VULNERABILITY SCANNING METASPLOITABLE 1

Abdi Bimantara
Abdibimantara91@gmail.com

github.com/Abdibimantara medium.com/@abdibimantara www.linkedin.com/in/abdi-bimantara-990a84149/

Daftar Isi

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 teah ditetapkan. Proses Reconnaissance ini akan menggunakan bantuan tools nmap guna melakuan scanning vulnerability yang terdapat pada target. Mesin yang dijadikan tagert tersebut adalah mesin Metasploitbale1 dari vulnhub. Dimana mesin ini merupakan mesin yang diperntukan 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. Beirkut 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 geratis di website resminya : 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 Enumuration

Service Enumuration 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.**

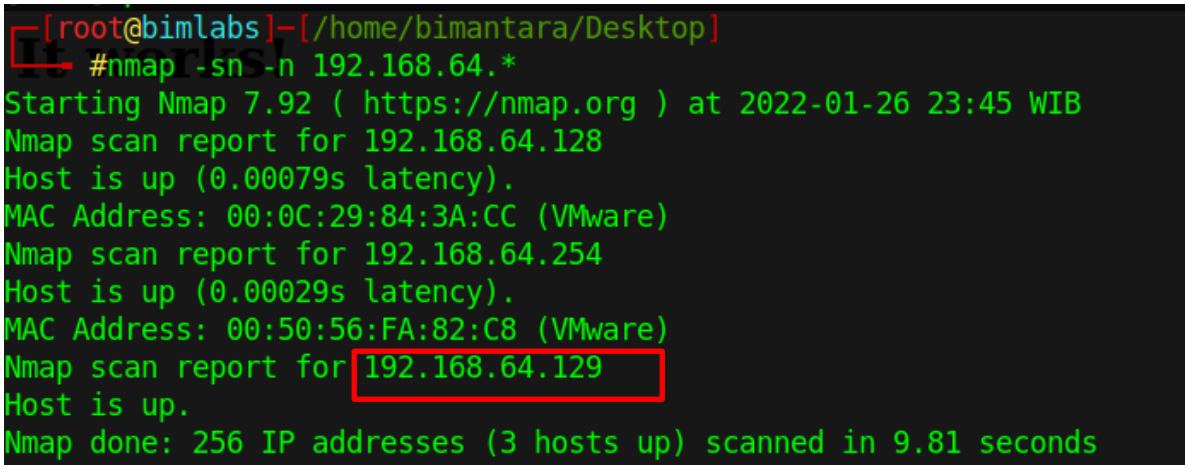
3.6. Vuln Scanning

Vulnerability scanning atau biasa dikenal dengan vuln scan adalah proses dimana si attacker akan melakkan proses scanning vulnerabilitie pada sitarget. 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. Beirkut adalah command dari proses vuln scanning yaitu **nmap -v –script vuln ip target.**

4. Implementasi Recconaissance

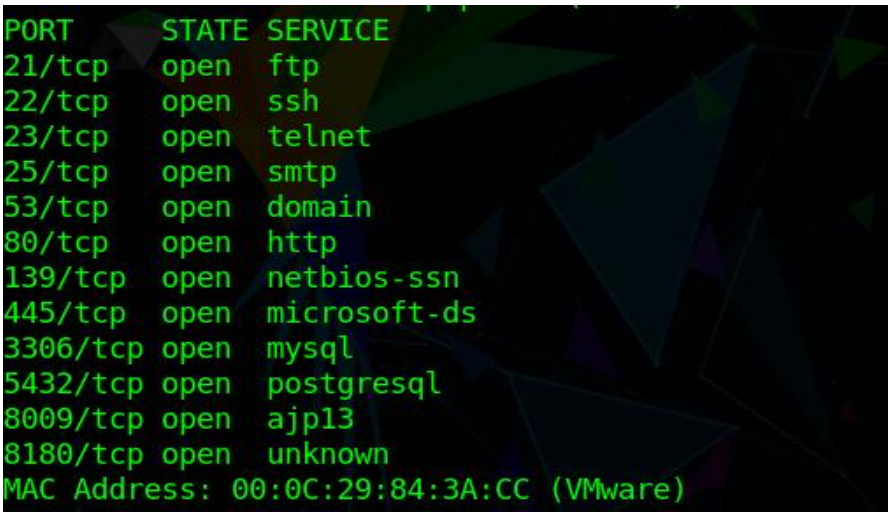
4.1. Host Discovery

Hasil dari host discovery menampilkan 3 ip dimana ip 192,168.64.128. disini kami mecoba 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.



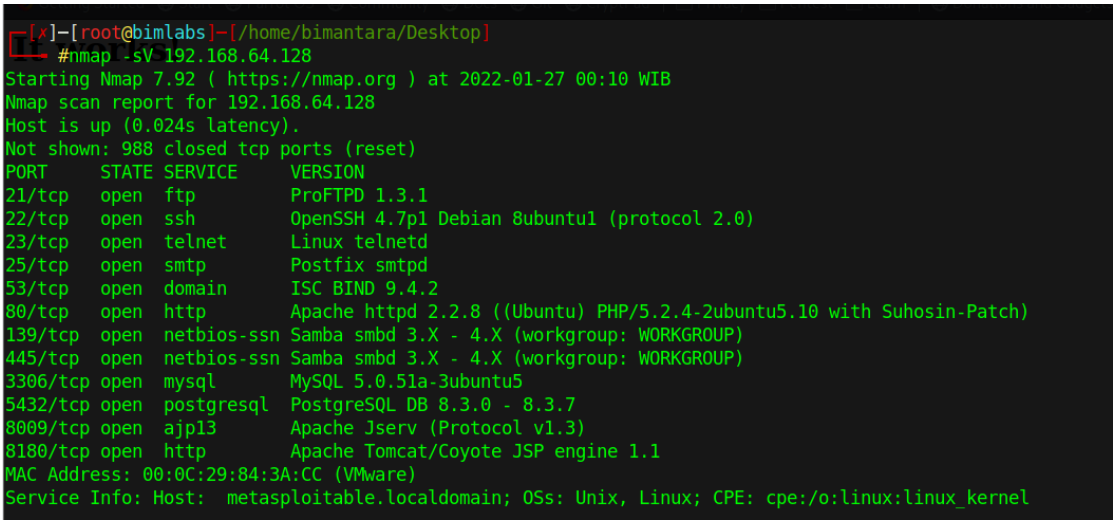
4.2. Port Scanning

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



4.3. Service Enumuration

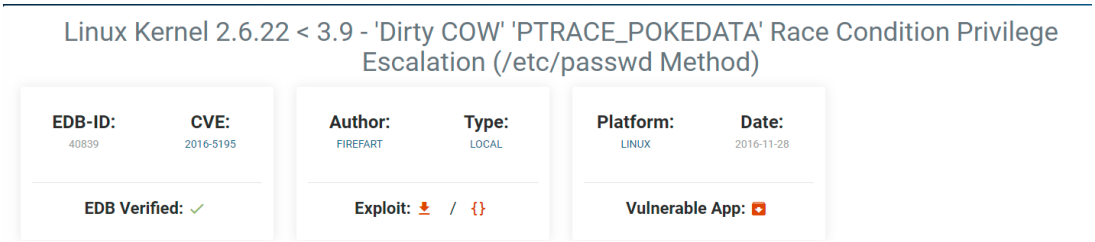
Tampak pada gambar dibawah, beberapa penjelasan mengeni service yang berjalan di mesin target. Informasi ini sangat berguna bagi seorang attacker, dikarenakan attacker dapat mengetahui service apa saja dan versi berapa yang sedang berjalan. Attacker pun dapat dengan mudah membuat atau mencari exploit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



4.4. OS Detection

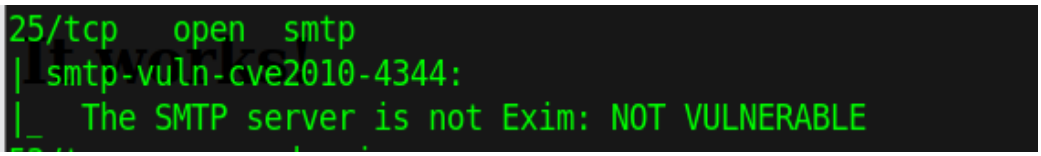
Melalui command nmap -O ip target menghasilkan informasi mengenai versi dari sistem operasi yang sedang berjalan pada mesin target. Diketahui Sistem Operasi yang sedang berjalan di mesin target adalah linux dan memiliki versi kernel 2.6.9 – 2.6.33.

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



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 tinggkat resiko yang cukup tinggi.

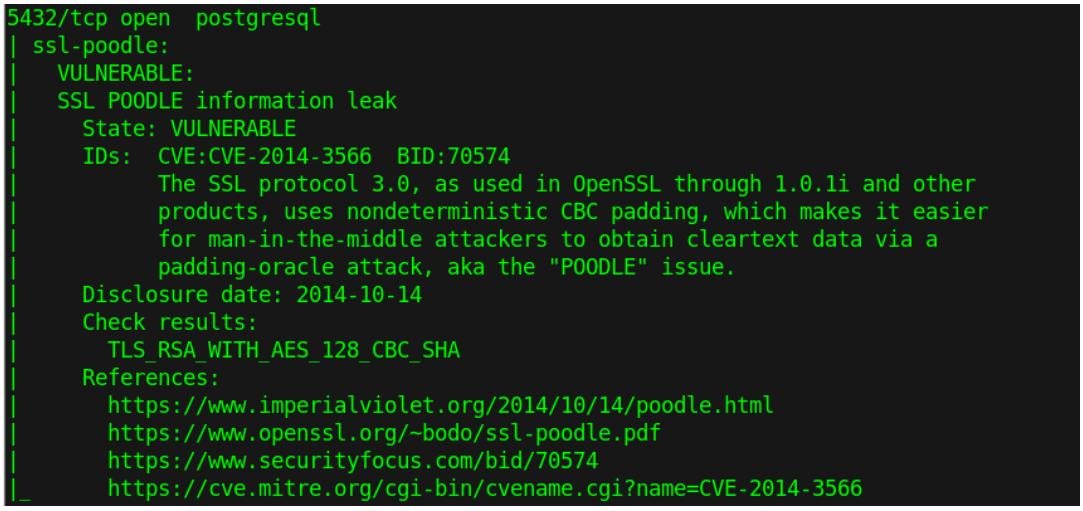


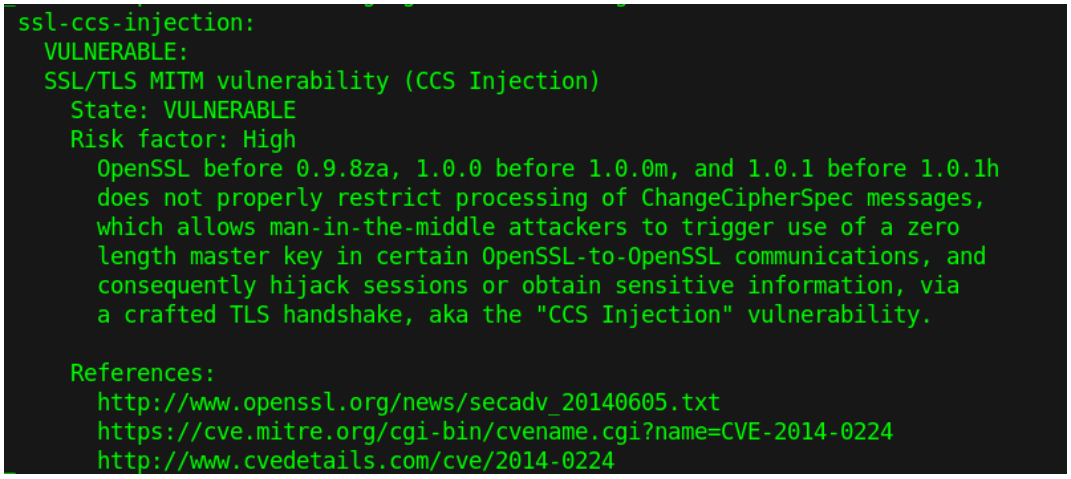
diketahui bahwa port 25 memang terbuka, namun port tersebut tidak memiliki kerentanan berdasarkan CVE2010-4344

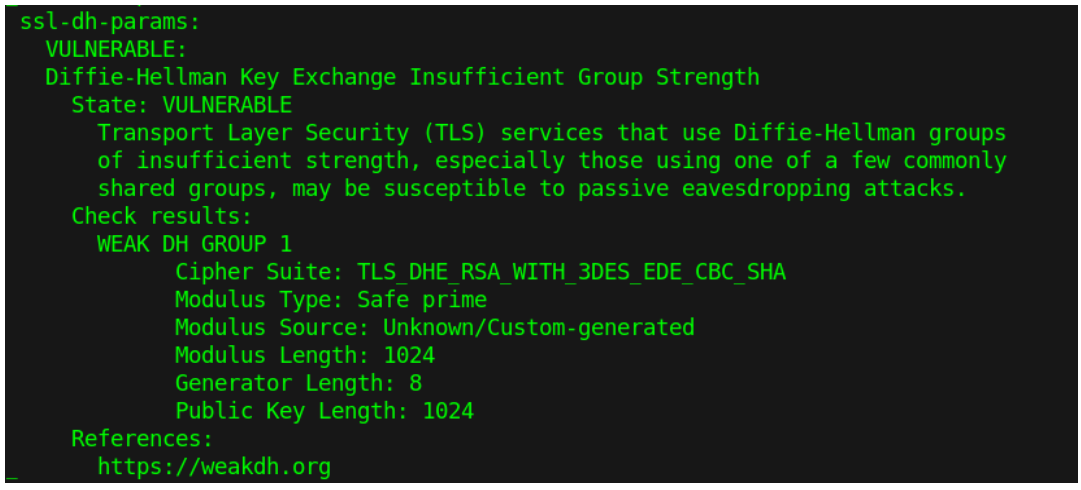
```
80/tcp   open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /phpinfo.php: Possible information file
|_  /icons/: Potentially interesting folder w/ directory listing
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-trace: TRACE is enabled
| http-slowloris-check:
|   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 scna terbsebut 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).







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

1. SSL POODLE information leak dimana vurlnerability ini memiliki code CVE2014-3566
2. SSL/TLS MITM vulnerability (CCS Injection) leak dimana vurlnerability ini memiliki code CVE2014-0244. Dan vulnerability ini memilii 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**