

**TUGAS KEAMANAN SISTEM INFORMASI**

**“FOOTPRINTING”**

**DOSEN PENGAMPU:**

**Gede Arna Jude Saskara, S.T.,M.T**

---



**Oleh:**

**I Gede Riyan Ardi Darmawan**

**(1815091037)**

**Sistem Informasi Kelas 4A**

**PROGRAM STUDI SISTEM INFORMASI**

**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK DAN KEJURUAN**

**UNIVERSITAS PENDIDIKAN GANESHA**

**TAHUN AKADEMIK 2019/2020**

**TUGAS 8 - KEAMANAN SISTEM INFORMASI**

Mata Kuliah : Keamanan Sistem Informasi

Kode Mata Kuliah : SIF1433-AmanSI

SKS : 3 SKS

Dosen Pengampu : Gede Arna Jude Saskara, S.T.,M.T

**Instruksi :**

Buatlah Tabel Target seperti yang terdapat pada materi (Berisi 5 Kolom yaitu : Nama, IP, Alive, OS, Service/ Port) dengan minimal 5 server/domain selain [www.undiksha.ac.id](http://www.undiksha.ac.id) dan [www.tokopedia.com](http://www.tokopedia.com) (masing-masing mahasiswa tidak boleh ada yang sama) (buat dokumentasi cara mencari data-data tersebut 1 website saja foto dokumentasi diberi watermark nama dan nim)

**Jawab :****Tabel Target :**

Nama	IP Address	Alive	OS Server	Services/Port Open
<a href="http://www.youtube.com">www.youtube.com</a>	172.217.31.78	Yes	OpenBSD 4.4	http (port 80), https (port 443)
<a href="http://www.kali.org">www.kali.org</a>	192.124.249.10	Yes	CatOS 7.6, CatOS 8.3	http (port 80), https (port 443)
<a href="http://www.ubuntu.com">www.ubuntu.com</a>	91.189.91.44 91.189.88.181 91.189.91.45	Yes Yes Yes	Linux 2.0.35 - Linux 2.0.36	ssh (port 22), http (port 80), https (port 443), rsync (port 873), nrpe (port 5666), jetdirect (port 9103)
<a href="http://www.debian.org">www.debian.org</a>	128.31.0.62 130.89.148.77 149.20.4.15	Yes Yes Yes	<i>No OS Matches For Host</i>	http (port 80), https (port 443)
<a href="http://www.facebook.com">www.facebook.com</a>	157.240.217.35	Yes	<i>No OS Matches For Host</i>	http (port 80), https (port 443)
<a href="http://www.000webhost.com">www.000webhost.com</a>	104.20.67.46 104.20.68.46	Yes Yes	Linux 2.6.18 - 2.6.22	http (port 80), https (port 443), http-proxy (port 8080), https-alt (port 8443)

<a href="http://www.google.com">www.google.com</a>	216.239.38.120	Yes	OpenBSD 4.0	http (port 80), https (port 443)
<a href="http://www.redhat.com">www.redhat.com</a>	23.192.207.55	Yes	Linux 4.4, Linux 2.6.18 - 2.6.22	http (port 80), https (port 443)
<a href="http://www.xubuntu.org">www.xubuntu.org</a>	162.213.33.176	No	Linux 4.4	http (port 80), https (port 443)
<a href="http://www.linuxmint.com">www.linuxmint.com</a>	192.124.249.53	Yes	Linux 4.4, Linux 3.10 - 3.12, Linux 4.9, Linux 2.6.18 - 2.6.22,cLinux 3.10 - 3.16, Linux 4.0	http (port 80), https (port 443)

### Dokumentasi :

1. Cek apakah server dalam keadaan *alive* dengan perintah *ping* urlwebsite

Target : [www.google.com](http://www.google.com)

```

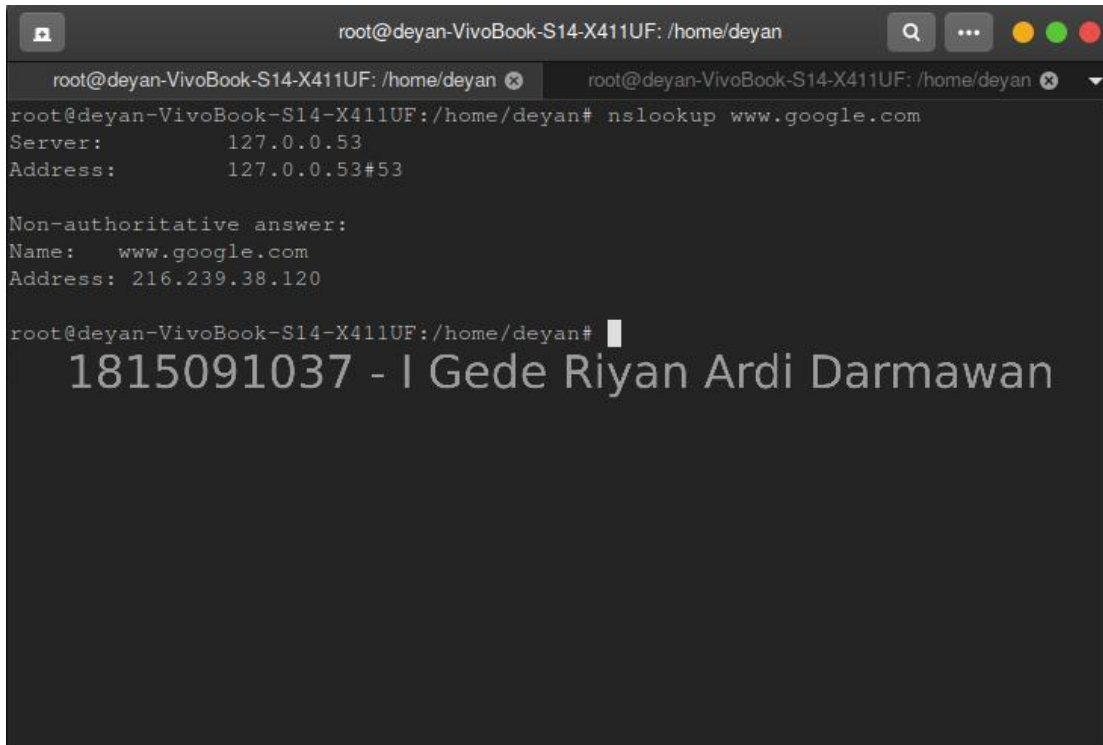
root@deyan-VivoBook-S14-X411UF: /home/deyan
root@deyan-VivoBook-S14-X411UF: /home/deyan
PING google.com (172.217.24.174) 56(84) bytes of data.
64 bytes from kul08s01-in-f14.1e100.net (172.217.24.174): icmp_seq=1 ttl=46 time
=68.0 ms
64 bytes from kul08s01-in-f14.1e100.net (172.217.24.174): icmp_seq=2 ttl=46 time
=66.0 ms
64 bytes from kul08s01-in-f14.1e100.net (172.217.24.174): icmp_seq=3 ttl=46 time
=85.1 ms
64 bytes from kul08s01-in-f14.1e100.net (172.217.24.174): icmp_seq=4 ttl=46 time
=90.5 ms
64 bytes from kul08s01-in-f14.1e100.net (172.217.24.174): icmp_seq=5 ttl=46 time
=83.4 ms
64 bytes from kul08s01-in-f14.1e100.net (172.217.24.174): icmp_seq=6 ttl=46 time
=81.5 ms
64 bytes from kul08s01-in-f14.1e100.net (172.217.24.174): icmp_seq=7 ttl=46 time
=77.3 ms
64 bytes from kul08s01-in-f14.1e100.net (172.217.24.174): icmp_seq=8 ttl=46 time
=75.7 ms
64 bytes from kul08s01-in-f14.1e100.net (172.217.24.174): icmp_seq=9 ttl=46 time
=83.5 ms
64 bytes from kul08s01-in-f14.1e100.net (172.217.24.174): icmp_seq=10 ttl=46 tim
e=102 ms
64 bytes from kul08s01-in-f14.1e100.net (172.217.24.174): icmp_seq=11 ttl=46 tim
e=72.3 ms

```

Dapat dipastikan server target dalam keadaan *alive*

2. Cek IP Address dengan perintah *nslookup* urlwebsite

Target : [www.google.com](http://www.google.com)



```

root@deyan-VivoBook-S14-X411UF: /home/deyan
root@deyan-VivoBook-S14-X411UF: /home/deyan# nslookup www.google.com
Server:          127.0.0.53
Address:         127.0.0.53#53

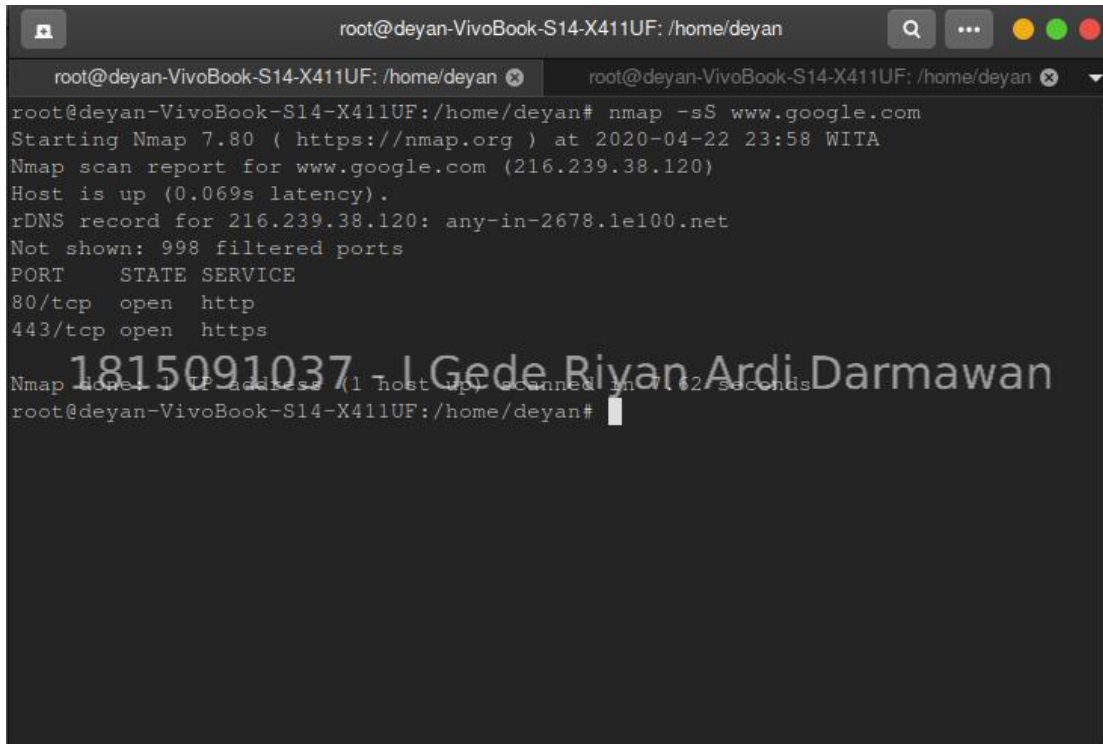
Non-authoritative answer:
Name:   www.google.com
Address: 216.239.38.120

root@deyan-VivoBook-S14-X411UF: /home/deyan#
  
```

Didapatkan bahwa alamat IP dari [www.google.com](http://www.google.com) adalah 216.239.38.120.

3. Cek port yang terbuka dengan perintah *nmap -sS* urlwebsite

Target : [www.google.com](http://www.google.com)



```

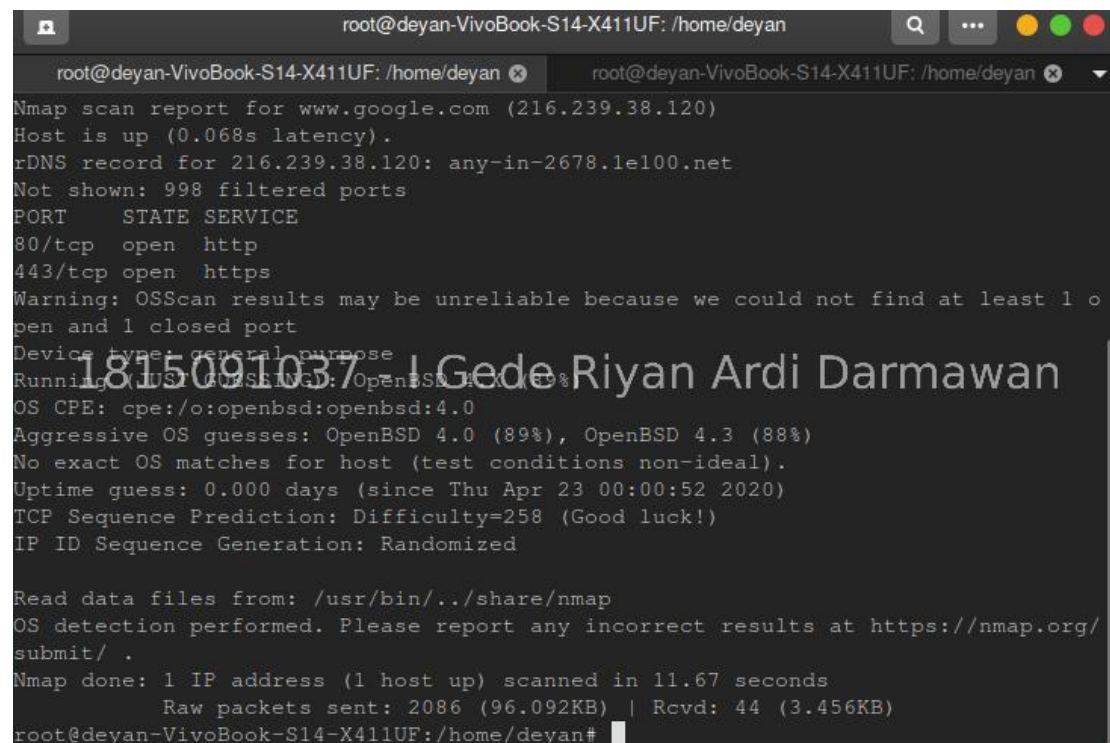
root@deyan-VivoBook-S14-X411UF: /home/deyan
root@deyan-VivoBook-S14-X411UF: /home/deyan# nmap -sS www.google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-22 23:58 WITA
Nmap scan report for www.google.com (216.239.38.120)
Host is up (0.069s latency).
rDNS record for 216.239.38.120: any-in-2678.1e100.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 7.62 seconds
root@deyan-VivoBook-S14-X411UF: /home/deyan#
  
```

Didapatkan bahwa [www.google.com](http://www.google.com) memiliki dua buah port yang terbuka yakni port 80 (http) dan port 443 (https).

4. Lakukan OS Fingerprinting dengan perintah `nmap -O -v urlwebsite -p nmapport` untuk mengecek melalui salah satu port yang terbuka atau `nmap -O -v urlwebsite` untuk mengecek secara keseluruhan melalui port yang terbuka

Target : [www.google.com](http://www.google.com)



```

root@deyan-VivoBook-S14-X411UF: /home/deyan
root@deyan-VivoBook-S14-X411UF: /home/deyan
Nmap scan report for www.google.com (216.239.38.120)
Host is up (0.068s latency).
rDNS record for 216.239.38.120: any-in-2678.1e100.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSED): OpenBSD 4.x (60%)
OS CPE: cpe:/o:openbsd:openbsd:4.0
Aggressive OS guesses: OpenBSD 4.0 (89%), OpenBSD 4.3 (88%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.000 days (since Thu Apr 23 00:00:52 2020)
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Randomized

Read data files from: /usr/bin/../../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.67 seconds
Raw packets sent: 2086 (96.092KB) | Rcvd: 44 (3.456KB)
root@deyan-VivoBook-S14-X411UF: /home/deyan#

```

Berdasarkan hal tersebut, didapatkan bahwa Operation System dari server [www.google.com](http://www.google.com) adalah OpenBSD 4.0 atau OpenBSD 4.3.

### Operation System :

Tugas ini dibuat dengan bantuan Linux Ubuntu 19.10 Operation System single boot.



