TIS13534P KOMUNIKASI DAN KEAMANAN DATA

Minggu 12 – Keamanan Web

Apa itu Web?

- Sebuah sistem server internet yang mendukung dokumen atau data terformat. Dan tentu saja grafis, audio, atau media lainnya.
- Kita bisa menjelajahi data-data tersebut hanya dengan satu klik saja. Inilah yang disebut dengan surfing

Web Saat ini

- Karena kemudahannya, Web terus menerus dikembangkan. Dari yang awalnya yang cuma web statis, menjadi web super dinamis.
- Web statis hanya menampilkan teks-teks saja
- Web dinamis sudah mendukung banyak format sehingga terlihat lebih interaktif

Keamanan Web

- Web adalah salah satu objek jaringan yang paling rawan terkena serangan jaringan.
- Dikarenakan konfigurasi server yang kurang tepat, atau ada beberapa bagian dari konfigurasi yang tidak di set.
- Sehingga hal-hal tersebut menyebabkan web server menjadi rawan serangan.

Lokasi Rawan Serangan

- Sebagian dari Sistem Operasi itu sendiri
- Konfigurasi dari HTTP server yang membuat halaman menjadi rawan
- Konfigurasi dari Database juga yang mengizinkan sembarang orang dapat masuk dengan mudah

Apa Motivasi Penyerang?

- Demi keuntungan finansial - Penipuan, pencurian, dan penjualan data pribadi
- Menganggu - mencegah ornag lain mengakses sistem, menyebarkan informasi palsu
- Pingin terkenal - Mengakses lubang keamanan yang sangat sulit untuk diakses

Mengapa Web Menjadi Target

- Kalah popularitas dikarenakan persaingan yang tidak seimbang.
- Politik/Protes dikarenakan ketidaksukaan masyarakat tertentu akan kebijakan yang diterapkan pemerintah
- Pekerja yang kecewa, dikarenakan kekecewaan yang dirasakan pekerja internal

Serangan Web

- Menggunakan **injeksi SQL** untuk mendapatkan akses database, memalsukan identitas pengguna, dan tentu saja mengubah/merusak database. Bahkan pencurian data kartu kredit pengguna.
- Menggunakan **Cross-Site Scripting (XSS)** untuk mengirim kode mencurigakan ke user pengguna lain dari pengguna website dengan memasukkan kode ke dalam aplikasi lalu dieksekusi di klien.
- Membuat web menjadi tidak mudah diakses dikarenakan serangan **Distributed Denial of Service Attacks (DDoS)**. DDoS membuat erpmintaan dari ribuan alamat IP dan mencoba membanjiri suatu website.
- Mengambil alih sesi user terpercaya dan membuat pembelian oline atas nama pengguna tersebut dengan menggunakan **Cross Site Request Forgery (CSRF).**

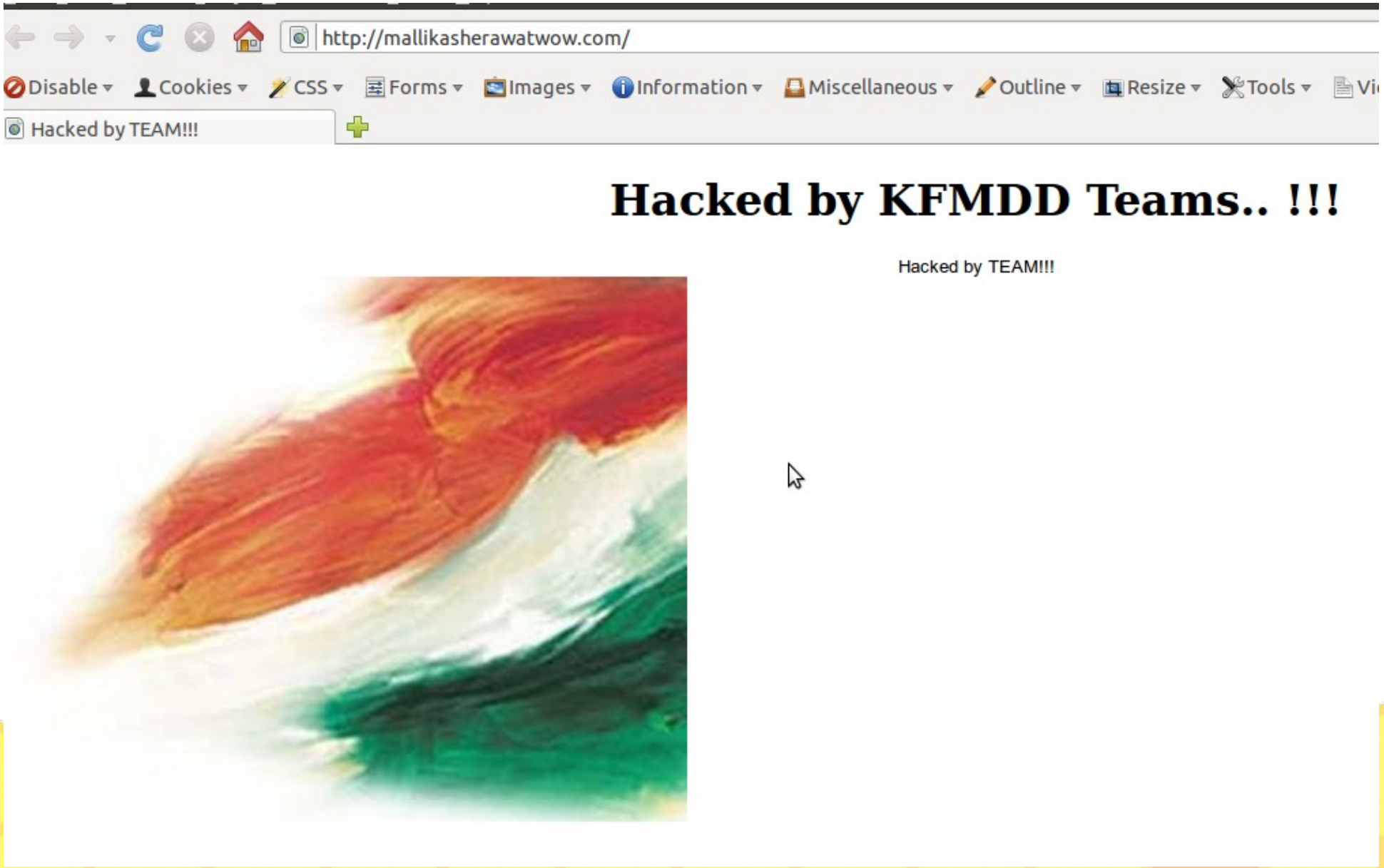
Akibat Dari Serangan

- Akun Root terambil alih (kerahasiaan)
  - Efek kerusakan bisa fatal
- Halaman database yang berubah (integrity: deface)
  - Tergantung dari berapa banyak halaman yang diubah
- Server menjadi susah diakses (availability)
  - Bisa diatasi dengan menutup port dan restart server

Web Deface

- Sebuah perbuatan mengubah tampilan sebuah halaman web tanpa izin dari pemilik situs
- Bertujuan sebagai cara menampilkan protes, kejahilan, atau merusak image dari situs yang dirubah
- Penyerang harus memiliki akses up-down file sebelum melakukan web deface

Contoh Web Deface

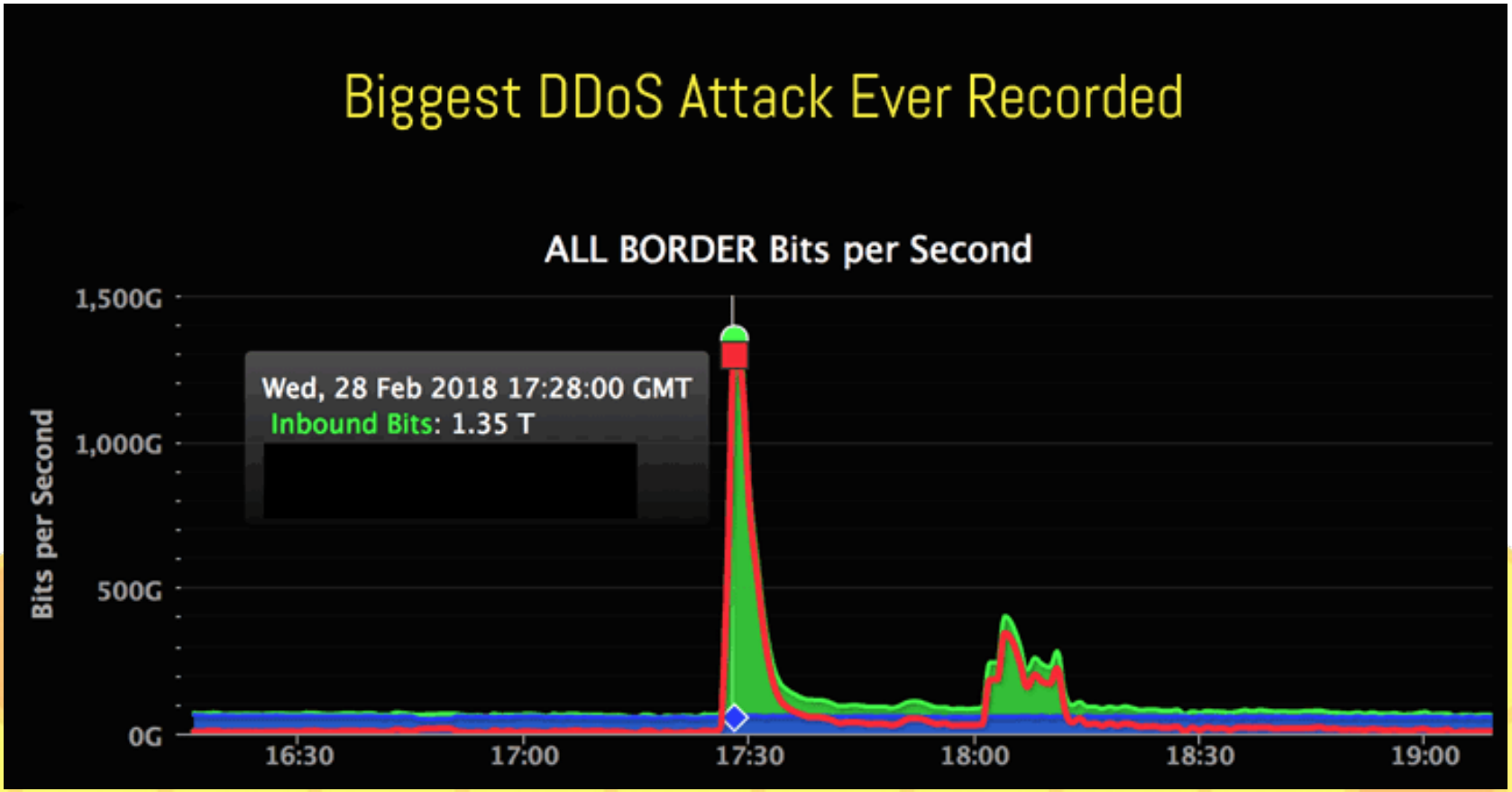


DDoS Web (Availability)

- Serangan request paket dari penyerang ke web server dalam jumlah besar dan berukuran yang berbeda-beda
- Bertujuan membuat server down, dan tidak bisa diakses orang lain.

DDoS Terbesar

- Di bulan Februari 2018, GitHub sebuah situs repositori kode terkena DDoS berukuran 1.35Tbs (Terabit second)



DDoS

- Penyerang menggunakan MemCached server untuk memperkuat serangan hingga 51ribu kali!
- Serangan ini menggunakan port UDP 11211 sebagai lubang penyerangan
- Serangan ini cukup dipicu dengan beberapa byte paket, namun dapat memicu ribuan lebih paket

- https://thehackernews.com/2018/03/biggest-ddos-attack-github.html

Injeksi SQL

- Serangan ini ditargetkan ke Database website dengan menggunakan perintah-perintah dalam SQL
- Sehingga penyerang bisa mendapatkan akses root/admin dari database tersebut dan dapat mencuri/merusak data yang ada

Cara Kerja Injeksi SQL

kondisi normal :

Select * from admin where username = input_username And password = input_password

Select * from admin where username = ‘administrator’ and Password = ‘admin’

Dapat dipastikan bahwa apabila field username terdapat record administrator dengan filed password terdapat admin penulis dapat melewati proteksi dan masuk kehalaman berikutnya ,akan tetapi apabila sebaliknya ,maka akan keluar pesan kesalahan yang kurang lebih isinya kita tidak bisa masuk ke halaman berikutnya

Cara Kerja Injeksi SQL

Select * from admin where username = ‘’ or ‘’ = ‘’ and Password = ‘’ or ‘’=”

Logika OR menyebabkan statement membalikan nilai false jadi true sehingga kita bisa masuk sebagai user yang terdapat pada record pertama dalam table admin

misalkan username = administrator , caranya cukupsederhana , pada textbox tempat menginput username isi dengan “administrator’—“

Select * from admin where username = ‘ administrator ‘—“

And password = ‘’ or ‘’=”

Tanda “—“ (dua tanda minus) di sql server berarti akhir dari statement sql.

Variabel Yang Bisa Dipakai

or 1=1--	" or 0=0 #	" or "a"="a
" or 1=1--	Or 0=0 #	') or ('a'='a
or 1=1--	' or 'x'='x	") or ("a"="a
' or 'a'='a	" or "x"="x	hi" or "a"="a
" or "a"="a	') or ('x'='x	hi" or 1=1 --
') or ('a'='a	' or 1=1--	hi' or 1=1 --
' or 0=0 --	" or 1=1--	hi' or 'a'='a
" or 0=0 --	or 1=1--	hi') or ('a'='a
or 0=0 --		hi") or ("a"="a
' or 0=0 #		‘or a=a--

Cara Mengatasi

- Melakukan pemblokiran perintah-perintah tertentu menggunakan SQL Query
- $aforbidden = array **(**
- "insert", "select", "update", "delete", "truncate",
- "replace", "drop", " or ", ";", "#", "--", "=" **)**;

Cross Site Scripting (XSS)

- Cross Site Scripting Suatu Jenis Serangan dengan cara memasukkan code/script HTML (javascript) kedalam suatu web site dan dijalankan melalui browser di client
- Contoh
- <FORM action=http://sembiring/admin/login.asp method=post>
- <input type=hidden name=A value="test' or 1=1--">
- </FORM>
- Apabila beruntung kita membuka page tersebut tidak perlu memasukan password dan username.

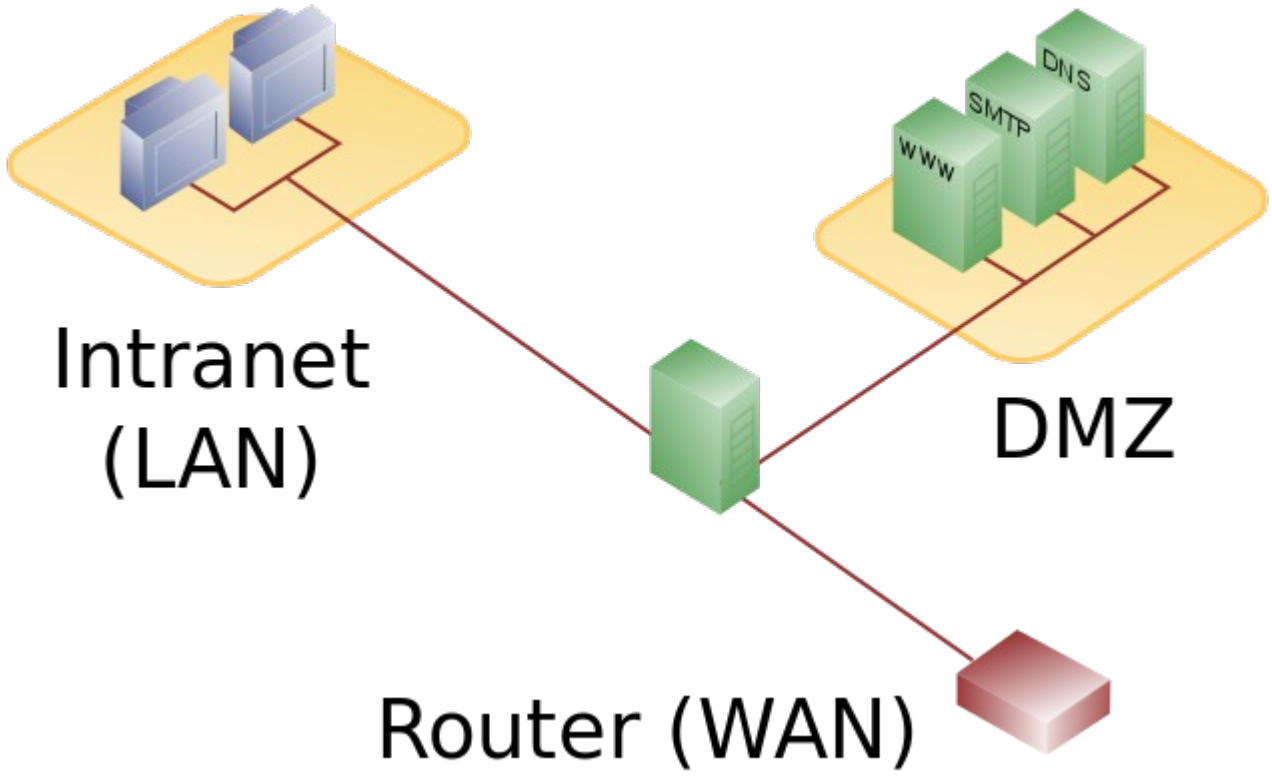
Pengamanan

- Tidak ada system yang 100 % Aman
- Gunakan Input Validation yang baik
- Setting at PHP.INI
- - Matikan error_log pada PHP
- - Disable Fungsi passthru, exec dan system pada phpallow_url_fopen = Off
- - Safe_mode = On
- - Sesuaikan dengan kebutuhan ! Selalu Update Patch terbaru untuk web server
- - Selalu Update Info

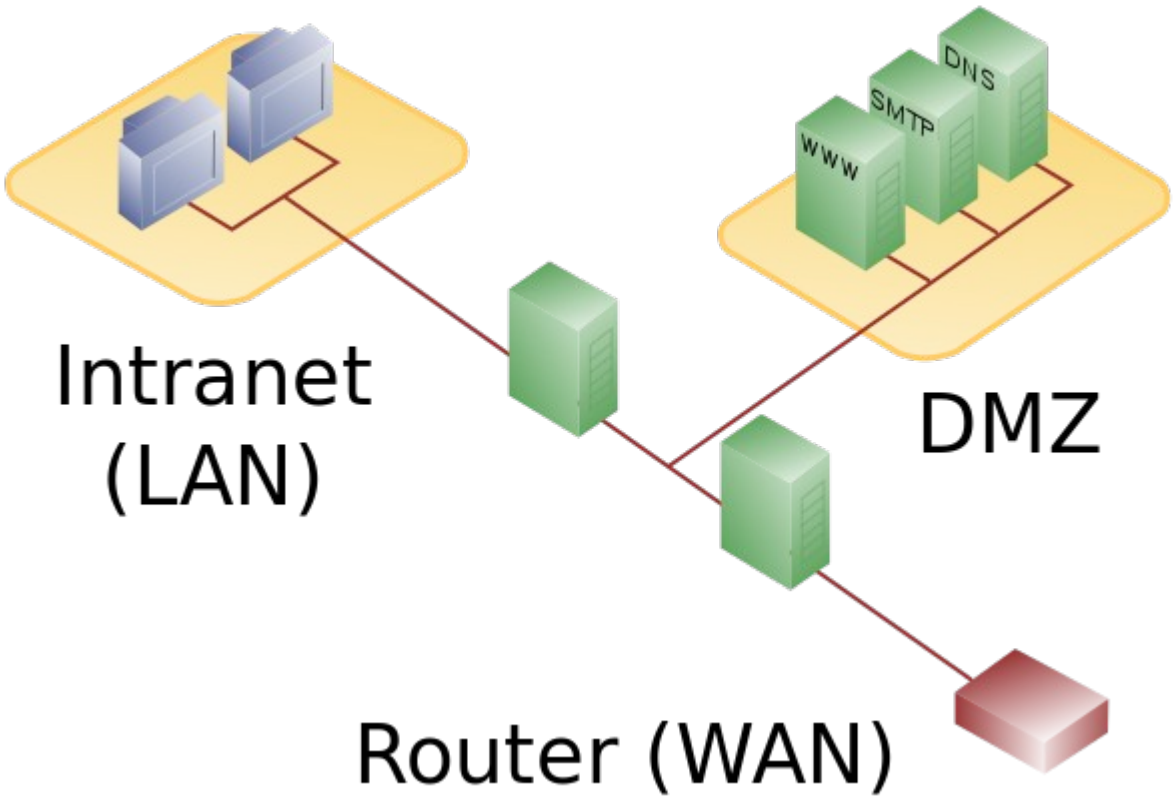
DMZ dan Web Server

- De-Militarized Zone adalah sebuah zona perbatasan di mana perangkat yang ada di sini terbuka terhadap internet luar yang tidak terpercaya
- Web Server diletakkan di area ini agar semua orang bisa mengakses server ini

DMZ 1 Firewall



DMZ 2 Firewall



Cont’d

- Selain web server, VOIP, FTP server, Mail server harus ditempatkan di DMZ
- DB server diletakkan di jaringan internal DMZ agar terlindungi dari serangan luar, selain itu DB server memiliki data yang sangat sensitif sehingga harus dilindungi

HTTPS dan SSL

- Menggunakan HTTPS dan SSL berarti koneksi antara pengguna dan server akan di enkripsi
- Diperlukan sertifikat digital yang dibuat oleh pihak-pihak tertentu sehingga website bisa dianggap terpercaya
- Hindari website yang TIDAK menggunakan HTTPS, lihat disebelah kiri URL

Peningkatan Keamanan

- Gunakan SSH dengan kunci bukan password
- Blok port yang digunakan untuk MySQL (port 3306)
- Gunakan Secure Socket Layer/TLS
- Matikan Service OS yang tidak perlu
- Melakukan Audit File System (akses permission)

Gunakan Virtualisasi

- Ketika kita akan melakukan hosting web, kita akan diberikan pilihan berupa Virtual Hosting, atau Real Hosting
- Dengan menggunakan Virtual Hosting, file-file utama di sistem operasi kita akan aman dari jangkauan orang lain

Keamanan DB

- Demi keamanan, Database dianjurkan untuk di backup setiap waktu. Ada satu cara yang sangat manjur, yaitu DB replication/DB mirror.
- Di mana terdapat dua database utama, yaitu DB Master dan DB Slave.
- Tergantung dari konfigurasi, kedua database ini bisa saling membantu ketika terjadi kerusakan

Kuis

1) Terdapat 2 model IPSec yang bisa digunakan untuk VPN. Jelaskan 2 model tersebut
2) Ilustrasikan paket IPv4 dan IPv6 ketika VPN IPSec aktif
3) Jelaskan apa itu e-mail spoofing, e-mail spamming, dan e-mail bombing!
4) Jelaskan mengapa dua firewall di lingkungan DMZ lebih aman daripada satu firewall?