Keamanan Jaringan Komputer

Reconnaissance Dan Vulnerability Website

Nama : Meidi Dwi Hafiz

Nim : 09011281520097

Dosen pengampuh : Deris Setiawan, M.T.,Ph.D

Jurusan Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

Reconnaissance merupakan tahap persiapan di mana attacker atau hacker mencari informasi-informasi mengenai target sebanyak-banyaknya untuk meluncurkan serangan. Dalam hal ini, pengumpulan data target dapat berupa informasi tentang organisasi yang diikuti oleh target, pegawai, operasi, jaringan, dan sistem yang dimiliki oleh target. Reconnaissance dibagi menjadi 2 tipe:

- Passive Reconnaissance, Tipe ini digunakan ketika attacker mengumpulkan informasi tanpa berinteraksi langsung dengan target. Contohnya, mencari informasi lewat internet, majalah, media sosial target.
- Active Reconnaissance, Attacker mencari informasi secara langsung berinteraksi dengan target. Bisa jadi tipe ini sangat beresiko. Ini berfungsi agar attacker dapat mencari celah untuk melakukan serangan. Contohnya seperti menelepon targetnya, atau bertanya kepada rekan kerja target.

Vulnerability adalah suatu kelemahan program/infrastruktur yang memungkinkan terjadinya exploitasi system. kerentanan atau vulnerability ini terjadi akibat ksalahan dalam merancang,membuat atau mengimplementasikan sebuah system . Berikut tipe kerentanan atau vulnerability :

- 1. **High Risk Alert Level 3 :** Kerentanan dikategorikan sebagai yang paling berbahaya, yang menempatkan target scan pada risiko maksimum untuk hacking dan pencurian data.
- 2. **Medium Risk Alert Level 2 :** Kerentanan disebabkan oleh server misconfiguration dan sitecoding yang lemah, yang memfasilitasi gangguan server dan intrusi.
- 3. **Low Risk Alert Leve 1 :** Kerentanan berasal dari kurangnya enkripsi lalu lintas data atau jalur direktori pengungkapan.
- 4. **Information Alert :** ini adalah item yang telah ditemukan selama scan dan yang dianggap menarik, misalnya kemungkinan pengungkapan alamat internal IP atau alamat email, atau pencocokan string pencarian ditemukan di database Google Hacking, atau informasi tentang layanan yang telah ditemukan selama scanning.

1. **Website Dalam Negeri : www.bukalapak.com**

Domain Profil :

Registrant	Bukalapak.com
Registrant Org	PT Bukalapak.com
Registrant Country	ID
Registrar	CV. Jogjacamp IANA ID: 1478 URL: http://resellercamp.com/ Whois Server: whois.resellercamp.com abuse@resellercamp.com (p) 6282141570000
Registrar Status	clientTransferProhibited
Dates	3,442 days old Created on 2009-09-09 Expires on 2026-09-09 Updated on 2018-02-21
Name Servers	NS-1492.AWSDNS-58.ORG (has 10,499 domains) NS-1890.AWSDNS-44.CO.UK (has 371 domains) NS-4.AWSDNS-00.COM (has 21,128 domains) NS-979.AWSDNS-58.NET (has 377 domains)
Tech Contact	Bukalapak.com PT Bukalapak.com Graha Prawira Lantai 2 Jl Mampang Prapatan Raya No 18, Jakarta Selatan, DKI Jakarta, 12720, ID zaky@bukalapak.com (p) 62217997358 (f) 62217997358
IP Address	103.64.14.17 - 1 other site is hosted on this server
IP Location	- Jakarta Raya - Jakarta - Pt Bukalapak.com
ASN	AS135448 IDNIC-BUKALAPAK-AS-ID PT Bukalapak.com, ID (registered May 19, 2016)
Domain Status	Registered And Active Website
IP History	16 changes on 16 unique IP addresses over 11 years
Registrar History	2 registrars with 2 drops
Hosting History	10 changes on 8 unique name servers over 11 years
Server Type	nginx

Background

Site title	Situs Belanja Online dan Jual Beli Mudah Terpercaya | Bukalapak	**Date first seen**	December 2009
Site rank	2339	**Primary language**	Indonesian
Description	Situs jual beli online terpercaya di Indonesia. Belanja online murah, aman dan nyaman dari jutaan toko online pelapak Bukalapak garansi uang kembali		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	https://www.bukalapak.com	**Netblock Owner**	PT Bukalapak.com
Domain	bukalapak.com	**Nameserver**	ns-979.awsdns-58.net
IP address	103.64.14.20 (VirusTotal)	**DNS admin**	xinuc@bukalapak.com
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	resellercamp.com	**Nameserver organisation**	whois.markmonitor.com
Organisation	PT Bukalapak.com, Graha Prawira Lantai 2 Jl Mampang Prapatan Raya No 18, Jakarta Selatan, 12720, Indonesia	**Hosting company**	*unknown*
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT Bukalapak.com Corporate / Direct Member IDNIC Gd. Plaza Cityview lt 1 Jl. Kemang Timur No.22 Pejaten Barat Jakarta Selatan 12510	103.64.14.18	Linux	nginx	11-Feb-2019
Akamai	88.221.40.200	Linux	nginx	7-Nov-2018
PT Bukalapak.com Corporate / Direct Member IDNIC Gd. Plaza Cityview lt 1 Jl. Kemang Timur No.22 Pejaten Barat Jakarta Selatan 12510	103.64.14.21	Linux	nginx	6-Sep-2018
PT Bukalapak.com Corporate / Direct Member IDNIC Gd. Plaza Cityview lt 1 Jl. Kemang Timur No.22 Pejaten Barat Jakarta Selatan 12510	103.64.14.20	Linux	nginx	20-Mar-2018
PT.BUKALAPAK.COM Biznet Data Center Jakarta	182.253.238.102	Linux	nginx	24-Jun-2017
PT.BUKALAPAK.COM Biznet Data Center Jakarta	182.253.238.100	Linux	nginx	4-Jun-2017
PT.BUKALAPAK.COM Biznet Data Center Jakarta	182.253.238.102	Linux	nginx	11-Apr-2017
PT.BUKALAPAK.COM Biznet Data Center Jakarta	182.253.238.100	Linux	nginx	9-Feb-2017
PT.BUKALAPAK.COM Biznet Data Center Jakarta	182.253.238.102	Linux	nginx	10-Jun-2016
SBKOM Company Jakarta Jakarta	202.67.13.2	Linux	nginx	26-Dec-2014

CVE (Common Vulnerabilities and Exposures List)

Jenis OS	CVE Name	Deskripsi
Linux	CVE-2019-7312	Pengungkapan plaintext terbatas ada di PRIMX Zed Entreprise untuk Windows sebelum 6.1.2240, Zed Entreprise for Windows (pengajuan kualifikasi ANSSI) sebelum 6.1.2150, Zed Entreprise untuk Mac sebelum 2.0.199, Zed Entreprise untuk Linux sebelum 2.0.199, Zed Pro for Windows sebelum 1.0.195, Zed Pro untuk Mac sebelum 1.0.199, Zed Pro untuk Linux sebelum 1.0.199, Zed Gratis untuk Windows sebelum 1.0.195, Zed Gratis untuk Mac sebelum 1.0.199, dan Zed Gratis untuk Linux sebelum 1.0. 199. Menganalisis wadah Zed dapat menyebabkan pengungkapan konten plaintext dari file yang sangat kecil (beberapa byte) yang disimpan di dalamnya.
	CVE-2019-7308	kernel / bpf / verifier.c di kernel Linux sebelum 4.20.6 melakukan spekulasi di luar batas yang tidak diinginkan pada aritmatika pointer dalam berbagai kasus, termasuk kasus cabang berbeda dengan keadaan berbeda atau batas sanitasi, yang mengarah ke serangan saluran samping.
	CVE-2019-6136	Masalah telah ditemukan di libIEC61850 v1.3.1. Ethernet_setProtocolFilter dalam hal / ethernet / linux / ethernet_linux.c memiliki SEGV, seperti yang ditunjukkan oleh sv_subscriber_example.c dan sv_subscriber.c.
nginx	CVE-2019-7401	NGINX Unit sebelum 1.7.1 memungkinkan penyerang menyebabkan buffer overflow berbasis heap dalam proses router dengan permintaan yang dibuat khusus. Ini dapat mengakibatkan penolakan layanan (proses router macet) atau mungkin memiliki dampak lainnya yang tidak ditentukan.

2. Website Pemerintahan : www.bekasikota.go.id

Domain Profil :

Registrar Status	
Dates	3,021 days old Created on 2010-11-04 Expires on 2019-11-09
Name Servers	NS2.BEKASIKOTA.GO.ID (has 1 domains) NS3.BEKASIKOTA.GO.ID (has 1 domains) NS4.BEKASIKOTA.GO.ID (has 1 domains)
Tech Contact	—
IP Address	103.119.138.2 is hosted on a dedicated server
IP Location	- Jawa Barat - Bekasi - Diskominfo Kota Bekasi
ASN	AS137379 IDNIC-DISKOMINFOBEKASIKOTA-AS-ID Diskominfo Kota Bekasi, ID(registered Jan 03, 2018)
Hosting History	2 changes on 2 unique name servers over 5 years
Server Type	Apache

Background

Site title	Situs Pemerintah Kota Bekasi	**Date first seen**	July 2011
Site rank	1467504	**Primary language**	Indonesian
Description	Website Resmi Pemerintah Kota Bekasi		
Keywords	pemkot, kota bekasi, walikota,		
Netcraft Risk Rating [FAQ]	7/10		

Network

Site	https://www.bekasikota.go.id	**Netblock Owner**	Diskominfo Kota Bekasi
Domain	bekasikota.go.id	**Nameserver**	ns3.bekasikota.go.id
IP address	103.119.138.2 (VirusTotal)	**DNS admin**	tfk@bekasikota.go.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	*unknown*
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT. Mora Telematika Indonesia Grha 9, 1st Floor Jl. Panataran No. 9 Jakarta Pusat 10320	103.85.62.132	Linux	Apache	7-May-2018

CVE (Common Vulnerabilities and Exposures List)

Jenis OS	CVE Name	Deskripsi
Linux	CVE-2019-7312	Pengungkapan plaintext terbatas ada di PRIMX Zed Entreprise untuk Windows sebelum 6.1.2240, Zed Entreprise for Windows (pengajuan kualifikasi ANSSI) sebelum 6.1.2150, Zed Entreprise untuk Mac sebelum 2.0.199, Zed Entreprise untuk Linux sebelum 2.0.199, Zed Pro for Windows sebelum 1.0.195, Zed Pro untuk Mac sebelum 1.0.199, Zed Pro untuk Linux sebelum 1.0.199, Zed Gratis untuk Windows sebelum 1.0.195, Zed Gratis untuk Mac sebelum 1.0.199, dan Zed Gratis untuk Linux sebelum 1.0. 199. Menganalisis wadah Zed dapat menyebabkan pengungkapan konten plaintext dari file yang sangat kecil (beberapa byte) yang disimpan di dalamnya.
	CVE-2019-7308	kernel / bpf / verifier.c di kernel Linux sebelum 4.20.6 melakukan spekulasi di luar batas yang tidak diinginkan pada aritmatika pointer dalam berbagai kasus, termasuk kasus cabang berbeda dengan keadaan berbeda atau batas sanitasi, yang mengarah ke serangan saluran samping.
	CVE-2019-6136	Masalah telah ditemukan di libIEC61850 v1.3.1. Ethernet_setProtocolFilter dalam hal / ethernet / linux / ethernet_linux.c memiliki SEGV, seperti yang ditunjukkan oleh sv_subscriber_example.c dan sv_subscriber.c.

3. Website Luar Negeri : www.ebay.com

Registrant	Domain Administrator
Registrant Org	eBay Inc.
Registrant Country	US
Registrar	MarkMonitor, Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895740
Registrar Status	clientUpdateProhibited, clientTransferProhibited, clientDeleteProhibited, serverUpdateProhibited, serverTransferProhibited, serverDeleteProhibited
Dates	8,593 days old Created on 1995-08-03 Expires on 2019-08-02 Updated on 2018-07-02
Name Servers	A1.VERISIGNDNS.COM (has 63,239 domains) A2.VERISIGNDNS.COM (has 63,239 domains) A3.VERISIGNDNS.COM (has 63,239 domains) NS1.P47.DYNECT.NET (has 298,627 domains) NS2.P47.DYNECT.NET (has 298,627 domains) NS3.P47.DYNECT.NET (has 298,627 domains) NS4.P47.DYNECT.NET (has 298,627 domains)
Tech Contact	Domain Administrator eBay Inc. 2145 Hamilton Avenue,, San Jose, CA, 95125, US hostmaster@ebay.com (p) 14083767400
IP Address	23.49.13.21 - 4 other sites hosted on this server
IP Location	- Washington - Seattle - Akamai Technologies Inc.
ASN	AS16625 AKAMAI-AS - Akamai Technologies, Inc., US (registered May 30, 2000)
Domain Status	Registered And Active Website
IP History	37 changes on 37 unique IP addresses over 14 years
Registrar History	2 registrars with 1 drop
Hosting History	4 changes on 5 unique name servers over 16 years

Background

Site title	Electronics, Cars, Fashion, Collectibles, Coupons and More | eBay	**Date first seen**	October 2004
Site rank	91	**Primary language**	English
Description	Buy and sell electronics, cars, fashion apparel, collectibles, sporting goods, digital cameras, baby items, coupons, and everything else on eBay, the world		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	https://www.ebay.com	**Netblock Owner**	Akamai International, BV
Domain	ebay.com	**Nameserver**	ns1.p47.dynect.net
IP address	23.218.93.145 (VirusTotal)	**DNS admin**	hostmaster@ebay.com
IPv6 address	*Not Present*	**Reverse DNS**	a23-218-93-145.deploy.static.akamaitechnologies.com
Domain registrar	markmonitor.com	**Nameserver organisation**	whois.markmonitor.com
Organisation	*unknown*	**Hosting company**	Akamai Technologies
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	NL		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Akamai	84.53.168.84	Linux	unknown	26-Jan-2019
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.102.84	Linux	unknown	2-Oct-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.246.162	Linux	unknown	13-Sep-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.141.13	Linux	unknown	31-Jul-2018
Akamai	92.122.199.254	Linux	unknown	9-Jul-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.246.162	Linux	ebay server	12-Apr-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.212.233.229	Linux	ebay server	9-Mar-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.102.84	Linux	ebay server	1-Mar-2018
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.141.13	Linux	ebay server	6-Feb-2018
Akamai Technologies	2.17.220.61	Linux	ebay server	20-Nov-2017

CVE (Common Vulnerabilities and Exposures List)

Jenis OS	CVE Name	Deskripsi
Linux	CVE-2019-7312	Pengungkapan plaintext terbatas ada di PRIMX Zed Entreprise untuk Windows sebelum 6.1.2240, Zed Entreprise for Windows (pengajuan kualifikasi ANSSI) sebelum 6.1.2150, Zed Entreprise untuk Mac sebelum 2.0.199, Zed Entreprise untuk Linux sebelum 2.0.199, Zed Pro for Windows sebelum 1.0.195, Zed Pro untuk Mac sebelum 1.0.199, Zed Pro untuk Linux sebelum 1.0.199, Zed Gratis untuk Windows sebelum 1.0.195, Zed Gratis untuk Mac sebelum 1.0.199, dan Zed Gratis untuk Linux sebelum 1.0. 199. Menganalisis wadah Zed dapat menyebabkan pengungkapan konten plaintext dari file yang sangat kecil (beberapa byte) yang disimpan di dalamnya.
	CVE-2019-7308	kernel / bpf / verifier.c di kernel Linux sebelum 4.20.6 melakukan spekulasi di luar batas yang tidak diinginkan pada aritmatika pointer dalam berbagai kasus, termasuk kasus cabang berbeda dengan keadaan berbeda atau batas sanitasi, yang mengarah ke serangan saluran samping.
	CVE-2019-6136	Masalah telah ditemukan di libIEC61850 v1.3.1. Ethernet_setProtocolFilter dalam hal / ethernet / linux / ethernet_linux.c memiliki SEGV, seperti yang ditunjukkan oleh sv_subscriber_example.c dan sv_subscriber.c.