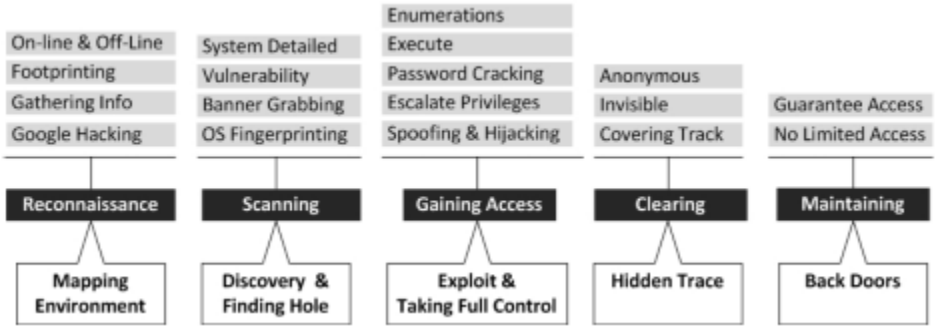
Muhammad Azriansyah 09011281320006
Keamanan Jaringan Komputer

Analisis Reconnaissance Result pada Website the-gazette.com



Fase-fase dalam melakukan proses *Hacking.*

Reconnaissance

Merupakan fase pertama dalam kegiatan hacking, sering disebut juga dengan istilah Footprinting, dimana hacker mencoba mendapatkan berbagai informasi mengenai target seperti nama domain, alamat IP, lokasi fisik, teknologi yang ada dan yang digunakan, kontak organisasi, dan informasi lainnya.

Fase ini terbagi menjadi dua, active reconnaissance dan passive reconnaissance. Tujuan pada fase ini adalah untuk memetakan sistem dan jaringan milik target. Hacker akan mencoba untuk menyusun semua sistem yang ada di dalam jaringan milik target, lalu mencoba untuk menyusun semua celah yang tersedia di dalam sistem tersebut.

Tools yang digunakan antara lain:

1. Network-tools.com
2. Netcraft.com

Informasi IP Address dan Site Rank (netcraft.com)

Background

Site title	the GazettE Official Site	**Date first seen**	August 2015
Site rank	496089	**Primary language**	English
Description	""		
Keywords	""		

Muhammad Azriansyah 09011281320006
Keamanan Jaringan Komputer

Network

Site	http://the-gazette.com	**Netblock Owner**	Upright Inc.
Domain	the-gazette.com	**Nameserver**	ns1.value-domain.com
IP address	113.42.230.185	**DNS admin**	hostmaster@the-gazette.com
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	discount-domain.com	**Nameserver organisation**	whois.discount-domain.com
Organisation	manager, 4-19-17-1F Eifuku, Suginami-ku, 168-0064, JP	**Hosting company**	UCOM Corporation
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	JP		

Informasi Creation dan Expired Date (network-tools.com)

Domain Name: THE-GAZETTE.COM
Registrar: GMO INTERNET, INC. DBA ONAMAE.COM
Sponsoring Registrar IANA ID: 49
Whois Server: whois.discount-domain.com
Referral URL: http://www.onamae.com/
Name Server: NS1.VALUE-DOMAIN.COM
Name Server: NS2.VALUE-DOMAIN.COM
Status: ok https://icann.org/epp#ok
Updated Date: 22-feb-2016
Creation Date: 27-mar-2015
Expiration Date: 27-mar-2017

Informasi Pembeli Domain (network-tools.com)

Registrar: GMO INTERNET, INC.
Registrar IANA ID: 49
Registrar Abuse Contact Email: abuse@gmo.jp
Registrar Abuse Contact Phone: +81.337709199
Domain Status: ok https://icann.org/epp#ok
Registry Registrant ID: Not Available From Registry
Registrant Name: nana obu
Registrant Organization: manager
Registrant Street: 4-19-17-1F Eifuku
Registrant City: Suginami-ku
Registrant State/Province: Tokyo
Registrant Postal Code: 168-0064
Registrant Country: JP
Registrant Phone: +81.353053809
Registrant Phone Ext:
Registrant Fax: +81.353053810
Registrant Fax Ext:
Registrant Email: obu@pscompany.co.jp

Muhammad Azriansyah 09011281320006
Keamanan Jaringan Komputer

Informasi Security (netcraft.com)

Security

Netcraft Risk Rating [FAQ]	1/10		
On Spamhaus Block List	No	On Exploits Block List	No
On Policy Block List	No	On Domain Block List	No

Informasi Sub-Domain (jika ada) (netcraft.com)

Results for the-gazette.com

Found 1 site

	Site	Site Report	First seen	Netblock	OS
1.	the-gazette.com		august 2015	upright inc.	unknown

Informasi Admin (network-tools.com)

Registry Admin ID: Not Available From Registry
Admin Name: nana obu
Admin Organization: manager
Admin Street: 4-19-17-1F Eifuku
Admin City: Suginami-ku
Admin State/Province: Tokyo
Admin Postal Code: 168-0064
Admin Country: JP
Admin Phone: +81.353053809
Admin Phone Ext:
Admin Fax: +81.353053810
Admin Fax Ext:
Admin Email: obu@pscompany.co.jp

Informasi Teknisi (network-tools.com)

Registry Tech ID: Not Available From Registry
Tech Name: nana obu
Tech Organization: manager
Tech Street: 4-19-17-1F Eifuku
Tech City: Suginami-ku
Tech State/Province: Tokyo
Tech Postal Code: 168-0064
Tech Country: JP
Tech Phone: +81.353053809
Tech Phone Ext:
Tech Fax: +81.353053810
Tech Fax Ext:
Tech Email: obu@pscompany.co.jp

Muhammad Azriansyah 09011281320006
Keamanan Jaringan Komputer

Informasi Web Server (netcraft.com)

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Upright Inc.	113.42.230.185	Linux	Apache/2.2.15 CentOS	24-Sep-2016

Informasi Teknologi (netcraft.com)

Site Technology

Fetched on 11th February 2017

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

Technology	Description	Popular sites using this technology
CentOS	*No description*	www.gsmarena.com , www.reimageplus.com , www.ilsole24ore.com
Apache	Web server software	www.bom.gov.au , www.libero.it , image4.pubmatic.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
jQuery	A JavaScript library used to simplify the client-side scripting of HTML	www.cnn.com , www.girlsofdesire.org , www.foxnews.com

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	www.googleadservices.com , bid.g.doubleclick.net , google.com

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	www.facebook.com , www.bbc.co.uk , www.ebay.com

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	www.xvideos.com , login.salesforce.com , login.live.com

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	www.repubblica.it , www.amazon.com , www.ebay.de

Analisa

Netcraft Risk Rating menunjukkan nilai 1/10, hal ini menunjukkan kemungkinan situs ini pernah terlibat kegitan phising di masa lalu atau karena belum begitu di trust oleh pihak Netcraft di karenakan usia website yang relatif masih muda.

Website tidak termasuk dalam block list spamhause, policy block list, exploit block list, dan domain block list, menandakan website yang bersangkutan memiliki konten yang cukup sehat dan belum terindikasi dengan isu-isu keamanan yang cukup berbahaya.

Berdasarkan hasil penelusuran Netcraft.com website yang bersangkutan tidak memiliki subdomain sehingga resiko serangan zombie dan hijacking dari subdomain yang tidak terurus ataupun di lupakan dapat di cegah.

Pada "Hosting History" the netblock owner, IP address(es), operating system, web server, memperlihatkan kapan server di ubah atau di perbaharui. Data-data di atas menjadi sangat-sangat berguna bagi Hacker, terutama tanggal perubahan akhir. Tanggal tersebut merepresentasikan secara umum kapan system terakhir di reboot dan di perbaharui .

Server yang di gunakan adalah Apache/2.2.15 CentOS, Versi yang cacat adalah seluruh generasi Apache 1.3 dan versi 2 hingga 2.0.36. Dengan adanya cacat tersebut, hacker dikabarkan dapat mengeksploitasi kerentanan dengan cara mengirimkan request pada server Apache bersangkutan. Server yang diserang hacker memanfaatkan kelemahan ini akan mengalami DoS. Alias server itu tak bisa diakses. Dalam sejumlah kasus, penyerangnya dapat menjalankan pilihan kodenya.Dengan celah tersebut, hacker dikabarkan dapat mengeksploitasi kerentanan dengan cara mengirimkan request pada server Apache bersangkutan.

Scripting website menggunakan jQuery. Cross-site scripting (XSS) kerentanan di jQuery sebelum 1.6.3, ketika menggunakan location.hash untuk memilih elemen, memungkinkan penyerang melalui remote untuk menyuntikkan skrip web yang mengeksploitasi atau HTML melalui tag dibuat.

Doctype website menggunakan HTML5. Serangan terhadap HTML5 tak terlihat, dan diam-diam dan umumnya menargetkan presentasi aplikasi dan lapisan logika. 10 ancaman terhadap HTML5 menargetkan XHR dan tag HTML5, komponen kaya fitur seperti browser SQL dan penyimpanan, dan DOM. Daftar ancamannya antara lain:

1. Bypass CSRF dengan XHR dan CORS

2. Jacking - klik, CORS, tab

3. HTML5 berbasis cross-site scripting menggunakan tag, events dan atribut

4. Menyerang penyimpanan dan variabel DOM

5. Memanfaatkan poin Browser SQL

6. Injection dengan Web Messaging dan Workers

7. Scripting lintas situs berbasis DOM dan isu-isunya

8. Serangan Offline dan cross-widget vektor

9. Isu Web socket

10. Serangan API dan protocol

Encoding karakter menggunkan UTF-8. Penggunaan sebenarnya dari UTF-8 terbuka untuk eksploitasi kanonikal. Awalnya, Unicode melarang generasi "non-shortest form" UTF-8, tetapi tidak menafsirkan dari "non-shortest form" UTF-8. Lalu diperbaiki di Unicode 3.0, karena masalah keamanan dapat muncul ketika perangkat lunak yang menafsirkan non-shortest form.

CSS pada website memiliki kerentanan, yang dikenal sebagai "Scripting Cross-Site", yang sama-sama dapat terjadi pada semua produk vendor ', dan bukan hasil dari kecacatan pada salah satu dari mereka. Sebaliknya, itu hasil dari praktik coding web umum tertentu. Scripting Cross-Site berpotensi memungkinkan pengguna jahat untuk memperkenalkan kode yang dapat di eksekusi sesuai keinginannya ke sesi web pengguna lain. Setelah kode berjalan, bisa di jalankan dalam jangkauan yang luas, dari pemantauan sesi web pengguna dan meneruskan salinan ke pelaku kejahatan, untuk mengubah apa yang ditampilkan pada layar pengguna. Bahkan bisa lebih berbahaya, script tersebut masih bertahan, sehingga saat pengguna kembali ke situs web, script pengguna berbahaya ini akan mulai berjalan lagi.