Security trên tầng Network:

- Ipsec là mặc định trên Ipv6, tùy chọn trên Ipv4
- Ipsec tác dụng: Xác thực (authentication), bảo mật (confidentiality), quản lí những khóa dùng để bảo mật
- VPN mạng riêng ảo
- Security Remote Access:
  + SSH remote và login vào hệ thống ở xa
  + SSTP
- Intranet (mạng riêng), cũng có application
- Internet cung cấp thêm application , internetwwork mạng kết nối với các mạng khác

Bảo mật từ tầng Application đến tầng Transport HTTPS + HTTP +SSL trong môi trường web

Tính toàn vẹn (hash function) integrity

Tính bí mật (cho vào đường ống) cònidentiality

DES

Mô hình OSI gồm 7 tầng: Application, Pre, session, Transport, Netwwork, Datalink, Phýical

Mô hình TCP/IP : Application, Transport, Network, Dât link, Phíical

Zero – Day attack

Sử dụng con virus đầu tiên xuất hiện để tấn công phần mềm diệt virs chưa được cập nhập loại đó

Virus nằm trong file + boot sector (cài lại hệ điều hành không hiệu quả) + flash web action script bị HTML 5 thay thế

Encrypted virus : 1 đoạn mã tạo key và mã hóa đoạn còn lại của virus làm thay đổi hình dạng của virus + khi hoạt động sẽ giải mã lại hình dạng ban đầu.

Polymorphic virus đa hình:

Nhân bản giống hình dạng con virus ban đầu.

Metamorphic virus siêu đa hình: nhân jbarn không giống hình dạng con virus ban đầu, có khả năng tự biến đổi hình dạng của nó.

Chương 7 Transport level security chứng chỉ SSL

Security Socket Layer nằm giữa tầng applcation và tầng Transport, lần đầu tiên do netscape dduaww ra (mô hình TCP/IP 4 lớp, application, transport, internet, netwwork, access

Forensic: chứng chỉ cho các điều tra viên trên môi trường mạng

Xây dựng đường hầm cho gói tin

Cơ chế tunnerling giống như việc chuyển giữa Ipv4, Ipv6 (App – Transport)

Gói tin Ipv4 gồm header + data => Ipv6 qua cơ chế tunerling được gắn thêm header

DOS, tấn công từ chối dịch vụ

Chuẩn bị mã độc: làm cái gì , cơ chế lấy lan(vào máy nạn nhân không quá dễ phát hiện) , trong điều kiện nào thì hoạt động

File pdf không nhiễm fiel .doc có nhiễm

MÃ độcL

Sống kí sinh: trapdoor – backdoor cửa sau không nhận bản tạo 1 cơ chế để quay trở lại xâm nhập

Logic bombs đoạn mã trong phần mềm, bt không thỏa mãm.

Troạn horese không nhân bản 1 đoạn mã độc chèn thêm vào chương trình có ích khác

Virus có nahan bản

Sống độc lập Worm + zombie

Dos không nhận đc kết nối

Giao thưc ARP Address Resdation Protocal dựa trên địa chỉ IP địa chỉ MAC tương ứng ánh xạ

Đởi địa chỉ Mac làm giả nó sử dụng wire shark,

Man in the middle attack làm cho dòng dữ liệu đi qua mình

IDS có hai loại HIDS, và NIDS

Phân loại Intrudes trong Textbox:

Masquaere giả dạng người khác

Misfeasor lạm quyền

Clandestine User ngăn cản việc kiểm tra

Black Hacker -> Crack