TUGAS KEAMANAN JARINGAN KOMPUTER
RECONNAISSANCE PT. Semen Batu Raja

NAMA: EDI SUKRISNO
NIM: 09011181320043

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER

Dalam melakukan Reconnaissance penulis menerapkan Active Reconnaissance dan juga Passive Reconnaissance.

1. **Passive Reconnaissance**

Pada Passive Reconnaissance penulis melakukan pencarian atau pengumpulan informasi melalui internet, adapun yang pertama dilakukan yaitu pencarian informasi menggunakan tools http://whois.domaintools.com/semenbaturaja.co.id/, dan didapat hasil sebagai berikut:

```
Domain ID:PANDI-DO42364
Domain Name:SEMENBATURAJA.CO.ID
Created On:03-Mar-2008 13:22:59 UTC
Last Updated On:11-Jan-2017 03:12:02 UTC
Expiration Date:05-Mar-2018 23:59:59 UTC
Status:ok
Registrant ID:H5309080
Registrant Name:Ricky Syahrial
Registrant Organization:PT. SEMEN BATURAJA (PERSERO) TBK
Registrant Street1:Jl. Seruni Lrg Kebun Raya 214 A, Putri Kembang Dadar - Bukit Bes
ar
Registrant City:Palembang
Registrant State/Province:Sumatra Selatan
Registrant Postal Code:30000
Registrant Country:ID
Registrant Phone:+62.8983008908
Registrant Email: ricky.ptsb@gmail.com
```

Network

Site	http://semenbaturaja.co.id	**Netblock Owner**	Shared Hosting Servers
Domain	semenbaturaja.co.id	**Nameserver**	ns1.idhostinger.com
IP address	31.220.110.158	**DNS admin**	hostmaster@semenbaturaja.co.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	pandi.or.id	**Nameserver organisation**	whois.PublicDomainRegistry.com
Organisation	Pt. Semen Baturaja (PERSERO) Tbk, Jl. Seruni Lrg Kebun Raya 214 A, Putri Kembang Dadar - Bukit Besar, Palembang, 30000, Indonesia	**Hosting company**	Hostinger Group
Top Level Domain	Indonesia (.co.id)	**DNS Security Extensions**	*unknown*
Hosting country	SG		

Dari hasil diatas terlihat semua informasi lengkap terkait dengan domain pusri.co.id, salah satunya yang menjadi sorotan penulis yaitu informasi Admin Name dan Admin Email, yaitu Ricky syahrial & risky.ptsb@gmail.com. Dari informasi ini penulis melakukan pencarian lebih jauh melalui Google Search dan didapat profil dari Ricky syahrial, yang di dapat dari LinkedIn, sebagai berikut: https://www.linkedin.com/in/ricky-syahrial-849663108

Dari informasi diatas diketahui bahwa Ricky syahrial menurupakan Kepala biro BUMN PT. Semen Baturaja (Persero) yang akan menjadi salah satu target dan sekaligus portal untuk mendapatkan informasi lainnya.

Informasi mengenai pegawai lainnya yang didapat dari LinkedIn melaui LinkedIn dari Muhammad Nur Hidayat, diantaranya yaitu:

1. Sahadi sadiek
   Publik Relation at PT. Semen Baturaja (Persero)
   https://www.linkedin.com/in/sahadi-sadiek-26506a109
2. Robbi Santoso
   Human Resources Departement at PT. Semen Baturaja (Persero) Tbk
   https://www.linkedin.com/in/ibnu-abdullah-b45049ab/
3. pramaja gusnady
   Investor Relations at PT. Semen Baturaja (Persero)
   https://www.linkedin.com/in/pramaja-gusnady-70601660
4. Yundika Alvionita
   Public Relations at PT. Semen Baturaja (Persero)
   https://www.linkedin.com/in/yundika-alvionita-aa740a100
5. Muhammad Okta Prayudy
   HRD Staff and Tax at PT. Semen Baturaja (Persero) Tbk
   https://www.linkedin.com/in/muhammad-okta-prayudy-9518a42
6. Ageng Purboyo
   Chief Financial Officer of PT. Semen Baturaja Tbk.
   https://www.linkedin.com/in/ageng-purboyo-24071a44
7. riza rakhmawati
   analisa keuangan di PT. Semen Baturaja (Persero)
   https://www.linkedin.com/in/riza-rakhmawati-a4193379
8. Diding Nuriska
   IT di PT. Semen Baturaja (Persero)
   https://www.linkedin.com/in/diding-nuriska-27a7564a
9. Benny Kurniawan
   Investor Relations Staff at PT. Semen Baturaja (Persero) Tbk
   https://www.linkedin.com/in/benny-kurniawan-49644761
10. Adjie Kuncoro
    Investor Relations at PT Bukit Asam (Persero) Tbk
    https://www.linkedin.com/in/benny-kurniawan-49644761

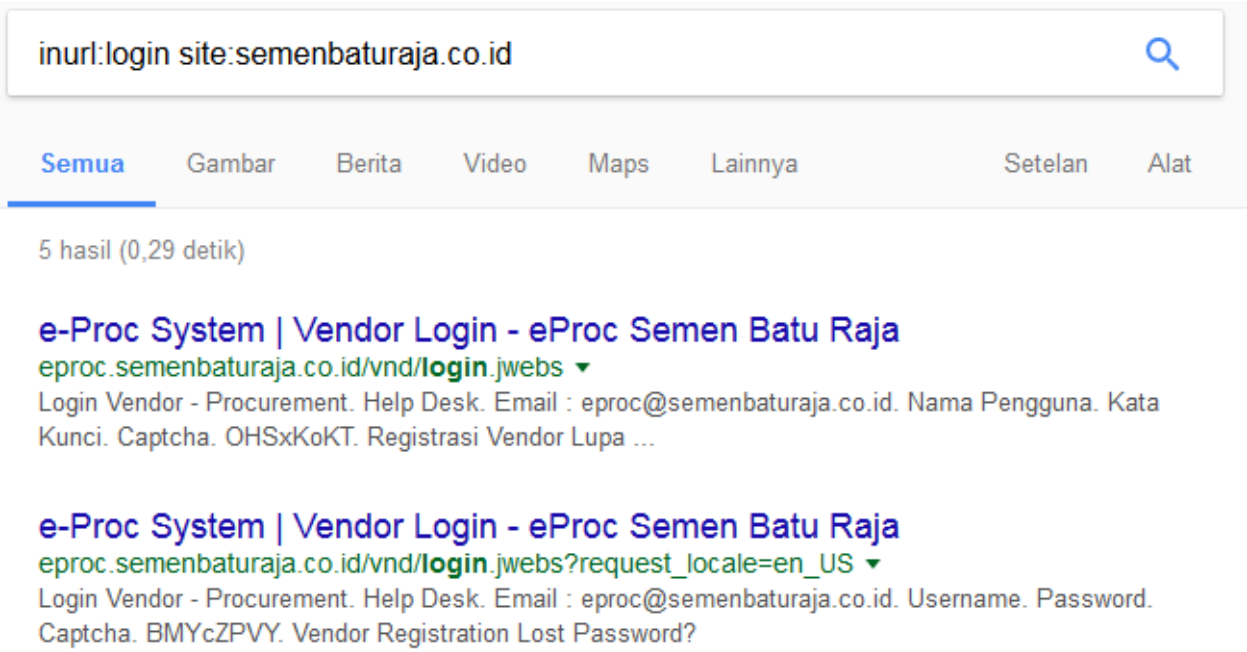
- Selanjutnya penulis melakukan scanning untuk mendapatkan informasi port berapa saja yang dibuka pada server PT. semen batu raja, informasi yang didapat dengan melakukan nmap scan pada semenbaturaja.co.id yaitu sebagai berikut:

```
Starting Nmap 6.00 ( http://nmap.org ) at 2017-02-15 14:35 EET
NSE: Loaded 17 scripts for scanning.
Initiating SYN Stealth Scan at 14:35
Scanning semenbaturaja.co.id (31.220.110.158) [100 ports]
Completed SYN Stealth Scan at 14:35, 4.85s elapsed (100 total ports)
Initiating Service scan at 14:35
Initiating OS detection (try #1) against semenbaturaja.co.id (31.220.110.158)
Retrying OS detection (try #2) against semenbaturaja.co.id (31.220.110.158)
Initiating Traceroute at 14:35
Completed Traceroute at 14:35, 4.18s elapsed
NSE: Script scanning 31.220.110.158.

[+] Nmap scan report for semenbaturaja.co.id (31.220.110.158)
Host is up.
All 100 scanned ports on semenbaturaja.co.id (31.220.110.158) are filtered

Too many fingerprints match this host to give specific OS details
```

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
80/tcp open http Apache httpd 2.2.16 ((Debian))
Device type: general purpose|WAP|media device|webcam
Running (JUST GUESSING): Linux 2.6.X|3.X|2.4.X (95%), Netgear embedded (89%), Western Digital embedded (89%), AXIS Linux 2.6.X (88%), PheeNet embedded (88%)
OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3 cpe:/o:linux:kernel:2.4.20 cpe:/o:axis:linux:2.6 cpe:/h:pheenet:wap-854gp
Aggressive OS guesses: Linux 2.6.18 - 2.6.32 (95%), Linux 2.6.35 (95%), Linux 2.6.32 - 2.6.35 (94%), Linux 2.6.22 (93%), Linux 2.6.17 - 2.6.36 (93%), Linux 2.6.19 - 2.6.35 (93%), Linux 2.6.22 (SPARC) (92%), Linux 3.0 - 3.1 (91%), Linux 2.6.26 (91%), Linux 2.6.38 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 3.164 days (since Sat Feb 11 05:27:36 2017)
Network Distance: 8 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)

Dari informasi diatas diketahui bahwa port yang dibuka hanya pada port 22 dan 80 yang mana merupakan port layanan ssh dan port http sedangkan port yang lainnya tidak dibuka seperti port 25 dan 53.

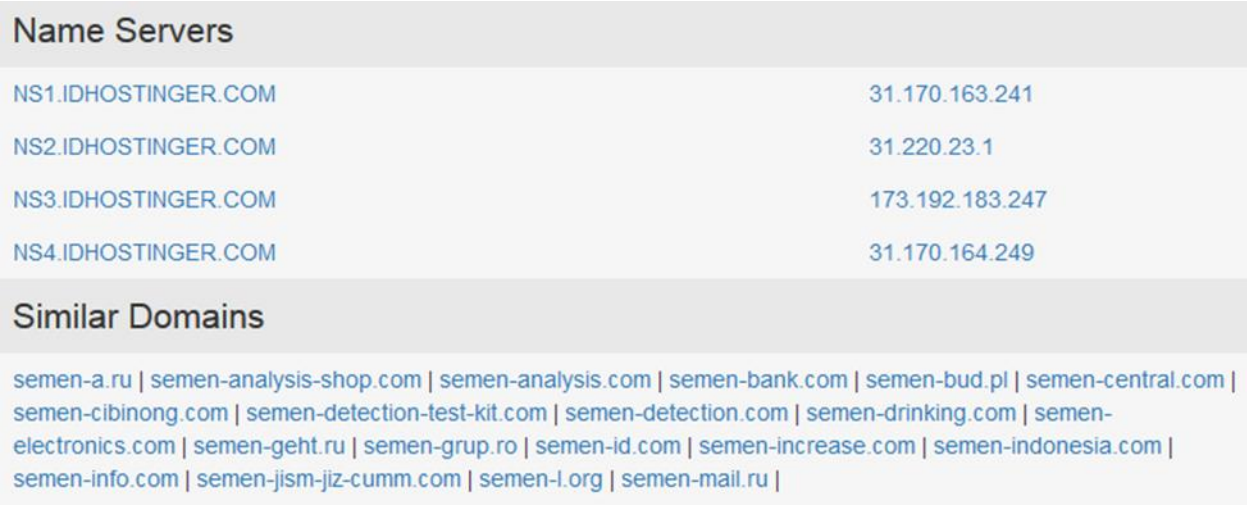
- Selanjutnya penulis melakukan pencarian portal login untuk memasuki situs pusri.co.id melalui Google Search, didapatkan hasil sebagai berikut:



http://eproc.semenbaturaja.co.id/vnd/login.jwebs

Penulis melakukan percobaan login dengan menggunakan sembarang username dan password, setelah melakukan berkali-kali try and error, diketahui bahwa tidak terdapat limit dan ada Re-captcha percobaan login dari user sehingga kita bisa mencoba sebanyak apapun untuk berusaha masuk ke salah satu domain semenbaturaja.co.id tersebut.

Informasi lainnya yang didapatkan dari who.is, yaitu: Informasi subdomain yang digunakan semenbaaturaja.co.id, https://who.is/whois/semenbaturaja.co.id



Informasi lainnya yang didapatkan dari
http://toolbar.netcraft.com/site_report?url=www.semenbaturaja.co.id yaitu:

Site	http://www.semenbaturaja.co.id	**Netblock Owner**	Shared Hosting Servers
Domain	semenbaturaja.co.id	**Nameserver**	ns1.idhostinger.com
IP address	31.220.110.158	**DNS admin**	hostmaster@semenbaturaja.co.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	pandi.or.id	**Nameserver organisation**	whois.PublicDomainRegistry.com
Organisation	Pt. Semen Baturaja (PERSERO) Tbk, Jl. Seruni Lrg Kebun Raya 214 A, Putri Kembang Dadar - Bukit Besar, Palembang, 30000, Indonesia	**Hosting company**	Hostinger Group
Top Level Domain	Indonesia (.co.id)	**DNS Security Extensions**	*unknown*
Hosting country	SG		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Shared Hosting Servers	31.220.110.158	Linux	openresty	15-Feb-2017
Indonesia Network Information Center Gedung Cyber Lt.3A Jl. Kuningan Barat No.8 Jakarta 12710	117.74.113.34	Linux	Apache	21-Sep-2011
PT. TELEKOMUNIKASI INDONESIA JL. KEBONSIRIH NO. 37 JAKARTA	222.124.142.80	Linux	Apache	21-Aug-2008
PT TELEKOMUNIKASI INDONESIA	203.130.226.74	Linux	Apache/2.2.0 Fedora	8-Feb-2007

Dari informasi yang didapat dari netcraft.net diatas hosting history pada tanggal 15 Februari 2017 semenbaturaja menggunakan openresty.