

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

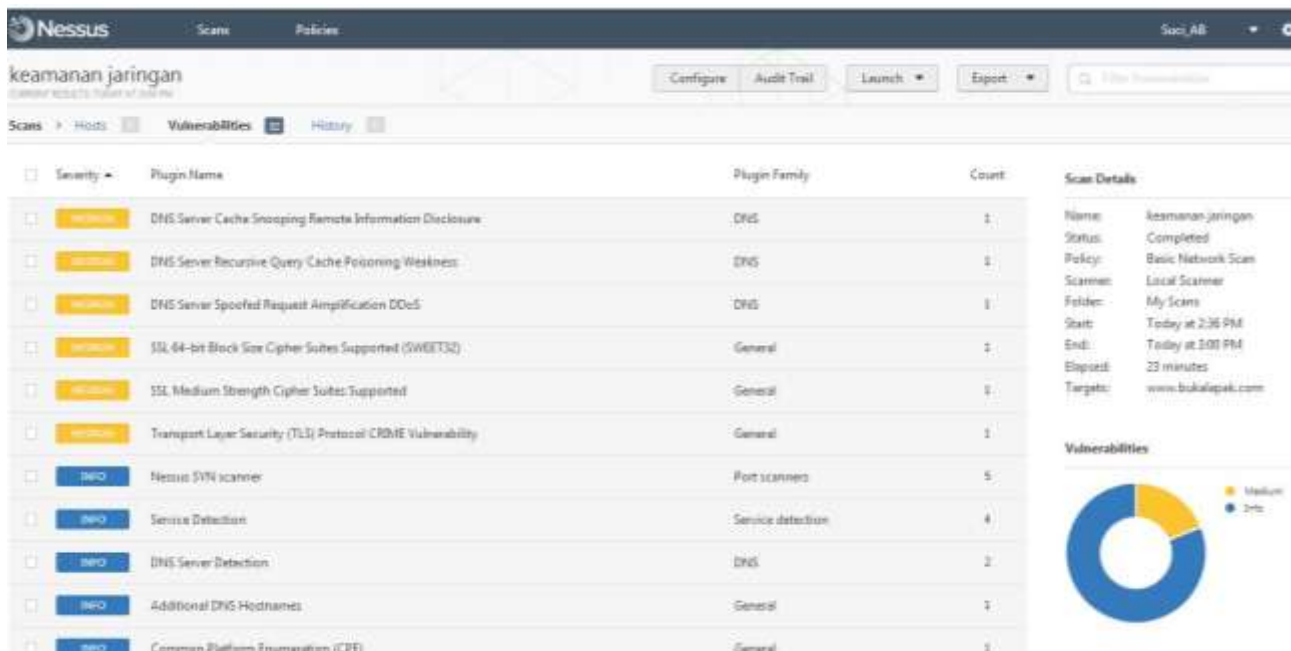
KEAMANAN JARINGAN KOMPUTER

SCANNING

Target scanning : www.bukalapak.com

Kali untuk melakukan scanning menggunakan aplikasi Nessus. Nessus adalah scanner keamanan jaringan yang harus digunakan oleh administrator system . Nessus adalah software yang gratis dan bebas di download. Nessus merupakan sebuah software scanning, yang dapat digunakan untuk meng-audit kewanaman sebuah sistem, seperti vulnerability, misconfiguration, security patch yang belum diaplikasikan, default password, dan denial of service Nessus berfungsi untuk monitoring lalu-lintas jaringan. Dikarenakan fungsi dari Nessus dapat digunakan untuk mendeteksi adanya kelemahan ataupun cacat dari suatu sistem maka Nessus menjadi salah satu tool andalan ketika melakukan audit keamanan suatu sistem.

Gambar dibawah ini merupakan hasil scanning target www.bukalapak.com menggunakan Nessus.



Gambar 1.

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

<input type="checkbox"/>	INFO	Device Type	General	1
<input type="checkbox"/>	INFO	DNS Sender Policy Framework (SPF) Enabled	DNS	1
<input type="checkbox"/>	INFO	HTTP Server Type and Version	Web Servers	1
<input type="checkbox"/>	INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	1
<input type="checkbox"/>	INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
<input type="checkbox"/>	INFO	Nessus Scan Information	Settings	1
<input type="checkbox"/>	INFO	Network Time Protocol (NTP) Server Detection	Service detection	1
<input type="checkbox"/>	INFO	OpenSSL Detection	Service detection	1
<input type="checkbox"/>	INFO	OS Identification	General	1
<input type="checkbox"/>	INFO	SSL / TLS Versions Supported	General	1
<input type="checkbox"/>	INFO	SSL Certificate Information	General	1
<input type="checkbox"/>	INFO	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)	General	1
<input type="checkbox"/>	INFO	SSL Cipher Block Chaining Cipher Suites Supported	General	1
<input type="checkbox"/>	INFO	SSL Cipher Suites Supported	General	1
<input type="checkbox"/>	INFO	SSL Perfect Forward Secrecy Cipher Suites Supported	General	1

Gambar 2.

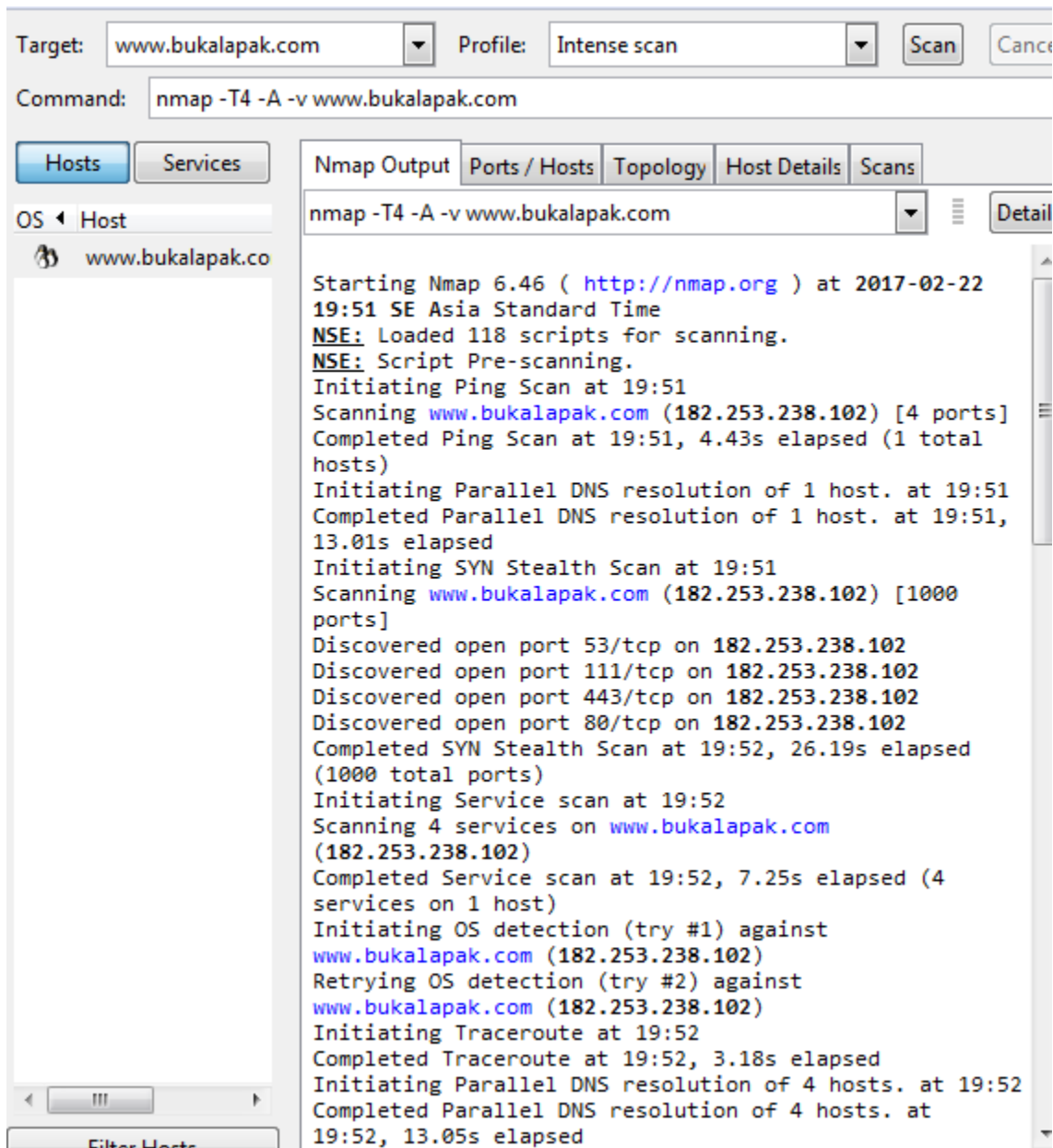
<input type="checkbox"/>	INFO	SSL Root Certification Authority Certificate Information	General	1
<input type="checkbox"/>	INFO	TCP/IP Timestamps Supported	General	1
<input type="checkbox"/>	INFO	TLS Next Protocols Supported	General	1
<input type="checkbox"/>	INFO	TLS NPN Supported Protocol Enumeration	Misc.	1
<input type="checkbox"/>	INFO	Traceroute Information	General	1
<input type="checkbox"/>	INFO	Web Server No 404 Error Code Check	Web Servers	1

Gambar 3.

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

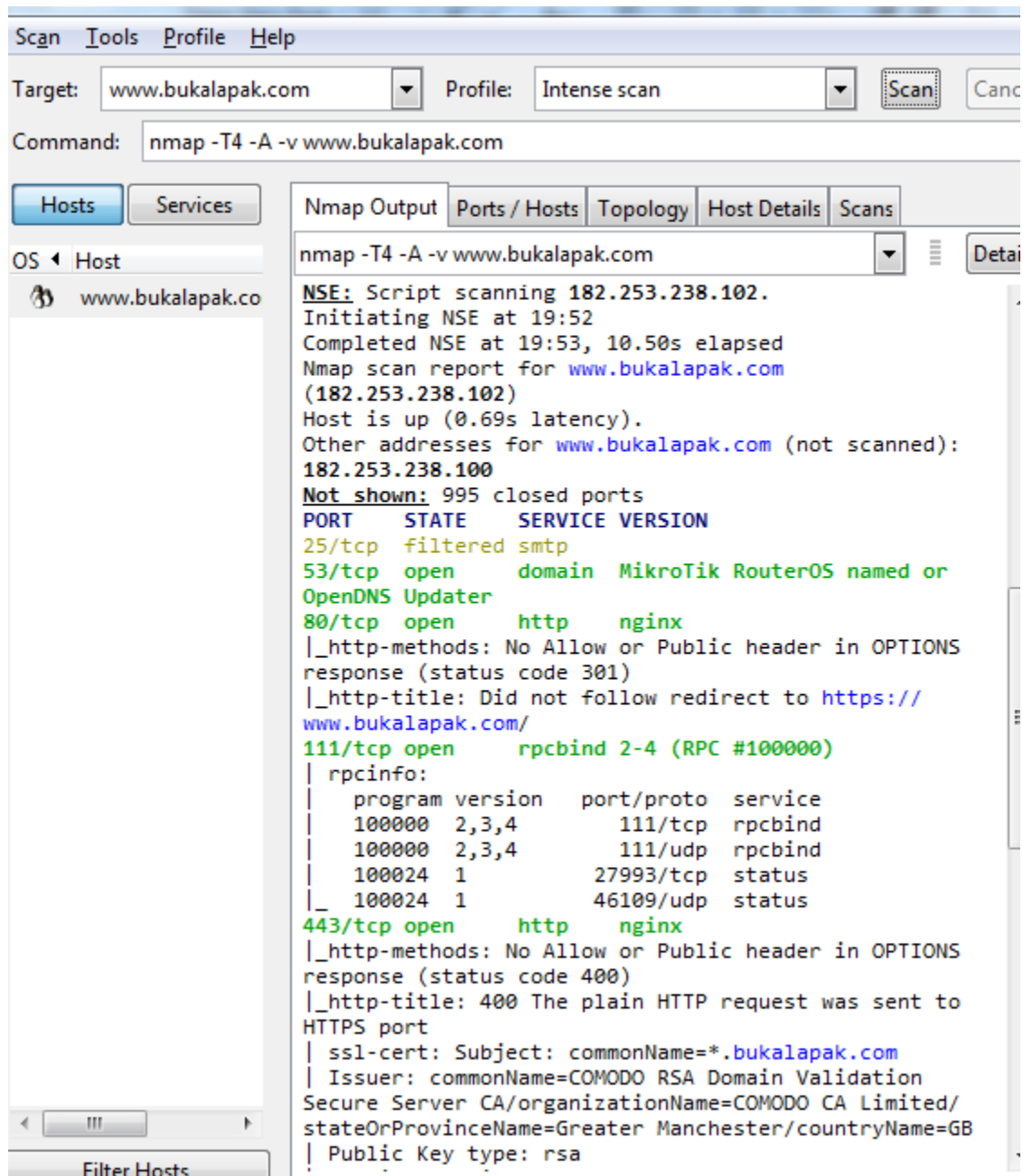


Gambar 4.

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER



Gambar 5.

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

The screenshot displays the Nmap GUI interface. At the top, the 'Target' field is set to 'www.bukalapak.com' and the 'Profile' is 'Intense scan'. The command line shows 'nmap -T4 -A -v www.bukalapak.com'. The main window is divided into two panes: 'Hosts' on the left and 'Nmap Output' on the right. The 'Hosts' pane shows the target 'www.bukalapak.com'. The 'Nmap Output' pane displays the following scan results:

```
nmap -T4 -A -v www.bukalapak.com
| Public Key bits: 2048
| Not valid before: 2016-03-21T00:00:00+00:00
| Not valid after: 2019-04-05T23:59:59+00:00
| MD5: 1a49 725e ae70 12ea c18a f275 5404 a723
|_SHA-1: 8e49 a53a 13e2 b6e8 a790 3a83 948a e088 b296
f211
Aggressive OS guesses: Linux 3.0 - 3.9 (96%), Linux
2.6.32 - 3.9 (94%), OpenWrt 12.09-rc1 Attitude
Adjustment (Linux 3.3 - 3.7) (93%), HP P2000 G3 NAS
device (93%), Linux 2.6.31 - 2.6.35 (92%), Linux
2.6.32 - 2.6.39 (91%), Linux 3.2 - 3.6 (91%), Linux
2.6.32 - 3.2 (91%), Netgear DG834G WAP or Western
Digital WD TV media player (91%), Linux 2.6.15 -
2.6.30 (90%)
No exact OS matches for host (test conditions non-
ideal).
Uptime guess: 0.084 days (since Wed Feb 22 17:52:33
2017)
Network Distance: 5 hops
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 421.00 ms bill.net (192.168.30.1)
2 ...
3 670.00 ms 36.77.64.1
4 657.00 ms 125.160.0.29
5 733.00 ms 182.253.238.102

NSE: Script Post-scanning.
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any
incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.08
seconds
```

Gambar 7.

NAMA : SUCI ANGGRAENI

NIM : 09011181320030

KEAMANAN JARINGAN KOMPUTER

Dapat dilihat dari gambar 4 sampai gambar 7, merupakan hasil dari scanning situs www.bukalapak.com yang pada gambar itu terdapat informasi menarik yakni informasi tentang output port yang aktif. Situs www.bukalapak.com menggunakan output port 25,53,80,111 dan 443. Pada hasil scanning tersebut output port yang aktif adalah output port 53,80,111 dan 433. Sedangkan output port 25 mengalami filtered. Difilter berarti bahwa sebuah firewall, filter, atau penghalang jaringan lainnya memblokir port sehingga Nmap tidak dapat mengetahui apakah ia terbuka atau tertutup. Tertutup port tidak memiliki aplikasi yang sedang mendengarkan, meskipun mereka dapat terbuka kapanpun. Port 25 menggunakan service version smtp, Port 53 menggunakan service version domain MikroTik RouterOS named or OpenDNS Updater, Port 80 menggunakan service version http nginx, Port 111 menggunakan service version rpcbind 2-4 (RPC #100000)

rpcinfo:

- program version port/proto service
- 100000 2,3,4 111/tcp rpcbind
- 100000 2,3,4 111/udp rpcbind
- 100024 1 27993/tcp status
- 100024 1 46109/udp status

Dan Port 443 menggunakan service version http nginx.