

TUGAS IV
MATA KULIAH KEAMANAN JARINGAN KOMPUTER



Oleh :

Rofby Hidayadi 09011281020132

Dosen Pengampuh : Deris Stiawan, M.T., Ph.D.

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2018

I. Judul Tugas

Reconnaissance Network Security – Facebook

II. Whois

Whois atau “who is” digunakan untuk mendapatkan data informasi domain tertentu seperti nama pemilik domain, ip address, name server dan umur domain. Adapun dari hasil “whois facebook.com” didapat beberapa informasi penting seperti berikut ini:

```
Domain Name: facebook.com
Registry Domain ID: 2320948 DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2016-11-29T12:28:07-0800
Creation Date: 1997-03-28T21:00:00-0800
Registrar Registration Expiration Date: 2025-03-29T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Facebook, Inc.
Registrant Street: 1601 Willow Road,
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 Administrator
```

Gambar 1. Whois facebook.com

```
Admin Organization: Facebook, Inc.
Admin Street: 1601 Willow Road,
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 Administrator
Tech Organization: Facebook, Inc.
Tech Street: 1601 Willow Road,
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: b.ns.facebook.com
Name Server: a.ns.facebook.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2018-03-27T07:03:10-0700 <<<
```

Gambar 2. Whois facebook.com

Dari hasil yang didapat ada beberapa informasi penting yang dapat dimanfaatkan untuk proses peretasan oleh orang-orang yang tidak bertanggung jawab, seperti waktu expire domain, registrant name, registrant organization, registrant street, registrant phone, dan email yang bisa di manfaatkan untuk melakukan social engineering.

III. Whatweb

Berikut adalah hasil dari “whatweb facebook.com” :

```
root@kali:~# whatweb facebook.com
http://facebook.com [301 Moved Permanently] Country[UNITED STATES][US], IP[157.240.7.35], RedirectLocation[https://facebook.com/], UncommonHeaders[x-fb-debug]
https://facebook.com/ [301 Moved Permanently] Country[UNITED STATES][US], IP[157.240.7.35], RedirectLocation[https://www.facebook.com/], Strict-Transport-Security[max-age=15552000; preload], UncommonHeaders[x-fb-debug]
https://www.facebook.com/ [200 OK] Cookies[fr,sb], Country[UNITED STATES][US], HTML5, HttpOnly[fr,sb], IP[157.240.13.35], Meta-Refresh-Redirect[? fb noscript=1], OpenSearch[osd.xml], PasswordField[pass,reg_passwd_], Script, Strict-Transport-Security[max-age=15552000; preload], UncommonHeaders[x-content-type-options,x-fb-debug], X-Frame-Options[DENY], X-XSS-Protection[0]
https://www.facebook.com/?_fb_noscript=1 [200 OK] Cookies[fr,noscript,sb], Country[UNITED STATES][US], HTML5, HttpOnly[fr,sb], IP[157.240.13.35], OpenSearch[osd.xml], PasswordField[pass,reg_passwd_], Script, Strict-Transport-Security[max-age=15552000; preload], UncommonHeaders[x-content-type-options,x-fb-debug], X-Frame-Options[DENY], X-XSS-Protection[0]
```

Gambar 3. Whatweb facebook.com

IV. Reverse IP Domain Check

Berikut adalah hasil reverse ip domain check pada facebook.com melalui <https://www.yougetsignal.com/tools/web-sites-on-web-server/> :

Reverse IP Domain Check

Remote Address

Found 103 domains hosted on the same web server as facebook.com (157.240.22.35).

It appears that the web server located at 157.240.22.35 may be hosting one or more web sites with explicit content. The web sites in question are highlighted in red below. There is a possibility that all of the web sites on this web server may be blocked by web filtering software. Search engine rankings for these web sites may be affected as well.

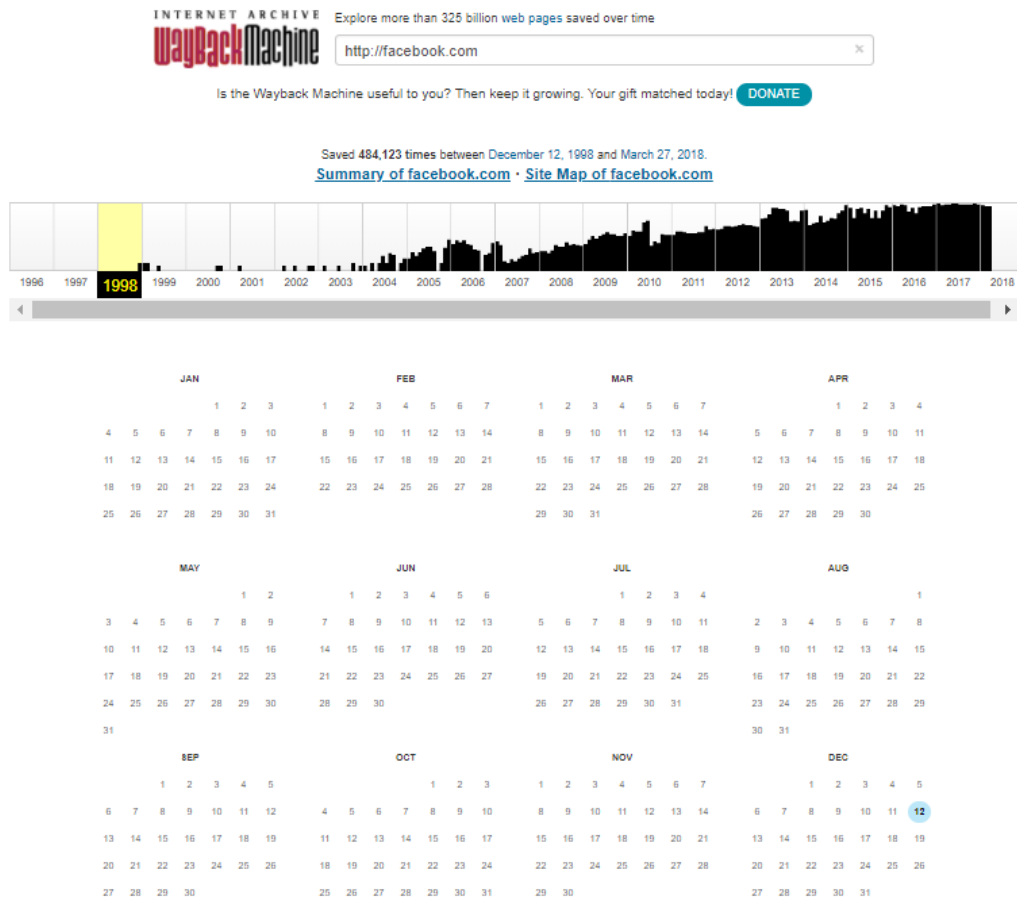
0.basic.fb.me	0.facebook.co
0.facebook.de	0.facebook.org
4810195241.facebook.co	4g.fb.me
admin.facebook.org	ads-dev.fb.me
ads.facebook.com	api.fb.me
api.google.com.fb.me.g.co.4g.fb.me	api4.fb.me
apps.ng.facebooklive.com	b-api.facebook.com
b-graph.facebook.com	blackberry.fb.me
bn-in.fb.me	br.facebookproxy.com
cdn.fb.me	claroideiastv.com.br.facebookproxy.com
claroideiastv.facebookproxy.com	clicknext.facebook.co
connect.facebook.com	connect.facebook.org
cyber.fb.me	de-de.fb.me
developers.odn.fb.me	edige-mqtt-mini-shv-01-sin0.facebook.co
facebook.com	facebook.com
fb.com	fb.me
fbcdn.net	fbsbx.com
fma.fb.me	free.facebook.co
free.facebook.co.za	free.facebook.org
free.fb.me	fucking_awesome.facebook.co
go.fb.me	google.facebook.co
google.facebook.org	graph.facebook.co
graph.facebook.org	h.fb.me
hotlink.fb.me	instagram.facebook.co
m.facebook.co	m.facebook.co.id
m.facebook.com	m.facebook.com.ar
m.facebook.com.br	m.facebook.com.mx
m.facebook.de	m.facebook.it
m.fb.me	messenger.fb.me
postmaster.facebook.com	proxy.fb.me
singapore.fb.me	smart.facebook.co
smart.fb.me	smartvoda.facebook.co
speed.facebook.co	speed.fb.me
star-mini.c10r.facebook.com	star-mini.c10r.facebook.com
star-mini.facebook.com	static.fb.me
sun.odn.facebook.co	sun.facebook.co
telkomsel.server.facebook.biz	viber.facebook.co
vip.facebook.com	vip.fb.me
wv.fb.me	wap.fb.me
web.odn.facebook.co	web.odn.facebook.org
web.facebook.co	work.facebook.org
www.facebook.co	www.facebook.co
www.facebook.co.id	www.facebook.com
www.facebook.com	www.facebook.com.ar
www.facebook.com.mx	www.facebook.com.ni
www.facebook.com.tr	www.facebook.com.www.facebook.com.mx
www.fb.com	www.fb.me
www.fb.x.fb.me	www.fbcdn.com
www.fbcdn.net	www.google.com.fb.me
x.facebook.co	x.facebook.com
x.fb.me	xb.fb.me
xs.fb.me	

Gambar 4. Reverse IP domain check facebook.com

Dari hasil reverse ip domain check, didapat informasi bahwa domain facebook.com bukanlah satu satunya domain yang hosted di satu web server, melainkan ada 103 domains, hal ini bisa memungkinkan peretasan dengan cara masuk ke sistem facebook.com melalui proses jumping dari website lain yang memiliki bug.

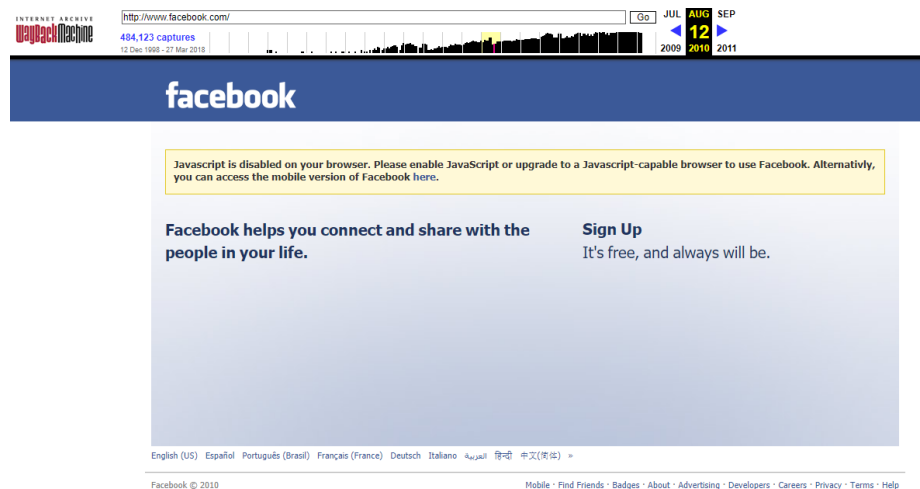
V. Archive

Berikut adalah hasil archive pada facebook.com melalui <https://web.archive.org> :



Gambar 5. Archive facebook.com

Dari informasi yang di dapat dari archive.org, website facebook pertama kali online pada 12 Desember 1998, webtool archive.org telah banyak merekam “jejak” website <http://facebook.com> yang mana informasi yang didapat berupa data penting di website tersebut, meskipun sudah di hapus dari server facebook.



Gambar 6. Hasil capture tampilan facebook.com pada 12 agustus 2010

VI. OS Fingerprint

Berikut adalah hasil dari OS fingerprint facebook.com (157.240.7.35) menggunakan tool nmap :

```
root@kali:~# nmap -O 157.240.7.35
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-28 04:34 WIB
Nmap scan report for edge-star-mini-shv-01-sin6.facebook.com (157.240.7.35)
Host is up (0.019s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|switch|phone|game console|VoIP adapter
Running (JUST GUESSING): Linux 1.0.X (88%), Cisco embedded (87%), Nokia Symbian OS (87%), Ouya embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:1.0.9 cpe:/h:cisco:catalyst_1900 cpe:/o:nokia:symbian_os cpe:/h:cisco:ata_188_
voip_gateway
Aggressive OS guesses: Linux 1.0.9 (88%), Cisco Catalyst 1900 switch (87%), Nokia 3600i mobile phone (87%), OUYA
game console (86%), Cisco ATA 188 VoIP adapter (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
```

Gambar 7. OS fingerprint facebook.com

Dari hasil OS fingerprint menggunakan tool nmap diatas, dapat kita ketahui tipe sistem operasi yang digunakan oleh server facebook.com adalah linux, dengan kernel versi 1.0.9, informasi seperti ini dapat digunakan untuk melakukan exploit ke sistem dengan cara mencari vulnerability versi kernel linux yang digunakan.

VII. Referensi

<https://www.yougetsignal.com/tools/web-sites-on-web-server/>

<https://web.archive.org>