**LAPORAN**

**JARINGAN KOMPUTER**

**SECURITY**



Disusun

Tania Yolanda (A11.2017.10055)

Dyanza (A11.2017.10081)

Benedictta Dinda P (A11.2017.10082)

Merry Christiani S (A11.2017.10085)

**PROGRAM STUDI TEKNIK INFORMATIKA S-1**

**UNIVERSITAS DIAN NUSWANTORO**

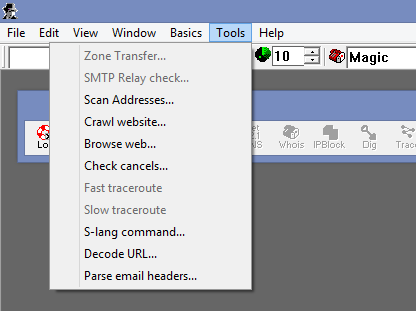
**2019**

1. **Sam Spade**

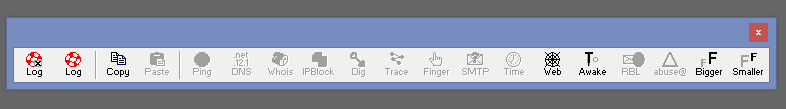
Samp Spade adalah nama alat perangkat lunak Windows yang dirancang untuk membantu melacak sumber-sumber spam e-mail. Selain itu, Samp Spade juga merupakan utilitas gratis yang berisi alat untuk mengumpulkan informasi tentang host internet, menganalisis header email, menampilkan kode situs web, dan melakukan beberapa tugas lainnya.

Website : https://www.sampspade.org

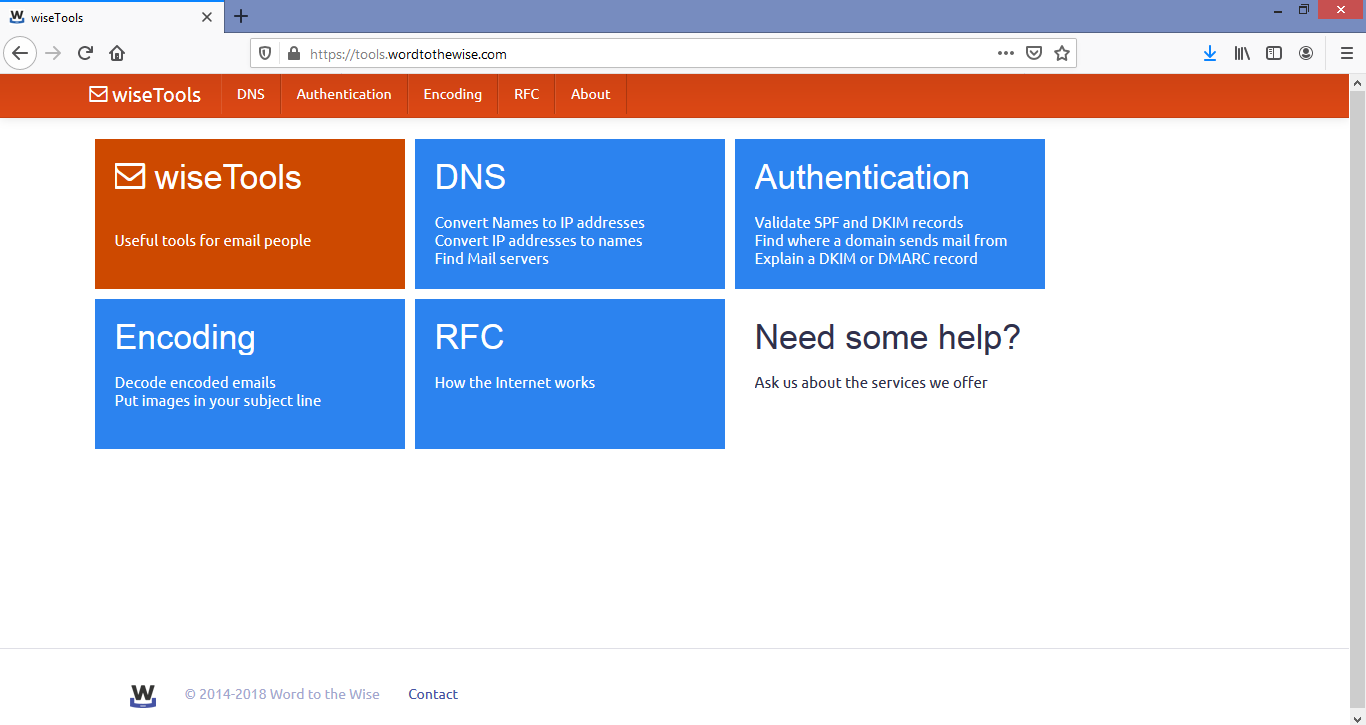
* Query tools



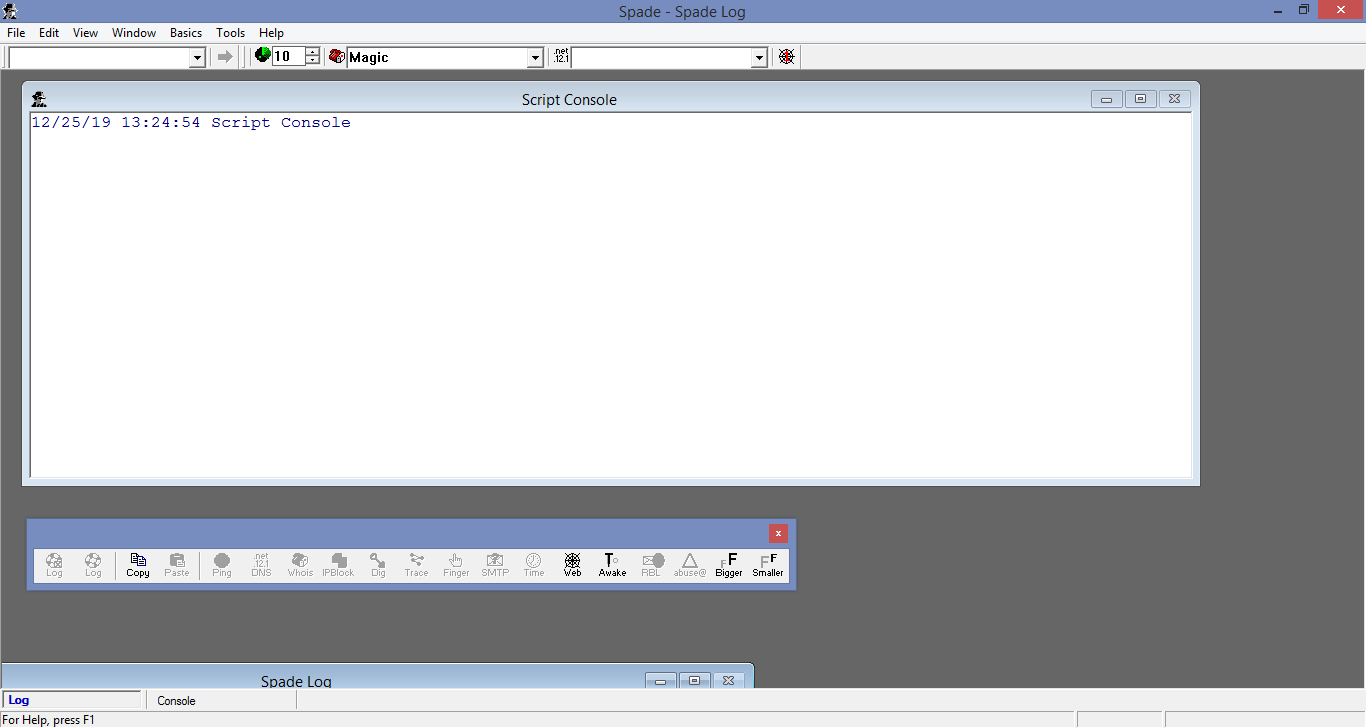
* Zone Transfer, meminta server DNS untuk mengetahui semua hal tentang domain
* SMTP Relay Check, untuk mengecek apakah server e-mail memungkinkan pengiriman pihak ketiga
* Scan Addresses, memindai serangkaian alamat IP yang sedang mencari port terbuka
* Crawl Website, mencari situs web, mencari alamat e-mail, link kantor/perusahaan, dan lain-lain
* Browse web, jelajah web dengan format http
* Check Cancels, mencari server berita untuk membatalkan pesan
* Fast and Slow Traceroute, menemukan route packet antara pengguna dan remote system
* S-Lang Command, mengeluarkan perintah scripting, berguna untuk skrip debugging
* Decode URL, menguraikan URL yang digelapkan
* Parse E-mail Headers, membaca header e-mail dan menebak asal-usul e-mail tersebut
* Toolbar



* Dua tombol Log, satu log dan menutup jendela saat ini (dimana hasil eksekusi ditampilkan), yang lain hanya mencatat tanpa menutup jendela saat ini.
* Tombol Copy dan tombol Paste
* Tombol Ping, Mengirim serangkaian paket ke host yang ditunjukkan dalam kotak alamat
* Tombol DNS, Melakukan nslookup pada host yang ditentukan di bilah alamat
* Tombol Whois, Memberikan informasi kepemilikan dan kontak untuk host yang ditentukan dalam bilah alamat
* Tombol IPBlock, Variasi whois digunakan untuk menentukan informasi kepemilikan dan kontak untuk blok alamat IP
* Tombol DIG (Domain Internet Groper), DIG adalah alat Layanan Nama Domain (DNS) canggih yang mengembalikan semua Catatan Sumber Daya yang tersedia untuk domain atau host tertentu, termasuk catatan awal otoritas (SOA), catatan pertukaran surat (MX), dan catatan server nama (NS)
* Tombol Trace, Traceroute menunjukkan paket rute yang dapat diambil ke host yang ditentukan di bilah alamat (karena internet selalu berubah, paket yang sebenarnya mungkin mengambil rute yang berbeda di beberapa tempat)
* Tombol Finger, Jari memperoleh informasi host / pengguna dari host yang menjalankan daemon jari

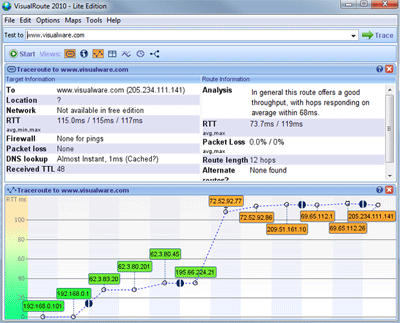


*Tampilan samp spade online*



*Tampilan aplikasi samp spade*

1. **VisualRoute 7.0**



Menampilkan jalur paket internet yang dilalui untuk mencapai tujuan yang ditentukan. Alat ini bekerja dengan mengidentifikasi alamat IP dari setiap hop di sepanjang jalan ke alamat jaringan tujuan.

Fitur dan Kelebihan :

* Tampilan Grafik Traceroute menyediakan data kunci dengan cara yang mudah dicerna

Hasil dari beberapa alat diagnostik jaringan yang penting diintegrasikan ke dalam laporan konektivitas secara keseluruhan, memberikan tampilan grafis dari laporan kinerja koneksi termasuk hilangnya paket dan latensi untuk setiap hop jaringan. Detail drill-down mudah terlihat dengan mouse di atas hop jaringan apa pun

* IP Location Reporting

Lokasi geografis fisik server jaringan dan router adalah informasi utama untuk memahami masalah rute, melihat jalur rute aktual di peta global memberikan gambaran instan tentang efisiensi dan jarak rute

* **Whois Lookups, Network Provider Reporting**

Mendapatkan pencarian instan informasi domain dari database di seluruh dunia, sehingga dapat melihat 'pemilik' terdaftar dari alamat IP atau domain

* OmniPath Multiple Path Discovery

Mendapatkan tampilan real-time dari semua rute yang mungkin ke tujuan dan dengan mudah membandingkan kinerja berbagai rute

* NetVu Multiple Route Topology Graph

Melihat tampilan tingkat tinggi semua rute jaringan untuk laporan penelusuran terbuka, memungkinkan identifikasi node jaringan yang umum untuk banyak rute dengan mudah, dan rute jaringan yang memiliki beberapa opsi jalur karena load balancers atau konfigurasi router

* Application Port Testing, Port Probing, DNS Performance Testing

Lacak port aplikasi spesifik untuk menguji apakah aplikasi penting tersebut aktif dan merespon seperti yang diharapkan

* Traceroute Tests from Visualware Servers

Uji dari server Visualware di Washington dan London untuk menguji konektivitas ke server atau perangkat jaringan pengguna

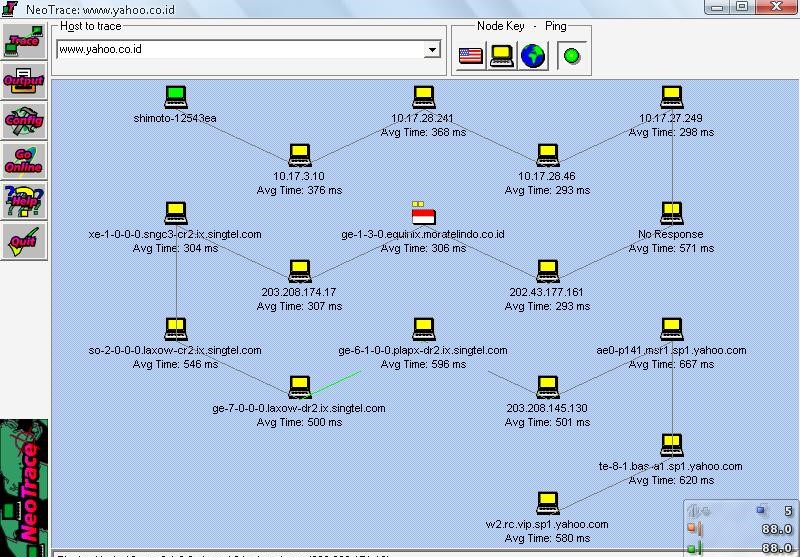
* Continuous Connection Testing with Report History

Pengujian jaringan terus menerus dari desktop VisualRoute ke lokasi jaringan lain mendukung siklus otomatis tes konektivitas untuk memantau penurunan kinerja yang mungkin terjadi dalam jangka waktu yang lama

Cara kerja nya yaitu cukup memasukkan alamat IP dari kemungkinan penyusup yang terdaftar di firewall atau log server, dan VisualRoute menunjukkan kepada Anda peta dunia dengan rute dari Anda ke sumber intrusi. Anda dapat menerapkan pendekatan yang sama untuk melacak sumber spam, dan karena VisualRoute dapat menampilkan informasi pendaftaran domain untuk setiap node atau jaringan dengan klik sederhana, pengguna siap melaporkan pelanggaran.

1. **NeoTrace**

**Sebuah** program utilitis untuk mengetahui dan mencari letak server serta berapa jauh server atau sebuah IP berada. Pemakaian NeoTrace bermanfaat untuk mencari jarak terdekat dalam menempatkan server web. Misalnya ingin menyimpan file pada sebuah server web/server gratis, tentunya sangat efektif sekali bila sebelumnya mengetahui berapa cepat dan seberapa jauh letaknya dari internet provider yang ada di Indonesia. Semakin dekat tentunya akan semakin cepat ping di akses dan semakin baik kemampuan server yang dimiliki akan menghindari lag atau terlalu lamanya data di download dari site yang dimiliki.



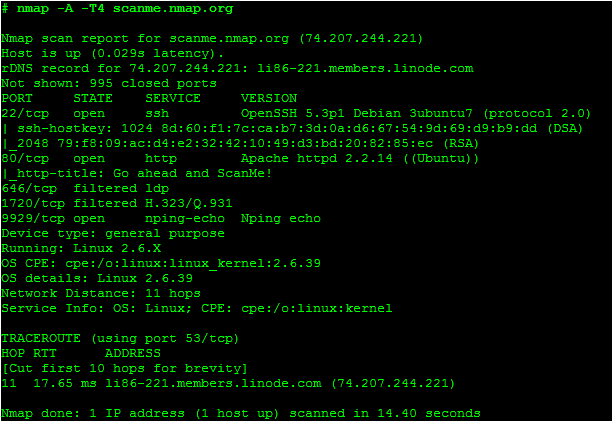
Karena jarak antara server komputer ke server komputer lain akan memerlukan waktu lama untuk didownload dan pada jam sibuk malah akan menghambat sehingga menampilkan data Source unreachable. Padahal servernya ada, tetapi karena terlalu jauh sehingga terlalu lama mendapat balasan dan terjadi Ping Out.

Tetapi fungsi NeoTrace tidak hanya untuk itu saja. NeoTrace dapat mengetahui kelambatan ping dari antar server dan HOP yang ada di Internet. Sehingga kita dapat mengetahui sebuah data dapat ditempuh mencapai berapa server (HOP). Serta melalui backbone mana server tersebut berada, atau kita dapat melihat dinegara mana letak server tersebut berada.

NeoTrace juga dapat melakukan penyimpulan data dari Ping server, misalnya berapa cepat untuk pengiriman data sekali jalan, atau secara rata-rata sekalipun. Atau melihat Backbone mana saja yang dilalui oleh packet data yang dikirim tersebut. Dan dapat membandingkan data antar server yang sedang diperiksa.

1. **Nmap**

Nmap ("Network Mapper") adalah alat open source untuk eksplorasi jaringan dan audit keamanan. Ia dirancang untuk secara cepat memindai jaringan besar, meskipun berfungsi dengan baik terhadap host tunggal.

Output dari Nmap adalah daftar target yang dipindai, dengan informasi tambahan pada masing-masing tergantung pada opsi yang digunakan. Kunci di antara informasi itu adalah "interesting ports table". Tabel itu mencantumkan nomor port dan protokol, nama layanan, dan negara.

Kelebihan Nmap :

* Mampu digunakan sebagai network inventory tools dan mapping IP, port, dan services.
* Mampu mendeteksi vulnerability di network.
* Port scanning.
* Relatif mudah digunakan.

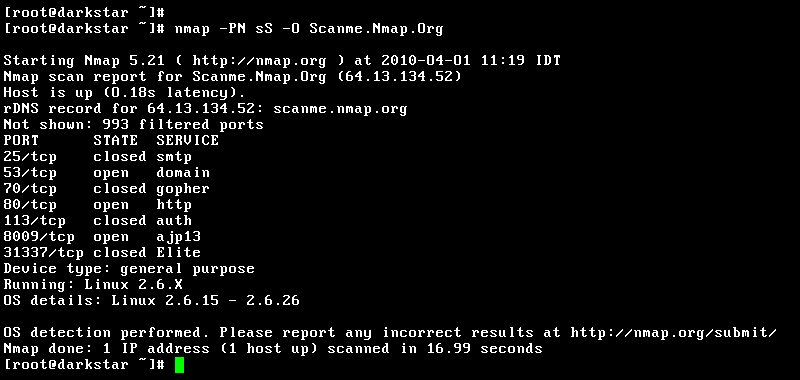
Kekurangan Nmap :

* Sulit menemukan issue tertentu terutama vulnerability dibagian aplikasi, nmap pada umumnya digunakan untuk menemukan celah vulnerability di bagian network.

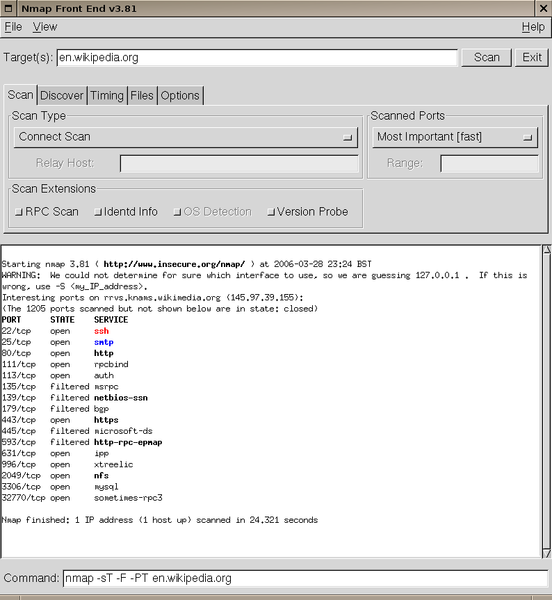
Fitur Nmap

* **Deteksi SO** deteksi SO dengan menggunakan fingerprint stack TCP/IP
* **Nmap Scripting Engine (NSE)** adalah salah satu fitur Nmap yang paling powerful dan fleksibel. Ia memungkinkan user untuk menulis (dan membagi) skrip sederhana (menggunakan bahasa pemrograman Lua) untuk mengotomasi beragam tugas jaringan.

1. NMap Win V1

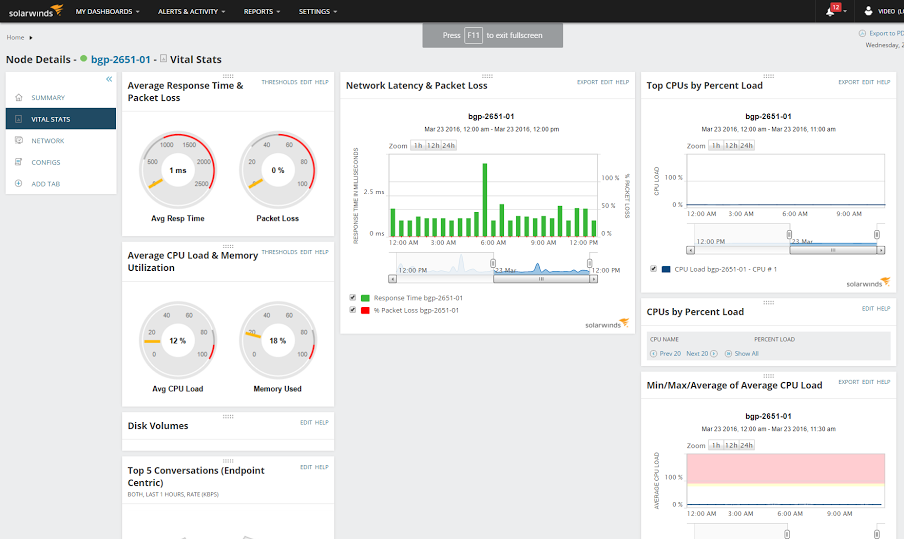
Nmap (Network Mapper) adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan port scanning

Fitur:

* Host Discovery, Mengidentifikasi host di jaringan. Misalnya, daftar host yang menanggapi permintaan TCP dan / atau ICMP atau membuka port tertentu
* Port Scanning, Menghitung port terbuka pada host target
* Version Detection, Menginterogasi layanan jaringan pada perangkat jarak jauh untuk menentukan nama aplikasi dan nomor versi
* OS Detection, Menentukan karakteristik sistem operasi dan perangkat keras pada perangkat jaringan
* Scriptable Interaction with the Target, Menggunakan Nmap scripting engine dan Bahasa Pemrograman Lua

1. **IP Network Browser**

IP Network Browser dapat memindai subnet dan menampilkan detail tentang perangkat di subnet. Setiap alamat IP dikirim PING. Untuk setiap alamat yang merespons, Browser Jaringan IP berupaya mengumpulkan lebih banyak informasi. Ini dilakukan dengan menggunakan SNMP (Simple Network Management Protocol). Agen SNMP harus aktif pada perangkat jarak jauh agar Browser Jaringan IP dapat mengumpulkan detail tentang perangkat tersebut.



1. **LAN Views 1.6**

Kumpulan alat untuk administrator jaringan, yang menggabungkan beberapa alat pengecekan jaringan ke dalam satu aplikasi. Di dalamnya terdapat penyadap jaringan (dengan filter), dan tampilan lalu lintas jaringan dengan alat-alat jaringan lainnya seperti port scan, ping, network connections dan paket statistics. Semua informasi ditampilkan dalam bentuk teks.