

TUGAS
KEAMANAN JARINGAN KOMPUTER



DISUSUN OLEH :

NAMA : INDAH SARI

NIM : 09011181320011

JURUSAN SISTEM KOMPUTER

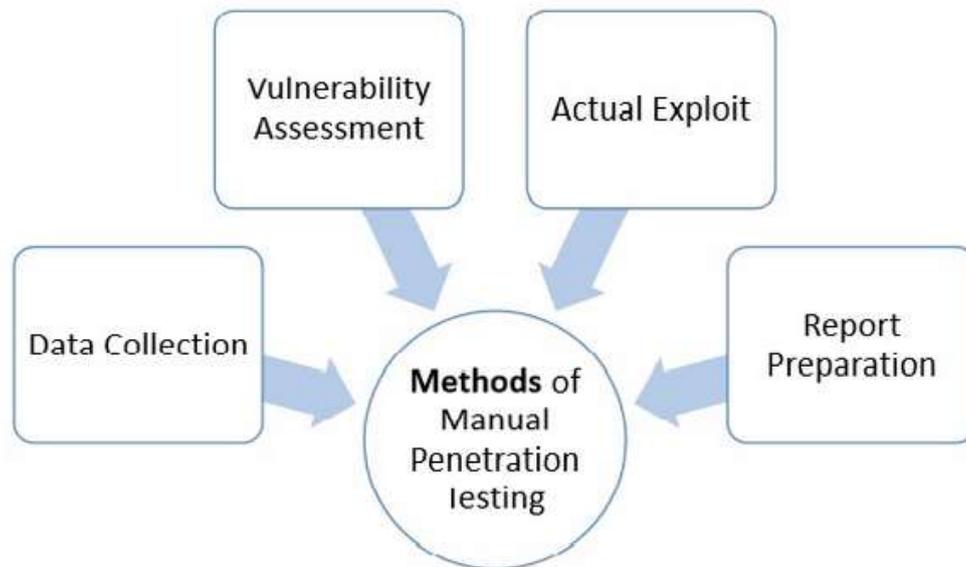
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017 – 2018

HASIL TRAINING ACTUAL EXPLOIT DI LEB

Methods of manual penetration testing ada 4 bagian yaitu; data collection, vulnerability assessment, actual exploit, dan report preparation. Seperti pada gambar di bawah ini:



Dari keempat metode penetrasi tes diatas pada percobaan ini membahas tentang actual exploit, dimana actual exploit adalah metode umum yang menggunakan tester expert untuk melancarkan serangan pada sistem target juga mengurangi risiko serangan.

Berikut langkah – langkah pengerjaan dari evaluasi keamanan sistem actual exploit:

Ada dua server yang disediakan saat percobaan yaitu: Ubuntu sebagai mesin pentes dan Down Vulnerable Linux (DVL) sebagai target.

Keterangan :

- IP DVL: 192.168.100.20
- IP Ubuntu: 192.168.100.10

Konfigure IP Address di DVL: ifconfig eth0 192.168.100.20 netmask 255.255.255.0, untuk menambahkan IP dan netmaks pada interface jaringan

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

Konfig ifconfig pada DVL, untuk menampilkan semua konfigurasi interface baik yang aktif maupun tidak. Berikut screenshotnya :

```
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 ~ #
```

Sama seperti melakukan perintah pada DVL sebelumnya lakukan konfigure IP Address di ubuntu: ifconfig eth0 192.168.100.10 netmask 255.255.255.0, untuk menambahkan IP dan netmaks pada interface jaringan

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

Sama seperti melakukan perintah pada DVL sebelumnya lakukan konfig ifconfig pada ubuntu, untuk menampilkan semua konfigurasi interface baik yang aktif maupun tidak. Berikut screenshootnya :

```
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#
```

Konfig ping pada ubuntu ke IP Address DVL : ping 192.168.100.20

```
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
```

Konfig ping pada DVL ke IP Address ubuntu : ping 192.168.100.20

```
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
```

Konfig Nmap -sV 192.168.100.20 pada ubuntu, dimana fungsi Nmap -sv adalah perintah untuk memeriksa service yg sedang berjalan pada port.

```
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#
```

Pada gambar diatas memiliki dua layanan (service) yang sedang aktif yaitu: IPP version cupp 1.1 dan MySQL version MySQL (unauthorized), dimana kedua layanan ini memakai Protocol TCP. Port yang sedang aktif pada IPP version cupp 1.1 adalah port 631, sedangkan port yang sedang aktif pada MySQL version MySQL (unauthorized) adalah port 3306.

Lakukan Konfig Nmap -sV 192.168.100.10 pada DVL sama seperti pada ubuntu sebelumnya, dimana fungsi Nmap -sv adalah perintah untuk memeriksa service yg sedang berjalan pada port.

```
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 following 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:(NULL,2
SF:9,"SSH-2.0-OpenSSH_6.6.1p1%Ubuntu-2ubuntu2%");
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 ~ #
```

Pada gambar diatas memiliki tiga layanan (service) yang sedang aktif yaitu: SSH version

(protocol 2.0), DOMAIN, dan HTTP version Apache httpd 2.4.7 ((ubuntu)), dimana ketiga layanan ini memakai Protocol TCP. Port yang sedang aktif pada SSH version (protocol 2.0) adalah port 22, Port yang sedang aktif pada DOMAIN adalah port 53, sedangkan port yang sedang aktif pada HTTP version Apache httpd 2.4.7 ((ubuntu)) adalah port 80.

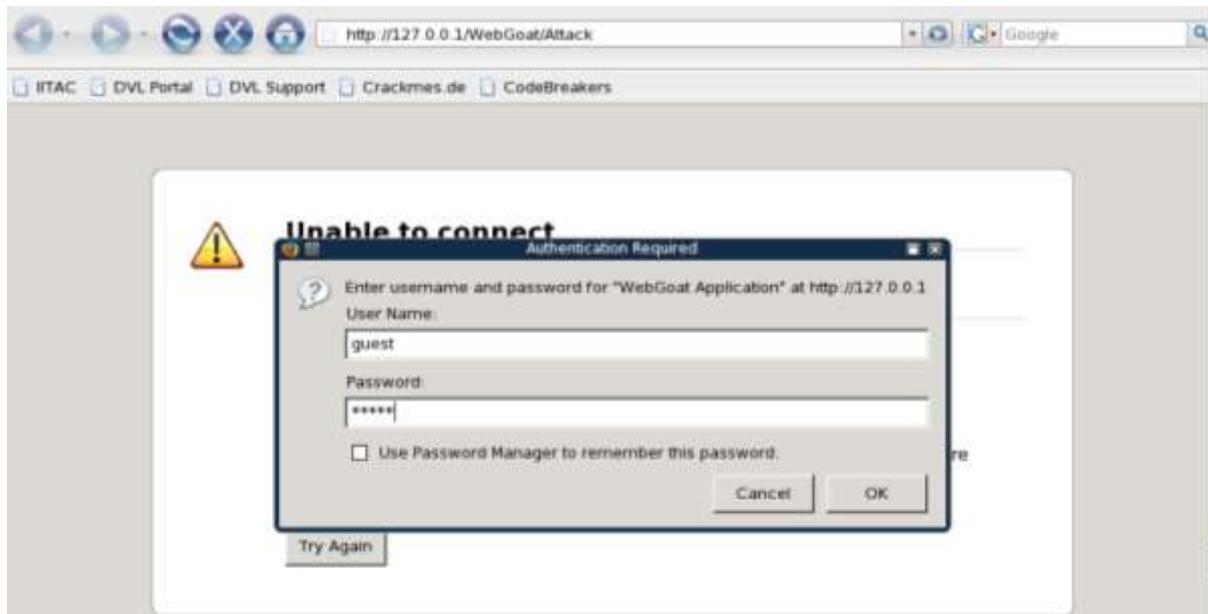
Service ssh menggunakan bruteforce mencoba melakukan input password menggunakan tool. Tools yg bisa digunakan Hydra, dan Nmap, disini kita menggunakan tools Hydra dan melakukan konfigurasi Hydra `-l -P password.list 192.168.100.10 ssh`

Startx di DVL untuk masuk ke tampilan GUI



Lakukan langkah langkah seperti pada gambar diatas agar menyambungkan koneksi jaringan internet untuk menampilkan WebGoat.

Search alamat <http://127.0.0.1/WebGoat/Attack>, setelah tampil tabel Authentication Required lalu masukkan user name “guest” dan password”guest”, klik OK.



Tampilan awal OWASP WebGoat V5.1, klik 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.



WebGoat Design Team

Bruce Mayhew
David Anderson
Rogan Dawes
Laurence Casey (Graphics)

Special Thanks for V5.1

OWASP Spring of Code
Erwin Geirnaert
(<http://www.zionsecurity.com>)

To all who have sent comments

Lesson Contributors

Aspect Security
Sherif Koussa
Romain Brechet

Documentation Contributors

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

Start WebGoat

Selanjutnya melakukan pencarian semua nama dengan last name “Smith” atau user name “Smith”, dengan memilih String SQL Injection lalu pilih Stage1: String SQL Injection. Dimana Tidak melakukan filter input yang masuk.

Logout ?

String SQL Injection

OWASP WebGoat V5.1 < Hints > Show Params Show Cookies Show Java Show Solution Lesson Plans

Admin Functions Restart this Lesson
 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
 Improper Error Handling
 Insecure Storage
 Denial of Service
 Insecure Configuration
 Web Services

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

Setelah di masukkan last name “Smith” akan menampilkan tabel seperti pada gambar diatas. Dimana hasil yang akan tampil dari tabel tersebut adalah yang menggunakan LAST_NAME Smith, dan menampilkan perintah: `SELECT * FROM user_data WHERE last_name = 'Smith'`

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	Joesph	Something	33843453533	AMEX		0

Mencoba melakukan perintah sendiri dengan mengisi last name test' or 1=1 -- ' Di awalnya dia akan menambahkan tanda petik dan akan membaca last name yg kita masukkan, dan menampilkan SELECT * FROM user_data WHERE last_name = 'test' or 1=1 -- ' dimana 'test' yang menampilkan query sedangkan or 1=1 -- hanya comment SQL. Maksud dari 1=1 adalah boolean TRUE walaupun 0=0 masih akan bernilai TRUE karena jika menampilkan hasil maka TRUE. Itulah kesalahan dr program karna tidak memfilter terlebih dahulu.

Kesimpulan: tujuan dari kegiatan evaluasi keamanan sistem ini untuk mengevaluasi sistem yg dibuat agar dapat mengetahui sejauh mana keamanan sistem informasi tersebut, apa kash sistem tersebut aman atau tidak nya dari serangan atau ancaman