TUGAS KEAMANAN JARINGAN KOMPUTER

RECONNAISSANCE PT. PUSRI

NAMA: SYAMSUDIN
NIM: 09011281320012

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER

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

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/pusri.co.id/, dan didapat hasil sebagai berikut:

Email: nur.hidayat@pusri.co.id is associated with ~2 domains
Registrant Org:PT. Pupuk Sriwidjaja Palembang is associated with ~2 other domains
Dates:Created on 1998-01-01 - Expires on 2018-09-01 - Updated on 2017-02-07
IP Address:222.124.4.120 - 1 other site is hosted on this server
IP Location:Indonesia - Sumatera Selatan - Palembang - Pt Multi Data Palembang
ASN:Indonesia AS17974 TELKOMNET-AS2-AP PT Telekomunikasi Indonesia, ID (registered Oct 08, 2001)
Whois History:61 records have been archived since 2010-02-13
Whois Server:whois.pandi.or.id
Website Title:PT Pupuk Sriwidjaja Palembang (Pusri) | Home
Server Type:Apache/2.2.16 (Debian)
Response Code:200
SEO Score:80%
Terms:715 (Unique: 324, Linked: 238)
Images:57 (Alt tags missing: 57)
Links:156 (Internal: 147, Outbound: 2)
Domain ID:PANDI-DO152371
Domain Name:PUSRI.CO.ID
IP Address: 222.124.4.120
Created On:01-Jan-1998 13:28:47 UTC
Last Updated On:07-Feb-2017 14:27:03 UTC
Expiration Date:01-Sep-2018 23:59:59 UTC
Status:clientTransferProhibited
Status:serverTransferProhibited
Registrant ID:MRG58933e915b2ba
Registrant Name:muhammad nur hidayat
Registrant Organization:PT. Pupuk Sriwidjaja Palembang
Registrant Street1:Jl. Mayor Zen Sei-Selayur
Registrant City:Palembang
Registrant State/Province:Sumatera Selatan
Registrant Postal Code:30118
Registrant Country:ID
Registrant Phone:+62.071171222232
Registrant FAX:+62.071171222232
Registrant Email:nur.hidayat@pusri.co.id
Admin ID:MRG58933e8e5b0e5
Admin Name:muhammad nur hidayat
Admin Organization:PT. Pupuk Sriwidjaja Palembang
Admin Street1:Jl. Mayor Zen Sei-Selayur
Admin City:Palembang

Admin State/Province:Sumatera Selatan
Admin Postal Code:30118
Admin Country:ID
Admin Phone:+62.071171222232
Admin FAX:+62.071171222232
Admin Email:nur.hidayat@pusri.co.id
Tech ID:MRG58933e8ccb45a
Tech Name:muhammad nur hidayat
Tech Organization:PT. Pupuk Sriwidjaja Palembang
Tech Street1:Jl. Mayor Zen Sei-Selayur
Tech City:Palembang
Tech State/Province:Sumatera Selatan
Tech Postal Code:30118
Tech Country:ID
Tech Phone:+62.071171222232
Tech FAX:+62.071171222232
Tech Email:nur.hidayat@pusri.co.id
Billing ID:MRG58933e8fd9fa7
Billing Name:muhammad nur hidayat
Billing Organization:PT. Pupuk Sriwidjaja Palembang
Billing Street1:Jl. Mayor Zen Sei-Selayur
Billing City:Palembang
Billing State/Province:Sumatera Selatan
Billing Postal Code:30118
Billing Country:ID
Billing Phone:+62.071171222232
Billing FAX:+62.071171222232
Billing Email:nur.hidayat@pusri.co.id
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.PUSRI.ORG
Name Server:NS2.PUSRI.ORG
Name Server:NS3.PUSRI.ORG
DNSSEC:Unsigned

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 Muhammad Nur Hidayat & nur.hidayat@pusri.co.id. Dari informasi ini penulis melakukan pencarian lebih jauh melalui Google Search dan didapat profil dari Muhammad Nur Hidayat, yang di dapat dari LinkedIn, sebagai berikut:

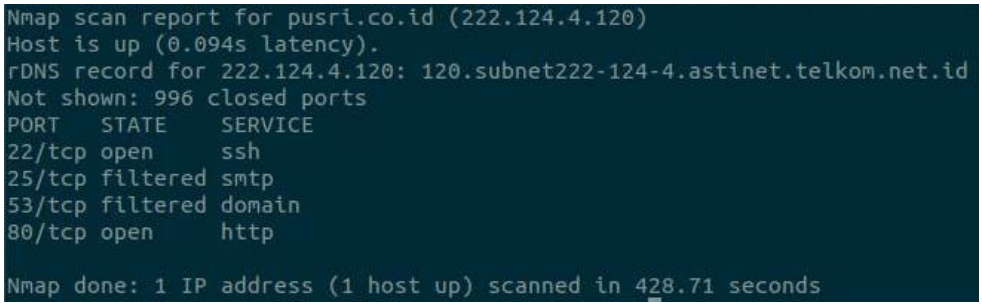
Muhammad Nur Hidayat
Network Administrator at PT. Pupuk Sriwidjaja
https://www.linkedin.com/in/muhammad-nur-hidayat-69543724/

Dari informasi diatas diketahui bahwa Muhammad Nur Hidayat menurupakan Network Administrator di PT. PUSRI 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. Annisa Rahayu
   Sales Staff for Commercial Products at PT. Pupuk Sriwidjaja Palembang
   https://www.linkedin.com/in/annisa-rahayu-93315064/
2. Ibnu Abdullah
   Knowledge Management PT Pupuk Sriwidjaja Palembang
   https://www.linkedin.com/in/ibnu-abdullah-b45049ab/
3. Muhammad Gustri Oktaviandi
   Internal Auditor at PT Pupuk Sriwidjaja Palembang
   https://www.linkedin.com/in/muhammad-gustri-oktaviandi-5b65ab59/
4. Syamsul Bahri
   Staf Penerimaan & Penempatan SDM at PT Pupuk Sriwidjaja Palembang
   https://www.linkedin.com/in/syamsul-bahri-12918993/
5. Citra Lestari
   Management Trainee at PT. Pupuk Sriwidjaja Palembang
   https://www.linkedin.com/in/citra-lestari-34353a105/
6. Yan Supranata Manurung
   Management Trainee at PT Pupuk Sriwidjaja Palembang
   https://www.linkedin.com/in/yan-supranata-manurung-892353b2/
7. Rahmat Aziz
   Production Planning & Control Department at PT Pupuk Sriwidjaja Palembang
   https://www.linkedin.com/in/rahmat-aziz-2212294a/
8. Handra Pandu
   Legal Manager at PT Pupuk Sriwidjaja Palembang
   https://www.linkedin.com/in/handra-pandu-3a390aaa/
9. Andhie Lesmana Syofian
   Marine Engineer at PT Pusri Palembang
   https://www.linkedin.com/in/andhie-lesmana-syofian-12a7a557/
10. Ferlyn Fachlevie
    Process Engineer at PT.Pupuk Sriwidjaja Palembang
    https://www.linkedin.com/in/ferlyn-fachlevie-01077164/
11. Mantya Hevar Rysta Kasih
    Maintenance Synergy Engineer at PT Pupuk Indonesia Palembang
    https://www.linkedin.com/in/hevar/
12. Zaki Abdullah
    Maintenance Planner at PT Pupuk Sriwidjaja Palembang
    https://www.linkedin.com/in/zaki-abdullah-a8879818/
13. Sapto Adi
    Fleet Manager at PT Pupuk Sriwidjaja Palembang
    https://www.linkedin.com/in/sapto-adi-02476847/
14. Rachmat Hamdani
    Plant Manager at PT Pupuk Sriwidjaja Palembang
    https://www.linkedin.com/in/rachmat-hamdani-65b7732b/

Selanjutnya penulis melakukan scanning untuk mendapatkan informasi port berapa saja yang dibuka pada server PT. PUSRI, informasi yang didapat dengan melakukan nmap scan pada pusri.co.id yaitu sebagai berikut:



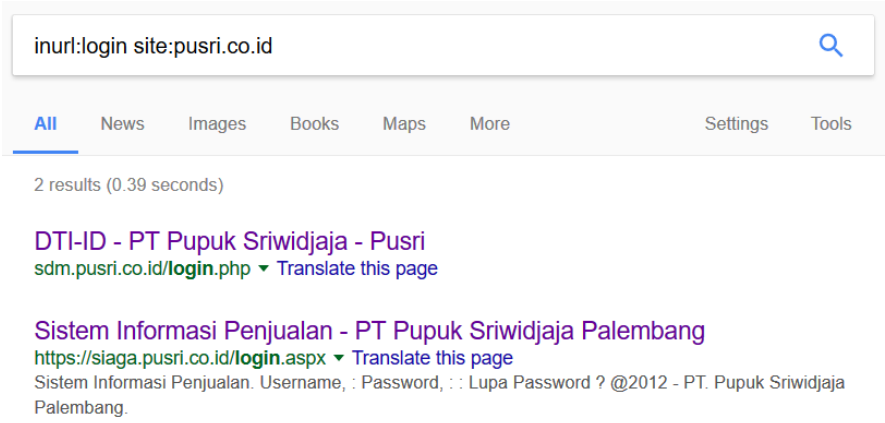
Berikut adalah informasi yang didapat dari tools https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap

Starting Nmap 6.00 (http://nmap.org) at 2017-02-14 09:23 EET
NSE: Loaded 17 scripts for scanning.
Initiating SYN Stealth Scan at 09:23
Scanning pusri.co.id (222.124.4.120) [100 ports]
Discovered open port 80/tcp on 222.124.4.120
Discovered open port 22/tcp on 222.124.4.120
Completed SYN Stealth Scan at 09:23, 1.63s elapsed (100 total ports)
Initiating Service scan at 09:23
Scanning 2 services on pusri.co.id (222.124.4.120)
Completed Service scan at 09:23, 6.54s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against pusri.co.id (222.124.4.120)
Retrying OS detection (try #2) against pusri.co.id (222.124.4.120)
Initiating Traceroute at 09:24
Completed Traceroute at 09:24, 0.26s elapsed
NSE: Script scanning 222.124.4.120.
[+] Nmap scan report for pusri.co.id (222.124.4.120)
Host is up (0.21s latency).
Not shown: 70 filtered ports, 28 closed ports
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!)

IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
TRACEROUTE (using port 3306/tcp)
HOP RTT ADDRESS
1 0.58 ms router1-lon.linode.com (212.111.33.229)
2 1.26 ms 109.74.207.10
3 0.62 ms 109.74.207.9
4 31.84 ms 195.66.226.8
5 213.58 ms 180.240.192.137
6 213.66 ms 97.subnet222-124-4.astinet.telkom.net.id (222.124.4.97)
7 213.63 ms 97.subnet222-124-4.astinet.telkom.net.id (222.124.4.97)
8 213.70 ms 120.subnet222-124-4.astinet.telkom.net.id (222.124.4.120)
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 19.46 seconds
Raw packets sent: 157 (11.294KB) | Rcvd: 248 (21.769KB)

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:



https://siaga.pusri.co.id/login.aspx
http://sdm.pusri.co.id/login.php

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

Informasi lainnya yang didapatkan dari tools pentest-tools.com, yaitu:

Informasi subdomain yang digunakan pusri.co.id, https://pentest-tools.com/information-gathering/find-subdomains-of-domain

Subdomain	IP address	Netname (whois)	Country (whois)
webmail.pusri.co.id	222.124.4.116	TLKM_D1_AST_MDP	ID
vpn.pusri.co.id	222.124.4.101	TLKM_D1_AST_MDP	ID
sms.pusri.co.id	222.124.4.110	TLKM_D1_AST_MDP	ID
webmail2.pusri.co.id	222.124.4.102	TLKM_D1_AST_MDP	ID
pop3.pusri.co.id	222.124.4.116	TLKM_D1_AST_MDP	ID
list.pusri.co.id	222.124.4.125	TLKM_D1_AST_MDP	ID
smtp.pusri.co.id	222.124.4.116	TLKM_D1_AST_MDP	ID
pop.pusri.co.id	222.124.4.116	TLKM_D1_AST_MDP	ID
www2.pusri.co.id	222.124.4.104	TLKM_D1_AST_MDP	ID
www1.pusri.co.id	222.124.4.104	TLKM_D1_AST_MDP	ID
mx.pusri.co.id	222.124.4.116	TLKM_D1_AST_MDP	ID
report.pusri.co.id	222.124.4.114	TLKM_D1_AST_MDP	ID
mail.pusri.co.id	222.124.4.116	TLKM_D1_AST_MDP	ID
www.pusri.co.id	222.124.4.120	TLKM_D1_AST_MDP	ID

Seperti sebelumnya penulis melakukan percobaan login pada salah satu subdomain pusri.co.id yaitu list.pusri.co.id dengan menggunakan sembarang username dan password, setelah melakukan berkali-kali try and error, diketahui bahwa tidak terdapat limit percobaan login dari user sehingga kita bias mencoba sebanyak apapun untuk berusaha masuk ke salah satu domain pusri.co.id tersebut.

Informasi directory yang digunakan pusri.co.id, https://pentest-tools.com/website-vulnerability-scanning/discover-hidden-directories-and-files

Directories	HTTP Code	HTTP Reason
/mail/	200	OK
/lib/	200	OK
/icons/	200	OK
/images/	200	OK
/application/	200	OK
/css/	200	OK

http://pusri.co.id/mail/
http://pusri.co.id/lib/
http://pusri.co.id/icons/
http://pusri.co.id/images/
http://pusri.co.id/application/
http://pusri.co.id/css/

Informasi lainnya yang didapat dari tools http://toolbar.netcraft.com/site_report?url=http://www.pusri.co.id, yaitu:

Background

Site title	PT Pupuk Sriwidjaja Palembang (Pusri) | Home	**Date first seen**	February 1997
Site rank		**Primary language**	Indonesian
Description	PT Pupuk Sriwidjaja Palembang (Pusri) adalah Badan Usaha Milik Negara yang didirikan sebagai pelopor produsen pupuk urea di Indonesia		
Keywords	Pupuk, Urea, Pupuk Subsidi, Pupuk Non Subsidi, Amoniak		

Network

Site	http://pusri.co.id	**Netblock Owner**	PT MULTI DATA PALEMBANG
Domain	pusri.co.id	**Nameserver**	ns1.pusri.org
IP address	222.124.4.120	**DNS admin**	root@pusri.co.id
IPv6 address	*Not Present*	**Reverse DNS**	120.subnet222-124-4.astinet.telkom.net.id
Domain registrar	pandi.or.id	**Nameserver organisation**	whois.pir.org
Organisation	PT. Pupuk Sriwidjaja Palembang, Jl. Mayor Zen Sei-Selayur, Palembang, 30118, Indonesia	**Hosting company**	PT Telekomunikasi Indonesia Tbk
Top Level Domain	Indonesia (.co.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen (Refresh)
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.4.120	Linux	Apache/2.2.16 Debian	13-Feb-2017
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	-	Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/5.2.5 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7	25-Mar-2009
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	unknown	24-Mar-2009
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.6 OpenSSL/0.9.8e PHP/5.2.5 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7	22-Mar-2009
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	Apache/2.2.4 Unix DAV/2 mod_ssl/2.2.4 OpenSSL/0.9.8d PHP/5.2.1 mod_apreq2-20051231/2.5.7 mod_perl/2.0.2 Perl/v5.8.7	3-Oct-2007
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.125	Linux	Apache/2.2.0 Unix DAV/2 mod_ssl/2.2.0 OpenSSL/0.9.8a PHP/5.1.2 mod_apreq2-20050712/2.1.3-dev mod_perl/2.0.2 Perl/v5.8.7	12-Mar-2007
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.120	Linux	Apache	4-Jun-2006
PT MULTI DATA PALEMBANG REGIONAL INTERNET PROVIDER JL. LINGKARAN I NO 305 PALEMBANG	222.124.7.120	Linux	Apache/2.0.54	17-Sep-2005
PT. IndoInternet Cyber Building, 8th Flr Jl. Kuningan Barat no 8 Jakarta 12710	202.159.31.240	-	Apache/2.0.52 Unix mod_perl/1.99_17 Perl/v5.8.4 mod_ssl/2.0.52 OpenSSL/0.9.7d PHP/4.3.10	4-Mar-2005
PT. IndoInternet Cyber Building, 8th Flr Jl. Kuningan Barat no 8 Jakarta 12710	202.159.31.240	Linux	Apache/1.3.28 Unix PHP/4.3.2 mod_gzip/1.3.19.1a mod_fastcgi/2.2.12 mod_perl/1.27	9-May-2004

Dari informasi yang didapat dari netcraft.net diatas hosting history pada tanggal 13 Februari 2017 PUSRI menggunakan web server Apache/2.2.16 yang mana versi terbaru dari Apache yang dirilis pada 20 Desember 2016 Apache/2.4.25.

Active Reconnaissance

Berikut ini adalah peta dan poster jaringan LAN dari PT. PUSRI yang penulis dapatkan: