

TUGAS KEAMANAN JARINGAN

“ Scanning “



OLEH :

NAMA : MARDIAH

NIM : 09011281320005

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

INDERALAYA

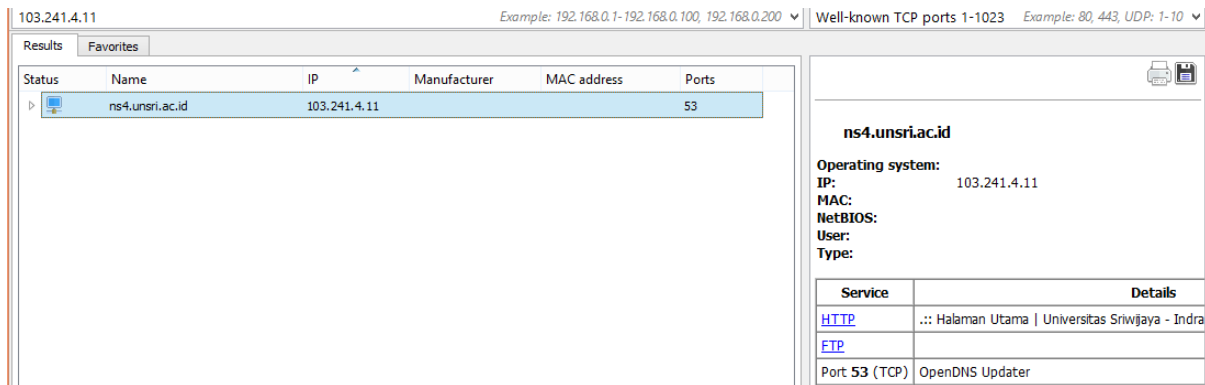
2017

Target : www.unsri.ac.id

IP : 103.241.4.11

Network scanner adalah metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/Network korban. Scanner biasanya bekerja dengan men-scan port TCP /IP dan servis servisnya dan mencatat respon dari komputer target. Dari scanner ini dapat diperoleh informasi mengenai port-port mana saja yang terbuka.

1. Pertama disini menggunakan tools port scanner kemudian masukkan ip address dari domain yang akan di scan, ip address domain diketahui dari tugas sebelumnya. Dengan menggunakan port scanner ini di dapat informasi yaitu salah satu port yang digunakan pada domain unsri.ac.id yaitu port 53 TCP. Berikut merupakan hasil scanning menggunakan port scanner :




2. Kedua menggunakan tools NetCraft dengan memasukkan nama domain yang akan di scan. Pada tools netcraft didapatkan informasi berupa history dari domain tersebut. Dengan begitu secara tidak langsung didapatkan informasi web server serta sistem operasi yang digunakan oleh universitas sriwijaya. Adapun sistem operasi yang digunakan oleh universitas sriwijaya yaitu linux dan menggunakan beberapa web server yaitu : Nginx, Apache, Nginx / 1.1.19, Apache / 2.2.22 Ubuntu, Apache / 2.2.3 Centos dan Apache / 2.2.8 Fedora. Berikut merupakan hasil scanning menggunakan NetCraft :

Background

Site title	::: Halaman Utama Universitas Sriwijaya - Indralaya, Sumatera Selatan	Date first seen	June 2000
Site rank		Primary language	Indonesian
Description	Not Present		
Keywords	Not Present		

Network

Site	http://unsri.ac.id	Netblock Owner	Universitas Sriwijaya
Domain	unsri.ac.id	Nameserver	ns4.unsri.ac.id
IP address	103.241.4.11	DNS admin	admin@unsri.ac.id
IPv6 address	Not Present	Reverse DNS	ns4.unsri.ac.id
Domain registrar	pandi.or.id	Nameserver organisation	whois.pandi.or.id
Organisation	Universitas Sriwijaya, Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236 Pakjo, Jln. Raya Palembang - Prabumulih Km. 32 Indralaya, OI, Sumatera Selatan, Palembang, 30138, Indonesia	Hosting company	unsri.ac.id
Top Level Domain	Indonesia (.ac.id)	DNS Security Extensions	unknown
Hosting country	 ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Universitas Sriwijaya University / Direct Member IDNIC Jl. Raya Palembang - Prabumulih Km. 32 Indralaya, Ogan Iilir Sumatera Selatan 30662, Indonesia	103.241.4.11	Linux	nginx	20-Feb-2017
Universitas Sriwijaya University / Direct Member IDNIC Jl. Raya Palembang - Prabumulih Km. 32 Indralaya, Ogan Iilir Sumatera Selatan 30662, Indonesia	103.241.4.11	Linux	nginx/1.1.19	24-Apr-2016
Universitas Sriwijaya University / Direct Member IDNIC Jl. Raya Palembang - Prabumulih Km. 32 Indralaya, Ogan Iilir Sumatera Selatan 30662, Indonesia	103.241.4.11	Linux	Apache	3-Mar-2016
PT Telkom Indonesias customer.	222.124.194.11	Linux	Apache	2-Nov-2013
PT Telkom Indonesias customer.	222.124.194.11	Linux	Apache/2.2.22 Ubuntu	25-Nov-2012
PT Telkom Indonesias customer.	222.124.194.11	Linux	Apache	6-Sep-2012
PT Telkom Indonesias customer.	222.124.194.11	Linux	Apache/2.2.3 CentOS	6-Aug-2012
PT Telkom Indonesias customer.	222.124.194.11	Linux	unknown	1-Mar-2011
PT Telkom Indonesias customer.	222.124.194.11	Linux	Apache/2.2.3 CentOS	26-Feb-2011
PT Telkom Indonesias customer.	222.124.194.11	Linux	Apache/2.2.8 Fedora	23-Mar-2009

3. Tools yang ketiga yaitu menggunakan Nmap. Pada Nmap juga memasukkan domain yang akan di scan. Dari scanning yang telah dilakukan dapat diketahui bahwa universitas sriwijaya memiliki 1000 port yang bisa discanning, namun dari 100 port yang tersedia, port yang dalam kondisi terbuka hanya 6 port, port dalam kondisi filtered ada 4 port, dan sisanya 90 adalah port yang tertutup.

⇒ Pada Nmap didapatkan informasi port – port yang open pada universitas sriwijaya yaitu :

Port 111 / tcp 103.241.4.11

Port 21 / tcp 103.241.4.11

Port 443 / tcp 103.241.4.11

Port 53 / tcp 103.241.4.11

Port 88 / tcp 103.241.4.11

Port 10000 / tcp 103.241.4.11

Port – port di atas yaitu melakukan service ftp, ssh, domain, rpcbind dan http

```
Starting Nmap 6.00 ( http://nmap.org ) at 2017-02-22 09:34 EET
NSE: Loaded 17 scripts for scanning.
Initiating SYN Stealth Scan at 09:34
Scanning ns4.unsri.ac.id (103.241.4.11) [100 ports]
Discovered open port 111/tcp on 103.241.4.11
Discovered open port 21/tcp on 103.241.4.11
Discovered open port 443/tcp on 103.241.4.11
Discovered open port 53/tcp on 103.241.4.11
Discovered open port 80/tcp on 103.241.4.11
Discovered open port 10000/tcp on 103.241.4.11
Completed SYN Stealth Scan at 09:34, 1.99s elapsed (100 total ports)
Initiating Service scan at 09:34
Scanning 6 services on ns4.unsri.ac.id (103.241.4.11)
Completed Service scan at 09:34, 11.66s elapsed (6 services on 1 host)
Initiating RPCGrind Scan against ns4.unsri.ac.id (103.241. at 09:34
Completed RPCGrind Scan against ns4.unsri.ac.id (103.241. at 09:34, 0.45s elapsed (1 port)
Initiating OS detection (try #1) against ns4.unsri.ac.id (103.241.4.11)
Retrying OS detection (try #2) against ns4.unsri.ac.id (103.241.4.11)
Initiating Traceroute at 09:35
Completed Traceroute at 09:35, 1.41s elapsed
NSE: Script scanning 103.241.4.11.
Initiating NSE at 09:35
Completed NSE at 09:35, 30.29s elapsed
```

[+] Nmap scan report for ns4.unsri.ac.id (103.241.4.11)

Host is up (0.21s latency).
Not shown: 93 closed ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.0.8 or later
22/tcp	filtered	ssh	
53/tcp	open	domain	ISC BIND 9.8.1-P1
80/tcp	open	http	nginx
111/tcp	open	rpcbind (rpcbind V2-4)	2-4 (rpc #100000)
443/tcp	open	http	nginx
10000/tcp	open	http	MiniServ 1.831 (Webmin httpd)

Device type: WAP|media device|general purpose|webcam|specialized|storage-misc
Running (JUST GUESSING): Netgear embedded (96%), Western Digital embedded (96%), Linux 2.6.X|3.X|2.4.X (95%), AXIS Linux 2.6
OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3 cpe:/o:axis:linux:2.6 cpe:/o:crestron:2_series cpe:/o:linux:kernel:2.4

Aggressive OS guesses: Netgear DG834G WAP or Western Digital WD TV media player (96%), Linux 2.6.38 - 3.2 (95%), Linux 3.0 -
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 8.858 days (since Mon Feb 13 12:59:50 2017)
Network Distance: 9 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 3389/tcp)

```
HOP RTT      ADDRESS
 1  2.07 ms   router1-lon.linode.com (212.111.33.229)
 2  55.00 ms  109.74.207.10
 3  81.87 ms  195.66.226.8
 4  30.29 ms  195.66.226.8
 5  238.70 ms 180.240.193.78
 6  256.09 ms 180.240.193.78
 7  217.41 ms 198.subnet222-124-73.p2p.telkom.net.id (222.124.73.198)
 8  234.85 ms 198.subnet222-124-73.p2p.telkom.net.id (222.124.73.198)
 9  227.48 ms ns4.unsri.ac.id (103.241.4.11)
```

OS and Service detection performed. Please report any incorrect results at <http://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 57.40 seconds
Raw packets sent: 266 (15.242KB) | Rcvd: 472 (32.896KB)

```
devi@devi-Lenovo-Z40-75 ~ $ nmap unsri.ac.id
Starting Nmap 7.01 ( https://nmap.org ) at 2017-02-22 15:10 WIB
Nmap scan report for unsri.ac.id (103.241.4.11)
Host is up (0.083s latency).
Other addresses for unsri.ac.id (not scanned): 64:ff9b::67f1:40b
rDNS record for 103.241.4.11: ns4.unsri.ac.id
Not shown: 991 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    filtered ssh
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
10000/tcp open  snet-sensor-mgmt
27352/tcp filtered unknown
```

⇒ Selanjutnya setelah melakukan scanning domain menggunakan netcraft didapatkan web server yang digunakan oleh domain tersebut. Disini universitas sriwijaya menggunakan beberapa jenis web server di antaranya :

Nginx / 1.1.19, Apache / 2.2.22 Ubuntu, Apache / 2.2.3 Centos dan Apache / 2.2.8 Fedora. Berikut penjelasan beberapa web server diatas berdasarkan CVE :

Name	Description
CVE-2013-5704	The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."
CVE-2012-4557	The mod_proxy_ajp module in the Apache HTTP Server 2.2.12 through 2.2.21 places a worker node into an error state upon detection of a long request-processing time, which allows remote attackers to cause a denial of service (worker consumption) via an expensive request.

Name	Description
CVE-2012-1006	Multiple cross-site scripting (XSS) vulnerabilities in Apache Struts 2.0.14 and 2.2.3 allow remote attackers to inject arbitrary web script or HTML via the (1) name or (2) lastName parameter to struts2-showcase/person/editPerson.action, or the (3) clientName parameter to struts2-rest-showcase/orders.
CVE-2011-2087	Multiple cross-site scripting (XSS) vulnerabilities in component handlers in the javatemplates (aka Java Templates) plugin in Apache Struts 2.x before 2.2.3 allow remote attackers to inject arbitrary web script or HTML via an arbitrary parameter value to a .action URI, related to improper handling of value attributes in (1) FileHandler.java, (2) HiddenHandler.java, (3) PasswordHandler.java, (4) RadioHandler.java, (5) ResetHandler.java, (6) SelectHandler.java, (7) SubmitHandler.java, and (8) TextFieldHandler.java.
CVE-2011-1772	Multiple cross-site scripting (XSS) vulnerabilities in XWork in Apache Struts 2.x before 2.2.3, and OpenSymphony XWork in OpenSymphony WebWork, allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) an action name, (2) the action attribute of an s:submit element, or (3) the method attribute of an s:submit element.
CVE-2007-1743	suexec in Apache HTTP Server (httpd) 2.2.3 does not verify combinations of user and group IDs on the command line, which might allow local users to leverage other vulnerabilities to create arbitrary UID/GID owned files if /proc is mounted. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root." In addition, because this is dependent on other vulnerabilities, perhaps this is resultant and should not be included in CVE.
CVE-2007-1742	suexec in Apache HTTP Server (httpd) 2.2.3 uses a partial comparison for verifying whether the current directory is within the document root, which might allow local users to perform unauthorized operations on incorrect directories, as demonstrated using "html_backup" and "htmleditor" under an "html" directory. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root."
CVE-2007-1741	Multiple race conditions in suexec in Apache HTTP Server (httpd) 2.2.3 between directory and file validation, and their usage, allow local users to gain privileges and execute arbitrary code by renaming directories or performing symlink attacks. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root."
CVE-2006-3747	Off-by-one error in the ldap scheme handling in the Rewrite module (mod_rewrite) in Apache 1.3 from 1.3.28, 2.0.46 and other versions before 2.0.59, and 2.2, when RewriteEngine is enabled, allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via crafted URLs that are not properly handled using certain rewrite rules.

Name	Description
CVE-2008-2364	The ap_proxy_http_process_response function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server 2.0.63 and 2.2.8 does not limit the number of forwarded interim responses, which allows remote HTTP servers to cause a denial of service (memory consumption) via a large number of interim responses.

Name	Description
CVE-2012-2089	Buffer overflow in ngx_http_mp4_module.c in the ngx_http_mp4_module module in nginx 1.0.7 through 1.0.14 and 1.1.3 through 1.1.18, when the mp4 directive is used, allows remote attackers to cause a denial of service (memory overwrite) or possibly execute arbitrary code via a crafted MP4 file.