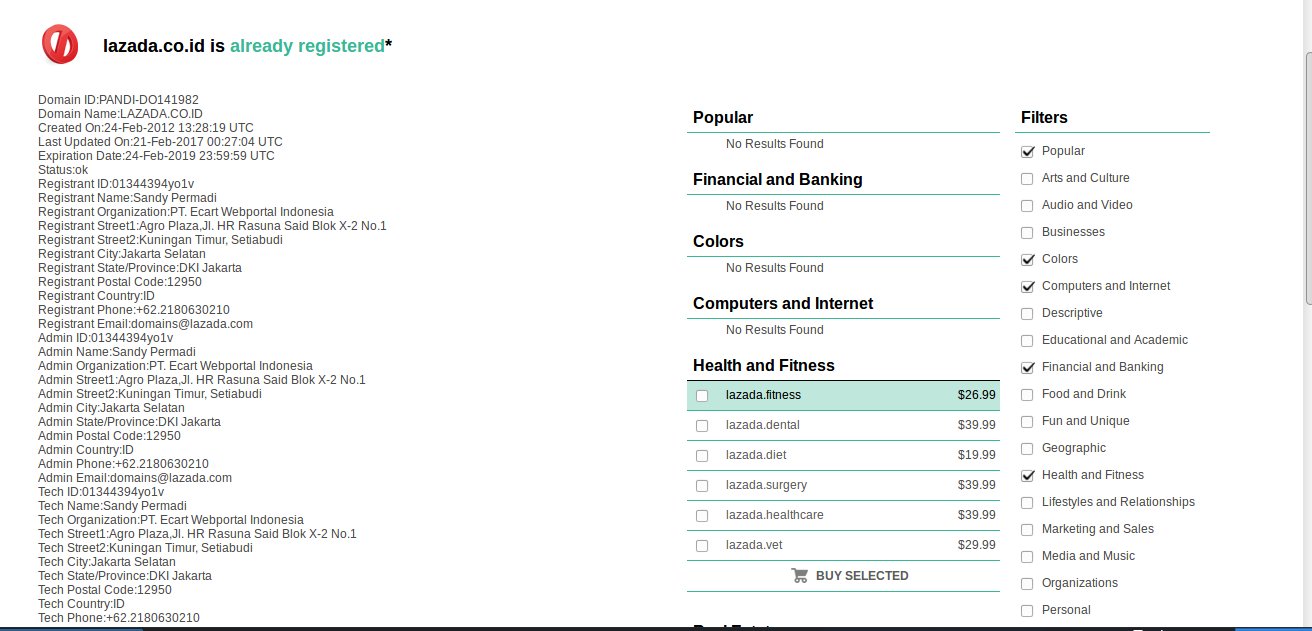
**Hasil Reconnaissance website lazada.co.id**

Sebelumnya saya akan menjelasakan pengertian reconnaissance, yang mana reconnaissance ini merupakan sebuah fase dalam persiapan sebelum attacker atau sebelum hacker/ penyerang melakulkan penyerangan yang mana kegiatan initinya adalah mengumpulkan informasi sebanyak mungkin mengenai sasaran yang akan mereka hadapi atau lakukan. Reconnaissance dibagi menjadi 2 yaitu active reconnaissance dan passif reconnaissance. Active reconnaissance merupakan pengumpulan data dengan cara bertatapan muka langsung atau terhubung secara langsung dengan sasaran sedangakan pasive reconnaissancemerupakan menggunakan media informasi seperti berita, internet dan lain-lainya. Yang mana langkah reconnaissance adalah sebagai berikut:

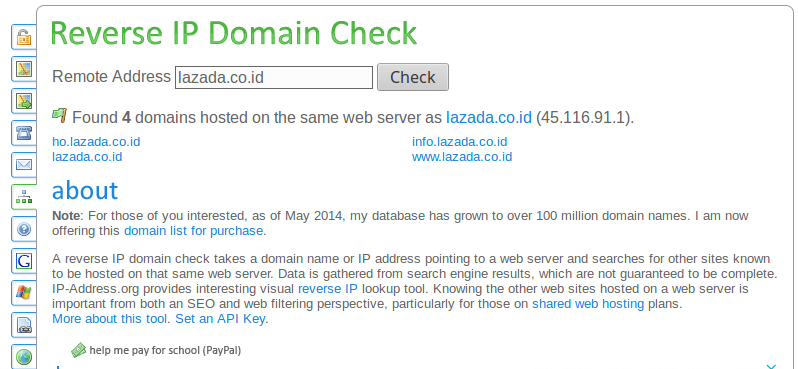
1. whois

Tahapan whois ini digunakan untuk mendapatkan data atau informasi dari domain yang akan kita reconnaissance sehingga informasi yang didapatkan seperti nama pemilik domain, ip address, nama server dan umur domain. Gambar dibawah ini merupakan hasil whois dari website lazada.co.id yang saya dapatkan adalah sebagai berikut:

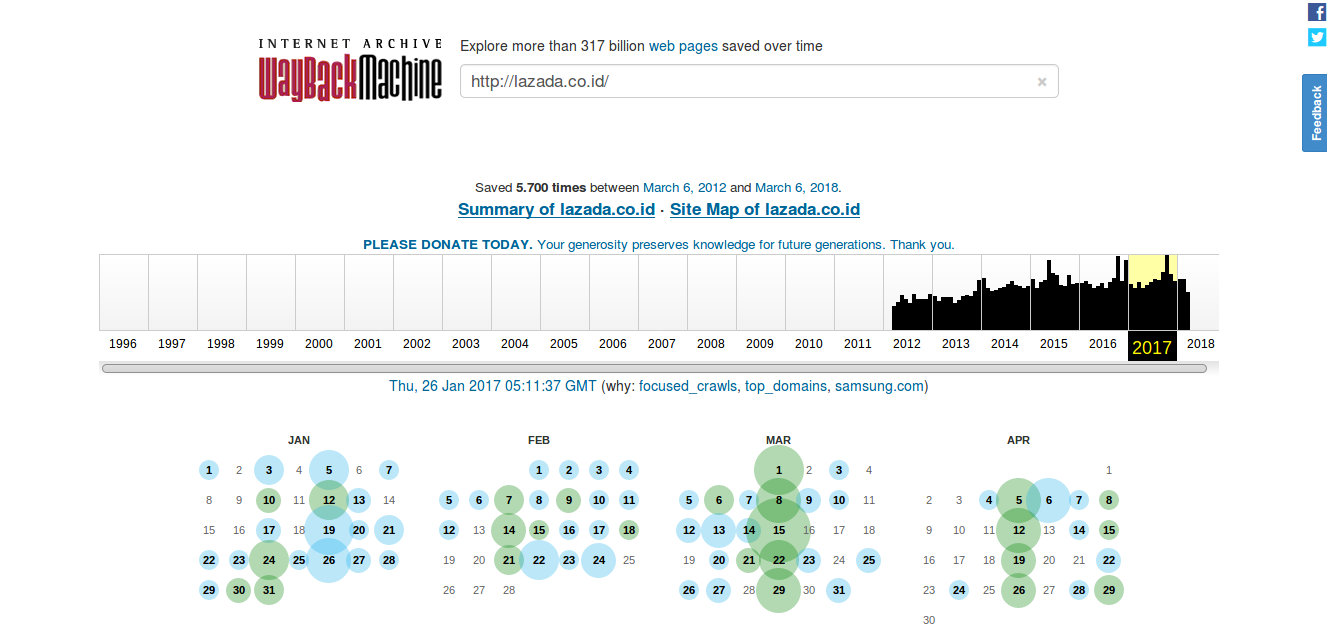


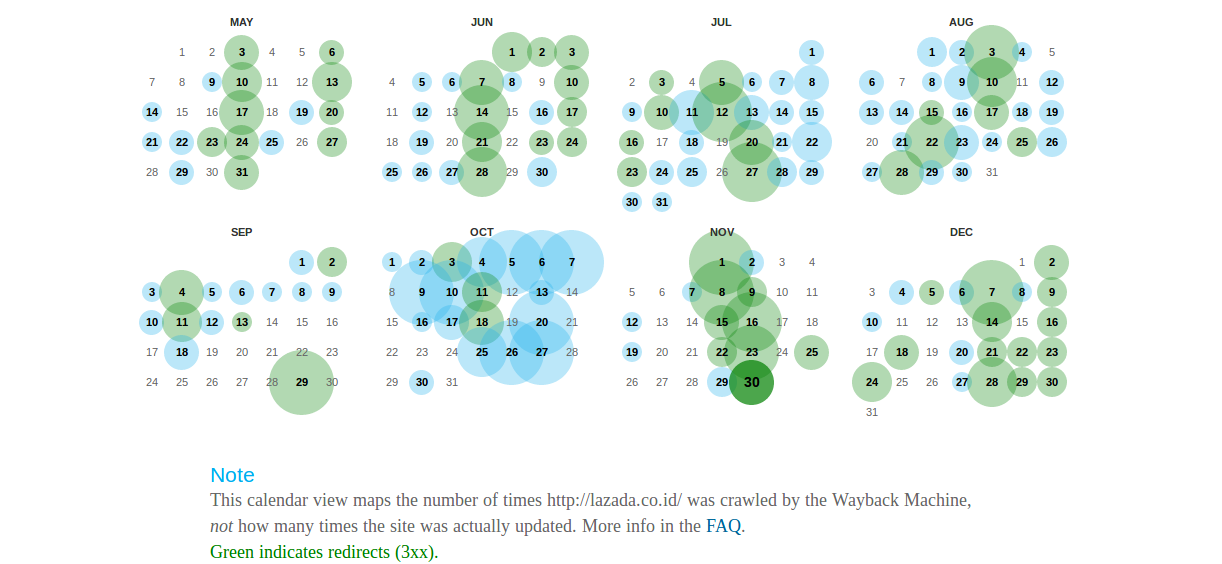
Jika kita lihat hasil dari screenshot diatas terdapat informasi yang sangat penting yang bisa dimanfaat oleh para hacker atau penyerang karena dalam data tersebut terdapat nomer phone, email dan alamat yang mana bisa dimanfaatkan untuk melakukan social engineering, salah satu kasus yang terjadi adalah pada tahun 2015 yang menimpa ID-SIRTII yang mana web portalnya kena serangan DNS Hijacking yang mana penyerang memanfaatkan informasi dari whois untuk melakukan social engineering ke penyedia layanan dns.

1. **Hasil Reverse Ip ke domain**



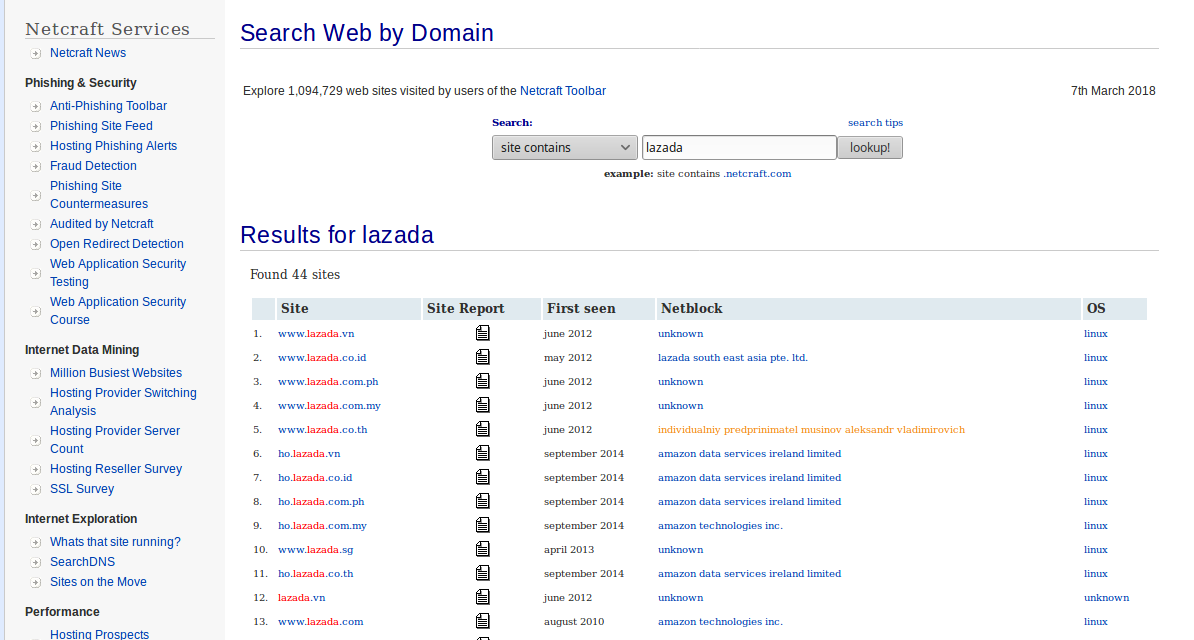
Jika kita lihat hasil reverse IP ke domain yang terdapat pada gambar diatas menunjukan bahwa domain lazada.co.id ini bukanlah satu-satunya domain yang hostnya disatu web server melainkan ada 4 domain yang berbeda, sebenarnya hal seperti ini lah yang dapat membahayakan apabila layanan website tersebut mempunyai informasi yang penting, karena penyerang bisa saja masuk kedalam sistem dengan melakukan jumping dari website lain yang mempunyai celah.





Dari gambar diatas menunjukan bahwa website lazada.co.id ini pertama kali online 6 maret 2012 dan webtool lazada.co.id pun telah banyak merekam aktivitas atau jejak yang dilakukan oleh lazada itu sendiri yang mana informasi tersebut bisa dimanfaatkan hacker untuk melakukan hal-hal yang dapat merugikan. Data penting itulah yang bisa dimanfaatkan oleh para hacker meskipun data atau informasi tersbut telah dihapus website lazada.co.id.

1. **Netcraf lazada**

****

****

Netcraft menunjukan bulan dan tahun mulai muncul lazada di beberapa negara dan menunjukan operanting system dengan menggunakan linux, sehingga memeberikan informasi yang berkaitan dengan domain yang dapat dijadikan sebagai target sehingga dengan informasi tersebut dapat dijadikan sebagai acuan untuk melakukan pengintaian terhadap website tersebut.