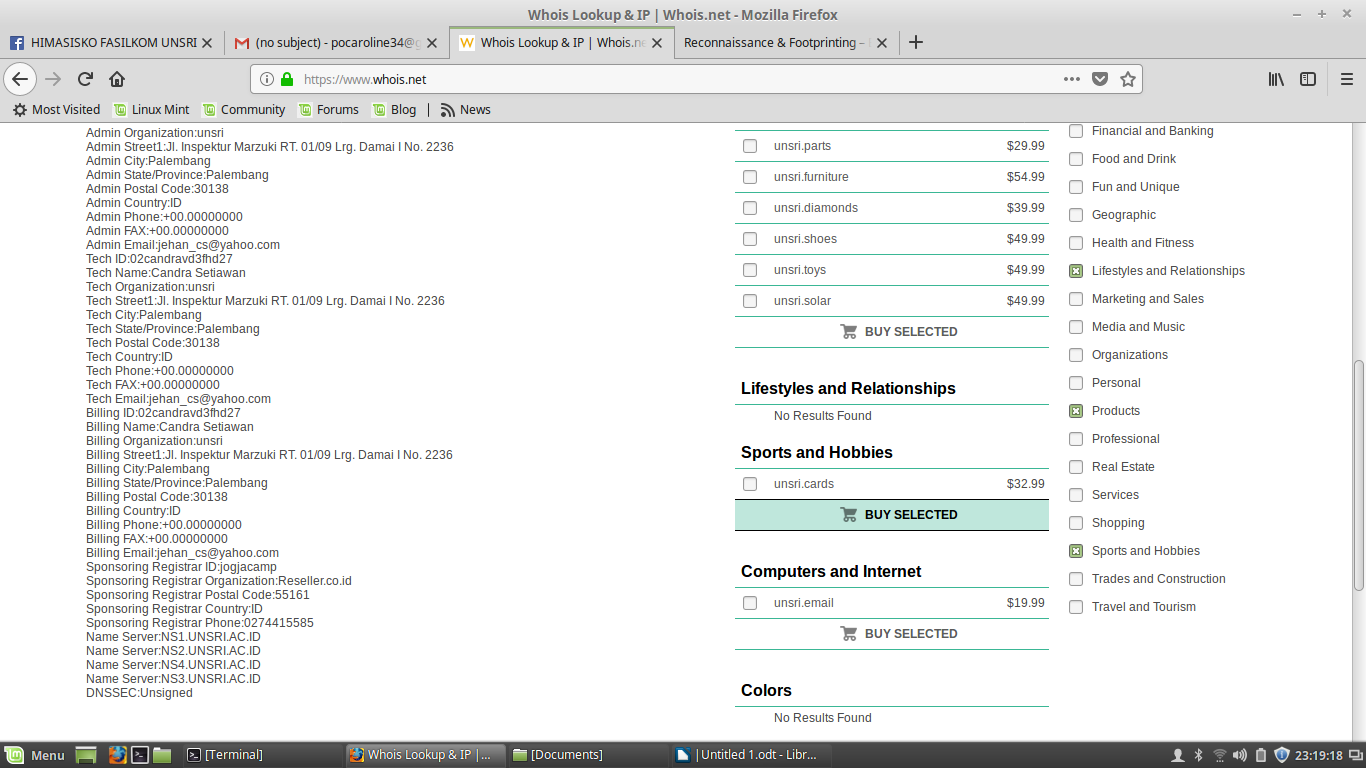
**Reconnaissance unsri.ac.id**

Reconnaisance adalah fase persiapan sebelum attacker melakukan penyerangan dimana mengumpulkan informasi sebanyak-banyaknya mengenai sasaran dan teknik ini menyertakan network scanning baik melalui jaringan internat atau external tanpa ijin.

**Whois**

whois digunakan oleh attacker untuk mendapatkan informasi dari suatu domain. Fungsi dari whois ini untuk mengetahui data-data info pemilik secara rinci dan informasi kapan expirednya suatu domain. Contohnya sebagai berikut :



**whatweb**

whatweb digunakan untuk mengetahui teknologi web apa yang digunakan suatu domain termasuk platform blogging, Content management system (CMS), web server, javascript library, perangkat yang diembedded dan paket statik/analistik. Contoh sebagai berikut:

http://unsri.ac.id [302] Cookies[PHPSESSID],

Email[yadiutama@unsri.ac.id],

HTTPServer[nginx], (WEB SERVER)

IP[103.241.4.11], (“IP UNSRI.AC.ID”)

JQuery[1.2.6],

Meta-Author[yadiutama@unsri.ac.id],

PHP[5.3.10-1ubuntu3.25], (PHP DAN SISTEM OPERASI YANG DIGUNAKAN)

PasswordField[password],

RedirectLocation[http://www.unsri.ac.id/],

Script[text/javascript],

Title[.:: Halaman Utama | Universitas Sriwijaya - Indralaya, Sumatera Selatan],

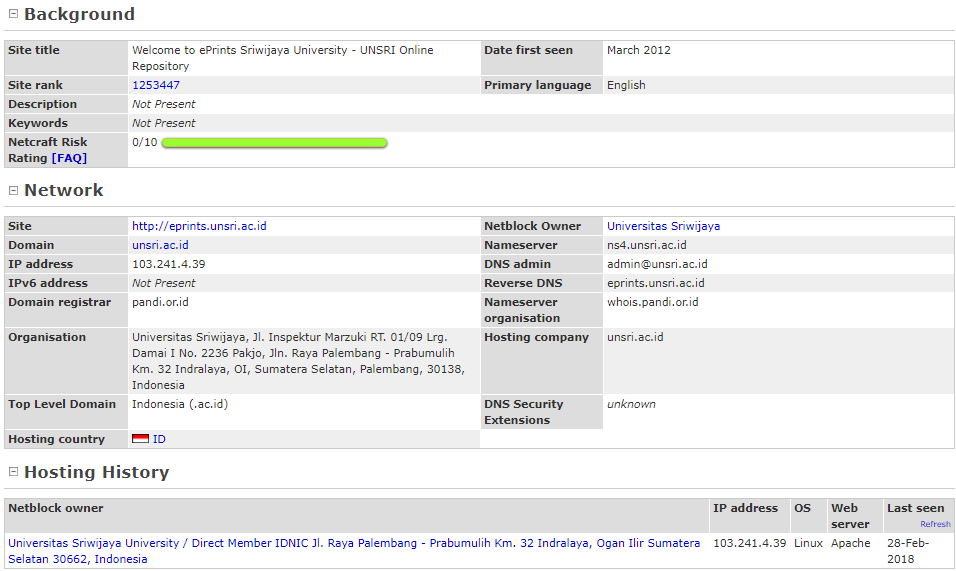
X-Powered-By[PHP/5.3.10-1ubuntu3.25],

nginx

**Netcraft.com**

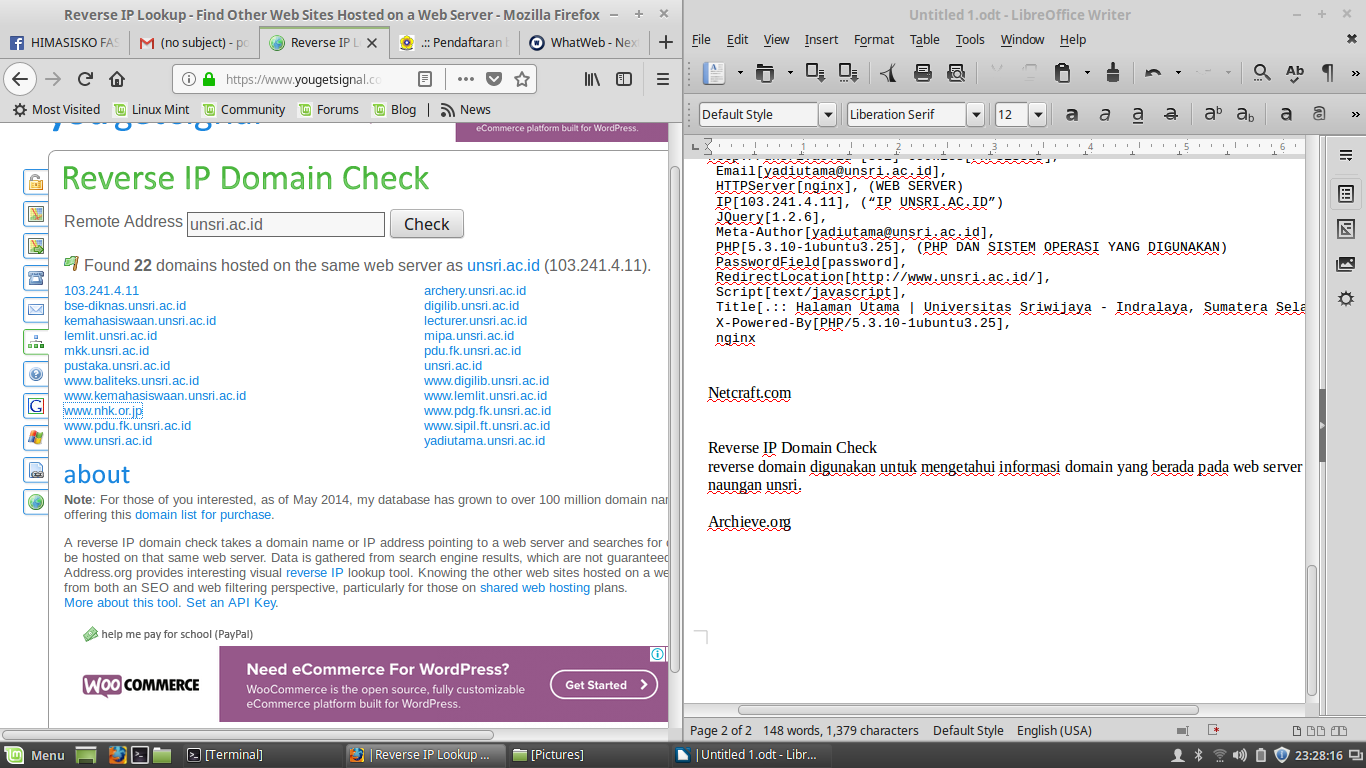
Digunakan untuk mendapatkan informasi mengenai unsri.ac.id seperti alamat IP, Name server, webserver, dan OS yang dipakai.





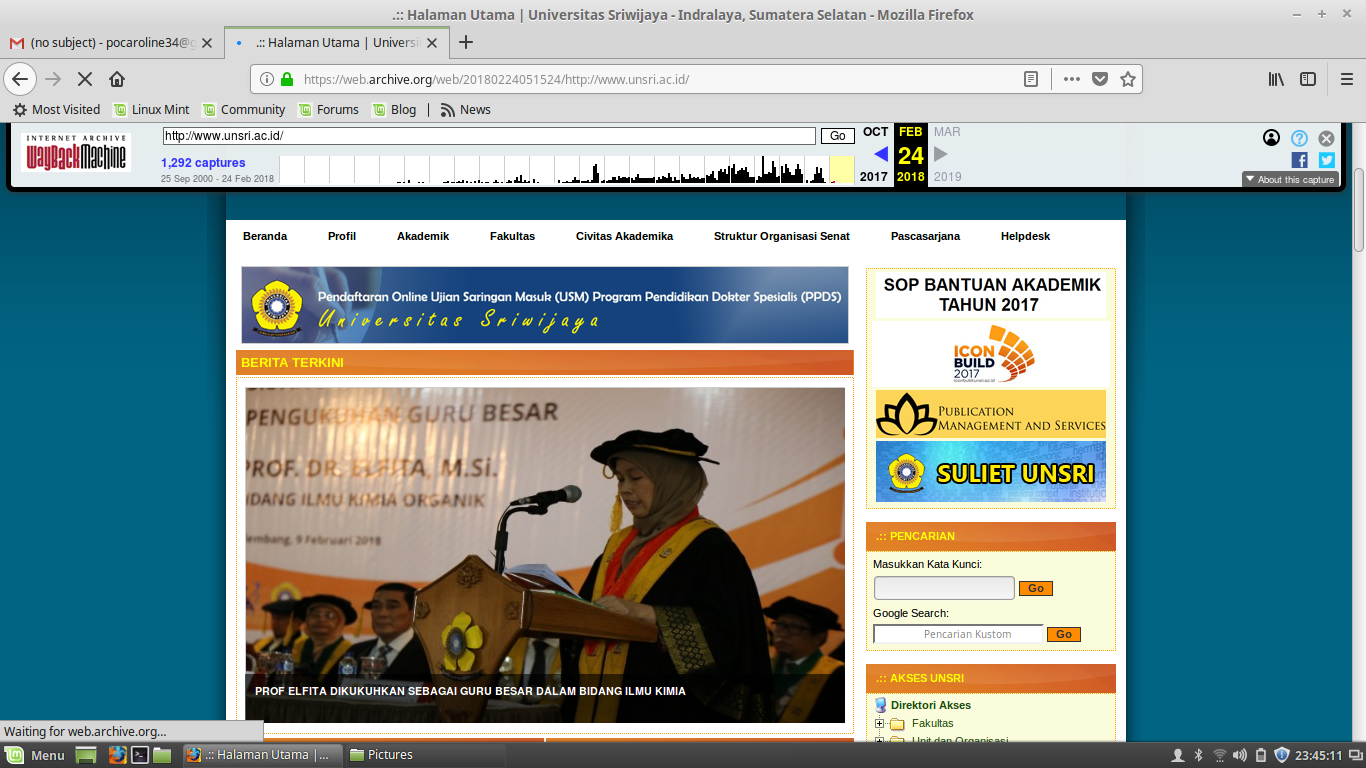
**Reverse IP Domain Check**

reverse domain digunakan untuk mengetahui informasi domain yang berada pada web server naungan unsri.



**Archieve.org**

archieve.org digunakan untuk melihat jejak rekam website yang telah disnapshot oleh archieve pada kurun-kurun waktu tertentu. Gambar berikut jejak rekam website unsri.ac.id pada tahun 2008



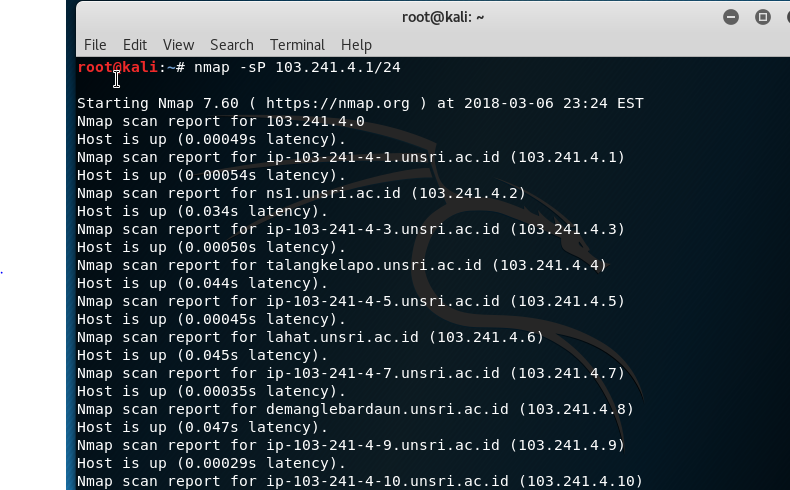
**Scanning Network**

Tahap pertama yang dilakukan adalah menggunakan nmap lalu masukan command

Nmap –sP (alamat Ip/subnet)

Untuk contoh kasus dibawah ini adalah

Nmap –sP 103.241.4.1/24

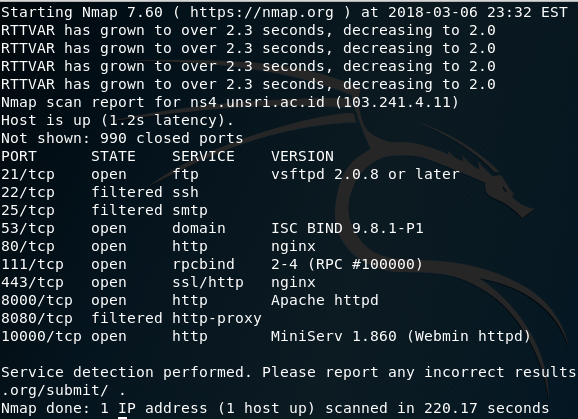


Hasil yang didapatkan adalah memperhatikan beberapa domain yang memiliki celah

**Scanning Port**

Lakukan scanning port dengan cara

Nmap –sV 103.241.4.11



Scanning port digunakan untuk melihat port apa yang terbuka pada alamat IP berikut

**Scanning OS**

Lakukan command sebagai berikut

Nmap –O 103.241.4.11



Gambar diatas menunjukan bahwa OS yang digunakan pada alamt IP tersebut namun hasil scanning menunjukan berbeda-beda pada setiap scanning namun dapat dikira-kira dengan melihat persentase terbesarnya.