

TUGAS  
KEAMANAN JARINGAN KOMPUTER



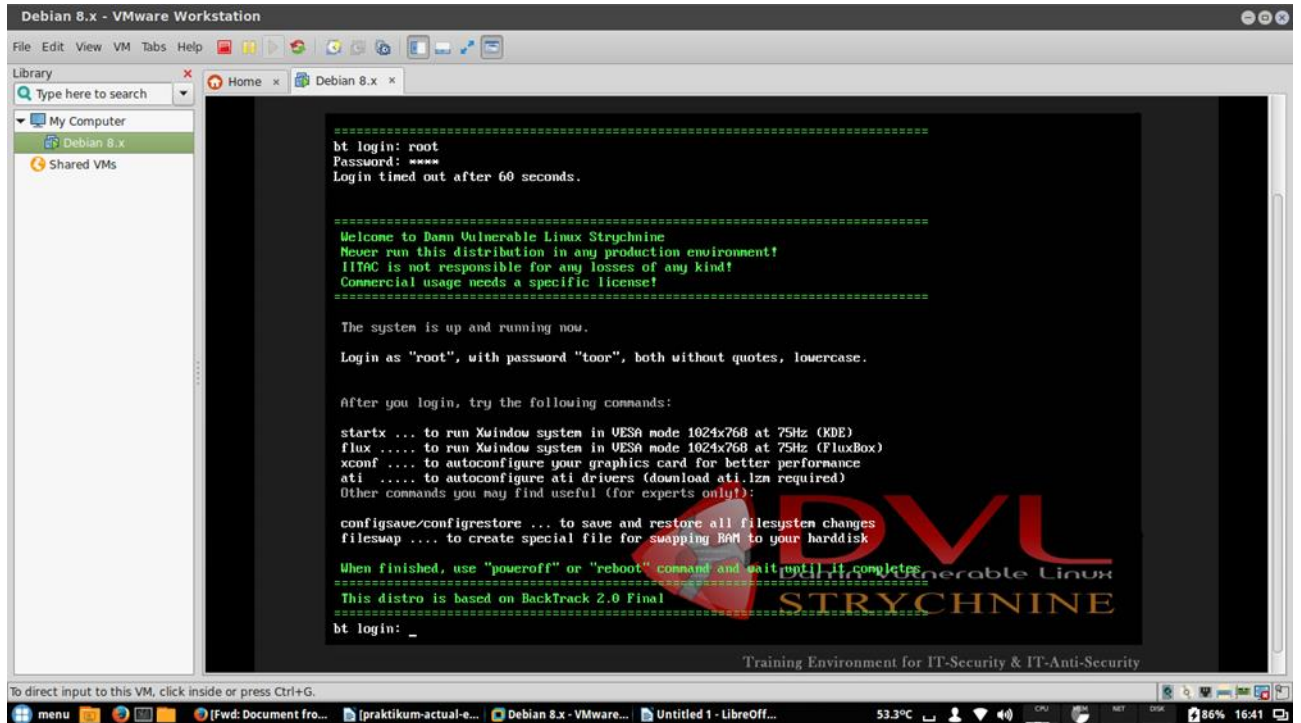
Nama : Dede Triseptiawan

Nim : 09011181320001

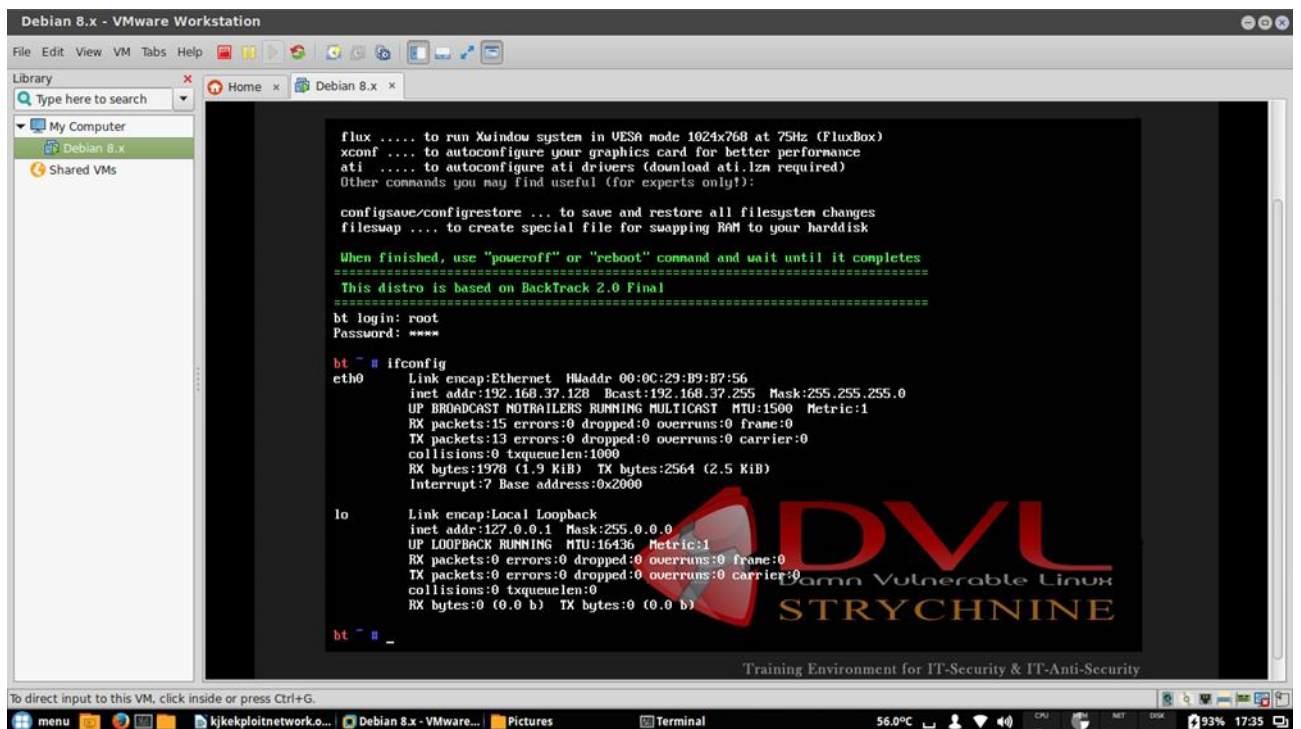
SISTEM KOMPUTER  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS SRIWIJAYA

2017

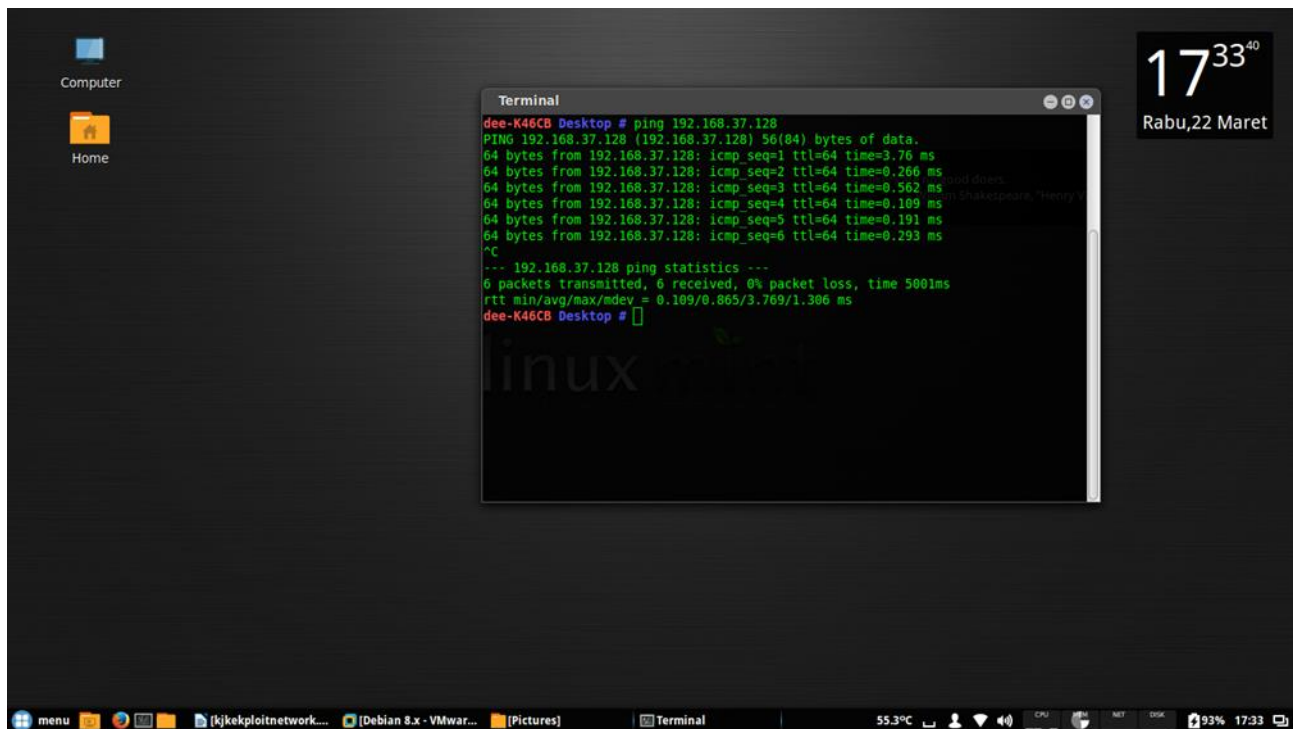
Pada percobaan actual exploit menggunakan DVL. DVL (damn vulnerable linux) adalah distribusi Linux terbentuk dari Debian dengan tujuan menjadi sebuah sistem yang sengaja rentan untuk tujuan praktek / belajar dalam hal Jaringan dan Keamanan Komputer.



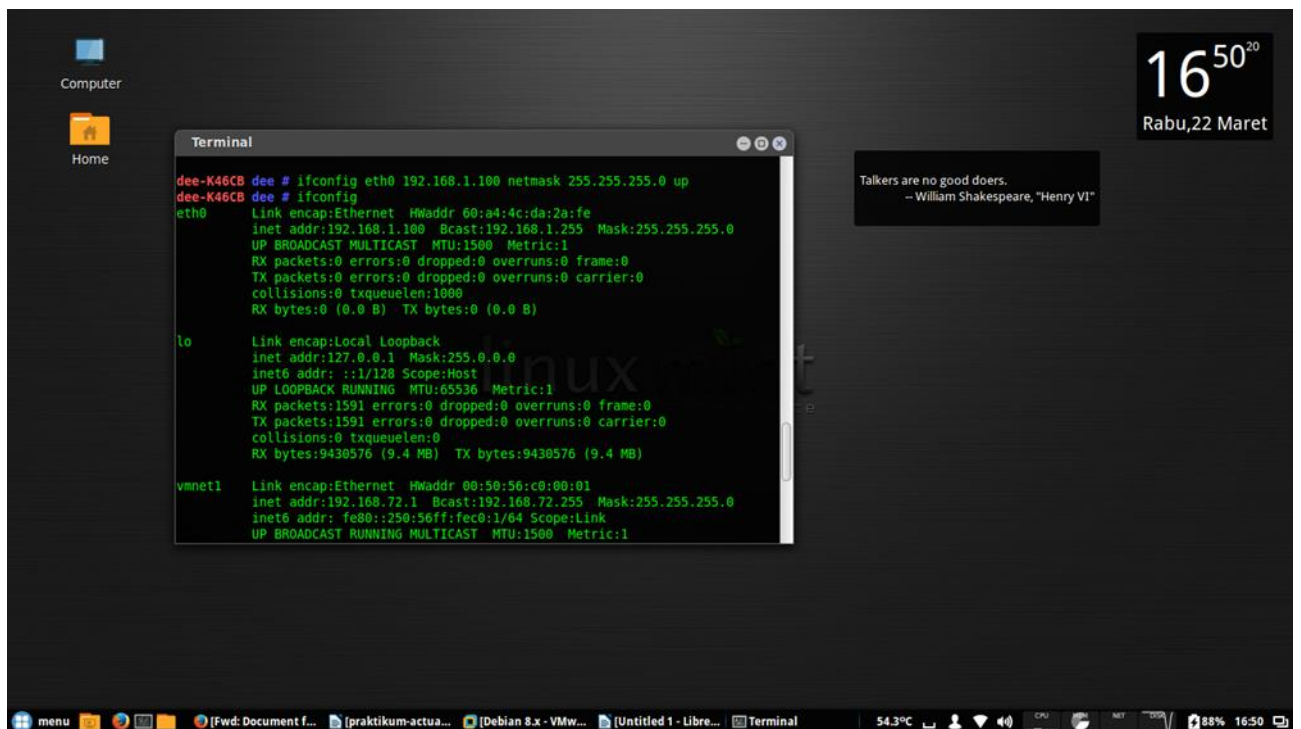
Yang pertama kita lakukan login ke DVL dengan user "root" dan pass "toor"



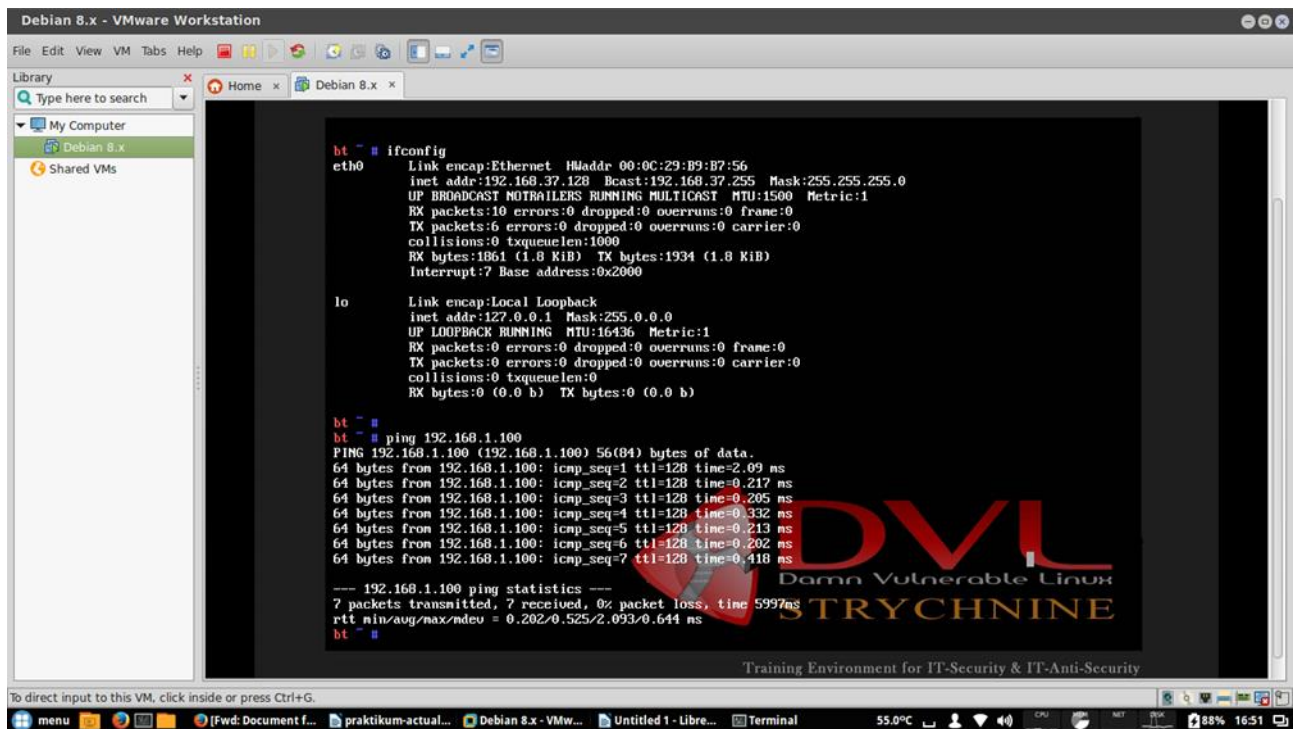
Kemudian kita melihat ip dari DVL tersebut dengan perintah ifconfig, didapatkan ip eth0 192.168.37.128



Kemudian kita coba tes ping dari client ke DVL apakah tersambung, pada gambar diatas tersambung



Kemudian kita buat ip eth0 client agar dapat di kenali DVL dan cek kembali tersambung atau tidak, dengan perintah ifconfig eth0 192.168.1.100 netmask 255.255.255.0 up



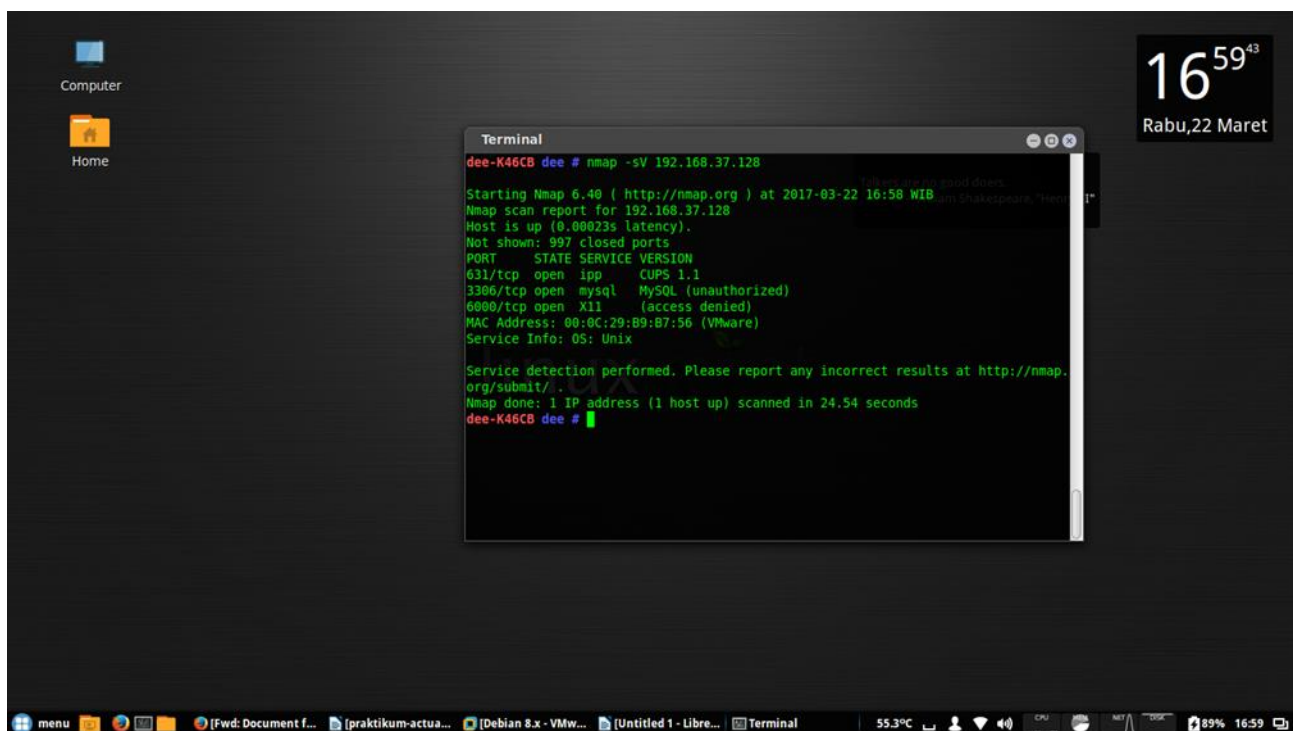
```
Debian 8.x - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian 8.x
Shared VMs

bt ~ # ifconfig
eth0   Link encap:Ethernet HWaddr 00:0C:29:B9:B7:56
       inet addr:192.168.37.128 Bcast:192.168.37.255 Mask:255.255.255.0
       UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500 Metric:1
       RX packets:10 errors:0 dropped:0 overruns:0 frame:0
       TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:1861 (1.8 KiB)  TX bytes:1934 (1.8 KiB)
       Interrupt:7 Base address:0x2000

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 ~ # ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data:
64 bytes from 192.168.1.100: icmp_seq=1 ttl=128 time=2.09 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=128 time=0.217 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=128 time=0.205 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=128 time=0.332 ms
64 bytes from 192.168.1.100: icmp_seq=5 ttl=128 time=0.213 ms
64 bytes from 192.168.1.100: icmp_seq=6 ttl=128 time=0.202 ms
64 bytes from 192.168.1.100: icmp_seq=7 ttl=128 time=0.418 ms
--- 192.168.1.100 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5997ms
rtt min/avg/max/ndev = 0.202/0.525/2.093/0.644 ms
bt ~ #
```

Setelah membuat ip di client, kita coba tes ping dari DVL ke client, dengan perintah ping 192.168.1.100. pada gambar diatas, dapat dilihat bahwa tersambung.



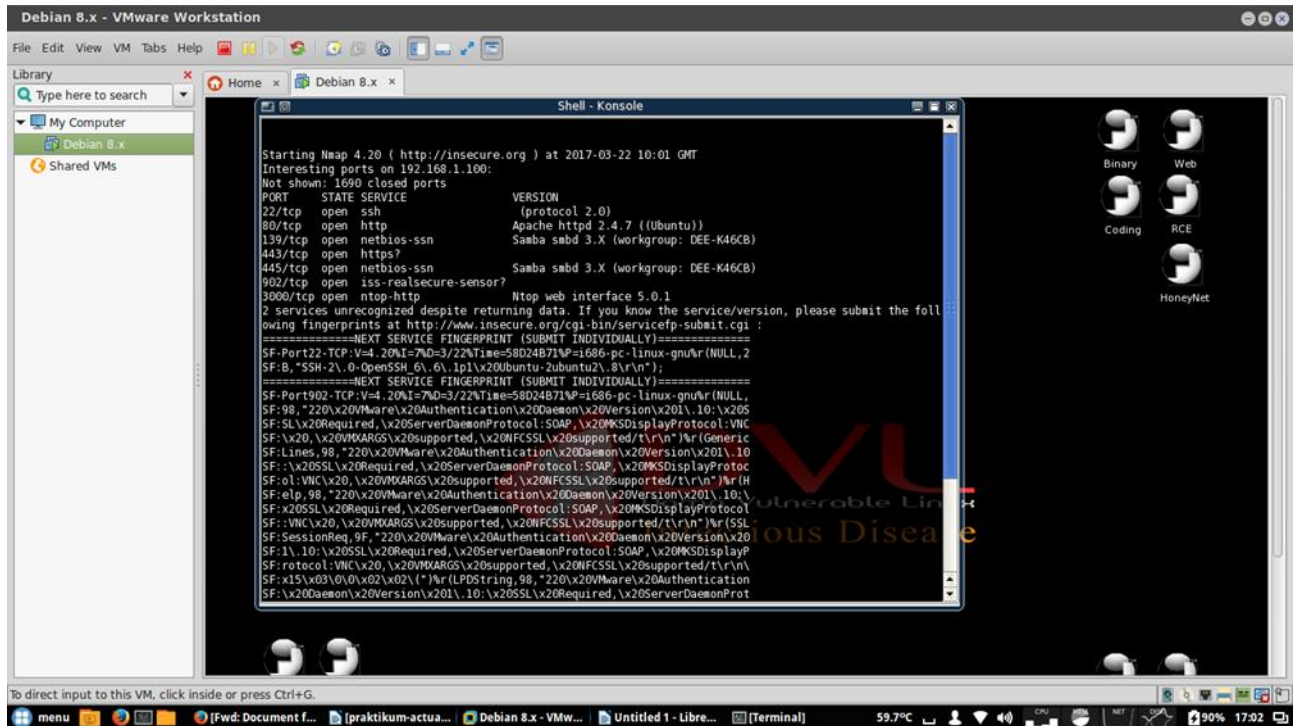
```
Computer
Home

Terminal
dee-K46CB dee # nmap -sV 192.168.37.128

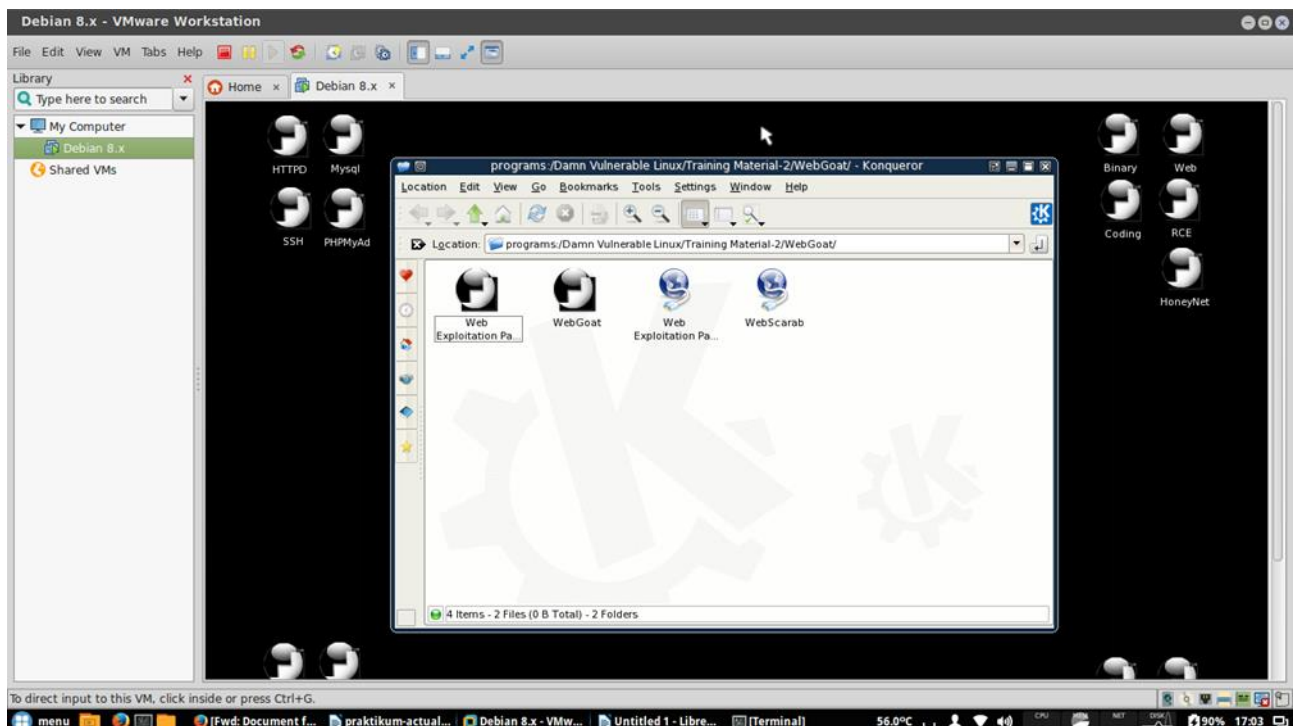
Starting Nmap 6.40 ( http://nmap.org ) at 2017-03-22 16:58 WIB
Nmap scan report for 192.168.37.128
Host is up (0.00023s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
631/tcp   open  ipp      CUPS 1.1
3306/tcp  open  mysql    MySQL (unauthorized)
6000/tcp  open  X11      (access denied)
MAC Address: 00:0C:29:B9:B7:56 (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 24.54 seconds
dee-K46CB dee #
```

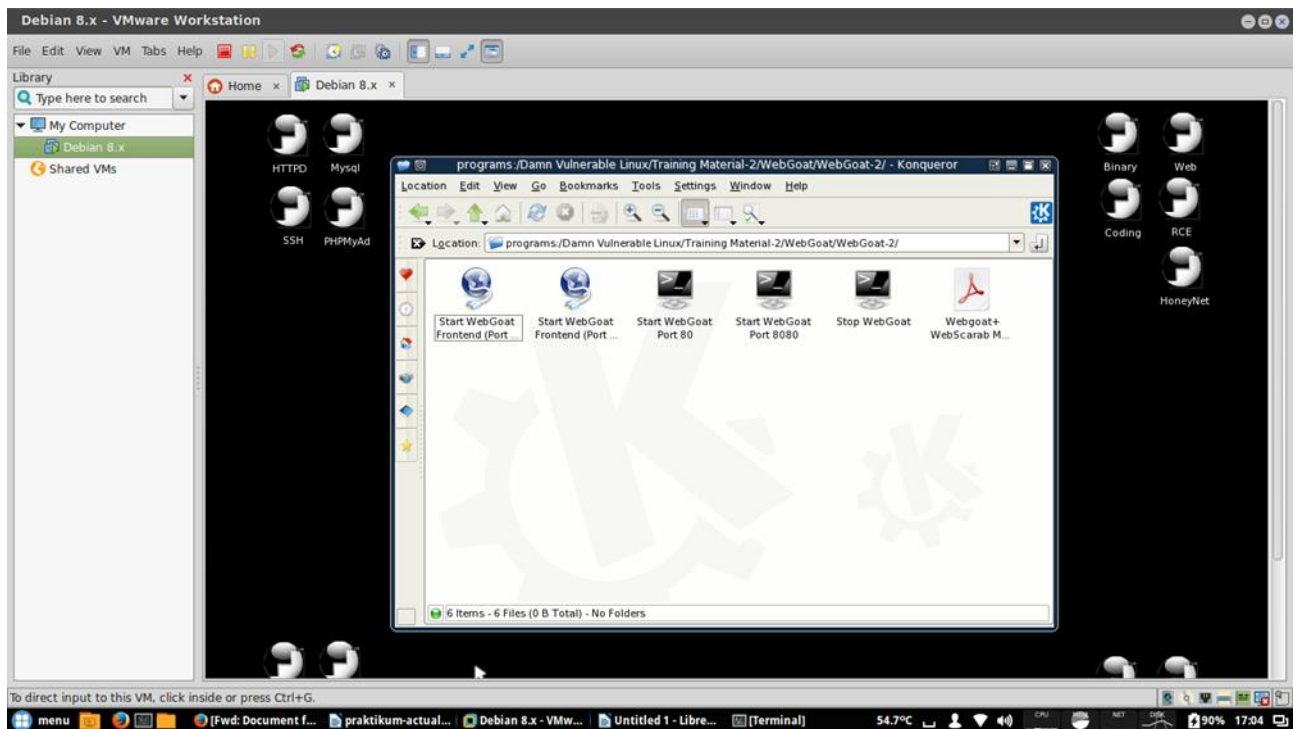
Kemudian kita ketik pada terminal client nmap -sV 192.168.37.128(ip target) DVL. Dapat dilihat layanan yang digunakan diantaranya mysql, x11, dll.



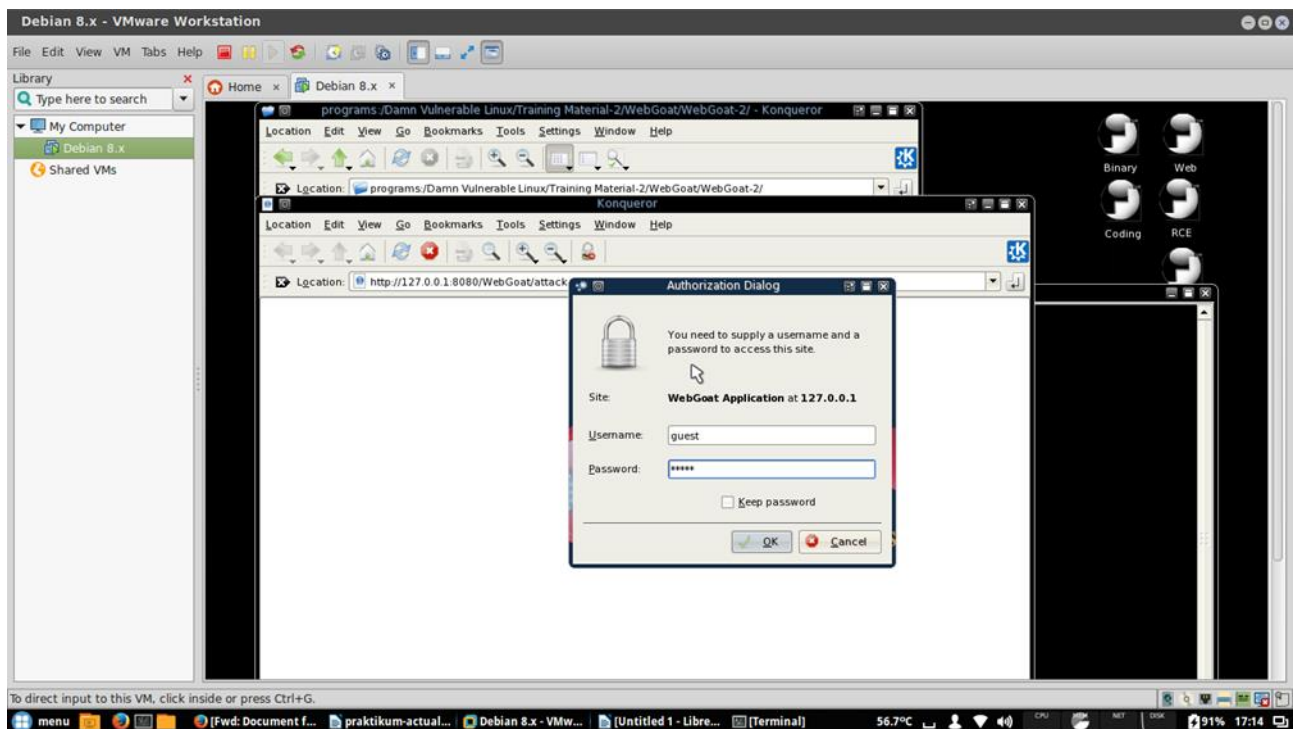
Kemudian kita cek kembali nmap -sV dari DVL ke client(192.168.1.100) dapat dilihat layanan yang digunakan diantaranya ssh, http, netbios-ssn, dll.



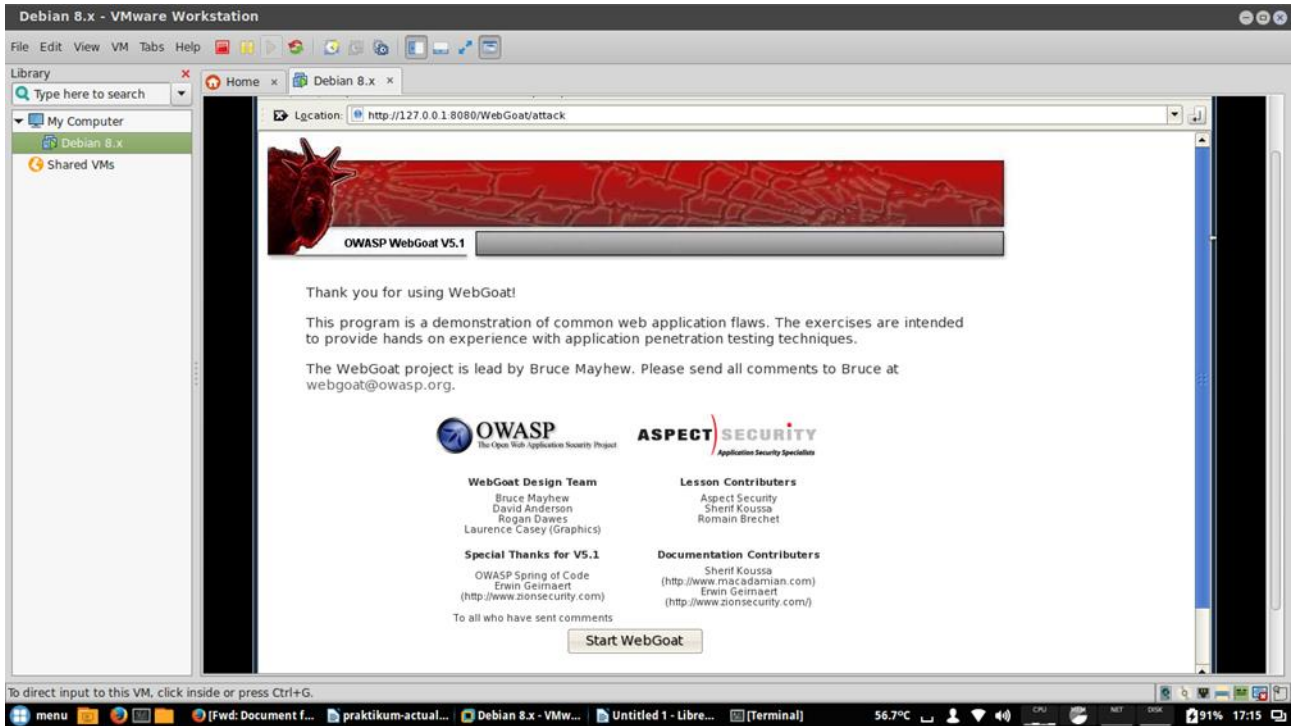
Kemudian kita klik webgoat, webgoat ini Web Goat adalah Project Open Source yang dapat digunakan agar orang lain bisa belajar web hacking.



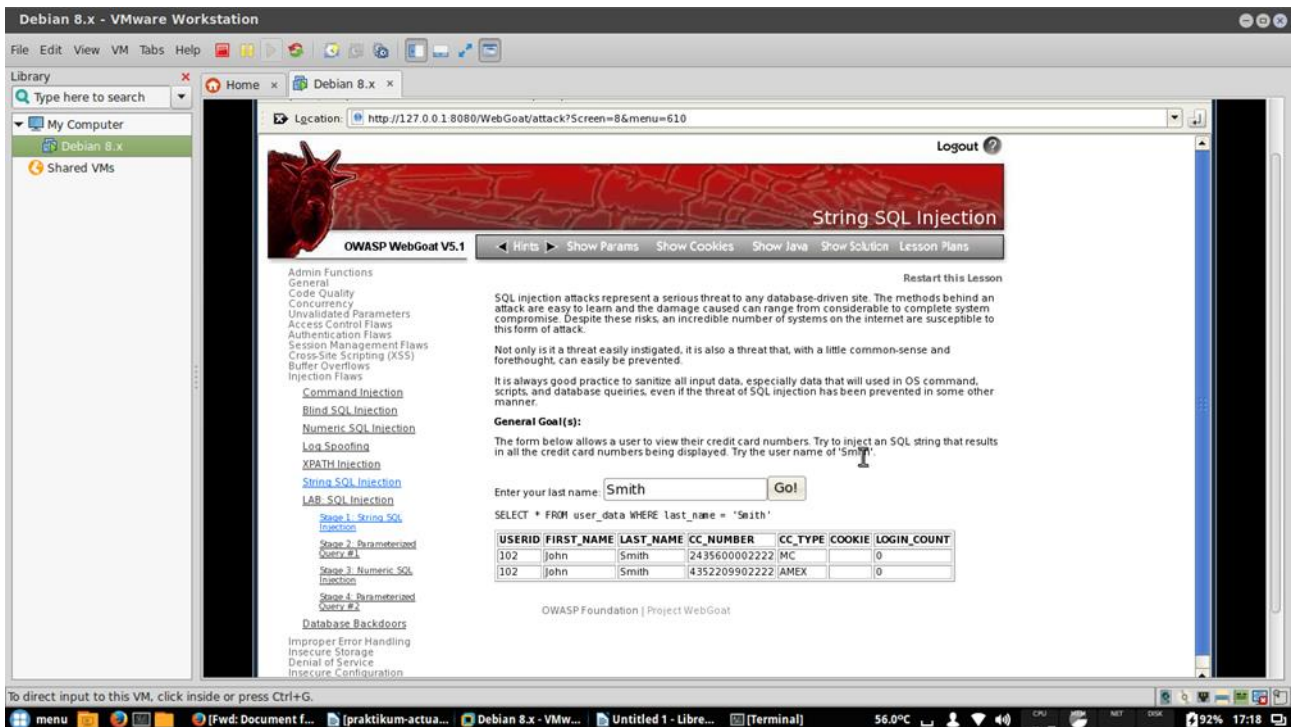
Kemudian klik start webgoat port 8080, untuk mengaktifkan webgoat. Setelah aktif, klik start webgoat frontend(port 8080), untuk membuka otomatis web localhost webgoat.



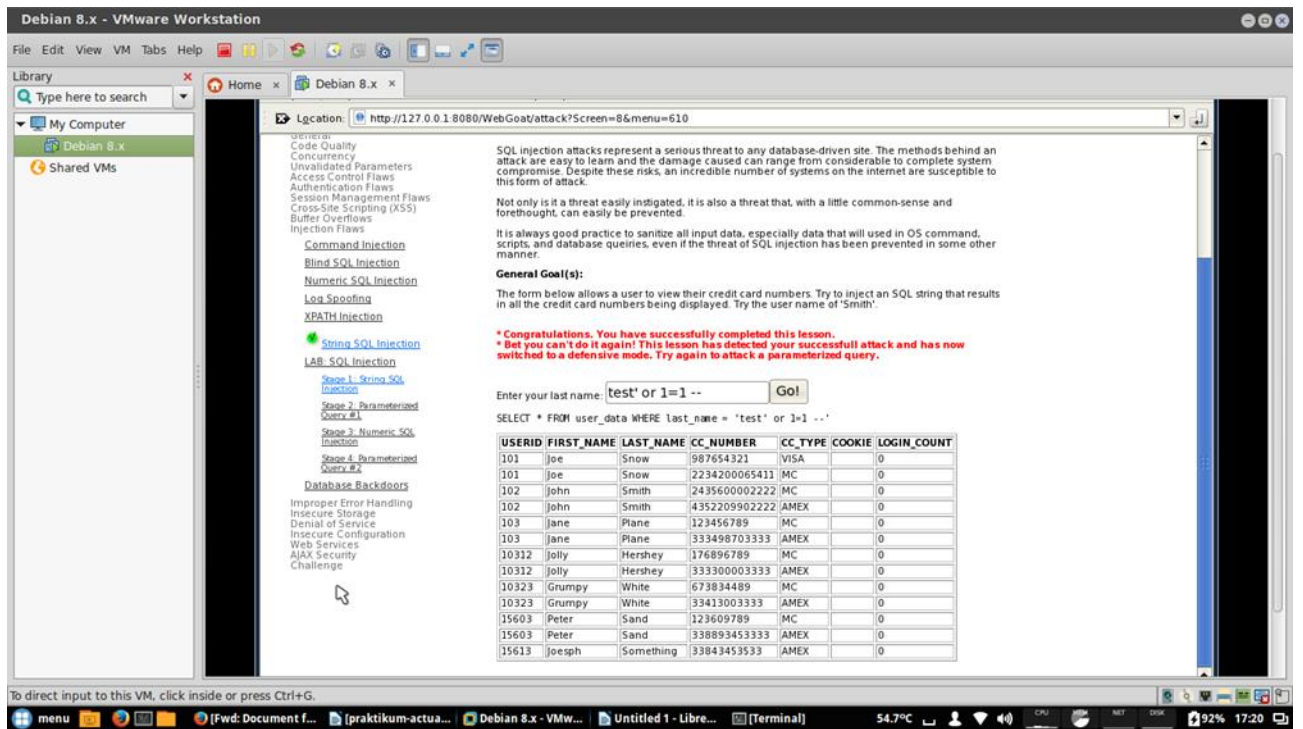
Setelah terbuka, masukkan username "guest" dan pass "guest"



Setelah terbuka, klik start webgoat



Berikutnya, klik injection flaws → string SQL injection, lalu kita coba masukkan nama Smith



Kemudian kita coba input test' or 1=1 – maksudnya test adalah nama file dari database, 1=1 boolean true, walaupun kita salah maka akan tetap true jawabannya.