KEAMANAN JARINGAN

PERTEMUAN 10

APA ITU KEAMANAN JARINGAN ?

- Suatu cara atau suatu sistem yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan.

KEAMANAN JARINGAN PADA LAN

- Pada jaringan LAN yang cakupannya lebih kecil dari WAN ataupun MAN, ini perlu diamankan jaringannya. Justru ketika pada jaringan LAN sudah tidak aman bisa jadi merembet kepada jaringan yang diatasnya.
- Dalam mengmankan jaringan LAN ini ada beberapa teknik pengamannya, baik menggunakan software ataupun hardwarenya.

MACAM-MACAM SERANGAN PADA JARINGAN LAN (1)

- Sniffing adalah Kegiatan penyadapan pada lalu lintas data di jaringan komputer.
- Sniffing dibagi menjadi 2 bagian :
  - Passive Sniffing adalah suatu kegiatan penyadapan tanpa merubah data atau paket apapun dijaringan.
  - Active Sniffing adalah kegiatan sniffing yang dapat melakukan perubahan paket data dalam jaringan agar bisa melakukan sniffing.

MACAM-MACAM SERANGAN PADA JARINGAN LAN (2)

- Spoofing adalah Serangan yang dilakukan dengan cara berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya.

- Macam-Macam Spoofing :
  - 1.IP-Spoofing adalah Serangan teknis yang rumit yang terdiri dari beberapa komponen
  - DNS Spoofing adalah Mengambil nama DNS dari sistem lain dengan membahayakan domain name server suatu domain yang sah.
  - Identity Spoofing adalah Suatu tindakan penyusupan dengan menggunakan identitas resmi secara ilegal.

TEKNIK MENGAMANKAN PADA JARINGAN LAN (1)

- Ada beberapa teknik mengamankan jaringan LAN, yaitu dengan sebuah aplikasi atau software ataupun dengan menggunakan sebuah hardware.
- Sniffer Paket — dapat pula diartikan 'penyadap paket'. Sniffer paket dapat dimanfaatkan untuk hal-hal berikut:
  - Mengatasi permasalahan pada jaringan komputer.
  - Mendeteksi adanya penyelundup dalam jaringan (Network Intusion).
  - Memonitor penggunaan jaringan dan menyaring isi isi tertentu.
  - Memata-matai pengguna jaringan lain dan mengumpulkan informasi pribadi yang dimilikanya (misalkan password).
  - Dapat digunakan untuk Reverse Engineer pada jaringan.
- Software Sniffer Paket antara lain wireshark, kismet, Tcpdump, Cain & Abel, Ettercap, Dsniff, Kismac

TEKNIK MENGAMANKAN PADA JARINGAN LAN (2)

- Microsoft Security Essentials adalah program keamanan gratis oleh Microsoft. Hal ini khusus dirancang untuk menjaga terhadap virus, spyware, dan software jahat lainnya.
- VLAN (Virtual Local Area Nerwork) adalah Suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN, hal ini mengakibatkan suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan.

TEKNIK MENGAMANKAN PADA JARINGAN LAN (3)

- Firewall adalah suatu cara/sistem/mekanisme yang diterapkan baik terhadap hardware , software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar
- Port Security adalah port security adalah sebuah trafik kontrol yang bekerja di layer 2 data link. Berfungsi untuk mendaftarkan dan membatasi perangkat end devices mana saja yang dapat terkoneksi pada suatu port di switch tersebut.

KEAMANAN INTERNET/WEB

- Setiap harinya 30,000 website telah di retas
- Ratusan tool gratis tersedia di internet untuk digunakan meretas website
- 70% menyerang melalui web app
- Kelemahan Web

AMANKAH DENGAN FIREWALL?

Hanya mitos

Port tertutup

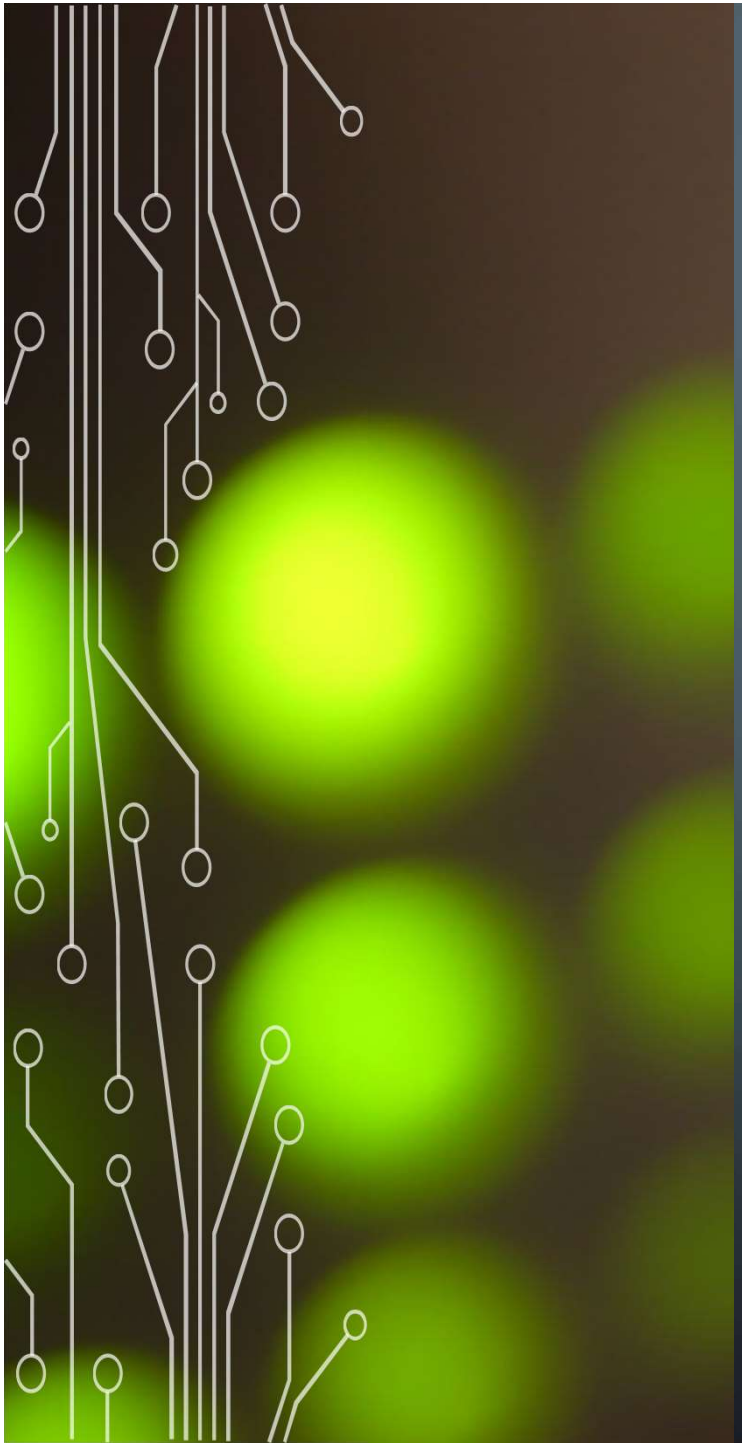
DAMPAK

- Dihapus/rusak
- Instal malware, botnet
- Diambil alih

Penyebabnya? Programmer yang kurang berpengalaman

BEBERAPA KELEMAHAN PADA WEB

- Injection (SQL)
- Otentikasi Rusak
- Terpaparnya Data Sensitif
- Entitas Eksternal XML
- Access Control Yang Lemah
- Kesalahan Konfigurasi Keamanan
- Cross Site Scripting (XSS)



CARA MELINDUNGI KEAMANAN WEB

- Dengan mengamankan coding, antara lain:
  - Validasi input
  - Attack Surface reduction

VALIDASI INPUT

- Jangan mempercayai user
- Menvalidasi data yang mereka input
- Mendeskripsikan secara eksplisit format input permintaan yang valid
- Buat blacklist validasi dan whitelist validasi

MENGKLASIFIKASIKAN DAN MEMPRIORITASKAN ANCAMAN

- STRIDE: threat Classification system (Microsoft)
- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial Of Service
- Elevation of Priviledge

ANCAMAN PASSWORD DALAM WEB

Brute Force

Dictionary Attack

PASSWORD YANG BAIK

- Minimum Password lebih Panjang misalkan 8 digit
- Terapkan Kompleksitas Kata Sandi
- Putar Password (90 Derajat)
- Keunikan Password
- Kata Sandi = username?
- Simpan password dengan benar

MENYIMPAN PASSWORD DALAM WEB

- Jangan simpan di Plaintext
- Gunakan Hash yang kuat
- SHA 256; SHA 512
- 5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721D1542D8
- Gunakan Salt

AUTENTIKASI DALAM WEB

Berbasis Password

Sistem Masuk Tunggal

Otentikasi Multi Faktor

Access protected resource

Session ID

AUTENTIKASI YANG AMAN

- SSL / TLS
- Penguncian Akun (jika login gagal)
  - Jumlah upaya
  - Jendela pengukuran
  - Periode Penguncian
- CAPTCHA (tes Turing publik yang sepenuhnya otomatis untuk membedakan Komputer & Manusia) - kekerasan
- Tidak ada akun Default
- Jangan menkredensial kode dengan keras
- Ingat dengan cookie kedaluwarsa

ACCESS CONTROL LIST

- Permission
- Read Write Execute

KEAMANAN EMAIL

Email:

- Sebuah pesan email umumnya terdiri dari 3 bagian yaitu: Header, Body dan signature.
- Email header berisi informasi tentang alamat pengirim, alamat penerima, informasi routing, waktu pengiriman, dan subjek email.
- Body adalah pesan yang dituliskan oleh pengirim. Selain itu attachment juga bagian dari body email. Dan bagian terakhir adalah signature (tanda tangan).

ANCAMAN TERHADAP EMAIL

- malicious email attachment
- malicious user redirection
- Phishing
- email hoax
- spam.

MALICIOUS EMAIL ATTACHMENT

- Attachment email yang berbahaya.
- Seringkali attachment digunakan untuk menyebarkan malware.
- Malicious user redirection adalah email yang berisi link atau tautan ke sebuah alamat web.
  - Tautan ini biasanya mengarahakan korban ke sebuah website yang berbahaya. Dikatakan berbahaya karena dengan mengunjungi web ini, komputer kita terinfeksi dengan malware.

MALICIOUS REDIRECTION

- Malicious redirection dibagi menjadi beberapa jenis:
  - referrer based
  - user agent based
  - cookie based
  - os based
- Sebaiknya berhati-hati bila menerima email yang mengandung link. Sebelum meng-klik link tersebut, sebaiknya discan dulu tautan tersebut dengan antivirus maupun URL scanner. Misalnya web virustatal.com.

PHISHING, HOAX DAN SCAM

- Teknik lainnya yang digunakan hacker adalah phishing. Email phishing biasanya digunakan untuk mencuri informasi akun password dll.
- Kemudian ada email hoax. Beberapa contoh email hoax bisa dilihat di web scamletters.com.
- Selanjutnya ada juga yang disebut Nigerian scam atau 419 scam. Email ini umumnya mengiming-imingi kita akan mendapat sejumlah uang yang banyak, tapi sebelumnya kita harus bayar dulu sejumlah uang.

SPAM

- Ancaman terakhir adalah email spam.
- Untuk mengatasi spam, saat ini telah ada berbagai tools anti spam. Misalnya ada SPAMfighter.

PENGAMANAN EMAIL

- Untuk mencegah hacking pada email:
  - Menggunakan password yang susah untuk dicrack.
  - Menggunakan teknik two-step authentication.
  - Saran lainnya adalah mematikan fitur keep signed in/remember me
  - Selalu gunakan halaman https
  - Menyediakan alamat recovery
  - Mematikan fitur preview email
  - Mengaktifkan fitur filtering email
  - Selalu melakukan scanning attachment dengan antivirus
  - Memeriksa fitur last account activity
  - Menggunakan enkripsi
  - Menggunakan digital signature.