

# TUGAS



*Oleh :*

Romi Bagaskara  
09121001015

SISTEM KOMPUTER  
UNIVERSITAS SRIWIJAYA  
PALEMBANG  
2016

Berikut ini adalah hasil Scanning pada domain [www.indowebster.com](http://www.indowebster.com) menggunakan Nmap – ZenMap GUI :

```
Nmap Output | Ports / Hosts | Topology | Host Details | Scans
nmap -p 1-65535 -T4 -A -v www.indowebster.com

Starting Nmap 7.11 ( https://nmap.org ) at 2016-03-26 03:12 Pacific Daylight Time
NSE: Loaded 138 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:12
Completed NSE at 03:12, 0.00s elapsed
Initiating NSE at 03:12
Completed NSE at 03:12, 0.00s elapsed
Initiating Ping Scan at 03:12
Scanning www.indowebster.com (175.103.59.41) [4 ports]
Completed Ping Scan at 03:12, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:12
Completed Parallel DNS resolution of 1 host. at 03:12, 13.00s elapsed
Initiating SYN Stealth Scan at 03:12
Scanning www.indowebster.com (175.103.59.41) [65535 ports]
Discovered open port 443/tcp on 175.103.59.41
Discovered open port 80/tcp on 175.103.59.41
Completed SYN Stealth Scan at 03:13, 51.54s elapsed (65535 total ports)
Initiating Service scan at 03:13
Scanning 2 services on www.indowebster.com (175.103.59.41)
Completed Service scan at 03:13, 18.48s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www.indowebster.com (175.103.59.41)
Retrying OS detection (try #2) against www.indowebster.com (175.103.59.41)
Initiating Traceroute at 03:13
Completed Traceroute at 03:13, 0.11s elapsed
Initiating Parallel DNS resolution of 12 hosts. at 03:13
Completed Parallel DNS resolution of 12 hosts. at 03:13, 13.00s elapsed
NSE: Script scanning 175.103.59.41.
Initiating NSE at 03:13
Completed NSE at 03:15, 70.97s elapsed
Initiating NSE at 03:15
Completed NSE at 03:15, 0.00s elapsed
Nmap scan report for www.indowebster.com (175.103.59.41)
Host is up (0.014s latency).
Other addresses for www.indowebster.com (not scanned): 175.103.59.241
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx
443/tcp   open  ssl/https nginx

Nmap Output | Ports / Hosts | Topology | Host Details | Scans
nmap -p 1-65535 -T4 -A -v www.indowebster.com

|_ http-methods:
|_ Supported Methods: HEAD
|_ http-robots.txt: 23 disallowed entries (15 shown)
|_ /report/File/* /profile/microsoft* /profile/windows*
|_ /microsoft /microsoft* /windows /windows* /all/microsoft
|_ /all/microsoft* /all/windows /all/windows*
|_ /category/video/microsoft* /category/video/microsoft /category/video/windows*
|_ /category/video/windows
|_ http-server-header: krn
443/tcp    open  ssl/https nginx
|_ http-robots.txt: 23 disallowed entries (15 shown)
|_ /report/File/* /profile/microsoft* /profile/windows*
|_ /microsoft /microsoft* /windows /windows* /all/microsoft
|_ /all/microsoft* /all/windows /all/windows*
|_ /category/video/microsoft* /category/video/microsoft /category/video/windows*
|_ /category/video/windows
|_ http-server-header: krn
|_ http-title: 400 The plain HTTP request was sent to HTTPS port
|_ ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ ssl-date: 2016-03-25T08:12:04+00:00; -ld02h0im47s from scanner time.
|_ tls-nextprotoneg:
|_ http/1.1
Device type: general purpose|WAP|broadband router|printer|webcam
Running (JUST GUESSING): Linux 2.6.X|2.4.X (94%), Asus embedded (89%), Lexmark embedded (85%), AXIS embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:asus:rt-ac66u cpe:/h:asus:rt-n16 cpe:/o:linux:linux_kernel:2.4.20 cpe:/h:lexmark:x644e
cpe:/h:axis:211_network_camera cpe:/o:linux:linux_kernel:2.6.20
Aggressive OS guesses: Linux 2.6.18 - 2.6.22 (94%), Tomato firmware (Linux 2.6.22) (89%), Asus RT-AC66U router (Linux 2.6) (89%), Asus RT-N16 WAP (Linux 2.6) (89%),
Asus RT-N66U WAP (Linux 2.6) (89%), Tomato 1.28 (Linux 2.6.22) (89%), Tomato 1.27 - 1.28 (Linux 2.4.20) (87%), Tomato 1.28 (Linux 2.4.20) (86%), Lexmark X644e
printer (85%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 17.553 days (since Tue Mar 08 12:58:11 2016)
Network Distance: 12 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Randomized

TRACEROUTE (using port 199/tcp)
HOP RTT ADDRESS
1 0.00 ms 192.168.100.1
2 0.00 ms 180.254.160.1

Nmap Output | Ports / Hosts | Topology | Host Details | Scans
nmap -p 1-65535 -T4 -A -v www.indowebster.com

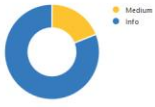
|_ http/1.1
Device type: general purpose|WAP|broadband router|printer|webcam
Running (JUST GUESSING): Linux 2.6.X|2.4.X (94%), Asus embedded (89%), Lexmark embedded (85%), AXIS embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:asus:rt-ac66u cpe:/h:asus:rt-n16 cpe:/o:linux:linux_kernel:2.4.20 cpe:/h:lexmark:x644e
cpe:/h:axis:211_network_camera cpe:/o:linux:linux_kernel:2.6.20
Aggressive OS guesses: Linux 2.6.18 - 2.6.22 (94%), Tomato firmware (Linux 2.6.22) (89%), Asus RT-AC66U router (Linux 2.6) (89%), Asus RT-N16 WAP (Linux 2.6) (89%),
Asus RT-N66U WAP (Linux 2.6) (89%), Tomato 1.28 (Linux 2.6.22) (89%), Tomato 1.27 - 1.28 (Linux 2.4.20) (87%), Tomato 1.28 (Linux 2.4.20) (86%), Lexmark X644e
printer (85%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 17.553 days (since Tue Mar 08 12:58:11 2016)
Network Distance: 12 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Randomized

TRACEROUTE (using port 199/tcp)
HOP RTT ADDRESS
1 0.00 ms 192.168.100.1
2 0.00 ms 180.254.160.1
3 0.00 ms 125.160.0.29
4 0.00 ms 61.94.115.205
5 32.00 ms 118.98.63.249
6 32.00 ms 157.subnet118-98-62.astinet.telkom.net.id (118.98.62.157)
7 32.00 ms 61.94.177.185
8 32.00 ms 61.94.117.237
9 16.00 ms 122.subnet125-160-9.speedy.telkom.net.id (125.160.9.122)
10 94.00 ms 218.100.36.2
11 31.00 ms 218.100.27.30
12 31.00 ms 175.103.59.41

NSE: Script Post-scanning.
Initiating NSE at 03:15
Completed NSE at 03:15, 0.00s elapsed
Initiating NSE at 03:15
Completed NSE at 03:15, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 180.22 seconds
Raw packets sent: 65821 (2.898MB) | Rcvd: 65784 (2.633MB)
```

Dari hasil scanning diatas, domain [www.indowebster.com](http://www.indowebster.com) menggunakan OS Linux Kernel 2.2 dan memiliki dua buah port yang terbuka, yaitu port 80/tcp dan port 443/tcp. Port 80/tcp merupakan port HTTP World Wide Web dari domain itu sendiri dan port 443/tcp adalah protokol yang didefinisikan untuk berkomunikasi tergantung pada aplikasi.

Untuk scanning domain [www.indowebster.com](http://www.indowebster.com) menggunakan Nessus, berikut ini adalah hasil scan pertama melalui Nessus :

Severity	Plugin Name	Plugin Family	Count	Host Details
MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	DNS	1	<b>Host Details</b> IP: 175.103.59.241 DNS: www.indowebster.com OS: Linux Kernel 2.2-4br /> Linux Kernel 2.4-4br /> Linux Kernel 2.6 Start: March 26 at 3:46 AM End: March 26 at 3:55 AM Elapsed: 9 minutes KB: <a href="#">Download</a>  <b>Vulnerabilities</b> 
MEDIUM	DNS Server Spoofed Request Amplification DDoS	DNS	1	
MEDIUM	SSL Certificate Cannot Be Trusted	General	1	
MEDIUM	SSL Certificate Expiry	General	1	
MEDIUM	SSL Version 2 and 3 Protocol Detection	Service detection	1	
INFO	Service Detection	Service detection	3	
INFO	Nessus SYN scanner	Port scanners	2	
INFO	Additional DNS Hostnames	General	1	
INFO	Common Platform Enumeration (CPE)	General	1	
INFO	Device Type	General	1	
INFO	DNS Server Detection	DNS	1	
INFO	Host Fully Qualified Domain Name (FGDN) Resolution	General	1	
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1	
INFO	Nessus Scan Information	Settings	1	
INFO	Network Time Protocol (NTP) Server Detection	Service detection	1	
INFO	OpenSSL Detection	Service detection	1	
INFO	OS Identification	General	1	
INFO	SSL / TLS Versions Supported	General	1	
INFO	SSL Certificate Information	General	1	
INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1	
INFO	SSL Cipher Suites Supported	General	1	
INFO	SSL Perfect Forward Secrecy Cipher Suites Supported	General	1	
INFO	TCP/IP Timestamps Supported	General	1	
INFO	TLS Next Protocols Supported	General	1	
INFO	TLS NPN Supported Protocol Enumeration	Misc.	1	
INFO	Traceroute Information	General	1	

Setelah mendapatkan hasil scan kemudian memilih “DNS Server Spoofed Request Amplification DDoS”, telah didapat CVE nya yaitu “CVE-2006-0987”

**MEDIUM** DNS Server Spoofed Request Amplification DDoS

---

**Description**

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone (".") and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

**Solution**

Restrict access to your DNS server from public network or reconfigure it to reject such queries.

**See Also**

<https://isc.sans.edu/diary/DNS+queries+for+/5713>

**Output**

```
The DNS query was 17 bytes long, the answer is 512 bytes long.
```

Port	Hosts
53 / udp / dns	www.indowebster.com

**Plugin Details**

Severity: Medium  
 ID: 35450  
 Version: \$Revision: 1.12 \$  
 Type: remote  
 Family: DNS  
 Published: 2009/01/22  
 Modified: 2015/11/18

---

**Risk Information**

Risk Factor: Medium  
 CVSS Base Score: 5.0  
 CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

---

**Reference Information**

[CVE: CVE-2006-0987](#)  
 OSVDB: 25895

Berikut adalah mapping CVE dari domain [www.indowebster.com](http://www.indowebster.com) :

CVE-ID	
<b>CVE-2006-0987</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
The default configuration of ISC BIND before 9.4.1-P1, when configured as a caching name server, allows recursive queries and provides additional delegation information to arbitrary IP addresses, which allows remote attackers to cause a denial of service (traffic amplification) via DNS queries with spoofed source IP addresses.	

CVE-ID	
<b>CVE-2007-0987</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Directory traversal vulnerability in index.php in Jupiter CMS 1.1.5 allows remote attackers to include and execute arbitrary local files via a .. (dot dot), or an absolute pathname, in the n parameter.	

CVE-ID	
<b>CVE-2008-0987</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Stack-based buffer overflow in Image Raw in Apple Mac OS X 10.5.2, and Digital Camera RAW Compatibility before Update 2.0 for Aperture 2 and iPhoto 7.1.2, allows remote attackers to execute arbitrary code via a crafted Adobe Digital Negative (DNG) image.	

CVE-ID	
<b>CVE-2009-0987</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Unspecified vulnerability in the Upgrade component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, and 10.2.0.3 allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	

CVE-ID	
<b>CVE-2010-0987</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Heap-based buffer overflow in Adobe Shockwave Player before 11.5.7.609 might allow remote attackers to execute arbitrary code via crafted embedded fonts in a Shockwave file.	

CVE-ID	
<b>CVE-2011-0987</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
The PMA_Bookmark_get function in libraries/bookmark.lib.php in phpMyAdmin 2.11.x before 2.11.11.3, and 3.3.x before 3.3.9.2, does not properly restrict bookmark queries, which makes it easier for remote authenticated users to trigger another user's execution of a SQL query by creating a bookmark.	