MEMBANDINGKAN ANALISA TRAFIK DATA PADA JARINGAN KOMPUTER ANTARA WIRESHARK DAN NMAP

Rika Rosnelly[1], Reza Pulungan[2]

STMIK Potensi Utama[1], Program Pascasarjana Ilmu Komputer UGM[2]
Jl. KL. Yos Sudarso Km. 6,5 No. 3A Tj. Mulia Medan[1], FMIPA UGM Sekip Utara Bulaksumur Yogyakarta 55281[2]
rika@potensi-utama.ac.id[1], pulungan@ugm.ac.id[2]

Abstrak

Sekarang ini jaringan komputer sudah menjadi suatu kebutuhan yang sangat penting untuk mempermudah pertukaran data antar komputer. Seiring dengan makin berkembangnya jumlah komputer pada suatu jaringan, maka makin bertambah pula tingkat kesulitan untuk mengelola jaringan tersebut. Suatu jaringan seyogyanya mempunyai peraturan mengenai bagaimana sebuah obyek atau aktifitas data yang bergerak melintas dalam jaringan. Analisis jaringan berhubungan erat kaitannya dengan menjaga keamanan sebuah jaringan ; analisis berguna untuk memecahkan permasalahan yang terjadi dalam jaringan. Analisis jaringan adalah kegiatan mendengar dan mengamati segala aktifitas yang terjadi dalam jaringan. Pada penelitian ini akan dibandingkan cara kerja yaitu wireshark dan NMap dalam mengamati traffic network serta menganalisa jenis paket apa saja yang sedang melalui network.

Kata kunci : *network traffic, wireshark, NMap*

1. Pendahuluan

Perkembangan pemakaian internet yang meningkat pesat saat ini menyebabkan permintaan akan mutu layanan (*Quality of services/QoS*) yang harus ditingkatkan. Tidak cukup jika hanya bisa terhubung ke internet, performa konektivitas menjadi faktor penting dalam penggunaan internet sekarang ini.

Dalam meningkatkan performa konektivitas tersebut, yaitu dengan memastikan bahwa lalu lintas data di jaringan berjalan lancar. Salah satu cara untuk melakukan ini adalah dengan mendebug jaringan dan mengamati lalu lintas data tersebut.

Jaringan TCP/IP terdiri atas keseluruhan paket dan cara terbaik untuk mendebug jaringan adalah dengan cara melacak paket. Network packet analyzer akan mencoba menangkap paket-paket yang melalui network kemudian menampilkan data paket sedetail mungkin. Kita dapat membayangkan network packet analyzer seperti alat ukur yang menganalisis data yang lalu-lalang pada kabel jaringan [1]. Dengan demikian kita dapat menentukan informasi yang tepat dari sumber yang benar. Untuk melacak paket kita dapat menggunakan wireshark dan NMap.

2. Analisa Trafik Data dengan Wireshark

Wireshark merupakan salah satu network analysis tool, atau disebut juga dengan protocol analysis tool atau packet sniffer. Wireshark dapat digunakan untuk troubleshooting jaringan, analisis, pengembangan software dan protocol serta untuk keperluan edukasi. Wireshark dikenal dengan nama Ethereal.

Wireshark memungkinkan anda pengguna mengamati data dari jaringan yang sedang beroperasi atau dari data yang ada di disk, dan langsung melihat dan mensortir data yang tertangkap. Informasi singkat dan detail

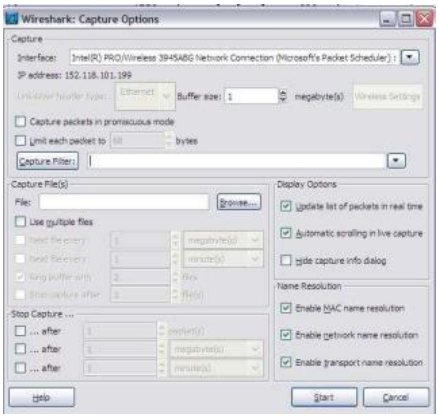
bagi masing-masing paket, termasuk full header dan porsi data, bisa diperoleh. Wireshark mempunyai beberapa fitur termasuk display filter language yang kaya dan kemampuan untuk merekonstruksi kembali sebuah aliran pada sesi TCP [2].

Paket sniffer sendiri dapat diartikan sebagai sebuah program atau tool yang memiliki kemampuan untuk 'mencegat' dan melakukan pencatatan terhadap traffic data dalam jaringan. Selama terjadi aliran data dalam jaringan, packet sniffer dapat menangkap protocol data unit (PDU), melakukan dekoding serta melakukan analisis terhadap isi paket berdasarkan spesifikasi RFC atau spesifikasi-spesifikasi yang lain.

Wireshark sebagai salah satu packet sniffer diprogram sedemikian rupa untuk mengenali berbagai macam protocol jaringan. Wireshark mampu menampilkan hasil enkapsulasi dan field yang ada di dalam PDU.

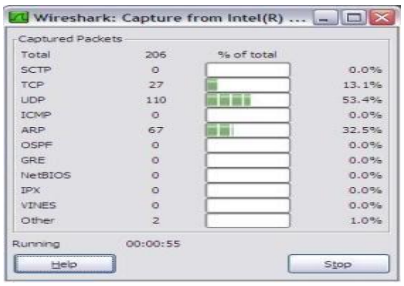
Cara menggunakan Wireshark serta contoh menjalankan capture PDU, prosedurnya adalah sebagai berikut

1. Jalankan Wireshark.
2. Untuk melakukan capture dengan memilih pilihan yang tersedia, pilih menu Capture>Option… akan tampil jendela seperti diperlihatkan pada Gambar 1.



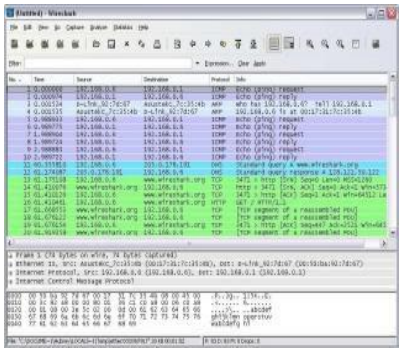
Gambar 1. Capture Option

3. Pada Jendela Capture Option, pilihlah interface Ethernet yang akan dicapture. Terlihat pada screenshot di atas terdapat 3 buah pilihan. Pilihan paling atas menunjukkan untuk melakukan capture pada Promiscuous Mode. Jika pilihan ini diaktifkan, maka Wireshark akan melakukan capture terhadap paket-paket yang ditujukan untuk komputer ini dan paket-paket yang terdeteksi oleh NIC dari komputer-komputer dalam satu segmen jaringan.
4. Pilihan kedua menunjukkan pilihan-pilihan untuk mengatur tampilan pada jendela Capture Option. Jika pilihan hide capture dialog info dinonaktifkan, ketika capture dimulai, Wireshark akan menampilkan jendela tambahan yang memberikan statistik persentase protokol yang ter-capture seperti diperlihatkan pada Gambar 2.



Gambar 2. Capture from intel(R)

5. Pilihan ketiga memberikan pilihan bahwa Wireshark akan menerjemahkan alamat jaringan dalam PDU menjadi nama. Mengaktifkan pilihan ini akan menambah PDU ekstra ke dalam data yang ter-capture.
6. Jendela Wireshark terdiri atas tiga bagian, seperti ditunjukkan pada screenshot pada Gambar 3.



Gambar 3. Jendela Wireshark

7. Packet List Pane menampilkan ringkasan dari paket-paket yang tertangkap oleh Wireshark. Memilih salah satu paket yang tampil pada bagian ini akan

memperlihatkan detail dari paket tersebut pada dua panel di bawahnya. Packet Detail Pane menampilkan detail dari paket yang dipilih pada Packet List Pane. Packet Byte Pane menunjukkan isi data dari sebuah paket dalam heksadesimal serta menunjukkan detail dari field yang dipilih pada Packet Detail Pane. Untuk memulai proses capture, klik pada tombol Start.

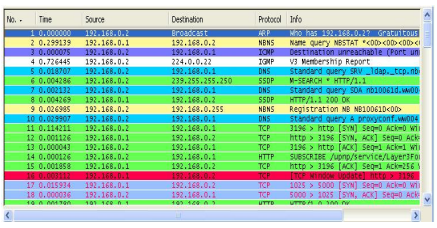
8. Buka command prompt dengan cara klik Start > Run… > ketikkan cmd > klik OK. Lakukan ping ke suatu dengan mengetikkan perintah ping IP Address.
9. Aktivitas ping tersebut akan terekam oleh Wireshark. Hasil capture dapat disimpan dengan memilih menu File > Save As… pada Wireshark.
10. Berdasarkan hasil capture Wireshark tersebut, informasi lalu lintas data dapat diperoleh dan dengan demikian kondisi jaringan secara umum dapat dianalisa.

Wireshark memiliki seperangkat fitur yang meliputi sebagai berikut [4]:

1. Tersedia untuk Unix, Linux dan Windows
2. Menangkap paket data dari antar muka jaringan
   Wireshark dapat menangkap lalu lintas dari banyak jenis jaringan media yang berbeda, termasuk LAN nirkabel juga. Media jenis tersebut didukung, tergantung pada banyak hal seperti sistem operasi yang digunakan.

3. Tampilan paket dengan informasi protokol yang sangat rinci.

Menampilkan paket pane daftar semua paket dalam file pengambilan yang aktif.
Berikut tampilan daftar paket pane ditunjukkan pada Gambar 4.



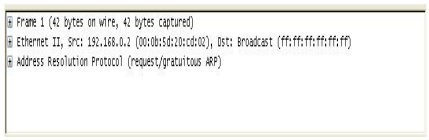
Gambar 4. Daftar Paket Pane

Setiap baris dalam daftar paket sesuai dengan satu paket dalam file ambil. Jika Anda memilih jalur dalam pane ini, lebih jelasnya akan ditampilkan dalam "Rincian Paket" dan "Packet Bytes".
Kolom default akan menampilkan:

- No : Jumlah paket dalam file ambil. Jumlah ini tidak akan berubah, bahkan jika tampilan filter digunakan.
- Time : stempel waktu dari paket. Format penyajian stempel waktu ini dapat berubah
- Source : Alamat dimana paket ini datang
- Destination : Alamat dimana paket berada
- Protocol : Nama protokol dalam versi pendek
- Info : Informasi tambahan tentang isi paket.

Berikut rincian paket pane menunjukkan paket saat ini (yang dipilih pada pane "Packet List") dalam bentuk yang lebih rinci.

Berikut tampilan detail paket pane ditunjukkan pada Gambar 5.



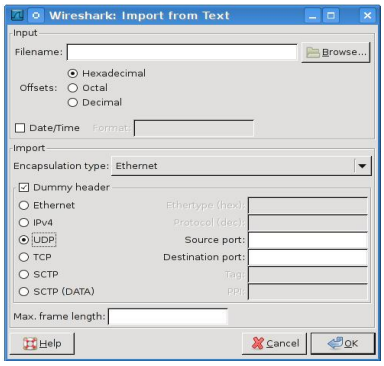
Gambar 5. Detail Packet Pane

Pane ini menunjukkan bidang protokol dan protokol dari paket yang dipilih pada panel "Packet List". Protokol dan bidang paket ditampilkan menggunakan pohon, yang dapat diperluas dan runtuh. Beberapa bidang protokol secara khusus ditampilkan :

- Generated Fields : Wireshark sendiri akan menghasilkan medan protokol tambahan yang dikelilingi oleh tanda kurung. Informasi dalam bidang ini berasal dari konteks diketahui paket lain di file ambil. Sebagai contoh, Wireshark melakukan urutan / mengakui analisis dari setiap aliran TCP, yang ditampilkan dalam [SEQ/analisis ACK] bidang protokol TCP.
- Link : Jika Wireshark terdeteksi hubungan lain paket di file tangkap, maka akan menghasilkan link ke paket tersebut. Link yang digarisbawahi dan ditampilkan dengan warna biru. Jika diklik ganda, Wireshark melompat ke paket yang sesuai.

4. Buka dan Simpan capture paket data
   a. Wireshark dapat membaca pada file capture disimpan sebelumnya. Untuk membacanya, cukup pilih menu atau item toolbar: "File / Open"
   untuk membuka file, hanya dengan mendrag file yang diinginkan dari file manager Anda dan mendrop itu ke jendela utama Wireshark's. Namun, drag-and-drop tidak tersedia dalam semua lingkungan desktop.

   b. Anda dapat menyimpan paket ditangkap hanya dengan menggunakan Save As... menu item dari menu File di dalam Wireshark. Anda dapat memilih paket untuk menyimpan dan yang format file yang akan digunakan.
5. Impor dan Ekspor paket data dari dan ke banyak program capture lainnya.
   a. Impor paket data
   Berikut kotak dialog "File Import" ditunjukkan pada Gambar 6.



Gambar 6. File Import

kontrol khusus dari dialog impor dibagi dalam dua bagian:

- Input
  Menentukan file input harus diimpor dan bagaimana itu harus ditafsirkan.
- Impor
  Tentukan bagaimana data yang akan diimpor. Parameter input adalah sebagai berikut:

a. Filename / Browse
   Masukkan nama dari file teks untuk impor. Anda dapat menggunakan Browse untuk mencari file.

b. Offset
   Pilih radix dari offset diberikan dalam file teks untuk mengimpor. Hal ini biasanya heksadesimal, namun desimal dan oktal juga didukung.

c. Date/Time
   Centang checkbox ini jika ada cap terkait dengan bingkai dalam file teks untuk mengimpor yang ingin Anda gunakan. Jika waktu saat ini digunakan untuk timestamping frame.

d. Format
   Ini adalah format specifier yang digunakan untuk mengurai cap waktu dalam file teks untuk impor. Menggunakan sintaks yang sederhana untuk menggambarkan format timestamp, menggunakan% H untuk jam,% M menit,% S untuk detik, dll langsung HH: MM: SS format ditutupi oleh% T. Untuk definisi penuh tampilan sintaks untuk strftime (3).

Parameter impor adalah sebagai berikut:

a. Type Enkapsulasi
   Di sini Anda dapat memilih jenis frame yang Anda impor. Ini semua tergantung dari jenis dump menengah untuk impor diambil. Ini daftar semua jenis yang Wireshark mengerti, sehingga untuk lulus menangkap isi file ke dissector kanan.

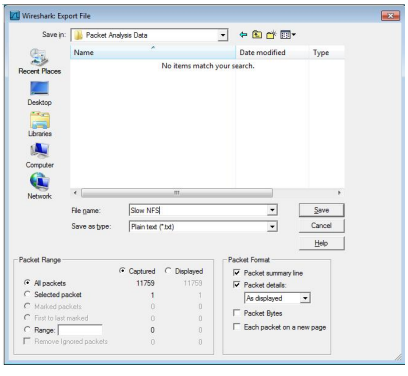
b. Dummy header
   Ketika enkapsulasi Ethernet dipilih, Anda harus pilihan untuk prepend header dummy ke frame untuk mengimpor. Header ini dapat memberikan Ethernet buatan, IP,

UDP atau TCP atau SCTP header dan data SCTP potongan. Ketika memilih jenis header dummy entri yang berlaku diaktifkan, yang lain berwarna abu-abu dan nilai-nilai default yang digunakan.

c. Max. frame length
yaitu menentukan berapa banyak data dari awal frame yang ingin diimpor. Jika kita membiarkannya terbuka maksimum diatur ke 64000 byte.
Setelah semua parameter input dan impor setup klik OK untuk memulai impor.
Jika data Anda saat ini tidak disimpan sebelumnya, Anda akan diminta untuk menyimpan terlebih dahulu, sebelum kotak dialog ditampilkan.
Ketika selesai akan ada file capture baru dimuat dengan frame yang diimpor dari file teks.

b. Ekspor paket data
Wireshark menyediakan beberapa cara dan format untuk mengekspor data paket. Bagian ini menjelaskan cara-cara umum untuk ekspor data dari Wireshark.
Kotak dialog "Export as Plain Text File"

Berikut kotak dialog Export as Plain Text File ditunjukkan pada Gambar 7.



Gambar 7. Export as Plain Text File

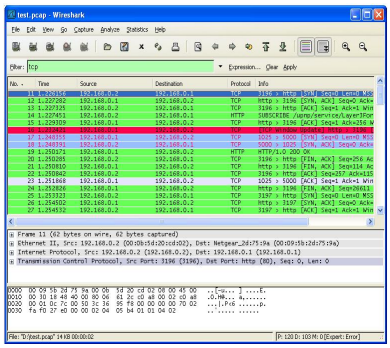
6. Filter paket dengan banyak kriteria
Wireshark memiliki dua bahasa penyaringan: Satu digunakan saat menangkap paket-paket, dan satu digunakan ketika menampilkan paket. Pada bagian ini kita mengeksplorasi jenis kedua filter: filter tampilan.

Filter tampilan memungkinkan untuk berkonsentrasi pada paket anda tertarik ketika bersembunyi yang saat ini tidak menarik. Mereka memungkinkan Anda untuk memilih paket oleh:

- Protokol
- Kehadiran lapangan
- Nilai lahan
- Perbandingan antara bidang

Untuk memilih paket berdasarkan jenis protokol, cukup ketik protokol pada Filter : fileds dalam toolbar filter dari jendela Wireshark dan tekan enter untuk memulai memfilter.

Berikut filtering pada protocol TCP ditunjukkan pada Gambar 8.

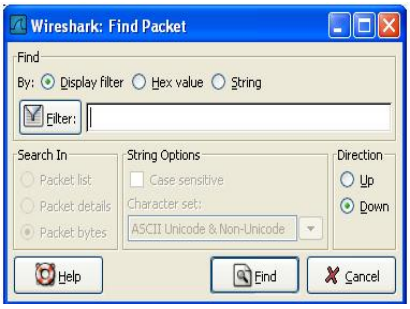


Gambar 8. Filtering pada protocol TCP

Seperti pada gambar 8 diatas, hanya paket protokol TCP ditampilkan sekarang (misalnya paket 1-10 yang tersembunyi). Penomoran paket akan tetap seperti sebelumnya, sehingga paket pertama yang ditampilkan adalah paket sekarang nomor 11.

7. Mencari paket dengan banyak criteria
Mencari paket dapat dengan mudah untuk ditemukan, yaitu dengan menangkap beberapa paket atau telah membaca dalam sebuah capture file yang disimpan sebelumnya. Cukup pilih Find Packet, menu item dari menu Edit. Wireshark

akan muncul kotak dialog yang ditunjukkan pada Gambar 9.



Gambar 9. Find Packet

8. Mewarnai tampilan paket berdasarkan filter
   Mekanisme yang sangat berguna yang tersedia di Wireshark pewarnaan paket. Anda dapat set-up Wireshark sehingga akan mewarnai paket sesuai dengan filter.

Ada dua jenis pewarnaan aturan dalam Wireshark, yang sementara yang hanya digunakan sampai Anda keluar dari program, dan yang permanen yang akan disimpan ke file preferensi sehingga mereka tersedia pada sesi berikutnya.

Sementara aturan pewarna dapat ditambahkan dengan memilih paket dan menekan tombol <ctrl> bersama dengan salah satu tombol angka. Ini akan membuat aturan pewarnaan yang didasarkan pada percakapan yang sedang dipilih. Ini akan mencoba untuk membuat percakapan filter berdasarkan TCP pertama, kemudian UDP, lalu IP dan Ethernet terakhir. Filter sementara juga dapat dibuat dengan memilih "Colorize dengan Filter Color> X" item menu ketika mengklik kanan pada pane paket-detail.

Untuk secara permanen mewarnai paket, pilih Coloring Rules, menu item dari menu View, Wireshark akan pop up " Coloring Rules " kotak dialog seperti yang ditunjukkan pada Gambar 10.

Gambar 10. Coloring Rules

9. Membuat berbagai statistik
   Wireshark menyediakan berbagai statistik jaringan yang dapat diakses melalui menu Statistik.
   Statistik ini berkisar dari informasi umum tentang file menangkap dimuat (seperti jumlah paket yang ditangkap), untuk statistik tentang protokol tertentu (misalnya data statistik tentang jumlah permintaan HTTP dan tanggapan tertangkap).

   Statistik umum:

   - Ringkasan tentang capture file.
   - Protokol Hirarki dari capture paket.
   - Percakapan misalnya lalu lintas antara alamat IP tertentu.
   - endpoint misalnya lalu lintas ke dan dari alamat IP.
   - grafik IO memvisualisasikan jumlah paket (atau serupa) dalam waktu.

   Protokol spesifik statistik:

   - layanan respon waktu antara permintaan dan respon dari beberapa protokol.
   - statistik berbagai protokol lain yang spesifik.

3. Analisa Trafik Data dengan NMap (*Network Mapper*)

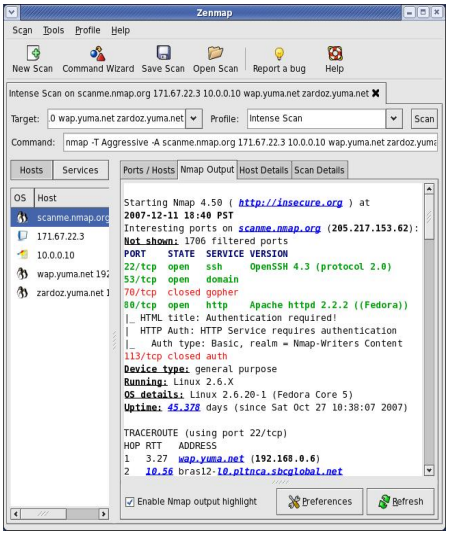
Scan adalah kegiatan probe dalam jumlah yang besar dengan menggunakan tool secara otomatis. Tool tersebut secara otomatis dapat mengetahui port-port yang terbuka pada host lokal maupun host remote, IP address yang aktif, bahkan bisa untuk mengetahui sistem

operasi yang digunakan pada host yang dituju. Contoh tool scanner adalah NMap [3].

Nmap (*Network Mapper*) merupakan salah satu tools eksplorasi jaringan, dan secara eksklusif menjadi salah satu andalan yang sering digunakan oleh administrator jaringan. Dengan Nmap kita dapat melakukan penelusuran ke seluruh jaringan dan mencari tahu service apa yang aktif pada port yang lebih spesifik. Nmap merupakan salah satu tools yang paling banyak digunakan untuk melakukan scanning jaringan dan terkenal sebagai tool yang multi platform, cepat dan ringan. Nmap berjalan pada semua jenis OS, baik mode console maupun grafis.

Nmap berjalan pada semua sistem operasi komputer utama, dan paket biner resmi tersedia untuk Linux, Windows, dan Mac OS X. Selain Nmap command-line klasik dieksekusi, suite Nmap mencakup GUI maju dan penampil hasil (Zenmap), transfer data yang fleksibel, redirection, dan alat debugging (Ncat), dan sebuah utilitas untuk membandingkan hasil scan (Ndiff).

Tampilan hasil NMap diperlihatkan pada Gambar 10.



Gambar 10. Penampil hasil NMap

NMap memiliki seperangkat fitur yang meliputi sebagai berikut [5]:

1. Host Discovery : mengidentifikasikan suatu komputer yang terdapat pada suatu jaringan Salah satu langkah pertama dalam misi network reconnaissance adalah mengurangi satu rentang IP (biasanya besar) ke sebuah daftar host yang aktif atau menarik. Memeriksa setiap port dari setiap alamat IP adalah lambat dan biasanya tidak perlu. Tentu saja apa yang membuat sebuah host menarik tergantung pada tujuan pemeriksaan. Administrator jaringan mungkin hanya tertarik pada host yang menjalankan layanan tertentu, sementara auditor keamanan ingin mengetahui semua device dalam satu alamat IP. Administrator mungkin nyaman cukup dengan menggunakan ping ICMP untuk menemukan host pada jaringan internalnya, sementara penetration tester eksternal mungkin menggunakan beragam probe dalam usahanya menghindari pembatasan firewall.

Oleh karena kebutuhan pencarian host sangat beragam, Nmap menawarkan sejumlah opsi untuk kustomisasi teknik yang dibutuhkan. Pencarian host seringkali disebut ping scan, namun ia lebih daripada sekedar melakukan pengiriman paket echo request ICMP yang diasosiasikan dengan tool terkenal ping. Pengguna dapat melewati langkah ping dengan list scan (-sL) atau dengan meniadakan ping (-PN), atau melakukan kombinasi probe multi-port TCP SYN/ACK, UDP, dan ICMP. Tujuan probe ini adalah memperoleh respon yang menunjukkan bahwa alamat IP sedang aktif (sedang digunakan oleh host atau device jaringan). Pada banyak jaringan, hanya sejumlah kecil persentase alamat IP yang aktif pada satu waktu. Hal ini terutama umum terjadi pada alamat IP privat seperti 10.0.0.0/8. Jaringan tersebut memiliki 16 juta IP, namun digunakan oleh perusahaan dengan mesin berjumlah kurang dari seribu. Pencarian host dapat menemukan mesin-mesin dalam lautan alamat IP.

Jika tidak diberikan opsi pencarian host, Nmap mengirimkan sebuah paket TCP ACK yang ditujukan ke port 80 dan sebuah query ICMP echo request ke setiap mesin target. Pengecualian atas hal ini adalah scan ARP digunakan untuk sembarang target yang ada pada jaringan ethernet lokal. Untuk user shell Unix biasa, sebuah paket SYN dikirimkan alih-alih paket ACK dengan menggunakan system call connect. Nilai-nilai baku ini sama

dengan opsi -PA -PE. Pencarian host ini seringkali cukup ketika melakukan pemeriksaan jaringan lokal, namun disarankan untuk melakukan probe pencarian yang lebih komprehensif ketika melakukan audit keamanan.

Opsi-opsi -P* (yang memilih tipe ping) dapat digabungkan. Anda dapat meningkatkan peluang anda menyusup firewall yang ketat dengan mengirimkan banyak jenis probe dengan menggunakan berbagai macam port/flag TCP dan kode ICMP. Perhatikan pula bahwa pencarian ARP discovery (-PR) secara baku dilakukan terhadap target pada jaringan ethernet lokal bahkan bila anda menspesifikasikan opsi -P* lain, karena ia selalu lebih cepat dan lebih efektif.

Secara baku, Nmap melakukan pencarian host dan lalu melakukan scan port terhadap setiap host yang ditentukan online. Hal ini benar bahkan bila anda menspesifikasikan tipe pencarian host yang tidak baku seperti probe UDP (-PU). Bacalah mengenai opsi -sP untuk mempelajari bagaimana melakukan hanya pencarian host, atau gunakan -PN untuk melewati pencarian host dan melakukan scan port untuk seluruh host.

1. Port Scanning : menghitung port mana saja yang terbuka pada satu komputer atau lebih

Meskipun selama ini Nmap telah mengalami perkembangan fungsionalitas, namun ia bermula sebagai sebuah scanner port yang efisien, dan hal itu tetap menjadi fungsi utamanya. Perintah sederhana nmap <*target*> akan memeriksa lebih dari 1660 port TCP pada host <*target*>. Ketika banyak scanner port secara tradisional membagi seluruh port ke dalam status terbuka (open) atau tertutup (closed), Nmap lebih granular. Ia membagi port menjadi enam status : open, closed, filtered, unfiltered, open|filtered, or closed|filtered.

Status ini bukan merupakan properti intrinsik dari port itu sendiri, namun menggambarkan bagaimana Nmap memandang mereka. Sebagai contoh, scan Nmap dari jaringan yang sama dengan target mungkin menampilkan port 135/tcp sebagai terbuka, sementara scan yang sama pada waktu dan opsi yang sama dari Internet mungkin menunjukkan bahwa port tersebut filtered.

Berikut Enam status port yang dikenali Nmap yaitu **:**

a. Open
   Sebuah aplikasi secara aktif menerima koneksi paket TCP atau UDP pada port ini. Menemukan port terbuka ini seringkali merupakan tujuan utama scanning port. Orang dengan pikiran keamanan *(security-minded)* tahu bahwa setiap port terbuka merupakan celah untuk serangan. Penyerang dan pen-testers ingin mengeksploitasi port terbuka, namun administrator berusaha menutup atau melindungi mereka dengan firewall tanpa mengganggu user yang berhak. Port terbuka juga menarik bagi scan bukan keamanan karena mereka memberitahu layanan yang dapat digunakan pada jaringan.

b. Closed
   Port tertutup dapat diakses (ia menerima dan menanggapi paket probe Nmap), namun tidak ada aplikasi yang mendengarkan padanya. Mereka bermanfaat dengan menunjukkan bahwa host up pada alamat IP tersebut (host discovery, atau ping scanning), dan sebagai bagian deteksi SO. Oleh karena port tertutup dapat dijangkau, bermanfaat untuk mencoba scan di waktu yang lain jikalau port tersebut terbuka. Administrator mungkin perlu mempertimbangkan untuk memblok port tersebut dengan firewall. Lalu mereka akan muncul dalam status filtered, yang akan didiskusikan.

c. Filtered
   Nmap tidak dapat menentukan apakah port terbuka karena packet filtering mencegah probenya mencapai port. Filter ini dapat dilakukan oleh device firewall, aturan pada router, atau software firewall pada host. Port ini membuat penyerang frustrasi karena mereka memberikan sedikit informasi. Terkadang mereka menanggapi dengan

pesan kesalahan ICMP misalnya tipe 3 kode 13 (tujuan tidak dapat dicapai: komunikasi dilarang secara administratif), namun yang lebih umum adalah filter yang hanya men-drop probe tanpa memberi tanggapan. Hal ini memaksa Nmap berusaha beberapa kali untuk memastikan probe tidak di-drop akibat jaringan yang padat. Hal ini sangat memperlambat proses scan.

d. Unfiltered
   Status unfiltered berarti bahwa port dapat diakses, namun Nmap tidak dapat menentukan apakah ia open atau closed. Hanya scan ACK, yang digunakan untuk mengetahui aturan firewall, menggolongkan port ke dalam status ini. Pemeriksaan port unfiltered dengan tipe pemeriksaan lain seperti Window scan, SYN scan, atau FIN scan, dapat membantu mengetahui apakah port terbuka.

e. Open|filtered
   Nmap menganggap port dalam status ini bila ia tidak dapat menentukan apakah port open atau filtered. Hal ini terjadi untuk jenis pemeriksaan ketika port terbuka tidak memberi respon. Tidak adanya tanggapan dapat pula berarti bahwa packet filter men-drop probe atau respon yang diberikan. Sehingga Nmap tidak dapat mengetahui dengan tepat apakah port terbuka atau difilter. Scan UDP, IP protocol, FIN, NULL, dan Xmas mengklasifikasikan port dengan cara ini.

f. Closed|filtered
   Status ini digunakan ketika Nmap tidak dapat menentukan apakah port tertutup atau di-filter. Ia hanya digunakan pada scan idle ID IP.

2. Version Detection : untuk menilai service apa yang digunakan pada suatu jaringan untuk dapat menentukan aplikasi dan versi yang digunakan.

Arahkan Nmap ke mesin remote dan ia dapat memberitahu anda bahwa port 25/tcp, 80/tcp, dan 53/udp terbuka. Dengan menggunakan database nmap-services yang berisi lebih dari 2.200 layanan yang dikenal, Nmap akan melaporkan bahwa port tersebut mungkin adalah server mail (SMTP), server web (HTTP), dan name server (DNS). Pencocokan ini biasanya akurat- sebagian besar daemon yang mendengarkan TCP port 25 adalah, mail server.

Setelah port TCP dan/atau UDP ditemukan dengan menggunakan salah satu metode scan, deteksi versi menginterogasi port tersebut untuk menentukan lebih jauh mengenai apa yang sedang berjalan. Database nmap-service-probes berisikan probe untuk melakukan query ke sejumlah layanan dan ekspresi pencocokan untuk mengenali dan memproses respon. Nmap berusaha menentukan protokol layanan (misalnya FTP, SSH, Telnet, HTTP), nama aplikasi (misalnya ISC BIND, Apache httpd, Solaris telnetd), angka versi, nama host, jenis device (misal printer, router), keluarga SO (misal Windows, Linux) dan terkadang detil lainnya seperti apakah X server terbuka untuk koneksi, versi protokol SSH, atau nama user KaZaA). Tentu saja, kebanyakan layanan tidak memberikan informasi ini. Jika Nmap dikompilasi dengan dukungan OpenSSL, ia akan koneksi ke server SSL untuk mendapatkan layanan yang berada di belakang lapisan enkripsi. Ketika ditemukan layanan RPC, Nmap RPC grinder (-sR) secara otomatis digunakan untuk menentukan program dan angka versi RPC. Beberapa port UDP diinformasikan dalam status open|filtered setelah scan port UDP tidak dapat menentukan apakah port terbuka atau disaring. Deteksi versi akan berusaha memperoleh respon dari port ini (sebagaimana dari port terbuka), dan merubah status port menjadi terbuka bila ia berhasil. Port TCP open|filtered diperlakukan dalam

cara yang sama. Perhatikan bahwa opsi -A di antaranya mengaktifkan deteksi versi.

Bila Nmap menerima respon dari sebuah layanan namun tidak dapat mencocokkannya ke database, ia akan mencetak fingerprint khusus dan sebuah URL untuk menyerahkannya bila anda tahu secara pasti apa yang berjalan pada port tersebut. Mohon meluangkan waktu beberapa menit untuk menyerahkannya sehingga dapat bermanfaat bagi semua orang. Berkat penyerahan ini, Nmap memiliki sekitar 3.000 pola yang sesuai untuk lebih dari 350 protokol seperti SMTP, FTP, HTTP, dsb.

3. OS Detection : menentukan OS apa yang digunakan suatu komputer pada suatu jaringan.

Salah satu fitur Nmap yang paling dikenal adalah deteksi SO dengan menggunakan fingerprint stack TCP/IP. Nmap mengirimkan serangkaian paket TCP dan UDP ke host remote dan menguji setiap bit paket responnya. Setelah melakukan serangkaian test seperti sampling TCP ISN, dukungan dan urutan opsi TCP, sampling ID IP, dan pemeriksaan ukuran jendela awal, Nmap membandingkan hasilnya ke database nmap-os-db yang berisi lebih dari seribu fingerprint SO yang dikenal dan mencetak detil SO bila terjadi kesesuaian. Setiap fingerprint menyertakan deskripsi SO tekstual dalam format bebas, klasifikasi yang memberikan nama vendor (misalnya Sun), SO di bawahnya (misalnya Solaris), generasi OS (misalnya 10), dan jenis device (fungsi umum, router, switch, konsol game, dsb.).

Jika Nmap tidak dapat menduga SO mesin, dan kondisinya bagus (misalnya paling tidak ditemukan satu port terbuka dan tertutup), Nmap akan memberikan URL yang dapat anda gunakan untuk menyerahkan fingerprint jika anda tahu (dengan pasti) SO yang berjalan di mesin itu. Dengan melakukan hal ini anda berkontribusi ke database sistem operasi yang dikenali Nmap dan karenanya ia akan lebih akurat.

Deteksi SO mengaktifkan beberapa tes lain yang menggunakan informasi yang dikumpulkan selama proses. Salah satunya adalah TCP Sequence Predictability Classification. Ukuran ini menentukan seberapa sulit memalsukan koneksi TCP ke host remote. Ia bermanfaat dalam mengeksploitasi relasi trust berbasis IP-sumber (rlogin, filter firewall, dsb) atau untuk menyembunyikan sumber serangan. Spoofing jenis ini jarang dilakukan lagi, namun banyak mesin masih rentan terhadapnya. Angka kesulitan aktualnya berdasarkan pada sampling statistik dan mungkin berfluktuasi. Umumnya lebih baik menggunakan klasifikasi bahasa Inggris seperti “worthy challenge” or “trivial joke”. Hal ini hanya dilaporkan dalam output normal dalam mode verbose (-v). Ketika digunakan mode verbose bersama dengan -O, pembuatan urutan ID IP ID juga dilaporkan. Kebanyakan mesin berada dalam kelas “incremental”, yang berarti mereka menaikkan field ID dalam header IP untuk setiap paket yang mereka kirim. Hal ini membuat mereka rentan atas beberapa serangan spoofing dan pengumpulan informasi tingkat tinggi.

Informasi ekstra lain yang disertakan dalam deteksi SO adalah menduga waktu uptime target. Tekniknya menggunakan opsi timestamp TCP (RFC 1323) untuk menduga waktu terakhir mesin direboot. Dugaan dapat tidak akurat akibat counter timestamp tidak diinisialisasi ke nol atau counter overflow dan kembali ke awal, sehingga ia hanya dicetak dalam mode verbose.

4. NMap Scripting Engine (NSE)

Nmap Scripting Engine (NSE) adalah salah satu fitur Nmap. NMap memungkinkan user untuk menulis (dan membagi) skrip sederhana (menggunakan bahasa pemrograman Lua,) untuk mengotomasi beragam tugas jaringan. Skrip-skrip tersebut dieksekusi secara parale dengan kecepatan dan efisiensi yang anda harapkan dari Nmap. User dapat mengandalkan beragam skrip yang didistribusikan dengan Nmap, atau menulis sendiri sesuai kebutuhan.

Untuk mencerminkan penggunaan yang berbeda dan untuk memudahkan pilihan skrip yang diinginkan, setiap skrip berisi field yang mengasosiasikannya dengan satu atau lebih kategori. Kategori yang ada saat ini adalah

safe, intrusive, malware, version, discovery, vuln, auth, and default.

4. Perbandingan analisa trafik antara Wireshark dengan NMap

Suatu jaringan seyogyanya mempunyai peraturan mengenai bagaimana sebuah obyek atau aktifitas data yang bergerak melintas dalam jaringan. Analisis jaringan berhubungan erat kaitannya dengan menjaga keamanan sebuah jaringan ; analisis berguna untuk memecahkan permasalahan yang terjadi dalam jaringan. Analisis jaringan adalah kegiatan mendengar dan mengamati segala aktifitas yang terjadi dalam jaringan baik komunikasi data dan sebagainya. Analisis jaringan berfungsi sebagai:

1. Penyelesaian masalah (Troubleshooting) jaringan.
2. Optimasi performa atau kinerja jaringan.
3. Perencanaan dan pengujian (Planning testing) jaringan.

Menjaga stabilitas dan reliabilitas sebuah kemampuan kinerja dan performa jaringan agar tidak mengganggu aktifitas penggunaan sistem jaringan. Oleh karena itu analisis terhadap lalu lintas data yang sedang berlangsung dalam sebuah jaringan dapat membantu dalam menjaga stabilitas dan reliabilitas performa jaringan. Wireshark merupakan Network Packet Analyzer yang memiliki kemampuan dalam menganalisis traffic packet data yang berkomunikasi di dalam jaringan, memiliki kecanggihan fitur dalam GUI-nya (Graphical User Interface). Oleh karenanya relative mempermudah dalam melakukan proses analysis. Tools yang digunakan dalam menganalisis trafik paket data disini adalah wireshark dan NMap. Berikut perbandingan antara wireshark dengan NMap ditunjukkan pada Tabel 1.

Tabel 1. Perbandingan Wireshark dengan NMap

No	Fitur	Wireshark	NMap
1	Model Program/Aplikasi	Installer/Portable	Installer
2	Tampilan Muka *(User Interface)*	GUI	GUI, Command
3	Platform	Windows, linux, OS X, Solaris, FreeBSD, NetBSD	Windows, linux, OS X, Solaris, FreeBSD, NetBSD
4	Distribusi Source Code	Open Source	Open Source
5	Scan Port	Ya	Ya
6	Dukungan Mode Script	Tidak	Ya
7	Scanning Packet	Ya	Ya
8	Deteksi SO Target	Tidak	Ya
9	Dukungan Network Interface	Ethernet, IEEE 802.11, Bluetooth, USB, Token Ring	Ethernet, IEEE 802.11,
10	Deteksi Service	Ya	Ya
11	Simpan hasil capture	Ya	Ya
12	Grafik Laporan	Ya	Ya
13	Mode Capture	Capture seluruh aktifitas jaringan	Capture berdasarkan target tujuan
14	Filter Capture	Ya	Tidak

5. Kesimpulan

Berdasarkan penjelasan pada makalah ini, dari tabel hasil perbandingan diatas yang didapat dari beberapa fitur antara wireshark dan NMap, terlihat bahwa tidak ada tools yang sempurna. Masing-masing tools memiliki kelebihan dan kekurangannya masing-masing.

Daftar Rujukan

[1] Sofana Iwan, Membangun jaringan komputer (Wire & Wireless) Untuk Pengguna Windows dan Linux, Informatika, 2008.
[2] Flickenger Rob, Jaringan Wireless di dunia berkembang, Creative Common Attribution ShareAlike 3.0, Edisi kedua, 2007, http://wndw.net.
[3] http://razmatech.com/keamanan-jaringan.html.
[4] http://www.wireshark.org.
[5] http://www.nmap.org.