KEAMANAN JARINGAN KOMPUTER

Disusun oleh:

Nama : Novit Hardianto

NIM : 09011281520086

.

Jurusan Sitem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2019

Reconnaissance adalah sebuah fase persiapan sebelum (attacker) melakukan penyerangan, dimana kegiatan intinya adalah mengumpulkan informasi sebanyak mungkin mengenai sasaran. Teknik ini akan menyertakan network scanning baik melalui jaringan internal atau external yang tentu saja tanpa mengantongi ijin.

Berikut contoh 3 reconnaissance website

1. Website pemerintah : www.palembang.go.id

   - Detail informration

Site	http://palembang.go.id	**Netblock Owner**	Indonesia Online Access
Domain	palembang.go.id	**Nameserver**	ns1.palembang.go.id
IP address	182.23.103.155 (VirusTotal)	**DNS admin**	root@palembang.go.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	PT. Aplikanusa Lintasarta
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

   - Whois

```
Domain Name: PALEMBANG.COM
Registry Domain ID: 6398594_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2018-05-11T11:53:32Z
Creation Date: 1999-05-10T14:36:27Z
Registrar Registration Expiration Date: 2019-05-10T14:37:01Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org
/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org
/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org
/epp#clientDeleteProhibited
Registrant Organization:
Registrant State/Province:
Registrant Country: SG
Registrant Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=PALEMBANG.COM
Admin Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=PALEMBANG.COM
Tech Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=PALEMBANG.COM
Name Server: NS1.DOMAINSAREFREE.COM
Name Server: NS2.DOMAINSAREFREE.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
```

CVE

CVE-2018-17189

Di server HTTP Apache versi 2.4.37 dan sebelumnya, dengan mengirim pesan permintaan lambat ke sumber daya polos, aliran H2 untuk permintaan itu tidak perlu ditempati oleh server yang membersihkan data yang masuk itu. Ini hanya memengaruhi koneksi HTTP / 2 (mod_http2).

CVE-2018-1302

Ketika aliran HTTP / 2 dihancurkan setelah ditangani, Apache HTTP Server sebelum versi 2.4.30 bisa menulis pointer NULL yang berpotensi ke memori yang sudah dibebaskan. Kolam memori yang dikelola oleh server membuat kerentanan ini sulit dipicu dalam konfigurasi biasa, reporter dan tim tidak dapat mereproduksi di luar build debug, sehingga diklasifikasikan sebagai risiko rendah.

CVE-2017-9804

Di Apache Struts 2.3.7 hingga 2.3.33 dan 2.5 hingga 2.5.12, jika aplikasi mengizinkan memasukkan URL dalam bidang formulir dan URLValidator bawaan digunakan, dimungkinkan untuk menyiapkan URL khusus yang akan digunakan untuk membebani berlebihan proses server saat melakukan validasi URL. CATATAN: kerentanan ini ada karena perbaikan tidak lengkap untuk S2-047 / CVE-2017-7672.

1. Website dalam negeri : www.liputan6.com

   - Detail informration

Site	http://liputan6.com	**Netblock Owner**	Amazon Technologies Inc.
Domain	liputan6.com	**Nameserver**	ns-1768.awsdns-29.co.uk
IP address	54.169.198.155 (VirusTotal)	**DNS admin**	awsdns-hostmaster@amazon.com
IPv6 address	*Not Present*	**Reverse DNS**	ec2-54-169-198-155.ap-southeast-1.compute.amazonaws.com
Domain registrar	amazon.com	**Nameserver organisation**	whois.nic.uk
Organisation	Whois Privacy Service, P.O. Box 81226, Seattle, 98108-1226, United States	**Hosting company**	Amazon - Asia Pacific (Singapore) datacenter
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	sg		

   - Who is

```
Domain Name: liputan6.com
Registry Domain ID: 15927627_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon.com
Registrar URL: https://registrar.amazon.com
Updated Date: 2018-11-18T23:44:33.293Z
Creation Date: 1999-12-23T11:02:59Z
Registrar Registration Expiration Date: 2019-12-23T11:02:59Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: registrar-abuse@amazon.com
Registrar Abuse Contact Phone: +1.2067406200
Reseller:
Domain Status: clientTransferProhibited https://icann.org
/epp#clientTransferProhibited
Domain Status: renewPeriod https://icann.org/epp#renewPeriod
Registry Registrant ID:
Registrant Name: On behalf of liputan6.com owner
Registrant Organization: Whois Privacy Service
Registrant Street: P.O. Box 81226
Registrant City: Seattle
Registrant State/Province: WA
Registrant Postal Code: 98108-1226
Registrant Country: US
Registrant Phone: +1.2065771368
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: owner-5177683@liputan6.com .whoisprivacyservice.org
Registry Admin ID:
Admin Name: On behalf of liputan6.com administrative contact
Admin Organization: Whois Privacy Service
Admin Street: P.O. Box 81226
Admin City: Seattle
```

```
Admin City: Seattle
Admin State/Province: WA
Admin Postal Code: 98108-1226
Admin Country: US
Admin Phone: +1.2065771368
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email:  admin-5177683@liputan6.com .whoisprivacyservice.org
Registry Tech ID:
Tech Name: On behalf of liputan6.com technical contact
Tech Organization: Whois Privacy Service
Tech Street: P.O. Box 81226
Tech City: Seattle
Tech State/Province: WA
Tech Postal Code: 98108-1226
Tech Country: US
Tech Phone: +1.2065771368
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email:  tech-5177683@liputan6.com .whoisprivacyservice.org
Name Server: ns-1515.awsdns-61.org
Name Server: ns-1768.awsdns-29.co.uk
Name Server: ns-213.awsdns-26.com
Name Server: ns-595.awsdns-10.net
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
```

CVE

CVE-2018-5763

Masalah ditemukan di OXID eShop Enterprise Edition sebelum 5.3.7 dan 6.x sebelum 6.0.1. Dengan memasukkan URL yang dibuat khusus, penyerang dapat membuat server toko terhenti dan karenanya, berhenti bekerja. Ini hanya valid jika OXID High Performance Option diaktifkan dan Varnish digunakan.

CVE-2017-8807

bf_stp_error dalam bin / varnishd / cache / cache_fetch.c di Varnish HTTP Cache 4.1.x sebelum 4.1.9 dan 5.x sebelum 5.2.1 memungkinkan penyerang jarak jauh untuk mendapatkan informasi sensitif dari memori proses karena buffer VFP_GetStorage lebih besar daripada yang dimaksudkan dalam tertentu keadaan yang melibatkan objek transien -sfile Stevedore.

CVE-2017-12425

Masalah ditemukan di Varnish HTTP Cache 4.0.1 hingga 4.0.4, 4.1.0 hingga 4.1.7, 5.0.0, dan 5.1.0 hingga 5.1.2. Pernyataan if salah dalam kode sumber varnishd berarti bahwa permintaan tidak valid tertentu dari klien dapat memicu pernyataan, terkait dengan Integer Overflow. Ini menyebabkan proses pekerja varnishd untuk membatalkan dan memulai kembali, kehilangan konten di-cache dalam proses. Seorang penyerang karena itu dapat menghentikan proses pekerja pernis pada permintaan dan secara efektif menjaga dari melayani konten - serangan Denial-of-Service. Nama file kode sumber tertentu yang berisi pernyataan yang salah bervariasi di setiap rilis

2. Website luar negeri : www.facebook.com

- Detail informration

Site	http://facebook.com	**Netblock Owner**	Facebook, Inc.
Domain	facebook.com	**Nameserver**	a.ns.facebook.com
IP address	157.240.1.35 (VirusTotal)	**DNS admin**	dns@facebook.com
IPv6 address	2a03:2880:f129:83:face:b00c:0:25de	**Reverse DNS**	edge-star-mini-shv-01-lht6.facebook.com
Domain registrar	registrarsafe.com	**Nameserver organisation**	whois.registrarsafe.com
Organisation	Facebook, Inc., 1601 Willow Rd, Menlo Park, 94025, United States	**Hosting company**	Facebook
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	US		

- Who is

```
Domain Name: FACEBOOK.COM
Registry Domain ID: 2320948_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrarsafe.com
Registrar URL: https://www.registrarsafe.com
Updated Date: 2018-07-23T18:17:13Z
Creation Date: 1997-03-29T05:00:00Z
Registrar Registration Expiration Date: 2028-03-30T04:00:00Z
Registrar: RegistrarSafe, LLC
Registrar IANA ID: 3237
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
Registrar Abuse Contact Phone: +1.6503087004
Domain Status: clientUpdateProhibited https://www.icann.org
/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://www.icann.org
/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://www.icann.org
/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited https://www.icann.org
/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://www.icann.org
/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://www.icann.org
/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Facebook, Inc.
Registrant Street: 1601 Willow Rd
Registrant City: Menlo Park
Registrant State/Province: CA
Registrant Postal Code: 94025
Registrant Country: US
Registrant Phone: +1.6505434800
Registrant Phone Ext:
Registrant Fax: +1.6505434800
```

```
Registrant Fax Ext:
Registrant Email:  domain@fb.com
Registry Admin ID:
Admin Name: Domain Admin
Admin Organization: Facebook, Inc.
Admin Street: 1601 Willow Rd
Admin City: Menlo Park
Admin State/Province: CA
Admin Postal Code: 94025
Admin Country: US
Admin Phone: +1.6505434800
Admin Phone Ext:
Admin Fax: +1.6505434800
Admin Fax Ext:
Admin Email:  domain@fb.com
Registry Tech ID:
Tech Name: Domain Admin
Tech Organization: Facebook, Inc.
Tech Street: 1601 Willow Rd
Tech City: Menlo Park
Tech State/Province: CA
Tech Postal Code: 94025
Tech Country: US
Tech Phone: +1.6505434800
Tech Phone Ext:
Tech Fax: +1.6505434800
Tech Fax Ext:
Tech Email:  domain@fb.com
Name Server: A.NS.FACEBOOK.COM
Name Server: B.NS.FACEBOOK.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2019-02-11T08:08:49Z <<<
```

```
Search results obtained from the RegistrarSafe, LLC WHOIS database are
provided by RegistrarSafe, LLC for information purposes only, to assist
users in obtaining information concerning a domain name registration record.
The information contained therein is provided on an "as is" and "as available"
basis and RegistrarSafe, LLC does not guarantee the accuracy or completeness
of any information provided through the WHOIS database.  By submitting a WHOIS quer
y,
you agree to the following: (1) that you will use any information provided through
the WHOIS only for lawful purposes; (2) that you will comply with all ICANN rules
and regulations governing use of the WHOIS; (3)  that you will not use any informat
ion
provided through the WHOIS to  enable, or otherwise cause the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail (i.e., spam); or
(4) that you will not use the WHOIS to enable or otherwise utilize high volume,
automated, electronic processes that apply to or attach to RegistrarSafe, LLC or
its systems. RegistrarSafe, LLC reserves the right to modify these terms
at any time and to take any other appropriate actions, including but not limited to
restricting any access that violates these terms and conditions. By submitting this
query, you acknowledge and agree to abide by the foregoing terms, conditions and po
licies.
```

CVE

CVE-2018-5379

Daemon Quagga BGP (bgpd) sebelum versi 1.2.3 dapat melipatgandakan kehabisan memori saat memproses bentuk tertentu dari pesan UPDATE, yang berisi daftar-cluster dan / atau atribut yang tidak dikenal. Serangan yang berhasil dapat menyebabkan penolakan layanan atau berpotensi memungkinkan penyerang untuk mengeksekusi kode arbitrer.

CVE-2018-5174

Dalam Pembaruan Windows 10 April 2018, Windows Defender SmartScreen menghormati bendera "SEE_MASK_FLAG_NO_UI" yang terkait dengan file yang diunduh dan tidak akan menampilkan UI apa pun. File yang tidak dikenal dan berpotensi berbahaya akan diizinkan untuk berjalan karena SmartScreen tidak akan meminta pengguna untuk mengambil keputusan, dan jika pengguna offline semua file akan diizinkan dibuka karena Windows tidak akan meminta pengguna untuk bertanya apa yang harus dilakukan . Firefox salah mengatur tanda ini

saat mengunduh file, menyebabkan perilaku yang kurang aman dari SmartScreen. Catatan: masalah ini hanya memengaruhi pengguna Windows 10 yang menjalankan pembaruan April 2018 atau lebih baru. Itu tidak mempengaruhi pengguna Windows lain atau sistem operasi lain. Kerentanan ini memengaruhi Thunderbird <52.8, Thunderbird ESR <52.8, Firefox <60, dan Firefox ESR <52.8.

CVE-2018-5142

Jika izin Tangkapan Media dan Aliran API diminta dari dokumen dengan URL "data:" atau "blob:", pemberitahuan izin tidak menampilkan dengan benar domain asal. Pemberitahuan menyatakan "Protokol tidak dikenal" sebagai yang diminta, mengarah ke kebingungan pengguna tentang situs mana yang meminta izin ini. Kerentanan ini memengaruhi Firefox <59