Tugas Keamanan Jaringan Komputer



Disusun Oleh:

Nama : Sigit Wijaya Pramono

NIM: 09011181419012

JURUSAN SISTEM KOMPUTER FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA 2018

Laporan Hands-on Port Scanning Menggunakan Nmap

1. Teori

Pada handson mata kuliah Keamanan Jaringan Komputer ini melakukan praktik secara langsung beberapa materi yang berhubungan dengan keamanan jaringan komputer, yaitu mulai dari *footprinting*, *scanning network*, dan *CVE*. Dimana dalam setiap topik-topik tersebut terdapat bagian-bagian lagi yang akan dibahas selanjutnya. Berikut merupakan penjelasan singkat dari setiap topik handson yang telah dilakukan:

a. Footprinting

Dalam proses ini terdapat beberapa step yang dilakukan, bisa dilakukan dalam terminal kali linux atau web browser. Diantaranya yaitu :

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.

- WhatWeb

WhatWeb merupakan sebuah tools enumeration web information gathering yang mempunyai fungsi untuk mencari informasi-informasi DNS(Domain Name Server), lokasi server, sub-domain, versi php, jenis database, ip addres, cms yang digunakan dan lain-lain.

- Netcraft

Netcraft adalah sebuah Perusahaan Jasa Internet yang berbasis di Bath, Inggris. Dan bergerak di bidang IT Security yang fungsinya melayani pelanggannya terutama di bidang keamanan Website, salah satu Tools yang dibuatnya adalah Netcraft Anti-Phising Toolbar.

- Reverse Domain

Reverse DNS adalah mapping alamat IP ke suatu nama domain. Jadi kebalikan dari DNS (forward/normal DNS) yang mapping nama domain ke alamat IP.

- Web Archive

Internet Archive adalah sebuah perpustakaan digital nirlaba yang memiliki misi "akses universal untuk semua pengetahuan. Internet

Archive menyediakan penyimpanan permanen dan akses publik bebas untuk koleksi bahan digital, termasuk situs web, musik, gambar bergerak, dan hampir tiga juta buku domain publik.

b. Scanning Network

Network scanning adalah metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/Network yang maksud

c. CVE (Common Vulnerabilities and Exposures)

Common Vulnerabilities and Exposures menyediakan metode referensi untuk kerentanan keamanan dan eksposur informasi yang diketahui. National Cybersecurity FFRDC, dioperasikan oleh Mitre Corporation, main, dengan dana dari Divisi Keamanan Cyber Nasional Departemen Keamanan Dalam Negeri Amerika Serikat.

2. Hasil dan Analisa

Pada percobaan yang pertama yaitu melakukan proses semacam identifikasi dari sebuah website, dimana website yang digunakan pada percobaan ini adalah website unsri.ac.id. Dengan menggunakan command "whois" pada terminal linux dan dilanjutkan dengan nama website maka akan di dapatkan hasil yang menjelaskan dengan sangat jelas data-data dari domain web tersebut, seperti gambar dibawah ini :

```
File Edit View Search Terminal Help

massgt:-# whois unsri.ac.id

Domain ID:PANDI-Do228145

Domain Name:UNSRI.AC.ID

Created On:01-Sep-1999 13:32:27 UTC

Last Updated On:15-Oct-2017 22:57:10 UTC

Expiration Date:31-Oct-2019 23:59:59 UTC

Status:clientTransferProhibited

Status:serverTransferProhibited

Registrant ID:candr12

Registrant Name:Candra Setiawan

Registrant Street1:31. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236 Pakjo

Registrant Street2:31. Raya Palembang - Prabumulih Km. 32 Indralaya, 0I, Sumatera Selatan

Registrant Street2:31. Raya Palembang - Prabumulih Km. 32 Indralaya, 0I, Sumatera Selatan

Registrant Street2:31. Raya Palembang - Prabumulih Km. 32 Indralaya, 0I, Sumatera Selatan

Registrant Street2:31. Raya Palembang

Registrant Country:ID

Registrant Country:ID

Admin Name:Candra Setiawan

Admin Organization:unsri

Admin Name:Candra Setiawan

Admin Organization:unsri

Admin Street1:31. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236

Admin Country:ID

Admin Pane:+00.00000000

Admin FAX:+00.00000000

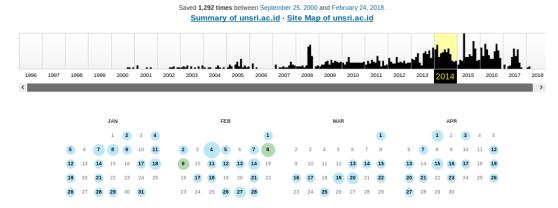
Admin FAX:+00.000000
```

Dari gambar diatas dapat dilihat dalam web dengan domain name unsri.ac.id data yang sangat lengkap mulai dari nama pendaftar, alamat, tanggal daftar, tanggal expired, danlain sebagainya. Dengan data-data tersebut dapat memudahkan siapa saja

untuk memperoleh informasi yang bisa dugunakan untuk segala macam hal. Berikutnya merupakan gambar dari hasil command whatweb:

```
massgt:~# whatweb www.unsri.ac.id
http://www.unsri.ac.id [200 OK] Cookies[PHPSESSID], Country[INDONESIA][ID], Emai
l[yadiutama@unsri.ac.id], Google-Analytics[Universal][UA-68096542-1,UA-9289835-
1], HTTPServer[nginx], IP[103.241.4.11], JQuery[1.2.6], Meta-Author[yadiutama@un
sri.ac.id], PHP[5.3.10-lubuntu3.25], Passwordfield[password], Script[text/javasc
ript], Title[.:: Halaman Utama | Universitas Sriwijaya - Indralaya, Sumatera Sel
atam], X-Powered-By[PHP/5.3.10-lubuntu3.25], nginx
massgt:~#
```

Dari hasil command whatweb situs unsri.ac.id didapatkan hasil data-data pribadi admin, dan data-data lain yang jelas mengenai web unsri.ac.id itu sendiri. Seperti country, email, HTTPServer menggunakan nginx, IP 103.241.4.11, dan lain sebagainya. Selanjutnya hasil dari web archive, utuk yang ini tidak menggunakan terminal di kali linux tetapi melalui web browser :



Pada gambar diatas menunjukkan hasil dari pencarian situs unsri.ac.id pada web.archive.org dan menampilkan arsip pada tahun 2014, disana terlihat ada beberapa lingkaran pada tanggal disetiap bulan dan itu menunjukkan bahwa pada setiap lingkaran tersebut menandakan jika pada tanggal itu situs web yang berkaitan melakukan satu kali update atau sejenisnya. Sedangakan untuk lingkaran dengan warna lebih gelap menandakan dua kali.

```
File Edit View Search Terminal Help

massgt:~# nmap -sV 103.241.4.1

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-14 01:08 WIB

Nmap scan report for ip-103-241-4-1.unsri.ac.id (103.241.4.1)

Host is up (0.038s latency).

Not shown: 991 closed ports

PORT STATE SERVICE VERSION

22/tcp open tcpwrapped

23/tcp open tcpwrapped

25/tcp filtered smtp

80/tcp open nagios-nsca Nagios NSCA

179/tcp open tcpwrapped

2000/tcp open bandwidth-test MikroTik bandwidth-test server

8181/tcp open http MikroTik router config httpd

8291/tcp open unknown

9090/tcp filtered zeus-admin

Service Info: OS: RouterOS; Device: router; CPE: cpe:/o:mikrotik:routeros

Service detection performed. Please report any incorrect results at https://nmap

.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 159.43 seconds
```

Gambar sebelumnya yaitu hasil dari proses scanning menggunakan nmap yang bertujuan untuk melihat port-port yang terbuka dengan command nmap –sV 103.241.4.1, disana terlihat bahwa dari hasil yang didapat ada beberapa port yang terbuka diantaranya yaitu port 22, 23, 80, 179, 2000, 8181, 8291, dan dengan protokol tcp. Tetapi dari semua port yang terbuka tersebut tidak semuanya memiliki versi yang sama antara satu sama lain. Selanjutnya yaitu scanning untuk melihat sistem operasi yang digunakan :

```
File Edit View Search Terminal Help

Not shown: 989 closed ports

PORT STATE SERVICE
21/tcp open ftp
22/tcp filtered ssh
25/tcp filtered smtp
53/tcp open domain
80/tcp open http
11/tcp open rpcbind
443/tcp open https
8000/tcp open http-alt
8080/tcp filtered http-proxy
9090/tcp filtered zeus-admin
10000/tcp open snet-sensor-mgmt
Aggressive 05 guesses: OpenWrt 12.09-rcl Attitude Adjustment (Linux 3.3 - 3.7) (
98%), Linux 3.13 or 4.2 (96%), XBMCbuntu Frodo v12.2 (Linux 3.X) (96%), Linux 3.2 - 3.8 (95%), Linux 2.6.32 - 3.1 (94%), Linux 3.2 (94%), Linux 2.6.32 - 3.13 (9
3%), Linux 3.8 (93%), Linux 3.2 - 3.10 (93%), Linux 3.2 - 3.16 (93%)
No exact 0S matches for host (test conditions non-ideal).
Network Distance: 8 hops

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/.
Nmap done: 1 IP address (1 host up) scanned in 8.80 seconds
massgt:~#
```

Pada gambar diatas menunjukkan hasil scanning *os type* menggunakan command nmap –O unsri.ac.id, yang bertujuan untuk mengidentifikasi sistem operasi yang digunakan. Dari gambar diatas dapat dilihat bahwa sistem operasi yang digunakan adalah linux yang mana terlihat ada beberapa jenis linux yang ada di dalam nya. Selanjutnya yaitu melakukan pencarian dalam CVE:

Sort Results By : CVE N	imber Descendi	ng CVE Numbe	r Ascending CVSS Score	Descending Nur	nber Of Exploits D	escending							
Total number of vulner	ubilities: 977 F	age: 1 (This P	age) 2 3 4 5 6 7 8 9	10 11 12 13	<u>14 15 16 17 18</u>	19 20							
Copy Results Download	Results												
# CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail
1 CVE-2012-0394	94	2	Exec Code	2012-01-08	2014-02-20	6.8	None	Remote	Medium	Not required	Partial	Partial	Parti
** DISPUTED ** The D behavior as not "a sec			t in Apache Struts before	2.3.1.1, when dev	veloper mode is u	sed, allows r	emote attackers to	execute arbit	trary commands vi	a unspecified vectors. N	IOTE: the ver	dor characte	erizes this
2 CVE-2014-2668	20	1	DoS	2014-03-28	2017-12-15	5.0	None	Remote	Low	Not required	None	None	Parti
E 012 202 1 2000	20												
	_	ws remote atta	ckers to cause a denial of	service (CPU an	d memory consu	mption) via th	he count parameter	to /_uuids.					
	_		ckers to cause a denial of DoS Exec Code Overflow +Info	service (CPU ar 2014-07-20	d memory consu 2017-12-08	mption) via ti	he count parameter None	Remote	Medium	Not required	Partial	Partial	Parti
Apache CouchDB 1.5.0 3 CVE-2014-0226 Race condition in the n	and earlier allo	1 ule in the Apach	DoS Exec Code	2014-07-20 4.10 allows remot	2017-12-08 be attackers to car	6.8 use a denial	None of service (heap-ba	Remote sed buffer ov	verflow), or possibly	, obtain sensitive crede	ntial informatio	n or execute	
Apache CouchDB 1.5.0 3 CVE-2014-0226 Race condition in the ri	and earlier allo	1 ule in the Apach	DoS Exec Code Overflow +Info e HTTP Server before 2.4	2014-07-20 4.10 allows remot	2017-12-08 be attackers to car	6.8 use a denial	None of service (heap-ba	Remote sed buffer ov	verflow), or possibly	, obtain sensitive crede	ntial informatio	n or execute	arbitrar
Apache CouchDB 1.5.0 3 CVE-2014-0226 Race condition in the mode, via a crafted req 4 CVE-2013-4212 Certain getText method	and earlier alk 362 od_status moduest that trigger 94 Is in the Actions	1 ule in the Apach s improper scor 1 Support controlle	DoS Exec Code Overflow +Info e HTTP Server before 2.4	2014-07-20 4.10 allows remote e status_handler: 2013-12-07 5.0.2 allow remote	2017-12-08 The attackers to calculate the attackers to calculate the attackers to expect the attackers the attac	6.8 use a denial es/generators	None of service (heap-bas/mod_status.c and	Remote sed buffer ov the lua_ap_s Remote	verflow), or possibly scoreboard_worker Medium	y obtain sensitive crede function in modules/lua Not required	ntial informatio /lua_request. Partial	n or execute	arbitrary Parti
Apache CouchDB 1.5.0 3 CVE-2014-0226 Race condition in the mode, via a crafted req 4 CVE-2013-4212 Certain getText method	and earlier alk 362 od_status moduest that trigger 94 Is in the Actions	ule in the Apach s improper scor 1 Support controlle .rol, which uses	DoS Exec Code Overflow +Info ee HTTP Server before 2. eboard handling within the er in Apache Roller before	2014-07-20 4.10 allows remote e status_handler: 2013-12-07 5.0.2 allow remote	2017-12-08 The attackers to calculate the attackers to calculate the attackers to expect the attackers the attac	6.8 use a denial es/generators	None of service (heap-bas/mod_status.c and	Remote sed buffer ov the lua_ap_s Remote	verflow), or possibly scoreboard_worker Medium	y obtain sensitive crede function in modules/lua Not required	ntial informatio /lua_request. Partial	n or execute	Parti in the
Apache CouchDB 1.5.3 3 CVE-2014-0226 Race condition in the mode, via a crafted req 4 CVE-2013-4212 Certain getText method getPage Title sub-URL 5 CVE-2013-1814	and earlier alk 362 od_status mod uest that trigger 94 is in the Action! to roller-ui/logir 200 in the User RF	ule in the Apach s improper scor Support controlle .rol, which uses 1 C API in Apach	DoS Exec Code Overflow -Hnfo the HTTP Server before 2. eboard handling within the ter in Apache Roller before a subclass of UlAction, 8	2014-07-20 4.10 allows remote status_handler: 2013-12-07 5.0.2 allow remote aka "OGNL Inject 2013-03-13	2017-12-08 te attackers to cal function in module 2017-08-28 te attackers to ex- tion." 2013-07-03	6.8 use a denial es/generators 6.8 ecute arbitra	None of service (heap-ba s/mod_status.c and None ry OGNL expression None	Remote sed buffer ov the lua_ap_s Remote ons via the fir	verflow), or possibly scoreboard_worker Medium st or second paran	y obtain sensitive crede function in modules/lue Not required neter, as demonstrated Single system	ntial information //ua_request. Partial by the pageTi	Partial None	Partii in the None
Apache CouchDB 1.5.1 3 CVE-2014-0226 Race condition in the nicode, via a crafted required to the condition of the condition	and earlier alk 362 od_status mod uest that trigger 94 is in the Action! to roller-ui/logir 200 in the User RF	ule in the Apact s improper scor Support controlle trol, which uses C API in Apach onse.	DoS Exec Code Overflow +Info ie HTTP Server before 2. eboard handling within the er in Apache Roller before a subclass of UlAction, 8 +Info	2014-07-20 4.10 allows remote status_handler: 2013-12-07 5.0.2 allow remote aka "OGNL Inject 2013-03-13	2017-12-08 te attackers to cal function in module 2017-08-28 te attackers to ex- tion." 2013-07-03	6.8 use a denial es/generators 6.8 ecute arbitra	None of service (heap-ba s/mod_status.c and None ry OGNL expression None	Remote sed buffer ov the lua_ap_s Remote ons via the fir	verflow), or possibly scoreboard_worker Medium st or second paran	y obtain sensitive crede function in modules/lue Not required neter, as demonstrated Single system	ntial information //ua_request. Partial by the pageTi	Partial None	Parti in the Non
Apache CouchDB 1.5.1 3 CVE-2014-0226 Race condition in the necode, via a crafted req 4 CVE-2013-4212 Certain getText method getPageTitle sub-URL 5 CVE-2013-1814 The users/get program hashes is the passwor	and earlier alidades 362 362 362 362 364 385 485 485 486 486 486 486 486 4	ule in the Apach s improper scor Support controlle .rol, which uses C API in Apach onse.	DoS Exec Code Overflow +Info the HTTP Server before 2. eboard handling within the r in Apache Roller before a subclass of UlAction, 8 +Info Rave 0.11 through 0.20	2014-07-20 4.10 allows remote status_handler! 2013-12-07 5.0.2 allow remote ka "OGNL Inject 2013-03-13 allows remote au 2012-06-21 in libwpd 0.8.8, a	2017-12-08 ue attackers to car unction in module 2017-08-28 te attackers to ex ion." 2013-07-03 thenticated users 2016-08-17 is used by OpenC	6.8 use a denial des/generators 6.8 ecute arbitra 4.0 to obtain set	None of service (heap-ba h/mod_status.c and None ry OGNL expression None nsitive information a	Remote sed buffer ov the lua_ap_s Remote ons via the fir. Remote sbout all user	verflow), or possibly scoreboard_worker Medium st or second paran Low accounts via the o	y obtain sensitive crede r function in modules/lue Not required neter, as demonstrated Single system ffset parameter, as dem	ntial informatic //ua_request. Partial by the pageTi Partial constrated by	Partial None Partial Partial	Partial Partia

Untuk proses yang ini yaitu mencari vurnability atau kerentanan suatu sistem, yang di gunakan untuk mecari kerentanannya pada kali ini yaitu apcahe. Dari hasil diatas dapat dilihat terdapat beberapa hasil, hasil tersebut beragam score kerentanannya, semakin besar score nya maka semakin besar pula kerentanannya.