ANALISIS KELAYAKAN JARINGAN KOMPUTER MENGGUNAKAN *ALAT SNIFFING* DAN *INTRUSION DETECTION SYSTEM* (IDS) (STUDI KASUS : FITRIA_HOTSPOT)

Nurmi Santi, Yudi Mulyanto
Informatika, Universitas Teknologi Sumbawa
nurmisanti7@gmail.com, yudi.mulyanto@uts.ac.id.

ABSTRAK

Keamanan jaringan komputer sebagai dari sebuah sistem informauh sangat penting untuk menjaga *validitas* dan *integritas* data serta menjamin ketersediaan layanan bagi penggunanya. Sebuah keamanan harus dapat dilindungi dari berbagai macam serangan dan beberapa usaha-usaha penyerangan oleh pihak yang tidak bertanggung jawab atau yang tidak berhak dalam mengakses sebuah internet. Fitriah_Hostpot saat ini sering menggalami gangguan dan banyaknya keluhan seperti penurunan peforma jaringan internet yang selanjutnya berimbas kesemua pengguna jaringan yang terhubung. IDS (*Intrusion Detection System)* yang bertugas melakukan pengawasan terhadap seranggan *Virus, Malicious, Trajon, Worm, DoS, Hacker, Spoofing, Sniffing, Spamming, Crackers* dan lain-lain. Metode penelitian yang digunakan adalah metode *Sniffing* penerapan sistem jaringan, Sehingga dalam melakukan pengujian keamanan jaringan pada penyedia internet khususnya Fitria Hotspot meliputi pengujian keamanan terhadap adanya serangan - serangan jaringan yang tidak bertanggung jawab. Hasil penelitian dapat disimpulkan bahwa *Snort* merupakan sistem yang dapat untuk mendeteksi adanya serangan jaringan atau penyalahgunaan jaringan sehingga diperlukan percobaan dengan melakukan penyerangan terhadap jaringan yang sudah dipasang *snort.*

***Kata Kunci** : Fitriah_Hostpot, Keamanan Jaringan, Sniffing, IDS (Intrusion Detection System), Snort*

1. PENDAHULUAN

Keamanan jaringan komputer sebagai dari sebuah sistem informasih sangat penting untuk menjaga *validitas* dan *integritas* data serta menjamin ketersediaan layanan bagi penggunanya. Sebuah keamanan harus dapat dilindungi dari berbagai macam serangan dan beberapa usaha-usaha penyerangan oleh pihak yang tidak bertanggung jawab atau yang tidak berhak dalam mengakses sebuah internet. Saat ini isu tentang keamanan jaringan menjadi sangat penting dan patut untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan selalu dapat diekploitasi oleh beberapa pihak yang tidak bertanggung jawab, baik itu WLAN maupun wired LAN. [1]

Keamanan jaringan menjadi sangat penting untuk diperhatikan, jaringan yang terhubung dengan internet pada dasarnya tidak aman dan dapat diekploitasi oleh para *hacker,* baik pada jaringan kabel maupun nirkabel. Keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer[2][3]

Fitriah_Hostpot merupakan perusahaan yang menyediakan layanan internet di sebuah desa yaitu di desa simu, fitriah_Hostpot beropersi dari bulan desember sampai dengan sekarang. Berdasarkan hasil wawancara dengan ibu Fitriah selaku pemilik usaha tersebut menggatakan bahwa layanan internet yang dibangun sangat bermanfaat bagi pengguna layanan tersebut. Akan tetapi beliau juga mengatakan bahwa layanan internetnya sering mengalami ganguan, dan sering terjadi penyerangan terhadap jaringan tersebut.

Oleh karena solusi yang bisa di gunakan adalah dengan mengembangkan system keamanan yang lebih kuatuntuk mengatasi adanya serangan-serangan dari luar baik dari keamanan jaringan,,keamanan data yang tesedia. sehingga data-data tersebut tetap aman. dengan menggunakan Alat *Sniffing* Dan *Intrusion Detection System* (IDS)

2. TINJAUAN PUSTAKA

2.1. Intrusion Detection System (IDS)

Sistem deteksi intrusi (IDS) adalah sistem yang memantau lalu lintas jaringan dan memantau sistem jaringan untuk aktivitas yang mencurigakan. Ketika IDS mendeteksi aktivitas mencurigakan yang terkait dengan koneksi jaringan, IDS memperingatkan administrator sistem atau jaringan [4]

Intrusion Detection System (IDS) merupakan sebuah sistem yang digunakan untuk melakukan deteksi adanya usaha-usaha penyusupan terhadap sebuah sistem dengan melakukan pengamatan trafik secara real-time [5]

2.2. Snort

Snort merupakan sebuah aplikasi atau *tool security* berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyusupan, penyerangan, pemindaian, dan beragam bentuk ancaman lainnya), sekaligus juga melakukan pencegahan [6]

2.3. Keamanan Jaringan

Keamanan dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan. Segi-segi keamanan didefinisikan lima poin, yaitu *Confidentiality,* Mensyaratkan bahwa informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang, Integrity, Mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang, *Availability,* Mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan*, Authentication,* Mensyaratkan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu, *Nonrepudiation,* Mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan [7]

2.4. Sniffing

Sniffing adalah bentuk kejahatan dunia maya dimana penjahat secara sengaja atau tidak sengaja mencuri *username* dan *password* orang lain, penjahat kemudian dapat menggunakan akun korban untuk melakukan penipuan atas nama korban atau memusnahkan atau menghapus data korban. Ini sering dilakukan dengan program *sniffer* yang bertindak sebagai penganalisa jaringan dan memonitor jaringan komputer. Program ini memungkinkan kartu jaringan (LAN *card*) untuk mengontrol penolakan semua paket data di jaringan, terlepas dari paket data mana yang telah melintasi jaringan dan kepada siapa paket data tersebut dikirimkan [8]

2.5. Wireshark

Wireshark merupakan salah satu *network analysis tool*, atau *packet sniffer. Wireshark* juga dapat menganalisis paket data secara *real time*. Artinya aplikasi *wireshark* ini akan mengawasi semua paket data yang keluar masuk melalui antar muka yang telah di tentukan oleh *user* sebelumnya. *Wireshark* dapat menganalisa paket data secara *real time* artinya, aplikasi *wireshark* akan mengawasi semua paket data yang keluar masuk melalui antarmuka yang telah ditentukan dan selanjutnya menampilkannya [9]

2.6. Ettercap

Ettercap adalah alat untuk analisis protokol jaringan dan audit keamanan. Ia memiliki kemampuan untuk mencegat lalu lintas pada jaringan, menangkap *password*, dan melakukan menguping aktif terhadap protokol umum. Untuk latihan ini saya akan menggunakan ARP untuk mengendus Keracunan LAN untuk password yang menggunakan SSL (*Hotmail, Gmail*, Dan lain-lain). [10]

2.7. Jaringan Komputer

Jaringan komputer adalah sekumpulan "koneksi" antara dua komputer atau lebih yang dihubungkan secara independen oleh media kabel atau nirkabel. Ketika dua komputer dapat bertukar data atau informasi, mereka dikatakan terhubung [11]

3. METODE PENELITIAN

Dalam penelitian yang akan di lakukan untuk pengumpulan data yaitu menggunakan metode mixed methods. *Mixed methods* adalah sebuah metode campuran dari kualitatif dan kuantitatif, sedangkan untuk metode analisis menggunakan *Intrusion Detection System* IDS. Adapun langkah-langkah penelitian sebagai berikut:

3.1. Metode Pengumpulan Data

Metode pengumpulan data yaitu dilakukan untuk memperoleh sebuah informasih yang dibutuhkan dalam rangka mencapai tujuan penelitian. Pengumpulan data yang digunakan dalam penelitian ini yaitu bersifat *mixed methods,* yang terdiri dari :

3.1.1. Wawancara

Pada tahapan ini penulis melakukan pengumpulan data secara langsung dengan pihak terkait. Wawancara dapat dilakukan secara bertatap muka dan tanya jawab secara langsung antara peneliti dengan narasumber, dalam hal ini penulis akan melakun wawancara langsung dengan, pemilik jaringan kompute yang terakses pada Desa Simu.

3.1.2. Observasi

Observasi dilakukan dengan cara pengamatan untuk dapat menentukan kebutuhan-kebutuhan yang diperlukan dalam melakukan analisis terhadap proses kinerja dari jaringan komputer dengan menggunakan metode *Intrusion Detection System* (IDS). Dalam tahap ini, peneliti melakukan observasi pada objek yang dituju, dimana pada penelitian ini, penulis mengambil data-data penelitian dan gambaran objek secara umum sebagai contoh untuk menganalisis pengoptimalan jaringan**.**

3.1.3. Studi Pustaka

Tahapan selanjutnya yaitu study kepustakaan atau study literature, pengumpulan data dilakukan dengan cara mencari referensi yang relevan menyangkut dengan penelitian yang akan dilakukan, referensi-referensi tersebut diperoleh peneliti dari buku-buku ilmiah, laporan penelitian terdahulu, karangankarangan ilmiah, skripsi, ketetapan ketetapan, buku tahunan, jurnal online dan sumber-sumber tertulis baik tercetak maupun elektronik lain.

Salah satu usaha yang dilakukan oleh peneliti dalam studi pustaka yaitu dengan memanfaatkan internet dimana internet merupakan tempat yang tepat dalam memperoleh data atau informasi dengan

cara membaca berbagai jurnal atau buku-buku yang ada, mencatat, mengkaji ulang, kemudian dituliskan.

3.2. Analisis kebutuhan sistem

Analisis kebutuhan sistem yang akan dibangun dapat dibagi menjadi dua aspek utama: kebutuhan perangkat keras dan kebutuhan perangkat lunak.

a. Kebutuhan perangkat lunak

Software yang digunakan untuk membuat sistem pendukung keputusan ini ditunjukan pada tabel dibawah ini:

Tabel 1 Kebutuhan Perangkat Lunak

No	Perangkat Keras	Keterangan
1	Laptop	Tosiba
2	Processor	Intel Core i3-7020U
3	*RAM*	*4 GB*
4	Smarphone	*Xiomi 5 plus*

b. Kebutuhan perangkat keras

*Hardware*yang dibangun dalam sistem pendukung keputusan ini dicantumkan dalam tabel di bawah ini.

Tabel 2 kebutuhan perangkat lunak

No	Perangkat Lunak	Keterangan
1	Sistem operasi	Kali Linux
2	Memonitoring Jaringan	Wireshark
3	Serangan	Ettercap
4	Mengukur penggunaan jaringan	*Snort*
5	Melakukan pemutusan jaringan secara paksa	*DDOS*

4. HASIL DAN PEMBAHASAN

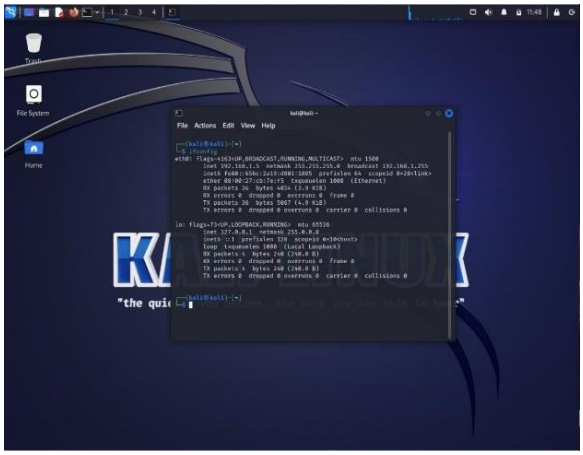
Analisis ini digunakan supaya dapat mengetahui keamanan yang ada di salah satu penyedia internet Fitria Hotspot. Sehingga skenario dalam melakukan pengujian keamanan jaringan pada penyedia internet khususnya Fitria Hotspot meliputi pengujian keamanan terhadap adanya serangan-serangan jaringan yang tidak bertanggung jawab. Dimana dalam melakukan pengujian ini memiliki *ip address* penyerangan dan *ip address client*/korban.

No	IP address penyerang	Ip address client/korban
1	192.168.1.5	192.168.1.0/24 192.168.1.49 192.168.1.16 192.168.1.13 192.168.1.3 192.168.1.6 192.168.1.4 192.168.1.8 192.168.1.18 192.168.1.7

Gambar 2. Tabel *Ip address*

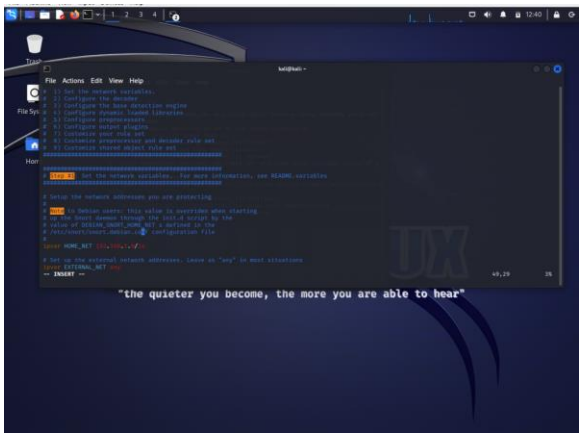
4.1. Analisa Hasil Penelitian

Dalam pengujian ini sebelum melakukan pemasangan *snort* pada sebuah komputer yang terhubung kedalam jaringan penyedia internet Fitria Hotspot, ada beberapa hal yang perlu diperlukan yang pertama *terkait ip address* dari *server,* dari *client* dan jika sudah terhubung dalam satu jaringan fitria hotspot baru dilakukan pemasangan snort pada komputer tersebut. *Snort* merupakan sistem yang dapat untuk mendeteksi adanya serangan jaringan atau penyalahgunaan jaringan sehingga diperlukan percobaan dengan melakukan penyerangan terhadap jaringan yang sudah dipasang *snort.* Pada gambar 2 merupakan tampilan dari ip address korban yang merupakan device *handphone* yang akan digunakan sebagai target penyerangan. Berikut ini gambar 3 merupakan IP *address* jaringan komputer sebagai penyerang:



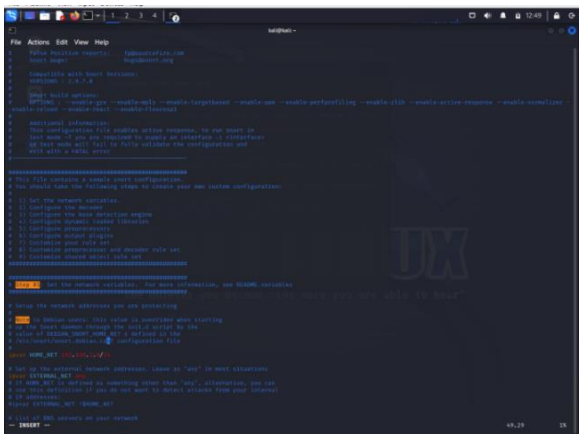
Gambar 3. *IP address* penyerang

Untuk menampilkan *ip address* penyerang pada komputer penyerangan dengan menggunakan sistem operasi kali linux dapat menuliskan *ifconfig* pada terminal sehingga akan memunculkan *ip address* penyerang 192.168.1.5 (penyerang). Sebelum melakukan tahap pengujian ada beberapa hal yang perlu dilakukan dalam pendeteksian *snort* apakah berjalan sesuai dengan harapan diantaranya dengan melakukan pembuatan *rule snort* terkait adanya ancaman supaya dapat terdeteksi oleh *snort*. Selanjutnya konfigurasi *snort* supaya *snort* dapat bekerja sebagai IDS untuk mendekteksi serangan. Dalam konfigurasi *snort* ada hal yang penting perlu untuk dilaksanakan seperti untuk memastikan *ip address client* yang ingin dilindungi pada folder *snort.conf* dan *snort.debian.conf*, sehingga *snort* dapat berjalan mendeteksi jika adanya percobaan penyerangan terhadap *ip client* tersebut.

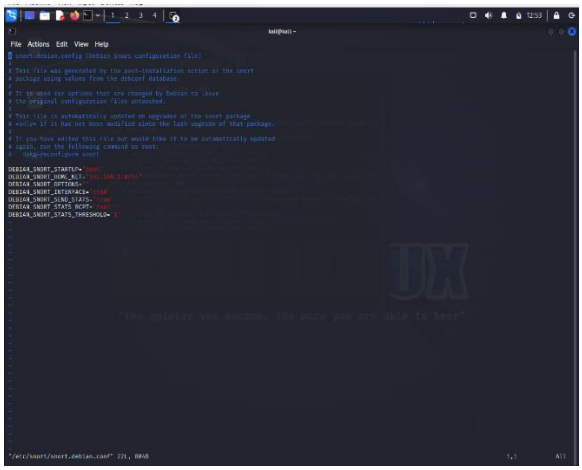


Gambar 4. Tampilan konfigurasi *ip address snort*

Pada gambar 4 diatas dapat dilihat *ip address* yang ingin dilindungi oleh *snort* yang dimana ip nya 192.168.1.0/24. Selanjutnya memilih *rules - rules snort* yang ingin diaktifkan seperti pada gambar 5



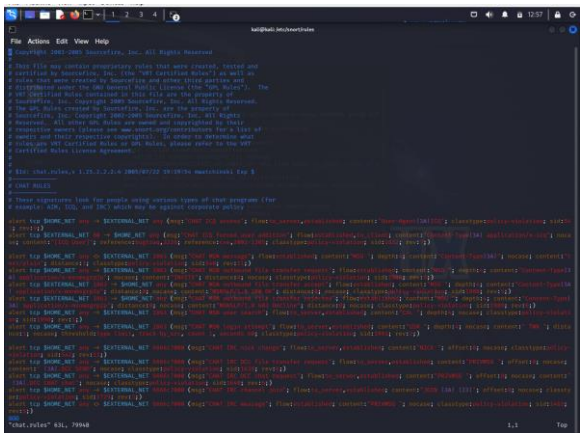
Gambar 5. Konfigurasi memilih pengaktifkan *rule snort*



Gambar 6. Konfigurasi pada folder *snort.debian.conf*

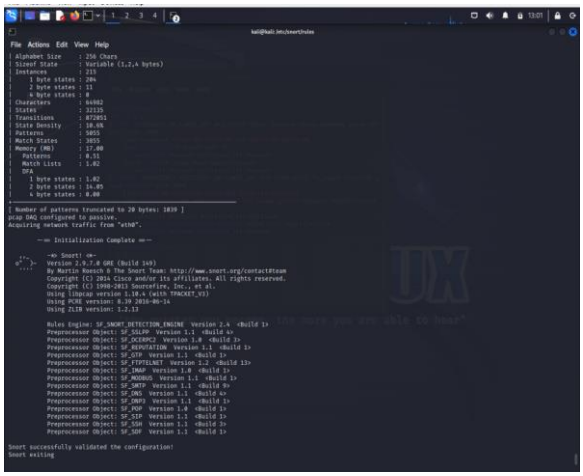
Selanjutnya konfigurasi pada folder *snort.debian.conf* maka langkah selanjutnya membuat rule *snort* supaya *snort* dapat mendeteksi serangan sesuai dengan serangan. Untuk lebih jelas dapat dilihat pada gambar 6

Setelah melakukan konfigurasi pada folder *snort.conf* dan *snort.debian.conf* maka langkah selanjutnya membuat *rule snort* supaya *snort* dapat mendeteksi serangan sesuai dengan serangannya. Untuk lebih jelas dapat dilihat pada gambar 7.



Gambar 7. *rules snort*

Pada gambar 7. diatas merupakan konfigurasi *rule snort* yang supaya *snort* dapat mendeteksi serangan berdasarkan jenis serangannya. setelah melakukan langkah diatas, maka langkah selanjutnya yaitu menjalankan snort dengan menggunakan perintah *sudo snort -T -i eth0 -c /etc/snort/snort.conf.*



Gambar 8. Hasil *compile snort*

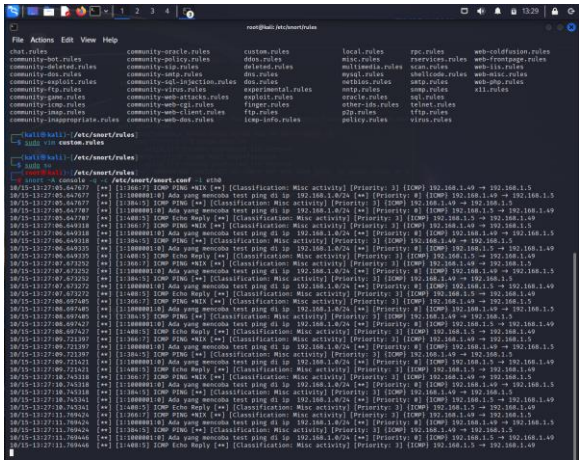
Pada gambar 8 merupakan hasil dari *compile* konfigurasi serta *rules snort* yang telah di *setting* sebelumnya

4.2. Tahapan Pengujian

4.2.1. ICMP (*Internet Control Message Protocol*)

Komputer yang sudah terpasang *snor*t akan mencoba mendeteksi adanya serangan atau aktivitas yang tidak wajar didalam jaringan yang terhubung ke *server.* ICMP merupakan suatu *protocol* yang

bertugas untuk mengirimkan pesan kesahalan dan kondisi lain yang memerlukan perhatian khusus. Berikut gambar 9 ini merupakan tampilan ping dari jaringan penyerang ke jaringan *client*/korban. Maka jika jaringan *client*/korban yang sudah terpasang *snort* maka akan tampil *snort* sebagai pendeteksi (adanya aktivitas ping).

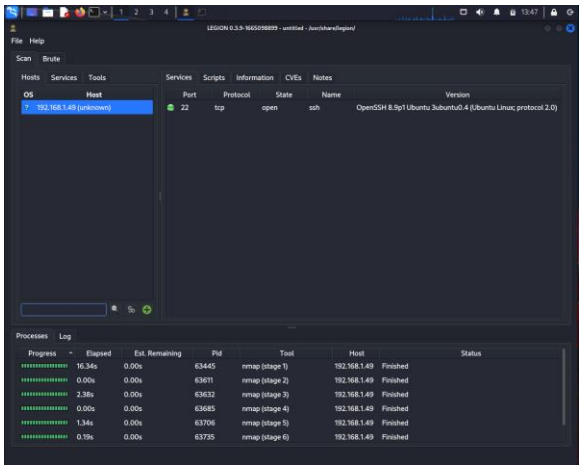


Gambar 9. ping ip address korban dari penyerang

Pada gambar 9 merupakan tampilan *client*/korban yang sudah terpasang *snort* maka akan menampilkan *alert* (peringatan) ada aktivitas ping, yang dimana itu dibuat berdasarkan *rules snort* yang telah dibuat

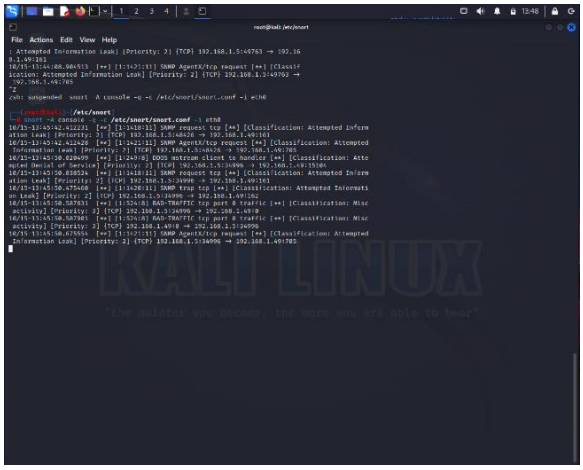
4.2.2. Nmap (*Port Scanning)*

Komputer yang sudah terpasang *snort* akan dicoba untuk melakukan metode penyerangan nmap yaitu serangan dengan *port scanning* dari komputer penyerang. *legion* merupakan sebuah aplikasi atau *tools* yang berguna untuk audit dan eksplorasi suatu keamanan jaringan. Berikut gambar 10 aplikasi nmap pada kali linux (*legion)* untuk melakukan pengujian ke *snort* apakah *snort* dapat membaca serangan nmap:



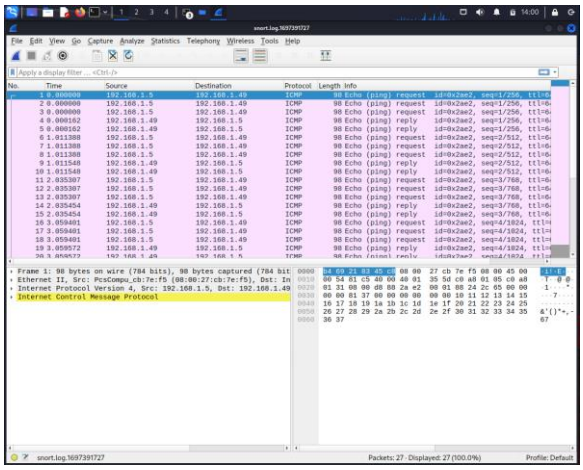
Gambar 10. *port scanning* ke *ip client* dengan menggunakan *legion*

Pada gambar 10 dapat dilihat setelah melakukan *port scanning* ke jaringan *client* maka jaringan *client* memiliki 1 *port* yang terbuka yang dimana *port* 22 tcp. sehingga ini merupakan sebuah celah dimana penyerangan dapat memasuki atau pun lebih mendalami untuk melakukan penyerangan kedalam jaringan. Pada gambar 11 merupakan tampilan komputer client yang terpasang *snort* maka akan mendeteksi adanya serangan atau aktivitas yang tidak wajar didalam jaringan. Sehingga *snor*t akan menampilkan pendeteksi *snort* seperti berikut ini pada gambar 11



Gambar 11. Peringatan *Port Scanning*

Gambar 11 merupakan hasil peringatan kepada komputer *client* bahwa terdapat sebuah serangan menggunakan *port scanning* yang dilakukan oleh komputer penyerang. Untuk melihat *log* hasil *snort* dapat dilihat pada folder /var/log/snort, seperti pada gambar 12

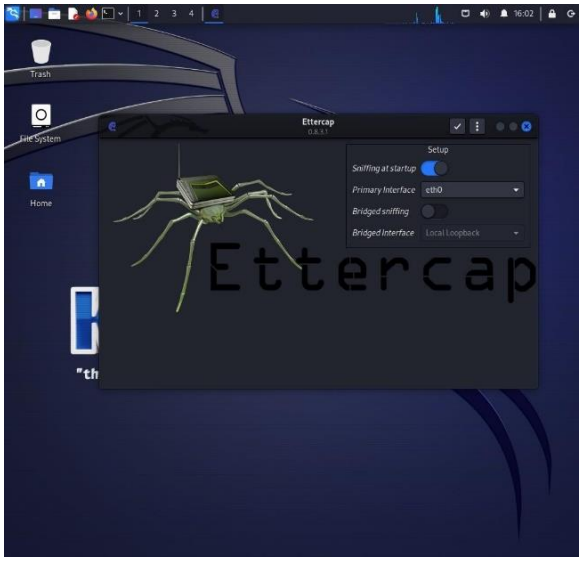


Gambar 12 Hasil Analisa *Snort Log*

Pada gambar 12 merupakan tampilan dari hasil *log snort* yang di buka menggunakan *wireshark.* Sedangkan pada gambar 13 merupakan tampilan *alert telegram* yang telah di konfigurasikan dengan *snort*, yang dimana jika terdapat serangan maka akan muncul *alert botsnort*.

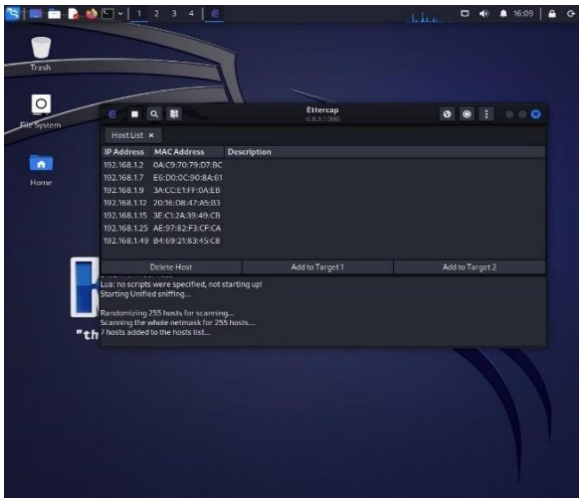
4.2.3. *Ettercap (Penetration Testing)*

Pada tahap ini dilakukan penyerangan pada korban dengan melakukan penyadapan pada paket data. Pengujian ini menggunakan aplikasi *Ettercap* sebagai alat uji. Tampilan *Ettercap* ditunjukan pada gambar 13



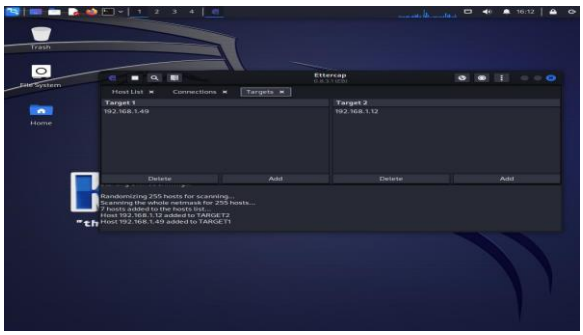
Gambar 13. Tampilan *Ettercap*

Pada tahapan ini sering disebut dengan *Man in The Middle Attack (MITM)* Kondisi awal yang dibutuhkan adalah *device* korban dan penyerang harus terhubung dengan satu jaringan yang sama dalam hal ini adalah Fitria Hotspot. Disini penyerang berperan sebagai pihak ketiga diantara target data *access point* yang menghubungkan antara target dan layanan internet. Pada konfigurasi *ettercap* yang menjadi target pertama adalah *gateway* dari *Access Point* yaitu 192.168.1.1 yang menjadi target kedua yaitu ip dari device korban yaitu 192.168.149. Berikut adalah tampilan saat menambahkan target ip kedalam alat *Ettercap*.



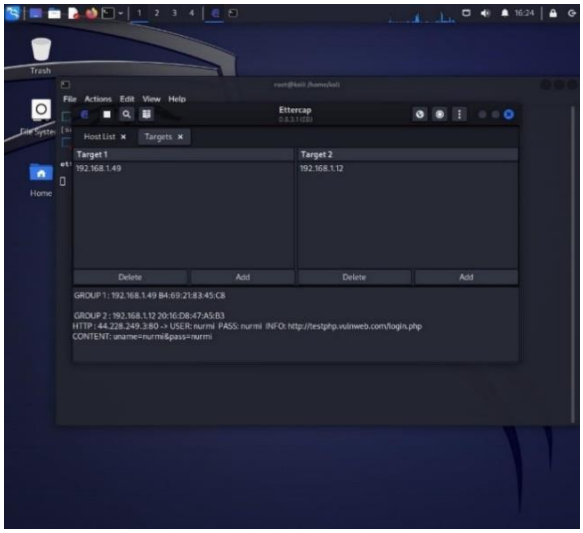
Gambar 14. Tampilan *list host Ettercap*

Pada gambar 14 dapat di perhatikan bahwa terdapat beberapa *list host* yang telah berhasil di *scanning* oleh *ettercap* dan dapat di tambahkan ke target 1 maupun target 2. Berikut adalah tampilan *Ettercap* saat di tambahkan target ip sebagai korban



Gambar 15. Tampilan tambah target *Ettercap*

Tahap selanjutnya yaitu melakukan ARP *Poising. Address Resolution Protocol (ARP)* adalah sebuah *protocol* dalam TCP/IP *Protocol Suite* yang bertanggung jawab dalam melakukan resolusi alamat ip dalam alamat Media *Access Control (MAC Address)*. Setelah itu proses *Snifing* dijalankan, untuk kemudian semacam merekam aktifitas *device* korban pada saat menggunakan internet. Dari percobaan proses *Sniffing* tersebut kemudian berhasil diperoleh proses *Snifing* tersebut kemudian berhasil diperoleh informasi bahwa komputer target mengakses situs *http://testphp.vulnweb.com/* berhasil merekam *user* nurmi serta *password* nurmi seperti yang di tampilkan pada gambar 16



Gambar 16 Tampilan Rekaman *Ettercap*

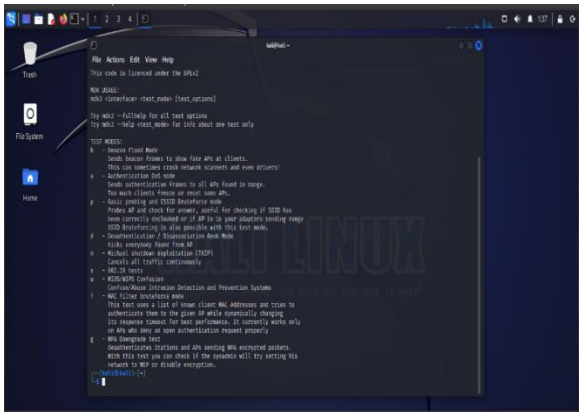
Pada gambar 16 dapat diperhatikan bahwa *ettercap* telah berhasil merekam aktivitas dari *device* korban yang mengakses halaman web http://testphp.vulnweb.com/ dan memasukan username nurmi serta sandi nurmi

Namun pada saat device korban mengakses halaman https://www.facebook.com/ *ettercap* gagal

merekam aktivitas *login* dari *devic*e korban. Setelah dianalisis ditemukan kegagalan dalam dalam proses *sniffing* berasal dari protol yang digunakan oleh *web server,* yaitu https. perbedaan antara *http* dengan *https* adalah *http* bekerja melalui sistem yang tereknsipsi sehingga dalam teori, informasi tidak dapat diakses oleh pihak selain korban dan *server* akhir.

Setelah itu kemudian pada *device* korban dicoba untuk mengkases *facebook* dengan cara mengetikan manual http://www.facebook.com/ pada kolom *url browser* yang digunakan, dalam hal ini *Google Chrome.* Namun hasilnya pada saat proses berjalan pada kolom *url* kembali lagi menjadi *https*.

Jadi dapat disimpulkan bahwa dengan menggunakan metode penyadapan paket atau sering disebut dengan *Man In The Middle Attack (MITM)* hanya berlaku jika korban mengakses *url* tanpa menggunakan *https.*



Gambar 17. *Tampilan MDK3*

Pada gambar 17 merupakan tampilan dari *tools MDK3* yang digunakan untuk melakukan serangan DDOS. Langkah pertama yang dilakukan adalah mengubah mode jaringan menjadi mode monitor dengan menggunakan command di bawah ini.

5. KESIMPULAN

Berdasarkan hasil pengujian pada bab IV penulis menarik kesimpulan bahwa dalam pengujian keamanan jaringan komputer Fitriah_Hostpot, dimana *snort* yang digunakan terbukti dapat melakkan pendeteksian terhadap adanya aktifitas yang tidak wajar, dimana sejumlah serangan kepada *client* terdeteksi setiap 15 menit dan *snort* dapat menerima pemberihuan sebanyak 140667 dan *snort* akan melakukan analisis terhadap paket serangan, sehingga *snort* akan merekam semua penerangan atau ancaman yang adaa pada jaringan komputer, mulai dari ancaman ICMP, TCP,maupun UDP, sehingga hasil dari analisis pada jaringan Fitriah Hostpot

DAFTAR PUSTAKA

[1] Y. Hae and W. Sulistyo, "Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen," vol. 8, no. 4, pp. 2095–2105, 2021.

[2] A. Fergina, M. I. Setia, M. Yusuf, and ..., "Analisis Monitoring Sistem Keamanan Jaringan Komputer menggunakan Software NMAP (Studi Kasus Jaringan di Universitas Nusa Putra)," *... Ilmu Komput. ...*, 2023, [Online]. Available: http://prosiding.sentimeter.nusaputra.ac.id/index.php/prosiding/article/view/45%0Ahttp://prosiding.sentimeter.nusaputra.ac.id/index.php/prosiding/article/download/45/41

[3] Amin Muftiadi, "Studi kasus keamanan jaringan komputer: analisis ancaman phisingterhadap layanan online banking," *Hexatech J. Ilm. Tek.*, vol. 1, no. 2, pp. 60–65, 2022.

[4] M. Aprianto, "Desain Dan Implementasi Intrusion Detection System Menggunakan Debian 7 Dan Snort," *J. Teknol. Pint.*, vol. 3, no. 3, pp. 1–20, 2023.

[5] J. D. Santoso, "Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System," *Infos*, vol. 1, no. 3, pp. 44–50, 2019.

[6] K. Pos, P. Kota, A. N. Ihsana, and A. Maslan, "Jurnal Comasie," vol. 05, 2020.

[7] I. K. N. A. Jaya, I. A. U. Dewi, and G. S. Mahendra, "Implementation of Wireshark Application in Data Security Analysis on LMS Website," *J. Comput. Networks, Archit. High Perform. Comput.*, vol. 4, no. 1, pp. 79–86, 2022, doi: 10.47709/cnahpc.v4i1.1345.

[8] A. Umasugi, M. D. Suratin, and S. Hamza, "Analisis Keamanan Jaringan Wifi Terhadap Packet Sniffing DiKampus a Universitas Muhammadiyah Maluku Utara," *Produktif J. Ilm. Pendidik. Teknol. Inf.* , vol. 6, no. 2, pp. 597–602, 2022, [Online]. Available: https://journal.umtas.ac.id/index.php/produktif/article/view/2460

[9] A. E. Tangkowit, V. R. Palilingan, and O. E. S. Liando, "Analisis Dan Perancangan Jaringan Komputer Di Sekolah Menengah Pertama," *Edutik J. Pendidik. Teknol. Inf. dan Komun.*, vol. 1, no. 1, pp. 69–82, 2021, doi: 10.53682/edutik.v1i1.1044.