

# Tugas Kuliah Keamanan Jaringan

Mencari informasi nama pemilik atau pendaftar dari suatu *domain*, *name server*, *mail server* dan *subdomain* pada level tertentu.

Pencarian informasi ini murni ditujukan untuk kepentingan akademis, sehingga tidak akan digunakan untuk kepentingan lain yang dapat merugikan pihak lain. Metode pencarian informasi akan dilaksanakan dengan menggunakan *tools* yang ada di internet, yaitu *who is*, *mx-record*, serta *zone transfer*. Pencarian informasi tentang nama pemilik atau pendaftar dari suatu *domain*, *name server*, *mail server* dan *subdomain* dapat dilakukan dengan menggunakan beberapa metode. Metode yang paling sederhana adalah dengan menggunakan fasilitas yang ada di internet. Berikut saya sampaikan beberapa pengertian dan penyedia fasilitas layanan untuk mendapatkan berbagai informasi tersebut.

## **WHO IS**

Whois adalah *query* dan respon protokol yang secara luas digunakan untuk melakukan *querying* (pencarian) database yang menyimpan user atau perwakilan yang terdaftar sebagai pengguna Internet resources seperti nama domain, alamat IP atau *autonomous system* dan juga untuk informasi tambahan yang lain. Beberapa laman website yang menyediakan layanan tersebut adalah [whois.domaintools.com](http://whois.domaintools.com) dan [www.magic-net.info](http://www.magic-net.info).

## **MX RECORD**

*MX Record* atau *A Mail eXchanger Record* adalah tipe dari *record resource* dalam DNS yang menspesifikasikan *mail server* yang bertugas untuk menerima email atas nama domain penerima dan preferensi nilai yang digunakan untuk memprioritaskan pengiriman mail jika *server mail* yang tersedia lebih dari satu. *MX Record* dari domain ini digunakan untuk menspesifikasi bagaimana email di routingkan dengan *Simple Mail Transfer Protocol* (SMTP). Laman website yang dapat membantu kita untuk menemukan informasi tersebut adalah [www.magic-net.info](http://www.magic-net.info) dan [www.mxtoolbox.com](http://www.mxtoolbox.com).

## **ZONE TRANSFER**

*Zone transfer* adalah salah satu jenis tipe transaksi pada DNS yang merupakan mekanisme yang tersedia bagi *administrator* untuk melakukan mereplikasi *database* yang berisi data DNS di satu set server DNS. Penerapan *Zone transfer* tugas kali ini ini adalah untuk mendapatkan *subdomain* level 4 pada domain yang dicari. Sebagai catatan, dari segi keamanan jaringan, seharusnya *zone transfer* tidak bisa dilakukan. Biasanya untuk dapat melakukan hal tersebut, seseorang harus mempunyai legalitas untuk akses atau menggunakan jaringan internal yang ada di organisasi tersebut.

Tools yang dapat digunakan adalah [www.magic-net.info](http://www.magic-net.info) atau *nslookup* yang tersedia di hampir seluruh OS. Langkah-langkahnya adalah sebagai berikut:

Ketik **nslookup**, kemudian akan tersambung ke name server ns1.x.edu.

Ketik **ls -d x.edu**. untuk menampilkan keseluruhan tipe subdomain.

Hasil keluarannya dapat langsung berbentuk file dengan mengetikkan **ls -d x.edu > "nama\_file".format file**, contoh: **ls -d x.edu > dns.txt**.

Pada pencarian yang harus dicari sbb :

1. Pemilik Domain
2. Name Server
3. MX Record
4. Zone Transfer