DDos ATTACK DETECTION BASED ON NEURAL NETWORK

Trần Nguyên Ngọc | tnn1999@mail.ru

Vấn đề an ninh hệ thống

4 mức độ cơ bản được quan tâm phát triển ứng dụng bảo mật:

- Mức độ các chương trình ứng dụng, đây là môi trường trực tiếp tương tác với người dùng như các phần mềm soạn thảo văn bản, thư điện tử, bảng tính…
- Mức độ hệ quản trị cơ sở dữ liệu (CSDL), phục vụ cho việc lưu trữ, quản lý thông tin như các hệ thống quản trị cơ sở dữ liệu Oracle, MS SQL Server, MS Access…
- Mức độ hệ điều hành, chịu trách nhiệm bảo đảm môi trường hoạt động cho các chương trình ứng dụng và cả các hệ quản trị CSDL.
- Mức độ mạng máy tính, chịu trách nhiệm bảo đảm môi trường tương tác giữa các nút thông tin (máy tính hoặc cụm máy tính) thông qua các chuẩn giao tiếp là các giao thức như TCP/IP, ISP/SPX, SMB/NetBIOS...

Ví dụ khai thác sơ hở

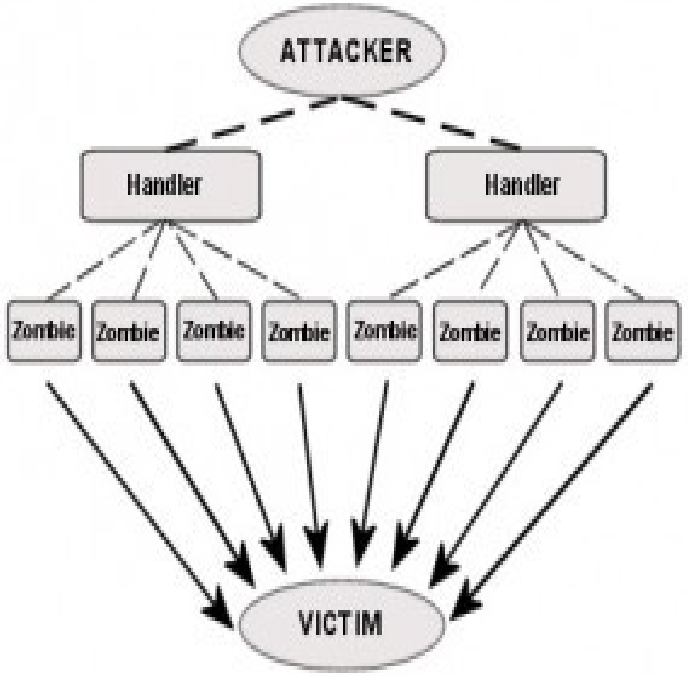
- Truy xuất CSDL thông qua các chương trình có lời gọi các câu truy vấn SQL mà vô tình hệ thống sơ hở cho phép truy cập vào CSDL (mức độ ứng dụng)
- Can thiệp trực tiếp các thông tin của hệ thống quản trị CSDL nếu có quyền khai thác (mức độ CSDL)
- Giải mã các tệp tin chứa CSDL thông qua hệ thống quản lý tệp tin (mức độ hệ điều hành)
- Chặn bắt các gói tin được truyền đi trên mạng (mức độ mạng)

DDoS

- Dos - Denial of service
- DDOS- distributed denial-of-service
- Chiến thuật đơn giản, hiệu quả đáng kể:

Bước 1: Kẻ tấn công xây dựng nên hệ thống các máy trạm (Zombie) **bị kiểm soát** (botnet), tức là những máy tính bị cài đặt các chương trình đặc biệt và sẽ bị huy động tấn công theo sự điều khiển của kẻ tấn công.

Bước 2: Kẻ tấn công **ra lệnh** cho các Zombie cùng tấn công / giám sát/ lấy cắp thông tin vào một địa chỉ nhất định theo một **kịch bản** cho trước.



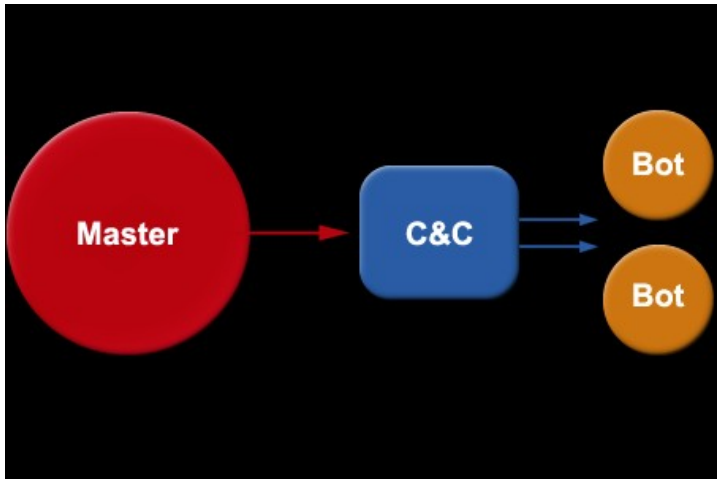
Đặc điểm & Xu hướng

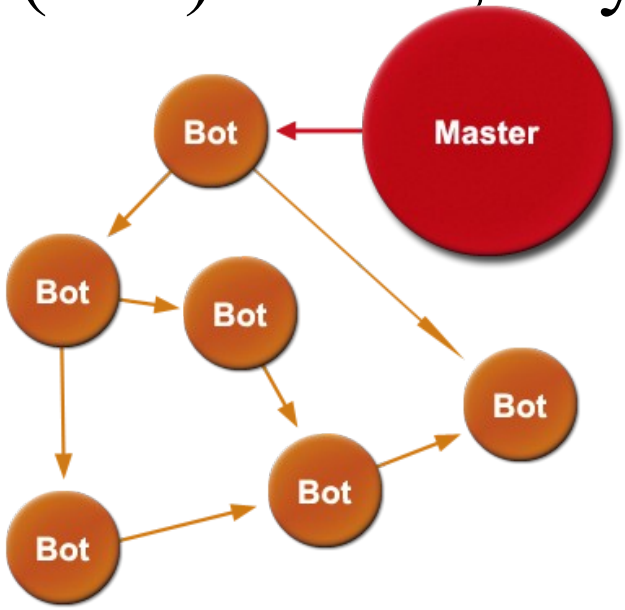
DDoS tiến hành khai thác các lỗ hổng bảo mật ở cả 4 mức độ nhằm: cài đặt trái phép các phần mềm điều khiển vào các máy tính của mạng botnet, phát động tấn công thông qua mạng Internet, làm ngưng trệ một số dịch vụ của hệ quản trị CSDL hoặc hệ điều hành

Xu hướng gần đây của các mạng botnet là sử dụng IP thật nên việc phát hiện nhanh, chính xác các cuộc tấn công DDoS trở nên phức tạp hơn.

Quản lý botnet

C&C,Tor Hidden Service (P2P) – Zeus, Skynet

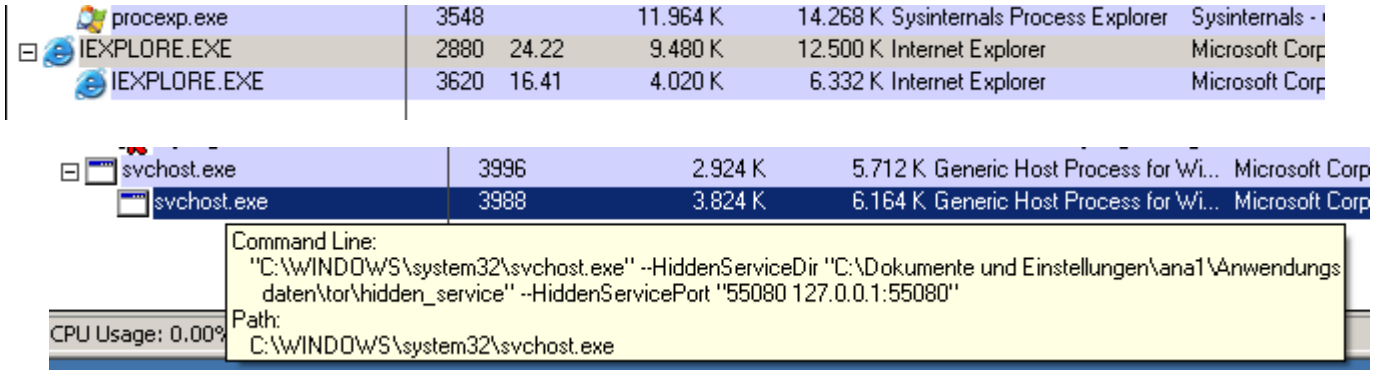




Phát hiện tấn công

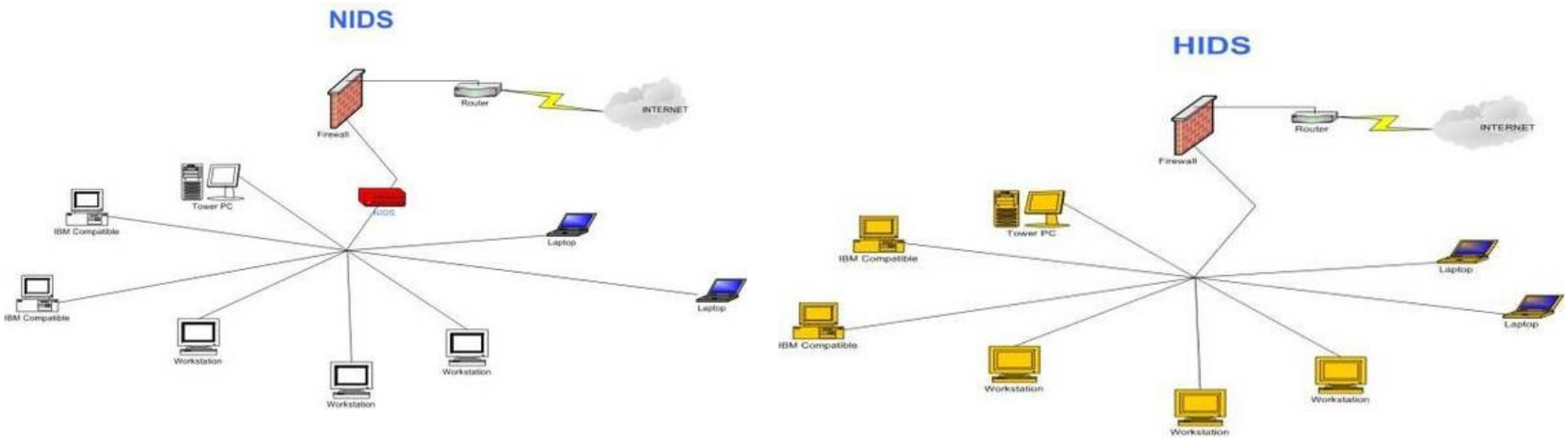
- Network based (đánh giá trên các nút mạng, phối hợp thông tin giữa các nút để đưa ra kết luận cuối cùng)
- Host based (đo các thông số RAM, CPU, …)

Ví dụ skynet (http://www.xakep.ru/post/59789/default.asp ngày 11.12.2012) khi phân tích IEXPLORE , SERVICE HOST:

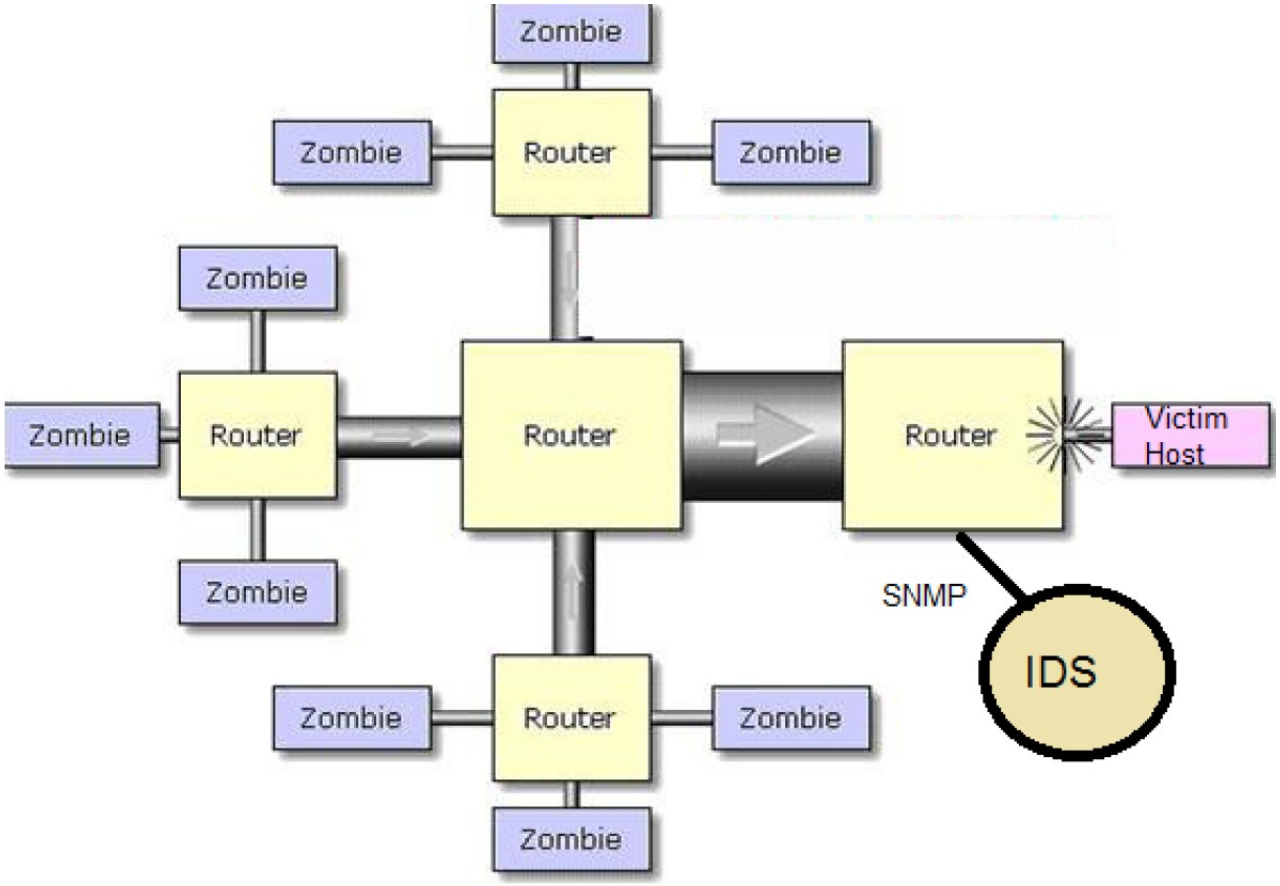


Chi tiết IDS

IDS- Intrusion Detection System theo 2 hướng

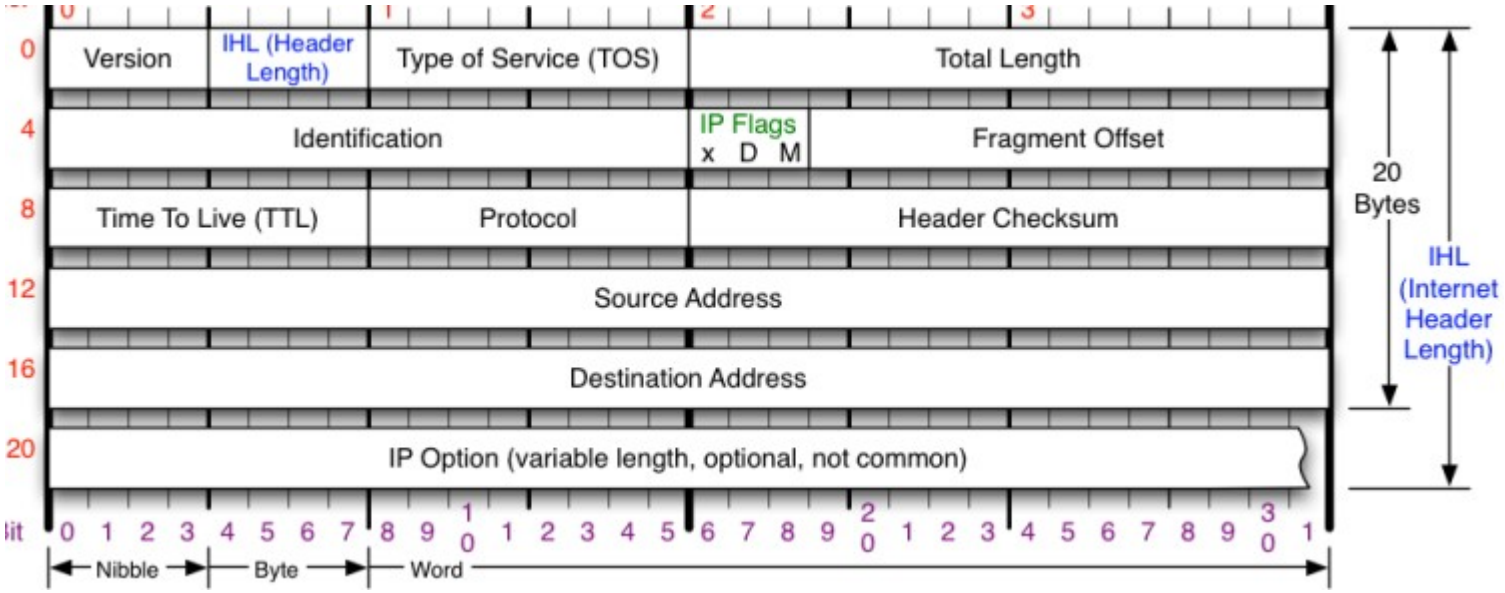


Hướng tiếp cận



Phân tích gói tin

IPv4 header



Đơn giản có thể dùng Rule

Ví dụ Ping of Death

(ip[2:2] - ((ip[0:l]&0x0f)*4) + ((ip[6:2]&0xlfff)*8)) > 65535

Land

ip[12:4] = ip[16:4]

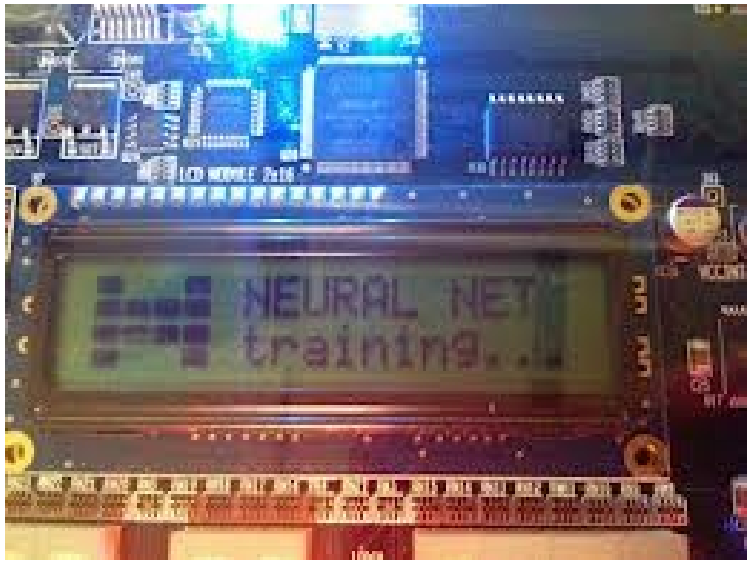
Phải phân tích mẫu, cần chuyên gia phân tích trực tiếp! Có thể khái quát các luật để thích nghi?

Machine learning?

Tại sao lựa chọn ANN?

Hiệu quả nhận dạng tương đương SVM, Adaboost…

Khả năng hiện thực FPGA



Features Selection

- Chỉ số IP phân tán (m)
- Khoảng cách thời gian truy cập (Δt)
- Lưu lượng thông tin trao đổi (d)
- Chỉ số khác biệt của dung lượng các gói tin (Δd)
- Chỉ số khác biệt các giao thức sử dụng (p)

Thử nghiệm

DARPA IDS- Lincoln Laboratory Scenario

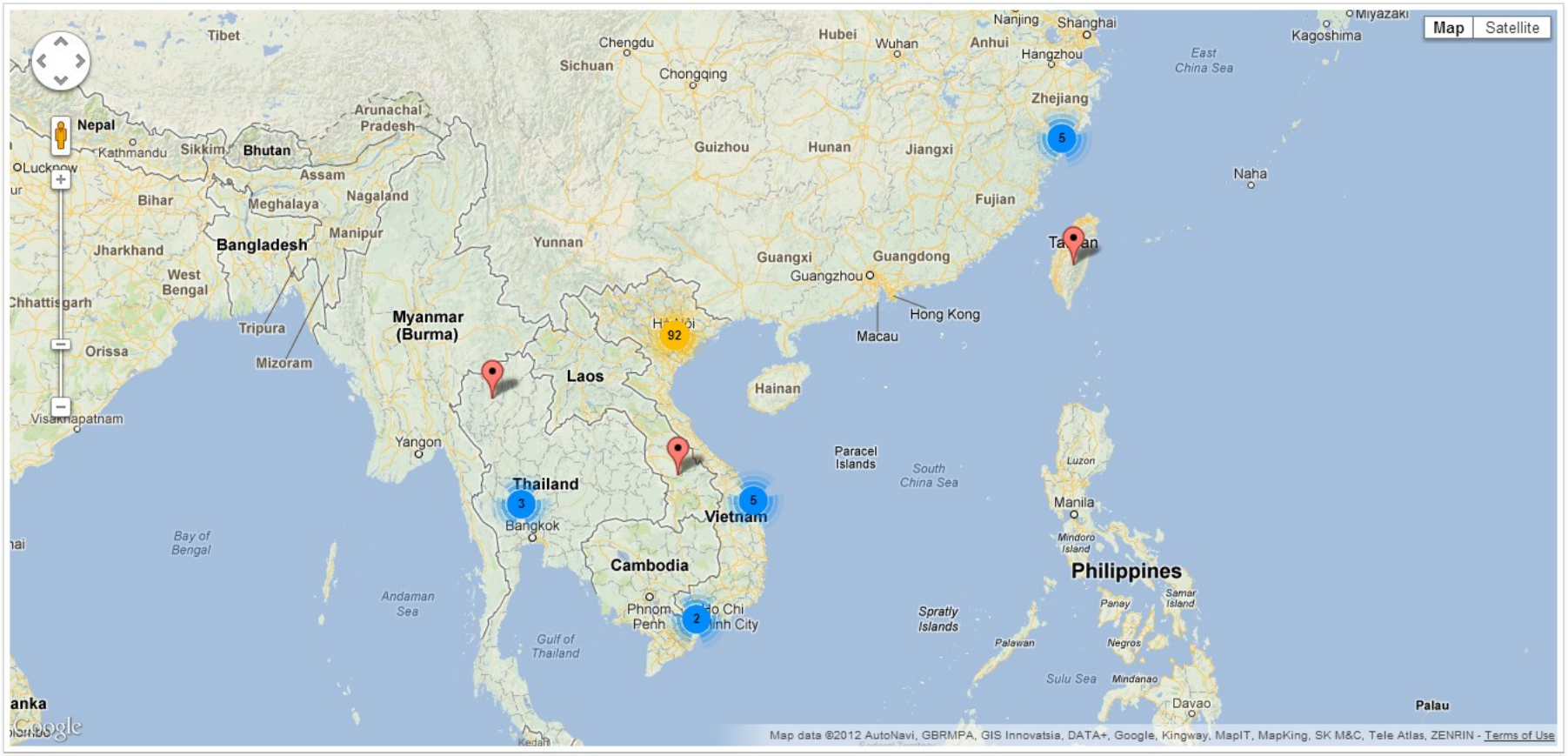
Low Orbit Ion Cannon (LOIC) TCP-SYN flooding.

MTA data + Solarwinds

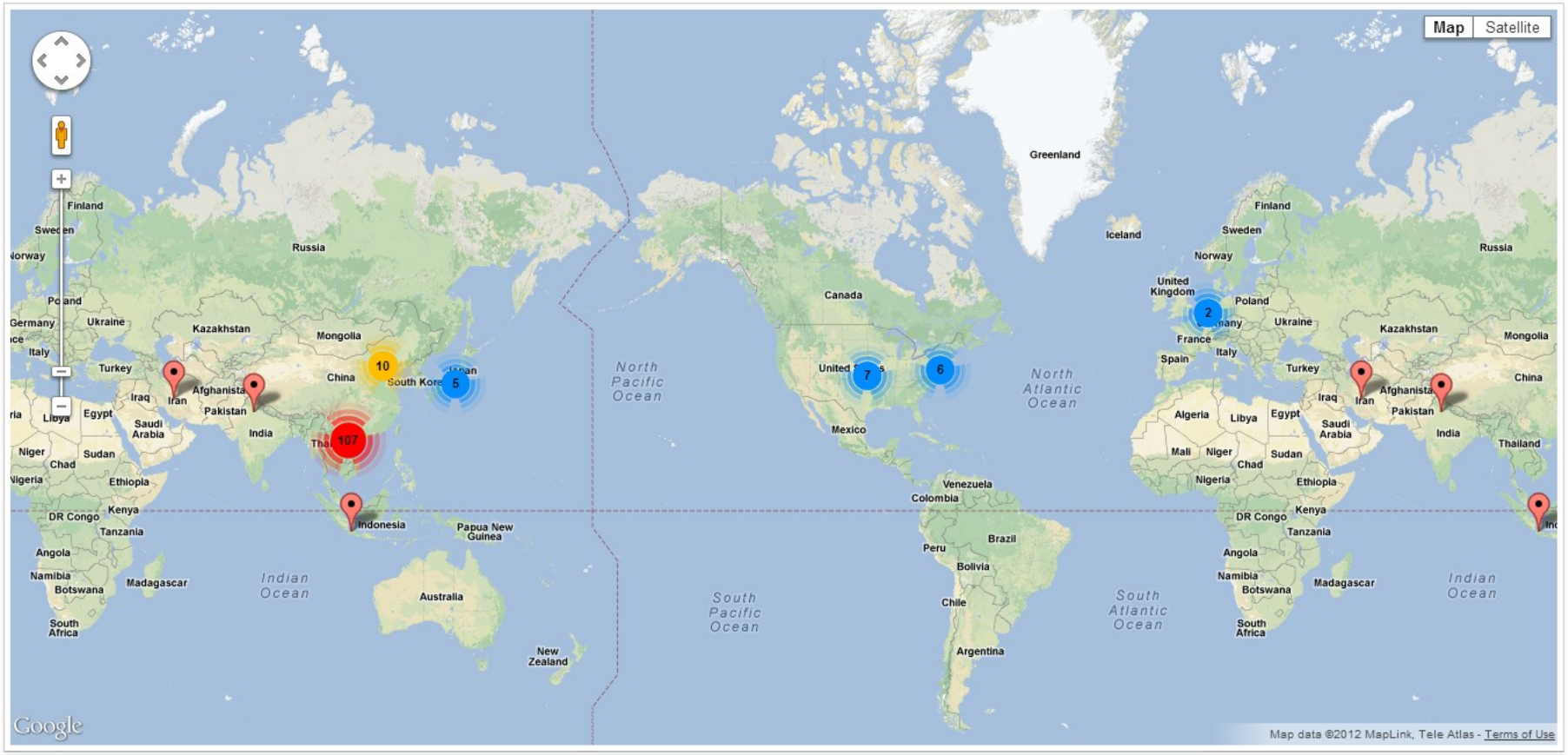
Network Performance Monitor

NetFlow Traffic Analyzer

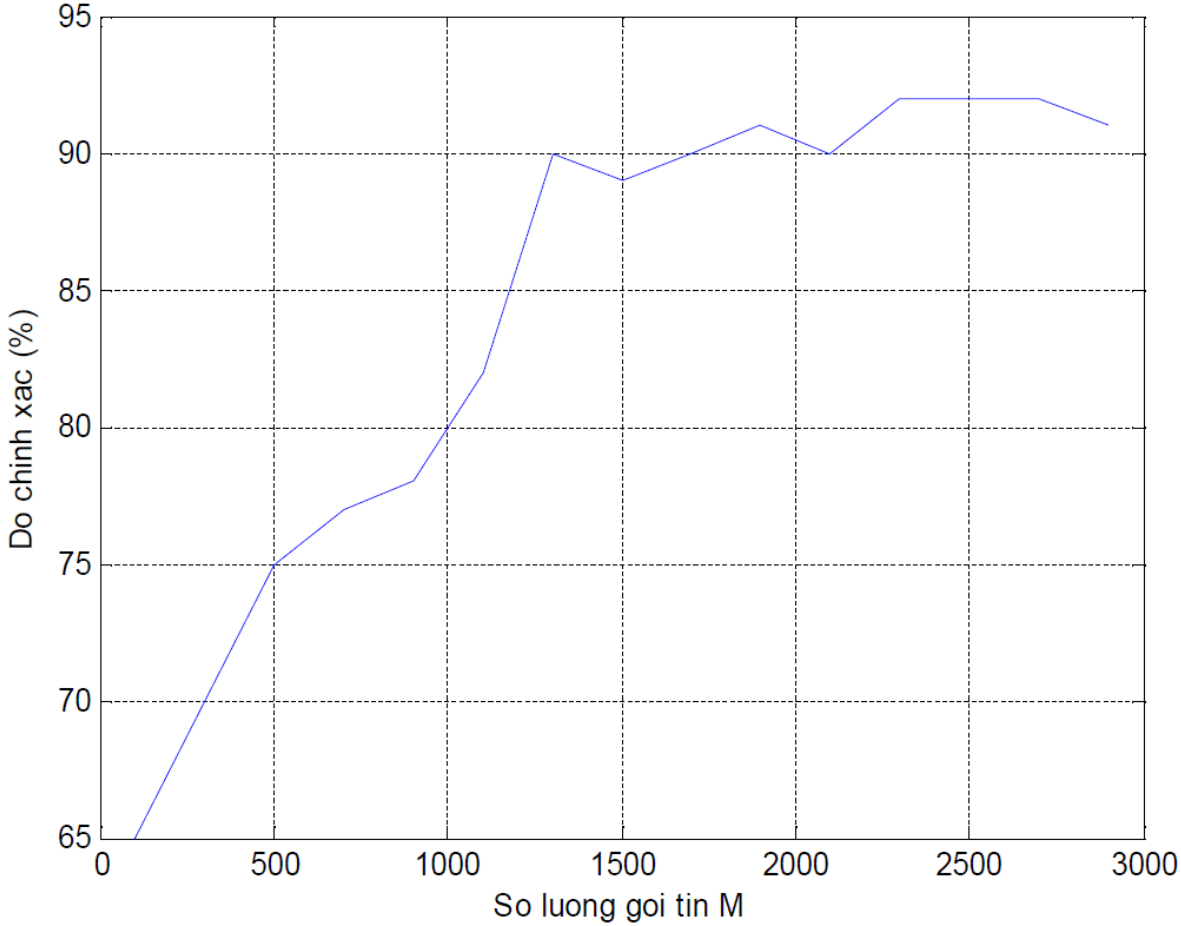
Kết quả Botnet marker



Botnet marker



Detection rate



Tài liệu tham khảo

1. Jaehak Yu, Hansung Lee, Myung-Sup Kim, Daihee Park. Traffic flooding attack detection with SNMP MIB using SVM. ELSEVIER, Computer Communications 31 (2008) 4212–4219.
2. R Vijayasarathy, Balaraman Ravindran, S V Raghavan. A system approach to network modeling for DDoS detection using a Naïve Bayesian classifier. Communication Systems and Networks (COMSNETS), 2011,P1-10.
3. Bailey, M. , Cooke, E. , Jahanian, F. , Yunjing Xu ,Karir M. A Survey of Botnet Technology and Defenses. Conference For Homeland Security, 2009. CATCH '09. Cybersecurity Applications & Technology. P299 – 304
4. Cisco Systems, “White paper – NetFlow Services and Applications”.
5. http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/2000/LLS_DDOS_1.0.html