

LAPORAN TUGAS KEAMANAN JARINGAN KOMPUTER
(TENTANG TRAINING EKSPLOITASI KEAMANAN)



NAMA : AGUS JULIANSYAH

NIM : 09011181320034

KELAS : SK8A

SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

Eksplorasi Keamanan

Keamanan jaringan menjadi semakin penting dengan semakin banyaknya waktu yang dihabiskan orang untuk berhubungan. Mengganggu keamanan jaringan sering lebih mudah daripada fisik atau lokal, dan lebih umum. Celah-celah keamanan jaringan sering digunakan untuk menjebol suatu sistem dibawah ini beberapa Eksploitasi yang dilakukan untuk masuk dalam keamanan suatu sistem.

Anatomi Suatu Serangan Hacking

1. Footprinting

Mencari rincian informasi terhadap sistem-sistem untuk dijadikan sasaran, mencakup pencarian informasi dengan search engine, whois, dan DNS zone transfer. hacker baru mencari-cari sistem mana yang dapat disusupi. Footprinting merupakan kegiatan pencarian data berupa:

-Menentukan ruang lingkup (scope) aktivitas atau serangan

-Network enumeration

-Interogasi DNS

-Mengintai jaringan

Semua kegiatan ini dapat dilakukan dengan tools dan informasi yang tersedia bebas di Internet. Kegiatan footprinting ini diibaratkan mencari informasi yang tersedia umum melalui buku telepon. Tools yang tersedia untuk ini di antaranya

-Teleport Pro: Dalam menentukan ruang lingkup, hacker dapat men-download keseluruhan situs-situs web yang potensial dijadikan sasaran untuk dipelajari alamat, nomor telepon,contact person,dan lain seagainya.

-Whois for 95/9/NT: Mencari informasi mengenai pendaftaran domain yang digunakan suatu organisasi. Di sini ada bahaya laten pencurian domain (domain hijack).

-NSLookup: Mencari hubungan antara domain name dengan IP address.

-Traceroute 0.2: Memetakan topologi jaringan, baik yang menuju sasaran maupun konfigurasi internet jaringan sasaran.

2.Scanning

Terhadap sasaran tertentu dicari pintu masuk yang paling mungkin. Digunakan ping sweep dan portscan.

3.Enumeration

Telaah intensif terhadap sasaran,yang mencari user account absah, network resource and share, dan aplikasi untuk mendapatkan mana yang proteksinya lemah. enumerasi sudah bersifat sangat intrusif terhadap suatu sistem. Di sini penyusup mencari account name yang absah,password,serta share resources yang ada. Pada tahap ini,khusus untuk sistem-sistem Windows, terdapat port 139 (NetBIOS session service) yang terbuka untuk resource sharing antar-pemakai dalam jaringan. Anda mungkin berpikir bahwa hard disk yang di-share itu hanya dapat dilihat oleh pemakai dalam LAN saja. Kenyataannya tidak demikian.NetBIOS session service dapat dilihat oleh siapa pun yang terhubung ke Internet di seluruh dunia! Tools seperti Legion,SMBSscanner ,atau SharesFinder membuat akses ke komputer orang menjadi begitu mudah (karena pemiliknya lengah membuka resource share tanpa password).

4.Gaining Access

Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran.Meliputi mengintip dan merampas password,menebak password, serta melakukan buffer overflow. gaining access adalah mencoba mendapatkan akses ke dalam suatu sistem sebagai user biasa.Ini adalah kelanjutan dari kegiatan enumerasi,sehingga biasanya di sini penyerang sudah mempunyai paling tidak user account yang absah,dan tinggal mencari passwordnya saja. Bila resource share-nya diproteksi dengan password, maka password ini dapat saja ditebak (karena banyak yang menggunakan password sederhana dalam melindungi komputernya).Menebaknya dapat secara otomatis melalui dictionary attack (mencobakan kata-kata dari kamus sebagai password) atau brute-force attack (mencobakan kombinasi semua karakter sebagai password).Dari sini penyerang mungkin akan berhasil memperoleh logon sebagai user yang absah.

5. Escalating Privilege

Bila baru mendapatkan user password di tahap sebelumnya, di tahap ini diusahakan mendapat privilese admin jaringan dengan password cracking atau exploit sejenis getadmin, sechole, atau lc_messages. Escalating Privilege mengasumsikan bahwa penyerang sudah mendapatkan logon access pada sistem sebagai user biasa. Penyerang kini berusaha naik kelas menjadi admin (pada sistem Windows) atau menjadi root (pada sistem Unix/Linux). Teknik yang digunakan sudah tidak lagi dictionary attack atau brute-force attack yang memakan waktu itu, melainkan mencuri password file yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem. Pada sistem Windows 9x/ME password disimpan dalam file .PWL sedangkan pada Windows NT/2000 dalam file .SAM.

6. Pilfering

Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke trusted system. Mencakup evaluasi trust dan pencarian cleartext password di registry, config file, dan user data.

7. Covering Track

Begitu kontrol penuh terhadap sistem diperoleh, maka menutup jejak menjadi prioritas. Meliputi membersihkan network log dan penggunaan hide tool seperti macam-macam rootkit dan file streaming. Penyerang sudah berada dan menguasai suatu sistem dan kini berusaha untuk mencari informasi lanjutan (pilfering), menutupi jejak penyusupannya (covering tracks), dan menyiapkan pintu belakang (creating backdoor) agar lain kali dapat dengan mudah masuk lagi ke dalam sistem. Adanya Trojan pada suatu sistem berarti suatu sistem dapat dengan mudah dimasuki penyerang tanpa harus bersusah payah melalui tahapan-tahapan di atas, hanya karena kecerobohan pemakai komputer itu sendiri.

8. Creating Backdoors

Pintu belakang diciptakan pada berbagai bagian dari sistem untuk memudahkan masuk kembali ke sistem ini dengan cara membentuk user account palsu, menjadwalkan batch job, mengubah

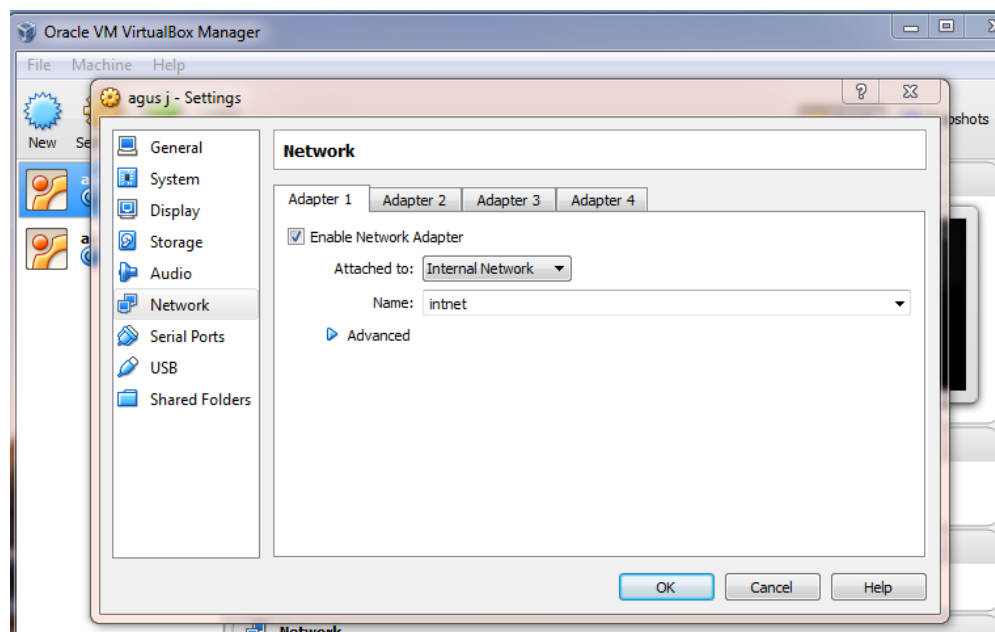
startup file, menanamkan servis pengendali jarak jauh serta monitoring tool, dan menggantikan aplikasi dengan trojan.

9. Denial Of Service

Bila semua usaha di atas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir. Meliputi SYN flood, teknik-teknik ICMP, Supernuke, land/latierra, teardrop, bonk, newtear, trincoo, smurf, dan lain-lain. Kalau penyerang sudah frustrasi tidak dapat masuk ke dalam sistem yang kuat pertahanannya, maka yang dapat dilakukannya adalah melumpuhkan saja sistem itu dengan menyerangnya menggunakan paket-paket data yang bertubi-tubi sampai sistem itu crash. Denial of service attack sangat sulit dicegah, sebab memakan habis bandwidth yang digunakan untuk suatu situs. Pencegahannya harus melibatkan ISP yang bersangkutan. Para script kiddies yang pengetahuan hacking-nya terbatas justru paling gemar melakukan kegiatan yang sudah digolongkan tindakan kriminal di beberapa negara ini.

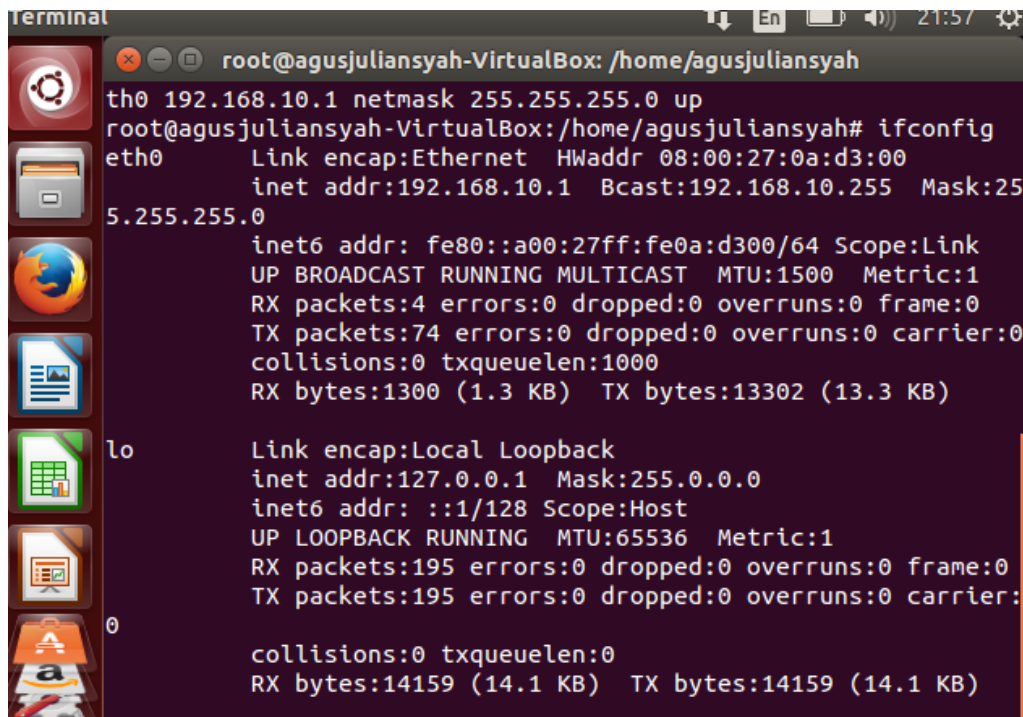
LANGKAH – LANGKAH LAPORAN TUGAS TENTANG EKSPLOTASI KEAMANAN

1. Mengatur setting network pada Ubuntu server dan DVL



Kita lihat tampilan di atas menunjukkan bahwa sebelum kita memulai Ubuntu server dan DVL nya kita harus mengubah networknya terlebih dahulu yang sebelumnya NAT kita ganti jadi internet network.

2. MEMBUKA ATAU MENGUBAH IFCONFIGNYA PADA UBUNTU SERVER



```
Terminal
root@agusjuliansyah-VirtualBox: /home/agusjuliansyah
eth0 192.168.10.1 netmask 255.255.255.0 up
root@agusjuliansyah-VirtualBox:/home/agusjuliansyah# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0a:d3:00
          inet addr:192.168.10.1  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0a:d300/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1300 (1.3 KB)  TX bytes:13302 (13.3 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:195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:195 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14159 (14.1 KB)  TX bytes:14159 (14.1 KB)
```

kita lihat bahwa tampilan langkah yang ke 2 menunjukkan bahwa ketika kita mau buka dan ingin mengganti ifconfignya untuk server dengan IP nya 192.168.10.1 dan NATMASK 255.255.255.0 untuk menyambungkan dan berkomunikasi dengan ifconfig pada DVL.

3. Membuka atau mengubah ifconfig yang ada di DVL

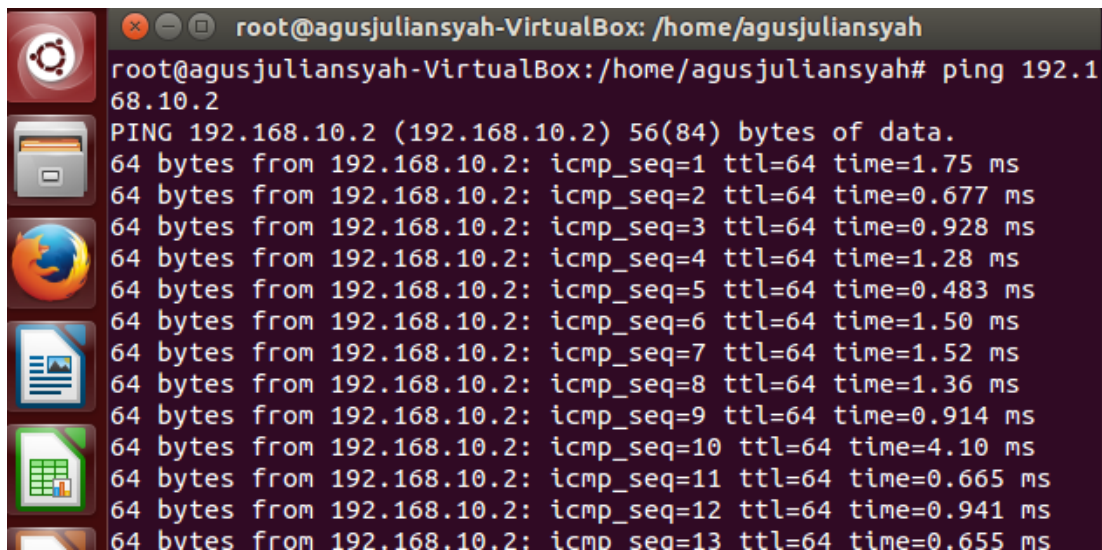


```
bt ~ # ifconfig eth0 192.168.10.2 netmask 255.255.255.0 up
bt ~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4D:8F:83
          inet addr:192.168.10.2  Bcast:192.168.10.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1782 (1.7 KiB)  TX bytes:1830 (1.7 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)
```

Pada tampilan di atas juga sama seperti tamplan pada langkah yang kedua ketika kita ingin membuka dan mengubah IFCONFIGNYA pada DVL untuk menyambung kan atau berkomunikasi dengan server dengan IP 192.168.10.2 dan NATMASK nya sama seperti server 255.255.255.0.

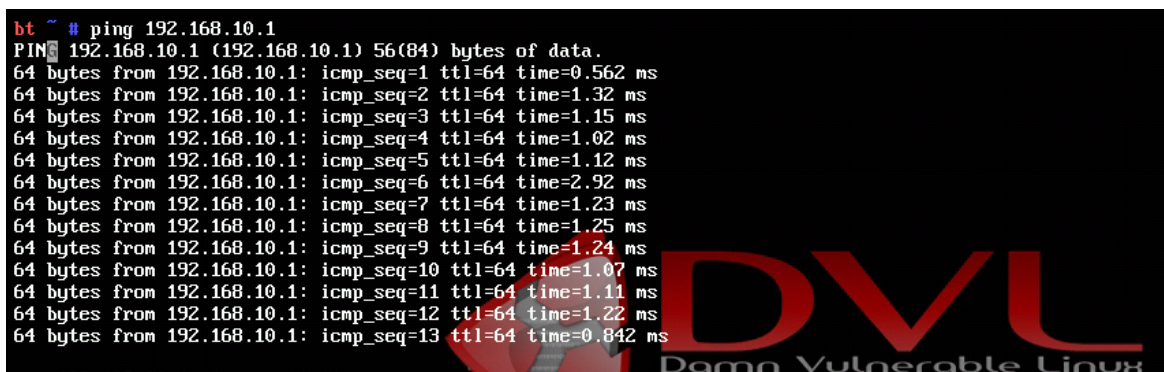
4. Melihat komunikasi antara ubuntu server ke DVL dengan IP 192.168.10.2



```
root@agusjuliansyah-VirtualBox: /home/agusjuliansyah
root@agusjuliansyah-VirtualBox:/home/agusjuliansyah# ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
64 bytes from 192.168.10.2: icmp_seq=1 ttl=64 time=1.75 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=64 time=0.677 ms
64 bytes from 192.168.10.2: icmp_seq=3 ttl=64 time=0.928 ms
64 bytes from 192.168.10.2: icmp_seq=4 ttl=64 time=1.28 ms
64 bytes from 192.168.10.2: icmp_seq=5 ttl=64 time=0.483 ms
64 bytes from 192.168.10.2: icmp_seq=6 ttl=64 time=1.50 ms
64 bytes from 192.168.10.2: icmp_seq=7 ttl=64 time=1.52 ms
64 bytes from 192.168.10.2: icmp_seq=8 ttl=64 time=1.36 ms
64 bytes from 192.168.10.2: icmp_seq=9 ttl=64 time=0.914 ms
64 bytes from 192.168.10.2: icmp_seq=10 ttl=64 time=4.10 ms
64 bytes from 192.168.10.2: icmp_seq=11 ttl=64 time=0.665 ms
64 bytes from 192.168.10.2: icmp_seq=12 ttl=64 time=0.941 ms
64 bytes from 192.168.10.2: icmp_seq=13 ttl=64 time=0.655 ms
```

Pada tampilan gambar di atas juga dapat kita lihat bahwa menunjukkan ketika kita ingin PING ke IP yang di pakai oleh DVL untuk melihat komunikasinya dengan IP nya 192.168.10.2 yang di pakai oleh DVL.

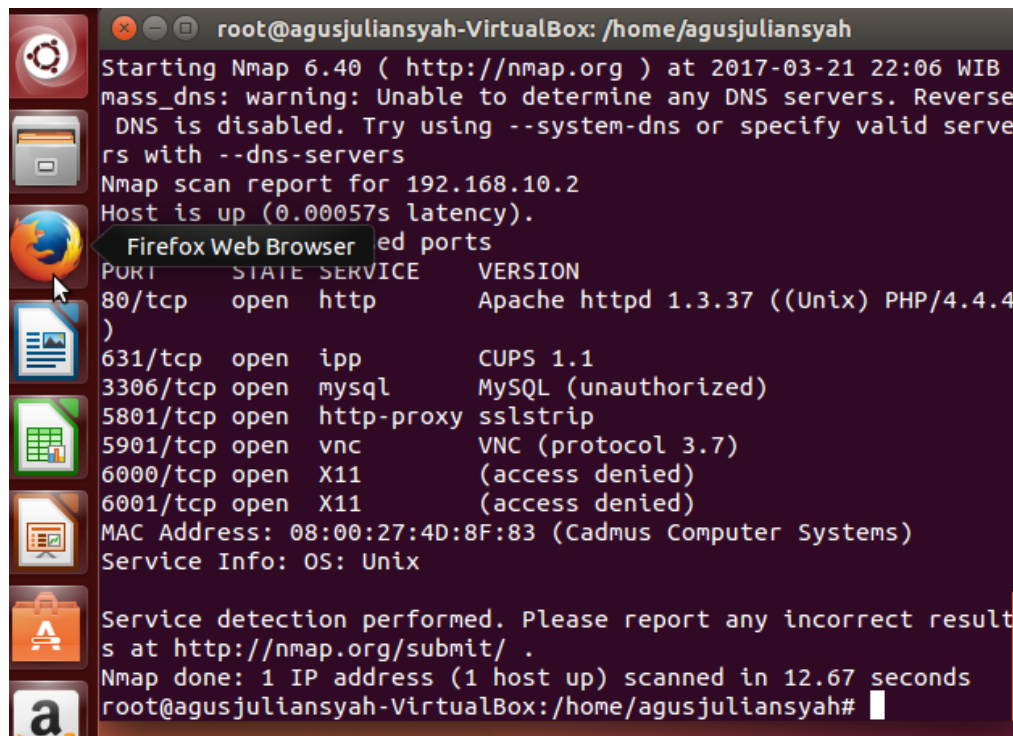
5. Melihat komunikasi antara DVL ke ubuntu server dengan IP 192.168.10.1



```
bt ~ # ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.562 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=1.32 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=1.15 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=1.02 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=64 time=1.12 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=64 time=2.92 ms
64 bytes from 192.168.10.1: icmp_seq=7 ttl=64 time=1.23 ms
64 bytes from 192.168.10.1: icmp_seq=8 ttl=64 time=1.25 ms
64 bytes from 192.168.10.1: icmp_seq=9 ttl=64 time=1.24 ms
64 bytes from 192.168.10.1: icmp_seq=10 ttl=64 time=1.07 ms
64 bytes from 192.168.10.1: icmp_seq=11 ttl=64 time=1.11 ms
64 bytes from 192.168.10.1: icmp_seq=12 ttl=64 time=1.22 ms
64 bytes from 192.168.10.1: icmp_seq=13 ttl=64 time=0.842 ms
```

Pada tampilan langkah kelima ini juga sama seperti langkah keempat yaitu menunjukkan bahwa ketika kita ingin PING kerserver untuk berkomunikasi dengan IP 192.168.10.1 yang di pakai oleh server.

6. Melihat servis yang di jalankan dengan menggunakan nmap

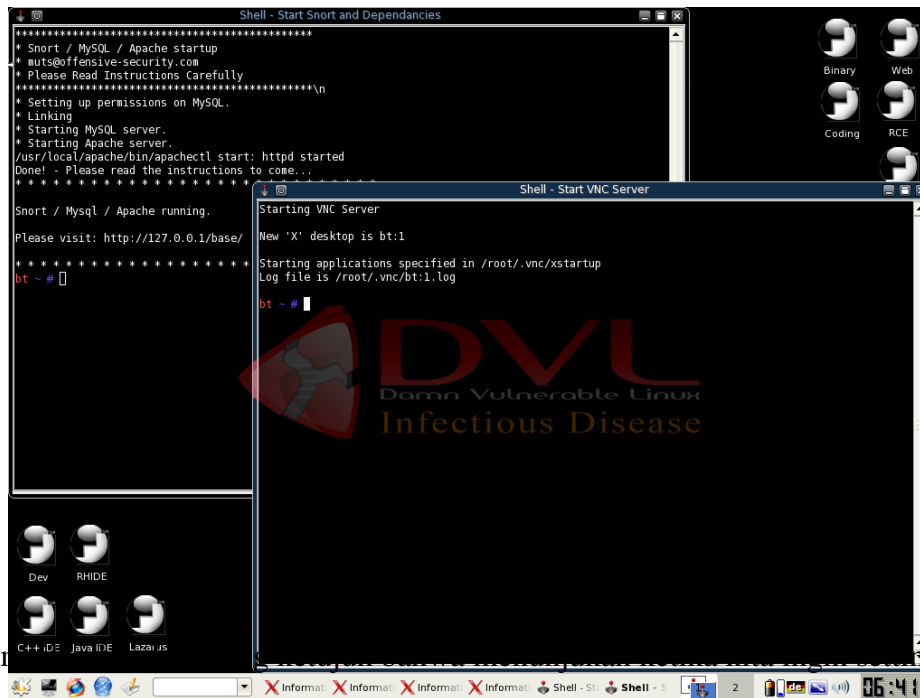


```
root@agusjuliansyah-VirtualBox: /home/agusjuliansyah
Starting Nmap 6.40 ( http://nmap.org ) at 2017-03-21 22:06 WIB
mass_dns: warning: Unable to determine any DNS servers. Reverse
DNS is disabled. Try using --system-dns or specify valid serve
rs with --dns-servers
Nmap scan report for 192.168.10.2
Host is up (0.00057s latency).
Open 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: 08:00:27:4D:8F:83 (Cadmus Computer Systems)
Service Info: OS: Unix

Service detection performed. Please report any incorrect result
s at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.67 seconds
root@agusjuliansyah-VirtualBox:/home/agusjuliansyah#
```

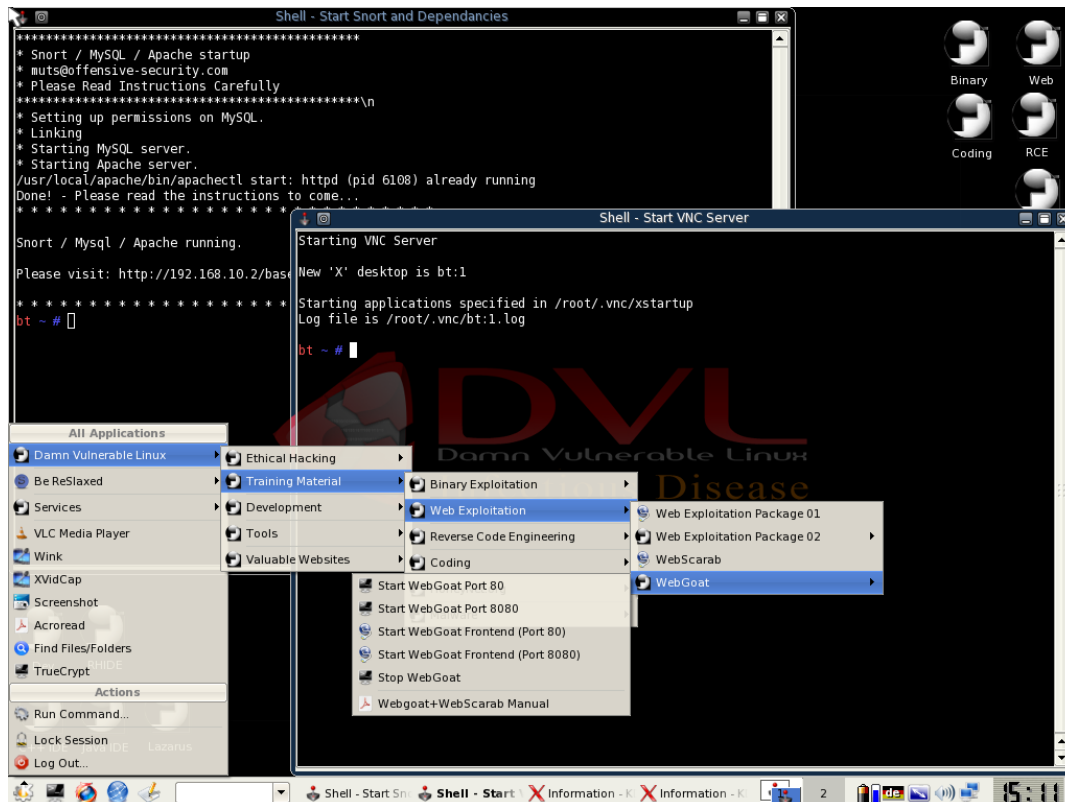
Pada tampilan gambar di atas menunjukkan bahwa kita dapat melihat tampilan servis dengan menggunakan server dengan IP 192.168.10.2 servis tersebut di jalankan dengan menggunakan nmap untuk scenningnya, bahwa tampilan di atas juga dapat kita lihat bahwa menunjukkan PORT, STATE, SERVICE, dan VERSION nya yang berbeda – beda.

7. Setting servis yang ada di DVL



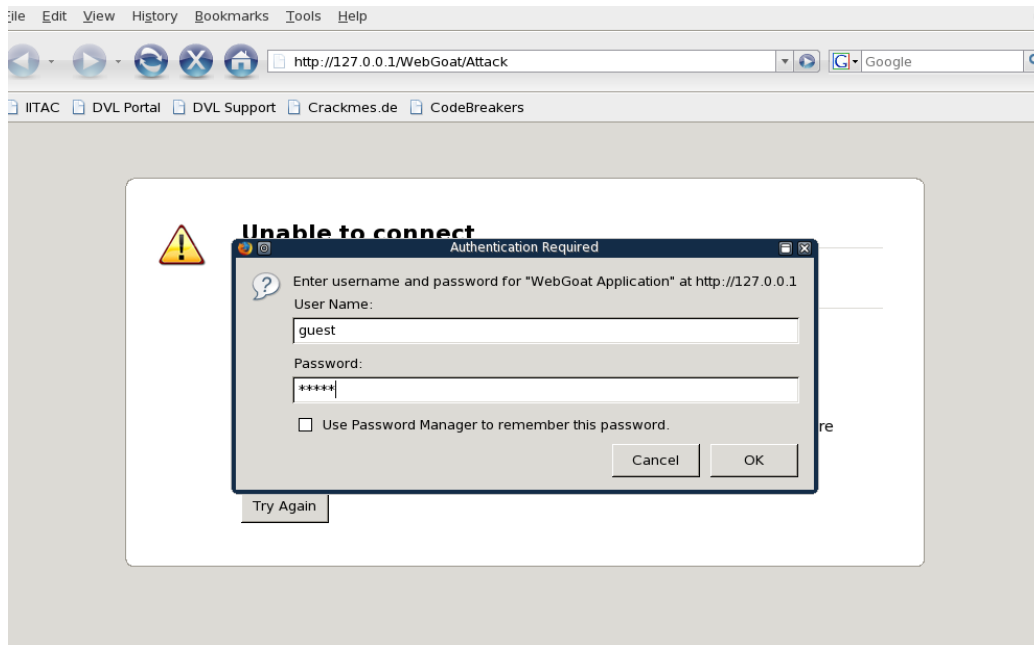
Pada terminal ini, kita akan setting servis yang ada pada DVL semua yang ada di servis harus kita setting menjadi start semua atau untuk memulai langkah berikutnya.

8. Mengatur DAMN VULNERABLE LINUX untuk webgoatnya yang ada di DVL pada PORT 80



Pada tampilan langka ke8 ini menunjukkan bahwa ketika kita mau mengatur DAMN VULNELABLE LINUX untu webgoat yang ada pada DVL ketika ingin starr webgoat pada PORT 80 karena untuk menampilkan webgoat pada langkah berikutnya.

9. Menampilkan webgoat yang telah di atur pada langkah ke8.



Pada tampilan gambar di atas menunjukkan bahwa ketika kita ingin menunjukan webgoat yang telah di start (mulai) pada langkah yang ke8 dan akan muncul webgoatnya di browser yang akan muncul juga webgoat application dengan IP 127.0.0.1 yang telah di atur di langkah ke8, kita juga akan masukan username dan password pada webgoat application untuk menampilkan langkah berikutnya.

10. Menampilkan hasil webgoat yaitu OWASP dan ASPECT SECURITY.



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

DWASP 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.msacadamian.com>)
Erwin Geirnaert
(<http://www.zionsecurity.com>)

[Start WebGoat](#)

Pada tampilan di atas bahwa menunjukkan hasil webgoat yaitu akan muncul OWASP DAN ASPECT SECURITY karena WebGoat di rilis hari ini. hal ini terutama rilis pemeliharaan lama tertunda, banyak perbaikan bug dan beberapa update. Mencobanya dan merasa bebas untuk mengirim komentar kepada saya, merekomendasikan pada Goole Plus, Bintang, atau mengajukan WebGoat Google Isu untuk bug, kesalahan ketik atau permintaan fitur. OWASP DAN ASPECT SECURITY memiliki masing – masing tipenya yaitu pada OWASP ada webgoat design team dan special thanks for Vs.1, pada ASPECT SECURITY ada lesson contributor dan documentation contributor yang akan mulai (start) webgoat nya untuk manampilkan langkah berikutnya.

11. Menampilkan untuk install OWASP webgoat VS.1

Pada tampilan gambar di atas bahwa menunjukkan ketika kita ingin menginstall OWASP webgoat dengan cara masukan last name karena WebGoat adalah aplikasi sengaja tidak aman web yang dikelola oleh OWASP dirancang untuk mengajarkan pelajaran keamanan aplikasi web." Di kelas kami, kami akan memasang WebGoat dan kemudian digunakan untuk untuk pelajaran pengantar dalam cross-site scripting (XSS) dan SQL Suntikan. Yang keren tentang WebGoat adalah bahwa ada lebih dari satu pelajaran serangan selusin masalah, petunjuk, dan solusi untuk memecahkan. aplikasi mandiri ini memungkinkan Anda untuk menggunakan aplikasi web dan kemudian menghubungkan untuk itu dan mencoba serangan hacking. Seperti yang akan Anda lihat di bawah, WebGoat sangat mudah untuk menginstal.

12. Menampilkan hasil installaasi OWASP webgoat VS.1 yang last namenya' smirt'

OWASP WebGoat V5.1

String SQL Injection

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
 Improper Error Handling
 Insecure Storage
 Denial of Service
 Insecure Configuration
 Web Services

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 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	2435600002222	MC		0
102	John	Smith	4352209902222	AMEX		0

OWASP Foundation | Project WebGoat

Pada tampilan gambar di atas menunjukan hasil installasi dan lalu ketika kita memasukan kata smith maka akan muncul di bawah nya select 'from user_data where last_name 'smith'' dan juga muncul data table yang berisi USER_DATA, FIRST NAME, LAST_NAME, CC_NUMBER, CC TYPE, COOKIE dan LOGIN_COUNT pada tampilan OWASP wegoat VS.1 yang ada pada gambar di atas yang memiliki 2 data saja.

13. Menampilkan hasil OWASP webgoat VS.1 yang last namenya 'test' or 1=1'

* 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	Joesph	Something	33843453533	AMEX		0

Pada tampilan langkah ke 13 ini sama seperti langkah ke 12 yaitu menampilkan hasil OWASP webgoat VS.1 yang berbeda hanya last name saja pada tampilan gambar di atas menampilkan last name 'test' or 1=1.. dan juga muncul data table yang berisi USER_DATA, FIRST NAME, LAST_NAME, CC_NUMBER, CC TYPE, COOKIE dan LOGIN_COUNT pada tampilan OWASP wegoat VS.1, ada juga yang berbeda tampilan langkah 12 dan 13 , langkah ke12 tadi hanya memiliki 2 data saja sedangkan langkah yang ke 13 memiliki 13 data yang 2 data yang sama tiap USER_DATA, FIRST NAME, LAST_NAME, CC_NUMBER, CC TYPE, COOKIE dan LOGIN_COUNT yang di tampilkan di table di atas.

KESIMPULAN

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, sayangnya sekali masalah keamanan ini seringkali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Keamanan server webgoat VS.1 biasanya merupakan masalah dari seorang administrator. Dengan memasang server webgoat VS.1 di sistem Anda, Anda membuka akses (meskipun secara terbatas) pada orang luar. Apabila

server Anda terhubung ke Internet dan memang server webgoat VS.1 Anda disiapkan untuk publik, Web Server dan database server bagaikan jantung dan otak dari organisme Internet. Dua komponen ini menjadi komponen pokok dari sebuah aplikasi webgoat VS.1 yang tangguh dan tepatlah keduanya menjadi target hacker. Ada beberapa aplikasi yang di pakai pada tugas ini seperti aplikasi pada SERVER dan pada DVL.