

KEAMANAN JARINGAN KOMPUTER

“scanning untuk mendapatkan data cve”



Disusun oleh :

Henny Pratiwi (09011281520129)

SISTEM KOMPUTER
FASILKOM INDERALAYA
UNIVERSITAS SRIWIJAYA
2018

Menggunakan software kali linux :

Foot printing

Untk mengetahui data seperti berikut :

```
root@kali:~# whois detik.com
Domain Name: DETIK.COM
Registry Domain ID: 1340701_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2017-07-27T08:19:18Z
Creation Date: 1998-05-29T04:00:00Z
Registry Expiry Date: 2018-05-28T04:00:00Z
Registrar: Network Solutions, LLC.
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS.DETIK.COM
Name Server: NS.DETIK.NET.ID
Name Server: NS1.DETIK.COM
Name Server: NS1.DETIK.NET.ID
Name Server: NS2.DETIK.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2018-03-14T07:45:55Z <<<
```

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

```
Domain Name: DETIK.COM
Registry Domain ID: 1340701_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2017-12-26T19:31:27Z
Creation Date: 1998-05-29T04:00:00Z
Registrar Registration Expiration Date: 2018-05-28T04:00:00Z
Registrar: NETWORK SOLUTIONS, LLC.
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
```

```
-----
Registry Registrant ID:
Registrant Name: Siberkom, PT. Agranet Multicitra
Registrant Organization:
Registrant Street: Aldevco Octagon Building lt 2
Registrant City: Jakarta
Registrant State/Province: DKI Jakarta
Registrant Postal Code: 12740
Registrant Country: IN
Registrant Phone: +62.217941177
Registrant Phone Ext:
Registrant Fax: +62.217941176
Registrant Fax Ext:
Registrant Email: sarwani@detik.com
Registry Admin ID:
Admin Name: Siberkom, PT. Agranet Multicitra
Admin Organization:
Admin Street: Aldevco Octagon Building lt 2
Admin City: Jakarta
Admin State/Province: DKI Jakarta
Admin Postal Code: 12740
Admin Country: IN
Admin Phone: +62.217941177
Admin Phone Ext:
Admin Fax: +62.217941176
Admin Fax Ext:
Admin Email: sarwani@detik.com
Registry Tech ID:
Tech Name: Siberkom, PT. Agranet Multicitra
Tech Organization:
Tech Street: Aldevco Octagon Building lt 2
```

```
root@kali:~# whatweb detik.com
http://detik.com [301 Moved Permanently] HTTPServer[nginx/id29], IP[103.49.221.211]
, RedirectLocation[http://www.detik.com/], Title[301 Moved Permanently], UncommonHe
aders[serverloc,x-content-type-options,access-control-allow-origin], X-XSS-Protection[1;mode=block], nginx[id29]
http://www.detik.com/ [200 OK] Frame, Google-Analytics[UA-51806390-1], HTML5, HTTPSe
rver[nginx/id24], IP[103.49.221.211], JQuery, Open-Graph-Protocol[article][1000006
07566694][187960271237149], Script[application/ld+json,text/javascript,text/x-handl
ebars], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[detik
com - Informasi Berita Terupdate Hari Ini], X-UA-Compatible[text], nginx[id24]
root@kali:~#
```

Scanning Network :

```
root@kali: ~
Berkas Sunting Tampilan Cari Terminal Bantuan
root@kali:~# ping 103.49.221.211
PING 103.49.221.211 (103.49.221.211) 56(84) bytes of data.
64 bytes from 103.49.221.211: icmp_seq=1 ttl=57 time=1044 ms
64 bytes from 103.49.221.211: icmp_seq=2 ttl=57 time=251 ms
64 bytes from 103.49.221.211: icmp_seq=3 ttl=57 time=308 ms
64 bytes from 103.49.221.211: icmp_seq=4 ttl=57 time=35.4 ms
64 bytes from 103.49.221.211: icmp_seq=6 ttl=57 time=653 ms
64 bytes from 103.49.221.211: icmp_seq=9 ttl=57 time=311 ms
64 bytes from 103.49.221.211: icmp_seq=10 ttl=57 time=171 ms
64 bytes from 103.49.221.211: icmp_seq=12 ttl=57 time=38.4 ms
64 bytes from 103.49.221.211: icmp_seq=13 ttl=57 time=59.7 ms
64 bytes from 103.49.221.211: icmp_seq=14 ttl=57 time=84.2 ms
64 bytes from 103.49.221.211: icmp_seq=15 ttl=57 time=264 ms
64 bytes from 103.49.221.211: icmp_seq=16 ttl=57 time=428 ms
64 bytes from 103.49.221.211: icmp_seq=17 ttl=57 time=90.0 ms
64 bytes from 103.49.221.211: icmp_seq=18 ttl=57 time=150 ms
64 bytes from 103.49.221.211: icmp_seq=19 ttl=57 time=29.8 ms
64 bytes from 103.49.221.211: icmp_seq=20 ttl=57 time=69.6 ms
64 bytes from 103.49.221.211: icmp_seq=21 ttl=57 time=77.6 ms
64 bytes from 103.49.221.211: icmp_seq=22 ttl=57 time=252 ms
64 bytes from 103.49.221.211: icmp_seq=23 ttl=57 time=73.1 ms
64 bytes from 103.49.221.211: icmp_seq=24 ttl=57 time=160 ms
64 bytes from 103.49.221.211: icmp_seq=25 ttl=57 time=1034 ms
64 bytes from 103.49.221.211: icmp_seq=26 ttl=57 time=434 ms
64 bytes from 103.49.221.211: icmp_seq=27 ttl=57 time=23.0 ms
64 bytes from 103.49.221.211: icmp_seq=28 ttl=57 time=200 ms
64 bytes from 103.49.221.211: icmp_seq=29 ttl=57 time=192 ms
64 bytes from 103.49.221.211: icmp_seq=30 ttl=57 time=35.7 ms
64 bytes from 103.49.221.211: icmp_seq=31 ttl=57 time=372 ms
64 bytes from 103.49.221.211: icmp_seq=32 ttl=57 time=60.8 ms
64 bytes from 103.49.221.211: icmp_seq=33 ttl=57 time=134 ms
root@kali:~# nmap -sP 103.49.221.211
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-14 15:21 WIB
Nmap scan report for 103.49.221.211
Host is up (0.14s latency).
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
root@kali:~# nmap -sP 103.49.221.211/24
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-14 15:22 WIB
Nmap scan report for 103.49.221.0
Host is up (0.0021s latency).
Nmap scan report for 103.49.221.1
Host is up (0.020s latency).
Nmap scan report for 103.49.221.2
Host is up (0.00069s latency).
Nmap scan report for 103.49.221.3
Host is up (0.00050s latency).
Nmap scan report for 103.49.221.4
root@kali:~# nmap -sV 103.49.211.211
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-14 15:26 WIB
Nmap scan report for 103.49.211.211
Host is up (0.012s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
554/tcp  open  rtsp      Hikvision 7513 POE IP camera rtspd
Service Info: Device: webcam

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 84.89 seconds
```

Scanning type os :

```
root@kali:~# nmap -O detik.com
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-14 15:53 WIB
Nmap scan report for detik.com (203.190.242.211)
Host is up (0.031s latency).
Other addresses for detik.com (not scanned): 103.49.221.211
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
8008/tcp  open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.89 seconds
root@kali:~#
```

```
root@kali:~# sudo nmap -O detik.com
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-14 15:56 WIB
Nmap scan report for detik.com (203.190.242.211)
Host is up (0.021s latency).
Other addresses for detik.com (not scanned): 103.49.221.211
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
8008/tcp  open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.33 seconds
```