

## BAB I

### PENDAHULUAN

#### 1.1 Latar Belakang Masalah.

*Windows* XP merupakan salah satu sistem operasi yang banyak digunakan dengan salah satu keunggulannya yaitu *User-Friendly*. Dibalik keunggulan tersebut, integritas sistem operasi untuk berjalan pada aplikasi jaringan jauh tertinggal dibandingkan sistem operasi lainnya seperti *Linux* atau *Unix*. Salah satu kelemahan sistem operasi ini yang banyak digunakan para penyusup adalah protokol RPC (*Remote Procedure Call*).

Serangan celah keamanan RPC Deom yang pernah populer di tahun 2003 terjadi pada tanggal 12 Agustus 2003 dimana dimanfaatkan dengan sangat baik oleh worm *Lovean* atau lebih dikenal dengan nama *Blaster* dan variannya menyebabkan semua komputer *Windows* NT / 2000 / XP / 2003 saling melakukan scanning untuk menyebarkan dirinya dan sempat menggegerkan jagad internet. Eksploitasi celah keamanan RPC Deom kemudain kembali muncul di tahun 2004 -2005 dimana *trend* yang terjadi adalah satu malware yang memiliki kemampuan mengeksploitasi berbagai celah keamanan dan terkadang satu *malware* mengeksploitasi belasan celah keamanan. Setelah serangan tersebut mereda, kelihatannya di akhir tahun 2008 ini kembali muncul peluang eksploitasi baru atas celah keamanan RPC Deom lagi dan kali ini cukup serius karena *Windows* XP dengan *Service Pack* 3 sekalipun tetap rentan terhadap eksploitasi celah keamanan RPC Deom baru ini.

## 1.2 Rumusan Masalah.

Setelah memaparkan latar belakang dari pada penelitian ini, penulis merumuskan permasalahan dalam penelitian ini dengan mengacu pada latar belakang tersebut yaitu:

1. Mengapa terjadi eksploitasi?
2. Persiapan apa yang dibutuhkan dalam melakukan eksploitasi ?.
3. Bagaimana melakukan eksploitasi pada operating sistem *Windows XP* pada jaringan lokal ?.
4. Eksploitasi seperti apa yang dihasilkan ?.
5. Bagaimana cara mengatasi terjadinya eksploitasi tersebut ?.

## 1.3 Batasan Masalah.

Dalam penelitian dan penulisan ini penulis akan membatasi ruang lingkup yang akan ditangani atau dibahas sehingga penilitain bisa lebih terfokus, ruang lingkup itu akan penulis batasi pada:

1. Jaringan komputer dalam hal ini berfokus pada jaringan *Local Area Network (LAN)*.
2. Sistem Operasi yang digunakan dalam penelitian baik yang digunakan dalam melakukan eksploitasi ataupun yang terkena eksploitasi adalah sistem operasi *windows XP (Windows XP Operating Sistem)*.

3. Pada penelitian ini target permasalahan terfokus pada eksploitasi *Remote Procedure Call (RPC)* pada *port* yang dianggap mudah untuk melakukan eksploitasi seperti *port* DCom 135 dan 445 pada sistem operasi *windows XP (Windows XP Operating System)*.

#### **1.4 Tujuan Penelitian.**

Tujuan yang ingin dicapai penulis dari penelitian ini adalah :

1. mencoba mengetahui celah pada sistem operasi *windows XP*.
2. setelah mengetahui adanya celah pada sistem tersebut kemudian penulis mempunyai tujuan untuk memberikan informasi kepada para pengguna jaringan komputer tentang bagaimana mengetahui ciri-ciri, tata cara serangan pada jaringan komputer dan bagaimana cara mengatasinya

#### **1.5 Manfaat Penelitian.**

Dalam penelitian ini penulis berharap semoga dapat memberikan manfaat bagi para pengguna jaringan komputer diantaranya: mahasiswa dan administrator jaringan. Untuk lebih detailnya akan penulis uraikan sebagai berikut :

##### **Pengguna non-IT**

Dalam hal ini orang yang awam tentang dunia komputer dan teknologi jaringan komputer. Pengguna ini hanya cenderung menggunakan teknologi jaringan komputer jika benar-benar membutuhkan. Sehingga tidak mengetahui apa dan bagaimana dampak dari sisi negatif dari jaringan komputer.

### Pengguna IT

Pengguna IT sama dengan pengguna non-IT namun yang membedakan, pengguna IT ini sering menggunakan teknologi jaringan komputer untuk memenuhi sebagian aktivitas sehari-harinya.

### Pengguna Mahasiswa

Pengguna mahasiswa yang dimaksudkan penulis adalah mahasiswa yang berkonsentrasi mempelajari dunia komputer baik jaringan, sistem, ataupun teknik.

### Administrator jaringan

Pengguna ini adalah orang yang benar-benar telah mengetahui seluk beluk jaringan komputer, mengetahui dampak baik positif ataupun negatif dan mengetahui tata cara mengatasi berbagai dampak negatif dari pada teknologi ini.

Dari semua pengguna yang telah penulis uraikan, harapan penulis semoga para pengguna dapat mengetahui dan mengerti salah satu sisi negatif dari pada teknologi komputer dan mengetahui bagaimana ciri-ciri, tata cara serangan pada jaringan komputer melalui RPC dan bagaimana cara mengatasinya. khusus bagi administrator jaringan komputer penulis menambahkan dan mengingatkan kiranya agar selalu waspada terhadap kecenderungan adanya pengguna jaringan komputer lain untuk menyusup sistem anda baik dengan teknik penyusupan yang sudah lama maupun teknik yang baru.

## 1.6 Metode Pengumpulan Data

Untuk mendapatkan hasil yang diinginkan maka pengumpulan data yang akurat sangat diperlukan dalam penyusunan laporan kegiatan penelitian ini. Karena tanpa kelengkapan data di lapangan suatu laporan kegiatan penelitian ini akan mengalami hambatan karena data merupakan komponen utama dalam penyusunan laporan yang paling penting. Untuk mendapatkan data tersebut penulis harus melakukan beberapa tahapan pengumpulan data penelitian, yaitu sebagai berikut :

penelitian dengan metode ini peneliti mengamati seluruh proses kegiatan

### 1 Metode Observasi ( *Observation* )

Penelitian mengamati secara langsung semua aktifitas yang dilakukan oleh objek instalasi, konfigurasi, *toll* yang dipakai.

### 2 Metode Wawancara ( *Interview* )

Dengan metode ini penulis dapat memperoleh penjelasan dan pengarahan Metode ini dimaksudkan untuk mendapatkan konsep-konsep teoritis

### 3 Metode Kepustakaan ( *Library* )

Langsung dari pihak yang terkait, menggunakan buku-buku sebagai bahan referensi dalam mendapatkan informasi-informasi yang dibutuhkan. Sistematika Penulisan.

## 1.7 Sistematika Penulisan

Penulisan skripsi ini akan dibahas dan disusun bab demi bab dengan sistematika penulisan sebagai berikut :

## **BAB I Pendahuluan**

Pada bab ini menjelaskan mengenai latar belakang masalah, identifikasi masalah, batasan masalah, tujuan penelitian, metodologi penelitian, serta sistematika penulisan.

## **BAB II Landasan Teori**

Bab landasan teori menguraikan teori-teori yang mendasari pembahasan secara detail, dapat berupa definisi - definisi atau model matematis yang langsung berkaitan dengan ilmu atau masalah yang diteliti.

## **BAB III . Metode Penelitian**

Bab ini menguraikan tentang gambaran obyek penelitian, langkah-langkah penelitian. Pada bab ini juga dilaporkan alat serta aplikasi sebagai alat bantu yang diperlukan dalam penelitian.

## **BAB IV . Implementasi dan Pembahasan**

Pada bab ini menjelaskan pembahasan tentang bagaimana implementasi Remote procedure call, penjelasan pengujian terhadap sistem, serta bagaimana menangani permasalahan yang ada pada sistem tersebut.

## **BAB V Penutup**

Berisi kesimpulan dan saran. Kesimpulan dan saran dikemukakan berdasarkan hasil penelitian dari penulis.

## **Daftar Pustaka**

Bahan-bahan yang merupakan referensi atau literatur atas



penelitian yang dikemukakan secara jelas. Daftar pustaka tersebut disusun dengan aturan penulisan daftar pustaka seperti lazimnya digunakan dalam penulisan skripsi.

