

KEAMANAN JARINGAN KOMPUTER

“ Scanning Domain Menggunakan Nmap “



NAMA : TIARA NUR AZMI PUSPA D

NIM : 09040581721003

PROGRAM STUDI TEKNIK KOMPUTER JARINGAN

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2019

Domain Dalam Negeri

BUKALAPAK.COM

```
nmap -T4 -A -v bukalapak.com
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-13 20:09 SE Asia Standard Time
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:09
Completed NSE at 20:09, 0.00s elapsed
Initiating NSE at 20:09
Completed NSE at 20:09, 0.00s elapsed
Initiating Ping Scan at 20:09
Scanning bukalapak.com (103.64.14.18) [4 ports]
Completed Ping Scan at 20:09, 3.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:09
Completed Parallel DNS resolution of 1 host. at 20:09, 16.54s elapsed
Initiating SYN Stealth Scan at 20:09
Scanning bukalapak.com (103.64.14.18) [1000 ports]
Discovered open port 443/tcp on 103.64.14.18
Discovered open port 80/tcp on 103.64.14.18
Completed SYN Stealth Scan at 20:09, 6.67s elapsed (1000 total ports)
Initiating Service scan at 20:09
Scanning 2 services on bukalapak.com (103.64.14.18)
Completed Service scan at 20:10, 12.46s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against bukalapak.com (103.64.14.18)
Retrying OS detection (try #2) against bukalapak.com (103.64.14.18)
Initiating Traceroute at 20:10
Completed Traceroute at 20:10, 0.15s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 20:10
Completed Parallel DNS resolution of 7 hosts. at 20:10, 16.57s elapsed
NSE: Script scanning 103.64.14.18.
Initiating NSE at 20:10
Completed NSE at 20:10, 3.12s elapsed
Initiating NSE at 20:10
Completed NSE at 20:10, 0.00s elapsed
Nmap scan report for bukalapak.com (103.64.14.18)
Host is up (0.055s latency).
Other addresses for bukalapak.com (not scanned): 103.64.14.17 103.64.14.20 103.64.14.21
nmap -T4 -A -v bukalapak.com
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
25/tcp    filtered smtp
80/tcp    open  http   nginx
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: nginx
|_ http-title: Did not follow redirect to https://www.bukalapak.com/
443/tcp   open  ssl/http nginx
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: nginx
|_ http-title: Did not follow redirect to https://www.bukalapak.com/
|_ ssl-cert: Subject: commonName=*.bukalapak.com
| Subject Alternative Name: DNS:*.bukalapak.com, DNS:bukalapak.com
| Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/organizationName=COMODO CA Limited/stateOrProvinceName=Greater Manchester/
countryName=GB
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-03-21T00:00:00
| Not valid after: 2019-04-05T23:59:59
| MD5: 1a49 725e ae70 12ea c18a f275 5404 a723
|_ SHA-1: 8e49 a53a 13e2 b6e8 a790 3a83 948a e088 b296 f211
|_ ssl-date: TLS randomness does not represent time
|_ tls-nextprotoneg:
|_ spdy/3.1
|_ http/1.1
Aggressive OS guesses: Linux 3.10 - 4.11 (95%), Linux 3.13 (95%), Linux 3.13 or 4.2 (94%), Linux 3.16 (94%), Linux 4.2 (94%), Linux 4.4 (94%), Linux 3.16
- 4.6 (93%), Linux 3.2 - 4.9 (93%), Linux 3.12 (92%), Linux 3.18 (92%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 16.651 days (since Mon Jan 28 04:33:24 2019)
Network Distance: 7 hops
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
TRACEROUTE (using port 21/tcp)
HOP RTT ADDRESS
1 22.00 ms 192.168.100.1
2 22.00 ms 36.65.32.1
3 22.00 ms 125.160.0.29
4 38.00 ms 61.94.115.205
5 132.00 ms 36.91.238.213
6 38.00 ms 36.91.238.214
7 38.00 ms 103.64.14.18
NSE: Script Post-scanning.
Initiating NSE at 20:10
Completed NSE at 20:10, 0.00s elapsed
Initiating NSE at 20:10
Completed NSE at 20:10, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.29 seconds
Raw packets sent: 1071 (48.808KB) | Rcvd: 2991 (125.269KB)
```

Domain Pemerintahan

KEMENKUMHAM.GO.ID

```
nmap -T4 -A -v kemenkumham.go.id
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-13 20:34 SE Asia Standard Time
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:34
Completed NSE at 20:34, 0.00s elapsed
Initiating NSE at 20:34
Completed NSE at 20:34, 0.00s elapsed
Initiating Ping Scan at 20:34
Scanning kemenkumham.go.id (103.111.28.80) [4 ports]
Completed Ping Scan at 20:34, 1.31s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:34
Completed Parallel DNS resolution of 1 host. at 20:34, 16.50s elapsed
Initiating SYN Stealth Scan at 20:34
Scanning kemenkumham.go.id (103.111.28.80) [1000 ports]
Discovered open port 443/tcp on 103.111.28.80
Discovered open port 80/tcp on 103.111.28.80
Completed SYN Stealth Scan at 20:35, 13.36s elapsed (1000 total ports)
Initiating Service scan at 20:35
Scanning 2 services on kemenkumham.go.id (103.111.28.80)
Completed Service scan at 20:35, 12.47s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against kemenkumham.go.id (103.111.28.80)
Retrying OS detection (try #2) against kemenkumham.go.id (103.111.28.80)
Initiating Traceroute at 20:35
Completed Traceroute at 20:35, 3.05s elapsed
Initiating Parallel DNS resolution of 11 hosts. at 20:35
Completed Parallel DNS resolution of 11 hosts. at 20:35, 16.53s elapsed
NSE: Script scanning 103.111.28.80.
Initiating NSE at 20:35
Completed NSE at 20:35, 9.64s elapsed
Initiating NSE at 20:35
Completed NSE at 20:35, 0.00s elapsed
Nmap scan report for kemenkumham.go.id (103.111.28.80)
Host is up (0.028s latency).

Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.7
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Did not follow redirect to https://www.kemenkumham.go.id/
443/tcp   open  ssl/ssl Apache httpd (SSL-only mode)
|_ http-generator: Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-robots.txt: 12 disallowed entries
|_ /joomla/administrator/ /administrator/ /bin/ /cache/
|_ /cli/ /includes/ /installation/ /language/ /layouts/
|_ /libraries/ /logs/ /tmp/
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia - K...
|_ ssl-cert: Subject: commonName=*.kemenkumham.go.id
|_ Subject Alternative Name: DNS:*.kemenkumham.go.id, DNS:kemenkumham.go.id
|_ Issuer: commonName=COMODO RSA Domain Validation Secure Server CA/organizationName=COMODO CA Limited/stateOrProvinceName=Greater Manchester/
countryName=GB
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
|_ Not valid before: 2017-09-13T00:00:00
|_ Not valid after: 2020-09-12T23:59:59
|_ MD5: b856 5043 f520 7ce3 eee9 dieb b762 8299
|_ SHA-1: 511c 717c c79e 754c 81dd 17d6 8dff 19b9 919d 30f2
|_ ssl-date: TLS randomness does not represent time
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 GUESSING): Linux 3.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:3
Aggressive OS guesses: Linux 3.10 - 3.16 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 30.923 days (since Sun Jan 13 22:26:30 2019)
Network Distance: 12 hops
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: www.kemenkumham.go.id

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 0.00 ms 192.168.100.1
2 94.00 ms 36.65.32.1
3 110.00 ms 125.160.0.29
4 110.00 ms 61.94.115.205
5 31.00 ms telkom.openixp.net (218.100.36.56)
6 31.00 ms tengiga-0-1.openixp.net (218.100.36.2)
7 31.00 ms iconpln.openixp.net (218.100.27.203)
8 47.00 ms 103.111.59.246
9 47.00 ms 85.175.iconpln.net.id (119.252.175.85)
10 ...
11 93.00 ms 103.111.28.86
12 31.00 ms 103.111.28.80

NSE: Script Post-scanning.
Initiating NSE at 20:35
Completed NSE at 20:35, 0.00s elapsed
Initiating NSE at 20:35
Completed NSE at 20:35, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.01 seconds
Raw packets sent: 2113 (98.040KB) | Rcvd: 89 (4.700KB)
```

Domain Luar Negeri

eBay.com

```
nmap -T4 -A -v eBay.com
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-13 20:48 SE Asia Standard Time
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:48
Completed NSE at 20:48, 0.00s elapsed
Initiating NSE at 20:48
Completed NSE at 20:48, 0.00s elapsed
Initiating Ping Scan at 20:48
Scanning eBay.com (66.211.160.86) [4 ports]
Completed Ping Scan at 20:48, 1.36s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:48
Completed Parallel DNS resolution of 1 host. at 20:48, 0.41s elapsed
Initiating SYN Stealth Scan at 20:48
Scanning eBay.com (66.211.160.86) [1000 ports]
Discovered open port 80/tcp on 66.211.160.86
Discovered open port 443/tcp on 66.211.160.86
Discovered open port 53/tcp on 66.211.160.86
Completed SYN Stealth Scan at 20:49, 17.41s elapsed (1000 total ports)
Initiating Service scan at 20:49
Scanning 3 services on eBay.com (66.211.160.86)
Completed Service scan at 20:50, 69.05s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against eBay.com (66.211.160.86)
Initiating Traceroute at 20:50
Completed Traceroute at 20:50, 9.17s elapsed
NSE: Script scanning 66.211.160.86.
Initiating NSE at 20:50
Completed NSE at 20:50, 9.11s elapsed
Initiating NSE at 20:50
Completed NSE at 20:50, 0.00s elapsed
Nmap scan report for eBay.com (66.211.160.86)
Host is up (0.24s latency).
Other addresses for eBay.com (not scanned): 66.135.216.190 66.211.185.25 66.135.209.52 66.211.181.123 66.211.162.12
rDNS record for 66.211.160.86: ebay.com
Not shown: 997 filtered ports
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           (generic dns response: NOTIMP)
80/tcp    open  http              Apache Tomcat/Coyote JSP engine 1.1
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache-Coyote/1.1
|_ http-title: Did not follow redirect to https://www.ebay.com
443/tcp   open  ssl/https        ebay server
|_ fingerprint-strings:
|_   FourOhFourRequest:
|_     HTTP/1.1 301 Moved Permanently
|_     Location: http://nice%20ports%2C/Tri%6Eity.txt%2ebak
|_   GetRequest, HTTPOptions, RTSPRequest:
|_     HTTP/1.1 301 Moved Permanently
|_     Location: http:///
|_   Help, SSLSessionReq, TLSSessionReq:
|_     HTTP/1.1 400 Bad Request
|_     Transfer-Encoding: chunked
|_     Date: Wed, 13 Feb 2019 13:49:52 GMT
|_     Connection: close
|_     Server: ebay server
|_   Kerberos:
|_     HTTP/1.1 400 Bad Request
|_     Transfer-Encoding: chunked
|_     Date: Wed, 13 Feb 2019 13:49:54 GMT
|_     Connection: close
|_     Server: ebay server
|_   LDAPSearchReq:
|_     HTTP/1.1 400 Bad Request
|_     Transfer-Encoding: chunked
|_     Date: Wed, 13 Feb 2019 13:50:06 GMT
|_     Connection: close
|_     Server: ebay server
```

```

LPDString:
HTTP/1.1 400 Bad Request
Transfer-Encoding: chunked
Date: Wed, 13 Feb 2019 13:50:05 GMT
Connection: close
Server: ebay server
_
http-methods:
_ Supported Methods: GET POST OPTIONS
_ http-server-header: ebay server
_ http-title: Did not follow redirect to https://www.ebay.com
_ ssl-cert: Subject: commonName=pages.ebay.com.au/organizationName=eBay, Inc./stateOrProvinceName=California/countryName=US
DNS:ebay.co.uk, DNS:ebay.com, DNS:ebay.com.au, DNS:ebay.com.hk, DNS:ebay.com.my, DNS:ebay.com.sg, DNS:ebay.de, DNS:ebay.es, DNS:ebay.fr, DNS:ebay.ie,
DNS:ebay.in, DNS:ebay.it, DNS:ebay.nl, DNS:ebay.ph, DNS:ebay.pl, DNS:ebay.ru, DNS:pages.befr.ebay.be, DNS:pages.benl.ebay.be, DNS:pages.cafrebay.ca,
DNS:pages.ebay.at, DNS:pages.ebay.be, DNS:pages.ebay.ca, DNS:pages.ebay.ch, DNS:pages.ebay.co.uk, DNS:pages.ebay.com.au, DNS:pages.ebay.com.hk,
DNS:pages.ebay.com.my, DNS:pages.ebay.com.sg, DNS:pages.ebay.de, DNS:pages.ebay.es, DNS:pages.ebay.fr, DNS:pages.ebay.ie, DNS:pages.ebay.in,
DNS:pages.ebay.it, DNS:pages.ebay.nl, DNS:pages.ebay.ph, DNS:pages.ebay.pl, DNS:pages.ebay.ru, DNS:porcelain.ebay.com, DNS:solutions.ebay.com, DNS:test-
pages.ebay.ca, DNS:www.ebay.be, DNS:www.solutions.ebay.com
_ Issuer: commonName=DigiCert SHA2 Secure Server CA/organizationName=DigiCert Inc/countryName=US
_ Public Key type: rsa
_ Public Key bits: 2048
_ Signature Algorithm: sha256WithRSAEncryption
_ Not valid before: 2018-06-10T00:00:00
_ Not valid after: 2019-06-11T12:00:00
_ MD5: a771 f6a1 cdc6 aff8 2f86 ed8a f546 5272
_ SHA-1: 490b ac54 51b6 bd49 6b14 db13 58e5 964e 4ade 1da8
_ ssl-date: 2019-02-13T13:50:32+00:00; -2s from scanner time.
_ tls-alpn:
_ http/1.1
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/
submit.cgi?new-service :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port53-TCP:V=7.70%I=7&D=2/13%Time=5C642066&P=i686-pc-windows-windows%R(
SF:DNSStatusRequestTCP,E,"\x0c\x00\x90\x04\x00\x00\x00");
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF-Port443-TCP:V=7.70%T=SSL&I=7&D=2/13%Time=5C642063&P=i686-pc-windows-win
SF:dows%R(GetRequest,36,"HTTP/1.1\x20301\x20Moved\x20Permanently\r\nLocat
SF:ion:\x20http://\r\n\r\n")%R(HTTPOptions,36,"HTTP/1.1\x20301\x20Moved\
SF:\x20Permanently\r\nLocation:\x20http://\r\n\r\n")%R(FourOhFourRequest,5
SF:9,"HTTP/1.1\x20301\x20Moved\x20Permanently\r\nLocation:\x20http://nic
SF:e%20ports%2C/Tri%6Eity).txt%2ebak\r\n\r\n")%R(RTSPRequest,36,"HTTP/1.1
SF:\x20301\x20Moved\x20Permanently\r\nLocation:\x20http://\r\n\r\n")%R(He
SF:lp,8A,"HTTP/1.1\x20400\x20Bad\x20Request\r\nTransfer-Encoding:\x20chun
SF:ked\r\nDate:\x20Wed,\x2013\x20Feb\x202019\x2013:49:52\x20GMT\r\nConne
SF:ction:\x20close\r\nServer:\x20ebay\x20server\r\n\r\n\r\n")%R(SSLsess
SF:ionReq,8A,"HTTP/1.1\x20400\x20Bad\x20Request\r\nTransfer-Encoding:\x20
SF:chunked\r\nDate:\x20Wed,\x2013\x20Feb\x202019\x2013:49:52\x20GMT\r\nCon
SF:nection:\x20close\r\nServer:\x20ebay\x20server\r\n\r\n\r\n")%R(TLS
SF:SessionReq,8A,"HTTP/1.1\x20400\x20Bad\x20Request\r\nTransfer-Encoding:
SF:\x20chunked\r\nDate:\x20Wed,\x2013\x20Feb\x202019\x2013:49:54\x20GMT\r\n
SF:Connection:\x20close\r\nServer:\x20ebay\x20server\r\n\r\n\r\n")%R(
SF:Kerberos,8A,"HTTP/1.1\x20400\x20Bad\x20Request\r\nTransfer-Encoding:\x
SF:20chunked\r\nDate:\x20Wed,\x2013\x20Feb\x202019\x2013:49:54\x20GMT\r\n
SF:Connection:\x20close\r\nServer:\x20ebay\x20server\r\n\r\n\r\n")%R(
SF:LPDString,8A,"HTTP/1.1\x20400\x20Bad\x20Request\r\nTransfer-Encoding:\x
SF:20chunked\r\nDate:\x20Wed,\x2013\x20Feb\x202019\x2013:50:05\x20GMT\r\n
SF:Connection:\x20close\r\nServer:\x20ebay\x20server\r\n\r\n\r\n")%R(
SF:LDAPSearchReq,8A,"HTTP/1.1\x20400\x20Bad\x20Request\r\nTransfer-Encodi
SF:ng:\x20chunked\r\nDate:\x20Wed,\x2013\x20Feb\x202019\x2013:50:06\x20GMT
SF:\r\n\r\nConnection:\x20close\r\nServer:\x20ebay\x20server\r\n\r\n\r\n")
SF:);
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|WAP|phone
Running: ipXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:uBi_vivaz
OS details: ipXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson UBi Vivaz mobile phone

Host script results:
|_clock-skew: mean: -2s, deviation: 0s, median: -2s

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 ... 30

NSE: Script Post-scanning.
Initiating NSE at 20:50
Completed NSE at 20:50, 0.00s elapsed
Initiating NSE at 20:50
Completed NSE at 20:50, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.12 seconds
Raw packets sent: 2174 (98.640KB) | Rcvd: 17 (776B)

```