

# Tugas 2 Keamanan Jaringan Komputer



**Bramantio Rizki Nugroho**

**NIM 09121001044**

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

## Scanning

Target : humblebundle.com

Tools yang digunakan : Zenmap 7.40

Hasil scanning dengan Zenmap 7.40

Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -T4 -A -v humblebundle.com				
Scanning humblebundle.com (104.20.35.236) [4 ports]				
Completed Ping Scan at 18:47, 0.91s elapsed (1 total hosts)				
Initiating Parallel DNS resolution of 1 host. at 18:48				
Completed Parallel DNS resolution of 1 host. at 18:48, 13.00s elapsed				
Initiating SYN Stealth Scan at 18:48				
Scanning humblebundle.com (104.20.35.236) [1000 ports]				
Discovered open port 80/tcp on 104.20.35.236				
Discovered open port 443/tcp on 104.20.35.236				
Discovered open port 8080/tcp on 104.20.35.236				
Discovered open port 8443/tcp on 104.20.35.236				
Completed SYN Stealth Scan at 18:48, 4.58s elapsed (1000 total ports)				
Initiating Service scan at 18:48				
Scanning 4 services on humblebundle.com (104.20.35.236)				
Completed Service scan at 18:48, 12.24s elapsed (4 services on 1 host)				

Hasil Pengamatan 1

1. IP target 104.20.35.236
2. Terdapat 1000 port
3. Menggunakan protocol tcp
4. Port yang open yaitu ; port 80, port 443, port 8080, port 8443

Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -T4 -A -v humblebundle.com				
Discovered open port 8443/tcp on 104.20.35.236				
Completed SYN Stealth Scan at 18:48, 4.58s elapsed (1000 total ports)				
Initiating Service scan at 18:48				
Scanning 4 services on humblebundle.com (104.20.35.236)				
Completed Service scan at 18:48, 12.24s elapsed (4 services on 1 host)				
Initiating OS detection (try #1) against humblebundle.com (104.20.35.236)				
Retrying OS detection (try #2) against humblebundle.com (104.20.35.236)				
Initiating Traceroute at 18:48				
Completed Traceroute at 18:48, 3.04s elapsed				
Initiating Parallel DNS resolution of 6 hosts. at 18:48				
Completed Parallel DNS resolution of 6 hosts. at 18:48, 13.00s elapsed				
<u>NSE:</u> Script scanning 104.20.35.236.				
Initiating NSE at 18:48				
Completed NSE at 18:49, 8.64s elapsed				
Initiating NSE at 18:49				
Completed NSE at 18:49, 0.00s elapsed				
Nmap scan report for humblebundle.com (104.20.35.236)				
Host is up (0.030s latency).				
Other addresses for humblebundle.com (not scanned): 104.20.34.236				
<u>Not shown:</u> 996 filtered ports				

## Hasil Pengamatan 2

1. Host sedang up dengan 0.030s latency
2. Ada IP lain target yang tidak ter-scan yaitu 104.20.34.236
3. Ada 996 port yang tidak ditampilkan karena telah di filtered

Berikut open port pada target :

Nmap Output					
Ports / Hosts					
Topology					
Host Details					
Scans					
Port	Protocol	State	Service	Version	
80	tcp	open	http	Cloudflare nginx	
443	tcp	open	http	Cloudflare nginx	
8080	tcp	open	http	Cloudflare nginx	
8443	tcp	open	http	Cloudflare nginx	

Berikut OS yang digunakan target :

Nmap Output

Ports / Hosts

Topology

Host Details

Scans

humblebundle.com (104.20.35.236)

Host Status

State: up

Open ports: 4



Filtered ports: 996

Closed ports: 0

Scanned ports: 1000

Up time: Not available

Last boot: Not available

Addresses

IPv4: 104.20.35.236

IPv6: Not available

MAC: Not available

Hostnames

Name - Type: humblebundle.com - user

Operating System

Name: Linux 3.18

Accuracy: 88%

Ports used

Port-Protocol-State: 80 - tcp - open

OS Classes

Type

Vendor

OS Family

OS Generation

Accuracy

general purpose

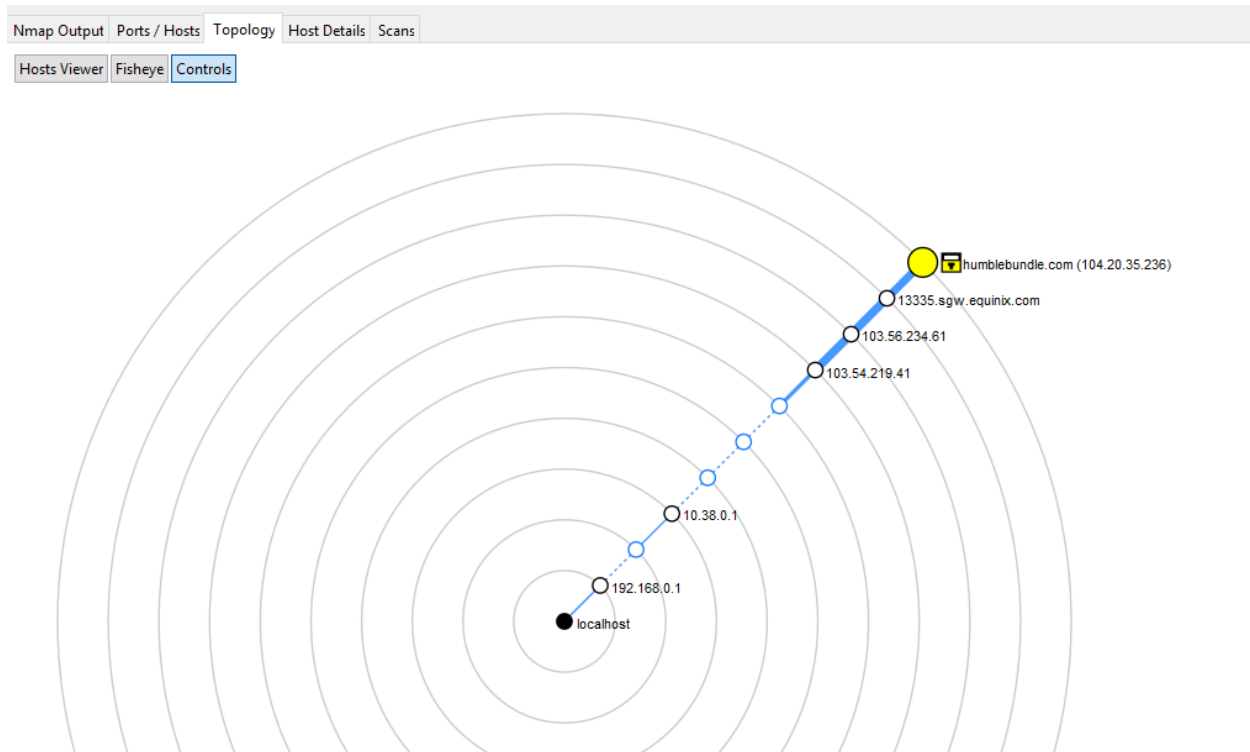
Linux

Linux

3.X

88%

Berikut topology hasil scanning :



Berikut beberapa CVE-id dari “nginx”

## [Nginx](#) » [Nginx](#) : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[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	<a href="#">CVE-2016-4450</a>			DoS	2016-06-07	2016-11-28	5.0	None	Remote	Low	Not required	None	None	Partial
os/unix/nginx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.														
2	<a href="#">CVE-2016-1247</a> <a href="#">59</a>			+Priv	2016-11-29	2017-02-23	7.2	Admin	Local	Low	Not required	Complete	Complete	Complete
The nginx package before 1.6.2-5+deb8u3 on Debian jessie, the nginx packages before 1.4.6-1ubuntu3.6 on Ubuntu 14.04 LTS, before 1.10.0-0ubuntu0.16.04.3 on Ubuntu 16.04 LTS, and before 1.10.1-0ubuntu1.1 on Ubuntu 16.10, and the nginx build before 1.10.2-r3 on Gentoo allow local users with access to the web server user account to gain root privileges via a symlink attack on the error log.														
3	<a href="#">CVE-2016-0747</a> <a href="#">399</a>			DoS	2016-02-15	2016-12-05	5.0	None	Remote	Low	Not required	None	None	Partial
The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 does not properly limit CNAME resolution, which allows remote attackers to cause a denial of service (worker process resource consumption) via vectors related to arbitrary name resolution.														
4	<a href="#">CVE-2016-0746</a>			DoS	2016-02-15	2016-12-05	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Use-after-free vulnerability in the resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (worker process crash) or possibly have unspecified other impact via a crafted DNS response related to CNAME response processing.														
5	<a href="#">CVE-2016-0742</a>			DoS	2016-02-15	2016-12-05	5.0	None	Remote	Low	Not required	None	None	Partial
The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (invalid pointer dereference and worker process crash) via a crafted UDP DNS response.														
6	<a href="#">CVE-2014-3616</a> <a href="#">284</a>				2014-12-08	2014-12-08	4.3	None	Remote	Medium	Not required	None	Partial	None
nginx 0.5.6 through 1.7.4, when using the same shared ssl_session_cache or ssl_session_ticket_key for multiple servers, can reuse a cached SSL session for an unrelated context, which allows remote attackers with certain privileges to conduct "virtual host confusion" attacks.														
7	<a href="#">CVE-2014-3556</a> <a href="#">77</a>				2014-12-29	2015-03-16	4.3	None	Remote	Medium	Not required	Partial	None	None
The STARTTLS implementation in mail/nginx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack, a similar issue to CVE-2011-0411.														
8	<a href="#">CVE-2011-4315</a> <a href="#">119</a>			DoS Overflow	2011-12-08	2017-01-31	5.0	None	Remote	Low	Not required	None	None	Partial
Heap-based buffer overflow in compression-pointer processing in core/nginx_resolver.c in nginx before 1.0.10 allows remote resolvers to cause a denial of service (daemon crash) or possibly have unspecified other impact via a long response.														

9	<a href="#">CVE-2010-2266</a>	<a href="#">20</a>	1 DoS Dir. Trav. Mem. Corr.	2010-06-15	2010-06-15	5.0	None	Remote	Low	Not required	None	None	Partial
<p>nginx 0.8.36 allows remote attackers to cause a denial of service (crash) via certain encoded directory traversal sequences that trigger memory corruption, as demonstrated using the "%c0.%c0." sequence.</p>													
10	<a href="#">CVE-2010-2263</a>	<a href="#">200</a>	2 +Info	2010-06-15	2010-06-18	5.0	None	Remote	Low	Not required	Partial	None	None
<p>nginx 0.8 before 0.8.40 and 0.7 before 0.7.66, when running on Windows, allows remote attackers to obtain source code or unparsed content of arbitrary files under the web document root by appending ::\$DATA to the URI.</p>													
11	<a href="#">CVE-2009-3898</a>	<a href="#">22</a>	Dir. Trav.	2009-11-24	2012-06-08	4.9	None	Remote	Medium	Single system	Partial	Partial	None
<p>Directory traversal vulnerability in src/http/modules/nginx_http_dav_module.c in nginx (aka Engine X) before 0.7.63, and 0.8.x before 0.8.17, allows remote authenticated users to create or overwrite arbitrary files via a .. (dot dot) in the Destination HTTP header for the WebDAV (1) COPY or (2) MOVE method.</p>													
12	<a href="#">CVE-2009-3896</a>	<a href="#">119</a>	DoS Overflow	2009-11-24	2013-09-11	5.0	None	Remote	Low	Not required	None	None	Partial
<p>src/http/nginx_http_parse.c in nginx (aka Engine X) 0.1.0 through 0.4.14, 0.5.x before 0.5.38, 0.6.x before 0.6.39, 0.7.x before 0.7.62, and 0.8.x before 0.8.14 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a long URI.</p>													
13	<a href="#">CVE-2009-2629</a>	<a href="#">119</a>	Exec Code Overflow	2009-09-15	2009-12-19	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
<p>Buffer underflow in src/http/nginx_http_parse.c in nginx 0.1.0 through 0.5.37, 0.6.x before 0.6.39, 0.7.x before 0.7.62, and 0.8.x before 0.8.15 allows remote attackers to execute arbitrary code via crafted HTTP requests.</p>													
<p>Total number of vulnerabilities : 13    Page : <a href="#">1</a> (This Page)</p>													