Nama : Muhamad Nur Khafid

Nim : 1310651079

1. A Network Topology

Sebuah jaringan komputer dapat dibagi atas kelompok jaringan eksternal (Internet atau pihak luar) kelompok jaringan internal dan kelompok jaringan eksternal diantaranya disebut DeMilitarized Zone (DMZ). - Pihak luar : Hanya dapat berhubungan dengan host-host yang berada pada jaringan DMZ, sesuai dengan kebutuhan yang ada. - Host-host pada jaringan DMZ : Secara default dapat melakukan hubungan dengan host-host pada jaringan internal. Koneksi secara terbatas dapat dilakukan sesuai kebutuhan. - Host-host pada jaringan Internal : Host-host pada jaringan internal tidak dapat melakukan koneksi ke jaringan luar, melainkan melalui perantara host pada jaringan DMZ, sehingga pihak luar tidak mengetahui keberadaan host-host pada jaringan komputer internal.

A. Security Information Management

Salah satu alat bantu yang dapat digunakan oleh pengelola jaringan komputer adalah Security Information Management (SIM). SIM berfungsi untuk menyediakan seluruh informasi yang terkait dengan pengamanan jaringan komputer secara terpusat. Pada perkembangannya SIM tidak hanya berfungsi untuk mengumpulkan data dari semua peralatan keamanan jaringan komputer tapi juga memiliki kemampuan untuk analisa data melalui teknik korelasi dan query data terbatas sehingga menghasilkan peringatan dan laporan yang lebih lengkap dari masing-masing serangan. Dengan menggunakan SIM, pengelola jaringan komputer dapat mengetahui secara efektif jika terjadi serangan dan dapat melakukan penanganan yang lebih terarah, sehingga organisasi keamanan jaringan komputer tersebut lebih terjamin.

B. IDS / IPS

Intrusion detection system (IDS) dan Intrusion Prevention system (IPS) adalah sistem yang digunakan untuk mendeteksi dan melindungi sebuah sistem keamanan dari serangan pihak luar atau dalam. Pada IDS berbasiskan jaringan komputer , IDSakan menerima kopi paket yang ditujukan pada sebuah host untuk selanjutnya memeriksa paket-paket tersebut. Jika ditemukan paket yang berbahaya, maka IDS akan memberikan peringatan pada pengelola sistem. Karena paket yang diperiksa adalah salinan dari paket yang asli, maka jika ditemukan paket yang berbahaya maka paket tersebut akan tetap mancapai host yang ditujunya.Sebuah IPS bersifat lebih aktif daripada IDS. Bekerja sama dengan firewall, sebuah IPS dapat memberikan keputusan apakah sebuah paket dapat diterima atau tidak oleh sistem. Apabila IPS menemukan paket yang dikirimkan adalah paket berbahaya, maka IPS akan memberitahu firewall sistem untuk menolak paket data itu. Dalam membuat keputusan apakah sebuah paket data berbahaya atau tidak, IDS dan IPS dapat memnggunakan metode

C. Signature based Intrusion Detection System : Telah tersedia daftar signature yang dapat digunakan untuk menilai apakah paket yang dikirimkan berbahaya atau tidak.
D. Anomaly based Intrusion Detection System : Harus melakukan konfigurasi terhadap IDS dan IPS agar dapat mengetahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Paket anomaly adalah paket yang tidak sesuai dengan kebiasaan jaringan komputer tersebut.
E. Port Scanning

Metode Port Scanning biasanya digunakan oleh penyerang untuk mengetahui port apa saja yang terbuka dalam sebuah sistem jaringan komputer. Cara kerjanya dengan cara mengirimkan paket inisiasi koneksi ke setiap port yang sudah ditentukan sebelumnya. Jika port scanner menerima jawaban dari sebuah port, maka ada aplikasi yang sedang bekerja dan siap menerima koneksi pada port tersebut.

F. Packet Fingerprinting

Dengan melakukan packet fingerprinting, kita dapat mengetahui peralatan apa saja yang ada dalam sebuah jaringan komputer. Hal ini sangat berguna terutama dalam

sebuah organisasi besar dimana terdapat berbagai jenis peralatan jaringan komputer serta sistem operasi yang digunakan.

2. 2. Berikut ini ada file ciphertext misterius

VGlkYWsgc2VnYW1wYW5nIGl0dWxhaCBtYXMgYnJvLiBkZWNyeXB0IGluaTogDQo2ODc0NzQ3MDNhMmYyZjY0NmMyZTY0NzI2ZjcwNjI2Zjc4MmU2MzZmNmQyZjczMmYzMjM0NjkzMTZiNzEzNjc5NjM2ZjZmNjg3MTZhNmMyZjYzNzI3OTcwNzQ2ZjMxNDY2YzYxNjcyZTZkNzAzMw==

Anda sebagai seorang ahli forensik diminta untuk menyelidiki maksud yang tersembunyi pada cipher tersebut. Berikan analisis Anda dan tuliskan langkah-langkah untuk menemukan "sesuatu" yang tersembunyi pada cipher tersebut.

Analisis:

1. Original text - 212 chars.
2. Letter frequencies
z : 29
m : 23
n : 21
y : 19
j : 15
c : 9
w : 9
t : 7
g : 7
i : 7
d : 5
x : 5
q : 4
o : 4
l : 4
k : 4
a : 3
v : 3
b : 3
h : 3
e : 2
u : 2
s : 1
r : 0
f : 0

p : 0