TUGAS KEAMANAN JARINGAN KOMPUTER

DISUSUN OLEH:

RATIH HANDAYANI

09011181419037

DOSEN PEMBIMBING: Dr. Deris Stiawan, M.T.

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

Hasil Reconnaissance Website olx.co.id

1. Footprinting

- Whois

  Whois berguna untuk menampilkan informasi domain id, domain name, tanggal website tersebut dibuat, expirated date, pengguna yang mendaftar pada website tersebut, dan lain-lain. Berikut ini adalah tampilan informasi yang saya dapat untuk website www.olx.co.id

```
Domain ID:PANDI-DO147976
Domain Name:OLX.CO.ID
Created On:16-Sep-2008 13:28:35 UTC
Last Updated On:12-Aug-2017 20:42:08 UTC
Expiration Date:19-Sep-2018 23:59:59 UTC
Status:clientTransferProhibited
Status:serverTransferProhibited
Registrant ID:01220853vqk3
Registrant Name:Indah Susanti
Registrant Organization:PT. TOKO BAGUS
Registrant Street1:Gedung Tifa lt.10 Jl.Kuningan Barat 1 no.26
Registrant City:Jakarta Selatan
Registrant State/Province:DKI Jakarta
Registrant Postal Code:12710
Registrant Country:ID
Registrant Phone:+62.215275520
Registrant Email:domreg@ipmirror.com
Admin ID:01222447ue3t
Admin Name:Domain Administrator
Admin Organization:PT. TOKO BAGUS
Admin Street1:Gedung Tifa lt.10 Jl.Kuningan Barat 1 no.26
Admin City:Jakarta Selatan
Admin State/Province:DKI Jakarta
Admin Postal Code:12710
Admin Country:ID
```

- Whatweb

  Whatweb berguna untuk menampilkan informasi apache, cookies, country, IP, dan server yang digunakan, dan lain-lain. Berikut ini adalah informasi yang didapat untuk website olx.co.id menggunakan whatweb:

  Dapat dilihat bahwa website olx.co.id server yang digunakan adalah nginx, versi apache yang digunakan adalah 2.4.7, dan lain-lain.

- Netcraft

  Dengan menggunakan toolbar.netcraft.com kita akan mendapatkan informasi diantaranya adalah tanggal launching website tersebut, domain register, nama server, dan lain-lain.

Background

Site title	OLX - Jual Cepat Beli Dekat	Date first seen	December 2008
Site rank	15712	Primary language	Indonesian
Description	OLX Indonesia, pusat jual beli online terbesar di Indonesia. Semua barang ada disini, dari handphone, komputer, otomotif, fashion bahkan rumah dan lowongan kerja.		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://olx.co.id	Netblock Owner	Amazon Technologies Inc.
Domain	olx.co.id	Nameserver	pdns1.ultradns.net
IP address	52.74.231.246	DNS admin	khairul.zebua@olx.co.id
IPv6 address	*Not Present*	Reverse DNS	ec2-52-74-231-246.ap-southeast-1.compute.amazonaws.com
Domain registrar	pandi.or.id	Nameserver organisation	whois.godaddy.com
Organisation	Pt. Toko Bagus, Gedung Tifa lt.10 Jl.Kuningan Barat 1 no.26, Jakarta Selatan, 12710, Indonesia	Hosting company	Amazon - Asia Pacific (Singapore) datacenter
Top Level Domain	Indonesia (.co.id)	DNS Security Extensions	Enabled
Hosting country	sg		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
PT Cyberindo Aditama Jakarta 10270	210.210.179.84	Linux	unknown	17-Jul-2017
PT Cyberindo Aditama Jakarta 10270	210.210.179.104	Linux	unknown	16-Jun-2017
PT Cyberindo Aditama Jakarta 10270	210.210.179.94	Linux	unknown	10-May-2017
PT Cyberindo Aditama Jakarta 10270	210.210.179.104	Linux	unknown	2-May-2017
PT Cyberindo Aditama Jakarta 10270	210.210.179.84	Linux	unknown	17-Apr-2017
PT Cyberindo Aditama Jakarta 10270	210.210.179.104	Linux	unknown	23-Mar-2017
PT Cyberindo Aditama Jakarta 10270	210.210.179.84	Linux	unknown	6-Mar-2017
PT Cyberindo Aditama Jakarta 10270	210.210.179.104	Linux	unknown	27-Feb-2017
PT Cyberindo Aditama Jakarta 10270	210.210.179.94	Linux	unknown	24-Feb-2017
PT Cyberindo Aditama Jakarta 10270	210.210.179.104	Linux	unknown	21-Feb-2017

- Reverse domain

Reverse IP Domain Check

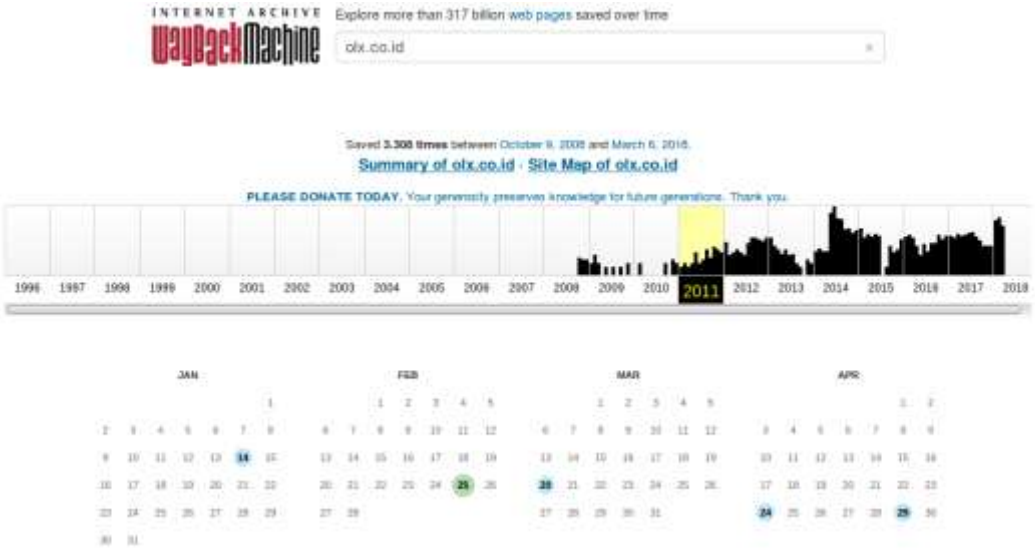
Remote Address olx.co.id Check

Found **1** domain hosted on the same web server as olx.co.id (52.74.231.246).

olx.co.id

Dari hasil reverse domain, di dapat bahwa domain olc.co.id adalah satu-satunya domain yang hosted di satu web server.

- Web archive



Informasi yang di dapat dari archive.org, website olx pertama kali online pada 9 Oktober 2008. Webtool archive.org ini merekam jejak website olx.co.id yang nantinya bisa dimanfaatkan penyerang dari informasi yang didapat pada web archive tersebut. Berikut ini adalah tampilan websiteolx pada 20 Maret 2011.

2. Scannning Network

- Scanning network

```
tamara@Tamara ~ $ nmap -sP 52.74.231.246

Starting Nmap 7.01 ( https://nmap.org ) at 2018-03-07 15:13 WIB
Nmap scan report for ec2-52-74-231-246.ap-southeast-1.compute.amazonaws.com (52.74.231.246)
Host is up (0.41s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.67 seconds
```

- Scanning service tersedia (port open)

```
tamara@Tamara ~ $ nmap -sV 52.74.231.246

Starting Nmap 7.01 ( https://nmap.org ) at 2018-03-07 15:15 WIB
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.51 seconds
```

- Scanning type OS

```
tamara@Tamara ~ $ sudo nmap -O 52.74.231.246
[sudo] password for tamara:

Starting Nmap 7.01 ( https://nmap.org ) at 2018-03-07 14:46 WIB
Nmap scan report for ec2-52-74-231-246.ap-southeast-1.compute.amazonaws.com (52.
74.231.246)
Host is up (0.015s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10, Linux 2.6.32 - 3.13, Linux 3.2 - 3.13, Linux 3.
4

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 934.76 seconds
```

3. CVE (Common Vulnerability Exposure)

Name	Description
CVE-2018-7492	A NULL pointer dereference was found in the net/rds/rdma.c __rds_rdma_map() function in the Linux kernel before 4.14.7 allowing local attackers to cause a system panic and a denial-of-service, related to RDS_GET_MR and RDS_GET_MR_FOR_DEST.
CVE-2018-7480	The blkcg_init_queue function in block/blk-cgroup.c in the Linux kernel before 4.11 allows local users to cause a denial of service (double free) or possibly have unspecified other impact by triggering a creation failure.
CVE-2018-7273	In the Linux kernel through 4.15.4, the floppy driver reveals the addresses of kernel functions and global variables using printk calls within the function show_floppy in drivers/block /floppy.c. An attacker can read this information from dmesg and use the addresses to find the locations of kernel code and data and bypass kernel security protections such as KASLR.
CVE-2018-6927	The futex_requeue function in kernel/futex.c in the Linux kernel before 4.14.15 might allow attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact by triggering a negative wake or requeue value.
CVE-2018-6926	In app/Controller/ServersController.php in MISP 2.4.87, a server setting permitted the override of a path variable on certain Red Hed Enterprise Linux and CentOS systems (where rh_shell_fix was enabled), and consequently allowed site admins to inject arbitrary OS commands. The impact is limited by the setting being only accessible to the site administrator.
CVE-2018-6794	Suricata before 4.1 is prone to an HTTP detection bypass vulnerability in detect.c and stream-tcp.c. If a malicious server breaks a normal TCP flow and sends data before the 3-way handshake is complete, then the data sent by the malicious server will be accepted by web clients such as a web browser or Linux CLI utilities, but ignored by Suricata IDS signatures. This mostly affects IDS signatures for the HTTP protocol and TCP stream content; signatures for TCP packets will inspect such network traffic as usual.
CVE-2018-6412	In the function sbusfb_ioctl_helper() in drivers/video/fbdev/sbuslib.c in the Linux kernel through 4.15, an integer signedness error allows arbitrary information leakage for the FBIOPUTCMAP_SPARC and FBIOGETCMAP_SPARC commands.
CVE-2018-6374	The GUI component (aka PulseUI) in Pulse Secure Desktop Linux clients before PULSE5.2R9.2 and 5.3.x before PULSE5.3R4.2 does not perform strict SSL Certificate Validation. This can lead to the manipulation of the Pulse Connection set.
CVE-2018-5750	The acpi_smbus_hc_add function in drivers/acpi/sbshc.c in the Linux kernel through 4.14.15 allows local users to obtain sensitive address information by reading dmesg data from an SBS HC printk call.
CVE-2018-5703	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.14.11 allows attackers to cause a denial of service (slab out-of-bounds write) or possibly have unspecified other impact via vectors involving TLS.