Muhammad Azriansyah 09011281320006 Keamanan Jaringan Komputer

Laporan Analisis Hands-On Lab Fase Exploitation

Evaluasi Keamanan Sistem

Exploit adalah sebuah kode yang menyerang keamanan_komputer secara spesifik. Exploit banyak digunakan untuk penentrasi baik secara legal ataupun ilegal untuk mencari kelemahan (Vulnerability) pada komputer tujuan. Bisa juga dikatakan sebuah perangkat lunak yang menyerang kerapuhan keamanan (security vulnerability) yang spesifik namun tidak selalu bertujuan untuk melancarkan aksi yang tidak diinginkan. Banyak peneliti keamanan komputer menggunakan exploit untuk mendemonstrasikan bahwa suatu sistem memiliki kerapuhan.

Memang ada badan peneliti yang bekerja sama dengan produsen perangkat lunak. Peneliti itu bertugas mencari kerapuhan dari sebuah perangkat lunak dan kalau mereka menemukannya, mereka melaporkan hasil temuan ke produsen agar produsen dapat mengambil tindakan. Meskipun demikian, exploit kadang menjadi bagian dari suatu malware yang bertugas menyerang kerapuhan keamanan.

Actual Exploit

- Langkah pertama set ip OS target (DVL) menjadi 192.168.100.20 dengan netmask 255.255.255.0.

```
bt ~ # ifconfig eth0 192.168.100.20 netmask 255.255.255.0_
```

- Lalu cek apakah ip pada OS telah berubah seperti yang di inginkan.

```
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 ~ #
```

- Kemudian, set OS attacker (Ubuntu) dengan ip 192.168.100.10 dengan netmask 255.255.255.0.

```
root@ubuntu:/home/ubuntu# ifconfig eth0 192.168.100.10 netmask 255.255.255.0
```

- Kemudian cek apakah OS attacker sudah terset ip-nya seperti yang di inginkan.

```
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#
```

- Lakukan ping dari OS attacker ke OS target untuk mengecek koneksi sudah ter-established atau belum.

```
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
```

- Lalu lakukan hal sebaliknya untuk mengecek kemampuan komunikasi antar OS.

```
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
```

- Lakukan perintah “Nmap –sV 192.168.100.10”, Nmap –sv (service yg sedang berjalan) lalu perhatikan hasilnya.

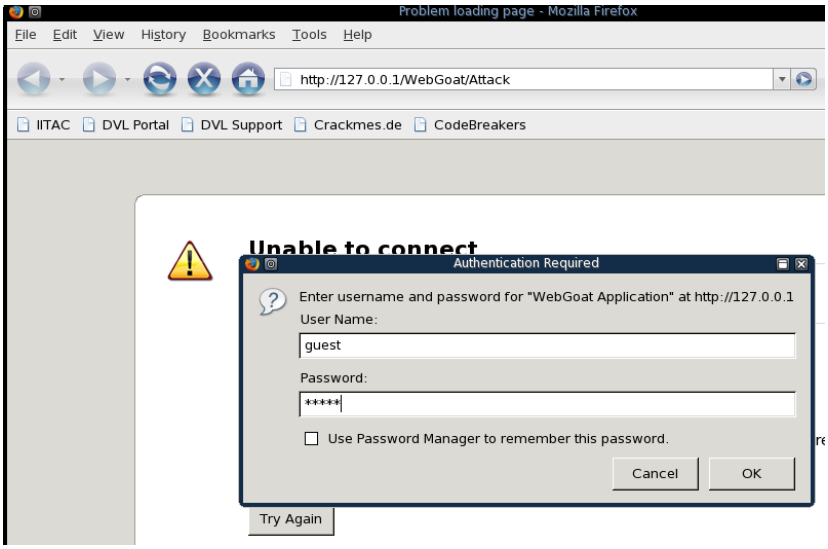
```
root@ubuntu:/home/ubuntu# nmap -sV 192.168.100.20

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#
```

```
bt ~ # nmap -sV 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 follow
 fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=4.20%I=7%D=3/16%Time=58C9FBCD%P=i686-pc-linux-gnu%r(NULL,2
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 ~ # _
```

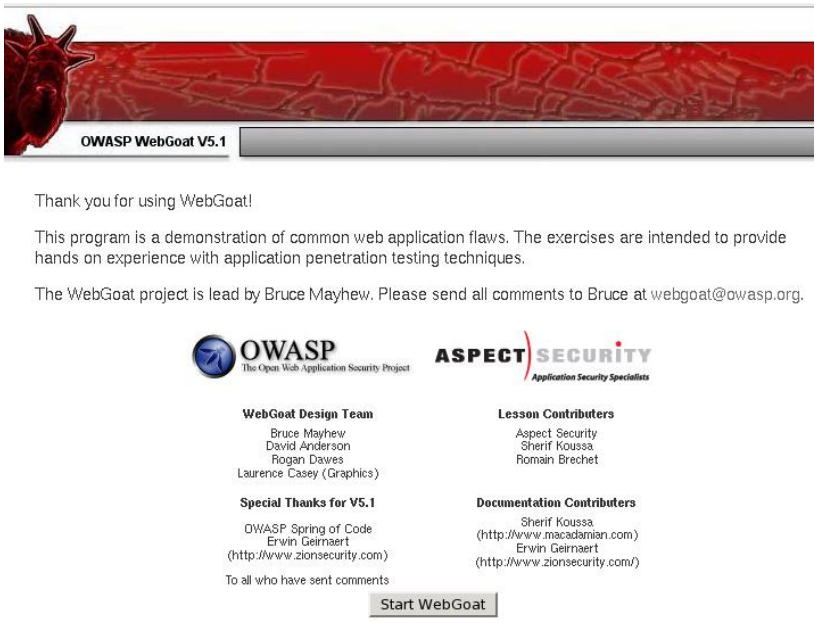
- Kemudian masuk ke bagian mengekseskusi bruteforce pada target, service ssh menggunakan bruteforce mencoba melakukan input password menggunakaan tool. Penggunaan tool sejatinya untuk menggantikan kemampuan manusia yang tidak secepat dan seakurat kerja mesin yang di lakukan dalam sepersekian detik untuk menjalankan command. Tools yang dapat di manfaatkan : Hydra dan Nmap.
- Menggunakan tool Hydra, jalankan command “Hydra -l –P password.list 192.168.100.10 ssh”.

- Pada OS target masuk ke tampilan GUI dengan command “startx”.

- Buka browser pada OS lalu kunjungi url “http://127.0.0.1/WebGoat/Attack”. Website ini di rancang untuk mengetes seberapa kuat akun yang kita pergunakan atau vulnerability-nya pada database berbasis SQL website-website yang kita atau orang lain kelola. Masukkan username “guest” dan password “guest” untuk menjalankan sistemnya.

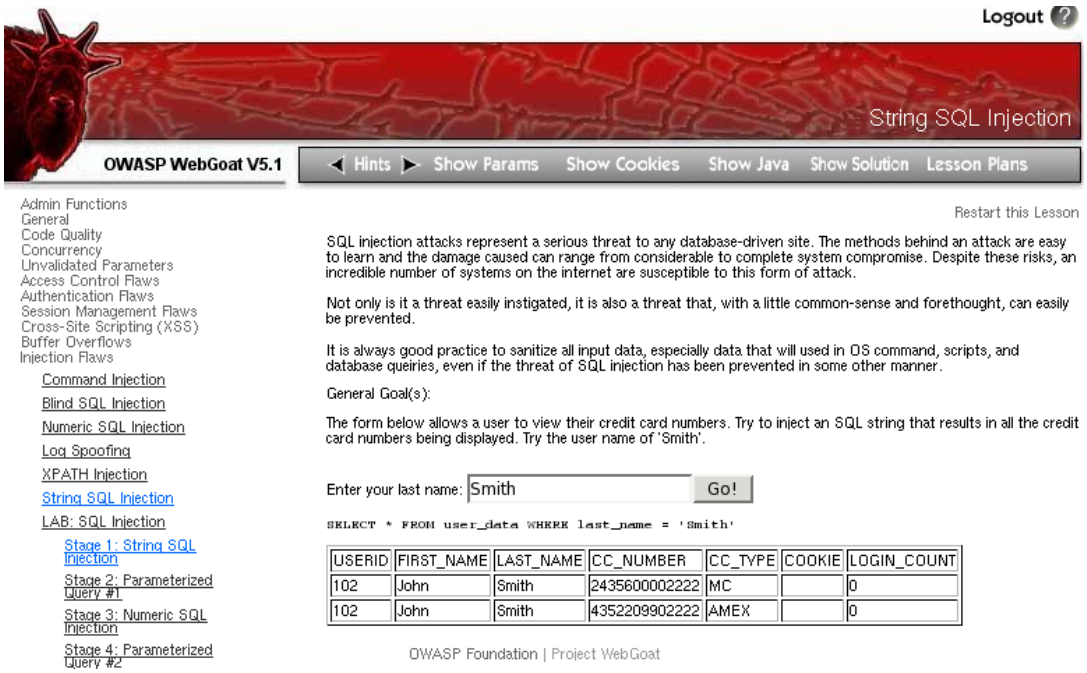


- Tampilan awal ketika masuk, lalu klik “Start WebGoat” untuk mulai menggunakan.

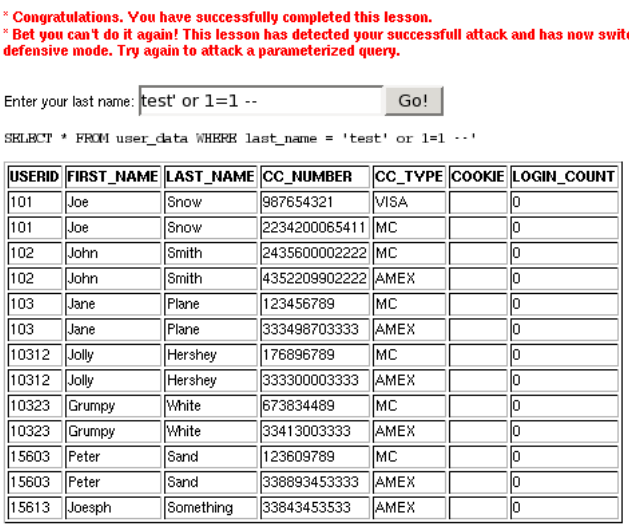


- Masukkan username yang cari vulnerabilitynya. Sebagai contoh masukkan username “Smith”.

- Kemudian sistem melakukan pencarian semua nama dengan last name Smith atau user name Smith. Programmer yang lalai akan membuat bughole yang bisa menyebabkan terjadi String SQL Injection, hal ini dapat terjadi karena tidak di lakukannya filter untuk inputan yang masuk.



- Setelah menginput dengan username “Smith”, kemudian ganti dengan “test’ or 1=1--“ untuk melakukan testing pada database.



- Kemudian melakukan seleksi. Pada tahap awalnya ialah menambahkan tanda petik dan akan membaca last name yg kita masukkan , maksud 1=1 adalah boolean true walaupun kita salah masih akan bernilai true. Hal tersebut kesalahan dari program karna tidak memfilter terlebih dahulu.
- Untuk mencegah serangan SQL Injection ini, kita bisa melakukan filtering pada data yang diinputkan user. Dan ada dua jenis data yang perlu kita filter, yaitu inputan yang berupa angka dan string (campuran angka, huruf, dan metakarakter).
- Buffer overflow, kalau tidak di filter akan menjadi vurnability di karenakan buffer memory pada sistem mengalami kepenuhan memori yang bisa menyebabkan perubahan alur eksekusi program sehingga menjalankan fungsi yang di inginkan attacker pada target. Pada masa sekarang para attacker menggunakannya untuk memperlambat performansi dari pada system OS target, karena serangan Buffer Overflow hanya efektif pada system OS lawas seperti Windows 95.