



# **VULNERABILITY SCANNING**

## **METASPLOITABLE 1**

**Abdi Bimantara**  
**Abdibimantara91@gmail.com**

 [github.com/Abdibimantara](https://github.com/Abdibimantara)  [medium.com/@abdibimantara](https://medium.com/@abdibimantara)  [www.linkedin.com/in/abdi-bimantara-990a84149/](https://www.linkedin.com/in/abdi-bimantara-990a84149/)

## Daftar Isi

<b>Latar Belakang .....</b>	<b>1</b>
<b>Spesifikasi Target .....</b>	<b>1</b>
<b>Landasan Teori .....</b>	<b>3</b>
Nmap.....	3
Host Discovery .....	3
Port Scanning .....	3
Service Enumeration.....	3
OS Detection .....	4
Vuln Scanning.....	4
<b>Impelementasi.....</b>	<b>4</b>
<b>Referensi.....</b>	<b>9</b>

## 1. Latar Belakang

Reconnaissance merupakan sebuah tahapan dimana seorang penyerang (attacker) melakukan proses persiapan sebelum melakukan proses penyerangan dalam sebuah sistem. Reconnaissance juga lebih dikenal dengan sebutan information gathering. Umumnya Teknik Reconnaissance ini dimulai dari mengumpulkan informasi sebanyak mungkin guna mendukung proses selanjutnya (penyerangan). Informasi yang dicari oleh attacker umumnya dimulai dari informasi kecil hingga yang sangat penting.

Tahapan Reconnaissance terbagi menjadi 2 tipe yaitu :

- Active Reconnaissance, Adalah tipe tahapan Reconnaissance yang dilakukan dengan cara melakukan pengumpulan informasi secara berhubungan langsung dengan target
- Pasive Reconnaissance, Adalah tipe tahapan Reconnaissance yang dilakukan dengan cara melakukan pengumpulan informasi tanpa berhubungan langsung dengan target. Pengumpulan informasi ini dapat dilakukan menggunakan media informasi seperti sosial media dan lain sebagainya

Pasive Reconnaissance akan diterapkan guna mencari informasi pada target yang telah ditetapkan. Proses Reconnaissance ini akan menggunakan bantuan tools nmap guna melakukan scanning vulnerability yang terdapat pada target. Mesin yang dijadikan target tersebut adalah mesin Metasploitable1 dari vulnhub. Dimana mesin ini merupakan mesin yang diperuntukan untuk diujicoba keamanannya.

## 2. Spesifikasi Target

Mesin yang dijadikan target dalam percobaan reconnaissance kali ini adalah mesin Metasploitable1. Dimana mesin ini merupakan mesin yang berjalan menggunakan sistem operasi linux. Berikut adalah penjelasan lebih lanjut mengenai mesin tersebut

Name	Metasploitable: 1
Date release	19 May 2010
Author	Metasploit
Series	Metasploitable

Size	545 MB
MD5	E54089BA72FE0127D06528DECAD9A6AE
SHA1:	1F6698611068FAD4D9661C336B5D888A0A880FE9

### 3. Landasan Teori

#### 3.1. Nmap

Network Mapping atau lebih dikenal dengan nmap. Nmap merupakan salah satu tools reconnaissance yang sering digunakan. Tools ini sangat berguna untuk mengumpulkan informasi dari target. Tools ini bersifat open source sehingga free dan juga mudah digunakan. Nmap dapat diwonload secara gratis di website resminya : [nmap.org](http://nmap.org).

#### 3.2. Host Discovery

Host Discovery merupakan salah satu dari serangkaian proses dari tahapan reconnaissance. Proses Host Discovery adalah proses dimana attacker akan melakukan Anetwork scanning sehingga mengetahui host host siapa saja yang terhubung di jaringan tersebut. Untuk melakukan proses Host Disvovery, kita dapat menggunakan bantuan tools nmap. Command dari proses host discovery ini yaitu **nmap -sn -n ip network\***.

#### 3.3. Port Scanning

Port Scanning juga merupakan salah satu dari serangkan proses reconnaissance. Umunya saat attacker melakukan reconnaissance, Port scanning wajib dilakukan. Dikarenakan Melalui Port scanning kita dapat dengan mudah mengetahui pintu atau gerbang mana yang akan dijadikan celah untuk attacker mulai menyerang. Command dari proses Port Scanning ini yaitu **nmap -sn -n ip target**.

#### 3.4. Service Enumeration

Service Enumeration merupakan proses dimana kita melakukan scanning network untuk mengetahui service apa saja yang berjalan di jaringan tersebut. Melalui proses ini, informasi yang didapatkan akan menjadi bahan bagi para attacker untuk

melakukan penyerangan nantinya. Command dari proses Service Enumuration ini yaitu **nmap -v -sV ip target**.

### 3.5. OS Detection

Os detection digunakan untuk kita mengetahui jenis sistem operasi apa yang digunakan oleh si target. Dengan kita mengetahui version dari sistem operasi tersebut, kita dapat mengetahui exploit apa yang cocok untuk versi sistem operasi tersebut. Command dari proses OS detection ini yaitu **nmap -O ip target**.

### 3.6. Vuln Scanning

Vulnerability scanning atau biasa dikenal dengan vuln scan adalah proses dimana si attacker akan melakukan proses scanning vulnerability pada si target. Dimana proses ini membutuhkan script untuk menjalankannya. Umumnya, script default sudah tersedia oleh nmap, namun ada beberapa kasus script menggunakan script yang harus dibuat sendiri. Berikut adalah command dari proses vuln scanning yaitu **nmap -v -script vuln ip target**.

## 4. Implementasi Reconnaissance

### 4.1. Host Discovery

Hasil dari host discovery menampilkan 3 ip dimana ip 192.168.64.128. disini kami mencoba melakukan test ping pada sisa dua ip lainnya. Namun yang merespon hanya ip 192.168.64.129, sehingga kami berasumsi ip tersebut adalah ip si target.

```
[root@bimlabs]--[home/bimantara/Desktop]
#nmap -sn -n 192.168.64.*
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-26 23:45 WIB
Nmap scan report for 192.168.64.128
Host is up (0.00079s latency).
MAC Address: 00:0C:29:84:3A:CC (VMware)
Nmap scan report for 192.168.64.254
Host is up (0.00029s latency).
MAC Address: 00:50:56:FA:82:C8 (VMware)
Nmap scan report for 192.168.64.129
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 9.81 seconds
```

## 4.2. Port Scanning

Proses dilanjutkan dengan melakukan port scanning. Hal ini bertujuan mengetahui port mana yang open dan bisa dijadikan pintu masuk serangan. Berdasarkan hasil yang didapatkan, terdapat 12 port yang terbuka

```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:84:3A:CC (VMware)
```

## 4.3. Service Enumeration

Tampak pada gambar dibawah, beberapa penjelasan mengenai service yang berjalan di mesin target. Informasi ini sangat berguna bagi seorang attacker, dikarenakan attacker dapat mengetahui service apa saja dan versi berapa yang sedang berjalan. Attacker pun dapat dengan mudah membuat atau mencari exploit yang tersedia di internet.

```
[*]-[root@bimlabs]-[/home/bimantara/Desktop]
#nmap -sV 192.168.64.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-27 00:10 WIB
Nmap scan report for 192.168.64.128
Host is up (0.024s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:84:3A:CC (VMware)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

## 4.4. OS Detection

Melalui command nmap -O ip target menghasilkan informasi mengenai versi dari sistem operasi yang sedang berjalan pada mesin target. Diketahui Sistem Operasi yang sedang berjalan di mesin target adalah linux dan memiliki versi kernel 2.6.9 – 2.6.33.

```
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

Melalui informasi yang telah didapatkan pada gambar diatas, ternyata os versio tersebut memiliki vulnerability. Dimana vulnerability ini terbukti dengan sudah terkesposnya script privilege escalation dalam exploithub seperti pada gambar dibawah ini.

Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTTRACE\_POKE\_DATA' Race Condition Privilege Escalation (/etc/passwd Method)

<b>EDB-ID:</b> 40839	<b>CVE:</b> 2016-5195	<b>Author:</b> FIREFART	<b>Type:</b> LOCAL	<b>Platform:</b> LINUX	<b>Date:</b> 2016-11-28
EDB Verified: ✓		Exploit: 📄 / 📄		Vulnerable App: 📄	

## 4.5. Vuln Scanning

Menggunakan script vuln scanning default dari nmap, tampak pada gambar diketahui bawah mesin target memiliki beberapa vulnerability. Dimana dari beberapa vulnerability tersebut ada yang memiliki tingkat resiko yang cukup tinggi.

```
25/tcp open smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
```

diketahui bahwa port 25 memang terbuka, namun port tersebut tidak memiliki kerentanan berdasarkan CVE2010-4344

```

80/tcp OpenSsl
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /phpinfo.php: Possible information file
|   /icons/: Potentially interesting folder w/ directory listing
| http-dombased-xss: Couldn't find any DOM based XSS.
| http-trace: TRACE is enabled
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|   State: LIKELY VULNERABLE
|   IDs: CVE:CVE-2007-6750
|   Slowloris tries to keep many connections to the target web server open and hold
|   them open as long as possible. It accomplishes this by opening connections to
|   the target web server and sending a partial request. By doing so, it starves
|   the http server's resources causing Denial Of Service.
|
|   Disclosure date: 2009-09-17
|   References:
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|     http://ha.ckers.org/slowloris/

```

```

http-vuln-cve2011-3192:
VULNERABLE:
Apache byterange filter DoS
State: VULNERABLE
IDs: CVE:CVE-2011-3192 BID:49303
The Apache web server is vulnerable to a denial of service attack when numerous
overlapping byte ranges are requested.
Disclosure date: 2011-08-19
References:
https://www.tenable.com/plugins/nessus/55976
https://www.securityfocus.com/bid/49303
https://seclists.org/fulldisclosure/2011/Aug/175
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
http-csrf: Couldn't find any CSRF vulnerabilities.

```

Pada port 80 yang dimana menjalankan servis HTTP, terdapat banyak sekali hasil scan. Dimana hasil scan tersebut tidak semuanya memiliki vulnerability. Namun pada port 80 tersebut memiliki vulnerability Slowloris DOS attack yaitu CVE-2007-6750. Selain vulnerability Slowloris DOS attack port tersebut memiliki vulnerability lainnya yaitu apache byterange filter Dos (CVE 2011-3192).



```

5432/tcp open  postgresql
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|   State: VULNERABLE
|   IDs:  CVE:CVE-2014-3566  BID:70574
|   The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|   products, uses nondeterministic CBC padding, which makes it easier
|   for man-in-the-middle attackers to obtain cleartext data via a
|   padding-oracle attack, aka the "POODLE" issue.
|   Disclosure date: 2014-10-14
|   Check results:
|   TLS_RSA_WITH_AES_128_CBC_SHA
|   References:
|   https://www.imperialviolet.org/2014/10/14/poodle.html
|   https://www.openssl.org/~bodo/ssl-poodle.pdf
|   https://www.securityfocus.com/bid/70574
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_

```

```

ssl-ccs-injection:
VULNERABLE:
SSL/TLS MITM vulnerability (CCS Injection)
State: VULNERABLE
Risk factor: High
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
does not properly restrict processing of ChangeCipherSpec messages,
which allows man-in-the-middle attackers to trigger use of a zero
length master key in certain OpenSSL-to-OpenSSL communications, and
consequently hijack sessions or obtain sensitive information, via
a crafted TLS handshake, aka the "CCS Injection" vulnerability.

References:
http://www.openssl.org/news/secadv_20140605.txt
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
http://www.cvedetails.com/cve/2014-0224

```

```

ssl-dh-params:
VULNERABLE:
Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
Transport Layer Security (TLS) services that use Diffie-Hellman groups
of insufficient strength, especially those using one of a few commonly
shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
WEAK DH GROUP 1
Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Modulus Type: Safe prime
Modulus Source: Unknown/Custom-generated
Modulus Length: 1024
Generator Length: 8
Public Key Length: 1024
References:
https://weakdh.org

```

Selanjutnya adalah port 5432 yaitu service postgresql. Dimana pada port ini terdapat 3 vulnerability yaitu

1. SSL POODLE information leak dimana vulnerability ini memiliki code CVE2014-3566
2. SSL/TLS MITM vulnerability (CCS Injection) leak dimana vulnerability ini memiliki code CVE2014-0244. Dan vulnerability ini memiliki skor yang tinggi
3. kerentanan pada Transport Layer Security (TLS) yang menggunakan Diffie-Hellman Keys

## Referensi

1. <https://www.offensive-security.com/metasploit-unleashed/vulnerability-scanning/>
2. <https://www.offensive-security.com/metasploit-unleashed/port-scanning/>
3. <https://www.exploit-db.com/exploits/40839>