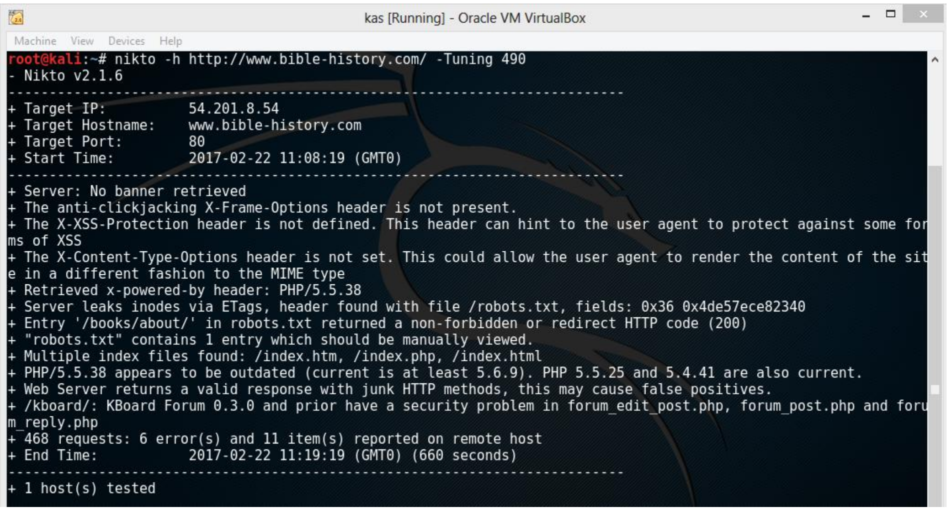
KEAMANAN JARINGAN KOMPUTER

Disusun Oleh :
Nama : Imam Mustofa
NIM : 09011181320028

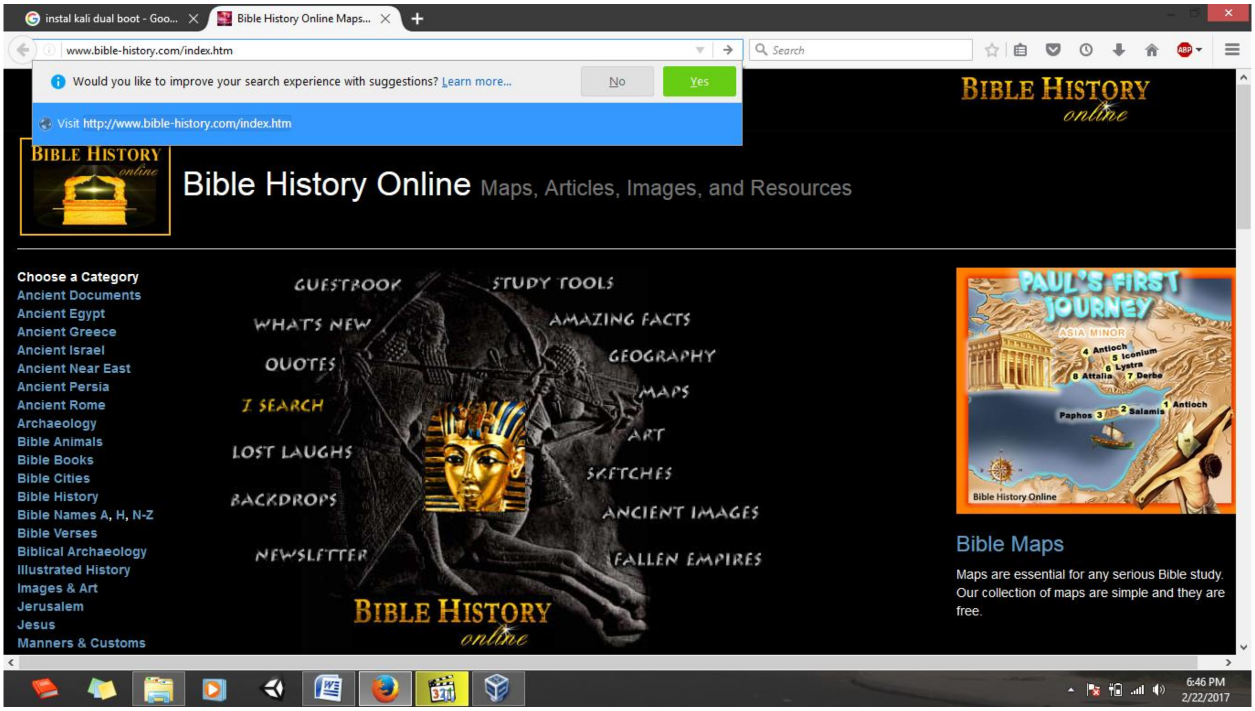
SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2017

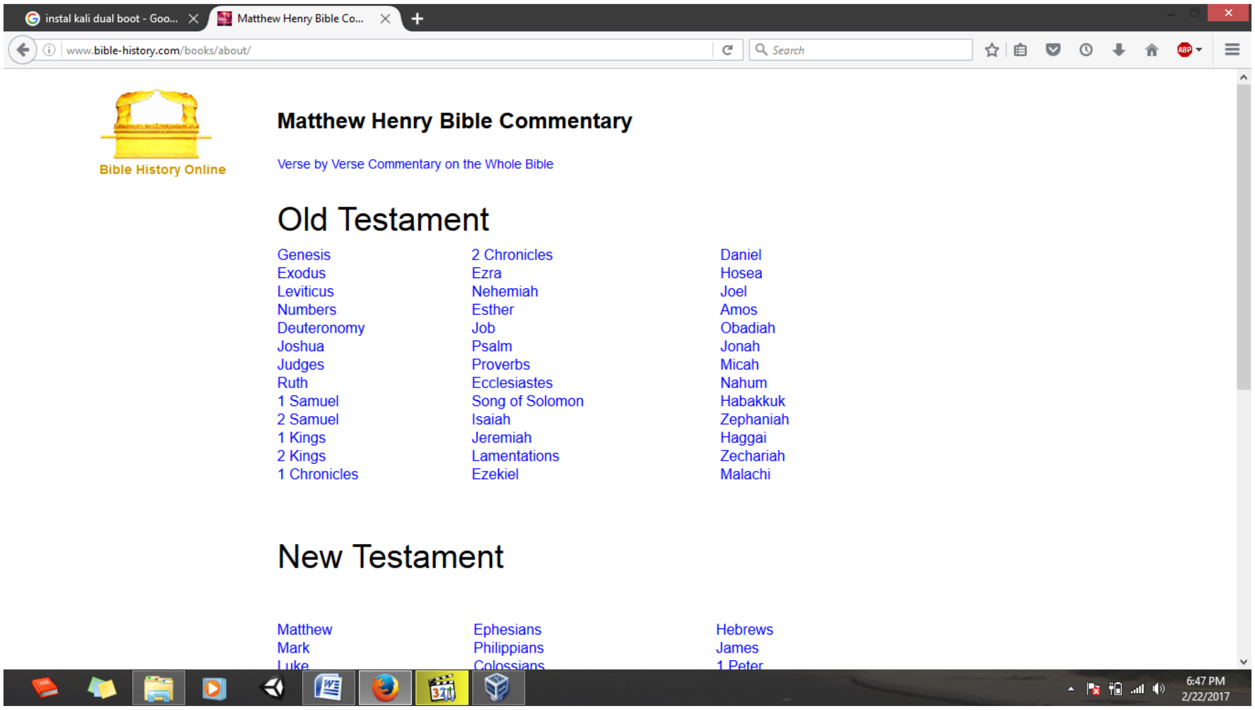
Berikut merupakan uraian tugas scanning sebuah alamat website untuk mendapatkan beberapa informasi krusial. Untuk percobaan, scanning menggunakan tools nikto yang disediakan oleh kali linux dengan objek www.bible-history.com. Dari hasil scanning didapatkan data seperti terlihat pada gambar berikut ini.


kas [Running] - Oracle VM VirtualBox
Machine View Devices Help

```
root@kali:~# nikto -h http://www.bible-history.com/ -Tuning 490
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          54.201.8.54
+ Target Hostname:    www.bible-history.com
+ Target Port:        80
+ Start Time:         2017-02-22 11:08:19 (GMT0)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some for
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ Retrieved x-powered-by header: PHP/5.5.38
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x36 0x4de57ece82340
+ Entry '/books/about/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Multiple index files found: /index.htm, /index.php, /index.html
+ PHP/5.5.38 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and foru
m_reply.php
+ 468 requests: 6 error(s) and 11 item(s) reported on remote host
+ End Time:           2017-02-22 11:19:19 (GMT0) (660 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Pada gambar diatas diperlihatkan informasi IP target dengan port 80. Hal penting yang didapatkan dari hasil list yaitu file robots.txt. untuk mendapatkan data tersebut, maka harus membuka alamat target secara manual dan ditambahkan entry yang didapatkan pada list yaitu /books/about/. Data ini terlihat pada gambar berikut.




instal kali dual boot - Goo...
Matthew Henry Bible Co...
www.bible-history.com/books/about/
Search
Bible History Online
6:47 PM
2/22/2017

Matthew Henry Bible Commentary

Verse by Verse Commentary on the Whole Bible

Old Testament

Genesis
Exodus
Leviticus
Numbers
Deuteronomy
Joshua
Judges
Ruth
1 Samuel
2 Samuel
1 Kings
2 Kings
1 Chronicles

2 Chronicles
Ezra
Nehemiah
Esther
Job
Psalm
Proverbs
Ecclesiastes
Song of Solomon
Isaiah
Jeremiah
Lamentations
Ezekiel

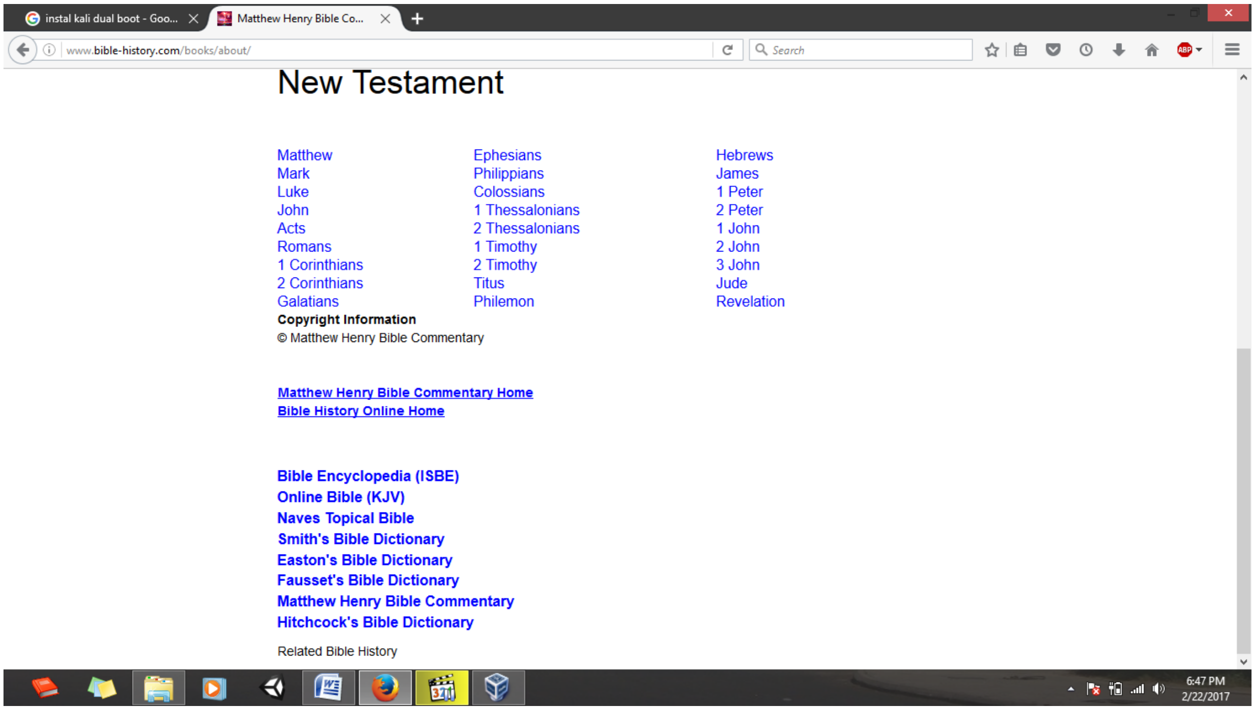
Daniel
Hosea
Joel
Amos
Obadiah
Jonah
Micah
Nahum
Habakkuk
Zephaniah
Haggai
Zechariah
Malachi

New Testament

Matthew
Mark
Luke

Ephesians
Philippians
Colossians

Hebrews
James
1 Peter


instal kali dual boot - Goo...
Matthew Henry Bible Co...
www.bible-history.com/books/about/
Search
6:47 PM
2/22/2017

New Testament

Matthew
Mark
Luke
John
Acts
Romans
1 Corinthians
2 Corinthians
Galatians

Ephesians
Philippians
Colossians
1 Thessalonians
2 Thessalonians
1 Timothy
2 Timothy
Titus
Philemon

Hebrews
James
1 Peter
2 Peter
1 John
2 John
3 John
Jude
Revelation

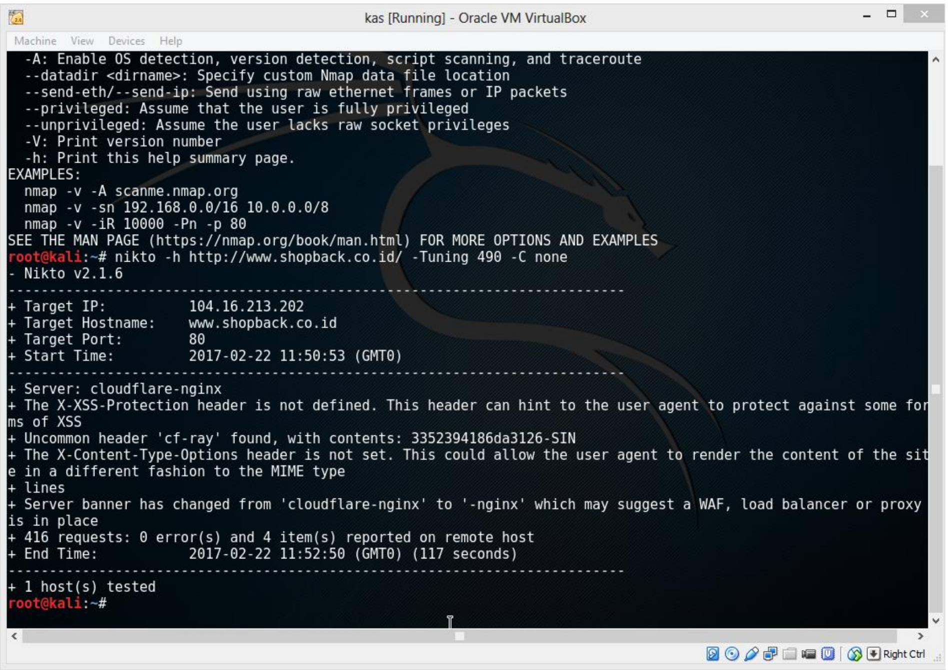
Copyright Information
© Matthew Henry Bible Commentary

Matthew Henry Bible Commentary Home
Bible History Online Home

Bible Encyclopedia (ISBE)
Online Bible (KJV)
Naves Topical Bible
Smith's Bible Dictionary
Easton's Bible Dictionary
Fausset's Bible Dictionary
Matthew Henry Bible Commentary
Hitchcock's Bible Dictionary

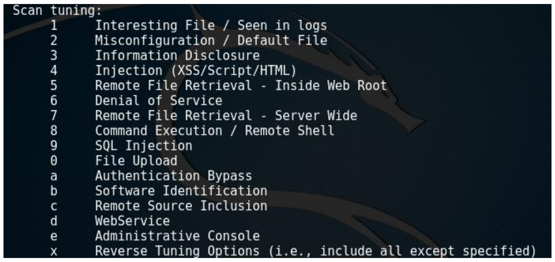
Related Bible History

Data about yang didapatkan yaitu data pemilik dari alamat target. Data ini didapatkan secara online dan dishare oleh pemilik sehingga masih bersifat umum.

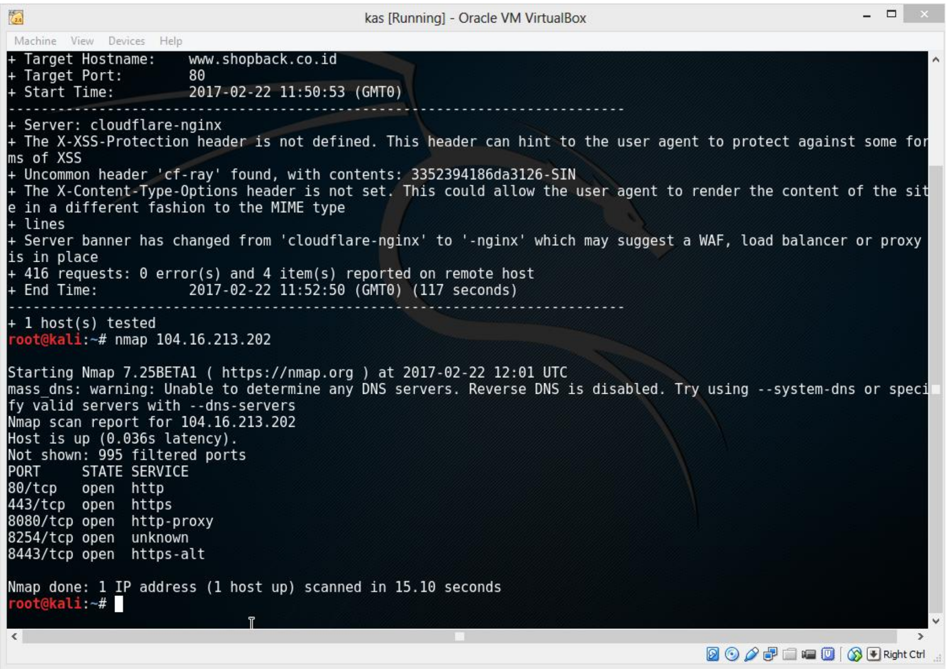


```
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nikto -h http://www.shopback.co.id/ -Tuning 490 -C none
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          104.16.213.202
+ Target Hostname:    www.shopback.co.id
+ Target Port:        80
+ Start Time:         2017-02-22 11:50:53 (GMT0)
---------------------------------------------------------------------------
+ Server: cloudflare-nginx
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some for
ms of XSS
+ Uncommon header 'cf-ray' found, with contents: 3352394186da3126-SIN
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ lines
+ Server banner has changed from 'cloudflare-nginx' to '-nginx' which may suggest a WAF, load balancer or proxy
is in place
+ 416 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2017-02-22 11:52:50 (GMT0) (117 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

Kemudian cara sebelumnya digunakan pada target dari tugas yang sebelumnya dan didapatkan data IP, port, dan server yang digunakan yaitu nginx. Hal ini terlihat pada gambar diatas. Dengan menggunakan alamat ip yang didapatkan, kemudian scanning website menggunakan tools nmap dari kali dan didapatkan hasil sebagai berikut. Perlu diketahui penggunaan angka 490 adalah urutan dari list tuning dari tool nikto. List dari tuning tersebut yaitu berisi



```
Scan tuning:
     1     Interesting File / Seen in logs
     2     Misconfiguration / Default File
     3     Information Disclosure
     4     Injection (XSS/Script/HTML)
     5     Remote File Retrieval - Inside Web Root
     6     Denial of Service
     7     Remote File Retrieval - Server Wide
     8     Command Execution / Remote Shell
     9     SQL Injection
     0     File Upload
     a     Authentication Bypass
     b     Software Identification
     c     Remote Source Inclusion
     d     WebService
     e     Administrative Console
     x     Reverse Tuning Options (i.e., include all except specified)
```

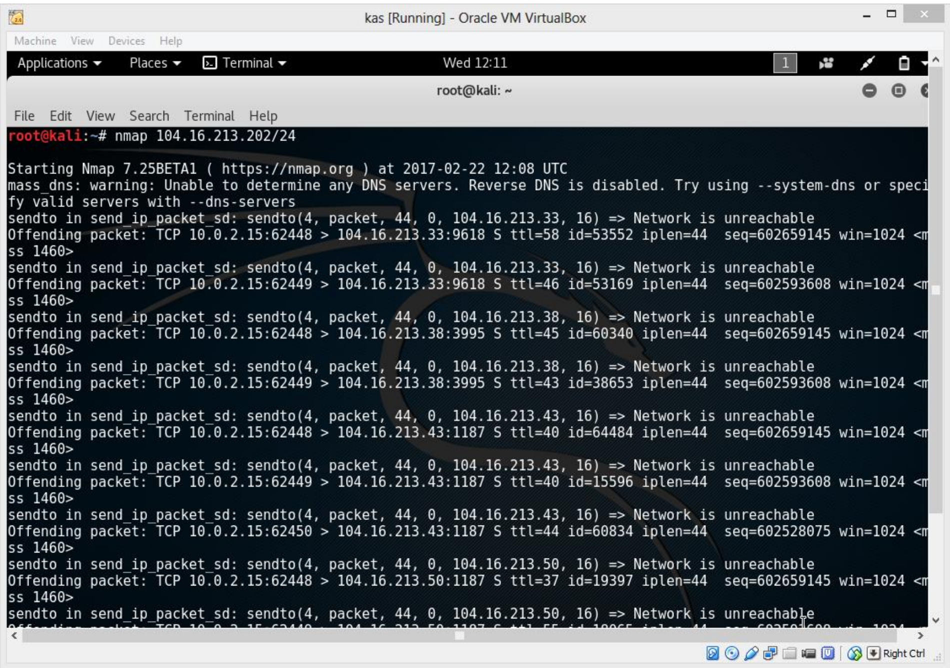

kas [Running] - Oracle VM VirtualBox
Machine View Devices Help
Right Ctrl

```
+ Target Hostname:    www.shopback.co.id
+ Target Port:        80
+ Start Time:         2017-02-22 11:50:53 (GMT0)
---------------------------------------------------------------------------
+ Server: cloudflare-nginx
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some for
ms of XSS
+ Uncommon header 'cf-ray' found, with contents: 3352394186da3126-SIN
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ lines
+ Server banner has changed from 'cloudflare-nginx' to '-nginx' which may suggest a WAF, load balancer or proxy
is in place
+ 416 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2017-02-22 11:52:50 (GMT0) (117 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~# nmap 104.16.213.202

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-02-22 12:01 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or speci
fy valid servers with --dns-servers
Nmap scan report for 104.16.213.202
Host is up (0.036s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8254/tcp open  unknown
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 15.10 seconds
root@kali:~# 
```

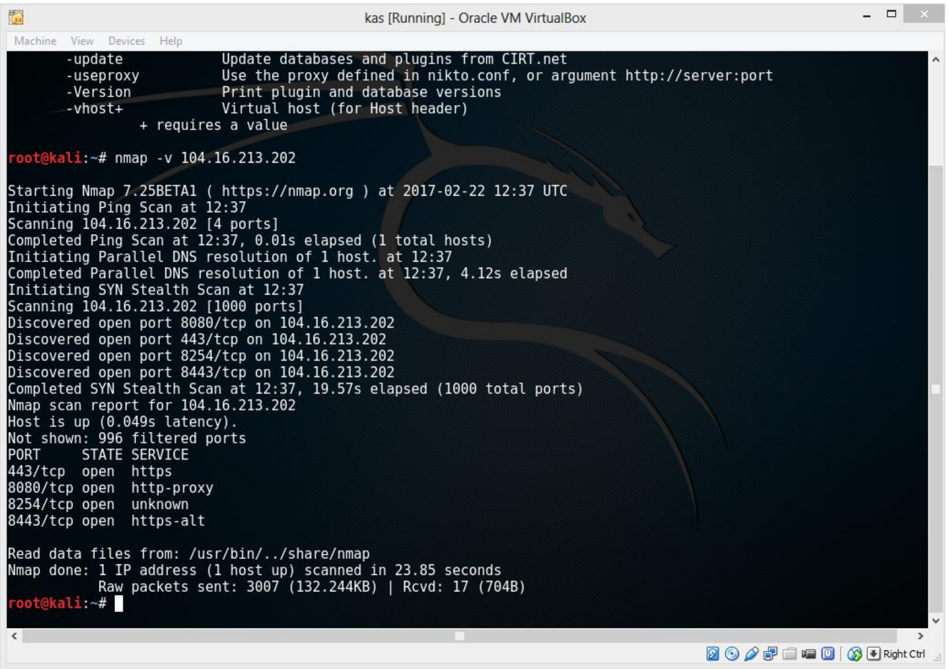
Hasil dari nmap yang diperoleh yaitu dengan latency 0.036 detik dan didapatkan server dns yang valid beserta beberapa service yang digunakan oleh server target.


kas [Running] - Oracle VM VirtualBox
Machine View Devices Help
Applications
Places
Terminal
Wed 12:11
1
root@kali: ~
File Edit View Search Terminal Help
Right Ctrl

```
root@kali:~# nmap 104.16.213.202/24

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-02-22 12:08 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or speci
fy valid servers with --dns-servers
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 104.16.213.33, 16) => Network is unreachable
Offending packet: TCP 10.0.2.15:62448 > 104.16.213.33:9618 S ttl=58 id=53552 iplen=44  seq=602659145 win=1024 <m
ss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 104.16.213.33, 16) => Network is unreachable
Offending packet: TCP 10.0.2.15:62449 > 104.16.213.33:9618 S ttl=46 id=53169 iplen=44  seq=602593608 win=1024 <m
ss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 104.16.213.38, 16) => Network is unreachable
Offending packet: TCP 10.0.2.15:62448 > 104.16.213.38:3995 S ttl=45 id=60340 iplen=44  seq=602659145 win=1024 <m
ss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 104.16.213.38, 16) => Network is unreachable
Offending packet: TCP 10.0.2.15:62449 > 104.16.213.38:3995 S ttl=43 id=38653 iplen=44  seq=602593608 win=1024 <m
ss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 104.16.213.43, 16) => Network is unreachable
Offending packet: TCP 10.0.2.15:62448 > 104.16.213.43:1187 S ttl=40 id=64484 iplen=44  seq=602659145 win=1024 <m
ss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 104.16.213.43, 16) => Network is unreachable
Offending packet: TCP 10.0.2.15:62449 > 104.16.213.43:1187 S ttl=40 id=15596 iplen=44  seq=602593608 win=1024 <m
ss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 104.16.213.43, 16) => Network is unreachable
Offending packet: TCP 10.0.2.15:62450 > 104.16.213.43:1187 S ttl=44 id=60834 iplen=44  seq=602528075 win=1024 <m
ss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 104.16.213.50, 16) => Network is unreachable
Offending packet: TCP 10.0.2.15:62448 > 104.16.213.50:1187 S ttl=37 id=19397 iplen=44  seq=602659145 win=1024 <m
ss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 104.16.213.50, 16) => Network is unreachable
```

Proses selanjutnya yaitu dengan scanning subnet 24, namun didapatkan network yang unreachable, yang terlihat pada gambar diatas.



```
       -update            Update databases and plugins from CIRT.net
       -useproxy          Use the proxy defined in nikto.conf, or argument http://server:port
       -Version           Print plugin and database versions
       -vhost+            Virtual host (for Host header)
                + requires a value

root@kali:~# nmap -v 104.16.213.202

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-02-22 12:37 UTC
Initiating Ping Scan at 12:37
Scanning 104.16.213.202 [4 ports]
Completed Ping Scan at 12:37, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:37
Completed Parallel DNS resolution of 1 host. at 12:37, 4.12s elapsed
Initiating SYN Stealth Scan at 12:37
Scanning 104.16.213.202 [1000 ports]
Discovered open port 8080/tcp on 104.16.213.202
Discovered open port 443/tcp on 104.16.213.202
Discovered open port 8254/tcp on 104.16.213.202
Discovered open port 8443/tcp on 104.16.213.202
Completed SYN Stealth Scan at 12:37, 19.57s elapsed (1000 total ports)
Nmap scan report for 104.16.213.202
Host is up (0.049s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
443/tcp  open  https
8080/tcp open  http-proxy
8254/tcp open  unknown
8443/tcp open  https-alt

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 23.85 seconds
           Raw packets sent: 3007 (132.244KB) | Rcvd: 17 (704B)
root@kali:~# 
```

Data dari gambar diatas yaitu memperlihatkan satu buah host active, empat buah port yang tertangkap layanan. Dan langkah selanjutnya yaitu memetakan layanan yang didapatkan untuk mencari kelemahan dari layanan tersebut sehingga didapatkan jalur data target.