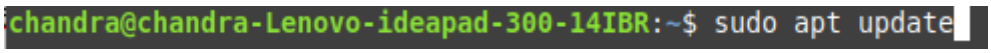
Nama : Chandra ariadi pratama
Kelas : TI411
Tugas Administrasi Jaringan 5

1. Langkah 1: Refresh Software Repositories Buka jendela terminal, dan masukkan yang berikut ini:



Langkah 2: Cara Instal Paket Squid di Ubuntu
Untuk menginstal Squid, jalankan perintah:

perintah untuk masuk ke konfigurasi squid!

File konfigurasi Squid ditemukan di ***/etc/squid/squid.conf***.

1. Buka file ini di editor teks Anda dengan perintah:

```
sudo nano /etc/squid/squid.conf
```

2. Navigasikan untuk menemukan **http_port option**. Biasanya, ini diatur untuk listen on Port 3218. Port ini biasanya membawa lalu lintas TCP. Jika sistem Anda dikonfigurasikan untuk lalu lintas di port lain, ubah di sini.

Anda juga dapat mengatur mode proxy menjadi transparan jika Anda ingin mencegah Squid mengganti request dan response Anda.

Ganti dengan dibawah ini:

http_port 1234 transparent

3. Navigasikan ke pilihan **http_acacess deny all**. Saat ini dikonfigurasi untuk memblokir semua lalu lintas HTTP. Ini berarti tidak ada lalu lintas web yang diizinkan.

Ganti dengan dibawah ini:

http_access allow all

4. Arahkan ke opsi **visible_hostname**. Tambahkan nama yang Anda inginkan ke entri ini. Ini adalah bagaimana server akan muncul kepada siapa pun yang mencoba untuk connect. Slahkan untuk Simpan perubahan (Save Changes) dan keluar (exit).

5. Restart layanan Squid dengan memasukkan:

```
sudo systemctl restart squid
```

2. Jenis serangan Hacker :

- Malware
  Jenis serangan hacker pertama adalah Malware. Malware merupakan sebutan untuk berbagai perangkat lunak berbahaya termasuk di dalamnya virus dan ransomware. Ketika masuk ke perangkat kalian, malware ini dapat melakukan berbagai hal seperti mengambil alih sistem perangkat kalian, membaca aktivitas kalian selama menggunakan perangkat tersebut dan bahkan mencuri data kalian.

- Phishing
  Phishing merupakan jenis serangan cyber yang bertujuan untuk memperoleh berbagai informasi penting dan sensitif seperti username, password, PIN dan sebagainya. Umumnya phishing ini dilakukan melalui layanan surat elektronik atau email yang di dalamnya terdapat attachment.

- DoS (Denial of Service)
  DoS atau Denial of Service merupakan serangan cyber yang dilakukan dengan cara mencegah pengguna mendapatkan akses ke suatu situs yang ingin dikunjungi dengan cara menganggu server situs tersebut. Untuk menganggu suatu server, para penyerang akan membanjiri situs tersebut dengan request dari banyak sekali komputer sehingga server tidak mampu menampung request baru lagi.

3. Sebutkan jenis – jenis IDS NIDS (Network Intrusion Detection System)

- SignatureBased
  IDS yang berbasis pada signature akan melakukan pengawasan terhadap paket-paket dalam jaringan dan melakukan pembandingan terhadap paket-paket tersebut dengan basis data signature yang dimiliki oleh sistem IDS ini atau atribut yang dimiliki oleh percobaan serangan yang pernah diketahui.

- AnomalyBased
  IDS jenis ini akan mengawasi traffic dalam jaringan dan melakukan perbandingan traffic yang terjadi dengan rata-rata traffic yang ada (stabil). Sistem akan melakukan identifikasi apa yang dimaksud dengan jaringan “normal” dalam jaringan tersebut, berapa banyak bandwidth yang biasanya digunakan di jaringan tersebut, protolkol apa yang digunakan, port-port dan alat-alat apa saja yang biasanya saling berhubungan satu sama lain didalam jaringan tersebut, dan memberi peringatan kepada administrator ketika dideteksi ada yang tidak normal, atau secara signifikan berbeda dari kebiasaan yang ada.

- PassiveIDS
  IDS jenis ini hanya berfungsi sebagai pendeteksi dan pemberi peringatan. Ketika traffic yang mencurigakan atau membahayakan terdeteksi oleh IDS maka IDS akan membangkitkan sistem pemberi peringatan yang dimiliki dan dikirimkan ke administrator atau user dan selanjutnya terserah kepada administrator apa tindakan yang akan dilakukan terhadap hasil laporan IDS.

- ReactiveIDS
  IDS jenis ini tidak hanya melakukan deteksi terhadap traffic yang mencurigakan dan membahayakan kemudian memberi peringatan kepada administrator tetapi juga mengambil tindakan proaktif untuk merespon terhadap serangan yang ada. Biasanya dengan melakukan pemblokiran terhadap traffic jaringan selanjutnya dari alamat IP sumber atau user jika alamat IP sumber atau user tersebut mencoba melakukan serangan lagi terhadap sistem jaringan di waktu selanjutnya.

4. Fungsi dari firewall

- Mengatur dan Mengontrol Lalu Lintas Jaringan
  Fungsi pertama yang dapat dilakukan oleh firewall adalah firewall harus dapat mengatur dan mengontrol lalu lintas jaringan yang diizinkan untuk mengakses jaringan privat atau komputer yang dilindungi oleh firewall. Firewall melakukan hal yang demikian, dengan melakukan inspeksi terhadap paket-paket dan memantau koneksi yang sedang dibuat, lalu melakukan penapisan (filtering) terhadap koneksi berdasarkan hasil inspeksi paket dan koneksi tersebut.

- Melindungi data
  Layaknya sistem keamanan jaringan pada umumnya, Firewall menjadi pelindung data-data internal yang Anda miliki agar tidak diakses oleh pihak lain, seperti hacker dan pengguna asing lainnya. Tanpa adanya firewall, data penting dan sensitif yang Anda miliki sangat rawan dicuri dan disalahgunakan. Anda tentu tidak ingin hal ini terjadi bukan?.

- Memblokir konten berbahaya
  Firewall juga berguna untuk memblokir konten-konten dari website yang tidak terpercaya. Anda bisa mengaturnya sendiri terkait konten-konten yang Anda izinkan untuk diakses. Secara default, Firewall akan membatasi akses ke situs download file ilegal yang memang sangat dibutuhkan banyak orang. Sementara dari segi pemerintah, firewall dimanfaatkan untuk memblokir akses situs-situs judi seperti Binomo, situs judi, hingga membatasi akses layanan netflix.

- Untuk memonitor bandwidth
  Bandwidth merupakan besaran transfer data yang dilakukan antara komputer client dengan komputer server dalam waktu tertentu. Dengan menggunakan firewall, Anda bisa membatasi penggunaan bandwidth untuk hal-hal tertentu dan memprioritaskan untuk konten lainnya.

5. Arsitekstrur firewall

1. Arsitektur dual-homed host
Arsitektur ini dibuat di sekitar komputer dual-homed host, yaitu komputer yang memiliki paling sedikit dua interface jaringan. Untuk mengimplementasikan tipe arsitektur dual-homed host, fungsi router pada host ini di non-aktifkan. Sistem di dalam firewall dapat berkomunikasi dengan dual-homed host dan sistem di luar firewall dapat berkomunikasi dengan dual-homed host, tetapi kedua sistem ini tidak dapat berkomunikasi secara langsung.

2. Arsitektur screened host
Arsitektur ini menyediakan service dari sebuah host pada jaringan internal dengan menggunakan router yang terpisah. Pengamanan pada arsitektur ini dilakukan dengan menggunakan paket filtering.

Tiap sistem eksternal yang mencoba untuk mengakses sistem internal harus berhubungan dengan bastion host. Bastion host diperlukan untuk tingkat keamanan yang tinggi. Bastion host berada dalam jaringan internal.

3. Arsitektur screened subnet

Arsitektur screened subnet menambahkan sebuah layer pengaman tambahan pada arsitektur screened host, yaitu dengan menambahkan sebuah jaringan parameter yang lebih mengisolasi jaringan internal dari jaringan internet.

Jaringan perimeter mengisolasi bastion host sehingga tidak langsung terhubung ke jaringan internal. Arsitektur ini yang paling sederhana memiliki dua buah screening router, yang masing-masing terhubung ke jaringan parameter. Router pertama terletak di antara jaringan parameter dan jaringan internal, dan router kedua terletak diantara jaringan parameter dan jaringan eksternal (biasanya internet).