SISTEM PENGESAN PENCEROBOHAN BERASASKAN IOT UNTUK RANGKAIAN WIFI DI RUMAH

Muhammad Badrul Amin bin Hilmi
Wan Fariza binti Paizi @ Fauzi

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

WIFI ialah singkatan daripada wireless fidelity bermaksud teknologi penghantaran maklumat tanpa wayar dengan mengakses internet menggunakan isyarat radio. Walaupun teknologi rangkaian tanpa wayar ini mempunyai kebaikan buat pengguna (pemilik WIFI di rumah) tetapi rangkain tanpa wayar ini mudah terdedah kepada serangan kerana ketidakcukupan penggunaan keselamatan dalam rangkaian tanpa wayar. Seterusnya penggunaan WIFI di rumah terdedah juga kepada serangan daripada kawasan sekeliling.

Oleh itu, kajian ini bertujuan untuk membantu pemilik WIFI yang berada di rumah lebih selamat daripada serangan sekeliling. Kaedah yang digunakan adalah dengan membina satu peranti Raspberry PI yang dapat mengesan dan menghalang jaringan WIFI daripada di ceroboh. Di akhir projek ini, masalah tentang ketidakcukupan penggunaan keselamatan dapat ditingkatkan

1 PENGENALAN

Hari ini, penggunaan WIFI dalam kehidupan manusia adalah sangat penting. WIFI adalah teknologi rangkaian tanpa wayar yang membolehkan peranti seperti komputer (komputer riba dan desktop), peranti mudah alih seperti telefon dan peralatan lain bersambung dengan jaringan internet. WIFI membolehkan peranti-peranti ini bertukar maklumat antara satu sama lain. Dengan berlakunya pertukaran maklumat ini wujudnya rangkaian. Penggunaan WIFI mempunyai kebaikan dan kelemahanya yang tersendiri. Dari sudut kelemahan WIFI, ia dapat

di lihat daripada segi keselamatan jaringan WIFI tersebut. Ini disebabkan daripada pengodam ataupun orang yang tidak bertanggungjawab yang tidak pernah berputus-asa untuk untuk memecahkan algoritma keselamatan yang terdapat di dalam keselamatan WIFI. (Cisco.com)

Impak yang terhasil daripada kelemahan keselamatan WIFI menyebabkan banyak jaringan WIFI menjadi tumpuan oleh orang yang cuba mendapatkan jaringan WIFI dengan percuma dan tidak terkecuali ada sesetengah daripada mereka cuba mencuri data peribadi pemilik jaringan WIFI tersebut. Terdapat sumber berita daripada "Newsweek" yang menulis bahawa jutaan rangkaian WIFI di rumah berisiko di godam dengan cara penggodam akan cuba mengakses rangkaian WI-FI, mengakses fail yang dikongsi dan mengakses peranti internet. Penggodam juga akan cuba memasukan virus-virus yang boleh membantu mereka untuk mengakses ke pemilik jaringan WIFI. (Jason Murdock, 2018)

2 PENYATAAN MASALAH

- Pemilik WIFI mengesyaki bahawa kelajuan WIFI lebih lambat berbanding hari-hari sebelumnya. Oleh itu, pemilik ingin mengetahui sama ada orang lain mengaksesnya tanpa kebenaran.
- Pemilik WIFI berasa risau jikalau data peribadinya di guna atau di curi oleh orang yang tidak bertanggungjawab.
- Pemilik jaringan WIFI ingin memastikan keselamatan WIFI dirumahnya berada dalam keadaan baik daripada penggodam.

3 OBJEKTIF KAJIAN

- Untuk membangunkan peranti yang boleh mengamankan WIFI dari orang asing atau penggodam dari akses ke jaringan WI-FI
- Untuk memantau WIFI dari aktiviti yang tidak dikenali yang cuba menyambung ke jaringan WIFI.

4 METOD KAJIAN

Projek ini akan menggunakan “Waterfall Model” kerana ia lebih berfokus kepada kerja projek sebelum projek ini dapat diteruskan kepada fasa-fasa lain. Projek ini harus berfungsi dengan sempurna terlebih dahulu.

4.1 Fasa Perancangan

Untuk fasa ini ialah fasa awal untuk pembangunan peranti pemantauan WI-FI. Pelbagai perkara proses perancangan telah dibuat seperti merancang tajuk. Kemudian dalam fasa ini juga merancang bagaimana untuk membuat projek ini berjaya. Di samping itu, carta ganth juga telah disediakan. Ini melibatkan membuat satu set rancangan untuk membantu dan membimbing melalui projek ini.

4.2 Fasa Analisis Keperluan

Objektif utama dalam fasa ini adalah memahami keperluan dan masalah pemantauan peranti WIFI akan datang. Semua keperluan item telah dipilih untuk digunakan saat mengembangkan alat pemantauan WI-FI

4.3 Fasa Reka Bentuk

Sebelum memulakan sesuatu program, perkara-perkara penting yang perlu dilakukan ialah memahami projek yang perlu dibangunkan dan tahap kebolehoperasian projek apabila dibangunkan sepenuhnya. Semasa fasa ini, konsep projek telah dilukis, bagaimana bahagiannya akan disambungkan antara satu sama lain. Rekabentuk dibina dan lakaran reka bentuk seperti sambungan peranti dengan sistem operasi.

4.4 Fasa Pengujian Dan Implementasi

Tahap pengujian dan pelaksanaan ialah fasa di mana penyediaan projek pemantauan WI-FI selesai dan konfigurasi. Alat pengawasan WI-FI akan diuji untuk memastikan peranti itu boleh

digerakkan seperti mencuba untuk mengakses tanpa kebenaran Pemilik menguji peranti tersebut adakah ia berkesan untuk menghalang daripada akses tanpa kebenaran.

4.5 Fasa Penyelenggaraan

Fasa sokongan adalah fasa terakhir dalam menyelesaikan peranti memantau WI-FI. Semua kertas kerja lengkap dan keseluruhan fungsi akan dibentangkan kepada penasihat projek untuk semakan.

5 HASIL KAJIAN

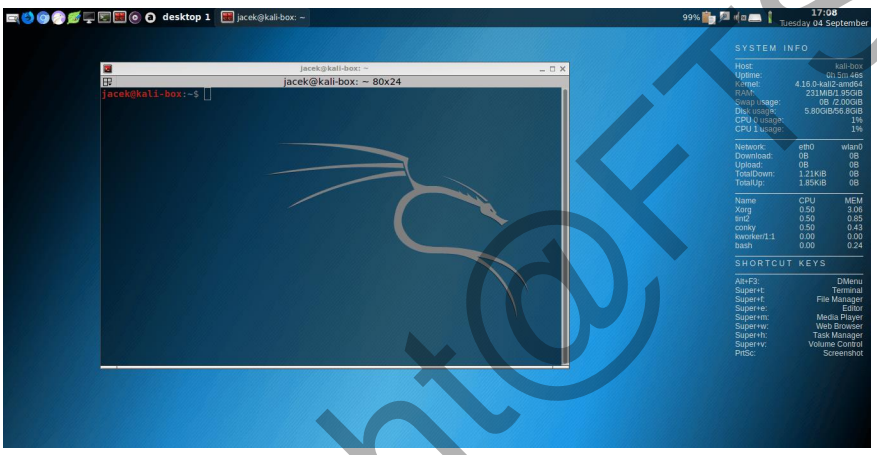
Bahagian ini membincangkan hasil daripada proses pembangunan system pengesan pencerobohan berasaskan IOT untuk rangkaian WIFI di rumah. Perangan yang mendalam tentang projek ini diperihalkan.

5.1 Penggunaan Raspberry Pi

Raspberry Pi hadir dalam saiz sebesar lebih kurang kad pengenalan kita, di mana beberapa komponen utama disertakan bersama-sama dengannya. Raspberry PI dibangunkan untuk memudahkan lebih ramai mempelajari pelbagai perkara berkaitan perkomputeran menggunakannya tanpa mengeluarkan kos yang tinggi. (JomGeek, 2018)

Raspberry hadir dengan beberapa port seperti HDMI (untuk dihubungkan ke monitor atau televisyen), port USB (untuk tetikus dan papan kekunci), dan juga port mikro-SD (untuk ruangan sistem dan fail). Ia hadir dalam dua variasi, iaitu set A dan juga Set B. Perbezaan kedua set ini adalah, Set B untuk Raspberry Pi hadir dengan sokongan port Ethernet yang membolehkan pengguna menghubungkan talian internet melaluinya. Untuk sokongan kuasa, ia menggunakan kabel mikro-USB yang sedia digunakan pada pelbagai peranti mudah-alih hari ini. (JomGeek, 2018)

5.2 PENGGUNAAN OPERASI KALI LINUX



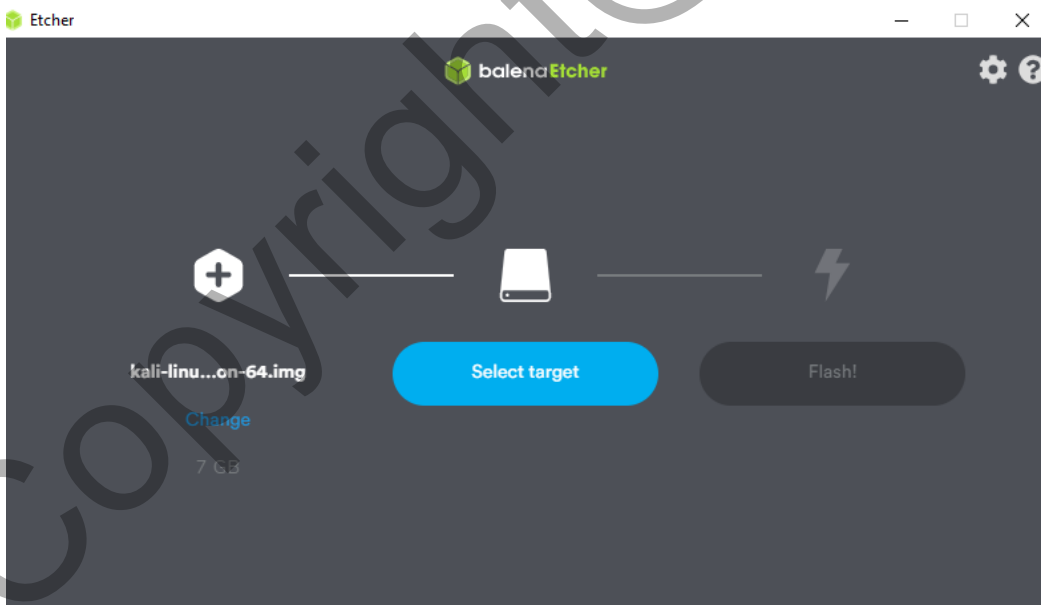
Rajah 3.2: Sistem operasi Kali Linux

Sistem Kali Linux adalah distribusi Linux berbasis Debian yang ditujukan untuk Penetration testing dan Pemeriksaan Keamanan Lanjutan. Sistem Kali Linux berisi beberapa ratus alat yang diarahkan untuk berbagai tugas keamanan informasi, seperti Pengujian Penetrasi, Penelitian Keamanan, Forensik Komputer dan Reversi Engineering. Kali Linux dikembangkan, didanai dan dikelola oleh Offensive Security, sebuah perusahaan pelatihan keamanan informasi terkemuka.

Kali Linux secara khusus disesuaikan dengan kebutuhan para profesional Penetration testing, dan oleh karena itu semua dokumentasi di situs ini mengasumsikan pengetahuan dan keakraban dengan sistem operasi Linux pada umumnya. Silakan lihat Haruskah Saya Menggunakan Kali Linux? Untuk lebih jelasnya tentang apa yang membuat Kali menjadi unik.

5.2.1 PEMASANGAN OPERASI KALI LINUX DI RASPBERRY PI

Pemasangan Operasi Kali Linux ini terlebih dahulu memerlukan perisian Etcher. Perisian Etcher ini berfungsi untuk menjadikan operasi Kali Linux sebagai *ISO Image* dan digunakan ketika proses bootable menggunakan *memory card*. Setelah proses ini selesai, *memory card* di pasang pada Raspberry pi untuk proses *bootable* seperti yang ditunjuk di Rajah 5.2 URL berikut telah dirujuk untuk membuat proses bootable untuk Kali Linux ISO menggunakan Balena Etcher: https://vitux.com/how-to-flash-burn-an-os-image-with-etcher-on-ubuntu/



Rajah 5.3: Kali Linux ISO menggunkan Balena Ethcer

5.3 PENGGUNAAN PERISIAN SNORT

Rajah 3.3: Perisian Snort

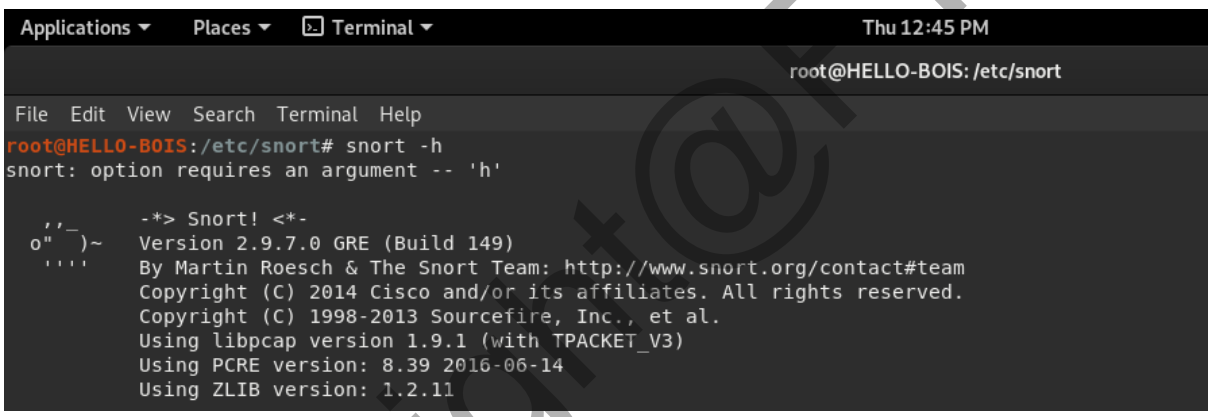
Snort menggunakan bahasa berasaskan peraturan, melaksanakan analisis protokol, pencarian / pencocokan kandungan, dan boleh digunakan untuk mengesan pelbagai serangan dan kuar, seperti limpahan penampan, imbasan port stealth, serangan CGI, probe SMB, percetakan cap jari OS, dan banyak lagi.

Peraturan snort yang terdapat didalamnya seperti mengesan serangan dan aktiviti berniat jahat. Pemilik juga boleh menulis peraturan tertentu seperti amaran, log, menjatuhkan sambungan, dll. Peraturan mempunyai sintaks yang mudah. Juga, pemilik boleh menulis semua peraturan dalam fail konfigurasi dan boleh mengedit apa yang dimahukan oleh sistem lain.

5.3.1 PEMASANGAN PERISIAN SNORT

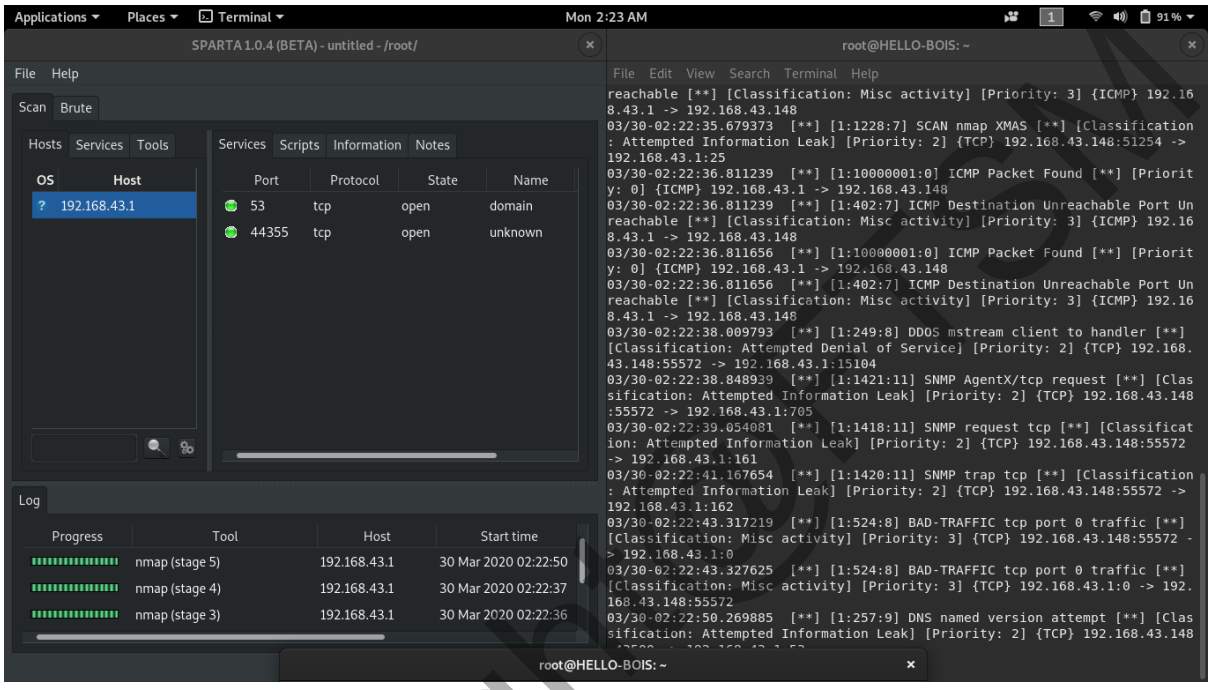
Perisian Snort digunakan untuk mengesan dan memantau pencerobohan keatas jaringan WIFI di rumah. Pemasangan snort di buat menggunakan *Command Line Interface (CLI)* seperti di bawah:

#apt-get install snort



Rajah 5.4 : Perisian Snort digunakan pada Operasi Kali Linux

5.4 AMARAN TERHADAP SERANGAN YANG DI TERIMA

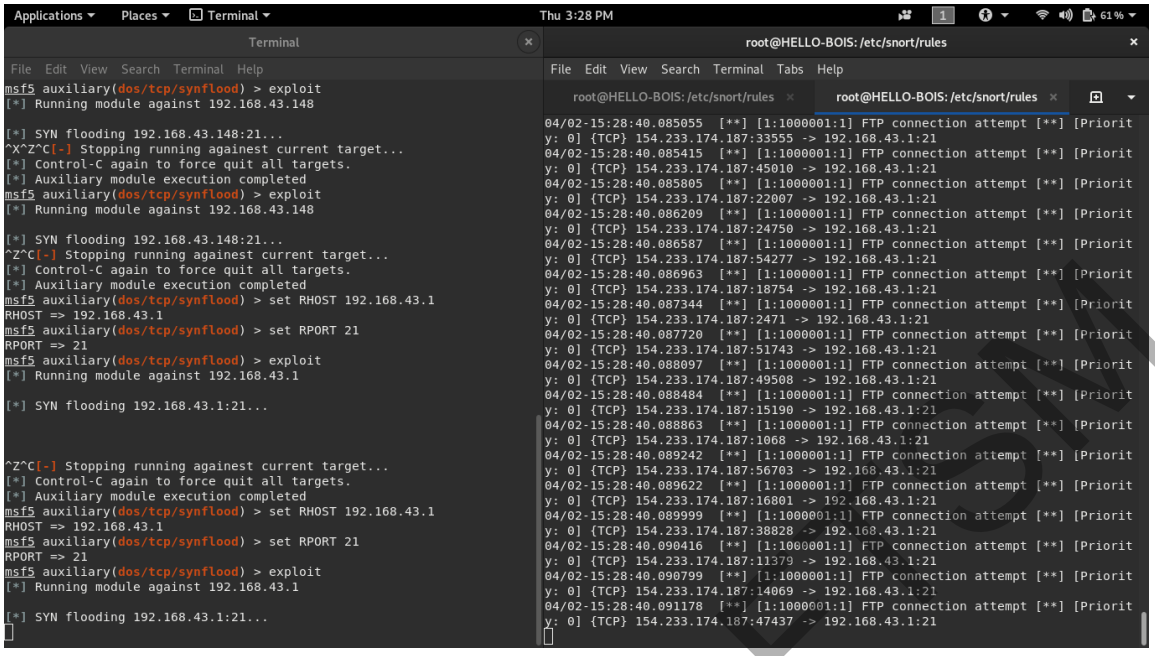


Rajah 6.1: Snort mengesan serangan daripada Nmap

Untuk berhubung dengan jaringan sasaran, penyerang perlu mencari networking enumeration menggunakan Protokol TCP ataupun Protokol UDP. Anggarkan peneyerang memilih TCP scanning untuk network enumeration. Maka peraturan yang sesuai perlu dimasukan kedalam direktori peraturan di dalam Snort. Contoh peaturan yang dimasukan kedalam direktori adalah seperti di bawah:

alert tcp any any -> 192.168.43.1 22 (msg: "NMAP TCP Scan";sid:10000005; rev:2;)

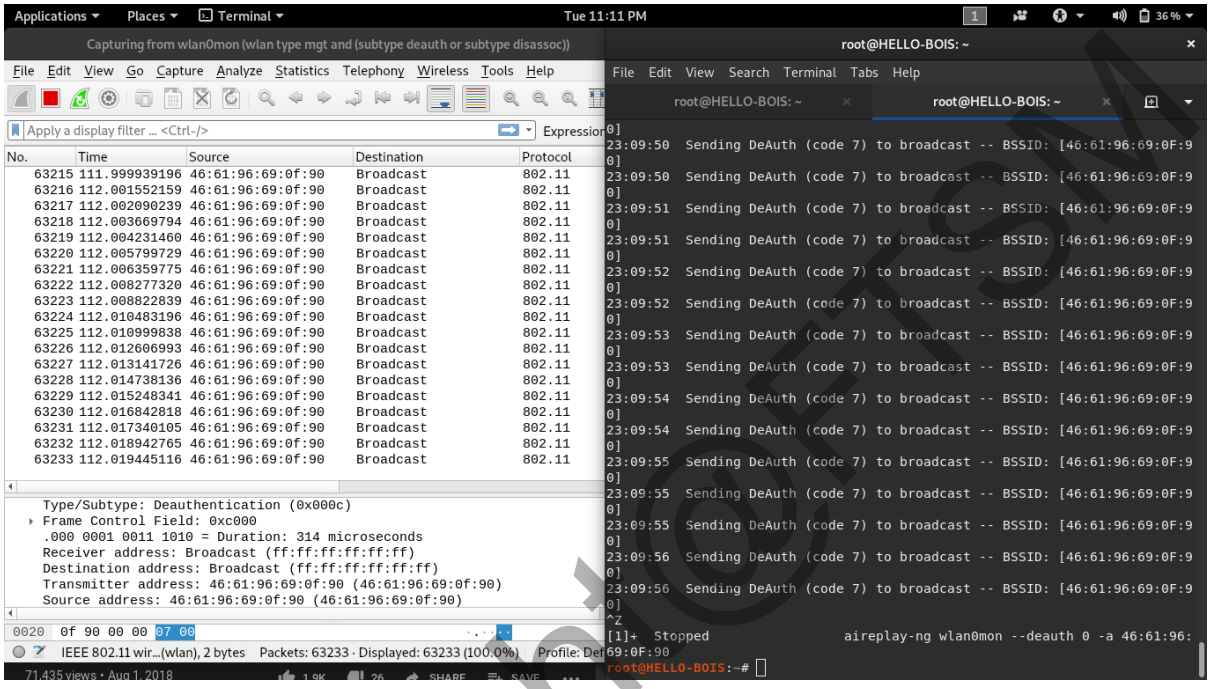
Peraturan ini hanyalah sesuai pada port 22 jika ingin mengimbas port yang lain hanya perlu menggantikan nombor port yang lain atau boleh menggunakan "**any**" untuk mengimbas ke semua port. Seperti rajah 5.4.1.1 Snort mengesan port 53 dan port 44355 yang beroperasi.



Rajah 6.2: Snort mengesan serangan daripada *synflood*

Bagi serangan seperti di atas, Snort mengesan pelbagai Protokol *File Tranfer Protocol (FTP)* yang cuba di hantar ke IP address mangsa serangan daripada penyerang. Serangan di atas lebih berfokus kepada port 21 dan jenis serangan adalah *Denial of Service (DOS).*

6.3 AMARAN PENCEROBOHAN MENGGUNAKAN WIRESHARK



Rajah 6.3: Wireshark mengesan serangan daripada jenis Deauth

Serangan seperti di atas adalah untuk mendapatkan WPA handshake mangsa bertujuan untuk memutuskan rangkaian WIFI. Penyerang cuba menghantar pelbagai jenis *Deauthentication*. Setelah penyerang mendapatkan WPA handshake mangsa, penyerang akan *decrypted* kata laluan mangsa.