UJIAN TENGAH SEMESTER MATA KULIAH KEAMANAN JARINGAN KOMPUTER

DISUSUN OLEH :

NAMA : AGUNG FITRIANDA

NIM : 09121001011

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

INDRALAYA

2016

Network Scanning

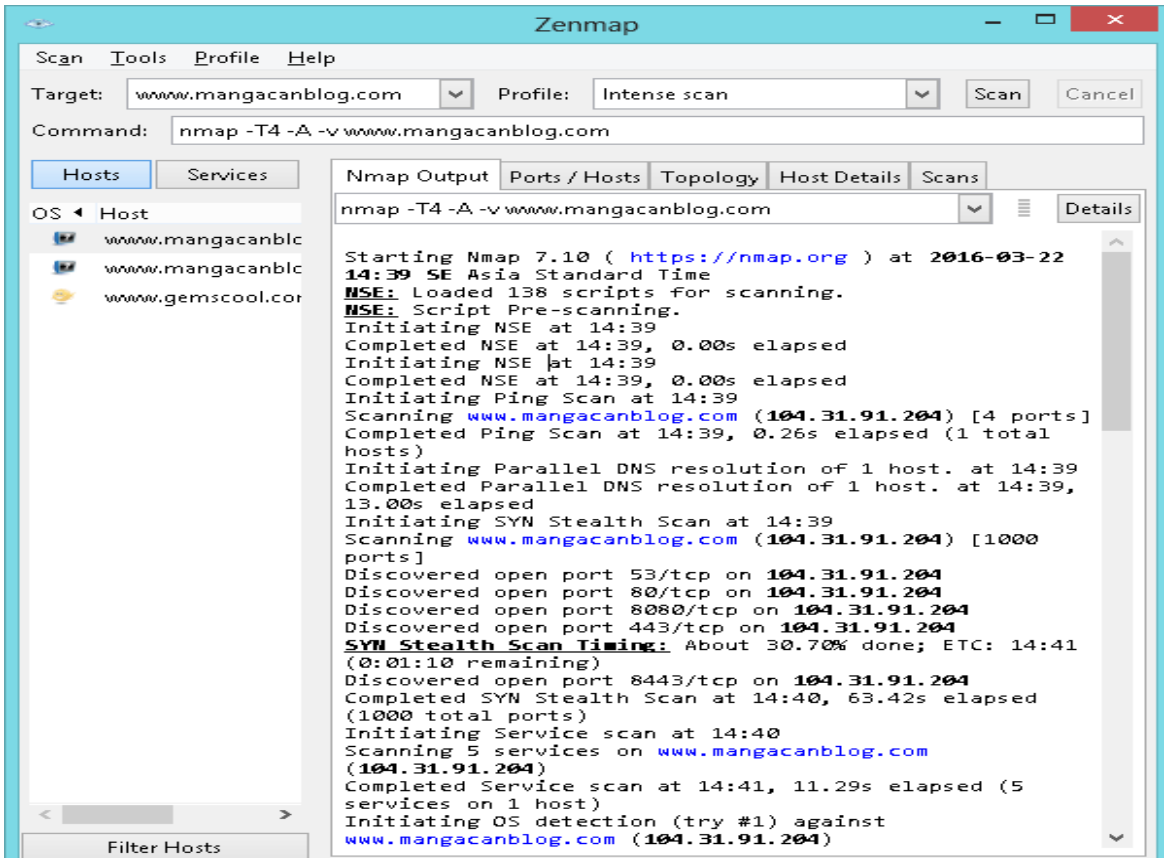
Pada percobaan kali ini, yang ingin dilakukan adalah mencoba proses network scanning, yaitu mencari informasi lebih banyak lagi tentang situs target menggunakan beberapa application scanning tools, sehingga diharapkan dengan percobaan ini, bisa mendapatkan informasi seperti open port berapa saja yang terbuka pada situs target, daemon atau servis apa saja yang berjalan pada situs target dan juga vulnerable atau kerentanan yang mungkin dapat ditemukan pada situs target tersebut, pada percobaan kali ini, scanning tools yang digunakan antara lain:

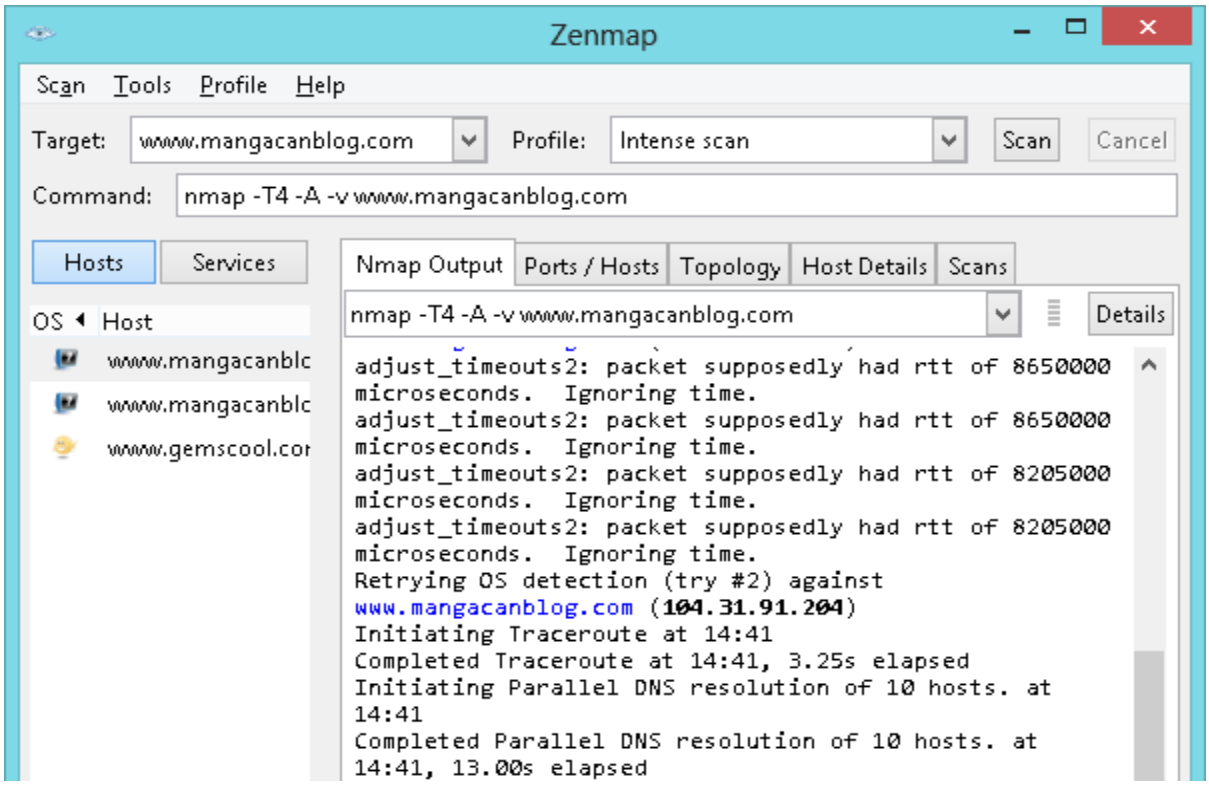
1. zen map,
2. nessus, dan
3. acunetix vulnerability scanner.

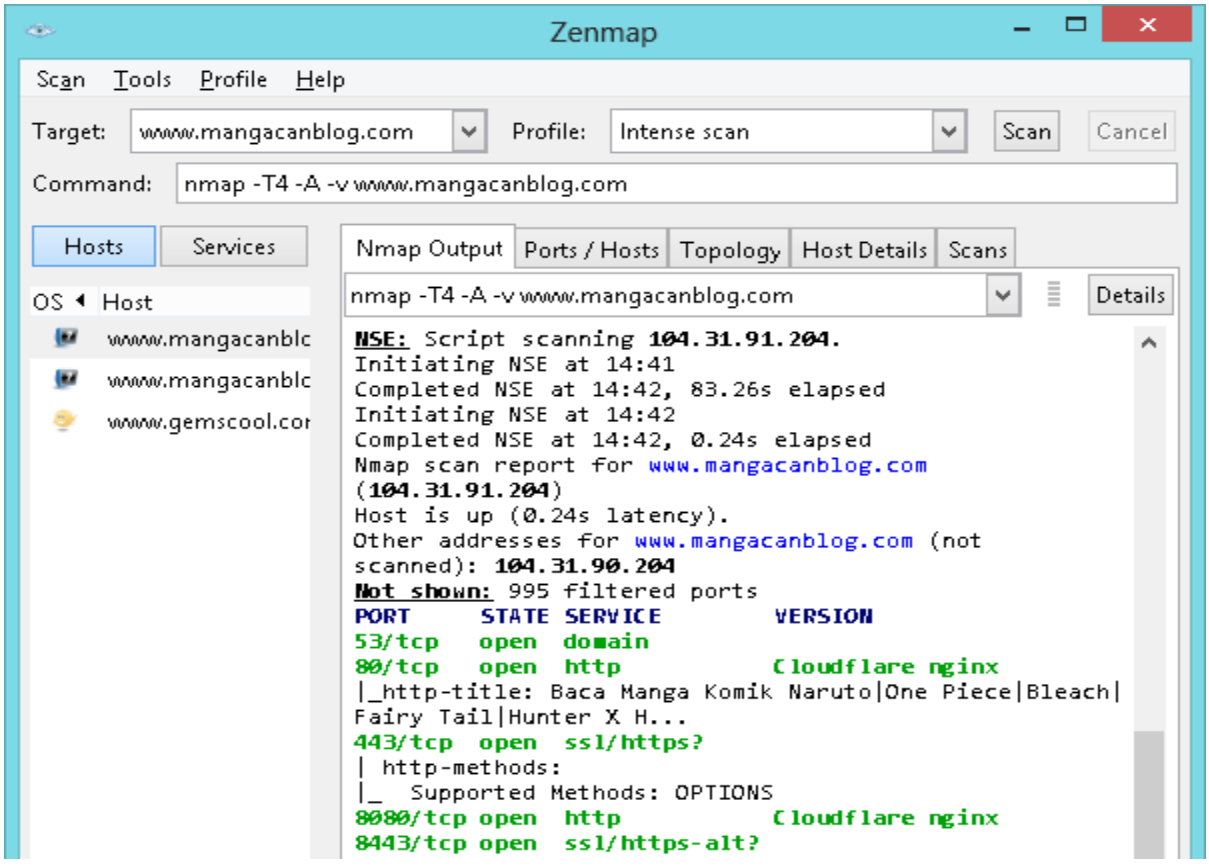
1. Scanning menggunakan Zenmap

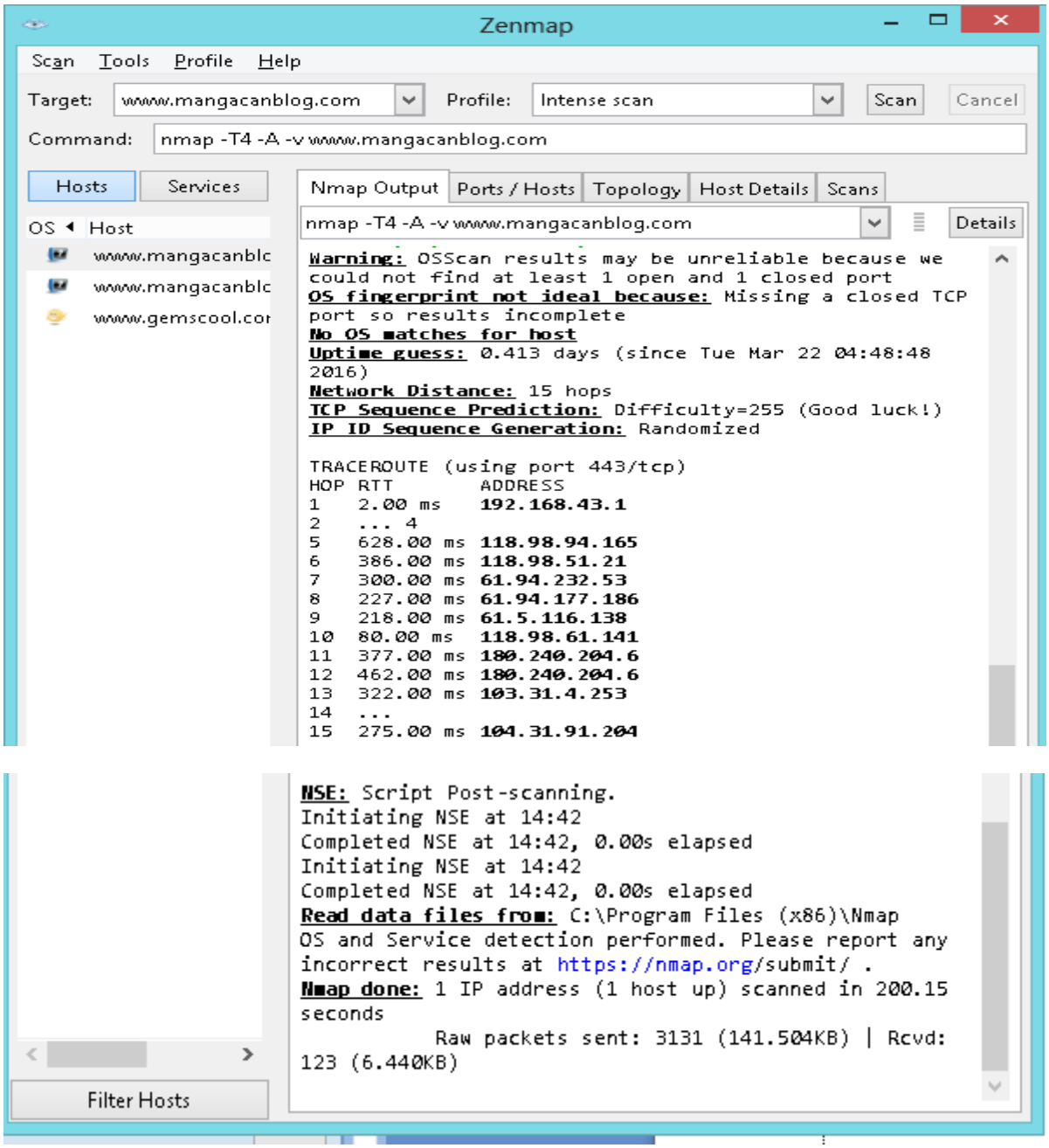
Situs Target : www.mangacanblog.com

Pada percobaan menggunakan aplikasi zenmap ini, kita sudah menentukan situs target, yaitu www.mangacanblog.com , kemudian,dengan aplikasi scanning tools zenmap ini, kita akan mencari open port mana saja yang ada pada situs target, artinya port tersebut terhubung dengan internet, pada tools zenmap, proses scanningnya adalah sebagai berikut :




Zenmap
Scan Tools Profile Help
Target: www.mangacanblog.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v www.mangacanblog.com
Hosts
Services
OS Host
www.mangacanblc
www.mangacanblc
www.gemscool.cor
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v www.mangacanblog.com
Details
adjust_timeouts2: packet supposedly had rtt of 8650000 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 8650000 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 8205000 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 8205000 microseconds. Ignoring time.
Retrying OS detection (try #2) against www.mangacanblog.com (104.31.91.204)
Initiating Traceroute at 14:41
Completed Traceroute at 14:41, 3.25s elapsed
Initiating Parallel DNS resolution of 10 hosts. at 14:41
Completed Parallel DNS resolution of 10 hosts. at 14:41, 13.00s elapsed


Zenmap
Scan Tools Profile Help
Target: www.mangacanblog.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v www.mangacanblog.com
Hosts
Services
OS Host
www.mangacanblc
www.mangacanblc
www.gemscool.cor
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v www.mangacanblog.com
Details
NSE: Script scanning 104.31.91.204.
Initiating NSE at 14:41
Completed NSE at 14:42, 83.26s elapsed
Initiating NSE at 14:42
Completed NSE at 14:42, 0.24s elapsed
Nmap scan report for www.mangacanblog.com (104.31.91.204)
Host is up (0.24s latency).
Other addresses for www.mangacanblog.com (not scanned): 104.31.90.204
Not shown: 995 filtered ports
PORT STATE SERVICE VERSION
53/tcp open domain
80/tcp open http Cloudflare nginx
|_http-title: Baca Manga Komik Naruto|One Piece|Bleach|Fairy Tail|Hunter X H...
443/tcp open ssl/https?
| http-methods:
|_ Supported Methods: OPTIONS
8080/tcp open http Cloudflare nginx
8443/tcp open ssl/https-alt?



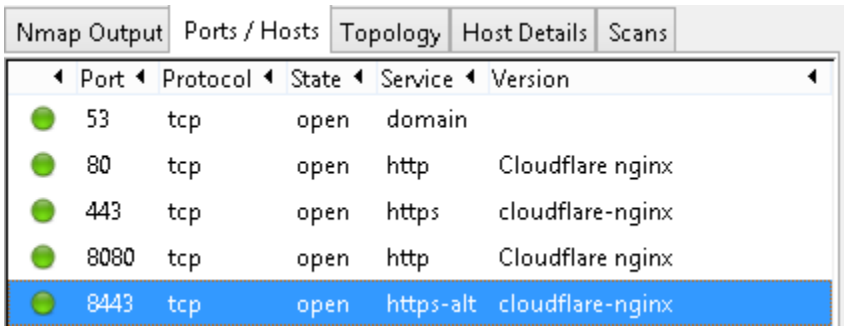
hasil proses scanning pada gambar diatas dapat diketahui informasi yang dimiliki oleh situs target tersebut, berupa IP yang dipakai oleh situs target www.mangacanblog.com yaitu 104.31.91.204, ditemukan juga port – port berapa saja yang terbuka, yaitu port 53, 80, 443, 8080, 844, network distance, yaitu 15 hop, peruteannya melalui :

hop 1 ip 192.168.43.1
hop 2 - 4 Request time out (tidak ditemukan hop ip route)
hop 5 ip 118.98.94.165
hop 6 ip 118.98.51.21
hop 7 ip 61.94.232.53

hop 8 ip 61.94.177.186
hop 9 ip 61.5.116.138
hop 10 ip 118.98.61.141
hop 11 ip 180.240.204.6
hop 12 ip 180.240.204.6
hop 13 ip 103.31.4.253
hop 14 request time out (tidak ditemukan hop ip route)
hop 15 104.31.91.204

dan juga raw paket data yang dikirim, yaitu 3131(dengan ukuran data sebesar 141.504kb) dan paket yang diterima yaitu 123 (ukuran data sebesar 6443kb), jadi paket yang tidak kembali yaitu 3131 – 123 = 3008 paket .

open port yang didapat adalah sebagai berikut :



Pada gambar diatas dapat diketahui bahwa port – port yang terbuka (ditandai dengan ikon hijau di sebelah kiri) adalah :

1. Port 53, yang merupakan port DNS, atau *Domain Name Server* port. Name Server menggunakan port ini.
2. Port 80, yang biasanya digunakan untuk web server, jadi ketika user mengetikan alamat IP atau hostname di web broeser maka web browser akan melihat IP tersebut pada port 80.
3. Port 443, adalah Secure Sockets Layer (SSL) Server Ketika Anda menjalankan server yang aman, Klien SSL ingin terhubung ke server aman Anda akan terhubung pada port 443. Port ini harus terbuka untuk menjalankan server Transaksi aman Anda sendiri.
4. Port 8080, adalah Common Web Cache dan port server Proxy Web.
5. Port 8443, port ini umumnya digunakan oleh produk apple, yaitu pada Layanan iCal (SSL), pada system operasi Mac OS X Server v10.5 dan versi lebih baru.

Daemon :

Setelah mendapatkan open port, dengan menggunakan tools zenmap ini juga, daemon atau service yang berjalan pada situs target dapat diketahui adalah sebagai berikut :

1. Pada port 53, protocol tcp, service yang digunakan sebagai domain
2. Pada port 80, protocol tcp, service yang digunakan adalah http dengan versi Cloudflare-nginx

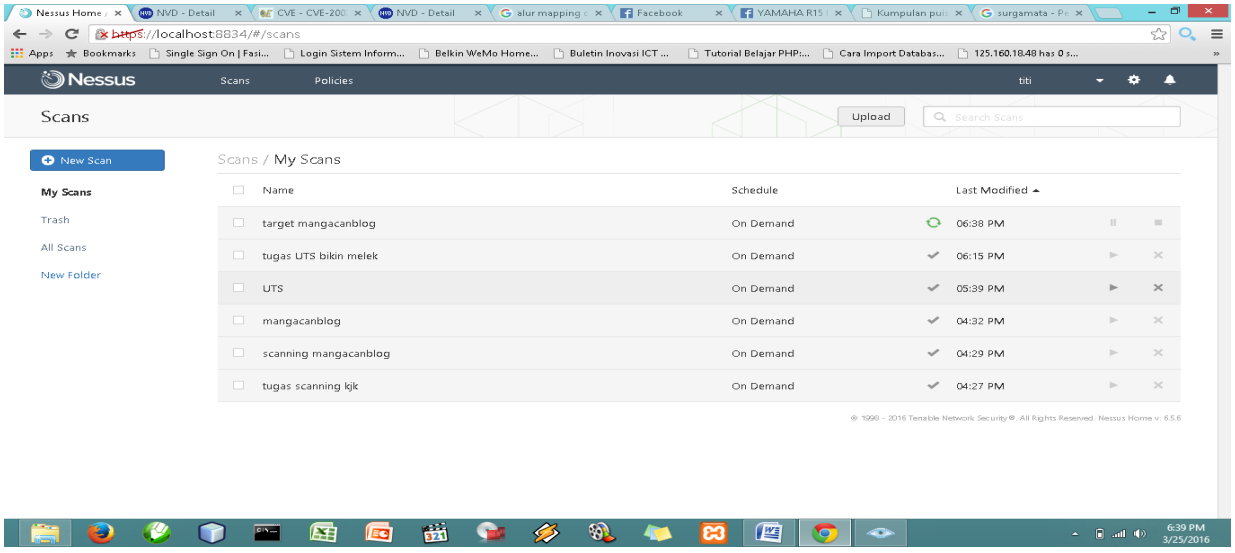
3. Pada port 443, protocol tcp, service yang digunakan adalah https dengan versi cloudflare-nginx
4. Pada port 8080, protocol tcp, service yang digunakan adalah http dengan versi cloudflare-nginx
5. Pada port 8443, protocol tcp, service yang digunakan adalah https-alt dengan versi cloudflare-nginx.

2. Scanning menggunakan nessus

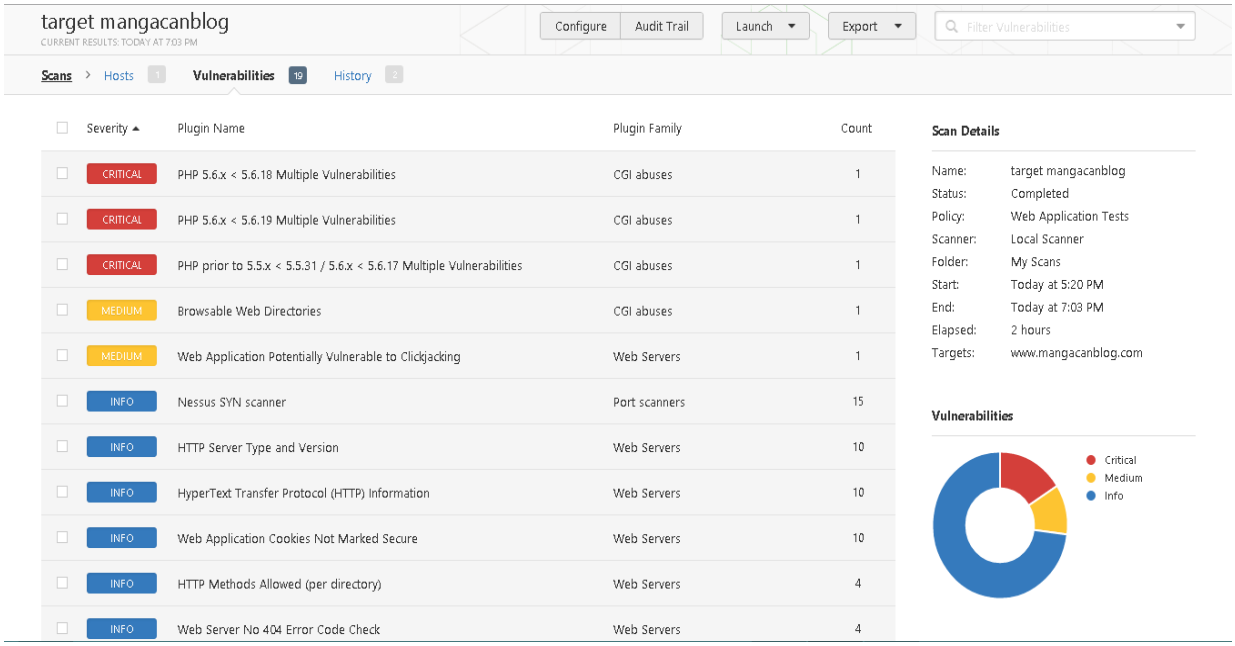
Pada percobaan kali kedua ini, tools yang digunakan adalah nessus scanning, tidak jauh berbeda dengan zenmap yang digunakan sebelumnya, Cuma dengan aplikasi nessus ini, informasi yang didapatkan lebih banyak, serta kita dapat mendapatkan informasi yang tidak dapat ditemukan menggunakan zenmap scanning tools, seperti vulnerable resreting dan CVE pada situs target.

Situs target : www.mangacanblog.com

Langkah awal adalah melakukan penginstalan nessus scanning di computer, setelah itu login ke situs nessus, kemudian memasukkan username dan password yang sudah kita buat sebelumnya, lalu setelah masuk ke nessus akun, selanjutnya adalah memulai proses scanning dengan memasukkan alamat target, dan setelah itu proses scanning sudah bisa dimulai dengan mengklik launch dan hasilnya adalah sebagai berikut (scan yang dipilih adalah target mangacanblog) :

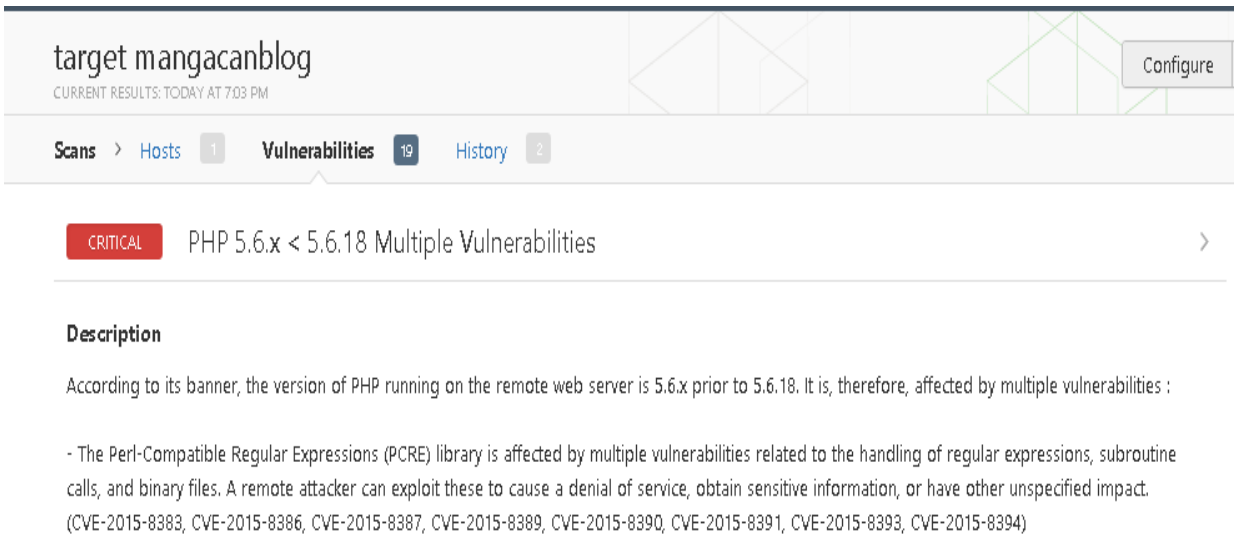


setelah beberapa saat, kemudian hasil scan akan muncul dan gambarnya adalah sebagai berikut:



Pada gambar, dapat diketahui bahwa terdapat 3 risk rating bernilai critical, hal ini merupakan vulnerability yang sangat besar dan memiliki peluang untuk dieksploitasi, pada gambar juga dapat ketahui bahwa risk rating tertinggi (critical) dapat kita kenali pada kolom merah, jadi dengan mendapatkan risk rating pada proses scanning ini, kita akan mendapatkan CVE (Common Vulnerability and Exposurz) ketiga risk rating yang bernilai critical dan juga memetakannya, yaitu adalah sebagai berikut :

Risk rating critical 1



Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

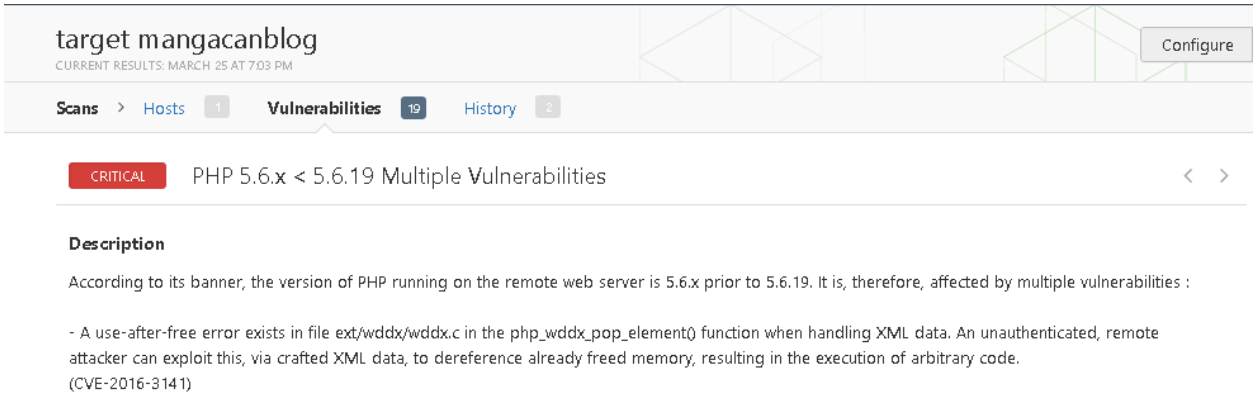
Vulnerability Information

CPE: cpe:/a:php:php
Patch Pub Date: 2016/02/04
Vulnerability Pub Date: 2015/11/23

Reference Information

CVE: CVE-2015-8383, CVE-2015-8386, CVE-2015-8387, CVE-2015-8389, CVE-2015-8390, CVE-2015-8391, CVE-2015-8393, CVE-2015-8394
OSVDB: 131055, 131059, 131060, 131062, 131063, 131064, 131066, 131067, 134028, 134029, 134030, 134031, 134032, 134033, 134034
BID: 79810, 82990

Risk rating critical 2



Risk Information

Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
IAVM Severity: I

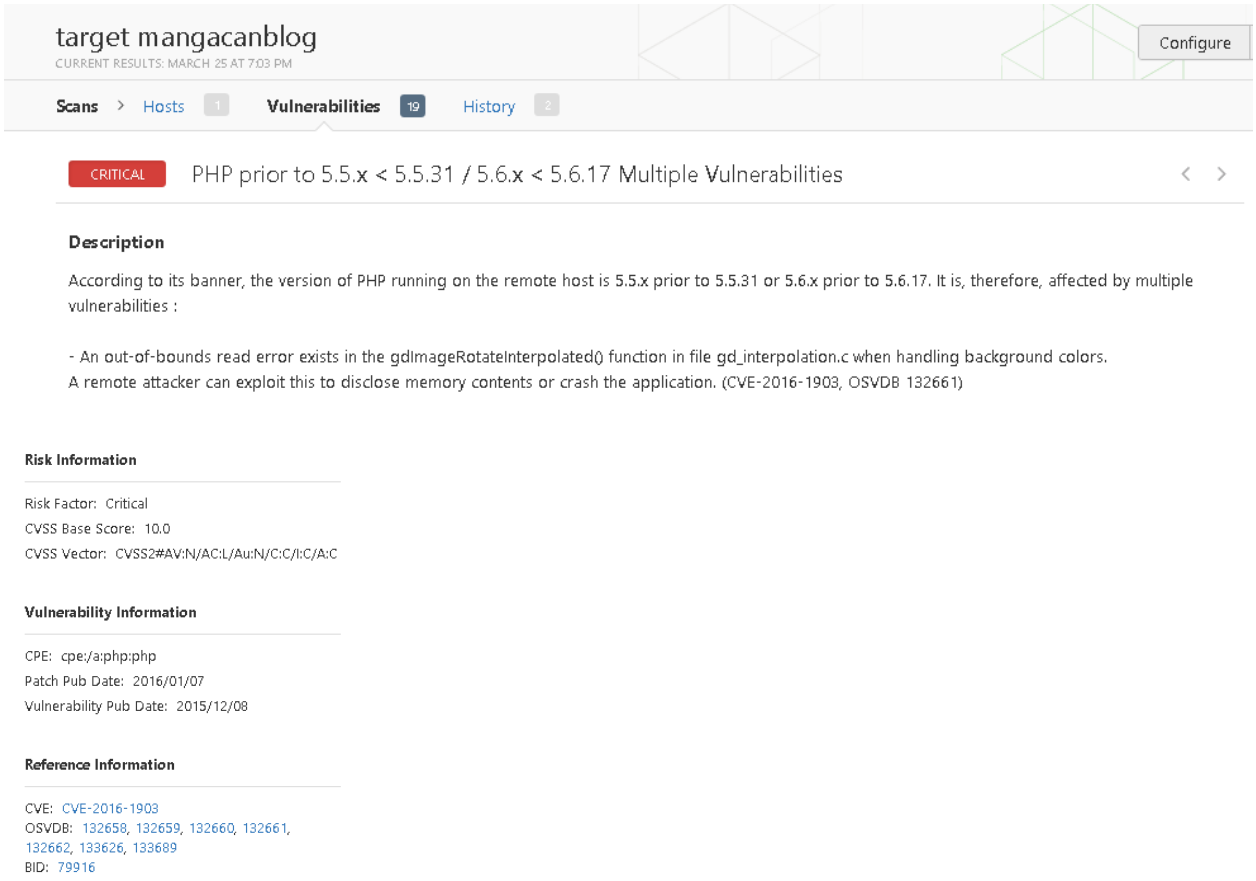
Vulnerability Information

CPE: cpe:/a:php:php
Patch Pub Date: 2016/03/03
Vulnerability Pub Date: 2016/02/09

Reference Information

CVE: CVE-2016-3141, CVE-2016-3142
OSVDB: 135224, 135225, 135344, 135345, 135346, 135347
IAVB: 2016-B-0052
BID: 84271, 84306, 84307, 84348, 84349, 84350, 84351

Risk rating critical 3 :



Dari gambar diatas, dapat diketahui bahwa CVE yang didapat pada proses scanning ini yang dimiliki oleh situs target www.mangacanblog.com adalah sebagai berikut :

CVE pada risk rating (critical) 1 :

1. CVE-2015-8383
2. CVE-2015-8386
3. CVE-2015-8387
4. CVE-2015-8389
5. CVE-2015-8390
6. CVE-2015-8391
7. CVE-2015-8393
8. CVE-2015-8394

CVE pada risk rating (critical) 2 :

1. CVE-2016-3141
2. CVE-2016-3142

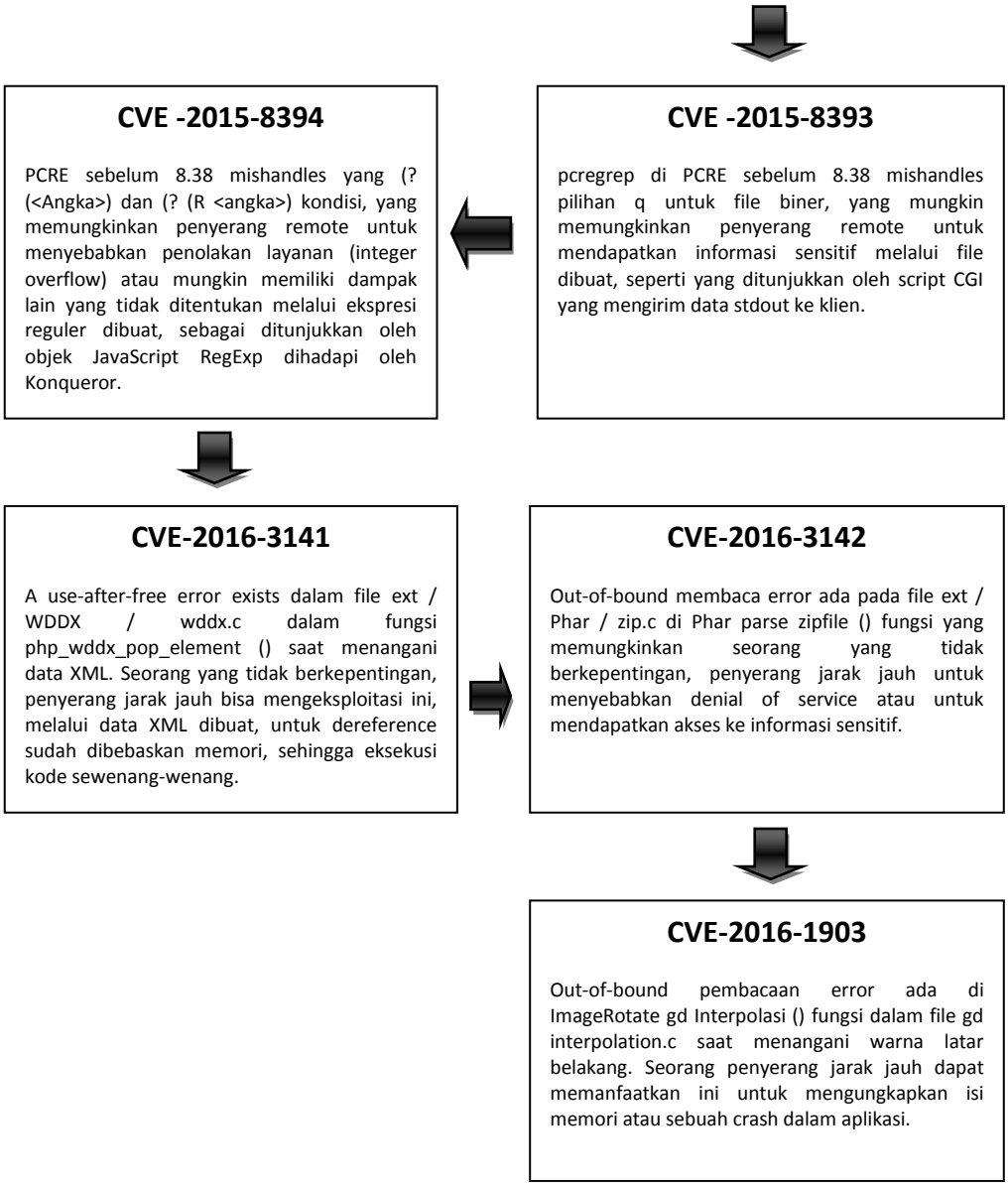
CVE pada risk rating (critical) 3 :

1. CVE-2016-1903

Setelah itu, dengan CVE yang telah kita dapatkan dalam proses scanning tadi, kita dapat memetakan CVE tadi seperti berikut (gabungan mulai dari CVE pada rsik rating critical 1 sampai 3) :

Deskripsi CVE keseluruhan pada risk rating critical 1:

Perl-Kompatibel Regular Expressions (PCRE) library dipengaruhi oleh beberapa kerentanan terkait dengan penanganan ekspresi reguler, panggilan subroutine, dan file biner. Seorang penyerang jarak jauh dapat memanfaatkan ini untuk menyebabkan penolakan layanan, mendapatkan informasi sensitif, atau memiliki dampak yang tidak ditentukan lain.

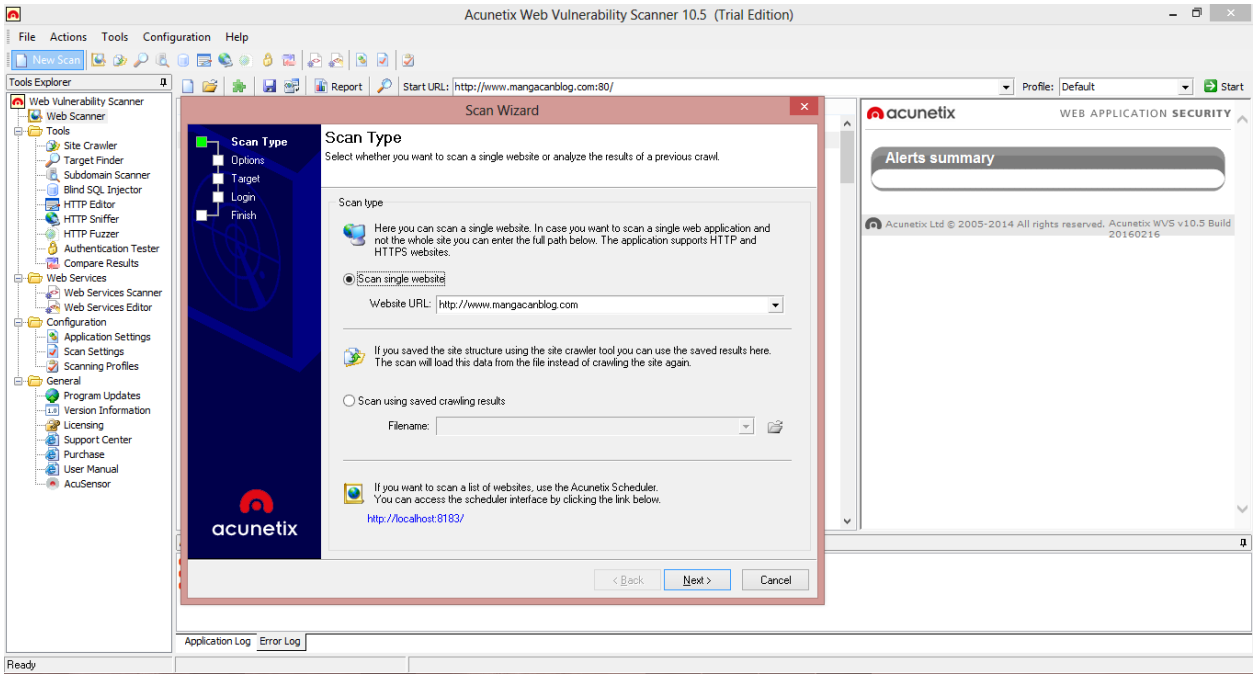


3. Scanning menggunakan acunetix vulverability scanner

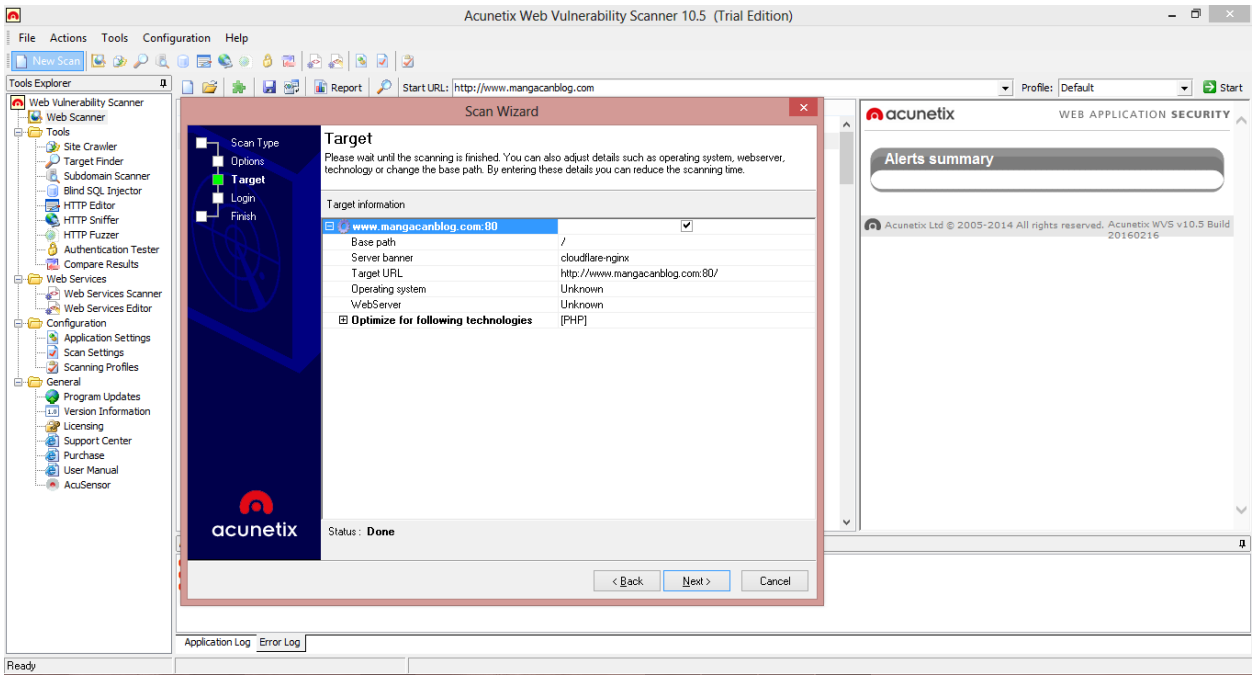
Pada percobaan yang ketiga ini, yang ingin dilakukan adalah sama seperti percobaan sebelumnya yaitu mencari informasi lagi tentang situs target, namun dengan menggunakan scanning tools yang berbeda, pada percobaan scanning ketiga ini, scanning tools yang digunakan adalah acuntix vulnerability scanner. Dengan scanning tools ini, kita bisa mendapatkan informasi yang diinginkan seperti open port dan vulnerability yang dimiliki oleh situs target.

Situs target : www.mangacanblog.com

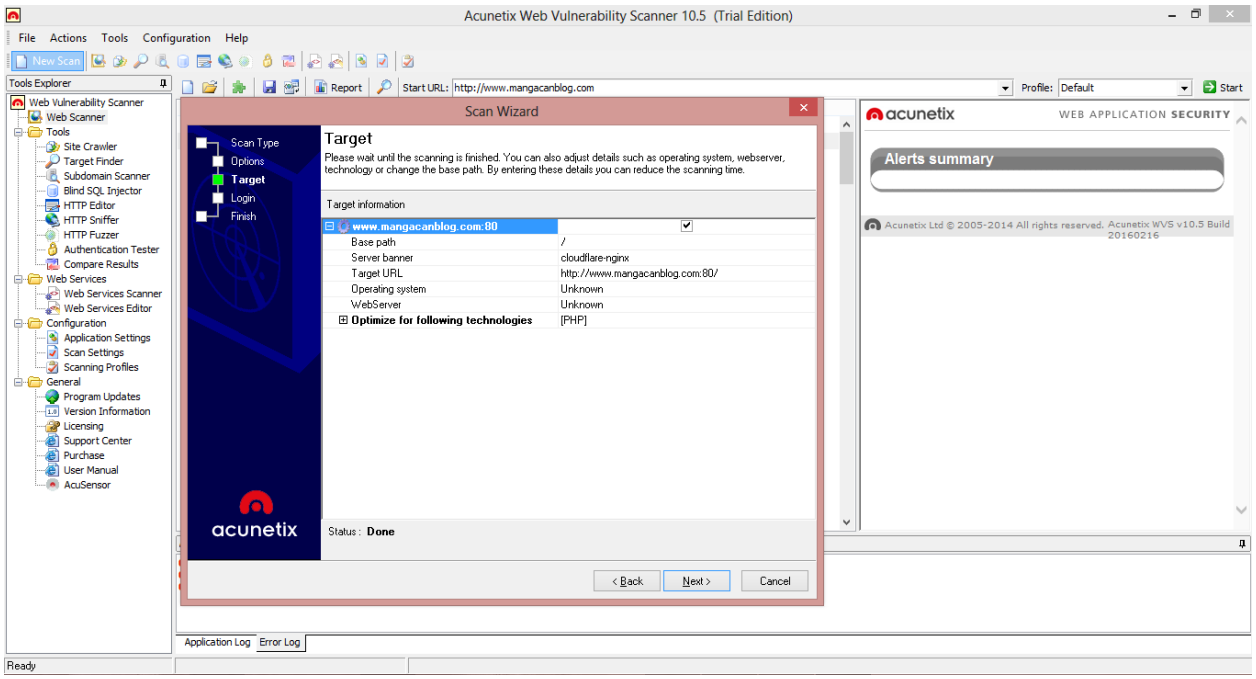
Langkah awal adalah melakukan penginstalan acunetix vulnerability scanner di computer, lalu setelah aplikasi acunetix telah terinstal di computer, maka proses scanning sudah bisa dilakukan. Berikut adalah gambar langkah awal memulai proses scanning.



Pada step ini, ketika aplikasi acunetix telah terbuka, kita bias langsung mengklik new scan yang ada di pojok kiri atas, kemudian pada menu di scan wizard, masukkan hostname situs target yang ingin scanning, pada percobaan ini situs target adalah www.mangacanblog.com .



Kemudian pada proses selanjutnya, informasi tentang situs target ada yang sudah ditemukan, misalnya tentang server yang digunakan, situs target menggunakan server cloudflare-nginx dan service yang digunakan berbasis PHP. Seperti pada gambar dibawah ini :



Lalu, proses scanning keseluruhan telah dimulai setelah melakukan setting pada scan wizard, dan untuk beberapa saat, hasil scanning akan muncul, seperti pada gambar dibawah ini :

Scanning open port :

Deskripsi port :

Open Port **25 / smtp**
Port Banner:

```
220 [104.31.90.204] ESMTP Smtpd; Sat, 26 Mar 2016 18:55:56 +0700
```

Open Port **53 / domain**

Open Port **80 / http**
Port Banner:

```
HTTP/1.1 403 Forbidden
Date: Sat, 26 Mar 2016 11:58:12 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: __cfduid=d664788ac61533cfe6c600cf0930d56ee1458993492;
expires=Sun, 26-Mar-17 11:58:12 GMT; path=/; domain=.35f75; HttpOnly
Cache-Control: max-age=15
Expires: Sat, 26 Mar 2016 11:58:27 GMT
X-Frame-Options: SAMEORIGIN
Server: cloudflare-nginx
CF-RAY: 289a6df01f6530d2-SIN

<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]>    <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]>    <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Direct IP access not allowed | CloudFlare</title></title>
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
<meta name="view
```

Open Port **443 / https**
Port Banner:

```
HTTP/1.1 400 Bad Request
Server: cloudflare-nginx
Date: Sat, 26 Mar 2016 12:07:46 GMT
Content-Type: text/html
Content-Length: 677
Connection: close

<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare-nginx</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

```
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

Open Port **2053 / knetd**
Port Banner:

```
HTTP/1.1 400 Bad Request
Server: cloudflare-nginx
Date: Sat, 26 Mar 2016 12:28:06 GMT
Content-Type: text/html
Content-Length: 677
Connection: close

<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare-nginx</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

Open Port **8080 / http-proxy**
Port Banner:

```
HTTP/1.1 403 Forbidden
Date: Sat, 26 Mar 2016 12:36:12 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: __cfduid=dcd52024198711c7d83378300d82bb47f1458995772;
expires=Sun, 26-Mar-17 12:36:12 GMT; path=/; domain=.35f67; HttpOnly
Cache-Control: max-age=15
Expires: Sat, 26 Mar 2016 12:36:27 GMT
X-Frame-Options: SAMEORIGIN
Server: cloudflare-nginx
CF-RAY: 289aa59ac4ee30a2-SIN

<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]>    <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]>    <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Direct IP access not allowed | CloudFlare</title></title>
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge,chrome=1" />
<meta name="robots" content="noindex, nofollow" />
```

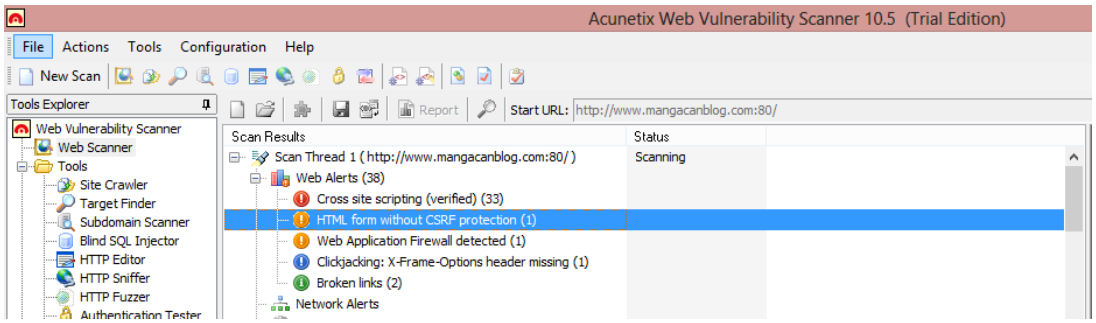
```
<meta name="view
```

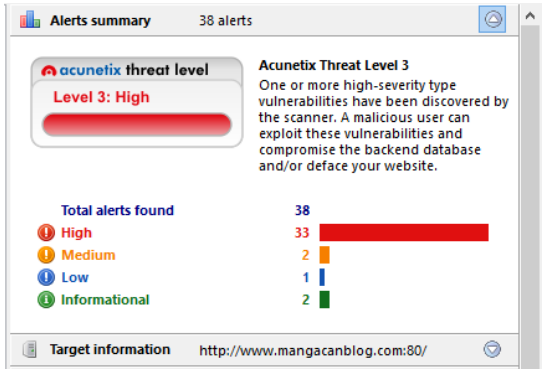
Open Port **8443 / https-alt**
Port Banner:

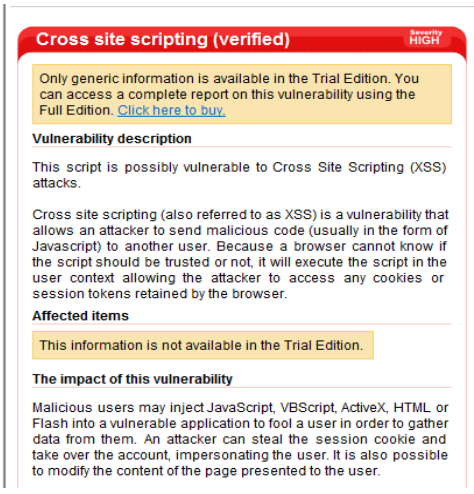
```
HTTP/1.1 400 Bad Request
Server: cloudflare-nginx
Date: Sat, 26 Mar 2016 12:36:30 GMT
Content-Type: text/html
Content-Length: 677
Connection: close

<html>
<head><title>400 The plain HTTP request was sent to HTTPS port</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<center>The plain HTTP request was sent to HTTPS port</center>
<hr><center>cloudflare-nginx</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

Scanning web vulnerability :







Pada hasi scanning, didapatkan web vulnerability yang dimiliki oleh situs target (mangacanblog.com), pada gambar dapat diketahui bahwa terdapat banyak vulnerability dimana risk ratingnya bernilai high (pada kolom merah), hal ini berarti situs target sangat rentan terhadap serangan atau berbagai macam tindak eksploitasi, berikut adalah penjelasan mengenai vulnerability pada situs target tersebut :

1. Cross site scripting
   script ini mungkin rentan terhadap Cross Site Scripting (XSS) serangan.
   scripting lintas situs (juga disebut sebagai XSS) adalah kerentanan yang memungkinkan penyerang untuk mengirimkan kode berbahaya (biasanya dalam bentuk Javascript) ke pengguna lain. Karena browser tidak bisa tahu apakah script harus dipercaya atau tidak, itu akan mengeksekusi script dalam konteks pengguna yang memungkinkan penyerang untuk mengakses cookie atau token sesi disimpan oleh browser.

   Dampak vulnerability:
   Pengguna berbahaya mungkin menyuntikkan JavaScript, VBScript, ActiveX, HTML atau Flash ke dalam aplikasi rentan untuk menipu pengguna untuk mengumpulkan data dari mereka. Seorang penyerang bisa mencuri cookie sesi dan mengambil alih akun, meniru pengguna. Hal ini juga memungkinkan untuk memodifikasi isi dari halaman disajikan kepada pengguna.