PROJECT 4
Port Scans dan Windows Firewall

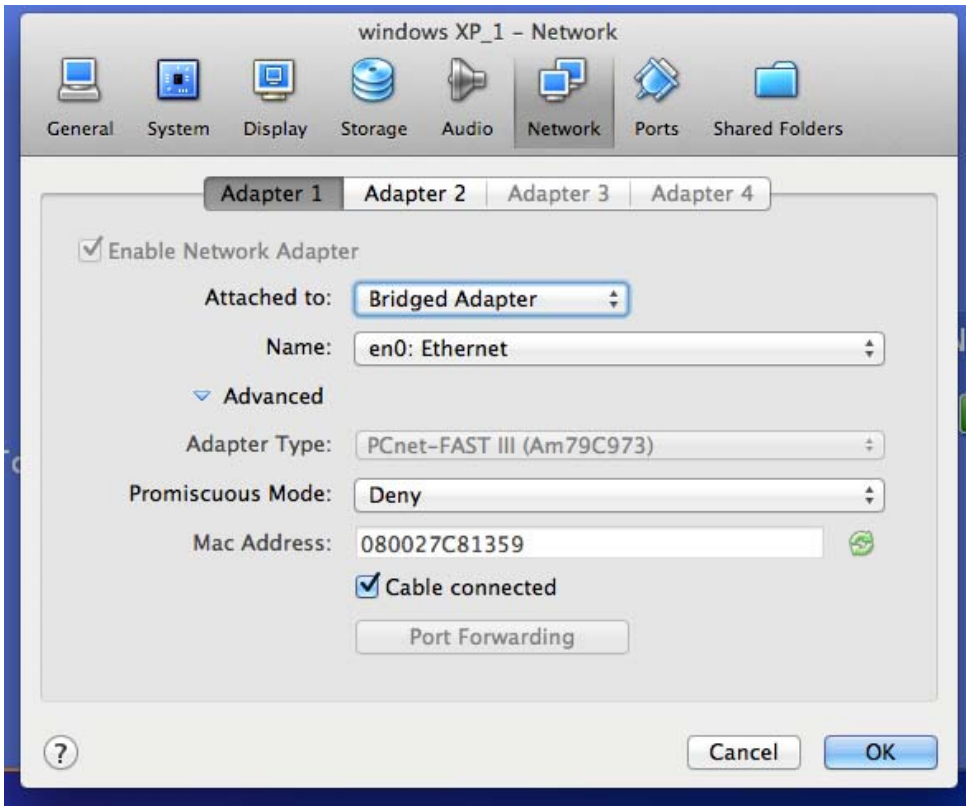
Kebutuhan dalam projek ini

- Dua komputer yang menjalankan Backtrack dan Windows versi apa saja, dengan akses Internet.
- Diperlukan hak akses admin pada kedua komputer tersebut .

Perhatian! Port scan merupakan perbuatan illegal! Port scan bisa dideteksi menggunakan intrusion detection systems dan bisa menempatkan kita dalam masalah. Jangan melakukan scan ke server lain, lakukan scan computer yang diizinkan. Komputer yang seharusnya boleh discan adalah computer yang ada dalam laboratorium atau komputer di rumah.

Persiapan Target

1. Saudara membutuhkan dua komputer virtual dalam projek ini: gunakan Backtrack sebagai **Scanner** dan komputer Windows yang dijalankan melalui VirtualBox sebagai **Target (Application-System-VirtualBox)**.
2. Jalankan komputer **Scanner** dan **Target**. Log in sebagai **Student** tanpa password.
3. Pastikan komputer windows yang dijalankan melalui VirtualBox dalam mode (bridged)

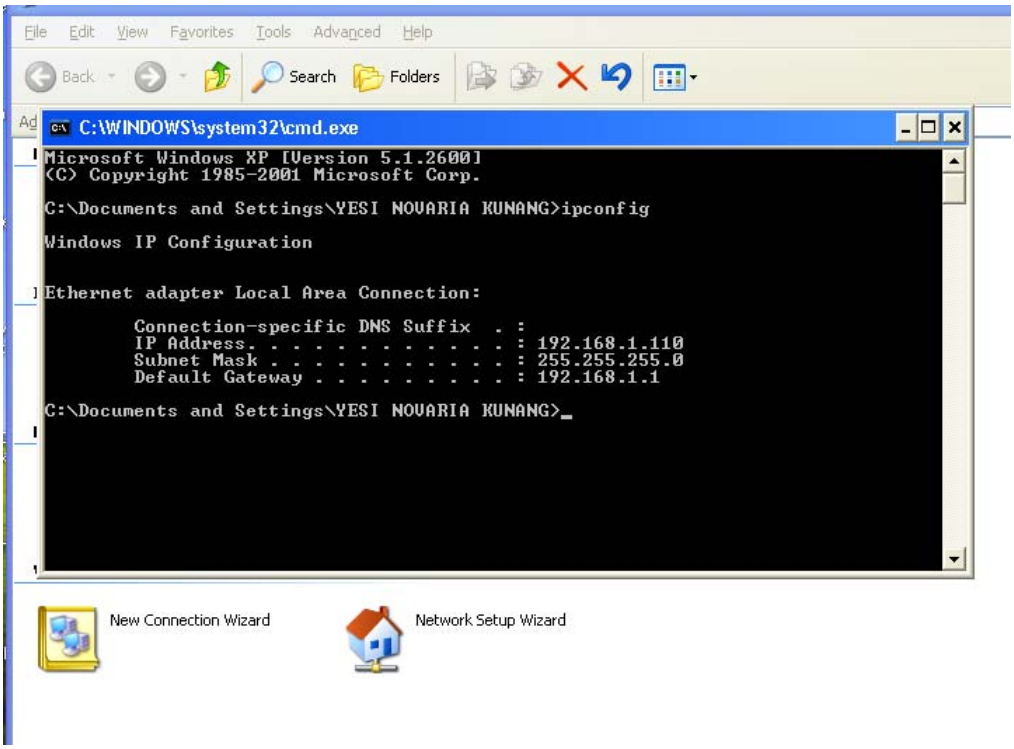


Seting di bagian atas jendela Virtual Box (Devices-Network Adapter)

Menentukan IP Address dari komputer Target

Target IP: _____

4. Pada Komputer **Target**, click **Start**. Di kotak **Search**, masukan **CMD** dan tekan tombol Enter.
5. Di jendela **Command Prompt** window, masukan menu **IPCONFIG** dan tekan tombol Enter. Akan Nampak beberapa IP addresses. Scroll dan cari ip yang berawalan **192.168.77**. IP address tersebut merupakan network interface yang mengkoneksikan komputer target dengan LAN laboratorium Foresec. Catat ip address tersebut.

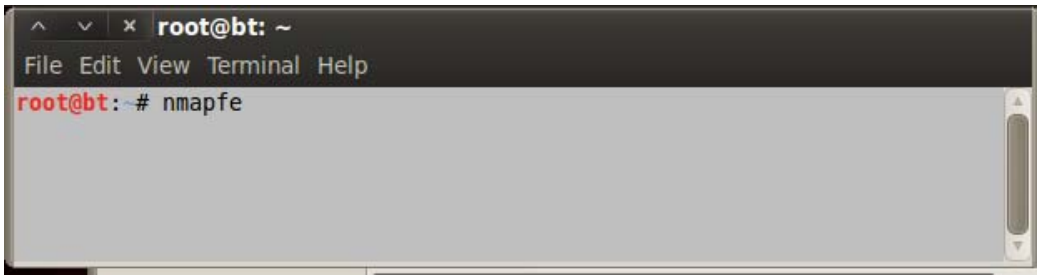


Matikan Firewall komputer target

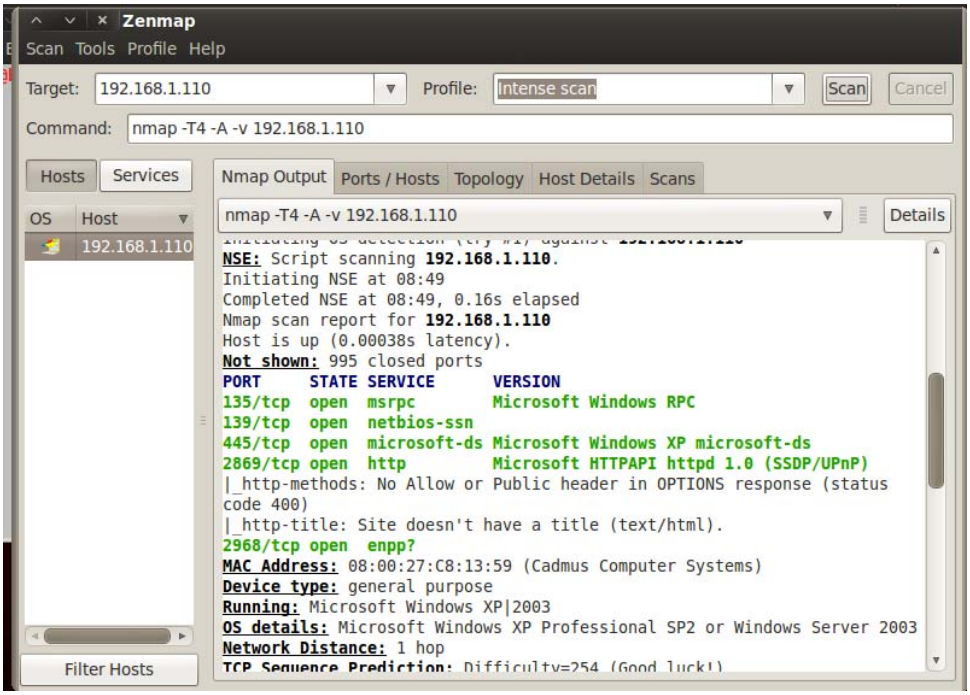
6. Pada komputer **Target**, tekan tombol logo Windows logo di kiri bawah keyboard (⊞). Ketikkan **FIREWALL** pada kotak pencarian.
7. "**Windows Firewall**" akan Nampak di Programs list. Pilih kemudian tekan tombol Enter.
8. "Control Panel ► System and Security ► Windows Firewall" akan terbuka. Di sisi kiri, click "**Turn Windows Firewall on or off**". Jika kotak pops up "User Account Control", click **Continue**.
9. Di kotak "System and Security ► Windows Firewall ► Customize Settings", click tombol "**Turn off Windows Firewall (not recommended)**". Click **OK**.

Melakukan Scanning komputer Target (Windows)

10. Dari jendela Backtrack (**Scanner Machine),** klik terminal kemudian ketikan Comand **"nmapfe"** kemudian tekan Enter.



11. Pada jendela **Zenmap**, di kotak **Target:** , masukan "**Target IP**" yang sudah kalian catat pada langkah 4. Click tombol **Scan**.
12. Nmap akan terlihat seperti gambar di bawah. Scroll down sampai tampil "**PORT STATE SERVICE VERSION**" pada tulisan berwarna biru dengan hasil tulisan berwarna hijau di bawahnya, seperti terlihat di halaman berikut.



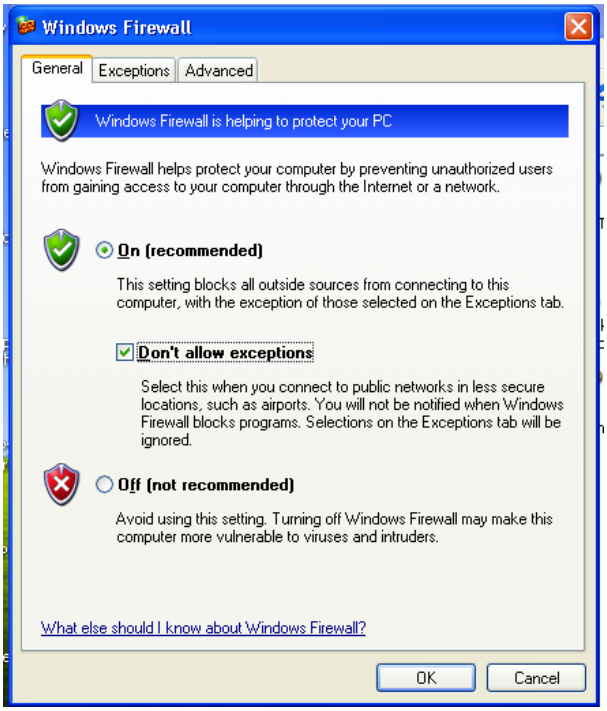
13. Tujuan dari proses scan ini adalah untuk melihat port yang terbuka pada komputer target, serta melihat apakah firewall nya bekerja atau tidak. Nmap seharusnya akan menampilkan sekurangnya satu port yang terbuka di komputer target—hampir semua komputer Windows memiliki ports 135, 139, dan 445 terbuka. Bisa jadi port lain juga terbuka. Port-port tersebut bisa jadi celah keamanan yang potensial bagi penyerang untuk masuk ke komputer tersebut (bisa dilihat di video yang diupload).

Simpan Screen Image

14. Pada komputer **Scanner**, pastikan jendela Zenmap terbuka, yang minimal menampilkan sekurangnya satu port yang terbuka.
15. Tekan tombol **PrintScrn** kopi seluruh desktop ke clipboard.
16. Simpan dengan nama **NamaKamu_Proj4a**. Simpan dengan format **JPEG** atau **PNG**.

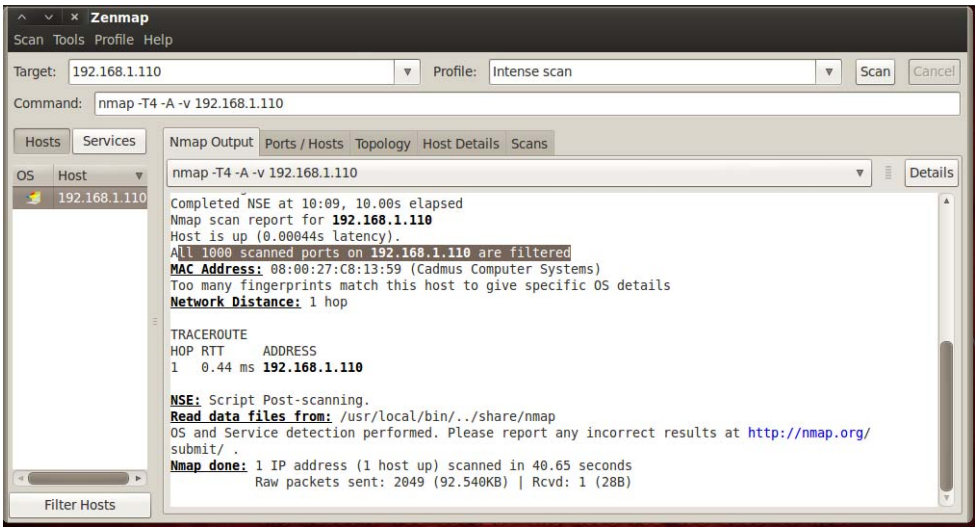
Aktifkan Firewall pada Komputer Target dengan No Exceptions

17. Pada **Komputer Target**, tekan tombol logo Windows pada bagian kiri bawah keyboard (⊞). Ketik **FIREWALL** ke dalam kotak pencarian.
18. "**Windows Firewall**" akan Nampak di daftar Programs list. Jika belum dipilih, tekan tombol panah untuk memilih. Kemudian tekan tombol Enter.
19. "Control Panel ► System and Security ► Windows Firewall" terbuka. Di sisi kiri, click "**Turn Windows Firewall on or off**". Jika tampil pops up "User Account Control", click **Continue**.
20. Pada kotak "System and Security ► Windows Firewall ► Customize Settings", click tombol "**Turn on Windows Firewall**". Pilih juga kotak"**Block all incoming connections, including those in the list of allowed programs**". Click **OK**.



Melakukan Scanning komputer Target

21. Pada komputer **Scanner Machine** (Backtrack), buka terminal ketikan "**nmapfe**" kemudian tekan tombol seperti pada point 10.
22. Pada jendela **Zenmap**, di kotak **Target:**, masukan "**Target IP**" pada langkah 11. Click tombol **Scan**.
23. Nmap menampilkan hasil seperti pada gambar di bawah. Scroll down dan cari pesan "**All 1000 scanned ports … are filtered**", seperti terlihat di gambar berikut.



24. Sekarang semua port tertutup. Firewall ini memberikan seting paling aman, akan tetapi akan mencegah komputer melakukan sharing file dan printer.

Simpan Screen Image

25. Pada **Scanner Machine (Backtrack)**, pastikan jendela Zenmap Nampak, yang memperlihatkan pesan "**All 1000 scanned ports … are filtered**".
26. Tekan tombol **PrintScrn kopikan seluruh** desktop ke clipboard.
27. Simpan dengan nama **NamaKamu_Proj 4b**. Simpan dengan format **JPEG atau PNG**.

Kumpulkan Hasil Project

28. Kirim melalui elearning project 4a dan 4b.

Catatan:

*Komputer **Scanner** bisa juga menggunakan komputer Windows dengan mendownload dan menginstal aplikasi nmap untuk windows yang bisa didownload di **nmap.com***

Last Modified: 15-10-12