KEAMANAN JARINGAN KOMPUTER

ANALISIS SCANNING

D
I
S
U
S
U
N

OLEH

Nama : Anggoro Prasetyo

Nim : 09121001064

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

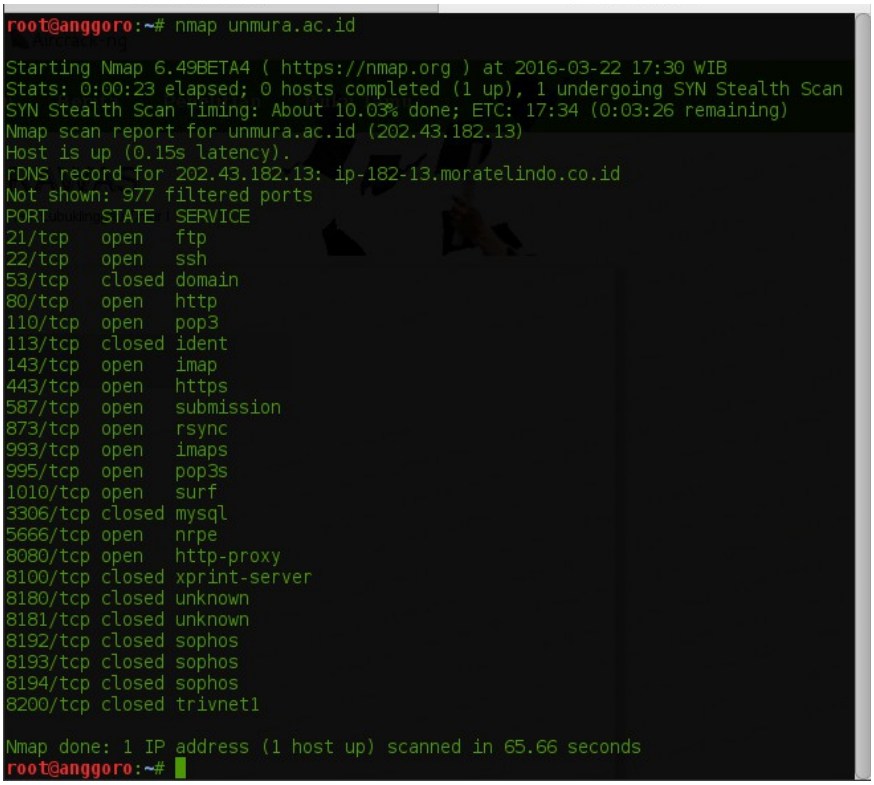
UNIVERSITAS SRIWIJAYA

INDRALAYA

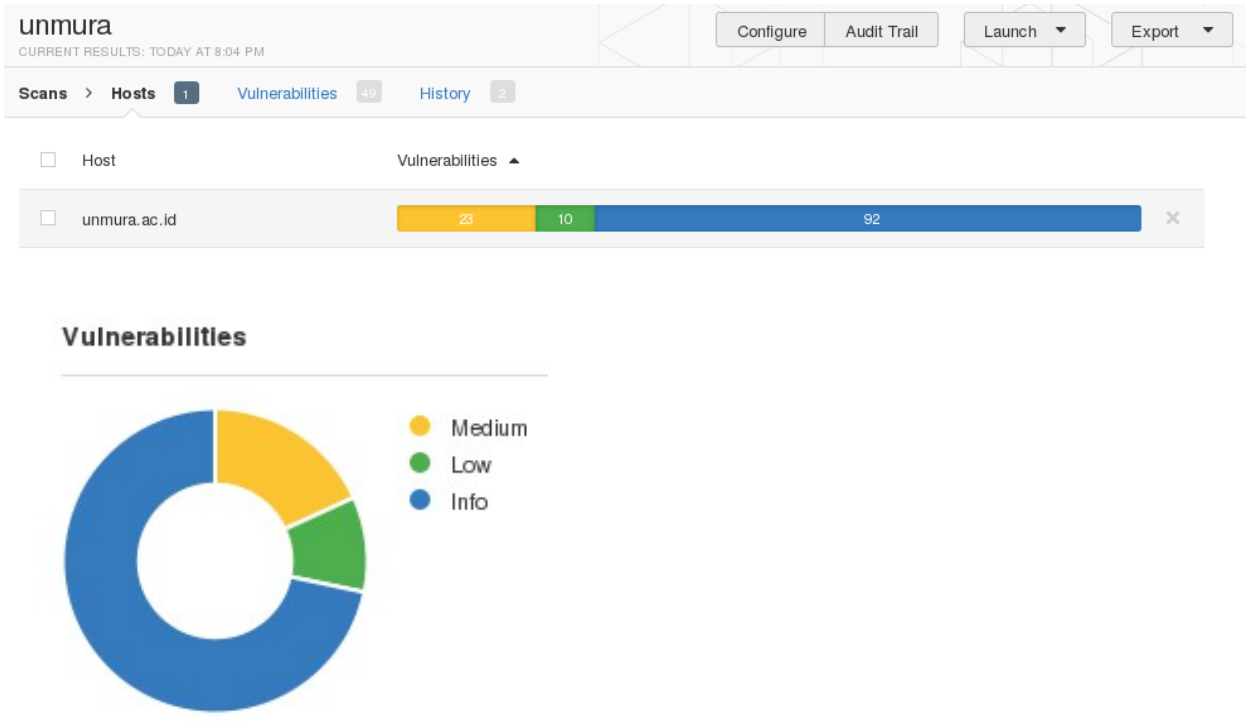
TAHUN AJARAN 2015/2016

1. SCANNING MENGGUNAKAN TOOLS

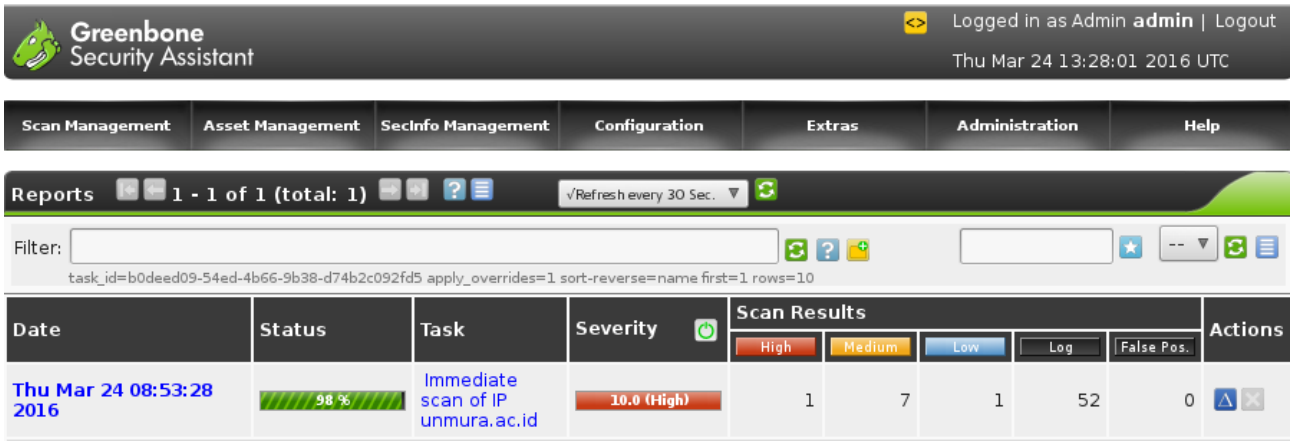
1.1. nmap

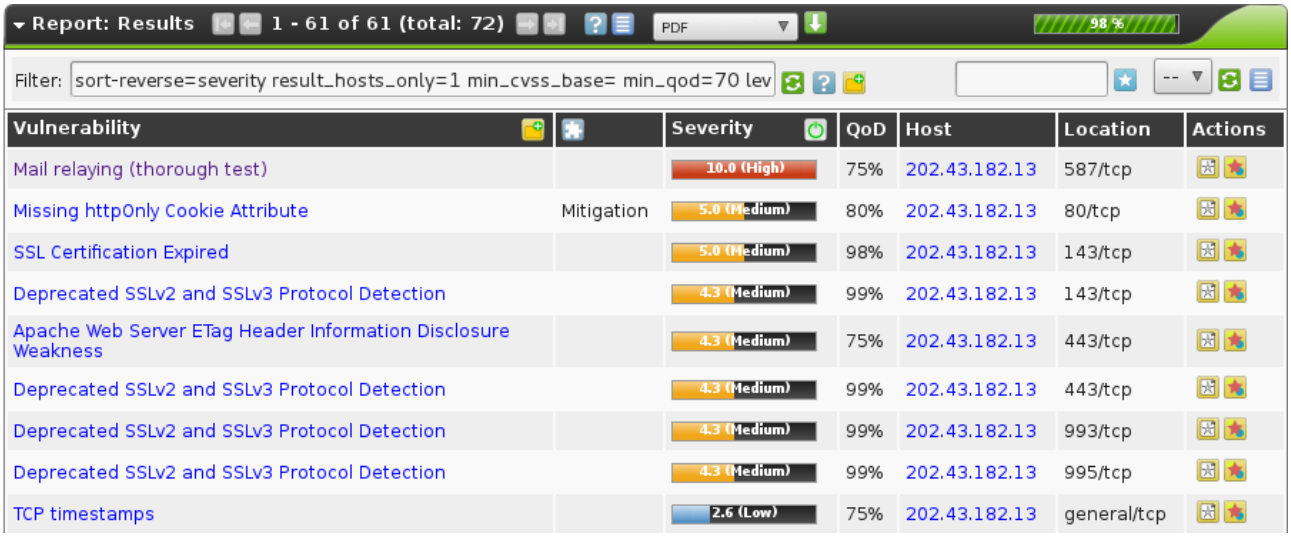


1.2. nessus



1.3. Openvas





2. ANALISIS HASIL SCANNING

2.1.open port

Disini saya hanya memfokuskan pada target 3 port yang terbuka berdasarkan scanning pada nmap yaitu :

80 dan 443 : http

HTTP (Hypertext Transfer Protocol, lebih sering terlihat sebagai http) adalah protocol yang dipergunakan untuk mentransfer dokumen dalam *World Wide Web* (WWW). Protokol ini adalah protokol ringan, tidak berstatus dan generik yang dapat dipergunakan berbagai macam tipe dokumen.

22 : ssh

SSH adalah Port Jaringan komputer yang bersifat logic adalah port 22. Port 22 ini merupakan port yang digunakan untuk mengaktifkan SSH atau *Secure Shell* pada jaringan komputer.

143: imap
IMAP (*Internet Message Access Protocol*) adalah protokol standar untuk mengakses/mengambil e-mail dari server. IMAP memungkinkan pengguna memilih pesan e-mail yang akan ia ambil, membuat folder di server, mencari pesan e-mail tertentu, bahkan menghapus pesan e-mail yang ada.

2.2. deamon
Secara detail service yang berjalan pada server dapt diketahui melalui tool tersebut

A. OS : Linux Kernel 2.6 on Debian 6.0 (squeeze)

Host Details

IP:	202.43.182.13
DNS:	unmura.ac.id
OS:	Linux Kernel 2.6 on Debian 6.0 (squeeze) HP 3PAR
Start:	Today at 7:38 PM

B. 80 : Apche httpd

```
root@anggoro:~# nmap -sV unmura.ac.id -p80

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-22 23:45 WIB
Nmap scan report for unmura.ac.id (202.43.182.13)
Host is up (0.098s latency).
rDNS record for 202.43.182.13: ip-182-13.moratelindo.co.id
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.03 seconds
```

C. 22 : OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)

```
root@anggoro:~# nmap -sV unmura.ac.id -p22

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-22 23:47 WIB
Nmap scan report for unmura.ac.id (202.43.182.13)
Host is up (0.099s latency).
rDNS record for 202.43.182.13: ip-182-13.moratelindo.co.id
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze8 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.04 seconds
```

D. 143 : Courier imapd (released 2010)

```
root@anggoro:~# nmap -sV unmura.ac.id -p143

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-03-22 23:44 WIB
Nmap scan report for unmura.ac.id (202.43.182.13)
Host is up (0.093s latency).
rDNS record for 202.43.182.13: ip-182-13.moratelindo.co.id
PORT    STATE SERVICE VERSION
143/tcp open  imap    Courier Imapd (released 2010)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.03 seconds
```

2.3. Vulnerabilities

port 80 dan 443 : http

MEDIUM Apache Server ETag Header Information Disclosure

Description

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

See Also

http://httpd.apache.org/docs/2.2/mod/core.html#FileETag

Output

```
Nessus was able to determine that the Apache Server listening on
port 443 leaks the servers inode numbers in the ETag HTTP
Header field :

  Source                : ETag: "8aa04-0-4e83ba17ed140"
  Inode number          : 567812
  File size             : 0 bytes
  File modification time : Oct.  8, 2013 at 14:31:57 GMT
```

Port	Hosts
443 / tcp / www	unmura.ac.id

Plugin Details

Severity:	Medium
ID:	88098
Version:	$Revision: 1.2 $
Type:	remote
Family:	Web Servers
Published:	2016/01/22
Modified:	2016/01/25

Risk Information

Risk Factor: Medium

CVSS Base Score: 5.0

CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS Temporal Vector: CVSS2#E:H/RL:OF/RC:ND

CVSS Temporal Score: 4.3

Vulnerability Information

CPE: cpe:/a:apache:http_server

Exploit Available: true

Exploit Ease: No exploit is required

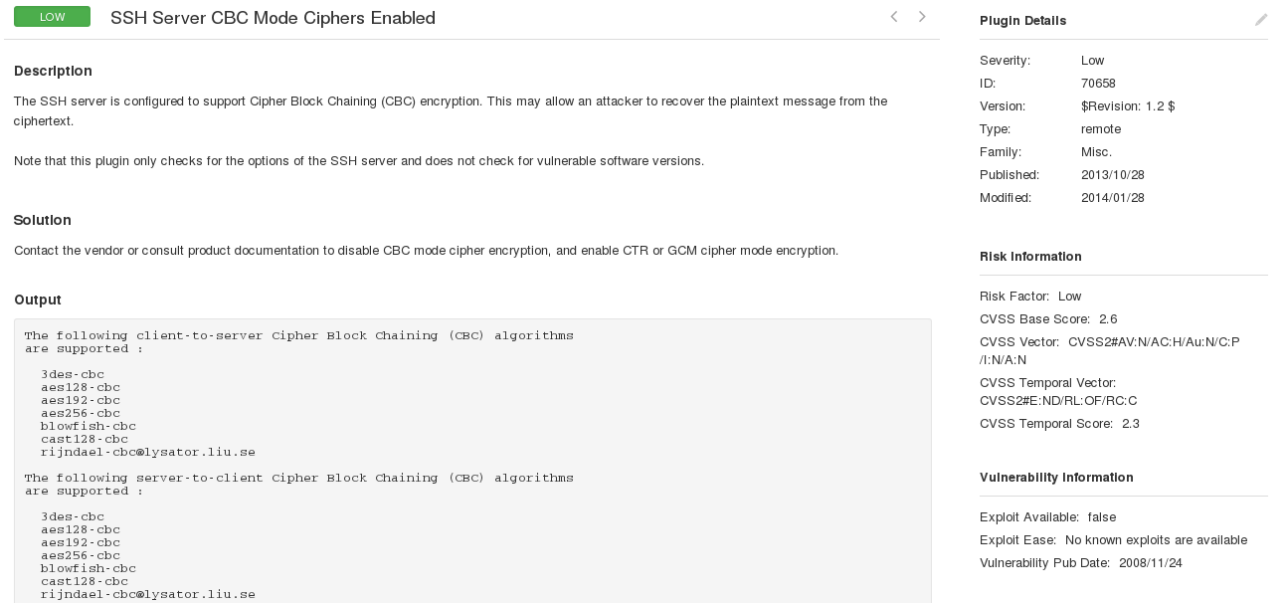
Vulnerability Pub Date: 2003/02/25

Web server jauh dipengaruhi oleh kerentanan keterbukaan informasi karena header ETag memberikan informasi sensitif yang bisa membantu penyerang, seperti jumlah inode dari file yang diminta.

Solusi

Memodifikasi header HTTP ETag dari web server untuk tidak menyertakan inode file dalam perhitungan ETag sundulan. Lihat dokumentasi Apache yang terkait untuk informasi lebih lanjut.

port 22 : SSH



LOW SSH Server CBC Mode Ciphers Enabled

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Output

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

Plugin Details

Severity:	Low
ID:	70658
Version:	$Revision: 1.2 $
Type:	remote
Family:	Misc.
Published:	2013/10/28
Modified:	2014/01/28

Risk Information

Risk Factor: Low

CVSS Base Score: 2.6

CVSS Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

CVSS Temporal Vector: CVSS2#E:ND/RL:OF/RC:C

CVSS Temporal Score: 2.3

Vulnerability Information

Exploit Available: false

Exploit Ease: No known exploits are available

Vulnerability Pub Date: 2008/11/24

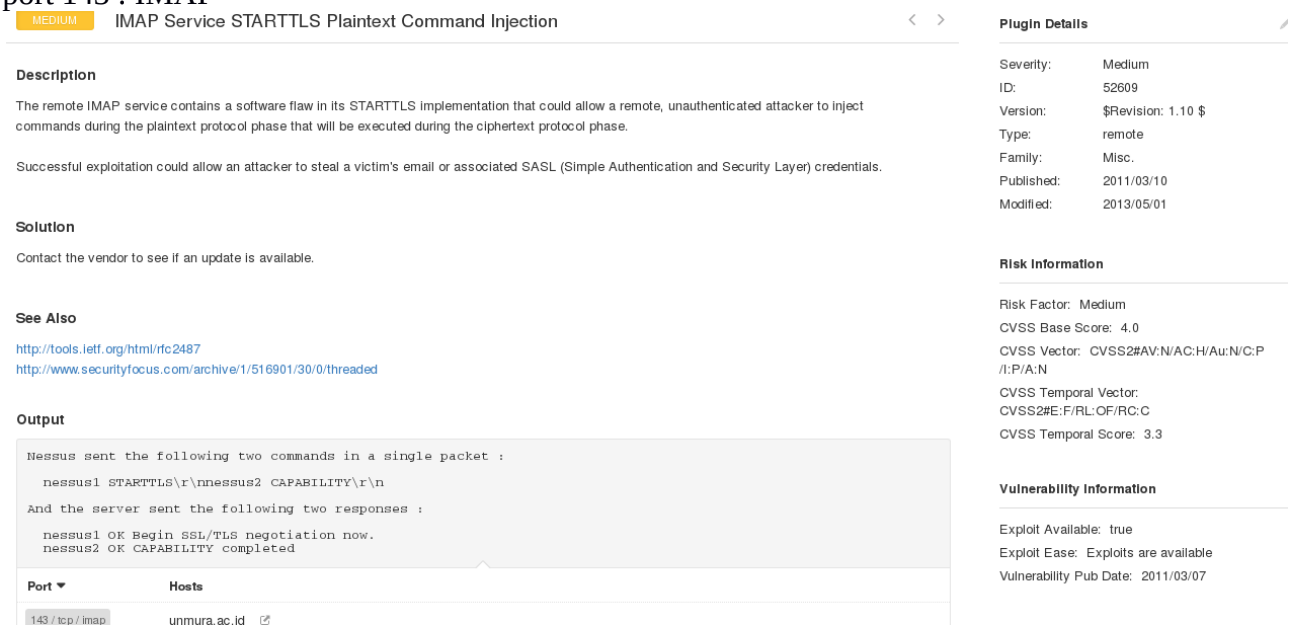
*Server SSH dikonfigurasi untuk mendukung Cipher Block Chaining (CBC) enkripsi. Hal ini dapat memungkinkan seorang penyerang untuk memulihkan pesan plaintext dari ciphertext.

Solusi
Hubungi vendor atau berkonsultasi dokumentasi produk untuk menonaktifkan CBC enkripsi modus cipher, dan memungkinkan RKT atau enkripsi modus GCM cipher.

*Server SSH dikonfigurasi untuk memungkinkan baik MD5 atau 96-bit MAC algoritma, yang keduanya dianggap lemah.

Solusi
Hubungi vendor atau berkonsultasi dokumentasi produk untuk menonaktifkan MD5 dan 96-bit MAC algoritma.

port 143 : IMAP



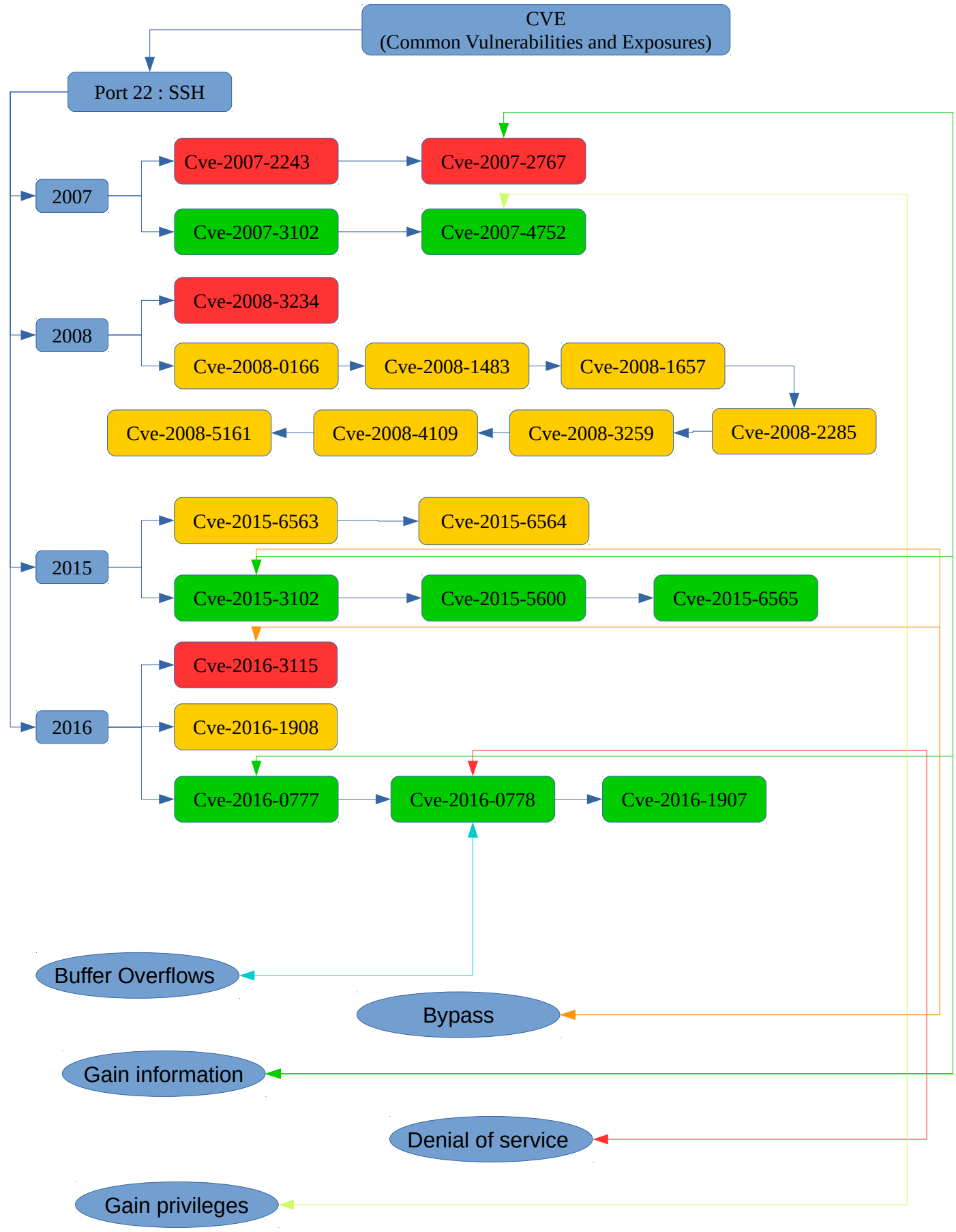
* Layanan IMAP mengandung cacat software dalam pelaksanaannya STARTTLS nya yang dapat memungkinkan remote, penyerang dikonfirmasi untuk menyuntikkan perintah selama fase protokol plaintext yang akan dijalankan selama fase protokol ciphertext. Jika eksploitasi sukses dapat memungkinkan penyerang untuk mencuri email korban atau SASL terkait (Authentication Sederhana dan Keamanan Layer) kredensial.

Solusi
hubungi vendor untuk melihat jika ada sistem update.

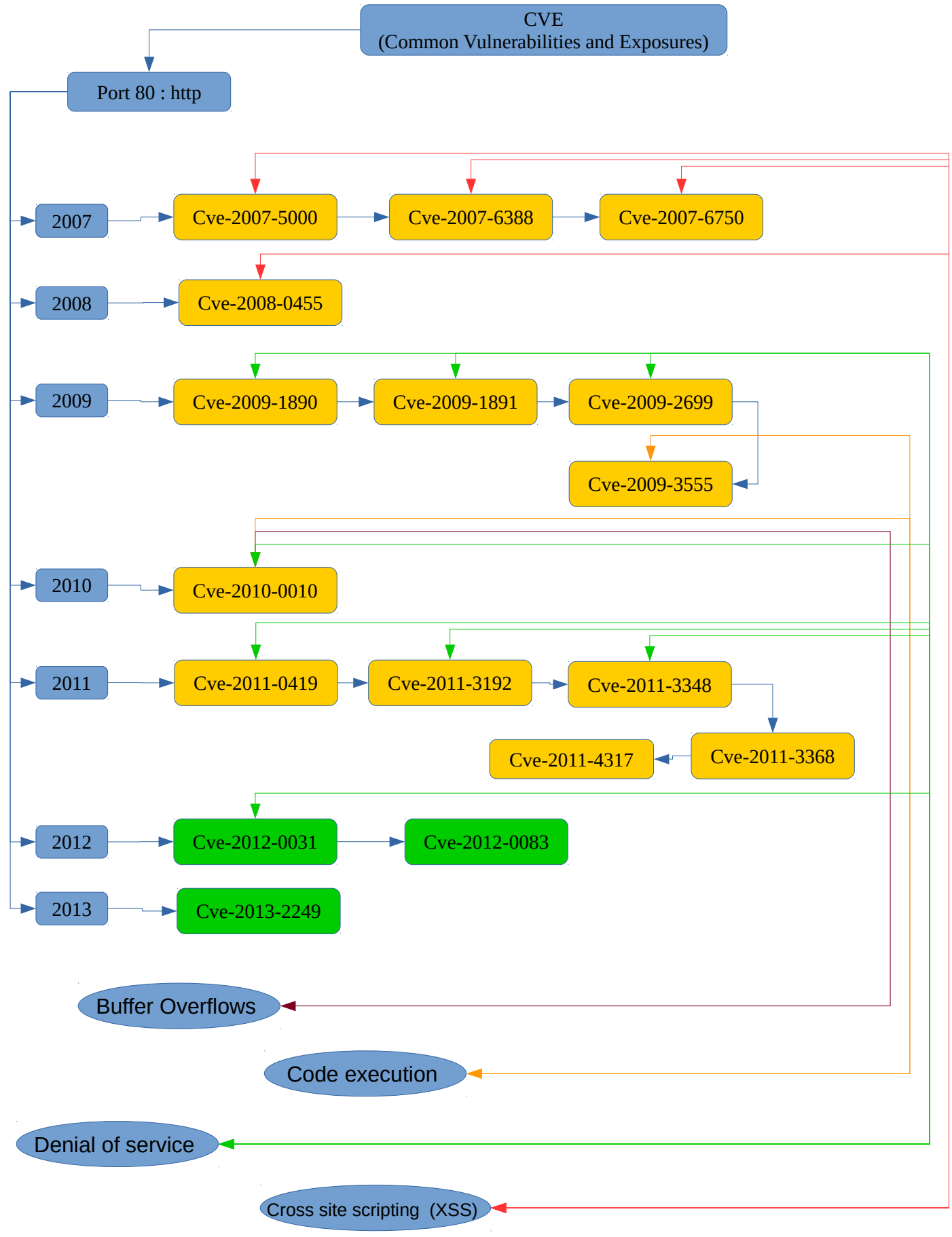
2.4. Mapping CVE
Dalam tools yang digunakan menunjukan kode CVE sebagai berikut:
80 : HTTP
CVE-2003-1418

22 dan 8080 : SSH
CVE-2008-5161

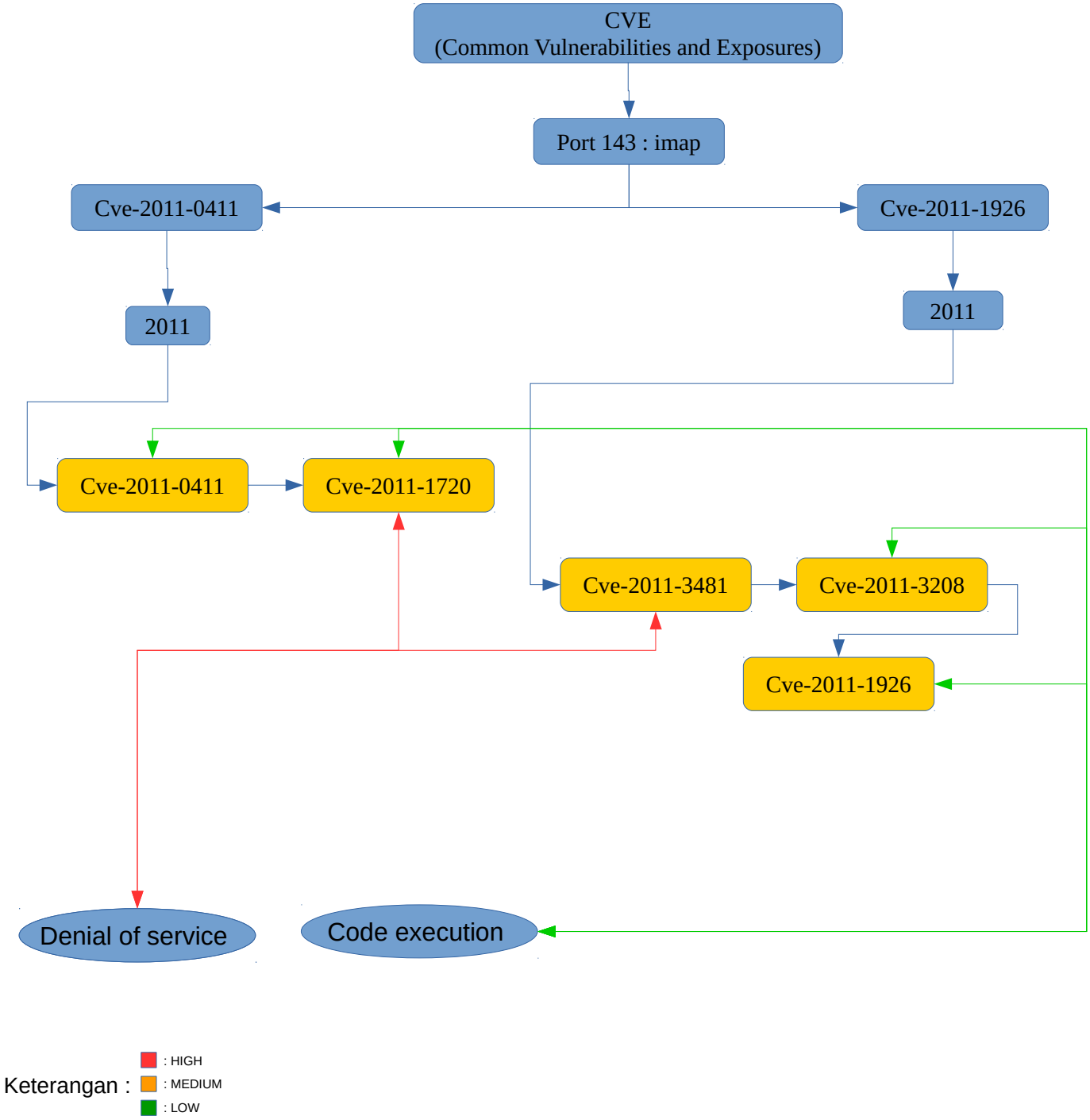
143 : IMAP
CVE-2011-0411, CVE-2011-1926



Keterangan :
- : HIGH
- : MEDIUM
- : LOW



Keterangan :
- : HIGH
- : MEDIUM
- : LOW



Keterangan :
- : HIGH
- : MEDIUM
- : LOW

Referensi :
1. nessus.org
2. nmap.org
3. openvas.org
4. cvedetails.com
5. security-tracker.debian.org/tracker/