

Tugas

Keamanan Jaringan Komputer



Disusun Oleh :

Nama : Sigit Wijaya Pramono

NIM : 09011181419012

**JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2018**

Laporan Hands-on Port Scanning Menggunakan Nmap

1. Teori

Pada handson mata kuliah Keamanan Jaringan Komputer ini melakukan praktik secara langsung beberapa materi yang berhubungan dengan keamanan jaringan komputer, yaitu mulai dari *footprinting*, *scanning network*, dan *CVE*. Dimana dalam setiap topik-topik tersebut terdapat bagian-bagian lagi yang akan dibahas selanjutnya. Berikut merupakan penjelasan singkat dari setiap topik handson yang telah dilakukan :

a. Footprinting

Dalam proses ini terdapat beberapa step yang dilakukan, bisa dilakukan dalam terminal kali linux atau web browser. Diantaranya yaitu :

- *Whois*

Whois adalah suatu prosedur untuk mendapatkan informasi mengenai sebuah domain. Informasi yang bisa di dapat meliputi siapa pemilik Domain, dimana alamatnya, no telepon, alamat email, kapan domain ini di daftarkan dan kapan domain ini akan expired.

- *WhatWeb*

WhatWeb merupakan sebuah tools enumeration web information gathering yang mempunyai fungsi untuk mencari informasi-informasi DNS(Domain Name Server), lokasi server, sub-domain, versi php, jenis database, ip address, cms yang digunakan dan lain-lain.

- *Netcraft*

Netcraft adalah sebuah Perusahaan Jasa Internet yang berbasis di Bath, Inggris. Dan bergerak di bidang IT Security yang fungsinya melayani pelanggannya terutama di bidang keamanan Website, salah satu Tools yang dibuatnya adalah Netcraft Anti-Phising Toolbar.

- *Reverse Domain*

Reverse DNS adalah mapping alamat IP ke suatu nama domain. Jadi kebalikan dari DNS (forward/normal DNS) yang mapping nama domain ke alamat IP.

- *Web Archive*

Internet Archive adalah sebuah perpustakaan digital nirlaba yang memiliki misi "akses universal untuk semua pengetahuan. Internet

Archive menyediakan penyimpanan permanen dan akses publik bebas untuk koleksi bahan digital, termasuk situs web, musik, gambar bergerak, dan hampir tiga juta buku domain publik.

b. Scanning Network

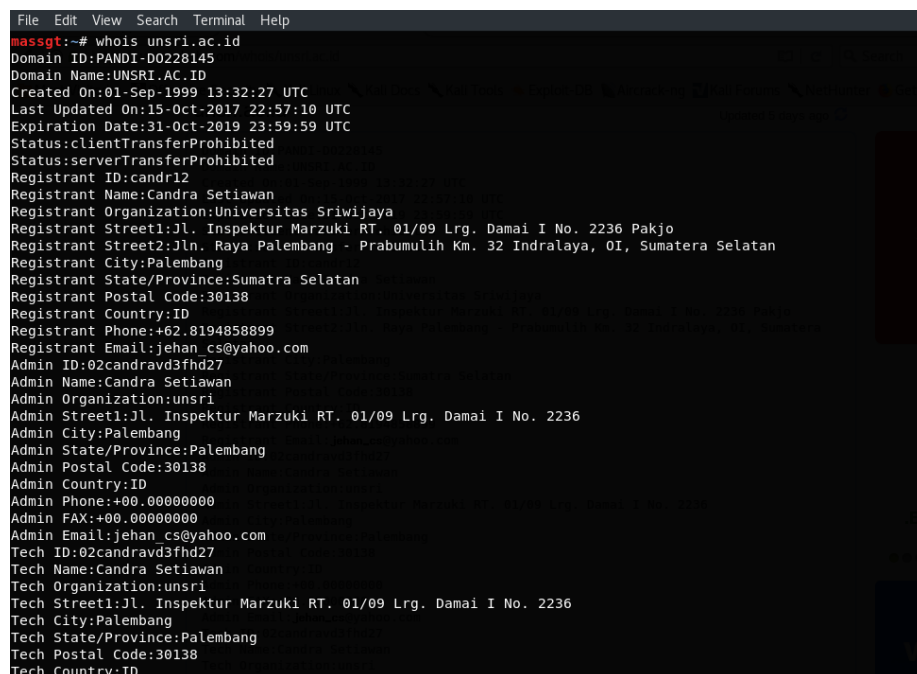
Network scanning adalah metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/Network yang maksud

c. CVE (*Common Vulnerabilities and Exposures*)

Common Vulnerabilities and Exposures menyediakan metode referensi untuk kerentanan keamanan dan eksposur informasi yang diketahui. National Cybersecurity FFRDC, dioperasikan oleh Mitre Corporation, main, dengan dana dari Divisi Keamanan Cyber Nasional Departemen Keamanan Dalam Negeri Amerika Serikat.

2. Hasil dan Analisa

Pada percobaan yang pertama yaitu melakukan proses semacam identifikasi dari sebuah website, dimana website yang digunakan pada percobaan ini adalah website unsri.ac.id. Dengan menggunakan command “whois” pada terminal linux dan dilanjutkan dengan nama website maka akan di dapatkan hasil yang menjelaskan dengan sangat jelas data-data dari domain web tersebut, seperti gambar dibawah ini :



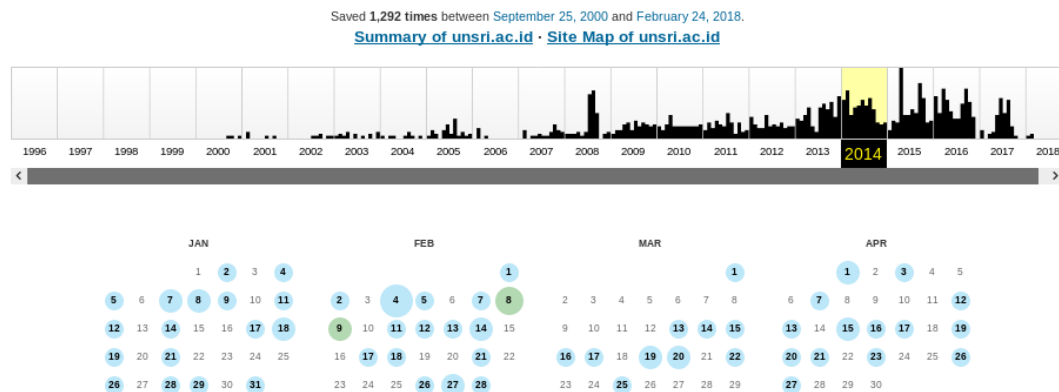
```
File Edit View Search Terminal Help
massgt:~# whois unsri.ac.id
Domain ID:PANDI-D0228145
Domain Name:UNSRI.AC.ID
Created On:01-Sep-1999 13:32:27 UTC
Last Updated On:15-Oct-2017 22:57:10 UTC
Expiration Date:31-Oct-2019 23:59:59 UTC
Status:clientTransferProhibited
Status:serverTransferProhibited
Registrant ID:candr12
Registrant Name:Candra Setiawan
Registrant Organization:Universitas Sriwijaya
Registrant Street1:Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236 Pakjo
Registrant Street2:Jln. Raya Palembang - Prabumulih Km. 32 Indralaya, OI, Sumatera Selatan
Registrant City:Palembang
Registrant State/Province:Sumatra Selatan
Registrant Postal Code:30138
Registrant Country:ID
Registrant Phone:+62.8194858899
Registrant Email:jehan_cs@yahoo.com
Admin ID:02candravd3fhd27
Admin Name:Candra Setiawan
Admin Organization:unsri
Admin Street1:Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236
Admin City:Palembang
Admin State/Province:Palembang
Admin Postal Code:30138
Admin Country:ID
Admin Phone:+00.00000000
Admin FAX:+00.00000000
Admin Email:jehan_cs@yahoo.com
Tech ID:02candravd3fhd27
Tech Name:Candra Setiawan
Tech Organization:unsri
Tech Street1:Jl. Inspektur Marzuki RT. 01/09 Lrg. Damai I No. 2236
Tech City:Palembang
Tech State/Province:Palembang
Tech Postal Code:30138
Tech Country:ID
```

Dari gambar diatas dapat dilihat dalam web dengan domain name unsri.ac.id data yang sangat lengkap mulai dari nama pendaftar, alamat, tanggal daftar, tanggal expired, danlain sebagainya. Dengan data-data tersebut dapat memudahkan siapa saja

untuk memperoleh informasi yang bisa digunakan untuk segala macam hal. Berikutnya merupakan gambar dari hasil command whatweb :

```
File Edit View Search Terminal Help
massgt:~# whatweb www.unsri.ac.id
http://www.unsri.ac.id [200 OK] Cookies[PHPSESSID], Country[INDONESIA][ID], Email[yadiutama@unsri.ac.id], Google-Analytics[Universal][UA-68096542-1,UA-92898935-1], HTTPServer[nginx], IP[103.241.4.11], JQuery[1.2.6], Meta-Author[yadiutama@unsri.ac.id], PHP[5.3.10-1ubuntu3.25], PasswordField[password], Script[text/javascript], Title[::: Halaman Utama | Universitas Sriwijaya - Indralaya, Sumatera Selatan], X-Powered-By[PHP/5.3.10-1ubuntu3.25], nginx
massgt:~#
```

Dari hasil command whatweb situs unsri.ac.id didapatkan hasil data-data pribadi admin, dan data-data lain yang jelas mengenai web unsri.ac.id itu sendiri. Seperti country, email, HTTPServer menggunakan nginx, IP 103.241.4.11, dan lain sebagainya. Selanjutnya hasil dari web archive, untuk yang ini tidak menggunakan terminal di kali linux tetapi melalui web browser :



Pada gambar diatas menunjukkan hasil dari pencarian situs unsri.ac.id pada web.archive.org dan menampilkan arsip pada tahun 2014, disana terlihat ada beberapa lingkaran pada tanggal disetiap bulan dan itu menunjukkan bahwa pada setiap lingkaran tersebut menandakan jika pada tanggal itu situs web yang berkaitan melakukan satu kali update atau sejenisnya. Sedangkan untuk lingkaran dengan warna lebih gelap menandakan dua kali.

```
File Edit View Search Terminal Help
massgt:~# nmap -sV 103.241.4.1

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-14 01:08 WIB
Nmap scan report for ip-103-241-4-1.unsri.ac.id (103.241.4.1)
Host is up (0.038s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  tcpwrapped
23/tcp    open  tcpwrapped
25/tcp    filtered smtp
80/tcp    open  nagios-nsc   Nagios NSCA
179/tcp   open  tcpwrapped
2000/tcp  open  bandwidth-test Mikrotik bandwidth-test server
8181/tcp  open  http         Mikrotik router config httpd
8291/tcp  open  unknown
9090/tcp  filtered zeus-admin
Service Info: OS: RouterOS; Device: router; CPE: cpe:/o:mikrotik:routeros

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.43 seconds
```

```
File Edit View Search Terminal Help
Not shown: 989 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    filtered ssh
25/tcp    filtered smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
443/tcp   open  https
8000/tcp  open  http-alt
8080/tcp  filtered http-proxy
9090/tcp  filtered zeus-admin
10000/tcp open  snet-sensor-mgmt
Aggressive OS guesses: OpenWrt 12.09-rc1 Attitude Adjustment (Linux 3.3 - 3.7) (98%), Linux 3.13 or 4.2 (96%), XBMCbuntu Frodo v12.2 (Linux 3.X) (96%), Linux 3.2 - 3.8 (95%), Linux 2.6.32 - 3.1 (94%), Linux 3.2 (94%), Linux 2.6.32 - 3.13 (93%), Linux 3.8 (93%), Linux 3.2 - 3.10 (93%), Linux 3.2 - 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.80 seconds
massgt:~#
```

Pada gambar diatas menunjukkan hasil scanning *os type* menggunakan command nmap -O unsri.ac.id, yang bertujuan untuk mengidentifikasi sistem operasi yang digunakan. Dari gambar diatas dapat dilihat bahwa sistem operasi yang digunakan adalah linux yang mana terlihat ada beberapa jenis linux yang ada di dalam nya. Selanjutnya yaitu melakukan pencarian dalam CVE :

[illegible]

Untuk proses yang ini yaitu mencari vulnerability atau kerentanan suatu sistem, yang di gunakan untuk mencari kerentanannya pada kali ini yaitu apcahe. Dari hasil diatas dapat dilihat terdapat beberapa hasil, hasil tersebut beragam score kerentanannya, semakin besar score nya maka semakin besar pula kerentanannya.