Task II

Keamanan Jaringan Komputer

Disusun Oleh :

Nama : Rido Rahmat

NIM : 09011181419018

Kelas : SK8Pil

Dosen Pembimbing :Deris StiawanM.T.,Ph.d

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

Monitoring

Pada tahap ini kita akan mencoba memonitoring target yang kita lakukan dengan beberapa cara yaitu bisa melalui sebuah terminal pada OS kali linux dan mendapatkan informasi dari website yang telah disediakan. Mendapatkan informasi dari target ada 5 web yang menyediakan informasi-informasi domain yang ingin digunakan. Berikut nama-nama/car-cara untuk mendapatkan informasi yaitu:

- Whois
- Whatweb
- Netcraft
- Report domain, dan
- Web archive

Dari nama-nama diatas ialah tempat untuk mendapatkna informasi-informasi yang penting dari sebuah target yang diinginkan

1. Whois

   Whois adalah suatu prosedur untuk mendapatkan informasi mengenai sebuah domain. Informasi yang bisa di dapat meliputi siapa pemilik Domain, dimana alamatnya, no telepon, alamat email, kapan domain ini di daftarkan dan kapan domain ini akan expired

   Cara mendapatkan informasi target dari whois dengan terminal di Ubuntu
   Di terminal cukup ketikan dengan ***whois domain target.***

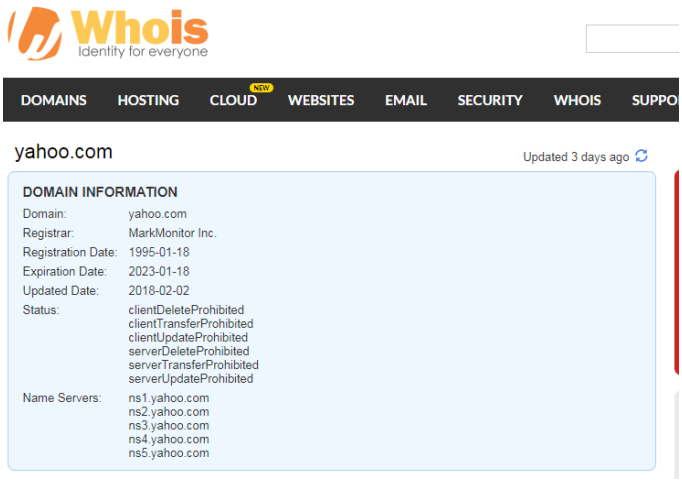
```
rido@rido-Lenovo-G40-70:~$ sudo apt-get install whois
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  snap-confine
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  whois
0 upgraded, 1 newly installed, 0 to remove and 154 not upgraded.
Need to get 34,0 kB of archives.
After this operation, 184 kB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu xenial/main amd64 whois amd64 5.2.11 [34,0 kB]
Fetched 34,0 kB in 1s (23,5 kB/s)
Selecting previously unselected package whois.
(Sedang membaca basis data ...  230253 berkas atau direktori telah terpasang.)
Preparing to unpack .../whois_5.2.11_amd64.deb ...
Unpacking whois (5.2.11) ...
Processing triggers for man-db (2.7.5-1) ...
Sedang menata whois (5.2.11) ...
rido@rido-Lenovo-G40-70:~$ whois yahoo.com
   Domain Name: YAHOO.COM
   Registry Domain ID: 3643624_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2018-02-02T01:07:18Z
   Creation Date: 1995-01-18T05:00:00Z
   Registry Expiry Date: 2023-01-19T05:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.YAHOO.COM
   Name Server: NS2.YAHOO.COM
   Name Server: NS3.YAHOO.COM
   Name Server: NS4.YAHOO.COM
   Name Server: NS5.YAHOO.COM
```

Gambar 1. Hasil whois

Dari gambar diatas bahwa ada beberapa informasi-informasi yang penting didapatkan dari target.

Target yang ditujuh ialah yahoo.com

Melalui internet



REGISTRANT CONTACT

Name:	Domain Administrator
Organization:	Yahoo! Inc.
Street:	701 First Avenue
City:	Sunnyvale
State:	CA
Postal Code:	94089
Country:	US
Phone:	+1.4083493300
Fax:	+1.4083493301
Email:	**domainadmin**@yahoo-inc.com

ADMINISTRATIVE CONTACT

Name:	Domain Administrator
Organization:	Yahoo! Inc.
Street:	701 First Avenue
City:	Sunnyvale
State:	CA
Postal Code:	94089
Country:	US
Phone:	+1.4083493300
Fax:	+1.4083493301
Email:	**domainadmin**@yahoo-inc.com

TECHNICAL CONTACT

Name:	Domain Administrator
Organization:	Yahoo! Inc.
Street:	701 First Avenue
City:	Sunnyvale
State:	CA
Postal Code:	94089
Country:	US
Phone:	+1.4083493300
Fax:	+1.4083493301
Email:	**domainadmin**@yahoo-inc.com

RAW WHOIS DATA

```
Domain Name: yahoo.com
Registry Domain ID: 3643624_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2018-02-01T16:42:27-0800
Creation Date: 1995-01-18T00:00:00-0800
Registrar Registration Expiration Date: 2023-01-18T21:00:00-0800
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:
```

2. Whatweb

   Whatweb sama halnya dengan whois. Berikut informasi yang didapatkan dari whatweb adalah

   Dari informasi yang didapatkan bahwa ip yang digunakan oleh target,HTTP server yang digunakan,domain dan sebagainya.

3. Netcraft

   Netcraft adalah informasi yang didapatkan dari netcraft ini sangat banyak yang didapatkan tidak halnya dengan informasi yang didapatkan dari whois dan whatweb. Di dalam netcraft informasi yang didapatkan terdapat informasi ssh nya. Berikut informasi yang didapatkan dari netcraft

Background

Site title	Yahoo	**Date first seen**	August 1995
Site rank	335	**Primary language**	English
Description	News, email and search are just the beginning. Discover more every day. Find your yodel.		
Keywords	yahoo, yahoo home page, yahoo homepage, yahoo search, yahoo mail, yahoo messenger, yahoo games, news, finance, sport, entertainment		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://www.yahoo.com	**Netblock Owner**	Yahoo! Europe
Domain	yahoo.com	**Nameserver**	ns1.yahoo.com
IP address	188.125.80.145	**DNS admin**	hostmaster@yahoo-inc.com
IPv6 address	2a00:1288:110:2:0:0:0:3008	**Reverse DNS**	media-router-fp2.prod.media.vip.ir2.yahoo.com
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	Verizon
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	IE	**Latest Performance**	Performance Graph

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Yahoo Europe	188.125.80.144	unknown	ATS	9-Mar-2018
Yahoo Europe	188.125.80.145	unknown	ATS	1-Mar-2018
Yahoo Europe	188.125.80.144	unknown	ATS	26-Feb-2018
Yahoo Europe	188.125.80.145	unknown	ATS	5-Feb-2018
Yahoo Europe	188.125.80.144	unknown	ATS	21-Jan-2018
Yahoo Europe	188.125.80.145	unknown	ATS	12-Jan-2018
Yahoo Europe	188.125.80.144	unknown	ATS	4-Jan-2018
Yahoo Europe	188.125.80.145	unknown	ATS	30-Dec-2017
Yahoo Europe	188.125.80.144	unknown	ATS	21-Dec-2017
Yahoo Europe	188.125.80.145	unknown	ATS	7-Dec-2017

HTTP Accelerator

A web accelerator is a proxy server that reduces web site access times.

Technology	Description	Popular sites using this technology
Apache Traffic Server	Open-source caching proxy server	www.tumblr.com, i.ebayimg.com, polaris.xfinity.com

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Asynchronous Javascript	*No description*	www.cnn.com, www.espn.com, www.ebay.co.uk
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	accounts.google.com, tap2-cdn.rubiconproject.com

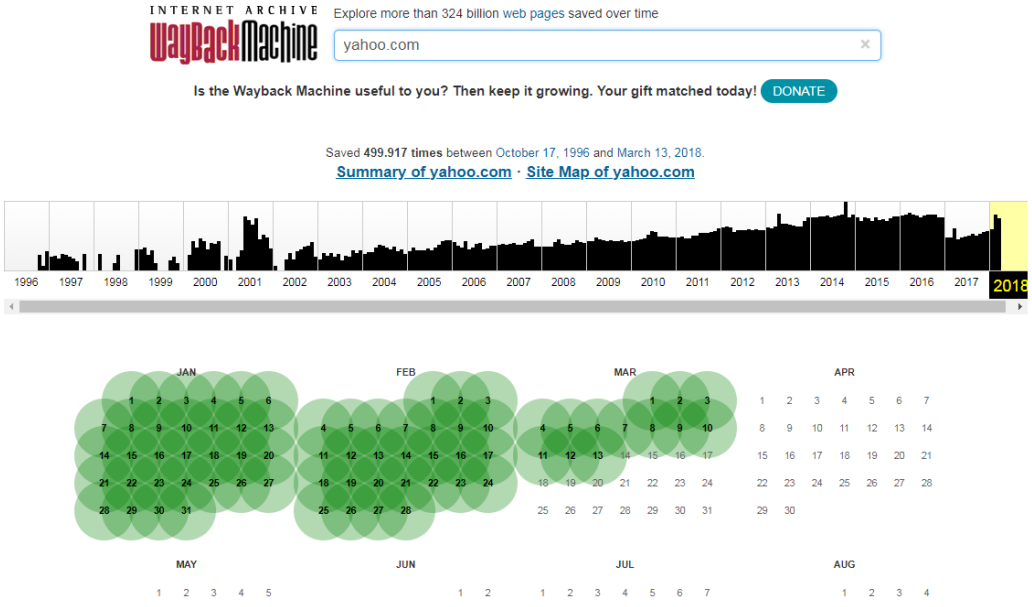
Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

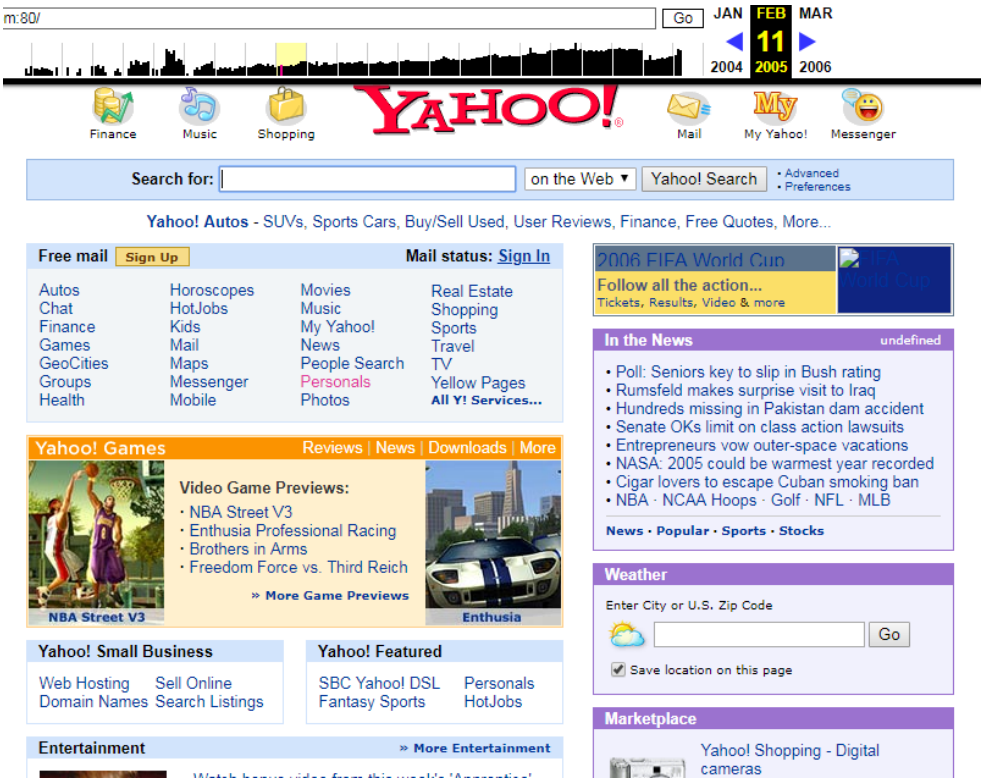
Technology	Description	Popular sites using this technology
Yahoo! User Interface Library	Open-source JavaScript and CSS library	www.geny.com, www.anime-sharing.com, www.nittaya.de
Google Hosted Libraries	Google API to retrieve JavaScript libraries	www.boursorama.com, www.sfr.fr, www.bloomberg.com

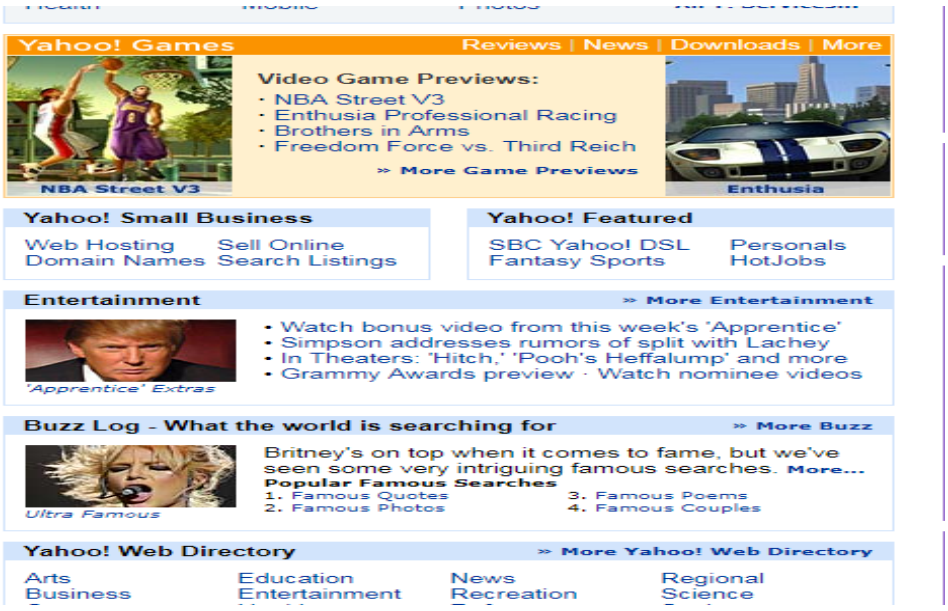
4. Web Archive

   Informasi yang didapatkan dari web archive ialah kita dapat mendapatkan informasi seperti tampilan dan traffic dari target. Berikut tempilan yang di dapatkan dari web arhive.



Dari informasi diatas terdapat warna-warna hijau yaitu informasi yang didapatkan dari kalender-kalender tersebut kita dapat mengetahui tampilan dari web tersebut dari tahun ke tahun. Berikut tampilan web yahoo.com





CVE 2003-1493 dari yahoo.com

– CVSS Scores & Vulnerability Types

CVSS Score	**5.0**
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is requi exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	CWE id is not defined for this vulnerability

– Products Affected By CVE-2003-1493

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	Application	HP	Openview Network Node Manager	5.0.1				Version Details Vulnerabilities
2	Application	HP	Openview Network Node Manager	6.0.1				Version Details Vulnerabilities
3	Application	HP	Openview Network Node Manager	6.1		Solaris		Version Details Vulnerabilities
4	Application	HP	Openview Network Node Manager	6.1				Version Details Vulnerabilities
5	Application	HP	Openview Network Node Manager	6.1		Hp Ux 10.x		Version Details Vulnerabilities
6	Application	HP	Openview Network Node Manager	6.1		Hp Ux 11.x		Version Details Vulnerabilities
7	Application	HP	Openview Network Node Manager	6.2		Solaris		Version Details Vulnerabilities
8	Application	HP	Openview Network Node Manager	6.2				Version Details Vulnerabilities
9	Application	HP	Openview Network Node Manager	6.2		Hp Ux 10.x		Version Details Vulnerabilities
10	Application	HP	Openview Network Node Manager	6.2		Hp Ux 11.x		Version Details Vulnerabilities
11	Application	HP	Openview Network Node Manager	6.2		Nt 4.x Windows 2000		Version Details Vulnerabilities
12	Application	HP	Openview Network Node Manager	6.4		Solaris		Version Details Vulnerabilities
13	Application	HP	Openview Network Node Manager	6.4				Version Details Vulnerabilities
14	Application	HP	Openview Network Node Manager	6.4		Hp Ux 11.x		Version Details Vulnerabilities