Vicko Bhayyu

09011181520036

**Reconnaissance website Universitas Sriwijaya (unsri.ac.id)**

Reconnaisance atau biasa disebut footprinting adalah situasi yang dilakukan oleh seorang hacker sebelum melakukan penyerangan, dengan mencari informasi sebanyak mungkin mengenai target serangan.

* Whois.com

Whois digunakan untuk oleh penyerang untuk mendapatkan informasi domain tertentu seperti nama pemilik domain, name server, dan kapan domain itu expired.

Dari sini didapat informasi mengenai website unsri.ac.id, sebagai berikut:

Domain ID:PANDI-DO228145

Domain Name:UNSRI.AC.ID

Created On:01-Sep-1999 13:32:27 UTC

Last Updated On:15-Oct-2017 22:57:10 UTC

Expiration Date:31-Oct-2019 23:59:59 UTC

Status:clientTransferProhibited

Status:serverTransferProhibited

Registrant ID:candr12

Registrant Name:Candra Setiawan

Registrant Organization:Universitas Sriwijaya

Registrant Street1:Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236 Pakjo

Registrant Street2:Jln. Raya Palembang - Prabumulih Km. 32 Indralaya, OI, Sumatera Selatan

Registrant City:Palembang

Registrant State/Province:Sumatra Selatan

Registrant Postal Code:30138

Registrant Country:ID

Registrant Phone:+62.8194858899

Registrant Email:email@yahoo.com

Admin ID:02candravd3fhd27

Admin Name:Candra Setiawan

Admin Organization:unsri

Admin Street1:Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236

Admin City:Palembang

Admin State/Province:Palembang

Admin Postal Code:30138

Admin Country:ID

Admin Phone:+00.00000000

Admin FAX:+00.00000000

Admin Email:email@yahoo.com

Tech ID:02candravd3fhd27

Tech Name:Candra Setiawan

Tech Organization:unsri

Tech Street1:Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236

Tech City:Palembang

Tech State/Province:Palembang

Tech Postal Code:30138

Tech Country:ID

Tech Phone:+00.00000000

Tech FAX:+00.00000000

Tech Email:email@yahoo.com

Billing ID:02candravd3fhd27

Billing Name:Candra Setiawan

Billing Organization:unsri

Billing Street1:Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236

Billing City:Palembang

Billing State/Province:Palembang

Billing Postal Code:30138

Billing Country:ID

Billing Phone:+00.00000000

Billing FAX:+00.00000000

Billing Email:email@yahoo.com

Sponsoring Registrar ID:jogjacamp

Sponsoring Registrar Organization:Reseller.co.id

Sponsoring Registrar Postal Code:55161

Sponsoring Registrar Country:ID

Sponsoring Registrar Phone:0274415585

Name Server:NS1.UNSRI.AC.ID

Name Server:NS2.UNSRI.AC.ID

Name Server:NS4.UNSRI.AC.ID

Name Server:NS3.UNSRI.AC.ID

DNSSEC:Unsigned

Dari sini penyerang mendapatkan informasi data-data dari pemilik domain seperti nama,alamat, email, nomor telepon ,dll. Dan mendapatkan informasi kapan expired-nya website unsri.ac.id.

Dalam kasus pertama, bisa saja penyerang merebut domain unsri.ac.id jika web administrator unsri.ac.id lupa ataupun telat memperbaharui masa aktif domain. Jika hal tersebut terjadi maka domain unsri.ac.id akan berpindah tangan pemilik.

Dalam kasus kedua, penyerang dapat melakukan social engineering ke penyedia layanan DNS terhadap informasi data pemilik domain seperti nama , alamat, email, nomor telepon sang pemilik domain.

* Whatweb.net

Informasi yang bisa didapat pada whatweb antara lain :

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

Email[yadiutama@unsri.ac.id],

HTTPServer[nginx],

IP[103.241.4.11],

JQuery[1.2.6],

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

PHP[5.3.10-1ubuntu3.25],

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

Penyerang dapat memanfaatkan informasi mengenai IP Address unsri.ac.id yakni 103.241.4.11 , server menggunakan nginx, serta versi PHP yang digunakan yakni 5.3.10-1ubuntu3.25.

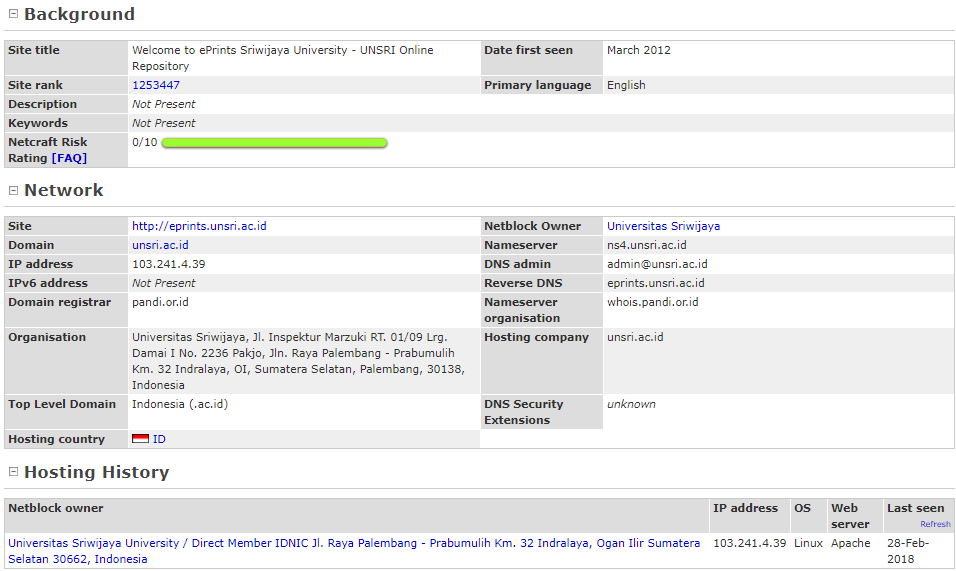
* Netcraft.com

Dari netcraft.com didapat informasi mengenai website yang berhubungan dengan unsri.ac.id



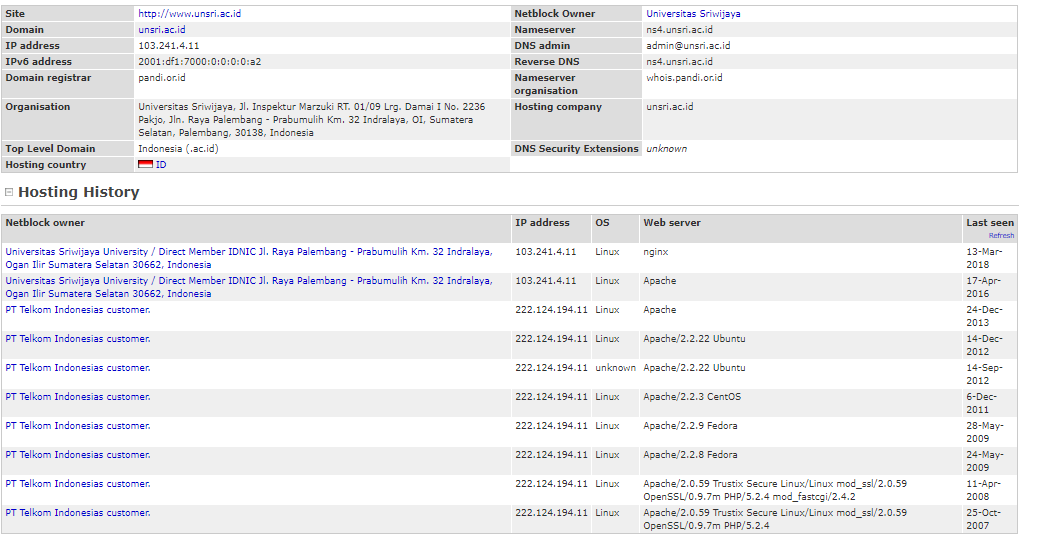
Terdapat 3 site yang berhubungan dengan unsri.ac.id

Eprints.unsri.ac.id



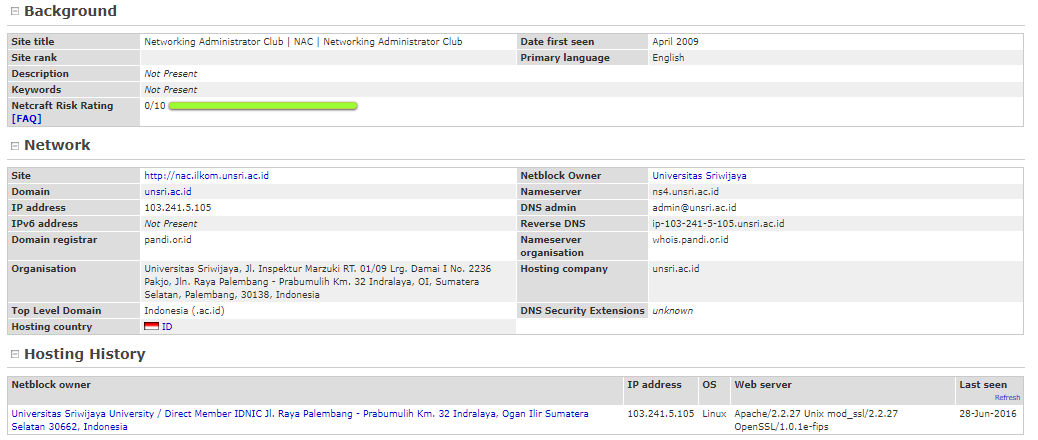
Didapat informasi mengenai IP address , Name server, OS yang digunakan, web server yang digunakan pada eprints.unsri.ac.id

Unsri.ac.id



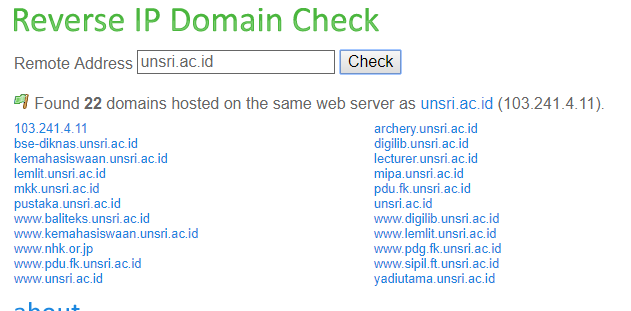
Didapat informasi mengenai history website unsri mengenai web server yang digunakan, netblock owner yang sebelumnya dipegang oleh PT. Telkom sekarang dipegang langsung oleh universitas sriwijaya. Pada saat dipegang oleh PT. Telkom tercatat versi dari web server yang digunakan. Namun untuk sekarang hanya diberikan informasi tentang jenis web server yang digunakan yakni nginx.

Nac.ilkom.unsri.ac.id



Pada web nac.ilkom.unsri.ac.id didapatkan informasi detail mengenai web server yakni versi apache, dan openssl. Hal ini dapat dimanfaatkan penyerang untuk mencari celah-celah pada web server yang digunakan.

* Reverse Domain

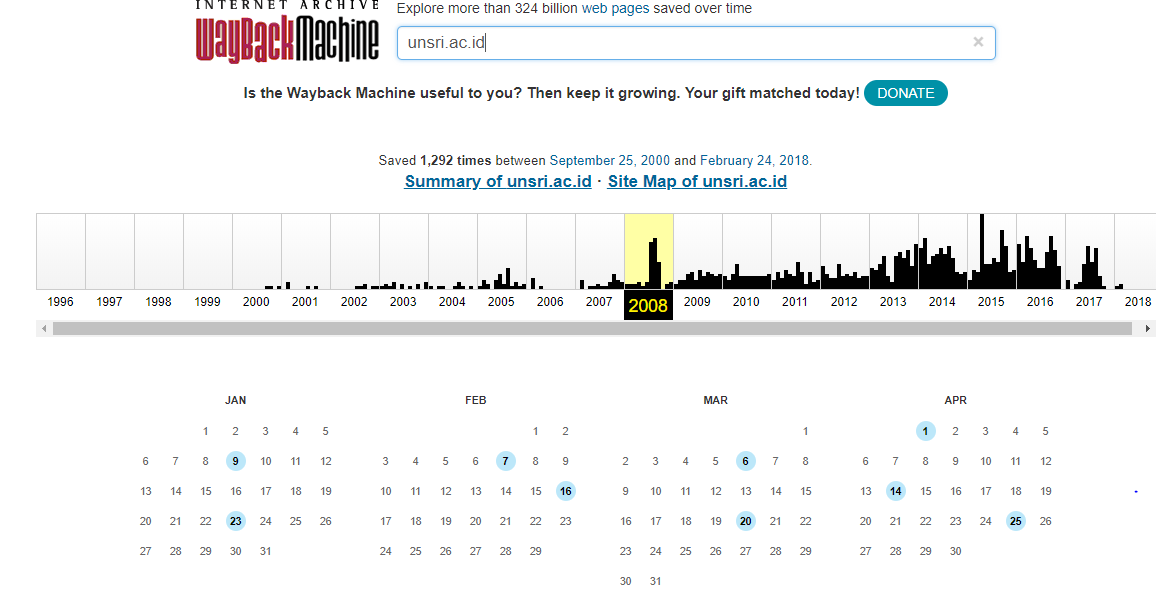


Dari reverse domain, penyerang mendapat informasi domain yang berada pada web server yang sama dengan unsri.ac.id.

Terdapat 22 domain, dari sini penyerang dapat melakukan footprinting ke masing-masing website untuk mencari celah yang dapat dimanfaatkan untuk melakukan jumping dari celah-celah tersebut.

* Archive.org

Archive.org menyimpan rekaman jejak website dari tahun ke tahun.



Rekaman jejak website unsri dari tahun 2000 – sekarang.



(Screenshot website unsri tanggal 7 Februari 2008)

Dari sini penyerang mungkin saja mendapat data-data penting website unsri.ac.id yang mungkin telah dihapus dari server.

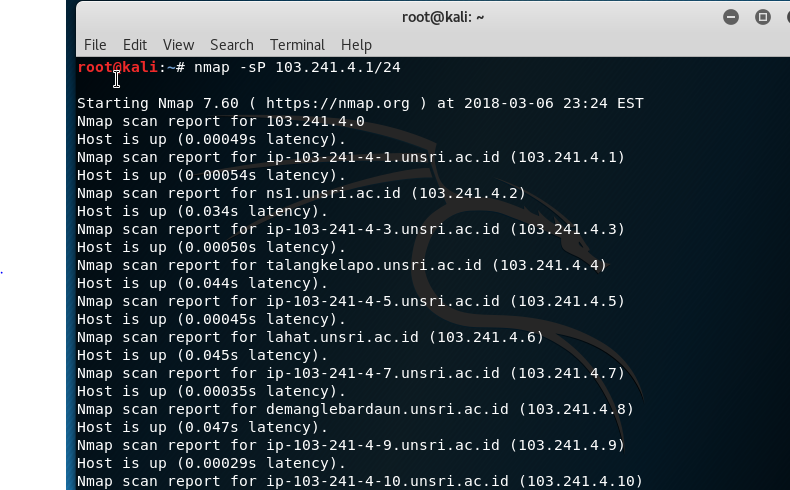
* Scanning Network

Menggunakan command nmap pada kali linux yakni :

Nmap –sP [IP Address website/subnet]

yang pada kali ini dilakukan scanning network terhadap IP Address unsri.ac.id yakni 103.241.4.1 – 103.241.4.255

Nmap –sP [103.241.4.1/24]



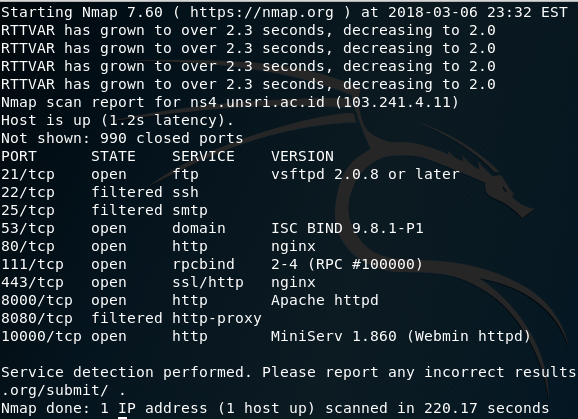
Didapatkan informasi mengenai domain host yang berhubungan dan 103.241.4.x dengan x dari 1 – 255.

Dari sini penyerang dapat melakukan footprinting terhadap IP address yang memiliki domain host, yang bisa saja terdapat celah karena beberapa domain tidak diperhatikan lagi.

* Scanning Port

Menggunakan command nmap pada kali linux melakukan scanning port ke IP address unsri.ac.id 103.241.4.11

Nmap –sV [103.241.4.11]



Didapatkan informasi mengenai port – port yang terbuka pada IP Address 103.241.4.11. Dari informasi ini penyerang dapat melakukan serangan terhadap port-port yang terbuka seperti ftp, http , dll.

* Scanning OS

Menggunakan command nmap kali linux

Nmap –O [103.241.4.11]



Informasi ini tidak 100% benar, seperti pada gambar diatas, nmap menebak OS yang digunakan pada IP address unsri adalah virtualbox 96%, dan QEMU 95%. Jika penyerang mendapatkan jenis OS yang digunakan 100%, penyerang dapat mencari celah pada OS tersebut.