

TUGAS

“KEAMANAN JARINGAN KOMPUTER”



Disusun Oleh :

Nama : Nova Dyati Pradista

Nim : 09011181320005

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA**

2017

TUGAS 2 : SCANNING

Berikut ditampilkan hasil dari scanning dengan domain www.tokopedia.com menggunakan Nmap:

Nmap output



```
Starting Nmap 6.46 ( http://nmap.org ) at 2017-02-22 16:00 SE Asia Standard Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 16:00
Scanning tokopedia.com (182.253.224.188) [4 ports]
Completed Ping Scan at 16:00, 0.34s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:00
Completed Parallel DNS resolution of 1 host. at 16:00, 15.53s elapsed
Initiating SYN Stealth Scan at 16:00
Scanning tokopedia.com (182.253.224.188) [1000 ports]
Discovered open port 443/tcp on 182.253.224.188
Discovered open port 80/tcp on 182.253.224.188
Discovered open port 53/tcp on 182.253.224.188
SYN Stealth Scan Timing: About 3.85% done; ETC: 16:13 (0:12:54 remaining)
SYN Stealth Scan Timing: About 5.70% done; ETC: 16:18 (0:16:49 remaining)
Increasing send delay for 182.253.224.188 from 0 to 5 due to 11 out of 16 dropped probes since last increase.
SYN Stealth Scan Timing: About 7.40% done; ETC: 16:20 (0:18:59 remaining)
SYN Stealth Scan Timing: About 10.55% done; ETC: 16:23 (0:20:21 remaining)
Increasing send delay for 182.253.224.188 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
```



```
SYN Stealth Scan Timing: About 24.40% done; ETC: 16:25 (0:19:13 remaining)
SYN Stealth Scan Timing: About 31.40% done; ETC: 16:26 (0:17:53 remaining)
SYN Stealth Scan Timing: About 36.65% done; ETC: 16:26 (0:16:34 remaining)
SYN Stealth Scan Timing: About 42.15% done; ETC: 16:26 (0:15:13 remaining)
SYN Stealth Scan Timing: About 48.05% done; ETC: 16:27 (0:13:51 remaining)
SYN Stealth Scan Timing: About 53.40% done; ETC: 16:27 (0:12:30 remaining)
SYN Stealth Scan Timing: About 58.70% done; ETC: 16:27 (0:11:09 remaining)
SYN Stealth Scan Timing: About 63.85% done; ETC: 16:27 (0:09:46 remaining)
SYN Stealth Scan Timing: About 68.90% done; ETC: 16:27 (0:08:24 remaining)
SYN Stealth Scan Timing: About 73.90% done; ETC: 16:27 (0:07:03 remaining)
SYN Stealth Scan Timing: About 78.85% done; ETC: 16:27 (0:05:42 remaining)
SYN Stealth Scan Timing: About 83.90% done; ETC: 16:27 (0:04:20 remaining)
SYN Stealth Scan Timing: About 88.95% done; ETC: 16:27 (0:02:59 remaining)
SYN Stealth Scan Timing: About 94.00% done; ETC: 16:27 (0:01:37 remaining)
Completed SYN Stealth Scan at 16:26, 1541.56s elapsed (1000 total ports)
Initiating Service scan at 16:26
Scanning 3 services on tokopedia.com (182.253.224.188)
Completed Service scan at 16:26, 6.08s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against tokopedia.com (182.253.224.188)
Retrying OS detection (try #2) against tokopedia.com (182.253.224.188)
Initiating Traceroute at 16:26
Completed Traceroute at 16:26, 9.18s elapsed
Initiating Parallel DNS resolution of 1 host. at 16:26
Completed Parallel DNS resolution of 1 host. at 16:26, 0.00s elapsed
```

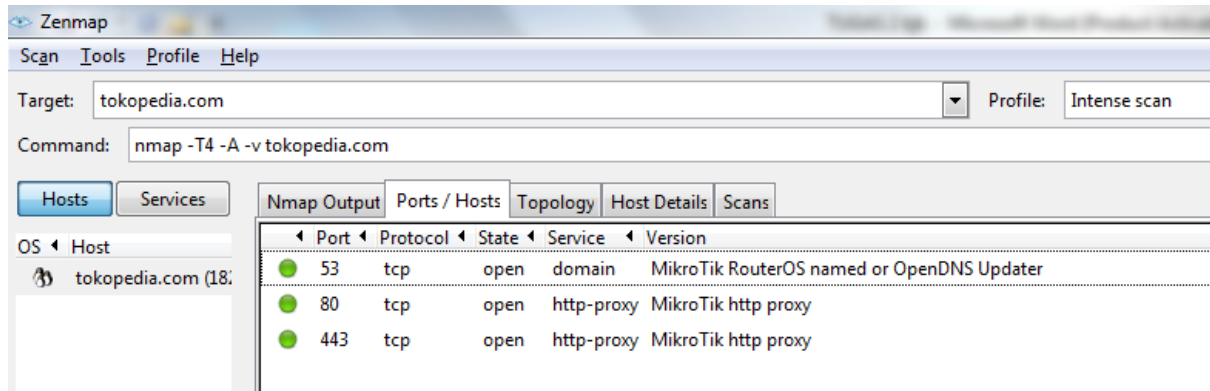


```
NSE: Script scanning 182.253.224.188.
Initiating NSE at 16:26
Completed NSE at 16:28, 144.50s elapsed
Nmap scan report for tokopedia.com (182.253.224.188)
Host is up (0.025s latency).
Other addresses for tokopedia.com (not scanned): 182.253.224.184
Not shown: 951 filtered ports, 46 closed ports
PORT      STATE SERVICE        VERSION
53/tcp    open  domain        MikroTik RouterOS named or OpenDNS Updater
80/tcp    open  http-proxy    MikroTik http proxy
443/tcp   open  http-proxy    MikroTik http proxy
Device type: phone|WAP
Running (JUST GUESSING): Linux 2.6.X|2.4.X (88%)
OS_CPE: cpe:/o:linux:linux_kernel:2.6.24 cpe:/o:linux:linux_kernel:2.4
Aggressive OS guesses: Linux 2.6.24 (Palm Pre mobile phone) (88%), DD-WRT v24-sp1 (Linux 2.4.36) (88%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 27.699 days (since Wed Jan 25 23:42:11 2017)
TCP Sequence Prediction: Difficulty=203 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 2725/tcp)
HOP RTT      ADDRESS
1 5.00 ms hotspot-id1.ilkom.unsri.ac.id (10.100.224.1)
2 ... 30

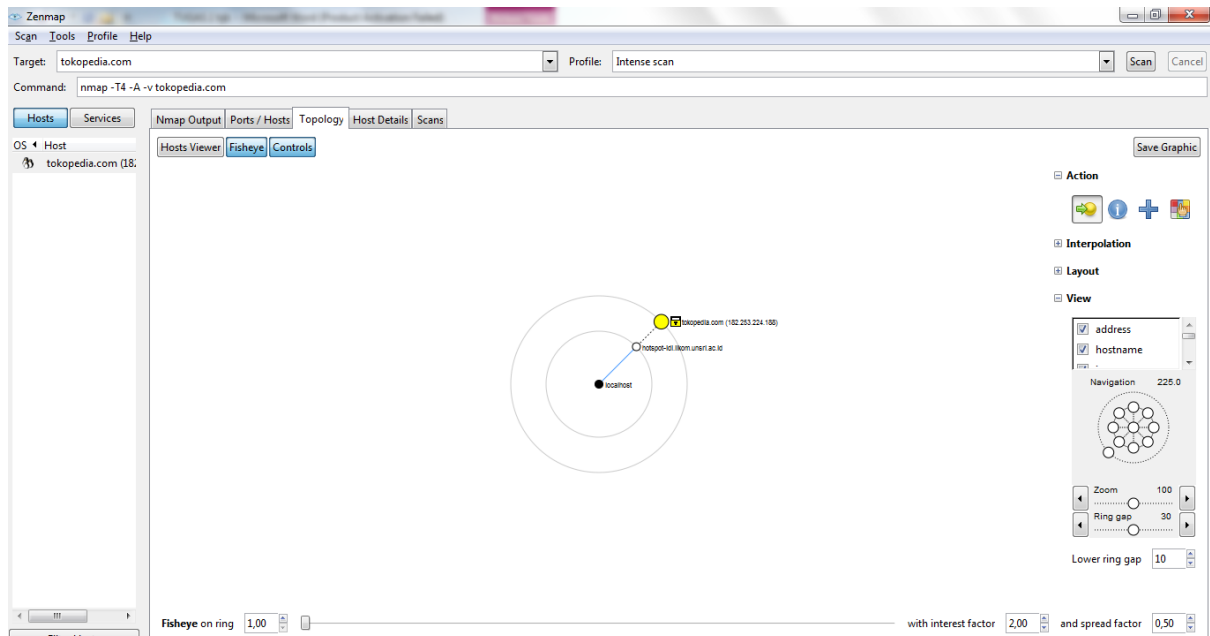
NSE: Script Post-scanning.
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1726.20 seconds
Raw packets sent: 2309 (106.612KB) | Rcvd: 97 (4.460KB)
```

Ports / Hosts



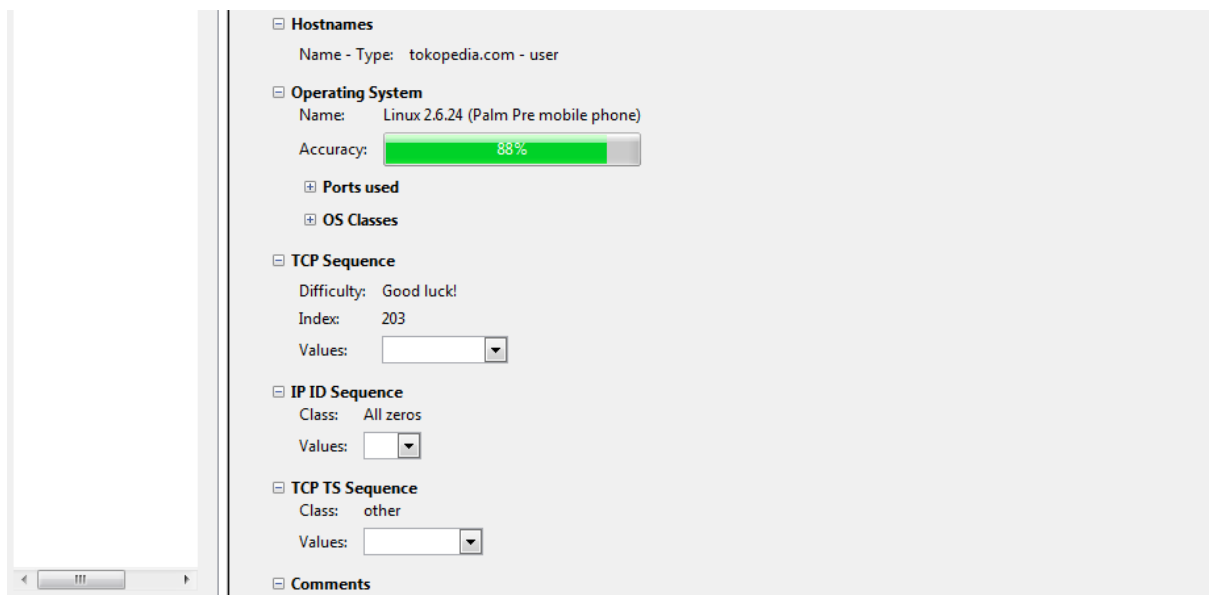
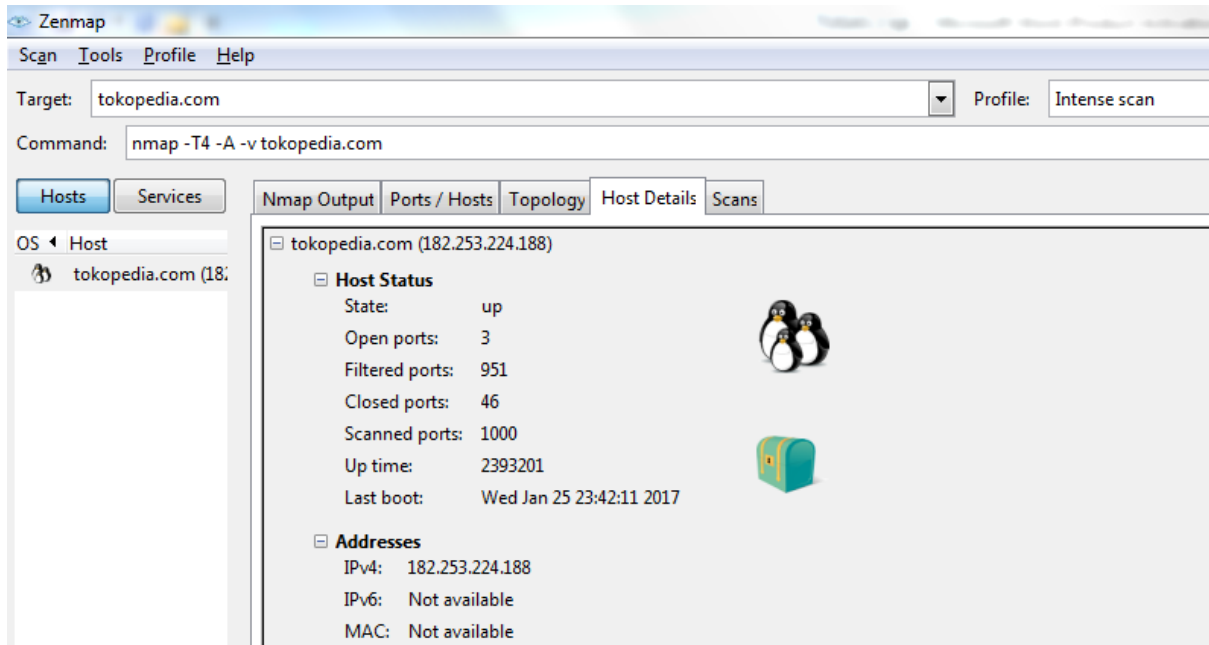
Gambar diatas menunjukkan port / host dari alamat domain www.tokoprdia.com yang memiliki 3 layanan service yaitu domain Mikrotik RouterOS named or OpenDNS Updater dengan port 53, http-proxy MikroTik http proxy dengan port 80, http-proxy MikroTik http proxy dengan port 443 yang masing – masing menggunakan protocol tcp dengan state open.

Topology



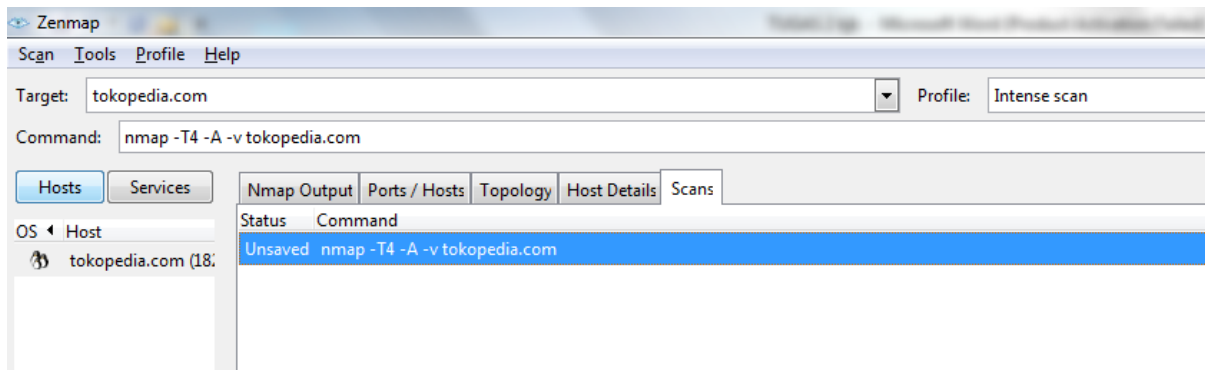
Gambar diatas menunjukkan topology dari alamat domain www.tokopedia.com 182.253.224.188 yang terhubung melalui localhost dari hotspot-idl-ikom.unsri.ac.id

Host details



Gambar diatas menunjukkan host details dengan alamat domain www.tokopedia.com 182.253.224.188 yang menampilkan masing – masing berupa host status, addresses, hostname, operating system, port used, os classes, tcp sequence, IP ID sequence, TCP TS sequence dan comments

Scans



Gambar diatas menunjukkan scans dari alamat domain www.tokopedia.com yang menunjukkan berupa status command unsave nmap-T4-v tokopedia.com

Hasil dari CVE www.tokopedia.com



Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

[Search CVE List](#) | [Download CVE](#) | [Update an ID](#) | [Request a CVE ID](#)

HOME > CVE > SEARCH RESULTS

Home | [CVE IDs](#) | [About CVE](#) | [Compatible Products & More](#) | [Community](#) | [Blog](#) | [News](#) | [Site Search](#)

TOTAL CVE IDs: **81977**

Section Menu

- CVE IDs**
 - Updates & Feeds
- Request a CVE ID**
 - Contact a CVE Numbering Authority (CNA)
 - Contact Primary CNA (MITRE) - CVE Request web form
 - Reservation Guidelines
- CVE LIST (all existing CVE IDs)**
 - Downloads
 - Search CVE List
 - Search Tips
 - View Entire CVE List (html)
- Reference Key/Maps
- NVD Advanced CVE Search**
 - CVE ID Scoring Calculator
- CVE Numbering Authorities**
 - Participating CNAs
 - Documentation for CNAs
 - Requesting CVE IDs from CNAs
- Documentation**
 - About CVE IDs
 - Terminology
 - Editorial Policies
 - Terms of Use
- ALSO SEE**
 - Common Vulnerability Scoring System (CVSS)
 - Common Vulnerability Reporting Framework (CVRP)
 - U.S. National Vulnerability Database (NVD)

Search Results

There are **9** CVE entries that match your search.

Name	Description
CVE-2014-9585	The vdso_addr function in arch/x86/vdso/vma.c in the Linux kernel through 3.18.2 does not properly choose memory locations for the vDSO area, which makes it easier for local users to bypass the ASLR protection mechanism by guessing a location at the end of a PMD.
CVE-2008-4315	tog-pegasus in OpenGroup Pegasus 2.7.0 on Red Hat Enterprise Linux (RHEL) 5, Fedora 9, and Fedora 10 does not log failed authentication attempts to the OpenPegasus CIM server, which makes it easier for remote attackers to avoid detection of password guessing attacks.
CVE-2008-2285	The ssh-vulnkey tool on Ubuntu Linux 7.04, 7.10, and 8.04 LTS does not recognize authorized_keys lines that contain options, which makes it easier for remote attackers to exploit CVE-2008-0166 by guessing a key that was not identified by this tool.
CVE-2006-4326	Stack-based buffer overflow in Justsystem Ichitaro 9.x through 13.x, Ichitaro 2004, 2005, 2006, and Government 2006; Ichitaro for Linux; and FormLiner before 20060818 allows remote attackers to execute arbitrary code via long Unicode strings in a crafted document, as being actively exploited by malware such as Trojan.Tarodrop. NOTE: some details are obtained from third party information.
CVE-2005-3106	Race condition in Linux 2.6, when threads are sharing memory mapping via CLONE_VM (such as linuxthreads and vfork), might allow local users to cause a denial of service (deadlock) by triggering a core dump while waiting for a thread that has just performed an exec.
CVE-2001-0851	Linux kernel 2.0, 2.2 and 2.4 with syncookies enabled allows remote attackers to bypass firewall rules by brute force guessing the cookie.
CVE-2000-0357	ORBit and esound in Red Hat Linux 6.1 do not use sufficiently random numbers, which allows local users to guess the authentication keys.
CVE-2000-0118	The Red Hat Linux su program does not log failed password guesses if the su process is killed before it times out, which allows local attackers to conduct brute force password guessing.
CVE-2000-0109	The mcsp Client Site Processor system (MultiCSP) in Standard and Poor's ComStock is installed with several accounts that have no passwords or easily guessable default passwords.

[BACK TO TOP](#)

SEARCH CVE USING KEYWORDS:

You can also search by reference using the [CVE Reference Maps](#).

For More Information: cve@mitre.org

Kesimpulan :

Scanning merupakan kegiatan probe dalam jumlah yang besar dengan menggunakan tool secara otomatis. Tool tersebut secara otomatis dapat mengetahui port – port pada saat host lokal maupun host remote, ip address yang aktif, bahkan bisa untuk mengetahui sistem operasi yang digunakan pada host yang dituju. Tool scanner yang saya gunakan adalah Nmap.

Scanning dapat dibedakan menjadi 3 yaitu :

- Port scanning, dilakukan untuk mengetahui service apa yang dijalankan oleh target berdasarkan well known ports.
- Network scanning, dilakukan untuk mengetahui aktifnya satu host dan ip address dari host tersebut.
- Vulnerability scanning, dilakukan untuk mengetahui sistem operasi, versi sistem operasi, maupun service pack yang digunakan.

Umumnya port scanning tools akan melakukan probe ke host target yang mudah di deteksi oleh IDS. Network scanning maupun vulnerability scanning juga mudah di deteksi oleh IDS, karena tetap melakukan interaksi dengan target.