Nama : Gunawan Praasetyo

Kelas : TI411

Tugas Administrasi Jaringan 5

1. **Tuliskan perintah untuk install proxy server dengan Squid**

#### Langkah 1: Refresh Software Repositories

Pastikan Anda bekerja dengan versi software terbaru yang tersedia.

Buka jendela terminal, dan masukkan yang berikut ini:

*sudo apt-get update*

#### Langkah 2: Cara Instal Paket Squid di Ubuntu

Untuk menginstal Squid, jalankan perintah:

*sudo apt-get install squid*

#### 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*

1. **Sebutkan tipe serangan yang bisa dilakukan oleh penyerang(Hacker)**

**DDoS** **Attack** (Distributed-Denial-of-Service Attack) adalah serangan yang dilakukan secara bertubi-tubi ke target korban. Serangan ini bisa berupa ping, atau permintaan koneksi.

Efek dari DDoS Attack adalah server menjadi overload dan tidak bisa diakses. Bagaimana tidak, pengunjung atau visitor asli jadi terhambat karena ada serangan tersebut. Resource akan naik dan mencapai limit server.

**Brute Force Attack** adalah serangan yang dilakukan dengan cara melakukan request secara bertubi-tubi ke website. Serangan ini biasanya upaya login secara berulang-ulang menggunakan username dan password yang dicocokkan satu per satu berupa wordlist.

Efek Brute Force Attack yaitu jika username dan password kamu ditebak dengan mudah, penyerang dapat segera mengakses dashboard admin website.

**Bug CMS/Framework** adalah serangan eksploitasi bug atau celah pada CMS/Framework oleh peretas. Serangan bug ini bisa diperbaiki dengan cara meng-update CMS atau Framework yang digunakan, dengan begitu hacker tidak mendapatkan pintu untuk melakukan atau mengeksekusi celah tersebut.

**Inject Malware**adalah serangan yang memungkinkan peretas (hacker) mengeksekusi script malware yang disisipi pada salah satu file yang kamu unggah ke website.

Biasanya inject malware terjadi karena kamu menggunakan plugin atau nulled theme (gratis) atau bajakan yang di-download dari website tidak resmi.

**Email Spamming** adalah serangan yang memungkinkan peretas melakukan pengiriman email secara bertubi-tubi, email spamming bisa berupa pengiriman email keluar (outgoing email) atau penerimaan email (incoming email). Hal ini bisa sangat mengganggu email website hingga reputasi website-mu.

1. **Sebutkan jenis – jenis IDS**

### **NIDS (Network Intrusion Detection System)**

IDS jenis ini ditempatkan disebuah tempat/ titik yang strategis atau sebuah titik didalam sebuah jaringan untuk melakukan pengawasan terhadap traffic yang menuju dan berasal dari semua alat-alat (devices) dalam jaringan. Idealnya semua traffic yang berasal dari luar dan dalam jaringan di lakukan di scan, namun cara ini dapat menyebabkan bottleneck yang mengganggu kecepatan akses di seluruh jaringan.

### **HIDS (Host Intrusion Detection System)**

IDS jenis ini berjalan pada host yang berdiri sendiri atau perlengkapan dalam sebuah jaringan. Sebuah HIDS melakukan pengawasan terhadap paket-paket yang berasal dari dalam maupun dari luar hanya pada satu alat saja dan kemudian memberi peringatan kepada user atau administrator sistem jaringan akan adanya kegiatankegiatan yang mencurigakan yang terdeteksi oleh HIDS.

### **Signature Based**

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.

### **Anomaly Based**

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.

### **Passive IDS**

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.

### **Reactive IDS**

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.

### **Implementasi IDS**

Salah satu contoh penerapan IDS di dunia nyata adalah dengan menerapkan sistem IDS yang bersifat open source dan gratis. Contohnya SNORT. Aplikasi Snort tersedia dalam beberapa macam platform dan sistem operasi termasuk Linux dan Window$. Snort memiliki banyak pemakai di jaringan karena selain gratis, Snort juga dilengkapi dengan support system di internet sehingga dapat dilakukan updating signature terhadap Snort yang ada sehingga dapat melakukan deteksi terhadap jenis serangan terbaru di internet.

1. **Fungsi dari firewall**

### **1.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?

### **2.Mencegah munculnya pesan yang tidak diinginkan**

Dengan adanya firewall, pesan-pesan yang tidak diinginkan dan terkesan mengganggu tidak akan muncul lagi di layar komputer Anda. Misalnya saja pesan yang mengatakan bahwa komputer Anda sedang dalam bahaya dan Anda diminta untuk memasang aplikasi tertentu saat itu juga.

Ingat, jangan mudah percaya dengan notifikasi mencurigakan seperti ini, karena sangat rawan disusupi oleh backdor atau malware yang bisa merekam segala aktivitas Anda di dunia maya.

### **3.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.

### **4.Bermain game online jadi lebih aman**

Kehadiran firewall juga membuat permainan game online menjadi lebih aman. Selama bermain game online, ada banyak pertukaran data yang terjadi begitu cepat. Agar terjamin keamanannya, Anda sebaiknya menggunakan firewall agar tidak ada malware yang menyusup ke komputer.

Ingat, potensi kejahatan tidak hanya terjadi pada situs-situs keuangan atau download saja tetapi bisa juga menyebar melalui game online atau bahkan sosial media.

### **5.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.

### **6.Untuk mengakses VPN**

VPN merupakan singkatan dari **Virtual Private Network**. VPN biasa digunakan untuk mengakses konten yang diblokir oleh pihak tertentu. Di Indonesia misalnya, jika kita menggunakan jaringan internet plat merah alias yang ada di bawah kendali BUMN, maka kita otomatis harus nurut dengan kebijakan seperti tidak bisa mengakses Netflix, Vimeo, dan lain sebagainya. Namun, Firewall memungkinkan Anda untuk menikmati layanan ini dengan mengaktifkan VPN.

1. **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).