**Instalasi Persiapan Lingkungan Praktikum**

**Instruksi installasi snort versi 2.xx di kali linux**

1. Buat file bernama "bullseye.list" di dalam direktori /etc/apt/sources.list.d/misal:

nano /etc/apt/sources.list.d/bullseye.list

|  |
| --- |
| sudo nano /etc/apt/sources.list.d/bullseye.list |

1. Tambahkan baris berikut ke dalam file tersebut:

deb http://deb.debian.org/debian bullseye main contrib non-free

|  |
| --- |
|  |

1. Jalankan:

sudo apt update

sudo apt install -t bullseye snort

|  |
| --- |
| sudo apt update    sudo apt install -t bullseye snort |

**Praktik Penggunaan Snort**

Berikut merupakan langkah-langkah yang perlu dilakukan dalam menyelesaikan praktikum:

1. Bukalah file pada /etc/snort/snort.conf dengan text editor favoritmu dan perhatikan konfigurasi tersebut serta jelaskan bagian rule dan network:

|  |
| --- |
| Rule    Network    Network: Ini adalah bagian yang mendefinisikan konfigurasi jaringan yang terkait dengan operasi Snort. Ini mencakup informasi seperti antarmuka jaringan yang digunakan untuk mendengarkan lalu lintas jaringan, subnet yang diawasi, dan konfigurasi alamat IP serta port untuk memfilter dan memantau.  Rule: Ini adalah bagian yang mendefinisikan aturan deteksi yang digunakan oleh Snort. Setiap aturan terdiri dari serangkaian kondisi atau pola yang jika terpenuhi, akan menghasilkan tindakan yang telah ditentukan. Aturan ini digunakan untuk mendeteksi aktivitas jaringan yang mencurigakan atau berpotensi berbahaya. Contoh aturan bisa berupa pola-pola spesifik dalam paket jaringan, seperti string yang muncul, alamat IP sumber atau tujuan, port, dan sebagainya.  Dalam konfigurasi snort.conf, kedua bagian ini akan menentukan bagaimana Snort akan memonitor dan merespons lalu lintas jaringan yang masuk. Hal ini memungkinkan Snort untuk berfungsi sebagai sistem deteksi intrusi (IDS) atau sebagai pencegah intrusi (IPS), tergantung pada konfigurasi dan pengaturan yang telah ditentukan. |

1. Kembali ke terminal dan jalankan command berikut untuk sniffing menggunakan snort:

sudo snort -v -d -e -i <network card yang ingin di cek>

Setelah itu, jalankan nmap untuk melakukan scanning pada ip address Anda

|  |
| --- |
| * -v: Opsi ini mengaktifkan mode verbose atau rinci. Ini akan menampilkan lebih banyak informasi selama eksekusi, seperti aturan yang dipicu, statistik lalu lintas, dan lainnya. * -d: Opsi ini mengaktifkan mode deteksi. Ini akan membuat Snort memproses dan mendeteksi lalu lintas jaringan yang diterima dari antarmuka yang ditentukan. * -e: Opsi ini memaksa Snort untuk menampilkan konten data paket jaringan dalam outputnya. Ini berguna untuk melihat isi paket secara langsung, yang dapat membantu dalam analisis deteksi. * -i <network card>: Opsi ini menentukan antarmuka jaringan yang akan digunakan oleh Snort untuk menangkap lalu lintas. Kita harus menentukan nama antarmuka jaringan (misalnya, eth0 untuk Ethernet) yang ingin gunakan untuk memantau lalu lintas.   Setelah menjalankan perintah Snort diatas, ketika menjalankan nmap untuk melakukan pemindaian pada alamat IP , Snort akan memulai pemantauan dan mendeteksi lalu lintas jaringan yang masuk sesuai dengan aturan yang dikonfigurasi  Outputnya akan berisi informasi tentang paket yang ditangkap, aturan yang dipicu, dan detil-detil lainnya sesuai dengan opsi yang digunakan (termasuk mode verbose dan mode deteksi). Selain itu, karena menggunakan opsi -e, juga akan menampilkan konten data dari paket jaringan dalam outputnya. |

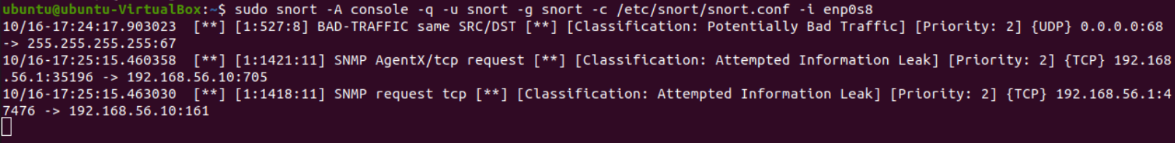
1. Hentikan snort dan jalankan command snort dibawah ini untuk mode packet logger:

sudo snort -dev -l ./log -b -i <network card yang ingin dicek>

Setelah itu, jalankan nmap untuk melakukan scanning pada ip address

|  |
| --- |
|  |

1. Jalankan command berikut untuk menjalankan snort dengan IDS mode:



sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i <network yang ingin dicek>

Setelah itu, jalankan nmap untuk melakukan scanning pada ip address Anda

|  |
| --- |
| -A console: Menetapkan output log ke konsol, sehingga pesan log dan peringatan ditampilkan langsung di terminal tempat Anda menjalankan Snort.  -q: Mode diam atau quiet. Ini mengurangi output yang dihasilkan oleh Snort, sehingga hanya pesan penting yang ditampilkan.  -u snort: Menetapkan pengguna yang akan dijalankan oleh Snort. Di sini, Snort akan dijalankan sebagai pengguna "snort".  -g snort: Menetapkan grup yang akan dijalankan oleh Snort. Dalam hal ini, Snort akan dijalankan dalam grup "snort".  -c /etc/snort/snort.conf: Menetapkan lokasi dan nama file konfigurasi Snort yang akan digunakan oleh Snort. Dalam kasus ini, konfigurasi Snort ditempatkan di /etc/snort/snort.conf.  -i <network yang ingin dicek>: Menetapkan antarmuka jaringan yang akan digunakan oleh Snort untuk mendengarkan lalu lintas jaringan. Anda harus menentukan nama antarmuka jaringan yang ingin Anda gunakan untuk memantau lalu lintas.  Sementara itu, perintah sudo nmap -sS <ip> menggunakan Nmap dengan opsi -sS untuk melakukan TCP SYN scan terhadap alamat IP yang ditentukan. Munculnya pesan "Attempted Information Leak" bisa disebabkan oleh hasil Nmap yang dianggap sebagai upaya untuk mencoba mendapatkan informasi rahasia atau sensitif. Dalam konteks keamanan, beberapa alat pemindaian seperti Nmap bisa dianggap sebagai alat potensial untuk mencoba mencari lubang keamanan atau mengumpulkan informasi tentang jaringan target. |

**Kesimpulan**

Pada bagian ini, tulislah kesimpulan apa saja yang didapat dari hasil melaksanakan

kegiatan-kegiatan pada bab ini.

|  |
| --- |
| File snort.conf digunakan untuk menentukan konfigurasi Snort seperti bagian "network" dan bagian "rule".  Bagian "network" mendefinisikan konfigurasi jaringan yang terkait dengan operasi Snort. Ini mencakup informasi seperti antarmuka jaringan yang digunakan untuk mendengarkan lalu lintas jaringan, subnet yang diawasi, dan konfigurasi alamat IP serta port untuk memfilter dan memantau.  Sementara itu, bagian "rule" mendefinisikan aturan deteksi yang digunakan oleh Snort. Setiap aturan terdiri dari serangkaian kondisi atau pola yang, jika terpenuhi, akan menghasilkan tindakan yang telah ditentukan. Aturan ini digunakan untuk mendeteksi aktivitas jaringan yang mencurigakan atau berpotensi berbahaya.  Kedua bagian ini menentukan bagaimana Snort akan memonitor dan merespons lalu lintas jaringan yang masuk. Ini memungkinkan Snort untuk berfungsi sebagai sistem deteksi intrusi (IDS) atau sebagai pencegah intrusi (IPS), tergantung pada konfigurasi dan pengaturan yang telah ditentukan.  Ketika menjalankan perintah Snort dengan opsi -v -d -e -i, Snort akan memulai pemantauan dan mendeteksi lalu lintas jaringan sesuai dengan aturan yang dikonfigurasi. Outputnya akan menampilkan informasi tentang paket yang ditangkap, aturan yang dipicu, dan konten data paket jaringan. Ketika nmap dijalankan untuk melakukan pemindaian pada alamat IP, Snort akan bereaksi sesuai dengan aturan yang telah ditetapkan, dan pesan log dan peringatan akan ditampilkan di terminal.  Selain itu, perintah Snort dengan opsi -A console -q -u snort -g snort -c /etc/snort/snort.conf -i <network> mengaktifkan mode IDS Snort dengan mengkonfigurasi output log ke konsol. Hal ini memungkinkan pesan log dan peringatan ditampilkan langsung di terminal. Opsi lainnya seperti mode diam (-q), pengguna (-u), grup (-g), lokasi file konfigurasi (-c), dan antarmuka jaringan (-i) juga ditetapkan. Ketika nmap dijalankan untuk melakukan pemindaian pada alamat IP, Snort akan memonitor dan mendeteksi lalu lintas jaringan sesuai dengan aturan yang dikonfigurasi, dan pesan log dan peringatan akan ditampilkan sesuai dengan opsi yang telah ditetapkan. |

**Evaluasi**

* + - 1. Apa perbedaan dan batasan-batasan antara IDS, IPS, dan Firewall?

|  |
| --- |
| Perbedaan dan batasan antara IDS, IPS, dan Firewall adalah sebagai berikut:  Firewall:   * Perbedaan: Bertindak sebagai penghalang antara jaringan internal dan eksternal, melakukan filtering terhadap lalu lintas berdasarkan aturan yang ditetapkan. * Batasan: Cenderung bersifat statis dan terbatas dalam mendeteksi serangan yang kompleks atau intrusi yang terjadi di dalam jaringan.   IDS (Intrusion Detection System):   * Perbedaan: Digunakan untuk mendeteksi dan memberi peringatan tentang aktivitas jaringan yang mencurigakan atau berpotensi berbahaya. * Batasan: Hanya memberikan peringatan tentang serangan yang terdeteksi, tetapi tidak mengambil tindakan langsung untuk mencegahnya.   IPS (Intrusion Prevention System):   * Perbedaan: Memperluas fungsionalitas IDS dengan tidak hanya mendeteksi serangan, tetapi juga mengambil tindakan preventif untuk mencegah serangan mencapai target. * Batasan: Implementasi yang tidak hati-hati dapat menyebabkan false positive atau false negative yang dapat mengganggu kinerja jaringan atau melewatkan serangan yang sebenarnya. |

* + - 1. Buatlah konfigurasi Snort IPS menggunakan DAQ AFPacket. Salah satu contoh konfigurasi snort IPS bisa dilihat di dokumentasi resmi berikut:



|  |
| --- |
| Ubah config Snort:  ## Under Step #2: add the following line config policy\_mode:inline  ## Configure DAQ variables for AFPacket config daq: config daq: afpacket config  daq\_mode: inline  config daq\_var: buffer\_size\_mb=1024 |