FAKULTAS ILMU KOMPUTER – SISTEM KOMPUTER

Universitas Sriwijaya

Muhamad Rifki || 09011181320049

TARGET SCANNING

Penetration testing merupakan tindakan yang membahayakan data (Whitaker, 2005) karena pelaku pengujian bersifat aktif dalam melakukan berbagai serangan untuk mencari kelemahan sistem. Penerapan penetration testing pada sebuah institusi membutuhkan perencanaan dan persiapan yang matang sehingga tidak beresiko besar yang bersifat merugikan pihak institusi selaku pemilik aset dan pihak pelaku pengujian. Metodologi yang digunakan untuk melakukan penetration testing untuk WLAN sudah ada seperti yang dikeluarkan oleh lembaga OIISG (Open Information System Security Group) yang terdokumentasi dalam ISSAF Penetration Testing. ISSAF (Information Systems Security Assessment Framework) merupakan kerangka kerja yang dapat digunakan sebagai acuan untuk melakukan assessment keamanan sistem. Berikut adalah kerangka kerja untuk melakukan penetration testing pada sebuah website menurut ISSAF.

1. Gathering information.
2. Scanning & Research.
3. Exploit & Attack.
4. Reporting & Presentation.

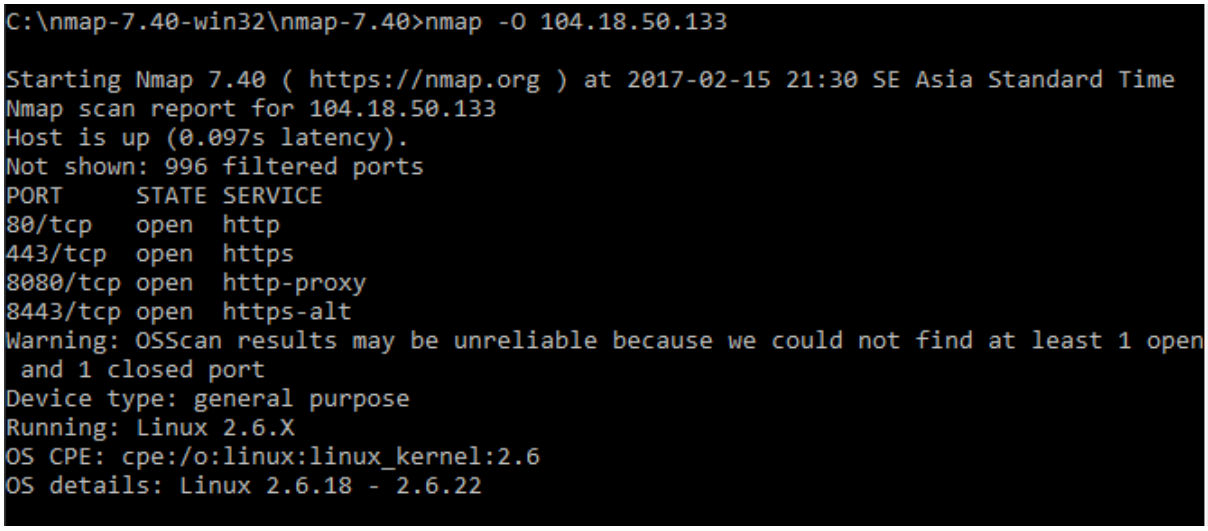
Tulisan ini akan membahas tahap kedua pada *penetration testing* yaitu target scanning dengan menggunakan tools yang sudah banyak bertebaran di internet. Salah satu tools yang populer untuk melakukan scanning adalah *nmap.*

Nmap (Network Mapper) adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan jenis kegiatan scanning, salah satunya adalah *port scanning*. Nmap dibuat oleh Gordon Lyon, atau lebih dikenal dengan nama Fyodor Vaskovich. Aplikasi ini digunakan untuk meng-audit jaringan yang ada. Dengan menggunakan tool ini, kita dapat melihat host yang aktif, port yang terbuka, Sistem Operasi yang digunakan, dan feature-feature scanning lainnya. Pada awalnya, Nmap hanya bisa berjalan di sistem operasi Linux, namun dalam perkembangannya sekarang ini, hampir semua sistem operasi bisa menjalankan Nmap.

1. **OS scanning**

Perintah ini berfungsi untuk mengetahui sistem operasi yang dipakai oleh target. Dalam kasus ini dapat dilihat bahwa website *revolusimental.go.id* menjalankan layanan sistem operasi linux versi 2.6.18 – 2.6.22. Selain sistem operasi yang dijalankan , Perintah tersebut juga dapat mendeteksi port – port yang terbuka pada website target. Terlihat dalam Gambar 1 tersebut port – port yang terbuka adalah port 80(http) , 443 (https) , 8080 (http - proxy) , 8443 (https - alt).

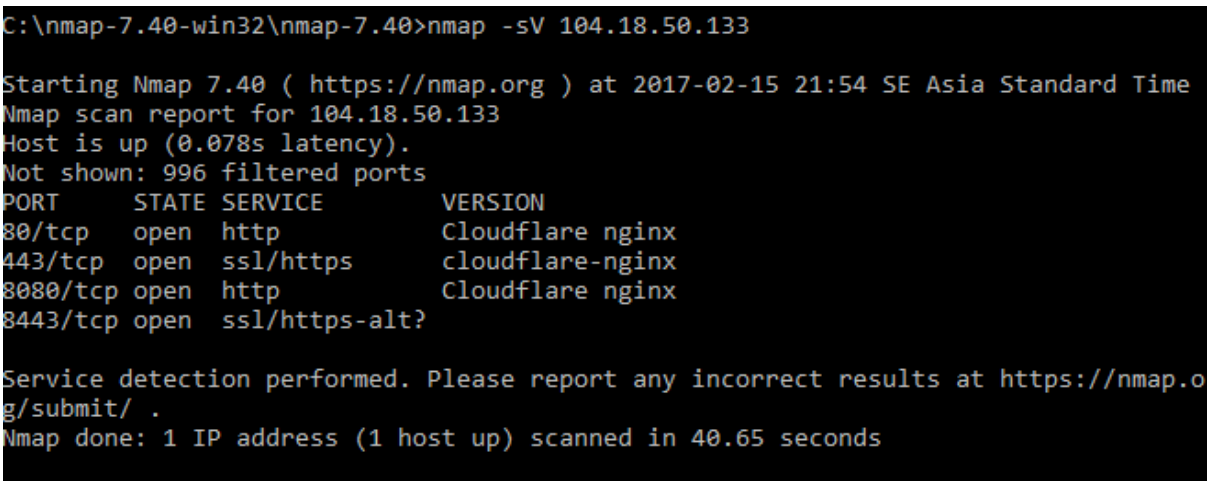
Gambar 1 (Perintah –O pada *nmap*)



2. **Port scanning**

Perintah ini hampir sama dengan perintah diatas, namun sedikit berbeda karena perintah tersebut dapat mendeteksi layanan pada target. Dapat dilihat target menggunakan nginx untuk semua port yang terdeteksi.

Gambar 2 (Perintah –sV pada *nmap*)



3. Service scanning

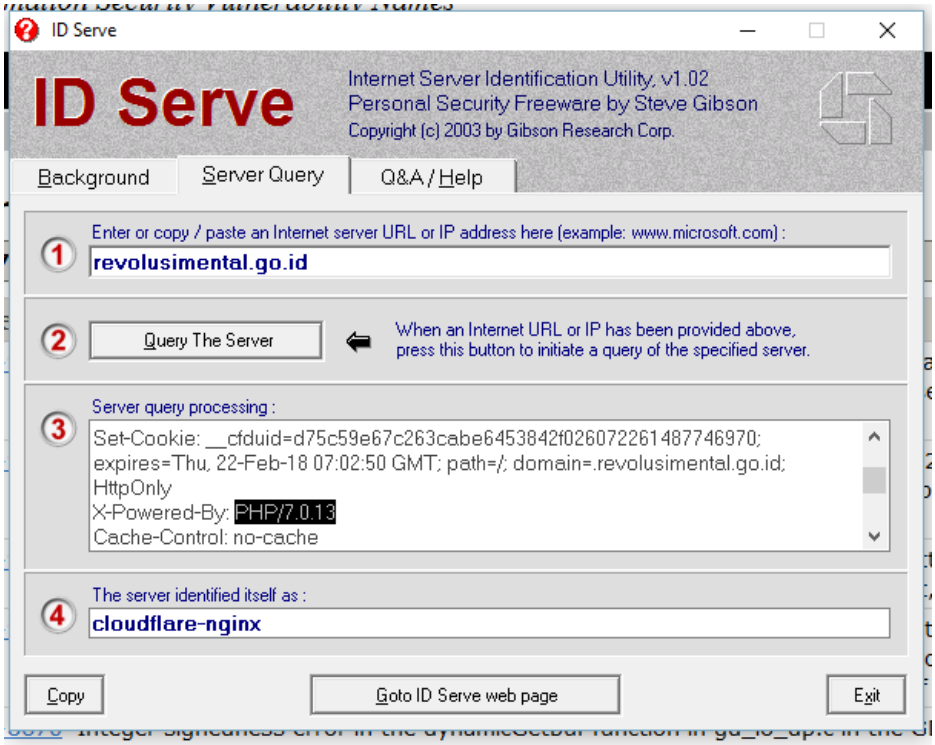
Apakah port scanning merupakan salah satu dari cybercrime? Salah satu langkah yang dilakukan cracker sebelum masuk ke server yang ditargetkan adalah melakukan pengintaian.

Cara yang dilakukan adalah dengan melakukan "service scanning" untuk melihat servis-servis apa saja yang tersedia di server target. Sebagai contoh, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server Sendmail, dan seterusnya.

Analogi hal ini dengan dunia nyata adalah dengan melihat-lihat apakah pintu rumah anda terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan atau tidak) dan seterusnya. Yang bersangkutan memang belum melakukan kegiatan pencurian atau penyerangan, akan tetapi kegiatan yang dilakukan sudah mencurigakan.

Service scanning pada website target (*revolusimental.go.id*) menggunakan tools ID SERVE.

(Gambar 3 (hasil service scanning menggunakan ID SERVE)



4. CVE (Common Vulnerabilities And Exposures)

CVE merupakan sebuah kamus untuk keamanan jaringan internet. Dimana pada website nya , tersedia jutaan vulnerabilities dan solusi yang sudah ditemukan oleh banyak pengembang. CVE juga dapat memudahkan hackers untuk melakukan serangan ke target dengan informasi informasi yang tersedia banyak pada CVE. Dalam kasus ini , setelah melakukan scanning ke website target dan mendapatkan informasi – informasi service atau layanan yang di gunakan oleh target, kita dapat mencari kelemahan – kelemahan service tersebut pada CVE.

Berikut adalah service yang digunakan oleh *revolusimental.go.id*

1. Cloudflare – nginx (web server)

   CVE 2016 – 4450

   Impact :
   Denial Of Service via network

   Description :
   A vulnerability was reported in nginx. A remote user can cause denial of service conditions on the target system. A remote user can send specially crafted data to trigger a null pointer dereference in the ngx_chain_to_iovec() function when saving the client request body to a temporary file and cause a worker process to crash.

   Solution :
   The vendor has issued a fix (1.10.1, 1.11.1).

   CVE 2013 – 4547

   Impact :

   restriction bypass problem

   Description :

   The nginx webserver was fixed to avoid a restriction bypass when a space in not correctly escaped

CVE 2016 – 1247

Discovered by: Dawid Golunski (@dawid_golunski) https://legalhackers.com

Description :

Nginx web server packaging on Debian-based distributions such as Debian or Ubuntu was found to create log directories with insecure permissions which can be exploited by malicious local attackers to escalate their privileges from nginx/web user (www-data) to root.
The vulnerability could be easily exploited by attackers who have managed to compromise a web application hosted on Nginx server and gained access to www-data account to escalate their privileges to root without any admin interaction thanks to cron.daily.

Solution :

Vulnerability fixed in the following packages:
Nginx 1.6.2-5+deb8u3 package on Debian
Nginx 1.10.0-0ubuntu0.16.04.3 on Ubuntu (16.04 LTS).

2. PHP 7.0.13

CVE 2016 – 9936
Description :
The unserialize implementation in ext/standard/var.c in PHP 7.x before 7.0.14 allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted serialized data.

CVE 2016 – 9935
Description :
The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.29 and 7.x before 7.0.14 allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.