

Nama : Pascal Adhi Kurnia Tarigan

NIM : 09011281520113

Scanning Open Port

Website Pemerintahan

<http://www.dpr.go.id/>

```
TARGET
-----
Domain http://www.dpr.go.id/
Server Banner: DPR Web Server
Target IP: 103.18.181.10

SERVER INFORMATION
-----
Ping:
PING www.dpr.go.id (103.18.181.10) 56(84) bytes of data.
64 bytes from 103.18.181.10 (103.18.181.10): icmp_seq=1 ttl=247 time=175 ms
64 bytes from 103.18.181.10 (103.18.181.10): icmp_seq=2 ttl=247 time=131 ms
64 bytes from 103.18.181.10 (103.18.181.10): icmp_seq=3 ttl=247 time=85.10 ms
64 bytes from 103.18.181.10 (103.18.181.10): icmp_seq=4 ttl=247 time=48.7 ms

--- www.dpr.go.id ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 48.741/110.133/175.075/47.418 ms

Traceroute:
traceroute to www.dpr.go.id (103.18.181.10), 30 hops max, 60 byte packets
 1 _gateway (192.168.43.1) 2.314 ms 2.149 ms 2.171 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 103.18.181.10 (103.18.181.10) 117.153 ms 117.027 ms 119.246 ms

Nslookup:
Server: 192.168.43.1
Address: 192.168.43.1#53

Non-authoritative answer:
*** Can't find www.dpr.go.id: No answer
Authoritative answers can be found from:
dpr.go.id
origin = ns-1109.awsdns-10.org
```

```
root@kali: ~
File Edit View Search Terminal Help
Completed NSE at 08:18, 12.25s elapsed
Initiating NSE at 08:18
Completed NSE at 08:18, 0.00s elapsed
Nmap scan report for m.detik.com (203.190.242.206)
Host is up (0.069s latency).
Other addresses for m.detik.com (not scanned): 103.49.221.206
rDNS record for 203.190.242.206: s2-206-242.190.203.detik.com
Not shown: 994 closed ports
PORT      STATE SERVICE VERSION
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    open  http   dtk21
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 301 Moved Permanently
|     Date: Tue, 19 Feb 2019 01:18:22 GMT
|     Content-Type: text/html
|     Content-Length: 182
|     Connection: close
|     Location: http://www.detik.com
|     Server: dtk21
|     X-XSS-Protection: 1;mode=block
|     X-Content-Type-Options: nosniff
|     Access-Control-Allow-Origin: *
```

```
root@kali: ~
File Edit View Search Terminal Help
| SF:Permanently</h1></center>\r\n<hr><center>nginx/dtx</center>\r\n</body>\
| SF:r\n</html>\r\n");
| Aggressive OS guesses: Linux 4.4 (91%), Linux 3.10 - 3.12 (90%), Linux 4.9 (89
% ), Linux 4.0 (88%), Linux 3.11 - 4.1 (87%), Linux 2.6.32 (87%), Linux 3.5 (87%)
, Linux 4.2 (87%), Synology DiskStation Manager 5.1 (87%), WatchGuard Firewall 1
1.8 (87%)
| No exact OS matches for host (test conditions non-ideal).
| Uptime guess: 32.408 days (since Thu Jan 17 22:31:24 2019)
| Network Distance: 11 hops
| TCP Sequence Prediction: Difficulty=254 (Good luck!)
| IP ID Sequence Generation: All zeros
|
| TRACEROUTE (using port 256/tcp)
| HOP RTT      ADDRESS
| 1  14.12 ms 192.168.43.1
| 2  ... 10
| 11 55.22 ms s2-206-242.190.203.detik.com (203.190.242.206)
|
| NSE: Script Post-scanning.
| Initiating NSE at 08:18
| Completed NSE at 08:18, 0.00s elapsed
| Initiating NSE at 08:18
| Completed NSE at 08:18, 0.00s elapsed
| Read data files from: /usr/bin/./share/nmap
```

Website Dalam Negeri

<https://www.detik.com>

```
root@kali: ~
File Edit View Search Terminal Help
#####
# Uniscan project #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 19-2-2019 8:17:3
=====
| [*] http://www.detik.com/ redirected to http://m.detik.com/
| [*] New target is: http://m.detik.com/
=====
| Domain: http://m.detik.com/
| Server: dtk19
| IP: 203.190.242.206
=====
=====
| PING
|
```

```
root@kali: ~
File Edit View Search Terminal Help
| Completed NSE at 08:18, 12.25s elapsed
| Initiating NSE at 08:18
| Completed NSE at 08:18, 0.00s elapsed
| Nmap scan report for m.detik.com (203.190.242.206)
| Host is up (0.069s latency).
| Other addresses for m.detik.com (not scanned): 103.49.221.206
| rDNS record for 203.190.242.206: s2-206-242.190.203.detik.com
| Not shown: 994 closed ports
| PORT      STATE SERVICE VERSION
| 25/tcp    filtered smtp
| 53/tcp    filtered domain
| 80/tcp    open  http   dtk21
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 301 Moved Permanently
|     Date: Tue, 19 Feb 2019 01:18:22 GMT
|     Content-Type: text/html
|     Content-Length: 182
|     Connection: close
|     Location: http://www.detik.com
|     Server: dtk21
|     X-XSS-Protection: 1;mode=block
|     X-Content-Type-Options: nosniff
|     Access-Control-Allow-Origin: *
```

```
root@kali: ~
File Edit View Search Terminal Help
| SF:Permanently</h1></center>\r\n<hr><center>nginx/dtx</center>\r\n</body>\
| SF:r\n</html>\r\n");
| Aggressive OS guesses: Linux 4.4 (91%), Linux 3.10 - 3.12 (90%), Linux 4.9 (89
| %), Linux 4.0 (88%), Linux 3.11 - 4.1 (87%), Linux 2.6.32 (87%), Linux 3.5 (87%)
| , Linux 4.2 (87%), Synology DiskStation Manager 5.1 (87%), WatchGuard Fireware 1
| 1.8 (87%)
| No exact OS matches for host (test conditions non-ideal).
| Uptime guess: 32.408 days (since Thu Jan 17 22:31:24 2019)
| Network Distance: 11 hops
| TCP Sequence Prediction: Difficulty=254 (Good luck!)
| IP ID Sequence Generation: All zeros

| TRACEROUTE (using port 256/tcp)
| HOP RTT      ADDRESS
| 1   14.12 ms 192.168.43.1
| 2   ... 10
| 11  55.22 ms s2-206-242.190.203.detik.com (203.190.242.206)

| NSE: Script Post-scanning.
| Initiating NSE at 08:18
| Completed NSE at 08:18, 0.00s elapsed
| Initiating NSE at 08:18
| Completed NSE at 08:18, 0.00s elapsed
| Read data files from: /usr/bin/../share/nmap
```


Website Luar negeri

<https://www.amazon.com/>

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# uniscan -u www.amazon.com -j
#####
# Uniscan project #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 19-2-2019 10:31:52
=====
| Domain: http://www.amazon.com/
| Server: Server
| IP: 54.192.149.36
```

```
root@kali: ~
File Edit View Search Terminal Help
=====
| NMAP
| Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-19 10:32 WIB
| NSE: Loaded 148 scripts for scanning.
| NSE: Script Pre-scanning.
| Initiating NSE at 10:32
| Completed NSE at 10:32, 0.00s elapsed
| Initiating NSE at 10:32
| Completed NSE at 10:32, 0.00s elapsed
| Initiating Ping Scan at 10:32
| Scanning www.amazon.com (54.192.149.36) [4 ports]
| Completed Ping Scan at 10:32, 0.08s elapsed (1 total hosts)
| Initiating Parallel DNS resolution of 1 host. at 10:32
| Completed Parallel DNS resolution of 1 host. at 10:32, 0.04s elapsed
| Initiating SYN Stealth Scan at 10:32
| Scanning www.amazon.com (54.192.149.36) [1000 ports]
| Discovered open port 443/tcp on 54.192.149.36
| Discovered open port 80/tcp on 54.192.149.36
| Completed SYN Stealth Scan at 10:32, 6.53s elapsed (1000 total ports)
| Initiating Service scan at 10:32
| Scanning 2 services on www.amazon.com (54.192.149.36)
| Completed Service scan at 10:32, 12.51s elapsed (2 services on 1 host)
```

```
root@kali: ~
File Edit View Search Terminal Help
| | tls-nextprotoneg:
| |_ http/1.1
| Warning: OSScan results may be unreliable because we could not find at least 1
| open and 1 closed port
| OS fingerprint not ideal because: Missing a closed TCP port so results incompl
ete
| No OS matches for host
| Uptime guess: 0.002 days (since Tue Feb 19 10:30:48 2019)
| Network Distance: 22 hops
| TCP Sequence Prediction: Difficulty=260 (Good luck!)
| IP ID Sequence Generation: All zeros
|
| TRACEROUTE (using port 443/tcp)
| HOP RTT ADDRESS
| 1 4.12 ms 192.168.43.1
| 2 ... 21
| 22 81.39 ms server-54-192-149-36.sin2.r.cloudfront.net (54.192.149.36)
|
| NSE: Script Post-scanning.
| Initiating NSE at 10:33
| Completed NSE at 10:33, 0.00s elapsed
| Initiating NSE at 10:33
| Completed NSE at 10:33, 0.00s elapsed
| Read data files from: /usr/bin/./share/nmap
```