NASKAH SOAL UJIAN TENGAH SEMESTER
Tahun Akademik 2023/2024

Kode MK : KKJA 57 2023-2 **Mata Kuliah : Keamanan Komputer dan Jaringan** **Hari/tanggal : Jumat, 3 Mei 2024** **Waktu : 18.00 – 19.30 WIB** **Prodi : Informatika** **Ruang : Online** **Dosen MK : Nikson Badua Putra, S.ST., M.T.**	Verifikasi Ketua Program Studi **Tifani Nabarian, S.Kom., M.T.I.**

Petunjuk : **(disesuikan dengan ketentuan dosen masing-masing)**

1. Jawablah dengan jelas pada lembar jawaban yang sudah disediakan
2. Jawaban hanya bisa ditulis pada form atau lembar jawaban yang telah disediakan. Bila kurang, bisa memintanya pada Pengawas Ujian. 3. Sifat ujian untuk mata kuliah ini: **Online**

LEMBAR SOAL

1. Jelaskan kegunaan Firewall, dan metode yang dimanfaatkan oleh operasional Firewall.

2. Jelaskan konfigurasi Access Control List (ACL) berikut.

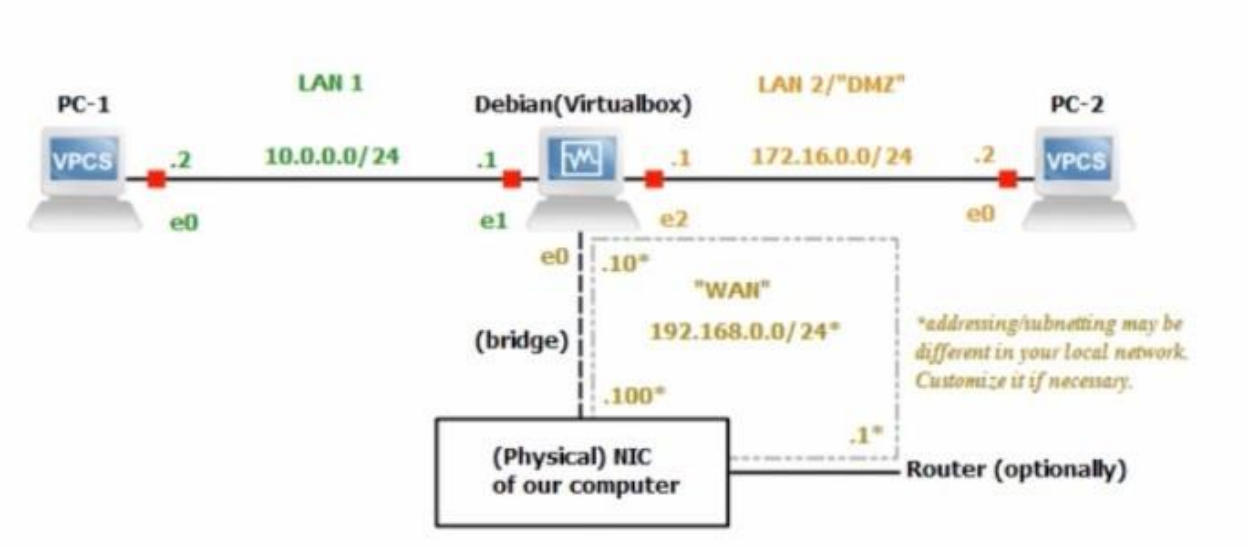
Int addr	Int port	Ext addr	Ext port	Action
*	*	129.63.8.52	*	block
192.63.8.254	110	*	*	allow

3. Jelaskan yang dimaksud dengan “trusted operating system” serta keterkaitannya dengan OS hardening.

4. Jelaskan konfigurasi hardening OS Windows berdasarkan Microsoft Security Baseline Windows 11 v22H2 berikut.

Policy Path	***Policy Setting Name***	***Windows 11***
Account Lockout	Account lockout duration	15

5. Jelaskan langkah – langkah konfigurasi jaringan berikut menggunakan environment GNS3 dna virtual box.



JAWABAN

1. Firewall digunakan untuk mengontrol lalu lintas jaringan antara jaringan yang aman (misalnya, jaringan lokal Anda) dan yang tidak aman (misalnya, Internet). Kegunaan utama dari firewall adalah untuk melindungi jaringan dari serangan yang tidak diinginkan, seperti serangan malware, serangan hacking, dan akses yang tidak sah.
   Metode yang dimanfaatkan oleh operasional firewall antara lain:
   - **Paket Filtering** : Firewall memutuskan apakah membiarkan atau memblokir paket berdasarkan aturan yang ditetapkan, seperti alamat IP, port, dan protokol.
   - **Stateful Inspection** : Firewall memonitor status koneksi jaringan dan memutuskan apakah sebuah paket sesuai dengan koneksi yang ada atau tidak.
   - **Proxy Service** : Firewall bertindak sebagai perantara antara klien dan server, memeriksa dan mengontrol lalu lintas sebelum meneruskannya.
   - **Application Layer Filtering** : Firewall memeriksa isi dari paket data untuk mengidentifikasi aplikasi atau protokol tertentu, dan kemudian mengambil tindakan berdasarkan informasi tersebut.

2. Konfigurasi Access Control List (ACL):
   - ACL adalah daftar aturan yang digunakan untuk mengontrol akses ke sumber daya jaringan berdasarkan berbagai kriteria seperti alamat IP, port, dan protokol.
     Konfigurasi ACL berikut:
     Int addr: Alamat IP internal.
     Int port: Port internal.
     Ext addr: Alamat IP eksternal.
     Ext port: Port eksternal.
     Action: Tindakan yang akan diambil, misalnya, 'block' atau 'allow'.
   - Penjelasan untuk setiap baris :
   - Baris pertama mengizinkan semua koneksi dari alamat IP eksternal 129.63.8.52 untuk semua port eksternal.
   - Baris kedua mengizinkan koneksi dari alamat IP internal 192.63.8.254 pada port internal 110 untuk semua alamat eksternal dan semua port eksternal.

3. Trusted Operating System (OS) dan Keterkaitannya dengan OS Hardening:
   - Trusted Operating System adalah sistem operasi yang telah dirancang dan dikonfigurasi sedemikian rupa sehingga dapat diandalkan untuk menjaga keamanan, integritas, dan ketersediaan data.
   - Keterkaitannya dengan OS hardening adalah bahwa dalam proses hardening, sistem operasi diatur dan dikonfigurasi untuk mengurangi serangan yang mungkin terjadi. Trusted OS menerapkan prinsip-prinsip keamanan yang ketat untuk memastikan bahwa sistem tersebut dapat dipercaya dalam lingkungan yang rentan terhadap serangan.

4. Konfigurasi Hardening OS Windows berdasarkan Microsoft Security Baseline Windows 11 v22H2:
    - Policy Path: Jalur ke pengaturan kebijakan.
    - Policy Setting Name: Nama pengaturan kebijakan.
    - Windows 11: Versi Windows yang terpengaruh.
    - Account Lockout:
      Account lockout duration : Menetapkan durasi waktu (dalam menit) ketika akun akan terkunci setelah sejumlah percobaan gagal masuk yang ditentukan. Dalam kasus ini, akun akan terkunci selama 15 menit setelah serangkaian percobaan masuk yang gagal.

5. Langkah langkah konfigurasi jaringan menggunakan GNS3 dna virtualbox
   Konfigurasi GNS3:
    1. Tambahkan VPCS sebagai PC-1 dan PC-2.
    2. Tambahkan Debian (VirtualBox).
    3. Beri alamat IP 10.0.0.2 untuk PC-1, 172.16.0.2 untuk PC-2, dan 10.0.0.1 serta 192.168.0.100 untuk Debian.
    4. Hubungkan PC-1, PC-2, dan Debian ke LAN 1.
    5. Hubungkan Debian ke LAN 2/DMZ.
    6. Hubungkan PC-2 ke "WAN" (interface Debian yang terhubung ke LAN 1).
    7. Pastikan adapter jaringan VirtualBox Debian terhubung ke jaringan fisik atau adapter GNS3
    8. Uji koneksi antara PC-1, PC-2, dan Debian.