xem thư mục c:\snort\log phát sinh alert khi duyệt trang facebook.com | Chụp ảnh các nội dung đã phát sinh  Chụp ảnh alert nếu có  Địa chỉ IP của trang facebook là gì?  Sử dụng nslookup để xem thông tin DNS của server |
| 6 | Tạo rule để phát hiện lưu lượng gói tin ping  Sử dụng wireshark để bắt các lưu lượng này, khi thực hiện ping từ máy Kali sang máy chạy Snort  Thực hiện ping từ máy Windows khác sang máy chạy Snort  Thực hiện ping từ máy Linux sang máy chạy Snort  Tạo luật phát hiện lệnh ping chỉ trong các máy nội mạng  Tạo lệnh bắt gói tin ping ra ngoài Internet, thử với google.com | Chụp ảnh các nội dung tương ứng  - Giao thức lệnh ping?  - filter cho Wireshark để lọc gói tin lệnh ping  - dữ liệu trong gói tin là gì, ở đâu  - tất cả các gói tin ping đều giống nhau? |
| 7 | Tạo rule để phát hiện quét mạng trong hệ thống  - Sử dụng netstat để phát hiện các port đang mở  - netstat –a –p TCP để phát hiện các tcp port đang lắng nghe, option –n để kiểm tra số hiệu port  - Sử dụng nmap/zenmap trong máy ảo Kali để quét mạng của máy chạy Snort  - Tạo luật để phát hiện SYN Scan (phát hiện SYN flag từ gói tin từ chương trình quét mạng)  - Test luật và kiểm tra alert | Host scaning, network scanning  - Chụp ảnh 1 số port phổ biến  - Liệt kê các cổng dịch vụ đã phát hiện với nmap  - Có bao nhiêu alert đã tạo? Có khi nào phát sinh alert nhầm không? |